H3C SecPath F100-C-A1 & F100-C-A2 Next Generation Firewalls

Product overview

H3C SecPath F100-C-A1 and F100-C-A2 firewalls are next-generation high-performance firewalls for small- and medium-size enterprises, campus network egress, and WAN branches to embrace the Web 2.0 era and follow the technology trend of deep security and network integration.

H3C SecPath F100-C-A1 and F100-C-A2 firewalls support 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-A1 and F100-C-A2 support multiple VPN services, such as L2TP VPN, GRE VPN, IPsec VPN, and SSL VPN. They can cooperate with intelligent endpoints to provide mobile office service, and provide rich routing capabilities, support RIP, OSPF, BGP, routing strategies, and policy routing based on applications and URLs. The firewalls also support IPv4/IPv6 security protection.

H3C SecPath F100-C-A1 firewall

H3C SecPath F100-C-A2 firewall

Features and benefits

High-performance software and hardware processing platform

F100-C-A1 and F100-C-A2 use advanced 64-bit multi-core high-performance processors and caches.

Carrier-level high availability

- Use H3C highly-available proprietary software and hardware platforms that have been proven by Telecom carriers and small- to medium-sized enterprises.
- Support H3C SCF, which can virtualize multiple devices into one device for unified resources management, 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.
- **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, 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 of Kaspersky to prevent, detect, and remove malicious code from network traffic.
- **Fast categorized filtering of URLs**—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 status 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**—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).

Wireless AC function：

- Maximum support for 64 APs, suggestion support for 16-32 APs. which could configure automatically and plug and play, Support unified management, configuration, and upgrade for wireless AP.
- Complete authentication technology for wireless terminals, support 802.1X/MAC/Portal authentication function

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.
- **In-service software upgrade (ISSU)**—Upgrades software with a minimum amount of downtime.
- **Log pagination**—Divides BLS, ATK, and CFGLOG files into five types of log files. The firewall supports backend log pagination, clearing, and specifying log parameters, pagination query, and configuring logs for an independent module.
- Cloudnet platform & APP management

Specifications

Item	F100-C-A1	F100-C-A2
Ports	5 × GE + 2 × SFP	10 × GE + 2 × SFP
Storage media	TF card with a maximum size of 500 GB	
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	SOP virtual firewall technology, which supports full virtualization of hardware resources, including CPU, memories, and storage 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,	

Item	F100-C-A1	F100-C-A2
	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/web page/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	

Item	F100-C-A1 F100-C-A2
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	Active/active and active/standby RBM 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-A1	F100-C-A2
Firewall Throughput(1518B)	1.2Gbps	1.2Gbps
Application layer throughput	600Mbps	600Mbps
IPS throughput	600Mbps	600Mbps
Threat Protection throughput	500Mbps	500Mbps
IPSec tunnel （site-to-site）	500	500
IPSec throughput(1400B)	150Mbps	250Mbps
SSL VPN users	500	500
SSL VPN throughput	80Mbps	100Mbps
Maximum concurrent sessions	900k	900k
Maximum New Connections per second	8,000	8,000

Ordering guide

Chassis

PID	Description
SecPath F100-C-A1-I	H3C SecPath F100-C-A1 Firewall Appliance
SecPath F100-C-A2-I	H3C SecPath F100-C-A2 Firewall Appliance

License

PID	Description
LIS-F100BAS-ACG-1Y	H3C SecPath F100-BAS Application Signature Update Service License,1 Year
LIS-F100BAS-ACG-3Y	H3C SecPath F100-BAS Application Signature Update Service License,3 Year
LIS-F100BAS-AV-1Y	H3C SecPath F100-BAS AV Anti-Virus Security Service License,1 Year
LIS-F100BAS-AV-3Y	H3C SecPath F100-BAS AV Anti-Virus Security Service License,3 Year
LIS-F100BAS-IPS-1Y	H3C SecPath F100-BAS IPS Signature Update Service License,1 Year
LIS-F100BAS-IPS-3Y	H3C SecPath F100-BAS IPS Signature Update Service License,3 Year
LIS-F100BAS-IPS/ACG-1Y	H3C SecPath F100-BAS IPS/ACG Signature Update Service License,1 Year
LIS-F100BAS-IPS/ACG-3Y	H3C SecPath F100-BAS IPS/ACG Signature Update Service License,3 Year
LIS-F100BAS-SSL-30	H3C SecPath F100BAS SSL VPN for 30 Users License
LIS-F100BAS-SSL-100	H3C SecPath F100BAS SSL VPN for 100 Users License
LIS-F100-BAS-TI-1Y	H3C SecPath F100-BAS Security Threat Update Service License,1 Year
LIS-F100-BAS-TI-3Y	H3C SecPath F100-BAS Security Threat Update Service License,3 Year
LIS-F100BAS-URL-1Y	H3C SecPath F100-BAS URL Signature Update Service License,1 Year
LIS-F100BAS-URL-3Y	H3C SecPath F100-BAS URL Signature Update Service License,3 Year
LIS-WX-1-BE	Enhanced Access Controller License,1 AP,for Verticals,for V7
LIS-WX-4-BE	Enhanced Access Controller License,4 AP,for Verticals,for V7
LIS-WX-8-BE	Enhanced Access Controller License,8 AP,for Verticals,for V7
LIS-WX-16-BE	Enhanced Access Controller License,16 AP,for Verticals,for V7

License Introduction

License	Feature	Before license installation	After license expiration	period
LIS-F100BAS-ACG	Application recognition (APR)	Updating APR signature library is not supported.	Updating APR signature library is not supported.	1 year 3 year
LIS-F100BAS-AV	Anti-virus	Anti-virus is not available and updating virus signature library is not supported.	Anti-virus is still available, but you cannot update the virus signature library or use the cloud query, enhanced inspection, and sandbox collaboration feature.	1 year 3 year
LIS-F100-BAS-TI	Threat intelligence (including IP reputation, URL reputation, and domain reputation)	Threat intelligence is not available and updating threat intelligence signature library is not supported.	Threat intelligence is still available, but updating threat intelligence signature library is not supported.	1 year 3 year
LIS-F100BAS-IPS	IPS	IPS is not available and updating IPS signature library is not supported.	IPS is still available, but updating IPS signature library is not supported.	1 year 3 year
LIS-F100BAS-SSL	SSL VPN	The system supports only the default maximum number of SSL VPN users.	N/A	Permanent
LIS-F100BAS-URL	URL filtering	URL cloud query is not available and updating URL signature library is not supported.	URL cloud query is not available and updating URL signature library is not supported.	1 year 3 year

New H3C Technologies Co., Limited

Hangzhou base
310 Liuhe Road, Zhijiang Science Park, Hangzhou, P.R.China
Zip: 310053
Tel: 0571-86760000
Fax: 0571-86760001
Version: 20150108-V1.0

http://www.h3c.com