WHITEPAPER

Über SD-WAN hinaus:

Zero-Trust-Sicherheit und das Internet als Unternehmens-WAN

Warum SD-WAN, sicherer Zugriff und Schutz vor Bedrohungen eine Einheit bilden

Akamai

Die Zukunft des Wide Area Network in Unternehmen

Wide Area Networks (WANs) gibt es seit den 1960er Jahren, also den Anfängen der Kommunikation zwischen verschiedenen Computern. Aufgrund neu aufkommender Technologien und steigender Anforderungen an Traffic werden sie fortlaufend weiterentwickelt und verbessert. Für moderne Unternehmen sind WANs die Infrastruktur, die ein standortübergreifendes, einheitliches Netzwerk ermöglicht.

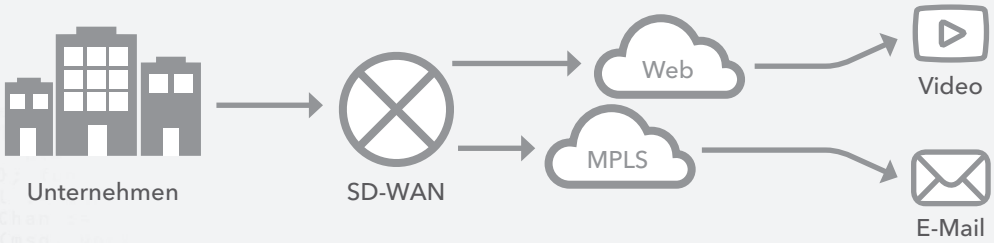
Diese wichtige Unterkonstruktion weist aber auch Einschränkungen auf. WANs bieten häufig eine geringe oder unzureichende Bandbreite und verursachen Probleme mit der Performance bestimmter Anwendungen. Außerdem sind sie nicht gleichbleibend zuverlässig und stellen möglicherweise ein Sicherheitsrisiko für Ihr Unternehmen dar. Darüber hinaus sind WANs häufig auf Mietleitungen eingerichtet oder werden von Serviceanbietern geleast, deren Infrastruktur öffentliche Internet Switching- oder Paket-Switching-Methoden wie Asynchronous Transfer Mode (ATM) und Multiprotocol Label Switching (MPLS) verwendet. Letzteres ist zwar eine etwas kostengünstigere Option, aber trotzdem noch sehr preisintensiv – und eignet sich zudem nicht gut für eine Skalierung.

Unternehmensnetzwerke im Wandel

Als Reaktion auf diese Performance-, Sicherheits- und monetären Herausforderungen setzen Unternehmen softwaredefinierte WANs (SD-WANs) ein, um gleichzeitig Kosten zu senken und flexibler zu sein.

Infolge der Innovation durch SDN (Software Defined Networking) und NFV (Network Function Virtualization), die ursprünglich in Rechenzentren eingesetzt wurden, führten IT-Abteilungen diese Technologie schnell für die Netzwerkverbindungen zwischen Unternehmen ein.

Einfach ausgedrückt, werden Daten und Kontrollebenen des WAN durch ein SD-WAN getrennt. Das SD-WAN überwacht die Performance der verschiedenen WAN-Datenverbindungen – MPLS, ATM und das Internet – und wählt je nach Traffic die am besten geeignete Verbindung basierend auf der aktuellen Verbindungsperformance, den Verbindungskosten und den Anforderungen der Anwendung oder des Services aus.



SD-WAN im Einsatz

Ein SD-WAN leitet E-Mails möglicherweise über MPLS weiter, da Latenz kein großes Problem darstellt und die Kosten pro Bit am niedrigsten sind. Umgekehrt kann das SD-WAN den Videokonferenztraffic über das Internet leiten, um eine optimale Performance und minimale Latenz zu gewährleisten. Damit entstehen jedoch höhere Kosten pro gesendetem Bit.

Könnte das Internet zum neuen Unternehmens-WAN werden?

SD-WANs können mit Sicherheit flexibel, effizient und kostengünstig sein, wenn sie mehrere Transportservices nutzen, einschließlich des öffentlichen Internets. Da es jedoch keine Performancegarantie und kein SLA für solche Transportoptionen gibt, nutzen SD-WANs das Internet ausschließlich für Anwendungen, deren Performance nicht kritisch ist.

Um das Internet effizienter, kostengünstiger und sicherer zu nutzen und mehr WAN-Traffic im Unternehmen bereitzustellen – und zwar so, dass dies mit den aktuellen SD-WAN-Bereitstellungen kombiniert werden kann –, müssen Sie einen Ansatz wählen, bei dem die Einschränkungen des Internets beseitigt werden. Eine Möglichkeit besteht im Einsatz einer Edge-Plattform, über die Geschäftsanwendungen sicher, schnell und zuverlässig über das Internet bereitgestellt werden, ohne diese öffentlich zugänglich zu machen. So können Sie Ihre aktuellen Investitionen in SD-WAN maximieren und gleichzeitig die Kosten weiter senken, wenn Sie mehr Traffic ins Internet verlagern.

Das Routing einer größeren Menge Unternehmenstraffic in das Internet ist angesichts der Entwicklung moderner Unternehmensnetzwerke einfach sinnvoll. Durch die steigende Anzahl von Cloud-Workloads in Verbindung mit unterschiedlichen und mobilen Nutzern und Geräten sind Workflows bereits heute stark vom Internet abhängig. Und dieser Trend breitet sich weiter aus.

Was wäre, wenn Sie dies noch einen Schritt weiterführen und ein sicheres, skalierbares und effizientes Unternehmens-WAN über das Internet einrichten könnten?

In diesem Whitepaper erörtern wir die Prozesse zur Transformation Ihres Netzwerks mit SD-WAN und Zero-Trust-Sicherheit. Gleichzeitig zeigen wir Ihnen, wie Sie Ihr Unternehmen so positionieren, dass es über SD-WAN hinaus ein vollständig internetbasiertes Unternehmensnetzwerk einführen kann.

Mit einer Edge-Plattform können Sie Geschäftsanwendungen sicher, schnell und zuverlässig über das Internet bereitstellen, ohne diese öffentlich zugänglich zu machen.

> *Bis zum Jahresende 2023 werden mehr als 90 % der Initiativen zur Erneuerung der WAN-Edge-Infrastruktur auf vCPE-Plattformen (Virtualized Customer Premises Equipment) oder Software/Appliances (Software Defined WAN, SD-WAN) im Vergleich zu herkömmlichen Routern basieren (aktuell sind es weniger als 40 %).“*
>
> *– Gartner, Magic Quadrant for WAN Edge Infrastructure, Oktober 2018*

Die Vorteile des SD-WAN

SD-WAN bietet in erster Linie einen Verbindungsausgleich, die automatische Gerätekonfiguration und die Einbindung von Sicherheitsservices von Drittanbietern. Der Wert dieser Funktionen, also ein verbessertes Nutzererlebnis, geringere Verbindungskosten und niedrigere Betriebskosten, kann erhebliche Auswirkungen haben. Es gibt genügend Belege für die zunehmende Akzeptanz und Befürwortung dieser Technologie.

Dutzende von Anbietern stellen unterschiedliche SD-WAN-Funktionen bereit. Diese lassen sich aber in drei allgemeinen Kategorien zusammenfassen:

1. *Flexible Verbindungssteuerung*
2. *Verwaltbarkeit*
3. *Service-Einbindung*

Flexible Verbindungssteuerung

Die erste Funktion, die flexible Verbindungssteuerung, ist die wichtigste Grundlage des SD-WAN. Da die Cloud für viele Unternehmen das wichtigste Ziel ist, ist es nicht praktikabel, den Traffic über ein privates Netzwerk an ein Rechenzentrum zurückzuleiten, das im Grunde als zentraler Kontrollpunkt dient. Das SD-WAN löst diese Herausforderung durch eine intelligente Steuerung des Traffics, einschließlich dynamischer Routenauswahl. Darüber hinaus werden beim SD-WAN lokale oder verzweigte Internetverbindungen eingerichtet, die auch als Direct Internet Access (DIA) bezeichnet werden und Traffic in die Cloud statt über ein Rechenzentrum leiten. Daher sind alle älteren Anwendungen, einschließlich Sprach- und Videoanwendungen, für MPLS-Verbindungen bestimmt, während Cloud-Anwendungen und Internettraffic direkt ins Internet geleitet werden.

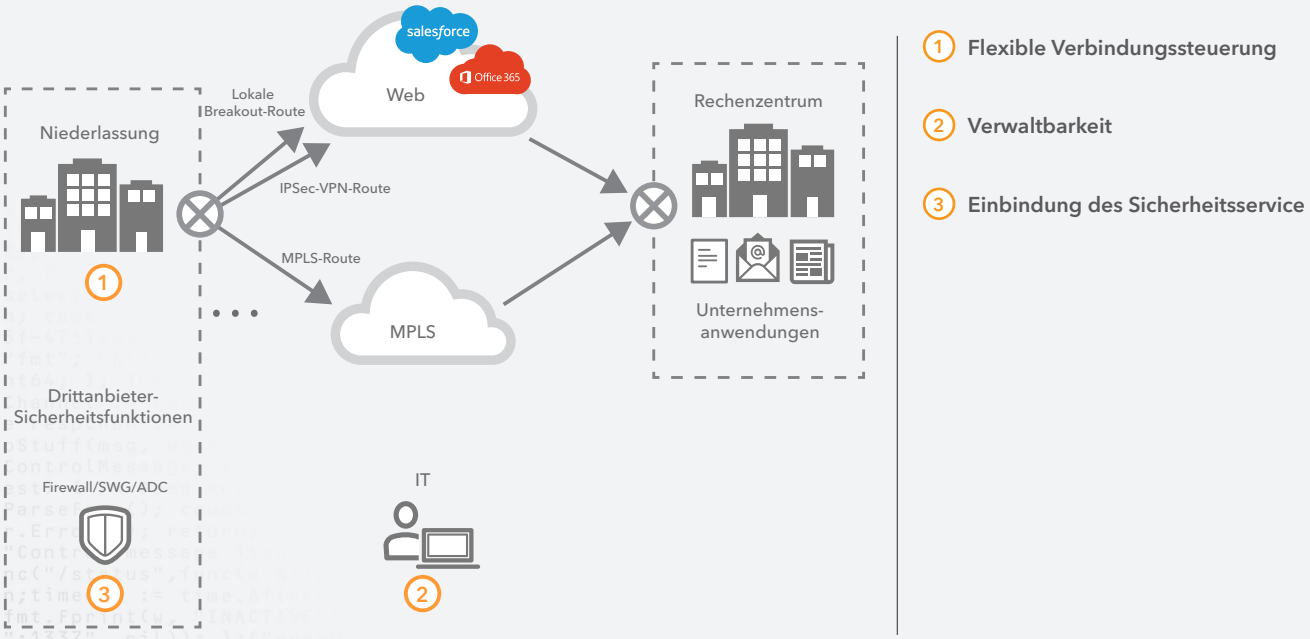
Verwaltbarkeit

Anbieter von SD-WAN können auch Verwaltungsfunktionen bereitstellen, mit denen sich der Betrieb und die Verwaltung von Netzwerkgeräten vereinfachen lassen. Seit den 1990er Jahren bestehen Unternehmens-WANs aus Netzwerkgeräten wie Multilayer-Switches und -Routern. Diese Geräte wurden größtenteils nach Appliance verwaltet. Anders ausgedrückt: Administratoren müssen mehrere Hundert bis mehrere Tausend Geräte einzeln konfigurieren und warten und den jeweiligen Software-Stack der Geräte im gesamten Unternehmen überwachen. Selbst wenn Routinginformationen dynamisch zwischen Geräten ausgetauscht werden oder mithilfe von Routingprotokollen eine hohe Verfügbarkeit hergestellt wird, ist der Aufwand enorm. Mit SD-WAN kann die gesamte Geräteverwaltung über eine einzige, zentrale Konsole erfolgen.

Service-Einbindung

Schließlich spezialisieren sich manche SD-WAN-Anbieter auf die Einbindung von Services. Die Mindestanforderung für ein WAN ist die IP-Erreichbarkeit, nämlich die Layer-3-Netzwerkverbindung im gesamten Unternehmen. Neben dem Netzwerk wurden aber auch die Sicherheitsfunktionen weiterentwickelt: Firewalls, Intrusion Protection Systems (IPS) und Application Delivery Controller, um nur einige zu nennen. In der Vergangenheit benötigten Sie ein kompliziertes Routingdesign, um diese Funktionen in das Netzwerk einzubinden, da die Geräte, die solche Services bereitstellen, in der Regel nicht in der Lage sind, mit dynamischen Routingprotokollen zu kommunizieren (Open Shortest Path First [OSPF], Border Gateway Protocol [BGP]). Dies führt wiederum zu einer komplexen Kombination aus statischem Routing und Neuverteilung. Mit SD-WAN sind diese häufig über Dritte bereitgestellten Technologien einfach konfigurierbar und über ein einheitliches Portal leicht zu verwalten.

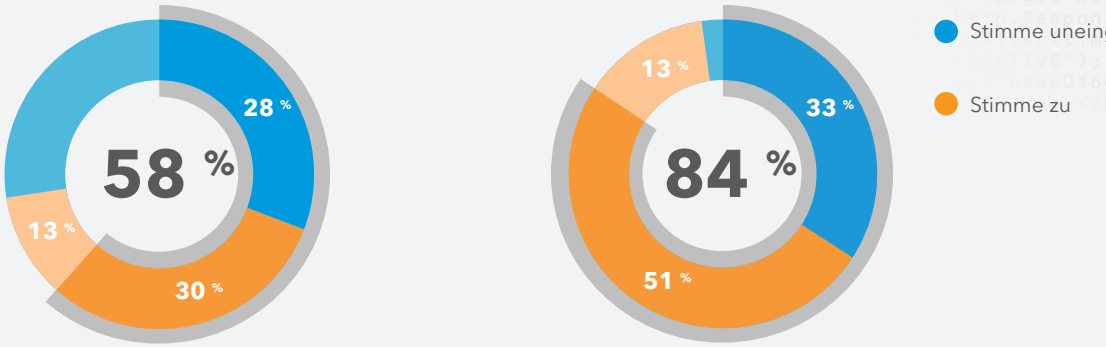
Geschäftliche Vorteile des SD-WAN



Ein neues Modell: Zero-Trust-Sicherheit

Neue Architekturen erfordern neue Sicherheitsfunktionen. Da immer mehr Transaktionen in die Cloud und das Internet verlagert werden, sind Netzwerke heute stark verteilt. Damit entstehen aber ganz automatisch zusätzliche Angriffsflächen. Anwendungen, Nutzer, Daten und Geräte wurden aus der herkömmlichen Kontrollzone verlagert, sodass die klassische Netzwerksicherheit der Vergangenheit angehört. Daher ist es nicht mehr praktikabel, ein Sicherheitsmodell zu entwickeln und umzusetzen, das auf dem Netzwerkübergang beruht. Eine moderne Verteidigungsstrategie muss die heutigen verteilten Workloads und Arbeitskräfte bewältigen können.

Inwieweit stimmen Sie zu/stimmen Sie nicht zu?



„Der Netzwerkübergang ist im heutigen technologischen Umfeld verteilter Cloudnetzwerke und mobiler/Remote-Nutzer unhaltbar."

„Aufgrund der digitalen Transformation müssen herkömmliche Sicherheitsstrategien (klassische Netzwerksicherheit) angepasst werden."

Forrester Research, Build Your Zero Trust Security Strategy With Microsegmentation, September 2018

Das Zero-Trust-Sicherheitsmodell besagt, dass es keine Unterscheidung zwischen intern und extern gibt und dass weder Nutzer und noch Geräte vertrauenswürdig sind. Für jede Zugriffsanfrage sind Authentifizierung und Autorisierung erforderlich. Anwendungen und Daten werden nur nach der Überprüfung bereitgestellt, und selbst dann nur auf vorübergehender Basis und in begrenztem Umfang. Dieses Sicherheitsframework behandelt alle Anwendungen so, als ob sie mit dem Internet verbunden sind. Das Netzwerk gilt als gefährdete und feindliche Umgebung. Darüber hinaus ist die Transparenz von entscheidender Bedeutung. Eine vollständige Protokollierung und Verhaltensanalyse sind ein absolutes Muss.

Zu den Kerngrundsätzen der Zero-Trust-Sicherheit gehören:

- *Der Zugriff muss auf alle Ressourcen sicher erfolgen – unabhängig von Standort oder Hostingmodell.*
- *Setzen Sie bei der Durchsetzung des Anwendungszugriffs eine Strategie mit „minimalen Berechtigungen" und einem „Default-Deny"-Ansatz ein.*
- *Überprüfen und protokollieren Sie den Traffic – für von Ihnen kontrollierte sowie auch für alle anderen Anwendungen. Nur so identifizieren Sie schädliche Aktivitäten.*

Die Zero-Trust-Sicherheit wird durch zwei Hauptkomponenten unterstützt:

- *Identitätssensibler Proxy für sicheren Anwendungszugriff*
- *Secure Internet Gateway zum Schutz von Nutzern*

Identitätssensibler Proxy für sicheren Anwendungszugriff

Wenn sich Nutzer, Daten und Anwendungen in der Cloud befinden und die Verbindung über den direkten Internetzugriff mit einem SD-WAN bereitgestellt wird, warum verlagern Sie dann nicht auch den Sicherheits- und DMZ-Stack in die Cloud? Auf diese Weise können Sie Zero Trust nutzen, um einen sicheren Zugriff auf die von Ihnen kontrollierten Anwendungen zu gewährleisten. Gleichzeitig mindern Sie das Risiko, das entsteht, wenn Nutzer auf nicht von Ihnen kontrollierte Anwendungen zugreifen.

Wenn Sie aktuell für den Zugriff auf Unternehmensanwendungen ein einfaches VPN-Setup nutzen, gewähren Sie wahrscheinlich jedem angemeldeten Nutzer IP-basierten Zugriff auf das gesamte Netzwerk. Dies ist jedoch äußerst riskant und verstößt gegen die Grundsätze der Zero-Trust-Sicherheit. Warum sollten Mitarbeiter im Callcenter Zugriffsberechtigungen für Quellcode-Repositorys haben? Warum sollte ein Auftragnehmer, der Ihr Abrechnungssystem verwendet, Zugang zu Kreditkarten-Verarbeitungsterminals haben? Zugriff sollte nur auf die Anwendungen gewährt werden, die für die Aufgaben einer Rolle erforderlich sind. Beim herkömmlichen VPN ist diese präzise Zugriffssteuerung nicht möglich. Es stützt sich nach wie vor stark auf ein Hub-and-Spoke-Netzwerkmodell.

Eine identitätssensible Proxy-Architektur (Identity-Aware Proxy, IAP) bietet über einen cloudbasierten Proxy Zugriff auf Anwendungen. Identität und Autorisierung erfolgen an der Edge und basieren auf „Need to know"-Prinzipien mit geringstmöglichen Berechtigungen, die dem Zugriff über SDPs (softwaredefiniertes Netzwerk) ähnlich sind, aber stattdessen standardmäßige HTTPS-Protokolle auf Anwendungsebene verwenden (Layer 7).

Die beiden Möglichkeiten zum Einsatz eines IAP

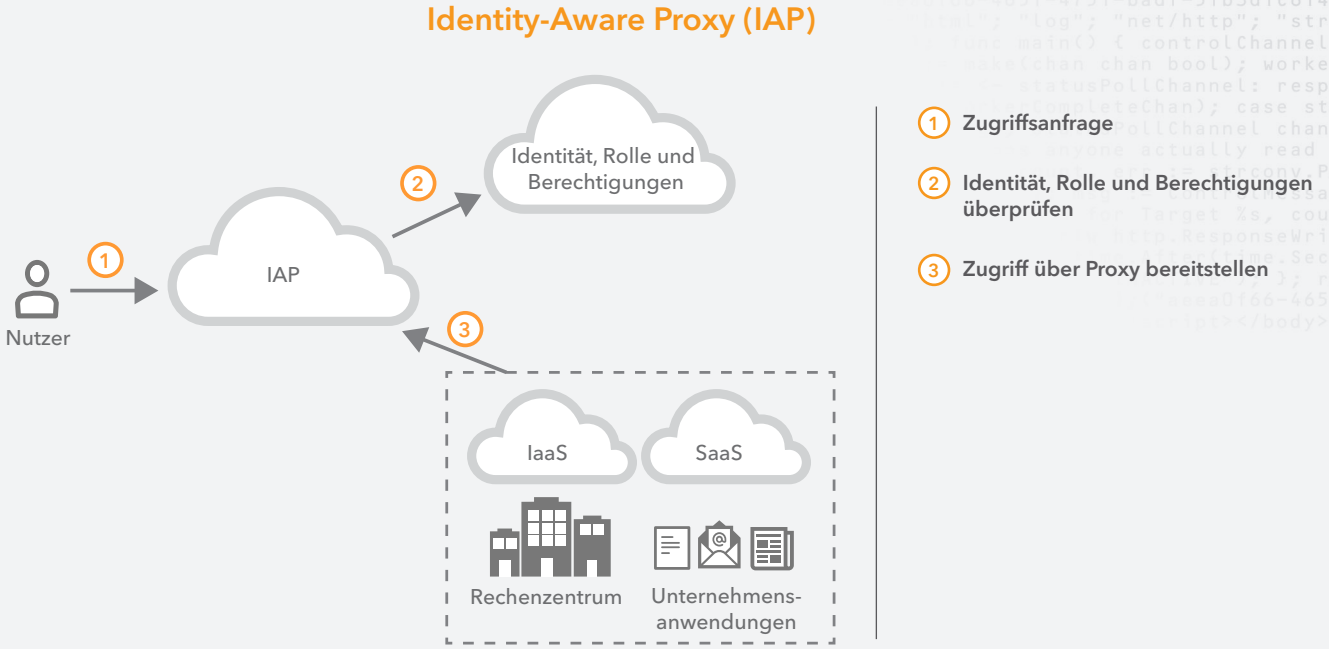
Sie integrieren ein CDN in länderübergreifende Transaktionen, um die Anwendungsreaktion zu verbessern.

ODER

Sie verwenden eine Web Application Firewall (WAF), um die Webserver des Unternehmens vor häufigen Schwachstellen wie SQL Injection und Cross-Site Scripting zu schützen.

Die Schlüsselkomponente eines IAP ist eine Identitätsquelle, die die Vertrauenswürdigkeit von Nutzern und Geräten (Authentifizierung) und deren Zugriffsrechte (Autorisierung) überprüft. Diese Identitätsquelle kann auf Unternehmensverzeichnissen oder cloudbasierten Identitätsanbietern beruhen. Selbst bevor die Identität eines Nutzers überprüft wird, kann durch die Prüfung des jeweiligen Gerätestatus sichergestellt werden, dass das Gerät, über das ein Zugriffsversuch unternommen wird, bestimmte Sicherheitskriterien erfüllt, z. B. ein Zertifikat, das neueste Betriebssystem, Passwortschutz oder dass eine angemessene Endpunkterkennungs- und Reaktionslösung installiert und betriebsbereit ist.

IAP hat im Vergleich zu anderen Zugangstechnologien einen bemerkenswerten Vorteil: Es werden nicht nur die Nutzer, sondern auch der Traffic der Nutzer überprüft, und einzelne Anwendungsanfragen können beendet, geprüft und autorisiert werden. Wenn eine Transaktion auf dem Proxy beendet ist, können zusätzliche Services integriert werden, die das Nutzererlebnis und den Anwendungsschutz verbessern.



Darüber hinaus verwendet der IAP Zugriffskontrollen auf Anwendungsebene anstelle von Firewall-Regeln. Konfigurierte Richtlinien können daher nicht nur Ports und IPs, sondern auch die Absichten von Nutzern und Anwendungen widerspiegeln. Wie SDPs lassen sich mit diesem Ansatz die Anwendungen und anderen Ressourcen in der Cloud oder hinter der Firewall verbergen, und für Webanwendungen ist er clientlos.

Aufgrund der zunehmenden Cloudnutzung ist die Migration von Unternehmensanwendungen ein thematischer Schwerpunkt. Viele Unternehmen haben Schwierigkeiten, die Cloud für cloudbasierte und herkömmliche Anwendungen gleichermaßen zu nutzen. Mit dem IAP können nicht nur Nutzer für native SaaS-Anwendungen authentifizieren werden, sondern auch ältere Anwendungen im Rechenzentrum als „SaaS" behandelt werden. Darüber hinaus werden Cloudmigration und Anwendungsmodernisierung durch einen Proxy ohne eine umfassende Strategie zum vollständigen Austausch von Komponenten erleichtert. Somit können Unternehmen einen methodischen, schrittweisen Ansatz für die Implementierung von Zero Trust verfolgen und gleichzeitig die technischen Anforderungen reduzieren, die mit veralteten Kontrollen am Netzwerkübergang und herkömmlichen VPNs verbunden sind.

Secure Internet Gateway zum Schutz von Nutzern

Ein wichtiger Aspekt bei der Umstellung auf ein Zero-Trust-Sicherheitsmodell besteht darin, dass Nutzer sicher bleiben, während sie auf nicht von Ihnen kontrollierte Anwendungen zugreifen. Bei jedem Klick im Internet sind Nutzer einer Vielzahl von Cyberbedrohungen ausgesetzt. In der Vergangenheit, als Nutzer noch an das Unternehmensnetzwerk und verwaltete Geräte gebunden waren, bestand der Schutz vor Malware, Ransomware und Phishing ganz einfach in der Einführung von Endpoint-Virenschutz, der Installation eines Appliance-Stacks in einem Rechenzentrum und der Zurückleitung des Traffics zur Inspektion und Kontrolle.

Mit Nutzern an mehreren Standorten wird das Internet zum Unternehmensnetzwerk der Wahl. Ein cloudbasiertes SIG bietet Ihnen einen sicheren Einstieg und schützt Nutzer an beliebigen Standorten auf proaktive Weise.

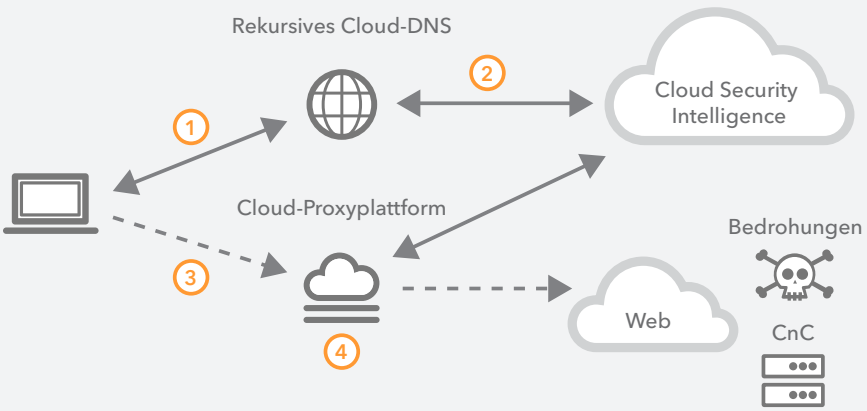
Heute befinden sich die Nutzer nicht mehr im Gebäude, Geräte werden nicht mehr verwaltet und das Internet wird zum bevorzugten Unternehmensnetzwerk. Die Konnektivität durch direkten Internetzugriff macht zentrale Sicherheitslösungen für Kontrolle und Inspektion überflüssig. Eine Alternative besteht darin, den Sicherheits-Appliance-Stack bei jeder Verbindung mit dem Internet zu replizieren. Für die meisten Unternehmen ist dies jedoch einfach – sowohl logistisch als auch finanziell – nicht möglich. Und was vielleicht noch wichtiger ist: Die inhärente Komplexität dieses Ansatzes führt zu Sicherheitsfehlern, die in direktem Widerspruch zu den Best Practices von Zero Trust stehen.

Eine einfachere, schnellere und kostengünstigere Methode zur Sicherung des Traffics über direkten Internetzugriff ist der Einsatz eines cloudbasierten Secure Internet Gateway (SIG). Ein SIG ist ein sicherer Einstieg in das Internet, bei dem Nutzer unabhängig von ihrem Standort proaktiv vor hoch entwickelten Bedrohungen geschützt werden, indem riskanter Traffic zur Kontrolle und Überprüfung an den Proxy geleitet wird. Dies wird erreicht, indem jede einzelne DNS-Anfrage untersucht, Anfragen an schädliche Domains blockiert, Anfragen an sichere Domains wie gewohnt bearbeitet und Anfragen für riskante Domains zur weiteren Überprüfung an einen Cloud-Proxy weitergeleitet werden.

Wenn der Proxy zu diesem Zeitpunkt eine HTTPS-Anfrage erhält, vergleicht er die angeforderte URL mit einer cloudbasierten Wissensdatenbank für Bedrohungsinformationen und blockiert schädliche URLs. Für alle anderen angeforderten URLs, die als riskant kategorisiert sind, sendet der Proxy den Webinhalt zur Inline-Payload-Analyse über mehrere Malware-Analyse-Engines. Diese Engines verwenden eine Reihe von Erkennungstechniken – Signatur, signaturlos und Machine Learning –, um bekannte Bedrohungen und bisher unbekannte Zero-Day-Bedrohungen zu identifizieren und zu blockieren. Durch eine Reihe von Erkennungsmethoden können Sie eine Payload je nach Inhaltstyp an die am besten geeignete Engine (oder Engines) leiten, um optimale Erkennungsraten zu gewährleisten und möglichst wenige False Positives zu erhalten.

Beachten Sie, dass sich dieser Ansatz deutlich von dem unterscheidet, der von älteren Sicherheits-Appliances wie Secure Web Gateways (SWGs) verwendet wird. Insbesondere wird der gesamte Internettraffic, sowohl der gute als auch der schädliche, von SWGs durch einen Proxy überprüft, was sich besonders negativ auf komplexe Webseiten und umfassendere HTTPS-Inhalte auswirken kann. Dieser Ansatz verschlechtert die Performance, führt zu Latenz und zu mehr Problemen mit nicht erreichbaren Websites und Anwendungen, die auftreten, wenn der gesamte Traffic über einen Proxy geleitet wird. Durch SWGs ergeben sich häufig mehr Sicherheitsvorfälle und False Positives, wodurch Helpdeskanfragen ausgelöst und IT-Ressourcen in Anspruch genommen werden.

Secure Internet Gateway-Architektur



1. **DNS-Lookup**
2. **Kategorisierung der Domain in Bezug auf gutartig, schädlich und verdächtig**
3. **Verdächtige Domänen werden an einen Cloud-Proxy umgeleitet**
4. **URL-Bedrohungsinformationen und Payload-Analyse**

Ein intelligenter selektiver Proxy kann DNS sowohl als Einstieg in das Internet als auch als erste Sicherheitsebene nutzen. So wird sicherer Traffic direkt durch das Internet geleitet, schädlicher Traffic gesperrt und nur risikoreicher Traffic per Proxy übermittelt. Das Ergebnis:

- *einfachere Sicherheit*
- *geringere Latenz und bessere Performance*
- *weniger Schaden für Webseiten und Anwendungen*

Netzwerktransformation mit geringerem Risiko: Implementierung von Zero Trust in einer SD-WAN-Umgebung

Viele Unternehmen, die zu internetbasierten Architekturen migrieren, betrachten SD-WAN aufgrund der Verbindungssteuerung und der Fähigkeit, die finanzielle Belastung durch MPLS-Eigentumsrechte potentiell zu senken, als Schlüsselfaktor. Möglicherweise verwenden sie Breitband- oder Wireless-Netzwerke, um die MPLS-Verbindungen zu erweitern oder zu ergänzen und so ein Hybrid-WAN zu schaffen. Wenn sie sich jedoch bereits für den direkten Internetzugriff entschieden haben, ist es sinnvoll, ein Sicherheitsmodell mit demselben Ansatz zu verwenden.

Gleichzeitig mit der Einführung von SD-WAN müssen Unternehmen ihr Sicherheitsframework am Netzwerkübergang zu einem Zero Trust-Framework an der Edge weiterentwickeln. Wie weit sind wir heute – und was kommt als Nächstes?

Netzwerke mit SD-WAN lassen sich je nach Denkweise und langfristiger Strategie des Unternehmens in der Regel mit einer der folgenden drei Situationen beschreiben:

1. *Herkömmliches privates WAN mit zentralisierter Verbindung, d. h. SD-WAN wird in Betracht gezogen, ist aber noch nicht implementiert*
2. *Hybride Implementierung von herkömmlichem privatem WAN an vorhandenen Standorten und SD-WAN an neueren Niederlassungen*
3. *Hauptsächlich SD-WAN*

Ein Zero-Trust-Sicherheitsansatz kann in all diesen Szenarien gut passen. Wenn das Unternehmen jedoch bereits SD-WAN in Betracht zieht oder implementiert, wird das Internet möglicherweise bereits als brauchbares Tool für ein Unternehmensnetzwerk genutzt und ist daher für die Verwendung einer Zero-Trust-Sicherheitsstrategie für die Netzwerkumgebung des Unternehmens bestens gerüstet.

Sehen wir uns nun die derzeit verwendeten Architekturen an, um zu ermitteln, wie Zero Trust jeweils implementiert werden könnte. Im Anschluss daran zeichnen wir ein Bild des gewünschten zukünftigen Szenarios.

Herkömmliches privates WAN mit zentraler Verbindung

Wenn die Beweggründe hinter der SD-WAN-Migration Kosten, Agilität und Flexibilität sind – Vorteile, die eine internetbasierte Netzwerkarchitektur bieten kann –, könnte es sinnvoll sein, SD-WAN komplett zu überspringen und direkt zu einem Zero-Trust-Framework zu wechseln. Ein IAP ermöglicht unabhängig vom Standort einen auf Zero Trust basierten Zugriff auf Anwendungen, während ein SIG Nutzern sicheren Internetzugang bietet – und das alles, ohne dass Unternehmen bei jeder Internetverbindung Sicherheitsstacks erstellen müssen.

Ein wichtiger Punkt: Wenn das Unternehmen bereits Echtzeitservices wie VoIP und Videokonferenzen über einen Internet-Cloudserviceanbieter unterstützt, ist es ideal positioniert, um eine internetbasierte Netzwerk- und Zugriffsarchitektur vollständig zu nutzen. Wenn diese Services weiterhin hauptsächlich vor Ort bereitgestellt werden, sollte möglicherweise ein gewisses Maß an „privater" Netzwerkkommunikation zwischen Standorten beibehalten werden, entweder privat (z. B. über MPLS) oder auf Grundlage des SD-WAN.

Hybridnetzwerk mit herkömmlichem WAN und SD-WAN

In diesem Szenario haben Unternehmen bereits den ersten Schritt hin zu einer effizienteren, internetbasierten Architektur getan.

Bei diesen Umgebungen sollten Sie sich unbedingt vor Augen führen, wie der Traffic der Nutzer gehandhabt wird:

- *Haben Nutzer direkten Internetzugang von Remote-Standorten oder wird die Internetverbindung nur für die Vernetzung mit den Hauptstandorten verwendet?*
- *Wo befinden sich die primären Nutzeranwendungen? Vor Ort, in einem Rechenzentrum oder in der Cloud?*
- *Wie stellen Nutzer bei Verwendung der Cloud eine Verbindung zu diesen Anwendungen her? Erfolgt dies über den direkten Internetzugriff von einer Niederlassung aus oder über eine Zurückleitung zu einer direkten Verbindung?*
- *Wie umfangreich ist die Nutzung von SaaS-Anwendungen?*
- *Wie umfassend ist der Sicherheitsstack für den direkten Internetzugriff auf Niederlassungsebene an jedem Standort?*

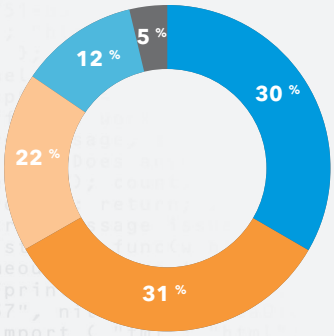
Natürlich variieren die Antworten auf diese Fragen je nach Behandlung des Nutzertraffics – und daher ist die Netzwerkmigration unterschiedlich komplex. Es gibt aber zwei Konstanten: Die Internetnutzung sowie die Notwendigkeit für einen Übergang von der klassischen Netzwerksicherheit zu einem Zero-Trust-Modell werden weiter ansteigen.

Nehmen wir zum Beispiel eine Situation, in der eine Verbindung mit direktem Internetzugriff von einem Remote-Standort aus besteht. Über ein SIG können zusätzlicher Schutz für den zentralisierten Sicherheitsstack gewährleistet sowie ein Teil des Stacks ersetzt werden, um Komplexität und Kosten zu reduzieren.

Wenn Nutzer auf cloudbasierte Anwendungen zugreifen, könnten mit einem IAP-basierten Ansatz sowohl die Sicherheit des Unternehmens als auch das Nutzererlebnis verbessert werden. Ein solcher Ansatz steigert möglicherweise auch die Anwendungsperformance, da über ein CDN direkter Zugriff auf Anwendungen über das Internet ermöglicht wird.

Und Sie können nach wie vor von einem herkömmlichen WAN zu einer SD-WAN-Umgebung wechseln. Dazu müssen Sie lediglich den direkten Internetzugriff für Remote-Standorte aktivieren und die Prinzipien der Zero-Trust-Sicherheit umsetzen.

Welche Pläne gibt es aktuell in Ihrem Unternehmen bezüglich des Einsatzes von Software Defined (SD-WAN)-Netzwerktechnologie?



- Wird bereits verwendet
- Wird innerhalb des nächsten Jahres getestet
- Einführung ist in den nächsten zwei Jahren geplant
- Wird in Betracht gezogen, aber keine konkreten Pläne
- Wird nicht in Betracht gezogen, keine Pläne

Forrester Research, Digital Transformation Drives Distributed Store Networks to the Breaking Point, April 2018

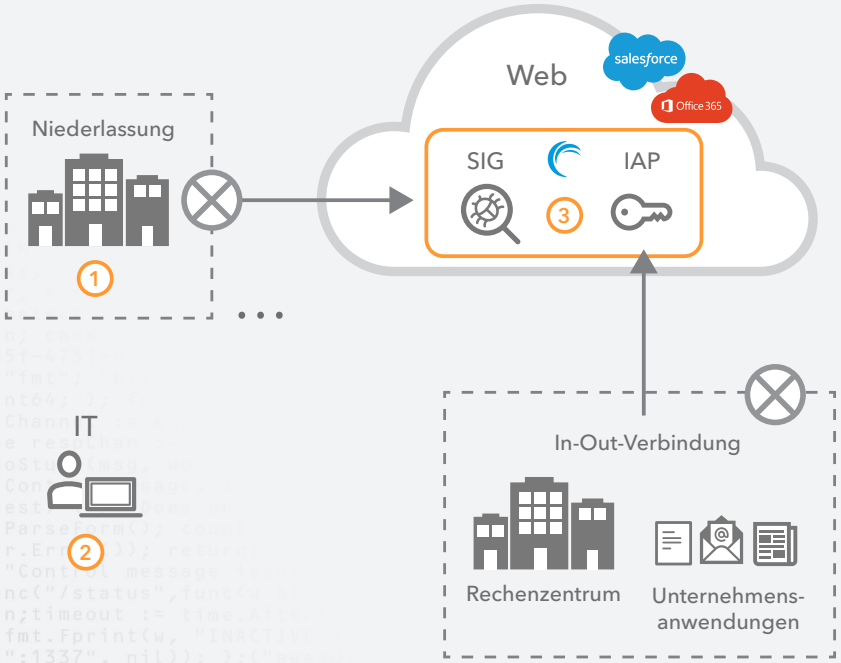
Hauptsächlich SD-WAN

In diesem Zustand ist es wahrscheinlich, dass das Unternehmen kein herkömmliches privates WAN-Netzwerk mehr nutzt, sondern für die Kommunikation zwischen Standorten intelligentes Routing über Internetverbindungen verwendet und damit die Vorteile des direkten Internetzugriffs voll ausschöpfen kann. Diese Unternehmen verlassen sich bereits an den meisten Standorten auf den Internetzugang. Daher ist die Entwicklung des Netzwerks über SD-WAN hinaus eine logische Entwicklung.

Der nächste Schritt? Beginnen Sie damit, Ihre Abhängigkeit von MPLS-Verbindungen zu reduzieren, indem Sie Anwendungen in das Internet verlagern, um Flexibilität und Kosteneffizienz zu erreichen. Selbst in einer Umgebung mit direktem Internetzugriff sind Unternehmensanwendungen über den IAP zugänglich. Wenn sich Anwendungen bereits in einer Cloudumgebung befinden, ist es nicht sinnvoll, durch Zurückleitung des Traffics an ein Rechenzentrum auf sie zuzugreifen, bevor an einem zentralen Standort eine Internetverbindung aufgebaut wird (z. B. über eine Direct Connect-Topologie).

Schließlich eignet sich diese Umgebung gut für einen zukünftigen Zustand mit reiner internetbasierter Konnektivität und internetbasiertem Zugang. Der Zugriff auf alle Unternehmensanwendungen, ob vor Ort oder cloudbasiert, kann dann über den direkten Internetzugriff erfolgen. Der gesamte Nutzertraffic kann über SIG gesichert werden. Und wenn internetbasierte Anbieter Echtzeitkommunikation wie Sprache und Video bereitstellen, sollte es möglich sein, SD-WAN und sogar das Unternehmens-WAN vollständig abzuschaffen. Dadurch könnten Kosten und Komplexität reduziert und die Sicherheit über ein Modell mit Zero-Trust-Architektur verbessert werden.

Wert der internetbasierten Architektur mit einem Zero-Trust-Sicherheitsmodell



1. **Einfachster Netzwerkzugriff**
   - Nur Internetzugriff
   - Kein Out-In-Zugriff
2. **Verwaltbarkeit**
   - Zentrale Verwaltung
   - Geräteüberwachung
   - Nutzerüberwachung
3. **Weitere Sicherheitskontrolle**
   - Verhindern von Zero-Day-Angriffen
   - Zentralisiertes AAA (Authentifizierung, Autorisierung und Accounts)
   - Überprüfung des Clientstatus
   - Verhindern von Phishing, Malware und CnC

Digitaler Wandel für Ihr Unternehmen

Die moderne geschäftliche Realität führt zu erhöhter Gefährdung in einer Umgebung, die bereits mit Risiken und Komplexität verbunden ist. Ein Netzwerkmodell, das durch Hub-and-Spoke-Transaktionen in einem privaten WAN gesteuert wird, ist ebenso veraltet wie ein Unternehmensschutz am Netzwerkübergang. Sowohl die Netzwerk- als auch die Sicherheitsarchitektur müssen sich weiterentwickeln. Ein SD-WAN ermöglicht zwar derzeit eine effiziente Verarbeitung von Traffic im Unternehmensnetzwerk sowie die Verlagerung von Workloads in die Cloud, aber dieses Netzwerkmodell ist langfristig nicht tragbar. Das Internet ist das Unternehmens-WAN der nahen Zukunft.

Akamai ist der Ansicht, dass die Verwendung von SD-WAN in Kombination mit den entsprechenden Zero-Trust-konformen Sicherheits- und Zugriffsservices der erste Schritt für den Übergang zum Internet als Unternehmensnetzwerk ist. Wenn Sie SD-WAN mit der Akamai Intelligent Edge Plattform kombinieren, können Sie universelle Zugriffs- und Sicherheitsrichtlinien anwenden und über das Internet für Ihre Anwendungen ein schnelles und zuverlässiges Endnutzererlebnis gewährleisten.

Akamai kann Sie bei der Entwicklung Ihres Netzwerks und Ihrer Sicherheitslösungen unterstützen. Wenden Sie sich an Ihr Account-Team, um mehr über die Zero-Trust-Bewertung von Akamai zu erfahren. Sie erhalten konkrete Empfehlungen von unseren Sicherheitsexperten zu ersten Schritten oder zur Weiterentwicklung Ihres Umstiegs auf Zero Trust. Oder lesen Sie *3 einfache Maßnahmen zur Umsetzung von Zero-Trust-Sicherheit*, um Informationen zu Ressourcen für den Einstieg zu erhalten.