FORTINET

OPRACOWANIE

Przewodnik operatora sieci: segmentacja ukierunkowana na cele

Podstawowe praktyki w zakresie łagodzenia ryzyka i zachowania zgodności w obrębie powierzchni ataku



Streszczenie

Segmentacja sieci, urządzeń, użytkowników i aplikacji jest od dawna dobrą praktyką uzupełniania zabezpieczeń działających na granicy sieci (ang. edge security) oraz podziału płaskich sieci wewnętrznych. W przypadku liderów działalności związanej z inżynierią i eksploatacją sieci, priorytetowo traktujących łagodzenie ryzyka, osiąganie zgodności oraz skuteczne zarządzanie stanem zabezpieczeń, obecne podejście do segmentacji jest jednak niewystarczające.

W tradycyjnie stosowanych podejściach poziom kontroli dostępu jest za mało szczegółowy, aby spełnić wymagania biznesowe. Opierają się one na ocenach zaufania, które szybko tracą na aktualności, a przy tym bazują na założeniu, że ochrona przed zagrożeniami istnieje cały czas, nawet jeśli w rosnącej powierzchni ataku organizacji są poważne luki. Taki charakter środowiska sieciowego sprawia, że operatorzy sieci nie są w stanie aktywnie zarządzać stanem zabezpieczeń — pozostawiają więc swoją organizację otwartą na większe ryzyko związane z bezpieczeństwem.

Gdy środowiska wielochmurowe, podejście „mobile-first", Internet Rzeczy (IoT) i inne inicjatywy związane z transformacją cyfrową powodują gwałtowne zwiększanie się powierzchni ataku, segmentacja ukierunkowana na cele (ang. intent-based segmentation) oferuje istotnie nowe podejście. Pozwala ono wyeliminować obecne wady segmentacji i sprawdza się w wielu różnych scenariuszach kontroli dostępu.



Jak przedsiębiorstwo może oczekiwać przejrzystej, kompleksowej widoczności, jeśli stosuje średnio 75 różnych narzędzi zapewniających bezpieczeństwo?[1]



Efektywna segmentacja musi bazować na celach biznesowych — to pomaga ustalić miejsce, sposób i zakres działań („gdzie?", „co?, i „jak?") niezbędnych do skutecznego egzekwowania zabezpieczeń.

Podstawowe zasady segmentacji ukierunkowanej na cele

Segmentacja ukierunkowana na cele (ang. intent-based segmentation) pozwala skutecznie przełożyć cele organizacji zarządzającej siecią na konkretne zasady dotyczące miejsca, sposobu i zakresu segmentacji zabezpieczeń:

- **Miejsce** („gdzie?") określa położenie granic między segmentami oraz logikę segmentowania zasobów IT.
- **Sposób** („jak?") ukierunkowuje działanie sieci na cel biznesowy poprzez silnie rozdrobnioną kontrolę dostępu, realizowaną w sposób ciągły na podstawie adaptacyjnej oceny zaufania.
- **Zakres** („co?") wymusza kontrolę dostępu poprzez zastosowanie wysokowydajnych, zaawansowanych zabezpieczeń (warstwa 7) w całej sieci.

Te trzy elementy działają w kontekście zintegrowanej struktury składników zabezpieczeń, która łączy się i komunikuje z innymi urządzeniami sieciowymi i infrastrukturalnymi. W ten sposób, bez zmiany architektury sieci, można skutecznie poprawić stan zabezpieczeń, łagodzić ryzyko oraz wspierać zgodność i efektywność operacyjną w całym przedsiębiorstwie.

Segmentacja pozwalająca spełniać cele biznesowe

Segmentacja ukierunkowana na cele wspiera dominujące **architektury makro- i mikro-segmentacji,** a także **segmentację na poziomie aplikacji, procesów i urządzeń końcowych**. Segmentując płaską sieć za pomocą jednej z tych technik segmentacji, operator sieci może tworzyć mniejsze powierzchnie ataku, którymi łatwiej zarządzać i które mogą być dodatkowo chronione za pomocą wysokowydajnych, zaawansowanych zabezpieczeń (warstwa 7).

Segmentacja ukierunkowana na cele umożliwia operatorom sieci tworzenie domen bezpieczeństwa lub segmentów zgodnie z celami biznesowymi. Aby jednak osiągać cel biznesowy, segmentacja musi zapewniać bardziej rozdrobioną kontrolę dostępu bazującą na **tożsamości użytkowników lub logice biznesowej**. Niezbędna jest także możliwość dostosowania kontroli dostępu na podstawie aktualnych ocen zaufania — poprzez przeszukiwanie zewnętrznej bazy danych, w której takie oceny są systematycznie rejestrowane.

Adaptacyjne oceny zaufania jako warunek świadomego zarządzania ryzykiem

W podejściach tradycyjnych kontrola dostępu bazuje na założeniu, że zaufanie wobec użytkowników, urządzeń i aplikacji jest niezmienne. W rzeczywistości wiarygodność wszystkich tych elementów często się zmienia, czy to w wyniku normalnych zmian w działalności gospodarczej, czy też w związku z nowo powstającymi zagrożeniami. Ponieważ zmiany w poziomie zaufania dramatycznie wpływają na stan zabezpieczeń w organizacji i nieodłącznie z nim związane ryzyko w sieci, stosowanie statycznych ocen zaufania sprawia, że operatorzy sieci są niebezpiecznie niedoinformowani.

Dlatego segmentacja ukierunkowana na cele łączy kontrolę dostępu ze stale aktualizowanymi poziomami zaufania. W bardziej kompleksowych rozwiązaniach opartych na segmentacji ukierunkowanej na cele informacje te pozyskiwane są zarówno ze źródeł wewnętrznych, jak i zewnętrznych.

Segmentacja ukierunkowana na cele daje lepszy wgląd w ryzyko nieodłącznie związane z siecią i opiera się na zdolności ciągłego oceniania stanu zabezpieczeń. **Usługi oceny zabezpieczeń** pozwalają zweryfikować konfigurację bezpieczeństwa sieci i umożliwiają analizę ryzyka oraz podatności na zagrożenia. Zapewniają również najlepsze praktyki w zakresie korygowania błędów w konfiguracji. Pozwalają też śledzić stan zabezpieczeń w czasie, porównać ogólny stan zabezpieczeń organizacji z innymi podobnymi podmiotami oraz oceniać go w odniesieniu do przyjętych standardów bezpieczeństwa. Organizacje powinny więc szukać rozwiązań oferujących aktualne informacje o zagrożeniach oraz funkcje oceny bezpieczeństwa w czasie rzeczywistym, zapewniające pełną widoczność podatności na zagrożenia na całej powierzchni ataku z poziomu jednego panelu. Dodatkowo, dzięki możliwościom oceny bezpieczeństwa, zespoły ds. inżynierii i eksploatacji sieci mogą nadawać priorytet korygowanym lukom w zabezpieczeniach oraz wskazywać nowe zagrożenia w miarę pojawiania się zmian, zarówno wewnątrz, jak i na zewnątrz sieci.



72% ruchu internetowego jest obecnie szyfrowane, a cyberprzestępcy wykorzystują go do infiltracji sieci i kradzieży danych.



Ze względu na zaawansowanie zagrożeń czołowi operatorzy sieci muszą stale oceniać stan zabezpieczeń w swoich środowiskach.

Skuteczna, wszechobecna ochrona przed zagrożeniami

W wielu organizacjach, które stosują kontrolę dostępu, brakuje wszystkich elementów bezpieczeństwa niezbędnych, aby ją skutecznie egzekwować. Te elementy, które są dostępne, niekoniecznie są zaś zintegrowane. Utrudnia to operatorom sieci wykrywanie rozwijających się zagrożeń oraz odpieranie ataków, zanim osiągną swój cel i doprowadzą do zainfekowania całego systemu.

SSL zawsze włączone w całej sieci. Aby skutecznie egzekwować politykę dostępu i bronić całej powierzchni ataku, w ramach segmentacji ukierunkowanej na cele zaleca się wysoce opłacalną i wysokowydajną zaawansowaną ochronę przed zagrożeniami (warstwa 7) oferowaną przez zapory nowej generacji (NGFW), których integralną funkcją jest inspekcja SSL.

Ponieważ 72% ruchu internetowego jest obecnie szyfrowane, kontrolowanie ruchu szyfrowanego za pomocą SSL lub w warstwach transportowych (TLS) staje się koniecznością[2]. Narażenie na działanie złośliwego oprogramowania, takiego jak Heartbleed, Poodle i Zeus pokazało, jak bardzo standard szyfrowania jest podatny na ataki[3]. Mimo to wiele organizacji obawia się wdrożenia pełnej inspekcji SSL ze względu na jej potencjalnie szkodliwy wpływ na przepustowość sieci i doświadczenia użytkowników. Dlatego zapory NGFW stosowane w segmentacji ukierunkowanej na cele powinny być wyposażone w **specjalnie skonstruowane, wysokowydajne procesory**, które pozwolą zminimalizować ograniczenie przepustowości. Dzięki temu funkcja inspekcji SSL we wszystkich zaporach NGFW może być zawsze włączona.

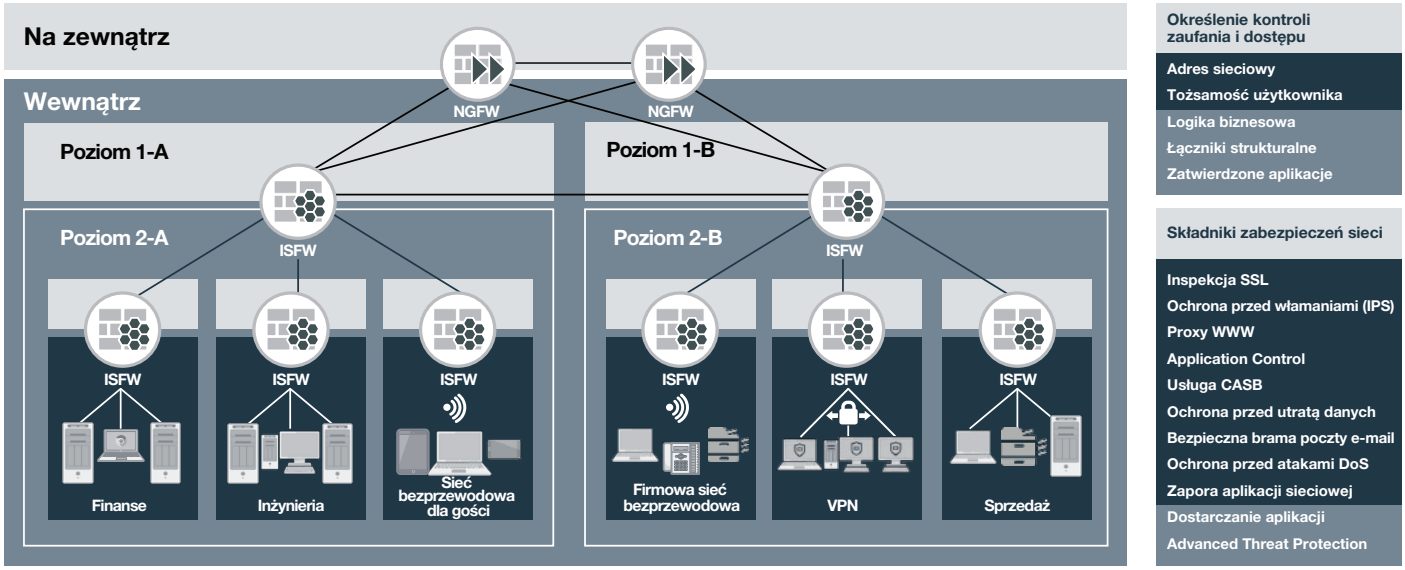
Ważną zasadą segmentacji ukierunkowanej na cele jest możliwość stosowania ochrony przed zagrożeniami wszędzie tam, gdzie jest potrzebna: zarówno w oddziałach firmy, jak i we wszystkich wykorzystywanych przez organizację środowiskach chmurowych. Niektórzy czołowi operatorzy sieci mogą się obawiać potencjalnych kosztów wdrożenia takich zasad. Wybór zapory NGFW od dostawcy oferującego różne rozwiązania fizyczne i wirtualne oraz zróżnicowane gęstości portów pozwala jednak zminimalizować całkowity koszt posiadania (TCO). Dzięki temu wdrożenie tego podejścia w całej organizacji staje się wykonalne.

Kompleksowe zarządzanie. Wdrożenie różnorodnych rozwiązań w zakresie ochrony przed zagrożeniami w całej sieci wymaga efektywnej, kompleksowej widoczności i właściwego zarządzania. Aby proaktywnie chronić całą sieć przed zagrożeniami pochodzącymi z dowolnej jej części, rozwiązania w zakresie segmentacji ukierunkowanej na cele powinny być wdrażane jako część zintegrowanej struktury bezpieczeństwa. Musi ona zapewnić kompleksowy wgląd w informacje i spójne środki kontroli zgodności z zasadami we wszystkich punktach egzekwowania zabezpieczeń.

Przypadki zastosowania

Segmentacja ukierunkowana na cele sprawdza się w wielu różnych scenariuszach kontroli dostępu. Poniżej podano dwa przykłady ilustrujące, w jaki sposób odpowiednia klasyfikacja kontroli dostępu oraz zaawansowana, wysokowydajna ochrona przed zagrożeniami dają lepszą kontrolę nad architekturą bezpieczeństwa i pomagają skuteczniej łagodzić ryzyko.

Przypadek zastosowania: zmniejszenie powierzchni ataku



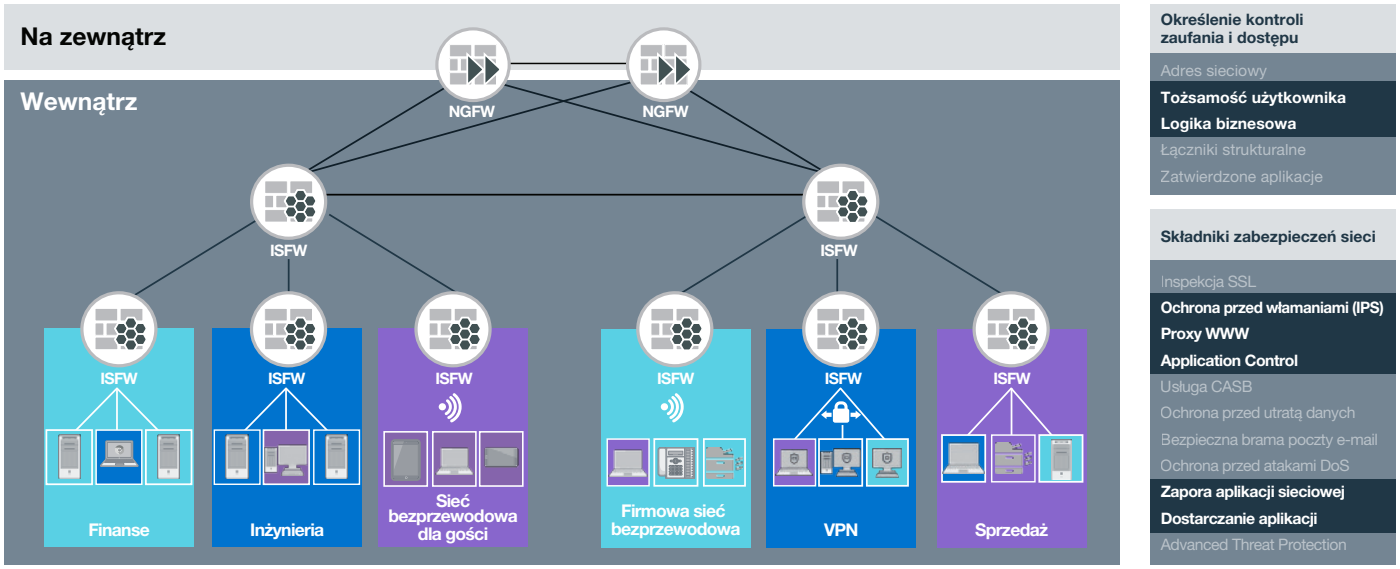
Rysunek 1. Przypadek zastosowania: łagodzenie ryzyka poprzez zmniejszenie powierzchni ataku

Jeżeli chodzi o ochronę zasobów sieciowych, większość przedsiębiorstw nie może polegać wyłącznie na zabezpieczeniach działających na granicy sieci. W razie naruszenia zabezpieczeń — czy to z powodu błędów konfiguracji, zainfekowania urządzeń łączących się z siecią wewnętrzną, czy też ataków „zero day" omijających kontrole bezpieczeństwa — w sieci muszą stale funkcjonować **dodatkowe warstwy obrony** (pokazane na rysunku 1 na granicach między poziomami 1 i 2, a także w obrębie poziomu 2).

Te dodatkowe zapory z segmentacją wewnętrzną wykorzystują różne środki kontroli bezpieczeństwa w celu powstrzymania wszelkich szkodliwych działań w chronionych przez nie strefach. Uwierzytelnianie opiera się w tym przypadku zazwyczaj na identyfikatorze zasobu (adresie sieciowym) lub tożsamości użytkownika. Warto podkreślić, że wprowadzenie segmentacji zabezpieczeń nie wymaga zmiany samej architektury sieci.

Wszystkie zapory komunikują się ze sobą i z jednopanelowym systemem zarządzania, co zapewnia pełną widoczność ruchu w sieci. Strukturalny system zarządzania pozwala skonsolidować działania w zakresie ochrony przed zagrożeniami z uwzględnieniem wszystkich składników zabezpieczeń, tworząc pełną ścieżkę audytu.

Przypadek zastosowania: osiągnięcie zgodności



Rysunek 2. Przypadek zastosowania: reagowanie na złożone wymogi dotyczące zgodności

Zachowanie zgodności z przepisami państwowymi i branżowymi to rzadko kwestia opcjonalna. Ze względów praktycznych trudno jednak rekonfigurować sieć za każdym razem, gdy zmienią się zasady lub wejdą w życie nowe przepisy.

Na przykład segmentacja zasobów na potrzeby zgodności ze standardem PCI DSS (Payment Card Industry Data Security Standard) poprzez wyodrębnienie podsieci finansowej (rysunek 2), byłaby niezwykle trudna. W rzeczywistych organizacjach nie wszystkie urządzenia w podsieci finansowej mogą podlegać wymogom zgodności z PCI; niektóre urządzenia podlegające PCI mogą natomiast znajdować się w innych podsieciach, a nawet w odległych lokalizacjach.

Dzięki segmentacji ukierunkowanej na cele zasady dostępu można definiować i egzekwować za pomocą połączonych strukturalnie składników zabezpieczeń. Zasobom i użytkownikom można przydzielać odpowiednie oznaczenia odnoszące się do zachowania zgodności ze standardem PCI — niezależnie od ich lokalizacji w sieci i od innych kontroli zgodności lub zasad dostępu mających do nich zastosowanie.

Podsumowanie

Segmentacja ukierunkowana na cele jest podejściem nowym, ale stanowi rozwiązanie gotowe do zastosowania w środowiskach produkcyjnych. Produkty i usługi niezbędne do wdrożenia tego podejścia są szeroko dostępne, a lista połączonych strukturalnie składników ochrony przed zagrożeniami stale się wydłuża.

Liderów w zakresie inżynierii i eksploatacji sieci zachęcamy do wdrażania rozwiązań potwierdzających skuteczność segmentacji ukierunkowanej na cele — albo poprzez naśladowanie przedstawionych tu przypadków zastosowania, albo poprzez wykorzystanie własnych wymagań biznesowych. Fortinet zademonstruje na życzenie, jak krok po kroku i w sposób mierzalny wprowadzić segmentację ukierunkowaną na cele, wdrażając kluczowe składniki i łącząc je z technologiami sieciowymi, które istnieją już w organizacji.

[1] Kacy Zurkus, „Defense in depth: Stop spending, start consolidating", CSO Online, 14 marca, 2016 r.

[2] „Q3 2018 Threat Landscape Report", Fortinet, 6 listopada, 2018 r.

[3] Ananda Rajagopal, „How SSL encryption gives a false sense of security", CSO Online, dostęp uzyskano 4 lutego, 2019 r.

FORTINET®

www.fortinet.com

Copyright © 2019 Fortinet, Inc. Wszelkie prawa zastrzeżone. Fortinet®, FortiGate®, FortiCare®, FortiGuard® oraz niektóre inne znaki są zastrzeżonymi znakami towarowymi spółki Fortinet, Inc. Pozostałe nazwy związane z Fortinet zawarte w niniejszym dokumencie również mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi Fortinet. Wszelkie inne nazwy produktów lub spółek mogą być znakami towarowymi ich odpowiednich właścicieli. Przedstawione w niniejszym dokumencie parametry wydajności i inne dane uzyskano podczas testów laboratoryjnych w warunkach idealnych, faktyczna wydajność może być zatem inna. Na wartość parametrów wydajności mogą mieć wpływ zmienne sieciowe, różnorodne środowiska sieciowe i inne uwarunkowania. Żadne ze stwierdzeń zawartych w tym dokumencie nie stanowi wiążącego zobowiązania ze strony Fortinet, a Fortinet odrzuca wszelkie wyraźne lub dorozumiane gwarancje i rękojmie, z wyjątkiem gwarancji udzielonych przez Fortinet na mocy wiążącej umowy z kupującym podpisanej przez głównego radcę prawnego Fortinet, w której Fortinet zagwarantuje, że określony produkt będzie działać zgodnie z wyraźnie wymienionymi w takim dokumencie parametrami wydajności, a w takim przypadku wyłącznie określone parametry wydajności wyraźnie wskazane w takiej wiążącej umowie pisemnej będą wiązać Fortinet. Wszelka tego typu gwarancja będzie dotyczyć wyłącznie wydajności uzyskiwanej w takich samych warunkach idealnych, w jakich Fortinet przeprowadza wewnętrzne testy laboratoryjne. Fortinet w całości odrzuca wszelkie wyraźne lub dorozumiane przyrzeczenia, oświadczenia i gwarancje związane z tym dokumentem. Fortinet zastrzega sobie prawo do zmieniania, modyfikowania, przenoszenia lub innego korygowania niniejszej publikacji bez powiadomienia (zastosowanie ma najnowsza wersja publikacji).

348072-0-1-PL 26 czerwca, 2019 9:32 AM

D:\PROJECTS2\Fortinet\P-344049\04_DTP (2019-06-26)\Work\WP-Solution-research-network-director-EN-A4_source-files\WP-Solution-research-network-director-PL-A4