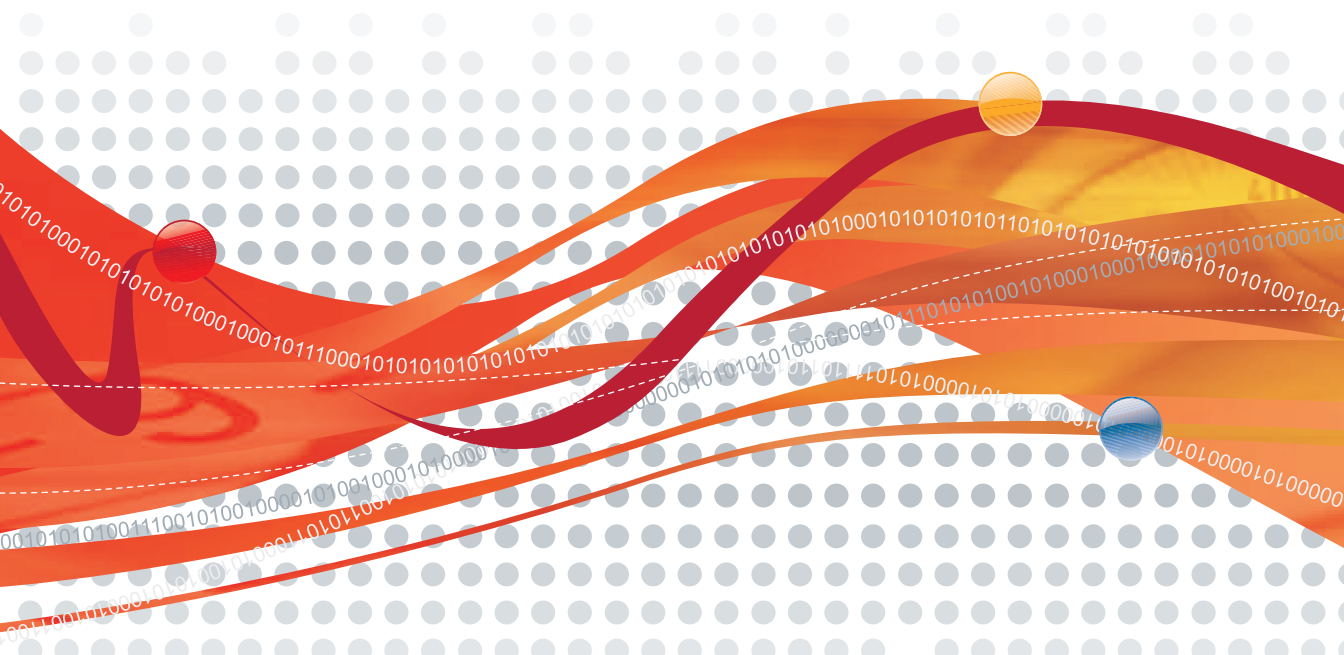
TREND MICRO™

防毒墙网络版[8]

适用于大中型企业

for Windows™ Vista™

安装和部署指南



Endpoint Security

文档部分编号 OSCM83936/81107

发布日期：2008 年 11 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

第 3 章 : 与趋势科技联系

第 1 章

规划客户机安装

本章中的主题：

安装需求

以下是在运行 Windows Vista （32 位 和 64 位 版本）的计算机上安装防毒墙网络版客户机的需求。

操作系统

- 带有 Service Pack 1 的 Windows Vista Business 版
- 带有 Service Pack 1 的 Windows Vista Enterprise 版
- 带有 Service Pack 1 的 Windows Vista Ultimate 版

- 带有 Service Pack 1 的 Windows Vista Home Premium 版
- 带有 Service Pack 1 的 Windows Vista Home Basic 版
- 防毒墙网络版支持在以下虚拟化应用程序中托管的 guest Windows Vista 操作系统中安装客户机：
  - 带有 Service Pack 1 的 Microsoft Virtual Server 2005 R2
  - VMware ESX Server 3.0 （ESX 服务器版）
  - VMware Server 1.0.3 （服务器版）
  - VMware Workstation 和 Workstation ACE 6.0 版

硬件

- 800MHz Intel Pentium 处理器或同等处理器；还支持 AMD™ x64 或 Intel 64 位处理器体系结构
- 1GB 内存
- 350MB 可用磁盘空间
- 支持分辨率为 800 x 600 颜色为 256 的显示器

其他

如果执行 Web 安装，则需要 Windows Internet Explorer 7.0 或更高版本

更新代理需求

- 800MHz Intel Pentium 处理器或同等处理器
- 700MB 可用磁盘空间
- 1GB 内存

不支持的功能

运行 Windows Vista 的计算机将拥有多数防毒墙网络版程序和功能，以下程序和功能除外：

- Microsoft Outlook™ 邮件扫描
- Check Point™ SecureClient™ 支持
- Cisco™ NAC 2
- 镜像安装实用程序 (ImgSetup.exe)

  注意： 即使不支持镜像安装，客户机也能够在服务器提示时自动更改 GUID。

- 感染源通知 （“警报服务”已移除）

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内置管理员权限。

Web 安装页面

指导贵组织中的用户转到 Web 安装页面并下载客户机安装文件 （请参阅*从 Web 安装页面安装* （第 2-2 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*通过客户机打包程序安装* （第 2-5 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*通过客户机打包程序安装*（第 2-5 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 2-9 页）
- *使用 Microsoft SMS 部署 MSI 软件包*（第 2-10 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 2-14 页））。

注意： 此安装方法不能用于运行 Windows Vista Home Basic 和 Home Premium 版（32 位和 64 位版本）的计算机。

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 2-16 页））。

注意： 此安装方法不能用于运行 Windows Vista Home Basic 和 Home Premium 版（32 位和 64 位版本）的计算机。

摘要

表 1-1　　防毒墙网络版客户机安装方法

	Web 安装页面	客户端数据包	使用 Microsoft SMS 部署的客户端数据包	使用 Active Directory 部署的客户端数据包	远程安装	TMVS
适合跨 WAN 部署	无	无	是	是	无	无
适合集中式管理	无	无	是	是	是	是
要求客户机用户的干预	是	是	是 / 无	是 / 无	无	无
要求 IT 资源	无	是	是	是	是	是
适合大规模部署	无	无	是	是	无	无
带宽消耗	高	低，如果已预设	低，如果已预设	高，如果客户机同时启动	高	高

第 2 章

安装防毒墙网络版客户机

安装场景：

建议的安装后任务：

其他任务：

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 安装页面安装

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 安装页面安装客户机程序。指导用户转到 Web 安装页面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哪些用户没有遵循那些用以从 Web 安装页面安装的指令（请参阅*使用漏洞扫描程序以验证客户机安装*（第 2-20 页）以获取详细信息）。

需求：

- 至少为将安全级别设置为允许 ActiveX™ 控件的 Microsoft Internet Explorer 7.0
- 计算机上的内置管理员权限

从 Web 安装页面上发送以下指令给用户以安装防毒墙网络版客户机。

从 Web 安装页面安装：

安装前

1. 使用内置管理员帐户登录到 Windows Vista 计算机。
2. 打开 Internet Explorer，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**。

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。

安装

1. 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://{ 防毒墙网络版服务器名称 }:{ 端口 }/officescan
   - 不具有 SSL 的防毒墙网络版服务器：

     http://{ 防毒墙网络版服务器名称 }:{ 端口 }/officescan
2. 单击**联网计算机**下的链接。
3. 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。出现提示时允许安装 ActiveX 控件。

   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

在未受保护计算机登录到网络时，登录脚本安装将防毒墙网络版客户机安装到这些计算机。“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. “登录脚本安装”将返回到其初始屏幕。

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

注意： AutoPcc.exe 不会自动将客户机安装到 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。

通过客户机打包程序安装

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 2-9 页）和*使用 Microsoft SMS 部署 MSI 软件包*（第 2-10 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 2-8 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. 选择安装软件包里包含的组件。

7. 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。

8. 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）。

9. 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。

10. 部署软件包。

    - 将软件包发送给用户，请他们在计算机上通过右键单击 .exe 文件并选中**作为管理员运行**来运行客户机软件包。

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，则可以：

- 使用 Active Directory 或 Microsoft SMS。请参阅*使用 Active Directory 部署 MSI 软件包*（第 2-9 页）或*使用 Microsoft SMS 部署 MSI 软件包*（第 2-10 页）。
- 启动 MSI 软件包 （在命令提示符中），并将防毒墙网络版客户机静默安装到运行 Windows Vista 的远程计算机。

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 *通过客户机打包程序安装*（第 2-5 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 *通过客户机打包程序安装* （第 2-5 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*通过客户机打包程序安装*（第 2-5 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 2-20 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 Vista 计算机上。确保您对目标计算机具有内置管理员权限，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。

注意： 此安装方法不能用于运行 Windows Vista Home Basic 和 Home Premium 版 （32 位和 64 位版本）的计算机。

从防毒墙网络版 Web 控制台安装：

安装前：

1. 在 Windows Vista 计算机上，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 > 高级安全 Windows 防火墙**。
   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。

安装：

1. 在 Web 控制台，单击**联网计算机 > 客户机安装 > 远程**。
2. 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。
3. 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。
4. 重复步骤 2 和步骤 3，添加多个计算机。
5. 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。
6. 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。

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： 此安装方法不能用于运行 Windows Vista Home Basic 和 Home Premium 版 （32 位和 64 位版本）的计算机。

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。

使用漏洞扫描程序安装防毒墙网络版客户机：

安装前：

1. 在 Windows Vista 计算机上，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 > 高级安全 Windows 防火墙**。
   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。

安装：

1. 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。
2. 单击**设置**。
3. 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。
4. 选择**为不受保护的计算机自动安装防毒墙网络版客户机**。
5. 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

您可以将防毒墙网络版评估版升级为完全版。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 1-3 页））。

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。

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载现有软件并替换为防毒墙网络版客户机。

注意： 防毒墙网络版只卸载客户机，而不是服务器。

要检查防毒墙网络版自动卸载的应用程序，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载现有的客户机防病毒软件，请执行以下任务：
  - 手动卸载现有的客户机防病毒软件。根据软件卸载过程，卸载后计算机可能需要 （或可能不需要）重新启动。
  - 使用*执行全新安装*（第 2-2 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，但是没有卸载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，卸载两个软件，然后使用*执行全新安装*（第 2-2 页）中介绍的任何一种方法安装防毒墙网络版客户机。

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

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 Personal Firewall （如果安装过程中启用了防火墙）
  - OfficeScan NT Proxy Service
  - OfficeScan NT 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： 漏洞扫描程序不能用于运行 Windows Vista Home Basic 和 Home Premium 版 （32 位和 64 位版本）的计算机。

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. 选择是使用正常，还是快速。正常更准确，但花费较长时间来完成。

   如果单击**正常**，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。

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。

卸载客户机

有两种方法可从客户机卸载防毒墙网络版程序：

- *从 Web 控制台卸载*（第 2-25 页）
- *运行客户机卸载程序*（第 2-26 页）

从 Web 控制台卸载

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

从 Web 控制台卸载客户机：

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载防毒墙网络版客户机的客户机，然后单击**任务 > 客户机卸载**。
3. 单击“客户机卸载”窗口中的**启动卸载**。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**启动卸载**立即将通知重新发送给未通知的客户机。
   b. 单击**停止卸载**，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载的客户机暂不处理此命令。

运行客户机卸载程序

如果授予用户卸载客户机程序的权限，指导他们从他们的计算机运行客户机卸载程序。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。

运行客户机卸载程序：

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 > 卸载防毒墙网络版客户机**。将显示 “防毒墙网络版客户机卸载” 窗口，并提示输入卸载密码。
2. 键入卸载密码，然后单击**确定**。防毒墙网络版将通知用户卸载的进度与卸载完成。

用户不需要重新启动客户端计算机来完成卸载。

第 3 章

与趋势科技联系

本章中的主题：

技术支持

趋势科技向所有已注册用户（必须在购买更新维护后）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 /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://cn.trendmicro.com/cn/support/techsupport/index.html 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

咨询电话：800-820-8876(021-63848622)

技术支持热线：800-820-8839(021-26037677)

传真：021-6384 1899

Web 地址：www.trendmicro.com.cn

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} 是趋势科技全球性的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。

您可以依赖以下售后服务：

- 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：

- 当前正在肆虐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://cn.trendmicro.com/cn/support/techsupport/index.html

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://cn.trendmicro.com/cn/support/techsupport/index.html。

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。