Kaspersky Guard@Net 技术白皮书

防病毒网关

==========

Kaspersky Guard@Net

==========

卡巴斯基实验室

Kaspersky Lab

目录

一、前言：

Internet 技术带领信息科技步入了全新的网络时代，随着网络应用的广泛普及，特别是 Web 技术迅猛发展，人们越来越依赖于通过 Internet 获取各种资讯。电子邮件，即时通讯，视频影像资料，地图搜索，应用程序等数据资源，通过简单的浏览器操作即可随时获取，正所谓“网络在手，天下我有”。

同时，面对网络应用的爆发性增长，用户的计算机系统也面临着更复杂的安全风险。计算机病毒、木马、盗号程序、钓鱼软件、黑客软件等，都可能对使用计算系系统的组织机构或个人的信息安全,造成相当严重的损害。早期的病毒代码的主要意图是破坏计算机系统的软、硬件部件，使系统不能正常运行。现代的网络病毒更明显的向恶意软件发展，这种病毒以通过盗取个人或组织机构的私密信息，获取不正当利益为目的。由于有直接的经济利益驱使，这种行为对社会和计算机用户所造成的破坏性也更大。

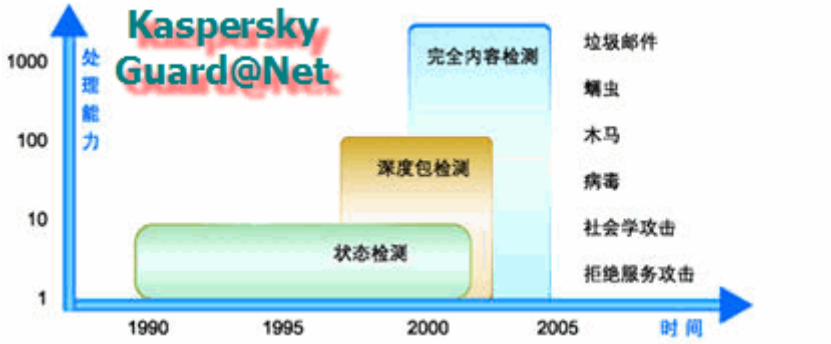
我们可以看到很多“成功”的攻击案例中，这些恶意软件的传播方式，已逐渐抛弃了通过传统的 E-Mail 传播，而通过广泛应用的 Web 服务实施传播和侵入，其隐秘性更强，破坏性也更大。谁能想到在浏览图片，观看视频影像资料的同时，恶意软件已利用系统漏洞，侵入了本地计算机系统，获取私密信息，而这一切又都是在“不知不觉”中发生的事实。

目前各个网络系统基本都配备有防火墙或入侵检测系统，作为保障组织机构内部网络安全的基础设施，此类系统所采用的技术通常是机械的数据报文检查和模式匹配技术。由于技术上的限制，这类系统对于网络流量中普遍存在的恶意软件只能“视而不见”。在很多“成功”的网络攻击案例中，都是在用户使用 Internet 下载应用程序，浏览图片或视频资讯的同时，被种植了盗号软件，木马程序等恶意软件。而这些受到侵害的计算机系统，通常又都是处于防火墙或入侵检测系统的“严密”保护中。这一现象，直接影响到网络安全业界的关注重心将转向如何在网络中检测并防御恶意软件的传播。

二、产品概述：

Kaspersky Guard@Net 系统就是针对网络安全所面临的新挑战应运而生的。Kaspersky Guard@Net 是一项针对病毒等恶意软件进行防御的硬件网络防护设备，可以协助企业防护各类病毒和恶意软件，对其进行隔离和清除。当企业在网络的 Internet 出口部署 Kaspersky Guard@Net 系统后，可大幅度降低因恶意软件传播带来的安全威胁，及时发现并限制网络病毒爆发疫情，同时它还集成了完备的防火墙，为用户构建立体的网络安全保护机制提供了完善的技术手段。

Kaspersky Guard@Net 系统为中小型企业及 ISP 提供了优秀的网络安全集成方案，广泛适用于政府、公安、军队、金融、证券、保险等多个领域。



三、Kaspersky Guard@Net 系统特性

强劲的恶意软件防护功能，Web 应用高效防护

Kaspersky Guard@Net 产品采用了独特的***虚拟并行系统*** 检测技术，在对网络数据进行网络病毒等恶意软件扫描的同时，会实时同步传送数据。这一技术的在系统中的应用，从根本上解决了以往对 Web 数据进行扫描操作时，普遍存在的性能瓶颈，在实际使用效果上远远超出了 ***“存储-扫描-转发”*** 的传统技术模式。

由于采用了***虚拟并行系统***技术，在保证不放过任何一个可能的恶意软件同时，大大减小了网络应用的请求响应时间，改善了用户体验效果。用户在使用 Kaspersky Guard@Net 系统对网络数据流量进行检测时，基本感觉不到数据扫描操作所带来的响应延迟，更不用担心错过精彩的网络实况播报。

适应于复杂的核心网络

Kaspersky Guard@Net 系统吸收了业界多年来在防火墙领域的设计经验和先进技术，支持众多网络协议和应用协议，如 802.1Q VLAN、PPPoE、802.1Q、Spanning tree 等协议，适用的范围更广泛，确保了用户的网络的“无缝部署”、“无缝防护”、“无缝升级”。

当 Kaspersky Guard@Net 设备处于透明工作模式时，相当于一台二层交换机。这种特性使 Kaspersky Guard@Net 产品具有了极佳的环境适应能力，用户无需改变网络拓扑，就可以零操作、零配置的升级到更全面的网络安全解决方案，同时也降低了因新增网络设备而导致的部署、维护和管理开销。

灵活的网络安全概念

Kaspersky Guard@Net 基于先进的安全区段概念实施安全策略的定制和部署，将从接口层面的访问控制提升到安全区段概念。Kaspersky Guard@Net 从概念上继承了传统防火墙的网络安全区域概念，也实现了很多突破。它默认各个安全区段间的安全级别是一样的，相互间的安全需求差异交由用户定制，为安

全策略的定制和部署提供了很大的灵活性，同时也避免了机械的将网络划分为 Internal，External 和 DMZ 的传统安全概念，能够完备灵活的表达不同网络、网段间的安全需求。

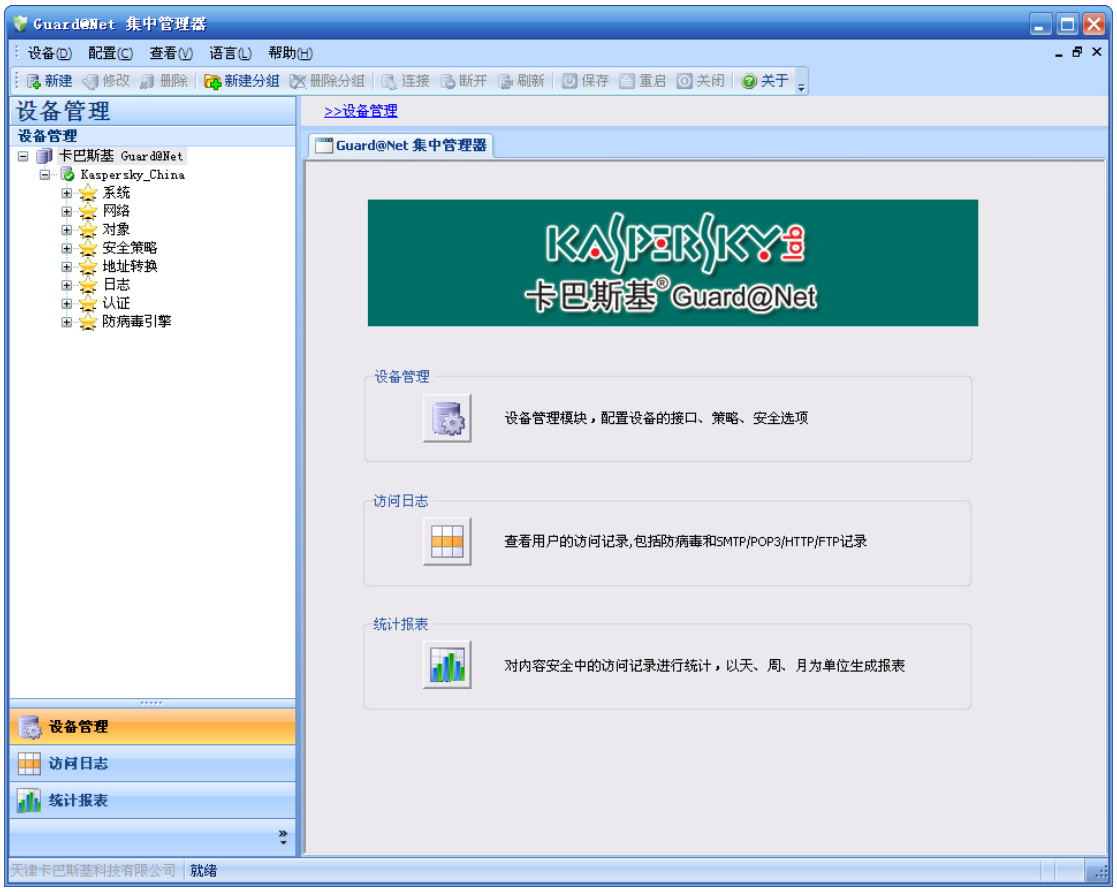
Kaspersky Guard@Net 系统还提供丰富的网络地址转换（NAT）功能支持，支持映像 IP 地址（MIP）、动态地址池的正向地址转换、反向地址转换。

集中管理，全局控制

Kaspersky Guard@Net 提供了功能强大的 Global Manager 图形化管理系统，该系统基于 Windows 平台运行。使用 Kaspersky Global Manager 系统，可以：

- ✓ 对多台不同地域的 Kaspersky Guard@Net 系统设备进行统一管理和配置
- ✓ 收集并审计分析多台 Kaspersky Guard@Net 设备发送的日志信息，包括事件日志，配置日志，安全日志和负载日志
- ✓ 对多台 Kaspersky Guard@Net 系统设备进行统一的固件升级，病毒库升级。
- ✓ 实时监控多台 Kaspersky Guard@Net 设备的运行状态和负载信息

如下图所示：



细致入微的系统日志和审计功能

Kaspersky Guard@Net 具备完善的网络访问日志记录和审计功能。

网络管理员在定制安全策略时，可根据需要，对网络行为、资源访问情况进行有选择地审计。当系统监测到有异常行为，病毒访问等事件时，将自动对其进行审计分析，以帮助管理员定制更完善的网络系统安全规则。

通过集成在 ***Global Manager*** 系统中的 ***Log & Report*** 模块，系统管理员可实时的查询系统提供的各类日志资讯。***Log & Report*** 模块还能对整个网络中的数据流量进行分析，极大的方便了系统管理员对设备日常运行情况，运行异常事件等进行进一步的审计和分析。

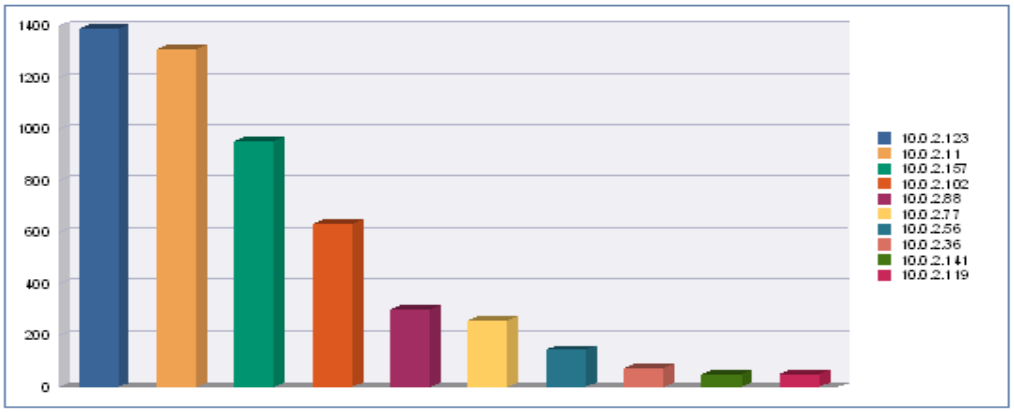
Log & Report 模块的审计效果图，支持缩放、二维，有鼠标移动提示，可以保存至本地，存储为 jpg 或 png 等格式，也可以导出为 HTML 格式。

如下图所示：

HTTP访问记录统计报表

打印日期： 2007-1-5　　上次修改日期： 2007-1-5

访问次数最多的前 10 名客户机



客户机	访问次数
10.0.2.123	1,388
10.0.2.11	1,311
10.0.2.157	954
10.0.2.102	632
10.0.2.88	301

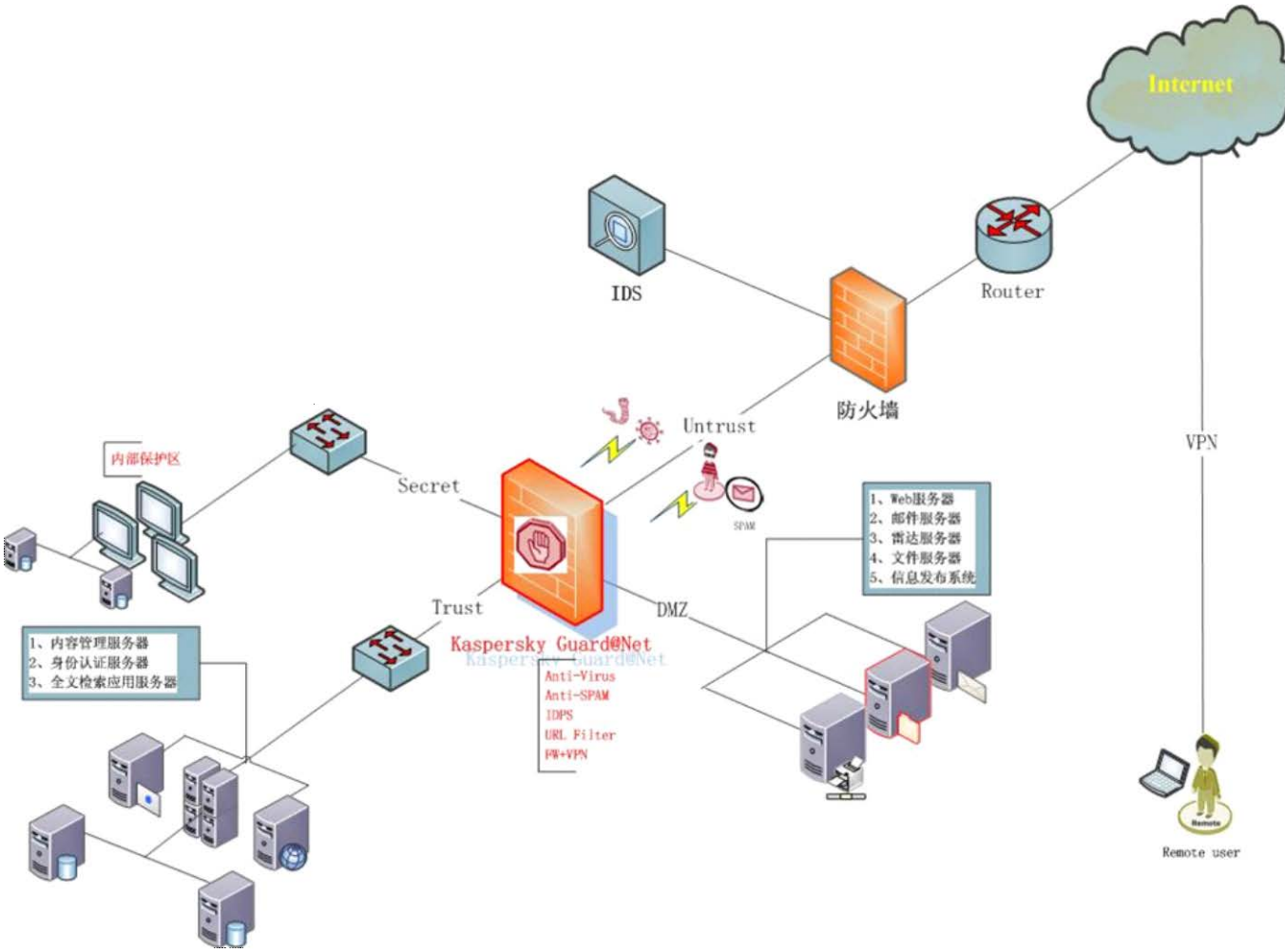
四、Kaspersky Guard@Net 系统规格

Kaspersky Guard@Net 系统		
类别	功能项	详细规格
网络安全性	工作模式	路由模式、透明模式、混合模式
	防病毒	支持对 HTTP,FTP,SMTP,POP3 四大协议防毒，对通过的数据进行在线病毒查杀，查杀邮件正文附件、网页及下载文件中包含的病毒
		病毒库自动更新，live update
		提供多种模式的扫描方式（快速，全面等不同级别）
		采用新一代的流模式扫描技术
	包过滤	基于状态检测的动态包过滤
		实现基于源/目的 IP 地址、源/目的 MAC 地址、源/目的端口、协议、时间等数据包快速过滤
		支持对时间，地址，服务定义对象和对象组
		支持不同功能区段的划分，区段间和区段内部策略的定义
	NAT	支持双向 NAT
		支持动态地址转换和静态地址转换
		支持多对一、一对多和一对一等多种方式的地址转换
		支持虚拟服务器功能
网络适应性	路由	支持静态路由
		支持 Vlan 路由，能够在不同的 VLAN 虚接口间实现路由功能。
		可有效地实现视频会议等多媒体应用
	VLAN	支持与交换机的 Trunk 接口对接，并且能够实现 Vlan 间通过安全设备传播路由
		支持 802.1Q，能进行 802.1Q 的封装和解封
		在同一个 Vlan 内能进行二层交换
		支持 802.1D 生成树协议。

	生成树	支持 ARP 代理、ARP 学习
	ARP	可设置静态 ARP
		支持 ADSL 接入功能，可满足中小企业的多种接入需求。
	接入	支持 PPPOE 拨号接入
		支持 Welf、Syslog 等多种日志格式的输出
安全管理	日志	支持通过第三方软件来查看日志
		支持日志分级，紧急、警报、错误、警告、通知、消息、调试、不记录日志
		支持对接收到的日志进行缓冲存储
		数据库备份
		支持网络接口监测、CPU 利用率监测、内存使用率监测、操作系统状况监测、网络状况监测、硬件系统监测、进程监测、进程内存监测、加密卡状况监测。
	监控	可根据配置文件进行错误恢复
		报警事件：内置了“管理”、“系统”、“安全”、“策略”、“通信”、“硬件”、“容错”、“测试”等多种触发报警的事件类
	报警	报警方式：采用邮件、控制台等多种报警方式，报警方式可以组合使用。
		支持 8 级优先级控制
安全系统	优先级	支持 OS 的备份
	双系统备份	支持硬件的 bypass
		支持生成树协议，Spanning Tree
	生成树协议	支持 STP 配置同步
		支持链路备份功能
	其它功能	支持双系统引导，当主系统损坏时，可以启用备用系统，不影响设备的正常使用

		支持本地配置、远程配置
		支持基于 SSH、SSL 的安全配置
		支持配置命令分级保护
	命令行	支持中英文切换
		支持命令超时、历史命令、命令补齐、命令帮助、命令错误提示等功能
		支持双系统升级，具有 Kaspersky Backup-Firmware 备份固件
	系统升级	支持远程维护和系统升级
		支持 TFTP 升级
		提供强大的报文调试功能，可以帮助网络管理员或安全管理员发现、调试和解决问题。
	报文调试	可以进行配置文件的备份、下载、删除、恢复和上载。
	配置恢复	系统内嵌第二个操作系统，提升整体可靠性，安全性。
		支持扩展 vpn，入侵防御检测，反垃圾邮件的模块
其它	扩展能力	

五、典型应用与解决方案


Internet
IDS
Router
防火墙
Untrust
VPN
内部保护区
Secret
SPAM
1、Web服务器
2、邮件服务器
3、雷达服务器
4、文件服务器
5、信息发布系统
Trust
DMZ
1、内容管理服务器
2、身份认证服务器
3、全文检索应用服务器
Kaspersky Guard@Net
Anti-Virus
Anti-SPAM
IDPS
URL Filter
FW+VPN
Remote user

六、服务支持

如果您想了解更多关于 Kaspersky Guard@Net 的详细信息，请登 www.itserv.net.cn，或直接拨打我们的客服电话：400-6863-683

深圳迪讯信息技术有限公司（防毒墙广东区总代）
地址：深圳市福田区福明路雷圳大厦裙楼 553 室,
电话 ：0755-28302121
传真： 0755-89208287
Email: service@dicent.com.cn