WHITEPAPER

Maximale Flexibilität mit der SASE-Lösung von Fortinet

Zusammenfassung

Digitale Innovationen, die Einbindung von Clouds und umfassende Umstellungen auf Homeoffices haben Netzwerke in letzter Zeit grundlegend verändert. Angesichts der zunehmenden Abhängigkeit von cloudbasierten Ressourcen wie SaaS-Anwendungen (Software-as-a-Service) und Daten, die vom Rechenzentrum in Multi-Cloud-Umgebungen verlagert werden, ist ein neuer Ansatz für den sicheren Netzwerk-Zugriff notwendig – insbesondere für die Problematik des „generellen Vertrauensvorschusses" in älteren Netzwerk-Architekturen.

Heutige Unternehmen benötigen einen sofortigen, ununterbrochenen Zugang zu Ressourcen, Daten und geschäftskritischen Anwendungen im Netzwerk und in der Cloud – überall, jederzeit und mit jedem Gerät. Zahlreiche Probleme infolge von digitalen Innovationen (wie z. B. dynamisch wechselnde Netzwerk-Konfigurationen oder eine rasant wachsende Angriffsfläche) führen dazu, dass die Security und Zugriffskontrolle vieler herkömmlicher Sicherheitslösungen für den Schutz von Anwendern und Unternehmen nicht mehr ausreicht.

„Kunden verlangen Einfachheit, Skalierbarkeit, Flexibilität, geringe Latenz und umfassende Konvergenz vom WAN-Edge- und Netzwerk-Security-Markt."[1]

Secure Access Service Edge (SASE) bietet Unternehmen einen neuen strategischen Ansatz, der Netzwerk-Security- und WAN-Funktionen kombiniert. Das Ziel von SASE ist es, die dynamischen Anforderungen heutiger Unternehmen an einen sicheren Zugriff zu unterstützen. Dies steht im Einklang mit der sicherheitsorientierten Netzwerk-Strategie, die Fortinet seit Jahren aktiv entwickelt und konsequent vorantreibt. SASE spielt eine entscheidende Rolle dabei, dass die Security überall bereitgestellt werden kann – vom WAN-Edge bis hin zu den Randbereichen von Clouds, Rechenzentren, Kernnetzwerken sowie auf den Endgeräten einer überwiegend mobilen Remote-Belegschaft.

Was genau bedeutet SASE?

Wie bei jeder neuen Technologiekategorie besteht immer noch eine gewisse Unsicherheit hinsichtlich der genauen Definition einer SASE-Lösung. Handelt es sich dabei ausschließlich um ein cloudbasiertes Angebot? Oder beinhaltet SASE auch physische Lösungen? Und welche Technologien werden für eine SASE-Lösung verwendet?

Während SASE im Allgemeinen als Cloud-Dienst klassifiziert wird, müssen für eine wirkungsvolle SASE-Integration im Netzwerk u. U. physische und cloudbasierte Lösungen gemeinsam verwendet werden. Mehrere Kombinationen sind möglich: SASE-Konnektivität mit Netzwerk-Zugriffskontrollen und Edge-Security-Geräten für Remote-Mitarbeiter, SD-WAN-Geräte (Software-Defined Wide Area Networking) mit umfassender Security-Funktionalität bis hin zur Integration mit Technologien wie WLAN-Controllern oder WLAN Access Points in Niederlassungen.

Zusätzlich zu einem grundlegenden Cloud-Schutz muss eine robuste SASE-Lösung auch Funktionen wie eine Netzwerk-Segmentierung oder Compliance-Anforderungen unterstützen, die die cloudbasierte Security nicht leisten kann, ohne dass der Datenverkehr extra zur Überprüfung in die Cloud übertragen werden muss. Aus diesem Grund bietet Fortinet mit die umfassendsten, flexibelsten SASE-Lösungen, die die Integration und Implementierung von Clouds und physischen Geräten abdecken.

Bei SASE dreht sich alles um den Secure Access

Vom Konzept her soll SASE die von SD-WAN-Anbietern verursachten Sicherheitsprobleme lösen, die bei innovativen Netzwerk-Lösungen keine umfassende Security integrieren. Fortinet hat dieses Problem von Anfang an erkannt und eine vollintegrierte Secure SD-WAN-Lösung mit robusten, integrierten Netzwerk- und Security-Funktionen entwickelt, die auf dem Markt ihresgleichen sucht. Dies alles ist Teil einer Plattform-Strategie aus sicherheitsorientierten Netzwerken und Security Fabric, die wir unseren Kunden seit Jahren anbieten.

Fortinet unterstützt eine vollständig integrierte SASE-Lösung mit der breitesten Palette an physischen und cloudbasierten Security-Lösungen auf dem Markt. Die Grundlage bilden folgende Sicherheitselemente:

- **SD-WAN-Lösung mit umfassenden Funktionen:** Als Herzstück der SASE-Lösung muss das SD-WAN z. B. eine dynamische Pfadauswahl, selbstheilende WAN-Funktionen sowie eine zuverlässige Anwendungs- und Benutzererfahrung für Geschäftsanwendungen bieten.
- **Next Generation Firewall (NGFW) als Gerät oder cloudbasierter FWaaS-Dienst (Firewall-as-a-Service):** SASE muss außerdem umfassende Sicherheitsfunktionen haben, die physische und cloudbasierte Szenarien abdecken. Unternehmen mit einer Homeoffice-Strategie benötigen beispielsweise eine Kombination aus Sicherheit am Netzwerk-Rand und interner Segmentierung –

damit keine durch Gäste oder IoT-Geräte (Internet der Dinge) eingeschleusten Bedrohungen auf zugriffsbeschränkte Ressourcen im Unternehmensnetzwerk überspringen –, kombiniert mit einer cloudbasierten Security für den Zugriff auf online oder in der Cloud bereitgestellte Ressourcen. Mit prozessorgestützter Hardware und einer skalierbaren cloudnativen Sicherheit lässt sich die gleiche hohe Leistung sowie maximale Flexibilität und Sicherheit für das gesamte Unternehmen erreichen.

- **Zero-Trust Network Access (ZTNA)**: Hiermit lassen sich Benutzer und Geräte identifizieren und für Anwendungen authentifizieren. Da ein solcher Zero-Trust-Netzwerkzugang eher eine Strategie als ein Produkt ist, umfasst er mehrere ineinandergreifende Technologien: Die Multi-Faktor-Authentifizierung (MFA) identifiziert alle Benutzer. Auf der physischen Seite umfasst ZTNA ein NAC-Gerät für die Netzwerk-Zugangskontrolle (Network Access Control), die Durchsetzung von Zugriffsrichtlinien und die Integration in die dynamische Netzwerk-Segmentierung, um den Zugriff auf Netzwerk-Ressourcen zu beschränken. Auf der Cloud-Seite unterstützt ZTNA beispielsweise die Mikrosegmentierung einschließlich Überprüfung des Datenverkehrs für eine sichere Ost-West-Kommunikation zwischen Benutzern sowie die ständige Sicherheit von Geräten inner- und außerhalb des Netzwerks. Durch die Kombination von physischen und cloudbasierten ZTNA-Diensten lässt sich ein sicherer Zugriff und die Durchsetzung von Richtlinien gewährleisten – unabhängig davon, ob Geräte und Benutzer On-Premises oder Off-Premises sind.
- **Sicheres Web-Gateway**: Hiermit werden Benutzer und Geräte vor Online-Gefahren geschützt, indem Internet-Security- und Compliance-Richtlinien durchgesetzt werden und bösartiger Internetverkehr herausgefiltert wird. Mit einem Secure Web Gateway lassen sich auch angemessene Internet-Nutzungsrichtlinien konsequent anwenden, um die Compliance sicherzustellen und Datenlecks zu verhindern.
- **CASB**: Mit einem cloudbasierten Dienst erhalten Unternehmen Kontrolle über ihre SaaS-Anwendungen, einschließlich Schutz des Anwendungszugriffs und der Beseitigung von Problemen, die mit einer Schatten-IT einhergehen. Dies muss mit einem On-Premises DLP kombiniert werden, um Datenverluste proaktiv zu verhindern.

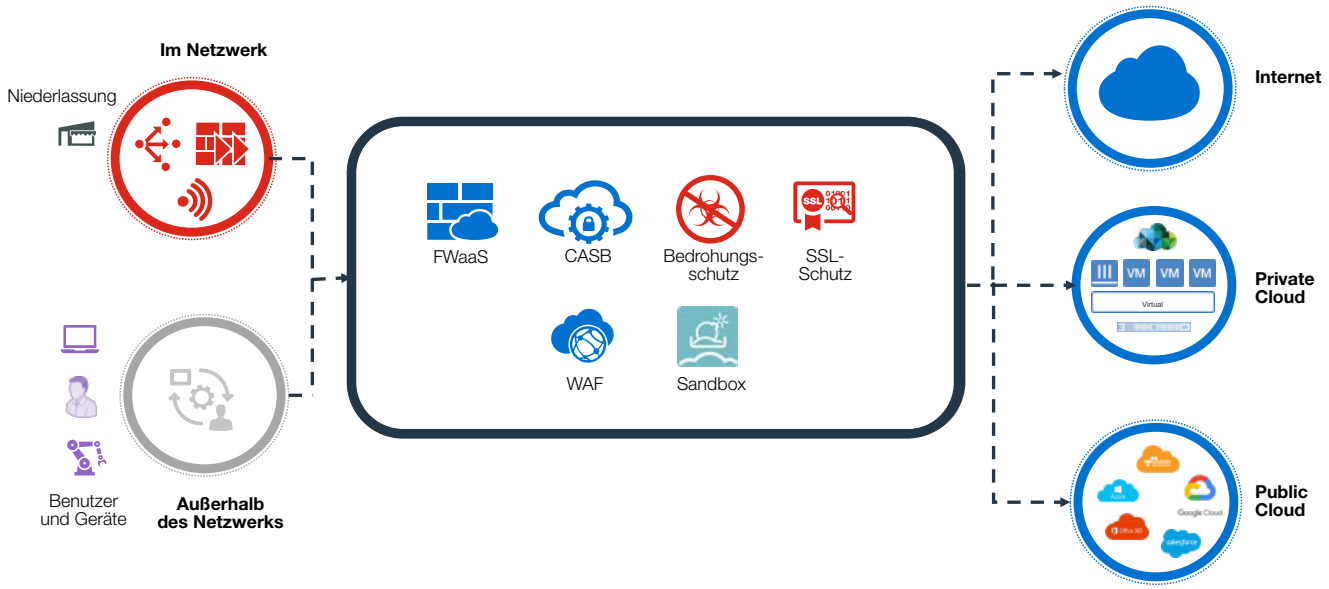

Abbildung 1: SASE-Diagramm

Erweiterung von SASE mit zusätzlichen Technologien

SASE wurde entwickelt, um digitale Innovationen zu verbessern und zu unterstützen. Ohne einen ganzheitlichen SASE-Ansatz laufen Unternehmen jedoch Gefahr, eine weitere isolierte Sicherheitslösung zu schaffen, die getrennt von der übrigen Security-Architektur verwaltet werden muss. Dies kann sowohl die Transparenz als auch die Kontrolle im gesamten Netzwerk stark beeinträchtigen. Fortinet bietet nicht nur die nötigen Kernelemente für eine robuste SASE-Lösung, sondern auch optionale Tools für eine höhere Sicherheit der Anwender und Geräte, die die SASE-Lösung verwenden. Diese Tools ermöglichen zudem die nahtlose Integration der Gesamtlösung in die größere Security Fabric.

Beispielsweise gewährleisten Technologien wie Endpoint Protection (EPP) und Endpoint Detection und Response (EDR) für den Endpunkt-Schutz die Sicherheit der Geräte, die SASE nutzen. Ein intelligentes virtuelles privates Netzwerk (VPN) sorgt für sichere Datenübertragungen und Transaktionen und kommt problemlos mit der Komplexität klar, die bei Verbindungen von Hunderten oder Tausenden Homeoffices oder Remote-Anwendern schnell entsteht. Durch das Hinzufügen sicherer WLAN- und LAN-Controller wird zudem gewährleistet, dass der ein- und ausgehende Netzwerk-Datenverkehr eine zusätzliche Prüfebene erhält.

Natürlich hat jedes Unternehmen andere Anforderungen. Es ergibt jedoch keinen Sinn, lediglich SASE-Kerntechnologien einzusetzen, wenn eine umfassendere Netzwerk- und Security-Lösung letztlich die besseren Geschäftsergebnisse liefert.

Viel Potenzial, aber zu wenige qualifizierte Anbieter

SASE wurde entwickelt, um die Herausforderungen heutiger Unternehmen bei der Zugriffskontrolle und der WAN-Security zu lösen. Das Problem ist jedoch, dass nur sehr wenige Anbieter für die Bereitstellung einer SASE-Komplettlösung qualifiziert sind. Beispielsweise wurden nur wenige Tools – insbesondere die Sicherheitskomponenten – getestet oder zertifiziert. Dies bedeutet, dass Kunden vorher nicht sicher wissen können, ob die Security-Dienste in der Praxis wirklich funktionieren.

Dass sich manche Anbieter selbst in diesem hochspezialisierten Cyber-Security-Markt gegen unabhängige Tests und Validierungen entscheiden, wenn ihre Lösungen Industriestandard erfüllen, ist bereits ein ernstes Problem. Verschärft wird dies aber zusätzlich, wenn SASE-Lösungen von Anbietern mit minimaler oder begrenzter Security-Erfahrung stammen, die schnell „irgendetwas auf den Markt werfen“, um auf den SASE-Zug aufzuspringen.

Der Fortinet-Vorteil

Bei Fortinet werden wir oft nach unserer SASE-Strategie gefragt. Damit SASE gut funktioniert, müssen alle Komponenten als ein einziges integriertes System zusammenarbeiten: Konnektivität, Netzwerk und Security. Für Fortinet ist das nichts Neues. Wir erfüllen die wichtigsten – und weit darüber hinausgehende – SASE-Anforderungen bereits seit Jahren mit unserer integrierten Security-Plattform- und Security-Fabric-Architektur. Das Ergebnis ist eine echte Konvergenz von Netzwerk- und Sicherheitsfunktionen als Teil eines sicherheitsorientierten Netzwerk-Ansatzes, mit dem sich digitale Innovationen noch schneller vorantreiben lassen – ohne Kompromisse bei der Sicherheit. Einige unserer Kunden, die SASE implementieren wollten, haben festgestellt, dass sie mit der leistungsstarken Security Fabric bereits über eine SASE-Lösung verfügen, wenn sie nur ein paar geringfügige Änderungen vornehmen.

Das Ziel von SASE ist die Lösung eines echten Problems. Aber es ist das gleiche Problem, für das Fortinet bereits seit langem Lösungen anbietet.

- Wir waren der erste große Security-Anbieter, der die Sicherheit vollständig in das SD-WAN integriert hat. Wir konnten eine einheitliche Komplettlösung schaffen, weil wir über jahrelange Erfahrung in beiden Bereichen verfügen: Netzwerk und Security.
- Wir sind dann noch einen Schritt weiter gegangen und haben den weltweit ersten SD-WAN-Prozessor entwickelt, der die Netzwerk- und Security-Funktionen beschleunigt. Damit erreichen wir das Leistungsniveau, das die anspruchsvollsten Netzwerk-Umgebungen von heute erfordern.
- Wir sind stolz darauf, dass Fortinet-Security-Tools derzeit die am besten getesteten, validierten und zertifizierten Lösungen der Branche sind.

Das alles bedeutet, dass die Bereitstellung der Art von SASE-Lösung, die Ihr Unternehmen benötigt, bereits Teil unseres Netzwerk- und Security-Ansatzes ist. Diese Lösung können wir zudem mit fortschrittlichen Konnektivitäts- und Sicherheitstechnologien anpassen, damit Ihre SASE-Lösung genau Ihre Anforderungen erfüllt. Die Fortinet Security Fabric kann auch vorhandene On-Premises- oder Cloud-Lösungen von Drittanbietern integrieren und einbinden. All diese Elemente lassen sich mit unserer zentralen Management-Konsole verwalten, um eine umfassende Transparenz und granulare Kontrolle über Ihr gesamtes Netzwerk – einschließlich Ihrer SASE-Umgebung – zu gewährleisten.

Fortinet ist einzigartig positioniert, um eine SASE-Komplettlösung für eine verlässliche, einheitliche Security im gesamten Netzwerk anzubieten – nicht nur am Cloud-Edge oder am WAN-Edge, sondern auch am Randbereich von Rechenzentren, Kernnetzwerken und Endpunkten. Auf diese Weise schaffen wir eine nahtlose Konnektivität, Transparenz und Kontrolle für Ihr Unternehmen.

Wir sind von der jüngsten Marktdynamik rund um SASE begeistert. Denn das bestätigt nicht nur unseren Security-Fabric-Ansatz um ein Weiteres, sondern auch, was wir seit Jahren sagen: Im Zeitalter von Cloud-Konnektivität und digitalen Innovationen müssen Netzwerk und Sicherheit zusammenwachsen. Es gibt kein Zurück zu veralteten, isolierten Architekturen. Mit Fortinet erhalten Sie Lösungen, die für das SASE-Zeitalter entwickelt wurden – und darüber hinaus.

[1] Frank Marsala: „The Future of Network Security Is in the Cloud“. Gartner, 13. September 2019.

FORTINET®

www.fortinet.com/de

18. Februar 2021, 18:03 Uhr

742476-0-0-DE