UNIS T1000-CN80-G-H1 入侵防御系统

产品概述

UNIS T1000-CN80-G-H1 入侵防御系统是紫光恒越技术有限公司（以下简称紫光恒越）伴随 Web2.0 时代的到来并结合当前安全与网络深入融合的技术趋势，针对大型企业园区网、运营商和数据中心市场推出核心芯片为国产芯片 CPU 的新下一代高性能万兆入侵防御产品。

UNIS T1000-CN80-G-H1 入侵防御系统支持多维一体化安全防护，可从用户、应用、时间、五元组等多个维度，对流量展开 IPS、AV、DLP 等一体化安全访问控制，能够有效的保证网络的安全；支持 RIP/OSPF/BGP/路由策略及基于应用与 URL 的策略路由；支持 IPv4/IPv6 双协议栈同时，可实现针对 IPv6 的状态防护和攻击防范。

UNIS T1000-CN80-G-H1 入侵防御系统采用互为冗余备份的 2 电源（1＋1 备份）模块，支持可插拔的交、直流输入电源模块，同时支持双机状态热备，充分满足高性能网络的可靠性要求；同时 UNIS T1000-CN80-G-H1 入侵防御系统在 1U 高的设备上提供 6GE（含一个管理口）+4 个千兆光口，支持两个接口接口卡，支持 8 千兆电口插卡/8 千兆光口插卡/4 万兆光口插卡扩展。

UNIS T1000-CN80-G-H1

产品特点

◆ **高性能的软硬件处理平台**

UNIS T1000-CN80-G-H1 入侵防御系统采用了先进的多核高性能国产处理器和高速存储器。

◆ **电信级设备高可靠性**

采用紫光恒越拥有自主知识产权的软、硬件平台。产品应用从电信运营商到中小企业用户，经历了多年的市场考验。支持 UNIS SCF 虚拟化技术，可将多台设备虚拟化为一台逻辑设备，完成业务备份同时提高系统整体性能。

◆ 强大的安全防护功能

- 支持丰富的攻击防范功能。包括：Land、Smurf、Fraggle、Ping of Death、Tear Drop、IP Spoofing、IP 分片报文、ARP 欺骗、ARP 主动反向查询、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描、端口扫描等攻击防范，还包括针对 SYN Flood、UPD Flood、ICMP Flood、DNS Flood 等常见 DDoS 攻击的检测防御。
- 支持 SOP 1:N 完全虚拟化。可在 UNIS T1000-CN80-G-H1 入侵防御系统模块上划分多个逻辑的虚拟入侵防御，基于容器化的虚拟化技术使得虚拟系统与实际物理系统特性一致，并且可以基于虚拟系统进行吞吐、并发、新建、策略等性能分配。
- 支持安全区域管理。可基于接口、VLAN 划分安全区域。
- 支持包过滤。通过在安全区域间使用标准或扩展访问控制规则，借助报文中 UDP 或 TCP 端口等信息实现对数据包的过滤。此外，还可以按照时间段进行过滤。
- 支持应用层状态包过滤（ASPF）功能。通过检查应用层协议信息（如 FTP、HTTP、SMTP、RTSP 及其它基于 TCP/UDP 协议的应用层协议），并监控基于连接的应用层协议状态，动态的决定数据包是被允许通过入侵防御或者是被丢弃。
- 支持验证、授权和计帐（AAA）服务。包括：基于 RADIUS/HWTACACS+、CHAP、PAP 等的认证。支持静态和动态黑名单。
- 支持静态路由、策略路由，以及 RIP、OSPF 等动态路由协议。
- 支持安全日志。
- 支持流量监控统计、管理。

◆ 灵活可扩展的一体化深度安全

- 与基础安全防护高度集成的一体化安全业务处理平台。
- 全面的应用层流量识别与管理：通过紫光恒越公司长期积累的状态机检测、流量交互检测技术，能精确检测 Thunder/Web Thunder（迅雷/Web 迅雷）、BitTorrent、eMule（电骡）/eDonkey（电驴）、QQ、MSN、PPLive 等 P2P/IM/网络游戏/炒股/网络视频/网络多媒体等应用；支持 P2P 流量控制功能，通过对流量采用深度检测的方法，即通过将网络报文与 P2P

协议报文特征进行匹配，可以精确的识别 P2P 流量，以达到对 P2P 流量进行管理的目的，同时可提供不同的控制策略，实现灵活的 P2P 流量控制。

- 高精度、高效率的入侵检测引擎。采用紫光恒越公司自主知识产权的 FIRST（Full Inspection with Rigorous State Test，基于精确状态的全面检测）引擎。FIRST 引擎集成了多项检测技术，实现了基于精确状态的全面检测，具有极高的入侵检测精度；同时，FIRST 引擎采用了并行检测技术，软、硬件可灵活适配，大大提高了入侵检测的效率。
- 实时的病毒防护，迅速、准确查杀网络流量中的病毒等恶意代码。
- 迅捷的 URL 分类过滤：提供基础的 URL 黑白名单过滤同时，可以配置 URL 分类过滤服务器在线查询。
- 全面、及时的安全特征库。通过多年经营与积累，紫光恒越公司拥有业界资深的攻击特征库团队，同时配备有专业的攻防实验室，紧跟网络安全领域的最新动态，从而保证特征库的及时准确更新。

◆ 业界领先的 IPv6

- 支持 IPv6 状态检测，真正意义上实现 IPv6 条件下的入侵防御功能，同时完成 IPv6 的攻击防范。

◆ 下一代多业务特性

- 集成链路负载均衡特性，通过链路状态检测、链路繁忙保护等技术，有效实现企业互联网出口的多链路自动均衡和自动切换。
- 一体化集成 SSL VPN 特性，满足移动办公、员工出差的安全访问需求，不仅可结合 USB-Key、短信进行移动用户的身份认证，还可与企业原有认证系统相结合、实现一体化的认证接入。
- DLP 基础功能支持，支持邮件过滤，提供 SMTP 邮件地址、标题、附件和内容过滤；支持网页过滤，提供 HTTP URL 和内容过滤；支持网络传输协议的文件过滤；支持应用层过滤，提供 Java/ActiveX Blocking 和 SQL 注入攻击防范。

◆ 专业的智能管理

- 支持智能安全策略：实现策略冗余检测、策略匹配优化建议、动态检测内网业务动态生成安全策略并推荐。
- 支持标准网管 SNMPv3，并且向下兼容 SNMP v1 和 v2。
- 提供图形化界面，简单易用的 Web 管理。
- 可通过命令行界面进行设备管理与入侵防御功能配置，满足专业管理和大批量配置需求。

- 通过安全管理中心实现统一管理，集安全信息与事件收集、分析、响应等功能为一体，解决了网络与安全设备相互孤立、网络安全状况不直观、安全事件响应慢、网络故障定位困难等问题，使 IT 及安全管理员脱离繁琐的管理工作，极大提高工作效率，能够集中精力关注核心业务。
- 基于先进的深度挖掘及分析技术，采用主动收集、被动接收等方式，为用户提供集中化的日志管理功能，并对不同类型格式（Syslog、二进制流日志等）的日志进行归一化处理。同时，采用高聚合压缩技术对海量事件进行存储，并可通过自动压缩、加密和保存日志文件到 DAS、NAS 或 SAN 等外部存储系统，避免重要安全事件的丢失。
- 提供丰富的报表，主要包括基于应用的报表、基于网流的分析报表等。
- 支持以 PDF 格式输出。
- 可通过 Web 界面进行报告定制，定制内容包括数据的时间范围、数据的来源设备、生成周期以及输出类型等。

◆ 安全服务链

支持基于 SDN 网络的部署模式，支持对数据流进行服务链 VXLAN 封装转发。

传统安全业务的部署，通常基于物理拓扑，将安全设备串行到业务流量路径当中，这种部署模式存在如下问题：

- 业务上线或业务变更需要调整整个路径下设备的策略，无法满足快速变更的需求。
- 设备能力扩展性较差，一旦出现性能不足，通常只能更换更高端的设备。设备的能力无法在多业务间共享。
- 传统基于路径的部署方式无法应用于 Overlay 网络。

新 IT 架构下，安全部署模式需要随之发生变化，基于 Overlay 网络构建集中的安全能力资源池。通过集中的控制器将需要进行安全防护的业务流量引流到安全能力中心进行防护，并且根据业务需求编排安全业务的防护顺序，也就是通常所说的服务链。由于实现了物理拓扑的解耦，所以能够很好地支持安全能力的弹性扩展及多业务能力共享。

产品规格

◆ 硬件规格

表 1-1 UNIS T1000-CN80-G-H1 硬件规格

项目	描述
接口	1个Console接口（RJ45） 2个外置USB 2.0接口 6个千兆以太电口(含一个管理口和1个HA接口) 4个千兆以太光口
扩展槽&扩展接口卡	2个扩展插槽 支持8电口bypass插卡、8千兆光口插卡、4万兆光口插卡
硬盘扩展插槽	2个硬盘扩展插槽，支持扩展2块SATA硬盘
内存配置	16G
Flash配置	8G
电源	外置2个电源扩展插槽，支持交流和直流，交流和直流不能混插
外型尺寸（W ×H ×D）	440mm×44mm×435mm
环境温度	工作：无硬盘0～45℃，带硬盘5～40℃ 非工作：-40～70℃
环境湿度	工作：10～80%，无冷凝 非工作：5～90%，无冷凝

◆ 软件规格

表 1-2 功能特性表

项目	描述
AAA服务	Portal认证、RADIUS认证、HWTACACS认证、PKI/CA（X.509格式）认证、域认证、CHAP验证、PAP验证
安全防护	虚拟IPS 安全区域划分 可以防御Land、Smurf、Fraggle、Ping of Death、Tear Drop、IP Spoofing、IP分片报文、ARP欺骗、ARP主动反向查询、TCP报文标志位不合法超大ICMP报文、地址扫描、端口扫描、SYN Flood、UPD Flood、ICMP Flood、DNS Flood等多种恶意攻击 基础和扩展的访问控制列表 基于时间段的访问控制列表 基于用户、应用的访问控制列表 动态包过滤

项目	描述
	ASPF应用层报文过滤 静态和动态黑名单功能 MAC和IP绑定功能 基于MAC的访问控制列表 支持802.1q VLAN透传
病毒防护	基于病毒特征进行检测 支持病毒库手动和自动升级 报文流处理模式 支持HTTP、FTP、SMTP、POP3协议 支持的病毒类型：Backdoor、Email-Worm、IM-Worm、P2P-Worm、Trojan、AdWare、Virus等 支持病毒日志和报表
深度入侵防御	支持对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件、DoS/DDoS等攻击的防御 支持缓冲区溢出、SQL注入、IDS/IPS逃逸等攻击的防御 支持攻击特征库的分类（根据攻击类型、目标机系统进行分类）、分级（分高、中、低、提示四级） 支持攻击特征库的手动和自动升级（TFTP和HTTP） 支持对BT等P2P/IM识别和控制
邮件/网页/应用层过滤	邮件过滤 SMTP 邮件地址过滤 邮件标题过滤 邮件内容过滤 邮件附件过滤 网页过滤 HTTP URL 过滤 HTTP 内容过滤 应用层过滤 Java Blocking ActiveX Blocking SQL 注入攻击防范
行为和内容审计	可基于用户对访问内容进行审计、溯源
数据防泄漏	对传输的文件和内容进行识别过滤，可准确识别常见文件的真实类型，如 Word、Excel、PPT、PDF、ZIP、RAR、EXE、DLL、AVI、MP4 等，并对敏感内容进行过滤
URL 过滤	支持对超过 50 种 URL 类别的预定义，支持 URL 规则黑白名单，并可以对访问 URL 的流量进行丢弃、重置、重定向、日志记录，列入黑名单等操作
应用识别与管控	可识别海量应用类型，访问控制精度到应用功能，例如：区分微信的登录、发送消息、接收消息，语音通话，图片等 应用识别与入侵检测、防病毒、内容过滤相结合，提高检测性能和准确率
路由特性	全面支持多种路由协议，如RIP、OSPF、BGP、IS-IS等
VXLAN	支持VXLAN服务链
IPv6	基于IPv6的状态及攻击防范 IPv6协议：IPv6转发、ICMPv6、PMTU、Ping6、DNS6、TraceRT6、Telnet6、DHCPv6 Client、DHCPv6 Relay等

项目	描述
	IPv6路由：RIPng、OSPFv3、BGP4+、静态路由、策略路由、PIM-SM、PIM-DM等 IPv6安全：NAT-PT、IPv6 Tunnel、IPv6 Packet Filter、Radius、IPv6域间策略、IPv6连接数限制等
高可靠性	支持SCF 2:1虚拟化 支持双机状态热备（Active/Active和Active/Backup两种工作模式） 支持双机配置同步 支持IPSec VPN的IKE状态同步 支持VRRP 支持外置BYPASS主机
易维护性	支持基于命令行的配置管理 支持Web方式进行远程配置管理 支持UNIS SecCenter安全管理中心进行设备管理 支持标准网管SNMPv3，并且兼容SNMP v1和v2 智能安全策略

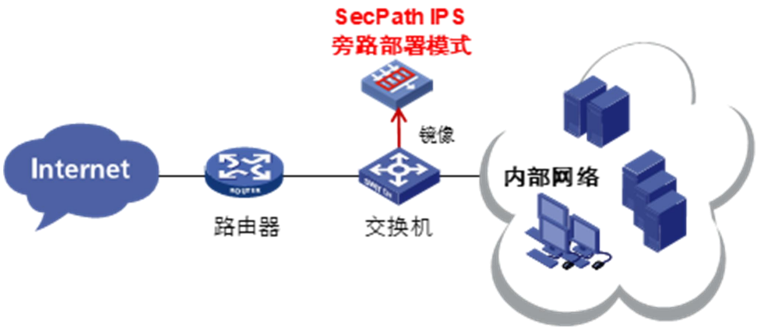
典型组网

◆ 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

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

◆ 主机选购一览表

主机	描述	备注
UNIS T1000-CN80-G-H1	UNIS T1000-CN80-G-H1主机	必配

◆ 电源模块选购一览表

电源模块	描述	备注
LSWM1PSRAC450A	450W交流电源（电源侧出风）	必配
LSWM1PSRDC450	450W直流电源（电源侧出风）	必配
LSWM1PSRAC450	450W交流电源（端口侧出风）	必配

注：电源至少配置 1 块，不支持混插。

◆ 接口卡选购一览表

接口卡	描述	备注
NS-NIM-TG4C-Z	4端口SFP+接口模块	选配
NS-NIM-GT8B-Z	8端口GE接口模块	选配
NS-NIM-GP8B-Z	8端口SFP接口模块	选配
NS-NIM-GT4GP4A	4端口GE电口(RJ45)+4端口千兆以太网光口(SFP,LC)接口模块	选配

◆ 硬盘选购一览表

硬盘	描述	备注
NS-SSD-480G-SATA	480GB 2.5inch SSD 硬盘模块	选配
NS-HDD-1TB-SATA	1TB 2.5inch SATA HDD 硬盘模块	选配

◆ License 选购一览表

项目	数量	备注
License 授权函-UNIS T1000 IPS 特征库升级服务-1 年-国内版	0-N	选配
License 授权函-UNIS T1000 IPS 特征库升级服务-3 年-国内版	0-N	选配

项目	数量	备注
License 授权函-UNIS T1000 AV 防病毒安全 License-1 年-国内版	0-N	选配
License 授权函-UNIS T1000 AV 防病毒安全 License-3 年-国内版	0-N	选配
License 授权函-UNIS T1000 应用识别特征库升级服务-1 年-国内版	0-N	选配
License 授权函-UNIS T1000 应用识别特征库升级服务-3 年-国内版	0-N	选配
License 授权函-UNIS T1000 WAF 特征库升级授权函-1 年-国内版;	0-N	选配
License 授权函-UNIS T1000 WAF 特征库升级授权函-3 年-国内版;	0-N	选配
License 授权函-UNIS T1000 安全威胁情报升级服务授权函-1 年-国内版	0-N	选配
License 授权函-UNIS T1000 安全威胁情报升级服务授权函-3 年-国内版	0-N	选配

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