

HUAWEI HiSecEngine USG6600E Series Firewalls (Fixed-Configuration)

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. The product provides pattern matching and encryption/decryption service processing acceleration functions, which greatly improve the firewall ability to process content security detection and IPSec services.

Product Appearances



HiSecEngine USG6600E Series (Fixed-Configuration)





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.
- Intelligent defense: DGA malicious domain name detection, malicious C&C detection, malicious encrypted C&C detection, and new brute-force cracking detection.

High performance

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

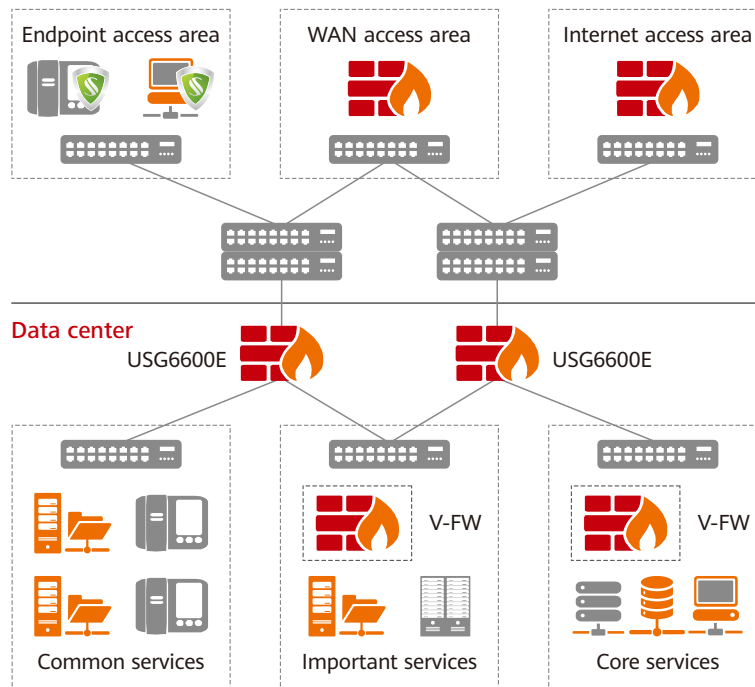
High port density

- The device has multiple types of interfaces, such as 40G, 10G, and 1G interfaces. Services can be flexibly expanded without extra interface cards.

Deployment

Small 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 40G, 10G, and 1G interfaces. Services can be flexibly expanded without extra interface cards.
- The 12-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 can extract packets of encrypted traffic to monitor threats in encrypted traffic in real time.
- The deception function is enabled on the firewalls to proactively respond to malicious scanning behavior, protecting enterprises 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.

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; manages policies in a unified manner.
Application identification and control	Identifies over 6000 applications and supports the access control granularity down to application functions; 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.

Feature	Description
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 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-proprietary 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.
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.

Feature	Description
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.
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	USG6605E-B	USG6615E	USG6625E	USG6635E	USG6655E
Firewall Throughput ¹ (1518/512/64-byte, UDP)	10/10/4 Gbit/s	12/12/12 Gbit/s	20/20/20 Gbit/s	30/30/30 Gbit/s	40/40/38 Gbit/s
Firewall Latency (64-byte, UDP)	18 μs	15 μs	15 μs	15 μs	15 μs
FW + SA + IPS Throughput ²	2.2 Gbit/s	10 Gbit/s	10 Gbit/s	13 Gbit/s	15 Gbit/s
FW + SA + IPS + Antivirus Throughput ²	2.2 Gbit/s	10 Gbit/s	10 Gbit/s	12 Gbit/s	14 Gbit/s
Concurrent Sessions (HTTP1.1) ¹	6,000,000	6,000,000	8,000,000	12,000,000	12,000,000
New Sessions/Second (HTTP1.1) ¹	80,000	200,000	200,000	400,000	400,000
Maximum IPsec VPN Tunnels (GW to GW)	4,000	8,000	8,000	15,000	15,000
Maximum IPsec VPN Tunnels (Client to GW)	4,000	8,000	8,000	15,000	15,000
IPsec VPN Throughput ¹ (AES-256 + SHA256, 1420-byte)	6 Gbit/s	10 Gbit/s	15 Gbit/s	20 Gbit/s	30 Gbit/s
SSL Inspection Throughput ³	550 Mbit/s	3 Gbit/s	3 Gbit/s	6 Gbit/s	6 Gbit/s
Concurrent SSL VPN Users (Default/Maximum)	100/1000	100/2000	100/2000	100/5000	100/5000
Security Policies (Maximum)	15,000	40,000	40,000	40,000	40,000
Virtual Firewalls	100	200	500	500	1000
URL Filtering: Categories	More than 130				
URL Filtering: URLs	A database of over 120 million URLs in the cloud				

Model	USG6605E-B	USG6615E	USG6625E	USG6635E	USG6655E
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-part management software based on SNMP, SSH, and Syslog Co-operation with third-party tools, such as Tufin, AlgoSec, and FireMmon Collaboration with anti-APT solution				
Centralized Management	Centralized configuration, logging, monitoring, and reporting is performed by Huawei eSight				
VLANs (Maximum)	4094				
VLANIF Interfaces (Maximum)	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.
 4. Some 10G ports and 40G ports are mutually exclusive. The ports can be configured as follows: 2 x 40GE (QSFP+) + 8 x 10GE (SFP+) + 16 x GE (RJ45) + 1 x USB or 1 x 40GE (QSFP+) + 12 x 10GE (SFP+) + 16 x GE (RJ45) + 1 x USB.
- *SA: indicates service awareness.

Hardware Specifications

Model	USG6605E-B	USG6615E	USG6625E	USG6635E	USG6655E
Dimensions (H x W x D) mm	43.6 x 442 x 420				
Form Factor/Height	1U				
Fixed Interface	16×GE (RJ45) + 8×GE Combo + 2×10GE (SFP+)	6×10GE (SFP+) + 6×GE (SFP) + 16×GE (RJ45)	2×40GE (QSFP+) + 12×10GE (SFP+) + 16×GE *(RJ45)		
Dedicated management port	Yes				
Bypass Port	Yes	--			
USB Port	1×USB 3.0	1×USB 2.0			
Weight	6.25kg	6.5kg	7.75		
External Storage	Optional SSD (1×2.5 inch) supported, 240 GB, HDD 1TB	Optional SSD (1×2.5 inch) supported, 240 GB, HDD 1TB			
Power Supply	100 V to 240 V				
Max power consumption of the machine	76.9W	118W	156W		
Power Supplies	Optional dual AC power supplies			Dual AC power supplies	
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				

*Some 10G ports and 40G ports are mutually exclusive. The ports can be configured as follows: 2 x 40GE (QSFP+) + 8 x 10GE (SFP+) + 16 x GE (RJ45) + 1 x USB or 1 x 40GE (QSFP+) + 12 x 10GE (SFP+) + 16 x GE (RJ45) + 1 x USB.

Ordering Information

Product	Model	Description
USG6605E	USG6605E-B-AC	USG6615E-B AC Host (16*GE (RJ45) + 8*GE Combo + 2*10GE SFP+, 1 AC power supply)
USG6615E	USG6615E-AC	USG6615E AC Host (6*10GE (SFP+) + 6*GE (SFP) + 16*GE, 1 AC power supply)
USG6625E	USG6625E-AC	USG6625E AC Host (6*10GE (SFP+) + 6*GE (SFP) + 16*GE, 1 AC power supply)
USG6635E	USG6635E-AC	USG6635E AC Host (2*40GE (QSFP+) + 12*10GE (SFP+) + 16*GE, 2 AC power supplies)
USG6655E	USG6655E-AC	USG6655E AC Host (2*40GE (QSFP+) + 12*10GE (SFP+) + 16*GE, 2 AC power supplies)
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-USG6605E-B-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6605E-B)
	LIC-USG6605E-B-IPS-3Y	IPS Update Service Subscribe 36 Months (Applies to USG6605E-B)
	LIC-USG6615E-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6615E)
	LIC-USG6615E-IPS-3Y	IPS Update Service Subscribe 36 Months (Applies to USG6615E)
	LIC-USG6625E-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6625E)
	LIC-USG6625E-IPS-3Y	IPS Update Service Subscribe 36 Months (Applies to USG6625E)
	LIC-USG6635E-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6635E)
	LIC-USG6635E-IPS-3Y	IPS Update Service Subscribe 36 Months (Applies to USG6635E)

Product	Model	Description
	LIC-USG6655E-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6655E)
	LIC-USG6655E-IPS-3Y	IPS Update Service Subscribe 36 Months (Applies to USG6655E)
URL Filtering Update Service	LIC-USG6605E-B-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6605E-B)
	LIC-USG6605E-B-URL-3Y	URL Update Service Subscribe 36 Months (Applies to USG6605E-B)
	LIC-USG6615E-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6615E)
	LIC-USG6615E-URL-3Y	URL Update Service Subscribe 36 Months (Applies to USG6615E)
	LIC-USG6625E-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6625E)
	LIC-USG6625E-URL-3Y	URL Update Service Subscribe 36 Months (Applies to USG6625E)
	LIC-USG6635E-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6635E)
	LIC-USG6635E-URL-3Y	URL Update Service Subscribe 36 Months (Applies to USG6635E)
	LIC-USG6655E-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6655E)
	LIC-USG6655E-URL-3Y	URL Update Service Subscribe 36 Months (Applies to USG6655E)
Antivirus Update Service	LIC-USG6605E-B-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6605E-B)
	LIC-USG6605E-B-AV-3Y	AV Update Service Subscribe 36 Months (Applies to USG6605E-B)
	LIC-USG6615E-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6615E)
	LIC-USG6615E-AV-3Y	AV Update Service Subscribe 36 Months (Applies to USG6615E)
	LIC-USG6625E-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6625E)
	LIC-USG6625E-AV-3Y	AV Update Service Subscribe 36 Months (Applies to USG6625E)
	LIC-USG6635E-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6635E)
	LIC-USG6635E-AV-3Y	AV Update Service Subscribe 36 Months (Applies to USG6635E)
	LIC-USG6655E-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6655E)
	LIC-USG6655E-AV-3Y	AV Update Service Subscribe 36 Months (Applies to USG6655E)

Product	Model	Description
Advanced Threat Protection	LIC-USG6605E-B-ATP-1Y	Advanced Threat Protection Subscription 12 Months (Applies to USG6605E-B)
	LIC-USG6605E-B-ATP-3Y	Advanced Threat Protection Subscription 36 Months (Applies to USG6605E-B)
	LIC-USG6615E-ATP-1Y	Advanced Threat Protection Subscription 12 Months (Applies to USG6615E)
	LIC-USG6615E-ATP-3Y	Advanced Threat Protection Subscription 36 Months (Applies to USG6615E)
	LIC-USG6625E-ATP-1Y	Advanced Threat Protection Subscription 12 Months (Applies to USG6625E)
	LIC-USG6625E-ATP-3Y	Advanced Threat Protection Subscription 36 Months (Applies to USG6625E)
	LIC-USG6635E-ATP-1Y	Advanced Threat Protection Subscription 12 Months (Applies to USG6635E)
	LIC-USG6635E-ATP-3Y	Advanced Threat Protection Subscription 36 Months (Applies to USG6635E)
	LIC-USG6655E-ATP-1Y	Advanced Threat Protection Subscription 12 Months (Applies to USG6655E)
	LIC-USG6655E-ATP-3Y	Advanced Threat Protection Subscription 36 Months (Applies to USG6655E)
Threat Protection Bundle (IPS, AV, URL)	LIC-USG6605E-B-TP-1Y	Threat Protection Subscription 12 Months (Applies to USG6605E-B)
	LIC-USG6605E-B-TP-3Y	Threat Protection Subscription 36 Months (Applies to USG6605E-B)
	LIC-USG6615E-TP-1Y	Threat Protection Subscription 12 Months (Applies to USG6615E)
	LIC-USG6615E-TP-3Y	Threat Protection Subscription 36 Months (Applies to USG6615E)
	LIC-USG6625E-TP-1Y	Threat Protection Subscription 12 Months (Applies to USG6625E)
	LIC-USG6625E-TP-3Y	Threat Protection Subscription 36 Months (Applies to USG6625E)
	LIC-USG6635E-TP-1Y	Threat Protection Subscription 12 Months (Applies to USG6635E)
	LIC-USG6635E-TP-3Y	Threat Protection Subscription 36 Months (Applies to USG6635E)
	LIC-USG6655E-TP-1Y	Threat Protection Subscription 36 Months (Applies to USG6655E)
	LIC-USG6655E-TP-3Y	Threat Protection Subscription 36 Months (Applies to USG6655E)

Product	Model	Description
Cloud Sandbox Inspection	LIC-USG6605E-B-CS-1Y	Cloud Sandbox Inspection 12 Months (Applies to USG6605E-B)
	LIC-USG6605E-B-CS-3Y	Cloud Sandbox Inspection 36 Months (Applies to USG6605E-B)
	LIC-USG6615E-CS-1Y	Cloud Sandbox Inspection 12 Months (Applies to USG6615E)
	LIC-USG6615E-CS-3Y	Cloud Sandbox Inspection 36 Months (Applies to USG6615E)
	LIC-USG6625E-CS-1Y	Cloud Sandbox Inspection 12 Months (Applies to USG6625E)
	LIC-USG6625E-CS-3Y	Cloud Sandbox Inspection 36 Months (Applies to USG6625E)
	LIC-USG6635E-CS-1Y	Cloud Sandbox Inspection 12 Months (Applies to USG6635E)
	LIC-USG6635E-CS-3Y	Cloud Sandbox Inspection 36 Months (Applies to USG6635E)
	LIC-USG6655E-CS-1Y	Cloud Sandbox Inspection 12 Months (Applies to USG6655E)
	LIC-USG6655E-CS-3Y	Cloud Sandbox Inspection 36 Months (Applies to USG6655E)
Flow Probe	LIC-USG6605E-B-FP	Flow Probe Function (Applies to USG6605E-B)
	LIC-USG6615E-FP	Flow Probe Function (Applies to USG6615E)
	LIC-USG6625E-FP	Flow Probe Function (Applies to USG6625E)
	LIC-USG6635E-FP	Flow Probe Function (Applies to USG6635E)
	LIC-USG6655E-FP	Flow Probe Function (Applies to USG6655E)
N1 License		
Foundation package function	N1-USG6605E-B-F-Lic	N1-USG6605E-B Foundation, Per Device
	N1-USG6615E-F-Lic	N1-USG6615E Foundation, Per Device
	N1-USG6625E-F-Lic	N1-USG6625E Foundation, Per Device
	N1-USG6635E-F-Lic	N1-USG6635E Foundation, Per Device
	N1-USG6655E-F-Lic	N1-USG6655E Foundation, Per Device
Advanced package function	N1-USG6605E-B-A-Lic	N1-USG6605E-B Advanced, Per Device
	N1-USG6615E-A-Lic	N1-USG6615E Advanced, Per Device
	N1-USG6625E-A-Lic	N1-USG6625E Advanced, Per Device
	N1-USG6635E-A-Lic	N1-USG6635E Advanced, Per Device
	N1-USG6655E-A-Lic	N1-USG6655E Advanced, 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.

Copyright © 2021 HUAWEI TECHNOLOGIES CO., LTD. All Rights Reserved.