

VMware vSphere

Virtuális Hálózatok Biztonsága

Zrubecz.Laszlo@andrews.hu

Andrews IT Engineering Kft.

- 1 Hálózatok
 - Fizikai hálózatok
 - Virtuális hálózatok
 - VLAN
- 2 ESX szerverek
 - Hardver környezet
 - ESX beállítások (ESXi, ESX)
- 3 vCenter Server
- 4 VMware vShield
 - vShield Manager
 - vShield Zones/vShield App
 - vShield Edge
 - vShield Endpoint
- 5 Virtuális gépek

Biztonság

„A biztonság NEM termék...”

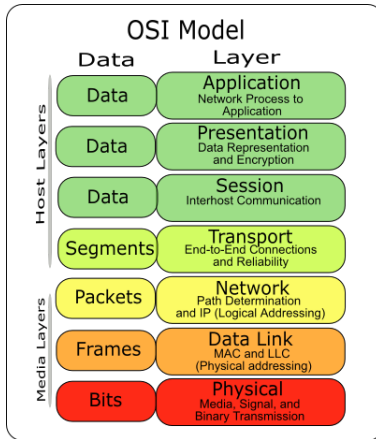
Biztonság

Biztonság <-----||-----> Kényelem

Hálózatok

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

OSI Model



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

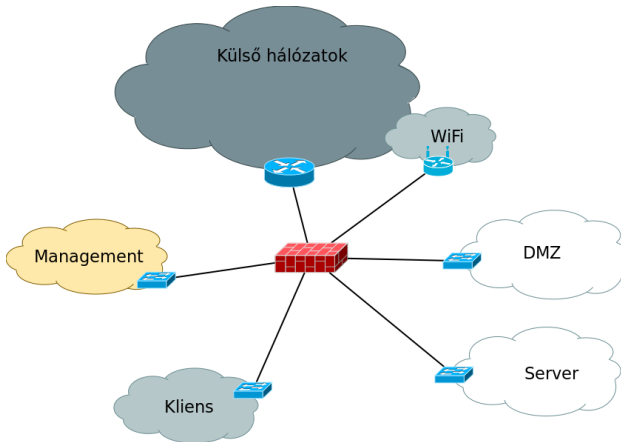
- Hálózati topológia
- Fizikai szeparáció
- Logikai szeparáció
- Tűzfal

Hálózatok

ESX szerverek
vCenter Server
VMware vShield
Virtuális gépek

Fizikai hálózatok
Virtuális hálózatok
VLAN

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 protokoll
- <http://www.google.com/search?q=VLAN+hacking>

VLAN - fizikai környezetben

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

VLAN - fizikai környezetben

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

VLAN - virtuális környezetben

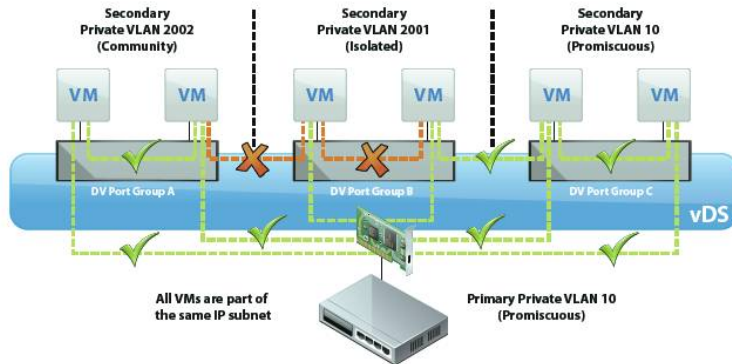
- Mitől jobb, mint fizikai környezetben?
 - a virtuális switch 'okosabb',
 - nem csak a VLAN ID-re épít, és nem kell bízni az ARP protokollban
 - a vhost és a vswitch is a vmkernel kezelése alatt vannak.
- Továbbra is hátrány:
 - a virtuális hálózatból kilépve elveszti a fenti előnyöket.

VLAN - virtuális környezetben

- Mitől jobb, mint fizikai környezetben?
 - a virtuális switch 'okosabb',
 - nem csak a VLAN ID-re épít, és nem kell bízni 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

The screenshot shows the VMware vSphere Configuration page for an ESXi host. The left sidebar contains a navigation tree with 'Hardware' and 'Software' sections. The 'Networking' section is expanded, showing two virtual switches: vSwitch0 and vSwitch1. vSwitch0 is connected to physical adapters vmnic0 and vmnic4. vSwitch1 is connected to physical adapters vmnic1 and vmnic5. The interface includes tabs for Summary, Virtual Machines, Resource Allocation, Performance, Configuration, Users & Groups, Events, and Permissions. The Configuration tab is active, and the Networking section is expanded to show the details of the virtual switches and their connections to physical adapters.

vesx-03.vservice.andrews.net VMware ESXi, 4.0.0, 294855

Summary Virtual Machines Resource Allocation Performance Configuration Users & Groups Events Permissions

View: Virtual Switch Distributed Virtual Switch

Networking

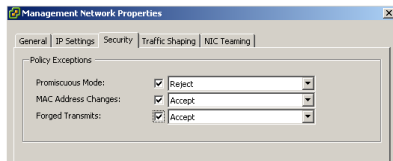
Virtual Switch: vSwitch0 [Remove...](#) [Properties...](#)

VMkernel Port	Physical Adapters
VMotion vmlk2 : 10.10.10.3	vmnic0 1000 Full vmnic4
FT logging vmlk1 : 10.10.11.3	
Management Network vmlk0 : 192.168.201.3	

Virtual Switch: vSwitch1 [Remove...](#) [Properties...](#)

VMkernel Port	Physical Adapters
iSCSI vmlk3 : 192.168.202.163	vmnic1 1000 Full vmnic5 1000 Full

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)

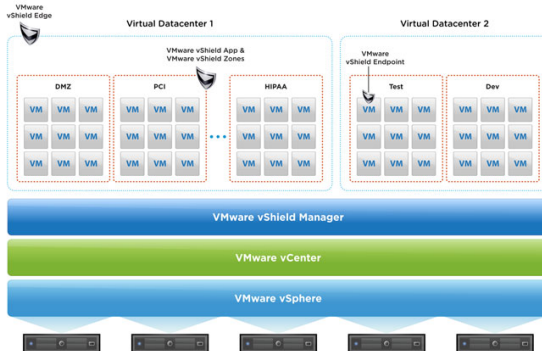
vCenter Server

- 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
- állapotartó 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

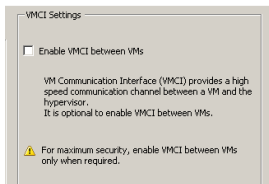
- VMware vShield Documentation
 - http://www.vmware.com/support/pubs/vshield_pubs.html

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

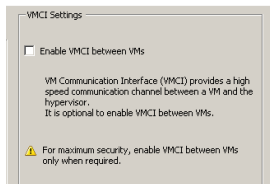


- Security Hardening Guide

- <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