

Virtualizace sít'ových prvků

Martin Pustka

Martin.Pustka@vsb.cz

EUROPEN, Herbertov, 11.-14.května 2014

O čem se budeme bavit...

- o virtualizaci síťových prvků provozovaných jako VM v virtualizačních infrastrukturách
- o tom, na co myslet a jaké dodržovat zásady při virtualizaci síťových prvků a služeb
- předpokládána je základní znalost poč. sítí

Základní pojmy

Virtualizační infrastruktury

- VMware vSphere, KVM, Hyper-V, XEN

Virtuální (virtualizovaný) systém

- virtuální server, směrovač

Virtuální (virtualizované) infrastruktury

- skupiny virtuálních systémů (servery, směrovače + servery)

Výhody - proč virtualizovat

- škálovatelnost technických prostředků
 - CPU, RAM, síťové pásmo lze navyšovat
 - změna technických kapacit nemusí znamenat výpadek virtualizovaného prvku, popř. je velmi krátký
- stabilita provozu
 - HA může zajišťovat také VI
 - využívání redundantních fyzických infrastruktur (sítě, živé migrace,...)

Výhody - proč virtualizovat

- snadná údržba a aktualizace
 - snapshoty
 - rychlé, vzdálené přepojování
- snadná obměna fyzického HW
 - vlastnost VI
 - s využitím živých migrací bez výpadku aplikace

Výhody - proč virtualizovat

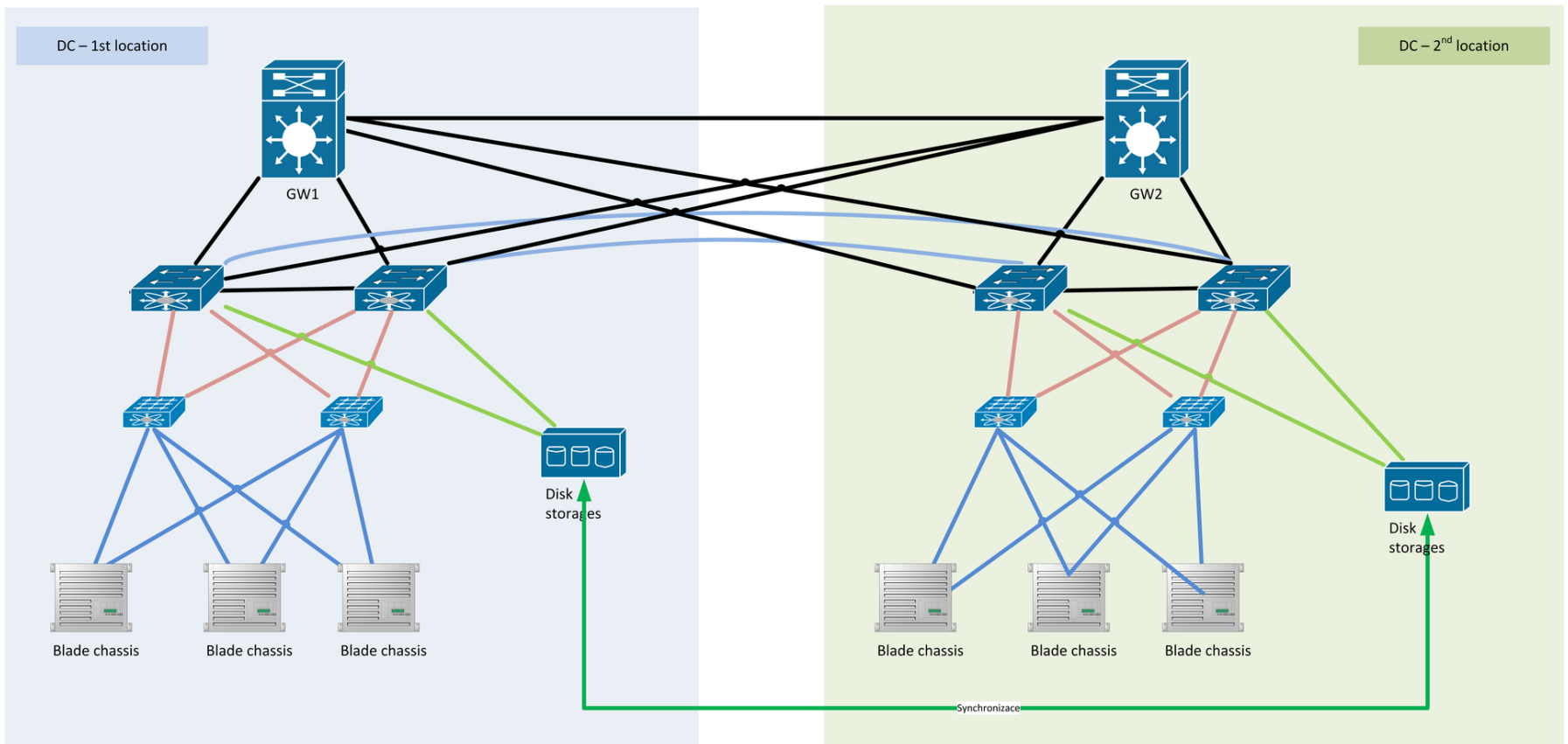
- flexibilní síťová infrastruktura
 - navyšování kapacit propojení bez výpadku služby
 - přepojení vNICů lze řešit vzdáleně a jednoduše
- finanční úspory
 - mohou být menší investiční náklady
 - menší náklady na provoz

Nevýhody

- neakcelerovaný síťový provoz bez přímého přístupu k hardware
- obvykle menší maximální výkon než který poskytují specializovaná síťová zařízení
- virtuální síťový prvek je méně efektivní než dedikované síťové zařízení
- závislost na dalších prvcích a jejich správné funkci

Fyzická infrastruktura DC

Basic DC topology, VSB – Technical University of Ostrava



Podmínky virtualizace

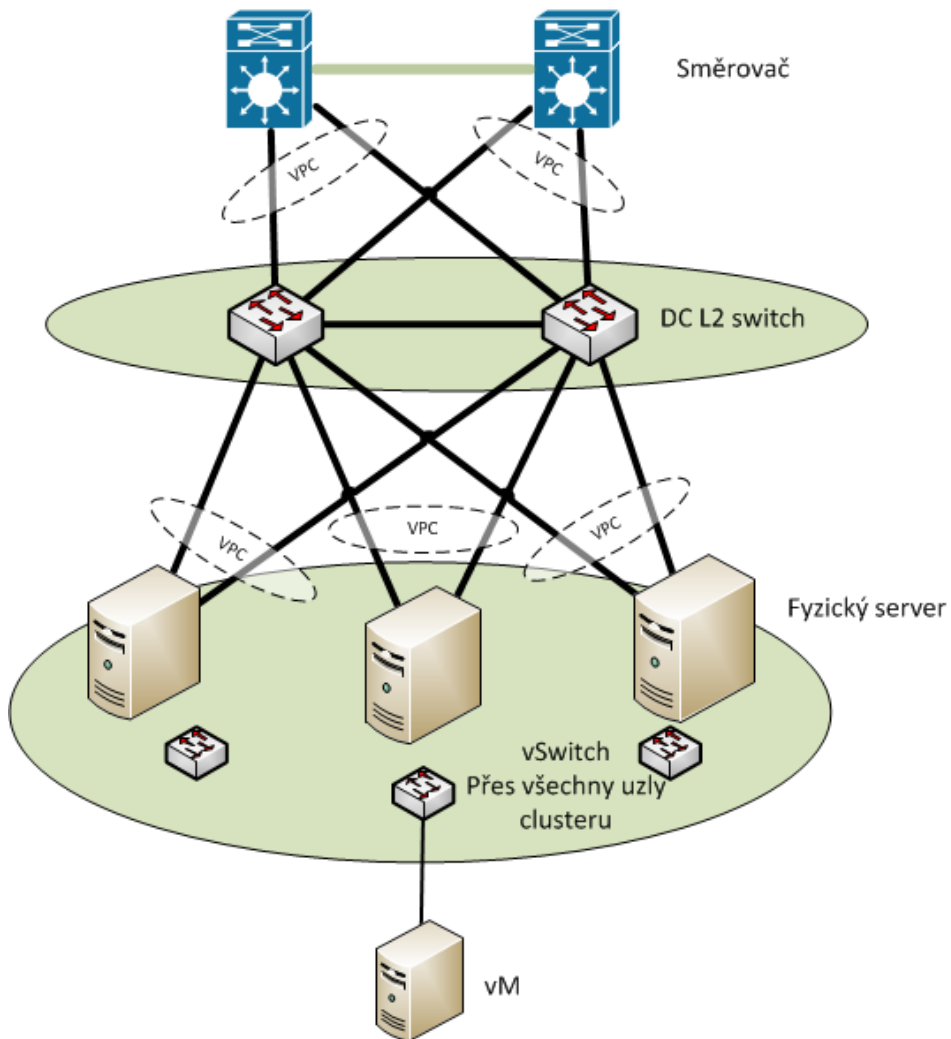
Minimální nutné podmínky virtualizace síťového prvku jsou:

1. Virtualizační infrastruktura nesmí záviset na virtuálním síťovém prvku a jeho správné funkci.
2. Správa virtualizační infrastruktury nesmí záviset na virtuálním síťovém prvku a jeho správné funkci.

Budování fyzické síťové infrastruktury

- cílem je mít dostatečné fyzické síťové kapacity, které lze bezvýpadkově rozšiřovat
- je vhodné zvažovat už 10GE technologie
- konvergovaná infrastruktura je výhodnější
- stavíme síť DC jednoduše jako L2 infrastrukturu

Sít'ové propojení VI

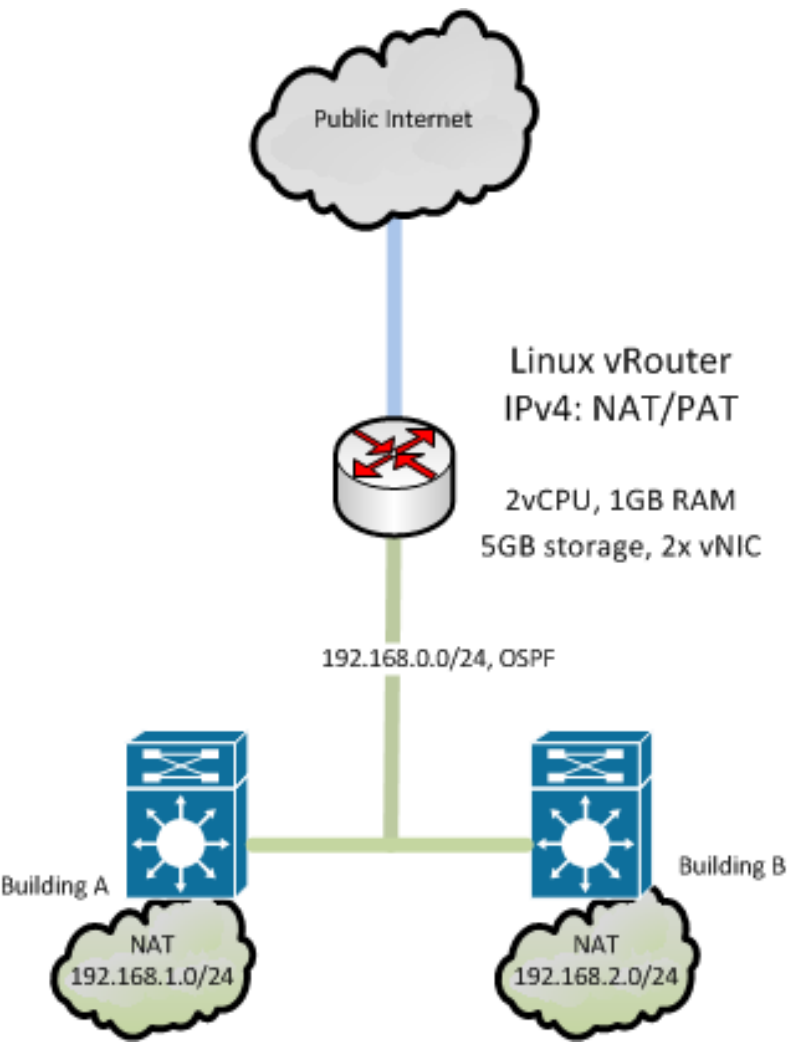


- redundance na každé z vrstev
 - směrovače
 - přepínače DC
 - virtualizační infrastruktura
- použití 10GE technologií
 - port-channel u 1GE může být zahlcen
 - režie pro živé migrace mezi fyzickými uzly - problém u 1GE
- využití stackování u DC přepínačů pro zvýšení redundance
- virtuální přepínače pro kontrolu vNICů

Služby vhodné pro virtualizaci

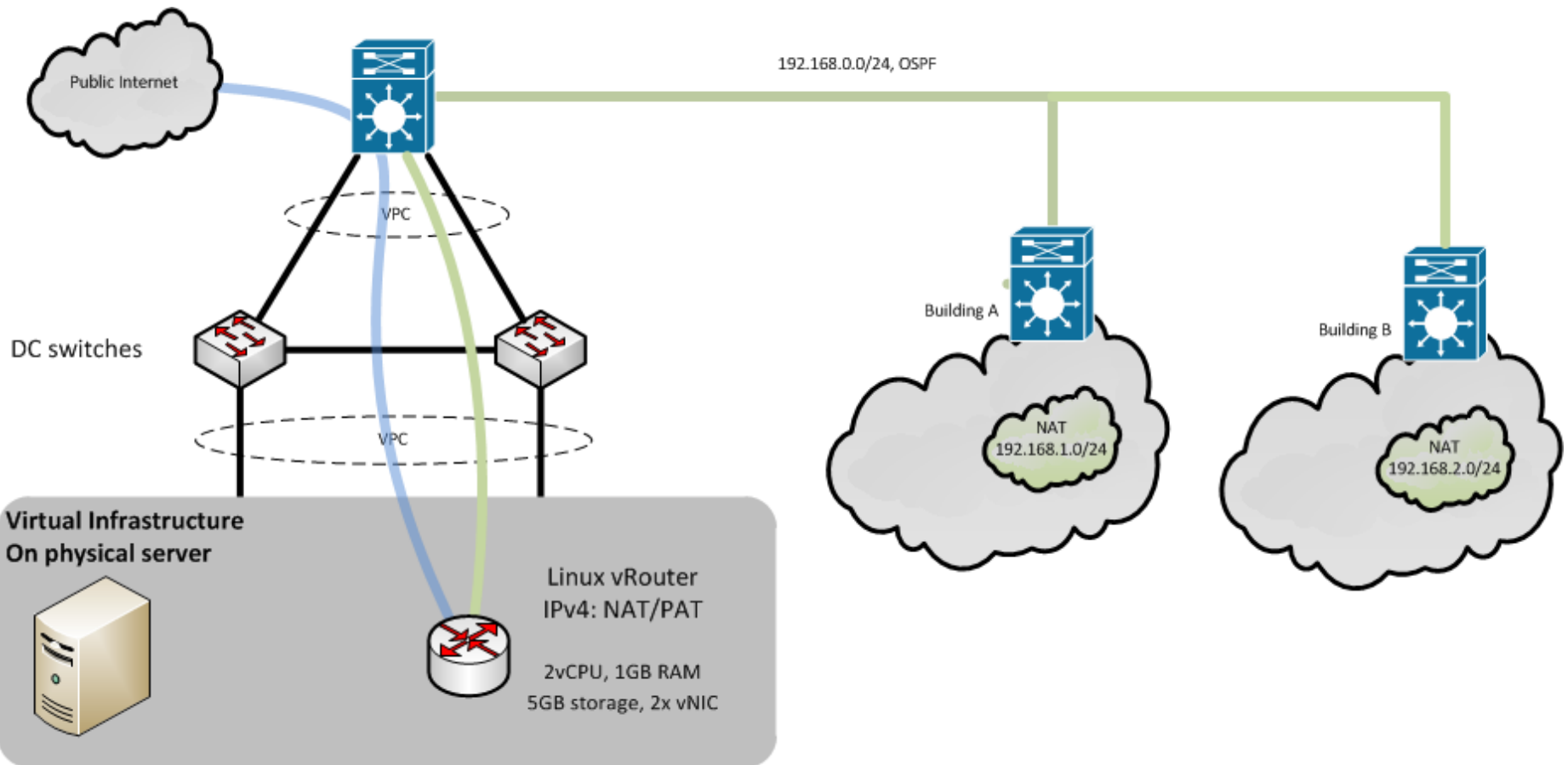
- jednoduché směrovače (i s funkcí NAT/PAT)
- VPN koncentrátoři pro uživatele i site-to-site spojení
- bezpečnostní prvky (např. IDS/IPS)
- směrovače nebo firewally virtuálních serverů
- BGP směrovače (RTBHR, route reflectory)
- prvky pro rozkládání provozu mezi virtuální systémy (load-balancery)
- ISATAP směrovače pro IPv6

NAT/PAT směrovače



- vRouter s Debian Linux
- dvě síťová rozhraní
- konzumuje malé kapacity
- OSPF
- v této konfiguraci odbavení účastníci MEJ
- směrování lokálních sítí na Catalyst6500 v separátní VRF instanci

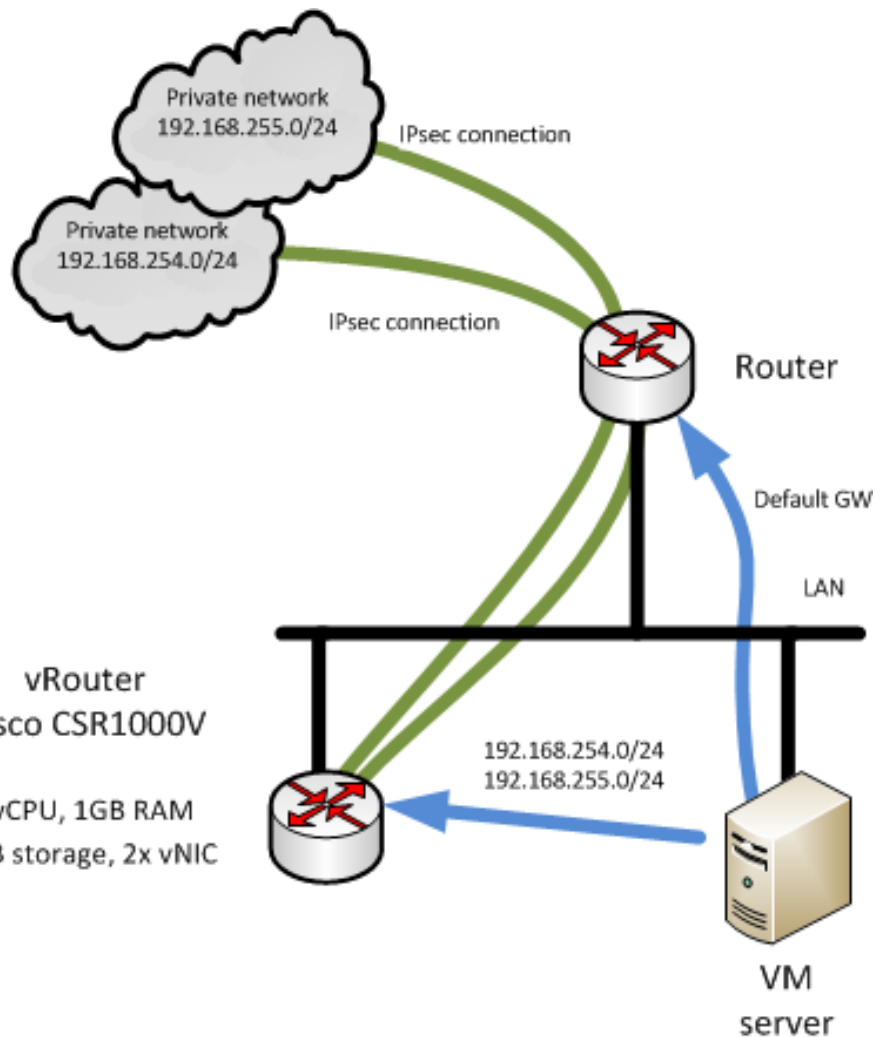
NAT/PAT směrovače



VPN koncentrátoři

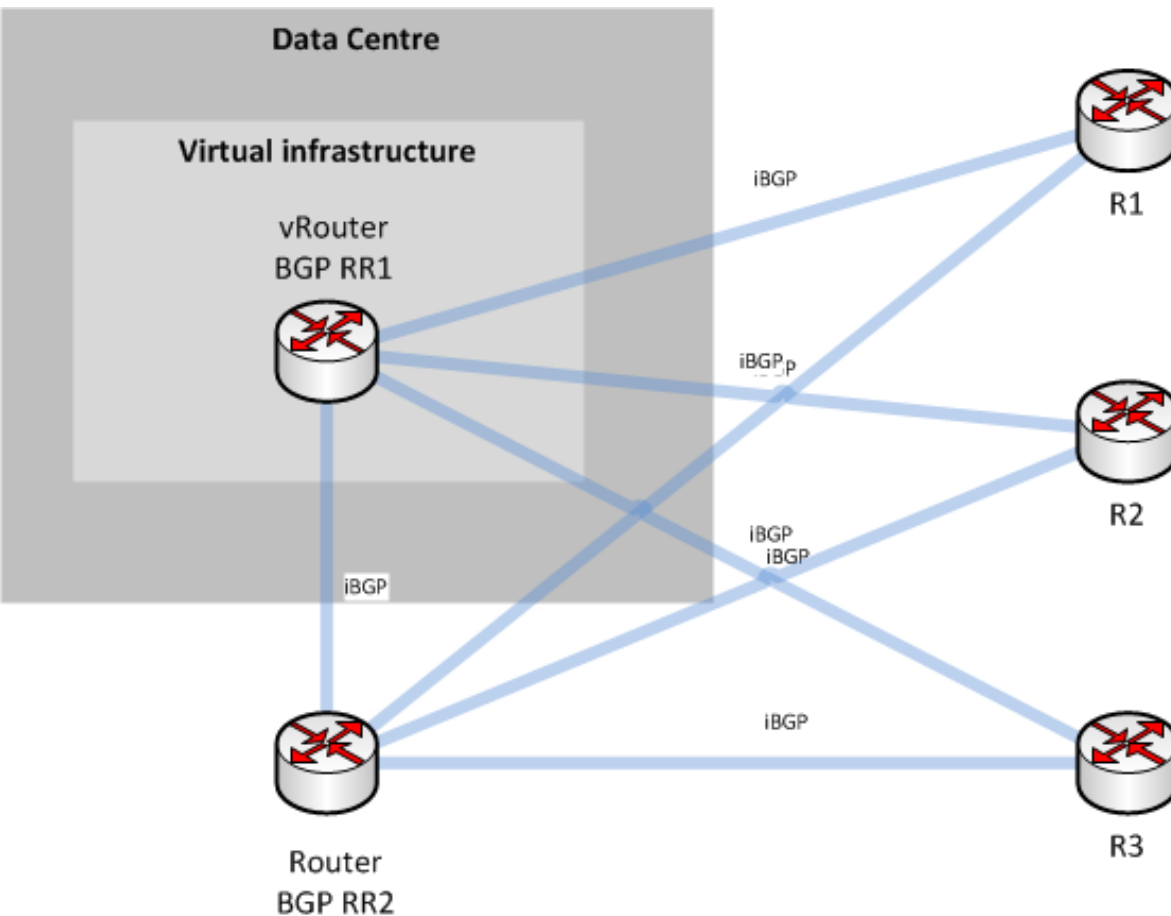
- náročné na CPU a RAM
 - kapacity, které VI poskytuje
- uživatelské vs. site-to-site spojení
- zvážit virtualizaci pokud jsou příliš velké datové toky

VPN tunely



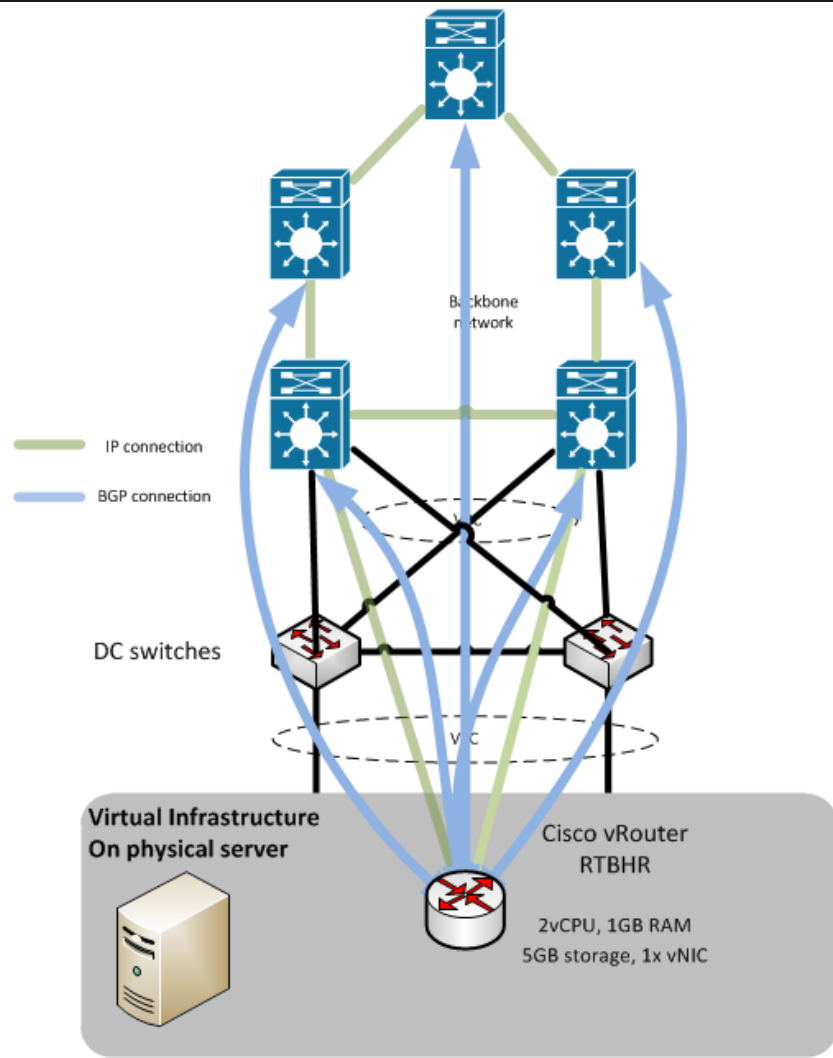
- službu VPN využívá více VM
- Internetový provoz přes fyzický směrovač
- zabezpečený provoz přes vRouter, který je licencovaný podle objemu provozu
- výhodou je jednotná správa přístupů

BGP route reflector



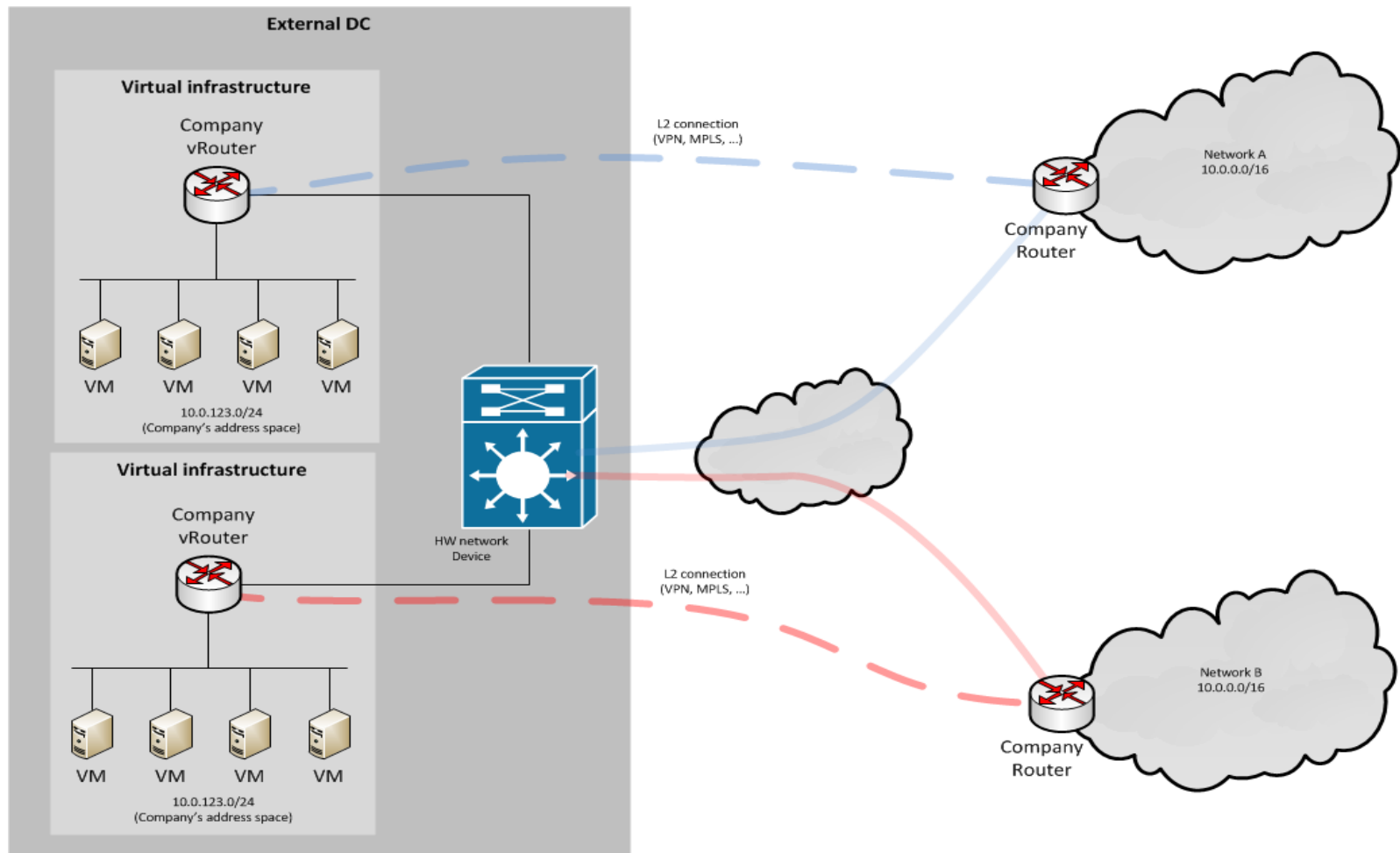
- min. dva BGP RR pro zajištění redundance
- pozor na splnění minimálních podmínek pro virtualizaci
- druhý RR jako fyzický nebo v jiné VI

RTBHR servery



- přes směrovač neprochází provoz
- jsou pouze distribuovány směrovací informace
- redundance řešeny na úrovni síťové infrastruktury DC
- při výpadku není ohrožen samotný provoz

Klasické směrovače IP provozu a propojení virt. infrastruktur



Doporučení

- Mějte strategii rozvoje síťové infrastruktury. Ujasněte si, které její části je vhodné virtualizovat, které prvky naopak pro virtualizaci vhodné nejsou.
- Nečekejte zásadní investiční úspory. výhodou bývá lepší flexibilita a škálovatelnost infrastruktury, úspory jsou zejména provozního charakteru (energie, prostor).
- Při virtualizaci dbejte na kompatibilitu s existující a provozovanou síťovou infrastrukturou, ale i s vaší virtualizační infrastrukturou.

Doporučení

- Mějte kvalitní, ale i jednoduchou síťovou infrastrukturu v rámci datového centra. Provoz virtuálních síťových prvků jde obvykle složitější cestou než u fyzických prvků, kde je propojení obvykle realizováno jedním fyzickým kabelem. Proto některé síťové problémy se mohou hůře ladit nebo dohledávat.
- Mějte k dispozici nástroje pro mirroring a monitoring provozu v rámci virtualizační infrastruktury.

Doporučení

- Nevirtualizujte takové části síťové infrastruktury, které jsou nezbytné pro její inicializaci nebo její běh.
- Podle stavu fyzické síťové infrastruktury můžete implementovat i takové aplikace, které vyžadují větší pásmo. Ujistěte se, popř. zajistěte, že tento provoz neomezí provoz ostatních systémů ve sdílené virtualizační infrastruktuře.

Závěr

Děkuji za pozornost...

... dotazy ?