HUAWEI Eudemon200E-G85 Firewalls (Fixed-Configuration)

With the continuous digitalization and cloudification of carrier services, networks play an important role in carrier operations, and must be protected. Network attackers use various methods, such as identity spoofing, website Trojan horses, and malware, to initiate network penetration and attacks, affecting the normal use of carrier networks.

Deploying firewalls on network borders is a common way to protect carrier network security. However, firewalls can only analyze and block threats based on signatures. This method cannot effectively handle unknown threats and may deteriorate device performance. This single-point and passive method does not pre-empt or effectively defend against unknown threat attacks. Threats hidden in encrypted traffic in particular cannot be effectively identified without breaching user privacy.

Huawei's next-generation firewalls provide the latest capabilities and work with other security devices to proactively defend against network threats, enhance border detection capabilities, effectively defend against advanced threats, and resolve performance deterioration problems. The product provides pattern matching and encryption/decryption service processing acceleration functions, which greatly improve the firewall ability to process content security detection and IPSec services.

Product Appearances

Eudemon200E-G85 Firewalls (Fixed-Configuration)

HUAWEI

Product Highlights

Comprehensive and integrated protection

- Integrates the traditional firewall, VPN, intrusion prevention, antivirus, data leak prevention, bandwidth management, URL filtering, and online behavior management functions all in one device.
- Interworks with the local or cloud sandbox to effectively detect unknown threats and prevent zero-day attacks.
- Implements refined bandwidth management based on applications and websites, preferentially forwards key services, and ensures bandwidth for key services.

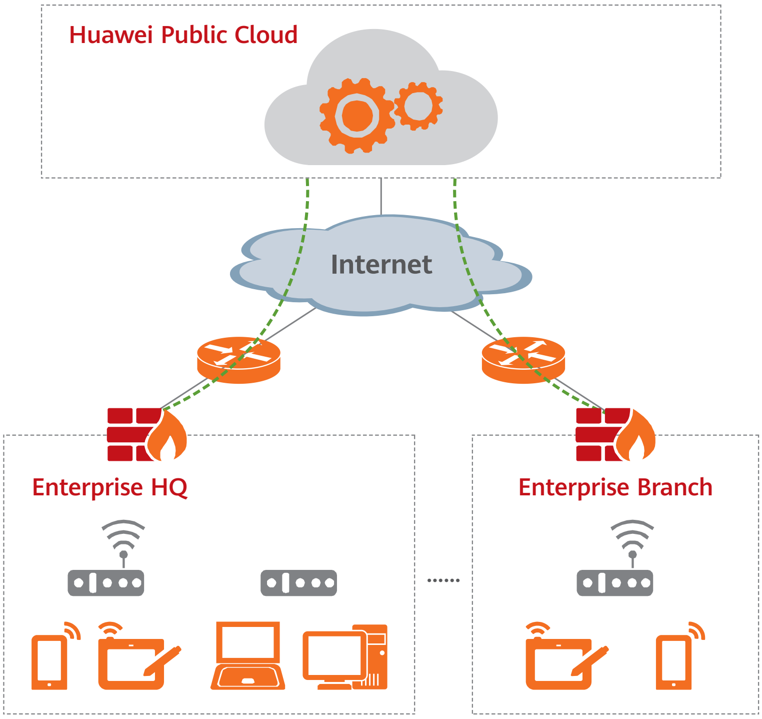
High performance

- Enables pattern matching and accelerates encryption/decryption, improving the performance for processing IPS, antivirus, and IPSec services.

Deployment

Cloud-based management

- Firewalls can proactively register with and be quickly incorporated into the cloud-based management platform to implement quick device deployment without manual attendance.
- Remote service configuration management, device monitoring, and fault management are used to implement cloud-based management of mass devices and simplify O&M.



Carrier border protection

- Firewalls are deployed at the network border. The built-in traffic probe can extract packets of encrypted traffic to monitor threats in encrypted traffic in real time.
- The deception function is enabled on the firewalls to proactively respond to malicious scanning behavior, protecting carriers against threats in real time.
- The policy control, data filtering, and audit functions of the firewalls are used to monitor social network applications to prevent data breach and protect carrier networks.

Software Features

Feature	Description
Integrated protection	Integrates firewall, VPN, intrusion prevention, antivirus, data leak prevention, bandwidth management, anti-DDoS, URL filtering, and anti-spam functions; provides a global configuration view; manages policies in a unified manner.
Application identification and control	Identifies over 6000 applications and supports the access control granularity down to application functions; combines application identification with intrusion detection, antivirus, and data filtering, improving detection performance and accuracy.
Cloud-based management mode	Initiates authentication and registration to the cloud-based management platform to implement plug-and-play and simplify network creation and deployment. Supports remote service configuration, device monitoring, and fault management, implementing the management of mass devices in the cloud.
Cloud application security awareness	Controls carrier cloud applications in a refined and differentiated manner to meet carriers' requirements for cloud application management.
Intrusion prevention and web protection	Accurately detects and defends against vulnerability-specific attacks based on up-to-date threat information. The firewall can defend against web-specific attacks, including SQL injection and XSS attacks.
Antivirus	Rapidly detects over 5 million types of viruses based on the daily-updated virus signature database.
Data leak prevention (DLP)	Inspects files to identify the file types, such as WORD, EXCEL, POWERPOINT, and PDF, based on file content, and filters the file content.
Bandwidth management	Manages per-user and per-IP bandwidth in addition to identifying service applications to ensure the network access experience of key services and users. Control methods include limiting the maximum bandwidth, ensuring the minimum bandwidth, and changing application forwarding priorities.
URL filtering	Provides a URL category database with over 120 million URLs and accelerates access to specific categories of websites, improving access experience of high-priority websites. Supports DNS filtering, in which accessed web pages are filtered based on domain names. Supports the SafeSearch function to filter resources of search engines, such as Google, to guarantee access to only healthy network resources.
Behavior and content audit	Audits and traces the sources of the accessed content based on users.

Feature	Description
Load balancing	Supports server load balancing and link load balancing, fully utilizing existing network resources.
Intelligent uplink selection	Supports service-specific PBR and intelligent uplink selection based on multiple load balancing algorithms (for example, based on bandwidth ratio and link health status) in multi-egress scenarios.
VPN encryption	Supports multiple highly available VPN features, such as IPSec VPN, SSL VPN, L2TP VPN, MPLS VPN, and GRE, and provides the Huawei-proprietary VPN client SecoClient for SSL VPN, L2TP VPN, and L2TP over IPSec VPN remote access.
DSVPN	Dynamic smart VPN (DSVPN) establishes VPN tunnels between branches whose public addresses are dynamically changed, reducing the networking and O&M costs of the branches.
SSL-encrypted traffic detection	Detects and defends against threats in SSL-encrypted traffic using application-layer protection methods, such as intrusion prevention, antivirus, data filtering, and URL filtering.
SSL offloading	Replaces servers to implement SSL encryption and decryption, effectively reducing server loads and implementing HTTP traffic load balancing.
Anti-DDoS	Defends against more than 10 types of common DDoS attacks, including SYN flood and UDP flood attacks.
User authentication	Supports multiple user authentication methods, including local, RADIUS, HWTACACS, AD, and LDAP. The firewall supports built-in Portal and Portal redirection functions. It can work with the Agile Controller to implement multiple authentication modes.
Security virtualization	Supports virtualization of multiple types of security services, including firewall, intrusion prevention, antivirus, and VPN. Users can separately conduct personal management on the same physical device.
Security policy management	Manages and controls traffic based on VLAN IDs, quintuples, security zones, regions, applications, URL categories, and time ranges, and implements integrated content security detection. Provides predefined common-scenario defense templates to facilitate security policy deployment. Provides security policy management solutions in partnership with FireMon and AlgoSec to reduce O&M costs and potential faults.
Diversified reports	Provides visualized and multi-dimensional report display by user, application, content, time, traffic, threat, and URL. Generates network security analysis reports on the Huawei security center platform to evaluate the current network security status and provide optimization suggestions.
Routing	Supports multiple types of routing protocols and features, such as RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+, and IPv6 IS-IS.
Deployment and reliability	Supports transparent, routing, and hybrid working modes and high availability (HA), including the Active/Active and Active/Standby modes.

Specifications

System Performance and Capacity

Model	Eudemon200E-G85
Firewall Throughput[1] (1518/512/64-byte, UDP)	8/8/4 Gbit/s
Firewall Latency (64-byte, UDP)	18 µs
Concurrent Sessions (HTTP1.1)[1]	4,000,000
New Sessions/Second (HTTP1.1)[1]	80,000
IPsec VPN Throughput[1] (AES-256 + SHA256, 1420-byte)	6 Gbit/s
SSL Inspection Throughput[2]	550 Mbit/s
Concurrent SSL VPN Users (Default/Maximum)	100/1000
Security Policies (Maximum)	15,000
Virtual Firewalls	100
URL Filtering: Categories	More than 130
URL Filtering: URLs	A database of over 120 million URLs in the cloud
Automated Threat Feedback and IPS Signature Updates	Yes, an industry-leading security center from Huawei (http://sec.huawei.com/sec/web/index.do)
Third-Party and Open-Source Ecosystem	Open API for integration with third-party products, providing RESTful and NetConf interfaces Other third-part management software based on SNMP, SSH, and Syslog Cooperation with third-party tools, such as Tufin, AlgoSec and FireMon Collaboration with anti-APT solution
Centralized Management	Centralized configuration, logging, monitoring, and reporting is performed by Huawei eSight and eLog
VLANs (Maximum)	4094
VLANIF Interfaces (Maximum)	1024

1. The performance is tested under ideal conditions based on RFC2544 and RFC3511. The actual result may vary with deployment environments.
2. SSL inspection throughput is measured with IPS enabled and HTTPS traffic using TLS v1.2 with AES128-GCM-SHA256.
*SA: indicates service awareness.

Hardware Specifications

Model	Eudemon200E-G85
Dimensions (H x W x D) mm	43.6 x 442 x 420
Form Factor/Height	1U
Fixed Interface	2 x 10GE (SFP+) + 8 x GE Combo + 2 x GE WAN
USB Port	1 x USB 2.0 + 1 x USB 3.0
Weight (Full Configuration)	5.8 kg
External Storage	Optional, SSD (M.2) card supported, 240 GB
AC Power Supply	100V to 240V
Typical power consumption of the machine	35 W
Power Supplies	Single AC power supply; optional dual AC power supplies
Operating Environment (Temperature/Humidity)	Temperature: 0°C to 45°C Humidity: 5% to 95%, non-condensing
Non-operating Environment	Temperature: -40°C to +70°C Humidity: 5% to 95%, non-condensing

Ordering Information

Product	Model	Description
Eudemon200E-G85	UEudemon200E-G85-AC	Eudemon200E AC Host (2*10GE (SFP+) + 8*GE Combo + 2*GE WAN, AC power)
	UEudemon200E-G85-DC	Eudemon200E DC Host (2*10GE (SFP+) + 8*GE Combo + 2*GE WAN, DC power)
Function License		
SSL VPN Concurrent Users	LIC-EDMLM-SSLVPN-100	Quantity of SSL VPN Concurrent Users (100 Users)
	LIC-EDMLM-SSLVPN-200	Quantity of SSL VPN Concurrent Users (200 Users)
	LIC-EDMLM-SSLVPN-500	Quantity of SSL VPN Concurrent Users (500 Users)
	LIC-EDMLM-SSLVPN-1000	Quantity of SSL VPN Concurrent Users (1000 Users)
Eudemon License		
IPS Update Service	LIC-E200E-G85-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to E200E-G85)
	LIC-E200E-G85-IPS-3Y	IPS Update Service Subscribe 36 Months (Applies to E200E-G85)
URL Filtering Update Service	LIC-E200E-G85-URL-1Y	URL Remote Query Service Subscribe 12 Months (Applies to E200E-G85)
	LIC-E200E-G85-URL-3Y	URL Remote Query Service Subscribe 36 Months (Applies to E200E-G85)

Product	Model	Description
Antivirus Update Service	LIC-E200E-G85-AV-1Y	AV Update Service Subscribe 12 Months (Applies to E200E-G85)
	LIC-E200E-G85-AV-3Y	AV Update Service Subscribe 36 Months (Applies to E200E-G85)
Threat Protection Bundle (IPS, AV, URL)	LIC-E200E-G85-TP-1Y-OVS	Threat Protection Subscription 12 Months (Applies to E200E-G85)
	LIC-E200E-G85-TP-3Y-OVS	Threat Protection Subscription 36 Months (Applies to E200E-G85)
Flow Probe Function	LIC-E200E-G85-FP	Flow Probe Function (Applies to E200E-G85)

GENERAL DISCLAIMER

The information in this document may contain predictive statement including, without limitation, statements regarding the future financial and operating results, future product portfolios, new technologies, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.