# Refurbished Firewall Cryptographic Processing Core Diagnostic Validation Report - Official Technical Overview & Hardware Datasheet

## EXECUTIVE SUMMARY

The Refurbished Firewall Cryptographic Processing Core Diagnostic Validation Report represents the definitive technical authority on the recertification and performance validation of carrier-grade firewall cryptographic processing cores. This document serves as the comprehensive validation framework for enterprise and service provider network security architects who require absolute assurance in refurbished cryptographic hardware. Each unit undergoes a rigorous multi-stage diagnostic protocol that validates cryptographic throughput, entropy generation quality, key management integrity, and sustained packet processing under maximum security load conditions. The diagnostic validation process ensures that every refurbished cryptographic processing core meets or exceeds original equipment manufacturer specifications for IPSec, SSL/TLS, and MACsec cryptographic operations, delivering full line-rate encryption and decryption capabilities without compromise. This report details the proprietary validation methodology, hardware-level diagnostic procedures, and certification criteria that establish the refurbished cryptographic core as a trusted, auditable, and fully warranted component of mission-critical network security infrastructure.



HARDWARE ARCHITECTURE & SILICON

The cryptographic processing core is built upon a dedicated security ASIC architecture that integrates multiple cryptographic engines, a true random number generator (TRNG), and a secure key store within a tamper-resistant package. The diagnostic validation process interrogates each silicon subsystem independently to verify functional integrity and performance parity with new-old-stock specifications. The cryptographic acceleration complex supports symmetric algorithms including AES-256-GCM, AES-256-CBC, ChaCha20-Poly1305, and 3DES, alongside asymmetric operations including RSA-4096, ECDSA P-384, and Diffie-Hellman key exchange. The secure key store is validated for zero key retention across power cycles, ensuring forward secrecy compliance. The entropy source is subjected to NIST SP 800-90B statistical validation to confirm the randomness quality required for

cryptographic key generation. Diagnostic validation includes boundary scan testing of the ASIC interconnect, memory integrity verification of the cryptographic context buffer, and sustained thermal stress testing to confirm operational stability across the full enterprise temperature range.

## KEY FEATURES & VALIDATION LOGIC

The diagnostic validation framework encompasses the following critical assessment domains:

- Cryptographic Throughput Validation: Sustained AES-256-GCM encryption and decryption at line-rate across all physical interfaces, with latency variance maintained within ±5% of OEM baseline specifications.
- Entropy Quality Assurance: Continuous statistical monitoring of the TRNG output during a 72-hour burn-in period, validated against NIST SP 800-90B and BSI AIS 31 standards.
- Key Management Integrity: Verification of secure key generation, storage, and zeroization procedures, including validation of tamper-evident hardware mechanisms and secure boot chain-of-trust.
- Protocol Conformance Testing: IPSec, SSL/TLS 1.3, and MACsec protocol operation validated against RFC and IEEE standards, including interoperability testing with major vendor implementations.

- Sustained Load Endurance: 168-hour continuous operation at 100% cryptographic load with automated error detection and correction verification.
- Power Cycle Resilience: 500 consecutive power cycles with full cryptographic context recovery and zero key material leakage between cycles.

## COMPLIANCE & STANDARDS

The Refurbished Firewall Cryptographic Processing Core Diagnostic Validation Report certifies compliance with the following standards and regulatory frameworks:

- FIPS 140-3 Level 2 Cryptographic Module Validation (where applicable to the validated module boundary)
- Common Criteria EAL4+ Protection Profile for Network Devices
- NIST SP 800-90B Entropy Source Validation
- NIST SP 800-38A through 800-38F Cryptographic Algorithm Validation
- IEEE 802.1AE MACsec Frame Security Standard
- IETF RFC 4301, 4303, 7296 (IPSec), and RFC 8446 (TLS 1.3)
- RoHS 2011/65/EU and WEEE 2012/19/EU Environmental Compliance
- UL 60950-1 and IEC 62368-1 Safety Certification
- ETSI EN 300 019 Environmental Test Standards for Telecom Equipment

TECHNICAL SPECIFICATIONS

[Text...]

| Parameter | Specification |
|---|---|
| Form Factor | 1RU Standard / Modular Chassis Compatible |
| Cryptographic Throughput | AES-256-GCM: 100 Gbps sustained bidirectional |
| Switching Capacity | Non-blocking 200 Gbps full-duplex fabric |
| Asymmetric Performance | RSA-4096: 45,000 ops/sec; ECDSA P-384: 120,000 ops/sec |
| Entropy Source | NIST SP 800-90B compliant TRNG, 72-hour validated |
| Key Store | Secure non-volatile storage, zero retention across power cycles |
| IPSec Tunnel Capacity | 50,000 concurrent tunnels at line-rate |
| MACsec Sessions | IEEE 802.1AE compliant, 10,000 secure channels |
| Power Supply | Dual Hot-Swappable Redundant AC/DC (-48V DC option) |

| | |
|---|---|
| Thermal Range | -5°C to +55°C operating, 0°C to +70°C short-term |
| Diagnostic Certification | 168-hour sustained load validation, full report provided |
| Mean Time Between Failures | > 450,000 hours validated MTBF |
| Warranty | 90-day comprehensive refurbishment warranty with diagnostics report |
| Compliance | FIPS 140-3 Level 2, Common Criteria EAL4+, RoHS, WEEE |

ORDERING SKU INFORMATION

