

UNIS T5000-CN30、UNIS T5000-CN60、UNIS T5000-CN80入侵检测与防御系统



UNIS T5000-CN30 / T5000-CN60 / T5000-CN80 产品外观图

产品概述

UNIS T5000-CN 系列产品是紫光恒越技术有限公司开发的业界领先的万兆 IPS 产品，包含 UNIS T5000-CN30、UNIS T5000-CN60、UNIS T5000-CN80 三个型号。UNIS T5000-CN 系列产品部署在客户网络的关键路径上，通过对流经该关键路径上的网络数据流进行 2 到 7 层的深度分析，能精确、实时地识别并阻断或限制黑客、蠕虫、病毒、木马、DoS/DDoS、扫描、间谍软件、协议异常、网络钓鱼、P2P、IM、网游等网络攻击或网络滥用，同时，UNIS T5000-CN 系列产品还具有强大、实用的带宽管理和 URL 过滤功能。

UNIS T5000-CN 系列产品是面向运营商及行业市场的高性能万兆 IPS 产品，硬件上基于国产多核处理器架构，为 1U 的独立盒式设备。提供 6 个扩展槽位，可支持千兆电口、千兆光口、万兆光口、40G 光口、100G 光口等丰富的接口卡，方便进行端口及业务扩充，支持双硬盘，满足日志存储需求。

在安全功能方面，UNIS T5000-CN 系列产品还一体化地集成了 IPS、AV、病毒、应用控制、URL 分类及自定义过滤等深度安全防御的功能，实现了基于用户、应用、时间、服务、IP 等多维度的策略控制功能。

在虚拟化和可靠性方面，基于领先的 UniwareV7 平台，支持多设备集群及 1:N 虚拟化。更好地适应云计算的要求的弹性扩展能力。

产品特点

◆ 高性能的软硬件处理平台

- UNIS T5000-CN 系列采用了专用的国产高性能处理器和高速存储器，可以提供超万兆以上的安全业务处理性能。
- UNIS T5000-CN 系列支持 6 个扩展槽位，可扩展支持 40G、100G 接口，方便业务扩容。
- UNIS T5000-CN 系列支持 2 个硬盘槽位，双硬盘支持 RAID 功能，日志存储稳定可靠。

◆ 完善的安全保障

业界完善的虚拟化解决方案

- 支持 N:1,1:N,N:1:M 等多种方式虚拟化，满足云计算资源池需求。

全面的网络安全防护能力

- 集成入侵防御与检测、病毒防护、带宽管理和 URL 过滤等功能，是业界综合防护技术领先的入侵防御/检测系统。通过深入到 7 层的分析与检测，实时阻断网络流量中隐藏的病毒、蠕虫、木马、间谍软件、网页篡改等攻击和恶意行为，实现对网络应用、网络基础设施和网络性能的全面保护。
- 丰富的攻击防范技术。同时支持 IPv4 和 IPv6。除提供普通的状态防火墙安全隔离技术外，针对异常报文攻击如 Land、smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、TCP 报文标志位不合法，地址欺骗攻击如 IP spoofing，扫描攻击如 IP 地址攻击、端口攻击，异常流量攻击如 Ack Flood、DNS Flood、Fin Flood、HTTP Flood、ICMP Flood、ICMPV6 Flood、Reset Flood、SYNACK Flood、SYN Flood、UDP Flood 等均能够提供有效防护。

全面、及时的攻击特征库

- 专业安全团队密切跟踪全球知名安全组织和厂商发布的安全公告，经过分析、验证所有这些威胁，生成保护操作系统、应用系统以及数据库漏洞的特征库。
- 特征库覆盖全面，包含了主流操作系统、主流网络设备、主流数据库系统、主流应用软件系统的全部漏洞特征，同时也包含了黑客、蠕虫、病毒、木马、DoS/DDoS、扫描、间谍软件、网络钓鱼、P2P、IM、网游等网络攻击或网络滥用特征。

丰富的响应方式

- 针对报文检测结果提供了丰富的响应方式，包括阻断、丢弃、允许、CP Reset、抓取原始报文、重定向、记录日志、告警等。
- 各响应方式可以相互组合，并且设备出厂内置了一些常用的动作组合，以方便客户使用。

完善的 IPv6 解决方案

- 所有特性全面支持 IPv6。
- 支持 IPv6 网络部署，支持 IPv6 管理、日志及审计。

电信级业务高可靠性

- 支持状态 1:1 热备功能，支持 Active/Active 和 Active/Passive 两种工作模式，实现负载分担和业务备份。
- 支持 SCF (安全集群系统)，支持多框集群和异构集群，实现灵活管理和弹性扩展。
- 故障隔离：软件模块化技术使软件的各个部分做到故障隔离。Uniware V7 的模块化设计，保证一个进程的异常不会影响其他进程以及内核的正常运行。软件的故障也可以通过自行恢复，不影响硬件的运行。

全面的管理监控手段

- 支持通过 Web-GUI、CLI、SSH 等多种手段管理设备。
- 基于角色的功能授权机制，可以实现到功能、命令行、菜单级的权限控制。
- 统一的 SSM 管理平台，可以实现设备的配置管理、性能监控、日志审计。
- 丰富的 MIB 节点便于外部设备进行性能监控。

开放的系统接口

- 开放接口：传统的网络操作系统为封闭的系统，有专用的系统概念和处理流程，缺乏开放性。而 Uniware V7 使用通用的 Linux 操作系统，回归了主流的软件实现方式。提供开放的标准编程接口，可供用户利用 UniwareV7 提供的基础功能，实现自己的专用功能，目前主要基于 Netconf 接口。
- TCL 脚本：Uniware V7 内嵌了 TCL 脚本执行功能，用户可以利用 TCL 脚本语言直接编写脚本，利用 Uniware V7 提供的命令行、SNMP Get、SET 操作，以及 Uniware V7 公开的编程接口等实现所需功能。
- EAA：可以在系统发生变化时执行预定义动作。在提高系统可维护性的同时，满足用户一些个性化需求。

产品规格

◆ T5000-CN30、T5000-CN60、T5000-CN80

项目	描述
接口	1个配置口 (CON) 2个外置USB host接口 业务接口选配，支持多种接口卡扩展
扩展槽位	6个，前插4个，后插2个 可支持8千兆光口接口卡、4万兆光口接口卡、8万兆光口接口卡等

硬盘扩展插槽	2 个硬盘扩展插槽，支持扩展 2 块 SSD 硬盘
电源	双电源，支持1+1 AC/DC冗余
风扇	4 个风扇
外型尺寸 (W×D×H)	442mm×435mm×44mm
环境温度	工作：0 ~ 45℃ 非工作：-40 ~ 70℃
环境湿度	工作：10 ~ 95%，无冷凝 非工作：5 ~ 95%，无冷凝

◆ 功能特性表

属性	说明	
网络安全性	DPI	支持IPS入侵检测与防御 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WAF 支持沙箱、蜜罐联动 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、ACK Flood、RST Flood、DNS Flood、HTTP 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、IP路由记录选项报文、Tracert报文 静态和动态黑名单功能 连接数限制

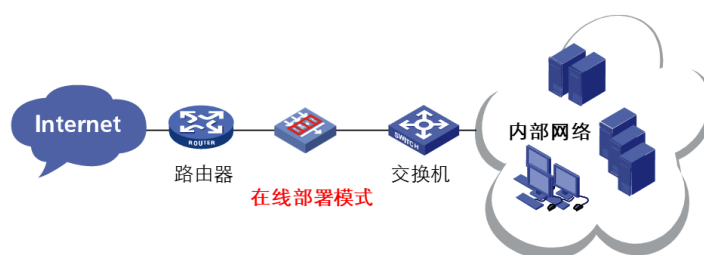
属性	说明	
	安全审计	攻击实时日志 域间策略匹配日志 黑名单日志 连接数限制日志 会话日志 流量统计和分析功能 安全事件统计功能
网络协议	IP服务	ARP <ul style="list-style-type: none"> • 静态 ARP • 动态 ARP • ARP 代理 • 免费 ARP DNS <ul style="list-style-type: none"> • 本地静态域名 • DNS Client NTP <ul style="list-style-type: none"> • NTP Client • NTP Server VLAN <ul style="list-style-type: none"> • 802.1q VLAN 透传
	IP路由	静态路由管理 策略路由 动态路由 <ul style="list-style-type: none"> • RIP-1/RIP-2 • OSPF • 路由策略

属性	说明	
高可靠性	支持集群部署 支持集群内1:1备份 支持选择性开启状态热备 支持静态链路聚合、支持动态链路聚合、支持跨设备链路聚合 支持链路质量探测NQA 支持BFD 支持软件不间断稳定升级，热补丁、ISSU 支持业务不间断处理，软件、硬件Bypass 支持与第三方网络、安全、镜像设备兼容对接使用	
部署方式	支持路由模式、透明模式、混合模式等。	
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

典型组网

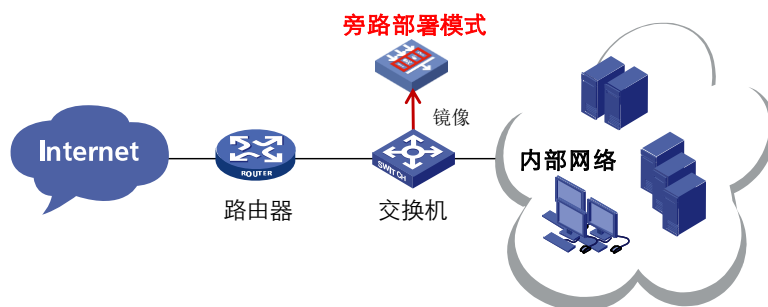
◆ IPS 在线部署方式

部署于网络的关键路径上，对流经的数据流进行 2-7 层深度分析，实时防御外部和内部攻击。



◆ IDS 旁路部署方式

旁路部署在网络上，对网络流量进行监测与分析，记录攻击事件并告警。



➤ 订购信息

◆ 主机及接口模块选购一览表

项目	数量	备注
T5000-CN30/T5000-CN60/T5000-CN80 主机	1	必配
接口模块 (4 万兆光口、8 万兆光口、8 千兆电口)	1-4	必配，至少一块

◆ License 选购一览表

项目	数量	备注
UNIS T5000-G 应用识别特征库升级服务授权函	0-N	选配
UNIS T5000-G AV 防病毒安全授权函	0-N	选配
UNIS T5000-G IPS/AV/ACG 特征库升级服务授权函	0-N	选配
UNIS T5000-G WAF 特征库升级授权函	0-N	选配

◆ 电源模块选购一览表

电源模块	描述	备注
PSR250-12A1-Z	UNIS 250W 交流电源模块	必配，至少选其一，至少配置 2 块，且不支持混插
PSR450-12A1-Z	UNIS 450W 交流电源模块	
PSR450-12D-Z	UNIS 450W 直流电源模块	

电源模块	描述	备注
PSR450-12AHD-Z	UNIS 450W 高压直流电源模块	

◆ 风扇模块选购一览表

风扇模块	描述	备注
LSPM1FANSB1-Z	UNIS 风扇模块(风扇侧出风)	必配 4 个

◆ 硬盘选购一览表

硬盘	描述	备注
NS-SSD-480G-SATA-M.2	UNIS 480GB M.2 SSD 硬盘模块	选配
NS-SSD-2T-SATA-M.2-Z	UNIS 2TB M.2 SSD 硬盘模块	选配

📖 说明：

“必配”表示所描述项目是设备正常运行的最小配置。

“选配”表示所描述项目是用户根据实际使用需要可选择配置。



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

Copyright ©2022 紫光恒越技术有限公司 保留一切权利
免责声明：虽然紫光恒越试图在本资料中提供准确的信息，但不保证资料的内容不含有技术性误差或印刷性错误，为此紫光恒越对本资料中的不准确不承担任何责任。
紫光恒越保留在没有通知或提示的情况下对本资料的内容进行修改的权利。