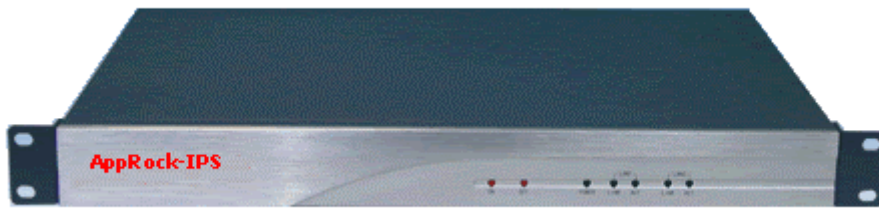


AppRock-IPS 入侵防御

简介

AppRock 入侵防御系统能够阻止蠕虫、病毒、木马、拒绝服务攻击、间谍软件、VOIP 攻击以及点到点应用滥用。通过深达第七层的流量侦测，AppRock 入侵防御系统能够在发生损失之前阻断恶意流量。利用华城技术提供的安全疫苗服务，入侵防御系统能得到及时的特征、漏洞过滤器、协议异常过滤器和统计异常过滤器更新从而主动地防御最新的攻击。此外，AppRock 的入侵防御系统是目前能够提供微秒级时延、高吞吐能力和带宽管理能力的强大的入侵防御系统。通过全面的数据包侦测，AppRock 的入侵防御系统提供百兆速率上的应用、网络架构和性能保护功能。应用保护能力针对来自内部和外部的攻击提供快速、精准、可靠的防护。由于具有网络架构保护能力，AppRock 的入侵防御系统保护 VOIP 系统、路由器、交换机、DNS 和其他网络基础设施免遭恶意攻击和防止流量出现异常。AppRock 的入侵防御系统的性能保护能力帮助客户来遏制非关键业务抢夺宝贵的带宽和 IT 资源，从而确保网路资源的合理配置并保证关键业务的性能。AppRock 产品型号可以满足从 SOHO 办公、中小企业、到大企业的各种组网需求。



产品特点

主动式的入侵防御

AppRock IPS 可以被“in-line”地部署到网络当中去，对所有流经的流量进行深度分析与检测，从而具备了实时阻断攻击的能力，同时对正常流量不产生任何影响。基于其高速和可扩展的硬件平台，AppRock IPS 不断优化检测性能，使其能够达到高吞吐量和低延时，同时可以对所有主要网络应用进行分析，精确鉴别和阻断攻击。事实上，AppRock IPS 所具备的超高性能与精确阻断能力，已经彻底重新定义了网络安全的内涵，并且从根本上改变了保护网络的方式，帮助客户实现持续降低 IT 成本、持续提高 IT 生产率的目标！

全面的安全保障

AppRock IPS 在跟踪流状态的基础上，对报文进行 2 层到 7 层信息的深度检测，可以在蠕虫、病毒、木马、DoS/DDoS、后门、Walk-in 蠕虫、连接劫持、带宽滥用等威胁发生前成功地检测并阻断，而且，AppRock IPS 也能够有效防御针对路由器、交换机、DNS 服务器等网络重

要基础设施的攻击。AppRock IPS 还支持基于访问控制列表（ACL）的检测、基于统计的检测、基于协议跟踪的检测、基于应用异常的检测、报文规范检测（Normalization）、IP 报文重组和 TCP 流恢复。以上机制协同工作，AppRock IPS 可以对流量进行细微粒度的识别与控制，有效检测流量激增、缓冲区溢出、漏洞探测、IPS 规避等一些已知的、甚至未知的攻击。

综合管理中心

AppRock 防火墙提供了多种配置方式，包括基于 Console 的命令行管理方式、普通的 WEB 管理方式、基于 SSL 的 WEB 管理方式和基于 SNMP V2 的网管平台。AppRock IPS 远程图形管理是集成在 IPS 设备中的基于安全 Web 的管理软件，可以提供对 IPS 进行管理的基本功能，包含配置、监测、报表等；

无缝部署

AppRock IPS 支持无缝部署，无论对已经建成的网络，还是正在建设中的网络，都可以很容易地将 AppRock IPS 嵌入进任何部分，并且不会对网络的拓扑、性能、运行带来任何改动。从逻辑上来看，AppRock IPS 就好像一道智能的安全防线，这道智能的安全防线从根本上解决了困扰网络的安全问题。无缝部署主要体现在以下方面：嵌入式部署（in-line）模型保证最简化的部署步骤，而不需要进行交换机镜像等复杂的配置，更不需要更改网络拓扑；检测接口不需要 IP 地址，一旦接入网络，立刻开始保护网络；同时保证自身对攻击源是隐身的，增强整网的安全性；高性能、低时延使得 AppRock IPS 无论被部署在网络内部还是边缘，都可以提供线速的精确检测和实时阻断能力，对网络业务的效率没有任何的损伤。同时，卓越的带宽管理能力将加速异常情况下的业务应用。

功能特性

攻击特征库	当前可检测攻击的最大数目	1,600+
攻击类型	蠕虫（Worm）	√
	引入蠕虫（Walk-in Worm）	√
	病毒（Virus）	√
	木马（Trojan）	√
	间谍软件（Spyware）	√
	广告软件（Adware）	√
	可疑代码（Suspicious）	√

	拒绝服务 (DoS/DDoS)	√
	带宽劫持 (Bandwidth Hijack)	√
	探测与扫描 (Reconnaissance)	√
	后门 (Backdoor)	√
	非法接入 (Invalid Access)	√
	混合威胁 (Blended Threat)	√
	VoIP 攻击 (VoIP Attack)	√
协议分析	VLAN	√
	ARP	√
	MPLS	√
	ICMP	√
	IP	√
	TCP	√
	UDP	√
	HTTP	√
	DNS	√
	RPC	√
	Telnet	√
	FTP	√
	IMAP	√
	SMTP	√
	SMB	√
应用跟踪-P2P (部分列表)	Kazaa	√
	eDonkey	√
	WinMX	√
	BT	√
应用跟踪-IM	MSN	√
	ICQ	√
	Yahoo Messenger	√
	Skype	√
应用跟踪	Oracle	√
	SQL	√
允许通过	Permit	√
阻断	Block	√
报警	Alert	√
限流	Rate Limit	√

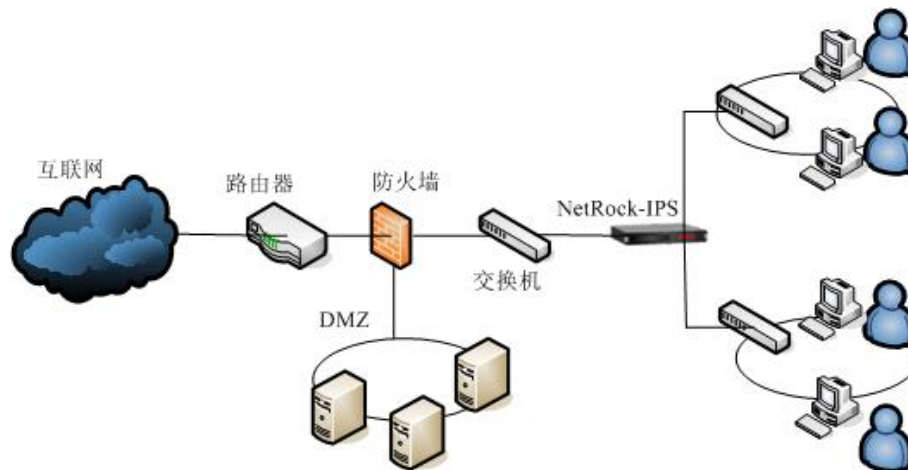
包追踪	Packet Trace	√
记录日志	Log	√
网管	SNMP	√
电子邮件	Email	√
日志	Syslog	√
面板 LED 指示	电源运行状态	√
	设备运行状态	√
命令行	初始化设备配置	√
Web 管理	集成在 IPS 设备中的基于 Web 的管理	√
定期发布	每周定期发布数字疫苗	√

系统配置

项 目	AppRock-IPS 描述
外型尺寸 (mm) 宽×深×高	482×370×45 (mm)
重量	5kg
插槽	PCI 扩展
固定接口	1 个 RS-232 配置口 4 个以太网口
处理器主频	2.4GHz
网络吞吐量 (Mbps)	200
安全过滤带宽 (Mbps)	200
用户数	不限制
固态存储	128MB
SDRAM	1GB
输入 电压	DC 额定电压: +5V
工作环境温度	0 ~ 60°C
环境湿度	5~ 90% 不结露
抗冲击	10G 峰-峰加速度 (11ms)
抗震动	5-17Hz, 0.1" 双峰位移; 17-640Hz, 1.5G 峰-峰加速度
电磁干扰	符合 FCC/VDE A 级标准

组网

这是常见的 IPS 部署案例，利用 IPS 保护内部网络免受各种攻击的威胁。



IPS 部署在内部网络交换机的通路上，检测所有流向内部网络的数据流量，对于任何攻击，都将进行实时阻断。

规则库配置

特征库名称	使能状态	过滤动作
ATTACK-RESPONSES	↑	⊗
BACKDOOR	↑	⊗
BAD-TRAFFIC	↑	⊗
CHAT	↑	⊗
DDOS	↑	⊗
DELETED	↑	⊗
DNS	↑	⊗
DOS	↑	⊗
EXPLOIT	↑	⊗
FINGER	↑	⊗
FTP	↑	⊗
ICMP	↑	⊗
ICMP-INFO	↑	⊗
IMAP	↑	⊗
INFO	↑	⊗

