UNIS W2000系列 Web应用防火墙

产品概述

UNIS W2000-G30

UNIS W2000-G50

随着网络技术的不断普及与发展，大部分政府部门、企业单位等各类组织机构选择通过 Web 应用服务来构建业务信息发布及交互应用平台，然而伴随着网络技术的迭代，各类信息安全攻防技术也在进化，黑色产业也逐渐的规模化，其 Web 业务系统所面临的威胁也就越来越多。

UNIS W2000-G 系列是紫光恒越技术有限公司（以下简称紫光恒越）自主研发的一款专注于第七层防护的 Web 应用安全产品，适用于各类用户应用场景下的等级保护等合规及自建需求。该产品采用重写的 TCP 协议栈及 PXM 多核调度处理引擎，高效精准的实现各类 SQL 及命令注入、跨站脚本攻击、网页挂马、扫描器扫描、多类敏感数据信息及网站指纹信息泄露、盗链行为等攻击的防护。同时，该产品支持透明代理模式、旁路监听/阻断模式、反向代理模式、混合等多种部署模式，另外在透明/反向代理部署模式下还支持多种 HA/软硬件 Bypass 方式，便于部署配置以及维护。

UNIS W2000 系列产品包括 W2000-G30、W2000-G50 共计两个型号，广泛适用于“金融、运营商、政府、公安、教育、能源、税务、工商、社保、卫生、电子商务”等所有涉及 Web 应用的各个行业。通过部署该产品，可以帮助用户解决目前所面临的各类网站安全问题。

产品特点

◆ **先进的重构协议栈及多核调度控制器**

◎采用全新自主设计的 TCP 协议栈，并且将 TCP 协议栈移植到用户空间层，打破了传统信息安全性能瓶颈；

◎采用自行开发的多核并行控制程序，实现 CPU 多核心均衡并行数据包的分发，根据 CPU 核心的负载程度动态的分配数据，最大化发挥 CPU 的处理能力。

◆ **轻量化的多安全引擎**

◎支持功能强大的 HTTP 代理检测引擎，通过特征库、协议安全、内容安全三大安全模块全面解决用户 Web 站点的 HTTP 安全问题；

◎支持经过优化的轻量型的 IPS 引擎，用于解决 Web 应用系统所依赖的周边环境安全问题；

◎支持针对 HTTP 及 FTP 协议的上传行为恶意代码检测引擎，有效避免重要的 Web 业务服务器沦为传播病毒、木马的源头；

◎支持低消耗的 Web 扫描引擎，帮助用户快发现并速识别 Web 应用相关明显漏洞。

◆ 精确的双向细粒度检测规则

◎针对 HTTP/HTTPS 流量数据进行双向多重过滤，精确识别协议中的各种要素（如 Cookie、Get 参数、Post 表单等），对其进行实时的在线或旁路拦截。解码预处理机制采用非简单的字符串的过滤，是在进行各种解码的基础上进行攻击检测，检测包括 URL 参数、Web 表单输入、HTTP header 等 Web 交互信息，同时对攻击的逻辑特点及行为进行分析过滤；

◎满足 OWASP TOP 10 绝大部分的威胁防御；

◎具备精准与模糊特征库分类。

◆ 多层次的 WebShell 防护

◎支持防御多种 WebShell 威胁。可针对 WebShell 上传，进行控制、过滤与阻断；

◎支持对 WebShell 访问返回页面进行内容检测，切断入侵者企图调用访问 WebShell 的行为，最后，实时检测过滤 WebShell 发起的各种攻击命令。

◆ 安全可视

◎支持可独立大屏展示的威胁监控及设备运行页面，安全趋势与设备运行状况一目了然；

◎具备详细的攻击数据统计信息，以攻击地图、数据排列统计图表等多种方式展现网站威胁及流量；

◎具备丰富的日志及报表展示功能，囊括 7 大类日志及攻击、访问、综合等多类报表的定制功能。

◆ 灵活可靠的部署方式

◎支持透明、反向、旁路、混合、聚合等多种接入部署方式；

◎支持 HA-主主/主备部署模式，并搭配多种失效检测方式；

◎支持软硬 bypass 业务逃生机制，保障业务优先。

↗ 产品规格

属性	W2000-G30	W2000-G50
部署模式	支持透明代理部署、反向代理部署、旁路侦测/阻断部署、混合模式部署	
防护功能	支持 SQL、命令、LDAP 等注入攻击特征防护	
	支持 XSS 攻击特征防护	
	支持溢出攻击特征防护	
	支持 WebShell 特征防护	
	支持 Shell 恶意代码特征防护	

	支持 Web 应用扫描攻击特征防护	
	支持异常 URL 特征防护	
	支持网页木马特征防护	
	支持自定义特征规则	
	支持网页方位合规及逐级访问防护	
	支持防盗链	
	支持参数合规检查	
	支持口令爆破防护	
	支持数据库错误信息/Web 目录内容/Web 程序代码/自定义数据类型泄露防护	
	支持危险文件类型上传/下载检查	
	支持自定义溢出参数检查	
	支持 CSRF 防护	
	支持 HTTP 协议检查	
属性	W2000-G30	W2000-G50
	支持短文件/文件夹防泄漏	
	支持禁用/敏感词防护	
	支持 HTTP 请求方法控制	
	支持爬虫防护	
	支持扫描阈值防护	
	支持网站隐身	

	支持 URL 访问控制
	支持 Cookie 安全过滤/溢出/白名单检查
	支持安全域名服务器挂马监控
	支持 URL 例外
	支持网络层 DOS/应用层 CC 攻击防护
	支持全局黑白名单防护
	支持动态黑名单防护
	支持轻量型 IPS/病毒上传特征防御
威胁可视	支持可独立显示的威胁可视展示页面，包括威胁地图/威胁分类/威胁趋势/设备运行状况 支持单独的 Web 威胁监控页面 支持单独的 IPS 威胁监控页面 支持单独的流量统计监控页面
自学习	支持访问来源黑白名单学习方式 支持访问目的 URL 黑名单学习方式 支持 URL 参数及 Cookie 学习 支持网站目录树学习 支持文件类型学习
静态页面缓存	支持防篡改模式 支持缓存类型设定

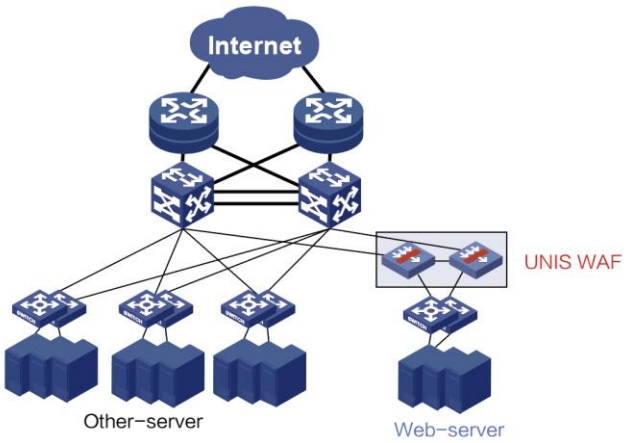
	支持缓存监控交互列表 支持缓存周期及空间大小设置	
日志	支持 Web 安全日志/入侵防御日志/病毒日志/爬虫日志/访问日志/管理员日志/系统日志 支持日志本地导出 支持日志外发	
报表	支持综合报表/Web 攻击报表/IPS 攻击报表/病毒报表/爬虫报表/访问报表 支持计划任务	
属性	W2000-G30	W2000-G50
	支持邮件发送 支持 HTML/CSV/XLS/DOC/PDF 等多种报表格式	
高可靠性	支持透明代理主主/主备部署 支持反向代理主备部署 支持硬件 bypass 支持性能阈值逃生软件 bypass	
HTTPS 代理	支持 HTTPS 服务器的防护	
告警	支持 syslog/邮件/短信/snmp-trap 等多种告警方式 支持邮件和短信告警汇聚	
设备管理	支持特有的读/写/审计权限分离用户设置	
	支持用户密码复杂度	

	支持特征库在线及离线更新
	支持特征库版本回滚
	支持自动保存配置
	支持如登录失败惩罚/信任主机等各类管理控制

典型组网

◆ **企业级 Web 应用安全透明代理部署方案**

UNIS W2000 系列 Web 应用防火墙可部署在企业 Web 应用服务器接入交换区，对 Web 应用服务区的所有服务器业务流量提供集中一站式的分析过滤功能，防范各种来自外部威胁的且不需要对原有逻辑拓扑进行任何改动，同时通过 HA 技术保证与原有的主备链路冗余同步，消除单点故障。

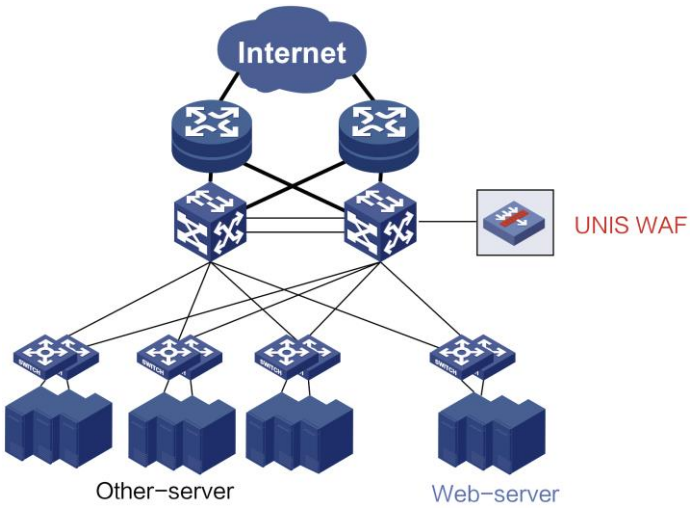


UNIS W2000-G 系列 Web 应用防火墙透明代理主备接入示意图

◆ **数据中心级 Web 应用安全反向代理部署方案**

UNIS W2000 系列 Web 应用防火墙可旁挂在数据中心交换机上，为了避免其他不必要的流量经过，一般通过接收出口或其他网关设备引导的定向 HTTP 访问流量并对原始数据头部进行相应修改，以达到隐藏真实服务器 IP 地址的目的，保护 Web 应用服务器免

遭外部威胁攻击。



UNIS W2000-G 系列 Web 应用防火墙反向代理接入示意图

紫光恒越技术有限公司

www.unisyue.com

北京基地
北京市海淀区中关村东路 1 号院 2 号楼 402 室
邮编：100084
电话：010-62166890
传真：010-51652020-116
版本：

客户服务热线
400-910-9998