

DIE WAHRHEIT ÜBER
SD-WAN

Überlegungen und Erfahrungen

becom Systemhaus GmbH & Co KG
05/2021



EINFÜHRUNG

WAS IST SD-WAN?

SD-WAN (Software Defined Wide Area Network) Lösungen bieten Ersatz für herkömmliche Formen der Standortvernetzung und sind völlig unabhängig von den eingesetzten WAN Transporttechnologien. SD-WAN bietet eine dynamische, richtlinienbasierte und anwendungsbezogene Pfadauswahl über mehrere WAN-Verbindungen und unterstützt hierbei Services für zusätzliche Dienste wie WAN Optimierung und Security. Dazu bietet SD-WAN eine vereinfachte, zentrale Orchestrierung und nativ implementierte Verschlüsselung .

SD-WAN adressiert drei grundlegende Anforderungen für WAN-Netzwerke:

- Erstkonfiguration und Deployment
- Geschwindigkeit und Zuverlässigkeit
- Sichtbarkeit und Kontrolle des Netzwerks

SD-WAN verspricht eine Verbesserung der WAN-Leistung und die Vereinfachung der Verwaltung durch Software und Automatisierung.

SD-WAN ist die Weiterentwicklung von Technologien, die es alle schon vor dem eigentlichen Begriff gab. Aber zusammengefasst und als einheitliche Architektur definiert, agieren diese Technologien effizienter und einfacher um die versprochenen Vorteile von SD-WAN in die Tat umzusetzen.

Die Einführung von SD-WAN im Unternehmen ist keine einfache Aufgabe. Es gibt dabei mehrere grundlegende Herausforderungen, die Unternehmen beachten müssen.

IDC

Der Markt für SD-WAN wird voraussichtlich mit 30,8 % durchschnittlicher jährlicher Wachstumsrate von 2018 bis 2023 auf einen Umsatz von 5,25 Milliarden US-Dollar wachsen.

Viele Unternehmen versuchen aktuell die Einführung von Cloud-Anwendungen zu beschleunigen und ihre Netzwerkinfrastruktur effizienter und zuverlässiger zu gestalten.

SD-WAN-Anbieter reiten auf dieser Wachstumswelle



HERAUSFORDERUNGEN DER IMPLEMENTIERUNG



Die Problemstellung und das Änderungs- Management werden oft unterschätzt

SD-WAN-Lösungen sind (noch) nicht selbstlernend und erfordern einen Benutzer, der definiert, welcher Verkehr im Netzwerk erlaubt ist und wie wichtig dieser Datenverkehr ist. Eine mögliche Option in der Konfiguration ist, allen Datenverkehr mit gleicher Priorität zu versehen und es der SD-WAN-Software zu überlassen die Last über die verfügbaren Bandbreiten zu verteilen.

Das kann durchaus genügen, wenn Sie nur eine oder zwei wichtige Anwendungen in Ihrem Netzwerk haben.

Für die Mehrheit der Unternehmen, die eine Vielzahl von Anwendungen haben, die einwandfrei funktionieren müssen, wird diese Strategie jedoch zu kurz greifen.

Da Unternehmensprozesse heutzutage schnellen Transformationen unterworfen sind, wird jede Planung, die Sie zu Beginn des Projekts vornehmen, schon während der Implementierungsphase erhebliche Änderungen erfahren. Dies kann zu Kosten- und Zeitüberschreitungen führen und sollte in jedem Fall bedacht werden.

Administratoren müssen Zeit investieren um zu analysieren, welche Ressourcen und Bandbreiten kritische Anwendungen tatsächlich benötigen und sollten dann hiervon ausgehend entsprechende Richtlinien und Schwellenwerte definieren.

FALSCHERWARTUNGEN

KOSTENEINSPARUNGEN UND DIE MÖGLICHKEITEN VOR ORT

Die Verfügbarkeit von kostengünstigen und breitbandigen WAN Anschlüssen an allen Ihren Geschäftsstandorten ist, gerade in Deutschland, in der Regel eine Illusion.

Einer der Gründe, warum SD-WAN als Alternative zu teureren MPLS-Netzwerken gesehen wird, ist die Tatsache, dass Sie mehrere kostengünstige Verbindungen gleichzeitig nutzen können, die eine gleiche oder bessere Leistung und Zuverlässigkeit als ein MPLS-Netzwerk bieten.

Für die Konnektivität über Glasfaser verfügen Sie im besten Fall über einen einzigen örtlichen Anbieter und auch für (V)DSL ist in der Regel der etablierte Ortsnetzbetreiber zuständig. Weitergehende Optionen für zusätzliche Kapazität und Redundanz können dann nur noch über nicht terrestrische Verbindungen realisiert werden. Diese Verbindungen sind jedoch oft mit hohen Kosten oder begrenztem Volumen verbunden und kommen somit vor allem als Backup in Betracht.

Wenn Sie die TCO (Total Cost of Ownership) betrachten, werden Sie feststellen, dass in vielen Fällen eine Migration zu SD-WAN eher ein kostenneutrales Upgrade als eine Kosteneinsparung ist – immer abhängig davon, wie hoch Ihre Bandbreitenanforderungen sind und in welchen Ländern Sie operieren.

Auch die Kosten und der Aufwand, die mit der Verwaltung mehrerer Breitbandanbieter an jedem Ihrer Standorte einher gehen, werden in der Regel unterschätzt.



Das Zusammenspiel mit der bestehenden Infrastruktur kann sehr komplex werden

Die meisten SD-WAN-Implementierungen werden parallel oder zusätzlich realisiert. Das bedeutet, dass die SD-WAN-Technologie zur bestehenden Netzwerkinfrastruktur hinzugefügt wird und dort eine oder mehrere Funktionalitäten in dieser Umgebung ersetzt. Diese Implementierungen nutzen Komponenten der alten Infrastruktur, einschließlich der Konnektivität, der Rechenzentren, Firewalls und Switches. Dies erfordert, dass die Administratoren in der Lage sein müssen, alle Herausforderungen des Zusammenspiels der Komponenten für das geplante SD-WAN Deployment genauestens zu identifizieren.

Wenn die SD-WAN-Lösung zum Beispiel ein bestehendes MPLS Netzwerk enthält ist es wahrscheinlich, dass Sie die Mitwirkung des MPLS Anbieters bei der Implementierung benötigen. Dies kann sich natürlich schwierig gestalten, wenn Sie SD-WAN einsetzen wollen, um zukünftig gänzlich auf die teure MPLS-Lösung verzichten zu können.

Obwohl all diese Herausforderungen die SD-WAN-Implementierung entmutigen können, sind die Hürden überwindbar, wenn Sie gut planen und sich realistische Ziele für die Implementierung setzen.

DESIGN UND ROLLOUT

Alle SD-WAN-Plattformen werden in der Regel mit einer webbasierten Konfigurationssoftware ausgeliefert, die es Netzwerk Administratoren ermöglicht, Richtlinien zu erstellen, welche dann auf das Netzwerk und die einzelnen Geräte angewendet werden.

Das ist ein großer technologischer Schritt, da man bislang noch über ein umfassendes Know-how über diverse Router und Switch CLI (Command Line Interface) verfügen musste, um ein Netzwerk zu erstellen und zu pflegen.

SD-WAN-Orchestrierungssoftware, ob Cloud-basiert oder on-premise, folgt einem gemeinsamen Schema:

- Erstellen von Vorlagen mit Verwaltungs- und Geräteinformationen, Regeln für den Datenverkehr und ggf. Sicherheitsrichtlinien.
- Anstelle der Konfiguration eines Geräts mit einem Konfigurationskript, wird einfach eine Vorlage angewendet mit gerätespezifischen Variablen und dem Gerät zugewiesen.



Wenn Sie jetzt sagen: "Das ist doch kein Zero Touch Deployment!" haben Sie Recht. SD-WAN-Plattformen bewerben mittlerweile Zero-Touch als Alleinstellungsmerkmal nicht mehr so sehr wie noch vor einiger Zeit. In der Realität erfordert SD-WAN zwar potenziell weniger manuelle Eingriffe als herkömmliche Netzwerk-Systeme, aber dennoch ist die anfängliche Einrichtung und Konfiguration von Richtlinien sowie die Herstellung der Interoperabilität mit der bestehenden Netzwerk Infrastruktur erforderlich.

Die SD-WAN Vorlagen vermeiden jedoch viele Fallstricke manueller Verwaltungen und sind eindeutig als Vorteil zu sehen.

- Mühsamer Aufwand zum Erlernen und Erstellen der CLI Konfigurationssyntax
- Großes Plattform-Knowhow erforderlich
- Hohe Fehlerquote
- Arbeitsintensiv in der Anwendung
- Die Aufrechterhaltung der Konsistenz laufender Konfigurationen ist schwierig
- Bei jeder Änderung, müssen die Vorlagen angepasst werden
- Änderungen werden während des Update Prozess nicht oder nur unvollständig übertragen
- Nicht jede Änderung ist mit jedem Gerät bzw. dessen Softwarestand kompatibel

NETZWERK KONFIGURATION

GESTERN UND HEUTE

CLI

- Identifizieren der notwendigen Ports, Protokolle und externen Hosts für die Anwendungen
- Erstellen einer Policy, um den Verkehr von internen Hosts zu den neuen externen Hosts zu erlauben mit allen notwendigen Ports und Protokollen
- Ausführen eines Batch Jobs mittels eines SSH-Skripting Tool (Secure Shell) , um die Änderung in die Routerkonfiguration zu schreiben, basierend auf einer aktuellen Geräteinventur
- Den Batch-Prozess so lange erneut ausführen, bis alle Geräte aktualisiert sind – ggf. sind auch noch manuelle Updates durchzuführen
- Aktualisieren aller Staging- oder Konfigurationsvorlagen
- Möglicherweise gleicher Vorgang für die Firewalls an den Standorten.

Was man nie vergessen darf bei Vorgängen dieser Art ist die Tatsache, dass man sich auch schnell mal einen "Ast absägen" kann, sprich durch falsche Konfiguration einen Standort vom Netz trennt.

Der Aufwand ist bei SD-WAN deutlich geringer und somit auch die Fehlerquote.

Sie benötigen natürlich immer noch fundiertes Wissen und Erfahrung, um Ihre Idealvorstellung für Sicherheit und Performance umzusetzen. Die neuen Tools reduzieren aber die Zeit für die Implementierung von Änderungen.

Beispiel: Sie haben ein Unternehmensnetzwerk mit 100 Standorten. Jeder Standort ist mit einem Router und einer Firewall versehen. Ihr Unternehmen migriert nun Software in die Cloud. Um dies umzusetzen, müssen Sie die Konfiguration all Ihrer Router und Firewalls anpassen, um einen reibungslosen Übergang zum neuen Service zu gewährleisten. Möglicherweise haben Sie Geräte unterschiedlicher Hersteller im Einsatz, was den Aufwand erheblich steigert.

SD-WAN

- Erstellen Sie eine neue Policy im SD-WAN Template, welches Sie ändern möchten
- Wählen Sie ERP Vorlage oder erstellen Sie eine
- Legen Sie die Parameter für den Traffic fest (interne vertrauenswürdige Hosts und Traffic Policy)
- Speichern Sie die Vorlage und wenden Sie diese dann auf Geräte (nach Gruppe oder Global) an



DAS SPANNUNGSDREIEICK

LEISTUNG, AUSFALLSICHERHEIT, KOSTEN

Gründe für die Einführung von SD-WAN sind der Bedarf an bandbreitenintensiven Applikationen, die Nutzung von Collaboration Tools und die Einführung von Cloud Technologien wie z.B. SaaS, PaaS etc..

Das große Versprechen von SD-WAN ist, dass Unternehmen zukünftig kostengünstigere Konnektivität nutzen können und damit eine bessere Zuverlässigkeit und Leistung als mit herkömmlichen WAN Anschlüssen oder MPLS-Netzwerken erzielen.

Während dies für einige Standorte zutreffen mag, stehen an abgelegenen oder schwer zugänglichen Lokationen möglicherweise überhaupt keine kostengünstigen High-Speed-Internet Zugänge zur Verfügung.

SD-WAN ist zwar in der Lage, einige der Probleme zu überwinden, die mit suboptimaler Konnektivität verbunden sind, trotzdem unterliegt Ihr SD-WAN-Netzwerk natürlich den physikalischen Gesetzen in Bezug auf den Durchsatz und die Latenz des darunter liegenden Netzwerks.

DIE STRATEGIE IHRER KONNEKTIVITÄT IST FUNDAMENTAL WICHTIG!

Bei der Prüfung Ihrer SD-WAN-Optionen sollte das darunterliegende Netzwerk bewertet werden, auf dem die SD-WAN-Plattform aufsetzt.

Typischerweise können Sie eine der folgenden Optionen basierend auf der Verfügbarkeit und Ihren Anforderungen wählen:

Hybrid - mit MPLS primär und einem Breitband-Backup

Primärer Zugang über Glasfaser mit einem Breitband- Backup

Primärer Zugang über Glasfaser mit LTE Backup

Duale Breitband Anschlüsse (DSL)

Einfacher Breitband Anschluss (DSL) mit LTE Backup

Optionen nach Kosten geordnet.



WEITERE ASPEKTE

- BEDEUTUNG UND GRÖSSE DES STANDORTS
- VERFÜGBARE KONNEKTIVITÄTSOPTIONEN

Wenn Sie sich zum Beispiel in Gegenden mit großen Bürogebäuden befinden, ist höchst wahrscheinlich auch Internet mit hohen Bandbreiten verfügbar.

Wenn Sie sich hingegen in abgelegenen Standorten befinden, können erhebliche Kosten für den Ausbau einer breitbandigen Internetverbindung entstehen. Das Gleiche gilt für die Verfügbarkeit von zwei Breitbandanschlüssen oder mehr am selben Standort. Mit der kontinuierlichen Verbesserung der Mobilfunknetze stellen viele Kunden mittlerweile fest, dass deren Geschwindigkeit und Zuverlässigkeit gleichwertig oder sogar besser ist als eine sekundäre drahtgebundene Anbindung. Dies hat zusätzlich den Vorteil, dass ein Bagger nicht beide Verbindungen gleichzeitig zerstören kann. Jede Branche hat andere Bedarfe bei der Konnektivität. Ein bewährter Ansatz für Einzelhändler ist der einer primären Breitbandanbindung in Kombination mit einem Mobilfunk Backup. Oder sogar eine duale Mobilfunkanbindung. Dieser Ansatz funktioniert in solch wettbewerbsintensiven Branchen sehr gut, weil er relativ kostengünstig und im Allgemeinen zuverlässig ist. Damit sind die Anforderungen eines typischen Einzelhandelsgeschäfts praktisch schon erfüllt.

Für Nicht-Einzelhandelsbranchen, in denen selbst wenige Sekunden Ausfallzeit eine erhebliche Geschäftsunterbrechung und einen Umsatzverlust bedeuten, kann sich ein hybrides Breitband Netzwerk in Kombination mit Glasfaser, (V)DSL und/oder Kabel Internet und Mobilfunk an jedem Standort lohnen. Diese Anschlüsse werden dann per SD-WAN hochverfügbar gebündelt.



Abwägen von Pfadauswahl, Steering und Session Erhaltung mit Nutzen und Kosten

Steering ist eines der grundlegenden Elemente von SD-WAN, da es elementar zum Versprechen von höherer Geschwindigkeit und Zuverlässigkeit beiträgt. Steering ist die Fähigkeit der SD-WAN-Software, den besten Pfad für den Netzwerkverkehr zu bestimmen, basierend auf vordefinierten Business Policies und den aktiv verfügbaren Verbindungen.



Neue Session wird angelegt

Ein Datenstrom trifft auf der SD-WAN-Appliance ein und eine neue Session wird aufgebaut. Die SD-WAN-Software wählt den besten Pfad basierend auf der Leistungsperformance und der eingestellten Business Policy.

Verschiedene Plattformen nutzen unterschiedliche Messverfahren für die Entscheidung welcher Link für eine neue Session ausgewählt wird.

Die große Frage ist hier:

Erfordert Ihr Netzwerkdesign die Aggregation des Datenstroms über mehrere Verbindungen?

Oder soll bestimmter Traffic über eine definierte Verbindung laufen, es sei denn, diese ist ausgefallen oder stark beeinträchtigt (d.h. traditioneller Failover)?

TO BE OR NOT TO BE!

SESSIONS, PFADWAHL UND UNTERBRECHUNGEN

Wenn Ihre zweite Anbindung z. B. nur über Mobilfunk läuft, möchten Sie wahrscheinlich diese Verbindung nur für sehr wichtigen Traffic reservieren. Und das auch nur, falls die primäre Verbindung komplett offline ist.

Wenn Ihre primäre Anbindung eine Hochgeschwindigkeits-Glasfaser- oder Kabelverbindung ist und Ihre zweite Anbindung eine langsame DSL-Verbindung ist, sollten Sie Ihren Datenverkehr nur dann über die langsamere DSL-Verbindung senden, wenn die Leistung der primären Verbindung unter einen vordefinierten Schwellenwert fällt.





Unterbrechungen ganz oder teilweise während aktiver Session

Wie reagiert die SD-WAN Lösung, wenn eine Session bereits über einer Verbindung aufgebaut ist und diese Verbindung abbricht oder verschlechtert wird, während die Session noch aktiv ist (z.B. Telnet oder ein VoIP-Anruf)?

Session basiertes Steering lässt es nicht zu, dass eine bereits aufgebaute Session auf eine andere Verbindung wechselt. Wenn Session basiertes Steering die einzig verfügbare Steering-Methode ist, würde dies zu einer unterbrochenen Session oder reduzierter Anwendungsleistung führen.

Es gibt allgemein zwei Methoden für aktives Steering (Session Erhaltung), die auf SD-WAN-Plattformen eingesetzt werden:

Link Steering, sowohl am Anfang der Session als auch aktiv während einer Session, ist somit ein großes Unterscheidungsmerkmal zwischen den Plattformen. Wichtig zu beachten: Wenn es um das Design des SD-WAN Netzwerkes geht, gibt es keine „One size fits all“ Lösung.

1. PAKETBASIERTES STEERING:

Hier kann die SD-WAN-Software eine Session auf einen alternativen Link verschieben, ohne die Session zu unterbrechen. Die Video Session oder der VoIP-Anruf können so also auf die verbliebene, noch funktionierende Verbindung wechseln, ohne dass es dabei zu einer wahrnehmbaren Unterbrechung kommt.

2. PAKET DUPLIZIERUNG:

Hier läuft die Session auf mehreren Verbindungen gleichzeitig. Wenn eine einzelne Verbindung unterbrochen oder beeinträchtigt ist, wird die Session auf der Verbindung fortgesetzt, die noch in Betrieb ist.

Es gilt zu beachten, dass sowohl das paketbasierte Steering als auch die Paket Duplizierung nur in einer Umgebung funktionieren, in der sich die SD-WAN Lösung auf beiden Seiten des WAN Edge befindet. Typischerweise bedeutet dies die Nutzung von eigenen Gateways oder des SD-WAN Betreibers. Diese Lösungen sind somit auch teurer als Optionen, die diese Funktionalität nicht enthalten.

Beachten Sie auch, dass dieses Design zwar die Session Erhaltung von wichtigen Anwendungen erhöht, jedoch mehr Hub-and-Spoke Routing von Paketen erfordert, was potenziell das Risiko eines großflächigen Ausfalls erhöht. Es ist also darauf zu achten, dass die Gateways / Hubs redundant ausgelegt sind. Lösungen mit Gateways können jedoch die Netzwerkperformance erhöhen, vor allem bei Kontinentübergreifenden Netzwerken.

KOSTEN- NUTZEN- ANALYSE

Sowohl das sog. Underlay (die Konnektivität), als auch das Overlay (SD-WAN) unterscheiden sich stark in Bezug auf Kosten und Leistungsfähigkeit. IT Entscheider müssen sich mit Bezug auf spezifische Anwendungsfälle ansehen, wie die Anschlüsse und Techniken sich unterscheiden und das Preis-Leistungs-Verhältnis abwägen.



-  Wie oft treten Verbindungsabbrüche und Stromausfälle bei der von mir genutzten Verbindung auf?
-  Ist Active Packet Steering innerhalb einer Session notwendig? Wie hoch wären die Kosten falls die Session unterbrochen würde?
-  Ist meine zweite Anbindung teuer (Mobilfunk) und möchte ich diese Verbindung ständig nutzen?
-  Was bedeutet es, wenn eine Session abbricht, während die SD-WAN-Appliance den Datenverkehr auf eine alternative Verbindung umleitet. Handelt es sich um eine wichtige Konferenz, ein Telefonat oder ist gar das Hochregallager gestört, oder ist es egal.
-  Habe ich hochbezahlte Mitarbeiter oder dringende Projekte, bei denen die Kosten einer verzögerten Übertragungen signifikant höher sind als die Kosten einer schnelleren Datenverbindung?



Sobald Sie Ihre spezifischen Anwendungsfälle identifiziert und abgewogen haben, können Sie Ihr Budget und die Strategie rund um alles was die Konnektivität betrifft festlegen.

Erst dann sind Sie in der Lage, auch einen objektiven Blick auf die Vorteile der dynamischen Traffic Steuerung von verschiedenen SD-WAN Plattformen zu werfen. Das ermöglicht Ihnen eine klarere Sicht auf das Kosten- und Nutzungsmanagement.



BLACKOUT BROWNOUT

SICHTBARKEIT, MONITORING UND WARTUNG

SD-WAN-Orchestrierungssoftware vereinfacht nicht nur die Erstkonfiguration und Bereitstellung, sondern kann auch verwendet werden, um:

-  Echtzeitanalysen zur Auslastung und Verfügbarkeit zu erhalten
-  Generieren von Alarmen via E-Mail- oder API bei Ausfällen oder Leistungseinbußen
-  Durchführen von Massen Konfigurationsänderungen mittels Templates

Verschiedene SD-WAN-Plattformen bieten unterschiedliche Grade an Transparenz, Kontrolle und Selbstheilungsfähigkeiten. Diese stellen zwar hervorragende Tools für die Feinabstimmung der Netzwerkkonfiguration und Kapazitätsplanung dar – gleichwohl gelten die folgenden Fakten sowohl für SD-WAN als auch ältere WAN-Technologien:

- Jede WAN Anbindungen wird irgendwann unterbrochen
- Verbindungsausfälle erfordern oft einen langwierigen Troubleshooting Prozess
- Mobilfunkverbindungen sind nach wie vor teuer und oft im Datenvolumen begrenzt

Einer der Vorteile von SD-WAN ist, dass die Software bei einem Blackout- oder Brownout-Szenario immer folgendes versuchen wird:



Den Traffic so zu priorisieren, dass die kritischsten Anwendungen die meiste Bandbreite erhalten



Den Traffic über alternative Links basierend auf Metriken zum Zustand dieser Verbindung senden



Die Verwendung von Forward Error Correction zur Verbesserung der Zuverlässigkeit der Datenübertragung

DIE FRAGE NACH DEM WIE

DIE WICHTIGSTE ÜBERLEGUNG BEI DER GEWICHTUNG DER SICHTBARKEITS- UND KONTROLLFUNKTIONEN EINER SD-WAN-PLATTFORM IST, WIE SIE SIE NUTZEN MÖCHTEN.



Wenn Sie erheblich in die Geschwindigkeit und Redundanz Ihres Underlay Netzwerks investiert haben, können Sie mit SD-WAN durch die erhöhte Transparenz und Sichtbarkeit des Netzes die Einhaltung der SLA's besser durchzusetzen.

All dies sollte unter dem Gesichtspunkt betrachtet werden, wie Sie SD-WAN nutzen wollen.

Wenn Sie z.B. Managed Service in Erwägung ziehen, werden Sie den Erfolg Ihrer Maßnahme an der Verfügbarkeit und Leistung des Netzes erkennen.

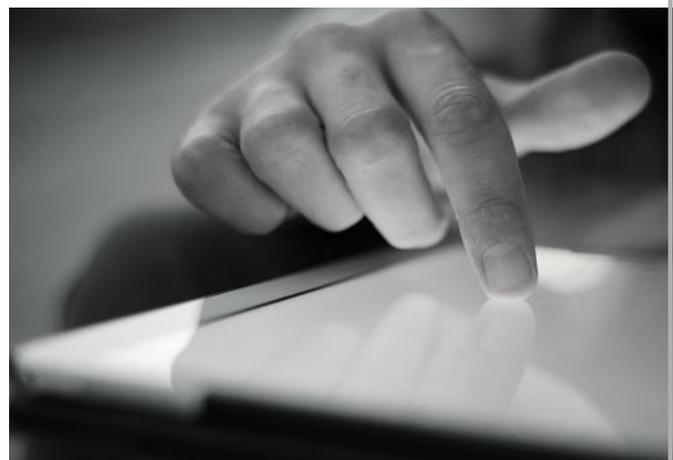
Auch sollte sich der Aufwand für Konfigurationsänderungen und das Bearbeiten von Trouble Tickets signifikant reduzieren.



Wenn Sie kostengünstige Verbindungen mit Mobilfunk Backup in Ihren Zweigstellen haben, ist es wahrscheinlich nicht wichtig, routinemäßig den Traffic zu optimieren, um sicherzustellen, dass Sie das Maximum aus Ihren bereitgestellten Links herausholen.

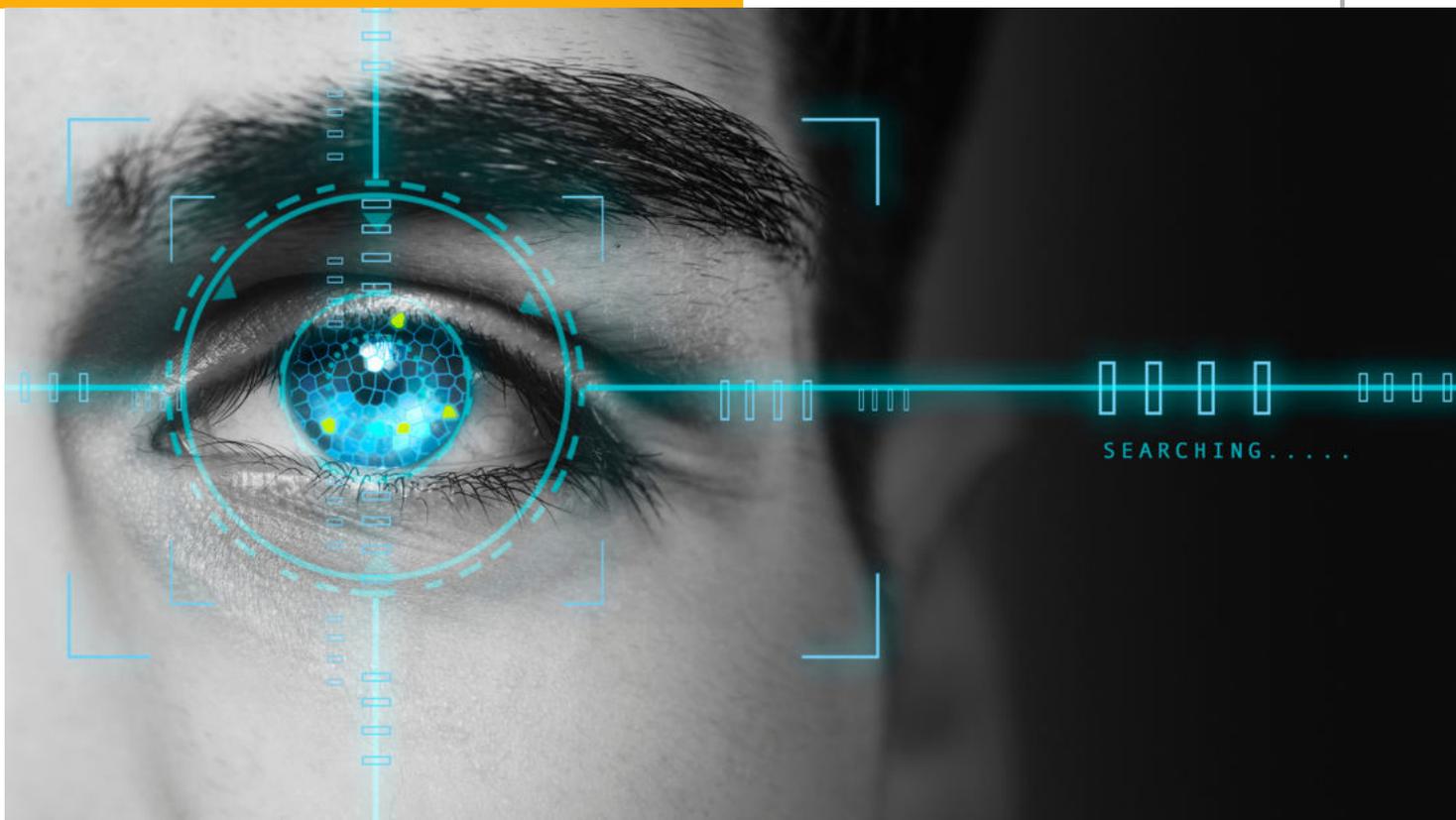


Sofern Sie Ihr SD-WAN selbst managen möchten, müssen Sie nicht nur den Zeitaufwand für die Messung und Abstimmung des Netzwerks, sondern auch die Art und Weise, wie Sie bei Ausfällen benachrichtigt werden, Ihren Incident-Management Prozess sowie die Eskalationsprozesse der Carrier und Ihres SD-WAN-Anbieters berücksichtigen.



SECURITY

Die Gartner-Definition von SD-WAN beinhaltet die Serviceverkettung für Funktionen wie WAN Optimierung, Firewalls, Webfilter etc.. Tatsächlich besteht die Anwendung von "Serviceverkettung" in den meisten SD-WAN Netzwerken aus dem Routing des Datenverkehrs durch die Firewall eines Drittanbieters.



Die ersten SD-WAN-Anbieter mussten eine Lösung dafür finden, dass ihre eingebauten Stateful Inspection Firewalls den Sicherheitsanforderungen einiger Unternehmen nicht genügten, insbesondere weil der gesamte Traffic nicht mehr durch das Rechenzentrum des Unternehmens zu einer zentralen Firewall geleitet wurde. Die ersten Lösungen beinhalteten, einfach eine Security-VNF (Virtual Network Function) auf der SD-WAN Appliance selbst zu betreiben oder den Traffic an eine Cloud-basierte Security Plattform zu senden. Aufgrund der geringen Adaption von VNF haben sich die meisten SD-WAN Anbieter mittlerweile für die Integrationen und Kooperation mit Cloud-basierten Security Anbietern entschieden. Das hat die Probleme nicht nur gemildert, sondern auch das Konzept von SASE (Secure Access Service Edge) geschaffen.

SASE ist ein Cloud basiertes Sicherheits-Framework, das SD-WAN perfekt ergänzt.

Es besteht aus einer Kombination von Netzwerksicherheitsfunktionen wie SWG (Secure Web Gateway), CASB (Cloud Access Security Broker), FWaaS (Firewall as a Service) und ZTNA (Zero Trust Network Access).

Der wichtigste Unterschied zu bisher eher netzwerkorientierten Lösungen (Firewalls) ist, dass die Sicherheit jetzt auf den User, den Kontext und weitere Parameter bezogen wird.

Dadurch werden mobile User, Cloudanwendungen als auch unterschiedliche Endgeräte besser unterstützt und geschützt.

WELCHE SICHERHEIT PASST ZU MEINEM UNTERNEHMEN?

- ❓ Wo liegen Ihre Applikationen? Bei Cloud Providern wie AWS, Google oder Azure, in Ihren eigenen Rechenzentren oder in den Rechenzentren eines Dienstleisters?
- ❓ Möchten Sie, dass Sicherheitsfunktionen in Ihrer Niederlassung oder in der Cloud ausgeführt werden?
- ❓ Verfügen Sie bereits über eine Security Plattform, die Sie integrieren möchten?



Viele Unternehmen nutzen Thin Clients und hosten Anwendungen auf ihrer eigenen Infrastruktur. Da bei dieser Architektur der Datenverkehr an bestimmte Rechenzentren gesendet werden muss, die die in der Regel auch dem Unternehmen gehören, ist es sinnvoller, die Sicherheit im Rechenzentrum zu gewährleisten als eine Cloud-basierte Firewall zu verwenden. Dies entspricht dem Sicherheitsansatz der "geschlossenen Infrastruktur".

Bei Unternehmen, die kein Hub-and-Spoke Netzwerk Design haben und alle Anwendungen über SaaS oder das Internet beziehen, kann zwischen der Sicherheit auf Standortebene gegenüber der Sicherheit in der Cloud entschieden werden.

Unternehmen können durchaus finanzielle und betriebliche Vorteile aus Plattformen ziehen, die SD-WAN und Sicherheit über ein gemeinsames Framework steuern, das dann über eine einzige Oberfläche verwaltet wird.

Auch wenn eine Multi-Vendor Strategie für WAN und Security nicht per se eine schlechte Wahl ist, so muss doch sichergestellt werden, dass die Interoperabilität untereinander gewährleistet ist und Sie in der Lage sind, den Zugriff und die Berechtigungen über die verschiedenen Steuerungsebenen einfach und effektiv verwalten können.

becom Systemhaus GmbH & Co. KG
Charlotte-Bamberg-Str. 6
35578 Wetzlar
+49 6441 96500
info@becom.net
www.becom.net

