ExperTeach

White Paper

Software-Defined Wide Area Networks (SD-WAN)

Funktion, Leistungsmerkmale, Security, Kosten & Szenarien

Veränderung der IT- und WAN-Architekturen

Die Nutzung von Cloud-Lösungen, mobiles Arbeiten, Home Office sowie das Edge Computing befinden sich voll im Trend und führen dazu, dass sich die IT-Architekturen wandeln. Zunehmend werden Cloud Services in Form von Infrastructure as a Service (IaaS) oder Software as a Service (SaaS) – allen voran Microsoft Office 365 – integriert. Gerade letzteres, welches über öffentliche IP-Adressen im Internet erreicht wird, stellt einen starken Treiber dar, die klassische Wide Area Network-Infrastruktur (WAN-Infrastruktur) zu überdenken.

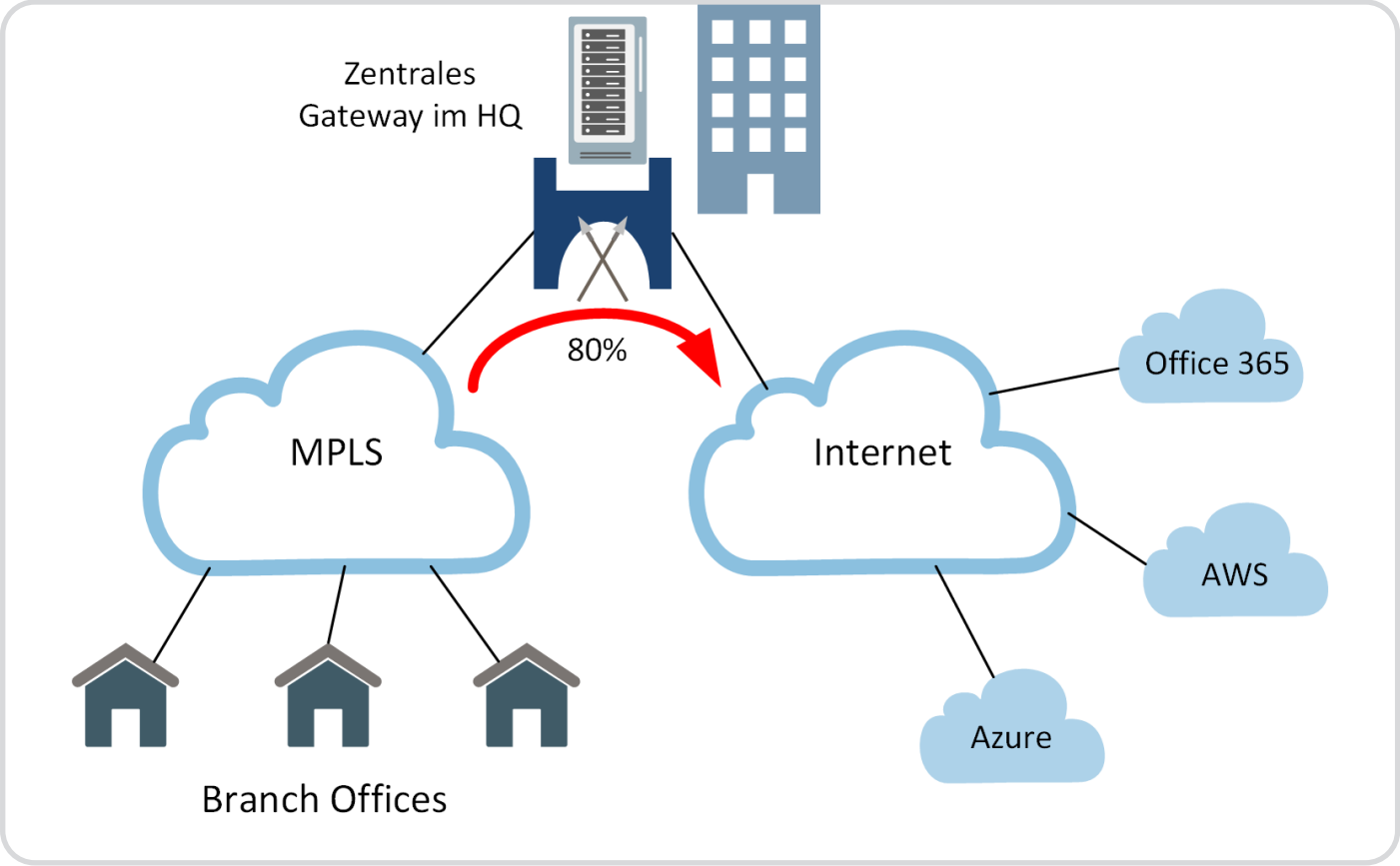

Bild 1: Ungünstige Verkehrsströme in klassischen WANs auf Grund der Nutzung von Cloud-Lösungen

Das Thema Internet of Things (IoT) befeuert zudem das Edge Computing, d. h. Rechenleistung muss dort bereitgestellt werden, wo sie benötigt wird, um die hohen Anforderungen bezüglich schneller IT-Verarbeitung abzubilden. Auch dieser Trend führt dazu, dass die klassischen Wide Area Network (WAN) Technologien, die meist aus Security-Gründen einen zentralen Übergang ins Internet vorsehen, nicht mehr genügen.

Sämtlichen Datenverkehr erst in die Zentrale oder zu einem Internet Break-out des Providers zu schicken, um von dort aus das Internet zu erreichen, führt in der Regel zu erhöhten Laufzeiten und einer verschlechterten Nutzererfahrung (Customer Experience), da auch die Bandbreiten für die Außenstellen aus Kostengründen meist stark limitiert sind. Diese als Backhaul-Ver-

kehr (engl. Rücktransport) bezeichneten Datenströme nehmen nicht selten einen Großteil des gesamten Datenverkehrs ein, da immer mehr Informationen in Richtung Internet fließen. Darüber hinaus leiden die klassischen WAN-Technologien wie Multiprotocol Label Switching (MPLS) oder Carrier Ethernet Services (CES) darunter, dass die Provider gerade in internationalen Projekten oft einigen Vorlauf benötigen, bevor sie Anbindungen bereitstellen können. Eine SD-WAN-Lösung, die jede beliebige Übertragungstechnologie und Anschlussvariante nutzen kann, ist hier deutlich im Vorteil. Durch die Einbindung von Mobilfunk-, Kabel- oder DSL-Verbindungen kann man der vom Business geforderten Agilität meist besser nachkommen.

SD-WAN-Architektur: Zentraler Controller, Underlay und Overlay

Eine SD-WAN-Architektur ist wie jede Software-Defined Networking-Technologie (SDN-Technologie) aus einem Underlay und einem Overlay aufgebaut. Beim Underlay-Netz handelt es sich um die physikalische Vernetzung der Lokationen über das WAN oder Internet, wobei jede beliebige Übertragungstechnologie eingesetzt werden kann. Dabei ist es wünschenswert, aber nicht notwendig, dass jede Lokation über wenigstens zwei Anschlüsse verfügt.

Auch wenn das Underlay beliebig wählbar ist, gilt es zu beachten, dass Funktionen wie Quality of Service (QoS) sowie ein guter Service und Support weiterhin von Vorteil sind. Zwar lassen sich im SD-WAN auch günstige Privatkundenanschlüsse verwenden. Fallen diese aber aus oder gibt es technische Probleme, kämpft man mit langen Entstörzeiten und Privatkunden-Hotlines.

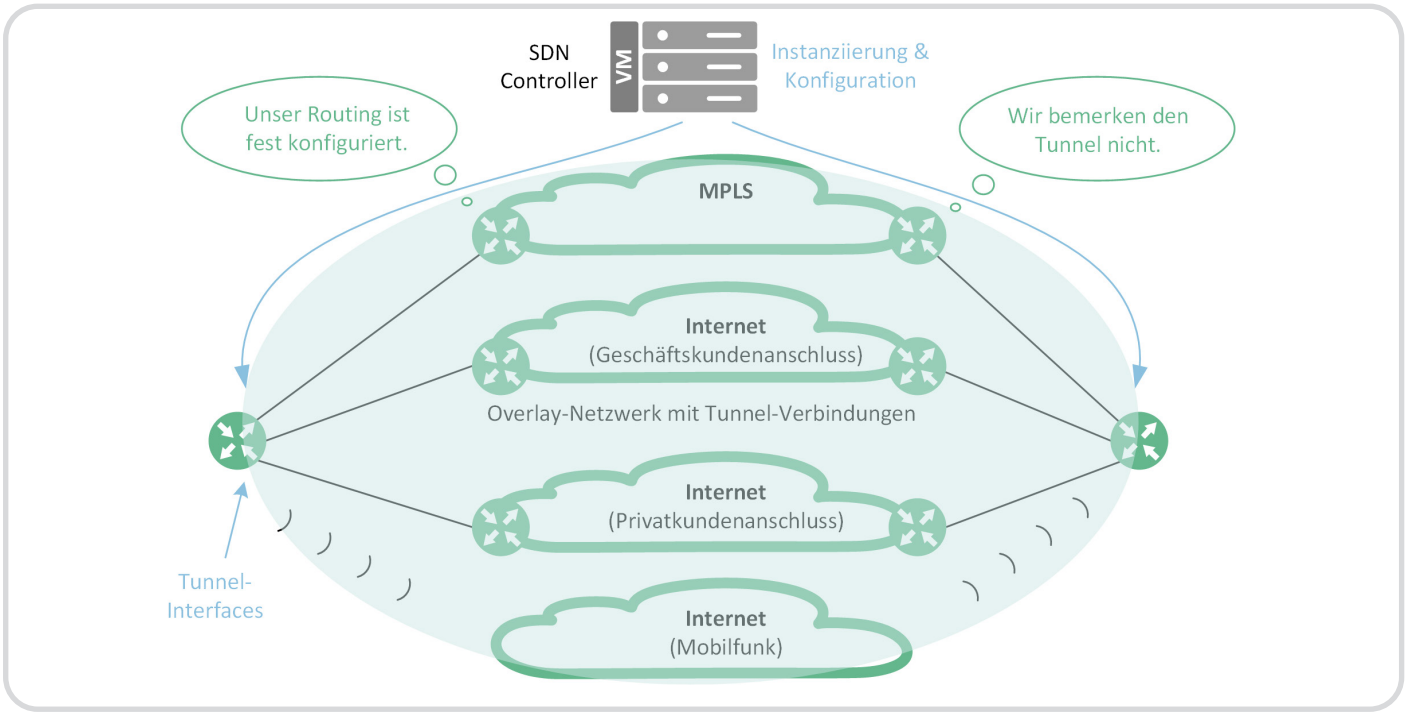

Bild 2: SD-WAN-Architektur: Beliebiges durch den Provider gestelltes Underlay. Overlay meist durch vom Controller veranlasste IPSec- oder GRE-Tunnel.

Das Overlay wird in der Regel mit IPSec- oder GRE-Tunneln gebildet, die meist einen verschlüsselten Datenaustausch mittels IPSec über das WAN gewährleisten. Eine Alternative hierzu bietet das Secure Vector Routing (SVR), welches via Network Address Translation (NAT) virtuelle Verbindungen schafft. All diesen Technologien ist es gemeinsam, dass sie logische Punkt-zu-Punkt-Verbindungen aufbauen, die bezüglich der Wegewahl unabhängig vom darunterliegenden Underlay sind.

Die Besonderheit, die allen SD-WAN-Lösungen gemeinsam ist, ist die Nutzung von Prefix-basierendem Destination-based IP Routing, welches in der Regel mittels applikationsspezifischem Routing realisiert wird. Klassische Router nutzen nur einen besten Weg und müssen über statische Regeln wie z. B. Policy-basiertes Routing gezwungen werden, für bestimmten Datenverkehr auch andere Wege zu nehmen.

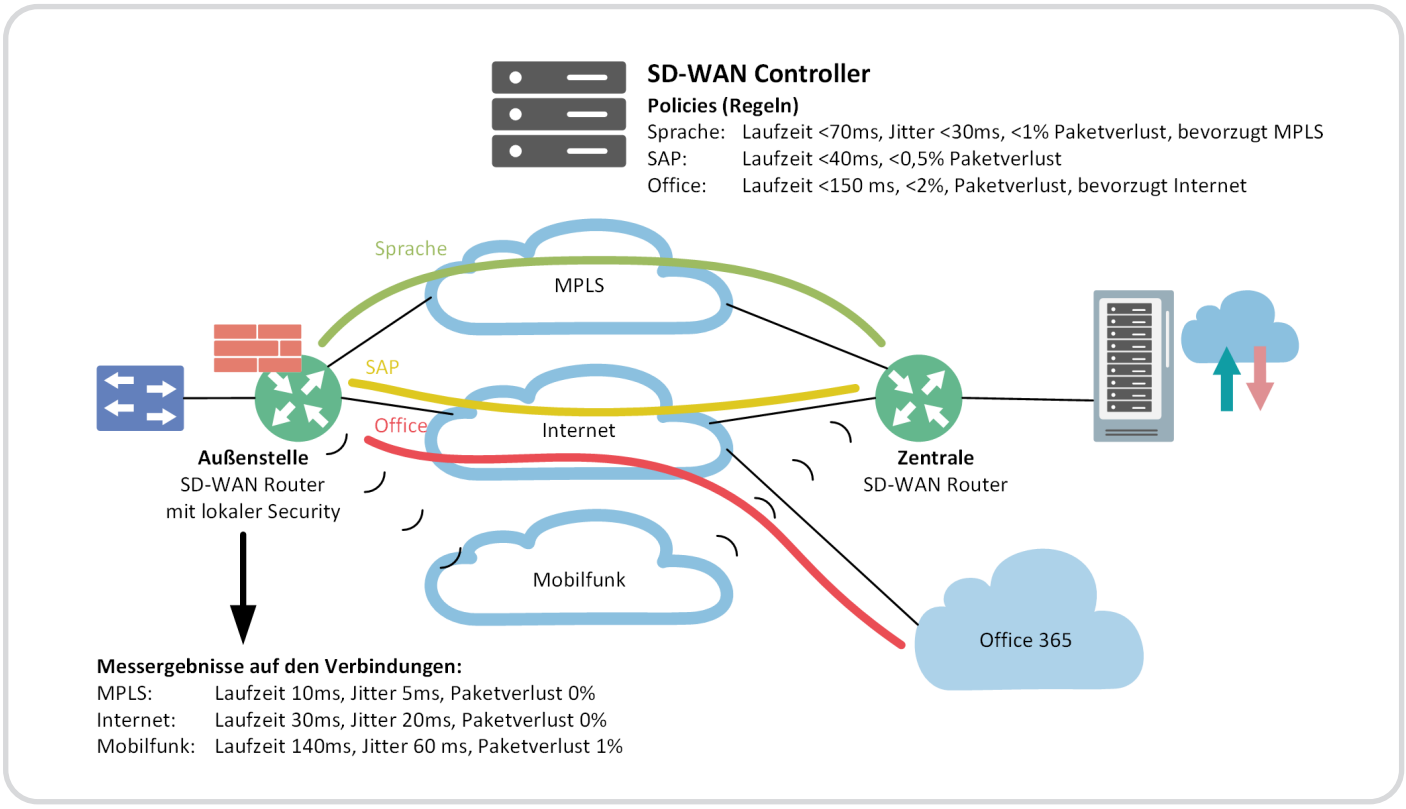

Bild 3: Routing-Entscheidung je Anwendung in Abhängigkeit von Quality of Service Policies und Messergebnissen

Hingegen bestimmen SD-WAN Router – die meist als Edge Router, Edge Devices oder Edge Appliances bezeichnet werden und Hardware Appliances oder x86-basierte Serversysteme darstellen – für jede Applikation dynamisch den besten Weg. Sie ermitteln hierzu mittels des Performance Monitorings die Quality of Service-Parameter (QoS-Parameter) Laufzeit (Latency), Laufzeitschwankungen (Jitter) und Paketverlustrate (Packet Loss) auf den verfügbaren Pfaden.

Kommt ein Datenpaket an, analysiert das Edge Device, um welche Applikation es sich handelt, und sucht nun die Policies (Regeln), die der Administrator für diese Anwendung hinterlegt hat. Der Administrator bedient sich zum Hinterlegen der Regeln des zentralen Controllers, der diese auf alle Edge Devices verteilt. Sie enthalten die einzuhaltenden Quality of Service-Parameter für eine Anwendung, die durch weitere Parameter wie z. B. die bevorzugte Verbindung (und damit die Übertragungstechnologie) ergänzt werden können.

Weitergehende Leistungsmerkmale

SD-WAN-Lösungen bieten neben dem Applikations-basierten Routing und der Auswertung der Quality of Service (QoS) Parameter eine Vielzahl weitergehender Leistungsmerkmale wie z. B.:

- Vereinfachte Administration und vereinfachtes Management: Einfache grafische Oberfläche, mit der man die komplette Lösung wie auch die Provider SLAs überwachen kann. Die Systeme finden sich selbstständig und bauen eine Topologie auf.
- Es lassen sich beliebige Übertragungstechnologien nutzen, was eine hohe Agilität und hohe Bandbreiten ermöglicht.
- Erleichterte Migration: Redundanzkonzepte sind teilweise automatisiert oder integriert, was Migrationen deutlich vereinfacht.
- Zero-Touch Provisioning (ZTP): Die Systeme in den Filialen können mittels einer Out-of-the-Box-Konfiguration vollautomatisiert bereitgestellt werden. Es wird nur eine IP-Konnektivität benötigt. Damit das Einbringen neuer Router trotzdem sicher ist, hinterlegen die Hersteller schon entsprechende Zertifikate auf den Komponenten.
- Optimierte Cloud-Konnektivität: Vollautomatisierte Bereitstellung von Cloud-Zugängen, z. B. über Azure Virtual WAN, AWS Transit Gateway oder das Google Cloud Network Connectivity Center oder optimierte Anbindung von SaaS-Anwendungen wie Microsoft Office 365. Die Cloud-Anbindung mittels SD-WAN bringt zahlreiche Vorteile im Vergleich zu klassischen IP VPN-Anschaltungen wie höhere Skalierbarkeit, höhere Visibilität etc.
- Next Generation Security: Oft sind in den SD-WAN Edge Devices Features enthalten wie standortübergreifende IPSec-VPN-Lösungen, eine integrierte Next-Generation Firewall (NGFW), Web Filtering, IPS und SSL-Inspektion.
- End-to-End Microsegmentation und Multiplexed VPN: Durch das Software Overlay lassen sich Lokationen wie auch Applikationen und Dienste beliebig voneinander via VPNs separieren.

- WAN Aggregation: Ein logisches Bonding (Aggregation) von über unterschiedliche Transportnetze führenden Tunnel-Verbindungen, um einen Link mit höherer Verfügbarkeit und Kapazität als die Einzelverbindungen zu schaffen.
- Path Optimization: Dies ist ein Mechanismus, um aus zwei oder mehr schlechten Verbindungen eine gute logische Übertragungsstrecke zu machen. Es werden hierfür Technologien wie Packet by Packet Rerouting oder das Versenden von dupliziertem Datenverkehr über zwei separate Wege genutzt, wobei der Ziel SD-WAN Router dann die doppelt ankommenden Daten nur einmal ausgibt.
- Forward Error Correction (FEC): Durch die Übertragung von Paritätsinformationen in sogenannten Schutzpakten können Bitfehler korrigiert und fehlerhafte Pakete wiederhergestellt werden.
- Application Optimization und WAN Acceleration: Übernahme von Aufgaben eines typischen WAN-Beschleunigers.
- VPN-based Key Rotation: Dynamische Verteilung und Erneuerung der IPSec Encryption Keys z. B. für PCI Compliance.
- Programmatic APIs: Zur Automatisierung und kundenspezifischen Anpassung der Lösung.
- Data Analytics: Die für jede Anwendung bestimmten QoS-Informationen können auch für das Troubleshooting, Design-Aspekte oder Anomaly Detection (Security) genutzt werden.
- Service Chaining: Flexibilität beim Abarbeiten von Data Flows, indem die auf das Datenpaket angewandten Funktionen und deren Reihenfolge applikationsbasiert angepasst werden können.
- Provider und Location Discovery: Optimierung von Troubleshooting und Konfiguration, indem Ort und Provider an dem die Edge Devices angeschlossen sind, exakt bestimmt werden.
- IPv6/IPv4 Dual Stack: Die meisten SD WAN-Lösungen unterstützen Dual Stack, sind also IPv4- und IPv6-fähig.

Security-Konzepte bei SD-WAN

Die Security spielt bei SD-WAN immer eine Hauptrolle. Es gibt zwei verschiedene Ausprägungen des Security-Themas. Zum einen müssen die Daten sicher übertragen werden, was man durch eine IPSec-Verschlüsselung erreicht. Zum anderen führt der Direct Internet Access (DIA) dazu, dass man auch die Außenstellen absichern muss. Letzteres ist ein ganz wesentlicher Aspekt, da dies sowohl technische Auswirkungen auf die Gestaltung der IT-Security-Lösung hat als auch finanziell stark zu Buche schlägt.

Die Außenstellen durch eine erhöhte lokale Security zu schützen, ist bezüglich der unmittelbar anfallenden Kosten die preiswertere Variante. Ob dieser Schutz als ausreichend angesehen werden kann, hängt sehr stark davon ab, für welchen Datenverkehr man diesen benötigt. So macht es einen großen Unterschied, ob man vielleicht nur einen lokalen Break-out für Office 365 und ein Gäste-WLAN benötigt oder ob mit den Firmenrechnern alle Dienste im Internet erreichbar sein sollen.

Im Falle, dass man nur den Datenverkehr für Microsoft Office 365 und das Gäste-WLAN ins Internet transportieren möchte, vertrauen viele Unternehmen auf eine relativ einfache und damit kostengünstige Security-Lösung. Da Office 365 schon einiges an Security-Funktionen mitbringt und sich dieser Standardschutz weiter erhöhen lässt, setzen viele Organisationen nur einen Router oder eine Firewall als Filter ein, so dass nur Office 365 Datenverkehr von speziellen IP-Adressen ins Netz darf, sofern zuvor eine Verbindung von innen, also aus der Zweigstelle, nach außen – also in die Office Cloud – aufgebaut wurde.

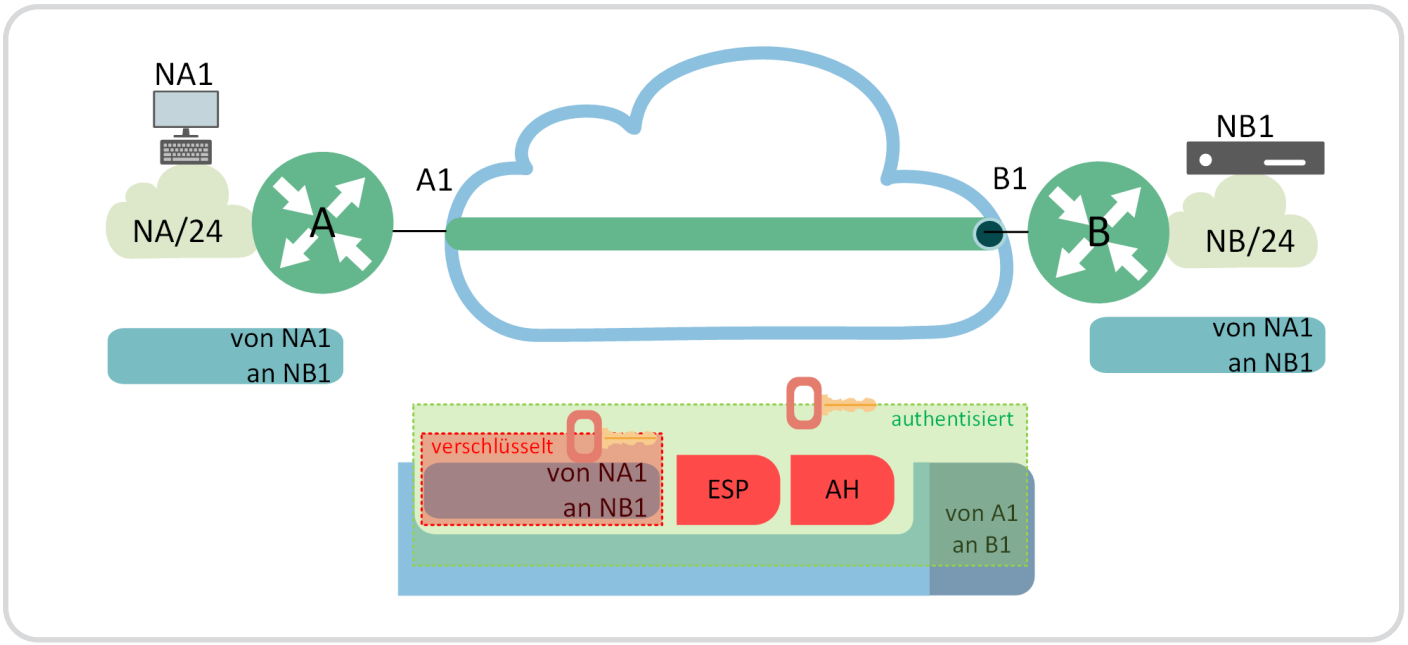

Bild 4: Eine mit IPSec verschlüsselte Übertragungsstrecke im SD-WAN

Das Gäste-WLAN separiert man logisch vom restlichen Netz und stellt sicher, dass nur Verbindungen von innen nach außen aufgebaut werden dürfen. Die Verantwortung für die Endgerätesicherheit legt man in die Hände des Gastes. Damit wäre für ein solches Szenario schon ein hohes Schutzniveau erreicht. Man riskiert nur, dass Schadcode, der Office 365 befallen hat, dann auch ins Netz gelangen könnte. Bisher gilt Microsoft Office 365 allerdings diesbezüglich als sehr sicher, insbesondere, wenn man sich der von Microsoft optional bereitgestellten Security-Lösungen bedient.

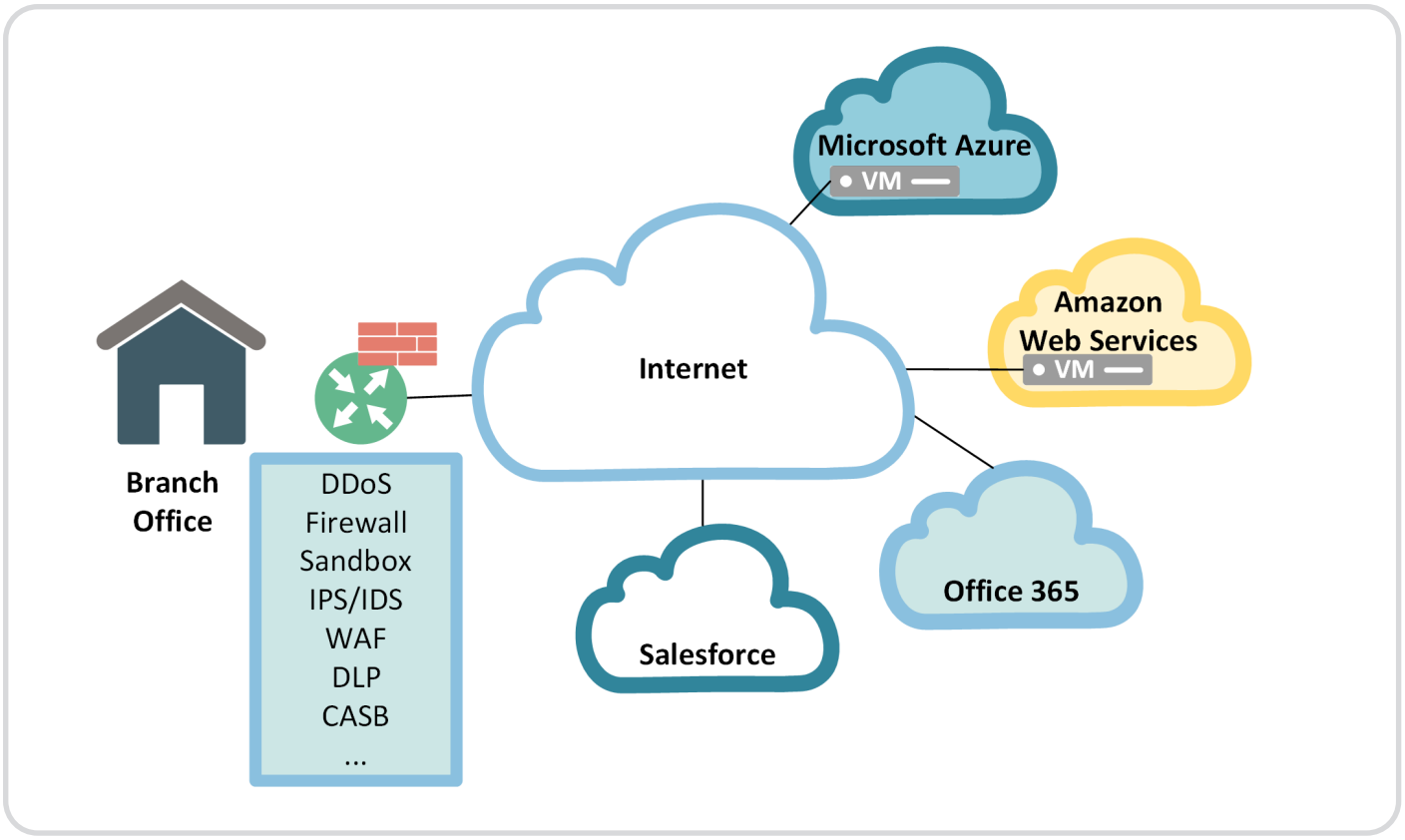

Bild 5: Bereitstellung einer lokalen Security in der Außenstelle

Anders sieht es aus, wenn die Mitarbeiter in der Außenstelle auch direkt ins Internet gehen sollen. Hier entsteht plötzlich eine Vielzahl potenzieller Angriffsvektoren und man muss die Außenstelle deutlich mit Schutzmaßnahmen aufrüsten, um nicht ein leichtes Einfallstor für Hacker zu schaffen. So setzt man am Perimeter heute standardmäßig Technologien wie einen Distributed Denial of Service-Schutz (DDoS-Schutz), Firewalling, Sandboxing, Intrusion Prevention System/Intrusion Detection System (IPS/IDS), Web Application Firewalling (WAF) mit URL Filtering, Data Loss Prevention (DLP), Cloud Access Security Broker (CASB) etc. ein.

Auch wenn sich so eine hohe lokale Security erreichen lässt, wird man in der Regel nicht das Schutzniveau erreichen, das mit einer Secure Access Service Edge-Lösung (SASE-Lösung) erzielbar ist. Sie schützt in der Regel deutlich besser vor Zero Day Attacks, ist dafür aber auch kostenintensiver.

GARTNER: “DMZs and legacy VPNs were designed for the networks of the 1990s and have become obsolete because they lack the agility needed to protect digital businesses.”

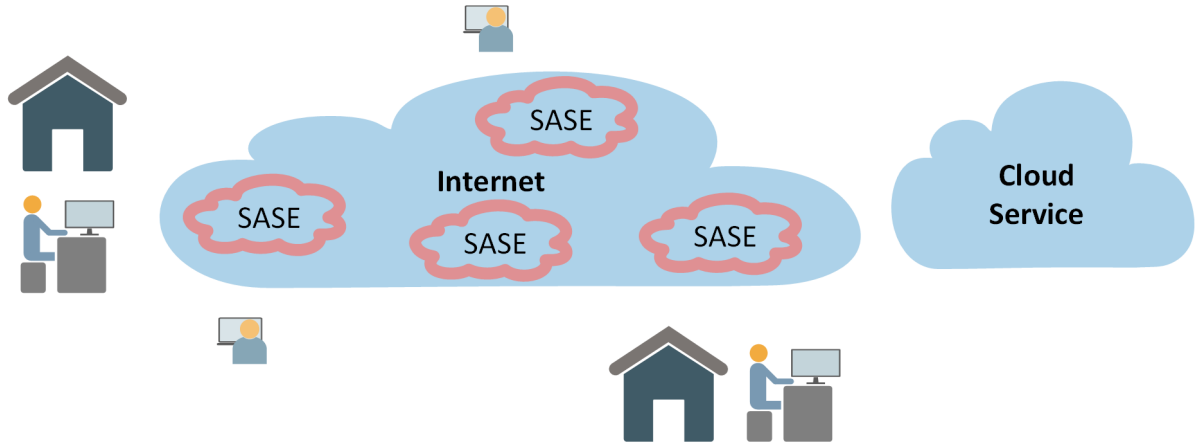

Bild 6: Den Cloud-basierten Secure Access Service Edge-Lösungen (SASE-Lösungen) gehört die Zukunft.

Schon 2016 sagte Gartner das Ende der klassischen Perimeter Security und VPN-Konstrukte voraus. Aufgrund der zunehmenden Dezentralisierung der IT, die durch die Cloud-Nutzung, Edge Computing sowie die zunehmenden Heimarbeitsplätze und mobilen Mitarbeiter forciert wurde, ist die Prognose, dass auch die Security-Lösungen in die Cloud wandern. Die Antwort auf diese neuen Anforderungen nannte Gartner Secure Access Service Edge (SASE). SASE beschreibt ein Cloud-Architekturmodell, welches Netzwerk- und Security as a Service-Funktionen vereint und diese als Cloud-Dienst zur Verfügung stellt.

SASE-Lösungen konsolidieren zahlreiche Netzwerk- und Sicherheitsfunktionen in einer Cloud-Plattform und bieten dem Nutzer viele Vorteile wie:

- Vereinfachung und Kostenersparnis – Keine eigene Security Hardware erforderlich und höhere Effizienz des Security-Teams
- Konsistentes Regelwerk
- Zusätzliches Know-how
- Schnelle Reaktion auf neuartige Bedrohungen
- Latenz- und Policy-optimiertes Routing
- Sichere Remote-Zugriffe
- Rollen-basierter Zugang anhand von Nutzer-, Geräte- und Anwendungsidentität oder Einsatzort

Die Umsetzung von SASE-Lösungen ist je nach Anbieter unterschiedlich. Es gibt jedoch einige wesentliche Security-Bestandteile, welche jede SASE-Lösung mitbringen sollte. Zu diesen gehören:

- SD-WAN
- Secure Web Gateway (SWG)
- Firewall as a Service (FWaaS)
- Cloud Access Security Broker (CASB)
- Zero Trust Network Access (ZTNA)

SASE-Lösungen sprießen gerade wie Pilze aus dem Boden. Nahezu jeder namhafte Hersteller von ganzheitlichen IT-Security-Lösungen bietet seinen Kunden diese moderne Cloud-basierte Security an. Dass die Kunden in ihrem Adaptionsverhalten etwas langsamer sind, ist vor allem darin begründet, dass eine lokale Security-Lösung weniger direkte Ausgaben erfordert und man auch nicht gänzlich auf eine lokale Security verzichten möchte.

Es erhärtet sich aber zusehends der Trend, dass SASE ein wichtiger Teil der Standardlösung zur Absicherung der Unternehmensnetze in den kommenden Jahren werden wird. Denn diese Lösungen sind besonders leistungsfähig und schützen insbesondere vor Zero Day Attacks deutlich besser als lokale Architekturen. Besonders sicherheitsbewusste Organisationen werden zudem eine leistungsstarke lokale Security in den Außenstellen einsetzen und somit eine Defense in Depth-Strategie nutzen.

Erhöhte Kosten durch SD-WAN

Oft wird das Thema SD-WAN unter dem Gesichtspunkt von möglichen Einsparungen gesehen, wobei stets die Optimierung der Übertragungskosten im Zentrum der Überlegungen steht. Diese lassen sich in vielen Fällen auch etwas reduzieren. Nicht selten stehen diesen Einsparungen aber erhöhte Kosten bei den SD-WAN Gateways gegenüber, die entweder neu angeschafft oder bei vorhandenen SD-WAN-fähigen Edge Devices auf Grund des verschlüsselten Overlays mehr Performance bringen müssen, was oftmals eine Hardware-Erneuerung erfordert.

Zudem wird für die erforderliche Intelligenz oft eine höhere Lizenzstufe benötigt. Addiert man dann noch die Kosten für die lokale Security wie auch die zentrale SD-WAN-Lösung, so stellt man in der Regel fest, dass die neue Lösung spürbar teurer ist als die alte. Generell kann man sagen, dass eine SD-WAN-Lösung deutlich teurer sein wird als eine klassische WAN-Lösung, die dem SD-WAN auch als Underlay dient. Ausnahmen lassen sich fast nur in internationalen Projekten finden, wenn durch SD-WAN überhöht teure MPLS-Verbindungen abgelöst werden können.

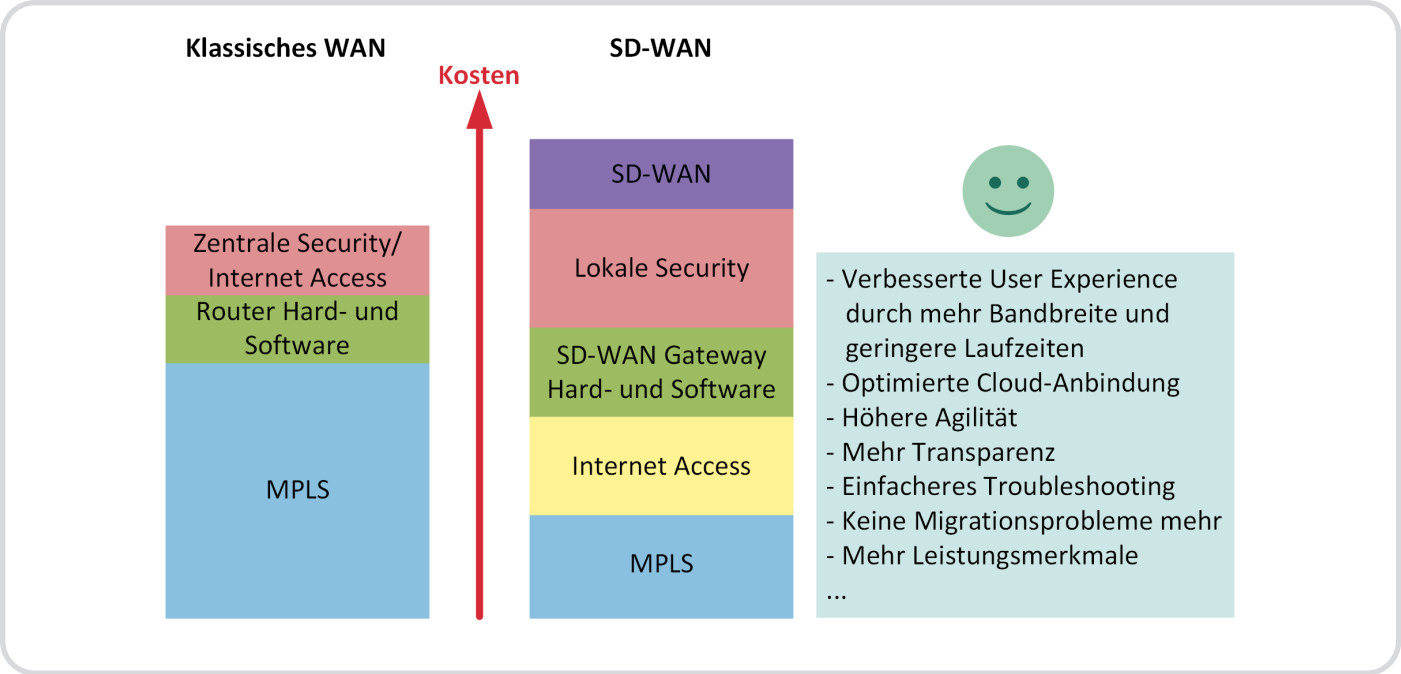

Bild 7: Typischer Kostenvergleich einer klassischen WAN- mit einer SD-WAN-Lösung

Grenzen des SD-WANs

Die Skalierbarkeit von SD-WAN-Lösungen ist bei vielen Herstellern eingeschränkt. Da im SD-WAN Overlay meist IPSec oder GRE Tunnel genutzt werden, um Punkt-zu-Punkt-Verbindungen aufzubauen, lässt sich eine Vollvermaschung in großen Netzen oft nicht mehr umsetzen. Eine Vollvermaschung ist aber gerade für Peer-to-Peer-Anwendungen wie Voice over IP wünschenswert, wo eine direkte Telefonverbindung von Außenstelle zu Außenstelle den Idealzustand darstellt.

Zugleich wirkt sich der zusätzliche Tunnel Overhead bei der Sprachübertragung besonders negativ aus. Aber auch in kleineren Netzen wird man von einer Any-to-Any-Konnektivität Abstand nehmen, da man beim Einsatz vieler Tunnel Interfaces entsprechend leistungsfähige Hardware auch in den kleinen Außenstellen benötigt. Viele Hersteller bieten daher an, dynamische Bedarfstunnel aufzubauen. Dies ist jedoch weniger komfortabel und performant wie eine Vollvermaschung via klassischer WAN-Technologie. Zudem sind die Bandbreiten im SD-WAN begrenzt. Zwar gib es die ersten 100 Gigabit-Schnittstellen, auslasten kann diese aber bisher keiner der führenden Anbieter. Denn das Performance Routing braucht sehr viel Rechenleistung, was auch einer der Hauptgründe ist, warum man das Applikations-basierte Routing nicht schon früher genutzt hat. Es ist ressourcensparender, eine Routing-Tabelle für alle Anwendungen zu betreiben, als für jede Anwendung Informationen vorzuhalten und spezifische Entschei-

dungen zu treffen. Die Tunnel Interfaces und die Verschlüsselung fressen zudem Hardware-Ressourcen und führen zu zusätzlichem Übertragungs-Overhead, was sich insbesondere bei Leitungen mit geringen Bandbreiten negativ auswirkt.

Immer dann wenn der Kunde Ende-zu-Ende verschlüsseln muss, ergibt sich für den Provider auch die Herausforderung, dass er nicht mehr erkennen kann, welche Applikation der Kunde transportiert. Damit tut sich der Service Provider schwer, eine SD-WAN-Lösung zu betreiben. Hierfür gibt es Workarounds, wie z. B. das Mapping von Differentiated Services Code Point (DSCP) Bits auf den äußeren IP Header oder eine Ent- und Verschlüsselung auf dem SD-WAN Edge Device, aber auch diese Lösungen schränken ein und erzeugen zusätzlichen Aufwand. Zudem gibt es heute noch keine Standardisierung der SD-WAN-Technologie, so dass man sich idealerweise auf einen Hersteller festlegt.

Setzt man zwei Hersteller ein oder soll der Anbieter gewechselt werden, entstehen Silos, die separat zu administrieren sind. Da die Hersteller nun auch noch die Software-Defined Networking-Technologien (SDN-Technologien) für LAN, WAN und Data Center verknüpfen, wird die Notwendigkeit durchgängiger Lösungen weiter gestärkt. Gerade bei Firmenakquisitionen ergibt sich zunehmend die Herausforderung, dass die daran beteiligten Unternehmen unterschiedliche SD-WAN-Technologien im Einsatz haben.

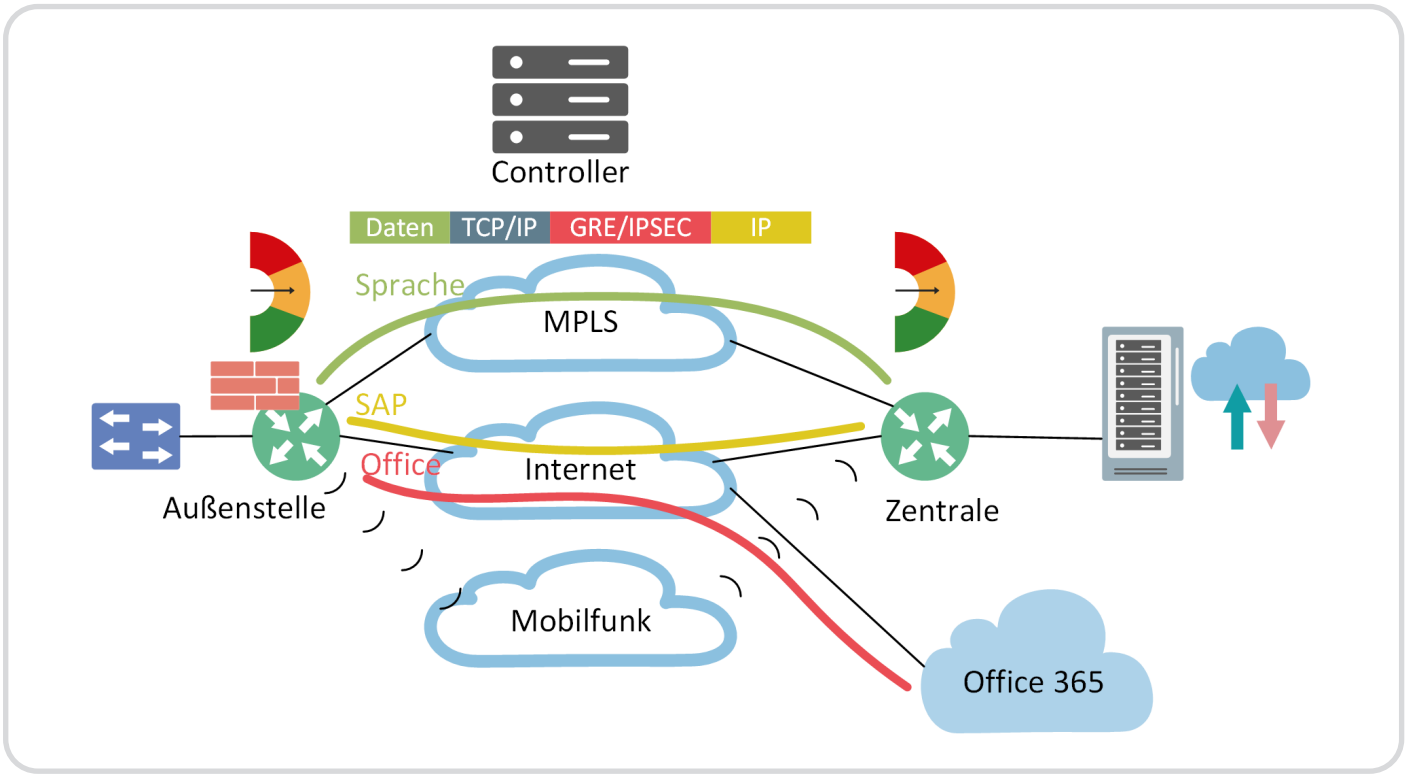

Bild 8: Overhead durch Applikations-basiertes Routing und das Tunneling der Pakete

Resümee

SD-WAN ist eine sehr zukunftsträchtige Technologie, welche die klassischen WAN-Architekturen Zug um Zug ablösen wird. Das Applikations-basierte Routing bringt viele Vorteile. Es erweist sich gerade bei der Nutzung von Cloud Services, Internet of Things und Edge Computing sowie für international tätige Unternehmen – auch wegen der dadurch erreichbaren Flexibilität und Agilität – von großem Vorteil.

Mit der Entscheidung für SD-WAN wird unmittelbar die Frage nach der passenden Security-Strategie aufgeworfen. Schränkt man den Direct Internet Access (DIA) für die Außenstellen stark ein oder nutzt man lokale Security und/oder Secure Access Service Edge (SASE)?
Wer sich für SD-WAN entscheidet, muss normalerweise tiefer in die Tasche greifen, kauft sich damit aber oftmals viele Vorteile ein. Die Hersteller entwickeln die SD-WAN-Technologie mit hoher Priorität weiter, so dass Kunden von vielen neuen Features profitieren können, während im WAN neue Leistungsmerkmale eher selten sind.

Da die Hersteller immer stärker danach streben, ihre Software-Defined Networking-Lösungen (SDN-Lösungen) in LAN und Data Center mit dem SD-WAN zu verknüpfen, empfiehlt es sich, eine homogene Netzwerkinfrastruktur-Lösung von einem Anbieter anzustreben und für LAN, WAN und Data Center eine möglichst durchgängige Lösung zu schaffen.

Trotz seiner vielen Vorteile ist SD-WAN nicht für jeden Kunden gleichermaßen geeignet. Wer keine Multi-Cloud-Strategie hat und vieles noch selbst abbildet – wie dies z. B. im Public Sector häufig der Fall ist – wird von SD-WAN nicht sehr profitieren. Gerade für die Telefonie sind die klassischen vollvermaschten Netzwerke ideal. Auch die Nutzung von Microsoft Office 365 rechtfertigt unter Abwägung aller Vor- und Nachteile meist noch keine SD-WAN-Lösung.

So lässt sich auch in klassischen WANs eine gute Anbindung erreichen. Organisationen, die vor allem national agieren und ein sehr statisches WAN haben, das wenige Änderungen erfährt, werden in der Regel nicht so sehr von SD-WAN profitieren. Daher sollte in diesen Fällen stets geprüft werden, ob die Vorteile von SD-WAN die zusätzlichen Ausgaben rechtfertigen. Nichtsdestotrotz muss man feststellen, dass die Zukunft der SD-WAN-Technologie gehört!

Haben Sie eine Frage zur Thematik? Gerne können Sie uns hierzu kontaktieren:

06074 48680 • kontakt@experteach.de

05.10.2021