Extreme Networks Fabric – od rozproszonej sieci do zautomatyzowanej architektury

Rozproszenie infrastruktury IT osiągnęło punkt, w którym tradycyjne modele zarządzania siecią przestały być skalowalne. Architektura Fabric proponuje zmianę podejścia: automatyzację, centralną propagację polityk i natywną odporność – zaprojektowane pod realia wielovendorowych środowisk produkcyjnych.

Sieć jako terra incognita – dlaczego rozproszone środowiska IT wymykają się kontroli

Rozproszona infrastruktura sieciowa – obejmująca punkty dostępowe, data center, chmurę i stanowiska zdalne – coraz częściej przekracza możliwości tradycyjnych modeli zarządzania. Problem nie jest nowy, ale jego skala rośnie szybciej niż zdolność organizacji do adaptacji. Wyniki badań prowadzonych wśród polskich przedsiębiorstw potwierdzają, że wyzwanie dotyczy nie tylko technologii, lecz także modelu operacyjnego.

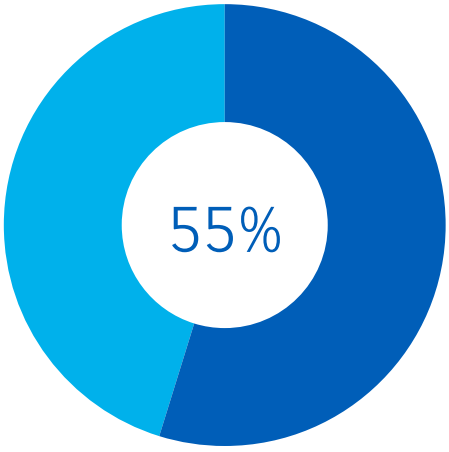
W realiach wielooddziałowej organizacji z hybrydowym modelem pracy sieć stała się strukturą, której nikt nie widzi w całości. Brak aktualnej inwentaryzacji, niekompletna dokumentacja i ograniczona telemetria powodują, że decyzje dotyczące konfiguracji, segmentacji czy polityk bezpieczeństwa podejmowane są na podstawie fragmentarycznych danych. Zamiast zarządzania opartego na procesach i powtarzalnych procedurach, dominuje tryb ad hoc – reaktywny, nieskalowalny i podatny na błędy. To niekoniecznie kwestia kompetencji zespołów, lecz konsekwencja narastającego długu w kontekście architektury, który z każdym kwartałem staje się trudniejszy do spłacenia.

Przeciążone IT i rosnące ryzyko

Działy IT operują pod stałą presją bieżących zgłoszeń, jednocześnie odpowiadając za utrzymanie ciągłości działania, wdrażanie nowych usług i egzekwowanie polityk bezpieczeństwa. Przy braku pełnej widoczności – od end-pointów i edge'a po zasoby chmurowe – efektywność operacyjna spada. Zespoły nie nadążają za oczekiwaniami biznesu, pracują reaktywnie i nie są w stanie holistycznie adresować kluczowych obszarów: bezpieczeństwa, wydajności i zgodności regulacyjnej. Efekt? Luki, które stają się widoczne dopiero w momencie incydentu, kiedy koszt naprawy jest już wielokrotnie wyższy niż koszt prewencji.

Rozproszenie zasobów, lokalizacji i pracowników postępuje, ale rzadko towarzyszy mu wdrożenie platformy zarządzania siecią zaprojektowanej „by design" do obsługi środowisk wielovendorowych.

Większość organizacji operuje na zestawie narzędzi pochodzących od różnych dostawców, które nie tworzą spójnego modelu operacyjnego. Brak centralnego punktu kontroli i korelacji zdarzeń uniemożliwia zarówno proaktywne zarządzanie, jak i szybką reakcję na zagrożenia. W efekcie diagnostyka incydentu wymaga żmudnego przeszukiwania wielu konsol i logów zamiast jednego, spójnego widoku.



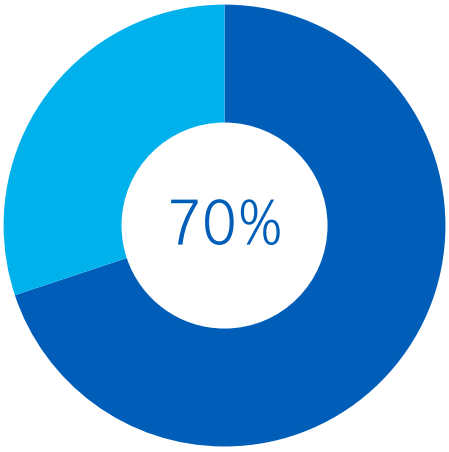
55% uczestników badania zwróciło uwagę na brak jednolitego systemu do zarządzania różnymi typami i lokalizacjami sieci

* źródło: Badanie Axians i Extreme Networks „Zarządzanie sieciami komputerowymi z chmury"

Integracja: cel, nie punkt wyjścia

Na rynku nie brakuje rozwiązań deklarujących natywną integrację z istniejącymi środowiskami. Argumenty – szybkie wdrożenie, mniej przestojów, niższe koszty – brzmią przekonująco na etapie presales. W praktyce każda kolejna warstwa „łatwo integrowalnego" narzędzia zwiększa złożoność stosu technologicznego i generuje dodatkowy narzut operacyjny.

Rzeczywista interoperacyjność wymaga standaryzacji API, ujednolicenia modeli danych i spójnej polityki zarządzania – a to wymaga strategicznego podejścia, nie zaś kolejnego zakupu. Zdolność do efektywnej integracji pozostaje celem, do którego większość organizacji dopiero zmierza.



Ponad 70% zespołów IT w dużych organizacjach deklaruje brak pełnej widoczności infrastruktury sieciowej. Główne przyczyny to wielovendorowość, rozproszona architektura i brak centralnej platformy zarządzania, która umożliwiałaby korelację zdarzeń w czasie rzeczywistym w jednym panelu.

* źródło: Badanie Axians i Extreme Networks „Zarządzanie sieciami komputerowymi z chmury"

Jacek Mądry
Network and Security Solutions Engineer w Axians

Brak pełnej widoczności rozproszonej infrastruktury to również jedno z najczęstszych wyzwań, z jakimi mierzę się na etapie przygotowania do wdrożeń. Teoretycznie wiedza ta powinna być zawarta w dokumentacji, jednak w praktyce schematy sieci często nie nadążają za rzeczywistością, stając się nieaktualne tuż po ich powstaniu. W dynamicznym środowisku IT, gdzie stale dołączane są nowe narzędzia i zasoby, sieć musi być traktowana jako struktura, która żyje. Dlatego systemy zarządzania, które w czasie rzeczywistym prezentują pełną topologię i wszystkie podłączone urządzenia, są dziś fundamentem, który powinna posiadać każda nowoczesna organizacja.

Extreme Networks Fabric. Architektura, która skaluje się razem z organizacją

W środowiskach, gdzie liczba podłączanych urządzeń i usług rośnie szybciej niż zdolność IT do ich obsługi, tradycyjna architektura sieciowa staje się wąskim gardłem. Extreme Networks Fabric to propozycja fundamentalnej zmiany reguł gry – przejścia od manualnego zarządzania topologią do modelu opartego na automatyzacji, centralnym definiowaniu polityk i natywnej skalowalności.

Dla zespołów sieciowych ważnym testem jakości architektury jest jej zachowanie w warunkach, których nie da się zaplanować: gwałtowny wzrost ruchu, podłączenie nowego oddziału, migracja usług między centrami danych czy nagłe rozszerzenie puli end-pointów wynikające z wdrożeń IoT. Tradycyjne podejście – oparte na statycznych VLAN-ach, ręcznej konfiguracji przełączników i segmentacji zależnej od fizycznej topologii – w takich scenariuszach generuje opóźnienia, błędy konfiguracyjne i ryzyko niedostępności usług. Fabric eliminuje te ograniczenia poprzez abstrakcję warstwy sieciowej. Oznacza to, że polityki są definiowane centralnie i propagowane automatycznie na całą infrastrukturę, niezależnie od lokalizacji fizycznej urządzenia czy jego producenta.

Skalowanie bez proporcjonalnego wzrostu złożoności

Jednym z najczęstszych źródeł problemów między IT a biznesem jest rozbieżność między tempem skalowania działalności a szybkością reakcji infrastruktury. Otwarcie nowej lokalizacji, uruchomienie dodatkowej linii produkcyjnej czy wdrożenie systemu IoT wymaga od sieci natychmiastowej gotowości – zarówno pod kątem przepustowości, jak i egzekwowania polityk dostępu.

W modelu klasycznym każda taka zmiana oznacza godziny pracy inżyniera i ryzyko niezgodności z resztą środowiska. Architektura Fabric zmienia tę dynamikę i pozwala na dodawanie nowych węzłów bez rekonfiguracji istniejącej infrastruktury.

Nowy przełącznik włączony do fabrica automatycznie dziedziczy polityki, segmentację i reguły bezpieczeństwa, eliminując konieczność ręcznego provisioningu. Czas wdrożenia nowego punktu sieciowego mierzony jest w minutach, nie zaś dniach roboczych.

Compliance a rzeczywistość operacyjna

Rosnące wymagania regulacyjne – od NIS2 przez DORA po branżowe standardy typu ISO 27001 – wymuszają na organizacjach ciągłą weryfikację polityk bezpieczeństwa i zdolność udowodnienia zgodności w dowolnym momencie. W środowiskach zarządzanych manualnie audyt zgodności to proces żmudny, czasochłonny i obarczony ryzykiem przeoczeń.

Fabric, dzięki centralnemu modelowi polityk i automatycznej propagacji reguł, zapewnia spójność konfiguracji w całej infrastrukturze. Każda zmiana polityki jest aplikowana globalnie, z pełną audytowalnością i możliwością weryfikacji stanu zgodności w czasie rzeczywistym. To nie eliminuje złożoności compliance, ale przenosi ją z poziomu manualnych checklist na poziom zautomatyzowanego, powtarzalnego egzekwowania polityk w całym środowisku produkcyjnym.

Piotr Szołkowski
Network and Security Solutions Architect w Extreme Networks

W rozmowach z klientami najczęściej powracające stwierdzenie: „dział IT nie ma czasu" nie dotyczy wyłącznie braku zasobów na nowe wdrożenia. To przede wszystkim efekt nieustannej, reaktywnej walki o nadążenie za dynamiką biznesu. Działy IT operują dziś pod stałą presją – próbując jednocześnie utrzymać ciągłość działania i wdrażać nowe usługi w realiach ograniczonych zasobów kadrowych. Gdy technologia staje się bardziej złożona niż zdolność zespołu do jej obsługi, organizacja nieuchronnie traci kontrolę nad infrastrukturą. Architektura Fabric pozwala przerwać ten cykl – umożliwiając skalowanie sieci bez proporcjonalnego wzrostu nakładów pracy.

Architektura Fabric

Architektura Fabric opiera się na zasadzie automatycznej propagacji polityk – nowe urządzenia włączone do sieci dziedziczą segmentację i reguły bezpieczeństwa bez ręcznej konfiguracji. Czas provisioningu nowego węzła skraca się z dni do minut, a spójność polityk jest gwarantowana niezależnie od skali środowiska.

Cechy Fabric, które zmieniają ekonomikę brzegu sieci

Architektura Fabric nie jest kolejną iteracją klasycznego podejścia do zarządzania siecią – to zmiana modelu operacyjnego. Każda z jej cech przekłada się bezpośrednio na przewagę konkurencyjną organizacji, szczególnie tam, gdzie rozgrywają się najważniejsze procesy biznesowe, czyli na brzegu sieci.

Automatyzacja jako fundament skalowalności

Tam, gdzie liczba urządzeń końcowych rośnie w tempie dziesiątek procent rocznie, ręczne zarządzanie konfiguracją przestaje być realistyczne. Fabric przenosi logikę konfiguracyjną na poziom polityk propagowanych automatycznie – od rdzenia po edge. Dla biznesu oznacza to skrócenie czasu uruchomienia nowej lokalizacji lub usługi z tygodni do godzin, bez angażowania dodatkowych zasobów inżynierskich. To również mniejsze ryzyko błędów wynikających z ręcznej konfiguracji – jednego z najczęstszych źródeł incydentów sieciowych.

Architektura Fabric zapewnia wielościeżkową komunikację z równoważeniem obciążenia na poziomie całej topologii, eliminując wąskie gardła typowe dla drzewiastych modeli przełączania. Każde nowe urządzenie podłączone do fabrica jest rozpoznawane i provisionowane automatycznie, dziedzicząc pełen zestaw polityk segmentacji i bezpieczeństwa. Na brzegu sieci, gdzie przybywa punktów dostępowych, sensorów IoT i stanowisk hybrydowych, ta zdolność decyduje o tym, czy IT nadąża za tempem rozwoju organizacji, czy staje się jego hamulcem. Eliminacja manualnego provisioningu oznacza także uwolnienie zespołów sieciowych od powtarzalnych zadań na rzecz projektów o wyższej wartości.

Integracja i uproszczenie stosu

Zamiast nakładania kolejnych warstw narzędzi, Fabric konsoliduje funkcje sieciowe w ramach jednej, spójnej architektury. Segmentacja, kontrola dostępu, mikrosegmentacja i widoczność ruchu realizowane są natywnie, bez konieczności integrowania rozwiązań third-party na każdym z tych poziomów.

W kontekście usług budowanych na edge'u – od usług lokalizacyjnych po dynamiczną kontrolę dostępu gości – eliminuje to złożoność, która w podejściu tradycyjnym generuje opóźnienia wdrożeń i nieproporcjonalnie wysokie koszty utrzymania.

Klasyczne protokoły STP, projektowane z myślą o eliminacji pętli, jednocześnie blokują redundantne ścieżki i ograniczają efektywność wykorzystania infrastruktury. Fabric rozwiązuje ten problem po stronie architektury. Pętle nie powstają dzięki natywnej enkapsulacji (opakowywanie danych w dodatkowy nagłówek, aby sieć mogła je przesyłać niezależnie od oryginalnego protokołu) i routingowi na każdym węźle, a wszystkie dostępne połączenia są aktywne i przenoszą ruch produkcyjny. Awaria pojedynczego elementu powoduje automatyczną rekonwergencję (proces, w którym sieć po awarii jednego łącza lub urządzenia samodzielnie przelicza trasy i przywraca przepływ ruchu alternatywnymi ścieżkami) bez przerwy w świadczeniu usług. Z perspektywy biznesowej to różnica między minutą niedostępności a godzinami diagnostyki i ręcznego odtwarzania konfiguracji. To różnica, która na brzegu sieci przekłada się bezpośrednio na ciągłość procesów operacyjnych.

Adam Mazurkiewicz
Network and Security Solutions Engineer
w Axians

Technologia Extreme Networks Fabric, oparta na standardzie Shortest Path Bridging (SPB), całkowicie zmienia sposób budowania infrastruktury. Dzięki działaniu w warstwie 2. urządzenia można po prostu wyjąć z pudełka i dowolnie połączyć, tworząc zautomatyzowaną strukturę. Fabric eliminuje problem pętli, który w tradycyjnych sieciach blokuje redundantne połączenia przez protokół STP, tutaj wszystkie ścieżki są aktywne, a dane zawsze przesyłane są najkrótszą drogą. Zapewnia to pełną niezależność od topologii fizycznej oraz automatyczną rekonwergencję w przypadku awarii, bez przerw w świadczeniu usług.

Partner wdrożeniowy dla nowoczesnej architektury sieciowej

Axians – marka należąca do grupy VINCI Energies – prowadzi działalność w obszarze ICT w Polsce oraz w kilkudziesięciu krajach na całym świecie. Jako integrator systemów IT, wspieramy przedsiębiorstwa prywatne, instytucje publiczne, operatorów i dostawców usług w rozwoju nowoczesnej infrastruktury oraz rozwiązań cyfrowych, dopasowanych do ich potrzeb i strategii biznesowych.

Oferujemy kompleksowe portfolio usług, obejmujące infrastrukturę sieciową, cyberbezpieczeństwo oraz rozwiązania chmurowe, zapewniając wsparcie na każdym etapie – od projektu, przez wdrożenie, aż po utrzymanie i rozwój środowiska IT

Nasi eksperci starannie dobierają technologie, które oferujemy naszym klientom. Firmy poszukujące wsparcia w cyfrowej zmianie swoich biznesów i procesów mogą być pewne, że zastosowane rozwiązania należą do światowej czołówki. Co ważniejsze – są technologiami sprawdzonymi i godnymi zaufania.

Wieloletnie partnerstwo z Extreme Networks opiera się na starannej selekcji technologii, a unikalne możliwości platformy Fabric pozwalają naszym ekspertom dostarczać rozwiązania idealnie dopasowane do strategii biznesowych klientów.

Dlaczego warto współpracować z Axians przy wdrażaniu rozwiązań Extreme Networks?

Axians zapewnia wsparcie eksperckiego zespołu certyfikowanych inżynierów oraz dedykowanego opiekuna projektu. Dzięki temu klienci otrzymują wysokiej jakości usługę, kompleksową obsługę end-to-end oraz rozwiązania dopasowane do swoich potrzeb. Indywidualnie dobrany model finansowania pozwala natomiast efektywnie zarządzać inwestycją technologiczną.

Nowy standard zarządzania infrastrukturą IT

Rosnące rozproszenie środowisk IT jednoznacznie pokazuje, że dalsze skalowanie infrastruktury wymaga odejścia od tradycyjnych modeli zarządzania na rzecz architektur opartych na automatyzacji i spójnych politykach operacyjnych. Podejście reprezentowane przez rozwiązania Extreme Networks, w szczególności koncepcję Fabric, umożliwia przejście od złożonych, trudnych w utrzymaniu struktur do zautomatyzowanego, odpornego i centralnie zarządzanego środowiska.

W praktyce oznacza to uproszczenie operacji, zwiększenie przewidywalności działania oraz zdolność do szybkiego skalowania infrastruktury w odpowiedzi na potrzeby biznesu. Współpraca z Axians pozwala przełożyć te założenia na realne wdrożenia – od etapu projektowania, przez implementację, po długofalowe zarządzanie środowiskiem – z uwzględnieniem specyfiki organizacji oraz optymalizacji kosztów.

Axians – Twój partner wdrożeniowy technologii Extreme Networks

axians

Axians IT Solutions Poland & Axians IT Services Poland
ul. Postępu 21D · 02-676 Warszawa
Tel.: +48 22 535 95 00 · E-mail: zapytaniaofertowe@axians.pl
www.axians.pl

Materiał powstał przy współpracy:

Extreme networks