Huawei USG6515E/USG6550E/USG6560E/USG6580E Next-Generation Firewalls

USG6515E/USG6550E/USG6560E/USG6580E

Overview

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 network processing chip provides pattern matching and encryption/decryption service processing acceleration functions, which greatly improve the firewalls ability 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, 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.

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.

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. 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.

Huawei USG6515E/USG6550E/USG6560E/USG6580E
Next-Generation Firewalls

Specifications

System Performance and Capacity

Model	USG6515E	USG6550E	USG6560E	USG6580E
IPv4 Firewall Throughput[1] (1518/512/64-byte, UDP)	2/2/1.5 Gbit/s	4/4/1.5 Gbit/s	6/6/1.5 Gbit/s	8/8/1.5 Gbit/s
FW+SA*+IPS Throughput[2]	1.5 Gbit/s	2.1 Gbit/s	2.2 Gbit/s	2.2 Gbit/s
Full Protection Throughput[3]	1.1 Gbit/s	1.6 Gbit/s	1.7 Gbit/s	1.8 Gbit/s
Concurrent Sessions[1] (TCP)	3,000,000	4,000,000	4,000,000	4,000,000
New Sessions/Second[1] (TCP)	70,000	78,000	80,000	80,000
IPSec VPN Throughput[1] (AES-256+SHA256, 1420-byte)	2 Gbit/s	3 Gbit/s	3 Gbit/s	3 Gbit/s
Maximum IPSec VPN Tunnels	4000	4000	4000	4000
SSL Inspection Throughput[4]	300 Mbit/s	450 Mbit/s	500 Mbit/s	550 Mbit/s
SSL VPN Throughput[5]	300 Mbit/s	450 Mbit/s	480 Mbit/s	500 Mbit/s
Concurrent SSL VPN Users (Default/Maximum)	100/500	100/1000	100/1000	100/1000
Firewall Policies (Maximum)	15,000	15,000	15,000	15,000
Virtual Firewalls (Maximum)	50	100	100	100
Dimensions (H×W×D) mm	44×442×420			
Form Factor/Height	1U			
Fixed Interface	2×10GE (SFP+) + 8×GE Combo + 16×GE + 2×GE WAN + 1×USB2.0 + 1×USB3.0			
USB Port	1×USB 2.0+1×USB 3.0 Ports			
MTBF	45.56 years			
Weight (Full Configuration)	5.8 kg			
Local Storage	Optional, SSD (M.2) supported, 64/240GB	Optional, SSD (M.2) supported, 240GB		
AC Power Supply	100V to 240V, 50/60Hz			
Power Consumption (Average/Maximum)	25W/55.16W			
Power Supplies	Single AC power supply; optional dual AC power supplies			
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, 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.
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.
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.

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.

*SA: Service Awareness.

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.