

VMWARE NSX DATA CENTER

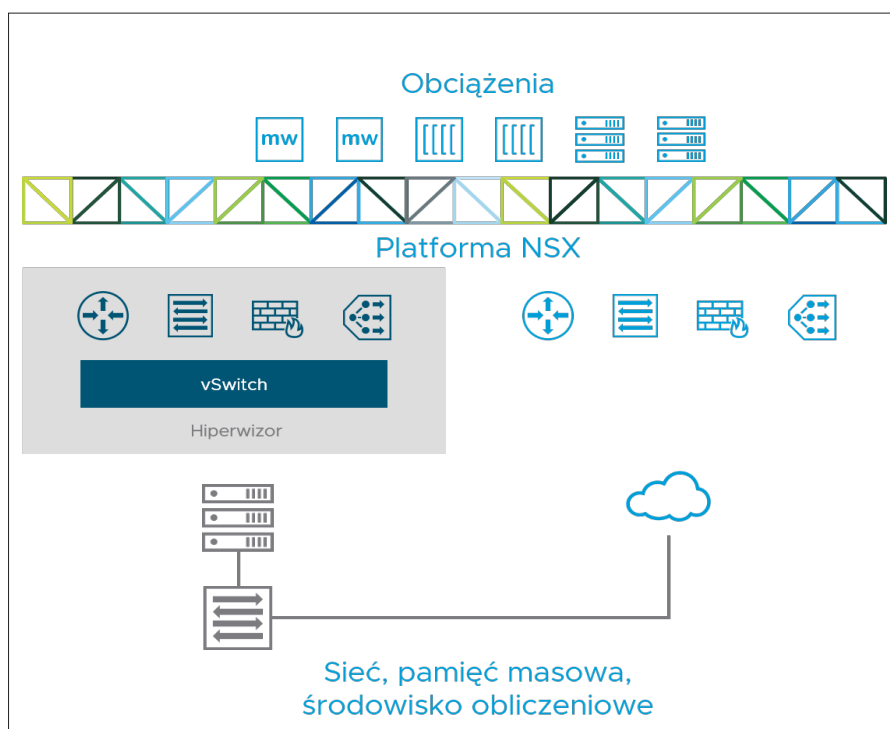
Platforma wirtualizacji sieci i zabezpieczeń

PODSTAWOWE INFORMACJE

VMware NSX® Data Center to platforma wirtualizacji sieci i zabezpieczeń umożliwiająca utworzenie wirtualnej sieci w chmurze, czyli sterowanego programowo rozwiązania do pracy w sieci, które obejmuje centra przetwarzania danych, chmury, urządzenia końcowe i elementy Internetu rzeczy. Dzięki rozwiązaniu NSX Data Center funkcje sieciowe i zabezpieczenia trafiają bliżej aplikacji niezależnie od miejsca jej uruchomienia – od maszyn wirtualnych przez kontenery po komputery bez oprogramowania. Sieci, podobnie jak maszyny wirtualne, można wdrażać i obsługiwać niezależnie od sprzętu, na którym działają. Platforma NSX Data Center programowo odtwarza cały model sieci oraz umożliwia utworzenie i wdrożenie w ciągu kilku sekund sieci o dowolnej topologii – od prostej do wielowarstwowej. Użytkownicy mogą tworzyć wiele sieci wirtualnych o zróżnicowanych wymaganiach, łącząc usługi oferowane za pośrednictwem platformy NSX lub szerokiego ekosystemu zintegrowanych rozwiązań innych firm – od zapór ogniowych nowej generacji po rozwiązania do zarządzania wydajnością – w celu budowania bardziej elastycznych i bezpiecznych środowisk. Usługi te można następnie rozszerzyć o wiele urządzeń końcowych oraz chmury.

GŁÓWNE KORZYŚCI

- Mikrosegmentacja i szczegółowe zabezpieczenia dla każdego obciążenia
- Skrócenie czasu wdrażania sieci z wielu dni do kilku sekund i podwyższenie efektywności operacyjnej dzięki automatyzacji
- Mobilność obciążeń niezależnie od fizycznej topologii sieci w centrach przetwarzania danych i między nimi
- Lepsze zabezpieczenia i zaawansowane usługi sieciowe dostarczane przez największych dostawców zewnętrznych



Rysunek 1. NSX Data Center: platforma wirtualizacji sieci i zabezpieczeń

Wirtualizacja sieci, zabezpieczenia i centrum danych sterowane programowo

Platforma VMware NSX Data Center całkowicie odmienia model operacyjny pracy w sieci, stanowiąc podstawę centrum danych sterowanego programowo (SDDC). Dzięki temu operatorzy centrów danych mogą osiągać poziomy elastyczności, bezpieczeństwa i ekonomii, które były nieosiągalne, gdy sieć centrów danych zależała ściśle od fizycznych składników sprzętu. Platforma NSX Data Center zapewnia kompletny zestaw elementów i usług sieci logicznej, w tym logiczne przełączanie, routing, zapórę ogniową, równoważenie obciążenia, VPN, jakość usług (funkcję QoS) i monitorowanie. Usługi te są dostarczane w sieciach wirtualnych za pośrednictwem dowolnej platformy zarządzania chmurą przy użyciu interfejsów API platformy NSX Data Center. Wdrażanie sieci wirtualnych odbywa się bez zakłócania działania istniejącej infrastruktury sprzętowej sieci.

Kluczowe cechy platformy NSX Data Center

Przełączanie	Możliwość rozszerzania logicznej sieci overlay drugiej warstwy w obrębie infrastruktury routingu (warstwa 3) i poza granice centrów przetwarzania danych. Obsługa sieci overlay opartych na VXLAN.
Routing	Routing dynamiczny między sieciami wirtualnymi wykonywany w sposób rozproszony w jądrze hiperwizora, routing skalowalny w poziomie z przełączaniem awaryjnym typu aktywny-aktywny przy użyciu routerów fizycznych. Obsługa protokołów routingu statycznego i dynamicznego (OSPF, BGP).
Zapora rozproszona	Rozproszona stanowa zapora ogniowa wbudowana w jądro hiperwizora obsługująca ruch do 20 Gb/s na hosta hiperwizora. Obsługa Active Directory i monitorowanie aktywności. Dodatkowo platforma NSX Data Center zapewnia zapórę działającą w trybie klient-serwer dzięki wykorzystaniu rozwiązania NSX Edge™.
Równoważenie obciążenia	Mechanizm równoważenia obciążenia L4-L7 z funkcją przenoszenia i przekazywania obciążenia SSL, sprawdzaniem stanu serwerów oraz regułami aplikacji, które zapewniają możliwość programowania i sterowania ruchem.
Sieć VPN	Obsługa funkcji sieci VPN dostępu zdalnego i między ośrodkami, niezarządzana sieć VPN umożliwiająca korzystanie z usług bramy do chmury.
Brama NSX	Zapewnianie pomostu między sieciami VXLAN i VLAN w celu utworzenia sprawnego połączenia do obsługi obciążeń fizycznych. Jest to zarówno standardowa funkcja rozwiązania NSX Data Center, jak i funkcja przełączników top-of-rack dostarczanych przez partnera z ekosystemu.
Interfejs programistyczny NSX Data Center	Interfejs programistyczny typu RESTful umożliwiający integrację z dowolną platformą zarządzania chmurą lub własnym rozwiązaniem do automatyzacji.
Operacje	Natywne funkcje obsługi, takie jak centralny CLI, traceflow, SPAN i IPFIX, umożliwiające rozwiązywanie problemów i aktywne monitorowanie infrastruktury. Integracja z takimi narzędziami jak VMware vRealize® Operations™ i vRealize Log Insight™ zapewniająca zaawansowane funkcje analizy i rozwiązywania problemów. Narzędzie Application Rule Manager i funkcja monitorowania urządzeń końcowych umożliwiają kompleksową wizualizację przepływu ruchu w sieci do warstwy 7, co pozwala zespołom tworzącym aplikacje na identyfikowanie urządzeń końcowych zarówno w centrach danych, jak i między nimi, oraz reagowanie przez tworzenie odpowiednich reguł bezpieczeństwa.
Mikrosegmentacja kontekstowa	NSX Data Center umożliwia tworzenie dynamicznych grup zabezpieczeń oraz skojarzonych zbiorów reguł opartych nie tylko na takich czynnikach jak adres IP czy MAC, ale również na obiektach i znacznikach VMware vCenter®, typie systemu operacyjnego oraz informacjach na temat aplikacji warstwy 7, co z kolei pozwala na mikrosegmentację na podstawie kontekstu aplikacji. Zbiór reguł opartych na weryfikacji tożsamości przy użyciu danych logowania z maszyn wirtualnych, usługi Active Directory i integracji zarządzania urządzeniami mobilnymi umożliwia utworzenie zabezpieczeń opartych na użytkowniku, w tym zabezpieczeń na poziomie sesji w zdalnych i wirtualnych środowiskach desktopowych.
Zarządzanie chmurą	Natywna integracja z vRealize Automation™ i OpenStack.
Integracja z rozwiązaniami innych producentów	Obsługa zarządzania, warstwy kontroli i integracji warstwy danych z rozwiązaniami innych producentów w szerokim zakresie kategorii, takich jak zapory ogniowe nowej generacji, IDS/IPS, oprogramowanie antywirusowe bez agenta, kontrolery dostarczania aplikacji, przełączanie, operacje i wgląd, zaawansowane funkcje bezpieczeństwa i inne.
Sieć i zabezpieczenia w wielu ośrodkach	Możliwość rozszerzania sieci i zabezpieczeń poza granice centrów przetwarzania danych niezależnie od fizycznej topologii — co umożliwia m.in. przywracanie po awarii i korzystanie z centrów danych aktywne-aktywne.

WIĘCEJ INFORMACJI

Odwiedź stronę www.vmware.com/go/nsx.

Więcej informacji na temat funkcji poszczególnych licencjonowanych edycji NSX można znaleźć pod adresem <https://kb.vmware.com/kb/2145269>.

Aby uzyskać więcej informacji lub nabyć produkty firmy VMware, należy zadzwonić pod numer 877-4-VMWARE (lub +1-650-427-5000 dla klientów spoza Ameryki Północnej), odwiedzić witrynę www.vmware.com/pl/products albo znaleźć w Internecie autoryzowanego sprzedawcę.

Scenariusze użycia

Zabezpieczenia

NSX Data Center umożliwia organizacjom dzielenie centrów przetwarzania danych na osobne segmenty zabezpieczeń, aż do poziomu indywidualnego zadania – niezależnie od miejsca jego przetwarzania. Zespoły IT mogą definiować reguły dla każdego obciążenia na podstawie kontekstu aplikacji i użytkowników, co umożliwia im natychmiastowe reagowanie na zagrożenia pojawiające się w centrach przetwarzania danych oraz wymuszanie stosowania reguł na poziomie aplikacji. Jeśli napastnikowi uda się przedrzeć przez zabezpieczenia obwodowe, to w odróżnieniu od tradycyjnych sieci nie będzie miał możliwości poziomego ruchu w centrum przetwarzania danych.

Automatyzacja

VMware NSX Data Center wirtualizuje wszystkie funkcje sieci i zabezpieczeń, by umożliwić szybsze wdrażanie i pełną automatyzację cyklu życia tradycyjnych i nowych aplikacji w wielu ośrodkach i chmurach. Automatyzacja żmudnych zadań, wdrażanie nowych natywnych aplikacji chmurowych i działania realizowane na bieżąco pozwalają organizacjom IT i programistom dotrzymać kroku firmom rozwijającym się w szybkim tempie.

Praca w sieci w wielu chmurach

Dzięki temu, że NSX Data Center oddziela funkcje sieciowe od sprzętu, reguły sieci i zabezpieczeń są powiązane z właściwymi im zadaniami. W przypadku awarii organizacja może z łatwością przeprowadzić replikację całych środowisk aplikacji do zdalnych centrów danych, przenieść je z jednego centrum danych do innego lub wdrożyć je w środowisku chmury hybrydowej. Wszystko to odbywa się w ciągu kilku minut – bez zakłócania działania aplikacji ani wprowadzania jakichkolwiek zmian w sieci fizycznej.

Sieć i zabezpieczenia w natywnych aplikacjach chmurowych

VMware NSX Data Center zapewnia natywną łączność sieciową w pełnym zakresie oraz zabezpieczenia aplikacji i mikrousług umieszczonych w kontenerach, oferując szczegółowe reguły dla poszczególnych kontenerów w toku projektowania nowych aplikacji. Umożliwia to natywną łączność między kontenerami (L3), mikrosegmentację na potrzeby mikrousług oraz kompleksowy wgląd w reguły sieci i zabezpieczeń zarówno w przypadku tradycyjnych, jak i nowych aplikacji.

Edycje VMware NSX Data Center

Standard

Dla organizacji potrzebujących elastyczności i automatyzacji sieci.

Professional

Dla organizacji potrzebujących funkcji dostępnych w wersji Standard rozszerzonych o mikrosegmentację, które mogą korzystać z urządzeń końcowych w chmurze publicznej.

Advanced

Dla organizacji wymagających funkcji dostępnych w wersji Professional rozszerzonych o zaawansowane usługi sieci i zabezpieczeń oraz możliwość integracji z rozległym ekosystemem, które mogą obejmować wiele ośrodków.

Enterprise Plus

Dla organizacji wymagających najbardziej zaawansowanych funkcji, jakie oferuje NSX Data Center, rozszerzonych o wgląd w sieć i działania związane z bezpieczeństwem realizowany przy użyciu vRealize Network Insight™ oraz mobilność chmury hybrydowej zapewnianą przez NSX Hybrid Connect.

ROBO

Dla organizacji szukających rozwiązań umożliwiających wirtualizację łączności i zabezpieczeń na potrzeby aplikacji w odległych biurach lub oddziałach.

	STANDARD	PROFESSIONAL	ADVANCED	ENTERPRISE PLUS	ROBO
NSX DATA CENTER¹					
Rozproszone przełączanie i routing	•	•	•	•	• ⁵
Zapora NSX Edge	•	•	•	•	•
Translacja adresów sieciowych NSX Edge	•	•	•	•	•
Programowe połączenie L2 ze środowiskami fizycznymi	•	•	•	•	
Routing dynamiczny z ECMP (aktywny-aktywny)	•	•	•	•	•
Integracja z platformami zarządzania chmurą ³	•	•	•	•	•
Zapora rozproszona		•	•	•	•
Sieć VPN (L2 i L3)		•	•	•	•
Integracja z NSX Cloud ⁴		•	•	•	•
Równoważenie obciążenia NSX Edge			•	•	•
Integracja z zaporą rozproszoną (Active Directory, AirWatch® i wstawianie usług innych firm)			•	•	•
Application Rule Manager			•	•	•
Sieć i zabezpieczenia w kontenerach			•	•	
Sieć i zabezpieczenia w wielu ośrodkach			•	•	
Integracja z bramami sprzętowymi			•	•	
Monitorowanie urządzeń końcowych				•	
Mikrosegmentacja kontekstowa (identyfikacja aplikacji, RDSH)				•	
+vREALIZE NETWORK INSIGHT ADVANCED²					
Widoczność ruchu (IPFIX) i monitorowanie sieci				•	
Planowanie zapory i zarządzanie nią				•	
Działania związane z wirtualizacją sieci i rozwiązywanie problemów				•	
+NSX HYBRID CONNECT ADVANCED²					
Migracja obciążeń na dużą skalę				•	
Optymalizacja sieci WAN na potrzeby migracji obciążeń				•	
Zarządzanie ruchem i obciążeniem wielu łączy				•	

¹ Najnowsze szczegółowe informacji o funkcjach można znaleźć w artykułach bazy wiedzy na temat funkcji NSX Data Center for vSphere i NSX-T™ Data Center.

² NSX Data Center Enterprise Plus obejmuje pełne wersje rozwiązań vRealize Network Insight Advanced i NSX Hybrid Connect Advanced.

³ Integracja obejmuje wyłącznie warstwy L2 i L3 oraz NSX Edge. Bez użycia grup zabezpieczeń.

⁴ Obciążenia chmury publicznej wymagają subskrypcji NSX Cloud.

⁵ Tylko przełączanie, oparte na VLAN.

