OPIS ROZWIĄZANIA

Uproszczenie operacji SD-WAN w środowiskach OT w celu uzyskania niezawodnej łączności

Streszczenie

Definiowane programowo sieci rozległe (SD-WAN) zaczynają zastępować tradycyjne sieci rozległe w oddziałach korzystających z technologii operacyjnej (OT). O ile rozwiązania SD-WAN zapewniają niezawodne połączenia służące do obsługi innowacji cyfrowych, wiele z nich nie udostępnia jednak skonsolidowanych funkcji zabezpieczeń i obsługi sieci zoptymalizowanych pod kątem działania w trudnych warunkach. Przedsiębiorstwa, które chcą wdrożyć rozwiązanie SD-WAN w swoich fabrykach, podstacjach lub np. na platformach wiertniczych, musiały łączyć ze sobą oddzielne produkty punktowe. W takiej sytuacji potrzebne jest natomiast podejście uproszczone, które poprawi efektywność, ograniczy ryzyko i nie nadwyręży budżetu. Wymagania te spełnia rozwiązanie Fortinet FortiGate Rugged Secure SD-WAN, które udostępnia zarówno przygotowane do działania w trudnych warunkach otoczenia zapory następnej generacji (NGFW), jak i zintegrowane mechanizmy analizy i zarządzania na potrzeby centralizacji i uproszczenia operacji SD-WAN.

Wdrażanie innowacyjnych rozwiązań w rozproszonych obiektach produkcyjnych

Fabryki, podstacje elektryczne i platformy wiertnicze wdrażają innowacyjne rozwiązania cyfrowe (m.in. aplikacje SaaS i aplikacje działające w czasie rzeczywistym, na przykład służące do przesyłania obrazu i dźwięku) w celu zwiększenia wydajności, poprawy komunikacji i wspomagania szybkiego rozwoju prowadzonej działalności. Stosowane w oddziałach tradycyjne architektury sieci rozległej nie są jednak w stanie sprostać za rozsądną cenę wymaganiom komunikacyjnym tych nowych technologii. Zaowocowało to coraz szerszym wdrażaniem architektur SD-WAN, które wykorzystują przystępniejsze cenowo bezpośrednie połączenia internetowe. Wartość skumulowanego rocznego wskaźnika wzrostu przychodów (CAGR) na rynku sieci SD-WAN wzrosła o 110% z 841 mln USD w 2018 r. do 1,77 mld USD w 2019 r.[1].

O ile jednak rozwiązania SD-WAN pozytywnie wpływają na niezawodność połączeń, 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.

Fortinet umożliwia korzystanie z rozwiązania SD-WAN w środowisku OT dzięki w pełni zintegrowanemu rozwiązaniu i narzędziu Fabric Management Center

- Zapora następnej generacji (NGFW)
- Funkcje SD-WAN
- Wzmocniona konstrukcja wytrzymująca wyższe temperatury, mocniejsze wibracje i większe zakłócenia elektromagnetyczne
- Bezobsługowe wdrożenie
- Scentralizowane zarządzanie
- Raportowanie i analityka
- Raporty dotyczące zgodności
- Integracja i automatyzacja

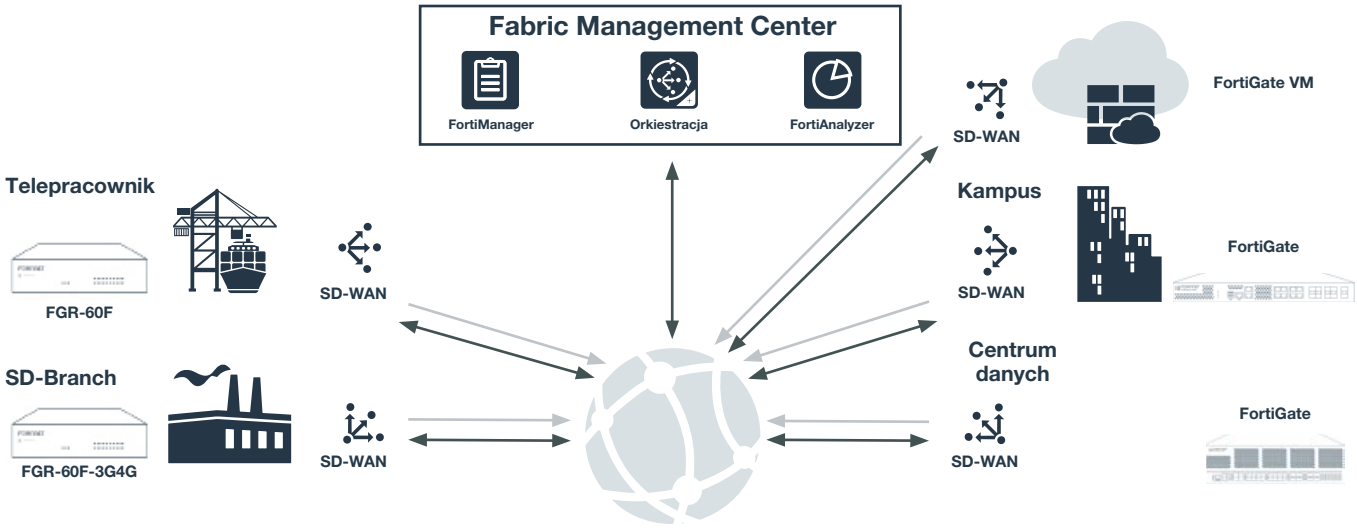
Z ankiety firmy Gartner wynika, że „dla 72% respondentów priorytetem w kontekście sieci rozległej jest bezpieczeństwo”[3].

Gartner

Narzędzia Fortinet upraszczają i zabezpieczają wdrożenia rozwiązań SD-WAN

Konsolidacja funkcji zabezpieczeń i obsługi sieci na potrzeby rozwiązań SD-WAN usprawnia proces ich wdrożenia w wielu oddziałach, w których panują niekontrolowane warunki otoczenia. Działanie to nie tylko zmniejsza powierzchnię ataku na przedsiębiorstwo, ale również upraszcza pracę działu IT bez uszczerbku dla wdrażania kolejnych innowacyjnych rozwiązań cyfrowych.

Jako zintegrowany element narzędzia Fabric Management Center, rozwiązanie FortiGate Rugged Secure SD-WAN może być zarządzane z poziomu jednej konsoli zapewnianej przez narzędzie SD-WAN Orchestrator (oferowane w pakiecie z narzędziem FortiManager)



Rysunek 1. Zapory Rugged FortiGate umożliwiają zarządzanie operacjami SD-WAN z poziomu jednej konsoli.

oraz udostępniać rozszerzone funkcje analityczne i ulepszone funkcje raportowania w ramach narzędzia FortiAnalyzer. Dzięki temu klienci mogą znacznie uprościć proces scentralizowanego wdrożenia, skorzystać z oszczędzającej czas automatyzacji oraz zastosować reguły ukierunkowane na działalność biznesową.

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

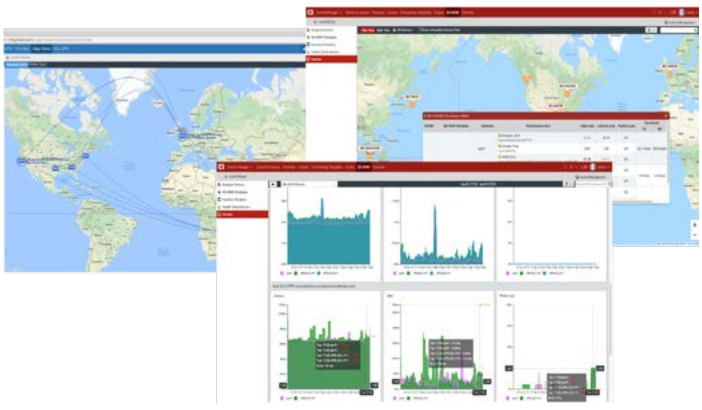
Bezobsługowe wdrożenie

Rozwiązanie FortiGate Rugged Secure SD-WAN przedsiębiorstwo może wdrożyć za pomocą narzędzia Fabric Management Center 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 centrali 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.

Scentralizowane zarządzanie w przedsiębiorstwie rozproszonym

Scentralizowane zarządzanie wszystkimi sieciami rozproszonymi w całym przedsiębiorstwie pomaga osobom zarządzającym siecią znacząco ograniczyć możliwości wystąpienia błędów konfiguracji, które mogą skutkować narażeniem na ryzyko cyberataku i awarii sieci.

Rozwiązanie Secure SD-WAN Orchestrator wchodzi w skład narzędzia Fabric Management Center, co pozwala klientom znacznie uprościć scentralizowane wdrożenie, skorzystać z oszczędzającej czas automatyzacji oraz zastosować reguły ukierunkowane na działalność biznesową. 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.



Raportowanie i analityka w rozwiązaniu SD-WAN

Rozszerzone funkcje analityczne dotyczące dostępności łączy sieci rozległej, uzgodnionych poziomów wydajności, ruchu aplikacji w środowisku uruchomieniowym oraz statystyk historycznych pozwalają zespołowi ds. infrastruktury na szybkie identyfikowanie i rozwiązywanie problemów z siecią. Fabric Management Center udostępnia zaawansowane funkcje telemetryczne związane z widocznością aplikacji i działaniem sieci co również przyspiesza rozwiązywanie problemów i przyczynia się do spadku liczby

zgłoszeń pomocy technicznej. Generowane na żądanie raporty SD-WAN udostępniają wymagane dla zapewnienia zgodności dodatkowe informacje na temat metod włamań, poziomu zaufania i dostępu do zasobów.

Ponadto Fabric Management Center udostępnia **raporty i zestawienia dotyczące monitorowania przepustowości** rozwiązań SD-WAN, **możliwości zapisywania w dzienniku i monitorowania historii poziomów usług** za pomocą zestawień, wykresów i raportów, funkcje konfigurowania powiadomień dotyczących poziomów usług, a także raporty i pulpity dotyczące używania aplikacji. Oferuje również **adaptacyjne narzędzia do obsługi reakcji** na zdarzenia dotyczące rozwiązania SD-WAN oraz możliwości zapisywania w dzienniku 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. Fabric Management Center udostępnia **konfigurowalne szablony regulacyjne** oraz **wstępnie sformatowane raporty** dla takich standardów, jak SAR (Security Activity Report), CIS (Center for Internet Security) i NIST (National Institute of Standards and Technology). Ponadto Fabric Management Center 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 Fabric Management Center, 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[5].

Zgodność z przepisami nie oznacza bezpieczeństwa. Najbardziej odporne na cyberzagrożenia są przedsiębiorstwa, dla których wspomniana zgodność jest tylko podstawą[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 Fabric Management Center 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 łagodzenia skutków ataku.

Rozwiązania FortiAnalyzer i Fabric Management Center automatyzują również wiele zadań realizowanych w ramach rozwiązań SD-WAN, aby odciążyć personel działu 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

Fabric Management Center oferuje zabezpieczenia klasy korporacyjnej oraz odpowiednie funkcje sieciowe w oddziałach, którym towarzyszą 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 Rugged Secure SD-WAN zapewnia najniższy w branży całkowity koszt posiadania (TCO), nawet dziesięciokrotnie niższy niż w przypadku konkurencyjnych rozwiązań[7].

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)[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 Rugged 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 Rugged 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. Rozwiązanie FortiGate Secure SD-WAN z narzędziem Fabric Management Center oferuje najlepsze w swojej klasie funkcje zarządzania i analizy SD-WAN, dzięki którym osoby zarządzające siecią mogą obniżyć koszty operacyjne i ryzyko na brzegach sieci.

[1] „Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q19 and 2019, Table 16.1", Gartner, marzec 2020 r.

[2] „Fortinet Recognized as a 2020 Gartner Peer Insights Customers' Choice for WAN Edge Infrastructure", Fortinet, 26 marca 2020 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] „Proactive, Actionable Risk Management with the Fortinet Security Rating Service", Fortinet, środa, 8 lipca 2020 r.

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

[7] „Fortinet Placed Highest in Ability to Execute in the Challengers Quadrant of the 2019 Gartner Magic Quadrant for WAN Edge Infrastructure", Fortinet, 4 grudnia 2019 r.

[8] „2019 Cost of a Data Breach Report", Ponemon Institute i IBM, 23 lipca 2019 r.

FORTINET®

www.fortinet.com

Copyright © 2020 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).

lutego 16, 2021 6:05 PM

476710-B-1-PL