Twoja Infrastruktura IT netf.pl

NETF, specjalizujemysię w sprzedaży zaawansowanej infrastruktury IT. Znajdą tu Państwo szeroki asortyment produktów od czołowych światowych producentów sprzętu i oprogramowania IT, w tym H3C, Huawei, Cisco, Juniper, Fortinet, a także Dell, IBM, CommVault i ESET. Dzięki współpracy z tymi renomowanymi partnerami, NETF zapewnia swoim klientom dostęp do najnowocześniejszych rozwiązań technologicznych.

Bezpieczeństwo,
Efektywność,
Optymalizacja

Grupa **NETF**, Netfront, Infopower, Agropower
Sukces poprzez profesjonalizm i doskonałość

H3C SecPath F5000-AI Firewall

Release Date: March, 2024

Overview

Nowadays, network attacks become increasingly complicated and fierce and occur with higher frequency and varieties of virus spread across the network, posing severe security risks on networks. H3C SecPath F5000-AI firewall series is designed to address these challenges and protect your network from increasingly sophisticated threats.

H3C SecPath F5000-AI firewall series includes the F5000-AI-15, F5000-AI-20, F5000-AI-40, F5000-AI120, F5000-AI160, F5000-AI360 models.

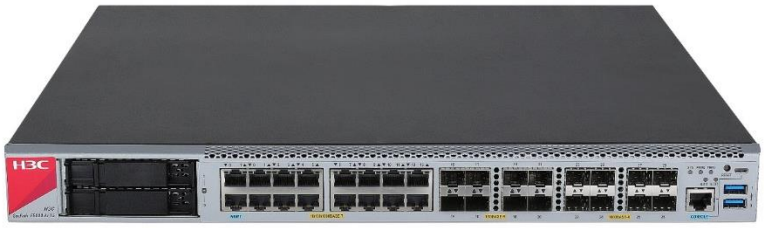
The F5000-AI-15, F5000-AI-20, and F5000-AI-40 firewalls are high-performance VPN-integrated 10G fixed-port firewalls intended for vertical markets. Designed with multicore processor hardware architecture, the F5000-AI-15 in a 1U footprint and F5000-AI-20 and F5000-AI-40 in a 2U footprint provide rich interfaces and great flexibility in interface expansion. As next-generation firewall products, they support large-size drives and can deliver abundant auditing functionalities.

The F5000-AI120/160/360 firewalls are 100G fixed-port firewalls intended for vertical and carrier markets. Designed with multicore processor hardware architecture, the F5000-AI-160 provides six 100G ports and provides twenty-eight 10-GE ports in a 1U footprint. They offer great flexibility in interface and drive expansion, provide rich security features and other advanced capabilities including IPS, AV, ACG, user-based security policy, encrypted traffic inspection, and interoperability with the cloud end, which brings them competitive advantage over their counterparts.

Beyond traditional firewall features such as access control, VPN, NAT, and DOS/DDOS attack defense, the firewall series is integrated with robust intrusion prevention features such as IPS, AV, application control, DLP, URL classification and filtering. This allows the firewall series to implement multi-dimensional security control based on users, applications, time ranges, geographic locations, and security status.

Incorporating AI computing power and technologies, the firewall series provides effective protection against unknown threats and APT attacks and simplifies O&M significantly.

The cutting-edge Comware 7 operating system running on the firewall series supports multi-device cluster building and 1:N virtualization, enabling the firewalls to scale resiliently to align with the cloud computing requirements.



H3C SecPath F5000-AI-15 firewall

H3C SecPath F5000-AI-20 firewall

H3C SecPath F5000-AI-40 firewall

H3C SecPath F5000-AI120 firewall

H3C SecPath F5000-AI160 firewall

H3C SecPath F5000-AI360 firewall

Features and Benefits

High-performance software and hardware platform

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

Carrier-level high availability

- Uses H3C highly-available 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 resource 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.

- **SOP 1:N virtualization**—Uses the container-based virtualization technology. An F5000-AI 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.

- **Application- and user-based access control**—Uses security policies with applications and users as basic elements in combination with deep security prevention to deliver next-generation 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. The firewall 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. 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.
- Realtime 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, 141 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, so the signature database is always precise and up to date.

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**—Uses the link state inspection and link busy detection technologies, and applies to a network egress to balance traffic among links.
- **Server load balancing**—Distributes network services to multiple servers for processing by using traffic distribution methods, support rich scheduling algorithms to distribute requests, e.g., random distribution algorithm, hash algorithm, weighted least connection algorithm, round-robin algorithm, weighted least connections algorithm etc.
- **Integrated SSL VPN**—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)**—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)**—The firewall supports Web attack identification and protection, such as cross-site scripting attacks and SQL injection attacks.
- **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)**—Identifies and protects against CC attacks effectively, and classifies network devices, Web servers, and databases based on their characteristics.

Intelligent management

- Intelligent security policy management, which detects duplicate policies, optimizes policy matching rules, and detects and recommends 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.
- 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 syslogs and binary stream logs) in the same format, and compress and store 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, 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.

Technical Specifications

Item	F5000-AI-15	F5000-AI-20	F5000-AI-40
Ports	1 × console port 2 × MGMT(RJ45) 2 × USB ports 14 × GE copper ports 8 × GE fiber ports 8 × 10-GE fiber ports	1 × console port 1 × MGMT(RJ45) 2 × USB ports 4 × GE combo interfaces	1 × console port 1 × MGMT(RJ45) 2 × USB ports 4 × GE combo interfaces
Interface modules (provided)	N/A	One interface module with eight GE copper ports One interface module with eight 10-GE fiber ports	One interface module with eight GE copper ports One interface module with eight GE fiber ports One interface module with eight 10-GE fiber ports
Expansion slots	2	6	5
Storage media	Drives	Drives	Drives
Ambient temperature	Operating without drives: 0°C to 45°C (32°F to 113°F) Operating with drives: 5°C to 40°C (41°F to 104°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.		

Item	F5000-AI-15	F5000-AI-20	F5000-AI-40
	CHAP authentication. PAP authentication.		
Firewall	Virtual firewall technology, fully virtualized allocation of hardware resources including CPU, memory, and storage. Security zone. 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. Dynamic packet filtering. 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, and DoS/DDoS attacks. Prevention against buffer overflow, SQL injection, and IDS/IPS bypass attacks. 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		

Item	F5000-AI-15	F5000-AI-20	F5000-AI-40
	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 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		
Environmental compliance	EU RoHS directive.		

Item	F5000-AI120	F5000-AI160	F5000-AI360
Ports	1 × console port 1 × MGMT(RJ45) 2 × USB ports 6 × QSPF+(100G/40G) 8 × SPF28(25G/10G) 20 × SPF+(10G/1G) 2 × HA (10G)	1 × console port 1 × MGMT(RJ45) 2 × USB ports 6 × QSPF+(100G/40G) 8 × SPF28(25G/10G) 20 × SPF+(10G/1G) 2 × HA (10G)	1 × console port 1 × MGMT(RJ45) 2 × USB ports 6 × QSPF+(100G/40G) 16 × SPF28(25G/10G) 12 × SPF+(10G/1G) 2 × HA (10G)
Storage media	Support for 2 × 960 GB SSDs		
Ambient temperature	Operating without drives: 0°C to 45°C (32°F to 113°F) Operating with drives: 5°C to 40°C (41°F to 104°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 technology, fully virtualized allocation of hardware resources including CPU, memory, and storage. Security zone. 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. Dynamic packet filtering. 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		

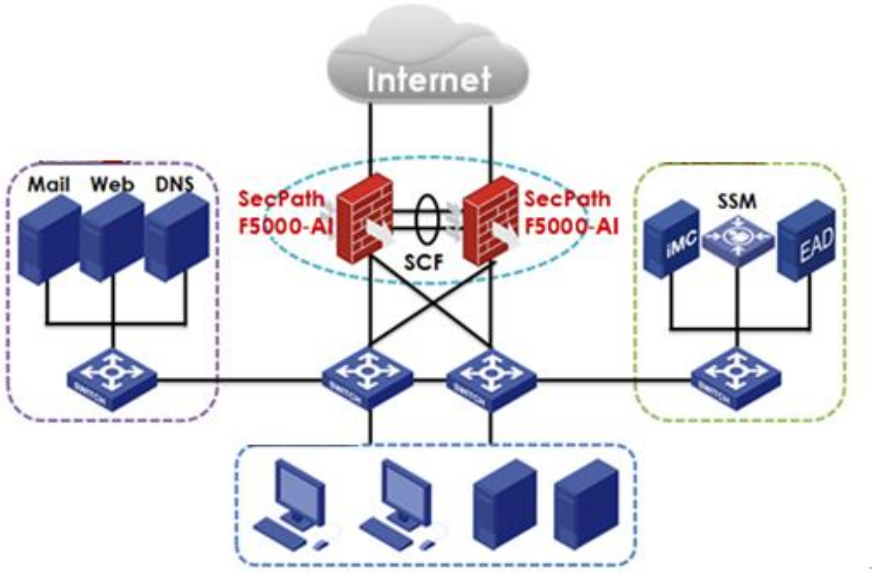
Item	F5000-AI120	F5000-AI160	F5000-AI360
	Virus types include Backdoor, Email-Worm, IM-Worm, P2P-Worm, Trojan, AdWare, and Virus. Virus logs and reports.		
Deep packet prevention	Prevention against command attacks such as hacker, worm/virus, Trojan, malicious code, spyware/adware, and DoS/DDoS attacks Prevention against buffer overflow, SQL injection, and IDS/IPS bypass attacks. 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.		

Item	F5000-AI120	F5000-AI160	F5000-AI360
	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		
Environmental compliance	EU RoHS directive.		

Performance

Items	F5000-AI-15	F5000-AI-20	F5000-AI-40	F5000-AI120	F5000-AI160	F5000-AI360
Firewall throughput	25Gbps	30Gbps	45Gbps	120Gbps	200Gbps	320Gbps
NGFW throughput (APR)	20Gbps	30Gbps	40Gbps	50Gbps	50Gbps	100Gbps
NGFW throughput (IPS+ APR)	14Gbps	18Gbps	20Gbps	30Gbps	35Gbps	45Gbps
NGFW throughput (IPS+AV+ APR)	14Gbps	18Gbps	20Gbps	25Gbps	35Gbps	40Gbps
Concurrent sessions	10M	16M	40M	40M	80M	100M
New sessions per second	300k	500k	600k	600k	700k	1M
SSL VPN concurrent users	10k	30k	30k	24k	48k	50k
SSL VPN throughput	1.8Gbps	2.5Gbps	2.5Gbps	2.5Gbps	2.5Gbps	2.5Gbps
IPSec VPN tunnels	8k	20k	24k	12k	24k	24k
IPSec throughput	5.5Gbps	16Gbps	16Gbps	40Gbps	45Gbps	50Gbps
Security policy	50k	50k	50k	120k	120k	120k

Application Scenarios



H3C SecPath F5000-AI series application scenario

- SCF 2:1 virtualization and reliable network design
- Powerful processing capabilities, and GE and 10-GE connections
- Powerful VPN encryption capabilities
- Excellent attack protection capabilities
- Email, webpage, and file filtering
- Abundant routing protocols, implementing integration of security and network

Ordering Information

PID	Description
Chassis	
NS-SecPath F5000-AI-15	H3C SecPath F5000-AI-15 Firewall Appliance
NS-SecPath F5000-AI-20	H3C SecPath F5000-AI-20 Firewall Appliance
NS-SecPath F5000-AI-40	H3C SecPath F5000-AI-40 Firewall Appliance
NS-SecPath F5000-AI120	H3C SecPath F5000-AI120 Firewall Appliance
NS-SecPath F5000-AI160	H3C SecPath F5000-AI160 Firewall Appliance

NS-SecPath F5000-AI360	H3C SecPath F5000-AI360 Firewall Appliance
Interface module	
NSQM1GT4PFC	4-port PFC interface module
NSQM1GP4FBA	4-port SFP interface module
NS-NIM-TG6A	6-port SFP+ interface module
NSQM1TG8A	8-port SFP+ interface module
NSQM1QG2A	2-port QSFP+ interface module
NSQM1GT8A	8-port GE interface module
NSQM1GP8A	8-port SFP interface module
NSQM1GT4PFCA	4-port PFC interface module
NSQM1G4XS4	4-port SFP and 4-port SFP+ interface module
Fan	
FAN-20F-2-A	Fan tray module (power to port airflow)
FAN-20B-2-A	Fan tray module (port to power airflow)
Power	
PSR250-12A1	250W AC power supply
PSR450-12D	450W DC power supply
PSR450-12AHD	450W HVDC power supply
PSR650B-12D1-A	650W DC power supply
PSR650B-12A1-A	650W AC power supply

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