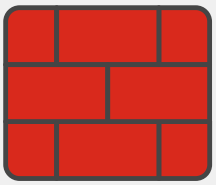
INFORMACJE BRANŻOWE

Zintegrowane zapory sieciowe — niezbędne rozwiązanie dla rozproszonego przedsiębiorstwa

Co to jest rozwiązanie oparte na zintegrowanej zaporze sieciowej?

Większość organizacji nie ma spójnych zabezpieczeń i widoczności w różnych segmentach swoich rozproszonych środowisk sieciowych, a cyberprzestępcy wykorzystują to na swoją korzyść. Ponieważ centra danych, kampusy, chmury i oddziały są ze sobą połączone, ruch wschód-zachód wzrósł, powodując, że zagrożenie występujące w jednej części sieci, szybko może rozprzestrzenić się na inne. Najskuteczniejszym sposobem na sprostanie temu wyzwaniu jest wdrożenie tych samych zabezpieczeń w każdej części sieci, umożliwiając w ten sposób scentralizowaną korelację zagrożeń i skoordynowaną ochronę wielu obszarów przedsiębiorstwa jednocześnie. Jednakże złożoność i różnice między różnymi ekosystemami sieciowymi mogą to utrudniać.



Firma Fortinet została uznana za lidera w raporcie Gartner® Magic Quadrant™ for Network Firewalls przez 13 kolejnych lat, a w najnowszym raporcie zajęła najwyższą pozycję w kategorii Ability to Execute.[1]

Zapory sieciowe mogą być wdrażane w celu zapewnienia krytycznych funkcji zapory NGFW w dowolnym miejscu w sieci — kampusie, centrum danych, chmurze, FWaaS i środowiskach SASE — z możliwością zdalnego, ujednoliconego zarządzania. Korzystanie z tego samego systemu operacyjnego pozwala stworzyć pojedynczą, zintegrowaną, skalowalną platformę, która może dostosowywać się do dzisiejszych dynamicznych i rozproszonych sieci. Ujednolicona konsola zarządzania umożliwia koordynację ochrony w różnych domenach IT, w tym w witrynach korporacyjnych, chmurach publicznych i prywatnych oraz wśród pracowników zdalnych. Dzięki takiemu zintegrowanemu podejściu zespoły IT mogą zautomatyzować procesy wykrywania zagrożeń i reagowania na nie, uruchamiać konfiguracje oraz egzekwować zasady bez tracenia czasu na wykonywanie czynności manualnych, zwłaszcza w obliczu niedoboru specjalistów z zakresu cyberbezpieczeństwa.

Potrzeba wprowadzenia zintegrowanych zapór sieciowych

Zapory sieciowe są niezbędne do ochrony sieci przed nieautoryzowanym dostępem i złośliwymi atakami. Działają one jak cyfrowi strażnicy, monitorując i kontrolując ruch sieciowy, aby zapobiec nieautoryzowanemu dostępowi, naruszeniom danych i innym zagrożeniom bezpieczeństwa. Rozwiązania te zostały zaprojektowane w celu sprostania czterem krytycznym wyzwaniom, przed którymi stoją dzisiejsze organizacje IT:

1. Złożona infrastruktura IT

Wiele z dzisiejszych zapór NGFW nie obsługuje kluczowych funkcji, zmuszając przedsiębiorstwa do zakupu oddzielnych rozwiązań bezpieczeństwa dla witryn korporacyjnych, publicznych i prywatnych środowisk chmurowych oraz urządzeń pracowników zdalnych. W rezultacie pojawiają się niespójności na szczeblu operacyjnym, w tym błędy konfiguracyjne, które mogą prowadzić do naruszeń bezpieczeństwa sieci.

2. Niedobór specjalistów ds. cyberbezpieczeństwa

Poza złożonością, produkty punktowe zwiększają ryzyko operacyjne ze względu na długi czas ich wdrożenia. Wiele produktów punktowych wymaga od zajmujących się cyberbezpieczeństwem pracowników działu IT przeznaczenia kolejnych godzin na naukę nowych funkcji i paneli kontrolnych. Naraża to przedsiębiorstwa na jeszcze większe ryzyko, ponieważ wiele stanowisk związanych z cyberbezpieczeństwem pozostaje nieobsadzonych ze względu na globalny niedobór specjalistów.

3. Wzrost liczby zaawansowanych zagrożeń

Złożoność i niedobory umiejętności w zakresie cyberbezpieczeństwa nie są jedynymi czynnikami stymulującymi zapotrzebowanie na zintegrowane zapory sieciowe. Liczba zaawansowanych, wyrafinowanych cyberzagrożeń szybko rośnie, w wielu przypadkach dzięki sztucznej inteligencji. Takie zaawansowane zagrożenia stają się coraz trudniejsze do wykrycia i coraz bardziej niszczycielskie dla firm. Wektory ataków obejmują sieć, aplikacje, treści i urządzenia. Na przykład oprogramowanie ransomware nadal zakłóca funkcjonowanie przedsiębiorstw z różnych branż, w tym przedsiębiorstw korzystających z technologii operacyjnej (OT), organów administracji rządowej i samorządowej, zakładów przemysłowych i placówek opieki zdrowotnej.

4. Rola mechanizmów sztucznej inteligencji i uczenia maszynowego

Złożoność, ręczny nadzór i coraz to nowe metody włamań wymagają skoordynowanej ochrony. Nie wystarczy już fakt, że zapora może obejmować różne obszary sieci, zapora taka musi bowiem korzystać z mechanizmów sztucznej inteligencji (AI) i uczenia maszynowego (ML), które są niezbędne do ochrony przed znanymi i nieznanymi zagrożeniami. Dodanie do zapory sieciowej zabezpieczeń opartych na tych mechanizmach umożliwia im nie tylko identyfikację i klasyfikację aplikacji, adresów URL, użytkowników, urządzeń, złośliwego oprogramowania i wielu innych elementów, ale również automatyzację egzekwowania zasad w różnych domenach. Mechanizmy sztucznej inteligencji i uczenia maszynowego są podstawą automatyzacji działania zapory sieciowej i mogą znacznie zmniejszyć nakłady pracy związanej z ochroną korporacyjnej infrastruktury IT.

Czego należy poszukiwać w rozwiązaniach zapór sieciowych dla środowisk hybrydowych?

Scentralizowane i ujednolicone zarządzanie

Najważniejszymi zaletami zapór sieciowych jest wykrywanie zagrożeń, zarządzanie zasadami i automatyzacja odpowiedzi w reakcji na zagrożenia w dowolnym miejscu w sieci przy użyciu wszystkich dostępnych narzędzi.

Funkcje ujednoliconego zarządzania pozwalają na koordynację i ujednolicenie domen w ramach jednego korporacyjnego rozwiązania zabezpieczającego infrastrukturę IT. Tym samym zapewniają prostą, zautomatyzowaną ochronę rozciągającą się od siedziby przedsiębiorstwa po chmurę i pracowników zdalnych. Ze względu na fakt, że przedsiębiorstwa mają odmienne wymagania dotyczące zarządzania różnymi zaporami sieciowymi, niezbędne jest wsparcie dla różnego typu platform, w tym, urządzeń fizycznych, maszyn wirtualnych, usług SaaS oraz usług zarządzania zaporami sieciowymi.

Zapora sieciowa musi również łączyć zespoły centrum zarządzania siecią (NOC) i centrum zarządzania bezpieczeństwem (SOC) w ramach jednej konsoli, która umożliwia monitorowanie całej powierzchni ataku i zarządzanie nią.

Urządzenia oparte na układach ASIC

Każde środowisko obecne w danej sieci ma specyficzne wyzwania związane z bezpieczeństwem. Witryny korporacyjne wymagają rozwiązań, które rozszerzają gamę zabezpieczeń, zapewniają spójną ochronę pozostając niewidocznymi dla użytkowników.

Współczesne organizacje wymagają wysokiej wydajności, potrzebują zatem urządzeń wyposażonych w dedykowane, specjalizowane układy scalone (Application-Specific Integrated Circuits, ASIC), zwiększających szybkość działania krytycznych zabezpieczeń. Urządzenie bezpieczeństwa oparte na dedykowanych układach ASIC może odciążyć wiele zasobochłonnych funkcji, takich jak realizacja funkcji zapory sieciowej, VPN, IPS, a nawet dekrypcji SSL/TLS lub głębokiej inspekcji pakietów (DPI). Układy ASIC mogą znacznie zwiększyć wydajność funkcji bezpieczeństwa w porównaniu z procesorami ogólnego przeznaczenia.

Natywna zapora sieciowa przeznaczona dla chmury

Natywna zapora sieciowa przeznaczona dla chmury chroni aplikacje w chmurze publicznej, wdrożone w środowiskach IaaS w modelu „Infrastructure-as-Code”. Dodanie do środowiska chmurowego natywnej zapory sieciowej zmniejsza nakład pracy związany z zapewnieniem bezpieczeństwa sieci poprzez zwiększenie widoczności przy jednoczesnym wyeliminowaniu konieczności konfigurowania, utrzymywania i przydzielania zasobów do tradycyjnej infrastruktury zapór sieciowych. W rezultacie zespoły ds. bezpieczeństwa mogą skupiać się na zarządzaniu zasadami.

Zapora sieciowa w środowisku wirtualnym

Zapora wirtualna jest powszechnie stosowana do ochrony środowisk zwirtualizowanych w definiowanych programowo centrach danych i środowiskach wielochmurowych. Zapora wirtualna to najtańsze i najbardziej przenośne rozwiązanie, dzięki czemu pracownicy działu IT mogą ją szybko przenosić pomiędzy chmurami. Zapory wirtualne w ramach sieciowej infrastruktury bezpieczeństwa umożliwiają budowę kompleksowego ekosystemu dla definiowanego programowo centrum danych. Wspomagają proces konsolidacji, chroniąc jednocześnie środowisko przy użyciu różnych funkcji bezpieczeństwa, wykraczających poza dynamiczne filtrowanie pakietów.

Zapora sieciowa jako usługa

Zapora jako usługa (Firewall-as-a-Service, FWaaS) to rozwiązanie oferowane w formie usługi chmurowej. Pozwala przedsiębiorstwom na uproszczenie i skalowanie infrastruktury IT. Pod wieloma względami przypomina zaporę sprzętową instalowaną lokalnie, zapewniając pełny zakres funkcji zapory NGFW, takich jak filtrowanie stron WWW, ochrona przed zaawansowanymi zagrożeniami, ochrona przed atakami (IPS) i zabezpieczenia DNS. Zapora sieciowa wdrożona w modelu FWaaS rozszerza swoje unikatowe możliwości na rozproszone urządzenia i użytkowników, łącząc niemal natychmiastową skalowalność ze scentralizowaną kontrolą.

Jeden system operacyjny

Szybka rozbudowa brzegów sieci zwiększyła wyzwania związane z wyborem właściwego rozwiązania zabezpieczającego w natłoku dostawców i rozwiązań punktowych. Różne rozwiązania punktowe nie mogą się ze sobą komunikować ani współdziałać, co nie daje szans na prowadzenie spójnej polityki bezpieczeństwa, zapewnienie kompleksowej widoczności i szerokie wprowadzenie automatyzacji. Ponadto utrzymanie i monitorowanie tak licznych rozwiązań hybrydowych, sprzętowych, programowych i X-as-a--Service nadmiernie obciąża zespoły ds. bezpieczeństwa.

Podstawą działania zapór sieciowych jest pojedynczy, wspólny system operacyjny, który konsoliduje liczne technologie i zastosowania w ramach uproszczonej struktury zarządzania i tworzenia polityk bezpieczeństwa. Podczas gdy ujednolicona konsola zarządzania konsoliduje operacje związane z obsługą, pojedynczy system operacyjny zapewnia możliwość współdziałania różnych typów implementowanych rozwiązań, w tym sprzętowych i wirtualnych zapór sieciowych, natywnych zapór sieciowych dla chmury oraz rozwiązań FWaaS.

Zalety zintegrowanych zapór sieciowych

Zintegrowane zapory sieciowe zapewniają korporacyjnym działom IT ogromne korzyści, w tym poprawę wydajności operacyjnej działu IT i ograniczenie ryzyka związanego z cyberbezpieczeństwem. W kontekście tych korzyści można ponadto wymienić ograniczenie ryzyka organizacyjnego, zmniejszenie zapotrzebowania na specjalistów ds. cyberbezpieczeństwa, dobrą ochronę przed znanymi i nieznanymi cyberzagrożeniami, automatyzację i koordynację za pośrednictwem mechanizmów sztucznej inteligencji i uczenia maszynowego, a także niższy całkowity koszt związany z posiadaniem i utrzymaniem rozwiązania.

[1] A Leader Positioned Highest in Ability to Execute, Fortinet, dostęp 13 września 2024 r.

FORTINET

www.fortinet.com

9 grudnia 2024 12:45 / 2133550-A-0-PL