NETWORKWORLD FROM IDG

GESPONSORTER CONTENT

E-Book

MIT SECURE SD-WAN ELASTISCHE NETZ-WERKGRENZEN SCHAFFEN

JUNIPER NETWORKS

IDG COMMUNICATIONS INC.

2020 wurden Millionen von Angestellten überall auf der Welt über Nacht zu Remote-Mitarbeitenden. Nun, da die Pandemie endlich abflacht, werden viele von ihnen nicht ins Büro zurückkehren - zumindest nicht ganz.

Laut einer Umfrage von PwC im Jahr 2021 (Remote Work Survey), erwarten tatsächlich mehr als die Hälfte aller Angestellten (55 %), weiterhin mindestens drei Tage die Woche von Zuhause zu arbeiten. Wahrscheinlich werden die Arbeitgeber sie dabei unterstützen. In derselben Umfrage gaben 52 % der Manager an, dass die Angestellten zuhause produktiver gearbeitet haben, 83 % waren sogar der Meinung, dass die Remote-Arbeit ein Erfolg war. Wahrscheinlich wird ein kombiniertes Modell zur Regel.

Dieser Wandel am Arbeitsplatz hat auch die Netzwerke verändert, die Unternehmen für ihre Geschäftszwecke nutzen. Es ist etwas ganz anderes, den Angestellten die Services innerhalb der relativ sicheren Grenzen einer Unternehmens-Firewall bereitzustellen, als Endnutzer mit den Anwendungen und Daten zu verbinden, die sie außerhalb der Netzwerkgrenze benötigen.

Die Unterstützung der Remote-Mitarbeitenden ist nicht die einzige Herausforderung. Die Pandemie beschleunigte die Einführung von Cloud- und Software-as-a-Service-Anwendungen (SaaS). Laut einer Umfrage von IDG im Jahr 2020, IDG Cloud Computing Survey, rechnen mehr als die Hälfte (55 %) der Unternehmen bis 2022 ganz oder überwiegend in der Cloud zu arbeiten. Im Durchschnitt erwarten sie, dass 36 % ihrer Anwendungen bis 2022 auf SaaS umstellen.

ERFOLGSGESCHICHTEN AUS DEM HOME OFFICE

Angestellte, die erwarten, weiterhin von Zuhause zu arbeiten

Manager, die denken, dass Angestellte zuhause effektiver arbeiten

Manager, die denken, dass die Remote-Arbeit ein Erfolg war

QUELLE: 22021 PWC REMOTE WORK – UMFRAGE

EINFÜHRUNG DER CLOUD

Unternehmen, die damit rechnen, bis 2022 ganz oder überwiegend in der Cloud zu arbeiten:

Unternehmen

Diese Unternehmen erwarten, dass 36 % ihrer Anwendungen bis 2022 auf SaaS umstellen

SaaS-Anwendungen

QUELLE: 2020 IDG CLOUD COMPUTING – UMFRAGE

PROBLEME MIT NETZWERKGRENZEN

Dieser rasante Wandel im Unternehmensnetzwerk hat weitreichende Auswirkungen auf das traditionelle Sicherheitsmodell am Netzwerk-Edge.. Zunächst einmal führt der massive Anstieg an Remote-Mitarbeitenden zu einer größeren Angriffsfläche. Wenn die Angestellten sich in den Büroräumen aufhalten, kann die IT eine verwaltete Desktopsicherheit bereitstellen, die Einstellung der Firewall verwalten und sicherstellen, dass es nur einen Weg in und aus dem Netzwerk gibt.

Wenn die Angestellten von Zuhause arbeiten, mag die IT vielleicht noch ihre Laptops und andere Geräte kontrollieren und in manchen Unternehmen dürfen die Angestellten sich nur über ein virtuelles privates Netzwerk einwählen.

Die IT hat aber keine Kontrolle über die anderen Geräte, die am „Netzwerk“ im Homeoffice der Mitarbeitenden angeschlossen sein können: Fernseher, private Router, Kameras oder Thermostate. Jedes dieser Geräte könnte eine Sicherheitslücke bedeuten - und sie alle teilen dasselbe Netzwerk mit dem unternehmenseigenen Laptop der Angestellten. Selbst wenn also das Laptop über VPN verbunden ist, wird das Unternehmen immer noch von Installationsrisiken am Arbeitsplatz im Homeoffice bedroht.

Zudem sind verschlüsselte Tunnel komplex und ihre Verwaltung und Skalierung mühsam. Sie belasten den Verarbeitungsaufwand und können die Benutzererfahrung trüben. Sollte die VPN-Erfahrung für die Angestellten zu abschreckend sein, um effizient zu arbeiten, könnten sie beginnen, die Unternehmensrichtlinien zu umgehen. In diesem Fall hilft auch kein VPN.

SICHERHEIT AUSSERHALB DER GRENZE

Die andere tiefgreifende Umstellung ist die zunehmende Arbeitsauslastung in der Cloud und den SaaS-Anwendungen. Jede Cloud und jeder Cloud-Service haben ihre eigene Sicherheitslösung, die konfiguriert und geschützt werden muss. Schließlich wird sich mehr als die Hälfte der normalen Nutzer im Unternehmen außerhalb der Firewall befinden – genau wie ein Großteil der Arbeitsauslastung.

Die Netzwerksicherheit kann mit diesen Veränderungen nicht Schritt halten und Cyberkriminelle nützen dies aus. So hat das FBI beispielsweise im April 2020 bekannt gegeben, dass es drei bis vier Mal so viele Beschwerden über Cyberangriffe erhalten hat als üblich. Die Hacker verwenden auch immer raffiniertere Methoden. Laut eines Berichts von Deloitte wurden bei 35 % der Cyberangriffe im Jahr 2020 bisher unbekannte Malware oder Methoden eingesetzt, im Vergleich zu 20 % vor der Pandemie.

Die Unternehmen müssen aufgrund der Pandemie auch ihre interne Netzwerkarchitektur überdenken. Die Netzwerkbandbreite wird beispielsweise durch die rasante Zunahme von Videokonferenzen massiv beeinträchtigt. Laut einem Bericht von Twilio haben 30 % der Unternehmen in 2020 zum ersten Mal eine Webkonferenz gehalten.

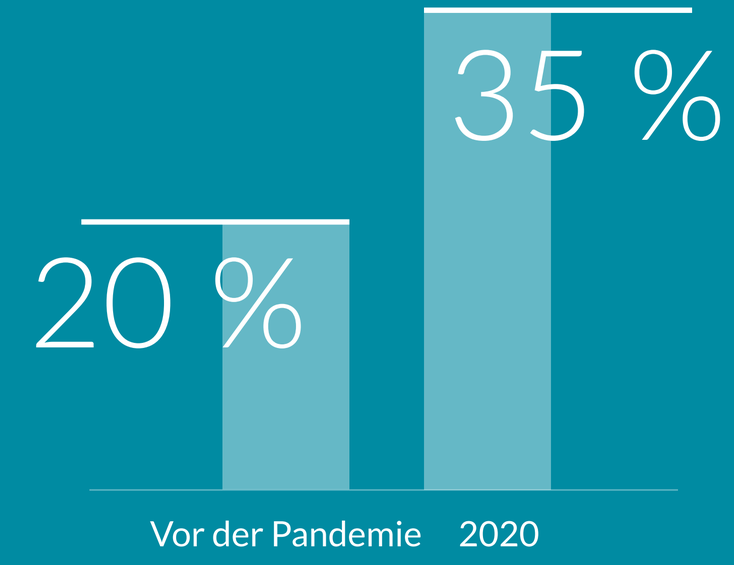
Live-Videostreaming ist eine Anwendung, die viel Bandbreite frisst. Dieser Effekt wird noch verstärkt, wenn die Angestellten Remote-Konferenzgespräche führen. Ohne Architektur zur Unterstützung von Videostreams zwischen Kollegen ist die eingehende Internetleitung schnell überlastet. Angesichts dieser Veränderungen ist es nicht erstaunlich, dass 70 % der Führungskräfte Investitionen in die IT-Infrastruktur planen, um die virtuelle Konnektivität zu sichern.

Anforderungen für ein modernes sicheres Netzwerk

Kurz gesagt: Das traditionelle perimeterbasierte Modell für die IT-Sicherheit in Unternehmen reicht nicht länger aus. Die IT kann nicht in allen Homeoffices der Mitarbeitenden eine Firewall bereitstellen. Zudem würde ein Backhaul zur Prüfung von allen Desktopverbindungen des Angestellten, SaaS und Cloud-Datenverkehr zum Datencenter des Unternehmens eine extreme Latenz bedeuten. Dies ist auch als „Datenverkehrstau“ bekannt, der das Netzwerk aufgrund geringer Leistung und Mehrkosten komplett unbrauchbar macht. Aus so vielen VPNs eine Hub-and-Spoke-Architektur aufzubauen würde zu einer äußerst komplizierten Verwaltung führen und nicht effektiv sein.

CYBERKRIMINELLE WERDEN IMMER RAFFINIERTER

Einsatz von bisher unbekannter Malware bzw. Cyberangriffsmethoden



QUELLE: DELOITTE

JUNIPER NETWORKS

DIE NEUEN NETZWERK-ANFORDERUNGEN

Auch wenn sich die Welt geändert hat, Angestellte, Partner und Kunden benötigen immer noch sofort einen stabilen und schnellen Zugang zu Anwendungen und Daten - unabhängig von ihrem Standort. Die neue Netzwerkarchitektur muss eine Reihe von entscheidenden Anforderungen erfüllen, damit sie den Erwartungen der Endnutzer entspricht, die Kosten im Zaum hält und komplexe Vorgänge vereinfacht.

Authentifizierung anhand der Identität und nicht des Standorts

Bei so vielen Geräten, Nutzern und Anwendungen außerhalb der Firewall, ist die Authentifizierung und der Zugang anhand von IP-Adressen schwierig, vor allem, weil IP-Adressen in Umgebungen mit automatischer Skalierung wie der Cloud sehr kurzlebig sind. Das Netzwerk sollte stattdessen in der Lage sein, ein System zu nutzen, das die Identität jedes Nutzers, das Gerät und die Arbeitsauslastung erkennt.

Wählen Sie einen Zero-Trust-Ansatz

Bei diesem Modell wird der gesamte Datenverkehr standardmäßig als nicht vertrauenswürdig behandelt und der Zugriff verweigert, es sei denn, er wurde identifiziert, authentifiziert und genehmigt. Zero Trust folgt dem Prinzip der minimalen Rechtevergabe, sodass jeder Nutzer, jedes Gerät und die Arbeitsauslastung von Richtlinien gesteuert werden, die Nutzern nur dann Zugang zu den Ressourcen gewähren, wenn sie diese für ihre Arbeit benötigen. Nicht mehr, nicht weniger.

Bei allem was Sie tun, sollten Sie Zero Trust berücksichtigen. Die Unternehmens-IT kann nicht weiter mit einer „von jedem Ort zum anderen"-Einstellung fortfahren. Seien Sie kritisch und verankern Sie Sicherheit in Ihrem Netzwerkpfad. Zero Trust ist ein leistungsstarkes Sicherheitsrahmenwerk. Tatsächlich wurde festgestellt, dass 40 % der IT- und Sicherheitschefs im letzten Jahr nach Zero Trust-Ansätzen suchten. Damit wurde es laut der Studie **IDG 2020 Security Priorities zur beliebtesten** Technologielösung.

Sorgen Sie für Sitzungszuverlässigkeit im Netzwerk

In der grundlegendsten Definition bedeutet eine Sitzung eine vorübergehende Verbindung zwischen zwei Netzwerkressourcen, die über diese kommunizieren können. Sitzungen sind bidirektional, was bedeutet, dass es zwei miteinander zusammenhängende Datenströme gibt. Ihre Ausrichtung hängt von der Ressource ab, die eine Sitzung eingeleitet hat. Danach haben die Sitzungen einen Status.

Diese Merkmale machen jede Sitzung einzigartig, sodass das Netzwerk Pakete und Ströme mit einer Sitzung verbinden kann. Aber anstatt einfach nur Pakete zu senden, entscheidet ein sitzungszuverlässiges Netzwerk dynamisch über das Routing anhand der Sitzungen, die Richtlinien durchsetzen und sicher über die Netzwerkgrenzen erweitert werden können. Dies ist ein viel einfacherer und agiler Ansatz für eine sichere Vernetzung.

Einer der großen Vorteile der Sitzungszuverlässigkeit ist die Möglichkeit, ein elastisches Netzwerk aufzubauen. Wie weiter oben beschrieben, planen viele Unternehmen, ihre Arbeitsauslastung in die Cloud zu verlagern - also muss das Unternehmen die Richtlinie bei der Verbindung zu Ressourcen auf Netzwerken durchsetzen können, die nicht von der IT gesteuert werden. Im wahrsten Sinne des Wortes muss die IT die Grenzen elastisch ausdehnen, um diese Ressourcen einzubinden. Mit dieser Flexibilität kann die IT für sichere Sitzungen sorgen, selbst wenn diese über Netzwerke eingeleitet werden, die sich ständig ändern.

Bauen Sie eine dezentrale Netzwerkarchitektur auf

Die Datenverarbeitung kann sich nicht länger nur auf den Core beschränken. Nutzer, Geräte und Arbeitsauslastung werden nun weit verteilt, manchmal liegen hunderte, wenn nicht tausende Kilometer zwischen ihnen und dem Datencenter. Bei solchen Distanzen kann man nicht einmal mehr mit Lichtgeschwindigkeit die Latenz überwinden und die Leistung wird somit gedrosselt. Die Daten müssen stattdessen am Edge verarbeitet werden - nahe am Endnutzer. Da die Hyperscale-Cloud-Anbieter den Edge ausbauen, wird dies zunehmend einfacher.

JUNIPER NETWORKS

SASE, SECURE ACCESS SERVICE EDGE

Nehmen Sie den Secure Access Service Edge, eine Netzwerkarchitektur, die besser bekannt ist als SASE (Betonung wie „sasi“). SASE fügt ein einheitliches Sicherheitsmanagement, SD-WAN, Firewall-as-a-Service, Cloud Access Security Broker, ein sicheres Web Gateway und eine Zero Trust Network Architecture (ZTNA) zusammen zu einem einzelnen Cloud-basierten Servicemodell, das Sicherheit näher an den Edge rückt.

Aber auch wenn SASE einige Funktionen einbindet, ist eine sichere sitzungsbasierte SD-WAN-Lösung entscheidend für eine SASE-basierte Architektur - eine, die mehrere Middlebox-Funktionen wie DPI, Firewall, und Load Balancing zu einem einzelnen Formfaktor minimieren und damit alles vereinfachen und Kosten senken kann.

Das Ergebnis ist eine unkomplizierte und agile Plattform, die an den sich ständig ändernden Geschäftsanforderungen ausgerichtet ist und erweitert oder verkleinert werden kann. Für eine Sitzungszuverlässigkeit ist es zudem viel einfacher, Software zu skalieren als unzählige, im Routing eingebaute Middleware-Boxen. In traditionellen perimeterbasierten Netzwerken war es schwierig und mühsam, Zero Trust zu ermöglichen, aber dieses Paradigma kann nun erreicht werden, wenn Sie die Sicherheitslösung mit der passenden SD-WAN-Lösung direkt ins Netzwerk integrieren.

Für eine Sitzungszuverlässigkeit ist es zudem viel einfacher, Software zu skalieren als unzählige, im Routing eingebaute Middleware-Boxen.

Unabhängig davon, wo sich Ihre digitalen Ressourcen befinden, schützt Sie dieser SD-WAN-Aufbau vor Angriffen. Das Netzwerk versteht die Netzwerkservices und leitet sie direkt zum richtigen Sicherheitsgerät weiter, unabhängig davon, ob dieses im Büro des Unternehmens oder in der Cloud ist.

Das heißt aber nicht, dass es keine traditionellen Grenzen und Firewalls mehr geben soll. Es ist immer noch sinnvoll, kleine Firewalls beispielsweise für den Unternehmenscampus einzusetzen und ein guter Netzwerkanbieter sollte ein Hybridmodell unterstützen können. Aber dies allein bietet nicht ausreichend Schutz, Agilität und Flexibilität in einem geografisch weit zerstreuten und sich dauernd änderndem Netzwerk. Dafür braucht man eine SD-WAN-Lösung mit einem SASE-Ansatz.

SEITENLEISTE

SESSION SMART™ SD-WAN VON JUNIPER NETWORKS

Wenn SASE eine SD-WAN-Lösung basteln würde, wäre es die Juniper Networks Session Smart™ SD-WAN (früher 128 Technology).

Anstelle einer tunnelbasierten Architektur werden die Session Smart™ Router durch ein sicheres Vektor-Routing versorgt und jede Sitzung mit Metadaten eingeleitet, um zu erkennen, ob es sich um eine vertrauenswürdige Quelle handelt. Diese kann jederzeit auf beliebig viele Router erweitert werden. Der Datenverkehr kann durch den Ansatz der standardmäßigen absoluten Zugriffsverweigerung leicht nach Gruppen und Nutzern aufgeteilt werden, um Zero Trust zu ermöglichen. Somit ist kein Point-to-Point-verschlüsselter Tunnel mehr erforderlich. Deshalb ist die Architektur hoch skalierbar, äußerst sicher und verringert Netzwerküberlastungen um mehr als 60 %. Das ist besonders wichtig, wenn die IT sich mit weit verzweigten Satellitverbindungen oder schwachen Heimnetzwerken herumschlagen muss. Mit Session Smart™ hat die IT uneingeschränkte Sichtbarkeit in den Datenverkehr im Netzwerk und kann so mit einer einzigen Informationsquelle ein globales Netzwerk vom Client zur Cloud verwalten.

Ein Alleinstellungsmerkmal von Session Smart™ SD-WAN ist die adaptive Verschlüsselung. Etwa 80 % des Datenverkehrs im Internet ist bereits verschlüsselt, also muss man ihn nicht noch einmal verschlüsseln. Dadurch würde vor allem der Verarbeitungsaufwand aufgebläht, was wiederum die Latenz erhöhen und der Leistung schaden würde. Das ist genau das, was in VPNs und vielen anderen traditionellen Netzwerksicherheitssystemen passiert. Über die Managementkonsole in Session Smart™ („Session Smart™ Conductor“) kann die IT leicht Richtlinien festsetzen, sodass verschlüsselter Datenverkehr von Quellen wie Zoom oder Microsoft 365 nicht noch einmal verschlüsselt werden muss. Stattdessen erkennt die Konsole, wann Daten von diesen und anderen SaaS-Anwendungen direkt und sicher ins Internet geleitet werden und dadurch zu einer optimalen Benutzererfahrung beitragen.

Da wir Session Smart™ SD-WAN nun unter das Dach von Juniper Networks gebracht haben, können sich unsere Kunden maschinelles Lernen und AIOps-Engines zur Selbstheilung des Netzwerks zunutze machen und den virtuellen Netzwerkassistenten Mist Systems Marvis verwenden, um rasch und unkompliziert Netzwerkstörungen festzustellen. Dadurch werden Ausfallzeiten und fatale manuelle Fehler erheblich verringert. Bei der Vernetzung übernimmt Session Smart™ die meisten Routinearbeiten, sodass der IT-Belegschaft mehr Zeit für Projekte bleibt, die Mehrwert bringen.

Sue Graham Johnston, VP/GM bei Juniper, meint: „Wenn Sie erst einmal diese weitreichende Aufteilung von Nutzern, Richtlinien usw. erreicht haben, können Sie die Vorteile des KI-basierten Modells nutzen, das Juniper gestaltet hat. Sie füttern die Daten in die Cloud, der Cloud-Betreiber setzt die Richtlinien fest und das Netzwerk läuft von alleine.“

Unternehmen wie Momentum Telecom, ein Service Provider für VoIP und Unified Communications waren von diesen Vorteilen beeindruckt und stellten Session Smart™ bereit.

„Wir haben die Geschwindigkeit, die Geradlinigkeit und die Netzwerkorchestrierung und wirklich jeden Aspekt des Produkts durchleuchtet und dann haben wir es in all unseren Datencentern und Büros eingerichtet.“ MARK MARQUEZ Executive VP of Technology, Momentum

Mark Marquez, Executive VP of Technology bei Momentum, erzählt: „Wir suchten eine SD-WAN-Lösung, die wirklich die Anforderungen unserer Kunden erfüllt und die Arbeit in ihren Unternehmen erleichtert. Aufgrund der vielen Anwendungen wollte man alles in die Cloud schieben. Wir haben uns die Sicherheit von Session Smart™ angesehen und auch die adaptive Verschlüsselung, die es bietet. Wir haben die Geschwindigkeit, die Geradlinigkeit und die Netzwerkorchestrierung und wirklich jeden Aspekt des Produkts durchleuchtet und dann haben wir es in all unseren Datencentern und Büros eingerichtet.“

Mehr erfahren unter **juniper.net**.

JUNIPER NETWORKS

SICHERES SD-WAN IN EINER SASE-ARCHITEKTUR: VIELE VORTEILE

Unternehmen können auf vielfältige Weise die Vorteile einer leistungsstarken Kombination aus einer sicheren SD-WAN-Lösung in einer SASE-basierten Architektur genießen.

Optimierte Benutzererfahrung

Die Benutzererfahrung ist heute so wichtig wie die Produktionszeit. Bei einer schlechten Benutzererfahrung bleibt die Frage der Sicherheit offen. Die IT braucht eine Netzwerklösung, die auf die Erfahrung achtet, Entscheidungen über Selbstdiagnose und Selbstheilung in Echtzeit trifft und globale Richtlinien für Sicherheit und Leistung unabhängig vom Standort des Benutzers anwendet.

Unkompliziertes WAN-Management

Nicht alle SD-WAN-Lösungen sind gleich. Die IT sollte einige Testläufe und Pilotprojekte der Lösungen durchführen. Kann die Lösung das Netzwerk modernisieren? Ist sie wirklich innovativ? Oder ist das nur „Schönrederei“? Diesen Unterschied zu erkennen ist wichtig, um einen günstigen ROI zu sichern.

Kosteneinsparungen

Mit der passenden SD-WAN-Lösung kann die IT in vielen Bereichen Kosten senken. Die IT kann die günstigeren Arten der Konnektivität wie Breitband anstatt MPLS nutzen, mit einem softwarebasierten Ansatz gebrauchstaugliche Whitebox-Hardware bereitstellen und viele Middlebox-Funktionen in einer einzigen Lösung zusammenfassen.

FAZIT:

Für die neue Welt der Arbeit, SaaS und die Cloud braucht man ein flexibleres und elastischeres Modell für die Netzwerksicherheit als je zuvor. Keine SD-WAN-Lösung kommt ohne den Zero-Trust-Ansatz aus, um Benutzer, Geräte und Workloads jenseits der Netzwerkgrenzen zu schützen, eine gute Leistung mit minimaler Latenz zu bieten und die Anforderungen einer SASE-Architektur zu erfüllen.

Wenn Sie mehr erfahren möchten, besuchen Sie unsere Website **www.juniper.net/de/de/products/routers/session-smart-router.html.**

JUNIPER NETWORKS