DH-SACG

Dahua Security Access Control Gateway

Video surveillance plays an increasingly important role in people's life. However, the cameras are usually distributed and deployed in unattended environments, they can easily become network attack sources once exploited by hackers. Dahua has launched SACG (Security Access Control Gateway) Series products, which provide a strong guarantee for the security access of video surveillance network cameras.

System Overview

DH-SACG solves the problem of private connection. Only trusted front-ends and legal traffic are allowed to access the network, so as to realize the security of core data area of video network.

Functions

Protocol Filtering
Granularly filters transmission traffic.
Only releases compliance data.

Real-time Blocking
Accurately identifies threats.
Blocks attacks in real time.

Flexible Deployment
Flexibly deployment of inline and bypass.
Seamlessly integrated into the surveillance network.

Ultra Low Latency
Processing latency < 20 μs.
No impact on video operations.

- Device identity authentication: SACG can actively scan current network devices (such as IPC, PC, and NVR) to build an asset library, and authenticate the identity of cameras for compliance through the device feature fingerprint technology, effectively blocking unauthorized devices.
- Transfer protocol filtering: SACG can identify and filter transferred data at the protocol level, by only releasing compliance data, such as videos and pictures, while blocking illegal traffic.SACG is compatible with the protocol features of mainstream surveillance device manufacturers
- Real-time blocking of threats: SACG can monitor access behaviors and transferred data of devices in a variety of ways, can block detected attacks and send alarms in real time.
- Asset status monitoring: SACG can monitor the operation status of cameras in real time, including information on device IP address, online and offline time, Front-ends status,Front-ends type, manufacturer brand, geographic location, device online rate, and the quality of access links.
- Unified security management: SACG can be integrated into the Dahua security management platform for unified management to intuitively present users with rich and real-time security operation status of the video surveillance system.

Scene

Front-ends access the network.

Technical Specification

Technical Specification

Model	DH-SACG200-S	DH-SACG1000	DH-SACG5000
Performance	200-channel 4M stream	500-channel 4M stream	1,500-channel 4M stream
Height	1U	1U	1U
Dimensions (W × D × H) (mm)	300 × 430 × 44.5	440 × 423 × 44	440 × 423 × 44
Power Consumption	40W	150W	150W
High Reliability	Hot standby and redundancy design of key components such as VRRP, power supply, and fan.		
Security Access	Authenticate access devices through IP, MAC, allowlist, and 802.1X protocol.		
Protocol Filtering	Supports standard transfer protocols ONVIF, SIP, and most of the Private protocols of mainstream video manufacturers		
Network Adaptability	Inline and bypass traffic direction deployment modes; static routing, RIP v1/2, OSPF, BGP, and policy routing.		
Configuration Management	Local configuration through the Console port		
	Local or remote configuration through Telnet or SSH		
	Remote configuration management through web		
	SNMP v1/v2/v3, unified operation and maintenance management, and NTP time sync		

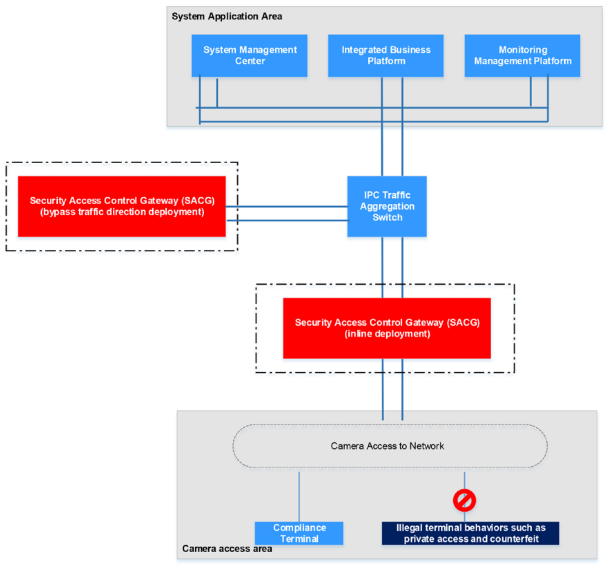
Ordering Information

Type	Model	Description
DH-SACG Series	DH-SACG200-S	Dahua Security Access Control Gateway
	DH-SACG1000	
	DH-SACG5000	

Application

Camera security access control:

SACG can be deployed inline in front of the aggregation switch or mounted on the aggregation switch for security access control of cameras.



Security isolation of the boundary among platforms

SACG can be used as a security isolating device to enable protocol filtering and access control for interactive traffic among platforms.