Xen Hypervisor security in VM isolation

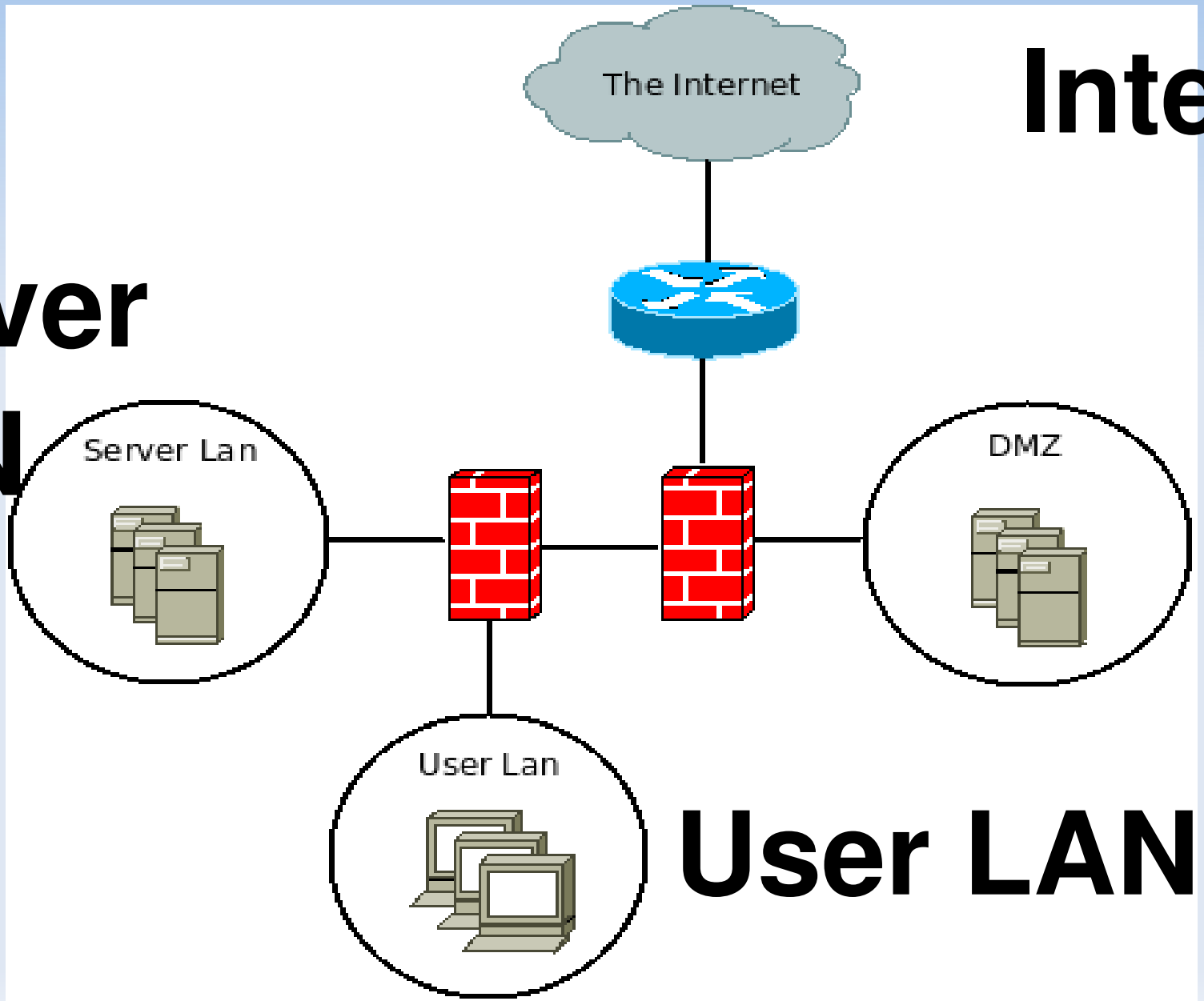
Yanick de Jong

4 February 2009

Research Question?

What are the risks involved with merging Xen servers in different segments of the network and put all virtual machines together on one machine?

Network Overview



Internet

Server LAN

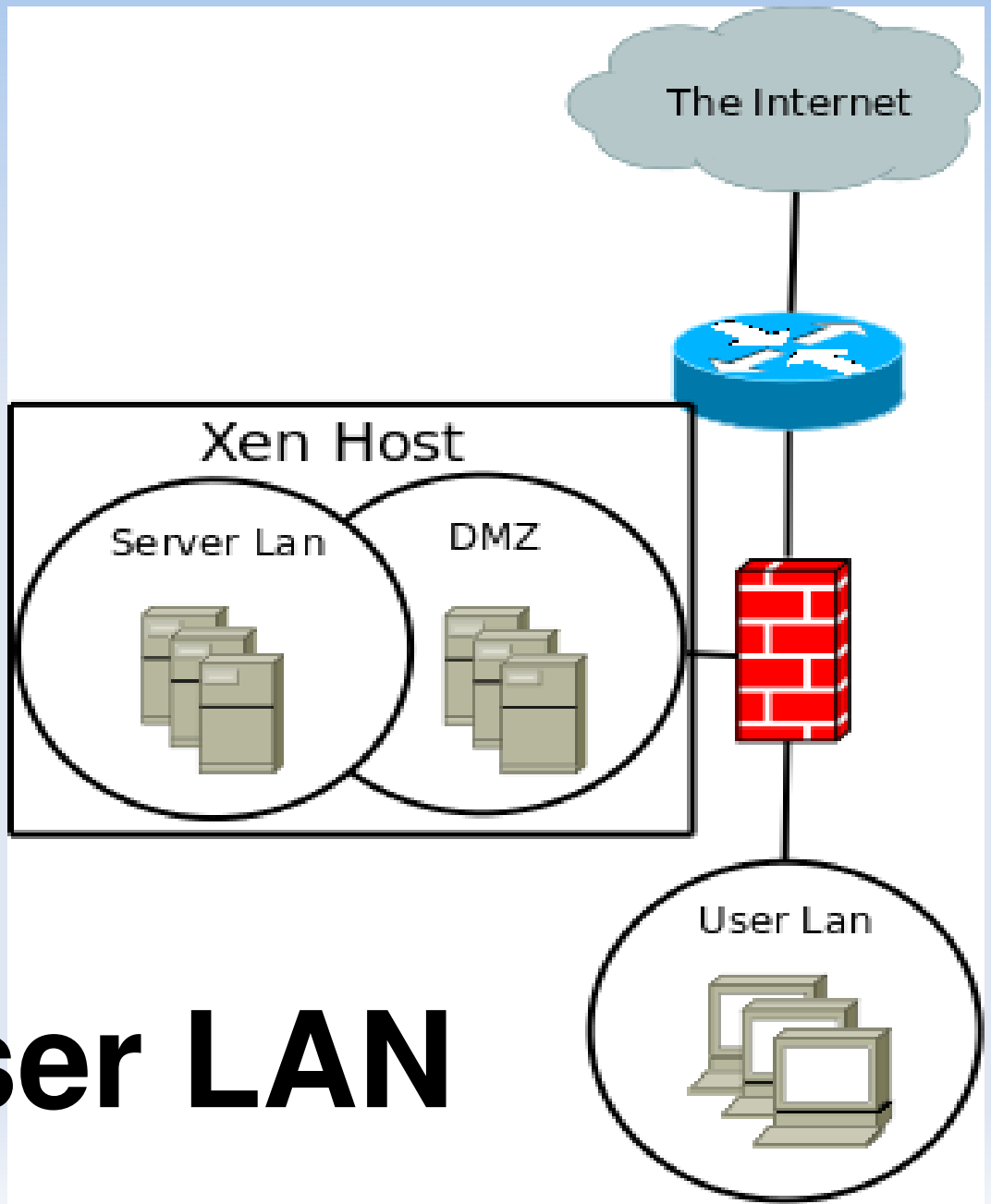
DMZ

User LAN

Network Overview

Internet

Server LAN & DMZ



User LAN

Subjects

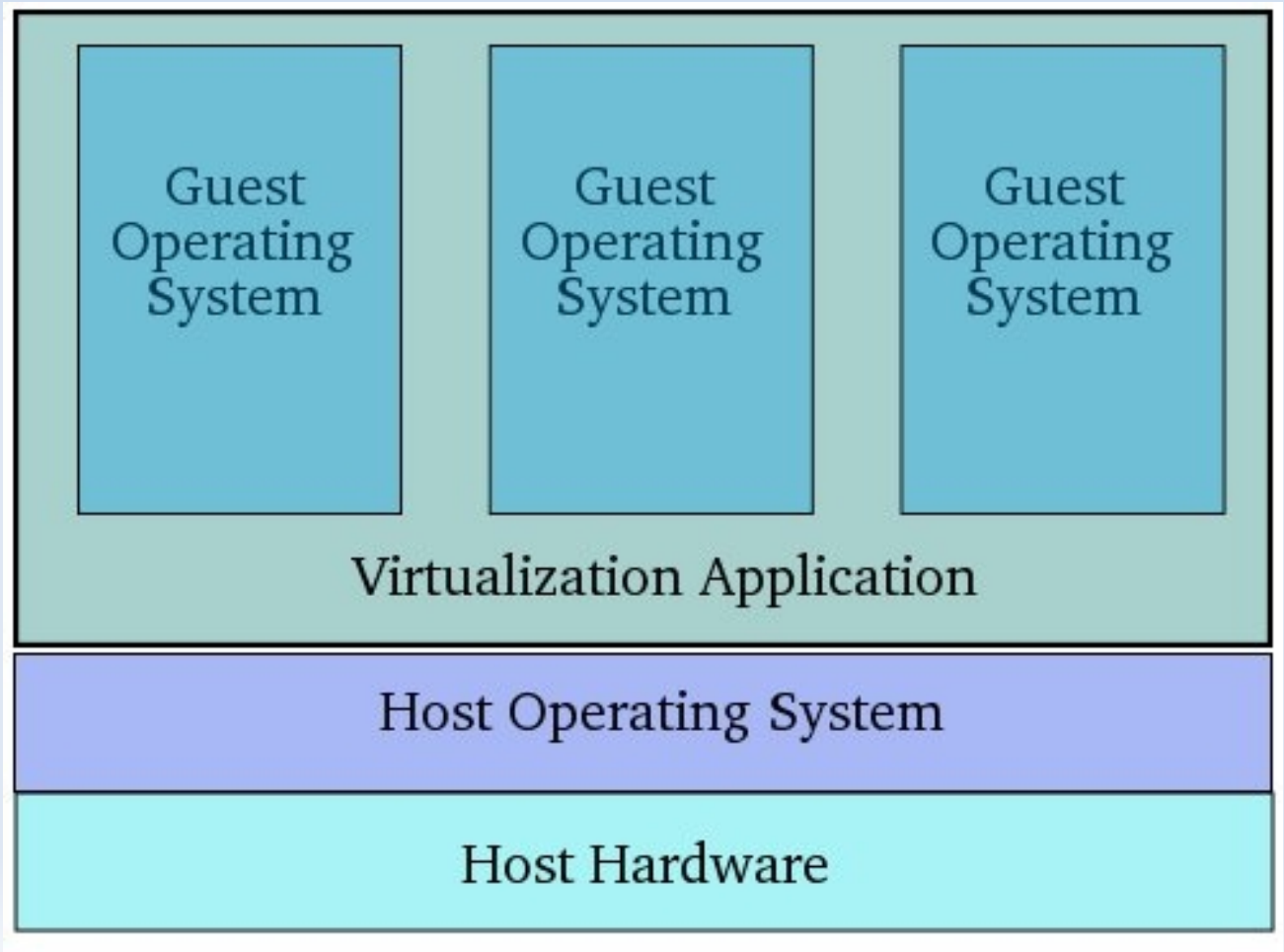
- Network
- System
- Disk allocation
- Memory
- Bridging
- DMA
- Conclusion

Network

- Defense in Depth
- Least Privilege

System (xen host)

- Single point of Failure
- Increase complexity



Virtual Machine

- Less risks
- Easy to restore

Disk Allocation

- **Writing outside allocated virtual machine diskspace**

Memory

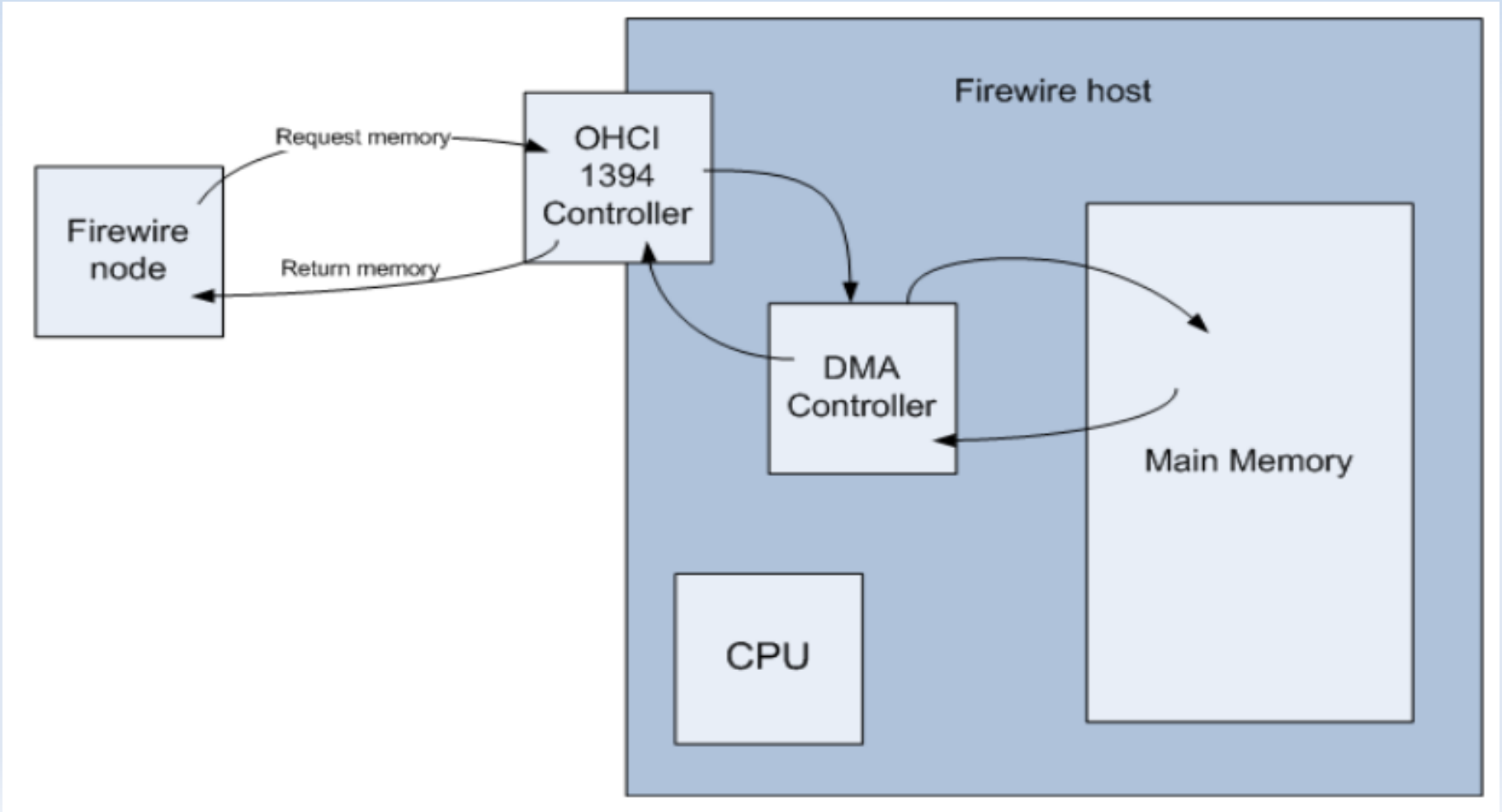
- Writing into memory
- Reading memory
- Reading memory from checkpointfile

Bridging

- All VM's on the same bridge
- VM's connected to physical networkcards
- VM's connected with vlan

DMA

- **Example – Reading memory (RAM) through the firewire port**



Conclusion

- **Network**
  - Defense in Depth
  - Least Privilege
- **Single point of failure**
  - Xen host

Questions ?