Secured Routing Platform: Edge Router Unicast Reverse Path Forwarding (uRPF) Anti-Spoofing Checklist

CORE SECURITY POSITIONING

The Edge Router Unicast Reverse Path Forwarding (uRPF) Anti-Spoofing Checklist represents a foundational security control plane enforcement mechanism for carrier-grade and enterprise edge routing platforms. In modern IP transport architectures, source address spoofing remains one of the most exploited vectors for volumetric denial-of-service (DDoS) attacks, amplification attacks, and botnet propagation. This document defines the authoritative operational, architectural, and silicon-level requirements for deploying uRPF across high-performance edge routing hardware. It is intended for network architects, security engineers, and pre-sales technical teams responsible for hardening Layer 3 trust boundaries.



HARDWARE MACSEC CAPABILITIES

The forwarding silicon on the subject edge routing platform supports line-rate uRPF enforcement without compromising packet throughput or latency budgets. Strict Mode uRPF is executed in hardware at the ingress pipeline stage, ensuring that every packet is validated against the Forwarding Information Base (FIB) before any exception path or CPU punt is considered. The platform provides dedicated ternary content-addressable memory (TCAM) slices for uRPF prefix lookup, enabling simultaneous execution of Strict, Loose, and Feasible Path uRPF modes per interface or sub-interface. Hardware-based MACsec (IEEE 802.1AE) can be coupled with uRPF to provide cryptographic link-layer integrity in addition to source-address validation.

PHYSICAL INTERFACE ISOLATION

Each physical line card maintains isolated ingress forwarding domains, preventing cross-slot spoofing leakage. The backplane fabric enforces a per-interface uRPF context that cannot be overridden by software misconfiguration. Interface-level uRPF is available on all 10G/25G/40G/100G/400G ports, with per-VLAN and per-VRF granularity. Unicast RPF check failures result in silent packet discard or ICMP unreachable generation, configurable per administrative policy.

DETAILED PARAMETERS

- Strict uRPF: Validates source address against the exact ingress interface in the FIB; default recommended mode for stub and access-edge interfaces.
- Loose uRPF: Validates only that the source prefix exists in the FIB regardless of ingress interface; suitable for asymmetric multi-homed deployments.
- Feasible Path uRPF: Uses the RPF table and considers all feasible paths, preventing drops in multihomed environments while retaining anti-spoofing efficacy.
- VRF-Aware uRPF: Supports per-VRF RPF tables for MPLS L3VPN and EVPN environments.
- Allow Self-Ping: Optional per-interface exemption for local management traffic.

- Allow Default Route: Enables uRPF validation when only a default route is present; recommended only on trusted core uplinks.
- Logging & Telemetry: Per-interface uRPF drop counters exported via gNMI, SNMP, and sFlow for real-time spoofing detection.

TELECOM CERTIFICATIONS

The platform complies with applicable telecom and security standards including but not limited to: IEEE 802.1AE (MACsec), RFC 2827 (BCP 38), RFC 3704 (Ingress Filtering for Multihomed Networks), RFC 5635, and MEF 10.3 for Carrier Ethernet service assurance. NEBS Level 3 and ETSI EN 300 019 environmental compliance are supported on carrier-grade SKUs.

SECURED TOPOLOGY

Recommended deployment model: uRPF Strict Mode on all customer-facing and peer-facing interfaces; Loose uRPF on upstream transit interfaces where asymmetric routing is expected; Feasible Path uRPF on multihomed enterprise WAN edges. Combine with RTBH (Remotely Triggered Black Hole) and BGP Flowspec for comprehensive anti-spoofing and DDoS mitigation.

Parameter	**Specification**

uRPF Modes	Strict, Loose, Feasible Path, VRF-Aware
Forwarding Enforcement	Hardware line-rate, ingress pipeline, TCAM-based
Interface Granularity	Per-physical port, per-VLAN, per-sub-interface, per-VRF
Supported Interface Speeds	1G / 10G / 25G / 40G / 100G / 400G
MACsec Support	IEEE 802.1AE, 128-bit and 256-bit cipher suites
Telemetry Export	gNMI, SNMPv3, sFlow, IPFIX
Compliance Standards	RFC 2827 (BCP 38), RFC 3704, MEF 10.3, NEBS Level 3
Redundant Power	Dual hot-swappable AC/DC, 1+1 redundancy
Form Factor	1RU to 14RU modular chassis options
Operating Temperature	0°C to 40°C (Commercial) / -40°C to 65°C (Hardened SKU)

