RAPORT

Skalowanie w celu zapewnienia wysoce skutecznych zabezpieczeń

6 kryteriów wyboru zapór nowej generacji

Streszczenie

Przejście na model pracy hybrydowej i szybkie wdrożenia usług w chmurze umożliwiły użytkownikom łączenie się z dowolnymi zasobami z dowolnego miejsca za pomocą dowolnego urządzenia. Elastyczność ta jest wprawdzie niezbędna, ale zwiększa powierzchnię ataku, a więc stanowi furtkę dla nowych zagrożeń. Organizacje muszą mieć pewność, że ich zabezpieczenia sieciowe pozwalają uzyskać pełny wgląd w całą rozproszoną infrastrukturę. Jeśli ten warunek nie jest spełniony, nie można skutecznie zapewniać ani koordynować ochrony, łącznie z wystarczająco szybkim wykrywaniem i eliminowaniem zagrożeń.

Połączenie zapór nowej generacji (next-generation firewall, NGFW) z usługami zabezpieczeń opartymi na sztucznej inteligencji umożliwia analizowanie zagrożeń w czasie rzeczywistym, co zapewnia użytkownikom wielowarstwowe zabezpieczenia, obejmujące zapobieganie włamaniom, skanowanie pod kątem złośliwego oprogramowania i filtrowanie stron internetowych w celu zapewnienia kompleksowej ochrony. Przekłada się to na krótsze przestoje i mniejsze ryzyko złamania zabezpieczeń danych, co ogranicza do minimum uszczerbek na reputacji i konieczność kosztownego odzyskiwania danych. W idealnej sytuacji usługi zabezpieczeń są ściśle zintegrowane z zaporą, oferując wartościową strategię wzmacniania zabezpieczeń sieci.

Zapory NGFW powinny zapewniać ochronę przed zagrożeniami na każdym brzegu sieci — w każdym oddziale, kampusie i centrum danych — bez żadnych kompromisów w zakresie wydajności i skuteczności. Aby efektywnie działały na poziomie całej organizacji, muszą też być częścią obszernej, zintegrowanej i zautomatyzowanej architektury zabezpieczeń oraz spełniać wymagania dotyczące skalowalności, kosztów posiadania i ochrony środowiska.

4,45 mln $

Według niedawnego raportu w 2023 roku średni światowy koszt złamania zabezpieczeń danych osiągnął rekordowy poziom 4,45 miliona dolarów. Oznacza to wzrost o 2,25% w porównaniu z poprzednim rokiem[1].

Wymogi brane pod uwagę podczas oceny zapór NGFW

Zapory NGFW odgrywają ważną rolę w obszarze ochrony przed zagrożeniami, zapewniając bezpieczeństwo od brzegu sieci po centrum danych, między segmentami wewnętrznymi oraz w chmurze. Zespoły ds. bezpieczeństwa stosują zapory NGFW, aby mieć wgląd w użytkowników, urządzenia, aplikacje i zagrożenia sieciowe oraz zyskać zaawansowaną ochronę przed zagrożeniami wszędzie tam, gdzie zajdzie taka potrzeba. Wybierając zaporę NGFW przeznaczoną na brzeg sieci lub do centrum danych, firma powinna wziąć pod uwagę sześć istotnych kryteriów.

1. **Zintegrowane usługi zabezpieczeń oparte na sztucznej inteligencji.** Usługi zabezpieczeń oparte na sztucznej inteligencji uzupełniają tradycyjne funkcje zapór o proaktywne wykrywanie zagrożeń, z uwzględnieniem ich ewoluujących form. Usługi te pomagają odciążyć zespoły ds. bezpieczeństwa, zwiększają efektywność zabezpieczeń i alokacji zasobów oraz usprawniają zarządzanie zabezpieczeniami, umożliwiając podejmowanie trafniejszych decyzji.

   Funkcje zapór NGFW ze zintegrowanymi usługami zabezpieczeń opartymi na sztucznej inteligencji wykraczają poza możliwości tradycyjnych zapór, ponieważ obejmują uczenie maszynowe, co pozwala na analizy ogromnych ilości danych w celu identyfikowania anomalii, które mogą sygnalizować szkodliwe działania. Dzięki sztucznej inteligencji zapora może dynamicznie dostosowywać zasady zabezpieczeń na podstawie wyników analiz ruchu sieciowego w czasie rzeczywistym. To zaś przekłada się na stosowanie odpowiednich i skutecznych środków bezpieczeństwa, a zatem i mniejsze ryzyko złamania zabezpieczeń oraz optymalizację alokacji zasobów.

2. **Skuteczność ochrony przed zagrożeniami.** Skuteczność ochrony przed zagrożeniami odzwierciedla to, jak dobrze spisuje się zapora NGFW, wykonując zadania pełnej ochrony przed zagrożeniami, w tym funkcje zapory, zapobieganie włamaniom, ochronę antywirusową i kontrolę aplikacji. Kluczowe znaczenie z perspektywy zapory NGFW ma utrzymanie wysokiej skuteczności, gdy jest aktywna pełna ochrona przed zagrożeniami. Wielu dostawców zapór NGFW nie informuje jasno, skąd się biorą ich deklaracje dotyczące skuteczności ochrony przed zagrożeniami. W przypadku udokumentowanych deklaracji skuteczności należy dokładnie sprawdzać, czy rzeczywiście opierają się na pomiarach dokonywanych pod obciążeniem i przy w pełni włączonej ochronie przed zagrożeniami.

3. **Zarządzanie w jednej konsoli.** Interfejs zarządzania to obszar, w którym wielu architektów zabezpieczeń napotyka utrudnienia w wyborze rozwiązania. Być może interfejsowi użytkownika i funkcjonalności systemu zarządzania poświęcono wiele uwagi. Jeśli jednak jest on ograniczony do zapory NGFW, zespoły ds. bezpieczeństwa muszą przełączać wiele konsol, aby oceniać luki w zabezpieczeniach i reagować na zagrożenia. Pełny wgląd w środowisko i kontrola są możliwe tylko wtedy, gdy zapora NGFW stanowi część obszernej, zintegrowanej architektury zabezpieczeń, w której informacje o zagrożeniach są automatycznie udostępniane innym urządzeniom sieciowym i od nich odbierane. Z perspektywy bezpieczeństwa efektywniejsze jest kompleksowe zarządzanie w ramach jednej konsoli. Zapewnia ono również korzyści na poziomie operacyjnym, ponieważ redukuje czas poświęcany na zadania administracyjne i koszty szkoleń.

4. **Zapewnianie szerszej strategii bezpieczeństwa.** Praca hybrydowa na zawsze zmieniła oblicze cyberbezpieczeństwa. Dodatkowo firmy często mają rozproszone biura, których funkcjonowanie zależy od zapasowych połączeń WAN. W wielu przypadkach wymagają one dodatkowych rozwiązań zabezpieczających, takich jak SD-WAN, dostęp do sieci zgodnie z zasadą zerowego zaufania (zero-trust network access, ZTNA) czy bezpieczny dostęp do usług na brzegu sieci (secure access service edge, SASE).

   Wielu dostawców zapór NGFW oferuje dodatkowe funkcje SD-WAN, ZTNA i SASE, które umożliwiają organizacjom mającym oddziały tworzenie wysoce dostępnych i wydajnych sieci. Oferty te nie są jednak idealne. Warto poszukać dostawcy, którego zapory NGFW mają w pełni zintegrowane i bezpieczne funkcje SD-WAN, ZTNA i SASE, co ułatwia konsolidację różnych rozwiązań cząstkowych i wymuszenie scentralizowanej kontroli. Taka konsolidacja obniża ogólne koszty inwestycji i ułatwia eliminowanie luk w zabezpieczeniach.

5. **Stosunek ceny do efektywności i inne aspekty operacyjne.** Niektórzy dostawcy skalują wydajność i skuteczność przez zwiększanie wielkości oraz podnoszenie cen swoich zapór NGFW, co może się kłócić z dążeniami firmy do ograniczania miejsca zajmowanego przez sprzętowe rozwiązania technologiczne. Warto postawić na zaporę NGFW, która zapewnia wymaganą wydajność i skuteczność przy jak najmniejszej obudowie. Wybór mniejszej zapory NGFW może się przełożyć na niższy całkowity koszt posiadania (TCO), oszczędność miejsca i mniejsze zużycie energii, a jest to dość istotne dla przedsiębiorstw dbających o środowisko. Koszty konserwacji i pomocy technicznej związane z zaporą NGFW również należy uwzględniać w całkowitym koszcie posiadania. Dojrzała technologia ma pod tym względem przewagę — podobnie jak oferta od dostawcy, który inwestuje mnóstwo środków w badania i projektowanie. Właściciele zapór NGFW, które należą do tej kategorii, mogą się spodziewać płynniejszych wdrożeń i mniejszej liczby zgłoszeń problemów technicznych. Jeśli chodzi o sprzętowe aspekty zapory NGFW, należy zwrócić uwagę na nadmiarowość zasilania i obsługę interfejsów sieciowych 40 GbE oraz 100 GbE. Opcje te zwiększają odporność i umożliwiają migrację do sieci o wyższej przepustowości.

6. **Niezależna weryfikacja przez zewnętrzny podmiot.** Wprawdzie bezpieczeństwo sieci jest szybko rozwijającą się branżą, jednak żadna firma nie może sobie pozwolić na ryzyko korzystania z niesprawdzonych rozwiązań bezpieczeństwa. Zamiast polegać na deklaracjach sprzedawców, architekci powinni się postarać o kontrolę zewnętrzną wykonywaną przez renomowane ośrodki testowania, na przykład cyberratings.org.

Najważniejsze aspekty zapór NGFW

Ponieważ zapora NGFW odgrywa kluczową rolę w ochronie całego przedsiębiorstwa — w tym danych zarówno samej firmy, jak i jej klientów — architekci zabezpieczeń powinni starannie przeanalizować dostępne opcje. W procesie oceniania rozwiązań NGFW najważniejsze mogą być ewentualne kompromisy między bezpieczeństwem a wydajnością. Możliwość zapewnienia spójnej i skonsolidowanej ochrony na wszystkich rozproszonych brzegach środowiska przy minimalnym ujemnym wpływie na wydajność ma wprost ogromne znaczenie.

Organizacje muszą jednak brać pod uwagę jeszcze inne kwestie. Zważywszy na ograniczenia w zakresie zużycia energii i miejsca w firmie, warto szczególnie mocno się zainteresować kompaktowymi rozwiązaniami NGFW, które mają minimalne wymagania dotyczące miejsca, a jednocześnie są wystarczająco elastyczne, aby można było je wdrożyć w centrum danych albo na brzegu sieci. Architekci zabezpieczeń powinni też zadbać, by zapora NGFW była zintegrowana z ogólną architekturą zabezpieczeń i zapewniała kompleksowy wgląd oraz obsługiwała automatyczne udostępnianie informacji o zagrożeniach między urządzeniami.

[1] Cost of a Data Breach Report 2023 (Raport o kosztach naruszenia ochrony danych w 2023 r.), IBM Security i Ponemon Institute.

12 lipca 2024 10:07

2155416-A-0-EN