Huawei Secospace USG6600 Series Next-Generation Firewall

USG6620/6630

USG6650/6660/6670/6680

Overview

Enterprise networks are evolving into next-generation networks that feature mobile broadband, big data, social networking, and cloud services. Yet, mobile applications, Web2.0, and social networks expose enterprise networks to the risks on the open Internet. Cybercriminals can easily penetrate a traditional firewall by spoofing or using Trojan horses, malware, or botnets.

HUAWEI Secospace USG6600 series is designed to address these challenges of Carrier, large- and medium-sized enterprises and next-generation data centers. It analyzes intranet service traffic from six dimensions, including application, content, time, user, attack, and location and then automatically generates security policies as suggestions to optimize the security management and provide high-performance application-layer protection for enterprise networks.

Note: USG6600 is next-generation firewall products series in USG (Unified Security Gateway) product family

Product Features

Granular Application Access Control

- Identifies the application-layer attacks and their application, content, time, user, and location information.
- Provides all-round visibility into service status, network environment, security postures, and user behaviors.
- Provides an analysis engine that integrates application identification and security functions, such as IPS, AV, and data leak prevention, to prevent application-based malicious code injections, network intrusions, and data interceptions.

Excellent Performance

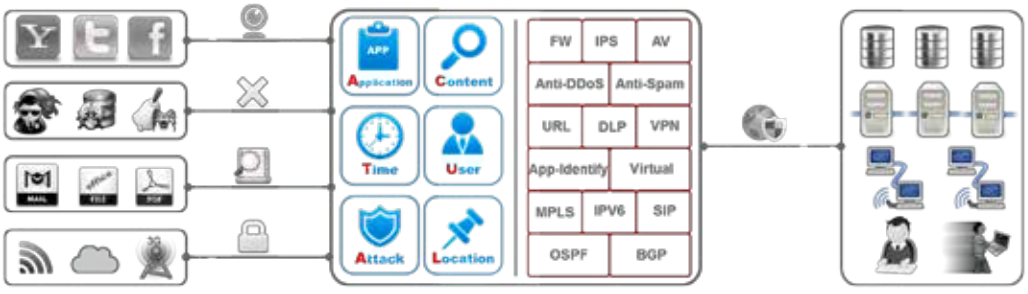
- Provides an Intelligent Awareness Engine (IAE) capable of parallel processing with all security functions enabled after intelligent application identification.
- Improves application-layer protection efficiency and ensures the 10G+ performance with all security functions enabled.

Easy Security Management

- Classifies 6000+ applications into 5 categories and 33 subcategories and supports application access control based on the subcategories.
- Complies with the minimum permission control principle and automatically generates policy tuning suggestions based on network traffic and application risks.
- Analyzes the policy matching ratio and discovers redundant and invalid policies to remove policies and simplify policy management.

Prevention of Unknown Threats

- Provide samples of worldwide suspicious threats. The USG6600 series executes suspicious samples within the sandbox in the cloud to monitor the activities of the samples and identifies unknown threats.
- Automatically extracts threat signatures and rapidly synchronizes the signatures to the devices to defend against zero-day attacks.
- Prevent Advanced Persistent Threat (APT) attacks using a reputation system.



Huawei Secospace USG6600 Series
Next-Generation Firewall

Specifications

Model	USG6620	USG6630	USG6650	USG6660	USG6670	USG6680
Firewall throughput	12 Gbit/s	16 Gbit/s	20 Gbit/s	25 Gbit/s	35 Gbit/s	40 Gbit/s
IPS throughput	5.8 Gbit/s	5.8 Gbit/s	8.8 Gbit/s	8.8 Gbit/s	8.8 Gbit/s	15 Gbit/s
IPS+AV throughput	5 Gbit/s	5 Gbit/s	8 Gbit/s	8 Gbit/s	8 Gbit/s	13 Gbit/s
Concurrent sessions	6,000,000	6,000,000	8,000,000	10,000,000	10,000,000	12,000,000
New sessions per second	200,000	250,000	300,000	350,000	400,000	400,000
VPN Throughput (IPSec)	12 Gbit/s	12 Gbit/s	15 Gbit/s	18 Gbit/s	18 Gbit/s	18 Gbit/s
Virtual firewalls	200	200	500	500	500	1,000
Fixed port	8GE+4SFP		2×10GE+8GE+8SFP		4×10GE+16GE+8SFP	
Expansion Slots	2×WSIC		6×WSIC		5×WSIC	5×WSIC
Interface module	WSIC: 2×10GE (SFP+)+8×GE (RJ45), 8×GE (RJ45), 8×GE (SFP), 4×GE (RJ45) BYPASS					
Height	1U		3U			
Dimensions (H×W×D)	442mm×421mm×43.6mm		130.5mm×442mm×415mm			
Weight (full configuration)	10 kg		24 kg			
HDD	Optional. Supports single 300 GB hard disks (hot swappable).		Optional. Supports 300 GB hard disks (RAID1 and hot swappable).			
Redundant power supply	Optional		Standard configuration			
AC power supply	100 V to 240 V		100 V to 240 V			
DC power supply	-48 V to -60 V		-48 V to -60 V			
Maximum power	170W		350W			700W
Operating environment	Temperature: 0°C to 40°C/5°C to 40°C(with optional HDD) Humidity: 10% to 90%					
Non-operating environment	Temperature: -40°C to 70°C/Humidity: 5% to 95%					
Functions						
Context awareness	ACTUAL (Application, Content, Time, User, Attack, Location)-based awareness capabilities					
	Eight authentication methods (local, RADIUS, HWTACACS, SecureID, AD, CA, LDAP, and Endpoint Security)					
Application security	Fine-grained identification of over 6000 application protocols, application-specific action, and online update of protocol databases					
	Combination of application identification and virus scanning to recognize the viruses (more than 5 millions), Trojan horses, and malware hidden in applications					
	Combination of application identification and content detection to identify file types and sensitive information to prevent information leaks					
Intrusion prevention	Provides over 5000 signatures for attack identification.					
	Provides protocol identification to defend against abnormal protocol behaviors.					
	Supports user-defined IPS signatures.					
Web security	Cloud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categories					
	Defense against web application attacks, such as cross-site scripting and SQL injection attacks					
	HTTP/HTTPS/FTP-based content awareness to defend against web viruses					
	URL blacklist and whitelist and keyword filtering					
Email security	Real-time anti-spam to detect and filter out phishing emails					
	Local whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by attachment type, size, and quantity					
	Virus scanning and notification for POP3/SMTP/IMAP email attachments					
Data security	Data leak prevention based on content awareness File reassembly and data filtering for more than 30 file types (including Word, Excel, PPT, and PDF), and file blocking for more than 120 file types					
Security virtualization	Virtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)					
Network security	Defense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks					
	VPN technologies: IPSec VPN, SSL VPN, L2TP VPN, MPLS VPN, and GRE					
Routing	IPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6					
Working mode and availability	Transparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/Standby mode					
Intelligent management	Evaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation to automatically optimize security policies. Supports policy matching ratio analysis and the detection of conflict and redundant policies to remove them, simplifying policy management.					
	Provides a global configuration view and integrated policy management. The configurations can be completed in one page.					
	Provides visualized and multi-dimensional report display by user, application, content, time, traffic, threat, and URL.					