Huawei USG6300 Series
Next-Generation Firewall (Box-shaped)

USG6330/6350/6360

USG6370/6380/6390

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 USG6300 series (Box-shaped) is designed to address these challenges, and providing a reliable and secure network for small and medium-sized enterprises. 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: USG6300 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.
- Flexible bandwidth management optimizes critical services, improves user experience, and cuts costs.
- Provides all-round visibility into service status, network environment, security postures, and user behaviors.

Excellent Performance

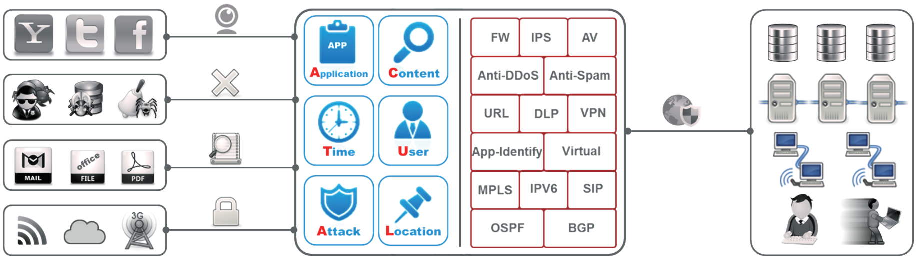
- Provides an Intelligent Awareness Engine (IAE) capable of parallel processing with all security functions enabled after intelligent application identification.
- Improves application-layer protection efficiency and ensures the 10G+ performance with all security functions enabled.

Easy Security Management

- Matches the cloud management platform. You can purchase the MSP management service to reduce investments on network management software and human resources.
- 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.

Comprehensive Protection

- Multiple defense functions in a single appliance, such as IPS, antivirus, and data leak prevention, to prevent application-based malicious code injections, network intrusions, and data interceptions.
- Implementing cloud-based URL category filtering to prevent threats caused by users' access to malicious websites and control users' online behaviors.
- Coordinate with sandbox, effectively defend APT attacks.



LEADING NEW ICT,
BUILDING A BETTER CONNECTED WORLD

HUAWEI

Huawei USG6300 Series
Next-Generation Firewall (Box-shaped)

Specifications

Model	USG6330	USG6350	USG6360	USG6370	USG6380	USG6390
IPV4 Firewall throughput[1] (1518byte, UDP)	1 Gbit/s	2 Gbit/s	3 Gbit/s	4 Gbit/s	6 Gbit/s	8 Gbit/s
FW + SA + IPS Throughput[2]	500 Mbit/s	950 Mbit/s	1.1 Gbit/s	2 Gbit/s	2 Gbit/s	2 Gbit/s
FW + SA + Antivirus Throughput[2]	500 Mbit/s	950 Mbit/s	1.1 Gbit/s	2 Gbit/s	2 Gbit/s	2 Gbit/s
Concurrent sessions (HTTP1.1)[1]	1,500,000	2,000,000	3,000,000	4,000,000	4,000,000	4,000,000
New sessions per second (HTTP1.1)[1]	30,000	30,000	30,000	60,000	70,000	80,000
IPsec VPN Throughput[1] (AES-128 + SHA1, 1420-byte)	700Mbit/s	800Mbit/s	900Mbit/s	3Gbit/s	3Gbit/s	3Gbit/s
Virtual firewalls	50	50	50	100	100	100
MTBF	11.58years	11.58years	11.58years	11.96years	11.96years	11.96years
Fixed port	4×GE(RJ45)+2×GE(Combo)			8×GE(RJ45)+4×GE(SFP)		
Expansion Slots	2×WSIC					
Interface module	2×10GE (SFP+)+8×GE (RJ45), 8×GE (RJ45), 8×GE (SFP), 4×GE (RJ45) BYPASS					
Height	1U					
Dimensions (W×D×H)	442mm×421mm×44.4mm					
Weight (full configuration)	10 kg					
HDD	Optional. Supports single 300 GB or 600G hard disks (hot swappable).					
Redundant power supply	Optional					
AC power supply	100 V to 240 V					
DC power supply	-					
Maximum power	170W					
Operating environment: (Temperature/ Humidity)	Temperature: 0°C to 45°C/5°C to 40°C(with optional HDD) Humidity: 5% ~ 95%/ 5% ~ 90% (with optional HDD)					
Non-operating environment	Temperature: -40°C to 70°C/Humidity: 5% to 95%					
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					
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). The firewall provides built-in portal and portal redirection functions.					
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 6000 signatures for attack identification.					
	Provides protocol identification to defend against abnormal protocol behaviors.					
	Supports user-defined IPS signatures.					
	Supports APT defense. Interworking with the Sandbox to detect and block the malicious files in the network.					
Web security	Cloud-based URL filtering with a URL category database that contains over 120 million URLs in over 130 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. Huawei-developed VPN client SecoClient to implement remote user access through SSL VPN, L2TP VPN, and L2TP over IPSec VPN.					
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.					
	Enterprise administrators can perform assessment over the current network security status by the network security report and providing the related optimization suggestions.					

1. 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.