



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 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.
- 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

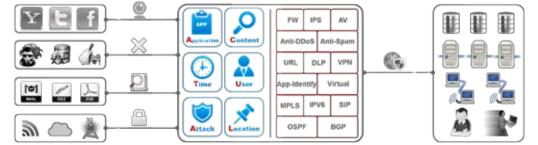
- Provides an Intelligent Awareness Engine (IAE) capable of parallel processing with all security functions enabled after intelligent application identification.
- Improves application-layer protection efficiency and ensures the 10G+ performance with all security functions enabled.

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 USG6300 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 ENTERPRISE ICT SOLUTIONS A BETTER WAY

Specifications

Description 1. Obts 2. Gality 2. Gality <th2. gality<="" th=""> <th2. gality<="" th=""> <th2< th=""><th>Model</th><th>USG6310</th><th>USG6320</th><th>USG6330</th><th>USG6350</th><th>USG6360</th><th>USG6370</th><th>USG6380</th><th>USG6390</th></th2<></th2.></th2.>	Model	USG6310	USG6320	USG6330	USG6350	USG6360	USG6370	USG6380	USG6390	
Pict trong/puit 300 Mbits 700 Mbits <t< td=""><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td></t<>						1				
IPS-AK Throughput 300 Mibits 700 Mibits 500 Mibits 11 Gabits 2 Gabits 3 Gab										
Concurrent seisons 300,000 500,000 3,000,000 4,000,000 4,000,000 4000,000 New seisons personal 10,000 20,000 30,000 30,000 70,000 80,000 VPN Throughput (PSec) 300Mbris 400Mbris 400Mbris <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>										
New sessions par second 10.000 20.000 30.000 80.000 60.000 90.000 80.000 Vin Throughpur (Psee) 300 Mubits 400 Mubits	3 1									
VIN Troughput (PSec) 300Mbits 400Mbits 400Mbits 30bits										
Virtual freewalls 20 50 50 100 100 100 Freed port 8GE 4GE-2Combo 8GE+4SFP 8GE+4SFP Expansion Slots - 2x4VGC 8GE+4SFP 8GE+4SFP Height Can be installed in rack 10 100 100 100 Weight füll configuration 11/4 42/421143.6 42/421143.6 -										
Fixed port GGE 4GE-2Combo GGE-4SFP Expansion S(S) - 2xVIS/C Interface module - 2xVIS/G Dimensions (Hx/WA) 300-2014.5 442-421'43.6 - Weight full configuration 1.7Mg 10 kg - Provides prover supply Adepter Optional - - Operating supprover supply Adepter Optional -										
Expansion Sides - 2xWSIC Interface module - 2xH05C [SPA+BasGE (RI45), 8xGE (SPA), 4xGE (RI45), BYAGE (RI45), 8xGE (SPA), 4xGE (RI45), BYAGE (R			20			50		100	100	
Interface module2x10GE (SP4)-8xGE (RU45), 8xGE (R										
Height Desktop 1U Dimensions (H-WV-D) 300*220*44.5 442*42*143.6 Weight (full configuration) 1.7kg 10 kg PDD Optional. Supports single 300 GB hard disks (hot swappable). Adepter AC power supply Adepter Optional. Supports single 300 GB hard disks (hot swappable). AC power supply - Optional. Supports single 300 GB hard disks (hot swappable). Maimum power 60W 170W Conserting environment. Temperature: 0°C to 40°C/Cr t		-								
Dimensions (H-WAD) 300*20*44.5 442*42*13.6 Weight (full configuration) 1.7kg 10 kg No Optional. Supports single 300 GB hard disks (hot swappable). Adepter Ap power supply 100 V to 240 V Optional. Supports single 300 GB hard disks (hot swappable). Ap power supply 100 V to 240 V Temperature: 0°C to 40°C/C to 40°C/C to 40°C/C to 40°C/C/H to ptional HDD) Maximum power 60W 170W Temperature: 0°C to 40°C/C to 40°C/C to 40°C/C to 40°C/C/H to ptional HDD. Maximum power Temperature: 0°C to 40°C/C to 40°C/C to 40°C/C/H to 40°C/H to 40°C/C/H to 40°C/C/H to 40°C/										
Weight full configuration 1.7kg 10 kg HDD - Optional. Supports single 300 GB hard disks (hot swappable). Redundant power supply Adepter Optional. Operating environment. Temperature: 0°C to 40°C/S°C to 40°C/S°C/S°C to 40°C/S°C/S°C to 40°C/S°C to 40°C/S°C/S°C to 40°C/S°C/S°C/S°C/S°C/S°C/S°C/S°C/S°C/S°C/S	Dimensions (HxWxD)			442*421*43.6						
HDD - Optional Optional Redundant power supply 100 V to 240 V Optional Ac power supply - - Maximum power 60W 170W Opperating environment: Temperature: 0°C to 40°C 5°C to 40°C(with optional HDD) Rementature/Humidity: 100 V to 240 V 170W Opperating environment: Temperature: 0°C to 40°C 5°C to 40°C(5°C to 40°C(with optional HDD) Rementature/Humidity: 100 V to 5906 Humidity: 1050 to 5906 Non-operating environment: Temperature: -40°C to 70°C/Humidity: 596 to 5956 Functions Entiperature: -40°C to 70°C/Humidity: 596 to 5956 Functions Context awareness ActUAL (Application, Content, Time, User, Attack, Location)-based awareness capabilities Context awareness Combination of application identification and virus scanning to recognize the viruses (more than 5 millions), Trojan horses, and malware hidden in application iscurity Finite automation to application iscurity Intrusion prevention Provides over 5000 application and content detection to identify at pps and sensitive information to prevent information leaks Perfores against web application attack, such as cross site scripting and 5QL injection attacks HTDM HTTP/HTTP/HTP/HTP/HTP/HTP/HTP/HTP/HTP/HT										
Redundant power supply Adepter Optional AC power supply 100 V to 240 V DC power supply 00 V to 240 V Deprover supply 60W 170W Temperature: 0°C to 40°C/5°C to 40°C/5°C to 40°C/S°C to 4				5						
AC power supply 100 ¹ to 240 V DC power supply 60W DC power supply 60W Operating environment Temperature: 0°C to 40°C To 40°C To 40°C (with optional HDD) (Emperature: Humidity) 100 ¹ to 5906 Non-operating environment Temperature: 0°C to 70°C/Humidity: 596 to 9566 Functions ACTUAL (Application, Content, Time, User, Attack, Location)-based awareness capabilities Context awareness Eight authentication methods (local, RADUS, HWTACACS, SecureD, AD, CA, LDAP, and Endpoint 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 application for application identification. Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Provides over 5000 signatures are attack identification. Provides over 5000 signatures and their out phising emails Local wheel MLR. fittering with a URL category database that contains over 85 million URLs in over 80 categories Virus scanning and notification for POP3/MIPIMAP email attachments Defense against web application rotocols, specific attacks Web security Real-time ant		Adenter								
DC power supply - Maximum power 60W 170W Maximum power 60W 170W Operating environment: Temperature: 0°C to 40°C Temperature: 0°C to 40°C/S°C to 40°C(with optional HDD) Humidity: 10% to 90% Humidity: 10% to 90% Humidity: 10% to 90% Functions ACTUAL (Application, Content, Time, User, Attack, Location)-based awareness capabilities Context awareness ACTUAL (Application, Content, Time, User, Attack, Location)-based awareness capabilities Context awareness Context awareness Continuation entropic (action, and online update of protocol databases Combination of application identification and virus scanning to recognize the viruses (more than 5 millions), Trojan horse, and malware hidden in applications Combination of application identification and content detection to identify file types and sensitive information to prevent information leaks Provides protocol identification to defend against abnormal protocol behaviors. Supports user defined IPS signatures. Web security Effest and whitelist and whitelist and keyword filtering Web security Real-time anti-span to deter ad filter out phising emails Local whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by attachment type, size, and auantity Vitrusi										
Maximum power 60W 170W Operating environment: Temperature: 0°C to 40°C for Co 40°C/s°C to 40°C/s°C t										
Operating environment: Temperature: 0°C to 40°C from 40°C5°C to 40°C (with optional HDD) (Iemperature/Humidity) Humidity: 10% to 90% Humidity: 10% to 90% Non-operating environment: Temperature: 40°C to 70°C/Humidity: 5% to 55% Functions ACTUAL (Application, Content, Time, User, Attack, Location)-based awareness capabilities 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) Fine-grained identification of over 6000 application protocols, application-specific action, and online update of protocol databases Application security Fine-grained identification and virus scanning to recognize the viruses (more than 5 millions), Trojan horses, and malware hidden in applications Intrusion prevention Provides protocol idatabases Colud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categories URb backlist and whitelist and keyword filtering Real-time anti-spam to detect and filter out phishing emails Local whitelist and backlist, remote real-time backlist, content filtering, keyword filtering, and mall filtering by attachment type, size, and quantity Virus scanning and notification for POP3/SMTP/IMAP email attachments Data security File reassembly and data filtering for mor				170\4/						
(Temperature/Humidity) Humidity: 10% to 90% Humidity: 10% to 90% Non-operating environment Temperature: -40°C to 70°C/Humidity: 59% to 95% Context awareness ACTUAL (Application, Content, Time, User, Attack, Location)-based awareness capabilities Eight authentication methods (local, RADUS, HWTACACS, SecureID, AD, CA, LDAP, and Endpoint 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 of application identification. Provides ver 5000 signatures for attack identification. Provides over 5000 signatures. Cloud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categories Veb security Defense against web application attacks, such as cross-site scripting and SQL injection attacks HTP/HTP/FTP-based content awareness to defend against web viruse Local whitelist and backits, content filtering Local whitelist and backits, remote real-time backits, content filtering, keyword filtering, and mail filtering by attachment type, size, and quantity. Virus scanning and notification of security features, forwarding statistics, users, management operations, views, and resources (su										
Non-operating environment Temperature: -40°C to 70°C/Humidity: 5% to 95% Functions ACTUAL (Application, Content, Time, User, Attack, Location)-based awareness capabilities Eight authentication methods (local, RADUS, HVTRACACS, SecureID, AD, CA, LDAP, and Endpoint Security) Fine-grained identification of over 6000 application protocols, application-specific action, and online update of protocol databases Application security Combination of oper 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 Application prevention Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Methods over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Methods over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Methods over 5000 signatures for attack identification. Provides protocol identification to defend against abnormal protocol behaviors. Supports user-defined IPS signatures. Coud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categories Methods add against web application attacks, su										
Functions ACTUAL (Application, Content, Time, User, Attack, Location)-based awareness capabilities Eight authentication methods (local, RADIUS, HWTACACS, SecureID, AD, CA, LDAP, and Endpoint Security) Fine-grained identification of over 6000 application protocols, application-specific action, and online update of protocol databases Application security 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 Provides over S000 signatures for attack identification. Provides over S000 signatures. Supports user-defined IPS signatures. 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/HTTP/SFTP-based content awareness Coal Whitelist and whitelist and keyword filtering. Real-time anti-spam to detect and filter out plashing emails Local Whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by attachment type, size, and quantify Virus scanning and notification of specific attacks, such as the SYN flood and UDP flood attacks VPN technologies: IPSec VPN, SSL VPN, L2TP VPN, MPLS VPN, and GRE		,								
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) Fine-grained identification of over 6000 application protocols, application-specific action, and online update of protocol databases Application security 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 Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Web security Combination of application attacks, such as cross-site scripting and SQL injection attacks. Real-time anti-span to detect and filter out phishing emails Local whitelist and keyword filtering Local whitelist and keyword filtering over 5000 signatures for over than 30 file types (including Word, Excel, PPT, and PDF), and file blocking for more than 120 file types Data securi		remperature:	-40°C to 70°C	Furnicity: 5%	10 95%					
Context awareness Eight authentication methods (local, RADIUS, HWTACACS, SecureID, AD, CA, LDAP, and Endpoint Security) Fine-grained identification of over 6000 application protocols, application-specific action, and online update of protocol databases Application security 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 protocol identification and content detection to identify file types and sensitive information to application identification. Web security Cloud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categories. UR blacklist and whitelist and keyword filtering Cloud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categories. UR blacklist and whitelist and keyword filter out phishing emails Cloud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categories. Data security Cloud-based on content awareness to defend against web viruses. UR blacklist and whitelist and keyword filtering. Real-time antispam to detect and filter out phishing emails Local whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by atatchoment type. size, and quantity	Functions		lication Contr	nt Time User	Attack Locatio	n) based awa	roposs capabilit	ioc		
Fine-grained identification of over 6000 application protocols, application-specific action, and online update of protocol databasesApplication securityFine-grained identification identification and virus scanning to recognize the viruses (more than 5 millions), Trojan horses, and malware hidden in applicationsApplication securityProvides over 5000 signatures for attack identification.Provides over 5000 signatures for attack identification.Provides over 5000 signatures for attack identification.Supports user-defined IPS signatures.Web securityCloud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categoriesDefense against web application attacks, such as cross-site scripting and SQL injection attacksHTTP/HTTPS/FIP-based content awareness to defend against web virusesReal-time anti-span to detect and filter out phishing emailsLocal whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by attachment type, size, and quantityVirus scanning and notification for POP3/SMTP/IMAP email attachmentsPata securityDefense against wore than 30 file types (including Word, Excel, PPT, and PDF), and file blocking 	Context awareness									
Application securityprotocol 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 leaksIntrusion preventionProvides over 5000 signatures for attack identification. Provides protocol identification to defend against abnormal protocol behaviors. Supports user-defined IPS signatures. 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/HTTP/FTP/based content awareness to defend against web viruses URL blacklist and whitelist and keyword filtering Virus scanning and notification for POP3/SMTP/IMAP 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 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 typesSecurity virtualizationDefense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks such as bandwidths and sessions)Network securityDefense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks standby modeNetwork securityIPvé: static routing, RIP, OSFP, BGP, and IS-IS Thybe. RNP, OSFPA3, BGP44, IPv6 IS-IS, IPv6 RD, and ACL6 Transpart, routing, or hybrid working mode and high availability (HA), including the Active/Ac										
Application security 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 Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Provides over 5000 signatures for attack identification. Provides over 5000 signatures. 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 Web security Real-time anti-span 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 arouning and notification of for POP3/SMTP/IMAP email attachments 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 Defense against wore than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks Network security Defense against more than 10 types of DDoS attacks, such as the SYN flood and UDP f										
Application security horses, and malware hidden in applications Combination of application identification and content detection to identify file types and sensitive information to prevent information leaks Provides over 5000 signatures for attack identification. Provides protocol identification to defend against abnormal protocol behaviors. Supports user-defined IPS signatures. Cloud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categories. Web security HTP/HTPS/FTP-based content awareness to defend against web viruses URL blacklist and whitelist and keyword filtering 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 File reasembly and data filtering for more than 30 file types (including Word, Excel, PPT, and PDF), and file blocking for more than 120 file types Recurity virtualization Virtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions) Detense 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 Ruting Fi										
Indress, and maivare hidden in applicationsCombination of application identification and content detection to identify file types and sensitive information to prevent information leaksProvides over 5000 signatures for attack identification.Provides over 5000 signatures for attack identification.Provides over 5000 signatures for attack identification.Provides over 5000 signatures.Cloud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categoriesDefense against web application attacks, such as cross-site scripting and SQL injection attacksHTTP/HTPS/FTP-based content awareness to defend against web virusesURL blacklist and whitelist and keyword filteringReal-time anti-spam to detect and filter out phishing emailsLocal whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by attachment type, size, and quantityVirus scanning and notification for POP3/SMTP/IMAP email attachmentsData securitySecurity virtualizationVirtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)Network securityDefense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks VPN technologies: IPSec VPN, SSL VPN, LZTP VPN, MPLS VPN, and GRERoutingIntelligent managementIntelligent managementIntelligent managementProvides to remove them, simplifying policy management.Provides a global configuration view and integrated policy management.Provides a global configuration view and	Application security									
Intrusion prevent information leaksProvides over 5000 signatures for attack identification.Provides protocol identification to defend against abnormal protocol behaviors.Supports user-defined IPS signatures.Cloud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categoriesDefense against web application attacks, such as cross-site scripting and SQL injection attacksHTTP/HTTPS/FTP-based content awareness to defend against web virusesURL blacklist and whitelist and keyword filteringReal-time anti-spam to detect and filter out phishing emailsLocal whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by attachment type, size, and quantityVirus scanning and notification for POP3/SMTP/IMAP email attachmentsData leak prevention based on content awarenessSecurity virtualizationSecurity virtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)Network securityNetwork securityProf. RIPng, OSPFV3, BGP4, IPV6 IS-IS, IPV6 RD, and ACL6Vorking mode and availabilityTransparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/ Standby modeProvides over servity policies to remove them, simplifying policy management. 										
Provides over 5000 signatures for attack identification. Intrusion prevention Provides protocol identification to defend against abnormal protocol behaviors. Supports user-defined IPS signatures. Cloud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categories Web security Defense against web application attacks, such as cross-site scripting and SQL injection attacks URL blacklist and whitelist and keyword filtering 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 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 Virus scanning and notifications, for SODS attacks, such as the SYN flood and UDP flood attacks Network security Defense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks Noting IPv4: static routing, RP, DSFP, BGP, and IS-IS Notking mode and availability Transparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/S tandby mode Intelligent management Provides a global configuration view and integrated policy										
Intrusion prevention Provides protocol identification to defend against abnormal protocol behaviors. Supports user-defined IPS signatures. 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/HTTP/FTP-based content awareness to defend against web viruses URL blacklist and whitelist and keyword filtering Eacl witelist and whitelist and keyword filtering Email security 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 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 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 IPV4: static routing, RP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6 Transparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Ac										
Supports user-defined IPS signatures.Web securityCloud-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/FIP-based content awareness to defend against web viruses URL blacklist and whitelist and keyword filtering 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 attachmentsData securityData 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 typesSecurity virtualizationVirtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)Network securityVPN technologies: IPSec VPN, SSL VPN, LZTP VPN, MPLS VPN, and GRENetwing mode and availabilityIPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPF3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6Working mode and availabilityTransparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/ randby modeIntelligent managementEvaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation to automatically optimize security policies. Supports policy management. Provides a global configuration view and integrated policy management. Provides a global configuration view and integrated policy management. Provides a global co										
Here Performance Perfo	Intrusion prevention									
Web security 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 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 leak prevention based on content awareness Data security Data leak prevention based on content awareness Security virtualization Yirul scanning for more than 30 file types (including Word, Excel, PPT, and PDF), and file blocking for more than 120 file types Network security Virtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions) Network security 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 PVe: static routing, RIP, OSPF, BGP, and IS-IS IPVe: static routing, RIP, OSPF, BGP, and IS-IS IPVe: static routing, or hybrid working mode and high availability (HA), including the Active/Active a										
Web securityHTTP/HTTPS/FTP-based content awareness to defend against web viruses URL blacklist and whitelist and keyword filtering 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 attachmentsData securityData 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 typesSecurity virtualizationVirtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)Network securityDefense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks VPN technologies: IPSec VPN, SSL VPN, LZTP VPN, MPLS VPN, and GRERoutingIPV4: static routing, RIP, OSPF BGP, and IS-IS IPV6: RIPng, OSPFV3, BGP4+, IPV6 IS-IS, IPV6 RD, and ACL6Working mode and availabilityTransparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/ Standby modeIntelligent managementEvaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation to automatically optimize security policies. Supports policy management. Provides a global configuration view and integrated policy management. The configurations can be completed in one page.										
H11P/H1PS/FIP-based Content awareness to defend against web Viruses URL blacklist and whitelist and keyword filtering 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 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 Routing IPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6 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 management. Intelligent management Provides a global configuration view and integrated policy management. The configurations can be completed in one page. <td>Web security</td> <td colspan="8"></td>	Web 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 IPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPF, BGP, and IS-IS IS I	Web security									
Email securityLocal whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by attachment type, size, and quantityVirus scanning and notification for POP3/SMTP/IMAP email attachmentsData securityData leak prevention based on content awarenessFile reassembly and data filtering for more than 30 file types (including Word, Excel, PPT, and PDF), and file blocking for more than 120 file typesSecurity virtualizationVirtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)Network securityDefense 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 GRERoutingIPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6Working mode and availabilityTransparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/ standby modeIntelligent managementEvaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation redundant policies to remove them, simplifying policy management.Provides a global configuration view and integrated policy management.The configurations can be completed in on page.										
Enhanceattachment type, size, and quantityVirus scanning and notification for POP3/SMTP/IMAP email attachmentsData securityData leak prevention based on content awarenessFile reassembly and data filtering for more than 30 file types (including Word, Excel, PPT, and PDF), and file blocking for more than 120 file typesSecurity virtualizationVirtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)Network securityDefense 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 GRERoutingIPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6Working mode and availabilityTransparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/ standby modeIntelligent managementEvaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation to automatically optimize security policies. Supports policy management. Provides a global configuration view and integrated policy management. The configurations can be completed in one page.		Real-time anti-spam to detect and filter out phishing emails								
Enhanceattachment type, size, and quantityVirus scanning and notification for POP3/SMTP/IMAP email attachmentsData securityData leak prevention based on content awarenessFile reassembly and data filtering for more than 30 file types (including Word, Excel, PPT, and PDF), and file blocking for more than 120 file typesSecurity virtualizationVirtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)Network securityDefense 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 GRERoutingIPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6Working mode and availabilityTransparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/ standby modeIntelligent managementEvaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation to automatically optimize security policies. Supports policy management. Provides a global configuration view and integrated policy management. The configurations can be completed in one page.	Empil cocurity	Local whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by								
Intelligent managementVirus scanning and notification for POP3/SMTP/IMAP email attachmentsVirus scanning and notification for POP3/SMTP/IMAP email attachmentsData leak prevention based on content awarenessFile reassembly and data filtering for more than 30 file types (including Word, Excel, PPT, and PDF), and file blocking for more than 120 file typesSecurity virtualizationVirtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)Network securityDefense 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 GRERoutingIPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6Working mode and availabilityTransparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/ Standby modeIntelligent managementEvaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation 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.										
Data leak prevention based on content awarenessData securityData security virtualizationSecurity virtualizationVirtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)Network securityDefense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks VPN technologies: IPSec VPN, SL VPN, L2TP VPN, MPLS VPN, and GRERoutingIPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6Working mode and availabilityFanaparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/ standby modeStandby modeIntelligent managementProvides a global configuration view and integrated policy management. The configurations can be completed in one page.										
for more than 120 file typesSecurity virtualizationVirtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)Network securityDefense 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 GRERoutingIPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6Working mode and availabilityTransparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/ Standby modeIntelligent managementEvaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation to automatically optimize security policies. Supports policy management. Provides a global configuration view and integrated policy management. The configurations can be completed in one page.		Data leak prevention based on content awareness								
for more than 120 file typesSecurity virtualizationVirtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)Network securityDefense 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 GRERoutingIPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6Working mode and availabilityTransparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/ Standby modeIntelligent managementEvaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation to automatically optimize security policies. Supports policy management. Provides a global configuration view and integrated policy management. The configurations can be completed in one page.	Data security	File reassembly and data filtering for more than 30 file types (including Word, Excel, PPT, and PDF), and file blocking								
Security virtualizationVirtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)Network securityDefense 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 GRERoutingIPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6Working mode and availabilityTransparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/ Standby modeIntelligent managementEvaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation to automatically optimize security policies. Supports policy management. Provides a global configuration view and integrated policy management. The configurations can be completed in one page.										
security virtualization as bandwidths and sessions) Network security Defense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks Network security Defense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks Routing IPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6 Transparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/ Standby mode 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.										
Network security Defense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks Network security Defense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks 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.										
Network security 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.										
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. one page. The configurations can be completed in one page.	Network security									
Routing 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.										
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.	Routing									
Working mode and availability 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.		Transparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/								
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.Intelligent managementProvides a global configuration view and integrated policy management. The configurations can be completed in one page.	Working mode and availability			nu working me		anaonity (HA),	including the A	netive/Active di	iu Active/	
Intelligent management 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.				bacad an the	accod traffic	d intelligently	apporates as li-	ion bound on the		
Intelligent management 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 a global configuration view and integrated policy management. The configurations can be completed in one page.							o analysis and	the detection o	i conflict and	
one page.	Intelligent management				, , ,	-	T I (1		1	
	<u> </u>	-	obal configurat	ion view and ir	ntegrated policy	management	. The configura	tions can be co	mpleted in	
Provides visualized and multi-dimensional report display by user, application, content, time, traffic, threat, and URL.		one page.								

enterprise.huawei.com