Czas odstawić routery w oddziałach do lamusa

Cztery największe zalety rozwiązań Secure SD-WAN

Coraz więcej przedsiębiorstw rezygnuje z routerów w oddziałach na rzecz rozwiązań Secure SD-WAN, aby przejść na model chmurowy i poprawić jakość sieci. Rozwiązania Secure SD-WAN są nie tylko łatwe w zarządzaniu, ale także zasadniczo upraszczają obsługę sieci rozległej.

Przedsiębiorstwa powinny wdrażać rozwiązania Secure SD-WAN, aby pomóc użytkownikom ze swoich oddziałów w lepszym wykorzystaniu funkcji współpracy i komunikacji zintegrowanej oraz krytycznych aplikacji SaaS, a także zapewnić im łatwy dostęp do zasobów w chmurze. Poniżej przedstawiono cztery najważniejsze przewagi rozwiązań Secure SD-WAN nad starszymi architekturami opartymi na routerach zainstalowanych w oddziałach:

1. Sprawniejsze działanie aplikacji

Routery działają w oparciu o pakiety, nie mogą zatem zapewnić dobrej widoczności aplikacji. Jako że większość przedsiębiorstw korzysta z aplikacji i usług chmurowych, brak możliwości identyfikacji aplikacji i usług o znaczeniu krytycznym dla prowadzonej działalności oraz niestosowanie mechanizmów obsługujących specyficzne potrzeby w zakresie przepustowości i możliwości podłączania może pogorszyć użyteczność takich aplikacji i usług.

Rozwiązania SD-WAN nie tylko udostępniają wszystkie funkcje tradycyjnego routera, w tym zaawansowany routing i opcje podłączenia do sieci rozległej, ale również:

- umożliwiają identyfikację i przełączanie aplikacji z wykorzystaniem dynamicznego wyboru ścieżek sieciowych w celu zapewnienia odpowiedniej jakości połączenia;
- mogą identyfikować aplikacje oraz zapewniać wymagane poziomy usług (SLA) dla tysięcy aplikacji takich jak O365, SalesForce.com i usługi komunikacji zintegrowanej;
- pozwalają na codzienne aktualizacje definicji aplikacji biznesowych w celu zapewnienia dokładnej identyfikacji aplikacji i wyboru optymalnych ścieżek sieciowych.

Rozwiązania Secure SD-WAN są łatwe w zarządzaniu i zasadniczo upraszczają obsługę sieci rozległej.

2. Łatwiejsze skalowanie i znaczne oszczędności wydatków kapitałowych (CapEx), jak i kosztów operacyjnych (OpEx)

Wydajność drogich łączy MPLS jest z góry określona, co oznacza, że nagły skok ruchu (wynikający na przykład z pojawienia się wielu połączeń w ramach komunikacji zintegrowanej lub potrzeby przetwarzania dużej ilości danych) może dotknąć każde przedsiębiorstwo. Dodawanie nowych routerów w oddziałach jest również procesem koszto- i czasochłonnym.

Rozwiązania SD-WAN mogą jednak pomóc w zastąpieniu łączy MPLS łączami szerokopasmowymi (DSL, 4G/5G, Ethernet) i uzyskaniu w wielu przypadkach nawet 40% oszczędności na kosztach operacyjnych. Ponadto umożliwiają przedsiębiorstwom dynamiczne i bezpieczne skalowanie do dziesiątek tysięcy oddziałów, bezproblemowe współdziałanie z istniejącymi infrastrukturami fizycznymi i chmurowymi oraz zdalne rozwiązywanie problemów w celu wyeliminowania kosztownych interwencji fizycznych ze strony wykwalifikowanych techników. Rozwiązanie Secure SD-WAN konsoliduje również w jednym produkcie szereg produktów punktowych, takich jak routery, zapory i narzędzia optymalizacji sieci rozległej, co pozwala uzyskać znaczne oszczędności wydatków kapitałowych.

3. Uproszczone zarządzanie i orkiestracja

Routery w oddziałach są często trudne w instalacji, aktualizacji i utrzymaniu (nawet jeśli w założeniu miały być rozwiązaniem wygodnym i łatwym w obsłudze). Ich konfiguracja wymaga znajomości interfejsu wiersza poleceń routera, a ze względu na jego złożoność rzadko może być wykonywana przez niespecjalistów pracujących zazwyczaj w oddziale.

Mechanizmy scentralizowanego zarządzania rozwiązaniami Secure SD-WAN sprawiają, że nowe usługi i reguły są zorientowane na aplikacje, a konfiguracje połączeń i zabezpieczeń oraz zmiany reguł mogą być bez problemu wdrażane kompleksowo w całej sieci rozległej, co 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.

4. Zintegrowane zabezpieczenia i praca sieciowa

Routery w oddziałach nie są w żadnym razie w pełni zintegrowanymi rozwiązaniami z zakresu bezpieczeństwa i sieci. Gdy łącza MPLS oferują rozszerzenie w postaci tzw. „split tunneling", aby umożliwić bezpośredni dostęp do Internetu, routery te nie dają odpowiedniej albo czasami wręcz żadnej możliwości zarządzania łączami lub połączeniami. Nawet gdy ruch sieciowy zostanie przeniesiony na alternatywną ścieżkę, routery te nie zapewniają błyskawicznego (krótszego niż sekunda) proaktywnego przełączania zapobiegającego zrywaniu połączeń, nie udostępniają funkcji minimalizowania problemów z przesyłaniem danych ani nie oferują mechanizmów takich jak dynamiczne buforowanie zmian opóźnienia transmisji. Nie są również zdolne do aktywnego regulowania ruchu, zanim przeciążenia nie staną się problemem. Co gorsza, ze względu na brak skutecznego zabezpieczenia połączenia wychodzące poza sieć MPLS narażają przedsiębiorstwo na dodatkowe ryzyko.

Należy zauważyć, że większość udanych wdrożeń rozwiązań SD-WAN wymaga w pełni zintegrowanego podejścia do bezpieczeństwa. Przykładem takiego zintegrowanego podejścia są zapory następnej generacji (NGFW), których podstawowymi elementami są funkcje ochrony przed włamaniami i złośliwym kodem, filtrowanie stron WWW oraz inspekca SSL. Bez takiego zintegrowanego podejścia rozwiązania SD-WAN stają się dla cyberprzestępców tylko kolejną ścieżką ataku na sieć przedsiębiorstwa.

Prawdziwa platforma potrzebuje narzędzi specjalnie zaprojektowanych do współdziałania jako jeden system, najlepiej z każdym elementem pracującym na tym samym systemie operacyjnym i zarządzanym z poziomu jednej konsoli. W ten sposób wszystkie transakcje są widoczne i kontrolowane, a informacje o wszelkich zagrożeniach i nietypowych zachowaniach — przekazywane do każdego zabezpieczenia w celu zapewnienia maksymalnej ochrony. W ramach takiego zintegrowanego systemu mechanizmy podłączania i funkcje sieciowe rozwiązania SD-WAN są nie tyle ściślej powiązane z zabezpieczeniami zainstalowanymi na platformie, ale są po prostu z nimi tożsame.

Co dalej

Z powyższych rozważań wynika, że niezbędne jest nie tylko dostrzeżenie potrzeby odejścia od tradycyjnej strategii sieci rozległej opartej na routerach, ale również staranne dobranie rozwiązań Secure SD-WAN zapewniających pełną gamę funkcji oraz możliwie jak największą liczbę zastosowań. W efekcie nowe wdrożenie rozwiązań SD-WAN nie tylko zaspokoi obecne potrzeby przedsiębiorstwa, ale będzie również zdolne do obsługi dynamicznie zmieniających się wymagań.

września 2, 2020 1:37 PM

692249-0-0-PL

Sandu SSD:Users:Shared:Previously Relocated Items:Security:proiecte DTP:TRANSFER:Argos-28.08.2020(Fortinet):livrat:Security Driven Networking_PL:flyer-SD-WAN-branch-routers-A4 Folder:flyer-SD-WAN-branch-routers-A4