USG6300 Next-Generation Firewall

With the proliferation of smart devices, such as smartphones and tablets, mobile apps, Web2.0, and social networking become integral parts of enterprise operation. The wide use of mobile devices improves the communication efficiency for enterprises, but blurs network borders and complicates security issues. Moreover, the traditional firewalls that implement access control only by IP address and port cannot cope with ever-increasing application layer threats.

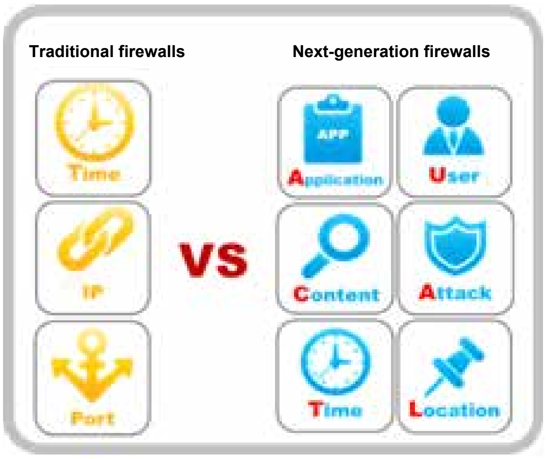
Against this background, Huawei launches the USG6300 series next-generation firewall to address these issues. The USG6300 is designed for Small to Medium-sized Business (SMB), branch offices, and chain enterprises. The USG6300 provides fine-grained service access control and service acceleration through context awareness by Application, Content, Time, User, Attack, or location (ACTUAL). The USG6300 integrates application-layer protection functions, such as Intrusion Prevention System (IPS) and antivirus with application identification technologies to improve the threat defense efficiency and accuracy. The USG6300 is a multi-purpose device that provides comprehensive protection to reduce the management cost. Fine-grained bandwidth management and QoS optimization greatly reduce enterprises' bandwidth leasing fees and ensure user experience in mission-critical services. In short, the USG6300 is a simple and efficient device that provides up-to-date next-generation security.

USG6300 Next-Generation Firewall

Product Features and Benefits

Accurate Access Control

Compared with traditional firewalls, the USG6300 provides fined-grained and more accurate access control. The USG6300 has the following features:



- Integrated protection: The USG6300 implements access control and protection by Application, Content, Time, User, Attack, or location (ACTUAL). It integrates application-layer defense and application identification. For example, the USG6300 can identify Oracle traffic and implement intrusion prevention specially for Oracle traffic to increase efficiency and reduce false positive rate.
- Application-specific: The USG6300 accurately identifies over 6000 applications (including mobile and web applications) and their functions, and then implements access control and service acceleration. For example, the USG6300 can identify the voice and data services of an instant message and apply different control policies for the services.
- User-specific: The USG6300 supports eight user authentication methods, such as RADIUS, LDAP, and AD authentication and synchronizes user information from the existing user authentication system. The USG6300 implements access control, QoS management, and in-depth protection by user.
- Location-specific: Based on the mappings between IP addresses and geographical locations, the USG6300 identifies the locations from which application traffic and attack traffic originates and promptly detects network exceptions. Then the USG6300 implements differentiated access control for locations, which can be user-defined for IP addresses.

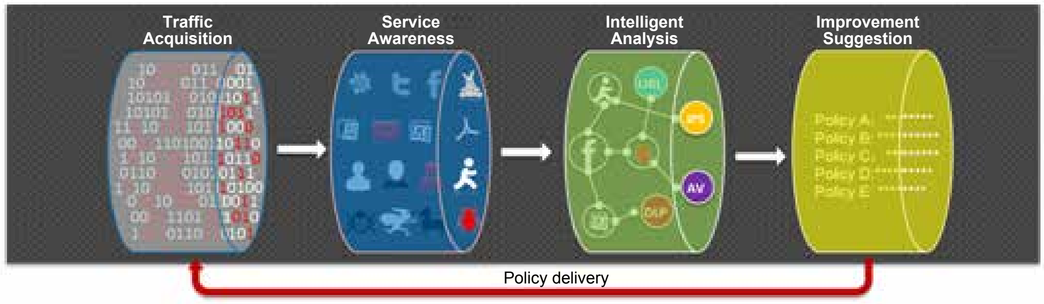
Overall Protection

As more information assets are accessible from the Internet, network attacks and information have been industrialized, requiring wider ranges of protections form next-generation firewalls. The USG6300 provides overall protection:

- Multi-purpose: The USG6300 integrates the traditional firewall, VPN, intrusion prevention, antivirus, data leak prevention, bandwidth management, and online behavior management functions all in one device, simplifying device deployment and improving management efficiency.
- IPS: The USG6300 can detect and defend against over 5000 vulnerabilities. It can identify and defend against web application attacks, such as cross-site scripting and SQL injection attacks.
- Antivirus: The high-performance antivirus engine of the USG6300 can defend against over five million viruses and Trojan horse. The virus signature database is updated daily.
- Data leak prevention: The USG6300 identifies and filters the files and content to be transferred. It can identify more than 120 file types to prevent virus attacks that are launched by modifying file name extensions. It can restore and implement content filtering for over 30 types of files, such as word, excel, PPT, PDF, and RAR files to prevent leaks of critical enterprise information.
- SSL decryption: The USG6300 serves as a proxy and implements application-layer protection for SSL-encrypted traffic, such as IPS, AV, data leak prevention, and URL filtering.

- Anti-DDoS: The USG6300 can identify and defend against over 5 million viruses and over 10 types of DDoS attacks, such as SYN flood and UDP flood attacks.
- Online behavior management: The USG6300 implements cloud-based URL category filtering to prevent threats caused by users' access to malicious websites and control users' online behaviors, such as posting. The USG6300 has a predefined URL category database that contains over 85 million URLs. In addition, the USG6300 audits users' network access records, such as posting and FTP operations.
- Secure interconnection: The USG6300 supports various VPN features, such as IPSec, SSL, L2TP, MPLS, and GRE VPN to ensure high-availability and secure interconnection between enterprise headquarters and branch offices.
- QoS management: The USG6300 flexibly controls upper and lower traffic thresholds and implements policy-based routing and QoS marking by application. It supports QoS marking for URL categories. For example, the packets for accessing financial websites are assigned a higher priority.
- Load balancing: The USG6300 supports server load balancing. In a multi-egress scenario, the USG6300 can implement load balancing with the egresses for applications according to link quality, bandwidth, and weights.
- Virtualization: The USG6300 supports virtualization of multiple security services, such as firewall, intrusion prevention, antivirus, and VPN services and implements independent management for different users on the same physical device.
- Prevent Advanced Persistent Threat (APT) attacks using a reputation system.

Simple Security Management

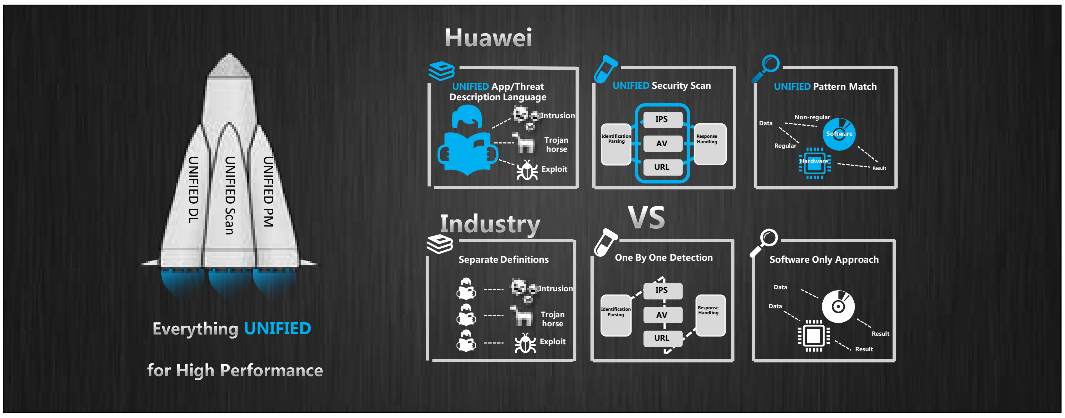


Next-generation firewalls provide a wider range of protections and more accurate access control than traditional firewalls. As a result, the configuration of the next-generation firewalls is complex, imposing higher requirements on the experience and skills of administrators. To reduce administration complexity, the USG6300 provides the smart policy feature, which has the following functions:

- Rapid deployment policy: The built-in scenario policy template allows administrators to rapidly deploy common protection policies without heavily relying on their experience and skills. For example, to use the network storage, the administrator can use only the "network disk" policy template to set up a series of policies. The policies allow users to download applications of the network disk category and perform virus detection but prevents them from uploading files.
- Intelligent optimization policy: The USG6300 generates policy tuning suggestions based on network traffic and application risks in compliance with the minimum privilege principle. The function is helpful when an enterprise needs to transform a large number of port-based firewall policies to application-based next-generation firewall policies.
- Intelligent policy cleanup: The USG6300 automatically discovers redundant and inactive policies for policy cleanup.

High Protection Performance

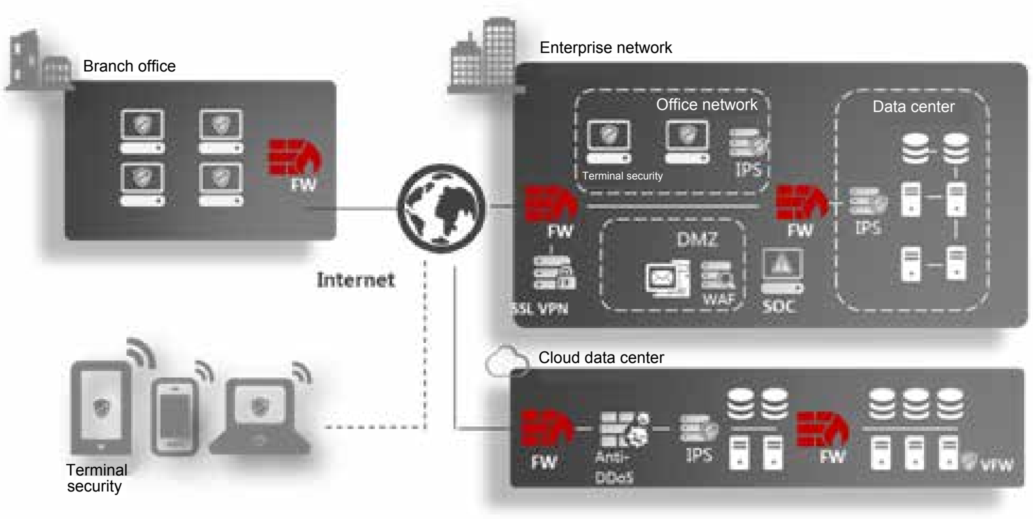
The performance of the UTM that has the application-layer protection function enabled is deteriorated and cannot meet current application-layer protection requirements. In contrast, the next-generation firewalls can retain high-performance when providing multiple-level protection.



The USG6300 uses the intelligence awareness engine (IAE) to ensure high performance in case of multiple-level protection. The IAE uses three core technologies:

- Unified signature description language: Application, IPS, and antivirus signatures are described in a unified language so that the USG6300 can match traffic with these signatures concurrently to improve the traffic processing efficiency.
- Integrated architecture: Unlike the serial processing of UTM security functions, the security services of the USG6300 are parallel. Therefore, the USG6300 can have multiple security services enabled and still retain high performance.
- Hardware acceleration: The USG6300 uses dedicated hardware for resource-consuming computing, such as packet encryption and decryption and regular expression matching. For common services, the USG6300 still uses the CPU for computing.

Typical Application Scenarios



Intranet Border Protection

- Deploy next-generation firewalls on intranet borders to control access by user.
- Implement user- and application-based policy control on mobile users for refined permission management and logging.
- Implement content filtering and auditing on email transfer, IM, and file transfer to monitor social networking applications and prevent data leaks.

Internet Egress Protection

- Deploy a next-generation firewall at the Internet egress to implement access control and prevent unauthorized access.
- Enable intrusion prevention and provide application-layer protection.
- Implement content filtering and auditing on email transfer, IM, and file transfer to monitor social networking applications and prevent data leaks.
- Implement user-, application-, and time-based QoS management to preferentially guarantee the service qualities for mission-critical users and services.
- Use URL categories and application blocking to prevent Trojan horse websites and non-work-related websites and monitor the accessible websites and network applications.

Cloud Data Center Border Protection

- 1. Deploy a next-generation firewall which virtualizes all security services and system resources to provide exceptional experience for each virtual system.
- 2. Enable the intrusion prevention function to effectively block attacks and provide differentiated defense functions in different virtual systems.
- 3. Enable anti-DDoS to remove DDoS traffic and protect data centers.

Remote VPN Access

- Deploy a next-generation firewall to establish reliable, controllable, and manageable tunnels for secure data transfer on the Internet.
- Provide SSL VPN across multiple platforms (including Windows, IOS, Android, Blackberry, and Symbian).

Specifications

Model	USG6320	USG6330	USG6350	USG6360	USG6370	USG6380	USG6390
Firewall throughput	2 Gbit/s	1 Gbit/s	2 Gbit/s	3 Gbit/s	4 Gbit/s	6 Gbit/s	8 Gbit/s
IPS throughput	700Mbit/s	500Mbit/s	950Mbit/s	1.1Gbit/s	2Gbit/s	2Gbit/s	2Gbit/s
IPS+AV throughput	700Mbit/s	500Mbit/s	950Mbit/s	1.1Gbit/s	2Gbit/s	2Gbit/s	2Gbit/s
Concurrent sessions	500,000	1,500,000	2,000,000	3,000,000	4,000,000	4,000,000	4,000,000
New sessions per second	20,000	30,000	30,000	30,000	60,000	70,000	80,000
VPN Throughput (IPSec)	400Mbit/s	400Mbit/s	400Mbit/s	400Mbit/s	3Gbit/s	3Gbit/s	3Gbit/s

Model	USG6320	USG6330	USG6350	USG6360	USG6370	USG6380	USG6390
Virtual firewalls	20	50	50	50	100	100	100
MTBF	19.06years	11.58years			11.96years		
Fixed port	8GE	4GE+2Combo			8GE+4SFP		
Expansion Slots	-	2 x WSIC			2 x WSIC		
Interface module	-	2 x 10GE (SFP+)+8 x GE (RJ45), 8 x GE (RJ45), 8 x GE (SFP), 4 x GE (RJ45) BYPASS					
Height	Desktop	1U					
Dimensions (H x W x D)	300*220*44.5	442*421*43.6					
Weight (full nfiguration)	1.7kg	10 kg					
HDD	-	Optional. Supports single 300 GB hard disks (hot swappable).					
Redundant power supply	-	Optional					
AC power supply	100 V to 240 V						
DC power supply	-						
Maximum power	60W	170W					
Operating environment: (Temperature/ Humidity)	Temperature: 0°C to 40°C Humidity: 10% to 90%	Temperature: 0℃ to 40℃/5℃ to 40℃(with optional HDD) Humidity: 10% to 90%					
Non-operating environment	Temperature: -40℃ to 70℃ Humidity: 5% to 95%						
Certifications							
Hardware	CB,CCC,CE-SDOC,ROHS,REACH&WEEE(EU),C-TICK,ETL,FCC&IC,VCCI,BSMI						
ICSA Labs	Firewall, IPS						

Functions

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)

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 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 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
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.