UNIS F1000-12T12F-G2 防火墙

产品概述

UNIS F1000-12T12F-G2 防火墙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的核心芯片为国产芯片 CPU 的全新下一代高性能防火墙。

UNIS F1000-12T12F-G2 防火墙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、威胁情报等一体化安全访问控制，能够有效保证网络的安全；支持多种 VPN 业务，如 VXLAN、GRE VPN、IPSec VPN 和 SSL VPN 等，与智能终端对接实现移动办公；提供丰富的路由能力，支持 RIP/OSPF 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 F1000-12T12F-G2 防火墙采用互为冗余备份的双电源（1 + 1 备份）模块，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 F1000-12T12F-G2 防火墙在 1U 高的设备上提供 12 个千兆电口+12 个千兆光口，支持两个灵活扩展的接口卡槽位，支持 4*万兆光口插卡。

UNIS F1000-12T12F-G2

产品特点

◆ 高性能的软硬件处理平台

UNIS F1000-12T12F-G2 防火墙采用了先进的全新 64 位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，经历了多年的市场考验。支持双机 HA，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、UDP Flood、ICMP Flood、DNS Flood 等常见 DDoS 攻击的检测防御。
- 支持 VRF 逻辑虚拟化。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防火墙或者是被丢弃。
- 支持验证、授权和计帐（AAA）服务。包括：基于 RADIUSTACACS+、CHAP、PAP 等的认证。支持静态黑名单和动态黑名单。
- 支持 NAT 和 NAT 多实例。
- 支持 VPN 功能。包括：支持 VXLAN、IPSec/IKE、GRE、SSL 等，并实现与智能终端对接。
- 支持丰富的路由协议。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。采用基于精确状态的全面检测引擎，该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，该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。支持用户自定义 IPS 规则
- 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。
- 支持威胁情报联动，支持与漏扫、IPS 等安全产品进行联动处置。
- 支持 Web 防护。
- 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 状态防火墙，真正意义上实现 IPv6 条件下的防火墙功能，同时完成 IPv6 的攻击防范。
- 支持 IPv4/IPv6 双协议栈，并支持 IPv6 数据报文转发、静态路由等功能。
- 支持 IPv6 各种过渡技术，包括、手工隧道、6to4 隧道、、ISATAP 隧道、 NAT46、NAT64 等。
- 支持 IPv6 一体化安全策略等安全技术。

◆ 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 SQL 注入攻击防范。

◆ 专业的智能管理

- 支持标准网管 SNMPv3，并且兼容 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防火墙功能配置，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、基于用户、基于接口的分析报表等。
- 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、订阅项目等。

产品规格

◆ 硬件规格

表 1-1 UNIS F1000-12T12F-G2 硬件规格

属性	UNIS F1000-12T12F-G2
接口	12个GE电口+12个GE光口
接口扩展槽位	2个
硬盘扩展槽位	2个
扩展接口卡	支持 4个万兆光接口的扩展卡
电源	2个电源，支持1+1 AC冗余
外型尺寸（W×D×H）	442mm×495mm×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

◆ 软件规格

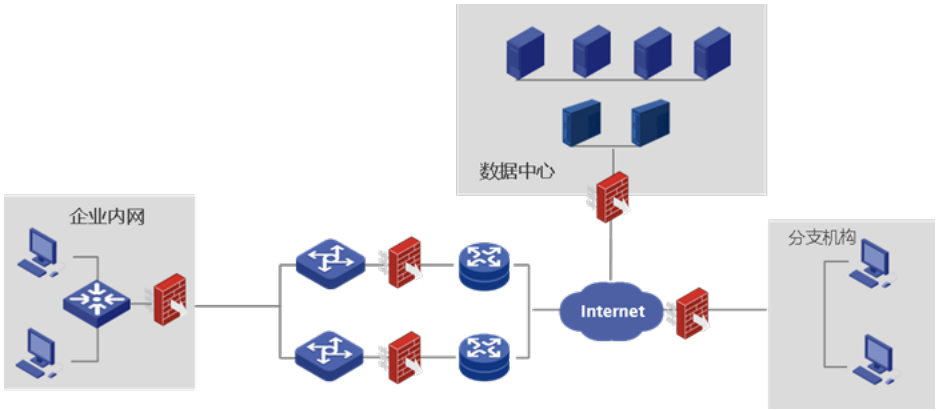
表 1-2 功能特性表

项目	描述
AAA服务	Portal认证、RADIUS认证、TACACS认证、域认证、CHAP验证、PAP验证
防火墙	虚拟防火墙 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、UDP 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 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 支持802.1q VLAN透传
负载均衡	支持链路及服务器负载均衡功能，支持基于应用、ISP等元素的智能选路，支持ICMP协议的健康监测，实现带宽繁忙、故障保护

项目	描述
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、IMAP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（紧急、高、中、低四级） 支持攻击特征库的手动升级（TFTP、FTP和HTTP）和自动升级 支持对BT等P2P/IM识别和控制
邮件/网页/应用层过滤	SMTP 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
行为和内容审计	可基于用户对访问内容进行审计、溯源
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 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
NAT	支持多个内部地址映射到同一个公网地址 支持多个内部地址映射到多个公网地址 支持内部地址到公网地址一一映射 支持源地址和目的地址同时转换 支持外部网络主机访问内部服务器 支持内部地址直映射到接口公网IP地址 支持DNS映射功能 可配置支持地址转换的有效时间 支持多种NAT ALG，包括TFTP、FTP、H.323、PPTP、SIP等
VPN	IPsec VPN、GRE VPN、SSL VPN
路由特性	全面支持多种路由协议，如RIP、OSPF等
VXLAN	支持VXLAN
IPv6	基于IPv6的状态防火墙及攻击防范 IPv6协议：IPv6转发、ICMPv6、Ping6、DNS6、TraceRT6、Telnet6、DHCPv6 Client、DHCPv6 Relay等

项目	描述
	IPv6路由：静态路由
高可靠性	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 支持标准网管SNMPv3，并且兼容SNMP v1和v2 支持智能安全策略

典型组网



在该典型组网中 UNIS F1000-12T12F-G2 防火墙可以实现：

- 高可靠网络设计
- 强大的处理能力
- 丰富的路由协议，实现安全与网络融合
- 强大的 VPN 加密处理能力
- 全面深度安全防御阻止恶意攻击，同时能够实现邮件、网页、文件过滤
- 丰富路由协议，实现安全与网络融合

订购信息

◆ **主机选购一览表**

主机	描述	备注
UNIS F1000-12T12F-G2	UNIS F1000-12T12F-G2主机	必配

◆ 接口卡选购一览表

接口卡	描述	备注
UNIS Sec-Card-4SFP Plus	4个万兆光接口的扩展插卡模块	选配

◆ 硬盘选购一览表

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

◆ License 选购一览表

项目	数量	备注
UNIS F1000-12T12F-G2 AV防病毒特征库升级服务	0-N	选配
UNIS F1000-12T12F-G2 IPS 防攻击特征库升级服务	0-N	选配
UNIS F1000-12T12F-G2 Web安全防护特征库升级服务	0-N	选配
UNIS F1000-12T12F-G2 ACG上网行为管理特征库（URL、恶意URL、APP）升级服务	0-N	选配
UNIS F1000-12T12F-G2 ALL (IPS防攻击特征库/AV病毒升级特征库/ACG上网行为管理特征库（URL、恶意URL、APP）升级服务)	0-N	选配
UNIS F1000-12T12F-G2 VPN客户端授权125个	0-N	选配
UNIS F1000-12T12F-G2 VPN客户端授权200个	0-N	选配
UNIS F1000-12T12F-G2 VPN客户端授权500个	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