VMWARE NSX CLOUD

Konzistentní sítě a zabezpečení pro aplikace nativně provozované ve veřejných cloudech

STRUČNÝ PŘEHLED

Řešení VMware NSX® Cloud poskytuje konzistentní sítě a zabezpečení pro aplikace nativně provozované ve veřejném cloudu. Řešení NSX Cloud používá stejnou vrstvu správy a řízení jako řešení NSX Data Center a vytváří tak jedno řešení pro sítě a zabezpečení od privátních datových center až po veřejné cloudy.

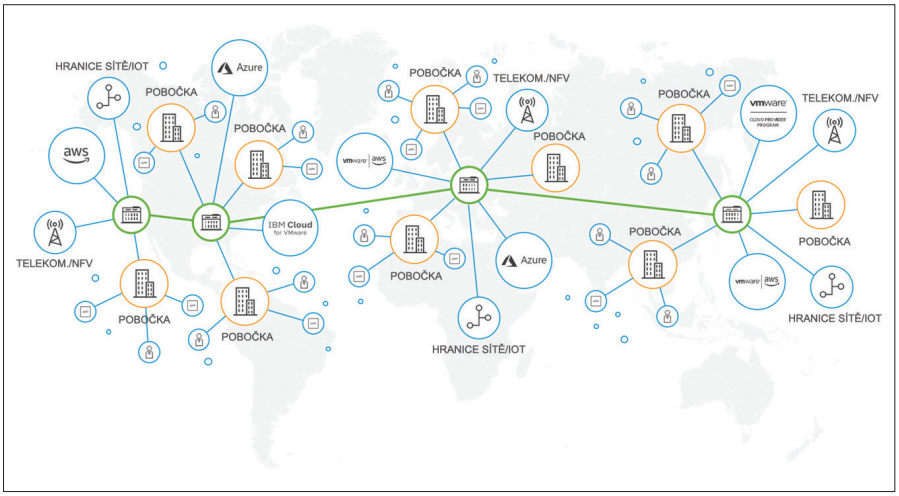
KLÍČOVÉ VÝHODY

Jednotné sítě a zabezpečení ve všech veřejných cloudech, například AWS a Azure, poskytují výrazně lepší škálovatelnost, možnosti řízení a přehled spolu s nižšími provozními náklady.

- Umožňuje jednoduché škálování napříč virtuálními sítěmi, zónami dostupnosti, oblastmi a veřejnými cloudy.
- Přesné řízení služeb pro zabezpečení a sítě zajišťuje ochranu a standardizaci aplikací.
- Kompletní přehled o sítích a zabezpečení umožňuje udržovat dobrý stav aplikací ve veřejných cloudech a jejich shodu s předpisy.

CENY

- Ceny se zakládají na předplatném a dostupné jsou licence na období 1 roku nebo 3 let.
- Ceny se zakládají na počtu virtuálních procesorů vCPU, které jsou využívány spuštěnými pracovními zatíženími ve veřejném cloudu, bez ohledu na počet virtuálních sítí (například počet virtuálních cloudů AWS VPC nebo počet virtuálních sítí Azure VNet).
- Případy použití jen v cloudu nevyžadují licenci na řešení NSX Data Center.



Obrázek 1: Virtuální cloudová síť

Síť vytvořená s ohledem na principy cloudu

Řešení VMware NSX Cloud poskytuje sítě a zabezpečení pro vaše aplikace nativně provozované ve veřejných cloudech. Spolu s produktovou řadou řešení VMware NSX vytváří řešení VMware NSX Cloud virtuální cloudovou síť a umožňuje softwarově definovaný přístup k práci se sítěmi, který překlenuje datová centra, cloudy, koncové body a věci.

Příklady použití

Konzistentní zabezpečení ve všech cloudech

Řešení NSX Cloud umožňuje používat zásady pro všechna pracovní zatížení provozovaná ve více veřejných cloudech. Řešení NSX Cloud používá stejnou řídicí a datovou vrstvu jako řešení NSX Data Center a umožňuje tak ucelenou správu zásad v datových centrech i cloudech. Zásady stačí definovat jednou a používat pro aplikační zatížení, která se mohou nacházet kdekoli – ve všech cloudových virtuálních sítích, oblastech a zónách dostupnosti nebo u více cloudových poskytovatelů. Zásady zabezpečení jsou dynamicky používány pro jednotlivá pracovní zatížení na základě atributů aplikace a značek definovaných uživateli. Neautorizovaná nebo napadená pracovní zatížení je dokonce možné automaticky umísťovat do karantény, pokud nepoužívají správné zásady zabezpečení pomocí mikrosegmentace.

Přesná kontrola nad cloudovými sítěmi

Řešení VMware NSX Cloud je navrženo pro nativní prostředí veřejných cloudů, jako je Amazon AWS nebo Microsoft Azure. Řešení NSX Cloud doplňuje nativní služby, které jsou dostupné od těchto poskytovatelů veřejných cloudů. Řešení NSX Cloud umožňuje pro pracovní zatížení i nadále bez omezení používat služby od poskytovatele veřejného cloudu pro infastrukturu a aplikace (například AWS ELB / Azure Load Balancer, AWS Route53 / Azure DNS, AWS Direct Connect / Azure ExpressRoute nebo Amazon RDS / Azure Database). Zajišťování a správu konfigurací je možné automatizovat prostřednictvím žádostí zasílaných přes rozhraní REST API s použitím stávajících automatizačních nástrojů.

POKUD CHCETE ZÍSKAT DALŠÍ INFORMACE NEBO ZAKOUPIT PRODUKTY SPOLEČNOSTI VMWARE:

VOLEJTE NA ČÍSLO:
+420 255 725 410 (v Severní Americe 877-4-VMWARE),

NAVŠTIVTE STRÁNKU:
www.vmware.com/cz/products/nsx-cloud.html nebo http://www.vmware.com/cz/products nebo si na internetu vyhledejte autorizovaného prodejce.

Kompletní přehled o provozu a možnosti jeho řízení

Řešení VMware NSX Cloud poskytuje standardní rozhraní a protokoly, které poskytují přístup k údajům o sítích a zabezpečení z cloudových sítí. Informace o tocích dat, paketech a událostech jsou dostupné prostřednictvím protokolu IPFIX, nástroje Traceflow, zrcadlení portů a standardu Syslog. Tyto údaje je možné přijímat do stávajících místních provozních nástrojů a získat pomocí nich podrobný a úplný přehled pro účely monitorování, řešení potíží a auditování. Tyto rozsáhlé provozní údaje pomáhají výrazně zkrátit čas potřebný na identifikaci a řešení problémů spojených se síťovým připojením, výkonem a zabezpečením v celém nasazení hybridního cloudu, včetně aplikací v místním prostředí a veřejném cloudu.

Hlavní funkce

Sítě a zabezpečení překlenující více cloudů a lokalit: Řešení NSX Cloud přináší funkce pro sítě a zabezpečení do koncových bodů, které se mohou nacházet ve více cloudech. Integrace s řešením NSX Data Center umožňuje správu sítí a zabezpečení napříč cloudy a lokalitami datových center.

Mikrosegmentace: Umožňuje získat kontrolu nad vnitřními datovými přenosy (east-west) mezi pracovními zatíženími aplikací, která jsou nativně provozována ve veřejných cloudech.

Skupiny zabezpečení: Je možné definovat skupiny a pravidla zabezpečení na základě rozsáhlé sady konstruktů zásad, jako jsou názvy instancí, typ operačního systému, identifikátor bitové kopie AMI nebo značky definované uživateli.

Dynamické zásady: Zásady zabezpečení jsou automaticky používány a vymáhány na základě atributů instancí a značek definovaných uživateli. Když jsou instance přesouvány v rámci cloudu nebo mezi cloudy, zásady je automaticky následují.

Umisťování instancí do karantény: Neautorizovaná nebo napadená pracovní zatížení, která jsou provozována ve veřejném cloudu bez zabezpečení pomocí mikrosegmentace, jsou umístěna do karantény. Instance v karanténě nemají povoleno komunikovat s cloudovou sítí.

Distribuovaná architektura: Architektura distribuované brány firewall řešení NSX Cloud eliminuje dodatečné přenosy přes další síťové segmenty, protože zásady jsou vymáhány na rozhraních virtuální sítě jednotlivých instancí a nejsou směrovány přes externí bránu firewall.

Brána firewall na hranicích sítě: Řešení NSX Cloud poskytuje stavové funkce brány firewall, které filtrují přenosy north-south mezi instancemi ve virtuálních sítích a veřejným internetem.

Rozhraní RESTful API: Rozhraní RESTful API a automatizační nástroje umožňují na požádání programově zajišťovat a konfigurovat infrastrukturu sítí a zabezpečení.

Šablony: Pomocí stávajících nástrojů pro automatizaci a orchestraci můžete vytvářet standardizované šablony aplikací a zjednodušit zajišťování a správu služeb sítě a zabezpečení ve všech veřejných cloudech.

Přehled o vnitřních datových přenosech (east-west): Pomocí stávajících nástrojů pro řízení provozu ihned po nasazení můžete získat přehled o vnitřních datových přenosech (east-west) v rámci virtuálních privátních cloudů VPC i mezi nimi.

Protokolování zabezpečení: Budete mít v reálném čase přehled o událostech zabezpečení, jako jsou zamítnutí nebo povolení a incidenty umisťování do karantény, a získáte možnost jejich kontroly a protokolování. Informace o událostech zabezpečení je možné zasílat na server využívající standard Syslog nebo server systému SIEM.

VMware, Inc., 3401 Hillview Avenue, Palo Alto CA 94304, USA, tel.: 877-486-9273, fax: 650-427-5001, www.vmware.com
VMware International Limited, Anděl Park Smíchov – Scott&Weber Office, Karla Engliše 3201/6, 150 00 Praha 5, Česká republika, tel.: +420 255 725 410, fax: +420 255 725 401, www.vmware.com/cz