What was announced?

Zscaler launched a **Zero Trust SD-WAN solution,** which claims to break away from the site-site VPN connectivity to securely connect branches, factories, and data centers.

- Zscaler launched 3 hardware and 1 VM form factor for small, medium, and large branch use cases.
- This launch is likely in response to the fact that Zscaler was not included in the Gartner Single Vendor SASE quadrant as it does not have a native SD-WAN solution to call it a Single Vendor SASE solution.
- Zscaler SD-WAN solution is technically just a traffic forwarding device that forwards traffic to Zscaler cloud for further inspection relying on customers' ISP connectivity.
- Today, all of their deployed base currently uses third-party SD-WAN. This will likely impact their relationship with existing SD-WAN vendors.

Summary

- Zscaler's Zero Trust SD-WAN solution is nothing more than its "branch connector" in hardware form factor and renamed as "Z-Connector." This was introduced last year during Zenith Live, and it is officially making it public now. Zero Trust SD-WAN Datasheet.
- The Branch Connector (now Z-connector) was launched one year ago, but in a VM form factor. Due to network/hardware limitations in a VM form factor, Zscaler faced a lot of scalability and deployment complications. This is likely one of the reasons why it finally went the hardware route.
- The Z-Connector is basically an internet gateway that forwards traffic to Zscaler ZIA or ZPA Cloud, depending on what the destination is.
- The main use cases are:
    - Site-site VPN replacement
    - IoT Discovery/Access
    - Accelerate M&A integrations
- The hardware makes a DTLS connection to ZIA for internet traffic and follows the ZTNA model (broker + Connector) to connect to the ZPA cloud for private applications. The branch connector is doing the same thing as its Zscaler Client, which is on an end-user device, but now it acts as an internet gateway.
- Z-Connector also acts as a DNS gateway.
- Since Zscaler is not using MPLS/IPsec connections and leveraging DTLS, it claims this eliminates the need for MPLS / SD-WAN / IPsec tunnels.
- This hardware supports some SD-WAN-like features, including:
    - Plug-n-play (zero-touch provisioning)
    - Multiple WAN links
    - Performance monitoring
    - BW control
- Lacks advanced SD-WAN capabilities (detailed in the key differentiators section below).
- The hardware supports firewall-like functionality for east-west traffic (granular LAN to LAN access control and L3 Access Control List). But TLS inspection and other policies apply on the cloud just like they do now for traffic from remote users or locations.
- Zscaler partnered with Lanner Whitenbox Solutions for the hardware. It was not built in-house.
- Zscaler continues to support 3rd party integration with other SD-WAN tools for its ZIA (SSE) solution.
- No information on pricing, and is not available for Federal Cloud.
- Lacks IPV6 support.
- This is an entirely new/different console to set up Branch/Cloud connectors, and it is not natively integrated into its ZIA or ZPA admin console. Zscaler provided a glimpse into its UI in a blog post.

Key Differentiators

The following represents the key differentiators Palo Alto Networks still has over Zscaler, even after this announcement.

- Management: Zscaler Z-Connector requires a separate new admin console for management and is not integrated with the existing ZIA or ZPA portal. Customers must learn a new portal, dashboard, logging, etc.
    - **Prisma SASE utilizes a single console for everything, including SASE and SD-WAN.**
- Max Branch Throughput: Zscaler supports 1 Gbps.
    - **Prisma SD-WAN supports: 3 Gbps (mid-large branch HW)**
- Hardware: Zscaler lacks the breadth of interface support.
    - **Prisma SD-WAN integrates 5G/LTE, POE, hardware bypass, and mGig (multi Gig) ports.**
- SD-WAN Functionality: Zscaler lacks advanced SD-WAN capabilities but does support plug-n-play (zero-touch provisioning), multiple WAN links (supports multiple ISP), performance monitoring, dynamic app-aware path selection (limited details on how this works), and BW control.
    - **Prisma SD-WAN supports advanced SD-WAN features:**
        - APP SLA-based Traffic Steering
        - APP-based prioritization QOS/QOE
        - App detection and Awareness
        - Middle mile optimization
        - Error correction (FEC or packet duplication)
- SD-WAN Integrations: Zscaler SD-WAN lacks comprehensive 3rd party integrations.
    - **Prisma SD-WAN integrates with other SSE vendors and supports our SD-WAN support automated 3rd party interaction via the Cloud Blade (e.g., Zoom, QSS, ServiceNow). It also supports IaaS Cloud Blade integration with Azure vWAN, gcpNCC, and AWS Cloud WAN.**
- Security: Zscaler hardware supports LAN-to-LAN access control and has an L3 Access Control List.
    - **Palo Alto Networks provides a stateful firewall on SD-WAN or NGFW via NGFW hardware.**
- TLS inspection: Zscaler SD-WAN forwards traffic to ZIA (internet/SaaS) and ZPA (private apps). Since it leverages the same ZPA flow, it does not support DLP/Threat inspection for private app traffic.
    - **Prisma SASE applies DLP/TP for Private Access.**
- **AIOPS-ADEM:** Zscaler SD-WAN currently does not integrate with ZDX (Zscaler Digital Experience), so it lacks granular visibility on application experience, segmented insights, or hop-by-hop insights for SD-WAN branches.
    - **Palo Alto Networks' AIOPS-ADEM solution provides App experience score, segmented insights, hop-by-hop insights, automatic root cause analysis, and remediation playbooks for infrastructure incidents/alerts.**

Feature Comparison Matrix

Zscaler Zero Trust SD-WAN GAP Analysis

SD-WAN Capabilities	Prisma SD-WAN	Zscaler Zero Trust SD-WAN
Platforms (with Encrypted Throughput)	ION 1200 - 250Mbps	ZT 400 - 200Mbps
	ION 2000 - 250Mbps	ZT 600 - 500Mbps
	ION 3200 - 500Mbps	ZT 800 - 1Gbps
	ION 5200 - 1Gbps	Virtual - Multi Gig
	ION 9200 - 3Gbps	
	ION 3102V - 100Mbps	
	ION 3104V - 200Mbps	
	ION 3108V - 350Mbps	
	ION 7108V - 3Gbps	
Onboarding	Zero Touch	Zero Touch
WAN Connectivity	Multiple ISP	2 ISPs
	MPLS	
	5G	
	LTE	
Overlay Connectivity	Standard VPN to Prisma Access	DTLS to Zero Trust Exchange
	Secure Fabric to DC and Branch	
	Standard VPN to 3rd Party vendor (*Including Zscaler)*	
WAN Routing	Static Routing with next hop reachability	Static Routing
	BGP	
LAN Routing	Static Routing with next hop reachability	Static Routing
	BGP	
	VRF	
	OSPF (In Progress)	
East West traffic	ZBFW (App based)	L3/L4 Policies
Branch Capabilities	VLAN	VLAN
	DHCP Server	DHCP Server

	DNS	DNS
	IoT Discovery	IoT Discovery
	Sub-Interfaces	Sub-Interfaces
	ISP monitoring	ISP Monitoring
	App defined policies	App Aware Path Selection
	App SLA assurance with FEC, Packet Duplication	
	App acceleration	
	SNMP	
	Syslog export	
	NTP	
	IPFIX	
	Virtual Interfaces	
	Multicast	
	User-ID	
	PoE	
	Switching with MST Spanning Tree	
	Port Authentication (802.1x)	
High Availability	Supported	Supported
	WAN redundancy using Fail to Wire	
Policy Path selection Options	Direct Internet	Direct Internet
	Secure Fabric to DC or Branch	ZIA/ZPA
	Standard VPN to Prisma Access	
	Standard VPN to 3rd Party vendors (Including Zscaler)	
	Direct MPLS	
Config, Visibility and Logging	Centrally managed	Fragmented ZIA, ZPA , Connector consoles and policies
	Incident Correlations	
	Predictive Insights for carriers	
	Site Health Score - ADEM powered	
	Application Health Score - ADEM powered	
	Audit Logs	