WHITEPAPER

Leistungsstarke Security für das gesamte Unternehmen

Sieben Kriterien für die Auswahl Ihrer nächsten Next-Generation-Firewall

Kurzfassung

Der Umstieg auf hybride Arbeitsmodelle und Cloud-Dienste bedeutet, dass Nutzer heutzutage über jedes Gerät und an jedem Standort auf sämtliche Ressourcen zugreifen können. Diese Flexibilität ist zwar unerlässlich, aber sie vergrößert auch die Angriffsfläche, was neuen Bedrohungen Tür und Tor öffnet. Daher müssen Unternehmen sicherstellen, dass ihr Netzwerk-Security-Ansatz umfassende Einblicke in die gesamte verteilte Infrastruktur bietet. Andernfalls ist kein effektiver und koordinierter Schutz möglich und Security-Teams können Bedrohungen nicht schnell genug erkennen und abwehren.

Mit einer Kombination aus Next-Generation-Firewalls (NGFWs) und den KI-gestützten Security Services von FortiGuard können Unternehmen ihre Nutzer umfassend schützen – dank Threat Intelligence in Echtzeit und mehrschichtigen Sicherheitskontrollen wie Intrusion Prevention, Malware-Scans und Website-Filterung. So minimieren sie Ausfallzeiten und kostspielige Wiederherstellungsmaßnahmen, senken das Risiko von Datenlecks und vermeiden einen Reputationsverlust. Durch die enge Verzahnung der Security Services mit der Firewall wird das Netzwerk optimal geschützt.

4,45 Mio. USD

Laut einer aktuellen Studie erreichten die Kosten eines Datenlecks 2023 im weltweiten Durchschnitt mit 4,45 Millionen US-Dollar eine neue Rekordmarke. Das ist ein Anstieg von 2,25 % gegenüber dem Vorjahr.[1]

NGFWs sollten Bedrohungen an jeder Schnittstelle zwischen Filial-, Campus- bzw. Data-Center-Netzwerk und der Außenwelt (dem Edge) blockieren, ohne die Leistung zu beeinträchtigen. Damit sie die gesamte Infrastruktur des Unternehmens abdecken, müssen sie Teil einer umfassenden, integrierten und automatisierten Security-Architektur sein und Faktoren wie Skalierbarkeit, Betriebskosten und umweltspezifische Anforderungen berücksichtigen.

So bewerten Sie NGFWs

NGFWs spielen eine wichtige Rolle beim Bedrohungsschutz: Ihre Sicherheitsvorkehrungen decken nicht nur die gesamte Infrastruktur vom Netzwerk-Edge bis hin zum Data Center ab, sondern auch die Verbindungen zwischen internen Netzwerksegmenten, in der Cloud und in OT-Umgebungen. Security-Teams müssen sich darauf verlassen können, dass NGFWs ihnen einen Überblick über Bedrohungen für Nutzer, Geräte, Anwendungen und Netzwerke liefern und bei Bedarf leistungsstarke Schutzmaßnahmen anwenden. Daher sollten Unternehmen bei der Auswahl einer NGFW die sieben folgenden wichtigen Kriterien beachten.

1. **Integrierte, KI-gestützte Security Services:** Security Services, die von künstlicher Intelligenz (KI) unterstützt werden, erweitern herkömmliche Firewall-Funktionen durch die proaktive Erkennung und Abwehr neuer – auch KI-basierter – Gefahren. Diese Dienste entlasten das Security-Team, verbessern die Effizienz von Sicherheitsvorkehrungen, erleichtern die Zuweisung von Ressourcen, vereinfachen das Security-Management und fördern eine bessere Entscheidungsfindung.

   NGFWs mit integrierten, KI-gestützten Security Services bieten weitaus mehr als herkömmliche Firewalls. Sie nutzen maschinelle Lernalgorithmen (ML), die riesige Mengen an Daten analysieren und Anomalien erkennen können, die auf schädliche Aktivitäten hinweisen. Eine KI-basierte Firewall kann den Netzwerkverkehr in Echtzeit analysieren und Sicherheitsrichtlinien dynamisch anpassen. So ist dafür gesorgt, dass relevante und effektive Security-Maßnahmen angewendet werden, das Risiko von Angriffen reduziert wird und Ressourcen effizienter zugewiesen werden.

2. **Leistungsstarker Bedrohungsschutz:** Die Schutzleistung gibt an, wie gut eine NGFW funktioniert, wenn alle Funktionen für den Bedrohungsschutz aktiviert sind: Firewall, Intrusion Prevention, Antivirus und Anwendungskontrolle. Eine NGFW muss in der Lage sein, auch im voll aktivierten Schutzmodus Höchstleistungen zu erbringen. Viele Anbieter von NGFWs bringen nicht klar zum Ausdruck, worauf ihre Leistungsangaben beim Bedrohungsschutz basieren. Unternehmen sollten die dokumentierte Leistungsfähigkeit daher sorgfältig analysieren, um sicherzustellen, dass sich die Angaben auf Tests mit voll aktiviertem Bedrohungsschutz beziehen.

3. **Zentrale Management-Konsole:** Bei der Auswahl einer geeigneten NGFW kommen viele Security-Architekten ins Stolpern, wenn es um die Management-Schnittstelle geht. Die Nutzeroberfläche und die Funktionen wurden wahrscheinlich genauestens unter die Lupe genommen, aber wenn die NGFW als alleinstehende Komponente verstanden wird, müssen die Security-Teams in der Praxis zwischen mehreren Dashboards hin- und herwechseln, um Sicherheitslücken zu analysieren und auf Bedrohungen zu reagieren. Umfassende Transparenz und Kontrolle sind nur erreichbar, wenn die NGFW in die weitere Security-Architektur eingebunden wird, damit Threat Intelligence mit anderen Netzwerkgeräten geteilt und automatisch empfangen werden kann. Unter dem Blickwinkel der Sicherheit ist eine zentrale Management-Konsole wesentlich effektiver. Zudem ermöglicht sie einen effizienteren Betrieb, reduziert den Verwaltungsaufwand und minimiert die Einarbeitungskosten.

4. **Umfassende Security-Strategie:** Hybride Arbeitsmodelle haben die Cybersecurity-Landschaft dauerhaft verändert und dezentrale Unternehmensstrukturen machen redundante WAN-Verbindungen zu Filialen und Niederlassungen erforderlich. Oftmals werden zusätzliche Security-Funktionen wie SD-WAN, ZTNA (Zero-Trust Network Access) und SASE (Secure Access Service Edge) benötigt.

   Viele NGFW-Anbieter stellen diese Funktionen als optionale Add-ons zur Verfügung, mit denen dezentral aufgebaute Unternehmen Hochleistungsnetzwerke mit Hochverfügbarkeit einrichten können. Solche aufgesetzten Produkte sind jedoch kein optimaler Ansatz. Sehen Sie sich stattdessen nach einem Anbieter um, der eine NGFW mit nativ integrierter, sicherer SD-WAN-, SASE- und ZTNA-Funktionalität bietet, die es Ihnen ermöglicht, Punktlösungen zu konsolidieren und Kontrollmaßnahmen zentralisiert durchzusetzen. So reduzieren Sie Ihre Gesamtinvestitionskosten und vermeiden Sicherheitslücken.

5. **Preis-Leistungs-Verhältnis und andere betriebswirtschaftliche Gesichtspunkte:** Manche Anbieter steigern die Schutzleistung, indem sie den Umfang (und den Preis) ihres NGFW-Angebots erhöhen. Damit wirken sie jedoch genau dem Trend entgegen, den moderne Unternehmen mit ihrem Bestreben verfolgen, die Technologie-Landschaft zu minimieren. Wählen Sie eine NGFW, die die erforderliche Leistung in einem möglichst kompakten Formfaktor bietet. Je kleiner der Formfaktor, desto geringer sind in der Regel auch die Gesamtbetriebskosten. Außerdem sparen Sie Platz und reduzieren Ihren Energieverbrauch – zwei wichtige Ziele für umweltbewusste Unternehmen. Auch die Wartungs- und Supportkosten für die NGFW müssen berücksichtigt werden. In dieser Hinsicht überzeugen technologisch ausgereifte Lösungen und Lösungen von Anbietern, die stark in Forschung und Entwicklung investieren. Die Vorteile für Sie als Kunden? Eine reibungslosere Bereitstellung und weniger Anrufe beim Support-Team des Anbieters. In Bezug auf die Hardware sollten Sie auf eine redundante Stromversorgung achten und sicherstellen, dass sowohl 40-GbE- als auch 100-GbE-Schnittstellen unterstützt werden, um eine hohe Resilienz zu gewährleisten und die Umstellung auf Netzwerke mit höherer Kapazität zu ermöglichen.

6. **ASICs als Erfolgsturbo:** ASICs sind spezielle Chips, die auf die Beschleunigung bestimmter Security-Funktionen ausgelegt sind, zum Beispiel die Verarbeitung von Paketen sowie die Ver- und Entschlüsselung. Unternehmen sollten sich nach einer NGFW mit zuverlässigen ASICs umsehen, die ein hohes Verkehrsaufkommen unterstützen, die für Echtzeitschutz vor modernen Bedrohungen erforderliche niedrige Latenz bieten und gleichzeitig den Energieverbrauch reduzieren. Das richtige ASIC-Design kann der Schlüssel zu einer effektiveren und kosteneffizienteren Sicherheitslösung sein.

7. **Validierung durch unabhängige Dritte:** Der Netzwerk-Security-Sektor ist schnelllebig und dynamisch, aber kein Unternehmen kann es sich leisten, in unzulänglich getestete Sicherheitslösungen zu investieren. Entscheidungsträger sollten sich nicht ausschließlich auf die Angaben des Anbieters verlassen, sondern Bewertungen von renommierten, unabhängigen Dritten wie cyberratings.org berücksichtigen.

Worauf es bei einer NGFW ankommt

Da NGFWs eine entscheidende Rolle beim Schutz des gesamten Unternehmens spielen (einschließlich IT- und OT-Umgebungen) und sowohl Geschäfts- als auch Kundendaten abdecken, sollten Security-Architekten bei der Auswahl große Sorgfalt walten lassen. Ein wichtiger Aspekt ist das Gleichgewicht zwischen Security und Leistung: Die NGFW muss konsistente, konsolidierte Sicherheitsabläufe an allen dezentralen Edge-Zugangspunkten bei minimaler Auswirkung auf die Leistung bieten.

Aber es gibt noch weitere Erwägungen. Um den Energie- und Platzbedarf möglichst gering zu halten, sollten Sie nach einer kompakten NGFW-Lösung mit minimalem Formfaktor suchen, die flexibel genug für den Einsatz im Data Center oder am Netzwerk-Edge ist. Außerdem sollte sich die NGFW in die weitere Security-Architektur einbinden lassen, umfassende Transparenz bieten und Threat Intelligence automatisch zwischen Geräten austauschen können.

[1] IBM Security und das Ponemon Institute, The Cost of a Data Breach Report 2023.

12. Dezember 2024 12:53 / 2155416-B-0-DE