Virtualios infrastruktūros sauga

Tinklai ir tinklų sauga virtualioje infrastruktūroje

Virtualus tinklas

Kompiuterių tinklas virtualioje infrastruktūroje kuriamas naudojant fizinius ir virtualius komponentus.

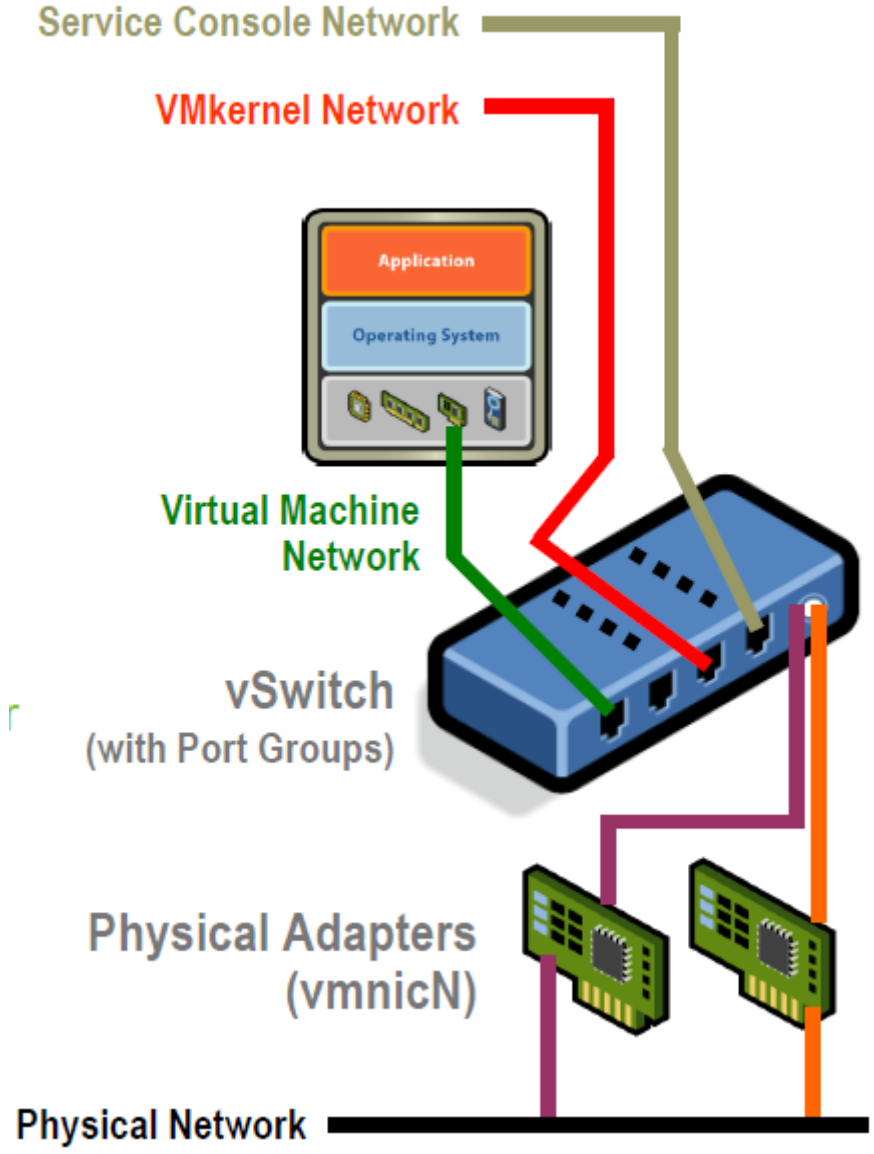
Fiziniai komponentai:

- Tinklo plokštės
- Komutatoriai
- Maršrutizatoriai

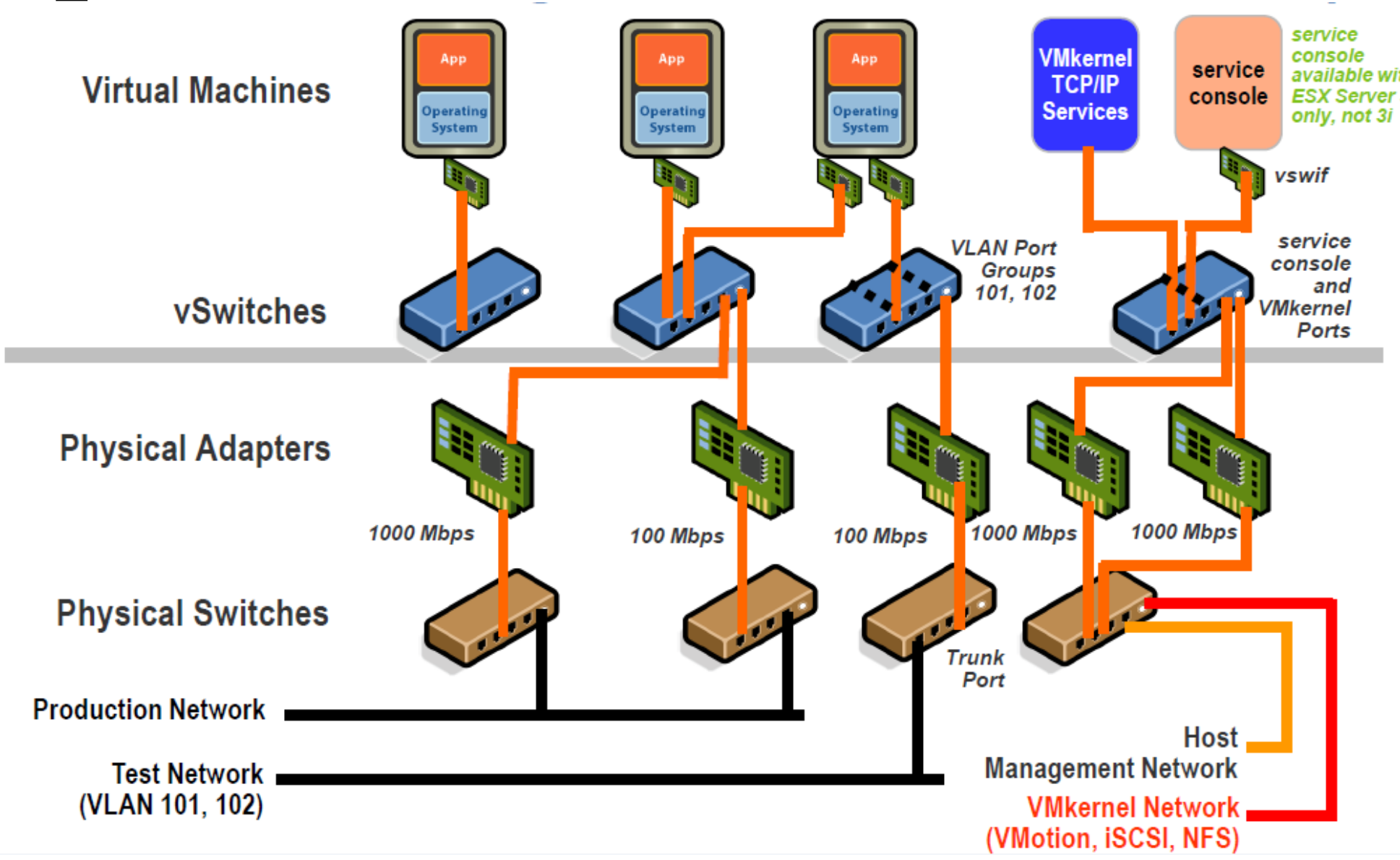
Virtualūs komponentai:

- Virtualios tinklo plokštės (vNIC)
- Vmkernel NIC (vmknic)
- Virtualūs komutatoriai
  - VM prievadai
  - vmkernel prievadai

Tinklo komponentai



Tinklo infrastruktūra



Virtualios mašinos pajungimas

Galimi trys būdai, kaip prijungti VM į tinklą:

- Naudoti VM prievadus
- Naudoti vmkernel prievadus
- Naudoti Service Console arba Management Network prievadus.

Virtualūs NIC

- vNIC – tai VM virtualios tinklo plokštės.
- VMkernel priklauso tinklo modulis, kuris dar vadinamas vmknic.

Vmware ESX gali emuliuoti tokias tinklo plokštes:

- AMD PCNET32, e1000 (*native*)
- vmxnet (paravirtualizuota)
- vmxnet2 (e1000) (paravirtualizuota)

Paravirtualizuota greitesnė nei *native.* VM gali turėti daugiausiai 4 vNIC.

Virtualus komutatorius

Virtualus komutatorius – tai VMkernel modulis, kuris suteikia tinklinį ryšį ESX serveriui. Tai 2 lygmens (Layer2) pagal OSI modelį įrenginys.

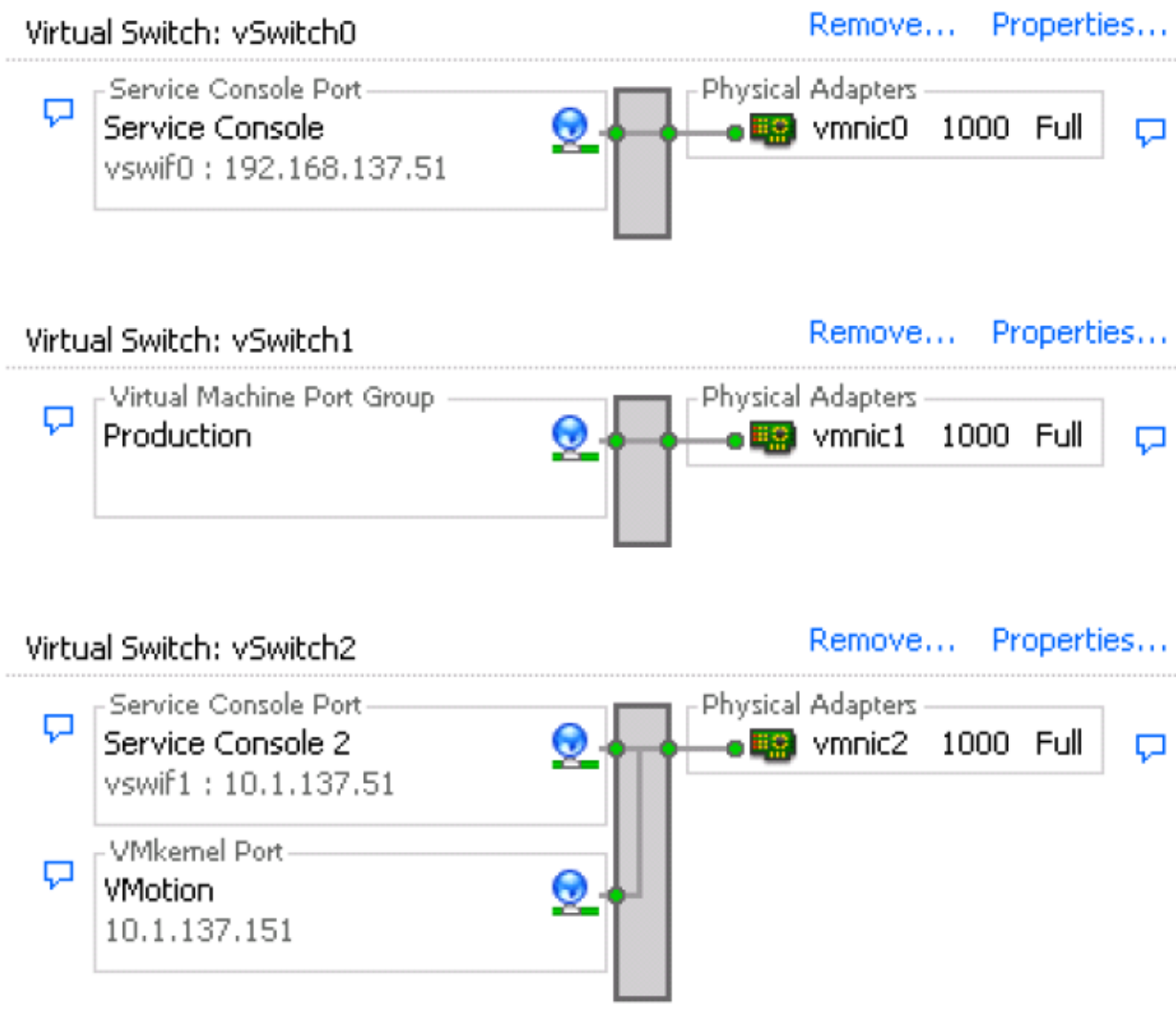
Virtualaus komutatoriaus pagalba galime prisijungti prie:

- valdymo tinklo – nuotoliniam prisijungimui prie ESX
- VM tinklo, kuriame užtikrinamas ryšys tarp VM
- IP saugyklos (NAS, iSCSI)
- Išorinio tinklo

Virtualus komutatorius kuriamas:

Configurations -> Networking lange.

Virtualaus tinklo infrastruktūra



Virtualus komutatorius

- Du ar daugiau virtualių komutatorių negali būti pajugti prie vienos fizinės tinklo plokštės.
- Komutatorius gali turėti 2 ir daugiau fizinių tinklo plokščių ir jas grupuoti (pvz. **nic teaming**) tam kad užtikrinti automatinį paketų paskirstymą ir padidintų patikimumą.
- Tinklo komutatorius, neturintis priskirtos nei vienos fizinės tinklo plokštės, suformuoja vidinį tinklą ESX serverio viduje, leidžiantį VM komunikuoti neišeinant į išorę.

Virtualus komutatoriaus prievadai

- Kiekviena virtuali tinklo plokštė (vNIC, service console, vmknic) yra prijungiama prie atitinkamos prievadų grupės.
- Grupių tipai: VM ir VMkernel. (ESX 3.5 papildomai turi Service Console, kuri nuo ESX v.4.0 nebenaudojama)
- Prievadų grupės tipas nustatomas kuriant ją.
- Prievadų grupė kuriama, norint sudaryti atskirą VLAN (802.1q).
- VM „mato“ viena kitą, jei jų vNIC yra toje pačioje prievadų grupėje.
- VLAN ID galimi nuo 0 iki 4095.

Virtualus komutatorius

vSwitch valdo prievadų grupę, tačiau neturi galimybės konfigūruoti atskiro prievado.

vSwitch turi visas žinomas Layer 2 apsaugas:

- packet sniffing,
- MAC spoofing,
- srauto ribojimą.

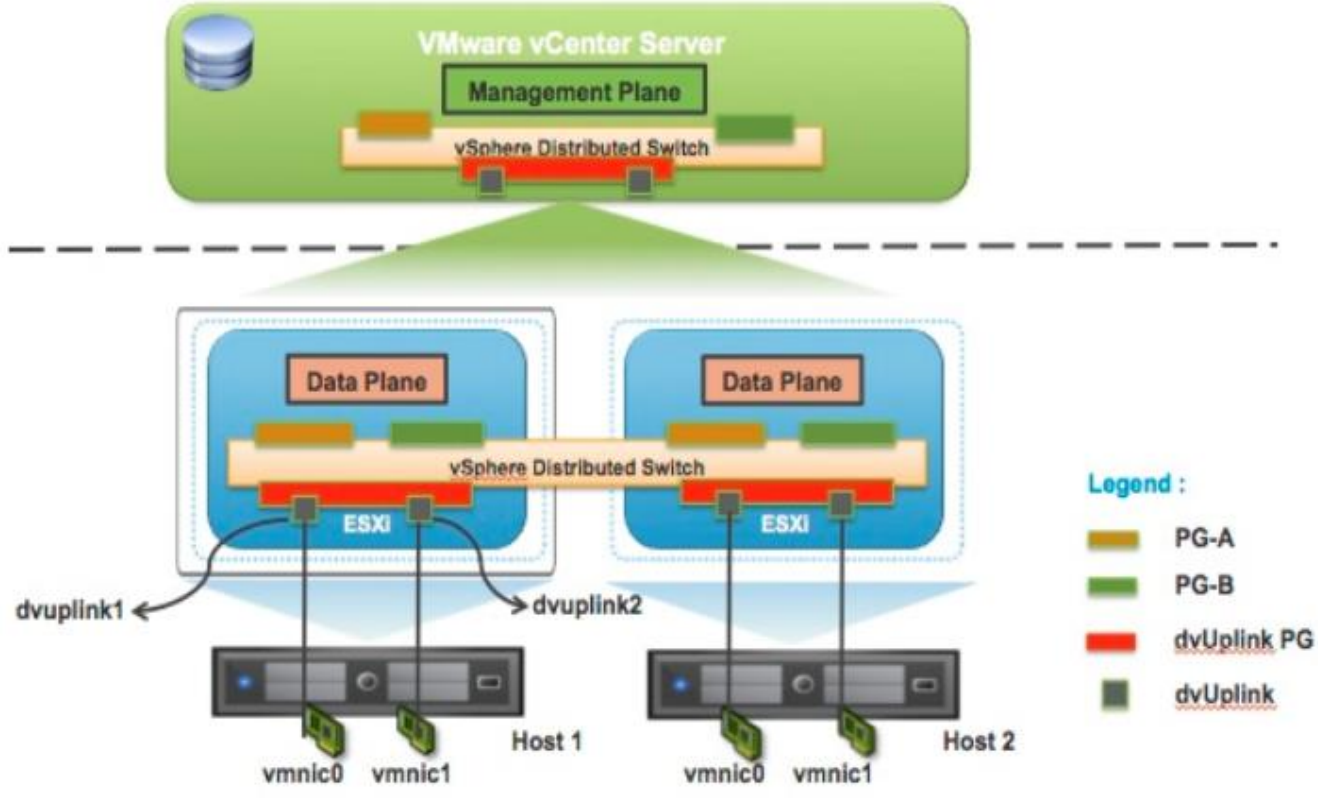
Nuo aukštesnio lygio (Layer 3) grėsmių turi būti apsisaugota naudojant VM vidines ugniasienes arba kitas priemones.

Paskirstytas virt.komutatorius

Distributed Virtual Switch (DVS) suteikia sistemos administratorius prieigą valdant tinklą.

- Centralizuotas vSwitch prievadų konfigūravimas, prievadų vardų suteikimas, filtravimas ir t.t.
- Link Aggregation Control Protocol (LACP) – suderina ir automatiškai konfigūruoja jungčių agregaciją tarp ESX serverių ir fizinių komutatorių.
- Tinklo monitoringas
  - Palaiko RSPAN ir ERSPAN protokolus nuotolinei tinklo analizei
  - IPFIX Netflow v. 10
  - SNMP v3

Paskirstytas virt.komutatorius



Prijungimų tikrinimas

Norint patikrinti ar teisingi fizinių tinklo plokščių ir virtualių komutatorių nustatymai, galima naudoti konsolės komandas (prisijungus per ssh):

```
> esxcfg-nics -l
> esxcfg-vswitch -l
```

esxcfg-nics komanda parodo fizinės tinklo plokštės MAC adresą ir sąryšį tarp fizinės ir virtualios tinklo plokštės vmnic.

VLAN kūrimas

Norint izoliuoti tarpusavyje virtualias mašinas, reikia sukurti prievadų grupes su nustatytomis VLAN reikšmėmis.

VLAN leidžia sukurti daug loginių LAN fiziniame tinklo segmente.

VLAN leidžia:

- Padidinti saugumą t.y. nusiųsti paketą į teisingą segmentą;
- Padidina našumą, nes VLAN turi savo transliavimo domeną;
- Sumažinti kainą, nes nereikalingi fiziniai komutatoriai.

VLAN apibrėžia IEEE 802.1Q standartas, pagal kurį formuojami papildomi laukai kadre:

indikacinis 802.1Q (2 bytes) + VLAN ID (2 bytes)

VLAN kūrimas

VLAN kuriami tinklo komutatoriuose grupuojant:

- **prievadus**
- **tinklo įrenginių MAC adresus**.

Prievadų grupavimo atveju vieno VLAN prievadams suteikiamas tas pats VLAN ID. Paketas iš vieno VLAN niekada nepereina į kitą VLAN.

Grupuojant MAC adresus, komutatoriaus konfigūracijoje turi būti surašyti visų įrenginių MAC adresai, kurie priklausys konkrečiam VLAN.
Toks grupavimas retai naudojamas dėl didelio rankinio darbo kiekio.

VLAN tipai

Naudojami tokie VLAN tipai:

- Numatytasis (default) VLAN
- Gimtasis (native) VLAN
- Duomenų (data) VLAN

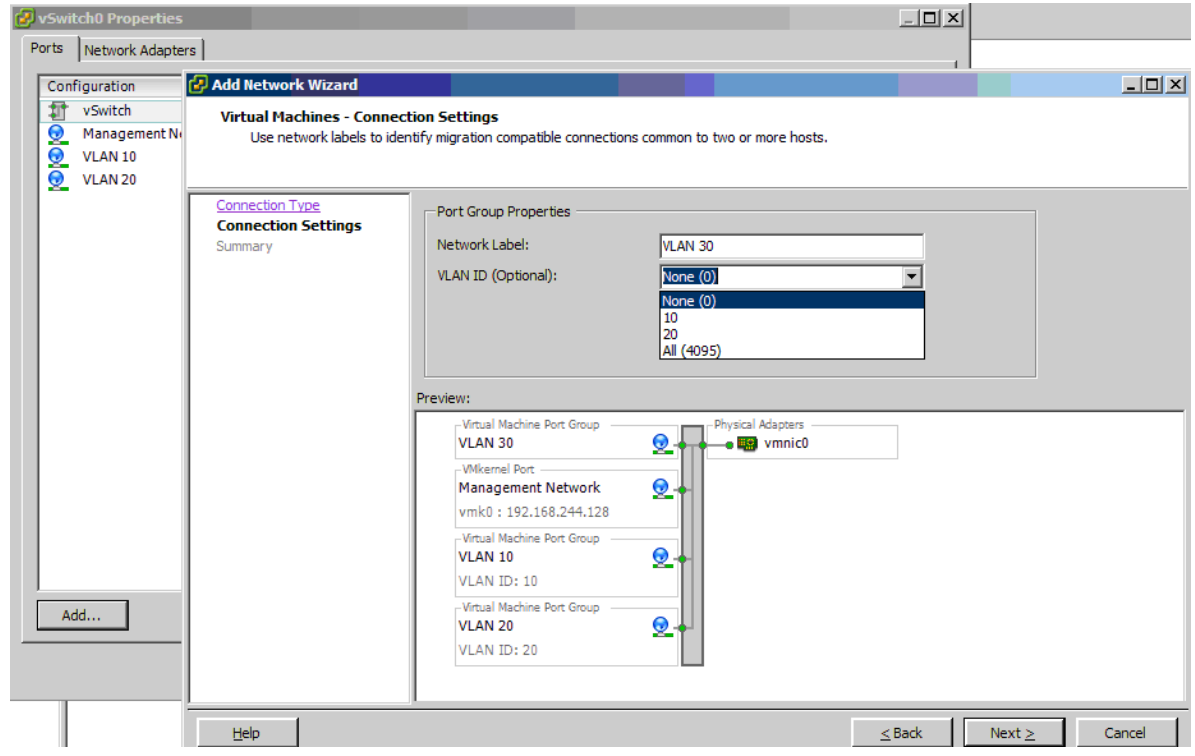
Numatytasis VLAN priskiriamas visiems komutatoriaus prievadams pirmą kartą užsikrovus sistemą. Numatytojo VLAN ID lygus 1 ir negali būti keičiamas (skaičius).

Gimtasis VLAN priskiriamas prie 802.1Q trunk port. 802.1Q trunk port persiunčia srautą, einantį iš bet kurio VLAN (tagged traffic) ir srautą, kuris nepriklauso jokiam VLAN.

Duomenų VLAN naudojamas vartotojų duomenų perdavimui.

VLAN kūrimas

VLAN kūrimas atliekamas pasirenkame virtualiųjų mašinų prievadų tipą ir nurodome pavadinimą ir „VLAN ID” reikšmę.

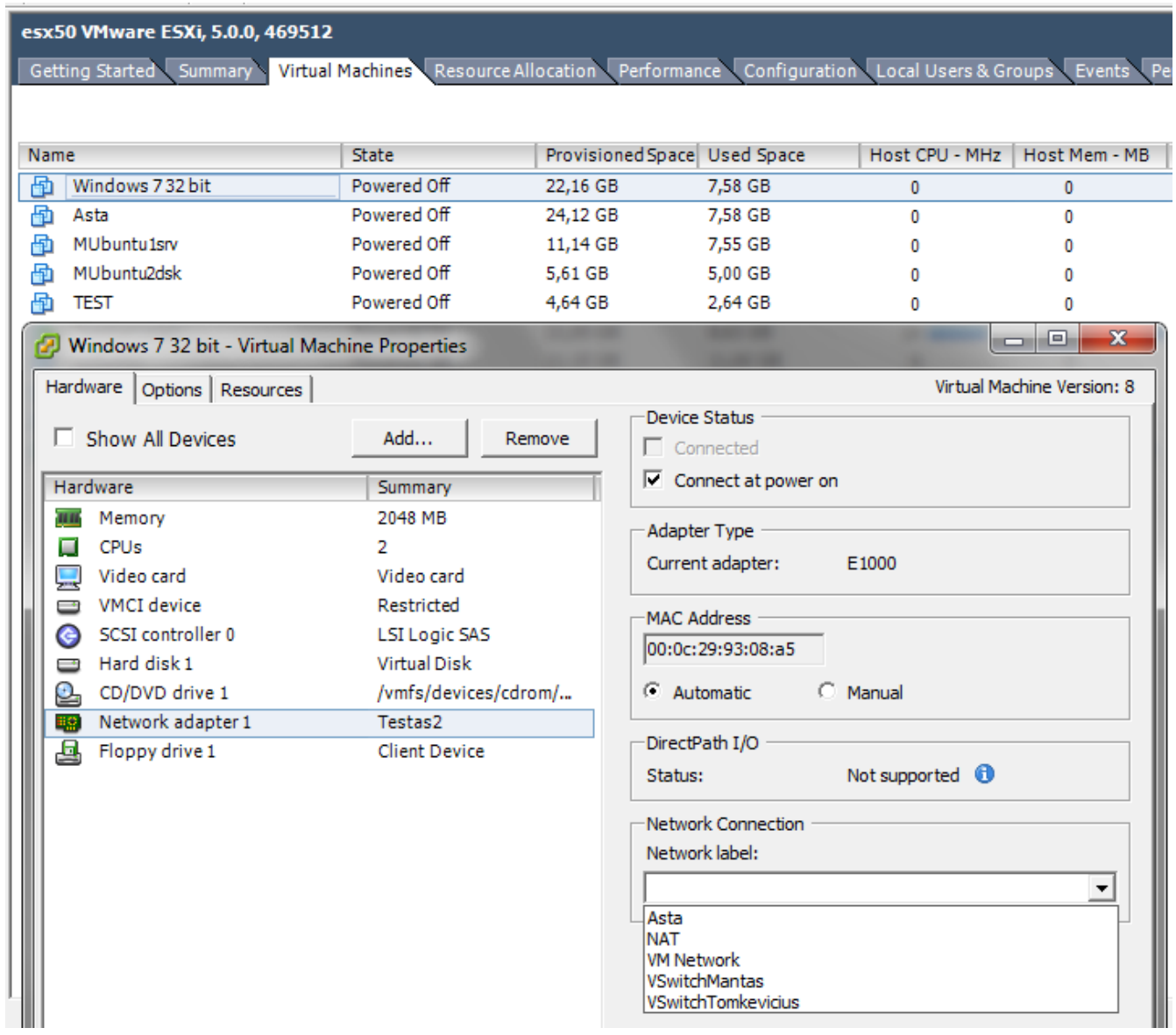


VLAN konfigūravimas

1. Sukuriami visi nurodyti virtualūs prievadai ir priskiriama VLAN ID reikšmė.

2. VM pajungimas prie VLAN atliekamas pasirinkus VM nustatymuose tinklo plokštę ir priskyrus jai atitinkamą VLAN. Analogiškai priskiriam tinklo plokštę komutatoriaus prievadų grupei ir kai nėra naudojami VLAN.

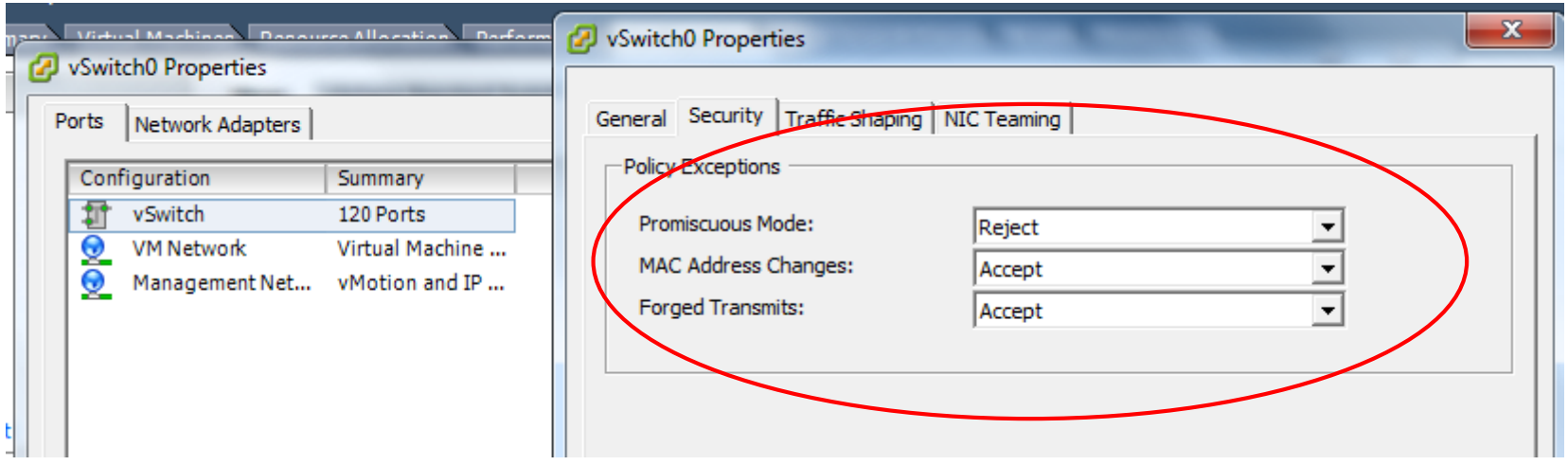
VM pajungimas prie VLAN



Virtualaus komutatoriaus sauga

Virtualaus komutatoriaus saugos nustatymai (Layer 2) išeinančiam srautui:

- Allow Promiscuouse Mode
- Allow MAC address Change
- Allow Forged Transmit



Virtualaus komutatoriaus sauga

Promiscuous Mode

- Reject – VM tinklo adapterio nustatymas į promiscous rėžimą nedaro įtakos adapterio darbui
- Accept – VM tinklo adapterį nustatymas į promiscous rėžimą leidžia tikrinti visus tinkle keliaujančius kadrus (IDS, Sniffer).

MAC address Change

- Reject – jei VM tinklo adapterio MAC adresas pakeičiamas į kitą nei nustatyta .vmx faile, kadrai atmetami.
- Accept - VM tinklo adapterio MAC adreso keitimas leidžiamas ir nesukelia jokių ribojimų.

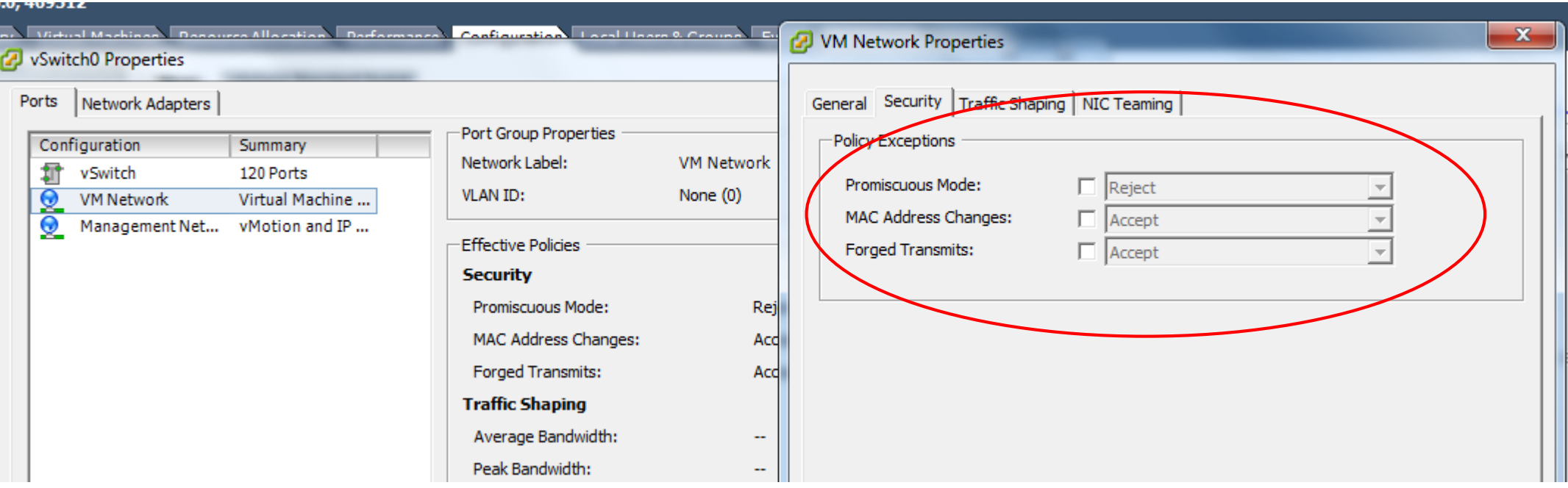
Forged Transmit

- Reject — bet kurie išeinantys kadrai su skirtingu MAC adresu, nei nustatyta adapteryje atmetami.
- Accept — nefiltruojama ir visi išeinantys kadrai yra praleidžiami.

Prievadų grupės sauga

Komutatoriaus saugos nustatymai paveldimi prievadams, nors priedų grupėms gali būti perrašomi analogiški trijų tipų saugos nustatymai tik su skirtingomis reikšmėmis:

- Allow Promiscuouse Mode
- Allow MAC address Change
- Allow Forged Transmit



Srauto valdymo principai

Tinklo srauto valdymas gali būti daromas tik **išeinančiam** srautui.

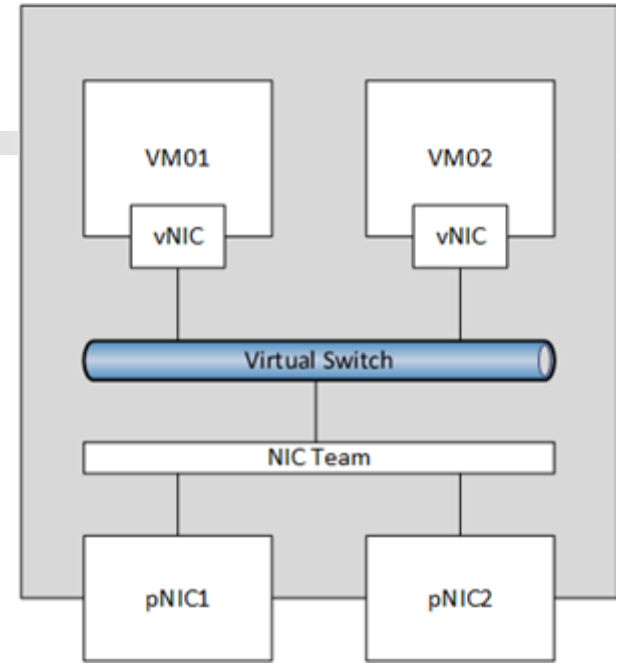
Išeinantis srautas valdomas apibrėžiant:

- Vidutinį pralaidumą (Kbps)
- Maksimalų (peak) pralaidumą (Kbps)
- Pliūpsnio (burst) dydį apskaičiuojamą kaip KB

Burst = Bandwidth * time

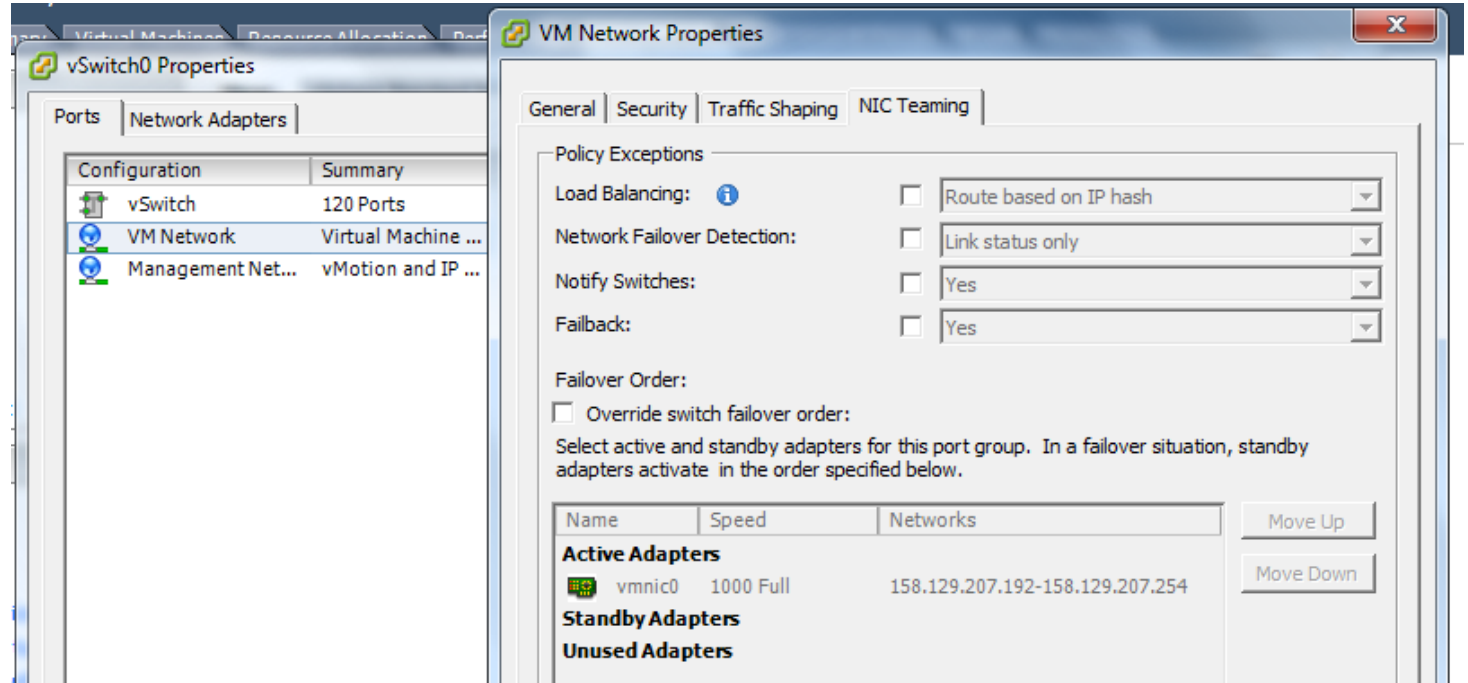
Įėjimo srautas turi būti valdomas fiziniuose maršrutizatoriuose.

pNIC grupės



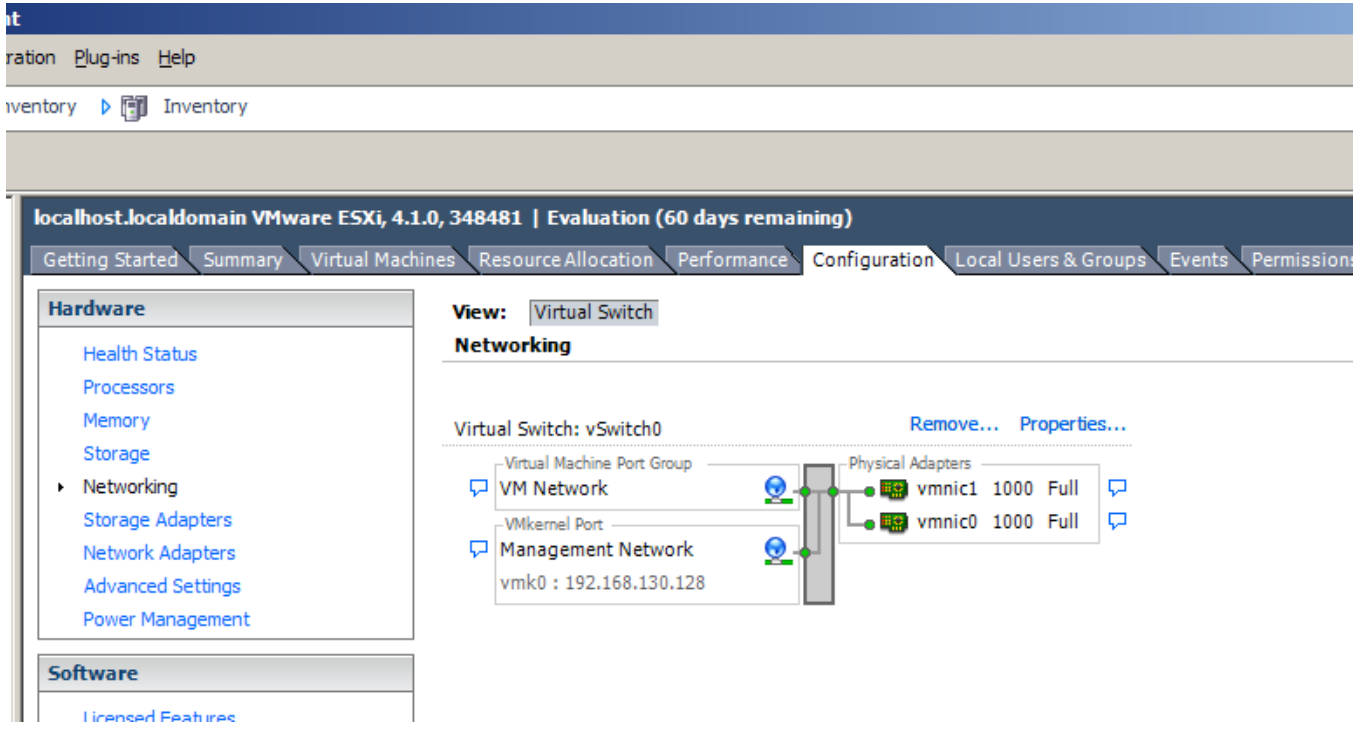
Virtualus komutatorius gali turėti:

- Dedikuota pNIC (1 vnt.)
- Keletą dedikuotų pNIC
  - Apkrovos balansavimui
  - Patikimumo (failover) didinimui



pNIC grupavimas

Norint gauti apkrovos balansavimo ar padidinto patikimumo sistemas, keli pNIC priskiriami vienam virtualiam komutatoriui ir apjungiami į grupę (NIC teaming).



Apkrovos balansavimas

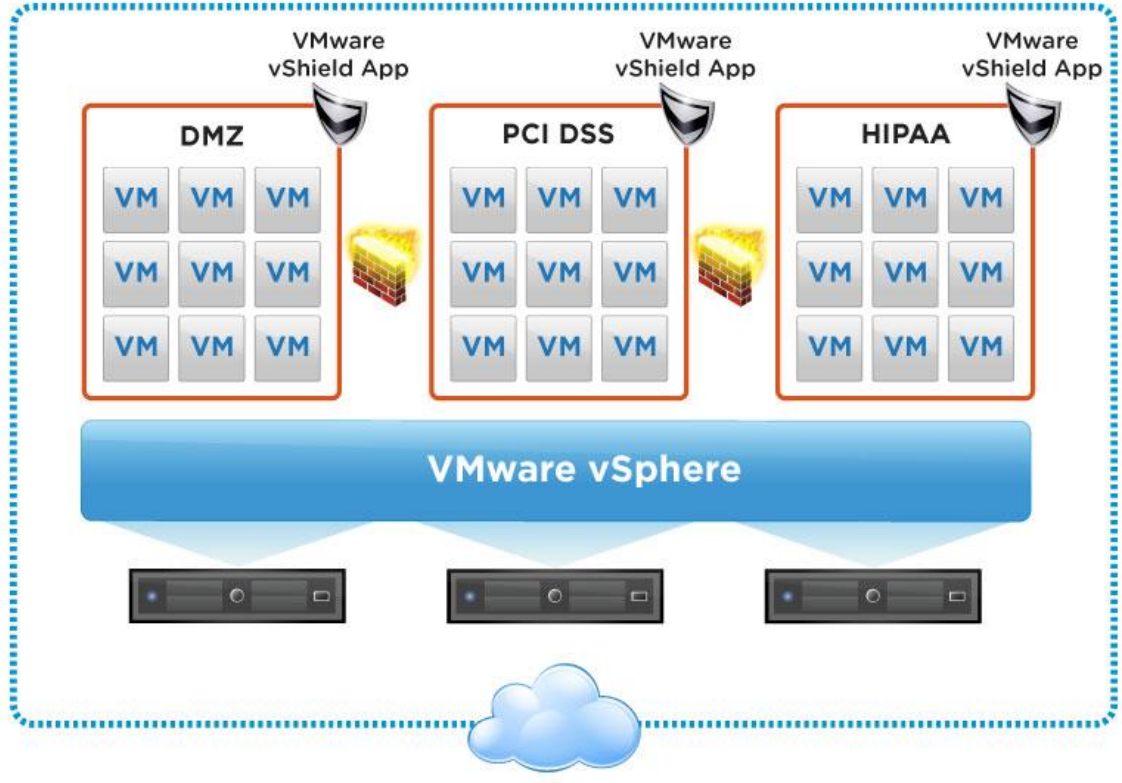
Balansuojant apkrovą, VMkernel nusprendžia per kurią pNIC IP paketas turi būti išsiųstas.

Balansavimui naudojami tokie maršrutizavimo algoritmai:

- pagal prievado ID (nesudaro CPU apkrovos)
- Pagal siuntėjo MAC hash (vidutinė CPU apkrova)
- Pagal IP hash (imlus CPU apkrovai, galimas didesnis išeinančio srauto pralaidumas per kelias pNIC, reikalingas 802.3ad palaikymas – link aggregation).

Saugumo zonos

Dėl lankstaus virtualių komutatorių konfigūravimo galimybių, virtualioje infrastruktūroje galimos įvairios saugumo zonos.



Tinklo gedimų detektavimas

- Tinklo gedimus aptinka VMkernel, kuri stebi:
  - Sujungimo (link) būseną
  - Srauto apkrovimą (beaconing)
- Gedimai yra apeinami (failover) konfigūruojant tinklo nustatymus:
  - Apkrovos balansavimą
  - Padidintą patikimumą
  - Atstatymo procedūras (failback) t.y. kai pNIC vėl prijungiama prie tinklo.

Tinklo gedimų detektavimas