Zaawansowane zabezpieczenia jako istotny element skutecznego rozwiązania SD-WAN

Spis treści

Streszczenie

Tradycyjne sieci rozległe (WAN) współczesnych przedsiębiorstw nie są już zdolne do sprostania wymaganiom transformacji cyfrowej i obsługi dużej liczby pracowników zdalnych. Modernizacja infrastruktury sieci rozległej stała się zatem nieunikniona[1]. W tym kontekście wiele przedsiębiorstw wdraża jako zamiennik sieci rozległe definiowane programowo (SD-WAN). Należy jednak zauważyć, że większości dostępnych obecnie na rynku rozwiązań SD-WAN brakuje kompleksowych, zaawansowanych funkcji, zwłaszcza w zakresie wbudowanych zabezpieczeń.

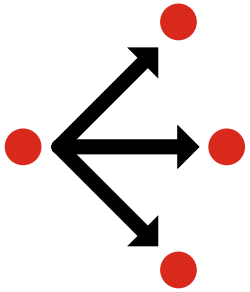
Aby dokonać pomyślnej transformacji sieci rozległej, przedsiębiorstwo potrzebuje podejścia, w ramach którego zaawansowane funkcje sieciowe i zabezpieczenia zostaną zintegrowane w jednym bezpiecznym rozwiązaniu SD-WAN. Ujednolicona platforma dla takiego rozwiązania może następnie zapewnić spójną ochronę i uprościć infrastrukturę sieciową, pozwalając jednocześnie na szczegółową kontrolę opartą na zasadach i zerowym zaufaniu do użytkowników.

Zabezpieczenia jako brakujące ogniwo w transformacji sieci rozległej

Wskutek połączenia nowych narzędzi cyfrowych, chmury obliczeniowej i dużej liczby pracowników wymagających zdalnego dostępu, tradycyjne architektury sieci rozległej nie są już zdolne do obsługi ruchu na brzegu sieci. Ponadto tradycyjne sieci rozległe używają drogich łączy MPLS oraz scentralizowanego systemu zabezpieczeń polegającego na przekierowywaniu ruchu przez centrum danych (backhauling) w przedsiębiorstwie. Taka zależna struktura przyczynia się do powstawania wąskich gardeł, które pogarszają wydajność użytkowników końcowych.

Jako nowocześniejszą alternatywę, wiele przedsiębiorstw wybiera do obsługi swoich potrzeb w zakresie wydajności sieci rozproszonych rozwiązanie SD-WAN. Rozwiązanie to zapewnia znacznie większe korzyści niż łącza MPLS zarówno pod względem przepustowości, jak i kosztów, ponieważ umożliwia dynamiczny wybór między powszechnie dostępnymi łączami internetowymi (np. LTE, DSL, 4G/5G, Ethernet). Jedną z istotnych zmian związanych z wdrożeniem rozwiązania SD-WAN jest jednak to, że takie bezpośrednie połączenia z chmurami i zasobami internetowymi omijają zabezpieczenia typu „hub-and-spoke” stosowane w tradycyjnych architekturach. Tak szerokie narażenie się na zagrożenia wymaga doskonałych zabezpieczeń, a wiele z dostępnych na rynku rozwiązań SD-WAN nie ma lub prawie nie ma żadnych takich wbudowanych zabezpieczeń.

W rezultacie wiele przedsiębiorstw dodaje do swojej infrastruktury różne narzędzia mające na celu wyeliminowanie problemów związanych z używanym rozwiązaniem SD-WAN. Takie silosowe podejście podnosi zarówno nakłady inwestycyjne, jak i koszty operacyjne, jednocześnie zwiększając złożoność infrastruktury i tworząc potencjalne luki umożliwiające cyberprzestępcom ominięcie zabezpieczeń. Liczba i stopień zaawansowania ataków stale rośnie, zintegrowane zabezpieczenia stają się zatem coraz bardziej istotne w kontekście każdego projektu transformacji sieci rozległej.



Łącza MPLS nie są zdolne sprostać radykalnym zmianom w wymaganiach sieciowych spowodowanych transformacją cyfrową i koniecznością obsługi coraz bardziej rozproszonej siły roboczej. Rozwiązanie SD-WAN nie będzie mieć z tym problemów[2].

Zalety bezpiecznego rozwiązania SD-WAN

Udana transformacja sieci rozległej musi być równie użyteczna dla wszystkich użytkowników oraz zapewniać bezpieczeństwo i efektywne działanie w skali. Aby uniknąć pułapek związanych z nieuporządkowanym podejściem do wdrożenia rozwiązania SD-WAN, przedsiębiorstwo powinno znaleźć produkt, który łączy w sobie zaawansowane funkcje sieciowe i zabezpieczenia. Powinien on ponadto oferować spójną ochronę, większą wydajność operacyjną oraz zaawansowane mechanizmy pozwalające przewidywać zmieniające się z czasem wymagania sieci.

Spójna ochrona

Zintegrowane bezpieczne rozwiązanie SD-WAN powinno zapewniać spójną ochronę, która kosztem bezpieczeństwa nie narazi na szwank wydajności. Ponadto powinno mieć wbudowane zaawansowane zabezpieczenia, w tym funkcje inspekcji danych zaszyfrowanych za pomocą protokołów SSL i TLS. Warto pamiętać, że większość rozwiązań SD-WAN nie oferuje odpowiedniej inspekcji, mimo że szyfrowanie SSL/TLS pokrywa obecnie około 85% ruchu sieciowego[3]. Niektóre rozwiązania oferują co prawda deszyfrowanie, nie są jednak zdolne do przeprowadzenia inspekcji całego ruchu, ponieważ w drastyczny sposób obniżają przez to wydajność sieci. Inne rozwiązania nie oferują znowu deszyfrowania TLS 1.3, co prowadzi do dopuszczenia do sieci wszelkich złośliwych kodów ukrytych w ruchu szyfrowanym tym protokołem. Jeśli bowiem nie zostanie sprawdzony cały ruch, złośliwe oprogramowanie i inne zagrożenia spokojnie ominą zabezpieczenia na brzegu sieci.

Nadawanie priorytetów aplikacjom krytycznym. Same łącza nie wystarczą do zapewnienia bezpieczeństwa, zwłaszcza w przypadku powszechnej pracy zdalnej. Efektywne rozwiązanie SD-WAN musi być zdolne do identyfikacji szerokiego zestawu aplikacji, aby móc uwzględnić wszystkie możliwe scenariusze. Zaawansowane, samoregenerujące się funkcje automatyzacji rozwiązania WAN mogą pomóc w zapewnieniu spójnego udostępniania aplikacji wszystkim użytkownikom. Wiele rozwiązań SD-WAN nie jest zdolnych ani do obsługi dużej liczby sygnatur aplikacji, ani do optymalizacji wydajności aplikacji. Prowadzi to do zmiennej użyteczności rozwiązania lub niemożności obsłużenia wszystkich potencjalnych przypadków użycia.

Zmniejszona powierzchnia ataku. Autonomiczne rozwiązanie SD-WAN to po prostu zaproszenie do ataku na sieć. Ochrona tego rozwiązania za pomocą autonomicznych zabezpieczeń ma poważne ograniczenia, ponieważ nie są one zdolne do dostosowania się do wymogów dynamicznych środowisk komunikacyjnych. Aby zatem chronić nowoczesne środowiska sieci rozległej, każde wdrożone rozwiązanie SD-WAN musi mieć wbudowane zaawansowane zabezpieczenia. Dzięki temu użytkownicy pracujący zdalnie i stacjonarnie oraz centra danych mogą korzystać ze wspólnego zestawu zasad bezpieczeństwa i kryteriów ich egzekwowania. Funkcje sieciowe, komunikacyjne i zabezpieczające zostaną wówczas tak ściśle zintegrowane, że mogą działać jako pojedyncze, ujednolicone rozwiązanie, nawet w warunkach dużej dynamiki.

Kompleksowe funkcje analityczne i raportowanie. Bezpieczne rozwiązanie SD-WAN musi zapewniać przedsiębiorstwu widoczność danych dotyczących wydajności sieci i aplikacji (zarówno w czasie rzeczywistym, jak i historycznie). Ponadto musi oferować rozszerzone funkcje analityczne i mechanizmy zapewnienia zgodności z przepisami. Dzięki wyposażonej w takie bogate funkcje analityczne rozwiązania SD-WAN pojedynczej konsoli do zarządzania zarówno siecią, jak i zabezpieczeniami, przedsiębiorstwo może precyzyjnie dostosowywać swoje zasady biznesowe i zasady bezpieczeństwa w celu poprawy użyteczności dla wszystkich użytkowników.

W ciągu ostatniego roku liczba ataków za pomocą oprogramowania ransomware zwiększyła się o 150%, a kwoty płacone przez ofiary wzrosły o 300%[4].

Jeszcze bardziej uproszczona infrastruktura

Rozwiązanie SD-WAN, które pozwala na płynne skalowanie i integrację funkcji sieciowych i zabezpieczeń, upraszcza projektowanie architektury i obsługę sieci rozproszonej oraz zarządzanie nią. Ponadto pomaga przedsiębiorstwom zautomatyzować dołączanie do sieci oddziałów zdalnych, konsolidując jednocześnie infrastrukturę sieci i zabezpieczeń. W rezultacie skraca się średni czas usunięcia problemu (MTTR) i zwiększa się zwrot z inwestycji (ROI).

Zintegrowane zabezpieczenia i funkcje sieciowe. Oparte na platformie podejście do rozwiązania SD-WAN obejmuje zaawansowane funkcje sieciowe i zabezpieczenia, które zostały zaprojektowane z myślą o współdziałaniu w ramach jednolitego systemu, najlepiej działającego pod kontrolą tego samego systemu operacyjnego i zarządzanego z poziomu jednej konsoli. Dzięki temu wszystkie transakcje są widoczne i kontrolowane, a informacje o wszelkich zagrożeniach lub anomaliach są przekazywane do każdego zabezpieczenia w ekosystemie na potrzeby zapewnienia maksymalnej ochrony. Kompleksowa, bezpieczna platforma SD-WAN może również skonsolidować szereg produktów punktowych, takich jak routery, zapory i dostępowe serwery proxy oferujące dostęp do sieci na zasadzie zerowego zaufania (ZTNA), w ramach jednego produktu, co prowadzi do uproszczenia architektury i obniżenia nakładów inwestycyjnych.

Uproszczone zarządzanie i orkiestracja. Mechanizmy scentralizowanego zarządzania bezpiecznym rozwiązaniem SD-WAN sprawiają, że nowe usługi i zasady są zorientowane na aplikacje, a konfiguracje połączeń i zabezpieczeń oraz zmiany zasad mogą być bez problemu wdrażane w całej sieci rozległej. Ogranicza to liczbę błędów oraz eliminuje konieczność osobnej konfiguracji i obsługi poszczególnych urządzeń lub usług. Wspomniane mechanizmy udostępniają również bogate funkcje analityczne, które pokazują wydajność aplikacji w czasie rzeczywistym i w ujęciu historycznym, pozwalając na szybkie rozwiązywanie problemów oraz poprawę wartości kluczowych wskaźników wydajności takich jak średni czas reakcji.

Łatwość skalowania. Skuteczne bezpieczne rozwiązanie SD-WAN może być również dynamicznie skalowane do obsługi tysięcy oddziałów, bezproblemowo współpracować z istniejącą infrastrukturą fizyczną i chmurową oraz pozwalać na zdalne rozwiązywanie problemów w celu uniknięcia kosztownych fizycznych interwencji inżynierów.

SD-Branch, ZTNA i SASE

Skuteczne bezpieczne rozwiązanie SD-WAN powinno nie tylko być przygotowane na bieżące wyzwania, ale również mieć zdolność do obsługi potrzeb związanych z siecią i zabezpieczeniami, które pojawią się w niedalekiej przyszłości. W tym celu powinno być zatem elastyczne i spójne oraz z czasem obniżać całkowity koszt posiadania (TCO). W tym kontekście można wyróżnić trzy konkretne funkcje, które wspomniane rozwiązanie powinno oferować w celu zaspokojenia krótko-, średnio- i długoterminowych potrzeb dotyczących sieci rozproszonej.

Oddział definiowany programowo (SD-Branch). Gdy oddziały przedsiębiorstwa mają bezpośredni dostęp do połączeń internetowych (przez sieć SD-WAN), dyrektorzy ds. sieci muszą wdrażać zabezpieczenia nowej generacji, jednocześnie umożliwiając stosowanie sieci WAN wykorzystującej wiele ścieżek w celu poprawy wydajności aplikacji. Rozszerzające funkcjonalność rozwiązania SD-WAN bezpieczne funkcje SD-Branch chronią zarówno połączenia przewodowe, jak i bezprzewodowe, oraz umożliwiają kontrolę dostępu oraz widoczność i monitoring wszystkich urządzeń podłączonych do sieci w oddziale[5]. Skuteczne wdrożenie bezpiecznego rozwiązania SD-Branch powinno bezproblemowo zintegrować funkcje sieciowe i zabezpieczenia na brzegu sieci WAN (sieć lokalna [LAN], bezprzewodowa sieć lokalna, kontrola dostępu do sieci oraz bezprzewodowa sieć rozległa).

Przedsiębiorstwa potrzebują rozwiązania SD-Branch, które zapewni większy zasięg, elastyczność i możliwość dostosowania bez uszczerbku dla bezpieczeństwa[6].

Dostęp do sieci na zasadzie zerowego zaufania (ZTNA). Przedsiębiorstwa potrzebują przewidywalnej wydajności aplikacji w różnych lokalizacjach oraz bezpieczeństwa. Współczesny paradygmat „pracy z dowolnego miejsca" wymaga zapewnienia dostępu do aplikacji każdemu użytkownikowi. Wbudowane mechanizmy ZTNA zwiększają bezpieczeństwo i wygodę użytkowników, ponieważ ograniczają ryzyko pojawienia się nieproszonych gości oraz upraszczają dostęp zarówno dla użytkowników w sieci, jak i poza siecią. Podstawową zasadą działania mechanizmu ZTNA jest nieprzyznawanie dostępu do zasobów żadnemu użytkownikowi ani urządzeniu wyłącznie na podstawie jego lokalizacji w sieci[7]. Należy zatem szukać bezpiecznego rozwiązania SD-WAN, które oferuje wbudowany dostępowy serwer proxy.

Bezpieczny dostęp na brzegu sieci (SASE). Przedsiębiorstwa każdej wielkości coraz częściej tworzą i wdrażają różne usługi chmurowe oraz przenoszą do chmury swoje aplikacje. Architektura SASE łączy w sobie rozwiązania SD-WAN i ZTNA oraz inne usługi i funkcje, aby w ten sposób utworzyć bezpieczną sieć opartą na chmurze i przystosowaną do obsługi chmur[8]. Ramy te pozwalają na zastosowanie zabezpieczeń chmurowych i ujednoliconego zarządzania.

W kontekście bezpieczeństwa sieci wdrożenie modelu SASE wymaga zastosowania i korzysta z zasady zerowego zaufania[9].

Jednolite podejście do obsługi połączeń pochodzących z różnych sieci

Współczesne sieci rozproszone muszą być zdolne do ujednolicenia operacji w sieciach kampusów, oddziałów, biur domowych, chmur publicznych i lokalnych centrów danych. Rozwiązanie SD-WAN, które integruje pełny zestaw funkcji sieciowych i zabezpieczeń, może umożliwić tego rodzaju transformację do ujednoliconej sieci rozległej, zapewniając zarówno odpowiednią wydajność, jak i ochronę tam, gdzie jest to potrzebne, czyli na coraz bardziej zwiększającym się brzegu sieci.

Po pierwsze skuteczne bezpieczne rozwiązanie SD-WAN powinno zapewniać spójną obronę bez poświęcania wydajności na rzecz bezpieczeństwa (lub odwrotnie). Ponadto powinno dawać zespołom IT większe możliwości działania dzięki uproszczeniu architektury, zarządzania i bieżących operacji w praktycznie dowolnej skali. Na koniec bezpieczne rozwiązanie SD-WAN powinno stanowić platformę oferującą zabezpieczenia przystosowane do przyszłych wymogów, tak aby przedsiębiorstwo mogło we własnym tempie wdrażać zaawansowane udoskonalenia architektury (np. SD-Branch, ZTNA lub SASE).

[1] Kiran Desai, „The Rapid Rise Of SD-WAN As Digital Acceleration Takes Root", Forbes, 3 września 2021 r.

[2] Ibid.

[3] Nirav Shah, „The Challenges of Inspecting Encrypted Network Traffic", Fortinet, 4 sierpnia 2020 r.

[4] Brenda R. Sharton, „Ransomware Attacks Are Spiking. Is Your Company Prepared?", Harvard Business Review, 20 maja 2021 r.

[5] Michael Xie, „Without Security, SD-Branch Is Just 'SD Risk'", Forbes, 24 kwietnia 2020 r.

[6] Ibid.

[7] Mike Chapple, „Why it's SASE and zero trust, not SASE vs. zero trust", TechTarget, 15 grudnia 2020 r.

[8] Ibid.

[9] Ibid.

FORTINET®

www.fortinet.com

7 lutego, 2022

1247417-0-0-PL