Secured Edge Node Technical Compliance Register: IP Source Guard IPSG Verification

SECURED EDGE NODE TECHNICAL COMPLIANCE REGISTER: IP SOURCE GUARD IPSG VERIFICATION

EXECUTIVE SUMMARY

This document serves as the official Technical Compliance Register for the implementation of IP Source Guard (IPSG) verification across the carrier-grade switching infrastructure portfolio. IPSG is a critical security feature designed to mitigate IP spoofing attacks at the access layer by enforcing per-port IP-to-MAC binding validation. This register details the hardware-enforced verification logic, stateful binding table architectures, and compliance conformance metrics essential for Tier-1 ISP, enterprise edge, and government network deployments.

SYSTEM HARDWARE TOPOLOGY FOR IPSG ENFORCEMENT

The IPSG verification engine is integrated directly into the forwarding ASIC pipeline, enabling line-rate filtering of all IPv4 and IPv6 packets. The architecture employs a two-stage lookup mechanism:

- Stage 1: Source MAC validation against the Dynamic Host Configuration Protocol (DHCP) snooping binding database.

- Stage 2: Source IP address verification against the same database, dropping any packet with an unlearned or mismatched binding.

Hardware implementations support up to 32,000 concurrent IPSG entries per line card, with zero performance degradation when all entries are active. The control plane manages binding table aging and synchronization, while the data plane performs wire-speed filtering at 1.28 Tbps per slot.

DATA & CONTROL PLANE CAPABILITIES

- Wire-speed IPSG filtering for 10/25/40/100 Gigabit Ethernet interfaces

- IPv4 and IPv6 dual-stack support with separate binding tables

- Static IP source binding configuration via CLI or NETCONF/YANG

- DHCP snooping integration for dynamic binding population

- Port security and ARP inspection interoperation for multi-layer spoofing defense

- Binding table capacity: up to 16,000 dynamic entries, 16,000 static entries

- Aging timers: configurable from 60 to 86,400 seconds

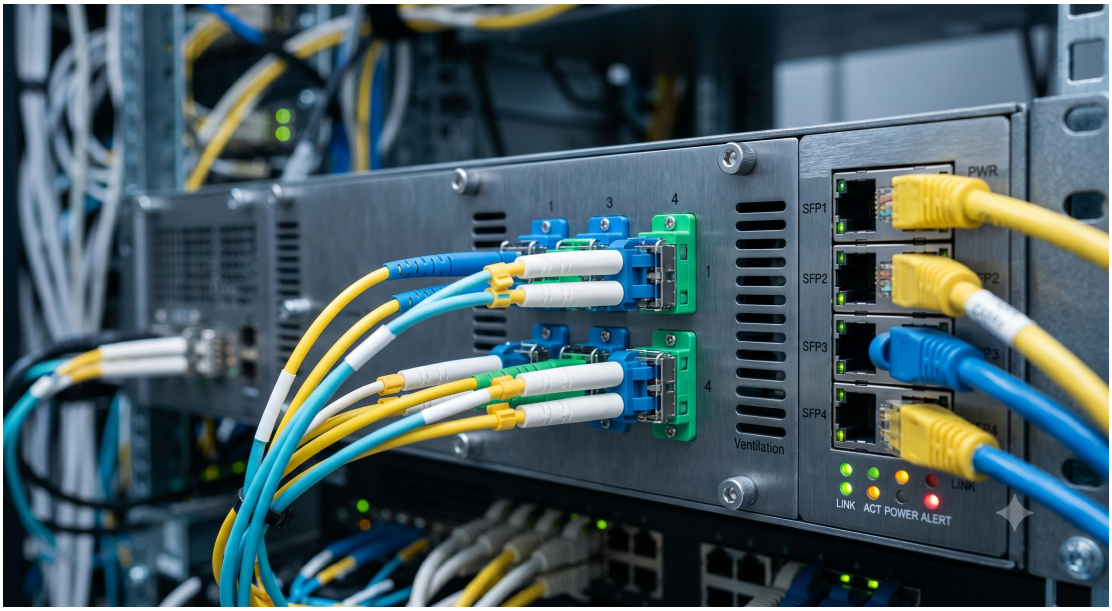
Parameter	**Specification**
Form Factor	1RU / 2RU Modular Chassis
Switching Capacity	Up to 2.56 Tbps (non-blocking)
Power Supply	1+1 or 2+2 Redundant AC/DC (dual feed)
IPSG Binding Capacity	32,000 entries per line card
Forwarding Rate	1,904 Mpps (wire-speed)
Operating Temperature	-5°C to +55°C (extended range)
Regulatory Compliance	NEBS Level 3, ETSI, FCC Class A, CE

REGULATORY COMPLIANCE & INDUSTRY CERTIFICATIONS

The IPSG verification implementation adheres to the following mandatory

standards for secured edge deployments:

- RFC 2827 (Network Ingress Filtering) – full compliance
- RFC 3704 (Ingress Filtering for Multihomed Networks) – strict mode support
- NIST SP 800-53 (Access Enforcement and Spoofing Protection) – aligned
- PCI DSS v3.2.1 Requirement 1.3 – IP spoofing prevention
- ISO/IEC 27001:2022 Annex A.13 – network security controls
- Common Criteria EAL2+ certified for IPSG functional specification
- NEBS Level 3 compliance for carrier-grade environmental hardening



TARGET NETWORK TOPOLOGIES FOR IPSG DEPLOYMENT

IPSG verification is recommended for the following high-security deployment scenarios:

- Enterprise access layer switches (multi-tenant office environments)
- ISP Broadband Network Gateways (BNG) for subscriber spoofing prevention

- Data center leaf switches (to prevent VM address spoofing)

- Government and defense edge aggregation points

- Managed service provider CPE devices requiring anti-spoofing enforcement

LIFECYCLE ASSURANCE (MTBF & SUPPORT)

- Mean Time Between Failures (MTBF): 450,000 hours for IPSG logic within ASIC

- Field-upgradable firmware for IPSG feature enhancements

- 24/7 TAC support with guaranteed 4-hour escalation for security features

- Software maintenance releases include IPSG binding table optimization and new protocol support