



Faster, high-performance and secure connectivity with comprehensive SASE solution



INTEGRATION HIGHLIGHTS

- ✓ Reduce operational complexity with fully automated workflows
- ✓ Faster and resilient connectivity with high-availability
- ✓ Improved security enforcement for applications on local internet breakout
- ✓ Intelligent, application-aware and self-healing networks

The Market Challenge

Organizations integrating Zscaler Internet Access (ZIA) with their SD-WAN solution struggle with slow, error-prone onboarding because traditional branch to ZIA connectivity requires manual tunnel setup, complex routing configurations, and application steering policy configuration. Misconfigurations can create poor user experiences, security gaps, and vulnerabilities. This leads to deployment delays, outages, and uneven security coverage. As environments scale to hundreds or thousands of branches, these manual processes become operational bottlenecks, increase risk, and make it difficult to deliver reliable connectivity, better security and a consistent user experience.

The Solution

Together, Zscaler and Versa automates a dual-vendor SASE deployment via automated API-based workflows, eliminating per-site, manual setup. Using reusable templates, it provisions connectivity from each CPE to primary and secondary Zscaler Point of Presence (PoP). This integration also ensures high availability SD-WAN appliances at branch connect with Zscaler. Additionally, these connections are established to Zscaler PoPs based on closest proximity and latency for better WAN resiliency. IPsec-based connectivity is supported from Versa Secure SD-WAN branches to Zscaler delivering easy onboarding at-scale across thousands of branches in minutes

Together, Zscaler and Versa deliver an automated, scalable SASE architecture that simplifies operations, improves application performance, and enforces consistent security across distributed environments.

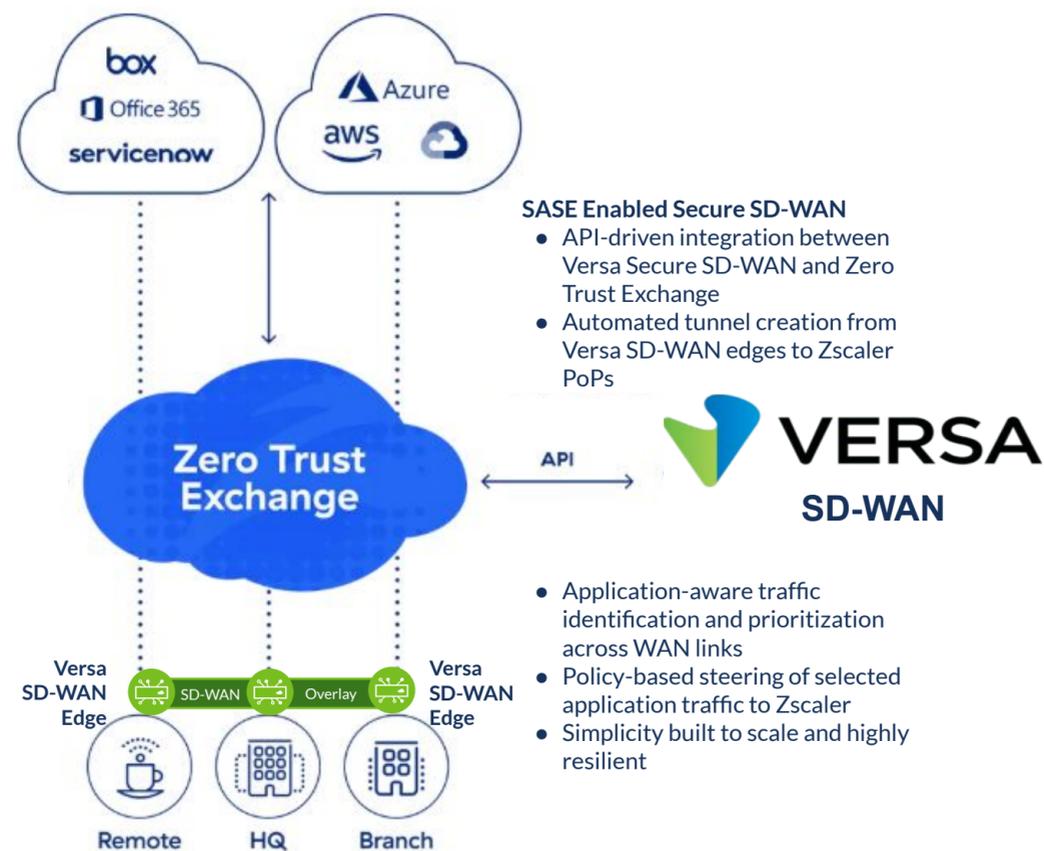
Solution Components Deep Dive

The integration simplifies onboarding of Zscaler SSE across Versa Secure SD-WAN sites by automating connectivity via API-driven, automated workflows

Versa builds secure tunnels from each WAN link to primary and secondary Zscaler PoPs. The secure tunnels from each WAN links are configurable in two modes: active-active, where both tunnels are used simultaneously, allowing load balancing or shared traffic across them, or active-standby, where one tunnel is active for traffic while the other is on standby, ready to take over in case the active one fails. Zscaler PoPs are chosen per site based on proximity, geo location and latency.

Once onboarded, Versa Secure SD-WAN delivers per-app local breakout and SLA-based path selection. Additionally, this eliminates application brownout using fast failover.

The integrated solution protects application traffic on direct internet connections/local internet breakout with Zscaler's comprehensive security capabilities like URL filtering, threat prevention, DLP, SWG, CASB.



The integrated solution ensures better connectivity, user experience, and resiliency through application-aware routing, WAN optimization, and self-healing capabilities like automated failover, packet correction, and AI-driven analytics.

KEY USE CASE

Accelerating SASE with Automated SD-WAN Integration

Organizations need a scalable way to onboard branch offices and data centers into a SASE architecture without manual configuration or operational overhead. The Zscaler and Versa integration uses API-driven automation to onboard Versa Secure SD-WAN branches, offices, and data centers into Zscaler Internet Access, including secure tunnel creation and sub-location support. Together, they enable Geo-Location based PoP selection, granular per-application traffic forwarding, high availability across WAN links, and consistent cloud-delivered security—accelerating time-to-value while improving user experience and security at scale.

The Versa and Zscaler integration transforms weeks of manual tunnel configuration into a simple, streamlined, and automated provisioning process. These automated workflows create a resilient architecture for integrating Zscaler with Versa Secure SD-WAN deployments.

Rahul Vaidya

Senior Director, Product Management at Versa Networks

Zscaler + Versa Benefits

ACTION	DESCRIPTION
Reduce operational complexity	Deploy IPSEC tunnels from Versa Secure SD-WAN to Zscaler PoPs across multiple links. With API-based automated workflows that bring up tunnels in minutes, IT teams can establish connectivity to Zscaler PoPs at scale across thousands of sites
Improve resiliency	Leverage all WAN links in active-active or active-standby fashion to load balance or failover for better bandwidth availability. Improve uptime and WAN resiliency by seamlessly failing over to redundant SD-WAN appliance in seconds
Deliver better security	Implement advanced security capabilities such as CASB, DLP, SWG, Threat Prevention, and URL filtering without the need for additional hardware through Zscaler's cloud-delivered security services.
Enable self-healing networks	Build a high-performance, resilient, and self-healing network by combining application-aware routing and AI-driven analytics with Versa Secure SD-WAN.
Enable faster connectivity	Eliminate the need to backhaul application traffic to datacenters and allows IT leaders to leverage broadband or direct internet links to access applications including SaaS and Cloud through secure tunnels between Versa Secure SD-WAN and ZIA.

Conclusion

With Zscaler + Versa, customers can now deliver automated SSE onboarding, latency-aware PoP selection, granular per-app forwarding, and resilient high availability across WAN links and SD-WAN appliances at scale. Moving to SASE solution is now accelerated with this integration that delivers time-to-value while improving user experience and security.

Learn more at www.zscaler.com/partners/technology



About Zscaler: Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest in line cloud security platform. Learn more at zscaler.com or follow us on X (Twitter) @zscaler.

©2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, and ZPA™ are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.