H3C SecPath Series F5000 Firewalls

Next Generation Firewalls

Release Date: November, 2019

New H3C Technologies Co., Limited

H3C SecPath Series F5000 Firewalls

Product overview

H3C SecPath F5000 series is the new-generation high-performance firewalls for large-scale enterprise campus networks, service providers, and data centers.
The F5000 firewall series meets the requirements of Web 2.0, and supports the following security and network features:

- Security protection and access control based on users, applications, time, five tuples, and content security. Typical security protection features include IPS, AV, and DLP.
- VPN services, including IPSec VPN, SSL VPN, L2TP VPN, GRE VPN, and ADVPN.
- Routing capabilities, including static routing, RIP, OSPF, BGP, routing policies, and application- and URL-based policy-based routing.
- IPv4 and IPv6 dual stacks, and state protection and attack prevention for IPv6.

F5000 series firewall uses one AC or DC power module, or two power modules of the same type for power redundancy. H3C SecPath F5000 series firewalls are 2U high and provide high-density GE and 10GE port access capabilities. F5000 series supports stateful failover to meet high availability requirements in high performance networks. The F5030/5060/5080 and the F5030-D/5060-D/5080-D with two MPUs provide replaceable fan trays that support front-to-rear aisles to meet data center requirements.

Following the latest ICSA Labs firewall security certification test cycle, H3C's next generation firewall appliances satisfied the complete set of ICSA Labs Corporate Firewall and Baseline Firewall security testing requirements. As a result, the H3C SecPath Firewall Family was awarded ICSA Labs Firewall Certification having met all of the testing requirements.

F5030/F5030-D Front View

F5030/F5030-D Rear View

F5060/F5060-D/F5080/F5080-D Front View

F5060/F5060-D/F5080/F5080-D Rear View

ICSA labs CERTIFIED FIREWALL - CORPORATE

Features and Benefits

High-performance software and hardware platforms

The firewall series is powered by advanced 64-bit multi-core processors and caches.

Carrier-level high availability

- Adopts H3C highly-available proprietary software and hardware platforms that have been successfully applied in many Telecom carriers and small- to medium-sized enterprises.
- Supports H3C SCF, which can virtualize multiple devices into one device for service backup and system performance improvement.

Powerful security protection features

- **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.
- **SOP 1:N virtualization**—Adopts the container-based virtualization technology. An F5000 firewall can be virtualized into multiple logical firewalls, which have the same features as the physical firewall. Each virtual firewall can have its own security policy and can be managed independently.
- **Security zone**—Allows users to configure security zones based on interfaces and VLANs.
- **Packet filtering**—Allows users 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. User can also configure time ranges during which packet filtering will be performed.
- **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.
- **AAA**—Supports authentication based on RADIUS/HWTACACS+, CHAP, PAP, and LDAP.
- **Blacklist**—Supports static blacklist and dynamic blacklist.
- **NAT and VRF-aware NAT**.
- **VPN**—Supports L2TP, IPsec/IKE, GRE, and SSL VPNs. Allows smart devices to connect to the VPNs.

- **Routing**—Supports static routing, RIP, OSPF, BGP, routing policies, and application- and URL-based policy-based routing.
- **Security logs**—Supports operation logs, zone pair policy matching logs, attack protection logs, DS-LITE logs, and NAT444 logs.
- **Traffic monitoring, statistics, and management.**

Flexible and extensible, integrated and advanced security

- Integrated security service processing platform—Highly integrates the basic and advanced security protection measures to a security platform.
- Application layer traffic identification and management.
    - Adopts 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 Thunder, Web Thunder, BitTorrent, eMule, eDonkey, WeChat, Weibo, QQ, MSN, and PPLive.
    - Adopts the deep inspection technology to identify P2P traffic precisely and provides multiple policies to control and manage the P2P traffic flexibly.
- Highly precise and effective intrusion inspection engine. The firewall uses the H3C-proprietary Full Inspection with Rigorous State Test (FIRST) engine and various intrusion inspection technologies to implement highly precise inspection of intrusions based on application states. The FIRST engine also supports software and hardware concurrent inspections to improve the inspection efficiency.
- Real-time virus protection. The firewall uses the stream-based antivirus engine to prevent, detect, and remove malicious code from network traffic.
- Massive URL category filtering. The firewall supports local + cloud mode, 139 category libraries, and over 20 million URL rules.
- Complete and updated security signature database. H3C has a senior signature database team and professional attack protection labs, guaranteeing the signature database is always precise and up to date.

Industry-leading IPv6 features

- IPv6 stateful firewall.
- IPv6 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.

Next-generation multi-service features

- **Integrated link load balancing feature**: This feature uses the link state inspection and link busy detection technologies, and applies to a network egress to balance traffic among links.
- **Integrated SSL VPN feature**: This feature can use USB-Key, SMS messages, and the enterprise's existing authentication system to authenticate users, providing secure access of mobile users to the enterprise network.
- **Data leakage prevention (DLP)**:The firewall 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.
- **Intrusion prevention system (IPS)**: Support real-time active interception of DOS, brute force disassembly, port scanning, sniffing, worms and other network attacks or malicious traffic, protect internal network information from infringement.
- **Antivirus (AV)**: The firewall uses a high-performance virus engine that can protect against more than 5 million viruses and Trojan horses. The virus signature database is automatically updated every day.
- **Unknown threat defense**:By cooperating with the situation awareness platform, the firewall can quickly detect attacks and locate problems. Once a single point is attacked, the firewall can trigger security warnings and take fast responses in the whole network.
- **Web Application Firewall (WAF)**—Deep web security protection. Support fine web application protection. For the most headache CC attacks, abnormal extraneous, 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.

Intelligent management

- Intelligent and unified security policy management, which detects duplicate policies,

- Unified security management provided by the H3C SSM, which can collect and analyze security information, and offer an intuitive view into network and security conditions, saving management efforts and improving management efficiency.
- Centralized log management based on advanced data drill-down and analysis technology. It can request and receive information to generate logs, compile different types of logs (such as sys-logs and binary stream logs) in the same format, and compress and store large amounts of logs. User can encrypt and export saved logs to external storage devices such as DAS, NAS, and SAN to avoid loss of important security logs.
- Abundant reports, including application-based reports and stream-based analysis reports.
- Export of reports in different formats, such as PDF, HTML, word, and txt.
- Report customization through the Web interface. Customizable contents include time range, data source device, generation period, and export format.

Service chain

Service chain is a forwarding technology used to guide network traffic through service nodes. It is based on the Overlay technology and combines the software defined network (SDN) centralized management theory. User can configure service chains by using a virtual converged framework controller (VCFC).

Service chain implements the following functions:

- Decoupling the tenant logical network and the physical network, and separating the control plane from the forwarding plane.
- Service resource allocation and deployment on demand with no physical topology restriction.
- Dynamic creation and automatic deployment of network function virtualization (NFV) resource pools.
- Tenant-specific service arrangement and modification without affecting the physical topology and other tenants.

Specifications

Items	**F5030/F5030-D**	**F5060/F5060-D** **F5080/F5080-D**
Dimensions (W × D × H)	440*650*88.4mm	440*650*88.4mm
USB	2	2
Weight	20kg	20kg

Items	F5030/F5030-D	F5060/F5060-D F5080/F5080-D
Power Supply	AC or DC, redundant	AC or DC, redundant
Power consumption (Max)	650W	650W
Storage	2 × 480G SSD	2 × 480G SSD
Flash	4GB	4GB
SDRAM	16G/16G	32G/32G/64G/64G
Fixed Ports	4 ×GE Combo 8 ×10/100/1000Base-T (fixed on slot4) 8 × 10G SFP+ ports(fixed on slot1)	4 × GE Combo 8 ×10/100/1000Base-T(fixed on slot4) 8 × SFP ports(fixed on slot5) 8 × 10G SFP+ ports(fixed on slot1)
Expansion slots	6/5; For F5030: slot1&slot4 occupied; Slot2&slot3 for high-speed modules (SFP+/QSFP+), slot 5/6/7/8 for low-speed modules (PFC/GE/SFP) For F5030-D: slot1&slot4 occupied; Slot7 pre-installed one main control engine. Slot2&slot3 for high-speed modules (SFP+/QSFP+), slot 5/6 for low-speed modules (PFC/GE/SFP); slot8 for redundant main control engine	5/4/5/4; For F5060/80: slot1&4&5 occupied; Slot2&slot3 for high-speed modules (SFP+/QSFP+), slot 6/7/8 for low-speed modules (PFC/GE/SFP) For F5060-D/5080-D: slot1&slot4&5 occupied; slot7 pre-installed one main control engine. Slot2&slot3 for high-speed modules (SFP+/QSFP+), slot6 for low-speed modules (PFC/GE/SFP); slot8 for redundant main control engine
Interface modules	8*SFP/8*GE/4*GE Bypass/8*SFP+/2*QSFP+/4SFP&4SFP+	8*SFP/8*GE/4*GE Bypass/8*SFP+/2*QSFP+/4SFP&4SFP+
Ambient temperature	Operating: 0°C to 45°C (32°F to 113°F) Storage: –40°C to +70°C (–40°F to +158°F)	
Operating mode	Route, transparent, or hybrid.	
AAA	Portal authentication. RADIUS authentication. HWTACACS authentication. PKI/CA (X.509 format) authentication. Domain authentication. CHAP authentication. PAP authentication.	
Firewall	Virtual firewall. Security zone. Attack 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.	

Items	F5030/F5030-D	F5060/F5060-D F5080/F5080-D
	Time range-based ACL. User-based and application-based access control. Dynamic packet filtering. ASPF application layer packet filtering. Static and dynamic blacklist function. MAC-IP binding. MAC-based ACL. 802.1Q VLAN transparent transmission.	
Load balancing	Link and server load balancing. Application- and ISP-based Intelligent route selection. Health monitoring through ICMP, UDP, and TCP. Port-, HTTP-, and SSL-based sticky methods to implement busy bandwidth and fault protection.	
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.	
Deep intrusion prevention	Prevention against 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.	
Email/webpage/application layer filtering	Email filtering SMTP email address filtering Email subject/content/attachment filtering Webpage filtering HTTP URL/content filtering Java blocking ActiveX blocking SQL injection attack prevention	
Behavior and content audit	User-based content audit and tracking.	
File filtering	Identification of file types such as Word, Excel, PPT, PDF, ZIP, RAR, EXE, DLL, AVI, and MP4, and filtering of sensitive information in the files.	
URL filtering	Over 50 types of signature-based URL filtering rules, and discarding, reset, redirection, logging, and blacklisting of packets matching the rules.	
Application identification and control	Identification of various types of applications, and access control based on specific functions of an application.	

Items	F5030/F5030-D	F5060/F5060-D F5080/F5080-D
	Combination of application identification and intrusion prevention, antivirus, and content filtering, improving detection performance and accuracy.	
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.	
VPN	L2TP VPN. IPSec VPN. GRE VPN. SSL VPN.	
Routing	Routing protocols such as RIP, OSPF, BGP, and IS-IS.	
VXLAN	VXLAN service chain.	
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+, static routing, policy-based routing IPv6 multicast: PIM-SM, and PIM-DM. IPv6 transition techniques: NAT-PT, IPv6 tunneling, NAT64 (DNS64), and DS-LITE. IPv6 security: NAT-PT, IPv6 tunnel, IPv6 packet filter, RADIUS, IPv6 zone pair policies, IPv6 connection limit.	
High availability	SCF 2:1 virtualization Active/active and active/standby stateful failover. Configuration synchronization of two firewalls IKE state synchronization in IPsec VPN. VRRP.	
Configuration management	Configuration management at the CLI. Remote management through Web. Device management through H3C SSM. SNMPv3, compatible with SNMPv2 and SNMPv1. Intelligent security policy	
EMC	FCC Part 15 (CFR 47) CLASS A ICES-003 CLASS A VCCI CLASS A	

Items	F5030/F5030-D	F5060/F5060-D F5080/F5080-D
	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/T 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	

Performance

	F5030	**F5030-D**	**F5060**	**F5060-D**	**F5080**	**F5080-D**
Firewall Throughput (1518Bytes)	35Gbps	35Gbps	50Gbps	50Gbps	80Gbps	80Gbps
NGFW Throughput	10Gbps	10Gbps	12Gbps	12Gbps	12Gbps	12Gbps
NGFW+IPS	10Gbps	10Gbps	12Gbps	12Gbps	12Gbps	12Gbps
NGFW+IPS+AV	8Gbps	8Gbps	8Gbps	8Gbps	8Gbps	8Gbps
Maximum concurrent sessions	16M	16M	40M	40M	80M	80M
Maximum New Connections per second	500K	500K	600K	600K	600K	600K
IPSec Throughput	14Gbps	14Gbps	16Gbps	16Gbps	18Gbps	18Gbps

Concurrent SSL-VPN Users	30K	20K	30K	20K	30K	20K

Ordering Information

SecPath Series F5000	
NS-SecPath F5030	H3C SecPath F5030 Firewall Host
NS-SecPath F5030-D	H3C SecPath F5030-D Firewall Host
NS-SecPath F5060	H3C SecPath F5060 Firewall Host
NS-SecPath F5060-D	H3C SecPath F5060-D Firewall Host
NS-SecPath F5080	H3C SecPath F5080 Firewall Host
NS-SecPath F5080-D	H3C SecPath F5080-D Firewall Host
Power Supply	For F5020/5040
PSR300-12A2-A	H3C 300W AC Power Supply
PSR300-12D2-A	H3C 300W DC Power Supply
Power Supply	For F5030/5060/5080 and F5030-D/5060-D/5080-D
PSR650B-12A1-A	650W AC Power Supply
PSR650B-12D1-A	650W DC Power Supply
Fan Tray	For F5030/5060/5080 and F5030-D/5060-D/5080-D
FAN-20B-2-A	H3C Fan Tray Module(Port to Power Airflow)
FAN-20F-2-A	H3C Fan Tray Module(Power to Port Airflow)
Modules	For F5020/5040
NSQM1G24XS6	H3C SecPath 24-port 1000M and 6-port 10G Ethernet Interface Module(12RJ45+12SFP+6SFP+)
Modules	For F5030/5060/5080 and F5030-D/5060-D/5080-D
NSQM1GT4PFCA	H3C SecPath Series F5000,4 Ports PFC Module
NSQM1GT8A	H3C SecPath Series F5000,8 Ports GE Module
NSQM1QG2A	H3C SecPath Series F5000,2 Ports QSFP+ Module
NSQM1GP8A	H3C SecPath Series F5000,8 Ports SFP Module
NSQM1TG8A	H3C SecPath Series F5000,8 Ports SFP+ Module
NSQM1G4XS4	H3C SecPath Series F5000,4-Port SFP,4-Port SFP+ Module
Hard Disk	For F5030/5060/5080 and F5030-D/5060-D/5080-D
NS-SSD-480G-SATA-SFF	H3C SecPath Series,480GB 2.5inch SATA SSD HardDisk Module
License	
LIS-F5000-IPS-1Y	H3C SecPath F5000,IPS Signature Update Service,1 Year
LIS-F5000-IPS-3Y	H3C SecPath F5000,IPS Signature Update Service,3 Years
LIS-F5000-AV-1Y	H3C SecPath F5000,AV Anti-Virus Security License,1 Year
LIS-F5000-AV-3Y	H3C SecPath F5000,AV Anti-Virus Security License,3 Years
LIS-F5000-ACG-1Y	H3C SecPath F5000,Application Signature Update Service,1 Year
LIS-F5000-ACG-3Y	H3C SecPath F5000,Application Signature Update Service,3 Years
LIS-F5000-LB	H3C SecPath F5000,LB License
LIS-F5000-SSL-75	H3C SecPath F5000,SSL VPN for 75 Users
LIS-F5000-SSL-500	H3C SecPath F5000,SSL VPN for 500 Users

LIS-F5000-SSL-1000	H3C SecPath F5000,SSL VPN for 1000 Users
LIS-F5000-SSL-3000	H3C SecPath F5000,SSL VPN for 3000 Users
LIS-F5000-URL-1Y	H3C SecPath F5000 URL Signature Update Service License,1 Year
LIS-F5000-URL-3Y	H3C SecPath F5000 URL Signature Update Service License,3 Years
LIS-IMC7-SVF5KA-75	H3C iMC-SSL VPN Authentication Client-F5000-75 License
LIS-IMC7-SVF5KB-500	H3C iMC-SSL VPN Authentication Client-F5000-500 License
LIS-IMC7-SVF5KC-1K	H3C iMC-SSL VPN Authentication Client-F5000-1000 License
LIS-IMC7-SVF5KD-3K	H3C iMC-SSL VPN Authentication Client-F5000-3000 License
LIS-F5000-WAF-1Y	H3C SecPath F5000 WAF Signature Update License,1 Year
LIS-F5000-WAF-3Y	H3C SecPath F5000 WAF Signature Update License,3 Years
Transceivers	
SFP-GE-SX-MM850-A	1000BASE-SX SFP Transceiver, Multi-Mode (850nm, 550m, LC)
SFP-GE-LX-SM1310-A	1000BASE-LX SFP Transceiver, Single Mode (1310nm, 10km, LC)
SFP-GE-LH40-SM1310	1000BASE-LH40 SFP Transceiver, Single Mode (1310nm, 40km, LC)
SFP-GE-LH40-SM1550	1000BASE-LH40 SFP Transceiver, Single Mode (1550nm, 40km, LC)
SFP-GE-LH80-SM1550	1000BASE-LH80 SFP Transceiver, Single Mode (1550nm, 80km, LC)
SFP-GE-LH100-SM1550	1000BASE-LH100 SFP Transceiver, Single Mode (1550nm, 100km, LC)
SFP-XG-LX220-MM1310	SFP+ Module(1310nm,220m,LC)
SFP-XG-SX-MM850-A	SFP+ Module(850nm,300m,LC)
SFP-XG-LX-SM1310	SFP+ Module(1310nm,10km,LC)
SFP-XG-LH40-SM1550	SFP+ Module(1550nm,40km,LC)
QSFP-40G-LR4-WDM1300	40GBASE-LR4 QSFP+ Optical Transceiver Module
Services	
SV-PS-SES-OS	Oversea Security Expert Service

The Leader in Digital Solutions

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

Disclaimer: Though H3C strives to provide accurate information in this document, we cannot guarantee that details do not contain any technical error or printing error. Therefore, H3C cannot accept responsibility for any inaccuracy in this document. H3C reserves the right for the modification of the contents herein without prior notification

http://www.h3c.com