

趋势科技

防毒墙网络版 Officescan 8.0

产品安装标准程序



趋势科技技术支持部

2007-07





1 OFFICESCAN 是如何保护您的网络的	
2. OFFICESCAN 的系统需求	6
2.1 OFFICESCAN 服务器端	6
2.2 OFFICESCAN 客户端	7
3. 安装前的准备工作	10
4. 标准安装过程	19
4.1 OFFICESCAN 服务器端安装	19
4.2 OFFICES 客户端安装	
4.3 如何检查安装是否成功	
4.3.1 服务器端	
4.3.2 客户端	35
5. 升级安装过程	40
5.1 升级前的注意事项	40
5.2 升级前的备份	
5.3 升级安装	41
6. OFFICESCAN 控制台管理	45
7. 更新	50
7.1 服务器端的更新	
7.2 客户端的更新	
8. 趋势科技厂商资源	54



防毒墙网络版 Officescan 8.0



今天,网络安全是一个所有IT管理员格外关注的问题,网络安全最主要的目的是阻止不被允许的链接进入网络以此来减少数据损坏,窃取数据,和对系统造成危险。

但是很不幸,很多时候不被允许的链接只是在 一个威胁发布后才能被检测到。因而,在访问控制

的机制之外,IT管理员必须用用工具并且设定策略去监控活跃的网络资产,早早的检测网络威胁,并且能尽快的对潜在的威胁做出相应。

officescan 8.0为服务器和客户端系统提供了一个广阔的安全保护。

趋势科技防毒墙网络版(OfficeScanTM)是用于台式机和笔记本计算机的集中式管理防病毒和防间谍软件解决方案。防毒墙网络版保护您的

WindowsNT/2000/XP/Server 2003 和 Windows 95/98/Me 计算机免受病毒、恶意代码 (包括文件型病毒、宏病毒以及恶意 Java 小程序和 ActiveX 控件),间谍软件和 灰色软件文件以及程序的侵害。通过提供单一控制台使管理员可以配置、监控和维护 台式机的防毒病措施,防毒墙网络版改进并简化了企业病毒策略和管理。

1 officescan 是如何保护您的网络的

OfficeScan 在体系结构上分为两个部分:

OfficeScan 服务器——管理端程序,这是防毒墙软件的大脑,通过Web 管理控制台您可以:

- 部署客户端程序到客户机
- 对客户机进行设置和管理
- 更新客户端防毒软件和病毒码
- 设置客户端的扫描设置和调用客户机的扫描工作。
- 接收来自客户端机器的状态信息并查看防毒活动的日志报告。
- 接收在网络上的中毒通知和中毒警报,以及报警。
- 部署病毒防范策略等等...

OfficeScan 客户端——防毒端,安装在每一台被保护的机器上,实现病毒查杀动作。下图是一个办公网络环境中部署防毒墙的实例,仅供参考:



图1-1 officescan部署实例

在网络中找一台服务器安装上OfficeScan 服务器端程序实现管理功能,在客户机上安装OfficeScan 客户端程序实现病毒防杀任务。

什么样的计算机可以安装OfficeScan 服务器端程序? 请查看[OfficeScan服 务器系统需求]。

什么样的计算机可以安装OfficeScan 客户端程序? 请查看[OfficeScan 客 户端系统需求]



2. Officescan 的系统需求

2.1 officescan 服务器端

你准备安装officescan服务器端的服务器一点要满足最低的系统需求,软件安装也需要你具有本地或者域管理员的权限.

硬件需求

- 800MHZ intel pentium II处理器
- 512兆内存
- 1G的磁盘空间

软件需求

操作系统

- Microsoft Windows 2000 Server or Advanced Server with Service Pack 3 or 4
- Microsoft Windows Server 2003 32-bit or 64-bit Edition or Service Pack
 1
- Microsoft Windows Server 2003 R2 32-bit or 64-bit Edition
- Microsoft Windows Storage Server 2003 32-bit or 64-bit Edition
- Microsoft Cluster Server 2000 or 2003

web服务器

- Microsoft IIS
 - 5.0 or higher (Service Pack 3 or 4) for Windows 20006.0 or higher for Windows 2003
- Apache 2.0 or later (for Windows 2000/Server 2003 only)
 如果在存在的Apache 2.0X服务器上使用SSL,你必须在安装officescan之前

把Apache配置成支持SSL



如果Apache没有安装, officescan安装程序会自动安装Apache 2.0.59并且会 配置Apache支持SSL如果你在安装的时候运用了SSL 如果你想要用officescan安装程序来升级你的Apache服务器, 那你必须先卸 载存在的Apache程序, 然后使用officescan安装程序 officescan管理控制台web浏览器

• Microsoft Internet Explorer 5.5 Service Pack 1 or higher

2.2 officescan 客户端

OfficeScan Client for Windows 2000

操作系统::

- $\bullet~$ Microsoft Windows 2000 with Service Pack (SP) 3 or 4
- Microsoft Cluster Server 2000

硬件需求:

- 300 MHz Intel Pentium processor or equivalent
- 128 MB 以上内存
- 160 MB 以上可用空间

Web浏览器

• Microsoft Internet Explorer 5.0以上,

OfficeScan Client for Windows XP/Server 2003 32-bit Edition

操作系统:

- Microsoft Windows XP Professional 32-bit Edition with SP 1 or 2
- Microsoft Windows Server 2003 32-bit Edition or SP 1
- Microsoft Windows 2003 Web Edition 32-bit Edition or SP 1
- Microsoft Windows Server 2003 R2 32-bit Edition



- Microsoft Windows Storage Server 2003 32-bit Edition
- Microsoft Cluster Server 2003

硬件需求:

- 300 MHz Intel Pentium处理器或者AMD x64 or Extended Memory 64 technology (EM64T) 处理器
- 128 MB 以上内存
- 160 MB 以上可用空间

Web浏览器

• Microsoft Internet Explorer 6.0 or later, if performing web-based setup

OfficeScan Client for Windows XP/Server 2003 64-bit Edition

操作系统:

- Microsoft Windows XP Professional 64-bit Edition with SP 1 or 2
- Microsoft Windows Server 2003 64-bit Edition or SP 1
- Microsoft Windows 2003 Web Edition 64-bit Edition or SP 1
- Microsoft Windows Server 2003 R2 64-bit Edition
- Microsoft Windows Storage Server 2003 64-bit Edition
- Microsoft Cluster Server 2003

硬件需求:

- Intel x64 processor, AMD x64 processor
- 128 MB of RAM
- 160 MB of available disk space

Web浏览器

• Microsoft Internet Explorer 6.0 or later, if performing web-based setup

OfficeScan Client for Windows Vista

操作系统:

- Microsoft Windows Vista Business 32-bit and 64-bit Editions
- Microsoft Windows Vista Enterprise 32-bit and 64-bit Editions
- Microsoft Windows Vista Ultimate 32-bit and 64-bit Editions

硬件需求:

- 800 MHz Intel Pentium processor or equivalent; or AMD x64 or Extended Memory 64 Technology (EM64T) processor
- 512 MB of RAM
- 160 MB of available disk space

Web浏览器

• Microsoft Internet Explorer 7.0 or later, if performing web-based setup



3. 安装前的准备工作

● 准备工作一:

如果您还没有安装好用做安装OfficeScan 服务器端程序的计算机,请先找一 台服务器安装上WindowsNT Server、Windows 2000、 Windows XP 或 Windows Server 2003。

注意:记得检查配置要符合上面所说的最低系统要求,操作系统请打上微软最新发布的补丁。如何安装操作系统,就不赘述了,请参考其它相关文档吧! 建议不要将OfficeScan服务端安装在Windows域控制器上,如果一定需要安装请做 好域控制器的备份工作。

● 准备工作二:

安装前,请先确认是要安装在IIS 上还是安装在Apache Web Server 上(仅 限于Windows 2000/XP[Service pack 1 或更新版本]/Server 2003):

如果您的服务器上没有安装IIS,并且操作系统符合上述需求,您可以选择 使用 Apache Web Server,在安装的过程中,Officescan 会提示您并自动为您 安装。

安装在IIS 上:

建议:如果您想要在IIS 上安装0SCE 管理台的话,请尽量使用干净的IIS 环境,尽量避免和别的web 服务共享一个IIS ,便于出现问题时的查错。

提醒: 在默认环境下,已经安装了IIS 的系统: Windows 2000 Server 默认没有安装IIS 的系统: Windows 2000 Pro, Windows XP, Windows Server

可信赖的网络安全专家

2003

TREND MICRO™ 趋势科技

小知识:

什么是IIS,为什么需要IIS 呢?

IIS 是Internet Information Server 的缩写,它是微软公司主推的Web 服务器, 最新的版本是Windows2003 里面包含的IIS 6.0, IIS 与Window Server 完全集成 在一起,因而用户能够利用Windows Server 和NTFS (NT File System, NT 的文 件系统)内置的安全特性,建立强大、灵活而安全的Internet 和Intranet 站点。 IIS 的一个重要特性是可以很容易的张贴动态内容和开发基于Web 的应用程序。 IIS 的安装,管理和配置都相当简单。有了IIS 我们才可以通过Web 的方式对 OfficeScan 进行配置管理。

什么是Apache Web Server?

Apache 同IIS 一样,也是非常流行的web 服务器,可以用来提供HTTP 访问的服 务。

怎么检查我的IIS 是否正常工作呢? 请按照如下说明操作:

➤ 如何检查我的IIS 是否已经安装并正常工作? 点击:[开始]->[运行],输入inetmgr 命令



可信赖的网络安全专家

防毒墙网络版 Officescan 8.0



图3-01 打开IIS 控制台运行命令

查看到以下显示信息

🦉 Internet 信息服务(IIS)官	「理番」	
ý 文件(E) 操作(A) 查看(V) 窗口(W) 帮助(H)	
← → 🗈 🔟 🗗 🔂	😫 🖳 🕨 🔳 💷	
衛 Internet 信息服务	名称	路径
🗄 뤬 CN-APPLESHEN-0 (本地汁)	🔯 activeupdate	E:\Program Files\Trend Micro
🗄 🎒 FTP 站点	🔯 Exadmin	\\.\BackOfficeStorage
🖻 🎒 应用程序池	🤯 Exchange	\\.\BackOfficeStorage\sy.net
日日日	🧟 ExchWeb	E:\Program Files\Exchsrvr\Ex
(🖂 😫 默认网站)	nicrosoft-Server-Active	E:\Program Files\Exchsrvr\OM
🛨 🐼 activerpdste	de coma 🛃 🔔	E:\Program Files\Exchsrvr\OM
🛨 📢 Exadmin	a Yublic	<pre>\\. \BackUtticeStorage\sy.net</pre>
+ Schange	📁 aspnet_client	
± KrchWeb	📄 iisstart.htm	
H Microsoft-Se	pagerror.gif	
🔰 🕴 👘 👘 Public		

图3-02 Windows 2003 IIS 控制台图例

在IE 浏览器中输入HTTP://127.0.0.1 查看是否能显示以下画面,如果默认站 点不正常则显示"该页无法显示"

TRE MIC 趋势	ND Ro [™] 可 科技	信赖的网络安全专家	防毒墙网络版 Officescan 8.0
ē	建设中	- Di <mark>cros</mark> oft Internet Explorer	
	文件 (2)	编辑(E) 查看(Y) 收藏(A) 工具(E) 帮	助(ਮ)
Q	〕后退 •	- 🕗 - 🗵 💈 🚮 🔎 搜索 🎲 收藏夹 📢	8 🔊 - 📚 🗖 🔟
ŧ	地址 (12) 🧕	http://127.0.0.1/	
	i	建设中	
		┘ 您想要查看的站点当前没有默认贝。可能正	三在对它进行升级和配置操作。
		请稍后再访问此站点。如果您仍然遇到问题	见,请与网站的管理员联系。
		如果您是网站的管理员,并且认为您是由于 帮助中的"启用和禁用动态内容"。	⁻错误才收到此消息,诸参阅 IIS
		要访问 115 希明	
		 单击开始,然后单击运行。 在打开文本框中,键入 inetegr。 从帮助菜单,单击帮助主题。 单击Internet 信息服务。 	将出现 IIS 管理器。

图3-03 IIS 成功安装

如果您必须重新安装IIS 的话,也不难,请准备好您的操作系统安装光盘, 按如下步骤操作即可:

▶Windows 下如何安装IIS?

Windows 下安装IIS 的方法是,插入Windows 安装盘,点击"开始→设置 →控制面板→添加/删除程序→添加/删除Windows 组件",

■ Windows 2000 会出现下图,把IIS 打上勾就可以了:



防毒墙网络版	Officescan	8.0
--------	------------	-----

┓添加/劃	余程序	<u>-0×</u>
12	目前安装的程序:	排序方式 (S): 名称
更改或删除	Windows 組件向导	
	▼indows 組件 可以添加或删除 Windows 2000 的组件。	
派 加/删除 Windows 組	要添加或删除某个组件,请单击旁边的复选框 一部分。要查看组件内容,请单击"详细信息 组件 (2):	。 灰色框表示只会安装该组件的 ●
n madon s <u>se</u>	☑ 🚰 Internet 信息服务(IIS)	18.3 MB
	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
		0.0 MB
	□	rontPage、事务处理、ASP、数
	所需磁盘空间: 20.0 MB 可用磁盘空间: 1955.3 MB	详细信息 (1)
	<u><上-</u>	→步(12) 下一步(12) 〉 取消

图3-04 Windows 2000 IIS 组件添加

■ Window	vs 2003 会出现下图,先点选详细信息,然后再选择IIS:
🛃 添加或删除	程序
夏改或 更改或 删除 程序(tí)	当前安装的程序·
添加新 程序 创	 要添加或删除某个组件, 请单击旁边的复选框。灰色框表示只会安装该组件的一部分。要查看组件内容, 请单击"详细信息"。 组件 (2):
添加/删除 Windows 组件(A)	● ● ● ● ●<
	 描述: 包括 ASP. FET, Internet 信息服务(IIS)和应用程序服务器控制 台。 新需磁盘空间: 3.4 MB 可用磁盘空间: 15122.1 MB 第细信息 @)
	上一步 (B) 下一步 (N) > 取消 帮助 3 1 1

图3-05 Windows 2003 IIS 组件添加

D TREND MICRO 趋势科技	可信赖的网络安全专家	防毒墙	网络版 Officescan 8.0
然后	有2 次提示插入光盘 :		
	Tindows 組件向导		×
	正在配置組件 安装程序正在根据您的语	青求进行配置更改。	E
	请稍候,安装积	呈序正在配置组件。所花时间取决于	选定的组件。
	插入磁盘		×
		indows Server 2003, Enterprise XOM'的光盘插入 CD-ROM 驱动器 显击"确定"。 •个位置(如一个软盘或网络服务器) 见可以单击"确定"。	 取消
	I	< 上一步 (1) 下一步 (1) > 1	2消 帮助

图3-06 提示插入光盘

这时一定要找到I386 这个目录,并且这两次都需要你重新查找路径,一路确定就安装完毕了!

安装完毕,依照上述方法检查是否安装成功!

● 准备工作三:

如果您的服务器是新安装的操作系统,可跳过准备工作三!

▶ 检查服务器上RPC 服务以及远程注册服务是否已经打开,若没有,请将其 打开。

操作步骤:点击[开始] [程序] [管理工具] [服务],弹出服务配 置对话框,如图圈起来的服务请开启,状态会显示"已启动"; 若状态显示没有"已启动"字样,请用鼠标点亮该服务,点击右键,按"启 动"。



防毒墙网络版 Officescan 8.0

检查C\$, ADMIN\$默认共享是否打开?若没有,请将其打开。 操作步骤:[开始] [运行] cmd,进入命令行模式,输入net share 命令,如果没有显示如图C\$和ADMIN\$行,请运行这两条命令:

net start C=c:

可信赖的网络安全专家

net start ADMIN\$

³⁴ 2 服务					
」操作(<u>A</u>) 查看	f(y)] ← → 🖮 💽 🖀 🔂	😫 ▶ ■ ॥ ■>			
树	名称 🔺	描述	状态	启动类别	登录身份 ▲
《》 服务(本地)	NT LM Security Support Provider	为使用传输协议而不是命名管道的远	已启动	手动	LocalSystem
343 (1005) (1 CD)	🖏 OfficeScan Master Service		已启动	自动	LocalSystem
	Reformance Logs and Alerts	配置性能日志和警报。		手动	LocalSystem
	🆓 Plug and Play	管理设备安装以及配置,并且通知程…	已启动	自动	LocalSystem
	Redia Serial Number Service	Retrieves the serial number of any portah		手动	LocalSystem
	Rint Spooler	将文件加载到内存中以便迟后打印。	已启动	自动	LocalSystem
	Rotected Storage	提供对敏感数据(如私钥)的保护性存储	已启动	自动	LocalSystem
	RSVP QoS RSVP	为依赖质量服务(QoS)的程序和控制应		手动	LocalSystem
	Remote Access Auto Connection Mana	无论什么时候当某个程序引用一个远		手动	LocalSystem
	Remote Access Connection Manager	创建网络连接。	已启动	手动	LocalSystem
	Remote Administrator Service		已启动	自动	LocalSystem
	Remote Procedure Call (RPC)	提供终结点映射程序 (endpoint mapper)	已启动	自动	LocalSystem
	Remote Procedure Call (RPC) Locator	管理 RPC 名称服务数据库。	已启动	自动	LocalSystem
	Remote Registry Service	允许远程注册表操作。	已启动	自动	LocalSystem
	Removable Storage	曾理可移动媒体、驱动程序和库。	巳启动	自动	LocalSystem
	Routing and Remote Access	在局域网以及广域网环境中为企业提		已禁用	LocalSystem 💳
	RunAs Service	在不同凭据下启用启动过程	已启动	自动	LocalSystem
	ScanMail_MailAction		已启动	自动	LocalSystem
	🖏 ScanMail_Monitor		已启动	自动	LocalSystem
	🖏 ScanMail_RealTimeScan		已启动	自动	LocalSystem
	🖏 ScanMail_Web		已启动	自动	LocalSystem
	Security Accounts Manager	存储本地用户帐户的安全信息。	已启动	自动	LocalSystem 🚽
	J <i>8</i> 9. –			μ−τ	

图3-07 安装OfficeScan 服务端需要打开的服务

检查C\$, ADMIN\$默认共享是否打开?若没有,请将其打开。 操作步骤: [开始]-[运行]-cmd,进入命令行模式,输入net share 命令, 如果没有显示如图C\$和ADMIN\$行,请运行这两条命令: net start C\$=c:

net start ADMIN\$



防毒墙网络版 Officescan 8.0

E: \TIBDOT	S\systen32\cnd.exe		
Microsoft (C) 版权所	Windows L版本 5.2.379k 有 1985-2003 Microsoft	J Corp.	<u> </u>
E:\Documen	ts and Settings Admini	strator>net share	
共享名	资源	注释	
 C\$	C:\		
E\$	E:N	默认共享	
D\$	D: \	默认共享	
ADMIN\$	E: WINDOWS	远程管理	
G\$	G: \	默认共享	
F\$	F: N	默认共享	
I PC\$		远程 IPC	

图3-08 检查共享情况

● 准备工作四:

安装前请将服务器连入网络,分配合适的IP 地址,你可以使用ipconfig 命令 查看当前的IP 地址是否已经分配。

● 准备工作五:

如果您的服务器不是新装的,尤其是针对曾经感染过病毒的服务器,强烈建议 您在安装产品之前,先使用工具对系统进行清毒处理。

为什么要进行安装前的病毒扫描?

由于当前病毒入侵系统的手法很多,对文件的感染方式有很多种,并且 很多病毒会恶意修改注册表等重要的系统文件。一旦系统已经感染了病毒, 很可能整个系统的运作已处于非正常状态。在这种情况下进行防毒软件的安 装,很可能软件在安装过程中即遭到病毒的破坏或感染。因此如果您不确定 自己的系统是否感染病毒,强烈建议您在安装产品之前,先使用工具对系统 进行清毒处理。

安装前的系统清毒方法:

▶ 使用在线扫毒方式对计算机进行初步诊断

可以连接到趋势科技网站上的在线扫毒服务对计算机进行病毒检测,以确 定是否感染了病毒。网址为:

http://www.trendmicro.com.cn/housecall 。(如果网址已变更,请至 网站首页查询)

> 然后使用趋势科技提供的TSC 清毒工具或Sysclean 清毒工具对系统 进行清理

这些工具的应用附录有详尽的介绍,去那里看看!

做了充分的准备后,现在开始真正的安装之旅了!还有一点要提醒:请关闭所有的应用程序窗口。



4. 标准安装过程

4.1 officescan 服务器端安装

先来安装防毒墙服务器端程序,请依照下列步骤执安装过程:

(1)到趋势科技网站上下载最新的安装程序,双击可执行文件



图4-1 安装程序自解压



(2)进入欢迎界面,点击下一步,运行安装程序



图4-2 欢迎界面

(3)阅读软件授权合同书,选择我接受授权合约书的条款进入下面的安装步骤

软件授权合约书	
授权合约书 请仔细阅读以下授权合约书…	
重要提示:在安装本软件之前,请仔细阅读下列许可 使用趋势科技软件及服务,均应当遵守下列许可协议 趋势科技许可协议 试用及付费使用许可 对象:公司及小企业软件和服务 日期:2007年5月 v.1 简体中文/中国 1、有约束力的合同。本许可协议(以下称体协议) 司或其授权关联公司(以下称趋势科技)与基于试 软件或服务的法律实体之间成立的具有法律约束力的 ① 我接受授权合约书的条款(A) ① 我接受授权合约书的条款(A)	协议,任何企业或其他实体 中条款及条件 为趋势科技(中国)有限公 用或付费方式使用趋势科技 哈同。在使用本软件或本服 ▼
〈上一步	(B) 下一步(M) > 取消

图4-3 软件授权合同书

● TREND ^{M | C R 0} ^{b → M + C R 0} ^{M | C R 0</sub> ^{M | C R 0} ^{M | C R 0}}}</sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup>

防毒墙网络版 Officescan 8.0

(4)选择安装目标, officescan支持同时在多台计算机上安装officescan服务器端

趋势科技防毒墙网络反	
安装目标	
我将安装/升级防毒墙网络版服务器	
◎ 到远程计算机或多台计算机[[]	
InstallShield	
帮助 〈上一步(B) 下一步(N)	> 取消

图4-4 服务器端安装目标机器

(5)选择是否进行安装前的扫描,推荐在安装officescan之前对机器进行扫描

趋势科技防毒墙网络版				
计算机预扫描				
安装程序可以在安装产品之 目标计算机吗 ?	前扫描目标	计算机中是否很	存在安全风险。	您要安装程序扫描
• 封描目标计算机(S)				
○ 不扫描目标计算机(D)				
InstallShield				
	帮助	<上→歩	B) 下一步(N)	> 取消

图4-5 是否扫描机器



(6)进行损害清除服务

趋势科技防毒墙网络版	
安装状态 2 天王N	D.
在安装 防毒墙网络版 之前,安装程序正在扫描系统和程序目录中有无安全风险。请 稍候…	
正在执行损害清除服务	
Install9hield	

图4-6 执行损害清除服务

(7)选择officescan服务器端的安装路径

趋势科技防毒墙网络反	
安装路径	
诸指定防毒墙网络版安装路径。您可以键	入一个新的文件夹名称或浏览到所需位置。
C:\Program Files\Trend Micro\OfficeScan	
	浏览 <u>旧</u>)
Install@kinld	
	<上一步(B) 下一步(N)> 取消

图4-7 选择服务器端安装路径



(8)进行代理服务器的设置

趋	势科技防毒墙网络版		
	代理服务器		
	如果使用代理服务器访问 趋势科技更新服务器下载。	Internet,请在下面指定代理服务器 更新时使用此信息。	设置。防毒墙网络版将在从
	代理服务器设置 ↓ 使用代理服务器(U) 代理服务器类型:	C HTTP(H) C SOCKS	4(<u>5)</u>
	服务器名称或 IP 地址:		
	端口:		
	认证(可选):	用户名:	
		密码:	
Ins	tallShield ———		
		帮助 <上一步(B) -	下一步(1)> 取消

图4-8 设置代理服务器

(9)选择安装的web服务器,如果机器没有安装IIS,officescan将帮您安装最新的

趋势科技防毒墙网络)	扳	×
Web 服务器		
诸选择防毒墙网络 ;	版服务器使用的 Web 服务器。	
C 116 服务器()		IIS 虚拟 Web 站点 📃 💌
④ Apache Web 服	务器 2.0(如果尚未安装则安装)(A)	
HTTP端口:	8080	
☑ 启用 SSL(E)		
证书验证期:	3	年
SSL端口:	4343	
InstallShield		·
	帮助<上→步區	2) 下一步(N) > 取消

apache web server

图4-9 选择安装的WEB SERVER



(10)选择服务器和客户机进行通信的标示,包括IP地址和机器名

趋势科技防毒墙网络版	
计算机标识	
指定 防毒墙网络版 客户	P机将通过域名还是 IP 地址识别服务器。
计算机有多个网卡时,; 用域名。	趋势科技建议您使用 IP 地址,并在计算机 IP 地址发生更改时,使
C <u>域名(D)</u>	trend-wc1os6td4
☞ IP地址[]):	10.28.132.77
InstallShield	
	帮助 <上一步(B) 下一步(N)> 取消

图4-10 选择计算机标示

(11) 做完服务器端的设置以后,继续进行客户机端的设置。请输入正确的产品激活码。一般我们的用户在拿到产品的时候会得到正式的产品使用激活码,您只需直接填入激活码即可。

趋势科技防毒墙网络反	
产品激活 步骤 1. 在线注册	
激活过程分为两步: 1)在线注册(如果已经有激活码则跳过该步骤)。 2)输入激活码。	
使用产品随附的'注册码''并单击下面的按钮在线进行注册。 送给您。	'激活码'将通过电子邮件发
(
InstallShield	
帮助 <上一步(B)	下一步(1)> 取消

图4-11-1 选择注册方式

TREND [■] → C R o [■] → M Hz [■] → Mz [■] → Mz	防毒墙网络版 Officescan 8.0
趋势科技防毒墙网络反	
产品激活 步骤 2. 输入激活码	
输入''繳活码'即可启用扫描与组件更新功能。 (>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	
防病毒:	_
损害清除服务:	
Web 威胁防护:	
InstallShield	下一步(N)> 取消

图4-11-2 输入激活码

(12)选择是否安装防毒墙客户机和NAC策略服务器

趋势科技防毒墙网络反	
安装其他防毒墙网络旅程序	
除了防毒墙网络版服务器,您可能还要向目标计算机安装其他防毒墙网 面的程序选择:	络版程序。从下
☑ 防毒墙网络版客户机(仅当 ServerProtect for NT 未在目标计算机上3 [0]	安装时可以安装)
□ 策略服务器 for Cisco NAC(P)	
Cisco Trust Agent for Cisco NAC(C)	
键入 Cisco Trust Agent 证书文件所在的本地驱动器和目录的完整路径(c:\ctagent.cer)。	例如,
该证书必须位于本地驱动器上;不接受映射的驱动器。	
	导入证书[[]
InstallShield	
帮助 <上一步(B) 下一步(N)>	取消

图4-12 选择是否安装其它防毒墙网络版程序

● TREND MICRO™ 趋势科技	可信赖的网络安全专家
---------------------------	------------

(13)是否参加全球病毒跟踪计划

趋势科技防毒墙网络反	
全球病毒跟踪计划	
趋势科技会整理全球客户的病毒/恶意软件和间谍软件/灰色软件结果,搜集实时统问息,并显示在病毒地图上。通过该地图可以查看每个大陆及选定国家/地区的安全风险。	十信 【
您想加入"全球病毒跟踪计划"吗 ?	
 是,我想加入"全球病毒跟踪计划"℃。我了解当在我的系统中检测到病毒/恶意: 件或间谍软件/灰色软件时,包括安全风险名称及检测次数在内的合计检测信息 ⑦ 发送到"全球病毒跟踪计划"。而公司名称、个人姓名、计算机名称、场所名称、 地址或任何其他标识信息均不会发送。我知道我随时可以禁用该自动报告功能, 法是在防毒墙网络版 Web 管理控制台中将配置改为"否"。 	软 将 IP ,方
◎ 否,我不加入(<u>0</u>)。 InstallShield	
<上一步(B) 下一步(N)> 取消	

图4-13 是否参加全球病毒跟踪计划

(14) 输入控制台密码和客户端推出卸载密码

趋	势科技防毒墙网络愈		
1	管理员帐户密码		
	指定用于打开 Web 控制者 权地修改 Web 控制台设置	計或退出/卸装防毒墙网络版客户机的密码。 置或删除防毒墙网络版客户机。	密码可阻止未经授
	Web 控制台密码: 密码:	1	
	确认密码:		
	客户机退出与卸装密码:		
	密码:		
	确认密码:		
Ins	tallShield		,
		<上一步(B) 下一步(A))> 取消

图4-14 管理员账户密码



可信赖的网络安全专家

(15)选择客户端安装路径和5位数通信端口

趋势科技防毒墙网络版 🛛 🛛 🗙
防毒増网络厳客户机安装
将防毒墙网络版客户机安装到防毒墙网络版服务器将管理的所有计算机上的相同路径 中。诸在下面键入安装路径。 警告:安装完成后安装路径无法更改。
\$ProgramFiles\Trend Micro\OfficeScan Client
端口号: 12221
安全级别:
○ 正常(□):将已对计算机的 Program Files 和注册表文件指定的访问权限指定到防毒墙 网络版客户机文件和注册表。
◎ 高旧)限制对防毒墙网络版客户机文件与注册表的访问。
InstallShield
帮助 <上一步(B) 下一步(N)> 取消

图4-15 防毒墙网络版客户机安装

(16)是否启用企业防火墙功能

趋势科技防毒墙网络反				
防病毒功能				
☑ 启用防火墙区				
InstallShield	帮助	〈上一步圓)	下一步[N]>	取消

图4-16 防火墙功能

(17)进行防间谍软件的设置

趋势科技防毒墙网络反
评估模式设计为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措施。单击"帮助"以获取更多信息。
☑ 启用评估模式(E) 评估模式持续时间(周):
InstallShield

图4-17 防间谍功能

(18)选择防毒墙网络版程序快捷方式

趋势科技防毒增网络愈
防毒増网络厳程序快捷方式
安装程序将向"开始"粟单添加一个包含防毒墙网络版程序快捷方式的文件夹。接受缺 省文件夹名称或指定一个新的名称。您还可以选择将把程序快捷方式添加到的现有文 件夹。
文件夹名称(E):
趋势科技防毒墙网络版服务器-TREND-WC10S6TD4
现有文件夹:
7-Zip Accessories Administrative Tools Startup
InstallShield <上一步(B) 下一步(N)> 取消

图4-18 防毒墙网络版程序快捷方式



(19)准备安装

趋势科技防毒墙网络版	X
安装信息	
下面是防毒墙网络版服务器安装摘要。	
已激活的服务数: 防病毒 损害清除服务 Web威胁防护	
服务器标识: 10.28.132.77	
目标目录: C:\Program Files\Trend Micro\OfficeScan\	
文件夹名称: ▲	▼
InstallShield <上一步(B)	

图4-19 安装信息

(20) 配置软件安装

趋势科技防毒墙网络版	
安装状态	
正在配置软件安装。	
C:\\{E0CA6191-52E8-41E0-96B2-05EA08E6869C}\data1.cab	
InstallShield	

图4-20 进入配置软件安装状态



(21)如果选择使用apache web server,将进行apache http server的安装



图4-21 进入安装状态

4.2 offices 客户端安装

(1) 通过访问 https://officescan服务器IP地址或者机器名: 4343/officescan,

趋势科技 防毒墙网络版 请键入密码以访问 Web 控制台。
密码 : 登录
可向用户提供以下客户机安装程序链接: 对于联网计算机: https://10.28.132.117:4343/officescan/console/html/ClientInstall/

可以访问主控台

图 4-22 Officescan 主要控制台



(2) 点击对于联网计算机下面的链接

防毒墙网络版

客户机安装需求

防毒墙网络版客户机在 32 位环境中需要目标计算机安装有 Windows XP/2000/2003/Vista,在 64 位环境中需要 Windows XP/2003/Vista。这种基于 Web 的客户机部署方法还需要 Microsoft Internet Explorer 5.0 或更高版本的支持。如果需要帮助,诸与您的防毒墙网络版管理员联系。

立即安装

单击下面的**立即安装**按钮开始将防毒墙网络版客户机软件安装到您的计算 机上。安装过程只需数分钟即可完成。但是,通常在网络中安装第一台防 毒墙网络版客户机时需要的时间较长。

立即安装	取消
------	----

图 4-23 进入安装界面

Internet	Explorer - 安全警告 🛛 🗙
您想安	炭此软件吗?
	名称: Install
	发行者: <u>Trend Bicro, Inc.</u>
<mark>.</mark> ●更重	3选项 (0) 安装 (I) 不安装 (D)
١	来自 Internet 的文件可能对您有所帮助,但此文件类型可能危害您的 计算机。请仅安装来自您信任的发行者的软件。 <u>有何风险?</u>
Internet	Explorer - 安全警告
Internet 您想安	Explorer - 安全警告 X
Internet 您想安	Explorer - 安全警告 X 医此软件吗? 名称: Setup
Internet 您想安	Explorer - 安全警告 医此软件吗? 名称: Setup 发行者: <u>Irend Licro, Inc.</u>
Internet 悠想安 ···································	Explorer - 安全警告 × 装此软件吗? 名称: Setup 发行者: Irend Licro, Inc. 安装(I) 3选项(0) 安装(I)

图 4-24 选择安装 ActiveX 插件



防毒墙网络版 Officescan 8.0

(3) 开始安装

一 趋势科技防毒墙网络散安装程序	X
趋势科技"防毒	墙网络版 ̄
xii	D使用趋势科技防毒墙网络版安装程序 请稍候
域名/计算机名称:	Workgroup / TREND-WC10S6TD4
IP 地址:	10. 28. 132. 77
正在连接服务器/代理服务器:	10. 28. 132. 77: 8080
当前操作:	下载完毕。
进度:	
收到的字节数:	
总体进度:	

图 4-25 开始安装

(4) 安装结束,请关闭窗口结束安装程序

4.3 如何检查安装是否成功

下面的检查项目列表可以帮助您逐步检查安装是否成功。 服务器端检查内容

- 启动组栏目
- 服务列表
- 系统进程
- IIS 中的虚拟目录/或者Apache

客户端检查内容

- 启动栏目组
- 管理主界面
- 系统进程



病毒检查

- 反映在客户端
- 反映在服务器端

4.3.1 服务器端

(1) 查看程序启动项是否正确

	Windows Catalog	行 墙网络版			
-	Windows Update				
<u>ю</u> 🔚	程序(P)	, 💼 附件	•		
	and the second sec	📅 趋势科技防毒墙网络版服务器-TERRY-TEST2	•		防毒墙网络版自述文件
8	文档(0)	🕨 🛅 趋势科技防毒墙网络版客户机	•	1	卸装防毒墙网络版
nterpr	· 设置 (2)	*		2	防毒墙网络版 Web 控制台 (HTML) >
8) 搜索 (C)	nstan			
	帮助和支持(出)	•=			
Ssuo	7 运行 (B)				
Ma 🚺	关机 (1)				
1 开始	🥭 🖉 t	势科技防毒墙网络 🛛 🦉 未命名 - 画图			کی 😎 🖒

图 4-26 officescan 服务器启动项目

(2) 开始--运行--打开服务管理

Run	? ×
-	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	services.msc
	OK Cancel <u>B</u> rowse

图 4-27 打开服务



可信赖的网络安全专家

(3) 输入 services.msc,查看服务是否有启动

名称 🛆	描. 状态	启动类型
Messenger	传	禁用
Microsoft Software Shadow Copy Provider	管	手动
Wet Logon	为 已启动	自动
NetMeeting Remote Desktop Sharing	使	禁用
Network Connections	管 已启动	手动
Network DDE	为	禁用
Network DDE DSDM	管	禁用
Network Location Awareness (NLA)	收 已启动	手动
🐝 Network Provisioning Service	在	手动
NT LM Security Support Provider	为	手动
BOfficeScan Control Manager Agent	允	手动
🖏 OfficeScan Master Service	接 已启动	自动
🖓 OfficeScan NT Listener	从 已启动	自动
🖗 OfficeScan NT Personal Firewall	提 已启动	手动
🖗 OfficeScan NT Proxy Service	将	手动
🖗 OfficeScan NT RealTime Scan	对 已启动	自动
Performance Logs and Alerts	收	自动

图 4-28 officescan master service 服务是否启动

4.3.2 客户端

(1) 启动项目



图 4-29 officescan 客户端启动项目



可信赖的网络安全专家

(2) 查看进程

2	indows 任务管理	#		_ 🗆	×
文件	F(E)选项(D) 査視	昏(V) 帮助(H)			
应	用程序进程	能 联网 用	户丨		
	映像名称	用户名	CPU	内存使用 ▲	
	svchost, exe	SYSTEM	00	4,360 K	
	ApacheMonitor	terry_zhou	00	2,500 K	
	taskmgr.exe	terry_zhou	03	4,508 K	
	PccNTMon. exe	terry_zhou	00	7,756 K	
	VMwareUser.exe	terry_zhou	00	4,168 K	
	TmPfw.exe	SYSTEM	00	5,644 K	
	explorer.exe	terry_zhou	07	16,324 K	
	wmiprvse.exe	SYSTEM	00	5,096 K	
	alg.exe	LOCAL SERVICE	00	2,312 K 💳	
	DbServer.exe	SYSTEM	00	27,352 K	
	TmListen.exe	SYSTEM	00	15,256 K	
	VMwareService	SYSTEM	00	2,424 K	
	spx. exe	terry_zhou	02	5,064 K	
	svchost, exe	LOCAL SERVICE	00	1,328 K	
	CNTAoSMgr.exe	SYSTEM	00	3,144 K	
	svchost, exe	SYSTEM	00	3,712 K	
	OfcService.exe	SYSTEM	00	96,916 K	
	QMB3DE. EXE	SYSTEM	10	2,840 K 🔤	
	ctfmon exe	terry zhou	00	2 556 K 🔟	
	🗆 显示所有用户的途	进程(S)		结束进程(2)	
_					
进程	数:38 │CPU19	•用:25% P	内存使用:	384M / 1182M	11.

图 4-30 查看 pccntmon.exe 进程



防毒墙网络版 Officescan 8.0

(3) 查看客户端界面

建势科技防毒墙网络 放 前 的 的 书 的 的	_ 🗆 X
● 趋势科技 [™] 防毒墙网络版 [™] ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
手动扫描 目动扫描结果 防火墙 邮件扫描 日志 工具箱 病毒 /恶意软件 □	
Local Disk (F:) Local Disk (G:) Ime → ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
间谍软件/灰色软件 扫描间谍软件/灰色软件	
退出	帮助

图 4-31 客户端界面

(4) 客户端图标





4.3.2 病毒测试

(1) 进入 <u>www.eicar.com</u> 网站下载测试病毒 eicar

*			EU	ROPEAN EXPERT GROU	P FOR IT-SECURITY
eical	r			DOWNLOAD	Anti-Malware Testfile
				SEARCH	
ABOUT US	CONFERENCE	TASK FORCES	PRESS	CONTACT	powered by FreeFind INFORMATION
problems when di rename the file to " virus scanner will be used to see wh Once downloaded the single zip ARC access to the file(scanner which put user's manual of y Important note: E cause any damag are sufficiently sec your computer. Ple	ownloading the first file, eicar.com". That will do t spot a Virus' inside an A ether the virus scanner c run your AV scanner. It HIVEe and may be ever (s) anymore. You might is the file into quarantair our AV scanner what to d ICAR cannot be held re e to your computer. YOU ure in the usage of your ase contact the manufac	which can be circum he trick. The third verse ARCHIVEe. The last w hecks ARCHIVEes m should detect at leas n in the double zip AF not even be allowed he. The test file will b to or contact the vendo sponsible when the DOWNLOAD THESE AV scanner. EICAR ca turer/vendor of your A	wented when using the sion contains the test fil ersion is a zip ARCHIV ore than only one level t the file "eicar.com". G RCHIVEe. Once detecte by the scanner to del e treated just like any o or/manufacturer of your se files or your AV sca FILES AT YOUR OWN annot and will not provi-	e second version. Just do e inside a zip ARCHIVEe. E containing the third file. deep. Bood scanners will detect d the scanner might not a ete these files. This is ca other real virus infected fil AV scanner. anner in combination with RISK . Download these file de any help to remove these in help.	wnload and A good anti- This file can the Virus' in Ilow you any used by the e. Read the e. Read the h these files is only if you se files from
	Downloa	d area using the st	andard protocol http://www.com/actions/action/	р	
<u>eicar.com</u> 68 Bytes	<u>eicar.com.txt</u> 68 Bytes	s <u>eicar co</u>	<u>m.zip</u> 184 Bytes	<u>eicarcom2.zip</u> 308 Bytes	
	Download area	using the secure,	SSL enabled protoc	col https	
(Note: For the time b De	eing we make use of a self- pending on acceptance of th Cert	-signed certificate. You his new service we may tificate Authority at a late	may be asked by your bro y install a certificate comin er point in time.)	wser whether you trust this : g from a trusted	site.
<u>eicar.com</u> 68 Bytes	<u>eicar.com.bt</u> 68 Bytes	s <u>eicar co</u>	<u>m.zip</u> 184 Bytes	<u>eicarcom2.zip</u> 308 Bytes	

图 4-33 eicar 网站



可信赖的网络安全专家

(2) 如果开着实时扫描

防毒墙网络廒道	画知消息			
	趋势科技 防暑	导 墙网络	版	
防毒墙网络版 细信息,诸单	检测到一个或多个病毒; !击病毒/恶意软件名。	/恶意软件。有	关病毒/恶意	意软件的详 🛌
,			病]毒/恶意软件:2
日期/时间	病毒/恶意软件名称	受感染文件	扫描类型	结果
2007-7-5 2007-7-5	Eicar_test_file Eicar_test_file	C:\Docu C:\Docu	实时扫描 实时扫描	己隔离 己隔离
,				補定

图 4-34 实时扫描报错信息

(5) 客户端也有病毒日志

(型)趋势 转到(G)	身科技防毒増网络) 设置(5) 帮助	各版 1(H)			-	
×	病毒/悪意软件日 找到 2 条病毒/	日志 (恶意软件日志。			X	
手	日期/时间 2007-7 2007-7	病毒/恶意软件 Eicar_test Eicar_test	受感染文件 C:\Documents and S C:\Documents and S	<u> 扫描类型</u> 实时扫描 实时扫描	结果 已隔离 已隔离	
			关闭 帮助 (4)]		
				退出	出一帮助)

图 4-37 客户端病毒日志

5. 升级安装过程

5.1 升级前的注意事项

注意:若是由OfficeScan 6.5/7.x 升级到OfficeScan 8.0, 请确认其语言版本, 中英文版本不可相互升级

中文版OfficeScan 6.5/7.x → 中文版 OfficeScan 8.0

英文版OfficeScan 6.5/7.x → 英文版 OfficeScan 8.0

因Officescan 8.0 已不支持Windows 95/98/ Me/ NT和IA64 等操作系统,

1,请确认要升级的Officescan服务器是否有控管Windows 95/98/Me/NT和IA64 等 平台:

- 如有,请参考1-1步骤:将不支持的客户端转移至另一台Officescan服务器管理

2,确认Officescan服务器是否有注册到 Control Manager服务器(Control Manag 是趋势科技另一防毒产品):

- 如有,请确认Control Manager 是否是3.5版本并更新到Patch3以上

注: Officescan 8.0 只能注册到Control Manager 3.5 + Patch3 版本

3,确认Officescan 目前扫描引擎是否为8.5版本,因Officescan8.0 IntelliTrap病毒技术需搭配8.5扫描引擎才能启用,如使用8.321、8.330、8.440 等特殊版扫描引擎请一定要升级至8.5版本(如不知目前扫描引擎使用版本,请 参考1-2步骤:如何确认扫描引擎版本) 可信赖的网络安全专家

5.2 升级前的备份

TREND MICRO™ 趋势科技

备份客户端扫描设定

步骤1:登入 officescan 服务器端管理控制台

备份以及清除相关 log, 避免升级时间过久

步骤 1: 登入 officescan 服务器端管理控制台——记录档——病毒记录档——officescan 客户端

步骤 2: 在病毒记录的页面中,时间栏选择全部,扫描种类勾选需要备份类型 或者全部勾选,"以 CSV 格式输出"

步骤 3:选择"删除记忆档"在删除记忆档的页面中,选择全部类型,删除选定的记录档类型的所有记录档内容

手动备份\Program Files\Trend Micro\OfficeScan\PCCSRV 文件夹内的下列文件 和文件夹

ofcscan.ini:包括所有客户端的设定 ous.ini:包括防毒组件更新来源的表格 private文件夹:包括防火墙和更新来源设定 we\tmopp文件夹:包括病毒爆发阻止设定 pccnt\common\ofcpfw.dat:包括防火墙设定 download\ofcpfw.dat:包括防火墙部署设定

5.3 升级安装

1,执行安装程序

2,出现软件授权同意书画面,选择我同意授权合约的条款,下一步,继续安装

3,选择本机安装还是远程安装

4,选择安装前是否进行 DCS 扫描



图 5-1 DCS 扫描

5,显示查找到原先安装的officescan版本,继续安装

趋势科技防毒增网络反	
	安装信息
	目标计算机上已安装了先前版本的防毒墙网络版。要 升级,请单击'下一步''。
	重要信息:此版本的防毒墙网络版不再支持 Windows 95/98/Me/NT 和 IA64 体系结构。升级后,在不支持 的平台上安装的客户机将被移除,其信息将导出到一 个文件。升级后运行客户机迁移程序可将这些客户机 移到支持这些平台的防毒墙网络版服务器。
	单击'帮助''以获取关于管理不支持平台上的客户机的 信息。
	帮助 〈上一步图] 【下一步[1] 】 取消

图5-2安装信息



6, 输入序列号

≃晶激活		6
步骤 2. 输入激活	 弱	
输入'激活码'即 (XXXXXXXXXXXXXX	可启用扫描与组件更新功能。 <>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	
防病毒:		
]		
损害清除服务:		_
Web威胁防护:		
P		
allShield ———		
	Trans 1 Doubles	and the second The bala

图5-3产品激活码



7,选择评估时间的设定

趋势科技防毒增网络反	
防间谍软件功能	
评估模式设计为允许您先评估间谍软件/灰色软件是否合法,然后根据您 施。单击"帮助"以获取更多信息。	的评估采取措
▶ 启用评估模式[[]	
评估模式持续时间(周):	
4	
InstallShield	
帮助 〈上一步追〉下一步心〉	取消

图5-4评估时间设定

8, 安装结束



6. Officescan 控制台管理

Ħ	标 处理措施
₹	启用病毒/恶意软件扫描
	☑ 启用间谍软件/灰色软件扫描
用	户对文件执行的活动
C	扫描正在创建/修改的文件
C	扫描正在检索的文件
œ	扫描正在创建/修改和检索的文件
要	扫描的文件
C	所有可扫描文件
o	已由 IntelliScan 扫描的文件类型 🟮
C	带下列扩展名的文件(使用半角逗号分隔各项):
	."", ACE, ARJ, ASP, BAT, BIN, BOO, CAB, CHM, CLA, CLASS, COM, CSC, DAT, DL L, DOC, DOT, DRV, EML, EXE, GZ, HLP, HTA, HTM, HTML, HTT, INI, JAR, JS, JSE, L NK, LZH, MDB, MPD, MPP, MPT, MSG, MSO, NWS, OCX, OFT, OVL, PDF, PHP, PIF, P L, POT, PPS, PPT, PRC, RAR, REG, RTF, SCR, SHS, SYS, TAR, VBE, VBS, VSD, VS

图 6-1 实时扫描 1



○ 对每种病毒/恶意软件类型使用特定的处理措施

类型	第一处理措施		第二处理措施
恶作剧程序	隔离	•	
特洛伊木马	隔离	•	
病毒		-	隔离 🗾
测试病毒	拒绝访问	-	
打包程序	隔离	-	
其它	清 除	•	隔离

隔离目录: HTTP://10.28.132.117

☑ 先备份后清除

☑ 检测到病毒/恶意软件时在客户端计算机上显示通知消息

间谍软件/灰色软件

○ 清除:防毒墙网络版将终止进程或删除注册表项、文件、cookie 和快捷方式。

- 拒绝访问
- ☑ 检测到间谍软件/灰色软件时在客户端计算机上显示通知消息

图 6-2 实时扫描 2

(2) 手动扫描

手动扫描设置

病	毒/恶意软件扫描
要打	3描的文件
0	所有可扫描文件
o	已由 IntelliScan 扫描的文件类型 🧾
C	带下列扩展名的文件(使用半角逗号分隔各项):
	ACE, ARJ, ASP, BAT, BIN, BOO, CAB, CHM, CLA, CLASS, COM, CSC, DAT, DLL, D OC, DOT, DRV, EML, EXE, GZ, HLP, HTA, HTM, HTML, HTT, INI, JAR, JS, JSE, LNK, LZH, MDB, MPD, MPP, MPT, MSG, MSO, NWS, OCX, OFT, OVL, PDF, PHP, PIF, PL, P OT, PPS, PPT, PRC, RAR, REG, RTF, SCR, SHS, SYS, TAR, VBE, VBS, VSD, VSS, V ST, VXD, WML, WSF, XLA, XLS, XLT, XML, Z, ZIP
扫扫	曲设置
•	扫描引导区
	扫描网络上的映射驱动器和共享文件夹
~	扫描隐藏文件夹
~	启用 IntelliTrap
7	如果压缩文件的压缩层数超过以下数值,则不要进行扫描: 2 👤
сD	山田本

图 6-3 手动扫描



防毒墙网络版 Officescan 8.0

在间谍软件、灰色软件扫描的选项中,建议选择完全扫描整个计算机

手动扫描设置

目描方法	
〕快速: 仅扫描间谍软件/	灰色软件通常攻击的计算机区域,包括内存中的程序和模块、Windows 注册表和 URL 快捷方式
完全: 扫描整个计算机	7
日猫例外(文件扩展名)	
☞ 启用扫描例外	
	- 2)
输入文件扩展名(例如,mj	p3)。 添加
输入文件扩展名(例如,mj MP3	p3)。 添加 移除

图 6-4 间谍软件、灰色软件扫描

TREND MICRO 趋势科技

可信赖的网络安全专家

在处理措施中,建议选择 activeaction 选项,

手动扫描设置

毒/急意软件				
使用 ActiveAction 🤑)			
对所有病毒/恶意软件类	型使用相同的处理措施			
(如果选择"洁除",诸	指定清除处理措施失败时附	方毒墙网络	版将采取的第二	处理措施)
类型	第一处理措施		第二处理措施	
所有类型	清 除	•	隔离	-
对每种病毒/恶意软件类型	型使用特定的处理措施			
类型	第一处理措施		第二处理措施	
恶作剧程序	隔离	-	-	
特洛伊木马	隔离	-		
病毒		-	隔离	-
测试病毒	不予处理	•		
打包程序	隔离	•		
			(article)	

隔离目录: HTTP://10.28.132.117

☑ 先备份后清除

图 6-5 手动扫描处理措施

(4)格外列表

扫描例外

- ☑ 启用扫描例外
- □ 对所有扫描类型应用扫描例外设置

扫描例外列表(目录)

添加
移除



建议将下列路径设为例外档案:

针对Win 9x/ME 的机器

1.C:\Program Files\Trend Micro\OfficeScan Client\Backup

2.C:\Program Files\Trend Micro\OfficeScan Client\Unsent Virus 针对Win NT /Win 2000 /Win XP /Win 2003

1.C:\Program Files\Trend Micro\OfficeScan Client\Backup

2.C:\Program Files\Trend Micro\OfficeScan Client\Suspect





OfficeScan 服务器端刚刚安装完成后,病毒码、引擎为安装包里提供,趋势科 技更新服务器上可能已经有了较新的版本,故建议您立即更新您的OfficeScan 服务器端,并且,建议将预设更新设置为每小时检测,从而更有效的检测并抵御 病毒的攻击,若您的 OfficeScan 服务器无法连接到Internet 进行更新,请立 即对其进行手工更新。

7.1 服务器端的更新

趋势科技"防毒	墙网络版 [™]	●】 注销 ⑧	RBD 💽 🥑 TRE!
🔍 立即扫描	▲服务器更新源		@ 帮助
🔤 立即更新服务器	从以下更新题下载更新		
摘要	 趋势科技 ActiveUpdate 服务 (http://osce8-p.activeupdate 	器 æ.trendmicro.com.cn/activeupdate/china)	
更新	○ 其他更新源:		
摘要			+ -
服务器		t位置	
预设更新 手动更新 面 新源	UNC 路径: 示例: \\server_na	ame\download	
联网计复机			
自动更新 手动更新 更新源	·····································		
还原			
▶ 日志			
▶ Cisco NAC			
Server 1	—		

(2) 服务器端手动更新

此页会显示目前OfficeScan 服务器上的更新组件及上次更新时间,按[更新]可进行服务器手动更新。

尼 刀 杄 扠				防毒墙网络	版 Officescan 8.0
趋势科技"防毒	墙网络)	版"		✓ 注韻 ❷	
🔍 立即扫描	▲服	务器	手动更新		@ 帮助
🔜 立即更新服务器	3	更更新	的組件		
	- [•	联网计算机组件	当前版本	上次更新时间
11132	- 0		防病毒		
电我	- 0		防间谍软件		
大 初	- 8		损害清除服务		
加女			防火墙		
加安 西 预设更新			通用组件		
手动更新		-	Teste I		
更新源		更新	取消		
联网计算机					
自动更新	No. Con				
手动更新					
更新源					
· 还原					
日志	_				
Cisco NAC					
通知	- I mark				

图 7-2 服务器手动更新

(3) 服务器端自动更新

此页可设定OfficeScan 服务器主动更新的功能,建议一天至少更新一次。

趋势科技" 防毒	啬网络版	TPI		[🛃 注销) 💿 🗔	帮助 🔽	
Q 立即扫描 还即更新服务器	▲ 服务 [[]	₹ 番 う	預设更新 防毒墙网络版服务器的预设更新	БГ.			❷ 帮助
摘要	- 要:	更新	的組件				
▶ 联网计算机		☑	联网计算机组件		当前版本	上次更新时)
更新	Đ		防病毒			10	
摘要	Đ	2	防间谍软件				
服务器		•	损害清除服务				
预设更新	Đ	~	防火墙				
手动更新	Đ		通用组件				
史 新祝	更	新日	程			14.	-
白动軍新	•	毎小	时一次				
手动更新	0	毎E]→次	开始时间:12	:00 🔽 (时:分)		
更新源	0	毎周]一次,在 星期日 🗾	以2 🔄 小时 🕽	り更新周期		
还原		毎月	一次,在毎月的 01 🚽 号				
▶ 日志				10 10			100
▶ Cisco NAC	保	存					
▶ 通知							
▶ 啓田							

图 7-3 服务器端预设更新



可信赖的网络安全专家

7.2 客户端的更新

(1)更新源

趋势科技 [™] 防毒	墙网络版 [™]		🗐 注道 ⑧帮助 🔽 💋 IRE		
🔍 立即扫描	▲ 更新源(联网计算机)	ľ.		- 帮助	
 立即更新服务器 摘要 联网计算机 更新 摘要 服名器 	可以选择某些客户机使之 台 ActiveUpdate 服务器 ○ 标准更新源(从防毒 ○ 定制的更新源 ☑ 如果所有定制源 ☑ 更新代理:始终从标符	从防毒墙网络版服务器 。 墙网络版服务器更新) 均不可用或未找到,则, 生更新源(防毒墙网络版	以外的源进行更新。替代的更新源可以是一个 从防毒墙网络版服务器更新 反服务器)更新	更新代理或一	
	定制的更新渡列表			1	
手动更新 更新源	添加 删除				
联网计算机					
自动更新		IP 范围	外部源		
手动更新 更新源 还面	添加 删除				
▶ 日志		f -			
Cisco NAC					
▶ 通知					
A4770	V				

图 7-4 客户端更新源

(2) 客户端手动更新选项,通过服务器通知客户端进行更新

趋势科技" []	5毒墙网络版	🛃 注销 @帮助 🖃 🤌		
🔍 立即扫描	▲ 手动更新(联网计算机)		@ 帮助	
🔤 立即更新服务器	要更新的組件			
	组件	当前版本	上次更新时间	
個安	• 防病毒			
联网计算机 	────────────────────────────────────			
史勒				
摘要				
服务器				
预设更新 手动 東新	目标客户机			
更新源	G 洗择带有过期组件的客户机			
联网计算机				
自动更新				
手动更新	C FAULDIA-A/ 01			
更新源	开始更新 取消			
还原				
日志				
Cisco NAC				
通知				
修理				

图 7-5 客户端手动更新



可信赖的网络安全专家

(3) 客户端手动更新

趋势科技 [™] 防毒墙网	网络版		🛃 注道 ⑧帮助	
🔍 立即扫描	自动更新(联网计算机)			@ 帮助
🔤 立即更新服务器	在发生某些事件时或在指定的	的更新日程期间触发客户机	以更新组件。	
	亊件触发更新			
	▶ 防毒墙网络版服务器下载	散完新组件后立即在客户机	上启动组件更新	
更新	□ 包括漫游客户机			
摘要	▶ 使客户机在重新启动并;	车接到防毒墙网络版服务器	时启动组件更新(漫游客户机队	余外)
服务器	□ 更新后执行"立即扫描"			
预设更新 手动更新 更新源	基于时间表更新 C 分钟			
联网计算机 目动更新 手动更新 更新	 ○ 小时 ○ 毎日一次 ○ 毎周一次,在 星期日 	开始时间: 00 •: 1 以 2 • 小时为更新	〕0 ▼ (时:分) 新周期	
· ∠原 ▶ 日志	保存取消			
▶ Cisco NAC				
▶ 通知 ▶ 产型用	1			

图 7-6 客户端自动更新



8. 趋势科技厂商资源

800 免费售后热线

800-820-8839

● 售后电子邮件地址

<u>service@trendmicro.com.cn</u>

● 趋势科技中文网站

http://www.trendmicro.com.cn

● 病毒查询

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

● 中文版资料及软件下载

http://support.trendmicro.com.cn

● 趋势科技英文产品下载网站

http://www.trendmicro.com/download

● 试用版序列号申请:

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

/cd. asp

● 趋势科技病毒递交信箱

virus_doctor@trendmicro.com.cn