# Von SD-WAN bis SASE: Anforderungen an eine sicherheitsorientierte Netzwerk-Strategie

**Digitale Innovationen zwingen alle Unternehmen, Netzwerke neu zu gestalten sowie Mitarbeitern und Kunden eine bessere Nutzererfahrung zu bieten. Der Perimeter – einst ein eng gefasster Zugangspunkt für den Netzwerk-Rand – erstreckt sich jetzt über die gesamte IT-Infrastruktur. Dadurch entstehen neue Anforderungen für die Randbereiche von Rechenzentren, WANs (Wide Area Network), LANs (Local Area Network) und Clouds. Zudem hat die Corona-Pandemie gezeigt, wie unverzichtbar Business-Continuity-Pläne sind, die einen flexiblen, umfassenden Fernzugriff jederzeit und überall gewährleisten.**

Zugleich steigen Raffinesse und Anzahl der Sicherheitsbedrohungen: Über ein Drittel der Datenschutzverletzungen im Jahr 2020 war das Ergebnis von Social Engineering[1] – nur einer von vielen Gründen, warum eine bessere Security sowie die Neugestaltung von Netzwerken für jedes Unternehmen von entscheidender Bedeutung sind.

Eine **sicherheitsorientierte Netzwerk-Strategie** beschleunigt die Konvergenz von Netzwerk und Security in der gesamten verbundenen Umgebung für alle Randbereiche und Benutzer – vom Netzwerk-Kern über Niederlassungen bis hin zur Cloud. Mit einer solchen Strategie sind Unternehmen in der Lage, die hochdynamischen Umgebungen von heute effektiv zu verteidigen und gleichzeitig Mitarbeitern und Kunden ausgezeichnete Nutzererfahrungen zu bieten.

Wird die Security von Grund auf integriert, können Netzwerke problemlos weiterentwickelt, erweitert und für digitale Innovationen angepasst werden. So lassen sich dringend benötigte moderne Netzwerke schaffen, die Next-Generation-Technologien wie Hyperscaling, Multicloud, 5G und andere sich schnell entwickelnde Trends unterstützen. Durch diese Konvergenz von Netzwerk und Security erhalten Unternehmen eine flexible Sicherheit, die jederzeit und überall gegeben ist.

**Eine sicherheitsorientierte Netzwerk-Strategie beschleunigt die Konvergenz von Netzwerk und Security in der gesamten verbundenen Umgebung für alle Randbereiche und Benutzer – vom Netzwerk-Kern über Niederlassungen bis hin zur Cloud.**

## Zentrale Elemente einer sicherheitsorientierten Netzwerk-Strategie

Eine sicherheitsorientierte Netzwerk-Strategie erfüllt insgesamt drei Anforderungen:

- **Management externer und interner Risiken für Benutzer im Netzwerk**
- **Bereitstellung einer flexiblen, cloudnativen Security für Benutzer außerhalb des Netzwerks**
- **Verbesserung der Nutzererfahrung bei gleichzeitiger Senkung der WAN-Kosten**

Der erste Schritt zum Erreichen eines sicherheitsorientierten Netzwerks besteht in der Implementierung von **Security-Hardware mit speziellen Sicherheitsprozessoren** oder ASICs. So lässt sich ein schneller Netzwerk- und Security-Betrieb sowie die **Konsolidierung aller Sicherheitsfunktionen** in Lösungen wie Netzwerk-Firewalls erreichen, ohne die Funktionalität oder Leistung zu beeinträchtigen. Die erforderlichen Anwendungsfälle umfassen ein sicheres SD-WAN (Software-Defined Wide Area Networking), NGFW (Next Generation Firewall), IPS (Intrusion Prevention System), SSL-Inspektion (Secure Sockets Layer), Application Control, Web-Filter, Antivirus, Anti-Malware, Sandbox sowie eine schnellere Segmentierung. (Letzteres ist besonders wichtig für eine sicherheitsorientierte Netzwerk-Strategie, da viele Firewalls nicht genug Rechenleistung für eine dynamische interne Segmentierung bieten.)

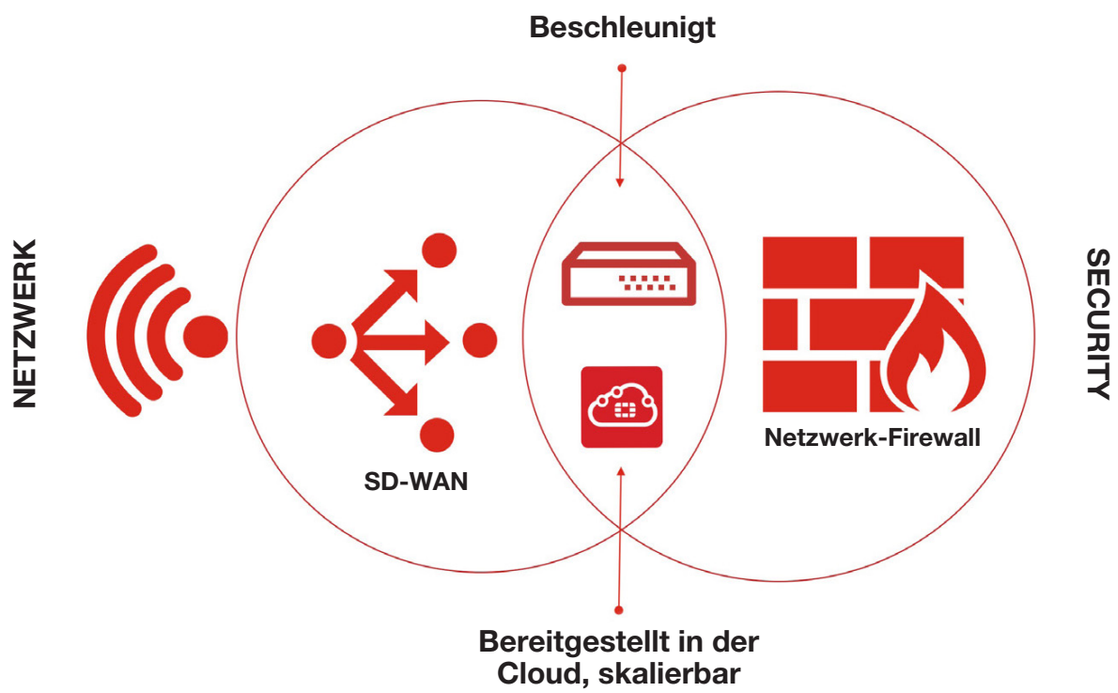
Mit einer **speziellen Cloud-Architektur** lässt sich die Netzwerk-Security-Konvergenz schaffen, die für eine Cloud-First-Strategie oder flexiblere Implementierungen notwendig ist.

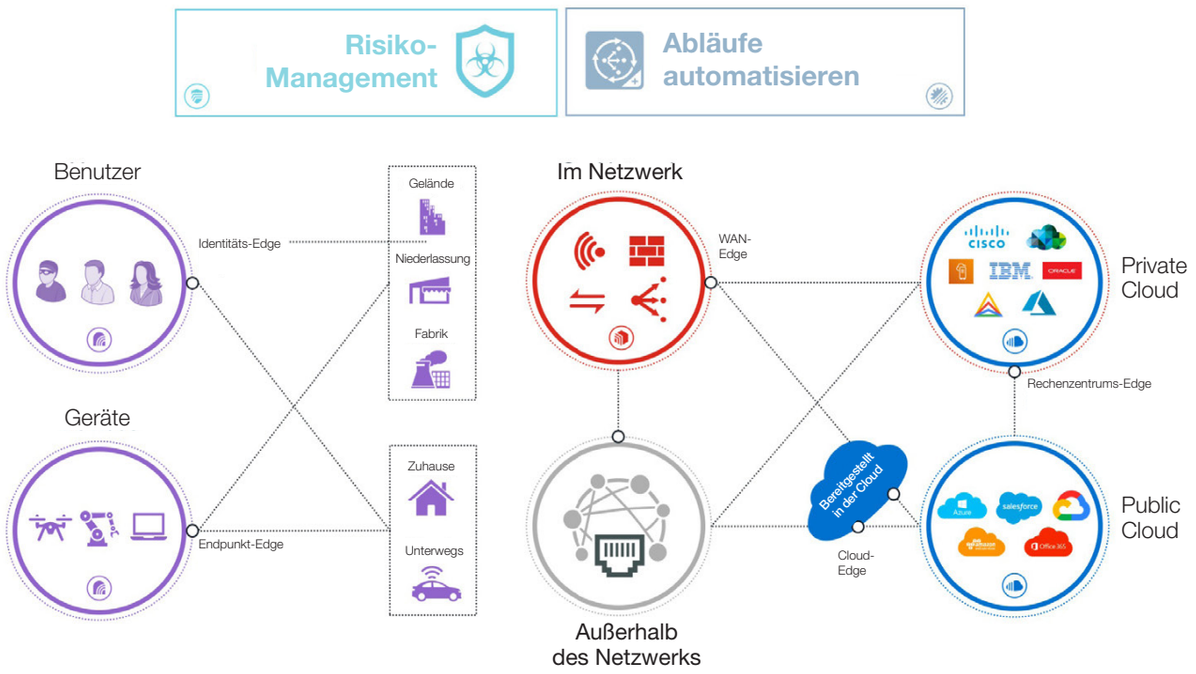
Netzwerk-Firewall-Lösungen müssen zudem künftig **hybride und Hyperscale-Rechenzentren sowie die Leistungsanforderungen von 5G unterstützen** können. Neue High-Performance-Innovationen – wie die schnelle Übertragung gewaltiger Datenmengen (so genannter „Elephant Flows“), Edge Computing, Schutz von HDTV und anderem Rich-Media-Verkehr, 5G-Netze und die dynamische Kern-Segmentierung – verlangen eine extrem leistungsstarke Next Generation Firewall. Die meisten NGFWs wurden jedoch nicht für solch hohe Anforderungen entwickelt und müssen zu enormen Mehrkosten aufgerüstet werden – sofern dies möglich ist.

Eine sicherheitsorientierte Netzwerk-Strategie setzt daher auf eine WAN-Edge-Transformation mit einem SD-WAN der Enterprise-Klasse, das vollständig in ein NGFW-Gerät integriert ist. Dank dieser Integration ist das **SD-WAN** wirklich sicher – im Gegensatz zu einer SD-WAN-Technologie, bei der die Security nachträglich ergänzt wird. Ein robuster Ansatz für ein SD-WAN umfasst auch KI-gestützte Prognose-Funktionen (Predictive Analytics), eine intuitive Orchestrierung und die Fähigkeit zur Selbstheilung.

Sicherheitsfunktionen müssen zudem so umfassend integriert werden, dass auch verkabelte und drahtlose Randbereiche geschützt sind. Nur so lässt sich eine einheitliche Security konsequent am LAN-Edge durchsetzen. Dies sind die **Voraussetzungen für integritätsbewusste, reaktionsschnelle Netzwerke**, die die Security bis zu Access- und Netzwerk-Edges erweitern.

Alle diese Randbereiche erfordern zudem ein **zentrales Management**, um die Komplexität zu verringern und Automatisierung zu ermöglichen – zwei Faktoren, die Netzwerke agiler machen.






## SASE – die richtige Grundlage für den Schutz des Cloud-Edge

Seit 2020 fällt im Zusammenhang mit sicherheitsorientierten Netzwerken immer wieder der Begriff SASE (Secure Access Service Edge). Dabei handelt es sich um ein neues Enterprise-Framework, das die Netzwerk-Security mit WAN-Funktionen kombiniert. SASE erfüllt damit – ganz im Sinne einer sicherheitsorientierten Netzwerk-Strategie – die dynamischen, sicheren Zugriffsanforderungen heutiger Unternehmen. Daher spielt SASE eine zentrale Rolle bei einer zuverlässigen Security-Implementierung am Cloud-Edge sowie beim Schutz von mobilen und Remote-Benutzern.

Obwohl SASE generell dem Cloud-Computing zugerechnet wird, kann die SASE-Integration ins Netzwerk unter gewissen Umständen auch eine physisch-cloudbasierte Lösung erfordern. Das kann z. B. eine Kombination aus SASE-Konnektivität mit Netzwerk-Zugriffskontrollen und Edge-Security-Geräten sein, um ein physisches SD-WAN-Gerät mit umfassender Sicherheitsfunktionalität zu unterstützen. Manchmal ist sogar eine Integration in Technologien wie WLAN-Controller oder WLAN Access Points in Niederlassungen notwendig. Entscheidend ist, dass Unternehmen mit SASE **Remote-Anwender** mit einer immer verfügbaren Security **schützen** können – unabhängig von deren Standort. Das verbessert die Nutzererfahrung und die Produktivität, weil der Cloud-Edge auf eine optimale Pfadwahl und geringe Latenzzeiten abgestimmt ist.

Ein SASE-Angebot und eine umfassende, sicherheitsorientierte Netzwerk-Strategie sind nicht dasselbe. Zusätzlich zu den grundlegenden cloudbasierten Sicherheitsfunktionen, die in der SASE-Standarddefinition beschrieben sind,[2] muss eine robuste SASE-Lösung auch Dinge wie eine Netzwerk-Segmentierung und Compliance-Anforderungen unterstützen. Letzteres kann eine cloudbasierte Security nicht bieten, ohne dass der Datenverkehr extra zur Überprüfung in die Cloud geschickt werden muss.

Mit SASE als Grundlage einer umfassenden, sicherheitsorientierten Netzwerk-Strategie erhalten Unternehmen dagegen genau die Art von Security und Leistung, die überall notwendig ist.

[1] „2020 Data Breach Investigations Report“. Verizon, Mai 2020.

[2] „The Future of Network Security Is in the Cloud“. Gartner, 13. September 2019.

FORTINET

www.fortinet.com/de



19. Februar 2021, 10:06 Uhr

745599-0-1-DE