LISTA KONTROLNA

10 ważnych kwestii dotyczących budowania zapory hybrydowej w topologii siatki

Współczesne zagrożenia wymagają nowego podejścia do zabezpieczeń sieci

Współcześni cyberprzestępcy — zarówno działający indywidualnie, jak i w ramach zorganizowanych grup przestępczych czy nawet na polecenie wrogich państw — są coraz bardziej wyrafinowani, sprawniej zorganizowani i lepiej finansowani[1]. Potwierdza to rosnąca liczba zagrożeń, takich jak zaawansowane ataki kierunkowe, ataki z użyciem oprogramowania typu ransomware i wiper — którym sprzyja wzrost popularności narzędzi typu „przestępstwo jako usługa" (Crime-as-a-Service, CaaS) — a także nowe ataki wymierzone w urządzenia nietradycyjne oraz coraz częstsze ataki wielopłaszczyznowe. Pojawiają się też nowe zagrożenia, wśród których warto wymienić ataki z użyciem sztucznej inteligencji oraz potencjalne obniżenie skuteczności narzędzi szyfrujących — będących podstawą większości współczesnych rozwiązań w dziedzinie cyberbezpieczeństwa — w wyniku działania komputerów kwantowych.

Zmiany nie dotyczą jednak wyłącznie zagrożeń. Trendy gospodarcze i społeczne o szerszym zasięgu skłaniają wiele firm do zmiany podejścia do kwestii bezpieczeństwa sieci w ramach nowych projektów transformacji cyfrowej. Internet rzeczy (Internet of Things, IoT), rozwój technologii chmur hybrydowych, ogromny wzrost zapotrzebowania na pracę zdalną, rozproszenie zasobów centrów danych i aplikacji, konwergencja technologii informatycznych (information technology, IT) i operacyjnych (operational technology, OT) oraz ciągły niedobór wykwalifikowanych specjalistów ds. zabezpieczeń to tylko niektóre z realiów, które zmuszają firmy do weryfikacji swoich strategii bezpieczeństwa.

Jednym z efektów tych zmian jest coraz powszechniejsza świadomość, że sieciowe narzędzia bezpieczeństwa — zwłaszcza zapory — nie mogą działać w izolacji. Powinny one współpracować, tworząc większą całość nazywaną zaporą hybrydową w topologii siatki (hybrid mesh firewall, HMF)[2]. Jest to ujednolicona platforma bezpieczeństwa zapewniająca skoordynowaną ochronę wielu obszarów infrastruktury IT firmy z uwzględnieniem komórek korporacyjnych, takich jak oddziały, kampusy, centra danych, chmury publiczne i prywatne czy pracownicy zdalni. Może ona stanowić podstawę szerszej struktury zabezpieczeń.

Aby osiągnąć ten cel, zapory HMF muszą być dostępne w różnych wariantach — jako urządzenia modularne, urządzenia dla dużych i małych placówek, maszyny wirtualne, zapory przeznaczone do chmur i rozwiązania w modelu „zapora jako usługa" (Firewall-as-a-Service, FWaaS). Dzięki temu można je wdrażać w dowolnym miejscu w sieci rozproszonej, skalować i dostosowywać w miarę rozbudowy sieci, a także płynnie integrować z innymi technologiami pod kątem współdzielenia kontekstu zabezpieczeń i stosowania automatyzacji.

Jedną z najważniejszych zalet zapory HMF jest możliwość objęcia działaniem popularnych obecnie środowisk wielochmurowych i hybrydowych centrów danych. Korzystając z ujednoliconej konsoli zarządzania, zapory HMF mogą koordynować ochronę w każdej domenie IT (komórki korporacyjne, chmury publiczne i prywatne oraz pracownicy zdalni). Dzięki temu firmowy dział IT może zautomatyzować swoje działania zabezpieczające, takie jak gromadzenie i korelowanie danych, wykonywanie dogłębnych analiz wspomaganych przez sztuczną inteligencję oraz koordynowanie spójnych reakcji w całej sieci bez duplikowania zadań, wielokrotnego tworzenia zasad czy marnowania czasu na ręczne wykonywanie zadań w sytuacji, gdy zasoby są ograniczone przez brak fachowców w dziedzinie cyberbezpieczeństwa.

Problem jednak w tym, że budowanie strategii opartej na zaporze HMF może być zniechęcające. Wiele firm uważa, że nie jest w stanie bez pomocy skutecznie zaprojektować, zbudować i wdrożyć działającego rozwiązania ze względu na mnóstwo opcji, niejasności i niekompletnych informacji. Dlatego właśnie przygotowaliśmy listę kontrolną, która ma ułatwić specjalistom ds. zabezpieczeń ocenę rozwiązań opartych na zaporach HMF oraz wybór oferujących je dostawców.

10 najważniejszych kwestii dotyczących budowania zapory Hybrid Mesh Firewall

Ocena możliwości wdrożenia zapór nowej generacji

Zapora Hybrid Mesh Firewall (HMF) to zintegrowany zestaw zapór nowej generacji (next-generation firewall, NGFW) wdrożonych w całej sieci i współpracujących ze sobą jako jedno rozwiązanie. Wśród typowych funkcji zapór NGFW warto wymienić głęboką inspekcję pakietów, IDS/IPS, inspekcję i kontrolę aplikacji, inspekcję ruchu SSL/SSH, filtrowanie witryn internetowych, zarządzanie jakością usług/przepustowością, a także wykrywanie szkodliwego oprogramowania i botnetów. Ponadto większość zapór NGFW udostępnia analizę zagrożeń, funkcje zabezpieczeń urządzeń mobilnych, zapobieganie utracie danych (data loss prevention, DLP), integrację z usługą Active Directory (AD), dynamiczną analizę (sandboxing) i otwartą architekturę, która pozwala firmom na dostosowanie kontroli aplikacji i integrację z szerszym ekosystemem powiązanych narzędzi i technologii.

Jednak biorąc pod uwagę obecny trend w kierunku pracy hybrydowej z naciskiem na mobilność, najbardziej zaawansowane zapory NGFW muszą również obsługiwać model zerowego zaufania, bezpieczną sieć SD-WAN i — co najważniejsze — funkcję natywnego działania jako aktywny składnik infrastruktury HMF.

Scentralizowane i ujednolicone zarządzanie

Integralną częścią każdej zapory HMF jest dobrze zaprojektowany system centralnego zarządzania, który pozwala efektywnie zarządzać rozproszoną i zintegrowaną architekturą bezpieczeństwa na jednym ekranie konsoli zarządzania. Najlepiej byłoby, gdyby to narzędzie obsługiwało zaawansowane funkcje analityczne i umożliwiało łatwą integrację z narzędziami zewnętrznymi — takimi jak Ansible (automatyzacja), Terraform (automatyzacja), ServiceNow (ITSM), Splunk (SIEM), Tufin (NSPM) itp. — w ramach wdrożeń na dużą skalę obejmujących rozwiązania wielu producentów. Wśród innych pożądanych funkcji warto wymienić scentralizowaną dystrybucję sygnatur zabezpieczeń, orkiestrację sieci SD-WAN w trybie nakładki, domeny administracyjne i automatyzację w środowisku wielu zapór.

Skuteczność

Aby system zabezpieczeń miał sens, musi być w stanie skutecznie wykrywać zagrożenia. Określenie skuteczności rozwiązań NGFW na własną rękę jest jednak trudne. Tu z pomocą przychodzą testy zewnętrzne. Jednym z wartościowych źródeł danych na temat skuteczności jest CyberRatings.org, organizacja non profit, której misją jest dbanie o transparentność i przejrzystość efektywności działania produktów i usług z zakresu cyberbezpieczeństwa. Raporty z testów zapór NGFW tych producentów, którzy zgodzili się na przetestowanie swoich produktów — jak firma Fortinet — są często dostępne na ich stronach internetowych. Z naszym najnowszym raportem można zapoznać się tutaj lub po zeskanowaniu kodu QR.

Automatyzacja

Aby skutecznie chronić się przed współczesnymi atakami, które są coraz szybsze i coraz bardziej zaawansowane, trzeba stosować zautomatyzowane rozwiązania sieciowe. Ich wdrożenie nie będzie jednak możliwe, gdy narzędzia rozmieszczone w różnych punktach sieci — w tym rozwiązania NGFW — będą od siebie odizolowane. Automatyzacja powinna umożliwiać aprowizowanie, konfigurowanie i optymalizowanie wszystkich urządzeń fizycznych i wirtualnych w sieci oraz zarządzanie nimi w ramach wspólnych procesów i oprogramowania. Automatyzując często używane funkcje oraz usprawniając i kontrolując powtarzalne procesy, można znacząco poprawić dostępność usług sieciowych i ogólny komfort korzystania z sieci.

Automatyzacja sieci pozwala ograniczyć liczbę błędów, poprawić skuteczność i w ostatecznym rozrachunku obniżyć koszty. Uwierzytelnianie i łączenie pracowników z siecią może odbywać się dynamicznie, co powinno wpłynąć na poprawę ogólnej produktywności w całej firmie. Dzięki funkcji automatycznej aprowizacji (ang. zero-touch provisioning) można szybko konfigurować nowe urządzenia i przygotowywać je do użycia przez pracowników, umożliwiając im praktycznie natychmiastowe rozpoczęcie pracy.

Sama automatyzacja sieci jednak nie wystarczy. Infrastruktura HMF powinna również obsługiwać automatyzację swoich funkcji zabezpieczeń. Automatyzacja zabezpieczeń umożliwia koordynację działań między różnymi składnikami siatki tworzącej zaporę w celu przyspieszenia wykrywania zdarzeń bezpieczeństwa i reagowania na nie. Konieczne jest monitorowanie zdarzeń występujących w dowolnym miejscu siatki oraz reagowanie w taki sposób, aby cała infrastruktura była chroniona.

Rozwiązania typu ASIC

Komórki korporacyjne i sprzęt w oddziałach firmy nie powinny ograniczać możliwości sieci. Jeśli jednak urządzenia i użytkownicy mają pracować szybko i wydajnie, w korporacyjnych sieciach i centrach danych we wdrożeniu HMF muszą działać rozwiązania zaprojektowane z myślą o skalowaniu funkcji zabezpieczeń. Jest to szczególnie istotne w przypadku wykonywania zadań wymagających dużej mocy obliczeniowej, takich jak sprawdzanie zaszyfrowanych danych czy streaming wideo, które stanowią ogromne obciążenie dla większości rozwiązań zabezpieczających.

Aby nie dopuścić do powstawania tego rodzaju „wąskich gardeł", trzeba zastosować lokalne rozwiązania sprzętowe z dedykowanymi układami scalonymi (application-specific integrated circuit, ASIC). Urządzenie zabezpieczające wyposażone w dedykowany układ ASIC może dzięki niemu odciążyć wiele funkcji bezpieczeństwa oraz sieciowych wymagających dużej ilości zasobów, takich jak zapora sieciowa, VPN, IPS, a nawet SSL lub głęboka inspekcja pakietów (DPI). Oznacza to, że komórki korporacyjne są chronione przez wielowarstwowe mechanizmy kontroli bezpieczeństwa, które nie mają negatywnego wpływu na wydajność i komfort użytkowania sieci.

Sztuczna inteligencja, uczenie maszynowe i analiza zagrożeń

Wraz ze wzrostem złożoności sieci i coraz liczniejszymi zagrożeniami konieczna jest skoordynowana ochrona. Zapory obejmujące różne obszary sieci nie są wystarczającym zabezpieczeniem. Aby skutecznie wykrywać znane i nieznane zagrożenia oraz chronić się przed nimi, trzeba wykorzystać możliwości sztucznej inteligencji i uczenia maszynowego (artificial intelligence/machine learning AI/ML).

Dzięki zabezpieczeniom wspomaganym przez AI/ML zapory HMF mogą identyfikować i klasyfikować aplikacje, adresy URL, użytkowników, urządzenia, szkodliwe oprogramowanie i nie tylko — jednocześnie automatyzując egzekwowanie zasad w różnych domenach. Sztuczna inteligencja i uczenie maszynowe stanowią podstawę funkcji automatyzacji zapór HMF i mogą znacznie ograniczyć konieczność ręcznego wykonywania zadań związanych z ochroną środowisk IT i OT w firmie.

Zapory różnych rodzajów i wielkości obsługiwane przez jeden system operacyjny

Nowoczesne firmy potrzebują zapór różnych rodzajów i różnej wielkości — od rozwiązań modularnych, z możliwością rozbudowy do dużych centrów danych i centrali korporacyjnych, przez urządzenia średniej wielkości do biur regionalnych i mniejsze urządzenia do oddziałów, aż po rozwiązania wirtualne do wdrożeń w chmurze prywatnej i publicznej. W niektórych przypadkach mogą być również potrzebne zapory przeznaczone do chmur i zapory FWaaS. Infrastruktura HMF musi być w stanie obsłużyć wszystkie te rozwiązania. Aby łatwiej było spełnić te wymagania, wszystkie rozwiązania powinny działać w tym samym systemie operacyjnym, a zarządzanie nimi powinno się odbywać w ramach tej samej platformy.

Elastyczne opcje cenowe zapór

Wraz z ewolucją potrzeb biznesowych firmy poszukują elastycznych możliwości wdrażania szerokiej gamy zapór sieciowych bez konieczności ograniczania się do jednego wariantu. Potrzebują też możliwości przenoszenia zasobów z miejsca na miejsce w miarę rozbudowy sieci. Elastyczne modele cenowe umożliwiają przystosowanie infrastruktury do zmiennych wymagań sieciowych, płacenie za faktycznie używane funkcje, dostosowywanie usług zabezpieczeń i efektywne zarządzanie budżetem. Oferują też większą elastyczność i kontrolę kosztów, co ma kluczowe znaczenie, gdy weźmie się pod uwagę dynamiczną i stale ewoluującą sytuację w obszarze bezpieczeństwa sieci.

Struktura bezpieczeństwa

Zapory HMF zapewniają solidną ochronę, ale są tylko częścią większej infrastruktury zabezpieczeń. Współczesne systemy zabezpieczeń wymagają również kompleksowej i zintegrowanej architektury cyberbezpieczeństwa, która zapewnia zaawansowaną ochronę i widoczność w całej infrastrukturze sieciowej. Podejście to musi uwzględniać pełną gamę rozwiązań bezpieczeństwa, w tym zapory, ochronę punktów końcowych, bezpieczny dostęp i zabezpieczenia chmurowe. Pozwala to uzyskać ujednolicony model składający się ze struktury i narzędzi, które mogą być podstawą nowoczesnego centrum operacji bezpieczeństwa (security operations center, SOC). Tego rodzaju struktura umożliwia wykrywanie zagrożeń i reagowanie na nie w czasie rzeczywistym, automatyzację zasad zabezpieczeń, centralizację konfiguracji i udostępnianie informacji o zagrożeniach w różnych składnikach systemu bezpieczeństwa, zapewniając spójną i skuteczną obronę przed cyberatakami.

Zacznij z zaufanym partnerem

Podejmując decyzje o zakupie systemów bezpieczeństwa, nie należy się ograniczać do kwestii technicznych. Warto pomyśleć o nawiązaniu partnerstwa, które może wykraczać poza cykl życia zakupionych produktów. Powinien to być partner, który może pochwalić się długą historią opracowywania innowacji i inwestowania nie tylko w technologię, ale także w usługi, wsparcie oraz — przede wszystkim — w badania nad bezpieczeństwem. Tylko wtedy będzie można skutecznie stawiać czoła cyberprzestępcom w miarę dalszego ewoluowania rozwiązań i strategii związanych z siecią i zabezpieczeniami. Dobrze jest wziąć pod uwagę takie wskaźniki, jak budżet na badania i rozwój, globalny zakres działalności, zweryfikowane dane analityczne, liczba zgłoszonych patentów, portfolio zintegrowanych rozwiązań oraz historia wykrywania zagrożeń typu zero-day.

Podsumowanie

Obecnie najlepszą praktyką jest zbudowanie infrastruktury bezpieczeństwa ze składników, które można połączyć w zaporę HMF. Ostatecznym celem powinno być utworzenie w pełni zintegrowanej struktury bezpieczeństwa łączącej zabezpieczenia i sieć w jednym rozwiązaniu. Zapory NGFW FortiGate firmy Fortinet zostały zaprojektowane od podstaw z myślą o infrastrukturze HMF, która z kolei może służyć jako podstawa szerszej struktury bezpieczeństwa, obejmującej szeroką gamę narzędzi zabezpieczających i sieciowych wyprodukowanych przez Fortinet i wielu naszych partnerów.

[1] Cyber Threat Predictions for 2023, FortiGuard Labs, 2022.

[2] Fortinet, „Hybrid Mesh Firewall", marzec 2023.

28 listopada 2023 11:47 AM

2197076-0-0-PL