VMWARE NSX DATA CENTER

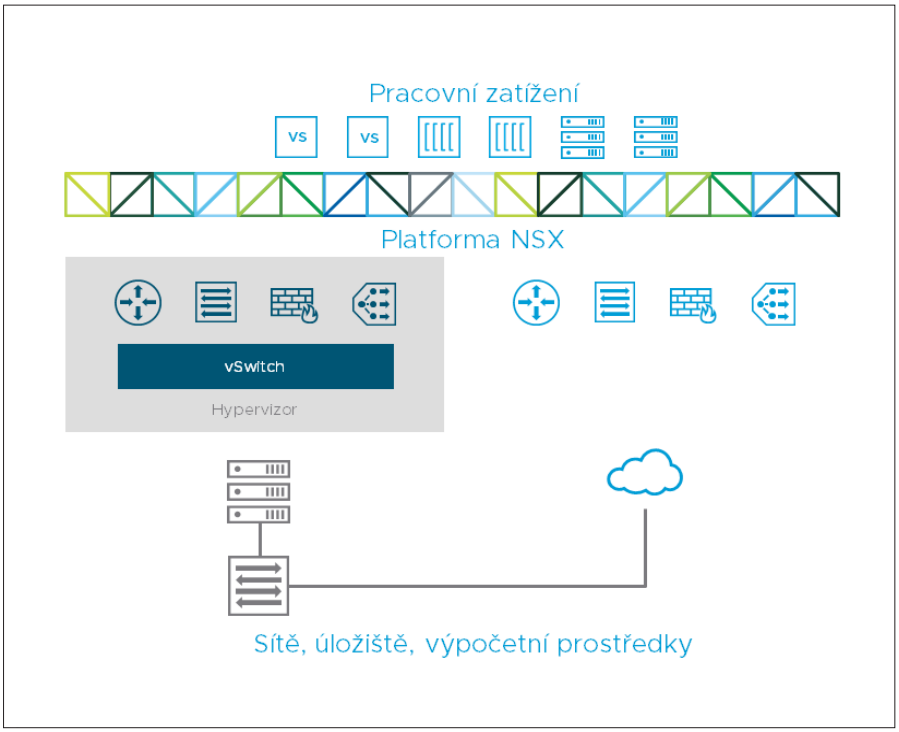
Platforma pro virtualizaci a zabezpečení sítí

STRUČNÝ PŘEHLED

Řešení VMware NSX® Data Center je platforma pro virtualizaci a zabezpečení sítí umožňující používat virtuální cloudovou síť v rámci softwarově definovaného přístupu k sítím, který překlenuje datová centra, cloudy, koncové body a věci. Při použití řešení NSX Data Center se síťové funkce a zabezpečení nacházejí blíže k aplikacím bez ohledu na to, kde jsou provozovány, od virtuálních počítačů přes kontejnery až po fyzický hardware. Podobně jako u provozního modelu virtuálních strojů je možné sítě zajišťovat a spravovat nezávisle na použitém hardwaru. Řešení NSX Data Center reprodukuje celý síťový model v softwaru, čímž umožňuje vytvořit a zajistit během několika sekund libovolnou topologii – od jednoduchých sítí až po složité vícevrstvé sítě. Uživatelé mohou vytvářet více virtuálních sítí s různými požadavky s využitím kombinace služeb nabízených řešením NSX a integrace s rozsáhlým ekosystémem řešení od třetích stran, od bran firewall nové generace až po řešení pro řízení výkonu, což umožňuje vybudovat prostředí, která jsou ze své podstaty pružnější a bezpečnější. Tyto služby je pak možné rozšířit do mnoha koncových bodů v rámci jednoho nebo více cloudů.

KLÍČOVÉ VÝHODY

- Mikrosegmentace a podrobně nastavitelné zabezpečení jsou poskytovány pro jednotlivá pracovní zatížení.
- Automatizace zkracuje dobu zajišťování sítě z několika dní na několik sekund a zvyšuje provozní efektivitu.
- Mobilita pracovních zatížených nezávisí na topologii fyzické sítě v rámci jednoho nebo více datových center.
- Ekosystém předních nezávislých dodavatelů poskytuje vyšší úroveň zabezpečení a pokročilé síťové služby.



Obrázek 1: NSX Data Center: platforma pro virtualizaci a zabezpečení sítí

Virtualizace sítě, zabezpečení a softwarově definované datové centrum

Řešení VMware NSX Data Center nabízí zcela nový provozní model pro sítě definované v softwaru, který je základem pro softwarově definovaná datová centra (SDDC). Provozovatelé datových center mohou nyní dosáhnout takové pružnosti, zabezpečení a úspor, které dříve nebylo možné realizovat, protože síť datového centra byla svázána s fyzickými hardwarovými komponentami. Řešení NSX Data Center nabízí úplnou sadu logických síťových prvků a služeb, včetně logického přepínání, směrování, bran firewall, vyrovnávání zatížení, sítí VPN, kvality služeb (QoS) a sledování stavu. Tyto služby jsou ve virtuálních sítích poskytovány prostřednictvím jakékoli platformy pro správu cloudů využívající rozhraní API řešení NSX Data Center. Virtuální sítě lze nasazovat bez narušení provozu na libovolný existující síťový hardware.

Hlavní funkce řešení NSX Data Center

Přepínání	Možnost překryvných rozšíření logické vrstvy L2 po směrované infrastruktuře (vrstvy L3) uvnitř datových center a za jejich hranicemi. Podpora překryvných síťových modelů na základě sítí VXLAN.
Směrování	Dynamické směrování mezi virtuálními sítěmi prováděné distribuovaně v jádru hypervizoru, směrování s horizontálním škálováním se zotavením po havárii typu aktivní-aktivní a fyzickými směrovači. Podpora protokolů pro statické i dynamické směrování (OSPF, BGP).
Distribuované funkce brány firewall	Distribuované stavové funkce brány firewall integrované do jádra hypervizoru, které nabízejí kapacitu brány firewall až 20 Gb/s na každého hostitele hypervizoru. Podpora služby Active Directory a sledování aktivity. Kromě toho může řešení NSX Data Center poskytovat také funkce brány firewall mezi klientem a datovým centrem (north-south) prostřednictvím řešení NSX Edge™.
Vyrovnávání zatížení	Vyrovnávání zatížení na vrstvách L4–L7 s režimem offload nebo pass-through protokolu SSL, kontrolou stavu serverů a pravidly pro aplikace s ohledem na možnosti programování a manipulace s provozem.
Síť VPN	Funkce sítí VPN mezi lokalitami a pro vzdálený přístup, nespravované sítě VPN pro služby cloudové brány.
Brána NSX	Podpora přemostění VXLAN-VLAN pro hladké připojování k fyzickým pracovním zatížením. Tato funkce je nativní v řešení NSX Data Center a současně ji poskytují přepínače třídy top-of-rack od partnerů v ekosystému.
Rozhraní API řešení NSX Data Center	Rozhraní RESTful API pro integraci s libovolnou platformou pro správu cloudů nebo vlastní automatizaci.
Provoz	Nativní provozní funkce, jako je centrální rozhraní příkazového řádku, sledování paketu (Traceflow), SPAN a IPFIX pro řešení potíží a proaktivní monitorování infrastruktury. Integrace s nástroji, jako jsou řešení VMware vRealize® Operations™ a vRealize Log Insight™, pro pokročilou analýzu a řešení potíží. Funkce správy aplikačních pravidel a monitorování koncových bodů umožňují plně vizualizovat toky dat v síti až do sedmé vrstvy, což aplikačním týmům pomáhá identifikovat koncové body v rámci jednoho nebo více datových center a reagovat vytvořením příslušných pravidel zabezpečení.
Mikrosegmentace zohledňující kontext	Řešení NSX Data Center umožňuje vytvářet dynamické skupiny zabezpečení a související zásady, které se zakládají kromě adresy IP a MAC i na dalších faktorech, včetně objektů a značek řešení VMware vCenter®, typu operačního systému a informací o aplikacích ze sedmé vrstvy, a díky tomu realizovat mikrosegmentaci na základě kontextu aplikací. Zásady založené na identitách, které využívají přihlašovací údaje z virtuálních strojů, služby Active Directory a integrace s řešením Mobile Device Management (MDM), zajišťují zabezpečení na základě uživatelů, včetně zabezpečení na úrovni relací v prostředích vzdálených nebo virtuálních desktopů.
Správa cloudu	Nativní integrace s řešeními vRealize Automation™ a OpenStack.
Integrace nezávislých partnerů	Podpora integrace s nezávislými partnery na úrovni vrstvy správy, řídicí a datové vrstvy v široké škále kategorií, jako jsou brány firewall nové generace, systémy IDS/IPS, antivirové programy bez agentů, ovládací systémy poskytování aplikací, přepínání, provoz a viditelnost, pokročilé zabezpečení a další.
Sítě a zabezpečení ve více lokalitách	Práci se sítěmi a zabezpečením můžete rozšířit za hranice datového centra bez ohledu na to, na jaké fyzické topologii pracujete – to vám umožní využívat funkce, jako je zotavení po havárii a konfigurace datových center typu aktivní-aktivní.

DALŠÍ INFORMACE

Navštivte stránky https://www.vmware.com/cz/products/nsx.html.

Další podrobnosti o funkcích licencování edice řešení NSX najdete na adrese https://kb.vmware.com/kb/2145269.

Další informace o všech produktech společnosti VMware a možnostech jejich zakoupení získáte na čísle +420 255 725 410 (v Severní Americe 877-4-VMWARE), na stránce http://www.vmware.com/cz/products nebo od autorizovaných prodejců, které si můžete vyhledat na internetu.

Příklady použití

Zabezpečení

Řešení NSX Data Center umožňuje organizacím rozdělit datové centrum na samostatné bezpečnostní segmenty, a to až na úrovni jednotlivých pracovních zatížení a nezávisle na tom, kde je pracovní zatížení provozováno. Týmy IT pak mohou definovat zásady pro jednotlivá pracovní zatížení na základě kontextu aplikací a uživatelů, což zaručuje okamžitou reakci na hrozby uvnitř datového centra a vynucování zásad až na úrovni aplikací. Na rozdíl od tradičních sítí tak platí, že pokud útoky proniknou vnější ochranou, nemohou postupovat laterálně do celého datového centra.

Automatizace

Řešení VMware NSX Data Center virtualizuje všechny funkce sítí a zabezpečení, a umožňuje tak rychlejší zavádění a kompletní automatizaci životního cyklu tradičních i nových aplikací s využitím konzistentních postupů ve všech lokalitách i cloudech. Automatizace rutinních úkolů, distribuce nových nativních cloudových aplikací a dlouhodobého provozu umožňuje oddělením IT a vývojářům držet krok se stále se zvyšujícím tempem podnikání.

Sítě překlenující více cloudů

Řešení NSX Data Center odděluje sítě prostřednictvím abstrakce od používaného hardwaru, a proto jsou zásady pro sítě a zabezpečení připojeny k příslušným pracovním zatížením. Organizace mohou snadno replikovat celá aplikační prostředí na vzdálená datová centra a zajistit tak zotavení po havárii, přenášet rychle pracovní zatížení z jednoho datového centra do jiného nebo je nasazovat do hybridních cloudových prostředí – to vše za několik minut, bez narušení činnosti jiných aplikací nebo manipulace s fyzickou sítí.

Sítě a zabezpečení pro nativní cloudové aplikace

Řešení VMware NSX Data Center poskytuje kontejnerizovaným aplikacím a mikroslužbám kompletní sadu funkcí pro sítě a zabezpečení a při vývoji nových aplikací umožňuje podrobně nastavovat zásady na úrovni jednotlivých kontejnerů. To umožňuje vytvářet nativně sítě mezi kontejnery na vrstvě L3, zajistit mikrosegmentaci mikroslužeb a získat kompletní přehled o zásadách pro sítě a zabezpečení pro tradiční i nové aplikace.

Edice řešení VMware NSX Data Center

Standard

Pro organizace vyžadující pružnost a automatizaci sítě.

Professional

Pro organizace, které vyžadují funkce edice Standard a navíc mikrosegmentaci a které mohou mít koncové body ve veřejných cloudech.

Advanced

Pro organizace, které vyžadují funkce edice Professional a navíc pokročilé služby pro sítě a zabezpečení spolu s integrací s rozsáhlým ekosystémem a které mohou mít více lokalit.

Enterprise Plus

Pro organizace, které potřebují nejpokročilejší funkce, jaké řešení NSX Data Center nabízí, a navíc chtějí získat přehled o sítích a provádět operace zabezpečení pomocí řešení vRealize Network Insight™ a dosáhnout mobility hybridního cloudu pomocí řešení NSX Hybrid Connect.

ROBO

Pro organizace, které chtějí virtualizovat sítě a zabezpečení pro aplikace ve vzdálených lokalitách nebo pobočkách.

	STANDARD	PROFESSIONAL	ADVANCED	ENTERPRISE PLUS	ROBO
NSX DATA CENTER[1]					
Distribuované přepínání a směrování	•	•	•	•	•[5]
Brána firewall poskytovaná řešením NSX Edge	•	•	•	•	•
Překlad adres NAT poskytovaný řešením NSX Edge	•	•	•	•	•
Softwarové přemostění na fyzické prostředí na vrstvě L2	•	•	•	•	
Dynamické směrování s ECMP (aktivní-aktivní)	•	•	•	•	•
Integrace s platformami pro správu cloudů[3]	•	•	•	•	•
Distribuované funkce brány firewall		•	•	•	•
Síť VPN (na vrstvách L2 a L3)		•	•	•	•
Integrace s řešením NSX Cloud[4]		•	•	•	•
Vyrovnávání zatížení pro řešení NSX Edge			•	•	•
Integrace s distribuovanými branami firewall (Active Directory, AirWatch® a vkládání služeb od třetích stran)			•	•	•
Správce aplikačních pravidel			•	•	•
Sítě a zabezpečení pro kontejnery			•	•	
Sítě a zabezpečení ve více lokalitách			•	•	
Integrace s hardwarovými branami			•	•	
Monitorování koncových bodů				•	
Mikrosegmentace zohledňující kontext (identifikace aplikací, RDSH)				•	
+vREALIZE NETWORK INSIGHT ADVANCED[2]					
Přehled o přenosech (IPFIX) a monitorování sítě				•	
Plánování a správa brány firewall				•	
Provoz a řešení problémů pro řešení NSX				•	
+NSX HYBRID CONNECT ADVANCED[2]					
Migrace rozsáhlých pracovních zatížení				•	
Optimalizace sítě WAN pro migraci pracovních zatížení				•	
Správa provozu a zatížení při využívání více spojení současně				•	

[1] Podrobný popis funkcí a nejnovější informace najdete v článcích znalostní báze Knowledge Base k řešením NSX Data Center for vSphere a NSX-T™ Data Center.

[2] Součástí edice NSX Data Center Enterprise Plus jsou plné verze řešení vRealize Network Insight Advanced a NSX Hybrid Connect Advanced.

[3] Integrace jen na vrstvách L2 a L3 a s řešením NSX Edge. Neumožňuje využívat skupiny zabezpečení.

[4] Pro pracovní zatížení ve veřejném cloudu je zapotřebí předplatné řešení NSX Cloud.

[5] Pouze přepínání, s využitím sítí VLAN.

vmware®

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

Č. položky: 169815wf-q3fy19-sddc-lnch-ds-nsx-dtactr-updt-a4
8/18