UNIS T1000-12T12F-G2 入侵检测与防御系统

产品概述

UNIS T1000-12T12F-G2 入侵检测与防御系统是业界领先的 IPS 产品，以在线或旁路的方式部署在网络的关键节点上，对数据进行 2-7 层的全面检查和分析，提供强大的 Web 防护功能，实时阻断和记录网络流量中的病毒、蠕虫、木马、间谍软件、网页篡改、注入攻击、跨站攻击、DDoS 攻击、漏洞扫描、异常协议、网络钓鱼等网络攻击，并有效地管理 IM 软件、P2P 工具、流媒体、网络游戏、股票软件等网络滥用行为，还集成了有效的带宽管理、URL 过滤、关键字过滤等功能，提供业界全面完善的 IPS 解决方案。UNIS T1000-12T12F-G2 入侵检测与防御系统提供不同档次的型号产品，适用于数据中心、大型网络边界、中小型企业等多种业务应用场景。

UNIS T1000-12T12F-G2

产品特点

◆ 多业务高性能

UNIS T1000-12T12F-G2 入侵检测与防御系统采用先进的多核架构，采用病毒库树形存储、流扫描处理等领先的防病毒技术，并采用零拷贝并行流处理等高效的防攻击技术，整个解析过程一次拆包，保证开启多重防护功能后依然保证高速度、低时延的安全防护。

◆ 精细、及时的入侵检测特征库

紫光恒越经过多年在网络安全领域沉淀和积累，打造了一支资深的攻击特征库团队和安全服务团队，随时关注业界新发现的安全漏洞和接收全球用户反馈的攻击特征，并在第一时间做出响应和提供更新，实时完善攻击特征库，提供及时全面的入侵防御。

◆ 专业的病毒查杀

UNIS T1000-12T12F-G2 入侵检测与防御系统拥有海量病毒特征库，配合先进的反病毒引擎，能够精准识别并清除流行木马和顽固病毒。新一代启发式检测技术，通过对程序行为的智能分析，及时发现新的未知病毒威胁，提示用户及时修复系统和第三方软件（Flash、Adobe Reader 等）漏洞，有效保障系统安全。针对纯扫描优化的产品架构，无系统监控，不占系统资源，是保护内网资源不受互联网病毒侵扰的绝佳选择。

◆ 文件上传过滤

UNIS T1000-12T12F-G2 入侵检测与防御系统内置病毒过滤引擎和实时更新的病毒特征库，可以对通过 HTTP 和 FTP 协议上传的文件进行病毒过滤和阻断，防止网站被恶意利用，成为病毒和木马传播的工具。

◆ 遏制带宽滥用

UNIS T1000-12T12F-G2 入侵检测与防御系统能够全面识别互联网常见应用，包括经常造成带宽滥用、工作效率降低的 BT 下载、IM 及时通讯、在线视频等。将 IPS 入侵系统部署于网络的出口，可以有效地遏制各种应用抢夺宝贵的带宽和 IT 资源，从而确保网络资源的合理配置和关键业务的服务质量，显著提高网络的整体性能。

◆ 远离恶意邮件

UNIS T1000-12T12F-G2 入侵检测与防御系统具有强大的反垃圾邮件功能，不仅可以做到收件人、发件人等的源头认证，还可以做到 SMTP 连接数限制、邮件大小限制、邮件内容关键字过滤等反垃圾邮件特性，更可以根据业务情况灵活自定义垃圾邮件策略。除此之外，反垃圾邮件策略还可以根据“贝叶斯”算法过滤垃圾邮件，让策略部署更简单、更智能。

◆ 六维一体化安全策略

UNIS T1000-12T12F-G2 入侵检测与防御系统的安全策略集成防攻击、防病毒、WAF、应用控制、带宽控制、身份认证六个管理维度，管理者可以根据不同的管控需求，为不同的用户定制不同的管理策略，灵活方便，维护简单，条理清晰，效果良好。

◆ 组网方式灵活

UNIS T1000-12T12F-G2 入侵检测与防御系统支持 RIP、OSPF、802.1Q 等网络特性，并支持在线或 IPS 旁路方式部署，支持路由模式、透明模式和混合模式，可在任意复杂的网络环境中灵活组网。

◆ 便捷的管理方式

UNIS T1000-12T12F-G2 入侵检测与防御系统支持本地管理和集中管理两种管理方式。当单台或小规模部署时，可通过本地命令行或者内置的 Web 界面进行图形化管理；在大规模部署时，可通过集中管理系统对分布部署的 IPS 入侵防御系统进行统一的配置策略下发、攻击事件监控和攻击事件分析。

◆ **高可靠性**

UNIS 入侵检测与防御系统支持软件 bypass 和硬件 bypass，能够从各个层面保证网络可靠性，在实现全面安全防护的同时，不会成为网络故障点，提升网络可靠性。

产品规格

属性	UNIS T1000-12T12F-G2
硬件平台	飞腾主机
管理接口	RJ45 x 1
Console口	RJ45 x 1(串口)
固定业务接口	12千兆电口+12千兆光口
扩展插槽数量	2
支持的扩展卡类型	4端口万兆接口卡
CPU	D2000
CPU主频	2.3GHz
CPU核数	8核
内存	32G内存
固态盘（内置）	512G
硬盘插槽数量	2
电源1+1冗余	支持
缺省配置重量	7.6Kg
外形尺寸（长×高×深/mm）	495mm×44mm×445mm
温度	工作：0～45℃
湿度	20% ~ 80% 非冷凝
输入额定电压	100 ~ 240V AC
最大输入电流	4A
功率	62W

功能特性

属性	说明	
网络安全性	安全防护	支持IPS，支持IPS自定义规则 支持应用控制及应用带宽管理 支持防病毒 支持URL过滤 支持应用识别 支持Web应用防护 支持威胁情报 支持工控白名单 支持bypass
	安全策略	实现安全区域划分 访问控制列表 基本ACL和高级ACL 基于安全区域的访问控制 基于时间段的访问控制 动态包过滤 MAC和IP绑定功能 基于MAC的访问控制列表

属性	说明	
	防范的网络攻击类型和网络滥用类型	蠕虫/病毒 木马 后门 DoS/DDoS攻击 探测/扫描 间谍软件 网络钓鱼 利用漏洞的攻击 SQL注入攻击 缓冲区溢出攻击 协议异常 IDS/IPS逃逸攻击 P2P滥用 IM滥用 网游滥用
	攻击防范	基本ACL和高级ACL 基于安全区域的访问控制 基于时间段的访问控制 ASPF DOS/DDOS攻击防范：包括SYN Flood、UDP Flood、ICMP Flood、DNS Flood、 畸形包攻击如：Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、IP分片报文攻击、分片报文攻击、TCP报文标志位不合法攻击、超大ICMP报文攻击、ICMP重定向或不可达报文 扫描窥探攻击防范：端口扫描、地址扫描、 静态和动态黑名单功能 连接数限制
	安全审计	攻击实时日志 域间策略匹配日志 黑名单日志 连接数限制日志 会话日志 流量统计和分析功能 安全事件统计功能

属性	说明	
网络协议	IP服务	ARP • 静态 ARP • 动态 ARP • ARP 代理 • 免费 ARP DNS • 本地静态域名 • DNS Server NTP • NTP Client VLAN • 802.1q VLAN 透传
	IP路由	静态路由管理 策略路由 动态路由 • RIP-1/RIP-2 • OSPF
高可靠性	支持 双机部署 支持选择性开启状态热备 支持静态链路聚合、 链路质量探测NQA	
配置管理	命令行接口	通过Console口进行本地配置 通过Telnet或SSH进行本地或远程配置 支持基于RBAC的细粒度权限控制，可以控制具体命令的权限 User-interface配置，提供对登录用户多种方式的认证和授权功能
	Web网管接口	支持通过Web方式进行配置 支持Web管理员的超时下线 支持Web用户的登录和鉴权 支持基于RBAC的细粒度权限控制，可以控制具体Web菜单的操作权限
	支持标准网管SNMP	支持SNMPV1、V2c和SNMPV3

部署方式

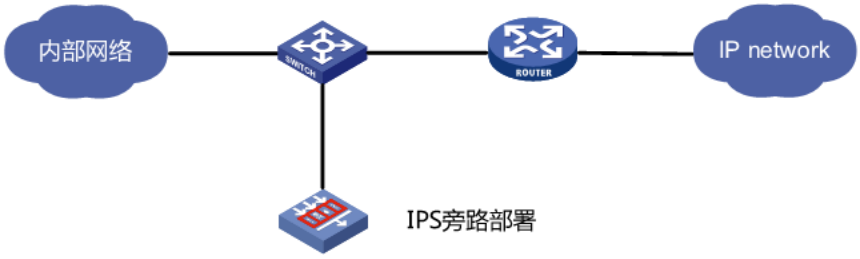
◆ IPS 在线部署方式

部署于网络的关键路径上，对经过的数据进行 2-7 层实时深度分析，防御内部和外部的攻击，管理双向的流量。

IPS在线部署

◆ IPS 旁路部署方式

对网络流量进行监测与分析，记录攻击事件并告警。



IPS旁路部署

紫光恒越技术有限公司

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：010-82054431
传真：010-82054401

www.unisyue.com

客户服务热线
400-910-9998