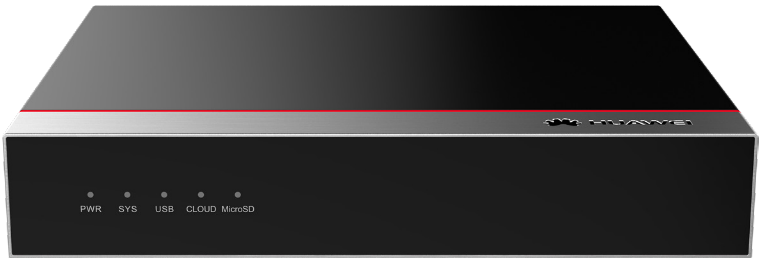
HUAWEI HiSecEngine USG6500E Series Firewalls (Desktop)

Huawei HiSecEngine USG6510E and USG6530E are new-generation desktop firewalls designed for small enterprises, industry branches, and chain business organizations. In addition to the traditional firewall management mode, the cloud-based management mode is supported. The cloud-based management mode provides plug-and-play, automated service configuration, automated and visualized O&M, and big data analytics for a large number of branches to access the network securely. The product provides pattern matching and encryption/decryption service processing acceleration capabilities, which greatly improve the performance for firewalls to process content security detection and IPSec services.

Product Appearances



HiSecEngine USG6500E Series (Desktop)

Product Highlights

Comprehensive and integrated protection

- Integrates the traditional firewall, VPN, intrusion prevention, antivirus, data leak prevention, bandwidth management, and online behavior management functions all in one device.
- Provides refined bandwidth management and guarantees bandwidth for key services based on applications and website categories, so that key services can be preferentially forwarded.

Quick deployment, simple O&M, and cloud-based management

- Initiates authentication and registration to the cloud-based management platform to implement plug-and-play and simplify network creation and deployment.
- Uses remote service configuration management, device monitoring, and fault management, implementing cloud-based management of mass devices and simplifying O&M.

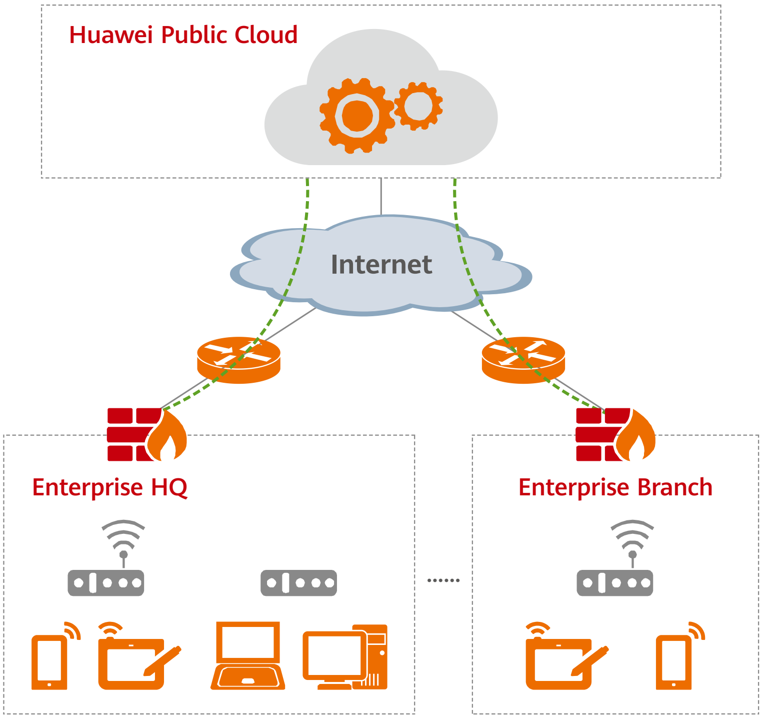
Performance improvement

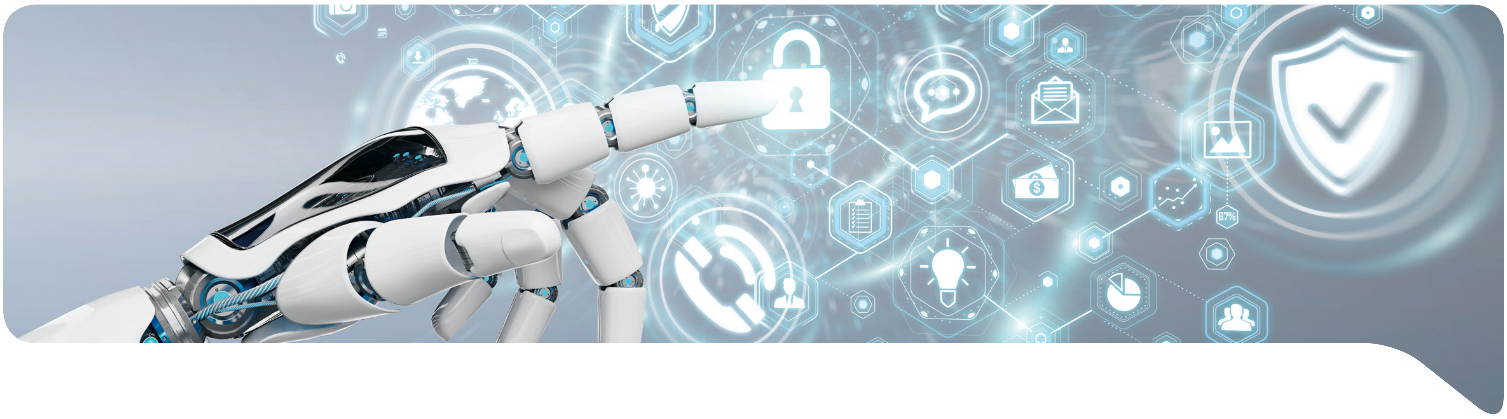
- Enables pattern matching and accelerates encryption/decryption, improving the performance for processing IPS, antivirus, and IPSec services.

Deployment

Cloud-based management

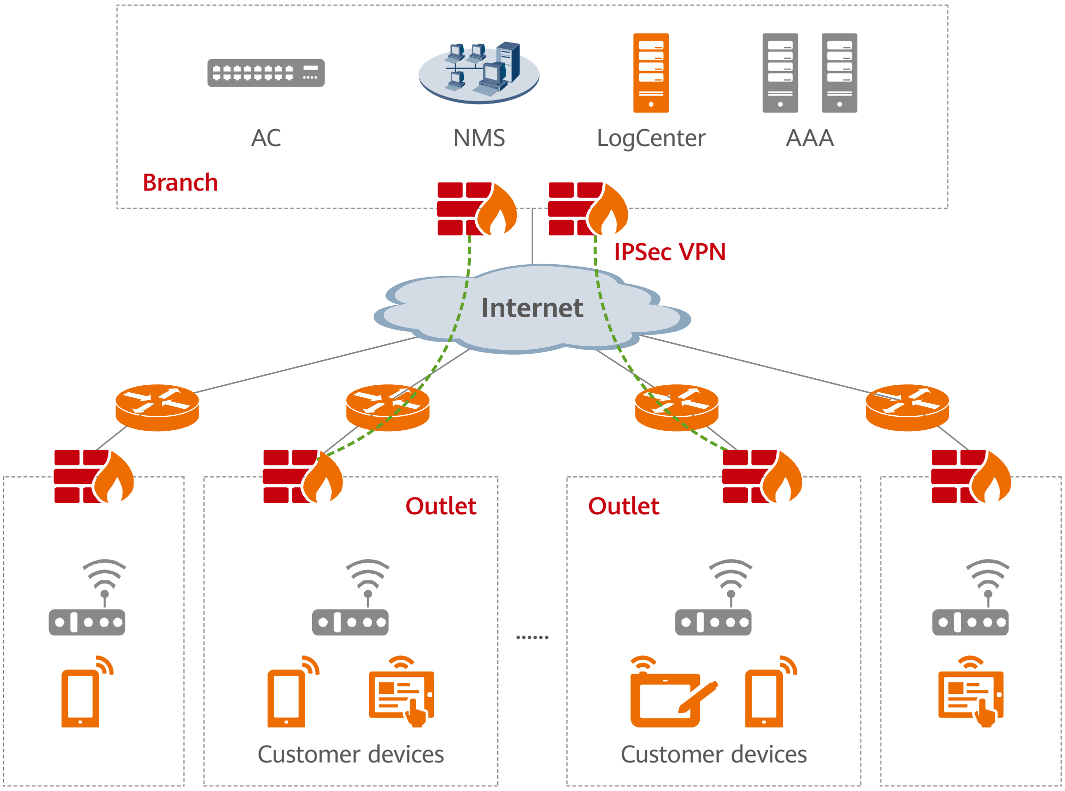
- Firewalls can proactively register with and be quickly incorporated into the cloud-based management platform to implement quick device deployment without manual attendance.
- Remote service configuration management, device monitoring, and fault management are used to implement cloud-based management of mass devices and simplify O&M.





Access to enterprise networks

- The devices support USB-based deployment, simplifying device deployment. Centralized management is supported to reduce device O&M costs.
- IPSec VPN ensures access security. IPSec intelligent uplink selection automatically detects link quality and performs intelligent tunnel switching to ensure service continuity.
- The devices can work with the Agile Controller to form a branch access security solution that provides services such as user authentication and portal customization. This solution implements unified authentication, unified O&M, and unified log management. Centralized service management eases the difficulty of managing branch offices while allowing for platform customization for branches to perform targeted marketing.



Software Features

Feature	Description
Integrated protection	Integrates firewall, VPN, intrusion prevention, antivirus, data leak prevention, bandwidth management, and URL filtering functions; provides a global configuration view and integrated policy management.
Application identification and control	Identifies common applications; supports application-specific access control; combines application identification with intrusion detection, antivirus, and data filtering, improving detection performance and accuracy.
Cloud-based management mode	Initiates authentication and registration to the cloud-based management platform to implement plug-and-play and simplify network creation and deployment. Supports remote service configuration, device monitoring, and fault management, implementing the management of mass devices in the cloud.
Cloud application security awareness	Controls enterprise cloud applications in a refined and differentiated manner to meet enterprises' requirements for cloud application management.
Intrusion prevention and web protection	Accurately detects and defends against vulnerability-specific attacks based on up-to-date threat information. The firewall can defend against web-specific attacks, including SQL injection and XSS attacks.
Antivirus	Rapidly detects over 5 million types of viruses based on the daily-updated virus signature database.
Data leak prevention (DLP)	Inspects files to identify the file types, such as WORD, EXCEL, POWERPOINT, and PDF, based on file content, and filters the file content.
Bandwidth management	Manages per-user and per-IP bandwidth in addition to identifying service applications to ensure the network access experience of key services and users. Control methods include limiting the maximum bandwidth, ensuring the minimum bandwidth, and changing application forwarding priorities.
URL filtering	Provides a URL category database with over 120 million URLs and accelerates access to specific categories of websites, improving access experience of high-priority websites. Supports DNS filtering, in which accessed web pages are filtered based on domain names. Supports the SafeSearch function to filter resources of search engines, such as Google, to guarantee access to only healthy network resources.
Behavior and content audit	Audits and traces the sources of the accessed content based on users.
Load balancing	Supports link load balancing to make full use of existing network resources.
Intelligent uplink selection	Supports service-specific PBR and intelligent uplink selection based on multiple load balancing algorithms (for example, based on bandwidth ratio and link health status) in multi-egress scenarios.
VPN encryption	Supports multiple highly available VPN features, such as IPSec VPN, SSL VPN, L2TP VPN, and GRE, and provides the Huawei-proprietary VPN client SecoClient for SSL VPN, L2TP VPN, and L2TP over IPSec VPN remote access.
DSVPN	Dynamic smart VPN establishes VPN tunnels between branches whose public addresses are dynamically changed, reducing the networking and O&M costs of the branches.
SSL-encrypted traffic detection	Detects and defends against threats in SSL-encrypted traffic using application-layer protection methods, such as intrusion prevention, antivirus, data filtering, and URL filtering.

Feature	Description
User authentication	Supports multiple user authentication methods, including local, RADIUS, HWTACACS, AD, and LDAP; supports built-in Portal and Portal redirection functions; works with the Agile Controller to implement multiple authentication modes.
Security virtualization	Supports virtualization of multiple types of security services, including firewall, intrusion prevention, antivirus, and VPN. Users can separately conduct personal management on the same physical device.
Policy Management	Manages and controls traffic based on VLAN IDs, quintuples, security zones, regions, applications, URL categories, and time ranges, and implements integrated content security detection. Provides predefined common-scenario defense templates to facilitate security policy deployment.
Diversified reports	Provides visualized and multi-dimensional report display by user, application, content, time, traffic, threat, and URL. Generates network security analysis reports on the Huawei security center platform to evaluate the current network security status and provide optimization suggestions.
Routing	Supports multiple types of routing protocols and features, such as RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+, and IPv6 IS-IS.
Deployment mode	Supports transparent, routing, and hybrid working modes.

1. The HiSecEngine USG6510E supports the detection of 2 million viruses.

Specifications

System Performance and Capacity

Model	USG6510E	USG6530E
Firewall Throughput[1] (1518/512/64-byte, UDP)	1.2/1.2/1.2 Gbit/s	4/4/3.6 Gbit/s
Firewall Latency (64-byte, UDP)	15 μs	18 μs
FW + SA + IPS Throughput[2]	0.6 Gbit/s	1.5 Gbit/s
FW + SA + IPS + Antivirus Throughput[2]	0.6 Gbit/s	1.5 Gbit/s
Concurrent Sessions (HTTP1.1)[1]	300,000	500,000
New Sessions/Second (HTTP1.1)[1]	20,000	30,000
Maximum IPsec VPN Tunnels (GW to GW)	1,000	2,000
Maximum IPsec VPN Tunnels (Client to GW)	1,000	2,000
IPsec VPN Throughput[1] (AES-256 + SHA256, 1420-byte)	1 Gbit/s	3 Gbit/s

Model	USG6510E	USG6530E
SSL Inspection Throughput[3]	200 Mbit/s	300 Mbit/s
Concurrent SSL VPN Users (Default/Maximum)	100/100	100/500
Security Policies (Maximum)	1,000	3,000
Virtual Firewalls	10	20
URL Filtering: Categories	More than 130	
URL Filtering: URLs	A database of over 120 million URLs in the cloud	
Automated Threat Feedback and IPS Signature Updates	Yes, an industry-leading security center from Huawei (http://sec.huawei.com/sec/web/index.do)	
Third-Party and Open-Source Ecosystem	Open API for integration with third-party products, providing RESTful and NetConf interfaces Other third-party management software based on SNMP, SSH, and Syslog Cooperation with third-party tools, such as Tufin, AlgoSec, and FireMon Collaboration with anti-APT solution	
Centralized Management	Centralized configuration, logging, monitoring, and reporting is performed by Huawei eSight.	
VLANs (Maximum)	4094	
VLANIF Interfaces (Maximum)	256	1024

1. The performance is tested under ideal conditions based on RFC2544 and RFC3511. The actual result may vary with deployment environments.
2. The Antivirus, IPS, and SA performance is measured using 100 KB HTTP files.
3. SSL inspection throughput is measured with IPS enabled and HTTPS traffic using TLS v1.2 with AES128-GCM-SHA256.

*SA: indicates service awareness.

Hardware Specifications

Model	USG6510E	USG6530E
Dimensions (H x W x D) mm	43.6 x 250 x 210	
Form Factor/Height	Desktop	
Fixed Interface	2 x GE (SFP) + 10 x GE	2 x 10GE (SFP+) + 10 x GE
USB Port	1 x USB 3.0	
Weight (Full Configuration)	1.5 kg	
External Storage	Optional, Micro-SD card supported, 64 GB	
AC Power Supply	100V to 240V	
Power	36 W	
Power Supplies	External power adapter	

Model	USG6510E	USG6530E

Operating Environment (Temperature/Humidity)	Temperature: 0°C to 45°C;
	Humidity: 5% to 95%, non-condensing;	

Non-operating Environment	Temperature: -40°C to +70°C Humidity: 5% to 95%, non-condensing;	

Ordering Information

Product	Model	Description
USG6510E	USG6510E-AC	USG6510E AC Host (2*GE (SFP) + 10*GE, with AC/DC Adapter)
USG6530E	USG6530E-AC	USG6530E AC Host (2*10GE (SFP+) + 10*GE, with AC/DC Adapter)
Function License		
SSL VPN Concurrent Users	LIC-USG6KE-SSLVPN-100	Quantity of SSL VPN Concurrent Users (100 Users)
	LIC-USG6KE-SSLVPN-200	Quantity of SSL VPN Concurrent Users (200 Users)
	LIC-USG6KE-SSLVPN-500	Quantity of SSL VPN Concurrent Users (500 Users)
NGFW License		
Threat Protection Bundle (IPS, AV, URL)	LIC-USG6510E-TP-1Y	Threat Protection Subscription 12 Months (Applies to USG6510E)
	LIC-USG6510E-TP-3Y	Threat Protection Subscription 36 Months (Applies to USG6510E)
	LIC-USG6530E-TP-1Y	Threat Protection Subscription 12 Months (Applies to USG6530E)
	LIC-USG6530E-TP-3Y	Threat Protection Subscription 36 Months (Applies to USG6530E)
Cloud Sandbox Inspection	LIC-USG6530E-CS-1Y	Cloud Sandbox Inspection 12 Months (Applies to USG6530E)
	LIC-USG6530E-CS-3Y	Cloud Sandbox Inspection 36 Months (Applies to USG6530E)
N1 License		
Foundation package function	N1-USG6510E-F-Lic	N1-USG6510E Foundation, Per Device
	N1-USG6530E-F-Lic	N1-USG6530E Foundation, Per Device

Note: Some parts of this table list the sales strategies in different regions. For more information, please contact your Huawei representative.

GENERAL DISCLAIMER

The information in this document may contain predictive statement including, without limitation, statements regarding the future financial and operating results, future product portfolios, new technologies, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.