LÖSUNGSPROFIL

Zscaler™ und SD-WAN

Absicherung der reinen Internet-Niederlassung

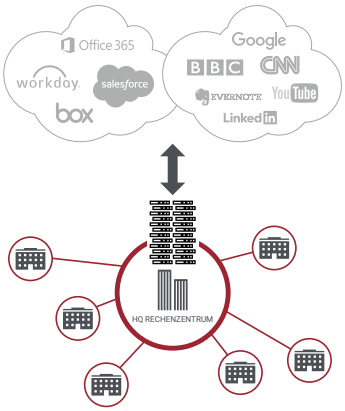
Zscaler und SD-WAN erleichtern den Wechsel von einem Hub-and-Spoke Netzwerk zu einer reinen Internetarchitektur in der Niederlassung, indem sie sichere lokale Internet-Breakouts ermöglichen.

Cloud-Apps sprengen traditionelle Architekturen

Für Organisationen, die Cloud-Anwendungen wie Office 365 nutzen, ist der alte Ansatz für das Routing von Traffic-Backhauling über MPLS zu einem zentralen Internet-Gateway per Hub-and-Spoke Architektur unzureichend. Um eine schnellere User Experience bieten zu können sowie Cloud-Anwendungen und -Services zu unterstützen, muss Internet-Traffic lokal geroutet werden.

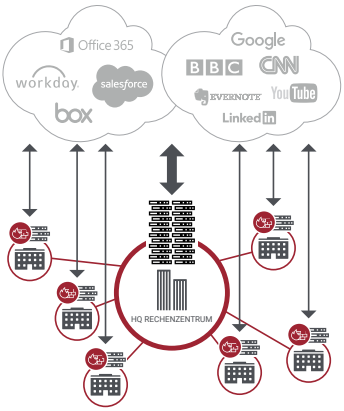
Um jedoch dasselbe Sicherheitsniveau wie am Internet-Gateway zu erreichen, müssen Organisationen den Stack von Sicherheits-Appliances in jeder Niederlassung replizieren, was in puncto Kauf, Einsatz und Verwaltung ein kostspieliges Unterfangen ist. Traditionelle Firewalls und UTMs sind eine unzulängliche Alternative, da sie weder SSL-verschlüsselten Traffic noch atypische Ports und Protokolle bewältigen können. Aufgrund dieser Herausforderungen entscheiden sich Unternehmen vermehrt für SD-WAN, um lokale Internet-Breakouts zu etablieren und eine schnellere User Experience zu gewährleisten.

Traditionelles Hub-and-Spoke



- Backhauling über MPLS ist teuer
- Führt zu unnötiger Latenz
- Beeinträchtigt die User Experience

Ausweitung von UTM/Firewall-Appliances



- Kostspielige Bereitstellung
- Hat Aufstockung von Appliances zur Folge
- Ist unmöglich zu verwalten
- Beeinträchtigt die Sicherheit von Niederlassungen
- Leistungsabbau bei SSL-Überprüfung und zusätzlichen Sicherheitsdiensten

SD-WAN und lokale Internet-Breakouts

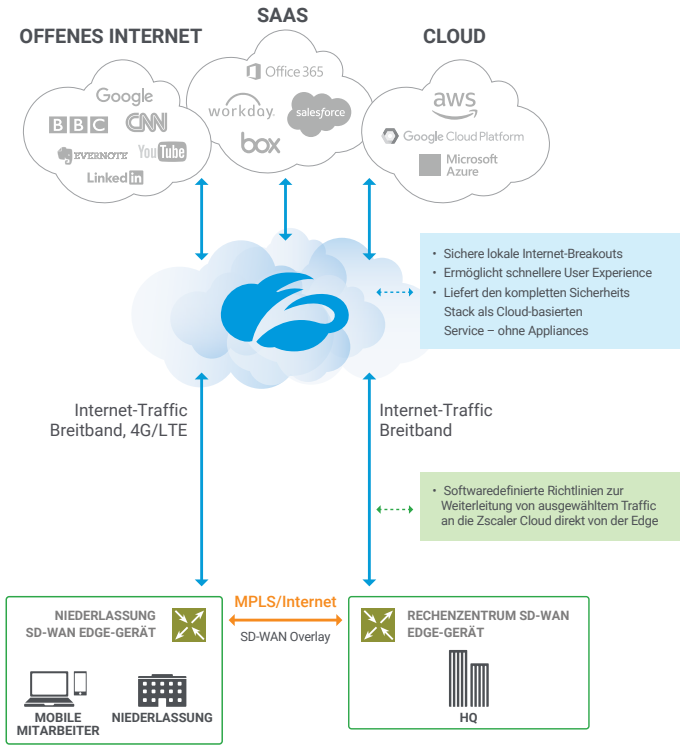
Softwaredefiniertes Wide Area Networking (SD-WAN) vereinfacht das Traffic-Routing in der Niederlassung und erleichtert die Einrichtung lokaler Internet-Breakouts. Anhand softwaredefinierter Richtlinien wird der beste Pfad ermittelt, um Traffic über Verbindungen von der Niederlassung zum Internet, zu Cloud-Anwendungen und zum Rechenzentrum zu routen. Durch die Festlegung von Richtlinien für alle Niederlassungen — über eine einzige Schnittstelle in der Cloud — können Organisationen neue Anwendungen und Services problemlos einsetzen und Richtlinien über viele Standorte hinweg verwalten. Dies lokalen Breakouts müssen allerdings abgesichert werden.

Zscaler: Die Cloud-Methode zum Sichern von SD-WAN

Zscaler sichert ausgehenden Internet-Traffic und bietet eine schnelle User Experience— ohne Backhauling und ohne Duplizierung sämtlicher Sicherheits-Appliances an jedem Standort.

Da die Cloud-Sicherheitsplattform von Zscaler den gesamten Security-Stack als Cloud-Service zur Verfügung stellt, gibt es keine Abstriche bei der Sicherheit. Und bei Zscaler sind Richtlinien nicht an einen physischen Standort gebunden; stattdessen folgen sie den Usern, um ihnen an jedem beliebigen Verbindungsort identischen Schutz zu gewährleisten.

Leiten Sie Internet-Traffic einfach an Zscaler weiter und beginnen Sie sofort mit der Untersuchung des gesamten Traffic — alle Ports und Protokolle, einschließlich SSL. Sie können Zugangs- und Sicherheitsrichtlinien für alle Standorte von einer einzigen Konsole aus festlegen und durchsetzen. Mit Zscaler lassen sich Cloud-Services flexibel skalieren, sodass Sie neue Services, wie Bandbreitenkontrolle, mit ein paar Clicks einsetzen können — ohne Leistungsabbau und ohne kostspielige Aufrüstung von Appliances.



SSL-Überprüfung mit SLA-gestützter Leistung

SL ist inzwischen das standardmäßige Kommunikationsprotokoll, und viele Bedrohungen wie Ransomware versuchen, sich innerhalb von SSL zu verbergen—und nutzen manchmal sogar andere Ports—Deshalb ist die Untersuchung des gesamten Traffic unerlässlich. SSL-Überprüfung bedeutet allerdings für die meisten Sicherheits-Appliances eine erhebliche Herausforderung; Entschlüsselung, Untersuchung und Neuverschlüsselung des Traffic dezimiert bekanntermaßen die Leistung der Firewall.[2] Die Zscaler Cloud-Firewall, ein Teil der Service-Plattform von Zscaler, untersucht den gesamten Traffic — alle Ports und Protokolle einschließlich SSL, fast ohne Latenz.

[1] *Transparenzreport – Google, https://www.google.com/transparencyreport/https/?hl=en*
[2] *Pirc, John W., „SSL Performance Problems: Significant SSL Performance Loss Leaves Much Room for Improvement." NSS Labs (https://www.nsslabs.com/linkservid/13C7BD87-5056-9046-93FB736663C0B07A/)*

Zscaler und SD-WAN

REDUZIERUNG VON KOSTEN UND KOMPLEXITÄT

Zscaler und SD-WAN ermöglichen sichere lokale Internet-Breakouts ohne die Kosten und die Komplexität von herkömmlichen Netzwerk- und Sicherheits-Appliances

SD-WAN

- Vereinfacht das Verbinden von Niederlassungen mit dem Internet mittels softwaredefinierter Richtlinien und macht das bei herkömmlichen Appliances notwendige Erstellen komplexer Zugangskontrolllisten überflüssig
- Verwendet mehrere Verbindungstypen in der Niederlassung (Breitband, VPN über Breitband, LTE und MPLS), um eine nahtlose Migration von Hub-and-Spoke Architektur zu erlauben

ZSCALER

- Sichert lokale Internet-Breakouts ab, indem der gesamte Security-Stack als Cloud-Service bereitgestellt wird, sodass in der Niederlassung keine eigenen Firewalls und UTMs mehr benötigt werden
- Ermöglicht sichere lokale Internet-Breakouts ohne Einsatz oder Verwaltung von Appliances
- Senkt die Kosten für MPLS-Backhauling

VEREINFACHTER IT-BETRIEB

Mit Zscaler und SD-WAN wird der Betrieb in den Niederlassungen vereinfacht, weil Sicherheit als Cloud-Service bereitgestellt wird und softwaredefinierte Richtlinien für das Routing von Traffic zum Einsatz kommen

SD-WAN

- Verwendet softwaredefinierte Richtlinien, die mittels einer einzigen Cloud-Konsole festgelegt und verwaltet werden, um zu bestimmen, wie Traffic weitergeleitet wird.

ZSCALER

- Macht Kauf, Einsatz und Verwaltung von Sicherheits-Appliances in all Ihren Niederlassungsstandorten überflüssig
- Ermöglicht die zentrale Definition von Sicherheits- und Zugangsrichtlinien von einer einzigen Konsole aus
- Setzt Richtlinienänderungen sofort an allen Standorten durch
- Erlaubt das Deployment von neuen Sicherheitsdiensten an allen Standorten innerhalb weniger Minuten mit ein paar Klicks
- Leitet Internet-Traffic lokal weiter, um eine schnelle User Experience zu gewährleisten
- Bietet Sicherheits- und Zugangskontrollen für ausgehenden Internet-Traffic an allen Ports, nicht nur 80 und 443, um Advanced Threats zu verhindern

SICHER UND SKALIERBAR

Zscaler stellt den gesamten Security-Stack als Cloud-Service zur Verfügung, damit User an jedem Verbindungsort gleich geschützt bleiben — im Café, dem Firmenhauptsitz oder der Niederlassung

ZSCALER

- Bietet das gesamte Spektrum an Sicherheits- und Zugangskontrollen als zweckbestimmten, Cloud-basierten Service - keine Abstriche bei der Sicherheit
- Führt komplette inline Inhaltsuntersuchung sowie Zugangskontrollen für alle Ports und Protokolle mit vollständiger Protokollierung durch
- Integrierte Überprüfung von SSL-Traffic
- Lässt Sich flexibel skalieren, um rasches Deployment neuer Funktionen (wie Bandbreitenkontrolle oder Data Loss Prevention) ohne Leistungsbeeinträchtigung oder Aktualisierung von Appliances zu ermöglichen
- Rückt den gesamten Security-Stack näher zum User, um identischen Schutz für alle User an jedem Verbindungsort zu gewährleisten

zscaler™

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com