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 M9000-X Series Multi-Service Security Gateway

Product description

H3C SecPath M9000-X series multi-service security gateway is H3C Technology Co., Ltd. (hereinafter referred to as H3C company) in combination with the development trend of cloud computing, 5G, Internet of Things, IPv6, big data and high-performance computing. A new generation of high-performance multi-service security gateway launched for commercial core network , large enterprise and campus network egress market.

H3C SecPath M9000-X has the highest firewall throughput performance of M9000 series products, and fully supports traffic content audit, encrypted application identification, attack defense, abnormal traffic cleaning, unknown threat detection, server abnormal outreach detection, sensitive data protection, and web application security Functions such as protection, access control, security domain division, blacklist, traffic monitoring, email filtering, web page filtering, and application layer filtering can effectively ensure network security; in-depth business security detection can provide more detailed protection for web servers. Adopt ASPF (Application Specific Packet Filter) application state detection technology, which can detect the connection state process and abnormal commands; support a variety of VPN services, such as L2TP VPN, GRE VPN, IPSec VPN, SSL VPN, MPLS VPN, etc., to meet a variety of High-performance VPN access requirements; support the most abundant NAT features in the industry to meet the NAT needs of major operators; provide rich routing capabilities, support static routing, RIP/OSPF/BGP/ISIS routing strategies and policy routing; fully support IPv4/IPv6 dual protocol stack.

H3C SecPath M9000-X series multi-service security gateway fully considers the high reliability requirements of network applications, adopts a leading multi-core fully distributed architecture, and the module is separated and pluggable design, which is convenient for flexible networking and expansion. The main control engine is 1+1 redundant, which provides unified configuration management of the whole machine and supports secure clustering; service engines and interface units support mixed insertion, and can be flexibly selected according to performance requirements; fan modules are redundant, and the fan frame supports fan status monitoring. Supports stepless speed regulation, and can automatically group speed regulation according to the ambient temperature and single board configuration; power module M+N backup, AC and DC power modules support hot swap, multi-power module load sharing, and can flexibly configure modules according to system power consumption Quantity, to ensure that the module works efficiently. All units of the equipment support hot swap, which fully meets the needs of network maintenance, upgrade and optimization.

M9000-X06

M9000-X10

Features

High-performance hardware and software processing platform

- Adopting a fully distributed architecture that separates control, business, and data, the hardware of the control engine, switching engine, business engine, and interface unit is separated, decoupling the key components of the system, and improving system reliability; the independent hardware switching engine supports high-performance security Business non-blocking processing and forwarding
- Independent high-performance control engine to realize unified system configuration management and secure cluster
- The security service engine adopts the latest multi-core high-performance processor, and the high-speed processing security service performance of a single board is the highest in the industry; a hardware board can simultaneously provide L2 - L7 comprehensive security defense, including firewall, NAT , LB , IPS , AV, ACG , VPN , etc.;
- The built-in modular software system supports multi-process scheduling, and the running space between processes is isolated . The abnormality of a single process will not affect other parts of the system , which improves system reliability ; supports authority management functions, based on features, command lines, system resources, and WEB management Equal levels define user read and write permissions, improve system security; support hot patch, support ISSU , realize system upgrade without interrupting business, and improve system usability

Carrier-grade equipment with high reliability

- Adopt the software and hardware platform with independent intellectual property rights owned by H3C. Product applications have gone through years of market tests from large and medium-sized enterprise users to major telecom operators
- Support RBM (remote hot backup technology) 1:1 hot backup function, support Active/Active and Active/Passive and other working modes, realize load sharing and business backup

Powerful security protection function

- Supports rich attack defense functions including: Land , Smurf , UDP Snork attack, UDP Chargen DoS attack (Fraggle), Large ICMP Traffic , Ping of Death , Tiny Fragment , Tear Drop , IP Spoofing , IP fragmentation packets, ARP spoofing, ARP active reverse query, TCP packet flag bit illegal, oversized ICMP packets, address scanning, port scanning and other attack defenses, including SYN Flood , Detection and defense of common DDoS attacks such as UPD Flood , ICMP Flood , DNS Flood, and CC .
- Supports unified management The host + multi-service engine is always managed as a network element in a unified manner, and there is no need to plan the IP address of each card, which saves the user's IP address and greatly reduces the complexity of deployment, and can realize comprehensive management of the equipment. Configuration management, performance monitoring and log auditing.
- Support intelligent flow distribution (IFF) After deploying multi-service cards, traffic is automatically load-shared among multiple service cards to achieve distributed processing.
- divide security zones based on interfaces and VLANs
- Supports packet filtering By using standard or extended access control rules between security zones, data packets can be filtered with the help of information such as UDP or TCP ports in the message, and it supports filtering according to time periods
- Supports authentication, authorization and accounting (AAA) services including: authentication based on RADIUS/HWTACACS+ / LDAP(AD) , CHAP , PAP , etc.
- Support static and dynamic blacklist
- Support static NAT, source address NAT, destination address NAT
- Support static and dynamic carrier CGN NAT
- Support P2P traversal technologies such as Fullcone and Hairpin
- Support VPN functions include: support L2TP, manual/automatic IPSec , GRE , MPLS VPN, etc.
- Support rich routing protocols Support IPv4, IPv6 static routing, equal-cost routing, policy routing, and dynamic IPv4 routing protocols such as BGP, RIPv2, OSPF , ISIS, etc., support dynamic IPv6 routing protocols such as BGP4+ , OSPFv3 , ISISV6
- Support security log Support operation log, inter-domain policy matching log, attack defense log; support DS-LITE log; support NAT444 log, support telecom, China Unicom, mobile format;
- Support traffic monitoring statistics and management.

Flexible and scalable integrated deep security

- The in-depth WEB security protection is not limited to the conventional IPS/AV protection. It provides detailed web application protection for intranet servers. For the most troublesome CC attacks on servers, abnormal outreach, SQL injection, HTTP slow attacks, cross- Common attacks such as website scripts, content detection and verification of various requests from web application clients to ensure their security and legality, real-time blocking of illegal requests, and effective protection of various websites.
- Unknown threat detection relying solely on feature analysis is no longer sufficient to deal with complex network

environments. In the face of typical APT (Advanced Persistent Threat, advanced persistent threat) attack sandbox technology is one of the most effective methods to defend against APT attacks. It is used to construct Isolated threat detection environment. The H3C Security Gateway sends network traffic to the sandbox for isolation and analysis, and the sandbox draws a conclusion on whether there is a threat. If a traffic is detected as malicious, the device will block the traffic.

- Terminal identification, shared management Terminal identification is an important prerequisite for establishing a secure connection to the Internet of Things, and is used to identify terminals in the Internet of Things. When terminal traffic flows through the device, the H3C Security Gateway can analyze and extract terminal information, such as the manufacturer and model of the terminal, and supports sending The user sends the log, prompting the user. At the same time, the application detection method and IPID detection method are used to identify and manage the behavior of sharing the Internet through NAT technology or proxy technology.
- Server abnormal outreach detection Server outreach protection is a protection mechanism for intranet servers, which can effectively identify active outreach behaviors of servers, formulate corresponding outreach protection strategies to identify abnormal messages, and output alarm information for management staff for further processing. It provides a basis for the administrator to check the server, thereby preventing the server from becoming a part of the botnet, launching external attacks or infiltrating internally.
- The high-precision and high-efficiency intrusion detection engine adopts the FIRST (Full Inspection with Rigorous State Test, comprehensive detection based on accurate state) engine with independent intellectual property rights of H3C. The FIRST engine integrates a number of detection technologies, realizes comprehensive detection based on accurate status, and has extremely high intrusion detection accuracy; at the same time, the FIRST engine adopts parallel detection technology, and the software and hardware can be flexibly adapted, which greatly improves the performance of intrusion detection. efficiency.
- Real-time virus protection flow engine virus checking technology, so as to quickly and accurately kill viruses and other malicious codes in network traffic .
- Comprehensive and timely security signature database Through years of operation and accumulation, H3C has a senior attack signature database team in the industry, and is equipped with a professional attack and defense laboratory to keep up with the latest developments in the field of network security, thereby ensuring timely and accurate update of the signature database .

Industry-leading IPv6

- Support IPv6 basic protocols Support TCP6, UDP6, RAWIP6, ICMPV6, PPPoEv6, DHCPV6 Server, DHCPv6 Client, DHCPV6 Relay, DNSv6, RADIUS6 and other protocols; support IPv6 routing protocols. Support static routing, BGP4+ \O SPFv3 \ ISISV6 routing policy and policy routing; support IPv6 ASPF.
- Support IPV6 attack defense. Support IPv6 Multicast.
- Various IPv6 transition technologies are supported, including NAT-PT, IPv6 Over IPv4 GRE tunnel, manual tunnel, 6to4 tunnel, IPv4 compatible IPv6 automatic tunnel, ISATAP tunnel, NAT444, DS-Lite, etc.

Next-generation multi-service features

- Integrated link load balancing feature, through link status detection, link busy protection and other technologies, effectively realize multi-link automatic balancing and automatic switching of enterprise Internet egress.
- Integrate SSL VPN features to meet the security access requirements of mobile office and employee business trips. It can

not only combine USB-Key and SMS for mobile user identity authentication, but also combine with the original authentication system of the enterprise to realize an integrated authentication interface. enter.

- DLP basic function support, support email filtering, provide SMTP email address, title, attachment and content filtering; support web page filtering, provide HTTP URL and content filtering; support file filtering of network transmission protocols; support application layer filtering, provide Java / ActiveX Blocking and SQL injection attack prevention.

Professional intelligent management

- Self-inspection operation and maintenance, policy risk tuning Through redundancy and hit analysis of security policies, redundant and missing security policies are identified to help administrators conduct in-depth analysis and processing of security policies on devices. At the same time, the application layer detection engine intelligently analyzes the potential risks in the traffic allowed by the security policy, and conducts an overall assessment of the safety factor of all security policies in the device.
- Supports standard network management SNMPv3, and is compatible with SNMP v1 and v2. Device management and security service configuration can be performed through the command line interface, meeting the needs of professional management and mass configuration
- Support packet capture based on interface and IP. Generate the captured packets with a .cap suffix file that can be recognized by Wireshark (a network packet analysis software), and save them to the local or external server for users to analyze and diagnose the traffic entering and exiting the device.
- Support the packet loss statistics function to analyze and record the detailed reasons for discarding packets in the forwarding process of the device and security business modules (such as: attack defense, session management, and connection limit, etc.)
- Support webpage diagnosis function When the intranet user accesses the webpage and there is a failure, the basic diagnosis of the network is carried out, and the cause of the failure is given.
- Support message trace function Support real flow, import message, construct message, etc., used to analyze and track each security business module in the device (such as: attack defense, uRPF, session management and connection limit, etc.) By viewing the detailed information of the packet trace records, it is helpful for the administrator to quickly troubleshoot and locate network faults.
- Graphical interface, providing easy-to-use web management
- Through H3C's self-developed management system, unified management is realized, which integrates functions such as security information and event collection, analysis, and response, and solves the problems of isolation of network and security devices, unintuitive network security status, slow response to security incidents, and difficulties in network fault location and other issues, so that IT and security administrators can get rid of tedious management work, can concentrate on core business, and greatly improve work efficiency
- normalizes logs in different formats (Syslog , binary flow logs, etc.). At the same time, high aggregation compression technology is used to store massive events, and log files can be automatically compressed, encrypted and saved to external storage systems such as DAS , NAS or SAN to avoid loss of important security events
- Provides rich reports, mainly including application-based reports, network flow-based analysis reports, etc.
- through the web interface, and the customized content includes the time range of the data, the source device of the data, the generation cycle and the output type, etc.

product specification

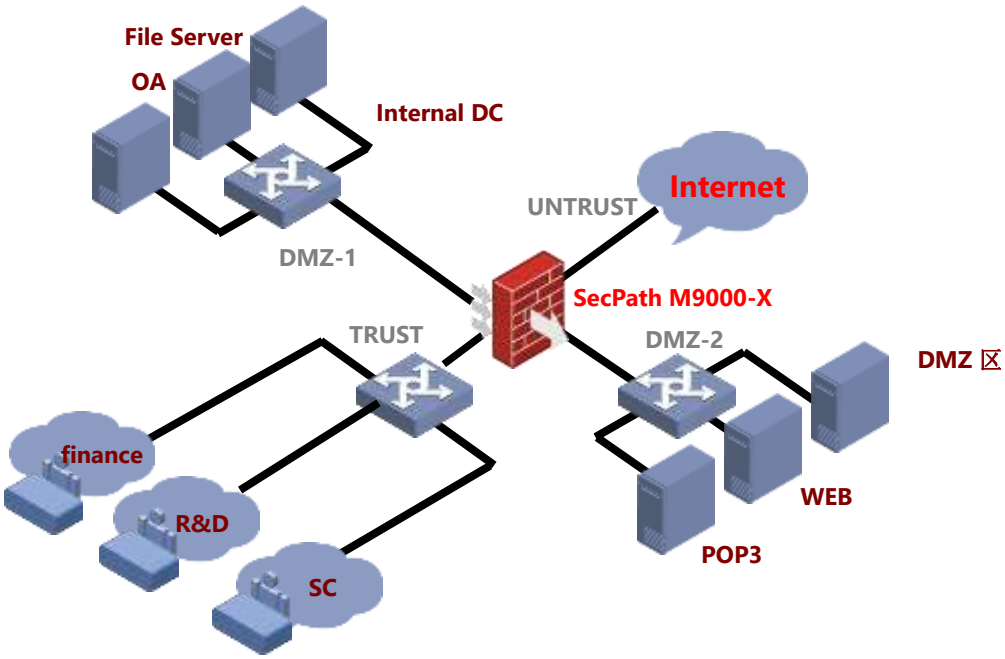
Attributes	M9000-X06	M9000-X10
Number of slots on the main control board	2	2
Number of service board slots	8	16
Number of slots on the SFU	4	4
redundant design	Main control, SFU, power supply, fan	Main control, SFU, power supply, fan
Dimensions (WXHXD)	440mm×264mm×857mm (6RU)	440mm×530mm×857mm (12 RU)
weight (kg)	< 120 kg	< 220 kg
Total power consumption (W)	<2252W	<3360W
ambient temperature	0 ～40 ℃ Non-working: -40～70℃	
operating mode	Routing mode, transparent mode, bridge mode	
AAA service	Portal authentication, RADIUS authentication, HWTACACS authentication, PKI/CA (X.509 format) authentication, domain authentication Support manual key, IKEv2, redundant VPN gateway, EAP authentication, IKEv2 redirection	
Multi-service security gateway	Virtual Multi-Service Security Gateway Security area division Can defend against Land, Smurf, Fraggle, Ping of Death, Tear Drop, IP Spoofing, IP Fragmentation, ARP spoofing, ARP active reverse query, TCP message flag bit illegal oversized ICMP message, address scanning, port scanning , SYN Flood, UPD Flood, ICMP Flood, DNS Flood and other malicious attacks Dynamic packet filtering, ASPF application layer packet filtering Static and dynamic blacklist functions MAC and IP binding function MAC-based access control list ICMPv6, DHCPv6 Support 802.1q VLAN transparent transmission MLD, ND	
security strategy	Access control lists based on domain name (domain name group), service, user, application, time period, etc. Supports strategic risk classification and application risk tuning Policies can be fuzzily queried to retrieve redundant and no-hit policies Supports policy grouping, and can be connected to third-party platforms through the NETCONF interface to create, delete, modify, and move policies Security monitoring based on state legitimacy Support access control based on black and white lists, and support one-click	

Attributes	M9000-X06	M9000-X10
	setting of black and white lists based on alarms	
routing function	Support static routing Support dynamic routing: RIP, OSPF, BGP, ISIS and other routing protocols Support policy routing based on source/destination IP, source/destination port, service, application type, user and user group, outbound/incoming interface, link state, etc.	
virus protection	Supports virus feature detection and protection based on IPV4 and IPV6 dual stacks, and can detect email viruses, web application viruses, common file viruses, Trojan horses, worms, malicious web pages, compressed data, packers and compressed packages (zip, gzip , tar) virus killing Support manual and automatic upgrade of virus database, support manual import of signature database Support cloud virus database Packet Flow Processing Mode Support HTTP, FTP, SMTP, POP3 protocol Supported virus types: Backdoor, Email-Worm, IM-Worm, P2P-Worm, Trojan, AD-Ware, Virus, etc. Support virus logs and reports	
web security protection	Support web security detection Support CC attack protection Supports server abnormal outreach detection, and can customize learning parameters Support web page hanging horse, Trojan horse, and other attack protection password and password brute force cracking detection and protection for common web services (including HTTP, FTP, SSH, SMTP, IMAP , etc.) , common database software (MySQL, Oracle, MSSQL)	
Deep Security	Supports defense against hacker attacks, worms/viruses, Trojan horses, malicious codes, spyware/adware, etc., can subdivide strategies and formulate intrusion defense templates according to different scenarios Supports Flood attacks at the application layer (HTTP, HTTPS, DNS, FTP, SIP, etc.), can set the learning time and threshold through machine self-learning, and automatically generate DDoS prevention strategies based on the results Support buffer overflow, SQL injection, IDS/IPS escape and other attack defense Support the classification of attack signature database (classification according to attack type and target machine system), grading (divided into four levels: high, medium, low, and prompt) Support manual and automatic upgrade of attack signature database (TFTP and HTTP) Support P2P/IM identification and control such as BT Support URL identification, support malicious URL blocking, and can connect with cloud URL server to expand the number of URL address databases For unknown threat attacks, support local and cloud sandbox docking to detect APT attacks in real time Supports docking and management with the unified security management platform, which facilitates the security situation protection of the entire network	
Encrypted traffic protection	Supports HTTPS proxy and ssl offloading, and can perform content detection and filtering, auditing, and attack protection on decrypted HTTPS encrypted traffic.	

Attributes	M9000-X06	M9000-X10
	It can finely classify and decrypt URLs to improve the protection effect	
Mail / Web/Application Layer Filtering	email filtering SMTP email address filtering email header filtering Email Content Filtering Email attachment filtering web filtering HTTP URL filtering HTTP content filtering Application Layer Filtering Java Blocking ActiveX Blocking Defense against SQL injection attacks	
Smart Bandwidth Control	Supports bandwidth guarantee based on user, IP, interface, and service, supports traffic shaping, and supports maximum/minimum flow and connection speed limit management for each IP and user It can support setting flow control policies based on application layer protocols, and can set maximum/minimum bandwidth, guaranteed bandwidth, protocol traffic priority, etc., and supports eight-level control	
load balancing	Support application layer link load balancing based on HTTP and HTTPS Support DNS transparent proxy, support DNS filtering, support intelligent DNS Support server load balancing Support global load Support link health status detection Support intelligent link selection	
NAT	Support multiple internal addresses mapped to the same public network address Support mapping of multiple internal addresses to multiple public network addresses Support one-to-one mapping from internal addresses to public network addresses Support port multiplexing technology, which can increase the upper limit of NAT conversion Supports simultaneous translation of source and destination addresses, real-time alarm when the usage of the source NAT address pool exceeds the limit Support external network hosts to access internal servers Support direct mapping of internal addresses to interface public IP addresses Support DNS mapping function Configurable valid time to support address translation Support multiple NAT ALGs, including DNS, FTP, H.323, ILS, MSN, NBT, PPTP, SIP, etc. Support NAT444, NAT64	
VPN	L2TP VPN, IPSec VPN, GRE VPN, MPLS VPN, SSL VPN Support IPv6 over IPv4 GRE tunnel	

Attributes	M9000-X06	M9000-X10
IPv6	IPV6 stateful firewall IPV6 inter-domain policy IPV6 Attack Defense IPV6 connection limit IPv6 protocol: I CMPv6 , PMTU , Ping6 , DNS6 , TraceRT6 , Telnet6 , DHCPv6 Client , DHCPv6 Relay , etc. IPv6 routing: RIPng , OSPFv3 , BGP4+ , static routing, policy routing, PIM-SM , PIM-DM , etc. IPv6 transition technology: NAT-PT , IPv6 Tunnel , NAT64 (DNS64), DS-LITE, etc.	
high reliability	Support RBM dual-machine state hot backup (Active/Active and Active/Backup two working modes) Support for asymmetric paths Support IKE state synchronization of IPSec VPN Support VRRP Support static and dynamic link aggregation Support continuous upgrade of ISSU Support hot patch technology, can upgrade smoothly, and support dual-machine hot backup for different versions of software Support BFD link detection	
Ease of maintenance	Supports command-line based configuration management Support web mode for remote configuration management Support H3C iMC management platform for device management Support standard network management SNMPv3, and compatible with SNMP v1 and v2 By means of simulated deployment, you can compare the policies to be deployed according to the learning results of business mutual visits, which is convenient for operation and maintenance personnel to manage security policies. At the same time, it supports black and white lists, application types, policy risks, security rules, mixed rules, etc. Security policy compliance check Supports security policy logs, NAT logs, security protection logs, and URL logs, which can contain the above types of log fields at the same time. NAT logs can support port segment allocation, and device logs can be polled and sent	
Environmental protection and certification	Support Europe's strict RoHS environmental protection certification	

Typical networking



H3C SecPath M9000 -X Typical Networking

- Dual-machine status hot backup technology, highly reliable network design
- Strong business processing capability
- Excellent VPN encryption processing ability
- Excellent anti-attack capability, effectively preventing single-packet, Flood and other attacks
- Rich routing protocols to achieve security and network integration

Optional information

Host purchase list

the host	describe	Remark
H3C SecPath M9000-X06	H3C SecPath M9000-X06 main chassis	Required
H3C SecPath M9000-X10	H3C SecPath M9000-X10 Main Enclosure	Required
SecPath M9000-X06 main control engine module	H3C SecPath M9000-X 06 main control engine	Mandatory, 1+1 redundant
SecPath M9000-X 10 main control engine module	H3C SecPath M9000-X 10 main control engine	Mandatory, 1+1 redundant

Security Service Engine Selection List

Security business module	describe	Remark
SecBlade Next Generation Firewall A Module	SecBlade Security Service Board	Optional
SecBlade next-generation firewall B module	SecBlade Security Service Board	Optional

Interface Unit Selection List

interface module	Remark
Interface Exchange A Module (SH)	Optional
Interface Exchange B Module (SH)	Optional
2-port 100G Ethernet optical interface (QSFP28)+16-port 10 Gigabit Ethernet optical interface module (SFP+)	Optional
4 ports 40G Ethernet optical interface (QSFP+)+16 ports 10 Gigabit	Optional
24-port 10 Gigabit Ethernet optical interface module (SFP+)	Optional
6-port 100G Ethernet optical interface module (QSFP28)	Optional

switching engine

switching engine	Remark
H3C SecPath M9000-X06 SFU, Class A	Required
H3C SecPath M9000-X10 SFU, Class A	Required

Power Module Selection List

power module	Remark
2400W AC power module	Required
2400W DC power module	Required

power module	Remark
3000W AC power module	Required
3000W AC&240V-380V High Voltage DC Power Module	Required

Fan Module Selection List

fan module	Remark
H3C fan frame module	Required

New H3C Technology Co., Ltd.
Beijing headquarters
Building 1, Lei Shing Hong Center, Courtyard No. 8, Guangshun South Street, Chaoyang District, Beijing
Zip code: 100102

Hangzhou Headquarters
No. 466, Changhe Road, Binjiang District, Hangzhou
Zip code: 310052
Tel: 0571-86760000
Fax: 0571-86760001

http://www.h.com 3c_

customer service hotline
400-810-0504