Präsentiert von:

netskope

Modernes SD-WAN für SASE

für dummies
A Wiley Brand

Alles verbinden, optimieren und sichern

Einheitliche Richtlinien und Erfahrungen an jedem Ort

Netzwerke mit AIOps in Echtzeit überwachen

Sonderausgabe von Netskope

Muhammad Abid
Parag Thakore

Über Netskope

Netskope, ein weltweit führender SASE-Anbieter, unterstützt Unternehmen bei der nahtlosen Integration von Netzwerk- und Sicherheitsfunktionen, der Nutzung von AIOps, der Anwendung von Zero-Trust-Prinzipien und KI/ML-Innovationen zur Sicherung von Daten mit hochleistungsfähiger Konnektivität und einem umfassenden Bedrohungsschutz. Die schnell und einfach zu nutzende Netskope-Plattform bietet optimierten Zugriff und Echtzeit-Sicherheit für Personen, Geräte und Daten, wo immer sie sich befinden. Netskope hilft seinen Kunden dabei, Risiken zu reduzieren, Leistung zu steigern und unübertroffene Einblicke in alle Aktivitäten von Cloud-, Web- und privaten Anwendungen zu erhalten. Tausende von Kunden vertrauen Netskope und seinem leistungsstarken NewEdge-Netzwerk bei der Bewältigung aufkommender Bedrohungen, neuer Risiken, technologischer Entwicklungen, unternehmens- und netzwerkbezogener Veränderungen sowie neuer gesetzlicher Anforderungen. Um zu erfahren, wie Netskope seine Kunden bei der Vorbereitung auf ihrer SASE-Reise unterstützt, besuchen Sie netskope.com.

Wir möchten uns bei einer Reihe von Personen bedanken, die dieses Buch möglich gemacht haben:

Bei Netskope: Amanda Anderson, Robert Arandjelovic, Madhavan Arunachalam, Chad Berndtson, Jason Clark, Fan Gu, Kathy Jacobsen, Jessica Jostes, Naveen Palavalli, Gerry Plaza, Carolyn Robinson, James Yokota

Bei Evolved Media: Shay Ben-Dov, Theresa Ingles, David Penick, Karen Queen, Vincent Rossmeier, Evan Sirof, Lauren Wagner, Dan Woods

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Modernes SD-WAN für SASE

für dummies®

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Modernes SD-WAN für SASE

Sonderausgabe von Netskope

Muhammad Abid und Parag Thakore

für dummies®

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Modernes SD-WAN für SASE für Dummies®, Sonderausgabe von Netskope

Veröffentlicht von
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2024 John Wiley & Sons, Inc., Hoboken, New Jersey

Kein Teil dieser Publikation darf ohne die vorherige schriftliche Genehmigung des Verlags weder elektronisch noch mechanisch, in Form einer Fotokopie, Aufnahme, durch Scannen oder anderweitig reproduziert, auf einem Datenträger gespeichert oder übertragen werden, es sei denn, dies ist unter Abschnitt 107 oder 108 des US-amerikanischen Urheberrechts (Copyright Act von 1976) zulässig. Genehmigungsanfragen an den Verlag sind an die Abteilung für Rechte und Lizenzen zu richten: Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, Fax (201) 748-6008 oder online unter http://www.wiley.com/go/permissions.

Marken: Wiley, die Bezeichnung „Für Dummies", das Dummies-Mann-Logo, Dummies.com, Making Everything Easier und darauf bezogene Gestaltungen sind Marken oder eingetragene Marken von John Wiley & Sons, Inc. und/oder seiner Tochtergesellschaften in den Vereinigten Staaten oder anderen Ländern und dürfen nicht ohne schriftliche Genehmigung verwendet werden. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber. John Wiley & Sons, Inc. steht mit keinem in diesem Buch genannten Produkt oder Anbieter in Beziehung.

HAFTUNGSBESCHRÄNKUNG/GEWÄHRLEISTUNGSAUSSCHLUSS: DER HERAUSGEBER UND DIE AUTOREN GEBEN KEINE ZUSICHERUNGEN ODER GARANTIEN IN BEZUG AUF DIE INHALTLICHE RICHTIGKEIT UND VOLLSTÄNDIGKEIT DIESES WERKES UND GEBEN AUCH SONST KEINERLEI GARANTIEN AB, INSBESONDERE HINSICHTLICH DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. GEWÄHRLEISTUNGEN KÖNNEN NICHT DURCH VERKAUFSVERTRETER, SCHRIFTLICHES VERKAUFSMATERIAL ODER WERBEAUSSAGEN FÜR DIESES WERK GESCHAFFEN ODER VERLÄNGERT WERDEN. DIE TATSACHE, DASS IN DIESEM WERK AUF EINE ORGANISATION, EINE INTERNETSEITE ODER EIN PRODUKT IN FORM EINES ZITATS UND/ODER EINER MÖGLICHEN QUELLE FÜR WEITERE INFORMATIONEN BEZUG GENOMMEN WIRD, BEDEUTET NICHT, DASS DER VERLAG UND DIE AUTOREN DEN VON DIESER ORGANISATION ODER DEN AUF DIESER INTERNETSEITE ODER VON DIESEM PRODUKT ZUR VERFÜGUNG GESTELLTEN INFORMATIONEN ODER SERVICES BZW. DEN VON IHNEN GEGEBENEN EMPFEHLUNGEN ZUSTIMMEN. DIESES WERK WIRD MIT DEM AUSDRÜCKLICHEN HINWEIS VERKAUFT, DASS DER VERLAG KEINE PROFESSIONELLEN DIENSTLEISTUNGEN ERBRINGT. DIE HIERIN ENTHALTENEN EMPFEHLUNGEN UND STRATEGIEN SIND UNTER UMSTÄNDEN NICHT FÜR IHRE SITUATION GEEIGNET. GEGEBENENFALLS SOLLTE DIE HILFE EINES PROFESSIONELLEN DIENSTLEISTERS IN ANSPRUCH GENOMMEN WERDEN. AUSSERDEM SOLLTE SICH DER LESER DARÜBER IM KLAREN SEIN, DASS SICH DIE IN DIESEM WERK AUFGEFÜHRTEN INTERNETSEITEN IN DEM ZEITRAUM ZWISCHEN DER ENTSTEHUNG DIESES WERKES UND DEM ZEITPUNKT DES LESENS MÖGLICHERWEISE GEÄNDERT HABEN ODER NICHT MEHR EXISTIEREN. WEDER DER VERLAG NOCH DIE AUTOREN HAFTEN FÜR HIERAUS ENTSTEHENDE SCHÄDEN, ENTGANGENENE GEWINNE ODER ANDERE KOMMERZIELLE SCHÄDEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SONDER-, NEBEN-, FOLGE- ODER ANDERWEITIGE SCHÄDEN.

Allgemeine Informationen zu unseren sonstigen Produkten und Services oder zur Erstellung eines individuellen Für Dummies-Buches für Ihr Unternehmen oder Ihre Organisation erhalten Sie von unserer Abteilung Business Development in den USA telefonisch unter Tel. 877-409-4177 oder per E-Mail unter info@dummies.biz. Alternativ können Sie uns auch auf www.wiley.com/go/custompub besuchen. Für Informationen zur Lizenzierung der Für Dummies-Marke für Produkte oder Services kontaktieren Sie bitte BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-21947-6 (pbk); ISBN 978-1-394-21948-3 (ebk)

Danksagung des Verlags

Die folgenden Personen haben bei der Erstellung dieses Buches mitgewirkt:

Editor: Elizabeth Kuball

Acquisitions Editor: Traci Martin

Editorial Manager: Rev Mengle

Client Account Manager: Jeremith Coward

Production Editor: Saikarthick Kumarasamy

Besondere Unterstützung: Nicole Sholly

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Inhaltsverzeichnis

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Einführung

Unsere Unternehmen und Gemeinden, ja unser ganzes Leben werden seit Jahrzehnten von Computernetzwerken unterstützt. Während sich die Computertechnik und die digitale Welt ständig weiterentwickeln, hinkt Enterprise Networking den technischen Fortschritten hinterher. Networking ist eine dynamische und lebendige Praxis, die von geschäftlichen Anforderungen, den verfügbaren technischen Innovationen und menschlichem Einfallsreichtum geprägt wird. Manchmal eilen die Netzwerke den praktischen Anwendungsmöglichkeiten voraus. In anderen Fällen verliert eine einst beeindruckende Technologie ihre Nützlichkeit und es entstehen neue Technologien, um aufkommende Anforderungen zu erfüllen.

Dies ist ein Buch zum Thema Enterprise Networking. Es betrachtet nicht nur die Geschichte von Unternehmensnetzwerken, sondern wirft auch einen Blick in ihre Zukunft. Es erklärt, wie Unternehmensnetzwerke mit den Entwicklungen der Cloud-zentrierten, vom Internet of Things (IoT) geprägten Mobile-First-Welt Schritt halten können. Die Vernetzungspraktiken der Vergangenheit hatten viele positive Seiten. Die damaligen Modelle und Technologien sind jedoch für moderne Unternehmen in einer zunehmend grenzenlosen Welt nicht mehr optimal.

Wir brauchen nicht nur eine neue Art der Vernetzung, sondern auch eine völlig neue Denkweise. Technische Fähigkeiten allein reichen nicht aus, um die Benutzer vielfältiger Geräte mit stark verteilten Zielorten und Anwendungen zu verbinden. Wir brauchen eine Vision für Netzwerke ohne Grenzen, die unsere grenzenlose und hypervernetzte Welt unterstützen können.

Über dieses Buch

Das Borderless Software-Defined Wide Area Network (SD-WAN) ist eine Möglichkeit zur Schaffung einer sichereren, zuverlässigeren und leistungsfähigeren Netzwerkarchitektur, die der heutigen hochgradig verteilten und Cloud-basierten Technologielandschaft gerecht wird. Dieses Buch soll Ihnen bei der Entwicklung eines Plans zur Implementierung dieser auf die moderne Welt ausgerichteten Netzwerklösung helfen. Da es sich um ein softwaredefiniertes System handelt, kann es auch an veränderte Geschäftsanforderungen angepasst werden. Und es kommt noch besser ist: Sie können damit auch produktiver arbeiten und Geld sparen.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Leichtfertige Annahmen

Die Grundlagen des Enterprise Networking und die Bedeutung des Internets für die Vernetzung sind Ihnen nicht fremd. Sie können leicht nachvollziehen, warum viele Unternehmen von einem herkömmlichen MPLS-WAN (Multiprotocol Label Switching) auf ein moderneres SD-WAN umgestiegen sind. Wahrscheinlich fragen Sie sich jedoch, was danach kommt. Sie haben erkannt, dass sich das Konzept des Arbeitsortes dauerhaft verändert hat und dass mobile Geräte, die IoT-Infrastruktur und die ständig wachsende Welt der SaaS-Anwendungen (Software-as-a-Service) und Cloud-Services diesen Wandel noch weiter vorantreiben wird. Sie möchten, dass die Netzwerkarchitektur Ihres Unternehmens diesen Entwicklungen nicht länger hinterherhinkt, sondern sich die Vorteile von Borderless SD-WAN zunutze macht, um den Anforderungen dieser sich ständig verändernden Welt gerecht zu werden.

In diesem Buch verwendete Symbole

In diesem Buch erscheinen gelegentlich einige Symbole am Rand, die ihre Aufmerksamkeit auf wichtige Informationen lenken sollen.


TIPP

Alles, was mit dem Tipp-Symbol gekennzeichnet ist, soll Ihnen eine bestimmte Aufgabe erleichtern.


NICHT VERGESSEN

Das Erinnerungssymbol hebt besonders wichtige Fakten hervor.


TECHNISCHES

Hochtechnische Informationen, die Sie getrost überspringen können, sind mit dem Symbol „Technisches“ versehen.


WARNUNG

Mit dem Warnsymbol gekennzeichnete Informationen sollten Sie besonders sorgfältig lesen, um sich unnötige Probleme zu ersparen.

Zusätzliche Informationen

Dieses Buch steckt voller nützlicher Informationen. Sollte Ihr Wissensdurst nach der Lektüre noch immer nicht vollends gestillt sein, gehen Sie einfach auf `www.netskope.com`.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- **Die Entwicklung des Wide-Area Network (WAN)**
- **Wie das WAN vom Software-Defined WAN (SD-WAN) abgelöst wurde**
- **Die „Remote-First"-Kultur und die Einschränkungen herkömmlicher SD-WANs**
- **Warum SD-WANs nicht effektiv genug sind**

Kapitel 1
Warum Netzwerktechnologie den Entwicklungen der modernen Computing-Landschaft hinterherhinkt

In der Geschichte der Netzwerktechnik hat es zahlreiche Wendepunkte gegeben. Alte Technologien werden ständig durch neue ersetzt. Local-Area Networks (LANs) wurden von WANs abgelöst, WANs wichen SD-WANs, und nun neigt sich auch das Zeitalter der SD-WANs dem Ende zu. An ihre Stelle tritt das „Next Big Thing" im Bereich Enterprise Networking: das Borderless SD-WAN. Dank dieser Entwicklung ist es nun möglich, sichere, kontextbezogene Konnektivität von jedem Ort aus nahtlos bereitzustellen – und das auf eine Art und Weise, die speziell auf die hybriden Arbeitsmodelle der Cloud-First-Welt zugeschnitten ist. Unternehmen, die diesen Modernisierungsprozess so zeitig wie möglich in Angriff nehmen, können sich mit einer flexibleren, sichereren und leistungsfähigeren IT-Infrastruktur einen Vorsprung gegenüber ihren Mitbewerbern verschaffen.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Die „One-to-One“-Welt

Vor langer Zeit, in einem Universum, das dem unseren sehr ähnlich war, mussten Unternehmensgalaxien in einer statischen, hardwareorientierten Welt überleben. Die Netzwerktechnik begann mit LANs, die Benutzer und Geräte im Gebäude miteinander verbanden – in der Regel den Hauptsitz oder die Zweigstellen eines Unternehmens. Alle Mitarbeiter kamen täglich ins Büro. Mithilfe von LANs konnten alle Personen, die sich am selben Ort aufhielten, im selben Netz zusammenarbeiten. Sämtliche der von diesen Nutzern benötigten Anwendungen mussten mit einem zentralen Rechenzentrum an einem zentralen Ort verbunden sein, und jede Aktion, die im Netzwerk stattfand, musste über dieses Rechenzentrum geleitet werden. Das funktionierte gut … zumindest eine Zeit lang.

NICHT VERGESSEN

LANs hatten ihre Einschränkungen – allen voran die Tatsache, dass sich alle Benutzer am selben Ort befinden mussten.

Als LANs durch WANs ersetzt wurden, konnten mehr Geräte an mehr Standorten eingesetzt und an Datenzentren angeschlossen werden, die mit dem Internet verbunden und durch eine Firewall geschützt waren. Jedes Gerät befand sich innerhalb eines physischen Perimeters, der Netzwerkfunktionen erfüllte.

Bei WANs mussten Zweigstellenmitarbeiter, die eine Verbindung zu Unternehmensanwendungen herstellen wollten, das private Netzwerk des Unternehmens – in der Regel über MPLS-Links (Multiprotocol Label Switching) – bis zurück zum zentralen Rechenzentrum durchqueren (MPLS ist eine weit verbreitete Netzwerktechnologie für private Netzwerke). Es war einfach zu schwierig und unpraktisch, Anwendungen in jeder Außenstelle zur Verfügung zu stellen. An einem zentralen Standort konnten die Anwendungen und das Netzwerk immerhin einheitlichen Kontroll- und Sicherheitsmaßnahmen unterzogen werden. Allerdings waren alle Zweigstellen gezwungen, sich über das WAN mit dem Rechenzentrum oder der Unternehmenszentrale zu verbinden.

Wenn ein Internetzugang erforderlich war, wurden die Benutzer von der Zentrale aus in alle im Internet gehosteten Geschäftsanwendungen und wieder zurück geleitet. Dieses als *Backhauling* bzw. *Hairpinning* bezeichnete Verfahren war jedoch äußerst umständlich.

Selbst Unternehmen mit globaler Präsenz mussten sich dieser Methoden bedienen, darunter internationale Finanzinstitute, krankenhausübergreifende Gesundheitssysteme und Restaurantketten mit POS-Kassensystemen (Point-of-Sale) wie Taco Bell oder McDonald’s.

In den 2000ern konnten Netzwerkbetreiber Sprach-, Video- und Datendienste mithilfe von MPLS-Verbindungen im selben Netzwerk

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

zusammenführen. MPLS stellt auch heute noch zuverlässige Netzwerkverbindungen zur Verfügung, die durch Service Level Agreements (SLAs) abgesichert sind. Es ist jedoch eine kostspielige Lösung, deren Planung und Bereitstellung mehrere Monate in Anspruch nehmen kann (siehe Abbildung 1–1).

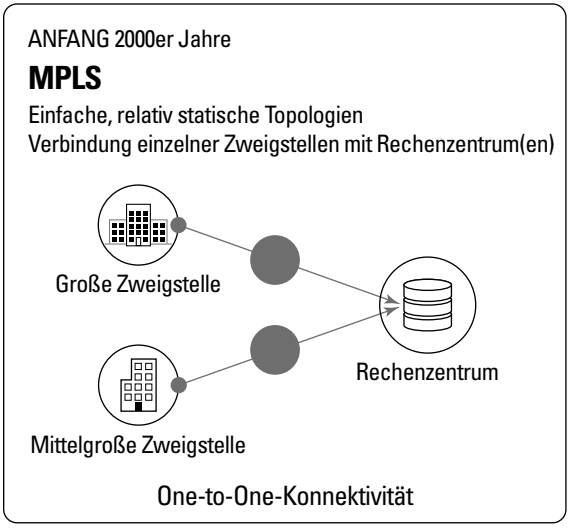

ABBILDUNG 1-1: In der „One-to-One"-Welt nutzen Zweigstellen MPLS, um sich mit einem zentralen Standort – dem Rechenzentrum – zu verbinden, wo alle Anwendungen gehostet werden.

Als Unternehmen jedoch begannen, vermehrt immersive Anwendungen zu nutzen (z. B. Video), reichte MPLS nicht mehr aus, um eine ausreichende Bandbreite an Zweigstellenstandorten bereitstellen. Außerdem war die Einrichtung und Wartung von MPLS nicht billig, und für den hohen Bandbreitenbedarf von Videodaten war die Lösung einfach zu kostenintensiv. Deshalb begannen viele Unternehmen, nach einer kostengünstigeren Alternative zu suchen. Was sie schließlich fanden, ist als *Internet-Transport* bekannt.

Die „One-to-Many"-Welt

Die Kosten für die MPLS-Bandbreite und die Verlangsamung der WAN-Bereitstellung waren die ersten Anzeichen dafür, dass die Netzwerkstrukturen der Vergangenheit nicht mehr mit den Anforderungen der Gegenwart mithalten konnten. Doch es gab auch noch andere Zeichen.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Unternehmen standen vor einer neuen Herausforderung, als sich Software und Speicherplatz zunehmend in den Online-Bereich verlagerten – ein Modell, das als Cloud Computing und Software-as-a-Service (SaaS) bekannt wurde. Sie mussten sicherstellen, dass Anwendungen, wie Microsoft 365 für Produktivität, Amazon Web Services (AWS) für Rechenleistung und Datenspeicherung und Google Cloud für Google Docs und andere Cloud-Services, sicher und mit zuverlässiger Leistung bereitgestellt und gewartet werden konnten. Als immersive videobasierte, cloudbasierte und SaaS-Anwendungen immer mehr an Bedeutung gewannen und sich die Art der Anwendungen änderte, erwies sich das Hinzufügen von MPLS-Bandbreite als zu kostspielig. Was konnten Unternehmen stattdessen tun? Sie brauchten einen digitalen Retter in der Not – und zwar schnell.

Glücklicherweise kam SD-WAN als logische Weiterentwicklung der WAN-Architektur gerade rechtzeitig ins Spiel. SD-WAN war eine moderne Technologie, die eine zentralisierte Steuerung innerhalb verteilter Infrastrukturen ermöglichte und damit viele der mit Cloud-Anwendungen verbundenen Probleme herkömmlicher WAN-Lösungen beseitigte.

Diese Technologie versprach, eine Vielzahl unterschiedlicher Transportwege (MPLS, Internet, Mobilfunknetz) zu nutzen und eine Leistung auf Unternehmensniveau über eine oder mehrere Verbindungen hinweg bereitzustellen. SD-WAN optimierte das Routing und die Priorisierung des Anwendungsdatenverkehrs, da die Netzwerkebene abstrahiert und der Datenverkehr auf der Grundlage zentral definierter und verwalteter Richtlinien weitergeleitet wird. SD-WAN versprach eine zuverlässige Konnektivität zwischen Nutzern in der Zweigstelle und dem Rechenzentrum sowie Cloud-Anwendungen (siehe Abbildung 1-2).

SD-WAN ermöglichte insbesondere

- eine sichere und verschlüsselte Verbindung über das öffentliche Internet, Mobilfunknetze und MPLS zu Anwendungen/Daten, sowohl On-Premises als auch in der Cloud
- die Verbindung eines zentralen Standorts (z. B. eines Rechenzentrums) mit vielen verteilten Standorten (z. B. Zweigstellen)
- die Weiterleitung und Priorisierung des Datenverkehrs je nach Art der genutzten Anwendung und der darin enthaltenen Daten

SD-WAN gab Unternehmen mehr Auswahl und eine größere Kontrolle. Sie konnten nun das Internet auf dynamische und effiziente Weise nutzen und hatten gleichzeitig die Möglichkeit, bei Bedarf MPLS zu verwenden. Da Internetverbindungen viel billiger waren als MPLS, nahmen die Kosten erheblich ab.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Die Verwendung von SD-WAN brachte auch einige Leistungsvorteile mit sich. Obwohl das öffentliche Internet manchmal nicht so zuverlässig ist wie MPLS, bietet das SD-WAN Funktionen, die die Benutzerfreundlichkeit verbessern und eine hohe Zuverlässigkeit gewährleisten. So war es zum Beispiel möglich, QoS-Funktionen (Quality of Service) bereitzustellen, um Daten bestimmte Prioritäten zuzuweisen. Außerdem gab es Link-Remediation-Funktionen zur Behebung von Verbindungsfehlern, z. B. die Vorwärtsfehlerkorrektur, um Probleme zu beheben und Verbindungen zu verbessern.

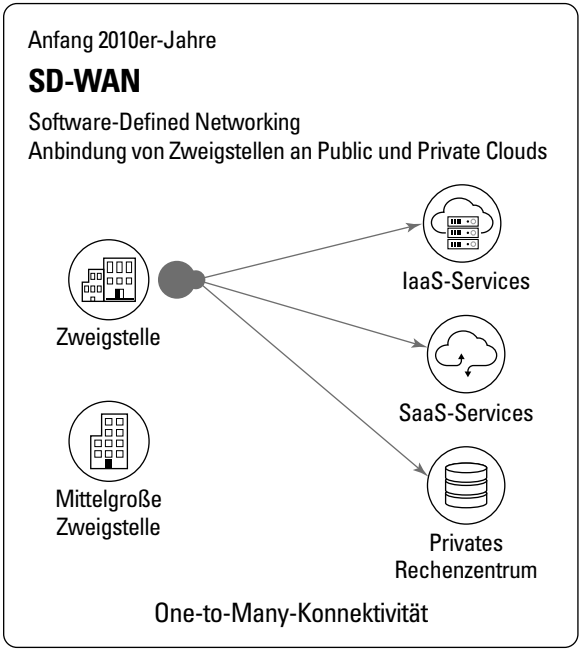

ABBILDUNG 1-2: In der „One-to-Many"-Welt leiten Zweigstellen den Datenverkehr nicht nur über MPLS an das zentrale Rechenzentrum weiter, sondern, dank SD-WAN, auch über MPLS und kostengünstige Internetverbindungen an mehrere Clouds.

Das Ergebnis? Sobald Unternehmen sich selbst von der Leistungsfähigkeit und Einfachheit internetbasierter SaaS-Anwendungen überzeugen konnten und nicht mehr auf Anwendungen im Rechenzentrum angewiesen waren, gab es kein Zurück mehr.

Hat dies zu einer utopischen Welt geführt, in der jedes Unternehmen mithilfe eines flexiblen und erschwinglichen Netzwerks die Vorteile der Cloud voll ausschöpfen konnte?

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Nun, das *wäre* der Fall gewesen ... wenn sich die Welt in der Zwischenzeit nicht schon wieder verändert hätte.

Die Herausforderung der „Many-to-Many"-Welt: SD-WAN am Wendepunkt

Heute befinden wir uns in einer neuen Ära – dem Zeitalter des Unternehmens ohne Grenzen (Abbildung 1-3), in der Benutzer, Geräte, Standorte und Clouds auf vielfältige Weise miteinander verbunden sind. Wir haben eine „Remote-First"-Kultur, in der immer mehr Arbeitskräfte die vier Wände des typischen Unternehmensbüros verlassen. Die Zunahme von Mikrozweigstellen, Multi-Cloud, Remote-Work, Telemedizin, Mobil- und IoT-Geräten (Internet of Things) zeigt, wie sich der Netzwerk-Perimeter des Unternehmens erweitert hat.

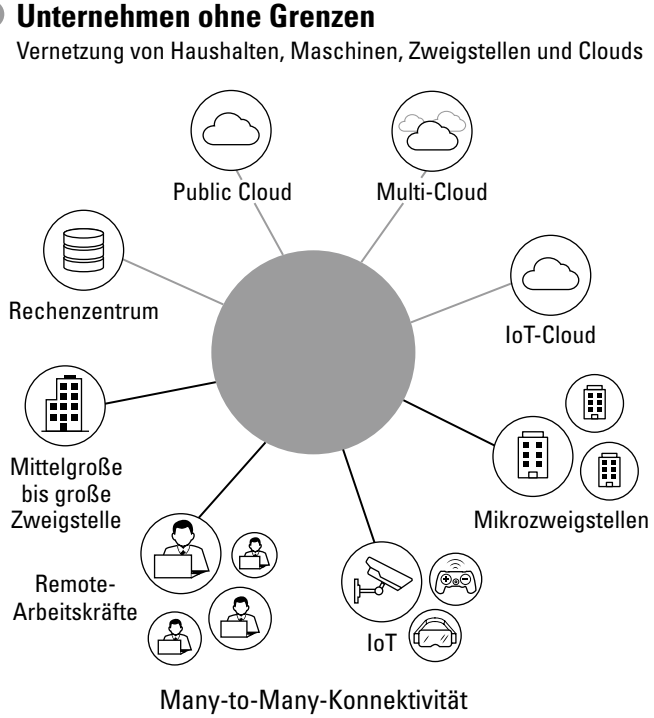

ABBILDUNG 1-3: In der „Many-to-Many"-Welt benötigen Unternehmen ohne Grenzen eine einfache, flexible, sichere und hochleistungsfähige Konnektivität, die alle Arten von Zweigstellen, Remote-Mitarbeitern und IoT-Geräten bis hin zu Rechenzentren und mehreren Clouds umfasst.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Das Gute an SD-WAN bestand darin, dass Unternehmen den Datenverkehr von Benutzern in Zweigstellen zu den gewünschten Zielen steuern konnten. Das gesamte System war jedoch an eine Reihe von Voraussetzungen gebunden, die von den zahlreichen Innovationsschüben der jüngsten Zeit ins Wanken gebracht wurden. Die folgenden Abschnitte bieten einen kurzen Überblick über die wichtigsten Trends, die die Effektivität des SD-WAN beeinträchtigt haben.

Zunahme von Apps und IoT-Geräten

Herkömmliche SD-WANs konnten ein paar tausend Anwendungen unterstützen. Das war am Anfang ausreichend. Angesichts der explosionsartigen Zunahme von Cloud-Anwendungen und IoT-Geräten stieß das Modell jedoch bald an seine Grenzen. Das SD-WAN war nicht darauf ausgelegt, diese neuen Anwendungen und Geräte auf der Grundlage eines umfangreichen Kontexts zu erkennen und zu kategorisieren oder angemessene Richtlinien für sie festzulegen. Was sich nicht verstehen und in sinnvolle Kategorien einteilen ließ, konnte auch nicht priorisiert oder gesichert werden.

IoT-Geräte spielen heute eine größere Rolle als je zuvor. Leider sind die derzeitigen Netzwerkarchitekturen nicht für die Konvergenz von IoT-, Betriebs- (OT) und Informationstechnologie (IT) ausgelegt. Der Mangel an umfassender Transparenz und granularer Kontrolle von IoT-Geräten birgt eine Reihe von Risiken für das Netzwerk. Um diese Risiken zu minimieren, ist eine fein abgestufte Segmentierung auf der Grundlage von künstlicher Intelligenz (KI) und maschinellem Lernen (ML) erforderlich, im Gegensatz zur herkömmlichen Segmentierung auf der Grundlage des Internetprotokolls (IP).

Hybrides Arbeiten

Da viele Arbeitnehmer heute nicht mehr an eine typische Unternehmenszweigstelle gebunden sind, können sie nicht durch SD-WAN-Netzwerke geschützt werden, die speziell auf die Bedürfnisse von Büroangestellten zugeschnitten waren. Heute kann jeder Benutzer und jedes Gerät selbst eine Zweigstelle sein. Die Zahl der außerhalb von Zweigstellen arbeitenden Mitarbeiter ist vor allem im Zuge der COVID-19-Pandemie dramatisch angestiegen, und zwar in einem Ausmaß, für das das SD-WAN niemals ausgelegt war. Mitarbeiter an jedem Arbeitsort erwarten und verdienen ein hochwertiges und sicheres Benutzererlebnis, das mit demjenigen in der Unternehmenszentrale vergleichbar ist.

Als viele Angestellte während der Pandemie nach Hause geschickt wurden, konzentrierten sich IT-Architekten vor allem auf die Sicherung von Fernzugriffsverbindungen. Der langfristigen Architekturplanung wurde meist nur wenig Beachtung geschenkt. Aus diesem Grund haben viele Unternehmen heute Schwierigkeiten damit, mehrere Punktlösungen für

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

die Remote-Konnektivität wie Virtual Private Networks (VPNs), Security Service Edge (SSE), Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP) und SD-WAN Appliances zu verwalten.

Anbindung von Nutzern an mehrere Clouds und Vernetzung von Clouds

Es ist nicht einfach, Verbindungen zwischen Benutzern, Geräten und Standorten mit einer oder mehreren Clouds herzustellen. Dieser Prozess wird vor allem dadurch erschwert, dass Aspekte wie Sicherheit, Geschwindigkeit und Netzwerkeffizienz nicht nachträglich hinzugefügt werden können, sondern von Anfang an integriert werden müssen. Dazu ist eine fortschrittliche Weiterentwicklung des gesamten Architekturdesigns erforderlich. Zu den Anwendungsfällen gehören u.a.:

- Für Benutzer: sicherer, optimierter Zugriff auf On-Premises- oder Cloud-Anwendungen über das unzuverlässige Internet
- Für Unternehmen: sichere, richtliniengesteuerte Kommunikation von Anwendung zu Anwendung über mehrere Clouds hinweg
- Für weltweit verteilte Zweigestellen: Zugriff auf Anwendungen über unzuverlässige Mid-Mile-Netzwerkverbindungen

All diese Anwendungsfälle haben eines gemeinsam: Sie benötigen ein verteiltes Netzwerk von Cloud Points of Presence (PoPs), die strategisch so positioniert sind, dass sie Sicherheit und Optimierung so nah wie möglich bei Benutzern, Geräten, Standorten und unterschiedlichen Cloud-Umgebungen bieten. Durch diese strategische Anordnung kann ein erstklassiges Nutzererlebnis gewährleistet werden. Ein PoP in San Francisco würde Anwendern in Bangalore zum Beispiel kein zufriedenstellendes Benutzererlebnis bieten.

Wireless First (4G/5G)

Eine „Many-to-Many"-Welt, in der die Mitarbeiter jederzeit und überall arbeiten können, erfordert eine größere Anzahl integrierter Drahtlosfunktionen, als das SD-WAN bieten kann. Schnelle und zuverlässige Verbindungen werden an den unterschiedlichsten Orten benötigt – zum Beispiel in einem Außendienstfahrzeug, das sich ständig in Bewegung befindet, auf Baustellen oder auf offenem Gelände – vor allem aber dort, wo kein Breitbandanschluss verfügbar ist oder wo dessen Einrichtung viel Zeit in Anspruch nehmen würde. Wireless-First-Verbindungen sind für eine Vielzahl von Szenarien erforderlich, und eine erweiterte Unterstützung für 4G/5G-Drahtlosverbindungen sollte eine Priorität und kein nachträglicher Gedanke sein.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Mikrozweigstellen

Die Bedeutung des Begriffs *Zweigstelle* hat sich im Laufe der Jahre verändert. Anfangs handelte es sich bei einer Zweigstelle fast immer um eine größere Gruppe von Benutzern. In unserer hochgradig verteilten Welt kann eine Zweigstelle aus fünf oder zehn Personen in einem kleinen Büro, in einer Bankfiliale oder auf einer Baustelle bestehen. Herkömmliche SD-WAN-Lösungen sind zu umständlich und zu schwerfällig, um eine große Anzahl von Mikrozweigstellen schnell anzubinden.

Was wirklich benötigt wird, ist ein kleines mobiles „All-in-One"-Gateway mit integriertem SD-WAN, Sicherheitsfunktionen, Edge Compute, Mobilfunk-Kommunikation, Zugangspunkt und Switch. Mikrozweigstellen sollten genau wie Zweigstellen in der Lage sein, selbst erstellte oder von Partnern entwickelte, leichtgewichtige Edge-Compute-Anwendungen zu unterstützen, um zusätzliche Server überflüssig zu machen und die Investitions- (CapEx) und Betriebskosten (OpEx) für Hardware zu reduzieren. Man kann sich das wie einen Anwendungsspeicher vorstellen, in dem eigene benutzerdefinierte Anwendungen oder Anwendungen aus einem Partnerkatalog ausgeführt werden können.

IT/OT-Konvergenz

Durch die zunehmende Verbreitung von IoT-Geräten, die Entwicklung intelligenter Produktionsanlagen und die Verwendung hochwertiger Ressourcen hat sich die Zweigstelle in der grenzenlosen Welt grundlegend verändert. In dieser Situation kann das SD-WAN beim Zugriff auf Anwendungen kein optimales Benutzererlebnis mehr bieten. Die neue Zweigstelle besteht aus hochwertigen Ressourcen, die in ähnlicher Weise auf Anwendungen zugreifen müssen. Bei diesen Maschinen kann es sich um Geldautomaten, Kräne, Betriebsroboter oder IoT-Sensoren handeln, die Daten erfassen, welche auf effiziente Weise weitergeleitet und mithilfe von KI-Verfahren automatisch analysiert werden müssen, um einen Mehrwert für das Unternehmen zu schaffen und eventuelle Störungen vorherzusagen.

Für einen effizienten Betrieb braucht man Rechenleistung am Netzwerkrand, damit jede leichtgewichtige, containerisierte und auf einen bestimmten Zweck zugeschnittene Anwendung problemlos ausgeführt werden kann. Ein Beispiel dafür wäre ein Glasfaserkabel auf einem Ölfeld, das Temperaturdaten nur dann an den cloudbasierten Analysedienst übermittelt, wenn ein vordefinierter Schwellenwert erreicht ist. Ebenso wichtig ist die effektive Ausführung von Day 1 Operations: Stellen Sie sich eine intelligente Produktionshalle mit einer computergesteuerten CNC-Maschine vor, die ihre Zustandsdaten kontinuierlich an ein KI-gestütztes Tool meldet, das ein Problem vorhersehen kann, bevor es

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

auftritt. Das für den Netzwerkbetrieb zuständige Personal kann aus der Ferne eine Verbindung zum Gerät herstellen, Probleme beheben und eine vorausschauende Wartung durchführen, wodurch Außendiensteinsätze vermieden und Kosten eingespart werden. Diese innovativen Funktionen ermöglichen die Konvergenz von IT und OT.

Einschränkungen des herkömmlicher SD-WAN in der modernen Welt

Herkömmliche Netzwerkarchitekturen stellen heute eher eine Belastung als eine Hilfe für Unternehmen dar, da sie die neuen Geschäftsanforderungen nicht mehr erfüllen können. Unternehmensnetzwerke waren nie für die dezentrale Arbeitswelt von heute ausgelegt. Der Aufbau moderner Netzwerke muss grundlegend überdacht werden, um eine enge Integration von Netzwerken und Sicherheit zu ermöglichen und auf der Grundlage von Zero-Trust-Prinzipien Sicherheit aus der Cloud bereitzustellen. Gemäß dieser Prinzipien – niemals vertrauen, immer überprüfen – sollte man niemals davon ausgehen, dass alles hinter der Unternehmensfirewall sicher ist. Bestehende Netzwerk- und Sicherheitstechnologien sind wie alte Ziegelsteine in einem modernen Glasgebäude: Sie werden in Unternehmensinfrastrukturen hineingezwängt und stören das Design, anstatt es zu verbessern. Sie sind nicht in der Lage, die heutigen Herausforderungen zu bewältigen, und bringen außerdem noch zusätzliche Probleme mit sich. Diese Situation ist alles andere als ideal.

Alle oben genannten Herausforderungen stellen eine Belastung für das SD-WAN dar. So wie einst das SD-WAN entwickelt wurde, weil das WAN mit einer von Zweigstellen dominierten Arbeitswelt nicht länger zurechtkam, so ist das SD-WAN nunmehr an einem Wendepunkt angelangt (manche würden sogar sagen, an seiner Belastungsgrenze), weil es mit einer „Many-to-Many"-Welt nicht zurechtkommt.

Die folgenden Abschnitte sollen verdeutlichen, warum das SD-WAN mittlerweile an seine Grenzen gestoßen ist.

Ein Netzwerk kann nicht durch Flickwerk verbessert werden

Das SD-WAN wurde nicht für die moderne Arbeitswelt entwickelt – und auch ein kleines Upgrade wird daran nichts ändern. Stellen Sie sich vor, Sie hätten eine komplette SD-WAN Appliance für jeden Remote-Mitarbeiter, jedes IoT-Gerät und jede Edge-Anwendung. Das ist so, als würde jeder Fluggast mit einem riesigen altmodischen Koffer an Bord gehen, der zu groß und unhandlich für ein modernes Gepäckfach ist. Es geht einfach nicht. Bisher reagierten Netzwerkteams auf neue Geschäftsanforderungen

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

üblicherweise mit neuen individuellen, maßgeschneiderten Lösungen. Früher bekam jede neue Idee ein neues elektronisches Gerät, heute ist es eine neue virtuelle Maschine (VM). SD-WAN-Appliances, Mobilfunk-Gateways in Zweigstellen, die für Konnektivität sorgen, zusätzliche Produkte zur Verknüpfung von Anwendungen mit mehreren Clouds und herkömmliche VPN-Clients: Sie alle folgen diesem Muster. Diese lose integrierten und getrennt verwalteten Punktlösungen führen jedoch zur Bildung von Technologiesilos.

Letztendlich muss die IT-Abteilung eine konsistente Leistung und zuverlässige Sicherheit für alle globalen Geschäftsressourcen gewährleisten, und das auf kostengünstige Weise und für jede Verbindung. Dies ist kein funktionales Problem, sondern eine architekturbezogene Herausforderung, die nur bewältigt werden kann, wenn IT-Silos beseitigt und Punktlösungen nicht als „Pflaster" eingesetzt werden, um neue Geschäftsanforderungen zu erfüllen. Das Prinzip „noch eine Box oder VM hinzufügen" ist für die neuen Geschäftsmodelle nicht mehr geeignet.

SD-WAN lässt sich nicht skalieren

SD-WAN kann nicht an die zunehmende Anzahl von Benutzern, Anwendungen und Geräten angepasst werden. Es gibt Zweigstellen jeder Größe. Sie können nur einige wenige Mitarbeiter oder Hunderte, wenn nicht gar Tausende Arbeitskräfte umfassen. Bei größeren Zweigstellen müssen SD-WAN-Lösungen in einem großen Cluster mit Lastausgleich betrieben werden, um effektiv zu sein. Stellen Sie sich ein Unternehmen mit Zehntausenden von Mitarbeitern vor, die über die ganze Welt verteilt sind, oder eine Produktionsumgebung mit mehr als 100.000 IoT- fähigen Maschinen, die verwaltet werden müssen. In derartigen Szenarien ist SD-WAN kaum in der Lage, die enormen Datenmengen, die zahlreichen Verbindungen oder die Komplexität der festzulegenden und durchzusetzenden Richtlinien und QoS-Regeln zu bewältigen.

SD-WAN mangelt es an wichtigen Funktionen

In der heutigen Arbeitswelt befindet sich der Kontrollpunkt nicht mehr an der Grenze einer Zweigstelle. Die Fähigkeit, ein Netzwerk zu konfigurieren und zu verwalten, darf nicht an einen physischen Perimeter gebunden sein. Und um Netzwerke und QoS verwalten zu können, müssen wir viel mehr über jede einzelne Verbindung wissen.

Dem SD-WAN fehlt es an Kontextbewusstsein. Es kann nicht verstehen, auf welche Anwendungen Benutzer zugreifen wollen und welche potenziellen Risiken damit verbunden sind, und es kennt weder die Bandbreite der verwendeten Geräte noch deren potenzielle Gefährdung. Unternehmen brauchen diese umfassenden Informationen jedoch, um fundierte

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Entscheidungen über die Priorisierung von Anwendungen treffen zu können. In der Praxis bedeutet dies, dass wesentlich umfangreichere Informationen über Nutzer, Anwendungen und Geräte benötigt werden. Dadurch sind Administratoren in der Lage, spezielle Regeln nicht nur für bestimmte Benutzer und Geräte festzulegen, sondern auch mithilfe von Zero-Trust-Prinzipien Risiken in einer Vielzahl von Kategorien zu verwalten.

Beim herkömmlichen SD-WAN wurde Sicherheit nachträglich hinzugefügt und nicht von vornherein integriert. Zweigstellen konnten direkt über das Internet mit mehreren Clouds kommunizieren – ein Prozess, der eine gravierende Sicherheitslücke eröffnete. Einige Unternehmen entschieden sich für eine verteilte Sicherheitslösung für jede einzelne Zweigstelle, die sich jedoch nicht leicht verwalten und skalieren ließ. Die Sicherheitsfunktionen konnten den mobilen Nutzern und Anwendungen nicht folgen. SD-WAN-Anbieter begannen sogar, im Zusammenhang mit Zweigstellen den Begriff *ausreichende Sicherheit* zu verwenden. „Ausreichende" Netzwerksicherheit ist kein Ersatz für beste Sicherheit, die Secure Access Service Edge (SASE; „sassy" ausgesprochen) bietet, eine cloudbasierte Architektur, die Netzwerk- und Sicherheitsdienste bereitstellt, um Benutzer, Anwendungen und Daten unabhängig von ihrem Standort zu schützen. Die Praxis hat gezeigt, dass Sicherheit aus der Cloud der richtige Ansatz ist. Eine von einem einzigen Anbieter bereitgestellte Lösung (SASE) bietet eine einheitliche Architektur mit vereinfachten Funktionen und Context-Sharing (dem Austausch von Kontextinformationen) zwischen SD-WAN und cloudbasierten Sicherheitsfunktionen (Kapitel 5 wird sich näher mit SASE befassen.)

SD-WAN macht sich weder KI noch ML zunutze

Herkömmliche SD-WAN-Lösungen nutzen weder ML noch fortschrittliche prädiktive Analysen, die effektive automatisierte Abläufe ermöglichen, um Netzwerkteams die Lösung von Problemen zu erleichtern, bevor sie auftreten, und um eine unübertroffene Erfahrung für jeden Benutzer und jede Anwendung zu bieten. Von einem modernen SD-WAN wird erwartet, dass es alle erforderlichen Daten im gesamten Netzwerk erfasst – pro Remote-Benutzer, Zweigstelle und Cloud-Workload – und KI/ML nutzt, um unternehmensweite prädiktive Erkenntnisse zu liefern, mit denen Netzwerktechniker leichter eine höhere Netzwerkleistung sicherstellen können, während Endbenutzer von einer höheren Produktivität profitieren.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Das SD-WAN kann kein hochwertiges Benutzererlebnis für mehr als 60.000 Anwendungen bieten

Eine typische SD-WAN-Implementierung versteht vielleicht die Merkmale von 3.000 oder 4.000 Anwendungen – doch was ist mit den 60.000 oder mehr Anwendungen in der modernen Anwendungslandschaft? Wenn die Merkmale und die Missionskritikalität dieser Anwendungen bekannt sind, können Maßnahmen zur Verbesserung des Benutzerlebnisses priorisiert werden. So sollte eine Person, die Zoom für geschäftliche Zwecke verwendet, ein optimiertes Benutzererlebnis erhalten, während jemand, der YouTube oder Spiele-Apps von der Arbeit aus nutzt, keine Optimierung benötigt.

Das SD-WAN macht die Nutzung der Steuerungsebene nicht leicht

Beim SD-WAN ist zwar die Datenebene von der Steuerungsebene getrennt, doch da die Steuerungsebene als DIY-Element (Do-it-yourself) vor Ort zur Verfügung steht, ist ihre Verwendung nicht gerade unkompliziert. Unternehmen sollten nach einem 100-prozentigen SaaS-basierten Controller Ausschau halten, der in der Lage ist, fortschrittliches Routing wie Border Gateway Protocol (BGP) und Open Shortest Path First (OSPF) zu unterstützen. Sie sollten auch auf die Infrastruktur achten, die die SSE-Funktionen bereitstellt, und prüfen, ob diese eine globale Abdeckung, umfassende Sicherheit an jedem Standort, ein umfassendes Peering mit Cloud-Anbietern und eine möglichst geringe Latenzzeit bietet, damit Kunden keine Kompromisse zwischen Sicherheitseffizienz und Leistung eingehen müssen – und das ist keine leichte Aufgabe. Bei einer Ein-Klick-Konfiguration von SSE-Funktionen für eine SD-WAN-Box in einer Zweigstelle wird automatisch der nächstgelegene PoP gefunden.

4G/5G-Mobilfunk war ein nachträglicher Gedanke

Eine erweiterte Unterstützung für 4G/5G-Mobilfunk muss von Anfang an und auf vielfältige Weise unterstützt werden: als integrierte Datentransportoption im SD-WAN-Gerät und als drahtlose WAN-Lösung, die die Reichweite des SD-WAN-Gateways erweitert. Möglicherweise sind es nicht nur Zweigstellen, die einen drahtlosen Zugriff benötigen, sondern auch mobile Geräte wie Lastwagen oder Roboter. Drahtloskonnektivität spielt in jedem dieser Zusammenhänge eine andere Rolle.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Die Architektur ist nicht in der Cloud entstanden

Die überwältigende Komplexität von Cloud-Netzwerken führt bei vielen Unternehmen zu großen Frustrationen, wenn Benutzer, Geräte und Standorte mit der Cloud oder mehreren Clouds verbunden werden müssen. Bei der Entwicklung der Architektur müssen Sicherheit, Geschwindigkeit und Netzwerkoptimierung als wesentliche Bestandteile der Konnektivität integriert werden, anstatt sie nachträglich hinzuzufügen. Die Anwendungsfälle reichen von einem Benutzer, der über eine unzuverlässige Internetverbindung einen sicheren, optimierten Zugriff auf On-Premises- oder Cloud-Anwendungen erhalten möchte, bis hin zu Zweigstellen, die weltweit verteilt sind und versuchen, über eine unzuverlässige Mid-Mile- oder Multi-Cloud-/App-to-App-Konnektivität sicher auf Anwendungen zuzugreifen. Die Anbindung an die Cloud erfordert aber auch, dass der PoP des Netzwerkes näher an den Benutzer heranrückt, um eine optimale Leistung und ein hochwertiges Benutzererlebnis zu gewährleisten.

SD-WAN ist nicht erweiterbar

Netzwerke werden heute zunehmend in die Cloud verlagert, und die Datenverarbeitung findet näher am Netzwerkrand statt. Anfangs versuchten viele SD-WAN-Anbieter, SD-WAN-VMs mittels Serviceverkettung mit von Partnern bereitgestellten Sicherheits-VMs vor Ort zu verbinden, die auf einer großen Appliance untergebracht waren. Viele dieser Sicherheits- und Netzwerkfunktionen sind jedoch inzwischen in die Cloud verlagert worden. Folglich besteht ein zunehmender Bedarf an leichtgewichtigen Datenverarbeitungsfunktionen, die sich näher an der Datenquelle befinden. Stellen Sie sich vor, ein Einzelhändler möchte, dass ein PoS-System zu 100 Prozent der Zeit verfügbar ist. Er würde das PoS-System als Edge-Compute-Anwendung verschieben, um die Hochverfügbarkeit aufrechtzuerhalten, oder, in der IoT-Welt, Azure IoT Edge am Edge ausführen. Andere Beispiele könnten Ihre eigenen benutzerdefinierten Anwendungen sein.

SD-WAN ist unflexibel und irrelevant

Der Erfolg jeder Technologie hängt von ihrer Relevanz in der gegenwärtigen Technologielandschaft ab. Es kommt immer auf den Kontext an. Trotz seiner ursprünglichen Vorteile unterstützt SD-WAN keine „Any-to-Any"- oder „Many-to-Many"-Verbindungen in der Art und Weise, wie sie heute von Unternehmen benötigt werden. Es lässt sich auch nicht gut skalieren – und Skalierbarkeit ist eigentlich ein Muss für jede Branche.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

NICHT VERGESSEN

Die glorreichen Tage des SD-WAN sind vorbei. Es ist zu starr und unflexibel, um mit dem Wandel in unserer hypervernetzten Welt mitzuhalten. Das SD-WAN muss nun in den Hintergrund treten und einer neuen Technologiegeneration die Bühne überlassen. Und so geht der Kreislauf der Innovation weiter.

WARNUNG

Gibt es keine gesicherte Anwendungserfahrung, keine einheitliche Sicherheit, Transparenz und Anwendungsverwaltung, so ist das wie bei einem Damm: Die Risse werden immer größer und die Katastrophe im Grunde unausweichlich. Benutzer und Geräte geraten in einen Abwärtsstrudel und sind nicht in der Lage, auf Remote-Ressourcen mit dem richtigen Leistungsniveau oder der nötigen Cybersicherheitsrichtlinie zuzugreifen. Was sollte ein IT-Architekt angesichts dieser Flut von neuen Anforderungen also tun? Unternehmen jeder Art und Größe benötigen heute ein SD-WAN, das in der „Many-to-Many"- und der „Any-to-Any"-Welt bestehen kann. Zum Glück gibt es bereits ein SD-WAN dieser Art. Netskope nennt es *Borderless SD-WAN* – und es geht weit über das hinaus, was ein herkömmliches SD-WAN bieten kann.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- **Die Vorteile von Netskope Borderless SD-WAN**
- **Absicherung eines Software-Defined Wide Area Network (SD-WAN)**
- **Die Anforderungen von Mikrozweigstellen**
- **Unterstützung von Endnutzern an jedem Ort**
- **Schnelle und zuverlässige Konnektivität mit 4G/5G**
- **Nutzung des Potenzials des Internets der Dinge (IoT)**
- **Vorteile von Borderless SD-WAN für Ihr Unternehmen**

Kapitel **2**

Die Vision eines vollständig realisierten SD-WAN: Zukunft ohne Grenzen

Das SD-WAN hat sich als Technologie durchgesetzt, weil Benutzer in Zweigstellen eine bessere Unterstützung für das Routing ihres Datenverkehrs über eine Kombination aus kostengünstigen Internetverbindungen und Multiprotocol Label Switching (MPLS) sowie QoS-Funktionen (Quality of Service) benötigten. Wie in Kapitel 1 beschrieben, veränderte sich die Welt in einer Weise, für die das SD-WAN nicht gerüstet war. Jede der in Kapitel 11 erwähnten Entwicklungen – die zunehmende Mobilität, die Verbreitung von Apps und IoT-Geräten sowie Multi-Cloud-Netzwerke – brauchen drahtlose Netzwerke, Edge Computing und Cloud-basierte Sicherheit. Diese

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Anforderungen bringen das herkömmliche SD-WAN und die dafür entwickelten Produkte an ihre Belastungsgrenze.

In diesem Kapitel gehen wir näher auf diese Probleme ein und erläutern, wie sie durch Netskope Borderless SD-WAN gelöst werden können.

Borderless SD-WAN: Netzwerke für eine „Many-to-Many"-Welt

Benutzer und Geräte, die im digitalen Meer treiben und mit vielen Clouds und Anwendungen interagieren, sind wie Segler, die sich ohne Kompass oder Karte durch die Weiten des Ozeans bewegen: Schutz und Optimierung sind oft so schwer zu finden wie ein Leuchtturm im Sturm. Selbst wenn ihnen ein Rettungsanker zugeworfen wird, entpuppt sich dieser oft als ein Sammelsurium von Lösungen, deren Zusammenführung ein administrativer Albtraum ist. Genau das wollen die meisten Unternehmen vermeiden.

Borderless SD-WAN zielt darauf ab, jeder Person und jedem Gerät von jedem Ort aus eine sichere und optimierte Konnektivität zu ermöglichen. Klingt perfekt, oder? Doch wie funktioniert das Ganze? Wie kann diese Vorstellung in die Tat umgesetzt werden?

Um das Borderless SD-WAN (siehe Abbildung 2-1) richtig erklären zu können, müssen wir uns zunächst ansehen, wie sechs aktuelle Szenarien in den Bereichen Computing, Networking und Sicherheit das herkömmliche SD-WAN in Frage stellen:

- Secure SD-WAN
- Mikrozweigstelle
- Endpoint SD-WAN
- Wireless WAN Gateway
- Intelligenter IoT-Zugang
- Multi-Cloud-Networking

Wir werden auf jede dieser Möglichkeiten näher eingehen und erklären, was in der Many-to-Many-Welt benötigt wird, warum das SD-WAN und die derzeitigen Lösungen unzureichend sind und wie Borderless SD-WAN Abhilfe schaffen kann.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

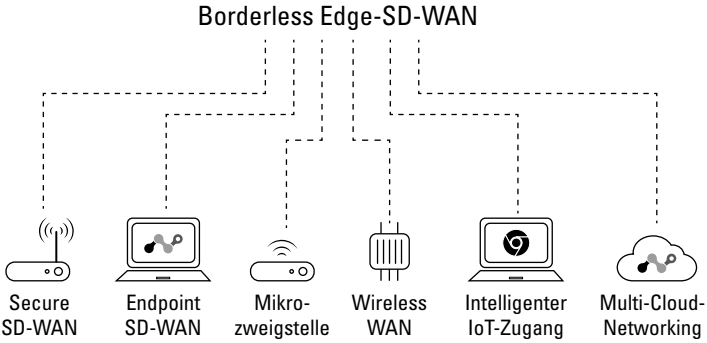

ABBILDUNG 2-1: Borderless SD-WAN unterstützt Software auf Laptops, Mobilfunk-Gateways sowie Anwendungen für kleine bis große Zweigstellen oder Rechenzentren und dient als virtuelles Gateway für Multi-Cloud-Networking.

Secure-SD-WAN

Die Themen Sicherheit und Networking waren schon immer eng miteinander verbunden. Wie bereits erwähnt, waren MPLS-Verbindungen nicht nur teuer und unflexibel, sondern es fehlte ihnen auch an Transparenz und Kontrolle auf Anwendungsebene. Das SD-WAN entstand als Reaktion auf die hohen Kosten von MPLS. Dank SD-WAN erhielten MPLS-Nutzer kostengünstige Internetverbindungen mit hoher Bandbreite, mit denen sie sich in Zweigstellen direkt mit verteilten On-Premises- und SaaS-Anwendungen (Software-as-a-Service) verbinden konnten. Das SD-WAN zielte darauf ab, dasselbe Leistungs- und Sicherheitsniveau über handelsübliche Breitbandverbindungen zur Verfügung zu stellen, was mit anwendungsbezogener Transparenz und Kontrolle effizient erreicht wurde. Administratoren konnten nun zum Beispiel Richtlinien festlegen, die Zoom eine höhere Priorität einräumten als Netflix.

NICHT VERGESSEN

Wir befinden uns nun wieder an einem Wendepunkt, der eine Weiterentwicklung des herkömmlichen SD-WANs erforderlich macht. Aufgrund der explosionsartigen Zunahme von Cloud-Anwendungen und IoT-Geräten reichen herkömmliche SD-WAN-Lösungen, deren Kontrollmechanismen auf anwendungsorientierten Richtlinien basieren, einfach nicht mehr aus, vor allem dann, wenn die jeweilige SD-WAN-Lösung keine Zero-Trust-Prinzipien anwendet.

Moderne Unternehmen benötigen ein Zero-Trust-fähiges, kontextbewusstes SD-WAN, um einen schnellen, zuverlässigen und sicheren Zugang zu jeder Anwendung und jedem Gerät an jedem Ort mit vollständiger Transparenz und den richtigen Kontrollmechanismen zu gewährleisten. Dies kann durch kontextbezogene Richtlinien erreicht werden, die Anwendungen, Anwendungsrisiken, Benutzer, Benutzerrisiken, Geräte und Geräterisiken berücksichtigen und den Netzwerkbetrieb dadurch intelligenter und sicherer machen.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Mit SD-WAN-Lösungen können Administratoren in der Regel Richtlinien für mehrere Tausend Anwendungen festlegen. Dies ist jedoch nur ein Bruchteil der im Internet und in der Cloud vorhandenen Anwendungen, deren Zahl weit über Zehntausende hinausgeht. Wie soll man Anwendungen kontrollieren, die man nicht erkennen kann? Einige dieser Anwendungen können unternehmensfähig sein, andere wiederum nicht. Die automatische Zuweisung von Prioritäten für den Datenverkehr an alle unterstützten Anwendungen stellt nach wie vor eine große Herausforderung dar. Anwendungen müssen von Netzbetriebsteams einzeln und manuell konfiguriert werden. Dieser Prozess ist extrem langwierig und fehleranfällig und lässt sich nicht für Zehntausende von Anwendungen skalieren.

Die Borderless SD-WAN-Lösung von Netskope ist in der Lage, eine Datenbank mit über 60.000 Anwendungen zu unterstützen. IT-Administratoren werden wohl kaum QoS-Richtlinien für jede einzelne dieser Anwendungen konfigurieren. Daher ist es wichtig, die Anwendungen mithilfe eines Cloud Confidence Index (CCI) zu bewerten. Der CCI ermöglicht die Bewertung der Unternehmensreife einer Anwendung, damit intelligente Standardwerte (Smart Defaults) für die QoS-gesteuerte Priorisierung des Datenverkehrs erstellt werden können, die sofort einsatzbereit sind. Dadurch wird dem Netzbetriebsteam die gesamte manuelle Arbeit abgenommen, was zu einem wesentlich effizienteren Betrieb führt. (Zoom hat zum Beispiel einen CCI von 82, der standardmäßig als hohe Priorität gekennzeichnet ist. SureVoIP hat einen CCI-Wert von 38 und wird daher grundsätzlich mit niedriger Priorität behandelt).

Die meisten Unternehmen wollen in der Lage sein, den Zustand ihrer Verbindungen zu den einzelnen Anwendungen kontinuierlich zu überwachen. Gleichzeitig möchten sie die Möglichkeit haben, Anwendungen in Sekundenschnelle von einer schlechten auf eine gute Verbindung umzuleiten. Außerdem wollen sie bei Bedarf Korrekturmaßnahmen vornehmen und das Transmission Control Protocol (TCP) optimieren können.

Das SD-WAN verwendete eine statische, auf IP-Adressen und Subnetzen basierende Segmentierung. Sicherheit leitete sich aus der Kenntnis und Kontrolle des Netzwerks ab. Dieser Ansatz funktionierte in der Vergangenheit durchaus gut. Wie sieht es mit der Mikrosegmentierung von IoT-Geräten am Edge aus, die kompromittiert wurden und Angreifern Zugang zum Unternehmensnetzwerk verschaffen? Herkömmliche SD-WANs bieten keine Transparenz über IoT-Geräte – eine Funktion, die mit der zunehmenden Verbreitung des IoT immer wichtiger wird. Mithilfe von kontextbewussten Funktionen, die auf künstlicher Intelligenz und maschinellem Lernen (KI/ML) basieren, werden alle verwalteten und nicht verwalteten IoT-Geräte automatisch erkannt und in Mikrosegmente unterteilt, damit die mit einem gefährdeten Gerät verbundenen

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Risiken gezielt verwaltet werden können. Ein IoT-Gerät wie eine Kamera könnte zum Beispiel Videos an eine nicht genehmigte Anwendung senden. Durch Mikrosegmentierung kann diese Kamera leicht blockiert werden, um den Ausbreitungsradius zu verringern, falls das IoT-Gerät kompromittiert worden ist.

Borderless SD-WAN erfüllt diese Anforderungen, da es wesentlich mehr Daten über Benutzer, Geräte, Anwendungen und Netzwerke erfasst. Der unfangreichere Kontext ermöglicht eine präzise Anwendung granularer Richtlinien.

Mikrozweigstelle

Der Begriff *Mikrozweigstelle* kann sich auf ein kleines Büro, ein Café oder ein Einzelhandelsgeschäft beziehen – im Grunde auf jeden Ort, an dem Menschen in der heutigen „Remote Work"-Kultur arbeiten. In diesen Szenarien mag es zwar nur wenige Benutzer oder Geräte geben, doch die Anforderungen an Konnektivität, QoS und Sicherheit sind genauso wichtig wie bei einer herkömmlichen Zweigstelle. Sie brauchen ein Thin-Gateway, das kostengünstig ist und eine erstklassige Konnektivität und Sicherheit bietet.

Borderless WAN unterstützt Mikrozweigstellen durch eine kompakte Software, die sich auf einem ebenso kompakten SASE-Gateway (Secure Access Service Edge) befindet, einem Hardwaregerät in einer Zweigstelle oder einer Mikrozweigstelle. Borderless SD-WAN führt Netzwerk- und Sicherheitsservices zusammen. Ein konsolidiertes SASE-Gateway ist die beste Lösung zur Bereitstellung von Borderless SD-WAN. Funktionen wie Mobilfunk-Konnektivität, SD-WAN, Wi-Fi, Sicherheit und Edge-Computing können in einem einzigen System zusammengeführt werden, das von einer Konsole aus bedient und durch eine einzige Richtlinie gesteuert wird. Das ideale System ist die Ein-Klick-Integration über eine einzige Konsole mit einem intelligenten Security Service Edge (SSE), der umfassende Sicherheitsfunktionen bereitstellt.. (Die herstellerunabhängige SASE-Plattform von Netskope bietet übrigens genau diese Kombination).

NICHT VERGESSEN

Mit Distributed Borderless SD-WAN wird es möglich, an jedem beliebigen Standort – von einem kleinen Büro bis hin zu einem Flottenfahrzeug in einer rauen Umgebung wie einem texanischen Ölfeld – ein Benutzererlebnis wie in einer Zweigstelle zu bieten. Dazu müssen mehrere Services von einem einzigen Gerät in einem kompakten, leichten Formfaktor aus unterstützt werden. Die meisten SD-WAN-Anbieter sind dazu nicht in der Lage; sie können SD-WAN nur für herkömmliche Zweigstellen anbieten.

Endpoint-SD-WAN

Ein sicherer und leistungsfähiger Remote-Zugriff wird heute häufig durch ein SD-WAN-Gerät in Kombination mit VPN-Softwareclients

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

(Virtual Private Network) erreicht. Allerdings kann dieses Arrangement für Remote-Benutzer unpraktisch sein, da sie nicht in den Genuss derselben nahtlosen Konnektivität kommen wie ihre Kollegen im Büro. Da Unternehmen sowohl von SD-WANs als auch von VPNs abhängig sind, müssen sie mehrere Anbieter, Geräte und Kostenstellen unter einen Hut bringen. Bei diesem Ansatz ist daher keine Skalierbarkeit gegeben.

Wenn ein VPN-Software-Client ohne SD-WAN-Gerät verwendet wird, treten zahlreiche Probleme auf. VPNs leiden zum Beispiel unter Problemen wie fehlender Transparenz, statischen Point-to-Point-Verbindungen, Latenzzeiten aufgrund von Backhauling und der Unfähigkeit, den Sprach- und Videoverkehr zu optimieren. Wenn man nicht erkennen kann, wer von wo aus auf welche Daten zugreift, kann dies die Produktivität der Benutzer in Verbindung mit unbemerkten Schwankungen der Netzwerkleistung direkt beeinträchtigen.

Herkömmliche VPNs sind darauf ausgelegt, den Datenverkehr zu VPN-Konzentratoren zu leiten, was aufgrund der suboptimalen Pfadauswahl zu zusätzlichen Latenzzeiten führt. SD-WAN-Lösungen können einige dieser Probleme überwinden. Sie sind jedoch hardwareabhängig und bieten keine Zero-Trust-Sicherheit. Außerdem lassen sie sich nicht an die Bedürfnisse jedes einzelnen Remote-Benutzers anpassen.

Moderne Belegschaften erwarten Zero-Trust-Sicherheit und zuverlässige Verbindungen, unabhängig von ihrem Aufenthaltsort. IT-Abteilungen wiederum brauchen Einfachheit und mehr Transparenz, um Remote-Benutzer optimal unterstützen zu können. Trotz der Bezeichnung „Software-Defined‘ ist das SD-WAN auf spezielle Hardware bzw. dedizierte Server angewiesen, vor allem in Zweigstellen.

Durch die Installation von SD-WAN auf einem Laptop lässt sich die Benutzererfahrung erheblich verbessern, unabhängig davon, wo der Benutzer auf das Netzwerk zugreift. Netzbetreiber erhalten einen vollständigen Überblick über alle genutzten Anwendungen und Verbindungen, was die Fehlersuche erheblich erleichtert. Selbst an Orten mit schwachen Internetverbindungen kann das auf einem Laptop installierte SD-WAN durch die Optimierung und Erstellung von QoS-Richtlinien zur Priorisierung des Datenverkehrs für latenzanfällige Anwendungen das Benutzererlebnis deutlich verbessern.

Da SD-WANs hardwarebasiert sind, ergeben sich Probleme, wenn das Volumen der Remote-Zugriffe weiter zunimmt. Betrachten Sie folgendes Beispiel: Ein großes Versicherungsunternehmen muss physische SD-WAN-Geräte an mehr als 25.000 Remote-Contact-Center-Agenten liefern. In einer Phase hoher Mitarbeiterfluktuation werden mehr als 500 Geräte pro Monat nicht an das Unternehmen zurückgegeben, was zu Sicherheitsrisiken, höheren Kosten und logistischen Problemen führt.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Dieses Szenario zeigt, wie dringend eine Lösung wie Borderless SD-WAN benötigt wird, die direkt auf dem Laptop eines Mitarbeiters ausgeführt werden kann.

Alternative Methoden für den Fernzugriff, wie Zero Trust/Zero Trust Network Access (ZTNA)-Systeme, haben ebenfalls ihre Nachteile. Die meisten Zero Trust/ZTNA-Clients bieten keine SD-WAN-Optimierung und die damit verbundenen Vorteile an, und die meisten SD-WAN-Anbieter können keine Zero Trust-Elemente bereitstellen und benötigen Hardware. Eine Lösung, die Zero-Trust-Funktionen und die Vorteile der Anwendungsoptimierung von SD-WAN in Form von Software vereint, kann das Beste aus beiden Welten bieten – und das ganz ohne Hardware. In der modernen Arbeitswelt wird ein 100 Prozent softwarebasierter, einheitlicher SASE-Client benötigt (siehe Abbildung 2-2).

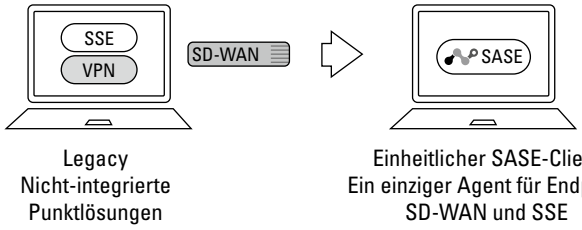

ABBILDUNG 2-2: Borderless SD-WAN unterstützt einen einheitlichen SASE-Client, der SD-WAN-Optimierung mit SSE-Sicherheit verbindet, um den Anforderungen der hybriden Belegschaften von heute gerecht zu werden.

NICHT VERGESSEN

Fernzugriff ist nur dann effektiv, wenn ein hochwertiges Benutzererlebnis und Zero-Trust-Sicherheit überall dort gewährleistet sind, wo Benutzer arbeiten. Einige spezialisierte Lösungen können diese Funktionen ebenfalls bieten, doch in diesen Fällen besteht das Problem darin, dass anstelle einer einzigen Borderless SD-WAN-Lösung eine Vielzahl von Produkten verwaltet werden muss.

Wireless WAN

Um in einer Many-to-Many-Welt überall und zu jeder Zeit arbeiten zu können, brauchen Anwender mehr als das, was SD-WAN an der Wireless-Front bietet. Sie brauchen schnelle und zuverlässige Konnektivität an jedem Ort, sei es in einem Außendienstfahrzeug, das ständig unterwegs ist, oder an einem stationären Zugangspunkt im Unternehmen, der ein starkes Signal liefert.

Das herkömmliche SD-WAN kann das nicht bieten. Borderless SD-WAN schon. Aus der Sicht des Kunden ergeben sich zwei Szenarien bzw. Anwendungsfälle.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Beim ersten Anwendungsfall sucht ein Unternehmen nach einer Lösung, die mehrere Funktionen wie SD-WAN, Sicherheit, Edge-Computing und Wireless-Gateway in einem einzigen Gerät vereint und die mit der Verwaltung komplexer Netzwerke und Kostenstellen verbundenen Probleme beseitigt. Das Wireless Gateway sollte globale Betreiber unterstützen und QoE-Funktionen (Quality of Experience) bieten, damit die Bandbreite der Anwendung dynamisch angepasst werden kann, um Kosten für teure Mobilfunkverbindungen einzusparen. Es kann zum Beispiel akzeptabel sein, Netflix als Anwendung mit mittlerer Priorität zu verwenden, wenn neben der Mobilfunkverbindung auch eine Breitbandverbindung zur Verfügung steht. Wenn die Breitbandverbindung ausfällt, kann eine dynamische QoS-Richtlinie Netflix über Mobilfunkverbindungen blockieren.

Beim zweiten Anwendungsfall wird Borderless SD-WAN als drahtloses WAN-Gateway-Gerät eingesetzt. Das Mobilfunk-Gateway von Netskope kann an der Wand oder Decke montiert und über ein PoE-Kabel (Power over Ethernet) mit Strom versorgt werden. Es bietet eine starke Signalstärke für das im IT-Schrank befindliche Borderless SD-WAN SASE-Gateway. Auf diese Weise können Unternehmen alle Geräte von einer einzigen Konsole aus verwalten und müssen nicht mehrere Anbieter oder Konsolen nutzen. Dank dieser Fähigkeit können Unternehmen Kosten einsparen und die Einschränkungen externer Antennen überwinden, die mit zunehmender Entfernung an Signalstärke verlieren und daher fast unbrauchbar werden, wenn die Entfernung zwischen dem Router im Schrank und dem Dach zu groß ist.

Multi-Cloud-Networking

Das herkömmliche SD-WAN kommt mit Multi-Cloud-Networking und automatisierten Abläufen nicht zurecht. Viele Unternehmen nutzen Dutzende von Clouds, die alle unterschiedliche Workloads hosten. Diese Unternehmen benötigen eine Netzwerklösung, die eine sichere Konnektivität zu all diesen Clouds bietet und gleichzeitig eine richtliniengesteuerte Kommunikation von Anwendung zu Anwendung ermöglicht. Einige neue Anbieter haben Cloud-Networking-Lösungen entwickelt, die die Transparenz und Kontrolle von Cloud-Verbindungen durch eine Reihe von Richtlinien und die automatische Konfiguration von Verbindungen unterstützen. Diese Multi-Cloud-Networking-Anbieter lösen ein wichtiges Problem: Sie erlauben es Unternehmen, ihre Workloads über ein einheitliches Dashboard in diese Clouds zu migrieren, das die für eine effektive Orchestrierung erforderliche Transparenz bietet. Eine tolle Sache – bis zu einem gewissen Punkt. Borderless SD-WAN geht noch einen Schritt weiter und bietet integrierte Sicherheits- und Optimierungsfunktionen für jeden Benutzer, jedes Gerät, jeden Standort und jede Cloud. Mit Borderless SD-WAN erhalten Kunden mit einem Klick Zugang zu SSE und können dadurch umfassende Sicherheitsfunktionen für jede Cloud gewährleisten.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Stellen Sie sich vor, Sie betreiben Tausende von Servern in mehreren Clouds, die Updates aus dem Internet abrufen müssen. Diese Server sind Cyber-Bedrohungen ausgesetzt. Wie kann ihre Sicherheit gewährleistet werden? Borderless SD-WAN nutzt sein umfassendes Kontextbewusstsein und seine Fähigkeit zur Integration mit Cloud-Automatisierungssystemen wie Terraform, um Richtlinien zur Steuerung der Inter-Cloud-Konnektivität, Netzwerkoptimierung und Sicherheit anzuwenden. Dieses Multi-Cloud-Networking wird über eine einzige, einheitliche Konsole verwaltet, über die die kompakte Software von Borderless SD-WAN problemlos in allen Clouds realisiert werden kann. Von dieser einheitlichen Konsole aus können diese Instanzen der Borderless SD-WAN-Software über automatisierte Cloud-Abläufe mit wichtigen Cloud-Anbietern wie Amazon Web Services (AWS) Transit Gateway, Azure Virtual Router und Google Cloud Platform (GCP) Cloud Router interagieren und Routen austauschen. Mit nur einem Klick erhalten Unternehmen Zugang zu Netskope Intelligent SSE und können sich mit integrierter Full-Stack-Security vor allen Cyberattacken schützen.

Borderless SD-WAN erweitert auch das Unternehmens-WAN, sodass Benutzer eine Verbindung zu mehreren Clouds herstellen und Public-Cloud-Infrastrukturen in die Borderless SD-WAN Fabric integrieren können. So können auf Benutzergeräten ausgeführte Anwendungen Cloud-Services wie Infrastructure-as-a-Service (IaaS) auf sichere und effiziente Weise nutzen.

Das Ergebnis: Borderless SD-WAN führt Netzwerk- und Sicherheitsfunktionen einheitlich an jedem Edge zusammen.

TIPP

Mit integrierter Sicherheit und Optimierung können Unternehmen einheitliche Richtlinien für das gesamte Netzwerk aufstellen, die alle Geräte und alle Benutzer in allen Clouds einbeziehen. Dadurch wird sichergestellt, dass die Richtlinien jederzeit konsistent sind, unabhängig davon, auf welche Cloud ein Benutzer zugreift. Welche Funktionen optimiert, zugelassen und eingeschränkt werden, hängt nicht von der verwendeten Cloud ab. Die einzelnen Clouds können nicht nur miteinander kommunizieren (AWS muss mit GCP kommunizieren, das wiederum mit Azure kommunizieren muss usw. Wer hätte gedacht, dass Clouds so gesprächig sind?). Verbindungen können auch sicher durch Multi-Cloud-Umgebungen geroutet werden. Genau so muss Multi-Cloud-Networking in der heutigen Zeit funktionieren, wenn man Best Practices befolgen will.

Intelligenter IoT-Zugang

Unternehmen erwarten heutzutage, dass ihr SD-WAN einen intelligenten Zugang zum IoT bietet. Sie möchten, dass ihre IoT-/Betriebstechnologie (OT)-fähigen Anlagen mit der Cloud verbunden werden, damit Edge Computing auf diesen Anlagen ausgeführt werden kann und nur die

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Daten an die Cloud weitergeleitet werden, die für die Analyse eines Problems und die proaktive Lösungsfindung notwendig sind. Gleichzeitig müssen sie in der Lage sein, die Vorteile von IoT-Funktionen für die Fernüberwachung, Fehlerbehebung, Datenerfassung und vorausschauende Wartung zu nutzen und unnötige Außendiensteinsätze zu reduzieren, die die Arbeits-, Kraftstoff- und andere Kosten in die Höhe treiben. Ohne diese Funktionen ist es schwierig, dem IoT-Ökosystem die gewünschte Investitionsrendite (ROI) abzugewinnen.

Ziel ist es, eine IoT-Anlage mit hochwertiger, sicherer Konnektivität mit Wireless und Edge Computing auszustatten.

Für eine CNC-Maschine (Computer Numerical Control) in einer Fabrik können robuste Borderless SD-WAN-Geräte zum Beispiel nicht nur Wi-Fi für Sensoren bereitstellen, sondern auch Edge-Computing-Funktionen unterstützen, um Informationen wie Temperatur- und Vibrationsdaten von Sensoren zu erfassen. Sie sammeln auch selektiv auf vordefinierten Schwellenwerten basierende nützliche Daten und sorgen dadurch für eine höhere betriebliche Effizienz bei deutlich geringeren Kosten.

Das Netskope SASE-Gateway unterstützt Zero-Touch-Provisioning und integriertes Edge-Computing, was die Rechenleistung näher an die Datenquelle bringt. Es kann Daten von IoT-Sensoren erfassen und extrahieren und übermittelt nur diejenigen Daten an die IoT-Cloud, die die vorgegebenen Schwellenwerte überschreiten. Dazu können Mobilfunk- oder andere Transportverbindungen genutzt werden. Es bietet ein skalierbares Application Lifecycle Management (ALM) und stellt sofort einsatzbereite Containerservices wie Azure IoT Edge Runtime sowie die Möglichkeit zur Ausführung anderer Services aus einem Servicekatalog für mobile Geräte bereit Kunden können sogar ihre eigenen benutzerdefinierten Anwendungen ausführen. Das SASE-Gateway von Netskope mit seinem entwicklerfreundlichen Software Development Kit (SDK) und Application Programming Interfaces (APIs) bietet nicht nur Auswahlmöglichkeiten und Flexibilität, sondern gibt Unternehmen auch die Möglichkeit, ihre eigenen Anwendungen einzubringen.

Zur Bereitstellung von Day-2-Support und laufender Wartung unterstützt das Borderless SD-WAN-Gateway über einen nativen IoT-Manager den externen Zugriff auf wertvolle Anlagen und beschleunigt dadurch die Problemlösung. Dank dieser Funktion werden Außeneinsätze vermieden und das IT-Personal kann die Fehlersuche und -diagnose aus der Ferne vornehmen. Da es Fehlfunktionen eines Geräts vorhersehen kann, ist es in der Lage, umgehend das richtige Ersatzteil zu schicken, um das Problem zu beheben. Auf diese Weise werden Betriebsunterbrechungen vermieden oder minimiert.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Was Sie von diesen neuen Fähigkeiten erwarten können

Unternehmen sollten hohe Anforderungen an die von einer Borderless SD-WAN-Lösung gebotenen neuen Fähigkeiten stellen. Im Folgenden finden Sie eine Liste der Anforderungen, die ein Borderless SD-WAN erfüllen muss, um optimale Sicherheit und Leistung zu gewährleisten. Dazu gehören Elemente, auf die wir bereits eingegangen sind, sowie einige zusätzliche Punkte. Es sollte:

- **Transparenz für Kontextbewusstsein schaffen.** Es ist nicht möglich, etwas zu überwachen, zu priorisieren oder zu verteidigen, das man nicht sehen kann.Eine Borderless SD-WAN-Lösung sollte während des gesamten Datenflusses eine möglichst umfassende Transparenz über Benutzer, Geräte, Anwendungen und Netzwerke bieten. Diese Informationen sollten möglichst in Echtzeit überwacht und aktualisiert werden.
- **Intelligente Zugriffs- und Routing-Funktionen bieten, die die Komplexität bei der Verwaltung beseitigen.** Halten Sie nach einer Lösung Ausschau, die die Konfiguration von SSE- und SD-WAN-Funktionen für SD-WAN-Geräte in Zweigstellen, für Remote-Benutzer, IoT-Geräte und Multi-Cloud-Umgebungen mit einem einzigen Klick ermöglicht. Die Lösung sollte den nächstgelegenen Point of Presence (PoP) automatisch ausfindig machen. Wichtig ist auch ein skalierbarer Cloud-Controller, der mit fortschrittlichen Routingverfahren wie Border Gateway Protocol (BGP) und Open Shortest Path First (OSPF) arbeiten kann.
- **Sicherheit aus der Cloud auf der Grundlage von Zero-Trust-Prinzipien bieten.** Sicherheit muss der Konnektivität überall hin folgen und in Echtzeit auf veränderte Bedingungen reagieren. Herkömmliche SD-WAN-Systeme versuchten, dieses Problem mit gebündelten Firewalls zu lösen. Bei diesem Ansatz konnte die Sicherheit jedoch nicht immer und überall mit mobilen Benutzern und Anwendungen Schritt halten. Eine eng mit intelligentem SSE integrierte Borderless SD-WAN-Lösung bietet SASE aus einer Hand. Sie ermöglicht die Nutzung einer einheitlichen Architektur mit Sicherheitsfunktionen für hybride Netzwerke und bietet Sicherheit vor Ort wie East-West-Firewalls, Intrusion Prevention System/Intrusion Detection System (IPS/IDS) und Segmentierung in Zweigstellen sowie einen vollständigen Schutz durch Cloud-basierte Sicherheitsmechanismen.
- **Skalierbare, KI-gesteuerte Abläufe bieten.** Borderless SD-WAN nutzt KI-gesteuerte Abläufe, um das Netzwerk auf allen Ebenen zu überwachen, einschließlich der Aktivitäten auf Benutzer-, Zweigstellen- und Cloud-Ebene, wodurch eine proaktive Fehlerbehebung und umfassende Analysen ermöglicht werden. Die frühzeitige Erkennung von

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Anomalien und Warnzeichen mithilfe von KI und ML trägt dazu bei, die Anzahl der Support-Tickets und die durchschnittliche Zeit bis zur Lösung eines Problems zu reduzieren, sodass Kunden groß angelegte Netzwerke betreiben können. Mit Hilfe von KI und ML lassen sich auch schlechte Netzwerkbedingungen automatisch korrigieren, um eine optimale Netzwerkleistung zu gewährleisten.

- **Ein sicheres Anwendungserlebnis und Sicherheit für Zehntausende von Anwendungen und IoT-Geräten bieten.** Eine typische SD-WAN-Implementierung kann vielleicht die Merkmale von drei- bis viertausend Anwendungen verstehen. Aufgrund der explosionsartigen Zunahme von Cloud-Anwendungen und des Internet der Dinge (IoT) muss eine Borderless SD-WAN-Lösung jedoch 60.000 oder mehr Anwendungen erkennen und automatisch priorisieren sowie riskante IoT-Geräte automatisch mikrosegmentieren.
- **Erweiterte Unterstützung für 4G/5G Mobilfunk bieten, die nicht nur ein nachträglicher Gedanke ist und auf vielfältige Weise unterstützt wird.** Mit Borderless SD-WAN können Benutzer sicher auf 4G- und 5G-Netzwerke zugreifen, wenn eine Breitbandverbindung nicht verfügbar ist oder wenn ihre Einrichtung zu viel Zeit in Anspruch nimmt. Diese Fähigkeit ist nicht nur für Zweigstellen, sondern auch für mobile Flotten oder Maschinen und Roboter wichtig.
- **Eine Cloudanbindungsstelle (Cloud-On-Ramp) bereitstellen, die Cloud, Netzwerk und Sicherheit zusammenbringt.** Für viele Unternehmen ist es äußerst frustrierend, Benutzer, Geräte und Standorte mit der Cloud oder mehreren Clouds zu verbinden, da Cloud-Netzwerke sehr komplex sind. Deshalb muss die Architektur so weiterentwickelt werden, dass Sicherheit, Geschwindigkeit und Netzwerkoptimierung integrale Bestandteile der Konnektivität sind und nicht nachträglich hinzugefügt werden. Zur Bereitstellung einer Borderless SD-WAN-Lösung und integrierter Sicherheit muss eine hochwertige Konnektivität in der Nähe der Benutzer und Geräte vorhanden sein, wo auch immer sie sich aufhalten. Eine globale Cloud mit PoPs an jedem geeigneten Ort ermöglicht die Ausführung von Funktionen am Netzwerkrand (Edge) und bietet eine qualitativ hochwertige Konnektivität und Performance für Cloud-On-Ramps.
- **Edge-Computing-Anwendungen bereitstellen, um die Nutzung neuer Services zu ermöglichen.** Am Netzwerkrand werden immer mehr containerisierte Anwendungen eingesetzt. Diese Entwicklung führt zu erheblichen Herausforderungen bei der Anwendungsverwaltung, denen die derzeitigen SD-WAN-Architekturen nicht gewachsen sind. Dies wäre zum Beispiel für einen IT-Administrator problematisch, der in einer Zweigstelle eine Anwendung seiner Wahl zur Überwachung digitaler Erfahrungen einsetzen möchte.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- **Warum eine Cloud-First-Architektur wichtig ist**
- **Komplexere Verwaltungs-, Steuerungs- und Datenebenen**
- **Einsatz von maschinellem Lernen (ML) und künstlicher Intelligenz (KI) zur Überwachung von Netzwerken in Echtzeit**

Kapitel 3
Wie funktioniert Borderless SD-WAN?

Der Spruch „Eine Vision ohne Umsetzung ist Halluzination“ wird Thomas Edison zugeschrieben und bewahrheitet sich in der Welt der Technik auch heute noch. In Texas würde man sagen: „Ein großer Cowboyhut macht noch keine Rinder“. Das Ziel der von Netskope entwickelten Version des Borderless Software-defined Wide Area Network (SD-WAN) war von Anfang an klar:Sowohl den Nutzern der Technologie als auch denjenigen, die sie konfigurieren, betreiben, optimieren und debuggen, sollte eine großartige Erfahrung geboten werden. Mit anderen Worten: Netskope nimmt die Umsetzung ernst. Netskope hat das Zeug!

Bei der Umsetzung von Netskope Borderless SD-WAN müssen neue Wege beschritten werden, da die Technologie sowohl den Umfang als auch die Reichweite des herkömmlichen SD-WAN erweitert und neue Anforderungen mit sich bringt, die einen Bruch mit der für SD-WAN verwendeten Architektur und ihren Verwaltungsfunktionen erfordern. Die Netzwerkarchitektur muss sich ebenfalls ändern, um Anwendern auf der ganzen Welt ein optimales Benutzererlebnis bieten zu können.

Zur Bereitstellung eines umfangreichen Spektrums von Services für eine große Anzahl von Benutzern, Zweigstellen, IoT-Geräten (Internet der Dinge) und Cloud-Umgebungen muss sich die Funktionsweise der

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Verwaltungs-, Steuerungs- und Datenebenen ändern. Ältere, auf Zweigstellen ausgerichtete Konfigurationen werden durch Richtlinien ersetzt, die das gewünschte Ergebnis auf Grundlage eines viel umfassenderen Kontexts über den Benutzer, das Gerät, die Anwendung, die Daten und das Netzwerk definieren. Deshalb funktioniert Borderless SD-WAN völlig anders und nutzt eine Cloud-native Architektur. In diesem Kapitel erfahren Sie, was das in der Praxis bedeutet.

Warum Borderless SD-WAN eine Cloud-First-Architektur benötigt

Da wir heute in einer Many-to-Many-Welt leben, hat die Anzahl der Benutzer, Geräte, Standorte und Clouds, die eine sichere, optimierte Konnektivität mit Borderless SD-WAN benötigen, erheblich zugenommen. So muss beispielsweise ein Unternehmen, das Tausende von Callcenter-Mitarbeitern auf ein Homeoffice-Modell umstellt, seine SD-WAN-Funktionen erheblich skalieren. Um diesen Arbeitskräften einen qualitativ hochwertigen Service bieten zu können, ist ein zuverlässiger Point of Presence (PoP) in der Nähe jedes einzelnen Mitarbeiters erforderlich. Dies lässt sich nur erreichen, wenn die Implementierung in die Cloud verlagert und eine neue Konnektivitätsstrategie eingeführt wird. Und genau das tut Borderless SD-WAN.

Viele Hersteller behaupten zwar, die von Borderless SD-WAN benötigte Cloud-native Architektur mit einer in der Cloud bereitgestellten Verwaltungs-, Steuerungs- und Datenebene anzubieten, doch tatsächlich trifft dies nur auf die wenigsten zu. In Wirklichkeit betreiben sie die Software als aktive Backup-Server in der Cloud. Bei dieser Strategie gibt es jedoch ein Problem: Sobald die Kapazität erschöpft ist, muss der Anbieter ständig aktive Backup-Server in der Cloud hochfahren, um den sich ändernden Kundenanforderungen gerecht zu werden. Angesichts der großen Anzahl von Geräten, Standorten und Benutzern, die miteinander verbunden werden müssen, ist es unmöglich, die Architektur zu skalieren. Dieser Ansatz ist daher nicht praktikabel. Wenn man eine Software-Implementierung einfach in die Cloud verlagert, bedeutet das nicht, dass das System das Skalierungspotenzial der Cloud-Technologie auch wirklich ausschöpft.

Um sich die Vorteile der Cloud zunutze zu machen, verwendet Borderless SD-WAN Software-Container und Microservices, die mithilfe der elastischen Ressourcen der Cloud unabhängig voneinander skaliert werden können. Dank dieser Architektur kann Borderless SD-WAN Tausende von Standorten, IoT-Geräten und Endpunkten bereitstellen und verwalten.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

TECHNISCHES

Borderless SD-WAN von Netskope basiert auf einer hochredundanten, verteilten Cloud-Plattform mit mehreren Redundanzebenen, Backup-Snapshots und Auto-Failover. Alle Komponenten der Borderless SD-WAN-Architektur werden in einem fehlertoleranten und redundanten Cluster bereitgestellt. Die Services werden aktiv-aktiv implementiert, was neben einer hohen Verfügbarkeit auch einen effektiven Lastausgleich gewährleistet.

Dadurch kann Borderless SD-WAN nicht nur unabhängig eine hohe Verfügbarkeit sicherstellen, sondern Services auch automatisch skalieren. Jeder Service wird hinter einem Cluster von Load Balancern bereitgestellt, die für Hochverfügbarkeit konfiguriert sind. Für jeden dieser Pools werden unterschiedliche Metriken zur Überwachung der Auslastung verwendet.

Wenn die Maschinen in einem Pool überlastet sind, werden weitere Maschinen hinzugefügt, um die Last zu verteilen. Die Services des Borderless SD-WAN sind außerdem zustandslos und können daher elastisch skaliert werden, sowohl über Serverinstanzen in jedem einzelnen Rechenzentrum als auch zwischen mehreren Rechenzentren, ohne dass es zu Ausfallzeiten oder Leistungseinbußen kommt.

Umgestaltung der Verwaltungs-, Steuerungs- und Datenebenen

Mithilfe von Borderless SD-WAN-Architekturen können die Verwaltungs-, Steuerungs- und Datenebenen wesentlich intelligenter und differenzierter gestaltet werden. In diesem Abschnitt stellen wir die neuen Ansätze für jede Ebene und die damit verbundenen neuen Möglichkeiten vor.

Die Verwaltungsebene

Die *Verwaltungsebene* entstand beim SD-WAN auf der Grundlage eines zentralen Service, der sich in der Regel auf einer virtuellen Maschine (VM) in einem Rechenzentrum oder auch in der Cloud befand. Ihre wesentliche Aufgabe bestand darin, die SD-WAN-Zweigstellengeräte im gesamten Netzwerk zu verwalten und sicherzustellen, dass sie bereitgestellt, aktualisiert und kontrolliert wurden, damit die SD-WAN-Software auf der Hardware des Unternehmens korrekt ausgeführt werden konnte. Das funktionierte gut, bis neue Herausforderungen auftauchten.

Heute müssen Unternehmen eine Fülle von IoT- und persönlichen Geräten sowie Laptops berücksichtigen, die mit dem Netzwerk und Multi-Cloud-Umgebungen verbunden sind. Da das Borderless SD-WAN all

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

diese vielfältigen Anwendungsfälle sowie die von ihnen erzeugten Daten und die Anwendungskonfiguration verwalten muss, hat sich die Verwaltungsebene grundlegend verändert. Sie ist Cloud-nativ, hochredundant und mandantenfähig geworden und lässt sich mit einer intuitiven, webbasierten Benutzeroberfläche einfach bedienen. Diese Entwicklung war notwendig, weil Borderless SD-WAN mehrere wichtige Funktionen erfüllen muss:

- **Software-Verwaltung bei verteilten Anwendungsfällen:** Eine ausgezeichnete Performance und sichere Konnektivität müssen auf jeden Benutzer, jedes Gerät, jede Zweigstelle und jede Multi-Cloud-Umgebungen ausgeweitet werden. Borderless SD-WAN hat die Aufgabe, die Software für diese verteilten Anwendungsfälle zu verwalten, was eine viel größere Herausforderung darstellt als die Verwaltung der Software für die zuvor von Unternehmen verwendeten kleineren Anzahl von SD-WAN-Boxen.
- **Daten- und Telemetrieverwaltung:** Es muss den gesamten vom Netzwerk empfangenen Daten- und Telemetrie-Traffic verwalten. Dies ist nur mit der von Borderless SD-WAN gebotenen Skalierbarkeit möglich.
- **Verwaltung des neuen Remote-Arbeitsmodells:** Es muss in der Lage sein, das neue Remote-Arbeitsmodell in großem Umfang zu unterstützen. Viele Unternehmen versuchen heute nicht mehr, einige hundert Außenstellen zu betreiben, sondern müssen stattdessen die Daten von Tausenden von Remote-Benutzern effizient und sicher verwalten und abrufen können.


TIPP

Mit Borderless SD-WAN profitieren Unternehmen von uneingeschränkten Konfigurationsmöglichkeiten und Transparenz über alle ihre Netzwerkgeräte auf Verwaltungsebene. Die Verwaltungsebene des Borderless SD-WAN kann auch Informationen über den Zustand von Anwendungen sowie automatische und sichere Software-Updates für alle Netzwerkgeräte gleichzeitig bereitstellen. Herkömmliche SD-WAN-Produkte können keinen derart umfassenden Überblick über das gesamte Netzwerk eines Unternehmens und alle Geräte bieten.

Die Steuerungsebene

Die *Steuerungsebene* ist der Bereich, in dem Unternehmen ihre Netztopologie aufbauen und verwalten können; sie ermöglicht es einer Zweigstelle, andere Zweigstellen zu „erkennen“. Beim herkömmlichen SD-WAN wurde diese Steuerungsebene in der Regel auf einem physischen Hardwaregerät ausgeführt, auf dem sich auch die SD-WAN-Datenebene befand. Bei einem Ausfall der Datenebene fiel allerdings auch die Steuerungsebene aus, sodass es keinerlei Ausfallsicherheit gab. Wenn

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

die Steuerungsebene wiederum keine Adjazenz-Kapazität mehr hatte (für Technik-Gurus: wenn die Steuerungsebene ein Border Gateway Protocol [BGP] verwendet, ist es das BGP, das keine Adjazenz-Kapazität mehr hat), mussten weitere SD-WAN-Geräte installiert werden, da die Steuerungsebene und die Datenebene auf demselben Router bzw. derselben Hardware liefen. Darüber hinaus war die Steuerungsebene des SD-WAN einfach nicht für die große Anzahl zu verwaltender Benutzer, Geräte, Zweigstellen und Multi-Cloud-Umgebungen ausgelegt.

Bei Borderless SD-WAN wird die Steuerungsebene in die Cloud verlagert und über Software-as-a-Service (SaaS) bereitgestellt. Sie interagiert mit einer lokalen Steuerungsebene wie BGP und Open Shortest Path First (OSPF), sodass es keinen physisch in die Unternehmensumgebung eingebundenen Controller mehr gibt. Sie ist ein vom Unternehmen genutzter Service wie Salesforce, Workday oder jede andere SaaS-Lösung. Durch die Bereitstellung der Steuerebene als SaaS ist Borderless SD-WAN nun in der Lage, bei Bedarf zu skalieren. Außerdem müssen sich Unternehmen nicht mehr um zusätzliche Hardware zur Steigerung der Kapazität der Steuerungsebene kümmern, wenn das Unternehmen wächst und neue Zweigstellen hinzukommen.

TIPP

Dank der Verlagerung der Steuerungsebene in die Cloud kann Borderless SD-WAN die Netzwerktopologie genauer und differenzierter verwalten als dies bisher möglich war. Angesichts der ständigen Erweiterung von Netzwerken und der zunehmenden Anzahl an persönlichen und IoT-Geräten sowie Verbindungen zu drahtlosen Gateways ist dies heute eine Notwendigkeit.

Borderless SD-WAN verlagert die Steuerungen vollständig in die Cloud und bietet ein Maß an Kontrolle, Einfachheit und Skalierbarkeit, das mit SD-WAN nicht möglich gewesen wäre.

Die Datenebene

Mit einem zu 100 Prozent SaaS-basierten Controller, der Transparenz über das gesamte Netzwerk und alle damit verbundenen Geräte bietet, erhalten Unternehmen nie dagewesene Einblicke in die Daten, die sich durch ihr Netzwerk bewegen, und können sich von komplexen On-Premises- und DIY-Controllern verabschieden.

Die *Datenebene* hat sich im Rahmen des Borderless SD-WAN-Paradigmas ebenfalls stark verändert. Bei MPLS stand die Weiterleitung von Paketen im Mittelpunkt. Die Entwicklung des herkömmlichen SD-WAN war ein großer Fortschritt, da Routing-Entscheidungen und -Richtlinien nun auf Anwendungen basierten. Die mit den Anwendungen, Benutzern und Geräten verbundenen Kontexte wurden dabei jedoch nicht berücksichtigt. Mit anderen Worten: Herkömmliche SD-WAN-Lösungen waren nicht in

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

der Lage, Richtlinien auf der Grundlage von Anwendungsrisiken bzw. den zwischen Benutzern oder Geräten bestehenden Risiken zu verwalten. Wie in Abbildung 3-1dargestellt, wurden dem SD-WAN Sicherheitsfunktionen nachträglich hinzugefügt. Sie waren entweder gerade mal ausreichend oder nur lose integriert. Dadurch war das System komplex und nicht in der Lage, Kontextinformationen zwischen dem Netzwerk und den Sicherheitsmechanismen auszutauschen.

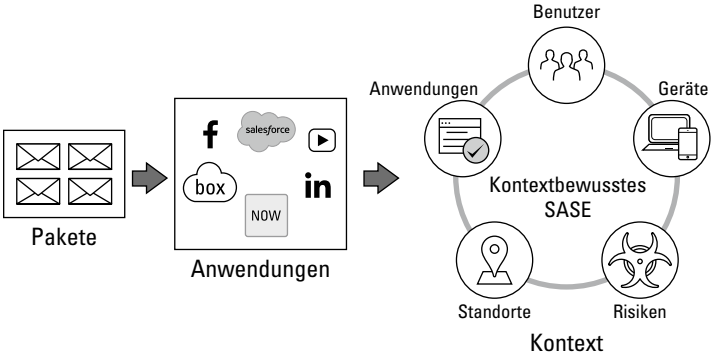

ABBILDUNG 3-1: Die kontextbezogenen Richtlinien von Borderless SD-WAN basieren auf dem Verständnis von Anwendungen, Benutzern, Geräten und den mit ihnen verbundenen Risiken, was den Netzwerkbetrieb (NetOps) intelligent und sicher macht.

In einer modernen Umgebung (siehe Abbildung 3-1) benötigen Unternehmen einheitliche Richtlinien für die Anwendungsperformance, den Zero-Trust-Zugriff und die Sicherheit aller Remote-Benutzer, Standorte, Geräte und Clouds. Borderless SD-WAN bietet diese Fähigkeiten auf einem völlig neuen Niveau:

- **Ein Klick zum Security Service Edge (SSE) automatisiert die Konnektivität von Borderless SD-WAN zu SSE.** Zudem können Services mühelos in Anspruch genommen werden, ohne Konfigurationen für die Weiterleitung des Datenverkehrs oder die Verwendung von PAC-Dateien (Proxy Auto-Configuration) erstellen zu müssen.
- **Borderless SD-WAN erweitert den Kontext in Bezug auf Benutzer, Geräte, Daten und Anwendungen, wodurch weitaus effektivere und differenziertere Richtlinien festgelegt und durchgesetzt werden können.** Mit Lösungen, die kontextbezogene Sicherheits- und Routing-Entscheidungen in der Cloud treffen können, lassen sich Benutzerrisiken besser verwalten und Geräterisiken können mit segmentierten Richtlinien in Echtzeit erkannt und bewältigt werden. So ist es möglich, 60.000+ Anwendungen zu identifizieren, automatisch zu

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

priorisieren und zu optimieren oder IoT-Geräterisiken auf der Grundlage von KI/ML zu erkennen.

- **Borderless SD-WAN sorgt auch dafür, dass sich Remote-Benutzer, Standorte, Geräte und Multi-Cloud-Umgebungen immer in der Nähe eines globalen Netzwerks von PoPs befinden.** In Verbindung mit SSE fügt sich Borderless SD-WAN an diesen PoPs zwischen Benutzer und Anwendungen ein. So kann es sein Potenzial entfalten und die Services zur Verfügung stellen, die für die Anwendung von Richtlinien und die Verbesserung der Servicequalität (QoS) mit integrierter Sicherheit benötigt werden. Damit das gelingt, müssen sich die Netzwerkverbindungen und die Borderless SD-WAN-Services netzwerktechnisch in der Nähe des Nutzers befinden. Wenn alle Borderless SD-WAN- und SSE-Funktionen in einem Rechenzentrum in Seattle ausgeführt werden, während sich Ihre Anwender oder Zweigstellen in Mumbai oder Berlin befinden, ist die Benutzererfahrung langsam und inkonsistent.

Deshalb hat Netskope ein globales Netzwerk von PoPs eingerichtet: NewEdge.

Netskope NewEdge ist eine speziell entwickelte Private Cloud, die Netzwerk- und Sicherheitsservices im großen Maßstab miteinander verbindet und On-Ramps mit niedrigen Latenzzeiten in mehr als 70 Regionen der Welt bereitstellt. Das NewEdge-Netzwerk ermöglicht die nahtlose Integration von Borderless SD-WAN- und SSE-Services und stellt gleichzeitig sicher, dass sich Benutzer, Zweigstellen, Standorte, Geräte und Multi-Cloud-Umgebungen weltweit in unmittelbarer Nähe zu diesen konvergenten Services befinden. SSE mit NewEdge bietet eine Reihe von Services an, darunter Next Generation Secure Web Gateway (NG-SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), SaaS Security Posture Management (SSPM), Cloud Security Posture Management (CSPM), Firewall-as-a-Service (FWaaS) und Data Loss Prevention (DLP). Borderless SD-WAN mit NewEdge stellt einen optimierten Weg für SaaS-Anwendungen und Mid-Mile-Services in der Cloud zur Verfügung. Die Kombination von NewEdge mit SSE und Borderless SD-WAN garantiert eine sichere und leistungsstarke Konnektivität für Cloud-, Web-, SaaS- und private Anwendungen.

Die Möglichkeiten künstlicher Intelligenz

Im Vergleich zum herkömmlichen SD-WAN können auf den Verwaltungsebenen von Borderless SD-WAN mehr KI-gesteuerte Prozesse implementiert werden. Unternehmen erhalten einen vollständigen Überblick über ihr Netzwerk und können dank KI in Echtzeit verfolgen, wie ein guter, sicherer Link für externe Geräte aussehen sollte, die sich mit

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

dem Netzwerk verbinden wollen. KI ist in der Lage, fehlerhafte Links zu erkennen und anhand des Kontextes und historischer Daten vorherzusagen, wann ein Link fehlerhaft werden könnte. KI und ML können bei solchen Problemen auch eine automatisierte Lösung bieten, z.B. Vorwärtsfehlerkorrekturen oder *automatisierte Link-Remediation* (eine Korrekturmaßnahme, die es Benutzern ermöglicht, automatisch auf einen besseren, aktuell verfügbaren Link auszuweichen, um eine zuverlässigere Verbindung zu erhalten). ML/KI können IoT-Geräte und deren Verhalten automatisch erkennen und problematische Geräte unter Quarantäne stellen.

Borderless SD-WAN bietet darüber hinaus wertvolle Flow-Analysen zur Anwendungsperformance im gesamten Netzwerk. In diesen Flows können Unternehmen jedes Gerät, das eine Anwendung nutzt, sowie die mit diesem Gerät verbundene Erfahrung verfolgen. Anhand dieser Daten werden automatisch Baselines ermittelt. Es bestimmt im Wesentlichen, wie eine „normale" Netzwerkperformance in Bezug auf Paketverluste oder Anwendungsflussstatistiken aussieht. Bei Baselines müssen auch die Zeit und die Netzwerkaktivität berücksichtigt werden, da Letztere je nach den normalen Geschäftszeiten der einzelnen Zweigstellen und Remote-Benutzer unterschiedlich sein kann.

Borderless SD-WAN hat auch eine integrierte „Flight-Tracker"-Ansicht, die jeden Benutzer und jede Zweigstelle Minute für Minute überwacht. Dadurch werden Probleme mit der Service-Level-Erfahrung sofort erkannt und Verstöße gegen die Service Level Agreements (SLA) der Dienstanbieter angezeigt. Der Flight Tracker vereinfacht die Verwaltung, da er Einblicke in Datenflüsse bietet (einschließlich des Ortes, an dem ein Fehler aufgetreten ist). Er weist auf Richtlinienverstöße hin und führt eine Anomalie-Erkennung durch.

Borderless SD-WAN bietet weit mehr als eine ML-basierte Fehleranalyse, damit Probleme bei Geräten in Zweigstellen tatsächlich behoben werden können. Dank seiner Auto-Discovery-Funktionen können zum Beispiel die Geräte identifiziert werden, die von der Zweigstelle oder vom Homeoffice aus auf Anwendungen zugreifen. Mithilfe des integrierten IoT-Managers kann die IT-Abteilung aus der Ferne eine Fehlerbehebung für diese Geräte durchführen, was die durchschnittliche Zeit bis zur Problemlösung erheblich verkürzt.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- Geschäftliche Vorteile von Borderless SD-WAN
- Vorteile für Endbenutzer
- Vorteile für Netzwerkexperten
- Kosteneinsparungen durch Borderless SD-WAN

Kapitel 4
Welche Vorteile bringt Borderless SD-WAN dem Unternehmen?

Borderless SD-WAN von Netskope bietet eine Reihe von Netzwerkfunktionen für die Bedürfnisse der modernen Welt. Es ist ein Software-Defined Wide Area Network (SD-WAN), das die heutigen Anforderungen hinsichtlich Mobilität, Flexibilität, integrierter Sicherheit und permanenter orts-, zeit- und geräteunabhängiger Verfügbarkeit erfüllt. So wie SD-WAN das WAN in die „One-to-Many"-Welt brachte, ermöglicht Borderless SD-WAN die Weiterentwicklung des Netzwerks für die „Many-to-Many"-Welt.

Von den Vorteilen dieser Umstellung profitieren nicht nur Netzwerkexperten. Sie sind jeden Tag im ganzen Unternehmen spürbar und verfügbar. Dies dürfte das Herz jedes Netzwerk-Freaks höherschlagen lassen!

Dieses Kapitel befasst sich mit den Vorteilen, von denen alle Benutzer täglich profitieren, sowie mit einigen fortgeschrittenen Funktionen für Netzwerkexperten, die für die Wartung der Technologie und Netzwerkinfrastruktur zuständig sind. Es soll aufzeigen, dass Borderless SD-WAN nicht nur eine Netzwerkfunktion ist, sondern auch leistungsstarke Konnektivität und nahtlos integrierte Sicherheit bietet. Damit ist Borderless

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

SD-WAN unverzichtba für Unternehmen, die jedem Anwender dasselbe Benutzererlebnis bieten möchten, unabhängig von seinem Aufenthaltsort..

Eine Plattform, eine Software, eine Richtlinie – ein einzigartiger Ansatz

Zunächst wollen wir einen Blick auf einige grundlegende Veränderung werfen, die Borderless SD-WAN für das gesamte Unternehmen bringt. Dieser Kontext ist für die weitere Analyse in diesem Kapitel von Bedeutung. Im Film hört man oft, dass jeder Mensch nach einem bestimmten Kodex oder einer persönlichen Philosophie leben sollte (dies scheint sowohl auf kriminelle Banden als auch gutwillige Aliens zuzutreffen). Dasselbe gilt auch für die Konnektivität. Beim Borderless SD-WAN lautet das Mantra „Power of One" (siehe Abbildung 4-1), ein Ansatz, der Unternehmen dabei hilft, ihre Abläufe zu optimieren.

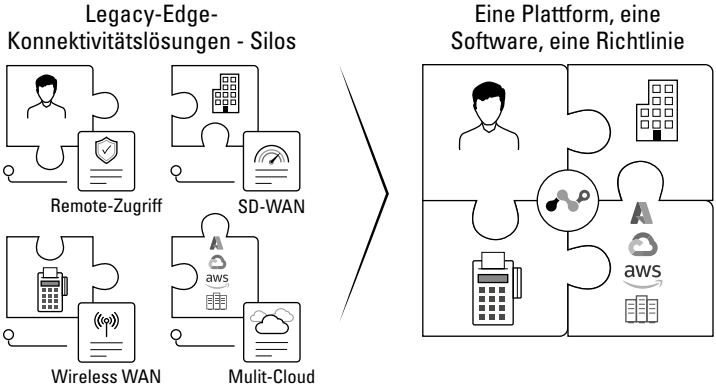

ABBILDUNG 4-1: Eine „Power-of-One"-Architektur kann für unterschiedliche Anwendungsfälle eingesetzt werden. Sie kann Netzwerk- und Sicherheitsfunktionen nahtlos integrieren, Kosten senken und Betriebsabläufe vereinfachen.

Diese „Power of One" manifestiert sich auf unterschiedliche Weise:

- **Es wird eine einheitliche Benutzererfahrung auf der Grundlage von Richtlinien geschaffen, die Benutzern unabhängig von ihrem Aufenthaltsort folgen.** Diese Einheitlichkeit wird durch eine kompakte Software gewährleistet, die überall dieselben SD-WAN-Funktionen bereitstellt – von einer Zweigstelle jeder Größe bis hin zu einem Laptop für das Arbeiten unterwegs. Dieselbe Software unterstützt auch Wireless-WAN-Funktionen, ermöglicht Multi-Cloud-Networking zur Vereinfachung der Konnektivität zwischen Anwendungen über mehrere

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Clouds hinweg, bietet intelligenten Zugriff auf das Internet der Dinge (IoT), um den Geschäftswerte vielfältiger Datenquellen zu erschließen, und ermöglicht die Fernüberwachung und Fehlersuche bei intelligenten Anlagen.

- **Alle Borderless SD-WAN-Lösungen werden über eine einzige Konsole verwaltet.**
- **Die Plattform integriert Netzwerk- und Sicherheitsfunktionen nahtlos und bietet einen sicheren, optimierten Zugang und ein einheitliches Benutzererlebnis, das gleichzeitig die Kosten für das Unternehmen reduziert und die Betriebsabläufe vereinfacht.**

Ein einheitliches Benutzererlebnis, das von einer einzigen umfassenden Plattform bereitgestellt wird, die eine gemeinsame Zero-Trust-Engine sowie gemeinsame DXM-Funktionen (Digital Experience Management) und Kontextinformationen für Netzwerk- und Sicherheitsservices nutzt: So stellt die „Power of One" letztendlich ein echtes Single-Vendor-SASE-Framework (Secure Access Service Edge) zur Verfügung (mehr dazu später in diesem Kapitel).

Klingt gut, oder? Das ist aber erst der Anfang. Lassen Sie uns mit den Vorteilen für Endbenutzer beginnen und dann den umfassenderen Nutzen von Borderless SD-WAN-Lösungen für die Netzwerkbetriebsteams und das Unternehmen insgesamt beleuchten.

Borderless SD-WAN macht Endbenutzern das Leben leichter

Borderless SD-WAN kommt jedem Benutzer zugute, der von überall aus arbeiten möchten. Das kann ein Angestellter in einer Zweigstelle sein, ein Analyst, der von zu Hause aus mit seinem Laptop auf Unternehmensanwendungen in aller Welt zugreifen muss, oder ein Contact-Center-Agent, der einem Kunden einen optimalen Service bieten will. Sogar ein Techniker, der in einem Fahrzeug auf einer Bohrinsel in einem Ölfeld arbeitet, kann davon profitieren. Zu den Vorteilen, die Borderless SD-WAN Geschäftsanwendern im Arbeitsalltag bringt, gehören unter anderem:

- **Flexibilität und Auswahlmöglichkeiten:** Benutzer können an jedem beliebigen Ort arbeiten (in einer Zweigstelle oder an einem dezentralen Ort, z. B. im Homeoffice, in einem Café, im Wohnmobil oder im Hotel) und erhalten überall dieselben SASE-Funktionen (SD-WAN und Security Service Edge [SSE]).
- **Optimierte Konnektivität:** Jeder Benutzer erhält einen hochperformanten Zugriff auf mehrere Clouds und Rechenzentren. Performance- und QoS-Probleme (Quality of Service) gehören damit der

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Vergangenheit an Selbst anspruchsvolle Anwendungen wie Zoom und Microsoft Teams funktionieren hervorragend, auch wenn die Verbindungen nicht optimal sind.

- **Geschäftskontinuität:**</26> Ein umfassender, von einem SASE-Gateway und einem einheitlichen SASE-Client bereitgestellter Sicherheitsmechanismus verhindert durch potenzielle Cyberangriffe verursachte Geschäftsunterbrechungen. Die Sicherheit begleitet Benutzer überall hin On-Premises, in Zweigstellen und an Remote-Standorte.
- **Zero Trust-Zugriff:** Derselbe kontextbewusste Zero-Trust-Zugriff ist überall verfügbar, sodass alle Anwender die Unternehmensrichtlinien jederzeit und an jedem Ort einhalten. Das System sorgt dafür, dass die Richtlinien den Benutzern folgen und sich an ihren jeweiligen Kontext anpassen.
- **Einfache Problembehebung:** IT-Administratoren können Endbenutzer mithilfe von KI-gesteuerten Abläufen und auf maschinellem Lernen basierenden Erkenntnissen aus der Ferne bei der Problemlösung unterstützen, Diagnosen vornehmen und die durchschnittliche Zeit bis zur Abarbeitung von Support-Tickets verkürzen, wodurch die Produktivität der Endbenutzer erheblich gesteigert wird.

Mit Borderless SD-WAN verbessert sich das Benutzererlebnis dramatisch. Für mobile Benutzer, z. B. in Flottenfahrzeugen, verbindet das SASE-Gateway SD-WAN, Switching, Routing, Wi-Fi und Wireless miteinander und ermöglicht durch die nahtlose Integration mit SSE einen sicheren, optimierten Zugriff auf alle Unternehmensanwendungen, unabhängig vom Aufenthaltsort der Anwender.

Benutzer, die an Remote-Standorten arbeiten, erzielen dank der zuverlässigen Konnektivität eine höhere Produktivität, selbst wenn die Verbindung nicht optimal ist. Borderless SD-WAN erreicht dies durch die kontinuierliche Optimierung der Benutzerverbindung zu jeder Anwendung, auch bei anspruchsvolleren, zeitkritischen Sprach- und Videoanwendungen wie Zoom und RingCentral. Wenn bei der Nutzung dieser Anwendungen Latenz, Jitter oder Paketverluste auftreten, behebt Borderless SD-WAN die Situation so reibungslos, dass der Benutzer nicht einmal merkt, dass ein Problem aufgetreten ist. Diese konsistente, qualitativ hochwertige Benutzererfahrung und sichere Konnektivität wird für alle Clouds und Rechenzentren zur Verfügung gestellt, unabhängig vom Gerät oder Aufenthaltsort des Benutzers.

Darüber hinaus erhalten alle Benutzer einheitliche Sicherheits- und Netzwerkoptimierungsrichtlinien mit Endpoint SD-WAN und SSE, die alle in einen einheitlichen SASE-Client integriert sind, der auf dem Laptop des Benutzers läuft und somit auch an Remote-Standorten dasselbe Benutzererlebnis wie in den Zweigstellen bietet. Der Zugriff und die

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Produktivität der Benutzer werden nicht eingeschränkt, ganz gleich, ob sie im Büro, zu Hause, in einem Wohnmobil oder am Strand arbeiten. Sie erhalten überall dieselbe Sicherheit und hochperformante Konnektivität (können Sie hier ein Muster erkennen?). Die Anwendungserfahrung ist immer dieselbe.

Der Benutzer hat jetzt mehr Flexibilität und mehr Auswahlmöglichkeiten, was die Arbeitsweise und den Arbeitsort anbelangt. Er muss sich keine Gedanken darüber machen, wo er sich aufhalten und welches Gerät er benutzen sollte, sondern kann von überall aus auf dieselben Anwendungen zugreifen wie im Büro. Das ist eine beeindruckende Fähigkeit! Wenn Sie von einem Hotelzimmer aus über eine Internetverbindung ein Zoom-Meeting leiten möchten, kann Ihr Laptop zum SD-WAN-Gerät werden, das für die Optimierung auf der letzten Meile sorgt, um automatisch ein hervorragendes Videoerlebnis zu bieten.

SSE Software-as-a-Service (SaaS) Security Posture Management (SSPM) überwacht kontinuierlich die Zoom-Umgebungen, um Fehlkonfigurationen, die die Sicherheit beeinträchtigen könnten, zu erkennen und zu beheben. Dadurch wird die Einhaltung von Branchenstandards und gesetzlichen Vorschriften gewährleistet.

Das Beste ist jedoch, dass der Benutzer nicht einmal weiß, dass Optimierungs- und Sicherheitsmaßnahmen durchgeführt werden. Er bemerkt nur, dass seine Verbindung stabil, sicher und optimiert ist. Die Reichweite ist so groß wie nie zuvor, und die Konnektivität ist überall gesichert. Borderless SD-WAN wurde für die heutige „Many-to-Many"-Welt entwickelt.

Wie Netzwerkexperten von Borderless SD-WAN profitieren

Nun wollen wir uns ansehen, welche Vorteile Netzwerkexperten wie Sie mit Borderless SD-WAN erzielen können es sind mindestens acht!

Betriebliche Vorteile durch AIOps

Netzwerkarchitekten und Betriebsteams profitieren von Verwaltungsfunktionen, die Netzwerkoptimierung, Sicherheit und Transparenz zusammenführen und zukunftssicher machen. Eine einzige Benutzeroberfläche bzw. Konsole legt die Richtlinien fest und überwacht und unterstützt die Problemlösung für alle Standorte, Benutzer und Geräte im Netzwerk. Alle Zweigstellen und Benutzer erhalten dieselbe Erfahrung und werden auf dieselbe Weise verwaltet. Dieselbe Borderless SD-WAN- und SSE-Orchestrierung für Zweigstellen, einschließlich der kontextbewussten Zero Trust-Richtlinien, die heute von Netzwerkteams

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

durchgesetzt und verwaltet werden, kann jetzt auch auf einzelne Benutzer angewendet werden, die den einheitlichen SASE-Client verwenden. Dieselbe Unterstützung über eine einzige Oberfläche wird auch für Multi-Cloud-Networking, drahtloses WAN und intelligente IoT-Zugriffslösungen bereitgestellt.

Mit Zero-Touch-Provisioning ist Ihr gesamtes Netzwerk, einschließlich aller Benutzer, Geräte, Standorte und Clouds, in wenigen Minuten online. Richtlinien können für das gesamte Netzwerk festgelegt und dann über alle Borderless SD-WAN-Gateways und Endpunkte mit denselben SD-WAN- und SSE-Funktionen verteilt werden. KI und ML erleichtern Netzwerkexperten die Überwachung und Optimierung des Netzwerks, indem sie Anomalien bei der Bandbreitennutzung erkennen, eine automatische Fehlerbehebung ermöglichen, proaktiven Support bieten und wertvolle Einblicke in Datenströme und Richtlinien liefern

Die Ergebnisse sind greifbar. Dank der konsolidierten Ansicht ihrer wichtigsten Netzwerklösungen auf einer Konsole können Netzwerkbetriebsteams alle Aspekte der Netzwerküberwachung, -berichterstattung und -verwaltung optimieren und ihre Zeit effizient für strategisch wichtige Langzeitprojekte einsetzen, die einen Mehrwert für das Gesamtwachstum des Unternehmens bringen.

Mehr Effizienz und Flexibilität mit kontextbewusstem SD-WAN

Borderless SD-WAN bietet umfassende Transparenz über alle Daten und Anwendungen, die Teil eines hybriden Netzwerks sind, und verbindet alle Standorte, Remote-Benutzer, IoT-Geräte und Multi-Cloud-Umgebungen. Diese Anwendungstransparenz ist zur Unterstützung von Benutzern wichtig, die viele unterschiedliche Anwendungen nutzen, darunter SaaS und verschiedene private und geschäftliche Anwendungen in der Cloud oder On-Premises. Unternehmen benötigen heute ein Zero-Trust-fähiges, kontextbewusstes SD-WAN mit uneingeschränkter Transparenz und geeigneten Kontrollmechanismen, um Benutzern einen schnellen, zuverlässigen und sicheren Zugang zu allen Anwendungen und Geräten an jedem Standort zu ermöglichen.

Borderless SD-WAN ist in der Lage, den Datenverkehr auf allen Ports standardmäßig nach Anwendungen zu klassifizieren. Entscheidend ist, die beste QoS für unternehmenskritische Anwendungen bereitzustellen und zu verhindern, dass Ressourcen, Bandbreite und Betriebszeit für weniger wichtige Anwendungen verwendet werden. Da es Zehntausende von SaaS-Anwendungen gibt, sind Netzwerkbetriebsteams nicht in der Lage, QoS-Richtlinien für jede einzelne Anwendung zu konfigurieren. Netskope SASE unterstützt eine Datenbank mit über 60.000 Anwendungen (wie in

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Kapitel <1 und an anderer Stelle beschrieben), die nach einem Cloud Confidence Index (CCI) kategorisiert sind, der die Unternehmensreife jeder Anwendung bewertet. Der CCI hilft dabei, Anwendungen automatisch den QoS-Richtlinien der richtigen Ebene zuzuordnen. In Kapitel 5 werden wir im Zusammenhang mit SASE näher darauf eingehen.

Netskope verfügt über eine Datenbank mit QoS-Richtlinien, die Anwendungen auf der Grundlage des CCI und anderer Kriterien zugewiesen werden. Durch diese automatische Zuordnung verringert sich der manuelle Arbeitsaufwand für das Netzbetriebsteam erheblich, was zu wesentlich effizienteren Betriebsabläufen führt.

Die kontextbewussten Funktionen von Netskope können um die automatische Erkennung aller verwalteten und nicht verwalteten IoT-Geräte und Mikrosegmente erweitert werden, damit die mit einem kompromittierten Gerät verbundenen Risiken effektiv bewältigt werden.

Größere Produktivität und Benutzerfreundlichkeit durch gesicherte Anwendungsperformance

Borderless SD-WAN trägt zu einer größeren Produktivität und einer besseren Zusammenarbeit bei, da es einen äußerst zuverlässigen, optimierten Zugang zu allen Anwendungen bietet, einschließlich aller UCaaS-Funktionen (Unified-Communication-as-a-Service). Mit geringem Aufwand können Netzwerkexperten mithilfe von SD-WAN-Funktionen, die in einer Zweigstelle, in der Cloud und auf persönlichen Laptops ausgeführt werden, ein deutlich verbessertes Benutzererlebnis schaffen. Dabei spielt es keine Rolle, ob die Anwender im Homeoffice, in einer Zweigstelle, einem Hotel oder einem Café arbeiten. Borderless SD-WAN kann die Netzwerkperformance mit einem sekundenschnellen Failover in Szenarien mit mehreren Links oder On-Demand-Wiederherstellung verbessern, selbst über eine einzelne, instabile Breitband-Internetverbindung.

Zukunftssicherheit Ihrer Investition mit einem vollständig SaaS-basierten Controller

SD-WAN-Controller wurden früher von IT-Administratoren manuell On-Premises installiert. Dieser DIY-Ansatz (Do-it-yourself) lässt sich nur schwer implementieren und skalieren. Mit vollständig SaaS-basierten Borderless SD-WAN-Controllern, die fortschrittliches Routing wie Border Gateway Protocol (BGP) und Open Shortest Path First (OSPF) unterstützen, können Unternehmen schnell neue Standorte einrichten und Remote-Standorte anbinden. Dank dieser Cloud-Controller-Funktion

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

sind Netzwerkexperten in der Lage, problemlos von einem auf Tausende von Standorten und Hunderttausende von Anwendern und IoT-Anlagen zu skalieren. Dabei sind eine mühelose Konfiguration, Verwaltung und Transparenz über alle Standorte hinweg weltweit gegeben.

Netzwerkexperten können ihre Netzwerke beliebig vergrößern. Sie müssen die Kapazität (die Anzahl der im SD-WAN-Netzwerk unterstützten Standorte) nicht im Voraus bestimmen. Ein SASE-Gateway oder -Client kann immer dann hinzugefügt werden, wenn eine neue Zweigstelle oder ein Remote-Benutzer online geschaltet werden muss. Da der Controller als SaaS-Service läuft, ist eine unbegrenzte Skalierung möglich. Das Netzwerk kann nun nach Bedarf erweitert werden. Und schon ist Ihr Unternehmen zukunftssicher!

Größere Reichweite und Flexibilität mit Wireless WAN

Die Geschäftswelt erstreckt sich heute weit über die Grenzen herkömmlicher kabelgebundener Netzwerke. Die Verfügbarkeit von Mobilfunkverbindungen garantiert Ihnen jedoch nicht, dass Sie die Konnektivität, QoS und Sicherheit erhalten, die für den Betrieb eines modernen Unternehmens erforderlich sind. Mit den Cloud-verwalteten Wireless-Gateways von Borderless SD-WAN können Sie Drahtloskonnektivität in ein stabiles, sicheres und optimiertes Netzwerk verwandeln, ganz gleich, ob Sie ein Ad-hoc-Netzwerk an einem Remote-Standort oder in einem temporären Büro einrichten oder schnelle, zuverlässige und unkomplizierte Drahtloskonnektivität bereitstellen möchten.

Das Borderless SD-WAN Wireless Gateway kann in Ihre bestehende Infrastruktur integriert und mit jeder SD-WAN-Lösung für primäre oder Backup-Mobilfunkunterstützung verbunden werden. Dies erleichtert die schnelle Erstellung von Netzwerkservices und erhöht die Produktivität und geschäftliche Agilität.

Transformation des Unternehmens mit SASE aus der Cloud

Mit herkömmlichen SD-WANs ist es schwierig, eine umfassende Transparenz und optimierte On-Ramps von jedem Benutzer oder Standort zu jeder Cloud, SaaS- oder privaten Anwendung zur Verfügung zu stellen. Selbst mit einer „kreativen“ Kombination aus „DIY“-SD-WAN-Hub-Installationen werden Provider-Umgebungen mit Latenzen belastet und bieten keine hochperformante Konnektivität. Hier ist die Qualität der Netzwerkinfrastruktur von entscheidender Bedeutung.

Netskope NewEdge ist die bestvernetzte Security Private Cloud der Welt. Sie deckt über 70 Regionen ab und führt Netzwerk- und

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Sicherheitsservices in großem Maßstab zusammen. NewEdge bietet global verteilte On-Ramps mit geringer Latenz, verfügt über umfangreiche Peerings und stellt in jeder Region volle Rechenleistung zur Verarbeitung des Datenverkehrs zur Verfügung. Die Infrastruktur steht 99,999 Prozent der Zeit zur Verfügung („Fünf Neunen") und bietet die besten Service Level Agreements (SLAs) der Branche. Das NewEdge-Netzwerk sorgt dafür, dass sich jeder Benutzer, jede Zweigstelle, jeder Standort, jedes Gerät und jede Multi-Cloud-Umgebung rund um den Globus in der Nähe von konvergentem Borderless SD-WAN mit SSE-Services befindet. Borderless WAN Cloud Hubs und SSE in einer global verteilten NewEdge-Infrastruktur bieten eine Reihe von Vorteilen:

- **Netskope Borderless SD-WAN mit NewEdge weitet die SD-WAN-Fabric von On-Premises-Standorten auf alle SaaS- und Cloud-Ressourcen aus.** Wenn z.B. Endpoint SD-WAN mit einem einheitlichen SASE-Client verwendet wird, kann der Zoom-Datenverkehr für einen Benutzer an einem Remote-Standort genauso optimiert werden wie für einen Benutzer in einer Zweigstelle des Unternehmens, der das Netskope SASE-Gateway verwendet. Ein weiteres Beispiel ist die Nutzung eines Middle-Mile-Service, der geografisch verteilte Zweigstellen mit einer Anwendung verbindet, die sich in der Zentrale auf einem anderen Kontinent befindet.
- **Durch die nahtlose Integration mit SSE bietet Borderless SD-WAN einen umfassenden Schutz vor sämtlichen Cybersecurity-Bedrohungen und ein Hochleistungsnetzwerk, das einen unterbrechungsfreien Geschäftsbetrieb gewährleistet.**
- **Borderless SD-WAN kann genutzt werden, um über mehrere Cloud-Umgebungen wie Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) verteilte Unternehmensressourcen in eine einheitliche Netzwerkstruktur einzubinden.** Durch fortschrittliches Routing und die native Integration mit Cloud-Anbietern kann Borderless SD-WAN unterschiedliche von diesen Anbietern abgedeckte Regionen verbinden und ermöglicht die Integration mit Netskope Intelligent SSE für Cloud-Workloads mit einem einzigen Klick.

Mithilfe dieser von Borderless SD-WAN bereitgestellten Funktionen können Unternehmen ihre Cloud-Nutzung mit leistungsstarker Konnektivität und dem richtigen Sicherheitsniveau beschleunigen. Sie müssen sich auch keine Sorgen mehr darüber machen, dass einige Ressourcen vor Ort und andere in der Cloud gehostet werden. Die schrittweise Migration zusätzlicher Infrastruktur in die Cloud wird vollständig unterstützt, ohne dass die Einschränkungen der bestehenden SD-WAN-Landschaft berücksichtigt werden müssen. Herkömmliche SD-WANs bieten nur eine

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

begrenzte Unterstützung für mehrere Clouds, was zu erheblichen logistischen Problemen führt – etwas, das Netzwerkexperten unbedingt vermeiden wollen.

NICHT VERGESSEN

Mit Borderless SD-WAN können Unternehmen bestimmen, wie jede Cloud mit jeder anderen Cloud kommuniziert und interagiert. Das ist eine großartige Cloud-Strategie für Unternehmen!

Absicherung des Unternehmens mit vollständigem SASE-Schutz

Borderless SD-WAN bietet ein vollständiges Paket an integrierten Sicherheitsfunktionen. Aus Netzwerksicht bietet Borderless SD-WAN hybride Netzwerksicherheit am Edge durch die Einbindung von Services wie Firewalls und Intrusion Prevention System (IPS) zur East-West-Segmentierung. Durch die Integration mit Netskope Intelligent SSE erhalten Sie einen vollständigen Schutz mit Funktionen für Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), Data Loss Prevention (DLP), SSPM, Cloud Security Posture Management (CSPM), Cloud Firewall und anderen Sicherheitsservices.

Die Netzwerk- und Sicherheitsservices der SASE-Lösung von Netskope basieren auf NewEdge, einer schnellen, zuverlässigen und konvergenten Cloud-nativen Plattform, die die umfassendste geografische Abdeckung in der Branche bietet (über 70 Regionen). Für die überwiegende Mehrheit der globalen Wissensarbeiter bedeutet dies eine Latenzzeit im einstelligen Millisekundenbereich. Unternehmen werden vor Cyberangriffen jeder Art und vor Datenexfiltration geschützt. Unterbrechungen werden auf diese Weise verhindert und Markenimage wird nicht geschädigt. SASE-Gateways und -Clients wählen automatisch den optimalen SSE-PoP (Point of Presence) für höchste Sicherheit und Optimierung aus. Netzwerkexperten begrüßen die Möglichkeit, SSE mit einem Klick sowohl für Zweigstellen als auch für Remote-Benutzer bereitzustellen. Das Ergebnis ist ein neues Konzept für die Konnektivität in der Cloud, das Unternehmen zu einer einzigartigen geschäftlichen Agilität verhilft.

Den Geschäftswert von Daten mit Edge Computing freisetzen

Borderless SD-WAN unterstützt Edge-Computing-Funktionen und bietet die Möglichkeit, sofort einsetzbare Containerservices wie Azure IoT Edge Runtime, Digital Experience Management usw. auszuführen. IT-Administratoren können einen Service aus einem Katalog auswählen oder ihre eigenen benutzerdefinierten Anwendungen einbringen. Mit ALM-Funktionen (Application Life-Cycle Management) können Unternehmen diese Services in großem Maßstab einführen und die jeweiligen Anwendungen

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

mit einem einzigen Klick auf Tausenden von SASE-Gateway-Geräten bereitstellen.

Senkung der IT-Gesamtkosten

Die von Borderless SD-WAN gebotenen Vorteile sorgen außerdem für einen konsolidierten Netzwerk-Footprint. Eine einzige, zentralisierte Lösung ersetzt das Multi-Vendor-SD-WAN durch das Produkt eines einzigen Anbieters. Es dürfte nicht überraschen, dass die Nutzung von weniger Anbietern mit deutlich niedrigeren Kosten für den Netzwerksupport einhergeht. Die Kosten, die für die Schulung des Betriebspersonals für zahlreiche Punktlösungen anfallen, können schnell die Investitions- und Betriebsausgaben für diese Produkte übersteigen.

Mit Borderless SD-WAN können isolierte, nicht integrierte Lösungen beseitigt werden, um Kosten zu sparen und eine höhere Investitionsrendite zu erzielen. Borderless SD-WAN reduziert die Komplexität, da mehrere Produkte und Konsolen durch eine einzige, kompakte Software ersetzt werden, die die wichtigsten Kundenanforderungen erfüllt. Netzwerkexperten haben mit Borderless SD-WAN mehr Kontrolle. Wir sind zwar keine Kontrollfreaks, aber das klingt wirklich gut! Kontrolle gehört schließlich zu unserem Job. Durch die zentralisierte Cloud-native Verwaltung des gesamten Netzwerks reduziert Borderless SD-WAN den Verwaltungsaufwand erheblich.

Mit Borderless SD-WAN können Unternehmen Kapitalausgaben (CapEx) einsparen und den gesamten IT-Betrieb vereinfachen. Mit nur einer Konsole, einer Automatisierungslösung und einer Software, die das gesamte Netzwerk steuert, können Unternehmen ihre Ausgaben senken und ihren Return on Investment (ROI) erhöhen. Kunden, die mit den Technologien von Netskope Borderless SD-WAN eine konvergente Architektur aufgebaut haben, konnten beispielsweise mindestens das Zehnfache ihrer Gesamtbetriebskosten (TCO) einsparen.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- Die Sicherheitsherausforderungen des Software-Defined Wide-Area-Netzwerks (SD-WAN)
- Vereinigung von Networking und Sicherheit mit Secure Access Service Edge (SASE)
- Der erfolgreiche Weg zu SASE

Kapitel 5
Beschleunigung der SASE-Einführung

Jetzt ist es an der Zeit, über die Integration der Sicherheit in das Netskope Borderless SD-WAN im Rahmen einer umfassenderen SASE-Architektur zu sprechen. Die Entwicklung von SASE wurde von Unternehmen vorangetrieben, die sich durch digitale Innovationen von ihren Mitbewerbern differenzieren wollten. Dadurch stieg der Bedarf an neuen digitalen Lösungen wie Cloud Computing und die Konvergenz von Netzwerk- und Sicherheitsfunktionen auf Produkt-, Architektur- und Unternehmensebene.

SASE kombiniert dabei Konzepte wie Zero Trust, SD-WAN und Security Service Edge (SSE). Dies führt zu einer neuen Sicherheits- und Netzwerkstrategie, die die Cloud und die neue Work-from-anywhere-Umgebung schützt und steuert. Zur Realisierung von SASE müssen sowohl das Netzwerk als auch die Sicherheit softwaredefiniert sein und aus der Cloud bereitgestellt werden. Die Realisierung von SASE erfordert die Konsolidierung und Integration von Sicherheitsmechanismen – darin liegt der Kern von SSE.

SSE verlagert kritische Prüf- und Kontrollpunkte in die vom Unternehmen genutzte(n) Cloud(s). Die Sicherheit ist nun dort angesiedelt, wo sich Daten, Anwendungen und Benutzer befinden – und wo Gefahren lauern. SSE lässt sich gut mit Borderless SD-WAN kombinieren, da es softwaredefiniert ist und seine kritischen Services direkt aus der Cloud

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

bereitgestellt werden. Dadurch wird die Konnektivität für jeden Benutzer, jedes Gerät, jeden Standort, jede Anwendung und jeden Teil der Unternehmensinfrastruktur optimiert, ohne dass der Geschäftsbetrieb eingebremst wird.

Durch die Verbindung von SD-WAN mit SSE erhalten Unternehmen die für ein wahrhaft sicheres Borderless SD-WAN erforderliche SASE-Lösung. Dieses Kapitel befasst sich mit den Sicherheitsproblemen, die in einer herkömmlichen SD-WAN-Umgebung auftreten können, und den neuen Technologien, mit deren Hilfe Unternehmen auch in einer Cloud-Architektur eine hohe Sicherheit erreichen.

Das Sicherheitsproblem von SD-WAN vor der Entwicklung von SASE

Borderless SD-WAN befähigt moderne Belegschaften, überall und mit jedem beliebigen Gerät zu arbeiten. Benutzer müssen in der Lage sein, auf jede von ihnen benötigte Anwendung zuzugreifen. Diese Anwendungen können sich heute an den unterschiedlichsten Orten befinden. Deshalb müssen sich Benutzer darauf verlassen können, dass sie unabhängig von ihrem Aufenthaltsort und den von ihnen genutzten Anwendungen Zugriff auf die wichtigsten Unternehmensfunktionen haben und dabei ein gleichbleibend gutes Benutzererlebnis erhalten. Aber auch diese Benutzer, Geräte, Websites und Anwendungen müssen vollständig abgesichert werden. Aus diesem Grund ist für Borderless SD-WAN ein geeigneter Sicherheitsstack vonnöten, der jeden Benutzer, jedes Gerät, jeden Standort, jede Anwendung und jeden Teil der Unternehmensinfrastruktur schützt.

Um die mit der nahtlosen Integration von Sicherheitsfunktionen in Borderless SD-WAN verbundenen Herausforderungen besser verstehen zu können, lohnt es sich, zunächst über das herkömmliche SD-WAN und seine Sicherheitsfunktionen in der Vergangenheit und Gegenwart nachzudenken.

Beim herkömmlichem SD-WAN werden alle Verbindungen von den physischen Grenzen einer Zweigstelle heraus hergestellt und gehen von dort zu einem oder mehreren Infrastructure-as-a-Service (IaaS)-, Platform-as-a-Service (PaaS)- oder Software-as-a-Service (SaaS)-Anbietern und einem Unified-Communication-as-a-Service (UCaaS)-Anbieter. Was das für Verbindungen sind, hängt von den Bedürfnissen der Benutzer und den Anwendungen ab, auf die sie zugreifen wollen. Eines der Hauptprobleme herkömmlicher SD-WANs war die Gewährleistung der Sicherheit. Die Sicherheit war die sprichwörtliche Achillesferse des herkömmlichen SD-WAN. An dieser Stelle sei ein wichtiger Punkt erwähnt: Das

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

herkömmliche SD-WAN kann nur einige tausend Anwendungen erkennen, priorisieren und schützen. In einer Zeit, in der die Zahl der Anwendungen ständig zunimmt, ist dies eine erhebliche Einschränkung.

Zunächst funktionierte das alles gut ...aber dann eben nicht mehr!

Als sich die Grenzen des Unternehmens auflösten, veränderte sich der Perimeter und dehnte sich über Zweigstellen hinweg aus. Er umfasste nun auch Mikrozweigstellen, Remote-Standorte, an denen sich Benutzer aufhielten, und IoT-Geräte (Internet-of-Things), die sich über alle Multi-Cloud-Edges erstreckten. Für alle diese Dinge gibt es eine gemeinsame Anforderung: Sie müssen geschützt werden. Netzwerkarchitekten begannen damit, mehrere punktuelle Sicherheits- und Konnektivitätsprodukte für diese neu entstandenen Grenzen oder Perimeter einzusetzen. Dieser Ansatz führte zu einem Netzwerk voller ungleichartiger und unzusammenhängender Technologien, die irgendwie zusammenwirken mussten. Das Ergebnis erwies sich oft als äußerst kompliziert, sowohl aus Sicht der Endnutzer als auch der ITOps. Eine fragmentierte Architektur kann Sicherheits- oder QoE-Richtlinien (Quality-of-Experience) nicht einheitlich auf alle Benutzer, Geräte, Standorte und Clouds anwenden. Hinzu kommt, dass sich Zehntausende von neuen Anwendungen nun in der Cloud befinden – ein Modell, für das das herkömmliche SD-WAN einfach nicht ausgelegt ist. Und bekanntlich kann man Dinge, die man nicht erkennen kann, weder priorisieren noch schützen. Herkömmliche SD-WANs hatten Probleme mit den vielen neu hinzukommenden Anwendungen, da sie sie nicht erkennen konnten!

Außerdem gab es keine Transparenz und granulare Kontrolle über das IoT, wodurch Unternehmen zusätzlichen Risiken ausgesetzt sind. Herkömmliche SD-WANs konnten die Auswirkungen kompromittierter Geräte nicht eindämmen. Zur Bereitstellung von SD-WAN-Services, die den heutigen Anforderungen von Unternehmen am Edge und im gesamten WAN gerecht werden, musste daher zusätzlicher Kontext mit Zero-Trust-Sicherheit in das Modell integriert werden.

Um bei SD-WANs eine umfassende Sicherheit zur Abwehr von Cyberangriffen zu erzielen, mussten einige Unternehmen den gesamten Datenverkehr an einen zentralen Standort weiterleiten, zum Beispiel ein Rechenzentrum. Von dort aus konnten sie sich mit dem Internet und mehreren Clouds verbinden, um IaaS-, PaaS- und SaaS-Services in Anspruch zu nehmen. Es gab zwar Sicherheitsmechanismen, aber die Benutzerfreundlichkeit wurde durch die mit dem Backhauling verbundenen Latenzprobleme beeinträchtigt. Um Backhauling und die damit verbundenen Latenzzeiten zu vermeiden, entschieden sich einige Unternehmen für eine verteilte Sicherheitslösung an jedem Standort. Andere ergänzten ihre bestehenden SD-WAN-Lösungen mit eigenständigen Sicherheitsgeräten. Manche Unternehmen setzten aufwändige Services

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

ein und verknüpften mehrere Geräte miteinander. Dadurch entstanden so genannte „Fat SD-WAN"-Lösungen, die kostspielig waren uns sich schwer verwalten und skalieren ließen. Einige SD-WAN-Anbieter mit elementaren Firewall-Fähigkeiten begannen, den Begriff *ausreichende Sicherheit* auf Zweigstellenebene zu verwenden. Eine „ausreichende" Netzwerksicherheit kann die bestmögliche Sicherheit nicht ersetzen, die Unternehmen so dringend benötigen.

Die Zusammenführung der Netzwerk- und Sicherheitsfunktionen für alle Remote-Benutzer, Zweigstellen, IoT- und Multi-Cloud-Umgebungen war ein enormer Balanceakt – und das ist noch stark untertrieben. Es war eine wahre Sisyphusarbeit. Stellen Sie sich vor, sie müssten den gesamten Sand von einem Strand wegtragen, aber Sandkorn für Sandkorn! (Wir wollten so viele Metaphern wie möglich in zwei Sätzen unterbringen, und das ist uns offensichtlich gelungen.)

Sicherheit aus der Cloud ebnet den Weg für SASE

Die Einführung und zunehmende Beliebtheit von Sicherheitslösungen aus der Cloud veranlasste viele SD-WAN-Anbieter zu einem Strategiewechsel. Sie begannen, mit den Cloud-Sicherheitsanbietern zusammenzuarbeiten, um die mit dem direkten Internetzugang über die Cloud verbundenen Risiken zu minimieren. Dieser Ansatz unterschied sich erheblich von dem bisherigen Verfahren, bei dem der SD-WAN-Traffic zur Sicherheitsprüfung durch die Rechenzentren des Unternehmens geleitet wurde (Hairpinning), was zu hohen Latenzzeiten oder zur Verteilung eines kompletten Sicherheitsstacks auf alle Zweigstellen führte.

Mit der Zeit erwies sich die Cloud-basierte Sicherheit als der beste Ansatz, und diese Erkenntnis ebnete den Weg für SASE. Viele Unternehmen wollen ihre Netzwerk- und Sicherheitsarchitekturen vereinheitlichen, um Arbeitsabläufe zu optimieren und die gemeinsame Nutzung von Kontextinformationen zwischen dem SD-WAN und Cloud-basierten Sicherheitslösungen zu ermöglichen, was letztendlich zu effektiveren und genaueren Kontrollen führt.

SASE: Die Vereinigung von Networking und Sicherheit

SASE und SSE verlagern die Sicherheit in die Cloud und machen sie dadurch effektiver als je zuvor. SSE bringt alle für SASE erforderlichen Sicherheitskomponenten, die zuvor aus separaten Anwendungen, Produkten oder Services von oftmals unterschiedlichen Anbietern bestanden,

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

in einer einheitlichen, integrierten Form zusammen, die mehr Möglichkeiten bietet, Effizienz erhöht und Komplexität sowie Kosten reduziert. SASE ist ein umfassendes Programm für den Umzug von Netzwerk- und Sicherheitsfunktionen in die Cloud. SSE konsolidiert alle erforderlichen Sicherheitsfunktionen, während Borderless SD-WAN alle erforderlichen Netzwerkfunktionen konsolidiert. Networking und Sicherheit werden dann von SASE konvergiert.

SASE bietet eine Reihe von integrierten Netzwerk- und Sicherheitsservices, die zum zentralen Kontrollpunkt für den gesamten Datenverkehr werden und eine konsistente Sicherheit für alle Benutzer, Daten, Geräte, Standorte und Anwendungen gewährleisten. SASE verbindet alle „Sinnesorgane" des Netzwerks und der Sicherheit mit einem einzigen Gehirn, das die Daten miteinander verknüpft, optimiert, interpretiert, das Ausmaß von Risiken erkennt und jederzeit in jedem Szenario die richtige Zugriffsebene bestimmt.

Netskope Intelligent SSE macht sich die Vorteile der Cloud in vollem Umfang zunutze. Es integriert unternehmenskritische Sicherheitsfunktionen wie Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), Data Loss Prevention (DLP), Cloud Security Posture Management (CSPM), SaaS Security Posture Management (SSPM), Digital Experience Management (DEM), Firewall-as-a-Service (FWaaS) usw. und sorgt dafür, dass sie optimal zusammenarbeiten. Durch Ein-Klick-Integration und Netskope NewEdge kann Borderless SD-WAN die Bereitstellung dieser SSE-Services möglichst nah am Zugriffspunkt von Personen, Daten und Anwendungen unterstützen. Die weltweit verteilten Points of Presence (PoPs) von NewEdge sorgen für eine möglichst geringe Latenz, sodass Benutzer jederzeit und überall auf jede gewünschte Anwendung zugreifen können. Dadurch werden eine hohe Performance und eine hochwertige Konnektivität gewährleistet, die die Einführung von SASE beschleunigen. Netskope NewEdge stellt auch Sicherheit mit SSE und On-Ramp zu jeder Cloud mit Borderless SD-WAN zur Verfügung. Dies schließt die Optimierung von geschäftskritischen UCaaS-Anwendungen ein.

Wie sieht es mit dem Edge aus, wo das SASE-Gateway angesiedelt ist und wo sich Benutzer und Geräte befinden? Das von der Borderless SD-WAN-Software unterstützte SASE-Gateway bietet standardmäßig fortschrittliches Layer 7-Firewalling und ein Intrusion Prevention System (IPS).

Der folgende Abschnitt geht näher auf die integrierten Sicherheitsfunktionen von Netskope SASE ein:

- **Klassifizierung:** Identifiziert und kennzeichnet sensible Informationen, idealerweise bei ihrer Erstellung, aber auch durch regelmäßige Scans von Datenspeichern.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

- **CASB:** Dient als Policy Enforcement Point, der zwischen den Verbrauchern und den Anbietern von Cloud-Services eingerichtet wird, um die Sicherheitsrichtlinien des Unternehmens beim Zugriff auf Cloud-basierte Daten oder Anwendungen durchzusetzen.
- **SWG:** Kontrolliert den Zugriff und schützt nur vor Web-Bedrohungen. Das Next-Generation SWG von Netskope bietet Funktionen zum Schutz vor Cloud-basierte Bedrohungen und Datenrisiken für persönliche Instanzen verwalteter Anwendungen, Tausende von Schatten-IT-Anwendungen und Cloud-Services.
- **ZTNA:** Setzt das Prinzip durch, dass keiner Instanz implizit vertraut bzw. Zugriff auf Unternehmensressourcen gewährt werden darf, bevor ihre Legitimität überprüft und bestätigt wurde. Beim Least-Privilege-Ansatz erhalten Benutzer nur Zugriff auf die Ressourcen, die sie tatsächlich benötigen – mehr nicht.
- **Remote browser isolation (RBI):** Trennt die Browser-Aktivität von den Endgeräten der Arbeitskräfte. Alle Browser-Aktivitäten werden in einem entfernten, Cloud-basierten Container gehostet und ausgeführt. Durch dieses Sandboxing werden Daten, Geräte und Netzwerke beim Browsen von Websites vor den unterschiedlichsten Bedrohungen geschützt.
- **FWaaS:** Bietet Netzwerksicherheit für alle ausgehenden Ports und Protokolle für einen sicheren, direkten Internetzugang über einen Agenten auf verwalteten Geräten oder Generic Routing Encapsulation (GRE) und Internet Protocol Security (IPsec).
- **DLP:** DLP verhindert die absichtliche und versehentliche Datenexfiltration durch bewussten oder unbeabsichtigten Datenmissbrauch. Netskope DLP ermöglicht die genaue Erkennung aller sensiblen Daten in jeder Form mit dem geringstmöglichen Fehlerpotential.
- **Bedrohungserkennung und Neutralisierung (auch als Advanced Threat Protection [ATP] bekannt):** Erkennt Anzeichen dafür, dass eine Umgebung kompromittiert wurde, und führt Maßnahmen durch, um die Wahrscheinlichkeit künftiger Angriffe zu verringern oder zu beseitigen.
- **CSPM:** Cloud Security Posture Management identifiziert und korrigiert Fehlkonfigurationen zwischen Unternehmen und den IaaS-Cloud-Umgebungen von Cloud-Service-Anbietern (CSP) wie Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP).
- **SSPM:** Bewertet die Konfiguration von SaaS-Anwendungen und beseitigt Fehlkonfigurationen, die Exfiltration, Impersonation oder andere Arten von Angriffen ermöglichen könnten.
- **On-Premises-Sicherheit:** Sicherheitsservices können auch On-Premises eingesetzt werden. Mit dem Borderless SD-WAN SASE-Gateway

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

kann East-West-Traffic auch die On-Premises Next-Generation Firewall (NGFW), IPS/Intrusion Detection System (IDS) usw. nutzen.

SASE ist eine Reise: Es gilt, sich erfolgreich durch die Landschaft zu navigieren

Eine robuste SASE-Architektur, die Borderless SD-WAN integriert, kann je nach den Anforderungen des Unternehmens viele Formen annehmen. Die erfolgreiche Umsetzung von SASE bringt per Definition weniger Anbieter, einfachere Abläufe, geringere Komplexität, niedrigere Kosten und eine schnellere, stabilere Netzwerkleistung mit umfassender Sicherheit mit sich. Eine dermaßen umfassende Verbesserung lässt sich nicht in einem Zug erreichen.

NICHT VERGESSEN

SASE ist eine Reise und keine Hau-Ruck-Aktion; die Konsolidierung von Anbietern nimmt in der Regel Zeit in Anspruch.

Viele Unternehmen nutzen bereits Cloud-basierte Sicherheitsprodukte von SSE-Anbietern und können das SD-WAN auswählen, das sich am besten in ihre vorhandenen Sicherheitslösungen einfügt. Wenn ein Unternehmen schon über ein Borderless SD-WAN-Produkt verfügt, kann es dieses in die von ihm gewählte Cloud-basierte Sicherheitslösung integrieren. Es gibt keinen richtigen oder falschen Ansatz. Am wichtigsten ist die Frage, welche Bedürfnisse das Unternehmen hat und wie es seine Geschäftsziele am besten erreichen kann.

In den folgenden Abschnitten werden die entscheidenden Vorteile einer Single-Vendor-SASE-Lösung beschrieben. Wir empfehlen, diese Punkte zu berücksichtigen, bevor Sie eine Entscheidung treffen. Manchmal kann 1 + 1 mehr als 2 ergeben.

Zero-Trust-basiertes, kontextbewusstes SASE

In der Cloud-Ära reicht Transparenz allein nicht mehr aus. Auch bei einem Bild mit höchster Auflösung kann man kleine Details übersehen, wenn man nicht weiß, wohin man schauen muss oder wonach man eigentlich sucht. Ein auf Benutzer, Geräte, Anwendungen und die damit verbundenen Risiken ausgerichteter, umfangreicher Kontext ist eine unabdingbare Voraussetzung für die Festlegung granularer SASE-Richtlinien. Ein solcher Kontext ist auch für die Umsetzung von Zero Trust entscheidend.

Der Kontext für die Netzwerk- und Sicherheitsfunktionen von Netskopes SASE kommt aus der Netskope Cloud XD (Xtreme Definition), auf der die Zero Trust Engine basiert. Als Teil der Netskope SASE-Architektur nutzt SSE von Netskope dieselbe Zero Trust Engine wie Borderless SD-WAN.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Dadurch können Kontextinformationen von konvergenten Sicherheits- und Netzwerkservices gemeinsam genutzt werden, und es gibt granulare Richtlinien, die auf der Erkennung von Anwendungen, Geräten und Benutzern sowie der Identifizierung der mit ihnen verbundenen Risiken basieren.

Netskope SSE und Borderless SD-WAN nutzen zum Beispiel eine gemeinsame Datenbank, um mehr als 60.000 Anwendungen zu identifizieren. Netskope bewertet jede Anwendung mit einem Cloud Confidence Index (CCI), der einen Score für die Unternehmensreife einer Anwendung liefert. Mit Netskope SSE können IT-Administratoren CCI nutzen, um die mit den unterschiedlichen Cloud-Services verbundenen Risiken zu bewerten und fundierte Entscheidungen über das Zulassen oder Sperren bestimmter Anwendungen in ihrer Umgebung zu treffen. Dies ermöglicht eine detaillierte Kontrolle über die Nutzung von Cloud-Services und gewährleistet die Einhaltung von Sicherheits- und Governance-Anforderungen. Borderless SD-WAN nutzt die von der CCI bereitgestellten Kontextinformationen, um für das Netskope SASE-Gateway sofort nutzbare, intelligente QoE-Standartwerte (Smart Defaults) festzulegen. Damit entfällt die komplizierte und zeitintensive Aufgabe, QoE-Regeln für Zehntausende von Anwendungen manuell zu konfigurieren. Durch die Nutzung von CCI-Informationen kann Borderless SD-WAN Netzwerkressourcen wie Bandbreite und Priorität dynamisch zuweisen und so eine optimale Leistung für wichtige Anwendungen sicherstellen (siehe Abbildung 5-1).

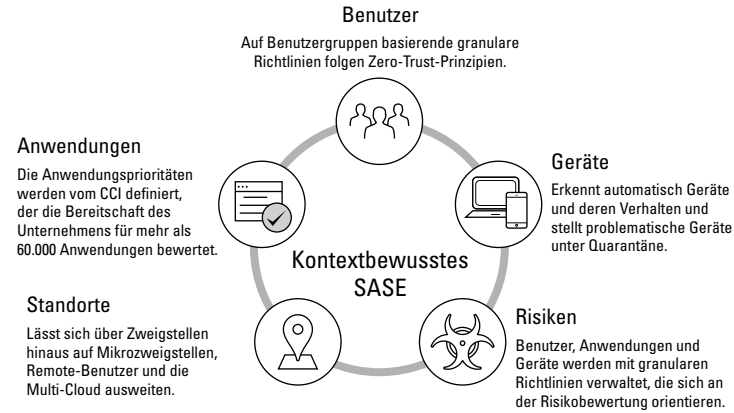

ABBILDUNG 5-1: Ein auf Benutzer, Geräte, Anwendungen und die damit verbundenen Risiken ausgerichteter, umfangreicher Kontext ist eine unabdingbare Voraussetzung für die Festlegung granularer SASE-Richtlinien.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Einheitliche Richtlinien und konsistente Benutzererfahrung an jedem Standort

Zweigstellen und Remote-Benutzer werden in den meisten Fällen nicht einheitlich behandelt. Bei der herkömmlichen SD-WAN-Unterstützung für Zweigstellenbenutzer gibt es weder Kontextbewusstsein noch Zero-Trust-Sicherheit. Das Borderless SD-WAN SASE-Gateway von Netskope hingegen ermöglicht die Nutzung von SD-WAN mit granularen Zero-Trust-Richtlinien und Kontextbewusstsein. Den üblicherweise zur Unterstützung von Remote-Benutzern verwendeten Virtual Private Networks (VPNs) fehlt es an Transparenz und Optimierungsmöglichkeiten. Netskope Endpoint SD-WAN hingegen erfüllt diese beiden Anforderungen. Mit Borderless SD-WAN und SSE-Integrationsfunktionen können moderne Unternehmen ein hochperformantes, kontextbewusstes SD-WAN sowohl für Zweigstellen als auch für Remote-Benutzer bereitstellen (siehe Abbildung 5-2).

Das Ergebnis ist ein einheitliches Richtlinien-Framework, das eine konsistente Erfahrung und Sicherheit bietet, die den Benutzern folgen. Mit Borderless SD-WAN können Netzwerkarchitekten und Betriebsteams eine einzige Plattform, Konsole und Richtlinie nutzen, um Richtlinien für Zweigstellen zu konfigurieren und zu verwalten, die jetzt auch für einzelne Benutzer an Remote-Standorten angewendet werden können. IT-Abteilungen von Unternehmen können nun Zweigstellen und einzelne Remote-Benutzer über eine einheitliche Zero-Trust- und Netzwerk-Performance-Richtlinie für die gesamte Unternehmensinfrastruktur verwalten, unabhängig davon, wo sich Ihre Benutzer, Anwendungen und Services befinden von einer einzigen, einheitlichen Plattform aus. Dieser einheitliche Ansatz sorgt für eine skalierbare Architektur, optimierte Abläufe, leistungsstarke Konnektivität und zuverlässige Sicherheit auf der Grundlage kontextbewusster Zero-Trust-Prinzipien.

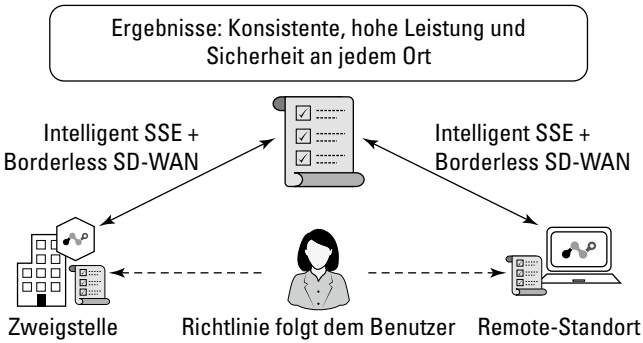

ABBILDUNG 5-2: IT-Teams können nun Zweigstellen und einzelne Remote-Benutzer über eine einzige, einheitliche Plattform mit einer einheitlichen Sicherheits- und Netzwerkleistungsrichtlinie verwalten, die dem Benutzer folgt.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

SASE aus der Cloud mit unübertroffener globaler Reichweite

Früher mussten Sicherheits- und Netzwerktechniker immer den bekannten Spagat zwischen mehr Sicherheit und besserer Leistung schaffen. Im Bereich der Netzwerksicherheit gibt es ein ungeschriebenes Gesetz: Man kann einfach nicht alles haben. Es gibt immer einen Kompromiss zwischen Leistung, Verfügbarkeit und Sicherheit. Die NewEdge-Plattform von Netskope bricht mit dieser Regel und erfüllt alle drei Anforderungen, ohne Kompromisse einzugehen.

Wie in Kapitel 3erwähnt, ist Netskope NewEdge heute mit einer weltweiten Abdeckung in mehr als 70 Regionen die führende Private Security Cloud. Es verbindet Netzwerk- und Sicherheitsservices erfolgreich und in großem Maßstab und bietet Traffic-On-Ramps mit niedriger Latenz, die den gesamten Globus umspannen. Dank umfangreicher Peering-Vereinbarungen und einer umfassenden Computing-Infrastruktur in jeder Region kann NewEdge den Datenverkehr effizient verarbeiten. Darüber hinaus garantiert Newedge eine überragende Verfügbarkeit von 99,999 Prozent („Fünf Neunen“)und die Einhaltung der branchenweit führenden Service Level Agreements (SLAs) für optimale Leistung und Zuverlässigkeit.

Mit dem NewEdge-Netzwerk (siehe Abbildung 5-3) kann jeder Benutzer, jede Zweigstelle, jeder Standort, jedes Gerät und jede Multi-Cloud-Umgebung auf der ganzen Welt nahtlos auf das integrierte Borderless SD-WAN mit SSE-Services zugreifen. Die in NewEdge verfügbaren SSE-Services umfassen ein breites Spektrum von Angeboten, darunter ein Next-Generation Secure Web-Gateway (NG-SWG), CASB, ZTNA, SSPM, CSPM, FWaaS und DLP. Die Netskope Borderless SD-WAN-Services im NewEdge-Netzwerk dehnen die Reichweite von SD-WAN effektiv auf SaaS- und Cloud-Ressourcen aus. Dies ermöglicht die Optimierung des Cloud-Datenverkehrs für Remote-Benutzer und Zweigstellen. Außerdem bietet es einen Mid-Mile-Service, der eine zuverlässige Konnektivität zwischen geografisch verteilten Zweigstellen und zentralisierten Anwendungen auf anderen Kontinenten ermöglicht.

Diese Kombination das NewEdge-Netzwerk, die SSE-Services und Borderless SD-WAN garantiert eine sichere und leistungsstarke Konnektivität für Cloud-, Web-, SaaS- und private Anwendungen. Unternehmen erhalten damit eine robuste Infrastruktur, die eine hervorragende Performance und einen geschützten Zugriff auf wichtige Ressourcen in unterschiedlichen Umgebungen ermöglicht.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

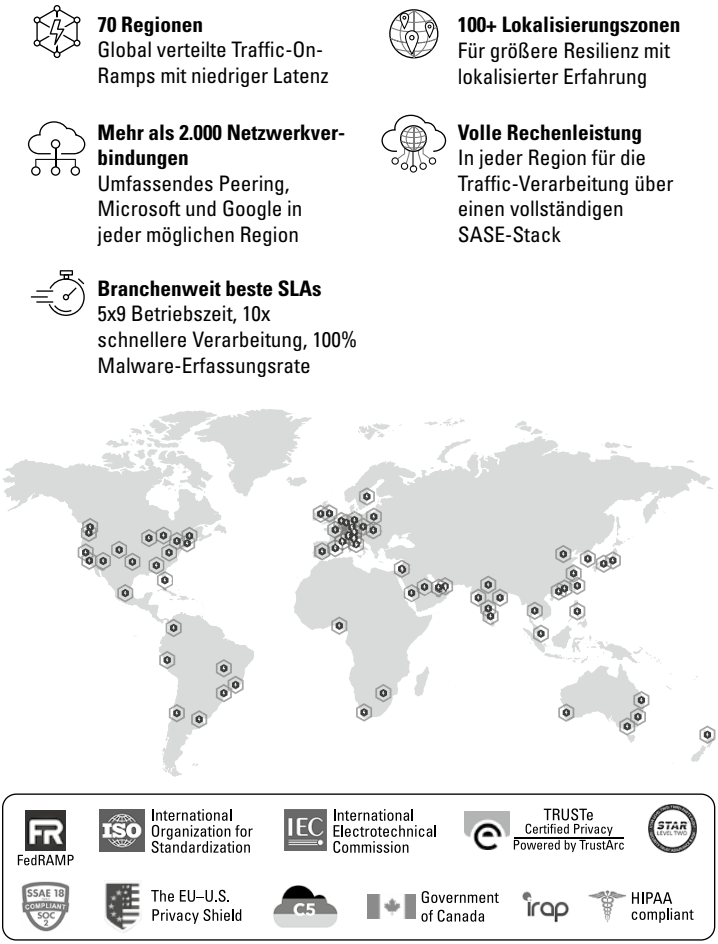

ABBILDUNG 5-3: NewEdge verbindet Netzwerk- und Sicherheitsservices in großem Maßstab und Traffic-On-Ramps mit niedriger Latenz, die sich über den gesamten Globus erstrecken.

Vereinheitlichung und Vereinfachung von ITOps

Benutzer, Geräte, Standorte und Clouds brauchen eine hohe Performance und sichere Any-to-Any-Verbindungen. Die bestehenden Ansätze resultieren in der Nutzung einer Vielzahl unterschiedlicher Einzelprodukte, die die Kosten und die Komplexität erhöhen. Mit seinem hochgradig integrierten Ansatz in Bezug auf Sicherheits- und Netzwerkservices bietet SASE wichtige Kostenvorteile.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Aus Netzwerk-Perspektive kann eine einzige, kompakte Borderless-SD-WAN-Software mehrere punktuelle Produkte überflüssig machen (z. B. SD-WAN für Zweigstellen, Fernzugriffs-VPN, Wireless-Gateways), Multi-Cloud-Edge usw.) und dadurch die Komplexität reduzieren (siehe Abbildung 5-4). SSE integriert mehrere Sicherheitsfunktionen in einem einzigen System, sodass es nicht mehr nötig ist, mehrere unterschiedliche Produkte zu verwenden, die keine Bedrohungsdaten miteinander austauschen können und dadurch die Sicherheitslage des Unternehmens beeinträchtigen. Wie bereits erwähnt, lassen sich Borderless SD-WAN und SSE nahtlos miteinander integrieren und nutzen dieselbe Zero-Trust-Engine. In Verbindung mit Anbieterkonsolidierung verringert SASE die Anzahl der Systeme, die überwacht und gewartet werden müssen, und führt zu einem verbesserten Netzwerkdesign, was wiederum die Betriebskosten senkt. Durch den Einsatz von künstlicher Intelligenz (KI) und die Automatisierung vieler Erkennungs- und Reaktionsprozesse wird die Anzahl der Support-Tickets reduziert und die durchschnittliche Zeit bis zur Lösung von Problemen erheblich verkürzt.

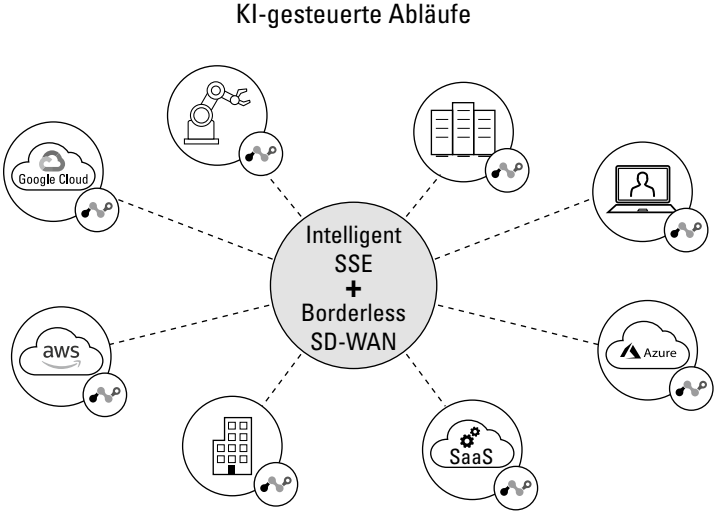

ABBILDUNG 5-4: SASE führt zur Konsolidierung mehrerer Anbieter, weniger zu überwachenden Systemen, einem einfacheren Netzwerkdesign und Kosteneinsparungen.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- Vielfältige Netzwerkarchitekturen zur Unterstützung des Unternehmens
- Nutzung einer für die Cloud entwickelten Lösung
- Sicherung und Optimierung der Konnektivität
- Intelligenter Netzwerkzugang und fortgeschrittenes Routing
- Umfassende Sicherheit für hybride Netzwerke
- Erstklassige Anwendungserfahrung an jedem Ort
- Größeres Kontextbewusstsein
- Künstliche Intelligenz (KI) und ihre Möglichkeiten
- Umsetzung einer Wireless-First-Strategie
- Flexibilität und Effizienz durch Container-Orchestrierung

Kapitel **6**

Die zehn wichtigsten Dinge, die Unternehmen für die Einführung von Borderless SD-WAN brauchen

Wenn Sie es bis hierher geschafft haben, denken Sie wahrscheinlich ernsthaft über die Einführung von Netskope Borderless SD-WAN nach, entweder jetzt oder in naher Zukunft. Wahrscheinlich fragen Sie sich angesichts aller aufgezeigten Möglichkeiten, in

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

welcher Hinsicht Borderless SD-WAN herkömmliche Software-Defined Wide Area Networks (SD-WAN) übertrifft und nach welchen differenzierten Funktionen Sie bei einer Borderless SD-WAN-Lösung Ausschau halten sollten, um sicherzustellen, dass sie die richtige Wahl für Ihr Unternehmen ist.

In Kapitel 5 zeigen wir, wie eine Single-Vendor-SASE-Lösung (Secure Access Service Edge) den gesamten Prozess vereinfachen und eine sichere, zuverlässige und optimierte Konnektivität für jeden Standort, jede Cloud, jeden Remote-Benutzer und jedes IoT-Gerät (Internet of Things) bieten kann. Alle Mitarbeiter eines Unternehmens können von den Vorteilen einer vollständig konvergierten SASE-Plattform profitieren, die betriebliche Abläufe vereinfacht, einheitliche Sicherheit bietet, die Netzwerkperformance verbessert und den Erfolg von SASE gewährleistet.

Mit der Single-Vendor-SASE-Lösung von Netskope sind Unternehmen in der Lage, ihre Architektur mit der „Power of One" (siehe Kapitel 4) zu vereinfachen, d. h. sie brauchen nur eine einzige Plattform, eine einzige kompakte Software und eine einzige Richtlinie zur Steuerung aller Netzwerk- und Sicherheitsfunktionen. Im Folgenden stellen wir zehn wesentliche Fähigkeiten vor, die Unternehmen auf dem Weg zur Einführung von Borderless SD-WAN unterstützen können.

TIPP

Falls Sie zu denjenigen gehören, die bei Büchern das Ende zuerst lesen, dann ist dieses Kapitel Ihr Einstieg in dieses Thema. Denken Sie in diesem Fall daran, dass die hier beschriebenen Funktionen nur den Rahmen für die Implementierung von Borderless SD-WAN-Lösungen bilden, die an anderer Stelle in diesem Buch ausführlich beschrieben werden. Dies sind die *wichtigsten* zehn Dinge, aber nicht die *einzigen*; die Liste dessen, was Borderless SD-WAN leisten kann, ist weitaus länger und in hohem Maße an die Bedürfnisse jedes einzelnen Unternehmens anpassbar. Verwenden Sie diese Liste als Grundlage für die wichtigsten Entscheidungen, die Sie bei der Einführung einer Lösung treffen müssen.

Unterstützung des Unternehmens durch SASE-Konvergenz

Beim Aufbau Ihrer Borderless SD-WAN- und Sicherheitsarchitektur gibt es keinen falschen Weg. Entscheidend ist, dass die Lösung den Anforderungen Ihres Unternehmens entspricht und Ihnen hilft, Ihre angestrebten technischen und geschäftlichen Ziele zu erreichen. Der einheitliche Ansatz von Borderless SD-WAN und Netskope Intelligent Security Service Edge (SSE) macht den Einsatz mehrerer Einzelprodukte überflüssig und erhöht die betriebliche Effizienz. Diese Konvergenz von Konnektivität

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

und Sicherheit deckt unterschiedliche Anwendungsfälle ab, darunter Multi-Cloud-Umgebungen, Zweigstellen jeder Größe, Remote-Benutzer und IoT. Durch eine einzige, kompakte Softwarelösung lässt sich Borderless SD-WAN nahtlos in Netskope Intelligent SSE integrieren, wodurch ein äußerst sicheres, optimiertes und hochperformantes Netzwerk für jeden Remote-Benutzer, jedes Gerät, jeden Standort und jede Cloud entsteht. Dieser integrierte Ansatz vereinfacht die Verwaltung und reduziert die Komplexität, sodass Unternehmen ihre Abläufe effektiv rationalisieren können.

Alle Vorteile der Cloud mit einer Cloud-First-Lösung ausschöpfen

Zur effektiven Implementierung hochleistungsfähiger SASE-Services ist ein Cloud-First-Ansatz für SD-WAN- und SSE-Services unerlässlich, da dieser für die erforderliche Flexibilität und Skalierbarkeit sorgt.

Borderless SD-WAN mit einer Cloud-gehosteten Verwaltung vereinfacht Betriebsabläufe durch eine zentrale Steuerung und ermöglicht eine schnelle Anbindung von Benutzern, Geräten, Standorten und Cloud-Ressourcen, oft innerhalb weniger Minuten. Mit umfassender Transparenz und auf Machine Learning (ML) basierenden Einblicken in das gesamte Netzwerk (siehe Kapitel 4) können Probleme schnell identifiziert werden, wodurch sich die Anzahl der Support-Tickets verringert und die Zeit zur Problemlösung erheblich reduziert wird. Dies unterstützt letztlich die Produktivität der Kunden.

Borderless SD-WAN basiert zudem auf einer klaren Trennung der Daten- und Steuerungsebene, was eine hohe Skalierbarkeit und Ausfallsicherheit gewährleistet. Die Steuerungsebene, die mit Routing-Protokollen wie Border Gateway Protocol (BGP) und Open Shortest Path First (OSPF) kompatibel ist, wird als Software-as-a-Service (SaaS) bereitgestellt. Damit entfallen komplexe DIY-Installationen von Controllern vor Ort, was die Verwaltung vereinfacht und die Gesamtkomplexität reduziert. Kapitel 3</17 enthält weitere Informationen zu diesem Thema.

Durch die Schaffung eines sicheren und von bestimmten Betreibern und Transportwegen unabhängigen Overlay schafft Borderless SD-WAN eine kontextbewusste Struktur, die Remote-Benutzer, IoT-Geräte, Zweigstellen/Rechenzentren und Multi-Cloud-Umgebungen miteinander verbindet. Darüber hinaus werden die Borderless SD-WAN- und SSE-Services auf Netskope NewEdge mit geografisch verteilten Points of Presence (PoPs) gehostet. Diese unmittelbare Nähe zu Benutzern und Anwendungen ermöglicht sichere und optimierte On-Ramps zu Public und Private

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Clouds sowie Optimierungen für anspruchsvolle Anwendungen wie Zoom und Microsoft 365.

Cloud-On-Ramps: Sichere und optimierte Konnektivität für die „Any-to-Any"-Welt

Borderless SD-WAN bietet eine umfassende Transparenz und optimierte On-Ramps für jeden Benutzer und jeden Standort. Gleichzeitig sorgt es für eine nahtlose Konnektivität zu verschiedenen Cloud-, SaaS- und privaten Anwendungen.

Mithilfe der hochgradig verteilten Cloud-Hubs von Netskope NewEdge erweitert Borderless SD-WAN die SD-WAN-Fabric eines Unternehmens von On-Premises-Standorten (z. B. Zweigstellen, regionalen Standorten, Campus, Rechenzentren, Remote-Standorten und mobilen Büros) und bringt sie so nah wie möglich an SaaS- und Cloud-Services, um die Performance zu optimieren.

Unabhängig davon, ob ein Benutzer von einem Remote-Standort mit einem Endpoint SD-WAN oder von einer Zweigstelle des Unternehmens mit einem Netskope SASE-Gateway auf Zoom zugreift: Der Datenverkehr wird in jedem Fall optimiert, um ein hochwertiges Benutzererlebnis zu schaffen. Gleichzeitig bietet Borderless SD-WAN mit NewEdge einen hoch optimierten Middle-Mile-Service mit niedriger Latenz, der geografisch verteilte Zweigstellen mit Anwendungen in Zentralen auf unterschiedlichen Kontinenten verbindet..

Die enge Integration von Borderless SD-WAN mit SSE als Bestandteil eines vollständigen SASE-Frameworks gewährleistet einen umfassenden Schutz vor Cyber-Bedrohungen und reduziert das Risiko von Geschäftsunterbrechungen.

Borderless SD-WAN bietet nicht nur SD-WAN-Funktionen für Zweigstellen und Remote-Benutzer, sondern kann auch über mehrere Cloud-Umgebungen verteilte Unternehmensressourcen in eine einheitliche Netzwerkstruktur einbinden, darunter Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP). Durch fortschrittliches Routing und die direkte Integration mit Cloud-Anbietern stellt Borderless SD-WAN nahtlose Verbindungen zwischen unterschiedlichen Regionen innerhalb dieser Cloud-Plattformen her. Darüber hinaus lässt sich Netskope Intelligent SSE für Cloud-Workloads mühelos mit einem einzigen Klick integrieren.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Intelligenter Netzwerkzugang und fortschrittliches Routing

Bei der Auswahl eines Produkts für Ihr Unternehmen sollte Flexibilität einer der wichtigsten Aspekte sein. Netskope Borderless SD-WAN bietet ein hohes Maß an Flexibilität, da es sich durch Ein-Klick-Zugriff nahtlos in Netskope Intelligent SSE integrieren lässt. Dies ermöglicht die nahtlose Integration von Borderless SD-WAN mit unterschiedlichen Sicherheitsservices wie Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), Data Loss Prevention (DLP), SaaS Security Posture Management (SSPM), Cloud Security Posture Management (CSPM), Firewall-as-a-Service (FWaaS) und bietet so einen umfassenden Schutz vor Cyberangriffen.

Die Sicherheitsintegration ist sowohl auf Zweigstellenebene über das SASE-Gateway als auch an jedem Remote-Standort über eine kompakte, einheitliche SASE-Client-Software verfügbar, die auf den Laptops der Benutzer und in Multi-Cloud-Umgebungen ausgeführt wird. Dadurch wird sichergestellt, dass einheitliche und zuverlässige Sicherheitsmechanismen vorhanden sind, ganz gleich, welches Gerät der Benutzer verwendet oder wo er sich aufhält. Die Unterstützung von fortschrittlichen Routing-Protokollen wie OSPF und BGP durch Borderless SD-WAN ermöglicht zudem eine reibungslose Integration in die bestehende Unternehmensinfrastruktur. Die Trennung der Steuerung- und Datenebene sowie die Schlüsselverteilung im Cloud-Maßstab sorgen auch für die Vereinfachung und Skalierbarkeit der Steuerungsebene, die effizient über die Cloud bereitgestellt werden kann.

Umfassende Sicherheit für hybride Netzwerke

Fakt ist: Die Einführung von SD-WAN ohne integrierte Sicherheit kann zu einer hohen Komplexität führen. Unternehmen müssen letztendlich zwei unterschiedliche Lösungen unter einen Hut bringen, was zu einem logistischen Albtraum werden kann. Dabei bereitet nicht nur die Verwaltung Kopfzerbrechen. Auch die Effektivität der Sicherheits- und SD-WAN-Komponenten kann unter diesen Umständen beeinträchtigt werden.

Doch keine Sorge! Borderless SD-WAN verfolgt einen hybriden Netzwerksicherheitsansatz, der Sicherheit vor Ort und in der Cloud integriert. Es verfügt über grundlegende Sicherheitsservices wie eine Next Generation

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Firewall (NGFW) und ein Intrusion Prevention System/Intrusion Detection System (IPS/IDS) direkt in seinem SASE-Gateway. Dadurch wird Ihr East-West-Traffic genau dort geschützt, wo es nötig ist.

Doch das ist noch nicht alles. Borderless SD-WAN geht einen Schritt weiter und bietet vollständigen Schutz durch fortschrittliche Sicherheitsservices, die über die Cloud bereitgestellt werden, darunter Next-Generation SWG (NG-SWG), CASB, ZTNA, SSPM, CSPM und FWaaS. Es ist wie eine Festung, die Ihr Netzwerk umgibt und es von allen Seiten verteidigt.

Erstklassige Anwendungserfahrung, überall und für jede Anwendung

Ein konsistentes, zuverlässiges und hochwertiges Anwendungserlebnis sollte für Unternehmen immer oberste Priorität haben. Genau aus diesem Grund ist die Einführung von Borderless SD-WAN so wichtig. Sie bietet Unternehmen die Möglichkeit, ihre Netzwerk-, Sicherheits- und Optimierungsstrategien mit Blick auf die Erreichung dieses Ziels zu überdenken.

Borderless SD-WAN beinhaltet zahlreiche Funktionen wie dynamische Pfadauswahl, Failover innerhalb von Sekunden, granulare kontextabhängige adaptive Quality of Experience (QoE), Link Remediation und TCP/UDP-Optimierung (Transmission Control Protocol/User Datagram Protocol). Durch das Zusammenwirken dieser Funktionen werden eine optimale Performance und Benutzerfreundlichkeit gewährleistet. Bei diesen Fähigkeiten sollten Unternehmen keine Kompromisse eingehen. Durch den Einsatz von Borderless SD-WAN können Unternehmen ihren Netzwerkansatz optimieren und Benutzern ein herausragendes Anwendungserlebnis bieten.

Kontextbewusste Erkennung von Benutzeridentität, Geräten und Anwendungsrisiken für bessere Kontrollen

Borderless SD-WAN ist kontextbewusst konzipiert und ermöglicht die Validierung von Benutzeridentität, Geräteinformationen und Anwendungsrisiken in Echtzeit. Auf der Grundlage dieses Kontextbewusstseins kann ein zuverlässigen Zero-Trust-Frameworks im Netzwerk etabliert werden. Borderless SD-WAN zeichnet sich zudem durch die Fähigkeit aus, die Konfiguration von Quality-of-Service-Richtlinien (QoS)

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

erheblich zu vereinfachen. Herkömmliche SD-WAN-Lösungen können nur einige tausend Anwendungen erkennen, und IT-Administratoren müssen die QoS-Richtlinien für diese Anwendungen einzeln konfigurieren, was sehr zeitraubend sein kann.

Die Zero-Trust-Engine von Netskope kann derzeit mehr als 60.000 Anwendungen erkennen und jeder von ihnen ein CCI-Rating (Cloud Confidence Index) zuweisen (siehe Kapitel 2). Diese CCI-Bewertung ist ein Indikator dafür, wie gut eine Anwendung für den Einsatz in Unternehmen geeignet ist. Bei Borderless SD-WAN nutzt Netskope diese CCI-Bewertungen, um sofort verfügbare, intelligente QoS-Standardwerte bereitzustellen. So muss das Netzwerkbetriebsteam QoS-Richtlinien nicht mehr manuell für jede Anwendung konfigurieren, was wertvolle Zeit und Mühe spart.

Die kontextbewussten Funktionen von Netskope gehen über die bloße Identifizierung von Benutzern und Anwendungen hinaus. Sie ermöglichen auch die automatische Erkennung aller IoT-Geräte, ganz gleich, ob es sich um verwaltete oder nicht verwaltete Geräte handelt, sodass Netskope die mit kompromittierten IoT-Geräten verbundenen Risiken leicht identifizieren und managen kann. Mit diesem hohen Kontextbewusstsein kann Netskope das Netzwerk auf der Grundlage von KI/ML effektiv mikrosegmentieren und den Zugriff sowie das Verhalten von IoT-Geräten eingrenzen und kontrollieren. Dies trägt dazu bei, die potenziellen negativen Auswirkungen eines kompromittierten Geräts zu mindern und das Risiko von unbefugten Zugriffen oder Datenverletzungen zu verringern.

Vereinfachte, automatisierte KI-gesteuerte Abläufe

Sie können sich das in etwa so vorstellen: Die Borderless SD-WAN-Lösung von Netskope ist Ihr treuer Helfer, der Ihnen immer zur Seite steht. Sie ist wie ein persönlicher Assistent, der sich um alle wichtigen Angelegenheiten kümmert, damit Sie sich auf das Wesentliche konzentrieren können. Durch die Automatisierung von Prozessen und KI-gesteuerte Abläufe vereinfacht diese Lösung Ihre Verwaltungsaufgaben auf ganz neue Weise. Das Onboarding von Kunden, die Einrichtung von SASE-Gateways, die Verwaltung von Endpoint-SD-WAN oder der Umgang mit Multi-Cloud-Umgebungen – all das kann ganz einfach über eine zentrale Verwaltungsplattform erledigt werden.

Doch das ist noch nicht alles. Die Möglichkeiten von ML machen diese Borderless SD-WAN-Lösung zu etwas ganz Besonderem. Sie lernt von Ihrem Netzwerk, analysiert den Datenverkehr und versteht Ihre Richtlinien, sodass Störungen proaktiv erkannt und behoben werden können,

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

bevor sie überhaupt zu Problemen werden. Es ist, als hätte man ein Team von Experten, das rund um die Uhr dafür sorgt, dass alles reibungslos läuft.

Oh, und haben wir schon die Zeiteinsparungen erwähnt? Dank autonomer Überwachung werden Anomalien in kürzester Zeit erkannt, und potenzielle Verletzungen der Service-Level-Agreements (SLA) von Dienstanbietern können vorhergesagt werden, bevor sie auftreten. Probleme lassen sich schneller lösen, Ausfallzeiten werden minimiert, und der Betrieb kann in kürzester Zeit wieder aufgenommen werden

Unterstützung für eine Wireless-First-Strategie

Eine umfassende Borderless SD-WAN-Lösung hält Ihnen in Sachen Konnektivität den Rücken frei und verfügt über ein transportunabhängiges Design, das sich an Ihre Bedürfnisse anpasst. Sie bietet die nötige Flexibilität, um 4G/5G-Konnektivitätsoptionen hinzuzufügen und von überall aus eine zuverlässige und mühelose Konnektivität zu gewährleisten. Einer der größten Vorteile dieser Lösung ist ihre Fähigkeit, Funksignalstärke zu optimieren. Auch wenn Sie sich in einer abgelegenen Außenstelle befinden oder einen temporären Arbeitsbereich ohne kabelgebundenen Breitbandzugang einrichten, können Sie sich auf eine solide und zuverlässige Verbindung verlassen. Die Lösung eignet sich perfekt für Situationen, in denen eine kabelgebundene Breitbandverbindung nicht verfügbar, nicht ideal oder sogar unmöglich ist.

Die Borderless SD-WAN-Lösung ist zudem auf die Interoperabilität mit globalen Betreibern ausgelegt. Sie funktioniert gut mit unterschiedlichen Betreibern auf der ganzen Welt, unter denen Sie denjenigen auswählen können, der Ihren Bedürfnissen am ehesten entspricht oder an Ihrem Standort am besten funktioniert. Ob Mikrozweigstellen, Büros mittlerer Größe oder umfangreiche Unternehmensumgebungen: Diese Lösung bietet die nötige Flexibilität und Skalierbarkeit, um Ihre Konnektivitätsanforderungen zu erfüllen.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Volle Unterstützung für Edge-Computing

Bei Borderless SD-WAN geht es vor allem um Flexibilität und Effizienz. Deshalb ist die Container-Orchestrierung ein entscheidender Faktor. Sie ermöglicht die einfache Verwaltung und Bereitstellung neuer Services am Gateway, ohne dass in jeder Zweigstelle eine Reihe von Servern unterhalten werden muss. Stellen Sie sich vor, Sie hätten einen Container für das Digital Experience Management auf Ihrem SASE-Gateway: Die Echtzeit-Überwachung der Benutzererfahrungen wäre damit ein Kinderspiel! Sie könnten dann auch IoT-Daten wie ein Profi durchforsten. Sie unterstützt Multi-Cloud-Umgebungen wie AWS IoT Greengrass und Azure IoT Hub, sodass Sie all die interessanten IoT-Daten direkt am Edge erfassen und analysieren können. „Cutting Edge" bekommt damit eine ganz neue Bedeutung!

Abbildung 6-1 zeigt die zehn in diesem Kapitel behandelten Fähigkeiten.

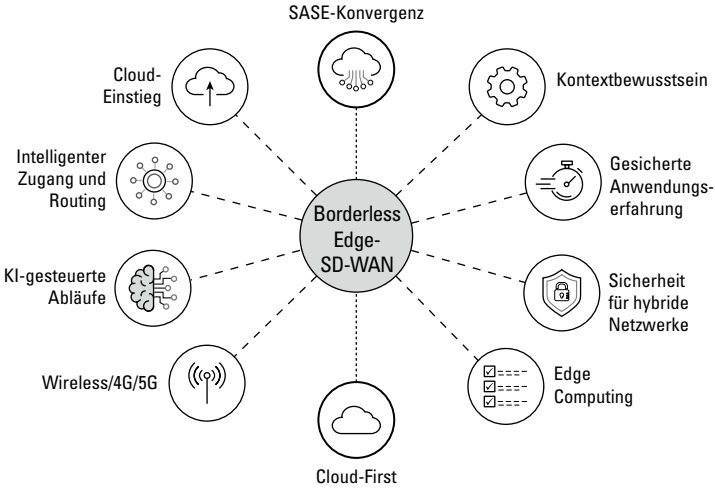

ABBILDUNG 6-1: Zehn Fähigkeiten, die Unternehmen bei der Einführung von Borderless SD-WAN unterstützen können.

Urheberrechtlich geschütztes Material © 2024 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Auf alles vorbereitet

Netskope, ein weltweit führender SASE-Anbieter, das Netzwerke und Sicherheit nahtlos in Unternehmen integriert, AIOps nutzt, Zero-Trust-Prinzipien und KI/ML-Innovationen anwendet, um Daten mit leistungsstarker Konnektivität und umfassendem Bedrohungsschutz zu sichern. Die Netskope-Plattform ist schnell und einfach zu bedienen und bietet optimierten Zugriff und Echtzeitsicherheit für Personen, Geräte und Daten, wo immer sie sich befinden. Netskope hilft Kunden dabei, Risiken zu reduzieren, die Performance zu steigern und einen unübertroffenen Einblick in alle Cloud-, Web- und privaten Anwendungsaktivitäten zu erhalten. Tausende Kunden vertrauen Netskope und seinem leistungsstarken NewEdge-Netzwerk, um aufkommende Bedrohungen, neue Risiken, Technologieverschiebungen, Organisations- und Netzwerkänderungen sowie neue regulatorische Anforderungen zu bewältigen. Erfahren Sie, wie Netskope Kunden dabei hilft, auf ihrer SASE-Reise auf alles vorbereitet zu sein und besuchen Sie **netskope.com/de/**

netskope

Die Anforderungen des Unternehmens ohne Grenzen mit Borderless SD-WAN erfüllen

Der Netzwerkperimeter des Unternehmens hat sich mit der Zunahme von Mikrozweigstellen, Multi-Cloud, Remote-Arbeit, Telemedizin, mobilen Flotten und dem Internet der Dinge (IoT) erweitert. Benutzer, Geräte, Standorte und Clouds sind heute stark verteilt und gleichzeitig auf vielfältige Weise miteinander verbunden. Borderless SD-WAN verfügt über neue Funktionen, die eine sichere, zuverlässige und schnelle Konnektivität auf der Grundlage von Zero-Trust-Prinzipien, skalierbare KI-gesteuerte Betriebsabläufe, eine sichere Anwendungserfahrung, Sicherheit für mehr als 60.000 Anwendungen, erweiterte Unterstützung für 4G/5G-Mobilfunk und viele weitere Vorteile bieten.

Der Inhalt ...

- Schnelle und zuverlässige Konnektivität erzielen
- Networking und Sicherheit nahtlos integrieren und SASE beschleunigen
- Sechs Lösungen und zehn Fähigkeiten für das Unternehmen ohne Grenzen
- Reduzierung der IT-Kosten und effizientere Budgetverwaltung
- Vereinfachte Architekturen und effizientere Abläufe

netskope

Parag Thakore und **Muhammad Abid** sind Führungskräfte bei Netskope und anerkannte Experten mit mehreren Patenten in den Bereichen Cloud Computing, Cybersicherheit und Netzwerke. Mit ihrer jahrzehntelangen Erfahrung in globalen Unternehmen wie Cisco, VeloCloud/VMWare, Infiot, Fortinet und T-systems waren sie maßgeblich an der Neudefinition von Enterprise WAN beteiligt und unterstützten die Einführung von SD-WAN und SASE.

Besuchen Sie Dummies.com®
für Schritt-für-Schritt-Anweisungen mit Bildern, Kurzanleitungen oder andere Bücher!

ISBN: 978-1-394-21947-6
Nicht für den Wiederverkauf

für dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.