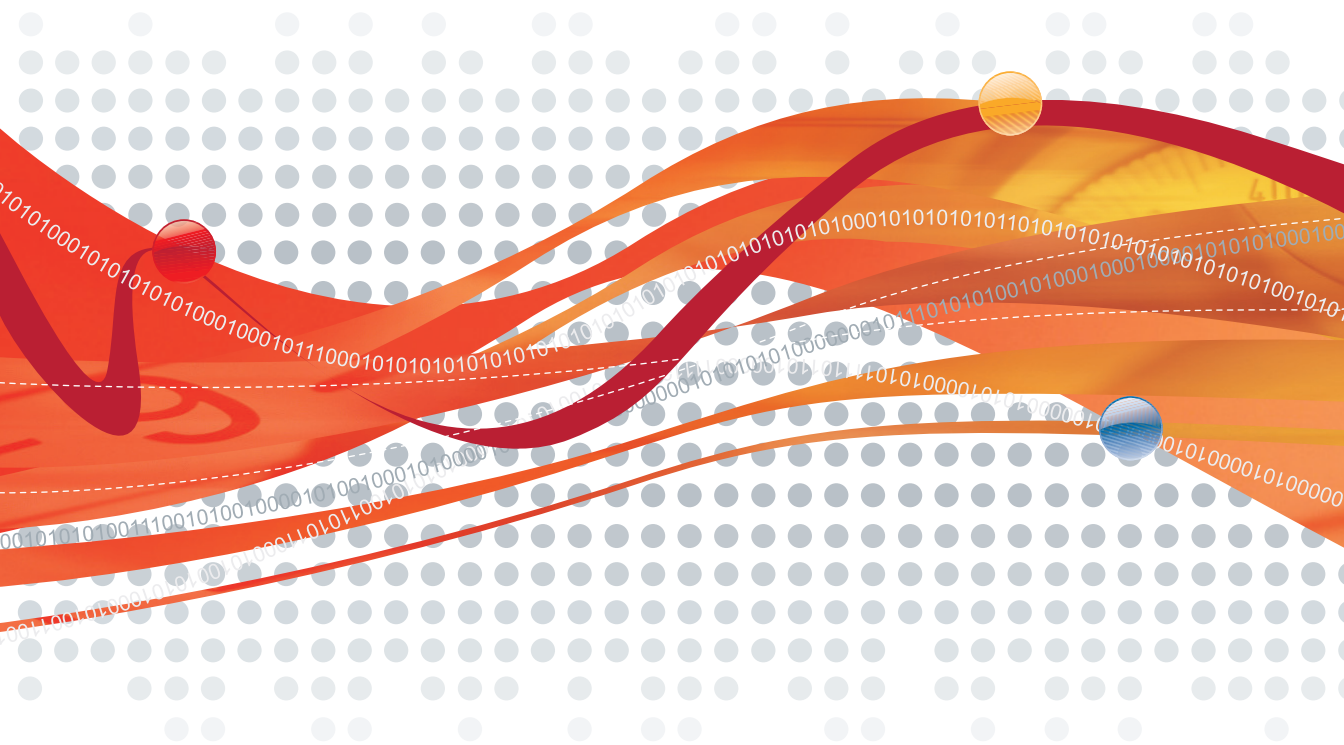
TREND MICRO

# OfficeScan™ Corporate Edition 8.0

针对企业台式机与网络服务器的综合性集成安全方案

## 管理员指南



Endpoint Security

Trend Micro Incorporated/ 趋势科技（中国）有限公司保留不经通知修改该文档及其所述产品的权利。在安装和使用本软件之前，请详阅自述文件、发布注释和最新版本的适用用户文档，这些都可从趋势科技 Web 站点获得：

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

趋势科技、趋势科技 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 是Trend Micro Incorporated/趋势科技（中国）有限公司的商标或注册商标。所有其他产品或公司名称均为其各自所有者的商标或注册商标。

版权所有 © 2001-2007 Trend Micro Incorporated/ 趋势科技（中国）有限公司。保留所有权利。

文档编号：OSCM83234/70529

发布日期：2007 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。

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

请在以下站点评估此文档：
http://www.trendmicro.com/download/zh-cn/default.asp

# 目录

## 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

- 防病毒 ..... 1-2
- 防火墙 ..... 1-3
- Web 威胁防护 ..... 1-3
- 组件复制 ..... 1-5
- 插件管理器 ..... 1-5
- Web 控制台管理 ..... 1-5
- 平台支持 ..... 1-6

关键功能和优点 ..... 1-7

- 安全风险防护 ..... 1-7
- 增强的防间谍软件功能 ..... 1-7
- 集中管理 ..... 1-7
- 安全和策略实施 ..... 1-8
- 防毒墙网络版防火墙 ..... 1-8
- 损害清除服务 ..... 1-11

防毒墙网络版服务器 ..... 1-12

防毒墙网络版服务器 ..... 1-13

防毒墙网络版组件与程序 ..... 1-20

- Hotfix、修补程序和 Service Pack ..... 1-24

安全风险 ..... 1-25

- 病毒和恶意软件 ..... 1-25
- 网络病毒 ..... 1-27
- 间谍软件和灰色软件 ..... 1-27

网络钓鱼攻击 ..... 1-31
防毒墙网络版文档 ..... 1-32
术语 ..... 1-33

## 第 2 章： 防毒墙网络版入门

Web 控制台 ..... 2-1
防毒墙网络版域 ..... 2-3
代理服务器设置 ..... 2-4
用于服务器组件更新的代理服务器 ..... 2-4
用于客户机组件更新的代理服务器 ..... 2-5
组件更新 ..... 2-6
更新源 ..... 2-6
组件复制 ..... 2-7
服务器更新 ..... 2-8
更新代理 ..... 2-12
客户机更新 ..... 2-14
组件更新权限和设置 ..... 2-19
组件还原 ..... 2-22
扫描设置 ..... 2-22
扫描类型 ..... 2-22
病毒 / 恶意软件扫描 ..... 2-24
间谍软件 / 灰色软件扫描 ..... 2-32
扫描权限 ..... 2-36
Web 站点信誉配置 ..... 2-37
Web 威胁 ..... 2-37
信誉分值 ..... 2-37
安全级别 ..... 2-37
Web 站点信誉策略和计算机位置 ..... 2-38
允许的 URL ..... 2-38

Web 站点信誉日志 ..... 2-39

第 3 章： 管理联网计算机

防毒墙网络版防火墙 ..... 3-2

策略 ..... 3-2
策略例外 ..... 3-3
概要文件 ..... 3-4
缺省设置 ..... 3-6
防火墙权限 ..... 3-8
防火墙测试 ..... 3-8
防火墙：如何禁用 ..... 3-8

爆发防护 ..... 3-9

爆发阻止 ..... 3-9
爆发阻止策略 ..... 3-9
爆发后任务 ..... 3-10

客户机通知 ..... 3-11

安全风险通知 ..... 3-11
其他通知 ..... 3-13

客户机 - 服务器连接验证 ..... 3-13

客户机权限和其他设置 ..... 3-14

全局客户机设置 ..... 3-16

客户机设置管理 ..... 3-18

Cisco NAC ..... 3-19

第 4 章： 管理防毒墙网络版服务器

趋势科技防毒墙控制管理中心 ..... 4-2

日志 ..... 4-2

联网计算机的日志 ..... 4-2
服务器更新日志 ..... 4-3
系统事件日志 ..... 4-4
日志删除 ..... 4-4

许可证 ..... 4-5

防毒墙网络版数据库备份 ..... 4-6

防毒墙网络版 Web 服务器信息 ..... 4-6

管理员通知 ..... 4-7

标准通知 ..... 4-8
爆发通知 ..... 4-8

Web 控制台密码 ..... 4-8

非活动客户机 ..... 4-9

隔离管理器 ..... 4-10

管理工具和客户机工具 ..... 4-10

全球病毒跟踪计划 ..... 4-12

第 5 章： 了解策略服务器 for Cisco NAC

组件和术语 ..... 5-2

组件 ..... 5-2
术语 ..... 5-3

Cisco NAC 体系结构 ..... 5-4

客户机验证顺序 ..... 5-5

策略服务器 ..... 5-7

策略服务器策略和规则 ..... 5-8

规则组成 ..... 5-9
缺省规则 ..... 5-11
策略组成 ..... 5-12
缺省策略 ..... 5-13

同步 ..... 5-14

证书 ..... 5-15

CA 证书 ..... 5-17

策略服务器系统需求 ..... 5-17

操作系统 ..... 5-17
硬件 ..... 5-18
Web 服务器 ..... 5-18
Web 控制台 ..... 5-18

Cisco Trust Agent (CTA) 需求 ..... 5-19

操作系统 ..... 5-19
硬件 ..... 5-19
其他 ..... 5-19

支持的平台和需求 ..... 5-20

第 6 章： 部署策略服务器 for Cisco NAC

策略服务器 for NAC 部署概述 ..... 6-2

Cisco Secure ACS 服务器登记 ..... 6-3

CA 证书安装 ..... 6-3

策略服务器 SSL 证书准备 ..... 6-6

Cisco Trust Agent 部署 ..... 6-8

Cisco Trust Agent 升级和部署 ..... 6-10
Cisco Trust Agent 安装验证 ..... 6-12

策略服务器 for Cisco NAC 安装 ..... 6-12

ACS 服务器配置 ..... 6-15

策略服务器 for Cisco NAC 配置 ..... 6-15

从防毒墙网络版配置策略服务器 ..... 6-16
策略服务器的摘要信息 ..... 6-17
策略服务器注册 ..... 6-18
规则 ..... 6-19
策略 ..... 6-19
客户机验证日志 ..... 6-19
客户机日志维护 ..... 6-20
管理工具 ..... 6-20

第 7 章： 使用控制管理中心管理防毒墙网络版

控制管理中心基本功能 ..... 7-2

趋势科技管理通信协议 ..... 7-3

降低网络负载和软件包大小 ..... 7-4
支持 NAT 和防火墙遍历 ..... 7-5
支持 HTTPS ..... 7-6
支持单向和双向通信 ..... 7-6
支持单点登录 (SSO) ..... 7-7

MCP 代理波动信号 ..... 7-7

时间表栏 ..... 7-8
正确的波动信号设置 ..... 7-9

防毒墙网络版注册 ..... 7-10

防毒墙网络版管理 ..... 7-10

产品目录 ..... 7-11
产品目录任务 ..... 7-11
防毒墙网络版配置 ..... 7-13
防毒墙网络版任务管理 ..... 7-14

防毒墙网络版日志 ..... 7-15
防毒墙网络版移除后恢复 ..... 7-17
搜索工具 ..... 7-18

目录管理器 ..... 7-19

目录管理器选项 ..... 7-19
目录管理器任务 ..... 7-20

临时 ..... 7-22

使用临时 ..... 7-23
与临时相关的任务 ..... 7-23

组件下载和部署 ..... 7-26

更新管理器 ..... 7-27
手动下载 ..... 7-27
预设下载例外 ..... 7-34
预设下载 ..... 7-35

报告 ..... 7-43

本地报告 ..... 7-44
全局报告 ..... 7-44
报告模板 ..... 7-45
报告概要文件 ..... 7-46
与报告相关的任务 ..... 7-47

第 8 章： 常见问题和故障排除资源

常见问题 ..... 8-1

组件更新 ..... 8-1
服务器管理 ..... 8-2
客户机管理 ..... 8-4
调试日志 ..... 8-5

故障排除资源 ..... 8-5

情况诊断工具 ..... 8-5

防毒墙网络版服务器日志 ..... 8-5
防毒墙网络版客户机日志 ..... 8-12

第 9 章： 与趋势科技联系

技术支持 ..... 9-1

加速您的支持呼叫 ..... 9-2

趋势科技知识库 ..... 9-3

TrendLabs ..... 9-3

安全信息中心 ..... 9-4

将可疑文件发送给趋势科技 ..... 9-4

文档反馈 ..... 9-5

附录 A： 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 .....A-1

防毒墙网络版集成 .....A-2

Check Point for 防毒墙网络版配置 .....A-4

安装 SecureClient 支持 .....A-5

附录 B： 词汇表

术语与定义 .....B-1

# 图表

普通客户机图标 ..... 1-14
漫游客户机图标 ..... 1-17
需要用户操作的客户机情况 ..... 1-17
客户机功能组件 ..... 1-19
防毒墙网络版组件 ..... 1-20
防毒墙网络版程序 ..... 1-22
病毒和恶意软件类型 ..... 1-25
间谍软件和灰色软件类型 ..... 1-27
防毒墙网络版文档中使用的术语 ..... 1-33
客户机组件更新过程中使用的代理服务器设置 ..... 2-5
组件更新选项 ..... 2-6
组件复制场景 ..... 2-10
更新代理的系统需求 ..... 2-13
选定客户机用户的组件更新权限 ..... 2-19
选定客户机用户的组件更新设置 ..... 2-19
预设更新场景 1 ..... 2-21
预设更新场景 2 ..... 2-21
病毒 / 恶意软件扫描条件 ..... 2-24
基于用户活动的实时扫描行为 ..... 2-25
全局病毒 / 恶意软件扫描设置 ..... 2-27
可用的病毒 / 恶意软件扫描处理措施 ..... 2-29
趋势科技建议的对病毒 / 恶意软件的扫描处理措施 ..... 2-30
其他病毒 / 恶意软件扫描处理措施选项 ..... 2-31
间谍软件 / 灰色软件扫描条件 ..... 2-32
可用间谍软件 / 灰色软件扫描处理措施 ..... 2-35
其他间谍软件 / 灰色软件扫描选项 ..... 2-36
客户机用户的扫描权限 ..... 2-36
缺省防火墙策略 ..... 3-6
缺省防火墙概要文件 ..... 3-7
缺省防火墙策略例外 ..... 3-7
选定客户机的权限和设置 ..... 3-14
全局客户机设置 ..... 3-16
策略服务器 for Cisco NAC 组件 ..... 5-2

与策略服务器 for Cisco NAC 相关的术语 ..... 5-3
缺省规则 ..... 5-11
Cisco NAC 证书 ..... 5-15
支持的平台和需求 ..... 5-20
控制管理中心功能 ..... 7-2
波动信号建议 ..... 7-9
控制管理中心产品目录 ..... 7-10
用于事件日志的搜索参数 ..... 7-16
用于安全日志的搜索参数 ..... 7-17
搜索参数 ..... 7-18
SCV 文件参数的名称和值 ..... A-4

第 1 章

# 防毒墙网络版简介

本章中的主题：


- *关于防毒墙网络版*（第 1-2 页）
- *此发行版的新功能*（第 1-2 页）
- *关键功能和优点*（第 1-7 页）
- *防毒墙网络版服务器*（第 1-12 页）
- *防毒墙网络版服务器*（第 1-13 页）
- *防毒墙网络版组件与程序*（第 1-20 页）
- *安全风险*（第 1-25 页）
- *防毒墙网络版文档*（第 1-32 页）

# 关于防毒墙网络版

趋势科技 ™ 防毒墙网络版 ™ 保护企业网络不受病毒、特洛伊木马、蠕虫病毒、黑客和网络病毒，再加上间谍软件和混合威胁攻击的危害。作为一个集成的解决方案，它可以保护台式机、便携式计算机和网络服务器，而基于 Web 的管理控制台可以使其轻松在每台客户机和服务器上设置协同的安全策略和部署自动更新。

通过与趋势科技网络病毒墙™或任何 Network Admission Control (NAC) 设备结合，防毒墙网络版可以在非兼容计算机上执行策略，然后补救、重定向、限制、拒绝或允许网络访问。

本章概述了防毒墙网络版的特性、功能和技术。

# 此发行版的新功能

防毒墙网络版包括以下新功能和增强：

## 防病毒

### 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 通过阻止带有实时压缩可执行文件的文件来帮助减少病毒 / 恶意软件进入您网络的风险。

要启用 IntelliTrap，请转到**联网计算机 > 客户机管理 > 设置 > { 扫描类型 } > 病毒 / 恶意软件**选项卡 **> 扫描设置**。

### GeneriClean

GeneriClean，也称为参照性清除，是一种即使没有病毒清除组件可用也能清除病毒 / 恶意软件的新技术。 GeneriClean 使用检测到的文件作为基础，确定检测到的文件是否在内存和注册表项中具有相应的进程 / 服务，然后将其一起移除。

## 防火墙

### 将允许的网络通信记入日志

除了根据防火墙策略允许或拒绝网络通信，防毒墙网络版客户机现在还可以将允许的网络通信记入日志，而且如果被授予权限，还能将这些日志发送给服务器。然后，无需中断客户机用户，您就可以审计来自客户端计算机的允许的网络通信并可以识别可能的恶意活动。

### 客户机防火墙日志

可以允许特定的客户机自动将防火墙日志发送到服务器（在**联网计算机 > 客户机管理 > 设置 > 权限和其他设置**中），并可制定发送日志的时间表（**联网计算机 > 全局客户机设置**）。

## Web 威胁防护

### Web 站点信誉

除了基于文件的扫描，防毒墙网络版现在还包括检测和阻止基于 Web 安全风险的功能，包括网络钓鱼攻击。请参阅 *Web 站点信誉配置*（第 2-37 页）以获取详细信息。

通过转到**联网计算机 > Web 站点信誉**来配置 Web 站点信誉设置。

## 防间谍软件

防毒墙网络版附带了新的间谍软件扫描和清除引擎，可以检测和清除比以前更多的间谍软件 / 灰色软件，误报更少。

该产品包括以下新功能：

### 实时检测

对文件系统进行实时间谍软件 / 灰色软件扫描会阻止或停止间谍软件执行。

### 间谍软件 / 灰色软件恢复

对间谍软件 / 灰色软件采取处理措施后，防毒墙网络版客户机会备份间谍软件 / 灰色软件数据，如果您认为间谍软件 / 灰色软件安全，则防毒墙网络版服务器可以随时将其恢复。可以选择要恢复的间谍软件 / 灰色软件数据段。

要恢复间谍软件 / 灰色软件，请转至**联网计算机 > 客户机管理 > 任务 > 间谍软件 / 灰色软件恢复**。

### 评估模式

评估模式允许您先评估间谍软件 / 灰色软件是否合法，然后根据您的评估采取处理措施。例如，可将合法的间谍软件 / 灰色软件添加到间谍软件 / 灰色软件批准列表。

要配置评估模式设置，请转到**联网计算机 > 全局客户机设置 > 间谍软件 / 灰色软件设置**。

### Rootkit 检测

此版本还包括了一个检测和移除 rootkit 的新组件。当前正在兴风作浪的 rootkit 破坏常规操作系统功能—应用程序通常假定其为合法的—以

获取对用户计算机的大部分控制权。如果不重新安装计算机，则移除 rootkit 将非常困难。

## 组件复制

每次防毒墙网络版更新其组件时，下载完整病毒码将占用大量带宽。此版本的防毒墙网络版仅下载新的可用病毒码，从而减少病毒码下载量。请参阅*组件复制*（第 2-7 页）以获取详细信息。

## 插件管理器

插件程序在产品发行版之外开发并且尚未完全集成到防毒墙网络版中。有了插件管理器，您不再需要等到产品发行才能开始使用插件程序。

这些程序开始可用时，插件管理器即会在防毒墙网络版 Web 控制台中显示它们，供防毒墙网络版服务器和防毒墙网络版客户机使用。然后可以从 Web 控制台中安装和管理上述程序，包括将客户机插件程序部署到客户机。

通过在 Web 控制台的主菜单上单击**插件管理器**来下载和安装插件管理器。安装后，可以检查可用的插件程序。

## Web 控制台管理

- 管理员和客户机用户现在可以各自管理防间谍软件和防病毒功能。
- 使用客户机树上的菜单项管理所有与客户机相关的任务。
- 通过在主菜单中单击 “通知”来管理 Web 控制台中的通知消息和设置。

## 平台支持

Microsoft 证实防毒墙网络版客户机支持 Windows™ Vista™ 平台 （32 位和 64 位）。

**注意：** 防毒墙网络版服务器不支持 Microsoft Vista。

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

- Microsoft Outlook™ 邮件扫描
- Check Point™ SecureClient™
- Cisco™ NAC 2
- 看守程序 DLL 注入功能
- 镜像安装实用程序 (ImgSetup.exe)

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

- 感染源通知 （“警报器服务”已移除）

# 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

防毒墙网络版保护您的联网计算机免受病毒 / 恶意软件、间谍软件 / 灰色软件和 Web 威胁的危害。防毒墙网络版客户机提供安全风险防护，向防毒墙网络版服务器报告事件以及从防毒墙网络版服务器获得更新。防毒墙网络版服务器托管 Web 控制台，从更新源 （例如，趋势科技 ActiveUpdate 服务器）下载更新以及启动客户机以更新组件。

## 增强的防间谍软件功能

防毒墙网络版可防御各种间谍软件，其中包括广告程序、拨号程序、恶作剧程序、远程访问工具和密码破解程序。通过使用全面最新的间谍软件数据库和定制的例外列表，可降低与间谍软件相关的延迟、崩溃和支持呼叫的风险。防毒墙网络版还阻止键盘侧录软件盗取机密信息，保持带宽以及保护企业生产率。这些能力完善了趋势科技 InterScan™ Web Security Suite 的功能，还提供了从 Web 网关到客户机 / 服务器网络的端对端间谍软件防护。

## 集中管理

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机和服务器。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机和服务器上的自动部署。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全面的报告。管理员可以执行远程管理，为个别台式机或组设置定制的策略以及锁定客户机安全设置。

## 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 自我防御网络中实现最有效的策略实施。防毒墙网络版还包括策略服务器，用于与 Cisco Access Control Server 自动进行通信。当与趋势科技网络病毒墙™ 或任何 Network Admission Control (NAC) 设备结合时，防毒墙网络版都可以检查试图进入网络的客户机，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将隔离此计算机及其所在的网段，直到所有 PC 都已更新或清除完成。

## 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机和服务器。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。

**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。有关互联网连接防火墙的详细信息，请参阅您的 Microsoft 文档。

### 网络通信过滤

防毒墙网络版防火墙过滤所有入站和出站的网络通信，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
- 源起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。

### 可定制的概要文件和策略

防毒墙网络版防火墙让您可以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机。这提供了为客户机组织和配置防火墙设置的高度定制的方法。

### 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；它监视到客户机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，过滤决定不仅基于概要文件和策略，还基于通过分析连接和过滤经过防火墙的数据包所建立的环境。

### 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机的特征码。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**：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。目标计算机会持续向自身发送 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。

### 客户机防火墙权限

您可以授予客户机用户在防毒墙网络版客户机控制台上查看他们的防火墙设置的权限。还可以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。

## 损害清除服务

损害清除服务™通过全自动过程，清除计算机上基于文件的病毒和网络病毒以及病毒和蠕虫病毒残留 （特洛伊木马、注册表项和含病毒的文件）。防毒墙网络版和损害清除服务是趋势科技企业防护战略 (EPS) 的关键组件，专为前瞻性管理病毒爆发周期 （从漏洞阻止到恶意代码消除）而设计。

有关企业防护战略的更多信息，请访问以下 Web 站点：

http://www.trendmicro.com/cn/home/enterprise.htm

### 损害清除服务解决方案

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
- 杀死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，因此不需要配置它。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。

# 防毒墙网络版服务器

防毒墙网络版基于 HTTP 的服务器是所有客户机配置、安全风险日志和客户机程序及更新的中央储存库。

该服务器执行两个重要功能：

- 安装、监控和管理联网计算机客户机
- 从趋势科技更新服务器下载组件并将它们分发给客户机

防毒墙网络版服务器可提供服务器与客户机之间的实时、双向通信。可以从基于浏览器的 Web 控制台 （可从网络中的任何虚拟位置访问）管理客户机。该服务器通过超文本传输协议 (HTTP) 与客户机（和使用服务器的客户机）通信。该服务器仅安装基于 HTTP 的客户机。如果客户端计算机不支持 TCP/IP，则无法安装基于 HTTP 的客户机。

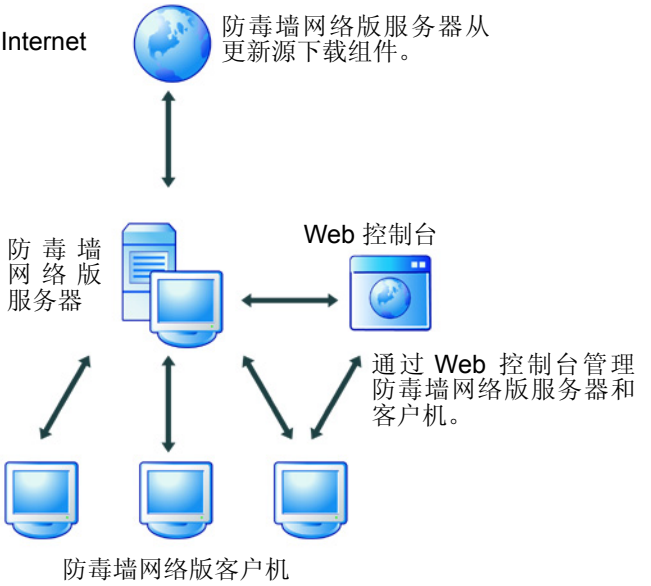



**图 1-1　　基于 HTTP 的服务器的工作原理**

## 防毒墙网络版服务器

通过在每台计算机上安装防毒墙网络版客户机可保护 Windows 计算机免受安全风险的危害。该客户机将提供三种扫描方法：实时扫描、预设扫描和手动扫描。

客户机会向作为其安装源的父服务器报告。可以通过使用客户机迁移程序工具使客户机向另一服务器报告（有关此工具的详细信息，请参阅联机帮助）。客户机会实时向服务器发送事件和状态信息以为您提供更新的客户机信息。事件的示例包括病毒 / 恶意软件检测、客户机启动、客户机关闭、扫描启动和更新完成。

从客户机控制台 （如果您授予用户此权限）和服务器 Web 控制台配置客户机上的扫描设置。要在整个网络上执行统一的桌面保护，请选择不要授予客户机修改扫描设置或移除客户机程序的权限。

防毒墙网络版客户机有两种类型：

- 普通客户机
- 漫游客户机

## 普通客户机

普通客户机与服务器保持持续的连接。防毒墙网络版系统托盘图标的变化反映了普通客户机的状态更改。

**注意：** 防毒墙网络版不仅对实时扫描使用实时扫描服务，还对手动扫描和预设扫描使用实时扫描服务。这表示如果实时扫描服务停止，客户端计算机将失去保护。如果实时扫描停止运行，则图标的颜色也会变为红色。

**表 1-1 普通客户机图标**

| 图标 | 状态 | 描述 | 实时扫描 |
|---|---|---|---|
| | 联机 | 所有组件为最新并且服务工作正常。 | 已启用 |
| | 联机 | 病毒码文件暂时尚未更新。 | 已启用 |
| | 联机 | 立即扫描、手动扫描或预设扫描正在运行。在病毒/恶意软件和间谍软件/灰色软件扫描过程中显示此图标。 | 已启用 |

**表 1-1　　普通客户机图标**

| 图标 | 状态 | 描述 | 实时扫描 |
|---|---|---|---|
| | 联机 | 实时扫描已禁用。<br>**注意：** 如果对间谍软件 / 灰色软件禁用了实时扫描，但却对病毒 / 恶意软件启用实时扫描，则客户机上的实时扫描状态为 “已启用”，且客户机图标为：<br> | 已禁用 |
| | 联机 | 实时扫描已禁用并且病毒码文件暂时尚未更新。 | 已禁用 |
| | 联机 | 实时扫描服务已停止。 | 已禁用 |
| | 联机 | 实时扫描服务已停止并且病毒码文件暂时尚未更新。 | 已禁用 |
| | 脱机 | 客户机与服务器已断开连接。 | 已启用 |
| | 脱机 | 客户机已从服务器断开连接并且病毒码文件暂时尚未更新。 | 已启用 |
| | 脱机 | 客户机已断开连接并且实时扫描已禁用。 | 已禁用 |
| | 脱机 | 客户机已从服务器断开连接；实时扫描已禁用；并且病毒码文件暂时尚未更新。 | 已禁用 |
| | 脱机 | 客户机已从服务器断开连接并且实时扫描服务已停止。 | 已禁用 |
| | 脱机 | 客户机已从服务器断开连接；实时扫描服务已停止；并且病毒码文件暂时尚未更新。 | 已禁用 |

### 漫游客户机

处于漫游模式中的客户机会被隔离，因此，无法与防毒墙网络版服务器通信。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。尽管与服务器的通信已中断，但如果漫游客户机连接到互联网并且配置为从更新代理或趋势科技 ActiveUpdate 服务器获取更新，则仍然可以更新组件。

应为长期与防毒墙网络版服务器失去连接的客户机分配漫游权限。要分配该权限，请转至**联网计算机 > 客户机管理 > 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机的更新：

- 客户机用户执行手动更新时
- 设置了自动更新部署并且将漫游客户机包含在将要更新的客户机中时
- 授予了客户机启用预设更新的权限时

有关如何更新客户机的详细信息，请参阅*客户机更新*（第 2-14 页）。

防毒墙网络版系统托盘图标的变为反映漫游客户机的状态。

**注意：** 防毒墙网络版不仅对实时扫描使用实时扫描服务，还对手动扫描和预设扫描使用实时扫描服务。这表示如果实时扫描服务停止，客户端计算机将失去保护。如果实时扫描停止运行，则图标的颜色也会变为红色。

**表 1-2 漫游客户机图标**

| 图标 | 描述 | 实时扫描 |
|---|---|---|
| | 所有组件为最新并且服务工作正常。 | 已启用 |
| | 实时扫描已禁用。 | 已禁用 |
| | 病毒码文件暂时尚未更新。 | 已启用 |
| | 实时扫描已禁用并且病毒码文件暂时尚未更新。 | 已禁用 |
| | 实时扫描服务已停止。 | 已禁用 |
| | 实时扫描服务已停止并且病毒码文件暂时尚未更新。 | 已禁用 |

## 所需的用户操作

如果客户机图标表示以下情况中的任意一种，则请执行必要的操作。

**表 1-3 需要用户操作的客户机情况**

| 情况 | 操作 |
|---|---|
| 暂时不更新的病毒码文件 | 客户机用户需要更新组件。从 Web 控制台中，可在**更新 > 联网计算机**中配置组件更新设置，或在**联网计算机 > 客户机管理 > 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。 |

| 情况 | 操作 |
| --- | --- |
| 实时扫描服务已停止 | 用户可以从 “Windows 服务”窗口手动启动该服务 (OfficeScan NT 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 > 客户机管理 > 设置 > 实时扫描设置**）。 |
| 实时扫描已禁用且客户机处于漫游模式 | 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。 |
| 与服务器断开连接的客户机 | 先从 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 > 联网计算机的日志 > 连接验证**）。如果验证后客户机仍处于断开连接状态：<br>• 如果连接状态在服务器和客户机上均为脱机，则请检查网络连接。<br>• 如果连接状态在客户机上为脱机但在服务器上为联机，则服务器域名可能已更改，而客户机将使用该域名连接到服务器（如果在服务器安装过程中选中域名） 。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 文件夹 }\system32\drivers\etc 文件夹中的“hosts”文件。<br>• 如果连接状态在客户机上为联机但在服务器上为脱机，则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机的通信，但是会允许客户机到服务器的通信。<br>• 如果连接状态在客户机上为联机但在服务器上为脱机，则客户机的 IP 地址可能已更改，但是其状态在服务器上还未更新（例如，重新加载客户机时）。可以尝试重新部署该客户机。 |

## 受支持的操作系统的客户机功能组件

防毒墙网络版客户机支持 Windows 2000、 XP/Server 2003 （32 位和 64 位）和 Vista 操作系统。

**表 1-4　　客户机功能组件**

| 功能 | Windows 2000 | Windows XP/Server 2003 （32 位） | Windows XP/Server 2003 （64 位） | Windows Vista |
|---|---|---|---|---|
| 手动扫描、实时扫描和预设扫描 | ✓ | ✓ | ✓ | ✓ |
| 组件更新（手动和预设更新） | ✓ | ✓ | ✓ | ✓ |
| 更新代理 | ✓ | ✓ | ✓ | ✓ |
| Web 站点信誉 | ✓ | ✓ | ✓ | ✓ |
| Microsoft Outlook 邮件扫描 | ✓ | ✓ | | |
| 防毒墙网络版防火墙 | ✓ | ✓ | ✓ | ✓ |
| 损害清除服务 | ✓ | ✓ | ✓ | ✓ |
| Cisco NAC 支持 | ✓ | ✓ | | |
| 插件管理器 | ✓ | ✓ | ✓ | ✓ |
| 漫游模式 | ✓ | ✓ | ✓ | ✓ |

**表 1-4　　客户机功能组件**

| 功能 | Windows 2000 | Windows XP/Server 2003（32 位） | Windows XP/Server 2003（64 位） | Windows Vista |
|---|---|---|---|---|
| SecureClient 支持 | ✓ | ✓ | | |

# 防毒墙网络版组件与程序

防毒墙网络版包括以下组件与程序：

**表 1-5　　防毒墙网络版组件**

| 组件 | 描述 |
|---|---|
| **防病毒** | |
| 病毒码 | 帮助防毒墙网络版识别表示病毒存在的病毒特征（独特模式位和字节）的文件（有关详细信息，请参阅*病毒码*（第 1-22 页）） |
| 病毒扫描引擎 | 对病毒 / 恶意软件进行扫描并采取适当处理措施的引擎；支持 32 位和 64 位平台 |
| IntelliTrap 特征码 | 用于检测打包为可执行文件的实时压缩文件的文件 |
| IntelliTrap 例外特征码 | 包含 “批准的”压缩文件列表的文件 |
| **防间谍软件** | |
| 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 | 对间谍软件/灰色软件进行扫描并采取适当处理措施的引擎；支持 32 位和 64 位平台 |

**表 1-5　　防毒墙网络版组件**

| 组件 | 描述 |
|---|---|
| 间谍软件主动监控特征码 | 用于实时间谍软件 / 灰色软件扫描的文件<br>**注意：** 仅当同时激活防病毒和 Web 威胁防护服务时，此组件才可用。 |
| Venus Spy Trap 引擎 | 允许应用程序监控新的可执行文件，并在发现间谍软件 / 灰色软件时删除间谍软件/灰色软件；支持 32 位和 64 位平台<br>**注意：** 当仅激活 Web 威胁防护服务时，此组件才可用。如果同时激活防病毒和 Web 威胁防护服务，此组件将不可用。 |
| **损害清除服务** | |
| 病毒清除引擎 | 引擎损害清除服务用于扫描及移除特洛伊木马和特洛伊木马进程；支持 32 位和 64 位平台 |
| 病毒清除模板 | 此模板由病毒清除引擎使用，可帮助识别特洛伊木马文件和进程，以便引擎可以清除它们 |
| **防火墙** | |
| 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的网络病毒；支持 32 位和 64 位平台 |
| 通用防火墙特征码 | 此文件类似于病毒码，可帮助防毒墙网络版识别表示病毒存在的病毒签名 （独特模式位和字节） |
| **Web 站点信誉** | |
| URL 过滤引擎 | 可简化防毒墙网络版和趋势科技 URL 过滤服务之间的通信的引擎。URL 过滤服务是一个将 URL 分级并向防毒墙网络版提供分级信息的系统。 |
| **公共组件** | |
| 防 rootkit 驱动程序 | 由间谍软件扫描引擎使用的内核方式驱动程序，提供绕开任何由 rootkit 引起的潜在重定向的功能；支持 32 位平台 |

**表 1-6　　防毒墙网络版程序**

| 程序 | 描述 |
|---|---|
| 客户机程序 | 防毒墙网络版客户机程序，提供抵御安全风险的实际防护；支持 32 位和 64 位平台 |
| Cisco Trust Agent | 用于启用客户机与路由器之间通信的支持 Cisco NAC 的程序；仅当如果安装有面向 Cisco NAC 的策略服务器时才有效。 |
| Hotfix 和安全修补程序 | 对客户相关问题或新发现的安全漏洞的工作区解决方案，可以从趋势科技 Web 站点下载，然后部署到防毒墙网络版服务器和 / 或客户机程序 |

**注意：** 除这些组件外，防毒墙网络版客户机还从防毒墙网络版服务器接收更新的配置文件。客户机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。

## 病毒码

趋势科技病毒扫描引擎使用一个外部数据文件，称为病毒码。病毒码包括帮助防毒墙网络版识别最新病毒 / 恶意软件和混合攻击的信息。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。

所有使用 ActiveUpdate 功能的趋势科技产品可以在趋势科技服务器上检测病毒码新版本的可用性，和/或自动轮询该服务器以获取最新文件。

**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。

可以从以下 Web 站点下载病毒码和其他防毒墙网络版病毒码文件，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/

### 趋势科技扫描引擎

所有趋势科技产品的核心是一个扫描引擎。扫描引擎最初是为了响应早期的文件型计算机病毒而开发的，现在已非常精密复杂，并且能够检测互联网蠕虫病毒、群发邮件、特洛伊木马威胁、网络钓鱼站点、间谍软件、网络利用以及病毒。扫描引擎可检测两种类型的威胁：

- **正在传播：**正在积极传播
- **已得到控制的：**已控制的病毒，不传播，但是开发出来用于研究

不是扫描每个文件的每个字节，而是引擎和病毒码文件协同工作，不仅识别病毒代码的指示特征，还识别文件中病毒可能隐藏的精确位置。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

趋势科技通过将多数对时间灵敏的病毒 / 恶意软件信息存储在病毒码中，能够将扫描引擎更新次数最小化，同时还会将防护保持最新。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

## Hotfix、修补程序和 Service Pack

在官方产品发布后，趋势科技经常会开发出 Hotfix、修补程序和 Service Pack，以解决问题，增强产品性能以及添加新功能。

以下是趋势科技可能发布的项的摘要：

- **Hotfix**：单个客户报告的问题的变通方法或解决方法。 Hotfix 特定于问题，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）。
- **安全修补程序**：针对安全问题且适用于所有客户部署的 Hotfix。Windows 安全修补程序包括一个安装程序，而非 Windows 修补程序通常有一个安装脚本。
- **修补程序**：一组解决多个程序问题的 Hotfix 和安全修补程序。趋势科技会定期提供修补程序。Windows 修补程序包括一个安装程序，而非 Windows 修补程序通常有一个安装脚本。

- **Service Pack**：足以成为产品升级的 Hotfix、修补程序和功能组件增强的组合。Windows 和非 Windows Service Pack 都包括一个安装程序和安装脚本。

您的供应商或技术支持提供商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、修补程序和 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。

**注意：** 缺省情况下，防毒墙网络版客户机可以安装 Hotfix。如果不想要客户机安装 Hotfix，则请通过在 Web 控制台中转至**联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 设置**选项卡更改客户机更新设置。

# 安全风险

安全风险是病毒 / 恶意软件、间谍软件 / 灰色软件和 Web 威胁的统称。防毒墙网络版可以保护计算机不受以下安全风险的危害：

## 病毒和恶意软件

现在有好几万个病毒 / 恶意软件，每天还有更多的被创建出来。虽然计算机病毒一度流行于 DOS 或 Windows，如今，通过利用企业网络、电子邮件系统和 Web 站点的漏洞，计算机病毒会导致更大量的损害。

**表 1-7　　病毒和恶意软件类型**

| 类型 | 描述 |
|---|---|
| 恶作剧程序 | 象病毒一样的程序，经常操纵计算机显示器上的内容 |

**表 1-7　　病毒和恶意软件类型**

| 类型 | 描述 |
|---|---|
| 特洛伊木马 | 可执行程序，不复制，而是驻留在系统上执行恶意行为，例如为电脑黑客潜入打开端口。特洛伊木马程序常常使用端口获得计算机的访问权。声称要清除计算机里的病毒，实际上将病毒入站计算机的应用程序，就是特洛伊木马程序的一个示例。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 | 执行复制的程序。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 页面上执行 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 Java 中、独立于操作系统的病毒代码 |
| 宏病毒 | 编码为应用程序的宏且通常包含在文档里的病毒 |
| VBScript、JavaScript 或 HTML 病毒 | 驻留在 Web 页面上且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），能将自身或片段的功能副本传播到其他计算机系统 （通常通过电子邮件） |
| 测试病毒 | 行为类似真的病毒的无害文件，病毒扫描软件可检测到。使用测试病毒 （例如， EICAR 测试脚本）以验证防病毒安装正在正常扫描。 |
| 加壳软件 | 压缩且 / 或加密的 Windows 或 Linux™ 可执行程序，通常为特洛伊木马程序。压缩可执行文件使得加壳软件更难以被防病毒产品检测到。 |

## 网络病毒

严格来说，通过网络传播的病毒不是网络病毒。上述病毒 / 恶意软件中，只有部分（例如，蠕虫病毒）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和阻止网络病毒。

## 间谍软件和灰色软件

您的计算机存在潜在威胁而没有病毒 / 恶意软件的风险。间谍软件 / 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的计算机性能产生不利影响，并为贵组织带来重大安全、机密和法律风险的应用程序或文件。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。

### 间谍软件 / 灰色软件的类型

防毒墙网络版可检测以下间谍软件 / 灰色软件类型：

**表 1-8　　间谍软件和灰色软件类型**

| 类型 | 描述 |
|---|---|
| 间谍软件 | 收集数据 （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 |
| 广告软件 | 显示广告并收集数据 （如， Web 冲浪首选项）以用于将未来广告的目标指向用户 |

**表 1-8　　间谍软件和灰色软件类型**

| 类型 | 描述 |
|---|---|
| 拨号程序 | 更改客户机的互联网设置，并强制计算机通过调制解调器拨打预配置的电话号码。这些通常是按呼叫付费，或者是会为贵组织产生高额费用的国际号码。 |
| 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 | 帮助黑客进入计算机 |
| 远程访问工具 | 帮助黑客远程访问及控制计算机 |
| 密码破解应用程序 | 帮助破解帐户的用户名和密码 |
| 其他 | 其他类型的潜在恶意程序 |

### 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授权合约书 (EULA)，用户在下载前必须接受此授权合约书。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，将有导致以下后果的潜在可能：

- **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运行在您网络上的其他应用程序或网络之外的其他位置。
- **丢失个人和公司信息：**并非间谍软件 / 灰色软件应用程序收集的所有数据都如同用户访问的 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输入以访问他们个人帐户 （例如，银行帐户）和访问网络资源的公司帐户的用户名和密码。
- **更高的法律责任风险：**如果您网络上的计算机资源被劫持，黑客可能能够利用您的客户端计算机在您网络外的计算机上发动攻击或安装间谍软件 / 灰色软件。如果您的网络资源参与这些类型的活动，将可能使贵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

您可以采取许多方法阻止间谍软件 / 灰色软件安装到您的计算机上。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*扫描类型*（第 2-22 页）以获取详细信息。
- 培养您的客户机用户进行以下操作：
  - 对于他们要下载及安装到计算机上的应用程序，阅读最终用户授权合约书 (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”，除非客户机用户确信该软件的创建者和他们查看的 Web 站点都可信。
  - 不理会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。趋势科技建议要求 Web 浏览器安装 ActiveX 控件之前提示用户。要提高 Internet Explorer™ (IE) 的安全级别，请转至**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，并仔细检查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未被防毒墙网络版检测为灰色软件，但您认为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。
- 将您的 Windows 操作系统始终更新到最新的 Microsoft 修补程序。请参阅 Microsoft Web 站点以了解详细信息。

## 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。该电子邮件包含一个到看似真实的 Web 站点的 URL （复制合法的电子邮件和 Web 网点非常容易），但是随后会更改所谓的后台 （即，所收集数据的收件人）。

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、信用卡号或社会安全号。

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*将可疑文件发送给趋势科技*（第 9-4 页）以获取详细信息。

# 防毒墙网络版文档

防毒墙网络版的文档集包括以下内容：

- **安装与部署指南**：PDF 文档，包括安装防毒墙网络版服务器和客户机的需求和过程
- **管理员指南**：PDF 文档，包含防毒墙网络版概述、入门信息、安全风险防护和防毒墙网络版管理
- **联机帮助**：编译为 WebHelp 格式的 HTML 文件，提供操作指导、使用建议和字段特定信息。可通过防毒墙网络版服务器和客户机控制台访问联机帮助。也有策略服务器控制台、漏洞扫描程序工具和防毒墙网络版主安装程序的帮助文件。
- **自述文件**：包含已知问题和基本安装步骤列表。该文件可能还包含联机帮助或印刷文档中尚未包括的最新产品信息。

可以在 http://www.trendmicro.com/download/zh-cn/ 下载最新版本的《安装与部署指南》以及 《管理员指南》。

## 术语

**表 1-9　　防毒墙网络版文档中使用的术语**

| 术语 | 描述 |
|---|---|
| 客户机 | 防毒墙网络版客户机程序 |
| 客户端计算机 | 安装有防毒墙网络版客户机的计算机 |
| 客户机用户 （或用户） | 在客户端计算机上管理防毒墙网络版客户机的人 |
| 服务器 | 防毒墙网络版服务器程序 |
| 服务器计算机 | 安装有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 |
| 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 |
| 产品服务 | 包括防病毒、损害清除服务和 Web 威胁防护 — 在防毒墙网络版安装过程中可以激活的所有功能 |
| 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 ofcservice.exe。 |
| 程序 | 包括防毒墙网络版客户机、 Cisco Trust Agent 和插件管理器 |
| 组件 | 负责对安全风险进行扫描、删除和采取处理措施 |

第 2 章

# 防毒墙网络版入门

本章中的主题：


- *Web 控制台*（第 2-1 页）
- *防毒墙网络版域*（第 2-3 页）
- *代理服务器设置*（第 2-4 页）
- *组件更新*（第 2-6 页）
- *扫描设置*（第 2-22 页）
- *Web 站点信誉配置*（第 2-37 页）


## 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 控制台使用标准的互联网技术，如 Java、CGI、 HTML 和 HTTP。

可以使用 Web 控制台执行以下操作：

- 管理在联网计算机上安装的客户机
- 将客户机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调用手动扫描
- 接收有关网络中安全风险的通知并查看由客户机发送的日志
- 使用电子邮件、寻呼机和 SNMP Trap 发布爆发

从网络中安装有所需的 Web 浏览器和通信协议的任一计算机中打开 Web 控制台。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：

- 在缺省站点上无 SSL：http://{ 防毒墙网络版服务器 }/OfficeScan
- 在虚拟站点上无 SSL：http://{ 防毒墙网络版服务器 }:{ 端口号 }/OfficeScan
- 在缺省站点上有 SSL：https://{ 防毒墙网络版服务器 }/OfficeScan
- 在虚拟站点上有 SSL：https://{ 防毒墙网络版服务器 }:{ 端口号 }/OfficeScan

**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。

# 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、运行相同任务的客户机。通过将客户机分组为域，可以同时对所有域成员配置、管理和应用相同的配置。

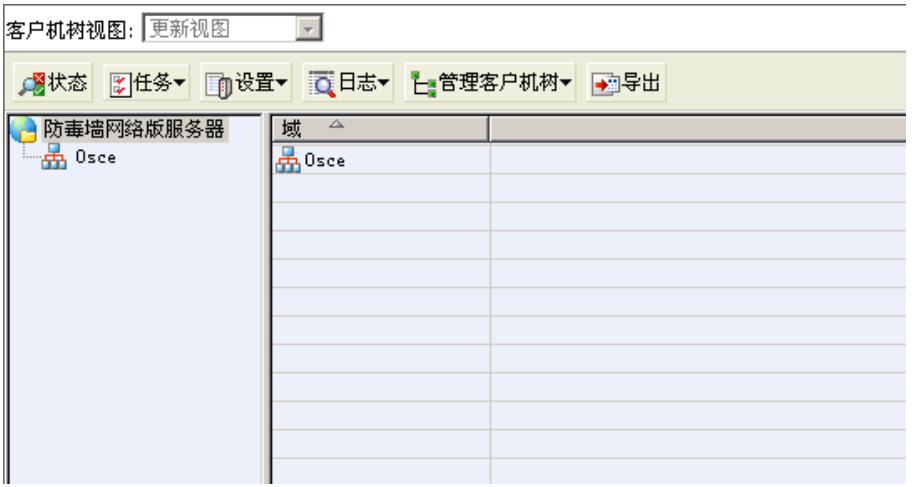



**图 2-1　　带有域列表的防毒墙网络版客户机树**

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

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

缺省情况下，防毒墙网络版模拟网络上的域。客户机树中的域名和客户机名与网络中的域名和计算机名同名。防毒墙网络版还根据网络上的域结构分配客户机。可以删除或重命名防毒墙网络版创建的域、创建一个新域、或将客户机从一个域转移到另一个域。

**提示：** 也可以通过现有的 NetBIOS、 Windows Active Directory™、或 DNS 域对客户机进行分组。要使用此设置，请在 Web 控制台中转至 **联网计算机 > 全局客户机设置 > 客户机分组**。

# 代理服务器设置

可以配置防毒墙网络版服务器以在连接到 ActiveUpdate 服务器时使用互联网代理服务器设置来更新组件。类似地，可以配置客户机以在与服务器通信和更新组件时使用内部网代理服务器设置。更新组件时客户机可以使用的其他设置包括自动代理服务器设置和用户配置的代理服务器设置 （如果授予用户配置代理服务器设置的权限）。

## 用于服务器组件更新的代理服务器

要配置服务器以使用代理服务器访问互联网和连接到 ActiveUpdate 服务器，请转至**管理 > 代理服务器设置 > Internet 代理服务器**。有关服务器组件更新的详细信息，请参阅*服务器更新*（第 2-8 页）。

## 用于客户机组件更新的代理服务器

防毒墙网络版客户机在自动更新过程中或执行“立即更新”时使用代理服务器设置。有关自动更新和立即更新的详细信息，请参阅*客户机更新方法*（第 2-15 页）。

**表 2-1　　客户机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 | • 在**联网计算机 > 全局客户机设置**中配置的自动代理服务器设置。<br>• 在**管理 > 代理服务器设置 > Intranet 代理服务器**选项卡中配置的内部网代理服务器设置。 | • 防毒墙网络版客户机将首先使用自动代理服务器设置来更新组件。<br>• 如果未启用自动代理服务器设置，则将使用内部网代理服务器设置。<br>• 如果两种设置都禁用，则客户机将不使用任何代理服务器设置。 |
| 立即更新 | • 在**联网计算机 > 全局客户机设置**中配置的自动代理服务器配置设置。<br>• 用户配置的代理服务器设置。可以在**联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 权限**选项卡中授予用户配置代理服务器设置的权限。 | • 防毒墙网络版客户机将首先使用自动代理服务器设置来更新组件。<br>• 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。<br>• 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机用户没有所需的权限，则更新组件时客户机将不使用任何代理服务器。 |

# 组件更新

要帮助确保客户机处于不受最新安全风险危害的状态，请定期更新防毒墙网络版组件。有关其他组件的信息，请参阅*防毒墙网络版组件与程序*（第 1-20 页）。

要配置防毒墙网络版以更新组件，请执行以下操作：

1. 更新服务器。请参阅*服务器更新*（第 2-8 页）。
2. 分配特定客户机以充当更新代理，并配置设置 （有关详细信息，请参阅*更新代理*（第 2-12 页））。
3. 更新客户机。请参阅*客户机更新*（第 2-14 页）。

## 更新源

选择更新源时，请考虑客户机和更新源之间的网络部分的带宽（有关更新如何影响网络通信的详细信息，请参阅 《*安装与部署指南*》）。下表描述了不同的组件更新选项和建议使用它们的时间。

**表 2-2　　组件更新选项**

| 更新选项 | 描述 | 建议 |
|---|---|---|
| ActiveUpdate 服务器 >> 防毒墙网络版服务器 >> 客户机 | 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，并将在客户机上启动组件更新。 | 如果防毒墙网络版服务器和客户机之间的网络无低带宽部分，则使用此方法。 |
| ActiveUpdate 服务器 >> 防毒墙网络版服务器 >> 更新代理 >> 客户机 | 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，并将在客户机上启动组件更新。然后充当更新代理的客户机将通知客户机更新组件。 | 如果防毒墙网络版服务器和客户机之间的网络有低带宽部分，则使用此方法以平衡网络上的网络通信负载。 |

**表 2-2　　组件更新选项**

| 更新选项 | 描述 | 建议 |
| --- | --- | --- |
| ActiveUpdate 服务器 >> 更新代理 >> 客户机 | 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，并通知客户机更新组件。 | 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。<br>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 >> 客户机 | 防毒墙外客户机直接从 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机的过程中遇到问题时，使用此方法。<br>在多数情况下，客户机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。 |

## 组件复制

可以从趋势科技 ActiveUpdate 服务器下载最新版本的完整病毒码文件时，也可以下载 14 个 “增量病毒码”。增量病毒码是完整病毒码文件的较小版本，说明了最新病毒码文件版本和先前完整的病毒码文件版本之间的差异。例如，如果最新版本为 175，则增量病毒码 v_173.175 包括在 V175 中、但不在 V173 中的签名（由于发布的病毒码编号增量为 2，因此 V173 是前一完整病毒码版本）。增量病毒码 v_171.175 包括在 V175 中但不在 V171 中的签名。

要减少下载最新病毒码时产生的流量，防毒墙网络版会执行组件复制，这是一种组件更新方法，其中防毒墙网络版服务器和更新代理只下载增量病毒码。

组件复制适用于以下组件：

- 病毒码
- 间谍软件特征码
- 间谍软件主动监控特征码
- 病毒清除模板
- IntelliTrap 例外特征码

有关防毒墙网络版服务器和更新代理的组件复制原理，请参阅以下各节：

- *防毒墙网络版服务器的组件复制过程*（第 2-9 页）
- *更新代理的组件复制过程*（第 2-14 页）

## 服务器更新

通常，趋势科技仅在防毒墙网络版新版本发布过程中更新扫描引擎。但是，趋势科技会定期发布病毒码文件以保持您的客户机防护为最新。由于定期提供病毒码文件更新，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病毒码文件。请参阅*更新代理*（第 2-12 页）以获取详细信息。

- 趋势科技建议每天更新以确保服务器和客户机都有最新的组件。
- 如果使用代理服务器连接到互联网，则请确保已适当配置代理服务器设置以成功下载更新。要配置代理服务器设置，请转至**管理 > 代理服务器设置**。
- 更新后，在**日志 > 服务器更新日志**中验证服务器更新日志。

### 服务器更新方法

防毒墙网络版将为您提供服务器的以下组件更新方法：

- **预设更新**：配置服务器以基于时间表检查更新源和自动下载任何可用的更新。要配置预设的更新设置，请转至**更新 > 服务器 > 预设更新**。
- **手动更新**：趋势科技建议安装 / 升级防毒墙网络版服务器后和有爆发时手动更新服务器组件。要手动更新服务器，请转至**更新 > 服务器 > 手动更新**或单击主菜单顶部的**立即更新服务器**。

### 服务器更新源

配置服务器以从趋势科技 ActiveUpdate 服务器或另一个源下载防毒墙网络版组件 （**更新 > 服务器 > 更新源**）。

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，自动通知客户机更新其组件。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**立即通知客户机。

---

**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机更新。

---

### 防毒墙网络版服务器的组件复制过程

有可用的新版本时立即更新组件可减小组件复制对服务器性能的影响。因此，请确保定期下载组件。

为帮助说明服务器的组件复制，请参考以下场景：

**表 2-3　　组件复制场景**

| | |
|---|---|
| 防毒墙网络版服务器上的完整病毒码 | 当前版本 : 171 |
| | 其他可用版本：<br>169　167　165　163　161　159 |
| ActiveUpdate 服务器上的最新版本 | 完整病毒码版本：175 |
| | 增量病毒码：<br>173.175　171.175　169.175　167.175　165.175　163.175　161.175<br>159.175　157.175　155.175　153.175　151.175　149.175　147.175 |

1. 防毒墙服务器将其当前完整病毒码版本与 ActiveUpdate 服务器上的最新版本进行比较。如果两个版本之差小于或等于 14，则服务器只下载代表两个版本之差的增量病毒码。

   **注意：** 如果此差值大于 14，则服务器自动下载完整版本的病毒码文件和 14 个增量病毒码。

   基于示例说明：

   - V171 与 V175 之差为 2。换言之，服务器没有 V173 和 V175。
   - 服务器将下载增量病毒码 171.175。此增量病毒码代表 V171 和 V175 之间的差异。

2. 服务器将该增量病毒码和其当前完整病毒码合并以生成最新的完整病毒码。

   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。
   - 服务器有 1 个增量病毒码 (171.175) 和最新的完整病毒码 (V175)。

3. 服务器基于服务器上可用的其他完整病毒码生成增量病毒码。如果服务器不生成这些增量病毒码，错过下载较早增量病毒码的客户机将自动下载完整病毒码文件，这将造成更大的网络流量。

   基于示例说明：

   - 由于服务器具有病毒码 V169、V167、V165、V163、V161 和 V159，因此它可以生成以下增量病毒码：

     169.175 167.175 165.175 163.175 161.175 159.175

   - 服务器不需要使用 V171，因为它已经具有增量病毒码 171.175。

   - 现在，服务器有 7 个增量病毒码：

     171.175 169.175 167.175 165.175 163.175 161.175 159.175

   - 服务器保留这最新的 7 个完整病毒码版本 （V175、 V171、 V169、 V167、 V165、 V163 和 V161）。并去除任何旧版本 (V159)。

4. 服务器将其当前增量病毒码与 ActiveUpdate 服务器上可用的增量病毒码进行比较。服务器下载它没有的增量病毒码。

   基于示例说明：

   - ActiveUpdate 服务器有 14 个增量病毒码：

     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有 7 个增量病毒码：

  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 个增量病毒码：

  173.175 157.175 155.175 153.175 151.175 149.175 147.175

- 现在，服务器有 ActiveUpdate 服务器上可用的所有增量病毒码。

5. 最新的完整病毒码和 14 个增量病毒码已提供给客户机。

## 更新代理

如果认识到客户机和防毒墙网络版服务器之间的网络的“低带宽”或“大流量”部分，则可以将防毒墙网络版客户机分配为充当更新代理，或充当其他客户机的更新源。这将帮助分摊向所有客户机部署组件的负担。

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，则趋势科技建议在每个段上至少允许一台客户机充当更新代理。

## 更新代理的需求和详细信息

**表 2-4. 更新代理的系统需求**

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

## 更新代理配置

1. 在**联网计算机 > 客户机管理 > 设置 > 更新代理设置**中授予客户机充当更新代理的权限。

2. 选择一个更新代理可以用于接收更新组件的更新源。

   **要启用更新代理以从防毒墙网络版服务器处获取组件更新，请转至更新 > 联网计算机 > 更新源。**

---

**注意：** 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。请参阅*更新代理*（第 2-12 页）以获取详细信息。

---

3. 在**更新 > 联网计算机 > 更新源 > 定制的更新源列表**中，指定将从更新代理更新的客户机，然后分配相应的更新代理。

**注意：** 单个更新代理可以处理的并行客户机连接的数量取决于计算机的硬件规格。

### 更新代理的组件复制过程

1. 更新代理将其当前完整病毒码版本与更新源上的最新版本进行比较。如果两个版本之差小于或等于 14，则更新代理只下载代表两个版本之差的增量病毒码。

**注意：** 如果此差值大于 14，则更新代理自动下载完整版本的病毒码文件。

2. 更新代理将其下载的增量病毒码和其当前完整病毒码合并以生成最新的完整病毒码。
3. 更新代理下载更新源上的所有剩余增量病毒码。
4. 最新的完整病毒码和所有 14 个增量病毒码已提供给客户机。

## 客户机更新

要确保客户机处于不受最新安全风险危害的状态，请定期更新客户机组件。有关防毒墙网络版组件的列表，请参阅*防毒墙网络版组件与程序*（第 1-20 页）。不能从 Web 控制台的**更新**菜单中升级防毒墙网络版程序。

**注意：** 有关防毒墙网络版客户机程序升级的信息，请参阅《安装与部署指南》。要升级 Cisco Trust Agent，请转至 **Cisco NAC > 代理部署**。

除组件外，防毒墙网络版客户机在客户机更新过程中还自动接收更新过的配置文件。客户机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。

更新客户机前，请验证服务器的组件为最新。有关如何更新服务器的信息，请参阅*服务器更新*（第 2-8 页）。

### 客户机更新方法

可以使用自动或手动更新在客户机上启动组件更新。还可以授予用户手动更新客户机组件的权限。

- **自动更新：**趋势科技建议您始终使用自动更新。它可移除置于执行手动更新的客户机上的负担，并可消除客户端计算机没有最新组件的风险。

  要配置自动更新设置，请转至**更新 > 联网计算机 > 自动更新**。还可以配置客户机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*用于服务器组件更新的代理服务器*（第 2-4 页）。

  - **事件触发更新：**服务器可以通知联机客户机在下载最新组件后更新组件，还可以在脱机客户机重新启动并连接到服务器时通知它们。（可选）更新后在客户端计算机上启动立即扫描 （手动扫描）。

---

**注意：** 如果防毒墙网络版服务器在下载组件后，无法向客户机成功发送更新通知，则会在 15 分钟自动重新发送通知。服务器在客户机响应之前，会连续发送更新通知，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。**使客户机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（漫游客户机除外）**，如果选择该选项更新组件，则组件更新将仍然继续。

---

- **基于时间表更新：**带有执行预设更新权限的客户机会根据指定的时间表检查更新的客户机更新源。指定时间表前，请选择可以执行预设更新的客户机。

  - 要向选定的客户机授予启用 / 禁用预设更新的权限，请转至**联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 权限**选项卡 **> 组件更新权限**。授予权限时，缺省设置为启用预设更新。如果客户机用户从客户机控制台禁用预设更新，则更新将不会在指定的更新日期和时间继续。

  - 要自动启用预设更新而无需客户机用户干预，请转到**联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 其他设置**选项卡 **> 更新设置**。

  有关将基于时间表更新与网络地址转换一起使用的信息，请参阅*使用 NAT 的客户机预设更新*（第 2-18 页）。

- **手动更新：**要启用手动更新，请转至**更新 > 联网计算机 > 手动更新**。趋势科技建议客户机组件严重过时和有爆发时手动更新客户机组件。客户机较长时间无法从更新源更新组件时，客户机组件将严重过时。

- **在客户机上立即更新：**要向客户机用户授予手动更新客户机组件的权限，请转至**联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 权限**选项卡 **> 组件更新权限**。授予该权限后，客户机用户右键单击系统托盘内的防毒墙网络版客户机图标时，可以使用 “立即更新”选项。还可以允许客户机以在 “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*用于服务器组件更新的代理服务器*（第 2-4 页）。

## 客户机更新源

客户机将从在**更新 > 联网计算机 > 更新源**中指定的更新源获取更新。可以选择防毒墙网络版服务器或定制的更新源。

### 更新源优先级

如果防毒墙网络版客户机无法从选定的更新源更新，则会尝试其他源。更新源优先级如下：

1. 首先是定制的更新源列表中的第一项 （如果从定制的源更新），接下来为第二项，以此类推。
2. 防毒墙网络版服务器 （如果选择直接从标准更新源更新，或在所有定制的更新源不可用的情况下，如果选择从防毒墙网络版服务器更新）。
3. 趋势科技 ActiveUpdate 服务器。这是最后可用的更新源。如果客户端计算机已有互联网连接，则可直接从趋势科技 ActiveUpdate 服务器更新组件。有两种方法可实施此选项：
   a. 通过转到**联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 其他设置**选项卡 **> 更新设置**，将 ActiveUpdate 服务器用作备份源。
   b. 强制客户机从 ActiveUpdate 服务器 （作为首选）更新。要执行此操作，请在**更新 > 联网计算机 > 更新源**中将 ActiveUpdate 服务器添加到 “定制的更新源列表”，并确保其位于该列表的顶部。将 ActiveUpdate 服务器作为更新源添加时，您需要其 URL，如下所示：http://www.trendmicro.com/download/zh-cn/。不能从浏览器打开此 URL。

**提示：** 趋势科技建议您将 ActiveUpdate 服务器用作备份源。强制所有客户机持续从 ActiveUpdate 服务器（作为首选）更新可极大地降低本地网络与 Internet 之间的网络带宽耗用。趋势科技建议您仅当从防毒墙网络版服务器或更新代理更新遇到问题时使用此选项。

## 使用 NAT 的客户机预设更新

如果网络使用网络地址转换 (NAT)，则会出现以下问题：

- 客户机在 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机更新和配置更改。

可以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机来解决这些问题。

**执行以下操作：**

- 在客户端计算机上安装防毒墙网络版客户机之前：
  - 在**更新 > 联网计算机 > 自动更新 > 基于时间表更新**中配置客户机更新时间表。
  - 在**联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 权限**选项卡 **> 组件更新权限**中授予客户机启用预设更新的权限。
- 如果在客户端计算机上已存在防毒墙网络版客户机：
  - 在**联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 权限**选项卡 **> 组件更新权限**中给于客户机执行 “立即更新” 的权限。
  - 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。

客户机更新时，会收到更新的组件和配置文件。

## 组件更新权限和设置

在**联网计算机 > 客户机管理 > 设置 > 权限和其他设置**中为选定的客户机配置更新权限和设置。

### 权限

**表 2-5　　选定客户机用户的组件更新权限**

| 选项 | 描述 | 客户机控制台导航 |
|---|---|---|
| 执行“立即更新” | 允许客户机用户手动更新客户机组件 | 右键单击系统托盘上的防毒墙网络版图标，然后单击“立即更新”。 |
| 启用预设更新 | 允许客户机用户启用 / 禁用预设更新。尽管用户具有启用 / 禁用预设更新的权限，但没有配置实际时间表的权限。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。 | 右键单击系统托盘上的防毒墙网络版图标，然后单击“{启用 / 禁用} 预设更新”。 |

### 其他设置

**表 2-6　　选定客户机用户的组件更新设置**

| 选项 | 描述 | 客户机控制台导航 |
|---|---|---|
| 客户机从趋势科技 ActiveUpdate 服务器下载更新 | 启动更新时，防毒墙网络版客户机首先从**更新 > 联网计算机 > 更新源**窗口中指定的更新源中获取更新。如果更新失败，则客户机尝试从防毒墙网络版服务器更新。如果从防毒墙网络版服务器更新失败，则选择此选项可使客户机能够尝试从趋势科技 ActiveUpdate 服务器更新。 | 无 |

**表 2-6　　选定客户机用户的组件更新设置**

| 选项 | 描述 | 客户机控制台导航 |
|---|---|---|
| 启用预设更新 | 此选项允许您启用 / 禁用选定客户机上的预设更新。 | 无 |
| 客户机可以更新组件，但不能升级客户机程序也不能部署 Hotfix | 此选项允许组件更新继续，但是阻止使用所有升级方法部署 Hotfix 和升级客户机。<br>如果不选择此选项，则所有客户机将同时连接到服务器以升级或安装 Hotfix。如果有很多客户机，则这可能大大影响服务器性能。<br>如果选择此选项，则计划如何将客户机升级或 Hotfix 在服务器上部署的影响最小化，然后再执行您的计划。<br>有关客户机升级方法的详细信息，请参阅*《安装与部署指南》*。 | 无 |

### 关于 “权限”选项卡和 “其他设置”选项卡中 “启用预设更新”选项的注释

有两种在选定客户机上启用 / 禁用预设更新的方法。

- 授予客户机启用 / 禁用预设更新的权限。
- 自己启用 / 禁用预设更新而没有任何用户的打扰。

可以选择一个或同时选择两个选项。有关这些选项的工作原理的信息，请参阅下面的两个表。

**表 2-7　　预设更新场景 1**

| 预设更新选项 | 状态 | 结果 |
|---|---|---|
| 在**权限**选项卡上 | 已启用 （用户具有启用 / 禁用预设更新的权限） | 如果客户机用户禁用预设更新，则在更新时间表指定的时间内，防毒墙网络版客户机将不会更新组件。否则，更新将继续。 |
| 在**其他设置**选项卡上 | 已启用或已禁用 | |

**表 2-8　　预设更新场景 2**

| 预设更新选项 | 状态 | 结果 |
|---|---|---|
| 在**权限**选项卡上 | 已禁用 | 在更新时间表指定的时间内，防毒墙网络版客户机将更新组件。 |
| 在**其他设置**选项卡上 | 已启用 | |

### 组件还原

还原是指恢复到先前的病毒码或病毒扫描引擎版本。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前一版本，以及病毒码的最近五个版本。

**注意：** 可以只还原病毒码和病毒扫描引擎。

防毒墙网络版将对运行 32 位和 64 位平台的客户机使用不同的扫描引擎。需要分别还原这些扫描引擎。所有类型的扫描引擎的还原过程都相同。

要还原组件，请转至**更新 > 还原**。

## 扫描设置

要配置扫描设置，请在 Web 控制台上转至**联网计算机 > 客户机管理 > 设置 > { 扫描类型 }**。

在**联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 权限**选项卡 **> { 防病毒 / 反间谍软件权限 }** 中授予客户机用户配置扫描设置的权限。

### 扫描类型

防毒墙网络版将提供多种扫描类型以保护您的客户机不受病毒 / 恶意软件和间谍软件 / 灰色软件的危害。

#### 实时扫描

防毒墙网络版实时扫描文件。如果防毒墙网络版没有检测到安全风险，则用户可以继续打开或保存文件。如果防毒墙网络版检测到一个安全风险，则显示内容为文件名和特定安全风险的通知消息。可以配置将在**通知 > 客户机用户通知**中显示的通知消息。

### 手动扫描

用户在客户机控制台中启动对病毒 / 恶意软件的手动扫描后，手动扫描会立即开始。扫描时间的长度取决于要扫描文件的数量及客户端计算机的硬件资源。间谍软件 / 灰色软件的扫描时间和范围取决于您或（具有手动扫描配置权限的）客户机用户指定的扫描方法。可以在 Web 控制台的 “手动扫描设置”页中选择使用的扫描方法。

### 预设扫描

预设扫描和手动扫描的扫描行为相似。唯一的区别是预设扫描在预设的日期和时间自动运行。使用预设扫描在客户机上使例行任务扫描自动化并提高扫描管理效率。

### 立即扫描

立即扫描和手动扫描是同一类型的扫描。唯一的不同是您使用 Web 控制台远程启动立即扫描，而用户在其客户端计算机上本地运行手动扫描。

## 病毒 / 恶意软件扫描

本部分为您提供可用的病毒 / 恶意软件扫描选项和设置。

### 病毒 / 恶意软件扫描条件

防毒墙网络版将提供以下病毒 / 恶意软件扫描条件：

**表 2-9　　病毒 / 恶意软件扫描条件**

| 扫描条件 | 选项和描述 | 扫描类型 |
|---|---|---|
| 要扫描的文件 | 选择一个：<br>• 所有可扫描文件：扫描用户打开或保存的所有文件<br>• 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，甚至是用无害扩展名伪装的文件。<br>• 仅带有指定的扩展名的文件 | 所有类型 |
| 扫描设置 | 多个选择：<br>• 扫描引导区：扫描客户端计算机硬盘的引导区<br>• 扫描网络上的映射驱动器和共享文件夹：扫描任何映射到客户端计算机的网络驱动器或文件夹<br>• 扫描隐藏文件夹<br>• 启用 IntelliTrap：阻止实时压缩可执行文件并将其与其他恶意软件特征配对。<br>• 不扫描层数多于指定压缩层数的压缩文件<br>• 在系统关闭期间扫描软盘 | <br>手动扫描、预设扫描、立即扫描<br>手动扫描、实时扫描<br>手动扫描<br>所有类型<br>所有类型<br>实时扫描 |
| CPU 使用率 | 选择一个：<br>• 高：不间断连续扫描文件<br>• 中：文件扫描时有短暂的暂停<br>• 低：文件扫描时有较长的暂停 | 手动扫描、预设扫描、立即扫描 |

**表 2-9　　病毒 / 恶意软件扫描条件**

| 扫描条件 | 选项和描述 | 扫描类型 |
|---|---|---|
| 用户对要扫描的文件执行的活动 | 选择一个：<br>• 扫描正在创建 / 修改的文件<br>• 扫描正在检索的文件<br>• 扫描正在创建 / 修改和检索的文件<br>有关用户活动的示例，请参阅表 2-10。 | 实时扫描 |
| 时间表 | 选择一个 （然后选择扫描开始时间）：<br>• 每日一次<br>• 每周一次<br>• 每月一次 | 预设扫描 |

**表 2-10　　基于用户活动的实时扫描行为**

| 活动 | 如果选定的选项是 ... | | |
|---|---|---|---|
| | 扫描正在创建 / 修改的文件 | 扫描正在检索的文件 | 扫描正在创建 / 修改和检索的文件 |
| 打开只读文件 | “实时扫描”未扫描该文件。 | “实时扫描”扫描该文件。 | “实时扫描”扫描该文件。 |
| 从排除扫描的目录中复制或移动文件 | 实时扫描将在目标目录中扫描该文件（如果防毒墙网络版没有排除此目录免于扫描）。 | “实时扫描”未扫描目标目录中的文件 | 实时扫描将在目标目录中扫描该文件（如果防毒墙网络版没有排除此目录免于扫描）。 |

### 病毒 / 恶意软件扫描例外

要提高扫描性能和跳过可引起假警报的扫描文件，可以排除特定文件、文件扩展名和目录。手动扫描、实时扫描、预设扫描和立即扫描都有其单独的例外列表。

要配置扫描例外设置，请转至**联网计算机 > 客户机管理 > 设置 { 扫描类型 }**。

- 对于手动扫描、预设扫描和立即扫描，请转至**病毒 / 恶意软件**选项卡 **> 扫描例外**。
- 对于实时扫描，请转至**目标**选项卡 **> 扫描例外**。

防毒墙网络版可在扫描中排除以下趋势科技产品的目录。如果有一个趋势科技产品未列在下面，则可以手动将产品目录添加到扫描例外列表。

- 防毒墙群件版 ™ for Microsoft Exchange （除 V7 外的所有版本）

  **注意：** 如果使用 V7，则可以将以下文件夹添加到例外列表：\Smex\Temp、 \Smex\Storage、 \Smex\ShareResPool\

- ScanMail eManager™ 3.11、 5.1、 5.11、 5.12
- 面向 Lotus Notes™ eManager NT 的防毒墙群件版
- 趋势科技防毒墙 ™ 邮件安全版
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan VirusWall 3.53
- InterScan FTP VirusWall

- InterScan Web VirusWall
- InterScan E-mail VirusWall
- InterScan NSAPI 插件
- InterScan eManager 3.5x

**注意：** 还可以通过转至**联网计算机 > 全局客户机设置 > 病毒 / 恶意软件扫描设置**配置防毒墙网络版，以将 Microsoft Exchange 2000/2003 目录从手动扫描、实时扫描、预设扫描和立即扫描中排除。对于 Microsoft Exchange 2007，需要手动将目录添加到扫描例外列表。有关扫描例外的详细信息，请参考 http://technet.microsoft.com/en-us/library/bb332342.aspx。

## 全局病毒 / 恶意软件扫描设置

在**联网计算机 > 全局客户机设置**中配置全局病毒 / 恶意软件扫描设置。

**表 2-11　　全局病毒 / 恶意软件扫描设置**

| 设置 | 描述 |
|---|---|
| 配置大型压缩文件的扫描设置 | 防毒墙网络版将检查文件大小和病毒/恶意软件计数限制以确定是否要扫描包含在压缩文件中的单个文件。<br>• **如果解压缩后文件大小超过 __ MB，则不对其进行扫描：**防毒墙网络版不扫描任何超过限制的文件。<br>• **防毒墙网络版检测到第 __ 个压缩文件中的病毒 / 恶意程序后即停止扫描：**防毒墙网络版已检测到指定数量的病毒 / 恶意软件时，将停止扫描压缩文件中剩余的未扫描文件。压缩文件中检测到的大量病毒 / 恶意软件造成了很大的威胁，并导致访问文件不安全。请考虑手动删除压缩文件，而不是使病毒扫描引擎对压缩文件中包含的每个被感染文件都采取处理措施。<br>• **清除压缩文件中的病毒：**对压缩文件中检测到的病毒 / 恶意软件的扫描处理措施为 “清除”。 |

**表 2-11　　全局病毒 / 恶意软件扫描设置**

| 设置 | 描述 |
|---|---|
| 最多扫描 __ 个 OLE 层 | 通过对象链接与嵌入 (OLE)，用户可以用一个应用程序创建对象，然后将这些对象链接到或嵌入第二个应用程序。 |
| 将“手动扫描”添加到客户端计算机的 Windows 快捷菜单中 | 启用此选项使用户可以通过右键单击 Windows 桌面上或 Windows 资源管理器内的文件或文件夹，然后单击**使用防毒墙网络版客户机扫描**来扫描文件和文件夹。 |
| 从实时扫描中排除防毒墙网络版服务器数据库文件夹 | 缺省情况下，防毒墙网络版不扫描自己的数据库。趋势科技建议保持此设置以防止在扫描过程中可能发生的任何对数据库可能的任何损坏。 |
| 扫描中排除 Microsoft Exchange 服务器文件夹 | 在手动扫描、实时扫描、预设扫描和立即扫描的过程中，防毒墙网络版不会扫描 Microsoft Exchange 2000/2003 服务器文件夹中是否有病毒 / 恶意软件。如果使防病毒和 Web 威胁防护服务同时激活，启用此选项也不会在实时扫描过程中扫描 Microsoft Exchange 文件夹中是否有间谍软件 / 灰色软件。<br>**注意：** 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。有关扫描例外的详细信息，请参考 http://technet.microsoft.com/en-us/library/bb332342.aspx，有关该过程的信息，请参阅 *病毒 / 恶意软件扫描例外*（第 2-26 页）。 |

## 病毒 / 恶意软件扫描处理措施

防毒墙网络版可以基于在**联网计算机 > 客户机管理 > 设置 > {扫描类型} > 处理措施**选项卡中指定的扫描设置针对病毒 / 恶意软件采取各种处理措施。可以使用 ActiveAction（趋势科技建议的扫描处理措施）或为每个病毒 / 恶意软件类型都定制扫描处理措施。如果选择 ActiveAction，则不再需要为每个病毒 / 恶意软件类型都指定扫描处理措施。有关每个病毒 / 恶意软件类型的详细信息，请参阅 *病毒和恶意软件*（第 1-25 页）。

以下是可用的扫描处理措施：

**表 2-12　　可用的病毒 / 恶意软件扫描处理措施**

| 扫描处理措施 | 描述 | 扫描类型 |
|---|---|---|
| 删除 | 删除受感染文件 | 所有类型 |
| 隔离 | 更名受感染文件并将其移动到客户端计算机的隔离目录（即，{ 防毒墙网络版客户机文件夹 }\Suspect）中。客户机连接到服务器时，会将隔离的文件发送到服务器的隔离目录中。防毒墙网络版将为服务器计算机中的隔离文件加密和更名。<br>缺省服务器隔离目录为 { 防毒墙网络版服务器文件夹 }\PCCSRV\Virus，该目录可以通过转至**联网计算机 > 客户机管理 > 设置 > { 扫描类型 } > 处理措施**选项卡来更改。还可以恢复加密的文件。 | 所有类型 |
| 清除 | 清除可清除的文件后才允许对该文件进行完全访问，或者使指定的下一处理措施处理非可清除文件。<br>如果选择 “清除”，则可以配置第二个处理措施。如果清除失败，则防毒墙网络版将采取此扫描处理措施。 | 所有类型 |
| 更名 | 将受感染文件的扩展名更改为 “vir”。用户最初不能打开该文件，但是将该文件与特定应用程序关联后即可打开该文件。打开更名的受感染文件时，病毒 / 恶意软件可能执行。 | 所有类型 |
| 不予处理 | 允许完全访问受感染文件，而不对该文件执行任何操作。用户可以复制 / 删除 / 打开该文件。 | 手动扫描、预设扫描、立即扫描 |
| 文件拒绝访问 | 拒绝访问 （复制、打开）受感染文件。客户机将不把该文件移动到其他位置 （与隔离相对）。用户可以手动删除该文件。 | 实时扫描 |

**表 2-13　　趋势科技建议的对病毒 / 恶意软件的扫描处理措施**

| 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 | 第一项处理措施 |
| 恶作剧程序 | 隔离 | 无 | 隔离 | 无 |
| 特洛伊木马 | 隔离 | 无 | 隔离 | 无 |
| 病毒 | 清除 | 隔离 | 清除 | 隔离 |
| 测试病毒 | 文件拒绝访问 | 无 | 不予处理 | 无 |
| 加壳软件 | 隔离 | 无 | 隔离 | 无 |
| 其它 | 清除 | 隔离 | 清除 | 隔离 |
| 常规 * | 不予处理 | 无 | 不予处理 | 无 |

* 趋势科技根据某些特征将此病毒 / 恶意软件类型标记为可疑。“不予处理”只是暂时的扫描处理措施。确定病毒 / 恶意软件是否是安全风险后，趋势科技将相应更改扫描处理措施。

## 其他病毒 / 恶意软件扫描处理措施选项

**表 2-14　　其他病毒 / 恶意软件扫描处理措施选项**

<table>
<tr><th colspan="3">选项</th><th>扫描类型</th></tr>
<tr><td colspan="3">请指定隔离目录。<br>防毒墙网络版将先把隔离的文件存储在客户端计算机的 \Suspect 文件夹中，然后将这些文件发送到指定的隔离目录。<br>请以 URL、UNC 路径或绝对文件路径格式指定隔离目录。如果使用 UNC 路径，则请确保隔离目录文件夹已共享给组“Everyone”，且对此组分配了读取和写入权限。<br>警告：如果指定了不正确的隔离目录，则防毒墙网络版客户机会将文件保留在 \Suspect 文件夹上，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“无法将隔离的文件发送到指定的隔离文件夹”。<br>隔离目录可以是以下目录中的任何一个：</td><td rowspan="6">所有类型</td></tr>
<tr><th>隔离目录</th><th>接受的格式</th><th>示例</th></tr>
<tr><td>防毒墙网络版服务器计算机上的目录</td><td>URL<br><br>UNC 路径</td><td>http://{防毒墙网络版服务器 } （这是缺省路径。）<br>\\{防毒墙网络版服务器 }\ofcscan\Virus</td></tr>
<tr><td>另一台防毒墙网络版服务器计算机上的目录（如果网络上有其他服务器）</td><td>URL<br>UNC 路径</td><td>http://{防毒墙网络版服务器 2}<br>\\{防毒墙网络版服务器 2}\ofcscan\Virus</td></tr>
<tr><td>网络上的另一台计算机</td><td>UNC 路径</td><td>\\{ 计算机名 }\temp</td></tr>
<tr><td>客户端计算机上的另一个目录</td><td>绝对路径</td><td>C:\temp</td></tr>
<tr><td colspan="3">先备份后清除<br>客户端计算机上的备份目录是 OfficeScan Client\Backup。可以解密备份文件。有关解密备份文件的信息，请参阅联机帮助。</td><td>所有类型</td></tr>
</table>

**表 2-14　　其他病毒 / 恶意软件扫描处理措施选项**

| 选项 | 扫描类型 |
| --- | --- |
| **检测到病毒 / 恶意软件时在客户端计算机上显示通知消息**<br>要定制通知消息，请转至**通知 > 客户机用户通知 > 病毒 / 恶意软件**选项卡。 | 实时扫描、预设扫描 |

## 间谍软件 / 灰色软件扫描

本部分为您提供可用的间谍软件 / 灰色软件扫描选项和设置。

### 间谍软件 / 灰色软件扫描条件

防毒墙网络版将提供以下间谍软件 / 灰色软件扫描条件：

**表 2-15　　间谍软件 / 灰色软件扫描条件**

| 扫描条件 | 选项和描述 | 扫描类型 |
| --- | --- | --- |
| 扫描方法 | 选择一个：<br>• 快速：仅扫描间谍软件 / 灰色软件通常攻击的计算机区域<br>• 完全：扫描整个计算机 | 手动扫描、预设扫描、立即扫描 |
| 用户对要扫描的文件执行的活动 * | 选择一个：<br>• 扫描正在创建 / 修改的文件<br>• 扫描正在检索的文件<br>• 扫描正在创建 / 修改和检索的文件<br>有关用户活动的示例，请参阅表 2-10。 | 实时扫描 |
| 要扫描的文件 * | 选择一个：<br>• 所有可扫描文件：扫描用户打开或保存的所有文件<br>• 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，甚至是用无害扩展名伪装的文件。<br>• 仅带有指定的扩展名的文件 | 实时扫描 |

**表 2-15　　间谍软件 / 灰色软件扫描条件**

| 扫描条件 | 选项和描述 | 扫描类型 |
|---|---|---|
| 时间表 | 选择一个 （然后选择扫描开始时间）：<br>• 每日一次<br>• 每周一次<br>• 每月一次 | 预设扫描 |

* 仅当同时激活防病毒和 Web 威胁防护服务时可用；当只激活 Web 威胁防护服务时不可用。

### 间谍软件 / 灰色软件扫描例外

要提高扫描性能和跳过可引起假警报的扫描文件，可以在间谍软件 / 灰色软件扫描中排除特定文件扩展名。手动扫描、实时扫描、预设扫描和立即扫描都有其单独的例外列表。

要配置扫描例外设置，请转至**联网计算机 > 客户机管理 > 设置 { 扫描类型 }**。

- 对于手动扫描、预设扫描和立即扫描，请转至**间谍软件 / 灰色软件**选项卡 **> 扫描例外**。
- 对于实时扫描，请转至**目标**选项卡 **> 扫描例外**。

### 间谍软件 / 灰色软件批准列表

可能存在某些应用程序和文件，防毒墙网络版认为是间谍软件或灰色软件，但您仍要允许客户端计算机保留。可以配置间谍软件 / 灰色软件批准列表 , 来阻止防毒墙网络版扫描这些应用程序和文件并阻止防毒墙网络版将其视为间谍软件 / 灰色软件。

防毒墙网络版的批准列表中最多可容纳 1024 种间谍软件 / 灰色软件。

- 要管理间谍软件 / 灰色软件批准列表，请转至**联网计算机 > 客户机管理 > 设置 > 间谍软件 / 灰色软件批准列表**。
- 要将已检测到的间谍软件 / 灰色软件添加到 “批准列表”，请转至以下位置中的其中一个：
    - 联网计算机 > 客户机管理 > 日志 > 间谍软件 / 灰色软件日志 > 间谍软件 / 灰色软件日志标准 > 间谍软件 / 灰色软件日志 > 添加到 “批准列表”
    - 日志 > 联网计算机的日志 > 安全风险 > 查看日志 > 间谍软件 / 灰色软件日志 > 间谍软件 / 灰色软件日志标准 > 间谍软件 / 灰色软件日志 > 添加到 “批准列表”

### 全局间谍软件 / 灰色软件扫描设置

在**联网计算机 > 全局客户机设置**中配置全局间谍软件 / 灰色软件扫描设置。

以下是可用的设置：

- **启用评估模式：**在评估模式中时，防毒墙网络版将记录间谍软件 / 灰色软件检测日志，但不会尝试清除间谍软件 / 灰色软件组件。清除将终止进程或删除注册表、文件、 cookie 和快捷方式。趋势科技提供评估模式以允许您先评估间谍软件 / 灰色软件是否合法，然后

根据您的评估采取适当的处理措施。例如，可将合法的间谍软件 / 灰色软件添加到批准列表中。

**注意：** 评估模式会覆盖任何用户配置的扫描处理措施。例如，即使您选择“清除”作为手动扫描的处理措施，在评估模式过程中，“不予处理”仍保留为扫描处理措施。

- **扫描 cookie**：缺省情况下，防毒墙网络版不扫描 cookie。如果您认为联网计算机中的 cookie 为潜在的安全风险，请选择此选项。

### 间谍软件 / 灰色软件扫描处理措施

防毒墙网络版可以基于在**联网计算机 > 客户机管理 > 设置 > {扫描类型} > 处理措施**选项卡中指定的扫描设置针对间谍软件 / 灰色软件采取各种处理措施。从该窗口的“间谍软件 / 灰色软件”部分的可用扫描处理措施中选择。有关间谍软件 / 灰色软件类型的信息，请参阅*间谍软件和灰色软件*（第 1-27 页）。

以下是可用的扫描处理措施：

**表 2-16　　可用间谍软件 / 灰色软件扫描处理措施**

| 扫描处理措施 | 描述 | 扫描类型 |
|---|---|---|
| 清除 | 终止进程或删除注册表项、文件、cookie 和快捷方式 | 手动扫描、实时扫描、预设扫描、立即扫描 |
| 不予处理 | 将间谍软件 / 灰色软件检测记入日志以进行评估 | 手动扫描、预设扫描、立即扫描 |
| 文件拒绝访问 | 拒绝访问（复制、打开）检测到的间谍软件 / 灰色软件组件 | 实时扫描 |

### 其他间谍软件 / 灰色软件扫描处理措施选项

**表 2-17　　其他间谍软件 / 灰色软件扫描选项**

| 选项 | 扫描类型 |
|---|---|
| 检测到间谍软件 / 灰色软件时显示通知消息。<br>要定制通知消息，请转至**通知 > 客户机用户通知 > 间谍软件 / 灰色软件**选项卡。 | 实时扫描、预设扫描 |

## 扫描权限

在**联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 权限**选项卡中授予选定的客户机用户以下扫描权限。

**表 2-18　　客户机用户的扫描权限**

| 选项 | 描述 | 客户机控制台导航 |
|---|---|---|
| 为病毒 / 恶意软件配置手动扫描、实时扫描和预设扫描设置 | 允许客户机用户配置其自身病毒 / 恶意软件扫描设置 | 设置 > { 扫描类型 } |
| 为间谍软件 / 灰色软件配置手动扫描、实时扫描和预设扫描设置 | 允许客户机用户配置其自身间谍软件/灰色软件扫描设置 | 设置 > { 扫描类型 } |
| 停止预设扫描 | 允许客户机用户停止正在运行的预设扫描（既针对病毒 / 恶意软件，也针对间谍软件 / 灰色软件） | 在预设扫描期间，右键单击系统托盘中的防毒墙网络版图标，然后单击“停止预设扫描”。 |
| 邮件扫描权限 | 允许客户机用户手动扫描其 Microsoft Outlook 邮件和附件中是否带有安全风险 | “邮件扫描”选项卡 |

# Web 站点信誉配置

在**联网计算机 > Web 站点信誉**中配置 Web 站点信誉设置。

## Web 威胁

Web 威胁包括一系列源自于互联网的广泛威胁。 Web 威胁的方式非常复杂，使用了各种文件和技术的组合，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，而非在受感染的计算机上，因此 Web 威胁创建者会不断修改其代码以免被检测到。

## 信誉分值

某个 URL 的“信誉分值”可确定其是否为 Web 威胁。趋势科技使用专门度量值来计算分值。

- 如果 URL 的分值符合为以下类别之一设置的范围，则趋势科技将 URL 分为“Web 威胁”、“很可能为 Web 威胁”或“可能为 Web 威胁”。
- 如果某个 URL 的分值超过了定义的阈值，则趋势科技认为访问该 URL 是安全的。

## 安全级别

有四个安全级别确定防毒墙网络版将允许还是阻止访问 URL。

- **高：**阻止以下几类 URL：未分级、属于 Web 威胁及可能成为 Web 威胁的 URL
- **中：**阻止以下几类 URL：未分级、属于 Web 威胁及很可能为威胁的 Web URL

- **中 - 低**：阻止以下几类 URL：属于 Web 威胁及很可能为威胁的 Web URL
- **低**：只阻止属于 Web 威胁的 URL

例如，如果设置安全级别为 “低”，则防毒墙网络版仅阻止其认为是 “Web 威胁”的 URL。切记：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。

安全级别最终由 Web 站点信誉策略引用。

## Web 站点信誉策略和计算机位置

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其任务。由于便携式计算机连接到多个网络，而且员工可能携带便携式计算机通过组织的网关，因此防毒墙网络版需要将 Web 威胁防护扩展到这些便携式计算机，即使它们从您的网络断开。Web 站点信誉策略确保无论客户端计算机在什么位置都能受到保护。

防毒墙网络版检查客户端计算机网关 IP 地址来确定其位置，然后将特定 Web 站点信誉策略应用到该计算机。如果计算机网关 IP 地址与您在 Web 控制台 “计算机位置”窗口中指定的任何一个 IP 地址匹配，则防毒墙网络版认为该计算机在 “内部”，否则便认为在 “外部”。

趋势科技建议在外部计算机上执行更严格的策略。如果已将趋势科技产品和 Web 站点信誉功能（例如 InterScan 网关安全设备或 InterScan Web 安全设备）一起使用，则趋势科技还建议对内部计算机禁用 Web 站点信誉。

## 允许的 URL

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

## Web 站点信誉日志

可以同时允许内部和外部计算机上的客户机向服务器发送 Web 站点信誉日志。如果想要分析防毒墙网络版阻止的 URL 并对您认为访问较安全的 URL 采取适当处理措施，请执行此操作。

第 3 章

# 管理联网计算机

本章中的主题：


- *防毒墙网络版防火墙*（第 3-2 页）
- *爆发防护*（第 3-9 页）
- *客户机通知*（第 3-11 页）
- *客户机 - 服务器连接验证*（第 3-13 页）
- *客户机权限和其他设置*（第 3-14 页）
- *全局客户机设置*（第 3-16 页）
- *客户机设置管理*（第 3-18 页）
- *Cisco NAC*（第 3-19 页）

# 防毒墙网络版防火墙

防毒墙网络版防火墙使用策略、例外和概要文件来组织和定制保护联网计算机的方法。有关防毒墙网络版防火墙的概要，请参阅*防毒墙网络版防火墙*（第 1-8 页）。

**注意：** 趋势科技建议在部署和启用防毒墙网络版防火墙前先卸装防毒墙网络版客户机上其他基于软件的防火墙应用程序。在同一台计算机上安装多个供应商的防火墙可能会产生意外的结果。

以下步骤是成功使用防毒墙网络版防火墙所必需的：

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：**例外允许客户机背离策略。使用例外可以指定客户机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，可以在一个策略中设置一组客户机的所有网络通信，但是可创建一个允许 HTTP 网络通信的例外以便客户机可以访问 Web 服务器。
3. **创建概要文件和将其分配到客户机：**防火墙概要文件包括一组客户机属性。每个概要文件都与一个策略相关联。当客户机与在概要文件中指定的属性相匹配时，将触发关联的策略。

## 策略

可以在**联网计算机 > 防火墙 > 策略**中配置防火墙策略和例外。

策略包括以下内容：

- **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：**启用 / 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*入侵检测系统*（第 1-9 页）。
- **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

## 策略例外

例外包括更具体的设置，以基于客户端计算机端口号和 IP 地址允许或阻止不同种类的网络通信。可以配置一个例外列表以与每个策略相关联。列表中的例外将覆盖策略中的**安全级别**设置。

### 防火墙策略例外类型

- **限定：**仅阻止指定类型的网络通信，并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通常易受攻击的客户机端口，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，并适用于阻止所有网络通信的策略。例如，您可能要允许客户机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）和客户机用于 HTTP 通信的端口的网络通信。
  - 客户机侦听端口 （可信）：**联网计算机 > 客户机管理 > 状态**。端口号在**基本信息**下。
  - 服务器侦听 （可信）端口：**管理 > 连接设置**。端口号在**联网计算机的连接设置**下。

### 防火墙策略例外设置

- **操作：**阻止或允许满足例外条件的网络通信

- **方向：**客户端计算机上的入站或出站网络通信
- **协议：**网络通信类型：TCP、 UDP、 ICMP
- **端口：**客户端计算机上用于执行操作的端口
- **客户端计算机 IP 地址：**网络上网络通信条件适用的计算机的 IP 地址

### 防火墙策略例外模板编辑器

可以在例外模板编辑器中编辑例外，并将它们应用于所有现有策略，或者可以编辑应用于单个策略的例外。

### 配置例外：一个示例

在爆发期间，可以选择阻止所有客户机网络通信，包括 HTTP 端口（端口 80）。但是，如果仍然想要授予阻止的客户机访问互联网的权限，则可以将 Web 代理服务器添加到例外列表。

## 概要文件

可以在**联网计算机 > 防火墙 > 概要文件**中配置防火墙概要文件和备用服务器。

防火墙概要文件通过允许您在应用策略前选择一台客户机或一组客户机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
- **客户机属性：**带有以下属性的客户机应用关联的策略：
  - **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机
  - **域：**属于特定防毒墙网络版域的客户机
  - **计算机：**带有特定计算机名的客户机

- **平台**：运行特定平台的客户机
- **登录名**：指定的用户已登录到的客户机
- **客户机状态**：客户机是联机还是脱机

选择客户机属性的任何组合以指定客户端计算机。

- **用户权限**：允许或阻止客户机用户执行以下操作：
  - 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机。可以通过转至**联网计算机 > 客户机管理 > 设置 > 权限和其他设置> 权限**选项卡将其他防火墙权限分配到选定的客户机用户。请参阅*防火墙权限*（第 3-8 页）以获取详细信息。

---

防毒墙网络版将防毒墙网络版防火墙概要文件以在列表中显示的顺序应用到客户机。例如，如果客户机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机。防毒墙网络版将忽略为该客户机配置的其他概要文件。

一个策略越是排他，则越需要将其放在该列表的顶部。例如，为单个客户机创建的策略应在顶部，接下来才是为一系列客户机、网络域和所有客户机创建的策略。

### 备用服务器

可以编辑备用服务器的列表，备用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。备用服务器可以是您网络上的任何计算机。

当启用备用服务器时，防毒墙网络版做以下假设：

- 连接到备用服务器的客户机联机，即使客户机无法与防毒墙网络版服务器通信。
- 应用于联机客户机的防火墙概要文件也适用于连接到备用服务器的客户机。

## 缺省设置

防毒墙网络版防火墙提供缺省策略、例外和概要文件以为您提供启动客户机防火墙防护策略的基础。缺省设置包括客户机上常见的情况，如安装 Cisco NAC Trust Agent 和需要访问适用于 Microsoft Exchange Web 控制台的防毒墙群件版。

**表 3-1　　缺省防火墙策略**

| 策略名称 | 安全级别 | 客户机设置 | 例外 | 建议使用 |
|---|---|---|---|---|
| 所有访问 | 低 | 启用防火墙 | 无 | 用于允许客户机无限制访问网络 |
| Cisco Trust Agent for Cisco NAC | 低 | 启用防火墙 | 允许通过端口 21862 的入站 / 出站 UDP 网络通信 | 客户机安装有 Cisco Trust Agent (CTA) 时使用 |
| TMCM 的通信端口 | 低 | 启用防火墙 | 允许通过端口 80 和 10319 的所有入站 / 出站 TCP/UDP 网络通信 | 客户机安装有 MCP 代理时使用 |
| 适用于 Microsoft Exchange (SMEX) 控制台的防毒墙群件版 | 低 | 启用防火墙 | 允许通过端口 16372 的所有入站 / 出站 TCP 网络通信 | 客户机需要访问 SMEX 控制台时使用 |

**表 3-1　　缺省防火墙策略**

| 策略名称 | 安全级别 | 客户机设置 | 例外 | 建议使用 |
|---|---|---|---|---|
| 趋势科技防毒墙邮件安全版 (IMSS) 控制台 | 低 | 启用防火墙 | 允许通过端口 80 的所有入站 / 出站 TCP 网络通信 | 客户机需要访问 IMSS 控制台时使用 |

**表 3-2　　缺省防火墙策略例外**

| 例外名称 | 操作 | 协议 | 端口 | 说明 |
|---|---|---|---|---|
| DNS | 允许 | TCP/UDP | 53 | 入站和出站 |
| NetBIOS | 允许 | TCP/UDP | 137,138,139,445 | 入站和出站 |
| HTTPS | 允许 | TCP | 443 | 入站和出站 |
| HTTP | 允许 | TCP | 80 | 入站和出站 |
| Telnet | 允许 | TCP | 23 | 入站和出站 |
| SMTP | 允许 | TCP | 25 | 入站和出站出站 |
| FTP | 允许 | TCP | 21 | 入站和出站 |
| POP3 | 允许 | TCP | 110 | 入站和出站 |

**注意：** 没有缺省例外会指定客户机。如果使用任何缺省例外，则请指定想要应用例外的客户机。

**表 3-3　　缺省防火墙概要文件**

| 概要文件名称 | 使用的策略 | 应用于客户机 |
|---|---|---|
| 所有客户机概要文件 | 所有访问 | 未指定 |

## 防火墙权限

请转至**联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 权限**选项卡以授予客户机用户执行以下操作的权限：

- 在客户机控制台中查看 “防火墙”选项卡
- **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：**不能从防毒墙网络版服务器 Web 控制台覆盖用户指定的设置。

  如果未启用该功能，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机控制台上的**网卡列表**下。

- **允许客户机向防毒墙网络版服务器发送防火墙日志：**如果选择了此选项，请在**联网计算机 > 全局客户机设置**中配置日志发送时间表。该时间表将仅适用于具有防火墙日志发送权限的客户机。

## 防火墙测试

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机上执行测试。有关测试过程，请参阅联机帮助。

**警告！** *请仅在受控的环境中测试防毒墙网络版客户机程序设置。请勿在已连接到网络或互联网 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。*

## 防火墙：如何禁用

使用防毒墙网络版 Web 控制台在客户机上禁用防毒墙网络版防火墙。需要创建不启用防火墙的新策略，然后将该策略应用于客户机。有关该过程，请参阅联机帮助。

还可以通过在**管理 > 产品许可证**窗口中停止来禁用所有客户机的防火墙。

# 爆发防护

防毒墙网络版提供多种在网络上管理爆发的方法。这些方法包括启用防毒墙网络版以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，向客户机发送爆发警报消息，以及清除被感染计算机。

## 爆发阻止

使用爆发阻止可以限制 / 拒绝对特定共享文件夹的访问，封闭端口，以及拒绝对选定客户机上特定文件和文件夹的写入访问。

**警告！** *在爆发期间仔细配置爆发阻止设置。不正确的配置可能导致无法预料的网络问题。*

启用爆发阻止之后，请验证绿色的复选标记已显示在客户机树上选定客户机的 **OPP** 列中。

禁用爆发阻止后，请扫描您的联网计算机上是否有安全风险以确保包括爆发。

## 爆发阻止策略

### 限制 / 拒绝访问共享文件夹

可以允许只读或拒绝完全访问网络上的共享文件夹，以阻止安全风险通过共享文件夹传播。

### 封闭端口

在爆发期间，可以封闭易受攻击的端口，这些端口可能被病毒 / 恶意软件用于获取对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，如果封闭可信端口，防毒墙网络版将无法在爆发期间与客户机通信。*

可以在**端口封闭设置**列表上修改条目的以下设置：

- **网络通信方向：**阻止入站和 / 或出站网络通信
- **端口号：**修改任一端口号或为列表中的每个条目输入一系列端口
- **网络通信协议：**指定 TCP、 UDP 或两者都指定
- **注释：**添加任何注释以描述列表中的条目

### 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主机计算机上的文件和文件夹。在爆发期间，可以配置防毒墙网络版阻止病毒 / 恶意软件修改或删除客户端计算机上的文件和文件夹。

## 爆发后任务

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

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 **在 { } 小时之后自动停止爆发阻止**内指定的时间后自动恢复这些设置。缺省设置为 48 小时。

# 客户机通知

配置客户机用户通知以通知或提醒用户有关需要他们注意的事件（如安全风险检测），并建议他们如何执行必要的操作。

## 安全风险通知

防毒墙网络版可以在选定的客户端计算机上显示通知消息，以通知用户在该计算机上检测到的安全风险。该消息将在发生以下情形后立即显示：

- 实时扫描和预设扫描可以检测病毒 / 恶意软件和间谍软件 / 灰色软件。
- 防毒墙网络版防火墙检测到防火墙策略违例。
- 防毒墙网络版阻止了违反 Web 站点信誉策略的 URL。

可以通过单击**通知 > 客户机用户通知**窗口中的选项卡然后在提供的文本框中输入新消息来修改用于不同安全风险的缺省消息。

---

**注意：** 有关防毒墙网络版可以发送给您和其他防毒墙网络版管理员的通知的信息，请参阅 *管理员通知*（第 4-7 页）。

---

### 病毒 / 恶意软件通知

- 客户机只显示病毒 / 恶意软件通知消息 （如果这样配置客户机）。可以通过依次选择以下项来配置此设置：**联网计算机 > 客户机管理 > 设置 > { 实时或预设扫描设置 } > 处理措施**选项卡。只有您在客户机树 （当单击**联网计算机 > 客户机管理**时）中选择的那些客户机才会显示该消息。

- 可以选择当客户机用户的计算机发出病毒 / 恶意软件时显示通知消息。要执行此操作，请转至**通知 > 客户机用户通知 > 病毒 / 恶意软件**选项卡。选中病毒 / 恶意软件感染源下的复选框，指定一个发送通知的间隔，然后有选择性地修改缺省通知消息。仅当启用 Windows Messenger 服务时，显示此通知消息。可以在 “服务” 窗口 （**控制面板 > 管理工具 > 服务 > Messenger**）中检查此服务的状态。

### 间谍软件 / 灰色软件通知

客户机只显示间谍软件 / 灰色软件通知消息 （如果这样配置客户机）。可以通过依次选择以下项来配置此设置: **联网计算机 > 客户机管理 > 设置 > { 实时或预设扫描设置 } > 处理措施**选项卡。只有您在客户机树（当单击**联网计算机 > 客户机管理**时）中选择的那些客户机才会显示该消息。

### 防火墙违例通知

客户机将只显示防火墙违例通知消息（如果这样配置客户机并且如果出站网络通信违反了防火墙设置）。可以通过依次选择以下项来配置此设置: **联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 权限**选项卡。

### Web 站点信誉通知

客户机只显示 Web 站点信誉通知消息 （如果这样配置客户机）。可以通过依次选择以下项来配置此设置: **联网计算机 > 客户机管理 > 设置 > 权限和其他设置 > 其他设置**选项卡。只有您在客户机树 （当单击**联网计算机 > 客户机管理**时）中选择的那些客户机才会显示该消息。

显示通知消息后，将在客户端计算机的浏览器中显示另一消息，通知用户如果他们认为 URL 可安全访问则将向防毒墙网络版管理员报告该 URL。

### 其他通知

防毒墙网络版可以在以下情况下显示通知。通过转至**联网计算机 > 全局客户机设置**启用这些通知。

- 如果病毒码在特定天数内保持过期状态
- 如果客户机用户需要重新启动计算机来加载内核模式驱动程序

  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。卸载前一版本和加载新版本的唯一方法就是重新启动计算机。重新启动计算机后，将自动安装新版本，无需再重新启动。

  安装 Hotfix 或升级软件包后，通知消息将显示在客户端计算机上。

## 客户机 - 服务器连接验证

防毒墙网络版使用图标在客户机树中表示客户机连接状态。但是，特定情况可能阻止客户机树显示正确的客户机连接状态。例如，如果意外拔除了客户端计算机的网络电缆，则客户机将不能通知服务器其已脱机。此客户机在客户机树中将仍显示为联机。

可以通过转至**联网计算机 > 连接验证**手动或预设验证客户机 - 服务器连接。

---

**注意：** 不能先选择特定域或客户机，然后再验证其连接状态。防毒墙网络版会验证所有已注册客户机的连接状态。

---

再次检查客户机树以在**日志 > 联网计算机的日志 > 连接验证**中验证客户机连接状态或查看连接验证日志。

# 客户机权限和其他设置

在**联网计算机 > 客户机管理 > 设置 > 权限和其他设置**中配置特定客户机的权限和其他设置。

**表 3-4　　选定客户机的权限和设置**

| 设置 | 描述 |
|---|---|
| 权限 | |
| 漫游权限 | 允许客户机处于漫游模式。有关详细信息，请参阅*漫游客户机*（第 1-16 页）。 |
| 防病毒、反间谍软件预设扫描和邮件扫描权限 | 允许客户机用户配置其自身扫描设置。有关详细信息，请参阅*扫描权限*（第 2-36 页）。 |
| 防火墙权限 | 有关详细信息，请参阅*防火墙权限*（第 3-8 页）。 |
| 工具箱权限 | 在客户机控制台上显示**工具箱**选项卡 “工具箱”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 检查客户机病毒码和病毒扫描引擎是否为最新。 |
| 代理服务器设置权限 | 允许客户机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代理服务器设置：<br>• 客户机执行 “立即更新”时。有关 “立即更新”功能的信息，请参阅*客户机更新方法*（第 2-15 页）。<br>• 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*代理服务器配置*（第 3-18 页）以获取详细信息。 |
| 组件更新权限 | 允许客户机用户配置其自身组件更新设置。有关详细信息，请参阅*其他设置*（第 2-19 页）。 |
| 客户机卸装 | 允许用户卸装（需要密码或无需密码）防毒墙网络版客户机<br>要从 Web 控制台启动静默客户机卸装，请转至**联网计算机 > 客户机管理 > 任务 > 客户机卸装**。 |

**表 3-4　　选定客户机的权限和设置**

| 设置 | 描述 |
| --- | --- |
| 客户机退出 | 允许用户暂时停止 （需要密码或无需密码）防毒墙网络版客户机 |
| 其他设置 | |
| 更新设置 | 有关详细信息，请参阅*其他设置*（第 2-19 页）。 |
| Web 站点信誉设置 | 如果防毒墙网络版阻止了一个违反 Web 站点信誉策略的 URL，则将在客户端计算机上显示通知消息 |
| 客户机安全性 | 允许或限制用户访问防毒墙网络版客户机文件与注册表<br>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。<br>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机文件夹、文件和注册表进行完全读取 / 写入访问。 |
| 客户机控制台访问限制 | 用户不能从系统托盘或 Windows “开始”菜单中访问客户机控制台，但是可以从防毒墙网络版客户机安装程序文件夹中访问。防毒墙网络版在后台运行并继续提供对安全风险的防护。 |

# 全局客户机设置

防毒墙网络版可将全局客户机设置应用于所有客户机，或者只应用于带有特定权限的客户机。在**联网计算机 > 全局客户机设置**中配置全局客户机设置。

**表 3-5　　全局客户机设置**

| 设置 | 描述 |
|---|---|
| 病毒 / 恶意软件扫描设置 | 有关详细信息，请参阅*全局病毒 / 恶意软件扫描设置*（第 2-27 页）。 |
| 间谍软件 / 灰色软件扫描设置 | 有关详细信息，请参阅*全局间谍软件 / 灰色软件扫描设置*（第 2-34 页）。 |
| 防火墙日志设置 | 可以授予某些客户机向防毒墙网络版服务器发送防火墙日志的权限。可以配置在此部分中发送时间表的日志。仅具有发送防火墙日志权限的客户机可使用此时间表。有关可以授予选定客户机的防火墙权限的信息，请参阅*防火墙权限*（第 3-8 页）。 |
| 警报设置 | 有关详细信息，请参阅*其他通知*（第 3-13 页）。 |

**表 3-5　　全局客户机设置**

| 设置 | 描述 |
| --- | --- |
| 保留的磁盘空间和看守程序设置 | • **看守程序服务：**意外中止（可能在客户机受黑客攻击时发生）后立即重新启动防毒墙网络版客户机。<br><br>恶意程序（即逆转录病毒，如 WORM_KLEZ.h）将通过关闭关键防病毒进程和删除防病毒解决方法使用的一些文件来反击防病毒解决方法。这使它们能够使用旧病毒进行感染，因此有了“逆转录病毒”之名。防毒墙网络版看守程序服务 (OfcDog.exe) 可通过执行以下操作保护防毒墙网络版客户机的状态：<br><br>• 监控 NT 实时扫描 (NtRtScan.exe) 和防毒墙网络版 NT Listener (TmListen.exe) 的状态。如果这些防毒墙网络版进程未运行，且未由正常系统进程停止，则看守程序服务将重新启动它们。它还将在客户端计算机上编写一个事件日志，并将该日志发送到服务器。<br><br>• 将所有 .exe 和 .dll 文件锁定在防毒墙网络版客户机目录中以防止其他程序甚至用户将其修改或删除。<br><br>缺省情况下，将随机命名看守程序服务以帮助防止其他程序将其中止。<br><br>• **防黑客模式：**随机为看守程序服务命名。这可帮助防止任何安全风险识别和中止该服务。<br><br>• **保留 { } MB 用于更新的磁盘空间：**为 Hotfix、病毒码文件、扫描引擎和程序更新分配一定量的客户机磁盘空间。缺省情况下，防毒墙网络版将保留 60MB 的空间。 |
| 网络病毒日志整合 | 客户机每个小时只发送一次网络病毒日志。有关网络病毒的详细信息，请参阅*病毒和恶意软件*（第 1-25 页）。 |
| 病毒 / 恶意软件日志带宽设置 | 在较短时间内从同一病毒 / 恶意软件中检测到多个感染时，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，从而在客户机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。在将病毒日志信息报告给服务器时，启用此功能有助于减少病毒 / 恶意软件日志的条目数和客户机占用的网络带宽量。 |

**表 3-5　　全局客户机设置**

| 设置 | 描述 |
| --- | --- |
| 代理服务器配置 | 手动配置代理服务器设置对于许多最终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。<br>启用后，客户机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是主要的代理服务器设置。有关自动更新和立即更新的信息，请参阅*客户机更新方法*（第 2-15 页）。<br>如果客户机不能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机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失败。<br>**注意：** 代理服务器认证不受支持。<br>• **自动检测设置：**通过 DHCP 或 DNS 自动检测管理员配置的代理服务器设置。<br>• **使用自动配置脚本：**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。 |
| 客户机分组 | 此选项通过 NetBIOS、Active Directory 或 DNS 域为客户机树中的客户机分组。 |

# 客户机设置管理

您可能想要多个防毒墙网络版客户机具有相同的扫描和 / 或客户机权限设置。通过防毒墙网络版，可以保存（导出）特定客户机扫描设置和权限并在以后将其复制（导入）到多个客户机。这提供了一种在众多客户机上配置相同设置的简便方法。

不能导出多个客户机的扫描和权限设置。仅能导出单个客户机、域或根的设置。

要导入和导出设置，请转至**联网计算机 > 客户机管理 > 设置 > { 导入或导出 } 设置**。

# Cisco NAC

面向 Cisco Network Admission Control (NAC) 的趋势科技策略服务器将评估防毒墙网络版客户机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机执行处理措施，以便将它们与贵组织的防病毒计划兼容。

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机组件。
- 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。

要帮助您分析防病毒策略的性能，请查看策略服务器日志（记录诸如评估客户机的时间和评估结果的信息）。

**注意：** 有关 Cisco NAC 技术的其他信息，请参阅 Cisco Web 站点 www.cisco.com/go/nac。

Cisco NAC 将在以下章节中详细讨论：

- *了解策略服务器 for Cisco NAC*（第 5-1 页）
- *部署策略服务器 for Cisco NAC*（第 6-1 页）

第 4 章

# 管理防毒墙网络版服务器

本章中的主题：


- *趋势科技防毒墙控制管理中心*（第 4-2 页）
- *日志*（第 4-2 页）
- *许可证*（第 4-5 页）
- *防毒墙网络版数据库备份*（第 4-6 页）
- *防毒墙网络版 Web 服务器信息*（第 4-6 页）
- *管理员通知*（第 4-7 页）
- *Web 控制台密码*（第 4-8 页）
- *非活动客户机*（第 4-9 页）
- *隔离管理器*（第 4-10 页）
- *管理工具和客户机工具*（第 4-10 页）
- *全球病毒跟踪计划*（第 4-12 页）

# 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。

请参阅*使用控制管理中心管理防毒墙网络版*（第 7-1 页）以获取详细信息。

# 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标识处于较高感染风险或攻击风险的客户机。还使用这些日志来检查客户机 - 服务器连接并验证组件更新是否成功。

## 联网计算机的日志

### 安全风险日志

安全风险包括病毒 / 恶意软件、间谍软件 / 灰色软件、防火墙违例和 Web 威胁。

对于间谍软件 / 灰色软件日志，如果您认为检测到的间谍软件 / 灰色软件是安全的，则可以将其添加到批准列表。有关批准列表的详细信息，请参阅*间谍软件 / 灰色软件批准列表*（第 2-34 页）。

对于防火墙违例日志，可以选择首先通知客户机向将日志发送给服务器以确保您可以使用最新的日志。已启用防毒墙网络版防火墙的防毒墙网络版客户机将防火墙事件存储在客户端计算机上的日志中。查看这些日志来分析防毒墙网络版防火墙性能。

### 组件更新日志

防毒墙网络版客户机会将病毒码更新日志发送给服务器。在“组件更新进度”窗口中，查看每间隔 15 分钟更新的客户机数以及更新的客户机总数。

### 连接验证日志

防毒墙网络版保留连接验证日志以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机通信。每次从 Web 控制台验证客户机 - 服务器连接时，防毒墙网络版都会创建一个日志条目。请参阅 *客户机 - 服务器连接验证*（第 3-13 页）。

### 间谍软件 / 灰色软件恢复日志

清除间谍软件 / 灰色软件后，防毒墙网络版客户机会备份间谍软件 / 灰色软件数据，如果您认为间谍软件 / 灰色软件是安全的，则防毒墙网络版服务器可以随时将其恢复。间谍软件 / 灰色软件恢复日志向您显示恢复结果。

## 服务器更新日志

防毒墙网络版在防毒墙网络版服务器上保留与组件更新相关的所有事件的日志。查看该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。

## 系统事件日志

防毒墙网络版还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。

防毒墙网络版日志将记录以下事件：

**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
- 数据库服务器已重新启动

**防火墙违例和共享文件夹会话的爆发通知：**

- 日志类型 （IDS 日志、防火墙日志、网络病毒日志）超出
- 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
- 数据库备份失败
- 数据库备份已取消

## 日志删除

要防止日志的大小占用过多的硬盘空间，可将防毒墙网络版配置为手动删除日志或根据时间表删除日志。

# 许可证

可以从 Web 控制台中查看和续订防毒墙网络版产品服务许可证。还可激活要使用新服务。

如果激活了防病毒服务，则可以启用 / 禁用防毒墙网络版防火墙。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机中的所有防火墙功能。

通过防毒墙网络版可以激活一个产品服务的多个许可证。从 Web 控制台中可查看服务的所有许可证 （活动的和过期的）。

许可证的状态显示在**管理 > 产品许可证**窗口的顶部。以下实例中将显示提醒信息：

### 完全版

- 宽限期结束前 30 天
- 当许可证到期且宽限期已过期

**注意：** 在此期间，您将无法获得技术支且无法执行组件更新。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。

### 评估 （试用）版

- 当许可证过期时

**注意：** 在此期间，防毒墙网络版将禁用组件更新、扫描和所有客户机功能组件。

# 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。服务器数据库发生损坏时，如果具有备份，可以轻松地将其恢复。可以随时手动备份数据库或配置备份时间表。

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。

**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。*

**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 \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，主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。可以配置两端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），则必须也要在防毒墙网络版中进行更改以确保其保持服务器 - 客户机通信并确保您仍能访问 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。

## 管理员通知

无论防毒墙网络版何时在任何客户机上或在安全风险爆发期间检测到安全风险，都可以通知您及贵组织中的其他防毒墙网络版管理员。在**通知 > 管理员通知**中配置通知设置。

**注意：** 要配置在客户端计算机上显示的通知设置，请参阅*客户机通知*（第 3-11 页）。

防毒墙网络版通过以下方式发送通知：

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

### 标准通知

防毒墙网络版附带一组缺省通知消息，只要防毒墙网络版在客户端计算机上检测到病毒 / 恶意软件或间谍软件 / 灰色软件，您及其他管理员就会收到这些通知。修改这些消息来适应您的需求。

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时才发送通知，因此需要您的干预。

### 爆发通知

配置防毒墙网络版通知您和其他防毒墙网络版管理员网络上的安全风险爆发。根据安全风险检测次数和检测周期定义爆发条件。在检测周期中，如果超过该检测次数，则防毒墙网络版发送通知。例如，如果指定检测次数为 100，则防毒墙网络版在检测到第 101 个病毒 / 恶意软件实例后将发送通知。

响应爆发非常重要。除非采取了正确的处理措施，否则爆发可以迅速传播至整个网络并传播到网络之外。

## Web 控制台密码

使用密码保护 Web 控制台，以防未经授权的用户修改防毒墙网络版的设置或从联网计算机中移除客户机程序。在安装过程中，防毒墙网络版安装程序会要求您指定 Web 控制台密码，但可以从 Web 控制台中修改密码，方法是转到**管理 > 控制台密码**。

如果忘记了控制台密码，请联系趋势科技技术支持来了解有关如何获取对 Web 控制台访问的说明。唯一的另外选择是卸装防毒墙网络版，然后重新安装。

# 非活动客户机

当使用客户机卸装程序从一台计算机移除客户机程序时，该程序将自动通知服务器。当服务器接收到此通知时，它将在此客户机树中移除客户机图标以显示该客户机已不再存在。

但是，如果使用其他方法移除客户机，如重新格式化计算机硬盘驱动器或手动删除客户机文件，则防毒墙网络版将不会注意到它的移除，并只把客户机显示为非活动。如果用户将客户机卸载或禁用较长的时间，则服务器还将把客户机显示为非活动。

要使客户机树只显示活动客户机，可以配置防毒墙网络版以从客户机树中自动移除非活动客户机。

# 隔离管理器

无论何时防毒墙网络版检测到一个安全风险且扫描处理措施为隔离，则它将为受感染文件加密，并将该文件移动到本地隔离文件夹，然后再将其发送到防毒墙网络版服务器。该服务器也为受感染文件加密以阻止它感染其他文件。

隔离文件夹的缺省位置：

**客户机：**{ 防毒墙网络版安装文件夹 }\OfficeScan Client\SUSPECT

**服务器：**{ 防毒墙网络版安装文件夹 }\OfficeScan\PCCSRV\Virus

缺省防毒墙网络版安装文件夹为 C:\Program Files\Trend Micro。

---

**注意：** 如果防毒墙网络版客户机由于任何原因 （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机隔离文件夹中。连接到防毒墙网络版服务器时，客户机将尝试重新发送该文件。

---

可以配置隔离文件夹的容量以及进行隔离的受感染文件的最大文件大小。有关详细信息，请参阅*其他病毒 / 恶意软件扫描处理措施选项*（第 2-31 页）。

# 管理工具和客户机工具

防毒墙网络版包括可完成各种防毒墙网络版任务的一组工具，其中包括服务器配置和客户机管理。

有两种类型的防毒墙网络版工具。请注意，不能从 Web 控制台运行任何此类工具。有关这些工具及其使用方法的详细信息，请参阅联机帮助。

- **管理工具：**开发以帮助您配置服务器和管理客户机
  - **登录脚本安装：**在未受保护计算机登录到网络时，自动将防毒墙网络版客户机安装到这些计算机
  - **漏洞扫描程序：**检测已安装的防病毒解决方案并搜索网络中的未受保护计算机
  - **服务器调节程序：**优化防毒墙网络版服务器的性能
- **客户机工具：**开发以帮助您增强客户机程序的性能
  - **客户机打包程序：**将防毒墙网络版客户机安装程序和更新文件压缩在自解压缩文件中，使用电子邮件、CD-ROM 或相似媒体来简化向客户机的交付过程。
  - **镜像安装实用程序：**创建防毒墙网络版客户机的镜像并将其克隆到网络中的其他计算机
  - **恢复加密的文件：**解密防毒墙网络版加密的受感染文件以便从该文件中检索必要信息
  - **客户机迁移程序：**如果在网络中有多个防毒墙网络版服务器，则将客户机从一台防毒墙网络版服务器转移到另一台防毒墙网络版服务器
  - **触探工具：**使用另一个文件的时间戳或计算机的系统时间来同步一个文件的时间戳
  - **ServerProtect 标准服务器迁移工具：**将 ServerProtect ™ 标准服务器程序迁移到防毒墙网络版客户机

---

**注意：** 在先前版本的防毒墙网络版中可用的一些工具在本版本中不可用。如果您需要使用以上未列出的特定工具，则请联系技术支持提供商。

---

# 全球病毒跟踪计划

可将安全风险扫描结果发送到“全球病毒跟踪计划”，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“全球病毒跟踪计划”。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 http://www.trendmicro.com.cn/wtc/。

第 5 章

# 了解策略服务器 for Cisco NAC

本章中的主题：


- *组件和术语*（第 5-2 页）
- *Cisco NAC 体系结构*（第 5-4 页）
- *客户机验证顺序*（第 5-5 页）
- *策略服务器*（第 5-7 页）
- *同步*（第 5-14 页）
- *证书*（第 5-15 页）
- *策略服务器系统需求*（第 5-17 页）
- *Cisco Trust Agent (CTA) 需求*（第 5-19 页）
- *支持的平台和需求*（第 5-20 页）

# 组件和术语

以下是一个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 5-1　　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机程序的计算机。要使用 Cisco NAC，客户端计算机还需要 Cisco Trust Agent。 |
| 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。<br>要获取受支持设备的列表，请参阅*支持的平台和需求*（第 5-20 页）。 |
| Cisco Secure Access Control Server (ACS) | 通过网络访问设备从客户机接收防毒墙网络版客户机防病毒数据，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机的说明）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机防病毒数据的程序。执行评估后，策略服务器确定防毒墙网络版客户机应执行的操作，然后通知该客户机执行这些操作。 |
| 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机的防病毒状态。 |

## 术语

熟悉以下与策略服务器 for Cisco NAC 相关的术语：

**表 5-2　　与策略服务器 for Cisco NAC 相关的术语**

| 术语 | 定义 |
|---|---|
| 安全状态 | 客户机上防病毒软是否存在和当前状态。在此实施中，安全状态是指防毒墙网络版客户机程序是否存在于客户端计算机上、某些防毒墙网络版客户机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机验证后，由策略服务器创建。包括告知防毒墙网络版客户机执行一组指定操作 （如启用实时扫描或更新防病毒组件）的信息。 |
| 客户机验证 | 评估客户机安全状态以及将状态令牌返回到客户机的过程 |
| 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机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机和策略服务器要执行的操作 （请参阅*策略服务器策略和规则*（第 5-8 页）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机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机和策略服务器要执行的操作 （请参阅*策略服务器策略和规则*（第 5-8 页）以获取详细信息）。 |
| 认证、授权与核算 (AAA) | 描述用于控制最终用户客户机访问计算机资源的三个主服务。认证是指标识客户机 （通常通过使用户输入用户名和密码完成）。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 / 或服务器之间连接。 |
| 数字证书 | 用于安全功能的附件。通常，证书通过 Web 服务器等服务器来认证客户机，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。 |

**表 5-2　　与策略服务器 for Cisco NAC 相关的术语**

| 术语 | 定义 |
|---|---|
| 远程认证拨号用户服务 (RADIUS) | 需要客户机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+) | 通过用于认证最终用户客户机的 AAA 命令启用的安全协议。Cisco ACS 服务器支持 TACACS+。 |

# Cisco NAC 体系结构

图 5-1 详细说明了带有上述组件的基本 Cisco NAC 体系结构。

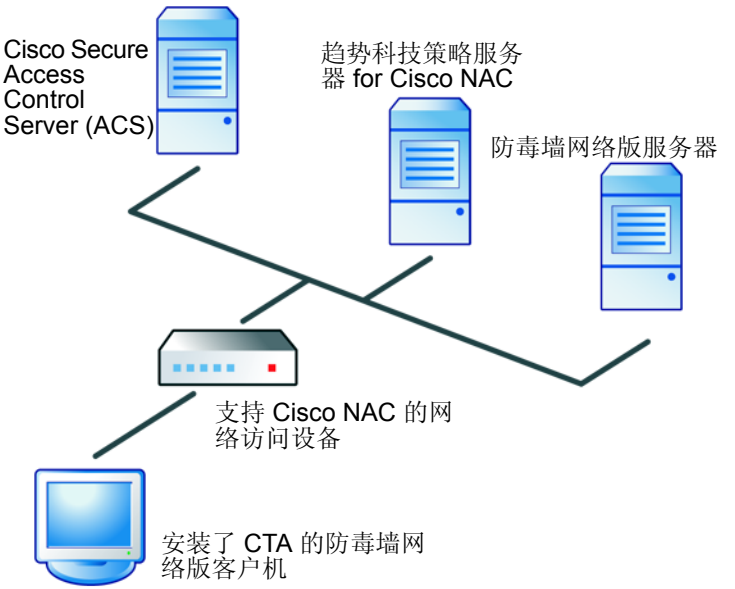



**图 5-1　　基本 Cisco NAC 体系结构**

图 5-1 中的防毒墙网络版客户机安装了 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机和其他 Cisco NAC 组件之间。

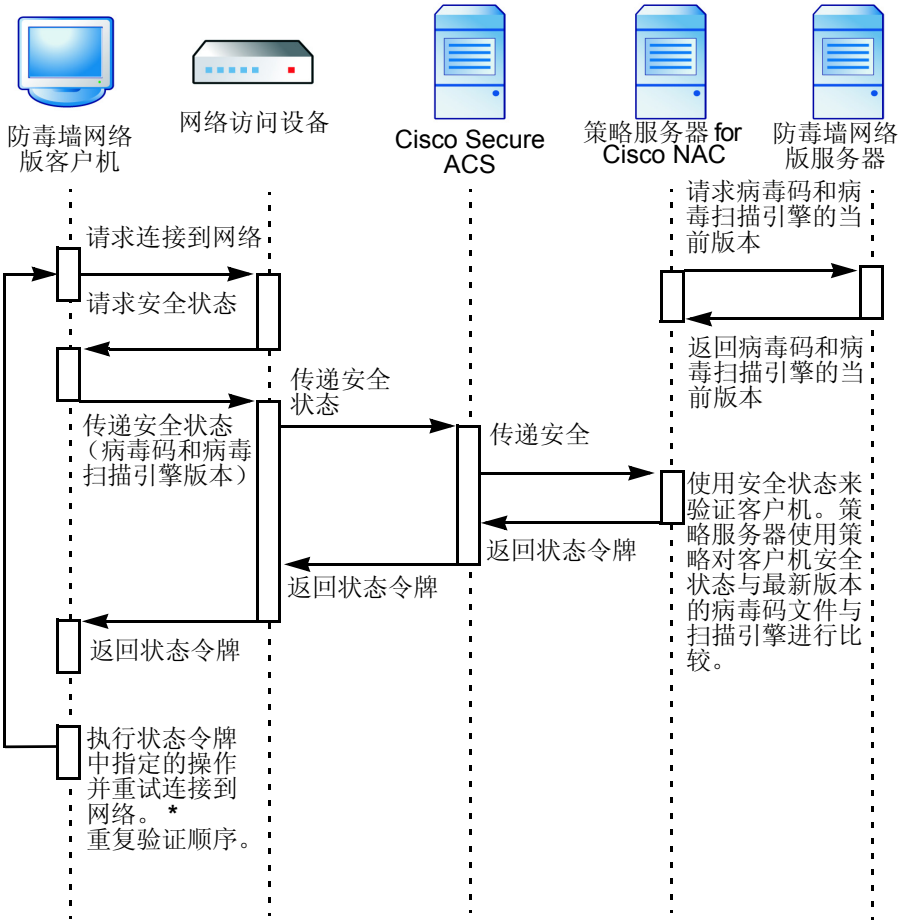
**注意：** 网络的体系结构将根据代理服务器、路由器或防火墙是否存在而不同。

## 客户机验证顺序

客户机验证指以下过程：评估防毒墙网络版客户机安全状态，并在策略服务器认为客户机处于风险中时返回客户机将执行的指令。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机。

图 5-2 详细说明了当防毒墙网络版客户机尝试访问网络时，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机的安全状态。
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. 在一个单独的过程中，策略服务器定期轮询防毒墙网络版服务器上的病毒码文件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机安全状态数据。
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机。
6. 最后，客户机执行状态令牌中配置的操作。




* 网络访问设备计时器过期后，客户机会重试访问网络。请参阅您的 Cisco 路由器文档以获取有关配置计时器的信息。

**图 5-2　　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机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（客户机是该服务器的成员）接收的病毒码文件和扫描引擎进行比较。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机。

当大量客户机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一个防毒墙网络版服务器的请求。图 5-3 详细说明了多个防毒墙网络版服务器和策略服务器的关系。

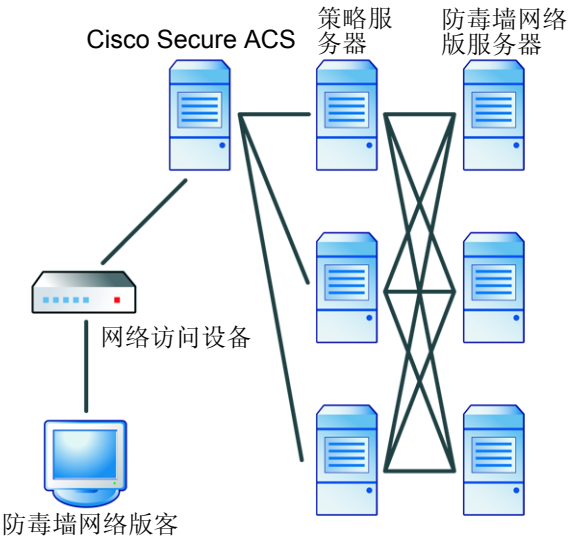



**图 5-3　　多个策略服务器 / 防毒墙网络版服务器的关系**

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策略和规则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机安全状态的特定条件。如果客户机安全状态与在规则中配置的条件匹配，则客户机和服务器会执行为该规则指定的操作 （请参阅*策略服务器和防毒墙网络版客户机操作*（第 5-10 页））。

*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*爆发阻止*（第 3-9 页）以获取有关网络模式的详细信息）。

如果防毒墙网络版客户机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机会执行为该规则配置的操作。但是，如果客户机安全状态与和该策略关联的规则中的任何条件都不匹配，则仍可在客户机和服务器要执行的策略中配置缺省操作 （请参阅*策略服务器和防毒墙网络版客户机操作*（第 5-10 页））。

**提示：** 如果希望防毒墙网络版域中的特定客户机与同一域中其他客户机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机分组到一起（请参阅*防毒墙网络版域*（第 2-3 页））。

## 规则组成

规则包括安全状态条件、与客户机关联的缺省响应以及客户机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
- **客户机实时扫描状态：**实时扫描是否已启用
- **客户机扫描引擎版本当前状态：**病毒扫描引擎是否为最新
- **客户机病毒码文件状态：**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旧特定数量的版本
  - 病毒码是否在在验证前特定天数内可用

### 规则的缺省响应

发生客户机验证时，响应帮助您了解网络中防毒墙网络版客户机的情况。显示在策略服务器客户机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**：客户机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**：任何其他情况

---

**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机操作

如果客户机安全状态与规则条件匹配，则策略服务器可以执行以下操作：

- 在策略服务器客户机验证日志中创建条目 （请参阅*客户机验证日志*（第 6-19 页）以获取详细信息）

如果客户机安全状态与规则条件匹配，则防毒墙网络版客户机可以执行以下操作：

- 启用客户机实时扫描以便防毒墙网络版客户机可以扫描所有已打开或已保存的文件（请参阅*实时扫描*（第 2-22 页）以获取详细信息）
- 更新所有防毒墙网络版组件 （请参阅*组件更新*（第 2-6 页）以获取详细信息）

- 启用实时扫描时或更新后扫描客户机 （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 5-3　　缺省规则**

| 规则名称 | 匹配条件 | 满足条件时进行响应 | 服务器操作 | 客户机操作 |
|---|---|---|---|---|
| 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 | 病毒码版本比客户机注册到的防毒墙网络版服务器上的版本至少旧一个版本。 | 检查 | 在客户机验证日志中创建条目 | • 更新组件<br>• 启用实时扫描或更新后，在客户机执行自动立即清除<br>• 在客户端计算机上显示通知消息<br>**注意：** 如果使用这条规则，趋势科技建议使用自动部署。自动部署帮助您在防毒墙网络版下载新组件后，确保客户机能立即接收最新的病毒码。 |
| 转换 | 客户端计算机正处于引导状态。 | 转换 | 无 | 无 |

**表 5-3　　缺省规则**

| 规则名称 | 匹配条件 | 满足条件时进行响应 | 服务器操作 | 客户机操作 |
|---|---|---|---|---|
| 隔离 | 病毒码版本比客户机注册到的防毒墙网络版服务器上的版本至少旧五个版本。 | 隔离 | 在客户机验证日志中创建条目 | • 更新组件<br>• 启用实时扫描或更新后，在客户机上执行自动立即清除和立即扫描。<br>• 在客户端计算机上显示通知消息 |
| 未防护 | 实时扫描状态被禁用。 | 受感染 | 在客户机验证日志中创建条目 | • 启用客户机实时扫描<br>• 在客户端计算机上显示通知消息 |

## 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，这允许您区分规则的优先次序。可以更改规则的顺序、添加新规则以及从策略中移除现有规则。

### 策略的缺省响应

策略与规则类似，包括缺省响应，该响应可帮助您在客户机验证时了解网络上的防毒墙网络版客户机的情况。但是，仅当客户机安全状态与策略中的规则都不匹配时，缺省响应才与客户机关联。

策略的响应与规则的响应相同 （请参阅*规则的缺省响应* （第 5-10 页）以获取响应列表）。

### 策略服务器和防毒墙网络版客户机操作

通过将客户机状态信息与策略的每个规则关联，策略服务器对客户机执行规则。基于 Web 控制台上指定的正在使用中的规则，规则按从顶到下的方式应用。如果客户机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机上。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机上。

缺省爆发模式策略使用“正常”规则评估防毒墙网络版客户机。该策略强制与此规则不匹配的所有客户机立即实施 “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机。该策略将不匹配任何这些规则的所有客户机归类为 “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。

### 策略名称：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
- 服务器操作：无
- 客户机操作：无

### 策略名称：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

- 服务器操作：在客户机验证日志中创建条目
- 客户机操作：
  - 启用客户机实时扫描
  - 更新组件
  - 启用实时扫描时或更新后，在客户机上执行立即扫描
  - 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*策略服务器的摘要信息*（第 6-17 页））。
- **按时间表**：设置使防毒墙网络版执行同步的时间表 （请参阅*管理工具*（第 6-20 页））。

# 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 5-4　　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机。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机。 |
| 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。<br>**注意：** 策略服务器 SSL 证书是可选的。但是，趋势科技建议您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。 |

图 5-4 详细说明了有关创建和部署 ACS 和 CA 证书的步骤：

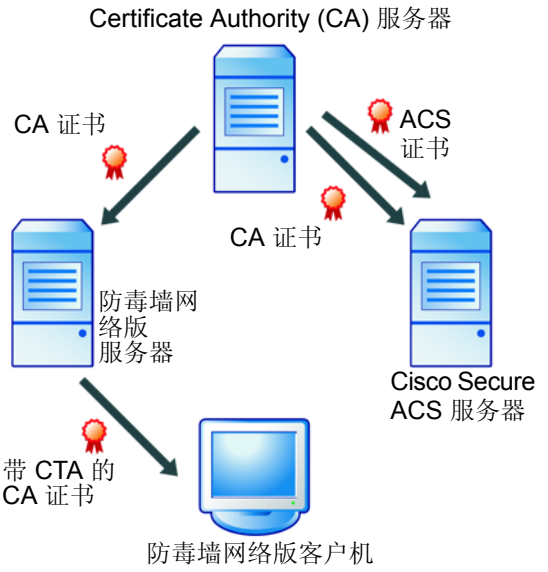



**图 5-4 ACS 和 CA 证书的创建与部署**

1. 在 ACS 服务器将签署请求发放到 CA 服务器之后，CA 会发放证书（ACS 证书）。然后， ACS 证书安装在 ACS 服务器上。请参阅 *Cisco Secure ACS 服务器登记*（第 6-3 页）以获取详细信息。
2. 从 CA 服务器导出 CA 证书并安装到 ACS 服务器上。请参阅 *CA 证书安装*（第 6-3 页）以获取详细信息。
3. 将相同的 CA 证书副本保存在防毒墙网络版服务器上。
4. 防毒墙网络版服务器使用 CTA 将 CA 证书部署到客户机。请参阅 *Cisco Trust Agent 部署*（第 6-8 页）以获取详细信息。

### CA 证书

安装了 CTA 的防毒墙网络版客户机首先在 ACS 服务器认证，然后才能传递客户机安全状态。可使用多种方法来认证（请参阅您的 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机证书。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机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机的机制。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 部署到客户机时分发证书（请参阅 *Cisco Trust Agent 部署*（第 6-8 页））。

---

**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机，则无需再进行此操作。

---

将证书分发到客户机之前，先在 CA 服务器登记 ACS 服务器，然后再准备证书（请参阅 *Cisco Secure ACS 服务器登记*（第 6-3 页））。

## 策略服务器系统需求

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

- Microsoft Windows 2000 Professional（Service Pack 2 或更高版本）

- Microsoft Windows 2000 Server （Service Pack 2 或更高版本）
- Microsoft Windows 2000 Advanced Server （Service Pack 2 或更高版本）
- Microsoft Windows XP Professional （Service Pack 1 或更高版本）
- Microsoft Windows Server 2003 Standard
- Microsoft Windows Server 2003 Enterprise
- Microsoft 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
- 颜色为 256 或更高时支持分辨率为 800 x 600 的显示器

### Web 服务器

- Microsoft Internet Information Server (IIS) V5.0 或 V6.0
- 对防毒墙网络版服务器和 Cisco NAC 策略服务器都仅支持 Apache 2.0.54。

### Web 控制台

要使用防毒墙网络版服务器管理 (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
- 颜色为 256 或更高时支持分辨率为 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

- Microsoft Windows NT 4.0
- Windows 2000 Professional Service Pack 4 和 Windows 2000 Server
- Windows XP Professional （直到 Service Pack 2）
- Windows Server 2003

### 硬件件

- 200MHz 单个或多个 Intel Pentium 处理器
- 对于 Windows NT 和 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 5-5　　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 |
| **VPN 集中器** | | | |

**表 5-5　　支持的平台和需求**

| 支持的平台 | 型号 | IOS 镜像 | 最小内存 / 闪存 |
|---|---|---|---|
| Cisco VPN 3000 系列 | 3005 - 3080 | V4.7 或更高版本 | 无 |
| **交换机** | | | |
| Cisco Catalyst 2900 | 2950, 2970 | IOS 12.1(22)EA5 | 无 |
| Cisco Catalyst 3x00 | 3550, 3560, 3750 | IOS 12.2(25)SEC | 无 |
| Cisco Catalyst 4x00 | Supervisor 2+ 或更高版本 | IOS 12.2(25)EWA | 无 |
| Cisco Catalyst 6500 | 6503、 6509、Supervisor 2 或更高版本 | CatOS 8.5 或更高版本 | Sup2 - 128MB<br>Sup32 - 256MB<br>Sup720 - 512MB |
| **无线访问接入点** | | | |
| Cisco AP1200 系列 | 1230 | 无 | 无 |

第 6 章

# 部署策略服务器 for Cisco NAC

本章中的主题：


- *策略服务器 for NAC 部署概述*（第 6-2 页）
- *Cisco Secure ACS 服务器登记*（第 6-3 页）
- *CA 证书安装*（第 6-3 页）
- *策略服务器 SSL 证书准备*（第 6-6 页）
- *Cisco Trust Agent 部署*（第 6-8 页）
- *策略服务器 for Cisco NAC 安装*（第 6-12 页）
- *ACS 服务器配置*（第 6-15 页）
- *策略服务器 for Cisco NAC 配置*（第 6-15 页）


**注意：** 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

# 策略服务器 for NAC 部署概述

请遵循以下步骤来部署策略服务器 for Cisco NAC：

1. **安装防毒墙网络版服务器：**在网络上安装防毒墙网络版服务器（请参阅 《*安装与部署指南*》）。

2. **安装防毒墙网络版客户机：**在希望策略服务器评估其病毒防护的所有客户机上安装防毒墙网络版客户机程序 （请参阅 《*安装与部署指南*》）。

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 *Cisco Secure ACS 服务器登记* （第 6-3 页））。

4. **导出并安装 CA 证书：**将 CA 证书导出到 ACS 服务器，并将副本保存在防毒墙网络版服务器上。此步骤仅当还未将证书部署到客户机和 ACS 服务器时才有必要 （请参阅 *CA 证书安装* （第 6-3 页））。

5. **部署 Cisco Trust Agent 和 CA 证书：**将 Cisco Trust Agent 和 CA 证书部署到所有防毒墙网络版客户机，以便客户机可以向策略服务器提交安全状态信息 （请参阅 *Cisco Trust Agent 部署* （第 6-8 页））。

6. **安装策略服务器 for Cisco NAC：**安装策略服务器 for Cisco NAC 以处理来自于 ACS 服务器的请求 （请参阅 *策略服务器 for Cisco NAC 安装* （第 6-12 页））。

7. **从策略服务器导出 SSL 证书：**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 *策略服务器 for Cisco NAC 安装* （第 6-12 页））。

8. **配置 ACS 服务器：**配置 ACS 服务器将状态验证请求转发给策略服务器 （请参阅 *ACS 服务器配置* （第 6-15 页））。

9. **配置策略服务器 for NAC：**创建和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机安全策略（请参阅*策略服务器 for Cisco NAC 配置*（第 6-15 页））。

---

**注意：** 以下步骤仅供参考，可能会根据 Microsoft 和 / 或 Cisco 界面的更新而更改。

执行本章中的任何任务前，请先验证网络中的网络访问设备是否能够支持 Cisco NAC（请参阅*支持的平台和需求*（第 5-20 页））。请参阅设备文档以查看安装和配置的说明。同时，在网络中安装 ACS 服务器。请参阅 Cisco Secure ACS 文档以查看相关说明。

---

## 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，请参阅您供应商的文档，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

防毒墙网络版客户机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 *CA 证书*（第 5-17 页）和 *Cisco Trust Agent 部署*（第 6-8 页））。

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，请参阅您供应商的文档。

---

**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 > 受信任根 > 证书**。
   j. 从列表中选择要分发到客户机和 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**字段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，以便可以将其使用 CTA 部署到客户机 （请参阅 *Cisco Trust Agent 部署*（第 6-8 页）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。

## 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。策略服务器安装程序自动生成 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） > 受信任根证书机构 > 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：C:\Program Files\Trend Micro\OfficeScan\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：C:\Program Files\Trend Micro\OfficeScan\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**字段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。

## Cisco Trust Agent 部署

Cisco Trust Agent (CTA) 支持防毒墙网络版客户机和支持 Cisco NAC 的网络访问设备之间的通信。在安装和部署防毒墙网络版服务器与防毒墙网络版客户机后，从 Web 控制台将 CTA 部署到防毒墙网络版客户机。 CTA 部署软件包中包括在防毒墙网络版服务器上保存的 CA 证书（请参阅 *CA 证书安装* （第 6-3 页））。

**注意：** 请首先在客户端计算机上安装 Windows Installer 2.0 或更高版本，然后再部署代理。

从防毒墙网络版 Web 控制台将 CTA 部署到客户机：

1. 打开防毒墙网络版服务器 Web 控制台。
2. 执行以下操作之一：
   - 如果已经将证书分发到客户机，请转到步骤 3。
   - 如果尚未将证书分发到客户机，请执行以下操作：
     i. 单击 **Cisco NAC > 客户机证书**。将显示 “导入客户机证书”窗口。
     ii. 键入已准备好的 CA 证书存储在服务器上的完整路径和文件名。有关准备 CA 证书的说明，请参阅 *CA 证书安装*（第 6-3 页）。
     iii. 单击**导入**。将显示证书信息。

---

**注意：** 在安装防毒墙网络版服务器的过程中，如果未接受 Cisco 授权合约书中的条款，则将无法部署代理。单击**代理部署**后，将再次显示许可证信息。阅读该授权合约书，然后单击**是**同意条款。

---

3. 单击菜单中的**代理部署**。将显示客户机树。
4. 选择要部署 CTA 的客户机或域，然后单击**部署代理**。将显示**代理安装 / 卸装**窗口。
5. 单击**安装 / 升级 Cisco Trust Agent**，然后单击**应用至全部客户机**。
6. 单击**关闭**。

---

**注意：** 如果在单击**安装 Cisco Trust Agent** 时，要部署代理的目标客户机未联机，则防毒墙网络版将在该客户计算机联机时自动完成任务。

---

如果在安装防毒墙网络版服务器之前已准备好 CA 证书，则可以在安装防毒墙网络版服务器的过程中部署 CTA。部署 CTA 的选项在主安装程序的“安装其他防毒墙网络版程序”窗口中。有关安装防毒墙网络版服务器的说明，请参阅 《*安装与部署指南*》。

**使用防毒墙网络版服务器主安装程序将 CTA 部署到客户机：**

1. 在 “安装其他防毒墙网络版程序”窗口中，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 最终用户客户机，则单击**下一步**。
   - 如果需要将证书分发到客户机：
     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 *CA 证书安装*（第 6-3 页）。
     iii. 单击**下一步**。
3. 继续进行防毒墙网络版服务器安装过程。

## Cisco Trust Agent 升级和部署

如果 Cisco NAC Access Control Server (ACS) 是 4.0 版或更高版本，则必须将 Cisco Trust Agent 升级到 2.0 版或更高版本。

**升级 CTA：**

1. 在主菜单上，单击 **Cisco NAC > 代理管理**。
2. 单击**使用 {CTA 版本 )**。防毒墙网络版将升级服务器上的代理。

3. 在主菜单上，单击**代理部署 > 部署代理**。
4. 单击**安装 / 升级 Cisco Trust Agent** 将代理手动部署到防毒墙网络版客户机。
5. 单击**仅应用到将来的客户机**保存设置而不部署代理；或单击**应用至全部客户机**部署代理。

手动替换 CTA 软件包：

如果有要使用的特定版本，则可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：

   **{ 防毒墙网络版安装文件夹 }\OfficeScan\PCCSRV\Admin\Utility\CTA\CTA-Package**

   **或者**

   **{ 防毒墙网络版安装文件夹 }OfficeScan\PCCSRV\Admin\Utility\CTA\CTA-Supplicant-Package**

2. 将以下文件复制到 { 防毒墙网络版安装文件夹 }\OfficeScan\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，这些文件将被压缩为 { 防毒墙网络版安装文件夹 }OfficeScan\PCCSRV\download\Product 下的 CTA 部署软件包 PostureAgent.zip。

### Cisco Trust Agent 安装验证

在将 CTA 部署到客户机后，通过查看客户机树来验证安装是否成功。客户机树包含标题为 **CTA 程序**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。

也可以验证 ctapsd.exe、ctaEoU.exe、ctatransapt.exe 和 ctalogd.exe 进程是否正在客户端计算机上运行。

## 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 CD 上的策略服务器安装程序
- 防毒墙网络版服务器主安装程序 （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：** 主安装程序在您指定的 Web 服务器上安装防毒墙网络版服务器和策略服务器 Web 控制台：IIS 或 Apache。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 服务器版本不是 2.0 或更高版本，安装程序将自动安装 Apache V2.0。

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以确保有效的通信。

---

**警告！** *安装 Apache Web 服务器之前，请参阅 Apache Web 站点以了解有关升级、修补程序和安全问题的最新信息：* 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过程。
4. 显示趋势科技策略服务器 for Cisco NAC 的 “欢迎”窗口时，单击**下一步**。将显示 “策略服务器 for Cisco NAC 授权合约书”窗口。
5. 阅读协议，然后单击**是**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 服务器上进行安装
   - **Apache 2.0 Web 服务器**：单击以在 Apache 2.0 Web 服务器上进行安装
9. 单击**下一步**。将显示 “Web 服务器配置”窗口。
10. 配置以下信息：

- 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
- 在**端口**旁键入将用作服务器侦听端口的端口。

---

**注意：** 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。

---

- 如果选择了将策略服务器安装在 IIS 服务器上，则还可以选择启用安全套接字层 (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。策略服务器的地址将为：
  - http://{ 策略服务器名称 }:{ 端口号 } 或
  - https://{ 策略服务器名称 }:{ 端口号 }（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。**

# 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。请参阅您的 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：** 您可以配置 ACS 服务器来执行阻止客户机访问网络等功能。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，请参阅您的 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机与 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：

- *从防毒墙网络版配置策略服务器*（自 6-16 页开始）描述如何在防毒墙网络版 Web 控制台上管理策略服务器。
- *策略服务器的摘要信息*（自 6-17 页开始）向您显示如何获取网络上策略服务器的概述。
- *策略服务器注册*（自 6-18 页开始）是配置策略服务器过程中的第一步。
- *规则*（自 6-19 页开始）向您显示如何创建和编辑组成策略的规则。

- *策略* （自 6-19 页开始）向您显示如何创建和编辑最终决定策略服务器测定客户机安全状态的规则。
- *客户机验证日志* （自 6-19 页开始）概述了如何使用日志来了解网络中客户机的安全状态。
- *管理工具* （自 6-20 页开始）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 “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**添加**。

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机，请向至少一个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、客户机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”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。

趋势科技建议您在网络中的所有策略服务器上配置相同的设置，以保持一致的防病毒策略。

### 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*同步*（第 5-14 页）。

## 策略服务器注册

至少使用一个防毒墙网络版服务器注册策略服务器，以便策略服务器可以获取病毒码和病毒扫描引擎版本信息（要了解有关验证过程中防毒墙网络版服务器发挥的作用的信息，请参阅*网络访问验证顺序*（第 5-6 页））。

**注意：** 要使策略服务器验证网络上的所有客户机，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步配置规则 （请参阅*规则组成* （第 5-9 页）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

配置完新规则或确保缺省规则符合您的安全实施需求后，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*策略组成*（第 5-12 页）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，并确定在客户机安全状态与所有规则不匹配时在客户机上要采取的操作。

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**。

## 客户机验证日志

在客户机使用策略服务器进行验证时，使用客户机验证日志查看有关客户机的详细信息。 ACS 服务器检索客户机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*客户机验证顺序* （第 5-5 页））。

---

**注意：** 要生成客户机验证日志，添加或编辑新规则或策略时，请选中**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 > 查看客户机验证日志**。

## 客户机日志维护

策略服务器在客户机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机验证日志的方式。

## 管理工具

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*从防毒墙网络版配置策略服务器*（第 6-16 页））
- **配置同步时间表：**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机的安全状态。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*同步*（第 5-14 页）以获取详细信息）。

**注意：** 可以随时在 “摘要”窗口中手动同步策略服务器和防毒墙网络版服务器 （请参阅*策略服务器的摘要信息*（第 6-17 页））。

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 7 章

# 使用控制管理中心管理防毒墙网络版

本章中的主题：


- *控制管理中心基本功能*（第 7-2 页）
- *趋势科技管理通信协议*（第 7-3 页）
- *MCP 代理波动信号*（第 7-7 页）
- *防毒墙网络版注册*（第 7-10 页）
- *防毒墙网络版管理*（第 7-10 页）
- *目录管理器*（第 7-19 页）
- *临时*（第 7-22 页）
- *组件下载和部署*（第 7-26 页）
- *报告*（第 7-43 页）

# 控制管理中心基本功能

趋势科技防毒墙控制管理中心管理在贵组织的本地网和广域网中部署的防毒墙网络版服务器。还可管理其他防病毒及内容安全产品和服务。

**表 7-1. 控制管理中心功能**

| 功能 | 描述 |
|---|---|
| 集中式配置 | 产品目录和层叠管理结构允许您从单个管理控制台中协调安全风险响应事务。<br>这帮助您确保贵组织实施的安全风险防护策略具有一致性。 |
| 前瞻性爆发阻止 | 使用爆发阻止服务 (OPS)，可采取前瞻性步骤来阻止网络中出现安全风险爆发。 |
| 安全通信基础架构 | 控制管理中心使用建立在安全套接层 (SSL) 协议上的通信基础架构。<br>根据使用的安全设置，控制管理中心可以对邮件进行加密或使用认证对其进行加密。 |
| 安全配置和组件下载 | 这些功能允许您配置安全管理控制台访问权限和组件下载。 |
| 任务委派 | 系统管理员可以赋予控制管理中心的管理控制台用户具有定制权限的个性化帐户。<br>用户帐户定义用户在控制管理中心网络上可以看到的内容和可执行的操作。通过用户日志跟踪帐户的使用。 |
| 命令跟踪 | 此功能允许您监控所有使用控制管理中心管理控制台执行的命令。<br>命令跟踪对于确定控制管理中心是否已成功执行了持续时间较长的命令（如病毒码更新和部署）十分有用。 |
| 按需产品控制 | 实时管理防毒墙网络版服务器。<br>控制管理中心可立即将管理控制台上所进行的配置修改发送给防毒墙网络版服务器。例如，系统管理员可以从管理控制台中运行 “手动扫描”，这在病毒爆发过程中是必不可少的。 |
| 集中式更新控制 | 从管理控制台更新防毒墙网络版组件。 |

**表 7-1. 控制管理中心功能**

| 功能 | 描述 |
| --- | --- |
| 集中式报告 | 使用全面的日志和报告获取防毒墙网络版性能的概述。 |

## 趋势科技管理通信协议

趋势科技管理通信协议 (MCP) 是趋势科技的下一代防毒墙网络版代理。 MCP 取代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：

- 降低网络负载和软件包大小
- 支持 NAT 和防火墙遍历
- 支持 HTTPS
- 支持单向和双向通信
- 支持单点登录 (SSO)

## 降低网络负载和软件包大小

TMI 使用一种基于 XML 的应用协议。尽管 XML 在协议设计中提供了一定程度的扩展性和灵活性，但是将 XML 应用为该通信协议的数据格式标准还是有以下缺点：

- 与其他数据格式（如 CGI 名称 - 值对和二进制结构）相比，XML 解析需要更多系统资源（该程序对防毒墙网络版服务器有很大影响）。
- 传输 XML 格式的信息需要的代理资源比其他数据格式大得多。
- 由于数据占用资源更多，数据处理性能变得更低。
- 数据包传输需要更长时间，传输速率低于其他数据格式。

MCP 的数据格式解决了这些问题。 MCP 的数据格式是 BLOB （二进制）流，其中每个项由名称 ID、类型、长度和值组成。这种 BLOB 格式具有以下优点：

- **数据传输大小比 XML 更小：**每种数据类型仅要求有限数量的字节来存储信息。这些数据类型是整数、无符号整数、布尔型和浮点型。
- **解析速度更快：**使用二进制格式，可以轻松地依次解析每个数据项。与 XML 比较，性能要高几倍。
- **设计灵活性提高：**还考虑到了设计灵活性，因为每个项都包括名称标识、类型、长度和值。没有严格的项顺序，只有需要的时候，才会在通信协议中显示问候项。

除了将二进制流格式应用于数据传输外，多种类型的数据都能打包在一个连接中，无论是否压缩。这种类型的数据传输策略可节省网络带宽并产生改良的可伸缩性。

## 支持 NAT 和防火墙遍历

由于 IPv4 网络上的可寻址 IP 有限，因此已广泛使用 NAT （网络地址转换）设备，以允许多个端点计算机连接到互联网。NAT 设备是通过将连接到 NAT 设备的计算机组成一个专用虚拟网络而实现这点的。连接到 NAT 设备的每台计算机都将有一个专用的虚拟专有 IP 地址。在向互联网发送请求之前，NAT 设备将把此专有 IP 地址转换为一个真实的 IP 地址。由于每个连接的计算机都使用虚拟 IP 而且网络应用程序没有意识到此行为，因此这可能会产生一些问题。这通常会产生意外的程序故障和网络连接问题。

对于与 TMCM 2.5/3.0 代理一起使用的产品，会假设一个先决条件。服务器所依赖的一个事实是，可以通过从服务器启动到代理的连接而联系到代理。这是一个所谓的双向通信产品，因为两端都可以启动到对方的连接。当代理处于 NAT 设备后面 （或控制管理中心处于 NAT 设备后面）时，这个假设就不成立了，因为该连接只能路由到 NAT 设备，而不是 NAT 设备后面的产品 （或处于 NAT 设备后面的控制管理中心）。一个常用的迂回方法是，在 NAT 设备上建立特定的映射关系，以指示它自动将入站请求路由到各自的代理。但是，这种解决方法需要用户介入，并且当需要大规模产品部署时，这样做的效果不太好。

MCP 通过引入了一个单向通信模型而解决了这个问题。使用单向通信，仅代理可以启动到服务器的网络连接。服务器不能启动到代理的连接。此单向通信对日志数据传输效果很好。但是，服务器分派命令是在被动模式下发生的。也就是说，命令部署依赖于代理向服务器轮询可用的命令。

## 支持 HTTPS

MCP 集成协议应用业界标准通信协议 (HTTP/HTTPS)。HTTP/HTTPS 与 TMI 比较有几个优点：

- IT 中的大多数人都熟悉 HTTP/HTTPS，这使得容易确定通信问题和发现这些问题的解决方法
- 对于多数企业环境，不需要在防火墙中打开额外的端口来允许数据包通过
- 可以使用为 HTTP/HTTPS 构建的现有安全机制，如 SSL/TLS 和 HTTP 摘要认证。

使用 MCP，控制管理中心有三个安全级别：

- **正常安全**：控制管理中心使用 HTTP 进行通信
- **中等安全**：如果支持 HTTPS，控制管理中心使用 HTTPS 进行通信，如果不支持 HTTPS，则使用 HTTP。
- **高安全**：控制管理中心使用 HTTPS 进行通信

## 支持单向和双向通信

MCP 支持单向和双向通信。

### 单向通信

NAT 遍历在真实世界的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 CGI 命令的查询或日志传输。为减少网络的影响，连接保持活动状态并尽可能地开放。随后的请求会使用现有打开的连接。即使丢失了该连接，通过 SSL 对同一主机的所有连接都得益于会话 ID 缓存，它大大减少了重新连接的时间。

### 双向通信

除单向通信外，还可以选择双向通信。它仍基于单向通信，但是有一个额外的通道来接收服务器的通知。这个额外的通道也是基于 HTTP 协议的。双向通信可以通过 MCP 代理改进从服务器实时分派和处理命令。

### 支持单点登录 (SSO)

通过 MCP，控制管理中心 3.5 现在支持防毒墙网络版和其他趋势科技产品的单次登录 (SSO) 功能。该功能允许用户登录到控制管理中心并访问防毒墙网络版，而无需再登录到防毒墙网络版控制台。

## MCP 代理波动信号

为了监控防毒墙网络版的状态， MCP 代理根据一个时间表轮询控制管理中心。轮询是为了指示防毒墙网络版服务器的状态，以及检查从控制管理中心向防毒墙网络版服务器发出的命令。然后控制管理中心管理控制台会显示产品的状态。这意味着防毒墙网络版服务器的状态不是实时的、每时每刻的网络状态的反映。控制管理中心在后台依次检查每个防毒墙网络版服务器的状态。并且在经过没有波动信号的固定时间段后，将其状态更改为脱机。

活动的波动信号不是控制管理中心用于确定防毒墙网络版状态的唯一方法。下面的方法也向控制管理中心提供防毒墙网络版服务器的状态：

- 控制管理中心从防毒墙网络版服务器接收日志。一旦控制管理中心从防毒墙网络版服务器成功接收任何类型的日志，即表示防毒墙网络版服务器工作正常。
- 在双向通信模式下，控制管理中心主动地发送通知消息来触发防毒墙网络版服务器检索未决命令。如果控制管理中心成功连接防毒墙网络版服务器，则产品工作正常并且该事件会被计为一次波动信号。

- 在单向通信模式下， MCP 代理会定期向控制管理中心发送查询命令。该定期查询行为和波动信号起着相似的作用，会被控制管理中心作为波动信号一样处理。

MCP 代理波动信号用以下方式实现：

- **UDP**：如果防毒墙网络版可以用 UDP 联系到服务器，这是负荷最小、最快的可用解决方案。但是，在 NAT 或防火墙环境下这不起作用。并且，防毒墙网络版无法确定控制管理中心的确收到了请求。
- **HTTP/HTTPS**：为了在 NAT 或防火墙环境下工作，可使用重负荷的 HTTP 连接传输波动信号。

控制管理中心既支持 UDP 机制也支持 HTTP/HTTPS 机制来报告波动信号。控制管理中心服务器会在注册过程期间确定防毒墙网络版服务器应用哪种模式。两者之间会另外进行一次单独的协议握手以确定模式。

除了简单地发送波动信号表明产品的状态以外，其他数据可以和波动信号一起上传到控制管理中心。数据通常包含要在控制台显示的防毒墙网络版服务器活动信息。

## 时间表栏

使用 “通信器预设程序”窗口中的时间表栏来显示和设置通信器时间表。该栏具有 24 个时段，每个时段都表示一天中的小时数。

蓝色时段表示“工作”状态或通信器向控制管理中心服务器发送信息的时间。白色时段表示空闲时间。通过切换特定时段可定义 “工作”或“空闲”时间。

最多可指定三个连续非活动期。下面的样本时间表栏仅显示两段非活动时间：

此栏指定的活动周期是从 0:00 A.M 至 7:00 A.M、8:00 A.M 至 3:00 P.M 以及 6:00 P.M 至 12:00 P.M。

## 正确的波动信号设置

选择波动信号设置时，请在显示最新通信器状态信息的需要和管理系统资源的需要之间保持平衡。趋势科技的缺省设置可以满足大多数情况。但是当您定制波动信号设置时，请考虑以下几点：

**表 7-2. 波动信号建议**

| 波动信号频率 | 建议 |
| --- | --- |
| 长时间间隔波动信号（60 分钟以上） | 波动信号的时间间隔越长，控制管理中心在控制管理中心管理控制台上反映通信器状态之前可能发生事件的数量就越多。<br>例如，如果和一个通信器的连接问题在波动信号之间得以解决，则即使其状态显示为 （非活动）或 （异常）与一个通信器进行通信也是可能的。 |
| 短时间间隔波动信号（60 分钟以下） | 波动信号之间的短时间间隔会在控制管理中心服务器上显示网络状态的最新情况。但这个选项对带宽要求较高。 |

# 防毒墙网络版注册

防毒墙网络版是一种独立产品，无需将其注册到控制管理中心。但是，通过注册到控制管理中心，您可以获得本章前面部分所述的好处。

请参考防毒墙网络版联机帮助来了解注册步骤。注册后，请执行以下操作：

1. 打开控制管理中心管理控制台。
2. 在**主菜单**中，单击**产品**。
3. 在最左侧菜单上，从列表中选择**被管理产品**，然后单击**转到**。
4. 查看是否显示了防毒墙网络版服务器。

# 防毒墙网络版管理

通过产品目录间接管理一个或多个防毒墙网络版服务器。使用目录管理器来定制产品目录组织。

**表 7-3. 控制管理中心产品目录**

| 产品目录树 | 图标 | 描述 |
|---|---|---|
| | | 新建实体或用户定义文件夹名称 |
| | | 防毒墙网络版服务器 |
| | | 连接状态 |

使用目录管理器安排产品目录。使用描述性文件夹对防毒墙网络版服务器进行分组，依据是其防护类型和控制管理中心网络管理模型。

## 产品目录

规划产品目录的结构时需谨慎，因为它会影响以下内容：

- **用户访问权限：**创建用户帐户时，控制管理中心提示用户可以访问的产品目录段。由于仅能授予单个段的访问权限，因此请谨慎规划产品目录。例如，授予对根段的访问权限也就授予了对整个产品目录的访问权限。
- **部署规划：**控制管理中心根据部署规划来部署组件和程序更新。这些规划部署到产品目录文件夹。因此，结构良好的目录将简化收件人的指定。
- **爆发阻止策略 (OPP) 部署：**OPP 依靠部署规划而有效地分发策略。

## 产品目录任务

### 访问防毒墙网络版缺省文件夹

新注册的防毒墙网络版服务器通常出现在**新建实体**文件夹中，这取决于代理安装过程中指定的用户帐户。控制管理中心通过在安装过程中指定的用户帐户的权限而确定防毒墙网络版服务器的缺省文件夹。

### 访问产品目录

使用产品目录来管理注册到控制管理中心服务器的防毒墙网络版。

---

**注意：** 查看和访问产品目录中的文件夹取决于帐户类型和用于登录到管理控制台的文件夹访问权限。

---

**访问产品目录：**

1. 在主菜单上单击**产品**。
2. 在最左侧菜单上，从列表中选择**被管理产品**，然后单击**转到**。

### 刷新产品目录

要刷新产品目录，在产品目录中，单击左侧菜单右上角处的**刷新**图标。

### 使用产品目录部署新组件

手动部署允许您按需更新防毒墙网络版组件。这在安全风险爆发期间尤为有用。

将其部署到防毒墙网络版服务器之前，请先下载新组件。

#### 使用产品目录手动部署新组件

1. 在主菜单上单击**产品**。
2. 在最左侧菜单上，从列表中选择**被管理产品**，然后单击**转到**。
3. 在左侧菜单上，选择所需的文件夹或防毒墙网络版服务器。
4. 在工作区上，单击**任务**选项卡。
5. 选择**部署病毒码文件 / 清除模板**或**部署引擎**。
6. 单击**下一步**。
7. 单击**立即部署**开始手动部署新组件。
8. 通过命令跟踪监控进度。
9. 单击**命令详细信息**链接来查看组件部署的详细信息。

### 查看防毒墙网络版状态摘要

“产品状态”窗口显示所有防毒墙网络版服务器和其他被管理产品的安全风险防护状态。

有两种方法可以查看防毒墙网络版状态摘要：

- 通过主页

- 通过产品目录

**通过主页访问：**

- 打开控制管理中心管理控制台时，主页的 “状态摘要”选项卡显示整个控制管理中心系统的摘要。此摘要与产品目录 Root 文件夹中 “产品状态”选项卡中提供的摘要完全相同。

**通过产品目录访问：**

1. 在主菜单上单击**产品**。
2. 在左侧菜单上，选择所需的文件夹或防毒墙网络版服务器。
   - 如果单击防毒墙网络版服务器，“产品状态”选项卡将显示该防毒墙网络版服务器的摘要。
   - 如果单击 Root 文件夹、新建实体或其他由用户定义的文件夹，则 “产品状态”选项卡显示整个控制管理中心系统的摘要

---

**注意：** 缺省情况下，状态摘要显示到查询之日为止的相当于一周的信息。可将该范围更改为**显示摘要**列表中可用的 “今天”、“上个星期”、“上两个星期”或 “上个月”。

---

## 防毒墙网络版配置

您可以根据文件夹分区逐个或按组配置防毒墙网络版服务器。使用文件夹的**配置**选项卡执行组配置。

---

**注意：** 当执行组配置时，请确认您希望组中所有防毒墙网络版服务器都具有相同的配置。否则，将应当具有相同配置的防毒墙网络版服务器添加到 “临时”文件夹以防止覆盖其他服务器的设置。

---

“配置”选项卡显示产品的 Web 控制台或控制管理中心生成的控制台。

配置防毒墙网络版：

1. 在主菜单上单击**产品**。
2. 在最左侧菜单上，从列表中选择**被管理产品**，然后单击**转到**。
3. 在左侧菜单上，选择所需的防毒墙网络版服务器或文件夹。
4. 在工作区上，单击**配置**选项卡。
5. 从 “选择产品”列表中选择 “防毒墙网络版”。

**注意：** 如果使用文件夹的 “配置”选项卡，则步骤 4 是必需的。

6. 在 “选择配置”列表中，选择要访问或配置的防毒墙网络版功能。
7. 单击**下一步**。将显示防毒墙网络版 Web 控制台。

## 防毒墙网络版任务管理

使用**任务**选项卡对防毒墙网络版调用可用操作。您可以在防毒墙网络版上执行以下任务：

- 复制配置内容
- 部署引擎
- 部署许可证概要文件
- 部署病毒码文件 / 清除模板
- 部署程序文件
- 启用实时扫描
- 立即启动扫描

将最新病毒码文件或扫描引擎部署到具有过期组件的防毒墙网络版服务器。要成功实现该操作，控制管理中心服务器必须具有来自趋势科技 ActiveUpdate 服务器的最新组件。执行手动下载以确保控制管理中心服务器上已具有当前组件。

**向防毒墙网络版发出任务：**

1. 访问产品目录。
2. 在左侧菜单上，选择所需的防毒墙网络版服务器或文件夹。
3. 在工作区上，单击**任务**选项卡。
4. 从**选择任务**列表中选择任务。
5. 单击**下一步**。
6. 通过命令跟踪监控进度。单击响应窗口中的**命令详细信息**链接来查看命令信息。

## 防毒墙网络版日志

使用**日志**选项卡可查询和查看某个组或特定防毒墙网络版服务器的日志。

**查询和查看防毒墙网络版服务器日志：**

1. 访问产品目录。
2. 在左侧菜单上，选择所需的防毒墙网络版服务器或文件夹。
3. 在工作区上，单击**日志**选项卡。
4. 选择客户机日志类型：

**事件日志：**

**a.** 提供以下搜索参数：

**表 7-4. 用于事件日志的搜索参数**

| 参数 | 描述 |
|---|---|
| 严重性 | 是指信息可用的程度。选项有：严重、警告、信息、错误、未知。请选中所选参数的复选框。 |
| 事件 | 指事件。选项有：所有事件、病毒爆发、模块更新、服务开启、服务关闭、安全违例、疑似爆发和设备状态。 |
| 产品 | 如果选择一个文件夹，则此列表显示属于该文件夹的防毒墙网络版服务器。要查看有关所有防毒墙网络版服务器的信息，请选择**全部**。 |
| 记录时间 | 查看所有日志，或只查看防毒墙网络版服务器在特定时间间隔内生成的那些日志。对于后一选项，您可以指定过去 24 小时、过去一天、过去一周、过去一个月或定制时间范围的日志。<br>如果选择 “指定的范围”，则为 “起始日期”和 “终止日期”选择适当的年、月和日。 |
| 日志排序标准 | 按照日期 / 时间、计算机名称、产品、事件或严重性对结果排序。 |
| 排序顺序 | 以升序和降序对结果排序。 |

**b.** 单击**显示日志**开始查询并显示查询的结果。

**安全日志：**

**a.** 选择一种查询类别，然后单击**查询**。

**b.** 提供以下搜索参数：

**表 7-5. 用于安全日志的搜索参数**

| 参数 | 描述 |
|---|---|
| 记录时间 | 查看所有日志，或只查看防毒墙网络版服务器在特定时间间隔内生成的那些日志。对于后一选项，您可以指定过去 24 小时、过去一天、过去一周、过去一个月或定制时间范围的日志。<br>如果选择 “指定的范围”，则为 “起始日期”和 “终止日期”选择适当的年、月和日。 |
| 日志排序标准 | 按照日期 / 时间、计算机名称、产品、事件或严重性对结果排序。 |
| 排序顺序 | 以升序和降序对结果排序。 |

**c.** 单击**显示日志**开始查询。“查询结果”窗口以表的格式显示结果。

**5.** 结果表格中**实体的生成时间**列表示控制管理中心服务器时间。

## 防毒墙网络版移除后恢复

以下情形可能导致控制管理中心从产品目录中删除防毒墙网络版：

- 重新安装控制管理中心服务器，然后选择 “删除现有记录”并创建新数据库选项。此选项使用现有数据库的名称创建新数据库。
- 用同名的另一数据库替换损坏的控制管理中心数据库
- 使用目录管理器误删除防毒墙网络版服务器

如果控制管理中心服务器的防毒墙网络版服务器记录丢失了，防毒墙网络版上的代理仍然 “知道”它们被注册到何处。代理将在 8 小时后或服务重新启动时自动重新注册。

要恢复从产品目录移除的防毒墙网络版，请打开防毒墙网络版 Web 控制台，转到**管理 > 控制管理中心设置**，然后单击**更新设置**。

## 搜索工具

使用 “搜索”按钮可快速执行以下操作：

- 向 “临时”中添加特定或一组防毒墙网络版服务器
- 在产品目录中查找特定防毒墙网络版服务器

**搜索文件夹或防毒墙网络版服务器：**

1. 访问产品目录
2. 在左侧菜单上，单击**搜索**。
3. 在工作区上，提供以下搜索参数：

**表 7-6. 搜索参数**

| 参数 | 描述 |
|---|---|
| 搜索 | 从下拉列表中选择搜索对象。<br>根据其名称、文件夹名称或计算机名称搜索被管理的防毒墙网络版服务器或通信器。 |
| 关键字 | 允许您按名称搜索对象。<br>选择**区分大小写**可缩小搜索结果的范围。 |
| 状态 | 为通信器或被管理的防毒墙网络版服务器选择适当连接状态<br>选项有：全部、活动、非活动、异常、产品活动和产品非活动。选择**全部**可搜索所有连接状态的对象。 |
| 产品 | 从列表中选择 “防毒墙网络版”。 |

4. 单击**开始搜索**开始搜索。

5. 控制管理中心以表格形式显示搜索结果。您可以选择直接创建临时子文件夹 （将在此处将搜索结果进行分组）。

# 目录管理器

注册到控制管理中心之后，防毒墙网络版服务器会首先显示在产品目录中的缺省文件夹下。

使用目录管理器可定制产品目录组织来符合您的管理模型需求。

该目录允许您创建、修改或删除文件夹以及在文件夹之间移动防毒墙网络版。但是，您不能删除或重命名 “新建实体”文件夹。

请谨慎组织属于每个文件夹的防毒墙网络版服务器。规划和实现文件夹及防毒墙网络版服务器结构时，请考虑以下因素：

- 产品目录
- 用户帐户
- 部署规划

根据地理位置或管理原因对防毒墙网络版服务器进行分组。

**访问目录管理器：**

1. 访问产品目录
2. 在左侧菜单上，单击**目录管理器**。

## 目录管理器选项

目录管理器提供以下选项：新建文件夹、删除、重命名、撤消、重做、剪切、粘贴和重置。

使用这些选项在控制管理中心网络中操作和组织防毒墙网络版服务器。

**在目录管理器中使用和应用更改：**

- 右键单击某个文件夹或防毒墙网络版服务器，将打开一个弹出菜单，该菜单显示可以执行操作列表。
- 单击 **+** 或文件夹显示属于某个文件夹的防毒墙网络版服务器。
- 重命名文件夹后按 **Enter** 键或单击任意位置。
- 单击**保存**应用您的更改并更新目录管理器组织。
- 单击**重置**放弃尚未保存的更改。

## 目录管理器任务

### 创建文件夹

将防毒墙网络版分组到不同的文件夹中以符合贵组织的控制管理中心网络管理模型。

**创建文件夹：**

1. 访问目录管理器。
2. 在工作区上，右键单击要创建新文件夹的位置。如果是首次构建树，则右键单击 Root 文件夹。
3. 从弹出菜单中选择**新建文件夹**。控制管理中心将在主文件夹下创建一个新的子文件夹。
4. 键入新文件夹的名称或使用缺省名称，然后按 **Enter** 键。
5. 单击**保存**。

除了“新建实体”文件夹，控制管理中心以升序列出所有其他文件夹，从特殊字符（!、#、$、%、(、)、*、+、-、半角逗号、半角句点、+、?、@、[、]、^、_、{、>、} 和 ~）、数字（0 到 9）或字母字符（a/A 到 z/Z）开始。

## 重命名文件夹或防毒墙网络版

**重命名文件夹或防毒墙网络版服务器：**

1. 访问目录管理器。
2. 在工作区上，右键单击要重命名的文件夹或防毒墙网络版服务器，然后从弹出菜单中选择**重命名**。该文件夹 / 防毒墙网络版服务器名称变为可编辑字段。
3. 键入新文件夹的名称或使用缺省名称，然后按 **Enter** 键。
4. 单击**保存**。

---

**注意：** 重命名防毒墙网络版服务器仅更改存储在控制管理中心数据库中的名称。对产品无任何影响。

---

## 移动文件夹或防毒墙网络版服务器

**将一个文件夹或防毒墙网络版服务器传输或移动到另一个位置：**

1. 访问目录管理器。
2. 在工作区上，选择要移动的文件夹或防毒墙网络版服务器。
3. 执行以下操作之一：
   - 将文件夹或防毒墙网络版服务器拖放到新的目标位置
   - 将文件夹或防毒墙网络版服务器剪切并粘贴到新的目标位置

4. 单击**保存**。

### 删除用户定义的文件夹

在目录管理器中删除用户定义的文件夹时请小心。您可能会误删除防毒墙网络版服务器，这会导致其从控制管理中心服务器取消注册。

**删除用户定义的文件夹：**

1. 访问目录管理器。
2. 在工作区上，右键单击要删除的文件夹，然后从弹出菜单中选择**删除**。
3. 单击**保存**。

**注意：** 不能删除 “新建实体” 文件夹。

## 临时

“临时”是防毒墙网络版服务器快捷方式的集合，它允许您专注于特定服务器而不需更改产品目录的组织。使用“临时”可以将更新部署到具有过期组件的几组产品中。

使用 “临时”时请考虑以下问题：

- 从管理控制台注销时，控制管理中心会删除所有防毒墙网络版服务器的快捷方式。
- 仅当您可以在产品目录中看见防毒墙网络版服务器时，才能将它们添加到 “临时”中。您无法生成不能访问的服务器的快捷方式。

## 使用临时

可以使用与在产品目录中操作防毒墙网络版服务器的相同方法在 “临时”中操作防毒墙网络版服务器。属于“临时”的文件夹和防毒墙网络版服务器具有相同的文件夹级和防毒墙网络版服务器级的控件。但是，控制管理中心按照您用户帐户的访问权确定您可以在防毒墙网络版服务器上执行的操作。

可以将 “临时”用于以下目的：

- 使用文件夹级访问权限向成组的防毒墙网络版服务器发出命令。
- 选择特定的防毒墙网络版服务器，然后使用可用的产品目录选项卡执行操作。

**访问目录：**

1. 访问产品目录
2. 在最左侧菜单上，单击**临时**。

## 与临时相关的任务

### 向 “临时”添加防毒墙网络版

有三种方法可向 “临时”添加防毒墙网络版：

- 从搜索结果中
- 从产品目录中
- 基于 “状态摘要”页面添加具有过期组件的防毒墙网络版

趋势科技建议您使用最后一种方法一次向“临时”添加一些防毒墙网络版服务器。“状态摘要”窗口提供关于哪些防毒墙网络版使用过期组件的信息。它简化了属于不同文件夹组的防毒墙网络版组的组件更新。

**注意：** 向 “临时”中添加防毒墙网络版服务器仅允许您确定具有过期组件的服务器，这样做不会触发自动部署。

### 从搜索结果中添加：

1. 在主菜单上单击**产品**。
2. 在左侧菜单上，单击**搜索**。
3. 在工作区上，搜索防毒墙网络版服务器或文件夹。
4. 在**被管理产品的临时子文件夹**字段中为将包含防毒墙网络版服务器快捷方式的 “临时”子文件夹指定子文件夹名称。

   **注意：** 步骤 4 是可选的。如果要创建属于 “临时”的多个文件夹级别，请在 “实体的临时子文件夹”字段中指定 \{ 文件夹名 （第一级） }\{ 子文件夹名 （第二级） }。

5. 单击**添加**。控制管理中心将防毒墙网络版从搜索结果添加到“临时”。

### 从产品目录中添加：

1. 访问产品目录。
2. 在左侧菜单上，选择要添加到 “临时”的防毒墙网络版服务器。
3. 按数字小键盘上的 “+”。

### 基于 “状态摘要”页面添加具有过期组件的防毒墙网络版：

1. 访问产品目录
2. 在左侧菜单上，选择所需的产品目录文件夹。
3. 在工作区上，单击**产品状态**选项卡。

4. 在“组件状态”表中，单击表示过期防毒墙网络版服务器数量的数字链接之一。根据您单击的链接，会打开“病毒码状态（过期）”、“扫描引擎状态（过期）”窗口，显示计算机名、产品名称、产品版本和过期组件的版本。

5. 单击“状态”页面中的**添加到临时**。控制管理中心使用按添加防毒墙网络版服务器的源页面命名的文件夹，向“临时”中添加防毒墙网络版服务器。例如，控制管理中心会将防毒墙网络版（从“扫描引擎状态（过期）”页面添加的）放到“扫描引擎状态（过期）”文件夹下。

---

**注意：** 单击**添加到临时**仅会添加状态页面上显示的防毒墙网络版服务器。如果防毒墙网络版服务器的列表超出一个窗口，则单击所有窗口上的**添加到临时**以添加所有具有过期组件的服务器。

---

6. 单击**返回**返回到“状态摘要”页面，然后继续处理下一个过期组件。重复这些指令，直到控制管理中心将所有过期的防毒墙网络版服务器添加到“临时”中。

## 从“临时”中移除防毒墙网络版

**从“临时”中移除防毒墙网络版服务器：**

1. 访问产品目录

2. 在左侧菜单上，单击**临时**。

3. 从“临时”列表上的可用防毒墙网络版服务器中，选择要移除的文件夹或防毒墙网络版服务器快捷方式。

4. 按数字小键盘上的“-”。

---

**注意：** 从管理控制台注销时，控制管理中心会移除“临时”中的所有防毒墙网络版服务器的快捷方式。

从“临时”中移除防毒墙网络版既不会断开防毒墙网络版的连接，也不会从控制管理中心服务器卸装 MCP 代理。

---

# 组件下载和部署

更新管理器集中了帮助您更新控制管理中心网络上组件的各种功能。趋势科技建议更新组件，以保持对最新安全风险的防范。

以下是要更新的组件：

- **病毒码文件 / 清除模板**：包括以下内容：
  - 病毒码
  - 间谍软件特征码
  - 病毒清除模板
  - 间谍软件主动监控特征码
  - IntelliTrap 特征码
  - IntelliTrap 例外特征码
  - 通用防火墙特征码
- **引擎**：包括以下内容：
  - 病毒扫描引擎 （32 位版和 64 位版）
  - 间谍软件扫描引擎 （32 位版和 64 位版）
  - Venus Spy Trap 引擎 （32 位版和 64 位版）
  - 病毒清除引擎 （32 位版和 64 位版）
  - 防 rootkit 驱动程序 （32 位版）
- **产品程序**：特定于产品的组件 （例如， Service Pack 发行版）

**注意：** 仅注册用户才能执行组件更新。有关详细信息，请参阅控制管理中心联机帮助中的 “注册并激活软件 > 了解产品激活”主题。

为了将控制管理中心网络流量降到最低，请禁用下载防毒墙网络版不使用的组件。

## 更新管理器

更新管理器提供了帮助您更新控制管理中心网络中组件的功能。

更新控制管理中心包括两个步骤：

- 下载组件：可以手动或通过预设来执行此操作
- 部署组件：手动或通过预设来执行此操作

## 手动下载

当第一次安装控制管理中心、网络受到攻击或希望在将新组件部署到网络前先进行测试时，请手动下载组件更新。

这是趋势科技建议的配置手动下载的方式。手动下载组件需要多个步骤：

**提示：** 如果已经配置了部署规划并配置了代理服务器设置，则可以略过步骤 1 和 2。

**步骤 1：**为组件配置一个部署规划

**步骤 2：**配置代理服务器设置 （如果使用代理服务器）

**步骤 3：**选择要更新的组件

**步骤 4：**配置下载设置

**步骤 5：**配置自动部署设置

**步骤 6：**完成手动下载

**手动下载组件：**

**步骤 1：为组件配置一个部署规划**

1. 在主菜单上单击**管理**。
2. 在更新管理器下的左侧菜单上，单击**部署规划**。将显示“部署规划”窗口。

**图 7-1.　　部署规划窗口**

3. 在工作区上，单击**添加新规划**。

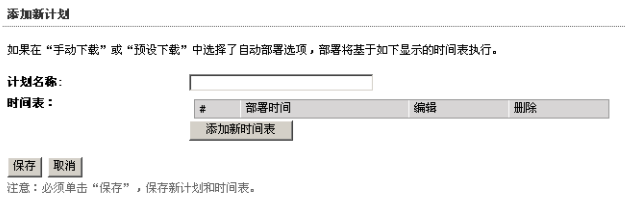



**图 7-2. 添加新规划窗口**

4. 在“添加新规划”窗口上的**规划名称**字段中键入一个部署规划名称。

5. 单击**添加新时间表**提供部署规划的详细信息。将显示 “添加新时间表”窗口。

**图 7-3. 添加新时间表窗口**

6. 在 “添加新时间表”窗口上，通过选择以下选项之一来选择一个部署时间表：

   - **延迟：**控制管理中心下载更新组件之后，控制管理中心会按照您指定的时间间隔延迟部署

     使用菜单指示持续时间，以小时和分钟为单位。

- **起始时间：**在特定的时间执行部署

  使用这些菜单指定该时间的时和分。

7. 选择将要应用该时间表的产品目录文件夹。控制管理中心将该时间表分配给所选文件夹下的所有防毒墙网络版服务器。

8. 单击**确定**。

9. 单击**保存**应用新的部署规划。

### 步骤 2：配置代理服务器设置 （如果使用代理服务器）

1. 单击**管理 > 系统设置**。将显示 “系统设置”窗口。

**图 7-4. 系统设置窗口**

2. 选中 “下载组件代理服务器设置”区域中的**使用代理服务器从 Internet 下载更新组件**复选框。

3. 在**主机名**字段中键入服务器的主机名或 IP 地址。
4. 在**端口**字段中键入一个端口号。
5. 选择协议：
   - HTTP
   - SOCKS
6. 如果服务器需要认证，则键入一个登录名和密码。
7. 单击**保存**。

## 步骤 3：选择要更新的组件

1. 单击**管理 > 更新管理器 > 手动下载**。将显示 “手动下载”窗口。

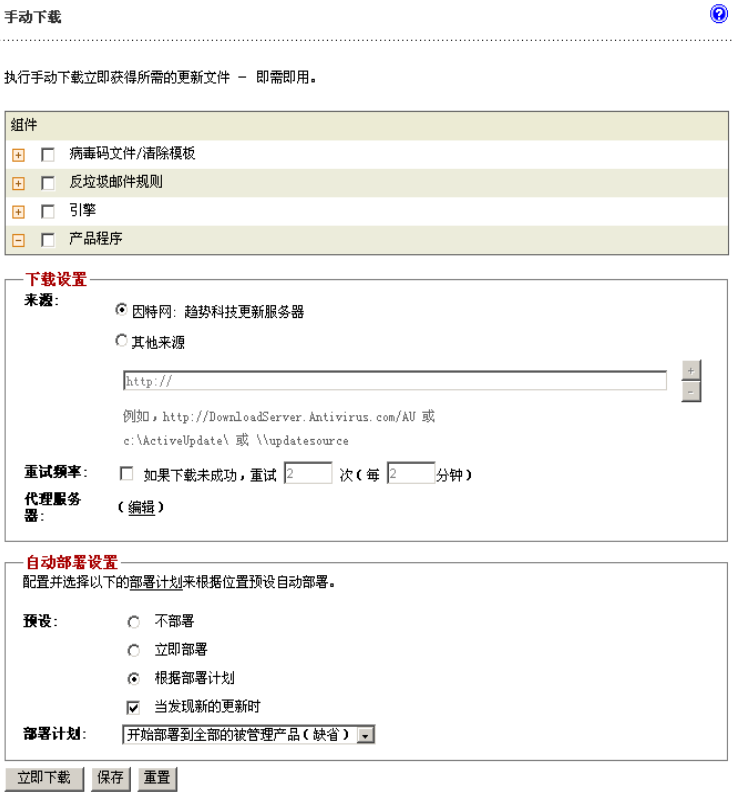



**图 7-5. 手动下载窗口**

2. 从“组件”区域中选择要下载的组件。

   a. 单击“+”图标展开每个组件组的组件列表。

   b. 选择要下载的防毒墙网络版组件。请参阅*防毒墙网络版组件与程序*（第 1-20 页）以获取详细信息。

### 步骤 4：配置下载设置

1. 选择更新源：

   - **Internet：趋势科技更新服务器：**从趋势科技 ActiveUpdate 服务器下载组件。
   - **其他更新源：**在随附的字段中键入更新源的 URL。

     选择“其他更新源”之后，可以指定多个更新源。单击“+”图标添加其他更新源。可以配置至多五个更新源。

2. 选择**重试频率**并指定下载组件的重试次数和重试之间的时间间隔。

---

**注意：** 在此窗口上单击**编辑**或**部署规划**之前，请先单击**保存**。如果不单击**保存**，您的设置将会丢失。

---

3. 如果在网络上使用 HTTP 代理服务器（即，控制管理中心服务器不能直接访问 Internet），请在“系统设置”窗口上单击**编辑**以配置代理服务器设置。

### 步骤 5：配置自动部署设置

1. 从“时间表”区域选择何时部署已下载的组件。选项有：

   - **不部署：**组件下载到控制管理中心，但不部署到防毒墙网络版。在以下条件下使用此选项：
     - 逐个部署到防毒墙网络版服务器

- 部署前测试已更新的组件

- **立即部署**：组件下载到控制管理中心，然后部署到防毒墙网络版服务器。
- **根据部署规划**：组件下载到控制管理中心，但根据所选择的时间表部署到防毒墙网络版服务器。
- **当发现新更新时**：当更新源中新组件可用时组件下载到控制管理中心，但根据所选择的时间表部署到防毒墙网络版服务器。

**注意：** 在此窗口上单击**编辑**或**部署规划**之前，请先单击**保存**。如果不单击**保存**，您的设置将会丢失。

2. 组件下载到控制管理中心之后，从**部署规划**列表中选择一个部署规划。
3. 单击**保存**。

### 步骤 6：完成手动下载

1. 单击**立即下载**，然后单击**确定**确认。将显示下载响应窗口。进度条显示下载状态。
2. 单击**命令详细信息**从 “命令详细信息”窗口查看详细信息。
3. 单击**确定**返回到 “手动下载”窗口。

## 预设下载例外

下载例外允许管理员在全天或者每天的特定时段中阻止控制管理中心下载趋势科技更新组件。

此功能对不想让控制管理中心在非工作日或者在非工作时间里下载组件的管理者特别有用。

配置预设下载例外：

1. 在主菜单上单击**管理**。
2. 在更新管理器下的左侧菜单上，单击**预设下载列外**。
3. 执行以下操作：
   - 要预设每日例外，在“每日预设例外”下，选中要阻止下载的日期的复选框，然后选中**不要在指定的日期下载更新**复选框。每个星期，在所选择的日期中所有的下载都会被阻止。
   - 要预设小时级别的例外，在“每小时预设例外”下，选中要阻止下载的时间的复选框，然后选中**不要在指定的小时内下载更新**复选框。每天，在所选择的小时中所有的下载都会被阻止。
4. 单击**保存**。

## 预设下载

配置组件的预设下载可将您的组件保持最新并保持网络安全。控制管理中心支持粒状组件下载。可以指定组件组和单个组件下载的时间表。所有时间表都是彼此独立的。预设组件组的下载，可以下载该组中的所有组件。

使用“预设下载”窗口可获得当前控制管理中心系统中组件的以下信息：

- **频率**：显示组件更新的频率
- **启用**：表示该组件的时间表是已启用还是已禁用
- **更新源**：显示更新源的 URL 或路径

配置预设组件下载需要多个步骤：

**步骤 1：**为组件配置一个部署规划

**步骤 2：**配置代理服务器设置 （如果使用代理服务器）

**步骤 3：**选择要更新的组件

**步骤 4：**配置下载时间表

**步骤 5：**配置下载设置

**步骤 6：**配置自动部署设置

**步骤 7：**启用时间表并保存设置

**配置和启用预设下载：**

**步骤 1：为组件配置一个部署规划**

**1.** 在主菜单上单击**管理**。

2. 在更新管理器下的左侧菜单上，单击**部署规划**。将显示“部署规划”窗口。

**图 7-6. 部署规划窗口**

3. 在工作区上，单击**添加新规划**。

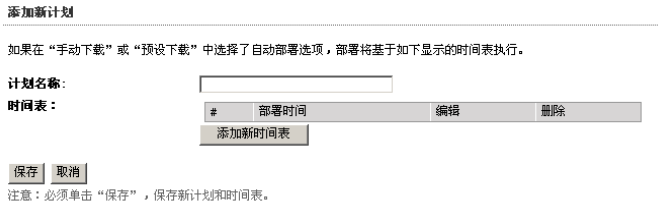



**图 7-7. 添加新规划窗口**

4. 在“添加新规划”窗口上的**规划名称**字段中键入一个部署规划名称。

5. 单击**添加新时间表**提供部署规划的详细信息。将显示 “添加新时间表”窗口。

6. 在 “添加新时间表”窗口上，通过选择以下选项之一来选择一个部署时间表：

   - **延迟**：控制管理中心下载更新组件之后，控制管理中心会按照您指定的时间间隔延迟部署

     使用菜单指示持续时间，以小时和分钟为单位。

   - **起始时间**：在特定的时间执行部署

     使用这些菜单指定该时间的时和分。

7. 选择将要应用该时间表的产品目录文件夹。控制管理中心将该时间表分配给所选文件夹下的所有防毒墙网络版服务器。

8. 单击**确定**。

9. 单击**保存**应用新的部署规划。

## 步骤 2：配置代理服务器设置 （如果使用代理服务器）

1. 单击**管理 > 系统设置**。将显示 “系统设置”窗口。

**图 7-8. 系统设置窗口**

2. 在**下载组件代理服务器设置**区域中，选中**使用代理服务器从 Internet 下载更新组件**复选框。
3. 在**主机名**字段中键入服务器的主机名或 IP 地址。
4. 在**端口**字段中键入一个端口号。
5. 选择协议：
   - HTTP
   - SOCKS
6. 如果服务器需要认证，则键入一个登录名和密码。

7. 单击**保存**。

步骤 3：选择要更新的组件

1. 单击**管理 > 更新管理器 > 预设下载**。将显示 “预设下载”窗口。

**图 7-9. 预设下载窗口**

2. 从 “组件”区域中选择要下载的组件。

   a. 单击 “+”图标展开每个组件组的组件列表。

   b. 选择要下载的防毒墙网络版组件。请参阅*防毒墙网络版组件与程序*（第 1-20 页）以获取详细信息。

将显示 { 组件名称 } 窗口。

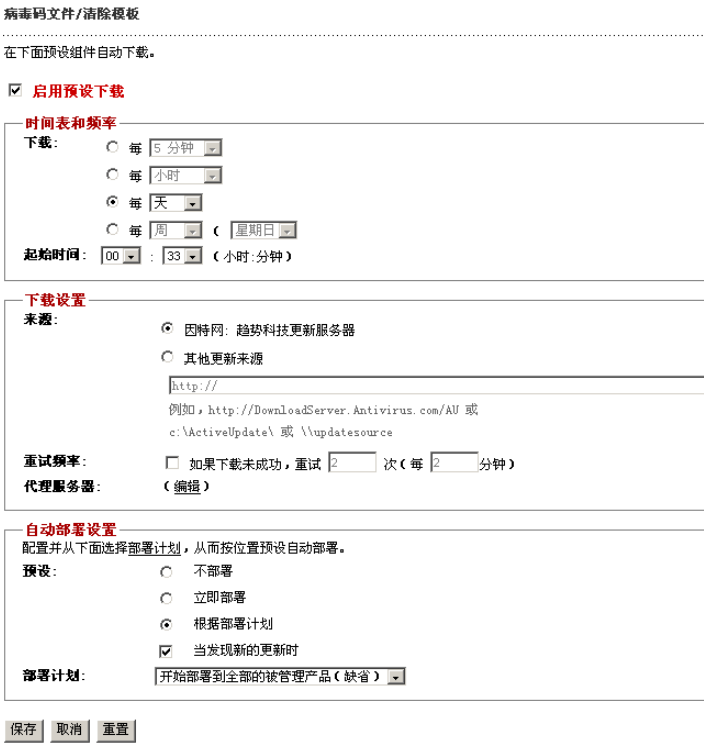



**图 7-10. { 组件名称 } 窗口**

## 步骤 4：配置下载时间表

1. 选中**启用预设下载**复选框来启用组件的预设下载。
2. 定义下载时间表。选择一个频率，然后使用相应的下拉菜单指定所需的时间表。您可以预设每分钟、每小时、每天或每周下载一次。
3. 使用**开始时间**菜单可指定预设开始生效的日期和时间。

### 步骤 5：配置下载设置

1. 选择更新源：

   - **Internet：趋势科技更新服务器：**从趋势科技 ActiveUpdate 服务器下载组件。
   - **其他更新源：**在随附的字段中键入更新源的 URL。

     选择 “其他更新源”之后，可以指定多个更新源。单击 “+” 图标添加其他更新源。可以配置至多五个更新源。

2. 选择**重试频率**并指定下载组件的重试次数和重试之间的时间间隔。

   **注意：** 在此窗口上单击**编辑**或**部署规划**之前，请先单击**保存**。如果不单击**保存**，您的设置将会丢失。

3. 如果在网络上使用 HTTP 代理服务器 （即，控制管理中心服务器不能直接访问 Internet），请在 “系统设置”窗口上单击**编辑**以配置代理服务器设置。

### 步骤 6：配置自动部署设置

1. 从 “时间表”区域选择何时部署已下载的组件。选项有：

   - **不部署：**组件下载到控制管理中心，但不部署到防毒墙网络版服务器。在以下条件下使用此选项：
     - 逐个部署到防毒墙网络版服务器
     - 部署前测试已更新的组件
   - **立即部署：**组件下载到控制管理中心，然后部署到防毒墙网络版服务器。

- **根据部署规划：**组件下载到控制管理中心，但根据所选择的时间表部署到防毒墙网络版服务器。
- **当发现新更新时：**当更新源中新组件可用时组件下载到控制管理中心，但根据所选择的时间表部署到防毒墙网络版服务器。

**注意：** 在此窗口上单击**编辑**或**部署规划**之前，请先单击**保存**。如果不单击**保存**，您的设置将会丢失。

2. 组件下载到控制管理中心之后，从**部署规划**列表中选择一个部署规划。
3. 单击**保存**。

**步骤 7：启用时间表并保存设置**

1. 单击“启用”栏中的状态按钮。
2. 单击**保存**。

# 报告

控制管理中心**报告**是关于在控制管理中心网络上发生的安全风险事件的在线数字集合。企业版提供了控制管理中心报告。

控制管理中心 3.5 根据以下类型对报告进行分类：

- 本地报告
- 全局报告

**注意：** 仅可通过父级服务器管理控制台配置**全局报告概要文件**选项。

## 本地报告

本地报告是关于由父级服务器管理的防毒墙网络版服务器的报告。本地报告不包括子级服务器生成的报告。使用“全局报告”选项可查看关于由注册到父级服务器的子级服务器管理的防毒墙网络版服务器的报告。

使用“本地报告”窗口可查看可用的一次性本地报告和预设的本地报告概要文件。

**访问本地报告：**

1. 在主菜单上单击**报告**。
2. 在 “报告”下的最左侧菜单中，单击**本地报告概要文件**。

---

**注意：** 当您有多个可用的报告时，按照 “报告概要文件”名称或 “创建日期”对报告排序。

---

## 全局报告

全局报告是关于由子级服务器及父级服务器管理的防毒墙网络版服务器的报告。

使用“全局报告”窗口可查看可用的一次性全局报告和预设的全局报告概要文件。

**访问全局报告：**

1. 在主菜单上单击**报告**。
2. 在 “报告”下的最左侧菜单中，单击**全局报告概要文件**。
3. 当多个报告可用时，按照 “报告概要文件”名称或 “上次创建日期”对报告排序。

**注意：** 仅父级服务器可以显示全局报告概要文件。

当您有多个可用的报告时，按照 “报告概要文件”名称或 “创建日期”对报告排序。

## 报告模板

报告模板描画了控制管理中心报告的外观。特别是，模板定义了在报告中显示哪些部分：

- 标题
- 报告主体
- 页脚

**注意：** 在控制管理中心 3.5 中间谍软件 / 灰色软件不再被视为病毒。此变化影响所有最初与病毒相关的报告中的病毒统计数。

要生成这些报告，请单击主菜单上的**报告**，然后单击导航菜单上“本地报告概要文件”下的**创建报告概要文件**。在工作区中显示的 “内容”选项卡中，您可以输入一个报告名称、一个可选的报告标题和一个可选的报告描述。使用**报告类别**列表来仔细查看以下列出报告类别。单击复选框中的标记，这将把相关报告包含在最终导出的报告文件中。

控制管理中心 3.5 也提供了 18 个模板作为 Crystal Report V9 文件 (*.rpt) 存储在 {root}\Program Files\Trend Micro\Control Manager\Reports 中。这些模板也适用于本地和全局报告。

## 报告概要文件

**概要文件**列出了报告的内容 （模板和格式）、目标、频率和收件人。您可以查看以下文件格式的报告：

- **RTF**：丰富文本格式；使用字处理程序 （例如 Microsoft Word）可查看 *.RTF 报告
- **PDF**：可移植的文档格式；使用 Adobe (TM) Reader (TM) 可查看 *.PDF 报告

- **ActiveX™ ：**ActiveX 文档；使用 Web 浏览器可查看 ActiveX 格式的报告

**注意：** 控制管理中心不能将 ActiveX 格式的报告作为电子邮件附件发送。

- **RPT：**Crystal Report 格式；使用 Crystal Smart Viewer 可查看 *.RPT 报告

生成报告之后，报告服务器会启动该报告文件格式的缺省查看器。对于 RPT 报告，您必须已安装 Crystal Smart Viewer。

## 与报告相关的任务

### 创建报告文件

创建报告概要文件的过程有五个步骤。创建本地报告或全局报告的过程十分相似。创建报告概要文件的过程如下：

**步骤 1：**选择创建本地报告还是全局报告

**步骤 2：**配置 “内容”选项卡设置

**步骤 3：**配置 “目标”选项卡设置

**步骤 4：**配置 “频率”选项卡设置

**步骤 5：**配置 “收件人”选项卡设置

**创建本地或全局报告概要文件：**

**步骤 1：选择创建本地报告还是全局报告**

1. 在主菜单上单击**报告**。
2. 执行以下操作之一：

- 要创建本地报告概要文件，请单击“报告”下的**本地报告概要文件**。
- 要创建全局报告概要文件，请单击“报告”下的**全局报告概要文件**。

3. 在左侧菜单中的“本地报告概要文件”或“全局报告概要文件”下，单击**创建报告概要文件**。

**图 7-11. “创建报告概要文件”窗口，“内容”选项卡**

步骤 2：配置“内容”选项卡设置

1. 在“本地报告”窗口工作区中**内容**选项卡下，在**报告名称**字段中为该报告键入一个名称，以标识该概要文件。
2. 在**报告标题**字段中为该报告键入一个标题（可选）。

3. 在**描述**字段中键入该报告概要文件的描述 （可选）。
4. 从**报告类别**列表中选择**台式机产品**。
5. 选择报告类型、要生成的特定报告以及输出格式。
6. 单击**下一步**进入**目标**选项卡。

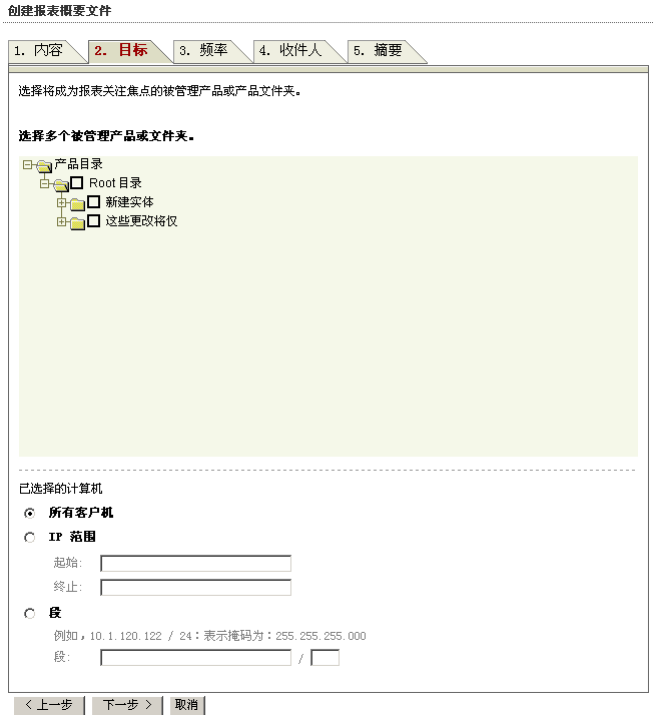



**图 7-12. “创建报告概要文件”窗口，“目标”选项卡**

**步骤 2：配置 “内容”选项卡设置**

1. 在工作区中的**目标**选项卡下，选择本地或全局报告的概要文件的目标：

   - 选择防毒墙网络版服务器或文件夹。该概要文件仅包含关于所选防毒墙网络版或文件夹的信息。
   - 选择子级服务器。该概要文件仅包含关于所选子级服务器的信息。选择父级服务器以便将所有子级服务器的被管理防毒墙网络版服务器包括在概要文件中。

2. 选择报告将包括的计算机：

   - **所有客户机：**所选防毒墙网络版服务器保护的所有客户机
   - **IP 范围：**选择要包括在报告中的客户机的 IP 范围
   - **网段：**选择要包含在报告中的客户机的 IP 范围和网段

3. 单击**下一步**进入**频率**选项卡。

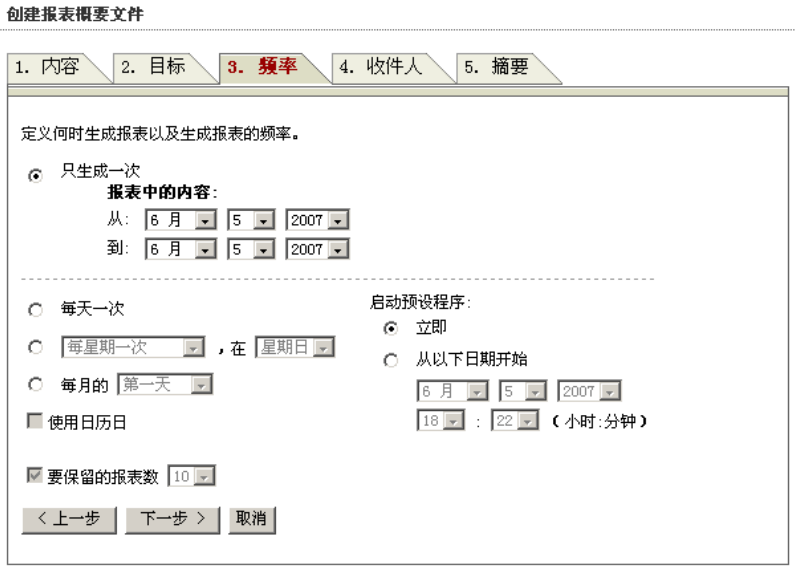



**图 7-13. “创建报告概要文件”窗口，“频率”选项卡**

步骤 4：配置 “频率”选项卡设置

1. 在工作区中的**频率**选项卡下，指定控制管理中心生成此报告的频率。您有以下选项：

   - **只生成一次：**提供您在 “从”和 “到”日期范围内指定的信息
   - **每日一次：**包含从创建时间 （前一天中午 12:00）起到当前时间的信息
   - **每星期一次或每两个星期一次：**包含相当于 7 或 14 天的信息；选择一星期内将触发报告服务器生成报告的一天

- **每月一次**：包含相当于 30 天的信息；选择某月份内将触发报告服务器生成报告的那一天（月初、15 日或月终）
- **使用日历日**：如果选中，则起始时间为第一天的 00:00:00，结束时间为生成前一天的 00:00:00

  如果未选中，则起始时间与第一天的生成小时值相同，结束时间是生成报告当天的生成小时值

2. 在**启动预设程序**下，指定报告服务器开始收集该报告信息的时间。选择以下操作之一：
   - **立即**：报告服务器在您保存报告概要文件后立即收集信息
   - **起始时间**：报告服务器在指定的日期和时间收集信息
3. 对于预设报告，请单击**要保留的报告数**，然后指定控制管理中心将在服务器上保留的实例。

---

**注意：** 控制管理中心会自动启用预设报告概要文件。要临时禁用生成报告，请导航至“本地预设报告”或“全局预设报告”窗口，然后取消选中设报告概要文件旁边的复选框。

---

4. 单击**下一步**进入**收件人**选项卡。

**图 7-14. “创建报告概要文件”窗口，“收件人”选项卡**

步骤 5：配置 “收件人”选项卡设置

1. 在工作区中的**收件人**选项卡下，从现有的控制管理中心用户和组中选择收件人。

   - 使用 >> 将收件人从**用户和组**列表添加到 “收件人”列表中。
   - 使用 << 从**收件人**列表中移除收件人。

2. 单击**将报告作为附件发送**，从而作为附件发送报告。否则，收件人将仅收到关于已生成的报告的电子邮件通知。

3. 单击**下一步**进入 “摘要” 选项卡。

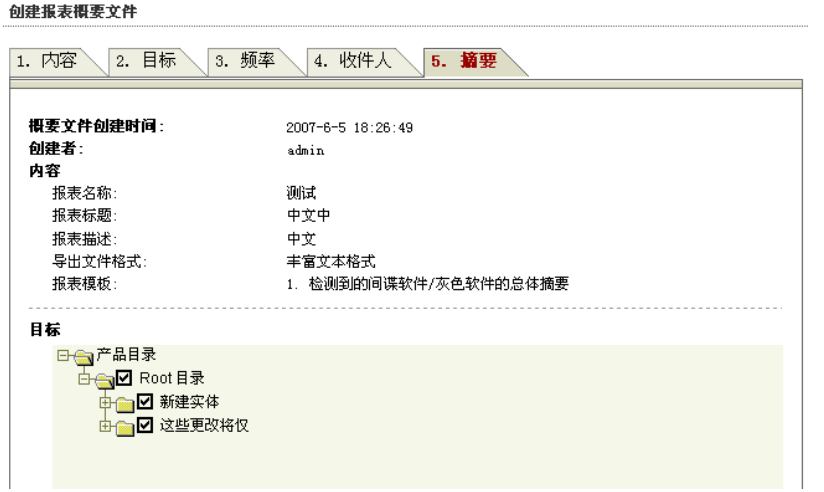



**图 7-15. “创建报告概要文件” 窗口，“摘要” 选项卡**

4. 在工作区中的 “**摘要**” 选项卡下，复查概要文件设置，然后单击**完成**保存该概要文件。

## 复查报告概要文件设置

使用 “概要文件摘要” 窗口来复查概要文件设置。

**访问概要文件摘要并复查报告概要文件：**

- 访问本地或全局报告

  在工作区中的 “概要文件摘要” 列下，单击**查看概要文件**。

- 访问本地或全局预设报告

  在工作区中的 “概要文件摘要” 列下，单击**查看概要文件**。

## 启用预设报告概要文件

缺省情况下，控制管理中心在概要文件创建后立即启用预设概要文件。在禁用概要文件（例如，在数据库或代理迁移期间）的情况下，可通过“预设本地报告”或“预设全局报告”窗口重新启用它。

**启用预设报告概要文件：**

1. 访问本地或全局预设报告。
2. 在工作区中的“报告概要文件”列下，单击概要文件的复选框。

   **单击“报告概要文件”旁边的复选框以选择或取消选择所有概要文件。**
3. 单击**启用**。

---

**注意：** 因为控制管理中心只生成这些报告一次，所以启用、禁用和编辑一次性概要文件的选项不可用。

---

## 生成按需预设报告

报告服务器根据指定的日期和时间生成预设报告。如果尚未到该日期和时间，可根据需要使用**立即运行**创建预设报告。

**生成按需预设报告：**

1. 在主菜单上单击**报告**。
2. 执行以下操作之一：
   - 要创建本地报告概要文件，请单击左侧菜单中“报告”下的**本地报告概要文件**
   - 要创建全局报告概要文件，请单击左侧菜单中“报告”下的**全局报告概要文件**

3. 在工作区中的 “可用报告”列下，单击相应的**查看**链接。

4. 在 “{ 概要文件名称 } 的可用报告”中的**生成自以下日期起的 { 频率 } 报告**下，指定起始的月份、日期和年份。

5. 单击**立即运行**。

根据报告的内容，生成报告可能需要几秒钟。控制管理中心完成报告生成后，该窗口即刷新，而该报告旁边的**查看**链接变为可用。

### 查看生成的报告

除了作为电子邮件附件发送外，您还可以使用“本地报告概要文件”或“全局报告概要文件”窗口查看可用的本地报告或全局报告。

**查看报告：**

1. 在主菜单上单击**报告**。

2. 执行以下操作之一：

   - 要创建本地报告概要文件，请单击左侧菜单中 “报告”下的**本地报告概要文件**
   - 要创建全局报告概要文件，请单击左侧菜单中 “报告”下的**全局报告概要文件**

3. 在工作区中的 “可用报告”列下，单击相应的**查看**链接。

   **在 “{ 概要文件名称 } 的可用报告”中，可以根据提交时间或阶段完成时间将报告排序。**

4. 在 “状态”列下，单击**查看报告**。用于打开该文件格式的缺省程序将打开。

第 8 章

# 常见问题和故障排除资源

本章中的主题：


- *常见问题*（第 8-1 页）
- *故障排除资源*（第 8-5 页）


## 常见问题

### 组件更新

#### 更新代理最多可以管理多少客户机？

数量取决于更新代理的硬件规格。但是，由于防毒墙网络版服务器一次将仅能通知 250 个防毒墙网络版客户机并暂时保持 250 通知队列，预计更新代理将不能同时处理超过 250 个下载进程。

即使在一个更新代理实例上，最大数才为 250 个更新请求。

### 每个防毒墙网络版客户机最多有多少个更新源？

更新源的最大数为1024。可以在 \OfficeScan\PCCSRV 文件夹中的 ous.ini 文件中找到此信息。

### 如果从更新代理更新组件失败，有何其他可选方案？

防毒墙网络版客户机从防毒墙网络版服务器获取更新。如果从防毒墙网络版服务器更新失败，则具有权限的客户机可以从 ActiveUpdate 服务器获取更新。

## 服务器管理

### 为避免 Microsoft Exchange 和防毒墙群件版 for Microsoft Exchange 的操作产生问题，应将那些文件和文件夹添加至扫描例外列表？

对于 Microsoft Exchange 2000/2003，无需将文件夹添加到扫描例外列表。只需转到**联网计算机 > 全局客户机设置 > 病毒 / 恶意软件扫描设置**，然后选择**从扫描中排除 Microsoft Exchange 服务器文件夹**。

如果您使用 Microsoft Exchange 2007，请参考以下页面以获取扫描例外的详细信息：

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

对于防毒墙群件版 for Microsoft Exchange，将排除对所有防毒墙群件版 for Microsoft Exchange 版本 （除版本 7）的扫描。您无需将这些版本的文件夹手动添加到例外列表。

如果使用版本 7，则将以下文件夹添加到例外列表：

- \Smex\Temp
- \Smex\Storage
- \Smex\ShareResPool\

### 将多个标准服务器迁移到防毒墙网络版服务器时，防毒墙网络版是否允许迁移 ServerProtect for Microsoft Windows 的设置？

注意：在此发布版中，在迁移过程中，防毒墙网络版服务器继承了 ServerProtect 密钥功能，比如多个预设扫描和设置。

### 如何禁用安全套接层 (SSL)？

1. 删除虚拟目录或缺省 Web 站点上的 OfficeScan 文件夹。
2. 打开一个命令提示符，然后转到 PCCSRV 文件夹。
3. 键入以下命令：svrinst -setvirdir -disablessl
4. 打开 Internet Information Services (IIS) 控制台，然后验证是否已重新创建了 OfficeScan 虚拟目录。
5. 右键单击 OfficeScan 站点或文件夹。
   - 如果已在独立虚拟站点上安装了防毒墙网络版，则移除表示 SSL 端口的端口 4343。
   - 如果防毒墙网络版安装在缺省 Web 站点下，则移除端口 443。
6. 保存更改。
7. 更改**开始**菜单中的防毒墙网络版链接。
   a. 转到 PCCSRV 文件夹。
   b. 查找带有 Internet Explorer 图标的文件 （除自述文件外）。
   c. 检查 **Web 文档**选项卡下的属性。
   d. 如下更改 URL。
      - 如果在缺省 Web 站点下安装：http://{ 服务器名称 }/officescan

- 如果在其他 Web 站点下安装：http://{ 服务器名称 }:8080/officescan

8. 启动防毒墙网络版 Web 控制台来验证是否已禁用 SSL。

### 防毒墙网络版服务器对 CodeBase 6.5 进行写入或读取操作时，是否提供认证？

注意：dbserver.exe 进程是唯一和 CodeBase 数据库交互的防毒墙网络版组件。它仅访问数据库，因此无需提供用户名和密码。

收到防毒墙网络版客户机的信息（例如组件版本）时，防毒墙网络版服务器向 Dbserver.exe 发送信息。然后 Dbserver.exe 修改数据库中的客户机记录以反映该客户机的组件信息。

### 部署新防火墙概要文件时，如何防止覆盖防毒墙网络版客户机例外列表？

打开 Web 控制台，然后转到**联网计算机 > 防火墙 > 概要文件**。在该窗口中，确保禁用**覆盖客户机安全等级 / 例外列表**选项。

## 客户机管理

### 什么是脱机和非活动的客户机？

脱机的客户机和防毒墙网络版服务器之间没有功能连接。发生此情况的原因有多种，例如计算机未插电、损坏、移动或关闭。

如果计算机在特定天数内保持脱机，则客户机状态变为“非活动”。要确定此天数，请打开 Web 控制台，然后转到**管理 > 非活动客户机**。

### 调试日志

**如何启用防毒墙网络版服务器和客户机的调试日志记录？**

请参考*防毒墙网络版服务器日志*（第 8-5 页）和*防毒墙网络版客户机日志*（第 8-12 页）。

## 故障排除资源

此部分向您提供可以用于解决防毒墙网络版服务器和客户机问题的资源列表。

请参考服务器的联机帮助的故障排除部分以获取对您可能遇到的防毒墙网络版问题的解决方法。联机帮助中提供的某些解决方法可将您引导到趋势科技的知识库。请确保您连接到 Internet，以打开知识库。

### 情况诊断工具

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

要获得此工具及相关文档，请联系您的技术支持提供商。

### 防毒墙网络版服务器日志

除了 Web 控制台上可以使用的日志外，还可以使用其他类型的日志（如调试日志）来解决产品问题。

---

**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，则移除日志文件。*

---

部分防毒墙网络版服务器日志如下：


- *使用 LogServer.exe 调试日志*（第 8-6 页）
- *本地安装 / 升级日志*（第 8-8 页）
- *远程安装 / 升级日志*（第 8-8 页）
- *组件更新日志*（第 8-8 页）
- *客户机打包程序日志*（第 8-9 页）
- *ServerProtect 标准服务器迁移工具调试日志*（第 8-9 页）
- *VSEncrypt 调试日志*（第 8-10 页）
- *控制管理中心 MCP 代理调试日志*（第 8-10 页）
- *病毒扫描引擎调试日志*（第 8-11 页）


## 使用 LogServer.exe 调试日志

**启用防毒墙网络版服务器、趋势科技漏洞扫描程序和策略服务器的调试日志记录：**

1. 登录到 Web 控制台。
2. 在 Web 控制台的标题中，单击 “MICRO” 中的 “C”。
3. 指定调试日志设置，然后单击**保存**。缺省文件名称为 ofcdebug.log。
4. 检查以下缺省位置中的日志文件：\PCCSRV\Log。

**禁用防毒墙网络版服务器、趋势科技漏洞扫描程序和策略服务器的调试日志记录：**

1. 登录到 Web 控制台。
2. 在 Web 控制台的标题中，在 “防”与 “毒”之间单击。
3. 取消选中**启用调试日志**，然后单击**保存**。

**启用服务器安装和升级的调试日志记录：**

可以在执行以下任务前启用调试日志记录：

- 卸装然后再次安装服务器。
- 将防毒墙网络版 8.0 升级到新版本。
- 执行远程安装 / 升级 （启动安装程序的计算机上启用了调试日志记录，且远程计算机上没有启用。）

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

   [debug]

   DebugLevel=9

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

### 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：**\PCCSRV\Web\Service\AU_Data\AU_Log

**获取服务器更新的详细信息：**

1. 创建名为 aucfg.ini 且具有以下内容的文件：

   [Debug]

   level=-1

   [Downloader]

   ProxyCache=0

2. 将文件保存到 \PCCSRV\Web\Service。

3. 重新启动防毒墙网络版主服务。

**停止收集服务器更新的详细信息：**

1. 删除 aucfg.ini。
2. 重新启动防毒墙网络版主服务。

### 客户机打包程序日志

**启用客户机打包程序创建的日志记录：**

1. 如下修改 \PCCSRV\Admin\Utility\ClientPackager 中的 ClnExtor.ini：

   [Common]

   DebugMode=3

2. 检查 C:\ 中的 ClnPack.log。

**禁用客户机打包程序创建的日志记录：**

打开 ClnExtor.ini 然后将 “DebugMode”值从 3 更改为 0。

### ServerProtect 标准服务器迁移工具调试日志

**启用 ServerProtect 标准服务器迁移工具的调试日志记录：**

1. 创建名为 ofcdebug.ini 且具有以下内容的文件：

   [Debug]

   DebugLog=C:\ofcdebug.log

   DebugLevel=9

2. 将文件保存到 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记录：

删除 ofcdebug.ini。

### VSEncrypt 调试日志

防毒墙网络版在用户帐户的临时文件夹中自动创建调试日志 (VSEncrypt.log)。例如， C:\Documents and Settings\{ 用户名 }\Local Settings\Temp。

### 控制管理中心 MCP 代理调试日志

在防毒墙网络版服务器 \PCCSRV\CMAgent 文件夹中的调试文件：

- Agent.ini
- Product.ini
- “控制管理中心设置”页的屏幕截图
- ProductUI.zip

启用 MCP 代理的调试日志记录：

1. 如下修改 PCCSRV\CmAgent 中的 product.ini：

   [Debug]

   debugmode = 3

   debuglevel= 3

   debugtype = 0

   debugsize = 10000

   debuglog = C:\CMAgent_debug.log

2. 从 “Windows 服务”窗口中重新启动 OfficeScan Control Manager Agent 服务。
3. 检查 C:\ 中的 CMAgent_debug.log。

**禁用 MCP 代理的调试日志记录：**

1. 打开 product.ini 然后删除以下内容：

   debugmode = 3

   debuglevel= 3

   debugtype = 0

   debugsize = 10000

   debuglog = C:\CMAgent_debug.log

2. 重新启动 OfficeScan Control Manager 服务。

### 病毒扫描引擎调试日志

**启用病毒扫描引擎的调试日志记录：**

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. 执行导致遇到的扫描问题的步骤。
5. 检查 %SystemRoot% 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”。

## 防毒墙网络版客户机日志

可以使用客户机日志 （例如调试日志）来解决客户机问题。

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

部分防毒墙网络版客户机日志如下：

- *使用 LogServer.exe 调试日志*（第 8-13 页）
- *全新安装日志*（第 8-13 页）
- *升级 /Hotfix 日志*（第 8-14 页）
- *损害清除服务调试日志*（第 8-14 页）
- *邮件扫描日志*（第 8-15 页）
- *客户机连接日志*（第 8-15 页）
- *客户机更新日志*（第 8-15 页）
- *爆发阻止调试日志*（第 8-16 页）
- *防毒墙网络版防火墙调试日志*（第 8-16 页）
- *Web 站点信誉调试日志*（第 8-17 页）
- *传输驱动接口 (TDI) 调试日志*（第 8-18 页）

### 使用 LogServer.exe 调试日志

**启用防毒墙网络版客户机的调试日志记录：**

1. 创建名为 ofcdebug.ini 且具有以下内容的文件：

   [Debug]

   Debuglog=C:\ofcdebug.log

   debuglevel=9

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1

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

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

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

**禁用防毒墙网络版客户机的调试日志记录：**

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：**\OfficeScan Client\Temp

### 损害清除服务调试日志

**启用损害清除服务的调试日志记录：**

1. 打开 \OfficeScan Client 中的 TSC.ini。
2. 如下所示修改以下行：DebugInfoLevel=3
3. 检查 \OfficeScan Client\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” 值从 3 更改为 0。

### 邮件扫描日志

**文件名：**SmolDbg.txt

**位置：**\OfficeScan Client

### 客户机连接日志

**文件名：**Conn_YYYYMMDD.log

**位置：**\OfficeScan Client\ConnLog

### 客户机更新日志

**文件名：**Tmudump.txt

**位置：**\OfficeScan Client\AU_Data\AU_Log

**获取客户机更新的详细信息：**

1. 创建名为 aucfg.ini 且具有以下内容的文件：

   [Debug]

   level=-1

   [Downloader]

   ProxyCache=0

2. 将文件保存到 \OfficeScan Client。
3. 重新加载客户机。

**停止收集客户机更新的详细信息：**

1. 删除 aucfg.ini。
2. 重新加载客户机。

### 爆发阻止调试日志

**文件名：**OPPLogs.log

**位置：**\OfficeScan Client\OppLog

### 防毒墙网络版防火墙调试日志

**启用通用防火墙驱动程序的调试日志记录：**

1. 在 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmcfw\Parameters 中添加以下数据：

   **类型：**DWORD 值 (REG_DWORD)

   **名称：**DebugCtrl

   **值：**0x111

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的调试日志记录：**

1. 删除注册表键中的 “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记录：**

1. 创建名为 Tmpfw.ini 且具有以下内容的文件：

   ```
   [debug]
   debug_on=yes
   debug_level=90
   log_path=C:\TmPfw.log
   ```

2. 将文件保存到 \OfficeScan Client。
3. 重新加载客户机。
4. 检查 C:\ 中的 TmPfw.log。

**禁用防毒墙网络版 NT 防火墙服务的调试日志记录：**

1. 打开 Tmpfw.ini 然后将“debug_on”的值从“yes”更改为“no”。
2. 重新加载客户机。

### Web 站点信誉调试日志

**启用 Web 站点信誉功能组件的调试日志记录：**

1. 如下所示编辑位于 \OfficeScan Client 中的 TmProxy.ini：

   ```
   [debug]
   debug_on=yes
   debug_level=90
   log_path=C:\TmProxy.log
   ```

2. 重新加载客户机。
3. 检查 C:\ 中的 TmProxy.log。

**禁用 Web 站点信誉功能组件的调试日志记录：**

1. 打开 TmProxy.ini 然后将 “debug_on”的值从 “yes”更改为 “no”。
2. 重新加载客户机。

### 传输驱动接口 (TDI) 调试日志

**启用 TDI 的调试日志记录：**

1. 在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters 中添加以下数据：

   **类型：**DWORD 值 (REG_DWORD)

   **名称：**Debug

   **值：**1111 （十六进制）

   **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. 删除注册表键中的 “Debug”和 “LogFile”。
2. 重新启动计算机。

第 9 章

# 与趋势科技联系

本章中的主题：


- *技术支持*（第 9-1 页）
- *趋势科技知识库*（第 9-3 页）
- *TrendLabs*（第 9-3 页）
- *安全信息中心*（第 9-4 页）
- *将可疑文件发送给趋势科技*（第 9-4 页）
- *文档反馈*（第 9-5 页）


## 技术支持

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

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

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

在中国，您可以通过电话、传真或电子邮件与趋势科技销售代表取得联系。

趋势网络科技 （中国）有限公司

上海市淮海中路 398 号世纪巴士大厦 8 楼

免费咨询电话：800-820-8876(021-63848622)

技术支持热线：800-820-8839(021-6100-6656)

传真：86-21-6384 1899

Web 地址：www.trendmicro.com.cn

电子邮件：service@trendmicro.com.cn

## 加速您的支持呼叫

联系趋势科技时，为加快问题解决的速度，请确保您可以提供以下详细信息：

- Microsoft Windows 和 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://www.trendmicro.com/cn/support

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

## TrendLabs

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

您可以信赖以下售后服务：

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

TrendLabs 已获得 ISO 9002 质量体系认证。

## 安全信息中心

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

可用信息：

- 当前正在传播或活动的病毒和恶意传播代码列表
- 计算机病毒谣言
- 互联网威胁预警
- 每周病毒报告
- 包括了已知病毒和恶意传播代码的名称和症状的全面列表的病毒百科全书。
- 术语表

## 将可疑文件发送给趋势科技

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

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

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

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

## 文档反馈

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

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

附录 A

# 使用第三方软件配置防毒墙网络版

本附录中的主题：


- *Check Point 体系结构和配置概述*（第 A-1 页）
- *Check Point for 防毒墙网络版配置*（第 A-4 页）
- *安装 SecureClient 支持*（第 A-5 页）


## 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(TM) SecureClient(TM) 完全集成。阅读此部分前请先熟悉一下 Check Point SecureClient OPSEC 文档。 OPSEC 文档可以在 www.opsec.com 处找到。

Check Point SecureClient 能够使用安全配置验证 (SCV) 检查确定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机系统的一组条件。第三方软件可以将这些条件的值传递给 Check Point SecureClient。Check Point SecureClient 然后可将这些条件与 SCV 文件中的条件相比较以确定客户机是否安全。

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机。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机。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 *Check Point for 防毒墙网络版配置* （第 A-4 页）。

## 防毒墙网络版集成

防毒墙网络版客户机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。SecureClient 然后将这些值与客户机 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，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 不会在 SCV 文件中自动更新病毒码文件号和扫描引擎版本号。无论何时防毒墙网络版更新了扫描引擎或病毒码文件，都需要在 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机的通信，从而为新病毒创造潜入系统的机会。

---

# 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. 从下面的 Check Point 下载站点下载 SCVeditor.exe：
   www.checkpoint.com/techsupport/ng/fp3_updates.html#opsecsdk

   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：** 如果您的 local.scv 文件已包括其他第三方软件的产品策略，则请通过单击**编辑 > 产品 > 添加**，然后在**添加**框内键入 **OfceSCV** 来创建新策略。

5. 现在添加五个参数。要添加一个参数，请单击**编辑 > 参数 > 添加**，然后在相应的框内键入**名称**和**值**。表 A-1 列出了参数的名称和值。参数的名称和值区分大小写，必须以表 A-1 中给定的顺序键入它们。

**表 A-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 } |

**表 A-1. SCV 文件参数的名称和值**

| 名称 | 值 |
|---|---|
| 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表 A-1 中花括号内的文本。可以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机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

如果有从专用虚拟网络 (VPN) 连接到办公室网络的用户，且他们的计算机上都同时安装了 Check Point SecureClient 和防毒墙网络版客户机，则可以要求他们安装 SecureClient 支持。此模块允许 SecureClient 在 VPN 客户机上执行 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是否有 图标或 Windows 的**添加或删除程序**窗口上是否有名为 **Check Point SecureClient** 的项来验证他们的计算机上是否安装有 Check Point SecureClient。

安装 SecureClient 支持：

1. 打开客户机控制台。
2. 单击**工具箱**选项卡。
3. 在 **Check Point SecureClient 支持**下，单击**安装 / 升级 SecureClient 支持**。将显示确定窗口。
4. 单击**是**。客户机将连接到服务器，并且还将下载模块。下载完成时，将显示 “注册防毒墙网络版 SCV” 的消息。
5. 单击**确定**。

# 词汇表

## 术语与定义

| 术语 | 描述 |
| --- | --- |
| HTTPS | 使用安全套接层 (SSL) 的超文本传输协议。 |
| Internet 控制消息协议 (Internet Control Message Protocol, ICMP) | 偶尔网关或目标主机会使用 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。 |
| Ping | 向 IP 地址发送 ICMP 回显请求并等待响应的实用工具。Ping 实用工具可以确定带有特定 IP 地址的计算机是否联机。 |

| 术语 | 描述 |
| --- | --- |
| SOCKS 4 | 一种 TCP 协议，由代理服务器用来在内部网络上的客户机之间或在 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 证书 | 建立安全 HTTPS 通信的数字证书 |
| Telnet | Telnet 是通过创建 “网络虚拟终端” 通过 TCP 进行终端设备交互的标准方法。有关详细信息，请参考 “Network Working Group RFC 854”。 |
| 安全套接层 (Secure Socket Layer, SSL) | SSL 是由 Netscape Communications Corporation 提议的方案，该方案使用 RSA 公共密钥密码系统加密和认证根据更高级别协议 （如 HTTP、 NNTP 和 FTP）传输的内容。 |
| 超文本传输协议 (Hyper Text Transfer Protocol, HTTP) | 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机的标准协议。 |
| 传输控制协议 (Transmission Control Protocol, TCP) | 连接导向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 依赖于地址解析的 IP 数据报。有关信息，请参考 “DARPA Internet Program RFC 793”。 |
| 动态 IP 地址 (Dynamic IP Address, DIP) | 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 可以根据可用资源为计算机分配新的 IP 地址。 |
| 动态主机控制协议 (Dynamic Host Control Protocol, DHCP) | 设备 （如计算机或交换机）必须有一个 IP 地址才能连接到网络，但是该地址不必为静态地址。DHCP 服务器使用动态主机控制协议，可以在每次设备连接到网络上时动态分配和管理 IP 地址。 |

| 术语 | 描述 |
| --- | --- |
| 文件传输协议 (File Transfer Protocol, FTP) | FTP 是用于将文件通过 Internet 从服务器传输到客户机的标准协议。有关详细信息，请参考“Network Working Group RFC 959”。 |
| 因特网协议 (Internet Protocol, IP) | “因特网协议规定了将数据块（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标识的主机。”(RFC 791) |
| 用户数据报协议 (User Datagram Protocol, UDP) | 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”。 |
| 最终用户授权和约书 (End User License Agreement, EULA) | 最终用户授权合约书或 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。<br>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。 |