

# UNIS F1000系列 防火墙

## ➤ 产品概述

UNIS F1000 系列防火墙是紫光恒越技术有限公司（以下简称紫光恒越）伴随数字化变革浪潮，结合当前安全与网络深度融合的技术趋势，针对多分支型企业机构，推出的安全网关产品，通过智能选路、广域网优化、安全策略、深度防御等功能，以更低的成本提供更快速、更可靠、更安全的广域网络接入。

UNIS F1000 系列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，对流量展开入侵防御和防病毒等一体化安全访问控制，能够有效的保证网络的安全；支持多种 VPN 业务，与智能终端对接实现移动办公；提供丰富的路由能力以适应各种复杂组网环境；支持 IPv4/IPv6 双协议栈，可实现针对 IPv6 的状态防护和攻击防范。UNIS F1000 系列防火墙包括：UNIS F1000-G5-G、UNIS F1000-G25-G、UNIS F1000-G35-G 三款产品。



UNIS F1000-G5-G



UNIS F1000-G25-G



UNIS F1000-G35-G

## 产品特点

### ◆ 高性能的软硬件处理平台

- 产品采用安全处理器+专用加速单元的架构。安全处理器负责处理安全业务，专用加速单元负责提升业务处理性能。。

### ◆ 电信级设备高可靠性

- 自研的硬件平台，保证设备长期稳定可靠运行。
- 软件模块化技术使软件的各个部分做到故障隔离。Uniware 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。软件的故障也可以自行恢复，不影响硬件的运行。
- 支持主备模式、双活模式，完成业务备份同时提高系统整体性能，双机主备模式切换时间 < 1s，双活模式支持网络层以及应用层会话保持，当主机故障时，双机切换不丢包。

### ◆ 强大的安全防护功能

- 支持支持应用管控、深度防御等能力实现从分支到总部，再到云端，全流程自动化的安全防护能力，保障链路安全、数据安全、业务安全，提高安全运维效率，降低安全运维成本。
- 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。
- 支持基于状态的策略管控。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。
- 支持多种协议的 ALG，动态进行数据通道的放行。

- 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 NAT。
- 支持 VPN 功能。包括：支持 L2TP、IPSec/IKE、GRE、SSL VPN 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。

#### ◆ 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：采用自研流引擎查毒技术，从而迅速、准确查杀网络流量中的病毒等恶意代码。
- 高效的 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。
- DLP 基础功能支持，支持网页过滤，提供 HTTP URL 过滤；支持应用层过滤，提供 Java/ActiveX Blocking 和 SQL 注入攻击防范。
- 全面、及时的安全特征库。通过多年经营与积累，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、动态路由及组播路由等功能。

- 支持 IPv6 ACL、Radius 等安全技术。

#### ◆ 移动办公特性

- 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。

#### ◆ 专业的智能管理

- 提供图形化界面，简单易用的 Web 管理。
- 支持标准网管 SNMPv3，并且兼容 SNMP v1 和 v2。
- 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。
- 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。

## 产品规格

### ◆ 硬件规格

表 1-1 硬件规格表

属性	UNIS F1000-G5-G	UNIS F1000-G25-G	UNIS F1000-G35-G
接口	1个Console接口 1个MGMT接口 2个USB 接口 2个千兆光口 2个bypass接口 8个千兆电口	1个Console接口 1个MGMT接口 2个USB 接口 8个千兆光口 16个千兆电口 4个万兆光口	1个Console接口 1个MGMT接口 2个USB接口 8个千兆光口 16个千兆电口 4个万兆光口
接口扩展插槽	/	1个接口扩展槽	1个接口扩展槽
存储扩展插槽	1个存储扩展插槽，支持扩展1块Micro SD卡	1个硬盘插槽，支持480G SSD\1T HDD硬盘扩展	1个硬盘插槽
电源	内置电源	双电源	内置100W双交流电源
外型尺寸 (W × D × H)	330mm×230mm×44mm	440mm x 460mm x 44mm	440mm x 460mm x 44mm
环境温度	工作：无硬盘0~45℃，带硬盘5~40℃ 非工作：-40~70℃	工作：无硬盘0~45℃，带硬盘5~40℃ 非工作：-40~70℃	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	工作：10~80%，无冷凝 非工作：5~90%，无冷凝	工作：10~80%，无冷凝 非工作：5~90%，无冷凝

### ◆ 软件规格

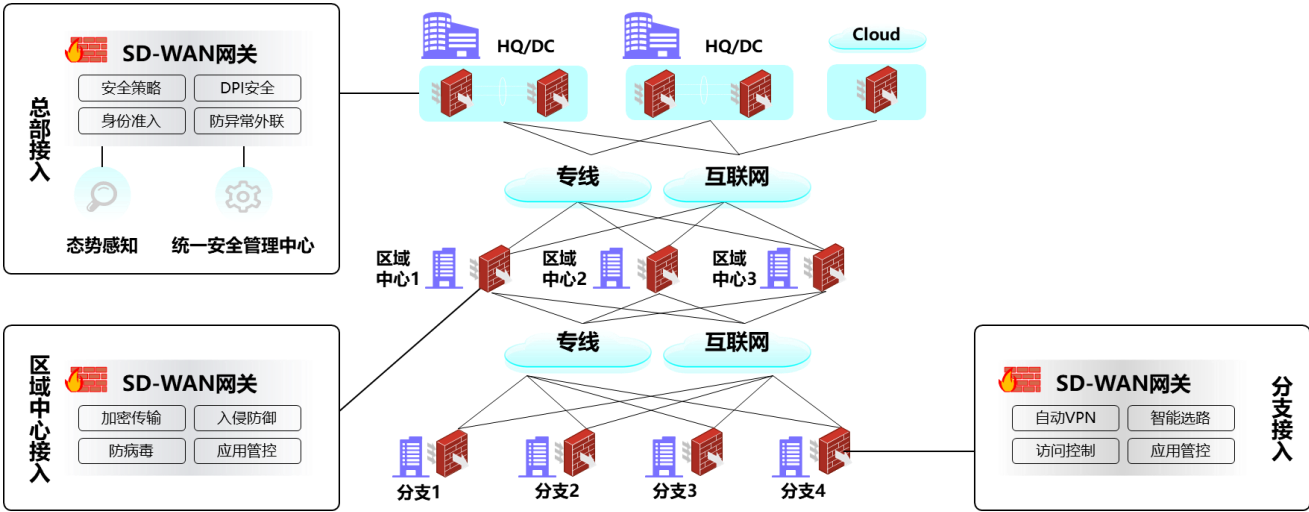
表 1-2 功能特性表

项目	描述
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、UPD Flood、ICMP Flood、DNS Flood 等多种恶意攻击 支持访问控制，能够基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、域名、服务、应用、时间、VLAN 等多种方式进行访问控制 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

项目	描述
	基于状态的策略管控 支持多种协议的 ALG 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
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
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
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。
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
VPN	L2TP VPN、IPsec VPN、GRE VPN、SSL VPN
路由特性	全面支持多种路由协议，如RIP、OSPF、BGP、IS-IS等；
IPv6	基于IPv6的状态防火墙及攻击防范

项目	描述
	<p>IPv6协议：IPv6转发、ICMPv6、PMTU、Ping6、DNS6、TraceRT6、Telnet6、DHCPv6 Client、DHCPv6 Relay等</p> <p>IPv6路由：RIPng、OSPFv3、BGP4+、静态路由、策略路由、PIM-SM、PIM-DM等</p>
易维护性	<p>支持基于命令行的配置管理</p> <p>支持Web方式进行远程配置管理</p> <p>支持安全管理平台（SMP）进行设备管理</p> <p>支持标准网管 SNMPv3，并且兼容SNMP v1和v2</p>

# 典型组网



# 订购信息

## 主机选购一览表

主机	描述	备注
F1000-G5-G	F1000-G5-G主机	必配
F1000-G25-G	F1000-G25-G主机	必配
F1000-G35-G	F1000-G35-G主机	必配

◆ 存储选购一览表

硬盘	描述	备注
NS-SSD-480G-SATA-SFF-Z	480G SSD硬盘	F1000-G[5][25][35]-G

◆ License 选购一览表

项目	数量	备注
License授权函-防火墙 IPS 特征库升级授权函	0-N	选配
License授权函-防火墙 AV 防病毒安全特征库升级授权函	0-N	选配
License授权函-防火墙URL特征库升级授权函	0-N	选配
License授权函-防火墙应用识别特征库升级授权函	0-N	选配
License授权函-防火墙安全威胁情报升级授权函	0-N	选配
License授权函-防火墙 TI/ACG/IPS/AV/URL组合特征库升级授权函	0-N	选配

unis

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](http://www.unisyue.com)

客户服务热线  
400-910-9998

Copyright © 2023 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。