Huawei USG6712E/USG6716E Next-Generation Firewalls

With the continuous digitalization and cloudification of enterprise services, networks play an important role in enterprise operations, and must be protected. Network attackers use various methods, such as identity spoofing, website Trojan horses, and malware, to initiate network penetration and attacks, affecting the normal use of enterprise networks.

Deploying firewalls on network borders is a common way to protect enterprise network security. However, firewalls can only analyze and block threats based on signatures. This method cannot effectively handle unknown threats and may deteriorate device performance. This single-point and passive method does not pre-empt or effectively defend against unknown threat attacks. Threats hidden in encrypted traffic in particular cannot be effectively identified without breaching user privacy.

Huawei's next-generation firewalls provide the latest capabilities and work with other security devices to proactively defend against network threats, enhance border detection capabilities, effectively defend against advanced threats, and resolve performance deterioration problems. Network Processors provide firewall acceleration capability, which greatly improves the firewall throughput.

Product Appearances

USG6712E/USG6716E

HUAWEI

Product Highlights

Comprehensive and integrated protection

- Integrates the traditional firewall, VPN, intrusion prevention, antivirus, data leak prevention, bandwidth management, URL filtering, and online behavior management functions all in one device.
- Interworks with the local or cloud sandbox to effectively detect unknown threats and prevent zero-day attacks.
- Implements refined bandwidth management based on applications and websites, preferentially forwards key services, and ensures bandwidth for key services.

More comprehensive defense

- The built-in traffic probe of a firewall extracts traffic information and reports it to the CIS, a security big data analysis platform developed by Huawei. The CIS analyzes threats in the traffic, without decrypting the traffic or compromising the device performance. The threat identification rate is higher than 90%.
- The deception system proactively responds to hacker scanning behavior and quickly detects and records malicious behavior, facilitating forensics and source tracing.

High performance

- 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.
- The throughput of a 1U device can reach 160 Gbit/s.

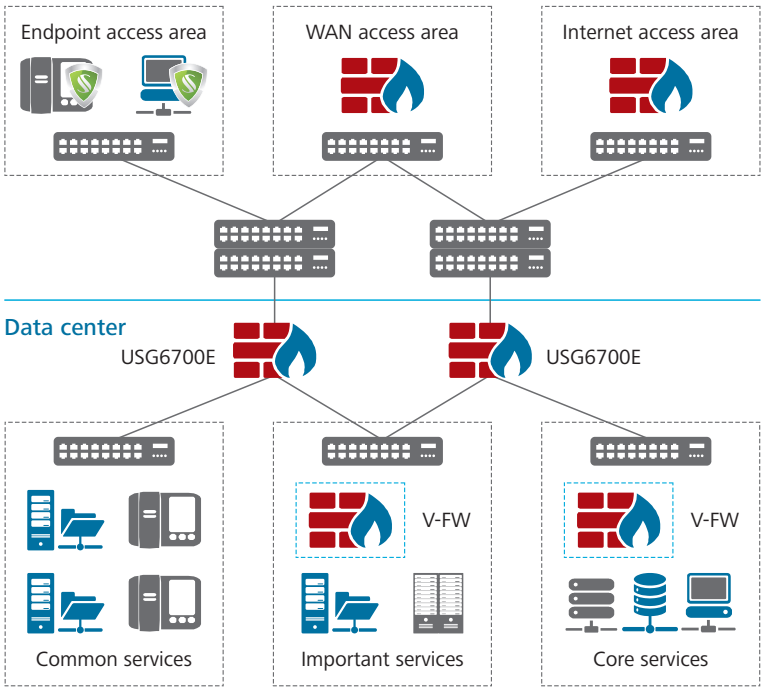
High port density

- The device has multiple types of interfaces, such as 100G, 40G, and 10G interfaces. Services can be flexibly expanded without extra interface cards.

Deployment

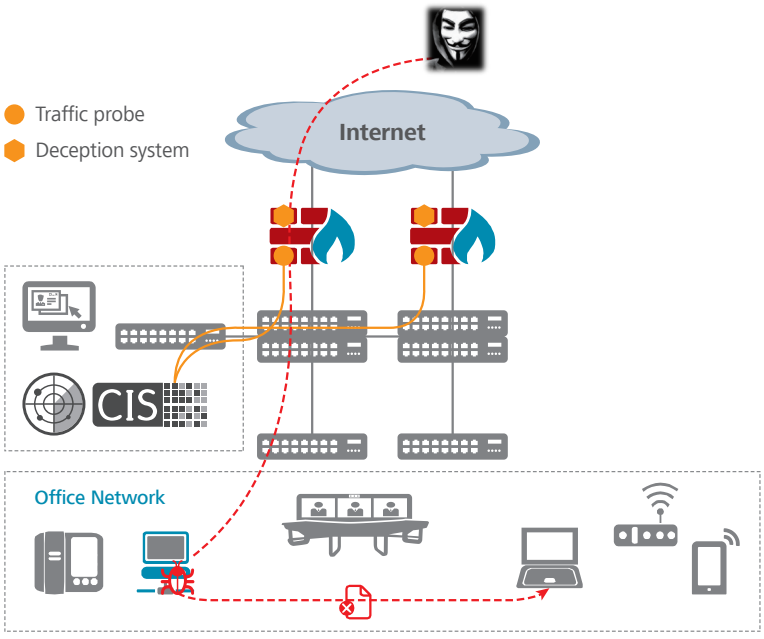
Data center border protection

- Firewalls are deployed at egresses of data centers, and functions and system resources can be virtualized. The firewall has multiple types of interfaces, such as 100G, 40G, and 10G interfaces. Services can be flexibly expanded without extra interface cards.
- The 18-Gigabit intrusion prevention capability effectively blocks a variety of malicious attacks and delivers differentiated defense based on virtual environment requirements to guarantee data security.
- VPN tunnels can be set up between firewalls and mobile workers and between firewalls and branch offices for secure and low-cost remote access and mobile working.



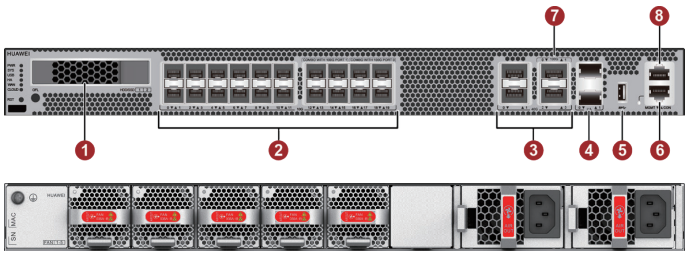
Enterprise border protection

- Firewalls are deployed at the network border. The built-in traffic probe extracts packets of encrypted traffic and sends the packets to the CIS, a big data analysis platform. In this way, threats in encrypted traffic are monitored in real time. Encrypted traffic does not need to be decrypted, protecting user privacy and preventing device performance deterioration.
- The deception function in enabled on the firewalls to proactively respond to malicious scanning behavior and associate with the CIS for behavior analysis to quickly detect and record malicious behavior, protecting enterprise against threats in real time.
- The policy control, data filtering, and audit functions of the firewalls are used to monitor social network applications to prevent data breach and protect enterprise networks.



Hardware

USG6712E/USG6716E



1. HDD/SSD Slot
2. 20 x 10GE (SFP+)
3. 4 x 40GE (QSFP+)
4. 2 x HA (SFP+)
5. 1 x USB3.0
6. 1 x GE (RJ45) management port
7. 2 x 100GE (QSFP28)
8. Console port

Software Features

Feature	Description
Integrated protection	Integrates firewall, VPN, intrusion prevention, antivirus, data leak prevention, bandwidth management, anti-DDoS, URL filtering, and anti-spam functions. Provides a global configuration view, and manages policies in a unified manner.
Application identification and control	Identifies over 6000 applications and supports the access control granularity down to application functions. 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 million types of viruses based on the daily-updated virus signature database.

Feature	Description
Anti-APT	Collaborates with the local or cloud sandbox to detect and block malicious files. Supports the flow probe information collection function to collect traffic information and send the collected information to the CIS(Cybersecurity Intelligence System) for analysis, evaluation, and identification of threats and APT attacks. Encrypted traffic does not need to be decrypted. The firewall can work with the CIS to detect threats in encrypted traffic. The firewall can proactively respond to malicious scanning behavior and work with the CIS to analyze behavior, quickly detect and record malicious behavior, and protect enterprises against threats in real time.
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 server load balancing and link load balancing, fully utilizing 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, MPLS 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 (DSVPN) 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
SSL offloading	Replaces servers to implement SSL encryption and decryption, effectively reducing server loads and implementing HTTP traffic load balancing.
Anti-DDoS	Defends against more than 10 types of common DDoS attacks, including SYN flood and UDP flood attacks.
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.
Security 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 and reliability	Supports transparent, routing, and hybrid working modes and high availability (HA), including the Active/Active and Active/Standby modes.

Specifications

System Performance and Capacity

Model	USG6712E	USG6716E
IPv4 Firewall Throughput[1] (1518/512/64-byte, UDP)	120/120/100 Gbit/s	160/160/100 Gbit/s
IPv6 Firewall Throughput[1] (1518/512/84-byte, UDP)	120/120/26 Gbit/s	160/120/26 Gbit/s
Firewall Throughput (Packet Per Second)	150 Mpps	150 Mpps
Firewall Latency (64-byte, UDP)	15 μs	15 μs

Model	USG6712E	USG6716E
FW+SA* Throughput[2]	55 Gbit/s	60 Gbit/s
FW+SA+IPS Throughput[2]	40 Gbit/s	40 Gbit/s
FW+SA+IPS+Antivirus Throughput[2]	35 Gbit/s	38 Gbit/s
Full Protection Throughput[3]	33 Gbit/s	36 Gbit/s
Full protection Throughput (Realworld)[4]	16 Gbit/s	18 Gbit/s
Concurrent Sessions (HTTP1.1)[1]	35,000,000	50,000,000
New Sessions/Second (HTTP1.1)[1]	1,400,000	1,600,000
IPSec VPN Throughput[1] (AES-256+SHA256, 1420-byte)	100 Gbit/s	120 Gbit/s
Maximum IPsec VPN Tunnels (GW to GW)	120,000	120,000
Maximum IPsec VPN Tunnels (Client to GW)	120,000	120,000
SSL Inspection Throughput[5]	18 Gbit/s	18 Gbit/s
SSL VPN Throughput[6]	10 Gbit/s	12 Gbit/s
Concurrent SSL VPN Users (Default/Maximum)	100/30000	100/30000
Firewall Policies (Maximum)	60,000	60,000
Virtual Firewalls (Maximum)	1,000	1,000
URL Filtering: Categories	More than 130	
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)	
Third-Party and Open-Source Ecosystem	Open API for integration with third-party products, providing RESTful and NetConf interface Other third-part management software based on SNMP, SSH, Syslog Co-operation 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 and eLog	
VLANs (Maximum)	4094	
VLANIF Interfaces (Maximum)	1024	

Model	USG6712E	USG6716E
High Availability Configurations	Active/Active, Active/Standby	

1. 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. Full protection throughput (Realworld) is measured with Firewall, SA, IPS, Antivirus and URL Filtering enabled, Enterprise Mix Traffic Model.
5. SSL inspection throughput is measured with IPS-enabled and HTTPS traffic using TLS v1.2 with AES128-GCM-SHA256.
6. SSL VPN throughput is measured using TLS v1.2 with AES128-SHA.

*SA: Service Awareness.

Note: All data in this document is based on USG V600R006.

Hardware Specifications

Model	USG6712E	USG6716E
Dimensions (H x W x D) mm	44 x 442 x 600	
Form Factor/Height	1U	
Fixed Interface	2*100G (QSFP28) + 2*40G (QSFP+) + 20*10GE (SFP+) + 2*10GE (SFP+) HA[1]	
USB Port	1 x USB 3.0	
MTBF	25 years	
Weight (Full Configuration)	12 kg	
Local Storage	Optional, SSD (1*2.5inch) supported, 240G/HDD (1*2.5inch supported, 1TB	
AC Power Supply	100V to 240V, 50/60Hz	
Power Consumption (Average/Maximum)	382.9W/566W	
Heat Dissipation	>1935.3 BTU/h	
Power Supplies	Dual AC power supplies	
Operating Environment (Temperature/Humidity)	Temperature: 0°C to 45°C (without optional HDD); 5°C to 40°C (with optional HDD) Humidity: 5% to 95% (without optional HDD), non-condensing; 5% to 95% (with optional HDD), non-condensing	
Non-operating Environment	Temperature: -40°C to +70°C Humidity: 5% to 95% (without optional HDD), non-condensing; 5% to 95% (with optional HDD), non-condensing	
Operating Altitude (maximum)	5,000 meters (without optional HDD); 3,000 meters (with optional HDD)	

Model	USG6712E	USG6716E
Non-operating Altitude (maximum)	5,000 meters (without optional HDD); 3,000 meters (with optional HDD)	
Noise	Maximum value < 72 dBA	

1. Some 10G ports and 100G ports are mutually exclusive. The ports can be configured as follows: 2 * 100G (QSFP28) + 2 * 40G (QSFP+) + 12 * 10GE (SFP+) + 2 * 10GE (SFP+) HA or 4 * 40G (QSFP+) + 20 * 10GE (SFP+) + 2 * 10GE (SFP+) HA

Certifications

Certifications	
Hardware	CB, CE-SDOC, ROHS, REACH&WEEE(EU), RCM, NRTL, FCC&IC, CCC, VCCI

Regulatory, Safety, and EMC Compliance

Certifications	
Regulatory Compliance	Products comply with EU directives 2014/30/EU (Low Voltage Directive), 2014/35/EU (EMC Directive), and 2011/65/EU (RoHS Directive).
Safety	• UL 60950-1 • CSA-C22.2 No. 60950-1 • EN 60950-1 • IEC 60950-1
EMC: Emissions	• EN55032 Class A • CISPR 32 Class A • ETSI EN 300 386 • AS/NZS CIPSR 32 • CAN/CSA-CISPR 32-17 • IEC 61000-3-2/EN 61000-3-2 • IEC 61000-3-3/EN 61000-3-3 • FCC CFR47 Part 15 Subpart B Class A • ICES-003 Class A • VCCI V-3 Class A
EMC: Immunity	• EN 55024 • CISPR 24 • ETSI EN 300 386

Ordering Guide

Product	Model	Description
USG6712E	USG6712E-AC	USG6712E AC Host (2*100G (QSFP28) + 2*40G (QSFP+) + 20*10GE (SFP+) + 2*10GE (SFP+) HA AC Power)
USG6716E	USG6716E-AC	USG6716E AC Host (2*100G (QSFP28) + 2*40G (QSFP+) + 20*10GE (SFP+) + 2*10GE (SFP+) HA, AC Power)
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)
	LIC-USG6KE-SSLVPN-1000	Quantity of SSL VPN Concurrent Users (1000 Users)
	LIC-USG6KE-SSLVPN-2000	Quantity of SSL VPN Concurrent Users (2000 Users)
	LIC-USG6KE-SSLVPN-5000	Quantity of SSL VPN Concurrent Users (5000 Users)
Virtual Firewall	LIC-USG6KE-VSYS-10	Quantity of Virtual Firewall (10 Vsys)
	LIC-USG6KE-VSYS-20	Quantity of Virtual Firewall (20 Vsys)
	LIC-USG6KE-VSYS-50	Quantity of Virtual Firewall (50 Vsys)
	LIC-USG6KE-VSYS-100	Quantity of Virtual Firewall (100 Vsys)
	LIC-USG6KE-VSYS-200	Quantity of Virtual Firewall (200 Vsys)
	LIC-USG6KE-VSYS-500	Quantity of Virtual Firewall (500 Vsys)
	LIC-USG6KE-VSYS-1000	Quantity of Virtual Firewall (1000 Vsys)
NGFW License		
IPS Update Service	LIC-USG6712E-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6712E)
	LIC-USG6712E-IPS-3Y	IPS Update Service Subscribe 36 Months (Applies to USG6712E)
	LIC-USG6716E-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6716E)
	LIC-USG6716E-IPS-3Y	IPS Update Service Subscribe 36 Months (Applies to USG6716E)
URL Filtering Update Service	LIC-USG6712E-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6712E)
	LIC-USG6712E-URL-3Y	URL Update Service Subscribe 36 Months (Applies to USG6712E)

Product	Model	Description
	LIC-USG6716E-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6716E)
	LIC-USG6716E-URL-3Y	URL Update Service Subscribe 36 Months (Applies to USG6716E)
Antivirus Update Service	LIC-USG6712E-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6712E)
	LIC-USG6712E-AV-3Y	AV Update Service Subscribe 36 Months (Applies to USG6712E)
	LIC-USG6716E-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6716E)
	LIC-USG6716E-AV-3Y	AV Update Service Subscribe 36 Months (Applies to USG6716E)
Threat Protection Bundle (IPS, AV, URL)	LIC-USG6712E-TP-1Y-OVS	Threat Protection Subscription 12 Months (Applies to USG6712E)
	LIC-USG6712E-TP-3Y-OVS	Threat Protection Subscription 36 Months (Applies to USG6712E)
	LIC-USG6716E-TP-1Y-OVS	Threat Protection Subscription 12 Months (Applies to USG6716E)
	LIC-USG6716E-TP-3Y-OVS	Threat Protection Subscription 36 Months (Applies to USG6716E)
Cloud Sandbox Inspection	LIC-USG67E-01-CS-1Y	Cloud Sandbox Inspection 12 Months (Applies to USG6712E)
	LIC-USG67E-01-CS-3Y	Cloud Sandbox Inspection 36 Months (Applies to USG6712E)
	LIC-USG67E-02-CS-1Y	Cloud Sandbox Inspection 12 Months (Applies to USG6716E)
	LIC-USG67E-02-CS-3Y	Cloud Sandbox Inspection 36 Months (Applies to USG6716E)
Flow Probe	LIC-USG6712E-FP	Flow Probe Function (Applies to USG6712E)
	LIC-USG6716E-FP	Flow Probe Function (Applies to USG6716E)

About This Publication

This publication is for reference only and does not constitute any commitments or guarantees. All trademarks, pictures, logos, and brands mentioned in this document are the property of Huawei Technologies Co., Ltd. or a third party.
For more information, visit http://e.huawei.com/en/products/enterprise-networking/security.