H3C SecPath F100-C-A3 Next Generation Firewall

Release Date: May,2020

H3C Technologies Co., Limited

H3C SecPath F100-C-A3 Next Generation Firewall

Product Description

H3C SecPath F100-C-A3 firewall supports multi-dimensional integrated security protection, which can perform integrated security access control of IPS, AV, DLP and other traffic from multiple dimensions such as user, application, time, and quintuple;
F100-C-A3 supports multiple VPN services, such as L2TP VPN, GRE VPN, IPSec VPN and SSL VPN, etc.
F100-C-A3 can cooperate with intelligent terminals to realize mobile office, and provide rich routing capabilities, support RIP / OSPF / BGP / routing strategies and policy routing based on applications and URLs; support IPv4 / IPv6 security protection.
The H3C SecPath F100-C-A3 firewall uses dual power supplies (1 + 1 backup) that are mutually redundant and supports the SCF technology of dual-machine cluster deployment to fully meet the reliability requirements of high-performance networks;

H3C SecPath F100-C-A3 NGFW

Highlights

Advanced network security platform

- 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 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).

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	F100-C-A3
Dimensions (W × D × H)	330mm*230mm*43.6mm
USB	2
Power Supply	2 AC fixed
Ports	1 × console port (CON)
	8 × Gigabit Ethernet fiber ports
Temperature	Operating: 0°C to 45°C
	Storage: –30°C to +70°C
Operation modes	Route, transparent, and hybrid
AAA	Local authentication
	RADIUS authentication, support PAP and CHAP authentication
	HWTACACS certification
	AD / LDAP authentication
	PKI certificate 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
	802.1Q VLAN transparent transmission
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
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 IMC SSM
	SNMPv3, compatible with SNMPv2 and SNMPv1
	Intelligent security policy
Environmental protection	EU RoHS compliance

Performance

	F100-C-A3
Firewall Throughput (1518Bytes)	500Mbps
NGFW Throughput	300Mbps
NGFW+IPS	300Mbps
NGFW+IPS+AV	200Mbps
Maximum concurrent sessions	1M
Maximum New Connections per second	24K
Free SSL-VPN License	15
Concurrent SSL-VPN Users	1K

Ordering Information

Item	Quantity	Remarks
SecPath F100-C-A3	1	

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