

Hálózati szolgáltatások virtualizált környezetben

Workshop 2013. Sopron

Zeisel Tamás
Konzultáns rendszermérnök
Cisco Magyarország

Hálózati model változás

Fizikai → Virtualizált → Felhő

FIZIKAI INFRASTRUKTÚRA

- Egy alkalmazás/ Szerver
- Statikus
- Manuális üzemeltetés



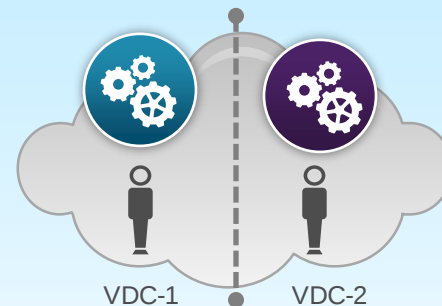
VIRTUALIZÁLT INFRASTRUKTÚRA

- Sok alkalmazás/ Szerver
- Mobilis
- Dinamikus üzemeltetés



FELHŐ INFRASTRUKTÚRA

- Több felhasználó/Server
- Rugalmas
- Automatikus, Skálázható



KONZISZTENS: Szabályrendszer, Jellemzők, Biztonság, Menedzsment

Nexus

7K/5K/3K/2K

WAAS, ASA, NAM, ACE

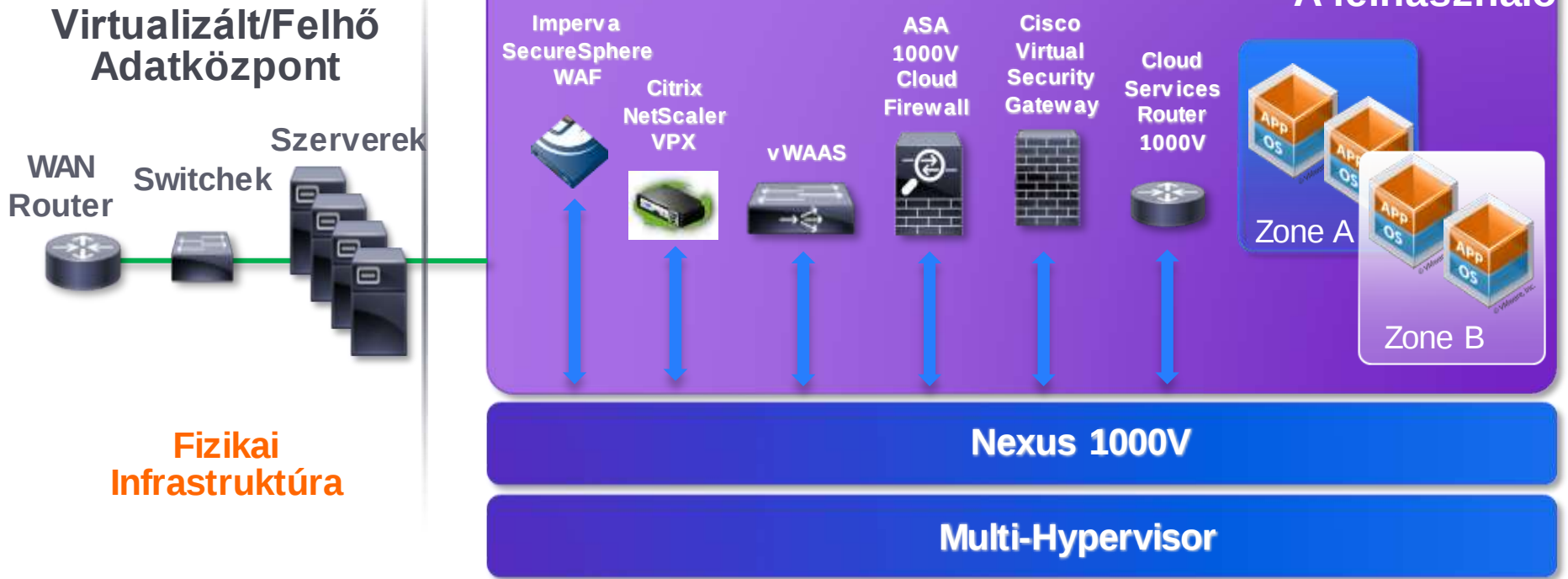
Nexus 1000V, VM-FEX

vWAAS, VSG, ASA1000V, Külső Alkalm.

* Virtual only

Cisco Virtualaizált hálózati szolgáltatások

Cloud Network Services



Nexus 1000V

- Elosztott switch
- NX-OS jellemzők

VSG

- VM-szintű kontroll
- Zone-based FW

ASA 1000V

- Edge firewall, VPN
- Protocol vizsgálat

vWAAS

- WAN optimalizálás
- Alkalmazás optimalizálás

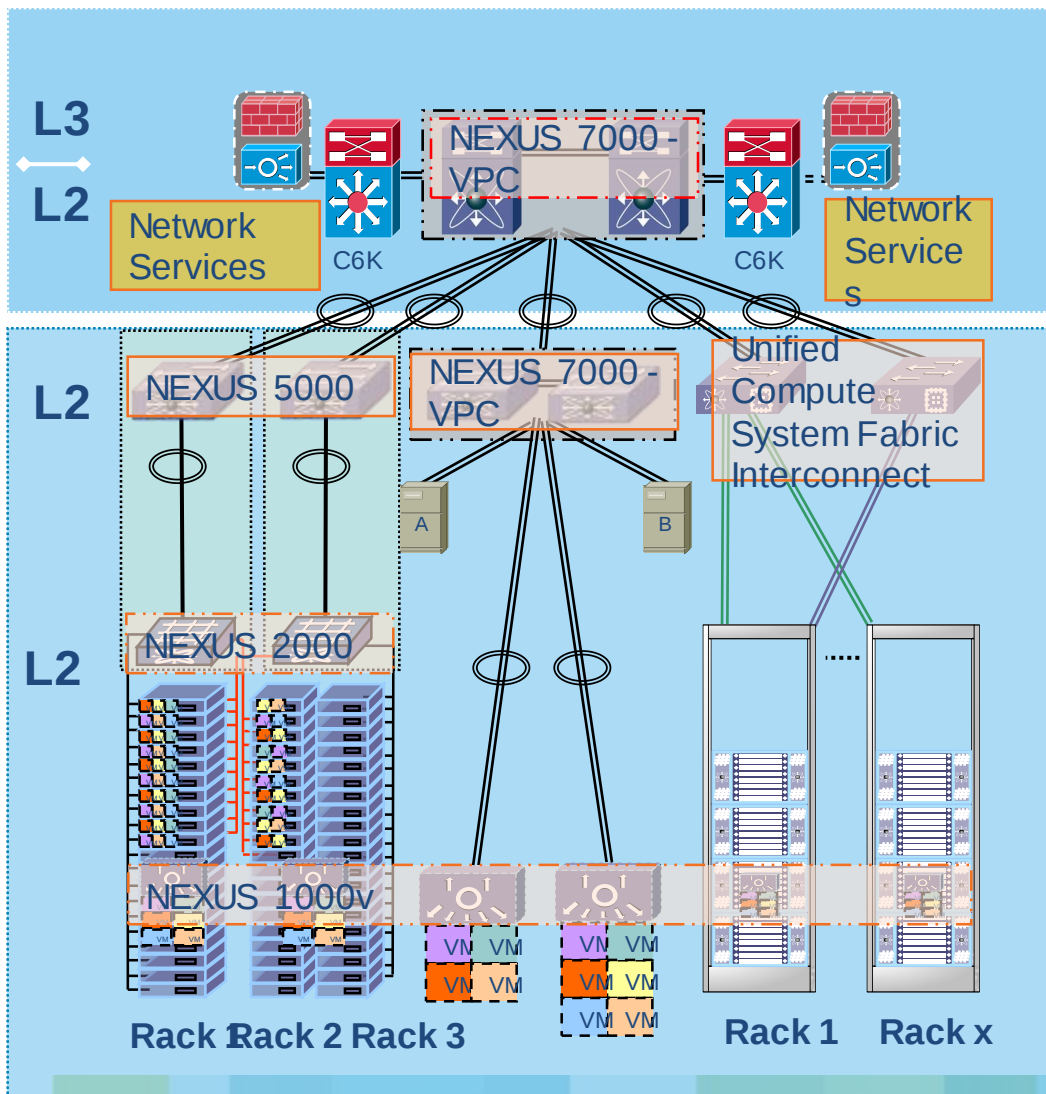
CSR 1000V (Cloud Router)

- WAN L3 gateway
- Routing és VPN

Ecosystem szolgáltatások

- Citrix NetScaler VPX virtual ADC
- Imperva Web App. Firewall

Virtuális szolgáltatások az adatközpontban



Aggregáció

- Tipikus L3/L2 határ.
- Fizikai hálózati szolgáltatások

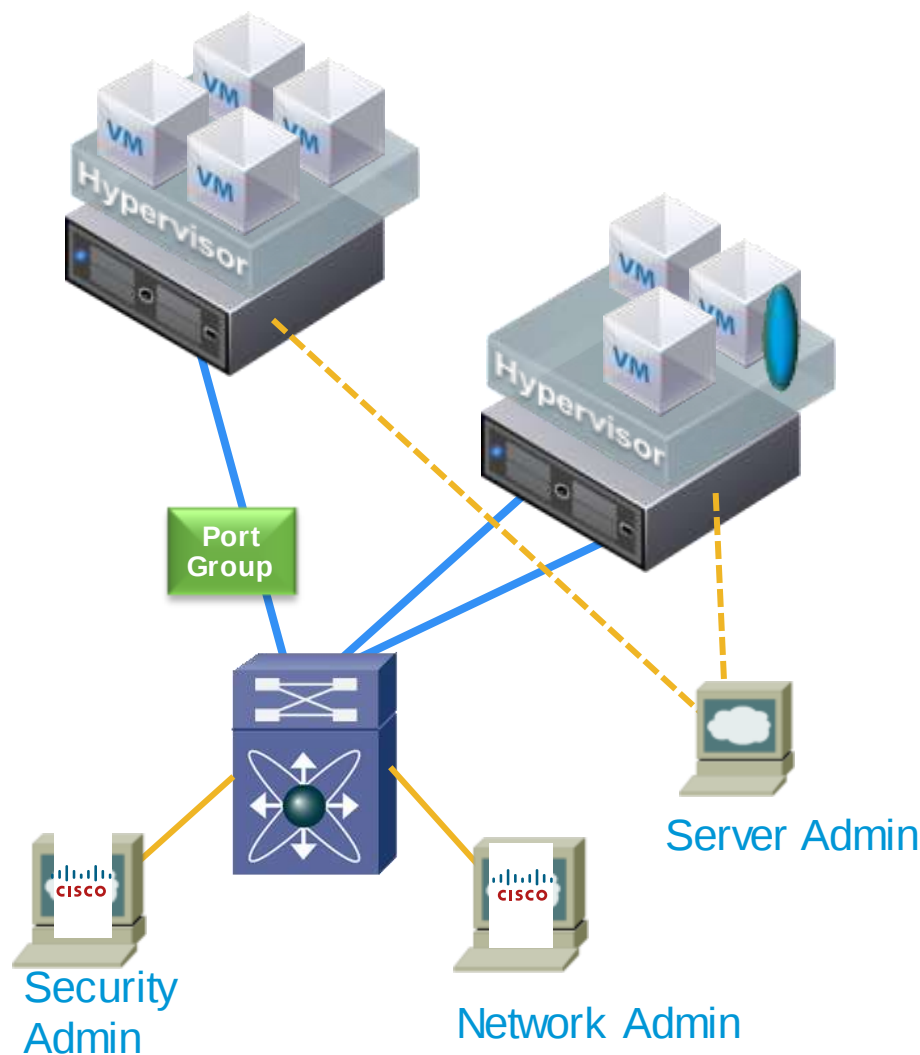
Egységes hozzáférés

- Adat/Tároló hálózati hozzáférés

Virtual hozzáférés

- Virtuális switchek
- Virtuális elosztott szolgáltatások

Szerver Virtualizálás hálózati követelményei



1. vMotion elmozdítja az egyes Vmeket a fizikai portok között
hálózati szabályrendszernek követnie kell a vMotion/Live Migration-t
2. Láthatóvá kell tenni és érvényre kell juttatni a hálózati/biztonsági szabályrendszert a lokálisan kapcsolt VM forgalomra
3. Felelősség megosztás

Cisco Virtual Network Link – VN-Link

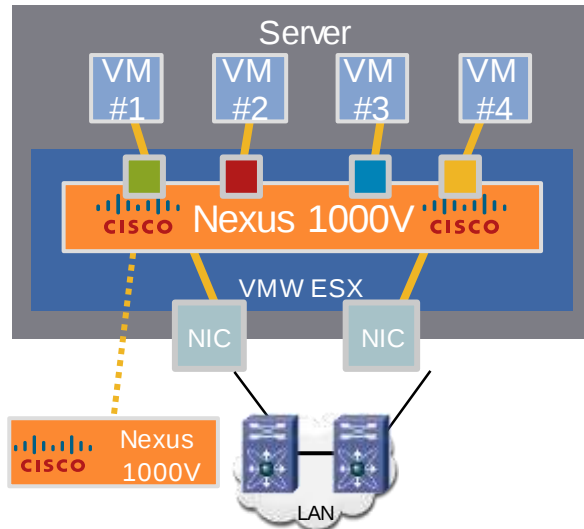
Hálózati Domén Virtualizáció

Szabály alapú
VM kapcsolódás

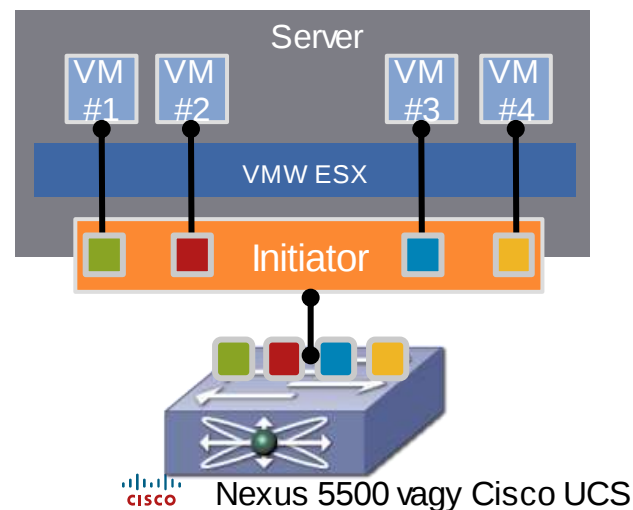
Hálózati és biztonsági
Szabályok mobilitása

Folyamatos működés

Cisco Nexus 1000V (Software alapú)

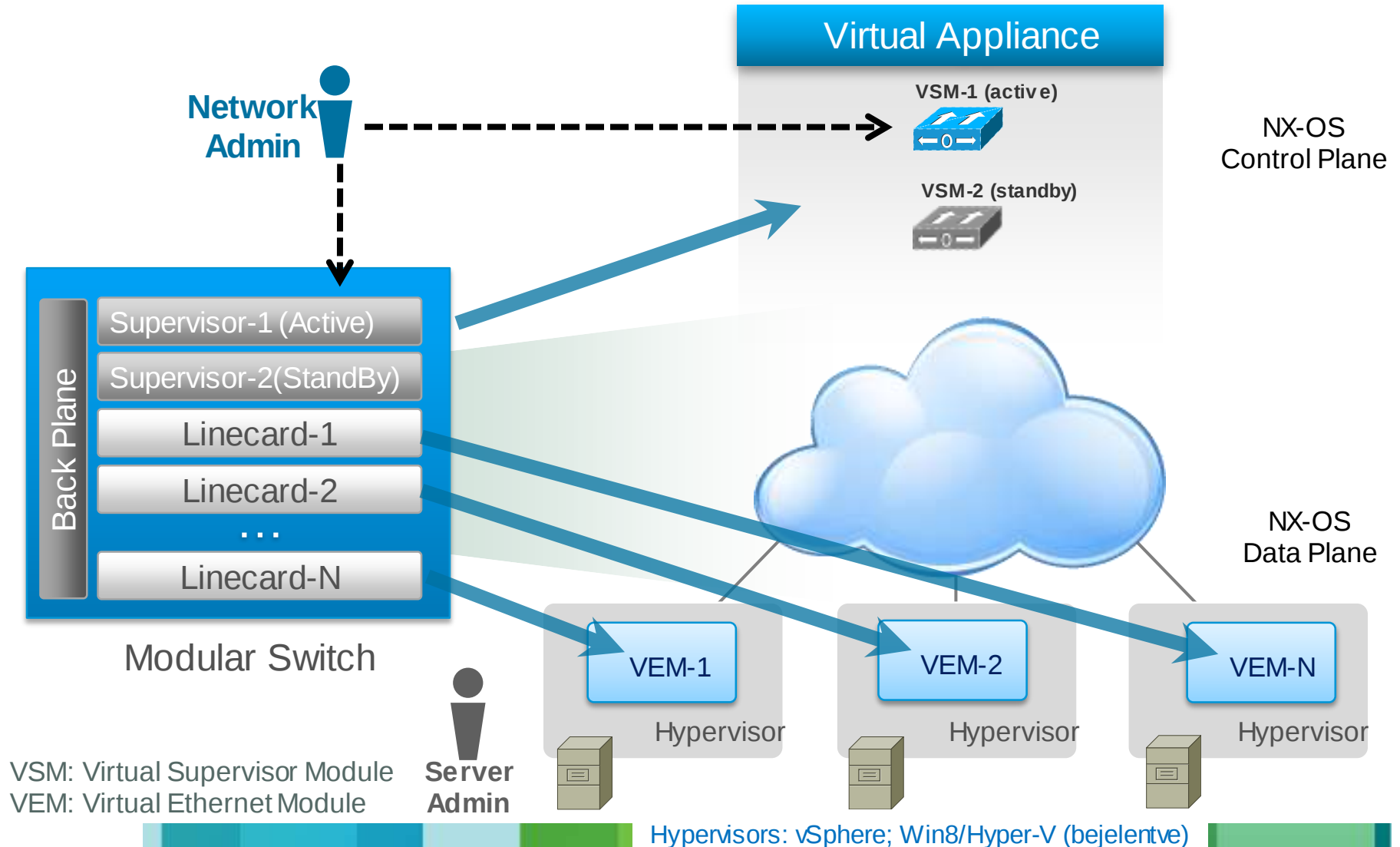


Nexus 5500, UCS VM-FEX (Hardware alapú)



Nexus 1000V Architektúra

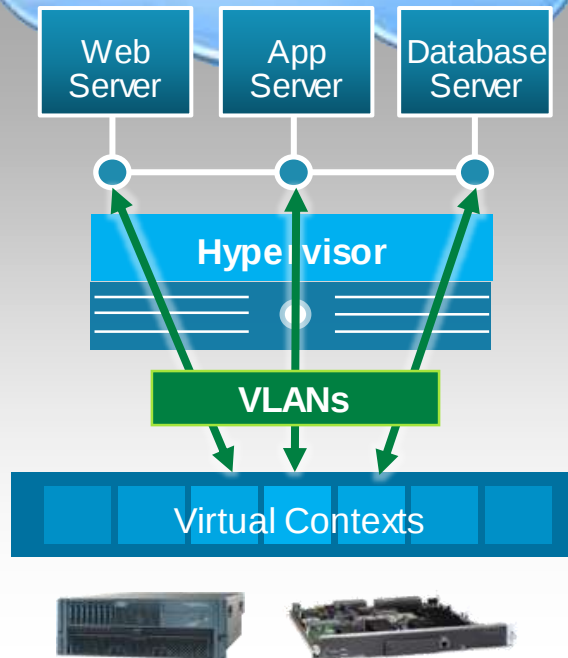
Fizikai világ leképzése a virtuálisra



Virtualizált/Felhő infrastruktúra környezetben

1

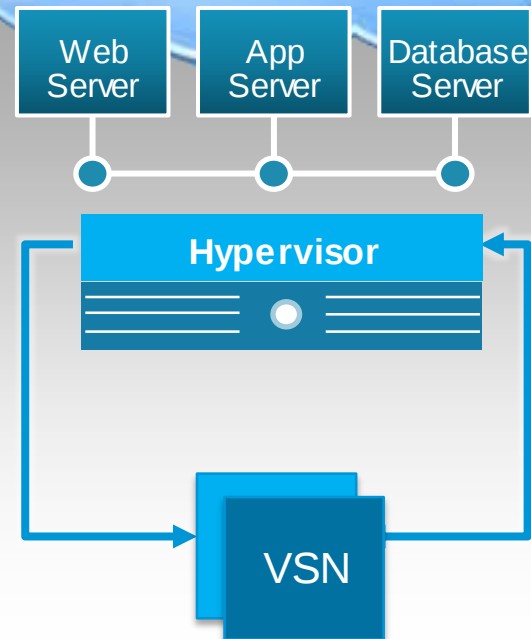
VM forgalmat rá kell irányítani
külső eszközre megfelelő
VLAN segítségével



Dedicated Service Nodes

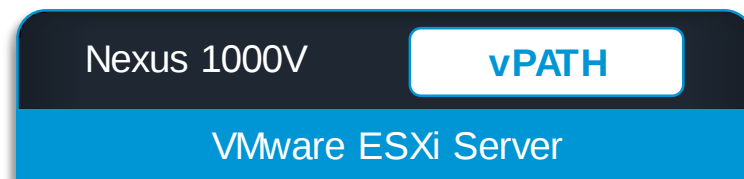
2

Hypervisor-alapú
virtuális hálózati szolgáltatás



Virtual Service Nodes

Mi a vPATH ?



- Nexus1000v Virtual Ethernet Module VEM-ba integrált intelligencia
- vPath fő funkciói:
 - Intelligens forgalom átirányítás virtuális hálózati szolgáltatások felé (VSG/ASA1000v, vWAAS...)
 - ARP alapú ellenőrzés
 - Flow entry table kezelés (optimalizálás)
- VPATH forgalom átirányítás N1000V service VLAN-ján keresztül

Biztonsági megoldások lehetőségei



FWSM



Belső Biztonság

- Belső hálózat szegmentálása
- VLANokhoz rendelt szabályrendszer
- Alkalmazás szintű vizsgálat
- Virtuális kontextek



ASA 55xx



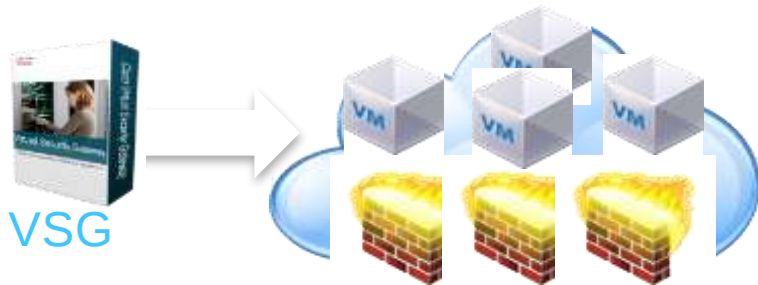
ASA 55xx



Internet Biztonság

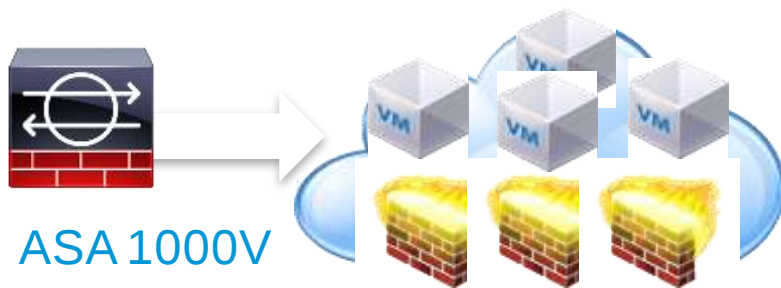
- Külső forgalom szűrés
- Alkalmazás protokoll támogatás
- VPN hozzáférés, betörésvédelem

Biztonsági megoldások lehetőségei



Virtual Security

- VM zonákhoz rendelt szabályrendszer
- Dinamikus skálázható
- VM tartalom alapú vezérlés



Virtual Security

- Stateful Firewall
- Protokoll vizsgálat
- VM Külső kapcsolódás

Biztonsági megoldások Virtuális környezetben

Zóna-alapú/állapot követő Tűzfalak

Virtual Security Gateway (VSG)



VM szintű Biztonság

VM attributum szerinti védelmi szabályok

Zóna-alapú védelem

Biztonsági zóna kialakítsa (DMZ)

Fejlett rugalmas Architektúra

Hatékony, skálázható model

ASA 1000V Cloud Firewall



Külső védelem

Protokol vizsgálat, NAT, VPN

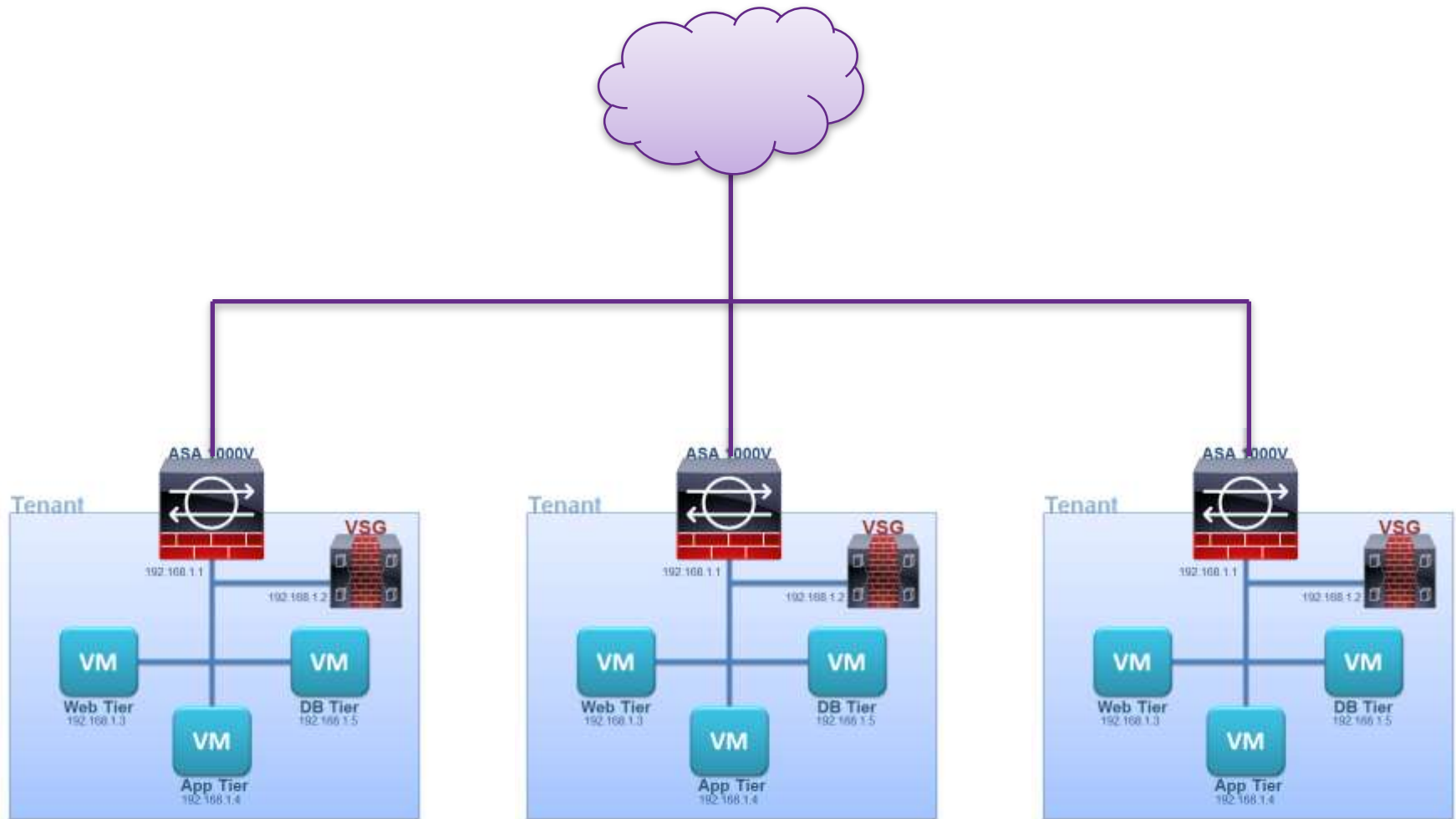
Többfelhasználós környezet

Gyors felhasználó szegmentálás

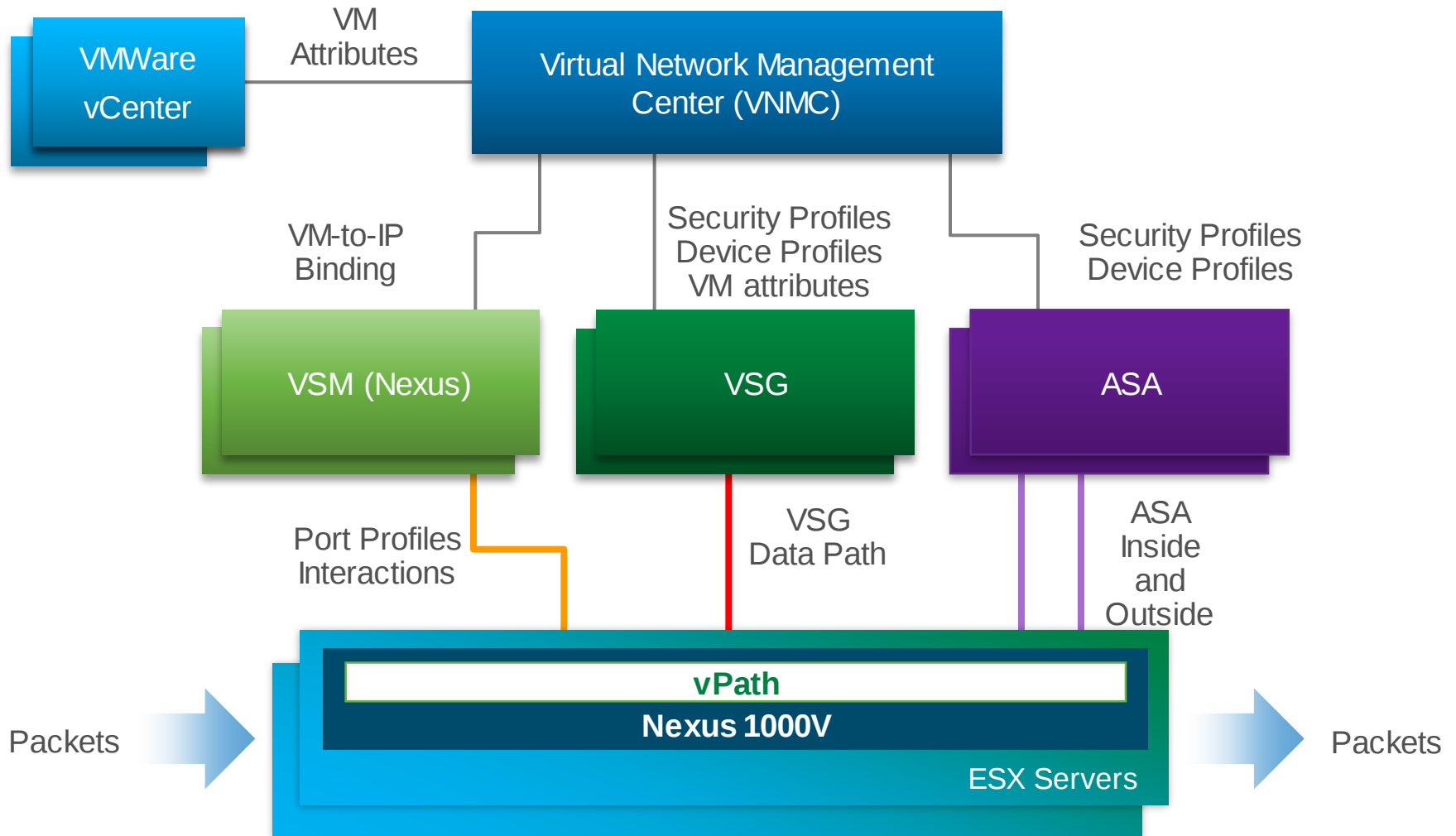
Megszokott ASA platform

Azonos ASA kód

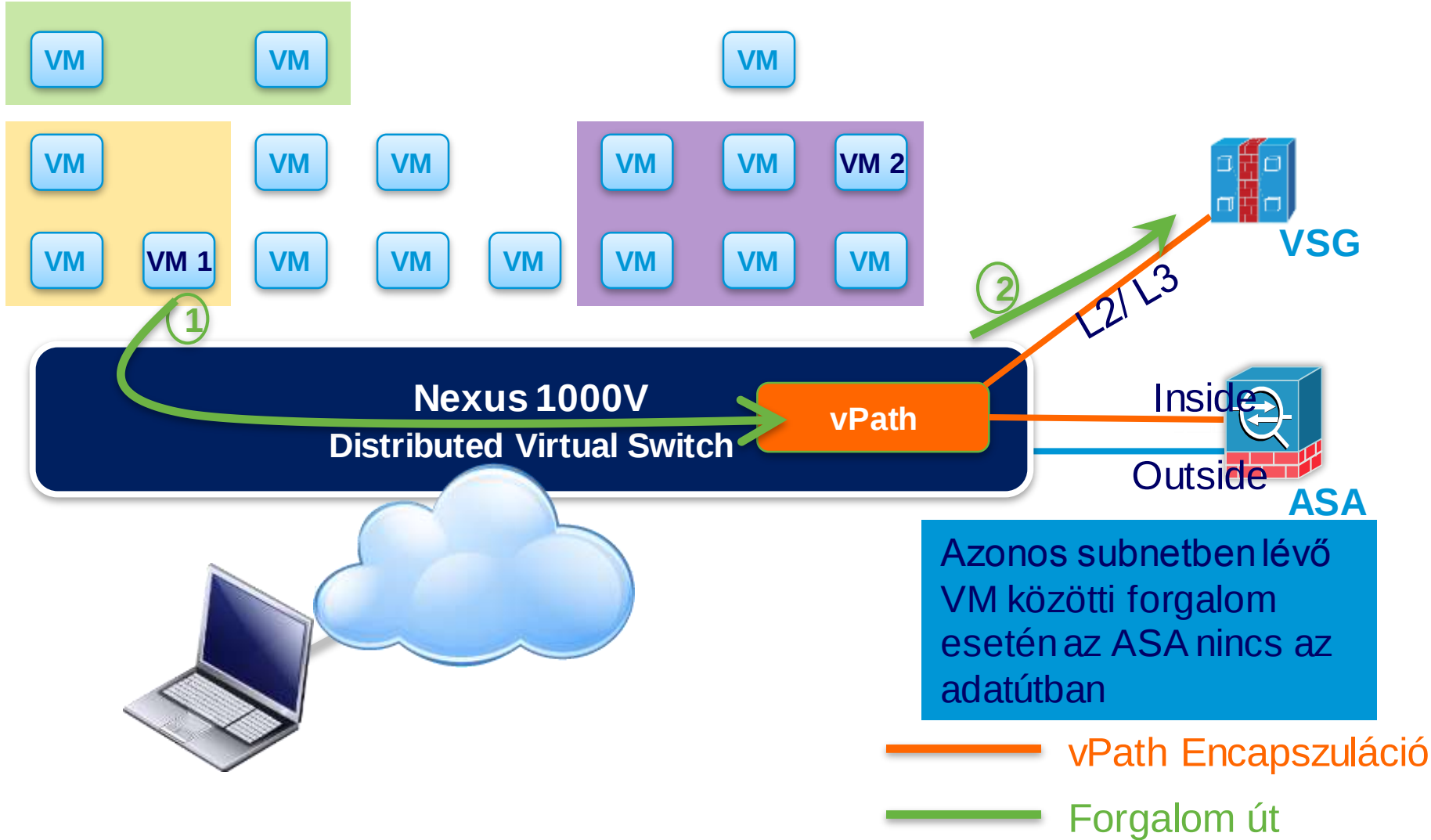
Többfelhasználós környezet



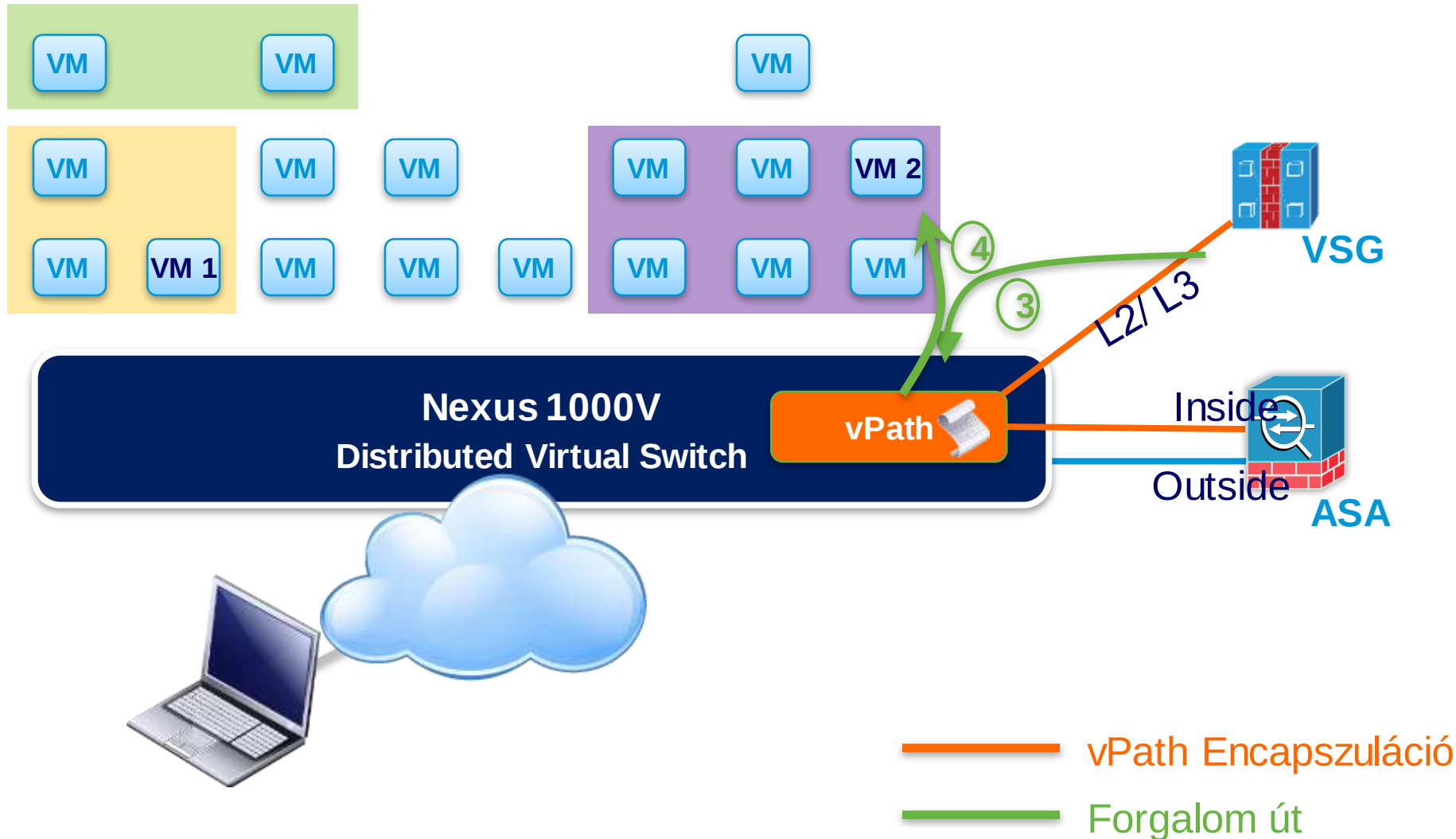
Rendszer architektúra



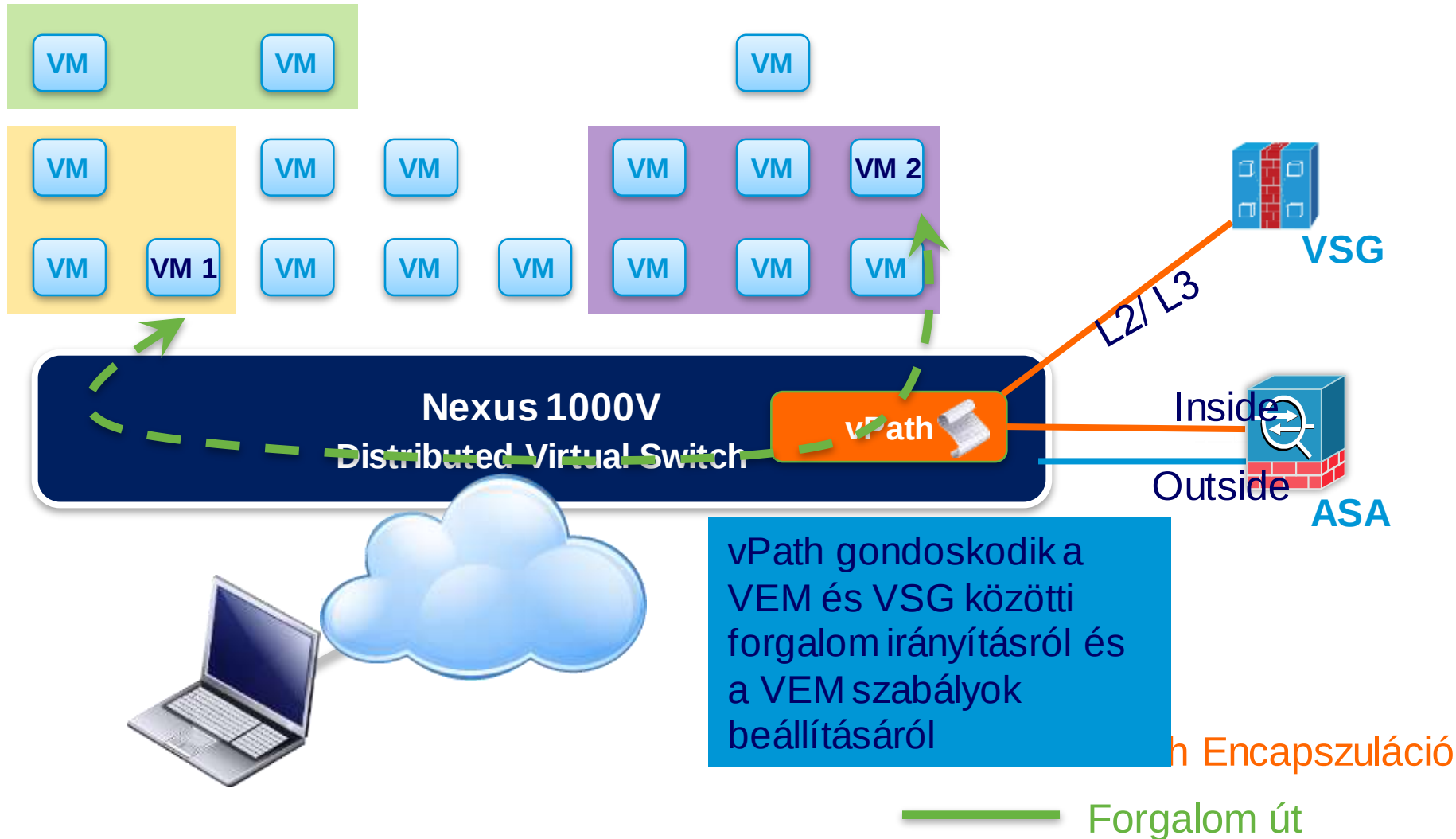
VM-VM forgalom



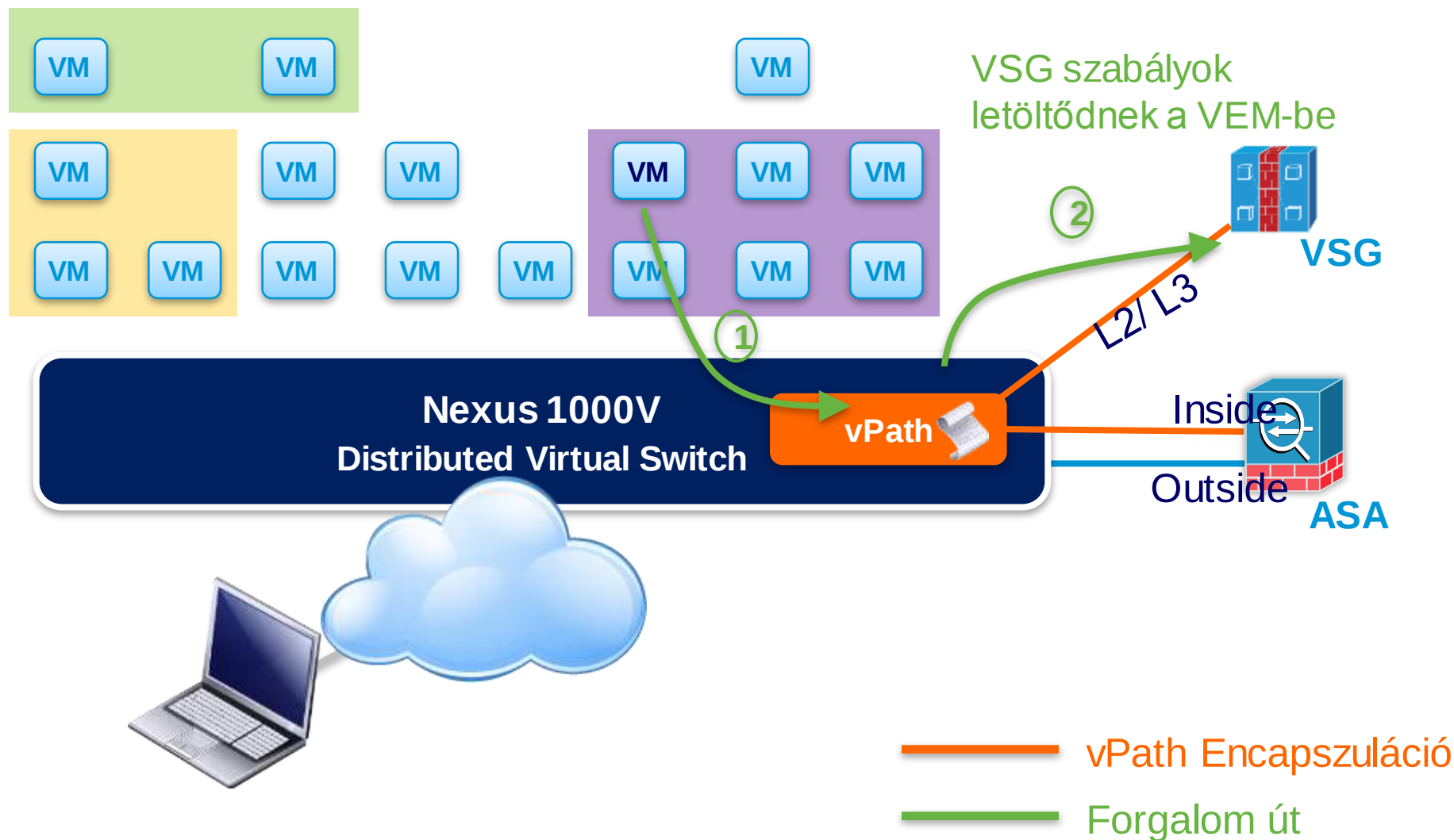
VM-VM forgalom



VM-VM forgalom

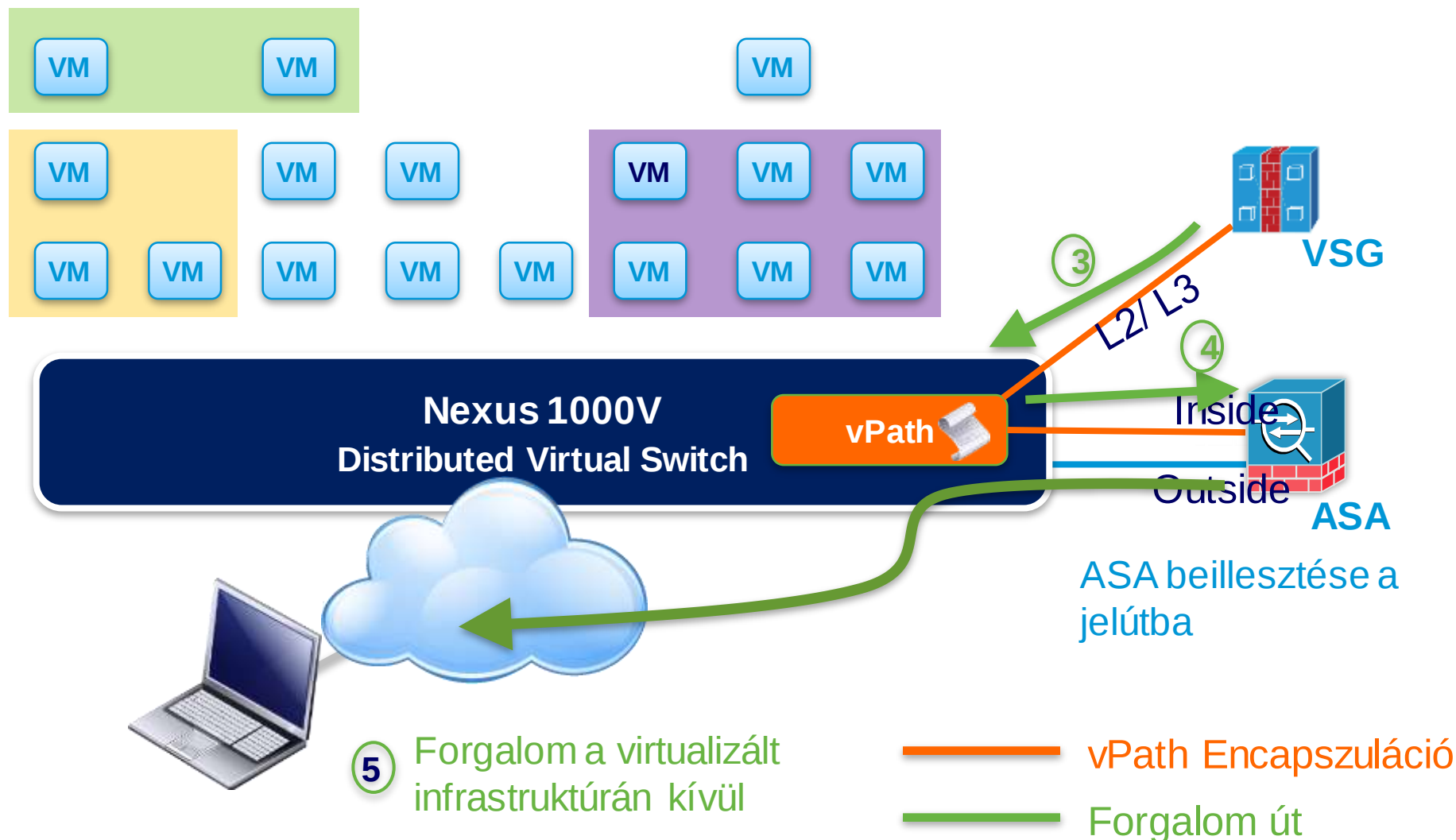


Szolgáltatások láncolása vPath 2.0



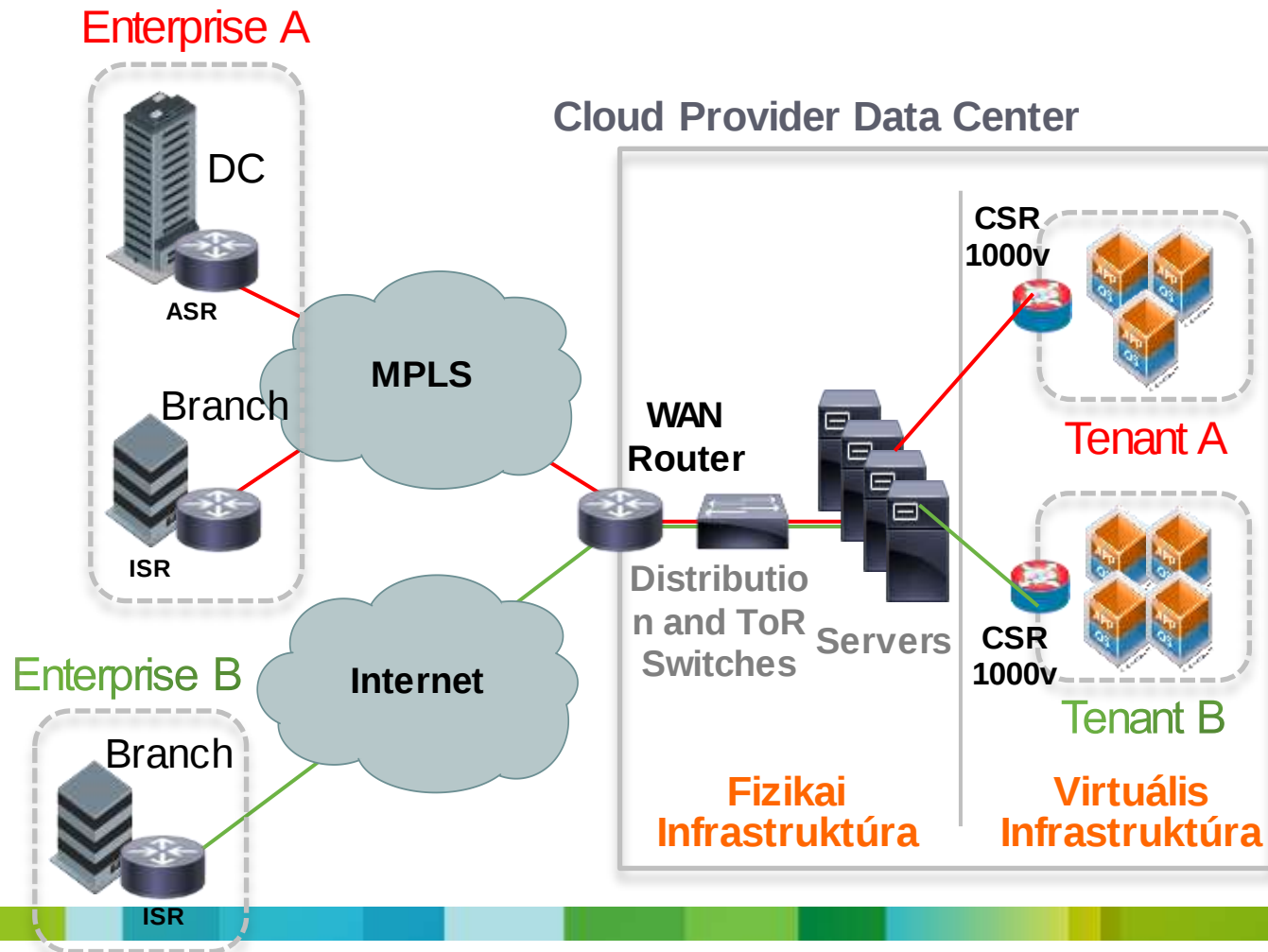
Szolgáltatások láncolása

vPath 2.0



CSR 1000v Felhő szolgáltatás biztosítása

Single Tenant WAN Gateway for Shared Infrastructure Environments



Rugalmas

- Hardware független
- Virt. Eth. portok

Programozható

RESTful API

- Konfigurálás
- Monitorozás

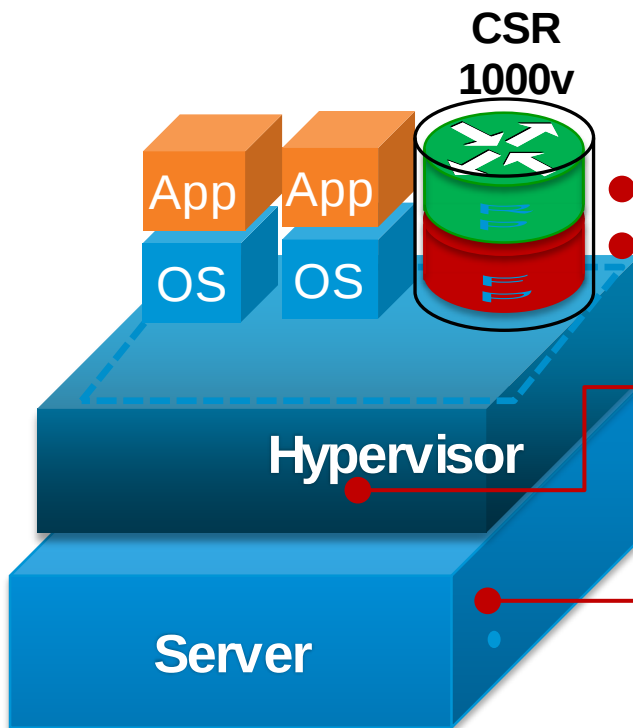
Bővíthető

- Kapacitás bővíthető
- Clone-ozható

CSR 1000v

- Cisco IOS XE Software Virtualizált változatban

Cisco IOS XE Cloud Edition



Cisco IOS XE szelektált feature set
Virtual Route Processor (RP)

Virtual Forwarding Processor (FP)

Egy felhasználóra optimalizált

Hypervisor függő

Szerver függő

Nexus 1010 / Nexus 1100

- Dedikált eszköz alapvetően VSM számára
- Virtual service blade support (VSB)
 - 6 per 1010 pair / 1110S pair
 - 10 per 1010X pair / 1110X pair
 - Jelenleg támogatott: VSM, VSG, vNAM, DCNM



- Nexus 1100 sorozat UCS C220M3 szerveren alapul



Thank you.

