FORTINET

Für Hacker kein Zutritt: So sichern Sie alle Edges

Inhalt

Kurzfassung

Moderne Nutzer benötigen ein modernes Netzwerk, das ihnen über jedes Gerät und an jedem Standort Zugriff auf sämtliche Ressourcen bietet. Zugleich steigen die Konnektivitätsanforderungen von Rechenzentren und Campusnetzwerken, die als Grundpfeiler hybrider IT-Architekturen eng mit Filialinfrastrukturen, privaten und öffentlichen Multi-Cloud-Netzwerken, den privaten Umgebungen von Telearbeitern und cloudbasierten SaaS-Lösungen verzahnt sein müssen. Infolgedessen stehen Security-Teams in aller Welt in der Pflicht, die verteilten, hochgradig dynamischen Netzwerkumgebungen ihrer Unternehmen lückenlos zu überwachen und sämtliche Nutzer und Geräte beim Zugriff auf Daten, Anwendungen und Workloads effektiv zu sichern und zu kontrollieren. Wenn Sie hier nachlässig sind, eröffnen Sie Cyberkriminellen bisher ungekannte Möglichkeiten zur Infiltration Ihres Netzwerks über Ihre Netzwerkränder – mit potenziell gravierenden Konsequenzen.

Dabei erweist es sich als erheblicher Nachteil, dass ältere Firewalls und andere konventionelle Security-Maßnahmen nicht für diese Anforderungen ausgelegt sind. Diese Lösungen wurden ursprünglich als statische Kontrollpunkte für Netzwerke mit hochgradig vorhersehbaren Workflows und Datenströmen entwickelt. Doch diese Zeiten sind längst vorbei. Die aktuellen Herausforderungen verlangen nach einer Hybrid Mesh Firewall (HMF). Mit einer solchen Lösung lassen sich Next-Generation-Firewalls in allen Formfaktoren standortübergreifend integrieren und zentral verwalten. Eine koordinierte Bedrohungsabwehr wird möglich. Außerdem können Sie Ressourcen und Nutzer an beliebigen Standorten schützen, die Kapazitäten verteilter Systeme konsolidieren, Management-Prozesse vereinfachen, Abläufe automatisieren und Ihre Services und Bandbreite dynamisch an immer neue geschäftliche Anforderungen anpassen.

Neue Herausforderungen

Obwohl das Rechenzentrum nach wie vor unverzichtbar ist, dient es nicht länger als zentrale Hosting-Plattform für Unternehmensanwendungen. Denn moderne Infrastrukturen unterstützen standortunabhängige Bereitstellungsmodelle. Das erschwert die lückenlose Verfolgung und Sicherung von Transaktionen, zumal immer mehr Workflows diverse Umgebungen und Anwendungen umfassen und sich die Quell- und Zielsysteme der von ihnen generierten Datenströme mehrfach ändern können.

Außerdem geraten konventionelle Firewalls im Zuge der fortschreitenden Umstellung auf 5G zunehmend an ihre Grenzen. Erschwerend kommt hinzu, dass mittlerweile mehr als 95 % des gesamten Datenverkehrs verschlüsselt sind.[1] Die Übertragung dieses Traffics erfolgt schwerpunktmäßig über SSL/TLS-Tunnel, die vor allem bei der Sicherung von Remote-Zugriffen und Transaktionen zum Einsatz kommen. Solche Verschlüsselungsmechanismen bieten Cyberkriminellen die Möglichkeit, schädliche Aktivitäten wie den Diebstahl von Unternehmensdaten oder die Einschleusung von Ransomware zu tarnen. Dabei machen sich Angreifer die Tatsache zunutze, dass die meisten Firewalls nicht in der Lage sind, verschlüsselte Daten ohne gravierende Auswirkungen auf die Netzwerkleistung und Nutzererfahrung zu entschlüsseln und zu überprüfen. Hackergruppen wissen genau, dass das Gros des verschlüsselten Traffics – insbesondere bei hohen Übertragungsgeschwindigkeiten – nicht kontrolliert wird.

Zugleich ergeben sich neue Sicherheitsanforderungen aus der flächendeckenden Umstellung auf Multi-Cloud-Umgebungen und hybride Arbeitsmodelle: Einerseits erweist sich die Cloud als ideales Fundament für die flexible Anwendungsbereitstellung, die bedarfsgerechte Skalierung wichtiger Funktionen und die Einrichtung neuer Zugriffsoptionen für Telearbeiter. Andererseits müssen zahlreiche geschäftskritische Anwendungen weiterhin im unternehmenseigenen Rechenzentrum gehostet werden, weil sie beispielsweise strengen Compliance- und Datenschutzanforderungen unterliegen, geistiges Eigentum beinhalten oder sensible Daten speichern. Dieser Spagat lässt sich nur mithilfe von leistungsstarken Datenverbindungen zwischen Nutzern und dem Rechenzentrum, zwischen dem Rechenzentrum und der Cloud, zwischen Nutzern und der Cloud sowie zwischen verschiedenen Rechenzentren bewältigen. Allerdings sind die meisten konventionellen Firewalls nicht für solche Hybrid-Infrastrukturen ausgelegt.

Um hier Abhilfe zu schaffen, richten die Verantwortlichen in vielen Unternehmen komplexe Behelfslösungen zur Verknüpfung der voneinander isolierten Umgebungen ein. Dies beeinträchtigt wiederum den Betrieb von Geräten, Servern, Switches, Routern, Firewalls, Loadbalancern und anderen Netzwerkkomponenten, die eigentlich für einen reibungslosen Datenaustausch zwischen Systemen und Anwendungen sorgen sollen. Außerdem bremst das rasante Wachstum der Zahl der Geräte und der übertragenen Datenvolumen die Management-, Monitoring- und Troubleshooting-Prozesse im Unternehmen aus.

Obwohl das Rechenzentrum weiterhin unverzichtbar ist, dient es nicht länger als zentrale Hosting-Plattform für Unternehmensanwendungen. Denn moderne Infrastrukturen unterstützen standortunabhängige Bereitstellungsmodelle.

Neue Lösungen

Betrieb und Sicherung hybrider Architekturen erfordern zum einen zentrale Monitoring-Prozesse, die das gesamte verteilte Netzwerk abdecken und Informationen über alle Nutzer und Geräte im Netzwerk sowie die von ihnen genutzten Anwendungen und Ressourcen erfassen. Zum anderen müssen Verhaltensanomalien und schädliche Aktivitäten in sämtlichen Umgebungen identifiziert werden können. Eine weitere Voraussetzung sind schnelle, koordinierte Abwehrmaßnahmen unter Einbeziehung sämtlicher Sicherheitssysteme. Um diese vielfältigen Herausforderungen zu meistern und expandierende Netzwerkee mit den zahlreichen Netzwerkrändern, den sogenannten Edges, im Griff zu behalten, haben viele Unternehmen mit der Implementierung von unterschiedlichen SASE- (Secure Access Service Edge), SD-WAN- (Software-Defined Wide Area Network) und ZTNA-Lösungen (Zero-Trust Network Access) begonnen. Diese Herangehensweise erhöht die Komplexität, behindert die unternehmensweite Überwachung, beeinträchtigt die Nutzererfahrung und erschwert eine effektive Reaktion auf akute Angriffe.

Zielführend ist dagegen ein auf Next-Generation-Firewalls (NGFW) basierender Ansatz, der die Funktionen vorhandener Sicherheitssysteme zusammenführt und auf diese Weise eine unternehmensweite Infrastruktur für kontextsensible, koordinierte Netzwerksicherheit schafft. So kombiniert etwa eine HMF-Lösung lokale und cloudnative Lösungen mit einer einheitlichen Verwaltungskomponente. Damit lassen sich die Abwehrmechanismen sämtlicher IT-Umgebungen aufeinander abstimmten – vom Hauptsitz des Unternehmens über Filial- und Campusinfrastrukturen bis hin zu Rechenzentren, öffentlichen und privaten Clouds sowie den Heimnetzwerken von Telearbeitern. Und weil ein HMF-Deployment von Haus aus interoperabel ist, kann es Betriebsprozesse straffen, Compliance-Vorgaben umsetzen, die Komplexität reduzieren und Effizienzsteigerungen durch Automatisierung erzielen. Dabei spielt es keine Rolle, ob Ihr Unternehmen nur On-Premises-Firewalls, ausschließlich Cloud-Firewalls oder eine Kombination aus beiden nutzt. In all diesen Fällen profitieren Sie von zentralisierten, einheitlichen Management-Prozessen für sämtliche Firewall-Deployments.

Zudem sind sich die Einsatzszenarien für Campusnetzwerke, Rechenzentren, Multi-Cloud-Umgebungen, Filialinfrastrukturen und Heimnetzwerke bemerkenswert ähnlich, sodass Sie überall für das gewünschte Maß an Sicherheit sorgen können. Die Umsetzung erfordert lediglich die Implementierung dreier grundlegender Funktionen – für Sicherheit, Konvergenz und Skalierbarkeit. Zusammengenommen bilden diese drei Konzepte eine ideale Grundlage für die Implementierung einer auf Ihre geschäftlichen Ziele ausgerichteten Strategie für eine nahtlose User Experience und effektiven Schutz.

Sicherheit

Ganz ohne Zweifel besteht Ihr wichtigstes Ziel darin, das Netzwerk vor sämtlichen Bedrohungen zu schützen. Doch falls dies einmal fehlschlägt, kommt es im nächsten Schritt darauf an, etwaige Störungen des Geschäftsbetriebs zu minimieren und möglichst schnell zu beheben. Hierfür muss Ihre NGFW erstens den gesamten Lebenszyklus sämtlicher Anwendungen abdecken und mit modernen Tools für beschleunigte App-Zugriffe kompatibel sein. Zweitens sollte sie über Webfilter mit leistungsstarken Funktionen zur Bilderkennung und Inhaltsanalyse verfügen und so für die Einhaltung von Nutzerrichtlinien und Compliance-Vorgaben sorgen.

Drittens benötigt Ihre NGFW-Lösung erweiterte Sicherheitsfunktionen zur Abwehr von bekannten und unbekannten Angriffen sowie ein integriertes Intrusion-Prevention-System (IPS) und Malwareschutz. Voraussetzung hierfür ist unter anderem, dass Bedrohungsdaten aus ergänzenden Produkten wie E-Mail-Security- und Sandboxing-Tools zur Aufdeckung und Blockierung der neuesten Bedrohungen genutzt werden.

Des Weiteren kommt es entscheidend auf ein hohes Maß an Interoperabilität mit EDR-Lösungen (Endpoint Detection and Response), Web Application Firewalls (WAF) und anderen Sicherheitssystemen an. Denn erst die Integration der nativen

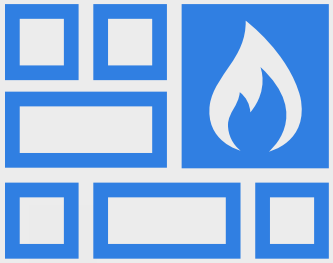
Schutzfunktionen mit anderen Technologien sorgt dafür, dass das Netzwerk effektiv gegen alle aktuellen und kommenden Bedrohungen gesichert ist.

Konvergenz

Zusätzlich sollte Ihr NGFW-Deployment bei komplexen Angriffen einen umfassenden Überblick über das Geschehen bieten und beispielsweise getarnte Aktivitäten zur Ausschleusung von Daten oder Einschleusung von Malware über HTTPS-Kanäle aufdecken. Grundlage hierfür ist die Zusammenführung wichtiger Netzwerk- und Sicherheitsfunktionen in einer integrierten Lösung, die entweder über eine On-Premises-NGFW oder ein cloudbasiertes SASE bereitgestellt werden kann und moderne Routing- und Konnektivitätssysteme mit dynamischem Schutz kombiniert.

Darüber hinaus muss Ihre NGFW in der Lage sein, sämtliche Nutzer, Geräte und Anwendungen zu erkennen und jede Zugriffsanfrage automatisch dem richtigen Netzwerksegment zuzuordnen. Das erfordert nativ integrierte Proxyservices, die es der Firewall ermöglichen, die anfängliche Zugriffsanfrage eines Geräts unter Einbeziehung von Endpunkt-Clients (für Nutzer und Server) und Netzwerkzugangskontrollen (für IoT- und IIoT-Geräte) zu bearbeiten. Weiterhin notwendig sind Funktionen zur Multi-Faktor-Authentifizierung, die die Rolle jedes Nutzers oder Geräts genau bestimmen, die jeweils geltenden Richtlinien abrufen und nur den Zugriff auf die für die jeweiligen Aufgaben benötigten Anwendungen und Segmente erlauben.

Dank dieser Features kann die NGFW Richtlinien standortübergreifend implementieren und durchsetzen, selbst wenn die Bereitstellungsumgebung von Anwendungen und Workflows häufig wechselt. Abgesehen davon profitieren die Verantwortlichen von konsistenten Orchestrierungsprozessen und einer zentralen Management-Konsole, mit der sich alle Nutzeraktivitäten, Betriebsabläufe und Transaktionen lückenlos überwachen lassen.



Eine NGFW kann Richtlinien standortüber-greifend implementieren und durchsetzen, selbst wenn die Bereitstellungsumgebung von Anwendungen und Workflows häufig wechselt.

Skalierbarkeit

Unabhängig von ihrem jeweiligen Standort und Formfaktor müssen alle Firewalls schnell sein – und zwar nicht nur heute, sondern auch in den kommenden Jahren. Grund hierfür sind die riesigen Datenvolumen, die von modernen Rechenzentren erzeugt und verarbeitet oder zur Erstellung von Big-Data-Modellen genutzt werden, sowie strenge Latenz- und Leistungsvorgaben für Hochgeschwindigkeitstransaktionen im Finanzwesen und extrem umfangreiche Multi-User-Umgebungen.

In all diesen Fällen kommt es entscheidend darauf an, wie schnell die implementierten Firewalls übertragene Daten überprüfen. Zudem muss eine NGFW das Netzwerk mit modernen, orchestrierten Sicherheitsfunktionen effektiv vor Blitzangriffen schützen und aufwendige Betriebs- und Bereitstellungsprozesse durch Automatisierung straffen. Auf diese Weise lassen sich sowohl zeitraubende manuelle Abläufe als auch Konfigurationsfehler (mitsamt den dadurch ermöglichten Ransomware-Angriffen und sonstigen Attacken) vermeiden.

Dabei besteht die größte Herausforderung darin, dass die meisten konventionellen Firewalls bereits stark ausgelastet sind. Sie lassen sich kaum an die wachsenden Anforderungen moderner Geschäftsmodelle anpassen, weil sie schlicht nicht für Hochleistungsanwendungen entwickelt wurden. Insbesondere verwenden sie nach wie vor Standardprozessoren, während andere Systeme wie Grafikkarten, Smartphones oder Cloud-Server bereits seit Längerem auf dedizierten Chips basieren. Damit verleugnen sie die Tatsache, dass sich der Netzwerkschutz mittlerweile zu einer äußerst rechenintensiven Aufgabe entwickelt hat: Um den aktuellen Anforderungen zu genügen, benötigen Sie leistungsstarke Firewall-Funktionen, die die Performance nicht beeinträchtigen, Ihr IT-Team entlasten und im Rahmen Ihres bestehenden Budgets erschwinglich sind.

[1] „HTTPS encryption on the web“, Google Transparency Report, abgerufen am 1. June 2023.

www.fortinet.com/de

.

2170366-0-0-DE