



H3C SecPath ACG1000 Application Control Gateway Datasheet

Product overview

The SecPath ACG1000 series is the latest generation of application control gateways introduced by H3C. Deploy this product in route, transparent bridging (TB), bypass mode, or a hybrid mode at critical network nodes. It consolidates application control, behavior auditing, and network optimization features, offering users a comprehensive and complete solution for all business application scenarios. For more information about the SecPath ACG1000 series, refer to the relevant documentation.

The SecPath ACG1000 series features the latest multi-core hardware architecture. It runs a virtual OS, which, with its efficient parallel scheduling algorithm and memory management mechanism, not only enhances traffic forwarding efficiency but also conducts thorough layer 2-7 inspections and analysis of data.

For effective management and auditing, use deep identification to precisely control and audit thousands of common applications, including IM chat software, P2P downloading software, stock trading software, online games, streaming media, and online video frequency.

Utilize multi-level 7-tuple flow control, precise blocking, and intelligent routing technologies to achieve robust bandwidth management features.

Use clear log management, wireless scenario compliance, and other features to offer users the most comprehensive, clearest, and most intuitive internet behavior solutions.

Views

	
SecPath ACG1000-AI-30	SecPath ACG1000-AI-50

Features and highlights

Fast deployment

To address the challenge of interconnecting multiple branches and rapidly deploying numerous devices at the headend, administrators face the pressing issue of varying technical skill levels among frontline staff. The SecPath ACG1000 series introduces a USB zero configuration feature that allows devices to mount and decipher predefined profiles directly from a USB drive, significantly easing the burden on headend operational staff and reducing deployment obstacles. The result is a quick, accurate, and straightforward deployment process. For more information about the USB zero configuration feature, refer to the SecPath ACG1000 series documentation.

Comprehensive high-end management

Use the SecPath ACG1000 series to switch the management mode to a three-level authorization system. After the switchover, each administrator account is assigned different permissions, creating checks and balances that restrict the super administrator's authority and ensure device security. This setup clearly defines the roles and responsibilities of each administrator.

Integrated policy management

The SecPath ACG1000 series integrates policy configuration with application control, behavior auditing, identity authentication, and security protection, allowing a single policy to configure multiple functional modules. This enables customization of management policies for different users based on varying control requirements, offering flexibility and ease of maintenance.

Comprehensive identity authentication

H3C focuses on user requirements, offering a variety of identity authentication methods.

- **Local Authentication:** Web-based authentication, username/password verification, IP/MAC/IP-MAC binding.

- **Single Sign-On:** Standard AD domain, log in once, authenticate multiple times.
- **Third-Party Authentication:** RADIUS, LDAP, etc.
- **App Certification:** Certify apps without data center software, no app modifications required, eliminating coordination and communication costs.
- **WeChat Authentication:** Connect to the merchant's WiFi to automatically prompt "One-click WeChat Connect to WiFi" and follow the WeChat official account.
- **Hybrid Authentication:** Configure the interface to select multiple authentication methods, allowing users to switch methods as needed.
- **Enable password-free login for user access.**

High-performance multi-service applications

The SecPath ACG1000 series employs an advanced multi-core schema, integrated with H3C's security operating system. It utilizes tree-based storage of protocol signatures, flow scanning, and parallel DPI/DFI technologies to ensure that the entire resolution process is completed in one go, maintaining high-speed, low-latency processing even with multiple behavior management features enabled.

Fast, easy, and reliable VPN security connection

The VPN module in the SecPath ACG1000 series features industry-leading technology that greatly reduces the maintenance workload for administrators in complex network environments. It supports rapid VPN deployment with zero configuration and automatic negotiation of tunnel interface flows without manual settings, allowing for fully automated convergence and autosensing across multiple lines, effectively addressing the issue of limited branch operation and maintenance capabilities. The innovative introduction of IPsec VPN cold backup not only ensures data encryption but also enhances the reliability of data transmission. Furthermore, the unique zero packet loss switchover technology ensures uninterrupted TCP services, enabling flawless High Availability (HA) transitions without disrupting VPN operations. For more information about HA transitions in VPN services, refer to the provided documentation.

Use the SecPath ACG1000 series products to support 4G networks and 4G IPsec VPN encrypted connections without altering the existing network schema. They automatically take over encrypted communication with the central end in the event of a main line fault. These products ensure data integrity, secure transmission, cost-effectiveness, and no network changes, allowing administrators to rest easy. For more information about the SecPath ACG1000 series, refer to the product documentation.

Detailed application management for networks

Use the SecPath ACG1000 series products to manage online behaviors with greater precision, not just by blocking network applications but by identifying specific actions within them. For instance, control over QQ goes beyond just "login actions" to recognize detailed activities like "receiving files," "sending files," "receiving messages," "sending messages," "logging out," "voice communication," and "all actions." Similarly, for WeChat, the system can identify and control various behaviors, ensuring a more orderly network through refined application management. For more

information about the control of specific actions within applications, refer to the detailed management capabilities of the product.

Fine-grained bandwidth management

The SecPath ACG1000 series uses technologies like seven-tuple flow control based on signature libraries, precise blocking, and intelligent routing to divide network egress bandwidth into logical channels. It also supports subdividing channels into subchannels for optimal bandwidth limitation and assurance. Additionally, it distributes complex traffic types across various network egress points, making it an ideal tool for enterprises to enhance bandwidth utilization and protect bandwidth investments. For more information about bandwidth management, refer to the product documentation.

Trace-based user behavior analysis

By analyzing multi-dimensional data such as customer network account activity, device usage, and time, H3C's Internet behavior and management products achieve visual management and auditing of user behavior. They clearly and intuitively display users' online activity trails, aiding network managers in crafting targeted network management policies. This ensures the rational and effective use of network resources and boosts work efficiency. Self-learning and fuzzy match are two of its key features.

User-defined applications

Use this feature to create applications not present in the audit device's library, such as OA and ERP, which the device cannot audit or control. The SecPath ACG1000 series supports customizing applications based on a signature of an unknown application, using URL, port, IP, domain name, and other dimensions. It also supports policy configuration and auditing, enabling administrators to conduct transparent audits of unknown applications.

Smart app cache for efficient application performance

The SecPath ACG1000 series innovatively caches apps locally on the device, allowing users to download files in just seconds, even for files tens of megabytes in size, significantly increasing the bandwidth utilization at exit points and accelerating downloading rates, enhancing user experience. It supports caching for both iOS and Android apps, including precise caching, dynamic caching, automatic app updates, and fuzzy match, leading the industry in technology. This approach opens new avenues for cost-effective customer end marketing and promotions. Combined with app identity authentication, it can enforce the promotion of merchants' apps, boosting installation rates and gaining more potential convertible users. For more information about app caching and identity authentication, refer to the product documentation.

Advertisement push

The SecPath ACG1000 series products offer a feature that allows for the pushing of advertisements to users. You can customize the ad type, content, and location, with support for up to three ad placements on PCs and full-screen ads on

mobile devices. This ad pushing capability, a key application in the e-commerce marketing phase, offers flexibility, interactivity, and precise targeting, significantly reducing the cost of ad delivery. Serving a large number of advertisers, it ensures that Internet ads are delivered to the right consumers in an appropriate manner, resulting in high precision and conversion rates. For more information about the use of this advertising feature in marketing, refer to the relevant section.

Clear post-event auditing

The SecPath ACG1000 series supports detailed, clear, and user-friendly log features, capturing comprehensive audit information such as user online behavior, traffic usage, website access, operating system, and device type. Customizable filters in the logs enable efficient post-event auditing by searching elements like IP address, authenticated users, accessed applications, URLs, and post content. Additionally, the ACG1000 series offers attractive reports with histograms, pie charts, and percentages to visually represent the network's status, aiding data-driven network management and planning. For more information about network management, refer to the appropriate documentation.

SSL website decryption & mailbox decryption

To ensure clear post-event auditing and protect corporate secrets, the SecPath ACG1000 series offers HTTPS auditing and mailbox decryption capabilities. This product line utilizes unique encrypted traffic identification technology, capable of recognizing behaviors on mainstream encrypted websites, search records, and emails. Administrators can customize targeted audits for users and encrypted websites, making network operations more transparent and understandable. For more information about the SecPath ACG1000 series, refer to the detailed introduction.

DNS transparency proxy

In multi-exit network environments with varying interface bandwidths, relying solely on load balancing for routing can lead to poor internet access performance. This necessitates a DNS proxy with data forwarding based on weight and privilege level rules to ensure optimal routing and network access. The SecPath ACG1000 series is the perfect solution to this issue, offering a simple, flexible, and unified DNS management system that provides seamless DNS proxy services to internal users.

The SecPath ACG1000 series offers a robust DNS transparency proxy that enables DNS forwarding load balancing based on weight and privilege level, static domain name mapping, and directed forwarding for specific domain names. This enhances network route selection and load balancing for users, significantly improving user experience. For more information about these features, refer to the product documentation.

Business alarm

The ACG1000 series products feature service alarms for monitoring critical components such as CPU, memory, sessions, overall system traffic, and IPsec VPN disconnections. They offer pop-up notifications and email alerts to quickly identify fault points and provide device state updates to network management, aiding in operations and

maintenance. For more information about these features, refer to the product documentation.

Technical specifications

Hardware specifications

Product model	ACG1000-AI-30	ACG1000-AI-50
Fixed service interfaces	The device features 18 Gigabit copper interfaces, 2 ten-gigabit fiber interfaces, 4 bypass interfaces, 8 combo interfaces, and 2 management interfaces.	The device features 16 Giga copper interfaces, 6 Giga fiber interfaces, 2 ten-Giga fiber interfaces, 4 combo interfaces, and 1 management interface.
Console port	1	1
Memory	4 GB	4 GB
Storage	Two M.2 slots for hard disks	One 2.5-inch hard disk slot
Mean time between failures (MTBF)	≥ 100000 hours	≥ 100000 hours
Default configuration weight	3.7 Kg	5.4 Kg
Dimensions (Length × Height × Depth/mm)	440*43.6*360mm	440*435mm
Temperature	Operating: 0 to 45°C Non-operating: -40 to 70°C	Operating: Without hard disks: 0°C to 45°C With hard disks: 5°C to 40°C. Non-operating: -40°C to 70°C
Humidity	Operating: 5% to 95%, non-condensing Non-operating: 5% to 95%, non-condensing	Operating: Without hard disks: 5%RH to 95%RH With hard disks: 10%RH to 90%RH Non-operating: 5%RH to 95%RH
Power supply	Dual power supplies	Optional dual power supplies
Maximum input current	1A	2A
Maximum power supply (W)	70 W	150 W
Hardware bypass	Yes	No

Software specifications

Level-1 SPEC	Level-2 SPEC	Level-3 SPEC	Level-4 SPEC
Network features	Deployment mode	Bypass	Monitors mirrored traffic on a single interface of a switch.
		Serial	Supports transparent, routed, hybrid (transparent + routed), multi-group bridging, and multi-port bridging configurations.

Level-1 SPEC	Level-2 SPEC	Level-3 SPEC	Level-4 SPEC
		Hybrid	Supports a mix of bypass and serial deployment strategies.
	Port mirroring	Mirroring interface	Physical interfaces support functioning as both mirroring interfaces and mirrored interfaces.
		Mirroring features	Supports mirroring the traffic from multiple physical interfaces to a single interface. Supports mirroring based on all traffic of an interface, as well as upstream or downstream traffic specifically.
	DHCP	DHCP service type	DHCP server DHCP relay proxy
	IPv4 routes	Routing table	Displays device routing information.
		Advanced route attributes	Supports asymmetric routing. Command line support for enforced source ingress and egress.
		Static routing	Supports multi-link load balancing based on routing weights.
		Policy-based routing	Policy routing based on 5-tuple, application, and time.
		ISP routing	Built-in ISP information for telecommunications, Unicom, Mobile, and education networks; ISP information can be customized.
		RIP	Supports RIPv1 and RIPv2.
		OSPF	Supports default route advertisement and route redistribution.
	NAT	General features	Supports source NAT, destination NAT, and static NAT. Supports one-click NAT loopback (bi-directional NAT).
		ALG	Dynamic ports support ALG protocols: H.323, SIP, FTP, TFTP, PPTP. FTP, TFTP, SIP support configuration on non-standard ports.
	Session limit	Rule Management	Supports IP-based session and per-second new connection limits (if referring to address objects, limits are applied to each IP address in the address object)
	Address detection	Interface Detection	Supports PING, TCP, and DNS address monitoring entries
		Address Detection Group	Supports multiple address detection subordinate group relationships
		Route Detection	Supports detecting routes to ensure their validity
	Link load balancing	Link load balancing	Supports seven-tuple link load balancing based on weight and priority
			Load balancing interface supports health detection
	Server load balancing	Server load balancing	Supports server load balancing based on source address hash + weight Supports detecting server group services or server health status
	DDNS	DDNS	Supports Peanut Shell DDNS client and domain name IP binding
Network optimization	APP dynamic cache	APP dynamic cache	Identifies the APP download to a specific server based on the terminal, and the device automatically downloads the APP according to the terminal's download address
	Application cache	Application cache	Supports file application caching, supports file caching with fuzzy matching of file names
	Quality of service	Quality of service	Supports PING, TCP, and DNS detection

Level-1 SPEC	Level-2 SPEC	Level-3 SPEC	Level-4 SPEC
	Management	Management	Supports custom interval time detection
Virtual router	VRF	Interface virtualization	The interface belongs to root by default, and after creating VRF, the interface can be added to the VRF. An interface can only belong to one VRF;
		IP address overlapping	Interfaces under different VRFs can be configured with the same IP address
		Static routing	Supports static routing
Intrusion prevention	Intrusion defense	Intrusion defense	Supports intrusion detection based on source, destination, and rule set Supports advanced intrusion defense alerts. Supports FTP and email notifications
		Signature library	System defines over 3000 rules, including Backdoor, bufferoverflow, dosddos, im, p2p, vulnerability, scan, webcgi, worm, and game.
Anti-virus	Virus protection	Virus protection	Scans and kills viruses in email body/attachments, web pages, and downloaded files
		Virus protection	Supports heuristic scanning and killing of unknown viruses
	General functions	Blacklist	Supports manual configuration Automatically adds sources triggering attack rules and IPS blocking rules to the blacklist
Security protection	Scan protection	General	Based on interface configuration, supports automatic addition to the blacklist
		Scanning methods	Port scanning, IP address scanning
	Abnormal packet protection	Abnormal package types	Ping of Death; Land-Base; Tear Drop; TCP flag; Winnuke; Smurf; IP options; IP Spoof; Jolt2
	ARP protection	ARP attack prevention	Supports ARP learning and active protection, prevents ARP Flood attacks
		ARP learning control	Interface-based ARP learning control
	Flood protection	Supported types	SYN Flood, UDP Flood, ICMP Flood, DNS Flood
Web protection	Basic configuration	Policy configuration	Supports policy matching based on source address, destination address, and service port
		Security configuration	Supports protection rules; fine-grained access control; anti-leeching; CSRF attack prevention; CC attack prevention; application hiding; web page tampering prevention
	Security protection	Rule protection	Built-in HTTP protocol check; protection against 11 types of common attacks such as general attacks and SQL injection attacks
		Fine-grained access control rules	Supports administrator-defined feature matching fields for fine-grained control
		Anti-leeching	Supports protection against the entire site, specific URLs, specific file types, etc.
		CSRF	Supports controlling access sources for specific URLs
		CC attack	Real-time monitoring and protection against the entire site and specific URLs, allowing administrators to configure trigger conditions
		Application hiding	Supports administrator configuration of specific fields for application hiding
Risk scanning	Port scanning	Scanning tasks	Supports administrator configuration of port scanning tasks for specific resources to identify potential risks in advance

Level-1 SPEC	Level-2 SPEC	Level-3 SPEC	Level-4 SPEC
	Weak password scanning	Scan results	Display of scan results, and supports administrator operations based on the scan results
		Scanning tasks	Supports administrator creation of weak password scanning tasks
		Scan results	Display of scan results, and supports administrator operations based on the scan results
		Dictionary management	Built-in password dictionary; also supports administrator import of password dictionaries
Traffic management	General functions	Configuration management	Add, delete, modify
	Traffic control	Line management	Bind interfaces Supports interface-based upstream and downstream bandwidth management
		Channel management	Support high, medium, and low priority channel settings Support channel matching based on application, user, source address, service, and time
	Exclusion policy	Exclusion policy	Support user and address exclusion
	Quota policy	Quota policy	Support quota policy based on duration and traffic Support blocking and flow control when exceeding the quota threshold
Decryption policy	HTTPS Website Decryption	HTTPS website decryption	Support policy-based HTTPS website decryption Support custom HTTPS website decryption Support predefined HTTPS website decryption
	SSL email decryption	SSL email decryption	Support decryption of SSL encrypted webmail Support decryption of SSL encrypted client-based email
Prevent shared internet access	Prevent shared Internet access	Prevent shared internet access	Support monitoring of shared network by user Support blocking and throttling as punishment methods Support configuration of user terminal threshold for shared network, support individual configuration for different terminals
Access control	IPv4 policy	policy	Seven-tuple policy matching conditions: user, application, source address, source interface, destination address, destination interface, service, time, and terminal type Support policy actions for application control, URL filtering, and terminal announcement push Policy-based long connection (aging time)
	IPv6 policy	Configuration management	Support 7-tuple policies with arbitrary users and applications
Internet behavior control and auditing	Application control	Application control	Support application control policies based on application configuration
		Email control	Support control for sender; recipient; subject content; email size; number of attachments
		Web keyword control	Support keyword control for search engines; http upload; http page content
		Virtual accounts	Support black and white list control for QQ virtual accounts

Level-1 SPEC	Level-2 SPEC	Level-3 SPEC	Level-4 SPEC	
		URL control	Support predefined and custom URL category filtering	
		Terminal notice	Support pushing terminal notice content based on policies	
	Application auditing	HTTP auditing	Support auditing web access; online communities; web search; HTTP outbound files; HTTP file downloads	
		Email auditing	Support auditing sending and receiving emails; webmail	
		Instant messaging	Support auditing chat content of QQ client; WeChat client; web QQ; web WeChat; mobile Fetion, etc.	
		Basic protocols	Support auditing FTP; TFTP; TELNET basic network protocol accounts, commands, etc.	
		Entertainment stocks	Support auditing stock entertainment accounts and comments	
		Network applications	Support auditing other major categories of network applications	
Statistical report	Report management	Report management	Support creating report tasks on a daily, weekly, monthly basis, as well as one-time reports. Report tasks can be enabled or disabled Support reports with various templates, and administrators can customize report templates Support sending reports via email and FTP Reports support PDF and HTML formats Subscription project support: device dimension; behavior management data statistics dimension; network quality dimension; network security dimension	
		Historical report	After completing the report task support, delete the local historical report, and also support keeping the local historical report Historical report space supports customization	
	Data statistics	Statistics	Supports data statistics based on various dimensions such as user online behavior count, user website access, user email audit, instant messaging, etc. Supports administrator-defined statistical time dimension Completed statistics data supports device-side display and export in report format	
	Report configuration	Disk management	Supports configuring disk space proportion for report function	
		External server	Supports email sending server and email account settings Supports FTP sending server settings External server supports connectivity verification	
		Global configuration	Supports setting the top number of users for report statistics Supports setting the start date for report statistics	
	VPN	IPsec VPN	IKE phase one negotiation mode	Supports IKEv1 Supports main mode and aggressive mode
			Encryption/HASH algorithm	International standard algorithms (DES/3DES/AES/MD5/SHA-1), supports national encryption algorithms
IPsec encapsulation			Supports ESP and AH encapsulation	

Level-1 SPEC	Level-2 SPEC	Level-3 SPEC	Level-4 SPEC
	IPsec quick VPN	IPsec cold backup	Supports IPsec cold backup, main VPN disconnects, and backup VPN triggers start building
		IPsec quick VPN	Supports IPsec quick VPN configuration Supports deployment in central and client modes
	SSL VPN	Global configuration	Supports configuring global functions for SSL VPN
		Resources	Support configuring network resources published by SSL VPN
		Users	Support local management accounts for SSL VPN, support AD and Radius integration
		Online users	Support real-time online monitoring of SSL VPN users
User management	User synchronization	Basic protection	Support basic protection for SSL VPN network
		SNMP synchronization	Support reading user-related information of network devices through SNMP protocol and entering the read information locally
		AD user synchronization	Support synchronizing users from AD server to local through LDAP protocol Support manual synchronization and automatic synchronization multiple times
		ARP scanning	Support synchronizing users scanned through ARP scanning to local
	User structure	Enter after authentication	Support synchronizing already authenticated users to local after various authentication strategies. Used as local users for policy invocation
		User organizational structure	Supports a standard tree structure for easy management and invocation of users.
	General functions	Temporary account	User accounts created locally can have an expiration date set for user validity.
		Suppress pseudo portal	Supports pseudo-portal suppression function (http-APP) (via command line).
	IPv6 support	HTTPS pop-up portal	Authentication portal prompted upon access via HTTPS.
		IPV6 users	Users can be bound to an IPV6 address.
	AAS linkage	Communicate with AAS	Integrates with AAS
	Portal escape	Portal escape	Enables fail-permit for authenticated users. Enables fail-permit for all users
User policy	IMC linkage	Communicate with IMC	Integrates with IMC
	Identification related	Identification scope	Set the IP address range for identification
	Redirection	Redirection page	Default redirection page
System management	System administrator	Policy	Matching items: source interface, source address, destination interface, destination address, time Supports WeChat, SMS, local, non-authentication, portal authentication, AD single sign-on, QR code authentication, hybrid authentication
		Account management	Login authentication methods support local authentication, Radius server authentication, LDAP server authentication
		Management settings	Supports separation of powers Supports account uniqueness check
	Authentication server	Radius	Supports remote authentication requests for multiple user third-party storage

Level-1 SPEC	Level-2 SPEC	Level-3 SPEC	Level-4 SPEC
		LDAP	Supports remote authentication requests for multiple user third-party storage Supports LDAP user and user group synchronization authentication
		Server group	Radius/LDAP Server Group, supports primary/backup and cluster
		SMS authentication	Supports seamless authentication Supports SMS verification code for identity verification and WiFi authentication
		AD single sign-on	Supports single sign-on authentication method for AD servers
		WeChat authentication	Supports WeChat Wi-Fi authentication method Supports mandatory follow function Supports seamless authentication
		Hybrid authentication	Supports hybrid authentication with multiple authentication methods
	System maintenance settings	Diagnostic tools	Ping, traceroute, TCP SYN detection
		Packet capture tool	Support capturing data packets according to filtering conditions Support downloading packets to local for viewing
		Information collection	Setting method: manual collection and automatic collection
			Collection content operation: download, view, delete
	Reliability	Hardware bypass	Power port power off bypass Power port startup process bypass
		Software bypass	IPS module software bypass: Instant CPU usage rate exceeds 70% and enters the detection process at 10:1 ratio, command line adjustable scale
	Dual machine hot standby HA	Primary/Standby, Primary/Primary mode	Support configuration, flow, feature library, interface status, IPsec VPN status synchronization
	SNMP	SNMP configuration	SNMP agent
			Version: v1, v2, v3
		trap	Trap version: v1, v2 Notification, v2Inform
	Domain related	DNS server	Support 4 DNS servers
		DNS transparent proxy	Support DNS weight ratio and priority transparent proxy based on outbound interface
	Configuration management	Configuration management	Supports saving multiple configuration files. Supports specifying configuration for the next startup. Supports configuration copy in and out for backup purposes.
	USB zero configuration	USB zero configuration	Supports firmware upgrades via USB drive. Supports configuration import from a USB drive. Enables zero-configuration deployment with a USB drive.
	Chinese and english version	Chinese and english version	Supports switching between Chinese and English versions.
	Customize management port	Customize management Port	Allows customization of the management port.

Level-1 SPEC	Level-2 SPEC	Level-3 SPEC	Level-4 SPEC
	System alarm	System alarm	Supports system resource alarms. Supports IPsec alarms. Supports email and pop-up alarms, with the pop-up showing the latest 10 alarm records by default.
	Wireless non-economical	Data table library	Locally generates database tables for user terminal logins and logouts, internet access logs, general content, AP information, venue information, virtual identities, search keyword information, BBS information, and email information.
		Platform vendor integration	Supports interfacing with the Chinese national standard (GA/WA3011.1-2015) data format. Enables direct integration with mainstream public security platforms such as Renzixing, Paibo, Aisi, Hongxu, Rui'an, Wangbo, Zhongxin, Hengbang, Zhao Wu, Yun Chen, Kuanguang Zhitong, Xiexun, and more.
		Authentication data	Supports standard radius servers. Supports non-standard UDP port 9999 for obtaining user authentication information. Enables active retrieval of user information using part of the AC MIB library. Support for authentication servers such as City Hotspot, Deep Blue, Tailink, Guanghua Crown Group, H3CIMC, SAM, and AMEI;
		Three-Layer audit	Supports user audit and traceability for fat APs from brands like FiberHome, Putian, Changhong, Hisense, etc.
		Data reporting cycle	Supports real-time data reporting and allows setting the reporting interval according to user requirements.
		Standard API interface	Compatible with standard telecom CRM systems, enabling active retrieval of location and AP information.
		Data transmission	Supports file transfer via FTP, FTPS, HTTP, UDP, and other methods. Supports file formats such as .ZIP, .syslog, .XML, .bcp, .ok, etc.

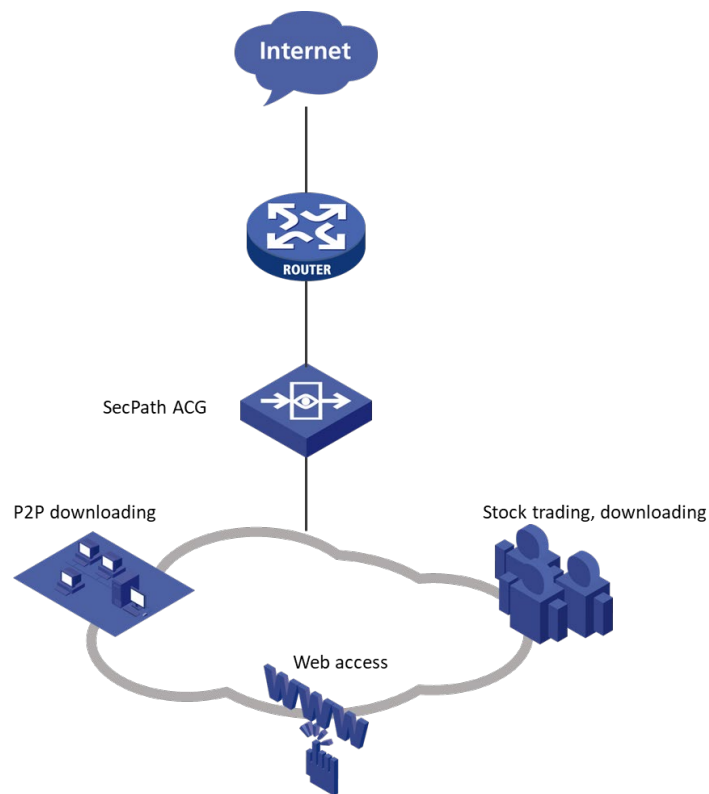
Performance specifications

Specification/item	ACG1000-AI-30	ACG1000-AI-50
Application throughput (all threat protection)	500M	1.5G
new connections per second	70000	150000
concurrent connections	1.5 million	4 million
Recommended Concurrent Users	3000	10,000

Application Scenarios

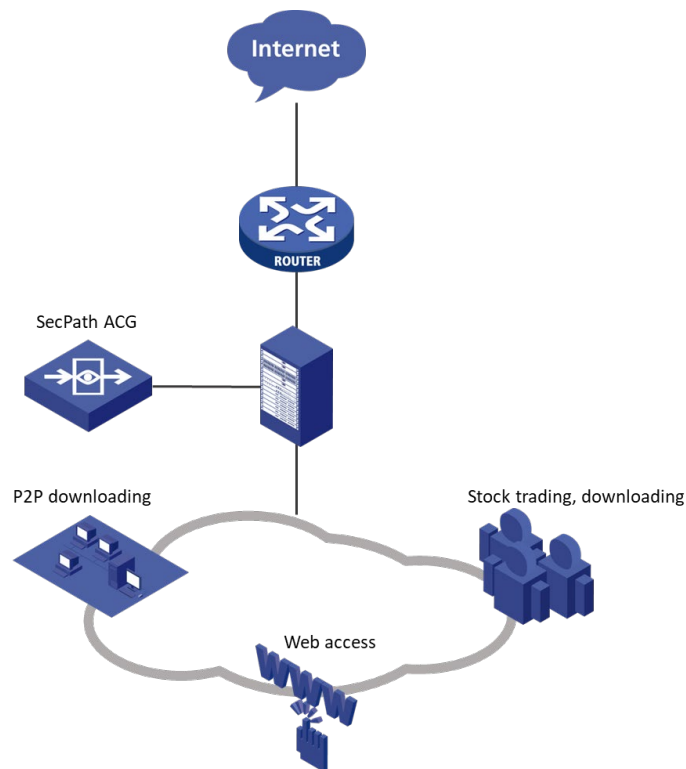
Route deployment

- For medium and large enterprise users, deploy transparently online at the network egress without altering the network topology.
- Monitor and manage various applications like online communities, P2P, instant messaging, online gaming, stock trading, network video frequency, network multimedia, and unauthorized website access to ensure bandwidth for critical applications and services.
- Analyze and audit user internet behavior.
- Support VPN, MPLS, VLAN, PPPoE, and other complex network environments.



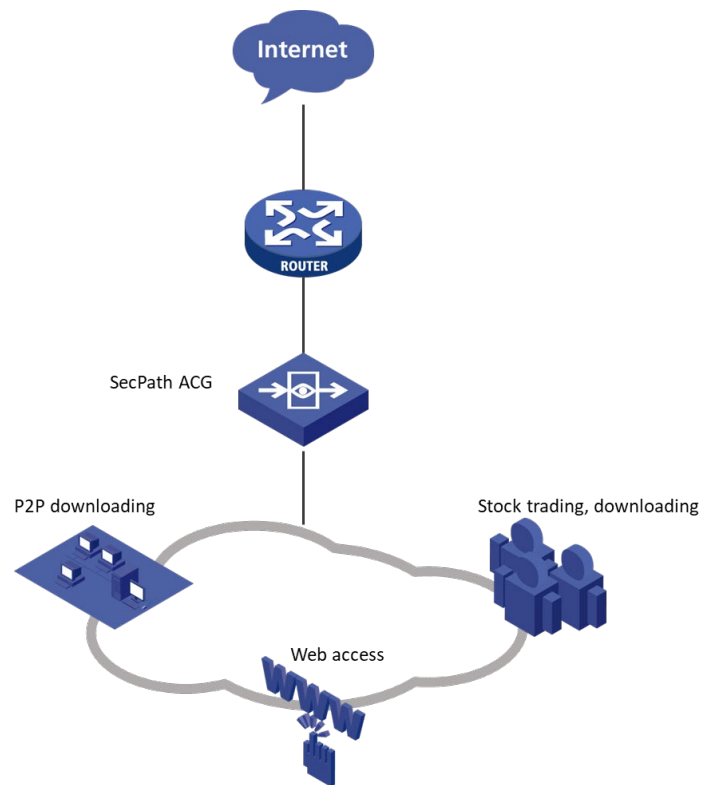
Bypass deployment

- Use this in scenarios where you want to audit behavior without changing the network topology, typically deployed at the core layer.
- Analyze and audit user internet behavior.
- The system offers log recording and export capabilities.



Transparent deployment

- Deploy this solution in data center server rooms with flexibility, using either serial routing or transparency at the data center exit, for straightforward implementation based on the actual network environment.
- Provide identity authentication to verify the legitimacy of users accessing the internet.
- Monitor and manage various applications such as network communities, P2P, instant messaging, online gaming, stock trading, network video, network multimedia, and access to illegal websites to ensure bandwidth for critical applications and services.





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
Fax: +86-571-86760001

Copyright ©2025 New H3C Technologies Co., Limited
Reserves all rights 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. H3C reserves the right for the modification
of the contents herein without prior notification.

<https://www.h3c.com>