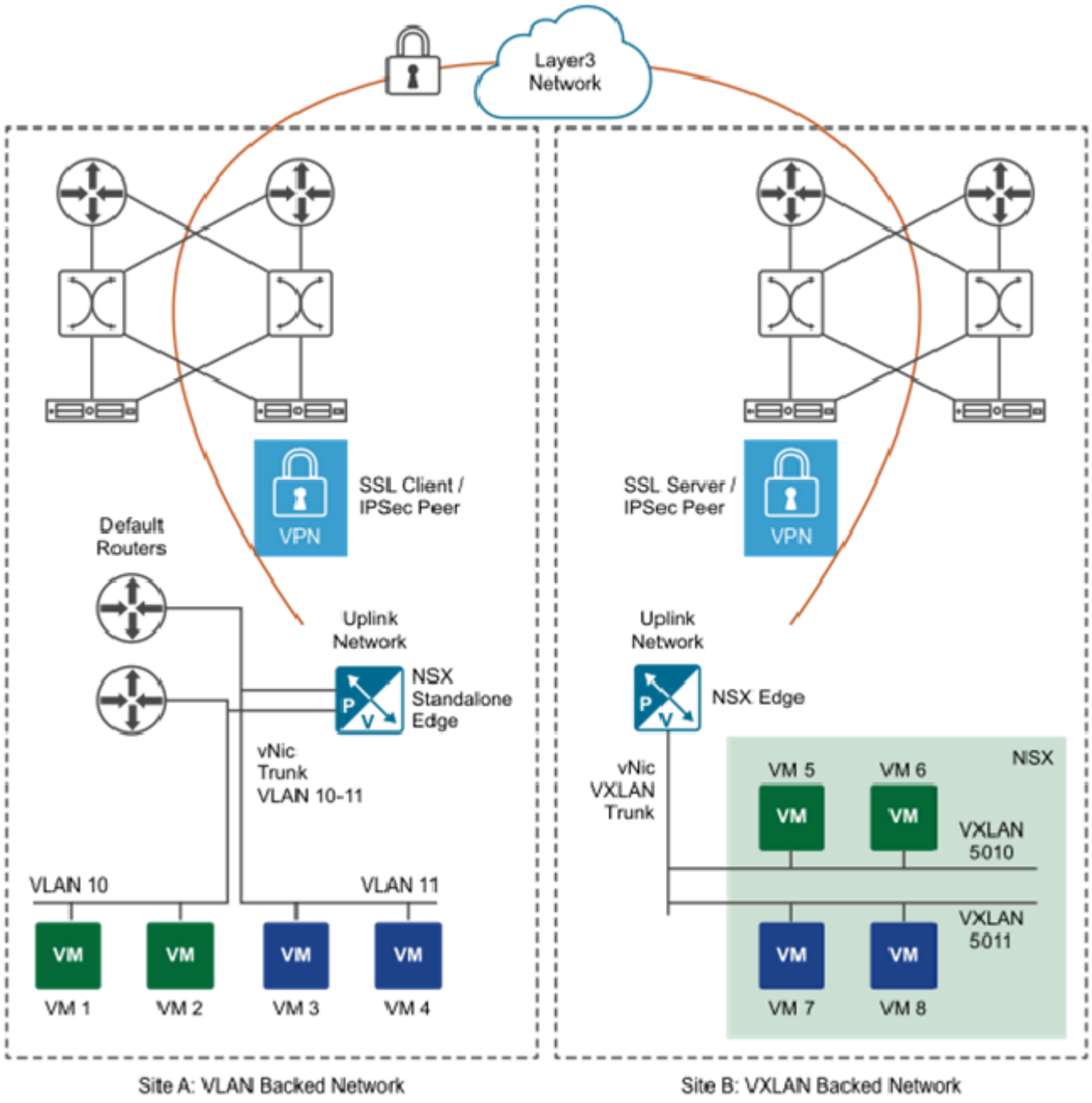
VMware NSX L2 VPN alebo Ako si ponechať IP adresu

V digitálnej dobe 21. storočia čoraz viac spoločností outsourcuje svoje IT riešenia a systémy k rôznym poskytovateľom na IT trhu ako súčasť znižovania nákladov. Aj keď v poslednom čase pozorujeme značný rozmach verejných cloudov, zákazníci požadujú nielen hostovanie IT riešení, ale majú záujem aj o ich správu.

Pri takomto prechode možno vybudovať systémy „from scratch“ s prípadnou migráciou dát alebo migrovať tieto systémy a aplikácie bežiace na fyzických alebo virtuálnych serveroch „as is“. Existuje mnoho technológií umožňujúcich túto migráciu systémov, ale čo ak je požiadavka ponechať originálne IP adresy?

Na prvý pohľad sa to môže zdať banálne, no pri definovaní migračného postupu to už také jednoduché nemusí byť. Problém spočíva v tom, že počas migrácie nemôžeme používať dve rôzne siete na úrovni Layer 3 modelu OSI bez toho, aby nedošlo k IP alebo routing konfliktu. Existuje možnosť migrovať všetky systémy súčasne a následne siete prepnúť, no takýto prístup „big bang“ má svoje nevýhody, napríklad dostupnosť systémov počas migrácie. Pri vyššom počte systémov je preto tento prístup prakticky nepoužiteľný.



Obr. 1 Sprístupnenie non-NSX lokality založenej na sieti VLAN do lokality NSX založenej na sieti VxLAN pomocou L2 VPN (zdroj: vmware.com)

Migráciu môže uľahčiť technológia od spoločnosti VMware, nazývaná NSX L2 VPN. Je to spojenie dvoch sietí cez heterogénne prostredie internetu alebo WAN na úrovni druhej

vrstvy modelu OSI. NSX je v podstate virtuálny server poskytujúci virtuálne sieťové služby, ako napríklad definovanie virtuálnych sietí (tzv. VxLANs), firewall, IPSec VPN, SSL VPN, load balancing a službu L2 VPN.

Už názov služby indikuje, že ide o sprístupnenie existujúcej siete na úrovni Layer 2 modelu OSI z lokality, kde je táto sieť definovaná, do cieľového dátového centra, kde má byť táto sieť dostupná. Konkrétnejšie VLAN A, definovaná na firewalle či routeri, bude sprístupnená cez internet alebo WAN do VxLAN B, ktorá je definovaná na NSX serveri. Sám L2 VPN tunel je vytvorený medzi NSX klientom (standalone appliance) spusteným v zdrojovej lokalite a NSX serverom v cieľovej lokalite. NSX klient inicializuje spojenie s NSX serverom na úrovni protokolu HTTP, kde sa pri následnej konfigurácii nadefinuje, ktoré konkrétne siete majú byť sprístupnené v cieľovej lokalite. Takto vytvorený tunel potom umožní priamu komunikáciu medzi zariadeniami, ktoré sú pripojené – či už do VLANov v zdrojovej, alebo VxLANov v cieľovej lokalite. Platí, že jedna VLAN je prepojená do jednej VxLAN. Iba na tejto úrovni možno uvažovať o priamej komunikácii na úrovni L2. Pri konfigurácii možno migrovať systémy postupne a ponechať im pôvodnú IP adresu po celý čas migrácie, až kým budú všetky systémy zmigrované, zdrojová sieť deaktivovaná a cieľová sieť sa stane hlavnou a jedinou s rozsahom IP pôvodnej siete.

Čo sa týka reálneho využitia tejto technológie, skutočnosť, že vytvorený L2 VPN tunel využíva internet, prípadne WAN, geografická vzdialenosť medzi zdrojovou a cieľovou lokalitou, ako aj limity nižších sieťových vrstiev určujú rýchlosť aj dostupnosť služby. Do verzie NSX 6.4.2 bola možnosť vytvoriť službu L2 VPN len ako tunel SSL, čo v praxi znamenalo, že všetka komunikácia v rámci jednej služby L2 VPN dokázala využiť potenciál iba jedného spojenia TCP/IP, čo môže byť limitujúce. Nedostatok bol odstránený vo verzii 6.4.2 a

vyššie, kde službu L2 VPN možno vytvoriť ako tunel IPSec.

Článok pripravil: ***Michal Kentoš***