OPIS ROZWIĄZANIA

Ochrona wdrożeń kampusowych za pomocą zapór NGFW Fortinet FortiGate

Streszczenie

Nowy model wdrożeń kampusowych znajduje zastosowanie w przypadku rozwijających się kampusów przedsiębiorstw i placówek edukacyjnych, w których trzeba połączyć i zabezpieczyć rosnącą liczbę budynków w ramach tej samej sieci. Odpowiednie zabezpieczenie sieci kampusu ma tu znaczenie decydujące, ponieważ pozwala na bezpieczny dostęp do Internetu i aplikacji wdrożonych w centrum danych i poszczególnych chmurach. Dobre zabezpieczenie sieci może skutecznie chronić ją przed zagrożeniami wewnętrznymi i zewnętrznymi, w tym przed nasilającymi się atakami za pomocą oprogramowania ransomware i command-and-control, które kryją się w zaszyfrowanych przepływach danych. Takie podejście wykracza daleko poza najważniejszą funkcję zabezpieczeń polegającą na zapobieganiu próbom penetracji sieci kampusu przez złośliwe oprogramowanie w drodze wykrywania, minimalizowania zakresu oraz powstrzymywania nieuniknionych ataków, którym udało się ominąć mechanizmy kontrolne na brzegu sieci.

Na bazie oferowanych przez firmę Fortinet zapór FortiGate NGFW przedsiębiorstwo może budować sieci oparte na zabezpieczeniach stanowiących integralną część architektury IT.

Szybsze łączenie technologii sieciowych i zabezpieczeń

Współczesne sieci charakteryzują się dużą dynamiką. Jednym z największych wyzwań dla nowoczesnej sieci jest obsługa pracowników zdalnych, niezależnie od tego czy pracują poza kampusem, czy też pracują, przemieszczając się po jego obszarze. W miarę rozszerzania się sieci przedsiębiorstwa poza granice kampusu, to raczej użytkownik, a nie sam brzeg sieci musi być szczególnie chroniony, i to bez wpływu na komfort jego pracy. Wraz z upowszechnianiem się różnych urządzeń i modeli pracy z każdego miejsca, powierzchnia ataku dramatycznie się zwiększa, ponieważ „podąża za użytkownikiem". Zabezpieczenia współczesnych sieci kampusowych muszą zatem kompleksowo chronić użytkowników w miejscu ich pracy, na bieżąco śledząc działanie aplikacji, procesów i innych działań, nawet jeśli miejsce pochodzenia i przeznaczenia danych zmienia się w połowie transakcji.

Taka zmiana paradygmatu, polegająca na odejściu od tradycyjnego modelu zabezpieczeń przypisanego do miejsca, wymaga zapewnienia większej widoczności i znajomości kontekstu wszędzie tam, gdzie znajduje się użytkownik (w sieci kampusu na kampusie, w sieci kampusu poza kampusem lub nawet poza siecią kampusu). Im więcej można zobaczyć, tym więcej można zabezpieczyć. Dobra widoczność to klucz do zapewnienia odpowiedniego stanu bezpieczeństwa sieci. Zapewnienie takiej proaktywnej ochrony we współczesnych środowiskach sieciowych charakteryzujących się dużą dynamiką wymaga jednak połączenia technologii sieciowych i zabezpieczeń w ramach jednego urządzenia. Podejście SDN (Security-Driven Networking, sieć oparta na zabezpieczeniach) jest coraz bardziej istotnym elementem działań mających na celu ochronę współczesnych złożonych sieci przy jednoczesnym utrzymaniu wydajności i komfortu pracy użytkowników. Jest to również kluczowa zaleta zapory następnej generacji (NGFW) Fortinet FortiGate.

Na bazie oferowanych przez firmę Fortinet zapór FortiGate NGFW przedsiębiorstwo może budować sieci oparte na zabezpieczeniach stanowiących integralną część architektury IT. W ten sposób można chronić każdy brzeg sieci w dowolnej skali, niezależnie od jego dynamiki, zapewniając jednocześnie większą widoczność oraz możliwość spójnego i skoordynowanego egzekwowania zasad w celu zagwarantowania wymaganej użyteczności sieci.

Wspomniane zapory Fortinet FortiGate są wyposażone w jedyne na świecie procesory SPU (Security Processing Unit), które zapewniają najwyższą w branży moc obliczeniową dla zaawansowanych zabezpieczeń warstwy 4 i 7. Oprócz szerokiego zestawu zaawansowanych i w pełni zintegrowanych funkcji bezpieczeństwa, zapory te oferują również szeroki wachlarz nowatorskich rozwiązań w ramach systemu FortiOS, takich jak zintegrowane rozwiązanie Zero Trust Network Access (ZTNA) oraz funkcje filtrowania filmów w czasie rzeczywistym. Urządzenia te zostały również rozszerzone o oparte na mechanizmach sztucznej inteligencji i uczenia maszynowego usługi FortiGuard, aby zapewnić intuicyjną, zautomatyzowaną i łatwą w zarządzaniu platformę NGFW. Zastosowane w tych urządzeniach innowacje pozwalają na lepsze zarządzanie ryzykiem, obniżenie kosztów i usprawnienie operacji, dzięki czemu klienci mogą dokonywać skalowania i unikać zakłóceń swojej działalności.

Ochrona, konsolidacja i automatyzacja dzięki zaporom NGFW Fortinet FortiGate

Ochrona — ograniczanie ryzyka związanego z bezpieczeństwem sieci kampusu bez uszczerbku dla jej użyteczności

Dla zespołów IT priorytetowe znaczenie ma ochrona sieci kampusu oraz zapewnienie jej dostępności i elastyczności. O ile jednak konieczność zapobiegania atakom jest niezmienna, zmieniają się środowiska wymagające ochrony. Zespoły zajmujące się siecią i zabezpieczeniami muszą mieć zatem pełną widoczność wdrożeń kampusowych, w tym wszystkich urządzeń i użytkowników, aby przeciwdziałać znanym i nieznanym zagrożeniom. Wymaga to połączenia technologii sieciowych i zabezpieczeń w ramach jednego rozwiązania zapewniającego odpowiednią widoczność i obsługę sieci. Im więcej urządzeń, użytkowników i aplikacji jest bowiem widocznych, tym większa jest znajomość kontekstu, co pomaga w tworzeniu lepszych i skuteczniejszych zasad. W uzupełnieniu takiej widoczności zapora FortiGate umożliwia zatem poznanie wspomnianego kontekstu, aby w ten sposób wzmocnić i utrzymać odpowiedni stan bezpieczeństwa w całej sieci kampusu.

W miarę podłączania do sieci kampusu coraz większej liczby urządzeń, zapora FortiGate może wykrywać i kontrolować urządzenia Internetu rzeczy (IoT), środowiska i systemy technologii operacyjnej (OT) oraz konkretnych użytkowników. Odbywa się to w ramach strategii gwarantowanego dostępu, która uwzględnia takie elementy, jak stan urządzenia, system operacyjny, status poprawek itp. W rezultacie można na bieżąco uwierzytelniać użytkowników dzięki zastosowaniu specjalnej technologii ZTNA, aby zapewniać spójne zasady bezpieczeństwa użytkownikom korzystającym z sieci na obszarze i poza obszarem kampusu.

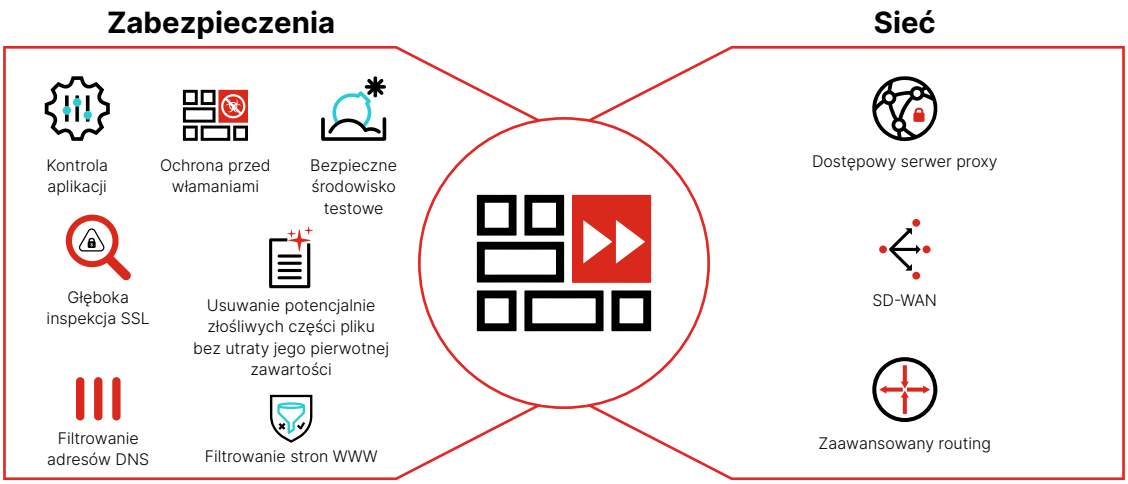
Kolejną wyjątkową strategią oferowaną przez zapory NGFW Fortinet FortiGate jest możliwość zmniejszenia powierzchni ataku dzięki użyciu zaawansowanych mechanizmów inspekcji, wdrożeniu dynamicznej segmentacji sieci oraz spójnego stosowaniu zasad w całej sieci kampusu. W ramach tej strategii można egzekwować zasady dostępu i ograniczać go do określonych zasobów dla poszczególnych użytkowników i na poziomie portów. Jest to możliwe dzięki integracji z oferowanymi przez Fortinet mechanizmami kontroli dostępu do sieci (NAC) oraz dzięki integracji architektury Security Fabric z przełącznikami i punktami bezprzewodowego dostępu Fortinet w celu zapewnienia szczegółowej kontroli dostępu. Ponadto można tu zbierać i reagować na informacje telemetryczne za pośrednictwem struktury wzajemnie połączonych zabezpieczeń w celu wykrywania zagrożeń wcześniej nieznanych (zero-day) i ataków za pomocą oprogramowania ransomware oraz zapobiegania im w czasie rzeczywistym, na podstawie informacji o zagrożeniach przekazywanych przez FortiGuard Labs.

Konsolidacja — obniżenie całkowitego kosztu posiadania sieci bez uszczerbku dla jej stanu bezpieczeństwa

Zespoły IT mogą lepiej chronić sieć kampusu, gdy korzystają z zabezpieczeń klasy korporacyjnej oferowanych w ramach najszybszego i najbardziej konkurencyjnego cenowo rozwiązania w branży. Zapora NGFW Fortinet FortiGate została zaprojektowana do obsługi funkcji wymagających dużej mocy obliczeniowej z szybkością wymaganą dla sieci, przedsiębiorstwo może zatem bez obaw konsolidować w zaporze FortiGate funkcje zapobiegania włamaniom (IPS), inspekcji SSL, ochrony aplikacji, filtrowania stron WWW, ochrony przed złośliwym oprogramowaniem itp. Wszystkie te funkcje mogą być uruchamiane jednocześnie bez uszczerbku dla przepustowości i dostępności sieci. Wynika to z zastosowania oferowanych przez zaawansowane procesory SPU dostępne w zaporach FortiGate innowacyjnych rozwiązań zwiększających wydajność.

Wszystko to jest oparte na systemie FortiOS, dzięki któremu całe portfolio produktów wspierających wizję sieci opartej na zabezpieczeniach (SDN) może być udostępnione w dowolnym środowisku i w dowolnej obudowie. Pozwala to na spójne wdrażanie zabezpieczeń kampusowych, w chmurze i w sieci rozległej, a nawet w kontenerach DevOps. Wdrażając jeden system zabezpieczeń w całej sieci, przedsiębiorstwo może zatem osiągnąć i utrzymać najwyższy poziom działania, bezpieczeństwa i obsługi sieci w ramach rozwiązań jednego dostawcy.

Konsolidacja funkcji w ramach zapór NGFW Fortinet FortiGate



Automatyzacja — uproszczenie operacji w celu zwiększenia widoczności i kontroli sieci

Zespoły IT muszą dostosowywać i skalować działania biznesowe w ramach powiększających się sieci. Aby robić to bezpiecznie, powinny zatem wdrażać nowe zabezpieczenia zapewniające kompleksową ochronę. Za pomocą narzędzia Fortinet Fabric Management Center (FMC), które kontroluje wszystkie wdrożone zapory FortiGate, zespoły te mogą usprawniać zarządzanie zaporami i zasadami w całej sieci kampusu oraz na wszystkich jej brzegach oraz zapewniać automatyczne aktualizacje wszystkich sieciowych urządzeń zabezpieczających z poziomu jednej konsoli.

W celu uproszczenia schematu zabezpieczeń warto skorzystać z interfejsów programowania aplikacji (API) i konektorów do architektury Fortinet Security Fabric w połączeniu z zaporą FortiGate, aby ujednolicić zabezpieczenia w wielu chmurach i zapewnić użytkownikom dostęp do aplikacji z dowolnego miejsca.

Zaawansowana funkcja zapory korzystająca z mechanizmów informowania o zagrożeniach w czasie rzeczywistym

Zapory NGFW muszą dokonywać filtrowania i inspekcji ruchu sieciowego w celu ochrony przedsiębiorstwa przed zagrożeniami wewnętrznymi i zewnętrznymi. Współczesne zapory NGFW mogą przeprowadzać głębszą inspekcję zawartości plików, aby identyfikować i blokować ataki typu „zero-day", ataki za pomocą oprogramowania ransomware lub zaawansowanego złośliwego oprogramowania oraz inne zagrożenia. Muszą również oferować mechanizmy inspekcji SSL (w tym TLS 1.3), kontroli aplikacji i zapobiegania włamaniom oraz zapewniać pełną widoczność całej powierzchni ataku. W miarę szybkich postępów w doskonaleniu metod włamań związanych z używaniem wielu chmur oraz umieszczaniem własnych serwerów i sprzętu sieciowego w zewnętrznych centrach danych, a także w miarę rozwoju przedsiębiorstw związanego z koniecznością zaspokajania coraz to większych potrzeb klientów i użytkowników, tradycyjne zapory NGFW nie są już zdolne do zapewnienia szeroko zakrojonej ochrony sieci. W efekcie spada użyteczność, zmniejsza się widoczność oraz pogarsza się stan bezpieczeństwa sieci. Współczesne zapory NGFW muszą zatem nie tylko blokować złośliwe oprogramowanie, ale również mieć możliwość skalowania wraz z siecią. Ponadto muszą zapewniać ścieżkę utrzymania elastyczności niezbędnej do podążania za zmianami w metodach włamań i zapewnienia bezpieczeństwa sieci w miarę pojawiania się nowych zagrożeń i wprowadzania nowych strategii sieciowych.

Zapory NGFW firmy Fortinet są wyjątkowo zdolne do wyprzedzania zmieniających się metod włamań, ponieważ nie tylko są wyposażone w specjalne procesory SPU i korzystają z zaawansowanego systemu operacyjnego FortiOS, ale również są zintegrowane z oferowanymi przez Fortinet mechanizmami informowania o zaawansowanych zagrożeniach oraz bazami danych organizacji badawczej FortiGuard Labs. Organizacja ta zatrudnia doświadczonych łowców zagrożeń, badaczy, analityków, inżynierów i danetyków oraz dysponuje najbardziej zaawansowanym na świecie systemem sztucznej inteligencji przeznaczonym do wykrywania i analizy zagrożeń. Jej misją jest przekazywanie klientom najlepszych w branży informacji o zagrożeniach, aby chronić ich przed złośliwymi cyberatakami. Misja ta jest realizowana w drodze przygotowywania raportów, aktualizowania informacji o zagrożeniach, współpracy z najlepszymi badaczami zagrożeń i organami ochrony porządku publicznego oraz codziennego przesyłania informacji o zagrożeniach do urządzeń FortiGate wdrożonych na całym świecie. Dzięki tym działaniom oferowane przez firmę Fortinet zabezpieczenia korzystają z najlepszych dostępnych informacji dotyczących identyfikacji zagrożeń i ochrony przed zagrożeniami, a klienci firmy Fortinet są na bieżąco informowani o najnowszych zagrożeniach, kampaniach, podmiotach i trendach, aby mogli podejmować proaktywne działania w celu lepszego zabezpieczenia swoich środowisk.

Zaawansowane zabezpieczenia każdego użytkownika, urządzenia i brzegu sieci

Zapora NGFW Fortinet FortiGate zapewnia przedsiębiorstwu kompleksową widoczność i bezpieczeństwo w celu ochrony dowolnego użytkownika, urządzenia lub brzegu sieci w dowolnej lokalizacji. Pozwala również wdrożyć architekturę opartą na zerowym zaufaniu, aby zagwarantować użytkownikom bezpieczny dostęp do aplikacji i zasobów niezbędnych do wykonywania pracy z dowolnego miejsca. W tym celu wykorzystuje mechanizmy, które umożliwiają na bieżąco uwierzytelniać użytkowników i urządzenia, efektywnie i dynamicznie monitorować zgodność z przepisami oraz elastycznie dostosowywać zabezpieczenia do zgłaszanych potrzeb.

Najlepsze w branży rozwiązania SDN firmy Fortinet bezproblemowo łączą w ramach jednej platformy zabezpieczenia, technologie sieciowe i niezbędne usługi FortiGuard oparte na mechanizmach sztucznej inteligencji i uczenia maszynowego. Takie zintegrowane podejście pozwala skuteczniej ograniczać ryzyko i dostosowywać się do wymogów współczesnych dynamicznych środowisk sieciowych, aby uniknąć zakłóceń prowadzonej działalności, wyeliminować złożoność wynikającą ze stosowania wielu produktów punktowych oraz osiągnąć najniższy w branży całkowity koszt posiadania (TCO). Wyjątkowa strategia SDN jest tutaj ściśle zintegrowana z infrastrukturą sieciową i architekturą zabezpieczeń przedsiębiorstwa, umożliwiając skalowanie i modyfikowanie sieci bez uszczerbku dla zabezpieczeń sieci i bez możliwości powstania luk w zabezpieczeniach, które mogłyby zostać wykorzystane przez nieupoważnione osoby.

Takie podejście następnej generacji jest niezbędne do skutecznej ochrony współczesnych, wysoce dynamicznych środowisk, ponieważ nie tylko zapewnia spójne egzekwowanie zasad w ramach dzisiejszych wysoce elastycznych brzegów sieci, ale także głęboko integruje zabezpieczenia z samą siecią.

Zabezpieczenia dostosowane do potrzeb konkretnego przedsiębiorstwa

Współczesne metody włamań ulegają ciągłym zmianom. Od ataków typu DDoS po ataki za pomocą oprogramowania ransomware, częstość, liczba i złożoność cyberataków nie wykazuje oznak spowolnienia. Każde przedsiębiorstwo potrzebuje zabezpieczeń dostosowanych do swojego niepowtarzalnego środowiska sieciowego, ponieważ nawet niewielkie zakłócenie działania infrastruktury sieciowej, choćby minuta przestoju lub opóźnienie w działaniu usługi, może narazić na szwank reputację, wyniki finansowe, a nawet długoterminową rentowność przedsiębiorstwa. Ponadto katastrofalne w skutkach cyberataki, których początkiem są często pozornie niegroźne włamania niewykryte przez stosowane zabezpieczenia sieciowe, mogą sprawić, że przedsiębiorstwo zostanie zmuszone do zapłacenia dotkliwych kar, a nawet do definitywnego zakończenia działalności. Problem w tym, że niewiele tradycyjnych zapór NGFW jest zdolnych do sprostania temu zadaniu.

Zapory NGFW Fortinet FortiGate zostały od podstaw zaprojektowane w celu zapewnienia skalowalnego poziomu bezpieczeństwa klasy korporacyjnej użytkownikom, brzegom sieci, kampusom, centrom danych, pracownikom zdalnym i chmurom. W miarę jak przedsiębiorstwa wychodzą poza centrum danych w związku z przejściem na hybrydowy system pracy i rosnącymi oczekiwaniami użytkowników, wdrożenie w kampusie staje się równie ważne jak główny użytkownik, przy czym zabezpieczenia muszą zapewniać bezproblemowe korzystanie przez użytkownika z różnych aplikacji, sieci i powiązanych funkcji.

Więcej informacji na ten temat można znaleźć pod adresem https://www.fortinet.com/products/next-generation-firewall.

7 lutego, 2022
1210304-0-1-PL