OPIS ROZWIĄZANIA

Uproszczenie działania rozwiązań SD-WAN dzięki zarządzaniu z poziomu jednej konsoli

Streszczenie

Definiowane programowo sieci rozległe (SD-WAN) szybko zastępują tradycyjne sieci rozległe w kontekście obsługi zdalnych lokalizacji i oddziałów. O ile rozwiązania SD-WAN zapewniają wydajność potrzebną do obsługi innowacji cyfrowych, wiele z nich nie udostępnia jednak skonsolidowanych funkcji zabezpieczeń i obsługi sieci. W efekcie wiele przedsiębiorstw musiało wdrożyć dodatkowy złożony zestaw narzędzi służących do ochrony wdrożonych rozwiązań SD-WAN i zarządzania nimi. W takiej sytuacji trzeba jednak zastosować podejście uproszczone, które poprawi efektywność, ograniczy ryzyko i nie nadwyręży budżetu. Każde z tych wymagań spełnia rozwiązanie FortiGate Secure SD-WAN, ponieważ udostępnia zarówno zapory następnej generacji (NGFW), jak i zintegrowane mechanizmy analizy i zarządzania na potrzeby centralizacji i uproszczenia utrzymania wdrożonych rozwiązań SD-WAN.

Fortinet upraszcza działanie rozwiązań SD-WAN (FortiGate, FortiManager, FortiAnalyzer)

- Bezobsługowe wdrożenie
- Scentralizowane zarządzanie
- Raportowanie i analityka
- Raporty dotyczące zgodności
- Integracja i automatyzacja

Wspomaganie innowacji przy jednoczesnym zabezpieczaniu rozwijających się przedsiębiorstw

Przedsiębiorstwa rozproszone wdrażają innowacje cyfrowe (m.in. aplikacje SaaS i oparte na protokole IP usługi przesyłania obrazu i dźwięku) w celu zwiększenia wydajności, poprawy komunikacji i wspomagania szybkiego rozwoju prowadzonej działalności. Stosowane w wielu oddziałach i odległych lokalizacjach tradycyjne architektury sieci rozległej nie są jednak w stanie sprostać wymaganiom komunikacyjnym tych nowych technologii. Zaowocowało to coraz szerszym wdrażaniem rozwiązań SD-WAN, które wykorzystują bardziej przystępne cenowo połączenia internetowe. Przewiduje się, że skumulowany roczny wskaźnik wzrostu przychodów (CAGR) na globalnym rynku sieci SD-WAN wzrośnie do 2022 r. o ponad 40%, a wartość tego rynku osiągnie 4,5 mld USD[1].

Z ankiety firmy Gartner wynika, że „dla 72% respondentów priorytetem w kontekście sieci rozległej jest bezpieczeństwo”[3].

Gartner

O ile jednak rozwiązania SD-WAN poprawiają przepustowość sieci, mogą również narażać przedsiębiorstwo na większe ryzyko. Z przeprowadzonego przez firmę Gartner badania wynika, że „w kontekście sieci rozległej klienci nadal chcą poprawiać jej wydajność i widoczność, ale priorytetem jest teraz bezpieczeństwo”[2].

W wielu przedsiębiorstwach potrzeba zabezpieczenia rozwiązań SD-WAN sprawiła, że osoby zarządzające siecią zaczęły wdrażać różne narzędzia i produkty punktowe, aby w ten sposób reagować na pojawiające się zagrożenia, wymogi regulacyjne lub innego rodzaju potrzeby. Podejście to zwiększa jednak złożoność infrastruktury i utrudnia nią zarządzanie, tworząc jednocześnie nowe luki w zabezpieczeniach na brzegach sieci.

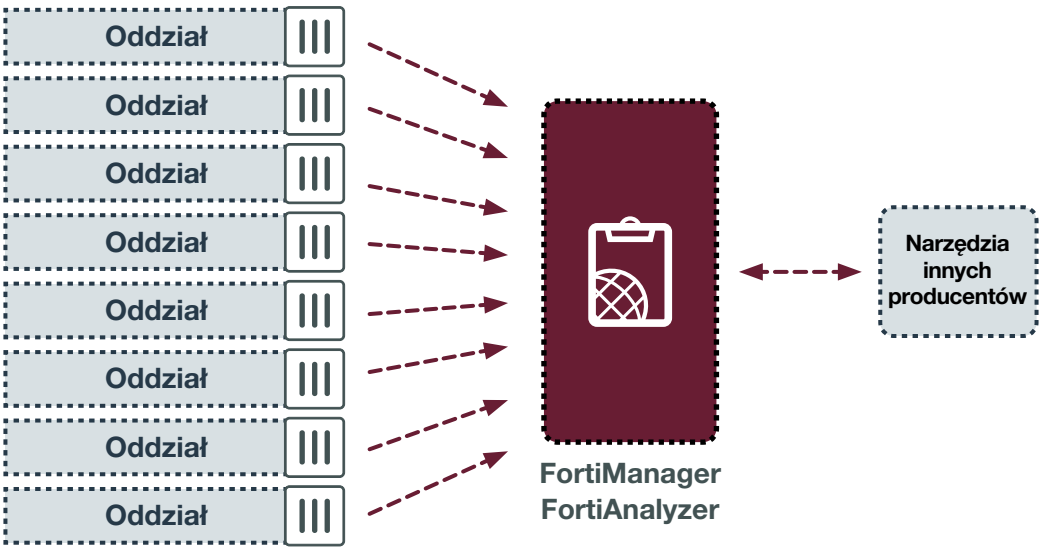
Narzędzia Fortinet upraszczają i zabezpieczają wdrożenia rozwiązań SD-WAN

Konsolidacja funkcji sieciowych i bezpieczeństwa na potrzeby rozwiązań SD-WAN eliminuje złożoność zdezagregowanej infrastruktury oddziałowej. Działanie to nie tylko zmniejsza powierzchnię ataku na przedsiębiorstwo, ale również upraszcza pracę działu IT bez uszczerbku dla wdrażania kolejnych inicjatyw cyfrowych.

Jako zintegrowana część architektury Fortinet Security Fabric, rozwiązania **FortiGate Secure SD-WAN** mogą korzystać z funkcji narzędzi **FortiManager** i **FortiAnalyzer** (urządzeń lub maszyn wirtualnych), aby upraszczać działanie rozwiązań SD-WAN w kilku krytycznych obszarach.

Bezobsługowe wdrożenie

Rozwiązanie Secure SD-WAN przedsiębiorstwo może wdrożyć za pomocą narzędzia FortiManager w ciągu kilku minut. Udostępniane przez to narzędzie funkcje bezobsługowego wdrożenia sprawiają, że wystarczy podłączyć urządzenia FortiGate do sieci w oddziale, a potem cała konfiguracja zostanie wykonana przez narzędzie FortiManager automatycznie z głównej siedziby za pośrednictwem połączenia szerokopasmowego. Pozwoli to uniknąć czaso- i kosztochłonnego wysłania personelu technicznego na miejsce wdrożenia. W celu przyspieszenia wspomnianego wdrożenia w oddziałach i zdalnych lokalizacjach mogą być również zastosowane jako szablony istniejące konfiguracje rozwiązań SD-WAN.



Rysunek 1. Rozwiązanie SD-WAN w konfiguracji z zaporami FortiGate NGFW oraz produktami FortiManager i FortiAnalyzer.

Scentralizowane zarządzanie w przedsiębiorstwie rozproszonym

Ponad połowa (52%) wszystkich naruszeń wynika z błędów ludzkich lub błędów systemu (reszta wynika z działań przestępców)[5]. Scentralizowane zarządzanie wszystkimi rozproszonymi sieciami w całym przedsiębiorstwie pomaga osobom zarządzającym siecią radykalnie ograniczyć możliwości wystąpienia błędów konfiguracyjnych prowadzących do narażenia sieci na ryzyko cyberataku lub awarii.

Wspomniane scentralizowane, skalowalne zarządzanie w rozwiązaniach FortiManager i FortiAnalyzer odbywa się z poziomu **jednej konsoli**. Oferowane przez Fortinet narzędzia do zarządzania mogą obsługiwać znacznie większe wdrożenia niż konkurencyjne rozwiązania (nawet do 100 tys. urządzeń FortiGate). Dzięki takim funkcjom, jak stosowanie szablonów na potrzeby konfiguracji rozwiązań SD-WAN i NGFW, zarządzanie konfiguracją klasy korporacyjnej i kontrola dostępu oparta na rolach, osoby zarządzające siecią mogą łatwiej ograniczać ludzkie błędy.

Z testów NSS Labs wynika, że za pomocą oferowanej przez rozwiązanie FortiGate Secure SD-WAN funkcji bezobsługowego wdrożenia można skonfigurować sieć w oddziale przedsiębiorstwa w czasie krótszym niż sześć minut[4].

Raportowanie i analiza w rozwiązaniu SD-WAN

Wraz ze wzrostem liczby oddziałów w przedsiębiorstwie i zwiększaniem się powierzchni ataku na brzegu sieci osoby zarządzające siecią muszą w coraz większym stopniu polegać na analizach prowadzonych w czasie rzeczywistym, aby jak najszybciej określać i identyfikować zagrożenia dla bezpieczeństwa sieci. Rozwiązanie FortiAnalyzer udostępnia tu kompleksowe dane dotyczące m.in. ruchu sieciowego, aplikacji sieciowych i ogólnego stanu sieci.

Ponadto oferuje **raporty i zestawienia dotyczące monitorowania przepustowości** rozwiązań SD-WAN, **możliwości rejestrowania i monitorowania historii poziomów usług** za pomocą zestawień, wykresów i raportów, funkcje konfigurowania powiadomień dotyczących poziomów usług, a także raporty dotyczące używania aplikacji i pulpitów. Ponadto rozwiązanie FortiAnalyzer oferuje **adaptacyjne narzędzia do obsługi reakcji** na zdarzenia dotyczące rozwiązania SD-WAN oraz możliwości rejestrowania i archiwizacji zdarzeń związanych z poziomem usług w różnych aplikacjach i interfejsach.

Raporty dotyczące zgodności

Klienci potrzebują niestandardowych raportów i narzędzi, aby potwierdzić audytorom przestrzeganie przepisów. Zarządzanie zgodnością od zawsze jest jednak dla działu IT kosztownym i pracochłonnym procesem, który często wymaga zaangażowania wielu pełnoetatowych pracowników oraz wielu miesięcy pracy w celu agregacji i normalizacji danych pochodzących z różnych zabezpieczeń punktowych.

Rozwiązania Fortinet przyspieszają proces raportowania zgodności, ponieważ upraszczają infrastrukturę bezpieczeństwa i eliminują konieczność stosowania wielu procesów ręcznych. FortiAnalyzer udostępnia **konfigurowalne szablony regulacyjne** oraz **wstępnie sformatowane raporty** dla takich standardów, jak PCI DSS (Payment Card Industry Data Security Standard), SAR (Security Activity Report), CIS (Center for Internet Security) i NIST (National Institute of Standards and Technology). Ponadto FortiAnalyzer udostępnia funkcje rejestracji **audytów** i **mechanizmy kontroli dostępu oparte na rolach (RBAC)**, aby zapewnić pracownikom dostęp tylko do tych informacji, których potrzebują do wykonywania swojej pracy.

Jako rozszerzenie funkcji rozwiązania FortiAnalyzer, usługa **FortiGuard Security Rating Service** uruchamia audyty pomagające działowi IT w identyfikacji krytycznych luk w zabezpieczeniach i słabych stron w konfiguracji architektury Security Fabric oraz wdrożeniu zalecanych najlepszych praktyk. W ramach wspomnianej usługi osoby zarządzające siecią mogą porównać stan zabezpieczeń swojego przedsiębiorstwa ze stanem zabezpieczeń innych firm z branży[6].

Integracja i automatyzacja

Z punktu widzenia efektywności zabezpieczenia muszą być płynnie zintegrowane w każdym obszarze rozproszonego przedsiębiorstwa, w tym w każdym jego oddziale i zdalnym biurze. Osoby zarządzające siecią muszą mieć pełną widoczność całej powierzchni ataku z jednej lokalizacji. Ponadto potrzebują narzędzi umożliwiających zautomatyzowaną reakcję na zagrożenia, aby skrócić czas od wykrycia ataku do usunięcia jego skutków oraz odciążyć personel działu IT od uciążliwych zadań ręcznych.

Rozwiązanie FortiManager pozwala skrócić czas usuwania skutków ataku z kilku miesięcy do kilku minut, dzięki koordynacji **opartych na politykach zautomatyzowanych reakcji** w ramach Fortinet Security Fabric — zintegrowanej architektury zabezpieczeń, która pozwala na automatyzację procesów związanych z zapewnieniem bezpieczeństwa i przekazywaniem informacji o zagrożeniach. Wysłany z jednego oddziału alert o wykrytym incydencie wraz z kontekstem pozwala administratorowi sieci na szybkie określenie sposobu dalszego postępowania w celu ochrony całego przedsiębiorstwa przed potencjalnym skoordynowanym atakiem. Niektóre zdarzenia mogą również zainicjować automatyczne zmiany konfiguracji urządzeń w celu natychmiastowego przeciwdziałania skutkom ataku.

Zgodność z przepisami nie oznacza bezpieczeństwa. Najbardziej odporne na cyberzagrożenia są przedsiębiorstwa, dla których wspomniana zgodność jest tylko podstawą[7].

Rozwiązania FortiAnalyzer i FortiManager automatyzują również wiele zadań realizowanych w ramach rozwiązań SD-WAN, aby odciążyć personel dział IT. Oba te produkty **mogą zostać zintegrowane z rozwiązaniami innych firm**, takimi jak systemy SIEM, zarządzanie usługami IT (ITSM) i DevOps (np. Ansible, Terraform), aby pozostawić bez zmian istniejące procesy i nie rezygnować z posiadanych zabezpieczeń i narzędzi sieciowych.

Korzyści, prosta obsługa i bezpieczeństwo

Dzięki połączeniu rozwiązań FortiGate Secure SD-WAN, FortiManager i FortiAnalyzer można nie tylko wdrożyć zabezpieczenia klasy korporacyjnej oraz odpowiednie funkcje sieciowe w oddziałach, ale również uzyskać następujące korzyści:

Niższy całkowity koszt posiadania (TCO). Zintegrowane podejście Fortinet do opartego na zabezpieczeniach rozwiązania SD-WAN obniża całkowity koszt posiadania (TCO) dzięki zmniejszeniu liczby wymaganych do zakupu narzędzi sieciowych i zabezpieczających, przy jednoczesnym ograniczeniu kosztów operacyjnych w wyniku uproszczenia zarządzania i automatyzacji procesów. Przejście na publiczne łącza szerokopasmowe oznacza zastąpienie drogich łączy MPLS przystępniejszymi cenowo opcjami. W tym przypadku FortiGate Secure SD-WAN zapewnia najniższy w branży całkowity koszt posiadania (TCO), nawet dziesięciokrotnie niższy niż w przypadku konkurencyjnych rozwiązań[8].

Większa wydajność. Jednocześnie Fortinet wprowadza dla rozwiązań SD-WAN uproszczoną infrastrukturę, która zmniejsza złożoność operacyjną zarówno w oddziale, jak i w całym rozproszonym przedsiębiorstwie. Rozwiązaniem FortiGate Secure SD-WAN można zarządzać z poziomu jednej, intuicyjnej konsoli. Dzięki rozwiązaniu FortiManager urządzenia FortiGate są gotowe do działania zaraz po podłączeniu. FortiManager umożliwia konfigurację scentralizowanych polityk i informacji o urządzeniach, a urządzenia FortiGate są automatycznie aktualizowane do najnowszej takiej konfiguracji. Wspomniana możliwość zarządzania z poziomu jednej konsoli obejmuje skalowalną zdalną kontrolę sieci i zabezpieczeń we wszystkich zdalnych lokalizacjach i oddziałach przedsiębiorstwa.

Ograniczenie ryzyka. Oferowane przez Fortinet funkcje śledzenia i raportowania pomagają przedsiębiorstwom w zapewnieniu zgodności z przepisami prawa ochrony prywatności, standardami bezpieczeństwa i przepisami branżowymi oraz zmniejszają ryzyko poniesienia kar i kosztów prawnych w przypadku naruszenia przepisów. FortiAnalyzer śledzi aktywność zagrożeń w czasie rzeczywistym, ułatwia ocenę ryzyka, wykrywa potencjalne problemy oraz pomaga neutralizować ich skutki. Dzięki ścisłej integracji z systemem FortiGate Secure SD-WAN umożliwia monitorowanie polityk zapór i pomaga zautomatyzować prowadzenie audytów zgodności w rozproszonych infrastrukturach przedsiębiorstwa.

Fortinet oferuje prawdziwe rozwiązanie SD-WAN oparte na zabezpieczeniach

Istnieje wiele zastosowań technologii SD-WAN opartych na zabezpieczeniach, podejście Fortinet sprawia, że rozwiązania Fortinet są najbardziej efektywne dla każdego typu projektu SD-WAN. Uproszczenie działania tych rozwiązań ma kluczowe znaczenie dla ich pomyślnego wdrożenia i rozbudowy w celu wsparcia inicjatyw z zakresu innowacji cyfrowych. Rozwiązania FortiGate Secure SD-WAN, FortiManager i FortiAnalyzer oferują najlepsze w swojej klasie funkcje zarządzania i analizy SD-WAN, dzięki którym osoby zarządzające siecią mogą obniżyć koszty operacyjne i ryzyko na brzegach sieci.

Średni koszt naruszenia ochrony danych (3,92 mln USD) rośnie wskutek złożoności systemu (+290 tys. USD), ale spada wskutek korzystania z informacji o zagrożeniach (-240 tys. USD) i analiz bezpieczeństwa (-200 tys. USD)[9].

[1] „SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022", IDC, 7 sierpnia 2018 r.

[2] Naresh Singh, „Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth", Gartner, 12 listopada 2018 r.

[3] „Fortinet Secure SD-WAN: Best-of-Breed NGFW and SD-WAN in a Single Offering", Gartner, listopad 2018 r.

[4] Ahmed Basheer, „Software-Defined Wide Area Network Test Report: Fortinet FortiGate 61E", NSS Labs, 19 czerwca 2019 r.

[5] „2018 Cost of a Data Breach Study", Ponemon Institute, lipiec 2018 r.

[6] „Proactive, Actionable Risk Management with the Fortinet Security Rating Service", Fortinet, 5 kwietnia 2019 r.

[7] Frances Dewing, „Compliance Is Not Security: Why You Need Cybersecurity Chops In The Boardroom", Forbes, 15 sierpnia 2019 r.

[8] „Fortinet SD-WAN gives the performance of a lifetime", Fortinet, 9 sierpnia 2018 r.

[9] „2019 Cost of a Data Breach Report", Ponemon Institute and IBM, lipiec 2019 r.

FORTINET®

www.fortinet.com

września2,20201:38PM

476710-0-1-PL