

H3C SecBlade FW Enhanced 防火墙业务模块

产品概述

H3C SecBlade FW Enhanced 是杭州华三通信技术有限公司（以下简称 H3C 公司）结合当前安全与网络深度融合的技术趋势，为满足超万兆时代的以太网带宽需求而推出的新一代 SecBlade 防火墙模块。

H3C SecBlade FW Enhanced 是业内第一款基于 40G 硬件平台的超万兆防火墙模块，目前可应用于 H3C S10500/S12500/S12500-X/S12500-F 系列交换机。通过 SecBlade FW Enhanced 防火墙模块，用户可灵活、迅速的在 S10500/S12500/S12500-X/S12500-F 系列以太网交换机当中整合防火墙、VPN 等安全功能，实现网络和安全防护的高度一体化。

H3C SecBlade FW Enhanced 能提供外部攻击防范、内网安全、流量监控、URL 过滤、应用层过滤等功能，有效的保证网络的安全。采用 H3C ASPF（Application Specific Packet Filter，基于应用层状态的包过滤）技术，实时检测应用层连接状态，实现 2-7 层安全防护。提供邮件告警、攻击日志、流日志和网络管理监控等功能，协助用户进行网络管理。

H3C SecBlade FW Enhanced 模块与基础网络设备融合，具有即插即用、扩展性强的特点，降低了用户管理难度，减少了维护成本。



H3C SecBlade FW Enhanced 防火墙业务模块

产品特点

高性能的软硬件处理平台

- SecBlade FW Enhanced 模块采用了专用的 64 位多核高性能处理器和高速存储器，单板性能最高可达 40Gbps。
- 独立业务处理资源，在高速处理安全业务的同时，以太网交换机的原有业务处理不会受到任何影响。
- 采用专业硬件 TCAM，保证大容量策略表项的高速检索。
- SecBlade FW Enhanced 模块基于 H3C 公司领先的 OAA（Open Application Architecture，开放应用架构）开发，通过内部多个高速 10G 以太接口与路由交换主体相连，保证了与业务插卡间通畅的数据转发。

电信级设备高可靠性

- 采用 H3C 公司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。
- 支持双机状态热备功能，支持 Active/Active 和 Active/Passive 两种工作模式，实现负载分担和业务备份。
- 支持跨设备的双机热备。

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。
- 支持虚拟防火墙。可在 SecBlade FW Enhanced 模块上划分多个逻辑的虚拟防火墙，每个虚拟防火墙有自己的安全策略，并且可以分别进行管理。
- 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 VPN 功能。包括：支持 L2TP、IPSec/IKE、GRE 等。
- 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。

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
- 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 H3C SecCenter 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

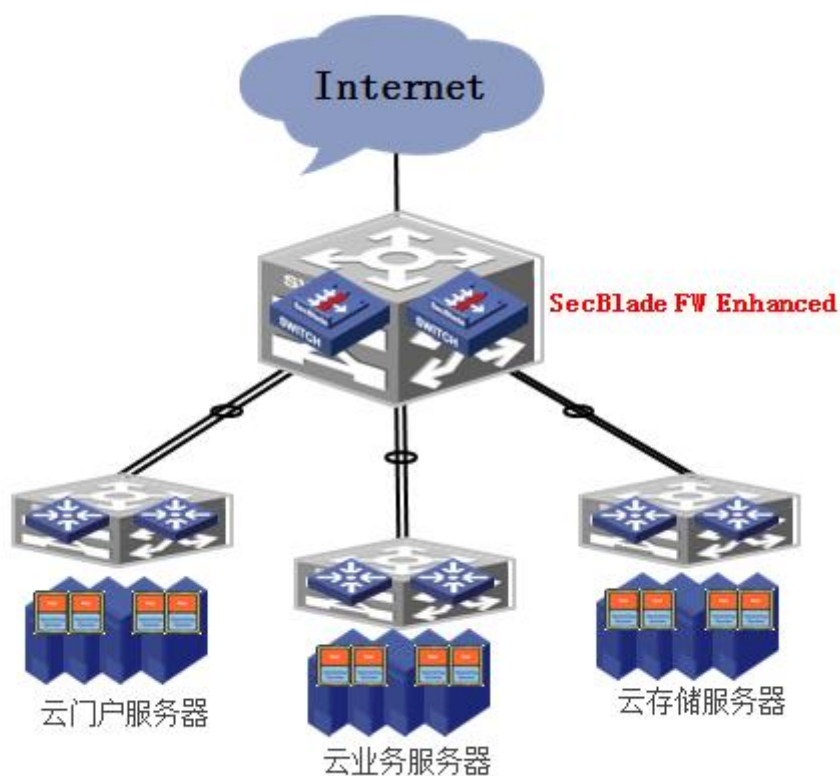
项目	描述		
应用于	S10500	S12500-X/S12500-F	S12500
尺寸(H × W × D)	40.1×399.2×376.8mm	40.1×399.2×498.8mm	40.1×399.2×376.8mm
重量	3.9kg	4.8kg	3.9kg
功耗范围	109~157W	128~168W	109~157W
SDRAM 配置	标配 4GB		
CF 卡	标配 256MB		
Flash 配置	4MB, 16bit 数据宽度		
接口	1 个配置口 (CON) 2 个千兆光电 Combo		
环境温度	工作: 0~45℃ 非工作: -40~70℃		
热插拔	支持		
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、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、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 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 基于 MAC 的访问控制列表 支持 802.1q VLAN 透传		
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		

项目	描述
	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 DNS、FTP、H.323、ILS、MSN、NBT、PPTP、SIP 等
VPN	L2TP VPN、IPSec VPN、GRE VPN
IPv6	基于 IPv6 的状态防火墙 IPv6 协议：IPv6 转发、ICMPv6、PMTU、Ping6、DNS6、TracerT6、Telnet6、DHCPv6 Client、DHCPv6 Relay 等 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
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 H3C 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
环保与认证	支持欧洲严格的 RoHS 环保认证

典型组网

云计算数据中心典型应用

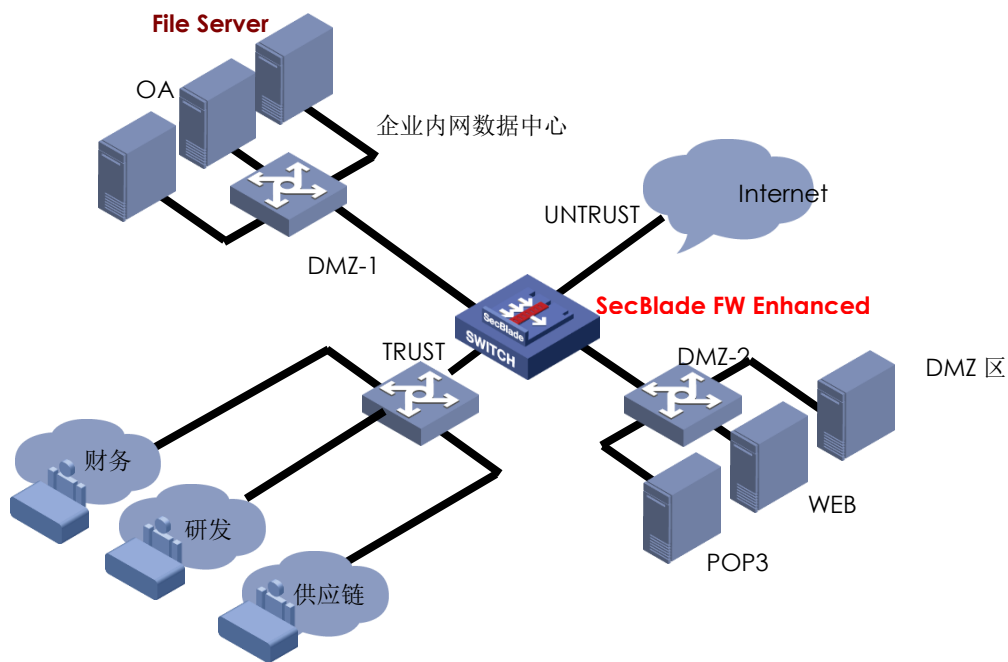
H3C SecBlade FW Enhanced 模块不仅能够提供高性能的防火墙，同时支持虚拟防火墙功能，一块 H3C SecBlade FW Enhanced 模块可虚拟成多台逻辑上的防火墙，每个虚拟防火墙有自己的策略且可进行独立管理，充分满足云计算数据中心的租户需求。



H3C SecBlade FW Enhanced 云计算数据中心组网应用示意图

园区网典型应用

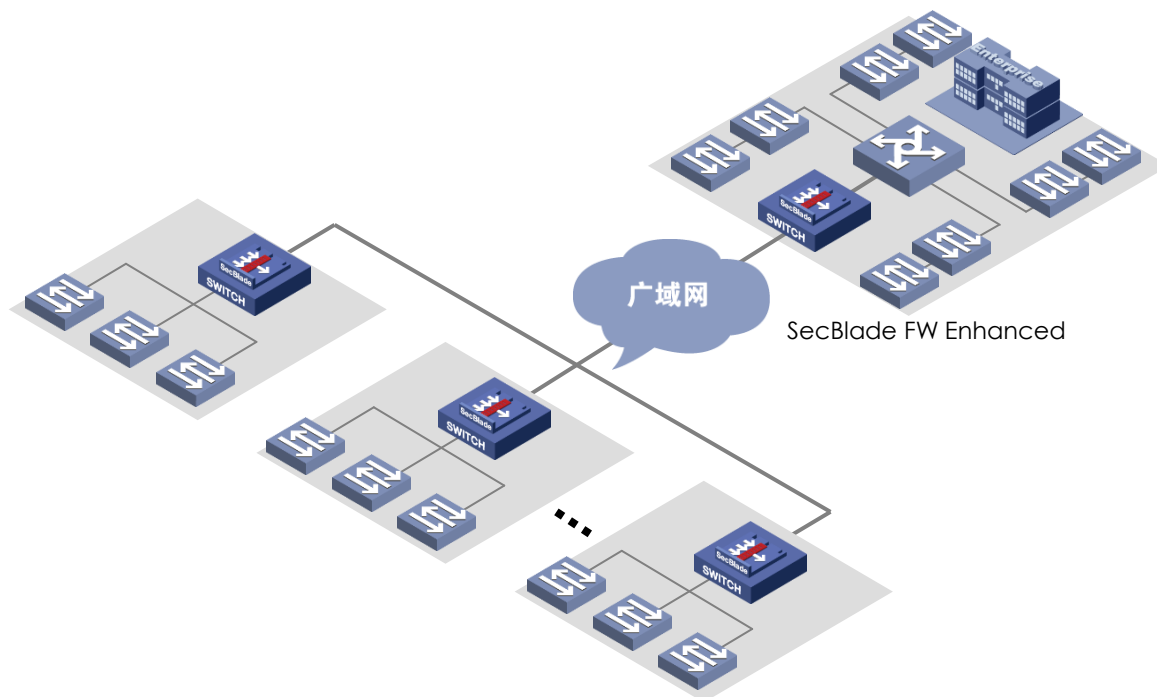
H3C SecBlade FW Enhanced 模块部署于网络核心/汇聚交换机上，对各网络区域进行高效的安全隔离与控制，实现网络和安全的一体化融合。H3C SecBlade FW Enhanced 模块可结合 S10500/S12500/S12500-X/S12500-F 系列交换机设备作为边界防护设备，防范各种外部攻击；也可作为内网访问控制设备，用以隔离不同安全等级的区域。



H3C SecBlade FW Enhanced 典型园区网应用示意图

分支机构远程接入应用

H3C SecBlade FW Enhanced 模块提供强大的 VPN 功能，帮助企业分支用户安全的访问公司总部资源，也可以满足分支机构访问公司本部资源的需求。



H3C SecBlade FW Enhanced VPN 组网应用示意图

订购信息

型号	描述	备注
LSU1FWCEA0	H3C S10500 防火墙增强业务模块	必配
LST1FW3A1	H3C S12500 防火墙增强业务模块	必配
LSTM1FW3B1	H3C S12500-X/S12500-F 防火墙增强业务模块	必配



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。