Secured Edge Node Technical Compliance Register: IPSec VPN Performance Testing Report

PRODUCT IDENTIFICATION

This document serves as the definitive technical compliance register for the IPSec VPN Performance Testing Report, detailing the validation framework, test bed architecture, and empirical performance metrics for the vendor's carrier-grade IPSec VPN acceleration hardware. This register is intended for network architects, security engineers, and procurement specialists requiring verifiable performance data for secure edge deployments.

The evaluation encompasses a comprehensive suite of performance tests conducted under controlled laboratory conditions, utilizing industry-standard traffic generators and measurement equipment. All metrics presented herein are derived from certified test procedures and represent steady-state performance levels achievable in a production network environment.

SYSTEM HARDWARE TOPOLOGY

The validation test bed is architected around a high-performance IPSec VPN acceleration platform, featuring a purpose-built cryptographic offload engine. The system topology comprises the Device Under Test (DUT) interconnected with Spirent TestCenter and Ixia traffic generation equipment via multiple 10GbE and 25GbE interfaces. The control plane is managed by an integrated dual-core ARM processor, while the data plane leverages a dedicated FPGA-based encryption module for wire-speed IPsec processing.

Network connectivity is established through a series of isolated VLANs to simulate realistic multi-tenant environments. The test bed includes a remote VPN gateway peer, configured with identical cryptographic parameters to ensure symmetrical performance evaluation. All connections are terminated

using SFP+ and SFP28 optical transceivers to guarantee signal integrity at high data rates.

DATA & CONTROL PLANE CAPABILITIES

The architecture separates control and data plane operations to maximize throughput and minimize latency. The control plane handles IKEv1/IKEv2 negotiation, Security Association (SA) management, and routing protocol exchanges, while the data plane performs high-speed encryption/decryption using AES-GCM-256, AES-CBC-256, and ChaCha20-Poly1305 algorithms. The cryptographic engine incorporates a true random number generator (TRNG) for key material generation and supports hardware-accelerated Public Key Infrastructure (PKI) operations for digital certificate validation.

Performance testing is divided into three primary categories: Throughput (measured in Gbps) with varying packet sizes (64, 256, 512, 1024, and 1518 bytes), Latency (measured in microseconds under 50% and 90% load conditions), and Simultaneous Tunnel Capacity (maximum number of active IPSec tunnels). Additionally, the platform is evaluated for its ability to maintain session persistence under dynamic routing changes and during control plane failover events.

COMPONENT BREAKDOWN

Core Component 1: Cryptographic Offload Processor - A custom ASIC designed for parallel encryption pipelines, supporting up to 100 Gbps of combined IPSec traffic.

Core Component 2: Network Interface Controllers - Dual-port 25GbE and quad-port 10GbE with RDMA over Converged Ethernet (RoCE) support.

Core Component 3: System Memory - 16GB DDR4 ECC with dedicated memory channels for SA and session table storage.

Core Component 4: Management Module - Out-of-band 1GbE management port with SSHv2 and SNMPv3 support, integrated with a hardware security module (HSM) for secure key storage.

Core Component 5: Power Supply Units - Dual, hot-swappable 550W AC/DC PSUs with 1+1 redundancy and 80 PLUS Platinum efficiency rating.

OPERATIONAL SPECS MATRIX

Test Scenario 1 (IMIX Traffic): The device achieves 98.7 Gbps of aggregate throughput using a mix of packet sizes (64B: 10%, 570B: 40%, 1518B: 50%) with AES-GCM-256 encryption. Average latency is recorded at 18 microseconds, with a maximum jitter of 4 microseconds under sustained load.

Test Scenario 2 (Full 64-Byte Packets): Under worst-case, small-packet

conditions (64 bytes), the platform delivers 45.2 Gbps, processing 78 million packets per second (Mpps), showcasing its ability to handle high packet-rate applications.

Test Scenario 3 (Tunnel Scalability): The system successfully establishes and maintains 16,384 active IPSec tunnels. SA establishment rate is measured at 720 new tunnels per second, with a session table lookup time of under 100 nanoseconds per packet.

Parameter	**Specification**
Maximum IPSec Throughput	100 Gbps (AES-GCM-256, 1518B packets)
Maximum IPSec Throughput (64B)	45.2 Gbps (78 Mpps)
Maximum Active IPSec Tunnels	16,384
SA Establishment Rate	720 tunnels per second
Latency (IMIX traffic, 50% load)	12 microseconds
Latency (IMIX traffic, 90% load)	18 microseconds
Form Factor	2RU Rack-Mountable Chassis
Network Interfaces	2x 25GbE SFP28, 4x 10GbE SFP+
Management Interfaces	1x 1GbE RJ45 (Out-of-Band), 1x Console RJ45
Cryptographic Algorithms	AES-GCM-256, AES-CBC-256, ChaCha20-Poly1305

IKE Versions	IKEv1 and IKEv2 with NAT-Traversal
Power Supply	Dual 550W AC/DC (1+1 Redundant)
Power Consumption (Typical)	425W
Operating Temperature Range	0°C to +45°C
Storage Temperature Range	-40°C to +70°C
Humidity (Operating)	5% to 90% (Non-Condensing)
MTBF (Telcordia SR-332)	350,000 hours
Regulatory Approvals	NEBS Level 3, FCC Part 15A, CE, RoHS
Cryptographic Certification	FIPS 140-2 Level 3

REGULATORY COMPLIANCE

This performance testing report is governed by a strict regulatory framework to ensure data integrity and reproducibility. All testing procedures adhere to the methodology defined in RFC 2544 (Benchmarking Methodology for Network Interconnect Devices) and RFC 3511 (Benchmarking Methodology for Firewall Performance). Specific deviations from these standards are documented in the test report annexes.

Environmental testing is conducted in accordance with Telcordia GR-63-CORE for physical protection and GR-1089-CORE for electromagnetic compatibility.

The hardware platform is certified for operation under NEBS Level 3 (Network Equipment Building Systems) standards, ensuring compliance for central office and data center deployments. Additional certifications include FCC Part 15 Class A, CE Mark (EN 55032/EN 55024), and RoHS Directive 2011/65/EU.

Security assurance is validated through FIPS 140-2 Level 3 certification for the cryptographic module, with the testing environment maintaining a documented chain of custody for all test equipment and software versions. The test report is subject to internal peer review and external audit to confirm adherence to the vendor's quality management system (ISO 9001:2015) and information security policy (ISO/IEC 27001:2013).