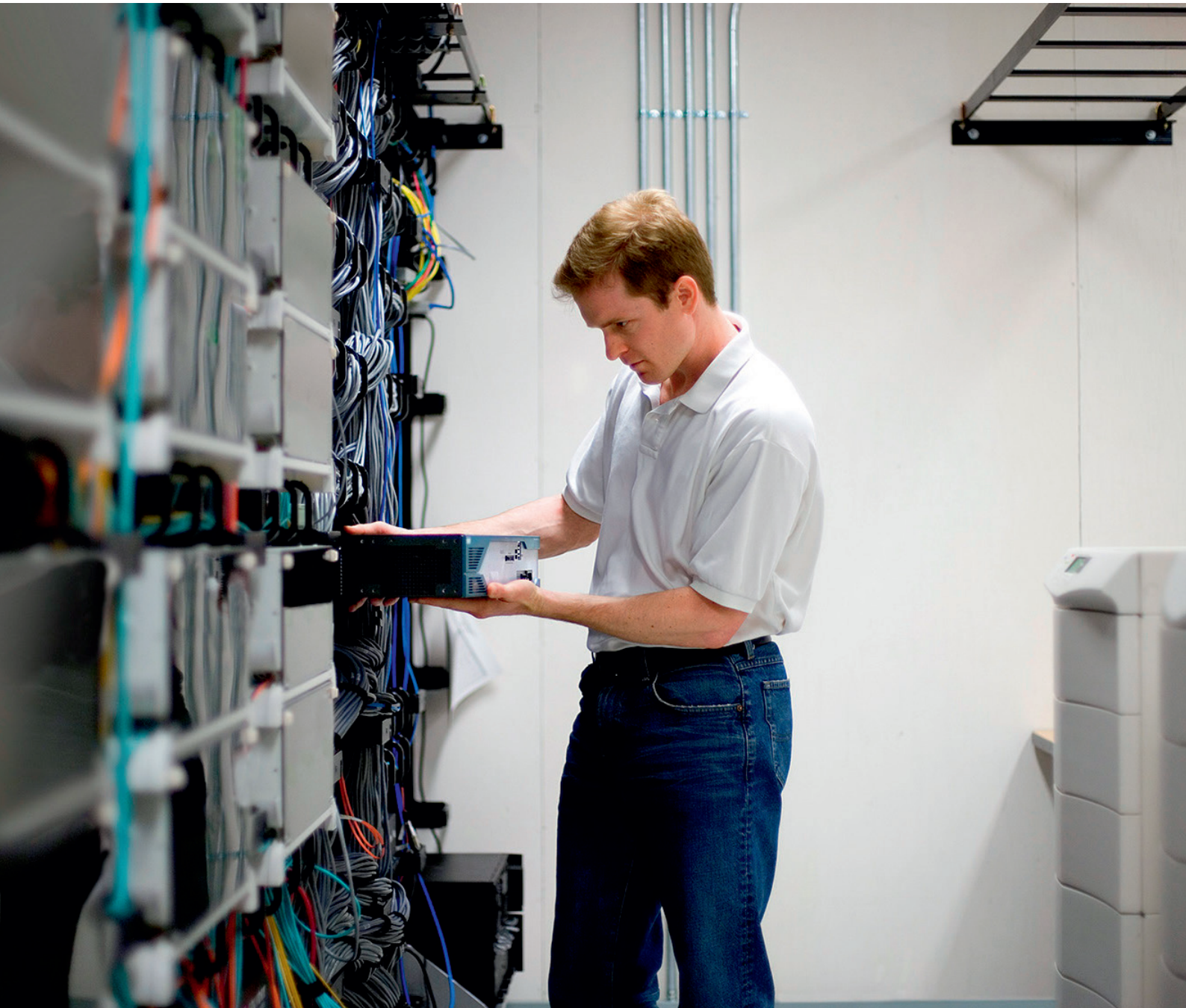
Inteligentny brzeg sieci pozwala spełniać potrzeby jutra już dziś



Konspekt

W nowej cyfrowej rzeczywistości biznesowej brzeg sieci nabiera newralgicznego znaczenia. Dotychczas niedoceniany, obecnie staje się punktem wyjścia do osiągnięcia sukcesu w procesie digitalizacji. Weźmy pod uwagę wszystko, co dzieje się na brzegu sieci:

- To pierwsza linia obrony przed podejrzaną lub złośliwą infiltracją urządzeń.
- To kanał dostarczający odbiorcom docelowym aplikacje i usługi, w które wiele zainwestowano.
- To strategiczne wrota łączące rozproszone organizacji.
- To most pomiędzy organizacją a klientami.
- To lokalizacja, gdzie podłączane i zarządzane są nowe urządzenia Internetu Rzeczy (IoT)
- To optymalne miejsce pozwalające rzeczywiście zrozumieć, co dzieje się w twojej firmie.

Brzeg sieci jest czasem wdrażany w przekonaniu, że wszystkie rozwiązania sieciowe są zasadniczo takie same. Cisco sprzeciwia się takiemu podejściu i wychodzi z założenia, że nowe cyfrowe przedsiębiorstwo potrzebuje inteligentnych rozwiązań na brzegu sieci.

Oferujemy rozwiązania i strategiczną funkcjonalność, które napędzają sukces przedsiębiorstwa. Cisco zwiększa potencjał nowego cyfrowego brzegu sieciowego, koncentrując się na następujących kwestiach:

- Obrona krytycznych zasobów na brzegu. 99,2% naruszeń bezpieczeństwa sieci firmowej może zostać zneutralizowanych jeśli sieć zostanie wykorzystana jako czujnik i narzędzie do egzekwowania zasad bezpieczeństwa. Można to zrealizować, zapewniając również głębszy wgląd w celu poprawy ochrony i szybszego reagowania.
- Zapewnianie świadomości aplikacji i urządzeń z osiem razy szybszym roamingiem i widocznością ponad 1200 aplikacji. Jest to możliwe dzięki partnerstwu strategicznemu z firmą Apple oraz innowacjom Wi-Fi.
- Szybkie przystosowywanie sieci w miarę rozwoju przedsiębiorstwa dzięki podejściu opartemu na oprogramowaniu w sieci bezprzewodowej LAN, LAN i WAN. Skutkuje to 79-procentowym obniżeniem kosztów wdrożenia dzięki zachowaniu rozdzielności między oprogramowaniem a sprzętem oraz wirtualizacji brzegu WAN.
- Platforma zaprojektowana w celu spełniania przyszłych potrzeb dzięki ustanowieniu opartej na standardach, programowalnej podstawy umożliwiającej szybkie dodanie nowej funkcjonalności, gdy jest ona potrzebna.
- Zapewnianie głębszego i szybszego wglądu w branży detalicznej i hotelarsko-gastronomicznej dzięki uzyskaniu szczegółowości danych lokalizacji na poziomie 1 metra na potrzeby podejmowania trafnych decyzji biznesowych.

Obecnie sieć ma zasadnicze znaczenie dla napędzania zmian w niemal wszystkich organizacjach w miarę jak przechodzenia przez nie procesu transformacji cyfrowej. Transformacja ta pomoże organizacjom zwiększyć elastyczność biznesową, poprawić wydajność, zacieśnić relacje z klientami, jak również chronić kluczową własność intelektualną oraz zasoby.

Brzeg sieci odgrywa zasadniczą rolę w tej transformacji i spoczywa na nim prawdopodobnie najszerszy zakres obowiązków w porównaniu z rdzeniem i siecią centrum danych. Jak pokazano na rys. 1, gdy porównamy każdą z warstw sieci, zakres obowiązków brzegu sieci w obrębie kampusu jest szeroki. Dotyczy to również oddziału.

Rys. 1. Warstwy sieci i ich funkcje

Rola brzegu sieci

Transformacja cyfrowa sprawia, że brzeg sieci jest istotny jak nigdy dotąd. Weźmy pod uwagę wszystko, co dzieje się na brzegu sieci:

- **To pierwsza linia obrony**. Brzeg jest miejscem, w którym polityka jest stosowana i weryfikowana bez ograniczania możliwości dostępu do potrzebnych elementów. Jeżeli brak jest właściwego zarządzania dostępem, przedsiębiorstwo może być narażone na infiltrację lub rozprzestrzenianie się zagrożeń, a nieodzowność kontroli dostępu wzrasta wraz z rozwojem charakteru zagrożeń. Urządzenia, oprogramowanie firmware, a nawet system operacyjny – wszystkie te elementy są słabymi ogniwami.

- **To kanał dostarczający aplikacje, w które wiele zainwestowano**. Brzeg sieci jest miejscem, w którym dokonuje się priorytetyzacja. Słabe funkcjonowanie brzegu spowoduje spowolnienie wdrażania aplikacji, co będzie skutkować zmniejszeniem zwrotu z inwestycji.

- **To strategiczna brama do łączenia rozproszonych organizacji**. Zapewnienie bezproblemowego funkcjonowania dla pracowników, partnerów i klientów, gdziekolwiek się znajdują, jest najważniejszą kwestią. Sieć gorszej jakości będzie powodować obniżenie poziomu usług świadczonych kluczowym odbiorcom.

- **To most pomiędzy organizacją a klientami**. Jeżeli przedsiębiorstwo należy do branży detalicznej lub hotelarsko-gastronomicznej, dostęp na poziomie niższym niż standardowy będzie hamował możliwość łączności z klientami na poziomie osobistym i niekorzystnie wpływał na wizerunek marki.

- **Został on stworzony w celu zasilania i obsługi rosnących wymagań urządzeń IoT**. Brzeg sieci przystosowuje się do środowiska fizycznego poprzez przenoszenie niemal wszystkich branż do epoki cyfrowej dzięki usprawnieniu operacji i obniżeniu kosztów. Bez odpowiedniej funkcjonalności na brzegu organizacje mogą pozostać w tyle pod względem redukcji kosztów i sprawności operacyjnej.

- **To optymalne miejsce pozwalające zrozumieć, co dzieje się w firmie**. W sieci rozproszonej tylko brzeg ma ogląd całości ruchu danych dzięki zbieraniu danych i analityce z brzegu. Na podstawie danych o użytkownikach, aplikacjach, urządzeniach i zagrożeniach przedsiębiorstwa mogą uzyskiwać wgląd rzeczywiście pomocny przy podejmowaniu lepszych decyzji dotyczących wsparcia pracowników, ograniczyć ryzyko i koszty oraz dostarczać informacje odbiorcom docelowym. Bez odpowiedniego poziomu konsekwentnej szczegółowości dane te stają się wypaczone i niemiarodajne

Czy standaryzacja brzegu jest zjawiskiem pozytywnym?

W przypadku całego szeregu rozwiązań brzegowych stosowane jest podejście do standaryzacji opierające się na elementach gotowych, z których budowane są brzegowe urządzenia sieciowe oraz projektowaniu podporządkowanemu standardom branżowym. Odbywa się to niejednokrotnie z myślą o ograniczeniu kosztów prac inżynieryjnych i produkcyjnych w zakresie sprzętu przez wykorzystanie już dostępnych projektów dostarczanych przez producentów elementów. Prowadzi to do standaryzacji brzegu. Podejście polegające na przedkładaniu kosztów i zarządzania nad dostarczanie kluczowych innowacji w dziedzinie rozwoju i bezpieczeństwa naraża przedsiębiorstwo na zwiększone ryzyko.

Jakie jest ryzyko?

Elementy i projekty są dostępne nie tylko dla producentów urządzeń. Mogą one również trafić do rąk osób, których zamiarem jest infiltracja sieci. Każde urządzenie podłączane do sieci jest punktem, w którym może nastąpić włamanie do sieci. Współczesne organizacje korzystając z coraz większej liczby urządzeń mobilnych i Internetu rzeczy (IoT) w coraz większym stopniu polegają na sieci, jako platformie umożliwiającej osiągnięcie sukcesu w biznesie. Organizacje muszą bardzo dokładnie przyjrzeć się rozwiązaniom w dziedzinie zabezpieczenia dostępu w każdym punkcie sieciowym – od brzegu do centrum danych.

Istnieje również ryzyko, że sieć trzeba będzie zaprojektować od nowa w przypadku zaistnienia nowej biznesowej potrzeby. Dostępne od ręki rozwiązania zostały zaprojektowane w celu spełniania wymagań dużej liczby bieżących zastosowań, ale są one ograniczone pod względem elastyczności i możliwości dostosowania. Są one również ograniczone pod względem przygotowania pod kątem nieprzewidzianego rozwoju sieci. Platforma sieciowa musi przystosowywać się do dzisiejszego szybko zmieniającego się cyfrowego świata.

Większość gotowych rozwiązań tworzonych jest pod kątem zgodności ze standardami branżowymi, które są istotne, jeżeli chodzi o zapewnienie podstawowego zestawu wymagań i funkcjonalności. Jednak standardy mogą ulec zmianie. Proces określania standardów jest często długotrwały, a wymagania producentów, projektantów aplikacji i użytkowników podlegają nieustannym i coraz szybszym zmianom. Organizacje wykorzystujące podejście oparte na standardach mogą pozostać w tyle w obliczu konieczności spełnienia zwiększonych wymagań użytkowników.

Żyjemy w czasach, w których punktem wyjściowym dla rozwiązania jest zapewnienie zgodności ze standardem, ale następnie może ono oferować możliwość rozwinięcia dodatkowej funkcjonalności, gdy zachodzi taka konieczność. Rozwiązania takie spełniają nowe wymagania cyfrowego świata, nie będąc przy tym ograniczone standardami, których poprawienie i ratyfikowanie może ciągnąć się latami.

Należy również wspomnieć o ryzyku naruszenia integralności urządzenia. Organizacje przestępcze przechwytują urządzenia w przypadku wysyłki globalnej, a następnie modyfikują elementy, np. zamieniają procesory lub integrują monitory, w celu uzyskania wrażliwych danych.

Jaki jest rzeczywisty koszt?

Często standaryzacja brzegu jest przeprowadzana w celu obniżenia kosztów prac inżynieryjnych i produkcyjnych, co pozwala na sprzedawanie niektórych rozwiązań za niższą cenę. Jednak w przypadku obliczania kosztów należy brać pod uwagę nie tylko czysty kapitał lub nawet koszt operacyjny, ale również koszt powiązany z ryzykiem. Każda organizacja jest inna, w związku z czym określenie rzeczywistych kosztów, reprezentatywnych dla wszystkich jest niemożliwe. Trzeba jednak wziąć pod uwagę następujące koszty:

- **Koszt naruszenia bezpieczeństwa**. W przypadku wielu organizacji własność intelektualna i zasoby są podstawą ich funkcjonowania. Jakie mogą być następstwa, jeżeli wpadną w niepowołane ręce? Organizacje przestępcze odznaczają się biegłością w czerpaniu zysków z cudzej własności intelektualnej i danych poprzez żądanie okupu, wymuszenia lub odsprzedaż oferującemu najwyższą cenę. Niektóre badania ujawniają przypadki odzyskiwania dokumentacji medycznej po zapłaceniu okupu w wysokości 40,00 USD za jedne akta. Gdy mamy do czynienia z tysiącami akt, szpitale mogą być zagrożone koniecznością płacenia ogromnych sum za odzyskanie swojej własności.

- **Koszt aplikacji istotnych dla działalności firmy, które nie zaadaptowały się wśród pracowników**. Wiele organizacji inwestuje poważny odsetek swojego budżetu w nowe aplikacje i systemy mające za zadanie zwiększenie wydajności. Jeżeli pracownicy mają niedobre doświadczenia z takimi aplikacjami lub usługami, nie będą chcieli z nich korzystać, a wtedy zwrot z inwestycji gwałtownie spadnie.

- **Koszt utraconych możliwości**. W ramach organizacji z branży detalicznej lub hotelarsko-gastronomicznej relacje z klientami nawiązuje się za pośrednictwem

ich urządzeń mobilnych. Jednak jeżeli klienci mają problemy z połączeniem się, wówczas organizacja traci możliwość nawiązania relacji z takim klientem i wpływania na jego pożądane zachowania.

- **Koszt braku widoczności**. Sieć brzegowa zawiera wiele informacji dotyczących użytkowników, ich urządzeń, aplikacji, z których korzystają, miejsc, które odwiedzają, a nawet informacji o obszarach, w których występują potencjalne zagrożenia. Bez tej widoczności organizacja może spędzić niezliczone godziny, próbując zrozumieć, w jaki sposób użytkownicy wchodzą w interakcje ze swoim otoczeniem, jak uzyskują dostęp do informacji i jak je konsumują, a nawet przeoczyć potencjalne zagrożenie, które można było zminimalizować odpowiednio wcześnie.

Cisco zapewnia inteligencję na brzegu

Cisco stosuje inne podejście niż standaryzacja brzegu. Inwestujemy duże kwoty w opracowywanie innowacji, które mają za zadanie pomóc organizacjom wkroczyć w epokę cyfrową. Koncentrujemy się na obronie krytycznych zasobów w celu wspierania zwiększenia świadomości w dziedzinie aplikacji i urządzeń oraz zapewnienia głębszego i szybszego wglądu. Cisco pomaga przystosować się do zmian związanych z rozwojem przedsiębiorstwa oraz przygotować się na wyzwania, które niesie przyszłość. Robimy to, tworząc jedyną w swoim rodzaju funkcjonalność od podstaw lub udoskonalając funkcjonalność już sprawdzonych elementów. Cisco zapewnia funkcjonalność pozwalającą sprostać wymaganiom brzegu sieci dziś i w przyszłości.

Ochrona krytycznych zasobów na brzegu

Brzeg sieci to pierwszy punkt nieuprawnionego lub wrogiego dostępu, ponieważ to właśnie tu odbywa się wprowadzanie do infrastruktury użytkowników i urządzeń. Potrzebne jest zaufanie, że jest on w stanie zidentyfikować i kontrolować wszystko, co przedostaje się do sieci.

Przyjęcie założenia, że standaryzacja bezpieczeństwa brzegu jest skuteczna sugeruje, że gotowe rozwiązania w dziedzinie bezpieczeństwa spełniają swoje zadanie. Jeżeli tak jest w istocie, to dlaczego kradzież informacji, wymuszenia i żądania okupu są szybko rozwijającą się branżą, której wartość sięga już 1 bln USD?

Aktualnie stosowane podejścia do bezpieczeństwa brzegu są nieskuteczne. Cisco jest liderem rynku innowacyjnych technologii umożliwiających rozpoznawanie osób i rzeczy oraz ich stanu przed umożliwieniem im dostępu do sieci i zezwoleniem na przemieszczanie się w jej obrębie.

Oto kilka innowacji Cisco® w dziedzinie bezpieczeństwa brzegu dla klientów Cisco oraz sposób ich wykorzystania:

- **Tożsamość oraz stan urządzenia i użytkownika**. Urządzenia brzegowe Cisco są zintegrowane z najbardziej kompleksowymi technologiami sond profilu punktu końcowego. Ponadto Cisco AnyConnect® Security Agent przeprowadza kontrolę stanu zgodności postawy i polityki przed umożliwieniem dostępu do sieci produkcyjnej. Najbardziej precyzyjna tożsamość punktu końcowego nie dopuszcza nieuprawnionych, zainfekowanych złośliwym oprogramowaniem urządzeń do sieci do momentu potwierdzenia, że są one bezpieczne i uprawnione.

- **Prawa dostępu zmieniające się w zależności od poziomu zagrożenia**. Dzięki integracji z Cisco Identity Services Engine prawa dostępu użytkowników i urządzeń można zmieniać automatycznie, stosownie do zmian ich poziomu zagrożenia STIX lub poziomu narażenia CVSS. STIX i CVSS są powszechnie wykorzystywanymi wyrażeniami do opisywania istotności zagrożeń bezpieczeństwa i podatności na zagrożenia.

- **Integracja segmentacji oparta na oprogramowaniu**. Tworzenie i zarządzanie segmentacją przy użyciu wirtualnych sieci LAN oraz list kontroli dostępu (ACL) jest zazwyczaj trudne, a jest jeszcze trudniejsze, gdy segmentacja staje się kluczowa dla zabezpieczenia operacji IoT. Urządzenia brzegowe Cisco są dostarczane z wbudowaną segmentacją opartą na oprogramowaniu Cisco TrustSec® w systemie operacyjnym oraz ASIC w celu zapewnienia łatwej, wysokowydajnej identyfikacji i segmentacji od punktu dostępowego do aplikacji w centrum danych.

- **Network as an Enforcer** (sieć jako narzędzie do egzekwowania zasad bezpieczeństwa). Jest to oparta na oprogramowaniu segmentacja wbudowana w urządzeniach brzegowych, umożliwiająca natychmiastowe i konsekwentne egzekwowanie polityki bezpieczeństwa w celu kontroli dostępu i ograniczenia zagrożeń. Dzięki integracji z Identity Services Engine technologie Cisco Stealthwatch oraz Cisco Security Technology Associate są w stanie wywołać politykę w celu ograniczenia zagrożenia.

- **Network as a Sensor** (sieć jako czujnik). Zaawansowana kompleksowa widoczność dzięki NetFlow oraz interpretacja przy użyciu Cisco Stealthwatch. Ponieważ wszystkie urządzenia brzegowe Cisco są wyposażone w Flexible NetFlow, możliwa jest kompleksowa widoczność przepływu w celu

wykrywania nietypowych zachowań. Standardowe technologie nie umożliwiają wykrywania zachowań obrazujących aktywność użytkowników po uzyskaniu dostępu do sieci oraz ich aktywności w Internecie.

- **Integracja Stealthwatch Learning Network**. Innowacja ta może umożliwiać wszystkim urządzeniom w oddziałach współużytkowanie danych o zachowaniu i zwiększenie wiedzy na temat zachowań dozwolonych, dzięki czemu możliwe jest funkcjonowanie szybsze, łatwiejsze i bardziej skalowalne.

- **Egzekwowanie szybkiej polityki obronnej**. Oznacza to możliwość wcześniejszego ustawienia polityk w celu reagowania na zdarzenia katastrofalne, np. szybko rozprzestrzeniające się złośliwe oprogramowanie typu zero-day lub ataki hakerskie. Dzięki naciśnięciu jednego przycisku można przywołać zmiany polityki dostępu dla każdego urządzenia w sieci w celu ograniczenia lub zatrzymania całej komunikacji aż do momentu wyeliminowania zagrożenia.

- **Tożsamość punktu końcowego IoT i automatyczna segmentacja**. Sondy w urządzeniach brzegowych Cisco pomagają zidentyfikować największy obecnie zbiór urządzeń medycznych IoT, a technologia ta rozwija się, obejmując wiele innych branż. Dzięki integracji z zaawansowanymi technologiami, takimi jak Identity Services Engine, sieciowe urządzenia brzegowe będą mogły lepiej identyfikować i automatycznie segmentować najbardziej zaciemnione punkty końcowe oraz automatycznie dodawać je w dyskretnych segmentach sieci w celu ich ochrony przed atakiem. W związku z tym gdy pracownik podłącza urządzenie do sieci, zostaje ono zidentyfikowane, zaklasyfikowane i umieszczone w odpowiednim i zabezpieczonym segmencie sieci.

- **Szybkie eliminowanie zagrożeń**. Urządzenia brzegowe Cisco integrują się z Identity Services Engine oraz TrustSec. Gdy Cisco lub partner w dziedzinie integracji technologii wykryje atak, można umieścić stanowiący zagrożenie punkt końcowy w segmencie sieci za pomocą polecenia IT lub automatycznie. Zagrożenia są wykrywane szybciej, a reakcja mająca na celu ich ograniczenie jest natychmiastowa.

- **Wykrywanie złośliwego oprogramowania w ruchu szyfrowanym**. Ponieważ hakerzy znajdują coraz trudniejsze do wykrycia sposoby na uzyskanie dostępu do sieci, Cisco wykorzystuje swoją możliwość badania ram sieci w celu identyfikacji złośliwego oprogramowania nawet w ruchu szyfrowanym.

- **Ochrona chmury oraz ochrona przed złośliwym oprogramowaniem i ransomware**. Integracja z Cisco Umbrella for Branch czyni z urządzeń brzegowych Cisco krytyczny element rozwiązania Cisco Ransomware. Umbrella uniemożliwia pracownikom dostęp do stron internetowych, które są podejrzane, zagrożone lub zawierają złośliwe oprogramowanie. Uniemożliwia również botom złośliwego oprogramowania i ransomware, dotarcie do ich jednostki macierzystej, co jest standardowo wymagane do funkcjonowania.

- Ochrona pracowników mobilnych. Pracownicy mobilni są prawdopodobnie najbardziej podatnym „punktem" przez który przenika złośliwe oprogramowanie, ponieważ często mają oni swobodny dostęp do Internetu, gdy znajdują się w zdalnej lokalizacji. Cisco AnyConnect Security Agent z VPN może zostać wzbogacony o Cisco Advanced Malware Protection i Cisco Umbrella for Mobility w celu utrzymania bezpieczeństwa poza siecią. Umożliwia również podłączenie do wielu urządzeń brzegowych Cisco za pośrednictwem VPN. Żadne z tych rozwiązań bezpieczeństwa wykorzystujących pojedynczego agenta nie będzie działać w standaryzowanym środowisku.

- Integralność urządzeń sieciowych. Hakerzy dysponują szerszym wachlarzem sposobów infiltracji i naruszania bezpieczeństwa systemów niż same tylko punkty podatne na włamania w aplikacjach i systemach operacyjnych. Atakują oni stos sprzętu lub oprogramowania urządzeń sieciowych, w związku z czym zabezpieczenie urządzenia sieciowego ma krytyczne znaczenie dla bezpieczeństwa. Podobnie jak ma to miejsce w przypadku systemów operacyjnych i aplikacji, słabe punkty urządzeń sieciowych będą z pewnością nadal wykrywane. Cisco stosuje rygorystyczne zasady w odniesieniu do opracowania oprogramowania i sprzętu, włącznie z testami regresyjnymi w celu zapewnienia klientom Cisco możliwości kontynuacji utrzymania godnej zaufania sieci.

Dokładniejsze dane i szybszy wgląd

Brzeg Cisco spełnia rolę źródła wiedzy na temat tego, co rzeczywiście dzieje się w firmie, z wglądem obejmującym użytkowników, urządzenia, których używają oraz aplikacje, do których uzyskują dostęp. Ma on możliwość zrozumienia i uczenia się od urządzeń w sieci w celu automatycznego przystosowywania się do zmian i potrzeb. Zapewnia dane w oparciu o lokalizacje w celu lepszego zrozumienia interakcji użytkowników z otoczeniem dla potrzeb podejmowania lepszych decyzji biznesowych, a także zapewnia funkcje śledzenia zagrożeń w celu zrozumienia sposobów infiltracji przedsiębiorstwa.

Dzięki Cisco IOx Fog Computing brzeg jest w stanie wybrać optymalną lokalizację, w siedzibie firmy lub w chmurze, dla potrzeb przetwarzania tych danych, co umożliwia organizacji poprawę wydajności i obniżenie kosztów. Analityka lokalizacji w Cisco Connected Mobile Experiences (CMX) oferuje szczegółową analitykę lokalizacji opartą na Wi-Fi i Bluetooth Low Energy (BLE) w celu zapewnienia realistycznego oglądu sposobu interakcji osób ze środowiskiem.

Organizacje typu B2C z branż takich jak sprzedaż detaliczna, hotelarstwo i gastronomia czy edukacja są w stanie uzyskać dokładność lokalizacji na poziomie poniżej 1 metra dzięki Wi-Fi + BLE i napędzać bezpośrednie zwiększenie dochodów. Przykłady zastosowań to 20-procentowe zwiększenie dochodów niezwiązanych z wynajmem pokoi w Hyatt Regency, trzykrotne zwiększenie czasu przebywania klientów oraz 80-procentowe zwiększenie zadowolenia odwiedzających centrum handlowe Stary Browar – a wszystko to przy jednoczesnym zapewnieniu spersonalizowanych usług mobilnych.

Dodatkowo Cisco Prime™ zapewnia kompleksową widoczność użytkowników końcowych, ich urządzeń oraz aplikacji, z których korzystają w sieci. Umożliwia to lepsze planowanie sieci, pomiar wdrażanych aplikacji oraz obniżenie kosztów.

Przystosowanie w miarę rozwoju przedsiębiorstwa dzięki automatyzacji

Gdy trzeba zarządzać większą liczbą użytkowników, urządzeń i lokalizacji, coraz bardziej niezbędna staje się automatyzacja procesów i nowych usług z funkcjonalnością dnia zerowego i dnia pierwszego. W przewodowej i bezprzewodowej przestrzeni dostępu struktura kampusu i centrum danych z rozłączoną nakładką oprogramowania pracującą na zindywidualizowanych układach ASIC (Application Specific Integrated Circuit) umożliwia:

- zwiększenie skali,
- pewność usług,
- bezpieczeństwo,
- inne usługi dla urządzeń fizycznych i wirtualnych, aplikacji oraz użytkowników.

Wirtualizacja sieci może umożliwić zarządzanie siecią i polityką według typu użytkownika w celu szybkiego uruchamiania i dostosowywania aplikacji oraz szybszego ograniczania zagrożeń. Jest to scentralizowane podejście mające na celu bezpieczne wdrożenie nowych lokalizacji w czasie kilku minut zamiast dni w przypadku dowolnego rodzaju połączenia.

Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) zapewnia centralnie kontrolowaną funkcjonalność Plug and Play (PnP) i łatwą jakość usług (QoS) dla potrzeb bezdotykowego wdrożenia na brzegu. Umożliwia również dynamiczną priorytetyzację krytycznych aplikacji.

Oprogramowanie dostarczane przez Cisco zapewnia elastyczność dostosowaną do potrzeb. Przy użyciu ściśle zintegrowanych platform oprogramowania i sprzętu jesteśmy w stanie zapewnić znaczące korzyści dla organizacji, które uwidocznią się w WAN i brzegu dostępowym. Elementy dostosowane do WAN obejmują szybki układ ASIC, a oprogramowanie do zarządzania chmurą sprawia, że Cisco Enterprise Network Functions Virtualization (Enterprise NFV) staje się rzeczywistością, w której można włączać usługi sieciowe w czasie kilku minut zamiast miesięcy. Enterprise NFV zapewnia funkcjonalności w zakresie mocy obliczeniowej, pamięci masowej, infrastruktury sieciowej, zarządzania oraz pewności świadczonych usług sieciowych, dzięki czemu można zredukować złożoność w obrębie oddziału i umożliwić nowe usługi na żądanie na brzegu.

Organizacje osiągnęły 79-procentowe obniżenie kosztów wdrożenia dzięki APIC-EM PnP oraz o 85% szybsze przydzielanie zasobów dzięki aplikacjom APIC-EM Intelligent WAN.

Przy dużej liczbie użytkowników i urządzeń łączących się z wszystkich rodzajów lokalizacji brzeg sieci może mieścić się w dużych kampusach lub małych lokalizacjach zdalnych. Globalne widoki topologii z automatycznymi funkcjonalnościami PnP znacząco obniżają koszt wprowadzenia do infrastruktury lub modernizacji urządzenia sieciowego, takiego jak przełącznik, router lub punkt dostępowy. Dodatkowe aplikacje w kontrolerze umożliwiają przydzielanie zasobów QoS w obrębie całej sieci, szybko zabezpieczając ruch istotny dla działalności firmy przed klientami pasma niekrytycznego. Specjalistyczne aplikacje, jak np. Intelligent WAN (IWAN), umożliwiają przydzielanie zasobów, monitorowanie i rozwiązywanie problemów w zakresie bezpieczeństwa, szyfrowania, wyboru ścieżki oraz widoczności i kontroli aplikacji w obrębie sieci WAN.

Dodatkowo oprogramowanie Cisco ONE™ oferuje cenny i elastyczny sposób na zakup oprogramowania dla brzegu. Na każdym etapie cyklu życia produktu Cisco ONE ułatwia zakup, zarządzanie i modernizację sieci.

Wraz z rozwojem inwestycji, dzięki ciągłym innowacjom, aktualizacjom i modernizacjom w zakresie urządzeń fizycznych i wirtualnych zapewniony jest wysoki poziom zwrotu z inwestycji.

Świadomość aplikacji i urządzeń

Cisco jest jedynym dostawcą, który nawiązał partnerstwo z liderem branży urządzeń mobilnych, firmą Apple, w celu zapewnienia wyższej jakości usług mobilnych. To partnerstwo strategiczne dla obu spółek pozwala wykorzystać inteligentne rozwiązania dla sieci w celu zapewnienia jak najlepszych usług Wi-Fi dzięki optymalnemu roamingowi. Innymi słowy, nasza współpraca zapewnia przyspieszenie aplikacjom istotnym dla działalności firmy w urządzeniach Apple iOS w miejscu pracy w celu zwiększenia wydajności pracowników.

Przedsiębiorstwa mogą oczekiwać nawet ośmiokrotnie szybszego roamingu, zwiększenia niezawodności połączeń Wi-Fi o 66% oraz obniżenia kosztów zarządzania siecią o 50% dzięki mniejszej liczbie SSID, a użytkownicy końcowi mogą wydłużyć trwałość baterii urządzenia iOS o 30%.

Od wielu lat Cisco dostarcza innowacje Wi-Fi wykraczające poza aktualne standardy i stanowiące punkt odniesienia dla kolejnych standardów. Technologia bezprzewodowa Cisco Aironet® zapewnia innowacje usprawniające częstotliwości radiowe, wydajność urządzenia oraz funkcjonowanie aplikacji. Cisco jest również pionierem w dziedzinie technologii Flexible Radio Assignment, optymalizującej wydajność sieci Wi-Fi bez ograniczenia dostępności częstotliwości radiowych. Umożliwia to bezprzewodowym punktom dostępowym identyfikowanie nagłych potrzeb w zakresie przepustowości bezprzewodowej i automatyczne przystosowywanie sieci bezprzewodowej w celu spełnienia tych potrzeb. Ma to krytyczne znaczenie w obszarach, w których gromadzi się duża liczba użytkowników rywalizujących o przepustowość bezprzewodową.

Podstawa funkcjonowania cyfrowego przedsiębiorstwa są aplikacje wykorzystywane do zwiększenia wydajności oraz do nawiązywania relacji z klientami. Cisco oferuje rozwiązanie Application Visibility and Control wykrywające aplikacje na brzegu sieci przewodowej i bezprzewodowej. Wykorzystujemy inteligentną kontrolę ścieżki w celu wyboru najlepszej ścieżki w sieci WAN przy jednoczesnej optymalizacji dostarczania za pośrednictwem przewodowej lub bezprzewodowej sieci LAN, aby zapewnić użytkownikom jak najlepsze funkcjonowanie aplikacji.

Organizacje mogą uzyskać pogłębiony wgląd w ponad 1200 aplikacji oraz priorytetyzować aplikacje istotne dla działalności firmy za pomocą jednego kliknięcia, dzięki APIC-EM i Cisco Prime Infrastructure.

Brzeg ma możliwość kontrolowania i poprawy jakości funkcjonowania pracowników w przestrzeni fizycznej. Cisco Digital Ceiling rozszerza korzyści zapewniane przez IoT dzięki konwergencji sieci w budynkach, w tym:

- oświetlenia,
- ogrzewania i chłodzenia,
- wideo IP,
- czujników IoT
- i wielu innych za pośrednictwem bezpiecznej i inteligentnej platformy sieciowej.

Digital Ceiling odblokowuje nowe możliwości pozwalając zwiększyć i wydajności pracowników i obniżyć koszty operacyjne związane z obsługą obiektów.

Przygotowanie na przyszłość

Brzeg Cisco, zaprojektowany z myślą o przyszłości, bez systemu operacyjnego Cisco IOS-XE o programowalności opartej na standardach i modelach, przygotowuje sieć do dodawania funkcjonalności i przystosowania do zmian w środowisku, przedsiębiorstwie lub branży. Dzięki temu brzeg sieci jest otwarty, programowalny i rozszerzalny.

Brzeg ewoluuje od modelu, w którym segmentacja i kontrola dostępu są dodawane do konfiguracji sieci, do w pełni zautomatyzowanego w zakresie polityki rozwiązania. W przyszłości sieci nie będą musiały mieć bezpośrednio przydzielanych zasobów. Co więcej, będzie można określić, którzy użytkownicy lub grupy mają dostęp do określonych uprzywilejowanych grup aplikacji lub danych, w siedzibie firmy lub w chmurze. Sieć będzie miała automatycznie przydzielane zasoby w celu wprowadzenia tej polityki w życie przy jednoczesnym umożliwieniu dużej elastyczności na potrzeby monitorowania, rozwiązywania problemów, naprawiania błędów lub stosowania dodatkowych usług do określonego ruchu.

Brzeg staje się również w pełni programowalny. Rozwiązania koordynacyjne mogą łączyć się z brzegiem za pomocą API opartych na modelach, skryptów Python lub innych narzędzi stylów Linux. Upraszcza to integrację brzegu z nowoczesnymi metodami opracowania oprogramowania, zapewniając elastyczność i dostosowanie na niespotykana dotąd skalę.

Ciągła innowacja na brzegu sieci

W obliczu spodziewanego ogromnego wzrostu liczby sieciowych połączeń i związanego z tym potencjału możliwości, spółki zaczynają dostrzegać, że ta transformacja będzie wymagała fundamentalnych zmian w ich infrastrukturze sieciowej oferujących możliwości zarządzania danymi i ich analizowania. Cisco wyznacza kierunek tej transformacji, napędzając innowacje w infrastrukturze sieci, zarządzaniu infrastrukturą i analityce w celu przekształcania danych w użyteczną wiedzę.

Celem Cisco jest zmiana w podejściu do rozwiązywania problemów z reaktywnego na proaktywne, oraz skrócenie czasu rozwiązywania problemów z dni do minut. Osiągniemy to, traktując każde urządzenie w sieci jak czujnik i element rozproszonego przetwarzania danych. Zbieranie danych z urządzeń na brzegu oraz rozproszenie przetwarzania bliżej źródła danych umożliwia realizację analityki z prędkością liniową w celu generowania użytecznego wglądu dzięki uczeniu się maszyn.

Dzięki największej zainstalowanej bazie i własnym rozwiązaniom ASIC Cisco umożliwiamy projektowanie sprzętu i oprogramowania zoptymalizowanego pod kątem analityki. Wystarczy wykorzystać moc zainstalowanej bazy. Połączenie rozwiązań przewodowych i bezprzewodowych w obrębie jednej sieci będzie oznaczać, że wiedza na brzegu może być pomocna w rozwiązywaniu problemów, występujących na brzegu lub w innym miejscu, w ciągu kilku sekund. A z czasem umożliwi nawet korygowanie potencjalnych problemów jeszcze zanim wystąpią. Pomoże to działom IT świadczyć usługi sieciowe na poziomie zagwarantowanym w umowie (SLA) oraz zapewnić wydajność aplikacji w przyszłości.

Wnioski

Kiedy tak wiele zależy od brzegu sieci, standaryzacja przewodowej i bezprzewodowej sieci LAN i WAN generuje ryzyko, które może skutkować naruszeniami bezpieczeństwa, utratą produktywności i dochodów, utratą możliwości oraz nikłym wglądem. Brzeg sieci Cisco umożliwia organizacjom uzyskanie czegoś więcej niż dostępne od ręki, podporządkowane standardom podejście, zapewniając wartościową wiedzę na brzegu sieci.

Podejście to umożliwia organizacji:

- ochronę działalności z pomocą mocnej pierwszej linii obrony,
- pewne dostarczanie aplikacji odbiorcom docelowym,
- zapewnianie bezproblemowego działania pracownikom w dowolnej lokalizacji,
- nawiązywanie relacji z klientami w celu pozyskania nowych źródeł dochodów,
- lepsze zarządzanie urządzeniami IoT i optymalizację środowiska fizycznego,
- zapewnienie optymalnego widoku tego, co rzeczywiście dzieje się w firmie.

Więcej informacji

Więcej informacji można znaleźć na naszej stronie Cisco Unified Access Technology pod adresem http://www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html.

C11-737691-00 08/16