VMware vSphere

Virtuális Hálózatok Biztonsága

Zrubecz.Laszlo@andrews.hu

Andrews IT Engineering Kft.

Biztonság

„A biztonság NEM termék...”

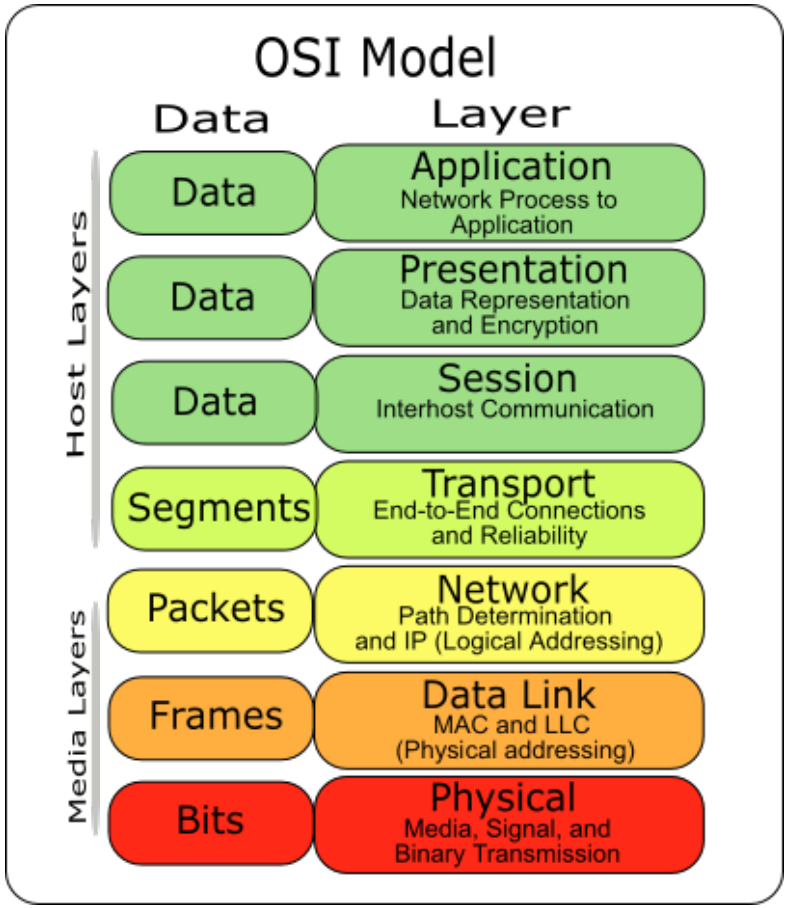
Biztonság

Biztonság <——-||——————————> Kényelem

Hálózatok

„Egy rendszer csak annyira biztonságos, mint a benne szereplő leggyengébb láncszem”

OSI Model


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Fizikai hálózatok

- Hálózati topológia
- Fizikai szeparáció
- Logikai szeparáció
- Tűzfal

Fizikai hálózatok

- Hálózati topológia
- Fizikai szeparáció
- Logikai szeparáció
- Tűzfal

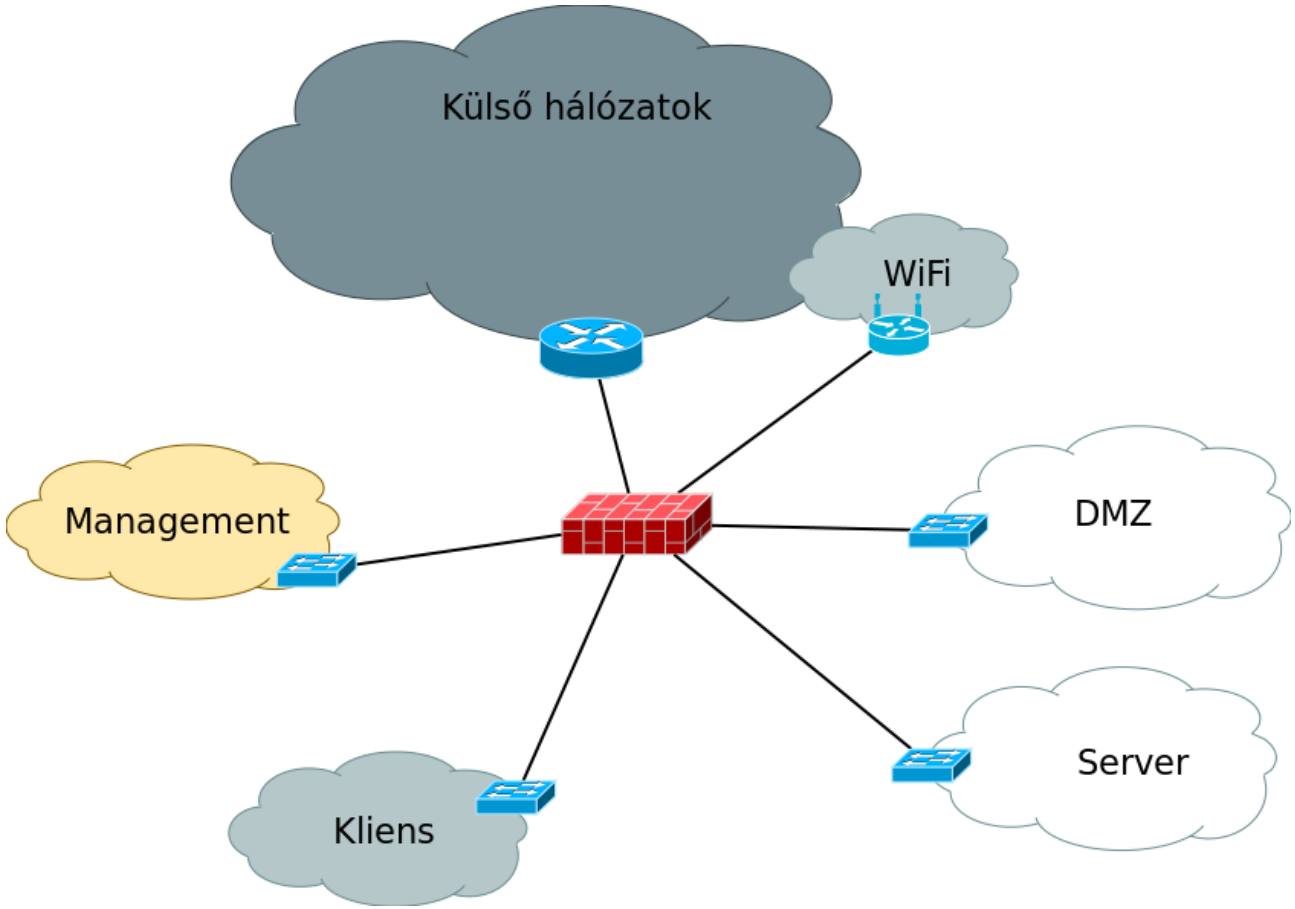
Fizikai hálózatok

- Hálózati topológia
- Fizikai szeparáció
- Logikai szeparáció
- Tűzfal

Fizikai hálózatok

- Hálózati topológia
- Fizikai szeparáció
- Logikai szeparáció
- Tűzfal

Ideális hálózati topológia



Virtuális hálózatok

- Management/Service Console
- VMotion
- Fault Tolerance logging
- iSCSI, NFS, FC
- Produktív hálózatok

Virtuális hálózatok

- Management/Service Console
- VMotion
- Fault Tolerance logging
- iSCSI, NFS, FC
- Produktív hálózatok

Virtuális hálózatok

- Management/Service Console
- VMotion
- Fault Tolerance logging
- iSCSI, NFS, FC
- Produktív hálózatok

Virtuális hálózatok

- Management/Service Console
- VMotion
- Fault Tolerance logging
- iSCSI, NFS, FC
- Produktív hálózatok

Virtuális hálózatok

- Management/Service Console
- VMotion
- Fault Tolerance logging
- iSCSI, NFS, FC
- Produktív hálózatok

VLAN - fizikai környezetben

- NEM biztonsági eszköz!
- Mi valósítja meg? - SWITCH!
- Mi a buktatója?
  - VLAN ID
  - ARP protokol
- http://www.google.com/search?q=VLAN+hacking

VLAN - fizikai környezetben

- NEM biztonsági eszköz!
- Mi valósítja meg? - SWITCH!
- Mi a buktatója?
  - VLAN ID
  - ARP protokol
- http://www.google.com/search?q=VLAN+hacking

VLAN - fizikai környezetben

- NEM biztonsági eszköz!
- Mi valósítja meg? - SWITCH!
- Mi a buktatója?
  - VLAN ID
  - ARP protokol
- http://www.google.com/search?q=VLAN+hacking

VLAN - virtuális környezetben

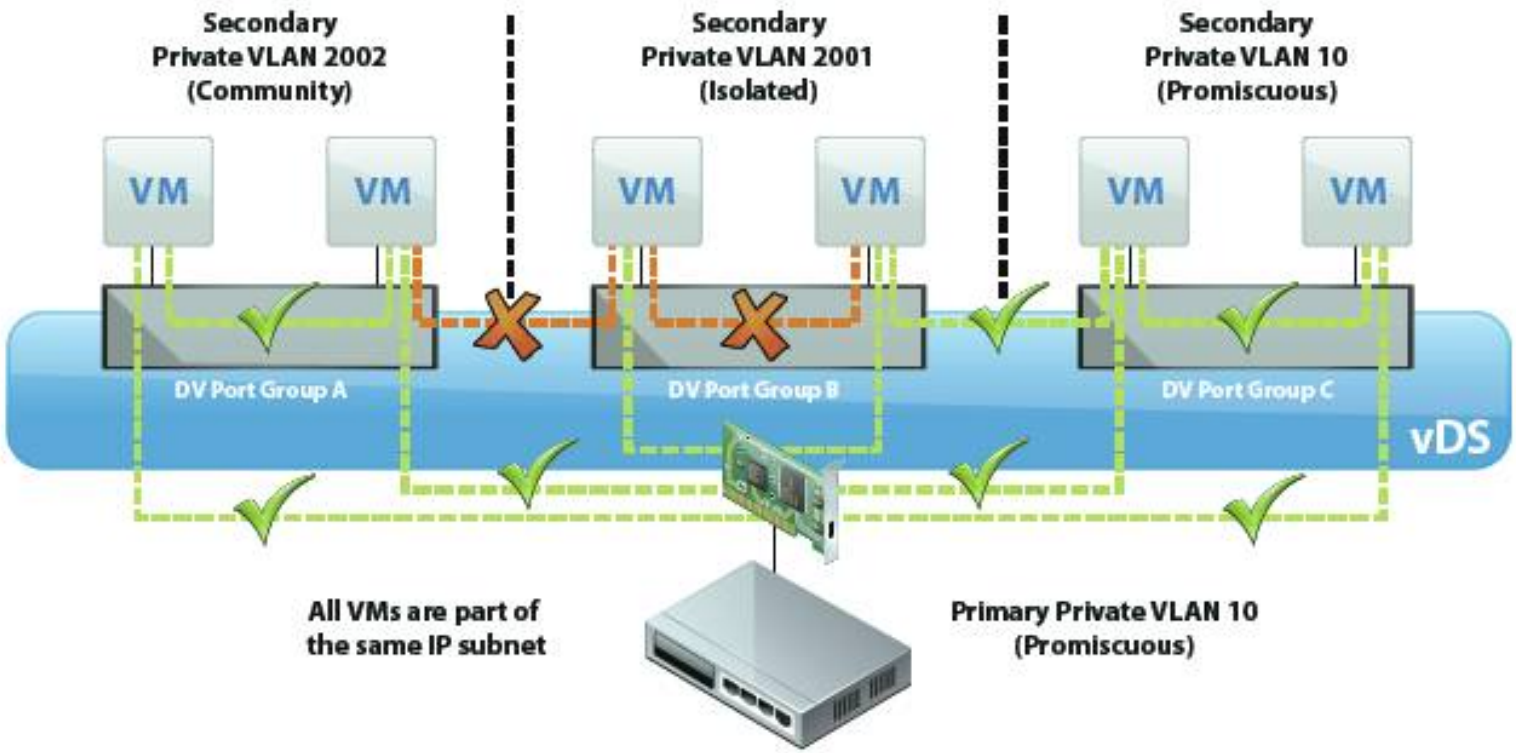
- Mitől jobb, mint fizikai környezetben?
  - a virtuális switch 'okosabb',
  - nem csak a VLAN ID-re épít, és nem kell bíznia az ARP protokollban
  - a vhost és a vswitch is a vmkernel kezelése alatt vannak.
- Továbbra is hátrány:
  - a virtuális hálózatból kilépve elveszti a fenti előnyöket.

VLAN - virtuális környezetben

- Mitől jobb, mint fizikai környezetben?
  - a virtuális switch 'okosabb',
  - nem csak a VLAN ID-re épít, és nem kell bíznia az ARP protokollban
  - a vhost és a vswitch is a vmkernel kezelése alatt vannak.
- Továbbra is hátrány:
  - a virtuális hálózatból kilépve elveszti a fenti előnyöket.

PVLAN

Figure 4 - Private VLANs provide a simple way of selectively isolating VMs without exhausting IP subnets.



Hardver

- Fizikai hozzáférés
- BIOS beállítások
- Management felület
- BLADE rendszerek

Hardver

- Fizikai hozzáférés
- BIOS beállítások
- Management felület
- BLADE rendszerek

Hardver

- Fizikai hozzáférés
- BIOS beállítások
- Management felület
- BLADE rendszerek

Hardver

- Fizikai hozzáférés
- BIOS beállítások
- Management felület
- BLADE rendszerek

ESX beállítások

- root jelszó
- ssh
- remote syslog
- lockdown mode
  - vSphere Client root-ként
  - CLI/RCLI root-ként
- SSL és tanúsítványok
- 'tech support mode'

ESX beállítások

- root jelszó
- ssh
- remote syslog
- lockdown mode
  - vSphere Client root-ként
  - CLI/RCLI root-ként
- SSL és tanúsítványok
- 'tech support mode'

ESX beállítások

- root jelszó
- ssh
- remote syslog
- lockdown mode
  - vSphere Client root-ként
  - CLI/RCLI root-ként
- SSL és tanúsítványok
- 'tech support mode'

ESX beállítások

- root jelszó
- ssh
- remote syslog
- lockdown mode
  - vSphere Client root-ként
  - CLI/RCLI root-ként
- SSL és tanúsítványok
- 'tech support mode'

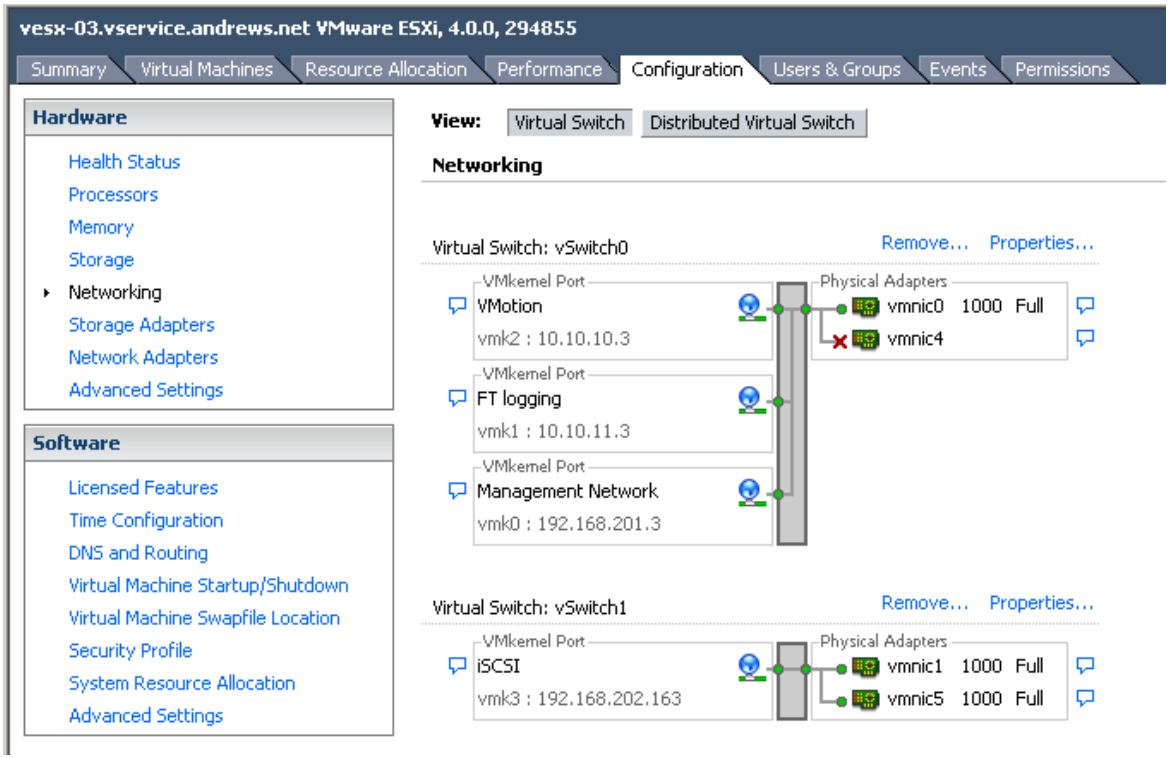
ESX beállítások

- root jelszó
- ssh
- remote syslog
- lockdown mode
  - vSphere Client root-ként
  - CLI/RCLI root-ként
- SSL és tanúsítványok
- 'tech support mode'

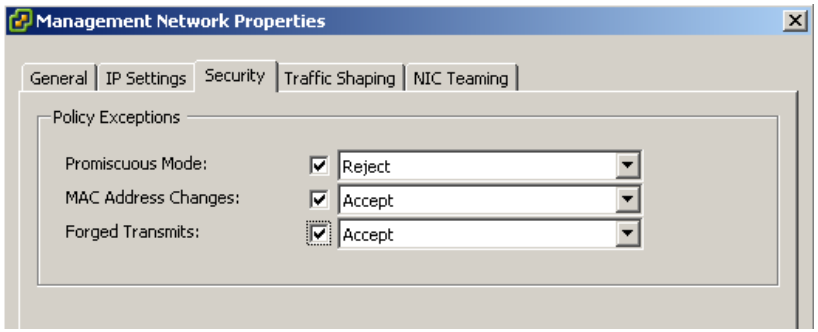
ESX beállítások

- root jelszó
- ssh
- remote syslog
- lockdown mode
  - vSphere Client root-ként
  - CLI/RCLI root-ként
- SSL és tanúsítványok
- 'tech support mode'

ESX beállítások - Hálózat



ESX beállítások - Hálózat



vCenter Server

- fizikai vagy virtuális?
- operációs rendszer
- felhasználók bejelentkezése
- vSphere Web Access
- Update Manager
- SSL és tanúsítványok
- ACL (jogosultságok)

vCenter Server

- fizikai vagy virtuális?
- operációs rendszer
- felhasználók bejelentkezése
- vSphere Web Access
- Update Manager
- SSL és tanúsítványok
- ACL (jogosultságok)

vCenter Server

- fizikai vagy virtuális?
- operációs rendszer
- felhasználók bejelentkezése
- vSphere Web Access
- Update Manager
- SSL és tanúsítványok
- ACL (jogosultságok)

vCenter Server

- fizikai vagy virtuális?
- operációs rendszer
- felhasználók bejelentkezése
- vSphere Web Access
- Update Manager
- SSL és tanúsítványok
- ACL (jogosultságok)

vCenter Server

- fizikai vagy virtuális?
- operációs rendszer
- felhasználók bejelentkezése
- vSphere Web Access
- Update Manager
- SSL és tanúsítványok
- ACL (jogosultságok)

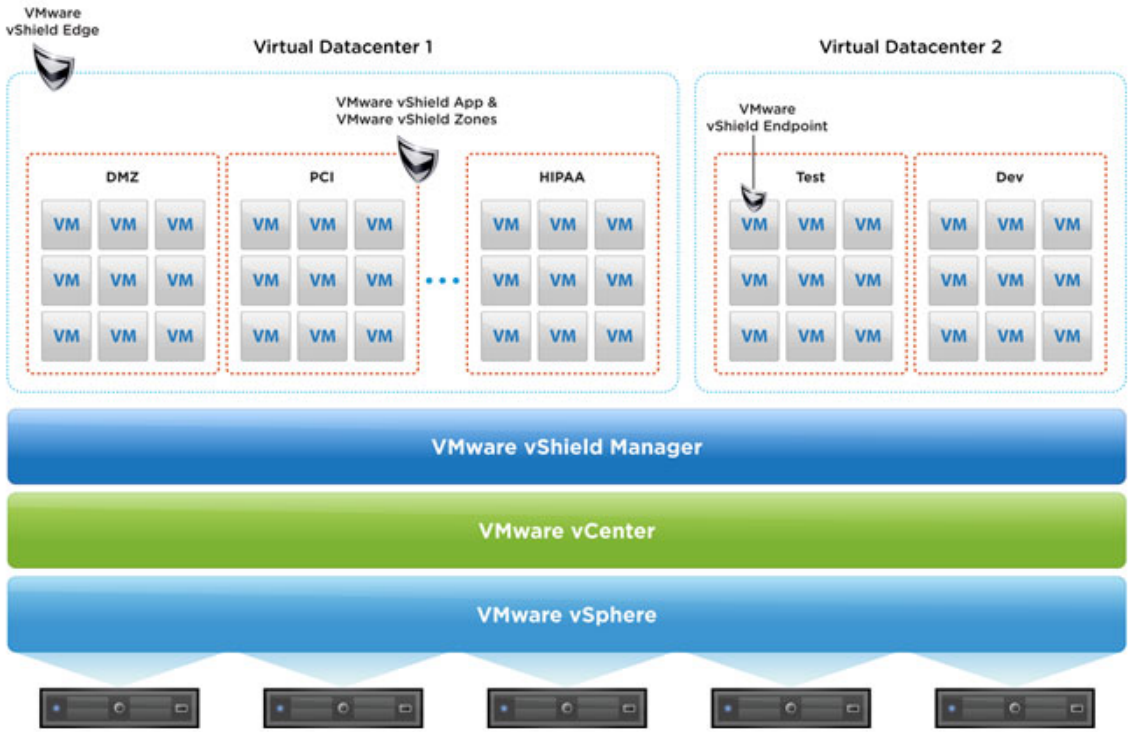
vCenter Server

- fizikai vagy virtuális?
- operációs rendszer
- felhasználók bejelentkezése
- vSphere Web Access
- Update Manager
- SSL és tanúsítványok
- ACL (jogosultságok)

vCenter Server

- fizikai vagy virtuális?
- operációs rendszer
- felhasználók bejelentkezése
- vSphere Web Access
- Update Manager
- SSL és tanúsítványok
- ACL (jogosultságok)

VMware vShield



vShield Manager

- Virtual Appliance
- Központi management eszköz a vShield termékcsaládhoz
- vCenter Server - 1 vShield Manager/vCenter
- vShield Manager UI vagy vSphere Client plug-in
- Követelmény: 100% uptime!

vShield Manager

- Virtual Appliance
- Központi management eszköz a vShield termékcsaládhoz
- vCenter Server - 1 vShield Manager/vCenter
- vShield Manager UI vagy vSphere Client plug-in
- Követelmény: 100% uptime!

vShield Manager

- Virtual Appliance
- Központi management eszköz a vShield termékcsaládhoz
- vCenter Server - 1 vShield Manager/vCenter
- vShield Manager UI vagy vSphere Client plug-in
- Követelmény: 100% uptime!

vShield Manager

- Virtual Appliance
- Központi management eszköz a vShield termékcsaládhoz
- vCenter Server - 1 vShield Manager/vCenter
- vShield Manager UI vagy vSphere Client plug-in
- Követelmény: 100% uptime!

vShield Manager

- Virtual Appliance
- Központi management eszköz a vShield termékcsaládhoz
- vCenter Server - 1 vShield Manager/vCenter
- vShield Manager UI vagy vSphere Client plug-in
- Követelmény: 100% uptime!

vShield Zones

- Virtual Appliance
- mit ’véd’?:Port group - 1 vShield Zones/ESX
- forrás IP és port; cél IP és port; protokoll
- állapottartó csomagszűrő

vShield Zones

- Virtual Appliance
- mit ’véd’?:Port group - 1 vShield Zones/ESX
- forrás IP és port; cél IP és port; protokoll
- állapottartó csomagszűrő

vShield Zones

- Virtual Appliance
- mit ’véd’?:Port group - 1 vShield Zones/ESX
- forrás IP és port; cél IP és port; protokoll
- állapottartó csomagszűrő

vShield Zones

- Virtual Appliance
- mit ’véd’?:Port group - 1 vShield Zones/ESX
- forrás IP és port; cél IP és port; protokoll
- állapottartó csomagszűrő

vShield App

- vShield Zones + Licenc
- mit ’véd’?: virtual NIC - 1 vShield App/ESX
- DRS, DPM, vMotion kompatibilis

vShield App

- vShield Zones + Licenc
- mit ’véd’?: virtual NIC - 1 vShield App/ESX
- DRS, DPM, vMotion kompatibilis

vShield App

- vShield Zones + Licenc
- mit ’véd’?: virtual NIC - 1 vShield App/ESX
- DRS, DPM, vMotion kompatibilis

vShield Edge

- Virtual Appliance
- Határvédelmi megoldás a virtuális és a fizikai hálózatok között
- Amit ’véd’: Port group - 1 vShield Edge/Port group
- Amit tud:
  - DHCP
  - NAT
  - VPN
  - Load Balance
  - remote syslog

vShield Edge

- Virtual Appliance
- Határvédelmi megoldás a virtuális és a fizikai hálózatok között
- Amit 'véd': Port group - 1 vShield Edge/Port group
- Amit tud:
  - DHCP
  - NAT
  - VPN
  - Load Balance
  - remote syslog

vShield Edge

- Virtual Appliance
- Határvédelmi megoldás a virtuális és a fizikai hálózatok között
- Amit 'véd': Port group - 1 vShield Edge/Port group
- Amit tud:
  - DHCP
  - NAT
  - VPN
  - Load Balance
  - remote syslog

vShield Edge

- Virtual Appliance
- Határvédelmi megoldás a virtuális és a fizikai hálózatok között
- Amit 'véd': Port group - 1 vShield Edge/Port group
- Amit tud:
  - DHCP
  - NAT
  - VPN
  - Load Balance
  - remote syslog

vShield Endpoint

- Hypervisor modul + Virtual Appliance
- mit ’véd’?: Virtuális gép operációs rendszerét
- víruskergető megoldás a vhost-ok számára
  - ’on demand’
  - ’on access’
- Követelmény: vSphere 4.1 vagy újabb

vShield Endpoint

- Hypervisor modul + Virtual Appliance
- mit ’véd’?: Virtuális gép operációs rendszerét
- víruskergető megoldás a vhost-ok számára
  - ’on demand’
  - ’on access’
- Követelmény: vSphere 4.1 vagy újabb

vShield Endpoint

- Hypervisor modul + Virtual Appliance
- mit ’véd’?: Virtuális gép operációs rendszerét
- víruskergető megoldás a vhost-ok számára
  - ’on demand’
  - ’on access’
- Követelmény: vSphere 4.1 vagy újabb

vShield Endpoint

- Hypervisor modul + Virtual Appliance
- mit ’véd’?: Virtuális gép operációs rendszerét
- víruskergető megoldás a vhost-ok számára
  - ’on demand’
  - ’on access’
- Követelmény: vSphere 4.1 vagy újabb

Bővebben

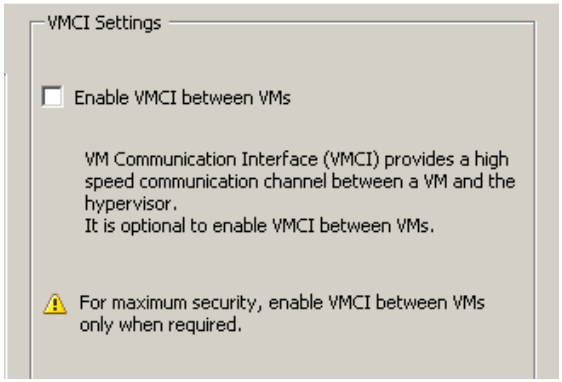
- VMware vShield Documentation
  - http://www.vmware.com/support/pubs/vshield_pubs.html

Virtuális gépek

- Kik üzemelteti a vhostokat?
- Kik üzemeltetik a virtuális környezetet?
- Biztonság vagy Kényelem?
- Ezen beállítások függetlenek a virtuális környezettől

Virtuális gépek

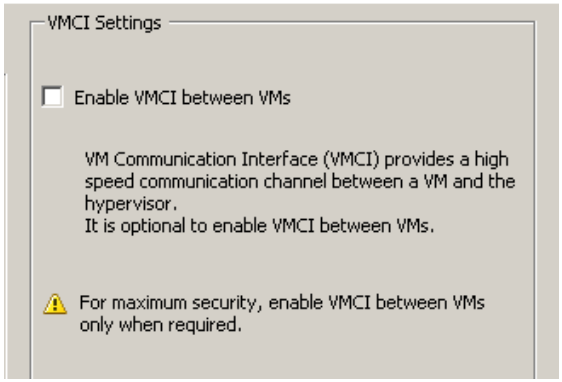
- VMware Tools - rootkit?
- VMCI



- Security Hardening Guide
  - http://www.vmware.com/resources/techresources/10109

Virtuális gépek

- VMware Tools - rootkit?
- VMCI



- Security Hardening Guide
  - http://www.vmware.com/resources/techresources/10109

“A biztonság NEM termék, hanem egy állapot amit igyekszünk folyamatosan fenntartani”

Köszönöm a figyelmet

“A biztonság NEM termék, hanem egy állapot amit igyekszünk folyamatosan fenntartani”

Köszönöm a figyelmet