



防毒墙网络版¹⁰

适用于大中型企业

管理员指南



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、eManager、InterScan、网络病毒墙、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。

版权所有 © 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 OSCM104079/90429

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 xviii

读者 xix

文档规则 xix

术语 xx

第 1 章： 防毒墙网络版简介

关于防毒墙网络版 1-2

此发行版的新功能 1-2

关键功能和优点 1-5

防毒墙网络版服务器 1-7

防毒墙网络版客户端 1-9

云安全服务器 1-10

第 2 章： 防毒墙网络版入门

Web 控制台 2-2

安全性摘要 2-5

防毒墙网络版客户端树 2-10

 客户端树常规任务 2-11

 高级搜索选项 2-12

 客户端树特定任务 2-12

防毒墙网络版域 2-19

安全合规 2-20

第 1 部分：保护联网计算机

第 3 章： 安装防毒墙网络版客户端

安装需求	3-2
安装方法	3-10
从 Web 安装页安装	3-12
启动基于浏览器的安装	3-14
使用“登录脚本安装”安装	3-14
使用客户端打包程序安装	3-17
客户端打包程序设置	3-19
使用 Active Directory 部署 MSI 软件包	3-22
使用 Microsoft SMS 部署 MSI 软件包	3-23
从防毒墙网络版 Web 控制台安装	3-26
从客户端磁盘镜像安装	3-27
使用漏洞扫描程序	3-28
安装防毒墙网络版客户端	3-32
管理常规设置	3-33
运行漏洞扫描	3-36
创建预设任务	3-38
配置其他漏洞扫描程序设置	3-39
迁移到防毒墙网络版客户端	3-40
从其他端点安全软件迁移	3-40
从 ServerProtect 标准服务器迁移	3-41
安装后	3-44
建议的安装后任务	3-45
卸载客户端	3-46
从 Web 控制台卸载客户端	3-46
运行客户端卸载程序	3-47
手动卸载客户端	3-48

第 4 章： 使防护保持最新

防毒墙网络版组件与程序	4-2
防病毒组件	4-2
损害清除服务组件	4-5
防间谍软件组件	4-5
防火墙组件	4-6
Web 信誉组件	4-6
行为监控组件	4-6
程序	4-7
更新概述	4-9
防毒墙网络版服务器更新	4-11
服务器更新源	4-13
用于服务器更新的代理服务器	4-14
服务器组件复制	4-14
服务器更新方法	4-17
预设更新	4-17
手动更新	4-18
服务器更新日志	4-18
云安全服务器更新	4-19
服务器更新设置	4-19
客户端更新	4-21
从防毒墙网络版服务器和定制源更新	4-22
定制的更新源	4-23
标准更新源	4-24
客户端更新方法	4-25
自动更新	4-25
手动更新	4-29
更新权限	4-30
客户端组件更新的代理服务器	4-31
客户端更新日志	4-32
客户端更新通知	4-32
组件还原	4-33

- 更新代理 4-34
 - 更新代理的系统要求 4-34
 - 更新代理配置 4-35
 - 更新代理的更新源 4-35
 - 更新代理的定制的更新源 4-36
 - 更新代理的标准更新源 4-37
 - 更新代理组件复制 4-38
 - 更新代理的更新方法 4-38
- 组件更新摘要 4-39

第 5 章： 保护计算机免受安全风险的危害

- 关于安全风险 5-2
 - 病毒和恶意软件 5-2
 - 间谍软件和灰色软件 5-4
 - 间谍软件/灰色软件进入网络的方式 5-5
 - 潜在风险和威胁 5-6
 - 预防间谍软件/灰色软件 5-7
- 扫描方法 5-8
 - 云安全扫描源 5-14
 - 标准列表 5-15
 - 定制列表 5-16
- 扫描类型 5-18
 - 实时扫描 5-18
 - 手动扫描 5-20
 - 预设扫描 5-21
 - 立即扫描 5-22
 - 启动立即扫描 5-23
- 所有扫描类型的通用设置 5-24
 - 扫描条件 5-24
 - 扫描例外 5-26

扫描处理措施	5-29
病毒/恶意软件扫描处理措施	5-29
间谍软件/灰色软件扫描处理措施	5-37
与扫描相关的权限	5-40
全局扫描设置	5-40
安全风险通知	5-41
管理员通知设置	5-41
针对管理员的安全风险通知	5-42
针对客户端用户的安全风险通知	5-43
安全风险日志	5-45
病毒/恶意软件日志	5-45
间谍软件/灰色软件日志	5-51
间谍软件/灰色软件恢复日志	5-53
爆发防护	5-53
爆发条件和通知	5-53
爆发阻止	5-56
爆发阻止策略	5-57
限制/拒绝访问共享文件夹	5-57
封闭端口	5-58
拒绝对文件和文件夹的写访问	5-59
禁用爆发阻止	5-59
设备控制	5-60
设备控制日志	5-62

第 6 章： 保护计算机免受基于 Web 的威胁

关于 Web 威胁	6-2
Web 信誉	6-2
位置感知	6-3
Web 信誉策略	6-3

Web 信誉允许的 URL 列表 6-5

Web 信誉的代理服务器 6-5

客户端用户的 Web 威胁通知 6-6

Web 信誉日志 6-7

第 7 章： 使用防毒墙网络版防火墙

关于防毒墙网络版防火墙 7-2

防火墙策略和概要文件 7-4

 防火墙策略 7-5

 添加和修改防火墙策略 7-6

 编辑防火墙例外模板 7-8

 防火墙概要文件 7-11

 添加和编辑防火墙概要文件 7-14

防火墙权限 7-15

向客户端用户发送的防火墙违例通知 7-16

防火墙日志 7-17

测试防毒墙网络版防火墙 7-18

禁用防毒墙网络版防火墙 7-19

第 2 部分： 管理防毒墙网络版服务器和客户端

第 8 章： 管理防毒墙网络版服务器

基于角色的管理 8-2

 用户角色 8-2

 添加和修改定制角色 8-5

 用户帐户 8-6

 添加和修改用户帐户 8-7

 添加一个或多个 Active Directory 帐户 8-9

趋势科技防毒墙控制管理中心	8-10
参考服务器	8-13
系统事件日志	8-15
管理日志	8-16
日志维护	8-18
使用授权	8-19
防毒墙网络版数据库备份	8-21
防毒墙网络版 Web 服务器信息	8-22
Web 控制台密码	8-23
隔离管理器	8-24
服务器调节程序	8-25
全球病毒实时监控计划	8-28

第 9 章： 管理客户端

计算机位置	9-2
网关设置导入程序	9-4
客户端权限和其他设置	9-5
漫游权限	9-6
扫描权限	9-7
预设扫描权限	9-8
防火墙权限	9-10
邮件扫描权限	9-12
工具箱权限	9-14
代理服务器设置权限	9-14
组件更新权限	9-15
卸载	9-15
退出	9-15
更新设置	9-15
Web 信誉设置	9-16

预设扫描设置	9-16
客户端安全设置	9-17
POP3 电子邮件扫描设置	9-17
客户端控制台访问限制	9-17
重新启动通知	9-17
全局客户端设置	9-18
扫描设置	9-19
预设扫描设置	9-23
防火墙日志设置	9-25
警报设置	9-25
防毒墙网络版服务重新启动	9-26
客户端自我保护	9-27
保留的磁盘空间	9-28
网络病毒日志整合	9-29
病毒/恶意软件日志带宽设置	9-29
代理服务器配置	9-29
客户端分组	9-30
客户端与服务器的连接	9-30
所需处理措施	9-35
客户端-服务器连接验证	9-37
连接验证日志	9-38
客户端代理服务器设置	9-39
内部代理服务器	9-39
外部代理服务器	9-40
客户端迁移程序	9-41
触探工具	9-42
客户端信息	9-43
导入和导出客户端设置	9-44
管理非活动客户端	9-45

第 3 部分：提供其他防护

第 10 章：策略服务器 for Cisco NAC

关于策略服务器 for Cisco NAC	10-2
组件和术语	10-2
Cisco NAC 体系结构	10-5
客户端验证顺序	10-6
策略服务器	10-8
策略服务器策略和规则	10-9
规则组成	10-9
缺省规则	10-11
策略组成	10-12
缺省策略	10-13
同步	10-14
证书	10-15
CA 证书	10-17
策略服务器系统要求	10-18
Cisco Trust Agent (CTA) 需求	10-19
支持的平台和需求	10-20
策略服务器 for NAC 部署	10-22
Cisco Secure ACS 服务器登记	10-23
CA 证书安装	10-23
Cisco Trust Agent 部署	10-25
在防毒墙网络版服务器安装期间部署 CTA	10-25
从防毒墙网络版 Web 控制台部署 CTA	10-26
Cisco Trust Agent 安装验证	10-29
策略服务器 for Cisco NAC 安装	10-29
策略服务器 SSL 证书准备	10-32
ACS 服务器配置	10-34

策略服务器 for Cisco NAC 配置	10-34
从防毒墙网络版配置策略服务器	10-35
策略服务器的摘要信息	10-36
策略服务器注册	10-37
规则	10-37
策略	10-37
客户端验证日志	10-38
客户端日志维护	10-38
管理	10-38

第 11 章：使用第三方软件配置防毒墙网络版

Check Point 体系结构和配置概述	11-2
防毒墙网络版集成	11-3
Check Point for 防毒墙网络版配置	11-4
安装 SecureClient 支持	11-6

第 12 章：获取帮助

故障排除资源	12-2
情况诊断工具	12-2
防毒墙网络版服务器日志	12-2
服务器使用 LogServer.exe 调试日志	12-3
安装日志	12-4
组件更新日志	12-5
客户端打包程序日志	12-5
ServerProtect 标准服务器迁移工具日志	12-6
VSEncrypt 日志	12-6
控制管理中心 MCP 代理日志	12-6
病毒扫描引擎日志	12-7
爆发日志	12-8
全球病毒跟踪日志	12-8

防毒墙网络版客户端日志 12-9

 客户端调试日志（使用 LogServer.exe） 12-9

 全新安装日志 12-10

 升级/Hotfix 日志 12-10

 损害清除服务日志 12-10

 邮件扫描日志 12-10

 客户端连接日志 12-11

 客户端更新日志 12-11

 爆发阻止日志 12-11

 防毒墙网络版防火墙日志 12-12

 Web 信誉和 POP3 邮件扫描日志 12-13

 传输驱动接口 (TDI) 日志 12-14

与趋势科技联系 12-15

 技术支持 12-15

 趋势科技知识库 12-16

 TrendLabs 12-17

 安全信息中心 12-17

 将可疑文件发送给趋势科技 12-18

 文档反馈 12-18

附录 A: 词汇表

表格清单

表 P-1. 防毒墙网络版文档 xviii

表 P-2. 文档规则..... xix

表 P-3. 防毒墙网络版术语 xx

表 1-1. 客户端功能..... 1-9

表 1-2. 云安全服务器类型之间的对比..... 1-12

表 2-1. 防毒墙网络版 Web 控制台 URL 2-3

表 2-2. 客户端管理任务..... 2-13

表 2-3. 计算机防护状态..... 2-22

表 3-1. Windows 2000 3-2

表 3-2. Windows XP/2003， 32 位版本 3-3

表 3-3. Windows XP/2003， 64 位版本 3-5

表 3-4. Windows Vista， 32 位和 64 位版本 3-6

表 3-5. Windows 2008， 32 位版本 3-7

表 3-6. Windows 2008， 64 位版本 3-8

表 3-7. 安装方法..... 3-10

表 3-8. 客户端软件包类型..... 3-17

表 3-9. 网络管理..... 3-28

表 3-10. 网络拓扑和体系结构..... 3-29

表 3-11. 软件/硬件规格	3-29
表 3-12. 域结构	3-30
表 3-13. 网络通信	3-30
表 3-14. 网络规模	3-31
表 3-15. 漏洞扫描程序检查的安全产品	3-33
表 3-16. TMVS.ini 文件中的 DHCP 设置	3-37
表 4-1. 服务器-客户端更新选项	4-9
表 4-2. 云安全服务器的更新过程	4-11
表 4-3. 由防毒墙网络版服务器下载的组件	4-11
表 4-4. 服务器组件复制场景	4-15
表 4-5. 客户端存储的防毒墙网络版组件	4-21
表 4-6. 事件触发更新选项	4-27
表 4-7. 客户端组件更新过程中使用的代理服务器设置	4-31
表 4-8. 更新代理的系统要求	4-34
表 5-1. 传统扫描和云安全扫描之间的对比	5-9
表 5-2. 扫描类型	5-18
表 5-3. 未通知的客户端场景	5-23
表 5-4. 趋势科技建议对病毒/恶意软件执行的扫描处理措施	5-31
表 5-5. 隔离目录	5-32

表 5-6. 防毒墙网络版可以解密和恢复的文件..... 5-34

表 5-7. 恢复参数..... 5-36

表 5-8. 安全风险通知的令牌变量..... 5-42

表 5-9. 爆发通知的令牌变量..... 5-55

表 5-10. 设备权限..... 5-60

表 7-1. 缺省防火墙策略..... 7-5

表 7-2. 缺省防火墙策略例外..... 7-9

表 9-1. 压缩文件情形和结果..... 9-21

表 9-2. 联机客户端图标..... 9-31

表 9-3. 脱机客户端图标..... 9-32

表 9-4. 漫游客户端图标..... 9-34

表 10-1. 策略服务器 for Cisco NAC 组件..... 10-2

表 10-2. 与策略服务器 for Cisco NAC 相关的术语 10-3

表 10-3. 缺省规则..... 10-11

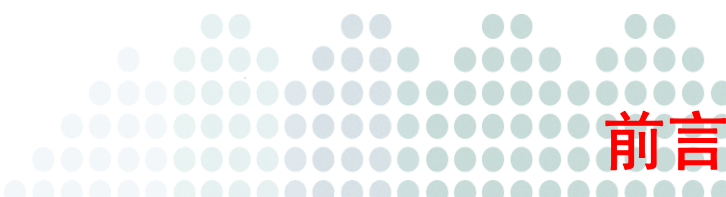
表 10-4. 缺省策略..... 10-13

表 10-5. Cisco NAC 证书..... 10-15

表 10-6. 支持的平台和需求..... 10-20

表 11-1. SCV 文件参数的名称和值 11-5

表 A-1. 特洛伊木马端口 A-10



前言

前言

欢迎使用《趋势科技™ 防毒墙网络版管理员指南》。本文档介绍入门信息、客户端安装过程以及防毒墙网络版服务器和客户端管理。

本章主题：

- 第 xviii 页的 [防毒墙网络版文档](#)
- 第 xix 页的 [读者](#)
- 第 xix 页的 [文档规则](#)
- 第 xx 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

从以下位置下载最新版本的 PDF 文档和自述文件：

<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：**负责设计和维护 Cisco NAC 服务器和 Cisco 联网设备的安全系统。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。
<文本>	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： 文本	提供配置说明或建议

表 P-2. 文档规则（续）

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

术语

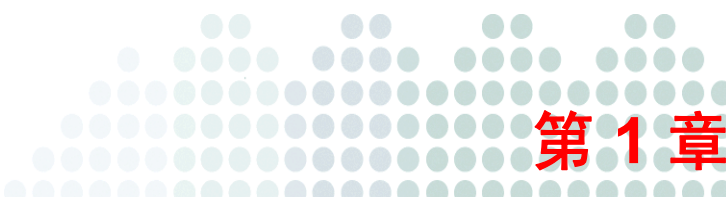
下表提供在整个防毒墙网络版文档中使用的正式术语：

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

防毒墙网络版简介

本章主题：

- 第 1-2 页的[关于防毒墙网络版](#)
- 第 1-2 页的[此发行版的新功能](#)
- 第 1-5 页的[关键功能和优点](#)
- 第 1-7 页的[防毒墙网络版服务器](#)
- 第 1-9 页的[防毒墙网络版客户端](#)
- 第 1-10 页的[云安全服务器](#)

关于防毒墙网络版

趋势科技™ 防毒墙网络版可保护企业网络免受恶意软件、网络病毒、基于 Web 的威胁、间谍软件和混合威胁攻击的危害。防毒墙网络版是集成的解决方案，包括驻留在端点的客户端程序和管理所有客户端的服务器程序。客户端保护端点并将其安全状态报告给服务器。通过基于 Web 的管理控制台，服务器可以轻松在每个客户端上设置协调的安全策略并部署更新。

防毒墙网络版由趋势科技云安全智能防护网络提供支持，该网络是新一代云客户端基础架构，可提供比传统方法更智能的安全性。独特的云端技术和轻量级客户端减少了对传统特征码下载的依赖，并且消除了通常与桌面更新相关的延迟。企业将受益于网络带宽增加、处理功耗降低及相关的成本节省。无论用户在哪里（公司网络、家中或路途中）进行连接，都可以直接访问最新防护。

此发行版的新功能

趋势科技™ 防毒墙网络版包括以下新功能和增强功能：

云安全扫描

云安全扫描将安全功能从端点移动到云端。云安全扫描是趋势科技云安全智能防护网络不可或缺的一部分，可以提供下列优点：

- 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。

有关云安全扫描部署信息，请参阅《趋势科技云安全扫描防毒墙网络版入门指南》。

Active Directory 集成

防毒墙网络版利用 Microsoft™ Active Directory™ 服务在组织中强制执行安全合规。通过定期轮询 Active Directory，防毒墙网络版可以检测无安全软件的计算机，并将客户端安装到计算机。防毒墙网络版还允许您通过用户的 Active Directory 帐户，向其分配 Web 控制台的访问权限。

有关详细信息，请参阅下列主题：

- 第 2-20 页的[安全合规](#)
- 第 8-2 页的[基于角色的管理](#)

基于角色的管理

基于角色的管理让您向其他管理员委派 Web 控制台管理任务，并且允许非管理员用户查看 Web 控制台项。可以先创建具有防毒墙网络版 Web 控制台功能的特定访问权限的用户角色，然后将这些角色分配给用户。通过创建定制用户帐户或使用现有的 Active Directory 帐户来管理用户。

单次登录支持可让用户从趋势科技防毒墙控制管理中心登录到防毒墙网络版 Web 控制台。

有关详细信息，请参阅第 8-2 页的[基于角色的管理](#)。

行为监控

行为监控可控制对外部存储设备和网络资源的访问，从而管制数据泄露或恶意软件感染带来的潜在威胁。此外，行为监控还可以使与安全相关的进程始终保持启动并运行，保护防毒墙网络版客户端文件和注册码，从而增强端点防护。

行为监控提供下列功能：

- 第 5-60 页的[设备控制](#)
- 第 9-27 页的[客户端自我保护](#)

平台支持

此产品版本支持在 Windows Server™ 2008 和虚拟化应用程序（如 VMware™）上安装服务器和客户端。

有关客户端安装需求的列表，请参阅第 3-2 页的 [安装需求](#)；有关服务器安装需求的列表，请参阅《安装和升级指南》。

产品增强功能

此产品发行版包括下列增强功能：

性能控制

性能控制在扫描期间执行以下操作，从而允许高效使用 CPU 资源：

- 检查防毒墙网络版 Web 控制台上配置的 CPU 使用率级别和计算机上的实际 CPU 占用情况。
- 如果出现下列情况，则调节扫描速度：
 - CPU 使用率级别为中或低
 - 实际 CPU 占用超出特定阈值

有关详细信息，请参阅第 5-25 页的 [CPU 使用率](#)。

预设扫描增强功能

具有预设扫描权限的用户可以推迟、跳过和停止预设扫描。有关详细信息，请参阅第 9-8 页的 [预设扫描权限](#)。

粒度 Web 信誉设置

配置 Web 信誉策略，并将这些策略分配给一个、多个或所有防毒墙网络版客户端。有关详细信息，请参阅第 6-3 页的 [Web 信誉策略](#)。

关键功能和优点

防毒墙网络版具有以下功能和优点：

安全风险防护

防毒墙网络版通过扫描文件，然后对每一个检测到的安全风险执行特定的处理措施来保护计算机免遭安全风险的侵扰。在短时间内检测到数量庞大的安全风险意味着病毒爆发。要抑制爆发，防毒墙网络版会强制执行爆发阻止策略并且隔离受感染的计算机，直到它们完全不存在风险。

防毒墙网络版使用云安全扫描来使扫描进程更有效率。此技术的工作原理是，将先前存储在本地计算机上的大量签名转移到[云安全服务器](#)。使用这种方法，持续增长的签名更新数量对“端点系统”的系统与网络影响将大大降低。

有关云安全扫描以及如何将其部署到客户端的信息，请参阅《趋势科技云安全扫描防毒墙网络版入门指南》。

Web 信誉

集成到防毒墙网络版的 Web 信誉技术可前瞻地保护公司网络内外的客户端计算机免受有恶意和可能有危险的 Web 站点的危害。Web 信誉可断开感染链并防止下载恶意代码。

损害清除服务

损害清除服务通过全自动过程，清除计算机中基于文件的病毒和网络病毒以及病毒和蠕虫残留（特洛伊木马、注册表项和含病毒的文件）。要处理由特洛伊木马造成的威胁和损害，损害清除服务将执行以下操作：

- 检测和移除活动的特洛伊木马
- 中断特洛伊木马创建的进程
- 修复特洛伊木马修改的系统文件
- 删除特洛伊木马留下的文件和应用程序

由于损害清除服务在后台自动运行，因此不需要对其进行配置。它运行时用户甚至没有察觉。但是，防毒墙网络版可能有时会通知用户重新启动计算机以完成移除特洛伊木马的过程。

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端。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。

注意： 可以在也启用 Windows 防火墙的 Windows XP 计算机上安装、配置和使用防毒墙网络版防火墙。但是，必须仔细管理策略以避免创建有冲突的防火墙策略和产生意外结果。例如，将一个防火墙配置为允许来自一个特定端口的网络通信，而其他防火墙阻止来自同一端口的网络通信，则防毒墙网络版会阻止网络通信。有关 Windows 防火墙的详细信息，请参阅 Microsoft 文档。

安全和策略实施

防毒墙网络版与 Cisco™ Trust Agent 无缝集成，以便在 Cisco 自我防御网络中启用最有效的策略实施。防毒墙网络版还包括策略服务器，用于与 Cisco 访问控制服务器自动进行通信。当与趋势科技™ 网络病毒墙或任何网络准入控制 (NAC) 设备集成时，防毒墙网络版都可以检查试图进入网络的客户端，然后补救、重定向、限制、拒绝或允许访问。如果某个计算机易受攻击或已受感染，防毒墙网络版可以自动隔离该计算机及其网段，直到完成所有的计算机更新或清除。

集中式管理

通过基于 Web 的管理控制台，管理员可以透明访问网络上的所有客户端和服务端。Web 控制台可协调安全策略、病毒码文件和软件更新在每台客户端和服务端上的自动部署。结合爆发阻止服务，Web 控制台可在病毒码文件可用前关闭感染站点，以及快速部署特定于攻击的安全策略以阻止或抑制爆发。防毒墙网络版还执行实时监控，提供事件通知以及传递全面的报告。管理员可以执行远程管理，为个别台式机或台式机组设置定制策略以及锁定客户端安全设置。

插件管理器和插件程序

插件程序以及新的产品版本、Service Pack 和 Patch，旨在将新功能和安全功能添加到防毒墙网络版，从而提高产品的性能。插件管理器可简化插件程序的安装、部署和管理。

防毒墙网络版服务器从趋势科技 ActiveUpdate 服务器下载插件管理器和插件程序，包括程序的新版本。

防毒墙网络版服务器

防毒墙网络版基于 HTTP 的服务器是所有客户端配置、安全风险日志及更新的中央储存库。

该服务器执行两个重要功能：

- 安装、监视和管理防毒墙网络版客户端
- 下载客户端所需的大多数组件。防毒墙网络版服务器从趋势科技 ActiveUpdate 服务器下载组件，然后将其分发到客户端

注意： 某些组件是由云安全服务器下载。有关详细信息，请参阅第 1-10 页的 [云安全服务器](#)。

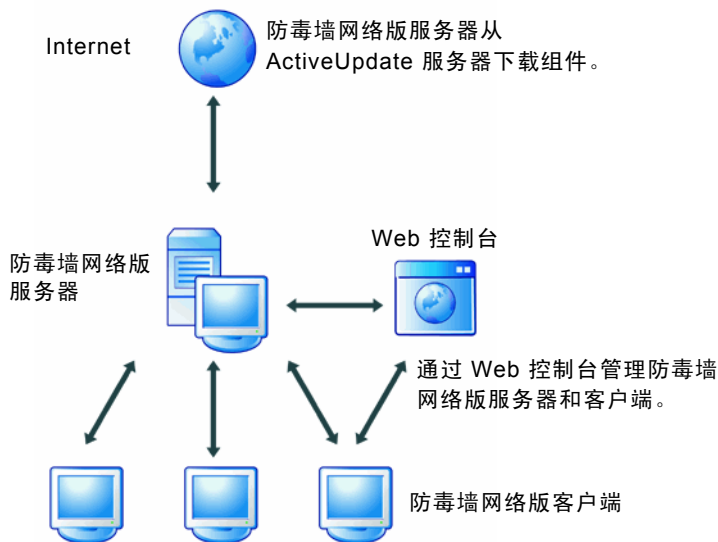


图 1-1. 防毒墙网络版服务器的工作原理

防毒墙网络版服务器可提供服务器与客户端之间的实时、双向通信。从基于浏览器的 Web 控制台（可从网络中的任何虚拟位置访问）管理客户端。服务器通过超文本传输协议 (HTTP) 与客户端（以及使用服务器的客户端）通信。

防毒墙网络版客户端

通过在每台计算机上安装防毒墙网络版客户端可保护 Windows 计算机免受安全风险的危害。客户端提供三种扫描方法：[实时扫描](#)、[预设扫描](#)和[手动扫描](#)。

客户端会向作为其安装源的父服务器报告。将客户端配置为通过使用[客户端迁移程序](#)工具向其他服务器报告。客户端将事件和状态信息实时发送到服务器。事件的示例包括病毒/恶意软件检测、客户端启动、客户端关闭、扫描启动和更新完成。

主要的客户端功能

计算机上的可用防毒墙网络版客户端功能取决于计算机的操作系统。

表 1-1. 客户端功能

功能	Windows 操作系统				
	2000	XP/ Server 2003 (32 位)	XP/ Server 2003 (64 位)	2008	Vista
手动扫描、实时扫描和预设扫描	是	是	是	是	是
组件更新（手动和预设更新）	是	是	是	是	是
更新代理	是	是	是	是	是
Web 信誉	是	是	是	是	是
Microsoft Outlook 邮件扫描	是	是	否	否	否
POP3 邮件扫描	是	是	是	是	是
防毒墙网络版防火墙	是	是	是	是	是
损害清除服务	是	是	是	是	是

表 1-1. 客户端功能（续）

功能	Windows 操作系统				
	2000	XP/ Server 2003 (32 位)	XP/ Server 2003 (64 位)	2008	Vista
Cisco NAC 支持	是	是	否	否	否
插件管理器	是	是	是	否	是
漫游模式	是	是	是	是	是
SecureClient 支持	是	是	否	否	否

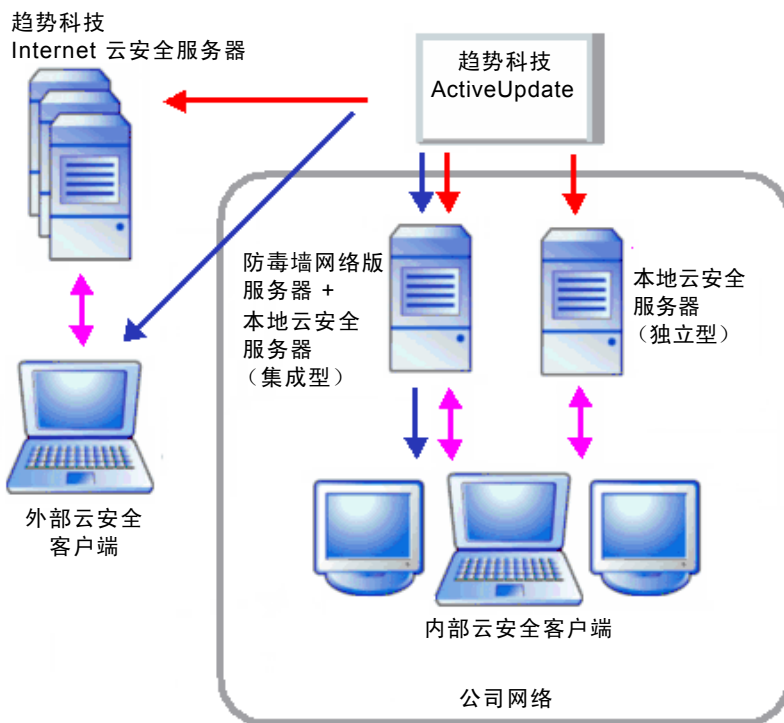
云安全服务器

云安全解决方案使用轻量级特征码，这些特征码协同工作，提供传统防恶意软件和防间谍软件特征码所能提供的相同防护。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。此病毒码每小时更新一次，它包含多数病毒码定义。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。在云安全解决方案中，客户端将趋势科技技术确定的识别信息发送到云安全服务器。客户端从不发送整个文件，而是使用识别信息确定文件的风险。

注意： 云安全解决方案中使用的其他特征码（称为云安全客户端病毒码）托管在客户端更新源（防毒墙网络版服务器或[定制的更新源](#)）上，供客户端下载。

云安全服务器与防毒墙网络版服务器之间不存在重叠的组件下载，因为每台服务器下载一组特定的组件。云安全服务器仅下载云安全云端病毒码，而防毒墙网络版服务器则下载所有其他组件。有关组件的详细信息，请参阅第 4-2 页的[防毒墙网络版组件与程序](#)。



>>云安全云端病毒码更新

>>扫描查询

>>云安全客户端病毒码更新

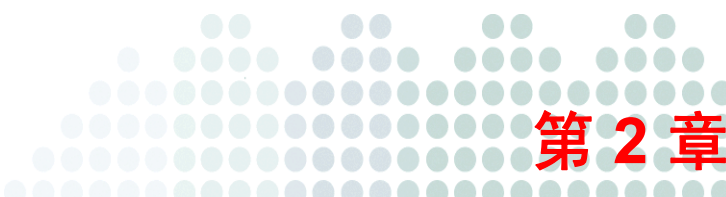
图 1-2. 趋势科技云安全扫描解决方法

云安全服务器类型

客户端连接到的云安全服务器取决于客户端的位置。内部云安全客户端连接到本地云安全服务器，而外部云安全客户端连接到趋势科技 Internet 云安全服务器。下表提供了这两种云安全服务器类型之间的对比：

表 1-2. 云安全服务器类型之间的对比

比较的基础	本地云安全服务器	趋势科技 Internet 云安全服务器
可用性	可用于内部客户端，即符合防毒墙网络版 Web 控制台上指定的位置条件的客户端。 有关位置条件的详细信息，请参阅第 9-2 页的 计算机位置	可用于外部客户端，即不符合防毒墙网络版 Web 控制台上指定的位置条件的客户端
用途	设计用于将扫描操作局限在公司网络内以提高效率	基于 Internet 的全局范围的基础架构，用于将云安全扫描服务提供给无法直接访问其公司网络的用户
服务器管理员	防毒墙网络版管理员安装和管理这些服务器	趋势科技维护此服务器
特征码更新源	趋势科技 ActiveUpdate 服务器	趋势科技 ActiveUpdate 服务器
客户端连接协议	HTTP 和 HTTPS	HTTPS



第 2 章

防毒墙网络版入门

本章主题：

- 第 2-2 页的 [Web 控制台](#)
- 第 2-5 页的 [安全性摘要](#)
- 第 2-10 页的 [防毒墙网络版客户端树](#)
- 第 2-19 页的 [防毒墙网络版域](#)
- 第 2-20 页的 [安全合规](#)

Web 控制台

Web 控制台是监控整个企业网络中的防毒墙网络版的中心点。该控制台提供一组缺省设置和缺省值，您可以根据安全需求和规范来配置这些缺省设置和缺省值。Web 控制台使用标准的 Internet 技术，如 Java、CGI、HTML 和 HTTP。

使用 Web 控制台执行以下操作：

- 管理在联网计算机上安装的客户端
- 将客户端聚集在逻辑域中以便同时配置和管理
- 设置扫描配置并在单个或多个联网计算机上启动手动扫描
- 配置关于网络中安全风险的通知并查看由客户端发送的日志
- 配置爆发条件和通知
- 通过配置角色和用户帐户将 Web 控制台管理任务委派给其他防毒墙网络版管理员

打开 Web 控制台

从网络上具有下列资源的任何计算机打开 Web 控制台：

- 300MHz Intel™ Pentium™ 处理器或同等处理器
- 128MB 内存
- 至少 30MB 的可用磁盘空间
- 在颜色为 256 或更高时，支持分辨率 800 x 600 的显示器
- Microsoft Internet Explorer™ 6.0 或更高版本

在 Web 浏览器上，根据防毒墙网络版服务器安装的类型在地址栏中键入以下内容之一：

表 2-1. 防毒墙网络版 Web 控制台 URL

安装类型	URL
缺省站点上无 SSL	http://<OfficeScan server>/OfficeScan
虚拟站点上无 SSL	http://<OfficeScan server>:<SSL port number>/ 防毒墙网络版
缺省站点上有 SSL	https://<OfficeScan server>/OfficeScan
虚拟站点上有 SSL	https://<OfficeScan server>:<SSL port number>/ 防毒墙网络版

注意： 如果从先前版本的防毒墙网络版升级，则 Web 浏览器和代理服务器缓存文件可能妨碍防毒墙网络版 Web 控制台正常加载。在浏览器和位于防毒墙网络版服务器和用来访问 Web 控制台的计算机之间的代理服务器上清除缓存内存。

登录帐户

在防毒墙网络版服务器安装期间，安装程序会创建一个 root 帐户并提示键入此帐户的密码。首次打开 Web 控制台时，键入“root”作为用户名和 root 帐户密码。如果忘记了密码，请与支持提供商联系以帮助重置密码。

定义用户角色并设置用户帐户以允许其他用户不使用 root 帐户访问 Web 控制台。用户登录到控制台时，他们可以使用您为他们设置的用户帐户。有关详细信息，请参阅第 8-2 页的[基于角色的管理](#)。

Web 控制台旗标

Web 控制台的旗标区域提供下列选项：



图 2-1. Web 控制台旗标区域

<帐户名称>：单击帐户名称（例如， root）以修改帐户的详细信息，如密码

注销：从 Web 控制台注销

帮助

- **新功能**：打开当前产品版本中包括的新功能列表页面
- **目录和索引**：打开 *防毒墙网络版服务器帮助*
- **知识库**：打开趋势科技知识库，您可以在其中查看 FAQ 和更新的产品信息，访问客户支持并注册防毒墙网络版
- **安全信息**：显示“趋势科技安全信息”页面，其中您可以阅读有关最新安全风险的信息
- **销售**：显示“趋势科技销售” Web 页面，其中您可以联系区域销售代表
- **支持**：显示“趋势科技技术支持” Web 页面，其中您可以提交问题并查找有关趋势科技产品常见问题的答案
- **关于**：显示包含产品概述和告诉您如何检查组件版本的页面

安全性摘要

打开防毒墙网络版 Web 控制台或者单击主菜单中的**摘要**时，将显示“摘要”窗口。查看产品使用授权的当前状态及总体安全风险防护的信息，并在需要立即干预的项（如病毒爆发或过期的组件）上采取措施。

提示： 定期刷新窗口以获取最新的信息。

产品使用授权状态

在此部分中查看产品使用授权的状态。



图 2-2. “摘要”窗口 — 产品使用授权状态部分

以下实例中将显示提醒信息：

如果您具有完全版使用授权

- 使用授权到期前 60 天。
- 在产品的宽限期内。宽限期的持续时间可能因地区而异。请通过趋势科技代表验证宽限期。
- 当使用授权到期且宽限期已过时。在此期间，您将无法获得技术支持或无法执行组件更新。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。

如果您具有评估版使用授权

- 使用授权到期前 14 天。
- 当使用授权过期时。在此期间，防毒墙网络版将禁用组件更新、扫描和所有客户端功能组件。

如果已经获取激活码，请转至**管理 > 产品使用授权**以续订使用授权。

联网计算机

所有选项卡显示下列信息：



图 2-3. “摘要”窗口 — “所有”选项卡

- 所有防毒墙网络版客户端与防毒墙网络版服务器的连接状态
- 检测到的安全风险数量
- 已在其中检测到安全风险的计算机

传统扫描选项卡显示下列信息：



图 2-4. “摘要”窗口 — “传统扫描”选项卡

- **传统扫描**客户端与防毒墙网络版服务器的连接状态
- 检测到的安全风险数量
- 已在其中检测到安全风险的计算机

云安全扫描选项卡显示下列信息：



图 2-5. “摘要”窗口 — “云安全扫描”选项卡

- **云安全扫描**客户端与防毒墙网络版服务器的连接状态
- 联机云安全客户端与云安全服务器的连接状态

注意： 仅联机客户端可以报告其与云安全服务器的连接状态。

如果客户端已从云安全服务器断开连接，则通过执行第 9-36 页的**客户端无法连接到云安全服务器**中的步骤恢复连接。

- 检测到的安全风险数量
- 已在其中检测到安全风险的计算机
- 云安全服务器列表
- 连接到每台云安全服务器的客户端数。单击该数字打开可在其中管理客户端设置的客户端树
- 对于每台云安全服务器，存在一个用于启动服务器控制台的链接

- **更多链接**（如果您的客户端连接到两个以上的云安全服务器）打开一个窗口，您可以在其中执行以下操作：
 - 查看客户端连接到的所有本地云安全服务器和连接到每台服务器的客户端数。单击该数字打开可在其中管理客户端设置的客户端树
 - 通过单击服务器的链接启动服务器的控制台

前 10 项安全风险统计

检测状态表上的链接打开包含前 10 项安全风险统计的窗口。

联网计算机的前 10 项安全风险统计

刷新

帮助

摘要 > 联网计算机的前 10 项安全风险统计

病毒/恶意软件统计：

病毒/恶意软件	
名称	感染数目

上次重置时间：

重置计数

受感染计算机		
名称	检测到的数目	日志

上次重置时间：

重置计数

感染源	
名称	检测到的数目

间谍软件/灰色软件统计：

间谍软件/灰色软件	
名称	感染数目

上次重置时间：

重置计数

受感染计算机		
名称	检测到的数目	日志

上次重置时间：

重置计数

图 2-6. “前 10 项安全风险”窗口

此窗口中的任务：

- 单击安全风险名以查看该安全风险的详细信息。
- 单击计算机名以查看特定计算机的总体状态。

- 单击对应于计算机名的**查看**以查看该计算机的安全风险日志。
- 单击**重置计数**以重置每张表的统计信息。

病毒爆发状态

病毒爆发状态表提供任何当前安全风险爆发的状态和上次爆发警报。

病毒爆发状态			
	类型	当前爆发	上次爆发
	病毒/恶意软件	无	无
	间谍软件/灰色软件	无	无
	防火墙违例	无	无

图 2-7. “摘要”窗口 — “病毒爆发状态”部分

单击警报的日期/时间链接以查看爆发详细信息。当防毒墙网络版检测到爆发时，它会重置爆发警报信息的状态并立即强制执行爆发阻止措施。

组件和程序

更新状态表包含可用组件和程序，可保护联网计算机免遭安全风险。

联网计算机的更新状态 (在线客户端: 1 云安全扫描: 1 传统扫描: 0)					全部折叠	全部展开
防病毒	当前版本	已更新	已过期	更新率		
云安全客户端病毒码	5.885.00	1	0	100%		
传统病毒码	6.202.60	0	0	0%		
IntelliTrap 特征码	0.115.00	1	0	100%		
IntelliTrap 例外特征码	0.441.00	1	0	100%		
病毒扫描引擎 (32 位)	8.950.1094	1	0	100%		
病毒扫描引擎 (64 位)	8.950.1094	0	0	0%		
防间谍软件	当前版本	已更新	已过期	更新率		
间谍软件病毒码	7.77	1	0	100%		
间谍软件主动监控特征码	0.783.00	0	0	0%		
间谍软件扫描引擎 (32 位)	6.2.3009	1	0	100%		
间谍软件扫描引擎 (64 位)	6.2.3009	0	0	0%		

图 2-8. “摘要”窗口 — 组件和程序部分

查看每个组件的当前版本。在**已过期**列下，查看带有过期组件的客户端数。如果存在需要更新的客户端，则单击数字链接开始更新。

对每个程序，通过单击对应于该程序的编号链接查看尚未升级的客户端。

注意： 要升级 Cisco Trust Agent，请转至 **Cisco NAC > 代理部署**。

防毒墙网络版客户端树

基于 Java 的客户端树显示服务器当前管理的所有客户端（分组为**防毒墙网络版域**）。将客户端分组为域，可以同时对所有域成员配置、管理和应用相同的配置。

访问主菜单中的某些功能时，客户端树会以主框架的形式显示。

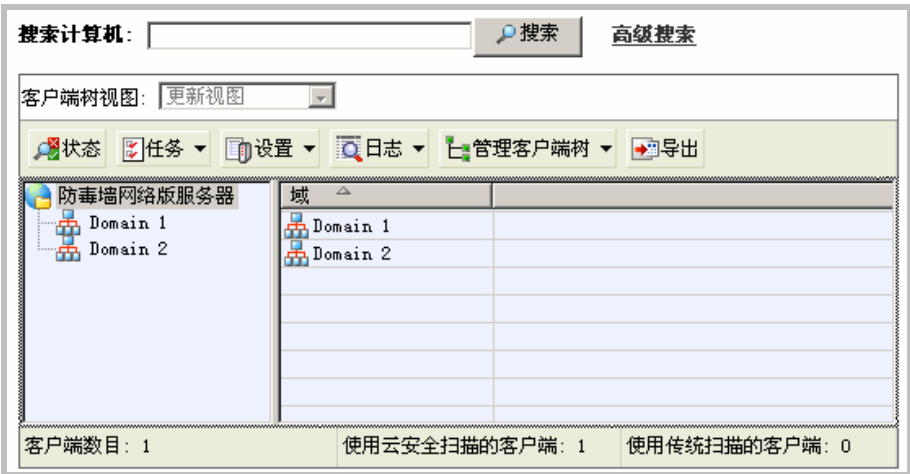


图 2-9. 防毒墙网络版客户端树

客户端树常规任务

下面是客户端树显示时可以执行的常规任务：

- 单击根图标  以选择所有域和客户端。当选择根图标然后选择客户端树上的某个任务时，将显示用于配置设置的窗口。在该窗口上，从下列常规选项作出选择：
 - **应用到全部客户端：**将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - **仅应用到将来的域：**仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。
- 要选择多个相邻的域或客户端，请单击范围内的第一个域或客户端，按住 SHIFT 键，然后单击范围内的最后一个域或客户端。
- 要选择一系列间断的域或客户端，按下 CTRL 键，然后单击您想要选择的域或客户端。
- 通过在 **搜索计算机** 文本框中指定客户端名称来搜索要管理的客户端。匹配客户端名称的列表将在客户端树中加亮显示。要获取更多搜索选项，请单击 **高级搜索**。
- 选择域后，客户端树表将展开以显示属于该域的客户端和包含每个客户端相关信息的所有列。要仅查看一组相关的列，请在客户端树视图中选择一项。
 - **更新视图：**显示所有组件和程序
 - **防病毒视图：**显示防病毒组件
 - **防火墙视图：**显示防火墙组件
 - **防间谍软件视图：**显示防间谍软件组件
 - **云安全扫描视图：**显示客户端（传统扫描或云安全扫描）和云安全扫描组件使用的扫描方法
 - **查看全部：**显示所有列
- 通过拖动列标题到客户端树中的不同位置来重新排列列。防毒墙网络版会自动保存新的列位置。
- 通过单击列名称根据列信息来排列客户端。

- 单击  刷新客户端树。
- 查看客户端树下的客户端统计，如客户端总数、云安全客户端数和传统客户端数。

高级搜索选项

根据以下条件搜索客户端：

- **基本条件：**包括关于计算机的基本信息，如 IP 地址、操作系统和 MAC 地址。

注意：按 IP 段搜索要求 IP 地址的一部分以第一个八位组开始。搜索将返回 IP 地址包含上述条目的所有计算机。例如，键入 10.5 将返回 IP 地址范围从 10.5.0.0 到 10.5.255.255 的所有计算机。

按 MAC 地址搜索要求用十六进制计数法表示的 MAC 地址范围，例如，000F3E341D51。

- **组件版本：**选中邻近组件名称的复选框，通过选择“早于”或“早于并包括”来缩小条件，然后键入版本号。缺省显示当前版本号。
- **状态：**包括客户端设置和实时状态。

指定搜索条件后单击**搜索**。满足条件的计算机名称列表将显示在客户端树中。

客户端树特定任务

在 Web 控制台上访问某些特定窗口时，将显示客户端树。客户端树上的菜单项特定于已访问过的窗口。这些菜单项允许执行特定任务，如配置客户端设置或启动客户端任务。要执行其中任何一个任务，首先选择该任务目标（将设置应用到所有客户端的根图标、一个或多个域或者一台或多台客户端），然后选择菜单项。

联网计算机 > 客户端管理

在此窗口上管理常规客户端设置。

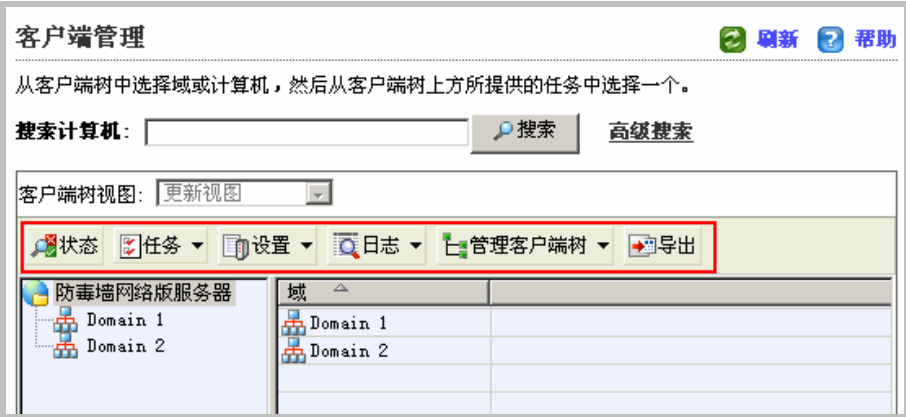


图 2-10. “客户端管理”窗口

任务：

表 2-2. 客户端管理任务

菜单按钮	任务
状态	查看客户端详细信息。有关详细信息，请参阅第 9-43 页的 客户端信息 。
任务	- 在客户端计算机上运行手动扫描。有关详细信息，请参阅第 5-23 页的 启动立即扫描。 - 卸载客户端。有关详细信息，请参阅第 3-46 页的 从 Web 控制台卸载客户端。 - 恢复间谍软件/灰色软件组件。有关详细信息，请参阅第 5-39 页的 间谍软件/灰色软件恢复。

表 2-2. 客户端管理任务（续）

菜单按钮	任务
设置	- 从可用扫描方法中进行选择。有关详细信息，请参阅第 5-8 页的扫描方法。 - 为每种扫描类型配置设置。有关详细信息，请参阅以下主题： - 第 5-20 页的手动扫描 - 第 5-18 页的实时扫描 - 第 5-21 页的预设扫描 - 第 5-22 页的立即扫描 - 将客户端指定为更新代理。有关详细信息，请参阅第 4-35 页的更新代理配置。 - 配置客户端权限和其他设置。有关详细信息，请参阅第 9-5 页的客户端权限和其他设置。 - 配置 Web 信誉策略。有关详细信息，请参阅第 6-3 页的Web 信誉策略。 - 配置设备控制设置。有关详细信息，请参阅第 5-60 页的设备控制。 - 配置间谍软件/灰色软件允许列表。有关详细信息，请参阅第 5-38 页的间谍软件/灰色软件允许列表。 - 导入和导出客户端设置。有关详细信息，请参阅第 9-44 页的导入和导出客户端设置。

表 2-2. 客户端管理任务（续）

菜单按钮	任务
日志	查看下列日志： - 第 5-45 页的 病毒/恶意软件日志 - 第 5-51 页的 间谍软件/灰色软件日志 - 第 7-17 页的 防火墙日志 - 第 6-7 页的 Web 信誉日志 - 第 5-62 页的 设备控制日志 管理日志。有关详细信息，请参阅第 8-18 页的 日志维护 。
管理客户端树	管理防毒墙网络版域。有关详细信息，请参阅第 2-19 页的 防毒墙网络版域 。
导出	将客户端列表导出为逗号分隔值 (.csv) 文件

联网计算机 > 爆发阻止

任务：指定并激活[爆发防护](#)设置。

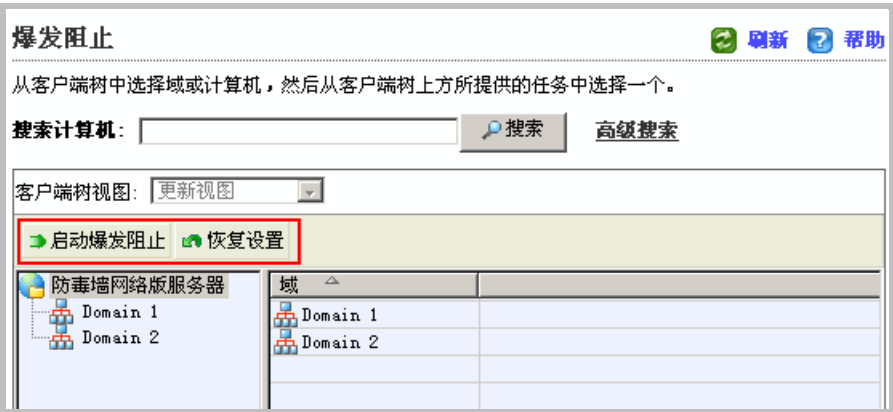


图 2-11. “爆发阻止”窗口

更新 > 联网计算机 > 手动更新 > 手动选择客户端

任务：在客户端上启动[手动更新](#)。



图 2-12. “组件更新”窗口

更新 > 还原 > 与服务器同步

任务：执行[组件还原](#)。

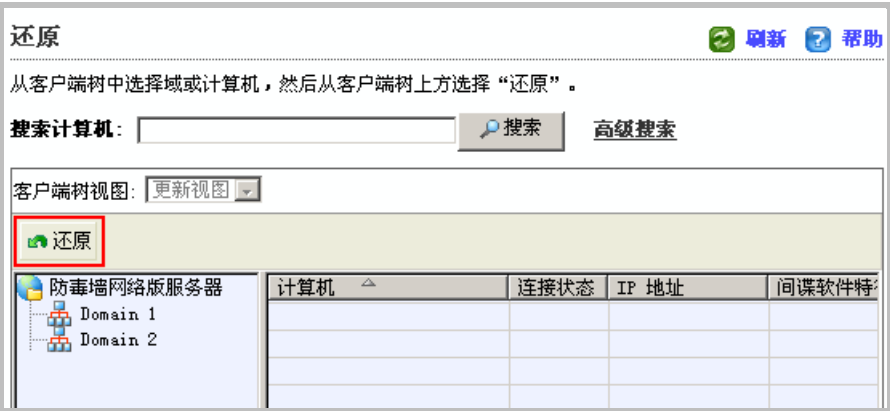


图 2-13. “还原”窗口

日志 > 联网计算机日志 > 安全风险

查看和管理此窗口上的日志。

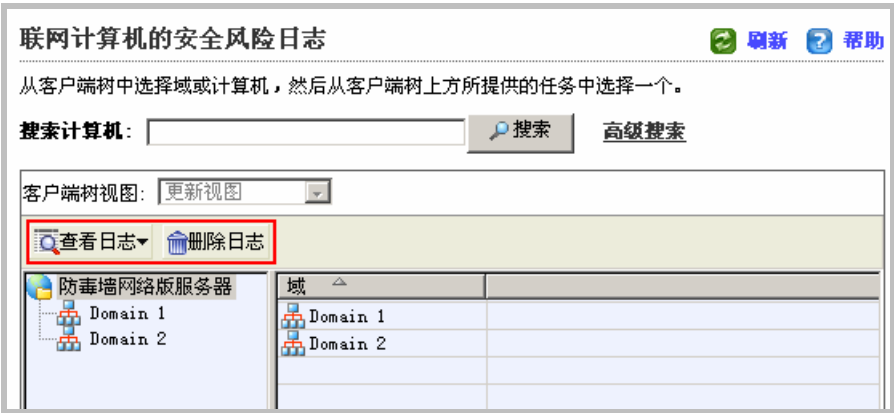


图 2-14. “安全风险日志”窗口

任务：

- 查看下列日志：
 - 病毒/恶意软件日志
 - 间谍软件/灰色软件日志
 - 防火墙日志
 - Web 信誉日志
 - 设备控制日志
- 执行日志维护。

Cisco NAC > 代理部署

任务：执行 **Cisco Trust Agent 部署**。

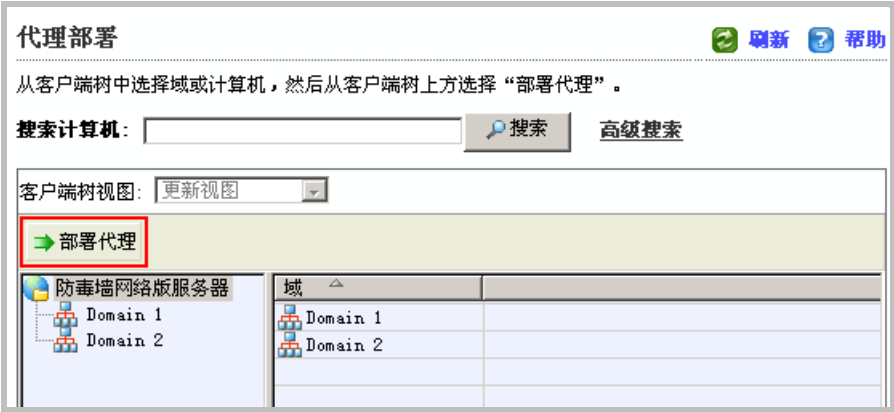


图 2-15. “代理部署”窗口

防毒墙网络版域

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端。通过将客户端分组为域，可以同时对所有域成员配置、管理和应用相同的配置。

为简化管理，根据部门或所执行的功能对客户端分组。另外，对更易受感染的客户端进行分组，以对它们应用更安全的配置。

缺省情况下，防毒墙网络版模拟网络上的域。客户端树中的域名和客户端名与网络上的域名和计算机名相同。防毒墙网络版还根据网络上的域结构分配客户端。删除或更名防毒墙网络版创建的域、创建新域、或将客户端从一个域转移到另一个域。

添加域：

导航路径：联网计算机 > 客户端管理 > 管理客户端树 > 添加域

1. 键入要添加的域名。
2. 单击**添加**。新的域将显示在客户端树中。

删除域或客户端：

导航路径：联网计算机 > 客户端管理 > 管理客户端树 > 删除域/客户端

1. 要删除域，请删除或移动域下的所有客户端。要将客户端移动到其他域，可以把它们拖放到目标域。
2. 当域为空时，单击**删除域/客户端**。
3. 要删除客户端，请单击**删除域/客户端**。如果选择了一个域，单击“删除域/客户端”将删除该域下所有的客户端。

注意： 虽然已删除的客户端不再在客户端树中显示，但并没有从客户端计算机将其卸载。防毒墙网络版客户端仍可执行依赖服务器的任务，例如，更新组件。但服务器未感知到客户端的存在，因此无法向该客户端发送配置或通知。

更名域:

导航路径: 联网计算机 > 客户端管理 > 管理客户端树 > 更名域

1. 键入域的新名称。
2. 单击**更名**。新的域名将显示在客户端树中。

移动客户端:

导航路径: 联网计算机 > 客户端管理 > 管理客户端树 > 移动客户端

1. 选择是否要将客户端移动到其他域或防毒墙网络版服务器。
 - a. 要将客户端移动到另一个域, 请选择**将选定的客户端移动到另一个域**, 从下拉列表选择域, 并决定是否将新域的设置应用到这些客户端。

提示: 或者, 在客户端树中, 将客户端拖放到其他域。

- b. 要将客户端移动到另一个防毒墙网络版服务器, 在**将选定的客户端移动到另一个防毒墙网络版服务器**下面, 输入服务器名称和 HTTP 端口号。
2. 单击**移动**。

安全合规

“安全合规”利用 Microsoft Active Directory™ 服务确定网络上计算机的安全状态。在查询 Active Directory 之后, Web 控制台显示计算机的安全状态。安全状态可以是以下任何状态:

- 由防毒墙网络版服务器管理
- 由另一个防毒墙网络版服务器管理
- 未安装防毒墙网络版客户端程序
- 无法访问

要使用“安全合规”, 请确保防毒墙网络版服务器计算机是 Active Directory 域的成员。

要强制实施安全合规，请执行下列任务：

1. 定义 **Active Directory 作用域和查询**。
2. 从 **Active Directory 查询结果** 检查不受保护的计算机。
3. 执行 **防毒墙网络版客户端安装**。
4. 配置 **预设查询**。

Active Directory 作用域和查询

首次使用“安全合规”时，需要定义 Active Directory 作用域，包括防毒墙网络版服务器将按需或定期查询的 Active Directory 对象。在定义作用域之后，启动查询进程。

配置 Active Directory 作用域并启动查询进程：

导航路径：安全合规

1. 在 Active Directory 作用域部分，单击**定义**。
2. 在打开的窗口中，Active Directory 结构将显示。选择要查询的对象。

提示： 首次进行查询时，选择少于 1000 个帐户的对象，然后记录需要使用多少时间才能完成这次查询。将此数据用作性能基准。

3. 在**高级设置**之下，指定防毒墙网络版服务器与客户端进行通信时使用的端口。在防毒墙网络版服务器安装期间，安装程序随机生成端口号。

提示： 要查看防毒墙网络版服务器使用的通信端口，请转至**联网计算机 > 客户端管理**并选择域。检查 **IP 地址** 列。端口号在 IP 地址后显示。保留端口号记录作为参考。

- a. 单击**指定端口**。
- b. 键入端口号并单击**添加**。重复此步骤，直到获得要添加的所有端口号。
- c. 单击**保存**。

4. 选择是否使用特定端口号检查计算机的连接。没有建立连接时，防毒墙网络版会立即将计算机视为无法访问。缺省端口号为 135。

提示： 启用此设置可加速 Active Directory 查询。无法建立到计算机的连接时，在将计算机视为无法访问之前，防毒墙网络版服务器不再需要执行所有其他连接验证任务。

5. 要保存 Active Directory 作用域并启动查询，请单击**保存并重新评估**。要仅保存设置，请单击**仅保存**。

“安全合规”窗口与查询结果一起显示。

注意： 查询可能需要很长时间才能完成，尤其是当查询作用域较大时。在“安全合规”窗口显示结果之前，一直不要执行其他查询。否则，当前查询会话将终止，并且查询进程重新启动。

Active Directory 查询结果

安全状态部分将计算机归类如下：

表 2-3. 计算机防护状态

状态	描述
由此防毒墙网络版服务器管理	计算机上安装的防毒墙网络版客户端由防毒墙网络版服务器管理。客户端为联机、脱机或漫游状态，并且运行此防毒墙网络版版本或早期版本。
由另一个防毒墙网络版服务器管理	计算机上安装的防毒墙网络版客户端由另一个防毒墙网络版服务器管理。客户端为联机状态，并且运行此防毒墙网络版版本或早期版本。
未安装防毒墙网络版客户端	防毒墙网络版客户端未安装在计算机上。

表 2-3. 计算机防护状态（续）

状态	描述
无法访问	防毒墙网络版服务器无法连接到计算机，因此无法确定计算机上是否安装有客户端，或者如果安装了客户端，则客户端是由其他防毒墙网络版服务器管理还是处于不受管理的状态。 注意： 防毒墙网络版服务器数据库包含服务器管理的客户端的列表。如果无法访问客户端计算机，但是防毒墙网络版服务器检测到它管理着计算机上安装的客户端，则计算机的状态为“由此防毒墙网络版服务器管理”。

建议的任务：

1. 在**安全状态**部分，单击数字链接显示客户端树中所有受影响的计算机。
2. 使用搜索和高级搜索功能仅搜索和显示满足搜索条件的计算机。

如果使用高级搜索功能，则指定下列项的完整名称：

- 计算机名称
- 防毒墙网络版服务器
- 防毒墙网络版域
- Active Directory 树

如果不知道确切的完整名称，请使用通配符 (*)。

如果名称不完全且没有指定通配符，则防毒墙网络版不会返回结果。

3. 要将计算机列表保存到文件，请单击**导出**。
4. 对于由其他防毒墙网络版服务器管理的客户端，使用客户端迁移程序工具让当前的防毒墙网络版服务器来管理这些客户端。有关此工具的详细信息，请参阅第 9-41 页的[客户端迁移程序](#)。

防毒墙网络版客户端安装

在安装此客户端之前，请注意以下事项：

1. 记录每台计算机的登录凭证。在安装期间，防毒墙网络版将提示您指定登录凭证。
2. 如果以下情况属实，则计算机上不会安装防毒墙网络版客户端：
 - 已将防毒墙网络版服务器安装在计算机上。
 - 计算机运行 Windows XP Home、Windows Vista™ Home Basic 和 Windows Vista Home Premium。如果计算机运行这些平台，则选择其他安装方法。有关详细信息，请参阅第 3-10 页的[安装方法](#)。
3. 如果目标计算机运行 Windows Vista Business、Enterprise 或 Ultimate Edition，则在计算机上执行以下步骤：
 - a. 启用内置管理员帐户并为该帐户设置密码。
 - b. 禁用 Windows 防火墙。
 - c. 单击**开始 > 所有程序 > 管理工具 > 高级安全 Windows 防火墙**。
 - d. 针对域概要文件、专用概要文件和通用概要文件，将防火墙状态设置为“关闭”。
 - e. 打开 Microsoft 管理控制台（单击**开始 > 运行**，键入 **services.msc**），然后启动 **Remote Registry** 服务。安装防毒墙网络版客户端时，请使用内置管理员帐户和密码。
4. 如果计算机上安装有趋势科技或第三方端点安全程序，则检查防毒墙网络版是否可以自动卸载该软件并将其替换为防毒墙网络版客户端。有关防毒墙网络版自动卸载的端点安全软件的列表，请打开 <[服务器安装文件夹](#)>\PCCSRV\Admin 中的以下文件。可以使用文本编辑器（如记事本）打开这些文件。
 - tmuninst.ptn
 - tmuninst_as.ptn

如果目标计算机上的软件不包括在列表中，请首先手动卸载它。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。

安装防毒墙网络版客户端：

导航路径：安全合规

1. 在客户端树顶部单击**安装**。

如果计算机上安装有早期防毒墙网络版客户端版本时单击**安装**，则会跳过安装而不会将客户端升级到此版本。要升级客户端，请参阅[第9-15页的更新设置](#)。

2. 为每台计算机指定管理员登录帐户，并单击**登录**。防毒墙网络版开始在目标计算机上安装客户端。
3. 查看安装状态。

预设查询

防毒墙网络版可以根据时间表自动查询 Active Directory。

配置查询时间表：

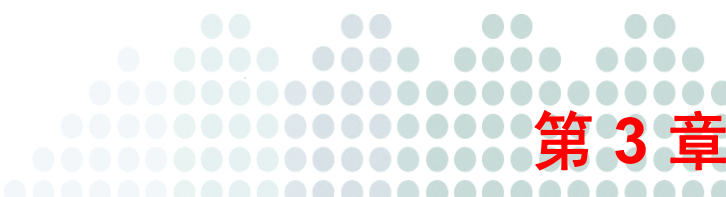
导航路径：安全合规

1. 在“安全合规”客户端树顶部单击**设置**。
2. 启用预设查询。
3. 指定时间表。如果指定每个月的第31天，而这个月少于31天，则在该月的最后一天进行评估。
4. 要保存时间表，单击“仅保存”。要执行查询而不保存时间表，请单击“立即查询”。

第 1 部分

保护联网计算机





第 3 章

安装防毒墙网络版客户端

本章主题：

- 第 3-2 页的 [安装需求](#)
- 第 3-10 页的 [安装方法](#)
- 第 3-40 页的 [迁移到防毒墙网络版客户端](#)
- 第 3-44 页的 [安装后](#)
- 第 3-46 页的 [卸载客户端](#)

安装需求

防毒墙网络版客户端可以安装到运行以下平台的计算机上：

- **Windows 2000**
- **Windows XP/2003， 32 位版本**
- **Windows XP/2003， 64 位版本**
- **Windows Vista， 32 位和 64 位版本**
- **Windows 2008， 32 位版本**
- **Windows 2008， 64 位版本**

表 3-1. Windows 2000

资源	需求
操作系统	• 带有 Service Pack 4 的 Windows 2000 • 带有 Service Pack 4 的 Windows 2000 Professional • 带有 Service Pack 4 的 Windows 2000 Server • 带有 Service Pack 4 的 Windows 2000 Advanced Server • 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 操作系统中安装客户端： • 带有 Service Pack 1 的 Microsoft Virtual Server 2005 R2 • 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

表 3-1. Windows 2000（续）

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 256MB，建议使用 512MB 可用磁盘空间 最低要求是 350MB 其他 在颜色为 256 或更高时，支持分辨率 800 x 600 的显示器

表 3-2. Windows XP/2003，32 位版本

资源	需求
操作系统	• 带有 Service Pack 2 的 Windows XP Professional 或更高版本 • 带有 Service Pack 3 的 Windows XP Home 或更高版本 • 带有 Service Pack 2 的 Windows Server™ 2003（Standard、Enterprise、Datacenter 和 Web 版）或更高版本 • 带有 Service Pack 2 的 Windows Server 2003 R2（Standard、Enterprise 和 Datacenter 版）或更高版本 • Windows Storage Server 2003 • 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 XP/2003 操作系统中安装客户端： • 带有 Service Pack 1 的 Microsoft Virtual Server 2005 R2 • 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

表 3-2. Windows XP/2003， 32 位版本（续）

资源	需求
硬件	处理器 300MHz Intel Pentium 或同等处理器 AMD™ 64 或 Intel 64 处理器体系结构 内存 最低要求是 256MB，建议使用 512MB 可用磁盘空间 最低要求是 350MB 其他 颜色为 256 时支持分辨率为 800 x 600 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 • 禁用 Windows XP 计算机上的简单文件共享，以便用户成功安装防毒墙网络版客户端程序（请参阅 Windows 文档来获取指导信息）

表 3-3. Windows XP/2003， 64 位版本

资源	需求
操作系统	• 带有 Service Pack 2 的 Windows XP Professional 或更高版本 • 带有 Service Pack 2 的 Windows Server 2003（Standard、Enterprise、Datacenter 和 Web 版）或更高版本 • 带有 Service Pack 2 的 Windows Server 2003 R2（Standard、Enterprise 和 Datacenter 版）或更高版本 • Windows Storage Server 2003 • 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 XP/2003 操作系统中安装客户端： • 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
硬件	处理器 • Intel x64 处理器 • AMD64 处理器 内存 最低要求是 256MB，建议使用 512MB 可用磁盘空间 最低要求是 350MB 其他 颜色为 256 吋支持分辨率为 800 x 600 的监视器

表 3-3. Windows XP/2003， 64 位版本（续）

资源	需求
其他	• 如果执行 Web 安装，则需要 Microsoft Internet Explorer 6.0 或更高版本 • 禁用 Windows XP 计算机上的简单文件共享，以便用户成功安装防毒墙网络版客户端程序（请参阅 Windows 文档来获取指导信息）

表 3-4. Windows Vista， 32 位和 64 位版本

资源	需求
操作系统	• 带有 Service Pack 1 的 Windows Vista™ Business Edition 或更高版本 • 带有 Service Pack 1 的 Windows Vista Enterprise Edition 或更高版本 • 带有 Service Pack 1 的 Windows Vista Ultimate Edition 或更高版本 • 带有 Service Pack 1 的 Windows Vista Home Premium Edition 或更高版本 • 带有 Service Pack 1 的 Windows Vista Home Basic Edition 或更高版本 • 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 Vista 操作系统中安装客户端： • 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

表 3-4. Windows Vista， 32 位和 64 位版本（续）

资源	需求
硬件	处理器 • 800MHz Intel Pentium 或同等处理器 • AMD64 或 Intel 64 处理器体系结构 内存 最低要求是 1GB，建议使用 1.5GB 可用磁盘空间 最低要求是 350MB 其他 颜色为 256 时支持分辨率为 800 x 600 的监视器
其他	如果执行 Web 安装，则需要 Windows Internet Explorer 7.0 或更高版本

表 3-5. Windows 2008， 32 位版本

资源	需求
操作系统	• 带有 Service Pack 1 的 Windows Server 2008（Standard、Enterprise、Datacenter 和 Web 版）或更高版本 • 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 2008 操作系统中安装客户端： • 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 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。

表 3-5. Windows 2008， 32 位版本（续）

资源	需求
硬件	处理器 • 最低 1GHz Intel Pentium 或同等处理器，建议使用 2GHz • AMD64 和 Intel 64 处理器体系结构 内存 最低要求是 512MB，建议使用 2GB 可用磁盘空间 最低要求是 350MB 其他 颜色为 256 时支持分辨率为 800 x 600 的监视器
其他	如果执行 Web 安装，则需要 Windows Internet Explorer 7.0 或更高版本

表 3-6. Windows 2008， 64 位版本

资源	需求
操作系统	• 带有 Service Pack 1 的 Windows Server 2008（Standard、Enterprise、Datacenter 和 Web 版）或更高版本 • 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 2008 操作系统中安装客户端： • 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 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。

表 3-6. Windows 2008， 64 位版本（续）

资源	需求
硬件	处理器 • 最低 1.4GHz Intel Pentium 或同等处理器，建议使用 2GHz • AMD64 和 Intel 64 处理器体系结构 内存 最低要求是 512MB，建议使用 2GB 可用磁盘空间 最低要求是 350MB 其他 颜色为 256 时支持分辨率为 800 x 600 的监视器
其他	如果执行 Web 安装，则需要 Windows Internet Explorer 7.0 或更高版本

兼容性列表

防毒墙网络版与以下第三方产品兼容：

- Citrix XenApp™ Server 4.5 和 5.0（32 位和 64 位）
- Microsoft ActiveSync™ 4.2、4.5
- Microsoft Cluster Server 2000
- Microsoft Cluster Server 2003
- Microsoft Office 2000、XP 和 2003
- Microsoft SQL Server™ 7.0、2000 和 2008
- 带有 Service Pack 2 的 Microsoft Systems Management Server (SMS) 2003 或更高版本
- Nortel VPN Client™（有限制）
- Outlook 邮件扫描支持 Microsoft Office Outlook™ 2000、2002、2003 和 2007

- POP3 邮件扫描支持以下电子邮件程序：
 - Becky!Internet Mail 2.0
 - Eudora™ 6.2
 - Microsoft Outlook Express 6.0
 - Microsoft Office Outlook 2000、2002、2003 和 2007
 - Mozilla Thunderbird™ 1.5 和 2.0
 - Netscape™ 7.2
 - Windows Mail （仅适用于 Windows Vista）
 - Foxmail 5.0 和 6.0
- Windows 2000、2003 和 2008 上的终端服务
- Windows Mobile Device Center 6 （32 位）
- Windows Mobile Device Center 6.1 （32 位和 64 位）
- Windows Server 2008 故障转移群集
- 带有 Service Pack 2 的 Windows XP Tablet PC 版

安装方法

本节概要介绍执行防毒墙网络版客户端全新安装的不同客户端安装方法。所有安装方法都要求目标计算机上的本地管理员权限。

表 3-7. 安装方法

安装方法/操作系统支持	部署注意事项					
	WAN 部署	集中管理	需求用户干预	需求 IT 资源	大规模部署	所用带宽
Web 安装页面 所有操作系统都支持	否	否	是	否	否	高
登录脚本安装 所有操作系统都支持	否	否	是	是	否	高，如果安装同时启动

表 3-7. 安装方法（续）

安装方法/操作系统支持	部署注意事项					
	WAN 部署	集中 管理	需求 用户干预	需求 IT 资源	大规模 部署	所用 带宽
客户端打包程序 所有操作系统都支持	否	否	是	是	否	低，如果 已预设
客户端打包程序（通过 Microsoft SMS 部署的 MSI 软件包） 所有操作系统都支持	是	是	是/否	是	是	低，如果 已预设
客户端打包程序（通过 Active Directory 部署的 MSI 软件包） 所有操作系统都支持	是	是	是/否	是	是	高，如果 安装同时 启动
从防毒墙网络版 Web 控制台 除以下操作系统外的所有操作 系统都支持： - Windows Vista Home Basic 和 Home Premium 版 - Windows XP Home 版	否	是	否	是	否	高
客户端磁盘镜像 除以下操作系统外的所有操作 系统都支持： - Windows Vista - Windows 2008 64 位平台	否	否	否	是	否	低

表 3-7. 安装方法（续）

安装方法/操作系统支持	部署注意事项					
	WAN 部署	集中管理	需求 用户干预	需求 IT 资源	大规模部署	所用带宽
趋势科技漏洞扫描程序 (TMVS) 除以下操作系统外的所有操作系统都支持： - Windows Vista Home Basic 和 Home Premium 版 - Windows XP Home 版	否	是	否	是	否	高

从 Web 安装页安装

如果已将防毒墙网络版服务器安装到运行以下平台的计算机，则用户可以从 Web 安装页面安装客户端程序：

- Windows 2000 Server
- 具有 Internet Information Server (IIS) 6.0 或 Apache 2.0.x 的 Windows Server 2003

要从 Web 安装页安装，您需要以下项：

- 安全级别设置为允许 ActiveX™ 控件的 Internet Explorer。所需版本如下：
 - Windows 2000 上为 5.0
 - Windows XP/Server 2003 上为 6.0
 - Windows Vista/2008 上为 7.0
- 计算机上的管理员权限

从 Web 安装页面向用户发送以下指令，以安装防毒墙网络版客户端。要通过电子邮件发送客户端安装通知，请参阅第 3-14 页的[启动基于浏览器的安装](#)。

从 Web 安装页安装：

1. 使用内置管理员帐户登录到计算机。
2. 如果安装到运行 Windows XP、Vista 和 2008 的计算机，请执行以下步骤：
 - a. 启动 Internet Explorer 并将防毒墙网络版服务器 URL（如 https://<防毒墙网络版服务器名称>:4343/officescan）添加到受信任的站点列表。在 Windows XP Home 中，通过转至工具 > **Internet 选项** > **安全** 选项卡，选择**受信任的站点**图标并单击**站点**，访问该列表。
 - b. 修改 Internet Explorer 安全设置以启用 **ActiveX 控件自动提示**。在 Windows XP 中，转至工具 > **Internet 选项** > **安全** 选项卡，然后单击**自定义级别**。
3. 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`
4. 单击登录页上的链接。
5. 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端。客户端安装即开始。出现提示时，允许 ActiveX 控件安装。安装后防毒墙网络版客户端图标将显示在 Windows 系统托盘中。

注意： 有关在系统托盘上显示的图标的列表，请参阅第 9-30 页的**客户端与服务器的连接**。

启动基于浏览器的安装

设置指示网络上的用户安装防毒墙网络版客户端的电子邮件。用户单击该电子邮件中提供的客户端安装程序链接可启动安装。

安装客户端前：

- 检查客户端[安装需求](#)。
- 确定网络上的哪些计算机当前尚不具有抵御安全风险的防护。执行以下任务：
 - 运行趋势科技漏洞扫描程序。此工具根据您指定的 IP 地址范围分析计算机，查找已安装的防病毒软件。有关详细信息，请参阅第 3-28 页的[使用漏洞扫描程序](#)。
 - 查询 Active Directory。有关详细信息，请参阅第 2-20 页的[安全合规](#)。

启动基于浏览器的安装：

导航路径：联网计算机 > 客户端安装 > 基于浏览器

1. 如果需要则修改电子邮件的主题行。
2. 单击**创建电子邮件**。将打开缺省邮件程序。
3. 向预期的收件人发送电子邮件。

使用“登录脚本安装”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端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 将客户端安装到不受保护的计算机并更新程序文件和组件。计算机必须属于域，才能通过登录脚本使用 AutoPcc。

客户端安装

当不受保护的 Windows 2000/Server 2003 计算机登录到被您修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端安装到该计算机上。但是，AutoPcc.exe 不会自动将客户端安装到 Windows XP/Vista/2008 计算机上。用户需要连接到服务器计算机，导航到 \\<服务器计算机名称>\ofcscan，右键单击 **AutoPcc.exe**，然后选择**以管理员身份运行**。

对于使用 AutoPcc.exe 的远程桌面安装：

- 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”文件夹，然后从该点执行 AutoPcc.exe。

程序和组件更新

AutoPcc.exe 更新程序文件以及防病毒、防间谍软件和损害清除服务组件。

Windows 2000/Server 2003/2008 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：

- <Server_name> 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”是安装防毒墙网络版客户端的 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 Server: \\Windows 2000 server\system drive\WINNT\SYSTEM32\domain\scripts\ofcscan.bat
- Windows Server 2003: \\Windows 2003 server\system drive\windir\sysvol\domain\scripts\ofcscan.bat
- Windows Server 2008: \\Windows 2008 server\system drive\windir\sysvol\domain\scripts\ofcscan.bat

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 <服务器名称> > 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**。确保该服务器是主要域控制器，并确保您具有对该服务器的管理员访问权限。“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。

4. 要修改用户配置文件的登录脚本，请从“用户”列表中选择用户配置文件，然后单击**添加**。
5. 要修改所有用户的登录脚本，请单击**全部添加**。
6. 要排除先前选择的用户配置文件，请从**选定的用户**列表中选择该名称，然后单击**删除**。
7. 要重置选择，请单击**全部删除**。
8. 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。

9. 单击**确定**。“登录脚本安装”将返回到其初始窗口。
10. 要修改其他服务器的登录脚本，请重复步骤 2 到 4。
11. 要关闭“登录脚本安装”，请单击**退出**。

使用客户端打包程序安装

客户端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上运行安装程序。

当向低带宽远程办公室中的客户端上部署客户端程序或组件时，客户端打包程序作用突出。使用客户端打包程序安装的防毒墙网络版客户端，将向服务器报告创建安装程序软件包的位置。

客户端打包程序的需求如下：

- 350MB 可用磁盘空间
- Windows Installer 2.0 （运行 MSI 软件包）

使用客户端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 <[服务器安装文件夹](#)>\PCCSRV\Admin\Utility\ClientPackager。
2. 双击 **ClnPack.exe** 运行该工具。客户端打包程序控制台将打开。
3. 选择要创建的软件包类型。

表 3-8. 客户端软件包类型

软件包类型	描述
安装	选择 安装 可将软件包创建为可执行文件。软件包安装防毒墙网络版客户端程序以及服务器上当前可用的组件。如果目标计算机已安装早期版本的防毒墙网络版客户端，运行可执行文件将升级客户端。
更新	选择 更新 可创建一个包含服务器上当前可用组件的软件包。软件包将创建为可执行文件。如果在客户端计算机上更新组件时存在问题，请使用此软件包。
MSI	选择 MSI 可创建一个符合 Microsoft Installer 软件包格式的软件包。软件包还安装防毒墙网络版客户端程序以及服务器上当前可用的组件。如果目标计算机已安装早期版本的防毒墙网络版客户端，运行 MSI 文件将升级客户端。

4. 配置以下设置（一些设置仅在选择特定软件包类型时才可用）：
 - **Windows 操作系统类型**
 - **扫描方法**
 - **静默方式**
 - **更新代理**
 - **强制用最新版本覆盖**
 - **禁用预扫描（仅用于全新安装）**
 - **Outlook 邮件扫描**
 - **Check Point SecureClient 支持**
 - **组件**
5. 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，此文件在防毒墙网络版服务器的 <**服务器安装文件夹**>\PCCSRV 文件夹中。
6. 在**输出文件**里，单击  指定要创建的客户端软件包的位置和文件名（例如， ClientSetup.exe）。
7. 单击**创建**。客户端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。
8. 部署软件包。

软件包部署准则：

1. 将软件包发送给用户，请他们在计算机上通过双击 .exe 或 .msi 文件运行客户端软件包。

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

2. 如果您的用户将在运行 Windows Vista 和 2008 的计算机上安装 .exe 软件包，请指示他们右键单击 .exe 文件，然后选择**以管理员身份运行**。

3. 如果已创建 .msi 文件，请通过执行以下任务部署软件包：
 - 使用 Active Directory 或 Microsoft SMS。请参阅第 3-22 页的 [使用 Active Directory 部署 MSI 软件包](#) 或第 3-23 页的 [使用 Microsoft SMS 部署 MSI 软件包](#)。
 - 启动 MSI 软件包（在命令提示符上），将防毒墙网络版客户端静默安装到运行 Windows XP、Vista 和 2008 的远程计算机。

客户端打包程序设置

Windows 操作系统类型

选择要为其创建软件包的操作系统。确保仅将软件包部署到运行该操作系统类型的计算机。创建另一个软件包以部署到其他操作系统类型。

扫描方法

选择软件包的扫描方法。有关详细信息，请参阅第 5-8 页的 [扫描方法](#)。

软件包中包括的组件取决于所选的扫描方法。有关详细信息，请参阅第 4-21 页的 [客户端更新](#)。

在选择扫描方法之前，请注意以下准则以帮助您高效部署软件包：

- 如果将使用软件包将客户端升级到此版本的防毒墙网络版，请在 Web 控制台上检查域级扫描方法。在控制台上，转至**联网计算机 > 客户端管理**，选择客户端所属的客户端树域，然后单击**设置 > 扫描方法**。域级扫描方法应与软件包的扫描方法一致。
- 如果将使用软件包执行防毒墙网络版客户端的全新安装，请检查客户端分组设置。在 Web 控制台上，转至**联网计算机 > 全局客户端设置**。验证目标计算机所属的 NetBIOS/Active Directory/DNS 域是否存在于客户端树上。如果该域存在，请检查为该域配置的扫描方法。如果该域不存在，请检查根级扫描方法（选择客户端树上的根图标 ，然后单击**设置 > 扫描方法**）。域级或根级扫描方法应该与软件包的扫描方法一致。
- 如果将使用软件包在使用此版本的防毒墙网络版的客户端上更新组件，请检查为客户端所属的客户端树域配置的扫描方法。域级扫描方法应该与软件包的扫描方法一致。

静默方式

此选项创建在客户端计算机后台安装的软件包，客户端注意不到，也不显示安装状态窗口。如果打算将软件包远程部署到目标计算机，请启用此选项。

更新代理

此选项将“更新代理”权限分配给目标计算机上的客户端。更新代理可帮助防毒墙网络版服务器将组件部署到客户端。有关详细信息，请参阅第 4-34 页的[更新代理](#)。

如果启用更新代理选项：

1. 使用预设更新配置工具启用和配置对代理的预设更新。有关详细信息，请参阅第 4-38 页的[更新代理的更新方法](#)。
2. 管理更新代理的防毒墙网络版服务器将无法同步或者将以下设置部署到代理：
 - 更新代理权限
 - 客户端预设更新
 - 从趋势科技 ActiveUpdate 服务器更新
 - 从其他更新源更新

因此，仅将客户端软件包部署到不受防毒墙网络版服务器管理的计算机。此后，将更新代理配置为从防毒墙网络版服务器之外的更新源（如定制更新源）获取其更新。如果希望防毒墙网络版服务器将设置与更新代理同步，请不要使用客户端打包程序，而应改为选择其他客户端安装方法。

强制用最新版本覆盖

此选项用服务器上当前可用的版本覆盖客户端上的组件版本。启用此选项可确保服务器和客户端上的组件保持同步。

禁用预扫描（仅用于全新安装）

如果目标计算机未安装防毒墙网络版客户端，则软件包在安装客户端之前先扫描计算机以查找安全风险。如果您确信目标计算机没有感染安全风险，请禁用预扫描。

如果启用预扫描，则安装程序将扫描计算机的最易受攻击区域以查找病毒/恶意软件，最易受攻击区域包括：

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

Outlook 邮件扫描

此选项安装 Outlook 邮件扫描程序，该程序扫描 Microsoft Outlook™ 邮箱以查找安全风险。有关详细信息，请参阅第 9-13 页的 [Outlook 邮件扫描](#)。

Check Point SecureClient 支持

此工具添加了对 Check Point™ SecureClient™ for Windows 2000/XP/Server 2003 的支持。SecureClient 在允许连接到网络之前会验证病毒码版本。有关详细信息，请参阅第 11-2 页的 [Check Point 体系结构和配置概述](#)。

注意： 在使用[云安全扫描](#)的客户端上，SecureClient 不验证病毒码版本。

组件

选择要在软件包中包含的组件。有关详细信息，请参阅第 4-2 页的[防毒墙网络版组件与程序](#)。

使用 Active Directory 部署 MSI 软件包

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，请参阅第 3-17 页的[使用客户端打包程序安装](#)。

使用 Active Directory 部署 MSI 软件包：

1. 打开 Active Directory 控制台。
2. 右键单击您要部署 MSI 软件包的组织单元 (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**程序包**。
6. 查找并选择 MSI 软件包。
7. 选择部署方法，然后单击**确定**。
 - **已指派：**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。
 - **已发布：**要运行 MSI 软件包，通知用户转到“控制面板”，打开“添加/删除程序”窗口，然后选择在网络上添加/删除程序的选项。显示防毒墙网络版客户端 MSI 软件包时，用户可继续安装客户端。

使用 Microsoft SMS 部署 MSI 软件包

如果服务器上安装了 Microsoft BackOffice SMS，请使用 Microsoft System Management Server (SMS) 部署 MSI 软件包。有关创建 MSI 文件的指导信息，请参阅第 3-17 页的[使用客户端打包程序安装](#)。

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。

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，请参阅第 3-44 页的[安装后](#)。

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

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. 浏览并选择由客户端打包程序创建的 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端”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，使用客户端打包程序创建具有 .exe 扩展名的“安装”软件包（不可创建 .msi 软件包）。有关详细信息，请参阅第 3-17 页的[*使用客户端打包程序安装*](#)。
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**公布此客户端“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。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端“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。

18. 当 Microsoft SMS 分发此公布程序（即防毒墙网络版客户端程序）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端安装到他们的计算机上。

从防毒墙网络版 Web 控制台安装

将防毒墙网络版客户端远程安装到已经连接到网络中的一台或多台计算机上。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端。

注意： 此安装方法不能在运行 Windows XP Home 以及 Windows Vista Home Basic 或 Home Premium 版（32 位和 64 位版本）的计算机上使用。

从防毒墙网络版 Web 控制台安装：

1. 如果计算机不是运行 Windows Vista，请跳过这一步。如果运行 Windows Vista Business、Enterprise 或 Ultimate 版，请执行以下步骤：
 - a. 启用内置管理员帐户并为该帐户设置密码。
 - b. 单击**开始 > 所有程序 > 管理工具 > 高级安全 Windows 防火墙**。
 - c. 针对域概要文件、专用概要文件和通用概要文件，将防火墙状态设置为“关闭”。
 - d. 打开 Microsoft 管理控制台（单击**开始 > 运行**，键入 **services.msc**），然后启动 **Remote Registry** 服务。安装防毒墙网络版客户端时，请使用内置管理员帐户和密码。
2. 在 Web 控制台，单击**联网的计算机 > 客户端安装 > 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，在页面上方的文本框里输入计算机名称，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。使用管理员帐户用户名和密码才能继续。
4. 键入用户名和密码，然后单击**登录**。目标计算机显示在**选定的计算机**表中。
5. 重复步骤 3 和步骤 4，添加多个计算机。
6. 准备好在目标计算机上安装客户端时，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端。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，该计算机名称将显示在**选定的计算机**列表的**域和计算机**列表中，并带绿色复选标记。

当所有目标计算机带着绿色复选标记显示在**选定的计算机**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。

从客户端磁盘镜像安装

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端的镜像并将其复制到网络中的其他计算机。

每个客户端安装都需要一个全局唯一标识号 (GUID)，这样服务器就可以分别识别客户端。使用名为 `imgsetup.exe` 的防毒墙网络版程序来为每个副本创建不同的 GUID。

注意： 此安装方法不能在运行 Windows Vista 和 2008 的计算机上使用。

创建防毒墙网络版客户端的磁盘镜像：

1. 在计算机上安装防毒墙网络版客户端。
2. 将 `ImgSetup.exe` 从 **<服务器安装文件夹>**\PCCSRV\Admin\Utility\ImgSetup 文件夹复制到此计算机。
3. 在此计算机上运行 `ImgSetup.exe`。将在 `HKEY_LOCAL_MACHINE` 下创建一个 `RUN` 注册码。
4. 使用磁盘镜像软件创建防毒墙网络版客户端的磁盘镜像。
5. 重新启动复制。`ImgSetup.exe` 将自动启动并创建一个新的 GUID 值。客户端会将此新的 GUID 报告给服务器，而服务器将为该客户端创建一个新的记录。

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，请手动更改被复制的防毒墙网络版客户端的计算机名称或域名。

使用漏洞扫描程序

使用漏洞扫描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，以及将防毒墙网络版客户端安装到计算机。为确定计算机是否受到保护，漏洞扫描程序会 ping 防病毒解决方案通常使用的端口。

漏洞扫描程序的功能

漏洞扫描程序执行以下功能：

- 监控网络上的动态主机配置协议 (DHCP) 请求，以便当计算机首次登录到网络时，漏洞扫描程序可以确定其状态。
- Ping 网络上的计算机以检查其状态并检索其计算机名称、平台版本及描述。
- 确定网络上安装的防病毒解决方案。漏洞扫描程序可以检测趋势科技™ 产品和第三方防病毒解决方案（包括 Norton AntiVirus™ Corporate Edition 和 McAfee™ VirusScan™ ePolicy Orchestrator™）。
- 通过电子邮件发送扫描结果或将结果导出为逗号分隔值 (CSV) 文件。

使用漏洞扫描程序时的注意事项

为帮助您决定是否使用漏洞扫描程序，请考虑以下因素：

网络管理

表 3-9. 网络管理

安装	漏洞扫描程序的效力
具有严格安全策略的管理	非常高效。漏洞扫描程序会报告是否所有计算机已安装防病毒软件。
分布在不同地点的管理职责	效率中等
集中式管理	效率中等
外包服务	效率中等
用户管理自己的计算机	效率不高。由于漏洞扫描程序会扫描网络的防病毒安装程序，因此让用户扫描自己的计算机并不可行。

网络拓扑和体系结构

表 3-10. 网络拓扑和体系结构

安装	漏洞扫描程序的效力
单个位置	非常高效。通过漏洞扫描程序可以扫描整个 IP 段，还可以轻松地 LAN 上安装防毒墙网络版客户端。
具有高速连接的多个位置	效率中等
具有低速连接的多个位置	效率不高。需要在各个位置上运行漏洞扫描程序并且防毒墙网络版客户端安装程序必须指向本地防毒墙网络版服务器。
远程计算机和隔离的计算机	效率不高。漏洞扫描程序无法扫描未连接到网络的计算机。

软件/硬件规格

表 3-11. 软件/硬件规格

安装	漏洞扫描程序的效力
基于 Windows NT 的操作系统	非常高效。漏洞扫描程序可以轻松地将防毒墙网络版客户端远程安装到运行基于 NT 操作系统（Windows XP Home 除外）的计算机。
混合操作系统	效率中等。漏洞扫描程序仅能将防毒墙网络版客户端安装到运行基于 Windows NT 操作系统的计算机。
桌面管理软件	效率不高。漏洞扫描程序不能和桌面管理软件一起使用。但是，它可以帮助跟踪防毒墙网络版客户端安装的进度。

域结构

表 3-12. 域结构

安装	漏洞扫描程序的效力
Microsoft Active Directory	非常高效。在漏洞扫描程序中指定域管理员帐户以允许防毒墙网络版客户端的远程安装。
工作组	效率不高。漏洞扫描程序使用不同管理帐户和密码将防毒墙网络版客户端安装到这些计算机时，可能会有困难。
Novell™ 目录服务	效率不高。漏洞扫描程序需要 Windows 域帐户来安装防毒墙网络版客户端。
对等	效率不高。漏洞扫描程序使用不同管理帐户和密码将防毒墙网络版客户端安装到这些计算机时，可能会有困难。

网络通信

表 3-13. 网络通信

安装	漏洞扫描程序的效力
LAN 连接	非常高效
512 Kbps	效率中等
T1 连接或更高	效率中等
拨号	效率不高。要花很长时间才可以完成安装防毒墙网络版客户端。

网络规模

表 3-14. 网络规模

安装	漏洞扫描程序的效力
超大型企业	非常高效。网络规模越大，越需要漏洞扫描程序来检查防毒墙网络版客户端安装。
中小企业	效率中等。对于小型网络，漏洞扫描程序可以是安装防毒墙网络版客户端的一个选项。其他客户端安装方法更加容易执行。

用户任务

从漏洞扫描程序执行以下任务：

- 第 3-32 页的 [安装防毒墙网络版客户端](#)
- 第 3-33 页的 [管理常规设置](#)
- 第 3-36 页的 [运行漏洞扫描](#)
- 第 3-38 页的 [创建预设任务](#)
- 第 3-39 页的 [配置其他漏洞扫描程序设置](#)

在另一台计算机上启动漏洞扫描程序

可以在防毒墙网络版服务器计算机之外的其他计算机上启动漏洞扫描程序。确保其他计算机运行 Windows 2000、2003 和 2008。无法在 Windows XP、Vista 上或者从终端服务器启动该工具。

在另一台计算机上启动漏洞扫描程序：

1. 连接到防毒墙网络版服务器计算机。
2. 将 <[服务器安装文件夹](#)>\PCCSRV\Admin\Utility 中的 **TMVS** 文件夹复制到其他计算机。
3. 复制 **TMVS** 文件夹后，双击 **TMVS.exe**。

安装防毒墙网络版客户端

漏洞扫描程序可以将防毒墙网络版客户端安装到远程计算机。但是，如果存在以下情况，则漏洞扫描程序将不安装客户端：

- 远程计算机已安装防毒墙网络版服务器或其他防病毒产品。
- 远程计算机运行 Windows XP Home、Windows Vista Home Basic 和 Windows Vista Home Premium。

要使用漏洞扫描程序安装防毒墙网络版客户端：

1. 如果运行 Windows Vista Business、Enterprise 或 Ultimate 版，请执行以下步骤：
 - a. 启用内置管理员帐户并为该帐户设置密码。
 - b. 单击**开始 > 所有程序 > 管理工具 > 高级安全 Windows 防火墙**。
 - c. 针对域概要文件、专用概要文件和通用概要文件，将防火墙状态设置为“关闭”。
 - d. 打开 Microsoft 管理控制台（单击**开始 > 运行**，键入 **services.msc**），然后启动 **Remote Registry** 服务。安装防毒墙网络版客户端时，请使用内置管理员帐户和密码。
2. 如果运行 Windows XP Professional（32 位或 64 位版本），请执行以下步骤：
 - a. 打开 Windows 资源管理器，然后单击**工具 > 文件夹选项**。
 - b. 单击**查看**选项卡并禁用**使用简单文件共享（推荐）**。
3. 导航到 TMVS 文件夹并双击 **TMVS.exe**。将显示趋势科技漏洞扫描程序控制台。

注意： 在防毒墙网络版服务器计算机上，TMVS 文件夹位于 **<服务器安装文件夹>\PCCSRV\Admin\Utility** 中。如果已将 TMVS 文件夹复制到另一台计算机，请导航到该计算机上的 TMVS 文件夹。

4. 单击**设置**。
5. 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称和端口号。
6. 选择为不受保护的计算机自动安装防毒墙网络版客户端。

7. 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端的安装。

管理常规设置

要配置和管理以下漏洞扫描程序设置，请导航到 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\TMVS，然后双击 **TMVS.exe**：

产品查询

选择要在网络上检查的产品。要防止误报，请选中所有复选框。单击产品名称旁的**设置**来验证漏洞扫描程序要检查的端口号。

手动配置每个产品（防毒墙服务器版 for Windows 和 Linux™ 以及 McAfee™ VirusScan™ ePolicy Orchestrator™ 除外）的端口设置。

漏洞扫描程序检查安全产品的方法：

表 3-15. 漏洞扫描程序检查的安全产品

产品	描述
防毒墙网络版客户端	漏洞扫描程序使用防毒墙网络版客户端的端口来检查是否安装了防毒墙网络版客户端。还检查 TMListen.exe 进程是否正在运行。如果从其缺省位置执行，则自动检索端口号。 如果已在防毒墙网络版服务器之外的其他计算机上启动了 TMVS，请检查其他计算机的通信端口，然后使用该端口。
趋势科技网络安全专家 (PC-cillin)	漏洞扫描程序使用端口 40116 检查是否安装了趋势科技网络安全专家。
防毒墙服务器版 for Windows	漏洞扫描程序使用 RPC 端点来检查 SPNTSVC.exe 是否正在运行。它返回包括操作系统及病毒扫描引擎、病毒码和产品版本在内的信息。漏洞扫描程序无法检测防毒墙服务器版信息服务器或防毒墙服务器版管理控制台。
防毒墙服务器版 for Linux	如果目标计算机没有运行 Windows，则漏洞扫描程序通过尝试连接到端口 14942 来检查其是否安装了防毒墙服务器版 for Linux。

表 3-15. 漏洞扫描程序检查的安全产品（续）

产品	描述
防毒墙群件版 for Microsoft Exchange™	漏洞扫描程序会加载网页 http://ipaddress:port/scanmail.html 来检查 Scanmail 的安装。缺省情况下，ScanMail 使用端口 16372。如果 ScanMail 使用不同端口号，则指定端口号。否则，漏洞扫描程序无法检测到防毒墙群件版 for Microsoft Exchange。
InterScan™ 系列	对于不同的产品，漏洞扫描程序各自的网页检查产品安装。 • 趋势科技防毒墙邮件安全版 5.x: http://localhost:port/eManager/cgi-bin/eManager.htm • InterScan eManager 3.x: http://localhost:port/eManager/cgi-bin/eManager.htm • InterScan VirusWall™ 3.x: http://localhost:port/InterScan/cgi-bin/interscan.dll
PortalProtect™	漏洞扫描程序加载 Web 页 http://localhost:port/PortalProtect/index.html 来检查产品安装。
Norton Antivirus™ Corporate Edition	漏洞扫描程序向 UDP 端口 2967（Norton Antivirus 企业版 RTVScan 的缺省端口）发送一个特殊令牌。安装有该防病毒产品的计算机使用特殊令牌类型响应。由于 Norton Antivirus 企业版通过 UDP 通信，因此不保证精确率。另外，网络通信可能会影响 UDP 等待时间。
McAfee VirusScan ePolicy Orchestrator	漏洞扫描程序向 TCP 端口 8081（提供服务器和客户端之间连接的 ePolicy Orchestrator 缺省端口）发送一个特殊令牌。安装有该防病毒产品的计算机使用特殊令牌类型响应。漏洞扫描程序无法检测到独立的 McAfee VirusScan。

协议

漏洞扫描程序使用以下协议检测产品和计算机：

- **RPC**：检测防毒墙服务器版 for NT
- **UDP**：检测 Norton AntiVirus 企业版客户端
- **TCP**：检测 McAfee VirusScan ePolicy Orchestrator
- **ICMP**：通过发送 ICMP 数据包检测计算机
- **HTTP**：检测防毒墙网络版客户端
- **DHCP**：如果它检测到一个 DHCP 请求，则漏洞扫描程序检查请求计算机上是否已安装了防病毒软件

检索计算机描述的方法

快速检索仅检索计算机名称。由于标准检索既检索域信息又检索计算机信息，因此花费较长时间来完成。如果选择标准检索，则设置漏洞扫描程序尝试检索计算机描述（如果可用）。

通知

要使结果自动发送给您自己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。

1. 在**收件人**中，键入收件人的电子邮件地址。
2. 在**发件人**中，键入电子邮件地址以让收件人知道谁发送了邮件。
3. 在**SMTP 服务器**中，键入 SMTP 服务器地址。例如，键入 smtp.company.com。SMTP 服务器信息是必需的。
4. 在**主题**中，键入邮件的新主题或接受缺省主题。
5. 单击**确定**。
6. 选择在不受保护的计算机上显示通知。单击**定制**来配置通知消息。在“通知消息”窗口中，键入新消息或接受缺省消息。单击**确定**。

漏洞扫描结果

将扫描结果保存到一个逗号分隔值 (CSV) 文件。要更改保存 CSV 文件的缺省文件夹，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**。

Ping 设置

启用漏洞扫描程序 ping 网络上的计算机以获取其状态。要指定漏洞扫描程序向计算机发送数据包以及等待响应的方式，请选择**允许漏洞扫描程序对网络上的计算机执行 ping 操作以检查其状态**，然后接受缺省设置或在**数据包大小和超时**文本框中键入新的值。

漏洞扫描程序还可以使用 ICMP OS 指纹验证来检测操作系统的类型。

防毒墙网络版服务器设置

键入防毒墙网络版服务器的名称和端口号。漏洞扫描程序可以将防毒墙网络版客户端自动安装到不受保护的计算机上。

单击**安装到帐户**来配置帐户。在“帐户信息”窗口中，键入允许安装的用户名和密码。单击**确定**。

漏洞扫描程序还可以将日志发送到防毒墙网络版服务器。

运行漏洞扫描

通过指定 IP 地址范围，可在多台计算机上运行漏洞扫描。

漏洞扫描还可以在从 DHCP 服务器请求 IP 地址的计算机上运行。漏洞扫描程序侦听端口 67（DHCP 服务器侦听 DHCP 请求的端口）。如果它检测到一个 DHCP 请求，则漏洞扫描程序检查请求计算机上是否存在防病毒软件。

在 IP 地址范围内手动运行漏洞扫描：

1. 导航到 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\TMVS，然后双击 **TMVS.exe**。将显示趋势科技漏洞扫描程序控制台。
2. 在**手动扫描**下，键入要检查的计算机的 IP 地址范围。

注意： 漏洞扫描程序仅支持 B 类 IP 地址范围，例如， 168.212.1.1 到 168.212.254.254。

3. 单击**开始**。漏洞扫描结果将显示在**手动扫描**选项卡下的**结果表**中。

注意： 如果计算机运行 Windows 2008，则在**结果表**中不显示 MAC 地址信息。

4. 要将结果保存为逗号分隔值 (CSV) 文件，请单击**导出**，找到要保存该文件的文件夹，键入文件名称，然后单击**保存**。

在从 DHCP 服务器请求 IP 地址的计算机上运行漏洞扫描：

1. 在以下文件夹下找到的 **TMVS.ini** 文件中配置 DHCP 设置：<**服务器安装文件夹**>\PCCSRV\Admin\Utility\TMVS。

表 3-16. TMVS.ini 文件中的 DHCP 设置

设置	描述
DhcpThreadNum=x	指定 DHCP 模式的线程数。最小值为 3，最大值为 100。缺省值为 3。
DhcpDelayScan=x	这是检查请求计算机已安装防病毒软件前的延迟时间。最小值为 0（不等待），最大值为 600。缺省值为 60。
LogReport=x	0 表示禁用日志记录，1 表示启用日志记录。 漏洞扫描程序将扫描结果发送到防毒墙网络版服务器并且日志显示在 Web 控制台的“系统时间日志”窗口中。
OsceServer=x	这是防毒墙网络版服务器的 IP 地址或 DNS 名称。
OsceServerPort=x	这是防毒墙网络版服务器上 Web 服务器的端口。

2. 导航到 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\TMVS，然后双击 **TMVS.exe**。将显示趋势科技漏洞扫描程序控制台。
3. 在**结果表**中，单击 **DHCP 扫描**选项卡。

注意： **DHCP 扫描**选项卡在运行 Windows 2008 的计算机上不可用。

4. 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。当检测到未受保护的计算机并验证该计算机的 IP 地址属于定义的 IP 地址范围时，漏洞扫描程序运行远程安装程序来安装防毒墙网络版客户端。
5. 要将结果保存为逗号分隔值 (CSV) 文件，请单击**导出**，找到要保存该文件的文件夹，键入文件名称，然后单击**保存**。

创建预设任务

通过在漏洞扫描程序中预设任务，可以定期检查网络中已安装的防病毒解决方案。这是一种自动运行任务的便利方法，无需每次都配置漏洞扫描程序。

创建预设任务：

1. 导航到 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\TMVS，然后双击 **TMVS.exe**。将显示趋势科技漏洞扫描程序控制台。
2. 在**结果表**中，单击 **DHCP 扫描**选项卡。

注意： **DHCP 扫描**选项卡在运行 Windows 2008 的计算机上不可用。

3. 在**预设扫描**下，单击**添加/编辑**。将显示“预设扫描”窗口。配置以下信息：
 - **名称：**键入预设扫描的名称。
 - **IP 地址范围：**键入要检查的计算机的 IP 地址范围。
 - **开始时间：**键入或选择扫描将要运行的时间。使用 24 小时制格式。
 - **频率：**选择扫描将运行的频率。从每天一次、每周一次或每月一次中进行选择。
 - **设置：**单击**使用当前设置**使用现有设置，或者单击**修改设置**。如果单击**修改设置**，则单击**设置**来更改配置。
4. 单击**确定**。您创建的预设扫描将显示在**预设扫描**下。
5. 要立即执行预设扫描，请单击**立即运行**。

配置其他漏洞扫描程序设置

一些漏洞扫描程序设置只能从 **TMVS.ini** 文件进行配置。

在 **TMVS.ini** 文件中修改设置：

1. 导航到 <[服务器安装文件夹](#)>\PCCSRV\Admin\Utility\TMVS，然后使用文本编辑器（如记事本）打开 **TMVS.ini**。

2. 要设置漏洞扫描程序要同时 ping 的计算机数量，请更改 EchoNum 的值。请指定一个 1 到 64 之间的值。

例如，如果要让漏洞扫描程序在同一时间 ping 60 台计算机，则键入 EchoNum=60。

3. 要设置漏洞扫描程序要同时检查防病毒软件的计算机数量，请更改 ThreadNumManual 的值。请指定一个 8 到 64 之间的值。

例如，如果要让漏洞扫描程序在同一时间检查 60 台计算机的防病毒软件，请键入 ThreadNumManual=60。

4. 要设置在运行预设任务时，漏洞扫描程序要同时检查防病毒软件的计算机数量，请更改 ThreadNumSchedule 的值。请指定一个 8 到 64 之间的值。

例如，如果要让漏洞扫描程序运行预设任务时在同一时间检查 60 台计算机的防病毒软件，则键入 ThreadNumSchedule=60。

5. 保存 **TMVS.ini**。

注意： 有关如何收集漏洞扫描程序的调试日志的信息，请参阅第 12-3 页的[服务器使用 LogServer.exe 调试日志](#)。

迁移到防毒墙网络版客户端

将在目标计算机上安装的端点安全软件迁移到防毒墙网络版客户端。

从其他端点安全软件迁移

安装防毒墙网络版客户端时，安装程序将检查在目标计算机上安装的任何趋势科技或第三方端点安全软件。安装程序可以自动卸载该软件，并将它替换为防毒墙网络版客户端。

有关防毒墙网络版自动卸载的端点安全软件的列表，请打开 <[服务器安装文件夹](#)>\PCCSRV\Admin 中的以下文件。使用文本编辑器（如记事本）打开这些文件。

- tmuninst.ptn
- tmuninst_as.ptn

如果目标计算机上的软件不包括在列表中，请首先手动卸载它。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。

客户端迁移问题

- 如果自动客户端迁移成功，但是用户安装防毒墙网络版客户端后使用时遇到问题，请重新启动计算机。
- 如果防毒墙网络版安装程序继续安装防毒墙网络版客户端，但是无法卸载其他安全软件，则这两个软件之间将存在冲突。卸载两个软件，然后使用第 3-10 页的 [安装方法](#) 中介绍的任何一种方法安装防毒墙网络版客户端。

从 ServerProtect 标准服务器迁移

ServerProtect™ 标准服务器迁移工具是一种可帮助您将运行趋势科技 ServerProtect 标准服务器的计算机迁移到防毒墙网络版客户端的工具。

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、2003 和 2008 计算机上运行该工具。

成功卸载 ServerProtect 标准服务器后，该工具安装防毒墙网络版客户端。它还将扫描例外列表设置（用于所有扫描类型）迁移到防毒墙网络版客户端。

安装防毒墙网络版客户端时，迁移工具客户端安装程序有时也许会超时，并通知您安装未成功。但是，可能已成功安装客户端。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。

迁移在以下情况下是不成功的：

- 如果远程客户端无法使用 NetBIOS 协议
- 如果端口 455、337 和 339 被封闭
- 如果远程客户端无法使用 RPC 协议
- 如果 Remote Registry 服务停止

注意： ServerProtect 标准服务器迁移工具不会卸载控管中心™ 代理（防毒墙服务器版）。有关如何卸载该代理的说明，请参考防毒墙服务器版和/或控制管理中心文档。

使用 ServerProtect 标准服务器迁移工具：

1. 在防毒墙网络版服务器计算机上，打开 <服务器安装文件夹>\PCCSRV\Admin\Utility\SPNSXfr，然后将文件 SPNSXfr.exe 和 SPNSXfr.ini 复制到 <服务器安装文件夹>\PCCSRV\Admin。
2. 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。

3. 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**选择**，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时再次自动查找防毒墙网络版服务器，请选中**自动查找服务器路径**复选框（缺省选中）。
4. 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**选择目标计算机**下单击以下选项之一：
 - **Windows 网络树**：显示网络中的域树。要使用这种方法选择计算机，请单击要从中搜索客户端计算机的域。
 - **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插入半角分号“;”。
 - **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 服务器在搜索客户端时没有响应，则搜索将停止响应。等待搜索超时。

5. 选择将运行 Windows Server 2003 的计算机加入搜索。
6. 选择重新启动运行 Windows Server 2003 的计算机。要使迁移在这些计算机上成功完成，必须重新启动计算机。选中此复选框以确保其自动重新启动。如果不选中**安装后重新启动**复选框，请在迁移后手动重新启动计算机。
7. 单击**搜索**。搜索结果将显示在“ServerProtect 标准服务器”下面。
8. 单击要执行迁移的计算机。
 - a. 要选择所有计算机，请单击**全选**。
 - b. 要取消选择所有计算机，请单击**取消全选**。
 - c. 要将列表导出到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。

9. 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. 选中**使用组帐户/密码**复选框。
- b. 单击**设置登录帐户**。将显示**输入管理员信息**窗口。
- c. 键入用户名和密码。

注意： 使用本地/域管理员帐户登录到目标计算机。如果使用权限不足的帐户（例如“Guest”或“标准用户”）登录，将无法执行安装。

- 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。

10. 单击**迁移**。

11. 如果计算机运行 Windows Server 2003，重新启动计算机后才能完成迁移。

安装后

完成安装后，验证以下内容：

防毒墙网络版客户端快捷方式

客户端计算机的 Windows 开始菜单中将出现趋势科技防毒墙网络版客户端的快捷方式。

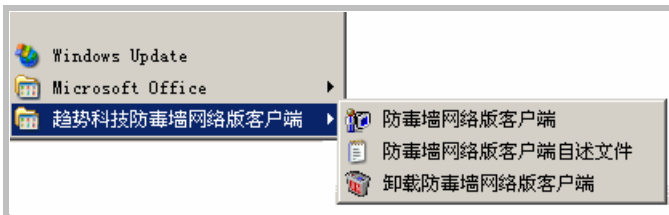


图 3-1. 防毒墙网络版客户端快捷方式

程序列表

趋势科技防毒墙网络版客户端在客户端计算机“控制面板”上的添加/删除程序列表上列出。

防毒墙网络版客户端服务

在 Microsoft 管理控制台上显示以下防毒墙网络版客户端服务：

- OfficeScan NT Listener
- OfficeScan NT Firewall （如果安装过程中启用了该防火墙）
- OfficeScan NT Proxy Service
- OfficeScanNT RealTime Scan
- Trend Micro Unauthorized Change Prevention Service （仅用于运行 x86 类型处理器的计算机）

客户端安装日志

客户端安装日志 OFCNT.LOG 存在于以下位置：

- %windir% （对于除 MSI 软件包安装之外的所有安装方法）
- %temp% （对于 MSI 软件包安装方法）

建议的安装后任务

趋势科技建议执行以下安装后任务：

组件更新

通知客户端更新其组件，以确保有抵御安全风险的最新防护。

有关详细信息，请参阅第 4-21 页的 [客户端更新](#)。

使用 EICAR 测试脚本测试扫描

欧洲计算机防病毒研究所 (European Institute for Computer Antivirus Research, EICAR) 开发了 EICAR 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防病毒产品。

执行测试扫描：

1. 启用客户端实时扫描。
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[4PZX54(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. 要检测网络上的其他计算机，请将 EICAR.com 文件附加到电子邮件中并发送到其中一台计算机。

提示： 趋势科技建议使用压缩软件（如 WinZip）对 EICAR 文件进行打包，然后执行其他测试扫描。

卸载客户端

有两种方法可从客户端卸载防毒墙网络版程序：

- 第 3-46 页的 [从 Web 控制台卸载客户端](#)
- 第 3-47 页的 [运行客户端卸载程序](#)

如果客户端还有 Cisco Trust Agent (CTA) 安装程序，则卸载防毒墙网络版客户端程序可能（或可能无法）删除代理。这取决于在部署代理时配置的设置。有关详细信息，请参阅第 10-28 页的 [部署 Cisco Trust Agent](#)。

如果在卸载防毒墙网络版客户端后 Cisco Trust Agent 仍存在，请从“添加/删除程序”窗口中手动删除它。

如果使用上述方法无法卸载客户端，请手动卸载客户端。有关详细信息，请参阅第 3-48 页的 [手动卸载客户端](#)。

从 Web 控制台卸载客户端

从 Web 控制台卸载客户端程序。仅当遇到程序问题时才执行卸载，然后立即重新安装它，以保护计算机免受安全风险的危害。

从 Web 控制台卸载客户端：

1. 单击防毒墙网络版 Web 控制台主菜单的 **联网的计算机 > 客户端管理**。将显示客户端树。
2. 在客户端树中，选择要卸载的客户端。
3. 单击 **任务 > 客户端卸载**。
4. 单击“客户端卸载”窗口中的 **启动卸载**。服务器将发送通知给该客户端。

5. 检查通知状态并验证是否有未收到通知的客户端。
 - 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端。
 - 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端。已经被通知并且已经执行卸载的客户端暂不处理此命令。

运行客户端卸载程序

如果授予用户卸载客户端程序的权限，指导他们从自己的计算机运行客户端卸载程序。

此过程要求用户指定卸载密码。确保仅与将运行卸载程序的用户共享密码，如果密码泄漏给了其他用户，请立即修改它。也可以在将卸载客户端的计算机上禁用密码。有关详细信息，请参阅第 9-5 页的[客户端权限和其他设置](#)。

运行客户端卸载程序：

1. 在 Windows 开始菜单上单击**程序 > 趋势科技防毒墙网络版客户端 > 卸载防毒墙网络版客户端**。

还可以执行以下步骤：

 - a. 单击**控制面板 > 添加或删除程序**。
 - b. 找到**趋势科技防毒墙网络版客户端**，然后单击**更改**。
 - c. 按照窗口上的指导信息操作。
2. 在系统提示时，键入卸载密码。防毒墙网络版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。

手动卸载客户端

仅当从 Web 控制台卸载客户端或运行卸载程序后遇到问题时，才执行手动卸载。

执行手动卸载：

1. 使用具有管理员权限的帐户登录到客户端计算机。
2. 右键单击系统托盘中的防毒墙网络版客户端图标，然后选择**退出防毒墙网络版**。如果系统提示您输入密码，则指定退出密码，然后单击**确定**。

注意： 在将退出客户端的计算机上禁用密码。有关详细信息，请参阅第 9-5 页的 [客户端权限和其他设置](#)。

3. 如果未指定退出密码，则从 Microsoft 管理控制台停止以下服务：
 - OfficeScan NT Listener
 - OfficeScan NT Firewall
 - OfficeScanNT RealTime Scan
 - OfficeScan NT Proxy Service
 - Trend Micro Unauthorized Change Prevention Service （如果计算机运行 x86 类型平台）
4. 单击**开始 > 程序**，右键单击**趋势科技防毒墙网络版客户端**，然后单击**删除**。
5. 打开注册表编辑器 (Regedit.exe)。

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。

6. 删除以下注册码：

如果在计算机上未安装其他趋势科技产品：

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro

对于 64 位计算机：

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro

如果计算机上安装了其他趋势科技产品，则仅删除以下注册码：

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfcWatchDog

对于 64 位计算机：

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\
OfcWatchDog

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp

对于 64 位计算机：

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\
PC-cillinNTCorp

7. 删除以下注册码/值：

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Uninstall\OfficeScanNT
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Run 下的 OfficeScanNT 监控程序 (REG_SZ)

8. 删除以下位置中以下注册码的所有实例：

位置：

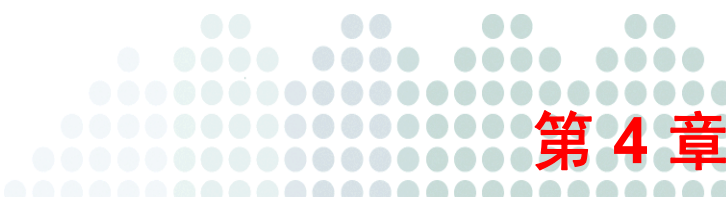
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services

键:

- nrtscan
- tncfw
- tmcomm
- TmFilter
- Tmlisten
- tmpfw
- TmPreFilter
- TmProxy
- tmtdi
- VSApiNt
- tmlwf (对于 Windows Vista/2008 计算机)
- tmwfp (对于 Windows Vista/2008 计算机)
- tmactmon
- TMBMServer
- tmevtmgr

9. 关闭注册表编辑器。
10. 单击**开始 > 设置 > 控制面板**，然后双击**系统**。
11. 单击**硬件选项卡**，然后单击**设备管理器**。
12. 单击**查看 > 显示隐藏的设备**。
13. 展开**非即插即用驱动程序**，然后卸载以下设备：
 - tmcomm
 - tmactmon
 - tmevtmgr
 - Trend Micro Filter
 - Trend Micro PreFilter
 - Trend Micro TDI Driver
 - Trend Micro VSAPI NT

- Trend Micro Unauthorized Change Prevention Service
 - Trend Micro WFP Callout Driver （对于 Windows Vista/2008 计算机）
14. 卸载通用防火墙驱动程序。
- a. 右键单击**网上邻居**，然后单击**属性**。
 - b. 右键单击**本地连接**，然后单击**属性**。
 - c. 在**常规**选项卡上，选择**趋势科技通用防火墙驱动程序**，然后单击**卸载**。
- 在 Windows Vista 计算机上，执行以下操作：
- a. 右键单击**网络**，然后单击**属性**。
 - b. 单击**管理网络连接**。
 - c. 右键单击**本地连接**，然后单击**属性**。
 - d. 在**网络**选项卡上，选择**趋势科技 NDIS 6.0 过滤器驱动程序**，然后单击**卸载**。
15. 重新启动客户端计算机。
16. 如果计算机上没有安装其他趋势科技产品，请删除 **Trend Micro** 安装文件夹（通常为 C:\Program Files\Trend Micro）。对于 64 位计算机，可在 C:\Program Files (x86)\Trend Micro 下找到安装文件夹。
17. 如果安装了其他趋势科技产品，则删除以下文件夹：
- <客户端安装文件夹>
 - Trend Micro 安装文件夹下的 **BM** 文件夹（通常为 C:\Program Files\Trend Micro\BM）



第 4 章

使防护保持最新

本章主题：

- 第 4-2 页的[防毒墙网络版组件与程序](#)
- 第 4-9 页的[更新概述](#)
- 第 4-11 页的[防毒墙网络版服务器更新](#)
- 第 4-19 页的[云安全服务器更新](#)
- 第 4-21 页的[客户端更新](#)
- 第 4-34 页的[更新代理](#)
- 第 4-39 页的[组件更新摘要](#)

防毒墙网络版组件与程序

防毒墙网络版利用组件和程序来保护客户端计算机免受最新安全风险的危害。通过运行手动或预设更新，使这些组件和程序保持最新。

除这些组件外，防毒墙网络版客户端还从防毒墙网络版服务器接收更新的配置文件。客户端需要这些配置文件应用新的设置。每次通过 Web 控制台修改防毒墙网络版设置时，配置文件也随之更改。

组件分为以下几组：

- **防病毒组件**
- **损害清除服务组件**
- **防间谍软件组件**
- **防火墙组件**
- **Web 信誉组件**
- **行为监控组件**
- **程序**

防病毒组件

病毒码

客户端计算机上的可用病毒码取决于客户端使用的扫描方法。有关扫描方法的信息，请参阅第 5-8 页的 [扫描方法](#)。

传统扫描

传统扫描期间使用的特征码称为**病毒码**，它包括帮助防毒墙网络版识别最新病毒/恶意软件和 **mixed threat attack（混合威胁攻击）** 的信息。趋势科技将每周创建和发布几次新版本的病毒码，并将在发现有特殊损害性的病毒/恶意软件后随时创建和发布新版本。

提示： 趋势科技建议预设至少每周自动更新一次，这是所有产品的缺省设置。

从以下 Web 站点下载病毒码和其他防毒墙网络版特征码文件，从中还可以找到当前版本、发布日期和包括在该文件中的所有新病毒定义列表：

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

云安全扫描

在云安全扫描模式中，防毒墙网络版客户端使用协同工作的两个轻量级特征码，这两个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。

云安全服务器托管**云安全云端病毒码**。此病毒码每小时更新一次，它包含多数病毒码定义。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。

客户端更新源（防毒墙网络版服务器或**定制的更新源**）托管**云安全客户端病毒码**。此特征码每天更新一次，它包含在云安全云端病毒码中未找到的所有其他特征码定义。客户端使用下载其他防毒墙网络版组件的相同方法，从更新源下载此特征码。

防毒墙网络版客户端使用云安全客户端病毒码和高级过滤技术，可以在不向云安全服务器发送扫描查询的情况下验证文件是否受到感染。客户端仅在扫描期间无法确定文件风险时才发送扫描查询。如果客户端无法在本地验证文件的风险，并且在多次尝试后，仍无法连接到任何云安全服务器：

- 将文件标记为要进行验证
- 暂时允许访问文件

当恢复与云安全服务器的连接后，会重新扫描所有的已标记文件。然后，对已经被确认为受感染的文件采取适当的扫描处理措施。

病毒扫描引擎

所有趋势科技产品的核心是扫描引擎，它最初是为了响应早期基于文件的计算机病毒而开发的。如今的扫描引擎非常完善，能够检测出各种类型的**病毒和恶意软件**。扫描引擎还可检测出以研究为目的而开发和使用的受控病毒。

扫描引擎不会扫描每个文件的每一字节，而是和特征码文件协作以识别以下项：

- 病毒代码的指示特征
- 文件中可能存在病毒的精确位置

防毒墙网络版可在检测到病毒/恶意软件后移除，并恢复文件的完整性。

国际计算机安全组织（包括 ICSA，国际计算机安全协会）每年都会证实趋势科技扫描引擎合格。

更新扫描引擎

通过将最具时效性的病毒/恶意软件信息存储在病毒码中，趋势科技最大程度地减少了扫描引擎更新次数，同时可使防护保持最新。然而，趋势科技将定期提供新的扫描引擎版本。趋势科技将在以下情况下发布新的引擎：

- 将新的扫描和检测技术纳入软件中
- 发现扫描引擎无法处理的新的可能有害的病毒/恶意软件
- 扫描性能的增强
- 添加了文件格式、脚本语言、编码和/或压缩格式

病毒扫描驱动程序

病毒扫描驱动程序监控用户对文件的操作。这些操作包括打开或关闭文件以及执行应用程序。此驱动程序有三个版本。一个版本适用于 Windows 2000，其名称为 **TmFilter.sys**。另外两个版本（**TmXPFlt.sys** 和 **TmPreFlt.sys**）适用于除 Windows 2000 之外的操作系统。TmXPFlt.sys 用于实时配置病毒扫描引擎，TmPreFlt.sys 用于监视用户操作。

注意： 此组件不显示在控制台上。要检查其版本，请导航到 <服务器安装文件夹>\PCCSRV\Pccnt\Drv。右键单击 .sys 文件，选择**属性**，然后转到**版本**选项卡。

IntelliTrap 特征码

IntelliTrap 特征码可以检测打包为可执行文件的实时压缩文件。

IntelliTrap 例外特征码

IntelliTrap 例外特征码包含“允许的”压缩文件的列表。

损害清除服务组件

病毒清除引擎

病毒清除引擎扫描并移除特洛伊木马和特洛伊木马进程。此引擎支持 32 位和 64 位平台。

病毒清除模板

病毒清除引擎使用病毒清除模板来识别特洛伊木马文件和进程，以便进行清除。

防间谍软件组件

间谍软件特征码

间谍软件特征码识别以下位置中的间谍软件/灰色软件：文件和程序、内存中的模块、Windows 注册表和 URL 快捷方式。

间谍软件扫描引擎

间谍软件扫描引擎扫描间谍软件/灰色软件，并对其执行适当的扫描处理措施。此引擎支持 32 位和 64 位平台。

间谍软件主动监控特征码

间谍软件主动监控特征码用于实时间谍软件/灰色软件扫描。只有传统客户端才使用此特征码。

云安全客户端使用云安全客户端病毒码实时扫描间谍软件/灰色软件。如果在扫描期间无法确定扫描目标的风险，则客户端将向云安全服务器发送扫描查询。

防火墙组件

通用防火墙驱动程序

通用防火墙驱动程序与通用防火墙特征码结合使用，以扫描客户端计算机中是否有网络病毒。此驱动程序支持 32 位和 64 位平台。

通用防火墙特征码

通用防火墙特征码类似于病毒码，可帮助防毒墙网络版识别病毒特征（表示存在网络病毒的独特位和字节模式）。

Web 信誉组件

URL 过滤引擎

URL 过滤引擎可促进防毒墙网络版和趋势科技 URL 过滤服务之间的通信。URL 过滤服务是对 URL 进行分级并将分级信息提供给防毒墙网络版的系统。

行为监控组件

行为监控驱动程序

此内核模式驱动程序监控系统事件并将其传递给行为监控核心服务，以便实施策略。

行为监控核心服务

此用户模式服务有下列功能：

- 提供 rootkit 检测
- 控制对外部设备的访问
- 保护文件、注册码和服务

行为监控配置特征码

行为监控驱动程序使用此特征码来识别普通系统事件并将其从策略实施范围中排除。

数字签名特征码

此特征码包含有效数字签名的列表，行为监控核心服务使用该列表来确定造成系统事件的源程序是否安全。

策略强制特征码

行为监控核心服务根据此特征码中的策略检查系统事件。

程序

客户端程序

防毒墙网络版客户端程序提供抵御安全风险的实际防护。

Cisco Trust Agent

Cisco Trust Agent 可以启用客户端与支持 Cisco NAC 的路由器之间的通信。此代理仅在安装策略服务器 for Cisco NAC 时起作用。

Hotfix、Patch 和 Service Pack

在官方产品发布后，趋势科技经常会开发以下项，以解决问题，增强产品性能或添加新功能：

- **hotfix**
- **Patch**
- **Security Patch（安全 Patch）**
- **Service Pack**

您的供应商或技术支持提供者可能会在这些项可用时与您联系。请访问趋势科技 Web 站点来获取有关新 Hotfix、Patch 和 Service Pack 发布的信息：

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

所有发布都包括一个包含有安装、部署和配置信息的自述文件。执行安装前，请仔细阅读该自述文件。

Hotfix 和 Patch 历史

当防毒墙网络版服务器将 hotfix 或 patch 文件部署到防毒墙网络版客户端时，客户端程序会在注册表编辑器中记录有关 hotfix 或 patch 的信息。可以使用后勤软件（如 Microsoft SMS、LANDesk™ 或 BigFix™）查询多个客户端的此信息。

注意： 此功能不记录仅部署到服务器的 hotfix 和 patch。

此功能从带有 patch 3 的防毒墙网络版 8.0 Service Pack 1 开始可用。

- 从带有 patch 3 或更高版本的 8.0 Service Pack 1 版本升级的客户端记录为版本 8 和 10 安装的 hotfix 和 patch。
- 从带有 patch 3 的 8.0 Service Pack 1 之前的版本升级的客户端仅记录为版本 10 安装的 hotfix 和 patch。

信息存储在以下键中：

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>
- 对于运行 x64 类型平台的计算机：
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product versio>

检查以下键：

- **键：** HotFix_installed
类型： REG_SZ
值： <Hot fix or patch name>
- **键：** HotfixInstalledNum
类型： DWORD
值： <Hot fix or patch number>

更新概述

所有组件更新都源自趋势科技 ActiveUpdate 服务器。在更新可用时，*防毒墙网络版服务器*和*云安全服务器（本地或全局）*将下载更新的组件。在两个服务器之间不存在组件下载重叠，因为每个服务器都下载一组特定的组件。

注意： 可以将防毒墙网络版服务器和云安全服务器都配置为从趋势科技 ActiveUpdate 服务器之外的源更新。为此，需要设置定制更新源。如果在设置此更新源时需要帮助，请联系技术支持提供商。

防毒墙网络版服务器和客户端更新

防毒墙网络版服务器下载客户端需要的大多数组件。它唯一不下载的组件是云安全云端病毒码（由云安全服务器下载）。

如果防毒墙网络版服务器管理大量的客户端，则更新可能会占用大量的服务器计算机资源，从而影响服务器的稳定性和性能。为解决此问题，防毒墙网络版提供了更新代理功能，允许某些客户端共享向其他客户端分发更新的任务。

下表描述了防毒墙网络版服务器和客户端的不同组件更新选项，以及建议的使用时机：

表 4-1. 服务器-客户端更新选项

更新选项	描述	建议
ActiveUpdate 服务器 防毒墙网络版 服务器 客户端	防毒墙网络版服务器将从趋势科技 ActiveUpdate 服务器（或其他更新源）接收更新的组件，并将在客户端上启动组件更新。	如果防毒墙网络版服务器和客户端之间无“低带宽”部分，请使用此方法。

表 4-1. 服务器-客户端更新选项（续）

更新选项	描述	建议
ActiveUpdate 服务器 防毒墙网络版 服务器 更新代理 客户端	防毒墙网络版服务器将从 ActiveUpdate 服务器（或其他更新源）接收更新的组件，并将在客户端上启动组件更新。然后充当更新代理的客户端将通知客户端更新组件。	如果防毒墙网络版服务器和客户端之间有“低带宽”部分，请使用此方法来平衡网络通信负载。
ActiveUpdate 服务器 更新代理 客户端	更新代理将直接从 ActiveUpdate 服务器（或其他更新源）接收更新的组件，并通知客户端更新组件。	仅当在从防毒墙网络版服务器或其他更新代理更新更新代理的过程中遇到问题时，使用此方法。 在多数情况下，更新代理从防毒墙网络版服务器或其他更新代理处接收更新的速度比从外部更新源处接收的速度快。
ActiveUpdate 服务器 客户端	防毒墙外客户端直接从 ActiveUpdate 服务器（或其他更新源）处接收更新的组件。	仅当在从防毒墙网络版服务器或其他更新代理更新客户端的过程中遇到问题时，使用此方法。 在多数情况下，客户端从防毒墙网络版服务器或更新代理处接收更新的速度比从外部更新源处接收的速度快。

云安全服务器更新

云安全服务器下载云安全云端病毒码。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： 有关云安全服务器的详细信息，请参阅第 1-10 页的 [云安全服务器](#)；有关服务器更新的详细信息，请参阅第 4-19 页的 [云安全服务器更新](#)。

下表描述了云安全服务器的更新过程。

表 4-2. 云安全服务器的更新过程

更新过程	描述
ActiveUpdate 服务器 Internet 云安全服务器	Internet 云安全服务器从趋势科技 ActiveUpdate 服务器接收更新。未连接到公司网络的云安全客户端向 Internet 云安全服务器发送扫描查询。
ActiveUpdate 服务器 本地云安全服务器	本地云安全服务器（集成型或独立型）从趋势科技 ActiveUpdate 服务器接收更新。已连接到公司网络的云安全客户端向本地云安全服务器发送扫描查询。

防毒墙网络版服务器更新

防毒墙网络版服务器下载以下组件并将它们部署到客户端：

表 4-3. 由防毒墙网络版服务器下载的组件

组件	分发	
	传统客户端	云安全客户端
云安全客户端病毒码	否	是
传统病毒码	是	否
病毒扫描引擎	是	是
病毒扫描驱动程序	是	是
IntelliTrap 特征码	是	是
IntelliTrap 例外特征码	是	是
病毒清除引擎	是	是

表 4-3. 由防毒墙网络版服务器下载的组件（续）

组件	分发	
	传统客户端	云安全客户端
病毒清除模板	是	是
间谍软件特征码	是	是
间谍软件扫描引擎	是	是
间谍软件主动监控特征码	是	否
通用防火墙驱动程序	是	是
通用防火墙特征码	是	是
URL 过滤引擎	是	是
行为监控驱动程序	是	是
行为监控核心服务	是	是
行为监控配置特征码	是	是
数字签名特征码	是	是
策略强制特征码	是	是

要使服务器可以将更新的组件部署到客户端，请配置自动更新设置。如果禁用自动更新，则服务器将下载更新，但不将它们部署到客户端。有关详细信息，请参阅第 4-25 页的 [自动更新](#)。

在 Web 控制台的“摘要”窗口上查看组件的当前版本，并确定带有更新组件和过期组件的客户端数。

趋势科技会定期发布特征码文件以使客户端防护保持最新。由于定期提供特征码文件更新，因此防毒墙网络版将使用一个名称为[组件复制](#)的机制，该机制允许更快速地下载特征码文件。请参阅第 4-14 页的[服务器组件复制](#)以获取详细信息。

如果使用代理服务器连接到 Internet，请使用正确的代理服务器设置成功下载更新。

服务器更新源

将防毒墙网络版服务器配置为从趋势科技 ActiveUpdate 服务器或从其他源下载组件。

服务器下载任何可用更新后，可以基于在**更新 > 联网计算机 > 自动更新**中指定的设置，自动通知客户端更新其组件。如果组件更新非常重要，则允许用户通过转至**更新 > 联网计算机 > 手动更新**立即通知客户端。

注意： 如果在**更新 > 联网计算机 > 自动更新**中未指定部署时间表或事件触发的更新设置，则服务器将下载更新但不通知客户端更新。

配置服务器更新源：

导航路径：更新 > 服务器 > 更新源

1. 选择想要下载组件更新的位置。

如果选择 ActiveUpdate 服务器，请确保该服务器具有 Internet 连接；如果使用代理服务器，请测试是否可以使用代理服务器设置建立 Internet 连接。有关详细信息，请参阅第 4-14 页的[用于服务器更新的代理服务器](#)。

如果选择定制更新源，请为此更新源设置相应的环境和更新资源。此外，还应确保服务器计算机和此更新源之间存在有效连接。如果在设置更新源时需要帮助，请联系技术支持提供商。

注意： 从更新源下载组件时，防毒墙网络版服务器使用组件复制。有关详细信息，请参阅第 4-14 页的[服务器组件复制](#)。

2. 单击保存。

用于服务器更新的代理服务器

将在服务器计算机上托管的服务器程序配置为从趋势科技 ActiveUpdate 服务器下载更新时使用代理服务器设置。服务器程序包括防毒墙网络版服务器和集成型云安全服务器。

配置代理服务器设置：

导航路径：管理 > 代理服务器设置 > “外部代理服务器”选项卡

1. 在**防毒墙网络版服务器计算机更新**部分中，选中相应的复选框以启用代理服务器。
2. 指定代理服务器协议、服务器名称或 IP 地址以及端口号。
3. 如果代理服务器要求认证，则在提供的文本框中键入用户名和密码。
4. 单击**保存**。

服务器组件复制

可以从趋势科技 ActiveUpdate 服务器下载最新版本的完全特征码文件时，也可以下载 14 个“增量特征码”。增量特征码是完全特征码文件的较小版本，说明了最新特征码文件和先前完全特征码文件版本之间的差异。例如，如果最新版本为 175，则增量特征码 v_173.175 包含在 V175 中但不在 V173 中的签名（由于特征码编号以 2 为增量发布，因此 V173 是前一完全特征码版本。增量特征码 v_171.175 包含在 V175 中但不在 V171 中的签名。

要减小下载最新特征码时生成的网络流量，防毒墙网络版执行组件复制（防毒墙网络版服务器或更新代理只下载增量特征码的组件更新方式）。有关更新代理如何执行组件复制的信息，请参阅第 4-38 页的[更新代理组件复制](#)。

组件复制适用于以下组件：

- 病毒码
- 云安全客户端病毒码
- 病毒清除模板
- IntelliTrap 例外特征码
- 间谍软件特征码
- 间谍软件主动监控特征码

组件复制场景

要解释用于服务器的组件复制，请参考以下场景：

表 4-4. 服务器组件复制场景

防毒墙网络版服务器上的完全特征码	当前版本： 171					
	其他可用版本： 169 167 165 163 161 159					
ActiveUpdate 服务器上的最新版本	173.175	171.175	169.175	167.175	165.175	
	163.175	161.175	159.175	157.175	155.175	
	153.175	151.175	149.175	147.175		

1. 防毒墙网络版服务器将其当前完全特征码版本与 ActiveUpdate 服务器上的最新版本进行比较。如果两个版本之间的差值小于等于 14，则服务器只下载代表这两个版本差值的增量病毒码。

注意： 如果此差值大于 14，则服务器自动下载完全版的特征码文件和 14 个增量特征码。

基于示例说明：

- V171 和 V175 之间的差值是 2。换言之，服务器没有 V173 和 V175。
 - 服务器将下载增量特征码 171.175。此增量特征码代表 V171 和 V175 之间的差值。
2. 服务器将增量特征码和其当前完全特征码合并以生成最新的完全病毒码。

基于示例说明：

- 在服务器上，防毒墙网络版将 V171 与增量病毒码 171.175 合并以生成 V175。
- 服务器具有 1 个增量病毒码 (171.175) 和最新的完全特征码 (V175)。

3. 服务器基于服务器上可用的其他完全特征码生成增量特征码。如果服务器没有生成这些增量特征码，未下载较早增量特征码的客户端将自动下载完全特征码文件，继而会产生更多网络通信。

基于示例说明：

- 由于服务器具有特征码 V169、V167、V165、V163、V161 和 V159，因此它可以生成以下增量特征码：

169.175 167.175 165.175 163.175 161.175 159.175

- 由于服务器已经具有增量特征码 171.175，因此它不需要使用 V171。
- 服务器现在具有 7 个增量特征码：

171.175 169.175 167.175 165.175 163.175 161.175 159.175

- 服务器保留最后 7 个完全特征码版本（V175、V171、V169、V167、V165、V163 和 V161）。并删除任何较旧版本 (V159)。

4. 服务器将其当前增量特征码与 ActiveUpdate 服务器上可用的增量特征码进行比较。服务器将下载它所没有的增量特征码。

基于示例说明：

- ActiveUpdate 服务器具有 14 个增量特征码：

173.175 171.175 169.175 167.175 165.175 163.175 161.175
159.175 157.175 155.175 153.175 151.175 149.175 147.175

- 防毒墙网络版服务器具有 7 个增量特征码：

171.175 169.175 167.175 165.175 163.175 161.175 159.175

- 防毒墙网络版服务器下载其他 7 个增量特征码：

173.175 157.175 155.175 153.175 151.175 149.175 147.175

- 该服务器现在具有 ActiveUpdate 服务器上可用的所有增量特征码。

5. 客户端可以使用最新的完全特征码和这 14 个增量特征码。

服务器更新方法

手动更新防毒墙网络版服务器组件，或通过配置更新时间表来更新它们。

要使服务器可以将更新的组件部署到客户端，请配置自动更新设置。如果禁用自动更新，则服务器将下载更新，但不将它们部署到客户端。有关详细信息，请参阅第 4-25 页的 [自动更新](#)。

手动更新

如果更新非常重要，请执行手动更新以便服务器可以立即获取更新。有关详细信息，请参阅第 4-18 页的 [手动更新](#)。

预设更新

防毒墙网络版服务器在预设的日期和时间连接到更新源，以获取最新组件。有关详细信息，请参阅第 4-17 页的 [预设更新](#)。

预设更新

将防毒墙网络版服务器配置为定期检查其更新源并自动下载任何可用更新。由于客户端通常从服务器获得更新，因此使用预设更新是确保安全风险防护始终保持最新的简单有效的方法。

配置服务器更新时间表：

导航路径：更新 > 服务器 > 预设更新

1. 选择**启用防毒墙网络版服务器的预设更新**。
2. 选择要更新的组件。
3. 指定更新时间表。对每日、每周和每月更新而言，这段时间即防毒墙网络版将执行更新的小时数。防毒墙网络版在此时间段的任意给定时间内进行更新。
4. 单击**保存**。

手动更新

在安装或升级服务器之后以及存在爆发时，在防毒墙网络版服务器上手动更新组件。

手动更新服务器：

导航路径：更新 > 服务器 > 手动更新

在 Web 控制台的主菜单上，单击“**立即更新服务器**”

1. 选择要更新的组件。
2. 单击**更新**。服务器将下载更新过的组件。

服务器更新日志

检查服务器更新日志，以确定更新某些组件时是否存在问题。日志包括防毒墙网络版服务器的组件更新。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅第 8-16 页的[管理日志](#)。

查看服务器更新日志：

导航路径：日志 > 服务器更新日志

1. 检查**结果**列以查看是否存在未更新的组件。
2. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。通常使用电子表格应用程序（例如 Microsoft Excel）来打开 CSV 文件。

云安全服务器更新

本部分论述如何在集成型云安全服务器中更新组件。有关在独立型服务器中更新组件的详细信息，请参阅《趋势科技云安全扫描防毒墙网络版入门指南》。

云安全服务器下载云安全云端病毒码。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。客户端不下载云安全云端病毒码。

注意： 云安全解决方案中使用的其他特征码（称为云安全客户端病毒码）托管在客户端更新源（防毒墙网络版服务器或[定制的更新源](#)）上，供客户端下载。

趋势科技每小时更新一次云安全云端病毒码。与防毒墙网络版服务器一样，云安全服务器也使用称为[组件复制](#)的机制，该机制允许更快地下载特征码文件。请参阅第 4-14 页的[服务器组件复制](#)以获取详细信息。

服务器更新设置

将云安全服务器配置为从趋势科技 ActiveUpdate 服务器或从其他源下载云安全云端病毒码。手动更新特征码或配置更新时间表。

配置服务器更新设置：

导航路径：云安全扫描 > 集成型服务器

1. 选择使用集成型云安全服务器。如果不选中该复选框：
 - 趋势科技云安全服务器服务 (iCRCSservice.exe) 将停止。
 - 集成型服务器将停止从 ActiveUpdate 服务器更新组件。
 - 客户端将无法向集成型服务器发送扫描查询。
2. 配置云安全服务器列表时，使用[服务器地址](#)下的信息。有关该列表的详细信息，请参阅第 5-14 页的[云安全扫描源](#)。

客户端可以使用 HTTP 和 HTTPS 协议连接到集成型服务器。HTTPS 的连接更安全，而 HTTP 使用的带宽更小。当客户端使用特定协议连接时，它们按其服务器地址识别集成型服务器。

提示: 由另一个防毒墙网络版服务器管理的客户端也可以连接到集成型服务器。在其他防毒墙网络版服务器的 Web 控制台上，将集成型服务器的地址添加到云安全服务器列表。

3. 查看云安全云端病毒码版本。要手动更新特征码，请单击**立即更新**。更新结果将显示在窗口顶部。
4. 要自动更新特征码，请启用预设更新并配置更新时间表。
5. 选择想要下载组件更新的位置。

如果选择 ActiveUpdate 服务器，请确保该服务器具有 Internet 连接；如果使用代理服务器，请测试是否可以使用代理服务器设置建立 Internet 连接。有关详细信息，请参阅第 4-14 页的[用于服务器更新的代理服务器](#)。

如果选择定制更新源，请为此更新源设置相应的环境和更新资源。此外，还应确保服务器计算机和此更新源之间存在有效连接。如果在设置更新源时需要帮助，请联系技术支持提供商。

6. 单击**保存**。

客户端更新

要确保客户端处于不受最新安全风险危害的状态，请定期更新客户端组件。更新客户端之前，请检查其更新源是否具有最新的组件。有关如何更新典型更新源（防毒墙网络版服务器）的信息，请参阅第 4-11 页的[防毒墙网络版服务器更新](#)。

下表列出了客户端存储在计算机上的所有组件和使用特定扫描方法时使用的组件。每个组件的更新源均为防毒墙网络版服务器或定制更新源。

注意： 云安全服务器下载云安全云端病毒码，但不会将此病毒码分发到客户端。当云安全客户端向云安全服务器发送扫描查询时，使用此特征码。

表 4-5. 客户端存储的防毒墙网络版组件

组件	可用性	
	传统客户端	云安全客户端
云安全客户端病毒码	否	是
传统病毒码	是	否
病毒扫描引擎	是	是
病毒扫描驱动程序	是	是
IntelliTrap 特征码	是	是
IntelliTrap 例外特征码	是	是
病毒清除引擎	是	是
病毒清除模板	是	是
间谍软件特征码	是	是
间谍软件扫描引擎	是	是

表 4-5. 客户端存储的防毒墙网络版组件（续）

组件	可用性	
	传统客户端	云安全客户端
间谍软件主动监控特征码	是	否
通用防火墙驱动程序	是	是
通用防火墙特征码	是	是
URL 过滤引擎	是	是
行为监控驱动程序	是	是
行为监控核心服务	是	是
行为监控配置特征码	是	是
数字签名特征码	是	是
策略强制特征码	是	是

从防毒墙网络版服务器和定制源更新

客户端可以从各种源获取更新，如防毒墙网络版服务器或定制的更新源。

配置客户端更新源：

导航路径：更新 > 联网计算机 > 更新源

1. 选择是从**标准更新源**（防毒墙网络版服务器）还是从**定制的更新源**更新。
2. 单击**通知所有客户端**。

定制的更新源

除了防毒墙网络版服务器外，客户端还可以从定制更新源进行更新。定制更新源可帮助减少定向到防毒墙网络版服务器的客户端更新流量，并允许无法连接到防毒墙网络版服务器的客户端获取及时的更新。在定制的更新源列表（最多可容纳 1024 个更新源）上指定定制的更新源。

提示： 趋势科技建议将一些客户端指定为**更新代理**，然后将它们添加到列表中。

配置定制的更新源列表：

导航路径：更新 > 联网计算机 > 更新源

1. 选择**定制的更新源**，然后单击**添加**。
2. 在显示的窗口中，键入将从更新源接收更新的客户端 IP 地址的范围。
3. 指定更新源。可以选择更新代理（如果已分配），或键入特定源的 URL。
4. 单击**保存**。
5. 通过单击 IP 范围链接来编辑更新源。在显示的窗口中修改设置，然后单击**保存**。
6. 通过选中复选框然后单击**删除**将更新源从该列表中移除。
7. 要移动更新源，请单击向上箭头或向下箭头。每次仅可移动一个源。

在设置并保存列表后，更新过程按如下方式进行：

1. 客户端从列表上的第一个条目更新。
2. 如果无法从第一个条目更新，则客户端将从第二个条目更新，依此类推。
3. 如果无法从所有条目更新，则客户端将检查是否启用了选项**如果所有定制源均不可用或未找到，则从防毒墙网络版服务器更新**。如果已启用，则客户端从防毒墙网络版服务器更新。

如果禁用该选项，则在满足以下任一条件时，客户端会尝试直接连接到趋势科技 ActiveUpdate 服务器：

- 在**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 其他设置**选项卡 > **更新设置**中，启用了选项**客户端从趋势科技 ActiveUpdate 服务器下载更新**。

- ActiveUpdate 服务器
(<http://osce10-p.activeupdate.trendmicro.com.cn/activeupdate/china>) 未包括在定制的更新源列表中。

4. 如果无法从所有可能的源更新，则客户端将退出更新过程。

标准更新源

防毒墙网络版服务器是客户端的标准更新源。如果将客户端配置为直接从防毒墙网络版服务器更新，则更新过程按如下方式进行：

1. 客户端从防毒墙网络版服务器获取更新。
2. 如果无法从防毒墙网络版服务器更新，则在满足以下任一条件时，客户端会尝试直接连接到趋势科技 ActiveUpdate 服务器：
 - 在**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 其他设置选项卡 > 更新设置**中，启用了选项**客户端从趋势科技 ActiveUpdate 服务器下载更新**。
 - ActiveUpdate 服务器
(<http://osce10-p.activeupdate.trendmicro.com.cn/activeupdate/china>) 是定制的更新源列表中的第一个条目。

提示： 仅当从防毒墙网络版服务器更新遇到问题时，才将 ActiveUpdate 服务器放置在列表的顶部。当客户端直接从 ActiveUpdate 服务器更新时，在网络和 Internet 之间会占用大量带宽。

3. 如果无法从所有可能的源更新，则客户端将退出更新过程。

客户端更新方法

从防毒墙网络版服务器或定制的更新源更新组件的客户端可以使用以下更新方法：

自动更新

客户端更新在发生某些事件时自动运行，或根据时间表运行。有关详细信息，请参阅第 4-25 页的 [自动更新](#)。

手动更新

如果更新非常重要，请使用手动更新以立即通知客户端执行组件更新。有关详细信息，请参阅第 4-29 页的 [手动更新](#)。

基于权限的更新

具有更新权限的用户可更好地控制在其计算机上更新防毒墙网络版客户端的方式。有关详细信息，请参阅第 4-30 页的 [更新权限](#)。

自动更新

自动更新免除了您通知所有客户端更新的负担，并消除了客户端计算机没有最新组件的风险。

除了组件以外，防毒墙网络版客户端还可在自动更新过程中接收更新的配置文件。客户端需要这些配置文件应用新的设置。每次通过 **Web 控制台** 修改防毒墙网络版设置时，配置文件也随之更改。要指定将配置文件应用于客户端的频率，请参阅下面的步骤 3。

注意： 可以将客户端配置为在自动更新过程中使用代理服务器设置。有关详细信息，请参阅第 4-31 页的 [客户端组件更新的代理服务器](#)。

有以下两种类型的自动更新：

事件触发更新

服务器可以通知联机客户端在下载最新组件后更新组件，还可以在脱机客户端重新启动并连接到服务器时通知它们。可选择在更新后是否对客户端计算机启动立即扫描（手动扫描）。

注意： 如果防毒墙网络版服务器在下载组件后，无法向客户端成功发送更新通知，则会在 15 分钟自动重新发送通知。服务器在客户端响应之前连续发送更新通知，最多 5 次。如果第五次尝试未成功，则服务器会停止发送通知。如果选择在客户端重新启动时更新组件的选项，然后连接到服务器，则组件更新将仍然继续。

基于时间表更新

运行预设更新是一种权限。需要首先选择具有该权限的客户端，然后这些客户端将基于时间表运行更新。

注意： 要将基于时间表的更新与网络地址转换一起使用，请参阅第 4-30 页的 *使用 NAT 的客户端预设更新*。

自动更新联网计算机组件：

导航路径：更新 > 联网计算机 > 自动更新

1. 选择将触发组件更新的事件。

表 4-6. 事件触发更新选项

选项	描述
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。	服务器在完成更新后立即通知客户端进行更新。频繁更新的客户端只需下载增量特征码，因此缩短了完成更新所用的时间（有关增量特征码的详细信息，请参阅第 4-14 页的 服务器组件复制 ）。但是，频繁更新可能会对服务器性能产生负面影响，尤其是大量的客户端同时更新时。 如果具有处于漫游模式的客户端，并且还希望更新这些客户端，请选择 包括漫游客户端 。有关漫游模式的详细信息，请参阅第 9-33 页的 漫游客户端 。
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）。	错过更新的客户端在建立与服务器的连接时立即下载组件。如果客户端处于脱机状态，或者安装了客户端的计算机没有启动和运行，则客户端可能会错过更新。
更新后执行“立即扫描”（漫游客户端除外）	服务器通知客户端在事件触发更新之后扫描。如果特定更新是对网络内已传播的安全风险的响应，请考虑启用此选项。

2. 选择客户端使用预设更新权限执行预设更新的频率。

如果已授予客户端预设更新权限，则继续执行下一步。

如果未授予客户端预设更新权限，请首先执行以下步骤：

- a. 转至[联网计算机 > 客户端管理](#)，然后选择希望其具有该权限的客户端。
- b. 单击[设置 > 权限和其他设置](#)。

*选项 1：*在[权限](#)选项卡下，转至[组件更新权限](#)部分。将看到[启用预设更新](#)选项。

选项 2: 在**其他设置**选项卡下，转至**更新设置**部分。将看到另一个**启用预设更新**选项。

如果要使客户端用户能够在客户端控制台上启用或禁用预设更新，请启用选项 1 和 2。保存设置后，更新将在客户端计算机上如预设的那样运行。仅当客户端用户右键单击系统托盘上的防毒墙网络版图标并选择**禁用预设更新**时，预设更新才会停止运行。

如果希望预设更新始终运行并防止客户端用户禁用预设更新，请启用选项 1 并禁用选项 2。

c. 保存设置。

3. 配置时间表。

- a. 如果选择**分钟**或**小时**，则可选择**每天只更新一次客户端配置**。如果未选择此选项，则防毒墙网络版客户端会在指定时间间隔检索服务器上可用的更新组件和任何更新的配置文件。如果选择此选项，则防毒墙网络版仅在指定的时间间隔更新组件，并且每天只更新一次配置文件。

提示: 趋势科技会经常更新组件；但是，防毒墙网络版配置设置可能更改不是很频繁。使用组件更新配置文件需要更多的带宽，还会增加防毒墙网络版完成更新所需的时间。出于这个原因，趋势科技建议选择每天只更新一次客户端配置。

- b. 如果选择**每日一次**或**每周一次**，则指定更新的时间和防毒墙网络版服务器将通知客户端更新组件的时间段。例如，如果开始时间为中午 12 点，时间段为 2 个小时，则防毒墙网络版会随机通知所有联机客户端从中午 12 点到下午 2 点更新组件。此设置可防止所有的联机客户端在指定的开始时间同时连接到服务器，极大地减少指向服务器的流量。

4. 单击**保存**。

将不会通知脱机客户端。如果在**事件触发更新**下选择了**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）**，则脱机客户端在时间段过期后变为联机时仍可更新组件。否则，如果启动手动更新，则脱机客户端会在下一个时间表才更新组件。

手动更新

客户端组件严重过期和有爆发时手动更新客户端组件。客户端较长时间无法从更新源更新组件时，客户端组件将严重过期。

除组件外，防毒墙网络版客户端在手动更新过程中还自动接收更新过的配置文件。客户端需要这些配置文件应用新的设置。每次通过 Web 控制台修改防毒墙网络版设置时，配置文件也随之更改。

手动更新客户端：

导航路径：更新 > 联网计算机 > 手动更新

1. 在窗口的顶部将显示防毒墙网络版服务器上当前可用的组件和上次更新这些组件的日期。在通知客户端更新之前，请确保组件是最新的。

注意： 手动更新服务器上的任何过期组件。有关详细信息，请参阅第 4-18 页的 [手动更新](#)。

2. 选择要更新的客户端。更新带有过期组件的客户端，或者从客户端树中选择特定客户端。
 - **选择带有过期组件的客户端：** 服务器搜索其组件版本早于服务器上版本的客户端，然后通知这些客户端更新。如果希望服务器还搜索与服务器具有有效连接的漫游客户端，请选择**包括漫游客户端**。单击**开始更新**。
 - **手动选择客户端：** 选择此选项后，单击**选择**。在打开的客户端树中，选择要更新的客户端，然后单击客户端树顶部的**启动组件更新**。

服务器开始通知每台客户端下载更新过的组件。要检查通知状态，请转至**更新 > 摘要**窗口。

使用 NAT 的客户端预设更新

如果本地网络使用 **NAT**，则可能出现以下问题：

- 客户端在 Web 控制台上将显示为脱机。
- 防毒墙网络版服务器无法成功通知客户端更新和配置更改。

通过使用预设更新将更新的组件和配置文件从服务器部署到客户端来解决这些问题。

执行下列步骤：

1. 在客户端计算机上安装防毒墙网络版客户端之前：
 - a. 在**更新 > 联网计算机 > 自动更新 > 基于时间表更新**中配置客户端更新时间表。
 - b. 在**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 权限选项卡 > 组件更新权限**中授予客户端启用预设更新的权限。
2. 如果在客户端计算机上已存在防毒墙网络版客户端：
 - a. 在**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 权限选项卡 > 组件更新权限**中授予客户端执行“立即更新”的权限。
 - b. 指导用户手动更新客户端计算机上的组件（通过右键单击系统托盘中的“防毒墙网络版”图标，然后单击“立即更新”）以获取更新的配置设置。

客户端更新时，会收到更新的组件和配置文件。

更新权限

授予客户端用户某些权限，如执行手动更新和启用预设更新。有关详细信息，请参阅第 9-15 页的[组件更新权限](#)。

将更新权限授予客户端：

1. 转至**联网计算机 > 客户端管理**。
2. 在客户端树上，选择将具有更新权限的客户端。
3. 单击**设置 > 权限和其他设置**，在**权限选项卡**下，转至**组件更新权限**部分。
4. 除了更新权限外，通过单击**其他设置选项卡**并转至**更新设置**部分为客户端配置更新相关的设置。有关详细信息，请参阅第 9-15 页的[更新设置](#)。

客户端组件更新的代理服务器

在自动更新期间，或者如果防毒墙网络版客户端具有执行“立即更新”的权限，则它们可以使用代理服务器设置。

表 4-7. 客户端组件更新过程中使用的代理服务器设置

更新方法	使用的代理服务器设置	用法
自动更新 有关详细信息，请参阅第 4-25 页的 自动更新 。	- 自动代理服务器设置。有关详细信息，请参阅第 9-29 页的代理服务器配置。 - 内部代理服务器设置。有关详细信息，请参阅第 9-39 页的内部代理服务器。	- 防毒墙网络版客户端将首先使用自动代理服务器设置来更新组件。 - 如果未启用自动代理服务器设置，则将使用内部代理服务器设置。 - 如果两种设置都禁用，则客户端将不使用任何代理服务器设置。
立即更新 (有关详细信息，请参阅第 9-15 页的 组件更新权限)	- 自动代理服务器设置。有关详细信息，请参阅第 9-29 页的代理服务器配置。 - 用户配置的代理服务器设置。可以授予客户端用户配置代理服务器设置的权限。有关详细信息，请参阅第 9-14 页的代理服务器设置权限。	- 防毒墙网络版客户端将首先使用自动代理服务器设置来更新组件。 - 如果未启用自动代理服务器设置，则将使用用户配置的代理服务器设置。 - 如果两种配置都禁用，或者如果禁用了自动代理服务器设置且客户端用户没有所需的权限，则更新组件时客户端将不使用任何代理服务器。

客户端更新日志

检查客户端更新日志，以确定在客户端上更新病毒码时是否存在问题。

注意： 在此产品版本中，只能从 Web 控制台查询病毒码更新的日志。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅第 8-16 页的 [管理日志](#)。

查看客户端更新日志：

导航路径：日志 > 联网计算机日志 > 组件更新

1. 要查看客户端更新数，请单击**进度**列下的**查看**。在显示的“组件更新进度”窗口中，查看每间隔 15 分钟更新的客户端数以及更新的客户端总数。
2. 要查看已更新病毒码的客户端，请单击**详细信息**列下的**查看**。
3. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。通常使用电子表格应用程序（例如 Microsoft Excel）来打开 CSV 文件。

客户端更新通知

当发生与更新相关的以下事件时，防毒墙网络版将通知客户端用户：

- 病毒码在特定天数后保持过期状态。
- hotfix 安装要求计算机重新启动以加载新内核模式驱动程序版本。

有关详细信息，请参阅第 9-25 页的 [警报设置](#)。

组件还原

还原是指恢复到先前的病毒码、云安全客户端病毒码和病毒扫描引擎版本。如果这些组件未正常运行，则将它们还原到其先前的版本。防毒墙网络版保留病毒扫描引擎的当前版本和先前版本，以及病毒码和云安全客户端病毒码的最近五个版本。

注意： 只能还原上述组件。

防毒墙网络版对于运行 32 位和 64 位平台的客户端使用不同的扫描引擎。您需要分别还原这些扫描引擎。还原过程对于所有类型的扫描引擎都相同。

还原病毒码、云安全客户端病毒码和病毒扫描引擎：

导航路径：更新 > 还原

1. 单击相应部分下面的**与服务器同步**。
 - a. 在显示的客户端树中，选择具有需要还原的组件的客户端。
 - b. 单击**还原**。单击窗口底部的**上一步**返回到“还原”窗口。
2. 如果服务器上存在较老版本的特征码文件，则通过单击**还原服务器和客户端版本**同时还原客户端和服务器的特征码文件。

更新代理

要向防毒墙网络版客户端分发部署组件的任务，请指定一些防毒墙网络版客户端充当更新代理或其他客户端的更新源。这有助于确保客户端及时接收组件更新，而不用将大量的网络通信定向于防毒墙网络版服务器。

如果网络按位置分段，且各段之间的网络链路流量负载较大，应在每个位置上至少指定一个更新代理。

更新代理的系统要求

充当更新代理的客户端必须满足以下需求：

表 4-8. 更新代理的系统要求

资源	需求
操作系统	Windows 2000、XP、Server 2003、Server 2008 或 Vista
硬件	处理器 800MHz Intel Pentium 或同等处理器 内存 • 最低 512MB，建议使用 1GB（Windows 2000、XP、Server 2003） • 最低 1GB，建议使用 1.5GB（Windows Vista、Server 2008） 可用磁盘空间 700MB 更新代理由于磁盘空间不足无法成功获取和部署组件。将具有充足磁盘空间的客户端指定为更新代理。 其他 在颜色为 256 或更高时，支持分辨率 800 x 600 的显示器
更新请求容量	取决于计算机的硬件规格

更新代理配置

更新代理配置过程分为两步：

1. 将一个客户端指定为更新代理。
2. 指定将从此更新代理更新的客户端。

注意： 单个更新代理可以处理的并行客户端连接的数量取决于计算机的硬件规格。

将一个客户端指定为更新代理：

导航路径：联网计算机 > 客户端管理 > 设置 > 更新代理设置

1. 选择客户端可以充当更新代理。
2. 单击保存。

指定将从更新代理更新的客户端：

导航路径：更新 > 联网计算机 > 更新源 > 定制的更新源列表

1. 单击添加。在显示的窗口中，键入客户端 IP 地址的范围。
2. 在更新代理文本框中，选择要为客户端指定的更新代理。
3. 单击保存。

更新代理的更新源

更新代理可以从各种源（如防毒墙网络版服务器或定制的更新源）获取更新。从 Web 控制台的“更新源”窗口配置更新源。

配置更新代理的更新源：

导航路径：更新 > 联网计算机 > 更新源

1. 选择是从更新代理的标准更新源（防毒墙网络版服务器）还是从更新代理的定制的更新源更新。
2. 单击通知所有客户端。

更新代理的定制的更新源

除了防毒墙网络版服务器外，更新代理还可以从定制更新源进行更新。定制更新源有助于减少定向到防毒墙网络版服务器的客户端更新流量。在定制的更新源列表（最多可容纳 1024 个更新源）上指定定制的更新源。有关配置列表的步骤，请参阅第 4-23 页的[定制的更新源](#)。

在设置并保存列表后，更新过程按如下方式进行：

1. 更新代理从列表上的第一个条目更新。
2. 如果无法从第一个条目更新，则代理将从第二个条目更新，依此类推。
3. 如果无法从所有条目更新，则代理将检查是否启用了选项**如果所有定制源均不可用或未找到，则从防毒墙网络版服务器更新**。如果已启用，则代理从防毒墙网络版服务器更新。

如果禁用该选项，则在满足以下任一条件时，代理会尝试直接连接到趋势科技 ActiveUpdate 服务器：

- 在**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 其他设置**选项卡 > **更新设置**中，启用了选项**客户端从趋势科技 ActiveUpdate 服务器下载更新**。
- ActiveUpdate 服务器
(<http://osce10-p.activeupdate.trendmicro.com.cn/activeupdate/china>) 未包括在定制的更新源列表中。

4. 如果无法从所有可能的源更新，则更新代理将退出更新过程。

如果启用了选项**更新代理：始终从标准更新源（防毒墙网络版服务器）更新**，并且防毒墙网络版服务器通知代理更新组件，则更新过程是不同的。过程如下：

1. 代理直接从防毒墙网络版服务器更新，并忽略更新源列表。
2. 如果无法从服务器更新，则在满足以下任一条件时，代理会尝试直接连接到趋势科技 ActiveUpdate 服务器：
 - 在**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 其他设置**选项卡 > **更新设置**中，启用了选项**客户端从趋势科技 ActiveUpdate 服务器下载更新**。

- ActiveUpdate 服务器 (<http://osce10-p.activeupdate.trendmicro.com.cn/activeupdate/china>) 是定制的更新源列表中的第一个条目。

提示: 仅当从防毒墙网络版服务器更新遇到问题时, 才将 ActiveUpdate 服务器放置在列表的顶部。当客户端直接从 ActiveUpdate 服务器更新时, 在网络和 Internet 之间会占用大量带宽。

3. 如果无法从所有可能的源更新, 则更新代理将退出更新过程。

更新代理的标准更新源

防毒墙网络版服务器是更新代理的标准更新源。如果将代理配置为直接从防毒墙网络版服务器更新, 则更新过程按如下方式进行:

1. 更新代理从防毒墙网络版服务器获取更新。
2. 如果无法从防毒墙网络版服务器更新, 则在满足以下任一条件时, 代理会尝试直接连接到趋势科技 ActiveUpdate 服务器:
 - 在**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 其他设置选项卡 > 更新设置**中, 启用了选项**客户端从趋势科技 ActiveUpdate 服务器下载更新**。
 - ActiveUpdate 服务器 (<http://osce10-p.activeupdate.trendmicro.com.cn/activeupdate/china>) 是定制的更新源列表中的第一个条目。

提示: 仅当从防毒墙网络版服务器更新遇到问题时, 才将 ActiveUpdate 服务器放置在列表的顶部。当更新代理直接从 ActiveUpdate 服务器更新时, 在网络和 Internet 之间会占用很大的带宽。

3. 如果无法从所有可能的源更新, 则更新代理将退出更新过程。

更新代理组件复制

与防毒墙网络版服务器类似，更新代理也可在下载组件时使用组件复制。有关服务器如何执行组件复制的详细信息，请参阅第 4-14 页的[服务器组件复制](#)。

更新代理的组件复制过程如下所述：

1. 更新代理将其当前完整特征码版本与更新源上的最新版本进行比较。如果两个版本之间的差值小于等于 14，则更新代理只下载代表这两个版本差值的增量病毒码。

注意： 如果此差值大于 14，则更新代理自动下载完全版的特征码文件。

2. 更新代理将其下载的增量特征码和其当前完全特征码合并以生成最新的完全病毒码。
3. 更新代理下载更新源上的所有剩余增量特征码。
4. 客户端可以使用最新的完全特征码和所有 14 个增量特征码。

更新代理的更新方法

更新代理使用可供常规客户端使用的相同更新方法。有关详细信息，请参阅第 4-25 页的[客户端更新方法](#)。

也可以使用预设更新配置工具，在使用客户端打包程序安装的更新代理上启用和配置预设更新。

注意： 如果更新代理是使用其他安装方法安装的，则此工具不可用。请参阅第 3-10 页的[安装方法](#)以获取详细信息。

使用预设更新配置工具：

1. 在更新代理计算机上，导航到 <[客户端安装文件夹](#)>。
2. 双击 **SUCTool.exe** 运行该工具。预设更新配置工具控制台将打开。
3. 选择**启用预设更新**。
4. 指定更新频率和时间。
5. 单击**应用**。

组件更新摘要

导航路径：更新 > 摘要

Web 控制台提供了“更新摘要”窗口，可通知您总体的组件更新状态，使您可以更新过期的组件。如果启用服务器预设更新，则该窗口还将显示下一个更新时间表。

定期刷新窗口以查看最新的组件更新状态。

注意： 要在集成型云安全服务器上查看组件更新，请转至[云安全扫描](#) > [集成型服务器](#)。

联网计算机的更新状态

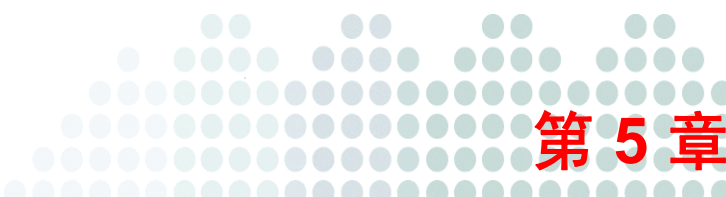
如果启动了对客户端的组件更新，请查看此部分中的以下信息：

- 已通知更新组件的客户端数。
- 尚未收到通知，但已经在通知队列中的客户端数。要取消通知这些客户端，请单击**取消通知**。

组件

在“更新状态”表中，查看防毒墙网络版服务器下载和分发的每个组件的更新状态。

对于每个组件，查看其当前版本和上次更新日期。单击编号链接以查看具有过期组件的客户端。手动更新具有过期组件的客户端。



第 5 章

保护计算机免受安全风险的危害

本章主题：

- 第 5-2 页的[关于安全风险](#)
- 第 5-8 页的[扫描方法](#)
- 第 5-18 页的[扫描类型](#)
- 第 5-24 页的[所有扫描类型的通用设置](#)
- 第 5-40 页的[与扫描相关的权限](#)
- 第 5-40 页的[全局扫描设置](#)
- 第 5-41 页的[安全风险通知](#)
- 第 5-45 页的[安全风险日志](#)
- 第 5-53 页的[爆发防护](#)
- 第 5-60 页的[设备控制](#)

关于安全风险

安全风险是病毒/恶意软件和间谍软件/灰色软件的统称。防毒墙网络版通过扫描文件，然后对每一个检测到的安全风险执行特定的处理措施来保护计算机免遭安全风险的侵扰。在短时间内检测到数量庞大的安全风险意味着爆发。防毒墙网络版可帮助抑制爆发，方法是执行爆发阻止策略并且隔离受感染的计算机，直到它们完全不存在风险。如果需要立即采取措施，通知和日志可帮助您跟踪安全风险和警报。

病毒和恶意软件

现在有好几个病毒/恶意软件，每天还有更多的被创建出来。如今的计算机病毒可通过利用企业网络、电子邮件系统和 Web 站点中的漏洞来导致大量损害。

防毒墙网络版可以保护计算机免受以下病毒/恶意软件类型的危害：

恶作剧程序

恶作剧程序是类似病毒的程序，它通常通过某种操控而使计算机显示器中显示某些内容。

特洛伊木马程序

特洛伊木马是可执行程序，它不复制，而是驻留在计算机上执行恶意行为，例如为电脑黑客潜入打开端口。这种程序经常使用 **Trojan Port（特洛伊木马端口）** 来获取计算机的访问权限。声称要清除计算机里的病毒，实际上将病毒传入计算机的应用程序，就是特洛伊木马程序的一个实例。传统的防病毒解决方案能检测和移除病毒，但不能处理特洛伊木马，尤其那些已经在系统上运行的特洛伊木马。

病毒

病毒是会复制的程序。要执行此操作，病毒需要将自己附在其他程序文件中，宿主程序一运行病毒就运行。

- **ActiveX 恶意代码：**驻留在 Web 页，执行 ActiveX™ 控件的代码
- **引导区病毒：**感染分区或磁盘的引导区的病毒
- **COM 和 EXE 文件感染源：**扩展名为 .com 或 .exe 的可执行程序
- **Java 恶意代码：**用 Java™ 编写或嵌入在其中的不依赖操作系统的病毒代码
- **宏病毒：**编码为应用程序的宏、并且通常包含在文档里的病毒
- **VBScript、JavaScript 或 HTML 病毒：**位于 Web 页中并通过浏览器下载的病毒
- **蠕虫病毒：**一个独立程序或一组程序，能将自身或自身的某个片段的功能副本传播到其他计算机，通常通过电子邮件传播

测试病毒

测试病毒是可由病毒扫描软件检测到的无害文件。使用测试病毒（例如，EICAR 测试脚本）可验证安装的防病毒软件是否可正常执行扫描。

加壳软件

加壳软件是压缩和/或加密的 Windows 或 Linux™ 可执行程序，通常为特洛伊木马程序。压缩可执行文件使防病毒产品更难以检测到加壳软件。

可能的病毒/恶意软件

具有某些病毒/恶意软件特征的可疑文件可划入此病毒/恶意软件类型。有关可能的病毒/恶意软件的详细信息，请参阅趋势科技联机病毒百科全书上的以下页：

http://threatinfo.trendmicro.com/vinfo/zh-cn/virusencyclo/default5.asp?vname=POSSIBLE_VIRUS

网络病毒

严格来说，通过网络传播的病毒不是网络病毒。只有部分病毒/恶意软件类型（例如，蠕虫病毒）才称得上是网络病毒。具体来说，网络病毒使用网络协议（例如，TCP、FTP、UDP、HTTP 和电子邮件协议）来复制。它们通常不篡改系统文件或修改硬盘驱动器的引导区。网络病毒感染客户端计算机的内存，强制客户端用通信淹没网络，引起延迟甚至网络完全瘫痪。由于网络病毒保留在内存里，因此一般的基于 I/O 的文件扫描方法通常检测不到。

防毒墙网络版防火墙使用通用防火墙特征码来识别并阻止网络病毒。有关详细信息，请参阅第 7-2 页的[关于防毒墙网络版防火墙](#)。

其他

“其他”包括未划入任何病毒/恶意软件类型下的病毒/恶意软件。

间谍软件和灰色软件

间谍软件和灰色软件是指不能归类为病毒或特洛伊木马，但是仍然可以对网络上计算机的性能产生不利影响的应用程序或文件。间谍软件和灰色软件会给组织带来重大安全、保密和合法性风险。通常间谍软件/灰色软件将执行各种不受欢迎并有威胁性的操作，如使用弹出窗口引起用户不愉快，记录用户的击键，以及将计算机漏洞暴露于攻击的威胁之下。

防毒墙网络版可以保护计算机免受以下间谍软件/灰色软件类型的危害：

间谍软件

间谍软件收集数据（例如，帐户用户名和密码、信用卡号和其他机密信息），并将这些数据传送给第三方。

广告程序

广告程序显示广告，并收集用于将来向用户发送广告的数据，例如，Web 冲浪首选项。

拨号程序

拨号程序更改客户端的 Internet 设置，可以强制计算机通过调制解调器拨打预配置的电话号码。这些号码通常是来电付费或国际号码，可导致组织必须支付大笔费用。

恶作剧程序

恶作剧程序导致计算机行为异常，例如，打开和关闭 CD-ROM 托盘以及显示许多消息框。

黑客工具

黑客工具可帮助黑客进入计算机。

远程访问工具

远程访问工具可帮助黑客远程访问和控制计算机。

密码破解程序

此类型的应用程序可帮助破解帐户的用户名和密码。

其他

“其他”包括未划入任何间谍软件/灰色软件类型下的潜在恶意程序。

间谍软件/灰色软件进入网络的方式

在用户下载在安装软件包中包括灰色软件应用程序的合法软件时，间谍软件/灰色软件经常会进入公司网络。大部分软件程序都包括最终用户许可协议 (End User License Agreement, EULA)，用户在下载前必须接受此许可协议。通常，EULA 会包括有关该应用程序的信息及其收集个人数据的预期用途的信息；但是，用户经常不会注意到此信息，或者不理解法律术语。

潜在风险和威胁

如果网络上存在有间谍软件和其他类型的灰色软件，则可能会导致以下后果：

降低计算机性能

为完成它们的任务，间谍软件/灰色软件应用程序经常需要大量的 CPU 和系统内存资源。

与 Web 浏览器相关的崩溃增加

某些类型的灰色软件（例如，广告程序），经常会在一个浏览器框或窗口中显示信息。根据这些应用程序中的代码与系统进程交互的方式，灰色软件有时可以导致浏览器崩溃或锁死，甚至可能要求计算机重新启动。

降低用户效率

由于需要关闭经常出现的弹出广告及处理恶作剧程序的负面影响，用户将不必要地打断他们的主要任务。

降低网络带宽

间谍软件/灰色软件应用程序通常会将它们收集的数据定期传送给网络上或网络之外运行的其他应用程序。

丢失个人和公司信息

间谍软件/灰色软件应用程序收集的所有数据并非都如同用户访问的 Web 站点列表一样是无害的。间谍软件/灰色软件还可以收集用户凭证，例如用于访问联机银行帐户和公司网络的凭证。

法律责任风险增加

如果网络上的计算机资源被劫持，黑客就有可能利用客户端计算机在网络外的计算机上发动攻击或安装间谍软件/灰色软件。如果网络资源参与这些类型的活动，将可能使组织承担由其他方造成的损失而引发的法律责任。

预防间谍软件/灰色软件

有多种方法可阻止间谍软件/灰色软件安装到计算机上。趋势科技建议坚持以下标准惯例：

- 配置所有类型的扫描（手动扫描、实时扫描、预设扫描和立即扫描）以扫描和移除间谍软件/灰色软件文件和应用程序。请参阅第 5-18 页的 [扫描类型](#) 以获取详细信息。
- 告知客户端用户执行以下操作：
 - 对于他们要下载及安装到计算机上的应用程序，阅读最终用户许可协议 (End User License Agreement, EULA) 及所包括的文档。
 - 对于要求授权以下载并安装软件的任何消息都单击“否”，除非客户端用户确信该软件的创建者和他们查看的 Web 站点都可信。
 - 不理睬主动发送的商业电子邮件（垃圾邮件），特别是如果垃圾邮件要求用户单击某个按钮或超链接。
- 配置确保安全限制级别的 Web 浏览器设置。配置 Web 浏览器使之在安装 ActiveX 控件之前提示用户。要提高 Internet Explorer™ 的安全级别，请转到 **工具 > Internet 选项 > 安全**，然后将滑块移动到较高级别。如果此设置导致您要访问的 Web 站点出现问题，请单击 **站点...**，然后将要访问的站点添加到受信任的站点列表。
- 如果使用 Microsoft Outlook，请配置安全设置，以便 Outlook 不会自动下载 HTML 项，例如，在垃圾邮件中发送的图片。
- 不允许使用对等文件共享服务。间谍软件和其他灰色软件应用程序可能会伪装成用户可能要下载的其他类型的文件，例如，MP3 音乐文件。
- 定期检查客户端计算机上安装的软件，查找可能是间谍软件或其他灰色软件的应用程序。如果发现某个应用程序或文件虽未被防毒墙网络版检测为灰色软件，但您认为它是某种类型的灰色软件，请将其发送给趋势科技：

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

TrendLabs 将分析您提交的文件和应用程序。

- 通过最新的 Microsoft Patch 使 Windows 操作系统保持最新。请参阅 Microsoft Web 站点以了解详细信息。

扫描方法

在扫描安全风险时，防毒墙网络版客户端既可以使用传统扫描，也可以使用云安全扫描。

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

云安全扫描是基于云端的新一代端点保护解决方案。该解决方案的核心是利用存储在云端的威胁签名的一种高级扫描体系结构。

扫描方法对比

下表提供了这两种扫描方法之间的对比：

表 5-1. 传统扫描和云安全扫描之间的对比

比较的基础	传统扫描	云安全扫描
可用性	可在该版本及所有早期防毒墙网络版版本中使用	可在该防毒墙网络版版本中启动
扫描行为	传统客户端在本地计算机上执行扫描。	- 云安全客户端在本地计算机上执行扫描。 - 在扫描期间，如果客户端无法确定文件的风险，那么它将通过将扫描查询发送到云安全服务器来验证风险。 - 客户端使用高级过滤技术“缓存”扫描查询结果。由于客户端不需要将同一扫描查询发送到云安全服务器，因此扫描性能得到改善。 - 如果客户端无法在本地验证文件的风险，并且在多次尝试后，仍无法连接到任何云安全服务器： - 客户端会将文件标记为要进行验证。 - 客户端允许临时访问该文件。 - 当恢复与云安全服务器的连接后，会重新扫描所有的已标记文件。然后，对已经被确认为受感染的文件采取适当的扫描处理措施。
正在使用且已更新的组件	除云安全客户端病毒码外，所有组件在更新源上均可用	除病毒码和间谍软件主动监控特征码外，所有组件在更新源上均可用
典型更新源	防毒墙网络版服务器	防毒墙网络版服务器

从传统扫描切换到云安全扫描

如果将客户端从传统扫描切换到云安全扫描，请注意以下事项：

1. 产品使用授权

要使用云安全扫描，请确保已激活以下服务的使用授权，并确保这些使用授权没有过期：

- 防病毒
- Web 信誉和防间谍软件

2. 云安全服务器

云安全客户端连接到**云安全服务器**以发送扫描查询，并对照云安全云端病毒码验证文件的风险。客户端连接到的云安全服务器取决于客户端的位置。*内部*客户端连接到**本地**云安全服务器，而*外部*客户端连接到趋势科技 Internet 云安全服务器。

Internet 云安全服务器

如果连接到 Internet 云安全服务器要求代理服务器认证，请指定认证凭证。有关详细信息，请参阅第 9-40 页的**外部代理服务器**。

本地云安全服务器

防毒墙网络版提供了两种类型的本地云安全服务器。这两种服务器具有相同的功能。

- **集成型：**安装程序包括集成型云安全服务器，该服务器在安装防毒墙网络版服务器的同一计算机上安装。

如果在安装防毒墙网络版服务器期间安装了集成型服务器，请配置此服务器的更新设置，确保其具有最新的更新。有关更新此服务器的详细信息，请参阅第 4-19 页的**云安全服务器更新**。

如果希望客户端通过代理服务器连接到此服务器，请配置代理服务器设置。有关详细信息，请参阅第 9-39 页的**内部代理服务器**。

提示： 考虑禁用服务器计算机上的防毒墙网络版防火墙。启用时，防毒墙网络版防火墙可能会影响集成型服务器的性能。有关禁用防毒墙网络版防火墙的信息，请参阅第 7-19 页的**禁用防毒墙网络版防火墙**。

- **独立型：**独立型云安全服务器安装在 VMware 服务器上。独立型服务器具有单独的管理控制台，不通过防毒墙网络版 Web 控制台进行管理。

如果没有安装其中任一服务器，请先安装这些服务器，然后再将客户端切换到云安全扫描。有关重新激活集成型服务器以及安装和管理独立型服务器的信息，请参考《趋势科技云安全扫描防毒墙网络版入门指南》。

提示： 趋势科技建议安装多个服务器，以用于故障转移。无法连接到特定服务器的客户端将尝试连接到已安装的其他服务器。

3. 云安全服务器列表

将已安装的云安全服务器添加到云安全服务器列表。客户端参考该列表确定要连接到的云安全服务器。如果客户端无法连接到特定服务器，将会尝试连接到该列表上的其他服务器。

有关配置该列表的详细信息，请参阅第 5-14 页的[云安全扫描源](#)。

4. 计算机位置设置

防毒墙网络版包括位置感知功能，可识别客户端计算机的位置，确定客户端连接到 Internet 云安全服务器还是本地云安全服务器。这样可确保无论客户端处于什么位置，都可以受到保护。

要配置位置设置，请参阅第 9-2 页的[计算机位置](#)。

5. 防毒墙网络版服务器

确保客户端可以连接到防毒墙网络版服务器。仅通知联机客户端切换到云安全扫描。脱机客户端变为联机状态时会收到通知。当漫游客户端变为联机状态时，或者运行预设更新（如果客户端具有预设更新权限）时，会收到通知。

此外，验证防毒墙网络版服务器是否具有最新的组件，因为云安全客户端需要从服务器下载云安全客户端病毒码。要更新组件，请参阅第 4-11 页的[防毒墙网络版服务器更新](#)。

6. 其他趋势科技产品

如果安装了趋势科技™ 网络病毒墙 Enforcer:

- 安装 Hotfix (网络病毒墙 2500 为 Build 1047, 网络病毒墙 Enforcer 1200 为 Build 1013)。
- 将 OPSWAT 引擎更新到 2.5.1017 版, 使产品可以检测客户端的扫描方法。

7. 要切换的客户端数量

通过一次切换较少数量的客户端, 可以高效使用防毒墙网络版服务器和云安全服务器资源。在客户端更改其扫描方法的同时, 这些服务器可以执行其他关键任务。

8. 时间选择

首次切换到云安全扫描时, 客户端需要从防毒墙网络版服务器下载云安全客户端病毒码的完全版。云安全云端病毒码仅由云安全客户端使用。

请考虑在非高峰时段切换, 以确保下载过程可在短时间内完成。另请考虑在没有客户端预设为从服务器更新时进行切换。此外, 在客户端上暂时禁用“立即更新”, 并在客户端切换到云安全扫描后重新启用。

9. 客户端树设置

扫描方法是可在根级、域级或单个客户端级上设置的粒度设置。切换到云安全扫描时, 可以:

- 创建新的客户端树域, 并分配云安全扫描作为其扫描方法。移动到此域的任何客户端都将使用云安全扫描。

注意: 移动客户端时, 启用**将新域的设置应用到选定的客户端**设置。

- 选择一个域并将它配置为使用云安全扫描。属于该域的传统客户端将切换到云安全扫描。
- 从域中选择一个或多个传统客户端, 然后将它们切换到云安全扫描。

注意: 对域扫描方法进行的任何更改都将覆盖为单个客户端配置的扫描方法。

从云安全扫描切换到传统扫描

将客户端切换回传统扫描时，请考虑以下因素：

1. 要切换的客户端数量

通过一次切换较少数量的客户端，可以高效使用防毒墙网络版服务器和云安全服务器资源。在客户端更改其扫描方法的同时，这些服务器可以执行其他关键任务。

2. 时间选择

切换回传统扫描时，客户端很可能会从防毒墙网络版服务器下载病毒码和间谍软件主动监控特征码的完全版。这些特征码文件仅由传统客户端使用。

请考虑在非高峰时段切换，以确保下载过程可在短时间内完成。另请考虑在没有客户端预设为从服务器更新时进行切换。此外，在客户端上暂时禁用“立即更新”，并在客户端切换到云安全扫描后重新启用。

3. 客户端树设置

扫描方法是可在根级、域级或单个客户端级上设置的粒度设置。切换到传统扫描时，可以：

- 创建新的客户端树域，并分配传统扫描作为其扫描方法。移动到此域的任何客户端都将使用传统扫描。

注意： 移动客户端时，启用**将新域的设置应用到选定的客户端**设置。

- 选择一个域并将它配置为使用传统扫描。属于该域的云安全客户端将切换到传统扫描。
- 从域中选择一个或多个云安全客户端，然后将它们切换到传统扫描。

注意： 对域扫描方法进行的任何更改都将覆盖为单个客户端配置的扫描方法。

更改扫描方法：

导航路径：联网计算机 > 客户端管理 > 设置 > 扫描方法

1. 选择使用传统扫描还是云安全扫描。
2. 如果在客户端树上选择域或客户端，请单击**保存**将设置应用到域或客户端。如果选择根图标 ，则从下列选项进行选择：
 - **应用到全部客户端：**将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - **仅应用到将来的域：**仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

云安全扫描源

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。

客户端连接到的云安全服务器取决于客户端计算机的位置。内部客户端连接到本地云安全服务器（集成型或独立型），而外部客户端连接到 **Internet** 云安全服务器。有关配置位置设置的详细信息，请参阅第 9-2 页的 [计算机位置](#)。

可以配置客户端，使其在连接到 **Internet** 云安全服务器时使用代理服务器设置。有关详细信息，请参阅第 9-40 页的 [外部代理服务器](#)。

如果已安装本地云安全服务器，则在防毒墙网络版 Web 控制台上配置云安全服务器列表。如果内部客户端需要发送扫描查询，则它会从该列表中选取一个服务器。如果客户端无法连接到第一个服务器，则会选取列表上的另一个服务器，依此类推。

提示： 分配独立型云安全服务器作为主要扫描源，将集成型服务器作为后备。这减少了定向到托管防毒墙网络版服务器和集成型服务器的计算机的扫描查询流量。独立型服务器也可以处理更多的扫描查询。

配置云安全服务器列表：

导航路径：云安全扫描 > 扫描源 > 内部客户端

1. 选择客户端将使用**标准列表**还是**定制列表**。
2. 单击**通知所有客户端**。云安全客户端自动参考您所配置的列表。

标准列表

标准列表由所有的内部云安全客户端使用。可以配置客户端，使其在连接到列表上的云安全服务器时使用代理服务器设置。有关详细信息，请参阅第 9-39 页的**内部代理服务器**。

配置标准列表：

导航路径：云安全扫描 > 扫描源 > 内部客户端

1. 单击**标准列表**链接。
2. 在打开的窗口中，单击**添加**并指定云安全服务器的地址（以 URL 格式）。

获取云安全服务器地址：

- 对于集成型云安全服务器，打开防毒墙网络版 Web 控制台，并转至**云安全扫描 > 集成型服务器**。
- 对于独立型云安全服务器，打开独立型服务器的控制台，并转至“摘要”页。

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。

3. 单击**测试连接**，验证是否可以建立到服务器的连接。当测试连接成功时，单击**保存**。
4. 单击**云安全服务器地址**下的链接修改服务器的地址。
5. 要打开本地云安全服务器的控制台，请单击**启动控制台**。
 - 对于集成型云安全服务器，将显示服务器的配置窗口。

- 对于独立型云安全服务器和其他防毒墙网络版服务器的集成型云安全服务器，将显示控制台登录窗口。
- 6. 要删除某个条目，请选中该服务器对应的复选框并单击**删除**。
- 7. 要将列表导出到 .dat 文件，请单击**导出**，然后单击**保存**。
- 8. 如果已从其他服务器导出列表，并希望将该列表导入到此窗口，请单击**导入**并找到该 .dat 文件。该列表将加载到窗口中。
- 9. 在窗口的顶部，选择客户端是按服务器在列表中出现的顺序参考服务器，还是随机参考服务器。如果选择**顺序**，请使用**顺序**列下的箭头将服务器在列表中上下移动。
- 10. 单击**保存**。

定制列表

如果选择定制列表，请为定制列表指定 IP 地址范围。如果客户端的 IP 地址在此范围内，则该客户端使用定制列表。

配置定制列表：

导航路径：云安全扫描 > 扫描源 > 内部客户端

1. 单击**添加**。
2. 在打开的窗口中，指定以下内容：
 - IP 地址范围
 - 客户端将用来连接到本地云安全服务器的代理服务器设置
3. 指定云安全服务器的地址（以 URL 格式）。

获取云安全服务器地址：

- 对于集成型云安全服务器，打开防毒墙网络版 Web 控制台，并转至**云安全扫描 > 集成型服务器**。
- 对于独立型云安全服务器，打开独立型服务器的控制台，并转至“摘要”页。

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。

4. 单击**测试连接**，验证是否可以建立到服务器的连接。当测试连接成功时，单击**保存**。
5. 要打开本地云安全服务器的控制台，请单击**启动控制台**。
 - 对于集成型云安全服务器，将显示服务器的配置窗口。
 - 对于独立型云安全服务器和其他防毒墙网络版服务器的集成型云安全服务器，将显示控制台登录窗口。
6. 要删除某个条目，请单击**删除**下的图标。
7. 选择客户端是按服务器在列表中出现顺序参考服务器，还是随机参考服务器。如果选择**顺序**，请使用**顺序**列下的箭头将服务器在列表中上下移动。
8. 单击**保存**。
9. 返回到“云安全扫描源”窗口，选择是否在客户端无法连接到定制列表上的任何服务器时参考标准列表。
10. 要修改 IP 地址范围及其对应的定制列表，请单击 **IP 范围** 下的链接。
11. 要将定制列表导出到 .dat 文件，请单击**导出**，然后单击**保存**。
12. 如果已从其他服务器导出定制列表，并希望将这些列表导入到此窗口，请单击**导入**并找到 .dat 文件。列表将加载到窗口中。

扫描类型

防毒墙网络版提供了以下扫描类型来保护客户端计算机免受安全风险的危害：

表 5-2. 扫描类型

扫描类型	描述
实时扫描	在接收、打开、下载、复制或修改计算机上的文件时，会自动扫描该文件 有关详细信息，请参阅第 5-18 页的 实时扫描 。
手动扫描	用户启动的扫描，它会扫描用户请求的一个文件或一组文件 有关详细信息，请参阅第 5-20 页的 手动扫描 。
预设扫描	根据管理员或最终用户配置的时间表，自动扫描计算机上的文件 有关详细信息，请参阅第 5-21 页的 预设扫描 。
立即扫描	管理员启动的扫描，扫描一个或多个目标计算机上的文件 有关详细信息，请参阅第 5-22 页的 立即扫描 。

实时扫描

实时扫描是持续进行的扫描。每次接收、打开、下载、复制或修改文件时，实时扫描就会扫描文件以查找安全风险。如果防毒墙网络版未检测到安全风险，则文件会留在其原位置，用户可以继续访问该文件。如果防毒墙网络版检测到安全风险，会显示一条通知消息，显示受感染文件的名称和特定的安全风险。

注意： 要修改该通知消息，请打开 Web 控制台，并转至[通知 > 客户端用户通知](#)。

配置实时扫描设置并将其应用于一个或多个客户端和域，或者应用于服务器管理的所有客户端。

配置实时扫描设置：

导航路径：联网计算机 > 客户端管理 > 设置 > 实时扫描设置

1. 在**目标**选项卡上，选中复选框以启用对病毒/恶意软件和间谍软件/灰色软件的实时扫描。如果禁用病毒/恶意软件扫描，则间谍软件/灰色软件扫描也会被禁用。

注意： 在病毒爆发期间，不能禁用实时扫描（如果原来处于禁用状态，将自动启用），以防止病毒修改或删除客户端计算机上的文件和文件夹。

2. 配置以下扫描条件：
 - 将触发实时扫描的**用户对文件执行的活动**
 - **要扫描的文件**
 - **扫描设置**
3. 指定**扫描例外**。
4. 单击**处理措施**选项卡，配置防毒墙网络版对检测到的安全风险执行的**扫描处理措施**。
5. 如果在客户端树上选择域或客户端，请单击**保存**将设置应用到域或客户端。如果选择根图标 ，则从下列选项进行选择：
 - **应用到全部客户端：**将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - **仅应用到将来的域：**仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

手动扫描

手动扫描是按需扫描，用户在客户端控制台上运行该扫描后会立即启动。完成扫描所需时间取决于要扫描的文件的数量及客户端计算机的硬件资源。

配置手动扫描设置并将其应用于一个或多个客户端和域，或者应用于服务器管理的所有客户端。

配置手动扫描设置：

导航路径：联网计算机 > 客户端管理 > 设置 > 手动扫描设置

1. 在**目标**选项卡上，配置以下扫描条件：
 - **要扫描的文件**
 - **扫描设置**
 - **CPU 使用率**
2. 指定**扫描例外**。
3. 单击**处理措施**选项卡，配置防毒墙网络版对检测到的安全风险执行的**扫描处理措施**。
4. 如果在客户端树上选择域或客户端，请单击**保存**将设置应用到域或客户端。如果选择根图标 ，则从下列选项进行选择：
 - **应用到全部客户端**：将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

预设扫描

预设扫描按指定的日期和时间自动运行。使用预设扫描在客户端上使例行任务扫描自动化并提高扫描管理效率。

配置预设扫描设置并将其应用于一个或多个客户端和域，或者应用于服务器管理的所有客户端。

配置预设扫描设置：

导航路径：联网计算机 > 客户端管理 > 设置 > 预设扫描设置

1. 在**目标**选项卡上，选中复选框以启用对病毒/恶意软件和间谍软件/灰色软件的扫描。如果禁用病毒/恶意软件扫描，则间谍软件/灰色软件扫描也会被禁用。
2. 配置以下扫描条件：
 - **时间表**
 - **要扫描的文件**
 - **扫描设置**
 - **CPU 使用率**
3. 指定**扫描例外**。
4. 单击**处理措施**选项卡，配置防毒墙网络版对检测到的安全风险执行的**扫描处理措施**。
5. 如果在客户端树上选择域或客户端，请单击**保存**将设置应用到域或客户端。如果选择根图标 ，则从下列选项进行选择：
 - **应用到全部客户端**：将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

立即扫描

立即扫描由防毒墙网络版管理员通过 Web 控制台远程启动，并且可以将一台或多台客户端计算机作为目标。

配置立即扫描设置并将其应用于一个或多个客户端和域，或者应用于服务器管理的所有客户端。

配置立即扫描设置：

导航路径：联网计算机 > 客户端管理 > 设置 > 立即扫描设置

1. 在**目标**选项卡上，选中复选框以启用对病毒/恶意软件和间谍软件/灰色软件的扫描。如果禁用病毒/恶意软件扫描，则间谍软件/灰色软件扫描也会被禁用。
2. 配置以下扫描条件：
 - [要扫描的文件](#)
 - [扫描设置](#)
 - [CPU 使用率](#)
3. 指定[扫描例外](#)。
4. 单击**处理措施**选项卡，配置防毒墙网络版对检测到的安全风险执行的[扫描处理措施](#)。
5. 如果在客户端树上选择域或客户端，请单击**保存**将设置应用到域或客户端。如果选择根图标 ，则从下列选项进行选择：
 - **应用到全部客户端：**将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - **仅应用到将来的域：**仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

启动立即扫描

在怀疑受感染的计算机上启动立即扫描。

启动立即扫描：

导航路径：联网计算机 > 客户端管理 > 任务 > 立即扫描

“立即扫描”快捷方式（在主菜单顶部）

- 1. 要在启动扫描前更改预先配置的立即扫描设置，请单击**设置**。将打开“立即扫描设置”窗口。有关详细信息，请参阅第 5-22 页的[立即扫描](#)。
- 2. 在客户端树中选择将执行扫描的客户端，然后单击**启动立即扫描**。服务器将发送通知给该客户端。

注意： 如果未选择任何客户端，防毒墙网络版将自动通知客户端树中的所有客户端。

- 3. 检查通知状态并验证是否有未收到通知的客户端。
- 4. 单击**选择未通知的计算机**，然后单击**启动立即扫描**，立即向未通知的客户端重新发送通知。

示例：客户端总数：50

表 5-3. 未通知的客户端场景

客户端树选择	已通知的客户端（单击“启动立即扫描”后）	未通知的客户端
无（自动选择所有 50 个客户端）	50 个客户端中的 35 个	15 台客户端
手动选择（选择了 50 个客户端中的 45 个）	45 个客户端中的 40 个	5 台客户端与其他 5 台客户端未包括在手动选择中

- 5. 单击**停止通知**可提示防毒墙网络版停止通知当前正通知的客户端。已收到通知并处于扫描进程中的客户端暂不处理此命令。
- 6. 对于已处于扫描进程的客户端，请单击**停止立即扫描**以通知其停止扫描。

所有扫描类型的通用设置

对于每种扫描类型，配置以下三组设置：**扫描条件**、**扫描例外**和**扫描处理措施**。将这些设置部署到一个或多个客户端和域，或者部署到服务器管理的所有客户端。

扫描条件

使用文件属性（如文件类型和扩展名），指定特定扫描类型应该扫描的文件。此外，指定将触发扫描的条件。例如，配置实时扫描，使其在每个文件下载到计算机后对文件进行扫描。

用户对文件执行的活动

选择对文件执行哪些活动将触发实时扫描。从以下选项中选择：

- **创建/修改：**扫描引入计算机的新文件（例如，下载文件后）或正在修改的文件
- **检索：**在打开文件时对文件进行扫描
- **创建/修改和检索**

例如，如果选择第三个选项，则将扫描下载到计算机的新文件，如果未检测到安全风险，则该文件将留在其当前位置中。当用户打开同一文件时（如果用户修改了文件，则在保存修改之前），将会扫描该文件。

要扫描的文件

从以下选项中选择：

- **所有可扫描文件：**扫描所有文件
- **已由 IntelliScan 扫描的文件类型：**只扫描已知可能包含恶意代码的文件，包括用无害扩展名伪装的文件。有关详细信息，请参阅第 A-4 页的 *IntelliScan*。
- **带有特定扩展名的文件：**仅扫描其扩展名包括在文件扩展名列表中的文件。添加新扩展名或删除任何现有的扩展名。

扫描设置

选择以下一个或多个选项：

- **扫描网络驱动器：**在手动扫描或实时扫描期间扫描映射到客户端计算机的网络驱动器或文件夹。
- **扫描隐藏文件夹：**在手动扫描期间，允许防毒墙网络版在计算机上检测隐藏文件夹然后扫描它们。
- **扫描压缩文件：**允许防毒墙网络版最多扫描指定的压缩层数并跳过对任何多余层的扫描。例如，如果最大值为两层，而要扫描的压缩文件有六层，防毒墙网络版将扫描两层并跳过剩余四层。

注意： 防毒墙网络版将 Office Open XML 格式的 Microsoft Office 2007 文件视为压缩文件。Office Open XML（Office 2007 应用程序的文件格式）使用 ZIP 压缩技术。如果想要对使用这些应用程序创建的文件进行病毒/恶意软件扫描，需要启用压缩文件扫描功能。

- **在系统关闭期间扫描软盘：**在关闭计算机之前扫描所有软盘以查找引导区病毒。这可防止任何病毒/恶意软件在用户从磁盘重新启动计算机时执行。
- **启用 IntelliTrap：**检测并移除压缩可执行文件中的病毒/恶意软件。有关详细信息，请参阅第 A-4 页的 *IntelliTrap*。
- **扫描引导区：**在手动扫描、预设扫描和立即扫描期间，扫描客户端计算机硬盘的引导扇区以查找病毒/恶意软件。

CPU 使用率

在扫描一个文件后和扫描下一个文件前，防毒墙网络版客户端可以暂停。此设置在手动扫描、预设扫描和立即扫描期间使用。

从以下选项中选择：

- **高：**不间断连续扫描文件
- **中：**如果 CPU 使用率高于 50%，则在文件扫描之间暂停；如果等于或低于 50%，则不暂停
- **低：**如果 CPU 使用率高于 20%，则在文件扫描之间暂停；如果等于或低于 20%，则不暂停

如果选择“中”或“低”，则启动扫描并且 CPU 使用率在阈值（50% 或 20%）范围内时，防毒墙网络版在扫描之间将不暂停，从而缩短了扫描时间。防毒墙网络版在处理中会使用更多的 CPU 资源，但是由于 CPU 占用率是最佳的，因此计算机性能不会受到严重影响。当 CPU 使用率开始超过阈值时，防毒墙网络版将暂停以降低 CPU 使用率，当使用率再次处于阈值范围内时会停止暂停。

如果选择“高”，则防毒墙网络版不检查实际的 CPU 占用率，会一直扫描文件而不暂停。

时间表

配置预设扫描将运行的频率和时间。从以下选项中选择，然后选择开始时间：

- 每日一次
- 每周一次
- 每月一次

扫描例外

配置扫描例外可提高扫描性能并跳过对导致假警报的文件的扫描。运行特定扫描类型时，防毒墙网络版检查扫描例外列表，以确定计算机上的哪些文件将从病毒/恶意软件和间谍软件/灰色软件扫描中排除。

启用扫描例外时，防毒墙网络版在以下情况下将不扫描文件：

- 文件是在特定目录下找到的。
- 文件名与例外列表中的任何名称匹配。
- 文件扩展名与例外列表中的任何扩展名匹配。

扫描例外列表（目录）

防毒墙网络版不扫描在计算机特定目录下找到的所有文件。最多可以指定 250 个目录。

您可以使用**排除趋势科技产品的安装目录**选项。如果选择此选项，防毒墙网络版会自动从扫描中排除以下趋势科技产品的目录：

- 防毒墙群件版™ for Microsoft Exchange（除版本 7 之外的所有版本）如果您使用 V7，请将以下文件夹添加到例外列表中：
 - \Smex\Temp
 - \Smex\Storage
 - \Smex\ShareResPool
- ScanMail eManager™ 3.11、5.1、5.11 和 5.12
- ScanMail for Lotus Notes™ eManager NT
- 趋势科技™ 防毒墙邮件安全版
- InterScan Web 安全套件 (IWSS)
- InterScan Web Protect
- InterScan VirusWall 3.53
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan E-mail VirusWall
- InterScan NSAPI Plug-in
- InterScan eManager 3.5x

如果您有未包括在列表中的趋势科技产品，请将该产品的目录添加到扫描例外列表中。

此外，通过转至**联网计算机 > 全局客户端设置 > 扫描设置**，可将防毒墙网络版配置为排除 Microsoft Exchange 2000/2003 目录。如果使用 Microsoft Exchange 2007，则需将该目录手动添加到扫描例外列表。有关扫描例外的详细信息，请参考以下站点：

<http://technet.microsoft.com/en-us/library/bb332342.aspx>

扫描例外列表（文件）

如果一个文件的文件名与此例外列表中包括的任何名称匹配，则防毒墙网络版将不扫描该文件。如果要排除在计算机上特定位置找到的文件，请包括文件路径，如 C:\Temp\sample.jpg。

最多可以指定 250 个文件。

扫描例外列表（文件扩展名）

如果一个文件的文件扩展名与此例外列表中包括的任何扩展名匹配，则防毒墙网络版将不扫描该文件。最多可以指定 250 个文件扩展名。在扩展名之前不需要添加英文句点 (.)。

对于实时扫描，在指定扩展名时，可使用星号 (*) 作为通配符。例如，如果不希望扫描扩展名以 D 开头（例如，DOC、DOT 或 DAT）的所有文件，请键入 D*。

对于手动扫描、预设扫描和立即扫描，可使用问号 (?) 或星号 (*) 作为通配符。

将扫描例外设置应用至所有扫描类型

防毒墙网络版允许您为特定扫描类型配置扫描例外设置，然后将相同设置应用至所有其他扫描类型。例如：

1 月 1 日，防毒墙网络版管理员 Chris 发现客户端计算机上有大量的 JPG 文件，并了解到这些文件不会造成任何安全威胁。Chris 在手动扫描的例外文件列表中添加了 JPG，然后将此设置应用至所有扫描类型。实时扫描、立即扫描和预设扫描现在已设置为跳过对 .jpg 文件的扫描。

一星期后，Chris 从实时扫描的例外列表中移除了 JPG，但是没有将扫描例外设置应用至所有扫描类型。现在将扫描 JPG 文件，但只在实时扫描期间才会扫描。

扫描处理措施

指定特定扫描类型检测到安全风险时防毒墙网络版客户端执行的处理措施。防毒墙网络版对病毒/恶意软件和间谍软件/灰色软件采用两组不同的扫描处理措施。

病毒/恶意软件扫描处理措施

防毒墙网络版执行的扫描处理措施取决于病毒/恶意软件类型，以及检测出病毒/恶意软件的扫描类型。例如，如果在手动扫描（扫描类型）过程中，防毒墙网络版检测到特洛伊木马程序（病毒/恶意软件类型），它将清除（处理措施）受感染文件。

有关不同的病毒/恶意软件类型的信息，请参阅第 5-2 页的[病毒和恶意软件](#)。

扫描处理措施

以下是防毒墙网络版可以对病毒/恶意软件执行的处理措施：

删除

防毒墙网络版会删除受感染文件。

隔离

防毒墙网络版会更名受感染文件，然后将其移动到客户端计算机上的临时隔离目录（位于 <[客户端安装文件夹](#)>\Suspect 中）。

接下来，防毒墙网络版客户端将隔离文件发送到指定的隔离目录。有关详细信息，请参阅第 5-32 页的[隔离目录](#)。

缺省隔离目录位于防毒墙网络版服务器上，在 <[服务器安装文件夹](#)>\PCCSRV\ Virus 下。防毒墙网络版会对发送至该目录的隔离文件进行加密。

如果需要恢复任何隔离文件，请使用 VSEncrypt 工具。有关使用此工具的信息，请参阅第 8-25 页的[服务器调节程序](#)。

清除

防毒墙网络版会先清除受感染文件，然后才允许对文件进行完全访问。

如果文件无法清除，防毒墙网络版会执行第二项处理措施，它可以是以下处理措施之一：隔离、删除、更名和不予处理。要配置第二项处理措施，请转至**联网计算机 > 客户端管理 > 设置 > {扫描类型} > 处理措施**选项卡。

更名

防毒墙网络版将受感染文件的扩展名更改为“vir”。用户最初不能打开更名的文件，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

防毒墙网络版不会对受感染文件执行任何处理措施，但会在日志中记录病毒/恶意软件检测情况。文件将留在它所在位置。

只有当防毒墙网络版在手动扫描、预设扫描和立即扫描期间检测到任何类型的**病毒**（“**可能的病毒/恶意软件**”除外）时，才能使用该扫描处理措施。防毒墙网络版不能在实时扫描期间使用该扫描处理措施，因为如果在检测到打开或执行受感染文件的尝试时不执行处理措施，会执行病毒/恶意软件。实时扫描期间可以使用所有其他扫描处理措施。

对于“可能的病毒/恶意软件”类型，防毒墙网络版始终都不会对检测到的文件执行任何处理措施（无论扫描类型是什么），以减少**false positive（误报）**。如果经过进一步的分析确认，该可能的病毒/恶意软件确实存在安全风险，则会发布新特征码，以允许防毒墙网络版执行适当的扫描处理措施。如果该可能的病毒/恶意软件实际上无害，则不会再检测它。

例如：

防毒墙网络版在名为“123.exe”的文件中检测到“x_probable_virus”，它不会在检测时执行任何处理措施。之后，趋势科技确认“x_probable_virus”是特洛伊木马程序，并发布新的病毒码版本。在加载新的病毒码版本后，防毒墙网络版会将“x_probable_virus”检测为特洛伊木马程序，如果针对此类程序的处理措施为“清除”，则会清除“123.exe”。

拒绝访问

该扫描处理措施只能在实时扫描期间执行。如果防毒墙网络版检测到打开或执行受感染文件的企图，它会立即阻止该操作。

用户可以手动删除受感染文件。

扫描处理措施选项

配置扫描处理措施时，从以下选项中选择：

使用 **ActiveAction**

ActiveAction 是针对特定类型的病毒/恶意软件的一组预配置的扫描处理措施。如果您不确定对每种类型的病毒/恶意软件采取何种扫描处理措施，请使用 **ActiveAction**。使用 **ActiveAction**，不必在定制扫描处理措施上花费时间。

注意： **ActiveAction** 不可用于间谍软件/灰色软件扫描。

下表详细说明了 **ActiveAction** 如何处理各种类型的病毒/恶意软件：

表 5-4. 趋势科技建议对病毒/恶意软件执行的扫描处理措施

病毒/恶意软件类型	实时扫描		手动扫描/预设扫描/立即扫描	
	第一项处理措施	第二项处理措施	第一项处理措施	第二项处理措施
恶作剧程序	隔离	N/A	隔离	N/A
特洛伊木马程序	隔离	N/A	隔离	N/A
病毒	清除	隔离	清除	隔离
测试病毒	拒绝访问	N/A	不予处理	N/A
加壳软件	隔离	N/A	隔离	N/A
其他	清除	隔离	清除	隔离
可能的病毒/恶意软件	不予处理	N/A	不予处理	N/A

对所有病毒/恶意软件类型使用相同的处理措施：

如果希望对除可能的病毒/恶意软件之外的所有类型的病毒/恶意软件执行相同的处理措施，请选择此选项。对于**可能的病毒/恶意软件**，处理措施始终为“不予处理”。

对每种病毒/恶意软件类型使用特定的处理措施：

手动选择每种病毒/恶意软件类型的扫描处理措施。对于**可能的病毒/恶意软件**，处理措施不可配置，始终为“不予处理”。

如果选择“清除”作为第一项处理措施，请选择在清除不成功时防毒墙网络版执行的第二项处理措施。如果第一项处理措施不是“清除”，则第二项处理措施不可配置。

隔离目录

如果受感染文件的处理措施是“隔离”，则防毒墙网络版客户端将加密该文件，并将它移动到临时隔离文件夹（位于 <**客户端安装文件夹**>\SUSPECT 中），然后将该文件发送到指定的隔离目录。接受缺省隔离目录（位于防毒墙网络版服务器计算机上），或者通过键入 URL、UNC 路径或绝对文件路径格式的位置来指定其他目录。

注意： 如果将来需要访问加密的隔离文件，则可以恢复它们。有关详细信息，请参阅第 5-34 页的**恢复加密的文件**。

有关何时使用 URL、UNC 路径或绝对文件路径的指导，请参考下表：

表 5-5. 隔离目录

隔离目录	可接受的格式	示例	注意
防毒墙网络版服务器计算机上的目录	URL	http://<osceserver>	这是缺省目录。
	UNC 路径	\\<osceserver>\ofcscan\Virus	配置此目录的设置，如隔离文件夹的大小。有关详细信息，请参阅第 8-24 页的 隔离管理器 。

表 5-5. 隔离目录（续）

隔离目录	可接受的格式	示例	注意
另一台防毒墙网络版服务器计算机上的目录 （如果网络上具有其他防毒墙网络版服务器）	URL	http://<osceserver2>	确保客户端可以连接到此目录。如果指定了不正确的目录，则防毒墙网络版客户端会将隔离文件保留在 SUSPECT 文件夹中，直到指定了正确的隔离目录。在服务器的病毒/恶意软件日志中，扫描结果是“无法将隔离文件发送到指定的隔离文件夹中”。
	UNC 路径	\\<osceserver2>\ofcscan\Virus	
网络上的其他计算机	UNC 路径	\\<computer_name>\temp	如果使用 UNC 路径，请确保隔离目录文件夹共享给“所有人”组并且向该组分配了读写权限。
该客户端计算机上的其他目录	绝对路径	C:\temp	

清除前备份文件

如果防毒墙网络版设置为清除受感染文件，则它可以首先备份该文件。备份文件后，如果将来需要该文件，就可以恢复它。防毒墙网络版加密备份文件以防止文件被打开，然后将文件存储在 <客户端安装文件夹>\Backup 文件夹中。

要恢复加密的备份文件，请参阅第 5-34 页的 [恢复加密的文件](#)。

检测到病毒/恶意软件时显示通知消息

当防毒墙网络版在实时扫描和预设扫描期间检测到病毒/恶意软件时，它可以显示通知消息，以通知用户有关检测的信息。

要修改通知消息，请转至通知 > 客户端用户通知 > 病毒/恶意软件选项卡。

恢复加密的文件

为防止打开受感染文件，防毒墙网络版在以下实例中对文件进行加密：

- 隔离文件之前
- 在清除文件之前备份文件时

防毒墙网络版提供了一种工具，用于在需要从文件检索信息时解密和恢复该文件。防毒墙网络版可以解密和恢复以下文件：

表 5-6. 防毒墙网络版可以解密和恢复的文件

文件	描述
客户端计算机上的隔离文件	这些文件可在 <客户端安装文件夹>\SUSPECT\Backup 文件夹中找到，7 天后会自动清除它们。这些文件还会上传到防毒墙网络版服务器上的指定隔离目录。
指定隔离目录中的隔离文件	缺省情况下，此目录位于防毒墙网络版服务器计算机上。有关详细信息，请参阅第 5-32 页的 隔离目录 。
备份的加密文件	这些文件是防毒墙网络版能够清除的受感染文件的备份。它们可在 <客户端安装文件夹>\Backup 文件夹中找到。要恢复这些文件，用户需要将它们移动到 <客户端安装文件夹>\SUSPECT\Backup 文件夹。 仅当在联网计算机 > 客户端管理 > 设置 > {扫描类型} > 处理措施选项卡中选择清除前备份文件时，防毒墙网络版才在清除前备份和加密文件。

警告！ 恢复受感染文件可能将病毒/恶意软件传播到其他文件和计算机。在恢复文件之前，隔离受感染的计算机，并将此计算机上的重要文件移动到备份位置。

解密和恢复文件：

如果文件在防毒墙网络版客户端计算机上：

1. 打开命令提示符并导航到 **<客户端安装文件夹>**。
2. 键入以下命令运行 VSEncode.exe：

```
VSEncode.exe /u
```

此参数将打开一个窗口，其中包含在 **<客户端安装文件夹>**\SUSPECT\Backup 下找到的文件的列表。

3. 选择一个要恢复的文件，然后单击**恢复**。该工具一次只能恢复一个文件。
4. 在打开的窗口中，指定将文件恢复到的文件夹。
5. 单击**确定**。文件将恢复到指定的文件夹。

注意： 在恢复文件后，防毒墙网络版有可能立即再次扫描该文件并将它视为被感染文件。为防止扫描该文件，请将它添加到扫描例外列表。有关详细信息，请参阅第 5-26 页的**扫描例外**。

6. 恢复完文件后，单击**关闭**。

如果文件在防毒墙网络版服务器或定制隔离目录中：

1. 如果文件在防毒墙网络版服务器计算机中，请打开命令提示符并导航到 **<服务器安装文件夹>**\PCCSRV\Admin\Utility\VSEncrypt。

如果文件在定制隔离目录中，请导航到 **<服务器安装文件夹>**\PCCSRV\Admin\Utility，并将 **VSEncrypt** 文件夹复制到定制隔离目录所在的计算机。

2. 创建一个文本文件，然后键入想要加密或解密文件的完整路径。

例如，要恢复 C:\My Documents\Reports 中的文件，请在文本文件中键入 C:\My Documents\Reports*.*。

防毒墙网络版服务器计算机上的隔离文件可在 **<服务器安装文件夹>**\PCCSRV\Virus 下找到。

3. 用 INI 或 TXT 扩展名保存文本文件。例如，在 C: 驱动器上将它保存为 **ForEncryption.ini**。
4. 打开命令提示符并导航到 **VSEncrypt** 文件夹所在的目录。

5. 键入以下命令运行 VSEncode.exe:

```
VSEncode.exe /d /i <INI 或 TXT 文件的位置>
```

其中:

<INI 或 TXT 文件的位置> 是所创建的 INI 或 TXT 文件的路径 (例如, C:\ForEncryption.ini)。

6. 使用其他参数发出各种命令。

表 5-7. 恢复参数

参数	描述
无 (没有参数)	加密文件
/d	解密文件
/debug	创建调试日志并将其保存到计算机。在客户端计算机上, 调试日志 VSEncrypt.log 是在 <客户端安装文件夹> 中创建的。
/o	覆盖加密或解密的文件 (如果该文件已存在)
/f <文件名>	加密或解密单个文件
/nr	不恢复原始文件名
/v	显示有关该工具的信息
/u	启动该工具的用户界面
/r <目标文件夹>	将文件恢复到的文件夹
/s <原始文件名>	原始加密文件的文件名

例如, 键入 VSEncode [-d] [-debug] 可以解密 **Suspect** 文件夹中的文件, 并创建调试日志。加密或解密文件时, 防毒墙网络版将在同一文件夹中创建解密的或加密的文件。在解密或加密文件之前, 请确保文件未被锁定。

间谍软件/灰色软件扫描处理措施

防毒墙网络版执行的扫描处理措施取决于检测出间谍软件/灰色软件的扫描类型。虽然可以为每种病毒/恶意软件类型配置特定的处理措施，但是只能为所有类型的间谍软件/灰色软件配置一种处理措施（有关不同类型的间谍软件/灰色软件的信息，请参阅第 5-4 页的[间谍软件和灰色软件](#)）。例如，如果防毒墙网络版在手动扫描（扫描类型）期间检测到任何类型的间谍软件/灰色软件，它会清除（处理措施）受影响的系统资源。

扫描处理措施

以下是防毒墙网络版可以对间谍软件/灰色软件执行的处理措施：

清除

防毒墙网络版终止进程或删除注册表、文件、cookie 和快捷方式

清除间谍软件/灰色软件后，防毒墙网络版客户端会备份间谍软件/灰色软件数据，如果您认为访问某间谍软件/灰色软件是安全的，则可以将其恢复。有关详细信息，请参阅第 5-39 页的[间谍软件/灰色软件恢复](#)。

不予处理

防毒墙网络版不会对检测到的间谍软件/灰色软件组件执行任何处理措施，但会在日志中记录间谍软件/灰色软件检测的情况。此处理措施只能在手动扫描、预设扫描和立即扫描期间执行。在实时扫描期间，处理措施是“拒绝访问”。

如果检测到的间谍软件/灰色软件包括在允许列表中，防毒墙网络版将不会执行任何处理措施。有关详细信息，请参阅第 5-38 页的[间谍软件/灰色软件允许列表](#)。

拒绝访问

防毒墙网络版拒绝访问（复制、打开）检测到的间谍软件/灰色软件组件。此处理措施只能在实时扫描期间执行。在手动扫描、预设扫描和立即扫描期间，处理措施是“不予处理”。

检测到间谍软件/灰色软件时显示通知消息

当防毒墙网络版在实时扫描和预设扫描期间检测到间谍软件/灰色软件时，它可以显示通知消息，以通知用户有关检测的信息。

要修改通知消息，请转至**通知 > 客户端用户通知 > 间谍软件/灰色软件**选项卡。

间谍软件/灰色软件允许列表

防毒墙网络版提供了间谍软件/灰色软件的“允许”列表，该列表包含不希望视为间谍软件或灰色软件的文件或应用程序。在扫描期间检测到特定间谍软件/灰色软件时，防毒墙网络版将检查允许列表，如果它在允许列表中找到匹配项，则不执行任何处理措施。

将允许列表应用于一个或多个客户端和域，或者应用于服务器管理的所有客户端。允许列表应用于所有**扫描类型**，这意味着在手动扫描、实时扫描、预设扫描和立即扫描期间将使用相同的允许列表。

将已检测到的间谍软件/灰色软件添加至允许列表：

导航路径：联网计算机 > 客户端管理 > 日志 > 间谍软件/灰色软件日志 > 间谍软件/灰色软件日志条件 > 间谍软件/灰色软件日志 > 添加到“允许列表”

日志 > 联网计算机日志 > 安全风险 > 查看日志 > 间谍软件/灰色软件日志 > 间谍软件/灰色软件日志条件 > 间谍软件/灰色软件日志 > 添加到“允许列表”

1. 指定防毒墙网络版将把允许的间谍软件/灰色软件仅应用到选定的客户端计算机还是应用到特定域。
2. 单击**添加**。防毒墙网络版将间谍软件/灰色软件添加至以下位置找到的允许列表：**联网计算机 > 客户端管理 > 设置 > 间谍软件/灰色软件允许列表**。

注意： 防毒墙网络版的允许列表中最多可容纳 1024 种间谍软件/灰色软件。

管理间谍软件/灰色软件允许列表:

导航路径: 联网计算机 > 客户端管理 > 设置 > 间谍软件/灰色软件允许列表

1. 在**间谍软件/灰色软件名称**表中, 选择间谍软件/灰色软件名称。要选择多个名称, 请在选择时按住 **Ctrl** 键。

还可以在**搜索**文本框中键入关键字, 然后单击**搜索**。防毒墙网络版将刷新该表, 显示与该关键字匹配的名称。

2. 单击**添加**。名称将移动到**允许列表**表中。
3. 要移除允许列表中的名称, 请选择名称, 然后单击**移除**。要选择多个名称, 请在选择时按住 **Ctrl** 键。
4. 如果在客户端树上选择域或客户端, 请单击**保存**将设置应用到域或客户端。如果选择根图标 , 则从下列选项进行选择:
 - **应用到全部客户端**: 将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - **仅应用到将来的域**: 仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

间谍软件/灰色软件恢复

清除间谍软件/灰色软件后, 防毒墙网络版客户端备份间谍软件/灰色软件数据。如果您认为某数据无害, 请通知联机客户端恢复该备份数据。根据备份时间选择要恢复的间谍软件/灰色软件数据。

注意: 防毒墙网络版客户端用户无法启动间谍软件/灰色软件恢复, 也不会得到客户端能够恢复哪些备份数据的通知。

恢复间谍软件/灰色软件:

导航路径: 联网计算机 > 客户端管理 > 任务 > 间谍软件/灰色软件恢复

1. 要查看各个数据段要恢复的项, 请单击**查看**。将显示一个新窗口。单击**后退**返回到上一窗口。
2. 请选择要恢复的数据段。

注意： 对于步骤 1 和 2，可以选择将数据导出到逗号分隔值 (CSV) 文件。

3. 单击**恢复**。防毒墙网络版会通知您恢复的状态。检查间谍软件/灰色软件恢复日志来获取完整报告。有关详细信息，请参阅第 5-53 页的[间谍软件/灰色软件恢复日志](#)。

与扫描相关的权限

具有扫描权限的用户可更好地控制在其计算机上扫描文件的方式。

扫描权限允许用户执行以下任务：

- 配置手动扫描、预设扫描和实时扫描设置。有关详细信息，请参阅第 9-7 页的[扫描权限](#)。
- 推迟、停止或者跳过预设扫描。有关详细信息，请参阅第 9-8 页的[预设扫描权限](#)。
- 允许对 Microsoft Outlook 和 POP3 电子邮件进行扫描以查找病毒/恶意软件。有关详细信息，请参阅第 9-12 页的[邮件扫描权限](#)。

全局扫描设置

将全局扫描设置应用于客户端有许多种方法。

- 特定扫描设置可以应用于服务器管理的所有客户端，或仅应用于具有某些扫描权限的客户端。例如，如果配置推迟预设扫描持续时间，则只有具有推迟预设扫描权限的客户端将使用该设置。
- 特定扫描设置可以应用于所有扫描类型或仅应用于特定扫描类型。例如，在同时安装了防毒墙网络版服务器和客户端的计算机上，可以从扫描中排除防毒墙网络版服务器数据库。但是，此设置仅在实时扫描期间应用。
- 扫描病毒/恶意软件或间谍软件/灰色软件，或者同时扫描它们时，可以应用特定扫描设置。例如，评估模式仅在间谍软件/灰色软件扫描期间应用。

要查看全局扫描设置，请参阅第 9-19 页的[扫描设置](#)。

安全风险通知

防毒墙网络版附带有一组缺省通知消息，用于通知您、其他防毒墙网络版管理员和客户端用户检测到的安全风险或发生的任何爆发。可以修改这些消息来适应您的需求。

管理员通知设置

检测到安全风险或者发生爆发时，防毒墙网络版管理员可以通过以下方式收到通知：

- 电子邮件
- 寻呼机
- **SNMP Trap**
- Windows NT 事件日志

有关安全风险通知的详细信息，请参阅第 5-42 页的[针对管理员的安全风险通知](#)。有关爆发通知的详细信息，请参阅第 5-53 页的[爆发条件和通知](#)。

配置管理员通知设置，以允许防毒墙网络版通过电子邮件、寻呼机和 SNMP Trap 成功发送通知。

配置管理员通知设置：

导航路径：通知 > 管理员通知 > 常规设置

1. 在提供的文本框中指定信息。
2. 对于 **SMTP 和 SNMP Trap 服务器 IP 地址** 文本框，指定 IP 地址或计算机名称。
3. 请指定一个 1 到 65535 之间的端口号。
4. 对于 **寻呼机号码** 文本框，允许使用以下字符：

0 到 9

#

*

,

- 5. 请指定一个 1 到 16 之间的 COM 端口。
- 6. 请指定一个难以推测的团体名称。
- 7. 单击**保存**。

针对管理员的安全风险通知

配置防毒墙网络版在检测到安全风险时发送通知，或仅当对安全风险的处理措施不成功因此需要您的干预时才发送通知。

注意： 要配置在客户端计算机上显示的通知设置，请参阅第 5-43 页的[针对客户端用户的安全风险通知](#)。

为管理员配置安全风险通知：

导航路径：通知 > 管理员通知 > 标准通知

- 1. 在**条件**选项卡中，指定是在防毒墙网络版检测到病毒/恶意软件和间谍软件/灰色软件时发送通知，还是仅当对这些安全风险的处理措施不成功时发送通知。
- 2. 在**电子邮件、寻呼机、SNMP Trap 和 NT 事件日志**选项卡中：
 - a. 为病毒/恶意软件和间谍软件/灰色软件启用通知。
 - b. 对于电子邮件通知，指定电子邮件收件人，并且接受或修改缺省主题。
 - c. 接受或修改缺省通知消息。
 - d. 使用令牌变量表示**消息**和**主题**文本框中的数据。

表 5-8. 安全风险通知的令牌变量

变量	描述
病毒/恶意软件检测	
%v	病毒/恶意软件名称
%s	感染了病毒/恶意软件的计算机

表 5-8. 安全风险通知的令牌变量（续）

变量	描述
%i	计算机的 IP 地址
%m	计算机的域
%p	病毒/恶意软件的位置
%y	病毒/恶意软件的检测日期和时间
%a	对安全风险执行的处理措施
%n	登录到受感染计算机上的用户的名称
间谍软件/灰色软件检测	
%s	感染了间谍软件/灰色软件的计算机
%i	计算机的 IP 地址
%m	计算机的域
%y	间谍软件/灰色软件的检测日期和时间
%T	间谍软件/灰色软件和扫描结果

e. 单击**保存**。

针对客户端用户的安全风险通知

在实时扫描和预设扫描检测到病毒/恶意软件和间谍软件/灰色软件之后，防毒墙网络版可以立即在客户端计算机上显示通知消息。启用通知消息，并根据需要修改其内容。

启用通知消息：

导航路径：联网计算机 > 客户端管理 > 设置 > {实时或预设扫描设置} > “处理措施”选项卡

1. 选择在检测到病毒/恶意软件或间谍软件/灰色软件时显示通知消息。
2. 如果在客户端树上选择域或客户端，请单击**保存**将设置应用到域或客户端。如果选择根图标 ，则从下列选项进行选择：
 - **应用到全部客户端：**将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - **仅应用到将来的域：**仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

修改通知消息的内容：

导航路径：通知 > 客户端用户通知

1. 单击**病毒/恶意软件**选项卡或**间谍软件/灰色软件**选项卡。
2. 在提供的文本框中修改缺省消息。
3. 要在客户端用户的计算机上出现病毒/恶意软件时显示通知消息：
 - a. 选中**病毒/恶意软件感染源**下的复选框。
 - b. 指定发送通知的时间间隔。
 - c. 修改缺省通知消息（可选）。

提示： 仅当启用 Windows Messenger 服务时显示此通知消息。在“服务”窗口（**控制面板 > 管理工具 > 服务 > Messenger**）中检查此服务的状态。

4. 单击**保存**。

安全风险日志

防毒墙网络版在检测到病毒/恶意软件或间谍软件/灰色软件时以及恢复间谍软件/灰色软件时，会生成日志。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅第 8-16 页的 [管理日志](#)。

病毒/恶意软件日志

防毒墙网络版在检测到病毒和恶意软件时，会生成日志。

查看病毒/恶意软件日志：

导航路径：日志 > 联网计算机日志 > 安全风险 > 查看日志 > 病毒/恶意软件日志

联网计算机 > 客户端管理 > 日志 > 病毒/恶意软件日志

1. 指定日志条件，然后单击**显示日志**。
2. 查看日志。日志包含以下信息：
 - 病毒/恶意软件的检测日期和时间
 - 受感染计算机
 - 病毒/恶意软件名称
 - 感染源
 - 受感染文件
 - 检测到病毒/恶意软件的扫描类型
 - **病毒/恶意软件扫描结果**（是否成功执行了扫描处理措施）
 - 日志详细信息（单击**查看**可查看详细信息。）
3. 要将日志保存为逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。通常使用电子表格应用程序（例如 Microsoft Excel）来打开 CSV 文件。

病毒/恶意软件扫描结果

A. 如果扫描处理措施成功

如果防毒墙网络版能够执行配置的扫描处理措施，则显示以下结果：

已删除

- 第一项处理措施是“**删除**”，并且受感染文件已删除。
- 第一项处理措施是“**清除**”，但清除未成功。第二项处理措施是“删除”，并且受感染文件已删除。

已隔离

- 第一项处理措施是“**隔离**”，并且受感染文件已隔离。
- 第一项处理措施是“清除”，但清除未成功。第二项处理措施是“隔离”，并且受感染文件已隔离。

已清除

受感染文件已清除。

已更名

- 第一项处理措施是“**更名**”，并且受感染文件已更名。
- 第一项处理措施是“清除”，但清除未成功。第二项处理措施是“更名”，并且受感染文件已更名。

拒绝访问

- 第一项处理措施是“**拒绝访问**”，当用户尝试打开受感染文件时，对该文件的访问被拒绝。
- 第一项处理措施是“清除”，但清除未成功。第二项处理措施是“拒绝访问”，当用户尝试打开受感染文件时，对该文件的访问被拒绝。
- 在实时扫描期间检测到**可能的病毒/恶意软件**。
- 即使扫描处理措施为“清除”（第一项处理措施）和“隔离”（第二项处理措施），实时扫描也可能拒绝访问感染了引导区病毒的文件。这是因为尝试清除引导区病毒可能会损害受感染计算机的主引导记录 (MBR)。运行“手动扫描”以便防毒墙网络版可以清除或隔离该文件。

已略过

- 第一项处理措施是“**不予处理**”。防毒墙网络版未对受感染文件执行任何处理措施。
- 第一项处理措施是“清除”，但清除未成功。第二项处理措施是“不予处理”，因此防毒墙网络版未对受感染文件执行任何处理措施。

已略过一个潜在安全风险

仅当防毒墙网络版在手动扫描、预设扫描和立即扫描期间检测到“可能的病毒/恶意软件”时，才显示此扫描结果。当防毒墙网络版检测到可能的病毒/恶意软件时，它会自动将“不予处理”用作扫描处理措施。有关可能的病毒/恶意软件以及如何向趋势科技提交可疑文件以进行分析的信息，请参考趋势科技联机病毒百科全书上的以下页面。

http://threatinfo.trendmicro.com/vinfo/zh-cn/virusencyclo/default5.asp?vname=POSSIBLE_VIRUS

B. 如果扫描处理措施不成功

如果防毒墙网络版无法执行配置的扫描处理措施，则显示以下结果：

无法清除，隔离未完成

清除是第一项处理措施。隔离是第二项处理措施，两项处理措施都未成功。

*解决方法：*请参阅下面的“暂时无法隔离”。

无法清除，删除未完成

清除是第一项处理措施。删除是第二项处理措施，两项处理措施都未成功。

*解决方法：*请参阅下面的“暂时无法删除”。

无法清除，更名未完成

清除是第一项处理措施。更名是第二项处理措施，两项处理措施都未成功。

*解决方法：*请参阅下面的“暂时无法更名”。

暂时无法隔离/暂时无法更名

说明 1

受感染的文件可能由另外一个应用程序锁定、正在执行或位于 CD 中。防毒墙网络版将在应用程序释放文件或文件执行完毕后再隔离/更名该文件。

解决方案

对于 CD 中的受感染文件，请考虑不要使用该 CD，因为病毒可能会感染网络上的其他计算机。

说明 2

受感染的文件位于客户端计算机的 Temporary Internet Files 文件夹中。由于用户在浏览 Web 时计算机会下载文件，因此 Web 浏览器可能已锁定受感染文件。Web 浏览器释放文件后，防毒墙网络版将隔离/更名文件。

解决方法：无

暂时无法删除

说明 1

受感染文件可能包含在压缩文件中，并且**联网计算机 > 全局客户端设置**中的**清除/删除压缩文件中的受感染文件**设置已禁用。

解决方案

启用**清除/删除压缩文件中的受感染文件**选项。启用时，防毒墙网络版会对压缩文件进行解压缩，清除/删除压缩文件中的受感染文件，然后重新压缩文件。

注意： 启用此设置可能增加扫描期间的计算机资源占用，扫描可能要用更长时间才能完成。

说明 2

受感染的文件可能由另外一个应用程序锁定、正在执行或位于 CD 中。防毒墙网络版将在应用程序释放文件或文件执行完毕后再删除该文件。

解决方案

对于 CD 中的受感染文件，请考虑不要使用该 CD，因为病毒可能会感染网络上的其他计算机。

说明 3

受感染的文件位于客户端计算机的 Temporary Internet Files 文件夹中。由于用户在浏览 Web 时计算机会下载文件，因此 Web 浏览器可能已锁定受感染文件。Web 浏览器释放文件后，防毒墙网络版将删除文件。

解决方法： 无

无法将隔离文件发送到指定的隔离文件夹中

尽管防毒墙网络版成功将一个文件隔离在客户端计算机上的 \Suspect 文件夹中，但它无法将该文件发送到指定的隔离目录。

解决方案

确定检测到该病毒/恶意软件的扫描类型（手动扫描、实时扫描、预设扫描或立即扫描），然后检查**联网计算机 > 客户端管理 > 设置 > {扫描类型} > 处理措施**选项卡中指定的隔离目录。

如果隔离目录在防毒墙网络版服务器计算机或另一台防毒墙网络版服务器计算机上：

1. 检查客户端是否可以连接到该服务器。
2. 如果使用 URL 作为隔离目录格式：
 - a. 确保您在“http://”后指定的计算机名称正确。
 - b. 检查受感染文件的大小。如果其大小超出**管理 > 隔离管理器**中指定的最大文件大小，则调整设置以适应该文件。还可以执行其他处理措施，如删除文件。
 - c. 检查隔离目录文件夹的大小，并确定其是否超过了在**管理 > 隔离管理器**中指定的文件夹容量。调整该文件夹容量，或手动删除隔离目录中的文件。
3. 如果使用 UNC 路径，请确保隔离目录文件夹共享给“所有人”组并且向该组分配了读写权限。还应检查隔离目录文件夹是否存在以及 UNC 路径是否正确。

如果隔离目录在网络上的另一台计算机中（对于此情形只能使用 UNC 路径）：

1. 检查客户端是否可以连接到该计算机。
2. 请确保隔离目录文件夹共享给“所有人”组并且向该组分配了读写权限。
3. 检查隔离目录文件夹是否存在。
4. 检查 UNC 路径是否正确。

如果隔离目录在客户端计算机的其他目录中（对于此情形只能使用绝对路径），请检查隔离目录文件夹是否存在。

无法清除文件

说明 1

受感染文件可能包含在压缩文件中，并且**联网计算机 > 全局客户端设置**中的“清除/删除压缩文件中的受感染文件”设置已禁用。

解决方案

启用**清除/删除压缩文件中的受感染文件**选项。启用时，防毒墙网络版会对压缩文件进行解压缩，清除/删除压缩文件中的受感染文件，然后重新压缩文件。

注意： 启用此设置可能增加扫描期间的计算机资源占用，扫描可能要用更长时间才能完成。

说明 2

受感染的文件位于客户端计算机的 Temporary Internet Files 文件夹中。由于用户在浏览 Web 时计算机会下载文件，因此 Web 浏览器可能已锁定受感染文件。Web 浏览器释放文件后，防毒墙网络版将清除文件。

解决方法： 无

说明 3

文件可能无法清除。有关详细信息和解决方法，请参阅第 A-12 页的 ***Uncleanable File（非可清除文件）***。

间谍软件/灰色软件日志

防毒墙网络版在检测到间谍软件和灰色软件时，会生成日志。

查看间谍软件/灰色软件日志：

导航路径：日志 > 联网计算机日志 > 安全风险 > 查看日志 > 间谍软件/灰色软件日志

联网计算机 > 客户端管理 > 日志 > 间谍软件/灰色软件日志

1. 指定日志条件，然后单击**显示日志**。
2. 查看日志。日志包含以下信息：
 - 间谍软件/灰色软件的检测日期和时间
 - 受感染的计算机
 - 间谍软件/灰色软件名称
 - 检测到间谍软件/灰色软件的扫描类型
 - 有关**间谍软件/灰色软件扫描结果**的详细信息（是否成功执行了扫描处理措施）
 - 日志详细信息（单击**查看**可查看详细信息。）
3. 将您认为无害的间谍软件/灰色软件添加到**间谍软件/灰色软件允许列表**。
4. 要将日志保存为逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。通常使用电子表格应用程序（例如 Microsoft Excel）来打开 CSV 文件。

间谍软件/灰色软件扫描结果

A. 如果扫描处理措施成功

第一级别结果是**成功**，无需任何处理措施。第二级别结果如下：

已清除

防毒墙网络版已终止进程或删除注册表、文件、cookie 和快捷方式。

已略过

防毒墙网络版未执行任何处理措施，但记录了间谍软件/灰色软件的检测情况进行评估。

拒绝访问

防毒墙网络版拒绝对检测到的间谍软件/灰色软件组件的访问（复制、打开）。

B. 如果扫描处理措施不成功

第一级别结果是“需要进一步的处理措施”。第二级别的结果将至少具有以下消息其中之一：

清除间谍软件/灰色软件存在风险

如果间谍软件扫描引擎尝试清除任何单个文件夹并满足以下条件，则将显示此消息：

- 要清除的项超过 250MB。
- 操作系统将使用该文件夹中的文件。正常系统操作可能也需要该文件夹。
- 该文件夹为根目录（如 C: 或 F:）。

解决方法： 请联系您的技术支持提供商以寻求帮助。

间谍软件/灰色软件扫描已手动停止。请执行一次完全扫描。

用户在扫描完成前停止了扫描。

解决方法： 运行“手动扫描”并等待扫描完成。

间谍软件/灰色软件已清除，需要重新启动。请重新启动计算机。

防毒墙网络版已清除间谍软件/灰色软件组件，但需要重新启动计算机才能以完成该任务。

解决方法： 立即重新启动计算机。

无法清除间谍软件/灰色软件。

在 CD-ROM 或网络驱动器中检测到间谍软件/灰色软件。防毒墙网络版无法清除在这些位置检测到的间谍软件/灰色软件。

解决方法： 手动移除受感染文件。

无法识别间谍软件/灰色软件扫描结果。请与趋势科技技术支持部门联系。

新版本的间谍软件扫描引擎提供防毒墙网络版尚未配置为可处理的一种新扫描结果。

解决方法： 要获取确定新扫描结果的帮助，请联系技术支持提供商。

间谍软件/灰色软件恢复日志

清除间谍软件/灰色软件后，防毒墙网络版客户端备份间谍软件/灰色软件数据。如果您认为某数据无害，请通知联机客户端恢复该备份数据。在日志中提供了有关哪些间谍软件/灰色软件备份数据已恢复、受感染的计算机和恢复结果的信息。

查看间谍软件/灰色软件恢复日志：

导航路径：日志 > 联网计算机日志 > 间谍软件/灰色软件恢复

1. 检查**结果**列，查看防毒墙网络版是否已成功恢复间谍软件/灰色软件数据。
2. 要将日志保存为逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。通常使用电子表格应用程序（例如 Microsoft Excel）来打开 CSV 文件。

爆发防护

当特定时间段检测到的病毒/恶意软件或间谍软件/灰色软件事件超出某一阈值时，即发生爆发。在网络中响应和抑制爆发有几种方法，其中包括：

- 允许防毒墙网络版监控网络上是否有可疑活动
- 封闭关键客户端计算机端口和文件夹
- 向客户端发送爆发警报消息
- 清理受感染计算机

爆发条件和通知

按照检测到安全风险的次数和检测期限定义爆发。定义爆发条件后，配置防毒墙网络版，使其向您和其他防毒墙网络版管理员通知爆发情况，以便您可以立即响应。

您可以通过以下方式接收通知：

- 电子邮件
- 寻呼机

- **SNMP Trap**
- Windows NT 事件日志

配置管理员通知设置，以允许防毒墙网络版通过电子邮件、寻呼机和 SNMP Trap 成功发送通知。有关详细信息，请参阅第 5-41 页的 [管理员通知设置](#)。

配置爆发条件和通知：

导航路径：通知 > 管理员通知 > 爆发通知

通知 > 管理员通知 > 爆发通知 > “共享文件夹会话”链接

1. 在 **条件** 选项卡中，指定每个安全风险的检测次数和检测期限。

提示： 趋势科技建议接受此窗口中的缺省值。

防毒墙网络版将在超出指定的检测次数时发送一个通知消息。例如，如果指定为 100，则防毒墙网络版在检测到第 101 个病毒/恶意软件实例后发送通知。

2. 允许防毒墙网络版监控网络中是否存在防火墙违例和共享文件夹会话。在 **共享文件夹会话** 下，单击数字链接以查看含有共享文件夹的计算机和访问共享文件夹的计算机。
3. 在 **电子邮件、寻呼机、SNMP Trap** 和 **NT 事件日志** 选项卡中：
 - a. 为病毒/恶意软件和间谍软件/灰色软件检测启用通知。

提示： 防毒墙网络版仅通过电子邮件报告防火墙违例和共享文件夹会话爆发。

- b. 对于电子邮件通知，指定电子邮件收件人，并接受或修改缺省电子邮件主题。（可选）选择要包括在电子邮件中的其他病毒/恶意软件和间谍软件/灰色软件信息。可以包括客户端/域名称、安全风险名称、检测的日期和时间、路径和受感染文件以及扫描结果。
- c. 接受或修改缺省通知消息。

d. 使用令牌变量表示消息和主题文本框中的数据。

表 5-9. 爆发通知的令牌变量

变量	描述
病毒/恶意软件爆发	
%CV	检测出的病毒/恶意软件的总数
%CC	感染了病毒/恶意软件的计算机总数
间谍软件/灰色软件爆发	
%CV	检测出的间谍软件/灰色软件的总数
%CC	感染了间谍软件/灰色软件的计算机总数
防火墙违例爆发	
%A	超出的日志类型
%C	防火墙违例日志数
%T	防火墙违例日志的累计时长
共享文件夹会话爆发	
%S	共享文件夹会话数
%T	共享文件夹会话的累计时长
%M	时间段，单位为分钟

4. 单击保存。

爆发阻止

发生爆发时，执行爆发阻止措施以响应和抑制爆发。配置阻止设置时需小心谨慎，因为不正确的配置可能导致不可预见的网络问题。

配置和激活爆发阻止设置：

导航路径：联网计算机 > 爆发阻止 > 启动爆发阻止

1. 执行以下任一爆发阻止策略：
 - [限制/拒绝访问共享文件夹](#)
 - [封闭端口](#)
 - [拒绝对文件和文件夹的写访问](#)
2. 选择爆发阻止保持有效的小时数。缺省值为 48 小时。可以在爆发阻止到期前手动恢复网络设置。

警告！ 不要允许爆发阻止无限期有效。要无限期阻止或拒绝对特定文件、文件夹或端口的访问，请直接修改计算机和网络设置，而不要使用防毒墙网络版来处理。

3. 接受或修改缺省客户端通知消息。

注意： 要配置防毒墙网络版以便使其在发生爆发时通知您，请转至[通知 > 管理员通知 > 爆发通知](#)。

4. 单击**启动爆发阻止**。所选的爆发阻止措施将显示在一个新窗口中。
5. 返回到客户端树中，检查 **OPP** 列。应用爆发阻止措施的计算机上将显示一个复选标记。

防毒墙网络版在系统事件日志中记录以下事件：

- 服务器事件（启动爆发阻止及通知客户端启用爆发阻止）
- 客户端事件（启用爆发阻止）

爆发阻止策略

发生爆发时，执行以下任一策略：

- **限制/拒绝访问共享文件夹**
- **封闭端口**
- **拒绝对文件和文件夹的写访问**

限制/拒绝访问共享文件夹

在爆发期间，限制或拒绝对网络上共享文件夹的访问，以阻止安全风险通过共享文件夹传播。

此策略生效时，用户仍然可以共享文件夹，但是此策略将不会应用于新共享的文件夹。因此，通知用户不要在爆发期间共享文件夹，或者再次部署策略以便将策略应用于新共享的文件夹。

限制/拒绝访问共享文件夹：

导航路径：联网计算机 > 爆发阻止 > 启动爆发阻止 > 限制/拒绝访问共享文件夹

1. 从以下选项中选择：

- **只读访问权限：**限制访问共享文件夹
- **拒绝完全访问**

注意： 只读访问设置不会应用至已经配置为拒绝完全访问的共享文件夹。

2. 单击**保存**。将再次显示“爆发阻止设置”窗口。

封闭端口

在爆发期间，封闭易受攻击的端口，病毒/恶意软件可能使用这些端口来获取客户端计算机的访问权限。

警告！ 仔细配置爆发阻止设置。封闭使用中的端口会导致基于这些端口的网络服务不可用。例如，如果封闭 **trusted port（可信端口）**，防毒墙网络版将无法在爆发期间与客户端通信。

封闭易受攻击的端口：

导航路径：联网计算机 > 爆发阻止 > 启动爆发阻止 > 封闭端口

1. 选择是否封闭可信端口。
2. 在**已封闭端口**列下选择要封闭的端口。
 - a. 如果表中没有端口，则单击**添加**。在打开的窗口中，选择要封闭的端口，然后单击**保存**。
 - **所有端口（包括 ICMP）**：封闭除可信端口之外的所有端口。如果还想封闭可信端口，则选中上一窗口中的“封闭可信端口”复选框。
 - **常用端口**：至少选择一个端口号，以便防毒墙网络版可以保存端口封闭设置。
 - **特洛伊木马程序常用的端口**：封闭特洛伊木马程序常用的端口。有关详细信息，请参阅第 A-10 页的 **Trojan Port（特洛伊木马端口）**。
 - **介于 1—65535 之间的端口号或端口范围**：可根据需要指定要阻止的网络通信方向和一些注释，例如，封闭指定端口的原因。
 - **Ping 协议（拒绝 ICMP）**：如果只想阻止 ICMP 数据包（例如，ping 请求），则单击。
 - b. 要编辑已封闭端口的设置，请单击端口号。
 - c. 在打开的窗口中，修改设置，然后单击**保存**。
 - d. 要从列表中移除端口，请选中端口号旁的复选框，然后单击**删除**。
3. 单击**保存**。将再次显示“爆发阻止设置”窗口。

拒绝对文件和文件夹的写访问

病毒/恶意软件可能会修改或删除宿主计算机上的文件和文件夹。在爆发期间，配置防毒墙网络版，使其阻止病毒/恶意软件修改或删除客户端计算机上的文件和文件夹。

拒绝对文件和文件夹的写访问：

导航路径：联网计算机 > 爆发阻止 > 启动爆发阻止 > 拒绝对文件和文件夹的写访问

1. 键入目录路径。键入要保护的目录路径后，单击**添加**。

注意： 键入目录的绝对路径，而不是虚拟路径。

2. 指定要在受保护的目录中保护的文件。选择所有文件，或根据特定文件扩展名选择文件。对于文件扩展名，可以指定不在列表中的扩展名，在文本框中键入该扩展名，然后单击**添加**。
3. 要保护特定文件，在**要保护的文件**下，键入完整文件名，然后单击**添加**。
4. 单击**保存**。将再次显示“爆发阻止设置”窗口。

禁用爆发阻止

确信已抑制爆发并且防毒墙网络版已清除或隔离所有受感染的文件时，通过禁用爆发阻止将网络设置恢复正常。

手动禁用爆发阻止：

导航路径：联网计算机 > 爆发阻止 > 恢复设置

1. 要通知用户爆发已结束，请选择**恢复原始设置后通知客户端用户**。
2. 接受或修改缺省客户端通知消息。
3. 单击**恢复设置**。

注意： 如果未手动恢复网络设置，则防毒墙网络版将会在“爆发阻止设置”窗口上的 __ 小时后自动将网络设置恢复正常中指定的小时数以后自动恢复这些设置。缺省设置为 48 小时。

防毒墙网络版在系统事件日志中记录以下事件：

- 服务器事件（启动爆发阻止及通知客户端启用爆发阻止）
 - 客户端事件（启用爆发阻止）
4. 禁用爆发阻止后，请扫描联网计算机上是否有安全风险以确保抑制了爆发。

设备控制

防毒墙网络版提供了设备控制功能，用于控制对连接到计算机的外部存储设备和网络资源的访问。设备控制有助于防止数据丢失和泄露，与文件扫描组合使用时可帮助防御安全风险。

设备控制仅在运行 x86 类型平台的计算机上可用。

管理对外部设备的访问：

导航路径：联网计算机 > 客户端管理 > 设置 > 设备控制

1. 选中用于启用设备控制的复选框。
2. 选择阻止还是允许连接到计算机的 USB 设备的自动执行功能 (autorun.inf)。
3. 选择每种设备类型的权限。

表 5-10. 设备权限

权限	设备上的文件	传入文件
完全访问	允许的操作：复制、移动、 打开、保存、删除、执行	允许的操作：保存、移动、 复制 这意味着可以将文件保存、 移动和复制到设备。
仅读和写	允许的操作：复制、移动、 打开、保存、删除 阻止的操作：执行	允许的操作：保存、移动、 复制

表 5-10. 设备权限（续）

权限	设备上的文件	传入文件
仅读和执行	允许的操作：复制、打开、执行 阻止的操作：保存、移动、删除	阻止的操作：保存、移动、复制
只读	允许的操作：复制、打开 阻止的操作：保存、移动、删除、执行	阻止的操作：保存、移动、复制
不能访问	自动阻止访问设备或网络资源的任何尝试。	阻止的操作：保存、移动、复制

注意： 防毒墙网络版中的扫描功能对设备权限起补充作用，并有可能覆盖这些权限。例如，如果权限允许打开某文件，但是防毒墙网络版检测到该文件感染了恶意软件，则将该文件执行特定的扫描处理措施，以清除恶意软件。如果扫描处理措施是“清除”，则文件将在清除恶意软件后打开。但是，如果扫描处理措施是“删除”，该文件将会被删除。

- 选择防毒墙网络版检测到未授权的设备访问（包括防毒墙网络版阻止的所有操作）时，是否在客户端计算机上显示通知消息。
- 如果在客户端树上选择域或客户端，请单击**保存**将设置应用到域或客户端。如果选择根图标，则从下列选项进行选择：
 - 应用到全部客户端：**将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - 仅应用到将来的域：**仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

设备控制日志

客户端记录未经授权设备访问实例，并将日志发送到服务器。持续运行的客户端聚集日志，并在 24 小时后发送这些日志。重新启动的客户端检查上次向服务器发送日志的时间。如果经过的时间超过 24 个小时，则客户端会立即发送日志。

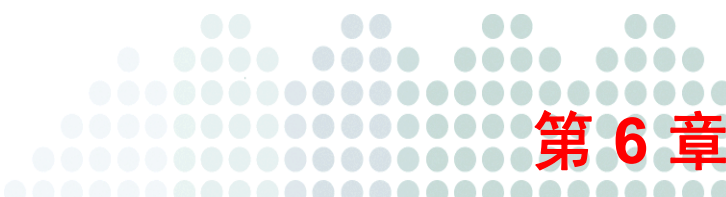
要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅第 8-16 页的 [管理日志](#)。

查看设备控制日志：

导航路径：日志 > 联网计算机日志 > 安全风险 > 查看日志 > 设备控制日志

联网计算机 > 客户端管理 > 日志 > 设备控制日志

1. 指定日志条件，然后单击**显示日志**。
2. 查看日志。日志包含以下信息：
 - 检测到未经授权访问的日期/时间
 - 连接外部设备或映射网络资源的计算机
 - 访问的设备类型或网络资源
 - 目标，即访问的设备或网络资源中的项
 - 访问者，它指定发起访问的位置
 - 对目标设置的权限



第 6 章

保护计算机免受基于 Web 的威胁

本章主题：

- 第 6-2 页的关于 Web 威胁
- 第 6-2 页的 Web 信誉
- 第 6-3 页的位置感知
- 第 6-3 页的 Web 信誉策略
- 第 6-5 页的 Web 信誉允许的 URL 列表
- 第 6-5 页的 Web 信誉的代理服务器
- 第 6-6 页的客户端用户的 Web 威胁通知
- 第 6-7 页的 Web 信誉日志

关于 Web 威胁

Web 威胁包括一系列广泛源自于 Internet 的威胁。Web 威胁的方式非常复杂，使用了各种文件和技术组合，而非单一的文件或方法。例如，Web 威胁创建者不断更改使用的版本或变种。由于 Web 威胁处于 Web 站点的固定位置，而非在受感染计算机上，因此 Web 威胁创建者会不断修改其代码以免被检测到。

近年来，曾经作为黑客、病毒编写者、垃圾邮件制造者和间谍软件制作者出现的个人现在统称为网络罪犯。Web 威胁可帮助这些人实现以下两个目标之一。一个目标是窃取信息以便后续销售。由此引起的后果是以身份丢失的形式泄漏机密信息。受感染计算机还可能成为传递 **phish attack（网络钓鱼攻击）** 或其他信息捕捉活动的带毒站点。除了以上影响之外，此威胁还可能腐蚀对 Web 商务的信心，从而破坏 Internet 事务所需的信任。第二个目标是劫持用户的 CPU，并将其用作开展牟利活动的工具。这些活动包括发送垃圾邮件或者以分布式拒绝服务攻击或点击付费活动的形式进行敲诈勒索。

Web 信誉

防毒墙网络版利用趋势科技的广泛 Web 安全数据库来检查用户尝试访问的 Web 站点的信誉。Web 站点的信誉与计算机上实施的特定 Web 信誉策略有关。根据正在使用的策略，防毒墙网络版将阻止或者允许对 Web 站点的访问。策略根据客户端的位置实施。

位置感知

在很多组织中，员工既使用台式机也使用便携式计算机来执行任务。由于便携式计算机连接到多个网络，而且员工可能会将其带到组织所在建筑物之外，因此防毒墙网络版需要扩展防护范围，这样即使这些便携式计算机从网络断开也能对其进行保护。**Web 信誉策略**可确保无论客户端计算机在什么位置都能受到保护。

客户端的位置（“内部”或“外部”）控制应用到计算机的策略。需要指定该位置是基于客户端计算机的网关 IP 地址，还是基于客户端与防毒墙网络版服务器或任何参考服务器的连接状态。

要配置位置感知设置，请参阅第 9-2 页的 **计算机位置**。

Web 信誉策略

Web 信誉策略控制防毒墙网络版是阻止还是允许对 Web 站点的访问。为确定要使用的适当策略，防毒墙网络版会检查客户端的位置。位置基于客户端计算机的网关 IP 地址或者客户端与防毒墙网络版服务器或任何参考服务器的连接状态。

如果有以下情形，客户端的位置为“内部”：

- 客户端的网关 IP 地址与在**计算机位置**窗口上指定的任意网关 IP 地址相匹配。
- 如果客户端可以连接到防毒墙网络版服务器或任意**参考服务器**。

否则，客户端的位置位于“外部”。

配置 Web 信誉策略：

导航路径：联网计算机 > 客户端管理 > 设置 > WEB 信誉设置

1. 配置**外部客户端**和**内部客户端**的策略。
2. 选中相应复选框以启用/禁用 Web 信誉策略。

提示： 如果已将趋势科技产品与 Web 信誉功能（如趋势科技网关安全设备 (IGSA)）一起使用，则趋势科技建议对内部客户端禁用 Web 信誉。

3. 从可用的 Web 信誉安全级别中选择：高、中或低

安全级别确定防毒墙网络版是允许还是阻止访问 URL。例如，如果安全级别设置为“低”，则防毒墙网络版将仅阻止已知是“Web 威胁”的 URL。随着安全级别设置的增高，Web 威胁检测率会提高，但误报的可能性也会增加。

4. 要提交 Web 信誉反馈，请使用提供的 URL。该 URL 将打开趋势科技 Web 信誉查询系统。
5. 选择是否允许防毒墙网络版客户端向服务器发送 **Web 信誉日志**。如果要分析防毒墙网络版正在阻止的 URL 并要对您认为可以安全访问的 URL 采取相应的操作，则允许客户端发送日志。
6. 单击**保存**。

Web 信誉允许的 URL 列表

允许的 URL 会绕过 Web 信誉策略。即使将 Web 信誉策略设置为阻止这些 URL，防毒墙网络版也不会阻止它们。将认为是安全的 URL 添加到允许的 URL 列表。

配置允许的 URL 列表：

导航路径：联网计算机 > 全局客户端设置

1. 转至“Web 信誉允许的 URL 列表”部分并单击该列表下面的链接。
2. 选择是为外部客户端配置列表还是为内部客户端配置列表。
3. 在文本框中指定 URL。
4. 选择是允许 URL 子站点还是仅 Web 页面。如果 URL 为 `www.example.com/update`，则防毒墙网络版会允许此 URL 下的所有页面，但将不会允许 `www.example.com`。
5. 单击**添加**。
重复步骤 3 到步骤 5，直到列表中包括希望允许的所有 URL 为止。
6. 单击**保存**。

Web 信誉的代理服务器

如果已将代理服务器设置为处理贵组织中的 HTTP 通信，并且要求在进行 Web 访问之前进行认证，请指定代理服务器认证凭证。当防毒墙网络版连接到趋势科技信誉服务器以确定用户尝试访问的 Web 站点是否安全时，需要使用这些凭证。

此防毒墙网络版版本仅支持一组认证凭证。

要配置代理服务器设置，请参阅第 9-40 页的[外部代理服务器](#)。

客户端用户的 Web 威胁通知

防毒墙网络版在阻止违反 Web 信誉策略的 URL 后，可以立即在客户端计算机上显示一条通知消息。需要启用通知消息并可选择修改通知消息的内容。

启用通知消息：

导航路径：联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > “其他设置”选项卡

1. 在 **Web 信誉设置** 下选择阻止 Web 站点时显示通知。
2. 如果在客户端树上选择域或客户端，请单击**保存**将设置应用到域或客户端。
如果选择根图标 ，则从下列选项进行选择：
 - **应用到全部客户端：**将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - **仅应用到将来的域：**仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

修改通知消息的内容：

导航路径：通知 > 客户端用户通知 > “WEB 信誉策略违例”选项卡

1. 在提供的文本框中修改缺省消息。

注意： 在客户端计算机上显示该通知消息之后，会在浏览器中显示另一条消息。该消息通知用户，如果他们认为该 URL 可以安全访问，则其将该 URL 报告给防毒墙网络版管理员。

2. 单击**保存**。

Web 信誉日志

配置内部客户端和外部客户端，以将 Web 信誉日志发送给服务器。如果想要分析防毒墙网络版阻止的 URL 并对您认为可以安全访问的 URL 采取适当处理措施，请执行此操作。

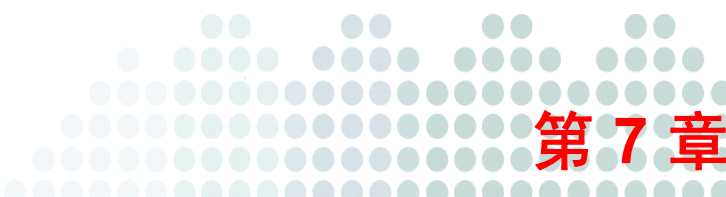
要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅第 8-16 页的 [管理日志](#)。

查看 Web 信誉日志：

导航路径：日志 > 联网计算机日志 > 安全风险 > 查看日志 > WEB 信誉日志

联网计算机 > 客户端管理 > 日志 > WEB 信誉日志

1. 指定日志条件，然后单击**显示日志**。
2. 查看日志。日志包含以下信息：
 - 防毒墙网络版阻止 URL 的日期/时间
 - 用户访问 URL 的计算机
 - 已阻止的 URL
 - URL 的风险等级
 - 指向趋势科技 Web 信誉查询系统的链接，该系统提供有关已阻止的 URL 的详细信息
3. 要将日志保存为逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。通常使用电子表格应用程序（例如 Microsoft Excel）来打开 CSV 文件。



第 7 章

使用防毒墙网络版防火墙

本章主题：

- 第 7-2 页的[关于防毒墙网络版防火墙](#)
- 第 7-4 页的[防火墙策略和概要文件](#)
- 第 7-15 页的[防火墙权限](#)
- 第 7-16 页的[向客户端用户发送的防火墙违例通知](#)
- 第 7-17 页的[防火墙日志](#)
- 第 7-18 页的[测试防毒墙网络版防火墙](#)
- 第 7-19 页的[禁用防毒墙网络版防火墙](#)

关于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端。通过中央管理控制台，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。

防毒墙网络版防火墙包括以下主要功能和优点：

网络通信过滤

防毒墙网络版防火墙过滤所有传入和传出的网络通信，可根据以下标准阻止某些类型的网络通信：

- 方向（入站/出站）
- 协议 (TCP/UDP/ICMP)
- 目标端口
- 源计算机和目标计算机

扫描网络病毒

防毒墙网络版防火墙还会在每个数据包中查找是否有网络病毒。有关详细信息，请参阅第 5-4 页的[网络病毒](#)。

可定制的概要文件和策略

防毒墙网络版防火墙让您配置策略以阻止或允许指定类型的网络通信。将策略分配到一个或多个概要文件，然后可将这些概要文件部署到指定的防毒墙网络版客户端。这提供了一种高度定制的为客户端组织和配置防火墙设置的方法。

基于状态的检查

防毒墙网络版防火墙是基于状态进行检查的防火墙；它监视到客户端的所有连接并记住所有连接状态。它可以确定任何连接中的特定条件，预测应采取的处理措施及检测正常连接中是否存在中断。因此，有效使用防火墙不仅涉及创建概要文件和策略，而且涉及分析连接和过滤通过防火墙的数据包。

入侵检测系统

防毒墙网络版防火墙还包括入侵检测系统 (IDS)。启用后，IDS 可以帮助确定网络数据包中可能表示会攻击客户端的特征码。防毒墙网络版防火墙可以帮助阻止以下众所周知的入侵：

- **Too Big Fragment: Denial of Service Attack（拒绝服务攻击）**，黑客将特大的 TCP/UDP 数据包定向到目标计算机。这会导致计算机缓存溢出，从而使计算机死机或重新启动。
- **Ping of Death**：拒绝服务攻击，黑客将特大的 ICMP 数据包定向到目标计算机。这会导致计算机缓存溢出，从而使计算机死机或重新启动。
- **Conflicted ARP**：一种攻击类型，黑客会向计算机发送带有相同源和目标 IP 地址的地址解析协议 (ARP) 请求。目标计算机将持续向自身发送 ARP 响应（其 MAC 地址），从而导致其死机或崩溃。
- **SYN Flood**：拒绝服务攻击，程序会将多个 TCP 同步 (SYN) 数据包发送到计算机，从而导致计算机持续发送同步应答 (SYN/ACK) 响应。这会耗尽计算机的内存，并最终导致计算机崩溃。
- **Overlapping Fragment**：与 Teardrop 攻击相似，这种拒绝服务攻击会向计算机发送重叠的 TCP 碎片。会覆盖第一个 TCP 碎片中的头信息，并有可能通过防火墙。然后防火墙可能会允许带有恶意代码的后续碎片通过，到达目标计算机。
- **Teardrop**：与 Overlapping Fragment 攻击相似，这种拒绝服务攻击涉及 IP 碎片。第二个或后面的 IP 碎片中的混淆偏移值会导致接收计算机的操作系统在尝试重新整理碎片时崩溃。
- **Tiny Fragment 攻击**：一种攻击类型，用一个很小的 TCP 碎片将第一个 TCP 数据包的头信息压到下一个碎片中。这可导致过滤网络通信的路由器忽略可能包含恶意数据的后续碎片。
- **Fragmented IGMP**：一种拒绝服务攻击，向目标计算机发送被分割的 IGMP 数据包，导致无法正确处理 IGMP 数据包。这会使计算机死机或变慢。
- **LAND Attack**：一种攻击类型，向计算机发送带有相同源地址和目标地址的 IP 同步 (SYN) 数据包，导致计算机向自身发送同步应答 (SYN/ACK) 响应。这会使计算机死机或变慢。

防火墙违例爆发监控

防火墙违例超出特定阈值（可能意味着发生攻击）时，防毒墙网络版防火墙会向指定收件人发送定制的通知消息。

客户端防火墙权限

授予客户端用户在防毒墙网络版客户端控制台上查看他们的防火墙设置的权限。还授予用户启用或禁用防火墙、入侵检测系统和防火墙违例通知消息的权限。

防火墙策略和概要文件

防毒墙网络版防火墙使用策略和概要文件来组织和定制保护联网计算机的方法。

提示： 在同一台计算机上安装多个防火墙可能会产生意外的结果。请考虑在部署和启用防毒墙网络版防火墙前先卸载防毒墙网络版客户端上其他基于软件的防火墙应用程序。

以下步骤是成功使用防毒墙网络版防火墙所必需的步骤：

1. 创建策略。该策略允许您选择一个安全级别，该级别可阻止或允许联网计算机上的网络通信和启用防火墙功能。
2. 将例外添加到该策略。例外允许客户端背离策略。使用例外可以指定客户端以及允许或阻止特定类型的网络通信，而不管策略中的安全级别设置。例如，在一个策略中阻止一组客户端的所有网络通信，但是创建一个允许 HTTP 网络通信的例外以便客户端可以访问 Web 服务器。
3. 创建概要文件并将其分配到客户端。防火墙概要文件包括一组客户端属性且与策略关联。当客户端与在概要文件中指定的属性相匹配时，将触发关联的策略。

防火墙策略

通过防火墙策略，您可以阻止或允许在策略例外中未指定的某些网络通信类型。策略还定义启用或禁用哪些防火墙功能。可将一个策略分配到一个或多个[防火墙概要文件](#)。

防毒墙网络版附带有一组缺省策略，可以修改或删除这些策略。

缺省防火墙策略如下：

表 7-1. 缺省防火墙策略

策略名称	安全级别	客户端设置	例外	建议使用
所有访问策略	低	启用防火墙	无	用于允许客户端无限制访问网络
Cisco Trust Agent for Cisco NAC	低	启用防火墙	允许通过端口 21862 的传入和传出 UDP 网络通信	客户端安装有 Cisco Trust Agent (CTA) 时使用
适用于趋势科技防毒墙控制管理中心通信端口	低	启用防火墙	允许通过端口 80 和 10319 的所有传入和传出 TCP/UDP 网络通信	客户端安装有 MCP 代理时使用
防毒墙群件版 for Microsoft Exchange 控制台	低	启用防火墙	允许通过端口 16372 的所有传入和传出 TCP 网络通信	客户端需要访问防毒墙群件版控制台时使用
趋势科技防毒墙邮件安全版控制台	低	启用防火墙	允许通过端口 80 的所有传入和传出 TCP 网络通信	客户端需要访问 IMSS 控制台时使用

如果具有所有缺省策略都未包括的要求，则另外创建新策略。

所有缺省的和用户创建的防火墙策略都显示在 Web 控制台上的防火墙策略列表中。

配置防火墙策略列表:

导航路径: 联网计算机 > 防火墙 > 策略

1. 要添加新策略, 请单击**添加**。如果要创建的新策略具有与现有策略类似的设置, 请选择现有策略, 然后单击**复制**。

要编辑现有策略, 请单击策略名称。

将显示策略配置窗口。请参阅第 7-6 页的[添加和修改防火墙策略](#)以获取详细信息。

2. 要删除现有策略, 请选中策略旁的复选框, 然后单击**删除**。
3. 要编辑防火墙例外模板, 请单击**编辑例外模板**。将显示“例外模板编辑器”。请参阅第 7-8 页的[编辑防火墙例外模板](#)以获取详细信息。

添加和修改防火墙策略

为每项策略配置以下内容:

- **安全级别:** 一个常规设置, 阻止或允许客户端计算机上的所有入站和/或所有出站网络通信。
- **防火墙功能:** 指定启用还是禁用防毒墙网络版防火墙、入侵检测系统 (IDS) 和防火墙违例通知消息。有关 IDS 的详细信息, 请参阅第 7-3 页的[入侵检测系统](#)。
- **策略例外列表:** 用于阻止或允许各种类型的网络通信的可配置例外列表。

添加策略:

导航路径: 联网计算机 > 防火墙 > 策略 > 添加

联网计算机 > 防火墙 > 策略 > 复制

1. 键入策略的名称。
2. 选择安全级别。选定的安全级别将不会应用到符合防火墙策略例外条件的网络通信。

3. 选择要用于策略的防火墙功能。

- 防火墙阻止传出数据包时，将显示防火墙违例通知消息。要修改该消息，请参阅第 7-16 页的[修改通知消息的内容](#)。
- 启用所有的防火墙功能向客户端用户授予权限，以启用/禁用该功能并修改客户端控制台中的防火墙设置。

警告！ 无法使用防毒墙网络版服务器 Web 控制台来覆盖用户配置的客户端控制台设置。

- 如果不启用上述功能，则从防毒墙网络版服务器 Web 控制台中配置的防火墙设置将显示在客户端控制台上的“网卡列表”下面。
- 客户端控制台**防火墙**选项卡**设置**下的信息始终反映从客户端控制台配置的设置，而不反映从服务器 Web 控制台配置的设置。

4. 在**例外**下，选择防火墙策略例外。这里所包含的策略例外是基于防火墙例外模板创建的。有关详细信息，请参阅第 7-8 页的[编辑防火墙例外模板](#)。

- 通过单击策略例外名称并更改所打开的页面中的设置来修改现有策略例外。

提示： 修改后的策略例外将仅适用于要创建的策略。如果希望该策略例外修改成为永久性的，则需要对防火墙例外模板中的策略例外做同样的修改。

- 单击**添加**以创建新的策略例外。在打开的页面中指定设置。

提示： 该策略例外同样仅适用于要创建的策略。要将此策略例外应用到其他策略，您需要先将其添加到防火墙例外模板中的策略例外列表。

5. 单击**保存**。

修改现有策略：

导航路径：联网计算机 > 防火墙 > 策略 > <策略名称>

1. 修改以下内容：

- 策略名称
- 安全级别
- 用于策略的防火墙功能
- 要包含在策略中的防火墙策略例外
 - 编辑现有策略例外（单击策略例外名称和更改打开的页面中的设置）。
 - 单击**添加**以创建新的策略例外。在打开的页面中指定设置。

2. 单击保存**将修改应用到现有策略。**

编辑防火墙例外模板

防火墙例外模板包含可根据客户端计算机的端口号和 IP 地址配置以允许或阻止不同类型网络通信的策略例外。创建策略例外后，编辑策略例外要应用的策略。

确定要使用的策略例外类型。有两种类型：

限定

仅阻止指定类型的网络通信，适用于允许所有网络通信的策略。使用限定策略例外的一个示例是阻止易受攻击的客户端端口，如特洛伊木马经常使用的端口。

许可

仅允许指定类型的网络通信，适用于阻止所有网络通信的策略。例如，您可能要允许客户端仅访问防毒墙网络版服务器和 Web 服务器。要执行此操作，请允许来自于可信端口（用以与防毒墙网络版服务器通信的端口）和客户端用于 HTTP 通信的端口的网络通信。

客户端侦听端口： **联网计算机 > 客户端管理 > 状态**。端口号在**基本信息**下。

服务器侦听端口： **管理 > 连接设置**。端口号在**联网计算机的连接设置**下。

防毒墙网络版附带有一组缺省防火墙策略例外，可以修改或删除这些例外。

表 7-2. 缺省防火墙策略例外

例外名称	处理措施	协议	端口	方向
DNS	允许	TCP/UDP	53	传入和传出
NetBIOS	允许	TCP/UDP	137、138、139、445	传入和传出
HTTPS	允许	TCP	443	传入和传出
HTTP	允许	TCP	80	传入和传出
Telnet	允许	TCP	23	传入和传出
SMTP	允许	TCP	25	传入和传出
FTP	允许	TCP	21	传入和传出
POP3	允许	TCP	110	传入和传出
LDAP	允许	TCP/UDP	389	传入和传出

注意： 缺省例外适用于所有客户端。如果希望缺省例外仅适用于某些客户端，请编辑该例外并指定客户端的 IP 地址。

如果从先前的防毒墙网络版版本升级，则 LDAP 例外不可用。如果在例外列表上没有看到此例外，请手动添加。

添加策略例外：

导航路径：联网计算机 > 防火墙 > 策略 > 编辑例外模板 > 添加

1. 键入策略例外的名称。
2. 选择防毒墙网络版将对网络通信执行的操作（阻止或允许满足例外条件的网络通信）和网络通信方向（客户端计算机上的入站或出站网络通信）。
3. 选择网络协议的类型：**TCP**、**UDP** 或 **ICMP**。
4. 指定客户端计算机上用于执行操作的端口。
5. 选择要包括在例外中的客户端计算机 IP 地址。例如，如果您选择“拒绝所有网络通信（入站和出站）”并键入网络中的单个计算机的 IP 地址，则在策略中包含有此例外的任一客户端都将无法向该 IP 地址发送数据或从该 IP 地址接收数据。
6. 单击**保存**。

编辑策略例外：

导航路径：联网计算机 > 防火墙 > 策略 > 编辑例外模板 > <策略例外名称>

1. 修改以下内容：
 - 策略例外名称
 - 防毒墙网络版将对网络通信执行的操作和网络通信方向
 - 网络协议的类型
 - 策略例外的端口号
 - 客户端计算机 IP 地址
2. 单击**保存**。

删除项：

导航路径：联网计算机 > 防火墙 > 策略 > 编辑例外模板

1. 选中要删除的例外旁的复选框。
2. 单击**删除**。

更改例外在列表中的顺序：

导航路径：联网计算机 > 防火墙 > 策略 > 编辑例外模板

1. 选中要移动的例外旁的复选框。
2. 单击**上移**或**下移**。例外的 ID 号更改以反映新位置。

保存例外列表设置：

导航路径：联网计算机 > 防火墙 > 策略 > 编辑例外模板

单击以下保存选项之一：

- **保存模板更改：**保存带有当前策略例外和设置的例外模板。此选项仅将该模板应用于在将来创建的策略，而不是现有的策略。
- **保存并应用到现有策略上：**保存带有当前策略例外和设置的例外模板。此选项将该模板应用于现有和将来的策略。

防火墙概要文件

防火墙概要文件通过允许您在应用策略前选择一台客户端或一组客户端必须具有的属性来提供灵活性。概要文件包括以下内容：

- **关联的策略：**每个概要文件都使用一个策略
- **客户端属性：**带有一个或多个以下属性的客户端应用关联的策略：
 - **IP 地址：**具有特定 IP 地址，其 IP 地址在某个 IP 地址范围内，或者其 IP 地址属于特定子网的客户端
 - **域：**属于特定防毒墙网络版域的客户端
 - **计算机：**带有特定计算机名的客户端
 - **平台：**运行特定平台的客户端
 - **登录名：**指定的用户已登录到的客户端计算机
 - **客户端连接状态：**客户端是联机还是脱机

注意： 如果客户端可以连接到防毒墙网络版服务器或任一[参考服务器](#)，则客户端处于联机状态；如果客户端无法连接到任何服务器，则客户端处于脱机状态。

- **用户权限：**允许或阻止客户端用户执行以下操作：
 - 更改在策略中指定的安全级别
 - 编辑与策略相关联的例外列表

注意： 这些权限仅适用于与概要文件中指定的属性相匹配的客户端。可以将其他防火墙权限分配给选定的客户端用户。有关详细信息，请参阅第 7-15 页的 [防火墙权限](#)。

防毒墙网络版附带有一个名为“所有客户端概要文件”、使用“[所有访问策略](#)”策略的缺省概要文件。可以修改或删除此缺省概要文件。也可以创建新的概要文件。所有缺省的和用户创建的防火墙概要文件（包括与每个概要文件关联的策略和当前概要文件状态）都显示在 Web 控制台上的防火墙概要文件列表中。管理概要文件列表并将所有概要文件部署到防毒墙网络版客户端。防毒墙网络版客户端将所有防火墙概要文件存储在客户端计算机中。

配置防火墙概要文件列表：

导航路径：联网计算机 > 防火墙 > 概要文件

1. 要添加新的概要文件，请单击**添加**。要编辑现有概要文件，请选择概要文件名称。

将显示概要文件配置窗口。请参阅第 7-14 页的 [添加和编辑防火墙概要文件](#) 以获取详细信息。

2. 要删除现有策略，请选中策略旁的复选框，然后单击**删除**。
3. 要更改概要文件在列表中的顺序，请选中要移动的概要文件旁的复选框，然后单击**上移**或**下移**。

防毒墙网络版按照列表中显示的顺序将防火墙概要文件应用到客户端。例如，如果客户端与第一个概要文件匹配，则防毒墙网络版会把为该概要文件配置的操作应用到该客户端。防毒墙网络版将忽略为该客户端配置的其他概要文件。

提示： 将排他性最强的策略放在列表顶部，这样效果最好。例如，将为单个客户端创建的策略移动到顶部，接下来才是为一系列客户端、网络域和所有客户端创建的策略。

4. 要管理参考服务器，请单击**编辑参考服务器列表**。

参考服务器是在防毒墙网络版服务器应用防火墙概要文件时作为其替换服务器的计算机。参考服务器可以是网络上的任何计算机。当启用参考服务器时，防毒墙网络版做以下假设：

- 连接到参考服务器的客户端联机，即使客户端无法与防毒墙网络版服务器通信。
- 应用于联机客户端的防火墙概要文件也适用于连接到参考服务器的客户端。

请参阅第 8-13 页的[参考服务器](#)以获取详细信息。

5. 保存当前设置并将概要文件分配到客户端：

- a. 选择是否**要覆盖客户端安全等级/例外列表**。此选项将覆盖所有用户配置的防火墙设置。
- b. 单击**向客户端分配概要文件**。防毒墙网络版将概要文件列表中的所有概要文件分配给所有客户端。
- c. 要保存当前设置，请单击**保存概要文件列表更改**。

6. 验证是否将概要文件成功分配到客户端：

- a. 转至**联网计算机 > 客户端管理**。从客户端树视图下拉框中，选择**防火墙视图**。
- b. 请确保在客户端树中的**防火墙**列下有绿色复选标记。如果与概要文件关联的策略启用入侵检测系统，则在 **IDS** 列下还存在绿色复选标记。
- c. 验证客户端是否应用了正确的防火墙策略。该策略在客户端树中的**防火墙策略**列下显示。

添加和编辑防火墙概要文件

客户端计算机可能需要不同级别的防护。通过防火墙概要文件，您可以指定要应用关联策略的客户端计算机，并授予客户端用户修改防火墙设置的权限。通常，每个正在使用的策略都需要一个概要文件。

添加概要文件：

导航路径：联网计算机 > 防火墙 > 概要文件 > 添加

1. 单击**启用该概要文件**以允许防毒墙网络版将该概要文件部署到防毒墙网络版客户端。
2. 键入名称以识别该概要文件和可选描述。
3. 选择此概要文件的策略。
4. 指定防毒墙网络版要应用该策略的客户端计算机。根据以下条件选择计算机：
 - IP 地址
 - 域：单击按钮打开客户端树，并从其中选择域。
 - 计算机：单击按钮打开客户端树，并从其中选择客户端计算机。
 - 平台
 - 登录名
 - 客户端状态
5. 选择是授予用户更改防火墙安全级别的权限，还是编辑可配置例外列表以允许指定类型的网络通信的权限。有关这些选项的详细信息，请参阅第 7-6 页的[添加和修改防火墙策略](#)。
6. 单击**保存**。

编辑概要文件：

导航路径：联网计算机 > 防火墙 > 概要文件 > <概要文件名称>

1. 单击**启用该概要文件**以允许防毒墙网络版将该概要文件部署到防毒墙网络版客户端。

修改以下内容：

- 概要文件名称和描述
- 分配给概要文件的策略
- 客户端计算机，根据以下条件：
 - IP 地址
 - 域：单击按钮打开客户端树，并从其中选择域。
 - 计算机：单击按钮打开客户端树，并从其中选择客户端计算机。
 - 平台
 - 登录名
 - 客户端状态
- 权限：选择向用户是授予更改防火墙安全级别的权限，还是授予编辑可配置例外列表以允许指定类型的网络通信的权限。有关这些选项的详细信息，请参阅第 7-6 页的[添加和修改防火墙策略](#)。

2. 单击**保存**。

防火墙权限

授予用户以下权限：

- 查看客户端控制台上的**防火墙**选项卡
- 启用或禁用防毒墙网络版防火墙和防火墙功能
- 允许客户端向服务器发送防火墙日志

有关这些权限的详细信息，请参阅第 9-10 页的[防火墙权限](#)。

向客户端用户发送的防火墙违例通知

在防毒墙网络版防火墙阻止违反防火墙策略的出站网络通信后，防毒墙网络版可以在客户端计算机上立即显示通知消息。在配置特定的防火墙策略时，授予用户启用通知消息或启用通知的权限。（可选）修改通知消息的内容。

要配置防火墙策略，请参阅第 7-6 页的[添加和修改防火墙策略](#)。

授予用户启用通知消息的权限：

导航路径：联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 权限选项卡

1. 在**防火墙权限**下，选择启用防毒墙网络版防火墙、入侵检测系统和防火墙违例通知消息。
2. 如果在客户端树上选择域或客户端，请单击**保存**将设置应用到域或客户端。如果选择根图标 ，则从下列选项进行选择：
 - **应用到全部客户端：**将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - **仅应用到将来的域：**仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

修改通知消息的内容：

导航路径：通知 > 客户端用户通知

1. 单击**防火墙违例**选项卡。
2. 在提供的文本框中修改缺省消息。
3. 单击**保存**。

防火墙日志

服务器上可用的防火墙日志由具有发送防火墙日志权限的客户端发送。将此权限授予特定客户端，以监控和分析防毒墙网络版防火墙阻止的客户端计算机上的网络通信。

有关防火墙权限的信息，请参阅第 9-10 页的[防火墙权限](#)。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅第 8-16 页的[管理日志](#)。

查看防火墙日志：

导航路径：日志 > 联网计算机日志 > 安全风险 > 查看日志 > 防火墙日志

联网计算机 > 客户端管理 > 日志 > 防火墙日志

1. 要确保为您提供最新的日志，请单击**通知客户端**。在继续执行下一步之前，留出一些时间供客户端发送防火墙日志。
2. 指定日志条件，然后单击**显示日志**。
3. 查看日志。日志包含以下信息：
 - 防火墙违例的检测日期和时间
 - 发生防火墙违例的计算机
 - 远程主机 IP 地址
 - 本地主机 IP 地址
 - 协议
 - 端口号
 - 描述：指出实际安全风险（例如，网络病毒或 IDS 攻击）或防火墙策略违例
 - 方向：是入站（接收）还是出站（发送）网络通信违反了防火墙策略
 - 进程：正在计算机上运行的导致防火墙违例的可执行程序或服务
4. 要将日志保存为逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。通常使用电子表格应用程序（例如 Microsoft Excel）来打开 CSV 文件。

测试防毒墙网络版防火墙

要帮助确保防毒墙网络版防火墙正常工作，请在 一个或一组客户端上执行测试。

警告！ 请仅在受控的环境中测试防毒墙网络版客户端程序设置。请勿在已连接到网络或 Internet 的客户端计算机上执行测试。执行此操作可能会将客户端计算机暴露在病毒、黑客攻击和其他风险中。

测试防火墙：

1. 创建并保存测试策略。配置设置以阻止要测试的网络通信的类型。例如，要阻止客户端访问 Internet，请执行以下操作：
 - a. 将安全级别设置为**低**（允许所有入站/出站网络通信）。
 - b. 选择**启用防火墙和发生防火墙违例时通知用户**。
 - c. 创建阻止 HTTP 网络通信的例外。
2. 通过选择将测试防火墙功能的客户端，创建和保存测试概要文件。将测试策略与测试概要文件关联。
3. 单击**向客户端分配概要文件**。
4. 验证部署。
 - a. 单击**联网计算机 > 客户端管理**。
 - b. 选择客户端属于的域。
 - c. 从客户端树视图中选择**防火墙视图**。
 - d. 检查在客户端树的**防火墙**列下是否有绿色复选标记。如果已为该客户端启用了入侵检测系统，则请检查在 **IDS** 列中是否还有绿色复选标记。
 - e. 验证客户端是否应用了正确的防火墙策略。该策略在客户端树中的**防火墙策略**列下显示。
5. 通过尝试发送或接收在策略中配置的网络通信类型来测试客户端计算机上的防火墙。
6. 要测试配置以阻止客户端访问 Internet 的策略，请打开客户端计算机上的 Web 浏览器。如果已将防毒墙网络版配置为发生防火墙违例时显示通知消息，则在发生出站网络通信违例时，会在客户端计算机上显示该消息。

禁用防毒墙网络版防火墙

可以在所有的或选定的客户端计算机上禁用防毒墙网络版防火墙。

在选定的计算机上禁用防毒墙网络版防火墙：

方法 A：创建一项新策略，并将它应用于客户端。

1. 创建一项不启用防火墙的新策略。有关创建新策略的步骤，请参阅第 7-6 页的[添加和修改防火墙策略](#)。
2. 将该策略应用于客户端。

方法 B：禁用防火墙驱动程序和服务

1. 禁用防火墙驱动程序。
 - a. 打开 **Windows 网络连接属性**。
 - b. 从网卡中清除**趋势科技通用防火墙驱动程序**复选框。
2. 禁用防火墙服务。
 - a. 打开命令提示符，然后键入 **services.msc**。
 - b. 从 Microsoft 管理控制台 (MMC) 禁用 **OfficeScan NT Firewall**。

在所有客户端计算机上禁用防毒墙网络版防火墙：

1. 在 Web 控制台上，转至**管理 > 产品使用授权 > 其他服务**部分。
2. 在**联网计算机的防火墙**行上，单击**禁用**。

第 2 部分

管理防毒墙网络版服务器和客户端



管理防毒墙网络版服务器

本章主题：

- 第 8-2 页的[基于角色的管理](#)
- 第 8-10 页的[趋势科技防毒墙控制管理中心](#)
- 第 8-13 页的[参考服务器](#)
- 第 8-15 页的[系统事件日志](#)
- 第 8-16 页的[管理日志](#)
- 第 8-19 页的[使用授权](#)
- 第 8-21 页的[防毒墙网络版数据库备份](#)
- 第 8-22 页的[防毒墙网络版 Web 服务器信息](#)
- 第 8-23 页的[Web 控制台密码](#)
- 第 8-24 页的[隔离管理器](#)
- 第 8-25 页的[服务器调节程序](#)
- 第 8-28 页的[全球病毒实时监控计划](#)

基于角色的管理

使用基于角色的管理功能可授予和控制访问防毒墙网络版 Web 控制台菜单和子菜单项的权限。如果组织中存在多个防毒墙网络版管理员，则此功能可帮助您将服务器管理任务委派给他们并管理每个管理员可访问的菜单项。此外，还可授予除管理员之外的人对 Web 控制台的“仅查看”权限。

基于角色的管理涉及下列任务：

1. 定义用户角色。
2. 配置用户帐户并为每个用户分配特定角色。

从[系统事件日志](#)查看所有用户的 Web 控制台活动。记录以下活动：

- 登录到控制台
- 修改密码
- 从控制台注销
- 会话超时（用户被自动注销）

用户角色

用户角色确定用户可访问的 Web 控制台菜单项。防毒墙网络版附带了一组内置用户角色，您无法修改或删除这些角色。如果内置角色都不符合要求，则添加定制角色。将每个定制角色配置为具有特定 Web 控制台菜单项和子菜单项的“查看”或“配置”权限。

所有内置和定制角色都显示在 Web 控制台上的“用户角色”列表上。

注意： 对于每个角色，对客户端树上特定防毒墙网络版域的访问都是无法控制的。如果客户端树可见，则将显示所有域。

内置角色如下：

Administrator

具有 Administrator 角色的用户可以配置所有菜单项。可以将此角色委派给其他防毒墙网络版管理员或具有丰富的防毒墙网络版知识的用户。

Power User

可以将此角色委派给要在 Web 控制台上执行特定管理任务的管理员。

1. 具有 Power User 角色的用户可以配置以下菜单项和子菜单项：

联网计算机 > 客户端安装

此菜单项为用户提供两种安装防毒墙网络版客户端的方法。有关详细信息，请参阅第 3-26 页的[从防毒墙网络版 Web 控制台安装](#)和第 3-14 页的[启动基于浏览器的安装](#)。

联网计算机 > 防火墙

此菜单项允许用户管理防火墙策略和概要文件。有关详细信息，请参阅第 7-4 页的[防火墙策略和概要文件](#)。

日志

此菜单项允许用户查看和管理日志。有关详细信息，请参阅第 8-16 页的[管理日志](#)。

立即扫描（位于主菜单顶部）

此菜单项允许用户在目标计算机上启动手动扫描。有关详细信息，请参阅第 5-23 页的[启动立即扫描](#)。

客户端树设置

每次客户端树显示时，都可以配置用户可见的所有设置。有关详细信息，请参阅第 2-12 页的[客户端树特定任务](#)。

2. 用户不具有以下菜单项的访问权限：
 - 插件管理器
 - 管理 > 用户角色
 - 管理 > 用户帐户
3. 用户具有所有其他菜单项的查看权限。

Guest User

将此角色委派给希望查看 Web 控制台以供参考的用户。

1. 具有 Guest User 角色的用户不具有以下菜单项的访问权限：

- 插件管理器
- 管理 > 用户角色
- 管理 > 用户帐户

2. 用户具有所有其他菜单项的查看权限。

配置用户角色列表：

导航路径：管理 > 用户角色

1. 要添加定制角色，请单击**添加**。如果要添加的角色具有与某个现有定制角色类似的设置，则选择该角色并单击**复制**。

要修改某个定制角色，请单击该角色名称。

显示角色配置窗口。请参阅第 8-5 页的[添加和修改定制角色](#)以获取详细信息。

2. 要删除定制角色，请选中该角色旁边的复选框，然后单击**删除**。

3. 要将定制角色保存到 .dat 文件，请选择这些定制角色并单击**导出**。如果要管理其他防毒墙网络版服务器，则使用该 .dat 文件将定制角色导入到该服务器。

4. 如果已保存另一台防毒墙网络版服务器上的定制角色，且希望将这些角色导入到当前防毒墙网络版服务器中，则单击**导入**并查找包含这些定制角色的 .dat 文件。

注意： 如果导入与“用户角色”窗口上的角色具有相同名称的角色，则将覆盖“用户角色”窗口上的角色。

添加和修改定制角色

添加定制角色：

导航路径：管理 > 用户角色 > 添加

管理 > 用户角色 > 复制

1. 为角色键入名称并可选择提供描述。
2. 在“可用的菜单项”列表上，显示 Web 控制台主菜单和子菜单项。将该角色配置为具有一个或多个菜单项的“查看”或“配置”权限。

注意： 如果选中**配置**下的复选框，则会自动选中**查看**下的复选框。

只有具有内置管理员角色的用户和使用在防毒墙网络版安装期间创建的 root 帐户的用户才可以配置角色和帐户。

定制角色可以具有**插件管理器**的“配置”权限，或者根本不具有任何访问权限。这是因为插件管理器是一个独立程序，防毒墙网络版不控制其功能。

3. 单击**保存**。新角色显示在“用户角色”列表上。

修改定制角色：

导航路径：管理 > 用户角色 > <角色名称>

1. 修改以下内容：
 - 描述
 - 可访问菜单项
2. 单击**保存**。

用户帐户

设置用户帐户并为每个用户分配特定角色。用户角色确定用户可查看或配置的 Web 控制台菜单项。

在防毒墙网络版服务器安装期间，安装程序会自动创建称为“root”的内置帐户。使用 root 帐户登录的用户可以访问所有菜单项。您无法删除 root 帐户，但是可以修改帐户详细信息，如密码和显示名称。如果忘记 root 帐户密码，请与技术支持提供商联系，以帮助您重置密码。

添加定制帐户或 Active Directory 帐户。所有用户帐户都显示在 Web 控制台上的“用户帐户”列表上。

防毒墙网络版用户帐户可用于执行“单点登录”。单点登录允许用户从趋势科技防毒墙控制管理中心控制台访问防毒墙网络版 Web 控制台。有关详细信息，请参阅以下过程。

配置用户帐户列表：

导航路径：管理 > 用户帐户

1. 要添加定制帐户或 Active Directory 帐户，请单击**添加**。要修改定制帐户，请单击该帐户名称。
显示帐户配置窗口。请参阅第 8-7 页的[添加和修改用户帐户](#)以获取详细信息。
2. 要添加一个或多个 Active Directory 帐户，请单击**从 Active Directory 添加**。请参阅第 8-9 页的[添加一个或多个 Active Directory 帐户](#)以获取详细信息。
3. 要修改一个或多个帐户的角色，请选择这些帐户并单击**更改角色**。在显示的窗口上，选择新角色并单击**保存**。
4. 要启用或禁用帐户，请单击**启用**下的图标。

注意： root 帐户不能禁用。

5. 要删除帐户，请选择该帐户并单击**删除**。

使用控制管理中心的防毒墙网络版用户帐户：

有关具体步骤，请参阅控制管理中心文档。

1. 在控制管理中心创建新的用户帐户。指定用户名时，键入防毒墙网络版 Web 控制台上显示的帐户名称。
2. 赋予新帐户对防毒墙网络版服务器的“访问”和“配置”权限。

注意： 如果控制管理中心用户具有防毒墙网络版的“访问”和“配置”权限，但是不具有防毒墙网络版帐户，则该用户无法访问防毒墙网络版。该用户将看到一条消息，其中包含用于打开防毒墙网络版 Web 控制台的登录窗口的链接。

使用控制管理中心的 root 帐户登录的用户即使没有防毒墙网络版帐户，也能访问防毒墙网络版。

添加和修改用户帐户

通过将用户的 Active Directory 帐户添加到“用户帐户”列表，将 Web 控制台访问权限分配给用户。

添加定制帐户或 Active Directory 帐户：

导航路径：管理 > 用户帐户 > 添加

1. 单击**启用此帐户**允许用户使用该帐户。

注意： 如果在用户已登录时禁用帐户，则在用户注销后将禁用该帐户。

2. 选择是添加定制帐户还是添加 Active Directory 帐户。
 - 对于定制帐户，键入用户名、全名和密码（需要确认）。可以选择为帐户键入电子邮件地址。

注意： 电子邮件地址仅用作参考。电子邮件帐户的所有者不会收到所创建帐户的通知电子邮件。

- 对于 Active Directory 帐户，指定帐户名称（用户名或组）和帐户所属的域。

包括完整帐户名和域名。如果帐户名和域名不完全，则防毒墙网络版将不会返回结果。

属于同一个组的所有成员会得到相同的角色。如果某个特定帐户至少属于两个组，并且其在两个组中具有不同的角色：

- 两个角色的权限会合并起来。如果用户配置了特定设置，但该设置的权限之间存在冲突，则应用较高的权限。
- 所有用户角色都会显示在系统事件日志中。例如，“User JohnDoe logged on with the following roles: Administrator, Power User”。

3. 选择帐户的角色。

4. 单击**保存**。

5. 如果添加了定制帐户，则将帐户详细信息发送给用户。如果添加了 Active Directory 帐户，则通知用户使用其域名和密码登录到 Web 控制台。

6. 如果用户的计算机运行的是 Windows 2000，则通知用户安装以下项目：

- Microsoft Patch KB890859
- Microsoft Patch KB924270
- Windows 2000 授权管理器运行库

注意： Authorization Manager Runtime 仅支持英语、法语、德语和日语版本。

修改定制帐户：

导航路径：管理 > 用户帐户 > <用户名>

1. 使用提供的复选框启用或禁用帐户。

注意： 不能禁用 Active Directory 组帐户。如果不希望组中的用户访问 Web 控制台，则从用户帐户列表中删除组。

2. 修改以下内容：
 - 全名
 - 密码
 - 电子邮件地址
 - 角色
3. 单击**保存**。

添加一个或多个 Active Directory 帐户

添加一个或多个 Active Directory 帐户：

导航路径：管理 > 用户帐户 > 从 Active Directory 添加

1. 通过指定用户名和帐户所属的域来搜索帐户（用户名或组）。

使用通配符 (*) 搜索多个帐户。如果不指定通配符，则包括完整帐户名。如果帐户名不完全，则防毒墙网络版将不会返回结果。
2. 当防毒墙网络版找到有效帐户时，它在**用户和组**下显示帐户名。单击向前图标 (>) 移动**所选用户和组**下的帐户。

如果指定 Active Directory 组，则属于同一个组的所有成员都会得到相同的角色。如果某个特定帐户至少属于两个组，并且其在两个组中具有不同的角色：

 - 两个角色的权限会合并起来。如果用户配置了特定设置，但该设置的权限之间存在冲突，则应用较高的权限。
 - 所有用户角色都会显示在系统事件日志中。例如，“User JohnDoe logged on with the following roles: Administrator, Power User”。
3. 选择帐户的角色。
4. 单击**保存**。
5. 通知用户使用他们各自的域名和密码登录到 Web 控制台。

6. 如果用户的计算机运行的是 Windows 2000，则通知用户安装以下项目：

- Microsoft Patch KB890859
- Microsoft Patch KB924270
- Windows 2000 授权管理器运行库

注意： Authorization Manager Runtime 仅支持英语、法语、德语和日语版本。

趋势科技防毒墙控制管理中心

趋势科技防毒墙控制管理中心是管理位于网关、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、第三方防病毒和内容安全产品的中央管理控制台。控制管理中心基于 Web 的管理控制台为整个网络内被管理产品和服务提供单个监控点。

控制管理中心允许系统管理员监控和报告活动，例如感染、安全性违例或病毒入口点。系统管理员可以下载组件并在整个网络内部署，以帮助确保防护的一致性和及时性。控制管理中心既允许手动更新又允许预设更新，还允许作为组或作为个体来配置和管理产品，以增加灵活性。

支持的控制管理中心版本

此防毒墙网络版版本支持控制管理中心 5.0 和 3.5。对这些控制管理中心版本应用最新的 Patch 和重要的 Hotfix，使控制管理中心能够对防毒墙网络版进行管理。要获取最新的 Patch 和 Hotfix，请与技术支持提供商联系或者访问趋势科技更新中心：

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

在安装防毒墙网络版之后，将其注册到控制管理中心，然后在控制管理中心管理控制台上配置防毒墙网络版的设置。有关管理防毒墙网络版服务器的信息，请参阅*控制管理中心文档*。

在此防毒墙网络版版本中集成控制管理中心

此防毒墙网络版版本在从控制管理中心管理防毒墙网络版服务器时包括下列功能和能力：

- 控制管理中心控制台上提供以下信息：
 - **行为监控组件**和版本信息
 - 供客户端使用的扫描方法（传统扫描和云安全扫描）
 - 客户端与云安全服务器的连接状态
 - 云安全服务器地址（URL 格式）
 - 云安全客户端病毒码信息
- 云安全客户端病毒码可以从控制管理中心控制台更新。
- 在控制管理中心控制台中，将以下设置从一台防毒墙网络版服务器复制到另一台：
 - 所有扫描类型（**实时扫描**、**手动扫描**、**预设扫描**和**立即扫描**）的扫描设置
 - **客户端权限和其他设置**
 - **Web 信誉策略**
 - **防火墙策略**
 - **防火墙概要文件**

注意： 如果将这些设置复制到尚未激活特定服务使用授权的防毒墙网络版服务器，则只有在激活该使用授权时这些设置才能生效。例如，如果没有激活 Web 信誉和防间谍软件使用授权，则 Web 信誉策略将被复制到防毒墙网络版服务器，但它将只在激活该使用授权时才生效。

将防毒墙网络版注册到控制管理中心：

导航路径：管理 > 控制管理中心设置

1. 指定实体显示名称，该名称就是将在控制管理中心显示的防毒墙网络版服务器的名称。缺省情况下，实体显示名称包括服务器计算机的主机名和此产品的名称（例如，Server01_OSCE）。

注意： 在控制管理中心，由控制管理中心管理的防毒墙网络版服务器及其他产品都称为“实体”。

2. 指定控制管理中心服务器 FQDN 或 IP 地址以及用于连接到该服务器的端口号。可选择是否以更高的安全性（使用 HTTPS）来连接。
3. 如果控制管理中心的 IIS Web 服务器需要认证，请键入用户名和密码。
4. 如果要使用代理服务器连接到控制管理中心服务器，请指定以下代理服务器设置：
 - 代理服务器协议
 - 服务器 FQDN 或 IP 地址和端口
 - 代理服务器认证的用户 ID 和密码
5. 决定是使用 **one-way communication（单向通信）** 还是 **two-way communication（双向通信）** 端口进行转发，然后指定 IP 地址和端口。
6. 要检查防毒墙网络版是否可以根据您指定的设置连接到控制管理中心服务器，请单击**测试连接**。如果成功建立连接，则单击**注册**。
7. 如果在注册后更改了此窗口上的任何设置，请在更改设置后单击**更新设置**，以向控制管理中心服务器通知这些更改。
8. 如果不再希望控制管理中心服务器管理防毒墙网络版，则单击**取消注册**。

在控制管理中心管理控制台上检查防毒墙网络版的状态：

1. 打开控制管理中心管理控制台。

要打开控制管理中心控制台，请在网络上的任意计算机上打开一个 Web 浏览器，然后键入以下内容：

对于控制管理中心 3.5：

`https://<Control Manager server name>/ControlManager`

对于控制管理中心 5.0：

`https://<Control Manager server name>/Webapp/login.aspx`

其中 <Control Manager server name> 是控制管理中心服务器的 IP 地址或主机名。

2. 在主菜单中，单击**产品**。
3. 从列表选择**被管理产品**。
4. 检查防毒墙网络版服务器图标是否显示。

参考服务器

防毒墙网络版客户端确定要使用哪种**防火墙概要文件**或**Web 信誉策略**的方式之一是，通过检查其与防毒墙网络版服务器的连接状态。如果某个内部客户端（或公司网络中的客户端）无法连接到服务器，则该客户端的状态将成为脱机状态。然后，该客户端将应用于外部客户端的防火墙概要文件或 Web 信誉策略。参考服务器可解决此问题。

与防毒墙网络版服务器失去连接的客户端将尝试连接到参考服务器。如果客户端与参考服务器成功建立连接，则其将应用于内部客户端的防火墙概要文件或 Web 信誉策略。

请注意以下事项：

- 将具有服务器功能的计算机（如 Web 服务器、SQL 服务器或 FTP 服务器）指定为参考服务器。最多可以指定 32 个参考服务器。
- 客户端将连接到参考服务器列表中的第一个参考服务器。如果无法建立连接，则客户端将尝试连接到列表中的下一个服务器。

- 防毒墙网络版客户端只有在确定要使用的防火墙概要文件或 Web 信誉策略时，才使用参考服务器。参考服务器不管理客户端或部署更新和客户端设置。防毒墙网络版服务器执行这些任务。
- 客户端不能将日志发送到参考服务器，也不能将参考服务器用作更新源。

管理参考服务器列表：

导航路径：联网计算机 > 防火墙 > 概要文件 > 编辑参考服务器列表

联网计算机 > 计算机位置 > 编辑参考服务器列表

1. 选择**启用参考服务器列表**。
2. 要向该列表添加计算机，请单击**添加**。
 - a. 指定计算机的 IP 地址、名称或完全限定域名 (FQDN)，例如：
 - computer.networkname
 - 12.10.10.10
 - mycomputer.domain.com
 - b. 键入客户端与此计算机通信时通过的端口。指定参考服务器上的任一开放联系端口（如端口 20、23 或 80）。

注意： 要指定同一参考服务器的其他端口号，请重复步骤 2a 和 2b。客户端将使用列表中的第一个端口号，如果连接未成功，则将使用下一个端口号。

- c. 单击**保存**。
3. 要编辑列表上的计算机设置，请单击计算机名。修改计算机名或端口，然后单击**保存**。
 4. 要从列表中删除计算机，请选择计算机名，然后单击**删除**。
 5. 要使计算机充当参考服务器，请单击**分配到客户端**。

系统事件日志

防毒墙网络版记录与服务器程序相关的事件，如关闭和启动。使用这些日志来验证防毒墙网络版服务器及服务是否工作正常。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅第 8-16 页的 [管理日志](#)。

查看系统事件日志：

导航路径：日志 > 系统事件日志

1. 在**事件描述**下查看是否有需要进一步处理措施的日志。防毒墙网络版将记录以下事件：

防毒墙网络版主服务和数据库服务器：

- 主服务已启动
- 主服务停止成功
- 主服务停止未成功

爆发阻止：

- 爆发阻止已启用
- 爆发阻止已禁用
- 最近 <分钟数> 内的共享文件夹会话数

数据库备份：

- 数据库备份成功
- 数据库备份未成功

基于角色的 Web 控制台访问：

- 登录到控制台
- 修改密码
- 从控制台注销
- 会话超时（用户被自动注销）

2. 要将日志保存为逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。通常使用电子表格应用程序（例如 Microsoft Excel）来打开 CSV 文件。

管理日志

防毒墙网络版保留有关安全风险检测、事件和更新的全面日志。使用这些日志来评估贵组织的防护策略并识别处于较高感染风险或攻击风险的客户端。还使用这些日志来检查客户端-服务器连接并验证组件更新是否已成功。

防毒墙网络版生成以下日志：

安全风险日志

防毒墙网络版在检测到病毒/恶意软件和间谍软件/灰色软件以及在恢复间谍软件/灰色软件时，将生成日志。有关安全风险日志的更多信息，请参阅下列主题：

- 第 5-45 页的 [病毒/恶意软件日志](#)
- 第 5-51 页的 [间谍软件/灰色软件日志](#)
- 第 5-53 页的 [间谍软件/灰色软件恢复日志](#)

防火墙日志

防毒墙网络版在检测到防火墙策略违例时，将生成日志。有关详细信息，请参阅第 7-17 页的 [防火墙日志](#)。

Web 信誉日志

防毒墙网络版在阻止已知或潜在恶意 Web 站点时，将生成日志。有关详细信息，请参阅第 6-7 页的 [Web 信誉日志](#)。

连接验证日志

防毒墙网络版生成连接验证日志，您可以利用这些日志来确定防毒墙网络版服务器是否可以与其所有已注册客户端通信。有关详细信息，请参阅第 9-38 页的 [连接验证日志](#)。

组件更新日志

服务器和客户端执行组件更新时，防毒墙网络版将生成日志。查看这些日志以验证防毒墙网络版是否成功下载了保持防护最新所需的组件。有关更新日志的更多信息，请参阅下列主题：

- 第 4-18 页的 [服务器更新日志](#)
- 第 4-32 页的 [客户端更新日志](#)

设备控制日志

当客户端检测到对连接到客户端计算机的设备进行未经授权的访问时，防毒墙网络版将生成日志。然后，客户端每天将日志发送到服务器一次。有关详细信息，请参阅第 5-62 页的 [设备控制日志](#)。

系统事件日志

防毒墙网络版生成系统更新日志，以便您随时了解使防毒墙网络版服务器正常运行的事件（如数据库备份和主服务重新启动）。有关详细信息，请参阅第 8-15 页的 [系统事件日志](#)。

调试日志

使用调试日志疑难排解防毒墙网络版服务器和客户端的问题。有关调试日志的更多信息，请参阅下列主题：

- 第 12-2 页的 [防毒墙网络版服务器日志](#)
- 第 12-9 页的 [防毒墙网络版客户端日志](#)

日志维护

要防止日志大小占用太多的硬盘空间，请从 Web 控制台手动删除日志或者配置日志删除时间表。

注意： 对于调试日志，禁用调试日志记录以停止收集日志。

根据时间表删除日志：

导航路径：日志 > 日志维护

1. 选择**启用预设日志删除**。
2. 选择要删除的日志类型。
3. 选择是删除所有选定日志类型的日志，还是仅删除特定天数前的日志。
4. 指定日志删除的频率和时间。
5. 单击**保存**。

手动删除日志：

导航路径：日志 > 联网计算机日志 > 安全风险 > 删除日志

联网计算机 > 客户端管理 > 日志 > 删除日志

1. 选择要删除的日志类型。
2. 选择是删除所有选定日志类型的日志，还是仅删除特定天数前的日志。
3. 单击**删除**。

使用授权

在 Web 控制台上可以查看、激活和续订防毒墙网络版产品服务使用授权，以及启用/禁用防毒墙网络版防火墙。防毒墙网络版防火墙是防病毒服务的一部分，防病毒服务还包括 Cisco NAC 和爆发阻止的技术支持。

注意： 可以在安装过程中启用防毒墙网络版防火墙。如果禁用防火墙，则防毒墙网络版将隐藏服务器和客户端上的所有防火墙功能。

在以下实例中，从 Web 控制台注销，然后再次登录：

- 激活以下产品服务的使用授权之后：
 - 防病毒
 - Web 信誉和防间谍软件

注意： 必须重新登录才能启用服务的完整功能。

- 启用或禁用防毒墙网络版防火墙后

查看使用授权信息：

导航路径：管理 > 产品使用授权

管理 > 产品使用授权 > 产品使用授权详细信息

管理 > 产品使用授权 > 产品使用授权详细信息 > 产品使用授权新激活码

1. 查看使用授权状态摘要，该摘要显示在窗口的顶部。

以下实例中将显示关于使用授权的提醒信息：

如果您具有完全版使用授权

- 在产品的宽限期内。宽限期的持续时间可能因地区而异。请通过趋势科技代表验证宽限期。
- 当使用授权到期且宽限期已过时。在此期间，您将无法获得技术支持或无法执行组件更新。扫描引擎将仍然扫描计算机，但将使用过期组件。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。

如果您具有评估版使用授权

- 当使用授权过期时。在此期间，防毒墙网络版将禁用组件更新、扫描和所有客户端功能组件。
2. 查看使用授权信息。使用授权信息部分将提供以下信息：
- **服务：**包括所有防毒墙网络版产品服务。
 - **状态：**显示“已激活”、“尚未激活”或“已过期”。如果产品服务有多个使用授权，且至少一个使用授权仍然处于活动状态，则显示的状态为“已激活”。
 - **版本：**显示“完全版”或“评估版”。如果同时具有完全版和评估版，则显示的版本为“完全版”。
 - **使用授权过期日期：**如果产品服务有多个使用授权，则将显示最晚过期时间。例如，如果使用授权过期时间为 12/31/2007 和 06/30/2008，则将显示 06/30/2008。

注意： 尚未激活的产品服务的版本和过期日期为“无”。

3. 通过防毒墙网络版可以激活一个产品服务的多个使用授权。单击产品服务名称以查看该服务的所有使用授权（不论处于活动状态还是已过期状态）。

激活或续订使用授权：

导航路径：管理 > 产品使用授权

管理 > 产品使用授权 > 产品使用授权详细信息

管理 > 产品使用授权 > 产品使用授权详细信息 > 产品使用授权新激活码

1. 单击产品服务名称。
2. 在打开的“产品使用授权详细信息”窗口中，单击**新激活码**。
3. 在打开的窗口中，键入激活码并单击**保存**。

注意： 在激活服务前先注册服务。有注册码和激活码的详细信息，请与趋势科技代表联系。

4. 返回到“产品使用授权详细信息”窗口，单击**更新信息**以使用新使用授权的详细信息和服务状态来刷新该窗口。此窗口还提供一个到趋势科技 Web 站点的链接，您可以利用该链接来查看关于您的使用授权的详细信息。

防毒墙网络版数据库备份

防毒墙网络版服务器数据库包含所有防毒墙网络版设置，包括扫描设置和权限。服务器数据库损坏时，如果具有备份，则可以将其恢复。随时手动备份数据库或者配置备份时间表。

备份数据库时，防毒墙网络版帮助您自动整理数据库碎片并修复所有可能的索引文件损坏。

检查系统事件日志以确定备份状态。有关详细信息，请参阅第 8-15 页的 [系统事件日志](#)。

提示： 趋势科技建议您为自动备份配置时间表。在服务器网络通信较低的非高峰时段期间备份数据库。

警告！ 不要使用任何其他工具或软件来执行备份。仅从防毒墙网络版 Web 控制台中配置数据库备份。

备份防毒墙网络版数据库：

导航路径：管理 > 数据库备份

1. 键入要保存数据库的位置。如果文件夹还不存在，则选择**不存在时创建文件夹**。包括驱动器和完整目录路径，例如

C:\OfficeScan\DatabaseBackup。缺省情况下，防毒墙网络版将备份保存在以下目录中：<[服务器安装文件夹](#)>\DBBackup

防毒墙网络版会在备份路径下创建一个子文件夹。文件夹名称表示备份的时间并且格式如下：YYYYMMDD_HHMMSS。防毒墙网络版保存 7 个最近的备份文件夹，自动删除较旧的文件夹。

2. 如果备份路径位于远程计算机（使用 UNC 路径），则键入合适的帐户名称和相应的密码。确保该帐户在上述远程计算机上具有写权限。

3. 配置备份时间表：
 - a. 选择**启用预设数据库备份**。
 - b. 指定备份频率和时间。
 - c. 要备份数据库并保存所做的更改，请单击**立即备份**。要仅保存而不备份数据库，请单击**保存**。

恢复数据库备份文件：

1. 停止防毒墙网络版主服务。
2. 使用备份文件覆盖 <**服务器安装文件夹**>\PCCSRV\HTTPDB 中的数据库文件。
3. 重新启动防毒墙网络版主服务。

防毒墙网络版 Web 服务器信息

在防毒墙网络版服务器安装过程中，安装程序会自动设置一个 Web 服务器（IIS 或 Apache Web 服务器），以使联网计算机能够连接到防毒墙网络版服务器。配置联网客户端计算机将要连接到的 Web 服务器。

如果从外部修改了 Web 服务器设置（例如，从 IIS 管理控制台），则请复制防毒墙网络版中的更改以确保其保持服务器-客户端通信并允许访问 Web 控制台。例如，如果手动更改了联网计算机的服务器的 IP 地址或如果为其分配了一个动态 IP 地址，则需要重新配置防毒墙网络版的服务器设置。

配置连接设置：

导航路径：管理 > 连接设置

1. 键入 Web 服务器的域名/IP 地址和端口号。

注意： 端口号是防毒墙网络版服务器与防毒墙网络版客户端进行通信时使用的 **trusted port（可信端口）**。

2. 单击**保存**。

Web 控制台密码

仅当服务器计算机不具有为使用[基于角色的管理](#)而所需的资源时，才可以访问用于管理 Web 控制台密码（在防毒墙网络版服务器安装期间创建的 root 帐户的密码）的窗口。例如，如果服务器计算机运行 Windows 2000，但没有安装 Authorization Manager Runtime，则可以访问该窗口。如果资源满足需要，则此窗口不显示，这时可以通过在[用户帐户](#)窗口中修改 root 帐户来管理密码。

如果忘记控制台密码且已将防毒墙网络版服务器注册到控制管理中心，则使用 root 帐户登录到控制管理中心控制台，然后更改密码。如果具有可以访问防毒墙网络版服务器的控制管理中心帐户，则也可以更改密码。

如果没有将防毒墙网络版注册到控制管理中心，请与技术支持提供商联系以获取如何访问 Web 控制台的说明。

更改 Web 控制台密码：

导航路径：管理 > 控制台密码

1. 在提供的文本框中键入当前的新密码。

注意： 新密码必须包含 1 到 128 个字母数字字符。

2. 确认新密码。
3. 单击**保存**。

隔离管理器

只要防毒墙网络版客户端检测到安全风险且扫描处理措施为隔离，它就会加密受感染文件并将其移动到位于 <客户端安装文件夹>\SUSPECT 中的本地隔离文件夹中。

将文件移动到本地隔离目录之后，客户端会将其发送到指定的隔离目录中。在**联网计算机 > 客户端管理 > 设置 > {扫描类型} > 处理措施**选项卡中指定该目录。指定隔离目录中的文件会被加密，以防止其感染其他文件。请参阅第 5-32 页的**隔离目录**以获取详细信息。

如果指定的隔离目录位于防毒墙网络版服务器计算机上，则在 Web 控制台中修改服务器的隔离目录设置。该服务器将隔离文件存储到 <服务器安装文件夹>\PCCSRV\Virus 中。

注意： 如果防毒墙网络版客户端由于任何原因（如，网络连接问题）无法将加密的文件发送到防毒墙网络版服务器，则加密的文件将仍然保留在客户端隔离文件夹中。连接到防毒墙网络版服务器时，客户端将尝试重新发送该文件。

配置隔离目录设置：

导航路径：管理 > 隔离管理器

1. 接受或修改隔离文件夹的缺省容量以及防毒墙网络版可以存储在隔离文件夹内的最大受感染文件大小。缺省值将显示在此窗口上。
2. 单击**保存隔离设置**。
3. 要移除隔离文件夹中的所有现有文件，请单击**删除所有隔离文件**。

服务器调节程序

使用服务器调节程序来优化使用参数的防毒墙网络版服务器的性能，以解决以下与服务器相关的性能问题：

下载

当请求从防毒墙网络版服务器更新的客户端（包括更新代理）数量超过服务器的可用资源时，服务器将客户端的更新请求移动到队列中并在资源可用时处理请求。客户端成功从防毒墙网络版服务器更新组件后，客户端通知服务器更新完成。设置防毒墙网络版服务器等待接收来自客户端的更新通知的最大时间（分钟）。还设置服务器尝试通知客户端执行更新以及通知客户端应用新配置设置的最大次数。如果服务器没有收到客户端通知，就会不断尝试。

缓存

防毒墙网络版服务器收到来自客户端的多个请求（例如，执行更新的请求）时，服务器尽其所能处理请求并将剩余的请求放入缓存中。服务器然后在资源可用时每次处理一个保存在缓存中的请求。为事件（例如客户端更新请求）和客户端日志报告指定缓存大小。

网络通信

网络通信量在一天中不断变化。要控制到防毒墙网络版服务器以及到其他更新源的网络通信流，请指定在一天中任何给定时间可以同时更新的客户端数。

服务器调节程序需要以下文件：**SvrTune.exe**

运行服务器调节程序：

导航路径：工具 > 管理工具 > 服务器调节程序

1. 在防毒墙网络版服务器计算机上，导航到 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\SvrTune。
2. 双击 **SvrTune.exe** 启动服务器调节程序。将打开服务器调节程序控制台。

3. 在 **Download** 下，修改以下设置：

Timeout for client

键入防毒墙网络版服务器等待从客户端接收更新响应的时间（分钟）。如果客户端在上述指定时间内没有响应，则防毒墙网络版服务器认为客户端不具有当前组件。如果通知的客户端超时，则为另一个正在等待通知的客户端提供一个位置。

Timeout for update agent

键入防毒墙网络版服务器等待从更新代理接收更新响应的时间（分钟）。如果通知的客户端超时，则为另一个正在等待通知的客户端提供一个位置。

Retry count

键入防毒墙网络版服务器尝试通知客户端执行更新或通知客户端应用新配置设置的最大次数。

Retry interval

键入防毒墙网络版服务器在两次通知尝试之间等待的时间（分钟）。

4. 在 **Buffer** 下，修改以下设置：

Event Buffer

键入防毒墙网络版存储在缓存中的报告给服务器的客户端事件（如更新组件）的最大数量。客户端的请求在缓存中等待时，到客户端的连接将断开。防毒墙网络版处理客户端报告时才建立到客户端的连接，并从缓存中将请求移除。

Log Buffer

键入防毒墙网络版存储在缓存中的报告给服务器的客户端日志信息的最大数量。客户端的请求在缓存中等待时，到客户端的连接将断开。防毒墙网络版处理客户端报告时才建立到客户端的连接，并从缓存中将请求删除。

注意： 如果向服务器报告的客户端数量很大，请增加缓存大小。但是，缓存大小越大，意味着服务器上的内存使用率越高。

5. 在 **Network Traffic** 下，修改以下设置：

Normal hours

单击表示您认为一天中网络通信正常的时间的单选按钮。

Off-peak hours

单击表示您认为一天中网络通信最低的时间的单选按钮。

Peak hours

单击表示您认为一天中网络通信为高峰的时间的单选按钮。

Maximum client connections

键入可以从“其他更新源”和防毒墙网络版服务器同时更新组件的最大客户端数量。键入各个时间段的最大客户端数量。达到最大连接数量时，客户端仅能在当前客户端连接关闭后再更新组件（可能是因为更新的完成或因为客户端响应时间达到了您在 **Timeout for client** 或 **Timeout for Update Agent** 文本框中指定的值）。

6. 单击 **OK**。将显示一个提示，询问您是否要重新启动防毒墙网络版主服务。

注意： 仅重新启动服务，而非计算机。

7. 单击 **YES** 保存服务器调节程序设置并重新启动服务。重新启动后，设置立即生效。

单击 **NO** 保存服务器调节程序设置但不重新启动服务。重新启动防毒墙网络版主服务或重新启动防毒墙网络版服务器计算机以使设置生效。

全球病毒实时监控计划

将安全风险扫描结果发送到“全球病毒实时监控计划”，以更好地跟踪安全风险爆发趋势。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。

安装防毒墙网络版后，防毒墙网络版安装程序会询问您是否想加入“全球病毒实时监控计划”。可以随时从 Web 控制台中更改设置。

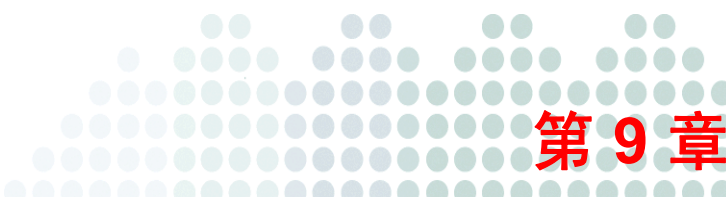
要查看当前趋势科技病毒地图，请访问以下站点：

<http://www.trendmicro.com/map/default.asp>

修改您在该计划中的参与情况：

导航路径：管理 > 全球病毒实时监控

1. 选择是加入该计划还是终止参与。
2. 单击**保存**。



第 9 章

管理客户端

本章主题：

- 第 9-2 页的 [计算机位置](#)
- 第 9-5 页的 [客户端权限和其他设置](#)
- 第 9-18 页的 [全局客户端设置](#)
- 第 9-30 页的 [客户端与服务器的连接](#)
- 第 9-39 页的 [客户端代理服务器设置](#)
- 第 9-41 页的 [客户端迁移程序](#)
- 第 9-42 页的 [触探工具](#)
- 第 9-43 页的 [客户端信息](#)
- 第 9-44 页的 [导入和导出客户端设置](#)
- 第 9-45 页的 [管理非活动客户端](#)

计算机位置

防毒墙网络版提供位置感知功能，可以确定应用到客户端以及连接的云安全服务器客户端的 **Web** 信誉策略。可连接到防毒墙网络版服务器或任何一个参考服务器的防毒墙网络版客户端位于内部，这意味着：

- 这些客户端会对内部客户端应用 **Web** 信誉策略。
- 如果这些客户端使用云安全扫描，则其将连接到本地云安全服务器。

如果无法建立连接，则客户端将对外部客户端应用 **Web** 信誉策略。如果这些客户端使用云安全扫描，则将连接到趋势科技 **Internet** 云安全服务器。

提示： 趋势科技建议在外部客户端上执行更严格的 **Web** 信誉策略。

指定该位置是基于客户端计算机的网关 IP 地址，还是基于客户端与防毒墙网络版服务器或任何参考服务器的连接状态。

网关 IP 地址

如果客户端计算机的网关 IP 地址与您在“计算机位置”窗口上指定的任何网关 IP 地址相匹配，则该计算机位置位于内部。否则，计算机位置位于外部。

客户端连接状态

如果防毒墙网络版客户端可以连接到防毒墙网络版服务器或 **Intranet** 中任何指定参考服务器，则计算机位置位于内部。此外，如果公司网络之外的某台计算机可与防毒墙网络版服务器/参考服务器建立连接，则其位置也位于内部。如果不符合以上任何条件，则计算机位置位于外部。

配置位置设置：

导航路径：联网计算机 > 计算机位置

1. 选择位置是基于**客户端连接状态**还是**网关 IP 和 MAC 地址**。

2. 如果选择**客户端连接状态**，则决定是否要使用参考服务器。有关详细信息，请参阅第 8-13 页的**参考服务器**。
 - a. 如果未指定参考服务器，当发生以下事件时，客户端将检查与防毒墙网络版服务器的连接状态：
 - 客户端从漫游模式切换到普通（联机或脱机）模式。
 - 客户端从一种扫描方法切换到另一种扫描方法。有关详细信息，请参阅第 5-8 页的**扫描方法**。
 - 客户端检测到计算机中的 IP 地址发生变化。
 - 客户端重新启动。
 - 服务器启动连接验证。有关详细信息，请参阅第 9-30 页的**客户端与服务器的连接**。
 - 应用全局设置时 Web 信誉位置条件发生变化。
 - 不再执行爆发阻止策略，并且已恢复爆发前设置。
 - b. 如果指定了参考服务器，客户端将首先检查其与防毒墙网络版服务器的连接状态，当与防毒墙网络版服务器的连接不成功时，客户端将检查其与参考服务器的连接状态。客户端每小时以及发生上述任一事件时，将检查连接状态。
3. 如果选择**网关 IP 和 MAC 地址**：
 - a. 在提供的文本框中键入网关 IP 地址。
 - b. 或者键入 MAC 地址。如果没有键入 MAC 地址，防毒墙网络版将包括所有属于指定 IP 地址范围的 MAC 地址。
 - c. 单击**添加**。
 - d. 重复步骤 a 到步骤 c，直到您添加完所有要添加的网关 IP 地址。
 - e. 使用网关设置导入程序工具导入网关设置列表。有关详细信息，请参阅第 9-4 页的**网关设置导入程序**。
4. 单击**保存**。

网关设置导入程序

防毒墙网络版检查计算机的位置，以确定要使用的 Web 信誉策略和要连接到的云安全服务器。防毒墙网络版识别位置的一种方法是通过检查计算机的网关 IP 地址和 MAC 地址。

可以在“计算机位置”窗口上配置网关设置，或者使用网关设置导入程序工具将网关设置列表导入到“计算机位置”窗口。

使用网关设置导入程序：

1. 准备包含网关设置列表的文本文件 (.txt)。在每一个行上，键入 IP 地址，也可根据需要键入 MAC 地址。使用半角逗号分隔 IP 地址和 MAC 地址。最大条目数为 4096。

例如：

10.1.111.222,00:17:31:06:e6:e7

10.1.111.223

10.1.111.224,00:17:31:06:e6:e7

2. 在服务器计算机上，转至 <服务器安装文件夹>\PCCSRV\Admin\Utility\GatewaySettingsImporter，然后双击 **GSImporter.exe**。

注意： 不能通过终端服务运行网关设置导入程序工具。

3. 在“网关设置导入程序”窗口上，浏览到在步骤 1 中创建的文件，然后单击**导入**。
4. 单击**确定**。网关设置显示在“计算机位置”窗口上，防毒墙网络版服务器会将设置部署到客户端。
5. 要删除所有条目，请单击**全部清除**。如果仅需要删除特定条目，则从**计算机位置**窗口将其删除。
6. 要将设置导出到文件，请单击**全部导出**，然后指定文件名和类型。

客户端权限和其他设置

授予用户在防毒墙网络版客户端上修改特定设置和执行高级别任务的权限。

提示: 要在整个组织内执行统一的设置和策略，请授予用户有限的权限。

配置权限及其他设置:

导航路径: 联网计算机 > 客户端管理 > 设置 > 权限和其他设置

1. 单击**权限**选项卡，然后配置下列用户权限:

- **漫游权限**
- **扫描权限**
- **预设扫描权限**
- **防火墙权限**
- **邮件扫描权限**
- **工具箱权限**
- **代理服务器设置权限**
- **组件更新权限**
- **卸载**
- **退出**

2. 单击**其他设置**选项卡，然后配置下列设置:

- **更新设置**
- **Web 信誉设置**
- **预设扫描设置**
- **客户端安全设置**
- **POP3 电子邮件扫描设置**
- **客户端控制台访问限制**
- **重新启动通知**

3. 如果在客户端树上选择域或客户端，请单击**保存**将设置应用到域或客户端。如果选择根图标 ，则从下列选项进行选择：
- **应用到全部客户端：**将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - **仅应用到将来的域：**仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

漫游权限

此权限允许用户启用漫游模式。在漫游模式下时，客户端不能通过防毒墙网络版服务器更新组件，也不能将日志发送到服务器。防毒墙网络版服务器也不能管理漫游客户端，包括启动任务和部署客户端设置。有关详细信息，请参阅第 9-33 页的 [漫游客户端](#)。

扫描权限

这些权限允许用户通过打开客户端控制台并选择**设置 > {扫描类型}**，来配置他们自己的手动扫描、实时扫描和预设扫描设置。



图 9-2. 客户端控制台上的扫描设置

下列设置是可配置的：

- 手动扫描：**要扫描的文件**、**扫描设置**、**CPU 使用率**、**扫描例外**、**扫描处理措施**
- 实时扫描：**用户对文件执行的活动**、**要扫描的文件**、**扫描设置**、**扫描例外**、**扫描处理措施**
- 预设扫描：**时间表**、**要扫描的文件**、**扫描设置**、**CPU 使用率**、**扫描例外**、**扫描处理措施**

预设扫描权限

设置为运行预设扫描的客户端可以具有推迟和跳过/停止预设扫描的权限。要允许用户利用这些权限，请通过配置防毒墙网络版在预设扫描运行前显示通知消息来提醒用户已授予他们的权限。

要显示通知消息，请转至**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > “其他设置”选项卡 > 预设扫描设置**，并启用**开始预设扫描前显示通知**。

通知消息在预设扫描运行前显示分钟数。要配置分钟数，请转至**联网计算机 > 全局客户端设置 > 预设扫描设置 > 在预设扫描开始前 __ 分钟提醒用户**。

推迟预设扫描

具有“推迟预设扫描”权限的用户可以执行下列操作：

- 在预设扫描运行前推迟预设扫描，然后指定推迟的时间长度。预设扫描只能推迟一次。
- 如果预设扫描正在进行中，则用户可以停止扫描并在以后重新启动它。然后，用户指定扫描重新开始前应经过的时间长度。当扫描重新开始时，所有以前扫描过的文件都会再扫描一遍。预设扫描在停止后只能重新启动一次。

注意： 用户可以指定的最小推迟时间长度/所用时间为 15 分钟。最大值为 12 小时 45 分钟，您可以转至**联网计算机 > 全局客户端设置 > 预设扫描设置 > 预设扫描最长推迟时间为 __ 小时 __ 分钟**来减少该时间。

跳过和停止预设扫描

启用此选项后，用户可以执行以下操作：

- 在预设扫描运行前跳过预设扫描
- 在预设扫描正在进行时停止预设扫描

在客户端计算机上推迟/跳过和停止预设扫描：

如果预设扫描尚未启动：

1. 右键单击系统托盘上的防毒墙网络版客户端图标，然后选择**预设扫描高级设置**。

注意： 如果通知消息已启用并设置为在预设扫描运行前显示分钟数，则用户无需执行此步骤。

2. 在所显示的通知窗口上，从下列选项中进行选择：
 - 推迟扫描 __ 小时 __ 分钟。
 - 跳过此预设扫描。下一次预设扫描在 <date> 的 <time> 运行。

如果预设扫描正在进行：

1. 右键单击系统托盘上的防毒墙网络版客户端图标，然后选择**预设扫描高级设置**。
2. 在所显示的通知窗口上，从下列选项中进行选择：
 - 停止扫描。在以下时间之后重新启动: __ 小时 __ 分钟。
 - 停止扫描。下一次预设扫描在 <date> 的 <time> 运行。

防火墙权限

防火墙权限允许用户配置他们自己的防火墙设置。所有用户配置的设置都不能被从防毒墙网络版服务器部署的设置所覆盖。例如，如果用户禁用了“入侵检测系统 (IDS)”，而您在防毒墙网络版服务器上启用了 IDS，则 IDS 在客户端计算机上仍然是禁用的。

在客户端控制台上显示“防火墙”选项卡

“防火墙”选项卡显示客户端上的所有防火墙设置并允许具有防火墙权限的用户配置他们自己的设置。

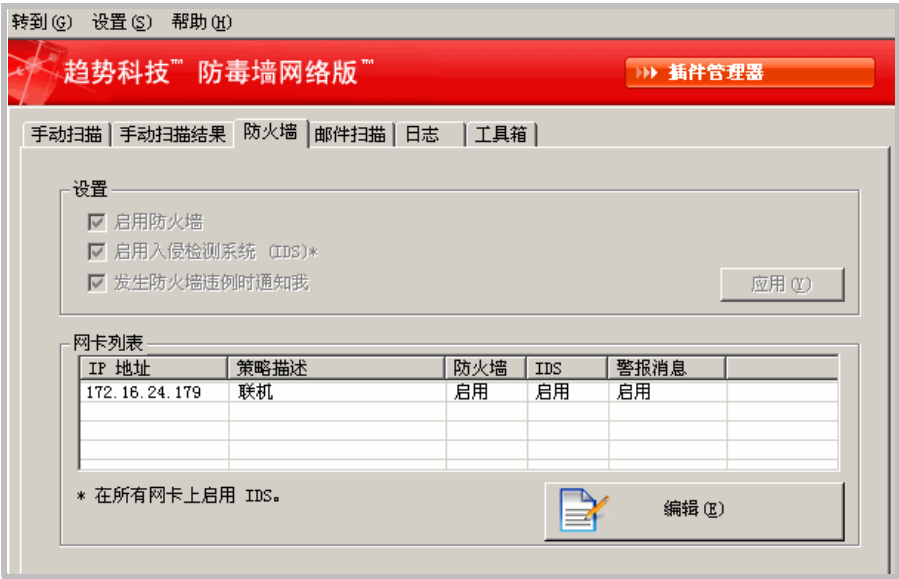


图 9-3. 客户端控制台上的“防火墙”选项卡

允许用户启用/禁用防毒墙网络版防火墙、入侵检测系统和防火墙违例通知消息

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端。如果授予用户启用或禁用该防火墙及其功能的权限，则警告他们不要长时间禁用该防火墙以避免计算机遭到入侵和黑客的攻击。

如果不授予用户这些权限，则从防毒墙网络版服务器 Web 控制台配置的防火墙设置将显示在客户端控制台上的**网卡列表**下。

允许客户端向防毒墙网络版服务器发送防火墙日志

选择此选项分析防毒墙网络版防火墙阻止和允许的网络通信。如果选择了此选项，请在**联网计算机 > 全局客户端设置 > 防火墙日志设置**部分中配置日志发送时间表。该时间表仅适用于具有防火墙日志发送权限的客户端。

要查看防火墙日志，请参阅第 7-17 页的[防火墙日志](#)。

邮件扫描权限

当客户端具有邮件扫描权限时，客户端控制台上将显示**邮件扫描**选项卡。邮件扫描包括 Outlook 邮件扫描和 POP3 邮件扫描。

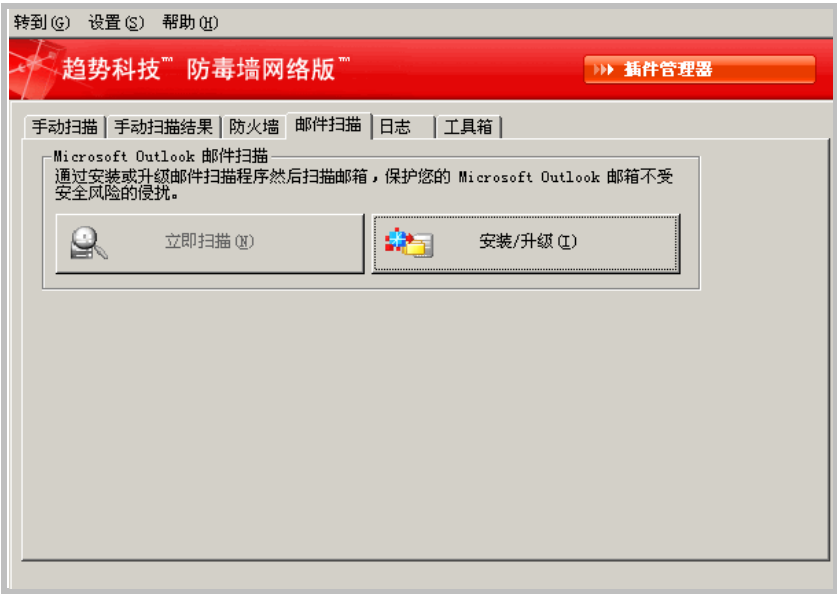


图 9-4. 客户端控制台上的“邮件扫描”选项卡

防毒墙网络版客户端不在客户端控制台的日志窗口中显示邮件扫描结果，也不将邮件扫描日志发送给服务器。Outlook 和 POP3 邮件扫描日志分别存储在客户端计算机上各自的日志文件中。有关邮件扫描日志的详细信息，请参阅第 12-10 页的[邮件扫描日志](#)和第 12-13 页的[Web 信誉和 POP3 邮件扫描日志](#)。

Outlook 邮件扫描

当客户端控制台上显示**邮件扫描**选项卡时，客户端用户可以立即配置 Outlook 邮件扫描设置，然后运行手动扫描以针对病毒或恶意软件扫描 Microsoft Outlook 电子邮件和附件。

注意： Outlook 邮件扫描不扫描间谍软件/灰色软件。

Outlook 邮件扫描是用户启动的扫描，这意味着仅当用户从**邮件扫描**选项卡运行手动扫描时才进行扫描。它不实时扫描电子邮件，并且不能配置为基于时间表自动运行。

POP3 邮件扫描

POP3 邮件扫描实时检查电子邮件和附件中的病毒/恶意软件，即在从 POP3 邮件服务器下载电子邮件时进行检查。要在**邮件扫描**选项卡上显示 POP3 邮件扫描配置选项，请转至**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 其他设置**选项卡并选择**扫描 POP3 电子邮件**。

注意： POP3 邮件扫描不扫描间谍软件/灰色软件。

POP3 邮件扫描仅实时扫描电子邮件。用户不能从客户端控制台手动启动扫描，并且不能将扫描配置为基于时间表自动运行。

不能通过 Web 控制台配置防毒墙网络版可对病毒/恶意软件采取的处理措施。用户在客户端控制台上配置处理措施。

POP3 邮件扫描程序与 Web 信誉程序共享防毒墙网络版 NT 代理服务 (TMPProxy.exe)。

工具箱权限

启用此权限时，客户端控制台上显示**工具箱**选项卡。“防火墙”选项卡允许用户安装 Check Point SecureClient 支持。防毒墙网络版提供一个工具，可使 Check Point SecureClient 检查客户端病毒码和病毒扫描引擎是否最新。



图 9-5. 客户端控制台上的“工具箱”选项卡

代理服务器设置权限

此权限允许客户端用户配置代理服务器设置。防毒墙网络版仅在以下实例上才使用用户配置的代理服务器设置：

- 客户端执行“立即更新”时。有关“立即更新”功能的信息，请参阅第 9-15 页的[组件更新权限](#)。
- 用户禁用自动代理服务器，或防毒墙网络版无法检测到自动代理服务器设置时。请参阅[第 9-29 页的代理服务器配置](#)以获取详细信息。

组件更新权限

更新权限允许客户端用户配置他们自己的更新设置。

执行“立即更新”

具有此权限的用户可以通过右键单击系统托盘上的防毒墙网络版图标并选择**立即更新**按需更新组件。还可以配置客户端以在“立即更新”过程中使用代理服务器设置。有关详细信息，请参阅第 9-29 页的[代理服务器配置](#)。

启用预设更新

此权限允许客户端用户启用/禁用预设更新。虽然用户具有启用/禁用预设更新的权限，但是他们无法配置实际时间表。必须在**更新 > 联网计算机 > 自动更新 > 基于时间表更新**中指定时间表。

卸载

此权限允许用户卸载（需要密码或无需密码）防毒墙网络版客户端。要从 Web 控制台启动静默客户端卸载，请转至**联网计算机 > 客户端管理 > 任务 > 客户端卸载**。

退出

此权限允许用户临时停止（需要密码或无需密码）防毒墙网络版客户端。

更新设置

客户端从趋势科技 ActiveUpdate 服务器下载更新

启动更新时，防毒墙网络版客户端首先从**更新 > 联网计算机 > 更新源**窗口中指定的更新源中获取更新。如果更新未成功，则客户端会尝试从防毒墙网络版服务器进行更新。如果从防毒墙网络版服务器更新未成功，则选择此选项可使客户端能够尝试从趋势科技 ActiveUpdate 服务器进行更新。

启用预设更新

选择此选项会强制所选客户端始终运行预设更新，除非用户具有启用/禁用预设更新的权限，并且用户禁用预设更新。有关该权限的详细信息，请参阅第 9-15 页的[组件更新权限](#)。

在**更新 > 联网计算机 > 自动更新 > 基于时间表更新**中指定更新时间表。

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

此选项允许继续进行组件更新，但是会阻止部署 Hotfix 和升级客户端。

如果不选择此选项，则所有客户端将同时连接到服务器进行升级或安装 hotfix。如果客户端数量很多，这可能极大地影响服务器性能。如果选择此选项，请计划如何将客户端升级或 hotfix 部署对服务器造成的影响降到最小，然后执行您的计划。

Web 信誉设置

防毒墙网络版在阻止违反 Web 信誉策略的 URL 后，会立即在客户端计算机上显示一条通知消息。此外，还可以通过转至**通知 > 客户端用户通知 > Web 信誉策略违例**选项卡来修改通知消息的内容。

预设扫描设置

启用此选项时，通知消息将在预设扫描运行前几分钟在客户端计算机上显示。系统会向用户通知扫描时间表（日期和时间）及其预设扫描权限，如推迟、跳过或停止预设扫描。有关预设扫描权限的详细信息，请参阅第 9-8 页的[预设扫描权限](#)。

分钟数是可配置的。要配置分钟数，请转至**联网计算机 > 全局客户端设置 > 预设扫描设置 > 在预设扫描开始前 __ 分钟提醒用户**。

客户端安全设置

此设置允许或限制用户访问防毒墙网络版客户端文件与注册表。

如果选择了“高”，则防毒墙网络版文件夹、文件和注册表的访问权限设置将与运行 Windows 2000/XP/Server 2003 的客户端计算机的 Program Files 文件夹的设置相同。

因此，如果 Program Files 文件夹的权限设置（Windows 中的“安全”设置）设置为允许完全读取/写入访问，则选择“高”依然允许用户对防毒墙网络版客户端文件夹、文件和注册表进行完全读取/写入访问。

POP3 电子邮件扫描设置

选择时，此设置在客户端控制台上启用 POP3 邮件扫描。此设置仅适用于具有邮件扫描权限的客户端。有关详细信息，请参阅第 9-12 页的[邮件扫描权限](#)。

客户端控制台访问限制

此设置不允许从系统托盘或 Windows “开始”菜单访问客户端控制台。从<[客户端安装文件夹](#)>单击 **PccNT.exe** 是用户访问客户端控制台的唯一方式。配置此设置后，请重新加载客户端，以使该设置生效。

此设置不禁用防毒墙网络版客户端。客户端在后台运行并继续提供抵御安全风险的保护。

重新启动通知

选择此选项可显示一则消息，提示用户重新启动客户端计算机以完成清除受感染文件。

对于实时扫描，该消息会在已扫描特定安全风险后显示。对于手动扫描、预设扫描和立即扫描，该消息仅在防毒墙网络版扫描完所有扫描目标后显示一次。

全局客户端设置

防毒墙网络版可将全局客户端设置应用于所有客户端，或者只应用于具有特定权限的客户端。

配置全局客户端设置：

导航路径：联网计算机 > 全局客户端设置

1. 配置下列设置：

- [扫描设置](#)
- [预设扫描设置](#)
- [Web 信誉允许的 URL 列表](#)
- [防火墙日志设置](#)
- [警报设置](#)
- [防毒墙网络版服务重新启动](#)
- [客户端自我保护](#)
- [保留的磁盘空间](#)
- [网络病毒日志整合](#)
- [病毒/恶意软件日志带宽设置](#)
- [代理服务器配置](#)
- [客户端分组](#)

2. 单击保存。

扫描设置

配置大型压缩文件的扫描设置

在手动扫描、实时扫描、预设扫描和立即扫描期间，扫描每个层中是否有病毒/恶意软件和间谍软件/灰色软件，服务器管理的所有客户端将检查以下设置：

如果压缩文件大小超过 __ MB，则不扫描其中的文件

防毒墙网络版不扫描超过该限制的任何文件。

对于压缩文件，仅扫描前 __ 个文件

在解压缩压缩文件之后，防毒墙网络版扫描指定数目的文件，而忽略其余文件（如果有）。

扫描 OLE 对象，最大层数： __

当文件包含多个对象链接与嵌入 (OLE) 层时，防毒墙网络版最多扫描指定的层数，而跳过其余层。

在手动扫描、实时扫描、预设扫描和立即扫描期间，服务器管理的所有客户端会检查此设置。扫描每个层中是否有病毒/恶意软件和间谍软件/灰色软件。

例如：

指定的层数是 2。文件中嵌入一个 Microsoft Word 文档（第一层），Word 文档中有一个 Microsoft Excel 电子表格（第二层），电子表格中有一个 JPG 文件（第三层）。防毒墙网络版将扫描 Word 文档和 Excel 电子表格，而跳过 JPG 文件。

将手动扫描添加到客户端计算机的 Windows 快捷菜单中

启用此设置时，服务器管理的所有客户端都将使用**防毒墙网络版客户端扫描**选项添加到 Windows 资源管理器的右键单击菜单中。当用户右键单击 Windows 桌面上或 Windows 资源管理器中的文件或文件夹并选择该选项时，手动扫描将扫描该文件或文件夹中是否有病毒/恶意软件和间谍软件/灰色软件。

从实时扫描中排除防毒墙网络版服务器数据库文件夹

如果防毒墙网络版客户端和服务端位于同一台计算机上，则客户端在实时扫描期间不会扫描服务器数据库中是否有病毒/恶意软件和间谍软件/灰色软件。

提示： 启用此设置可防止扫描期间可能发生的数据库损坏。

从扫描中排除 Microsoft Exchange 服务器文件夹

如果防毒墙网络版客户端与 Microsoft Exchange 2000/2003 服务器位于同一台计算机上，则在手动扫描、实时扫描、预设扫描和立即扫描期间，防毒墙网络版不会扫描 Exchange 服务器文件夹中是否有病毒/恶意软件和间谍软件/灰色软件。

对于 Microsoft Exchange 2007 文件夹，需要手动将这些文件夹添加到扫描例外列表。有关扫描例外详细信息，请访问以下 Web 站点：

<http://technet.microsoft.com/en-us/library/bb332342.aspx>

有关配置扫描例外列表的步骤，请参阅第 5-26 页的 *扫描例外*。

清除/删除压缩文件中的受感染文件

当服务器管理的所有客户端在手动扫描、实时扫描、预设扫描和立即扫描期间在压缩文件中检测到病毒/恶意软件时，如果满足以下条件，则客户端将清除或删除受感染文件。

- “**清除**”或“**删除**”是防毒墙网络版设置执行的措施。通过转至**联网计算机 > 客户端管理 > {扫描类型} > 处理措施**选项卡，查看防毒墙网络版对受感染文件采取的措施。
- 启用该设置。启用此设置可能增加扫描期间的计算机资源占用，扫描可能要用更长时间才能完成。这是因为防毒墙网络版需要解压缩压缩文件，清除或删除压缩文件中的受感染文件，然后重新压缩该文件。

- 支持该压缩文件格式。防毒墙网络版仅支持某些压缩文件格式，包括 ZIP 和 Office Open XML（使用 ZIP 压缩技术）。Office Open XML 是 Microsoft Office 2007 应用程序（例如 Excel、PowerPoint 和 Word）的缺省格式。

注意： 有关支持的压缩文件格式的完整列表，请联系技术支持提供商。

例如，将实时扫描设置为删除受病毒感染的文件。在实时扫描解压缩名为 *abc.zip* 的压缩文件并在压缩文件中检测到受感染文件 *123.doc* 之后，防毒墙网络版将删除 *123.doc*，然后重新压缩 *abc.zip*，现在可以对其进行安全访问。

下表说明了在不符合所有这些条件时会发生的情况。

表 9-1. 压缩文件情形和结果

“清除/删除压缩文件中的受感染文件”的状态	防毒墙网络版设置执行的处理措施	压缩文件格式	结果
已启用	清除或删除	不支持 示例: <i>def.rar</i> 包含受感染文件 <i>123.doc</i> 。	防毒墙网络版加密 <i>def.rar</i> ，但不会对 <i>123.doc</i> 执行清除、删除或任何其他处理措施。
已禁用	清除或删除	支持/不支持 示例: <i>abc.zip</i> 包含受感染文件 <i>123.doc</i> 。	防毒墙网络版不会对 <i>abc.zip</i> 和 <i>123.doc</i> 执行清除、删除或任何其他处理措施。

表 9-1. 压缩文件情形和结果（续）

“清除/删除压缩文件中的受感染文件”的状态	防毒墙网络版设置执行的 处理措施	压缩文件格式	结果
已启用/ 已禁用	非清除或删除 （即执行以下 之一：更名、隔 离、拒绝访问或 不予处理）	支持/不支持 示例： <i>abc.zip</i> 包含受感染文件 <i>123.doc</i> 。	防毒墙网络版对 <i>abc.zip</i> 而 不是 <i>123.doc</i> 执行配置的 处理措施（更名、隔离、 拒绝访问或不予处理）。 如果处理措施为： 更名： 防毒墙网络版会将 <i>abc.zip</i> 更名为 <i>abc.vir</i> ，但 不会更名 <i>123.doc</i> 。 隔离： 防毒墙网络版会隔离 <i>abc.zip</i> （ <i>123.doc</i> 和所有 未感染的文件都会被隔离）。 不予处理： 防毒墙网络版不 会对 <i>abc.zip</i> 和 <i>123.doc</i> 执行任何处理措施，但会 记录病毒检测情况。 拒绝访问： 在打开 <i>abc.zip</i> 时防毒墙网络版会拒绝对它 的访问（ <i>123.doc</i> 和所有 未感染文件都无法打开）。

启用评估模式

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，然后根据您的评估采取适当的处理措施。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](#)。

在评估模式下时，防毒墙网络版会执行以下扫描处理措施：

- **不予处理**：在手动扫描、预设扫描和立即扫描期间
- **拒绝访问**：在实时扫描期间

注意： 评估模式会覆盖任何用户配置的扫描处理措施。例如，即使您在手动扫描期间选择“清除”作为扫描处理措施，当客户端处于评估模式下时，“不予处理”仍保留为扫描处理措施。

扫描 Cookie

如果将 Cookie 视为潜在的安全风险，则选择此选项。选择此选项后，在手动扫描、预设扫描、实时扫描和立即扫描期间，服务器管理的所有客户端都将扫描 Cookie 中是否有间谍软件/灰色软件。

预设扫描设置

仅设置为运行预设扫描的客户端使用下列设置。预设扫描可以扫描病毒/恶意软件和间谍软件/灰色软件。

在预设扫描开始前 __ 分钟提醒用户

防毒墙网络版将在预设扫描运行前数分钟显示一条通知消息，以提醒用户扫描时间表（日期和时间）和您授予他们的任何预设扫描权限。

通过转至**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > “其他设置”选项卡 > 预设扫描设置**，可以启用/禁用通知消息。禁用时，不显示提醒。

预设扫描最长推迟时间为 __ 小时 __ 分钟

只有具有“推迟预设扫描”权限的用户才可以执行下列操作：

- 在预设扫描运行前推迟预设扫描，然后指定推迟的时间长度。
- 如果预设扫描正在进行中，则用户可以停止扫描并在以后重新启动它。然后，用户指定扫描重新开始前应经过的时间长度。当扫描重新开始时，所有以前扫描过的文件都会再扫描一遍。

用户可以指定的最大推迟时间长度/所用时间为 12 小时 45 分钟，您可以在提供的文本框中指定小时数和/或分钟数来减少该时间。

当预设扫描持续时间超过 __ 小时 __ 分钟时自动停止扫描

超过指定的时间长度且扫描尚未完成时，防毒墙网络版将停止扫描。防毒墙网络版会立即将在扫描期间检测到的任何安全风险通知给用户。

当便携计算机的电池组可用时间低于 __ % 且其交流电适配器未插电时跳过预设扫描

如果防毒墙网络版检测到便携计算机的电池电量很低且交流电适配器没有连接到任何电源上，则当预设扫描启动时防毒墙网络版会立即跳过扫描。如果电池电量很低，但交流电适配器已连接到电源上，则扫描会继续进行。

继续未执行的预设扫描

如果因防毒墙网络版在预设扫描的日期和时间没有运行，从而预设扫描未启动，则当防毒墙网络版在设置预设扫描运行的确切时间运行时，将会启动扫描，而不考虑日期。

防火墙日志设置

可以授予某些客户端向防毒墙网络版服务器发送防火墙日志的权限。在此部分中配置日志发送时间表。只有具有发送防火墙日志权限的客户端可使用此时间表。

有关可用于所选客户端的防火墙权限的信息，请参阅第 9-10 页的[防火墙权限](#)。

警报设置

防毒墙网络版可以在以下实例中显示通知：

如果传统病毒码文件在 __ 天后没有更新则在 Windows 任务栏上显示警报图标

警报图标在 Windows 任务栏上显示，提醒用户更新病毒码。服务器管理的所有客户端都将应用此设置。

如果客户端计算机需要重新启动以加载内核模式驱动程序，则显示通知消息

安装 Hotfix 或包括新版本的内核模式驱动程序的升级软件包后，驱动程序的前一版本可能仍然在计算机上。退出前一版本并安装新版本的唯一方法是重新启动计算机。重新启动计算机后，将自动安装新版本，无需再重新启动。

客户端计算机在安装 Hotfix 或升级软件包后，通知消息会立即显示。

防毒墙网络版服务重新启动

防毒墙网络版重新启动意外停止响应（而不是由正常系统进程停止）的客户端服务。

配置下列设置以重新启动客户端服务：

防毒墙网络版客户端服务意外终止后，自动重新启动该服务

防毒墙网络版重新启动下列服务：

- **OfficeScan NT Listener (tmlisten.exe)：**接收来自防毒墙网络版服务器的命令和通知，并简化客户端到服务器的通信
- **OfficeScanNT RealTime Scan (ntrtscan.exe)：**对防毒墙网络版客户端执行实时扫描、预设扫描和手动扫描
- **OfficeScan NT Proxy Service (TmProxy.exe)：**在将网络通信传递给目标应用程序之前，先对其进行扫描。

__ 分钟后重新启动服务

服务停止时，防毒墙网络版在重新启动服务前等待若干分钟。

如果首次尝试重新启动服务不成功，请重试 __ 次

指定重新启动服务的最大重试次数。如果服务在最大重试次数后仍然停止，则手动重新启动服务。

__ 小时后重置重新启动失败计数

如果服务在用尽最大重试次数后仍然停止，则防毒墙网络版会等待若干小时，然后重置失败计数。如果这些小时过后服务仍然停止，则防毒墙网络版会重新启动服务。

客户端自我保护

客户端自我保护为防毒墙网络版客户端提供保护其正常运行所需的进程及其他资源的方式。客户端自我保护帮助阻止程序或实际用户尝试禁用防恶意软件防护。

保护防毒墙网络版客户端安装文件夹中的文件

为防止其他程序（甚至用户）修改或删除防毒墙网络版文件，防毒墙网络版在根 <[客户端安装文件夹](#)> 中锁定了以下文件：

- 扩展名为 .exe、.dll 和 .sys 的所有数字签名的文件
- 某些不具有数字签名的文件包括：
 - bspatch.exe
 - bzip2.exe
 - INETWH32.dll
 - libcurl.dll
 - libeay32.dll
 - libMsgUtilExt.mt.dll
 - msvcm80.dll
 - MSVCP60.DLL
 - msvcp80.dll
 - msver80.dll
 - OfceSCV.dll
 - OFCESCVPack.exe
 - patchbld.dll
 - patchw32.dll
 - patchw64.dll
 - PiReg.exe
 - ssleay32.dll
 - Tmeng.dll
 - TMNotify.dll
 - zlibwapi.dll

保护防毒墙网络版客户端进程

防毒墙网络版阻止终止下列进程的所有尝试：

- **tmlisten.exe**：接收来自防毒墙网络版服务器的命令和通知，并简化客户端到服务器的通信
- **ntrtscan.exe**：对防毒墙网络版客户端执行实时扫描、预设扫描和手动扫描
- **TmProxy.exe**：在将网络通信传递给目标应用程序之前，先对其进行扫描
- **TmPfw.exe**：提供数据包级防火墙、网络病毒扫描和入侵检测能力
- **TMBMSRV.exe**：控制对外部存储设备的访问并阻止对注册码和进程的未授权更改

注意： 在此版本中，只能将此设置部署到运行 x86 类型处理器的客户端。

保护防毒墙网络版客户端注册码

防毒墙网络版阻止修改、删除下列注册码和子键下的条目或者向其中添加新条目的所有尝试：

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMCSS

注意： 在此版本中，只能将此设置部署到运行 x86 类型处理器的客户端。

保留的磁盘空间

防毒墙网络版可以为 Hotfix、病毒码文件、扫描引擎和程序更新分配一定量的客户端磁盘空间。缺省情况下，防毒墙网络版保留 60MB 的磁盘空间。

网络病毒日志整合

启用此选项时，防毒墙网络版客户端仅每小时向服务器发送一次网络病毒日志。有关网络病毒的详细信息，请参阅第 5-4 页的[网络病毒](#)。

病毒/恶意软件日志带宽设置

在较短时间内检测到多处由同一病毒/恶意软件导致的感染时，防毒墙网络版将整合病毒日志条目。防毒墙网络版可多次检测到同一单个病毒/恶意软件，从而在客户端将日志信息发送到服务器时快速填写病毒/恶意软件日志并占用网络带宽。启用此功能可帮助在将病毒日志信息报告给服务器时同时减少所生成的病毒/恶意软件日志条目数和客户端占用的网络带宽量。

代理服务器配置

手动配置代理服务器设置对于许多终端用户而言是个复杂的任务。使用自动代理服务器设置可以确保在不需要任何用户干预的情况下应用正确的代理服务器设置。

如果启用，则客户端通过自动更新或立即更新更新组件时，自动代理服务器设置将用作主代理服务器设置。有关自动更新和立即更新的信息，请参阅第 4-25 页的[客户端更新方法](#)。

如果客户端无法使用自动代理服务器设置连接，则具有配置代理服务器设置权限的客户端用户可以使用用户配置的代理服务器设置。否则，使用自动代理服务器设置的连接将不成功。

注意： 代理服务器认证不受支持。

自动检测设置

防毒墙网络版通过 DHCP 或 DNS 自动检测管理员配置的代理服务器设置。

使用自动配置脚本

防毒墙网络版使用网络管理员设置的代理服务器自动配置 (PAC) 脚本检测适当的代理服务器。

客户端分组

此设置仅在客户端安装期间使用。安装程序检查目标计算机所属的网络域。如果客户端树已存在该域名，则目标计算机上的客户端将分组到该域下，并应用为该域配置的设置。如果该域名不存在，则防毒墙网络版将该域添加到该客户端树上，将该客户端分组到该域下，然后将根设置应用到该域和该客户端。

指定安装程序将检查 NetBIOS、Active Directory 还是 DNS 域名。

客户端与服务器的连接

客户端计算机的系统托盘上的图标指示客户端与防毒墙网络版服务器及云安全服务器（如果客户端使用[云安全扫描](#)）的连接状态。

当图标指示以下情况之一时，用户需要采取处理措施：

- 暂时尚未更新特征码。
- 实时扫描已禁用。
- 实时扫描服务已停止。防毒墙网络版不仅将实时扫描服务用于实时扫描，还用于手动扫描和预设扫描。这表示如果实时扫描服务停止，客户端计算机将失去保护。
- 未将云安全客户端连接到任何云安全服务器。

有关这些情况之一发生时用户可以执行的步骤，请参阅第 9-35 页的[所需处理措施](#)。

联机客户端

联机客户端与服务器保持持续的连接。防毒墙网络版服务器可以启动任务并将设置部署到这些客户端。

表 9-2. 联机客户端图标

图标	扫描方法	描述
	传统扫描	所有组件为最新并且服务工作正常。
	传统扫描	特征码文件暂时尚未更新。 实时扫描已启用。
	传统扫描	实时扫描已禁用。
	传统扫描	特征码文件暂时尚未更新。 实时扫描已禁用。
	传统扫描	实时扫描服务已停止。
	传统扫描	特征码文件暂时尚未更新。 实时扫描服务已停止。
	云安全扫描	客户端可以连接到云安全服务器。 所有服务正常工作。
	云安全扫描	客户端可以连接到云安全服务器。 实时扫描已禁用。
	云安全扫描	客户端可以连接到云安全服务器。 实时扫描服务已停止。
	云安全扫描	客户端无法连接到云安全服务器。 实时扫描已启用。

表 9-2. 联机客户端图标（续）

图标	扫描方法	描述
	云安全扫描	客户端无法连接到云安全服务器。 实时扫描已禁用。
	云安全扫描	客户端无法连接到云安全服务器。 实时扫描服务已停止。

脱机客户端

脱机客户端与服务器断开连接。防毒墙网络版服务器无法管理这些客户端。

表 9-3. 脱机客户端图标

图标	扫描方法	描述
	传统扫描	实时扫描已启用。
	传统扫描	特征码文件暂时尚未更新。 实时扫描已启用。
	传统扫描	实时扫描已禁用。
	传统扫描	特征码文件暂时尚未更新。 实时扫描已禁用。
	传统扫描	实时扫描服务已停止。
	传统扫描	特征码文件暂时尚未更新。 实时扫描服务已停止。
	云安全扫描	客户端可以连接到云安全服务器。 实时扫描已启用。

表 9-3. 脱机客户端图标（续）

图标	扫描方法	描述
	云安全扫描	客户端可以连接到云安全服务器。 实时扫描已禁用。
	云安全扫描	客户端可以连接到云安全服务器。 实时扫描服务已停止。
	云安全扫描	客户端无法连接到云安全服务器。
	云安全扫描	客户端无法连接到云安全服务器。 实时扫描已禁用。
	云安全扫描	客户端无法连接到云安全服务器。 实时扫描服务已停止。

漫游客户端

漫游客户端不能通过防毒墙网络版服务器更新组件，也不能将日志发送到服务器。防毒墙网络版服务器也无法启动任务并将客户端设置部署到漫游客户端。根据各种因素（如客户端计算机的位置或网络连接状态），漫游客户端也许可以与防毒墙网络版服务器通信，也许不能。

具有漫游权限的用户可以在防毒墙网络版服务器干预（如服务器启动的扫描）阻止他们完成某项任务（例如，执行演示时）时启用漫游模式。具有 Internet 连接的漫游客户端如果配置为从更新代理或趋势科技 ActiveUpdate 服务器获取更新，则其仍可以更新组件。

为长期与防毒墙网络版服务器失去连接的客户端分配漫游权限。要分配该权限，请转至**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 权限**选项卡。

只在以下情形中才会发生对漫游客户端的更新：

- 客户端用户执行手动更新时
- 设置包括漫游客户端的自动更新部署时
- 授予了客户端启用预设更新的权限时

有关如何更新客户端的详细信息，请参阅第 4-21 页的[客户端更新](#)。

表 9-4. 漫游客户端图标

图标	扫描方法	描述
	传统扫描	实时扫描已启用。
	传统扫描	实时扫描已禁用。
	传统扫描	特征码文件暂时尚未更新。 实时扫描已启用。
	传统扫描	特征码文件暂时尚未更新。 实时扫描已禁用。
	传统扫描	实时扫描服务已停止。
	传统扫描	特征码文件暂时尚未更新。 实时扫描服务已停止。
	云安全扫描	客户端可以连接到云安全服务器。 实时扫描已启用。
	云安全扫描	客户端可以连接到云安全服务器。 实时扫描已禁用。
	云安全扫描	客户端可以连接到云安全服务器。 实时扫描服务已停止。
	云安全扫描	客户端无法连接到云安全服务器。 实时扫描已禁用。

表 9-4. 漫游客户端图标（续）

图标	扫描方法	描述
	云安全扫描	客户端无法连接到云安全服务器。 实时扫描已禁用。
	云安全扫描	客户端无法连接到云安全服务器。 实时扫描服务已停止。

所需处理措施

如果客户端图标表示以下情况中的任意一种，则请执行必要的操作：

暂时尚未更新特征码文件

客户端用户需要更新组件。从 Web 控制台中，在**更新 > 联网计算机**中配置组件更新设置，或者在**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 权限选项卡 > 组件更新权限**中向用户授予更新权限。

实时扫描服务已停止

用户可以通过单击**开始 > 运行**，并键入 **services.msc** 从 Microsoft 管理控制台手动启动服务（OfficeScanNT RealTime Scan）。

实时扫描已禁用

从 Web 控制台启用实时扫描（**联网计算机 > 客户端管理 > 设置 > 实时扫描设置**）。

实时扫描已禁用且客户端处于漫游模式下

用户需要先禁用漫游模式。禁用漫游模式后，请从 Web 控制台中启用实时扫描。

公司网络中的客户端已断开与服务器的连接

从 Web 控制台验证连接（[联网计算机 > 连接验证](#)），然后再检查连接验证日志（[日志 > 联网计算机日志 > 连接验证](#)）。

如果验证后客户端仍处于断开连接状态：

1. 如果连接状态在服务器和客户端上均为脱机，则请检查网络连接。
2. 如果连接状态在客户端上为脱机但在服务器上为联机，则服务器域名可能已更改，而客户端使用该域名连接到服务器（如果在服务器安装过程中选择了域名）。将防毒墙网络版服务器的域名注册到 DNS 或 WINS 服务器，或将该域名和 IP 信息添加到客户端计算机的 <Windows folder>\system32\drivers\etc 文件夹中的“hosts”文件。
3. 如果连接状态在客户端上为联机但在服务器上为脱机，请检查防毒墙网络版防火墙设置。防火墙可能会阻止服务器到客户端的通信，但是会允许客户端到服务器的通信。
4. 如果连接状态在客户端上为联机但在服务器上为脱机，则客户端的 IP 地址可能已更改，但是其状态未反映在服务器上（例如，重新加载客户端时）。请尝试重新部署客户端。

客户端无法连接到云安全服务器

1. 检查是否已正确配置下列[计算机位置](#)设置：
 - 参考服务器和端口号
 - 网关 IP 地址
2. 检查标准或自定义扫描服务器列表上的云安全服务器地址是否正确。
3. 测试是否可以建立使用服务器地址的连接。还要确保在配置列表后单击[通知所有客户端](#)。有关详细信息，请参阅第 5-14 页的[云安全扫描源](#)。
4. 检查云安全服务器和防毒墙网络版客户端上的下列配置文件是否同步：
 - sscfg.ini
 - ssnotify.ini

5. 从注册表验证客户端是否已连接到公司网络。
- 键：
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC Scan\Scan Server
- 如果 LocationProfile=1，则客户端已连接到网络，并且应该连接到本地云安全服务器。
 - 如果 LocationProfile=2，则客户端未连接到网络，并且应该连接到 Internet 云安全服务器。在 Internet Explorer 中，检查客户端计算机是否可以浏览 Internet 网页。
6. 检查用于连接到云安全服务器（本地和全局）的[内部代理服务器](#)和[外部代理服务器](#)设置。

客户端-服务器连接验证

防毒墙网络版 Web 控制台的客户端树上显示客户端与防毒墙网络版服务器的连接状态。



图 9-6. 显示客户端与防毒墙网络版服务器的连接状态的客户端树

特定情况可能阻止客户端树显示正确的客户端连接状态。例如，如果意外拔下了客户端计算机的网络电缆，则客户端将不能通知服务器其已脱机。此客户端在客户端树中将仍显示为联机。

手动验证客户端-服务器连接，或者允许防毒墙网络版执行预设验证。不能先选择特定域或客户端，然后再验证其连接状态。防毒墙网络版验证所有已注册客户端的连接状态。

验证客户端-服务器连接:

导航路径：联网计算机 > 连接验证

1. 要手动验证客户端-服务器连接，请转至**手动验证**选项卡，然后单击**立即验证**。
2. 要自动验证客户端-服务器连接，请转至**预设验证**选项卡。
 - a. 选择**启用预设验证**。
 - b. 选择验证频率以及开始时间。
 - c. 单击**保存**保存验证时间表。
3. 检查客户端树以验证其状态或查看连接验证日志。

连接验证日志

防毒墙网络版保留连接验证日志使您可以确定防毒墙网络版服务器是否能和其所有已注册客户端通信。每次从 **Web** 控制台验证客户端-服务器连接时，防毒墙网络版都会创建一个日志条目。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅第 8-16 页的 [管理日志](#)。

查看连接验证日志:

导航路径：日志 > 联网计算机日志 > 连接验证

1. 通过检查**状态**列查看连接验证结果。
2. 要将日志保存为逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。通常使用电子表格应用程序（例如 Microsoft Excel）来打开 CSV 文件。

客户端代理服务器设置

连接到内部和外部服务器时，将防毒墙网络版客户端配置为使用代理服务器设置。

内部代理服务器

客户端可以使用内部代理服务器设置连接到网络中的下列服务器：

防毒墙网络版服务器计算机

服务器计算机托管防毒墙网络版服务器和集成型云安全服务器。客户端连接到防毒墙网络版服务器以更新组件，获取配置设置和发送日志。客户端连接到集成型云安全服务器以发送扫描查询。

本地云安全服务器

本地云安全服务器包括所有独立型云安全服务器及其他防毒墙网络版服务器的集成型云安全服务器。客户端连接到这些服务器以发送扫描查询。

配置内部代理服务器设置：

导航路径：管理 > 代理服务器设置 > “内部代理服务器”选项卡

1. 选中相应复选框以启用代理服务器的使用。
2. 指定代理服务器名称或 IP 地址，以及端口号。
3. 如果代理服务器要求认证，则在提供的文本框中键入用户名和密码。
4. 单击**保存**。

外部代理服务器

防毒墙网络版服务器和客户端在连接到趋势科技托管的服务器时，可以使用外部代理服务器设置。本主题讨论客户端的外部代理服务器设置。有关服务器的外部代理服务器设置，请参阅第 4-14 页的[用于服务器更新的代理服务器](#)。

客户端使用在 Internet Explorer 中配置的代理服务器设置连接到趋势科技 Internet 云安全服务器和 Web 信誉服务器。如果需要代理服务器认证，则客户端将使用在此窗口中指定的认证凭证（用户 ID 和密码）。

趋势科技 Internet 云安全服务器

当云安全客户端位于公司网络之外时，它们连接到 Internet 云安全服务器来发送扫描查询。

Web 信誉服务器

客户端连接到趋势科技 Web 信誉服务器以确定用户尝试访问的网站是否安全。

配置代理服务器认证凭证：

导航路径：管理 > 代理服务器设置 > 外部代理服务器

1. 在**客户端与趋势科技服务器的连接**部分，键入代理服务器认证所需的用户 ID 和密码。

下列代理服务器认证协议受支持：

- 基本访问认证
- 摘要访问认证
- 集成 Windows 认证

2. 确认密码。

3. 单击**保存**。

客户端迁移程序

如果网络上存在多个防毒墙网络版服务器，则使用客户端迁移程序工具将客户端从一台防毒墙网络版服务器转移到另一台。将新的防毒墙网络版服务器添加到网络后，如果希望将现有防毒墙网络版客户端转移到新服务器，则此程序非常有用。

注意： 这两台服务器必须具有相同的语言版本。如果使用客户端迁移程序将运行早期版本（如版本 7.x）的防毒墙网络版客户端移动到当前版本的服务器，则客户端会自动升级。

运行客户端迁移程序：

1. 在防毒墙网络版服务器上，转至 **<服务器安装文件夹>**\PCCSRV\Admin\Utility\IpXfer。
2. 将 **IpXfer.exe** 复制到客户端计算机。如果客户端计算机运行 x64 类型平台，则复制 **IpXfer_x64.exe**。
3. 在客户端计算机上打开命令提示符，然后导航到将该可执行文件复制到的文件夹。
4. 使用以下语法运行客户端迁移程序：

```
<executable file name> -s <server_name> -p <server_listening_port>  
[- c<client_listening_port>]
```

其中：

<executable file name> 是 IpXfer.exe 或 IpXfer_x64.exe

<server_name> 是目标防毒墙网络版服务器（该客户端要转移到的服务器）的名称

<server_listening_port> 是目标防毒墙网络版服务器的侦听端口（或 **trusted port（可信端口）**）。要在防毒墙网络版 Web 控制台上查看侦听端口，请在主菜单中单击**管理 > 连接设置**。

<client_listening_port> 是客户端计算机用于与服务器通信的端口号。

5. 要确定该客户端是否现已报告给其他服务器，请执行以下操作：
 - a. 在客户端计算机上，右键单击系统托盘中的防毒墙网络版客户端程序图标。
 - b. 选择**防毒墙网络版控制台**。
 - c. 在此菜单中单击**帮助**，然后选择**关于**。
 - d. 在**服务器名称/端口**文本框中检查作为该客户端报告对象的防毒墙网络版服务器。

注意： 如果该客户端未显示在管理它的新防毒墙网络版服务器的客户端树中，则请重新启动新服务器的主服务 (ofservice.exe)。

触探工具

“触探工具”会将一个文件的时间戳与另一个文件的时间戳或计算机系统时间进行同步。如果尝试在防毒墙网络版服务器上部署 **hotfix** 未取得成功，请使用“触探工具”更改该 Hotfix 的时间戳。这将使防毒墙网络版将该 hotfix 文件解释为新文件，从而使服务器再次尝试自动部署此 hotfix。

运行“触探工具”：

1. 在防毒墙网络版服务器上，转至 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\Touch。
2. 将 **TMTouch.exe** 复制到包含有要更改的文件的文件夹。如果要将文件的时间戳与另一个文件的时间戳进行同步，请使用“触探工具”将两个文件放在同一位置。
3. 打开命令提示窗口，然后转到“触探工具”的位置。

- 键入以下命令：

```
TmTouch.exe <destination file name> <source file name>
```

其中：

<destination file name> 是要更改其时间戳的 Hotfix 文件的名称

<source file name> 是要复制其时间戳的文件的名称

注意： 如果未指定源文件名，该工具会将目标文件时间戳设置为计算机的系统时间。

对目标文件使用通配符 (*)，但不能对源文件名使用。

- 要验证是否已更改时间戳，请在命令提示符下键入 **dir**，或者在 Windows 资源管理器中检查文件的属性。

客户端信息

查看关于防毒墙网络版客户端的重要信息，包括权限、客户端软件详细信息及系统事件。

查看客户端信息：

导航路径：联网计算机 > 客户端管理 > 状态

- 通过展开客户端计算机的名称查看选定客户端的状态。通过**重置**按钮可以将安全风险计数设置回零。
- 如果选择多个客户端，则请单击**全部展开**以查看所有选定客户端的详细信息。

导入和导出客户端设置

您可能需要防毒墙网络版客户端具有相同的扫描和/或客户端权限设置。通过防毒墙网络版，可以保存（导出）特定客户端扫描设置和权限并在以后将其复制（导入）到多个客户端。这提供了一种在众多客户端上配置相同设置的简便方法。

不能导出多个客户端的扫描和权限设置。仅能导出单个客户端、域或根的设置。

提示： 如果将具有相似防护需求的客户端分组到一个域，趋势科技建议您先配置其中一个客户端的设置，然后导出其设置，再将设置文件导入到域中剩余的客户端。

将客户端设置导出到文件：

导航路径：联网计算机 > 客户端管理 > 设置 > 导出设置

1. 单击任一链接以查看选定客户端或域的设置。
2. 单击**导出**保存设置。设置保存为 .dat 文件。
3. 单击**保存**，然后指定要保存 .dat 文件的位置。
4. 单击**保存**。

导入客户端设置：

导航路径：联网计算机 > 客户端管理 > 设置 > 导入设置

1. 单击**浏览**在计算机上找到 .dat 文件，然后单击**导入**。显示“导入设置”窗口，其中显示设置的摘要。
2. 单击任一扫描或权限设置链接来查看有关这些设置的详细信息。
3. 导入设置。
 - 如果在客户端树上选择了根图标，则通过选择**应用至全部域**，然后单击**应用到目标计算机**来导入设置。
 - 如果选择了域，则通过选择**应用到属于选定的域的所有计算机**，然后单击**应用到目标计算机**来导入设置。
 - 如果选择了若干个客户端，则通过单击**应用到目标计算机**来导入设置。

管理非活动客户端

当使用客户端卸载程序从一台计算机删除客户端程序时，该程序将自动通知服务器。当服务器接收到此通知时，它将在客户端树中删除客户端图标以显示该客户端已不再存在。

但是，如果使用其他方法删除客户端，如重新格式化计算机硬盘驱动器或手动删除客户端文件，则防毒墙网络版将不会注意到它的删除，只是把客户端显示为非活动。如果用户将客户端退出或禁用较长的时间，服务器还是会将该客户端显示为非活动。

要使客户端树仅显示活动客户端，请配置防毒墙网络版以从客户端树中自动删除非活动客户端。

自动删除非活动客户端：

导航路径：管理 > 非活动客户端

1. 选择允许自动删除非活动客户端。
2. 选择“非活动期超过 __ 天后自动删除客户端”。
3. 单击“保存”。

第 3 部分

提供其他防护



策略服务器 for Cisco NAC

本章主题：

- 第 10-2 页的 *关于策略服务器 for Cisco NAC*
- 第 10-2 页的 *组件和术语*
- 第 10-5 页的 *Cisco NAC 体系结构*
- 第 10-6 页的 *客户端验证顺序*
- 第 10-8 页的 *策略服务器*
- 第 10-14 页的 *同步*
- 第 10-15 页的 *证书*
- 第 10-18 页的 *策略服务器系统要求*
- 第 10-19 页的 *Cisco Trust Agent (CTA) 需求*
- 第 10-20 页的 *支持的平台和需求*
- 第 10-22 页的 *策略服务器 for NAC 部署*

本章包括安装和配置策略服务器 for Cisco NAC 的基本说明。有关配置和管理 Cisco Secure ACS 服务器以及其他 Cisco 产品的详细信息，请在以下 Web 站点参阅最新的 Cisco 文档：

<http://www.cisco.com/univercd/home/home.htm>

关于策略服务器 for Cisco NAC

趋势科技策略服务器 for Cisco Network Admission Control (NAC) 将评估防毒墙网络版客户端上防病毒组件的状态。策略服务器配置选项使您能够配置设置以对处于风险中的客户端执行处理措施，以便将它们与组织的安全计划相兼容。

这些处理措施包括：

- 指导客户端计算机更新其防毒墙网络版客户端组件
- 启用实时扫描
- 执行“立即扫描”
- 在客户端计算机上显示一条通知消息以通知用户防病毒策略违例

有关 Cisco NAC 技术的其他信息，请参阅 Cisco Web 站点：

www.cisco.com/go/nac

组件和术语

以下是各种组件和重要术语的列表，您需要熟悉它们以了解和使用策略服务器 for Cisco NAC。

组件

以下组件在实施趋势科技的策略服务器 for Cisco NAC 过程中是必需的：

表 10-1. 策略服务器 for Cisco NAC 组件

组件	描述
Cisco Trust Agent (CTA)	安装在客户端计算机上且允许它与其他 Cisco NAC 组件进行通信的程序。
防毒墙网络版客户端计算机	安装了防毒墙网络版客户端程序的计算机。要使用 Cisco NAC，客户端计算机还需要 Cisco Trust Agent。

表 10-1. 策略服务器 for Cisco NAC 组件（续）

组件	描述
网络访问设备	支持 Cisco NAC 功能的网络设备。受支持的网络访问设备包括一系列的 Cisco 路由器、防火墙和访问接入点以及具有终端访问控制器访问控制系统 (TACACS+) 或远程拨号用户服务 (RADIUS) 协议的第三方设备。 要获取受支持设备的列表，请参阅第 10-20 页的 支持的平台和需求 。
Cisco Secure Access Control Server (ACS)	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，并将其传递到用于评估的外部用户数据库的服务器。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。
策略服务器	接收和评估防毒墙网络版客户端防病毒数据的程序。执行评估后，策略服务器确定防毒墙网络版客户端应执行的处理措施，然后通知该客户端执行这些处理措施。
防毒墙网络版服务器	向策略服务器报告当前病毒码和病毒扫描引擎版本，策略服务器使用此信息评估防毒墙网络版客户端的防病毒状态。

术语

熟悉以下与策略服务器 for Cisco NAC 相关的术语：

表 10-2. 与策略服务器 for Cisco NAC 相关的术语

术语	定义
安全状态	客户端上防病毒软件是否存在及其当前状态。在此实施中，安全状态是指防毒墙网络版客户端程序是否存在于客户端计算机上、某些防毒墙网络版客户端设置的状态以及病毒扫描引擎和病毒码是否是最新的。
状态令牌	在防毒墙网络版客户端验证后，由策略服务器创建。包括告知防毒墙网络版客户端执行一组指定操作（如启用实时扫描或更新防病毒组件）的信息。

表 10-2. 与策略服务器 for Cisco NAC 相关的术语（续）

术语	定义
客户端验证	评估客户端安全状态以及将状态令牌返回到客户端的过程。
策略服务器规则	包括策略服务器用以衡量防毒墙网络版客户端安全状态的可配置条件的准则。规则还包括在安全状态信息与条件匹配的情况下客户端和策略服务器要执行的操作（请参阅第 10-9 页的 策略服务器策略和规则 以获取详细信息）。
策略服务器策略	策略服务器衡量防毒墙网络版客户端安全状态的一组规则。策略还包括在与策略关联的规则中的条件与安全状态不匹配的情况下，客户端和策略服务器执行的操作（请参阅第 10-9 页的 策略服务器策略和规则 以获取详细信息）。
认证、授权与核算 (AAA)	描述用来控制终端用户客户端访问计算机资源的三个主服务。认证是指识别客户端（通常通过让用户输入用户名和密码来完成）。授权是指用户所具有用于发送特定命令的权限。核算是指会话期间使用的资源度量，通常存储于日志中。Cisco Secure Access Control Server (ACS) 是对 AAA 服务器的 Cisco 实施。
Certificate Authority (CA)	网络上的一个权威，该权威分发数字证书以执行认证和保护计算机和/或服务器之间的连接。
数字证书	用于安全的附件。通常，证书通过 Web 服务器等服务器来认证客户端，并包含以下内容：用户身份信息、公共密钥（用于加密）和验证证书是否有效的 Certificate Authority (CA) 数字签名。
远程认证拨号用户服务 (RADIUS)	需要客户端输入用户名和密码的认证系统。Cisco Secure ACS 服务器支持 RADIUS。
终端访问控制器访问控制系统 (TACACS+)	通过用于对最终用户客户端进行认证的 AAA 命令启用的安全协议。Cisco ACS 服务器支持 TACACS+。

Cisco NAC 体系结构

下图说明基本 Cisco NAC 体系结构。

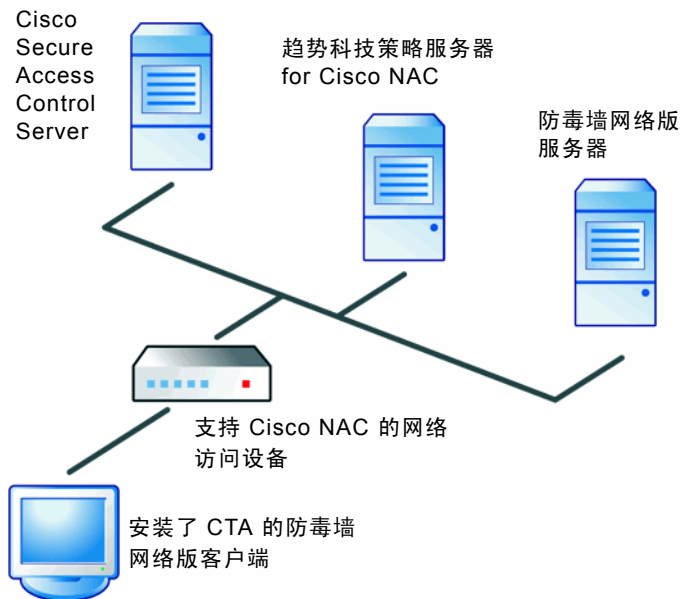


图 10-7. 基本 Cisco NAC 体系结构

此图中的防毒墙网络版客户端安装了 CTA，并且只能通过支持 Cisco NAC 的网络访问设备来访问网络。网络访问设备位于客户端和其他 Cisco NAC 组件之间。

注意： 网络的体系结构将根据代理服务器、路由器或防火墙是否存在而不同。

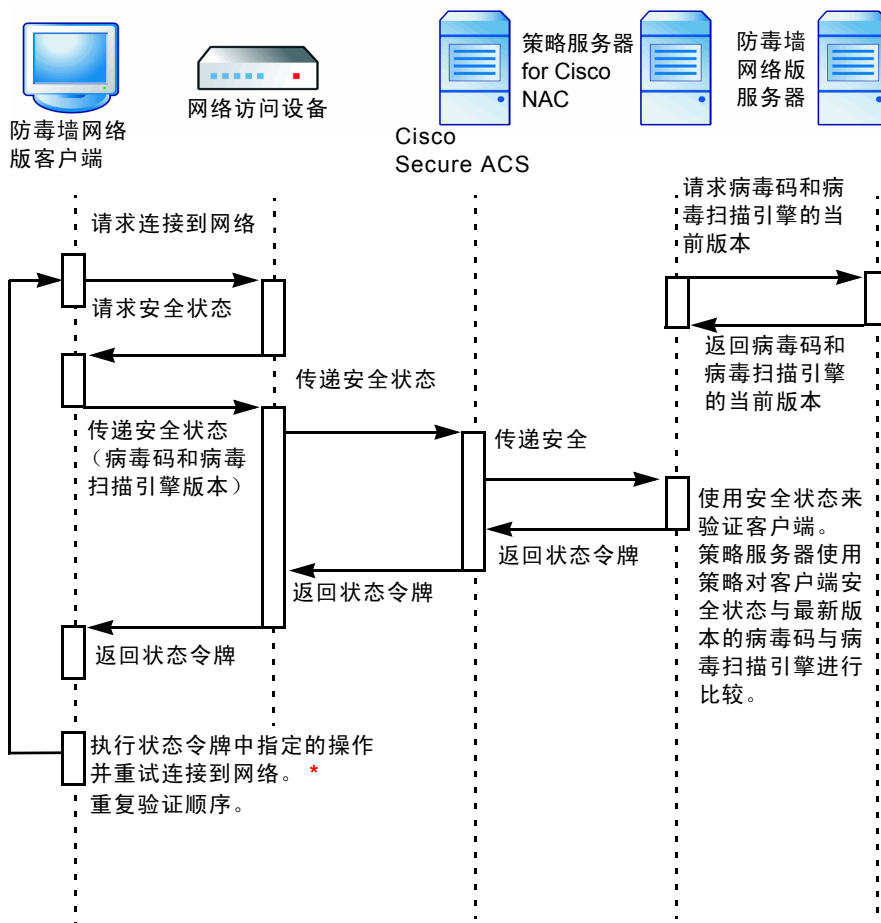
客户端验证顺序

客户端验证指以下过程：评估防毒墙网络版客户端安全状态，并在策略服务器认为客户端处于风险中时返回客户端要执行的指令。策略服务器使用可配置的规则和策略验证防毒墙网络版客户端。

下面是防毒墙网络版客户端尝试访问网络时，事件发生的顺序：

1. Cisco 网络访问设备首先在尝试访问网络时请求客户端的安全状态。
2. 然后网络访问设备将安全状态传递给 ACS 服务器。
3. ACS 服务器将安全状态传递给执行评估的策略服务器。
4. 在一个单独的进程中，策略服务器定期轮询防毒墙网络版服务器上的病毒码和病毒扫描引擎版本信息以使其数据保持最新。然后，策略服务器使用您配置的策略来比较这些信息与客户端安全状态数据。
5. 比较完成后，策略服务器创建状态令牌，并将其传递回防毒墙网络版客户端。

6. 客户端执行状态令牌中配置的操作。



* 网络访问设备计时器过期后，客户端会重试访问网络。请参阅 Cisco 路由器文档以获取有关配置计时器的信息。

图 10-8. 网络访问验证顺序

策略服务器

策略服务器负责评估防毒墙网络版客户端的安全状态并负责创建状态令牌。它将安全状态与从防毒墙网络版服务器（客户端是该服务器的成员）接收的病毒码和病毒扫描引擎进行比较。它将状态令牌返回到 Cisco Secure ACS 服务器，该服务器会接着将此令牌从网络访问设备传递到客户端。

当大量客户端同时尝试访问网络时，在单个网络上安装更多策略服务器可以提高性能。如果某个策略服务器无法操作，这些策略服务器还可以用作备份。如果一个网络上有多个防毒墙网络版服务器，策略服务器将处理已在其中注册的所有防毒墙网络版服务器的请求。同样，多个策略服务器可以处理已在所有策略服务器上注册的单个防毒墙网络版服务器的请求。

下图说明了多个防毒墙网络版服务器和策略服务器的关系。

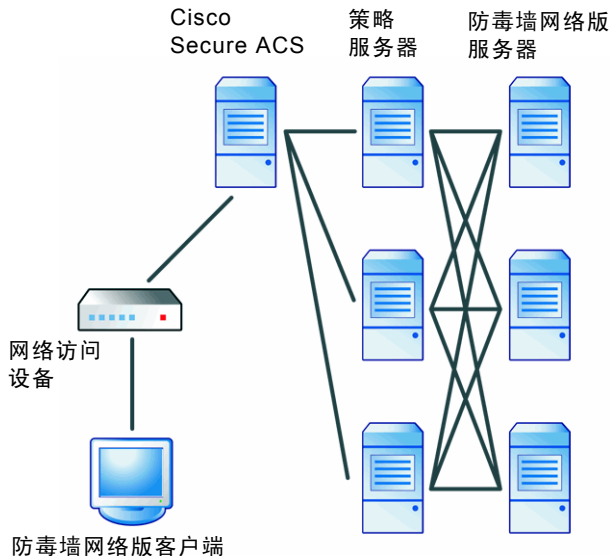


图 10-9. 多个策略服务器/防毒墙网络版服务器的关系

也可以在安装了防毒墙网络版服务器的同一计算机上安装策略服务器。

策略服务器策略和规则

策略服务器使用可配置的规则和策略来帮助实施贵组织的安全准则。

*规则*包括策略服务器用于比较防毒墙网络版客户端安全状态的特定条件。如果客户端安全状态与在规则中配置的条件匹配，则客户端和服务器会执行为该规则指定的操作（请参阅第 10-10 页的[策略服务器和防毒墙网络版客户端处理措施](#)）。

*策略*包括一个或多个规则。为网络上每个已注册防毒墙网络版服务器的爆发模式和正常模式分配一个策略（请参阅第 5-53 页的[爆发防护](#)以获取有关网络模式的详细信息）。

如果防毒墙网络版客户端安全状态与属于该策略的规则中的条件匹配，则防毒墙网络版客户端会执行为该规则配置的操作。但是，如果客户端安全状态和与该策略关联的规则中的任何条件都不匹配，则仍可在客户端和服务器要执行的策略中配置缺省操作（请参阅第 10-10 页的[策略服务器和防毒墙网络版客户端处理措施](#)）。

提示： 如果希望防毒墙网络版域中的特定客户端与同一域中的其他客户端具有不同的爆发模式和正常模式策略，趋势科技建议重新构建域以将具有相似需求的客户端进行分组（请参阅第 2-19 页的[防毒墙网络版域](#)）。

规则组成

规则包括安全状态条件、与客户端关联的缺省响应以及客户端和策略服务器执行的操作。

安全状态条件

规则包括以下安全状态条件：

- **客户端计算机状态：**客户端计算机是否处于引导状态
- **客户端实时扫描状态：**实时扫描是否已启用
- **客户端扫描引擎版本当前状态：**如果病毒扫描引擎为最新
- **客户端病毒码文件状态：**病毒码的新旧程度。策略服务器通过检查以下内容之一来确定这些状态：

- 病毒码文件是否比策略服务器早几个版本
- 病毒码是否在在验证前特定天数内可用

规则的缺省响应

进行客户端验证时，响应帮助您了解网络中防毒墙网络版客户端的情况。显示在策略服务器客户端验证日志中的这些响应与状态令牌相对应。从以下缺省响应中选择：

- **正常：**客户端计算机符合安全策略且未受感染。
- **检查：**客户端需要更新其防病毒组件。
- **受感染：**客户端计算机受感染或处于感染风险中。
- **转换：**客户端计算机正处于引导状态。
- **隔离：**客户端计算机正处于感染的高风险中且需要隔离。
- **未知：**其他情况。

注意： 无法添加、删除或修改响应。

策略服务器和防毒墙网络版客户端处理措施

如果客户端安全状态与规则条件匹配，则策略服务器可以执行以下处理措施：

- 在策略服务器客户端验证日志中创建条目（请参阅第 10-38 页的[客户端验证日志](#)以获取详细信息）

如果客户端安全状态与规则条件匹配，则防毒墙网络版客户端可以执行以下操作：

- 启用客户端实时扫描以便防毒墙网络版客户端可以扫描所有已打开或已保存的文件（请参阅第 5-18 页的[实时扫描](#)以获取详细信息）
- 更新所有防毒墙网络版组件（请参阅第 4-2 页的[防毒墙网络版组件与程序](#)以获取详细信息）
- 启用实时扫描或更新后扫描客户端（立即扫描）
- 在客户端计算机上显示通知消息

缺省规则

策略服务器提供缺省规则，以为您配置设置提供基础。这些规则涵盖常见及建议的安全状态条件和操作。缺省情况下可用以下规则：

表 10-3. 缺省规则

规则名称	匹配条件	满足条件时进行响应	服务器处理措施	客户端处理措施
正常	已启用实时扫描状态，且病毒扫描引擎和病毒码为最新。	正常	无	无
检查	病毒码版本比客户端注册到的防毒墙网络版服务器上的版本至少早一个版本。	检查	在客户端验证日志中创建条目	- 更新组件 - 启用实时扫描或更新后，对客户端执行自动立即清除 - 在客户端计算机显示通知消息 提示：如果使用此规则，请使用自动部署。自动部署帮助您在防毒墙网络版下载新组件后，确保客户端接收最新的病毒码。
转换	客户端计算机正处于引导状态。	转换	无	无

表 10-3. 缺省规则（续）

规则名称	匹配条件	满足条件时进行响应	服务器处理措施	客户端处理措施
隔离	病毒码版本比客户端注册到的防毒墙网络版服务器上的版本至少早五个版本。	隔离	在客户端验证日志中创建条目	- 更新组件 - 启用实时扫描或更新后，在客户端执行自动立即清除和立即扫描 - 在客户端计算机显示通知消息
未防护	实时扫描状态被禁用。	受感染	在客户端验证日志中创建条目	- 启用客户端实时扫描 - 在客户端计算机显示通知消息

策略组成

策略包括任意数量的规则、缺省响应和操作。

规则实施

策略服务器以特定的顺序实施规则，这使您能够区分规则的优先次序。更改规则的顺序、添加新规则以及从策略中删除现有规则。

策略的缺省响应

策略与规则类似，包括缺省响应，该响应可帮助您在进行客户端验证时了解网络上的防毒墙网络版客户端的情况。但是，仅当客户端安全状态与策略中的规则都不匹配时，缺省响应才与客户端关联。

策略的响应与规则的响应相同（请参阅第 10-10 页的[规则的缺省响应](#)以获取响应列表）。

策略服务器和防毒墙网络版客户端处理措施

通过将客户端状态信息与策略的每个规则关联，策略服务器对客户端执行规则。基于 Web 控制台上指定的正在使用中的规则，规则按从上到下的顺序应用。如果客户端状态与这些规则中的任何一个匹配，与该规则相应的操作将部署到客户端上。如果规则都不匹配，则缺省规则将适用并且与缺省规则相应的操作将部署到客户端上。

缺省爆发模式策略使用“正常”规则评估防毒墙网络版客户端。该策略强制与此规则不匹配的所有客户端立即实施“受感染”响应的操作。

缺省正常模式策略使用所有非“正常”规则（“转换”、“未保护”、“隔离”和“检查”规则）评估防毒墙网络版客户端。该策略将不匹配任何这些规则的所有客户端归类为“正常”，并且应用“正常”规则的操作。

缺省策略

策略服务器提供缺省策略，以为您配置设置提供基础。有两种策略，一种适用于正常模式，另一种适用于爆发模式。

表 10-4. 缺省策略

策略名称	描述
缺省正常模式策略	- 与策略相关的缺省规则：转换、未防护、隔离和检查 - 如果所有规则均不匹配则响应：正常 - 服务器处理措施：无 - 客户端处理措施：无

表 10-4. 缺省策略（续）

策略名称	描述
缺省爆发模式策略	- 与策略相关的缺省规则：正常 - 如果所有规则均不匹配则响应：受感染 - 服务器处理措施：在客户端验证日志里创建条目 - 客户端处理措施： - 启用客户端实时扫描 - 更新组件 - 启用实时扫描时或更新后，在客户端上执行立即扫描 - 在客户端计算机上显示通知消息

同步

定期将策略服务器与已注册防毒墙网络版服务器同步，以使策略服务器上病毒码与病毒扫描引擎的版本和服务器爆发状态（正常模式或爆发模式）与防毒墙网络版服务器相同。使用以下方法执行同步：

- 手动：**可随时在“摘要”窗口上执行同步（请参阅第 10-36 页的[策略服务器的摘要信息](#)）。
- 按时间表：**设置同步时间表（请参阅第 10-38 页的[管理](#)）。

证书

Cisco NAC 技术使用以下数字证书在各种组件之间成功建立通信：

表 10-5. Cisco NAC 证书

证书	描述
ACS 证书	在 ACS 服务器和 Certificate Authority (CA) 服务器之间建立可信通信。在将 ACS 证书保存在 ACS 服务器上之前，Certificate Authority 服务器会先签署此证书。
CA 证书	使用 Cisco ACS 服务器认证防毒墙网络版客户端。防毒墙网络版服务器将 CA 证书（包括 Cisco Trust Agent）部署到 ACS 服务器和防毒墙网络版客户端。
策略服务器 SSL 证书	在策略服务器和 ACS 服务器之间建立安全 HTTPS 通信。在策略服务器安装过程中，策略服务器安装程序会自动生成策略服务器 SSL 证书。 策略服务器 SSL 证书是可选的。但是，请使用该证书以确保仅加密数据才能在策略服务器和 ACS 服务器之间传送。

下图说明了关于创建和部署 ACS 和 CA 证书的步骤：

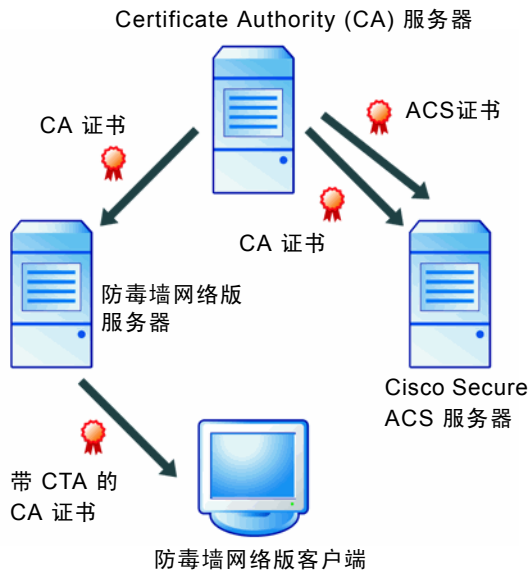


图 10-10. ACS 和 CA 证书的创建与部署

1. ACS 服务器向 CA 服务器发出证书签署请求后，CA 会产生名为 ACS 证书的证书。然后，ACS 证书安装在 ACS 服务器上。请参阅第 10-23 页的 [Cisco Secure ACS 服务器登记](#) 以获取详细信息。
2. 从 CA 服务器导出 CA 证书并安装到 ACS 服务器。请参阅第 10-23 页的 [CA 证书安装](#) 以获取详细信息。
3. 将相同的 CA 证书副本保存到防毒墙网络版服务器。
4. 防毒墙网络版服务器使用 CTA 将 CA 证书部署到客户端。请参阅第 10-25 页的 [Cisco Trust Agent 部署](#) 以获取详细信息。

CA 证书

安装了 CTA 的防毒墙网络版客户端首先在 ACS 服务器认证，然后才能传递客户端安全状态。可使用多种方法来认证（请参阅 [Cisco Secure ACS 文档](#) 以获取详细信息）。例如，您可能已经启用了使用 Windows Active Directory 的 Cisco Secure ACS 的计算机认证，Windows Active Directory 可以被配置为在有新计算机添加到活动目录中时自动生成最终用户客户端证书。有关说明，请参阅 [Microsoft Knowledge Base Article 313407, HOW TO: Create Automatic Certificate Requests with Group Policy in Windows](#)（如何在 Windows 中使用组策略来自动创建证书请求。）

对于具有自己的 Certificate Authority (CA) 服务器但其最终用户客户端尚未具有证书的用户，防毒墙网络版提供了一种将根证书分发到防毒墙网络版客户端的机制。在防毒墙网络版安装过程中或从防毒墙网络版 Web 控制台中分发证书。防毒墙网络版在其将 Cisco Trust Agent 部署到客户端时分发证书（请参阅第 10-25 页的 [Cisco Trust Agent 部署](#)）。

注意： 如果已从 Certificate Authority 获得了证书或已生成了自己的证书且将其分发到了最终用户客户端，则无需再进行此操作。

将证书分发到客户端之前，先在 CA 服务器登记 ACS 服务器，然后再准备证书（请参阅第 10-23 页的 [Cisco Secure ACS 服务器登记](#) 获取详细信息）。

策略服务器系统要求

安装策略服务器之前，请先检查计算机是否满足以下需求：

操作系统

- 带有 Service Pack 4 的 Windows 2000 Professional
- 带有 Service Pack 4 的 Windows 2000 Server
- 带有 Service Pack 4 的 Windows 2000 Advanced Server
- 带有 Service Pack 2 的 Windows XP Professional 或更高版本（32 位和 64 位）
- 带有 Service Pack 2 的 Windows Server 2003（标准版和企业版）或更高版本（32 位和 64 位）
- Windows Cluster Server 2000

硬件

- 300MHz Intel Pentium II 处理器或同等处理器
- 128MB 内存
- 300MB 可用磁盘空间
- 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) V5.0 或 V6.0
- Apache Web 服务器 2.0 或更高版本（仅适用于 Windows 2000/XP/Server 2003）

Web 控制台

要使用防毒墙网络版服务器 Web 控制台，需要以下配置：

- 133MHz Intel Pentium 处理器或同等处理器
- 64MB 内存
- 30MB 可用磁盘空间
- 在颜色为 256 或更高时，支持分辨率 800 x 600 的显示器
- Microsoft Internet Explorer 5.5 或更高版本

Cisco Trust Agent (CTA) 需求

将 Cisco Trust Agent 部署到客户端计算机之前，请先检查计算机是否满足以下需求：

操作系统

- Windows 2000 Professional Service Pack 4 和 Windows2000 Server
- 带有 Service Pack 2 的 Windows XP Professional 或更高版本（32 位）
- 带有 Service Pack 2 的 Windows Server 2003（标准版和企业版）或更高版本（32 位）

硬件

- 200MHz 单个或多个 Intel Pentium 处理器
- 对于 Windows 2000，内存为 128MB
- 对于 Windows XP 和 Windows 2003 内存为 256MB
- 5MB 可用磁盘空间（建议为 20 MB）

其他

- Windows Installer 2.0 或更高版本

支持的平台和需求

以下平台支持 Cisco NAC 功能：

表 10-6. 支持的平台和需求

支持的平台	型号	IOS 镜像	最小内存/闪存
路由器			
Cisco 830 和 870 系列	831、836、837	IOS 12.3(8) 或更高版本	48MB/8MB
Cisco 1700 系列	1701、1711、1712、1721、1751、1751-V 和 1760	IOS 12.3(8) 或更高版本	64MB/16MB
Cisco 1800 系列	1841	IOS 12.3(8) 或更高版本	128MB/32MB
Cisco 2600 系列	2600XM 和 2691	IOS 12.3(8) 或更高版本	96MB/32MB
Cisco 2800 系列	2801、2811、2821、2851	IOS 12.3(8) 或更高版本	128MB/64MB
Cisco 3600 系列	3640/3640A 和 3660-ENT 系列	IOS 12.3(8) 或更高版本	48MB/16MB
Cisco 3700 系列	3745、3725	IOS 12.3(8) 或更高版本	128MB/32MB
Cisco 3800 系列	3845、3825	IOS 12.3(8) 或更高版本	256MB/64MB
Cisco 7200 系列	720x 和 75xx	IOS 12.3(8) 或更高版本	128MB/48MB

表 10-6. 支持的平台和需求（续）

支持的平台	型号	IOS 镜像	最小内存/闪存
VPN 集中器			
Cisco VPN 3000 系列	3005 - 3080	V4.7 或更高版本	N/A
交换机			
Cisco Catalyst 2900	2950、 2970	IOS 12.1(22)EA5	N/A
Cisco Catalyst 3x00	3550、 3560、 3750	IOS 12.2(25)SEC	N/A
Cisco Catalyst 4x00	Supervisor 2+ 或更高版本	IOS 12.2(25)EWA	N/A
Cisco Catalyst 6500	6503、 6509、 Supervisor 2 或更高版本	CatOS 8.5 或更高版本	Sup2 - 128MB Sup32 - 256MB Sup720 - 512MB
无线访问接入点			
Cisco AP1200 系列	1230	N/A	N/A

策略服务器 for NAC 部署

以下步骤仅供参考，这些步骤可能会随 Microsoft 和/或 Cisco 界面的更新而更改。

执行任何任务之前，请验证网络中的网络访问设备是否能支持 Cisco NAC（请参阅第 10-20 页的[支持的平台和需求](#)）。请参阅设备设置文档和配置说明。同时，在网络中安装 ACS 服务器。请参阅 Cisco Secure ACS 文档，以了解指导信息。

1. 在网络上安装防毒墙网络版服务器（请参阅《安装和升级指南》）。
2. 在希望策略服务器评估其防病毒防护的所有客户端上安装防毒墙网络版客户端程序。
3. 登记 Cisco Secure ACS 服务器。通过使 ACS 服务器发出证书签署请求，在 ACS 服务器与 Certificate Authority (CA) 服务器之间建立可信关系。然后将 CA 签署的证书（称为 ACS 证书）保存在 ACS 服务器上（请参阅第 10-23 页的[Cisco Secure ACS 服务器登记](#)以获取详细信息）。
4. 将 CA 证书导出到 ACS 服务器，并将副本存储到防毒墙网络版服务器。此步骤仅当还未将证书部署到客户端和 ACS 服务器时才有必要（请参阅第 10-23 页的[CA 证书安装](#)）。
5. 将 Cisco Trust Agent 和 CA 证书部署到所有防毒墙网络版客户端，以便客户端可以向策略服务器提交安全状态信息（请参阅第 10-25 页的[Cisco Trust Agent 部署](#)）。
6. 安装策略服务器 for Cisco NAC 以处理来自 ACS 服务器的请求（请参阅第 10-29 页的[策略服务器 for Cisco NAC 安装](#)）。
7. 将 SSL 证书从策略服务器导出到 Cisco ACS 服务器，以便在两个服务器之间建立安全 SSL 通信（请参阅第 10-29 页的[策略服务器 for Cisco NAC 安装](#)）。
8. 配置 ACS 服务器以将状态验证请求转发给策略服务器（请参阅第 10-34 页的[ACS 服务器配置](#)）。
9. 配置策略服务器 for NAC。创建并修改策略服务器规则和策略以实施贵组织的防毒墙网络版客户端安全策略（请参阅第 10-34 页的[策略服务器 for Cisco NAC 配置](#)）。

Cisco Secure ACS 服务器登记

在 Certificate Authority (CA) 服务器登记 Cisco Secure ACS 服务器以建立两个服务器之间的可信关系。以下步骤适用于运行 Windows Certification Authority 服务器来管理网络上证书的用户。如果使用其他 CA 应用程序或服务，请参阅供应商的文档，并参阅 ACS 服务器文档以获取如何登记证书的说明。

CA 证书安装

防毒墙网络版客户端在发送安全状态数据之前，会先在 ACS 服务器认证。CA 证书对进行此认证是必需的。首先，从 CA 服务器中将 CA 证书导出到 ACS 服务器和防毒墙网络版服务器，然后创建 CTA 代理部署软件包。该软件包包括 CA 证书（请参阅第 10-17 页的 [CA 证书](#) 和第 10-25 页的 [Cisco Trust Agent 部署](#)）。

执行以下步骤导出并安装 CA 证书：

- 从 Certificate Authority 服务器中导出 CA 证书
- 将其安装在 Cisco Secure ACS 服务器上
- 将一份副本存储在防毒墙网络版服务器上

注意： 以下步骤适用于运行 Windows Certification Authority 服务器来管理网络上证书的用户。如果使用其他 Certification Authority 应用程序或服务，请参阅供应商的文档。

导出和安装要分发的 CA 证书：

1. 从 Certificate Authority (CA) 服务器中导出证书：
 - a. 在 CA 服务器上，单击**开始 > 运行**。将打开“运行”窗口。
 - b. 在打开框中键入 **mmc**。将打开一个新的管理控制台窗口。
 - c. 单击**文件 > 添加/删除管理单元**，将显示**添加/删除管理单元**窗口。
 - d. 单击**证书**，然后单击**添加**。将打开**证书管理单元**窗口。
 - e. 单击**计算机帐户**，然后单击**下一步**。将打开“选择计算机”窗口。

- f. 单击**本地计算机**，然后单击**完成**。
 - g. 单击**关闭**关闭**添加独立管理单元**窗口。
 - h. 单击**确定**关闭**添加/删除管理单元**窗口。
 - i. 在控制台的树视图中，单击**证书 > 受信任的根证书颁发机构 > 证书**。
 - j. 从列表中选择要分发到客户端和 ACS 服务器的证书。
 - k. 单击**操作 > 所有任务 > 导出...**将打开“证书导出向导”。
 - l. 单击**下一步**。
 - m. 单击**DER 编码二进制 x.509**，然后单击**下一步**。
 - n. 输入文件名称，然后浏览到导出证书的目标目录。
 - o. 单击**下一步**。
 - p. 单击**完成**。将显示一个确认窗口。
 - q. 单击**确定**。
2. 在 Cisco Secure ACS 上安装证书。
- a. 单击**系统配置 > ACS 证书安装 > ACS Certification Authority 安装**。
 - b. 在 **CA 证书文件**文本框中键入证书的完整路径和文件名。
 - c. 单击**提交**。Cisco Secure ACS 提示您重新启动服务。
 - d. 单击**系统配置 > 服务控制**。
 - e. 单击**重新启动**。Cisco Secure ACS 将重新启动。
 - f. 单击**系统配置 > ACS Certificate 管理 > 编辑证书信任列表**。将显示“编辑证书信任列表”窗口。
 - g. 选择对应于您在步骤 b 中已导入的证书的复选框，然后单击**提交**。Cisco Secure ACS 提示您重新启动服务。
 - h. 单击**系统配置 > 服务控制**。
 - i. 单击**重新启动**。Cisco Secure ACS 将重新启动。

3. 将证书（.cer 文件）复制到防毒墙网络版服务器计算机，以便将其与 CTA 一起部署到客户端（请参阅第 10-25 页的 [Cisco Trust Agent 部署](#) 以获取详细信息）。

注意： 将证书存储在本地驱动器上，不要存储在映射驱动器上。

Cisco Trust Agent 部署

Cisco Trust Agent (CTA) 是托管在防毒墙网络版服务器和安装到客户端的程序，它可启用防毒墙网络版客户端向 Cisco ACS 报告防病毒信息。

在防毒墙网络版服务器安装期间部署 CTA

如果在安装防毒墙网络版服务器之前已准备好 CA 证书，则在安装防毒墙网络版服务器的过程中部署 CTA。部署 CTA 的选项在安装程序的“安装其他防毒墙网络版程序”窗口上。有关安装防毒墙网络版服务器的说明，请参阅《安装和升级指南》。

使用防毒墙网络版服务器安装程序将 CTA 部署到客户端：

1. 在“安装其他防毒墙网络版程序”窗口上，选择 **Cisco Trust Agent for Cisco NAC**。
2. 执行以下操作之一：
 - 如果已经将证书分发到 Cisco Secure NAC 最终用户客户端，则单击 **下一步**。
 - 如果需要将证书分发到客户端：
 - i. 则单击 **导入证书**。
 - ii. 查找并选择已准备好的证书文件，然后单击 **确定**。有关准备证书文件的说明，请参阅第 10-23 页的 [CA 证书安装](#)。
 - iii. 单击 **下一步**。
3. 继续进行防毒墙网络版服务器安装过程。

从防毒墙网络版 Web 控制台部署 CTA

如果在服务器安装过程中未选择此选项来安装/升级 CTA，则可从 Web 控制台执行此操作。安装/升级 CTA 之前，将客户端证书部署到客户端。

注意： Certificate Authority (CA) 服务器会生成客户端证书文件。向趋势科技销售代表请求证书文件。

准备好安装/升级后，请检查要在 **Cisco NAC > 代理服务器管理** 中安装的 CTA 的版本，然后将 CTA 安装到 **Cisco NAC > 代理部署** 中的客户端。“代理部署”窗口还向您提供卸载 CTA 的选项。

部署 CTA 之前，在运行 Windows 2000/XP 的防毒墙网络版客户端上安装 Windows Installer 2.0 for NT 4.0。

导入客户端证书

客户端（或 CA）证书使用 Cisco ACS 服务器来对最终用户客户端进行认证。防毒墙网络版服务器随 Cisco Trust Agent (CTA) 将 CA 证书一同部署到客户端。因此，在部署 CTA 之前，将该证书导入到防毒墙网络版服务器。

导入证书：

1. 打开防毒墙网络版服务器 Web 控制台并单击 **Cisco NAC > 客户端证书**。
2. 键入证书的确切文件路径。
3. 键入存储在服务器上已准备好的 CA 证书的完整路径和文件名（例如：C:\CiscoNAC\certificate.cer）。有关准备 CA 证书的说明，请参阅第 10-23 页的 [CA 证书安装](#)。
4. 单击**导入**。要清除该文本框，请单击**重置**。

Cisco Trust Agent 版本

将 CTA 安装到客户端之前，请检查要安装的 CTA 版本（Cisco Trust Agent 或 Cisco Trust Agent Supplicant）。这两个版本的唯一区别是 Supplicant 软件包为计算机和最终用户提供层 2 认证。

如果 Cisco NAC Access Control Server (ACS) 是版本 4.0 或更高版本，则将客户端上的 Cisco Trust Agent 升级到版本 2.0 或更高版本。

检查 CTA 版本：

1. 打开防毒墙网络版服务器 Web 控制台并单击 **Cisco NAC > 代理服务器管理**。
2. 单击**使用< CTA 版本>**。防毒墙网络版服务器开始使用新版本。

手动替换 CTA 软件包：

如果存在要使用的特定版本，则手动替换防毒墙网络版服务器上的 CTA 软件包。

1. 在要使用的 CTA 版本中，将 CTA.msi 文件复制到以下文件夹：

<**服务器安装文件夹**>\PCCSRV\Admin\Utility\CTA\CTA-Package

或者

<**服务器安装文件夹**>\PCCSRV\Admin\Utility\CTA\CTA-Supplicant-Package

2. 将下列文件复制到 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\CTA\ PosturePlugin: TmabPP.dll、tmabpp.inf 和 TmAbPpAct.exe。
3. 在 Web 控制台中，转到 **Cisco NAC > 代理管理**，然后单击**使用 <CTA 版本>**。

代理升级后，会将这些文件压缩为 PostureAgent.zip（作为 <**服务器安装文件夹**>\PCCSRV\download\Product 下的 CTA 部署软件包）。

部署 Cisco Trust Agent

部署 Cisco Trust Agent，防毒墙网络版客户端可以将防病毒信息报告给 Cisco ACS。

从防毒墙网络版 Web 控制台将 CTA 部署到客户端：

1. 打开防毒墙网络版服务器 Web 控制台并单击**代理部署**。将显示客户端树。

注意： 在安装防毒墙网络版服务器的过程中，如果未接受 Cisco 许可协议中的条款，则将无法部署代理。单击**代理部署**后，将再次显示使用授权信息。阅读该许可协议，然后单击**是**同意条款。

2. 选择要部署 CTA 的客户端或域，然后单击**部署代理**。将显示**代理安装/卸载**窗口。
3. 单击**安装/升级 Cisco Trust Agent**。卸载防毒墙网络版客户端时，可选择卸载 Cisco Trust Agent。

注意： 还可以使用此窗口卸载或保留客户端上的 CTA 状态。

4. 如果在客户端树上选择域或客户端，请单击**保存**将设置应用到域或客户端。如果选择根图标 ，则从下列选项进行选择：
 - **应用到全部客户端：** 将设置应用到所有现有客户端和添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
 - **仅应用到将来的域：** 仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

注意： 如果在单击**安装 Cisco Trust Agent** 时，要部署代理的目标客户端未联机，则防毒墙网络版将在该客户计算机联机时自动完成任务。

Cisco Trust Agent 安装验证

在将 CTA 部署到客户端后，通过查看客户端树来验证安装是否成功。客户端树包含标题为 **Cisco Trust Agent** 的列，该列可以在**更新**、**查看全部**或**防病毒**视图中看到。成功的 CTA 安装将包含 CTA 程序的版本号。

另外验证客户端计算机上是否正在运行下列进程：

- ctapsd.exe
- ctaEoU.exe
- ctatransapt.exe
- ctaIogd.exe

策略服务器 for Cisco NAC 安装

有两种安装策略服务器的方法：

- 企业 DVD 上的策略服务器安装程序
- 防毒墙网络版服务器的主安装程序（在同一计算机上安装防毒墙网络版服务器和策略服务器）

注意： 主安装程序在 IIS 或 Apache Web server 上安装防毒墙网络版服务器和策略服务器 Web 控制台。如果安装程序在系统上没有找到 Apache 服务器，或者如果现有的 Apache 服务器安装不是版本 2.0，安装程序将自动安装 Apache 版本 2.0。

ACS 服务器、策略服务器和防毒墙网络版服务器必须位于同一网段中才能确保有效的通信。

安装 Apache Web 服务器之前，请参阅 Apache Web 站点以了解有关升级、Patch 和安全问题的最新信息：

<http://www.apache.org>

使用策略服务器安装程序安装策略服务器 for Cisco NAC:

1. 登录到将安装策略服务器 for Cisco NAC 的计算机。
2. 在企业 CD 中查找策略服务器 for Cisco NAC 安装程序软件包。
3. 双击 **setup.exe** 以运行安装程序。
4. 请遵循安装说明。

可以将策略服务器安装到防毒墙网络版服务器计算机上。

从防毒墙网络版服务器主安装程序中安装策略服务器 for Cisco NAC:

1. 在防毒墙网络版服务器主安装程序的“安装其他防毒墙网络版程序”窗口中，选择**策略服务器 for Cisco NAC**。
2. 单击**下一步**。
3. 继续进行防毒墙网络版服务器安装，直到趋势科技策略服务器 for Cisco NAC 的“欢迎”窗口出现。
4. 单击**下一步**。将显示“许可证协议”窗口。
5. 阅读协议，然后单击**我接受许可证协议中的条款**继续。将显示“选择目标位置”窗口。
6. 根据需要修改缺省的目标位置，方法是单击**浏览...** 并选择安装策略服务器的新目标位置。
7. 单击**下一步**。将显示“Web 服务器”窗口。
8. 选择策略服务器的 Web 服务器：
 - **IIS 服务器:** 单击以在现有的 IIS Web 服务器上安装
 - **Apache Web 服务器 2.0:** 单击以在 Apache Web 服务器 2.0 上进行安装
9. 单击**下一步**。将显示“Web 服务器配置”窗口。
10. 配置以下信息：
 - a. 如果选择在 IIS 服务器上安装策略服务器，则选择以下之一：
 - **IIS 缺省 Web 站点:** 单击安装为 IIS 缺省 Web 站点
 - **IIS 虚拟 Web 站点:** 单击安装为 IIS 虚拟 Web 站点

- b. 在**端口**旁键入将用作服务器侦听端口的端口。当策略服务器和防毒墙网络版服务器在同一计算机上且使用同一 Web 服务器时，则端口号如下所示：
 - **Apache Web 服务器/IIS Web 服务器在缺省的 Web 站点上：**策略服务器和防毒墙网络版服务器共享同一端口
 - **二者都在虚拟 Web 站点的 IIS Web 服务器上：**策略服务器的缺省侦听端口是 8081，SSL 端口是 4344。防毒墙网络版服务器的缺省侦听端口是 8080，SSL 端口是 4343。
 - c. 如果选择了将策略服务器安装在 IIS 服务器上，则可以使用安全套接层 (SSL)。键入 SSL 端口号和保持 SSL 证书有效的年限（缺省值是 3 年）。如果启用了 SSL，则此端口号将用作服务器的侦听端口。策略服务器的地址如下：
 - http://<Policy Server name>:<port number> 或者
 - https://<Policy Server name>:<port number> （如果启用了 SSL）
11. 单击**下一步**。
 12. 指定策略服务器控制台密码，然后单击**下一步**。
 13. 指定 ACS 服务器认证密码，然后单击**下一步**。
 14. 查看安装设置。如果满足设置，则单击**下一步**开始安装。否则，单击**上一步**转到上一窗口。
 15. 安装完成时，单击**完成**。防毒墙网络版服务器主安装程序将继续进行其余的防毒墙网络版服务器安装。

策略服务器 SSL 证书准备

要在 ACS 服务器和策略服务器之间建立安全 SSL 连接，请准备专用于 SSL 的证书。安装程序自动生成 SSL 证书。

准备要分发的策略服务器 SSL 证书：

1. 从 MMC 上的“证书存储”中导出证书。

如果策略服务器运行 IIS：

- a. 在策略服务器上，单击**开始 > 运行**。将打开“运行”窗口。
- b. 在**打开**框中键入 **mmc**。将打开一个新的管理控制台窗口。
- c. 单击**控制台 > 添加/删除管理单元**，将显示“添加/删除管理单元”窗口。
- d. 单击**添加**。将显示**添加独立管理单元**窗口。
- e. 单击**证书**，然后单击**添加**。将打开**证书管理单元**窗口。
- f. 单击**计算机帐户**，然后单击**下一步**。将打开“选择计算机”窗口。
- g. 单击**本地计算机**，然后单击**完成**。
- h. 单击**关闭**关闭**添加独立管理单元**窗口。
- i. 单击**确定**关闭**添加/删除管理单元**窗口。
- j. 在控制台的树视图中，单击**证书（本地计算机） > 受信任的根证书颁发机构 > 证书**。
- k. 从列表中选择证书。

注意： 通过双击证书并选择**属性**来检查证书指纹。该指纹应与 IIS 控制台中证书的指纹相同。

要进行验证，请打开 IIS 控制台并右键单击**虚拟 Web 站点**或缺省**Web 站点**（取决于安装策略服务器的 Web 站点），然后选择**属性**。单击**目录安全性**，然后单击**查看证书**以查看证书详细信息，包括指纹。

- l. 单击**操作 > 所有任务 > 导出...**将打开“证书导出向导”。
- m. 单击**下一步**。
- n. 单击**DER 编码二进制 X.509**或**Base 64 编码 X.509**，然后单击**下一步**。
- o. 输入文件名称，然后浏览到导出证书的目标目录。
- p. 单击**下一步**。
- q. 单击**完成**。将显示一个确认窗口。
- r. 单击**确定**。

如果策略服务器运行 Apache 2.0:

- a. 获取证书文件 server.cer。该文件的位置取决于您首先安装了哪个服务器（防毒墙网络版服务器还是策略服务器）。
 - 如果在安装策略服务器前先安装了防毒墙网络版服务器，则该文件位于以下目录中：
 <服务器安装文件夹>\PCCSRV\Private\certificate
 - 如果在安装防毒墙网络版服务器前先安装了策略服务器，则该文件位于以下目录中：
 <服务器安装文件夹>\PolicyServer\Private\certificate
 - b. 将证书文件复制到 ACS 服务器。
2. 在 Cisco Secure ACS 上安装证书。
- a. 在 ACS Web 控制台上，单击**系统配置 > ACS 证书安装 > ACS Certification Authority 安装**。
 - b. 在 **CA 证书文件**文本框中键入证书的完整路径和文件名。

- c. 单击**提交**。Cisco Secure ACS 提示您重新启动服务。
- d. 单击**系统配置 > 服务控制**。
- e. 单击**重新启动**。Cisco Secure ACS 将重新启动。

ACS 服务器配置

为允许 Cisco Secure ACS 将认证请求传递到策略服务器 for Cisco NAC，请在**外部策略**中添加策略服务器 for Cisco NAC 以使外部用户数据库可用于认证。请参阅 ACS 服务器文档以查看有关如何在新外部策略中添加策略服务器的说明。

注意： 配置 ACS 服务器来执行阻止客户端访问网络之类的任务。这些 ACS 功能超出了趋势科技策略服务器 for Cisco NAC 实施的范围，因此未包括在本文档中。有关配置其他 ACS 功能的详细信息，请参阅 ACS 文档。

策略服务器 for Cisco NAC 配置

安装了防毒墙网络版与策略服务器并部署了防毒墙网络版客户端与 Cisco Trust Agent 后，请配置策略服务器 for Cisco NAC。要配置策略服务器，请从防毒墙网络版 Web 控制台中访问策略服务器 Web 控制台，方法是转到 **Cisco NAC > 策略服务器**，然后单击“策略服务器”链接。

本节描述策略服务器配置的以下方面：

- 第 10-35 页的[从防毒墙网络版配置策略服务器](#)描述如何在防毒墙网络版 Web 控制台上管理策略服务器。
- 第 10-36 页的[策略服务器的摘要信息](#)向您显示如何获取网络上策略服务器的概述。
- 第 10-37 页的[策略服务器注册](#)是配置策略服务器过程中的第一步。
- 第 10-37 页的[规则](#)向您显示如何创建和编辑组成策略的规则。
- 第 10-37 页的[策略](#)向您显示如何创建和编辑最终决定策略服务器测定客户端安全状态的规则。

- 第 10-38 页的 [客户端验证日志](#) 概述了如何使用日志来了解网络中客户端的安全状态。
- 第 10-38 页的 [管理](#) 描述了如何更改策略服务器密码和如何设置同步的时间表。

从防毒墙网络版配置策略服务器

配置策略服务器的第一步是向防毒墙网络版服务器添加安装的策略服务器。此操作使您可以从防毒墙网络版 Web 控制台中打开策略服务器 Web 控制台。

添加策略服务器：

1. 在防毒墙网络版 Web 控制台的主菜单上，单击 **Cisco NAC > 策略服务器**。将显示“策略服务器”窗口，该窗口显示所有策略服务器的列表。
2. 单击**添加**。将显示“新建策略服务器”窗口。
3. 键入服务器用于 HTTPS 通信的完整策略服务器地址和端口号（例如：https://policy-server:4343/）。另外，键入服务器的可选描述。
4. 键入登录到策略服务器 Web 控制台时要使用的密码并确认密码。
5. 单击**保存**。

删除策略服务器：

1. 在防毒墙网络版 Web 控制台的主菜单上，单击 **Cisco NAC > 策略服务器**。将显示“策略服务器”窗口，该窗口显示所有策略服务器的列表。
2. 选中要删除的策略服务器旁的复选框。
3. 单击**删除**。

注意： 要验证网络上的所有客户端，请向至少一台策略服务器添加所有防毒墙网络版服务器。

策略服务器的摘要信息

“摘要”窗口包含有关策略服务器的信息，包括策略和规则的配置设置、客户端验证日志以及注册到策略服务器的防毒墙网络版服务器。

策略服务器 for Cisco NAC 的 IP 地址和端口号显示在“摘要”窗口的顶部。

配置摘要表显示向策略服务器注册的防毒墙网络版服务器数、策略服务器策略以及组成策略的规则。

查看和修改策略服务器的配置摘要详细信息：

1. 在防毒墙网络版 Web 控制台的主菜单上，单击 **Cisco NAC > 策略服务器**。将显示“策略服务器管理”窗口，该窗口显示所有策略服务器的列表。
2. 单击要查看其详细信息的策略服务器的服务器名称。将显示“摘要”窗口，该窗口显示**配置摘要**表。
3. 单击要查看其配置设置的项目旁边的链接：
 - **已注册的防毒墙网络版服务器：**当前在网络上的防毒墙网络版服务器
 - **策略：**已注册的防毒墙网络版服务器可以使用的策略服务器策略
 - **规则：**组成策略的策略服务器规则

提示： 如果希望网络中的多个策略服务器具有相同的设置（包括相同的规则和策略），则将设置从一个服务器中导出然后导入到其他服务器。趋势科技建议在网络中的所有策略服务器上配置相同的设置，以保持防病毒策略一致。

将策略服务器与已注册的防毒墙网络版服务器同步：

在“摘要”窗口中，单击**与防毒墙网络版同步**。将显示“摘要 — 同步结果”窗口，该窗口显示以下只读信息：

- **防毒墙网络版服务器名称：**已注册防毒墙网络版服务器的主机名或 IP 地址和端口号
- **同步结果：**表示同步是否成功
- **上次同步时间：**上次成功同步的日期

有关同步的详细信息，请参阅第 10-14 页的**同步**。

策略服务器注册

至少在一台防毒墙网络版服务器中注册策略服务器，这样策略服务器才能得到病毒码和病毒扫描引擎版本信息。有关防毒墙网络版服务器在验证过程中发挥的作用的信息，请参阅第 10-6 页的[客户端验证顺序](#)。

注意： 要使策略服务器验证网络上的所有客户端，请向至少一个策略服务器添加所有防毒墙网络版服务器。

可从“防毒墙网络版服务器”窗口中添加新防毒墙网络版服务器或编辑现有防毒墙网络版服务器的设置，方法是转到策略服务器 Web 控制台然后单击**配置 > 防毒墙网络版服务器**。

规则

规则是策略的构建块，它组成了策略。请按照策略服务器配置中的下一个步骤配置规则。请参阅第 10-9 页的[规则组成](#)以获取详细信息。

要访问 Cisco ACS 规则的 Web 控制台窗口，请转到策略服务器 Web 控制台，然后在主菜单上单击**配置 > 规则**。

策略

配置新规则或者确保缺省规则符合安全实施需求之后，请配置已注册的防毒墙网络版服务器可以使用的策略。请参阅第 10-12 页的[策略组成](#)以获取详细信息。

添加新 Cisco NAC 策略或编辑现有 Cisco NAC 策略以确定当前实施的规则，并确定在客户端安全状态与所有规则不匹配时在客户端上要采取的操作。

要访问 Cisco ACS 策略的 Web 控制台窗口，请转到策略服务器 Web 控制台，然后在主菜单上单击**配置 > 策略**。

客户端验证日志

在客户端使用策略服务器进行验证时，使用客户端验证日志查看有关客户端的详细信息。ACS 服务器检索客户端安全状态数据并将其发送到策略服务器（将该数据与策略和规则比较）时验证发生（请参阅第 10-6 页的[客户端验证顺序](#)）。

注意： 要生成客户端验证日志，请在添加或编辑新规则或策略时选中**服务器端处理措施**下的复选框。

要访问 Cisco ACS 日志的 Web 控制台窗口，请转到策略服务器 Web 控制台，然后在主菜单上单击**日志 > 查看客户端验证日志**。

客户端日志维护

策略服务器在客户端验证日志达到指定大小时对其进行归档。在达到指定的数量后，策略服务器还将删除日志文件。通过在策略服务器 Web 控制台上单击**日志 > 日志维护**来指定策略服务器维护客户端验证日志的方式。

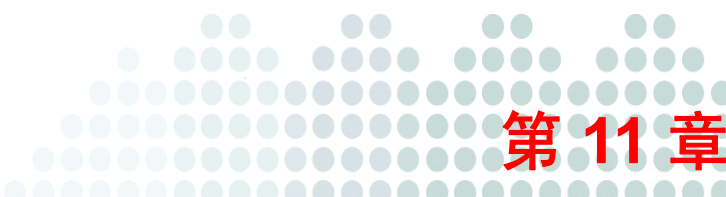
管理

在策略服务器上执行以下管理任务：

- **更改密码：**添加策略服务器时更改配置的密码（请参阅第 10-35 页的[从防毒墙网络版配置策略服务器](#)）
- **预设同步：**策略服务器需要定期获取防毒墙网络版服务器上病毒码和病毒扫描引擎的版本，以评估防毒墙网络版客户端的安全状态。因此，您无法启用或禁用预设同步。缺省情况下，策略服务器每五分钟就和防毒墙网络版服务器同步一次（请参阅第 10-14 页的[同步](#)以获取详细信息）。

注意： 可以在“摘要”窗口中随时手动同步策略服务器和防毒墙网络版服务器（请参阅第 10-36 页的[策略服务器的摘要信息](#)）。

要访问 Cisco ACS 管理任务的 Web 控制台窗口，请转到策略服务器 Web 控制台，然后在主菜单上单击“管理”。



第 11 章

使用第三方软件配置防毒墙网络版

本章主题：

- 第 11-2 页的 *Check Point 体系结构和配置概述*
- 第 11-4 页的 *Check Point for 防毒墙网络版配置*
- 第 11-6 页的 *安装 SecureClient 支持*

Check Point 体系结构和配置概述

可以使用开放式安全平台 (OPSEC) 框架内的安全配置验证 (SCV) 来将安装的防毒墙网络版与 Check Point™ SecureClient™ 集成。阅读此部分之前，请参阅 Check Point SecureClient OPSEC 文档。OPSEC 文档可以在以下网站上找到：

<http://www.opsec.com>

Check Point SecureClient 能够使用安全配置验证 (SCV) 检查来确认连接到网络的计算机的安全配置。SCV 检查是定义安全配置的客户端系统的一组条件。第三方软件可以将这些条件的值传递给 Check Point SecureClient。然后，Check Point SecureClient 可将这些条件与 SCV 文件中的条件相比较，以确定客户端是否安全。

定期执行 SCV 检查以确保只允许安全配置的系统连接到网络。

SecureClient 使用策略服务器将 SCV 检查传送到在该系统注册的所有客户端。管理员可以使用 SCV 编辑器在策略服务器上设置 SCV 检查。

SCV 编辑器是由 Check Point 提供的工具，允许您修改 SCV 文件以传送到安装的客户端。要运行 SCV 编辑器，请在策略服务器上找到并运行 SCVeditor.exe。在 SCV 编辑器中，打开 C:\FW1\NG\Conf 文件夹中的文件 local.scv（如果 Check Point 防火墙的安装路径与缺省设置不同，请将 C:\FW1 替换为该安装路径）。

有关使用 SCV 编辑器打开和修改 SCV 文件的特定指导信息，请参阅第 11-4 页的 *Check Point for 防毒墙网络版配置*。

防毒墙网络版集成

防毒墙网络版客户端可以定期将病毒码号和病毒扫描引擎号传递给 SecureClient 以进行验证。然后，SecureClient 将这些值与客户端 local.scv 文件中的值相比较。

下面是 local.scv 文件在文本编辑器中打开时的外观：

```
(SCVObject
:SCVNames (
: (OfceSCV
:type (plugin)
:parameters (
:CheckType (OfceVersionCheck)
:LatestPatternVersion (701)
:LatestEngineVersion (7.1)
:PatternCompareOp (">=")
:EngineCompareOp (">=")
)
)
)
:SCVPolicy (
: (OfceSCV)
)
:SCVGlobalParams (
:block_connections_on_unverified (true)
:scv_policy_timeout_hours (24)
)
)
```

在此示例中，如果病毒码文件的版本为 701 或更高版本，且扫描引擎号为 7.1 或更高版本，则 SCV 检查会允许通过防火墙的连接。如果扫描引擎或病毒码文件的版本较旧，则会阻止所有通过 Check Point 防火墙的连接。使用 SCV 编辑器在策略服务器的 local.scv 文件上修改这些值。

注意： Check Point 不会自动更新 SCV 文件中的病毒码文件号和扫描引擎版本号。只要防毒墙网络版更新了扫描引擎或病毒码文件，就需要在 local.scv 文件中手动更改条件的值以使它们为最新。如果未更新扫描引擎和病毒码版本，则 Check Point 将允许来自具有较旧病毒码文件或扫描引擎的客户端的通信，从而给新病毒带来潜入系统的机会。

Check Point for 防毒墙网络版配置

要修改 local.scv 文件，需要下载并运行 SCV 编辑器 (SCVeditor.exe)。

配置安全配置验证文件：

1. 从 Check Point 下载站点下载 SCVeditor.exe。SCV 编辑器是 OPSEC SDK 软件包的一部分。
2. 在策略服务器上运行 SCVeditor.exe。将打开 SCV 编辑器控制台。
3. 展开 **Products** 文件夹，然后选择 **user_policy_scv**。
4. 单击**编辑 > 产品 > 修改**，然后在**修改**框内键入 **OfceSCV**。单击**确定**。

注意： 如果 local.scv 文件已包括其他第三方软件的产品策略，请通过单击**编辑 > 产品 > 添加**，然后在**添加**框中键入 **OfceSCV** 来创建新策略。

5. 单击**编辑 > 参数 > 添加**，然后在相应的框中键入**名称**和**值**，以添加参数。下表列出了参数的名称和值。参数的名称和值是区分大小写的。按表中给出的顺序键入它们。

表 11-1. SCV 文件参数的名称和值

名称	值
CheckType	OfceVersionCheck
LatestPatternVersion	<当前病毒码文件号>
LatestEngineVersion	<当前扫描引擎号>
LatestPatternDate	<当前病毒码文件发布日期>
PatternCompareOp	>=
EngineCompareOp	>=
PatternMismatchMessage	
EngineMismatchMessage	

键入最新病毒码文件号和扫描引擎号替换花括号中的文本。通过单击防毒墙网络版 Web 控制台的主菜单上的**更新和升级**查看客户端的最新病毒码和扫描引擎版本。病毒码版本号将显示在表示受保护客户端的百分比的饼图的右侧。

6. 选择**阻止未经过 SCV 验证的连接**。
7. 单击**编辑 > 产品 > 执行**。
8. 单击**文件 > 生成策略文件**以创建文件。选择现有的 local.scv 文件覆盖它。

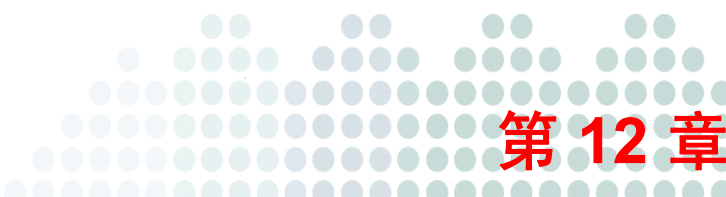
安装 SecureClient 支持

如果用户从专用虚拟网络 (VPN) 连接到办公室网络，且他们的计算机上都安装了 Check Point SecureClient 和防毒墙网络版客户端，请指导这些用户安装 SecureClient 支持。此模块允许 SecureClient 在 VPN 客户端上执行 SCV 检查，从而确保只允许安全配置的系统连接到网络。

用户可以通过检查系统托盘上的  图标来验证他们是否已在计算机上安装 Check Point SecureClient。用户还可以检查 Windows 的**添加/删除程序**窗口上是否存在名为 **Check Point SecureClient** 的项。

安装 SecureClient 支持：

1. 打开客户端控制台。
2. 单击**工具箱**选项卡。
3. 在 **Check Point SecureClient 支持**下，单击**安装工具**。将显示确定窗口。
4. 单击**是**。客户端将连接到服务器，并且还将下载模块。下载完成后，防毒墙网络版将显示一条消息。
5. 单击**确定**。



第 12 章

获取帮助

本章主题：

- 第 12-2 页的[故障排除资源](#)
- 第 12-15 页的[与趋势科技联系](#)

故障排除资源

此部分提供可以用于解决防毒墙网络版服务器和客户端问题的资源列表。

- [情况诊断工具](#)
- [防毒墙网络版服务器日志](#)
- [防毒墙网络版客户端日志](#)

情况诊断工具

趋势科技“情况诊断工具”(CDT)会在发生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。

在防毒墙网络版支持的所有平台上运行该工具。要获得此工具及相关文档，请联系您的技术支持提供商。

防毒墙网络版服务器日志

除可在 Web 控制台上访问的日志之外，您还可以使用其他类型的日志（例如调试日志）解决产品问题。

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。

服务器使用 LogServer.exe 调试日志

使用 LogServer.exe 为以下项目收集调试日志：

- 防毒墙网络版服务器基本日志
- 趋势科技漏洞扫描程序
- 利用 Active Directory 的防毒墙网络版功能
- 基于角色的管理
- 云安全扫描
- 策略服务器

启用调试日志记录：

1. 登录到 Web 控制台。
2. 在 Web 控制台的旗标中，单击“防毒墙网络版”中“毒”和“墙”之间的空隙。
3. 指定调试日志设置。
4. 单击**保存**。
5. 检查以下缺省位置中的日志文件 (ofcdebug.log)：<服务器安装文件夹>\PCCSRV\Log。

禁用调试日志记录：

1. 登录到 Web 控制台。
2. 在 Web 控制台的旗标中，单击“防毒墙网络版”中“毒”和“墙”之间的空隙。
3. 清除**启用调试日志**。
4. 单击**保存**。

启用服务器安装和升级的调试日志记录：

在执行以下任务前启用调试日志记录：

- 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（调试日志记录在启动安装程序的计算机上启用，而非在远程计算机上启用）。

执行下列步骤：

1. 将位于 <服务器安装文件夹>\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。

安装日志

本地安装/升级日志

文件名：OFCMAS.LOG

位置：%windir%

远程安装/升级日志

在启动安装程序的计算机上：

文件名：ofcmasr.log

位置：%windir%

在目标计算机上:

文件名: OFCMAS.LOG

位置: %windir%

组件更新日志

文件名: TmuDump.txt

位置: <服务器安装文件夹>\PCCSRV\Web\Service\AU_Data\AU_Log

获取详细的服务器更新信息:

1. 使用以下内容创建名为 aucfg.ini 的文件:

```
[debug]
```

```
level=-1
```

```
[Downloader]
```

```
ProxyCache=0
```

2. 将该文件保存到 <服务器安装文件夹>\PCCSRV\Web\Service。
3. 重新启动防毒墙网络版主服务。

停止收集详细服务器更新信息:

1. 删除 aucfg.ini。
2. 重新启动防毒墙网络版主服务。

客户端打包程序日志

启用客户端打包程序创建过程的日志记录:

1. 修改 <服务器安装文件夹>\PCCSRV\Admin\Utility\ClientPackager 中的 ClnExtor.ini 文件, 如下所示:

```
[Common]
```

```
DebugMode=1
```

2. 检查 C:\ 中的 ClnPack.log。

禁用客户端打包程序创建过程的日志记录：

1. 打开 ClnExtor.ini。
2. 将“DebugMode”的值从 3 更改为 0。

ServerProtect 标准服务器迁移工具日志

启用 ServerProtect 标准服务器迁移工具的调试日志：

1. 使用以下内容创建名为 ofcdebug.ini 的文件：

```
[debug]
```

```
DebugLog=C:\ofcdebug.log
```

```
DebugLevel=9
```

2. 将该文件保存到 C:\。
3. 检查 C:\ 中的 ofcdebug.log。

禁用 ServerProtect 标准服务器迁移工具的调试日志：

删除 ofcdebug.ini。

VSEncrypt 日志

防毒墙网络版自动在用户帐户的临时文件夹中创建该调试日志 (VSEncrypt.log)。例如， C:\Documents and Settings\<User name>\Local Settings\Temp。

控制管理中心 MCP 代理日志

<服务器安装文件夹>\PCCSRV\CMAgent 文件夹中的调试文件

- Agent.ini
- Product.ini
- 控制管理中心“设置”页面的屏幕截图
- ProductUI.zip

启用 MCP 代理的调试日志：

1. 修改 <服务器安装文件夹>\PCCSRV\CmAgent 中的 product.ini，如下所示：

```
[debug]
debugmode = 3
debuglevel= 3
debugtype = 0
debugsize = 10000
debuglog = C:\CMAgent_debug.log
```

2. 从 Microsoft 管理控制台重新启动 OfficeScan 控管中心代理服务。
3. 检查 C:\ 中的 CMAgent_debug.log。

禁用 MCP 代理的调试日志：

1. 打开 product.ini 并删除以下内容：

```
debugmode = 3
debuglevel= 3
debugtype = 0
debugsize = 10000
debuglog = C:\CMAgent_debug.log
```

2. 重新启动防毒墙网络版控制管理中心服务。

病毒扫描引擎日志

启用病毒扫描引擎的调试日志：

1. 打开注册表编辑器 (regedit.exe)。
2. 转到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters。
3. 将 “DebugLogFlags” 的值更改为 “00003eff”。

4. 执行导致您所遇到的扫描问题的步骤。
5. 检查 %windir% 中的 TMFilter.log。

禁用病毒扫描引擎的调试日志记录：

将 “DebugLogFlags” 的值恢复为 “00000000”。

爆发日志

当前防火墙违例爆发日志

文件名: Cfw_Outbreak_Current.log

位置: <服务器安装文件夹>\PCCSRV\Log\

上次防火墙违例爆发日志

文件名: Cfw_Outbreak_Last.log

位置: <服务器安装文件夹>\PCCSRV\Log\

当前病毒/恶意软件爆发日志

文件名: Outbreak_Current.log

位置: <服务器安装文件夹>\PCCSRV\Log\

上次病毒/恶意软件爆发日志

文件名: Outbreak_Last.log

当前爆发: <服务器安装文件夹>\PCCSRV\Log\

全球病毒跟踪日志

文件名: wtc.log

位置: <服务器安装文件夹>\PCCSRV\Log\temp

防毒墙网络版客户端日志

使用客户端日志（如调试日志）来解决客户端问题。

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。

客户端调试日志（使用 LogServer.exe）

启用防毒墙网络版客户端的调试日志记录：

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 [<客户端安装文件夹>](#) 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。

禁用防毒墙网络版客户端的调试日志记录：

删除 ofcdebug.ini。

全新安装日志

文件名：OFCNT.LOG

位置：

- %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）

升级/Hotfix 日志

文件名：upgrade.log

位置：<客户端安装文件夹>\Temp

损害清除服务日志

启用损害清除服务的调试日志记录：

1. 打开 <客户端安装文件夹> 中的 TSC.ini。
2. 如下所示修改下行：

DebugInfoLevel=3

3. 检查 <客户端安装文件夹>\debug 中的 TSCDebug.log。

禁用损害清除服务的调试日志记录：

打开 TSC.ini，然后将 “DebugInfoLevel” 的值从 3 更改为 0。

清除日志

文件名：yyyymmdd.log

位置：<客户端安装文件夹>\report\

邮件扫描日志

文件名：SmolDbg.txt

位置：<客户端安装文件夹>

客户端连接日志

文件名: Conn_YYYYMMDD.log

位置: <客户端安装文件夹>\ConnLog

客户端更新日志

文件名: Tmudump.txt

位置: <客户端安装文件夹>\AU_Data\AU_Log

获取详细的客户端更新信息:

1. 使用以下内容创建名为 aucfg.ini 的文件:

```
[debug]
```

```
level=-1
```

```
[Downloader]
```

```
ProxyCache=0
```

2. 将文件保存到 <客户端安装文件夹> 中。
3. 重新加载客户端。

停止收集详细的客户端更新信息:

1. 删除 aucfg.ini。
2. 重新加载客户端。

爆发阻止日志

文件名: OPPLogs.log

位置: <客户端安装文件夹>\OppLog

防毒墙网络版防火墙日志

启用 Windows Vista/2008 计算机上的通用防火墙驱动程序的调试日志记录：

1. 在以下两项中添加其下面的数据：
 - a. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlwfp\Parameters:
 - 类型：DWORD 值 (REG_DWORD)
 - 名称：DebugCtrl
 - 值：0x00001111
 - b. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlwf\Parameters:
 - 类型：DWORD 值 (REG_DWORD)
 - 名称：DebugCtrl
 - 值：0x00001111
2. 重新启动计算机。
3. 检查 C:\ 中的 wfp_log.txt 和 lwf_log.txt。

启用 Windows 2000/XP/2003 计算机上的通用防火墙驱动程序的调试日志记录：

1. 将以下数据添加到 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlcfw\Parameters 中：
 - 类型：DWORD 值 (REG_DWORD)
 - 名称：DebugCtrl
 - 值：0x00001111
2. 重新启动计算机。
3. 检查 C:\ 中的 cfw_log.txt。

禁用通用防火墙驱动程序（所有操作系统）的调试日志：

1. 删除注册码中的 “DebugCtrl”。
2. 重新启动计算机。

启用防毒墙网络版 NT 防火墙服务的调试日志：

1. 编辑位于 <客户端安装文件夹> 中的 TmPfw.ini，如下所示：

```
[ServiceSession]
```

```
Enable=1
```

2. 重新加载客户端。
3. 检查 C:\temp 中的 TmPfw.log。

禁用防毒墙网络版 NT 防火墙服务的调试日志：

1. 打开 TmPfw.ini，然后将“Enable”值从 1 更改为 0。
2. 重新加载客户端。

Web 信誉和 POP3 邮件扫描日志

启用 Web 信誉的调试日志记录和 POP3 邮件扫描功能：

1. 编辑位于 <客户端安装文件夹> 中的 TmProxy.ini，如下所示：

```
[ServiceSession]
```

```
Enable=1
```

```
LogFolder=C:\temp
```

2. 重新加载客户端。
3. 检查 C:\temp 中的 TmProxy 日志。

禁用 Web 信誉的调试日志记录和 POP3 邮件扫描功能：

1. 打开 TmProxy.ini，然后将“Enable”值从 1 更改为 0。
2. 重新加载客户端。

传输驱动接口 (TDI) 日志

启用 TDI 的调试日志记录：

1. 将以下数据添加到
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\
Parameters 中：

键 1

- 类型：DWORD 值 (REG_DWORD)
- 名称：Debug
- 值：1111 （十六进制）

键 2

- 类型：字符串值 (REG_SZ)
- 名称：LogFile
- 值：C:\tmtdi.log

2. 重新启动计算机。
3. 检查 C:\ 中的 tmtdi.log。

禁用 TDI 的调试日志记录：

1. 删除注册码中的 “Debug” 和 “LogFile” 。
2. 重新启动计算机。

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免费全球支持。

- 获取全球技术支持办公室的列表：

<http://cn.trendmicro.com/cn/support/techsupport/index.html>

- 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

TrendLabsSM 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。

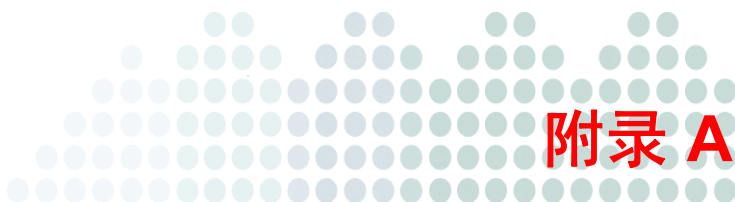
virus_doctor@trendmicro.com.cn

- 还可以使用基于 Web 的提交表格：

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

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。



词汇表

ActiveUpdate

ActiveUpdate 是许多趋势科技产品的通用功能。在连接到趋势科技更新 Web 站点后，可使用 **ActiveUpdate** 通过 Internet 下载最新的特征码文件、扫描引擎、程序及其他趋势科技组件文件。

Compressed File （压缩文件）

单个文件，它包含一个或多个单独的文件以及用于由合适的程序（如 WinZip）提取的信息。

Cookie

一种存储有关 Internet 用户的信息（如名称、首选项和兴趣）的机制，Cookie 存储在 Web 浏览器中以供日后使用。当您下次访问浏览器具有其 Cookie 的 Web 站点时，浏览器会将该 Cookie 发送到 Web 服务器，然后 Web 服务器可以使用它向您显示定制的 Web 页。例如，您可能进入一个名称吸引您的 Web 站点。

Denial of Service Attack（拒绝服务攻击）

拒绝服务 (DoS) 攻击是指计算机或网络上导致“服务”（即网络连接）丢失的攻击。通常，DoS 攻击会对网络带宽产生负面影响或使系统资源（如计算机的内存）超载。

DHCP

动态主机控制协议 (Dynamic Host Control Protocol, DHCP) 是一种将动态 IP 地址分配给网络中设备的协议。通过动态寻址，设备每次连接到网络时，可以使用不同的 IP 地址。在一些系统中，设备的 IP 地址甚至可以在它仍处于连接状态时发生更改。DHCP 还支持混合使用静态和动态 IP 地址。

DNS

域名系统 (DNS) 是一种主要在 Internet 中使用的通用数据查询服务，用于将主机名转换为 IP 地址。

当 DNS 客户端从 DNS 服务器请求主机名和地址数据时，此过程称为解析。基本的 DNS 配置可导致服务器执行缺省解析。例如，一个远程服务器向另一个服务器查询当前区域中计算机上的数据。远程服务器中的客户端软件查询解析程序，解析程序将答复来自其数据库文件的请求。

Domain Name（域名）

系统的完整名称，由其本地主机名和其域名组成，例如 `tellsitall.com`。域名应该足以确定 Internet 上任何主机的唯一 Internet 地址。此过程（称为“名称解析”）使用域名系统 (DNS)。

Dynamic IP Address（动态 IP 地址）

动态 IP 地址是由 DHCP 服务器分配的 IP 地址。计算机的 MAC 地址将保持不变，但是，DHCP 服务器可以根据可用资源为计算机分配新的 IP 地址。

End User License Agreement（最终用户许可协议）

最终用户许可协议或 EULA 是软件出版商和软件用户之间的合法合同。它通常概括出了对用户方的限制，用户可以通过在安装过程中不单击“我接受”而拒绝签订协议。当然，单击“我不接受”将终止软件产品的安装。

在安装某个免费软件过程中显示的 EULA 提示消息上单击“我接受”时，许多用户会不经意地同意在其计算机上安装间谍软件和其他类型的灰色软件。

False Positive（误报）

当安全软件错误地将某个文件检测为受到感染时，即发生误报。

FTP

文件传输协议 (FTP) 是用于将文件通过 Internet 从服务器传输到客户端的标准协议。有关详细信息，请参考“Network Working Group RFC 959”。

hotfix

Hotfix 是针对客户报告的单个问题的解决方法或解决方案。Hotfix 特定于某个问题，因此不会发布给所有客户。Windows Hotfix 包括一个安装程序，而非 Windows Hotfix 没有（通常需要停止守护程序，复制文件以覆盖安装过程中其对应文件，然后再重新启动守护程序）。

缺省情况下，防毒墙网络版客户端可以安装 Hotfix。如果不要客户端安装 Hotfix，则请通过在 Web 控制台中转至**联网计算机 > 客户端管理 > 设置 > 权限和其他设置 > 其他设置**选项卡更改客户端更新设置。

如果您尝试在防毒墙网络版服务器上部署 hotfix 未成功，请使用“触探工具”更改该 hotfix 的时间戳。这将使防毒墙网络版将该 hotfix 文件解释为新文件，从而使服务器再次尝试自动部署此 hotfix。关于此工具的详细信息，请参阅第 9-42 页的[触探工具](#)。

HTTP

超文本传输协议 (HTTP) 是用于将 Web 页面（包括图形和多媒体内容）通过 Internet 从服务器传输到客户端的标准协议。

HTTPS

使用安全套接层 (SSL) 的超文本传输协议。HTTPS 是 HTTP 的变种，用于处理安全事务。

ICMP

网关或目标主机偶尔会使用 Internet 控制消息协议 (ICMP) 与源主机进行通信，例如，报告数据报处理过程中出现的错误。ICMP 将把 IP 基础支持用作更高级别的协议，但是，ICMP 实际上是 IP 的组成部分，由每个 IP 模块实施。在以下几个情况下会发送 ICMP 消息：例如，当数据报不能达到其目标时，当网关没有转发数据报的缓冲能力时，以及当网关可以将主机定向为在较短的路由上发送网络通信时。因特网协议的设计不是绝对可靠。这些控制消息的目的是在通信环境中提供有关问题的反馈，而不是使 IP 可靠。

IntelliScan

IntelliScan 是一种识别要扫描的文件的方法。对于可执行文件（如 .exe 文件），可根据文件内容确定真实文件类型。对于非可执行文件（如 .txt 文件），可根据文件头确定真实文件类型。

使用 IntelliScan 会提供以下好处：

- **性能优化：**由于使用的系统资源最少，因此 IntelliScan 不会影响客户端上的应用程序。
- **更短的扫描周期：**因为 IntelliScan 使用真实文件类型识别，所以只扫描易受感染的文件。因此，扫描时间比扫描所有文件所需的时间要明显短很多。

IntelliTrap

病毒编写者经常通过使用实时压缩算法来尝试绕开病毒过滤。IntelliTrap 通过阻止实时压缩可执行文件和将其与其他恶意软件特征配对来帮助减少此类病毒进入网络的风险。由于 IntelliTrap 将这样的文件识别为安全风险，可能错误地阻止安全文件，因此，启用 IntelliTrap 时，请考虑隔离（不要删除或者清除）文件。如果用户经常交换实时压缩可执行文件，请禁用 IntelliTrap。

IntelliTrap 使用以下组件：

- 病毒扫描引擎
- IntelliTrap 特征码
- IntelliTrap 例外特征码

IP

“因特网协议 (IP) 规定了将数据块（称为数据报）从源到目标的传输，其中源和目标是由固定长度的地址识别的主机。” (RFC 791)

Java File（Java 文件）

Java 是 Sun Microsystems 开发的通用编程语言。Java 文件包含 Java 代码。Java 支持以独立于平台的 Java “applet” 形式为 Internet 编程。applet 是用 Java 编程语言编写的程序，可以包括在 HTML 页中。当使用支持 Java 技术的浏览器查看包含 applet 的页面时，applet 会将其代码传输到您的计算机，浏览器的 Java 虚拟机会执行 applet。

LDAP

轻型目录访问协议 (LDAP) 是一种应用程序协议，用于查询和修改通过 TCP/IP 运行的目录服务。

Listening Port（侦听端口）

侦听端口用于客户端连接的数据交换请求。

MCP Agent（MCP 代理）

趋势科技管理通信协议 (MCP) 是趋势科技用于被管理产品的下一代代理。MCP 替换了趋势科技管理基础架构 (TMI)，作为控制管理中心与防毒墙网络版通信的方法。MCP 具有一些新功能：

- 减少网络负荷和软件包大小
- 支持 NAT 和防火墙遍历
- HTTPS 支持
- 单向和双向通信支持

- 支持单点登录 (SSO)
- 集群节点支持

Mixed Threat Attack （混合威胁攻击）

混合威胁攻击利用企业网络中的多个入口点和漏洞，例如“Nimda”或“Code Red”威胁。

NAT

网络地址转换 (NAT) 是将地址池中的安全 IP 地址转换为临时的、外部的、已注册的 IP 地址的标准。这样，具有分配的专用 IP 地址的可信网络就可以访问 Internet。这还意味着您不必获取网络中每个计算机的已注册 IP 地址。

NetBIOS

网络基本输入输出系统 (NetBIOS) 是一个将诸如网络能力之类的功能添加到磁盘操作系统 (DOS) 基本输入/输出系统 (BIOS) 的应用程序接口 (API)。

One-way Communication （单向通信）

NAT 穿越在真实网络环境里已经日益成为一个重大问题。为处理此问题，MCP 使用了单向通信。单向通信使用 MCP 代理启动到服务器的连接，并轮询来自服务器的命令。每个请求是一条类似 CGI 命令的查询或日志传输。为减少网络的影响，MCP 代理保持连接活动，并打开尽可能多的连接。后继请求使用现有打开的连接。如果连接中断，所有到同一主机的 SSL 连接将受益于会话 ID 缓存，该缓存能极大地降低重新连接时间。

Patch

Patch 是解决多个程序问题的一组 Hotfix 和安全 Patch。趋势科技会定期提供 Patch。Windows Patch 包括一个安装程序，而非 Windows Patch 通常有一个安装脚本。

Phish Attack（网络钓鱼攻击）

网络钓鱼（Phish 或 Phishing）是一种正在迅速发展的欺诈形式，它通过伪造合法的 Web 站点来试图欺骗 Web 用户以盗取私人信息。

通常情况下，没有疑心的用户会收到一封听上去很紧急的（并且看起来真实的）电子邮件，告诉他们现在他们的帐户出现了问题，必须要立即解决以免帐户中止。电子邮件中将包括一个 URL，指向一个外观跟实际站点一模一样的 Web 站点。复制合法的电子邮件与 Web 站点很容易，但是随后会更改所谓的后台，也就是接收被收集的数据的目标系统。

该电子邮件提示用户登录到站点并确认一些帐户信息。黑客会接收用户提供的数据，如登录名、密码、信用卡号或社会保险号。

网络钓鱼欺诈快速、便宜且易于维持。它对于从事犯罪活动的那些罪犯也有相当大的潜在利润。甚至是了解计算机的用户都难以察觉网络钓鱼。执法部门也难以跟踪。更糟的是无法对其起诉。

请向趋势科技报告怀疑是网络钓鱼站点的任一 Web 站点。请参阅第 12-18 页的[将可疑文件发送给趋势科技](#)以获取详细信息。

Ping

Ping 是向 IP 地址发送 ICMP 回显请求并等待响应的实用工具。Ping 实用工具可以确定使用特定 IP 地址的计算机是否联机。

POP3

邮局协议 3 (POP3) 是存储电子邮件以及将其从服务器传输到客户端电子邮件应用程序的标准协议。

Proxy Server（代理服务器）

代理服务器是接受带有特殊前缀的 URL 的 World Wide Web 服务器，用于从本地缓存或远程服务器提取文档，然后将 URL 返回给请求方。

RPC

远程过程调用 (RPC) 是一种允许在一个主机上运行的计算机程序导致在另一个主机上执行代码的网络协议。

Security Patch （安全 Patch）

安全 Patch 关注的重点是适合部署到所有客户的安全问题。Windows 安全 Patch 包括一个安装程序，而非 Windows Patch 通常有一个安装脚本。

Service Pack

Service Pack 是足以成为产品升级包的 Hotfix、Patch 和增强功能的组合。Windows 和非 Windows Service Pack 都包括一个安装程序和安装脚本。

SMTP

简单邮件传输协议 (SMTP) 是一种用于通过 Internet 在服务器之间以及从客户端到服务器传输电子邮件的标准协议。

SNMP

简单网络管理协议 (SNMP) 是一种支持监控连接到网络的设备是否出现应进行管理的情况的协议。

SNMP Trap

简单网络管理协议 (SNMP) 陷阱是向网络管理员发送通知的方法，网络管理员使用的管理控制台应支持此协议。

防毒墙网络版可以将通知存储在管理信息库 (MIB) 中。可以使用 MIB 浏览器来查看 SNMP trap 通知。

但是，防毒墙网络版不维护本地 MIB 文件。如果已安装了趋势科技防毒墙控制管理中心，则可以下载控制管理中心 MIB 文件，并在防毒墙网络版中将其与支持 SNMP 协议的某个应用程序（如 HP™ OpenView）配合使用。

使用控制管理中心 MIB 文件：

1. 访问控制管理中心管理控制台。
2. 在主菜单上单击**管理**。将显示一个下拉菜单。
3. 单击**工具**。
4. 在工作区域上，单击**控制管理中心 MIB 文件**。
5. 在“文件下载”窗口上，选择**保存**，指定服务器上的某个位置，然后单击**确定**。
6. 将文件复制到防毒墙网络版服务器，提取控制管理中心 MIB 文件 **cm2.mib**（管理信息库 (MIB) 文件）。
7. 使用支持 SNMP 协议的应用程序（如 HP OpenView）导入 **cm2.mib**。

SOCKS 4

SOCKS 4 是一种 TCP 协议，由代理服务器用来在内部网络上的客户端之间或在 LAN 和外部的计算机或服务器之间建立连接。SOCKS 4 协议提出连接请求，设置代理服务器线路并在 OSI 模型的应用程序层中继数据。

SSL

安全套接层 (SSL) 是一种由 Netscape 设计的协议，用于提供在应用程序协议（如 HTTP、Telnet 或 FTP）和 TCP/IP 之间分层的数据安全。此安全协议为 TCP/IP 连接提供了数据加密、服务器认证、消息完整性和可选的客户端认证。

SSL Certificate（SSL 证书）

此数字证书建立安全的 HTTPS 通信。

TCP

传输控制协议 (Transmission Control Protocol, TCP) 是面向连接的且端对端的可靠协议，设计用来适应支持多网应用程序的分层协议层次结构。TCP 根据 IP 数据报来进行地址解析。有关信息，请参考“DARPA Internet Program RFC 793”。

Telnet

Telnet 是一种借助创建“网络虚拟终端”来进行终端设备交互（通过 TCP）的标准方法。有关详细信息，请参考“Network Working Group RFC 854”。

Trojan Port（特洛伊木马端口）

特洛伊木马端口通常由特洛伊木马程序用来连接到计算机。在爆发期间，防毒墙网络版会封闭特洛伊木马程序可能使用的以下端口号：

表 A-1. 特洛伊木马端口

端口号	特洛伊木马程序	端口号	特洛伊木马程序
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer

表 A-1. 特洛伊木马端口（续）

端口号	特洛伊木马程序	端口号	特洛伊木马程序
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Trusted Port（可信端口）

服务器和客户端使用可信端口来相互通信。

如果在爆发后封闭可信端口然后将网络设置恢复正常，则客户端将不会立即恢复与服务器的通信。仅经过了您在“爆发阻止设置”窗口中指定的时间（小时）后，才恢复客户端与服务器的通信。

防毒墙网络版使用 HTTP 端口（缺省情况下，8080）作为服务器上的可信端口。在安装过程中，可输入不同的端口号。要封闭此可信端口和客户端上的可信端口，请选中“端口封闭”窗口上的“封闭可信端口”复选框。

在安装过程中，主安装程序随机生成客户端可信端口。

确定可信端口：

1. 访问 <服务器安装文件夹>\PCCSRV。
2. 使用文本编辑器（如记事本）打开 ofcscan.ini 文件。
3. 对于服务器可信端口，搜索字符串“Master_DomainPort”，然后检查与该字符串相邻的值。例如，如果字符串显示为 Master_DomainPort=80，这表示服务器上的可信端口是端口 80。

4. 对于客户端可信端口，搜索字符串“Client_LocalServer_Port”，然后检查邻近该字符串的值。例如，如果字符串显示为
Client_LocalServer_Port=41375，这表示客户端上的可信端口是端口 41375。

Two-way Communication（双向通信）

除单向通信外，还可以选择双向通信。双向通信基于单向通信，但附加了一个基于 HTTP 的通道以接收服务器通知，从而提高通过 MCP 代理实时分发和处理来自服务器命令的能力。

UDP

用户数据报协议 (User Datagram Protocol, UDP) 是一种用于 IP 的无连接通信协议，使应用程序可以向其他程序发送消息。有关信息，请参考“DARPA Internet Program RFC 768”。

Uncleanable File（非可清除文件）

病毒扫描引擎无法清除以下文件：

受特洛伊木马感染的文件

特洛伊木马是执行意外或未授权操作（通常是恶意操作，例如显示消息、删除文件或格式化磁盘）的程序。特洛伊木马不感染文件，因此不需要清除。

解决方法： 防毒墙网络版使用病毒清除引擎和病毒清除模板来移除特洛伊木马。

受蠕虫病毒感染的文件

计算机蠕虫病毒是可以将其自身功能性副本或段传播到其他计算机系统的自包含程序（或程序集）。传播通常通过网络连接或电子邮件附件进行。由于文件是自包含程序，因此蠕虫病毒无法清除。

解决方法： 趋势科技建议删除蠕虫病毒。

已写保护的受感染文件

解决方法： 去掉写保护以允许防毒墙网络版清除该文件。

受密码保护的文件

包括受密码保护的压缩文件或受密码保护的 Microsoft Office 文件。

解决方法： 去掉密码保护以便防毒墙网络版清除这些文件。

备份文件

扩展名为 RB0 到 RB9 的文件为受感染文件的备份副本。防毒墙网络版将创建受感染文件的备份，以防在清除过程中病毒/恶意软件损坏文件。

解决方法： 如果防毒墙网络版成功清除受感染文件，则不需要保留备份副本。如果计算机正常运行，则可以删除备份文件。

回收站中的受感染文件

由于系统正在运行，因此防毒墙网络版可能无法删除回收站中的受感染文件。

解决方法：

对于使用 NTFS 文件系统运行 Windows 2000/XP/Server 2003 的计算机，执行以下步骤：

1. 以管理员权限登录到计算机。
2. 关闭所有正在运行的应用程序以防止其锁定文件，锁定将使 Windows 无法删除该文件。
3. 打开命令提示符，然后键入以下命令来删除这些文件：

```
cd \  
  
cd recycled  
  
del *.* /S
```

最后的命令删除回收站中的所有文件。

4. 检查文件是否已被删除。

对于运行其他操作系统（或不使用 NTFS 的 NT 平台）的计算机，执行以下步骤：

1. 在 MS-DOS 模式下重新启动计算机。
2. 打开一个命令提示符，然后键入以下命令来删除这些文件：

```
cd \  
  
cd recycled  
  
del *.* /S
```

最后的命令删除回收站中的所有文件。

3. 在正常模式下重新启动计算机。

Windows Temp 文件夹或 Internet Explorer 临时文件夹中的受感染文件

防毒墙网络版可能无法清除 Windows Temp 文件夹或 Internet Explorer 临时文件夹中的受感染文件，因为计算机正在使用它们。要清除的文件可能是 Windows 操作所需的临时文件。

解决方法：

对于使用 NTFS 文件系统运行 Windows 2000/XP/Server 2003 的计算机，执行以下步骤：

1. 以管理员权限登录到计算机。
2. 关闭所有正在运行的应用程序以防止其锁定文件，锁定将使 Windows 无法删除该文件。
3. 如果受感染文件在 Windows Temp 文件夹中：

- a. 打开命令提示符并转到 Windows Temp 文件夹（缺省情况下，对于 Windows XP/Server 2003 计算机，位于 C:\Windows\Temp，对于 Windows NT/2000 计算机，位于 C:\WinNT\Temp）。

- b. 键入以下命令来删除这些文件：

```
cd temp
attrib -h
del *.* /S
```

最后的命令删除 Windows Temp 文件夹中的所有文件。

4. 如果受感染文件在 Internet Explorer 临时文件夹中：

- a. 打开命令提示符并转到 Internet Explorer Temp 文件夹（缺省情况下，对于 Windows 2000/XP/Server 2003 计算机，位于 C:\Documents and Settings\<您的用户名>\Local Settings\Temporary Internet Files）。

- b. 键入以下命令来删除这些文件：

```
cd tempor~1
attrib -h
del *.* /S
```

最后的命令删除 Internet Explorer 临时文件夹中的所有文件。

- c. 检查文件是否已被删除。

对于运行其他操作系统（或那些不使用 NTFS 的）的计算机：

1. 在 MS-DOS 模式下重新启动计算机。
2. 如果受感染文件在 Windows Temp 文件夹中：
 - a. 出现命令提示符后，请转至 Windows Temp 文件夹。Windows XP/Server 2003 中 Windows Temp 文件夹的缺省位置为 C:\Windows\Temp。Windows 2000 中 Windows Temp 文件夹的缺省位置为 C:\WinNT\Temp。
 - b. 打开命令提示符，然后键入以下命令来删除这些文件：

```
cd temp  
attrib -h  
del *.* /S
```

最后的命令删除 Windows Temp 文件夹中的所有文件。
 - c. 在正常模式下重新启动计算机。
3. 如果受感染文件在 Internet Explorer 临时文件夹中：
 - a. 出现命令提示符后，请转到 Internet Explorer 临时文件夹。Windows 2000/XP/Server 2003 中 Internet Explorer 临时文件夹的缺省位置为 C:\Documents and Settings\<您的用户名>\Local Settings\Temporary Internet Files。
 - b. 键入以下命令：

```
cd tempor~1  
attrib -h  
del *.* /S
```

最后的命令删除 Internet Explorer 临时文件夹中的所有文件。
 - c. 在正常模式下重新启动计算机。