Huawei USG6500E Series AI Hardware Firewall Deep Packet Filtering Metrics - Official Technical Overview & Hardware Datasheet

EXECUTIVE SUMMARY

The Huawei HiSecEngine USG6500E Series AI Firewall represents a purpose-built enterprise security platform engineered for small-to-medium enterprises and chain organizations requiring deep packet filtering with hardware-accelerated threat inspection. The platform integrates a multi-core architecture with dedicated forwarding, encryption, and pattern-matching co-processing engines, delivering measurable acceleration for content security inspection and IPsec traffic processing. At the silicon level, the USG6500E embeds an AI algorithm acceleration hardware unit rated at 8 TOPS (16-bit floating-point), specifically designed to support advanced threat defense model execution at line-rate without degrading forwarding performance. The deep packet filtering subsystem leverages Huawei's proprietary Content-based Detection Engine (CDE) alongside the NGE threat defense engine, achieving a 95% detection rate for unknown threat variants through local AI inference. This document provides a comprehensive technical overview of the USG6500E Series deep packet filtering hardware metrics, interface configurations, and deployment specifications for enterprise edge security architectures.



HARDWARE ARCHITECTURE & SILICON

The USG6500E Series is built upon a multi-core processor architecture that offloads critical deep packet inspection functions to dedicated hardware co-processors. Three primary acceleration engines operate in parallel with the general-purpose CPU: a network processor (NP) for small-packet forwarding, a pattern-matching engine for signature-based content inspection, and an encryption/decryption co-processor for IPsec and SSL workloads. This architectural separation ensures that enabling deep packet filtering features—such as intrusion prevention, antivirus, and application identification—does not collapse throughput as observed in software-only firewall designs. The embedded AI acceleration silicon provides 8 TOPS of 16-bit floating-point compute, enabling on-box execution of PE Class 2.0 AI algorithms for malicious file detection and unknown threat variant identification. The CDE engine

performs data type identification, content extraction, and scanning in a pipelined hardware-assisted flow, supporting the detection of over five million virus signatures with daily updates. The NGE engine handles IPS, antivirus, and URL filtering functions, with the URL classification database exceeding 120 million entries.

KEY FEATURES & DEEP PACKET FILTERING LOGIC

- Hardware-Accelerated Deep Inspection: The pattern-matching co-processor accelerates IPS and antivirus signature evaluation, delivering up to 2x improvement in content security processing throughput compared to software-only inspection paths.
- AI-Driven Unknown Threat Detection: The 8 TOPS AI accelerator executes PE Class 2.0 inference models locally, achieving a 95% detection rate for previously unknown malicious file variants without cloud round-trip latency.
- Application Identification at Function Granularity: The deep packet filtering engine identifies more than 6,000 applications and can distinguish between application functions — for example, separating WeChat text messages from voice messages—for precise access control.
- Integrated Threat Defense Pipeline: Firewall, VPN, IPS, antivirus, data leak prevention, bandwidth management, Anti-DDoS, URL filtering, and anti-spam functions operate under a unified policy framework with a global configuration

view.

- Encrypted Traffic Inspection Without Decryption: The platform interworks with Huawei HiSec Insight to detect threats in encrypted traffic flows without requiring SSL/TLS decryption, preserving user privacy while maintaining security visibility.

- IPv6 Deep Packet Filtering: Full IPv6 capability extends deep inspection to IPv6 traffic, including IPv6 intrusion detection, virus filtering, attack protection, and IPSec6, supporting enterprise IPv6 migration without security degradation.

COMPLIANCE & STANDARDS

The USG6500E Series aligns with enterprise security deployment requirements across multiple dimensions. The platform supports IPSec VPN, SSL VPN, L2TP VPN, and GRE, with cryptographic algorithm support including DES, 3DES, AES, SHA, and the Chinese SM2/SM3/SM4 suite. For IPv6 transition scenarios, the device provides NAT66, DSLite tunneling, 64 translation, and 66 translation capabilities alongside dual-stack operation. The threat defense engines receive automated signature updates from Huawei's security center, ensuring continuous compliance with emerging threat intelligence. The platform has been recognized in the Gartner Magic Quadrant for Network Firewalls as a Challenger for consecutive years and holds vulnerability management system certification.

TECHNICAL SPECIFICATIONS

The following table summarizes the core hardware and deep packet filtering metrics for the primary USG6500E Series models. Performance values are representative of the fixed-configuration 1RU models (USG6525E, USG6555E, USG6565E, USG6585E) unless otherwise noted.

Parameter	**Specification**
Form Factor	1RU fixed-configuration chassis (USG6525E/6555E/6565E/6585E); desktop form factor for USG6510E/6530E
Fixed Interfaces (USG6525E/6555E/6565E/6585E)	2 x 10GE SFP+ + 8 x GE Combo + 2 x GE WAN
Fixed Interfaces (USG6510E/6530E)	2 x GE SFP + 10 x GE (USG6510E); 2 x 10GE SFP+ + 10 x GE (USG6530E)
AI Acceleration Hardware	8 TOPS (16-bit floating-point) dedicated AI inference engine
Co-Processing Engines	Network Processor (NP), pattern-matching engine, encryption/decryption engine

Threat Detection Engine	NGE (IPS/AV/URL) + CDE (AI-based malicious file detection, PE Class 2.0)
Unknown Threat Detection Rate	95% (AI local inference)
Application Identification	6,000+ applications, function-level granularity
Virus Signature Coverage	5,000,000+ signatures, daily updates
URL Classification Database	120,000,000+ URLs
Local Storage	Optional M.2 SSD, 64 GB / 240 GB (model-dependent)
IPv6 Deep Inspection	IPv6 IPS, virus filtering, attack protection, IPSec6, NAT66, DSLite, 64/66 translation
VPN Protocols	IPSec, SSL, L2TP, GRE; SM2/SM3/SM4, AES, SHA, DES, 3DES
Management	Cloud management (plug-and-play), Web UI 2.0, SNMP, NETCONF
Power Supply	Single AC (USG6525E-AC); redundant configurations per model variant

ORDERING SKU INFORMATION

Base system configurations are differentiated by fixed interface complement and throughput tier. The USG6525E provides 2 x 10GE SFP+ ports, 8 x GE Combo ports, and 2 x GE WAN ports in a 1RU chassis. The USG6555E, USG6565E, and USG6585E scale deep packet filtering throughput progressively within the same 1RU form factor. Security subscription licenses are ordered separately as 1-year or 3-year terms for IPS, URL filtering, and antivirus signature updates, with SKU patterns including LIC-USG6525E-IPS-1Y, LIC-USG6555E-URL-3Y, and LIC-USG6585E-AV-1Y. Local storage for logging and content caching is available as an optional M.2 SSD module in 64 GB or 240 GB capacities, depending on model.

