Cloud-Dienste effizient, sicher und zuverlässig untereinander und mit anderen SaaS-Diensten vernetzen

Maschenvielfalt

Christoph Puppe

Wer Multi-Cloud nutzt, kommt früher oder später um die Vernetzung zwischen Clouds nicht herum. Software-defined Cloud Interconnection (SDCI), auch Network as a Service (NaaS) oder Multi-Cloud-Routing (MCR) genannt, und IPsec-Overlay-Netze setzen sich durch. Doch lauern diverse Stolperfallen.

Ein zentrales Thema beim Vernetzen von Cloud-Diensten ist Durchsatz, aber auch Zuverlässigkeit und Schutz vor Mitlesen sind zu beachten. So wie Software-defined WAN (SD-WAN) die Vernetzung von Standorten untereinander und mit der Cloud vereinfacht, hat sich auch die Vernetzung der Cloud-Service-Provider (CSP) untereinander verändert (siehe Glossar). Hier sind – wie auch bei Multi-Cloud selbst – die teilweise erheblichen Unterschiede der CSP zu beachten.

Eine NaaS-Plattform, die in allen großen CSP zu Hause ist, muss diese Unterschiede überbrücken und dem Anwender eine gemeinsame Sicht auf alle Netze bieten. Sie muss möglichst viele der notwendigen und wünschenswerten Sicherheits- und Performancefeatures enthalten. Die gemeinsame Sicht und die gleichen Features überall sind notwendig, denn der Betrieb in einer Multi-Cloud-Umgebung ist bereits sehr komplex. Wenn die Betriebsmannschaft für jeden CSP die Eigenheiten beachten muss, gerät dies schnell so unübersichtlich, dass Betrieb, Überwachung und Audits die Teams vor große Herausforderungen stellen.

Eine Sicherheitsarchitektur ist unerlässlich

Auch in der Cloud dürfen nur die Dienste öffentlich erreichbar sein, die das auch unbedingt benötigen. Wie auch inhouse sollten eigentlich nur die Firewall und über diese das Anwendungsgateway Dienste für fremde Netze bereitstellen. Die in diesem Artikel vorgestellten Optionen zum Verbinden von Diensten bei unterschiedlichen CSP ermöglichen genau dieses Design für Multi-Cloud. Sie bieten die Möglichkeit, die Erreichbarkeit zwischen internen Netzwerken bei unterschiedlichen CSP herzustellen. So sind die Services in diesen Netzen (VCP oder vNET) nur für andere Dienste in diesen Netzen erreichbar.

Die Alternative wäre, die Dienste bei allen CSP über eine öffentliche IP-Adresse anzubieten und den Datenverkehr darüber abzuwickeln. Der Nachteil dabei ist offensichtlich: Nur die Authentifizierung am Dienst verbleibt als Sicherheitsgrenze. Und sollte der Dienst eine Verwundbarkeit haben, die keinen Log-in benötigt (Pre-Auth), wäre er Angreifern schutzlos ausgeliefert. Die Zielrichtung hier ist daher, mehrere Sicherheitsgrenzen gleichzeitig einzusetzen. Und die durch die VPN und vNET ermöglichten internen Netzwerke sind hier der Netzperimeter, der seit 20 Jahren totgesagt wird, aber zusammen mit „Identity as the Perimeter“ immer noch eine der zentralen Grundlagen zur Absicherung ist. So schlicht es klingt, so wirkungsvoll ist es bis heute, die Zahl der möglichen Angreifer durch Firewalls und minimale Regelungen für Datenverkehr stark zu reduzieren.

Vielschichtige Wunschliste

Die Wünsche an ein Netzwerk, sein Management, Überwachung und Sicherheit sind mannigfaltig. Der erste Punkt ist sicherlich Verfügbarkeit. Erwartet werden fast 100 Prozent und die CSP bieten dies für ihre öffentlichen und internen Netzwerke zuverlässig an. Ausfälle sind selten und wenn sie vorkommen, oft auf eine Region beschränkt, wobei auch großflächige Ausfälle vorkommen können. Zur Zuverlässigkeit gehört auch eine gleichmäßige und niedrige Latenz. Schwankungen in der Latenz sind heute wie ein Ausfall zu betrachten, und sollte eine Netzwerkverbindung langsam sein, kann dies erhebliche Auswirkungen auf die darüber laufenden Dienste haben. Nur ein lückenloses Monitoring der Verfügbarkeit des Netzwerks inklusive Messung der Latenz bringt die notwendige Sichtbarkeit, die für das Management erforderlich ist.

Eine weitere Grundlage ist das Routing, das die Netzwerke bei den CSP und in den eigenen Niederlassungen miteinander verbinden muss. Dabei ist dann die Sicherheit zu beachten, denn diese Netzsegmente sollten nur über mindestens Paket-

© Copyright by Heise Medien.
Persönliches PDF für Christoph Puppe aus 99096 Erfurt

Glossar

CSP – Cloud-Service-Provider: hier zumeist die großen, auch Hyperscaler genannten Anbieter, die viele Standorte haben: AWS, Azure, Google Cloud Platform, Oracle Cloud, IBM Cloud und Alibaba.

OnRamp – Zugriffspunkt zum Netz des CSP: eine direkte physische Verbindung in Form eines Routers des CSP im Rechenzentrum, zu dem der Betreiber des Rechenzentrums eine virtuelle oder physische Leitung legen kann.

MPLS – Multiprotocol Label Switching: Routing zwischen mehreren Edge-Routern eines Netzanbieters, bei dem alle Standorte aller Kunden über ein gemeinsames Netzwerk miteinander verbunden sind und jeder Kunde nur seine Daten sieht.

NaaS – Network as a Service: Derzeit steht dies für mehrere Angebote. Generell ist es wie SD-WAN ein API-getriebener Dienst, der Netzwerkdienste zwischen CSP und Kunden bereitstellt, aber auch ein IPsec-Mesh meinen kann.

SD-WAN – Software-defined Wide Area Network: der Zusammenschluss aller physischen Verbindungen und deren gemeinsame Verwaltung, der Nachfolger von MPLS.

VPC – Virtual Private Cloud bezeichnet ein virtuelles Netzwerk beim CSP, das nur zu einem Kunden gehört und dessen Konfiguration in dessen Verantwortung liegt. Heißt bei Azure vNET. Es sind IPv4-Netze aus dem RFC1918-Bereich, die aus dem Internet nicht erreichbar sind, sofern der Kunde weder Gateway noch Firewall betreibt. Es ist quasi das Intranet in der Cloud.

filter miteinander reden. Besser noch sind erweiterte Sicherheitsoptionen wie Intrusion Prevention, Data Leakage Prevention und natürlich das einfache Anwendungssicherheitsgateway wie eine Web-Application-Firewall, die Verbindungen auf Layer 7 begutachtet.

Das alles betrifft den Datenverkehr innerhalb dieser VPC. Der Schutz dieses als intern zu betrachtenden Netzes vor Angriffen von außen ist auch zu beachten. Denial of Service (DoS) ist hier genauso Thema wie Abhören und Verändern der Daten in Bewegung. Gegen DoS hilft nur ein CSP, der die öffentlichen IP-Adressen seiner Kunden vor diesen Angriffen schützen kann. Hier sind die großen Hyperscaler gut aufgestellt und auch heftige DoS-Angriffe lassen sich viel besser bei einem CSP überstehen als in einer eigenen Infrastruktur.

Manche CSP haben auch besondere Netzwerkverbindungen innerhalb der eigenen Infrastruktur, die Verbindungen zu anderen Kunden über nicht öffentliche IP-Adressen erlauben. Ein Beispiel dafür ist der Private Link bei Azure und AWS, bei GCP heißt der Dienst Private Service Connect. Er verbindet die privaten Netze eines Kunden mit einem Dienst desselben oder eines anderen Kunden und nutzt dafür nur das interne Netzwerk des CSP ohne öffentliche IP-Adressen. Innerhalb der eigenen vNET respektive VPC bei einem CSP sind alle Dienste einfach miteinander zu vernetzen, weshalb dieser Artikel auf diesen Fall nicht weiter eingeht.

X-TRACT

- Software-defined Cloud Interconnection (SDCI) bietet viele Optionen beim Vernetzen von Standorten sowie eigenen und fremden Cloud-Services.
- SDCI-/NaaS-Anbieter rechnen Egress nach Bandbreite und nicht nach Volumen ab.
- Selbst gebaute IPsec-Meshes oder kommerzielle Angebote können eine Alternative zu physischen SDCI sein oder diese ergänzen.

Andere Standorte und CSP anbinden

Geht es darum, Daten zwischen unterschiedlichen CSP oder den eigenen Standorten auszutauschen, bieten die CSP zwar große Bandbreiten in das Internet und ein eigenes Peering, Zusatzdienste wie Private Link gehören jedoch nicht dazu. Hier fehlt den Firmen sicherlich auch die unbedingte Motivation, Kunden einen einfachen Weg aus dem eigenen Netz zu Diensten bei anderen CSP als Service anzubieten.

Für das Anbinden der eigenen Standorte gibt es allerdings viele Optionen. Die CSP selbst bieten entweder VPN oder Standleitungen zu ihren Rechenzentren an. Letztere oder der OnRamp (siehe Glossar) heißt bei jedem CSP anders: Azure bezeichnet es als ExpressRoute, AWS als Direct Connect und GCP als Cloud Interconnect. Die Alternative zu diesen Angeboten sind die SD-WAN-Anbieter, die neben der Vernetzung der Standorte auch die CSP-Anbindung ermöglichen. Diese Angebote hinsichtlich Service, Leistung und Preis zu vergleichen, ist ein eigenes Thema und könnte wahrscheinlich ein Buch füllen. Eine Beschreibung der Grundlagen findet sich in unserem Schwestermagazin c't [1]. Auch wer in seinem RZ oder beim

© Copyright by Heise Medien.
Persönliches PDF für Christoph Puppe aus 99096 Erfurt

genutzten Colocation-RZ keinen OnRamp eines CSP hat, kann die Vorteile der direkten Verbindungen nutzen. Die SD-WAN-Anbieter betreiben zumeist einen Router an einem oder mehreren OnRamp-Standorten des CSP. Wer also bereits einen größeren Provider für die physische Anbindung der Standorte nutzt, hat wahrscheinlich auch die Möglichkeit, sich über diesen mit den CSP zu verbinden.

Die Anbindung der Benutzer wird heute oft unter dem Stichwort Secure Access Service Edge (SASE) geführt [2]. Beides sei hier kurz erwähnt, denn eine Multi-Standort-, Multi-Cloud- und Remote-Arbeitsplatz-Netzarchitektur muss all diese Themen beachten und zu einer gemeinsamen und sicheren Lösung finden.

Option 3rd-Party physical Interconnect

Einige große Carrier treten mit ihren Netzen als NaaS-Anbieter (Network as a Service) in direkte Konkurrenz zu den Verbindungsoptionen der CSP. Sie haben eigene OnRamps zu den Hyperscalern und der über diese Zugänge übertragene Datenverkehr wird hauptsächlich vom NaaS-Anbieter abgerechnet. Der CSP berechnet nur den Egress-Traffic bis zur Region, wo der OnRamp angeschlossen ist, was erheblich preiswerter ist als der Datenverkehr zwischen Regionen des CSP, besonders wenn diese weit auseinanderliegen. Weil diese Anbieter zumeist mehrere Dutzend oder Hunderte Locations als OnRamp nutzen, sind damit auch Verbindungen zwischen VPC in unterschiedlichen Regionen des gleichen CSP möglich. Da alle CSP sowohl Egress-Traffic als auch Transfers zwischen Regionen in Rechnung stellen, kann dies erheblich Kosten sparen. So kostet bei GCP ein Gigabyte zwischen Regionen auf unterschiedlichen Kontinenten schon 0,08 US-Dollar, während für eine direkte Verbindung über einen anderen Carrier nur ein monatliches Fixum in Abhängigkeit von der Bandbreite anfällt.

Die Anbieter dieser Netzverbindungen zu und zwischen den CSP sind Firmen wie Equinix, MegaPort, PacketFabric, Unitas und interCloud sowie einige andere im Markt für NaaS oder Software-defined Cloud Interconnect (SDCI). So bietet Equinix einen Cloud-PoP nur für die Kunden im eigenen Rechenzentrum an, andere Carrier wie MegaPort sind rechenzentrumsneutral, kümmern sich auch um die letzte Meile zwischen den Standorten der Kunden und ihren PoPs und stellen dann über eigene Leitungen die Verbindung zu den OnRamps der CSP her. Die Anbieter sind hier dafür verantwortlich, dass der Datenverkehr sicher transportiert wird, wie es auch schon bei MPLS-Diensten der Fall ist.

Option Virtual Interconnect

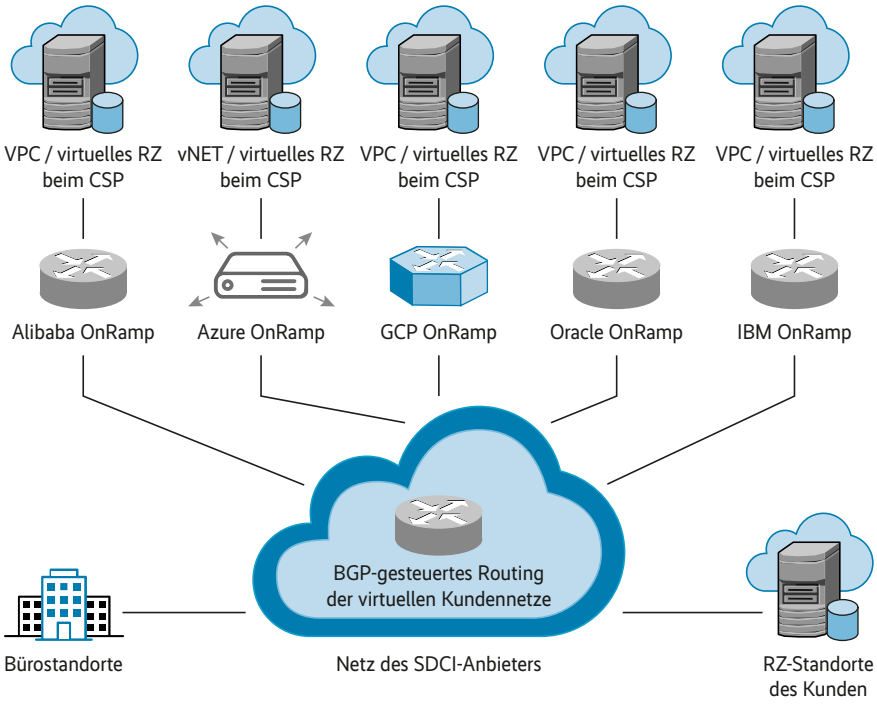
Wer seine VPC und vNET bei unterschiedlichen CSP verbinden möchte, kann dies auch über ein IPsec-Mesh mit Routern in den VPC bei den CSP einrichten. Dieser Ansatz geht den Weg des geringsten Widerstands und nutzt von den CSP zumeist nur die einfachsten Basisdienste wie ein lokales Netzwerk und eine öffentliche IP-Adresse. Eine eigene Linux-VM stellt dann den Router inklusive Firewall und Verwaltung bereit. Mehrere VMs bei einem oder mehreren CSP und den eigenen Standorten verbinden sich über IPsec zu einem virtuellen Transitnetz. Sie können aber auch die von den CSP angebotenen Optionen wie VPN-Gateways, VPC-Peerings, private Links und direkte Verbindungen wie ExpressRoute nutzen.

Der Kunde kann in diesem Netz dann festlegen, welche internen IPs in welchen VPC und an welchem Standort miteinander reden können und welche Firewallregeln dafür gelten. Die Verwaltung erfolgt dabei über eine vom Anbieter bereitgestellte Zentrale, die alle Router kontrolliert und auch überwacht. Dieser Ansatz umgeht die Unterschiede der diversen CSP und kann so Anwendern eine einheitliche Oberfläche mit immer gleichen Features in allen Netzwerken bieten. Die Einrichtung erfordert Service-Accounts beim CSP, die teilweise weitreichende Rechte haben.

Im Prinzip ist diese Methode nicht anders als ein SD-WAN. Eine Control Plane für diverse Verbindungen vereinfacht das Management. Edge-Router stellen die Verbindung zu den Cloud- und anderen, beispielsweise physischen Standorten her. Wie die Edge-Router miteinander verbunden sind, sollte für den Anwender transparent sein. Aber wie immer ist es notwendig, die Physik hinter dem virtuellen Dienst zu kennen, möchte man Sicherheit, Verfügbarkeit, Bandbreite und Latenzen richtig einschätzen.

Neben den Kosten für die IaaS-Instanzen und die Lizenzen für eine Managementsoftware fallen für die Datenverbindungen noch die jeweiligen Egress-/Ingress-Kosten der CSP an. Bei der Bandbreitenplanung ist auch zu beachten, dass hier die Interface-Leistungsfähigkeit der IaaS-Instanzen der limitierende Faktor ist. Diese unterscheidet sich von der der Standleitungen teils erheblich. So bewältigt ein Azure ExpressRoute bis zu 100 GBit/s, aber die größte VM ermöglicht im Moment nur 40 GBit/s. ExpressRoute kann also 2,5-mal schneller sein als eine VM.

Bei Azure verhält es sich genau umgekehrt. Dort bietet die schnellste „Direct



Eine Software-defined Cloud Interconnection (SDCI) in der schematischen Übersicht. Da hier die Leitungen nicht verschlüsselt sind, ist ein IPsec-Mesh als Overlay zu empfehlen (Abb. 1).

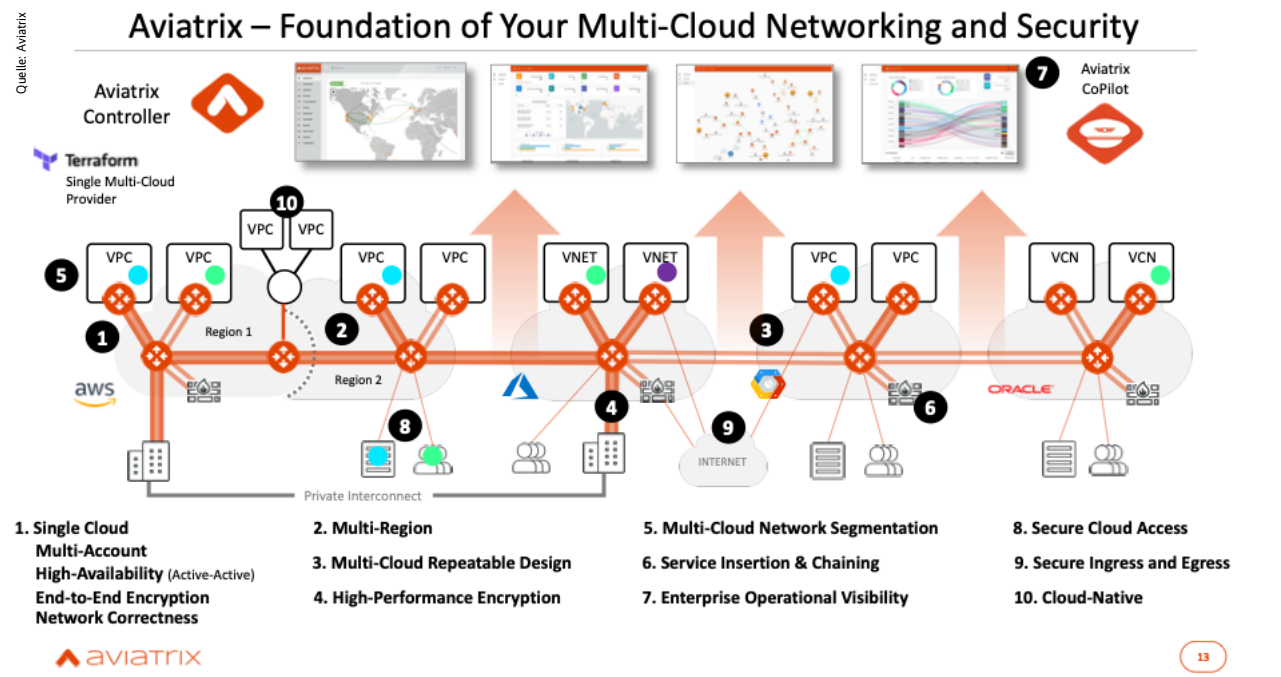
© Copyright by Heise Medien.
Persönliches PDF für Christoph Puppe aus 99096 Erfurt

Aviatrix

Einer der Marktführer in der NaaS-Sparte und selbst ernannter Erfinder des „Multi Cloud Networking“ ist Aviatrix. Seine Software ist bei AWS, Azure, GCP, Alibaba und OCI über den Marketplace erhältlich. Im sogenannten FireNet kann das Tool die virtuellen Firewalls der Hersteller Palo Alto Networks, FortiGate, CheckPoint, Netgate PFsense und Barracuda einbinden. Das Aviatrix-Gateway enthält aber auch eine eigene Stateful Firewall.

Aviatrix hat keine eigenen Leitungen oder Peering Points. Es nutzt die öffentlichen IP-Adressen der virtuellen Router für IPsec-Tunnel und beherrscht auch GRE-Tunnel über AWS Direct Connect, für Azure und GCP ist dies nicht verfügbar. Bei allen dreien ist allerdings IPsec über die jeweiligen Direktverbindungen möglich. Mit der „Insane Mode Encryption“ umgeht Aviatrix die Limits der CSP und ermöglicht sehr viel höheren Durchsatz, indem es pro CPU-Core einen IPsec-Tunnel nutzt und diese bündelt. Für solche Verbindungen innerhalb von AWS nutzt Aviatrix Peering.

Vertrieben wird die Software für die Router als virtuelle Appliance für den Einsatz beim CSP und als die CloudN-Appliance als Hardware für die Anbindung von Standorten (siehe ix.de/zz6b). Zusätzlich hat der Anbieter die Analysesoftware CoPilot im Portfolio. Sie bietet Anwendern Einsicht in die aktuelle Auslastung, Datenverbindungen, Qualität der Verbindungen, Routingeinträge in allen Edges und mit ThreatIQ ist auch eine Erkennung von Angriffen enthalten.



Das von Aviatrix initiierte Multi Cloud Networking beherrscht unterschiedliche Anbindungen an die CSP-Netzwerke, wobei die roten Verbindungen mit IPsec realisiert sind (Abb. 2).

Connect“-Option nur 10 GBit/s und die schnellste IaaS-Instanz 100 GBit/s. GCP schafft für Instanzen und auch für den Cloud Interconnect bis zu 100 GBit/s. Alle CSP verteilen die Bandbreite allerdings über alle Interfaces. Also stehen einer VM mit 100 GBit/s und drei Beinchen in drei VPC plus einer öffentlichen IP-Adresse bei gleichmäßiger Auslastung auf allen vier virtuellen Interfaces nur je 25 GBit/s zur Verfügung. Nicht alle Drittanbieter nutzen diese direkten Verbindungen und nicht alle sind in der Lage, die Bandbreite vollständig auszunutzen, da IPsec auf den Gateways der CSP auf 1,25 GBit/s limitiert ist.

Eine solche Lösung kann im Prinzip jeder selbst aus Open-Source-Werkzeugen bauen oder auch spezialisierte Images wie den Juniper-vMX-3D-Router dafür nutzen. Auch die virtuellen Firewalls von CheckPoint, F5 und anderen bieten oft IPsec- und Routingoptionen, die das Internet oder einen der physischen Interconnect Anbieter als Transit-LAN nutzen können. Dazu gehört dann allerdings auch der Aufbau der Überwachung, Firewalls und so weiter. Der Kasten „Aviatrix“ stellt exemplarisch ein kommerzielles Produkt vor.

Fazit

Die Netzarchitektur entscheidet über die Performance, die Sicherheit und auch die Kosten. Das ist in der Cloud nicht anders als in On-Premises-Installationen. Eine Verbindung zwischen Standorten, Nutzern und den CSP erfordert immer eine physische Verbindung zu einem Transfernetz. Dies ist bei den virtuellen Optionen in vielen Fällen das allgemeine Internet.

Wer mehr Daten transportiert, wird schnell die OnRamps der CSP nutzen und diese vielleicht auch mit SD-WAN oder den IPsec-Meshes kombinieren. Denn die OnRamps sind wie ein MPLS erst mal unverschlüsselt und auch die Authentifizierung der Gegenstellen dieser Anbindungen obliegt der Verantwortung des RZ-Betreibers und des CSP. Wird aus Versehen ein OnRamp mit dem falschen Port im RZ verbunden, wird es im schlimmsten Fall zu einer Verbindung mit internen Netzen im Intranet oder mit Netzen anderer Kunden kommen. Dann hilft wie früher auch nur eine Verschlüsselung. (avr@ix.de)

Quellen

[1] Markus Stubbing; Soft geleitet; SD-WAN vereinfacht das Routing in verteilten Netzen; c’t 23/2021, S. 128

[2] Benjamin Pfister; Komplettpaket; Kurz erklärt: Secure Access Service Edge (SASE); *iX* 7/2021, S. 104

[3] Weiter Informationen zu Aviatrix: ix.de/zz6b

Christoph Puppe

ist Managing IT Security Architect und Auditteamleiter für ISO 27001 nach Grundschutz bei SVA System Vertrieb Alexander GmbH, Mitautor des Grundschutz-Kompendiums und ehemaliger Penetrationstester.

© Copyright by Heise Medien.
Persönliches PDF für Christoph Puppe aus 99096 Erfurt