

H3C SecPath M9000-AI-E Multiservice Security Gateway Series

Product overview

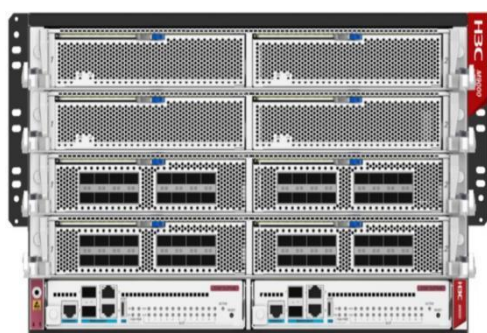
To embrace the trend towards cloud computing, 5G, IoT, IPv6, big data, and high-performance computing, H3C designed the new-generation high-performance SecPath M9000-AI-E multiservice security gateway series for cloud computing data centers, Carrier-Grade NAT (CGN), large-sized enterprises, and campus networks.

H3C SecPath M9000-AI-E series uses dual GPUs + dual CPUs + AI chip architecture and AI-powered new computing module to deliver the following features:

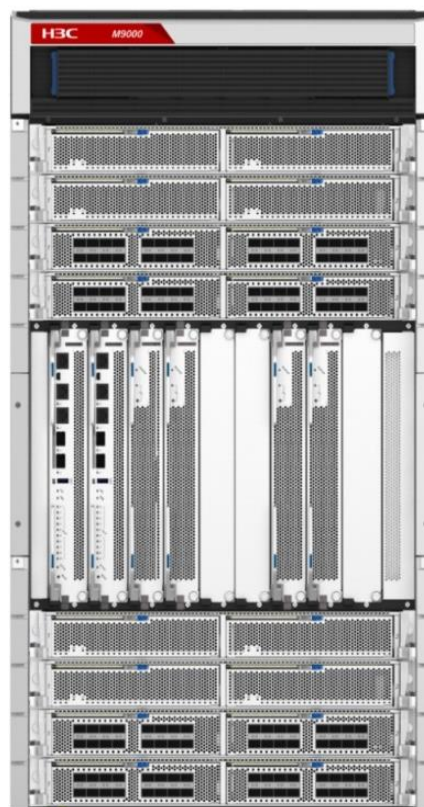
- All-around attack defense, abnormal traffic cleaning, unknown threat detection, server connection detection, sensitive data protection, Web application firewall (WAF), access control, security zone, denylist, traffic monitoring, mail filtering, webpage filtering, and application layer filtering, which effectively ensure network security.
- Deep packet inspection (DPI) to provide robust protection for Web servers.
- Application Specific Packet Filter (ASPF), which can inspect connection status and detect exceptional commands.
- VPN services, including L2TP VPN, GRE VPN, IPsec VPN, and MPLS VPN.
- CGN services.
- Routing capabilities, including static routing, RIP, OSPF, BGP, and ISIS routing policies, and policy-based routing.
- IPv4 and IPv6 dual stacks.

The H3C SecPath M9000-AI-E series provides the following hardware features to meet the following network availability, maintenance, upgrade, and optimization requirements:

- Multi-core, fully distributed, and modular hardware architecture, allowing for more flexibility in networking and scaling.
- 1+1 MPU redundancy, unified configuration management, and security cluster.
- Fan tray redundancy, fan status monitoring, and stepless speed regulation, which enables automatic fan speed adjusting based on temperature and card configuration.
- M+N power module backup, AC and DC power module hot swapping, and load sharing. You can configure power modules based on system power consumption.
- Mixed installation of service modules and interface modules for various performance requirements.
- Hot swapping of all modules.



M9000-AI-E8



M9000-AI-E16

Features and benefits

High-performance software and hardware platforms

- Uses fully distributed hardware architecture with separation of control, service, and data, and decouples key system components to improve reliability. Uses independent switching engine to implement high-performance security service processing and forwarding.
- Uses high-performance MPUs to implement unified configuration management and security cluster.
- Has the highest service processing speed per card in the industry. Each card is capable of providing all Layer 2 to Layer 7 security features, including firewall, NAT, LB, IPS, AV, ACG, and VPN, simultaneously.
- Uses built-in TCAM to ensure high speed searching for a great number of policy entries.
- Uses built-in modular software system for multi-process scheduling to improve system reliability. Processes are running separately. The failure of a single process does not affect other processes of the system.
- Supports authority management to define read-write authorities of users based on feature, command line, system resource, and Web management level to improve system security.
- Supports hot patching and ISSU, which allow system upgrading without interrupting services to improve system usability.

Carrier-level high availability

- Uses H3C highly-available proprietary software and hardware platforms that have been proven by Telecom carriers and medium- to large-sized enterprises.
- Supports 1:1 stateful failover: active/active stateful failover for load sharing and active/standby stateful failover for backup.
- Supports N:N stateful failover, providing load sharing and service backup.
- Supports Security Cluster Framework (SCF), including multi-chassis cluster and heterogeneous cluster.

Powerful security protection features

- **Attack protection**—Detects and prevents various attacks, including Land, Smurf, UDP Snork attack, UDP Chargen DoS attack (Fraggle), large ICMP packet, ping of death, tiny fragment, Tear Drop, IP spoofing, IP fragment, ARP spoofing, reverse ARP lookup, invalid TCP flag, IP/port scanning, and common DDoS attacks such as SYN flood, UDP flood, ICMP flood, DNS flood, and CC.
- **Unified management**—Manages the host and service modules as a single network element. You do not need to plan IP addresses for each card. This function saves IP addresses, facilitates deployment, and realizes comprehensive configuration management, performance monitoring, and log auditing.
- **IFF**—Intelligent Flow Forwarding (IFF), which balances traffic on the deployed service modules to implement distributed traffic processing.
- **SCF**—Supports multi-chassis cluster, which simplifies management and deployment, and implements resilient extension of security services and security performance.
- **SOP**—Security ONE platform. It provides virtual firewall functions by using container-based virtualization technology.
 - Process-based isolation among SOPs.
 - Static and dynamic system resource dividing at a high level of granularity based on the unified OS kernel.
 - SOP quantity adjustment based on system requirements.
 - SOP capability adjustment based on user requirements.
- **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.
- **AAA**—Supports authentication based on RADIUS/HWTACACS+/LDAP(AD), CHAP, and PAP.
- **Denylist**—Supports static denylist and dynamic denylist.
- **NAT**—Supports static NAT, source address NAT, destination address NAT, static CGN NAT, and dynamic CGN NAT.
- **P2P traversal**—Supports Fullcone and Hairpin.
- **VPN**—Supports L2TP, IPsec/IKE, GRE, and MPLS VPN.
- **Routing**—Supports IPv4 and IPv6 static routing, ECMP routing, policy-based routing, IPv4 routing protocols (such as BGP, RIPv2, OSPF, and ISIS), and IPv6 routing protocols (such as BGP4+, OSPFv3, and ISISv6).

- **Security logs**—Supports operation logs, interzone policy matching logs, attack protection logs, DS-LITE logs, and NAT444 logs.
- **Traffic monitoring, statistics, and management.**

Flexible and extensible, integrated and advanced deep security

- **Robust Web protection**—In addition to conventional IPS/AV solutions, the gateway provides precise and granular Web application protection for internal servers to effectively prevent the most troublesome CC attacks on servers, illegal server connections, and common attacks such as SQL injections, HTTP slow attacks, and cross-site script attacks. It checks various requests from Web application clients to ensure their security and validity, and blocks illegal requests in real time. These bring robust security for all websites.
- **Unknown threats prevention**—In the current complicated network environment, feature analysis alone is no longer adequate to prevent attacks and threats. The gateway supports using the sandbox solution to construct an isolated environment for threat detection and prevention. It sends network traffic to the sandbox for isolated analysis and blocks malicious traffic. With sandbox, the gateway delivers the most effective solution to prevent typical advanced persistent threats (APTs).
- **Endpoint identification**—Endpoint identification is a prerequisite for establishing secure IoT connections. When traffic from an endpoint flows through the gateway, the gateway can analyze and extract information about the endpoint, such as the vendor and model name, and it can send a log message to the user when the endpoint information changes (such as change of the camera vendor). In addition, the gateway can use Application Recognition (APR) and IPID trail tracking to detect network sharing behaviors through a NAT device or proxy.
- **Server connection detection (SCD)**—SCD monitors internal servers and prevents them from becoming part of a botnet, launching attacks, or performing internal network penetration. SCD enables the gateway to learn the connections initiated by designated servers. The learning results provide the basis for the administrator to create SCD policies to monitor and log illegal connections initiated by the servers.
- **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.
- **Real-time anti-virus protection**—Uses the Kaspersky stream-based anti-virus module to prevent, detect, and remove malicious codes from network traffic.
- **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

- Basic IPv6 protocols, including TCP6, UDP6, RAWIP6, ICMPV6, PPPoEv6, DHCPV6 Server, DHCPV6 Client, DHCPV6 Relay, DNSv6, and RADIUS6.
- IPv6 routing protocols, including IPv6 static routing, IPv6 routing policies (BGP4+\OSPFv3\ISISV6), and policy-based routing.
- IPv6 ASFP.
- IPv6 attack protection.

- 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.

Next-generation multi-service features

- **Integrated link load balancing**—Using link state inspection and link busy detection technologies, applies link load balancing 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.
- **Basic 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

- **Policy hit analysis and policy optimization**—Analyzes and identifies redundant and unmatched security policies for the administrators to have an informed, further analysis and handling of the policies. The application layer detection engine on the gateway can analyze potential risks in the traffic allowed by the security policy intelligently, and conduct an overall assessment of the safety levels for all security policies in the gateway.
- **Comprehensive management methods**—Allows professional and powerful CLI management as well as simple and easy Web management, supports SNMPv3, and is compatible with SNMPv1 and SNMPv2c.
- **Port- and IP-based packet capture**—Captures incoming and outgoing packets, and generates and saves the packet capture records to a .cap file on the local device or a remote server, for you to use a packet analyzer such as Wireshark to view the file for traffic analysis.
- **Packet loss analytics**—Provides statistics about packets dropped during the forwarding process and by the security services (such as attack prevention, session management, and connection limit services) for analysis of detailed reasons for packet discarding.
- **Webpage diagnosis**—Conducts basic diagnosis of the network when the internal network user fails to access the webpages and provides reasons for the failure.
- **Packet trace**—Uses real traffic, imported packets, and constructed packet to trace packet processing by security services (such as attack protection, uRPF, session management, and connection limit services), and provides detailed information about the packets to help the administrators troubleshoot network failures.
- **Centralized network security management with H3C Security Service Manager (SSM)**—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.

- **Report customization from the Web interface**—Customizable contents include time range, data source device, generation period, and export format.

Specifications

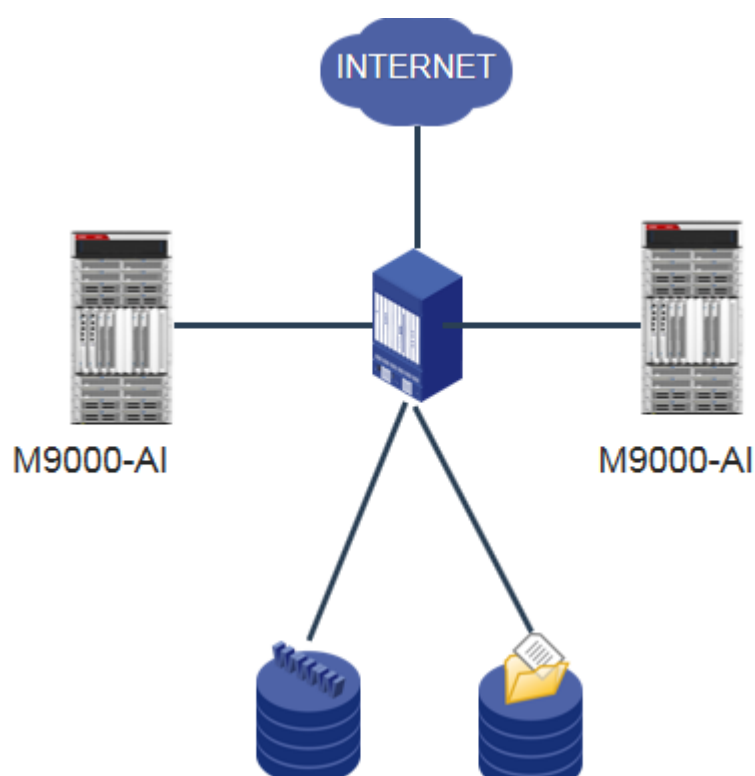
Item	M9000-AI-E8	M9000-AI-E16
Supervisor engine module slots	2	2
Service module slots	8	16
Switching fabric module slots	4	4
Redundancy design	Redundant supervisor engine modules, switching fabric modules, power supplies, and fan trays	Redundant supervisor engine modules, switching fabric modules, power supplies, and fan trays
Dimensions (H × W × D)	264 × 440 × 857 mm (10.39 × 17.32 × 33.74 in), 6 RU	841.7 × 440 × 640 mm (33.14 × 17.32 × 25.20 in), 19 RU
Weight	< 140 kg (308.64 lb)	< 220 kg (485.01 lb)
Power consumption	< 2252 W	< 3360 W
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, bridge	
AAA	Portal, RADIUS, HWTACACS, PKI/CA (X.509 format) , and domain authentications Manual key, IKEv2, redundant VPN gateway, EAP authentication, IKEv2 redirection Virtual multi-service security gateway Security zone Attack protection against malicious attacks, such as land, smurf, fraggle, ping of death, tear drop, 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 Dynamic packet filtering	
Multiservice security gateway	ASPF application layer packet filtering Static and dynamic blacklist function MAC-IP binding MAC-based ACL ICMPv6, DHCPv6 802.1Q VLAN transparent transmission MLD, ND	
Security policy	ACL with rule matching criteria including security zone (security zone group), service, user, application, and time range. Security level evaluation for security policies, security policy optimization Fuzzy search for security policies, including redundant and unmatched security policies	

Item	M9000-AI-E8	M9000-AI-E16
Routing	Policy grouping	
	Policy creation, deletion, editing, migration on a third-party platform	
	State validity-based security monitoring	
Anti-virus protection	Access control by allowlist and denylist, one-key setting of allowlist and denylist	
	Static routing	
	Dynamic routing protocols: RIP, OSPF, BGP, IS-IS	
Web security protection	Policy-based routing with support for traffic matching criteria including source IP address, destination IP address, source port number, destination port number, service, application type, user, user group, incoming interface, outgoing interface, and link state	
	IPv4 and IPv6 dual-stack virus signature detection and protection, protecting against mail viruses, Web application viruses, common file viruses, Trojans, worms, malicious webpages, compressed data, shelling and compressed package (zip, gzip, tar) viruses	
	Manual and automatic upgrade of the signature library, manual import of signature libraries	
Deep packet inspection	Cloud virus signature library	
	Stream-based processing	
	Virus detection based on HTTP, FTP, SMTP, and POP3	
HTTPS encrypted traffic inspection	Support for detection of Backdoor, Email-Worm, IM-Worm, P2P-Worm, Trojan, AdWare, and Virus	
	Virus logs and reports	
	Web security detection	
Email/webpage/application layer filtering	CC attack prevention	
	Server connection detection, allowing for learning parameter configuration	
	Prevention against attacks such as webpage hanging horse and Trojan	
	Prevention against brute force cracking of passwords for common Web services (including HTTP, FTP, SSH, SMTP, and IMAP) and common database software (such as MySQL, Oracle, and MSSQL)	
	Prevention of attacks such as hacker, worm/virus, Trojan, malicious code, spyware/adware	
	Application scenario-specific security policy and attack defense template	
	Application layer (HTTP, HTTPS, DNS, FTP, and SIP) flood attack defense	
	Automatic generation of DDoS attack prevention policies through threshold-based and self-learning techniques	
	Prevention of attacks such as 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	
	URL identification, malicious URL blocking, interoperation with a cloud URL server to expand the number of addresses in the URL address database	
	Local and cloud sandbox interoperation to detect APT attacks in real time and prevent unknown threats	
	Support for integration into a unified security management platform for network-wide security protection	
	SSL proxy and SSL decryption, decrypting the HTTPS traffic from the client (or server), implementing content security checks, auditing, and attack defense for the traffic	
	Refined classification and decryption of URLs	
	Email filtering	
	SMTP email address filtering	

Item	M9000-AI-E8	M9000-AI-E16
Intelligent bandwidth control	Email subject/content/attachment filtering	
	Webpage filtering	
	HTTP URL/content filtering	
	Java blocking	
	ActiveX blocking	
	SQL injection attack prevention	
	Bandwidth guarantee for specific users, IP addresses, interfaces, or services	
Load balancing	Traffic shaping	
	Maximum traffic limit, minimum traffic limit, or connection limit setting by user or IP	
	Application layer protocol-based flow control policy settings, including maximum/minimum bandwidth, guaranteed bandwidth, and protocol traffic priority	
	HTTP- and HTTPS-based application layer link load balancing	
	Transparent DNS proxy, DNS filtering, intelligent DNS	
	Server load balancing	
	Global load balancing	
NAT	Link health monitoring	
	Intelligent link selection	
	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 capacity expansion through port reuse	
	NAT of both source address and destination address, source NAT address pool usage alarm	
VPN	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	
	NAT444, NAT64	
	L2TP VPN	
IPv6	IPSec VPN	
	GRE VPN	
	SSL VPN	
	IPv6 over IPv4 GRE tunnels	
	IPv6 status firewall	
	IPv6 interzone policy	
	IPv6 attack protection	
High availability	IPv6 connection limit	
	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, PIM-SM, and PIM-DM	
	IPv6 transition techniques: NAT-PT, IPv6 tunneling, NAT64 (DNS64), and DS-LITE	
	Active/active and active/standby stateful failover	

Item	M9000-AI-E8	M9000-AI-E16
Configuration and management	IFF	
	SCF	
	Asymmetric-path mode stateful failover	
	IKE-based IPsec	
	VRRP	
	Static and dynamic link aggregation	
	ISSU	
	Patch	
	HA with support for software of different versions	
	BFD	
	Configuration management at the CLI	
	Remote management through Web	
	Device management through H3C IMC	
	SNMPv3, compatible with SNMPv2c and SNMPv1	
	Security policy optimization by simulating deployment of security policies and comparing the results	
	Compliance and legitimacy check of security policies by denylist, allowlist, application type, policy risk level, security rule, and hybrid rule.	
Environmental protection	Security policy logs, NAT logs, attack defense logs, URL logs	
	Logs containing any combinations of security policy, NAT, attack defense, and URL information	
	Log sending at intervals	
	EU RoHS compliance	

Application scenarios



H3C SecPath M9000-AI-E series application scenario

- Stateful failover and reliable network design
- Powerful process capabilities
- Powerful VPN encryption capabilities
- Excellent attack protection capabilities to prevent single packet and flood attacks
- Abundant routing protocols, implementing integration of security and network

Ordering guide

Chassis

BOM part No	Model name	Description
0235A3DF	NS-SecPath M9000-AI-E8	H3C SecPath M9000-AI-E8 Multiservice Security Gateway Appliance
0235A3DE	NS-SecPath M9000-AI-E16	H3C SecPath M9000-AI-E16 Multiservice Security Gateway Appliance

Supervisor engine modules

Install two supervisor engine modules for 1+1 redundancy.

BOM part No	Model name	Description
0231ABY8	NSQM5SUP08A1	H3C SecPath M9000-AI-E8 Supervisor Engine Module, Type A
0231ABY9	NSQM5SUP16A1	H3C SecPath M9000-AI-E16 Supervisor Engine Module, Type A

Switching fabric modules

BOM part No	Model name	Description
0231ABY4	NSQM5FAB08A1	H3C SecPath M9000-AI-E8 Switching Fabric Module, Type A
0231AC17	NSQM5FAB16A1	H3C SecPath M9000-AI-E16 Switching Fabric Module, Type A

Service modules

BOM part No	Model name	Description
0231AE4D	NSQM5AIASKA1	H3C SecPath M9000-AI-E AI Security Engine Module
0231ABYF	NS-FWEMPA1	H3C SecPath M9000-AI-E SecBlade V Next Generation Firewall A Module (MP)

Interface modules

BOM part No	Model name	Description
0231ABY7	NSQM5MBSHA1	H3C SecPath M9000-E Interface Switch A Module (SH)
0231ABY6	NS-C300-TG24A1	H3C SecPath M9000-AI-E 24-Port 10Gb Ethernet Optical Interface Module (SFP+)
0231ABY2	NS-C300-CGQ2TG16A1	H3C SecPath M9000-AI-E 2-Port 100Gb Ethernet Optical Interface (QSFP28)+16-Port 10Gb Ethernet Optical Interface Module (SFP+)
0231ABY5	NS-C300-QG4TG16A1	H3C SecPath M9000-AI-E 4-Port 40Gb Ethernet Optical Interface (QSFP+)+16-Port 10Gb Ethernet Optical Interface Module (SFP+)
0231ABY3	NS-C600-CGQ6A1	H3C SecPath M9000-AI-E 6-Port 100Gb Ethernet Optical Interface Module (QSFP28)

Power supplies

BOM part No	Model name	Description
0231ABYD	PSR3000-54AHD-E	3000W AC & 240V-380V HVDC Power Supply Module
0231ABYB	PSR3000-54A-E	3000W AC Power Supply Module
0231ABYA	PSR2400-54D-E	2400W DC Power Supply Module
0231ABYC	PSR2400-54A-E	2400W AC Power Supply Module

Fan trays

BOM part No	Model name	Description
0231ABYE	FAN-120B-2-A8	H3C Fan Tray Module 8A,Rear-Out Airflow
0231ABYG	FAN-120B-2-A16	H3C Fan Tray Module 16A,Rear-Out Airflow



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

Copyright ©2017 New H3C Technologies Co., Limited Reserves all rights
Disclaimer: although H3C trying to in this materials provide accurate information, there is no guarantee that the material content contains no technical error or printing sex mistake, for this H3C in this material accurate does not undertake any responsibility. H3C retained in no Notice or hint of the contents of this material right to change.

<http://www.h3c.com>