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

H3C SecPath Series

F5000 Firewalls

Next Generation Firewall

Release Date: May, 2022

Overview

H3C SecPath firewall F5000 series is a new generation of high-performance security gateways for large-scale enterprise campus networks, service providers, and data centers.

The F50X0 firewall 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 content security. Typical security protection features include IPS, AV, and DLP.
- VPN services, including IPsec VPN, SSL VPN, L2TP VPN, GRE VPN, and ADVPN.
- 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 firewall series uses one AC or DC power supply, or two power supplies of the same type for power redundancy. It is 2U high and provides high-density GE and 10GE port access capabilities. It supports stateful failover to meet high availability requirements in high performance networks. The F5030/60/80 and the F5030-D/60-D/80-D with two MPUs provide replaceable fan trays that support front-to-rear aisles to meet data center requirements.

F5030/F5060/F5080

F5030-D/F5060-D/F5080-D

Features and Benefits

High-performance software and hardware platforms

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

Carrier-level high availability

- Uses H3C high 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 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 F50X0 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.
- **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, PAP, and LDAP.
- **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 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, 139 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 feature. This feature uses the link state inspection and link busy detection technologies, and applies to a network egress to balance traffic among links.
- Integrated SSL VPN feature. This feature can use 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 6 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.

Intelligent management

- Intelligent and unified security policy management, which 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.

- 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 syslog 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.

Service chain

Service chain is a forwarding technology used to guide network traffic through service nodes. It is based on the Overlay technology and combines the software defined network (SDN) centralized management theory. You can configure service chains by using a virtual converged framework controller (VCFC).

Service chain implements the following functions:

- Decoupling the tenant logical network and the physical network, and separating the control plane from the forwarding plane.
- Service resource allocation and deployment on demand with no physical topology restrictions.
- Dynamic creation and automatic deployment of network function virtualization (NFV) resource pools.
- Tenant-specific service arrangement and modification without affecting the physical topology and other tenants.

Technical Specifications

Item	F5030/F5030-D	F5060/F5080/F5060-D/F5080-D
Ports	4 × Gigabit combo interfaces 8 × Gigabit Ethernet copper ports 8 × 10-Gigabit Ethernet ports	4 × Gigabit combo interfaces 8 × Gigabit copper ports 8 × Gigabit fiber ports 8 × 10-Gigabit Ethernet ports
Expansion slots	6/5	5/5/4/4
Storage media	2 × 480G SSD drives (optional)	
Ambient temperature	Operating: 0°C to 45°C (32°F to 113°F) Non operating: –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. 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, 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.	
Load balancing	Link and server load balancing. Application- and ISP-based Intelligent route selection. Health monitoring through ICMP, UDP, and TCP. Port-, HTTP-, and SSL-based sticky methods to implement busy bandwidth and fault protection.	

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 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
Behavior and content audit	User-based content audit and tracking.
File filtering	Identification of file types such as Word, Excel, PPT, PDF, ZIP, RAR, EXE, DLL, AVI, and MP4, and filtering of sensitive information in the files.
URL filtering	Over 50 types of signature-based URL filtering rules, and discarding, reset, redirection, logging, and blacklisting of packets matching the rules.
Application identification and control	Identification of various types of applications, and access control based on specific functions of an application. Combination of application identification and intrusion prevention, antivirus, and content filtering, improving detection performance and accuracy.
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.

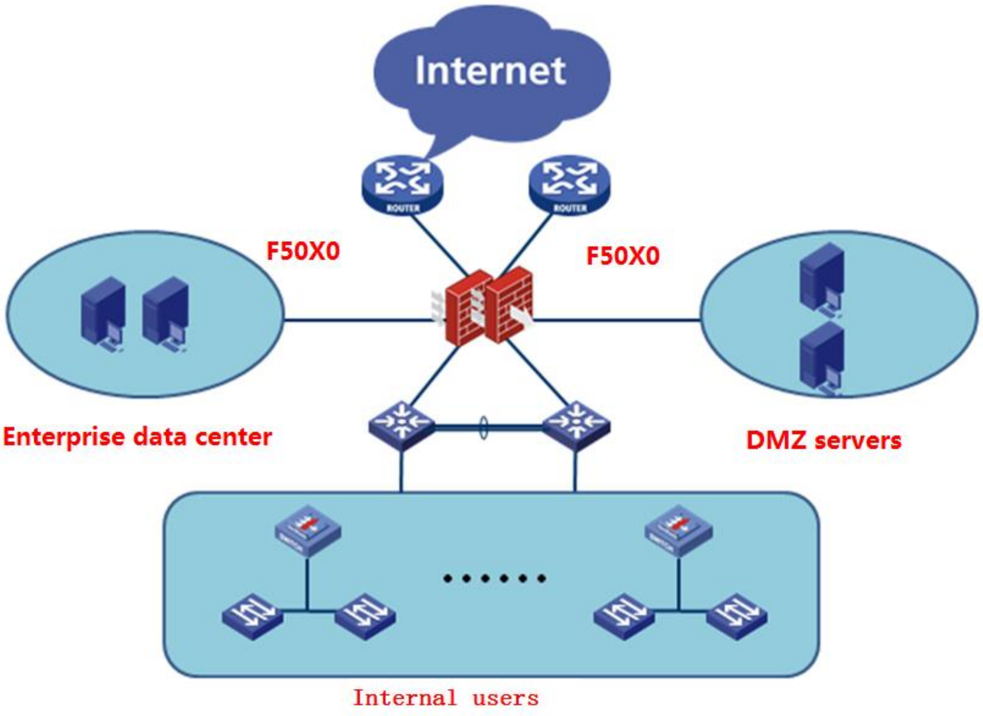
	NAT ALGs for NAT ALG, including DNS, FTP, H.323, ILS, MSN, NBT, PPTP, and SIP.
VPN	L2TP VPN. IPsec VPN. GRE VPN. SSL VPN. SM1 hardware encryption algorithm, SM2, SM3, and SM4 encryption algorithms.
Routing	Routing protocols such as RIP, OSPF, BGP, and IS-IS.
VXLAN	VXLAN service chain.
IPv6	IPv6 status 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. Built-in bypass module. External bypass host.
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

Performance

Items	F5030/ F5030-D	F5060/ F5060-D	F5080/ F5080-D
L4 FW throughput	40Gbps	50Gbps	80Gbps
NGFW throughput (APR)	20Gbps	20Gbps	20Gbps
NGFW throughput (IPS+ APR)	18Gbps	18Gbps	18Gbps

NGFW throughput (IPS+AV+ APR)	18Gbps	18Gbps	18Gbps
Concurrent sessions	16M	40M	80M
New sessions per second	500k	600k	600k
SSL VPN concurrent users	30k/20k	30k/20k	30k/20k
SSL VPN throughput	2.8Gbps	3.5Gbps	4.6Gbps
IPSec VPN tunnels	20k/25k	24k/25k	50k/25k
IPSec throughput	16Gbps	16Gbps	17Gbps
Security policy	50k	50k	50k

Application Scenarios



H3C SecPath F5000 series application scenario

- SCF N:1 virtualization and reliable network design
- Powerful processing capabilities
- Powerful VPN encryption capabilities
- Excellent attack protection capabilities
- Email, webpage, and file filtering

- Abundant routing protocols, implementing integration of security and network

Ordering Guide

Chassis

Item	Quantity	Remarks
H3C SecPath F5030	1	Required
H3C SecPath F5030-D	1	Required
H3C SecPath F5060	1	Required
H3C SecPath F5060-D	1	Required
H3C SecPath F5080	1	Required
H3C SecPath F5080-D	1	Required

Interface modules

Item	Description	Remarks
NSQM1GT8A	8-port GE copper interface module	Optional for F5030/60/80 and F5030-D/60-D/80-D (with two MPUs)
NSQM1GP8A	8-port GE fiber interface module	Optional for F5030/60/80 and F5030-D/60-D/80-D (with two MPUs)
NSQM1GT4PFCA	4-port PFC interface module	Optional for F5030/60/80 and F5030-D/60-D/80-D (with two MPUs)
NSQM1TG8A	8-port SFP+ fiber transceiver module	Optional for F5030/60/80 and F5030-D/60-D/80-D (with two MPUs)
NSQM1QG2A	2-port QSFP+ fiber transceiver module	Optional for F5030/60/80 and F5030-D/60-D/80-D (with two MPUs)
NSQM1G4XS4	4-port SFP and 4-port SFP+ fiber transceiver module	Optional for F5030/60/80 and F5030-D/60-D/80-D (with two MPUs)

Drive

Item	Description	Remarks
Drive	480G drive	Optional for F5030/60/80 and F5030-D/60-D/80-D (with two MPUs)

Fan trays

Item	Description	Remarks
LSWM1BFANSCB	Power supply side	Optional for F5030/60/80 and F5030-D/60-D/80-D (with two MPUs) Two fan trays are required, and they must be the same model.
LSWM1BFANSC	Port side	Optional for F5030/60/80 and F5030-D/60-D/80-D (with two MPUs) Two fan trays are required, and they must be the same model.

Power supplies

Item	Description	Remarks
LSVM1AC650	650W AC power supply	Optional for F5030/60/80 and F5030-D/60-D/80-D (with two MPUs) A minimum of one is required. You can install one AC or DC power supply, or install two AC power supplies or two DC power supplies for redundancy.
LSVM1DC650	650W DC power supply	Optional for F5030/60/80 and F5030-D/60-D/80-D (with two MPUs) A minimum of one is required. You can install one AC or DC power supply, or install two AC power supplies or two DC power supplies for redundancy.

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

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.