Zero-Trust Access Gateway Enforcement on ISP Enterprise Perimeter Firewalls - Official Technical Overview & Hardware Datasheet

EXECUTIVE SUMMARY

Zero-Trust Access Gateway Enforcement on ISP Enterprise Perimeter Firewalls represents a purpose-built security and routing platform designed to operationalize zero-trust principles at the carrier edge. Unlike conventional perimeter firewalls that rely on implicit trust zones, this solution enforces continuous identity and device posture verification for every session traversing the ISP enterprise boundary. It integrates high-throughput policy enforcement, hardware-anchored cryptographic attestation, and line-rate forwarding into a single carrier-grade chassis, enabling service providers to deliver managed zero-trust access services to enterprise customers without compromising backbone performance.

The platform terminates IPsec, TLS, and MACsec tunnels at the perimeter, applies micro-segmentation policies per subscriber or device, and integrates with external identity providers via SAML, OIDC, and RADIUS. All policy decisions are logged, auditable, and exportable to SIEM platforms, satisfying regulatory mandates for access traceability. With dual hot-swappable power supplies, redundant fans, and field-replaceable line cards, the system maintains carrier-grade availability while enforcing zero-trust controls at scale.



HARDWARE ARCHITECTURE & SILICON

The Zero-Trust Access Gateway Enforcement platform is built on a modular 2RU chassis with a non-blocking switch fabric and dedicated security co-processors. The data plane leverages a programmable ASIC pipeline that performs packet classification, tunnel encapsulation/decapsulation, and policy lookup in a single pass, ensuring no performance penalty for encrypted traffic. A separate security engine accelerates AES-GCM, SHA-2, and elliptic-curve cryptography, enabling IPsec throughput up to 200 Gbps per line card.

Control plane functions run on redundant x86 host processors with secure boot, TPM 2.0, and measured launch. The hardware root of trust ensures that only signed firmware images execute, preventing supply-chain tampering. Interface

isolation is enforced at the PHY level, with dedicated management ports physically separated from data ports. MACsec is supported on all 10/25/40/100GbE interfaces, providing hop-by-hop encryption for untrusted links.

KEY FEATURES & ROUTING LOGIC

- Zero-Trust Policy Engine: Per-session identity verification using mTLS, device certificates, and contextual signals such as geolocation, time-of-day, and endpoint posture.
- Micro-Segmentation: Granular east-west and north-south policy enforcement with up to 1 million concurrent sessions and 256,000 security groups.
- Hardware-Accelerated IPsec/TLS: Line-rate encryption with support for IKEv2, Suite B, and post-quantum hybrid key exchange.
- MACsec on All Ports: IEEE 802.1AE-2018 compliant hop-by-hop encryption for 10GbE to 400GbE interfaces.
- Identity Provider Integration: Native SAML 2.0, OIDC, RADIUS, and LDAP connectors; SCIM for automated user provisioning.
- Continuous Authentication: Session re-evaluation every 30 seconds; automatic quarantine on posture change.
- SIEM & Syslog Export: Structured logging in CEF, LEEF, and JSON formats; streaming telemetry via gNMI.

- Carrier-Grade Redundancy: Dual hot-swappable AC/DC power supplies, N+1 fan trays, and hitless software upgrades.

COMPLIANCE & STANDARDS

The platform complies with major telecommunications and security standards, including:

- IEEE 802.1AE-2018 (MACsec)
- IEEE 802.1X-2020 (Port-Based Network Access Control)
- IETF RFC 7296 (IKEv2), RFC 8221 (IPsec Cryptographic Algorithms)
- NIST SP 800-207 (Zero Trust Architecture)
- NIST FIPS 140-3 (Cryptographic Module Validation)
- Common Criteria EAL4+ (under evaluation)
- NEBS Level 3 (GR-1089, GR-63)
- MEF 3.0 CE, MEF 6.3, MEF 10.4
- RoHS, WEEE, and REACH environmental directives

TECHNICAL SPECIFICATIONS

The system supports up to 400 Gbps of zero-trust enforcement throughput per chassis, with 2RU and 4RU configurations. It offers 48x 10/25GbE, 16x 40/100GbE, and 4x 400GbE line cards, all with MACsec capability. The security

engine delivers 200 Gbps IPsec and 150 Gbps TLS inspection. Latency is under 3 microseconds for policy enforcement and under 5 microseconds for encryption. The platform supports up to 1 million concurrent zero-trust sessions and 256,000 security groups. Dual redundant AC or DC power supplies, front-to-back airflow, and operating temperature range of 0°C to 45°C.

Parameter	Specification
Form Factor	2RU or 4RU Modular Chassis
Switching Capacity	Up to 400 Gbps zero-trust enforcement throughput
IPsec Throughput	200 Gbps per chassis
TLS Inspection Throughput	150 Gbps per chassis
Concurrent Sessions	1,000,000 zero-trust sessions
Security Groups	256,000 micro-segmentation groups
MACsec Support	IEEE 802.1AE-2018 on all 10/25/40/100/400GbE ports
Interface Options	48x 10/25GbE, 16x 40/100GbE, 4x 400GbE per line card
Latency	Under 3 µs policy enforcement, under 5 µs encryption
Power Supply	Dual Hot-Swappable Redundant AC/DC

Cooling	N+1 Hot-Swappable Fan Trays, Front-to-Back Airflow
Operating Temperature	0°C to 45°C
Compliance	NIST SP 800-207, FIPS 140-3, Common Criteria EAL4+, NEBS Level 3, MEF 3.0

ORDERING SKU INFORMATION

- ZTAG-2RU-CHASSIS: 2RU chassis with dual control processors, 4 line card slots, 2 power supplies, 3 fan trays.

- ZTAG-4RU-CHASSIS: 4RU chassis with dual control processors, 8 line card slots, 4 power supplies, 6 fan trays.

- ZTAG-LC-48X25: 48-port 10/25GbE line card with MACsec and hardware security engine.

- ZTAG-LC-16X100: 16-port 40/100GbE line card with MACsec and hardware security engine.

- ZTAG-LC-4X400: 4-port 400GbE line card with MACsec and hardware security engine.

- ZTAG-SW-ZT: Zero-trust policy software license, per 100,000 sessions.

- ZTAG-SW-IDP: Identity provider integration license, per 10,000 users.

- ZTAG-PWR-AC: 2000W AC hot-swappable power supply.

- ZTAG-PWR-DC: 2000W DC hot-swappable power supply.

- ZTAG-FAN: Hot-swappable fan tray.

