TREND MICRO™

防毒墙网络版 10

适用于大中型企业

安装和升级指南

Endpoint Security

趋势科技 （中国）有限公司保留对本文档以及此处所述产品进行更改而不通知的权利。在安装并使用本软件之前，请阅读自述文件、发布说明和最新版本的用户文档，这些文档可以通过趋势科技的以下 Web 站点获得：

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

Trend Micro、 Trend Micro t- 球徽标、防毒墙网络版、控制管理中心、损害清除服务、防毒墙群件版、 ServerProtect 和 TrendLabs 都是趋势科技 （中国）有限公司/Trend Micro Incorporated 的商标、注册商标或服务商标。所有其他产品或公司名称可能是其各自所有者的商标或注册商标。

2001-2009 趋势科技 （中国）有限公司/Trend Micro Incorporated。保留所有权利。

文档编号 OSCM104080/90429

发布日期：2009 年 6 月

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

趋势科技防毒墙网络版的用户文档介绍该软件的主要功能组件以及针对贵组织生产环境的安装说明。在安装和使用该软件之前，请详细阅读。

有关如何使用软件中特定功能的详细信息，可在联机帮助文件和趋势科技 Web 站点上的在线知识库中获得。

趋势科技一直致力于改进其文档。如对该文档或趋势科技的任何其他文档有任何问题、意见或建议，请通过 **service@trendmicro.com.cn** 与我们联系。我们始终欢迎您的反馈。

目录

前言

防毒墙网络版文档 vi
读者 vii
文档规则 vii
术语 viii

第 1 章： 规划防毒墙网络版的安装和升级

全新安装需求 1-2
升级需求 1-7
防毒墙网络版 8.x 服务器 1-7
防毒墙网络版 8.x 客户端 1-9
防毒墙网络版 7.x 服务器 1-9
防毒墙网络版 7.x 客户端 1-11
产品版本与密钥 1-13
完全版和评估版 1-13
注册码和激活码 1-14
全新安装注意事项 1-14
防毒墙网络版服务器的位置 1-15
远程安装 1-15
服务器性能 1-15
专用服务器 1-16
安装期间的扫描方法部署 1-16
网络通信 1-17
第三方安全软件 1-19
Active Directory 1-19
Web 服务器 1-19

升级注意事项 1-20
防毒墙网络版设置和配置 1-20
不支持的操作系统 1-21
升级期间的扫描方法部署 1-22
安装和升级清单 1-22
规划试验部署 1-28
已知兼容性问题 1-28

第 2 章： 安装和升级防毒墙网络版

执行防毒墙网络版服务器的全新安装 2-2
升级防毒墙网络版服务器和客户端 2-2
升级方法 1：禁用自动客户端升级 2-3
升级结果 （联机客户端） 2-5
升级结果 （脱机客户端） 2-6
升级结果 （漫游客户端） 2-6
升级方法 2：将客户端移动到防毒墙网络版 10 服务器 2-6
升级结果 2-8
升级方法 3：启用自动客户端升级 2-9
升级结果 2-10
执行静默安装/升级 2-10
从评估版升级 2-12
安装程序安装窗口 2-12
许可协议 2-15
安装目标 2-16
预扫描 2-18
安装路径 2-19
代理服务器设置 2-20
Web 服务器设置 2-21
服务器计算机识别 2-24
注册和激活 2-25

集成型云安全服务器安装 2-27
远程安装目标 2-30
目标计算机分析 2-32
防毒墙网络版程序 2-33
Cisco Trust Agent 安装/升级 2-35
Cisco Trust Agent 许可协议 2-36
全球病毒实时监控计划 2-37
管理员帐户密码 2-38
客户端安装路径 2-39
防病毒功能 2-41
防间谍软件功能 2-42
程序文件夹快捷方式 2-43
安装信息 2-44
策略服务器安装 2-45
防毒墙网络版服务器安装完毕 2-46

安装后任务 2-47
验证服务器安装或升级 2-47
更新防毒墙网络版组件 2-49
检查缺省设置 2-49
使用 Client Mover for Legacy Platforms 2-50
将防毒墙网络版注册到控制管理中心 2-52
安装插件管理器 2-53

执行服务器卸载 2-53
在卸载防毒墙网络版服务器之前 2-53
卸载防毒墙网络版服务器 2-55

第 3 章： 获取帮助

故障排除资源 3-2
情况诊断工具 3-2
安装日志 3-2
服务器调试日志 3-3
客户端调试日志 3-4

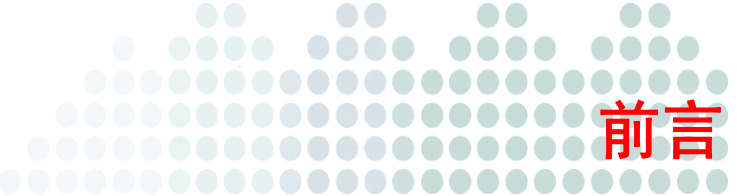
与趋势科技联系 3-5
技术支持 3-5
趋势科技知识库 3-6
TrendLabs 3-7
安全信息中心 3-7
将可疑文件发送给趋势科技 3-8
文档反馈 3-8

附录 A： 示例部署

基本网络 A-2

多个站点网络 A-2
总公司部署 A-4
远程站点 1 部署 A-5
远程站点 2 部署 A-6

附录 B： 旧版防毒墙网络版功能



前言

欢迎使用 《趋势科技™ 防毒墙网络版™ 安装和升级指南》。本文档介绍安装防毒墙网络版服务器以及升级服务器和客户端的需求和过程。

注意： 有关安装客户端的信息，请参阅 《管理员指南》。

本章主题：

- 第 vi 页的*防毒墙网络版文档*
- 第 vii 页的*读者*
- 第 vii 页的*文档规则*
- 第 viii 页的*术语*

防毒墙网络版文档

防毒墙网络版文档包括：

表 P-1. 防毒墙网络版文档

文档	描述
《安装和升级指南》	PDF 文档，介绍安装防毒墙网络版服务器以及升级服务器和客户端的需求和过程。
《管理员指南》	PDF 文档，介绍入门信息、客户端安装过程以及防毒墙网络版服务器和客户端管理。
趋势科技云安全扫描防毒墙网络版入门指南	PDF 文档，帮助用户了解云安全扫描概念，准备使用云安全扫描所需的环境，并管理云安全客户端。
帮助	编译为 WebHelp 或 CHM 格式的 HTML 文件，提供操作指导、使用建议和特定文本框的信息。可通过防毒墙网络版服务器、客户端、策略服务器控制台和防毒墙网络版主安装程序访问帮助。
自述文件	包含已知问题和基本安装步骤的列表。该文件可能还包含帮助或印刷文档中尚未包括的最新产品信息。
知识库	一个包含解决问题和故障排除信息的联机数据库。提供有关已知产品问题的最新信息。要访问知识库，请转到以下 Web 站点： http://cn.trendmicro.com/cn/support/techsupport/index.html

可从以下 Web 站点下载 PDF 文档和自述文件的最新版本：

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

读者

防毒墙网络版文档供以下用户使用：

- **防毒墙网络版管理员：**负责防毒墙网络版管理，包括服务器和客户端的安装和管理。这些用户应具有高级联网和服务器管理知识。
- **Cisco NAC 管理员：**负责使用 Cisco™ NAC 服务器和 Cisco 联网设备设计和维护安全系统。他们应具有使用此设备的经验。
- **最终用户：**在其计算机上安装了防毒墙网络版客户端的用户。他们的计算机技能不一，从初学者到高级用户不等。

文档规则

为了帮助您轻松地查找和解释信息，防毒墙网络版文档使用以下规则：

表 P-2. 文档规则

规则	描述
全大写	首字母缩略词、缩写以及某些命令和键盘按键的名称。
粗体	菜单和菜单命令、命令按钮、选项卡、选项和任务。
斜体	对其他文档或新技术组件的引用。
工具 > 客户端工具	在各个过程开头显示的“片语”帮助用户导航到相关 Web 控制台窗口。多条片语表明有多种转到同一窗口的方式。
<Text>	表明应将尖括号内的文本替换为实际数据。例如， C:\Program Files\<file_name> 可以是 C:\Program Files\sample.jpg。
注意： text	提供配置说明或建议。

表 P-2. 文档规则 （续）

规则	描述
提示： text	提供最佳做法信息和趋势科技建议。
警告！ text	提供有关可能危害网络中计算机的活动的警告。

术语

下表提供在整个防毒墙网络版文档中使用的正式术语：

表 P-3. 防毒墙网络版术语

术语	描述
客户端	防毒墙网络版客户端程序。
客户端计算机或端点	已安装防毒墙网络版客户端的计算机。
客户端用户 （或用户）	在客户端计算机上管理防毒墙网络版客户端的用户。
服务器	防毒墙网络版服务器程序。
服务器计算机	已安装防毒墙网络版服务器的计算机。
管理员 （或防毒墙网络版管理员）	管理防毒墙网络版服务器的人。
控制台	用于配置和管理防毒墙网络版服务器和客户端设置的用户界面 用于防毒墙网络版服务器程序的控制台称为 “Web 控制台”，而用于客户端程序的控制台称为 “客户端控制台”。
安全风险	病毒/恶意软件、间谍软件/灰色软件和 Web 威胁的统称。

表 P-3. 防毒墙网络版术语 （续）

术语	描述
产品服务	包括防病毒、损害清除服务以及 Web 信誉和防间谍软件 — 它们都是在防毒墙网络版服务器安装期间激活的。
防毒墙网络版服务	由 Microsoft 管理控制台 (MMC) 托管的服务。例如，防毒墙网络版主服务的 ofcservice.exe。
程序	包括防毒墙网络版客户端、Cisco Trust Agent 和插件管理器。
组件	负责对安全风险进行扫描、检测和采取处理措施。
客户端安装文件夹	计算机上包含防毒墙网络版客户端文件的文件夹。如果在安装期间接受缺省设置，您将在以下任一位置找到安装文件夹： **C:\Program Files\Trend Micro\OfficeScan Client** **C:\Program Files (x86)\Trend Micro\OfficeScan Client**
服务器安装文件夹	计算机上包含防毒墙网络版服务器文件的文件夹。如果在安装期间接受缺省设置，您将在以下任一位置找到安装文件夹： **C:\Program Files\Trend Micro\OfficeScan** **C:\Program Files (x86)\Trend Micro\OfficeScan** 例如，如果在服务器安装文件夹的 \PCCSRV 下找到一个特定的文件，则该文件的完整路径是： C:\Program Files\Trend Micro\OfficeScan\PCCSRV\<file_name>
云安全客户端	已配置为使用云安全扫描的防毒墙网络版客户端。
传统客户端	已配置为使用传统扫描的防毒墙网络版客户端。

第 1 章

规划防毒墙网络版的安装和升级

本章主题：

- 第 1-2 页的*全新安装需求*
- 第 1-7 页的*升级需求*
- 第 1-13 页的*产品版本与密钥*
- 第 1-14 页的*全新安装注意事项*
- 第 1-20 页的*升级注意事项*
- 第 1-22 页的*安装和升级清单*
- 第 1-28 页的*规划试验部署*
- 第 1-28 页的*已知兼容性问题*

全新安装需求

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

以下是执行防毒墙网络版服务器的全新安装的需求：

表 1-1. 防毒墙网络版服务器系统要求

资源	需求
操作系统	**Windows 2000** • 带有 Service Pack 4 的 Microsoft™ Windows™ 2000 Server • 带有 Service Pack 4 的 Windows 2000 Advanced Server • Microsoft Cluster Server 2000 安装以下项以使用基于角色的管理功能： • Microsoft Patch KB890859 • Microsoft Patch KB924270 • Windows 2000 授权管理器运行库 **Windows 2003** • 带有 Service Pack 2 的 Windows Server™ 2003 （Standard、Enterprise 和 Datacenter 版）或更高版本， 32 位和 64 位版本 • 带有 Service Pack 2 的 Windows Server 2003 R2 （Standard、Enterprise 和 Datacenter 版）或更高版本， 32 位和 64 位版本 • Windows Server 2003 R2， 32 位和 64 位版本 • Microsoft Cluster Server 2003

表 1-1. 防毒墙网络版服务器系统要求 （续）

资源	需求
	Windows 2008 • 带有 Service Pack 1 的 Windows Server 2008 （Standard、Enterprise、 Datacenter 和 Web 版）或更高版本， 32 位和 64 位版本 • Microsoft Cluster Server 2008 如果 Windows 2008 在服务器核心或 Hyper-V™ 环境中运行，则无法安装防毒墙网络版。
虚拟化	防毒墙网络版支持在以下虚拟化应用程序中托管的来宾 Windows 2000/2003/2008 操作系统中安装服务器： • VMware™ ESX™/ESXi Server 3.5 （服务器版） • VMware Server 1.0.3 或更高版本 （服务器版） • VMware Workstation 和 Workstation ACE Edition 6.0 也可以将服务器安装到带有 Service Pack 1 的 Microsoft Virtual Server 2005 R2 上托管的来宾 Windows 2000 和 2003 （32 位）操作系统上。

表 1-1. 防毒墙网络版服务器系统要求 （续）

资源	需求
硬件 （适用于 Windows Server 2008）	**处理器** • 至少 1GHz Intel™ Pentium™ 或同等 x86 处理器以及 1.4 GHz x64 处理器；建议使用 2 GHz 处理器 • 至少 1.86GHz Intel Core2Duo™ （如果安装集成型云安全服务器） • AMD™ 64 和 Intel 64 处理器体系结构 **内存** • 最低要求是 512MB，建议使用 2GB • 最低要求是 1GB （如果安装集成型云安全服务器） **可用磁盘空间** • 最低要求是 2.8 GB （如果本地安装防毒墙网络版服务器、防毒墙网络版客户端、策略服务器 for Cisco™ NAC 和集成型云安全服务器） • 最低要求是 3.2GB （如果远程安装防毒墙网络版服务器、防毒墙网络版客户端和集成型云安全服务器） **其他** • 千兆网络接口卡 (NIC) • 在颜色为 256 或更高时，支持分辨率 800 x 600 的显示器

表 1-1. 防毒墙网络版服务器系统要求 （续）

资源	需求
硬件 （适用于所有其他平台）	**处理器** • 800MHz Intel Pentium 或同等处理器 • 至少 1.86GHz Intel Core2Duo™ （如果安装集成型云安全服务器） **内存** • 最低要求是 512MB，建议使用 1GB • 最低要求是 1GB （如果安装集成型云安全服务器） **可用磁盘空间** • 最低要求是 2.8 GB （如果本地安装防毒墙网络版服务器、防毒墙网络版客户端、策略服务器 for Cisco NAC 和集成型云安全服务器） • 最低要求是 3.2GB （如果远程安装防毒墙网络版服务器、防毒墙网络版客户端和集成型云安全服务器） **其他** • 千兆网络接口卡 (NIC) • 在颜色为 256 或更高时，支持分辨率 800 x 600 的显示器

Web 服务器	• Microsoft Internet Information Server (IIS)
	  • 在 Windows 2000 上：版本 5.0
	  • 在 Windows Server 2003 上：版本 6.0
	  • 在 Windows Server 2008 上：版本 7.0
	• Apache™ Web server 2.0.x
	注意： 如果计算机中安装了非 2.0.x 版本的 Apache Web 服务器，防毒墙网络版将安装和使用 2.0.63 版。但不会删除现有的 Apache Web 服务器。

表 1-1. 防毒墙网络版服务器系统要求 （续）

资源	需求
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” • 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

以下是启动和访问 Web 控制台的需求。

表 1-2. Web 控制台需求

资源	需求
硬件	**处理器** 300MHz Intel Pentium 处理器或同等处理器 **内存** 最低要求是 128MB **可用磁盘空间** 最低要求是 30MB **其他** 在颜色为 256 或更高时，支持分辨率 800 x 600 的显示器
浏览器	Microsoft Internet Explorer™ 6.0 或更高版本

升级需求

此版本的防毒墙网络版支持从以下版本升级：

- 9.98 build 1017 （或防毒墙网络版 10 Beta IV）
- 8.x
  - 8.0
  - 8.0 Service Pack 1

  如果从 8.x 版升级，服务器和客户端可能需要其他计算机资源才能运行此版本的防毒墙网络版。有关详细信息，请参阅第 1-7 页的*防毒墙网络版 8.x 服务器*和第 1-9 页的*防毒墙网络版 8.x 客户端*。
- 7.x
  - 7.3
  - 7.0

  如果从 7.x 版升级，服务器和客户端可能需要其他计算机资源才能运行此版本的防毒墙网络版。有关详细信息，请参阅第 1-9 页的*防毒墙网络版 7.x 服务器*和第 1-11 页的*防毒墙网络版 7.x 客户端*。

防毒墙网络版 8.x 服务器

此版本支持 **8.x** 版支持的所有操作系统。

在升级之前，请执行以下任务：

1. 应用所需的 Microsoft Service Pack。
   - Service Pack 4 (Windows 2000 Server)
   - Service Pack 2 或更高版本 (Windows Server 2003)

2. 检查服务器计算机是否需要其他资源才能运行此版本的防毒墙网络版。有关详细信息，请参考下表。

表 1-3. 防毒墙网络版 10 和 8.x 服务器最低需求之间的差别

资源	防毒墙网络版 8.x 服务器需求	防毒墙网络版 10 服务器需求
处理器	800MHz Intel Pentium 或同等处理器	1.86GHz Intel Core2Duo™（如果安装集成型云安全服务器）
内存	512MB	1GB （如果安装集成型云安全服务器）
磁盘空间	1GB	• 2.8 GB （如果本地安装防毒墙网络版服务器、防毒墙网络版客户端、策略服务器 for Cisco NAC 和集成型云安全服务器） • 3.2GB （如果远程安装防毒墙网络版服务器、防毒墙网络版客户端和集成型云安全服务器）
Web 服务器	Apache Web 服务器 2.0 或更高版本	Apache Web 服务器 2.0.x
浏览器 （用于 Web 控制台和 Web 安装页）	带有 Service Pack 1 的 Microsoft Internet Explorer 5.5 或更高版本	Microsoft Internet Explorer 6.0 或更高版本

防毒墙网络版 8.x 客户端

此版本支持 **8.x** 版本支持的所有操作系统。

运行 Windows XP Professional 和 Windows Server 2008 的客户端需要其他的 Microsoft Service Pack。请在升级之前应用这些 Service Pack。

- Service Pack 2 或更高版本 (Windows XP Professional)
- Service Pack 2 或更高版本 (Windows Server 2003)
- Service Pack 1 或更高版本 (Windows Server 2008)

对于支持的其他操作系统，在 8.x 版中和在此版本中所需 Service Pack 是相同的。

防毒墙网络版 7.x 服务器

可以升级运行以下操作系统的防毒墙网络版 **7.x** 服务器：

- Windows 2000 Server
- Windows Server 2003

无法升级运行以下操作系统的防毒墙网络版服务器：

- Windows NT 系列
- Windows XP Professional

在升级之前，请执行以下任务：

1. 应用所需的 Microsoft Service Pack。
   - Service Pack 4 (Windows 2000 Server)
   - Service Pack 2 或更高版本 (Windows Server 2003)

2. 检查服务器计算机是否需要其他资源才能运行此版本的防毒墙网络版。有关详细信息，请参考下表。

表 1-4. 防毒墙网络版 10 和 7.x 服务器最低需求之间的差别

资源	防毒墙网络版 7.x 服务器需求	防毒墙网络版 10 服务器需求
处理器	300MHz Intel Pentium II 处理器或同等处理器	• 800MHz Intel Pentium 或同等处理器 • 1.86GHz Intel Core2Duo™（如果安装集成型云安全服务器）
内存	128MB	• 512MB • 1GB （如果安装集成型云安全服务器）
磁盘空间	• 600MB（防毒墙网络版 7.3） • 300MB（防毒墙网络版 7.0）	• 2.8 GB （如果本地安装防毒墙网络版服务器、防毒墙网络版客户端、策略服务器 for Cisco NAC 和集成型云安全服务器） • 3.2GB （如果远程安装防毒墙网络版服务器、防毒墙网络版客户端和集成型云安全服务器）
Web 服务器	Apache Web 服务器 2.0 或更高版本	Apache Web 服务器 2.0.x
浏览器（用于 Web 控制台和 Web 安装页）	带有 Service Pack 1 的 Microsoft Internet Explorer 5.5 或更高版本	Microsoft Internet Explorer 6.0 或更高版本

防毒墙网络版 7.x 客户端

可以升级运行以下操作系统的防毒墙网络版 **7.x** 客户端：

- Windows 2000
- Windows XP Professional
- Windows XP Home
- Windows Server 2003

无法升级运行以下操作系统的防毒墙网络版 7.x 客户端：

- Windows 95
- Windows 95 OSR2
- Windows 98
- Windows 98 SE
- Windows Me
- Windows NT 4.0
- Intel Itanium™ 体系结构操作系统

如果具有运行不支持的操作系统的客户端，并希望继续管理这些客户端，请保留防毒墙网络版 7.x 服务器。请参阅第 1-21 页的*不支持的操作系统*以获取详细信息。

提示：可以在防毒墙网络版 7.x 服务器 Web 控制台上检查客户端的操作系统。单击**客户端**并转至**平台**列。

Windows 2000

在升级运行 Windows 2000 的客户端之前，请执行以下任务：

1. 应用 Service Pack 4 或更高版本。
2. 检查客户端计算机是否需要其他资源才能运行此版本的防毒墙网络版。有关详细信息，请参考下表。

表 1-5. 防毒墙网络版 10 和 7.x 客户端最低需求之间的差别

资源	防毒墙网络版 7.x 客户端需求	防毒墙网络版 10 客户端需求
处理器	150MHz Intel Pentium 处理器或同等处理器	300MHz Intel Pentium 处理器或同等处理器
内存	64MB	256MB
磁盘空间	• 160MB（防毒墙网络版 7.3） • 80MB（防毒墙网络版 7.0）	350MB

Windows XP Professional、Windows XP Home 和 Windows Server 2003

在升级运行 Windows XP Professional、XP Home 和 Server 2003 的客户端之前，请执行以下任务：

1. 应用所需的 Microsoft Service Pack。
   - Service Pack 2 或更高版本 (Windows XP Professional)
   - Service Pack 3 (Windows XP Home)
   - Service Pack 2 或更高版本 (Windows Server 2003)

2. 检查客户端计算机是否需要其他资源才能运行此版本的防毒墙网络版。有关详细信息，请参考下表：

表 1-6. 防毒墙网络版 10 和 7.x 客户端最低需求之间的差别

资源	防毒墙网络版 7.x 客户端需求	防毒墙网络版 10 客户端需求
磁盘空间	• 160MB（防毒墙网络版 7.3） • 80MB（防毒墙网络版 7.0）	350MB
内存	128MB	256MB

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评估版。两个版本需要不同类型的激活码。如果没有激活码，请注册该产品。

完全版

完全版包括所有产品功能和技术支持，并在使用授权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订使用授权，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计算机不受最新安全风险的侵扰。通过在到期前或到期后购买维护续订来续订使用授权。

评估版

评估版包括所有产品功能。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、扫描和所有客户端功能。

注册码和激活码

在安装期间，安装程序提示您为以下服务指定激活码：

- 防病毒
- 损害清除服务™ （可选）
- Web 信誉和防间谍软件

如果没有激活码，请使用产品附带的注册码。安装程序自动地将您重定向到趋势科技 Web 站点，您可以在那里注册产品。

http://www.trendmicro.com.cn/corporate/techsupport/online_registration/cd.asp

在注册产品后，趋势科技将向您发送激活码。

如果没有注册码或激活码，请与趋势科技销售代表联系。有关详细信息，请参阅第 3-5 页的*与趋势科技联系*。

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

全新安装注意事项

在执行防毒墙网络版服务器的全新安装时，请注意以下事项：

- 第 1-15 页的*防毒墙网络版服务器的位置*
- 第 1-15 页的*远程安装*
- 第 1-15 页的*服务器性能*
- 第 1-16 页的*专用服务器*
- 第 1-16 页的*安装期间的扫描方法部署*
- 第 1-17 页的*网络通信*
- 第 1-19 页的*第三方安全软件*
- 第 1-19 页的 ***Active Directory***
- 第 1-19 页的 ***Web 服务器***

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端之间放置一个防火墙，或将服务器和所有客户端都放在单个网络防火墙之后。如果服务器和其客户端之间有防火墙，则将该防火墙配置为允许客户端和服务器侦听端口之间的网络通信。

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端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，安装程序会检查目标计算机是否满足服务器安装的需求。

确保安装可以继续：

- 在每台目标计算机上，使用管理员帐户而不是本地系统帐户启动 Remote Registry 服务。可从 Microsoft 管理控制台 （单击**开始 > 运行**，然后键入 **services.msc**）管理 Remote Registry 服务。
- 记录计算机的主机名和登录凭证 （用户名和密码）。
- 验证计算机是否满足防毒墙网络版服务器系统要求。有关详细信息，请参阅第 1-2 页的*全新安装需求*。

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 2GB 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端的数量取决于多个因素，如可用服务器资源和网络拓扑。请与趋势科技代表联系以帮助确定服务器可以管理的客户端数。

防毒墙网络版服务器通常可以管理的客户端的数量如下所述：

- 带有 2GHz 双处理器和 2GB 内存的防毒墙网络版服务器通常可以管理 3000 到 5000 个客户端
- 带有 3GHz 双处理器和 4GB 内存的防毒墙网络版服务器通常可以管理 5000 到 8000 个客户端

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：

- 计算机处理的 CPU 负载
- 如果计算机执行其他功能

如果目标计算机具有其他功能，请选择不运行关键应用程序或资源密集型应用程序的计算机。

安装期间的扫描方法部署

在此版本的防毒墙网络版中，可以将客户端配置为使用云*安全扫描*或*传统扫描*。

传统扫描

传统扫描是所有早期防毒墙网络版版本使用的扫描方法。传统客户端将所有防毒墙网络版组件存储在客户端计算机上，并在本地扫描所有文件。

云安全扫描

云安全扫描利用在云端存储的威胁签名。在云安全扫描模式中，防毒墙网络版客户端首先在本地扫描安全风险。如果客户端在扫描期间无法确定文件的风险，它将连接到云安全服务器。

云安全扫描具有以下功能和优点：

- 在云端提供快速、实时的安全状态查找功能
- 减少针对新出现的威胁提供防护所需的总体时间
- 减少在特征码更新期间占用的网络带宽大多数特征码定义更新只需要传送到云端，而不是许多端点
- 减少整个公司范围内特征码部署所涉及的成本和开销
- 降低端点上的内核内存占用。内存占用随时间的推移以最低限度增加。

扫描方法部署

如果执行防毒墙网络版服务器全新安装，且安装后未在 Web 控制台上更改扫描方法，则安装的所有客户端将使用传统扫描。在安装每个客户端后，可以将所有或一定数量的客户端配置为使用云安全扫描。有关详细信息，请阅读《趋势科技云安全扫描防毒墙网络版入门指南》中的部署准则。

网络通信

规划部署时，请考虑防毒墙网络版产生的网络通信。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
- 通知客户端下载更新的组件
- 通知客户端配置的更改

执行以下操作时客户端会产生网络通信：

- 启动
- 更新组件
- 更新设置和安装 hotfix
- 扫描安全风险
- 在漫游模式和普通模式之间切换
- 在传统扫描和云安全扫描之间切换

组件更新期间的网络通信

更新组件时，防毒墙网络版会产生大量的网络通信。为了减少在组件更新期间产生的网络通信，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。

定期更新的客户端只下载增量特征码。否则，它们下载完全特征码文件。

趋势科技将定期发布新的病毒码文件。一旦发现具有破坏性的病毒/恶意软件正在迅速传播后，趋势科技还会立即发布新的特征码文件。

更新代理和网络通信

如果客户端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，请将选定的防毒墙网络版客户端指定为更新代理，或其他客户端的更新源。这将帮助分摊向所有客户端部署组件的负担。

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，并充当本地网络上其他客户端计算机的分发点。有关更新代理的详细信息，请参阅 《管理员指南》。

趋势科技防毒墙控制管理中心和网络通信

趋势科技防毒墙控制管理中心管理位于网关、邮件服务器、文件服务器和企业桌面级别的趋势科技产品和服务。控制管理中心基于 Web 的管理控制台为整个网络内的产品和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。具有快速、可靠的 Internet 连接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。控制管理中心然后将这些组件部署到具有不可靠的 Internet 连接或没有 Internet 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，请参阅控制管理中心文档。

第三方安全软件

从将安装防毒墙网络版服务器的计算机删除第三方端点安全软件。这些应用程序可能会阻止防毒墙网络版服务器的成功安装或影响其性能。在删除第三方安全软件后立即安装防毒墙网络版服务器和客户端，以保护计算机免受安全风险的侵扰。

注意： 防毒墙网络版无法自动卸载任何第三方防病毒产品的服务器组件，但是可以卸载客户端组件。有关详细信息，请参阅《管理员指南》。

Active Directory

验证所有防毒墙网络版服务器是否为 Active Directory 域的一部分，以利用基于角色的管理和安全合规功能。

Web 服务器

防毒墙网络版 Web 服务器的功能如下：

- 允许用户访问 Web 控制台
- 从客户端接受命令
- 允许客户端响应服务器通知

可以使用 IIS Web 服务器或 Apache Web 服务器。如果使用 IIS Web 服务器，请确保服务器计算机没有运行 IIS 锁定的应用程序。在安装期间，安装程序自动停止再重新启动 IIS 服务。

如果使用 Apache Web 服务器，则管理员帐户是在 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，请创建运行 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、 Patch 和安全问题的最新信息，请参考 http://www.apache.org。

升级注意事项

在升级防毒墙网络版服务器和客户端时，请注意以下事项：

- 第 1-20 页的*防毒墙网络版设置和配置*
- 第 1-21 页的*不支持的操作系统*
- 第 1-22 页的*升级期间的扫描方法部署*

防毒墙网络版设置和配置

在升级防毒墙网络版服务器之前，备份防毒墙网络版数据库和重要配置文件。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。

备份和恢复防毒墙网络版数据库和配置文件：

1. 通过转至**管理 > 数据库备份**，从防毒墙网络版 **8.x/7.x** Web 控制台备份数据库。

   有关详细说明，请参阅这些产品版本的 《管理员指南》或服务器帮助。

   警告！ 不要使用任何类型的备份工具或应用程序。

2. 从 Microsoft 管理控制台停止防毒墙网络版主服务。
3. 手动备份在 <**服务器安装文件夹**>\PCCSRV 下找到的以下文件和文件夹：
   - **ofcscan.ini**：全局客户端设置
   - **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\OfcPfw2.dat**：包括防火墙设置
   - **Download\OfcPfw2.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
   - **HTTPDB 文件夹**：包括防毒墙网络版数据库

4. 升级防毒墙网络版服务器。有关详细信息，请参阅第 2-2 页的*升级防毒墙网络版服务器和客户端*。

注意： 如果遇到升级问题，请将步骤 3 中的备份文件复制到目标计算机上的 <**服务器安装文件夹**>\PCCSRV 文件夹，并重新启动防毒墙网络版主服务。

不支持的操作系统

防毒墙网络版不再支持 Windows 95、98、Me、NT 或 Itanium 体系结构平台。如果打算从防毒墙网络版 7.x 升级到此版本，并具有运行这些操作系统的防毒墙网络版 7.x 客户端：

1. 不要将所有的防毒墙网络版 7.x 服务器都升级到此版本的防毒墙网络版。
2. 至少指定一个防毒墙网络版 7.x 服务器（父服务器）来管理运行不支持的操作系统的客户端。
3. 在升级其他服务器之前：
   a. 为每个服务器打开 Web 控制台，并单击主菜单上的**客户端**。
   b. 从客户端树，选择要移动的客户端，然后单击**移动**。
   c. 在**将选定的客户端移动到另一个防毒墙网络版服务器**下指定父服务器的计算机名称/IP 地址和服务器侦听端口。
   d. 单击**移动**。

如果已升级防毒墙网络版服务器，但是没有移动不支持的客户端，请参阅第 2-50 页的*使用 Client Mover for Legacy Platforms* 以获取指导信息。

升级期间的扫描方法部署

在此版本的防毒墙网络版中，可以将客户端配置为使用**云安全扫描**或**传统扫描**。

如果从早期版本升级防毒墙网络版服务器，并且已启用自动客户端升级，则服务器管理的所有客户端在升级后自动使用传统扫描。在升级后，可以将所有或一定数量的客户端配置为使用云安全扫描。有关详细信息，请阅读《趋势科技云安全扫描防毒墙网络版入门指南》中的部署准则。

如果不打算部署云安全扫描，或者如果将在所有客户端升级后部署它，请参阅第 2-2 页的*升级防毒墙网络版服务器和客户端*。

安装和升级清单

在安装或升级防毒墙网络版服务器时，安装程序会提示您提供以下信息：

表 1-7. 安装清单

安装信息	期间所需信息			
	本地/静默全新安装	远程全新安装	本地/静默升级	远程升级
安装路径 缺省的服务器安装路径是： • C:\Program Files\Trend Micro\OfficeScan • C:\Program Files (x86)\Trend Micro\OfficeScan（*对于 x64 类型平台*） 如果选择不使用缺省路径，请确定安装路径。如果路径不存在，安装程序会为您创建它。	是	是	否	是

表 1-7. 安装清单 （续）

安装信息	期间所需信息			
	本地/静默全新安装	远程全新安装	本地/静默升级	远程升级
代理服务器设置 如果防毒墙网络版服务器通过代理服务器连接到 Internet，请指定以下内容： • 代理服务器类型 （HTTP 或 SOCKS 4） • 服务器名称或 IP 地址 • 端口 • 代理服务器认证凭证	是	是	否	是
Web 服务器设置 Web 服务器 （Apache 或 IIS Web 服务器）运行 Web 控制台 CGI 并接受来自客户端的命令。指定以下内容： • HTTP 端口：缺省端口是 8080。如果使用 IIS 缺省 Web 站点，请检查 HTTP 服务器的 TCP 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。大多数组织将这些端口号用作 HTTP 通信的缺省 TCP 端口。如果当前使用缺省端口号，请改用其他端口号。 *如果启用安全连接：* • SSL 证书有效期 • SSL 端口 （缺省：4343）	是	是	否	是

表 1-7. 安装清单 （续）

安装信息	期间所需信息			
	本地/静默全新安装	远程全新安装	本地/静默升级	远程升级
注册 注册产品以接收激活码。要进行注册，需要以下内容： *对于老用户* • 在线注册帐户 （登录名和密码） *对于没有帐户的用户* • 注册码	是	是	是	是
激活 获取以下产品服务的激活码： • 防病毒 • 损害清除服务 • Web 信誉和防间谍软件	是	是	是	是
集成型云安全服务器安装 如果选择安装集成型服务器，请指定以下内容： • SSL 证书有效期 • SSL 端口	是	是	是	是

表 1-7. 安装清单 （续）

安装信息	期间所需信息			
	本地/静默全新安装	远程全新安装	本地/静默升级	远程升级

远程安装目标
确定将安装/升级防毒墙网络版服务器的计算机。准备以下内容：
• 计算机名称或 IP 地址的列表
• （可选）一个包含目标计算机或 IP 地址列表的文本文件
文本文件内容示例：
`us-user_01`
`us-admin_01`
`123.12.12.123`
	否	是	否	是

远程安装计算机分析 安装程序在执行目标计算机分析之前提示您提供以下信息： • 目标计算机上具有“作为服务登录”权限的管理员帐户的用户名和密码	否	是	否	是
安装其他防毒墙网络版程序 如果安装 Cisco Trust Agent，请准备以下内容： • Cisco Trust Agent 证书文件	是	否	否	否
管理员帐户密码 安装程序会创建一个 root 帐户，以用于执行 Web 控制台登录。指定以下内容： • root 帐户密码 通过指定以下内容，防止在未经授权的情况下卸载或退出防毒墙网络版客户端： • 客户端卸载/退出密码	是	是	否	否

表 1-7. 安装清单（续）

安装信息	期间所需信息			
	本地/静默全新安装	远程全新安装	本地/静默升级	远程升级
客户端安装路径 指定将在客户端计算机上安装防毒墙网络版客户端的目录。指定以下内容： • 安装路径：缺省的客户端安装路径是 $ProgramFiles\Trend Micro\OfficeScan Client。如果选择不使用缺省路径，请确定安装路径。如果路径不存在，安装程序会在客户端安装期间创建它。 • 客户端通信端口号：防毒墙网络版随机生成端口号。接受生成的端口号或指定新的端口号。	是	是	否	否
程序文件夹快捷方式 防毒墙网络版服务器安装文件夹的快捷方式会显示在 Windows“开始”菜单中。缺省快捷方式名称是**趋势科技防毒墙网络版服务器-<Server_name>**。如果不希望使用此缺省名称，请确定其他名称。	是	否	否	否

表 1-7. 安装清单 （续）

安装信息	期间所需信息			
	本地/静默全新安装	远程全新安装	本地/静默升级	远程升级

策略服务器安装
如果选择安装策略服务器 for Cisco NAC，请准备以下信息：
• 安装路径：如果不接受缺省安装路径，请指定将在本地计算机上安装策略服务器的位置。
• Web 服务器配置：为选定的 Web 服务器指定以下设置：
  • HTTP 端口 （缺省：8081）
  • 如果启用安全连接：
  • SSL 证书有效期
• SSL 端口 （缺省：4344） Web 控制台密码：指定用于登录到策略服务器控制台的密码。
• ACS 服务器认证：ACS 服务器通过网络访问设备从客户端接收防毒墙网络版客户端防病毒数据，并将其传递到外部用户数据库以用于评估。指定登录凭证 （用户名和密码）。
	是	否	否	否

规划试验部署

执行全面部署前，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。它为安装团队提供了一个预演和改善部署过程的机会。它还允许您测试部署计划是否满足组织的安全计划。

有关示例防毒墙网络版部署，请参阅第 A-1 页的*示例部署*。

选择试验站点

选择与生产环境相匹配的试验站点。尝试模拟可充分演示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，请创建恢复计划或还原计划。

评估试验部署

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）。有关详细信息，请参考第三方应用程序的文档。

Microsoft Small Business Server

在运行 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服务器之前，记录 ISA 所用的服务器端口。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，则锁定以下防毒墙网络版文件可能会阻止防毒墙网络版客户端和服务器的通信：

- 配置 (.ini) 文件
- 数据 (.dat) 文件
- 动态链接库 (.dll) 文件
- 可执行 (.exe) 文件

防止 URLScan 干涉客户端-服务器通信：

1. 在防毒墙网络版服务器计算机上停止 World Wide Web Publishing 服务。
2. 修改 URLScan 配置文件以允许上面指定的文件类型。
3. 重新启动 World Wide Web Publishing 服务。

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端，则防毒墙网络版需要访问客户端要扫描的所有文件。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。此设置可以在 Web 控制台上进行配置（**联网计算机 > 全局客户端设置 > 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。

SQL Server

可以扫描 SQL Server™ 数据库。但是，这可能会降低访问数据库的应用程序的性能。请考虑将 SQL Server 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。如果要运行 ICF，请将防毒墙网络版侦听端口添加到 ICF 例外列表。有关如何配置例外列表的详细信息，请参阅防火墙文档。

第 2 章

安装和升级防毒墙网络版

本章主题：

- 第 2-2 页的*执行防毒墙网络版服务器的全新安装*
- 第 2-2 页的*升级防毒墙网络版服务器和客户端*
- 第 2-10 页的*执行静默安装/升级*
- 第 2-12 页的*从评估版升级*
- 第 2-12 页的*安装程序安装窗口*
- 第 2-47 页的*安装后任务*
- 第 2-53 页的*执行服务器卸载*

执行防毒墙网络版服务器的全新安装

要执行全新安装，请在满足防毒墙网络版服务器**全新安装需求**的计算机上运行安装程序。有关安装窗口和配置选项的信息，请参阅第 2-12 页的*安装程序安装窗口*。

安装服务器后，从 Web 控制台配置防毒墙网络版服务器设置，然后将防毒墙网络版客户端安装到计算机。

有关客户端的全新安装方法和指导信息，请参阅 《管理员指南》或防毒墙网络版服务器帮助。

升级防毒墙网络版服务器和客户端

根据网络带宽和防毒墙网络版服务器所管理的客户端数量，在服务器升级之后错开组中的客户端升级或立即升级所有客户端。

如果打算同时升级客户端和部署云安全扫描，请参阅 《趋势科技云安全扫描防毒墙网络版入门指南》。

如果在升级后所有客户端都将使用传统扫描，请使用以下升级方法之一：

- 第 2-3 页的*升级方法 1：禁用自动客户端升级*
- 第 2-6 页的*升级方法 2：将客户端移动到防毒墙网络版 10 服务器*
- 第 2-9 页的*升级方法 3：启用自动客户端升级*

升级方法 1：禁用自动客户端升级

通过禁用自动客户端升级，可以先升级服务器，然后升级组中的客户端。如果要升级大量的客户端，请使用此升级方法。

第 1 部分：在防毒墙网络版 8.x 或 7.x 服务器上配置更新设置和权限

对于防毒墙网络版 8.x：

1. 转至**更新 > 联网计算机 > 自动更新**。
2. 禁用以下选项：
   - 防毒墙网络版服务器下载完新组件后立即在客户端上启动组件更新。
   - 使客户端在重新启动并连接到防毒墙网络版服务器时启动组件更新（漫游客户端除外）。
3. 转至**联网计算机 > 客户端管理**。
4. 从客户端树，通过选择根图标 来选择所有客户端。
5. 单击**设置 > 权限和其他设置**，然后转至**其他设置**选项卡。
6. 启用**客户端可以更新组件，但不能升级客户端程序也不能部署 Hotfix**。
7. 单击**应用到全部客户端**。

对于防毒墙网络版 7.x：

1. 转至**更新 > 客户端部署 > 自动部署**。
2. 禁用以下选项：
   - 防毒墙网络版服务器下载完新组件后立即部署到客户端。
   - 重新启动客户端时部署到客户端 （仅适用于防毒墙网络版客户端，漫游客户端除外）。
3. 在主菜单上单击**客户端**。
4. 从客户端树，通过选择根图标 来选择所有客户端。
5. 单击**客户端权限/设置**。
6. 在 “更新设置”下，启用**禁止程序升级和 hotfix 部署**。

7. 单击**全部应用**。

提示： 如果网络环境复杂，并且有大量的客户端，则将设置部署到联机客户端可能需要一段时间。在升级之前，请分配足够的时间以便将设置部署到所有客户端。不应用设置的客户端将自动升级。

第 2 部分：升级防毒墙网络版服务器

有关升级防毒墙网络版服务器的详细信息，请参阅第 2-12 页的*安装程序安装窗口*。

完成安装之后但在升级客户端之前立即使用 Web 控制台配置防毒墙网络版服务器设置。有关如何配置防毒墙网络版设置的详细指导信息，请参考 《管理员指南》或防毒墙网络版服务器帮助。

第 3 部分：升级防毒墙网络版客户端

1. 转至**联网计算机 > 客户端管理**。
2. 在客户端树上，选择要升级的客户端。通过选择域或域中的特定客户端错开升级。

   提示： 首先升级更新代理。通过充当其他客户端的更新源，更新代理可帮助减少定向到防毒墙网络版服务器的流量。

3. 单击**设置 > 权限和其他设置**，然后转至**其他设置**选项卡。
4. 禁用**客户端可以更新组件，但不能升级客户端程序也不能部署 Hotfix**。
5. 转至**更新 > 联网计算机 > 自动更新**。
6. 启用以下选项：
   - 防毒墙网络版服务器下载完新组件后立即在客户端上启动组件更新。
   - 使客户端在重新启动并连接到防毒墙网络版服务器时启动组件更新（漫游客户端除外）。

升级结果 （联机客户端）

自动升级

当发生以下任一事件时联机客户端将开始升级：

- 防毒墙网络版服务器下载新组件并通知客户端进行更新。
- 客户端重新加载。
- 客户端重新启动，然后连接到防毒墙网络版服务器。
- 运行 Windows 2000、2003 和 XP Professional 的客户端计算机登录到使用登录脚本安装程序 (AutoPcc.exe) 修改其登录脚本的服务器。
- 预设更新运行在客户端计算机上 （仅适用于具有预设更新权限的客户端）。

手动升级

如果上述事件都未发生，则执行以下任一任务立即升级客户端：

- 创建并部署 EXE 或 MSI 客户端软件包。

  注意： 有关创建客户端软件包的指导信息，请参阅 《管理员指南》。

- 指示客户端用户在客户端计算机上运行**立即更新**。
- 如果客户端计算机运行 Windows 2000、 2003、 XP Professional、 2008 或 Vista™ （除 Vista Home 外的所有版本），请指示用户执行以下步骤：
  - 连接到服务器计算机。
  - 导航到 \\<服务器计算机名称>\ofcscan。
  - 启动 **AutoPcc.exe**。
- 如果客户端计算机运行 Windows XP Home 或 Vista Home，则指示用户右键单击 **AutoPcc.exe**，然后选择**以管理员身份运行**。
- 启动手动客户端更新。

启动手动客户端更新：

1. 转至**更新 > 联网计算机 > 手动更新**。
2. 选择**手动选择客户端**，然后单击**选择**。
3. 在打开的客户端树中，选择要升级的客户端。
4. 单击客户端树顶部的**启动组件更新**。

升级结果 （脱机客户端）

脱机客户端变为联机状态时，它们将升级。

升级结果 （漫游客户端）

漫游客户端变为联机状态时，或者运行预设更新时 （如果客户端具有预设更新权限），它们将升级。

升级方法 2：将客户端移动到防毒墙网络版 10 服务器

执行防毒墙网络版 10 服务器的全新安装，然后将客户端移动到此服务器。移动客户端时，它们将自动升级到防毒墙网络版 10。

第 1 部分：执行防毒墙网络版服务器的全新安装，然后配置服务器设置

1. 在计算机上执行防毒墙网络版 10 服务器的全新安装。有关详细信息，请参阅第 2-12 页的*安装程序安装窗口*。
2. 打开防毒墙网络版 10 Web 控制台，并转至**更新 > 联网计算机 > 自动更新**。
3. 启用以下选项：
   - 防毒墙网络版服务器下载完新组件后立即在客户端上启动组件更新。
   - 使客户端在重新启动并连接到防毒墙网络版服务器时启动组件更新（漫游客户端除外）。
4. 转至**联网计算机 > 客户端管理**。
5. 从客户端树选择根图标。
6. 单击**设置 > 权限和其他设置**，然后转至**其他设置**选项卡。
7. 禁用**客户端可以更新组件，但不能升级客户端程序也不能部署 Hotfix**。

8. 单击**应用到全部客户端**。
9. 记录以下防毒墙网络版 10 服务器信息。移动客户端时在防毒墙网络版 **8.x/7.x** 服务器上指定以下信息：
   - 计算机名称或 IP 地址
   - 服务器侦听端口

     要查看服务器侦听端口，请转至**管理 > 连接设置**。端口号将显示在该窗口上。

第 2 部分：升级防毒墙网络版客户端

对于防毒墙网络版 8.x：

1. 在 Web 控制台上，转至**更新 > 摘要**。
2. 单击**取消通知**。此功能清除服务器通知队列，这将防止将客户端移动到防毒墙网络版 10 服务器时出现问题。

警告！ **立即执行后续步骤。如果在移动客户端之前更新了服务器通知队列，则客户端可能无法成功移动。**

---

3. 转至**联网计算机 > 客户端管理**。
4. 从客户端树中选择要升级的客户端。通过选择域或域中的特定客户端错开升级。

提示： 首先升级更新代理。通过充当其他客户端的更新源，更新代理可帮助减少定向到防毒墙网络版服务器的流量。

---

5. 单击**管理客户端树 > 移动客户端**。
6. 在**将选定的客户端移动到另一个防毒墙网络版服务器**下，指定防毒墙网络版 10 服务器计算机名称/IP 地址和服务器侦听端口。
7. 单击**移动**。

对于防毒墙网络版 7.x：

1. 在 Web 控制台上，单击主菜单上的**客户端**。
2. 从客户端树中选择要升级的客户端。通过选择域或域中的特定客户端错开升级。

   提示： 首先升级更新代理。通过充当其他客户端的更新源，更新代理可帮助减少定向到防毒墙网络版服务器的流量。

3. 单击**移动**。
4. 在**将选定的客户端移动到另一个防毒墙网络版服务器**下，指定防毒墙网络版 10 服务器计算机名称/IP 地址和服务器侦听端口。
5. 单击**移动**。

升级结果

- 联机客户端开始移动并升级。
- 脱机客户端在变为联机状态时，它们将移动并升级。防毒墙网络版 8.x/7.x 服务器会继续管理这些客户端。
- 漫游客户端变为联机状态时，或者运行预设更新时 （如果客户端具有预设更新权限），它们将移动并升级。

注意： 可以在升级所有客户端后卸载防毒墙网络版 7.x 或 8.x 服务器。

升级方法 3：启用自动客户端升级

在将防毒墙网络版服务器升级到此版本后，服务器将立即通知它管理的所有客户端进行升级。

如果服务器管理的客户端数量很小，请考虑允许客户端立即升级。也可以使用前面讨论的升级方法。

第 1 部分：在防毒墙网络版 8.x 或 7.x 服务器上配置设置

对于防毒墙网络版 8.x：

1. 转至**更新 > 联网计算机 > 自动更新**。
2. 启用以下选项：
   - 防毒墙网络版服务器下载完新组件后立即在客户端上启动组件更新。
   - 使客户端在重新启动并连接到防毒墙网络版服务器时启动组件更新（漫游客户端除外）。
3. 转至**联网计算机 > 客户端管理**。
4. 从客户端树选择根图标。
5. 单击**设置 > 权限和其他设置**，然后转至**其他设置**选项卡。
6. 禁用**客户端可以更新组件，但不能升级客户端程序也不能部署 Hotfix**。
7. 单击**应用到全部客户端**。

对于防毒墙网络版 7.x：

1. 转至**更新 > 客户端部署 > 自动部署**。
2. 启用以下选项：
   - 防毒墙网络版服务器下载完新组件后立即部署到客户端。
   - 重新启动客户端时部署到客户端 （仅适用于防毒墙网络版客户端，漫游客户端除外）。
3. 在主菜单上单击**客户端**。
4. 从客户端树，通过选择根图标来选择所有客户端。
5. 单击**客户端权限/设置**。
6. 在 “更新设置”下，禁用**禁止程序升级和 hotfix 部署**。

7. 单击**全部应用**。

提示： 在升级防毒墙网络版服务器之前，分配足够的时间以便将设置部署到所有客户端。

第 2 部分：升级防毒墙网络版服务器

有关升级防毒墙网络版服务器的详细信息，请参阅第 2-12 页的*安装程序安装窗口*。

升级结果

- 在服务器升级完成后，联机客户端会立即升级。
- 脱机客户端变为联机状态时，它们将升级。
- 漫游客户端变为联机状态时，或者运行预设更新时 （如果客户端具有预设更新权限），它们将升级。

执行静默安装/升级

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

1. 可通过运行安装程序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：

   - 安装程序只显示本地安装 （全新安装或升级）的窗口。有关将显示的相关窗口，请参阅第 2-12 页的*安装程序安装窗口*。
   - 如果打算将防毒墙网络版服务器升级到此版本，请从安装有防毒墙网络版服务器的计算机创建响应文件。
   - 如果打算执行全新安装，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。

将安装程序配置记录到响应文件：

注意： 此过程不安装防毒墙网络版，它只将安装程序配置记录到响应文件。

1. 打开一个命令提示符，然后键入防毒墙网络版 **setup.exe** 文件的目录。例如，“CD C:\OfficeScan Installer\setup.exe”。
2. 键入以下命令：

   ```
   setup.exe -r
   ```

   - r 参数触发安装程序启动并将安装详细信息记录到响应文件。
3. 执行安装程序中的安装步骤。
4. 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，然后键入安装软件包的目录。
3. 键入以下命令：

   ```
   setup.exe -s <-f1path>setup.iss <-f2path>setup.log。
   ```

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

   其中：

   - **-s**：触发安装程序执行静默安装。
   - **<-f1path>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"。
   - **<-f2path>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。安装程序以静默方式将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

评估版快到期时，防毒墙网络版将在“摘要”窗口中显示一条通知消息。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。当有完全版使用授权时，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** > **产品使用授权**。将显示“产品使用授权”窗口。
3. 如果有激活码，请在**新激活码**文本框中键入它，然后单击**保存**。
4. 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。

安装程序安装窗口

下面列出了本地、远程或静默安装或升级防毒墙网络版服务器时显示的安装窗口（按顺序排列）。

表 2-1. 安装窗口和任务

窗口	本地/静默全新安装	远程全新安装	本地/静默升级	远程升级
欢迎使用	✓	✓	✓	✓
许可协议	✓	✓	✓	✓
安装目标	✓	✓	✓	✓
预扫描	✓	✓	✓	✓

表 2-1. 安装窗口和任务 （续）

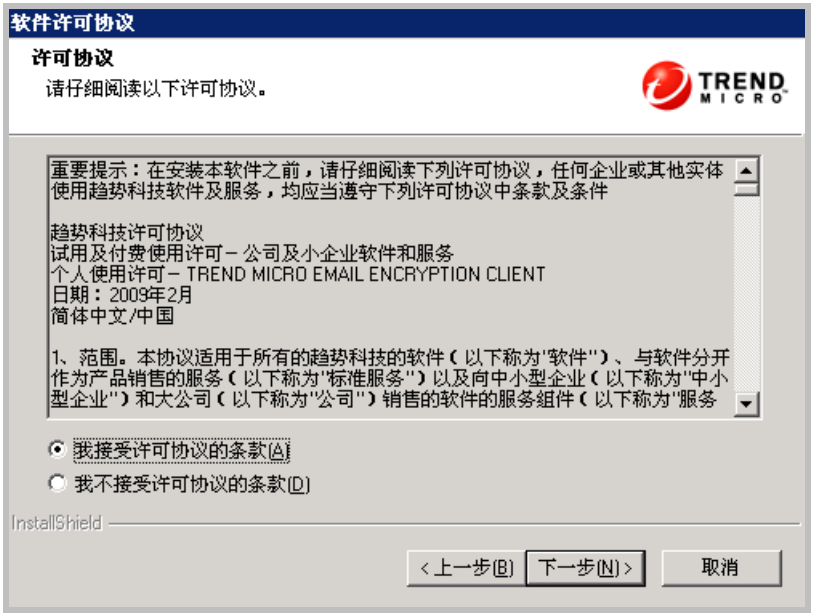
窗口	本地/静默全新安装	远程全新安装	本地/静默升级	远程升级
安装状态 （计算机分析） **注意：** 完成分析可能需要一些时间，尤其在 HTTP 服务器初始化期间。	✓		✓	
安装路径	✓	✓		✓
代理服务器设置	✓	✓		✓
Web 服务器设置	✓	✓		✓
服务器计算机识别	✓	✓		✓
注册和激活	✓	✓	✓	✓
集成型云安全服务器安装	✓	✓	✓	✓
远程安装目标		✓		✓
目标计算机分析		✓		✓
防毒墙网络版程序	✓	✓		✓
Cisco Trust Agent 安装/升级	✓			
Cisco Trust Agent 许可协议	✓			

表 2-1. 安装窗口和任务 （续）

窗口	本地/静默全新安装	远程全新安装	本地/静默升级	远程升级
全球病毒实时监控计划	✓	✓		
管理员帐户密码	✓	✓		
客户端安装路径	✓	✓		
防病毒功能	✓	✓		
防间谍软件功能 执行本地升级时，如果以前已激活 Web 信誉和防间谍软件使用授权，则不显示此窗口。	✓	✓	✓	✓
程序文件夹快捷方式	✓			
安装信息	✓	✓	✓	✓
防毒墙网络版服务器安装	✓	✓	✓	✓
策略服务器安装	✓			
防毒墙网络版服务器安装完毕	✓	✓	✓	✓

许可协议

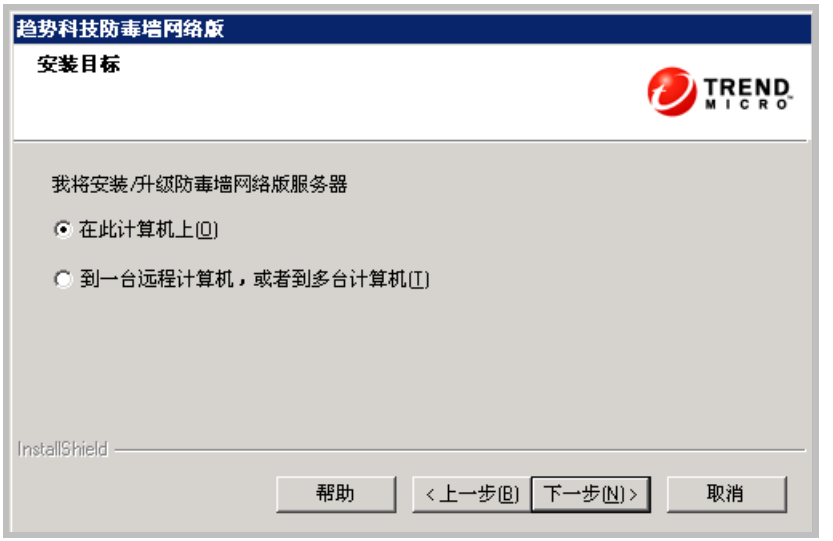
图 2-1. “许可协议”窗口



仔细阅读许可协议，只有接受许可协议条款后才能继续安装。如果不接受许可协议条款，则安装无法继续。

安装目标

图 2-2. “安装目标”窗口



运行安装程序，然后将防毒墙网络版服务器安装在安装程序启动时所在的计算机上或网络中的其他计算机上。如果安装程序检测到在目标计算机上有较早版本的防毒墙网络版，它将提示您升级。只有以下版本的防毒墙网络版可以升级到此版本：

- 9.98 build 1017 （或防毒墙网络版 10 Beta IV）
- 8.0
- 8.0 Service Pack 1
- 7.3
- 7.0

远程安装/升级说明

如果远程安装/升级，安装程序会检查目标计算机是否满足服务器安装/升级的需求。继续执行前：

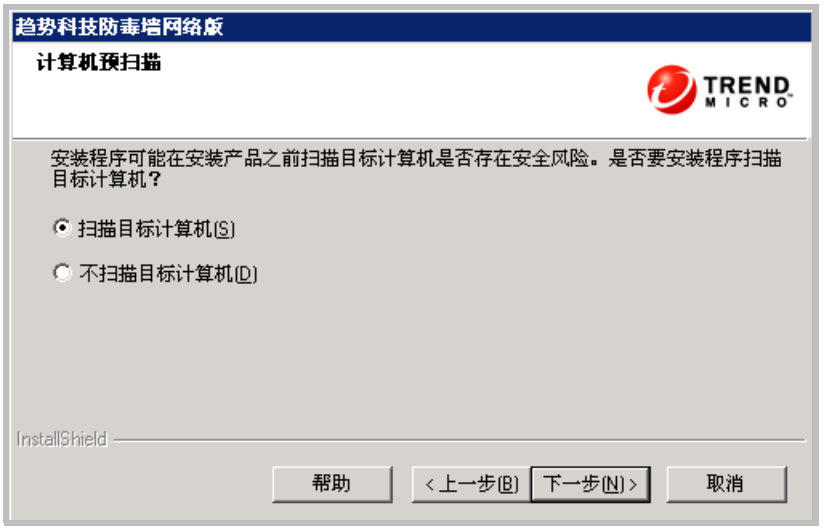
- 确保您对目标计算机具有管理员权限。
- 记录计算机的主机名和登录凭证（用户名和密码）。
- 验证目标计算机是否满足安装防毒墙网络版服务器的需求。
- 如果将此计算机用作 Web 服务器，请确保该计算机安装有 Microsoft IIS 服务器 5.0。如果选择使用 Apache Web 服务器，并且如果目标计算机中没有该服务器，安装程序将自动安装此服务器。

对于本地升级，防毒墙网络版将保持来自先前安装的原始设置，包括服务器名称、代理服务器信息和端口号。您无法在升级时修改这些设置。请在升级后从防毒墙网络版 Web 控制台修改它们。

对于远程升级，需要重新输入所有这些设置。但是，由于服务器将使用先前版本的设置，因此在服务器升级后这些设置将被忽略。

预扫描

图 2-3. “计算机预扫描”窗口



在防毒墙网络版服务器安装开始之前，安装程序会扫描目标计算机，查看是否存在病毒和恶意软件。安装程序扫描计算机中最容易受到攻击的区域，其中包括：

- 引导区和引导目录 （检查引导区病毒）
- Windows 文件夹
- Program Files 文件夹

安装程序可以对检测到的病毒/恶意软件和特洛伊木马程序执行以下处理措施：

- **删除**：删除受感染文件。
- **清除**：清除可清除的文件后才允许对该文件进行完全访问，或者使指定的下一处理措施处理非可清除文件。

- **更名：**将受感染文件的扩展名更改为 “vir”。用户最初不能打开该文件，但是将该文件与特定应用程序关联后即可打开该文件。打开更名的受感染文件时，病毒/恶意软件可能会执行。
- **不予处理：**允许完全访问受感染文件，而不对该文件执行任何操作。用户可以复制/删除/打开该文件。

如果执行本地安装，则在单击**下一步**时执行扫描。如果执行远程安装，则就在实际安装之前执行扫描。

安装路径

图 2-4. “安装路径”窗口

接受缺省安装路径或指定一个新路径。

仅当执行远程全新安装时，指定的安装路径才适用。对于远程升级，防毒墙网络版将使用先前版本的设置。

代理服务器设置

图 2-5. “代理服务器”窗口

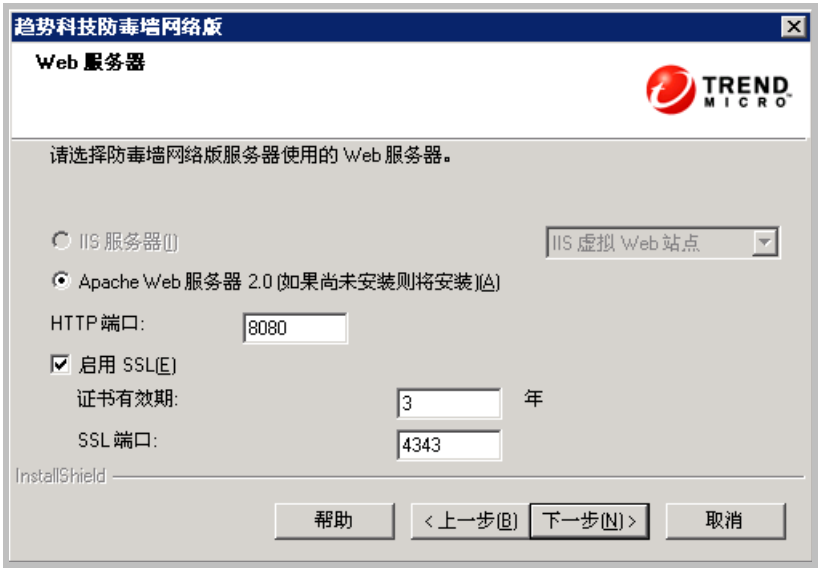
防毒墙网络版服务器使用 HTTP 协议进行客户端与服务器通信，以及连接到趋势科技 ActiveUpdate 服务器并下载更新。如果代理服务器处理网络上的 Internet 通信，则防毒墙网络版需要该代理服务器设置来确保该服务器可以从 ActiveUpdate 服务器下载更新。

您可以在安装期间跳过指定代理服务器设置，然后在安装后从防毒墙网络版 Web 控制台指定代理服务器设置。

仅当执行远程全新安装时，代理服务器设置才适用。对于远程升级，防毒墙网络版将使用先前版本的设置。

Web 服务器设置

图 2-6. “Web 服务器”窗口



防毒墙网络版 Web 服务器托管 Web 控制台，允许管理员运行控制台通用网关接口 (CGI) 以及接受来自客户端的命令。Web 服务器将这些命令转换为客户端 CGI，然后将它们转发给防毒墙网络版主服务。

仅当执行远程全新安装时， Web 服务器设置才适用。如果执行远程升级，则防毒墙网络版将使用先前版本的设置。

Web 服务器

如果安装程序检测到目标计算机上同时安装有 IIS 和 Apache Web 服务器，则您可以选择这两个 Web 服务器中的任何一个。如果在目标计算机上这两个服务器都不存在，则您无法选择 IIS，防毒墙网络版会自动安装 Apache Web 服务器 2.0.63。

如果使用 Apache Web 服务器:

- Apache Web 服务器 2.0.x 是必需的，并且只能在 Windows 2000、XP、2003 和 2008 上使用。如果计算机上存在 Apache Web 服务器，但版本不是 2.0.x，则防毒墙网络版将安装并使用 2.0.63 版。不删除现有的 Apache Web 服务器。
- 如果启用 SSL 且存在 Apache Web 服务器 2.0.x，则 Apache Web 服务器必须预配置有 SSL 设置。
- 默认情况下，管理员帐户是在 Apache Web 服务器上创建的唯一帐户。

提示： 趋势科技建议创建其他帐户，并从该帐户运行 Web 服务器。否则，如果恶意黑客控制了 Apache 服务器，防毒墙网络版服务器可能会非常危险。

- 安装 Apache Web 服务器之前，请参考 Apache Web 站点以了解有关升级、patch 和安全问题的最新信息。

如果使用 IIS Web 服务器:

- Windows 2000 需要 Microsoft Internet Information Server (IIS) 5.0 版；Windows Server 2003 需要 6.0 版；Windows Server 2008 需要 7.0 版。
- 不要将 Web 服务器安装在运行 IIS 锁定应用程序的计算机上，因为这可能阻止成功安装。有关详细信息，请参阅 IIS 文档。

HTTP 端口

Web 服务器在 HTTP 端口侦听客户端请求，然后将这些请求转发给防毒墙网络版主服务。此服务在指定的客户端通信端口将信息返回给客户端。在安装过程中，安装程序随机生成客户端通信端口号。

防毒墙网络版使用的端口号与 HTTP 服务器用于 TCP 网络通信的端口号相同。在许多组织中，此端口为端口 80 或 8080。防毒墙网络版缺省端口为 8080。

如果启用 SSL，防毒墙网络版将使用 SSL 端口 （缺省端口为 4343）替换该 HTTP 端口。

SSL 支持

如果想要在 Web 控制台与服务器之间，以及服务器与趋势科技 ActiveUpdate 服务器之间进行安全通信，请启用安全套接层 (SSL)。 SSL 提供了抵御黑客的额外防护层。尽管防毒墙网络版将在 Web 控制台上指定的密码发送到防毒墙网络版服务器之前会对它们进行加密，但黑客仍然可以嗅探数据包并且在不解密数据包的情况下“重放”数据包以获取对控制台的访问权限。SSL 隧道可阻止黑客嗅探穿过网络的数据包。

使用的 SSL 版本取决于 Web 服务器支持的版本。

如果选择了 SSL，安装程序将自动创建 SSL 连接所需的 SSL 证书。该证书包含服务器信息、公共密钥和私有密钥。

每个 SSL 证书的有效期为三年。在该证书过期后管理员仍然可以使用它。但是，每次使用同一证书调用 SSL 连接时都将显示警告消息。

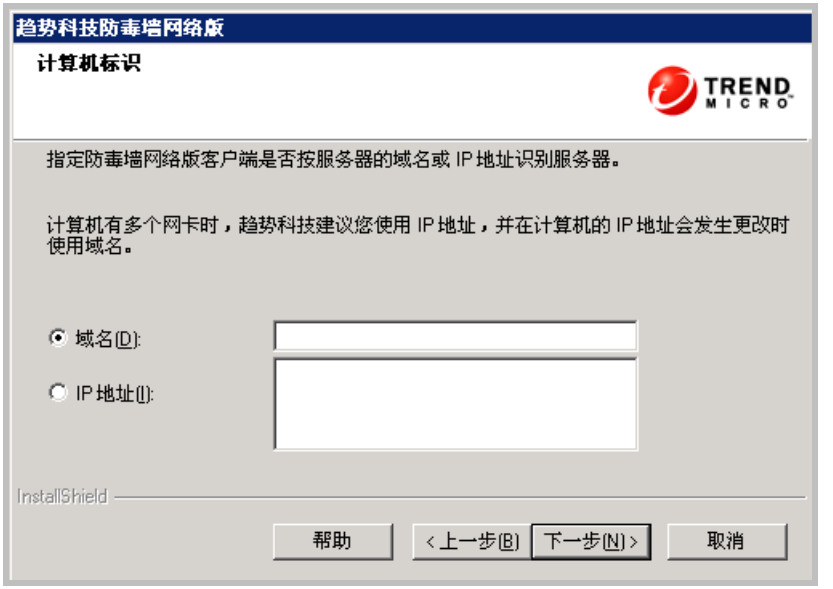
通过 SSL 进行通信的工作原理：

1. 管理员从 Web 控制台通过 SSL 连接向 Web 服务器发送信息。
2. Web 服务器使用所需的证书响应 Web 控制台。
3. 浏览器使用 RSA 加密执行密钥交换。
4. Web 控制台使用 RC4 加密向 Web 服务器发送数据。

虽然 RSA 加密更安全，但是它会降低通信流速度。因此，它只用于密钥交换，而 RC4 作为较快的替代方式用于数据传输。

服务器计算机识别

图 2-7. “计算机识别”窗口



仅当执行远程全新安装时，在此窗口上选择的选项才适用。对于远程升级，防毒墙网络版将使用先前版本的设置。

指定防毒墙网络版客户端是否按其域名或 IP 地址识别服务器计算机。

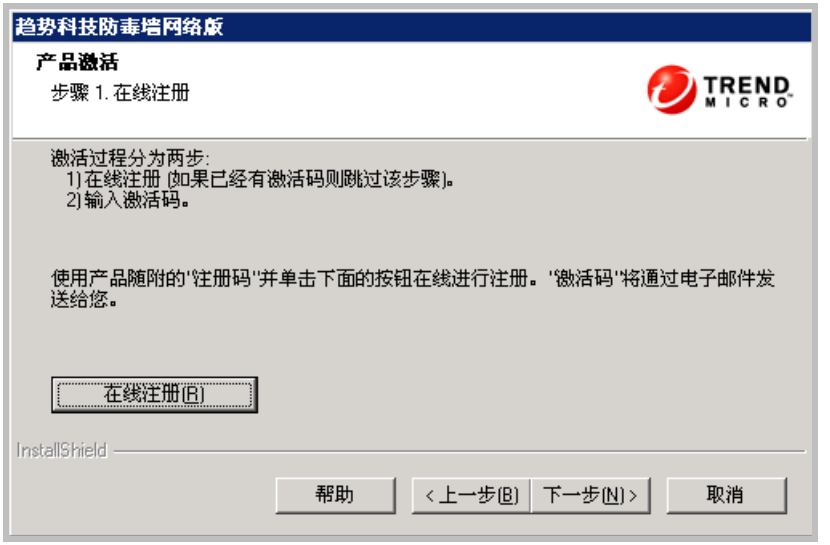
如果按 IP 地址识别服务器计算机，并且您更改了其 IP 地址，则防毒墙网络版服务器和客户端将无法进行通信。恢复通信的唯一方式是重新部署所有客户端。如果按域名识别服务器客户端，并且您更改了其域名，相同的处理方式也适用。

在大多数网络中，服务器计算机的 IP 地址比其域名更可能发生改变，因此通常首选按域名识别服务器计算机。如果防毒墙网络版从 DHCP 服务器获取 IP 地址，也不建议更改 IP 地址。

如果使用静态 IP 地址，请按服务器的 IP 地址识别服务器。此外，如果服务器计算机有多个网络接口卡 (NIC)，请考虑使用这些 IP 地址中的一个，而不要使用域名，这可确保客户端与服务器成功通信。

注册和激活

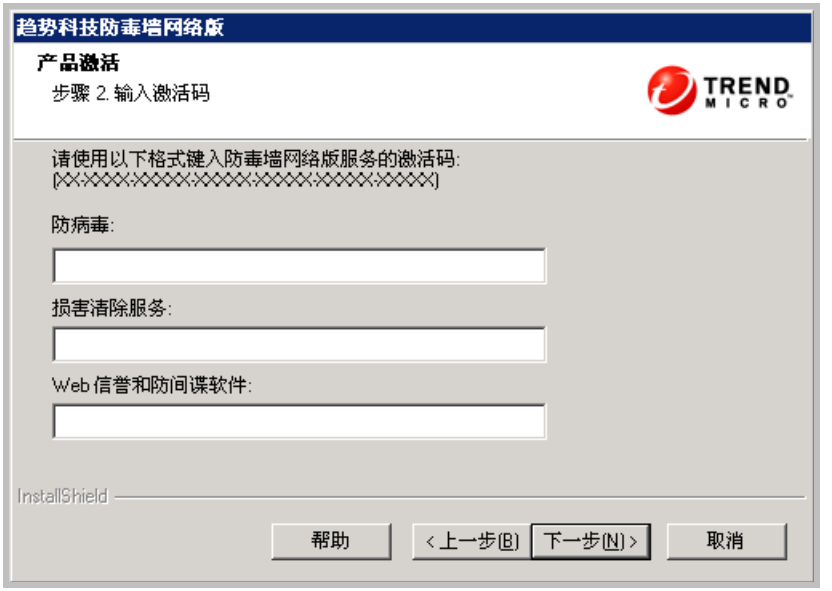
图 2-8. “产品注册”窗口



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。

如果您没有激活码，请单击**在线注册**。安装程序会将您引导到趋势科技注册网站。当您完成注册表单后，趋势科技会发送带有激活码的电子邮件。然后，您可以继续安装过程。

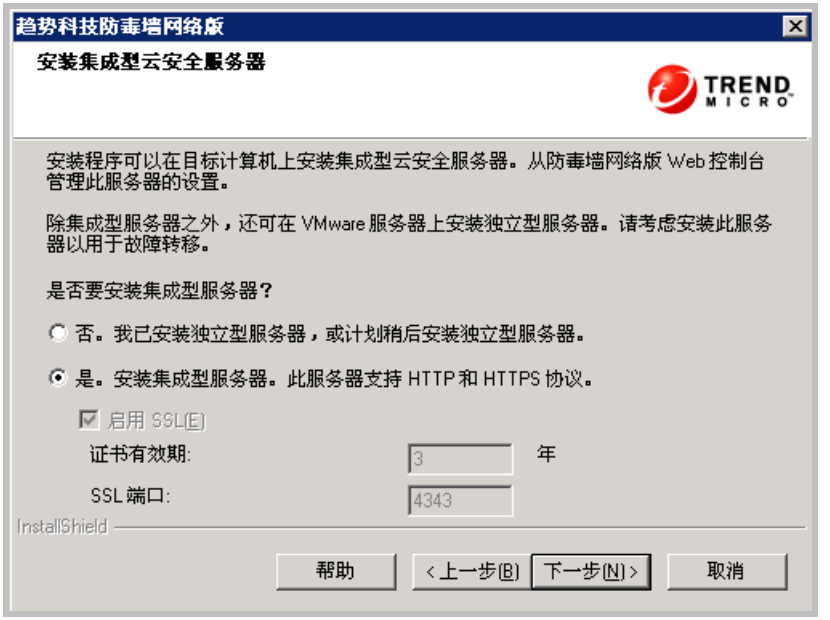
图 2-9. “产品激活”窗口



如果已经具有激活码，则继续安装过程并指定这些代码。激活码区分大小写。

集成型云安全服务器安装

图 2-10. “安装集成型云安全服务器”窗口



防毒墙网络版云安全扫描解决方案使用协同工作的轻量级特征码，该特征码可提供传统防恶意软件和防间谍软件特征码提供的相同防护。这些特征码源自趋势科技 ActiveUpdate 服务器，它们可用于云安全服务器和防毒墙网络版服务器。

云安全服务器托管云安全云端病毒码，该病毒码每小时更新一次，并且包含大多数的特征码定义。云安全客户端不下载此特征码。客户端通过将扫描查询发送到云安全服务器，根据特征码验证潜在威胁。

注意： 在云安全扫描解决方案中使用的名为“云安全客户端病毒码”的另一特征码，在防毒墙网络版服务器上托管并由客户端下载。

如果客户端可以连接到公司网络，则它会将扫描查询发送到本地云安全服务器。安装程序包括在安装防毒墙网络版服务器的同一计算机上安装的本地云安全服务器 （称为集成型云安全服务器）。在防毒墙网络版服务器 Web 控制台上管理集成型服务器的设置。

安装几个本地云安全服务器，以用于故障转移。除集成型服务器之外，还可在 VMware 服务器上安装独立型云安全服务器。独立型服务器具有与集成型服务器相同的作用和功能。它具有一个单独的管理控制台，而不是从防毒墙网络版 Web 控制台进行管理。有关独立型服务器的信息，请参阅 《趋势科技云安全扫描防毒墙网络版入门指南》。

提示：由于集成型云安全服务器和防毒墙网络版服务器在同一台计算机上运行，因此在这两个服务器的峰值流量过程中，计算机的性能可能会大大降低。要减少定向到防毒墙网络版服务器计算机的流量，请将独立型云安全服务器指定为主要扫描源，并将集成型服务器指定为备份源。有关配置客户端的扫描源的信息，请参阅 《管理员指南》。

使用授权

激活以下服务的使用授权以使用云安全扫描：

- 防病毒
- Web 信誉和防间谍软件

有关防毒墙网络版使用授权的详细信息，请参阅第 2-25 页的*注册和激活*。

如果不激活使用授权，仍然可以安装集成型云安全服务器，但是客户端将无法使用云安全扫描或连接到任何云安全服务器。请与趋势科技代表联系以了解使用授权和激活的注意事项。

客户端连接协议

客户端可以使用 HTTP 和 HTTPS 协议连接到集成型云安全服务器。 HTTPS 的连接更安全，而 HTTP 使用的带宽更小。

用于安全连接的 SSL 端口号取决于要用于防毒墙网络版服务器的 Web 服务器（Apache 或 IIS）。请参阅第 2-21 页的 ***Web 服务器设置***以获取详细信息。

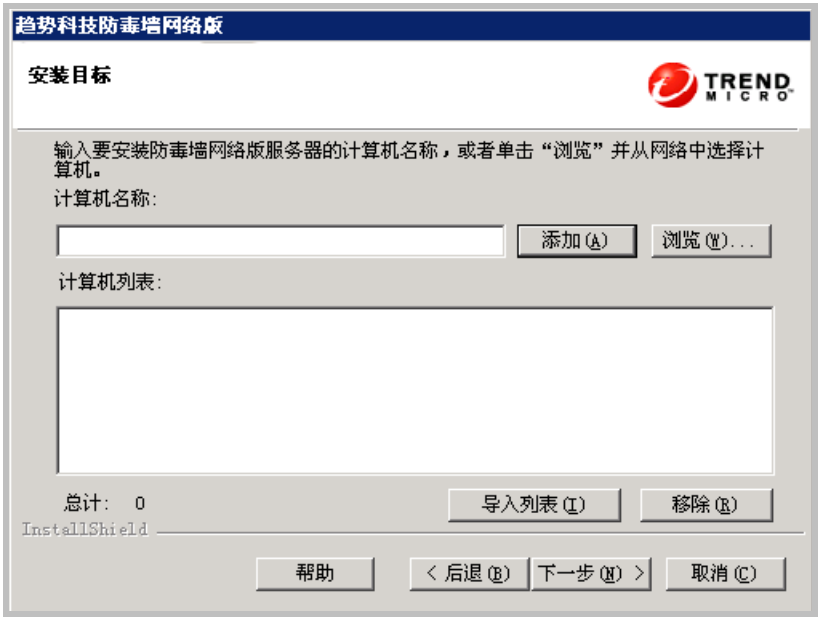
表 2-1. 防毒墙网络版服务器和集成型云安全服务器的 SSL 端口号

防毒墙网络版 Web 服务器设置	防毒墙网络版服务器 SSL 端口	集成型云安全服务器 SSL 端口
启用了 SSL 的 Apache Web 服务器	4343	4343
禁用了 SSL 的 Apache Web 服务器	N/A	4345
启用了 SSL 的 IIS 缺省 Web 站点	443	443
禁用了 SSL 的 IIS 缺省 Web 站点	N/A	443
启用了 SSL 的 IIS 虚拟 Web 站点	4343	4345
禁用了 SSL 的 IIS 虚拟 Web 站点	N/A	4345

如果客户端通过代理服务器连接到集成型服务器，则需要从 Web 控制台配置内部代理服务器设置。有关配置代理服务器设置的信息，请参阅 《管理员指南》。

远程安装目标

图 2-11. “远程安装目标”窗口



指定要安装防毒墙网络版的目标计算机。可以手动键入计算机的主机名或 IP 地址。单击**浏览**可以搜索网络中的计算机。

还可以通过单击**导入列表**从一个文本文件中导入计算机名。如果同时安装到多台计算机，并且所有计算机都通过了分析，安装程序会按它们在该文本文件中列出的顺序依次安装防毒墙网络版服务器。

在文本文件中：

- 每行指定一个计算机名。
- 使用统一命名约定 (UNC) 格式 （例如， \\test）。
- 只能使用以下符号：a-z、 A-Z、 0-9、半角句号 (.) 和 连字符 (-)。

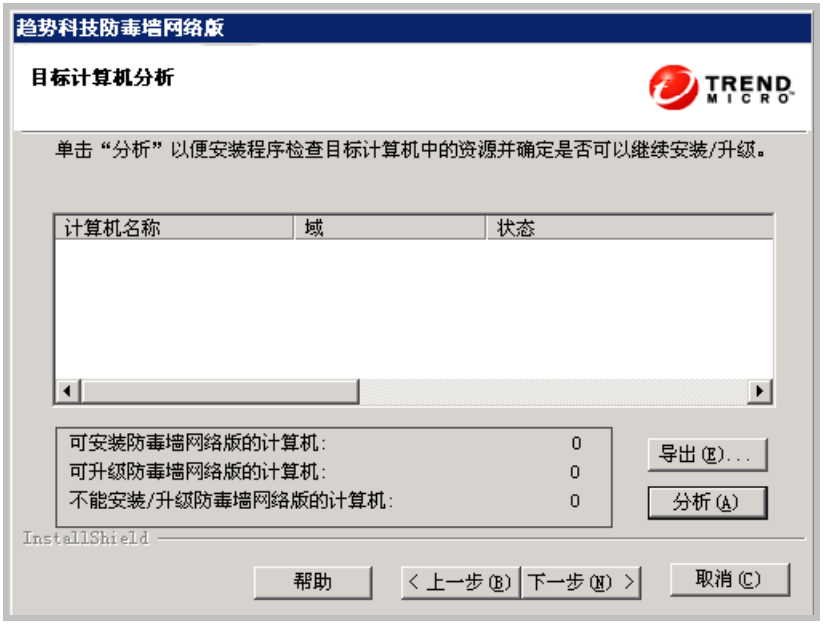
以下提示可确保远程安装可以继续：

- 确保您对目标计算机具有管理员权限。
- 记录计算机的主机名和登录凭证 （用户名和密码）。
- 验证目标计算机是否满足安装防毒墙网络版服务器的系统需求。
- 如果将此计算机用作 Web 服务器，请确保该计算机安装有 Microsoft IIS 服务器 5.0。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。
- 请勿将您启动安装程序所在的计算机指定为目标计算机。改为在计算机上运行本地安装。

指定目标计算机后，单击**下一步**。安装程序将检查这些计算机是否满足防毒墙网络版的安装需求。

目标计算机分析

图 2-12. “目标计算机分析”窗口



允许继续远程安装之前，安装程序需要先确定选定的目标计算机是否可以安装防毒墙网络版服务器。要开始分析，请单击**分析**。安装程序可能会要求您提供用于登录到目标计算机的管理员用户名和密码。分析后，安装程序会在窗口中显示结果。

当安装到多个计算机上时，如果至少一个计算机通过了分析，安装就会继续。安装程序会将防毒墙网络版服务器安装到该计算机上，并忽略未通过分析的计算机。

在远程安装期间，安装过程只在您启动安装程序所在的计算机中显示，而其他目标计算机不显示安装过程。

防毒墙网络版程序

图 2-13. “安装其他防毒墙网络版程序”窗口

选择安装以下防毒墙网络版程序：

防毒墙网络版客户端

客户端程序可提供抵御安全风险的实际防护。因此，要保护防毒墙网络版服务器计算机抵御安全风险，还需要有该客户端程序。选择在服务器安装期间安装客户端是一种确保自动保护服务器的便利方法。这样还避免了在安装服务器后安装客户端的其他任务。

注意： 在安装服务器后将该客户端安装到网络上的其他计算机。请参阅 《管理员指南》以了解客户端安装方法。

如果升级防毒墙网络版，则不显示此窗口。

如果当前在服务器计算机上安装了趋势科技或第三方端点安全软件，则防毒墙网络版也许能够或可能无法自动卸载该软件并将它替换为防毒墙网络版客户端。请与支持提供商联系以了解防毒墙网络版自动安装的软件的列表。如果无法自动卸载该软件，请先手动卸载它，再继续进行防毒墙网络版安装。

Cisco Network Admission Control (NAC) 程序

Cisco NAC 通过实施准入权限以及防病毒和安全策略，专注于控制网络内的安全风险。 Cisco NAC 允许客户端计算机与网络进行关于安全问题的通信。

类似于防毒墙网络版， Cisco NAC 具有服务器组件 （策略服务器 for Cisco NAC）和客户端组件 （Cisco Trust Agent 或 CTA）。要使用 Cisco NAC，需要有支持它的 Cisco 路由器，并且需要连接到 Cisco Admission Control Server (ACS)。

注意： 如果未激活防病毒服务，则 Cisco NAC 程序不可用。

如果执行远程服务器安装，您将无法安装/升级策略服务器或 CTA。执行远程安装后，从防毒墙网络版 Web 控制台将 CTA 安装到客户端，以及通过从防毒墙网络版安装程序软件包运行策略服务器安装程序安装策略服务器。有关 Cisco NAC 的详细信息，请参考 《管理员指南》。

策略服务器 for Cisco NAC

类似于防毒墙网络版 Web 控制台，策略服务器 for Cisco NAC 是基于 Web 的控制台，可以在其中配置网络准入策略。策略服务器会始终验证客户端特征码文件和扫描引擎是否最新。

可以在同一计算机和同一缺省 Web 站点上运行防毒墙网络版服务器和策略服务器，或者将它们安装到不同计算机上。如果将它们安装在同一台计算机上，安装程序可以在服务器安装期间同时安装它们，也可以在以后安装策略服务器。如果将策略服务器安装到其他计算机上，请在该计算机上运行策略服务器安装程序。

请从防毒墙网络版安装程序软件包访问策略服务器安装程序。

Cisco Trust Agent for Cisco NAC (CTA)

CTA （在防毒墙网络版服务器内托管并安装到客户端上的程序）使防毒墙网络版客户端可以将防病毒信息报告给 Cisco ACS。

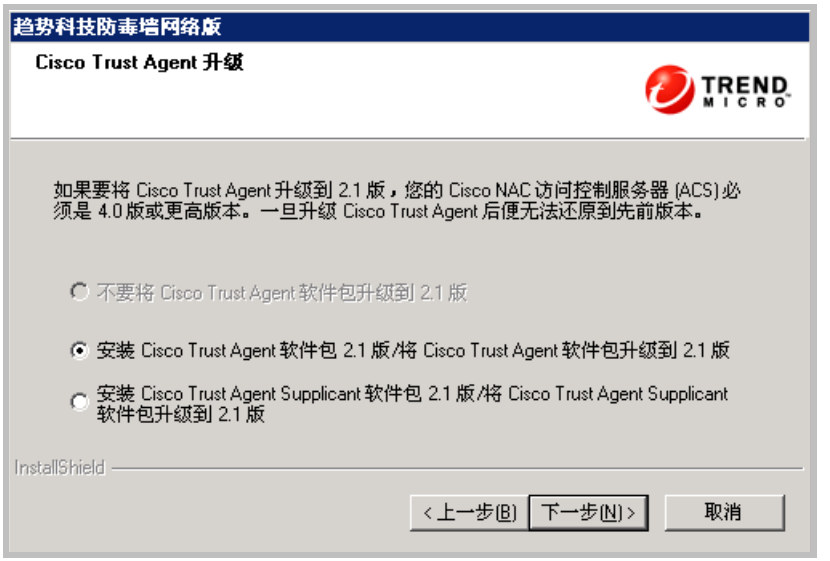
如果在服务器安装期间选中此选项，防毒墙网络版服务器会自动将 CTA 安装到该服务器将管理的所有客户端上。在下一窗口中，安装程序会提示要安装 Cisco Trust Agent 还是安装 Cisco Trust Agent Supplicant。这两个版本的唯一区别在于， Supplicant 软件包提供了用于计算机和最终用户的第 2 层认证。

如果不选择此选项，您仍然可以从 Web 控制台将 CTA 安装到客户端上（**Cisco NAC > 代理部署**）。但是，每次有新客户端添加到服务器上时您都需要执行此操作。有关从 Web 控制台安装 CTA 的信息，请参考防毒墙网络版服务器帮助。

CTA 安装需要一个证书文件 (.cer)， CTA 将使用此文件创建一个与 Cisco ACS 进行的加密通信会话。 Certificate Authority (CA) 服务器生成该证书文件。请向您的趋势科技代表请求证书文件，然后在服务器安装期间或从 Web 控制台输入该证书 （**Cisco NAC > 客户端证书**）。

Cisco Trust Agent 安装/升级

图 2-14. “Cisco Trust Agent 升级”窗口



如果执行全新安装，则仅当在前一窗口中选择安装 Cisco Trust Agent 时才显示此窗口。选择要安装到客户端的 CTA 软件包。

如果要升级，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)。如果要升级，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，则仍可以从 Web 控制台安装它。

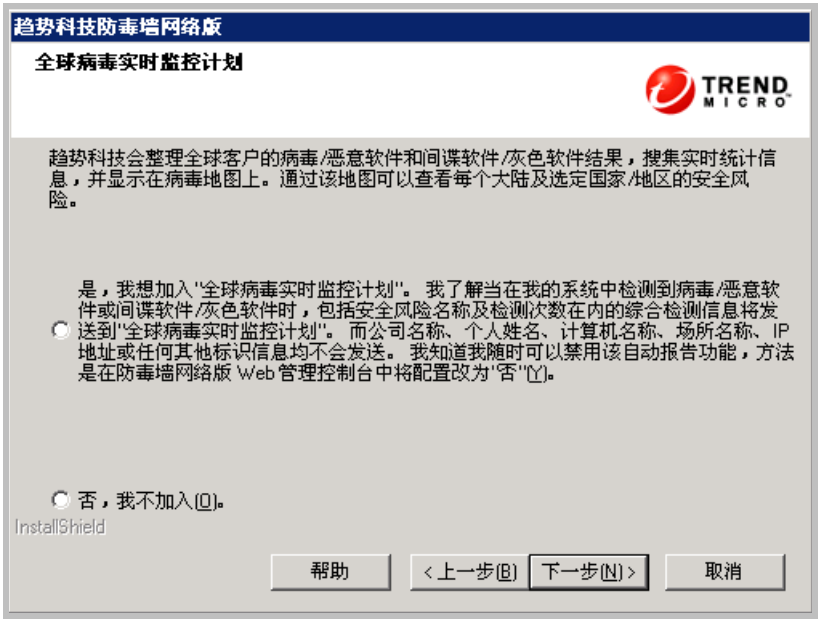
Cisco Trust Agent 许可协议

图 2-15. “Cisco Trust Agent 许可协议”窗口

仔细阅读许可协议，只有接受许可协议条款后才能继续安装。

全球病毒实时监控计划

图 2-16. “全球病毒实时监控计划”窗口



可将安全风险扫描结果发送到 “全球病毒实时监控计划”，以更好地监控安全风险爆发趋势。参加此项计划，有助于您尝试更好地了解安全风险的发展和传播。

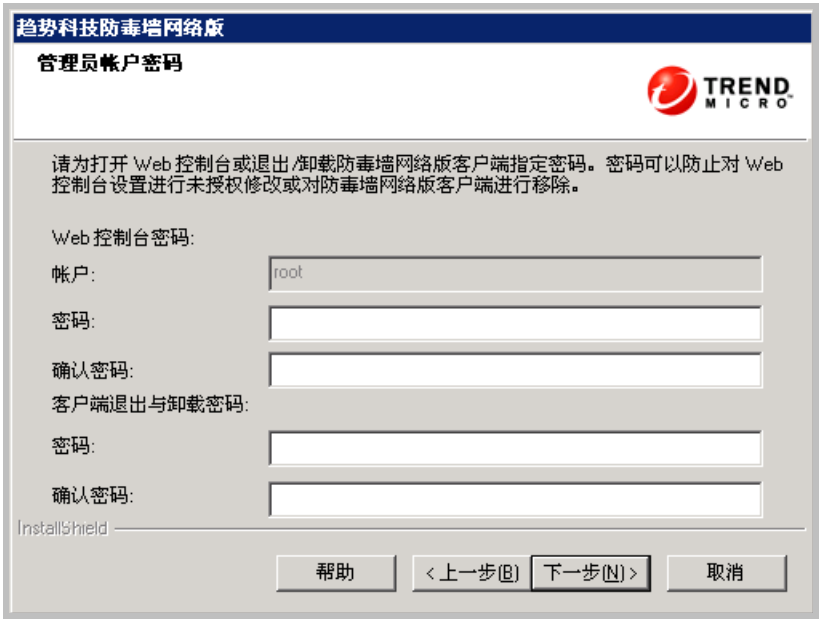
可以随时从 Web 控制台终止参与该计划。

要查看当前趋势科技病毒地图，请访问以下站点：

http://wtc.trendmicro.com/wtc/default.asp

管理员帐户密码

图 2-17. “管理员帐户密码”窗口



指定密码以执行以下操作：

访问 Web 控制台

在安装期间安装程序会创建 root 帐户。root 帐户拥有对所有防毒墙网络版 Web 控制台功能的完全访问权限。使用此帐户登录还允许管理员创建定制用户帐户，其他用户可以使用它们登录到 Web 控制台。用户可以配置或查看一个或多个 Web 控制台功能，具体取决于其帐户的访问权限。

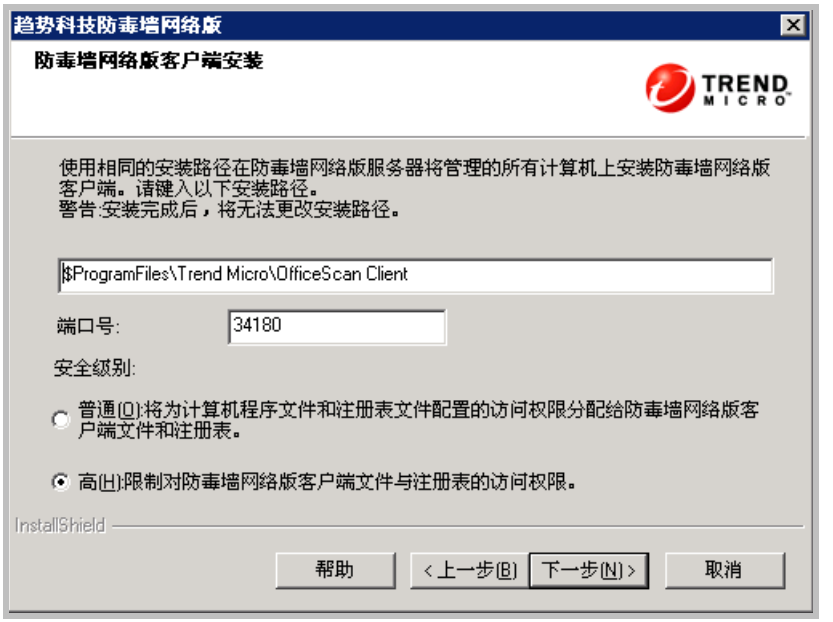
指定一个只有您和其他防毒墙网络版管理员知道的密码。如果忘记了密码，请与支持提供商联系以帮助重置密码。

退出和卸载防毒墙网络版客户端

指定密码以防止在未经授权的情况下卸载或退出防毒墙网络版客户端。仅当客户端功能存在问题时才卸载或退出客户端，并及时安装/重新加载它。

客户端安装路径

图 2-18. “防毒墙网络版客户端安装路径”窗口



接受缺省客户端安装设置或指定其他客户端安装路径。如果安装目录上的磁盘空间不足，请更改路径。

提示：趋势科技建议使用缺省设置。

如果指定其他安装路径，请键入静态路径或使用变量。如果键入的路径包括客户端上不存在的目录，安装程序将在客户端安装期间自动创建该目录。

在键入静态客户端安装路径时，请键入包括驱动器盘符的驱动器路径。例如，C:\Program Files\Trend Micro\OfficeScan Client。

注意： 在安装完防毒墙网络版服务器之后，就不能修改客户端安装路径了。将要安装的所有防毒墙网络版客户端都将使用同一安装路径。

为客户端安装路径指定变量时，请使用以下变量：

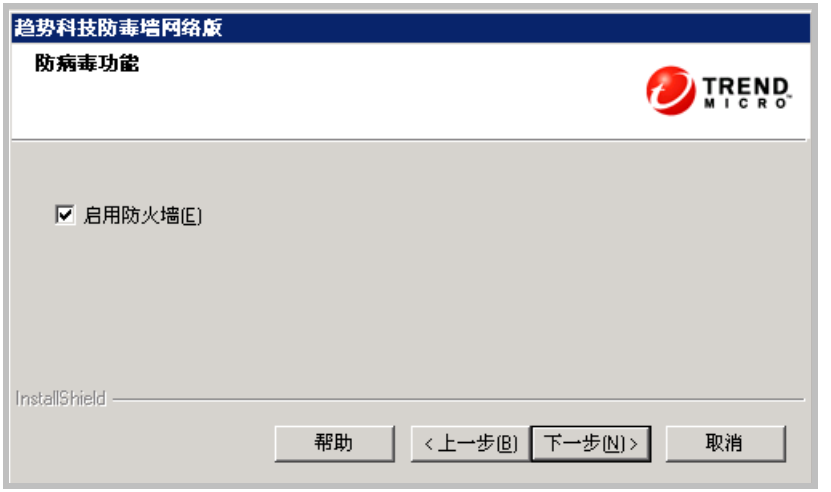
- **$BOOTDISK**：计算机启动硬盘的盘符，缺省为 C:\
- **$WINDIR**：Windows 目录，缺省为 C:\Windows
- **$ProgramFiles**：在 Windows 中自动创建的 Program Files 目录，通常用于安装软件，默认为 C:\Program Files

在此窗口上还可以配置以下设置：

- **端口号**：安装程序会随机生成此端口号，防毒墙网络版服务器使用此端口号与客户端通信。可以指定其他端口号。
- **安全级别**：安装防毒墙网络版后，可以从防毒墙网络版控制台更改安全级别（**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 其他设置**）
  - **普通**：允许客户端对客户端计算机上的防毒墙网络版客户端文件夹、文件和注册表进行读/写操作。
  - **高**：限制客户端访问防毒墙网络版客户端文件夹、文件和注册表（缺省）。如果选择 “高”，则防毒墙网络版文件夹、文件和注册表的访问许可设置将从 Program Files 文件夹继承 （对于运行 Windows 2000、 XP 或 Server 2003 的客户端计算机）。

防病毒功能

图 2-19. “防病毒功能”窗口



仅当激活防病毒服务时，才显示此窗口。

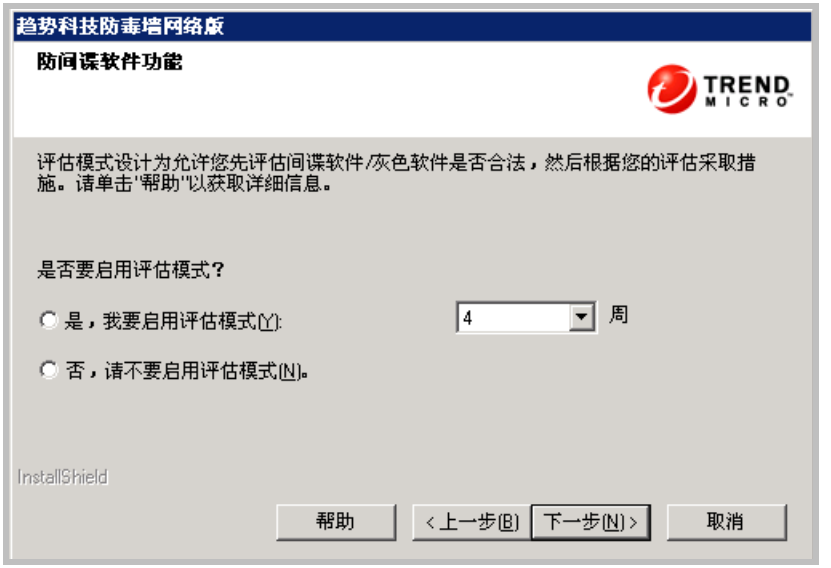
防毒墙网络版防火墙

防毒墙网络版防火墙使用基于状态的检查、高性能的网络病毒扫描和清除来保护网络上的客户端和服务器。可以创建按 IP 地址、端口号或协议过滤连接的规则，然后将这些规则应用到不同的用户组中。

可以选择禁用防火墙，稍后从防毒墙网络版服务器 Web 控制台启用它。

防间谍软件功能

图 2-20. “防间谍软件功能”窗口



仅当激活 Web 信誉和防间谍软件服务时，才显示此窗口。

处于评估模式时，服务器管理的所有客户端都将记录在手动扫描、预设扫描、实时扫描和立即扫描期间检测到的间谍软件/灰色软件，但是不会清除间谍软件/灰色软件组件。清除操作将终止进程或删除注册表项、文件、 cookie 和快捷方式。

趋势科技提供评估模式以允许您评估趋势科技检测为间谍软件/灰色软件的项目，然后根据您的评估配置适当的处理措施。例如，如果您认为检测出的间谍软件/灰色软件不存在安全风险，则可以将其添加至间谍软件/灰色软件允许列表。

安装后，请参考《管理员指南》以了解要在评估模式期间采取的建议处理措施。

通过在此窗口中指定星期数，将评估模式配置为只在特定时期内生效。安装后，可以从 Web 控制台更改评估模式设置（**联网计算机 > 全局客户端设置 > 仅间谍软件/灰色软件扫描设置**）。

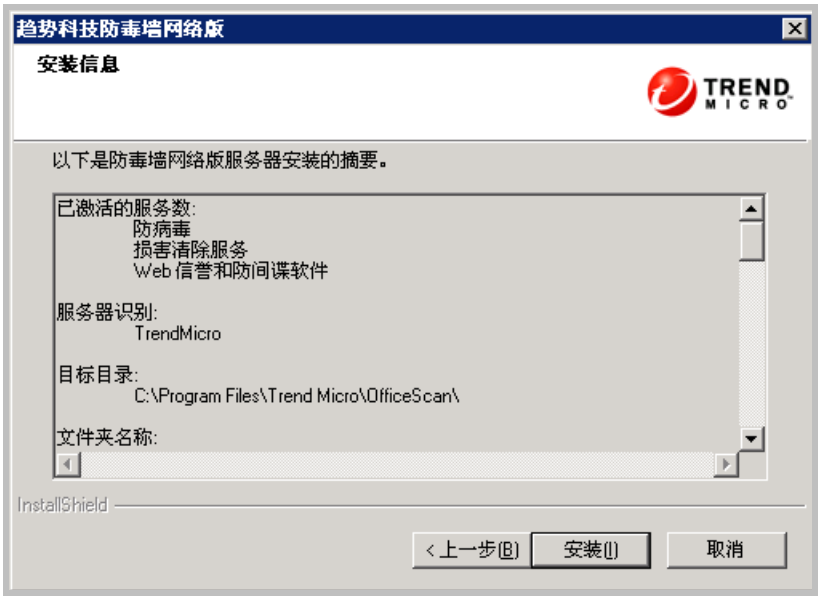
程序文件夹快捷方式

图 2-21. “防毒墙网络版程序快捷方式”窗口

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

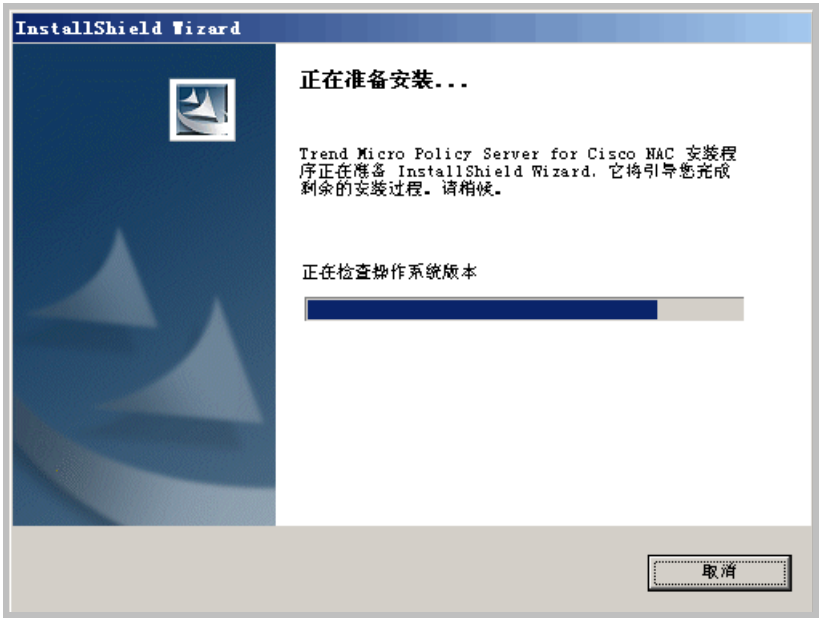
图 2-22. “安装信息”窗口



此窗口提供安装设置的摘要。查看安装信息并单击**上一步**更改任一设置或选项。要开始安装，请单击**安装**。

策略服务器安装

图 2-23. “策略服务器安装”窗口



如果选择安装策略服务器 for Cisco NAC，则将显示此窗口。“策略服务器安装”窗口上显示的设置和选项与在防毒墙网络版服务器安装期间指定的大多数设置类似。

- **许可协议：**接受许可协议的条款以继续。
- **安装路径：**接受缺省安装路径或者指定将在本地计算机上安装策略服务器的位置。
- **Web 服务器：**指定是否使用 IIS 或 Apache Web 服务器。
- **Web 服务器配置：**为选定的 Web 服务器指定设置。
- **Web 控制台密码：**指定用于访问策略服务器控制台的密码。虽然可以从防毒墙网络版启动该控制台，但是该控制台独立于防毒墙网络版服务器控制台。

- **ACS 服务器认证：**ACS 服务器通过网络访问设备从客户端接收防毒墙网络版客户端防病毒数据，并将其传递到外部用户数据库以用于评估。在稍后的过程中， ACS 服务器还会将评估的结果 （其中可能包括防毒墙网络版客户端的说明）传递到网络访问设备。
- **安装信息：**查看安装信息。

防毒墙网络版服务器安装完毕

图 2-24. “安装完毕”窗口

安装完毕后，查看自述文件以了解有关产品和已知问题的基本信息。

还可以启动 Web 控制台以开始配置防毒墙网络版设置。

安装后任务

执行以下安装后任务：

- 第 2-47 页的*验证服务器安装或升级*
- 第 2-49 页的*更新防毒墙网络版组件*
- 第 2-49 页的*检查缺省设置*
- 第 2-50 页的*使用 Client Mover for Legacy Platforms*。仅当具有运行 Windows 95、98、Me、NT 或 Itanium 体系结构的客户端时才执行此任务。
- 第 2-52 页的*将防毒墙网络版注册到控制管理中心*。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。
- 第 2-53 页的*安装插件管理器*

验证服务器安装或升级

完成安装或升级后，验证以下内容：

表 2-2. 安装或升级防毒墙网络版后要验证的项目

要验证的项目	详细信息
防毒墙网络版服务器快捷方式	服务器计算机的 Windows **开始**菜单中将出现趋势科技防毒墙网络版服务器的快捷方式。
程序列表	**趋势科技防毒墙网络版服务器**在服务器计算机控制面板的**添加/删除程序**列表中列出。
防毒墙网络版 Web 控制台	在 Internet Explorer 浏览器上键入以下 URL： • HTTP 连接：http://<OfficeScan server name>:<port number>/OfficeScan • HTTPS 连接：https://<OfficeScan server name>:<port number>/OfficeScan 其中 <OfficeScan server name> 是防毒墙网络版服务器的名称或 IP 地址。 将显示 Web 控制台登录窗口。

表 2-2. 安装或升级防毒墙网络版后要验证的项目 （续）

要验证的项目	详细信息
防毒墙网络版服务器服务	在 Microsoft 管理控制台上将显示以下防毒墙网络版服务器服务： • 防毒墙网络版主服务 （应该正在运行） • 趋势科技云安全服务器 （如果已安装集成型云安全服务器，启动类型为 “手动”） • 趋势科技策略服务器 for Cisco NAC （如果已安装） • 防毒墙网络版 Active Directory 集成服务 （如果基于角色的管理功能正常工作） • OfficeScan 控管中心代理
防毒墙网络版服务器进程	打开 Windows 任务管理器时，以下防毒墙网络版进程正在运行： • OfcService.exe • DBServer.exe • iCRCService.exe （如果已安装集成型云安全服务器） • OfcCMAgent.exe （如果防毒墙网络版服务器已注册到控制管理中心）
服务器安装日志	服务器安装日志 OFCMAS.LOG 存在于 %windir% 中。
注册码	存在以下注册码： HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan
程序文件夹	防毒墙网络版服务器文件可在 <**服务器安装文件夹**> 下找到。

更新防毒墙网络版组件

安装或升级防毒墙网络版后，在服务器上更新组件。

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。如果这些设置不符合您的安全需求，请在 Web 控制台上对其进行修改。有关 Web 控制台上可用设置的详细信息，请参考防毒墙网络版服务器帮助和 《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计算机免受安全风险的侵扰。通过转至**联网计算机 > 客户端管理 > 设置 > {扫描类型}**，从 Web 控制台修改扫描设置。

全局客户端设置

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端，或者具有特定权限的所有客户端。通过转至**联网计算机 > 全局客户端设置**，从 Web 控制台修改全局客户端设置。

客户端权限

缺省客户端权限包括在客户端控制台上显示**邮件扫描**和**工具箱**选项卡。通过转至**联网计算机 > 客户端管理 > 设置 > 权限和其他设置**，从 Web 控制台修改缺省客户端权限。

使用 Client Mover for Legacy Platforms

防毒墙网络版客户端不再支持 Windows 95、98、Me、NT 或 Itanium 体系结构平台。如果防毒墙网络版客户端运行其中任一平台，并且已将管理它们的服务器升级到版本 10：

- 将不升级防毒墙网络版客户端。
- 防毒墙网络版 10 服务器会停止管理客户端。这些客户端的状态将变为“断开连接”。
- 防毒墙网络版 10 服务器将客户端的信息保存到一个名为 **unsupCln.txt** 的文件。使用此文件将客户端 “移动”到具有相同版本的服务器。移动意味着指定新的服务器来管理客户端。
- 在防毒墙网络版 10 服务器计算机上，运行名为 Client Mover for Legacy Platforms 的工具。此工具通知客户端它们将由一个新服务器管理，并检查是否已成功移动客户端。当客户端收到通知时，它们将注册到其新的父服务器。

移动客户端：

1. 准备一个新的父服务器。此服务器的版本应该与要移动的客户端的版本相同。
2. 记录服务器的计算机名称/IP 地址和服务器侦听端口。这些详细信息是移动客户端时所必需的。

   通过转至**管理 > 连接设置**，从服务器的 Web 控制台获取服务器侦听端口。
3. 在防毒墙网络版 10 服务器计算机上，导航到 <服务器安装文件夹>\PCCSRV\Admin\Utility\ClientMover，然后运行 **clientmover.exe**。

4. 在命令窗口中，键入以下命令：

   ClientMover /P:<ExportDataPath> /S:<ServerIP:port> /N

   其中：

   - **ExportDataPath**：包含客户端信息的文件 (unsupCln.txt) 的路径和文件名。
   - **ServerIP:port**：新父服务器的 IP 地址和服务器侦听端口号。
   - **/N**：一个命令，用于通知客户端，然后将客户端移动到新父服务器。此命令与 /V 命令结合使用。

   例如：

   ClientMover /P:"C:\Program Files\TrendMicro\OfficeScan\PCCSRV\Private\unsupcln.txt" /S:123.12.12.123:23456 /N

5. 使用 /V 命令可验证该工具是否已成功移动客户端。此命令会将防毒墙网络版 10 服务器的 IP 地址与新父服务器的 IP 地址进行比较。如果 IP 地址相同，则该工具将无法移动客户端。

   例如：

   ClientMover /P:"C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Private\unsupcln.txt" /S:123.12.12.123:23456 /V

6. 检查结果：

   a. 在 \PCCSRV\Private\ 中访问结果日志。日志的文件名是 unsupcln.txt.log.<date_time>。

      例如：unsupcln.txt.log.20080101_123202

   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。备份文件的名称是 unsupcln.txt.bak。

   已更新的 unsupcln.txt 文件中的示例条目：

   ```
   ------------------------------------------------------------
   x12xx345-6xxx-78xx-xx91-234x567x8x91 1234567891 23456 0
   ------------------------------------------------------------
   ```

其中：

- “x12xx345-6xxx-78xx-xx91-234x567x8x91”是客户端的 GUID。
- “1234567891”是客户端的 IP 地址 （十进制）。
- “23456”是客户端侦听端口。
- “0”是结果，它表示通知已完成。

  其他可能的结果：

  - 1 = 客户端通知成功
  - 2 = 客户端通知不成功
  - 3 = 验证成功
  - 4 = 验证不成功

unsupcln.txt.log.<date_time> 文件中的示例条目：

```
------------------------------------------------------------
x12xx345-6xxx-78xx-xx91-234x567x8x91 123.12.12.123:23456
无法发送通知。请检查网络或客户端状态。
------------------------------------------------------------
```

其中：

- “x12xx345-6xxx-78xx-xx91-234x567x8x91”是客户端的 GUID。
- “123.12.12.123:23456”是客户端的 IP 地址和侦听端口。
- 结果是 “无法发送通知。请检查网络或客户端状态”。

7. 使用 /F 命令可以不检查当前客户端状态而强制通知或验证。

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*防毒墙网络版服务器帮助*。

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端的插件程序。从 Web 控制台安装和管理上述程序，包括将客户端插件程序部署到客户端。

通过在 Web 控制台的主菜单上单击**插件管理器**来下载插件管理器。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： 有关安装需求和指导信息，请参考插件管理器自述文件。

执行服务器卸载

如果使用防毒墙网络版服务器时遇到问题，请使用卸载程序从计算机安全地删除服务器程序，然后再重新安装它。

在卸载防毒墙网络版服务器之前

在卸载服务器之前，请将它管理的客户端移动到具有相同版本的防毒墙网络版服务器。如果打算稍后重新安装服务器，请考虑备份服务器数据库和配置文件。

将客户端移动到其他防毒墙网络版服务器

防毒墙网络版 Web 控制台提供了一个选项，可用于将服务器管理的客户端移动到其他防毒墙网络版服务器。

将客户端移动到其他防毒墙网络版服务器：

1. 记录其他防毒墙网络版服务器的以下信息。在移动客户端时，将需要这些信息。
   - 计算机名称或 IP 地址
   - 服务器侦听端口

     要查看服务器侦听端口，请转至**管理 > 连接设置**。端口号将显示在该窗口上。

2. 在要卸载的服务器的 Web 控制台上，转至**联网计算机 > 客户端管理**。
3. 从客户端树中选择要升级的客户端，然后单击**管理客户端树 > 移动客户端**。
4. 在**将选定的客户端移动到另一个防毒墙网络版服务器**下，指定其他防毒墙网络版服务器的服务器计算机名称/IP 地址和服务器侦听端口。
5. 单击移动。

如果所有客户端都已移动且已由其他防毒墙网络版服务器管理，则卸载防毒墙网络版服务器是安全的。

备份和恢复防毒墙网络版数据库和配置文件

在卸载防毒墙网络版服务器之前，备份防毒墙网络版数据库和重要配置文件。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。

备份和恢复防毒墙网络版数据库和配置文件：

1. 通过转至**管理 > 数据库备份**，从防毒墙网络版 Web 控制台备份数据库。有关指导信息，请参阅 《管理员指南》或防毒墙网络版服务器帮助。

   警告！ 不要使用任何类型的备份工具或应用程序。

2. 从 Microsoft 管理控制台停止防毒墙网络版主服务。
3. 手动备份在 <服务器安装文件夹>\PCCSRV 下找到的以下文件和文件夹：
   - **ofcscan.ini**：全局客户端设置
   - **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\OfcPfw2.dat**：包括防火墙设置
   - **Download\OfcPfw2.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
   - **HTTPDB 文件夹**：包括防毒墙网络版数据库
4. 卸载防毒墙网络版服务器。有关详细信息，请参阅第 2-53 页的*执行服务器卸载*。

5. 执行全新安装。有关详细信息，请参阅第 2-2 页的*执行防毒墙网络版服务器的全新安装*。
6. 安装完成后，打开 Microsoft 管理控制台 （单击**开始 > 运行**，然后键入 **services.msc**）。
7. 右键单击 **OfficeScan Master Service**，然后单击**停止**。
8. 将备份文件复制到目标计算机上的 <**服务器安装文件夹**>\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。
9. 重新启动防毒墙网络版主服务。

卸载防毒墙网络版服务器

使用卸载程序卸载防毒墙网络版服务器和集成型云安全服务器。

如果在使用卸载程序时遇到问题，请手动卸载服务器。

注意： 有关卸载防毒墙网络版客户端的指导信息，请参阅 《管理员指南》。

使用卸载程序卸载防毒墙网络版服务器：

1. 如果已在服务器计算机上执行了全新安装，请跳过此步骤。

   如果已将服务器从早期版本升级到此版本：

   a. 如果当前安装了插件管理器，请卸载插件管理器。

   b. 如果未安装插件管理器，请删除在 HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\ 中找到的 **AOS** 注册码。

2. 运行卸载程序。访问卸载程序有两种方法。

   方法 A

   a. 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 > 卸载防毒墙网络版**。将显示确定窗口。

   b. 单击**下一步**。服务器卸载程序将提示您输入管理员密码。

   c. 键入管理员密码，然后单击**下一步**。服务器卸载程序将开始删除服务器文件。将显示确定消息。

   d. 单击**完成**关闭卸载程序。

方法 B

a. 在 Windows “添加/删除程序”窗口上双击防毒墙网络版服务器程序。

b. 单击**控制面板 > 添加或删除程序**。找到并双击 “趋势科技防毒墙网络版服务器”。按照窗口上的指导信息操作，直到系统提示您输入管理员密码。

c. 键入管理员密码，然后单击**下一步**。服务器卸载程序将开始删除服务器文件。将显示确定消息。

d. 单击**完成**关闭卸载程序。

手动卸载服务器：

第 1 部分：集成型云安全服务器卸载

1. 打开 Microsoft 管理控制台，然后停止防毒墙网络版主服务。
2. 打开命令提示符，然后转至 <服务器安装文件夹>\PCCSRV。
3. 运行以下命令：

   ```
   SVRSVCSETUP.EXE -uninstall
   ```

   此命令卸载与防毒墙网络版相关的服务，但不删除配置文件或防毒墙网络版数据库。
4. 导航到 <服务器安装文件夹>\PCCSRV\private，然后打开 **ofcserver.ini**。
5. 如下所示修改以下设置：

表 2-3. ofcserver.ini 设置

设置	指导信息
WSS_INSTALL=1	将 1 更改为 0
WSS_ENABLE=1	删除此行
WSS_URL=https://<computer_name>:4345/tmcss/	删除此行

6. 导航到 <服务器安装文件夹>\PCCSRV，然后打开 **OfUninst.ini**。删除以下几行：
   - 如果使用 IIS Web 服务器：

     ```
     [WSS_WEB_SERVER]
     ServerPort=8082
     IIS_VhostName=Smart Scan Server (Integrated)
     IIS_VHostIdx=5
     ```

     注意： IIS_VHostidx 的值应该与以下行所示的 “isapi” 值相同：

     ROOT=/tmcss,C:\Program Files\Trend Micro\OfficeScan\PCCSRV\WSS\isapi,,<value>

     ```
     [WSS_SSL]
     SSLPort=<SSL port>
     ```
   - 如果使用 Apache Web 服务器：

     ```
     [WSS_WEB_SERVER]
     ServerPort=8082
     [WSS_SSL]
     SSLPort=<SSL port>
     ```
7. 打开命令提示符，然后转至 <服务器安装文件夹>\PCCSRV。
8. 运行以下命令：

   ```
   Svrsvcsetup -install
   Svrsvcsetup -enablessl
   Svrsvcsetup -setprivilege
   ```
9. 验证是否已删除以下项目：
   - Microsoft 管理控制台中的趋势科技云安全服务器服务
   - 云安全服务器性能计数器
   - 云安全服务器 （集成型） Web 站点

第 2 部分：防毒墙网络版服务器卸载

1. 打开注册表编辑器并执行以下步骤：

   警告！ 接下来的步骤要求您删除注册码。不正确地更改注册表会导致严重的系统问题。请始终在进行任何注册表更改前创建备份副本。有关详细信息，请参阅注册表编辑器帮助。

   a. 导航到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\。

   b. 验证是否已删除 **ofcservice** 永久保存数据。

   c. 导航到 HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\OfficeScan\，然后删除 **OfficeScan** 永久保存数据。

      对于 64 位计算机，路径是 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfficeScan\。

   d. 导航到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\，然后删除 **OfficeScan Management Console-<服务器名称>** 文件夹。

2. 导航到 <服务器安装文件夹>\PCCSRV 文件夹，然后取消共享 **PCCSRV** 文件夹。
3. 重新启动服务器计算机。
4. 导航到 <服务器安装文件夹>\PCCSRV，然后删除 **PCCSRV** 文件夹。
5. 从 Internet 信息服务 (IIS) 控制台中删除防毒墙网络版 Web 站点。

   a. 打开 IIS 控制台。

   b. 展开 **ServerName**。

   c. 如果已在单独的 Web 站点上安装了防毒墙网络版，请转至 **Web 站点**文件夹，然后删除**防毒墙网络版**。

   d. 如果已在 “缺省 Web 站点”下安装了防毒墙网络版虚拟目录，请转至**缺省 Web 站点**，然后删除防毒墙网络版虚拟目录。

第 3 章

获取帮助

本章主题：

- 第 3-2 页的*故障排除资源*
- 第 3-5 页的*与趋势科技联系*

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 3-1. 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%
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%
客户端安装日志	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：

- 卸载，然后再次安装服务器。
- 将防毒墙网络版升级到新版本。
- 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，则删除日志文件。**

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 <Server Installation Folder>\PCCSRV\Private 中的“LogServer”文件夹复制到 C:\。
2. 使用以下内容创建名为 ofcdebug.ini 的文件：

   [debug]

   DebugLevel=9

   DebugLog=C:\LogServer\ofcdebug.log

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1
3. 将 ofcdebug.ini 保存到 C:\LogServer。
4. 执行适当的任务 （即卸载/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。

客户端调试日志

您还可先启用调试日志记录，再安装防毒墙网络版客户端。

警告！ **调试日志可能会影响客户端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，则删除日志文件。**

要在防毒墙网络版客户端计算机上启用调试日志记录：

1. 使用以下内容创建名为 ofcdebug.ini 的文件：

   [debug]
   Debuglog=C:\ofcdebug.log
   debuglevel=9
   debugLevel_new=D
   debugSplitSize=10485760
   debugSplitPeriod=12
   debugRemoveAfterSplit=1

2. 将 ofcdebug.ini 发送给客户端用户，指示他们将该文件保存到 C:\。LogServer.exe 在客户端计算机每次启动时自动运行。指示用户不要关闭在计算机启动时打开的 LogServer.exe 命令窗口，因为这会指示防毒墙网络版停止调试日志记录。如果用户关闭了该命令窗口，他们可以通过运行位于 \OfficeScan Client 中的 LogServer.exe 再次开始调试日志记录。
3. 对于每台客户端计算机，检查 C:\ 中的 ofcdebug.log。
4. 要禁用防毒墙网络版客户端的调试日志记录，请删除 ofcdebug.ini。

与趋势科技联系

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。

趋势科技 （中国）有限公司向所有已注册用户提供全球支持。

- 获取全球技术支持办公室的列表：

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

- 获取最新趋势科技产品文档：

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

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
邮编：200020

咨询电话：800-820-8876(021-63848622)
传真：021-6384 1899
技术支持热线：800-820-8839 (021-26037677)
技术问题在线提交：**http://www.trendmicro.com.cn/SR**

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 Service Pack 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://cn.trendmicro.com/cn/support/techsupport/index.html

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技术支持工程师，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/vinfo/zh-cn/

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
- Internet 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”（Internet 威胁的源意向，例如间谍软件和病毒）。

- 将电子邮件发送到以下地址并指定 “网络钓鱼或带毒站点”为主题。

  virus_doctor@trendmicro.com.cn

- 还可以使用基于 Web 的提交表格：

  http://cn.trendmicro.com/cn/support/techsupport/index.html#onlinesubmit

文档反馈

趋势科技一直致力于改进其文档。如对该文档或趋势科技的任何其他文档有任何问题、意见或建议，请通过 **service@trendmicro.com.cn** 与我们联系。我们始终欢迎您的反馈。

附录 A

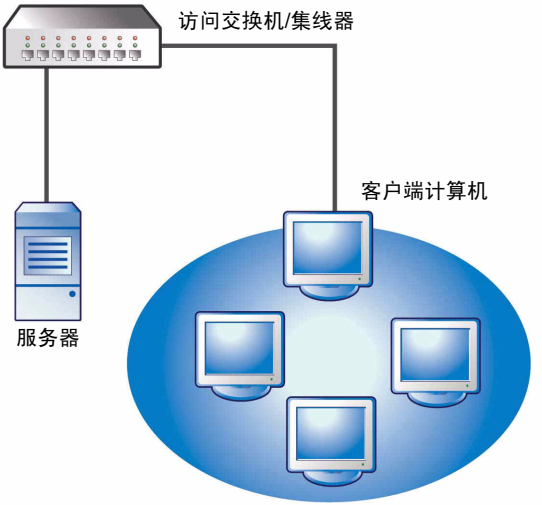
示例部署

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方式。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 A-1 描述了防毒墙网络版服务器和客户端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 A-1. 基本网络拓扑



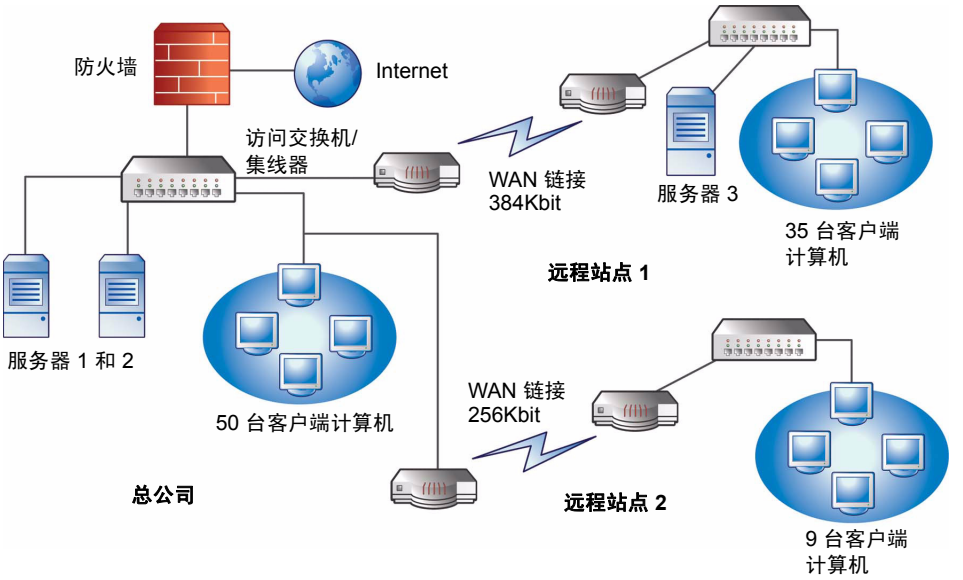
多个站点网络

对于带有多个访问接入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。
- 确定每个办公室的当前带宽利用率。

下图更清楚地描述了如何以最佳方式部署防毒墙网络版。图 A-2 描述了一个多站点网络拓扑。

图 A-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，请参阅第 2-2 页的***执行防毒墙网络版服务器的全新安装***。
2. 识别可用客户端安装方法，并排除不满足要求的方法。有关客户端安装方法的更多信息，请参阅 《管理员指南》。

   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。

   - 客户端软件包部署

     客户端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端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 《管理员指南》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) 格式的客户端软件包，然后将该客户端软件包部署到 DFS。请参阅 《管理员指南》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，因此客户端软件包部署对带宽的影响最小。

还可以通过 Active Directory 部署客户端软件包。有关详细信息，请参阅 《管理员指南》。

将 WAN 上的组件更新的影响最小化：

1. 指定一台客户端充当远程站点 1 上的更新代理。
   a. 打开 Web 控制台，然后转至**联网计算机 > 客户端管理**。
   b. 在客户端树中，选择要充当更新代理的客户端，然后单击**设置 > 更新代理设置**。
2. 从更新代理选择远程站点 1 中用于更新组件的客户端。
   a. 转至**更新 > 联网计算机 > 更新源**。
   b. 选择**定制的更新源**，然后单击**添加**。
   c. 在显示的窗口中，键入远程站点 1 中客户端计算机的 IP 地址范围。
   d. 选择**更新源**，然后从下拉列表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 的带宽可用。

安装防毒墙网络版客户端的最佳方法是使用与远程站点 1 中所使用的相同的 MSI 格式的客户端软件包。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)。

可以选择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目录。在单台计算机上创建共享目录后，将客户端软件包复制到该目录所需的开销比将客户端安装到九台计算机所需的开销少。

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。

这些方法可将安装网络通信保持为本地网络的通信，并最小化 WAN 上的网络通信。

要将 WAN 上组件更新的影响最小化，还可以指定一台客户端充当更新代理。请参阅第 A-5 页的*远程站点 1 部署*以获取详细信息。

附录 B

旧版防毒墙网络版功能

此部分提供在早先的防毒墙网络版版本中可用但在此版本中不再可用的功能列表。

表 B-2. 旧版防毒墙网络版功能

功能	可用性		防毒墙网络版 10 中的状态
	8.x	7.x	
趋势科技防毒墙网络版 for Wireless	否	是	趋势科技防毒墙网络版 for Wireless 已由 Trend Micro Mobile Security™ 所取代， Trend Micro Mobile Security™ 可用作插件程序。
无线防御管理程序	否	是	无线防御管理程序已由 Trend Micro Mobile Security 所取代，Trend Micro Mobile Security 可用作插件程序。
DCS 扫描（客户端启动的）	否	是	在扫描期间，自动执行 DCS 扫描。

表 B-2. 旧版防毒墙网络版功能 （续）

功能	可用性		防毒墙网络版 10 中的状态
	8.x	7.x	
DCS 立即清除（服务器启动的）	否	是	在扫描期间，自动执行 DCS 立即清除。
预设清除（全局客户端设置）	否	是	在扫描期间，自动执行预设清除。
病毒爆发监控程序	否	是	病毒爆发监控程序设置在**通知 > 管理员通知 > 爆发通知 > 共享文件夹会话**下配置。
防火墙病毒爆发监控程序	否	是	防火墙病毒爆发监控程序设置在**通知 > 管理员通知 > 爆发通知 > 防火墙违例**下配置。
防毒墙网络版看守程序	是	是	防毒墙网络版看守程序的功能 （重新启动意外停止的防毒墙网络版客户端服务）由防毒墙网络版客户端执行。服务重新启动设置在 Web 控制台的全局客户端设置窗口中配置。