FORTINET

Niezbędne funkcje efektywnego i bezpiecznego rozwiązania SD-WAN — przewodnik dla liderów

Spis treści

Streszczenie

Przedsiębiorstwa dążą do zastąpienia przestarzałych infrastruktur sieci rozległych (WAN) bezpiecznymi, programowo definiowanymi sieciami (SD-WAN) w wyniku oddziaływania trzech głównych trendów.

- Cyfrowe przyspieszenie, które angażuje usługi Software-as-a-Service (SaaS) i Infrastructure-as-a-Service (IaaS), zwiększa zapotrzebowanie na ruch, podnosi koszty i ogranicza wydajność łączy MPLS (Multiprotocol Label Switching) w tradycyjnych rozwiązaniach WAN.

- Model pracy zdalnej (WFA), który na początku pandemii miał być rozwiązaniem krótkoterminowym, obecnie stał się nową normą. Przedsiębiorstwa muszą zapewnić pracownikom zdalnym bezpieczny i niezawodny dostęp do wszystkich swoich zasobów.

- Cyberprzestępcy są aktywni bardziej niż kiedykolwiek, a innowacje w zakresie cyberprzestępczości jako usługi sprawiają, że nawet niezaawansowani hakerzy mogą szybko i łatwo przeprowadzać bardzo zaawansowane ataki.

Rozważając zakup rozwiązania SD-WAN, należy zatem zwrócić uwagę na trzy kluczowe kwestie, aby wyjść naprzeciw tym trendom. Efektywne rozwiązanie musi bowiem oferować zintegrowane funkcje potrzebne do wydajnego zarządzania, w tym zarządzania na poziomie operacyjnym, doskonałą jakość doświadczeń (QoE) zarówno dla użytkowników, jak i pracowników działu IT, a także kompleksowe zabezpieczenia.

Wstęp

W obliczu cyfrowego przyspieszenia, pracy zdalnej i coraz bardziej zaawansowanych cyberataków, zwiększa się zapotrzebowanie na przepustowość w celu bezpiecznego zapewniania użytkownikom oczekiwanego środowiska pracy, a wymagania dotyczące sieci SD-WAN stają się coraz bardziej złożone. Wiele dostępnych obecnie na rynku rozwiązań jest jednak niekompletnych. Wyzwania takie jak ograniczona skalowalność, brak automatyzacji upraszczającej operacje oraz słaba integracja z rozwiązaniami chmurowymi i SaaS mogą sprawić, że wspomniane środowisko będzie dla użytkownika niekomfortowe, co z kolei może podważyć korzyści płynące z wdrożenia rozwiązania SD-WAN. Ponadto zapewnienie bezpośredniego połączenia z Internetem za pośrednictwem SD-WAN oznacza, że ruch nie przechodzi już przez centrum danych, w którym mogłyby działać odpowiednie zabezpieczenia. Aby zatem rozwiązanie SD-WAN było skuteczne, musi obejmować rozbudowany zestaw narzędzi sieciowych, łączy i zabezpieczeń zdolnych do obsługi i dostosowywania się do dynamicznego charakteru dzisiejszych sieci. Musi być ponadto zdolne do szybkiego wdrażania rozwiązań chmurowych, przechodzenia z wdrożeń regionalnych na globalne, obsługi kolejnych biur lub oddziałów, a także uwzględnienia pracy zdalnej.

Początkowo SD-WAN było uznawane za rozwiązanie o dość wąskim zastosowaniu, ale z czasem stało się platformą do budowy rozwiązania SD-Branch i SASE. Jako platforma musi być zatem zdolne do płynnej obsługi migracji i ujednoliconego nim zarządzania.

“Oczekuje się, że wartość globalnego rynku SD-WAN wzrośnie do 13,7 mld USD do 2027 r., przy skumulowanym rocznym wskaźniku wzrostu (CAGR) na poziomie 31,9% w okresie prognozy[1].”

Odpowiedź SD-WAN na wymagania biznesowe

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. Takie innowacje w zakresie sieci WAN z dodatkowymi łączami operatora można z kolei wykorzystać do zapewnienia nadmiarowości, równoważenia obciążenia oraz optymalizacji ruchu z i do aplikacji. Samo zarządzanie siecią WAN staje się również mniej kosztowne, co sprawia, że w dającej się przewidzieć przyszłości rynek rozwiązań SD-WAN będzie się nadal dynamicznie rozwijać.

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

Optymalne rozwiązanie SD-WAN dla przedsiębiorstwa zależy od wymagań w obszarach, taki jak:

- Bezpieczeństwo
- Wydajność aplikacji
- Łatwość wdrażania aplikacji i zasobów w różnych chmurach obliczeniowych
- Uproszczenie operacji dzięki scentralizowanemu zarządzaniu w dowolnej skali.

Aby sprostać tym wymaganiom biznesowym, przedsiębiorstwo potrzebuje kompleksowej oferty SD-WAN z wbudowanymi zabezpieczeniami i możliwościami skalowania wydajności w dowolnym zakresie. Oferta taka powinna również obejmować zapewnienie scentralizowanej widoczności i funkcji zarządzania.

Ponieważ oddziały przedsiębiorstwa mają bezpośredni dostęp do Internetu za pośrednictwem szerokopasmowych połączeń z SD-WAN, idealnym rozwiązaniem jest zatem integracja SD-WAN i firewalla nowej generacji (NGFW) w ramach jednego urządzenia lub jednej maszyny wirtualnej.

Zamiast odrębnych routerów WAN i zabezpieczeń, takich jak firewall i bezpieczne bramy sieciowe (SWG), wszystkie te funkcje powinno pełnić jedno rozwiązanie NGFW.

Poprawione poziomy usług dzięki zdolności do rozpoznawania aplikacji

Wydajność ma kluczowe znaczenie, efektywne rozwiązanie SD-WAN musi zatem zapewniać szybkie, dynamiczne możliwości przełączania i identyfikacji aplikacji. Obejmuje to głęboką inspekcję danych zaszyfrowanych za pomocą protokołów SSL (Secure Sockets Layer) lub TLS (Transport Layer Security) bez pogorszenia wydajności. Funkcje inspekcji zaszyfrowanych danych muszą również obejmować zdolność do sprawdzania pakietów na potrzeby poprawnego przełączania ruchu przez rozwiązanie SD-WAN.

Z technicznego punktu widzenia zadaniem rozwiązania SD-WAN jest udostępnienie aplikacjom możliwie najefektywniejszego w danym momencie połączenia z siecią rozległą, w tym połączenia w ramach bezprzewodowej sieci LTE/5G. Aby zapewnić optymalną wydajność aplikacji, rozwiązanie SD-WAN musi być zatem zdolne do zidentyfikowania wielu różnych aplikacji i zastosowania odpowiednich zasad routingu dla konkretnych aplikacji. Bez tych funkcji aplikacje SaaS oraz połączenia audio-wideo mogą działać wolno i ograniczać produktywność użytkowników końcowych.

Zaawansowane rozwiązanie SD-WAN może rozpoznawać aplikacje według ich znaczenia dla prowadzonej działalności. Aplikacje o znaczeniu krytycznym (takie

jak Office 365, Salesforce lub SAP), ogólne aplikacje zwiększające produktywność (takie jak Dropbox) i aplikacje społecznościowe (X, Instagram) mogą mieć różne priorytety routingu. Z kolei odrębne zasady mogą być stosowane dla wybranych aplikacji podrzędnych (takich jak Word lub OneNote z pakietu Office 365).

Dzięki uzyskaniu tak głębokiej i szerokiej widoczności w zakresie wzorców ruchu i wykorzystania aplikacji można przydzielać zasoby sieci rozległej w sposób lepiej odpowiadający potrzebom biznesowym.

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

Zautomatyzowane rozpoznawanie ścieżek sieciowych. Zdolność rozpoznawania aplikacji umożliwia zarządzanie ruchem w ramach dostępnego pasma dla konkretnych aplikacji i użytkowników. Gwarantowane poziomy usług (SLA) SD-WAN mogą być łatwo zdefiniowane w drodze dynamicznego wyboru najlepszego połączenia w sieci rozległej, w tym połączenia w ramach bezprzewodowej sieci LTE/5G, dla zadanych warunków biznesowych. W przypadku aplikacji o niskim i średnim priorytecie można określić kryteria jakości, a rozwiązanie SD-WAN wybierze wówczas odpowiednie łącze. W przypadku aplikacji o wysokim i krytycznym priorytecie można natomiast zdefiniować ścisłe poziomy usług oparte na wartościach wskaźników mierzących fluktuacje, utratę pakietów i opóźnienia.

Automatyczne przełączanie awaryjne. Technologia rozpoznawania ścieżek może automatycznie przełączać ruch sieciowy na najlepszą ścieżkę sieci rozległej w czasie krótszym niż sekunda, w tym na połączenia w ramach bezprzewodowej sieci WAN LTE/5G. Tego rodzaju automatyzacja jest wbudowana w rozwiązanie SD-WAN, aby zwiększyć wygodę obsługi i użyteczność tego rozwiązania dla użytkowników końcowych oraz zwiększyć ich produktywność**.**

Przywracanie funkcjonalności ścieżek sieci rozległej. Funkcja przywracania funkcjonalności ścieżek sieci rozległej korzysta z mechanizmu kodowania korygującego (ang. forward error correction, FEC) i duplikacji pakietów, aby przezwyciężyć niekorzystne uwarunkowania sieci rozległej takie jak słabej jakości lub pełne zakłóceń 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. Funkcja duplikacji pakietów wysyła kopie pakietów wieloma dostępnymi ścieżkami alternatywnymi, w tym bezprzewodowymi połączeniami LTE/5G zapewniającymi dostęp do sieci WAN. Poprawia to jakość działania aplikacji wykorzystywanych w czasie rzeczywistym.

Nadawanie priorytetów aplikacjom. Dzięki możliwości definiowania reguł biznesowych właściwych dla poszczególnych aplikacji można zapewnić najlepsze możliwe wykorzystanie przepustowości poprzez dodanie funkcji precyzyjnego nadawania priorytetów jakości usług (QoS) dla aplikacji o znaczeniu krytycznym, przy jednoczesnym ograniczaniu przepustowości dla aplikacji o znaczeniu niekrytycznym, które mogą mieć wpływ na wydajność i doświadczenia użytkownika końcowego**.**

Agregacja tuneli w celu maksymalnego wykorzystania dostępnej przepustowości. W przypadku aplikacji wymagających większej przepustowości rozwiązanie SD-WAN powinno umożliwiać rozdzielenie ruchu na poziomie pakietów, w celu ich jednoczesnego przesłania w ramach nie jednego, ale dwóch tuneli, aby maksymalnie wykorzystać dostępną przepustowość..

Bezpieczne rozwiązanie SD-WAN podstawą transformacji sieci[2]

Uproszczone zarządzanie i wyższy całkowity koszt posiadania

Osoby zarządzające siecią są często w rozterce w związku z wdrażaniem urządzeń 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 zarządzać zarówno siecią rozległą, jak i zabezpieczeniami z osobnych konsol.

Rozwiązanie Secure SD-WAN rozwiązuje oba te problemy (z wdrożeniem i zarządzaniem), co obniża całkowity koszt posiadania tego rozwiązania.

Bezobsługowe wdrożenie. Dzięki funkcjom uproszczonego wdrażania przedsiębiorstwo może wysyłać do odległych lokalizacji nieskonfigurowane urządzenia SD-WAN. Po podłączeniu ich do sieci powinny automatycznie połączyć się z odpowiednią usługą, która w ciągu kilku sekund uwierzytelnia takie urządzenia zdalne i podłącza je do systemu centralnego zarządzania.

Zarządzanie z poziomu jednej konsoli. Scentralizowana widoczność wszystkich wdrożonych w rozproszonym przedsiębiorstwie urządzeń SD-WAN ma znaczenie kluczowe. Należy tu uwzględnić uproszczony przepływ pracy umożliwiający wdrażanie i aktualizowanie reguł za pomocą kilku prostych kliknięć/etapów.

Rozwiązanie SD-WAN powinno być zdolne do automatycznego budowania połączeń typu „full mesh overlay” i zarządzania nim, z uwzględnieniem opcji bezprzewodowych połączeń LTE/5G zapewniających dostęp do sieci WAN, w celu zapewnienia bezpiecznej łączności między lokalizacjami.

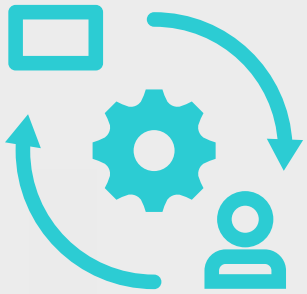
Dzięki wspomaganym przepływom pracy, automatyzacji warstwy sieciowej i uproszczonym regułom biznesowym, czas poświęcany przez personel działu IT na wdrażanie i zmiany infrastruktury skraca się z miesięcy do minut.

Raportowanie i analityka w rozwiązaniu SD-WAN. Rozszerzone funkcje analityczne dotyczące dostępności łączy sieci rozległej, uzgodnionych poziomów wydajności, przepływu danych do i z aplikacji pozwalają zespołowi ds. infrastruktury na szybkie identyfikowanie i rozwiązywanie problemów z siecią.

Funkcje te obejmują:

- raporty i zestawienia dotyczące monitorowania przepustowości rozwiązania SD-WAN;
- możliwości zapisywania w dzienniku i monitorowania historii poziomów usług za pomocą zestawień, wykresów i raportów;
- mechanizmy konfigurowania powiadomień dotyczących poziomów usług;
- raporty i pulpity dotyczące używania aplikacji;
- 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.

Funkcje bramy dostępu do aplikacji. Pozwala to przedsiębiorstwu na hostowanie aplikacji w dowolnym miejscu przy zastosowaniu spójnych mechanizmów kontroli reguł, aby umożliwić i zabezpieczyć obsługę hybrydowych modeli pracy przy zapewnieniu użytkownikom niezawodnego i doskonałego środowiska pracy.



„Dzięki odpowiedniemu bezpiecznemu rozwiązaniu SD-WAN przedsiębiorstwa mogą budować sieci jutra[3]”.

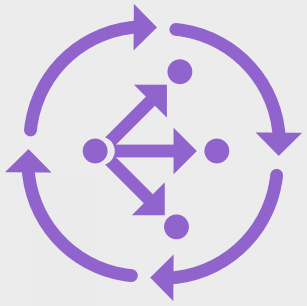
Zarządzanie złożonością wielu chmur

Dostęp do rozproszonej chmury przy niskich opóźnieniach. Idealne, bezpieczne rozwiązanie SD-WAN zapewnia natychmiastowy dostęp do wielu chmur takich jak Office 365. Ponadto wbudowane zabezpieczenia stanowią kolejną warstwę zapewniającą bezpieczny dostęp do tych aplikacji, zapewniając jednocześnie cechujące się niskim opóźnieniem połączenie za pośrednictwem publicznych łączy internetowych. W rezultacie łącza te mogą wejść w skład zaufanej i niezawodnej infrastruktury WAN.

Jest to szczególnie istotne w sytuacji, gdy pracownicy zdalni korzystają z zaawansowanych, bogatych w funkcje, hostowanych w chmurze aplikacji do obsługi połączeń głosowych i wideokonferencji. Aplikacje te udostępniają rozszerzone funkcje audio-wideo, ale wymagają również większej przepustowości. W większości przypadków wspomniany ruch danych może być również szyfrowany, co zwiększa obciążenie związane z inspekcją ruchu. w przypadku aplikacji szyfrowanych mechanizmy wykrywania aplikacji podrzędnych i stosowania inspekcji SSL zapewniają, że ruch do i z tych aplikacji zostanie przekierowany do najbardziej wydajnego łącza WAN w celu zapewnienia optymalnego działania.

Łączność w chmurze publicznej. Technologia SD-WAN może odgrywać kluczową rolę w łączności w chmurze. Bramy SD-WAN mogą kierować ruch do i z aplikacji łączami zdefiniowanymi w regułach oraz automatycznie konfigurować tunele IPsec (Internet Protocol Security) do usług chmurowych różnych dostawców i pomiędzy nimi (wszystko z poziomu scentralizowanej konsoli).

Oznacza to, że rozwiązanie SD-WAN może być używane jako chmurowa sieć nakładkowa służąca do łączenia oddziałów przedsiębiorstwa z usługami w chmurze, sieciami wirtualnymi w ramach jednej chmury publicznej, a nawet z wieloma chmurami. Zdolność tego rozwiązania do nadawania priorytetów ruchowi według aplikacji umożliwia priorytetowe traktowanie najbardziej krytycznego ruchu, a jego zdolność do przełączania ruchu między wieloma trasami w celu uzyskania najlepszej wydajności sprawia, że idealnie nadaje się jako nakładka na wiele chmur. Zasady dostępu i bezpieczeństwa są scentralizowane, a administratorzy mają pełną widoczność ruchu do i z aplikacji, wydajności i bezpieczeństwa.



„Rozwiązanie SD-WAN działa najlepiej w ramach platformy obejmującej wdrożenia wielochmurowe, dostęp do sieci na zasadzie zerowego zaufania itp.[4]”.

Sprawdzone, kompleksowe zabezpieczenia

Rozwiązanie Secure SD-WAN musi zapewniać niezawodną ochronę przed zagrożeniami, w tym zabezpieczenia od warstwy 3 do warstwy 7. Należy do nich:

- Pełna ochrona przed zagrożeniami, w tym zapora sieciowa, system ochrony przed włamaniami (IPS) i wirusami oraz mechanizmy kontroli aplikacji
- Wydajne odszyfrowywanie i szczegółowa inspekcja pakietów SSL/TLS, w tym TLS 1.3, działające przy minimalnym spadku wydajności, 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 opóźnienia

Rozwiązanie Secure SD-WAN powinno również monitorować polityki i reguły zapory sieciowej oraz wskazywać 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 rozwiązaniem zapewniającym ściślejszą integrację oraz uproszczone funkcje zarządzania operacjami w oddziałach. Zastosowanie oddzielnych infrastruktur WAN i LAN nie tylko jednak zwiększa złożoność sieci w oddziałach (więcej urządzeń do wdrażania i aktualizacji za pomocą wielu konsol zarządzania), ale także ogranicza widoczność i kontrolę operacji oraz podnosi prawdopodobieństwo pojawienia się luki w zabezpieczeniach, którą mogą wykorzystać hakerzy. Odpowiednie rozwiązanie SD-WAN rozwiąże te problemy i przyspieszy wdrożenie modelu SD-Branch.

Zabezpieczenie wszystkich użytkowników

Rozwiązanie Secure Access Service Edge (SASE) pomaga rozszerzyć bezpieczny dostęp i wydajną łączność na użytkowników przebywających w dowolnym miejscu na świecie. Rozwiązanie to oferuje cały zestaw funkcji sieciowych i zabezpieczeń, w tym bezpieczną bramę sieciową (SWG), uniwersalny dostęp do sieci w modelu zerowego zaufania (ZTNA), działające w dwóch trybach oprogramowanie pośredniczące w dostępie do chmury CASB nowej generacji, usługi Firewall-as-a-Service (FWaaS) oraz integrację z rozwiązaniem Secure SD-WAN. Dzięki takiemu ujednoliconemu rozwiązaniu można:

- Wyeliminować luki w zabezpieczeniach
- Uprościć operacje oraz zwiększyć bezpieczeństwo i możliwości analizy danych dotyczących sieci.
- Przejść na model biznesowy oparty na kosztach operacyjnych z prostymi licencjami dla użytkownika

„Zdolność do dokładnego rozpoznawania aplikacji jest niezbędna do zapewnienia właściwych priorytetów aplikacjom o znaczeniu krytycznym dla przedsiębiorstwa. Większość rozwiązań SD-WAN nie jest jednak w stanie obsłużyć ruchu szyfrowanego[5]”.

W usługach Google ponad 90% ruchu podlega szyfrowaniu[6]”.

Właściwy wybór na nierównym rynku SD-WAN

Aplikacje i narzędzia chmurowe, w tym funkcje audio-wideo, stają się coraz ważniejsze dla przedsiębiorstw rozproszonych, dlatego przedsiębiorstwa te muszą być zdolne do czerpania korzyści z innowacji cyfrowych bez narażania na szwank swojego bezpieczeństwa, bez ograniczania wydajności aplikacji oraz bez uszczerbku dla produktywności użytkowników końcowych.

Aby zatem czerpać korzyści z rozwiązań SD-WAN, przedsiębiorstwo powinno najpierw starannie je ocenić. Rzadko kiedy rozwiązania te korzystają z jednego systemu operacyjnego w celu zapewnienia prawdziwej integracji funkcji SD-WAN i funkcji zabezpieczeń. Takie kompleksowe, zintegrowane funkcje zarządzane z poziomu jednej konsoli i w dowolnej skali są niezbędne, a mimo to niewielu dostawców je oferuje. Ponadto efektywne rozwiązanie SD-WAN musi mieć zaawansowane funkcje, aby zapewnić oczekiwaną jakość QoE dla użytkowników końcowych i personelu działu IT oraz poprawić wydajność operacyjną na brzegach sieci WAN i chmury.

[1] „Software-Defined Wide Area Network (SD-WAN) Market by Component (Solutions (Software and Appliances) and Services), Deployment Type (On-Premises and Cloud), End User (Service Providers and Verticals), and Region - Global Forecast to 2027", Markets and Markets, dostęp z dnia 18 kwietnia 2023 r.

[2] Nirav Shah, „Secure SD-WAN: The Foundation for Network Transformation", 30 czerwca 2022 r.

[3] Nirav Shah, „Using Fortinet Secure SD-WAN to Build Tomorrow's Networks", 30 sierpnia 2022 r.

[4] Nirav Shah, „SD-WAN Works Best as Part of a Platform", 26 stycznia 2022 r.

[5] Nirav Shah, „Enabling Self-Healing SD-WAN from the WAN Edge to the Cloud Edge", Fortinet, 22 czerwca 2021 r.

[6] „HTTPS encryption on the web", Google, dostęp z kwietnia 2023 r.

FORTINET

www.fortinet.com

16 listopada 2023

372656-C-0-EN