VMWARE NSX CLOUD

Spójne rozwiązania sieci i zabezpieczeń dla aplikacji uruchamianych natywnie w chmurach publicznych

PODSTAWOWE INFORMACJE

VMware NSX® Cloud oferuje spójne rozwiązania sieci i zabezpieczeń dla aplikacji uruchamianych natywnie w chmurze publicznej. NSX Cloud korzysta z tych samych warstw zarządzania i kontroli co platforma NSX Data Center, dostarczając jedno rozwiązanie sieci i zabezpieczeń z prywatnego centrum przetwarzania danych do chmury publicznej.

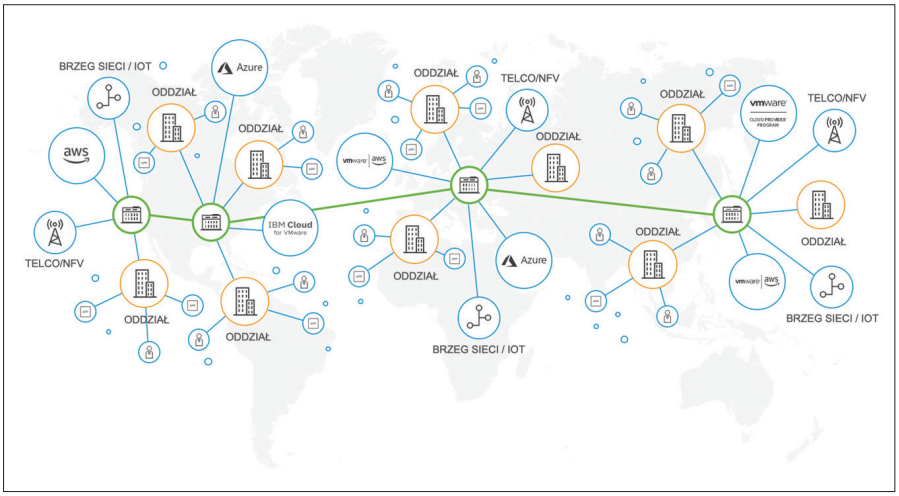
GŁÓWNE KORZYŚCI

Wspólne rozwiązanie sieci i zabezpieczeń w chmurach publicznych, takich jak AWS i Azure, znacząco poprawia skalowalność, kontrolę i wgląd w dane, obniżając koszty operacyjne.

- Prosta skalowalność w obrębie sieci wirtualnych, stref dostępności, regionów i chmur publicznych.
- Precyzyjna kontrola usług w zakresie sieci i zabezpieczeń zapewnia ochronę i standaryzację aplikacji.
- Kompleksowy wgląd w dane sieci i zabezpieczeń wspiera dobrą kondycję i zgodność aplikacji z przepisami w chmurach publicznych.

CENY

- Ceny oparte na modelu subskrypcji obejmujących licencje na 1 rok i 3 lata
- Oparte na procesorach wirtualnych używanych przez realizowane obciążenia w chmurze publicznej, niezależnie od liczby sieci wirtualnych (np. AWS VPC, Azure VNet)
- Licencja na NSX Data Center nie jest wymagana w przypadku użycia tylko w chmurze



Rysunek 1. Wirtualna sieć w chmurze

Sieć zbudowana zgodnie z regułami chmury

VMware NSX Cloud oferuje rozwiązania sieci i zabezpieczeń dla aplikacji uruchamianych natywnie w chmurach publicznych. Razem z rodziną rozwiązań VMware NSX usługa VMware NSX Cloud umożliwia 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.

Scenariusze użycia

Spójne zabezpieczenia we wszystkich chmurach

NSX Cloud umożliwia stosowanie zbioru reguł do obciążeń realizowanych w wielu chmurach publicznych. NSX Cloud korzysta z tych samych warstw kontroli i danych co platforma NSX Data Center, zapewniając kompleksowe zarządzanie zbiorem reguł obejmujące centra przetwarzania danych i chmury. Zbiór reguł jest definiowany tylko raz i stosowany do obciążeń w dowolnym miejscu — w różnych sieciach wirtualnych w chmurze, regionach, strefach dostępności i u wielu dostawców chmury. Reguły zabezpieczeń są dynamicznie egzekwowane dla każdego obciążenia na podstawie atrybutów aplikacji i znaczników zdefiniowanych przez użytkownika. Złośliwe i niebezpieczne obciążenia można nawet automatycznie poddawać kwarantannie, jeśli nie zastosowano do nich właściwego zbioru reguł zabezpieczeń mikrosegmentacji.

Precyzyjna kontrola nad siecią w chmurze

Usługa VMware NSX Cloud została zaprojektowana pod kątem natywnych środowisk chmury publicznej, takich jak Amazon (AWS) i Microsoft Azure. NSX Cloud uzupełnia natywne usługi oferowane przez tych dostawców chmury publicznej. Używając NSX Cloud, można w dalszym ciągu bez ograniczeń korzystać z infrastruktury i usług aplikacyjnych dostawcy chmury publicznej do obsługi zadań (np. AWS ELB/Azure Load Balancer, AWS Route53/Azure DNS, AWS Direct Connect/Azure ExpressRoute oraz Amazon RDS/Azure Database). Przydzielanie zasobów i zarządzanie konfiguracją można zautomatyzować za pomocą żądań interfejsu programistycznego REST, korzystając z istniejących narzędzi do automatyzacji.

WIĘCEJ INFORMACJI O PRODUKTACH FIRMY VMWARE I MOŻLIWOŚCIACH ICH ZAKUPU MOŻNA UZYSKAĆ

TELEFONICZNIE

877-4-VMware (lub +1-650-427-5000 dla klientów spoza Ameryki Północnej)

W INTERNECIE

www.vmware.com/pl/products/nsx-cloud.html lub http://www.vmware.com/pl/products, by zapoznać się z ofertą autoryzowanego sprzedawcy.

Kompleksowa kontrola operacyjna i wgląd w dane

VMware NSX Cloud oferuje standardowe interfejsy i protokoły zapewniające dostęp do danych sieci i zabezpieczeń z sieci w chmurze. Informacje o przepływach, pakietach i zdarzeniach są dostępne za pośrednictwem funkcji IPFIX, Traceflow, dublowania portów i dziennika systemu. Z danych tych można korzystać za pomocą istniejących lokalnych narzędzi operacyjnych w celu uzyskania kompleksowego, szczegółowego wglądu na potrzeby monitorowania, rozwiązywania problemów i audytu. Ten szeroki zestaw danych operacyjnych pozwala radykalnie skrócić czas identyfikacji i rozwiązywania problemów z łącznością sieciową, wydajnością i bezpieczeństwem w całym wdrożeniu chmury hybrydowej, co obejmuje także aplikacje lokalne i w chmurze publicznej.

Najważniejsze funkcje

Sieć i zabezpieczenia w wielu chmurach i ośrodkach: NSX Cloud dostarcza rozwiązania sieciowe i zabezpieczenia do urządzeń końcowych w wielu chmurach. Dzięki integracji z platformą NSX Data Center umożliwia zarządzanie siecią i bezpieczeństwem w obrębie wielu chmur i centrów przetwarzania danych.

Mikrosegmentacja: zapewnia kontrolę nad ruchem poziomym między zadaniami aplikacji realizowanymi natywnie w chmurach publicznych.

Grupy zabezpieczeń: grupy i reguły zabezpieczeń można definiować w oparciu o wiele elementów zbioru reguł, takich jak nazwa instancji, typ systemu operacyjnego, identyfikator AMI i znaczniki definiowane przez użytkownika.

Dynamiczny zbiór reguł: reguły zabezpieczeń są dynamicznie stosowane i egzekwowane na podstawie atrybutów instancji i znaczników zdefiniowanych przez użytkownika. Zbiór reguł automatycznie śledzi instancje przenoszone w obrębie chmur i między nimi.

Instancje kwarantanny: obciążenia ryzykowne lub powiązane z oszustwem, które są realizowane w chmurze publicznej bez zabezpieczeń mikrosegmentacji, mogą być poddawane kwarantannie. Instancje objęte kwarantanną nie mogą komunikować się z siecią w chmurze.

Architektura rozproszona: architektura zapory rozproszonej usługi NSX Cloud eliminuje dodatkowe skoki i ruch w sieci, ponieważ reguły są egzekwowane w interfejsie sieci wirtualnej każdej instancji, a nie przekazywane przez zewnętrzną zaporę ogniową.

Zapora Edge: NSX Cloud oferuje stanową zaporę ogniową, która filtruje poziomy przepływ ruchu między instancjami w sieciach wirtualnych i publicznym Internecie.

Interfejs programistyczny RESTful: interfejs programistyczny RESTful i narzędzia do automatyzacji umożliwiają programowe przydzielanie zasobów do infrastruktury sieci i zabezpieczeń oraz jej konfigurowanie na żądanie.

Szablony: przy użyciu istniejących narzędzi do automatyzacji i orkiestracji można tworzyć ustandaryzowane szablony aplikacji oraz upraszczać przydzielanie zasobów i zarządzanie usługami sieci i zabezpieczeń w chmurach publicznych.

Wgląd w dane o ruchu poziomym: istniejące narzędzia do przeprowadzania dalszych działań codziennego zarządzania pozwalają uzyskać wgląd w ruch poziomy w obrębie wirtualnych chmur prywatnych i między nimi.

Rejestrowanie zdarzeń zabezpieczeń: można korzystać z wglądu w dane w czasie rzeczywistym i prowadzić audyt zdarzeń zabezpieczeń, takich jak zezwolenia i odmowy czy zdarzenia kwarantanny. Informacje o zdarzeniach zabezpieczeń można wysyłać do dziennika systemowego lub serwera SIEM.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Faks 650-427-5001 www.vmware.com/pl

Pozycja nr: 149451wf-vmw-q2fy19-sddc-launch-ds-nsx-cld-a4
6/18