



Zero Trust SD-WAN im Überblick

Vorteile:

Weniger Komplexität

Beseitigen Sie das Gewirr aus Site-to-Site-VPNs und Overlay-Routing.

Bessere User Experience

Vermeiden Sie unnötigen Datenverkehr und verbessern Sie die Leistung von SaaS- und Cloud-Apps ohne Kompromisse in Sachen Sicherheit. Sicherheits- und Bandbreitenrichtlinien werden auf über 150 Zscaler-Rechenzentren weltweit angewendet.

Mehr Sicherheit

Verkleinern Sie Ihre Angriffsfläche und senken Sie das Risiko einer weiteren Ausbreitung etwaiger Angriffe, wie sie bei herkömmlichem SD-WAN häufig vorkommt. Vereinfachen Sie die User-zu-App- und App-zu-App-Segmentierung mit der cloudnativen Zero Trust Exchange.

Mit Zero Trust SD-WAN verbinden Sie Niederlassungen, Fabriken und Rechenzentren sicher und ohne komplexe VPNs. So gewährleisten Sie Zero-Trust für User, IoT-/OT-Geräte und Anwendungen gemäß Ihren Richtlinien. Mit der Kombination aus dem Branchenführer Zscaler Zero Trust Exchange und einer nahtlosen Konnektivität für Standorte, Clouds und User können Unternehmen ihr SASE-Framework (Secure Access Service Edge) auch auf ihre Zweigstellen ausweiten.

Warum kein herkömmliches SD-WAN?

Herkömmliches SD-WAN vergrößert die Angriffsfläche und begünstigt die Ausbreitung von Bedrohungen, die wiederum Ihre Angreifbarkeit erhöht. Zudem verbindet herkömmliches SD-WAN die einzelnen Standorte per Site-to-Site-VPN; das erhöht allerdings die Netzwerkkomplexität, da die Unternehmen so weiterhin auf Routingtabellen angewiesen sind. Die gerouteten Overlays werden als vertrauenswürdig eingestuft, sodass Unternehmenseinheiten, die sich mit dem Netzwerk verbinden, uneingeschränkter Zugriff auf kritische Ressourcen erhalten. Inzwischen haben viele Bedrohungen ihren Ursprung in kompromittierten Usern, IoT-/OT-Geräten oder den Servern von Zweigstellen.

Zero Trust SD-WAN

- Zscaler Zero Trust SD-WAN bietet Zweigstellen und Fabriken schnellen und zuverlässigen Zugriff auf das Internet sowie SaaS- und private Anwendungen mit einer Direct-to-Cloud-Architektur, die ein hohes Maß an Sicherheit gewährleistet und zudem noch einfach zu bedienen ist.
- Durch die Verbindung von Usern und IoT-/OT-Geräten mit Anwendungen über die Zero Trust Exchange wird nicht zuletzt auch die Ausbreitung von Bedrohungen verhindert.
- Vereinfachte Zweigstellenkommunikation ohne komplexes Routing, VPNs und Firewalls; stattdessen eine flexible Weiterleitung und unkomplizierte Richtlinienverwaltung mit dem bewährten ZIA- und ZPA-Framework

Anwendungsbereiche

Site-to-Site-VPNs ersetzen

Tauschen Sie das Durcheinander von Site-to-Site-VPNs, die Zweigstellen, Fabriken und Rechenzentren miteinander verbinden, gegen unkompliziertes Plug-and-Play für eine einfache Bedienung und mehr Sicherheit ein.

Sicherer IoT-/OT-Zugriff

IoT-/OT-Ressourcen müssen regelmäßig von Mitarbeitern und Drittanbietern überprüft werden, um ihre Verfügbarkeit zu gewährleisten und Störungen durch Geräte- und Prozessausfälle zu vermeiden. Zero Trust SD-WAN vereinfacht den Zugriff auf Ihre IoT-/OT-Ressourcen auch ohne VPNs und exponierte Ports und ermöglicht einen komplett abgeschotteten, clientlosen Remote-Desktop-Zugriff auf interne RDP- und SSH-Zielsysteme für Vertragspartner und Auftragnehmer.

Schnellere M&A-Einbindung

Sparen Sie sich die Zusammenführung von Routing-Domains und die Übertragung überlappender IP-Adressen. Verbinden Sie neue User mit wichtigen Ressourcen wie Active Directory, indem Sie Ihre neuen Standorte einfach um Plug-and-Play-Appliances ergänzen.

Erkennung und Klassifizierung von IoT-Geräten

IT-Teams übersehen gerne ungenehmigte, unbekannte IoT-Geräte, die sich mit dem Filialnetzwerk verbinden. Doch gerade diese erhöhen das Risiko einer Malware-Infektion im gesamten Unternehmen. Zscaler erkennt und klassifiziert Geräte, verschafft der IT damit einen umfassenden Überblick in deren Verhalten und entsprechend die Möglichkeit für geeignetere Richtlinien für die Zugriffskontrolle.

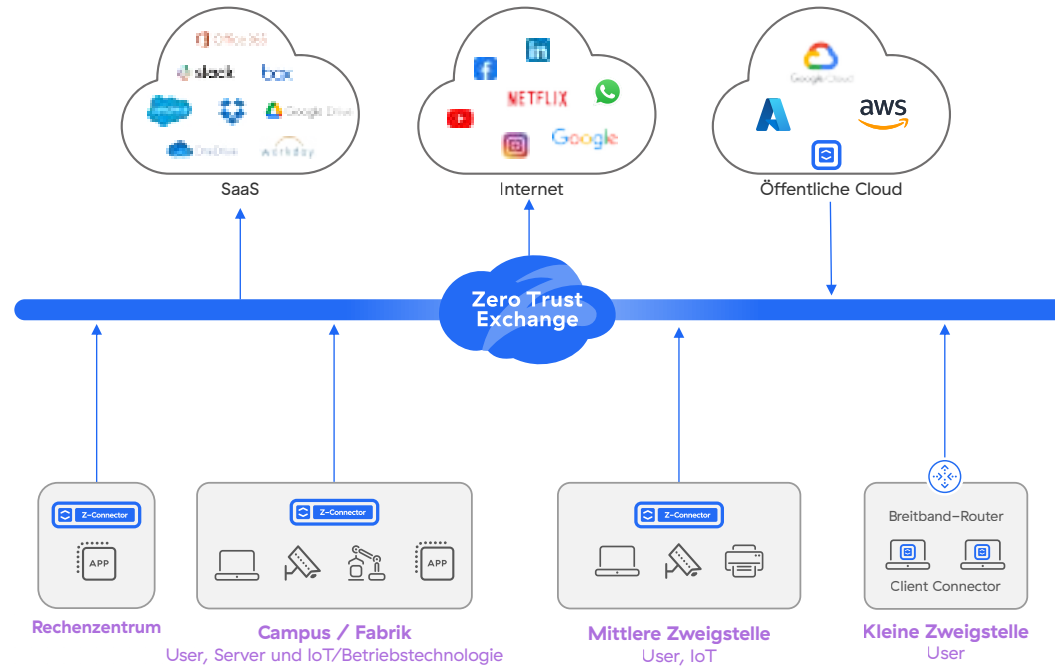






Abb. 1: Zero Trust SD-WAN

Zero Trust SD-WAN ist eine Plug-and-Play-Appliance, die virtuell und analog erhältlich ist.

Zero Trust SD-WAN: Hardware- und Software

Funktion	ZT 400	ZT 600	ZT 800	ZT VM
				
Typ	Kleine und mittelgroße Niederlassungen	Kleine und mittelgroße Niederlassung	Mittelgroße und große Niederlassung	Zweigstelle und Rechenzentrum
Übertragungsrate/ Hypervisor	200 Mbit/s	500 Mbit/s	1 Gbit/s	KVM, ESXi
Physikalische Anschlüsse	4	6	8	N/A
Zero-Touch-Bereitstellung	✓	✓	✓	✓
Detaillierte Weiterleitungsrichtlinien für Internet, private Anwendungen und WAN-Direktverkehr	✓	✓	✓	✓
URL-Filterung, Dateitypkontrolle und Cloud-Firewall-Richtlinien für internetgebundenen Datenverkehr	✓	✓	✓	✓
ZPA-Richtlinien mit Zero Trust für IoT-Geräte und Server	✓	✓	✓	✓
Zentrale Übersicht und Protokollierung	✓	✓	✓	✓

 | Experience your world, secured.™

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen finden Sie auf [zscaler.de](https://www.zscaler.de) oder auf Twitter unter [@zscaler](https://twitter.com/zscaler).

© 2024 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ und weitere unter www.zscaler.com/terms aufgeführte Marken sind entweder (i) eingetragene Marken bzw. Dienstleistungsmarken oder (ii) Marken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.