Secured Edge Node Technical Compliance Register: NAT and Firewall Integration on Cisco Routers

# SECURED EDGE NODE TECHNICAL COMPLIANCE REGISTER: NAT AND FIREWALL INTEGRATION ON CISCO ROUTERS

## EXECUTIVE SUMMARY

This document serves as the definitive technical compliance and performance register for the integration of Network Address Translation (NAT) and advanced firewall services on the Cisco ASR 1000 Series Aggregation Services Routers. Designed for the modern secured edge node, this platform redefines carrier-grade infrastructure by converging high-performance routing with stateful security services. The Cisco ASR 1000 Series natively supports multi-gigabit NAT and Zone-Based Firewall (ZFW) throughput, delivering up to 20 Gbps of integrated services without compromising on system resiliency or control-plane integrity . This register details the architectural innovations, performance matrices, and compliance standards that establish this platform as the cornerstone of secure, high-density enterprise and service provider edge networks.


SYSTEM ARCHITECTURE & HARDWARE OVERVIEW

The foundation of this secured edge solution lies in the Cisco QuantumFlow Processor, a revolutionary silicon architecture that centralizes all forwarding and service plane operations . This design ensures complete logical and physical separation between the system routing, forwarding, and I/O planes, creating a robust environment where security services do not degrade forwarding performance . The platform is available in multiple chassis configurations—the 2RU ASR 1002, 4RU ASR 1004, and 6RU ASR 1006—all sharing common modular components including the Route Processor (RP), Embedded Services Processor (ESP), and SPA Interface Processor (SIP) .

The Embedded Services Processor (ESP) is the heart of the security and forwarding engine. Available in three performance tiers—ESP5, ESP10, and

ESP20 — it provides from 5 to 20 Gbps of system bandwidth. Critically, for firewall and NAT operations, the ESP executes all Layer 4 to Layer 7 zone-based firewall session processing and NAT session setup, including Application Layer Gateways (ALGs) . This offloads the control plane, ensuring that route processing and network management functions remain uninterrupted even under heavy attack or high-volume traffic loads.

## NATIVE FIREWALL AND NAT CAPABILITIES

The integration of NAT and firewall on the Cisco ASR 1000 moves beyond basic packet filtering, offering a stateful, application-aware security perimeter. The platform supports both traditional Access Control Lists (ACLs) and the more granular Zone-Based Firewall (ZFW) policy model . ZFW allows network architects to define security policies based on zones (e.g., inside, outside, DMZ), providing a more intuitive and secure method for controlling traffic flows. Stateful inspection is applied to traffic zones, enabling deep packet inspection up to Layer 7 for protocols such as HTTP, SMTP, FTP, and VoIP signaling (SIP, H.323) .

For NAT, the platform provides robust Carrier-Grade NAT (CGN) capabilities, including NAT44 and Port Address Translation (PAT) . The Cisco QuantumFlow Processor handles the complete session setup, capable of sustaining millions of

concurrent translations. The platform supports a wide range of NAT application awareness, including Skinny Client Control Protocol (SCCP), DNS, and RTSP . High-speed NAT and firewall translation logging is facilitated through NetFlow Event Logging (NEL), which uses NetFlow v9 templates to export session creation and teardown records to external collectors, enabling comprehensive auditing and capacity planning .

## HIGH AVAILABILITY AND STATEFUL FAILOVER

A critical requirement for the secured edge node is non-stop operation. The Cisco ASR 1000 Series introduces industry-leading high-availability features for integrated services through its Box-to-Box High Availability (B2BHA) and stateful failover mechanisms .

The platform supports Stateful Switchover (SSO) and Nonstop Forwarding (NSF) for routing. For security services, the NAT and Zone-Based Firewall state information is fully synchronized . Within a single chassis, every completed NAT or firewall session is replicated from the active ESP to the standby ESP, ensuring that a data-plane hardware failure does not interrupt existing sessions .

For inter-chassis redundancy, the Box-to-Box HA feature enables an active-standby pair of routers to maintain a synchronized translation database .

This ensures that in the event of a full router failure, the standby unit can instantaneously take over as the active translator without any loss of application traffic flows . This stateful failover capability extends to the Zone-Based Firewall, making the ASR 1000 the first Cisco routing platform to offer this level of application resiliency traditionally found only in dedicated security appliances .

TECHNICAL SPECIFICATIONS

| **Feature** | **ESP5** | **ESP10** | **ESP20** |
|---|---|---|---|
| Firewall Throughput | 5 Gbps | 10 Gbps | 20 Gbps |
| Concurrent NAT Sessions | High Scale | 500,000 | 500,000+ |
| NAT Sessions Per Second | High Scale | 20,000 | 20,000 |
| IPSec Tunnels | 4,000+ | 4,000+ | 4,000+ |
| NetFlow Records | 500,000 | 1,000,000 | 2,000,000 |

PROTOCOL INTEROPERABILITY AND SCALABILITY

The Cisco ASR 1000 demonstrates extensive protocol interoperability, crucial for complex edge deployments. It supports VRF-Aware Software Infrastructure (VASI) NAT, which enables inter-VRF NAT configurations on Cisco IOS XE, a common requirement for multi-tenant service provider environments . This allows network operators to configure NAT services on traffic flowing between different VRF instances using paired VASI interfaces .

Scalability is a key differentiator, as detailed in the performance matrix. The platform supports up to 8 million NAT translations in certain profiles, highlighting its readiness for large-scale deployments . The ESP20, for example, supports up to 500,000 concurrent NAT sessions and can establish up to 20,000 sessions per second . This scalability is underpinned by the platform's ability to store the full Internet routing table and support advanced routing protocols such as OSPF, BGP, and EIGRP without impacting forwarding performance .

REGULATORY COMPLIANCE AND INFRASTRUCTURE SECURITY

This section serves as the compliance register for the platform, verifying adherence to stringent industry standards. The ASR 1000 is designed with a security-first architecture, featuring total isolation of control and data planes to mitigate Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks . Control-plane protection mechanisms ensure that only legitimate management and routing traffic is processed by the route processor, safeguarding the network's core infrastructure.

Compliance and operational assurance are further reinforced through:

- In-Service Software Upgrade (ISSU): Enables nonstop router operation during software upgrades, a critical requirement for carrier-grade compliance .

- Modular Software Design: Minimizes the impact of software failures and lowers operational expenses (OpEx) .

- Secure Management Access: Supports SNMPv3, SSH, and encrypted syslog for secure remote management .

- Environmental and Safety Standards: The platform is certified to meet rigorous telecommunications and safety standards, making it suitable for both enterprise data centers and carrier central offices.

By integrating these security and resilience features into a single routing platform, the Cisco ASR 1000 dramatically reduces the total cost of ownership (TCO) while ensuring that the secured edge node remains a protected, compliant, and highly available gateway to the network.