H3C SecPath Series
F1000-AI Firewalls

Next Generation Firewalls

Release Date: February, 2021

New H3C Technologies Co., Limited

H3C SecPath Series F1000-AI Firewalls

Product overview

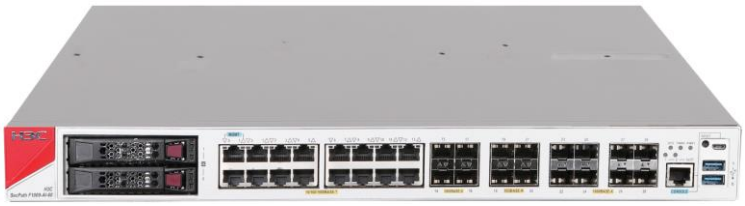
H3C SecPath Series F1000-AI firewalls bring innovative Artificial Intelligence (AI) capabilities to small and medium enterprises, campus egress, and WAN branches.

H3C SecPath Series F1000-AI 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 other elements. Typical security protection features include IPS, AV, and DLP.
- VPN services, including L2TP VPN, GRE VPN, IPsec VPN, and SSL VPN.
- 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.

F1000-AI-10 Front View

F1000-AI-10 Rear View



F1000-AI-60/70 Front View

F1000-AI-60/70 Rear View

F1000-AI-80 Front View

F1000-AI-80 Rear View

F1000-AI-90 Front View

F1000-AI-90 Rear View

F1000-AI-25 Front View

F1000-AI-25 Rear View

F1000-AI-35 Front View

F1000-AI-35 Rear View

F1000-AI-55 Front View

F1000-AI-55 Rear View

F1000-AI-65 Front View

F1000-AI-65 Rear View

F1000-AI-75 Front View

F1000-AI-75 Rear View

Features and Benefits

High-performance software and hardware platforms

The F1000 series uses advanced 64-bit multi-core processors and caches.

Carrier-level high availability

- Uses H3C proprietary software and hardware platforms that have been proven by Telecom carriers and small- to medium-sized enterprises.

- Supports H3C SCF, which can virtualize multiple devices into one device for unified resources management, service backup, and system performance improvement.

Powerful security protection

- **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 N:1 virtualization**—Uses the container-based virtualization technology. An F1000 series 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 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.
- **AAA**—Supports authentication based on RADIUS/HWTACACS+, CHAP, and PAP.
- **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 DPI 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.**
  - 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 Thunder, Web Thunder, BitTorrent, eMule, eDonkey, WeChat, Weibo, QQ, MSN, and PPLive.
  - Uses the deep inspection technology to identify P2P traffic precisely and provides multiple policies to control and manage the P2P traffic flexibly.
  - H3C SecPath NGFW support over 7,000 protocols and over 6,000 applications, which are updated every 2 weeks.
- **Highly precise and effective intrusion inspection engine**—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.
- **Realtime virus protection**—uses the stream-based antivirus engine to prevent, detect, and remove malicious code from network traffic.
- **Categorized filtering of massive URLs**—uses the local+cloud mode to provide 139 categorized and 130 million URL libraries, and support over 20 million URL filtering rules, provides basic URL filtering blacklist and whitelist and allows you to query the URL category filtering server on line.
- **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.

Industry-leading IPv6 features

- 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.

Next-generation multi-service features

- **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**—Uses 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)**—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.
- **Anti-virus (AV)**—Uses a high-performance virus detection engine and a daily updated virus signature database to prevent attacks from over 5 million viruses.
- **Unknown threat prevention**—Uses the situation awareness platform to fast detect and locate threats. This ensures that the firewall can take global security measures as soon as a single point is under attack.
- **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 security policy management—Detects duplicate policies, optimizes policy matching rules, detects and proposes security policies dynamically generated in the internal network.
- SNMPv3—Compatible with SNMPv1 and SNMPv2.
- CLI-based configuration and management.
- Web-based management, with simple, user-friendly GUI.
- H3C IMC SSM unified management—Collects and analyzes security information, and offers 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—Requests and receives information to generate logs, compiles different types of logs (such as syslogs and binary stream logs) in the same format, and compresses and stores large amounts of logs. You 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—Include application-based reports and stream-based analysis reports.
- Various exported report formats—Include PDF, HTML, word, and txt.
- Report customization through the Web interface—Customizable contents include time range, data source device, generation period, and export format.

Specifications

Item	F1000-AI-10	F1000-AI-60/70	F1000-AI-80/90	F1000-AI-25/35/55	F1000-AI-65/75
Dimensions (W × D × H)	440mm×260mm ×44.2mm	440mm×435mm×44.2mm			
USB 3.0	2	2	2	2	2
rack mounted	Yes	Yes	Yes	Yes	yes
Weight	3.7kg	10.0kg	10.0kg	5.4kg	5.6kg
Power Supply	AC	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	39W	180W	180W	23W	46W
MTBF(Year)	77.36	45.39	43.2	53.38	50.31
Ports	1 × Console port (CON) 2 × Management port 18 × Gigabit Ethernet copper ports 4 × Gigabit Ethernet Bypass ports 8 ×Gigabit Ethernet Combo ports 2 × 10-Gigabit Ethernet fiber ports	1 × Console port (CON) 2 × Management port 12 × Gigabit Ethernet fiber ports 14 × Gigabit Ethernet copper ports 4 × 10-Gigabit Ethernet fiber ports	1 × Console port (CON) 2 × Management port 8 × Gigabit Ethernet fiber ports 14 × Gigabit Ethernet copper ports 8 × 10-Gigabit Ethernet fiber ports	1 × Console port (CON) 1 × Management port 6 × Gigabit Ethernet fiber ports 16 × Gigabit Ethernet copper ports 4 × Gigabit Ethernet Combo ports 2 × 10-Gigabit Ethernet fiber ports	1 × Console port (CON) 1 × Management port 4 × Gigabit Ethernet fiber ports 16 × Gigabit Ethernet copper ports 4 × Gigabit Ethernet Combo ports 6 × 10-Gigabit Ethernet fiber ports
Expansion slots	0	2/4	4	2	2
Interface modules	N/A	4-port GE PFC interface module 4-port GE fiber interface module 4-port 10-GE fiber interface module 6-port 10-GE fiber interface module	4-port GE PFC interface module 4-port GE fiber interface module 4-port 10-GE fiber interface module 6-port 10-GE fiber interface module	4-port GE PFC interface module 4-port GE fiber interface module 4-port 10-GE fiber interface module	4-port GE PFC interface module 4-port GE fiber interface module 4-port 10-GE fiber interface module 6-port 10-GE fiber interface module
Storage	480G M.2	2 × 480G SSD	2 × 480G SSD	1 × 480G SSD/ 500G HDD/1TB HDD	2 × 480G SSD/ 500G HDD/1TB HDD
Flash	4GB	4GB	8GB	4GB	4GB

SDRAM	2GB	8G	16G	4GB/4GB/8GB	8G
Temperature	Operating: 0°C to 45°C (32°F to 113°F) Storage: –40°C to +70°C (–40°F to +158°F)				
Operation modes	Route, transparent, and hybrid				
AAA	Portal authentication RADIUS authentication HWTACACS authentication PKI/CA (X.509 format) authentication Domain authentication CHAP authentication PAP authentication				
Firewall	SOP virtual firewall technology, which supports full virtualization of hardware resources, including CPU, memories, and storage Security zone allocation 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 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				
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				
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				
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
IPSEC VPN	ESP-DES-CBC/ESP-3DES-CBC/ESP-AES-128-CBC/ESP-AES-192-CBC/ESP-AES-256-CBC/ ESP-AES-128-GCM/ESP-NULL/SM1-cbc-128/SM4-cbc
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+, 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
IEEE	IEEE 802.1X
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 IMC SSM SNMPv3, compatible with SNMPv2 and SNMPv1 Intelligent security policy
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

Performance

	F1000-AI-10	**F1000-AI-25**	**F1000-AI-35**	**F1000-AI-55**	**F1000-AI-60**	**F1000-AI-70**	**F1000-AI-65**	**F1000-AI-75**	**F1000-AI-80**	**F1000-AI-90**
Firewall Throughput (1518Bytes)	1.5Gbps	3Gbps	4Gbps	6Gbps	8Gbps	9Gbps	10Gbps	15Gbps	20Gbps	25Gbps
NGFW Throughput	600Mbps	2.5Gbps	3Gbps	3.5Gbps	4.5Gbps	4.5Gbps	5Gbps	5.5Gbps	6Gbps	15Gbps
NGFW+IPS	600Mbps	2.5Gbps	3Gbps	3.5Gbps	4.5Gbps	4.5Gbps	5Gbps	5.5Gbps	6Gbps	14Gbps
NGFW+IPS+AV	500Mbps	1.5Gbps	2Gbps	2.5Gbps	4Gbps	4Gbps	4.5Gbps	5Gbps	5.5Gbps	14Gbps
Maximum concurrent sessions	0.9M	2.5M	2.5M	5M	5M	5M	5M	5M	10M	10M
Maximum New Connections per second	15K	30K	40K	50K	80K	80K	100K	120K	150K	240K

Ordering Information

SecPath Series F1000-AI	
NS-SecPath F1000-AI-10	H3C SecPath F1000-AI-10 Firewall Appliance
NS-F1000-AI-25	H3C SecPath F1000-AI-25 Firewall Appliance
NS-F1000-AI-35	H3C SecPath F1000-AI-35 Firewall Appliance
NS-F1000-AI-55	H3C SecPath F1000-AI-55 Firewall Appliance
NS-F1000-AI-60	H3C SecPath F1000-AI-60 Firewall Appliance
NS-F1000-AI-65	H3C SecPath F1000-AI-65 Firewall Appliance
NS-F1000-AI-70	H3C SecPath F1000-AI-70 Firewall Appliance
NS-F1000-AI-75	H3C SecPath F1000-AI-75 Firewall Appliance
NS-F1000-AI-80	H3C SecPath F1000-AI-80 Firewall Appliance
NS-F1000-AI-90	H3C SecPath F1000-AI-90 Firewall Appliance
Power Supply	
PSR150-A1-B	150W AC Power Supply
PSR150-D1-B	150W DC Power Supply
PSR250-12A1	250W AC Power Supply Module(Air Outlets in Panel)
PSR450-12D	450W DC Power Supply Module (Air Outlets in Panel)
PSR450-12AHD	450W HVDC Power Supply Module (AC/336V HVDC Input Supported, Air Outlets in Panel)
Modules	
NSQM1GT4PFC	H3C SecPath F1000 Series PFC Card
NSQM1TG4FBA	H3C SecPath F1000 Series, 4 Ports SFP+ Module
NSQM1GP4FBA	H3C SecPath F1000 Series, 4 Ports SFP Module
NSQM1NIMTG6A	H3C SecPath F1000 Series 6-Port Ten-Gigabit Ethernet Optical Interface Module(SFP+)
Hard Disk	
NS-HDD-500G-SATA-SFF	H3C SecPath Series,500GB 2.5inch SATA HDD HardDisk Module
NS-HDD-1T-SATA-SFF	H3C SecPath Series,1TB 2.5inch SATA HDD HardDisk Module
NS-SSD-480G-SATA-SFF	H3C SecPath Series,480GB 2.5inch SATA SSD HardDisk Module
License	
LIS-F1000-IPS1-1Y	H3C SecPath F1000,IPS Signature Update Service,1 Year
LIS-F1000-IPS3-3Y	H3C SecPath F1000,IPS Signature Update Service,3 Years
LIS-F1000-AV-1Y	H3C SecPath F1000,AV Anti-Virus Security License,1 Year
LIS-F1000-AV-3Y	H3C SecPath F1000,AV Anti-Virus Security License,3 Years
LIS-F1000-ACG1-1Y	H3C SecPath F1000,Application Signature Update Service,1 Year
LIS-F1000-ACG3-3Y	H3C SecPath F1000,Application Signature Update Service,3 Years
LIS-F1000-LB	H3C SecPath F1000,SLB License, permanent authorization
LIS-F1000-SSL-25	H3C SecPath F1000,SSL VPN for 25 Users
LIS-F1000-SSL-125	H3C SecPath F1000,SSL VPN for 125 Users
LIS-F1000-SSL-500	H3C SecPath F1000,SSL VPN for 500 Users

LIS-F1000-SSL-1000	H3C SecPath F1000,SSL VPN for 1000 Users
LIS-F1000-URL-1Y	H3C SecPath F1000 URL Signature Update Service License,1 Year
LIS-F1000-URL-3Y	H3C SecPath F1000 URL Signature Update Service License,3 Years
LIS-IMC7-SVF1KA-25	H3C iMC-SSL VPN Authentication Client-F1000-25 License
LIS-IMC7-SVF1KB-125	H3C iMC-SSL VPN Authentication Client-F1000-125 License
LIS-IMC7-SVF1KC-500	H3C iMC-SSL VPN Authentication Client-F1000-500 License
LIS-IMC7-SVF1KD-1K	H3C iMC-SSL VPN Authentication Client-F1000-1000 License
LIS-F1000-WAF-1Y	H3C SecPath F1000 WAF Signature Update License,1 Year
LIS-F1000-WAF-3Y	H3C SecPath F1000 WAF Signature Update License,3 Year
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)
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

http://www.h3c.com