天清汉马防火墙技术白皮书

启明星辰信息技术有限公司
地址：北京市海淀区中关村南大街 12 号 188 信箱
电话：010-62149966
传真：010-62146778
网址：www.venustech.com.cn

目　录

启明星辰信息技术有限公司
地址：北京市海淀区中关村南大街 12 号 188 信箱
电话：010-62149966
传真：010-62146778
网址：www.venustech.com.cn

启明星辰信息技术有限公司
地址：北京市海淀区中关村南大街 12 号 188 信箱
电话：010-62149966
传真：010-62146778
网址：www.venustech.com.cn

安全问题在 IP 网络中的提出

网络期待服务质量、安全性、可信任性、可运营性

全球的电信网、因特网、企业网都正处在一个发展的关键阶段。人们面临网络建设方向的选择，期待服务质量(QoS)、安全性、可信任性、可运营性等一系列关键技术问题的解决。从目前电信网的发展看，第一，时分复用(TDM)技术已经不是未来的发展方向。时分复用设备虽然还在生产，但全世界的时分复用设备的研发已全面停止；第二，由于 ATM 的许多标准并未得到验证，因此它并不是未来的发展方向；第三，现在的 IP 网是基于传统的因特网理念，以用户自律为基础的网络，自由发展缺少管理，是一个非盈利的商业模型，因此，传统的因特网不会成为未来电信网的发展方向。

因特网对信息化的普及和发展起到了巨大的推动作用，是非常成功的。但是，由于因特网没有一个正常盈利的商业模型。网络缺乏有效的管理和运营手段，面临着诸如安全、服务质量等方面的问题，特别是无法有效支持实时业务成为限制其发展的最大障碍。

在企业网业务已经全面 IP 化之后，由于传统 IP 网的安全与服务质量难以得到保证，造成目前在企业网建设中 IP 数据网、视频网、语音网分别建设，大大增加了建网与管理成本。建设一个能承载综合业务，具有高服务质量保证、可管理、可控制、可信任特点的 IP 网络成为迫切的需求。

网络安全越来越重要

随着越来越多的人使用网络并通过网络获取信息、进行交流和沟通、参与网上贸易，网络对于当今中国社会的影响也愈来愈深、愈来愈广。从这个意义上看，网络化已经成为我国现代化进程中的一个重要特征。在网络不断发展、网民不断增加、网络应用不断拓展的同时，人们也面临着一个越来越显急迫、越来越显重要的问题：谁来关注网络安全？

据有关方面估计，目前我国 55%以上的计算机受到过病毒的感染，80%的中文网站缺乏完善的安全保护系统，经济部门 70%的信息安全设备来自国外，特别是我国网络系统和网络设备使用的关键芯片与核心软件大部分依赖进口，客观上留下了很大隐患。如果网络安全解决不好，不仅会造成巨大的经济损失，甚至会危及国家的安全和社会的稳定。

相对于高速发展的信息产业，中国的信息安全产品和服务市场发展滞后，这一现状已严重威胁到国家信息安全。作为信息安全产业的一部分，网络安全产业的整体状况与此相似。特别令人担忧的是：中国不仅有其他国家普遍存在的网络安全问题，还严重缺乏网络技术的自主性，在核心技术上一直依赖国外企业。有专家提出：从保障信息安全的国家战略出发，政府支持、引导企业开发和研制具有自主知识产权的网络安全产品，已刻不容缓，大力发展

自主的网络安全技术和产品势在必行。

从网络产品的结构看，防火墙软件和防杀毒软件仍然是目前网络安全软件市场中主要的安全产品，分别占据了市场份额的 33.3%和 39.0%。相比较而言，技术难度更大、资源整合更强的网络安全整体解决方案则显得明显不足。

网络安全的内容

信息安全产品体系结构

信息安全产品分为四个层次：基础安全设备、终端安全设备、网络安全设备、系统安全设备等。这些信息安全产品可以组成不同的行业安全解决方案。

信息安全产品体系见下图：

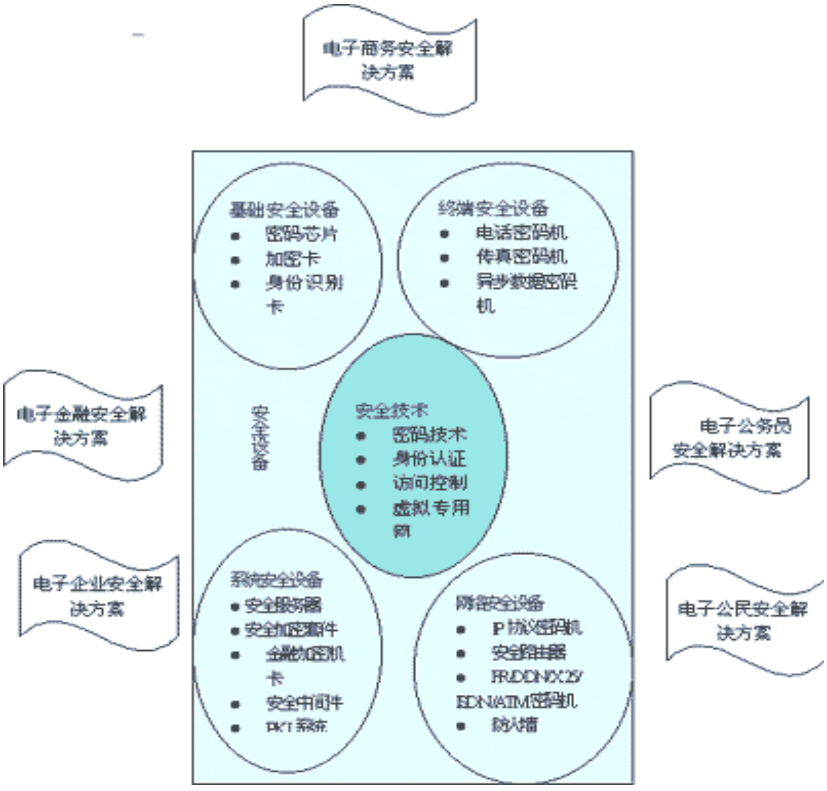


图1 安全产品体系结构

网络安全设备主要包括：防火墙、入侵检测、VPN、网关防病毒、流量分析整形、认证授权计费网关等。其中防火墙、入侵检测、VPN 和网关防病毒市场占有相对较高的几类产品。而网关防病毒往往又归入防病毒产品，作为一个相对独立的产品体系。

网络安全产品介绍

防火墙

防火墙是最主要的网络安全产品，目前所占的市场份额也最大。防火墙的技术也经历了一个比较长的发展过程，由最初的简单包过滤，发展到基于状态的包过滤，后来又发展到基于应用代理的包过滤，目前发展到基于状态包过滤、应用代理、内容过滤、集中管理的一种综合的网络安全产品。现阶段的防火墙已经不是一个传统意义上的防火墙，而是融合了入侵检测、实时防御、病毒内容过滤、VPN 加密隧道、以及路由、QoS、策略路由等网络特性的一个相对完整的网络安全解决方案。

IDS/IPS

IDS 即入侵检测系统，是一种对网络攻击行为进行检测预警的安全技术。作为防火墙的合理补充，入侵检测技术能够帮助用户检测、定位网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、攻击识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息。入侵检测被认为是防火墙之后的第二道安全防范措施，能够在不影响网络性能的情况下对网络进行监测。它可以防止或减轻网络上的安全威胁。

IPS 即入侵防御系统，是在准确检测网络攻击的基础上，自动进行访问控制的防御系统。网络入侵检测系统在诞生之初，仅仅是一个纯粹的审计型系统，它最大的问题在于只能检测攻击，但不能阻止攻击。后来逐步具备了一些阻断网络层攻击行为的能力，可以对 TCP、UDP 进行阻断，发展为主动式入侵检测系统，之后又发展为入侵联动系统。但入侵联动系统需要防火墙等其它设备的配合，增加了系统实施的复杂性。后来就逐步发展为网络入侵防御系统。入侵防御实际上就是一种入侵检测和防火墙的混合产品，将入侵检测和防火墙进行更紧密的结合。

VPN

VPN 即虚拟专用网络，为我们提供了一种利用公共网络实现企业内部专用网络的远程访问的安全连接方式。VPN 既可以是一个独立的网络安全产品，也可以是防火墙产品的一个功能组成部分，现阶段的绝大多数防火墙都将 VNP 功能作为了其标准的安全配置。

VPN 的技术有很多种，包括 PPTP、L2TP、IPSec、SSL VPN、MPLS 等，目前在网络安全领域应用最多的还是基于加密的 IPSec VPN。

隔离网闸产品

隔离网闸产品是一种新型的网络安全产品，应用于重要服务器和关键子网的入口处，在保持内外网络物理隔离的同时，进行适度的、可控的内外网络数据交换，提供比防火墙级别更高的安全保护，属于准物理隔离。与防火墙不同的是，隔离网闸产品是在安全隔离的基础上提供数据交换，而防火墙是在数据交换的基础上提供安全保障。隔离网闸产品主要适用于军事、政府、金融、安全机构等安全要求很高的行业，但其对业务的影响非常巨大，特别是交互型的业务，因此它的应用范围受到了极大的限制。

安全运营管理平台

安全运营管理平台并不是作为一个独立的产品出现，而是作为其它产品的管理、配置、信息整合工具。但随着安全方面网络管理的比重越来越大，集中统一、智能化的安全管理已显得越来越重要。业界提出了一个 SIM（安全信息管理）的概念，并有很多公司对在这方面进行了大量的实践，起到了很好的效果。

SIM 是指通过一个中央管理平台，收集整合来自各种各样安全产品的大量数据，并且从海量数据中提取用户关心的数据，呈现给用户，帮助用户对这些数据进行关联性分析和优先级分析。虽然 SIM 产品能处理各种安全工具的信息，但它们不能分辨其他的网络流量，而 NMS（网络管理系统）可以提供其它流量的信息，两者的融合给企业提供了一个完整的平台。

网关防病毒

网关防病毒产品不同于常见的基于主机的防病毒产品。传统的主机防病毒软件处理的对象是文件，而网关防病毒产品处理的则是网络数据包，因此，网关防病毒需要完全不同的防病毒引擎。

网关防病毒产品根据实现方式基本上分为两种，一种是通过协议分析还原技术对数据流进行应用重组，然后进行病毒特征匹配；另一种实际上就是代理服务器，相对前一种实现方式要简单的多，但性能的降低也是非常大的。

我们的安全解决方案

目前的网络安全产品更趋向于提供一个全方位的安全解决方案，这也是我们致力的方向。天清汉马防火墙就是基于这样一种设计思想，在高性能防火墙的基础上集成了 VPN、网关病毒过滤、Netflow 流量统计分析、AAA 认证计费等众多产品功能于一体，是国内第一

款 all in one 纯硬件防火墙，并具有电信级的性能和稳定性。

天清汉马防火墙可以为电信、邮政、政府、教育、能源、金融、企业等各部门现有的网络提供最有效、最彻底的保安措施，同时保证用户安全高速地访问全球公共资源。同时我们还为用户提供完善的网络安全管理解决方案和全面的安全服务，以便更好的满足用户的需求。

天清汉马防火墙功能特性

访问策略	状态包过滤
	链路层包过滤
	自适应安全包过滤
	安全策略预编译
NAT	源地址转换
	目的地址转换
	源端口转换（很少用到）
	目的端口转换
	源/目的地址转换支持地址池
	静态一对一双向地址转换
	服务器负载分担
	H.323 视频语音业务支持
工作模式	路由模式
	透明模式
	混合模式
路由特性	静态路由
	策略路由
	动态路由协议 RIP、OSPF
应用级过滤	透明应用代理
	网关病毒过滤
用户接入认证	WEB 认证，Portoal 页面推送
	802.1x 接入认证
	PPPoE 接入认证
用户认证策略	基于源或目的的认证策略
	基于业务的认证策略
用户认证与计费	本地认证、计费
	Radius 认证、计费
带宽管理(QoS)	1K 粒度用户带宽管理
	用户流量优先级控制
	流量整形及带宽分配
网络资源管理	系统总连接数限制

启明星辰信息技术有限公司
地址：北京市海淀区中关村南大街 12 号 188 信箱
电话：010-62149966
传真：010-62146778
网址：www.venustech.com.cn

	系统半连接数限制
	系统每分钟新建半连接数限制
	基于源主机的连接数限制
	基于目的主机的连接数限制
	系统连接老化时间自动调整
DHCP 特性	防火墙充当 DHCP 服务器
	防火墙作 DHCP 中继
	防火墙作为 DHCP 客户端
PPPoE	防火墙作为 PPPOE 客户端拨号动态获取 IP
VLAN 特性	VLAN 终结路由
	VLAN 透传
路由特性	静态路由
	策略路由
	动态路由协议 RIP
	动态路由协议 OSPF
防 IP 地址盗用	用户、IP 地址 、MAC 地址绑定
	ARP 代理
智能 TCP 代理	Intercept 模式
	Gateway 模式
防网络滥用	防 BT 下载
IDS 联动	支持 IDS 联动
网关病毒检测	可检测 5 万多种病毒
	支持 SMTP、POP3、IMAP 三种邮件协议
	发现病毒提示报警信息
	病毒事件实时监控、查询、统计、分析、报表
	病毒扫描引擎及病毒特征库实时在线升级更新
HTTP 内容过滤	HTTP 协议路由代理
	HTTP 协议透明代理
	URL 字符串模式匹配过滤规则
	域名过滤
	非法目录过滤
	URL 长度过滤
	二进制代码过滤
	请求属性过滤
	URL 重定向
	URL 地址自动 DNS 解析
	基于时间的 URL 过滤规则
	Method 过滤
	Script 过滤
	Applet 过滤

	Object 过滤
	Cookies 过滤
邮件过滤	发件人邮箱过滤
	发件人邮箱域名过滤
	收件人邮箱过滤
	收件人邮箱域名过滤
	SMTP 协议内容过滤
	附件名称过滤
	附件扩展名过滤
	邮件标题过滤
	根据发送人发送邮件的频率，防邮箱炸弹攻击。
	根据邮件特定的标题及附件名称，防病毒邮件攻击
	对符合过滤条件的邮件内容进行监控
	对所有邮件内容进行监控
二层隧道协议 L2TP	L2TP 用户本地认证、计费
	L2TP 用户 Radius 认证、计费
	客户端软件兼容
三层隧道协议 GRE Tunnel	组播及路由协议支持
三层隧道协议 IPSec	加密算法（DES、3DES、）
	高级加密算法（AES）
	L2TP 隧道加密
	GRE 隧道加密
	Hub&Spoke 集中器
	IPSec NAT 穿越
	动态多点 VPN
	同网络段 VPN 支持
	与第三方 VPN 的产品兼容
	硬件加密
灾难恢复	CF 卡引导
	网络引导
双机热备冗余备份	两台或多台防火墙互为备份
	“之”字型路由支持
	与其他支持 VRRP 的网络设备互为备份
负载均衡	两台或多台防火墙流量负载分担
	防火墙多出接口流量负载分担
命令行管理	Console（RS-232）
	Telnet
	SSH

	安全管理隧道
GUI 图形界面	安全管理隧道
	多域集中管理
分级管理	管理员权限分级
	功能模块配置权限分级
系统升级	Xmodem、Zmodem 方式
	TFTP 方式
	FTP 方式
	CF 卡方式
事件日志	实时监控
	实时报警（邮件、声音、手机短信）
	Syslog、SNMP 支持
	深层日志分析
	分析报表
	第三方日志接口
NetFlow	源主机的流量日志
	目的主机流量日志
	基于业务的流量日志
	防火墙接口流量日志
	TOP N 流量日志
	TOP N 连接日志
	流量或连接数的“基线”告警
管理功能	日志管理和日志审计
	支持图形界面 / 命令行安全管理方式

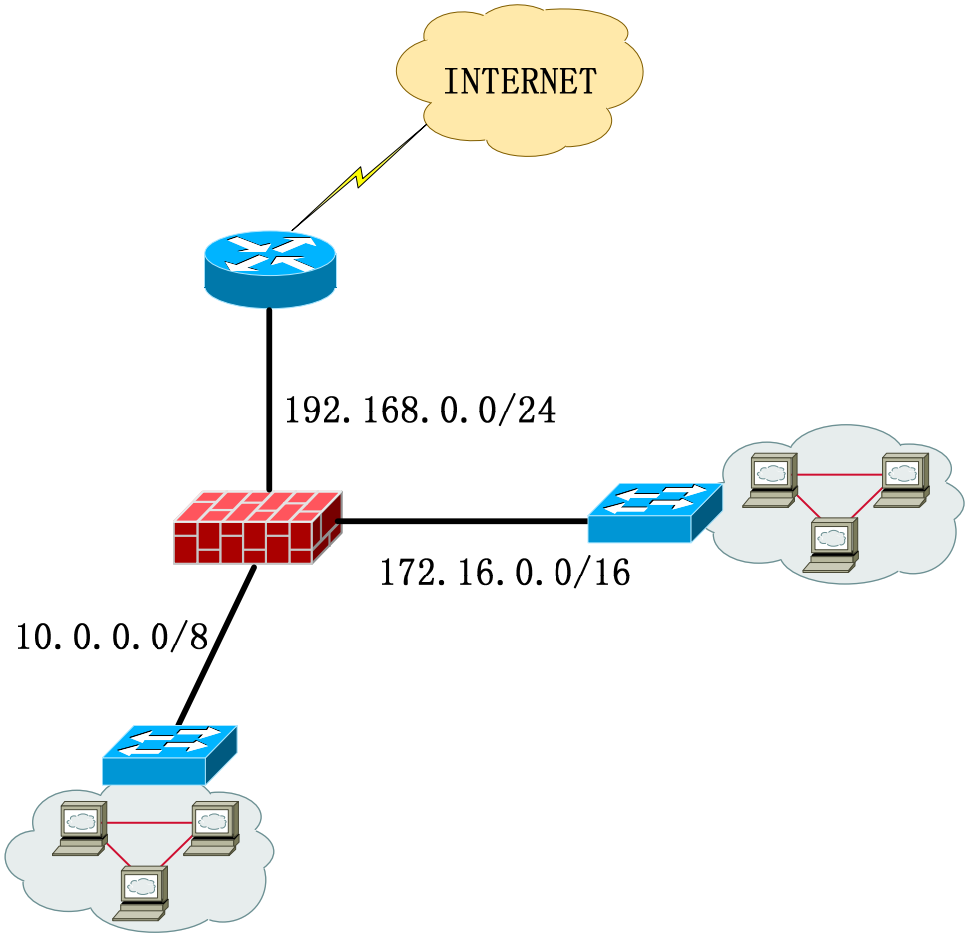
天清汉马防火墙安全产品主要功能

多样化的接入模式

天清汉马防火墙可以工作在路由模式、透明模式和混合模式。多样化的接入模式可以使天清汉马防火墙适合各种网络结构，满足用户的不同需求。

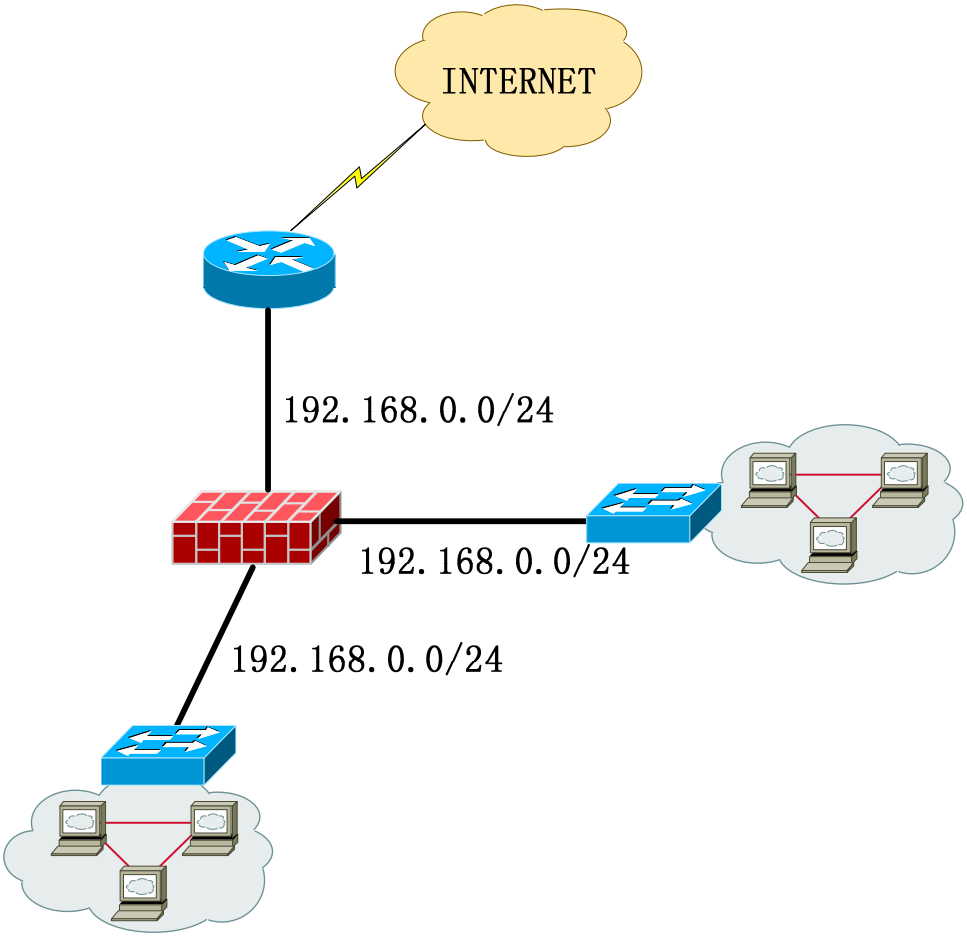
路由接入模式

路由模式是传统防火墙的工作模式，工作在路由模式下的防火墙可以让不同网段的主机通过路由转发的方式互相通讯。下图给出一个路由接入模式的典型使用环境。



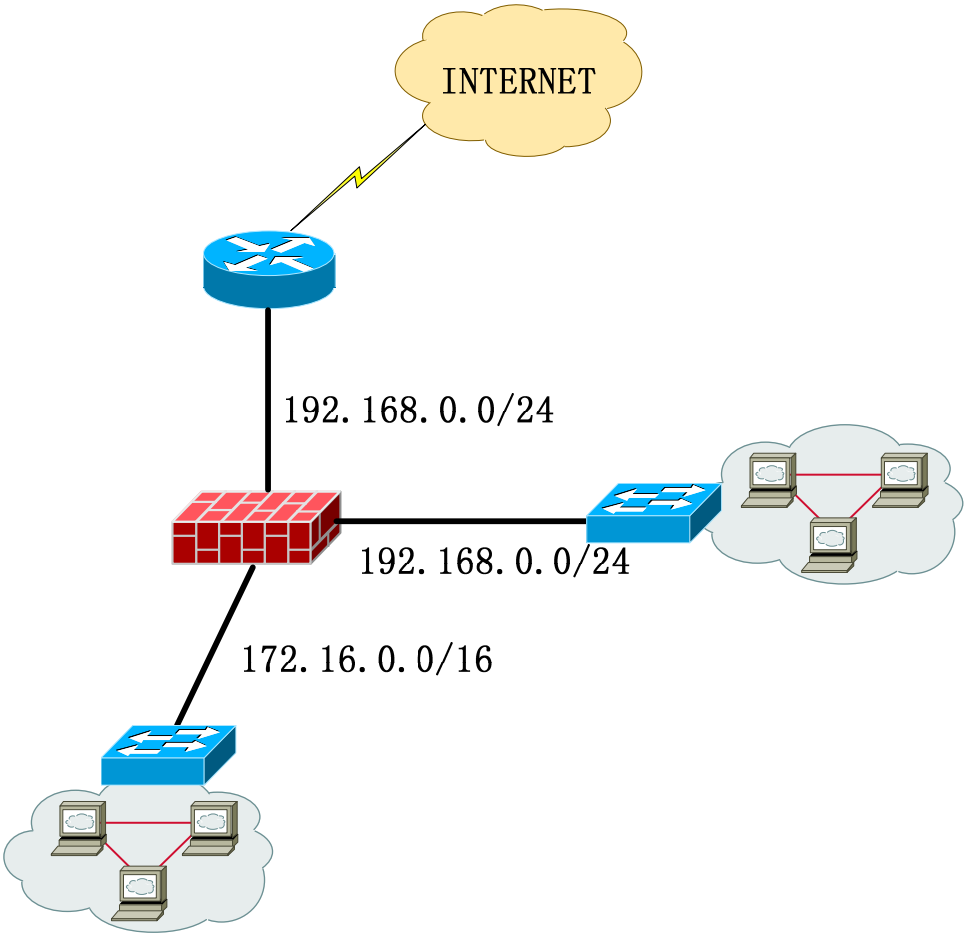
透明接入模式

天清汉马防火墙提供的透明接入模式，使防火墙很好的适应现有的网络拓朴环境，有时防火墙的架设是在网络运行以后，这时网络的配置已经完成，如果防火墙不能工作在透明模式的话，就需要重新更改大量的网络配置，更要重新调整路由器的设置，而使用透明模式能极大的提高防火墙的可用性，不需要更改内部客户端的网络配置，也不需要变动路由器的配置，就可以实现方便的架入天清汉马防火墙。下图给出一个透明接入模式的典型使用环境。



混合接入模式

路由模式和透明模式各有各的优点，但优点不能共存，工作在路由模式下的防火墙不能透明的接入已有网络中，而工作在透明模式的防火墙却不具有路由功能。天清汉马防火墙提供的混合模式融合了以上两种模式的优点，同一个网络接口既可以工作于透明模式，也可以工作在路由模式，用户可以根据自己的需要方便的配置，更加提高了天清汉马防火墙的可用性和适应性。下图给出一个混合接入模式的典型使用环境。



完善的防火墙功能

天清汉马防火墙提供的自适应安全过滤功能、基于状态的访问控制和资源控制、透明应用代理和内容过滤等功能，能够在不影响性能的情况下，更好的保护内部主机和网络的安全，防止 DOS 和 DDOS 攻击。

基于状态的包过滤技术

天清汉马防火墙的过滤模块位于 TCP/IP 网络协议的数据链路层和 IP 层之间，能够监控每一个通过网络的封包。天清汉马防火墙可以根据每个数据包的源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、协议、源端口、目的端口以及数据包通过的时间，决定是否对这个数据包予以放行，或者把它过滤掉。

一般的包过滤防火墙所看到的网络数据包是孤立存在的，允许和拒绝完全取决于包头的信息（源地址、目的地址、端口号等），是无状态的，对每个数据包都进行独立的规则检测，效率非常低，而且功能非常有限，无法真正实现对被保护区域的保护功能。

而天清汉马防火墙采用基于状态的包过滤，提供了更高的效率和安全性，通过跟踪网络包的状态来决定对网络包的处理（放行还是过滤），不仅考虑每个网络包，而且考虑网络包的历史关联性。在进行规则匹配时，将包的连接状态记录下来，同一连接的包，只检查第一个包，以后该连接的包就可以不用通过规则检查，而只需要检查状态表里该包所属的连接状态，如果该连接的包状态中显示已通过检查，表示该网络包属于已建立的合法连接，则不需要对该包进行检查，可以通过，同时更新状态表。这样就提高了包过滤的效率。

天清汉马防火墙基于状态的包过滤功能还可以通过状态表来实现截断所有进入一个特定被保护区域的通信，只允许那些由区域内部首先发起连接的网络包能够进入区域内部，从而更好的保护被保护区域的内部主机。

自适应安全过滤

天清汉马防火墙自适应安全过滤使用先进的安全域概念。天清汉马防火墙的每个接口（物理接口或虚拟接口）所连接的网络属于一个不同的安全域，天清汉马防火墙本身也作为一个安全域。每个安全域都有一个安全级别。

基于“安全域”的访问控制有效的解决了传统防火墙防内不防外的局限，可以把内网中具有不同安全等级的网段划分成独立的安全域，不同的安全域依据其安全等级设置安全级别，不需要添加过多的访问控制策略，就可以限制内网中安全等级低的网络对安全等级高的网络的访问。

即天清汉马防火墙在使用最简单的配置的情况下，提供了更加细粒度的安全访问控制，保证即使在安全级别比较低的区域中出现安全裂缝，也不会影响到其他安全域。

天清汉马防火墙本身也被看作一个安全域，因此我们能够更好的实现对设备本身的保护作用。

多访问策略下的高性能保证

一般防火墙在配置数目较少的访问策略（ACL）条目时性能很好，但由于实际用户的需要，在增加 ACL 条目后，性能却急剧下降。

而天清汉马防火墙却不存在这样的问题，它提供的 ACL 预编译功能可以保证，在配置很多条的访问策略（ACL）条目的情况下，天清汉马防火墙自身性能保持恒定，不会受到影响。

基于状态的资源控制

一般的防火墙产品在受到大量 DOS（Denial of Service）攻击时，会因为所有的连接资源都被攻击所占用，使得正常数据包无法通过设备，从而阻碍正常的通信。

一个好的安全产品，应该对自身的安全性和可靠性提出更高的要求。

天清汉马防火墙具有很高的对自身安全性和可靠性的保护，它提供的基于状态的资源控制功能，可以保证在天清汉马防火墙受到大量的攻击的时候，不会由于连接资源全部被占用，而阻碍正常的数据通信，还可以根据实际网络情况，限制一些内部主机的连接数目，保护这些内部主机，使其不受攻击。

天清汉马防火墙基于状态的资源控制功能，在以下几种情况出现时，通过监视所有连接的状态，限制特定协议的连接数目和高低警戒线，能够有效的防止天清汉马防火墙设备浪费连接资源，同时保证正常数据通过：

- 连接长时间没有应答，一直处于半连接状态；
- 连接已经建立，但长时间没有数据穿过；
- 设备受到半连接攻击；
- 墨中协议的网络病毒存在；

天清汉马防火墙还可以通过限制发起连接的外部主机的连接数，以及被访问的内部主机或内部主机某个端口的连接数，保护某些内部主机，使其不受攻击。

VPN 功能

VPN 技术通过建立加密隧道进行加密通信，形成虚拟专用网在异地局域网间通过互联网提供安全可靠的网络使用环境。它可以节省企业的通信费用，特别是替代企业已有的专线，并且提高企业网络的可管理性，降低企业的通信成本。

天清汉马防火墙集成了 VPN 功能，能够个用户提供更完备的安全解决方案。

天清汉马防火墙提供 IPSEC VPN 和 L2TP 功能。

天清汉马防火墙的 IPSEC VPN 支持 NAT traversal、DPD、X.509 认证等功能。

实现的算法包括：MD5、SHA1、512 位 SHA2、DES、3DES、AES（128/192/256 bit）、TWOFISH、CAST、BLOWFISH

强大的 NAT 功能

天清汉马防火墙可以为用户提供完整的地址转换解决方案，它同时支持基于源地址转换的 NAT（包括 dynamic NAT、PAT 和 static NAT）、基于目标地址转换的 NAT。天清汉马防火墙可以解决企业公有网络地址不足的问题，隐藏内部网络结构，还可以实现负载均衡功能。

基于源地址的 NAT

基于源地址的NAT可以用于在内部网络用户访问公有网络地址时将内部网络用户使用的内部IP地址转换为公有网络地址。这样的实现不仅可以解决企业公有网络地址不足的问题，同时对公有网络来说，访问全部是来自于经过防火墙转换后的地址，并不认为是来自内

部网络的某个地址，可以有效的隐藏内部网络结构，减少对内部的攻击。

Dynamic NAT指动态的将源地址转换映射到一个相对较小的地址池中，对于同一个源IP地址，不同的连接可能映射到地址池中不同的地址；

PAT是指将所有源地址都映射到同一个地址上，通过端口的映射实现不同连接的区分。

Static NAT是一种一对一的双向地址映射，主要用于内部服务器向外提供服务的情况。在这种情况下，内部服务器可以主动访问外部，外部也可以主动访问这台服务器，相当于在内、外网之间建立了一条双向通道。

天清汉马防火墙除支持以上三种基于源地址的NAT外，还支持基于目标地址的NAT。

基于目标地址的 NAT

基于目标地址的 NAT 是一种单向的针对目标地址的映射，主要用于内部服务器向外部提供服务的情况，它与 static NAT 的区别在于它是单向的。外部可以主动访问内部，内部却不可以主动访问外部。

如果内部网络用户对公有网络提供访问服务（如 Web 、FTP 等）的服务器地址是保留 IP 地址，或者想隐藏服务器的真实 IP 地址，就可以使用基于目标地址的 NAT 来对目的地址进行转换，这样能有效的隐藏内部服务器信息，对服务器进行保护。

还可以使用天清汉马防火墙基于目标地址的 NAT 实现负载均衡的功能，它即可以将一个目标地址转换为多个内部服务器地址；也可以通过

DHCP 服务器和 DHCP 中继功能端口的映射将不同的端口映射到不同的机器上。

天清汉马防火墙提供的DHCP服务器与DHCP中继功能能够很好的满足用户的需求。

对于没有架设DHCP服务器的企业，天清汉马防火墙的DHCP服务器功能可以省去企业为单独设置DHCP 服务器所消耗的成本，并且为用户统一分配IP 地址、子网掩码、默认网关、DNS 等必要网络参数，方便了网络的统一管理。

天清汉马防火墙的任意接口都支持DHCP 服务器功能，不限于内网。

对于已架设DHCP服务器的企业，天清汉马防火墙的DHCP中继功能能够使企业继续使用原有的DHCP服务器分配地址，尽量少的更改用户的配置。

接入认证

天清汉马防火墙将接入认证功能与防火墙功能、入侵检测功能有机的结合起来，提供更完善的解决方案。

天清汉马防火墙提供健全的用户安全保证措施以及方便的用户管理措施：

1. 异常断线监测，使用 KEEP-ALIVE 报文，定时在天清汉马防火墙和用户之间发送，误差不超过 1 秒，当天清汉马防火墙检测到用户异常下线会向 Radius 记帐服务器发送结束记帐信息，保证用户记帐信息的完整性和可靠性。

2. 最大闲置时间监测，当用户在这段时间内没有任何流量发生，天清汉马防火墙会自动认为用户下线，从而发送结束记帐信息，从而不会发生由于用户遗忘而造成超长话单的问题。

3. 最大会话时间闲置，用户可以在 Radius 认证服务器上为每个用户设定一个最大会话时间限制，当到达这个时间，天清汉马防火墙会强制用户下线，不会造成用户滥用网络资源情况。

天清汉马防火墙可以在本地或 RADIUS 服务器对接入认证用户进行认证、授权和计费。天清汉马防火墙提供以下三种接入认证方式

WEB 接入认证

用户不用安装客户端软件，当用户使用 IE 时，如果用户没有通过认证，用户访问任何 URL 时将会被强制到认证页面，用户只有通过认证后才可以正常使用网络资源。当用户认证通过后可以给用户推送门户页面。

WEB 接入认证支持 CHAP、PAP 认证。

PPPoE 接入认证

用户使用 PPPoE 客户端进行认证，只有通过认证的用户才可以正常使用网络资源。当用户认证通过后可以给用户推送门户页面。

PPPoE 接入认证支持 CHAP、PAP、MS-CHAP、MS-CHAPv2 认证。

802.1x 接入认证

用户使用 PPPoE 客户端进行认证，只有通过认证的用户才可以正常使用网络资源。

802.1x 接入认证支持 EAP、CHAP 认证。

NetFlow

NetFlow 技术为 Cisco 发明的技术，能够有效地提供网络流量测量，包括流量计帐和分析，基于应用的计帐和分析，也可以根据网络流量分布来查看网络带宽，是否足够以便升级网络，或者监视网络分析是否受到 DOS 攻击。

NetFlow 能够提供非常有价值的信息：当前什么用户在使用网络，什么应用，什么时间段利用，以及网络流量的流向。NetFlow 可以把设备通过的流量以 UDP 包形式发送给收集器，由收集器收集并分析、整理，提供给网络管理员整个网络利用情况，可以做到实时收集实时分析，随时掌握整个网络。

天清汉马防火墙支持版本 5，与 Cisco 兼容。

QoS 功能

天清汉马防火墙提供 PQ、DDR 等多种 QoS 机制，还可以实现按接入认证用户保证服务质量。天清汉马防火墙按接入认证用户保证服务质量功能采用灵活的匹配引擎，可以按用户名、用户组、特征字以及用户级别实现匹配。

天清汉马防火墙不但能够保证高优先级的数据得到优先处理，而且能够对高优先级的数据进行带宽限制，这样能够防止高优先级的数据占用所有的带宽，而导致低优先级的应用“饿死”。

天清汉马防火墙的 QoS 功能可以支持 16K 用户。

冗余备份功能

恢复性和冗余性已成为当今网络交换中的重要特性，目前指定缺省网关一般有两种方法，一种是使用如最短路径优先（OSPF）协议或路由信息协议（RIP）等动态路由协议来确定正确的缺省网关。 动态路由协议能够绕过任意故障点来选择最佳网关，但是对终端系统的处理开销较大，而且收敛过程慢。另一种方法是使用静态配置的缺省网关来减少处理开销。目前许多终端系统都是使用这种方法来来实现默认网关配置。但这种方法的风险是使作为缺省网关的路由器成为单一故障点。这就意味着终端系统无法快速知道路由器和与之相联的局域网连接是否已经失败，而且系统检测链路失败与替代路由器进行交换需要很长时间。这对于使用缺省网关进行广域网接入或访问其它局域网网域的终端系统来说是一场灾难。

对于需要网络可靠性高的业务，天清汉马防火墙采用虚拟路由冗余协议(VRRP) 提供冗余备份功能。

VRRP 协议介绍

VRRP 协议被设计运行于具有多播能力的局域网中，给局域网中的主机提供网关备份功能。使用 VRRP 可以将局域网中的多个路由设备（包括天清汉马防火墙）配置为互相之间作路由备份的虚拟路由器组，该组中的所有路由器采用 VRRP 协议来实现路由器之间以及路由器与所在局域网之间的镜像。如果一台路由器出现故障，其它的路由器会自动代替失效的路由器绕过故障点重新路由，路由的恢复时间仅在数秒之内，且此过程对于终端系统是透明的。

VRRP 路由器有两种状态：主路由器和备份路由器。VRRP 在路由器组中根据一定规则选出一台作为主路由器，负责转发数据包。其他路由器则作为备份路由器。主路由器通过定时发送 VRRP 通告包来与其他备份路由器通信，以保证备份路由器及时了解主路由器的状态。正常情况下，备份路由器不处理发往虚拟路由器的数据包。当主路由器发生故障时，备份路由器在一定的时间内没有收到主路由器发送的 VRRP 通过包，就会迅速转换成主路由器，接管主路由器的工作，从而将对路由转发功能的影响减到最小。这样就提供了在故障发生时快速、有效的解决方法。

天清汉马防火墙冗余备份功能实现

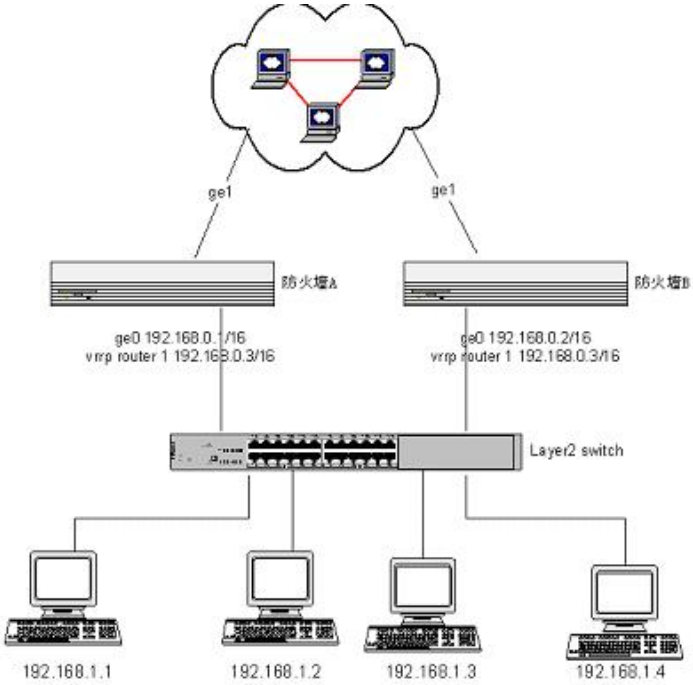
参与冗余备份的几台天清汉马防火墙使用同一个虚拟的 IP，通过配置 VRRP 虚拟路由器的优先级选举出主控设备；首先由主控设备对请求进行应答，并真正工作；　　天清汉马防火墙通过 VRRP 通告报文探测其它设备的运行状况，一旦探测到主控设备出现故障，备份设备就会迅速接管主控设备，不会影响到任何数据包的路由转发和处理，这样就提供了在故障发生时更快、更有效的解决方法，进一步提高了关键业务运行的可靠性。

典型配置

案例描述

防火墙 A 和防火墙 B 的接口 ge0 上启用一个 VRRP 虚拟路由器，ID 为 1。这样防火墙 A 和防火墙 B 的接口 ge0 可以相互备份。
防火墙 A 接口 ge0 的 IP 地址是 192.168.0.1/16，防火墙 B 接口 ge0 的 IP 地址是 192.168.0.2/16。VRRP 虚拟路由器 1 的虚拟 IP 为 192.168.0.3/16。局域网中的主机都将默认网关设为 VRRP 虚拟路由器 1 的虚拟 IP 地址 192.168.0.3/16。

案例组网图



启明星辰信息技术有限公司
地址：北京市海淀区中关村南大街 12 号 188 信箱
电话：010-62149966
传真：010-62146778
网址：www.venustech.com.cn

负载均衡

天清汉马防火墙基于目标地址的 NAT 功能可以实现服务器负载均衡功能，VRRP 可以实现设备本身的负载均衡。

对于访问流量比较大的 WEB、MAIL 等服务器的负载均衡，可以通过将一台 WEB 服务器使用几台 WEB 服务器来代替，每台 WEB 服务上的内容完全相同，他们具有不同的内部服务器地址。用户访问 WEB 服务器时使用的是 WEB 服务器的外部地址，这几台 WEB 服务器的外部地址完全相同，这样通过天清汉马防火墙基于目标地址的 NAT 功能，当用户访问 WEB 服务器时，天清汉马防火墙就会将 WEB 服务器的外部地址转换成多个内部服务器地址，每个用户的访问流量，甚至同一用户每次的访问流量都会被方法给不同的 WEB 服务器，这样就减轻了每台 WEB 服务器的负担；

对于为了节省 IP 地址等原因，将 WEB、MAIL、FTP 等服务由同一台服务器来完成的情况，也可以通过天清汉马防火墙基于目标地址的 NAT 功能，将 WEB、MAIL、FTP 等功能由不同的服务器来完成，不同的服务器具有不同的内部服务器地址，但是他们都具有一个相同的外部地址，这样当用户访问这一外部地址不同的功能时，天清汉马防火墙就可以通过端口的不同，将外部地址转换位不同的内部服务器地址。

对于天清汉马防火墙自身的负载均衡功能，可以通过 VRRP 来实现。将两台天清汉马防火墙 A、B 都加入两个 VRRP 虚拟路由器 1、2，天清汉马防火墙 A 作为 VRRP 虚拟路由器 1 的主控设备，而天清汉马防火墙 B 作为 VRRP 虚拟路由器 2 的主控设备，将内部网络中的一部分主机的默认网关设为 VRRP 虚拟路由器 1 的虚拟 IP 地址，另一部分主机的默认网关设为 VRRP 虚拟路由器 2 的虚拟 IP 地址，这样就可以实现天清汉马防火墙自身的负载均衡功能。

细粒度的分级管理

天清汉马防火墙实现细粒度分级管理，对于管理员按照可以行使的权限分为 16 个级别，不同级别的管理员具有不同的权限，具有最高级别的管理员叫做超级管理员，只有超级管理员才可以修改管理员信息，不具有最高级别的管理员不能修改系统的管理策略。

超级管理员可以定制天清汉马防火墙各个配置功能的级别，低级别的管理员不能使用级别高的配置功能，从而可以更好的防止有人恶意更改防火墙安全策略。

日志审计功能

天清汉马防火墙提供丰富的日志信息，用户可根据特定的需要进行日志选项（不做日志、记录某一类型的日志等），天清汉马防火墙使用模块化的日志结构，采用模块、级别和处理方式相结合的方式配置日志，可以对单一模块、多个模块的组合以及所有模块指定处理方式。

天清汉马防火墙日志主要分为以下几类：

管理日志、包过滤日志、代理服务器日志、入侵监测日志、NetFlow日志，提供从Debug到Emergency 的八种级别的日志信息。

天清汉马防火墙日志可以实时传送到Syslog日志服务器，为用户提供方便的日志过滤筛选、相关性分析、日志审计备份等功能。

告警功能

天清汉马防火墙支持丰富的告警方式，给管理员提供多种手段了解网络运行安全情况及防火墙系统自身运行情况。管理员可以依据管理的方便性灵活的定制哪一类报警信息使用哪种告警方式。主要有以下3种方式：

振铃：　　以响铃方式通知管理员

短信：　　通过向管理员设定的手机号码发送短信来发送报警信息

电子邮件：　通过向管理员设定的电子邮件帐号发送电子邮件来发送报警信息

网关病毒过滤功能

网关防病毒功能是在网关处对通过的网络数据流进行病毒扫描以保护用户网络不受计算机病毒的侵害。网关防病毒与主机防病毒的最大区别在于主机防病毒产品保护的范围仅仅是所在主机自身上的文件系统，而网关防病毒保护的范围则是用户网络中的所有主机，同时还可以避免网络内部的主机主动传播病毒到网络外部的主机。

近几年接二连三涌现出来的对全球网络造成严重危害的一些网络蠕虫病毒，如：“红色代码”、“尼姆达”、“SQL蠕虫王”“冲击波”、“振荡波”等，无一例外的结合了蠕虫病毒和黑客程序的双重特性，利用一些已知的系统漏洞进行传播破坏，给网络用户造成了无法估量的损失。可以说蠕虫病毒和黑客程序相结合的模式已经成为未来病毒的一个发展趋势，而且会愈演愈烈。对于这种病毒，单纯的防火墙或单纯的防病毒网关都无法做到很好的防范，必须要防火墙和防病毒网关的整合产品才能有效解决。

单纯的防火墙并不能阻止计算机病毒进入网络内部，网络用户对病毒的防护一般依靠在网络内部的所有主机上安装主机防病毒产品来提供最后也是唯一的保护。需要注意的是主机防病毒产品是一种需要普通用户经常维护和管理的软件，如果没有经常的维护和病毒库的更新等，主机防病毒产品所能提供的保护是无法得到有效保证的。但是如果由网络管理员统一对网络主机的防病毒产品统一进行更新和升级，则因为工作量巨大，很难完成。实际上维护一台电脑的软硬件，特别是维护软件系统正常运行是一项艰巨、枯燥、极耗时间和精力的工作。一般一个网管人员能够维护25台主机软硬件的维护就已经是超负荷了，而在现实的企业网络环境中，平均一个网管人员要照顾的主机数目通常上百台。这就进一步造成了使用单机防病毒软件的局域网，只要达到二三十台主机以上，对病毒侵扰就基本上处于不设防状态。

网关防病毒功能很好的解决了这种困境，一方面可以大大降低网络管理的成本，另一方面则因为可以进行统一的升级等维护工作的特点，大大提高了网络内部计算机对病毒的防护能力。

网关防病毒不同于常见的基于主机的防病毒。传统的主机防病毒处理的对象是文件，而网关防病毒处理的则是网络数据包，因此，网关防病毒需要完全不同的防病毒引擎。

网关防病毒的实现方式基本上分为两种，一种是通过协议分析还原技术对数据流进行应

用重组，然后进行病毒特征匹配；另一种实际上就是代理服务器，相对前一种实现方式要简单的多，但性能的降低也是非常大的。天清汉马的防病毒功能采用的就是第一种实现方式，目前支持最常用的三种邮件协议的病毒检测，包括SMTP、POP3和IMAP。

天清汉马防火墙的网关病毒过滤功能是真正意义上的防病毒网关，而不像某些产品所号称的具有防病毒功能，但实际上仅仅能够阻挡一些由网络蠕虫病毒发出的攻击包，却无法过滤通过网络传播的病毒文件。

天清汉马防火墙最大的功能特点就是把防火墙和网关防病毒等功能有机地整合在一起。这对于防止像“红色代码”、“尼姆达”、“SQL蠕虫王”、“冲击波”、“震荡波”等利用网络安全漏洞，通过网络攻击进行传播的恶性病毒非常有效。因为现在的病毒发展趋势是越来越多的同时具有蠕虫病毒和黑客攻击程序的双重特性(这种病毒的典型特征之一就是一般都会体现在网络的异常上)，防病毒软件仅仅能够对单纯的病毒进行查杀，但是对于黑客的攻击则根本无能为力，因为这种攻击是通过一些安全漏洞进来的，就像一扇有许多窟窿的大门，如果没有防火墙的保护，那么各种各样的网络蠕虫病毒就可以通过这些窟窿不断的从互联网上涌进来，防病毒软件在门里是无论如何杀不完的，这就是为什么现在很多企业在部署了网络版防病毒软件之后，仍然会遭到病毒的攻击而导致网络不正常甚至瘫痪的原因所在。因此，只有在防火墙和网关病毒过滤协同工作时才能够对这些黑客型网络蠕虫病毒进行有效的防治和查杀。

单就防病毒技术来说，天清汉马的大容量病毒库以及高效而多样的检测方法相是其它同类产品所无法比拟的。具体来说：

1、 病毒库

当配置病毒扫描时，天清汉马防病毒扫描引擎提供两种扫描方式分别对应两种病毒库：

1) 标准病毒库：这个病毒库覆盖了超过30,000 多种病毒，一般情况下用户选择这一病毒库即可有效地过滤掉常见的绝大多数的病毒。
2) 扩展病毒库：这个病毒库覆盖了超过50,000 多种病毒，基本上包括了所有已知的病毒。

2、扫描引擎

天清汉马采用国际先进的新一代病毒扫描引擎技术，以巧妙而精确的算法保证了在检测大量病毒时仍然保持高速而准确的检测结果。天清汉马防病毒扫描引擎主要采用了以下几种常用的检测方法：

（1）特征码识别法

特征扫描通过扫描目标文件，查找已知的标识病毒特征的字符串(byte-string)。 如果某一特定病毒的所有字符串都匹配, 则认为该文件中感染了此病毒。

（2）广谱特征码

原本的特征码是病毒中一串有这种病毒自己特色的指令序列，然而对多形性病毒情况就没这么简单，大量的多态病毒不同形态之间甚至没有超过三个连续字节是相同的。为了对付这种情况，首先特征码的获取不可能再是简单的取出一段代码来，而是分段的，中间可以包含任意的内容(也就是增加了一些不参加比较的“掩码字节”，在出现“掩码字节”的地方，出现什么内容都不参加比较)。

（3）启发式扫描

启发式扫描是根据对标示病毒行为的字符串进行扫描。例如，在下面的程序段中：

8f02bcc87fd0a25b7052744bbab670b59ad157bc74288d8367a524675

病毒扫描引擎能匹配下面的特征：

8f02bcc * 4675 - 该程序打开一个文件。

8f ?? 524675 - 该程序终结自身。

天清汉马防病毒扫描引擎还采用了一些比较先进的检测方法，如：

（1）OLE分离技术

宏扫描从MS Office文件中提取宏， 根据已知的宏病毒字符串对宏进行检测。同时， 对宏中的代码行为进行分析，识别宏病毒。

（2）病毒脱壳技术

天清汉马防病毒扫描引擎可以对加壳的病毒先进行脱壳，然后再进行检测。

（3）压缩格式病毒检测技术

天清汉马防病毒扫描引擎不但能够检测普通格式的病毒，还能够查杀多种压缩格式的病毒，如ZIP，GZIP，RAR，ARJ，ARC，LZH，CAB，ZOO，TAR和CHM等。

（4）木马、黑客程序检测技术

针对网络上流行的木马、黑客程序，天清汉马防病毒扫描引擎采用了独特的特征&行为双重检测技术，可以对其进行有效的阻断。

（5）高速的协议分析、还原和内容检测技术

天清汉马防病毒扫描引擎采用先进的高速协议分析、还原和内容检测技术，通过精心设计的算法保证了在检测大量病毒时仍然保持高速而准确的检测结果。