

**Konsolidacja funkcji
sieciowych i zabezpieczeń
może zmniejszyć podatność
oddziałów na ataki**

Streszczenie

W miarę korzystania przez przedsiębiorstwa z kolejnych aspektów transformacji cyfrowej (DX) — takich jak rozwiązania chmurowe, Internet rzeczy (IoT) i urządzenia mobilne — ich powierzchnia ataku gwałtownie się zwiększa, a ryzyko włamania rośnie. Organizacje rozproszone z co najmniej jednym oddziałem zdalnym korzystają na przykład z sieci rozległych definiowanych programowo (SD-WAN). Sama sieć SD-WAN nie rozwiązuje jednak trzech powiązanych ze sobą problemów dotyczących bezpieczeństwa, do których należą 1) konieczność ochrony wielu brzegów sieci WAN, 2) brak wglądu w informacje o punktach końcowych i 3) złożoność infrastruktury oddziałów. Rozwiązanie, w którym funkcje sieciowe i zabezpieczenia zostały skonsolidowane, może natomiast pomóc dyrektorom odpowiedzialnym za technologie sieciowe i działanie sieci w uproszczeniu infrastruktury, zapewniając jednocześnie większe bezpieczeństwo i wydajność w oddziałach. Zastosowanie w organizacjach rozproszonych zintegrowanego podejścia wykorzystującego koncepcję oddziału definiowanego programowo (SD-Branch) może poprawić widoczność, kontrolę i łatwość zarządzania, a jednocześnie obniżyć całkowity koszt posiadania (TCO).

Spis treści

01 Zwiększająca się powierzchnia ataku w przedsiębiorstwie rozproszonym.....	4
02 Zabezpieczanie krawędzi sieci WAN.....	5
03 Zabezpieczanie punktów końcowych	7
04 Zabezpieczanie warstwy dostępowej oddziału.....	8
05 Kompleksowe bezpieczeństwo oddziału.....	10

01 Zwiększająca się powierzchnia ataku w przedsiębiorstwach rozproszonych

Zastosowanie nowych technologii w ramach transformacji cyfrowej (DX) jest źródłem specyficznych trudności dla rozproszonych organizacji posiadających sieci oddziałów.

Konieczność zabezpieczenia wielu krawędzi sieci

WAN. Krawędź sieci WAN w sieci oddziałów staje się coraz trudniejsza do ochrony. Pierwszym problemem jest szybko rosnące natężenie ruchu — skutek rosnącej popularności aplikacji typu SaaS (oprogramowanie jako usługa), narzędzi chmurowych, technologii Voice over IP (VoIP) i usług wideo. Istotne są także rozprzestrzenianie się zagrożeń w bezprzewodowych punktach dostępowych oraz liczba i typy urządzeń, które uzyskują do nich dostęp. Efektem takiej ewolucji krawędzi sieci WAN są luki, które wymagają zabezpieczenia.

Wgląd w informacje o stanie sieci. Sieci oddziałów muszą też obsługiwać wiele innych urządzeń końcowych (przewodowych i bezprzewodowych). Należą do nich różne osobiste urządzenia mobilne pracowników, dostawców i gości, a także coraz liczniejsze i bardziej różnorodne urządzenia należące do Internetu rzeczy (IoT).

Nie wszystkie mają zaktualizowane oprogramowanie systemowe, w którym „załatano” wszystkie luki, a wiele z nich (zwłaszcza w przypadku IoT) w ogóle nie ma żadnych wbudowanych funkcji bezpieczeństwa.

Co więcej, nie wszystkie z tych urządzeń są w ogóle widoczne dla zespołów odpowiedzialnych za działanie lub bezpieczeństwo sieci.

Złożoność. Większość firm podchodzi do infrastruktury w sposób reaktywny i niezintegrowany: polega to zwykle na dodawaniu nowych funkcji sieciowych i doraźnym usuwaniu luk w zabezpieczeniach poprzez dodanie nowego urządzenia. Z czasem powstają w ten sposób środowiska niezwykle złożone. Trudno jest w nich zarządzać zwłaszcza dużą liczbą izolowanych zabezpieczeń punktowych — zarówno pod względem kosztów, jak i czasu — a jednocześnie w systemie zabezpieczeń nadal pozostają luki. Cenny czas i zasoby pochłania także wdrażanie technologii w oddziałach.

Dyrektorzy odpowiedzialni za technologie sieciowe i działanie sieci potrzebują zatem rozwiązania, które może zagwarantować bezpieczeństwo, wydajność, niezawodność i dostępność w oddziale. Skuteczne podejście do bezpieczeństwa sieci musi oferować wysoką, skalowalną wydajność, jednocześnie integrując wiele funkcji sieciowych i zabezpieczeń w ramach jednego rozwiązania. Wymaga też wdrożenia architektury zabezpieczeń sieci, która umożliwi scentralizowaną kontrolę zasad i zapewni przejrzystość informacji o stanie sieci na całej powierzchni ataku.

02 Zabezpieczanie krawędzi sieci WAN

Tradycyjne sieci WAN stały się zbyt kosztowne: łącza MPLS są drogie, a zapotrzebowanie na przepustowość i natężenie ruchu stale się zwiększa (to wynik powszechności wykorzystania aplikacji SaaS).

Sieci SD-WAN mogą umożliwić oddziałom wprowadzenie transformacji cyfrowej (DX) oraz uzyskanie oszczędności i poprawę wydajności. Aby się to udało, muszą jednak oferować zarówno funkcje sieciowe, jak i zabezpieczenia — a nie jest wcale przesądzone, że zagwarantuje to odpowiednią wydajność. Skuteczne rozwiązanie SD-WAN powinno:

- łączyć różne funkcje sieciowe i związane z bezpieczeństwem w jednym rozwiązaniu;
- oferować bezobsługowe wdrażanie w sieci oddziałów, co pozwoli zminimalizować całkowity koszt posiadania (TCO);
- wykorzystywać niezawodne zabezpieczenia wbudowane w zapory sieciowe SD-WAN (bez konieczności kupowania oddzielnych urządzeń zabezpieczających i zarządzania nimi);
- optymalizować przepustowość sieci (świadomość aplikacji i obsługa wielu łączy szerokopasmowych);
- kontrolować ruch w warstwie szyfrowanej SSL/TLS bez obniżania wydajności sieci, aby zapewnić użytkownikom optymalną produktywność.



Przewiduje się, że skumulowany roczny wskaźnik wzrostu przychodów (CAGR) na globalnym rynku sieci SD-WAN wzrośnie do 2022 r. o ponad 40%, a wartość tego rynku sięgnie 4,5 mld USD¹.

03 Zabezpieczanie punktów końcowych

Bezpieczeństwo wymaga teraz także widoczności oraz możliwości kategoryzowania i zabezpieczania wszystkich podłączonych punktów końcowych — zwłaszcza „niewidocznych” urządzeń IoT, które mogą być wdrażane bez oficjalnego zatwierdzenia zespołu odpowiedzialnego za operacje sieciowe lub IT. Stworzenie ujednoliconej platformy w całej organizacji może dodatkowo zapewnić pełny wgląd w dane wszystkich podłączonych urządzeń w sieci oddziałów.

Gdy już wszystkie urządzenia w sieci są wykryte i widoczne, scentralizowane funkcje zarządzania oddziału definiowanego programowo (SD-Branch) powinny pozwalać dynamicznie zarządzać dostępem do sieci i egzekwować oparte na politykach środki kontroli, zapewniające spójny poziom bezpieczeństwa wszystkim użytkownikom, aplikacjom i punktom końcowym — w tym również podatnym na ataki urządzeniom IoT. Rozwiązanie powinno obejmować zautomatyzowaną kontrolę dostępu (np. w celu poddania kwarantannie szczególnie podatnych lub podejrzanych urządzeń), a także wykrywanie anomalii i możliwości reagowania na incydenty w celu szybkiego zapobieżenia ich skutkom, co zmniejszy obciążenie personelu odpowiedzialnego za systemy informatyczne.

Cyberprzestępcy często „celują” właśnie w urządzenia IoT działające na szczególnie podatnych na ataki brzegach sieci oddziałów. Szacuje się, że do 2020 r. 25% wszystkich ataków będzie dotyczyło urządzeń IoT².

04 Zabezpieczanie warstwy dostępowej oddziału

Integracja platform WAN i LAN może dodatkowo zwiększyć wydajność i bezpieczeństwo sieci. Aby uprościć infrastrukturę oddziału, dyrektorzy ds. sieci mogą skonsolidować jednocześnie wiele specjalizowanych urządzeń udostępniających funkcje sieciowe (jak np. routery czy systemy równoważące obciążenie), a także określone funkcje bezpieczeństwa (np. system ochrony przed włamaniami (IPS), wykrywanie zagrożeń).

Współbieżna obsługa sieci przewodowych i bezprzewodowych przez zaporę następnej generacji (NGFW) poszerza możliwości bezpiecznego rozwiązania SD-WAN o warstwę dostępową oddziału — łącząc zabezpieczenia NGFW, przełączniki, wzmacniacze i punkty dostępowe w jednym, obsługującym wiele platform i urządzeń rozwiązaniu. To zmniejsza złożoność infrastruktury, upraszczając zarządzanie oddziałami w kontekście bezpieczeństwa, dostępu do sieci i sieci SD-WAN. Pozwala też wyeliminować urządzenia wielu dostawców, wiele interfejsów i systemów operacyjnych, które mogą wymagać dużych nakładów pracy od ograniczonego liczbowo personelu, a jednocześnie usunąć luki w systemie zabezpieczeń połączeń między różnymi systemami i urządzeniami.

Skuteczne rozwiązanie powinno też pomóc w zwiększeniu sprawności (zwinności) działania dzięki skonsolidowanej konsoli do zarządzania, co zwiększa widoczność danych o stanie systemu i ułatwia kontrolę. Aby całkowity koszt posiadania (TCO) rozwiązania był jak najmniejszy, jego wdrażanie powinno się odbywać bezobsługowo.



Przeciętne przedsiębiorstwo stosuje ponad 75 różnych zabezpieczeń — wiele z nich pełni tylko jedną funkcję lub służy zachowaniu zgodności z jednym wymogiem³.

05 Kompleksowe bezpieczeństwo oddziału

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. Skuteczne wdrożenie w oddziale powinno bezproblemowo zintegrować funkcje sieciowe i zabezpieczenia we wszystkich wspomnianych wyżej obszarach: na krawędzi sieci WAN, w warstwie dostępowej i w punktach końcowych.

W ocenie rozwiązania pod kątem ogólnej optymalizacji funkcjonowania sieci w oddziale oraz poprawy bezpieczeństwa przydatne mogą być następujące pytania:

- Czy rozwiązanie skutecznie konsoliduje funkcje sieciowe i zabezpieczenia w całym oddziale?
- Czy rozwiązanie zapewnia pełną widoczność informacji o stanie systemu i umożliwia szczegółową kontrolę urządzeń i użytkowników?
- Czy rozwiązanie oferuje scentralizowaną konsolę do zarządzania z możliwością egzekwowania globalnych zasad?
- Czy wydajność, niezawodność lub wartość (TCO) rozwiązania są potwierdzone niezależnymi certyfikatami lub testami?
- Czy testowanie obejmuje ocenę wydajności w kontekście określonych potrzeb, takich jak aplikacje SaaS lub wydajność VoIP i wideo?

¹ „[SD-WAN Infrastructure Market Poised to Reach \\$4.5 Billion in 2022](#)”, IDC, 7 sierpnia 2018 r.

² „[25% Of Cyberattacks Will Target IoT In 2020](#)”, Retail TouchPoints, data uzyskania dostępu: 21 marca 2019 r.

³ Kacy Zurkus, „[Defense in depth: Stop spending, start consolidating](#)”, CSO Online, 14 marca 2016 r.



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).