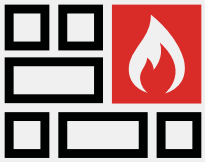
Hybrid Mesh Firewall — niezbędne rozwiązanie dla rozproszonego przedsiębiorstwa

Czym jest Hybrid Mesh Firewall?

Współczesny cyberprzestępca wykorzystuje fakt, że większości przedsiębiorstw brakuje spójnej widoczności w różnych segmentach ich rozproszonych sieci. Ze względu na sieć połączeń istniejącą między centrami danych (CD), kampusami, chmurami i oddziałami, ruch wschód-zachód nasila się, umożliwiając szybkie rozprzestrzenianie się udanego naruszenia dokonanego w jednej części sieci na inne jej części. Najbardziej efektywnym sposobem poradzenia sobie z taką sytuacją jest wdrożenie dokładnie takich samych zabezpieczeń w każdej części sieci, zapewniając w ten sposób scentralizowaną korelację zagrożeń i skoordynowaną ochronę w wielu obszarach infrastruktury informatycznej przedsiębiorstwa jednocześnie. Złożoność środowiska i różnice między różnymi ekosystemami sieciowymi utrudniają jednak to zadanie. Z tego względu firma Gartner zaczęła opowiadać się za szerokim zastosowaniem hybrydowych zapór Hybrid Mesh Firewall (HMF).



„Do 2026 r. ponad 60% przedsiębiorstw będzie korzystać z co najmniej jednego typu zapory, co będzie je skłaniać do wdrażania Hybrid Mesh Firewall ”[1]

Hybrid Mesh Firewall łączą w sobie zdolność do wdrażania krytycznych funkcji zapory NGFW w dowolnym miejscu sieci (kampusie, centrum danych oraz środowiskach wirtualnych/chmurowych i FWaaS/SASE) ze zdolnością do zdalnego, ujednoliconego zarządzania. W rezultacie powstaje zintegrowana platforma, która może objąć współczesne dynamiczne i rozproszone sieci, być w ich ramach skalowana i do nich się dostosowywać. Z poziomu swojej ujednoliconej konsoli zarządzania zapora HMF umożliwia koordynację ochrony we wszystkich domenach IT (witryny korporacyjne, chmury publiczne i prywatne oraz urządzenia pracowników zdalnych). Dzięki takiemu zintegrowanemu podejściu zespoły IT mogą zautomatyzować procesy wykrywania zagrożeń i reagowania na nie, orkiestrować konfiguracje oraz egzekwować zasady bez tracenia czasu na wykonywanie zadań ręcznych, zwłaszcza w obliczu niedoboru specjalistów z zakresu cyberbezpieczeństwa.

Potrzeba zapór HMF

Z przygotowanego przez firmę Gartner najnowszego badania Magic Quadrant dla zapór sieciowych wynika, że „do 2026 r. ponad 60% przedsiębiorstw będzie korzystać z co najmniej jednego typu zapory, co będzie je skłaniać do wdrażania Hybrid Mesh Firewall ”. Autorzy raportu dodają, że „wraz z ewolucją zapór sieciowych w kierunku Hybrid Mesh Firewall oraz pojawieniem się zapór chmurowych i modelu FaaS (Firewall-as-a-Service), wybór najbardziej odpowiedniego dostawcy staje się swoistym wyzwaniem”.

Wymienione poniżej rozwiązania mają za zadanie sprostać czterem najważniejszym wyzwaniom, przed którymi stoją dzisiejsze działy IT.

1. Zarządzanie złożoną infrastrukturą IT

Wiele z dzisiejszych zapór NGFW nie obsługuje funkcji HMF, co zmusza przedsiębiorstwa do zakupu oddzielnych zabezpieczeń dla witryn korporacyjnych, publicznych i prywatnych środowisk chmurowych oraz urządzeń pracowników zdalnych. W rezultacie pojawiają się niespójności na szczeblu operacyjnym, a zwłaszcza błędne konfiguracje, które mogą prowadzić do naruszeń bezpieczeństwa sieci.

2. Niedobór specjalistów ds. cyberbezpieczeństwa

Produkty punktowe nie tylko komplikują działanie, ale także zwiększają narażenie przedsiębiorstwa na ryzyko ze względu na długi czas wdrożenia. Wiele produktów punktowych wymaga od zajmujących się cyberbezpieczeństwem pracowników działu IT przeznaczenia kolejnych godzin na naukę nowych funkcji i paneli kontrolnych. Rodzi się tu kolejne, jeszcze większe ryzyko, ponieważ ponad jedna trzecia stanowisk związanych z cyberbezpieczeństwem pozostaje nieobsadzona ze względu na globalny niedobór specjalistów.

3. Wzrost liczby zaawansowanych zagrożeń

Złożoność i niedobory specjalistów ds. cyberbezpieczeństwa nie są jedynymi czynnikami stymulującymi zapotrzebowanie na zapory HMF. Na całym świecie istnieją realne, rosnące zagrożenia w postaci zaawansowanych cyberataków. Takie zaawansowane zagrożenia są coraz trudniejsze do wykrycia i coraz bardziej niszczycielskie dla przedsiębiorstw. 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 i uczenia maszynowego, które są niezbędne do ochrony przed znanymi i nieznanymi zagrożeniami. Dodanie do zapory HMF zabezpieczeń opartych na takich 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 HMF i mogą znacznie zmniejszyć nakłady pracy ręcznej związanej z ochroną korporacyjnej infrastruktury IT.

Co powinna oferować zapora Hybrid Mesh Firewall

Scentralizowane i ujednolicone zarządzanie

Najważniejszymi zaletami zapory HMF są zdolności do wykrywania zagrożeń, zarządzania zasadami i automatycznej orkiestracji reakcji na zagrożenia w dowolnym miejscu w sieci przy użyciu każdego dostępnego narzędzia. Jeśli oddzielne domeny, takie jak witryny korporacyjne, chmury publiczne i prywatne oraz urządzenia pracowników zdalnych, wymagają różnych paneli kontrolnych, oznacza to, że w przedsiębiorstwie nie używa się zapory HMF.

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 lokalizacji przedsiębiorstwa po chmurę i pracowników zdalnych. Ze względu na fakt, że różne przedsiębiorstwa mają różne wymagania w zakresie zarządzania rozproszonymi zaporami sieciowymi, obsługiwane muszą być wszystkie elementy, w tym urządzenia, maszyny wirtualne, usługi SaaS i zarządzane usługi zapór.

Zapora HMF 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 swoiste wyzwania związane z bezpieczeństwem. Witryny korporacyjne wymagają urządzeń, które mogą skalować zabezpieczenia, zapewniając spójną ochronę bez wpływu na doświadczenia użytkowników. Zapora HMF nigdy nie powinna być przyczyną powstawania wąskich gardeł w sieci.

Współczesne organizacje wymagają wysokiej wydajności, potrzebują zatem urządzeń wyposażonych w udoskonalone układy scalone specjalnego przeznaczenia (Application-Specific Integrated Circuits, ASIC), aby zwiększyć szybkość działania krytycznych zabezpieczeń. Urządzenie zabezpieczające oparte na niestandardowych układach ASIC może odciążyć wiele zasobochłonnych funkcji, takich jak funkcje zapory, VPN, IPS, a nawet SSL lub szczegółowej inspekcji pakietów (DPI). Dzięki temu witryny korporacyjne są chronione wielowarstwowymi zabezpieczeniami niewpływającymi na wydajność sieci.

Zapora natywna dla chmury

Zapora natywna dla chmury chroni obciążenia aplikacji w chmurze publicznej wdrożonych w środowiskach IaaS w modelu „Infrastructure-as-Code". Ponadto dodanie do środowiska chmurowego natywnej zapory HMF zmniejsza obciążenie związane z operacjami bezpieczeństwa sieci poprzez zwiększenie widoczności przy jednoczesnym wyeliminowaniu konieczności konfigurowania, utrzymywania i przydzielania zasobów do infrastruktury oprogramowania zapory. W rezultacie zespoły ds. bezpieczeństwa mogą skupiać się na zarządzaniu zasadami.

Zapora wirtualna

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 między chmurami. Zapory wirtualne w ramach zapory HMF umożliwiają budowę kompleksowego ekosystemu bezpieczeństwa dla definiowanego programowo centrum danych. Wspomagają wówczas proces konsolidacji, chroniąc jednocześnie środowisko przy użyciu różnych cyberzabezpieczeń wykraczających poza dynamiczne filtrowanie pakietów.

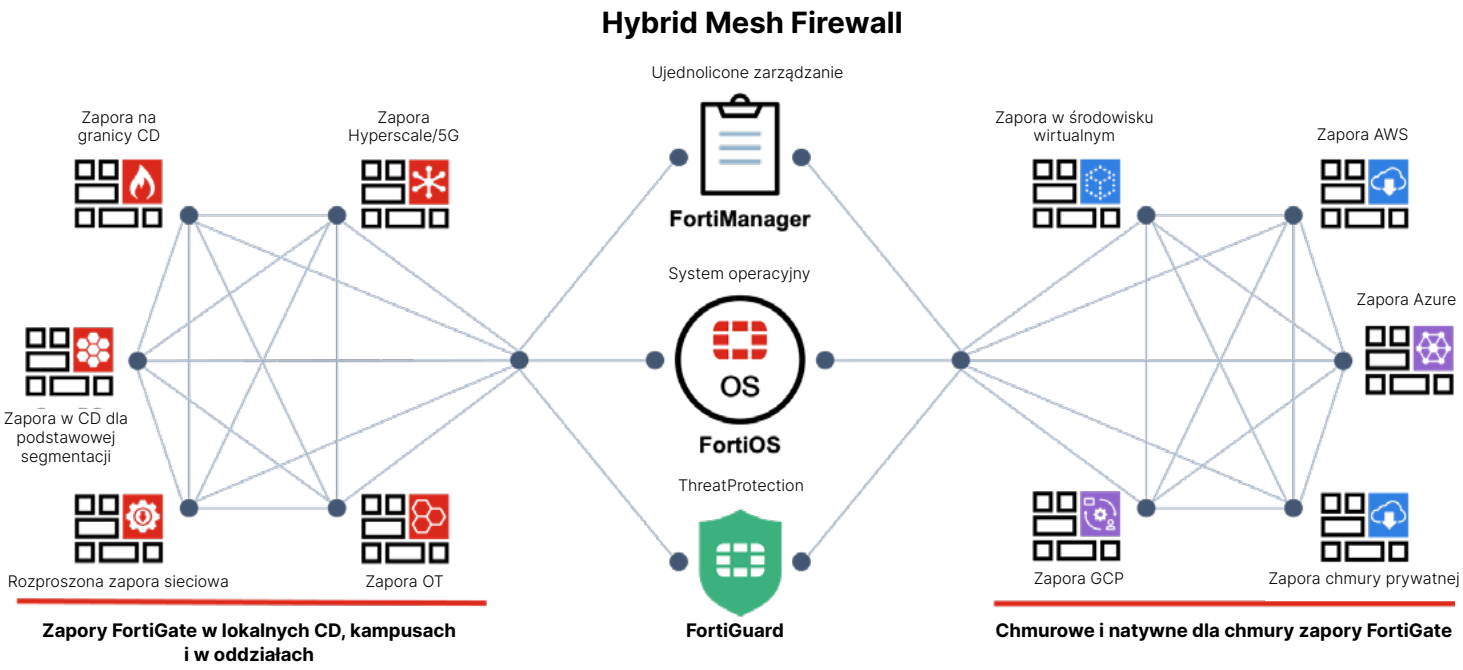
Zapora jako usługa

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 włamaniami (IPS) i zabezpieczenia DNS. Zapora HMF 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 zapór HMF jest natomiast pojedynczy system operacyjny, który konsoliduje liczne technologie i zastosowania w ramach uproszczonej struktury zarządzania i tworzenia polityk bezpieczeństwa. Podczas gdy ujednolicona konsola zarządzania konsoliduje operacje frontonu, pojedynczy system operacyjny zapewnia, że różne wdrożenia (urządzenia, wirtualne i natywne dla chmury zapory oraz agenty FWaaS), mogą ze sobą współdziałać w systemie zaplecza.



Korzyści z Hybrid Mesh Firewall

Hybrid Mesh Firewall 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 posiadania.

Wybór najlepszego rozwiązania Hybrid Mesh Firewall

Nie wszystkie przedsiębiorstwa rozumieją znaczenie zapory HMF. Przy tak dużym szumie marketingowym znalezienie o niej istotnych informacji może być dla potencjalnych klientów nie lada wyzwaniem. W wielu przypadkach to, co jest reklamowane jako zapora HMF, to raczej chaotyczny zestawem niekompletnych rozwiązań, niszowy produkt punktowy, który nie działa w każdym środowisku, tradycyjna zapora bez funkcji hybrydowych lub zbiór niewspółdziałających ze sobą rozwiązań.

Potrzebne jest zatem rozwiązanie, które łączy w sobie funkcje zapory NGFW, elastyczność szerokiej gamy formatów, wydajność i skalowalność wynikające z zastosowania zaawansowanych układów ASIC, wspólny system operacyjny zapewniający spójność i interoperacyjność między wdrożeniami, zaawansowane usługi oparte na sztucznej inteligencji, aby dostosować działania do najnowszych zagrożeń, oraz ujednolicone mechanizmy zarządzania, orkiestracji i reagowania. Taka zapora HMF (dostępna w różnych rodzajach obudowy) może następnie działać, korelować dane i reagować jako jednolite rozwiązanie w dowolnym miejscu, w dowolnym środowisku i przez cały czas.

[1] Gartner, „Magic Quadrant for Network Firewalls", Rajpreet Kaur, Adam Hils, Tom Lintemuth, 19 grudnia 2022 r.

FORTINET

www.fortinet.com

8 listopada 2023 10:25 AM

2133550-0-0-PL