

Secured Edge Node Technical Compliance Register: ZTE ZSR V2 Series Enterprise Router IPSec VPN Encryption Throughput

SECURITY POSITIONING

The ZXR10 ZSR V2 Series represents ZTE's next-generation intelligent integrated multi-service router platform, engineered to consolidate routing, switching, wireless connectivity, security, and VPN gateway functions into a single, cohesive hardware asset. Within the context of enterprise perimeter defense and branch interconnect security, the ZSR V2 Series distinguishes itself through the integration of a dedicated multi-performance encryption engine and a hardened IPSec protocol operating system. This architectural decision is predicated on the premise that contemporary enterprise edge nodes can no longer afford the latency and management overhead associated with traversing external, discrete encryption appliances. Instead, the ZSR V2 Series embeds line-rate cryptographic processing directly into the forwarding plane, delivering encryption capabilities that are directly comparable to dedicated IPSec gateway hardware. The platform is positioned to serve as the cryptographic anchor for site-to-site communications between headquarters and branch offices, as well as for remote access scenarios requiring robust data confidentiality, integrity verification, and origin authentication.



LINE-RATE ENCRYPTION CAPABILITIES

The cryptographic throughput of the ZSR V2 Series is not an ancillary feature but a central design tenet. The hardware architecture leverages a multi-core CPU design that separates the control plane from the forwarding plane, ensuring that IPSec encapsulation, encryption, and decryption operations do not starve routing protocol interaction or system management tasks. The dedicated encryption engine is calibrated to sustain high-throughput IPSec VPN tunnels without inducing the throughput penalties typically observed when encryption is bolted onto legacy routing platforms. For the ZXR10 3800-8 and 2800-4 models, the system supports advanced cryptographic algorithms, including both commercial and state cryptography standards, ensuring compliance with diverse regulatory environments. The platform's IPSec implementation encompasses standard authentication methods including

pre-shared keys and X.509 digital certificates, supporting main mode and aggressive mode IKE negotiations to accommodate both static and dynamic branch addressing scenarios. Furthermore, the integration of hardware-based QoS mechanisms, including Hierarchical QoS (H-QoS), allows the ZSR V2 Series to maintain deterministic latency and jitter profiles for encrypted voice and video traffic traversing IPSec tunnels, preventing the cryptographic processing from introducing unacceptable degradation to real-time applications.

PHYSICAL TAMPER-RESISTANCE

Beyond cryptographic algorithm support, the ZSR V2 Series incorporates foundational physical and logical security mechanisms designed to harden the edge node against tampering and unauthorized access. The platform supports stateful firewall inspection, control-plane security, and CPU security protection, establishing a defense-in-depth posture that complements the IPSec tunneling layer. The hardware design includes intelligent fan control and thermal monitoring, which, while primarily intended for longevity and acoustic performance, also contribute to stable operation under sustained cryptographic loads, reducing the risk of thermal-induced instability that could compromise tunnel availability. For deployment in physically accessible locations, the modular chassis design with hot-swappable fan and power modules ensures that maintenance activities do not require full system

shutdown, preserving the operational integrity of established VPN sessions during hardware servicing. The platform further supports MAC and IP binding, anti-ARP attack mechanisms, and control of TCP session counts, providing Layer 2 and Layer 3 hardening that prevents lateral movement within the encrypted domain and mitigates the risk of session hijacking or resource exhaustion attacks targeting the cryptographic subsystem.

DETAILED PARAMETERS

The ZSR V2 Series encompasses multiple chassis configurations, each calibrated for distinct throughput and deployment scales. The flagship ZXR10 3800-8, a 3RU modular chassis, provides the highest forwarding and cryptographic capacity, suitable for headquarters aggregation and high-density branch concentration points. The ZXR10 2800-4, a 2RU platform, offers a balanced profile for mid-sized enterprise sites, while the ZXR10 1800-2S serves compact branch locations with fixed and modular interface flexibility. All models in the series integrate the IPSec VPN function natively, with the encryption throughput scaling proportionally with the multi-core forwarding engine capacity. The platform supports a comprehensive suite of VPN technologies beyond IPSec, including GRE, L2TP, DMVPN, and MPLS VPN, enabling hierarchical and hybrid tunnel topologies that can be tailored to the specific security and connectivity requirements of each node within the enterprise

WAN.

TECHNICAL SPECIFICATIONS

The following table consolidates the key hardware and cryptographic parameters relevant to IPSec VPN deployment across the ZSR V2 Series.

Parameter	Specification
Form Factor	1RU (1800-2S) / 2RU (2800-4) / 3RU (3800-8) Modular Chassis
Forwarding Performance	1 Mpps to 5 Mpps (varies by model and service engine)
IPSec VPN Support	Site-to-Site, Remote Access (L2TP over IPSec), GRE over IPSec, DMVPN, GET VPN
Encryption Algorithms	Commercial cryptographic algorithms; State Cryptography Administration (SCA) commercial codes supported
Authentication Methods	Pre-Shared Key (PSK); X.509 Digital Certificates
IKE Modes	Main Mode (static peers); Aggressive Mode (dynamic peers)

Power Supply	1+1 Redundant AC/DC (2800-4, 3800-8); AC or DC single (1800-2S)
Redundancy Features	Power module redundancy, hot-swappable fan and boards, VRRP, BFD, link aggregation FRR
Operating Temperature	-5°C to 45°C (standard); -40°C to 70°C (storage)
IPv6 Certification	IPv6 Ready Logo Phase-2 Gold Certified

REGULATORY CERTIFICATIONS

The ZXR10 ZSR V2 Series has undergone rigorous third-party validation to substantiate its compliance with international standards. Notably, the platform has achieved IPv6 Ready Logo Phase-2 Gold Certification from the IPv6 Forum, confirming that its dual-stack and transition implementations—including IPsec over IPv6 — conform to IETF RFC specifications for consistency and interoperability. The hardware adheres to RoHS manufacturing directives, utilizing lead-free materials and compliant processes. For markets with specific cryptographic accreditation requirements, the ZSR V2 Series supports State Cryptography Administration commercial algorithms, enabling lawful

deployment in jurisdictions that mandate domestic cryptographic standards for encrypted communications. The platform's power supply modules and thermal design are engineered to meet international safety and electromagnetic compatibility standards, with AC and DC variants available to suit diverse facility infrastructures.

PERIMETER DEPLOYMENT

In a representative enterprise perimeter topology, the ZXR10 3800-8 or 6802 router is positioned at the headquarters Internet egress, terminating IPSec tunnels from distributed branch nodes. Branch locations deploy ZXR10 1800-2S or 2800-4 platforms, establishing site-to-site IPSec VPNs with pre-shared key authentication and main mode IKE negotiation for sites with static public addresses. For branches with dynamic addressing (DSL or DHCP-based WAN links), the headquarters gateway is configured for aggressive mode negotiation, utilizing hostname-based peer identification to maintain tunnel establishment despite address volatility. Remote access users may connect via L2TP over IPSec, with the headquarters ZSR V2 acting as the L2TP Network Server (LNS) while IPSec provides the outer cryptographic envelope for the tunneled PPP sessions. For high-availability deployments, dual gateway configurations with VRRP or dynamic routing failover ensure that IPSec tunnel state is preserved or rapidly re-established in the event of a primary node failure, maintaining the continuity

of encrypted application traffic across the WAN.

