Secured Routing Platform - Official Technical Overview & Hardware Datasheet

CORE SECURITY POSITIONING

This document serves as the definitive technical reference and product datasheet for the Secured Routing Platform, a next-generation edge gateway router engineered to establish a new benchmark for network infrastructure security, performance, and operational resilience. Designed for the demanding environments of enterprise campuses, carrier points of presence, and distributed branch locations, this platform delivers integrated, hardware-accelerated security without compromising line-rate forwarding performance. It represents a strategic evolution in edge routing, moving beyond traditional perimeter defense to embed security at the very core of the data plane.



HARDWARE MACSEC CAPABILITIES

The cornerstone of the platform's security architecture is its comprehensive, hardware-accelerated implementation of IEEE 802.1AE (MACsec). This is not a software overlay but a deeply integrated function within the packet forwarding ASIC, enabling wire-speed encryption and decryption for all traffic traversing the interface. By securing data at Layer 2, the platform provides robust protection against man-in-the-middle attacks, eavesdropping, and other physical-layer vulnerabilities across the entire network fabric.

- **Line-Rate MACsec Encryption:** The dedicated hardware engine supports 256-bit encryption keys, ensuring data confidentiality and integrity at speeds matching the platform's full switching capacity. This eliminates the performance penalty typically associated with software-based encryption solutions.
- **Flexible Key Agreement:** Full support for the MACsec Key Agreement (MKA) protocol (IEEE 802.1X-2010) allows for dynamic, centralized key management and distribution. This integrates seamlessly with existing RADIUS and AAA infrastructures, providing policy-based access control and automated key rotation.
- **Comprehensive Interface Support:** MACsec is available across a wide range of physical interface types, including Gigabit Ethernet (RJ45) and Fiber (SFP/SFP+), ensuring security can be enforced on both copper and optical links

throughout the network.

- **Multi-level Security:** The implementation supports both static (pre-shared key) and dynamic (MKA) operation modes, providing deployment flexibility to match operational requirements.

PHYSICAL INTERFACE ISOLATION

Beyond cryptographic security, the platform incorporates advanced physical isolation mechanisms to safeguard the integrity of the hardware and the network. These measures are critical for multi-tenant environments and for preventing accidental or malicious misconfiguration.

- **Hardware-Based Line Card Isolation:** Each line card and its associated interfaces are logically and electrically isolated at the hardware level. This prevents a failure or security compromise on one port from impacting traffic or control plane operation on other ports.
- **Secure Management Plane:** A dedicated management Ethernet port and an out-of-band (OOB) serial console port provide physically separated access for system administration. This management plane can be entirely firewalled from the data plane, ensuring administrative access remains available even during network anomalies.
- **Hardware Root of Trust (e.g., TPM):** The platform incorporates a dedicated

security co-processor (Trusted Platform Module) to establish a hardware root of trust. This secures the boot process, verifies the integrity of the system firmware and OS image, and provides secure storage for cryptographic keys and certificates, preventing unauthorized software execution and platform tampering.

- **Discrete Port Disablement:** Individual physical interfaces can be administratively disabled at the hardware level, providing a mechanism to shut down compromised or unused ports to prevent unauthorized physical access.

DETAILED PARAMETERS

TECHNICAL SPECIFICATIONS

The following table details the key hardware and performance parameters for the Secured Routing Platform.

Parameter	Specification
Form Factor	1RU Standard (19-inch Rack Mountable)
Switching Capacity	360 Gbps (Full-Duplex)
Throughput	Up to 268 Mpps (64-byte packets)
Processor / CPU	Multi-core x86 Network Processor

	(e.g., 4-core, 2.4 GHz)
Memory	16 GB DDR4 ECC, 64 GB M.2 SATA SSD for storage
Power Supply	Dual Hot-Swappable Redundant AC (100-240VAC, 50/60Hz), Optional DC (-48VDC)
Power Consumption (Typical)	120W (Base Chassis without optics)
Network Interfaces	8x 1/10 Gigabit Ethernet SFP+ ports, 4x 10/100/1000BASE-T RJ45 ports (Combo), 2x 40 Gigabit Ethernet QSFP+ uplink ports
Management Ports	1x RJ45 10/100/1000BASE-T (Out-of-Band), 1x RJ45 Serial Console
MACsec Support	Yes, Hardware-Accelerated (IEEE 802.1AE) on SFP+ and QSFP+ ports
Security Features	Hardware Root of Trust (TPM 2.0), Secure Boot, Control Plane Policing (CoPP)
Operating Temperature	0°C to 45°C (32°F to 113°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Operating Humidity	10% to 90% (non-condensing)
MTBF	> 250,000 hours at 25°C

TELECOM CERTIFICATIONS

To ensure reliable operation within diverse and demanding telecommunications environments, the Secured Routing Platform has been rigorously tested and certified against a comprehensive suite of industry standards.

- **Safety:** UL 60950-1 / CSA C22.2 No. 60950-1, EN 60950-1, IEC 60950-1, and the updated EN 62368-1 for Audio/Video, Information and Communication Technology Equipment.
- **EMC:** FCC Part 15 (Class A), EN 55032 (Class A), EN 55024, CISPR 32, and VCCI for EMC compliance.
- **Environmental:** NEBS GR-63-CORE and NEBS GR-1089-CORE (Level 3), ensuring resilience to environmental stress such as temperature extremes, humidity, vibration, and electromagnetic interference.
- **Regulatory:** RoHS and WEEE compliance for environmental sustainability.
- **Carrier Ethernet:** MEF 9, MEF 14, and MEF 26 certified, confirming compliance with Carrier Ethernet service definitions, performance metrics, and management standards.
- **Security:** FIPS 140-2 validated cryptographic module (pending), providing

assurance on the strength and integrity of the implemented cryptographic algorithms.

SECURED TOPOLOGY

The Secured Routing Platform is ideally positioned as a high-performance, security-centric gateway at the edge of enterprise campus networks, between a trusted internal infrastructure and untrusted external networks (e.g., WAN or internet). In a typical deployment, the platform connects to multiple internal distribution switches via high-speed fiber uplinks using secured MACsec connections. Multiple routers can be deployed in an active/active or active/standby configuration using VRRP or similar protocols for high availability. A dedicated management network provides secure out-of-band access for administration and monitoring. This architecture ensures that all inter-site and external traffic is cryptographically isolated and integrity-checked at the network boundary, delivering unmatched security and performance.

