HUAWEI USG6620/6630 Next-Generation Firewalls

---Best-in-Class Security for Medium-sized Businesses

Huawei USG6620/6630 next-generation firewalls are designed for network egresses of medium-sized businesses or branch offices of large enterprises. The firewalls accurately identify more than 6,000 applications and implement fine-grained access control. Application-layer defense functions, such as Intrusion Prevention System (IPS) and antivirus, are used with application identification technologies to improve the threat prevention efficiency and accuracy, providing users with full-fledged network border protection capabilities. The firewalls use the industry-leading Smart Policy technology to automatically fine-tune and simplify existing security policies, reducing the overall operational costs and delivering continuous, simple, and effective next-generation network security.

Highlights

Third-party proven security capability

- Obtained Firewall, IPS, IPsec, and SSL VPN certifications from the ICSA Labs
- Obtained the highest-level CC certificate (EAL4+), ranking among the highest security levels in the world

Comprehensive and integrated protection

- Multiple security functions, including firewall, VPN, intrusion prevention, and online behavior management, for complete versatility
- Accurately identify more than 6000 applications to deliver fine-grained access control and improve the quality of key services
- Detection and prevention of unknown threats, such as zero-day attacks, using sandboxing and the reputation system*

Flexible bandwidth management, improving Internet access experience

- Differentiated user bandwidth and quota management for fair and prioritized bandwidth usage
- Application-based bandwidth management to prioritize bandwidth for mission-critical applications
- Modification of URL category priority

Visualized management and operation

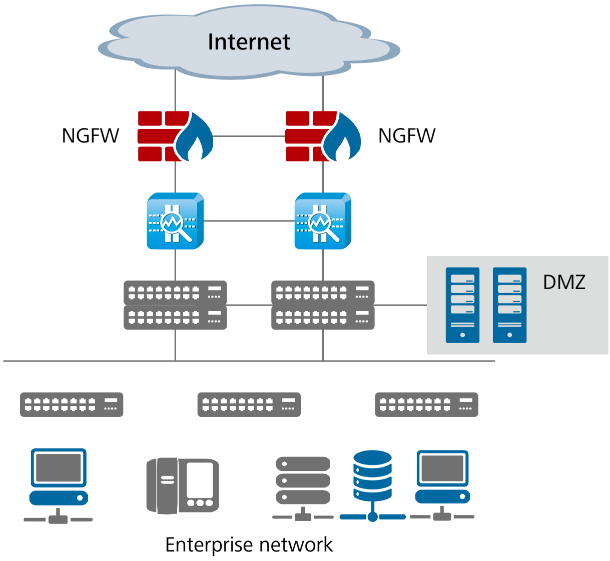
- Deliver diversified reports to provide all-around visibility into service status, network environment, security posture, and user behavior

- Provide a web UI that offers a variety of easy-to-use and visualized management and maintenance functions, with which you can easily view logs and reports, manage configurations, and diagnose faults. The quick wizard on the web UI helps you configure important features with ease
- Support both NETCONF and RESTCONF northbound APIs, which enable you to centrally configure and maintain the firewalls using an upper-level controller to simplify O&M

Deployment

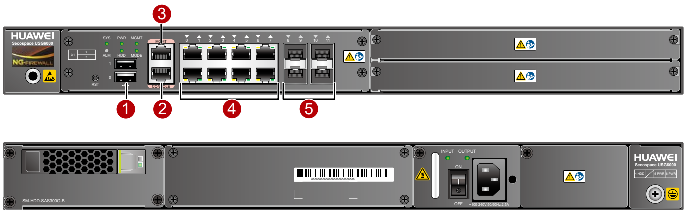
Border protection for medium-sized businesses

- Block all unauthorized access attempts at enterprise network egresses.
- Provide real-time 10-Gigabit-level application-layer threat prevention, even when IPS is enabled.
- Perform data filtering and auditing on files transmitted through sources such as email and IM to monitor social network applications and prevent data leaks.
- Deliver user- and application-specific bandwidth management to guarantee service quality for core users and of mission-critical services.
- Support online behavior management based on URL categories and applications to block access to malicious websites and websites irrelevant to work.



Hardware

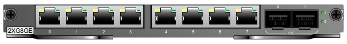
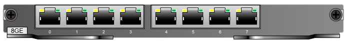
USG6620/6630



Interfaces

1. 2 x USB Ports
2. Console Port
3. 1 x GE (RJ45) Management Port
4. 8 x GE (RJ45) Ports
5. 4 x GE (SFP) Ports

Table 1. Wide Service Interface Cards (WSICs) for USG6600 Series

Feature	2XG8GE	8GE
		
Technical Specification		
Integrated Ports	2 x 10GE (SFP+), 8 x GE (RJ45)	8 x GE (RJ45)

Feature	8GEF	4GE-BYPASS
Technical Specification		
Integrated Ports	8 x GE (SFP)	4 x GE (RJ45) BYPASS

Software Features

Function	Description
Integrated Protection	Provides firewall, VPN, intrusion prevention, antivirus, data leak prevention, bandwidth management, Anti-DDoS, URL filtering, and anti-spam functions.
Application Identification and Control	Identifies common applications, supports application-specific access control, and combines application identification with intrusion prevention, antivirus, and data filtering to improve detection performance and accuracy.
Intrusion Prevention and Web Protection	Obtains the latest threat information in a timely manner for accurate detection and prevention of vulnerability exploits and web attacks, such as cross-site scripting and SQL injection attacks.
Antivirus	Rapidly detects over five million types of viruses through the daily-updated signature database.
Anti-APT*	Interworks with the sandbox to detect and block malicious files.
Data Leak Prevention	Inspects files to identify the file type, such as WORD, EXCEL, POWERPOINT, and PDF, based on file contents, and filters sensitive content.
Bandwidth Management	Manages per-user and per-IP bandwidth in addition to identifying service applications to prioritize mission-critical services and users through methods such as peak bandwidth and committed bandwidth, policy-based routing (PBR), and application forwarding priority adjustment.
URL Filtering	Can access a URL category database of over 120 million URLs to manage access by URL category, such as blocking malicious URLs and accelerating access to specified categories.
Behavior and Content Audit	Audits and traces the sources of URL access based on the user IP address and requested content.
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-homing scenarios.

Function	Description
VPN Encryption	Supports multiple highly reliable VPN features, such as IPsec VPN, SSL VPN, L2TP VPN, and GRE. Provides a VPN client (SecoClient,* developed in-house) for remote user access through SSL VPN, L2TP VPN, and L2TP over IPsec VPN. Supports IPsec intelligent link selection and dynamic IPsec tunnel switchover to improve link availability.
SSL Encrypted Traffic Detection	Serves as a proxy to detect and defend against threats in SSL-encrypted traffic using application-layer protection methods such as intrusion prevention, antivirus, data filtering, and URL filtering.
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, SecurID, AD, CA, LDAP, and Endpoint Security.
Security Virtualization	Allows users to create and manage virtual security services, including firewall, intrusion prevention, and antivirus services, on the same physical device.
Policy Management	Provides predefined common-scenario defense templates to facilitate security policy deployment. Automatically evaluates risks in security policies and provides tuning suggestions. Detects redundant and conflicting policies to remove unnecessary and incorrect policies.
	Provides the firewall policy management solution in partnership with FireMon to reduce O&M costs and potential faults.*
Diversified Reports	Provides visualized and multi-dimensional reports by user, application, content, time, traffic, threat, and URL.[1]
	Generates network security analysis reports on the Huawei security center platform to evaluate the current network security status and provide optimization suggestions.*
Routing	Supports IPv4 static routes, policy-based routing, routing policies, multicast, RIP, OSPF, BGP, and IS-IS. Supports IPv6 static routes, policy-based routing, routing policies, RIPng, OSPFv3, BGP4+, and IPv6 IS-IS.
Working Mode and High Availability	Supports multiple working modes (transparent, routing, and hybrid), high availability modes (active/active and active/standby), and link high-availability technologies (IP-Link, BFD, and Link-group).
Device Management Capability	Built-in Web UI: Provides abundant device management and maintenance functions, including log report, configuration, and troubleshooting.
	eSight network management: Manages the performance, alarms, resources, configurations, and topology of the entire network.
	Agile Controller: Implements application- and user-specific security policy control in the Huawei SDN Agile Network Solution.*
	LogCenter security event management system: Provides functions such as security posture awareness, report management, log audit, and centralized alarm management.
	API: Supports both NETCONF* and RESTCONF northbound APIs to enable users to centrally configure and maintain firewalls via an upper-level controller to simply the O&M.

1: If no hard disk is inserted, you can view and export system and service logs. By inserting a hard disk, you can also view, export, customize, and subscribe to reports.

Functions marked with * are supported only in USG V500R001 and later versions.

Specifications

System Performance and Capacity

Model	USG6620	USG6630
IPv4 Firewall Throughput[1] (1518/512/64-byte, UDP)	12/12/5.5 Gbit/s	16/16/5.5 Gbit/s
IPv6 Firewall Throughput[1] (1518/512/84-byte, UDP)	12/12/6 Gbit/s	16/16/6 Gbit/s
Firewall Throughput (Packets Per Second)	8 Mpps	8 Mpps
Firewall Latency (64-byte, UDP)	16 μs	16 μs
FW + SA* Throughput[2]	10 Gbit/s	12 Gbit/s
FW + SA* Throughput (Realworld)[3]	7 Gbit/s	9 Gbit/s
FW + SA + IPS Throughput[2]	5.8 Gbit/s	5.8 Gbit/s
FW + SA + Antivirus Throughput[2]	5 Gbit/s	5 Gbit/s
FW + SA + IPS + Antivirus + URL Throughput[2]	4 Gbit/s	5 Gbit/s
FW + SA + IPS + Antivirus Throughput (Realworld)[3]	3 Gbit/s	4 Gbit/s
Concurrent Sessions (HTTP1.1)[1]	6,000,000	6,000,000
New Sessions/Second (HTTP1.1)[1]	200,000	250,000
IPsec VPN Throughput[1] (AES-128 + SHA1, 1420-byte)	9 Gbit/s	12 Gbit/s
Maximum IPsec VPN Tunnels (GW to GW)	15,000	15,000
Maximum IPsec VPN Tunnels (Client to GW)	15,000	15,000
SSL Inspection Throughput[4]	160 Mbit/s	160 Mbit/s
SSL VPN Throughput[5]	1 Gbit/s	1.2 Gbit/s
Concurrent SSL VPN Users (Default/Maximum)	100/2,000	100/2,000
Security Policies (Maximum)	40,000	40,000
Virtual Firewalls (Default/Maximum)	10/200	10/200
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[6]	Open APIs for integration with third-party products through RESTCONF and NETCONF interfaces Other third-party management software based on SNMP, SSH, and syslog Collaboration with third-party tools, such as FireMon Collaboration with Anti-APT solution	
Centralized Management	Centralized configuration, logging, monitoring, and reporting is performed by Huawei eSight and LogCenter	
VLANs (maximum)	4,094	

Model	USG6620	USG6630
Virtual Interfaces (maximum)	1,024	
High Availability Configurations	Active/Active, Active/Standby	

1. Performance is tested under ideal conditions based on RFC 2544 and RFC 3511. The actual result may vary with deployment environments.
2. Antivirus, IPS, and SA performances are measured using 100 KB of HTTP files.
3. Throughput is measured with the Enterprise Traffic Model.
4. SSL inspection throughput is measured with IPS-enabled and HTTPS traffic using TLS v1.2 with AES256-SHA.
5. SSL VPN throughput is measured using TLS v1.2 with AES128-SHA.
6. USG6000 V100R001 supports only the RESTCONF interface and cannot interwork with sandbox or third-party tools.

*SA indicates Service Awareness.

Hardware Specifications

Model	USG6620	USG6630
Dimensions (H x W x D) mm	44.4 x 442 x 421	
Form Factor/Height	1U	
Fixed Interfaces	8 x GE (RJ45) + 4 x GE (SFP)	
USB2.0 Port	2 x USB Ports	
Expansion Slot	2 WSIC*	
Expansion I/O	WSIC: 2 x 10 GE(SFP+) + 8 x GE (RJ45), 8 x GE (RJ45), 8 x GE (SFP), 4 x GE (RJ45) BYPASS	
Maximum Number of Interfaces	24 x GE (RJ45) + 4 x GE (SFP) + 4 x 10 GE (SFP+) or 20 x GE (SFP) + 8 x GE (RJ45)	
MTBF	10.08 years	
Weight (Full Configuration)	8.7 kg	
Local Storage	Optional. Supports a 300 GB hard disk (The hard disk is hot-swappable, but the hard disk card is not.)	
AC Power Supply	100V to 240V, 50/60Hz	
Power Consumption (Average/Maximum)	87.85W/165.37W	
Heat Dissipation	564 BTU/h	
Power Supplies	Single 170W AC power supply; optional 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 90% (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 90% (with optional HDD), non-condensing	
Operating Altitude (maximum)	5,000 meters (without optional HDD); 3,000 meters (with optional HDD)	
Non-operating Altitude (maximum)	5,000 meters (without optional HDD); 3,000 meters (with optional HDD)	
Noise	63 dBA	

*WISC is not hot-swappable.

Certifications

Certifications	
Software	ICSA Labs: Firewall, IPS, IPsec, SSL VPN CC: EAL4+
Hardware	CB, CE-SDOC, ROHS, REACH&WEEE(EU), RCM, ETL, FCC&IC, VCCI, BSMI

Regulatory, Safety, and EMC Compliance

Certifications	
Regulatory Compliance	Products comply with CE markings per directives 2014/30/EU and 2014/35/EU.
Safety	• UL 60950-1 • CSA-C22.2 No. 60950-1 • EN 60950-1 • IEC 60950-1
EMC: Emissions	• CNS 13438 Class A • EN 55022 Class A • CISPR 22 Class A • ETSI EN 300 386 • ETSI EN 201 468 • AS/NZS CISPR 22 • CAN/CSA-CISPR 22-10 • IEC 61000-6-4/EN 61000-6-4 • 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	• CNS 13438 Class A • EN 55024 • CISPR 24 • ETSI EN 300 386 • ETSI EN 201 468 • IEC 61000-6-2/EN 61000-6-2

Ordering Guide

Product	Model	Description
USG6620	USG6620-AC	USG6620 AC Host(8GE(RJ45)+4GE(SFP), 8GB Memory, 1 AC Power)
USG6620-BDL	USG6620-BDL-AC	USG6620 AC Host(8GE(RJ45)+4GE(SFP), 8GB Memory, 1 AC Power, with IPS-AV-URL Function Group Update Service Subscribe 12 Months)
USG6630	USG6630-AC	USG6630 AC Host(8GE(RJ45)+4GE(SFP), 8GB Memory, 1 AC Power)
USG6630-BDL	USG6630-BDL-AC	USG6630 AC Host(8GE(RJ45)+4GE(SFP), 8GB Memory, 1 AC Power, with IPS-AV-URL Function Group Update Service Subscribe 12 Months)
Business Module Group		
WSIC	WSIC-8GE	8GE Electric Ports Interface Card

Product	Model	Description
WSIC	WSIC-4GEBYPASS	4GE Electric Ports Bypass Card
WSIC	WSIC-8GEF	8GE Optical Ports Interface Card
WSIC	WSIC-2XG8GE	2*10GE Optical Ports+8GE Electric Ports Interface Card
Hard Disk Group		
HDD	SM-HDD-SAS300G-B	300GB 10K RPM SAS Hard Disk for 1U rack Gateway
Power Module		
Power	Power-AC-B	170W AC power module
Function License		
SSL VPN Concurrent Users	LIC-SSL-100-USG6000	Quantity of SSL VPN Concurrent Users(100 Users)
	LIC-SSL-200-USG6000	Quantity of SSL VPN Concurrent Users(200 Users)
	LIC-SSL-500-USG6000	Quantity of SSL VPN Concurrent Users(500 Users)
	LIC-SSL-1000-USG6000	Quantity of SSL VPN Concurrent Users(1000 Users)
	LIC-SSL-2000-USG6000	Quantity of SSL VPN Concurrent Users(2000 Users)
Virtual Firewall	LIC-VSYS-10-USG6000	Quantity of Virtual Firewall (10 Vsys)
	LIC-VSYS-20-USG6000	Quantity of Virtual Firewall (20 Vsys)
	LIC-VSYS-50-USG6000	Quantity of Virtual Firewall (50 Vsys)
	LIC-VSYS-100-USG6000	Quantity of Virtual Firewall (100 Vsys)
	LIC-VSYS-200-USG6000	Quantity of Virtual Firewall (200 Vsys)
NGFW License		
IPS Update Service	LIC-IPS-12-USG6600	IPS Update Service Subscribe 12 Months
	LIC-IPS-36-USG6600	IPS Update Service Subscribe 36 Months
URL Filtering Update Service	LIC-URL-12-USG6600	URL Filtering Update Service Subscribe 12 Months
	LIC-URL-36-USG6600	URL Filtering Update Service Subscribe 36 Months
Anti-Virus Update Service	LIC-AV-12-USG6600	Anti-Virus Update Service Subscribe 12 Months
	LIC-AV-36-USG6600	Anti-Virus Update Service Subscribe 36 Months
IPS-AV-URL Function Group	LIC-IPSAVURL-12-USG6600	IPS-AV-URL Function Group Subscribe 12 Months
	LIC-IPSAVURL-36-USG6600	IPS-AV-URL Function Group Subscribe 36 Months
Basic License		
Content Filtering	LIC-CONTENT	Content Filtering Function

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.