UNIS T5000 系列 入侵检测系统

产品概述

UNIS T5000-G20

UNIS T5000 系列产品是业界领先的 IDS 产品，T5000 系列包括 T5000-G20 产品。

UNIS T5000 系列 IDS 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、实时地识别并与安全平台配合阻断或限制黑客、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 系列产品还具有强大、实用的带宽管理和 URL 过滤功能。

T5000-G20 是面向运营商及行业市场的高性能超万兆 IDS 产品，硬件上基于多核处理器架构，为 2U 的独立盒式 IDS 产品。提供 12 个千兆以太电口 + 12 个千兆以太光口 + 4 个万兆以太口，并提供一个扩展槽位用于进行端口及业务扩充。

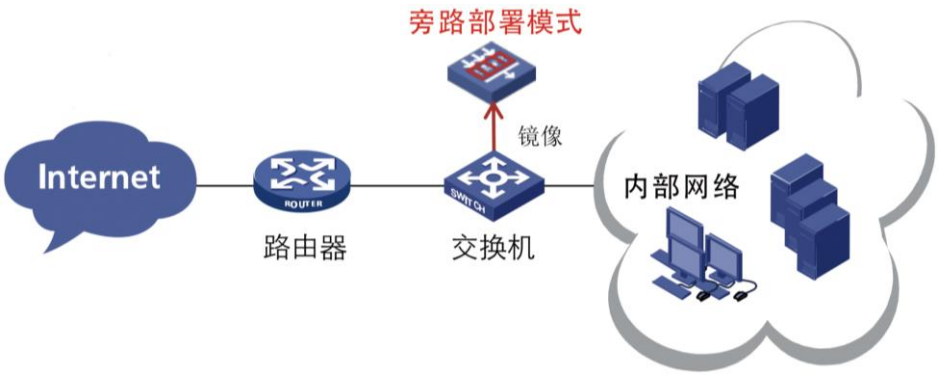
在安全功能方面，UNIS T5000 系列还一体化地集成了 IDS、带宽管理、防病毒、应用控制、URL 分类及自定义过滤等深度安全防御的功能，实现了基于用户、应用、时间、安全状态等多维度的策略控制功能。

在虚拟化和可靠性方面，支持多设备集群及 1:1 虚拟化，更好地适应云计算的要求，具备弹性扩展能力。

典型组网

IDS 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。



产品特点

高性能的软硬件处理平台

UNIS T5000 系列入侵检测系统采用了专用的 64 为多核高性能处理器和高速缓存器，UNIS T5000 系列可以提供千兆/万兆安全业务处理性能。

UNIS T5000 系列采用 CPU+Switch 架构，CPU 进行安全业务处理，Switch 实现多业务端口的扩展。

完善的安全保障

业界最完善的虚拟化解决方案。

支持 N:1，1:N，N:1:M 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最领先的入侵检测系统。通过深入到 7 层的分析与检测，与安全系统配合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。

通过了微软的 MAPP（Microsoft Active Protections Program）认证，可以提前获得微软的漏洞信息。

攻击特征库通过了国际权威组织 CVE（Common Vulnerabilities & Exposures，通用漏洞披露）的兼容性认证，在系统漏洞研究和攻击防御方面达到了业界顶尖水平。并关注国内特有的网络安全状况，及时对国内特有的攻击提供防御。

通过部署于全球的蜜罐系统，实时掌握最新的攻击技术和趋势，以定期（每周）和紧急（当重大安全漏洞被发现）两种方式发布，并自动或手动地分发到 IDS 设备中，使用户的 IDS 设备在漏洞被公布的同时立刻具备防御零时差攻击的能力。

◆ 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、限流、TCP 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。

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 Uniware V7 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

硬件规格

属性	T5000-G20
接口	1 个配置口（CON） 主机自带 8 个千兆光口+16 个千兆电口+2 个万兆电口
外型尺寸 （W×H×D）	440×443.1×88.1mm
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

属性	说明	
网络安全性	DPI	支持 IDS 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 bypass
	防范的网络攻击类型和网络滥用类型	蠕虫/病毒 木马 后门 文件病毒 DoS/DDoS 攻击 探测/扫描 间谍软件 网络钓鱼 网络病毒 利用漏洞的攻击 SQL 注入攻击
		缓冲区溢出攻击 协议异常 IDS 逃逸攻击 P2P 滥用 IM 滥用 网游滥用

	防火墙	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 状态防火墙 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
	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 静态ARP 动态ARP ARP代理 免费ARP DNS 本地静态域名

		DNS Client NTP NTP Client NTP Server
	IP路由	静态路由管理 策略路由 动态路由 RIP-1/RIP-2 OSPF 路由策略
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 链路质量探测NQA 支持BFD 热补丁 ISSU	
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

北京紫光恒越网络科技有限公司

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：010-62166890
传真：010-51652020-116
版本：

http://www.unishy.com

客户服务热线
400-910-9998