

HUAWEI HiSecEngine USG6500E 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 USG6500E 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: AI-powered DGA malicious domain name detection, malicious C&C detection, malicious encrypted C&C detection, and new brute-force cracking detection.

Note: Currently, the USG6575E-B support intelligent defense.

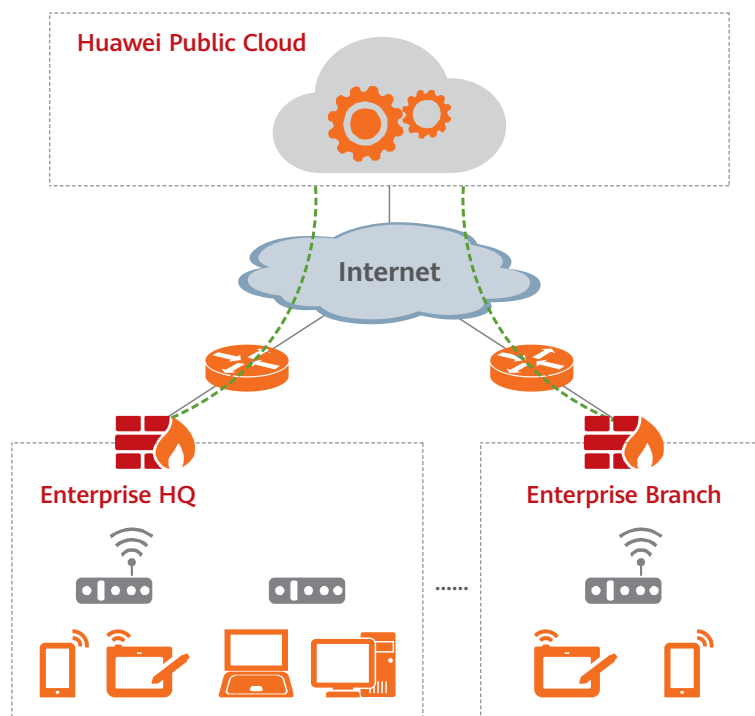
High performance

- 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.





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. |
| 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. |

| Feature | Description |
|---------------------------------|--|
| URL filtering | <p>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.</p> <p>Supports DNS filtering, in which accessed web pages are filtered based on domain names.</p> <p>Supports the SafeSearch function to filter resources of search engines, such as Google, to guarantee access to only healthy network resources.</p> |
| 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. |
| Security policy management | <p>Manages and controls traffic based on VLAN IDs, quintuples, security zones, regions, applications, URL categories, and time ranges, and implements integrated content security detection.</p> <p>Provides predefined common-scenario defense templates to facilitate security policy deployment.</p> <p>Provides security policy management solutions in partnership with FireMon and AlgoSec to reduce O&M costs and potential faults.</p> |
| Diversified reports | <p>Provides visualized and multi-dimensional report display by user, application, content, time, traffic, threat, and URL.</p> <p>Generates network security analysis reports on the Huawei security center platform to evaluate the current network security status and provide optimization suggestions.</p> |



| Feature | Description |
|----------------------------|---|
| 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 | USG6525E | USG6555E | USG6565E | USG6575E-B | USG6585E |
|--|--|----------------|----------------|--------------|--------------|
| Firewall Throughput ¹ (1518/512/64-byte, UDP) | 2/2/2 Gbit/s | 4/4/3.6 Gbit/s | 6/6/3.6 Gbit/s | 7/7/4 Gbit/s | 9/8/4 Gbit/s |
| Firewall Latency (64-byte, UDP) | 18 μs | 18 μs | 18 μs | 18 μs | 18 μs |
| FW + SA + IPS Throughput ² | 1.5 Gbit/s | 2.1 Gbit/s | 2.2 Gbit/s | 2.2 Gbit/s | 2.2 Gbit/s |
| FW + SA + IPS + Antivirus Throughput ² | 1.5 Gbit/s | 2.0 Gbit/s | 2.2 Gbit/s | 2.2 Gbit/s | 2.2 Gbit/s |
| Concurrent Sessions (HTTP1.1) ¹ | 3,000,000 | 4,000,000 | 4,000,000 | 6,000,000 | 4,000,000 |
| New Sessions/Second (HTTP1.1) ¹ | 70,000 | 78,000 | 80,000 | 80,000 | 80,000 |
| Maximum IPsec VPN Tunnels (GW to GW) | 4,000 | 4,000 | 4,000 | 4,000 | 4,000 |
| Maximum IPsec VPN Tunnels (Client to GW) | 4,000 | 4,000 | 4,000 | 4,000 | 4,000 |
| IPsec VPN Throughput ¹ (AES-256 + SHA256, 1420-byte) | 2 Gbit/s | 4 Gbit/s | 6 Gbit/s | 6 Gbit/s | 6 Gbit/s |
| SSL Inspection Throughput ³ | 300 Mbit/s | 450 Mbit/s | 500 Mbit/s | 550 Mbit/s | 550 Mbit/s |
| Concurrent SSL VPN Users (Default/Maximum) | 100/500 | 100/1000 | 100/1000 | 100/1000 | 100/1000 |
| Security Policies (Maximum) | 15,000 | 15,000 | 15,000 | 15,000 | 15,000 |
| Virtual Firewalls | 50 | 100 | 100 | 100 | 100 |
| URL Filtering: Categories | More than 130 | | | | |
| URL Filtering: URLs | A database of over 120 million URLs in the cloud | | | | |

| Model | USG6525E | USG6555E | USG6565E | USG6575E-B | USG6585E |
|---|---|----------|----------|------------|----------|
| 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 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 and eLog | | | | |
| 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.

*SA: indicates service awareness.

Hardware Specifications

| Model | USG6525E | USG6555E | USG6565E | USG6575E-B | USG6585E |
|--------------------------------------|---|--|---|---|--|
| Dimensions (H×W×D) mm | 43.6×442×420 | | | | |
| Form Factor/Height | 1U | | | | |
| Fixed Interface | 2×10GE (SFP+) + 8×GE Combo + 2×GE WAN | | 16×GE (RJ45) + 8×GE Combo + 2×10GE (SFP+) | | 2×10GE (SFP+) + 8×GE Combo + 2×GE WAN |
| Dedicated management port | Yes | | | | |
| Bypass Port | -- | | Yes | | -- |
| USB Port | 1×USB 2.0 + 1×USB 3.0 | | 1×USB 3.0 | | 1×USB 2.0 + 1×USB 3.0 |
| Weight (Full Configuration) | 5.8 kg | | | | |
| External Storage | Optional, SSD (M.2) card supported, 64 GB/240 GB | Optional, SSD (M.2) card supported, 240 GB | | Optional SSD (1×2.5 inch) supported, 240 GB/960G, HDD 1TB | Optional, SSD (M.2) card supported, 240 GB |
| AC Power Supply | 100V to 240V | | | | |
| Max power consumption of the machine | 40 W | | 76.9 W | | 40 W |
| Power Supplies | Single AC power supply; optional dual AC power supplies | | | | |

| Model | USG6525E | USG6555E | USG6565E | USG6575E-B | USG6585E |
|---|--|----------|----------|------------|----------|
| 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 |
|----------|---------------|--|
| USG6525E | USG6525E-AC | USG6525E AC Host (2*10GE (SFP+) + 8*GE Combo + 2*GE WAN, AC power) |
| USG6555E | USG6555E-AC | USG6555E AC Host (2*10GE (SFP+) + 8*GE Combo + 2*GE WAN, AC power) |
| USG6565E | USG6565E-AC | USG6565E AC Host (2*10GE (SFP+) + 8*GE Combo + 2*GE WAN, AC power) |
| USG6575E | USG6575E-B-AC | USG6575E-B AC Host (16*GE (RJ45) + 8*GE Combo + 2*10GE SFP+, 1 AC Power) |
| USG6585E | USG6585E-AC | USG6585E AC Host (2*10GE (SFP+) + 8*GE Combo + 2*GE WAN, 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) |

| NGFW License | | |
|-----------------------|-----------------------|---|
| IPS Update Service | LIC-USG6525E-IPS-1Y | IPS Update Service Subscribe 12 Months (Applies to USG6525E) |
| | LIC-USG6525E-IPS-3Y | IPS Update Service Subscribe 36 Months (Applies to USG6525E) |
| | LIC-USG6555E-IPS-1Y | IPS Update Service Subscribe 12 Months (Applies to USG6555E) |
| | LIC-USG6555E-IPS-3Y | IPS Update Service Subscribe 36 Months (Applies to USG6555E) |
| | LIC-USG6565E-IPS-1Y | IPS Update Service Subscribe 12 Months (Applies to USG6565E) |
| | LIC-USG6565E-IPS-3Y | IPS Update Service Subscribe 36 Months (Applies to USG6565E) |
| | LIC-USG6575E-B-IPS-1Y | IPS Update Service Subscribe 12 Months (Applies to USG6575E-B) |

| Product | Model | Description |
|---------------------------------|-----------------------|---|
| | LIC-USG6575E-B-IPS-3Y | IPS Update Service Subscribe 36 Months (Applies to USG6575E-B) |
| | LIC-USG6585E-IPS-1Y | IPS Update Service Subscribe 12 Months (Applies to USG6585E) |
| | LIC-USG6585E-IPS-3Y | IPS Update Service Subscribe 36 Months (Applies to USG6585E) |
| URL Filtering Update Service | LIC-USG6525E-URL-1Y | URL Update Service Subscribe 12 Months (Applies to USG6525E) |
| | LIC-USG6525E-URL-3Y | URL Update Service Subscribe 36 Months (Applies to USG6525E) |
| | LIC-USG6555E-URL-1Y | URL Update Service Subscribe 12 Months (Applies to USG6555E) |
| | LIC-USG6555E-URL-3Y | URL Update Service Subscribe 36 Months (Applies to USG6555E) |
| | LIC-USG6565E-URL-1Y | URL Update Service Subscribe 12 Months (Applies to USG6565E) |
| | LIC-USG6565E-URL-3Y | URL Update Service Subscribe 36 Months (Applies to USG6565E) |
| | LIC-USG6575E-B-URL-1Y | URL Update Service Subscribe 12 Months (Applies to USG6575E-B) |
| | LIC-USG6575E-B-URL-3Y | URL Update Service Subscribe 36 Months (Applies to USG6575E-B) |
| | LIC-USG6585E-URL-1Y | URL Update Service Subscribe 12 Months (Applies to USG6585E) |
| | LIC-USG6585E-URL-3Y | URL Update Service Subscribe 36 Months (Applies to USG6585E) |
| Antivirus Update Service | LIC-USG6525E-AV-1Y | AV Update Service Subscribe 12 Months (Applies to USG6525E) |
| | LIC-USG6525E-AV-3Y | AV Update Service Subscribe 36 Months (Applies to USG6525E) |
| | LIC-USG6555E-AV-1Y | AV Update Service Subscribe 12 Months (Applies to USG6555E) |
| | LIC-USG6555E-AV-3Y | AV Update Service Subscribe 36 Months (Applies to USG6555E) |
| | LIC-USG6565E-AV-1Y | AV Update Service Subscribe 12 Months (Applies to USG6565E) |
| | LIC-USG6565E-AV-3Y | AV Update Service Subscribe 36 Months (Applies to USG6565E) |
| | LIC-USG6575E-B-AV-1Y | AV Update Service Subscribe 12 Months (Applies to USG6575E-B) |
| | LIC-USG6575E-B-AV-3Y | AV Update Service Subscribe 36 Months (Applies to USG6575E-B) |

| Product | Model | Description |
|---|--------------------------|---|
| | LIC-USG6585E-AV-1Y | AV Update Service Subscribe 12 Months (Applies to USG6585E) |
| | LIC-USG6585E-AV-3Y | AV Update Service Subscribe 36 Months (Applies to USG6585E) |
| Threat Protection Bundle (IPS, AV, URL) | LIC-USG6525E-TP-1Y-OVS | Threat Protection Subscription 12 Months (Applies to USG6525E) |
| | LIC-USG6525E-TP-3Y-OVS | Threat Protection Subscription 36 Months (Applies to USG6525E) |
| | LIC-USG6555E-TP-1Y-OVS | Threat Protection Subscription 12 Months (Applies to USG6555E) |
| | LIC-USG6555E-TP-3Y-OVS | Threat Protection Subscription 36 Months (Applies to USG6555E) |
| | LIC-USG6565E-TP-1Y-OVS | Threat Protection Subscription 12 Months (Applies to USG6565E) |
| | LIC-USG6565E-TP-3Y-OVS | Threat Protection Subscription 36 Months (Applies to USG6565E) |
| | LIC-USG6575E-B-TP-1Y-OVS | Threat Protection Subscription 12 Months (Applies to USG6575E-B) |
| | LIC-USG6575E-B-TP-3Y-OVS | Threat Protection Subscription 36 Months (Applies to USG6575E-B) |
| | LIC-USG6585E-TP-1Y-OVS | Threat Protection Subscription 12 Months (Applies to USG6585E) |
| | LIC-USG6585E-TP-3Y-OVS | Threat Protection Subscription 36 Months (Applies to USG6585E) |
| Cloud Sandbox Inspection | LIC-USG6525E-CS-1Y | Cloud Sandbox Inspection 12 Months (Applies to USG6525E) |
| | LIC-USG6525E-CS-3Y | Cloud Sandbox Inspection 36 Months (Applies to USG6525E) |
| | LIC-USG6555E-CS-1Y | Cloud Sandbox Inspection 12 Months (Applies to USG6555E) |
| | LIC-USG6555E-CS-3Y | Cloud Sandbox Inspection 36 Months (Applies to USG6555E) |
| | LIC-USG6565E-CS-1Y | Cloud Sandbox Inspection 12 Months (Applies to USG6565E) |
| | LIC-USG6565E-CS-3Y | Cloud Sandbox Inspection 36 Months (Applies to USG6565E) |
| | LIC-USG6575E-B-CS-1Y | Cloud Sandbox Inspection 12 Months (Applies to USG6575E-B) |
| | LIC-USG6575E-B-CS-3Y | Cloud Sandbox Inspection 36 Months (Applies to USG6575E-B) |
| | LIC-USG6585E-CS-1Y | Cloud Sandbox Inspection 12 Months (Applies to USG6585E) |
| | LIC-USG6585E-CS-3Y | Cloud Sandbox Inspection 36 Months (Applies to USG6585E) |

| Product | Model | Description |
|-----------------------------|-----------------------|--|
| | LIC-USG6575E-B-AI-1Y | AI Detection Model Upgrades Available in 12 Months (Applies to USG6575E-B) |
| | LIC-USG6575E-B-AI-3Y | AI Detection Model Upgrades Available in 36 Months (Applies to USG6575E-B) |
| Advanced Threat Protection | LIC-USG6575E-B-ATP-1Y | Advanced Threat Protection Subscription 12 Months (Applies to USG6575E-B) |
| | LIC-USG6575E-B-ATP-3Y | Advanced Threat Protection Subscription 36 Months (Applies to USG6575E-B) |
| Flow Probe Function | LIC-USG6525E-FP | Flow Probe Function (Applies to USG6525E) |
| | LIC-USG6555E-FP | Flow Probe Function (Applies to USG6555E) |
| | LIC-USG6565E-FP | Flow Probe Function (Applies to USG6565E) |
| | LIC-USG6575E-B-FP | Flow Probe Function (Applies to USG6575E-B) |
| | LIC-USG6585E-FP | Flow Probe Function (Applies to USG6585E) |
| N1 License | | |
| Foundation package function | N1-USG6525E-F-Lic | N1-USG6525E Foundation, Per Device |
| | N1-USG6555E-F-Lic | N1-USG6555E Foundation, Per Device |
| | N1-USG6565E-F-Lic | N1-USG6565E Foundation, Per Device |
| | N1-USG6575E-B-F-Lic | N1-USG6575E-B Foundation, Per Device |
| | N1-USG6585E-F-Lic | N1-USG6585E Foundation, Per Device |
| Advanced package function | N1-USG6525E-A-Lic | N1-USG6525E Advanced, Per Device |
| | N1-USG6555E-A-Lic | N1-USG6555E Advanced, Per Device |
| | N1-USG6565E-A-Lic | N1-USG6565E Advanced, Per Device |
| | N1-USG6575E-B-A-Lic | N1-USG6575E-B Advanced, Per Device |
| | N1-USG6585E-A-Lic | N1-USG6585E 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 © 2020 HUAWEI TECHNOLOGIES CO., LTD. All Rights Reserved.