
# HUAWEI NGFW Security Software Datasheet

## ---Precise and Comprehensive Protection

In addition to all the functions of conventional firewalls, Huawei NGFW also provides more advanced security functions, such as IPS and anti-malware functions, to identify applications and prevent application-layer threats. Huawei NGFW provides a global context awareness architecture for granular controls based on application, content, time, user, attack, and location (ACTUAL). The innovative SmartPolicy technology and management interfaces that can be easily integrated simplify the O&M management. The Intelligence Awareness Engine (IAE) uses an integrated architecture to perfectly balance security and performance. Huawei NGFW provides next-generation security featuring comprehensive protection, granular control, and O&M simplicity to meet the requirements of enterprise networks on access control, scope of protection, usability, and performance in the new ICT landscape.

### Comprehensive security and trustworthy capability

With professional content security functions, such as application identification, IPS, antivirus, and DLP, Huawei NGFW provides comprehensive and integrated protection to reduce both network security risks and management costs. Huawei NGFW's security capability has been tested by trustworthy third-party organizations, such as CC, ICSA, and NSS Labs in the industry, and has earned the "Recommended" rating of NSS Labs for its outstanding and industry-leading 98.1% overall security effectiveness and 99.95% live network threat detection rate.

### Powerful knowledge base and diverse reports

The integrated inspection mechanism, preinstalled signature database, and powerful IAE accurately identify over 6300 applications and distinguish different functions of applications, and the knowledge base can be constantly updated to keep current on emerging threats. The diverse reports provide visibility into service status, network environment, security postures, and user behaviors. Meanwhile, the web UI allows administrators to quickly view and understand the activities and threats on networks in real time.

### Efficient and reliable platforms

Huawei has many years of experience in the design and manufacturing of carrier-class products, such as the carrier-class hardware and proprietary VRP network operating system, which are used in NGFW products to provide carrier-class high availability in hardware, software, and links. The proprietary high-performance IAE and automatic analysis and signature extraction platform can quickly react to emerging threats to provide in-time, accurate, and effective protection.

## Feature

### Security

The ACTUAL-based awareness of Huawei NGFW provides accurate access control and comprehensive threat prevention.

### Accurate Access Control

- Innovative next-generation context awareness and access control. The global awareness by application, content, time, user, attack, and location detects and prevents application-layer threats.
- Integrated next-generation content security. The IAE integrates security functions and application identification to protect application exploits and consequent breaches, such as malware infection, network intrusion, and data theft.

### Comprehensive threat prevention

- Advanced content security. The application identification, IPS, antivirus, and DLP prevent complex application-layer threats.
- Quick response to unknown threats. The security sandbox and reputation system prevent zero-day attacks and other unknown threats.

| Feature | Description | The USG Advantage | Specification |
|---|---|---|---|
| **Firewall** | NGFWs can perform security detection based on the protocol status of protocols in multiple layers and support integrated security policies based on networks, users, and applications. | • The multi-core hardware platform builds high-performance firewalls. The all-in-one mechanism is cost-effective and meets all-round network security requirements.<br>• Comprehensive protocol awareness and filtering mechanisms enable administrators to rapidly filter packets based on users and actual environments.<br>• NGFWs can identify over 6300 web protocols and web apps, including mobile apps. They can also identify encrypted P2P, IM, and VoIP apps for granular management and control. | • Working modes: transparent, routing, and hybrid<br>• ASPF for application protocols: FTP, RTSP, H323, SIP, QQ, ICQ, MSN, PPTP, SQL.NET, MMS, DNS, NetBIOS, ILS, RSH, SCCP, Java Blocking, ActiveX Blocking, SMTP, and HTTP<br>• Port mapping<br>• Protocol status check for TCP, UDP, SCTP, and ICMP<br>• Blacklist and whitelist<br>• Multi-dimensional security policies: source/destination IP address, source/destination port, service, time range, user, application, and source/destination security zone<br>• Application identification: 6300+ applications, including user-defined, micro, and enterprise applications<br>• Security zone: four default zones (untrust, trust, local, and DMZ) and user-defined security zones |
| **IPS** | Intrusion prevention detects intrusions, such as buffer overflow attacks, Trojan horses, and worms, by analyzing network traffic and takes actions to quickly terminate the intrusions. | • Recommended NGFW by NSS Labs<br>• Obtained ICSA Network IPS certification<br>• Vulnerability-based detection for more effective defense<br>• Applicable to different types of network deployment requirements: IPS blocking, IDS alerting but not blocking | • Vulnerability signature database: 6000+<br>• User-defined signatures<br>• Matching based on regular expressions for higher matching capabilities<br>• Detection of evasion techniques, such as IP fragmentation, TCP segmentation, and other application layer evasion techniques<br>• Web defense, such as SQL injection and XSS detection<br>• Detection on abnormal behavior, such as brute force cracking<br>• Detection on C&C malicious domain names, botnets, worms, and Trojan horses<br>• Response actions alert, block, and isolate (isolation period)<br>• Attack forensics and post-event audit<br>• Filtering signatures based on operating systems, directions, severities, applications, protocols, and categories and setting an action |
| **URL filtering** | Regulate online behavior by controlling which URLs users can access to protect enterprise networks from malicious websites. | • Support a URL category database over 100 million URLs in 45 categories and 137 sub-categories for granular management and control for various access requests.<br>• URL filtering allows you to manage users' online behavior on an individual basis, by user or user group, by schedule, and through security zones.<br>• URL filtering technology allows you to change the DSCP priorities of URL access packets based on categories of requested URLs, so that other network devices can take differentiated actions. | • URLs in the URL category database: 120 million+<br>• Filtering based on user-defined blacklists and whitelists<br>• Filtering of malicious URLs<br>• Filtering of HTTPS URLs<br>• A maximum of 256 user-defined URL categories<br>• A maximum of 8192 user-defined URLs<br>• Local deployment of URL servers |

| Feature | Description | The USG Advantage | Specification |
|---|---|---|---|
| **Antivirus** | Identify and remove viruses to secure the network and prevent problems, such as corruption, privilege escalation, and system crash. | • The high-performance flow detection antivirus engine can defend against 5 million types of viruses and Trojan horses.<br>• The antivirus function is integrated into a firewall without extra hardware systems, providing a low-cost antivirus solution for small- and medium-sized enterprises. | • Virus database: 5 million<br>• Antivirus detection on files transferred using HTTP, FTP, SMTP, POP3, IMAP4, SMB, NFS, and HTTPS<br>• Antivirus detection on compressed files in .zip, .gzip, and .tar formats<br>• Actions on attachments including block, alert, declare, and delete<br>• Application exceptions in antivirus detection<br>• Virus exceptions<br>• A maximum of eight levels of file compression (By default, three levels of file compression are supported.) |
| **DLP** | Prevent the sending of confidential files attempted through modifying the file name extension and filter the content of files to prevent leaks of enterprise key information. | • Reduce the risks of confidential information leaks.<br>• Reduce enterprises' legal risks caused by employees' browsing, publishing, or transmitting illegal information.<br>• Prevent employees from browsing and searching for contents irrelevant to work, improving working efficiency. | • Identified file types: 120+<br>• Identification of real file types to prevent evasion attempted by changing file name extension<br>• Data filtering for common types of files, such as Office and PDF files<br>• Filtering of web pages, search keywords, microblogs, and Internet posts<br>• Filtering of file types and data for decompressed files<br>• A maximum of eight levels of file compression (By default, three levels of file compression are supported.)<br>• Setting of the maximum decompression size of a compressed file (1 to 200 MB). The default value is 100 MB |
| **Mail filtering** | Check IP addresses and filters mail content to enhance mail system security. | • By cooperating with a third-party DNSBL server, the firewall can block spam and consequent security risks.<br>• Provide the email address check function. You can set mail sending and download permissions based on employees' email addresses. In addition, you can control mail attachments to prevent information leaks through attachments. | • Spam filtering<br>• Mail recipient, sender, and title filtering<br>• Filtering of keywords in mail bodies<br>• Filtering of mail attachment names and content keywords<br>• Filtering based on the number of sent or received mail attachments (0 to 10)<br>• Filtering based on the size of sent or received mail attachments (1 to 20,480 KB)<br>• Mail transfer encoding formats: 7bit, 8bit, Base64, QP, and MS TNFF<br>• Mail encapsulation formats: MIME and UUEncode |
| **Application behavior control** | Accurately control and audit user online behavior, including upload, download, and browsing. | • Application behavior control can combine with objects, such as users and time ranges, for differentiated management of application behavior. | • Control over such behavior as HTTP upload, download, and browsing<br>• Control over such behavior as FTP upload, download, and deletion<br>• Control over the size of transferred files. You can set the POST alarm or blocking threshold to 1 MB and set the threshold to 1 GB for other types of download and upload.<br>• Online behavior audit, including mail behavior, IM login and logout, HTTP audit (microblog, posting, web page browsing, file transfer, and search), and audit of FTP commands and file transfer |
| **Anti-APT** | Interwork with Huawei sandbox to detect and defend against malicious files. | • Support integration of third-party antivirus software into the sandbox to detect known viruses in files<br>• Support detection of unknown threats in files<br>• Reduce latency through the high detection performance of the sandbox | • Sandbox detection on files transferred using HTTP(S)/FTP/SMTP(S)/POP3(S)/IMAP4(S)/SMB/NFS<br>• Sharing of detection results with URL and antivirus modules<br>• Detection on PE, PDF, Office, web page, image, and flash files<br>• PE static heuristic detection<br>• Web static detection and web sandbox detection<br>• Virtual environment detection<br>• DGA domain name detection<br>• Botnet, Trojan horse, and worm traffic detection<br>• Detection using third-party antivirus engines<br>• Automatic updates of engines<br>• Cloud sandbox detection |
| **Anti-DDoS** | Detect multiple types of network attacks and protect the hosts in intranets. | • High-performance anti-DDoS algorithms<br>• Auto-learning of defense policy baselines<br>• IP reputation database that can be dynamically updated and block zombie hosts | • Defense against scanning attacks, including IP sweep and port scanning attacks<br>• Defense against malformed-packet attacks including IP spoofing, IP fragment detection, Teardrop, Smurf, Ping of Death, Fraggle, WinNuke, Land, TCP flag validity check |

| Feature | Description | The USG Advantage | Specification |
|---|---|---|---|
| | | | • Defense against special packet control attacks, including oversized ICMP packet control, ICMP unreachable packet control, ICMP redirect packet control, Tracert, IP source route packet control, IP route record packet control, IP timestamp packet control<br>• Defense against DDoS attacks, including SYN-flood, UDP-flood, UDP-frag-flood, HTTP-flood, HTTPS-flood, DNS-request-flood, DNS-reply-flood, and SIP-flood<br>• IP reputation database<br>• Baseline learning |
| **VPN** | Provide secure and reliable connections without changing network status. Users can configure different types of VPNs for branches to access the headquarters or for employees to access enterprise networks. | • Provide high-performance hardware encryption and decryption capabilities<br>• Support automatic negotiation of IKE parameters, simplifying customers' tunnel configuration; support IKE mode selection and extended authentication, meeting requirements for communication with multiple vendors<br>• Support IPsec hot standby to avoid service interruption if the active firewall fails<br>• Support DHCP over IPsec, meeting the requirement for interconnection with base stations in LTE scenarios<br>• Support IKEv2 redirection, implementing IPsec tunnel and VPN traffic load balancing through IPsec clusters<br>• Support DSVPN, the branch with mutative IP address can access to VPN network dynamically. | • IPsec VPN:<br>- IKEv1 and IKEv2 (RFC 4306)<br>- Remote peer: static IP, dynamic DNS, and configuration of two IP addresses or host names at the same time<br>- Authentication method: certificate, RSA key, and pre-shared key<br>- IPsec phase 1 mode: aggressive and main mode; NAT traversal<br>- IPsec phase 2 encapsulation mode: tunnel and transport modes<br>- Phase 1/Phase 2 proposal encryption: DES \| 3DES \| AES-128 \| AES-192 \| AES-256 \| SM4 \| AES-GCM-128 \| AES-GCM-256<br>- Phase 1/Phase 2 proposal authentication: MD5 \| SHA1 \| SHA2-256 \| SHA2-384 \| SHA2-512 \| SM3<br>- Phase 1/Phase 2 Diffie-Hellman group: 1, 2, 5, 14, 15, 16, 19, 20, 21<br>- IKEv2 PRF: AES-XCBC-128 \| HMAC-MD5 \| HMAC-SHA1 \| HMAC-SHA2-256 \| HMAC-SHA2-384 \| HMAC-SHA2-512<br>- IKEv1 XAuth support as client or server mode<br>- IKEV2+EAP authentication<br>- Dead peer detection<br>- Replay detection: configurable width of the anti-replay window.<br>- Network resource pushing: IP, WINS, and DNS server addresses, domain names, and DHCP server addresses.<br>- Reverse route injection.<br>• IPsec VPN deployment modes: Gateway to gateway, Client to Gateway, DSVPN (Hub-spoke).<br>• IPsec VPN configuration options: route-based or policy-based.<br>• IPsec VPN QoS: Per-tunnel traffic limiting: DSCP priorities of IKE packets, DSCP negotiation for traffic to be encrypted or decrypted, and QoS pre-classification<br>• IPsec VPN high availability: Link redundancy, hot standby, and cluster<br>• VPN monitoring and diagnosis: IPsec connection status monitoring, statistics on encrypted and decrypted traffic, and diagnosis of tunnel negotiation failure causes<br>• Other VPN support: DSVPN, LAC/LNS, L2TP over IPsec, GRE, GRE over IPsec, DHCP over IPsec. |
| **SSL VPN** | Enable users to remotely access resources in an internal network. Administrators can configure SSL VPN virtual gateways to control the access of remote users to the internal network in refined granularity. | • SSL VPNs in different virtual systems can share public IP addresses in the public system.<br>- Two-factor authentication: user name + certificate; user name + password + soft/hard token code.<br>- Selection of optimal links.<br>- Isolation between virtual gateways. | • Virtual gateway isolation: Each virtual gateway can have its own access address and authentication mode and manage its own users, roles, and resources.<br>• Customization: Users can customize the login page, home page, logo, welcome message, and title.<br>• Multiple authentication modes: local user authentication, third-party server authentication (including AD, LDAP, RADIUS, and HWTACACS), certificate authentication, and two-factor authentication.<br>• Role-based resource authorization and access control.<br>• Host environment check: Check antivirus software, operating systems, firewall software, ports, and processes on hosts and allow only qualified clients to access.<br>• Cache and file cleanup: Clear caches and specific files generated during SSL VPN logins in a timely manner. |

| Feature | Description | The USG Advantage | Specification |
|---|---|---|---|
| | | | • Multiple access modes for access to different types of resources:<br>- Web proxy mode: allows remote users to access web applications on the internal network and supports two types of resources: web-link and web-rewrite. The access to web-link resources requires a browser plug-in. Mobile devices and PCs can directly access web-rewrite resources through browsers, such as the Internet Explorer, Chrome, FireFox, and UC.<br>- File sharing mode: allows remote users to use browsers to access SMB and NFS file sharing resources on an internal network.<br>- Port forwarding mode: allows remote users to access TCP applications in C/S architecture on an internal network. The applications include Telnet, SSH, VNC, Outlook, and FTP (passive mode) applications.<br>- Network extension mode: allows remote users to access IP resources on an internal network and supports three tunnel splitting modes: full tunnel, split tunnel, and user-defined.<br>• Automatic selection of optimal links. |
| **PKI** | As PKI entities, firewalls use public key technology to ensure identity authentication, confidentiality, data integrity, and non-repudiation during transmission. PKI provides certificate management security services for network applications. | • Certificates used on Huawei firewalls can be managed in a unified manner and used for encryption and decryption functions.<br>- Support four common formats: DER, PEM, PKCS12, and PKCS7. Huawei firewalls can apply for and update certificates through SECP and CMPv2 in online mode. | • Certificate formats: DER, PEM, PKCS12, and PKCS7<br>• Certificate application methods: SCEP-based certificate application and update, CMPv2-based certificate application and update, offline application of device certificates, and LDAP-based certificate download (LDAPv2 and LDAPv3 supported)<br>• Certificate status check modes: HTTP, LDAP, SCEP-based CRL download, and OCSP<br>• RSA key pair management: Multiple RSA key pairs can be created. RSA key pairs can be imported and exported in standard formats (PEM and PKCS#12). Key pairs can be backed up and restored. RSA key pairs can be backed up in batches in hot standby scenarios. |
| **MPLS VPN** | MPLS L3VPN is supported. Firewalls can serve as PEs. | • Interconnect IP and MPLS networks. Firewalls are deployed at MPLS VPN borders to provide security, access control, and IPsec VPN access services.<br>• Firewalls can also serve as PEs to simply network deployment. | • MPLS VPN:<br>- L3VPN: Static LSP, MPLS LDP<br>- MPLSv4, MPLSv6<br>- BGP/MPLS IP VPN, BGP/MPLS IPv6 VPN |
| **Signaling security** | Support security check and filtering for GTP signaling on the wireless core network and SCTP attack defense. | • Support the check and filtering of various GTP protocol fields and defense against overbilling attacks, protecting packets on GPRS networks.<br>• Support SCTP basic status check, SCTP attack defense, and SCTP NAT, meeting security requirements of the core network. | • GTP packet validity check; filtering based on type, length, IE, and extension header; log statistics<br>• Defense against GTP overbilling attacks<br>• SCTP multihoming management<br>• SCTP status check, validity check, and filtering<br>• SCTP NAT |

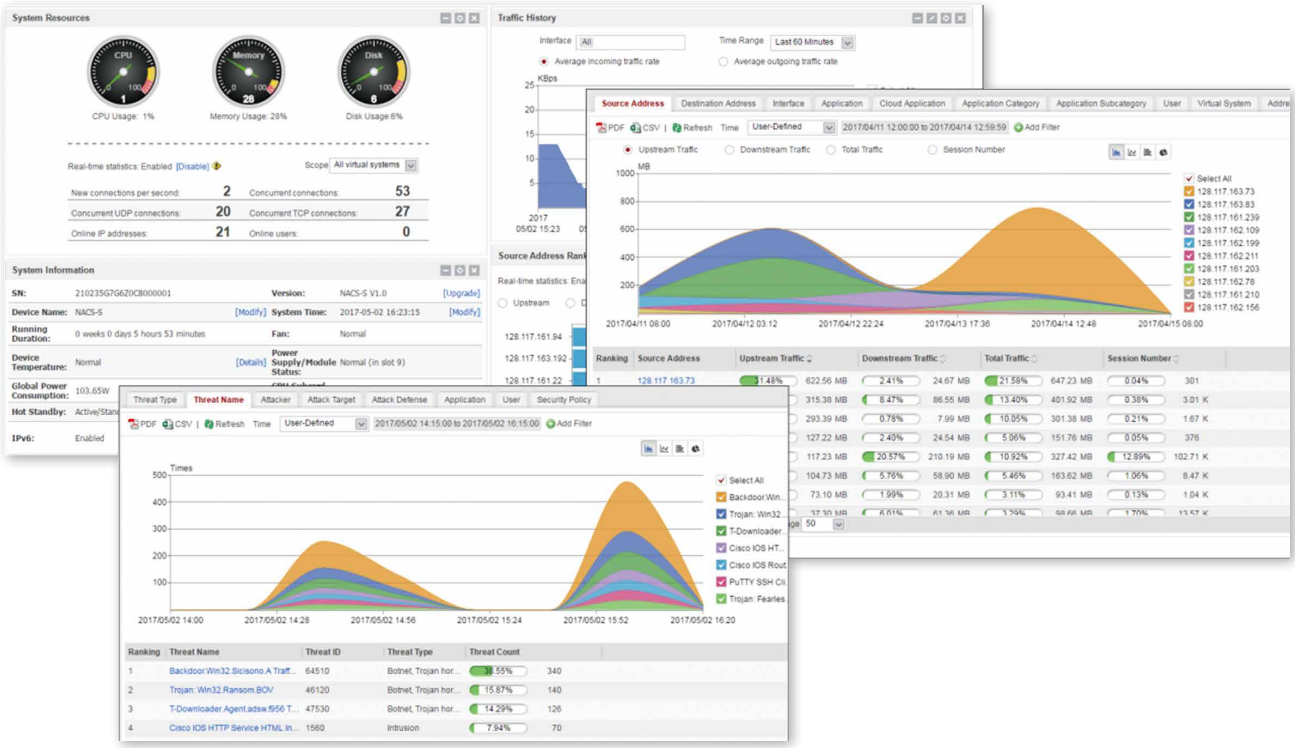
## Visualized management

### Diverse reports

- The traffic, threat, application, URL, and user reports provide visibility into service status, network environment, security postures, and user behaviors.
- The network security analysis reports generated by Huawei security center display the analysis of traffic, threats, and web browsing and data disclosure activities for administrators to understand security vulnerabilities and take mitigation measures.

### Simple security management

- Supports cloud-based management and enables Huawei Agile Controller-Cloud Manager to manage and configure the firewalls.
- The built-in security policy templates simplify policy configuration, and the Huawei-proprietary SmartPolicy technology help administrators optimize and clean up security policies, reducing TCO by 30%.
- The USB deployment technology allows for zero-experience deployment and requires nothing more than plugging the pre-installed USB flash drive to complete the initial configuration, reducing deployment time by 90%.
- The built-in full-featured web UI, network management system and controller, northbound APIs that can be easily integrated, and third-party optimization tools simplify O&M management.




| Feature | Description | The USG Advantage | Specification |
|---|---|---|---|
| **Virtual system** | Multiple logical firewalls can be created on one physical firewall. | • Support many virtual systems with minimum performance degradation, meeting the requirements of a network with many tenants.<br>• Support virtual system resource allocation, meeting operating requirements.<br>• Support communication between virtual systems. | • Virtual system administrators, rights- and domain-based management<br>• Import, export, and saving of virtual system configuration files<br>• Virtual system resource allocation and limitation (bandwidth, concurrent connections, connection rate, policies, users/user groups, online users, security groups, and SSL VPN concurrent users)<br>• Virtual system traffic diversion modes: VLAN, interface, IP address<br>• Allocating interfaces and VLANs to virtual systems<br>• 100 virtual systems for free (only for USG6000s) |

| Feature | Description | The USG Advantage | Specification |
|---|---|---|---|
| **Internet access user management** | With various authentication methods, firewalls directly apply policies to users for granular user management. | • Control network behavior and permissions by user or IP address, providing user-based management for network behavior control and network permission allocation, implementing refined management.<br>• Provide visibility into and statistics on threats and traffic for auditing network behaviors of users.<br>• Map users to dynamic IP addresses and implement policy control based on users. | • Local Portal Authentication<br>• 3rd-party authentication: RADIUSs/LDAP/AD<br>• Welcome/authentication/questionnaire pages customization<br>• Remote portal authentication<br>• Single sign-on (SSO) supported only in RADIUS, AD, and TSM authentication |
| **Device management** | Configure and manage individual devices using the CLI or GUI or centrally manage devices using the eSight network management system (NMS), which is connected to the cloud platform for automatic management. | • Provide convenient and friendly man-machine configuration interfaces.<br>• Centrally manage both firewalls and Huawei network devices, such as routers and switches, through the NMS.<br>• Using the NETCONF or RESTCONF interface based on the YANG model, firewalls can interconnect with third-party cloud management platforms or the open-source OpenStack, simplifying O&M. | • Login to the CLI through the console port, Telnet, SSH, or the CLI console on the web UI<br>• Access to the web UI through HTTPS<br>• Local, HWTACACS server, and RADIUS server authentication for administrators<br>• Firewall monitoring and management through eSight, which can receive firewall logs and alarms as well as perform NAT source tracing<br>• Support for two types of northbound interfaces: NETCONF and RESTCONF interfaces |
| **Intelligent management** | Provide multiple basic configuration optimization capabilities to help administrators better design and optimize device and service management. | • Use predefined or user-defined objects and policy templates to simplify policy definition and make policies easy to understand and maintain.<br>• SmartPolicy helps administrators in policy redundancy analysis, policy matching analysis, and policy tuning, facilitating security management.<br>• Intrusion prevention profiles can be automatically generated using security posture awareness based on application and OS information used by assets on enterprise networks, improving management efficiency. | • Policy object: geographical region or region group, application or application group, service or service group, domain name group, endpoint or endpoint group<br>• Predefined policy templates<br>• Policy redundancy analysis: identifying duplicate and overlapping policies<br>• Policy matching analysis: simplifying policies based on dynamic policy matching statistics<br>• Policy tuning: defining security policies in compliance with the least privilege principle<br>• Security posture awareness: automatically generating intrusion prevention profiles based on application and OS information used by enterprise assets |
| **Logs and reports** | Administrators can view logs and reports to obtain the characteristics of users, applications, security events, and traffic, and take actions based on log details and reports. | • Powerful log processing capability of LogCenter that can store a large number of logs and display threats<br>• Support syslog, binary, netflow, and multiple third-party log formats, all of which can be encrypted<br>• Support scheduled report sending, report customization, and automatic report sending.<br>• Display threat sources and targets through threat and traffic maps | • Local log storage (when local disks are available) and log sending<br>• Dedicated log server (LogCenter) for processing large-volume logs<br>• Supported log formats: syslog and binary<br>• Encrypted transmission of logs of all formats<br>• Configurable storage ratio of different types of logs<br>• Log report by saving time, period, type, or email recipient<br>• Scheduled report sending, report customization, and automatic report sending<br>• Reports on traffic statistics, threats, URLs, policy matching, file blocking, and data filtering<br>• Display of global traffic distribution with details, such as traffic ranking, volume, direction, source IP address, and destination IP address on traffic maps<br>• Display of global threat distribution with details, including the attack source and destination regions and detailed attack information on threat maps |

## Platform

### Reliable and efficient hardware and software platforms

- The support for IPv4 and IPv6 stacks and various routing and switching protocols, diverse interface types, and virtual interfaces accommodate to different networking environments and deployment requirements.
- The new and integrated architecture of the IAE allows the parsing results to be used in multiple subsequent parallel processes to maintain high performance even when multiple defense functions are enabled. The constant update of the signature database keeps enterprises current on emerging security threats.

### Carrier-class availability

- The high-availability hardware design, robust software system, hot standby, link redundancy, and hot backup technologies ensure the stability and high availability.
- The optimal route selection for IPsec allows for dynamic switchover between IPsec tunnels, coupled with intelligent ISP link selection, policy-based routing, and global routing policies in multihoming scenarios, improving the stability and availability of network services.

| Feature | Description | The USG Advantage | Specification |
|---|---|---|---|
| **Interface management** | Support various physical-layer and link-layer access modes. | • Support many types of interfaces and diversified interface features, meeting various networking requirements. | • Ethernet interfaces: GE, 10 GE, 40 GE (supported only by USG9000s), and 100 GE (supported only by USG9000s)<br>• Eth-Trunk and LACP<br>• Ethernet subinterfaces and VLANs<br>• POS interfaces and IP-Trunk (POS interfaces bundled, supported only by USG9000s)<br>• 4G LTE Cellular WAN interfaces<br>• WLAN interfaces |
| **Basic network** | Support basic L2 and L3 networks and application protocols. | • Support various network protocols and provide basic routing capabilities without routers and switches, reducing deployment costs.<br>• Measure the performance of various protocols running on networks through the NQA function.<br>• Collect statistics on network traffic through NetStream for accounting, network management, and attack analysis. | • Basic physical and link-layer protocols: VLAN, PPP, PPPoE, HDLC, and 4G LTE<br>• Basic network protocols: ARP, ICMP, DNS, DHCP, and DHCP Snooping<br>• Support for IPv6: static routes, RIPng, OSPFv3, BGP4+, PBR, IPv6 over IPv4, IPv4 over IPv6, NAT64, hot standby, IPsec, ACL6, bandwidth management, security policies, and various security functions<br>• NQA<br>• NetStream |
| **Routing** | Support IPv4 and IPv6 routing protocols and abundant routing features for network connectivity. | • Based on Huawei VRP, firewalls support abundant routing features to meet various networking requirements.<br>• Comprehensive IPv4 and IPv6 routing features ensure smooth transition from IPv4 to IPv6. | • Static routes<br>• Routing protocols, RIP/RIPng, OSPF/OSPFv3, IS-IS, and BGP/BGP4+<br>• Routing policies<br>• Equal-cost multi-path routes<br>• Route iteration |
| **PBR** | Select routes based on user-defined policies. | • PBR takes precedence over routing tables. Compared with routes in routing tables, PBR specifies forwarding paths for special services based on more dimensions, including the incoming interface, source/destination security zone, source/destination IP address, user, service, and application, increasing flexibility in packet forwarding control. | • Single-next-hop forwarding<br>• Multi-next-hop load balancing<br>• Uplink selection based on bandwidth, priority, or link quality<br>• User- or application-based PBR |

| Feature | Description | The USG Advantage | Specification |
|---|---|---|---|
| **NAT** | Support multiple address and port translation technologies as well as the NAT ALG function. | • Support multiple address and port translation technologies for communication between private and public networks.<br>• Support the NAT ALG function for application-layer packet parsing and address translation. | • NAT No-PAT, NAPT, Smart NAT, EasyIP, NAT Server, triplet NAT, hairpin access, and Destination NAT<br>• NAT ALG for DNS, FTP, H.323, ICQ, ILS, MMS, MSN, NetBIOS, PPTP, QQ, RSH, RTSP, SCCP, SIP, SQLNET, and STUN |
| **IPv6/CGN** | Use NAT444, NAT64, DS-Lite, and CGN for smooth transition from IPv4 to IPv6. | • Support NAT444, DS-Lite, and NAT64.<br>• Support port pre-allocation and incremental allocation. Port ranges can be pre-allocated to users before NAT to improve data source tracing efficiency for log servers.<br>• Support the PCP mechanism to control packet forwarding through upstream devices, reducing keepalive traffic between applications.<br>• Support static mapping for rapid source tracing. | • IPv6: IPv6 over IPv4 tunnel, IPv4 over IPv6 tunnel<br>• CGN: NAT444, NAT64, DS-Lite, PCP, Port range allocation, static NAT mappings |
| **High Availability** | Ensure the stable running of firewalls in three aspects: hardware, software, and links. | • Provide carrier-class high availability mechanisms, such as dual MPUs and SFU redundancy (USG9000).<br>• Ensure service continuity through dual power module backup, hardware bypass, external link detection, and internal software monitoring switchover. | • Dual power modules<br>• Hardware bypass card<br>• Dual MPUs and SFU redundancy (USG9000)<br>• Hot standby: active/standby, active/active, and mirror modes, supporting automatic and manual backup of sessions<br>• VRRP: simple, MD5 authentication, VRRP6<br>• Link-level high availability mechanisms, such as link-group, IP-link, and BFD (interworking with multiple types of routing protocols)<br>• Health check for intelligent uplink selection<br>• Configuration files for disaster recovery |
| **QoS (available only on USG9000)** | Use traffic policing, traffic shaping, and queuing to forward service traffic based on priorities. | • Implement high-performance multi-level queue scheduling based on hardware, improving forwarding efficiency.<br>• Adjust bandwidth allocation based on traffic types to ensure that mission-critical services are prioritized. | • Priority mapping (dot1p-dscp, dscp-dot1p, dscp-dscp, and dot1p-dot1p)<br>• CAR<br>• Traffic shaping<br>• WRED<br>• HQoS for multi-level queue scheduling based on hardware<br>• Application-specific QoS |
| **Bandwidth management** | Limit or prioritize bandwidth to improve the efficiency of bandwidth and prevent bandwidth exhaustion. | • Bandwidth management helps administrators properly allocate bandwidth resources to improve network operating quality. | • Global bandwidth limitation: maximum bandwidth, guaranteed bandwidth, and maximum number of concurrent connections<br>• Per-user bandwidth limitation: maximum bandwidth, guaranteed bandwidth, and maximum number of concurrent connections<br>• Per-IP bandwidth limitation: maximum bandwidth, guaranteed bandwidth, and maximum number of concurrent connections<br>• Bandwidth limitation based on interfaces, applications, and public IP addresses<br>• Traffic priority in traffic profile: re-marking DSCP values in packets<br>• Query of traffic details based on traffic policies |

| Feature | Description | The USG Advantage | Specification |
|---|---|---|---|
| **Intelligent uplink selection** | In a multihoming scenario, a firewall can intelligently select ISP links for load balancing. | • Distribute DNS packets to ISP DNS Servers based on security policies, implementing load balancing from sources.<br>• Provide sticky load balancing. That is, forward and return traffic is sent through the same ISP link. This mechanism accelerates access to internal servers.<br>• When serving as an IPsec gateway, a firewall uses IPsec intelligent uplink selection to dynamically switch IPsec tunnels for load balancing based on IPsec tunnel quality. | • WAN load balancing<br>- Algorithm: bandwidth weight/link quality<br>- Health check: ICMP, TCP, DNS, RADIUS, and HTTP<br>- ISP route preference based<br>- DNS transparent proxy<br>- DNS Rewriting with inbound traffic<br>- IPsec tunnel quality detection and intelligent uplink selection |
| **SLB** | SLB improves service processing capabilities of servers in a server cluster. | • Server Load Balancing (SLB) helps improve the service processing capability of enterprises, improve server performance expansion, and facilitate network operation, maintenance, and adjustment.<br>• High-performance Layer-4 SLB improves forwarding efficiency.<br>• Support multiple load balancing algorithms and support application-specific load balancing.<br>• Support multiple server health detection capabilities for service continuity. | • Layer-4 SLB<br>• Load balancing algorithms: source IP hash, weighted source IP hash, round robin, weighted round robin, least connections, and weighted least connections<br>• Load balancing protocols: TCP, UDP, and IP<br>• Sticky session based on source IP addresses<br>• Health check for real servers: ICMP, TCP, DNS, HTTP, and RADIUS<br>• Real-time statistics on concurrent connections on virtual servers<br>• Five-minute statistics on traffic, sessions, and traffic ratio on real servers |

## 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.

Copyright©2017 Huawei Technologies Co., Ltd. All rights reserved.