

Wie Sie mit SD-WAN Ihre Sicherheit erhöhen

WHITEPAPER

Die vielleicht wichtigste und umfassendste Strategie im Bereich IT-Infrastruktur ist die Entwicklung in Richtung Software-definierter Umgebungen. Eine gute Definition von Software-definierter Infrastruktur lautet wie folgt:

Eine Recheninfrastruktur, die vollständig von Software kontrolliert wird, ohne menschliches Eingreifen im Betrieb. Sie arbeitet unabhängig von Hardware-spezifischen Abhängigkeiten und ist programmatisch erweiterbar.

Diese Vorteile treiben die schnelle Einführung von Software-definierten Wide Area Networks (SD-WANs) voran. Das WAN ist eine entscheidende Komponente einer flexiblen IT-Infrastruktur und muss viele der gleichen Vorteile bieten wie andere Aspekte der Infrastruktur auch: Effizienz, Einfachheit, Transparenz und Skalierbarkeit.

Ausserdem bieten neue und sichere SD-WAN-Dienste neben den typischen Vorteilen auch eine wesentlich verbesserte Plattform zur Erhöhung der Sicherheit des Unternehmens. Die wirklich sichere SD-WAN-Lösung trägt dazu bei, viele der heiklen Probleme in Sachen Cybersicherheit zu lösen, mit denen Unternehmen konfrontiert sind, wenn sie öffentliche Netzwerke für sensible Arbeitsabläufe nutzen. Sichere SD-WAN-Dienste bieten dem Netzwerkmanager oder Administrator neue Möglichkeiten. In der Vergangenheit war MPLS häufig die einzige Technologie, die effektiv dafür genutzt werden konnte, eine sichere Netzwerkinfrastruktur bereitzustellen. Mit neuen sicheren SD-WAN-Diensten ist es nun jedoch möglich, hochsichere hybride Netzwerke zu implementieren. Dies verändert die Spielregeln grundlegend und bietet weitaus mehr Flexibilität und effizientere Optionen.



Custom Media



Erhöhte Sicherheit im SD-WAN ist eine entscheidende Verbesserung. Beispielsweise kann die Nutzung des direkten Internetzugangs die Wirksamkeit aktueller Sicherheitslösungen vereiteln, wenn das Netzwerk zur „Hintertür“ wird. Angesichts vieler SD-WAN-Angebote, die sich ausschliesslich auf die Kosten konzentrieren und wenig zur Erhöhung der Sicherheit leisten, geht es vorausschauenden Unternehmen heute viel stärker darum sicherzustellen, dass eine SD-WAN Installation keine Schwachstellen in Zweigstellen mit direktem Internetzugang verursacht. Zusätzlicher Schutz wird durch die Nutzung von Connectivity-as-a-Service (CaaS)-Angeboten erreicht, die alle ISP-Verbindungen zentral verwalten. Diese Art von Service stellt sicher, dass Sicherheitsrichtlinien und Cyberschutz-Produkte konsequent für alle ISP-Verbindungen implementiert werden.

BRANCHENFÜHRENDE SD-WAN-LÖSUNGEN MÜSSEN INTEGRIERTE SICHERHEIT BIETEN

Eines der grundlegendsten Probleme des traditionellen Ansatzes zur Netzwerksicherheit liegt in der Vorgehensweise, zuerst das Netzwerk aufzubauen und danach die Sicherheit zu ergänzen. Das ist kein Problem, das auf Fehlentscheidungen von Sicherheits- oder Netzwerkexperten zurückzuführen ist, sondern vielmehr darauf, dass bestehende Netzwerke abgesichert werden müssen, nachdem sie bereits im Einsatz sind. Bei der Implementierung eines neuen SD-WAN-Dienstes besteht die Möglichkeit, Sicherheitsfunktionen in das Netzwerk zu integrieren, schon während es installiert wird. Dies bietet zahlreiche Vorteile, wie zum Beispiel die Möglichkeit der:

- Anwendung von Sicherheitsrichtlinien und Schutz im gesamten Netzwerk, und zwar in konsistenter Weise
- zentralen Verwaltung für das gesamte SD-WAN, die vollständige Transparenz bietet, wodurch die Sicherheit erhöht wird
- Gewährleistung, dass Patches und Updates schneller eingespielt und im gesamten Netzwerk verteilt werden

Dieser Ansatz hilft auch dem SecOps-Team: Seine Arbeitsbelastung wird reduziert, wenn durch den Einsatz von SD-WAN-Lösungen die Sicherheit im gesamten WAN konsistent garantiert wird. Mit dem Einsatz einer sicheren SD-WAN-Lösung beginnen NetOps und SecOps enger

zusammenzuarbeiten. Die Integration von SecOps- und NetOps-Teams ist ein wichtiger Fortschritt und führt zu einer besseren Kommunikation und Interaktion, was seinerseits ebenfalls die allgemeine Sicherheit erhöht.

Ein weiterer wichtiger Vorteil von sicherem SD-WAN ist die Unterstützung der digitalen Mitarbeiter. Die moderne Belegschaft ist nicht nur sehr mobil und agil, sondern auch sehr dynamisch, da Zeitarbeiter, Auftragnehmer und Partner häufig kommen und gehen. Ältere Ansätze zur Sicherung des Netzwerkzugriffs, die ein erhebliches manuelles Eingreifen von Netzwerk- oder Sicherheitsexperten erfordern, sind da keine gute Lösung. Secure SD-WAN ist demgegenüber eine wesentliche Verbesserung. Die Anwender werden es sehr schätzen, dass sie jedes beliebige Netzwerk nutzen können und stets mit der gleichen Performance ihrer genutzten Anwendungen rechnen können. Darüber hinaus ist diese Leistung überall verfügbar und die Beseitigung der Abhängigkeit von Usern zur Gewährleistung der Netzwerksicherheit eliminiert ein grosses Nutzungshindernis, das den Benutzer oft dazu zwingt, sich tief in die Technologie einzuarbeiten.

Die Cloud ist ein weiterer wichtiger Aspekt für die Bereitstellung sicherer SD-WANs der nächsten Generation. Die deutliche Mehrheit der Grossunternehmen hat bereits mehrere Cloud-Services unter Vertrag. Ein mittelständisches Unternehmen wird über viele Cloud-Dienste und eine Reihe von Cloud-Anbietern verfügen. Untersuchungen von RightScale¹ zeigen, dass das durchschnittliche Unternehmen bereits fünf verschiedene Clouds nutzt, und eine Studie von Logic Monitor² schätzt, dass bis 2020 83 Prozent der Workloads in der Cloud liegen werden. Für die Nutzung mehrerer Cloud-Dienste ist ein Netzwerk erforderlich, das reibungslos einen leistungsfähigen Zugriff auf jede dieser Clouds ermöglichen und sicherstellen kann, dass keine der Clouds zu einem Silo wird. Ein einziges logisches SD-WAN, das die Verwaltung und Bereitstellung von Bandbreite für alle Clouds gewährleistet, ist der beste Ansatz, um eine breite Nutzung der Cloud zu ermöglichen. Diese Art der Bereitstellung ermöglicht es dem Unternehmen auch sicherzustellen, dass die für die Gewährleistung der Performance erforderliche Bandbreite für alle Clouds auf die effizienteste Weise zur Verfügung steht.

¹„CloudComputingTrends:2018StateoftheCloudSurvey“(UmfragezumStatusderCloud2018),RightScale,13.Februar2018
²„83% Of Enterprise Workloads Will Be in the Cloud By 2020“, Louis Columbus, Forbes, 7. Januar 2018



SD-WAN-DIENSTE MIT INTEGRIERTER SICHERHEIT ELIMINIEREN SCHWACHSTELLEN

Im Hinblick auf Cybersicherheit kann die unkontrollierte Nutzung öffentlicher Netzwerkdienste neue Schwachstellen mit sich bringen. Dies erschwert die Arbeit der Netzwerkadministratoren wie auch der Sicherheitsingenieure. Sichere SD-WAN-Dienste können viele dieser Schwachstellen und potenziellen Einstiegspunkte entschärfen. SD-WAN-Lösungen, die nicht über integrierte Sicherheit verfügen, wirken überholt oder eignen sich nur für bestimmte und genau definierte Prozesse, die die Risiken auffangen können.

Aus diesem Grund sollten Unternehmen ihr Kaufinteresse auf SD-WAN-Dienste mit integrierter Sicherheitsfunktionalität richten. Um effektiv zu sein, sollte die Sicherheit als integrale Komponente des Angebots umgesetzt und nicht lediglich ein ergänzendes Sicherheitsprodukt eines Drittanbieters sein. Der wichtigste Grund für die Konzentration auf sichere SD-WAN-Dienste ist, dass eine dynamische Netzwerknutzung ohne Vorwarnung Schwachstellen verursachen kann, wenn ungesicherte neue oder andere Netzwerke verwendet werden. Um diesem Problem abzuhelpfen, muss Sicherheit in allen Netzwerken implementiert werden.

Einige Netzwerk- und Sicherheitsteams haben die Angst vor Sicherheitsbedrohungen in öffentlichen Netzwerken zum Anlass genommen, sich nur auf MPLS- oder private Netzwerke zu konzentrieren. Doch wenn Sicherheit in der richtigen Weise in IP-Netzwerke integriert ist, werden die Probleme entschärft. Entscheidend für die Sicherheit ist, dafür zu sorgen, dass wichtige Sicherheitsfunktionen im gesamten SD-WAN konsequent implementiert werden. Dazu gehören:



Firewall



**Datenverkehrs-
überwachung**



Verschlüsselung

OPEN SYSTEMS LIEFERT SICHERE SD-WAN-LÖSUNGEN

Open Systems ist ein führender Anbieter im Bereich Secure SD-WAN. Im Rahmen dieser Führungsrolle bietet das Unternehmen SD-WAN-Dienste mit integrierter Sicherheitsfunktionalität, die einen konsistenten Schutz für

alle Ihre ISPs gewährleisten. Dies führt zu einer drastischen Vereinfachung des Betriebs. Es ist nicht mehr notwendig, jedes IP-Netzwerk einzeln zu verwalten und zu sichern oder spezifische Routing-Regeln zu erstellen, um weniger sichere Netzwerke zu meiden.

Der SD-WAN-Dienst nutzt das CaaS-Angebot von Open Systems. Der Kunde kann alle ISP-Leitungen mit einem Dienst verwalten, die Providerauswahl optimieren, dynamische Leitungsskalierung nutzen und von einem schnelleren Bestellprozess profitieren, während gleichzeitig die Sicherheit für diese verschiedenen Leitungen gewährleistet ist. Dies ist sehr vorteilhaft, da das CaaS-Angebot von Open Systems Carrier- und Transport-unabhängig ist und so dem Kunden mehr Möglichkeiten bietet.

Die Secure SD-WAN-Lösung des Unternehmens überbrückt die Kluft zwischen den Mitarbeitern von NetOps und dem Sicherheitsteam. Sicherheitsexperten können sich darauf verlassen, dass kritische Sicherheitsfunktionen wie Firewall, Datenverkehrsüberwachung und Verschlüsselung auf ISP-Leitungen genauso genutzt werden wie bei anderen Netzwerken und Netzbetreibern. Dadurch wird die betriebliche Komplexität des Netzwerks drastisch reduziert. Viele Netzwerk-Verwundbarkeiten lassen sich auf inkonsistente Bereitstellung von Sicherheitsrichtlinien oder -produkten zurückführen, die das Resultat einer zu hohen Komplexität des Netzwerks ist. Das hat zur Folge, dass man nie sicher sein kann, dass alle Leitungen geschützt sind.

WICHTIGE ERKENNTNISSE

Der Einsatz von SD-WAN nimmt drastisch zu, und in vielen Fällen ist es ein Mittel zur Verringerung von Netzwerkkomplexität, die mit Schwachstellen einhergehen kann. Allerdings ist SD-WAN lediglich ein Anfang zur Verringerung des Risikos. Der Einsatz eines sicheren SD-WAN-Angebots, das die wichtigsten Sicherheitstechnologien enthält, verbessert die Abwehr des Unternehmens und bietet weitaus mehr Schutz. Wahrscheinlich erhöht die Implementierung von SD-WAN-Diensten ohne Sicherheit die Gefahr eher, als dass sie sie reduziert.

Die Verwendung eines sicheren SD-WAN bietet die meisten Sicherheitsvorteile, die sich aus der „Software-Definiertheit“ anderer Aspekte der Infrastruktur ergeben: konsequente Anwendung von Richtlinien, konsistente Implementierung spezifischer Sicherheitstechnologien und -werkzeuge sowie umfassende Transparenz in der gesamten Infrastruktur. Dieses Denken, in Kombination mit der Implementierung anderer einzigartiger Sicherheitsfunktionen, prägt das Secure SD-WAN-Angebot von Open Systems. **Dieser Service stellt einen grossen Fortschritt bei der Bereitstellung sicherer, agiler und kosteneffizienter Netzwerke dar. Weitere Informationen finden Sie unter <https://www.open.ch/de>**