Virtualios infrastruktūros sauga

3 paskaita

Virtualios saugyklos: lokalios ir tinklinės, protokolai

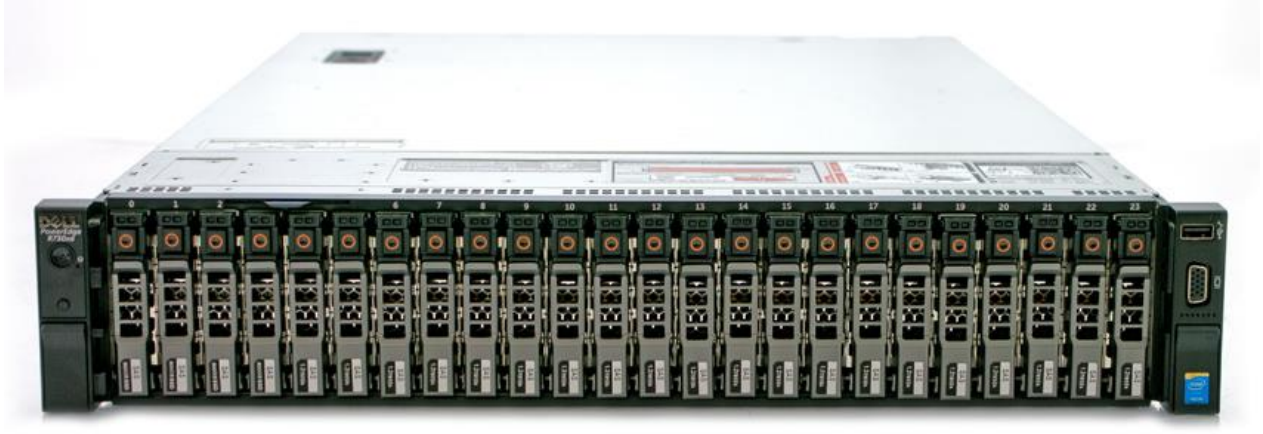
Saugyklų tipai

VMware ESXi palaiko tokias tinklo saugyklas:

- **SAN – Storage Area Network** (saugyklų tinklas)
  - Fibre Channel
  - iSCSI
- NAS - **Network Attached Storage** (per TCP/IP tinklą prijungta saugykla)

VMware ESX saugykla gali būti ir lokaliame serverio diske (diskuose).

Tinklo saugyklų teorija



Saugyklų diskų prijungimo sąsajos

- **SATA –** Serial ATA jungtis, pralaidumas iki 600 MB/s (SATA-3).
  Bit error rate BER = 1.0e-15,
  Mean time between failure 1.2 e+6 h.
- **Fibre Channel** (Fibre Channel (FC) sąsaja – tai nuosekli sąsaja, šiuo metu ji pagrindinė SAN tinkluose. Pralaidumas iki 12.75 Gbps)
- **SCSI –** Small Computer System Interface. Pralaidumas iki 320MB/s.
- **SAS** – Serial Attached SCSI. Pralaidumas iki 6 Gbps, palaiko iki 16384 įrenginių. BER = 1.0 e-16.
  Mean time between failure 1.6 e+6 h
- **NL-SAS** - SATA diskas su SAS sąsaja (7.2K rpm)
  BER = 1.0 e-15. MTBF = 1.2 e+6 h

Diskų charakteristikos

Uždelsimo priklausomybė nuo disko plokštelės sukimosi dažnio.

Rotational speed [rpm]	Average latency [ms]
15,000	2
10,000	3
7,200	4.16
5,400	5.55
4,800	6.25

HDD elektros sąnaudos

Elektros sąnaudos = Diametras^2 x RPM $^{2.8}$ x plokštelių skaičius

	Capacity (GB)	Price	Platters	RPM	Diameter (inches)	Average seek (ms)	Power (watts)	I/O/sec	Disk BW (MB/sec)	Buffer BW (MB/sec)	Buffer size (MB)	MTTF (hrs)
SATA	500	$375	4 or 5	7,200	3.7	8–9	12	117	31–65	300	16	0.6M
SAS	37	$150	1	15,000	2.6	3–4	25	285	85–142	300	8	1.2M

Saugyklų įrenginių prijungimo metodai naudojant TCP/IP

- **Ethernet interface** - Ethernet tinklo sąsaja gali būti naudojama kaip Layer 2 (*kanalinis lygmuo*) technologija TCP/IP tinklu perduoti duomenis ir padaryti jas prieinamas nutolusiems įrenginiams.
- **Network Attached Storage (NAS)**
- **iSCSI** (Internet SCSI – tai transporto protokolas, kuris inkapsuliuoja SCSI komandas į TCP/IP datagramą ir perduoda ją kompiuterinių tinklu gaunančiai pusei).
- **iFCP** (Internet Fibre Channel Protocol (iFCP) - tai mechanizmas duomenų persiuntimui iš/į Fibre Channel saugyklų įrenginius SAN tinkle arba Internetu per TCP/IP).
- **FCIP** - Fibre Channel over IP (FCIP) - tai Fibre Channel tunelio arba saugyklų tunelio protokolas.

NAS

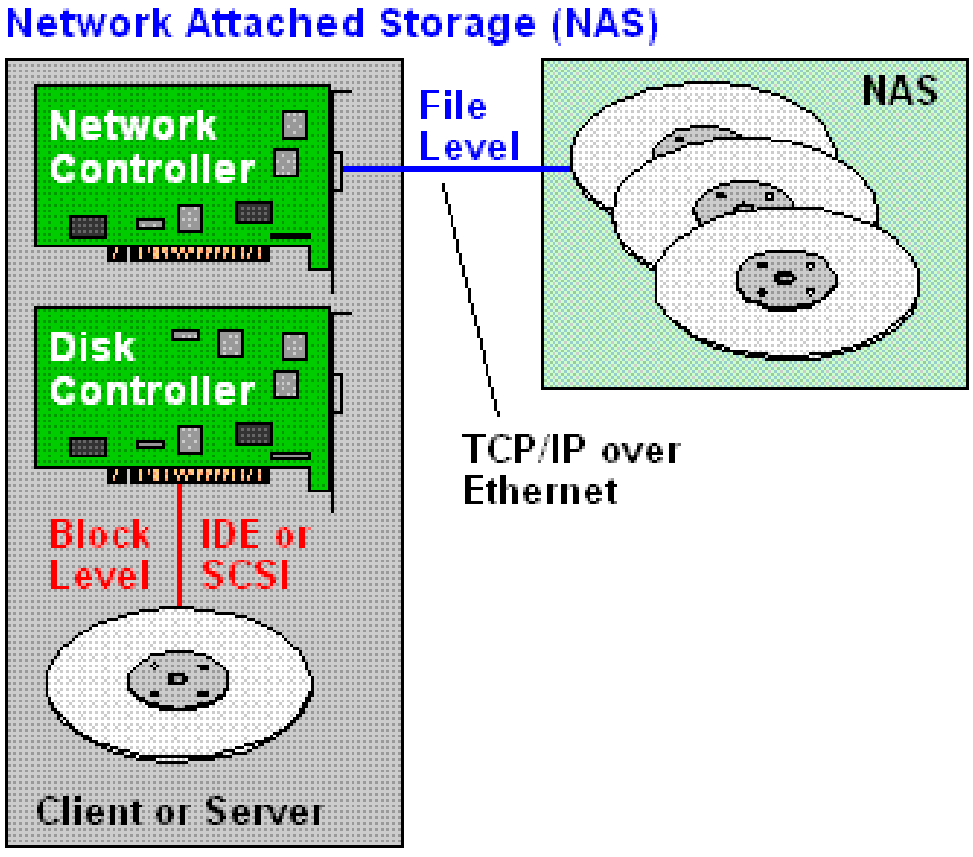
Network Attached Storage (NAS) – tai tokie saugyklų elementai, kurie prijungiami prie egzistuojančio kompiuterių tinklo ir dalinasi su kitais tinkle esančiais kompiuteriams savo resursais. Duomenys pasiekiami kaip failai. Kitais žodžiais NAS – tai tinkle esantys failų serveriai.

NAS saugyklų architektūrą sudaro:

- NAS procesorius (gateway/head), užtikrinantis priėjimą prie failų per kompiuterių tinklą
- vienas ar daugiau įrenginių, kuriuose saugomi duomenys
- sąsaja su kompiuterių tinklu – tinklo plokštės.

NAS elementai gali būti prijungti prie bet kokio tipo kompiuterių tinklo TCP/IP, NetBEUI, IPX/SPX (Ethernet, Token Ring, FDDI, ATM, SoNET, Frame Relay...).

NAS paskirtis



NAS sistemos buvo sukurtos siekiant sumažinti problemas dėl DAS, kuomet reikdavo administruoti visumą serverių kiekvieną atskirai, buvo prastai sprendžiamos sistemų patikimumo, plėtimo ir našumo problemos.

NAS lengvai naudojamos ir plečiamos, leidžia dalinti heterogeninius resursus, užtikrina centralizuotą administravimą ir valdymą, taip pat suteikia didesnį patikimumą.

NAS failų persiuntimo protokolai

NAS sistemose duomenų saugojimas paremtas failų saugojimo principu. Kadangi failai yra sudaryti iš blokų, todėl NAS naudoja metaduomenis, kad nustatyti ryšį tarp failo ir blokų. Ši procedūra yra paslėpta nuo išorinių serverių, kuriems NAS – tai failų ir katalogų serveris.

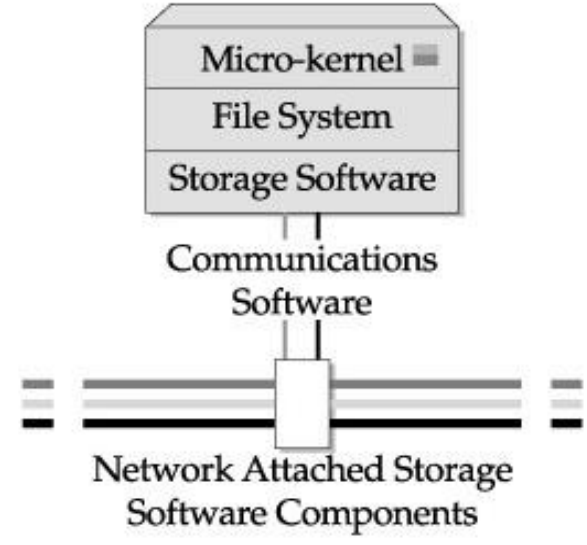
Protokolai, naudojami failų persiuntimui NAS sistemose:

- **NFS** - Network File System (SUN)
- **CIFS** – IBM& Microsoft's Common Internet File System.
- **Apple FS**
- **HTTP**
- **FTP**

NAS programinė įranga

NAS sistemos į kompiuterių tinklą pajungiamos, kaip nepriklausomi tinklo komponentai, todėl saugyklos valdymui ir administravimui naudojamas procesorius (kompiuteris) ir programinė įranga, kuri gali būti suskirstyta į tris komponentus:

- NAS micro-kernel (optimizuota operacinė sistema DART, Data ONTAP, FreeNAS - FreeBSD)
- Failų sistemos programinė įranga ir komunikacijų protokolai (NFS, CIFS, FTP, Apple FS)
- Saugyklos diskų kontrolės programinė įranga (RAID, FC-AL)



NAS nauda

NAS įrenginiai – tai loginės failinės sistemos įrenginiai lokaliame kompiuterių tinkle.

NAS įrenginių našumas priklauso:

- HDD charakteristikų (uždelsimo, pralaidumo, aps/min, buferio)
- HDD sąsajų pralaidumo, uždelsimo
- Spartinančiosios atminties darbo
- Tinklo plokštės spartos (uždelsimas, pralaidumas)

NAS privalumas – duomenų saugykla pasiekiama visiems tinkle esantiems kompiuteriais ir matomas, kaip tinklinis HDD.

NAS trūkumas – tai jautrus tinklo stabilumui ir pralaidumui įrenginys. Bet koks sutrikimas kompiuterių tinkle, stabdo duomenų pasiekimo greitį.

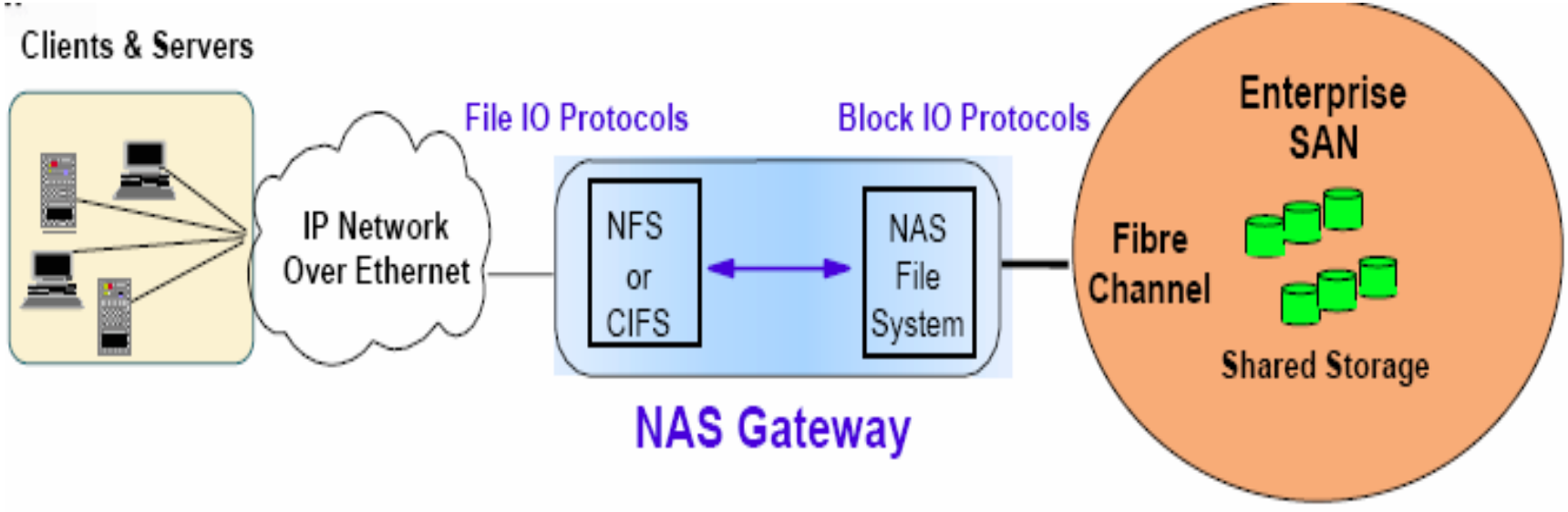
NAS saugyklų taikymai

NAS leidžia serveriams pasiekti saugyklas taikant “file-based” protokolus.

NAS leidžia sukurti paprastas, mažų kainų, subalansuoto apkrovimo ir patikimas sistemas. Pavyzdžiui:

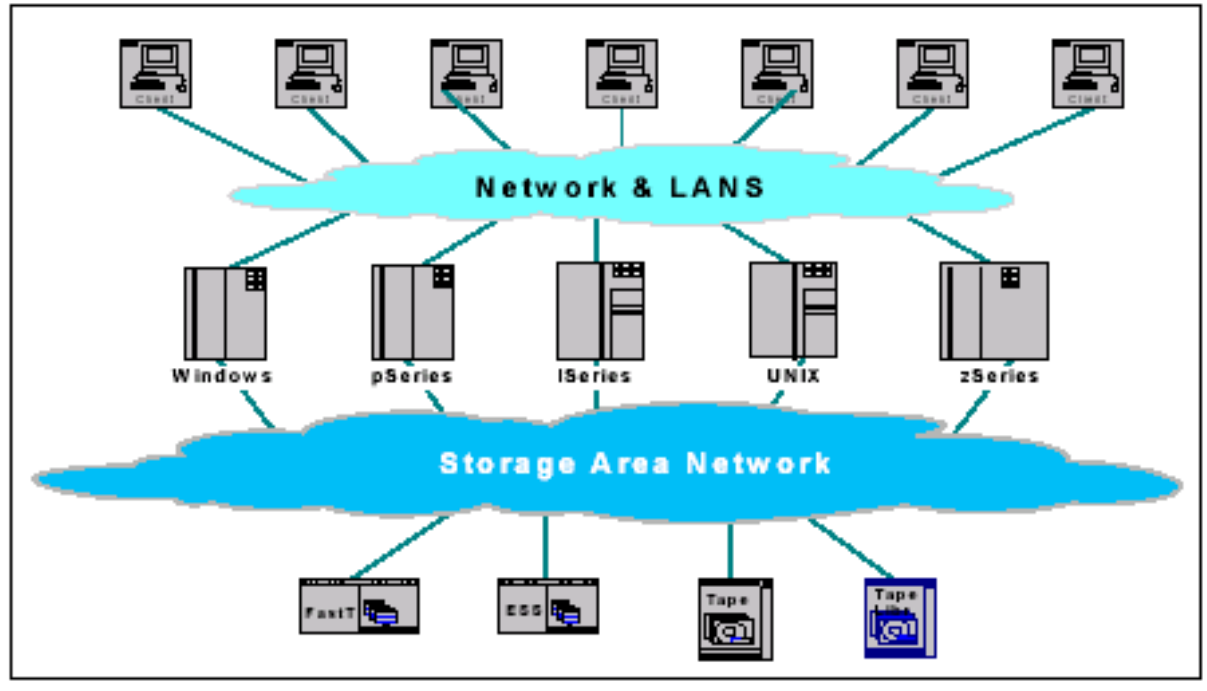
- Korporatyvinė e-pašto sistema;
- Subalansuoto apkrovimo web serveriai, kurie naudoja NAS, kaip duomenų saugyklas;
- Vartai į SAN saugyklas (NAS gateway/Head). Tai leidžia integruoti NAS ir SAN infrastruktūras į vieną globalią saugyklų infrastruktūrą.
- Rezervinių kopijų (backup) saugykla

NAS gateway


Clients & Servers
IP Network
Over Ethernet
File IO Protocols
Block IO Protocols
NFS
or
CIFS
NAS
File
System
NAS Gateway
Enterprise
SAN
Fibre
Channel
Shared Storage

SAN

SAN – tai specializuotas didelio pralaidumo duomenų saugyklas jungiantis tinklas. Jis kartais vadinamas *“the network behind the servers.”* SAN leidžia tinklo sujungimus “any-to-any”, naudojant tokius tinklo elementus: maršrutizatorius, vartus (gateways), šakotuvus, komutatorius ir dirigentus(directors). Jis eliminuoja tradicinį dedikuotą sujungimą tarp serverio ir saugyklos ir tam panaudoją saugyklų tinklą.



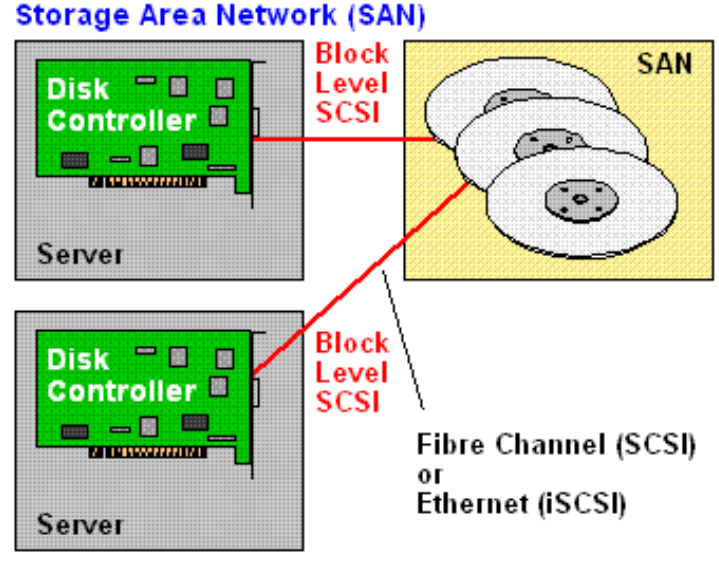
SAN komunikacinė infrastruktūra

Storage Network Industry Association (SNIA) apibrėžia SAN kaip tinklą, skirtą duomenų persiuntimui tarp kompiuterinių sistemų ir saugyklų elementų.

SAN komunikacinę infrastruktūrą sudaro:

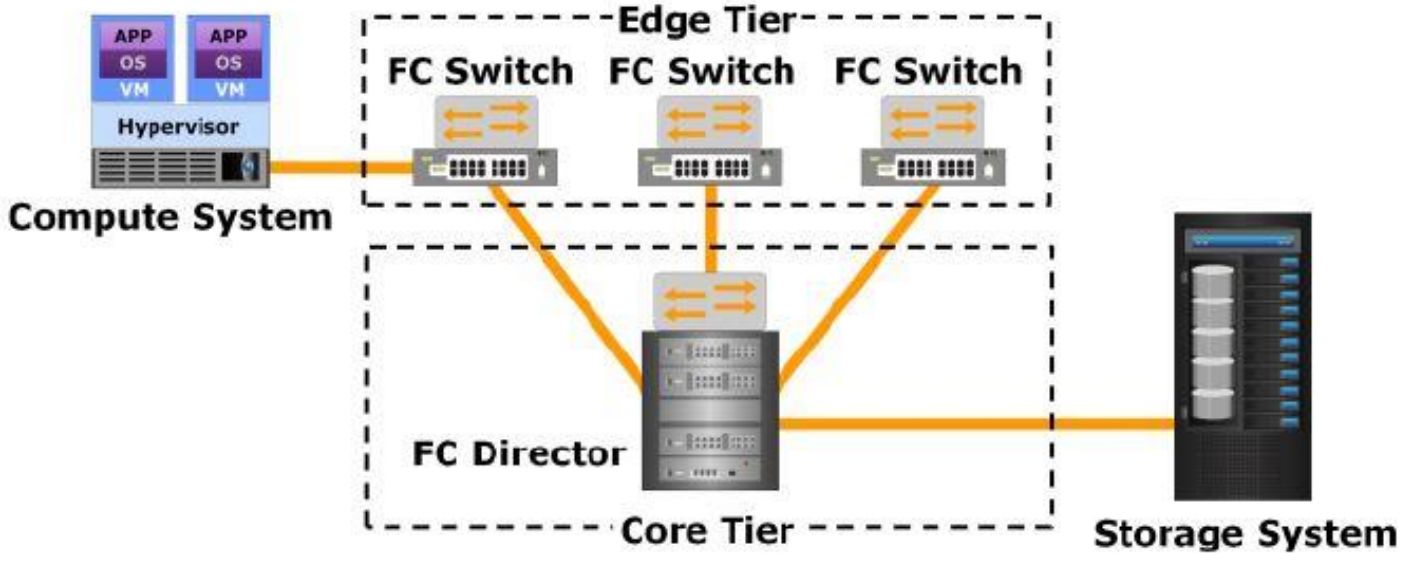
- **Fiziniai sujungimai;**
- **Valdymo lygmuo**, kuris administruoja sujungimus tarp saugyklų elementų ir serverių taip, kad duomenų persiuntimas vyktų saugiai ir patikimai.

SAN duomenų persiuntimas paremtas **blokiniu** I/O servisu.



SAN pajungimas

Paprasčiausia SAN pajungimo prie serverių schema.



SAN tinklo technologijos

SAN tinklui dažniausiai naudojamos komunikacijų technologijos:

- Fibre Channel
- iSCSI

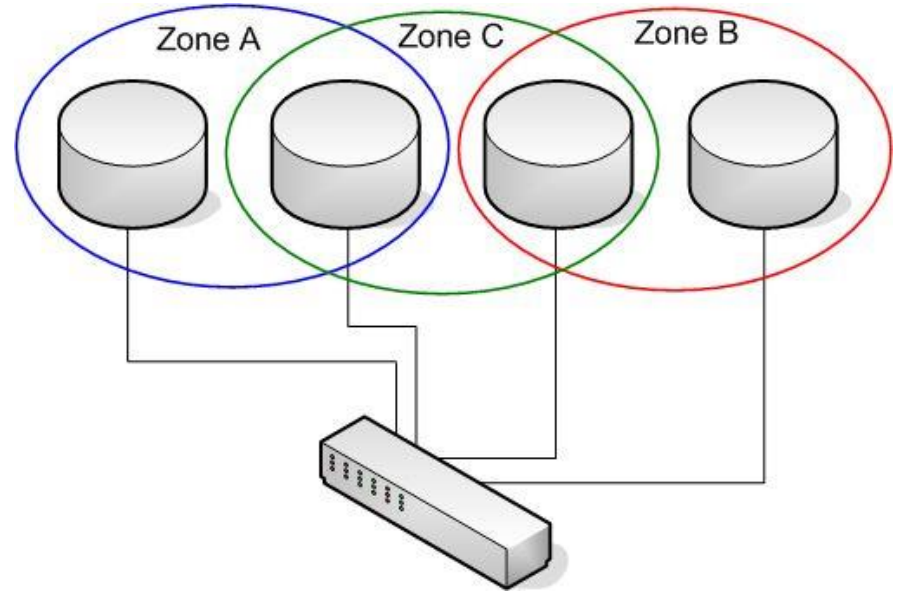
Jos apima fizinį, tinklo ir transporto lygmenis (OSI modelis) ir palaiko paslaugų klases (*Class of Services*) t.y. leidžia apibrėžti duomenų srauto perdavimo kontrolę ir kokybę.

SAN saugyklų zonos

Siekiant užtikrinti duomenų saugumą t.y. atskirti kritinius, svarbius ar mažiau svarbius duomenis, SAN naudoja diskų skirstymą į zonas. Zonai galima apibrėžti skirtingas teisės vartotojams.

Dažniausiai naudojamos komutuojamos zonos, kurios skirstomos į:

- Soft zoning
- Hard zoning



SAN zonos

- *Hard zoning* atveju z**onos apibrėžiamos naudojant SAN komutatoriaus portus**. Tokia konfigūracija reikalauja, kad duomenų srautai būtinai praeitų per komutatorių tam, kad galima būtų juos reguliuoti.
- *Soft zoning* skirstymas remiasi įrenginių **grupavimu pagal WWN** (World Wide Name t.y. unikalūs FC įrenginių vardai), o ne pagal portus, kaip *Hard zoning* atveju.
- **Soft zoning pranašumas** – lankstumas pernešant įrenginį iš vieno komutatoriaus prie kito.
- **Soft zoning trūkumas** – mažiau saugus, nes pakeitus paketo antraštės informaciją, galima patekti į kitą zoną.

LUN maskavimas

- LUN (logical unit number) – tai unikalus SCSI (FC) įrenginio identifikatorius. Pvz. */dev/dsk/c1t2d3s4*
- LUN maskavimas – tai autorizuoto priėjimo prie LUN metodas, kai serveriams priskiriami tik tam tikri LUN, su kuriais jis gali dirbti.
- LUN maskavimas gali būti realizuotas:
  - HBA
  - Tiltuose (bridges)
  - Maršrutizatoriuose (routers)
  - RAID kontroleriuose

SAN nauda

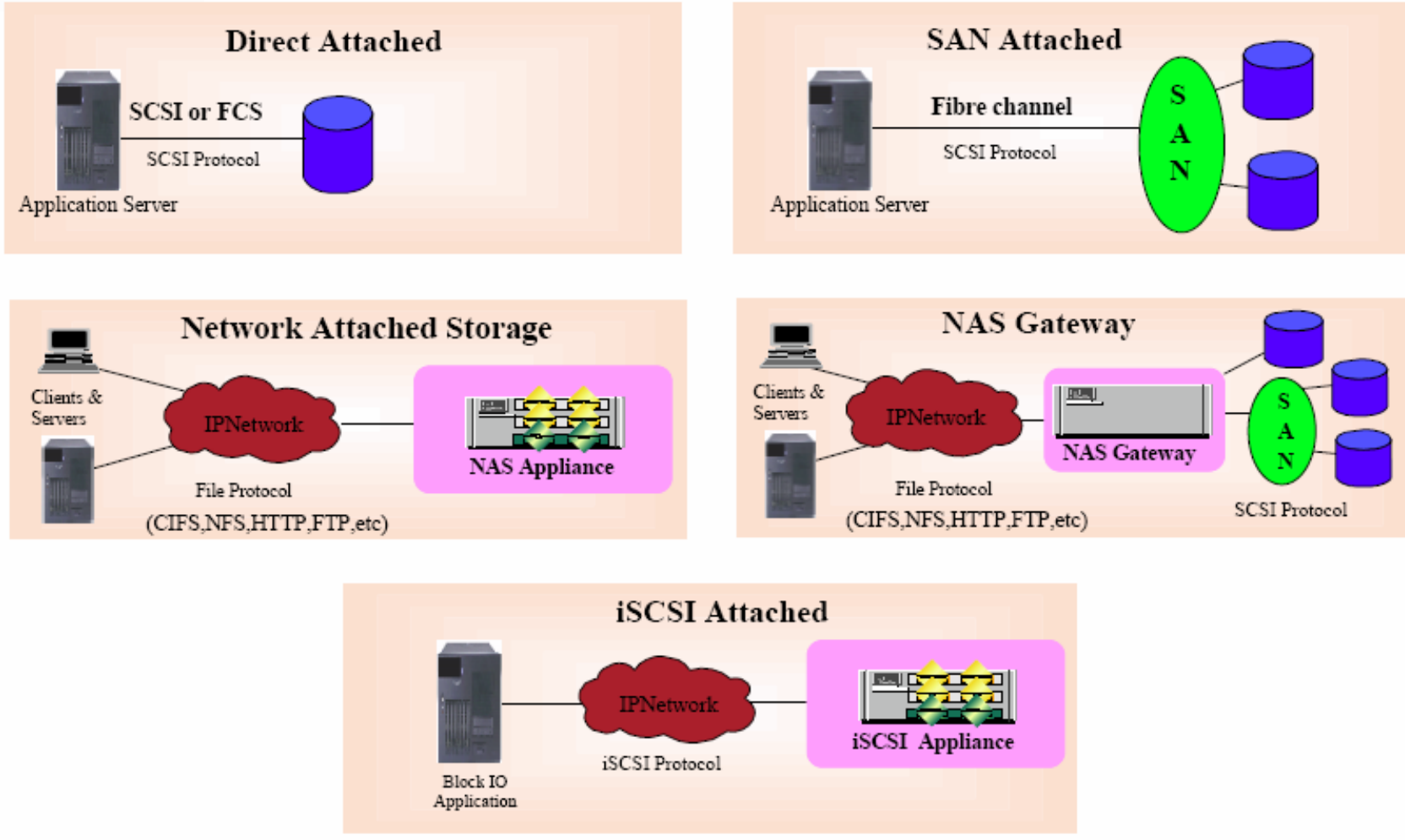
- **Geresnis pasiekiamumas**: Saugyklos nepriklausomos nuo aplikacijų bei pasiekiamos skirtingais keliais (dėl SAN tinko topologijos). Tai užtikrina didesnį patikimumą, pasiekiamumą.

- **Didesnis našumas**: Saugyklų apkrovimas nepriklauso nuo serverių apkrovimo. Naudojamas atskiras tinklas.

- **Centralizuotas ir konsoliduotas saugojimas**: paprastesnis valdymas, plėtimas, didesnis pasiekiamumas ir patikimumas.

- **Duomenų persiuntimas į nuotolines vietas**: nuotolinės duomenų kopijos leidžia apsisaugoti nuo nelaimingų įvykių ir piktybiško atakavimo.

Saugyklos trumpai



IP storage (IP saugyklos)

Internetas ir dauguma didžiųjų tinklų paremti TCP/IP protokolu naudoja **failų** persiuntimo principą. Tai apribojimas DAS ir SAN saugykloms, kadangi jose naudojamas **blokinis** I/O principas.

Tam, kad integruoti minėtas saugyklas į IP tinklą, naudojami specialūs transporto protokolai:

- iSCSI - Internet SCSI
- iFCP - Internet Fibre Channel Protocol
- FCIP - Fibre Channel over IP

IP storage (IP saugyklos)

- **Internet Small Computer Systems Interface (iSCSI)** protokolas apibrėžia taisykles kaip turi būti persiunčiami blokai per TCP/IP tinklą inkapsuliuojant SCSI komandas.
- **Fibre Channel over TCP/IP (FCIP)** -tai mechanizmas, sudarantis tunelį *Fibre Channel over IP-based* tinklui. Tai leidžia sujungti Fibre Channel SAN saugyklas, su TCP/IP naudojant papildomą sublygmenį transporto protokole.
- **Internet Fibre Channel Protocol (iFCP)** palaiko Fibre Channel Layer 4 FCP over TCP/IP. Tai lyg vartų protokolas, kur TCP/IP komutavimo ir maršrutizavimo komponentai pakeičia, praplečia Fibre Channel fabric.

iSCSI

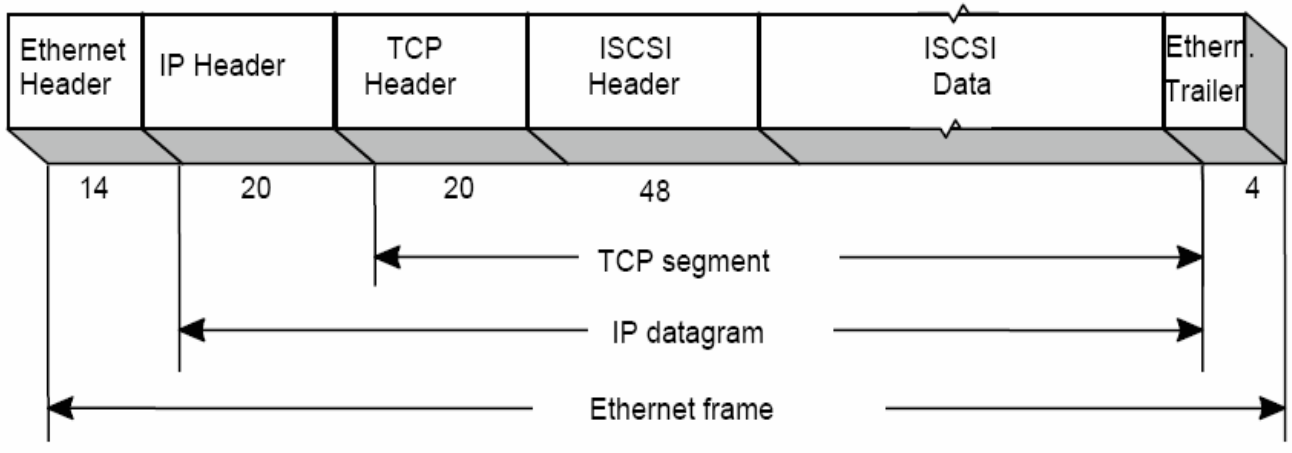
iSCSI – tai komunikacinis protokolas skirtas IP tinklu perduoti SCSI komandas ir duomenų blokus.

Fiziniame lygmenyje iSCSI palaiko Gigabit Ethernet, todėl gali būti tiesiogiai jungiamas į tokį tinklą.

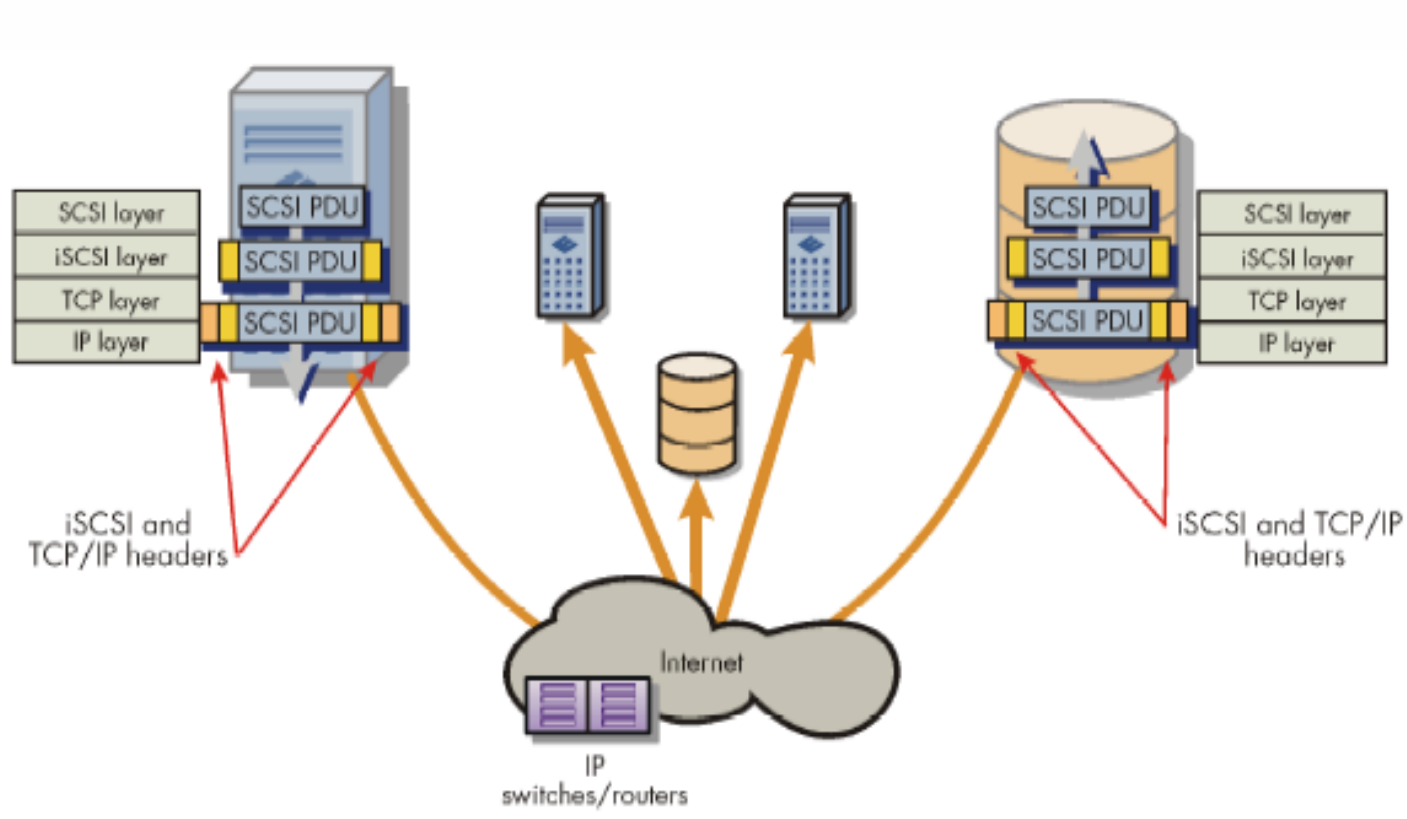
iSCSI nustato taisykles, kaip persiųsti duomenų blokus, per TCP/IP tinklą.

iSCSI leidžia SCSI-3 komandas inkapsuliuoti į TCP/IP paketą ir išsiųsti IP tinklu.

iSCSI protokolas turi būti palaikomas siuntėjo ir gavėjo pusėse.



iSCSI protokolo lygmenys



iSCSI komunikacijos apkrauna Target įrenginio CPU, todėl dalis apkrovos t.y. paketų inkapsuliacija perkeliama į HBA.

Tai vadinama **TCP offload engine** technologija (TOE).

iSCSI komunikacijų principas

iSCSI turi kliento/serverio architektūrą, čia vadinamą Initiator/Target sistema.

Initiator – tai klientinis įrenginys t.y. serveris, kuri **inicijuoja duomenų poreikį** t.y. reikalauja blokinio lygmens duomenų, kurie turi būti persiųsti IP tinklu.

iSCSI target – tai saugykla, kuris teikia blokinio lygmens priėjimą prie diskų ir juostų.

Skirtumas tarp kliento/serverio architektūros ir Initiator/Target sistemos:

- kliento/serverio sistemoje vienas serveris aptarnauja daug klientų vienu metu
- initiator/target sistemoje tik vienas iSCSI initiator gali kalbėtis su iSCSI target vienu metu (one-to-one).

Software Initiators

- *Cisco iSCSI Driver* – vienas pirmųjų iSCSI initiator
- *IBM iSCSI Software Initiator for AIX*
- *HP HP-UX iSCSI Software Initiator*
- *Microsoft iSCSI Software Initiator for Windows*

iSCSI adresų sistema

iSCSI naudojasi globalia IP adresų schema.

iSCSI įrenginiai turi dviejų tipų identifikatorius: iSCSI vardus ir iSCSI adresus.
Visi iSCSI initiators/targets turi pastovų autorizuotą iSCSI vardą (IQN), kuris identifikuoja įrenginį pagal jo vietą arba IP adresą. Specifikacija nustato RFC 3720.

iSCSI adresas nustato įrenginio vietą ir yra pririštas prie IP adreso, porto numerio, iSCSI įrenginio vardo. Pavyzdys:

iSCSI adreso formatas:
iSCSI://<domain name>:<port>/<iSCSI name>
iSCSI://diskfarm1.acme.com:80/fqn.com.disk-vendor.diskarray.45678

iSCSI vardas:
fqn.com.disk-vendor.diskarray.45678

iSCSI saugos problema

Problema

iSCSI protokole autentifikacijai naudojamas CHAP protokolas (*Chalenge-handshake authentication protocol*), bet tolesni duomenų persiuntimai atliekami atviru tekstu.

Sprendimas – naudoti saugius tunelius, VPN, IPsec.

CHAP protokolas

- **Challenge-Handshake Authentication Protocol (CHAP)** - autentifikuoja vartotojus arba tinklus. CHAP specifikacija apibrėžta RFC 1994.
- CHAP autentifikacijos schema pagrįsta PPP protokolu,

- CHAP leidžia patikrinti slaptažodį nesiunčiant jo atviru tekstu tinkle.
- Slaptažodis turi būti žinomas klientui ir serveriui, o autentifikavimas **trigubo rankų paspaudimo** principu:
  - Autentifikatorius (iniciatorius) siunčia žinutę
  - Gavėjas atsako išsiųsdamas hash reikšmę iniciatoriui
  - Iniciatorius sulygina gautą reikšmę su savo suskaičiuota reikšme.

FCIP (FC over IP protokolas)

FCIP - tai FC paketų perdavimo metodas, kai Fibre Channel paketai inkapsuliuojami ir transportuojami TCP/IP tinklu. Tai leidžia panaudoti aplikacijas, kurios buvo pritaikytos Fibre Channel SAN, vykdyti ir IP tinkle. Šis protokolo pagalba išplečiamas FC SAN panaudojimas IP tinkle.

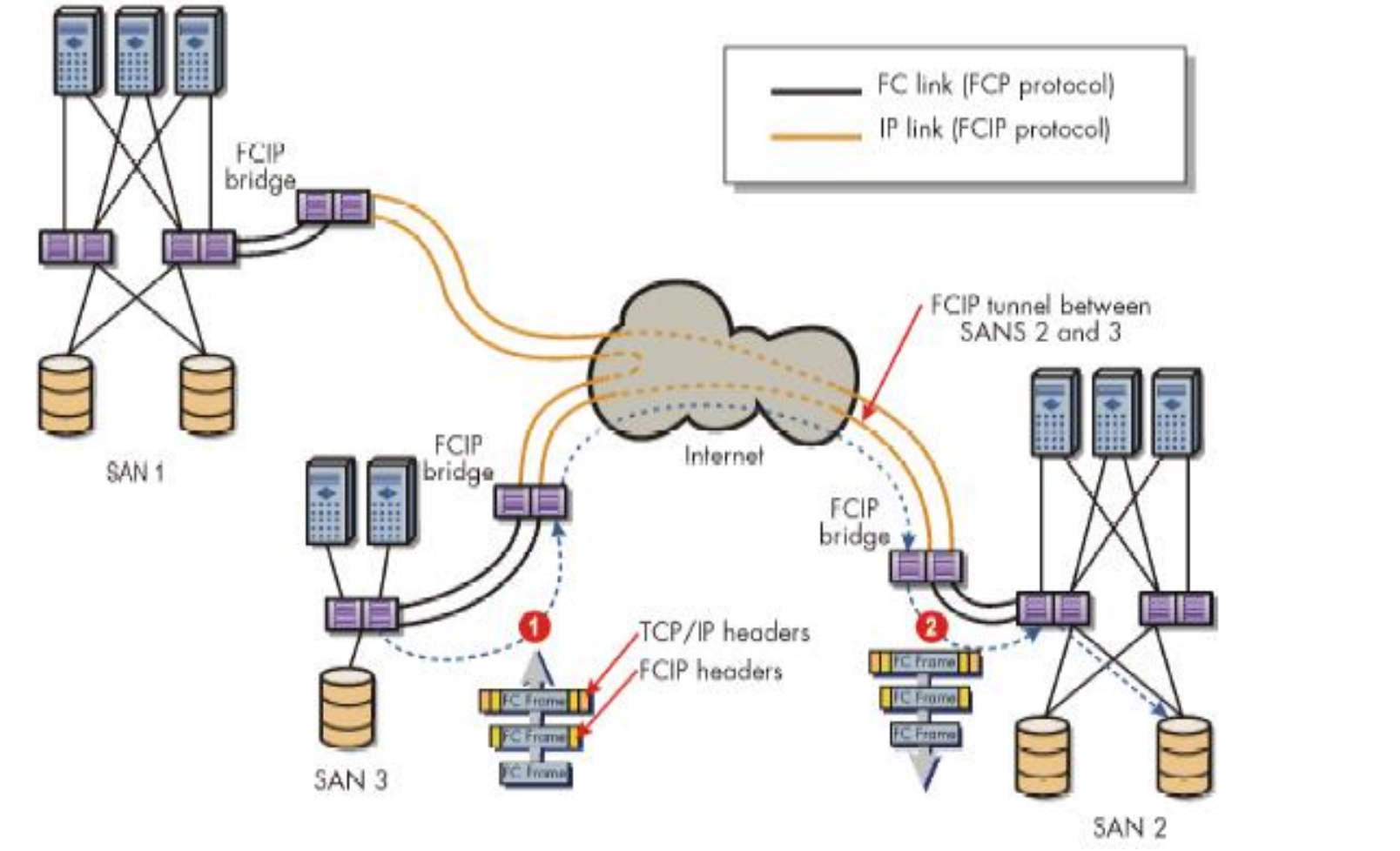
FCIP – tai tunelio sudarymo protokolas, kuris naudoja TCP/IP kaip transportą, išlaikant nepaliestą (neišgadintą) Fibre Channel servisą.

FCIP remiasi IP-based tinko servisu valdant perkrovimus ir administruojant tinklą.

FCIP remiasi TCP/IP ir Fibre Channel metodais atstatinėjant duomenis ir analizuojant duomenų perdavimo klaidas.

FCIP vartai naudojami prijungiant Fibre Channel SAN prie IP tinklų.

FCIP



1. FC frame is encapsulated into FCIP packet, then into TCP/IP packet, and sent over FCIP tunnel to destination device in SAN 2.
2. FC frame is unencapsulated and forwarded to correct local device in SAN 2.

iFCP – internet FC protokolas

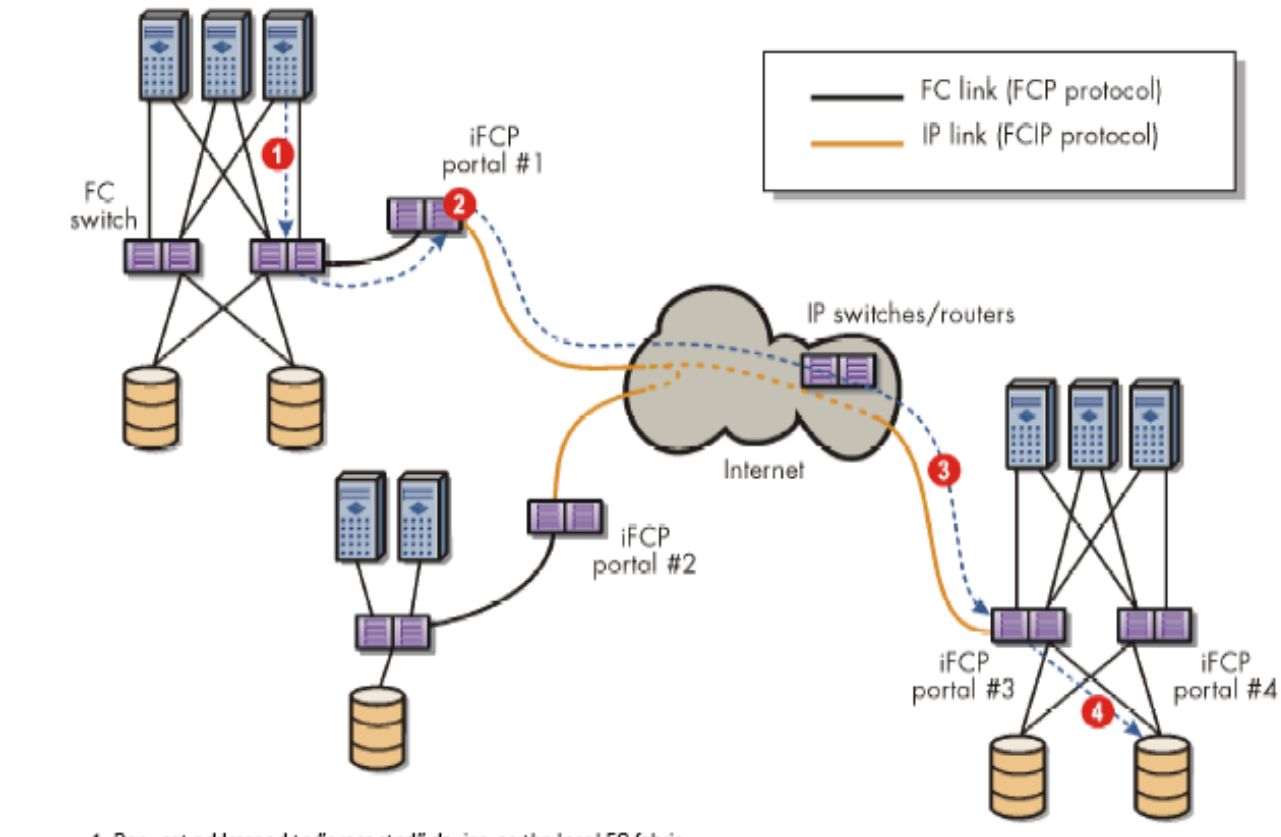
Kaip FCIP, **iFCP inkapsuliuoja Fibre Channel kadrus ir persiunčia juos IP tinklais**.
Pagrindinis skirtumas tarp FCIP ir iFCP protokolų - tai adresavimo schemoje.

FCIP protokolas naudoja *point-to-point* tunelį, kuris leidžia sujungti du FC SAN Etherneto pagalba ir sukurti didesnį SAN.

iFCP – tai protokolas skirtas *gateway-to-gateway* schemai. Jis sujungia FC ir IP adresus ir leidžia FC kadrams pasiekti reikiamą adresą.

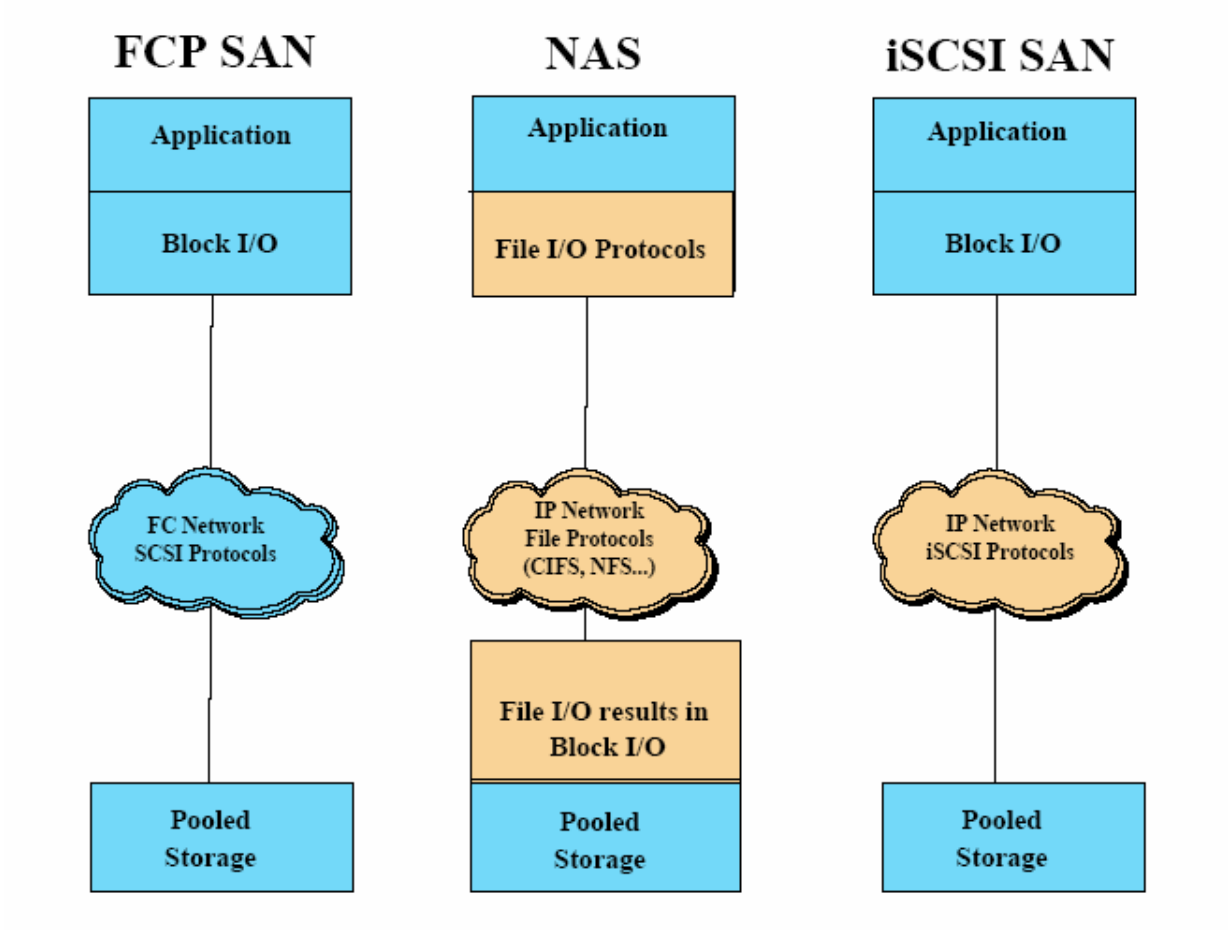
Priešingai nei FCIP protokole, iFCP adresavimo schema leidžia kiekvienam sujungtam SAN naudotis nuosava vardų erdve.

iFCP



1. Request addressed to "presented" device on the local FC fabric.
2. iFCP portal encapsulates FC frame into IP packet addressed to the appropriate remote iFCP portal IP address. The packet also contains the remote FC address of the requested device.
3. Packet is routed to remote iFCP portal.
4. iFCP portal unpackages the FC frame and forwards to correct local device. Request addressed to actual FC address of remote FC device.

iSCSI, FCP NAS palyginimas



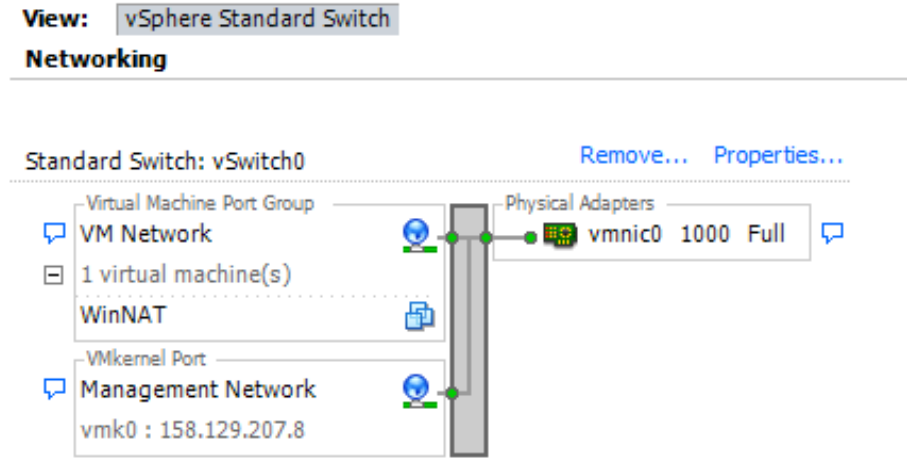
VMware ESX tinklo saugykla

VMFS

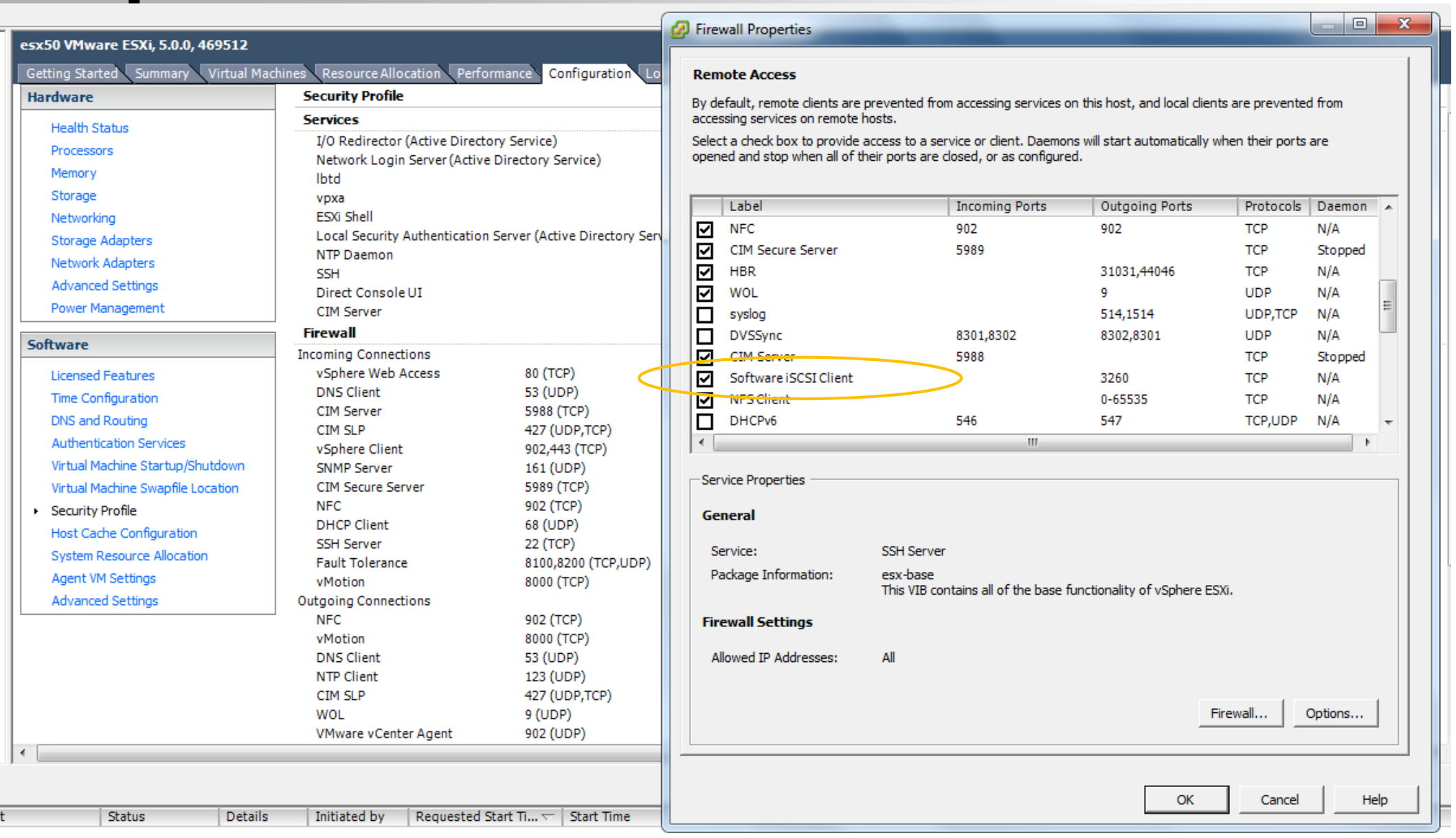
- Failų saugojimui naudojama VMFS (virtual machine file system).
- Maksimalus VMFS dydis viename LUN – 2TB, bet išplečiama iki 64 TB
- LVM gali agreguoti LUN formuodamas didesnę FS.
  - Pvz. norint sukurti 6TB VMFS, sukuriame 3 x 2TB ir sujungiame.
- Maksimalus failo dydis – 2TB
- VMFS – klasterinė failų sistema. Naudojami metaduomenys informacijai apie failus saugojimui.

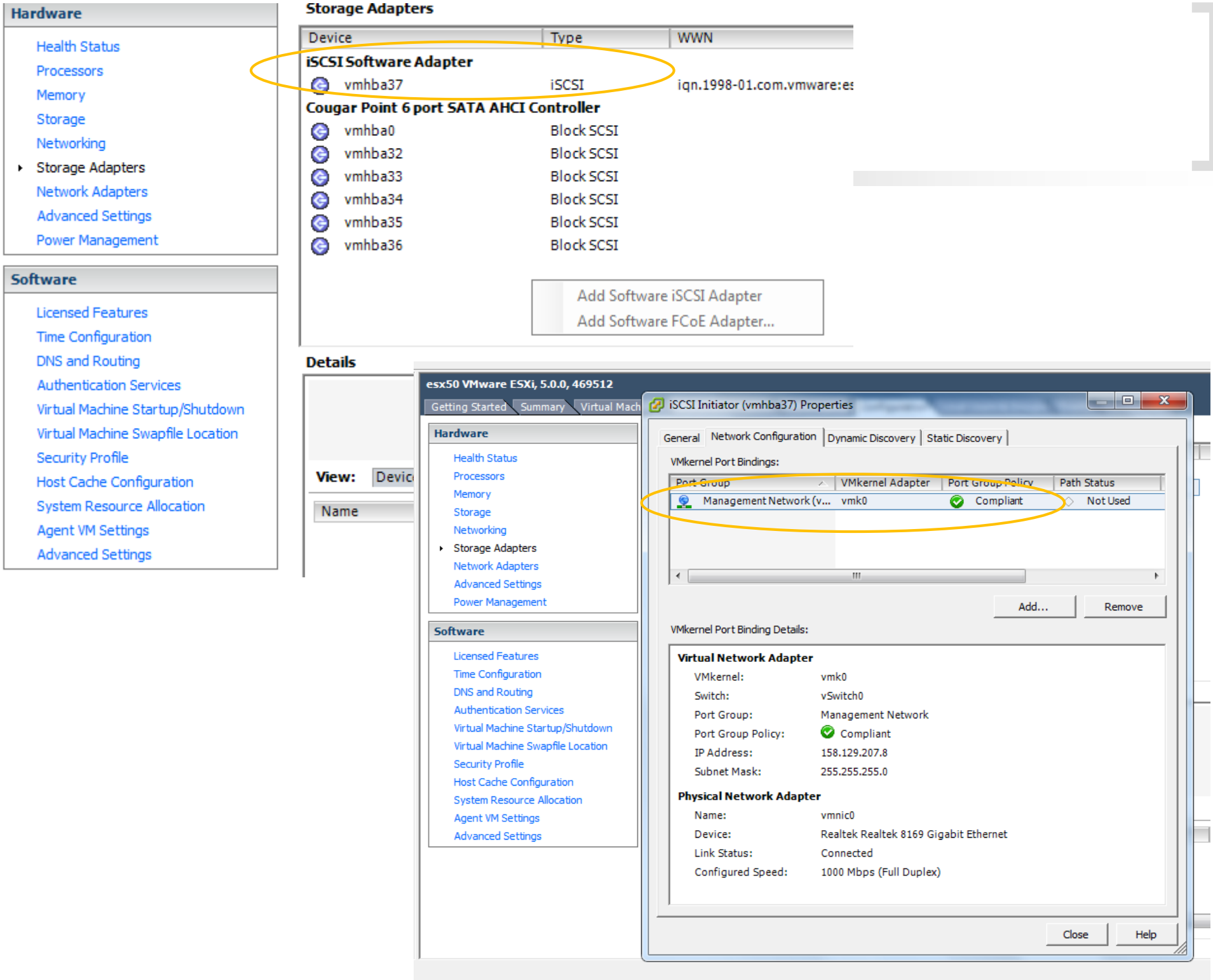
iSCSI saugykla

- Palaiko aparatūrinį ir programinį (*vmkiscsid demonas*) iSCSI iniciavimą branduolio VMkernel lygmenyje.
- iSCSI prijungimas vyksta per VMkernel portų grupę.
- Turi būti atidarytas
  3260 portas,
  konfigūruojant
  ESXi Firewall



ESX firewall konfigūravimas



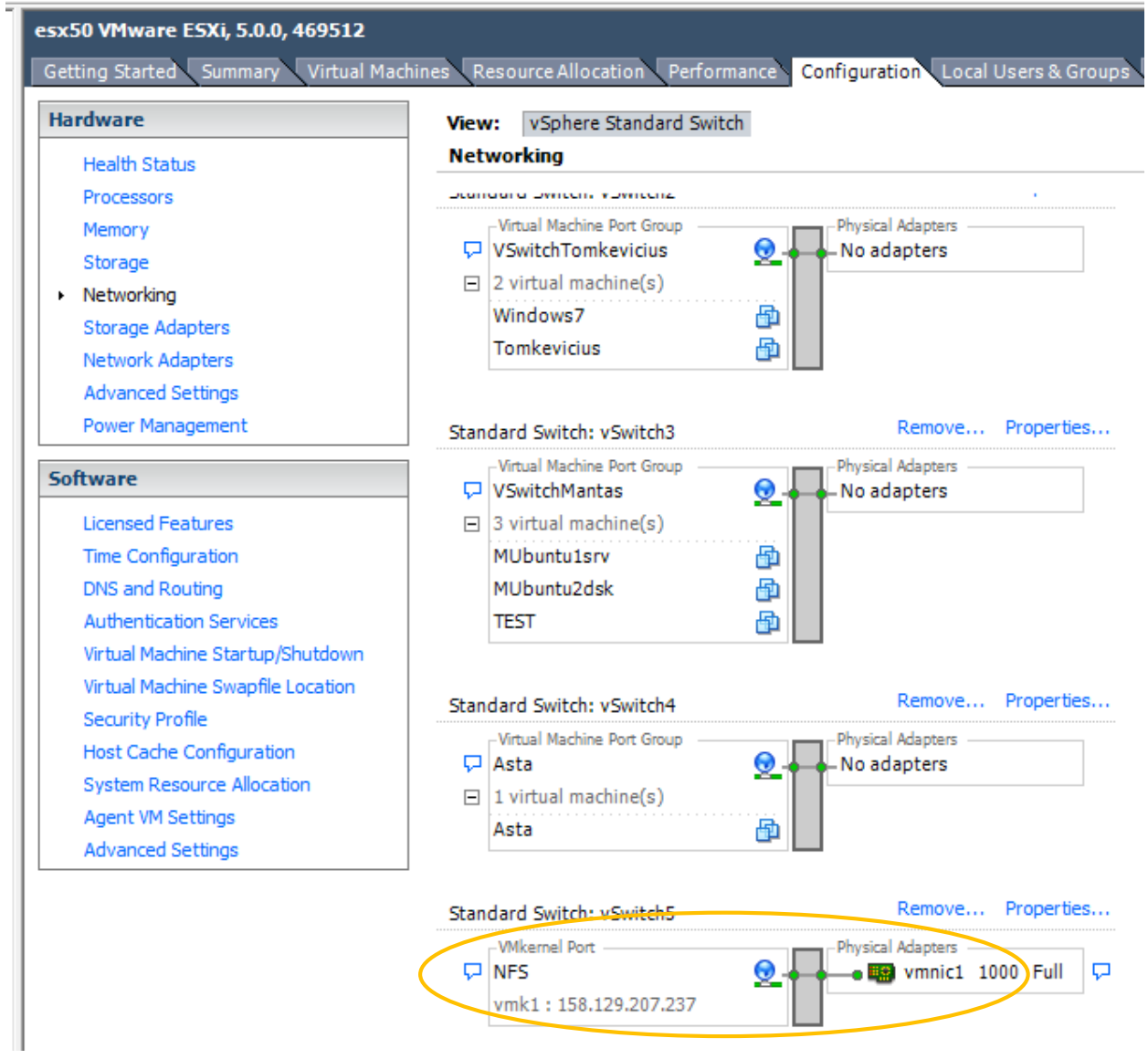

Hardware
Health Status
Processors
Memory
Storage
Networking
Storage Adapters
Network Adapters
Advanced Settings
Power Management
Software
Licensed Features
Time Configuration
DNS and Routing
Authentication Services
Virtual Machine Startup/Shutdown
Virtual Machine Swapfile Location
Security Profile
Host Cache Configuration
System Resource Allocation
Agent VM Settings
Advanced Settings
Storage Adapters
Device
Type
WWN
iSCSI Software Adapter
vmhba37
iSCSI
iqn.1998-01.com.vmware:es
Cougar Point 6 port SATA AHCI Controller
vmhba0
Block SCSI
vmhba32
Block SCSI
vmhba33
Block SCSI
vmhba34
Block SCSI
vmhba35
Block SCSI
vmhba36
Block SCSI
Add Software iSCSI Adapter
Add Software FCoE Adapter...
Details
View:
Devic
Name
esx50 VMware ESXi, 5.0.0, 469512
Getting Started
Summary
Virtual Mach
Hardware
Health Status
Processors
Memory
Storage
Networking
Storage Adapters
Network Adapters
Advanced Settings
Power Management
Software
Licensed Features
Time Configuration
DNS and Routing
Authentication Services
Virtual Machine Startup/Shutdown
Virtual Machine Swapfile Location
Security Profile
Host Cache Configuration
System Resource Allocation
Agent VM Settings
Advanced Settings
iSCSI Initiator (vmhba37) Properties
General
Network Configuration
Dynamic Discovery
Static Discovery
VMkernel Port Bindings:
Port Group
VMkernel Adapter
Port Group Policy
Path Status
Management Network (v...
vmk0
Compliant
Not Used
Add...
Remove
VMkernel Port Binding Details:
Virtual Network Adapter
VMkernel:
vmk0
Switch:
vSwitch0
Port Group:
Management Network
Port Group Policy:
Compliant
IP Address:
158.129.207.8
Subnet Mask:
255.255.255.0
Physical Network Adapter
Name:
vmnic0
Device:
Realtek Realtek 8169 Gigabit Ethernet
Link Status:
Connected
Configured Speed:
1000 Mbps (Full Duplex)
Close
Help

NFS saugykla

- NFS klientas yra integruotas į ESXi ir leidžia prisijungti prie NFS serverio.
- NFS saugyklos galimybės:
  - Naudoti Vmotion
  - Sukurti ir laikyti VM NFS saugykloje
  - Saugoti VM šablonus ir ISO atvaizdus
  - Užkrauti VM iš NFS saugyklos
- VMkernel komutatorius naudojamas NFS saugyklai prijungti. VMkernel portas turi pasiekti NFS serverį per tinklą.

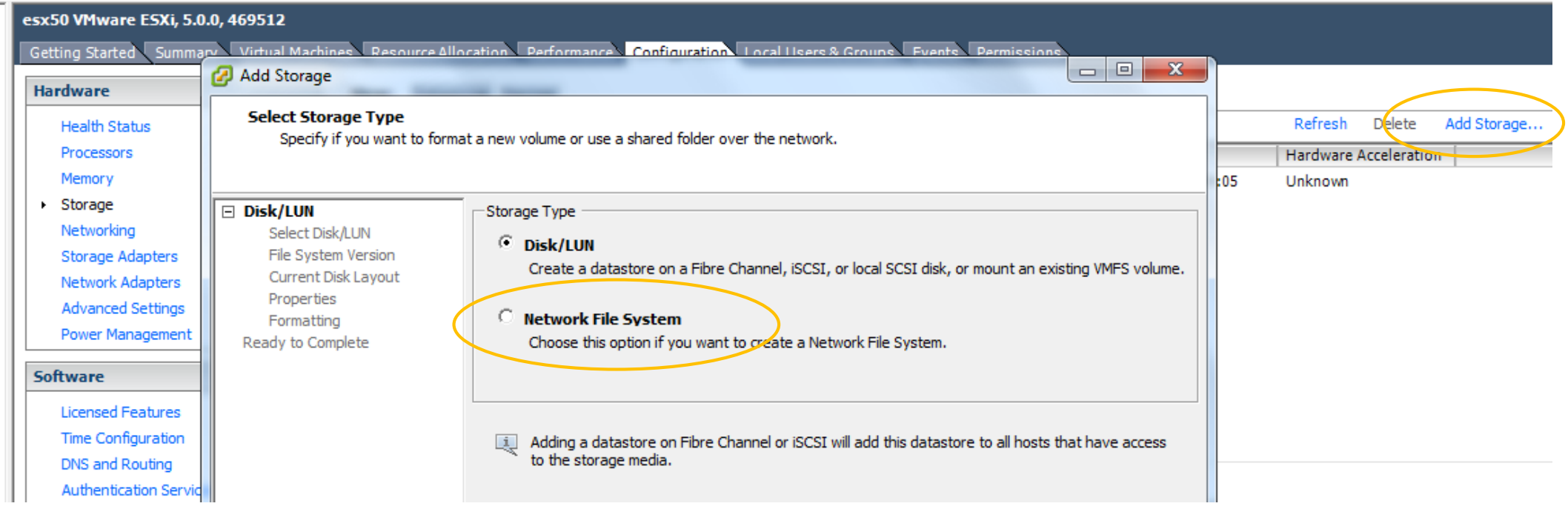
NFS konfigūravimas

1. Sukuriame naują VMkernel switch ir priskiriame naują IP adresą, skirtingą nei turi service console.
2. Prijungiame NFS katalogą konfiguruodami „Storage“ skyrių



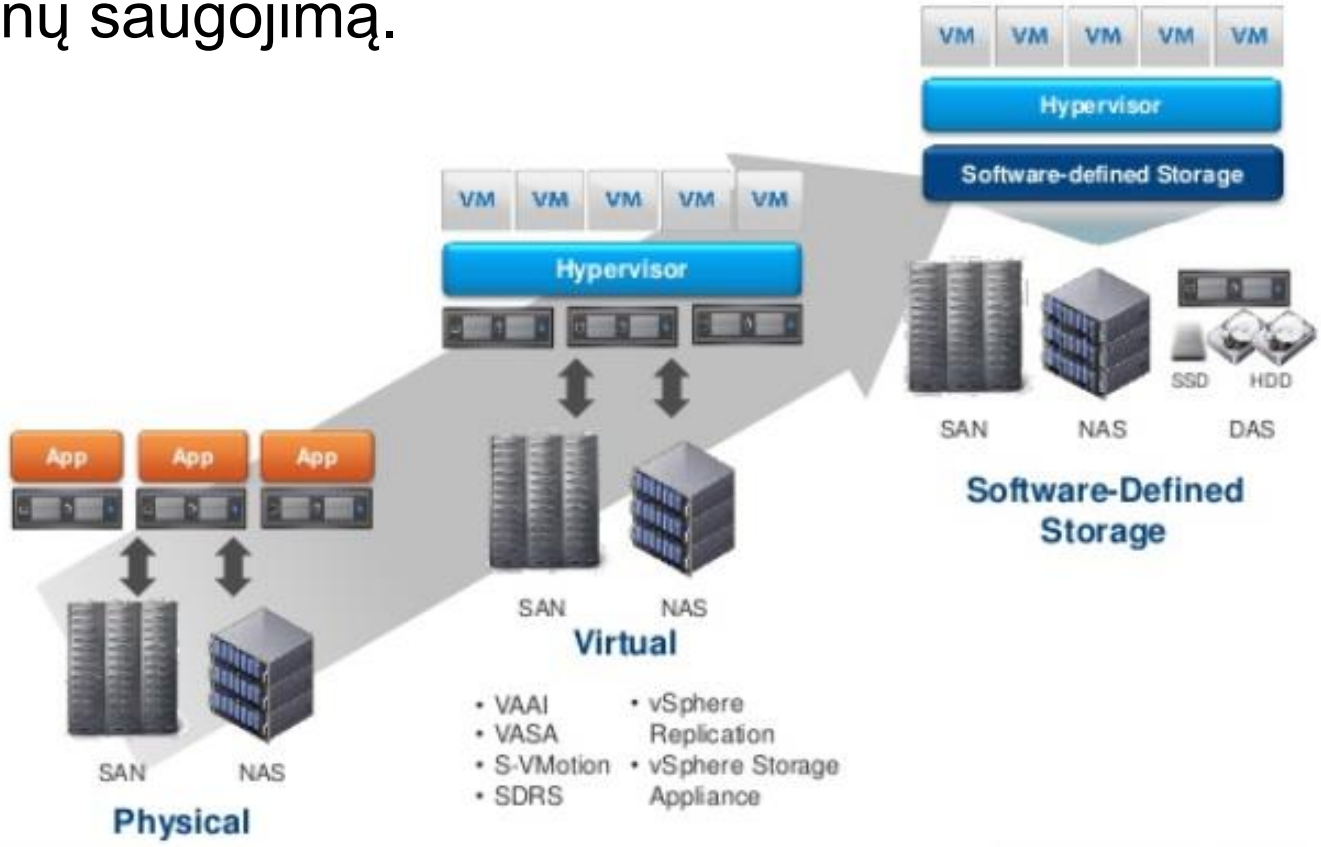
Saugyklų montavimas

Tinklo saugyklos montuojamos pasirinkus *Add storage* iš Storage grupės.



Software Defined Storage

SDS – tai duomenų saugyklų virtualizavimo technologija, kurios esmė duomenų saugojimą ir apdorojimą perkelti nuo specializuotų saugyklų į nebrangius x86 architektūra paremtus serverius, naudojant atskirą programinį sluoksnį kuris atsakingas už duomenų saugojimą.



Software Defined Storage

SDS modeliai

1. Programinis sluoksnis, kuris virtualizuoja duomenų saugyklos resursus (DataCore SAN Symphony, IBM SVC)

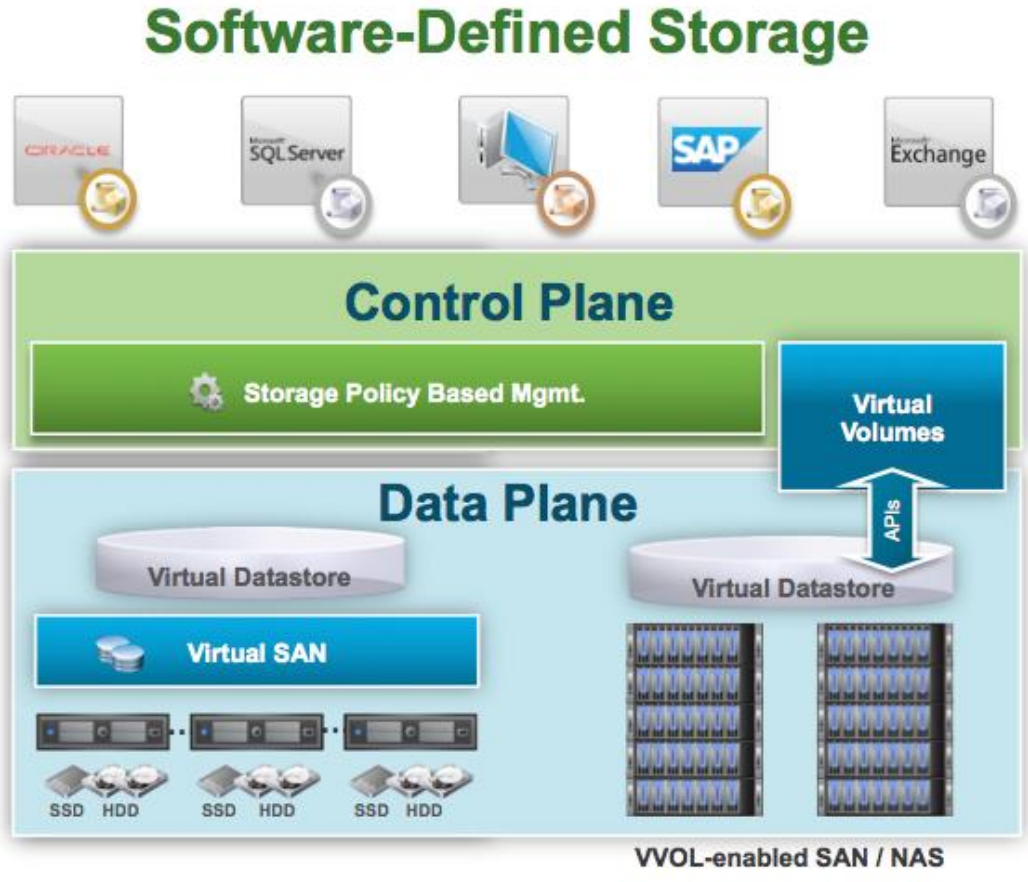
   Tikslas – apjungti skirtingas SAN, NAS, DAS tipo saugyklas į virtualią saugyklą ir ją pateikti VM‘ams.

2. Programinis sluoksnis apjungiantis skirtinguose serveriuose esančius HDD ir SSD diskus suformuojant virtualią saugyklą. (EMC ScaleIO, VMWare vSAN).

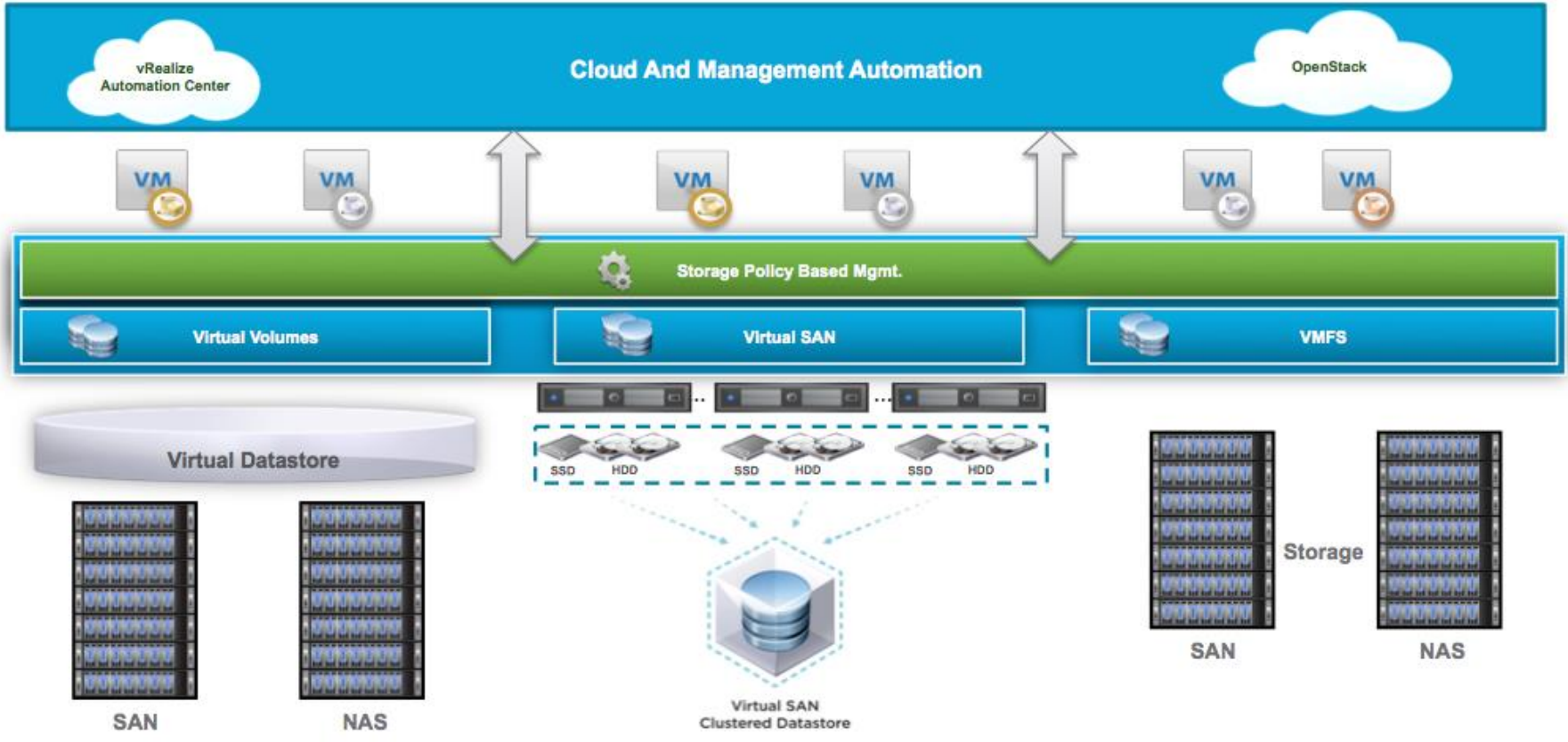
   Serveriuose esantys diskai grupuojami į telkinį, kuris valdomas programine įranga. Dalis grupės serverių atlieka SAN valdiklių funkciją, o kiti mazgai naudojami duomenų saugojimui.
   Tie patys serveriai gali skirti resursus ir VM‘ams (CPU, RAM, NIC ...)
   t.y. būti naudojami VM paleidimui/

Software Defined Storage

Principinė SDS schema



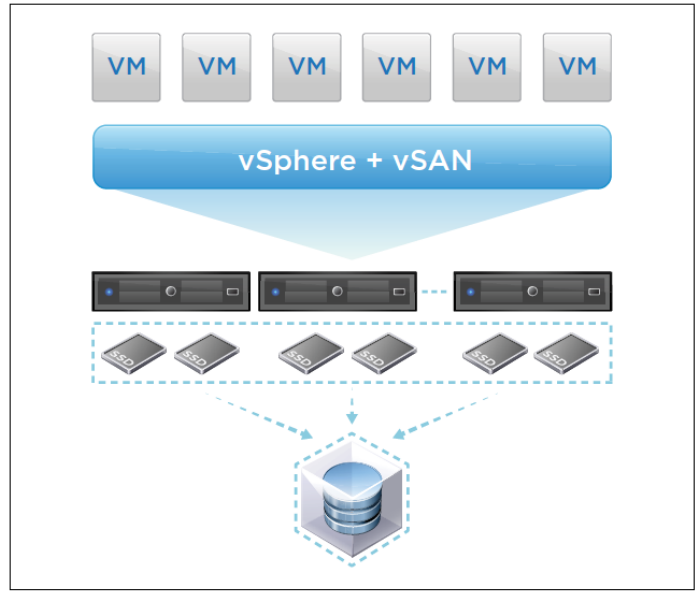
SDS valdymas



vSAN

vSAN – tai VMWare technologija, kurios pagalba galime apjungti serverių lokalius diskus į SDS saugyklą.

- Integruotas hypervisoriaus modulis
- vSAN kontroliuoja tiesioginį I/O duomenų kelią ir priima greitą duomenų sprendimą, kur turi būti talpinami duomenys
- Pasiekiamas didelis našumas neapkraunant procesoriaus ir atmintis



vSAN reikalavimai

Serveris

- 1GB NIC; 10GB NIC
- SATA/SAS HBA or RAID controller
- Bent vienas SSD (caching device)
- Bent vienas HDD/SSD duomenų saugyklai

Klasteris

- Min. 2 serverisi (max. 64 serveriai)

vSAN gali būti konfigūruojamas naudojant tik SSD diskus (all-flash) arba kaip hibridinė HDD-SSD saugykla (hybrid storage).

SDS

Efektyvumas: SDS leidžia naudoti duomenų dedublikavimas ir kompresija, realizuoti RAID kontrolerio funkcijas (RAID 5/6), leidžia pasiekti iki 10 kartų geresnį saugyklos vietos išnaudojimą, mažinti kainą.

Plečiamumas: SDS turi paskirstytą architektūrą, kuri leidžia į klasterį prijungti iki 64 serverių. Virtualios saugyklos našumas ar talpa gali būti plečiami nepriklausomai pridedant papildomą serverį.

SDS

Automatizavimas: VM saugyklos resursų pateikimas ir automatizavimas atliekamas naudojant VM-centric policy. SDS turi apkrovos balansavimo mechanizmą leidžiantį tolygiai paskirstyti apkrovą serveriams ir tolygiai pildyti diskus.

Flash-Optimized: vSAN minimizuoja saugyklos uždelsimą (storage latency) naudojant SSD diskus.