网康科技 NETENTSEC

网康Web应用防火墙 WAF

——Web立体防护　协同安全服务

“三位一体”的Web安全防护

增值服务

- 网站加速
- 负载均衡
- 攻击分析
- 应用监控

产品价值

精细化Web安全防护
防护7大类Web攻击威胁。精细化的规则配置，发挥最大的安全防护功能，有效应对OWASP Top10定义的威胁及其变种。

HTTPS卸载/加速
针对SSL加密应用，WAF根据业务模型提供HTTPS卸载和HTTPS加速应用，从而保证服务器的安全性和可靠性。

完整的网页防篡改解决方案
提供网页监控、同步、发布功能。基于文件夹驱动级保护技术和事件触发机制，有效保护网页不被篡改。

HTTPS网守应用
提供HTTP转换成HTTPS的网守服务，能为客户提供无缝HTTPS服务，从而最大保护客户数据安全性。

Web防扫描
监控Web扫描行为，并对扫描行为实时进行记录、分析、阻断。

网页挂马主动诊断
提供网页挂马检测功能，全面检查是否被植入恶意代码，防止客户端主机沦为攻击者的肉鸡，同时防止客户端的敏感信息泄露。

专业DDoS防护
采用主动监测加被动跟踪相结合的防护技术，实时辨别多种DDoS攻击，高效完成DDoS攻击的过滤和防护，有效防止最常见的CC和SynFlood攻击。

Web扫描支持
网康WAF提供Web漏洞扫描系统，定期对客户Web资源进行安全体检，从而进行事前防范和处理。

产品特点

01 一体化防护
三位一体：监测+防护+补偿
支持WAF与防篡改一体化联动

02 云监控
通过网康云安全平台，实时监控指定的网站，定期输出网站应用报告及安全报告

03 高稳定
双系统运行
支持HA

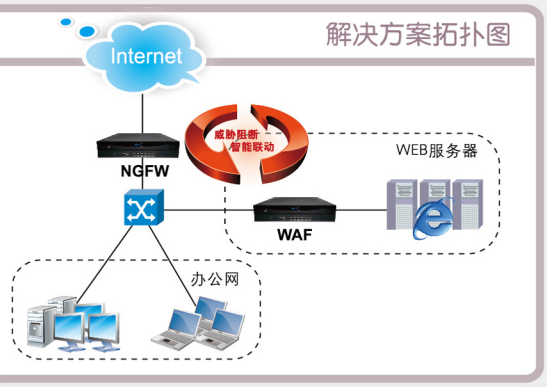
咨询热线：400-678-3600　网康官网：www.netentsec.com　网康科技　地址：北京市海淀区中关村东路66号世纪科贸大厦A座3层（100190）

网康科技 NETENTSEC

更多信息请咨询网康服务热线：400-678-3600

NGFW+WAF 专业的内外网整体安全解决方案

解决方案拓扑图



NGFW与WAF的产品定位

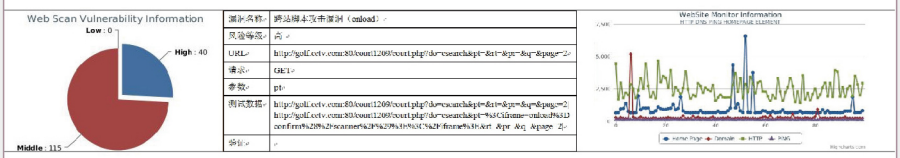
名称	NGFW	WAF
产品目标	应对当今网络边界威胁而定义的新一代安全设备	针对Web应用威胁的专业安全防护设备
防御范围	可信安全域与非可信安全域之间的网络攻击、木马、病毒、蠕虫、僵尸等边界安全	由Web应用（基于HTTP、HTTPS协议）的各种协议漏洞和应用漏洞所导致的Web攻击、泄密等恶意行为
部署位置	网络边界出口	Web Server前端
技术架构	流技术	代理技术

拓扑图

监控政府、教育、金融、大企业等各行业的Web应用安全和运行状况

网康“云监控”服务平台

安全监控 应用监控



“云监控”定期输出的应用安全和运行状况报告

WAF 功能列表

网络部署	透明模式部署、路由模式部署、网关模式部署、旁路模式部署、云部署
	VLAN划分，支持多VLAN环境下的部署
	链路聚合(Channel)部署，提高链路带宽
网络层安全	支持网络层访问控制
	支持URL级别访问控制
	支持IP级别黑、白名单
Web安全	识别和阻断SQL注入，Cookie注入，命令注入、跨站脚本(XSS)注入、WebShell攻击
	对网页请求/响应内容中的非法关键字进行检测、过滤
	能识别和阻断敏感信息泄露，恶意代码攻击、错误配置攻击、隐藏字段攻击、会话劫持攻击、参数篡改攻击、缓冲区溢出攻击、弱口令攻击
	能控制网络爬虫，能控制网络扫描行为
	提供多种威胁处理方式：返回错误码、重定向、监控、默认动作等
	支持HTTPS卸载和应用加速：即客户端到服务器端可以任意选择HTTPS和HTTP，强化应用层安全。比如从客户端到WAF使用HTTPS，从WAF到服务器使用HTTP（HTTPS）
	支持HTTPS网守服务，提供安全的网络访问
	采用基于行为分析的检测技术，对0day攻击能够很好地防范
Web应用加速	具备系统内嵌应用加速模块，通过对各类静态页面及部分脚本高速缓存，提高访问速度
负载均衡	服务器负载均衡设备：支持多服务器的负载均衡，工作在网关模式，对保护的多台负载WEB服务器，达到平均分发、按比例分发、负载分摊、响应比分摊等多种负载均衡模式
	具有网络层负载均衡功能
	协同现有均衡器协同工作：能配合现有的负载均衡设备协同工作，支持任意部署，而不影响客户现有拓扑
	支持链路负载均衡和自动路由选择
升级系统	支持系统的离线升级
	支持规则库的离线升级及在线自动升级
	每月提供一次规则升级；紧急事件第一时间提供升级

网页防篡改	能进行跨不同服务器的网页防篡改
	采用内核级防篡改保护，能及时阻止并报告攻击事件
	支持Windows、Linux、Unix三个操作系统的网页防篡改
	支持超过4GB以上网页防篡改保护和恢复功能，以适应客户业务发展需要
DDOS支持	支持Syn-Proxy代理模式抵御DDos攻击
	支持对Http的GET CC攻击防范
	支持每客户端和服务器的连接数限制
	支持SYNFlood，ICMPFlood，UDPFlood防范
	支持对每服务器进行的Icmp，Udp，Tcp的流量控制
审计功能及告警	1）对攻击事件进行审计，记录访问的时间、IP、事件类型、资源、参数等 2）对受保护的内容访问的升级 3）对与系统自身安全相关的下列事件产生审计记录 4）管理员登陆后进行的操作行为 5）对安全策略进行添加、修改、删除等操作行为 6）对管理角色进行增加、删除和属性修改等操作行为 7）对其他安全功能配置参数的设置或更新等行为
	支持syslog、SNMP协议、邮件等多种告警方式、短信报警
报表功能	系统支持对一定时期（包括年、月、周）的攻击进行统计并查询
	系统须能够对遭受攻击按照攻击次数、防护的网站、遭受攻击的网页、攻击类型、攻击时间（或者发现攻击的时间）等进行统计并排名
	能够根据访问防护的网站、被篡改内容、篡改内容的类型、试图进行的篡改、成功的篡改、发现的日期、事件发生的日期等条件进行详细信息的查询
Web扫描	提供Web安全扫描功能
	自定义Web安全扫描任务，定期进行Web安全扫描，报告自动发送管理员
	对Web扫描事件进行分析，提供Web验证功能，防止误报
冗余功能	支持双机热备，主主模式运行，主备模式运行
	支持VRRP协议，VRRP组管理
	支持双系统冗余备份，保证系统，不停机