

网络卫士过滤网关系统

TopFilter

产品说明



北京市海淀区上地东路1号华控大厦100085

电话: +8610-82776666

传真: +8610-82776677

服务热线: +8610-8008105119

<http://www.topsec.com.cn>

版权声明

本手册的所有内容，其版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、转译或任意引用。本手册没有任何形式的担保、立场倾向或其他暗示。

若因本手册或其所提到的任何信息引起的直接或间接的资料流失、利益损失，天融信及其员工恕不承担任何责任。本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信恕不承担另行通知之义务。

版权所有 不得翻印© 1995-2009 天融信公司

商标声明

本手册中所谈及的产品名称仅做识别之用，而这些名称可能属于其他公司的注册商标或是版权，其他提到的商标，均属各该商标注册人所有，恕不逐一列明。

TopSEC®天融信

信息反馈

<http://www.topsec.com.cn>

目 录

1	产品概述	1
2	产品特点介绍	1
3	产品功能	4
4	运行环境与标准	5
5	典型应用	7
	1) 部署在网关处.....	7
	2) 部署在分段的企业网络中.....	8
6	产品资质	9

1 产品概述

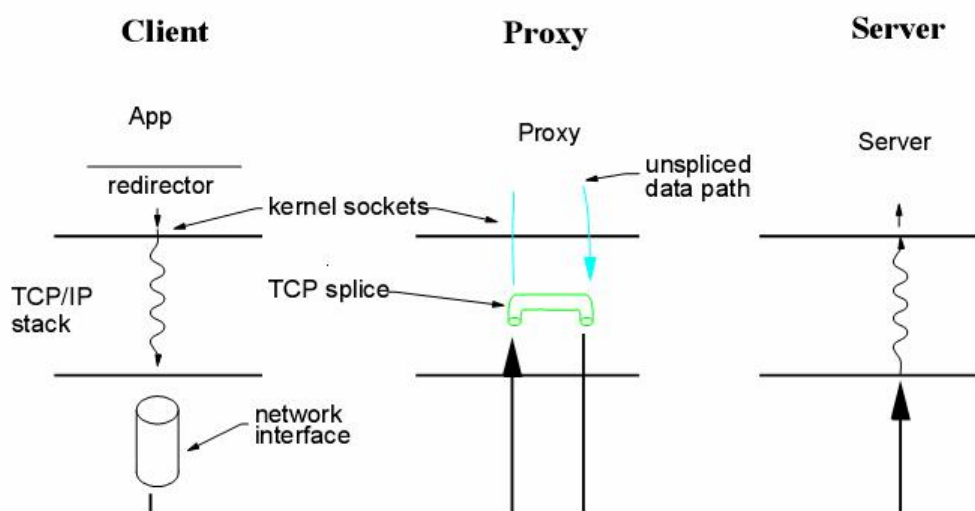
天融信网络卫士过滤网关系统防病毒网关采取了一个与单机防护不同的基于网络的病毒防护方案。它被设计成安装在网络边缘，在病毒侵入网络之前实时的阻止它们，并且运用先进的检测技术解决了传统病毒网关类产品会造成网络延时的问题。网络卫士防病毒网关具有真正的即插即用能力，部署好之后就可以进行网络协议数据的病毒过滤功能；目前过滤网关基本可以支持主要的网络协议，SMTP、IMPA4、POP3、HTTP 以及 FTP 协议。

2 产品特点介绍

独创的 TCP 粘合技术

天融信防病毒网关基于透明代理技术实现。透明代理技术的优点是可以在应用层实现复杂的过滤。缺点是降低设备的吞吐，并且造成较大的网络延迟。TCP 粘合技术显著的提升了透明代理的性能，大大降低了通信延时。连接粘合后的性能接近内核的路由转发。

TCP 粘合连接的原理如下图所示。该结构与应用级代理的最大不同在于：客户端和服务端之间的连接在操作系统的核心层进行连接粘合。TCP 粘合避免了数据包从核心空间到用户空间的拷贝和多次 socket 系统调用导致的上下文切换，显著提高了转发的性能，并且大大降低了通信延迟。



全面的病毒防护解决方案

网络卫士过滤网关具有病毒防护、防间谍软件、反垃圾邮件、防网络钓鱼欺诈等全面的防护功能。

网络卫士过滤网关防病毒网关可以处理以下协议：SMTP、POP3、HTTP、FTP 和 IMAP，全面保护公司邮件、WEB 使用以及文件传输过程对病毒的防护解决方案。而且管理员可以自行选择对病毒的处理方式，包括清除病毒、删除文件、隔离病毒或是记录日志的方式。而且还可以在相应的协议中设置一些附加功能，如对关键字的过滤，对特定文件类型的扫描和过滤等功能。

透明扫描

大多数传统的解决方案工作在 OSI 的应用层，以代理的方式截获数据进行扫描：客户机首先连接到防病毒网关，防病毒网关再连接到真正的服务器，转发并扫描通过的数据流，这种方法丢失了很多有用的客户端及服务器的信息。邮件服务器往往需要知道客户机的地址来决定是否允许客户端通过它发送邮件，特别是现在的垃圾邮件实在是泛滥成灾，这一点尤其重要。网络卫士防病毒网关工作在 3-7 层（图 2-3），它能够完整地保留这些信息，使企业的网络更安全。

OSI 网络层次	覆盖面	
7. 应用	传统的防病毒软件	天融信网络卫士防

6. 表示		病毒网关
5. 会话		
4. 传输		
3. 网络		
2. 数据链路		
1. 物理		

【图 2-3】网络层的扫描

同时支持单双通道的病毒扫描

网络卫士过滤网关防病毒网关提供灵活的部署方案，根据客户的需要，它可以被部署在网络的任何地方，并且可以配置成单或双通道的病毒扫描模式。首先，网关是最合理和有效的部署位置，它可以从公司网络的入口处直接封堵住病毒；第二，可以将它部署在邮件服务器之间，分担网络负载；第三，可以将它部署在每个需要保护的网段中，分别进行病毒的扫描和防护。

网络卫士过滤网关在配置的时候可以设置成单通道的病毒防护模式；或者设置成双通道的病毒防护模式，用户除了可以象单通道的防护模式单独保护内网，也可以利用同一台过滤网关的第二条扫描通道单独对防火墙的 DMZ 区的服务器组实现病毒防护，更加增强了安全性，节省了企业的成本。

即插即用，管理简单

网络卫士防病毒过滤网关，不需要改动现有网络的任何设置。一旦部署的位置被确定，只需要连接上网线，开启电源就可以进行扫描。扫描时只需要配置管理 IP 地址。安装向导会指导管理员进行基本的设置，十分简单易懂。该设备采用 B/S 架构设计，提供了一个基于浏览器的启发性管理界面，管理员可以实现方便的远程管理。

高可用性

网络卫士过滤网关防病毒网关支持双机热备，并具有 Bypass 功能，在遇到异常情况时，能自动切换到 Bypass 状态，保证网络环境的高度畅通性；同时防病毒网关为了适应网络流量非常大的复杂情况，在系统内核中做了适当的处理，防止由于流量过大造成设备当机的情况，可以保证用户网络不中断。

与天融信的安全管理软件充分融合

网络卫士过滤网关防病毒网关可以与天融信的安全管理软件充分融合，实现天融信的整体安全防护的理念。它可以与接受 TopPolicy 的策略分发，支持 TP 的管理；为 TA 提供完全的日志供安全审计和分析，提供了详细的报告。天融信通过对安全产品的整合来最大程度的保护用户的安全需求。

过滤垃圾邮件

网络卫士过滤网关防病毒网关采用业界领先的黑名单和白名单技术，实时、准确地过滤垃圾邮件，保证公司不受垃圾邮件的干扰；同时可以阻挡通过邮件通道传播病毒，造成的公司邮件服务器接收的大量垃圾邮件。

3 产品功能

功能类别		说明
安全功能	完全的病毒防护	内嵌完整的卡巴斯基杀毒引擎，支持100万余种病毒查杀，防御病毒、木马、蠕虫，支持绝大多数压缩、加壳病毒查杀。
	即插即用的透明接入方式	过滤网关采用即插即用的思路设计，以透明网桥方式部署在企业网络中，无需改变企业内部的网络配置，从而使安装工作变得非常简单。一旦部署完成，网络卫士防病毒网关就开始对企业网络进行病毒防护，保障网络不受病毒侵害。
	全面的协议保护	过滤网关对 SMTP、POP3、IMAP、HTTP 和 FTP 等应用协议进行病毒扫描和过滤，有效地防止可能的病毒威胁。
	内容过滤功能	过滤网关支持对数据内容进行检查，可以采用关键字过滤，URL过滤等方式来阻止非法数据进入企业网络，同时支持对Java等小程序进行过滤等，防止可能的恶意代码进入企业网络。
	阻断文件列表	常用的识别文件类型的方法是根据文件的扩展名，而这种方法可以通过简单的修改文件扩展名逃避。过滤网关通过文件内容识别文件类型，有效的阻断非法类型的文件进入企业网络。
	连接数控制	过滤网关可以对源地址做并发连接数限制，支持单个地址、网段、IP地址范围。
	病毒隔离	过滤网关支持病毒隔离功能，管理员可以方便的管理隔离区，可以选择把隔离区的内容发送给管理员或者删除。
	反垃圾邮件	过滤网关采用业界领先的黑名单技术实时检测垃圾邮件并阻止其进入企业网络，为企业节省宝贵的带宽。

	信任站点	过滤网关不对信任站点做病毒扫描，大大的降低了病毒扫描引擎的负担。
	蠕虫防护	过滤网关可以实时检测到日益泛滥的蠕虫攻击，并对其进行实时阻断，从而有效防止企业网络因遭受蠕虫攻击而陷于瘫痪。
管理功能	友好的管理界面	过滤网关采用基于 Web 的管理界面，用户只需打开浏览器，就可以方便地通过 HTTPS 协议对过滤网关进行有效管理。
	自动在线升级	过滤网关可以按照管理员设定的更新策略自动连接到天融信公司的升级服务器，升级最新的病毒库，保证企业网络得到最有效的保护。
日志与报表	日志功能	网络卫士防病毒网关提供完整的病毒日志、访问日志和系统日志等记录。
	统计报表功能	并可根据日志数据生成多种格式 的统计图形化统计报表，形象直观，方便管理员的管理工作。
	丰富的流量统计	过滤网关支持丰富的流量统计功能，包括接口流量统计、地址流量统计、IP 连接数统计。
监控和报警功能	强大的监控功能	网络卫士防病毒网关提供强大的监控功能，可以监控过滤网关系统资源、网络流量、当前会话数、当前病毒扫描信息等，极大地方便管理员对过滤网关进行监控。
	报警功能	报警配置用于当某个病毒突然爆发时，网络卫士防病毒网关可向网络管理员发送报警信息。
高性能	TCP 粘合技术	网关构建在高性能的硬件平台上，采用高效的扫描算法和 tcp 粘合技术，最大限度地提高过滤效率与处理性能。

4 运行环境与标准

电源：

TF-8404-Virus / TF-8504-Virus 电源：

电压：AC100~240V

频率：60~50HZ

电流：8~5A

功率：400W (MAX)

冗余：支持

TF-7704-Virus 电源：

电压：AC100~240V

频率：60~50HZ

电流：8~5A

功率：350W (MAX)

冗余：不支持

TF-7504-Virus / TF-7604-Virus 电源:

电压: AC90~260V±10%

频率: 63~47Hz

电流: 8~5A

功率: 200W (MAX)

冗余: 不支持

尺寸:

TF-8404-Virus / TF-8504-Virus 尺寸:

深*宽*高: 570×426×89 (mm)

TF-7704-Virus 尺寸:

深*宽*高: 520×426×44 (mm)

TF-7504-Virus / TF-7604-Virus 尺寸:

深*宽*高: 330x426x44 (mm)

环境:

TF-8404-Virus / TF-8504-Virus / TF-7704-Virus 环境:

运行温度: 0~40 摄氏度

非运行温度: -40~70 摄氏度

相对湿度: 5~95%RH, 非冷凝

TF-7504-Virus / TF-7604-Virus 环境:

运行温度: 0~45 摄氏度

非运行温度: -20~65 摄氏度

相对湿度: 10~90%RH, 非冷凝

国家标准:

GB/T18336-2001

GB/T18019-1999

GB/T18020-1999

参考的安全规范及标准(相对参考):

GB4943-2001

UL 1950

TUV-IEC 950

电磁兼容标准:

GB9254-1998

GB17618-1998

FCC Class A

IEC 61000-4-2 (静电放电 ESD 抗扰度)

IEC 61000-4-3 (射频电磁场抗扰度)

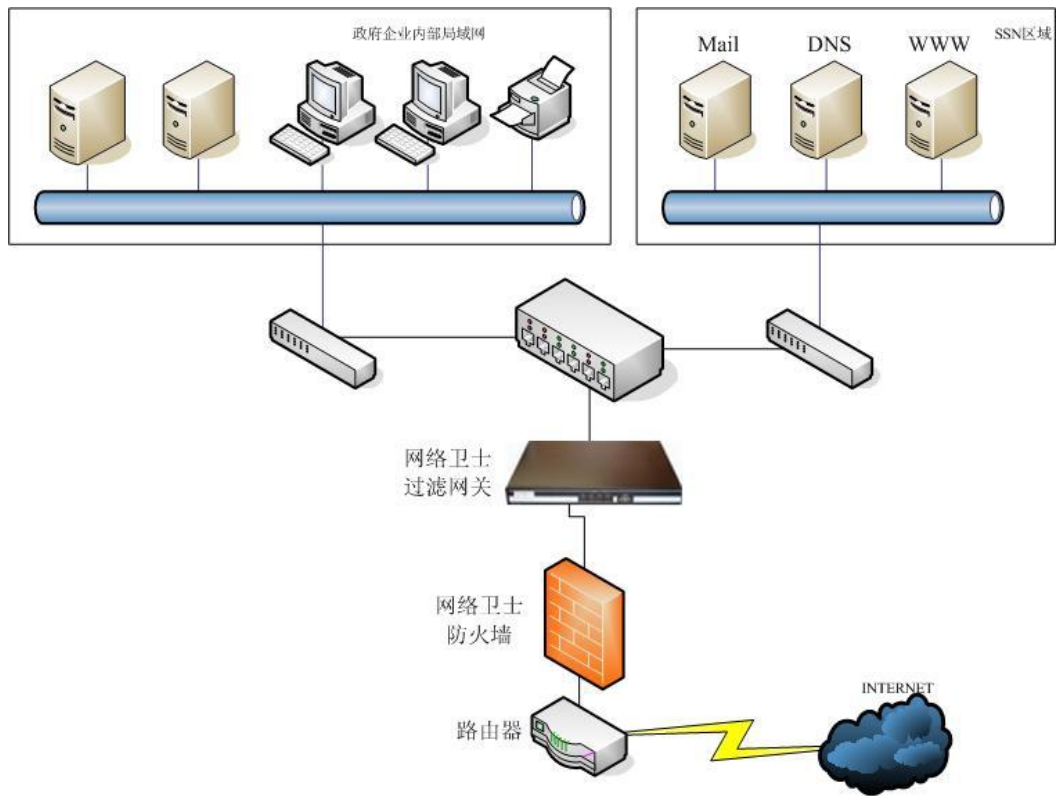
IEC 61000-4-4 (电快速瞬变 EFT 抗扰度)

IEC 61000-4-5 (浪涌 Surge 抗扰度)

5 典型应用

1) 部署在网关处

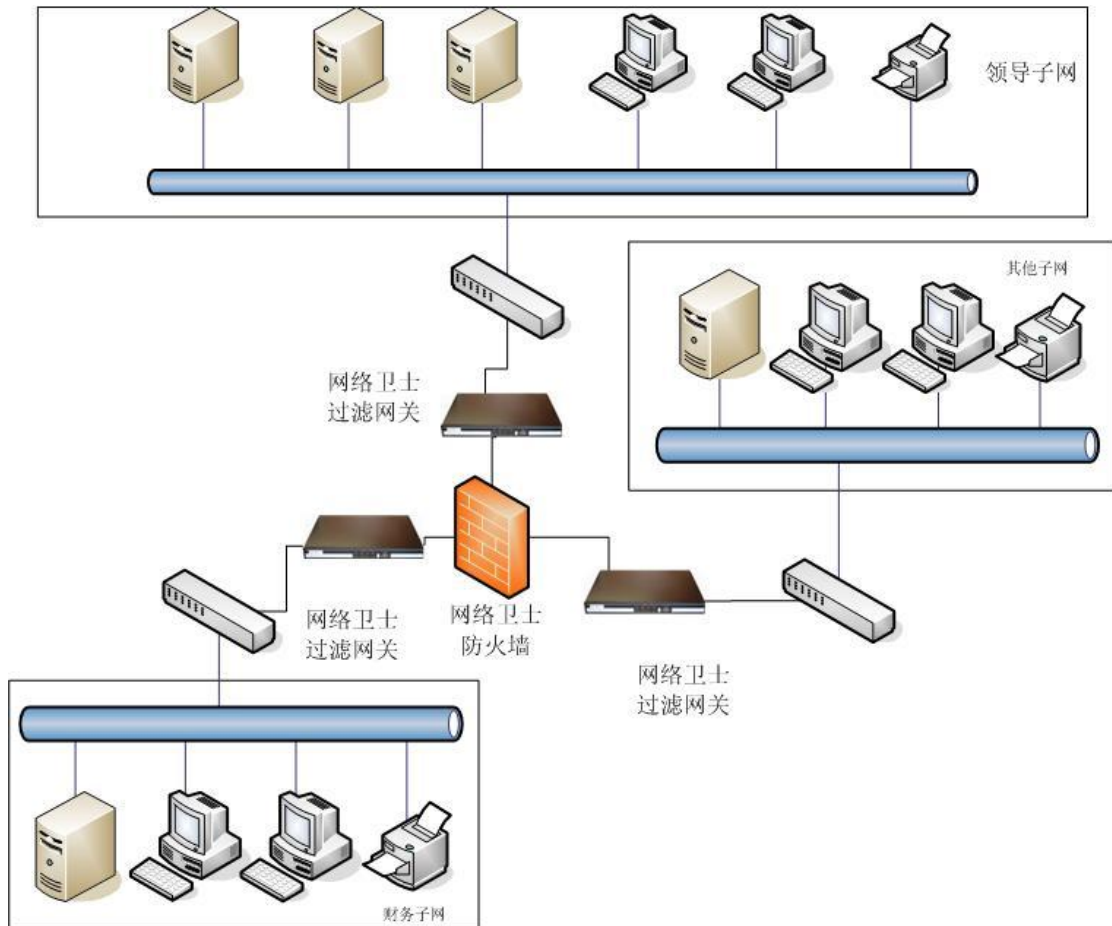
可以将网络卫士过滤网关部署在防火墙和中心交换机之间。网关是最合理和有效的部署位置，网络病毒往往从那里进入公司网络。将网络卫士过滤网关部署在网关处，可以在病毒进入网络并阻塞网络之前就清除它。



【图 4-1】 部署在网关处

2) 部署在分段的企业网络中

企业将网络分段有多种原因：有些企业是为了分割网络负载，有的是为了保护机密信息而把某个小组隔离开来，例如，财务部门与日常工作部门。



【图 4-2】 分段网络的保护

6 产品资质

证书名称	颁发单位
《计算机信息系统安全专用产品销售许可证》	公安部
《国家信息安全认证产品型号证书》	中国国家信息安全测评认证中心
《军用信息安全产品认证证书》	中国人民解放军信息安全测评认证中心

声明:

1. 本手册所提到的产品规格及资讯仅供参考, 有关内容可能会随时更新, 天融信恕不另行通知。
2. 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异,

此可能产生的差异为正常现象，相关问题请咨询天融信客户服务中心 400-610-5119 或者 800-810-5119。

3. 本手册中没有任何关于其他同类产品的对比或比较，天融信也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，天融信对此没有任何立场。
4. 本手册中提到的信息为正常公开的信息，若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。