TRZY PRZYPADKI TRANSFORMACJI ODDZIAŁÓW PRZEDSIĘBIORSTWA ZA POMOCĄ TECHNOLOGII FORTINET SECURE SD-WAN

OPRACOWANIE



STRESZCZENIE

Transformacja cyfrowa (DX) tradycyjnych sieci w oddziałach oferuje szereg korzyści dla rozproszonego przedsiębiorstwa. Wiele przedsiębiorstw zastępuje swoje sieci rozległe o ograniczonej wydajności sieciami rozległymi definiowanymi programowo (SD-WAN), które zapewniają szybsze połączenia, oszczędności i inne korzyści. Sieciom SD-WAN towarzyszą jednak również określone wyzwania. Oferowane przez firmę Fortinet zapory następnej generacji (NGFW) FortiGate obejmują technologię Secure SD-WAN, która w ramach jednego rozwiązania zapewnia zarówno funkcje sieciowe, jak i funkcje zabezpieczeń. Funkcje te pozwalają uzyskać odpowiedni poziom widoczności i kontroli aplikacji oraz wysokiej jakości połączenia audio i wideo, a także umożliwić skonsolidowane zarządzanie sieciami i zabezpieczeniami w oddziałach oraz zapewnić zaawansowaną ochronę przed zagrożeniami. Na trzech poniższych przykładach przedstawiono sposób, w jaki rozwiązania firmy Fortinet pozwalają skorzystać ze wszystkich zalet architektury SD-WAN bez uszczerbku dla bezpieczeństwa sieci.

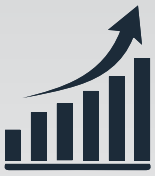


WSTĘP

Transformacja cyfrowa zmusza kierownictwo przedsiębiorstwa do oceny kosztów, ryzyka i zdolności związanych z posiadaną architekturą sieci. Tradycyjne sieci rozległe korzystają z prywatnych łączy MPLS, które są drogie, ale wydajne. Większość tradycyjnych sieci rozległych ma architekturę „hub-and-spoke", która przekierowuje ruch sieciowy z oddziałów z powrotem do głównego centrum danych przedsiębiorstwa na potrzeby filtrowania i kontroli bezpieczeństwa przesyłanych danych.

O ile proces ten (ang. „backhauling") jest bezpieczny, znacznie jednak spowalnia działanie sieci, do czego dochodzą jeszcze wymagania dotyczące transformacji cyfrowej zwiększające obciążenia związane z ruchem z oddziałów w rozproszonych przedsiębiorstwach. Przedsiębiorstwa poszerzają zakres stosowania aplikacji SaaS (Software-as-a-Service), jak również innych narzędzi chmurowych takich jak narzędzia VoIP (Voice-over-IP) i technologie wideokonferencyjne. Przesył dźwięku i obrazu stwarza duże wymagania dla zasobów sieciowych, zwłaszcza w obliczu zgłaszanych przez użytkowników w przedsiębiorstwie dużych oczekiwań co do bardzo wysokiej jakości i wydajności tego typu usług.

Sieci SD-WAN rozwiązują wspomniane wyżej problemy związane z kosztami przepustowości i opóźnieniami w ruchu, umożliwiając przedsiębiorstwu zastąpienie łączy MPLS publicznymi łączami szerokopasmowymi (na przykład 4G/LTE i 5G). Sieć SD-WAN kieruje ruch sieciowy z oddziałów do chmury, centrali lub innych oddziałów, zapewniając bezpośredni dostęp do aplikacji i usług chmurowych. Sprawia to, że sieci SD-WAN są bardzo popularnym wyborem w kontekście transformacji przedsiębiorstw. Jak ostatnio zauważyli analitycy firmy Gartner „...zgodnie z naszą najnowszą prognozą wydatki użytkowników końcowych na rozwiązania SD-WAN wzrosną z 475 mln USD w 2017 r. do 2,32 mld USD w 2022 r. przy pięcioletnim skumulowanym wskaźniku wzrostu na poziomie 37,4%"[1].



Według naszych najnowszych prognoz wydatki użytkowników końcowych na rozwiązania SD-WAN wzrosną z 475 mln USD w 2017 r. do 2,32 mld USD do 2022 r., przy pięcioletnim skumulowanym wskaźniku wzrostu na poziomie 37,4%.



WYZWANIA DOTYCZĄCE SIECI SD-WAN

Sieć SD-WAN oferuje z natury szybsze i tańsze połączenia niż tradycyjne sieci rozległe, nie zapewnia jednak sama wszystkich oczekiwanych korzyści. Mimo jej zdolności do transformacji działania sieci w oddziałach, należy jeszcze rozwiązać kilka problemów, aby w pełni skorzystać z jej potencjału:

Brak widoczności. Sieć SD-WAN zazwyczaj nie zapewnia widoczności aplikacji na poziomie oddziałów. Może to prowadzić do pojawiania się w sieci aplikacji niezatwierdzonych przez dział IT (Shadow IT), w tym aplikacji SaaS, które mogą stanowić zagrożenie dla bezpieczeństwa lub zgodności, a także ograniczeń przepustowości wynikających z marnowania jej przez użytkowników w oddziałach na nieistotne aplikacje takie jak Pandora lub YouTube.

Złożoność. Oprócz innych typów złożoności będących efektem wdrożenia technologii związanych z transformacją cyfrową, architektura SD-WAN może być trudna w zarządzaniu w odniesieniu do wszystkich oddziałów, ponadto rozwiązywanie pojawiających się problemów może być utrudnione. Większość rozwiązań nie oferuje jednego interfejsu zarządzania na potrzeby całościowego nadzoru i kontroli nad siecią we wszystkich oddziałach przedsiębiorstwa. Zwiększa to obciążenie nie tak znowu licznych pracowników działu IT i często jest przyczyną pojawiania się luk w zabezpieczeniach sieci.

Zabezpieczenia. Bez scentralizowanej ochrony zapewnianej dzięki przekierowywaniu ruchu przez centrum danych (backhauling), zastąpienie łączy MPLS bezpośrednimi szerokopasmowymi łączami internetowymi naraża przedsiębiorstwo na nowe zagrożenia, zwłaszcza w obliczu coraz liczniejszych i coraz bardziej wyrafinowanych cyberataków. Skuteczne wdrożenie rozwiązań SD-WAN wymaga zastosowania dodatkowych zabezpieczeń w infrastrukturze przedsiębiorstwa, które zapewnią ochronę tych łączy i pozwolą na inspekcję dużej ilości przesyłanych danych bez uszczerbku dla wydajności sieci.

Aby sprostać tym wyzwaniom, można zastosować jedno podejście do skutecznego wdrożenia SD-WAN, które łączy funkcje sieciowe i funkcje bezpieczeństwa w ramach jednolitej architektury. Rozwiązanie Fortinet **Secure SD-WAN** może zostać uruchomione w połączeniu z zaporami następnej generacji **FortiGate**. FortiGate łączy funkcje tych zapór z funkcjami sieci SD-WAN w jednym rozwiązaniu, które poprawia zarówno wydajność, jak i bezpieczeństwo sieci rozległej. Zapewnia również skuteczną ochronę we wszystkich oddziałach przedsiębiorstwa dzięki spójnemu egzekwowaniu zasad z poziomu jednej konsoli. Ponadto pozwala przedsiębiorstwom na ograniczenie ryzyka związanego z transformacją cyfrową. Trzy typowe przypadki zastosowania prezentują sposób, w jaki rozwiązanie Secure SD-WAN może okazać się rozwiązaniem najważniejszych problemów przedsiębiorstwa w kontekście bezpieczeństwa sieci, a jednocześnie zapewnić przedsiębiorstwu większe korzyści biznesowe.



Klienci nadal dążą do poprawy wydajności i widoczności sieci rozległej, ale obecnie najważniejsze jest dla nich bezpieczeństwo. W rzeczywistości 72% respondentów przyznało, że w przypadku sieci rozległej bezpieczeństwo jest dla nich najważniejsze[2].

ANALIZA PRZYPADKU — TRANSFORMACJA CYFROWA W ODDZIAŁACH PRZEDSIĘBIORSTWA

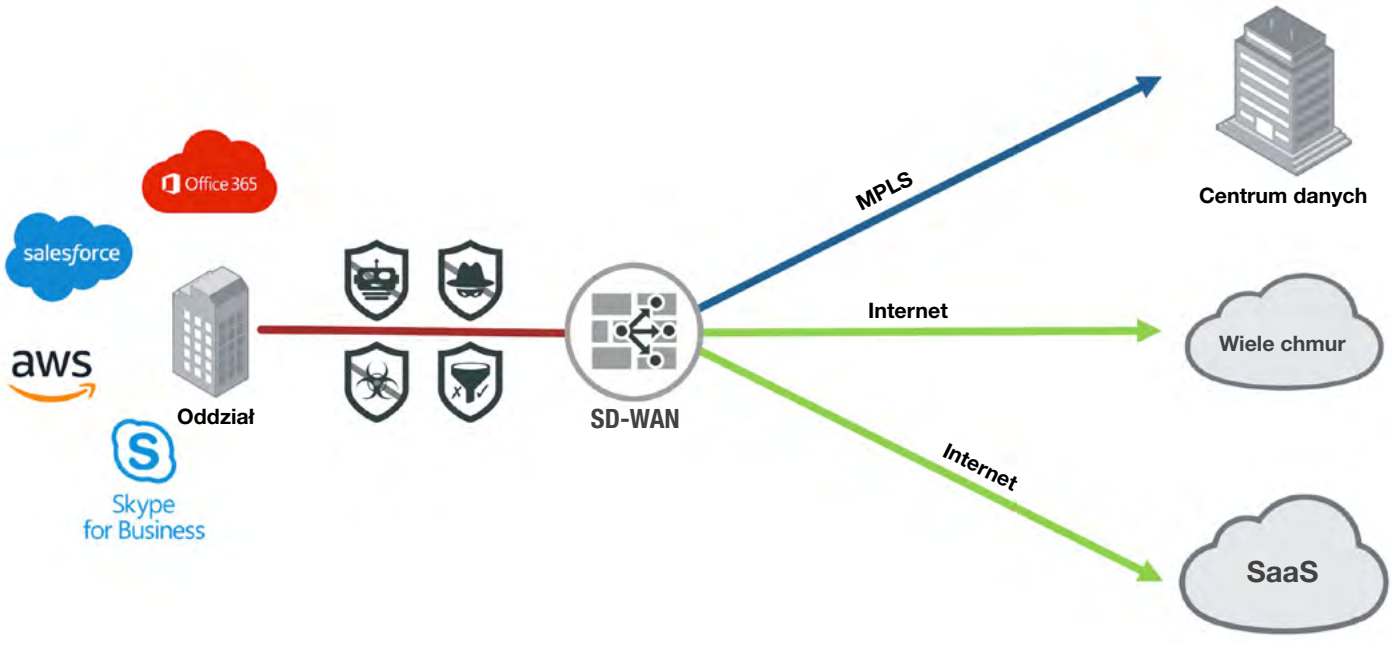
Rozproszone przedsiębiorstwa z wieloma oddziałami szukają skutecznych metod wdrożenia krytycznych aplikacji SaaS (takich jak Microsoft Office 365) i innych usług chmurowych w celu poprawy wydajności operacyjnej i zmniejszenia kosztów. Według jednego z najnowszych raportów 60% przedsiębiorstw wdrożyło już przynajmniej niektóre aplikacje SaaS[4], a tempo wzrostu liczby takich wdrożeń będzie coraz szybsze: w latach 2018–2023 skumulowany roczny wskaźnik wzrostu wartości globalnego rynku aplikacji SaaS ma wynieść 21,2%[5].

Ze względu na ograniczenia związane z łączami MPLS i przekierowywaniem ruchu przez centrum danych większość tradycyjnych infrastruktur sieci rozległej nie jest zdolna do efektywnej obsługi dodatkowego obciążenia sieci generowanego przez usługi chmurowe. Problemy w tym zakresie obejmują niską przepustowość, ograniczoną widoczność i kontrolę, małą użyteczność oraz dłuższe opóźnienia. Zdolność sieci SD-WAN do zapewnienia inteligentnego podziału obciążenia w przypadku ruchu między wieloma połączeniami szerokopasmowymi w celu zwiększenia wydajności sieci, dynamicznego wykonywania operacji i oszczędności kosztów może jednak złagodzić te problemy. Sieć SD-WAN zapewnia też oddziałom przedsiębiorstwa wszystkie korzyści w zakresie wydajności aplikacji chmurowych, ale tylko wtedy, gdy używane przez nią łącza są bezpieczne.

Zapora następnej generacji FortiGate z technologią Secure SD-WAN (wchodząca w skład architektury Fortinet Security Fabric) oferuje zaawansowane funkcje, które zabezpieczają bezpośredni dostęp do Internetu i pozwalają m.in. na kompleksowe zapobieganie zagrożeniom. Są to przede wszystkim funkcje filtrowania stron WWW, ochrony przed włamaniami i złośliwym oprogramowaniem oraz wykrywania zagrożeń (inspekcja SSL i sandboxing dzięki integracji z rozwiązaniem FortiSandbox).

SaaS

64% decydentów w zakresie IT uważało, że tempo wdrażania w ich przedsiębiorstwie aplikacji SaaS przewyższało jego zdolności do zabezpieczenia tych aplikacji[3].



RYSUNEK 1. ZAPORA FORTIGATE Z TECHNOLOGIĄ SECURE SD-WAN MOŻE PRZYCZYNIĆ SIĘ DO TRANSFORMACJI ARCHITEKTURY ODDZIAŁÓW PRZEDSIĘBIORSTWA.

Widoczność i kontrola to również ważne czynniki wpływające na akceptację korzystania z aplikacji SaaS przez większą liczbę pracowników oddziałów. Poszczególni pracownicy mogą bowiem sami instalować aplikacje chmurowe niezatwierdzone przez dział IT, co może skutkować bezpośrednim wprowadzeniem złośliwego oprogramowania do sieci oddziałów, tworzyć luki w zabezpieczeniach, a nawet naruszać przepisy prawa ochrony prywatności i regulacje branżowe. Technologia Secure SD-WAN zapewnia pełną widoczność i kontrolę aplikacji dzięki kilku kluczowym funkcjom:

Szeroko zakrojona zdolność do rozpoznawania aplikacji. Technologia Fortinet Secure SD-WAN korzysta z funkcji identyfikacji pierwszego pakietu w celu inteligentnego rozpoznawania aplikacji po pierwszym przesłanym pakiecie na podstawie danych z bazy zawierającej sygnatury ponad trzech tysięcy aplikacji (liczba ta stale rośnie w miarę rozwoju sieci cyfrowej i wzrostu liczby zagrożeń). Nowe aplikacje, także w przypadku zaszyfrowanego ruchu generowanego przez aplikacje chmurowe, są identyfikowane i klasyfikowane za pośrednictwem oferowanej na zasadzie subskrypcji opcjonalnej usługi **FortiGuard**. Zapory FortiGate mogą na bieżąco otrzymywać aktualne informacje o zagrożeniach od specjalistów z FortiGuard Labs w celu zapewnienia efektywniejszego routingu aplikacji oraz ochrony przed zagrożeniami w czasie rzeczywistym.

Raportowanie i monitorowanie zgodności. Oferowane przez sieć SD-WAN funkcje bezpiecznego śledzenia i raportowania pomagają zapewnić zgodność z przepisami prawa ochrony prywatności, normami bezpieczeństwa i regulacjami branżowymi, jednocześnie zmniejszając ryzyko poniesienia kar i kosztów obsługi prawnej wynikających z ewentualnego braku wspomnianej zgodności. Funkcje te umożliwiają śledzenie zagrożeń w czasie rzeczywistym, ułatwiają ocenę ryzyka, wykrywają potencjalne problemy i łagodzą ich skutki. Ponadto monitorują zasady zapór i pomagają zautomatyzować działania związane z audytami zgodności. Oferowana przez firmę Fortinet usługa **określania ratingu bezpieczeństwa** obejmuje najlepsze praktyki dotyczące stosowania norm PCI DSS, przepisów HIPAA (Health Insurance Portability and Accountability Act) i innych regulacji. W ramach tej usługi oceniony zostaje również stan bezpieczeństwa przedsiębiorstwa, który można następnie porównać z oceną wystawioną innym podobnym przedsiębiorstwom.



„…obszary, w których rozwiązanie SD-WAN szczególnie się wyróżnia to zadowolenie klientów z wydajności aplikacji VoIP i aplikacji wideokonferencyjnych[6]”.

ANALIZA PRZYPADKU — OBNIŻENIE KOSZTÓW OPERACYJNYCH SIECI ROZLEGŁEJ DZIĘKI WYSOKIEJ WYDAJNOŚCI APLIKACJI

Wymagania dotyczące przepustowości rosną, co oznacza wzrost kosztów operacyjnych dla działu IT. W efekcie wiele przedsiębiorstw zastępuje tradycyjne sieci rozległe (z drogimi łączami MPLS) rozwiązaniami SD-WAN w celu obniżenia wspomnianych kosztów operacyjnych. Gdy przedsiębiorstwo zaczyna korzystać z tanich łączy do sieci rozległej, często napotyka na problemy związane z wydajnością aplikacji, zwłaszcza w przypadku wymagających dużej przepustowości narzędzi komunikacyjnych takich jak aplikacje VoIP i aplikacje wideokonferencyjne. W takim przypadku krytyczne znaczenie dla zapewnienia optymalnego ruchu dla takich narzędzi ma zdolność do zbierania szczegółowych danych dotyczących wyboru ścieżek sieci rozległej.

Zautomatyzowane rozpoznawanie ścieżek sieciowych. Jest to kluczowa funkcja systemu operacyjnego Fortinet FortiOS, która optymalizuje wydajność aplikacji w drodze wyboru najbardziej efektywnej trasy dla ruchu generowanego przez aplikacje SaaS, VoIP i inne aplikacje o znaczeniu krytycznym dla przedsiębiorstwa na podstawie szczegółowych danych dotyczących wyboru ścieżek sieci rozległej (w tym danych o opóźnieniach, fluktuacjach i utracie pakietów). Z tego względu rozwiązanie Secure SD-WAN ułatwia zdefiniowanie poziomów usług sieci SD-WAN na potrzeby umów z klientami, zapewniając optymalne łącza dla każdej aplikacji za pomocą wbudowanych w system operacyjny FortiOS zaawansowanych funkcji sieciowych.

Utrzymanie wysokiej jakości działania aplikacji komunikacyjnych jest szczególnie ważne dla oddziałów przedsiębiorstwa, które opierają się na współpracy podczas realizacji operacji produkcyjnych. Podczas przeprowadzonych w 2018 r. przez NSS Labs testów zmierzono zadowolenie klientów z wydajności aplikacji VoIP i aplikacji wideokonferencyjnych oferowanej przez różne rozwiązania SD-WAN. Okazało się, że technologia Fortinet Secure SD-WAN otrzymała najwyższe oceny zarówno w przypadku aplikacji VoIP (najwyższy wynik), jak i aplikacji wideokonferencyjnych, a także ogólną ocenę „Zalecana”[7].

Dostęp do oddziału przez nakładkową sieć VPN. Wirtualna sieć prywatna (VPN) służy do zapewnienia bezpiecznego połączenia sieciowego z oddziałem poprzez utworzenie chronionego tunelu zestawionego na gorzej zabezpieczonych łączach sieciowych (na przykład publicznych łączach internetowych). Jedną z przyczyn popularności sieci SD-WAN jest fakt, że łączy ona w sobie opłacalność sieci VPN korzystających z łączy internetowych z wydajnością i sprawnością sieci VPN korzystających z łączy MPLS[8].

Technologia Fortinet Secure SD-WAN zapewnia zarządzanie zdalnym dostępem przez sieć VPN, aby umożliwić przedsiębiorstwu utrzymanie odpowiednich poziomów ochrony i inspekcji przy zapewnieniu wysokiego poziomu widoczności i kontroli. Dotyczy to danych i aplikacji obsługiwanych nie tylko przez środowisko SD-WAN, ale również w całej sieci rozproszonej.

Dla przedsiębiorstwa z wieloma oddziałami wydajne skalowanie nakładkowych sieci VPN jest kolejną niezbędną funkcją bezpiecznej i efektywnej sieci SD-WAN. Nakładkowe sieci VPN zazwyczaj korzystają z wielu warstw wspomnianych tuneli sieciowych na oddział. W przypadku posiadania wielu oddziałów duża liczba tych tuneli może negatywnie wpłynąć na wydajność sieci. Zapora następnej generacji FortiGate korzysta z zaawansowanych, specjalnych procesorów obsługujących funkcje zabezpieczeń (ang. security processors, SPU), które zwiększają wydajność i poprawiają skalowalność w przypadku korzystania z dużej liczby takich nakładkowych sieci VPN.

ANALIZA PRZYPADKU — UPROSZENIE SIECI ZA POMOCĄ MODELU ODDZIAŁU DEFINIOWANEGO PROGRAMOWO „SD-BRANCH”

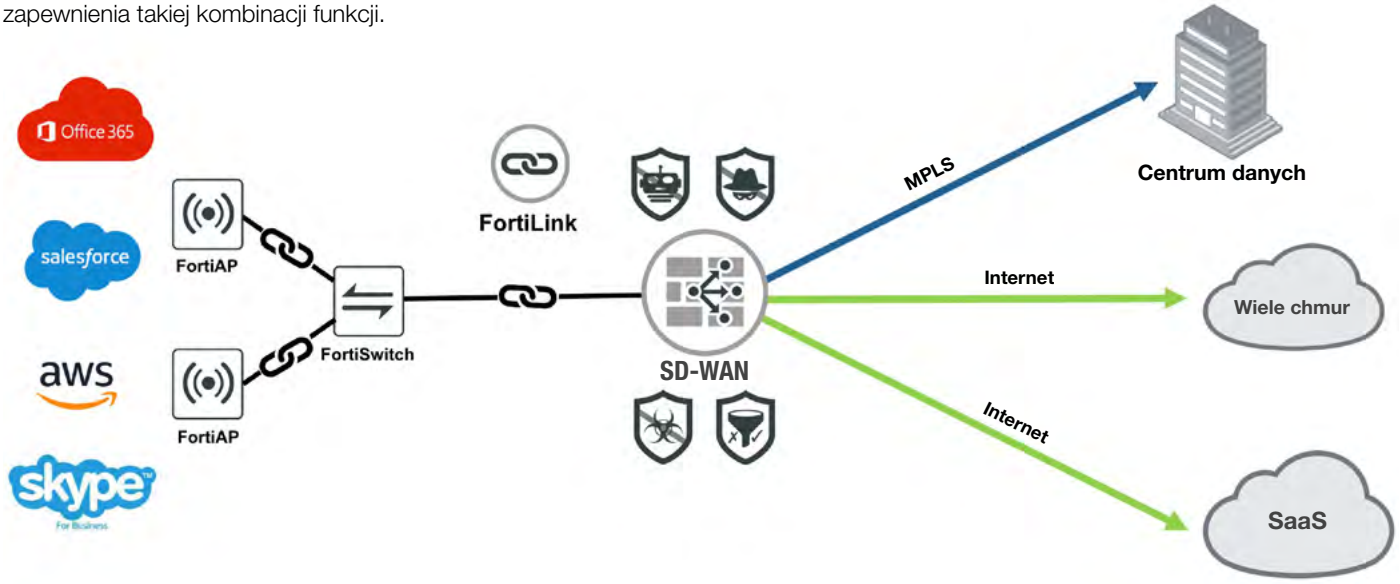
Według analityków firmy Gartner „użytkownicy również dostrzegają potrzebę sieci rozległych (WAN), które można efektywnie zintegrować z lokalnymi bezprzewodowymi sieciami LAN w oddziałach oraz wdrażanymi aplikacjami związanymi z Internetem rzeczy. Umożliwia to konwergencję i ściślejszą integrację między używanymi w oddziałach platformami WAN i LAN”[9].

Wiele oddziałów przedsiębiorstwa może chcieć jednocześnie zastępować urządzenia WAN i LAN rozwiązaniami zapewniającymi taką ściślejszą integrację oraz uproszczone funkcje zarządzania operacjami w oddziałach. Zastosowanie oddzielnych infrastruktur WAN i LAN nie tylko zwiększa złożoność sieci w oddziałach (więcej urządzeń do wdrażania i aktualizacji za pomocą wielu konsol zarządzania), ale także ogranicza widoczność i kontrolę operacji oraz zwiększa prawdopodobieństwo pojawienia się luki w zabezpieczeniach, którą mogą wykorzystać hakerzy.

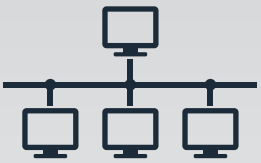
Model **oddziału definiowanego programowo (SD-Branch)** eliminuje te problemy, ponieważ ujednolica działania sieci WAN i LAN w ramach jednego rozwiązania. Zapora następnej generacji FortiGate (wchodząca w skład architektury Fortinet Security Fabric) z technologią Secure SD-WAN może zostać zintegrowana z rozwiązaniami FortiAP i FortiSwitch przy użyciu specjalnego protokołu FortiLink. Pozwala to klientom na zarządzanie podłączonymi do sieci LAN lokalnymi punktami końcowymi (takimi jak urządzenia związane z Internetem rzeczy) oraz automatyczne poddawanie kwarantannie urządzeń wykazujących symptomy ataku (IoC). Umożliwiane przez rozwiązania firmy Fortinet wdrożenia modelu oddziału definiowanego programowo (rys. 2) zapewniają ścisłą integrację sieci WAN i LAN, uproszczoną obsługę, bezpieczeństwo i najniższy w branży całkowity koszt posiadania.

Zarządzanie z poziomu jednej konsoli. Firma Fortinet udostępnia jedną konsolę zapewniającą widoczność zarówno sieci, jak i jej zabezpieczeń na potrzeby scentralizowanego zarządzania siecią SD-WAN oraz jej konfiguracji i monitorowania. Firma Fortinet jest uznawana za lidera zarówno na rynku zapór dla przedsiębiorstw, jak i systemów ujednoliconego zarządzania zagrożeniami (UTM)[10 11] i dobrze rozumie potrzeby przedsiębiorstw zarówno z punktu widzenia bezpieczeństwa, jak i funkcji sieciowych. Technologia Fortinet Secure SD-WAN konsoliduje w ramach jednego rozwiązania kilka funkcji punktowych w oddziale takich jak funkcje routingu, optymalizacji sieci rozległej, sieci SD-WAN i zabezpieczeń.

Bezobsługowe wdrożenie. Wdrożenie sieci SD-WAN powinno być równie łatwe jak włączanie dowolnej funkcji i tak to dokładnie wygląda w przypadku technologii Fortinet Secure SD-WAN. Nowe oddziały mogą być szybko podłączone i zabezpieczone bez dodatkowych kosztów ogólnych i bez konieczności angażowania do tego wielu specjalistów. Rozwiązanie firmy Fortinet upraszcza infrastrukturę i oferuje model oddziału definiowanego programowo ze skonsolidowanymi funkcjami sieci WAN i LAN oraz zaawansowanymi zabezpieczeniami. Żaden inny producent nie jest zdolny do zapewnienia takiej kombinacji funkcji.



RYS. 2. OBSŁUGIWANY PRZEZ ROZWIĄZANIA FORTINET OGÓLNY MODEL ODDZIAŁU DEFINIOWANEGO PROGRAMOWO KONSOLIDUJE INFRASTRUKTURY SIECI WAN I LAN



„Użytkownicy również dostrzegają potrzebę sieci rozległych (WAN), które można efektywnie zintegrować z bezprzewodowymi sieciami lokalnymi (LAN) w oddziałach oraz wdrażanymi aplikacjami związanymi z Internetem rzeczy. Umożliwia to konwergencję i ściślejszą integrację między używanymi w oddziałach platformami WAN i LAN”[9].



KORZYŚCI Z WDROŻENIA SIECI SD-WAN

Wraz z ciągłym rozwojem aplikacji SaaS, aplikacji VoIP i aplikacji wideokonferencyjnych, sieć SD-WAN może pomóc rozproszonemu przedsiębiorstwu w uzyskaniu korzyści wynikających z transformacji cyfrowej bez uszczerbku dla wydajności sieci i produktywności użytkowników końcowych.

Problemy dotyczące wydajności i bezpieczeństwa, które często są obecne w przypadku sieci SD-WAN, są eliminowane w wyniku zastosowania technologii Fortinet Secure SD-WAN — integralnego składnika architektury Fortinet Security Fabric i zapory następnej generacji FortiGate. Technologia Secure SD-WAN pozwala przedsiębiorstwu na szybkie wdrażanie aplikacji chmurowych bez uszczerbku dla zachowania bezpieczeństwa. Pomaga to w obniżeniu kosztów operacyjnych przy jednoczesnym zachowaniu wysokiej wydajności usług VoIP, usług VPN i usług wideokonferencyjnych oraz upraszcza infrastrukturę sieciową w oddziałach w drodze połączenia sieci i jej zaawansowanych zabezpieczeń w ramach jednolitego rozwiązania.

Firma Gartner nie promuje dostawców, produktów ani usług prezentowanych w swoich publikacjach badawczych, ani nie zaleca użytkownikom wybierania tylko dostawców uzyskujących najwyższe oceny lub określonych w inny sposób. Publikacje badawcze firmy Gartner zawierają opinie pracowników jej działu badawczego i nie należy ich uznawać za stwierdzenia stanu faktycznego. Gartner odrzuca wszelkie wyraźne i dorozumiane gwarancje i rękojmie co do tego badania, w tym gwarancje co do jego wartości handlowej lub przydatności do określonego celu.

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

[2] Ibid.

[3] Conner Forrest, „Businesses are adopting SaaS too fast to properly secure it", TechRepublic, 10 kwietnia 2018 r.

[4] „SaaS Adoption Rising", Computer Economics, listopad 2018 r.

[5] „Global Software-as-a-Service (SaaS) Market Outlook (2018–2023)", Business Wire, 14 listopada 2018 r.

[6] Linda Hardesty, „Quality of Experience Is What Distinguishes SD-WAN Products, Says NSS Labs", SDX Central, 9 sierpnia 2018 r.

[7] Nirav Shah, „Fortinet Secure SD-WAN Gives the Performance of a Lifetime, Recommended by NSS Labs", Fortinet, 9 sierpnia 2018 r.

[8] Zeus Kerravala, „Understanding Virtual Private Networks (and why VPNs are important to SD-WAN)", Network World, 13 kwietnia 2018 r.

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

[10] Adam Hils, Jeremy D'Hoinne, and Rajpreet Kaur, „Magic Quadrant for Enterprise Network Firewalls", Gartner, 4 października 2018 r.

[11] Rajpreet Kaur, Claudio Neiva, „Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)", Gartner, 20 września 2018 r.

SIEDZIBA GŁÓWNA
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Stany Zjednoczone
Tel.: +1.408.235 7700
www.fortinet.com/sales

POLSKA
ul. Złota 59
Budynek Lumen II
(6 piętro)
00-120 Warszawa
Polska

BIURO SPRZEDAŻY — REGION EMEA
905 rue Albert Einstein
06560 Valbonne
Francja
Tel.: +33 4 8987 0500

BIURO SPRZEDAŻY — REGION APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

CENTRALA — AMERYKA ŁACIŃSKA
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel.: +1 954 368 9990

Copyright © 2018 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).

maja 21, 2019 9:29 AM

342544-0-1-PL

wp-three-use-cases-for-transforming-A4