# UNIS F1000-CN60/80 防火墙

## 产品概述

UNIS F1000-CN60/80 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新下一代高性能万兆防火墙产品。

UNIS F1000-CN60/80 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，提供丰富的路由能力，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 F1000-CN60/80 防火墙采用互为冗余备份的双电源（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。

UNIS F1000-CN60

UNIS F1000-CN80

## 产品特点

### ◆ 高性能的软硬件处理平台

UNIS F1000-CN60/80 采用了先进的 64 位多核高性能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 F1000-CN60/80 模块上划分多个逻辑的虚拟防火墙，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 RADIUS/HWTACACS+、CHAP、PAP 等的认证。
- 支持静态和动态黑名单。
- 支持 NAT 和 NAT 多实例。
- 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 UNIS 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。

### ◆ 全面便捷的扩展功能

- 可以通过功能授权的方式增加网络审计、病毒防护、入侵防御/检测、Web 应用防护、URL 过滤等功能。
- 基于自研软件的先进架构可根据市场发展趋势，在不更改产品硬件架构和形态的基础上，通过功能授权的方式拓展相关安全特性。

### ◆ 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 各种过渡技术，包括 NAT-PT、IPv6 Over IPv4 GRE 隧道、手工隧道、6to4 隧道、IPv4 兼容 IPv6 自动隧道、ISATAP 隧道、NAT444、DS-Lite 等。
- 支持 IPv6 ACL、Radius 等安全技术。

### ◆ 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 UNIS IMC SSM 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、HTML、WORD 和 TXT 等多种格式输出。
- 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。

## ◆ 产品规格

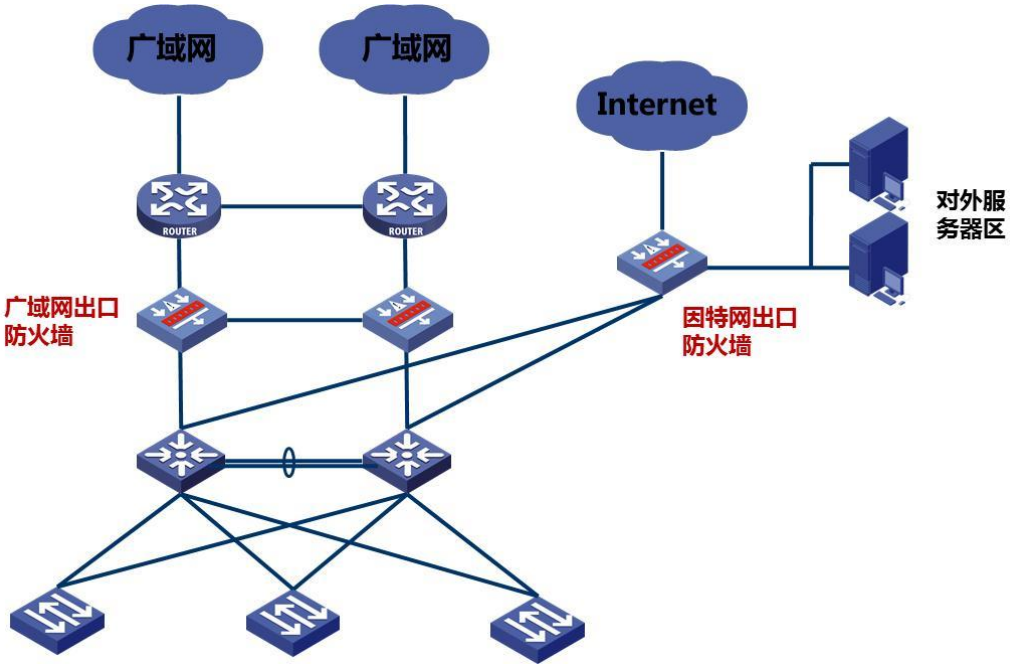
| 项目 | F1000-CN60 | F1000-CN80 |
| --- | --- | --- |
| 接口 | 1个Console接口（RJ45或者MicroUSB）<br>1个RJ45管理口<br>2个外置USB 2.0接口<br>15个千兆以太电口<br>8个千兆以太光口 | 1个Console接口（RJ45或者MicroUSB）<br>1个RJ45管理口<br>2个外置USB 2.0接口<br>15个千兆以太电口<br>8个千兆以太光口<br>2个万兆以太光口 |
| 扩展槽位 | 2个（支持PFC模块、4端口千兆光子卡、6端口万兆光子卡） | |
| 硬盘扩展槽位 | 2个硬盘扩展插槽，支持扩展2块SATA硬盘 | |
| 外形尺寸 | 440mm×44mm×435mm | |
| 电源 | 2个冗余电源槽位，支持热插拔，220V±10%，50Hz±2Hz | |
| 环境温度 | 工作：无硬盘0～45℃，带硬盘5～40℃<br>非工作：-40～70℃ | |
| 环境湿度 | 工作：10～95%，无冷凝<br>非工作：5～95%，无冷凝 | |
| 运行模式 | 路由模式、透明模式、混杂模式 | |
| AAA服务 | Portal认证、RADIUS认证、HWTACACS认证、PKI /CA（X.509格式）认证、<br>域认证、CHAP验证、PAP验证 | |
| 防火墙 | 虚拟防火墙<br>安全区域划分<br>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<br>基础和扩展的访问控制列表<br>基于时间段的访问控制列表<br>基于用户、用用的访问控制列表<br>动态包过滤<br>ASPF应用层报文过滤<br>静态和动态黑名单功能<br>MAC和IP绑定功能<br>基于MAC的访问控制列表<br>支持802.1q VLAN 透传 | |
| 邮件/网页/应用层过滤 | 邮件过滤<br>SMTP 邮件地址过滤<br>邮件标题过滤<br>邮件内容过滤<br>邮件附件过滤<br>网页过滤<br>HTTP URL 过滤<br>HTTP 内容过滤<br>应用层过滤 | |

| 项目 | F1000-CN60 | F1000-CN80 |
| --- | --- | --- |
| | Java Blocking<br>ActiveX Blocking<br>SQL 注入攻击防范 | |
| NAT | 支持多个内部地址映射到同一个公网地址<br>支持多个内部地址映射到多个公网地址<br>支持内部地址到公网地址一一映射<br>支持源地址和目的地址同时转换<br>支持外部网络主机访问内部服务器<br>支持内部地址直映射到接口公网IP地址<br>支持DNS映射功能<br>可配置支持地址转换的有效时间<br>支持多种NAT ALG，包括DNS、FTP、H.323、ILS、MSN、NBT、PPTP、SIP等 | |
| IPv6 | 基于IPv6的状态防火墙及攻击防范<br>IPv6协议：IPv6转发、ICMPv6、PMTU、Ping6、DNS6、TraceRT6、Telnet6、DHCPv6 Client、DHCPv6 Relay等<br>IPv6路由：RIPng、OSPFv3、BGP4+、静态路由、策略路由、PIM-SM、PIM-DM等<br>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<br>支持双机状态热备（Active/Active和Active/Backup两种工作模式）<br>支持双机配置同步<br>支持IPSec VPN的IKE状态同步<br>支持VRRP | |
| 易维护性 | 支持基于命令行的配置管理<br>支持Web方式进行远程配置管理<br>支持UNIS SecCenter安全管理中心进行设备管理<br>支持标准网管 SNMPv3，并且兼容SNMP v1和v2<br>智能安全策略 | |
| 环保与认证 | 支持欧洲严格的RoHS环保认证 | |

## 典型组网防火墙应用

F1000-CN 系列防火墙部署在广域网出口及 Internet 出口提供对外访问的安全控制及 NAT，同时通过防火墙的攻击防范及深度安全防御功能保护 DMZ 区的服务器。

◆ **出口安全防护**




◆ **VPN 应用**

F1000-CN 系列集成了丰富的 VPN 功能，包括 IPSec VPN、SSL VPN、 L2TP VPN 等，可以作为中小型企业的出口网关设备提供移动用户的 SSL VPN 接入，也可以作为广域网组网的分支或二三级中心设备提供 site-to-site 的 IPSec VPN 接入。IPSEC 业务和 SSLVPN 业务支持采用国密算法。

图1-1 VPN 应用组网图-远程接入

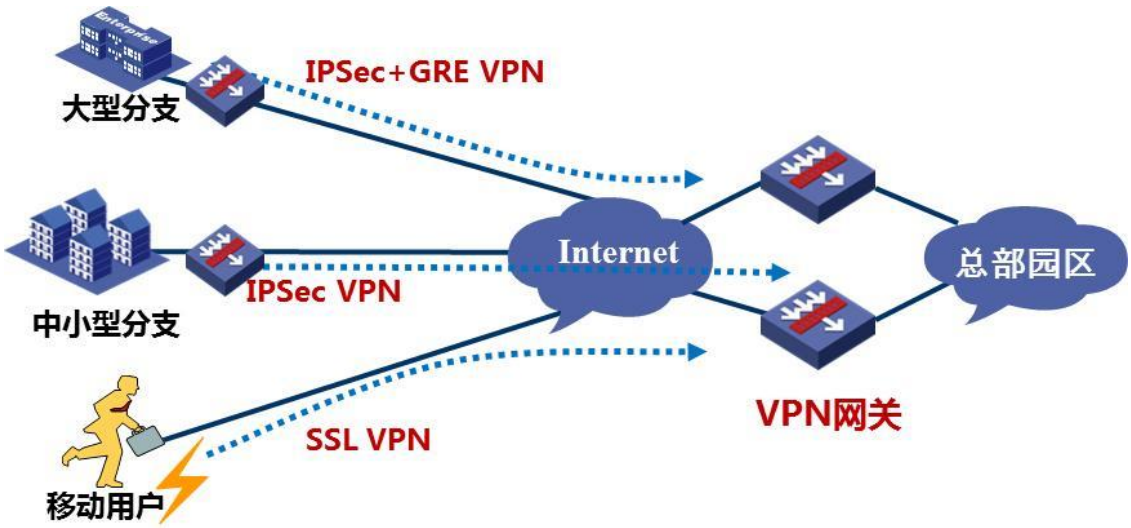
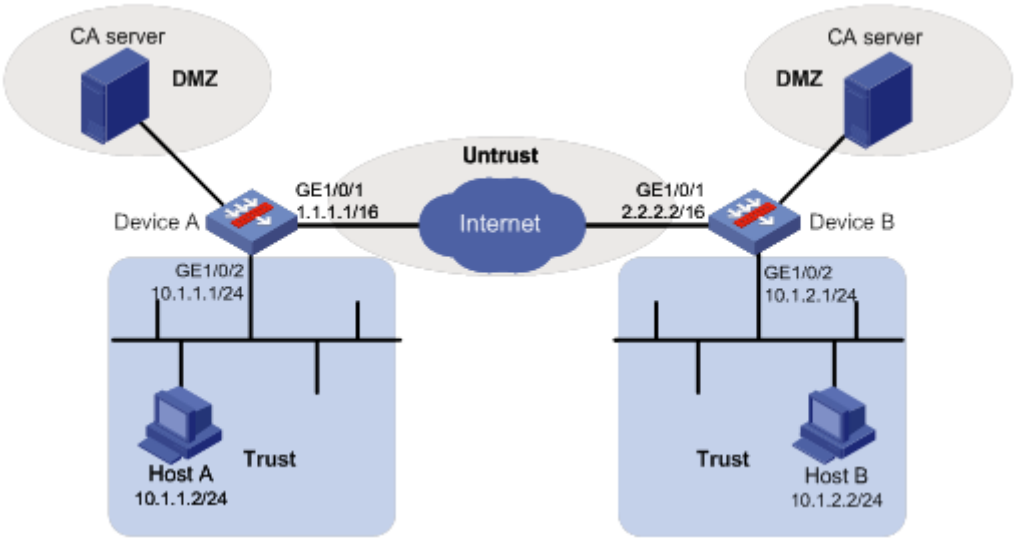


图1-2 VPN 应用组网图-Site-to-Site IPSec VPN




## 订购信息

◆ **主机选购一览表**

| 模块 | 数量 | 备注 |
|---|---|---|
| F1000-CN60 | 1 | 必配 |
| F1000-CN80 | 1 | 必配 |
| 480GB SATA SSD硬盘模块 | 2 | 选配 |
| PFC模块 | 1 | 选配 |
| 4SFP接口卡 | 1 | 选配 |
| 6SFP+接口卡 | 1 | 选配 |

◆ **电源模块选购一览表**

| 电源模块 | 备注 |
|---|---|
| 交流电源模块 | 选配 |
| 直流电源模块 | 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**