LERNEN LEICHT GEMACHT

Versa Networks Sonderausgabe

SASE

für dummies®

- Zukunftssicherheit für Ihr Unternehmen
- Optimierung von Sicherheit und Anwendungsleistung
- Schutz eines expandierenden Netzwerkperimeters

Präsentiert von

VERSA NETWORKS

Kumar Mehta, MSE
Apurva Mehta, MSCS

Über Versa Networks

Versa Networks, der führende Anbieter von SASE, kombiniert umfassende Sicherheit, erweiterte Netzwerkfunktionen, SD-WAN mit vollem Funktionsumfang, echte Mandantenfähigkeit und ausgeklügelte Analysen über die Cloud, vor Ort oder als Kombination aus beidem, um SASE-Anforderungen für kleine bis extrem große Unternehmen und Serviceprovider zu erfüllen. Versa SASE bietet sichere, skalierbare und zuverlässige unternehmensweite Netzwerke und Sicherheit, erhöht die Leistung von Multicloud-Anwendungen und senkt die Kosten erheblich. Tausende von Kunden weltweit mit hunderttausenden von Standorten vertrauen Versa ihre Netzwerke, Sicherheit und Clouds an. Versa Networks ist ein Privatunternehmen und wird finanziert von Sequoia Capital, Mayfield, Artis Ventures, Princeville Global Fund, RPS Ventures, Triangle Peak Partners, Verizon Ventures, Comcast Ventures und Liberty Global Ventures.

Weitere Informationen finden Sie unter www.versa-networks.com oder folgen Sie Versa Networks auf Twitter unter @versanetworks.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

SASE

Versa Networks Sonderausgabe

**von Kumar Mehta, MSE,
und Apurva Mehta, MSCS**

für dummies®

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

SASE für Dummies®, Versa Networks Sonderausgabe

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

Copyright © 2022 John Wiley & Sons, Inc., Hoboken, New Jersey

Kein Teil dieser Publikation darf ohne die vorherige schriftliche Genehmigung des Verlags in irgendeiner Form oder auf irgendeine Weise – sei es elektronisch, mechanisch, in Form einer Fotokopie oder Aufnahme, durch Scannen oder anderweitig – reproduziert, auf einem Datenträger gespeichert oder übertragen werden, außer dies ist unter Abschnitt 107 oder 108 des Copyright Act 1976 der Vereinigten Staaten 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, The Dummies Way, 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 VERLAG UND DER AUTOR GEBEN KEINE ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN IN BEZUG AUF DIE INHALTLICHE RICHTIGKEIT UND VOLLSTÄNDIGKEIT DIESES WERKES UND LEHNEN AUSDRÜCKLICH ALLE GEWÄHRLEISTUNGEN AB, INSBESONDERE GEWÄHRLEISTUNGEN HINSICHTLICH DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. GEWÄHRLEISTUNGEN KÖNNEN NICHT DURCH VERKAUFS- ODER WERBEMATERIALIEN BEGRÜNDET ODER VERLÄNGERT WERDEN. DIE HIERIN ENTHALTENEN EMPFEHLUNGEN UND STRATEGIEN SIND UNTER UMSTÄNDEN NICHT IN JEDER SITUATION GEEIGNET. DIESES WERK WIRD MIT DEM AUSDRÜCKLICHEN HINWEIS VERKAUFT, DASS DER VERLAG KEINE RECHTLICHEN DIENSTLEISTUNGEN, KEINE DIENSTLEISTUNGEN IM BEREICH DES RECHNUNGSWESENS UND KEINE ANDEREN PROFESSIONELLEN DIENSTLEISTUNGEN ERBRINGT. FALLS PROFESSIONELLE HILFE BENÖTIGT WIRD, SOLLTE DIE HILFE EINES PROFESSIONELLEN DIENSTLEISTERS IN ANSPRUCH GENOMMEN WERDEN. WEDER DER VERLAG NOCH DER AUTOR HAFTEN FÜR HIERAUS ENTSTEHENDE SCHÄDEN. DIE TATSACHE, DASS IN DIESEM WERK AUF EINE ORGANISATION ODER INTERNETSEITE IN FORM EINES ZITATS UND/ODER EINER MÖGLICHEN QUELLE FÜR WEITERE INFORMATIONEN BEZUG GENOMMEN WIRD, BEDEUTET NICHT, DASS DER AUTOR ODER DER VERLAG DEN VON DIESER ORGANISATION ODER DEN AUF DIESER INTERNETSEITE ZUR VERFÜGUNG GESTELLTEN INFORMATIONEN BZW. DEN VON IHNEN GEGEBENEN EMPFEHLUNGEN ZUSTIMMT. AUSSERDEM SOLLTE DER LESER BEDENKEN, 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.

ISBN 978-1-119-83637-7 (pbk); ISBN 978-1-119-83477-9 (ebk)

Hergestellt in den Vereinigten Staaten von Amerika

10 9 8 7 6 5 4 3 2 1

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

Danksagung des Verlags

Die folgenden Personen haben bei der Erstellung dieses Buches mitgewirkt:

Project Editor: Elizabeth Kuball

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: William Hull

Production Editor: Tamilmani Varadharaj

Besondere Unterstützung: Kelly Ahuja, Monnia Deng, Aviva Garrett, Christina Hattingh, Sunil Ravi, Rohan Ravindranath, Faithe Wempen, Michael Wood, Chitresh Yadav

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Inhaltsverzeichnis

EINFÜHRUNG 1
Über dieses Buch 1
Zugrundeliegende Voraussetzungen 2
In diesem Buch verwendete Symbole 2
Weitere Schritte 3

KAPITEL 1: **Was ist SASE?** 5
SASE – eine Einführung 6
Vom WAN zum SD-WAN 6
Schutz für Webgateways und Telearbeiter 7
Sicherer Cloud-Zugang 7
Gesundes Misstrauen 8
Schutz gegen Bedrohungen 9
Malware-Schutz für Vertrauliche Daten 9
Arbeiten in Echtzeit mit erweitertem Routing 10
Anforderungen an eine SASE-Lösung 10
Hardwareneutralität 10
Single-Pass-Architektur 11
Elastische horizontale Skalierung 12
Container und Microservices 12
Globale Verteilung 13
Inline-Verschlüsselung 13
Segmentierung mit Multimandantenfähigkeit 13
Bereitstellung einer SASE-Lösung 14

KAPITEL 2: **Ein modernes Unternehmen werden** 15
Erweiterung des Netzwerkperimeters 16
Arbeiten mit älteren WANs 17
Arbeiten mit modernen WANs 18
Reduzierung der Hardwarekomplexität und -kosten 19
Mehr Sicherheit und mehr Leistung 21
Hintergründe der Trends zur digitalen Transformation 21
Einführung von Cloud und Mobilität 22
Weitgehende Akzeptanz des mobilen Arbeitens 22

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

KAPITEL 3: **Netzwerktechnik als Ausgangspunkt** 25
Aufbau auf SD-WAN 25
Verwendung von Anschlussstellen 26
Auffahrt mit SD-WAN-Technologie 26
Integrierte Sicherheit: die Grundlage von SD-WAN 28
Echtes SD-WAN 29
Erweiterte Routing-Funktionen 31
Servicequalität 33
Optimierung des Datenverkehrs 33
WAN-Optimierung 34
Globale Verteilung 35
Mandantenfähigkeit und Segmentierung 36
5G-Architektur 36
Weniger Komplexität 37

KAPITEL 4: **Erweiterung der Sicherheit auf Client und Cloud** 39
Die Entwicklung der Netzwerksicherheit 40
Erkennung und Verhinderung des Eindringens in Systeme 41
Next-Generation Firewalls 41
IDPS (Intrusion Detection and Prevention System) 42
DNS-Sicherheit 43
Verwaltung und Kontrolle von Sicherheitsbedrohungen 44
Unified Threat Management 44
Malware-Schutz 44
Dynamische sichere Web-Gateways 45
ZTNA und der neue Perimeter für Nutzer und Geräte 47
Sicherung der Cloud 48
Cloud Access Security Broker 48
DLP in der Cloud 49
Remote-Browser-Isolierung 51
Analyse des Verhaltens von Nutzern und Entitäten 52
Feinabstimmung der Zugriffsverwaltung 53
Schutz sensibler Daten 54
Entschärfung von Malware 54

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

KAPITEL 5: **Nutzung von SASE** 55
Verstehen, wie SASE die digitale Transformation ermöglicht 55
Multicloud-Implementierung 56
Cloudnativ und flexibel 57
Zuverlässiges Management 57
Schnellere Administration und Bereitstellung 57
Vereinfachter Überblick 58
Vollständige Kontrolle über Nutzer, Anwendungen und Geräte 58
Schutz Ihrer Vermögenswerte 59
Bessere Datensicherheit und Compliance 60
Inline-Verschlüsselung 60
Isolierung und Segmentierung 61
Kostensenkung 61
Betrachtung eines Anwendungsbeispiels aus einem realen Unternehmen 62

KAPITEL 6: **Evaluierung von SASE Best Practices** 65
Architekturen im Vergleich 65
Abstimmung technologischer und betrieblicher Anforderungen 66
Die Herausforderungen der Nachrüstung von Sicherheit 68
Nutzung der Vorteile einer Single-Pass-Lösung 68
Elastische Skalierung 69
Effiziente Nutzung einer einzigen Software 69
Kontextbezogene Sicherheit und kontextbezogener Zugriff 70
Single-Pass- und cloudnative Vorteile 71
Planung für Skalierbarkeit, Performance und die Zukunft 72

KAPITEL 7: **Zehn Dinge, die bei einer SASE-Lösung zu beachten sind** 73

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Einführung

Die Unternehmen werden mit unterschiedlichen externen und internen Gefahren konfrontiert. Cybersicherheitsbedrohungen sind ausgeklügelter, tiefgehender, weiter verteilt und multidimensionaler als je zuvor. Gleichzeitig ermöglichen digitale Initiativen, technologische Modernisierung und Cloud-Innovationen eine stärkere physische Verteilung von Anwendungen, Benutzern und Geräten was es Unternehmen erschwert, zu kontrollieren, was in ihre Netzwerke gelangt und aus ihnen herauskommt.

Diese beispiellose Zunahme von Anwendungen und Benutzern in Kombination mit zunehmend weitgreifenden Sicherheitsschwachstellen erfordert einen innovativen Verbindungs- und Schutzansatz unter Nutzung der Skalierbarkeit der Cloud. Die Mikrosegmentierung von Netzwerk, Sicherheit, Anwendungen und Benutzern allein ist nicht mehr akzeptabel, um die Sicherheit von Daten, Ressourcen und Anwendungen zu gewährleisten.

Zur Bewältigung dieser Herausforderungen müssen Unternehmen in der Lage sein, Netzwerkservices bereitzustellen, die so vielfältig und geografisch verteilt sind wie die Anwendungen und Nutzer, die sie nutzen. Glücklicherweise sind umfassende und integrierte Sicherheit, Netzwerkbetrieb und Visibilität über die Cloud heute im gleichen Umfang und mit der Performance möglich, die einst nur bei On-Premises-Lösungen zur Verfügung standen.

Da Sie sich für dieses Buch entschieden haben, gehen wir davon aus, dass Sie daran interessiert sind, dies auch für Ihr Unternehmen zu verwirklichen. Fangen wir also an.

Über dieses Buch

Secure Access Service Edge (SASE) bietet eine Möglichkeit, die von Gefahren bedrohte moderne Unternehmensnetzwerklandschaft durch vertrauenswürdige Sicherheitslösungen zu schützen. Das Funktionsspektrum reicht weit über ältere Sicherheitsarchitekturen hinaus und umfasst Identität, Vertrauen und Kontext unabhängig von Verbindung, Nutzer, Gerät oder Anwendung. SASE ermöglicht zudem die durchgängige, konsistente und allgegenwärtige Bereitstellung von Richtlinien sowie die Erfüllung von Sicherheits-, Netzwerk-, Anwendungs-, Nutzer- und Geschäftsanforderungen.

Dieses Buch behandelt alles, was Sie über SASE wissen müssen. Sie erfahren, welche Aspekte es umfasst, wie es Unternehmen und

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Organisationen nutzt, wie es zur Sicherheit beiträgt, wie es am besten implementiert wird und wie Sie seine Funktionsmerkmale bestmöglich nutzen können.

Zugrundeliegende Voraussetzungen

Wir haben uns beim Verfassen dieses Buches ein wenig weiter aus dem Fenster gelehnt und einige Annahmen über Sie aufgestellt. Wir gehen von Folgendem aus:

- Sie sind eine Fachkraft für IT-, Netzwerk-, oder Informationssicherheit.
- Sie sind mit den grundlegenden IT-, Netzwerk- und Sicherheitsthemen vertraut.
- Sie sind sich der Schwachstellen bewusst, die die Netzwerk- und Netzwerksicherheitslandschaft durchdringen.
- Sie sind nicht mit dem Status quo zufrieden – Sie wollen einen neuen Ansatz, um die Kosten und Komplexität von Legacy-Lösungen und -Produkten einzudämmen.

In diesem Buch verwendete Symbole

Um die Navigation zu den nützlichsten Informationen zu erleichtern, markieren diese Symbole Schlüsseltext:

Das Symbol „Merke!“ markiert wichtige Punkte, die Sie sich einprägen sollten.

Lesen Sie diese optionalen Passagen, wenn Sie eine technischere Erklärung wünschen.

Das Symbol „Tipp“ markiert Informationen, die Ihnen Zeit und Mühe sparen können.

Achten Sie auf diese potenziellen Fallstricke auf dem Weg.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Weitere Schritte

Das Buch wurde als Handbuch und Nachschlagewerk geschrieben, so dass Sie entweder es in einem Stück lesen oder direkt zu den Teilen springen können, die Sie am meisten interessieren. Egal, wie Sie sich entscheiden, Sie können nichts falsch machen. Beide Wege führen zum selben Ergebnis – zu einem besseren Verständnis von SASE und den Schritten und Technologien, die Sie für die weitere Entwicklung benötigen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- Merkmale von SASE
- Anforderungen an eine SASE-Lösung
- Bereitstellung einer SASE-Lösung

Kapitel 1
Was ist SASE?

Die Art und Weise, wie Unternehmen Geschäfts- und Produktivitätsservices für interne und externe Mitarbeiter, Partner und Kunden bereitstellen, hat sich im Laufe der Zeit erheblich verändert. Immer mehr Unternehmen machen sich neue Technologien wie die Cloud, Software-as-a-Service (SaaS), Telearbeit-Lösungen und das Internet of Things (IoT) zunutze.

Beim Versuch, neue Funktionen bereitzustellen und eine umfassendere Sicherheit zu gewährleisten, können sie jedoch leicht in eine Zwickmühle geraten. Mitarbeiter und Kunden fordern die Migration zur Cloud und Mobilität, um eine höhere Flexibilität, Agilität und Zuverlässigkeit zu erreichen. Das vergrößert jedoch die Angreifbarkeit des Netzwerks erheblich. Veraltete Architekturen können den damit verbundenen Leistungs- und Sicherheitsanforderungen einfach nicht mehr gerecht werden. Jetzt ist es an der Zeit, die im Unternehmen eingesetzten Systeme und Tools neu zu bewerten.

Unternehmen sollten ein neues IT-Modell einführen, das herkömmliche ineffiziente WAN-Architekturen überflüssig macht. Es sollte Mitarbeitern die Möglichkeit bieten, flexibel zu arbeiten (Homeoffice) und gleichzeitig für einen starken Sicherheitsstatus sorgen. SASE kann dabei helfen.

Das *Secure Access Services Edge* (SASE) ist eine Netzwerkarchitektur, die von Gartner für Sicherheitslösungen für das „Cloud-Zeitalter" eingeführt wurde. In diesem Kapitel erklären wir die Merkmale von SASE und erläutern, welche Anforderungen eine SASE-Lösung erfüllen muss.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

SASE – eine Einführung

SASE ist keine einzelne Technologie, sondern eine ganze Reihe von Funktionen, darunter:

- Software-Defined WANs (SD-WANs)
- Secure Web Gateways (SWGs)
- Cloud Access Security Brokers (CASBs)
- Zero Trust Network Access (ZTNA)
- Firewall-as-a-Service (FWaaS)

Im Zusammenspiel können diese SASE Funktionen Ihren Netzwerken bei der Erfüllung hoher Sicherheitsanforderungen helfen, ohne dass Sie Kompromisse in Bezug auf Technologie, Flexibilität oder Funktionen eingehen müssen. Lassen Sie uns nun einen Blick auf jede dieser Technologien werfen.

Vom WAN zum SD-WAN

Man könnte herkömmliche IT-Infrastruktur mit einem umzäunten Garten vergleichen. Mitarbeiter verbanden sich von einer Filiale aus mit dem Netzwerk des Unternehmens und griffen dabei über ein privates, sicheres Site-to-Site-WAN auf die im privaten Rechenzentrum gehosteten Anwendungen zu. Die Internetkonnektivität wurde zentral vom Firmen Standort oder Rechenzentrum aus bereitgestellt und gesichert.

Die nächste Netzwerkgeneration stellte erstmals SD-WANs vor. Ein SD-WAN ist ein Netzwerk, bei dem die Netzwerkhardware vom softwarebasierten Kontrollsystem getrennt ist. SD-WANs der ersten Generation waren in der Lage, Anwendungen zu identifizieren und Richtlinien zur Steuerung des Datenverkehrs zu nutzen. Außerdem brachten sie Kostenvorteile mit sich. SD-WANs der zweiten Generation stellten ein vollständiges Netzwerk mit integrierter Sicherheit zur Verfügung und ermöglichten sichere Internet-Breakouts über Direct Internet Access (DIA) an jedem beliebigen Standort, damit sich Nutzer direkt mit der Cloud und SaaS-Anwendungen verbinden konnten.

Heutzutage greifen Telearbeiter jederzeit und von überall auf Anwendungen zu. Viele Unternehmen nutzen SaaS für geschäftskritische Anwendungen und migrieren ihre Workloads von Private- zu Multi-Cloud-Architekturen, die ihre Anforderungen in Bezug auf Geschwindigkeit, Agilität und Geschäftsmodel besser erfüllen können.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

MERKE!

Wir befinden uns im sogenannten „Cloud-Zeitalter“, in dem Netzwerkgrenzen zunehmend verschwimmen und sich in einen fließenden, strukturlosen Netzwerkrand – den sogenannten „Edge“ – verwandeln. Die IT muss in der Lage sein, ein sicheres, zuverlässiges und dynamisches Nutzer-, Kunden- und Anwendungserlebnis zu bieten, das verbessert, gemessen, überwacht und diagnostiziert werden kann.

Schutz für Webgateways und Telearbeiter

Ein Secure Web Gateway (SWG) schützt die Geräte von Telearbeitern vor Internetbedrohungen. Es verhindert, dass sie mit unerwünschter Software oder Malware infiziert werden, und unterstützt die Durchsetzung von unternehmensinternen Sicherheits und gesetzlichen Richtlinien. Ein SWG umfasst Folgendes:

- URL-Filterung (Uniform Resource Locator)
- Schutz vor Malware und Viren
- Funktionen zur Anwendungsidentifizierung und -kontrolle
- Verhinderung von Datenverlust

SWGs können als On-Premises-Hardware, als virtuelle Maschine, cloudbasierte Services oder hybrid als kombinierte On-Premises- und Cloud-Elemente implementiert werden.

HINWEIS

Die auf dem Markt angebotenen cloudbasierten SWG-Lösungen unterscheiden sich hinsichtlich ihrer technischen Ausgereiftheit erheblich voneinander.

Sicherer Cloud-Zugang

Ein CASB bietet Produkte und Services, mit denen Sicherheitsdefizite bei der Nutzung von Cloud-Services durch Unternehmen angegangen werden können. Die Technologie schützt die von immer mehr Anwendern genutzten Cloud-Services (sowohl innerhalb als auch außerhalb des herkömmlichen Perimeters) und die immer häufiger werdende Bereitstellungen von direktem Cloud-to-Cloud-Zugang. CASBs sind entweder lokale oder cloudbasierte Punkte zur Durchsetzung von Sicherheitsrichtlinien, die zwischen Konsumenten und Anbietern von Cloud-Services eingerichtet werden, um die Sicherheitsrichtlinien des Unternehmens beim Zugriff auf cloudbasierte Daten oder Anwendungen durchzusetzen. Ein CASB kann Folgendes:

- Daten, Anwendungen und das Nutzerverhalten bei Cloud-Services über die Programmierschnittstelle (APIs) des Anbieters prüfen

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

- zwischen Benutzern und Cloud-Services eingesetzt werden oder als Alternative Remote Browser Isolation (RBI) anbieten
- Transparenz und Zugriffskontrolle für jeden Benutzer, jedes Gerät und jeden Standort zur Verfügung stellen
- mit einem bestehenden Identitätsanbieter, SIEM-Tool (Security Information and Event Management) und UEM-Produkt (Unified Endpoint Management) des Unternehmens integriert werden
- eine Vielzahl von Analysemethoden bei der Überwachung des Verhaltens von Anwendern, Drittanbieteranwendungen und Daten einsetzen
- durch die Verwendung unterschiedlicher Methoden bösartige und/oder unerwünschte Sitzungen identifizieren und entsprechend reagieren
- zwischen geschäftlichen und privaten Instanzen von Cloud-Services unterscheiden und den Datenaustausch zwischen ihnen begrenzen oder verhindern

MERKE!

CASB-Anbieter verstehen, dass bei Cloud-Services ein anderes Schutzziel im Mittelpunkt steht: Es sind immer noch Ihre Daten, aber die Systeme in denen sie verarbeitet und gespeichert werden gehören Dritten.

CASBs ermöglichen eine zentrale simultane Einhaltung von Richtlinien für alle Benutzer und Geräte über mehrere Cloud-Services hinweg. Sie bieten eine granulare Transparenz und Kontrolle über Benutzeraktivitäten und sensible Daten.

Gesundes Misstrauen

Anders als bei herkömmlichen LAN-Segmenten (Local Area Network) und IP-Adressen innerhalb des Perimeters geht ZTNA davon aus, dass kein Benutzer und kein Gerät vertrauenswürdig ist. Da der Internetzugang mittlerweile überall möglich ist, haben sich die herkömmlichen Vertrauensgrenzen aufgelöst.

ZTNA umfasst eine oder auch mehrere Anwendungen mit einer identitäts- und kontextbasierten logischen Zugriffsgrenze. Diese „verborgenen“ Anwendungen werden nicht erkannt und der Zugriff darauf wird über einen Trust Broker auf eine Reihe benannter Entitäten beschränkt. Der Broker bestätigt die Identität, den Kontext und die Richtlinienkonformität der angegebenen Teilnehmer, bevor der Zugriff gestattet wird. Gleichzeitig unterbindet er Seitwärtsbewegung zu anderen Bereichen des Netzwerks. Durch ZTNA kann die Angriffsfläche erheblich reduziert werden, da Vermögenswerte für die Öffentlichkeit nicht sichtbar sind. Eine Zero-Trust-Architektur ist ein entscheidender Bestandteil einer

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

SASE-Strategie, da sie den Datenverkehr nur zwischen authentifizierten Benutzern, Geräten und Anwendungen zulässt.

TIPP

Um ein Zero-Trust-Modell zu implementieren, muss das Unternehmen den zu schützenden Bereich definieren und bestimmen, wo sich Vertrauliche Informationen befinden und wer auf sie zugreifen darf. Dazu sind einige Sicherheitsmaßnahmen wie einheitliche Richtlinien, Multi-Faktor-Authentifizierung (MFA), Mikrosegmentierung und das Einrichten von Zugriffsrechten nach dem Prinzip der geringsten Rechte erforderlich.

Schutz gegen Bedrohungen

Next-Generation Firewalls (NGFWs) sind Deep Packet Inspection-Engines, die über die Untersuchung und Blockierung von Ports/Protokollen hinausgehen und eine Datenanalyse auf Anwendungsebene ermöglichen. Moderne NGFWs integrieren Folgendes:

- die Funktionen herkömmlicher Stateful Firewalls
- anwendungsorientierte Deep Packet Inspection von Inhalten
- Unified Threat Management (UTM), einschließlich Intrusion Detection and Prevention Systems (IDPSs)
- eine höhere Transparenz über die gesamte Angriffsfläche hinweg
- Flexibilität in einer sich ständig weiterentwickelnden Bedrohungslandschaft

HINWEIS

Da die Bedrohungslandschaft aufgrund von DIA und der zunehmenden Einführung von Multi-Cloud-Lösungen immer größer wird, sind herkömmliche Firewalls nicht mehr in der Lage, einen ausreichenden Schutz zu bieten. Das führt letztendlich zu einem schwachen Sicherheitsstatus. NGFWs und UTM sind für eine gute Sicherheitshygiene unerlässlich.

Malware-Schutz für Vertrauliche Daten

Datenlecks treten auf, wenn persönliche oder andere Vertrauliche Daten wie Kontonummern, Gesundheitsdaten oder Benutzernamen/Passwörter versehentlich offengelegt werden. Datendiebstahl tritt auf, wenn ein Angreifer aktiv in ein System eindringt und sich Zugriff auf Informationen verschafft, um sie zu entwenden oder zu beschädigen.

TIPP

Zum Schutz Vertraulicher Daten müssen Unternehmen eine Sicherheitssoftware installieren, die Malware- und Virenschutzfunktionen umfasst und regelmäßig aktualisiert werden kann.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

SASE sorgt dafür, dass nur diejenigen Personen auf sensible Anwendungen und Daten zugreifen können, die diese Daten laut Unternehmensrichtlinie tatsächlich benötigen – und zwar unabhängig vom Standort des Benutzers/der Anwendung oder der zwischen ihnen verwendeten Übertragungstechnologie.

Arbeiten in Echtzeit mit erweitertem Routing

Intelligentes Routing bietet einzigartige integrierte Funktionen, darunter Pfadoptimierung, rasche Konvergenz, Fehlerkorrekturen im Datenverkehr, Quality of Experience (QoE) für jede Anwendung und Verschlüsselung.

Zur korrekten Ausführung des SASE-Modells ist es unerlässlich, die Bandbreitenauslastung des Datenverkehrs am Netzwerk-Edge zu verstehen und sichtbar zu machen. Eine Edge-Architektur mit verteilten Services nutzt das gleiche Modell, das für die Skalierung von Rechenressourcen verwendet wird: Bei steigender Nachfrage werden zusätzliche Server oder virtuelle Maschinen (VMs) hinzugefügt, um das höhere Datenverkehrsvolumen zu bewältigen und die Übertragungsgeschwindigkeit/Datenübertragungsrate konstant zu halten

Anforderungen an eine SASE-Lösung

SASE bietet dynamische, kontextbezogene Sicherheitsfunktionen auf der Grundlage von Identitätsinformationen. Diese Funktionen werden hauptsächlich als Cloud-Service bereitgestellt. Eine effektive SASE-Lösung muss eine Reihe von Mindestanforderungen erfüllen, die im Folgenden zusammengefasst werden.

Hardwareneutralität

Herkömmliche Zweigstellen- und Site-to-Site-Hardwarearchitekturen haben vielen Unternehmen gute Dienste geleistet. Allerdings haben sie auch zur Anhäufung von Geräten in jeder Filiale geführt, wovon jede nur eine Funktion erfüllt. Dieser Appliance- Ausbreitung ist nicht flexibel genug, erfordert mehrere Management-Systeme, um Änderungen vorzunehmen, und Mitarbeiter, die mit den Produkten unterschiedlicher Anbieter vertraut sind. Außerdem benötigt dieser IT-Ansatz übermäßig viel Platz und Strom. Das Unternehmen ist zudem an eine herstellerabhängige Architektur gebunden und kann nicht problemlos auf andere Technologie umsteigen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Mit einer Single-Stack-Softwarelösung, die auf einem Bare-Metal-Server als VM oder Container bereitgestellt wird, kann man hingegen viel Platz, Energie, Zeit und Aufwand sparen. Gleichzeitig zeichnet sich eine derartige Lösung durch eine wesentlich bessere Skalierbarkeit, Performance und Verwaltbarkeit aus. Die Lösung umfasst Folgendes:

- Applikationserkennung
- einen vollständig abgesicherten Stack
- SWG
- SD-WAN und anwendungsbasierte Verkehrssteuerung
- Routing
- Quality of Service (QoS)
- Kompression
- Verschlüsselung
- WAN-Optimierung

Single-Pass-Architektur

In einer Umgebung mit getrennten Single-Service- Geräten werden Pakete von einem Gerät an das nächste weitergegeben. Jedes davon kopiert das Paket in den Speicher, entpackt den Inhalt, analysiert die Daten und den Kontext, wendet eine Entscheidung oder Richtlinie an, verpackt das Paket wieder und leitet es an das nächste Gerät in der Kette weiter. Oft muss jedes Gerät das Paket dekomprimieren/entschlüsseln und diesen Vorgang vor der Übertragung erneut durchführen. Dieser Prozess ist zeitaufwändig und beeinträchtigt die Leistung erheblich.

Eine Single-Pass-Architektur mit Servicekette, wie in Abbildung 1-1 dargestellt, optimiert die Performance, da jeder Vorgang nur einmal ausgeführt werden muss:

- Sie entpackt (und entschlüsselt) das Paket im Speicher.
- Sie macht den Inhalt für alle Sicherheits-, Routing-, Richtlinien, Filter- und ggf. weitere Funktionen kontextbasierend verfügbar.
- Sie verpackt das Paket zur Übertragung (und verschlüsselt es).

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

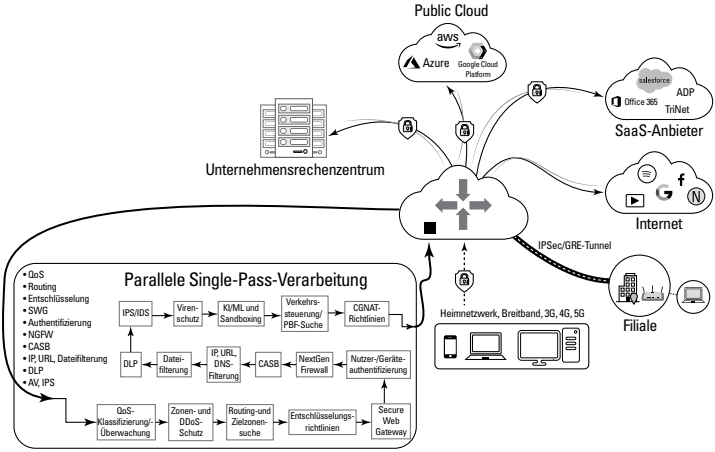


ABBILDUNG 1-1: Verarbeitungsprozess bei einer Single-Pass-Architektur.

Elastische horizontale Skalierung

Eine Single-Pass-Architektur reduziert die Latenzzeit und verbessert die Performance erheblich. Gleichzeitig reduziert sie das Sicherheitsrisiko und den Bedarf an Platz, Strom und speziell geschultem IT-Personal. Sie ist effizient und lässt sich horizontal skalieren, indem mehrere zugrunde liegende Kerne oder Speicher genutzt werden.

Da die integrierte softwarebasierte Lösung auf einem Bare-Metal-Server, auf einer VM oder in einem Container ausgeführt werden kann, ist sie als cloudbasierter Service bereitstellbar, der eine erhöhte Flexibilität bietet.

TECHNISCHES

Durch die Verwendung voll automatisierter Orchestrierungsfunktionen über eine zentrale Oberfläche kann eine Filiale vorübergehend in der Cloud instanziiert und dann ebenso einfach wieder außer Betrieb genommen werden. Ein Homeoffice könnte zum Beispiel als Filiale definiert werden.

Container und Microservices

Ein *Microservice* ist eine serviceorientierte Anwendung, die sauber gekapselt, unabhängig bereitstellbar und skalierbar ist. Jeder Service ist für eine bestimmte Aufgabe zuständig und kommuniziert über einfache APIs mit anderen Services, wenn ein größeres, komplexes Geschäftsproblem gelöst werden muss.

Eine auf einem Microservices-Design basierende cloudnative SASE-Lösung hat eine fließende Architektur, die in Public oder Private Clouds

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

ausgeführt werden kann, was die horizontale Skalierung einfach und flexibel macht.

MERKE!

Die wesentlichen Vorteile einer Microservices-Architektur sind Ausfallsicherheit, Skalierbarkeit und die Fähigkeit, Funktionen zu isolieren.

Globale Verteilung

Durch die Nutzung global verteilter SASE-fähiger Points of Presence (POPs), die über Colocation-Einrichtungen, POPs von Serviceanbietern und Infrastructure-as-a-Service (IaaS) angeboten werden, können Latenzzeiten reduziert und die Leistung von Netzwerksicherheitsservices verbessert werden. Eine SASE-Lösung muss verteilte POPs zur Verfügung stellen, die den Anforderungen digitaler Unternehmen hinsichtlich Zugriffslatenz und Datenhoheit gerecht werden. Dadurch wird auch eine optimale lokalisierte Endnutzererfahrung gewährleistet.

Inline-Verschlüsselung

Beim Schutz von Transaktionen und der Übertragung von Daten spielt Verschlüsselung eine entscheidende Rolle. SASE-Anbieter müssen in der Lage sein verschlüsselte Sitzungen, bei Bedarf und auf der Grundlage von Richtlinien, zu überprüfen. Diese Lösung basiert idealerweise auf einer softwarebasierten und skalierbaren Architektur. SASE-Lösungen sollten die umfassende Inline-Inspektion des verschlüsselten Datenverkehrs (mit Entschlüsselung und anschließender Neuverschlüsselung) ermöglichen, idealerweise aus der Cloud und ohne den Einsatz von proprietärer Hardware.

TIPP

Sie müssen Verschlüsselungsfunktionen für hohe Bandbreiten (Hardware oder Software) zur Verfügung stellen, um Anwendern eine akzeptable QoE zu bieten.

Segmentierung mit Multimandantenfähigkeit

SASE sorgt durch die Isolierung und Segmentierung des Datenverkehrs für ausreichenden Schutz. Cloudnative SASE-Architekturen sind multimandantenfähig, d. h. mehrere Kunden können die zugrunde liegende Transportebene gemeinsam nutzen. Eine Architektur mit nur einer einzigen Instanz ist hingegen mit potenziell höheren Kosten verbunden.

Bei einer mehrinstanzenfähigen Architektur werden Betriebsumgebung, Konfigurationen, Profile, Berechtigungen, Richtlinien und die Abwicklung der Datenübertragung jedes Mandanten vollständig voneinander getrennt. Dadurch wird eine hohe Sicherheit zwischen den einzelnen Partitionen der gemeinsam genutzten Ressource gewährleistet.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Diese Partitionierung sorgt für eine hohe Zuverlässigkeit, Verfügbarkeit und Skalierbarkeit und bringt gleichzeitig Kosteneinsparungen, Flexibilität und Sicherheit für die IT-Abteilung mit sich. Eine mehrinstanzenfähige Plattform lässt sich leicht skalieren und an steigende Anforderungen anpassen.

MERKE!

Eine mehrinstanzenfähige Architektur muss unbedingt *alle* Umgebungen jedes Mandanten umfassen, nämlich die Verwaltungs-, die Steuerungs- und die Datenübertragungsebene.

TIPP

Jede gemeinsam genutzte SASE- oder Cloud-Ressource, ob Gateways, Controller und Orchestrierungsplattformen, muss mehrere Instanzen unterstützen.

Bereitstellung einer SASE-Lösung

Eine effektive SASE-Lösung muss flexible On-Premises-, Cloud- oder kombinierte Hybridmodelle unterstützen. Sie muss einheitliche Sicherheits-, Netzwerk- und Unternehmensrichtlinien vor Ort und in der Cloud bereitstellen – und dies für Benutzer und Daten, die sich an jedem beliebigen Ort der Welt befinden können.

Eine flexible SASE-Lösung bietet eine globale cloudnative Architektur, in der Cloud-Instanzen einfach per Mausklick bereitgestellt werden können – unabhängig davon, ob es sich um eine Public, Private oder eine Kombination von beiden handelt.

Sie verbindet einen Endnutzer dauerhaft mit dem optimalen SASE-Gateway und berücksichtigt dabei die Entfernung zwischen Endnutzer und SASE-Gateway sowie die Serviceauslastung auf den SASE-Gateways.

TIPP

Eine SASE-Infrastruktur beseitigt die mit der Interkonnektivität von Multi-Cloud-Architekturen verbundenen Herausforderungen und stellt eine nahtlose, dynamische und sichere Overlay-Konnektivität zur Datenübertragungs- und Steuerungsebene jeder Cloud her.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- **Transformation des Netzwerkperimeters**
- **Konsolidierung von Komplexität und Kosten**
- **Optimierung von Sicherheit und Leistung**
- **Digitale Transformation als Priorität**

Kapitel 2
Ein modernes Unternehmen werden

Die Geschäftsabwicklung moderner Unternehmen erfolgt in der Client-to-Cloud-Ära. Laut Gartner wurden „Netzwerk- und Netzwerksicherheitsarchitekturen für ein sich seinem Ende näherndes Zeitalter entwickelt und sind nicht in der Lage, die dynamischen Anforderungen an den sicheren Zugriff von digitalen Unternehmen effektiv zu erfüllen". Vorbei ist die Zeit, in der alle Mitarbeiter in einem physischen Gebäude arbeiteten und alle Ihre Unternehmensressourcen in privaten Rechenzentren gehalten wurden, die sowohl physisch als auch digital gesichert waren.

Das Unternehmensrechenzentrum ist nicht mehr der Fokus für Anwendungen, und der fixe Netzperimeter existiert nicht mehr. Initiativen zur digitalen Transformation und die Einführung von SaaS-Anwendungen (Software as a Service) und Cloud-basierten Services haben das Unternehmensnetzwerk vollständig verändert. In der heutigen IT-Welt:

- arbeiten Nutzer mehr außerhalb des traditionellen Unternehmensnetzwerks als innerhalb.
- werden mehr Workloads in der Cloud als im Unternehmensrechenzentrum verarbeitet.
- werden SaaS-Anwendungen häufiger als lokal installierte Anwendungen verwendet.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

- befinden sich mehr sensible Daten außerhalb als innerhalb des Unternehmensrechenzentrums.
- ist mehr Datenverkehr für öffentliche Cloud-Dienste bestimmt als für das Unternehmensrechenzentrum.
- fließt mehr Datenverkehr von Zweigstellen zu öffentlichen Clouds als zum Unternehmensrechenzentrum.

In diesem Kapitel erfahren Sie mehr über die Sicherung des neuen softwaredefinierten Netzwerkperimeters, die Aufrechterhaltung und Verbesserung der Quality of Experience (QoE) und der Anwendungsleistung, die Trends der digitalen Transformation in modernen Unternehmen und darüber, wie Sie die Hardware- und Netzwerkkomplexität reduzieren und gleichzeitig Ihr Netzwerk vereinfachen und das Management rationalisieren können.

Erweiterung des Netzwerkperimeters

Jahrzehntelang setzten Unternehmen auf verschiedene WAN-Technologien (Wide Area Network), wie Mietleitungen, Frame Relay und Asynchronous Transfer Mode (ATM), um physische Standorte sicher zu verbinden. In jüngerer Zeit wurde Multiprotocol Label Switching (MPLS) zur weitverbreiteten WAN-Technologie für sichere Verbindungen zwischen Unternehmensstandorten und schuf damit einen geschützten Bereich hinter der Gartenmauer.

Der Perimeter ist im Wandel begriffen und MPLS ist hervorragend geeignet, Unternehmensbüros sicher miteinander zu verbinden. Es ist jedoch teuer, unflexibel, auf eine feste Bandbreite begrenzt, langsam in der Bereitstellung und unzureichend für die Verbindung von Home-Offices, mobilen Geräten oder zeitweiligen Standorten.

Das gestrige Festnetzwerk hat statische Zweigstellen über dedizierte MPLS-Leitungen mit einem Hub-Standort und/oder einer Unternehmenszentrale oder einem Rechenzentrum verbunden. Alles war privat. Es war sicher, weil es privat war. Heutige Client-to-Cloud-Netzwerke verbinden WFA- Benutzer (Work-from-Anywhere) von zu Hause und an mobilen Standorten über das Internet mit global verteilten Cloud-Ressourcen, wobei Workloads auf Kosten, Leistungsanforderungen oder Bedarfsvolumen basierend dynamisch den Standort wechseln können. In einem cloudzentrierten Unternehmen sind Nutzer und Geräte omnipräsent, ebenso wie die Netzwerkfunktionen, auf die sie einen sicheren Zugriff benötigen. Das bedeutet, dass auch sichere Zugangsdienste überall verfügbar sein müssen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Der fixe Gebäudeperimeter von gestern wurde auf einen softwaredefinierten Client-to-Cloud-Perimeter erweitert, der zeitweise zwischen einem WFA-Nutzergerät, das über das Internet mit einem dynamischen Cloud-Standort verbunden ist, existiert. Für diesen Client-to-Cloud-Perimeter sind genaue und dynamische Sicherheitsmaßnahmen, die auf Identität und Kontext basieren, unverzichtbar.

Arbeiten mit älteren WANs

Herkömmliche WAN-Architekturen sicherten den unternehmensweiten Perimeter, indem sie den gesamten Zugriff auf Ressourcen außerhalb des Unternehmens (einschließlich der Cloud) über eine zentralisierte Internetverbindung sicherten, die vom Sicherheitsteam verwaltet und mit Firewalls geschützt wurde, wie in Abbildung 2-1 dargestellt. Stellen Sie sich die Komplexität, die Warteschlangen und die Verzögerungen vor, wenn alle international fliegenden Passagiere durch einen einzigen internationalen Flughafen geschleust würden. Wie würde sich das anfühlen?

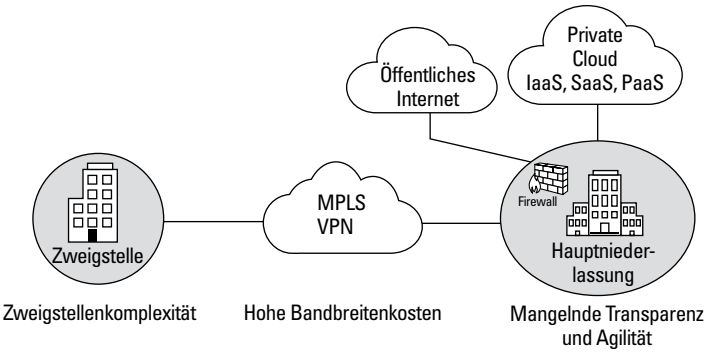


ABBILDUNG 2-1: Herkömmliche WAN-Architektur

Wenngleich Legacy-Architekturen in der Vergangenheit, als sich alle Mitarbeiter und Unternehmensressourcen an fixen, privaten Unternehmensstandorten befanden und der Internetzugang für geschäftliche Zwecke minimal war, hinreichend gut funktionierten, wiesen sie dennoch erhebliche Nachteile auf:

- Signifikante Zweigstellenkomplexität
- Hohe Bandbreitenkosten
- Mangelnde Transparenz und Agilität

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Arbeiten mit modernen WANs

SD-WAN 1.0-Lösungen integrierten das Internet als alternative Transportoption zu MPLS, wobei die alte Netzwerktopologie beibehalten wurde, wie in Abbildung 2-2 dargestellt. Dadurch konnten die MPLS-Kosten gesenkt werden, aber es wurde weder die Sicherheit noch die schlechte QoE für Cloud- und SaaS-Anwendungen angesprochen. Nutzer wurden nicht direkt mit der Cloud verbunden.

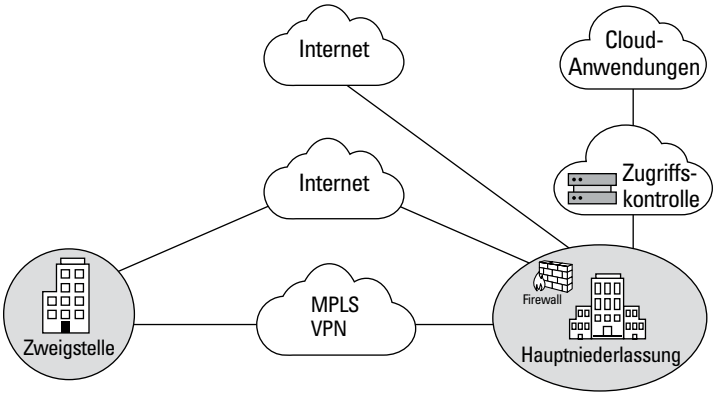


ABBILDUNG 2-2: SD-WAN 1.0-Architektur.

Diese Lücke konnte zwar mit der Nachrüstung von Sicherheitslösungen geschlossen werden, was aber mit zusätzlichen Kosten und Komplexität einherging, da an jedem Standort mehrere zweckgebundene Appliances vorhanden waren – eine erhebliche Belastung in einem Netzwerk mit vielen kleinen Standorten wie zum Beispiel im Einzelhandelsgeschäften.

TECHNISCHES

Nachträglich implementierte Sicherheitslösungen boten jedoch nur Cloud-Sicherheit für den ausgehenden Datenverkehr, während Standorte weiter Internetbedrohungen durch den eingehenden Datenverkehr aus der Cloud ausgesetzt blieben. Zur Kontrolle und Segmentierung des Datenverkehrs, zum Schutz vor DoS-Angriffen (Denial of Service) sowie zur Unterbindung einer seitlichen Ausbreitung von Malware und Angreifern erfordert der Perimeter in der Filiale weiter Sicherheitsmaßnahmen vor Ort. Eine Bank könnte beispielsweise aus Compliance-Gründen den Datenverkehr für Einzelhandel, Geldautomaten und Investmentservices segmentieren oder ein Unternehmen könnte den Gast-WLAN-Datenverkehr auf Basis von Sicherheitsrichtlinien segmentieren. Einige Unternehmen könnten ausgehenden HTTP-Datenverkehr (Hypertext Transfer Protocol) über einen Cloud-Sicherheitsdienst prüfen, aber On-Premises-Sicherheit zum Schutz des Nicht-HTTP-Datenverkehrs

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

bereitstellen. Die entscheidende Komponente in jedem Szenario ist die einfache und kosteneffiziente Einbettung der Sicherheit in das SD-WAN über den gesamten Enterprise-Edge.

MERKE!

Eine Lösung der zweiten Generation – sicheres SD-WAN – umfasst den kompletten Netzwerkbetrieb und integrierte Sicherheit in einem einzigen Software-Stack. Diese Lösung, wie in Abbildung 2-3 dargestellt, ermöglicht es Unternehmen schließlich, an jedem Standort eine sichere Direktausfahrt aus dem Internet zu implementieren und eine Expressauffahrt zu Cloud- und SaaS-Anwendungen zu schaffen. Diese Architektur bietet darüber hinaus

- Vereinfachung, mit einem einzigen Gerät an jedem Standort
- Niedrigere Bandbreitenkosten
- Mehr Agilität und Transparenz
- Koexistenz mit erweiterter Cloud-Sicherheit

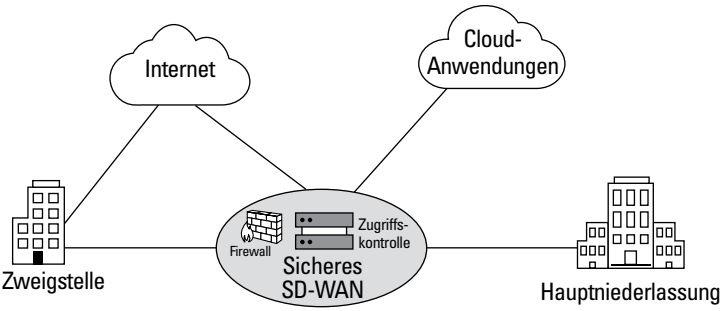


ABBILDUNG 2-3: Sichere SD-WAN-Architektur

Reduzierung der Hardwarekomplexität und -kosten

Der an jedem Standort eines Unternehmensnetzwerks bereitgestellte Stapel proprietärer Appliances führt schnell zu einem Anstieg der Kosten und Komplexität. In der Regel handelt es sich um Produkte für einzelne, punktuelle Aufgaben von einer Vielzahl von Anbietern, auf die Folgendes zutrifft:

- IT-Mitarbeiter müssen Kenntnisse vieler verschiedener herstellerspezifischer Schnittstellen und technischer Produktdetails besitzen
- Erfordern eine manuelle und fehleranfällige Koordination von Konfigurationen und Richtlinien

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

- Weisen sehr unterschiedliche Funktionalität für die Fehlerbehebung auf
- Mangelnde „Dashboard"-Sichtbarkeit über das gesamte Netzwerk hinweg
- Sind nicht automatisiert
- Erfordern die Verfolgung vieler Software-Versionen und Sicherheits-Patches

Die gravierende Zunahme von Appliances ist ein maßgebliches Hemmnis für das schnelle und flexible Handeln eines Unternehmens. Jede kleine Änderung erfordert mehrere Eingriffsstellen und mehrere Wartungsfenster.

Sichere SD-WAN-Lösungen der zweiten Generation, wie in Abbildung 2-4 dargestellt, überwinden diese Herausforderung, indem sie umfassende Netzwerk- und Sicherheitsfunktionen in einem einzigen Software-Stack integrieren. Dies ist der bevorzugte Ansatz für moderne Unternehmen und wird voraussichtlich der primäre Ansatz für eine sichere Site-to-Site- und direkte Client-to-Cloud-Konnektivität zwischen Nutzern und Cloud-Ressourcen bleiben. Darüber hinaus kann eine sichere SD-WAN-„Zweigstelle" auf einer virtuellen Plattform in der Cloud bereitgestellt werden, was mehr Bereitstellungsflexibilität und Agilität für die Handhabung des Datenverkehrs bietet, der nicht von einem physischen Gebäude ausgeht. Dieser Ansatz erlaubt zudem eine Automatisierung und eine zentrale Dashboard-Sichtbarkeit für alles im Netzwerk, einschließlich Internet und Cloud-Netzwerksegmenten.

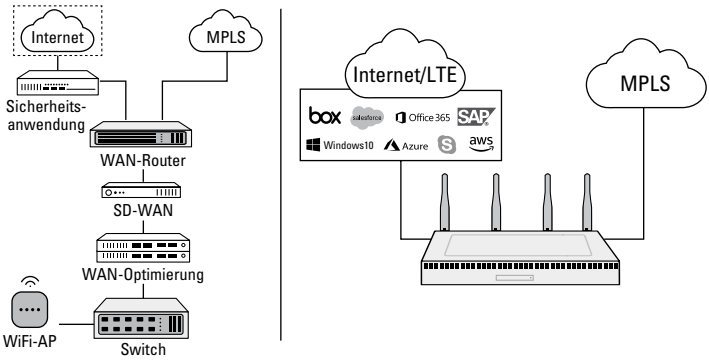


ABBILDUNG 2-4: Sichere SD-WAN-Appliance-Konsolidierung.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Mehr Sicherheit und mehr Leistung

Unternehmen stehen im Zusammenhang mit der Bereitstellung von sicheren Client-to-Cloud-Verbindungen in älteren Netzwerk- und Sicherheitsarchitekturen vor großen Herausforderungen. Aufgrund des weitgesteckten strukturlosen Perimeters und der allgegenwärtigen Internetkonnektivität des modernen Netzwerks bieten die Mitarbeiter und Ressourcen eines Unternehmens eine erheblich größere Angriffsfläche für die Arten, den Umfang und die Raffinesse der Bedrohungen, denen Ihre Nutzer und Ressourcen ausgesetzt sind.

Zu den wichtigsten IT-Herausforderungen zählen

- **Benutzerfreundlichkeit:** Die IT muss eine konsistente, verlässliche und sichere Nutzererfahrung anhand einer automatisierten, umfassenden Richtlinie auf der Basis von Nutzeridentität, Kontext, Sicherheits-/Compliance-Richtlinien des Unternehmens und einer kontinuierlichen Vertrauensbewertung bieten.
- **Sicherheit:** Um Compliance-Standards zu erfüllen und Netzwerkumgebungen mit strukturlosen Perimetern zu schützen, muss sich das Unternehmen vor Angriffen an allen Internet-Berührungspunkten schützen. Dies ist der neue Perimeter.
- **Transparenz:** Die IT benötigt eine Echtzeit- und historische Sicht von Nutzern, Geräten, Anwendungen und Sitzungen, unabhängig vom Standort, gleich, ob privat oder öffentlich. Das Netzwerk muss in der Lage sein, die durchschnittlich zur Identifizierung der Ursache eines Problems erforderliche Zeit zu verkürzen.
- **Automatisierte Kontrolle:** Die Umgebung muss eine einheitliche Richtlinienautomatisierung für Nutzer, Netzwerk und Sicherheit bieten, die dynamisch und automatisch durchgesetzt wird.
- **Sparen, um zu investieren:** Die IT muss alle oben genannten Punkte ohne Erhöhung der Personalzahlen oder des Budgets erreichen. Das Erarbeiten von Möglichkeiten, das Unternehmen und sein Netzwerk zu modernisieren und zu transformieren und gleichzeitig Geld zu sparen, ist für moderne Unternehmen von entscheidender Bedeutung.

Hintergründe der Trends zur digitalen Transformation

Die Trends zu Cloud Computing und Cloud Storage, SaaS, Infrastructure as a Service (IaaS), Mobilität, allgegenwärtiger Internetkonnektivität und WFA-Mitarbeitern machen herkömmliche WAN-Architekturen

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

obsolet. Diese Trends erfordern fortschrittliche Sicherheitslösungen für den Schutz Ihrer Nutzer und Ressourcen.

Einführung von Cloud und Mobilität

Eine ältere WAN-Architektur – mit einem einzigen Internet-Zugangspunkt in einer sicheren, hinter einer leistungsstarken Firewall abgeschotteten Unternehmenszentrale – wird ein Unternehmen, das nur eine einzige Cloud nutzt, dennoch nur mit Mühe versorgen können, und das mit Defiziten bei QoE und schwächerer Anwendungsleistung aufgrund der suboptimalen Konnektivität und des unzureichenden Routings des Datenverkehrs.

MERKE!

Multicloud-Migration wird schnell zur Norm, aber älteren WAN-Architekturen fehlt es gänzlich an der für die Versorgung einer Multicloud-Umgebung erforderlichen Funktionalität. Die herkömmliche Hub-and-Spoke-Konnektivität zur Verbindung von Nutzern in Filialen über statische MPLS-Leitungen mit einer Firewall im Rechenzentrum funktioniert in modernen Multicloud-Umgebungen einfach nicht, wo der Internet-Perimeter in ein verteiltes Modell übergegangen ist, in dem jede Filiale und jeder Nutzer direkten und optimierten Cloud-Zugriff haben muss.

Für den ordnungsgemäßen Betrieb von Multicloud ist eine Kombination von SD-WAN und mehrstufiger Sicherheit erforderlich. Die Verbindung einer Unternehmensgeschäftsstelle mit mehreren Clouds erfordert cloudintelligente, dynamische Multipath-Konnektivität und robuste Netzwerk- und Sicherheitsfunktionen wie Routing, SD-WAN, CGNAT (Carrier-Grade Network Address Translation), DOS-Prävention, stateful Firewall, NGFW (Next-Generation Firewall), URL-Filterung (Uniform Resource Locator), DLP (Data Loss Prevention), IPS (Intrusion Prevention System), Virenschutz, IP-Filterung (Internet Protocol), Dateifilterung, Anti-Malware, Erkennung von seitlicher Ausbreitung und SSL-Proxy (Secure Sockets Layer).

TIPP

Der Schlüssel zu einer reibungslosen Multicloud-Migration ist eine integrierte, vielseitige und cloudnative Multi-Service-Plattform mit integrierter Sicherheit.

Weitgehende Akzeptanz des mobilen Arbeitens

Infolge der COVID-19-Pandemie ist ein mehrheitliches WFA-Personal praktisch über Nacht zur Realität geworden. Die staatlich verordnete Quarantäne zuhause führte zu einem dramatischen Anstieg des zuvor nur langsam ansteigenden Trends. Ein hoher Prozentsatz der

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Unternehmen akzeptiert heute, dass WFA die „neue Normalität“ ist und erwartet für die Zukunft eine deutlich stärkere gemeinsame Nutzung von Immobilien, die die alte Norm von unternehmenseigenen und für nur einen Zweck oder eine Aktivität bestimmten Gebäuden ersetzt.

Unternehmensnutzer sind unter anderem Mitarbeiter, Kunden und Partner, die Multicloud-gehostete Anwendungen von überall nutzen – zu Hause, in Filialen, auf dem Campus oder unterwegs. Diese Client-to-Cloud-Ära erfordert dynamische, sichere und zuverlässige Nutzer- und Anwendungserfahrungen. Ein digitales Unternehmen muss Folgendes sein:

- Für Kunden von überall zugänglich
- Ein überall verfügbares digitales Geschäftsportal

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- Nutzung eines SD-WAN als Ausgangspunkt
- Definition eines echten SD-WAN
- Bereitstellung eines konsistenten Erfahrung

Kapitel 3
Netzwerktechnik als Ausgangspunkt

Das Ziel von Secure Access Service Edge (SASE) ist es, Nutzern einen sicheren WFA-Zugriff (Work-from-Anywhere) auf alle Anwendungen und Daten zu ermöglichen, unabhängig davon, ob diese in einem Rechenzentrum, auf einer Cloud-Plattform oder bei einem SaaS-Anbieter (Software as a Service) bereitgehalten werden. Das ist, was heutige Unternehmen wollen und brauchen.

In diesem Kapitel erfahren Sie, wie SD-WAN-Technologie (Software-Defined Wide Area Network) mit der Bereitstellung dieser Funktionalität die Grundlage von SASE bildet. SD-WAN ist der Schlüssel zu SASE und die Technologie der Wahl, die dem Unternehmen sozusagen als WAN-Auffahrtsrampe zu SASE und Multicloud-Konnektivität dient. SASE umfasst gehostetes SD-WAN, Sicherheit und Routing in der Cloud.

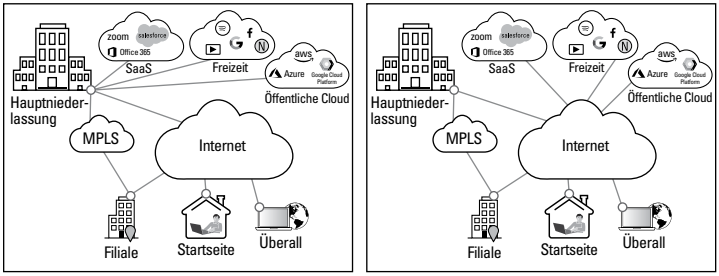
Aufbau auf SD-WAN

Trends bei Cloud Computing und Services, verteilten Workloads, wachsenden WFA-Mitarbeiterzahlen und Direct Internet Access (DIA) haben herkömmliche WAN-Architekturen überholt.

SD-WAN-Technologie ermöglicht eine Client-to-Cloud-Architektur: Internetbasierte Backbones, Routing des Datenverkehrs von überall, direkter Cloud-Zugriff und Pfadauswahl zur Optimierung der QoE (Quality of Experience). Abbildung 3-1 vergleicht die Netzwerke der

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Vergangenheit mit den Netzwerken, die wir in den heutigen Unternehmen sehen.



Netzwerke in der Vergangenheit | Netzwerke heute

ABBILDUNG 3-1: Modernisierung der Netzwerkpfade.

Verwendung von Anschlussstellen

Der *Service Edge* ist der Point of Presence (POP), an dem der Datenverkehr von WFA-Endpunkten und Cloud-Anwendungen gesichert und direkt – oder über den besten alternativen Pfad – zum Ziel weitergeleitet wird, ohne durch einen starren Mittelpunkt gezwängt zu werden.

TIPP

Die SASE-Technologie muss an jeder Auf- und Abfahrtsstelle bereitgestellt werden, um – unabhängig vom Standort – den Datenverkehr zwischen Nutzern, Geräten und Cloud-Ressourcen zu sichern.

Auffahrt mit SD-WAN-Technologie

Die SD-WAN-Technologie bietet mehrere Schlüsselfunktionen zur Ermöglichung einer optimalen Performance in einer Client-to-Cloud-Umgebung:

- Applikationserkennung und Datenklassifizierung
- DIA und intelligente Verkehrssteuerung
- Globale Gateways zur Sicherung der Auffahrt von jedem Standort aus

Beim Routing des Datenverkehrs von WFA-Mitarbeitern muss der Anwendungsdatenverkehr genau und sofort klassifiziert werden. Wenn die Kinder zuhause zusammen über eine Breitbandverbindung lernen und der Ehepartner bei einer Konkurrenzfirma arbeitet, dann sind die Anwendungsklassifizierung, die Sicherheit, die Priorisierung und Steuerung des Datenverkehrs Ihres Mitarbeiters bis hin zum Endgerät von größter Bedeutung.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Die Anwendungsklassifizierung erfolgt mittels Deep Packet Inspection (DPI) auf Basis von Anwendungssignaturen und heuristischer Analyse, die dynamisch und regelmäßig aktualisiert werden. Mithilfe der Anwendungsklassifizierung wird die Anwendungskategorie identifiziert. Anwendungskategorien können Anwendungsfamilien und -unterfamilien, Risiko-Tags, Produktivitäts-Tags und ein Tag umfassen, das den Datenverkehr als geschäftsorientiert oder nicht kennzeichnet.

TECHNISCHES

Wenn die DPI-Engine die vollständig qualifizierten Domänennamen (FQDN) und IP-Adressen (Internet Protocol) von SaaS-Anbietern dynamisch abfragen kann, beginnt die SaaS-Anwendungsidentifizierung bereits beim ersten Paket im Datenstrom. So wird sichergestellt, dass alle Datenströme sofort mit den entsprechenden Richtlinien verknüpft und entsprechend behandelt werden.

SD-WANs sind deutlich agiler und mit geringeren Transportkosten über Ihr gesamtes Netzwerk hinweg verbunden als herkömmliche Architekturen. Der Einsatz eines lokalen DIA-Breakout in Zweigstellen oder für mobile Mitarbeiter erlaubt dem Datenverkehr, den effizientesten und optimalen Pfad für den Zugriff auf Cloud-Anwendungen zu nutzen.

HINWEIS

Diese neu erschlossenen Internet-Routen vergrößern die Angriffsfläche Ihres Netzwerks – Gefahr durch Malware und Angriffe – im Vergleich zum herkömmlichen privaten MPLS-Netzwerk (Multiprotocol Label Switching) erheblich.

Die Sicherung des DIA-Datenverkehrs ist eine primäre Aufgabe von SASE. SASE muss jede Sitzung und jeden Standort schützen und seine Sicherheitsfunktionen umfassen deshalb zumindest Folgendes:

- Eine voll funktionsfähige NGFW-Firewall (Next-Generation Firewall)
- URL-Filterung (Uniform Resource Locator)
- SSL-Verschlüsselung/-Entschlüsselung (Secure Sockets Layer)
- IDPS (Intrusion Detection and Prevention System)
- Antivirus
- Anti-Malware
- SWG (Secure Web Gateways)
- ZTNA (Zero Trust Network Access)
- CASB (Cloud Access Security Brokers)
- DLP (Data Loss Prevention):

SD-WAN-Gateways sind weltweit verfügbar und bieten verteilten, sicheren, zuverlässigen und leistungsstarken Zugriff auf

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Cloud-Anwendungen, -Services und -Ressourcen zusätzlich zur SASE-Bereitstellung über die Cloud. Unternehmen können über eigene Gateways (ihren eigenen SASE-Service) verfügen oder Provider-Gateways (den SASE-Service eines Anbieters) nutzen.

Wie in Abbildung 3-2 dargestellt, authentifizieren Gateways Nutzer, autorisieren mit ZTNA geschützten Anwendungszugriff und sichern das Unternehmensnetzwerk vor externen Bedrohungen und optimieren gleichzeitig die QoE und den Direktzugriff auf Cloud-Anwendungen. SD-WAN-Cloud-Gateways mit integrierten SASE-Funktionen bieten umfassende Sicherheit und QoE für Geschäftsanwendungen sowie eine direkte, optimale Steuerung des Cloud-/SaaS-Datenverkehrs.

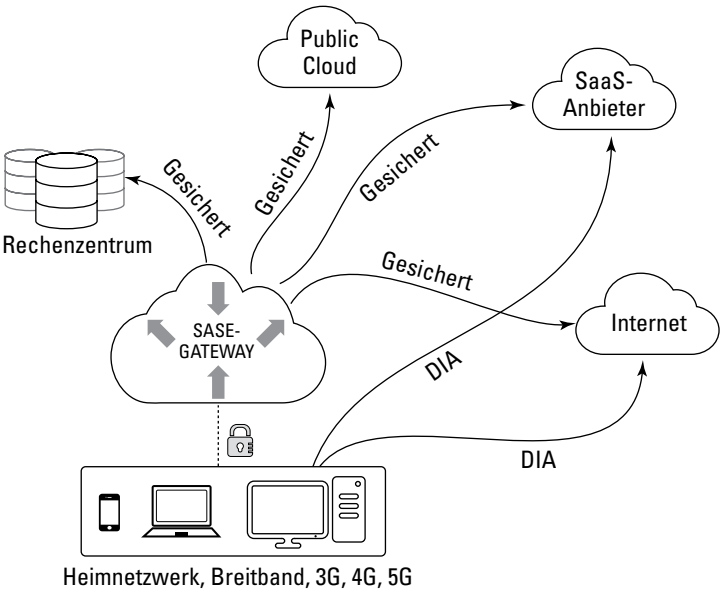


ABBILDUNG 3-2: SASE-Gateway für Nutzer und Geräte.

Integrierte Sicherheit: die Grundlage von SD-WAN

Kontextbezogene Sicherheit gewährt Zugriff auf Basis mehrerer Faktoren, einschließlich der Identität der Entität, des Echtzeitkontexts, der Sicherheits- und Compliance-Richtlinien des Unternehmens und der kontinuierlichen Bewertung der Vertrauenswürdigkeit im Verlauf der Sitzungen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

MERKE!

Secure SD-WAN ist eine einheitliche Software-Stack-Architektur mit integrierten Sicherheitsfunktionen, die nahtlosen kontextbezogenen Schutz basierend auf Nutzer, Gruppe, Standort, Gerät, Verhalten, Anwendung und Inhalt bietet. Integrierte Funktionen sind unter anderem

- **Schutz Ihrer Nutzer, Standorte und Geräte:** Sicherheit muss dort greifen, wo der Datenverkehr im Netzwerk eintrifft und wo er es verlässt – unabhängig vom Standort: zuhause, mobiler Standort, Zweigstelle oder Cloud-Software-Workload. Datenverkehr kann sich an jedes beliebige Internetziel richten. Sicherheitsmaßnahmen müssen dynamisch inline auf alle Datenströme und auf Basis des mit dem jeweiligen Datenstrom verbundenen Risikos angewendet werden.
- **Besondere Sicherheitsüberlegungen für Cloud-Services:** Ein SD-WAN bietet SaaS-Optimierung, DIA-Sicherheit und Cloud-Gateways. Die SASE-Funktion des SD-WAN stellt sicher, dass der gesamte Datenverkehr auf jedem Pfad gesichert ist. In einer VPC-Implementierung (Virtual Private Cloud) kann ein virtueller SD-WAN-Standort mit SASE vorhanden sein, um der VPC dieselbe Sicherheit wie der „Filiale" zu bieten.
- **Bedrohungen stoppen, bevor sie zu großen Problemen werden:** Cloud-Migration, hybride Computerumgebungen und WFA – sowie immer ausgefeiltere Angriffe – stellen eine Bedrohung dar, die einen disziplinierten und dynamischen Sicherheitsansatz erfordert, der über Verteidigungs- und Perimeterstrategien hinausgeht. Unternehmen benötigen heute eine aktive, umfassende Cybersicherheit, die eine kontinuierliche Überwachung, schnelle Reaktion auf Vorfälle und proaktive Bedrohungsbewertung umfasst. Und all das bei gleichzeitiger Optimierung der Anwendungs-Performance und QoE.
- **Integration von Sicherheit für den gesamten Datenverkehr und Sicherung des Zugriffs für alle Endpunkte:** SD-WAN-Sicherheit muss heute verteilt, durch cloudbasierte Präsenz ergänzt, flexibel, einfach und überall verfügbar sein.

Echtes SD-WAN

Nicht allen SD-WAN-Architekturen liegt die für die heutige Bedrohungslandschaft erforderliche reibungslose Edge-Sicherheit inne. Unterschiedliche SD-WAN-Architekturen, -Designs und -Bereitstellungsansätze liefern unterschiedliche Ergebnisse.

SASE ist eine Erweiterung der SD-WAN-Funktionen zur Bereitstellung einer cloudbasierten Netzwerk- und Sicherheitslösung. Die Umsetzung

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

erfolgt über ein verteiltes System aus Edge-Software und Cloud-Gateways, um konsistente, einheitliche und globale Richtlinien über Cloud-, Heim-, Mobil- und On-Premise-Standorte hinweg durchzusetzen. SD-WAN ist die Auffahrtsrampe zu SASE und die Technologie der Wahl für Unternehmens-WAN und Multicloud-Konnektivität. SASE umfasst gehostetes SD-WAN, Sicherheit und Routing in der Cloud. Da SD-WAN die Grundlage für SASE bildet, müssen Unternehmen die wesentlichen Attribute berücksichtigen, die für eine echte SD-WAN-Lösung erforderlich sind.

Cloud-Gateways erweitern das SD-WAN-Backbone eines Unternehmens von den Standorten (Filialen, regionale Standorte, Campus, Rechenzentren und Home Offices) bis zur „Türschwelle" von SaaS und anderen Cloud-Ressourcen rund um die Welt. SASE konvergiert Netzwerk- und Sicherheitsdienste in der Cloud, vor Ort oder als Kombination aus beidem, wie in Abbildung 3-3 dargestellt.

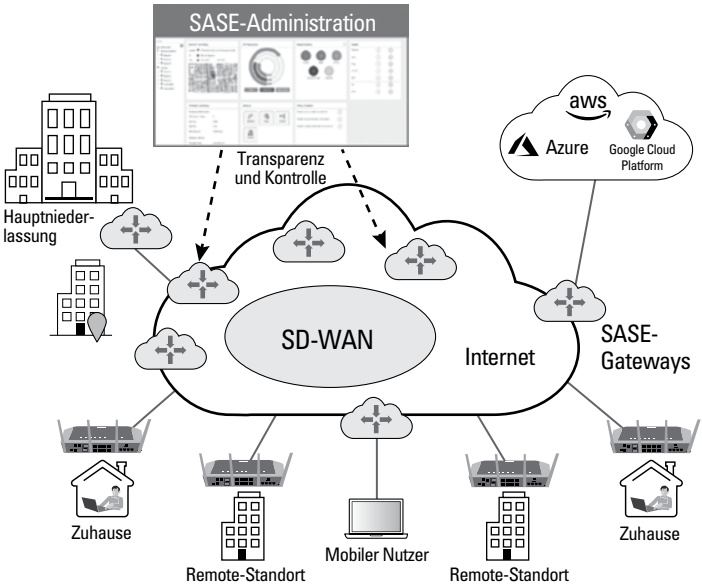


ABBILDUNG 3-3: SD-WAN ist die Grundlage von SASE.

In den nächsten Abschnitten erfahren Sie mehr über einige der Attribute, die ein echtes SD-WAN auszeichnen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Erweiterte Routing-Funktionen

Einige SD-WAN-Umgebungen erfordern erweiterte Routing-Funktionen, um einen reibungslosen Datenverkehr und eine gute QoE zu gewährleisten. Diese Umgebungsattribute sind unter anderem

- das Vorhandensein von Underlay- und Overlay-Netzwerken
- individuelle, dynamische IPsec-Tunnel (Internet Protocol Security) für den sicheren Zugriff auf Gateways und andere Cloud-Ressourcen
- ein zwischengelagertes Netzwerk zur Verbindung der Cloud-Gateways, die ein Traffic-Engineering-Protokoll ausführen, um die beste QoE zu gewährleisten, indem der optimale Pfad zu SaaS, Cloud-Serviceprovidern und Remote-Standorten auf der Grundlage des angebotenen End-to-End-Service-Level-Agreements (SLA) ausgewählt wird.

TECHNISCHES

SD-WAN-Netzwerke bieten Skalierbarkeit, Anpassungsfähigkeit und schnelle Ausfallkonvergenz, unabhängig davon, ob sie vor Ort, in der Cloud oder durch eine Hybridlösung bereitgestellt werden. SD-WANs bieten leistungsstarkes, anwendungsbewusstes, intelligentes Routing, das durch die Optimierung von Routingprotokollen eine hohe QoE-Skalierbarkeit garantiert, dies umfasst

- Internet Protocol Version 4 (IPv4), statisches Routing
- Internet Protocol Version 6 (IPv6), statisches Routing
- Open Shortest Path First, Version 2 (OSPFv2)
- Open Shortest Path First, Version 3 (OSPFv3)
- Border Gateway Protocol (BGP)
- Multiprotokoll-Erweiterungen für BGP (MP-BGP)
  - MPLS-basierte virtuelle private Layer-3-Netzwerke (VPNs)
  - MPLS-basierte Ethernet VPNs (EVPNs)
  - Virtual Extensible LAN (VXLAN)-basiertes EVPN
- Routing Information Protocol (RIP)
- Internet Group Management Protocol, Version 2 (IGMPv2)
- Internet Group Management Protocol, Version 3 (IGMPv3)
- Protocol Independent Multicast Sparse Mode (PIM-SM)
- Protocol Independent Multicast Source-Specific Multicast (PIM-SSM)
- Virtual Router Redundancy Protocol (VRRP)
- Policy-basiertes Routing (PBR)

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Bidirektionale Weiterleitung (bidirectional Forwarding, BFD) wird in Verbindung mit Routingprotokollen zur Zustandsüberwachung auf der Kontrollebene und zur Ermöglichung einer schnellen Ausfallkonvergenz verwendet.

Ein SD-WAN bietet die Steuerung des Datenverkehrs pro Paket, Richtlinien pro Anwendung, FEC (Forward Error Correction), Replikation, Erstpaketidentifizierung von SaaS-Anwendungen, aktives Sondieren, passive Inline-Überwachung und kombinative Bewertungsberechnungen für die Pfadauswahl.

SD-WAN unterstützt zahlreiche erweiterte Funktionen, darunter

- **Erweiterte Sprach- und Videofunktionen:** In der Industrie gilt das MOS (Mean Opinion Score) als das beste Maß für die Sprach- und Video-QoE. Basierend auf Konfiguration und Underlay-Performance werden Sprach- und Videodatenströme dynamisch auf den Pfad umgeschaltet, der die erforderliche MOS-Bewertung bietet.
- **Verkehrskonditionierung und -wiederherstellung:** Bei einer Beeinträchtigung aller verfügbaren Pfade können abhelfende Techniken wie FEC und Paketklonen Datenströme wiederherstellen, bei denen Paketausfälle auftreten.
- **SaaS-Anwendungsoptimierung:** Messungen und Verlaufsberichte der SaaS-Anwendungsleistung nutzen passive Inline-Analysen des TCP-Datenverkehrs (Transmission Control Protocol) und aktive TCP- und HTTP-Probes (Hypertext Transfer Protocol) für jede SaaS-Anwendung. Aktive und passive Leistungskennzahlen werden verwendet, um den besten Pfad für jede SaaS-Anwendung auszuwählen.
- **Erweiterte Routing-Entscheidungen basierend auf End-to-End-SLA:** Bei der Next-Hop-SLA-Überwachung fehlt es an der für zufriedenstellende QoE-Ergebnisse erforderlichen End-to-End-Pfadkenntnis. Um eine hervorragende QoE-Qualität zu erreichen, müssen Entscheidungen zur Verkehrssteuerung auf Basis der End-to-End-SLA des Pfads getroffen werden.
- **Anwendungstransparenz:** SD-WAN erkennt mithilfe einer integrierten DPI-Engine automatisch Tausende von Anwendungen, die verschiedene Mechanismen nutzt, wie zum Beispiel:
  - Netzwerkbasierte Identifikation (Quelladresse, Zieladresse, Port, Protokoll)
  - Signatur-/musterbasierte Identifizierung
  - Protokollparser (wie DPI)
  - Transport Layer Security Handshake

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

- Heuristik
- IPS-Signaturbasierte Identifizierung
- URL-Kategorisierung und -Filterung

Ein SD-WAN muss auch verschlüsselte Anwendungen identifizieren, und die Identifizierung darf durch das Vorhandensein eines Webproxys nicht beeinträchtigt werden.

Servicequalität

TECHNISCHES

Ein SD-WAN-Edge-Gerät sollte die Priorisierung des Datenverkehrs unterstützen (z. B. hoch, niedrig, strikt hoch), ein gewichtetes Verteilungsverfahren (Weighted Round Robin, WRR), hierarchisches Queuing, zufällige Früherkennung auf Zufallsbasis (Random Early Detection, RED), gewichtetes RED, Taildrops, Traffic Shapers, hierarchische Shaper, Traffic Policing und Datenklassifizierung auf Basis eines umfassenden Satzes von Parametern. Darüber hinaus sollte es auch in der Lage sein, Traffic Marking, Remarking, ToS-Berücksichtigung (Type of Service) und Differentiated Services Code Point (DSCP) sowie 802.1p-Prioritätsbits zu verwenden. Remarking und Shaping können auf den Richtlinien von Layer 4 bis Layer 7 basierend konfiguriert werden.

Ein SD-WAN unterstützt außerdem mehrere Eingangswarteschlangen, um sicherzustellen, dass Pakete gemäß konfigurierten Planungsprioritäten verarbeitet werden, um lange Wartezeiten und Latenzen zu vermeiden. Bei einer Überbelegung werden Pakete mit geringerer Priorität (einschließlich SD-WAN-Datenverkehr) bei ihrem Eintreffen im System verworfen.

Optimierung des Datenverkehrs

Da Unternehmensanwendungen zunehmend über die Cloud genutzt werden, müssen für eine gleichbleibend hohe Leistung dieser Anwendungen verschiedene Funktionen zur Datenverkehrsoptimierung sowohl für den internetgebundenen Datenverkehr als auch für den herkömmlichen Datenverkehr im privaten Netzwerk eingesetzt werden.

SD-WAN-Funktionen, die zur Bereitstellung einer optimalen Performance für SaaS-Anwendungen genutzt werden, sind unter anderem

- Identifizierung von First-Paket-Anwendungen
- Intelligente Pfadauswahlmechanismen
- Passive Leistungsüberwachung mittels Inline-Analyse des TCP-Datenverkehrs zu allen SaaS-Anwendungen, um den kurzfristigen Verlauf der Anwendungsleistung pro Pfad zu erfassen

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

- Aktive TCP- und HTTP-Tests für jede SaaS-Anwendung, um den kurzfristigen Verlauf der Anwendungsleistung pro Pfad zu erfassen
- Zur Auswahl des besten Pfads für jede SaaS-Anwendung werden aktive und passive Leistungskennzahlen verwendet
- Kombination des lokalen, direkten Ausgangs mit dem SaaS-Gateway-Ausgang

Zur Gewährleistung der QoE muss bekannt sein, wann ein bestimmter Pfad überlastet ist, und der Datenverkehr dann intelligent umgeleitet wird. Ein SD-WAN misst kontinuierlich SLA-Eigenschaften für alle Pfade, um den optimalen Pfad zu bestimmen, der die Anforderungen an die Anwendungsleistung erfüllt.

Die End-to-End-QoS des Netzwerks wird mit aktiven/passiven Sonden zwischen Zweigen/Knoten über unterschiedliche Zugangskreise, über diverse Transportwege und für jede spezifische Datenverkehrsklasse gemessen.

TECHNISCHES

Connectivity Fault Management/Y.1731 wird verwendet, um alle möglichen Pfade zu anderen in Ihrem Netzwerk bereitgestellten Zweigen zu überwachen. Jede Richtung jedes Pfades wird unabhängig überwacht. Über verschiedene Zugangsleitungen wird eine Datenbank mit SLA-Informationen (Latenz, Jitter, Paketverlust, Roundtrip-Verzögerung) zu anderen VPN-Standorten erstellt. SLA-Messungen erfolgen pro Weiterleitungsklasse. Two-Way Active Measurement Protocol (TWAMP) und ICMP-basierte Messungen erfassen SLA-Eigenschaften an Nicht-SD-WAN-Endpunkten, während die Antwortzeit für Saas-Anwendungen mit HTTP-basierten Messungen genauer erfasst wird.

TIPP

Eine ausgereifte SD-WAN-Lösung nutzt sowohl den aktiven Datenverkehr als auch synthetische Testpakete zur SLA-Bewertung für einen gegebenen Pfad.

SD-WAN-Maßnahmen zur Steuerung und SASE- Funktionen zur Sichergung des Datenverkehrs dienen zur Erhaltung der QoE. Die SD-WAN-Pfadauswahllogik muss unabhängig davon, wo sich der Nutzer befindet und welche Pfade für die Anwendung verfügbar sind, den optimalen Pfad bestimmen.

WAN-Optimierung

Zum Erreichen hoher Durchsatzraten für jede TCP-Anwendung sowie für den Datenverkehr, der über Verbindungen mit hoher Latenz läuft, wie zum Beispiel transkontinentale oder Satellitenverbindungen, ist eine WAN-Optimierung erforderlich.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Ein SD-WAN verwendet die folgenden WAN-Optimierungstechniken:

- **TCP-Optimierung:** TCP-Proxy-basierte Optimierungen helfen, auch unter schwierigen Netzwerkbedingungen einen hohen Durchsatz aufrechtzuerhalten, auch bei hoher Latenz und hohem Verlust.
- **Verbesserte Überlastungskontrolle, Verlusterkennung und -reparatur:** Hierzu gehören Mechanismen wie die BBR-basierte Überlastungskontrolle (Engpassbandbreite und Roundtrip-Zeit), Verlusterkennung nach kürzlich erfolgten Bestätigungen (RACK), TLP (Tail Loss Probing) und Rate Pacing.
- **Intelligentes Puffermanagement:** Hiermit wird verhindert, dass Datenübertragungen in BDP-Netzwerken (Bandwidth Delay Product) durch Puffer begrenzt werden.
- **Ermöglichung von Hochleistungsoptionen:** Dazu gehören selektives ACK (SACK), Fensterskalierung und Zeitstempeloptionen.
- **Deduplikation:** Bei dieser Methode handelt es sich um die Optimierung an zwei Knotenpunkten – einem nahe am Client und einem nahe am Server – bei der große Datenblöcke durch eine kürzere Signatur repräsentiert werden.
- **Kompression:** Zustandslose, verlustfreie Komprimierungsmethoden wie ZIP werden oft zur weiteren Komprimierung eines deduplizierten Datenstroms verwendet, wenn dieser über das Netzwerk gesendet wird, können aber auch für sich allein verwendet werden.
- **Caching:** Optimierung an einem Endpunkt für Anwendungen wie HTTP oder SMB (Server Message Block). Inhalte (Dateien) können auf dem Edge-Gerät zwischengespeichert werden, sodass nachfolgende Anfragen für dieselbe Datei lokal beantwortet werden und wiederholte WAN-Datenübertragungen vermieden werden.

Globale Verteilung

SASE bietet verteilte Points of Presence und ein Portfolio von Traffic-Peering-Beziehungen, die sich an den Anforderungen des Unternehmens an Zugriffslatenz und Datenresidenz ausrichten. Dies ist auch für die Endnutzer-QoE ausschlaggebend.

Das Internet wird als kurze Verbindung zu einem SASE-Cloud-Gateway genutzt, wo der Datenverkehr anhand von Richtlinien überprüft und mithilfe von Fast-Path-Routing und Peering-Arrangements für die beste Performance optimiert wird.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Mandantenfähigkeit und Segmentierung

Eine mandantenfähige Architektur trennt die Betriebsumgebung, Profile, Berechtigungen, Richtlinien und Abwicklung des Datenverkehrs jedes Mandanten vollständig von denen anderer Mandanten. Dadurch wird eine hohe Sicherheit für die Partition eines jeden Mandanten einer gemeinsam genutzten Ressource gewährleistet.

SD-WAN- und SASE-Lösungen sollten die native Segmentierung mit einer echten mandantenfähigen Implementierung unterstützen, die die Datenebene, die Kontrollebene, die Verwaltungsebene und die Analyse jedes Mandanten voneinander trennt. Jeder Mandant kann über mehrere virtuelle Routing- und Weiterleitungssysteme (VRF), virtuelle LANs (VLANs) und Serviceketten verfügen. Jedes Segment kann Folgendes aufweisen

- Eine einzigartige, das WAN umspannende Topologie
- Integrierte Netzwerksicherheit pro Segment
- Eine Reihe konfigurierter interner oder externer Dienste (wie Sicherheit und WAN-Optimierung) und Serviceketten
- Service-Profile
- Zugriffskontrolle auf Basis von Rollen und Verantwortlichkeiten

HINWEIS

Eine mandantenfähige Architektur muss unbedingt alle Umgebungen jedes Mandanten umfassen – die Verwaltungs-, Kontroll- und Datenebene. Es müssen separate, mandantenspezifische Overlay-Tunnel für den Datenverkehr – Verwaltung, Kontrolle und Daten – jedes Mandanten vorhanden sein.

Jede gemeinsam genutzte SASE- oder Cloud-Ressource erfordert die Unterstützung der Mandantenfähigkeit. Cloudnative SASE-Architekturen sind fast immer mandantenfähig, wobei mehrere Kunden die zugrunde liegende Datenebene gemeinsam nutzen.

5G-Architektur

Die enge Integration von SD-WAN, Sicherheit, Cloud und 5G resultiert in einer nahtloseren Bereitstellung. Das SD-WAN ist die Träger(Daten-)Ebene für die 5G/Edge-Cloud und ist die Methode, mit der 5G Network Slicing implementiert wird.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Die Edge-to-Edge-Integration von SD-WAN und Edge-Computing-Architektur beschleunigt 5G-Bereitstellungen und ermöglicht ein besseres Device-to-Cloud-Erlebnis. SASE entlastet Sicherheitsfunktionen für eine bessere Auslastung des 5G- Kernnetzwerks und senkt die Kosten durch die gemeinsame Nutzung der mobilen Infrastruktur mithilfe der Mandantenfähigkeit. SD-WAN ist ein Enabler für 5G Network Slicing, während SASE die Sicherheit für 5G DIA bietet. SASE und SD-WAN ermöglichen die einfache und skalierbare Bereitstellung Tausender 5G-Mobilfunkstandorte.

Weniger Komplexität

SD-WAN- und SASE-Lösungen werden zunehmend zur Konnektivitätslösung der Wahl für Unternehmen. Die Einfachheit von SASE beginnt mit einem einzigen cloudnativen System – cloudnative SD-WAN-Netzwerke sind speziell für cloudbasierte Anwendungen und Dienste konzipiert.

Cloudnative Systeme weisen eine plastische Architektur auf, die sich leicht in unterschiedliche Umgebungen einfügen und verschieben lässt. Die Architektur lässt sich bei Datenverkehrsschwankungen problemlos nach oben oder unten skalieren, sodass die Wahrscheinlichkeit von Unterbrechungen während der Spitzenzeiten für Nutzer deutlich geringer ist.

Die Flexibilität, Skalierbarkeit und Dynamik von SASE bewirken eine Entflechtung der mit dem Management von lokalen und hybriden Cloud-Komponenten verbundenen Komplexität. Die cloudnative SASE-Architektur sorgt für eine konsistente Durchsetzung von Richtlinien, um den IT-Aufwand zu reduzieren, und gewährleistet eine positive Nutzererfahrung, um die Akzeptanz zu erhöhen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- Fortentwicklung der Netzwerksicherheit
- Einbruchschutz
- Handhabung von Sicherheitsbedrohungen
- Implementierung von Cloud-Sicherheit
- Kontrolle des Nutzerzugriffs

Kapitel 4
Erweiterung der Sicherheit auf Client und Cloud

Der fixe Perimeter von Unternehmensnetzwerken wurde zunächst mit der zunehmenden Popularität von Cloud-Anwendungen und -Speicherangeboten aufgeweicht. löste sich dann fast vollständig auf, als Nutzer und Geräte in Filialen und WFA-Mitarbeiter (Work-from-Anywhere) über das Internet auf Unternehmensressourcen zugreifen konnten. Dieser Trend resultiert in individuellen „virtuellen Perimetern", die nur den Nutzer, das Gerät und die Anwendung umschließen und die Unterschiede zwischen dem Zugriff von innerhalb oder außerhalb des Unternehmensnetzwerks aufheben.

In dieser Umgebung muss die Sicherheit an die Identität und den Kontext des Nutzers, des Geräts, den Transport, den Zugriffstyp, die Ressource auf die zugegriffen wird und die für die Transaktion geltende Zugriffsrichtlinie gebunden und durchgesetzt werden.

Sicherheit muss flexibel, agil und dynamisch sein, um jeder Kombination von Nutzern und Ressourcen zu dienen. Zur Gewährleistung der QoE (Quality of Experience) müssen Sicherheitsdienste auch skalierbar und leistungsfähig sein; sie müssen die Transaktion zuverlässig sichern und die Nutzerproduktivität optimieren.

In diesem Kapitel erfahren Sie, wie sich Sicherheitsmethoden und -dienste entwickelt haben, um den strukturlosen, softwaredefinierten Internetperimeter eines modernen Unternehmens zu schützen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Die Entwicklung der Netzwerksicherheit

Der herkömmliche Sicherheitsansatz für Unternehmensnetzwerke trennte interne Ressourcen von der Außenwelt durch eine fixe, klar definierte Grenze. Perimeter-Firewalls schützten die interne Infrastruktur nach außen hin: Sie inspizierten und untersagten unerwünschten Datenverkehr und blockierten den Einblick und Zugang von außen.

Trends und Bedrohungen im Zuge der digitalen Transformation – wie zum Beispiel nicht verwaltete Nutzergeräte, IoT-Geräte (Internet of Things), Phishing, die Erweiterung des Perimeters in die Cloud durch Saas (Software-as-a-Service)/IaaS(Infrastructure-as-a-Service), DIA (Direct Internet Access), LTE-Transport (Long-Term Evolution) zu Hause und an Unternehmensstandorten sowie WFA-Mitarbeiter – haben den Perimeter zu einem virtuellen und dynamischen Element anstelle einer fest installierten Infrastruktur an bestimmten Standorten reduziert.

Das Konzept eines *softwaredefinierten Perimeters* (SDP) basiert auf der Idee der Defense Information Systems Agency (DISA), Verbindungen auf die absolut notwendigen zu beschränken, anstatt allem innerhalb des fixen Perimeters des Unternehmensnetzwerks zu vertrauen. Die SDP-Arbeitsgruppe der Cloud Security Alliance (CSA) machte SDP bekannt, um hochsichere, vertrauenswürdige End-to-End-Netzwerke für eine breite Unternehmensnutzung zu schaffen.

MERKE!

SDP arbeitet nach dem Zero-Trust-Modell und vertraut von Haus aus nichts, sondern erlaubt den Zugriff pro Sitzung auf Basis von Authentifizierung und Richtlinien. Es gibt kommerzielle, Open-Source-Implementierungen von SDP, wie sie von CSA veröffentlicht werden, zum Beispiel Googles BeyondCorp.

Software Defined Networking (SDN) hat alle Aspekte des Netzwerkbetriebs – einschließlich Perimeter und WAN (Wide Area Network) – in ein reines Software-Modell umgewandelt. Grundlegend für die SDN-Architektur sind die separaten, isolierten Kontroll- und Datenebenen. Diese Trennung ermöglicht sowohl die Kontrolle des SD-WAN (software-defined WAN) als auch der SDP-Kontrollebene in einem Netzwerk, was es Unternehmen wiederum ermöglicht, SD-WAN und SD-Sicherheit in derselben Softwarekontrollkomponente zu implementieren. Da es sich um reine Software handelt, ist die Bereitstellung auf Bare-Metal-Appliances (White-Box- oder Branded-Appliances) und virtuellen Maschinen oder VMs (in privaten oder öffentlichen Clouds) möglich. Alle Netzwerk- und Sicherheitsfunktionen sind tief in einen einzigen Software-Stack integriert, sodass der Betrieb am Netzwerk-Edge und in der Cloud sich einfach und flexibel gestaltet.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

TIPP

Zur Realisierung von SASE muss eine Lösung in der Lage sein, als Broker für verlässliche Client-to-Cloud-Sicherheit mit einer integrierten softwaredefinierten Architektur zu agieren. Abbildung 4-1 zeigt, wie Unternehmen erweiterte SD-WAN-Funktionen und Sicherheitsfunktionen für die Realisierung von SASE integrieren müssen.

Erweiterte SD-WAN-Funktionen				
ZTP	Anwendungs-ID	Testpakete, Inline-Messungen	FEC	Packet Striping
Dynamische IPSec-Overlays	Anwendungs-PBF	SD-WAN Fabric Traffic Management	Paket-Klonen	DIA-Verkehrsoptimierungen
NAT Traversal	Anwendungs-QoS	Anwendungs-TE, Anwendungs-SLA	Mandantenfähigkeit	Integrierte Sicherheit
Sicherheitsfunktionen (alle softwaredefiniert)				
NG-Firewall	DOS-Prävention	Geräteauthentifizierung	IPsec	Nutzer- und Gruppenauthentifizierung
CGNAT	HTTP/SSL-Proxy	DNS-Sicherheit	URL-Filterung	Web- und IP-Feeds
Malware-Sandboxing	IPS/IDS	Virenschutz	Dateifilterung	Transparenz und Analysen
CASB	ZTNA/SDP	UEBA	Geräteidentifikation	DLP

ABBILDUNG 4-1: SD-WAN und Sicherheitsfunktionen.

Erkennung und Verhinderung des Eindringens in Systeme

Es bieten sich mehrere Möglichkeiten an, Bedrohungen und Schwachstellen zu erkennen und zu verhindern. In den folgenden Abschnitten werden die gängigen auf dem Markt erhältlichen Lösungen beschrieben.

Next-Generation Firewalls

Firewalls der nächsten Generation (NGFWs) sind für heutige Netzwerke unerlässlich. Sie umfassen herkömmliche Stateful Inspection, bieten aber mit Deep Packet Inspection (DPI) für identitätsbasierte Transparenz und Kontrolle auf Anwendungsebene ein Plus an Funktionalität. NGFWs erfüllen weiter ihre wichtige Funktion bei der Netzwerksicherheit und entwickeln sich weiter, um auch erweiterte Anwendungsbereiche wie die öffentliche Cloud und die verteilte Edge-Sicherheit abzudecken.

Die neuesten NGFWs integrieren bisher autarke Funktionen, wie Intrusion- und Malware-Erkennung und -schutz.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IDPS (Intrusion Detection and Prevention System)

Ein *Intrusion Detection and Prevention System* (IDPS) ist eine eigenständige physische und/oder virtuelle Appliance, die den Netzwerkverkehr entweder vor Ort oder in virtualisierten/öffentlichen Cloud-Umgebungen überprüft. Sie vereint die Funktion zweier unterschiedlicher Systeme: eines Intrusion Detection Systems (IDS) und eines Intrusion Prevention Systems (IPS).

In der Regel setzt ein Unternehmen ein IDPS ein, um den Netzwerkverkehr zu prüfen, der die Sicherheitsvorrichtungen am Rande des Netzwerks wie Firewalls und sichere Web- und E-Mail-Gateways passiert hat. Viele Unternehmen verlassen sich zwar immer noch nur auf Detektion (IDS), viele andere setzen jedoch zusätzlich Appliances inline (IPS) ein, um erkannte Bedrohungen zu blockieren.

Aktuelle Bereitstellungsmodelle integrieren IPS-Funktionen in die NGFW, statt sie in separaten Einheiten zu implementieren. Ein IDPS ermöglicht die Erkennung anhand verschiedener Methoden – wie Signaturen, Protokollanomalien, diverse Analysemethoden, Verhaltensüberwachung und Heuristik, Sandboxing und Bedrohungsdaten (Threat Intelligence, TI) –, um unerwünschten und/oder bösartigen Datenverkehr aufzudecken und ihn zu melden oder verschiedene Maßnahmen zu ergreifen.

Alle oben genannten Methoden ergänzen die IDPS-Funktionen mit mehr Kontext, um den Zeitaufwand für die Verarbeitung von Warnmeldungen durch Analysten zu verringern und Fehlalarme zu reduzieren oder zu bestätigen.

Bei der Inline-Bereitstellung kann ein IDPS verschiedene Techniken zum Erkennen und Blockieren von Angriffen anwenden, die mit hoher Zuverlässigkeit erkannt werden.

Zwei wachsende Trends sind die Verwendung von Transport Layer Security (TLS) zur Verschlüsselung des Datenverkehrs und die Verwendung von HTTP für diverse Anwendungen. Zur Durchsetzung effektiver Sicherheitsrichtlinien und Verhinderung von Bedrohungen muss die TLS-Entschlüsselung in NGFW und IPS integriert werden.

Die Gesamtleistung der Lösung verbessert sich, wenn ein Paket nur einmal entpackt und analysiert wird und alle Sicherheitsfunktionen gleichzeitig auf den Paketinhalt angewandt werden.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

TIPP

Die beste Performance wird erzielt, wenn TLS-Entschlüsselung, IDS, IPS und Firewalls in einem einzigen Software-Stack kombiniert werden.

DNS-Sicherheit

Das Domain Name System (DNS) wurde in den 1980er Jahren zur Vereinfachung des Internets entwickelt, lange bevor jemand ernsthaft über bewährte Sicherheitsmethoden oder Security-by-Design-Ansätze nachdachte. Das DNS-Protokoll verfügt über keine integrierten Sicherheitsvorkehrungen, sodass Angreifer das DNS-System kompromittieren und Datenverkehr auf gefälschte oder betrügerische Websites umleiten können. Cache Poisoning und Man-in-the-middle sind zwei bekannte DNS-Angriffsarten, bei denen es das Ziel des Hackers ist, den Webverkehr umzuleiten, indem die Zuordnung von Domänennamen zu IP-Adressen (Internet Protocol) geändert wird.

MERKE!

Da er keine eigene implizite Sicherheit bietet, muss der DNS-Datenverkehr mit verschiedenen DNS-Sicherheitsmechanismen wie DNS-Security (DNSSEC), DNS-Proxy, DNS-Filterung und IPS/IDS gesichert werden.

DNSSEC ist eine Erweiterung von DNS, die eine Public-Key-Infrastruktur (PKI) nutzt, die DNS-Angriffe erschwert. DNSSEC verwendet eine standardisierte Methode für die Authentifizierung von DNS-Transaktionen, die eine Überprüfung des Absenders und der Integrität der Nachricht ermöglicht.

DNSSEC ist ein breiter gefasstes Konzept, das eine Vielzahl technischer Lösungen für die Handhabung von Sicherheitsgefährdungen und die Verhinderung von Angriffen auf DNS-Server und -Transaktionen umspannt. Zusätzlich zu DNSSEC können Sicherheitsfunktionen wie DNS-Proxy und DNS-Filterung verwendet werden, um DNS-Angriffe wie DNS-Hijacking, DNS-Snooping und DNS-Tunneling anzusprechen.

Der DNS-Proxy-Mechanismus erzwingt, dass DNS-Abfragen immer an den DNS-Server des Unternehmens oder einen vertrauenswürdigen DNS-Server weitergeleitet werden.

Die DNS-Filterung wertet den Zugriff auf nicht erlaubte und/oder schädliche Websites, Webseiten und IP-Adressen aus und blockiert diesen. DNS ordnet Domänennamen IP-Adressen zu, damit Computer Netzwerkressourcen finden können, und die DNS-Filterung ermöglicht einem Unternehmen, den Zugriff auf Internetressourcen innerhalb des Unternehmensnetzwerks zu kontrollieren. Mithilfe von Techniken wie Allow/Deny-Listen und Informationen zu Bedrohungen kann DNS-Filterung für Geräte innerhalb und außerhalb des Unternehmensnetzwerks

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

verwendet werden, um zu steuern, welche Host-Adressen mit DNS-Anforderungen aufgelöst werden können.

Verwaltung und Kontrolle von Sicherheitsbedrohungen

Alle herkömmlichen Sicherheitsmechanismen – Firewalls, IPS/IDS, Malware, Virenschutz, Mitarbeiterberechtigung, Nutzer- und Ressourcenauthentifizierung sowie URL-/Website-Filterung – werden jetzt dynamisch auf jede Transaktion im Netzwerk angewandt, egal ob vor Ort oder in der Cloud.

Unified Threat Management

Unified Threat Management (UTM) ist ein Rahmenbegriff für die umfassende Sicherung des Anwendungszugriffs mittels einer Reihe von Funktionen zum Schutz vor Bedrohungen, wie zum Beispiel NGFW, Data Loss Prevention (DLP), IPS, IDS, Malware-Erkennung, Virenschutz, Spamschutz, TLS-Entschlüsselung, IP-/URL-/DNS-Filterung, Dateifilterung, Remotezugriff für mobile Mitarbeiter (VPNs) und eine zentrale Verwaltungskonsole .

Malware-Schutz

Technologisch führende UTM-Malware-Erkennung überprüft den Datenverkehr beim Durchqueren des Sicherheitspunkts und extrahiert Dateien für die Malware-Analyse, wie in Abbildung 4-2 dargestellt. Die Malware-Erkennung zielt auf zwei Kategorien ab:

- **Inspektion von bekannter Malware:** Hier kommen Reputation (Dateifilterung) und Signaturen (Antivirus) zur Anwendung.
- **Erkennung von unbekannter Malware:** Dies erfordert ausgefeilte prädiktive Methoden wie algorithmische Analyse und Prognose (Scoring/Prognose auf Basis künstlicher Intelligenz (KI)) und Sandboxing mit Verhaltensanalyse, um festzustellen, ob Inhalte potenziell schädlich sind.

Obwohl einige Lösungen alles an die Sandbox senden, verwenden die meisten Triage-Methoden. Bei der Triage werden bekannt schlechte Dateien (Signaturstil) herausgefiltert und bekannt gute Dateien an den nächsten Schritt des Prozesses weitergeleitet. Damit wird die Anzahl der Dateien begrenzt, die eingehend geprüft werden müssen – die sogenannte „graue Liste“.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

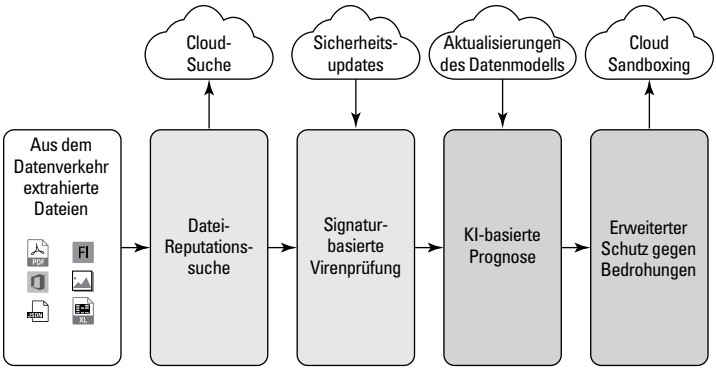


ABBILDUNG 4-2: Identifizierung bekannter und unbekannter Malware.

TECHNISCHES

Ein Malware-Schutzsystem (Malware Protection System, MPS) könnte bei der Triage darauf vertrauen, wo es physisch angeordnet ist. Wenn ein MPS zum Beispiel hinter einem sicheren Web-Gateway (SWG) angeordnet oder mit einem IPS integriert ist, das Malware-Scans durchführt, endet trivialere Malware nicht beim aufwändigeren MPS. Einige MPSs wenden ihre eigene Heuristik auf Inhalt und/oder Netzwerkverkehr an oder führen eine schnelle Emulation durch, bevor sie entscheiden, dass eine Datei ausführlicher überprüft werden muss.

Die meisten MPS-Lösungen nutzen Reputationslisten (Allow- und Deny-Listen) für die Eingrenzung von grauen Listen. MPSs errechnen im Verlauf der Triage typischerweise Risikobewertungen auf Grundlage verschiedener Merkmale und konfigurierbarer Richtlinieneinstellungen, um Dateien weiterzuleiten oder weiter zu prüfen.

Die Malware-Erkennung verwendet eine Kombination aus statischen und dynamischen Analysetechniken, um festzustellen, ob eine bestimmte Datei schädlich ist. Statische Analysetechniken umfassen Erkennungsmethoden wie File Reputation, Signatur-/regelbasierte Inspektion, Heuristik, Emulation, Maschinenlernen (ML) und KI.

Wenn die Erkennungsmethoden der statischen Analyse die Datei nicht eindeutig als harmlos oder schädlich identifizieren, analysiert das System die Datei dynamisch, indem es sie in einer Sandbox-Umgebung startet. Durch eine Kombination aus statischer und dynamischer Analyse können Systeme Schäden durch bekannte Malware und Zero-Day-Malware verhindern.

Dynamische sichere Web-Gateways

Ein sicheres Web-Gateway (SWG) schützt Unternehmen und Nutzer vor dem Zugriff und der Infektion durch böswilligen Webverkehr sowie

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

vor der Kontamination durch manipulierte Websites, die Malware oder Viren enthalten.

SWGs wurden in der Vergangenheit dazu verwendet, den Zugriff von Endnutzern in Unternehmen auf zeitverschwenderische oder sonstig inakzeptable Websites zu verhindern, haben sich aber seither weiterentwickelt. SWGs haben heute einen breiteren Sicherheitsfokus im Vergleich zu ihrer früheren, streng betrieblichen Rolle. Einige Funktionen, die häufig von einem heutigen SWG unterstützt werden, sind:

- URL-Filterung
- Malware-Schutz, bei dem das SWG den Datenverkehr aus dem Internet unter Verwendung bekannter Malware-Signaturen sowie bisher noch nicht angetroffener Verhaltensweisen der Malware überprüft
- IPS/IDS
- Anwendungsidentifizierungs- und -kontrollfunktionen
- Native oder integrierte DLP-Funktionen
- Zentrale Verwaltung und Protokollierung

Das SWG wertet die Anwendungsrichtlinie auf Basis des Nutzer-, Geräte- und Standortkontexts aus und gewährt nur dann Zugriff, wenn die Richtlinie die Anforderung auf Basis des Identitätskontexts zulässt. Wenn das System den Zugriff erlaubt, informiert das SWG den Client über das zu verwendende Gateway und das Gateway, das den Zugriff auf die Anwendung regelt, über den Nutzer-/Geräte-/Standortidentitätskontext.

Die Bereitstellungsarchitekturen für SWG sind unter anderem

- Explicit Mode Forward Proxy
- Inline-Modus
- Transparent-Modus
- DNS-basiert
- Cloudbasiert

TIPP

Cloudbasierte SWGs schützen Nutzer, wo immer sie sich befinden, unabhängig davon, ob sie derzeit in einem Unternehmensbüro arbeiten, unterwegs oder anderswo tätig sind.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

ZTNA und der neue Perimeter für Nutzer und Geräte

Eine *ZTNA-Lösung* (Zero Trust Network Access) umgibt eine oder auch mehrere Anwendungen mit einer identitäts- und kontextbasierten logischen Zugriffsgrenze.

MERKE!

ZTNA bietet kontrollierten identitäts- und kontextbezogenen Zugriff auf Ressourcen und reduziert so die Angriffsfläche.

Wenn ein Nutzer versucht, in einer Umgebung ohne Vertrauensstellung auf eine Anwendung zuzugreifen, erzwingt die Sicherheitssoftware die Authentifizierung und wertet die Zugriffsrichtlinie für die Anwendung basierend auf Nutzer, Gerät und Standort aus. Sie überprüft die Identität mithilfe eines unternehmensspezifischen Authentifizierungssystems wie Active Directory oder Single Sign-On (SSO) unter Verwendung der Security Assertion Markup Language (SAML). Abhängig vom Kontext und den Sicherheitsanforderungen kann sie zusätzlich zum unternehmensspezifischen Authentifizierungssystem auch eine Multifaktor-Authentifizierung (MFA) veranlassen.

Im Zuge der digitalen Transformation nutzen viele Unternehmen mehr Anwendungen, Dienste und Daten, die sich außerhalb ihrer traditionellen Grenzen befinden als innerhalb. Cloudbasierte ZTNA-Dienste setzen die Sicherheitskontrollen dort an, wo sich auch die Nutzer und Anwendungen befinden: in der Cloud.

Mit der Einführung eines Zero-Trust-Modells wird die gesamte Sicherheit auf Identität ausgerichtet: Nutzer, Anwendungen, Geräte, Dienste und Systeme. Durch die Normalisierung der Nutzererfahrung für den Anwendungszugriff eliminiert ZTNA die Unterscheidung zwischen dem Arbeiten innerhalb und außerhalb des Unternehmensnetzwerks.

MERKE!

Eine SASE-Lösung delegiert die Authentifizierung an die Infrastruktur und überwacht den Netzwerkverkehr direkt. Sie lässt sich in SSO und föderierte Dienste integrieren, um eine verbindliche, das gesamte Unternehmen umspannende Übersicht darüber bereitzustellen, „wer was verwendet“.

Eine breite Palette möglicher richtlinienbasierter Reaktionen richtet sich an der beobachteten Risikostufe aus, einschließlich Blockierung, MFA, Reduzierung von Nutzerberechtigungen, Erzwingen einer Passwortänderung, Erfordernis eines Autorisierungsprogramms oder Isolierung des Nutzers vom Internet. Alle Reaktionen können basierend auf Identität, Verhalten, Risikostufe und anderen Ereigniskontexten ausgelöst werden.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Sicherung der Cloud

Zusätzlich zu den herkömmlichen Sicherheitsdiensten wurden neue, auf die Cloud fokussierte Services eingerichtet, nachdem Unternehmen begannen, zur Cloud zu wechseln, zum Beispiel Cloud Access Security Broker (CASB), Remote Browser Isolation (RBI) und User and Entity Behavioral Analytics (UEBA). Diese Services sind für jede Transaktion von entscheidender Bedeutung – sie führen alte und neue Sicherheitsmechanismen zusammen.

TIPP

Nur durch die Kombination traditioneller Sicherheitsmechanismen mit neuen cloudnativen Sicherheitsansätzen können Unternehmen eine sichere Client-to-Cloud-Implementierung für ihre SASE-Implementierung erreichen.

Cloud Access Security Broker

CASB-Produkte und -Services, die vor Ort oder in der Cloud bereitgestellt werden, schließen Sicherheitslücken bei der Nutzung von Cloud-Diensten durch ein Unternehmen. Diese Technologie resultiert aus der Notwendigkeit, Cloud-Services zu sichern, ihnen sicheren Zugriff durch sowohl innerhalb als auch außerhalb des herkömmlichen Unternehmensperimeters befindliche Nutzer zu ermöglichen und einen sicheren Cloud-to-Cloud-Zugriff zu unterstützen.

Bei CASB-Produkten und Cloud-Services unterscheidet sich das Schutzziel von dem eines On-Premises-Sicherheitssystems. Die Daten gehören zwar noch immer dem Unternehmen, sie werden aber in Systemen verarbeitet und gespeichert, die jemand anderem gehören. CASB bietet eine Zentralstelle für Richtlinien und Governance, die gleichzeitig über mehrere Cloud-Services hinweg sowohl für Nutzer als auch Geräte angewandt werden und einen granularen Einblick in und Kontrolle über Nutzeraktivitäten und sensible Daten gewähren.

Einige Anbieter und Service-/Cloudprovider bieten cloudgehostete Sicherheit als Service als Teil ihres Portfolios sowohl in On-Premises- als auch in providerbasierten Modellen an. Diese Produkte und Services bieten einen globalen Überblick der Standorte, an denen die CASB-Softwareknoten bereitgestellt werden (siehe Abbildung 4-3). Unternehmen nutzen den nächstgelegenen oder praktischsten Point of Presence für den schnellen und sicheren Netzwerk- und Anwendungszugriff auf die Cloud-Infrastruktur.

MERKE!

CASB bietet fünf wichtige Sicherheitsfunktionen: Erkennung von Cloud-Anwendungen, Datensicherheit, adaptive Zugriffskontrolle, Malware-Erkennung und Analyse des Nutzer- und Entitätsverhaltens.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

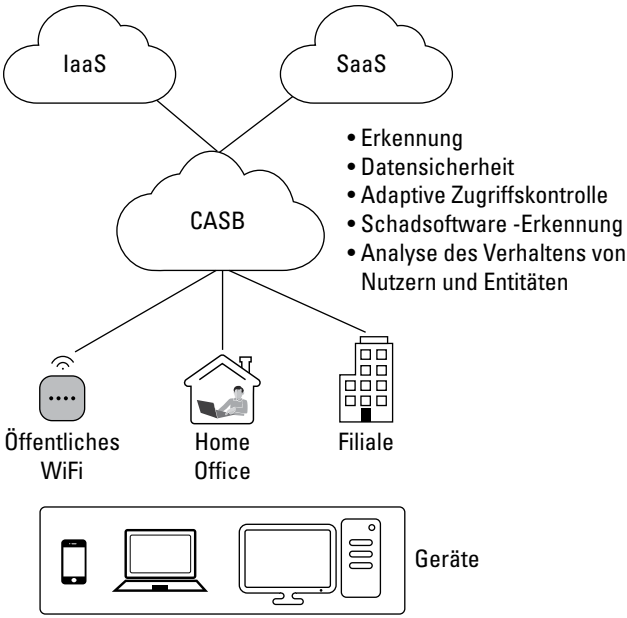


ABBILDUNG 4-3: CASB-Architektur.

CASB hilft Unternehmen in folgender Hinsicht:

- Identifizieren und Bewerten aller verwendeten Cloud-Anwendungen (sanktionierte Anwendungen sowie auch im Schatten arbeitende und bösartige IT)
- Durchsetzung von Richtlinien für das Management von Cloud-Anwendungen
- Erstellen und Durchsetzen granularer Richtlinien zur Regelung der Handhabung von sensiblen Daten, einschließlich compliance-bezogener Inhalte
- Verschlüsselung oder Tokenisierung sensibler Inhalte zur Gewährleistung des Datenschutzes
- Erkennen und Blockieren von ungewöhnlichem Verhalten, das auf böswillige Aktivitäten hinweist
- Integration von Cloud-Transparenz und Kontrollen mit bereits vorhandenen Sicherheitslösungen

DLP in der Cloud

Die Data Loss Prevention-Technologie zur Verhinderung von Datenverlusten (auch als Technologie zur *Verhinderung von Datenlecks* bezeichnet)

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

wurde entwickelt, um zu verhindern, dass Daten dort verwendet werden oder sich dort befinden, wo sie nicht sein sollten. Die Technologie ist seit langem verfügbar und wird mit unterschiedlichem Erfolg eingesetzt. DLP-Anbieter nutzen die Konzepte „Daten im Ruhezustand", „Daten in Bewegung" und „Daten in Gebrauch" für die Strukturierung von DLP-Architekturen.

TECHNISCHES

DLP folgt dem Ansatz „Inhalt + Kontext" für die Datenverwaltung. DLP-Systeme analysieren die Daten innerhalb eines Dokuments (DLP arbeitet fast ausschließlich mit unstrukturierten Daten), um deren Inhalt zu ermitteln, den Kontext zu analysieren (unter anderem Standort, Nutzer, System und Prozess) und wendet dann Kontrollen an, die durch die vom Sicherheitsteam implementierten Richtlinien bestimmt werden.

TIPP

DLP ist in einer Vielzahl von Produkten zu finden, weshalb es hilfreich sein könnte, DLP als Funktion und nicht als Markt zu betrachten. Zunehmend kompetente DLP-Funktionen finden sich nicht nur in DLP-Unternehmenssuiten, sondern kommen auch in SaaS- und IaaS-Umgebungen als native Kontrollen sowie in sicheren Web- und E-Mail-Gateways, CASBs und Firewalls zum Einsatz.

Da Unternehmen zunehmend verteilte, verwaltete Cloud-Anwendungen einsetzen, wird es immer schwieriger, Transparenz und Kontrolle über Daten in der Cloud zu erlangen, sei es im Ruhezustand (gespeicherte Daten), in Verwendung (Daten, die von einem Nutzer geöffnet wurden) oder in Bewegung (Daten, die zwischen Standorten verschoben werden). Die Fähigkeit, alle drei Datenzustände zu schützen, ist unerlässlich, um Datenschutzverstöße zu verhindern – insbesondere, wenn sich Daten durch die Clouds von Drittanbietern bewegen.

In der modernen Umgebung muss DLP nun zusätzlich zu On-Premises auch zu einer Cloud-Funktion werden, um Transparenz und Schutz für sensible Daten in SaaS/IaaS-Anwendungen zu bieten. Dies ist auch notwendig, um die sensiblen und kritischen Informationen eines Unternehmens vor Cyberangriffen, Insider-Bedrohungen und einer absichtlichen oder versehentlichen Exponierung zu schützen.

MERKE!

Cloudnatives DLP kann sehr effektiv sein, da die Cloud Service Provider (CSPs) selbst den besten Zugriff auf die von ihnen gespeicherten Daten und die Möglichkeit haben, Operationen an diesen durchzuführen. Drittparteien sind auf die vom CSP bereitgestellten APIs (Application Programming Interfaces) begrenzt, die einige erst gar nicht anbieten.

Cloudnatives DLP stellt CASB-Lösungen einen Teil der Funktionen zur Verfügung, die zum Schutz von Daten in der Cloud zusammenarbeiten können. Jede Cloud-Nutzung muss durch eine Kombination der CASB inhärenten Funktionalität und der Unterstützung von APIs für multicloudnative DLPs geschützt werden.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

TIPP

Cloudbasiertes DLP ist eine primäre CASB-Funktion. Geschäftsregeln klassifizieren und schützen vertrauliche und kritische Informationen und stellen die erforderlichen Sicherheitskontrollen bereit, damit Nutzer Daten nicht versehentlich oder böswillig teilen können.

Remote-Browser-Isolierung

RBI verlagert die Ausführung der Browseraktivität eines Nutzers vom Client-Gerät auf einen Remote-Server – mit On-Premises- oder Cloud-Hosting. Dies bietet Schutz vor browserbasierten Sicherheitslücken und ermöglicht anonymes Surfen und einen risikofreien offenen Internetzugang.

Während der Nutzer im öffentlichen Internet surft, ist der Remote-Browser vom physischen Endpunkt und dem Unternehmensnetzwerk des Nutzers isoliert. Angriffe auf die Remote-Browser-Sitzung bleiben so auf die virtuelle Umgebung beschränkt. Jede Browser-Sitzung wird in einer isolierten Umgebung ausgeführt, die jegliche Infektion der Arbeitsumgebung des Nutzers verhindert. Angriffe auf Browser-Ebene werden zwar erwartet, aber bei der Verwendung eines Remote-Browsers können sie keine anderen Systeme erreichen und sich dort einnisten. Die Bedrohung wird somit beseitigt, da Sitzungen nach jeder Verwendung zurückgesetzt werden.

RBI hilft auch bei DLP, insbesondere wenn nicht verwaltete/nicht vertrauenswürdige Geräte für den Zugriff auf vertrauliche oder sensible Informationen verwendet werden. Anstatt den nicht verwalteten Geräten das Herunterladen der Informationen/Dateien zu ermöglichen, lädt das System die vertraulichen Informationen in die isolierte Remote-Browserinstanz herunter. Die nicht verwalteten/nicht vertrauenswürdigen Geräte sehen nur eine visuelle Darstellung der Daten.

RBI kann in zwei Varianten implementiert werden. Eine dient als primärer Schutzschild, wobei alle Standorte mittels RBI präsentiert und andere Filter (hauptsächlich Standortkategorisierung) nach Bedarf angewendet werden. Die andere erfüllt die Funktion eines herkömmlichen Web-Proxy, die Sites selektiv mithilfe von RBI auf Basis der Website-Reputation präsentiert. Das funktioniert folgendermaßen:

- Nutzersitzungen werden anhand der URL-Filterung und -Kategorisierung auf Risiken überprüft.
- Risikobehaftete Websites werden über einen Remote-Browser präsentiert.
- Bereinigte Seiten (vorwiegend Bilddateien) werden im Browser des Nutzers präsentiert.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Wie in Abbildung 4-4 dargestellt, folgt RBI einem selektiven CDR-Ansatz (Content Disarm and Reconstruction) für Webbrowser-Sitzungen. Eine RBI-Funktion arbeitet in der Regel auf eine von zwei Arten:

- Durch Rendern eines Bildes einer Webseite im Browser des Nutzers mittels eines Plug-ins oder HTML5-Rendering
- Durch Extrahieren lesbarer Informationen aus der HTML einer Webseite und Rekonstruktion im Browser des Nutzers

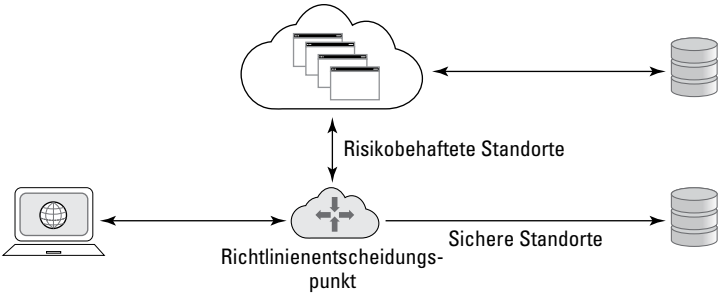


ABBILDUNG 4-4: RBI in Aktion.

Analyse des Verhaltens von Nutzern und Entitäten

UEBA (User and Entity Behavior Analytics) verwendet sogenannte Packaged Analytics für die Bewertung der Aktivität von Nutzern und anderen Entitäten (wie Hosts, Anwendungen, Netzwerkverkehr und Datenspeicher). UEBA entdeckt Bedrohungen und potenzielle Vorfälle, die in der Regel als Aktivitäten aufgezeigt werden, die, Zeit- und Peer-Groups übergreifend, in den Standardprofilen und -verhaltensweisen von Nutzern und Entitäten anomal sind.

MERKE!

Die am häufigsten von Unternehmen angestrebten Anwendungsfälle sind die Erkennung von/Reaktion auf Bedrohungen und die Erkennung von/Reaktion auf Insider-Bedrohungen (hauptsächlich kompromittierte Insider, manchmal aber auch böswillige Insider). Weitere Anwendungsfälle wären zum Beispiel die Überwachung auf unbefugten Datenzugriff und nicht autorisierte Datenbewegungen, verdächtige Aktivitäten privilegierter Nutzer sowie böswillige oder nicht autorisierte Aktivitäten von Mitarbeitern. UEBA überwacht auch den ungewöhnlichen Zugriff auf und die Nutzung von Cloud-Ressourcen und unterstützt eine verbesserte Erkennung aus bestehenden sicherheitstechnischen Investitionen, zum Beispiel CASB und Identity and Access Management (IAM).

UEBA-Lösungen werden gelegentlich auch für nicht-cybersecurity-zentrierte Anwendungsfälle wie Betrug oder Mitarbeiterüberwachung eingesetzt. Diese erfordern jedoch häufig Nicht-IT- und nicht

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

sicherheitsrelevante Datenquellen oder spezifische Analysemodelle, die von fundierten Fachkenntnissen in den jeweiligen Domänen abgeleitet werden.

Wo SWG-Systeme Identität zur Anwendung von punktspezifischen Richtlinien nutzen, erweitert ein UEBA-System den Richtlinienumfang auf die Anwendung kontextbasierter Richtlinien (siehe Abbildung 4-5). Ob ein Nutzer rechtmäßig auf Daten zugreifen darf, wird nicht nur abhängig von seinen Zugriffsberechtigungen bestimmt, sondern auch auf Grundlage seines bisherigen Verhaltens.

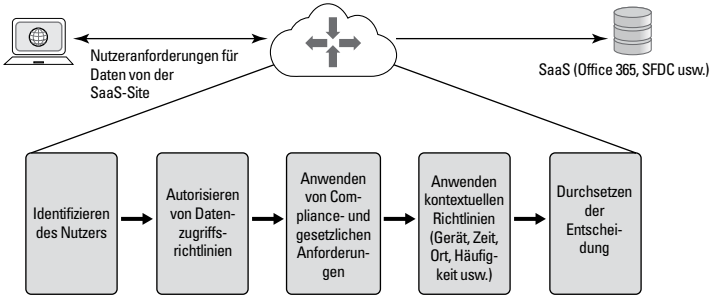


ABBILDUNG 4-5: UEBA ermöglicht kontextbasierte Richtlinien.

UEBA-Systeme erkennen anomales Verhalten anhand historischer Aufzeichnungen und diese Erkennungsmethode ermöglicht intelligente Zugriffsentscheidungen. Wenn ein Nutzer beispielsweise häufig versucht, auf Dateien mit vertraulichen Informationen zuzugreifen, kann das System den Nutzer blockieren und Administratoren benachrichtigen, während es einem Nutzer den einmaligen Zugriff auf eine einzelne Datei gestatten kann.

Feinabstimmung der Zugriffsverwaltung

Wenn ein Nutzer für den Anwendungszugriff auf ein SASE-Gateway umgeleitet wird, führt das SDP-Gateway erneut die Geräte- und Nutzerauthentifizierung durch und überprüft den Ursprungsort der Anforderung.

TECHNISCHES

Im Anschluss an die Authentifizierung erhält das SASE-Gateway stellvertretend für die Anwendung Authentifizierungstokens für den Nutzer. Beispiele für Tokens sind SAML-Assertions, NTLM-Token (NT LAN Manager), Kerberos-Token und die grundlegenden Nutzername- und Passwortfelder der Anwendungsanforderung. Das SASE-Gateway kann eine SSO-Nutzererfahrung für jede Anwendung bereitstellen und als Identitätsbroker für den Nutzer fungieren.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Schutz sensibler Daten

Eine SASE-Lösung sollte den Kontext der Daten/Anwendungen verstehen, auf die zugegriffen wird, und in der Lage sein, adaptive Maßnahmen zu ergreifen, zum Beispiel das Hochladen/Herunterladen sensibler Daten zu blockieren, wenn ein zu hohes Risiko erkannt wird.

TIPP

Ein entscheidendes Bewertungskriterium ist Vielfältigkeit bei der Definition von Richtlinien für sensible Daten. Daten müssen mithilfe von APIs überprüft werden, um ein Verständnis des Datenkontexts zu erlangen und nützliche Richtlinien (wie Verschlüsselung oder Wasserzeichen) anzuwenden, wenn die Daten die Cloud verlassen.

SASE ermöglicht Sicherheitsteams die Bereitstellung eines reichhaltigen Satzes von Netzwerksicherheitsdiensten auf konsistente und integrierte Weise, um die digitale Transformation und die Mobilität der Mitarbeiter zu unterstützen.

Entschärfung von Malware

Die Einführung von SASE verbessert die Soft-Perimeter-Sicherheit von Nutzern, Geräten und Anwendungen unabhängig vom Standort. In SASE-Lösungen, die die Überprüfung von Inhalten (Identifizierung sensibler Daten und Malware) unterstützen, ist die Überprüfung jeder Zugriffssitzung und die Anwendung desselben Satzes von Richtlinien möglich. Ein SASE-System könnte beispielsweise in Salesforce, Facebook und cloudgehosteten Anwendungen nach vertraulichen Daten suchen und dabei eine einzige Richtlinie verwenden, die unabhängig vom Standort des Nutzers/Geräts konsistent angewendet wird. Idealerweise sollte das SASE-System in der Lage sein, Inhalte in einem einzigen Durchgang sowohl auf vertrauliche Daten als auch auf Malware zu überprüfen.

Darüber hinaus sind die angewandten Überprüfungsfunktionen konsistent, sofern die Anwendung per Richtlinie erfolgt, und zwar unabhängig davon, worauf die Entität zugreift. Das SASE-System kann zum Beispiel Inhalte über alle Verbindungen hinweg auf vertrauliche Daten und Malware überprüfen.

MERKE!

SASE-Lösungen sollten den Kontext der Daten verstehen – ob der Inhalt sensibel oder schädlich ist. Der Datenkontext ist entscheidend für die Festlegung von Zugriffsrichtlinien, das Verständnis und die Priorisierung von Risiken sowie die entsprechende Anpassung von Zugriffsrichtlinien. Lösungen, denen dieser Kontext fehlt, sind in ihrer Fähigkeit eingeschränkt, umfassende kontextbezogene, adaptive SASE-Entscheidungen zu treffen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- Ermöglichung der digitalen Transformation
- Zentralisierung von Verwaltung und Kontrolle
- Umsetzung konsistenter Unternehmensrichtlinien
- Zeit und Geld sparen
- Bewertung eines realen SASE-Unternehmens

Kapitel 5
Nutzung von SASE

Chief Information Officers (CIOs) moderner Unternehmen brauchen exemplarische Client-to-Cloud-Erfahrungen, die sicher, zuverlässig, skalierbar und unkompliziert sind. SASE bietet genau das.

In diesem Kapitel erfahren Sie, wie Sie den größten Nutzen aus Ihrer SASE-Lösung (Secure Access Service Edge) schöpfen, wie SASE Sie bei der digitalen Transformation Ihres Unternehmens unterstützt, wie Sie sie handhaben, wie Sie Ihre Vermögenswerte schützen und wie Sie Kosten senken können.

Verstehen, wie SASE die digitale Transformation ermöglicht

SASE ermöglicht eine unternehmensweite digitale Transformation mit Client-to-Cloud-Sicherheit, einem cloudnativen Ansatz und horizontaler Elastizität, wie in Abbildung 5-1 dargestellt.

Die Zeit ist vorbei, in der alle Mitarbeiter in einem physischen Gebäude arbeiteten und alle Ihre Unternehmensressourcen in einem privaten Rechenzentrum untergebracht und sowohl physisch als auch digital gesichert waren. Die herkömmliche IT-Infrastruktur ist ungeeignet für die Unterstützung und Sicherung von cloudgehosteten Anwendungen, Direct Internet Access (DIA), nicht IT-verwalteten Nutzergeräten, überall arbeitenden WFA-/mobilen Nutzern, bandbreitenintensiven und

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

verzögerungsempfindlichen Sprach- und Videoanwendungen sowie ungesicherten IoT-Geräten (Internet of Things). Unternehmen, die diese Technologien und Architekturen einsetzen möchten, müssen den Sprung in die digitale Transformation wagen.

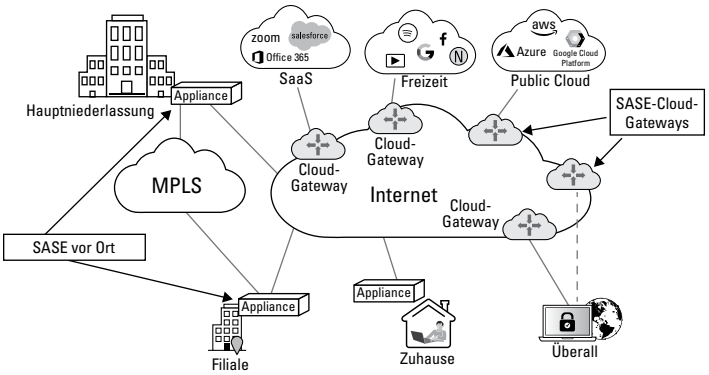


ABBILDUNG 5-1: Ein integriertes SASE-Unternehmen.

Die Transformation von Netzwerken und der Geschäftsumgebung erfordert moderne Funktionen wie Multicloud-Bereitschaft, umfassende integrierte Sicherheit, skalierbares erweitertes Routing, Optimierung und Verbesserung der Verkehrssteuerung sowie ein hohes Maß an Transparenz und leistungsstarken Analysen.

MERKE!

Software-defined Wide Area Network (SD-WAN)/SASE-Architekturen, die all diese Funktionen integrieren, sind der einzige praktikable Ansatz für die Unterstützung der Trends und Technologien, die der modernen Ära der digitalen Transformation eigen sind.

Multicloud-Implementierung

Multicloud-Umgebungen umfassen mehrere SaaS- (Software as a Service), IaaS- (Infrastructure as a Service), öffentliche und On-Premises-Clouds und finden deshalb eine immer breitere Verwendung. Dieses Netzwerkmodell bietet Vorteile wie die Vermeidung einer Herstellerbindung, die Minimierung von Kosten und die Verbesserung von Disaster-Recovery-Optionen. Es bringt aber auch Herausforderungen in Bezug auf Sicherheit und Datenschutz mit sich.

Eine SASE-Infrastruktur eliminiert die mit der Interkonnektivität von Multicloud-Architekturen verbundenen Problemstellungen, indem sie automatisch dynamische, übergeordnete Konnektivität sowohl für die Daten- als auch die Kontrollebene jeder Cloud erkennt – und nahtlos realisiert. Die Konnektivitätstopologie ist automatisiert und in wenigen Minuten einsatzbereit – vollständig durch Verschlüsselung

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

gesichert – und die Kontrollebene über die verschiedenen Clouds hinweg wird durch das Tunnelgeflecht normalisiert, um die vollständige globale Transparenz des Netzwerks zu gewährleisten.

Cloudnativ und flexibel

Eine SASE-Lösung ist cloudnativ und baut für Flexibilität und Automatisierung auf Cloud-Prinzipien auf. Die Elastizität der Cloud ermöglicht Nutzern eine hoch konsistente, vorhersehbare Quality of Experience (QoE) ohne das Risiko der Verlangsamung, des Ausfalls oder der Nichtverfügbarkeit von Services.

Ressourcen werden automatisch bereitgestellt – ohne dass der Endnutzer etwas von dem Prozess mitbekommt. IT-Aufgaben werden damit erheblich vereinfacht, sodass das Personal mehr Zeit hat, sich auf sein Kerngeschäft zu konzentrieren.

Zuverlässiges Management

SASE arbeitet aus der Cloud, um alle Netzwerk- und Sicherheitsfunktionen unter einem einheitlichen Rahmenkonzept bereitzustellen.

Ein SD-WAN mit SASE eliminiert den administrativen Aufwand für die Beschaffung, Installation, Konfiguration und Verwaltung einzelner Ausrüstungselemente und ermöglicht Sicherheitsteams die Optimierung der Verwaltung aller Netzwerk- und Sicherheitsaktivitäten anhand einer einzigen Lösung und einer einheitlichen Richtlinie. In den folgenden Abschnitten umreißen wir einige der von SASE gebotenen Managementvorteile.

Schnellere Administration und Bereitstellung

Mit der richtigen SD-WAN-mit-SASE-Architektur sind Bereitstellung und Überwachung weitgehend automatisiert. Nachdem umfassende Richtlinien festgelegt sind, erfolgen die Konfigurations- und Bereitstellungsaktivitäten des Netzwerks automatisch.

Eine echte SASE-Lösung verbessert zudem die Netzwerkzuverlässigkeit und -leistung in Verbindung mit SD-WAN-Funktionen. Sie erreicht dies, weil sie anwendungsbewusst ist, Verkehrsmuster überwacht, den Datenverkehr dynamisch steuert und die Auswahl des Transportweges optimiert. Diese Funktionen stellen sicher, dass alle Anwendungen – insbesondere Sprach- und Videoanwendungen – nahtlos und zuverlässig ausgeführt werden, um einen unterbrechungsfreien Service bereitzustellen und die QoE zu maximieren.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Das global verteilte System mit SASE-fähigen Cloud-Gateways erweitert die Bereitstellung im Unternehmen auf den nahtlosen Cloud-Zugriff, unabhängig davon, ob die Bereitstellung durch Unternehmen, Serviceprovider oder Anbieter erfolgt. Cloud-Gateways sind an vielen globalen Standorten in direkter Nähe fast aller Cloud-Services verfügbar. Führende Cloud-Gateways sind untereinander über Traffic-Engineered Middle Mile-Technologien oder Public Cloud Backbones wie Azure oder Amazon Web Services (AWS) verbunden.

Vereinfachter Überblick

Die sichere Verwaltung Ihres Netzwerks erfordert eine vollständige Betriebstransparenz. Eine SASE-Architektur bietet Nutzer-, Anwendungs- und Geräteansichten im gesamten Unternehmen: On-Premises, in privaten und öffentlichen Clouds oder mit dem Internet verbunden, wie in Abbildung 5-2 dargestellt.

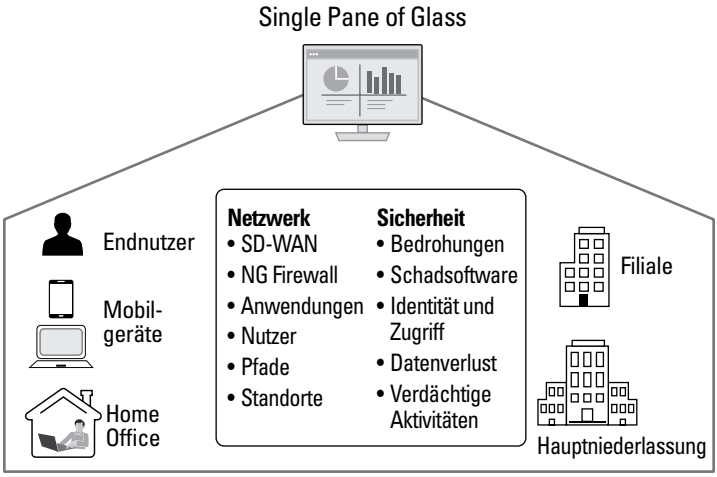


ABBILDUNG 5-2: Eine Konsole für Transparenz und Kontrolle.

MERKE!

Ältere Netzwerkbetrachtungen konzentrierten sich auf IT-verwaltete Geräte, Rechenzentren und Zweigstellen, während digital transformierte SASE Architekturen sich auf Geräte, Benutzer und Anwendungen konzentrieren.

Vollständige Kontrolle über Nutzer, Anwendungen und Geräte

Eine SD-WAN/SASE-Architektur bietet Einblick in die Anwendungsleistung, Probleme mit der Anwendungskonnektivität, Probleme auf

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

der Kontrollebene wie Denial-of-Service(DOS-)Angriffe oder Protokollstürme, unautorisierte Datenströme sowie Underlay- oder Overlay-Probleme.

Das System klassifiziert den Anwendungsverkehr automatisch im Hinblick auf die QoE und filtert nicht sanktionierte Anwendungen heraus. Diese jederzeit verfügbaren Informationen zur Anwendungssicherheit helfen dem IT-Personal, geeignete Richtlinienänderungen vorzunehmen, Sicherheitsrisiken zu minimieren, wichtige Einblicke zu gewinnen, Fehler schneller zu beheben und besser informierte Entscheidungen zu treffen, wie in Abbildung 5-3 dargestellt.

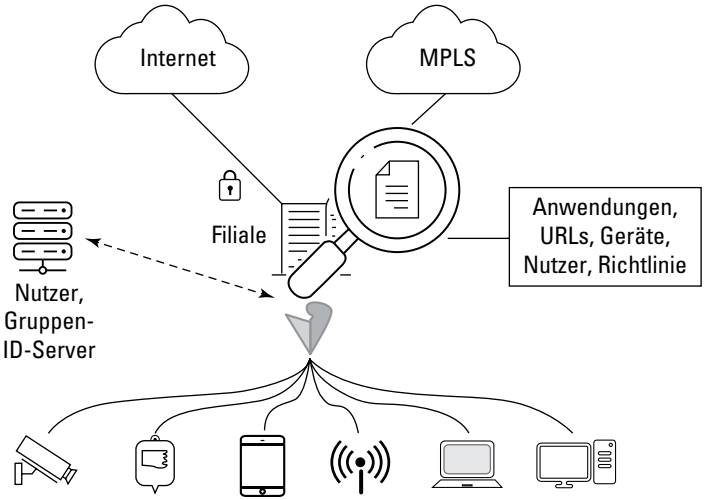


ABBILDUNG 5-3: Verwaltung von Nutzern und Geräten.

Schutz Ihrer Vermögenswerte

Mit SASE können Sicherheitsteams Cloud-Plattformen, Rechenzentren, Zweigstellen und WFA-/mobile Nutzer unter einem Schirm mit einer kohärenten Sicherheitsrichtlinie schützen, die jedem Nutzer auf jedem Gerät und überall zur Verfügung gestellt wird. Die SASE-Sicherheitsrichtlinie ist auf den dynamischen Identitäts- und Zugriffskontext fokussiert, statt auf alte fixe, vertrauenswürdige/nicht vertrauenswürdige Netzwerkgrenzen.

TIPP

Die zentrale Kontrolle von Sicherheitsrichtlinien trägt zur Eliminierung von Fragmentierung, Schwachstellen und falsch konfigurierten Richtlinien bei.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Im Folgenden stellen wir einige Möglichkeiten vor, wie SASE zum Schutz Ihrer Vermögenswerte beitragen kann.

Bessere Datensicherheit und Compliance

Für viele Unternehmen beginnt die Pflege der Sicherheitshygiene und die Befolgung von Datenschutz- und Sicherheitsstandards damit, zu verfolgen, welche vertraulichen Informationen über Kunden gespeichert werden, und dann Regeln zu entwickeln, um den Zugriff auf diese Informationen zu schützen.

SASE setzt Compliance durch, indem sichergestellt wird, dass nur Personen mit den richtigen Anmeldeinformationen auf sichere Systeme und Datenbanken mit sensiblen Kundendaten zugreifen können. RBAC-Richtlinien (Role-Based Access Control) werden konsistent angewendet und UEBA-Systeme (User and Entity Behavior Analytics) verfolgen den Zugriff und die Vorgänge innerhalb des Systems mit Protokollen und Audit-Trails.

Die Transparenz und Kontrolle eines SASE-Frameworks senken die Wahrscheinlichkeit einer Datenschutzverletzung, indem die Angriffsfläche verkleinert und laterale Bewegungen begrenzt werden. Datenschutzverletzungen schaden dem Ruf eines Unternehmens, untergraben das Vertrauen seiner Kunden und implizieren eine wahrgenommene Fahrlässigkeit beim Schutz der Privatsphäre und der Sicherheit der Kunden.

MERKE!

Eine SASE-Lösung bietet eine einfache Möglichkeit, Daten zu schützen und Compliance-Anforderungen durch identitätsgesteuerten Zugriff zu erfüllen.

Inline-Verschlüsselung

Verschlüsselung ist in modernen Netzwerken unerlässlich, um Daten während der Übertragung zu schützen. Zu diesem Zweck werden schon lange virtuelle private Netzwerke (VPNs) verwendet, aber die Ver- und Entschlüsselung ist rechenintensiv und kann die Anwendungsleistung beeinträchtigen. Statisch definierte VPN-Tunnel in Legacy-Netzwerken können zu schlechten Entscheidungen bei der Steuerung des Datenverkehrs führen.

Führende SASE-Lösungen umfassen Optionen für software- und hardwarebeschleunigte Verschlüsselung, die eine schnellere Verarbeitung und manipulationssichere Schlüsselspeicherung ermöglichen.

MERKE!

In einer dynamischen Softwareverschlüsselungsarchitektur muss das System die Schlüssel schützen, indem es sie sie niemals über den Datenverkehrspfad sendet.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Um sowohl Sicherheit als auch eine gute QoE zu gewährleisten, müssen verschlüsselte Tunnel im SD-WAN-Overlay-Netzwerk automatisiert, dynamisch und flexibel eingerichtet und aufgelöst werden.

Isolierung und Segmentierung

Eine SASE-Lösung bietet Sicherheit durch Netzwerkisolierung, Segmentierung und Mandantenfähigkeit. Die Segmentierung verlangsamt eine Datenschutzverletzung, da der Angreifer aus einem Netzwerksegment ausbrechen muss, um auf Ressourcen in anderen Segmenten zugreifen zu können. Eine Trennschicht zwischen verschiedenen Servern mit sensiblen Daten reduziert das Risiko von Datenverlust/Diebstahl und das Ausmaß von Schäden am Unternehmen.

Kostensenkung

Die Installation heterogener, proprietärer Einzelprodukte in Zweigstellen ist kostspielig, führt zu einer unkontrollierten Ausbreitung, ist komplex in der Verwaltung und ermöglicht weder WFA noch optimiert sie den Cloud-Zugriff. Eine SASE-Architektur, in der alle Netzwerk- und Sicherheitsfunktionen in einem einzigen Software-Stack integriert sind, reduziert die Kapitalinvestitionen, erlaubt IT-Mitarbeitern die Konzentration auf strategische Aufgaben und ermöglicht eine kohärente Implementierung von Sicherheitsrichtlinien.

Zu den Kosteneinsparungen, die mit einer SASE-Architektur erzielt werden, gehören

- **Kosteneinsparungen bei der Bandbreite:** DIA bewirkt zusammen mit SASE-fähigen Cloud-Gateways eine deutliche Reduzierung des Datenverkehrs über Hubs, Rechenzentren und VPN-Aggregatoren in Legacy-Netzwerken. SASE beseitigt zentrale Sicherheitsinspektionen und verteilt die Durchsetzung von Richtlinien über das globale Netzwerk.
- **Kosteneinsparungen bei Netzwerkverwaltung und IT-Personal:** Ein veralteter Netzwerk-Service verkettet mehrere Sicherheits- und Routing-Appliances an jedem Standort. SASE konsolidiert alle Netzwerk- und Sicherheitsdaten in einem automatisierten, mandantenfähigen, cloudnativen Software-Stack mit einer einzigen, zentralen Orchestrierung, wodurch Kosten, Komplexität und die Koordination von Konfigurationen unterschiedlicher Anbieter eliminiert werden.
- **Kosteneinsparungen bei der Sicherheit:** Multicloud-Umgebungen und WFA-Personal, das DIA nutzt, haben die Angriffsfläche des Unternehmens vergrößert. Verstöße sind schädlich und teuer. SASE

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

verwendet einen Zero-Trust-Ansatz für den Netzwerkzugriff (ZTNA) für Clouds, DIA, nicht verwaltete Client-Geräte, IoT, Rechenzentren, Zweigstellen und WFA-Nutzer und schützt all dies mit einer dynamischen, einheitlichen Sicherheitsrichtlinie für jede Kommunikationssitzung. ZTNA bietet adaptiven, identitätsbewussten und präzisen Zugriff. ZTNA verbessert die Flexibilität, Agilität und Skalierbarkeit des Anwendungszugriffs, sodass Unternehmen wachsen können, ohne interne Anwendungen direkt mit dem Internet zu verbinden, wodurch das Risiko von Angriffen reduziert wird.

- **Kosteneinsparungen bei der Skalierbarkeit:** Die Erweiterung von Netzwerk und Sicherheit auf neue Standorte in einem alten Netzwerk ist kostspielig. Zu den üblichen Aufgaben gehören die Bereitstellung von Standardprodukten, das Einrichten von VPNs für Remote-Mitarbeiter, die Aktualisierung von VPN-Aggregatoren und die Sicherstellung (oft manuell), dass unterschiedliche Sicherheitskonfigurationen keine Konflikte verursachen oder Schlupflöcher aufweisen. Eine SASE-Architektur bietet einfach skalierbare Netzwerk- und Sicherheitsfunktionen direkt in der Cloud, implementiert eine zentrale, zusammenhängende Sicherheitsrichtlinie und verteilt sie automatisch.

Betrachtung eines Anwendungsbeispiels aus einem realen Unternehmen

Die in Abbildung 5-4 dargestellte traditionelle WAN-Architektur (Wide Area Network) der Acme Bank spiegelt nicht mehr wider, wie ihre Kunden mit Bankdienstleistungen interagieren. Cafés werden zu Finanzzentren. Kunden können mit mobilen Geräten Schecks einlösen und Einzahlungen vornehmen. Bankmitarbeiter interagieren bei der Beratung zu Finanzfragen und Konten über Tablets mit Kunden. Einige der Anwendungen wurden in die öffentliche Cloud verlagert, und die Bank hat begonnen, SaaS für CRM- und ERP-Systeme (Customer Relationship Management) zu verwenden. Die Bank muss auch Folgendes tun:

- Die Abhängigkeit von Service-Providern verringern
- Die Bereitstellungszeit für neue Standorte durch den Einsatz von Breitband, Long Term Evolution (LTE) und 5G zu verkürzen
- Den sicheren Zugang für Kunden und Mitarbeiter gewährleisten
- Die Anwendungsleistung zu verbessern
- ZTNA für Anwendungen in der öffentlichen Cloud und SaaS-Anwendungen bereitstellen

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

- Den sicheren WFA-Zugriff auf Anwendungen in der öffentlichen Cloud, über SaaS und einige „genehmigte" internetbasierte Dienste zulassen
- Das Failover aller Anwendungen und Telefonsysteme verbessern
- Mehr Transparenz und Kontrolle über Nutzer und Geräte erreichen

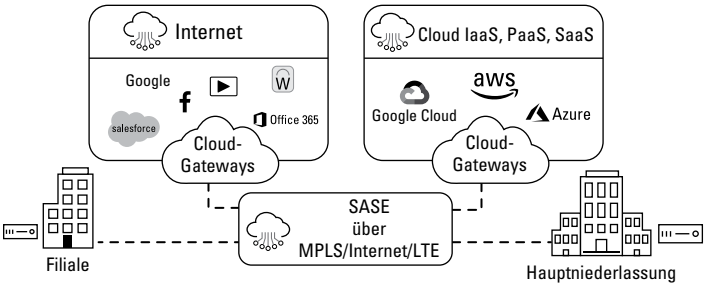


ABBILDUNG 5-4: Acme Bank-Architektur.

Die Acme Bank entschied sich für eine SASE-Architektur, die auf einer einzigen, multifunktionalen Plattform mit cloudnativem Service, Routing, SD-WAN, mehrschichtiger Sicherheit und UEBA bereitgestellt wird. Dadurch wurde der Infrastrukturbedarf sowohl vor Ort als auch in der Cloud vereinfacht, die Kosten wurden gesenkt und die Verwaltung automatisiert.

Die Bank führt außerdem in Rekordzeit Verbindungen zu Home Offices, Konferenzstandorten und Roadshows mit schnellen, zuverlässigen und sicheren SASE-Services ein. Alle wichtigen SASE-Funktionen wie WAN-Edge, Secure Web Gateway (SWG), Next-Generation Firewall (NGFW), Stateful Firewall, Uniform Resource Locator (URL)-Filterung, Data Loss Prevention (DLP), Intrusion Prevention System (IPS), Intrusion Detection System (IDS), Antivirus, Internet Protocol (IP)-Filterung, Dateifilterung, Cloud Access Security Broker (CASB), Remote Browser Isolation (RBI), Anti-Malware, Lateral Movement Detection und Secure Sockets Layer (SSL) Proxy sind vollständig in den cloudnativen SASE-Service integriert, der durch CPE-basierte Dienste (Customer Premises Equipment) vor Ort ergänzt wird.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- Verständnis der SASE-Architektur
- Nutzung der Vorteile von Single-Pass
- Zukunftssicherheit für Ihr Unternehmen

Kapitel 6
Evaluierung von SASE Best Practices

Secure Access Service Edge (SASE) ist sowohl eine Architektur als auch eine Implementierung. Es ist von entscheidender Bedeutung, verschiedene Implementierungen zu evaluieren, um sicherzustellen, dass Sie eine Architektur auswählen, die die erwarteten Sicherheitsvorteile und gleichzeitig die erforderliche Skalierbarkeit und Performance bietet.

In diesem Kapitel erfahren Sie mehr über SASE-Architekturattribute, die Vorteile einer mandantenfähigen Single-Pass-Softwareimplementierung und die Planung einer SASE-Implementierung, die den Anforderungen von heute und morgen gerecht wird.

Architekturen im Vergleich

Eine gute SASE-Architektur muss mehrere wichtige Attribute aufweisen, darunter die folgenden:

- Sie muss in jedem vorhandenem Netzwerk und jeder Infrastruktur koexistieren, was bedeutet, dass sie in jeder *Brownfield*-Umgebung (Mischung aus neuen und bereits vorhandenen/Legacy-Systemen) realisierbar sein sollte.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

- Sie muss auf einer soliden, sicheren Architektur mit der Flexibilität und Skalierbarkeit aufbauen, die für die Bereitstellung in jeder Cloud-Umgebung erforderlich ist – Equinix, Amazon Web Services (AWS), Azure, Google Cloud, Alibaba und vielen anderen.
- Sie muss die Ausführung in Containern/Microservices oder Bare-Metal-Geräten unterstützen und für die Leistungsoptimierung skalierbar sein.
- Sie muss cloudnativ, multiservice- und mandantenfähig sein.
- Sie muss eine zentrale Verwaltung mit dezentraler Sicherheitsdurchsetzung haben und die Durchsetzung von Richtlinien über strategisch platzierte, global verfügbare Points of Presence (PoPs) ermöglichen.
- Sie muss den Security Policy Enforcement Point verwenden, der dem Nutzer/Gerät, von dem aus der Zugriff auf die Anwendung erfolgt, am nächsten liegt.
- Sie muss über einen praxiserprobten, effektiven und vor Eindringen geschützten Sicherheits-Stack verfügen, der eine Vielzahl von Klassifizierungs- und Erkennungsfunktionen sowie Mechanismen zur Durchsetzung von Richtlinien bereitstellt.
- Sie muss softwaredefiniertes Wide Area Network (SD-WAN), Routing und Verschlüsselung mit Sicherheitsfunktionen kombinieren, um die beste Nutzer-/Anwendungserfahrung zu bieten und gleichzeitig alle Aspekte der Sicherheit durchzusetzen.

TIPP

Flexibilität und Auswahl sind die wichtigsten Überlegungen für eine gute SASE-Implementierung.

Abstimmung technologischer und betrieblicher Anforderungen

Unternehmen müssen die technologischen Anforderungen stets mit den betrieblichen Anforderungen in Einklang bringen. Die in Abbildung 6-1 dargestellte komplexe Legacy-Zweigstellenarchitektur resultiert daraus, dass beim Erscheinen neuer technologischer Anforderungen eine Technologielösung auf der anderen aufgebaut wird: WAN-Optimierung (Wide Area Network), Firewall der nächsten Generation (NGFW), Unified Threat Management (UTM), SD-WAN und LTE-Zugriffslösungen (Long Term Evolution).

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

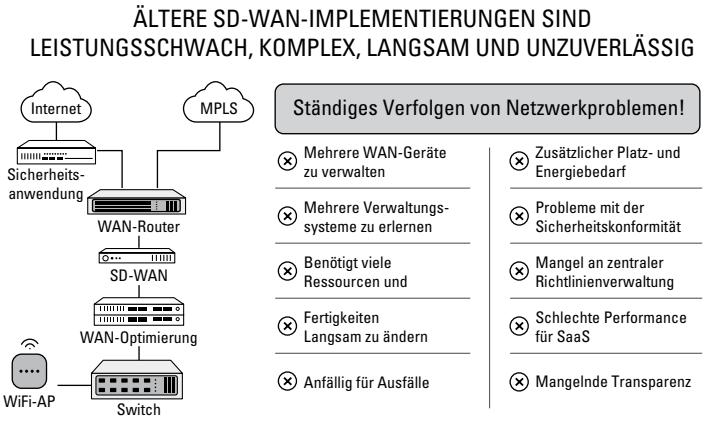


ABBILDUNG 6-1: Legacy-Hardware in Filialen.

Im Laufe der Zeit zögert das IT-Personal möglicherweise, etwas an der Architektur zu ändern, da sie ja irgendwie funktionstüchtig ist und schwierig zu reparieren wäre, wenn eine anstehende Änderung eine Reihe von Funktionen beeinträchtigen würde. Dieser gerade eben funktionstüchtige Status quo geht jedoch mit immensen Kosten hinsichtlich Komplexität und Ineffizienz einher.

TIPP

Es braucht eine wesentlich einfachere Architektur, die sowohl hinsichtlich Investitions- als auch Betriebskosten effizient ist. Wenn Sie nicht mehrere Geräte verwalten müssen, müssen Sie sich auch nicht in mehrere Managementsysteme einarbeiten oder mit der Entwicklung mehrerer Produkte Schritt halten.

Je nach Faktoren wie der Größe des Unternehmens, der Komplexität der Infrastruktur, den Sicherheitsanforderungen und der globalen Präsenz sollten Unternehmen eine SASE-Implementierung unter eigener Regie, von einem Serviceprovider angebotene SASE-Services oder eine Kombination beider in Betracht ziehen.

MERKE!

Aufgrund der tiefgreifende Auswirkung von SASE-Installationen muss die SASE-Architektur nicht nur Skalierbarkeit für die Datenebene, sondern auch für die Kontroll- und Verwaltungsebene bieten. Dies ermöglicht es großen Netzwerkbetriebs- und Sicherheitsteams eine effektive Bereitstellung von SASE-Services auf breiter Ebene für eine große Anzahl von Mandanten und bietet gleichzeitig die Möglichkeit, hybride Betriebsmodelle bereitzustellen, bei denen Aspekte der Services gemeinsam durch den Serviceprovider und das Unternehmen verwaltet werden.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Die Herausforderungen der Nachrüstung von Sicherheit

Eine Lösung nach der anderen nachzurüsten, um eine SASE-Lösung zusammenzustellen, bedeutet, dass jede einzelne Lösung eine andere Codebasis aufweist und jede von ihnen unterschiedliche Angriffsflächen bietet. Es ist nahezu unmöglich, eine solche zusammengewürfelte Architektur hochsicher zu gestalten oder ihre Einhaltung von Standards und Vorschriften nachzuweisen.

Darüber hinaus beansprucht eine derart nachgerüstete Architektur mehr Platz und Energie bei schlechterer Leistung. Eine für SASE nachgerüstete Legacy-Sicherheitslösung resultiert in unnötigen Schritten, Sicherheitslücken und dem Offenlegen von Schwachstellen.

Nutzung der Vorteile einer Single-Pass-Lösung

Eine ideale SASE-Implementierung ist ein vollständig integrierter Software-Stack (wie in Abbildung 6-2 dargestellt), der nicht auf die Verkettung von Services oder die Verbindung mehrerer Funktionen/Services unterschiedlicher Anbieter über mehrere Geräte hinweg angewiesen ist. Bei den SASE-Lösungen einiger Anbieter handelt es sich um ein Flickwerk aus Funktionen, die aus einer Reihe von Übernahmen oder von anderen Anbietern stammen.

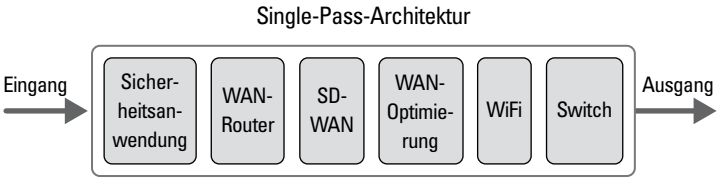


ABBILDUNG 6-2: Daten, die einen Single Pass durchlaufen.

HINWEIS

Die Branche stellt seit Jahren Kombinationen von Einzweckmaschinen (physisch und/oder virtuell) bereit, aber diese Strategie ist aufgrund der inhärenten Verarbeitungslatenz, unvorhersehbaren Angriffsflächen und allgemeinen Komplexität unzureichend, um Ihnen den Weg in die Zukunft zu bahnen. Um die Latenz zu reduzieren, sollte SASE den Datenverkehr unter Verwendung einer Single-Pass-Architektur überprüfen, bei der der Datenstrom geöffnet (möglicherweise entschlüsselt) und nur ein einziges Mal unter paralleler Verwendung mehrerer Policy Engines, idealerweise im Arbeitsspeicher, überprüft wird, ohne dass Inspektionsdienste verkettet werden müssen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Elastische Skalierung

TIPP

Höchstleistung wird durch den Einsatz einer Multicore-CPU mit einer Single-Pass-Architektur für die Parallelverarbeitung erzielt. Dieses Modell realisiert eine extrem elastische, skalierbare und wirtschaftliche SASE-Implementierung.

Eine leistungsstarke SASE-Implementierung zeichnet sich durch die folgenden Attribute aus:

- Ist Multicore und Multithread
- Unterstützt die DPDK-Schnittstelle (Data Plane Development Kit)
- Überträgt Pakete effizient, ohne viel Kopieren oder Kontextwechsel und umgeht wo möglich den Kernel
- Hat eine Parallelverarbeitungs-Softwarearchitektur
- Dupliziert keine Funktionen. Jede Funktion wird nur einmal ausgeführt und ihre Ergebnisse werden von anderen Funktionen genutzt

Effiziente Nutzung einer einzigen Software

Die SASE-Architektur basiert auf Leistungsmerkmalen und Funktionen, die von Grund auf in einem einzigen Software-Stack entwickelt wurden, in den Sicherheit bereits eingebettet ist: Secure Web Gateway (SWG), NGFW, Stateful Firewall, Uniform Resource Locator(URL-)Filterung, Data Loss Prevention (DLP), Intrusion Prevention System (IPS), Antivirus, Internet Protocol(IP-)Filterung, Dateifilterung, Cloud Access Security Broker (CASB), Remote Browser Isolation (RBI), Anti-Malware, Lateral Movement Detection, und SSL-Proxy (Secure Sockets Layer), erweitertes skalierbares Routing, voll ausgestattetes SD-WAN, WAN-Optimierung, UEBA (User and Entity Behavior Analytics) und mehr.

Konvergierte SASE (siehe Abbildung 6-3) stellt sicher, dass Pakete nicht separat und unabhängig jedes Funktionsmodul durchlaufen, wiederholt verarbeitet werden und so zu Ineffizienz, schlechter Leistung und potenziellen Sicherheitsschwachstellen führen.

Sicherheitsfunktionen müssen sich problemlos in die SASE-Architektur mit einer einzigen Softwarelösung integrieren lassen oder Teil dieser Architektur sein. Idealerweise sollten leistungsfähige Sicherheitsfunktionen von Beginn der Entwicklung in den einzelnen Software-Stack integriert werden – so konzipiert, dass sie alle als eine Einheit zusammenarbeiten.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

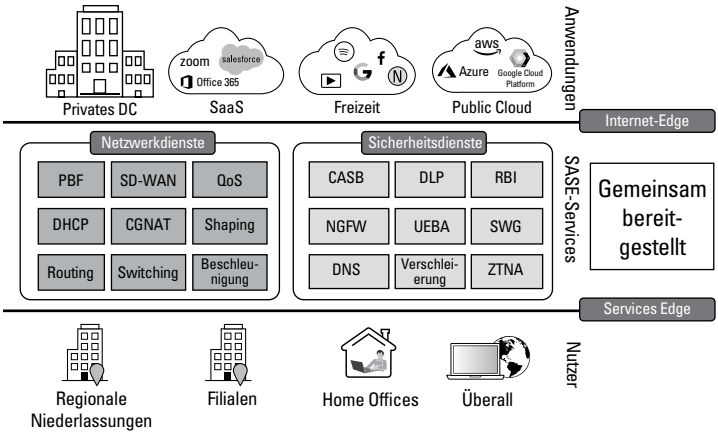


ABBILDUNG 6-3: Konvergierte Netzwerk- und Sicherheitsdienste.

Eine echte SASE-Architektur sollte folgende Merkmale aufweisen:

- Verwendet ein einziges, einheitliches Verwaltungssystem
- Ist leistungsoptimiert
- Ist für Software as a Service (SaaS) optimiert
- Hat einen einzigen Software-Stack mit eingebetteter Best-of-Breed-Sicherheit
- Ist softwarebasiert und hardwareneutral, benötigt keine proprietäre Hardware
- Stellt minimale Anforderungen an das IT-Personal hinsichtlich der Verwaltung
- Ist anpassungsfähig und agil
- Ist widerstandsfähig gegen Ausfälle
- Bietet vollständige Transparenz und Analytik

Kontextbezogene Sicherheit und kontextbezogener Zugriff

Sie müssen in der Lage sein, Ihre Nutzer und Geräte vollständig zu verstehen und zu segmentieren. Dies erfordert eine mandantenfähige Architektur.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

MERKE!

Cloudnative SASE-Architekturen sind fast immer mandantenfähig und ermöglichen mehreren Kunden die Nutzung der zugrunde liegenden Datenebene. Einige Anbieter verwenden stattdessen eine dedizierte Instanz für jeden Kunden, aber die Architektur kann die Skalierbarkeit beeinträchtigen. Die Versorgung einzelner Mandanten führt in der Regel zu geringeren Dichten und potenziell höheren Kosten, die an das Unternehmen weitergegeben werden.

Mandantenfähigkeit erzielt Sicherheit, indem die Richtlinien, Konfigurationen, Protokolle und Analysen eines Mandanten von denen der anderen getrennt bleiben. Eine derartige Architektur schützt die Nutzer, Geräte und Daten einer Abteilung, selbst wenn eine andere Abteilung – die unter einem anderen Mandanten gehostet wird – bedroht ist. Dieser Ansatz schränkt den Schadensumfang bei einer Datenschutzverletzung erheblich ein.

Die rollenbasierte Zugriffskontrolle (RBAC) ist für das Erreichen kontextbezogener Sicherheit von entscheidender Bedeutung. In einer mandantenfähigen Umgebung ermöglicht die Konfiguration von Sicherheitsrichtlinien der richtigen Person am richtigen Gerät den Zugriff auf die richtige Anwendung, und nur das.

TIPP

Mandantenfähigkeit gewährleistet die Isolation der Daten verschiedener Mandanten, während RBAC sicherstellt, dass Nutzerberechtigungen festlegen, auf welche Anwendungsdaten von welchen Benutzern innerhalb eines Mandanten zugegriffen wird.

Single-Pass- und cloudnative Vorteile

Zur Realisierung maximaler Flexibilität bei geringsten Latenzzeiten und Ressourcenanforderungen ist eine cloudnative Single-Pass-Architektur von Vorteil. Eine gut konzipierte Implementierung führt den Großteil der Services parallel (Single-Pass) aus, idealerweise im gleichen Cloud-Service-Stack, am gleichen Standort und zur gleichen Zeit. Es sollte nur ein einziges Mal erforderlich sein, den Datenverkehr zu öffnen, zu analysieren, neu zu verschlüsseln und weiterzuleiten. So werden aufwändiges Kopieren von Paketen mit hoher Latenz und Inkonsistenzen in der Serviceausführung vermieden.

HINWEIS

Nicht aufeinander abgestimmte, nachgerüstete Lösungen bieten weder die zum Schutz von Nutzern und Geräten erforderliche Netzwerktransparenz und -kontrolle, noch die Verwaltungstools zur Einhaltung von Industriestandards und behördlichen Vorschriften/Gesetzen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Planung für Skalierbarkeit, Performance und die Zukunft

Die organisatorische Planung muss nicht nur das heutige Geschäftsumfeld, sondern auch einen Weg in die Zukunft umfassen. Eine zukunftssichere SASE-Architektur muss eine neue Welle von Technologien unterstützen, wie IoT-Geräte, BYOD-Geräte (Bring-Your-Own-Device), Smart Manufacturing, Augmented Reality (AR), Virtual Reality (VR) und Unified Communications as a Service (UCaaS), die ihre eigenen Herausforderungen im Hinblick auf Sicherheit und Konnektivität mit sich bringen.

TIPP

Jede SASE-Lösung, die Sie heute auswählen, muss über Jahre hinweg skalierbar und leistungsfähig sein und Sicherheit für neue technologische und geschäftliche Entwicklungen wie 5G bieten, die exponentiell mehr Rechenleistung erfordern.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- **Von besserer Sicherheit profitieren**
- **Finden der benötigten Größenordnung und Leistung**
- **Unterstützung der neuesten Technologien und Standards**

Kapitel 7
Zehn Dinge, die bei einer SASE-Lösung zu beachten sind

Es ist wichtig, verschiedene Secure Access Service Edge (SASE)-Lösungen zu bewerten, um sicherzustellen, dass Sie ein Angebot auswählen, das die von Ihnen erwarteten Sicherheitsvorteile bietet und gleichzeitig eine sogenannte Single-Pane-of-Glass sowie den Umfang und die Leistung bietet, die Sie benötigen. Hier sind zehn wichtige Punkte, die bei einer SASE-Implementierung zu beachten sind:

- **Bereitstellungsoptionen** sollten eine Implementierung über die Cloud, vor Ort oder eine Kombination beider zu jedem beliebigen Standort oder Gerät für jeden Anwendungstyp ermöglichen. Ein cloudbasiertes Bereitstellungsmodell sollte in der Lage sein, dem Stack dynamisch neue Services oder mehr Rechenleistung hinzuzufügen.
- **Eine Architektur mit geringer Latenz und hoher Performance mit paralleler Single-Pass-Verarbeitung** in einem einzigen Software-Stack, die alle oder die meisten der wichtigsten SASE-Funktionen wie WAN-Edge (Wide Area Network), Secure Web Gateway (SWG), Next-Generation Firewall (NGFW), Stateful Firewall, Uniform Resource Locator(URL-)Filterung, Data Loss Prevention (DLP), Intrusion Prevention System (IPS), Intrusion Detection System (IDS), Antivirus, Internet Protocol(IP-)Filterung, Dateifilterung, Anti-Malware, Lateral Movement Detection und Secure Sockets Layer (SSL) Proxy

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

umfasst. Es sollte keine Serviceverkettung zum Kombinieren von Services erforderlich sein.

- **Ein verteiltes System von Cloud-Gateways** rund um die Welt, zur Versorgung vorhandener oder neuer Nutzer und Anwendungen. Es sollte über Cloud-Gateways verfügen, die über ein Traffic Engineering-Protokoll miteinander verbunden sind. Dies garantiert die bestmögliche Leistung hinsichtlich der Anwendungsqualität (QoE) durch die Auswahl des optimalen Pfads zu Software-as-a-Service (SaaS), Cloud-Anbietern und Remote-Standorten auf Basis von End-to-End-Service-Level-Agreements (SLAs).
- **Eine einzige Verwaltungskonsole** zur globalen Konfiguration, Wartung und Überwachung des Systems mit Transparenz für Standorte, Dienste, Anwendungen, Nutzer und Geräte.
- **Ein zukunftssicheres Design und eine Architektur**, die Standardprotokolle, flexible APIs (Application Programming Interfaces) und die Integration in die vorhandene Infrastruktur unterstützt.
- **Skalierbare Paketierung, flexible Preisgestaltung und ein Wachstumsmodell** (Pay-as-you-grow/shrink) mit einer mandantenfähigen Cloud und On-Premises-Design.
- **Unterstützung von integrierter DLP als Cloud-Funktion** zusätzlich zu einer On-Premises-Funktion, um Transparenz und Schutz für sensible Daten und APIs zu Multicloud-Umgebungen zu bieten. Cloudnative DLP kann sehr effektiv sein, da die CSPs selbst den besten Zugriff auf die von ihnen gespeicherten Daten haben und die Möglichkeit Operationen an diesen durchzuführen.
- **Integrierte UEBA-Funktionalität (User and Entity Behavior Analytics)**, die Analysen zur Bewertung der Aktivität von Nutzern und anderen Entitäten wie Hosts, Anwendungen, Netzwerkverkehr und Datenspeicher bereitstellt. Mit UEBA können Sie Bedrohungen und potenzielle Vorfälle erkennen, indem im Vergleich mit Standardprofilen und Nutzerverhalten anomale Aktivitäten identifiziert werden. UEBA sollte Unternehmen bei der Erkennung von und Reaktion auf Bedrohungen, externe wie interne, (hauptsächlich kompromittierte Insider, manchmal böswillige Insider) unterstützen.
- **Unterstützung von Remote Browser Isolation (RBI)** mit einem selektiven Ansatz zur Entschärfung und Wiederherstellung von Inhalten für Web-Browser-Sitzungen. Die Unterstützung der selektiven Anwendung von RBI kann restriktivere URL-Reputationsrichtlinien für hochsensible Umgebungen ermöglichen.
- **Eine cloud-, hardware- und transportunabhängige Architektur** mit Unterstützung für das Internet der Dinge (IoT), 5G, künstliche Intelligenz (KI), Maschinenlernen (ML) und Anpassungsfähigkeit an andere neue Technologien.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Schützen Sie Ihr Unternehmensnetzwerk mit innovativen Lösungen

Secure Access Service Edge (SASE) bietet eine Möglichkeit die von Gefahren bedrohte moderne Unternehmensnetzwerklandschaft durch vertrauenswürdige Sicherheitslösungen zu schützen Das Funktionsspektrum reicht weit über das älterer Sicherheitsarchitekturen hinaus und umfasst Identität, Vertrauen und Kontext unabhängig von Verbindung, Nutzer, Gerät oder Anwendung. In diesem Buch erfahren Sie, was SASE umfasst, wie sie Unternehmen und Organisationen nutzt, wie sie die Sicherheit unterstützt, wie sie am besten implementiert wird und Sie ihre besten Funktionsmerkmale nutzen können.

Inhalt:

- Verstehen der Funktionen und Anforderungen von SASE
- Schutz des Netzwerkperimeters
- Optimierung von Sicherheit und Leistung
- Geringere Kosten und Komplexität
- Bereitstellung eine Erlebnisses konsistenten
- Zentralisierung von Verwaltung und Kontrolle

VERSA NETWORKS

Kumar Mehta ist ein Visionär, der mehrere bahnbrechende Netzwerk- und Sicherheitsprodukte geleitet hat. **Apurva Mehta** ist ein renommierter Ingenieur, der branchenführende Produkte in den Bereichen Netzwerk, Sicherheit und Packet-Core entwickelt hat, die Umsätze in Milliardenhöhe generiert haben.

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

ISBN: 978-1-119-83637-7
Nicht für den Wiederverkauf

für dummies®

WILEY END USER LICENSE AGREEMENT

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