

Secure SD-WAN — podręcznik dla osób odpowiedzialnych za sieci

**Sieci tworzone z myślą o bezpieczeństwie
zapewniają kompleksową ochronę na brzegu
sieci rozległej**

Spis treści

Streszczenie	3
Wstęp.....	4
Którędy do sieci SD-WAN?	6
Najlepsza sieć SD-WAN? Tylko od Fortinet.....	7
Szczególnie zabezpieczone funkcje sieciowe	14
Na zmiennym rynku sieci SD-WAN rozwiązania Fortinet są dobrym wyborem	15

Streszczenie

Innowacje cyfrowe, takie jak bezpośrednie połączenia z dostawcą chmury (cloud on-ramp) aplikacji SaaS i IaaS, przyczyniają się do zwiększenia przychodów i wydajności w rozproszonych przedsiębiorstwach. Wynikające z wdrożenia tych technologii wymogi związane z rosnącym ruchem sieciowym istotnie zwiększają jednak koszty i ograniczają wydajność łączy MPLS w ramach tradycyjnych infrastruktur sieci rozległej (WAN). W rezultacie większość specjalistów ds. sieci zamierza zastąpić te przestarzałe infrastruktury WAN jakąś formą definiowanej programowo sieci rozległej (SD-WAN). W tym kontekście dziesiątki tysięcy klientów wybierają rozwiązanie FortiGate Secure SD-WAN, które udostępnia w ramach jednego rozwiązania funkcje sieciowe i funkcje zabezpieczeń. Rozwiązanie to poprawia wydajność aplikacji, pozwala na skonsolidowane zarządzanie siecią i zapewnia zaawansowaną ochronę przed zagrożeniami.

Wstęp

O ile wybór odpowiedniego dla danej implementacji rozwiązania SD-WAN może wymagać pójścia na kilka kompromisów, ich przedmiotem nigdy jednak nie powinno być bezpieczeństwo. Istnieją różne modele integracji sieci SD-WAN z zaawansowanymi mechanizmami bezpieczeństwa, ale tylko jeden z nich nazywa się „Secure SD-WAN”. Firma Fortinet, najbardziej wiarygodna marka w dziedzinie bezpieczeństwa sieci, wzbogaciła swoje doskonałe zapory FortiGate następnej generacji (NGFW) o najlepsze w swoim rodzaju funkcje SD-WAN, aby zapewnić optymalną wydajność aplikacjom o znaczeniu krytycznym udostępnianym w modelu oprogramowania jako usługi (SaaS) oraz narzędziom do przesyłania obrazu i dźwięku. Jednocześnie zapory te pomagają chronić przedsiębiorstwo przed najnowszymi zagrożeniami i coraz bardziej zaawansowanymi atakami.



Według szacunków firmy IDC globalny skumulowany roczny wskaźnik wzrostu przychodów ze sprzedaży infrastruktury i usług sieci SD-WAN wyniesie ponad 40%, a przychody te osiągną do 2022 r. wartość 4,5 mld USD¹.

Którędy do sieci SD-WAN?

Sieci SD-WAN pomagają efektywniej i ekonomiczniej korzystać z dostępnych usług sieci rozległej, aby użytkownicy w ramach całego rozproszonego przedsiębiorstwa mieli więcej swobody w angażowaniu klientów, optymalizowaniu procesów biznesowych i dokonywaniu innowacji. Samo zarządzanie siecią WAN staje się również mniej kosztowne, co sprawia, że w dającej się przewidzieć przyszłości rynek rozwiązań SD-WAN będzie nadal dynamicznie się rozwijać.

Aby zaspokoić zgłaszane na tym rynku potrzeby, w ostatnich kilku latach pojawiło się dużo rozwiązań SD-WAN, ale nie wszystkie z nich były równie dobre.

Specjaliści i analitycy zajmujący się sieciami SD-WAN twierdzą, że wdrożenie optymalnego dla przedsiębiorstwa rozwiązania SD-WAN zależy od wymogów dotyczących wydajności aplikacji, priorytetów bezpieczeństwa oraz umiejętności pracowników działu IT. Powszechnie zaleca się również, aby oprócz rozwiązania SD-WAN przedsiębiorstwo używało również zapory NGFW w celu zapewnienia odpowiedniego bezpieczeństwa, ponieważ za pośrednictwem połączeń szerokopasmowych w sieci SD-WAN oddziały przedsiębiorstwa są bezpośrednio podłączone do Internetu. Aby spełnić

wspomniane wymogi biznesowe, przedsiębiorstwo potrzebuje zatem FortiGate Secure SD-WAN — kompleksowego rozwiązania SD-WAN, które jako jedyne ma wbudowane funkcje zabezpieczeń i zapewnia wydajność oczekiwaną od sieci SD-WAN.

Najlepsza sieć SD-WAN? Tylko od Fortinet

Rozwiązanie FortiGate Secure SD-WAN zastępuje odrębne routery sieci rozległej, funkcje optymalizacji sieci rozległej i urządzenia zabezpieczające takie jak zapory i bezpieczne bramy sieciowe (SWG) pojedynczą zaporą NGFW FortiGate. Zapewnia ono najlepszą w branży wydajność oraz funkcje rozpoznawania aplikacji, zautomatyzowanego wyboru optymalnych ścieżek sieciowych oraz obsługi wirtualnych sieci prywatnych VPN w sieci rozległej WAN. Rozwiązanie FortiGate Secure SD-WAN zapewnia zabezpieczenie sieci oddziałów z doskonałą wydajnością wynikającą ze zdolności do szybkiej identyfikacji aplikacji i zautomatyzowanego wyboru optymalnych ścieżek sieciowych.

Rozwiązanie FortiGate Secure SD-WAN zapewnia następujące funkcje:

- Szybka identyfikacja aplikacji
- Zwiększenie dokładności rozpoznawania i wydajności aplikacji
- Możliwość aktualizacji bazy danych aplikacji wynikami analiz przeprowadzonych przez FortiGuard Labs

Lepsze poziomy usług dzięki zdolności do rozpoznawania aplikacji

Rozwiązanie FortiGate Secure SD-WAN korzysta z nowego specjalizowanego układu scalonego mieszczącego w sobie całą potrzebną funkcjonalność SOC4 ASIC, który pozwala na szybsze przełączanie aplikacji i wyjątkowo wydajną ich identyfikację. Rozwiązanie to zapewnia również funkcje inspekcji danych zaszyfrowanych za pomocą protokołów SSL i TLS przy najniższym możliwym negatywnym wpływie na wydajność. Funkcje inspekcji zaszyfrowanych danych obejmują zdolność do inspekcji pakietów na potrzeby poprawnego sterowania ruchem przez SD-WAN.

Z technicznego punktu widzenia zadaniem sieci SD-WAN jest udostępnienie aplikacjom możliwie najefektywniejszego w danym momencie połączenia z siecią rozległą. Aby zapewnić optymalną wydajność aplikacji, rozwiązania SD-WAN muszą być zatem zdolne do zidentyfikowania wielu różnych aplikacji i zastosowania odpowiednich zasad routingu na poziomie konkretnych aplikacji. Bez tych funkcji aplikacje SaaS oraz połączenia audio i wideo mogą działać wolno i ograniczać produktywność użytkowników końcowych.

W tym kontekście rozwiązanie FortiGate Secure SD-WAN korzysta z bazy danych aplikacji zawierającej sygnatury ponad 5000 aplikacji (baza ta jest na bieżąco aktualizowana danymi z FortiGuard Labs). FortiGate Secure SD-WAN identyfikuje i klasyfikuje aplikacje (także zaszyfrowany ruch generowany przez aplikacje chmurowe) już na podstawie pierwszego pakietu.



**FortiGate Secure SD-WAN
automatycznie rozpoznaje
i optymalnie trasuje ponad
5000 aplikacji.**

Zapora FortiGate NGFW może być skonfigurowana tak, aby rozpoznawać aplikacje według ich znaczenia dla prowadzonej działalności. Aplikacjom, które mają dla przedsiębiorstwa znaczenie krytyczne (na przykład Office 365, Salesforce lub SAP), aplikacjom zwiększającym produktywność (na przykład Dropbox) lub aplikacjom społecznościowym (na przykład Twitter) mogą być zatem nadane różne priorytety routingu. Dla aplikacji podrzędnych dla wspomnianych (na przykład dla aplikacji Word lub OneNote w ramach pakietu Office 365) również mogą zostać zastosowane odrębne polityki. Dzięki uzyskaniu tak głębokiej i szerokiej widoczności w zakresie wzorców ruchu i wykorzystania aplikacji można przydzielać zasoby sieci rozległej w sposób lepiej dostosowany do potrzeb biznesowych.

Łatwe zwiększenie efektywności sieci rozległej

Rozwiązanie FortiGate Secure SD-WAN znacząco upraszcza proces transformacji starszej infrastruktury brzegowej sieci rozległej, aby zwiększyć wydajność aplikacji, użyteczność i bezpieczeństwo. Po skonfigurowaniu reguł działania sieci rozległej na podstawie znaczenia (krytyczności) aplikacji, wymagań wydajnościowych, polityk zabezpieczeń i innych czynników, rozwiązanie FortiGate Secure SD-WAN zaczyna się nimi kierować. Zapory NGFW FortiGate z układami SOC4 ASIC zapewniają działanie zabezpieczeń dziesięciokrotnie szybsze niż w rozwiązaniach konkurencyjnych².

Jeśli chodzi o wydajność sieci rozległej, warto tu wymienić następujące funkcje rozwiązania FortiGate Secure SD-WAN:

Zautomatyzowany wybór optymalnych ścieżek

sieciowych. Zdolność do rozpoznawania aplikacji pozwala na trasowanie aplikacji priorytetowych w ramach dostępnej przepustowości sieci na podstawie konkretnych parametrów aplikacji i użytkownika. Nowy układ SOC4 ASIC zapewnia rozwiązaniu FortiGate Secure SD-WAN najszybsze w branży możliwości przełączania aplikacji. Poziomy usług rozwiązania SD-WAN (SLA) mogą być łatwo zdefiniowane w drodze dynamicznego wyboru najlepszego połączenia w sieci rozległej dla zadanych warunków biznesowych. W przypadku aplikacji o niskim i średnim priorytecie można określić kryteria jakości, a produkty FortiGate wybiorą wówczas dla tych aplikacji najlepsze połączenia. W przypadku aplikacji o wysokim i krytycznym priorytecie można natomiast zdefiniować ścisłe poziomy usług oparte na wartościach wskaźników mierzących fluktuacje, utratę pakietów i opóźnienia.

Sieć nakładkowa w sieci WAN. Responsywne **sieci nakładkowe VPN** zapewniają użytkownikom w oddziałach przedsiębiorstwa lepszą jakość sieci. Udostępniane przez **chmurowy kontroler nakładkowej sieci VPN** funkcje orkiestracji, zawarte w subskrybcyjnej licencji **360 Protection Bundle**, upraszczają wdrożenie nakładkowej sieci VPN dzięki chmurowym funkcjom automatycznej konfiguracji.

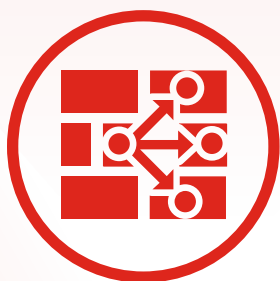
Automatyczne przełączanie awaryjne. W przypadku problemów z podstawową ścieżką sieci rozległej technologia rozpoznawania ścieżek może automatycznie przełączać ruch sieciowy na najlepsze dostępne łącze. Tego rodzaju automatyzacja jest wbudowana w zaporę FortiGate NGFW, aby zwiększyć wygodę obsługi i użyteczność tego rozwiązania dla użytkowników końcowych oraz zwiększyć ich produktywność.

Poprawa jakości ścieżek sieci rozległej. Funkcja poprawiania jakości ścieżek sieci rozległej korzysta z mechanizmu kodowania korygującego (ang. forward error correction, FEC), aby przezwyciężyć niekorzystne uwarunkowania sieci rozległej takie jak słabej jakości lub pełne szumy łącza. Korzystnie wpływa to na jakość przesyłanych danych i zapewnia większą użyteczność usług takich jak usługi przesyłania obrazu i dźwięku. Wspomniany mechanizm dodaje do pakietów wychodzących dodatkowe dane korygujące, które umożliwiają odzyskanie danych ewentualnie utraconych wskutek błędów w transmisji. Poprawia to jakość działania aplikacji wykorzystywanych w czasie rzeczywistym.

Agregacja tuneli w celu maksymalnego wykorzystania dostępnej przepustowości. W przypadku aplikacji wymagających większej przepustowości rozwiązanie FortiGate Secure SD-WAN umożliwia rozkładanie ruchu per pakiet, w celu ich jednoczesnego przesłania w ramach nie jednego, ale dwóch nakładkowych tuneli w celu maksymalnego wykorzystania dostępnej przepustowości.

Uprozczone zarządzanie i najniższy w branży całkowity koszt posiadania (TCO)

Osoby zarządzające siecią są często w rozterce w związku z wdrażaniem urządzeń brzegowych SD-WAN w licznych oddziałach przedsiębiorstwa i odległych lokalizacjach. Wysłanie personelu technicznego na miejsce wdrożenia jest drogie, nie wspominając już o tym, że liczba dostępnych inżynierów jest często ograniczona. Z drugiej strony wysłanie w pełni skonfigurowanych urządzeń też nie jest bezpieczne. Ponadto po wdrożeniu urządzeń brzegowych personel techniczny musi często zarządzać funkcjami optymalizacji sieci rozległej i funkcjami bezpieczeństwa za pomocą dwóch różnych interfejsów. FortiGate Secure SD-WAN rozwiązuje oba te problemy (z wdrożeniem i zarządzaniem), co obniża całkowity koszt posiadania tego rozwiązania.



Podczas przeprowadzonych w 2019 r. przez NSS Labs testów dotyczących rozwiązań SD-WAN technologia FortiGate Secure SD-WAN otrzymała drugi raz z rzędu ocenę „Zalecana” z uwagi na najniższy całkowity koszt posiadania (TCO) oraz możliwość szybkiego bezobsługowego wdrożenia³.

Bezobsługowe wdrożenie. Dzięki oferowanym przez FortiGate Secure SD-WAN funkcjom uproszczonego wdrażania przedsiębiorstwo może wysyłać do odległych lokalizacji nieskonfigurowane zapory NGFW FortiGate. Po podłączeniu ich do sieci zapora FortiGate automatycznie łączy się z usługą FortiDeploy na platformie FortiCloud. W ciągu kilku sekund FortiDeploy uwierzytelnia takie urządzenia zdalne i podłącza je do centralnego systemu FortiManager.

Zarządzanie z poziomu jednej konsoli. Rozwiązanie FortiManager zapewnia scentralizowaną widoczność wszystkich wdrożonych w rozproszonym przedsiębiorstwie zapór NGFW FortiGate obsługujących sieć Secure SD-WAN. Bardzo intuicyjne wizualizacje ułatwiają monitorowanie fizycznej i logicznej topologii sieci zarówno na poziomie ogólnym, jak i szczegółowym, jeśli potrzebne jest dokładniejsze zbadanie ewentualnego problemu. Administrator może aktualizować i instalować we wszystkich lokalizacjach obowiązujące w przedsiębiorstwie polityki dotyczące sieci rozległej oraz w razie potrzeby konfigurować poszczególne urządzenia.

Dla użytkowników, którzy potrzebują bezpiecznej komunikacji w ramach publicznych łączy internetowych, można natomiast jednym kliknięciem skonfigurować wirtualną sieć prywatną. Wszystko to oszczędza czas i upraszcza zarządzanie siecią SD-WAN (lokalnie lub w chmurze), łagodząc presję wywieraną na nieliczny zespół IT. Firma Fortinet oferuje jedno z nielicznych rozwiązań, które pozwala na zarządzanie zabezpieczeniami, mechanizmami kontroli dostępu i funkcjami sieci SD-WAN z poziomu jednej i tej samej konsoli.

Całkowity koszt posiadania (TCO). FortiGate Secure SD-WAN zapewnia jeden z najniższych w branży stosunków kosztu posiadania na Mb/s oraz możliwość bezobsługowego wdrożenia w oddziale w czasie krótszym niż sześć minut⁴. Zastosowanie publicznych łączy szerokopasmowych oznacza, że drogie łącza MPLS mogą być zastąpione opcjami przystępniejszymi cenowo. Za pomocą rozwiązania firmy Fortinet, które jest niezależne od metod przesyłu danych, przedsiębiorstwa mogą korzystać z całej dostępnej przepustowości w drodze stosowania połączeń w trybie aktywne — aktywne.



**Drugi rok z rzędu rozwiązanie
FortiGate Secure SD-WAN
zapewnia najniższy w branży
całkowity koszt posiadania
(według testów NSS Labs)⁵.**

Bezpieczeństwo sieci

Firma Fortinet udostępnia najlepszą w swojej klasie, sprawdzoną sieć SD-WAN, która zapewnia wysoką wydajność oraz jest bardzo dobrze chroniona. Zapory NGFW FortiGate z układami SOC4 ASIC oferują również najszybsze w branży działanie zabezpieczeń sieci SD-WAN. W przeprowadzonych przez NSS Labs w 2019 r. testach funkcji sieciowych definiowanych programowo sieci rozległych (SD-WAN) rozwiązanie Fortinet po raz drugi z rzędu otrzymało ocenę „Zalecane”⁶.

W szczególności rozwiązanie FortiGate Secure SD-WAN zapewnia zaawansowaną ochronę przed zagrożeniami dla sieci SD-WAN, w tym zabezpieczenia od warstwy 3 do warstwy 7, które nie są powszechnie spotykane w innych rozwiązaniach SD-WAN z zaporą:

- Pełna ochrona przed zagrożeniami, w tym zaporą, system ochrony przed włamaniami (IPS) i wirusami oraz mechanizmy kontroli aplikacji
- Głęboka inspekcja pakietów SSL/TLS obsługująca dużą przepustowość z minimalnym negatywnym wpływem na wydajność, aby przedsiębiorstwo nie musiało na rzecz pełnej ochrony przed zagrożeniami poświęcać dostępnej przepustowości
- Filtrowanie stron WWW na potrzeby bezpiecznego korzystania z Internetu bez konieczności stosowania oddzielnej, bezpiecznej bramy internetowej (SWG)

- Bardzo duża wydajność sieci rozległej w kontekście aplikacji chmurowych, w tym doskonała wydajność nakładkowej sieci VPN zapewniająca dużą użyteczność i niewielkie opóźnienia⁷

Zapory FortiGate wspierające Secure SD-WAN monitorują również polityki i reguły zapory oraz wskazują najlepsze działania mające na celu poprawę ogólnego stanu bezpieczeństwa przedsiębiorstwa. Pozwala to na łatwiejsze zapewnienie zgodności ze standardami bezpieczeństwa, normami branżowymi i przepisami prawa ochrony prywatności. Zautomatyzowane procesy audytu i raportowania pozwalają oszczędzić roboczogodziny personelu oraz ograniczyć ryzyko błędów i przeoczeń.

Obsługa modelu oddziału definiowanego programowo (SD-Branch)

Wiele oddziałów przedsiębiorstwa chce jednocześnie zastępować urządzenia WAN i LAN rozwiązaniami zapewniającymi 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. Aby rozwiązać te problemy, rozwiązanie FortiGate Secure SD-WAN zawiera akcelеровane sprzętowo rozszerzenie bezpieczeństwa w warstwie dostępowej, co pozwala na wdrożenie modelu oddziału definiowanego programowo (SD-Branch).

Na zmiennym rynku sieci SD-WAN rozwiązania Fortinet są dobrym wyborem

Ze względu na fakt, że stosowanie narzędzi i aplikacji chmurowych (takich jak usługi przesyłania obrazu i dźwięku) staje się dla przedsiębiorstw coraz bardziej niezbędne, rozwiązanie FortiGate Secure SD-WAN może ułatwić z nich korzystanie bez uszczerbku dla wydajności aplikacji, produktywności użytkowników końcowych lub bezpieczeństwa danych.

Skalowalne rozwiązanie FortiGate Secure SD-WAN pomaga w dobrej obsłudze coraz większej liczby odległych lokalizacji, coraz większej przepustowości niezbędnej dla aplikacji o znaczeniu krytycznym, coraz większej liczby usług chmurowych itp.

Rozwiązanie FortiGate Secure SD-WAN jest stosowane na całym świecie w przedsiębiorstwach z tak odległych od siebie branż, jak branża finansowa, przemysłowa, usługowa i detaliczna. Bez względu na to, czy niezbędna jest obsługa kilkuset mobilnych punktów końcowych, czy dziesiątków tysięcy oddziałów, użytkownicy rozwiązania FortiGate Secure SD-WAN otrzymują optymalny dla siebie zestaw doskonałych zabezpieczeń i funkcji SD-WAN.

¹ „[SD-WAN Infrastructure Market Poised to Reach \\$4.5 Billion in 2022](#)”, IDC, 8 sierpnia 2018 r.

² Na podstawie wewnętrznych testów firmy Fortinet.

³ „[Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report](#)”, 19 czerwca 2019 r.

⁴ Ibid.

⁵ Ibid.

⁶ Ibid.

⁷ Ibid.



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 rękojnie, 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 działał 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).