



H3C SecPath F1000

Series Firewalls

Next Generation Firewalls

Release Date: December, 2019



H3C SecPath F1000 Series Firewalls

Product overview

H3C SecPath F1000 series firewalls are next generation high-performance firewalls for small and medium enterprises, campus egress, and WAN branches.

H3C SecPath F1000 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 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.

The F1000 series is 1U high and provides a maximum of 24 Gigabit Ethernet ports and two 10-Gigabit Ethernet ports. It supports 1+1 power module redundancy and H3C's SCF (Security Converged Framework) virtualization technology.

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.



F1020/F1030/F1050/F1060 Front View



F1020/F1030/F1050/F1060 Rear View



F1070/F1080 Front View



F1070/F1080 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.
- **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 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

- **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)**—Supports identification and prevention of Web attacks, such as cross-site scripting (XSS) and SQL injection (SQLi).
- **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.

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	F1020	F1030/F1050/F1060	F1070/F1080
Dimensions (W × D × H)	440mm × 435mm × 44.2mm		
USB	2	2	2
Weight	6.75kg	7.3kg	8.5kg
Power Supply	2 AC fixed	2 AC fixed	Dual modular, AC or DC
Power consumption	79W	79W	116W
MTBF(Year)	102.6	98.6/102.6/52.1	76.6/72.1
Ports	1 × console port (CON) 8 × Gigabit Ethernet fiber ports 16 × Gigabit Ethernet copper ports	1 × console port (CON) 8 × Gigabit Ethernet fiber ports 16 × Gigabit Ethernet copper ports	1 × console port (CON) 8 × Gigabit Ethernet fiber ports 16 × Gigabit Ethernet copper ports 2 × 10-Gigabit Ethernet fiber ports
Expansion slots	1	2	2
Interface modules	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	4-port GE PFC interface module 4-port GE fiber interface module 4-port 10-GE fiber interface module
Storage	1 × 480G SSD/500G HDD	1 × 480G SSD/500G HDD/1T HDD	2 × 480G SSD/500G HDD/1T HDD
Flash	1GB	1GB	1GB
SDRAM	2GB	4G/4G/8G	8G/16G
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		

	<ul style="list-style-type: none"> 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 802.1Q VLAN transparent transmission
Antivirus	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> L2TP VPN IPSec VPN GRE VPN SSL VPN
IPv6	<ul style="list-style-type: none"> IPv6 status firewall



	<p>IPv6 attack protection</p> <p>IPv6 forwarding</p> <p>IPv6 protocols such as ICMPv6, PMTU, Ping6, DNS6, TraceRT6, Telnet6, DHCPv6 Client, and DHCPv6 Relay</p> <p>IPv6 routing: RIPng, OSPFv3, BGP4+, static routing, policy-based routing</p> <p>IPv6 multicast: PIM-SM, and PIM-DM</p> <p>IPv6 transition techniques: NAT-PT, IPv6 tunneling, NAT64 (DNS64), and DS-LITE</p> <p>IPv6 security: NAT-PT, IPv6 tunnel, IPv6 packet filter, RADIUS, IPv6 zone pair policies, IPv6 connection limit</p>
High availability	<p>SCF 2:1 virtualization</p> <p>Active/active and active/standby stateful failover</p> <p>Configuration synchronization of two firewalls</p> <p>IKE state synchronization in IPsec VPN</p> <p>VRRP</p>
Configuration management	<p>Configuration management at the CLI</p> <p>Remote management through Web</p> <p>Device management through H3C IMC SSM</p> <p>SNMPv3, compatible with SNMPv2 and SNMPv1</p> <p>Intelligent security policy</p>
Environmental protection	<p>EU RoHS compliance</p>
EMC	<p>FCC Part 15 (CFR 47) CLASS A</p> <p>ICES-003 CLASS A</p> <p>VCCI CLASS A</p> <p>CISPR 22 CLASS A</p> <p>EN 55022 CLASS A</p> <p>AS/NZS CISPR22 CLASS A</p> <p>CISPR 32 CLASS A</p> <p>EN 55032 CLASS A</p> <p>AS/NZS CISPR32 CLASS A</p> <p>CISPR 24</p> <p>EN 55024</p> <p>EN 61000-3-2</p> <p>EN 61000-3-3</p> <p>ETSI EN 300 386</p> <p>GB 9254</p> <p>GB 17625.1</p> <p>YD/T 993</p>
Safety	<p>UL 60950-1</p> <p>CAN/CSA C22.2 No 60950-1</p> <p>IEC 60950-1</p> <p>EN 60950-1</p> <p>AS/NZS 60950-1</p> <p>FDA 21 CFR Subchapter J</p>

GB 4943.1

Performance

	F1020	F1030	F1050	F1060	F1070	F1080
Firewall Throughput (1518Bytes)	1.5Gbps	2.5Gbps	4Gbps	5Gbps	8Gbps	10Gbps
NGFW Throughput	800Mbps	1.2Gbps	1.5Gbps	2Gbps	2.5Gbps	3Gbps
NGFW+IPS	800Mbps	1.2Gbps	1.5Gbps	2Gbps	2.5Gbps	3Gbps
NGFW+IPS+AV	700Mbps	1Gbps	1.2Gbps	1.8Gbps	2Gbps	2.5Gbps
Maximum concurrent sessions	1M	2.5M	3M	5M	5M	10M
Maximum New Connections per second	30K	40K	50K	80K	120K	150K
IPSec Throughput	600Mbps	800Mbps	800Mbps	1.2Gbps	1.5Gbps	1.5Gbps
Concurrent SSL-VPN Users	1K	1K	1K	2K	4K	6K

Ordering Information

SecPath F1000 Series	
NS-SecPath F1020	H3C SecPath F1020 Firewall, 16*10/100/1000BASE-T Ports,8*100/1000 BASE-X SFP Ports,1*Slot
NS-SecPath F1030	H3C SecPath F1030 Firewall,16*10/100/1000BASE-T Ports,8*100/1000 BASE-X SFP Ports,2*Slots
NS-SecPath F1050	H3C SecPath F1050 Firewall,16*10/100/1000BASE-T Ports,8*100/1000 BASE-X SFP Ports,2*Slots
NS-SecPath F1060	H3C SecPath F1060 Firewall, 16*10/100/1000BASE-T Ports,8*100/1000 BASE-X SFP Ports,2*Slots
NS-SecPath F1070	H3C SecPath F1070 Firewall, 16*10/100/1000BASE-T Ports,8*100/1000 BASE-X SFP Ports,2*10G/1G BASE-X SFP+ Ports,2*Slots
NS-SecPath F1080	H3C SecPath F1080 Firewall, 16*10/100/1000BASE-T Ports,8*100/1000 BASE-X SFP Ports,2*10G/1G BASE-X SFP+ Ports,2*Slots
Power Supply	
PSR150-A1-B	150W AC Power Supply
PSR150-D1-B	150W DC Power Supply
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
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,LB License
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
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)



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

Copyright ©2019 New H3C Technologies Co., Limited Reserves all rights

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>