H3C SecPath F5000 Firewall

Next Generation Firewall

Product overview

H3C SecPath F5000 firewalls provide customers with professional and robust network security protection to safeguard data centers, IT infrastructure, and data assets. H3C SecPath F5000 firewalls can be deployed in multiple modes to address the increasingly complex network and digital environment. Meanwhile, H3C SecPath F5000 firewalls integrate a management platform (H3C CloudNet) that supports cloud deployment and offer a variety of subscribed professional security services to assist customers in tackling security challenges.

Views

	
H3C SecPath F5030/F5060/F5080 firewall	H3C F5030-D/F5060-D/F5080-D firewall

Features and highlights

Hybrid Deployment Architecture

H3C SecPath F5000 firewalls can adapt to different scenario requirements. Whether the enterprise environment is

complex and changeable or pursuing high-efficiency and agility, they can fit perfectly.

All firewall shares a unified operating system Comware, ensuring operational consistency and convenience, and greatly reducing operation and maintenance costs. With this innovative design, H3C firewalls build an all-round, reliable, and user-friendly network security protection system for customers, fully safeguarding enterprise network security.

Also, firewalls can be managed by H3C management platform, enabling consistent distribution, detailed management and dynamic adjustment of policies based on risk levels across hardware, virtualized, cloud-native, and containerized firewalls. The firewalls also feedback the networking changes, security logs and attack findings back to the platform, helping constructing the security situation. In this regard the firewalls and platform work as a whole.

Comware: One Core, Every Defense

Comware is a unified network security operating system designed based on the TCP/IP architecture. H3C hardware firewall, virtualized firewall, cloud firewall, and containerized firewall all run on this operating system. It supports comprehensive networking and security functions and has high scalability. At the same time, it provides high visibility to simplify operation and maintenance procedures. Sharing this common core system, H3C SecPath F5000 firewalls provide every defense in all types of scenarios. Firewall-as-a-service (FWaaS) together with SASE can be easily delivered no matter what the embodiment is.

Comware has a modularized designs presenting abundant features while keeping high reliability. It also quickly reacts to changing technology and realizes rapid delivery.

The comprehensive TCP/IP protocol stack functionality allows the firewall to participate in network deployments with any topology, ensuring seamless integration. Comware supports multi-CPU, multi-core and multi-processing, enhancing data forwarding and processing efficiency.

Carrier-Level High Availability

H3C excels in hardware design. Its elite R&D team meticulously designs from chip to system level, using advanced tech for innovative architecture optimization, ensuring high performance.

Notably, H3C firewalls are highly reliable. They endure rigorous tests. With redundant designs for key components, failure risks are minimized, firmly supporting digital transformation across industries.

Meanwhile, the Comware operating system offers a variety of selectable reliability technologies to ensure high-reliability at the network level.

Supports the RBM (Remote Backup Mechanism) technology, enabling real-time backup of business data and meeting the requirements of active-active and active-standby networking.

Integrated, Flexible and Advanced Protection

H3C SecPath F5000 firewalls boast outstanding security capabilities, integrating functions such as intrusion detection, virus protection, and URL filtering. They can accurately identify and block various malicious traffic, preventing the invasion of viruses and Trojans. The powerful application identification technology can manage a vast number of network applications. Meanwhile, intelligent security policies help flexibly address complex threats. From the network perimeter to the interior, it builds a comprehensive security defense line, safeguarding the security of enterprise information assets.

Intrusion prevention system (IPS)

Supports real-time active interception of DOS, brute force disassembly, port scanning, sniffing, worms and other network attacks or malicious traffic protecting internal network information from infringement.

Application layer traffic identification and management

Uses the state machine and traffic exchange inspection technologies to detect traffic of P2P, IM, network game, stock, network video, and network multi-media applications, such as Facebook, X(twitter), Youtube, Thunder, BitTorrent, eMule, eDonkey, WeChat, Weibo, QQ and MSN. H3C firewalls use the deep inspection technology to identify P2P traffic precisely and provides multiple policies to control and manage the P2P traffic flexibly. Also, H3C SecPath F5000 firewalls support over 7,000 protocols and over 10,000 applications, which are updated every 2 weeks.

Categorized filtering of massive URLs

Uses the local+cloud mode to provide 143 categorized and 130 million URL rules*, providing basic URL filtering blacklist and whitelist and allows you to query the URL category filtering server on line.

Web Application Firewall (WAF)

Deep web security protection. Supports web application protection. For the most CC attacks, SQL injection, HTTP slow attacks, cross-site-scripts and other common attacks, content detection and verification of various requests from web application clients are carried out to ensure their security and legitimacy, and illegal requests are blocked in real time, So as to effectively protect all kinds of websites.

Data leakage prevention (DLP)

Supports email filtering by SMTP mail address, subject, attachment, and content, HTTP URL and content filtering, FTP file filtering, and application layer filtering (including Java/ActiveX blocking and SQL injection attack prevention).

Unknown threat prevention

Uses the situation awareness platform to quickly detect and locate threats. This ensures that the firewall can take global security measures as soon as a single point is under attack. The firewalls support an enhanced AI feature, which enables a more professional AI-based detection capability for unknown threats. The firewalls can also send the unidentified files to sandbox(H3C SecCenter CSAP-ATD).

Flood Attack protection

Detects and prevents various attacks, including Land, Smurf, Fraggle, ping of death, Tear Drop, IP spoofing, IP fragment, ARP spoofing, reverse ARP lookup, invalid TCP flag, large ICMP packet, IP/port scanning, and common DDoS attacks such as SYN flood, UDP flood, DNS flood, and ICMP flood.

Complete and updated security signature database

H3C has a senior signature database team and professional attack protection labs that can provide a precise and up-to-date signature database.

Security zone

Allows you to configure security zones based on interfaces and VLANs.

Packet filtering

Allows you to apply standard or advanced ACLs between security zones to filter packets based on information contained in the packets, such as UDP and TCP port numbers. You can also configure time ranges during which packet filtering will be performed.

Access control

Supports access control based on users and applications and integrates deep intrusion prevention with access control.

ASPF

Dynamically determines whether to forward or drop a packet by checking its application layer protocol information and state. ASPF supports inspecting FTP, HTTP, SMTP, RTSP, and other TCP/UDP-based application layer protocols.

Blacklist

Supports static blacklist and dynamic blacklist.

- * URL libraries in cloud can be extended to 500 million

Intelligent Management

H3C Cloudnet Capacity

H3C SecPath F5000 firewalls can be managed by H3C Cloudnet management platform in the cloud. This integration combines functions such as firewall management, security information and event collection, analysis, and response. Moreover, it enables management across various cloud scenarios, including public clouds, private clouds, hybrid clouds, and traditional IDCs.

H3C SecCenter CSAP-SMP

SMP platform helps customers to manage the firewalls. SMP mainly focuses on local management installed in customer's own environment.

Web GUI and CLI

Web-based management, with simple, user-friendly GUI and integrated CLI-based configuration and management.

Intelligent security policy management

Detects duplicate, redundant or conflicting policies, optimizes policy configurations, detects and proposes security policies dynamically generated in the internal network.

Abundant reports

Include application-based reports and stream-based analysis reports, with various exported report formats, including PDF, HTML, TXT and Microsoft Word. The reports can be customized covering different contents.

Security logs

H3C SecPath F5000 firewalls support various logs including operation logs, security policy logs, threat logs, URL filtering logs, traffic logs and NAT logs.

Comprehensive Networking and VPN Features

Comware natively integrates the networking features with security. This allows firewalls to be deployed in any topology to adapt to customers' different requirements.

Routing

Supports static routing, RIP, OSPF, BGP, routing policies, and application- and URL-based policy-based routing. These allow firewalls to integrate into any complicated networking topologies.

NAT

Supports multiple NAT modes, enabling efficient address translation between private networks and the public network. This allows multiple internal network devices to share a public IP for Internet access. It has a precise port mapping function to open internal services as needed. With intelligent address pool management, it allocates resources reasonably.

Integrated link load balancing feature

Uses link state inspection and link busy detection technologies, and applies to a network egress to balance traffic among links.

Integrated SSL VPN feature

Supports 2FA, and the enterprise's existing authentication system to authenticate users, providing secure access of mobile users to the enterprise network.

VPN Tunnels

Supports L2TP, IPsec/IKE, GRE to establish reliable and encrypted data channels.

Industry-leading IPv6 Features

Abundant IPv6 features help customers migrate their businesses from IPv4 to IPv6 smoothly. Various IPv4-IPv6 technologies also allow firewall to be deployed in dual stacks.

- NAT46/NAT64/NAT66
- IPv6 stateful firewall.
- IPv6 related attack protection.
- IPv6 data forwarding, IPv6 static routing and dynamic routing, and IPv6 multicast.
- IPv6 transition technologies, including NAT-PT, IPv6 over IPv4 GRE tunnel, manual tunnel, 6to4 tunnel, automatic IPv4-compatible IPv6 tunnel, ISATAP tunnel, NAT444, and DS-Lite.
- IPv6 ACL and RADIUS.

SD-WAN Security

The H3C SecPath F5000 firewalls have powerful SDWAN deployment capabilities. The firewalls can flexibly adapt to various network scenarios, easily integrate different link resources such as broadband and dedicated lines, and achieve intelligent routing. In enterprise branch networks and working with H3C AD-WAN controller, it can quickly build secure and stable WAN connections. Through a centralized management platform, it can uniformly manage firewalls in different locations, optimize network configurations in real-time, reduce operation and maintenance costs, provide efficient and reliable WAN network connection guarantees for enterprises, and help enterprises carry out their businesses efficiently.

Zero-touch deployment

Allows customers to launch network services at low cost and high efficiency.

Comprensive Protection

The comprehensive security capabilities of the firewall protect the security of the headquarters and branch departments.

High Visibility

The unified management platform simplifies firewall management and provides rich visibility to monitor the network and security situation.

IoT Security

H3C SecPath F5000 firewalls combined with the management platform can identify various IoT devices based on terminal information such as MAC addresses, IP addresses, and protocols, providing users with visibility into the entire network assets. The firewalls support classifying IoT devices and performing protocol and behavior control on them based on the classifications and various tags, creating a secure operating environment for IoT. It also supports vulnerability scanning and monitoring of IoT devices, providing targeted protection in a timely manner to continuously ensure the security status of IoT devices.

H3C SecPath F5000 firewalls also serve as a security platform for OT scenario. The firewalls can deeply identify dozens

of industrial control protocols and achieve precise management and control through protocol analysis and behavior modeling. The firewalls support customized strategies for OT process, enabling fine-grained access control and abnormal blocking based on protocol commands and traffic characteristics. This effectively defends against illegal operations and vulnerability attacks, ensuring the compliance of industrial control systems and the continuity of business operations.

Technical specifications

Hardware specifications

Item	F5030	F5030-D	F5060	F5060-D	F5080	F5080-D
Dimensions (W × D × H)	440mm×660mm×88.1mm	440mm×660mm×88.1mm	440mm×660mm×88.1mm	440mm×660mm×88.1mm	440mm×660mm×88.1mm	440mm×660mm×88.1mm
USB	2	2	2	2	2	2
Rack mounted	Yes	Yes	Yes	Yes	Yes	Yes
Weight	20.1Kg	20.1Kg	20.1Kg	20.1Kg	20.1Kg	20.1Kg
Power supply	Dual hot-swappable, AC or DC	Dual hot-swappable, AC or DC	Dual hot-swappable, AC or DC	Dual hot-swappable, AC or DC	Dual hot-swappable, AC or DC	Dual hot-swappable, AC or DC
Power consumption	191W	250W	191W	250W	192W	250W
MTBF(Year)	35.68	34.71	38.14	33.41	33.36	35.68
Ports	Host： 4×Combo(GE) Bundle： Slot4: 8×GE Slot1: 8×1/10G SFP+	Host： 4×Combo(GE) Bundle： Slot4: 8×GE Slot1: 8×1/10G SFP+	Host： 4×Combo(GE) Bundle： Slot5: 8×SFP Slot4: 8×GE Slot1: 8×1/10G SFP+	Host： 4×Combo(GE) Bundle： Slot5: 8×SFP Slot4: 8×GE Slot1: 8×1/10G SFP+	Host： 4×Combo(GE) Bundle： Slot5: 8×SFP Slot4: 8×GE Slot1: 8×1/10G SFP+	Host： 4×Combo(GE) Bundle： Slot5: 8×SFP Slot4: 8×GE Slot1: 8×1/10G SFP+
Expansion slots	6	6	5	5	5	5
Interface modules	8×GE Interface Module 8×GE SFP Interface Module 4×GE PFC Interface Module 4×GE SFP+ 4×1/10G SFP+ Interface Module 8×1/10G SFP+ Interface Module 2×40GE QSFP+ Interface Module					
Storage	480G/1.92T/3.84T/7.68T SSD (Raid0/Raid1)					
Flash	4G	4G	4G	4G	4G	4G

Item	F5030	F5030-D	F5060	F5060-D	F5080	F5080-D
SDRAM	16G	16G	32G	32G	64G	64G
Latency	16us	16us	16us	16us	16us	16us
Temperature	Operating: without hard disk 0°C～45°C, with hard disk 5°C～40°C Storage: Temperature：-40°C～70°C					
Environmental protection	EU RoHS Compliance					
EMC	FCC Part 15 (CFR 47) CLASS A ICES-003 CLASS A VCCI CLASS A CISPR 22 CLASS A EN 55022 CLASS A AS/NZS CISPR22 CLASS A CISPR 32 CLASS A EN 55032 CLASS A AS/NZS CISPR32 CLASS A CISPR 24 EN 55024 EN 61000-3-2 EN 61000-3-3 ETSI EN 300 386 GB 9254 GB 17625.1 YD/T 993					
Safety	UL 60950-1 CAN/CSA C22.2 No 60950-1 IEC 60950-1 EN 60950-1 AS/NZS 60950-1 FDA 21 CFR Subchapter J GB 4943.1					

Software specifications

Item	Description
Operation modes	Route, transparent, and hybrid

Item	Description
AAA	Portal authentication RADIUS authentication HWTACACS authentication PKI/CA (X.509 format) authentication Domain authentication CHAP authentication PAP authentication
Firewall	Context virtual firewall technology, which supports full virtualization of hardware resources, including CPU, memories, and storage Security zone allocation Security policy redundancy analysis Protection against malicious attacks, such as land, smurf, fraggle, ping of death, teardrop, IP spoofing, IP fragmentation, ARP spoofing, reverse ARP lookup, invalid TCP flag, large ICMP packet, address/port scanning, SYN flood, ICMP flood, UDP flood, and DNS query flood Basic and advanced ACLs Time range-based ACL User-based and application-based access control ASPF application layer packet filtering Static and dynamic blacklist function MAC-IP binding MAC-based ACL MAC-Limitation 802.1Q VLAN transparent transmission Traffic policy Connection limit policy Bandwidth control
Antivirus	Signature-based virus detection Manual and automatic upgrade for the signature database Stream-based processing Virus detection based on HTTP, FTP, SMTP, and POP3 Virus types include Backdoor, Email-Worm, IM-Worm, P2P-Worm, Trojan, AdWare, and Virus Virus logs and reports

Item	Description
Deep intrusion prevention	Prevention against common attacks such as hacker, worm/virus, Trojan, malicious code, spyware/adware, DoS/DDoS, buffer overflow, SQL injection, and IDS/IPS bypass Attack signature categories (based on attack types and target systems) and severity levels (including high, medium, low, and notification) Manual and automatic upgrade for the attack signature database (TFTP and HTTP). P2P/IM traffic identification and control Detection of the real source IP address of HTTP packet Source tracing and alarming base on attack event: log, email alert, collect hit statistics, packet capture, upload packet capture files
Email/webpage/application layer filtering	Email filtering SMTP email address filtering Email subject/content/attachment filtering Flow-based web filtering HTTP URL/content filtering Java blocking ActiveX blocking HTTPS traffic filtering: SNI extraction based on SSL negotiation process SQL injection attack prevention
Asset-security analysis	Botnet Analysis: analyses all security logs related to botnets and supports displaying information about hosts that might be zombie hosts, including zombie host IP and peer IP Security Analysis: analyzes health status of hosts and supports displaying the number of compromised hosts and security event distribution in graphs and tables Threat case management: an alarm resource pool to store threat logs and allows users to add the logs to cases for ease of log management.
NAT	Many-to-one NAT, which maps multiple internal addresses to one public address Many-to-many NAT, which maps multiple internal addresses to multiple public addresses One-to-one NAT, which maps one internal address to one public address NAT of both source address and destination address External hosts access to internal servers Internal address to public interface address mapping NAT support for DNS Setting effective period for NAT NAT ALGs for NAT ALG, including DNS, FTP, H.323, ILS, MSN, NBT, PPTP, and SIP NAT64 Policy, NAT translation between IPv4 networks and IPv6 networks NAT66 Policy, NAT translation between IPv6 networks

Item	Description
VPN	L2TP VPN IPSec VPN GRE VPN SSL VPN ADVPN
IPSEC	IKEv1, IKEv2 negotiation IPsec smart link selection IPsec Reverse Route Injection Peer address backup and switchback
IPSEC VPN Authentication Algorithm	MD5/SHA1/SM3
IPv6	IPv6 status firewall IPv6 attack protection IPv6 forwarding IPv6 protocols such as ICMPv6, PMTU, Ping6, DNS6, TraceRT6, Telnet6, DHCPv6 Client, and DHCPv6 Relay IPv6 routing: RIPng, OSPFv3, BGP4+, IPv6 static routing, IPv6 policy-based routing IPv6 multicast: PIM-SM, and PIM-DM IPv6 transition techniques: NAT-PT, IPv6 tunneling, NAT64 (DNS64), NAT66, and DS-LITE IPv6 security: NAT-PT, IPv6 tunnel, IPv6 packet filter, RADIUS, IPv6 zone pair policies, IPv6 connection limit
High availability	RBM with Active/active and active/standby stateful failover RBM with Mirroring Mode Configuration synchronization of two firewalls IKE state synchronization in IPsec VPN VRRP Track
Virtualization	Context: virtualized logical firewalls vSystems: lightweight virtualized independent logical firewalls
Configuration management	Remote management through Web GUI Configuration management at the CLI SNMPv3, compatible with SNMPv2 and SNMPv1 Intelligent security policy Managed by H3C SDN controller
Maintenance and diagnostics	Packet trace Packet capture IPsec diagnosis Dropped-Packet statistics

Performance specifications

Item	F5030/F5030-D	F5060/F5060-D	F5080/F5080-D
Firewall throughput (1518 Bytes)	30Gbps	50Gbps	80Gbps
Firewall throughput (512 Bytes)	25Gbps	30Gbps	40Gbps
Application layer throughput(APP)	30Gbps	40Gbps	40Gbps
Application layer throughput(APP+IPS+WAF)	18Gbps	20Gbps	20Gbps
Threat protection throughput(APP+IPS+AV+URL)	16Gbps	18Gbps	18Gbps
IPSec tunnel (site-to-site)	8,000/8,000	12,000/8,000	24,000/8,000
IPSec throughput(1400 Bytes)	18Gbps	18Gbps	18Gbps
SSL VPN users	12,000/12,000	24,000/12,000	48,000/12,000
SSL VPN throughput	2.5Gbps	3.5Gbps	3.6Gbps
Concurrent sessions	16M	40M	80M
News sessions /second	500K	600K	600K
Security policies	50,000	50,000	50,000
Context*	16	32	64
vSystem	256	512	512

- *The number is halved after the Deep packet inspection function is enabled.

Ordering information

Item		Description
Hardware appliance	H3C SecPath F5030	H3C SecPath F5030 Firewall Appliance
	H3C SecPath F5030-D	H3C SecPath F5030-D Firewall Appliance
	H3C SecPath F5060	H3C SecPath F5060 Firewall Appliance
	H3C SecPath F5060-D	H3C SecPath F5060-D Firewall Appliance

Item		Description
	H3C SecPath F5080	H3C SecPath F5080 Firewall Appliance
	H3C SecPath F5080-D	H3C SecPath F5080-D Firewall Appliance
Modules	NSQM1GT8A	8-port GE copper interface module
	NSQM1GP8A	8-port GE fiber interface module
	NSQM1GT4PFCA	4-port PFC interface module
	NSQM1TG8A	8-port SFP+ fiber transceiver module
	NSQM1QG2A	2-port QSFP+ fiber transceiver module
	NSQM1G4XS4	4-port SFP and 4-port SFP+ fiber transceiver module
Hard disk	NS-SSD-480G-SATA-SFF	H3C SecPath Series,480GB 2.5inch SATA SSD HardDisk Module
	NS-SSD-1.92T-SATA-SFF	H3C SecPath Series 1.92TB 2.5inch SATA SSD Module
	NS-SSD-3.84T-SATA	H3C SecPath 3.84TB 2.5inch SATA SSD Module
	NS-SSD-7.68T-SATA	H3C SecPath 7.68TB 2.5inch SATA SSD Module
FAN	FAN-20F-2-A	Fan tray module (power to port airflow)
	FAN-20B-2-A	Fan tray module (port to power airflow)
Power supply	PSR650B-12A1-A	650W DC power supply
	PSR650B-12D1-A	650W AC power supply
	PSR650B-12AHD-F	650W HVDC Power Supply

Subscriptions

Service Category	Service offering
Security services	H3C SecPath F5000 firewalls IPS Signature Update License
	H3C SecPath F5000 firewalls URL Signature Update License
	H3C SecPath F5000 firewalls AV antivirus Signature Update License
	H3C SecPath F5000 firewalls Application Identification Signature Update License
	H3C SecPath F5000 firewalls WAF Signature Update License
	H3C SecPath F5000 firewalls TI Signature Update License
Networking services	H3C SecPath LB License
VPN services	H3C SecPath SSL VPN for X users
Advanced service	Overseas security expert daily service

New H3C Technologies Co., Limited
Beijing Headquarters
Tower 1, LSH Center, 8 Guangshun South Street, Chaoyang
District, Beijing, China
Zip: 100102
Hangzhou Headquarters
No.466 Changhe Road, Binjiang District, Hangzhou, Zhejiang,
China Zip: 310052
Tel: +86-571-86760000
Fax: +86-571-86760001

https://www.h3c.com