

中科神威防火墙V4.0

技术白皮书

**北京中科网威信息技术有限公司**

**2018年7月**

# 前言

自2009年Gartner定义下一代防火墙以来，下一代防火墙在安全业界得到了很蓬勃的发展。

但是，当前下一代防火墙宣传大多是围绕着统一检测引擎、基于应用深入检测、流量可视等功能点，都只是对于UTM产品某一个或几个功能点的强化，这些对于客户的网络安全防护没有革命性的突破，无法满足当前网络大变革环境下的安全防护需求。

中科网威认为，防火墙要能称之为“下一代防火墙”（下一代防火墙，Next Generation Firewall），首先要满足虚拟化网络安全防护的需要，面向数据中心、私有云及共有云的云安全需求，并且彻底摒弃网关与终端的割裂式孤岛安全防护，为客户提供完整的、简单易用、低成本的安全防护解决方案。

因此，中科网威推出了“下一代防火墙”，不仅在统一检测引擎、基于用户、应用、内容的细粒度安全控制、一站式配置、流可视等方面具有优势，更重要的是面向云计算、面向虚拟化、面向未来，立足于云安全，为数据中心、公共云和私有云提供安全防护解决方案。

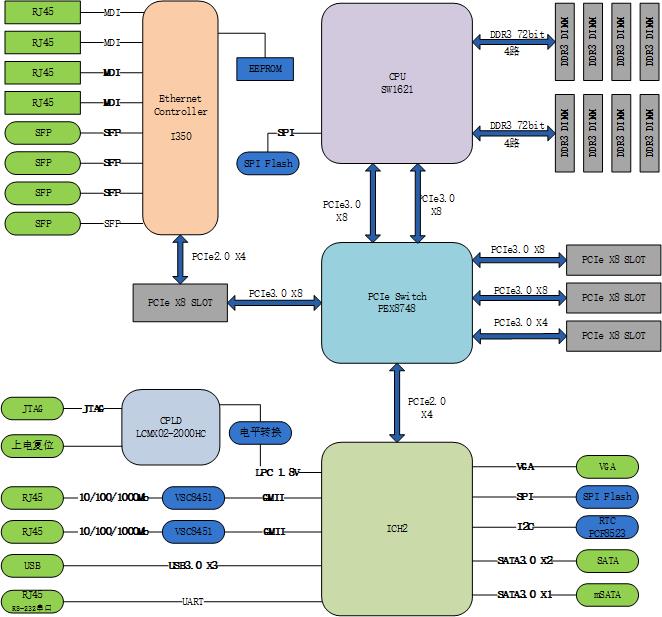
最新发布的中科神威系列安全产品在功能完善性、稳定性和性能上做了很大改进，支持态势感知地图上显示网络安全事件热点，让网络安全管理员全面掌握全网安全势态。

# 中科神威防火墙

## 主要技术

### 国产自主可控软硬件平台

中科神威防火墙系列的硬软件完全由中科网威自主设计，其中硬件平台的核心处理器采用了目前国内性能最好的第三代申威处理器SW1621，该处理器采用28nm生产工艺，16核，主频2.0GHz，每秒浮点运算次数高达512G，采用64位自主精简指令集，对溢出式攻击和恶意代码有天然的免疫能力。同时采用的为配合申威处理器而专门研制的申威国产IO套片集成了PCI-E 交换功能、桥片功能和I/O功能，支持多种通用高速接口和低速接口并具有片上智能维护系统，可以替代非国产的桥片和I/O芯片，提高了整个硬件平台的国产化程度，也使整个主板的设计更加紧凑、兼容。



那么，软件如何充分利用多核硬件架构以提升性能呢？

图4-3是网威ISOS系统平台内部逻辑结构，它把最耗费CPU资源的网络数据处理放在数据平面，由多个CPU并行处理。

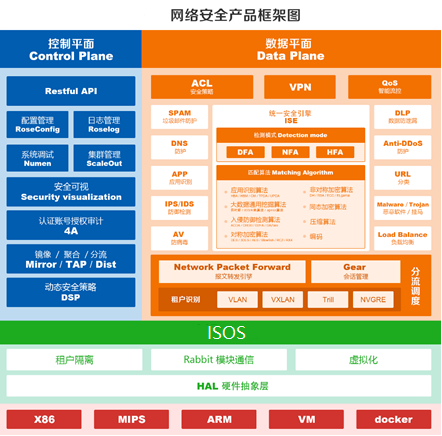


图4-3 网威ISOS系统平台内如逻辑结构图

如图4-3所示，ISOS系统被划分为控制平面（Control Plane）、数据平面（Data Plane）、以及硬件抽象层、操作系统ISOS，控制平面主要负责对系统管理、协议处理、数据转发进行控制；数据平面专门负责数据转发、安全过滤业务处理，从TCP/IP协议栈应用层数据均在数据平面进行处理，每个Core均实现了IPV4、MPLS引擎，可以并行处理网络数据包；系统虚拟层主要为控制平面和数据平面提供统一的系统服务接口，包括内存管理、时钟管理、任务管理、中断管理、文件系统管理、设备管理等；底层驱动和BSP负责各种设备的初始化、寄存器设置和控制以及报文收发控制等。

### 统一安全引擎ISE技术

IPS、DPI、AV等特性都需对报文进行深度扫描，由于UTM的设计理念决定了每个报文需要经过多次扫描，严重影响了UTM的处理性能。如果防火墙能做到对每个报文只是做一次扫描后提取到后续业务处理所需全部信息，那么防火墙性能就不会像UTM那样，随着开启的功能越多性能越低。

中科神威防火墙 V4.0将应用识别、内容检测、URL过滤、入侵检测、病毒识别五个处理引擎合为一个，采用自创高效的HFA正则匹配算法，实现对报文的高效一次性处理。中科神威防火墙V4.0统一安全引擎ISE的一次扫描提取报文的信息会根据开启的深度扫描功能动态调整，避免不必要的资源消耗。应用高性能的硬件平台，全部功能均启动，中科神威防火墙V4.0可处理10Gbps吞吐，业内领先。

### 业界领先的HFA一体化扫描算法

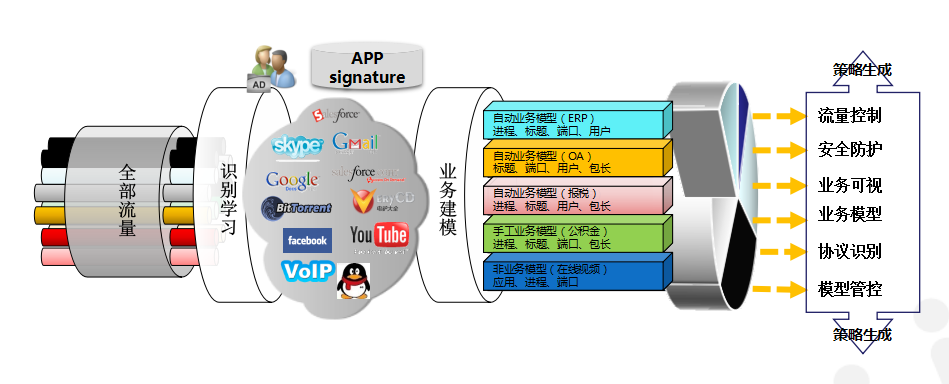
中科网威的HFA（Hybrid Finite Automation)结合了DFA和NFA两种算法的优势，其空间占用与NFA相近，性能却超过DFA；能在最小的空间占用基础上获取最佳的时间性能，极大限度地提高一体化深度探测的效率，极大地提高下一代防火墙的性能。

中科网威的HFA算法，能够在加载了数十万条数量级特征库的条件下，达到每核数10G的扫描性能，强劲的性能轻松满足复杂的应用层深度探测扫描的需求。

中科网威的HFA算法，采用分时复用和解压缩技术，使得百兆内存即可容纳百万数量级复杂特征库，很好地解决了内存占用与性能直接的矛盾；采用特征库预编译和预处理技术，使得算法性能同特征库的条目不相关，使得算法时间复杂度达到理论最优值；并且，通过对特征库预编译和预处理算法的不断改进和优化，使得特征库的预处理和加载迅速，无需等待即可预处理完成，使得特征库配置和更新同ISE处理无缝结合。

### 应用识别技术

大部分的即时通讯类应用在协商、数据通信过程都加密，并且加密算法不断更新，以防止被破解。同时，随着移动互联网的兴起，越来越多的应用采用https作为承载的协议，既能够穿越防火墙，同时内容得到高强度的加密。



鉴于应用通信加密已经成为主流，加密应用的加密算法和行为都在不断地变化，中科网威持续跟踪应用的环境，找出每种加密应用的“根本性”行为进行建模，从而避免了频繁的更新特征库。同时，中科神威防火墙V4.0采用多种行为分析算法来达到准确识别应用的目的，比如主机行为分析、主机端口关联、连接关联、TCP端口序列分布规律、UDP端口聚类分布规律、报文大小、前128或256字节指纹、报文时间戳、历史行为与实时行为关联、父子连接关联、跨资源访问行为关联、隧道解封、TCL脚本控制、引擎插件协助等。

### 智能流量管理技术

在网络内部，可能存在用户带宽分配不均、被病毒感染主机发生异常流量的情况，需要带宽划分，连接数控制等手段解决。另一方面，对于高优先级流量——实时语音、邮件、重要领导等需要专门的带宽保证措施。

网威ITM智能流量管理模块实现了8层通道、基于通道优先级进行差分化服务、保证带宽等特性，用户可以结合应用识别、3A用户管理等模块去细粒度、精准地控制流量，从而优化出口带宽，保证关键业务的通畅并使带宽得到充分高效地利用。

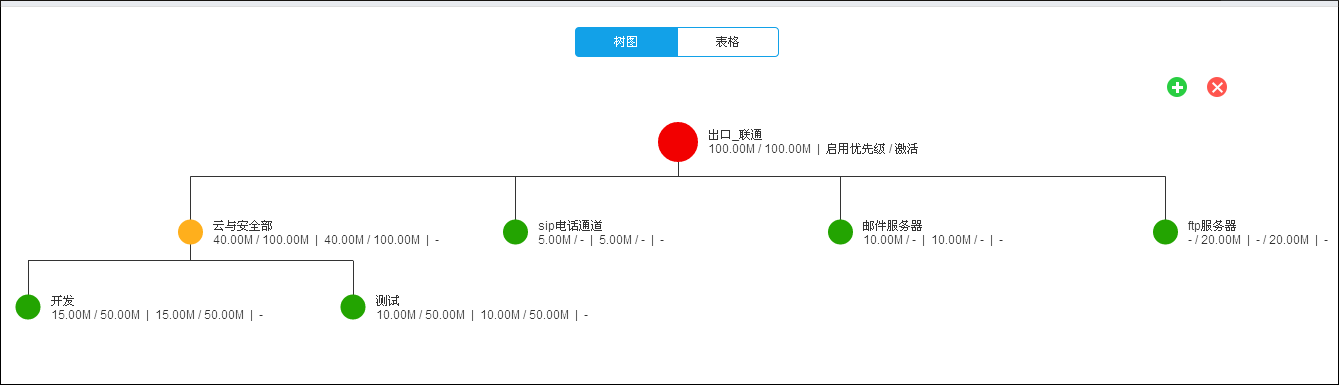


图4-4 通道配置

### 多维度流可视技术

流可视化不仅是下一代防火墙一个必不可少的功能，更是当今信息化的需求。要将网络系统中的各种流量信息、安全信息、事件信息、风险健康指数等信息细粒度、全方位地收集、统计、存储、分析、显示出来，需要一个可展性良好的流可视框架。

中科神威防火墙V4.0吸收和改进了网威流控产品的流可视框架，并根据下一代防火墙的流可视化的要求，重新设计和研发出基于指标、类型、时间的多级立体全方位可扩展流可视框架。能够根据用户需求，快速添加统计指标；能够根据用户制定的统计粒度，增加统计类型；并根据统计信息的时效性进行实时分析显示或者存储，以便历史统计分析查询，形成分析报表。

网威多级立体全方位可扩展流可视框架不仅能够根据用户的要求进行细粒度的统计分析，还会收集实时流量情况、安全信息、网络设备状态信息等信息，并综合统计所得数据，通过一定的关联分析算法得出系统中的网络安全指数、应用安全指数以及应用安全等级等指导、警示性数据，为网管配置提供参考。

多维度流可视技术支持用户和应用的双向钻取，用户可以查看任一用户的应用行为分布，也可以查看任一应用的用户分布，实时方便。

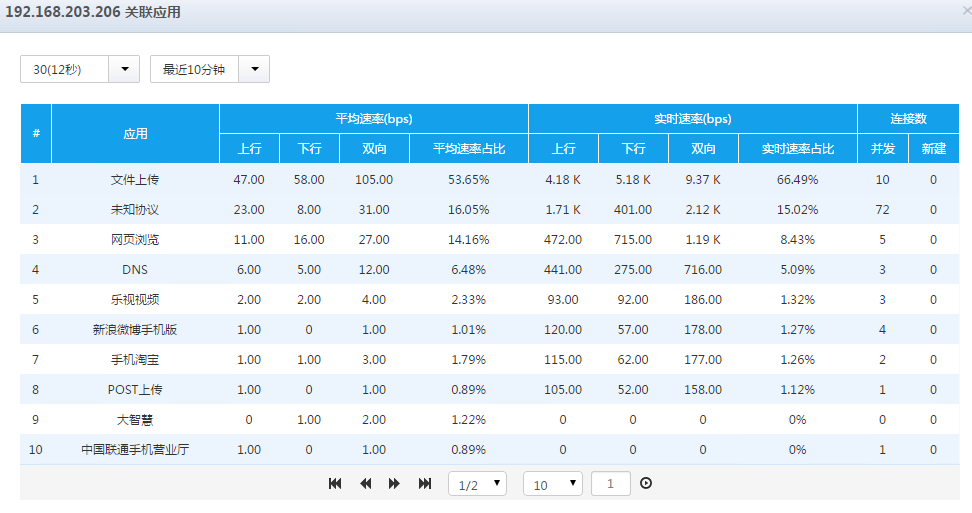


图4-5 用户钻取应用

### 一虚多和多虚一的虚拟化技术

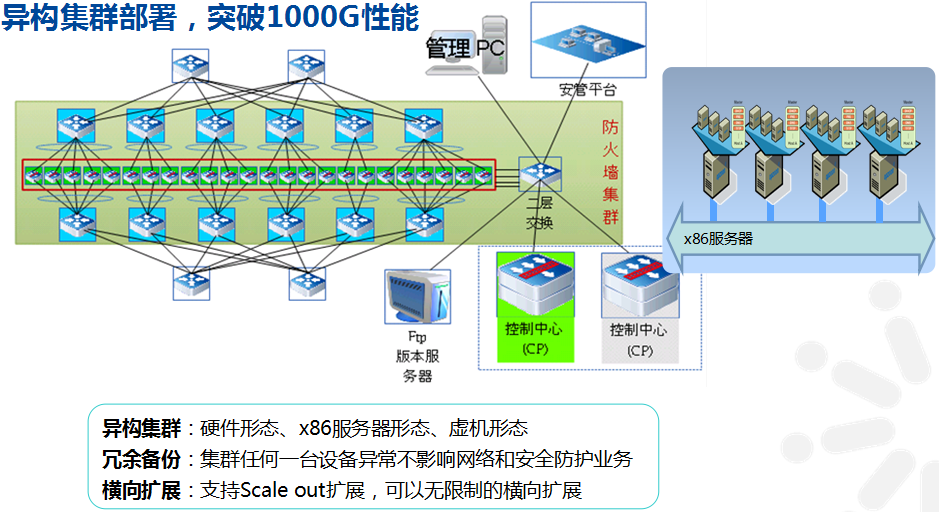
1）基于Hypervisor的“一虚多”防火墙虚拟化技术

中科神威防火墙V4.0通过对网威安全操作系统ISOS进行Hypervisor适配的改进和重构，使得网威安全操作系统ISOS能够在如vm、kvm、Xen等多种Hypervisor系统上执行，完美支持防火墙虚拟化。为中科神威防火墙V4.0软件形态产品提供基础，使得中科网威软件形态的下一代防火墙产品能够很好地适应云计算生态环境，很好地为公有云、私有云等云数据中心提供安全保障和安全服务。

2）基于云租户的安全隔离技术

为了满足云计算中云租户对安全的需求，中科神威防火墙V4.0网关支持添加/删除租户；并通过基于云租户的安全隔离技术，使得中科神威防火墙V4.0网关能够支持基于VLAN、AAA、VXLAN、Trill、NVGRE等方式进行租户定义，并对租户制定丰富的隔离和安全防护策略，实现租户安全隔离，为租户提供安全服务。

3）基于防火墙集群的“多虚一”超级防火墙技术

数据中心或者云数据中心中的各种计算设备、网络设备、存储设备一般都不会是单台部署，而是以集群的方式来无限扩容，来支持日益增长的信息化、网络化需求。面向未来的下一代防火墙也一样要支持集群化，满足无限扩容的需求。

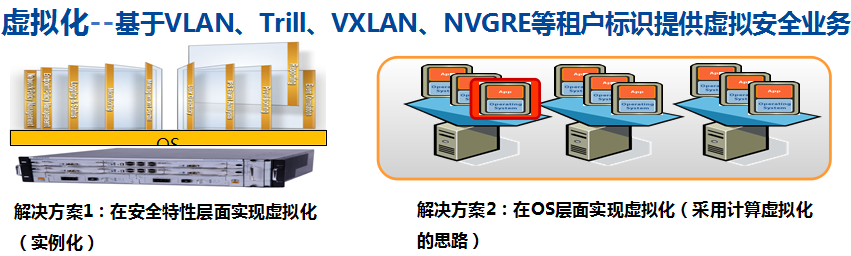
中科神威防火墙V4.0利用聚合技术结合自研集群协议而形成的“多虚一”虚拟化集成技术，可以将多台（最多可到128台）防火墙虚拟成一台防火墙，让多个设备集群起来工作，将多台防火墙虚拟成一台性能卓越的超级防火墙技术，解决了单台设备的瓶颈问题。

该技术可以自动探测集群中设备的状态去迁移数据流量，当流量进入集群时，会自动根据集群状态将数据迁移到同一台设备上处理，从而保证了一些和连接状态有关的功能在集群下也可以正常工作。为了方便管理，可以在控制中心可以对所有集群中的设备下发命令，也可以远程到集群中的任何设备查看状态和下发命令。设备的加入和离开也是动态的，可以弹性工作。

中科神威防火墙V4.0在“多虚一”虚拟化集成技术的基础上，可支持scale out集群部署，实现动态可调整、性能扩展无极限的数据中心安全或云数据中心安全解决方案。

### 自主知识产权的ISOS网威安全操作系统

**1）立足多硬件平台跨越，支持虚拟化**

网威安全操作系统不仅支持mips多核平台和arm平台，更支持目前热点的其X86多核平台，能在多款通用服务器上无障碍运行，通过对虚拟化的支持，更能在OPV、VM、Kvm等多款Hypervisor虚机环境中运行； 

**2）立足并行计算，面向高性能**

通过提高CPU主频，来提升单CPU系统整体性能的途径遇到了瓶颈。多CPU系统一起完成某项任务，必须要解决多CPU之间资源竞争、多CPU之间信息同步等问题，因此需要并行计算技术。

基于网威的并行计算技术，中科神威防火墙V4.0很好地解决了多CPU之间的负载均衡Load Balance、资源竞争、信息同步等问题。

采用Pipeline、Parallel、Mix三种模式，并动态调整多CPU负载均衡Load Balance策略。

采用加锁、原子操作、私有化、延迟释放等方式，有效解决了多CPU资源竞争难题。

采用共享内存、消息通信、无锁队列、中断、预取cache等方法，使得多CPU之间信息实现同步与共享

**3）立足交互可编程化，面向第三发开发支持**

现在的网络需求越来复杂，对智能化交互的需求越来越突出。面对庞大复杂的网络生态环境，下一代防火墙不可能独立工作，需要同其他网络设备、安全设备、管理软件等进行交互，而且是自动化的智能交互，无需人工干预。

面对这样的趋势和需求，网威ISOS网威云安全操作系统立足于智能交互的可编程化需求，提供丰富的Restful API接口，以便支持第三发开发。当前网威ISOS网威云安全操作系统的命令行cli交互、web交互、与网威SOC安管系统的交互，以及在网威OPV的云安全服务，都是通过网威ISOS网威云安全操作系统Restful API接口实现的。

## 主要功能

### 系统管理

管理方式：支持PXE远程安装、智能平台管理接口（IPMI）、提供管理友好的中英文Web图形界面配置，支持Telnet、SSH、串口登陆命令行模式配置；支持配置管理IP控制列表、SNMP网管协议以及邮件报警。

系统监控：包括系统信息、CPU利用率、内存利用率、接口流量、会话查询、电源指示灯，以及应用风险系数和安全系数等显示。

网络工具：支持ping、hping、tracert,等网络测试工具，通过ping、traceroute 、ARP测试、TCP测试、HTTP测试手段判断网络和应用的联通性。

时间同步：支持本地和NTP时间同步。

集中管理：可通过安全管理系统实现对防火墙的集中设备监控、集中日志审计、安全报警以及安全策略的分发等功能。

### 用户管理及认证

用户管理：支持“三权分立”的用户管理体系，web管理支持密码连续登录错误自动锁定账号，密码长度不低于10位且要求字母和数字组合。

AAA认证：支持本地认证、Radius认证、Tacacs+认证、CA 认证、LDAP/AD 认证；支持认证策略（策略认证联动）、重定向IP(认证代理)、Portal 服务器认证接口。

证书管理：支持本地证书管理（包括申请，下载，吊销，根证书/CRL列表下载）；支持第三证书管理（证书/CRL列表/私钥导入，第三方证书删除）；支持OCSP"。

### 网络适应性

工作模式：支持透明、路由、旁路和混合四种工作模式。

路由：支持静态路由、策略路由、OSPF、RIPv1/v2、BGPv4路由等；支持路由表查看。

网络接口：支持802.1Q、Vlan Trunk、vlan 子接口；支持链路802.3ad聚合；支持逻辑桥接口、自定义HA心跳口和管理接口。

NAT：支持SNAT、DNAT、NAT地址池等；支持Full Cone NAT特性，比如EIM、EIF、NAT sticky、Hair-pinning等。

DHCP：支持DHCP Client、DHCP Relay、DHCP Server、DHCP Pool。

DNS：支持本地DNS解析，DNS自学习安全缓存，DNS静态缓存。

PPPoE：支持PPPoE Server/Client、PPPoE 用户管理、路由手动添加和自动下发。

ARP：支持静态ARP和免费 ARP设置，以及动态ARP显示。

DDNS：支持DDNS动态域名。

### 安全防护模式

**1）基于网络**

会话数限制：会话数可控，分别按照协议、用户和策略等多种条件实现会话数统计和控制两种功能，控制粒度精确到单个IP。

ALG：可控制FTP、H.323、H.323GK、TNS、PPTP、MMS、RTSP、SIP、XDMCP等ALG。

黑名单：可根据报文的源IP地址进行过滤。

IP/MAC绑定：可绑定IP/MAC地址，且可自动探测和做唯一性检查。

本地安全：可限定主机或接入接口对本地服务的访问，如SSH和HTTP等服务。

**2）基于应用**

应用识别：支持应用特征库与分析引擎分离，且应用特征库在线实时升级；支持应用特征建模以识别特征变化频繁或加密应用；支持自定义应用特征。

基于应用实施防护：支持基于应用制定安全策略和针对具体应用的功能控制，以及对未知应用部署安全策略。

**3）基于用户**

用户识别与认证：支持用户分类管理与认证；支持本地认证、Radius认证、Tacacs+认证、CA 认证、LDAP/AD 认证；支持认证策略（策略认证联动）、重定向IP(认证代理)、Portal 服务器认证接口。

基于用户实施防护：基于用户制定安全策略；支持多种针对未通过认证的用户的安全策略。

**4）基于云租户**

租户添加/删除：支持添加/删除租户(删除时，自动删除租户下的配置以及配置文件等）。

租户属性配置：支持以多种方式定义租户，如：VLAN、Trill、NVGRE、VXLAN(后2种只有在透明传输下有效)；支持租户间完全逻辑隔离，租户部署的策略相互之间没有影响。

基本功能：支持租户独立的配置和租户间视图的切换；支持租户模式下IP地址配置的隔离、直连路由生成的隔离和下静态ARP的隔离。

基础资源对象：支持基于租户的安全策略、地址对象/地址组/地址池/权重地址、自定义服务对象/服务组、时间对象/时间组以及ALG中常用协议（包括FTP、TFTP、H323、TNS、MMS、PPTP、XDMCP、SIP等）隔离。

安全功能：支持基于租户的NAT、IP地址配置、IP\_MAC绑定、病毒过滤和防挂马、IPS入侵防御检测技术、攻击防护、应用识别、文件控制、ARP防护、内容安全特性（邮件、网页的内容过滤）、策略/静态/多出口路由。

**5）基于云主机**

云平台：能够配置云平台的认证信息（云平台类型，管理节点IP地址，管理员用户名和密码），能够与云平台进行管理认证通信，支持OPV-Suite、VMware、Openstack认证和通信。

动态安全策略：可以根据虚拟机的特征标记从云平台获取到虚拟机的IP地址，且可以动态更新，这样在虚拟机发生IP变化时，动态安全策略就和更新组内的IP地址，在安全策略中引用动态安全策略后，就可以保持这一条安全策略不动，防火墙设备可以自动更新策略内的IP地址表对固定的虚拟机进行安全策略控制，节省人力资源，降低出错风险；支持虚拟机的操作系统信息，网络信息，UUID，集群信息，虚拟机名称等可以描述一台或一类虚拟机的特征参数信息。

安全防护：支持动态地址的安全防护，支持动态地址的动态安全策略。

**6）基于虚身份**

应用账号识别：支持腾讯QQ、百度、阿里、人人网、新浪、猫扑、豆瓣、网易、飞信等主流社交媒体的账号识别和安全保护。

审计/告警：有效记录用户的网络动作（如登录QQ、发送邮件），通过声音等方式对特定账号进行告警，监控用户的网络动作

虚拟人口库：可以收集用户的所有虚拟身份（网络应用账号），形成虚拟人口库。如果与真实人口库对接，对于规范网络行为、处理网络犯罪等有积极作用。

安全防护：在应用识别的基础上，支持基于应用账号的防护，即针对特定的账号流量做安全策略。支持单应用账号的安全防护；支持应用账号组的安全防护。

### 特征库支持

统一管理：web页面下统一对设备支持的特征库进行查看、更新及自定义操作。

种类细分：在传统IPS、AV和应用特征库基础之上，增加了木马库，webmail、垃圾邮件等特征库。

实时更新：提供统一、稳定、实时的特征库升级服务。

支持客户定制：针对webmail、应用特征库可以根据客户需求实现定制。

### 虚拟专用网(VPN)

协议与标准：支持标准IPSec协议，能够与多家主流厂商VPN设备/客户端软件互联互通，实现端-端的互通加密访问；支持特有的SSL vpn连接方式，并可自定义vpn通道的访问资源，实现Client-端的加密访问。

VPN种类：支持PPTP VPN、Ipsec vpn、SSL VPN以及GRE VPN、L2TP VPN(L2TP-LAC/L2TP--LNS)。

认证方式：支持本地用户名/密码认证，可利用此方式为基石与其他认证方式结合；支持第三方认证体系进行无缝集成，如LDAP、 Microsoft AD、Radius等，便于接入人员身份的统一管理；支持SSL帐号密码防暴力破解功能，保障用户密码的安全性；支持第三方CA体系进行结合，并支持OCSP服务器，融入PKI体系；支持SSL VPN设备自建CA中心功能，可极大的降低企业使用成本；支持基于SSL VPN接入终端的硬件鉴权，可以自动审批，并支持多对多绑定策略，有效防止非法终端接入。

数据加密和封装：支持3DES、DES、AES128、AES192、AES256等加密算法；支持AH和ESP封装模式以及MD5、SHA1、SHA2、HMAC-MD-5、HMAC-SHA256等通用摘要算法。

SSL vpn易用性：支持多种windows操作系统，如win7、winxp、win sever等；支持对包括登陆前和登录后界面的整体界面定制，满足客户个性化风格的要求；支持关闭IE时最小化到系统托盘，开机自动SSL登陆，断线重连，可跳转至SSO配置、个人配置,方便用户快捷操作SSL VPN。

SSL vpn接入优化和管控：支持选择性缓存动态Web页面，提升Web类资源的访问速度；支持针对全网IP资源进行加速优化，提高针对IP资源的访问速度；支持对资源服务器智能选择，实现对资源服务器接入的负载均衡Load Balance，进而提高访问效率；支持基于时间、接入IP、终端、接入线路、应用规则的客户端准入控制策略和资源访问授权策略；支持基于基于用户、用户组的流量控制以及会话控制，防止单个客户流量过大，挤占带宽的情况，提高访问体验。

SSL vpn管理：支持基于角色的方式控制vpn接入用户的访问权限；支持内部资源高细粒度划分，如可以按照URL、服务类、IP等各项资源；支持利用安管系统进行集中管理和维护、智能升级、实时监控。

### 应用管控

用户策略：可基于用户制定安全策略，并对未通过认证用户实施阻断、记录日志、告警、限制流量等安全策略。

URL分类：内置URL分类库，支持80多类、1000多万条URL信息。

URL过滤：可对URL地址以及域名进行过滤，且支持黑名单和白名单。

应用安全策略：可基于应用制定安全策略，实现对特定用户、用户组、IP、IP组实现限制。

应用识别：内置1700多种应用特征库，可准确识别各种IM、P2P、网络游戏、流媒体、股票等应用，并可自定义。

P2P管理：可识别管理100多种P2P应用，规则库实时升级，P2P流量管理可精准到1kbps。

IM管理：可对加密型或非加密型聊天软件进行管理、拦截、限流，并可分项管理聊天程序的登录/聊天/传输文件/语音/视频等，支持的聊天程序包括QQ、阿里旺旺、YY语音、陌陌电脑版、飞信、新浪UC、Skype、Google Talk、PoPo Build、iChat等10多类。

移动APP管理：支持基于安卓和苹果OS开发的多种聊天软件和社交软件，如，QQ、微信、新浪微博、YY语音、糗粨、网易新闻等。

WebIM管理：可对基于Web的聊天进行登录和禁止控制，包括QQ、微信、Google Talk、AIM、eBuddy.com、阿里旺旺、YY Live等。

非法隧道管理：可检查TCP应用层内容，分析并控管VPN Tunnel网络行为，包括VNN、SoftEther、TinyVPN、PacketiX、HTTP-Tunnel、Tor等。

在线游戏管理：可对QQGame、QQ对战平台、3d坦克、11对战平台、OurGame、Cga.com.cn Game、QQFO Game、Popkart Game等流行在线游戏实现阻断管理；对国内主流网游实现管用，如英雄联盟、穿越火线、地下城与勇士、魔兽世界、梦幻传奇、大话系列、劲舞团等30多种；以上内容还可根据客户需求定制更新。

关键字过滤：支持HTTP1.0和HTTP1.1协议，支持多种编码协议如UTF8、GB2312和BIG5；可对通过gzip或deflate的算法压缩的web页面进行动态自动解压缩，并采用内存缓存、包存储结构以及动态调整缓存空间等方式提供更快的响应速度，和用户使用体验，同时降低了用户访问后端服务器的压力。

移动代码过滤 ：可对Java，JavaScript,ActiveX、java applet、shellcode、cookie、identity等移动代码过滤。

应用设定：可对FTP、SMTP、POP3等应用进行设定，并过滤。

控制粒度：内容过滤规则可精确到单个用户和每个ip。

### 应用安全防护

深度包检测：内嵌深度包检测引擎，针对数据包进行深度过滤检测。

Web过滤防护：可以阻断内部用户访问非法的网址或访问含有非法内容的网页；支持自定义URL过滤策略、关键字过滤策略、蠕虫过滤策略；支持攻击邮件告警。

FTP过滤防护：可以对穿透防火墙的FTP服务进行过滤审计；支持通过预定义过滤文件名实现对FTP数据流的区分控制。

VPN隧道防护：支持对vpn隧道内的内容检查和防护。

应用协议分析：支持对数据流量的协议分析。

### IPS入侵防御检测技术

入侵检测技术：支持基于IP碎片重组、TCP流重组、会话状态跟踪、应用层协议解码等数据流处理方式的攻击识别；支持模式匹配、异常检测、统计分析，以及抗IDS/IPS逃逸等多种检测技术；支持IPS报文取证。

协议解析：可依据应用行为自动识别协议类型，如HTTP、SMTP、POP3、FTP、Telnet、VLAN、MPLS、ARP、GRE等多种协议，并可进行防护解析。

特征规则：内置攻击特征库，特征数量超过3,500条，定期更新特征库；可基于TCP/ICMP/UDP协议自定义攻击特征，可阻挡蠕虫、木马、间谍软件、广告软件、缓冲区溢出、扫描、非法连接、SQL注入、XSS跨站脚本等多种攻击。

IPS统计报表：IPS统计日志可以提供报表导出功能。

### AVG病毒防护

病毒库：采用先进的、不断更新的病毒库，支持手动和在线自动升级方式。

扫描模式：支持代理模式和流模式两种病毒扫描方式。

邮件代理：支持病毒处理动作设置、扫描文件大小设置；支持基于SMTP、PoP3、SMTP等协议代理的病毒扫描。

协议查毒：支持ftp、http、smtp、pop3、imap、等协议病毒扫描；支持自定义非标准端口下应用协议的AVG病毒防护，如qq特征。

阻断类型：支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型的病毒；支持所有常见文件格式的病毒查杀，可自定义文件阈值大小、类型；支持新一代虚拟脱壳和行为判断技术，准确查杀各种变种病毒、未知病毒。

隔离设置：支持指定隔离位置、隔离导出、隔离删除和隔离内容查看

信息统计：支持防病毒信息统计

### 垃圾邮件防护

垃圾邮件规则库：定期更新的特征库，支持手动、自动的升级方式。

检测机制：支持SMTP、POP3、IMAP4协议下的垃圾邮件检测，基于反中转的垃圾邮件识别和过滤，对邮件的内容扫描。

识别算法：支持贝叶斯算法、完整性分析、启发式规则、关键字检测等智能区分垃圾邮件。

邮件数量控制：支持对同一账号的邮箱连接数量，邮件发送频率进行数量限制，能够识别无效收件人。

邮件过滤：支持邮件服务器地址的黑、白名单，或邮件地址、主题、正文、附件名、附件内容、邮件整体大小、附件尺寸等多种组合条件进行过滤；支持正常转发，拒绝丢弃，退回并信息告知，标记后转发，延迟发送等多种过滤动作；支持按照邮件发件人/收件人隔离邮件。

邮件抗攻击：支持对邮件服务器的DDoS攻击防护。

webmail防垃圾邮件：支持webmail关键字检测、webmail发件人阻断检测、webmail保存正文和附件。

垃圾邮件统计：支持防垃圾邮件信息统计。

### 二至七层Anti-DDoS技术

全局防护：支持防护ARP洪水、防护反向ARP查询、防护arp欺骗：防护arp欺骗，广播应答防护、特征检查防护、检查应答、禁止更新缓存；支持防护分片洪水、防护分片洪水、防护分片洪水、防护ip地址欺骗、防护本地icmp攻击。

防护洪水攻击：支持防护本地icmp攻击、防护SYN/ACK洪水、防护ACK洪水、防护HTTP洪水、防护CC洪水、防护远程ICMP洪水、防护数据流洪水、防护UDP协议洪水、防护最大连接数攻击、防护端口扫描功能。

防扫描攻击：支持类型包括：Fraggle攻击、Smurf攻击、Land攻击、WinNuke攻击、SYN/FIN扫描攻、Null 扫描攻击、全Xmas扫描攻击、Xmas扫描攻击、ping of death攻击。

防护特定工具攻击：支持防护trinoo工具攻击、防护tfn工具攻击、防护tfn2k工具攻击、防护stacheldraht工具攻击。

基于BGP流量牵引和回注：支持BGP本地/邻居信息配置、BGP访问控制列表、BGP路由牵引及回注；支持查看BGP路由映射信息、BGP配置/BGP邻居信息。

### DNS防护

DNS防护：支持dns域名黑名单、dns域名控制列表、DNS风暴防护、防护远程DNS查询洪水。

DNS监测：支持统计监测的采样率、DNS监测、自定义统计监测的域名、自定义统计监测的域名、显示自定义统计监测域名信息、DNS监控&DDoS-DNS统计图表。

DNS安全缓存 ：支持dns自学习安全缓存、DNS静态安全缓存、三方确认安全缓存、查看系统中所有安全缓存、查看观察表中的安全缓存。

DNS安全控制：支持静态域名功能、自定义静态域名。

DNS告警审计：支持定义静态域名、定义静态域名、显示DNS全局总数统计信息。

DNS信息查看：查看DNS防护模块的运行状态。

### 智能流量管控QoS

流量分类：采用基于优化的高速流匹配技术， 以多种依据（源IP/目的IP/IP范围/源端口/目的端口/端口范围/接口/用户/安全策略/空间/网络协议/应用协议等）对流量进行分类。

流量控制：可基于应用分类/应用协议/应用行为等方式进行多层次流量控制；支持一条策略即可实现针对每个用户/IP的细粒度带宽控制；支持针对上/下行带宽分别实时流量控制；支持黑白名单等方式实时流量控制；支持基于用户、安全策略、应用等分类的组合流量控制。

流量镜像Mirror：支持将流量通过镜像口镜像出去，供第三方设备存储、分析、审计等。

带宽限制：基于多种方式（源IP/目的IP/源端口/目的端口/时间/时程/应用程序/接口/用户/策略/空间/网络协议等）设定最小带宽和最大使用带宽；支持单IP流量上限控制。

带宽切割：将每条链路切割成多组彼此互不影响的通道（PIPE），每个通道可再分割多个虚拟通道（Virtual Channel），设定带宽管理规则。

优先级设定：支持对通过设备的IP报文修改IP优先级、ToS字段以达到优化整网带宽的目的。

响应时间管理和分析：持续跟踪应用程序/服务器响应时间变化情况，改善控制策略以保障网络应用最大的可用性和性能。

智能带宽管理：检查带宽使用状况，自动调整各个应用的使用水平，保证关键业务的可靠性和可用性。

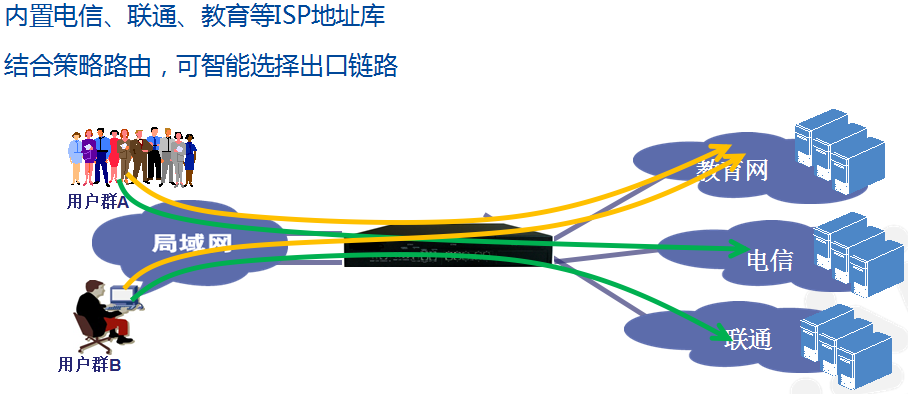
带宽借用：依据网络带宽利用率，可智能地利用闲余带宽。

流量模型自学习：依据网络流量的状态，可自动学习并生成流量最优的策略。

### 负载均衡Load Balance

负载均衡Load Balance特性：支持基于多种方式划分的负载均衡Load Balance，如按照服务器、链路、应用等不同方面划分；支持故障链路/服务/端口/不参加调度和故障恢复链路自动加入调度。

基于服务器：支持通过端口号过滤流量进行负载均衡Load Balance；支持通过传输层协议类型过滤流量进行负载均衡Load Balance；支持通过端口号+传输层协议类型过滤流量进行负载均衡Load Balance；支持8中调度算法（轮叫调度、加权轮叫调度、源地址散列调度、目标地址散列调度、最小连接调度、加权最小连接调度、基于局部性的最小连接调度和带复制的基于局部性的最小连接调度）。



基于Outbound链路：支持通过IP地址过滤流量进行负载均衡Load Balance；支持通过端口号过滤流量进行负载均衡Load Balance；支持通过传输层协议类型过滤流量进行负载均衡Load Balance；支持通过IP+端口号+传输层协议类型过滤流量进行负载均衡Load Balance；支持8中调度算法（轮叫调度、加权轮叫调度、源地址散列调度、目标地址散列调度、最小连接调度、加权最小连接调度、基于局部性的最小连接调度和带复制的基于局部性的最小连接调度）。

基于Inbound链路：支持通过响应DNS请求对访问服务器的流量进行负载均衡Load Balance；支持4种调度算法（轮叫调度、加权轮叫调度、源地址散列调度和目标地址散列调度）。

基于http重定向：支持当服务器负载均衡Load Balance不能提供本地http服务时，从远程数据中心调度服务器提供http服务；支持静态就近性和动态就近性两种调度算法。

基于DNS：支持对多个数据中心的多条链路进行负载均衡Load Balance；支持静态就近性和动态就近性两种调度算法 。

健康探测：支持协议健康探测，如HHTP、ICMP、SMTP、SSL和TCP等协议

### 高可靠性

双机热备：支持主-主、主-备和非对称路由三种模式的双机热备，且切换时间小于1秒。

负载均衡Load Balance：支持最多4个节点，通过VRRP协议实现集群负载均衡Load Balance。

HA 监控：支持HA状态实时查看。

同步：支持配置同步、session同步。

### Scale OUT集群部署

部署方式：支持 3以上设备部署，最多可支持 200多台，可透明和路由部署。

集群管理：设备可自动加入集群，和动态退出集群，在中心设备上能对指定的设备或所有成员设备下方配置，定制升级方案。

集群监控：管理中心能监控控所有成员的状态。

网络适应性：支持动态增减设备数量，同连接定向同设备处理保证安全策略可用，自动根据链路状态牵引流量。

集群间同步：时间同步、配置同步、连接状态同步、ARP表同步等。

### 安全审计

日志存储及管理：支持将日志存储在本地，标配1T日志存储硬盘，完美满足公安部82号令,至少保留用户行为日志60天的要求（存储时间跟数据流量大小有直接关系，此给出的是标准应用参考存储时间）；支持设置日志服务器，将日志发送到网络中统一的日志服务器上，进行统一收集、管理；支持全部日志按天和统一格式（如：ozlog-20141013.log）存储，可以通过web页面查看历史日志列表，且可以针对列表日志进行删除、导出等操作；支持日志存储空间支持预定义警戒值，达到存储警戒值后实现日志的覆盖存储，保证新日志的有效记录；支持历史日志，保证设备掉电后仍然可以保留上次运行的日志记录，为网络安全和设备的运行维护提供了宝贵的日志信息和资料。

日志查看：持日志定制，按照不同用户需求查看所需的日志类型（可以一个或多个）同时，亦可以屏蔽不需要的日志类型（一个或多个）；支持web页面下对日志的过滤，查找，导出，删除等操作；支持基于三权分立定义不同用户对设备日志拥有不同的权限；支持各种功能日志记录，如vpn、ips、病毒日志等，方便定位网络故障。

内容审计：支持自定义审计接口，可将内容镜像到专用内容审计产品上；可根据用户需求，自定义需要镜像的数据流量，如按照用户、网络、应用协议、策略、物理接口等等。

### 安全可视Security Visualation

流量分析：可高速分析与统计2至7层网络流量。

应用状态显示 实时图表显示用户连接数、当前会话数、应用使用排名等信息。

流量统计：提供多种统计方式，如基于用户、应用、接口、安全策略等因素进行统计显示。

报表分析：提供多种报表，可依据五元组、应用协议、时间点/时间段等元素自定义报表内容并显示。

告警通知：可对接口流量/应用/协议的异常状态进行告警，并以Email/SNMP Trap/声音等方式通知管理员。

安全事件地图展示：1、包括按源地区和目的地区展现进行查询。2、地图上展现的威胁类型：病毒、入侵防范、僵木蠕、攻击防范、全部威胁3、包括最近一个小时、一天和一个月进行详细查询。4、光标指向该地域的名称及攻击数，点击该地域跳出详细信息列表5、严重程度通过颜色进行区分：支持地图上用不同颜色展示不同次数的攻击。6、基于地理位置的威胁分析。7、基于威胁事件类型的地图展示。

ISP地址列表：ISP地址列表可通过web手动导入进行升级。可随时更新变化的地址列表与负载均衡Load Balance使用统一文件，避免繁琐

## 主要特色

### 立足虚拟化，面向云安全

中科神威防火墙V4.0顺应时代发展的要求，提供了灵活的安全解决方案，既可以在云环境下提供安全服务，又可以支持集群部署，组成超级防火墙，另外，中科神威防火墙V4.0提供丰富的Restful API，支持与第三方联动。

**1）一虚多，按需提供安全服务**

针对云计算的虚拟化运行环境的要求，中科神威防火墙V4.0支持基于基于Hypervisor的“一虚多”防火墙虚拟化技术，能在如vm、kvm、Xen等多种Hypervisor系统上执行，完美支持防火墙虚拟化，提供按需的虚拟化安全需要。

**2）多虚一，提供超级防火墙服务**

同时，中科神威防火墙V4.0利用聚合技术结合自研集群协议而形成的“多虚一”虚拟化集成技术，可将多台防火墙虚拟成一台防火墙，让多个设备集群起来工作，将多台防火墙虚拟成一台性能卓越的超级防火墙技术，解决了单台设备的瓶颈问题，实现动态可调整、性能扩展无极限的数据中心安全或云数据中心安全解决方案。

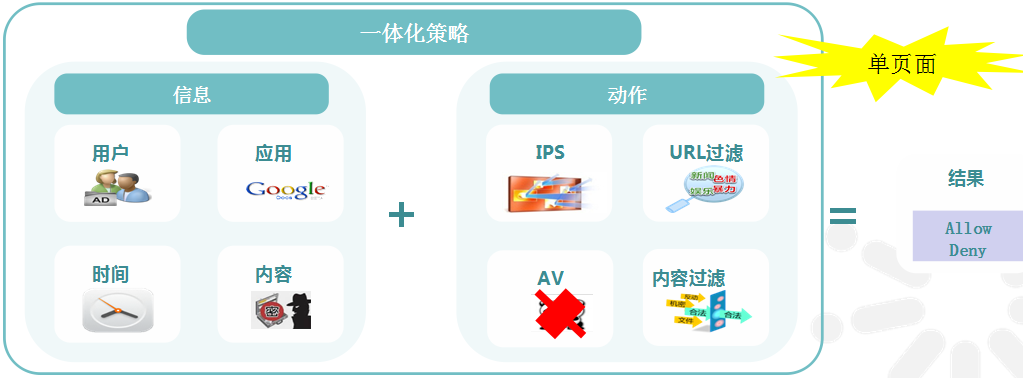
**3）立足交互可编程化，面向第三发开发支持**

面对日益重要的智能化交互趋势和需求，中科神威防火墙V4.0立足于智能交互的可编程化需求，提供丰富的Restful API接口，以便支持第三发开发。基于面向第三方开发的防火墙、Anti-DDoS、IPS等安全特性的Restful API，中科神威防火墙V4.0支持了命令行cli交互、web交互、与网威SOC安管系统的交互。

基于这些安全特效的Restful API以及设备管理的Restful API，中科神威防火墙V4.0支持第三发开发，能和第三方设备或软件无障碍交互和联动，在数据中心及其他网络环境中实现统一的、相互影响和关联、智能的信息安全防护体系。

### 一站式管理，简化网管维护

在传统的UTM设备中，与处理引擎相对独立一样，配置管理界面中各功能配置也是相对独立的，在配置完成防火墙策略配置后，要启动入侵检测就要到IPS配置页面配置，要启动应用识别要要到应用控制页面配置，等等。这就对维护UTM的技术人员提出了很高的技术要求，无法满足设备配置人性化需求。



中科神威防火墙V4.0提供了一站式配置界面，并且功能模板化，可用通过配置向导，简单点击选择，拥有简单网络知识的运维人员就可以在几分钟内完成专业的网络和策略配置。

### 多深度解析技术融合，引擎一体化

中科神威防火墙V4.0将应用识别、内容检测、URL过滤、入侵检测、病毒识别等多种深度探测技术处理引擎合为一个，采用自创高效的HFA正则匹配算法，实现对报文一次匹配，结果多业务共享的高效一次性处理,降低匹配冗余度，提高应用层处理效率。支持包含IPS，挂马，AV，文件控制，URL防护，数据防护在内各种应用业务，中科神威防火墙V4.0ISE的一次扫描提取报文的信息会根据开启的深度扫描功能动态调整，避免不必要的资源消耗。

中科神威防火墙V4.0应用安全业务策略的下发和存储采用二叉树的形式，使其多条策略的匹配效率变得高效。

**1）自创高效的HFA正则匹配算法**

采用分时复用和解压缩技术，使得百兆内存即可容纳百万数量级复杂特征库，很好地解决了内存占用与性能直接的矛盾；采用特征库预编译和预处理技术，使得算法性能同特征库的条目不相关，使得算法时间复杂度达到理论最优值；并且，通过对特征库预编译和预处理算法的不断改进和优化，使得特征库的预处理和加载迅速，无需等待即可预处理完成，使得特征库配置和更新同ISE处理无缝结合。

**2）动态识别技术**

中科神威防火墙V4.0不仅仅是对流量的报文特征进行识别，还结合安全漏洞的特征码识别、安全威胁特征码识别、攻击行为特征识别、应用流量行为识别等动态识别技术，能预测并识别未来可能出现的攻击和协议。

**3）细分特征库**

支持统一管理，web页面下统一对设备支持的特征库进行查看、更新及自定义操作；种类细分，在传统IPS、AV和应用特征库基础之上，增加了木马库，webmail、垃圾邮件等特征库；提供统一、稳定、实时的特征库升级更新服务；支持客户自定义特征码及自定义行为特征，针对webmail、应用特征库可以根据客户需求实现定制。

### 智能化：内部智能协防，外部智能联动

**1）内部各安全功能智能协防、有机统一**

设备内部各安全业务之间通过报文状态缓存、会话连接、内部联动机制等相互协防，有机统一。

**2）外部人、云、机智能联动、共建智能信息安全防御体系**

中科神威防火墙V4.0通过网威云安全操作系统ISOS提供的Restful 标准的面向第三方开发的API接口，能同外部设备实现无障碍交互和联动，接收和分析其他设备通过Restful API发送过来的信息，在对这些信息进行综合关联分析的基础上，修正或改变本地安全策略，以在数据中心及其他网络环境中实现统一的、相互影响和关联、智能的信息安全防护体系。

### 网络适应性灵活，可非破坏性网络嵌入

中科神威防火墙V4.0具有良好的网络适应，即可以接入到二层网络，也可以接入到三层网络，更可以在不改变现有网络的基础上，非破坏性嵌入网络，支持支持透明、路由等传统方式，也支持旁路/回注、非对称路由、混合等多种接入方式。

中科神威防火墙V4.0适应网络未来发展趋势，支持IPv6网络互联以及相关安全防护。

### 二到七层协议保护,全面专业安全保障

中科神威防火墙V4.0全面支持二到七层协议保护，为用户提供全面专业安全保障。

**1）传统防火墙功能**

中科神威防火墙V4.0支持最基础的包过滤、NAT、ALG、会话数限制、黑名单、IP/MAC绑定、本地安全策略等传统防火墙功能。

**2）二到七层Anti-DDoS攻击**

中科神威防火墙V4.0支持二到七层Anti-DDoS攻击。中科神威防火墙V4.0的Anti-DDoS功能采用了特征识别、反探校验、状态监测、智能学习、连接限制等技术，支持各种基于单包、基于流、基于应用（如web应用）、基于攻击工具、蠕虫连接型DDOS攻击、以及其他普通常见等多种DDOS攻击的防护。独创的多核并行计算算法和智能防护算法，对攻击行为进行智能分析，动态形成攻击特征库，可有效防护SYN Flood、CC等二十多种攻击，保障正常业务不受影响。

**3）入侵检测防御IDP**

中科神威防火墙V4.0基于HFA一体化检测和协议分析技术，可阻挡蠕虫、木马、间谍软件、广告软件、缓冲区溢出、扫描、非法连接、SQL 注入、XSS 跨站脚本等各种攻击，能对网络中的垃圾信息和诱骗信息识别和阻断、隔离，以此为用户提供攻击检测和防御。

**4）上网行为管控**

中科神威防火墙V4.0基于HFA一体化检测和协议分析技术，通过协议识别、各种应用安全特征库能够有效实现灵活的应用识别、应用管控、内容过滤、URL过滤以及URL库分类，确保绿色上网。

**5）应用安全防护**

中科神威防火墙V4.0支持各种应用的安全防护，对常用的DNS、WEB、FTP、SMTP等常见协议进行深入分析和具有针对性的安全防护；对具有加密特性的VPN隧道也能进行安全性防护；通过些协商识别和HFA算法扫描，也能对其他应用协议进行安全防护.

**6）AVG病毒防护**

中科神威防火墙V4.0在ISE中有机融合了自主开发的病毒扫描引擎，支持支持ftp、http、smtp、pop3、imap等协议的病毒扫描以及qq特征自定义病毒扫描、识别和处理，从而对网络中的病毒进行有效的阻断或隔离，确保网络环境的安全。

**7）垃圾邮件防护**

中科神威防火墙V4.0在ISE中有机融合了垃圾邮件扫描引擎，支持SMTP、POP3、IMAP4协议下的垃圾邮件检测，根据邮件的各种关键信息对邮件进行设备和过滤，阻断或隔离垃圾邮件，确保网络环境的干净。

### “七位一体”，细粒度安全防护

中科神威防火墙V4.0不仅在纵向上支持二到七层协议保护，在横向上提供基于五元组的、基于用户的、基于应用的、基于内容的、基于云租户、基于云主机、基于虚身份的“七位一体”细粒度安全防护。

**1）基于五元组的安全防护**

中科神威防火墙V4.0能支持最基础的基于网络二、三、四层的解析，并能够根据二层、三层、四层各层头部中的字段及其字段组合进行粒度划分，进而进行各粒度的应用安全防护。一般情况下使用五元组或其中的源IP地址、源端口、四层协议类型、目的IP地址、目的端口的个体和组合进行粒度划分，进而进行安全防护。

**2）基于用户的安全防护**

中科神威防火墙V4.0在用户管理和多种AAA认证协议的支持下，可支持基于认证用户的包括二到七层协议保护在内的各种安全防护。用可以根据用户配置灵活的安全防护策略。

中科神威防火墙V4.0支持本地用户和网络用户管理，支持“三权分立”的用户管理体系。

中科神威防火墙V4.0支持多种AAA协议认证以及证书认证，为用户提供灵活的用户管理策略。

中科神威防火墙V4.0通过将用户和用户组对象相互，并将这些对象作为ACL的一个匹配条件，从而支持基于应用的各种安全业务。

**3）基于应用的安全防护**

中科神威防火墙V4.0内置1700多种应用特征库，可准确识别各种IM、P2P、网络游戏、流媒体、股票等应用，并可自定义应用特征以便识别。中科神威防火墙V4.0应用识别采取多级式识别，分为应用大类、应用、应用内部子应用等多级，提供灵活的协议识别。

在应用识别基础上，中科神威防火墙V4.0将应用对象化，支持应用对象及应用对象组，将应用对象和应对象组作为ACL的一个匹配条件，从而支持基于应用的各种安全业务。中科神威防火墙V4.0基于应用实施防护的共鞥，支持细粒度应用管控，支持基于应用制定安全策略，支持多种针对未知应用的安全策略，支持针对具体应用的功能控制。

**4）基于内容的安全防护**

中科神威防火墙V4.0基于HFA一体化检测和协议分析技术，支持基于内容的安全防护。

自创的HFA深度解析技术算法，保证关键字、URL等内容过滤功能的高效。

支持有常见编码规则应用的内容过滤。

支持有流行压缩算法应用的内容过滤。

支持基于报文和流特征指纹的加密应用阻断。

支持WEB应用相关协议的解析与阻断、隔离。

支持邮件应用相关协议的解析与阻断、隔离，支持AS。

**5）基于虚身份的安全防护**

应用账号识别：支持腾讯QQ、百度、阿里、人人网、新浪、猫扑、豆瓣、网易、飞信等主流社交媒体的账号识别和安全保护。

审计/告警：有效记录用户的网络动作（如登录QQ、发送邮件），通过声音等方式对特定账号进行告警，监控用户的网络动作

虚拟人口库：可以收集用户的所有虚拟身份（网络应用账号），形成虚拟人口库。如果与真实人口库对接，对于规范网络行为、处理网络犯罪等有积极作用。

安全防护：在应用识别的基础上，支持基于应用账号的防护，即针对特定的账号流量做安全策略。支持单应用账号的安全防护；支持应用账号组的安全防护。

### 三层七层VPN助力远程虚拟互联

中科神威防火墙V4.0提供了多种远程安全接入的方式，包括IPSec、PPTP、SSL等多种VPN接入方式，并能够与多家主流厂商的Ipsec VPN网关和客户端软件互联互通。

**1）IPSEC VPN**

使用PPPoe、GRE、IPSec体系等技术实现三层的远程虚拟互联，确保企业VPN的安全，支持多达十种常见不常见的IPSec应用场景。

中科神威防火墙V4.0的IPSec VPN既能够提供网关到网关的安全隧道，也支持客户端到网关的隧道，支持与各种基于标准IPSec协议的VPN设备互联，可以方便地实现星型或者网状结构的VPN拓扑，并提供隧道内的路由功能。

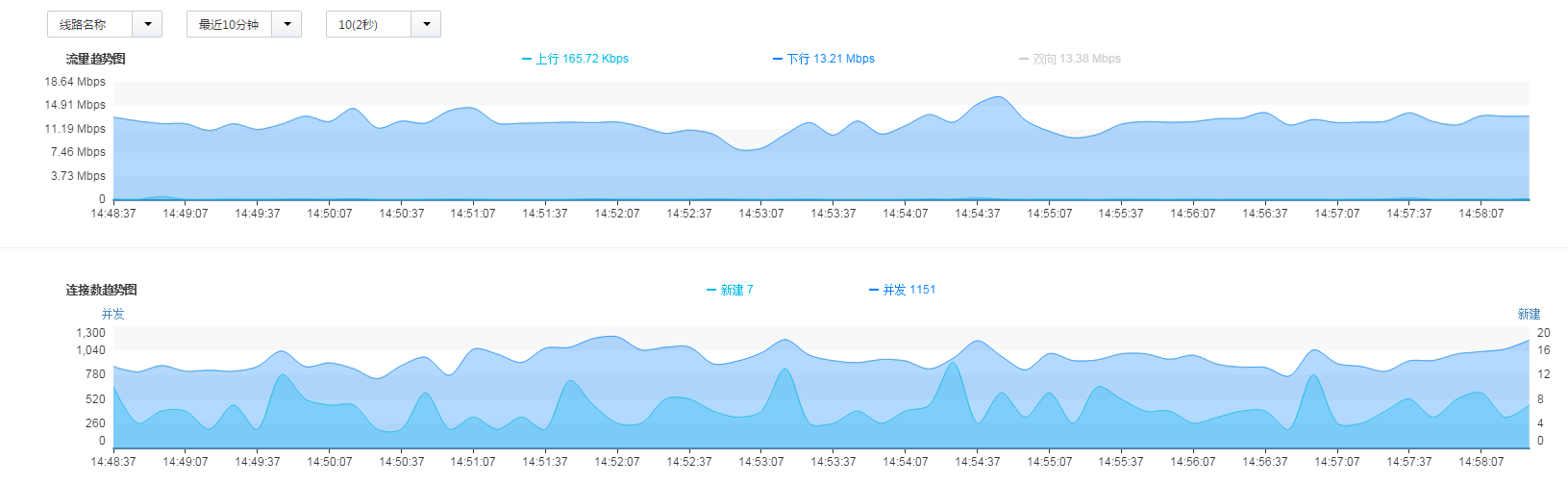
**2）SSL VPN**

中科神威防火墙V4.0网关使用SSL代理、SSL VPN相关技术，实现基于SSL安全的远程互联，简化企业网络配置和免除VPN客户端。支持SSL帐号密码防暴力破解功能，支持多种windows操作系统，支持对包括登陆前和登录后界面的整体界面定制，满足客户个性化风格的要求；支持选择性缓存动态Web页面，提升Web类资源的访问速度；支持基于角色的方式控制vpn接入用户的访问权限，并能利用安管系统进行集中管理和维护、智能升级、实时监控。

### 细则全方位流可视化，全局则安全风险指

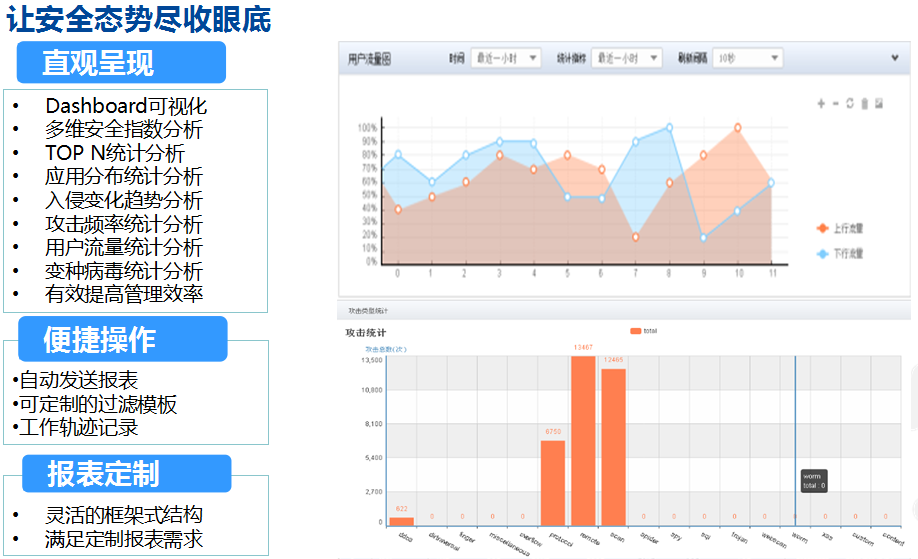
**1）细致详尽的全方位安全可视Security Visualation化**

中科神威防火墙V4.0基于网威云安全操作系统ISOS的多级立体全方位可扩展的流可视框架，开发出多种详尽的流实时可视功能；支持与网威SOC安管系统的联动，以实现各种流相关信息的历史详尽记录和可视化、分析和报表。中科神威防火墙V4.0支持基于接口的流量统计、基于应用的流量统计、基于应用的流量统计、基于p2p的流量统计、基于各种维度相组合的流量统计；支持应用识别分布及各应用具体分布情况；支持抗攻击事件、IPS事件、内容过滤事件等统计和报表。



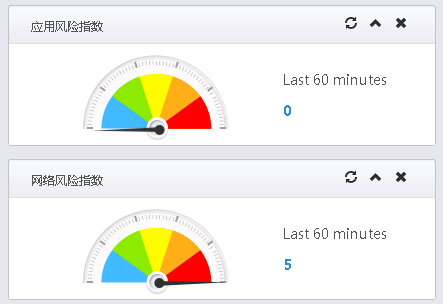






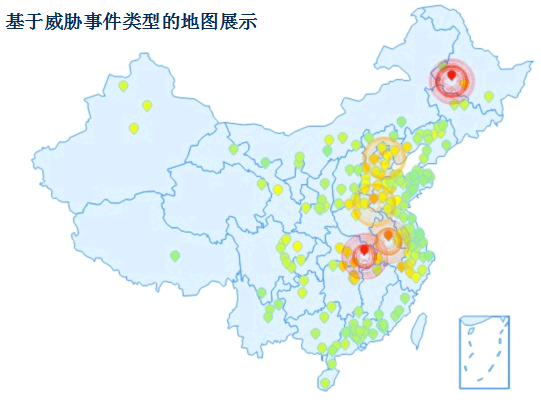
**2）基于全局理念的安全指导指数**

中科神威防火墙V4.0不仅提供在各种详细复杂的流量统计和流可视，还在主动检测技术的基础上，通过定期探测和收集监控网络中的各设备、应用服务、各网络节点、当前网络安全事件状况等信息，再加通过一定算法和关联、综合分析，提炼出网络环境中的网络安全指数、应用安全指数以及应用安全等级等指导、警示性数据，从总体评估网络的风险情况和应用的可用性，为网管配置提供参考。



**3）攻击态势感知展示**

中科神威防火墙V4.0支持基于安全事件的地图展示:支持包括按源地区和目的地区展现进行查询；支持地图上展现的威胁类型：病毒、入侵防范、僵木蠕、攻击防范、全部威胁；支持包括最近一个小时、一天和一个月进行详细查询；支持光标指向该地域的名称及攻击数，点击该地域跳出详细信息列表；支持严重程度通过颜色进行区分：支持地图上用不同颜色展示不同次数的攻击。



中科神威防火墙V4.0支持基于地理位置的威胁分析。

中科神威防火墙V4.0支持基于威胁事件类型的地图展示。

# 解决方案

## 小型企业和分支机构

**现状和需求**

关注上网行为管理功能；

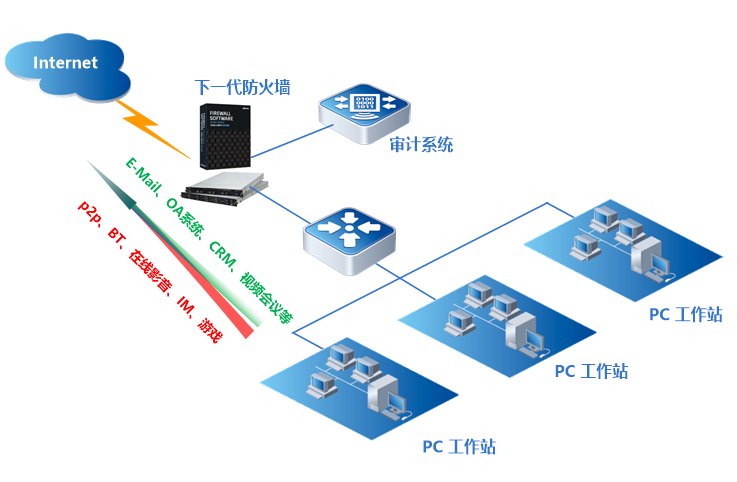
有闲置主机，投入越小越好。

**网威方案**

下载安装中科神威防火墙V4.0软件，即可获得企业级的下一代防火墙，解决对员工的上网行为的应用管控和带宽限制，并提供专业的VPN功能，满足外出员工接入和上级单位上联的需求。

如使用低配置主机，则建议采用中科神威防火墙V4.0服务器版软件，直接安装并运行在主机上。

如使用高性能服务器，则建议采用中科神威防火墙V4.0虚拟化版软件，与CRM或ERP等VM系统并行运行，实现对重要系统的安全防护同时，管控上网行为。



图一 中科神威防火墙V4.0小型企业和分支机构解决方案示意图

## 传统企业网

**现状和需求**

采用传统IT建设方案，需要厂商提供持续的技术服务支持。

主要关注设备处理性能和IPS入侵防御检测技术能力。

**网威方案**

建议选购网威软硬一体的下一代防火墙硬件。中科神威防火墙V4.0提供了专业的入侵检测、病毒过滤、挂马网站识别、DDoS流量清洗等IPS入侵防御检测技术功能。



图二 中科神威防火墙V4.0传统企业网解决方案示意图

## 私有云数据中心

**现状和需求**

基于终端虚拟化和服务器虚拟化技术，组建了终端数据不落地的云数据中心。

重点关注网络边界的安全防护、VM间的安全隔离和数据防泄漏。

**网威方案**

建议在网络边界部署网威软硬一体的下一代防火墙设备，在服务器的VM环境中部署中科神威防火墙V4.0虚拟化版软件。

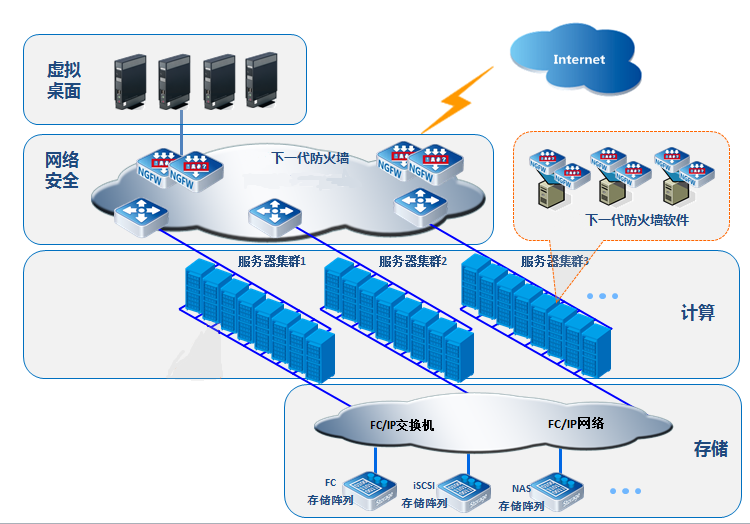
提供高性能的NAT功能，实现内网隐藏；

提供专业的IPS入侵防御检测技术功能，拦截入侵攻击行为；

可审计内部数据的导入和导出，对于导出数据可透明的打标签和加密，严防数据泄露；

提供专用的终端管理软件，管理终端外设，实现数据不落地，避免数据外泄；

提供VPN功能，满足外出员工接入和私有云间互联的需求。



图三 中科神威防火墙V4.0私有云数据中心解决方案示意图

## 公有云数据中心

**现状和需求**

安全防护功能以服务方式提供，可以按用户需要选择启用。

安全防护功能需要丰富，可模块化提供给用户。

**网威方案**

建议在网络边界或安全域边界部署高性能的中科神威防火墙V4.0设备，或者选用下一代防火墙服务器版软件安装于高性能服务器上。

通过API接口，中科神威防火墙V4.0可以与租户管理系统联动，带宽保障、IPS入侵防御检测技术、DDoS流量清洗、防病毒等等功能模块可按租户需要选择购买启动。

图四 中科神威防火墙V4.0公有云数据中心解决方案示意图

# 结束语

中科网威针对目前网络安全的形势，在具有自主知识产权的中科网威ISOS安全操作系统的基础上，推出具有二到七层协议保护，“七位一体”细粒度安全防护的面向云计算、面向虚拟化、面向未来，面向数据中心、公共云和私有云安全防护解决方案的下一代防火墙。并在智能化、面向第三方的开发支持、多深度解析技术融合的引擎一体化、流及安全可视Security Visualation、一站式配置上具有独创技术和强劲的竞争力。基于中科神威防火墙V4.0的私有云和共有云安全解决方案必将在安全领域和云计算领域掀起一轮新的“革命”。