

H3C SecBlade NGFW 防火墙业务模块

产品概述

H3C SecBlade NGFW 是新华三技术有限公司（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 多业务防火墙模块。随着网络应用的不断深化，网络安全变得越来越重要。将网络安全融入到网络应用和网络设备中，是目前和未来网络发展的必然趋势。

H3C SecBlade NGFW 是一款超万兆高性能防火墙模块，可应用于 H3C S5130HI/S5560EI/S5560X-EI/S5560HI/S5800EI/S6800/S6900/S7500E-XS/S7500E/S7500E-X/S7600 /S7600-X/S10500/S12500-S/S12500-X/S12500X-AF/S12500F-AF 交换机以及 SR88-X/SR88-X-S/CR16K-F 路由器，为用户提供融合多业务的一体化网络安全解决方案。

H3C SecBlade NGFW 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；支持多种 VPN 业务，如 L2TP VPN、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/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。

H3C SecBlade NGFW 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。



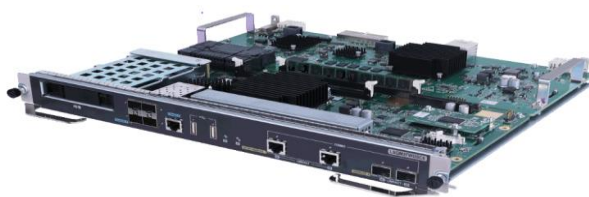
H3C S51/55 系列交换机 SecBlade NGFW 防火墙业务模块



H3C S68/S69 系列交换机 SecBlade NGFW 防火墙业务模块



H3C S75/S105 系列交换机 SecBlade NGFW 3代防火墙业务模块



H3C S75/S105 系列交换机 SecBlade NGFW Lite 代防火墙业务模块



H3C S75/S105 系列交换机 SecBlade NGFW 4 代防火墙业务模块



H3C S125X-AF SecBlade NGFW 4 代防火墙业务模块



H3C SR88-X SecBlade NGFW 4 代防火墙业务模块

产品特点

高性能的软硬件处理平台

- SecBlade NGFW 模块采用了专用的 64 位多核高性能处理器和高速存储器。
- 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。
- SecBlade FW NGFW 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。
- 最新支持 SOP 1:N 完全虚拟化。可在 H3C SecBlade NGFW 设备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。
- 支持基于应用、用户的访问控制，将应用与用户作为安全策略的基本元素，并结合深度防御实现下一代的访问控制功能。
- 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、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 DPI 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 H3C 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 H3C 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 Kaspersky 公司的流引擎查毒技术，从而迅速、准确查杀网络流量中的病毒等恶意代码。
- 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，H3C 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 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。

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 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

属性	H3C SecBlade NGFW
应用于	S5130HI/S5560EI/S5560X-EI/S5560HI/S5800EI/S6800/S6900/S7500E-XS/S7500E/S7500E-X/S7600 /S7600-X/S10500/S12500-S/S12500-X/S12500X-AF/S12500F-AF交换机以及SR88-X/SR88-X-S/CR16K-F路由器
功耗范围	109~157W
SDRAM配置	至少8G
CF卡	标配4G
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	<p>SOP虚拟防火墙技术，支持CPU、内存、存储等硬件资源划分的完全虚拟化安全区域划分</p> <p>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</p> <p>基础和扩展的访问控制列表</p> <p>基于时间段的访问控制列表</p> <p>基于用户、应用的访问控制列表</p> <p>ASPF应用层报文过滤</p> <p>静态和动态黑名单功能</p> <p>MAC和IP绑定功能</p> <p>基于MAC的访问控制列表</p> <p>支持802.1q VLAN 透传</p>
病毒防护	<p>基于病毒特征进行检测</p> <p>支持病毒库手动和自动升级</p> <p>报文流处理模式</p> <p>支持 HTTP、FTP、SMTP、POP3 协议</p> <p>支持的病毒类型：Backdoor、Email-Worm、IM-Worm、P2P-Worm、Trojan、AdWare、Virus 等</p> <p>支持病毒日志和报表</p>

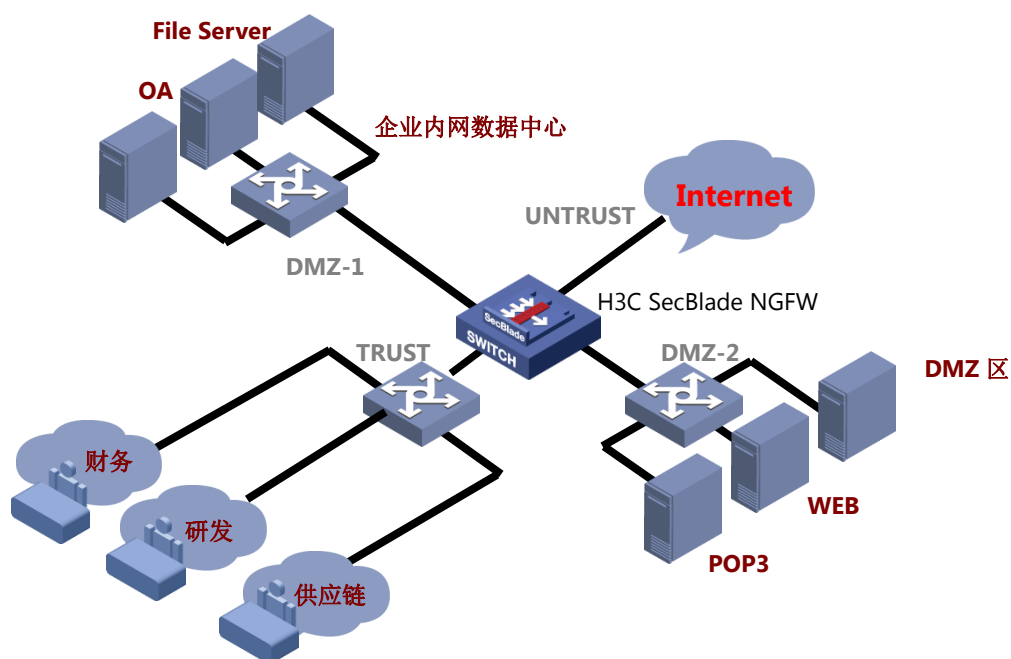
属性	H3C SecBlade NGFW
深度入侵防御	<p>支持对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件、DoS/DDoS 等常见的攻击防御</p> <p>支持缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御</p> <p>支持攻击特征库的分类（根据攻击类型、目标机系统进行分类）、分级（分高、中、低、提示四级）</p> <p>支持攻击特征库的手动和自动升级（TFTP 和 HTTP）</p> <p>支持对 BT 等 P2P/IM 识别和控制</p>
邮件/网页/应用层过滤	<p>邮件过滤</p> <p>SMTP 邮件地址过滤</p> <p>邮件标题过滤</p> <p>邮件内容过滤</p> <p>邮件附件过滤</p> <p>网页过滤</p> <p>HTTP URL 过滤</p> <p>HTTP 内容过滤</p> <p>应用层过滤</p> <p>Java Blocking</p> <p>ActiveX Blocking</p> <p>SQL 注入攻击防范</p>
NAT	<p>支持多个内部地址映射到同一个公网地址</p> <p>支持多个内部地址映射到多个公网地址</p> <p>支持内部地址到公网地址一一映射</p> <p>支持源地址和目的地址同时转换</p> <p>支持外部网络主机访问内部服务器</p> <p>支持内部地址直接映射到接口公网IP地址</p> <p>支持DNS映射功能</p> <p>可配置支持地址转换的有效时间</p> <p>支持多种NAT ALG，包括DNS、FTP、H.323、ILS、MSN、NBT、PPTP、SIP等</p>
VPN	L2TP VPN、IPSec VPN、GRE VPN、SSL VPN
IPv6	<p>基于IPv6的状态防火墙及攻击防范</p> <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> <p>IPv6安全：NAT-PT、IPv6 Tunnel、IPv6 Packet Filter、Radius、IPv6域间策略、IPv6连接数限制等</p>

属性	H3C SecBlade NGFW
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
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 SSM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
环保与认证	支持欧洲严格的RoHS环保认证

典型组网

园区网典型应用

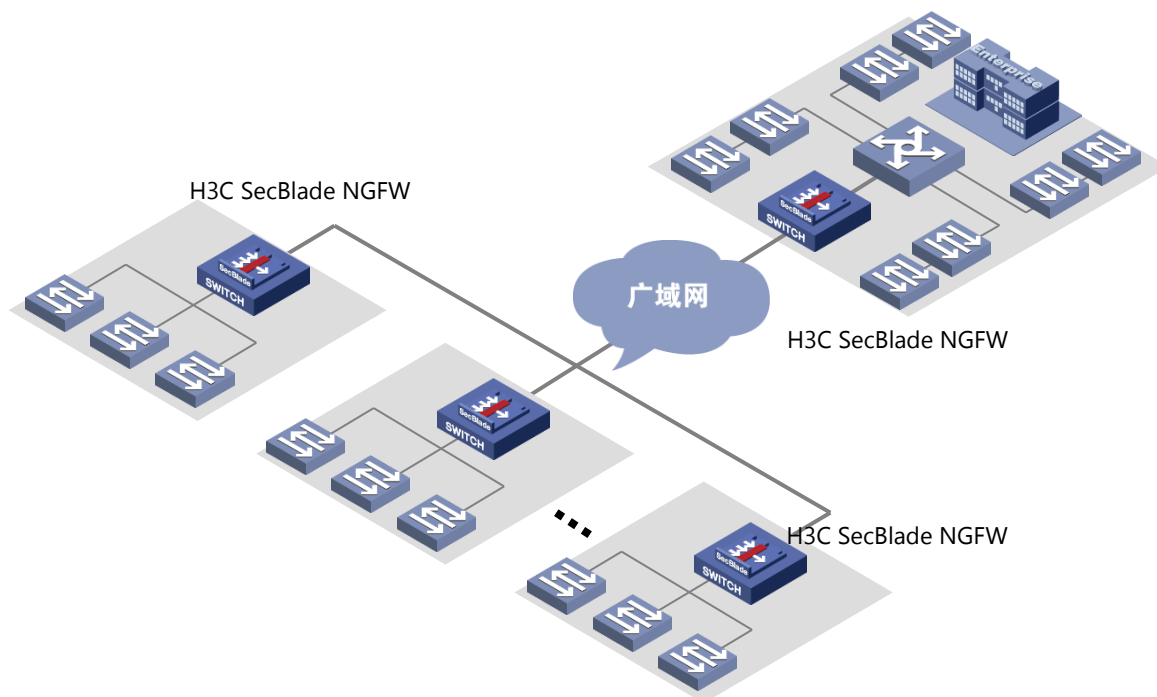
H3C SecBlade NGFW 模块部署于网络核心/汇聚交换机上，对各网络区域进行高效的安全隔离与控制，实现网络和安全的一体化融合。H3C SecBlade NGFW 模块可结合 S75E/S10500 系列交换机设备作为边界防护设备，防范各种外部攻击；也可作为内网访问控制设备，用以隔离不同安全等级的区域。



H3C SecBlade NGFW 典型园区网应用示意图

分支机构远程接入应用

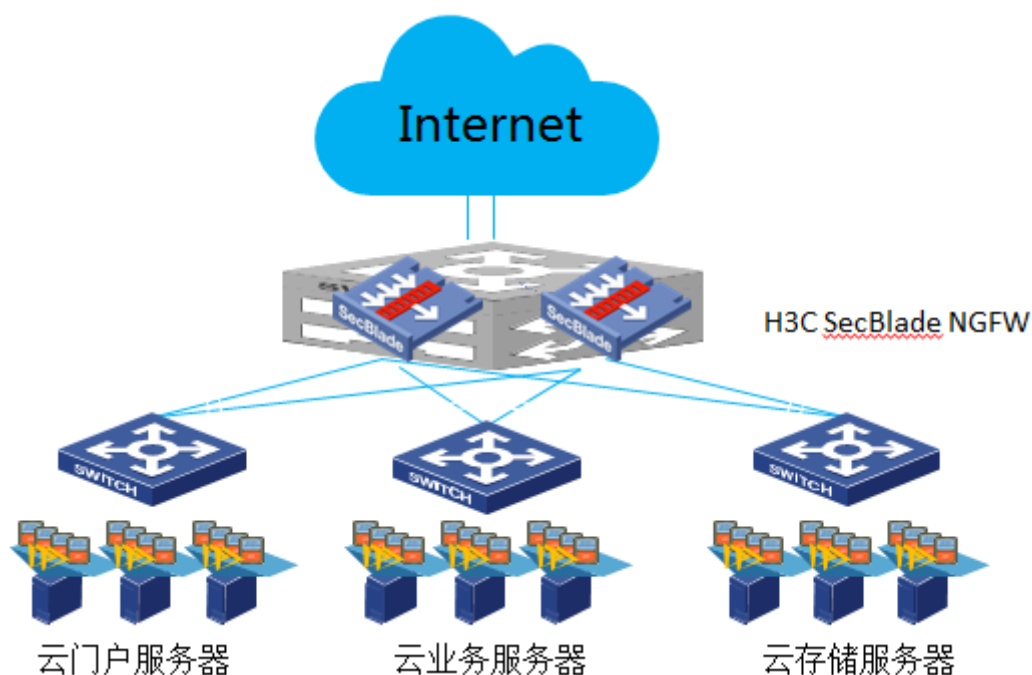
H3C SecBlade NGFW 模块提供强大的 VPN 功能，帮助企业分支用户安全的访问公司总部资源，也可以满足分支机构访问公司本部资源的需求。



H3C SecBlade NGFW VPN 组网应用示意图

云计算数据中心典型应用

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

订购信息

描述	数量范围	备注
功能模块-H3C NGFW 防火墙增强模块-国内版	1	必配
License 授权函-H3C IPS 特征库升级服务-1年-国内版	1	选配
License 授权函-H3C IPS 特征库升级服务-3年-国内版	1	选配
License 授权函-H3C IPS 防病毒安全-1年-国内版	1	选配
License 授权函-H3C IPS 防病毒安全-3年-国内版	1	选配
License 授权函-H3C 应用识别特征库升级服务-1年-国内版	1	选配
License 授权函-H3C 应用识别特征库升级服务-3年-国内版	1	选配
License 授权函-H3C LB 授权函-国内版	1	选配
License 授权函-H3C 流量分析增强模块-国内版	1	选配
License 授权函-H3C SSL VPN 200 个用户-国内版	1	选配
License 授权函-H3C SSL VPN 500 个用户-国内版	1	选配
License 授权函-H3C SSL VPN 1000 个用户-国内版	1	选配
License 授权函-H3C SSL VPN 3000 个用户-国内版	1	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。

新华三技术有限公司

北京总部
北京市朝阳区广顺南大街8号院 利星行中心1号楼
邮编: 100102

杭州总部
杭州市高新技术产业开发区长河路466号
邮编: 310052
电话: 0571-86760000
传真: 0571-86760001

<http://www.h3c.com>

客户服务热线
400-810-0504

Copyright © 2018 新华三技术有限公司 保留一切权利
免责声明: 虽然 H3C 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 H3C 对本资料中的不准确不承担任何责任。
H3C 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。