



CO NALEŻY ROZWAŻYĆ PODCZAS WYBORU SIECI ROZLEGŁEJ DEFINIOWANEJ PROGRAMOWO (SD-WAN)

SPIS TREŚCI

WSTĘP

1

CZĘŚĆ 1: PROBLEMY Z TRADYCYJNĄ SIECIĄ ROZLEGŁĄ

2

- WYSOKI CAŁKOWITY KOSZT POSIADANIA
- WDROŻENIA I WIDOCZNOŚĆ W CHMURZE
- ZABEZPIECZENIA W CENTRUM DANYCH
- ODPORNOŚĆ NA AWARIE I CIĄGŁOŚĆ DZIAŁANIA

CZĘŚĆ 2: SZEŚĆ KWESTII DO ROZWAŻENIA PODCZAS WYBORU SIECI SD-WAN

4

- WDRAŻANIE APLIKACJI CHMUROWYCH
- ROZPOZNAWANIE APLIKACJI
- ROZPOZNAWANIE ŚCIEŻEK SIECIOWYCH
- ZABEZPIECZENIA I ZGODNOŚĆ
- OBSŁUGA WIELU KANAŁÓW SZEROKOPASMOWYCH
- CAŁKOWITY KOSZT POSIADANIA

STRESZCZENIE

11

WSTĘP

Przedsiębiorstwa stoją obecnie w obliczu wyzwań związanych z ceną, wydajnością i elastycznością tradycyjnych sieci rozległych. Bardzo duże tempo wzrostu sprzedaży usług chmury publicznej (28,6% r/r w 2017 r.)¹ sprawiło, że przedsiębiorstwa muszą szukać efektywniejszych rozwiązań sieciowych zdolnych do obsługi rozproszonego ruchu między oddziałami a odległymi lokalizacjami.

Do konkretnych problemów, z którymi borykają się przedsiębiorstwa korzystające z tradycyjnych sieci rozległych, można zaliczyć:

- Wysoki całkowity koszt posiadania
- Długie cykle przydzielania zasobów
- Stopniowy spadek wydajności w miarę nasilania się ruchu w chmurze

- Nieodpowiednią nadmiarowość i odporność na awarie
- Brak zdolności rozpoznawania możliwości podłączenia aplikacji

Aby lepiej zarządzać posiadaną siecią rozległą, przedsiębiorstwa zaczynają stosować nowe podejście do swoich rozproszonych sieci oddziałowych, czyli **sieć rozległą definiowaną programowo (ang: software-defined wide area network, SD-WAN)**. Rozwiązanie to nie tylko zapewnia większą wydajność, sprawność i elastyczność operacyjną, ale jest również znacznie tańsze. Nie wszystkie rozwiązania SD-WAN są jednak równie dobre.

¹ „Worldwide Public Cloud Services Revenue Growth Remains Strong in the First Half of 2017”, IDC, 6 listopada 2017 r.

01 PROBLEMY Z TRADYCYJNĄ SIECIĄ ROZLEGŁĄ

Dobre działanie tradycyjnej sieci rozległej trudno jest zapewnić, ponieważ jest ona niemal w całości ograniczona do drogich łączy w technologii MPLS. Jednocześnie bardzo szybkie upowszechnianie się aplikacji chmurowych w rozproszonych organizacjach powoduje duży wzrost zapotrzebowania na przepustowość sieci. W miarę narastania tych potrzeb infrastruktury, tradycyjne sieci rozległe stają się coraz droższe i trudniejsze we wdrażaniu i zarządzaniu. Według **wyników, ankiety przeprowadzonej podczas zorganizowanej w 2016 r. przez firmę analityczną Gartner konferencji poświęconej centrom danych, „ponad 80% respondentów uznało swoje sieci rozległe za słabe i wolne, podatne na przestoje lub zbyt drogie, podczas gdy jedynie 20% respondentów stwierdziło, że ich sieci rozległe są przystępne cenowo i odpowiednio sprawne”².**

Wysoki całkowity koszt posiadania

- W przypadku tradycyjnych sieci rozległych **przepustowość jest droga**. Sieci te zapewniają łączność między oddziałami i jakość usług dzięki zastosowaniu drogich łączy w technologii MPLS. Ponadto czas wdrożenia tych łączy jest długi, co negatywnie wpływa na rozwój i ogólną produktywność przedsiębiorstwa.
- Wspomniane sieci cechują się również **większą złożonością**. Zastosowanie różnych zabezpieczeń i funkcji sieciowych sprawia, że pojawia się więcej elementów do monitorowania. Nasila ten problem zarządzanie z poziomu interfejsu wiersza poleceń. Interfejs ten wymaga poświęcenia mnóstwa czasu na śledzenie zapisów dziennika, zwiększa możliwość pojawienia się błędów człowieka oraz obniża ogólną produktywność pracowników.

² Gartner, Market Guide for WAN Edge Infrastructure, Andrew Lerner, Neil Rickard, marzec 2017 r.

Wdrożenia i widoczność w chmurze

- Tradycyjne sieci rozległe oferują **niezadowalającą widoczność chmury**, ponieważ mogą jedynie zapewnić widok na poziomie pakietów i tras, a nie aplikacji.
- Sieci te mogą również tworzyć **wąskie gardła wydajności**, które negatywnie wpływają na produktywność pracowników przedsiębiorstwa, zwłaszcza w kontekście rosnących wymagań dotyczących chmury. Ze względu na fakt, że ruch jest przekierowywany przez centrum danych, dane mają do pokonania dłuższą trasę i pojawiają się większe opóźnienia. Ponadto **ruch w tradycyjnej sieci rozległej nie jest inteligentny** i nie można za pomocą reguł przypisać go do odpowiedniego kanału szerokopasmowego.

Zabezpieczenia w centrum danych

- Używane przez większość tradycyjnych sieci rozległych prywatne łącza MPLS pozwalają na wdrożenie scentralizowanych zabezpieczeń. Ruch jest kierowany do centrum danych (ang: backhauling) w ramach typowej architektury sieci „hub-and-spoke”, w której wszystkie dane przechodzące przez sieć mogą być sprawdzone i przefiltrowane. O ile sam ruch jest zabezpieczony, wiąże się to jednak ze **spadkiem wydajności**.
- Tradycyjne sieci rozległe celowo **nie mają bezpośredniego dostępu do Internetu** za pośrednictwem łączy publicznych, co ogranicza możliwości korzystania w ich ramach ze stale



rozszerzającej się oferty usług chmurowych, w tym aplikacji SaaS.

- Do tego niektóre przedsiębiorstwa kupują rozwiązania sieciowe i zabezpieczenia oddzielnie, co skutkuje pojawianiem się **odrębnych urządzeń z oddzielnymi konsolami**, a to z kolei **ogranicza widoczność sieci**. W efekcie wszystkie operacje stają się bardziej złożone i czasochłonne.

Odporność na awarie i ciągłość działania

- Dostępne w przypadku sieci rozległych opcje awaryjnego przełączania dla MPLS (sieci 4G/3G) **nie są niezawodne** i przedsiębiorstwa nie mają zapewnionej wymaganej **odporności na awarie**. Może to powodować zakłócenia i przestoje w realizacji regularnych operacji biznesowych oraz powodować spadki produktywności.

02 SZEŚĆ KWESTII DO ROZWAŻENIA PODCZAS WYBORU SIECI SD-WAN

Stojące w obliczu wszystkich wspomnianych problemów z tradycyjnymi sieciami rozległymi przedsiębiorstwa potrzebują innej infrastruktury, która będzie prostsza, bardziej opłacalna i zdolna do lepszej obsługi aplikacji chmurowych.

W przeciwieństwie do tradycyjnych architektur sieci rozległej **sieć SD-WAN** może dynamicznie rozprowadzać ruch po różnych lokalizacjach i automatycznie reagować na zmieniające się reguły dotyczące aplikacji, aby zapewnić większą wydajność. W efekcie sieć taka jest sprawniejsza i bardziej opłacalna w porównaniu z tradycyjnymi rozwiązaniami sieciowymi.

Firma analityczna Gartner przewiduje, że „w ciągu następnych dwóch lat 25% przedsiębiorstw wdroży sieć rozległą definiowaną programowo”³. Dostępne na rynku produkty SD-WAN różnych producentów znacznie się jednak od siebie różnią w kategoriach funkcjonalności, opcji wdrożenia i zarządzania, zapewnianej widoczności, kosztów oraz wskaźnika ceny do wydajności.

Poniżej przedstawionych zostało sześć najważniejszych korzyści, które powinny zostać uzyskane po zakupie dla przedsiębiorstwa rozwiązania SD-WAN.

³ Gartner, Market Guide for WAN Edge Infrastructure, Andrew Lerner, Neil Rickard, marzec 2017 r.



1. WDRAŻANIE APLIKACJI CHMUROWYCH

Według firmy analitycznej IDC sprzedaż usług chmury publicznej rośnie w tempie 28,6% r/r⁴. Dynamika ta skutkuje upowszechnianiem się aplikacji chmurowych w przedsiębiorstwach. Obecnie typowe przedsiębiorstwo korzysta już z około 30 różnych aplikacji SaaS⁵.

Sprawy komplikuje fakt, że rosnący odsetek osób, które dokonują zakupu i korzystają z aplikacji SaaS, to osoby niebędące specjalistami ds. IT. W 2017 r. kupujący niereprezentujący działu IT wydali na zakup tych aplikacji więcej (150,7 mln USD) niż kupujący z działów IT (64,7 mln USD)⁶.

W perspektywie dalszego wzrostu liczby aktywnych aplikacji chmurowych wdrożenie sieci SD-WAN może ułatwić przedsiębiorstwom obsługę większej liczby aplikacji SaaS bez uszczerbku dla wydajności sieci lub produktywności użytkowników końcowych. W szczególności sieć SD-WAN eliminuje konieczność przesyłania ruchu generowanego przez aplikacje chmurowe przez centrum danych, ponieważ zapewnia bezpośredni dostęp internetowy do sieci w odległych lokalizacjach. To rozwiązanie w wyraźnym stopniu zmniejsza opóźnienia i ogranicza liczbę utraconych pakietów.

⁴ „Worldwide Public Cloud Services Revenue Growth Remains Strong in the First Half of 2017”, IDC, 6 listopada 2017 r.

⁵ Nirav Shah and Bill McGee, „[Empowering Distributed Enterprises with Secured SD-WAN](#)”, Fortinet, dostęp z dnia 16 grudnia 2017 r.

⁶ „[Technology Purchases from Line of Business Budgets Forecast to Grow Faster Than Purchases Funded by the IT Organization](#)”, IDC, 23 marca 2017 r.



Z sieci SD-WAN mogą korzystać przedsiębiorstwa z wielu branż, chociaż największe korzyści mogą być uzyskane w branżach wymienionych poniżej:

- **Ochrona zdrowia.** Przedsiębiorstwa z branży ochrony zdrowia zazwyczaj mają wiele placówek, z których użytkownicy muszą mieć dostęp do usług SaaS używanych na potrzeby m.in. opieki nad pacjentami oraz obsługi elektronicznej dokumentacji medycznej, księgowości i finansów. Wszystkie te funkcje wymagają dużej przepustowości, a tradycyjne sieci rozległe nie są już zdolne do obsłużenia rosnących wymogów związanych z aplikacjami chmurowymi w szerokiej infrastrukturze tego typu przedsiębiorstw. Bezpieczna sieć SD-WAN oferuje natomiast elastycznie regulowaną, przystępną cenowo przepustowość, aby lepiej zaspokoić rosnące potrzeby personelu medycznego w zakresie korzystania ze wspomnianych aplikacji, dzięki czemu można lepiej opiekować się pacjentami i zapewnić bezpieczeństwo prywatnym informacjom medycznym.

- **Sieci sprzedaży detalicznej.** Obecnie sieci sprzedaży detalicznej łączą sprzedaż stacjonarną ze sprzedażą internetową i w coraz większym stopniu polegają na konwergentnym pakiecie chmurowych narzędzi do obsługi handlu elektronicznego, aby za jego pomocą koordynować wszystkie aspekty prowadzonej działalności, w tym zarządzanie zapasami, przetwarzanie płatności i analizę danych klientów. Do obsługi setek lub nawet tysięcy swoich placówek sieci sprzedaży detalicznej mogą stosować sieci SD-WAN, aby zapewnić lepsze działanie wielu aplikacji sieciowych w bardzo rozproszonych lokalizacjach, nawet w okresach zwiększonej sprzedaży.

- **Przetwórstwo przemysłowe.** Podobnie jak w przypadku sieci sprzedaży detalicznej nowoczesne przedsiębiorstwa z branży przemysłowej i przetwórstwa przemysłowego korzystają z różnych skoordynowanych aplikacji SaaS w celu lepszej realizacji wielu różnych swoich funkcji na różnych obszarach w kraju i za granicą. Rygorystyczne warunki i krytyczny charakter związany z wykonywaniem tych funkcji oznacza, że wspomniane aplikacje nie mogą być bez poważnych konsekwencji ograniczane przez limity dotyczące wydajności. Bezpieczna sieć SD-WAN oferuje przystępną cenowo i elastycznie regulowaną przepustowość na potrzeby obsługi różnych funkcji, w tym funkcji automatycznego zarządzania łańcuchem dostaw, sprzedaży międzynarodowej i sterowania przemysłowego istotnego z punktu widzenia bezpieczeństwa pracowników i optymalizacji produktywności.

2. INFORMACJE O APLIKACJACH

Statyczny charakter infrastruktury tradycyjnej sieci rozległej może istotnie zmniejszyć wydajność aplikacji w sieci rozproszonej. Dobre rozwiązanie SD-WAN powinno obsługiwać coraz częściej niezbędną potrzebę zapewnienia **pełnej widoczności aplikacji**, aby administratorzy mogli łatwiej monitorować wzorce ruchu i zarządzać nimi, równoważyć zapotrzebowanie na przepustowość oraz skalować wydajność w ramach całego rozproszonego przedsiębiorstwa. W tym przypadku sieć SD-WAN przechowuje bieżące informacje o wszystkich aplikacjach i optymalizuje ich działanie w drodze inteligentnego trasowania oraz nadawania aplikacjom odpowiednich priorytetów na podstawie przepustowości sieci i potrzeb użytkowników. Informacje o każdej aplikacji obejmują jej stan i zapotrzebowanie na zasoby.

3. ROZPOZNAWANIE ŚCIEŻEK SIECIOWYCH

Obecność funkcji rozpoznawania ścieżek sieciowych oznacza, że dane rozwiązanie jest zdolne do **automatycznego nadawania priorytetów trasowaniu aplikacji** w ramach dostępnej przepustowości sieci na podstawie specyfiki konkretnej aplikacji i użytkownika. Wspomniana funkcja zapewnia odpowiednie poziomy usług konkretnych aplikacji i jest zdolna do dynamicznego wyboru najlepszego w danej sytuacji łącza/połączenia sieci rozległej. Dzięki temu można nadać odpowiednie priorytety poszczególnym aplikacjom na podstawie ich znaczenia, pory dnia i innych czynników.



W przeciwieństwie do tradycyjnych usług sieci rozległej opartych na MPLS (o ograniczonej i drogiej dostępności) sieci SD-WAN zapewniają przystępną cenowo alternatywę dla tradycyjnych routerów sieci rozległej i obsługują dowolne metody przesyłu danych (MPLS, Internet, LTE itp.). Sieci SD-WAN pozwalają ponadto na inteligentny podział obciążenia w przypadku ruchu między wieloma połączeniami szerokopasmowymi, aby zapewnić większą efektywność sieci i dynamiczne wykonywanie operacji w ramach rozproszonego przedsiębiorstwa. Funkcja rozpoznawania ścieżek sieciowych pozwala również zmaksymalizować korzyści płynące z lepszych możliwości podłączania sieci SD-WAN.



4. ZINTEGROWANE ZABEZPIECZENIA I ZGODNOŚĆ

Bez scentralizowanych mechanizmów zabezpieczeń stosowanych w związku z kierowaniem ruchu przez centrum danych, zastąpienie technologii MPLS bezpośrednimi połączeniami szerokopasmowymi z Internetem wymaga wdrożenia dodatkowych zabezpieczeń w infrastrukturze przedsiębiorstwa, zwłaszcza w sytuacji, gdy zwiększa się liczba i stopień wyrafinowania cyberataków.

Rozproszone funkcje sieciowe i funkcje zabezpieczeń w sieciach rozległych okazały się być nieskuteczne i nieefektywne. Obecnie, według firmy analitycznej Gartner, „sieci rozległe definiowane programowo zawierają już zabezpieczenia brzegu sieci, ale ponad 90% dostawców tych sieci nie jest tradycyjnymi dostawcami zabezpieczeń,

co sprawia, że klienci zastanawiają się, czy mogą polegać wyłącznie na takich wbudowanych mechanizmach tego rodzaju”⁷. Taka sytuacja sprawia, że odpowiednie zabezpieczenie sieci może wiązać się z wyższymi wydatkami na konfigurację i większym całkowitym kosztem posiadania, nie wspominając już o wyższym ryzyku wynikającym z potencjalnych luk w zabezpieczeniach mogących występować wskutek zastosowania odmiennych technologii sieciowych i technologii zabezpieczeń. W perspektywie 50% wzrostu ruchu szyfrowanego protokołem SSL w najbliższych latach, ruch taki musi być starannie sprawdzany pod kątem złośliwego oprogramowania bez uszczerbku dla wydajności sieci⁸.

⁷Gartner, Four Architectures to Secure SD-WAN, Bjarne Munch, Greg Young, październik 2017 r.

⁸Nirav Shah and Bill McGee, „[Empowering Distributed Enterprises with Secured SD-WAN](#)”, Fortinet, dostęp z dnia 16 grudnia 2017 r.



Mechanizmy zabezpieczeń dostępne w ramach rozwiązania klasy NGFW to podstawowy wymóg związany z zapewnieniem bezpośredniego dostępu do Internetu w architekturze sieci SD-WAN. Są one niezbędne w celu ograniczenia ryzyka udanych ataków w ramach całej szerokiej sieci. Funkcje zabezpieczeń na zaporze NGFW zdolne do obsługi sieci SD-WAN powinny obejmować:

- **Zintegrowaną platformę**, która obejmuje zarówno funkcje sieciowe, jak i zabezpieczeń w ramach jednego urządzenia, co poprawia bezpieczeństwo rozproszonego środowiska przy jednoczesnym uproszczeniu kontroli i obniżeniu kosztów inwestycji.
- **Funkcję inspekcji SSL**, która chroni rozproszoną sieć przed złośliwym oprogramowaniem i innymi

zagrożeniami ukrytymi w zaszyfrowanym ruchu sieciowym. Wspomniana funkcja może odszyfrowywać sesje, weryfikować zaszyfrowane pakiety oraz znajdować i blokować ewentualne zagrożenia.

- **Funkcję filtrowania stron WWW**, która jest pierwszą linią obrony przed atakami z sieci WWW. Funkcja ta blokuje dostęp do złośliwych, zhakowanych lub nieodpowiednich stron WWW.
- **Wysoko wydajne rozwiązania IPsec VPN** są niezbędne w udanych wdrożeniach sieci SD-WAN. Mechanizmy IPsec zapewniają bezpieczną wymianę danych między dwoma lub więcej hostami w drodze uwierzytelniania i szyfrowania każdego pakietu IP w ramach sesji komunikacyjnej wirtualnej sieci prywatnej.
- **Funkcje raportowania i monitorowania zgodności** ułatwiają zapewnienie przestrzegania standardów branżowych i przepisów prawnych, tym samym ograniczając ryzyko narażenia się na kary finansowe i koszty obsługi prawnej na wypadek naruszenia bezpieczeństwa. Zapora NGFW powinna również udostępniać funkcje raportowania służące do śledzenia w czasie rzeczywistym sytuacji dotyczącej zagrożeń, aby ułatwiać dokonywanie oceny ryzyka, wykrywanie potencjalnych problemów i łagodzenie ich skutków. Funkcje te powinny również monitorować reguły i zasady dla zapory oraz automatyzować audyty zgodności.

5. OBSŁUGA WIELU KANAŁÓW SZEROKOPASMOWYCH

Jak już wspomniano przy opisie funkcji rozpoznawania ścieżek sieciowych, kontroler sieci SD-WAN powinien być zdolny to mieszania i dopasowywania do siebie różnych łączy szerokopasmowych (Internet, MPLS, LTE itp.) na potrzeby bezpośredniego korzystania z publicznych łączy internetowych. Sieć SD-WAN jest niezależna od metody przesyłu danych i operatora, możliwości jej podłączania nie zależą już zatem od technologii MPLS i zawodnych funkcji awaryjnego przełączania w sieciach 3G/4G, które narażają operacje biznesowe na ryzyko przestojów. Dzięki wykorzystaniu publicznego Internetu jako opcji awaryjnego przełączania sieć SD-WAN oferuje **większą nadmiarowość i odporność na awarie**, co zapobiega spadkom wydajności i przestojom.

6. CAŁKOWITY KOSZT POSIADANIA

Zastosowanie publicznych łączy szerokopasmowych oznacza, że drogie łącza MPLS mogą być zastąpione przystępniejszymi cenowo opcjami takimi jak publiczne łącza internetowe lub łącza LTE. Może to przynieść wymierne oszczędności kosztów operacyjnych w porównaniu z tradycyjnymi sieciami rozległymi.

Ponadto dzięki zintegrowaniu funkcji kontroli sieci i zabezpieczeń w ramach **jednej konsoli do zarządzania** sieć SD-WAN staje się bardziej przejrzysta i łatwiejsza w zarządzaniu. W efekcie pracownicy zajmujący się zabezpieczeniami sieci mogą poświęcać mniej czasu na



zarządzanie różnymi aspektami operacji dotyczących sieci i zabezpieczeń oraz związanych z nimi zdarzeń.

Dobra sieć SD-WAN powinna również obsługiwać **bezobsługowe wdrażanie** w celu efektywniejszego podłączania do niej kolejnych oddziałów. Funkcje te pozwalają przedsiębiorstwom dynamiczniej się rozwijać dzięki funkcjom szybkiego przydzielania zasobów, sprawnej konfiguracji, automatycznego uwierzytelniania, centralnego monitorowania i pomocy. Wspomniana możliwość bezobsługowego wdrażania pozwala zaoszczędzić mnóstwo czasu w porównaniu z bardziej pracochłonnymi procesami podłączania kolejnych oddziałów do środowiska tradycyjnej sieci rozległej.

PODSUMOWANIE

Tradycyjne sieci rozległe przestały już być efektywnym rozwiązaniem dla dzisiejszych rozproszonych przedsiębiorstw. Dzięki wdrożeniu sieci rozległych definiowanych programowo (SD-WAN) przedsiębiorstwa przezwyciężają natomiast istotne problemy związane z bezpieczeństwem i funkcjonowaniem sieci. Firma analityczna Gartner wskazuje, że „do 2018 r. ponad 40% projektów odświeżenia infrastruktury brzegowej sieci rozległej będzie oparta o urządzenia vCPE lub SD-WAN, a nie tradycyjne routery⁹”.

⁹Gartner, Market Guide for WAN Edge Infrastructure, Andrew Lerner, Neil Rickard, marzec 2017 r.

Na rynku dostępnych jest obecnie wiele różnych rozwiązań SD-WAN, decydenci ds. IT powinni zatem starannie sprawdzić każde z nich. Może w tym pomóc powyższe sześć kwestii do rozważenia. Warto przy tym pamiętać, że Fortinet Secure SD-WAN integruje rozszerzone funkcje sieci SD-WAN w ramach sprawdzonego rozwiązania korzystającego z zabezpieczeń i funkcji sieciowych następnej generacji, które poprawiają efektywność działania sieci bez uszczerbku dla jej bezpieczeństwa.

The image features a dark blue, monochromatic background of a city skyline at night. Overlaid on the city are several glowing white dots connected by thin, curved white lines, creating a network or data flow visualization. The dots are positioned at various heights and locations, suggesting a global or multi-tier network architecture. The city buildings are silhouetted against a slightly lighter blue sky, with some lights visible on the buildings.

FORTINET®

www.fortinet.com

Copyright © 2018 Fortinet, Inc. Wszelkie prawa zastrzeżone. 02.02.18

154319-A-0-EN