Huawei USG6600E Next-Generation Firewall Deep Packet Inspection Engine - Official Technical Overview & Hardware Datasheet

EXECUTIVE SUMMARY

The Huawei USG6600E series represents a paradigm shift in perimeter security architecture, engineered to address the exponential growth of encrypted traffic and the corresponding degradation of deep packet inspection (DPI) efficacy. Traditional firewalls suffer from severe performance penalties when tasked with decrypting and inspecting TLS/SSL flows, often forcing administrators to choose between security fidelity and network throughput. The USG6600E resolves this dichotomy through a dedicated hardware acceleration architecture that integrates the Adaptive Security Engine (ASE) with pattern matching and cryptographic co-processing engines . This purpose-built silicon offloads computationally intensive DPI tasks — including signature matching for intrusion prevention, antivirus scanning, and application identification—from the main CPU, ensuring line-rate inspection even when advanced security profiles are enabled. Designed for medium-to-large enterprise data centers and campus borders, the platform delivers up to 80 Gbit/s of throughput in a compact 1U form factor, establishing a new benchmark for security density and energy efficiency in next-generation firewall (NGFW) deployments .



ARCHITECTURE & CHASSIS DESIGN

The USG6600E hardware architecture is centered on a proprietary Network Processor (NP) coupled with dedicated co-processing engines for pattern matching and encryption/decryption . This heterogeneous compute topology ensures that the data plane remains non-blocking even under heavy inspection loads. The NP handles high-speed packet forwarding and flow table management, while the pattern matching engine performs deterministic finite automaton (DFA) traversal for IPS signatures at wire speed. The cryptographic engine accelerates IPSec and SSL/TLS operations, preserving CPU cycles for management and logging functions.

The chassis is a fixed-configuration 1U appliance available in multiple port densities, ranging from 12×GE copper plus 8×GE SFP and 4×10GE SFP+ on the

entry model, to high-density variants featuring 4×40GE QSFP+ alongside 28×10GE SFP+ ports . This port flexibility eliminates the need for additional interface cards in most deployment scenarios, reducing bill-of-materials complexity and improving mean time between failures (MTBF) by removing electromechanical connectors. Optional onboard storage (SSD up to 240 GB or HDD up to 1 TB) supports local logging, on-box threat analytics, and caching for URL filtering databases .

HARDWARE FEATURES

The Deep Packet Inspection capability of the USG6600E is underpinned by three distinct hardware engines. First, the Content-based Detection Engine (CDE) leverages AI-accelerated pattern matching to scan for malware signatures across hundreds of millions of virus samples, achieving a 95% detection rate for unknown variants through behavioral heuristics . Second, the intrusion prevention system (IPS) engine performs stateful protocol anomaly detection and signature matching without introducing jitter, a critical requirement for real-time voice and video traffic traversing the firewall. Third, the application identification engine classifies over 6,000 applications — including granular control within applications such as distinguishing WeChat text from voice—by analyzing packet payloads and behavioral patterns, not merely port numbers .

For encrypted traffic inspection, the platform adopts a dual-pronged approach. It can perform native TLS decryption using the onboard crypto engine for compliance-heavy environments, or it can leverage the embedded flow probe to extract metadata from encrypted sessions and transmit it to Huawei HiSec Insight for behavioral analysis without decryption . This latter capability preserves privacy and eliminates the latency associated with proxy-based decryption, while still identifying command-and-control (C2) traffic, DGA domains, and encrypted brute-force attacks.

COMPLIANCE & STANDARDS

The USG6600E series is designed to meet the stringent requirements of enterprise and government network security frameworks. It supports IPv6 fully, including dual-stack operations, IPv6 policy routing, and IPv6-aware threat detection, aligning with global IPv6 transition mandates . The platform complies with Common Criteria (CC) EAL4+ certification criteria for firewall and VPN security targets, ensuring independent validation of its security functional requirements. For cryptographic compliance, the device supports SM2/SM3/SM4 algorithms for Chinese markets and standard AES/SHA families for international deployments, meeting FIPS 140-2 and 商用密码认证 requirements where applicable.

TECHNICAL SPECIFICATIONS

The following table summarizes the hardware and performance parameters of representative models within the USG6600E family, illustrating the scalability of the DPI engine across different throughput tiers.

Parameter	**Specification**
Form Factor	1RU fixed-configuration chassis
Switching Capacity	Up to 80 Gbit/s (model dependent)
DPI/NGFW Throughput	12 Gbit/s to 20 Gbit/s (FW+IPS+AV, mixed traffic)
IPS Throughput	12 Gbit/s (dedicated engine)
IPSec VPN Throughput	20 Gbit/s to 30 Gbit/s (AES-256+SHA256, 1420-byte)
Concurrent Sessions	6,000,000 to 12,000,000 (HTTP 1.1)
New Sessions/Second	200,000 to 400,000
Fixed Interfaces	Varies: 12×GE RJ45 + 8×GE SFP + 4×10GE SFP+ up to 4×40GE QSFP+ + 28×10GE SFP+
Power Supply	1+1 Redundant AC/DC (optional or standard, model dependent)
Operating Temperature	0°C to 45°C

Storage	Optional SSD 240GB / HDD 1TB

ORDERING OPTIONS

Customers may select from a graduated model hierarchy based on required inspection throughput and port density. Entry-level models (USG6610E/6620E) suit branch or mid-size campus egress with 1G/10G mixed interfaces and NGFW throughput suitable for 1-5 Gbit/s inspection needs. Mid-range models (USG6630E/6650E) deliver 12-20 Gbit/s of combined firewall, IPS, and antivirus throughput for data center border protection. High-end fixed-configuration models (USG6680E) offer up to 80 Gbit/s forwarding capacity and 4 × 40GE interfaces for collapsed core deployments . All models support optional dual redundant AC or DC power supplies and are available with or without bundled SSL VPN user licenses. Advanced security subscriptions — including IPS signature updates, antivirus databases, and URL filtering categories — are licensed separately on a per-device, per-year basis.

