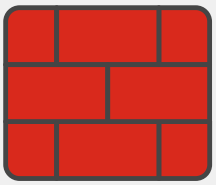
SECURITY INSIGHTS

# Integrierte Netzwerk-Firewalls: Unverzichtbar für dezentrale Unternehmen

## Was ist eine integrierte Netzwerk-Firewall-Lösung?

Moderne Unternehmen sind heutzutage hochgradig vernetzt. Alles ist miteinander verbunden – von Rechenzentren und Unternehmensgeländen mit Campus-Netzwerken bis hin zu Niederlassungen und der Cloud. Dennoch fehlt vielen Unternehmen eine einheitliche Sicherheit und Transparenz über die unterschiedlichen Segmente ihrer verteilten, weitläufigen Netzwerke. Dazu kommt, dass der Datenverkehr im Netzwerk (auch als „Ost-West-Verkehr“ oder „horizontaler Traffic“ bezeichnet) durch diese starke Vernetzung zugenommen hat. Für Cyberkriminelle ist diese Mischung aus mangelnder Transparenz, umfassender Vernetzung und einem hohen Ost-West-Verkehrsaufkommen ideal: Sind Angreifer erst einmal in das Unternehmensnetzwerk eingedrungen, können sie sich ungehindert quer darin bewegen. Diese Gefährdungssituation lässt sich am effektivsten lösen, wenn in jedem Teil des Netzwerks die gleiche hohe Sicherheit herrscht und für verschiedene IT-Bereiche des Unternehmens eine zentrale Bedrohungskorrelation sowie ein koordinierter Schutz bereitgestellt werden. In der Praxis hat sich allerdings gezeigt, dass die Komplexität und Unterschiede zwischen unterschiedlichen Netzwerk-Ökosystemen die Umsetzung einer solchen einheitlichen Sicherheit und Transparenz erschweren.



Fortinet wird seit 13 Jahren in Folge im Gartner® Magic Quadrant™ für Netzwerk-Firewalls als Leader eingestuft und hat im jüngsten Gartner-Bericht für seine Umsetzungsfähigkeit und Visionskraft die beste Bewertung in der Kategorie „Ability to Execute“ erhalten.[1]

Wenn Sie überall in Ihrem Netzwerk kritische NGFW-Funktionen mit einem einheitlichen Remote-Management bereitstellen möchten, empfiehlt sich die Implementierung von Netzwerk-Firewalls. Ideal ist, wenn zudem alle Elemente einer Sicherheitslösung das gleiche Betriebssystem verwenden. Denn dann, erhält alles den gleichen starken Schutz – vom Campus-Netzwerk bis hin zum Rechenzentrum, Clouds, FWaaS und SASE-Umgebungen. So wird eine einzige, integrierte Plattform geschaffen, die sich für die heutigen dynamischen, verteilten Netzwerke erweitern, skalieren und anpassen lässt. Mit einer einheitlichen Managementkonsole wird eine koordinierte Security über Wenn Sie überall in Ihrem Netzwerk kritische NGFW-Funktionen mit einem einheitlichen Remote-Management bereitstellen möchten, empfiehlt sich die Implementierung von Netzwerk-Firewalls. Ideal ist, wenn zudem alle Elemente einer Sicherheitslösung das gleiche Betriebssystem verwenden. Denn dann IT-Bereiche hinweg erreicht, die von Unternehmensstandorten, Public und Private Clouds bis hin zu Remote-Arbeitsplätzen alles wirksam schützt. Dank diesem integrierten Ansatz können IT-Teams die Bedrohungserkennung und Reaktionsmaßnahmen automatisieren, Konfigurationen koordinieren und Richtlinien durchsetzen, ohne Zeit mit manuellen Aufgaben zu verschwenden – ein wichtiger Punkt angesichts des eklatanten Fachkräftemangels im Cybersecurity-Bereich.

## Integrierte Netzwerk-Firewalls sind keine Option, sondern ein Muss

Netzwerk-Firewalls sind unverzichtbar, um Netzwerke vor unbefugtem Zugriff und bösartigen Angriffen zu schützen. Sie fungieren wie ein digitaler „Wachschutz mit Einlasskontrolle“: Als Gatekeeper überwachen und kontrollieren diese integrierten Firewalls den gesamten Netzwerkverkehr, um einen unbefugten Zugriff, Datenverletzungen und andere Sicherheitsbedrohungen zu verhindern. Solche Lösungen wurden zur Bewältigung von vier kritischen Herausforderungen entwickelt, denen sich IT-Teams heute gegenübersehen:

### 1. IT-Komplexität

Da bei vielen NGFWs wichtige Funktionen fehlen, bleibt IT-Teams nichts anderes übrig, als separate Security-Lösungen für Unternehmensstandorte, Public Clouds, Private Clouds und Remote-Arbeitsplätze einzusetzen. Das führt jedoch zu einem operativen Chaos mit Problemen wie Fehlkonfigurationen, wodurch das Netzwerk anfällig werden kann.

### 2. Lücken bei der Cybersecurity-Kompetenz

Isolierte Einzellösungen verschlimmern nicht nur die Komplexität, sondern setzen das Unternehmen einem zusätzlichen Risiko aus, da ihre Inbetriebnahme in der Regel lange dauert. Mehrere Einzellösungen bedeuten, dass Ihre Cybersecurity-Experten aus der IT mehr Zeit darin investieren müssen, sich mit den neuen Funktionen und Dashboards vertraut zu machen. Dies stellt ein noch größeres Risiko für Unternehmen dar angesichts der Tatsache, dass viele Cybersecurity-Stellen wegen des weltweiten Fachkräftemangels derzeit unbesetzt bleiben und personell begrenzte Security-Teams ohnehin schon an der Belastungsgrenze arbeiten.

### 3. Anstieg hochkomplexer Bedrohungen

Neben der IT-Komplexität und fehlenden Cybersecurity-Experten spricht auch die weltweit wachsende Gefahr durch hochkomplexe Cyberbedrohungen für integrierte Netzwerk-Firewalls. Hochkomplexe, ausgefeilte Cyberbedrohungen nehmen in rasantem Tempo zu, da viele Angreifer heute mit künstlicher Intelligenz (KI) arbeiten. Mit Angriffsvektoren, die vom Internet über Anwendungen, Content und Geräte reichen, haben diese dynamischen, immer schwerer zu erkennenden Bedrohungen verheerende Auswirkungen auf Unternehmen. Ransomware ist beispielsweise weiterhin ein erheblicher Störfaktor in allen Branchen und Sektoren, einschließlich bei Betriebstechnologie (OT), staatlichen Stellen auf Landes-, Regional- und Kommunalebene, Fertigungsunternehmen oder Einrichtungen des Gesundheitswesens.

### 4. Rolle von KI/ML und Bedrohungsinformationen

Komplexität, die Gefahr, Sicherheitslücken bei manuellen Abläufen zu übersehen, und eine sich verschärfende Bedrohungslage erfordern einen koordinierten Schutz. Es genügt nicht, wenn Ihre Firewall verschiedene Netzwerkbereiche abdeckt. Sie muss außerdem künstliche Intelligenz (KI) und maschinelles Lernen (ML) einsetzen – zwei Funktionen, die zum Schutz vor bekannten und unbekannten Bedrohungen unverzichtbar sind. Mit einer KI/ML-gestützten Security können Netzwerk-Firewalls nämlich nicht nur Anwendungen, Web-URLs, Benutzer, Geräte, Malware und vieles mehr identifizieren und klassifizieren, sondern auch die Richtliniendurchsetzung für unterschiedlichste Bereiche automatisieren. KI/ML ist quasi das Herzstück der Netzwerk-Firewall-Automatisierung und kann den manuellen Aufwand beim Schutz der Unternehmens-IT erheblich reduzieren.

## Worauf Sie bei einer Netzwerk-Firewall-Lösung für hybride Umgebungen achten sollten

### Zentrales, einheitliches Management

Die wichtigsten Vorteile von Netzwerk-Firewalls sind die Bedrohungserkennung, das Richtlinienmanagement und die automatische Koordinierung der Bedrohungsabwehr im gesamten Netzwerk mit allen Ihnen zur Verfügung stehenden Tools.

Ein einheitliches Management koordiniert und vereinheitlicht Ihre unterschiedlichen Sicherheitsbereiche zu einer einzigen unternehmenstauglichen IT-Security. Das Ergebnis ist ein unkomplizierter, automatisierter Schutz, der alle Unternehmensstandorte bis hin zur Cloud und zu Remote-Mitarbeitern sichert. Wichtig dabei: Da jedes Unternehmen andere Anforderungen an das Management unterschiedlicher Netzwerk-Firewalls hat, müssen sämtliche Formfaktoren unterstützt werden – einschließlich Appliances, VMs, SaaS und Managed Firewall Services.

Ihre Netzwerk-Firewall sollte außerdem Ihre Teams vom Network Operations Center (NOC) und Security Operations Center (SOC) über eine einzige „Schaltzentrale“ zusammenbringen, die das Management und Monitoring Ihrer gesamten Angriffsfläche ermöglicht.

### Appliances mit ASICs

Jede Umgebung in Ihrem Netzwerk hat besondere Sicherheitsanforderungen. Unternehmensstandorte benötigen Appliances, die Security-Funktionen skalieren können und einen einheitlichen Schutz bieten, ohne die Benutzererfahrung zu beeinträchtigen.

Angesichts der hohen Performance-Anforderungen heutiger Unternehmen sind Appliances sinnvoll, die mit, leistungsstarken ASICs arbeiten. Solche Spezial-Chips beschleunigen wichtige Security-Dienste enorm: Eine Security Appliance mit eigens entwickelten ASICs übernimmt z. B. rechenintensive Funktionen wie den Firewall-Schutz, VPN, IPS, die SSL-Inspektion oder sogar eine Deep Packet Inspection (DPI), ohne das Netzwerk auszubremsen. Verglichen mit Standardprozessoren können solche speziellen Security-ASICS die Leistung von Sicherheitsfunktionen erheblich steigern.

### Cloudnative Firewall

Cloudnative Firewalls schützen die Workloads von Public-Cloud-Anwendungen, die in IaaS-Umgebungen als Infrastructure-as-Code bereitgestellt werden. Eine cloudnative Netzwerk-Firewall für Ihre Cloud-Umgebung entlastet Ihr Netzwerk-Security-Team in mehrfacher Hinsicht: Sie erhalten nicht nur umfassende Transparenz über das Netzwerk, sondern es entfallen auch Aufgaben wie die Konfiguration, Bereitstellung und Wartung der Firewall-Softwareinfrastruktur. Diese Arbeitserleichterung hat den Vorteil, dass Security-Teams sich intensiver auf das Richtlinienmanagement konzentrieren können.

### Virtuelle Firewall

Virtuelle Firewalls werden häufig zum Schutz virtualisierter Umgebungen in softwaredefinierten Rechenzentren und Multi-Cloud-Umgebungen eingesetzt. Da es sich um die kostengünstigste und portabelste Lösung handelt, können IT-Mitarbeiter eine virtuelle Firewall schnell von Cloud zu Cloud verschieben. Als Teil einer Netzwerk-Firewall-Lösung lässt sich mit virtuellen Firewalls ein umfassendes Security-Ökosystem für Ihr softwaredefiniertes Rechenzentrum mit unterschiedlichsten Cybersecurity-Diensten aufbauen, die über ein Stateful Firewalling hinausgehen. Das unterstützt Sie bei der Konsolidierung und schützt gleichzeitig Ihre Umgebung vor hochkomplexen, dynamischen Bedrohungen.

### Firewall-as-a-Service (FWaaS)

FWaaS bezeichnet eine Firewall-Lösung, die als cloudbasierter Dienst bereitgestellt wird. Dadurch können Unternehmen ihre IT-Infrastruktur vereinfachen und skalieren. In vielerlei Hinsicht ähnelt eine FWaaS-Lösung der Hardware-Firewall, die Sie On-Premises einsetzen. So bietet FWaaS das gesamte Spektrum an Next-Gen-Firewall-Funktionen, wie Web-Filter, erweiterter Bedrohungsschutz, IPS oder DNS-Security. Wird eine Netzwerk-Firewall als FWaaS-Lösung bereitgestellt, profitieren Sie noch stärker, da sich diese umfassende Funktionalität dann auf Benutzer und Geräte überall im Unternehmensnetzwerk erweitern lässt. Sie erhalten damit eine nahezu sofortige Skalierbarkeit mit zentraler Steuerung.

### Ein einziges Betriebssystem

Die rasante Erweiterung von Netzwerkrändern hat die Komplexität durch zu viele Einzellösungen und verschiedene Anbieter verschlimmert. Die Folge: Isolierte Lösungen können keine Informationen austauschen und nicht zusammenarbeiten, was einheitliche Sicherheitsrichtlinien, eine durchgängige Transparenz und Prozessautomatisierungen unmöglich macht. Infolgedessen bringt die Wartung und Überwachung der Fülle an Hybrid-, Hardware-, Software- und X-as-a-Service-Lösungen mittlerweile die meisten Security-Teams an die Belastungsgrenze oder erweist sich als unlösbare Aufgabe.

Ein einziges Betriebssystem ist ideal, wenn Sie Komplexität abbauen wollen, weil damit zahlreiche Technologien und Anwendungsfälle in einem einzigen, vereinfachten Richtlinien- und Management-Framework konsolidiert werden. Frontend-Prozesse werden mit einer zentralen Management-Konsole vereinheitlicht und ein einziges Betriebssystem für Appliances, virtuelle Firewalls, cloudnative Firewalls und FWaaS-Agenten gewährleistet die Backend-Interoperabilität.

## Vorteile von integrierten Netzwerk-Firewalls

Integrierte Netzwerk-Firewalls bringen enorme Vorteile für die Unternehmens-IT. Dazu gehören mehr operative Effizienz, einfachere Cybersecurity-Operations, ein geringeres Risiko für das gesamte Unternehmen, ein robuster Schutz vor bekannten und unbekannten Cyberbedrohungen, KI/ML-gestützte Automatisierung und Koordination sowie niedrigere Gesamtbetriebskosten. Zugleich erhalten Sie damit eine Lösung, die den Mangel an Cybersecurity-Experten in Ihren Teams auffängt.

[1] „A Leader Positioned Highest in Ability to Execute". Fortinet, abgerufen am 13. September 2024.





20. November 2024 14:04 Uhr / 2133550-A-0-DE