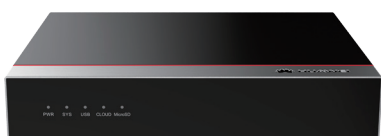# Huawei USG6510E/USG6510E-POE/ USG6530E Next-Generation Firewalls

USG6510E/USG6510E-POE/USG6530E

Overview

Huawei USG6510E, USG6510E-POE and USG6530E are next-generation desktop firewalls designed for small enterprises, industry branches, and chain business organizations. In addition to the traditional firewall management mode, the cloud management mode is supported. The cloud management mode provides plug-and-play, automated service configuration, automated and visualized O&M, and big data analysis for a large number of branches to access the network securely. The network processing chip based on the ARM architecture 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 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, cloud management

- Initiates authentication and registration to the cloud 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.

Chip-based performance improvement

- Uses the network processing chip based on the ARM architecture, improving forwarding performance significantly.
- Enables chip-level pattern matching and accelerates encryption/ decryption, improving the performance for processing IPS, antivirus, and IPSec services.

Deployment

Cloud-based management

- Firewalls proactively register with and quickly incorporated into the cloud 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.

HUAWEI TECHNOLOGIES CO., LTD.

Specifications

System Performance and Capacity

Model	USG6510E	USG6510E-POE	USG6530E
IPv4 Firewall Throughput[1] (1518/512/64-byte, UDP)	1.2/1.2/1 Gbit/s	1.2/1.2/1 Gbit/s	4/4/1.2 Gbit/s
FW+SA*+IPS Throughput[2]	0.6 Gbit/s	0.6 Gbit/s	1.5 Gbit/s
Full Protection Throughput[3]	0.45 Gbit/s	0.45 Gbit/s	1.1 Gbit/s
Concurrent Sessions[1] (TCP)	300,000	300,000	500,000
New Sessions/Second[1] (TCP)	20,000	20,000	30,000
IPSec VPN Throughput[1] (AES-256+SHA256, 1420-byte)	1 Gbit/s	1 Gbit/s	2 Gbit/s
Maximum IPSec VPN Tunnels	1,000	1,000	2,000
SSL Inspection Throughput[4]	200 Mbit/s	200 Mbit/s	300 Mbit/s
SSL VPN Throughput[5]	200 Mbit/s	200 Mbit/s	300 Mbit/s
Concurrent SSL VPN Users (Default/Maximum)	100/100	100/100	100/500
Firewall Policies (Maximum)	1,000	1,000	3,000
Virtual Firewalls (Maximum)	10	10	20
Dimensions (H×W×D) mm	44×250×210		
Form Factor/Height	Desktop		
Fixed Interface	2×GE(SFP)+10×GE	2×GE(SFP)+10×GE(GE0/0/0 to GE 0/0/3 support PoE)	2×10GE(SFP+)+10×GE
USB Port	1×USB 2.0 Ports		
MTBF	57.29 years		
Weight (Full Configuration)	1.5 kg		
Local Storage	Optional, a 128 GB Micro-SD card can be added		
AC Power Supply	100V to 240V, 50/60Hz		
Power Consumption (Average/Maximum)	17.3W/19.6W	82.8W/85.1W	19.3W/21.1W
Power Supplies	External Power Adapters		
Operating Environment (Temperature/Humidity)	Temperature: 0°C to 45°C Humidity: 5% to 95%, non-condensing		
URL Filtering: URLs	Can access a database of over 120 million URLs in the cloud		
Automated Threat Feed and IPS Signature Updates	Yes, an industry-leading security center from Huawei (http://sec.huawei.com/sec/web/index.do)		
High Availability Configurations	Active/Active, Active/Standby		
Certifications			
Hardware	CB, CE-SDOC, ROHS, REACH&WEEE(EU), RCM, NRTL, FCC&IC, CCC, VCCI		

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. The firewall combines application identification with intrusion detection, antivirus, and data filtering, improving detection performance and accuracy.
Cloud-based management mode	The firewall initiates authentication and registration to the cloud management platform to implement plug-and-play and simplify network creation and deployment. Service configuration, device monitoring, and fault management can be performed remotely, 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 million6 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-developed VPN client SecoClient for SSL VPN, L2TP VPN, and L2TP over IPSec VPN remote access.
DSVPN	Dynamic smart VPN (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.
User authentication	Supports multiple user authentication methods, including local, RADIUS, HWTACACS, AD, and LDAP. The firewall supports built-in Portal and Portal redirection functions. It can work 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. Provides security policy management solutions in partnership with FireMon and AlgoSec to reduce O&M costs and potential faults.
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 performance is tested under ideal conditions based on RFC2544, 3511. The actual result may vary with deployment environments.
2. Antivirus, IPS, and SA performances are measured using 100 KB HTTP files.
3. Full protection throughput is measured with Firewall, SA, IPS, Antivirus and URL Filtering enabled. Antivirus, IPS and SA performances are measured using 100 KB HTTP files.
4. SSL inspection throughput is measured with IPS enabled and HTTPS traffic using TLS v1.2 with AES128-GCM-SHA256.
5. SSL VPN throughput is measured using TLS v1.2 with AES128-SHA.
6. The USG6510E/USG6510E-POE supports the detection of 2 million viruses.
*SA: Service Awareness.

About This Publication