



Huawei USG6305/6310S/6320 Desktop Next-Generation Firewall



USG6305



USG6305-W



USG6310S



USG6310S-W



USG6310S-WL-OVS



USG6320

Product Overview

Huawei USG6305/6310S/6320 series desktop next-generation firewalls are security gateway products designed for small enterprises, branches, and chain businesses. This series of products integrate various security functions and support multiple IPv4/IPv6 routing protocols, applicable to all kinds of small network access scenarios. The USG6305/6310S/6320 series provides GE and Wi-Fi interfaces in the down link to directly provide Wi-Fi access services and provides GE uplink interfaces and 3G/4G LTE backup links for emergency Internet access services.

The USG6305/6310S/6320 series desktop next-generation firewalls can be deployed with the Agile Controller to form enterprise branch security access solutions, providing unified authentication of wired and wireless users, and portal customization services. Centralized service management can reduce branch management pressures and can also provide flexible service customization platforms for precise marketing in business shops.

Product Features

Comprehensive protection, meeting compliance requirements

- Provides nine professional capabilities, such as the firewall, VPN, and online behavior management capabilities, fully meeting security compliance requirements.
- Supports local storage expansion using a 64 GB SD card, records user access logs (such as IP addresses before and after NAT and URLs), and supports compliance audit.
- Provides a URL category database with 120 million URLs to prevent access to malicious and illegitimate websites to meet the compliance requirements and provides URL blacklist and whitelist to prevent or allow access to specific websites.

Fast deployment, simple management

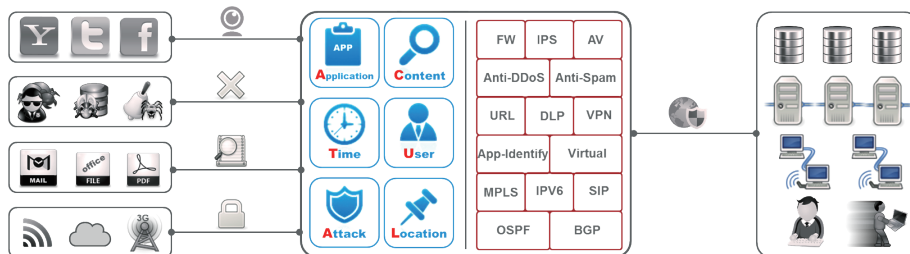
- Matches the cloud management platform. You can purchase the MSP management service to reduce investments on network management software and human resources.
- Supports zero-configuration deployment using the USB disk to improve deployment efficiency.
- Provides a web UI for comprehensive configuration management. You can use an eSight to manage multiple USG6300s.

Flexible bandwidth management, improving Internet access experience

- Identifies common applications and preferentially forwards key application traffic based on application-based bandwidth management.
- Provides differentiated user bandwidth management and quota management for ensure bandwidth for VIPs.
- Allows you to modify the priority of the traffic to specified URL categories to accelerate the access to key websites.

Precise marketing, business development

- Proactively pushes business development services through APP and advertisement.
- Supports various authentication methods, such as portal authentication and allows portal page customization.



LEADING NEW ICT,
BUILDING A BETTER CONNECTED WORLD



Huawei USG6305/6310S/6320

Desktop Next-Generation Firewall

Specifications

Model	USG6305	USG6305-W	USG6310S	USG6310S-W	USG6310S-WL-OVS	USG6320
Fixed port	4× GE(RJ45)	4×GE(RJ45)	8×GE(RJ45)	8×GE(RJ45)	8×GE(RJ45)	8×GE(RJ45)
USB2.0 port	Supported	Supported	Supported	Supported	Supported	Supported
WIFI	-	Supports 2.4G+5G dual-frequency. Supports 802.11a/b/g/n/ac	-	Supports 2.4G+5G dual-frequency. Supports 802.11a/b/g/n/ac	Supports 2.4G+5G dual-frequency. Supports 802.11a/b/g/n/ac	-
4G LTE	The USB port can house a 4G LTE data card.				The slot supports such standards as 4G LTE, 3G UMTS, and 2G GSM. The USB port can house a 4G LTE data card.	The USB port can house a 4G LTE data card.
Product model	Desktop					Desktop
Dimensions (W×D×H) mm	300×220×44					300×220×44.5
Weight (full configuration)	1.7 kg					1.7 kg
Local storage	Optional, can house expandable 64 GB micro SD cards					-
Power consumption	24 W					36 W
AC power supply	100 V to 240 V					100 V to 240 V
Operating environment: (Temperature/ Humidity)	Temperature: 0°C to 45°C Humidity: 5% to 95%					
Non-operating environment	Temperature: -40°C to 70°C Humidity: 5% to 95%					
Certifications						
Software	ICSA Labs: Firewall, IPS, IPSec, SSL VPN CC: EAL4+					
Hardware	CB, CCC, CE-SDOC, ROHS, REACH&WEEE(EU), C-TICK, ETL, FCC&IC, VCCI, BSMI					
Functions						
Context awareness	ACTUAL (Application, Content, Time, User, Attack, Location)-based awareness capabilities					
User authentication methods	Eight authentication methods (local, RADIUS, HWTACACS, SecureID, AD, CA, LDAP, and Endpoint Security), built-in portal and portal redirection.					
Application security	Fine-grained identification of over common application protocols, application-specific action, and online update of protocol databases Combination of application identification and content detection to identify file types and sensitive information to prevent information leaks					
Intrusion prevention	Provides protocol identification to defend against abnormal protocol behaviors. Supports user-defined IPS signatures.					
Web security	Cloud-based URL filtering with a URL category database that contains over 120 million URLs in over 130 categories Defense against web application attacks, such as cross-site scripting and SQL injection attacks HTTP/HTTPS/FTP-based content awareness to defend against web viruses URL blacklist and whitelist and keyword filtering					
Email security	Local whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by attachment type, size, and quantity Virus scanning and notification for POP3/SMTP/IMAP email attachments					
Data security	Data leak prevention based on content awareness File reassembly and data filtering for more than 30 file types (including Word, Excel, PPT, and PDF), and file blocking for more than 120 file types					
Security virtualization	Virtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)					
VPN	VPN technologies: IPSec VPN, SSL VPN, L2TP VPN, and GRE. Huawei-developed VPN client SecoClient to implement remote user access through SSL VPN, L2TP VPN, and L2TP over IPSec VPN					
Routing	IPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, and ACL6					
Working mode	Transparent, routing, or hybrid working mode					
Intelligent management	Evaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation to automatically optimize security policies. Supports policy matching ratio analysis and the detection of conflict and redundant policies to remove them, simplifying policy management. Provides a global configuration view and integrated policy management. The configurations can be completed in one page. Provides visualized and multi-dimensional report display by user, application, content, time, traffic, threat, and URL. Enterprise administrators can perform assessment over the current network security status by the network security report and providing the related optimization suggestions.					