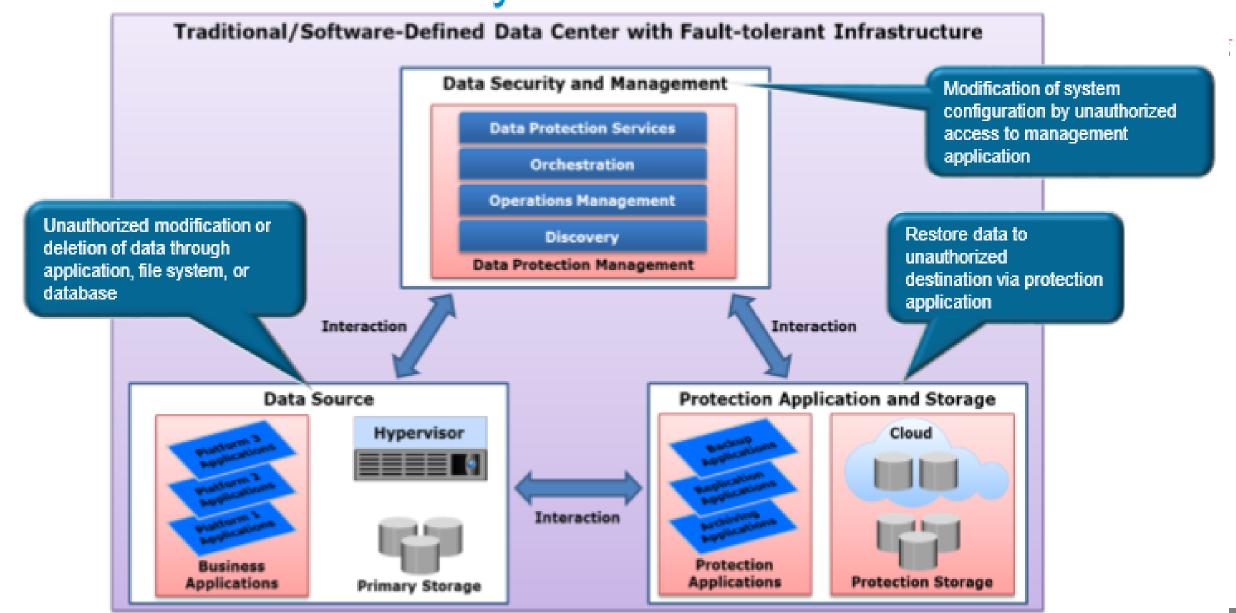


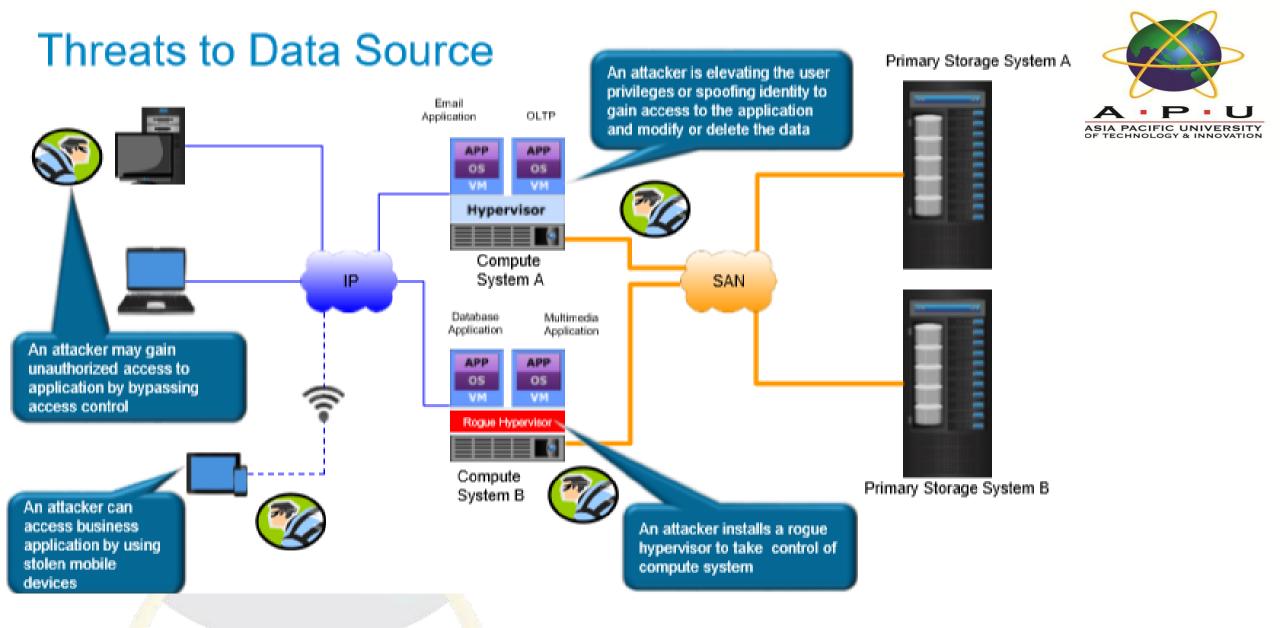
Data Protection and Management

Security

Introduction to Security Threats

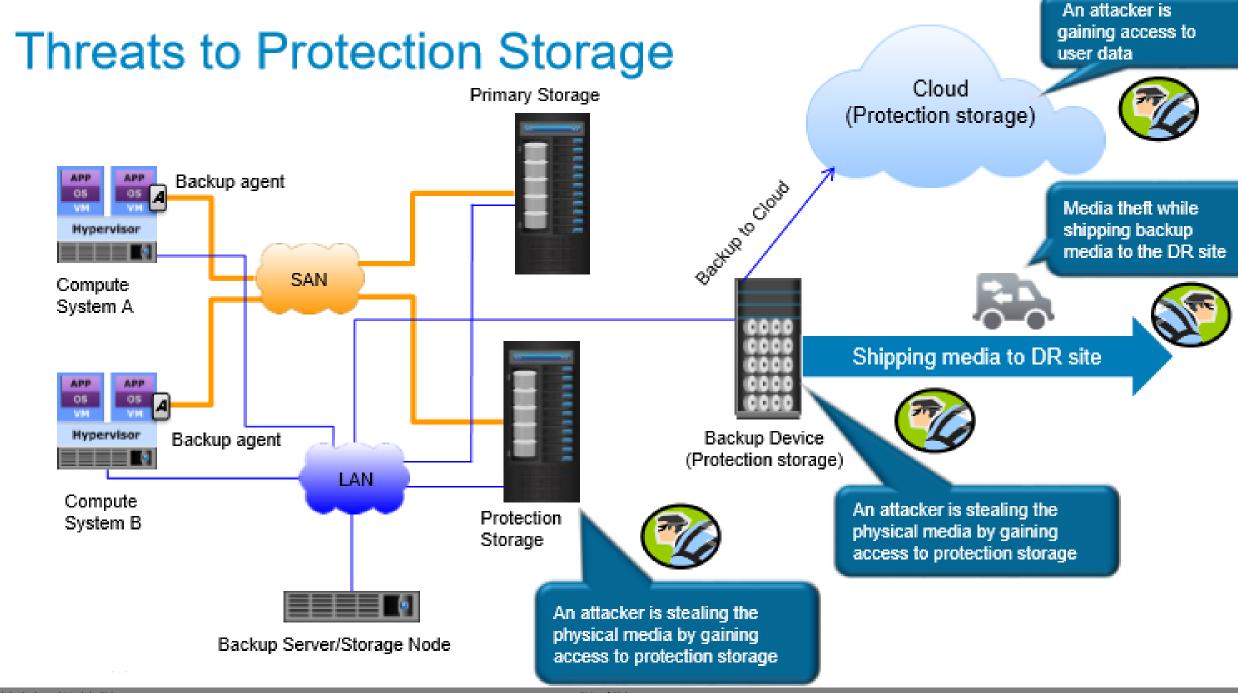


Title of shides

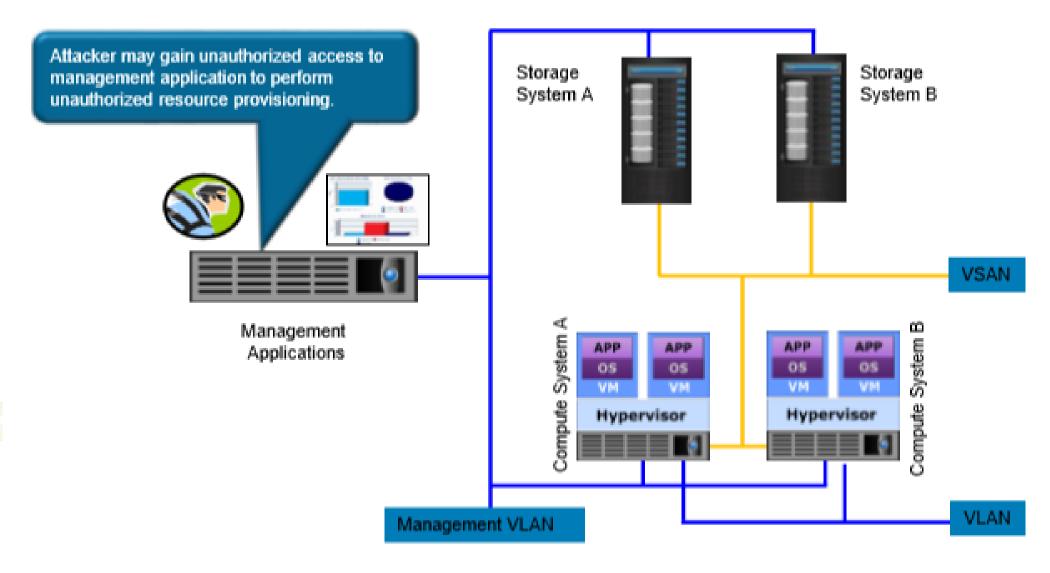


Threats to Protection Applications

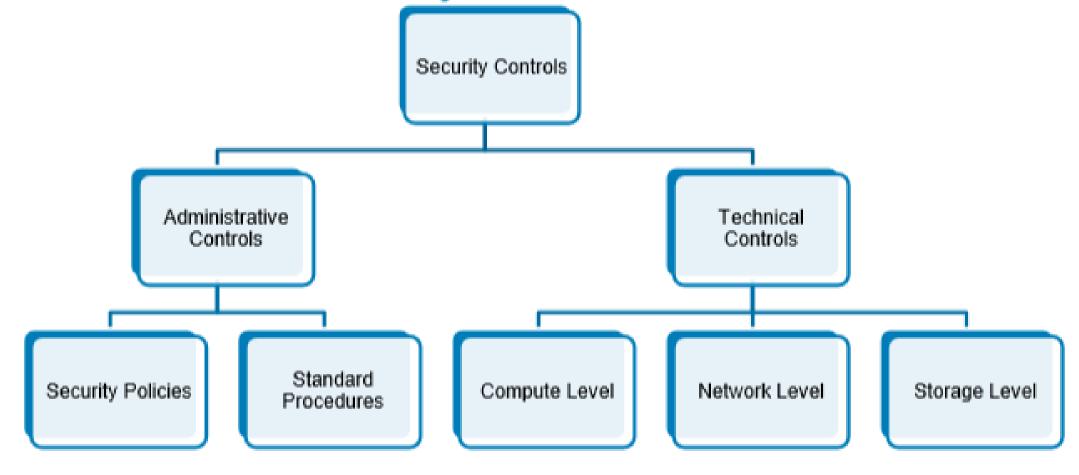
Storage System A – Replication Software Installed An attacker is elevating the user privileges or spoofing identity to perform Backup agent unauthorized remote replication Hypervisor Compute System A SAN Backup agent Hypervisor Backup Device Remote Compute System B Replication LAN An attacker is exploiting vulnerabilities in the backup application to perform data Storage System B – Replication Software Installed recovery to unauthorized compute system B Backup Server/Storage Node



Threats to Management Applications



Introduction to Security Controls



Security controls can be classified as preventive, detective, and corrective

Key Security Controls

Physical security

Identity and access management

Role-based access control

Firewall

Intrusion detection and prevention system

Virtual private network

Virtual LAN and virtual SAN

Zoning

LUN Masking

Discovery domain

Securing hypervisor

Securing management server

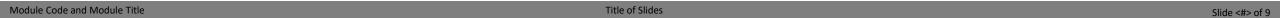
VM, OS, and application hardening

Malware protection software

Mobile device management

Data encryption

Data shredding



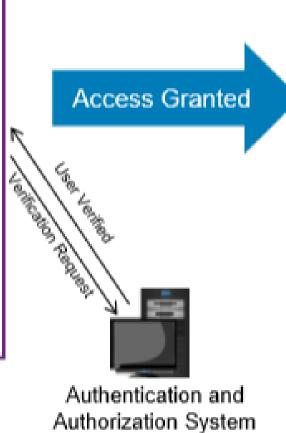
Physical Security Disable all unused devices and ports Provide 24x7x365 onsite security guard Implement biometric or security badge-based authentication Physical security controls Install surveillance cameras Install sensors and alarms

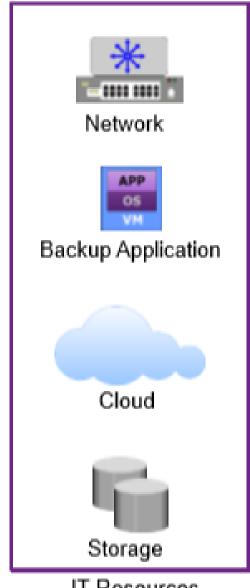
Identity and Access Management





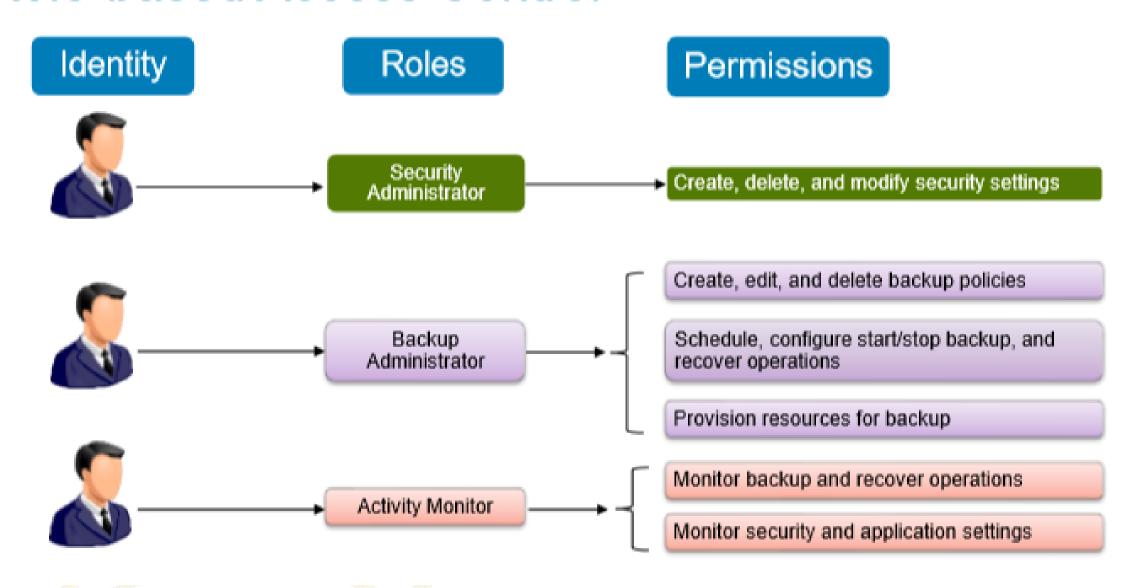






IT Resources

Role-based Access Control



Firewall

Filtering rules are based on parameters such as source and destination address, port numbers, and protocols

Authorized data packets are allowed

Internal Network

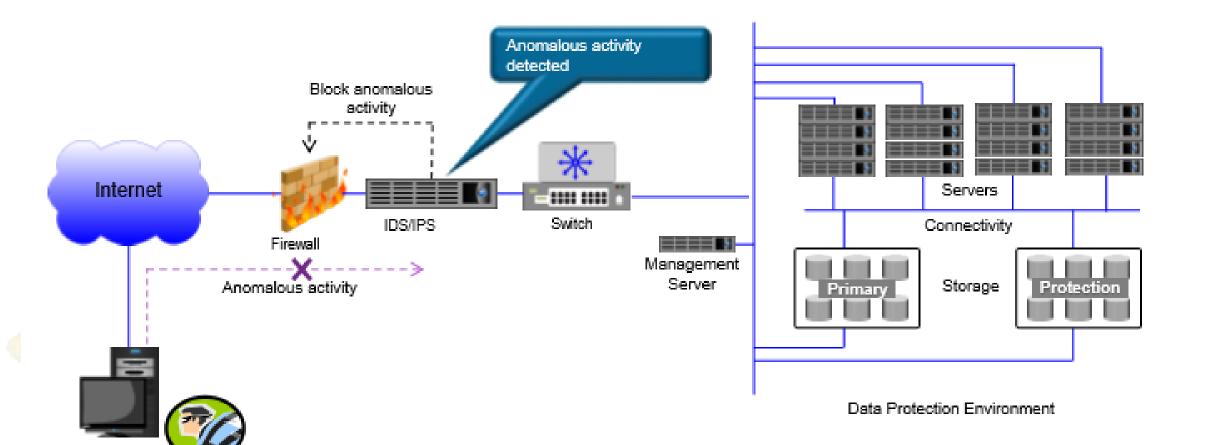
External Network

Unauthorized data packets are dropped

- Authorized data packets are allowed
- Unauthorized data packets are dropped

- Firewall's effectiveness depends on robust and extensive definition of rules
- Firewall can be physical or virtual

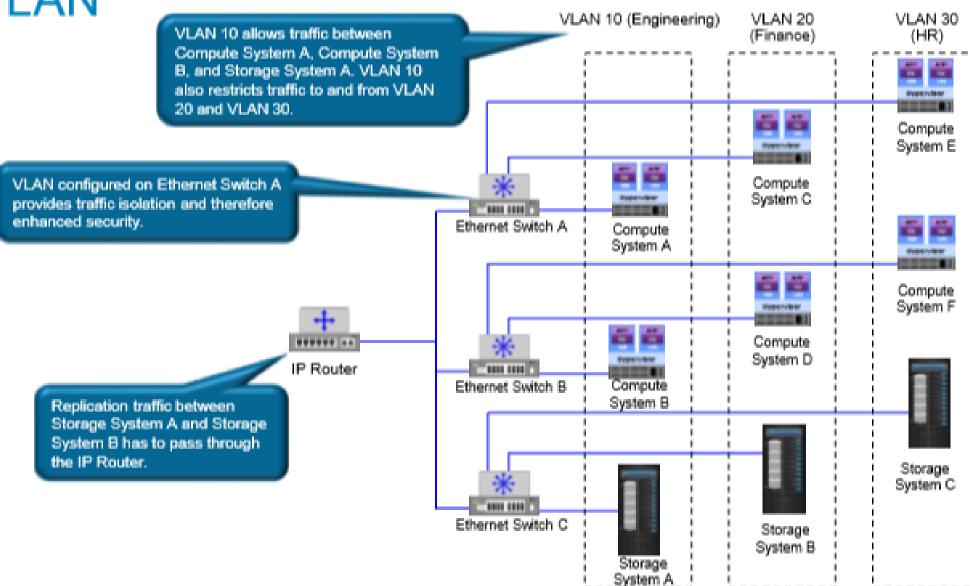
Intrusion Detection and Prevention System



Attacker

Virtual Private Network Organization needs to perform remote replication between two sites using VPN connection ******** VPN-enabled Internet VPN-enabled Standby Server Application | router router Server VPN connection established SAN SAN LAN LAN Tunnel Storage Clients Storage Clients. VPN connection established Disaster Recovery Site Primary Site Remote user connects to the Remote User corporate network using VPN connection C MPN Client

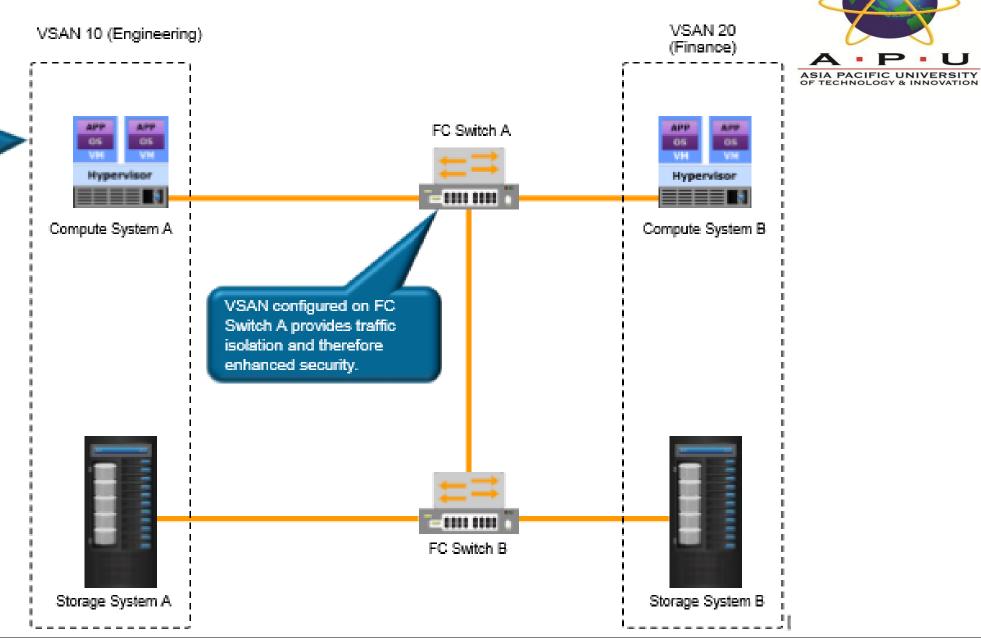






VSAN

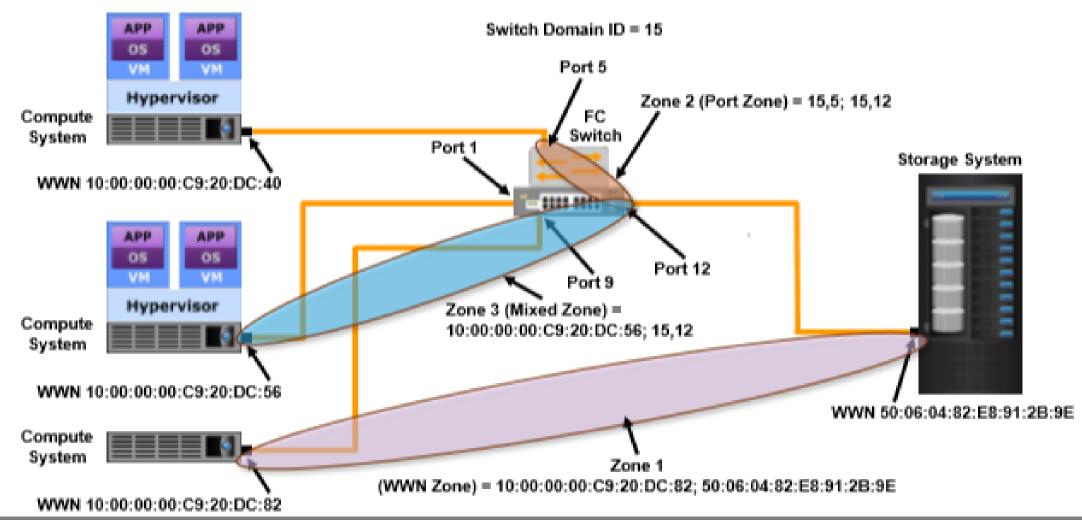
VSAN 10 allows traffic between Compute System A and Storage System A. VSAN 10 also restricts traffic from VSAN 20.





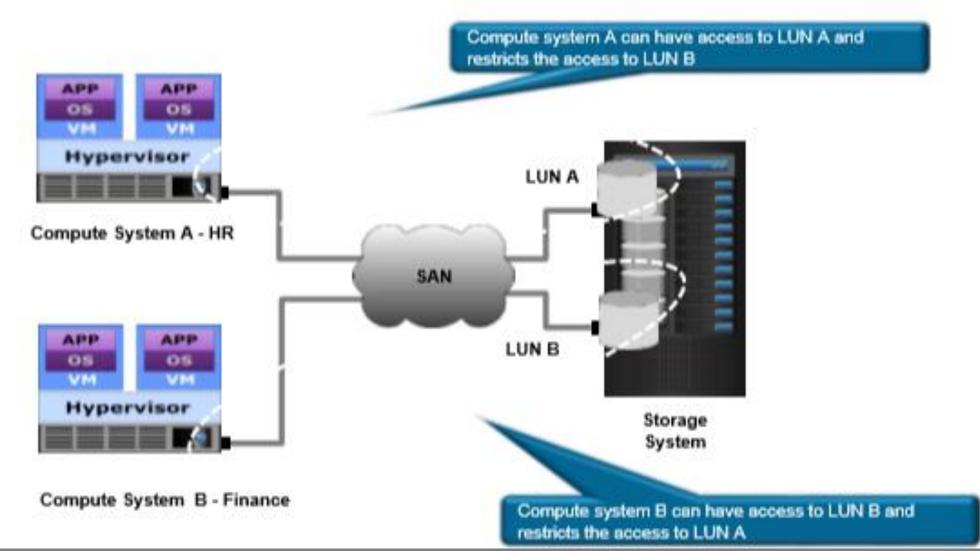
Zoning

An FC switch-based control that enables node ports connected to an FC SAN to be logically segmented into groups and communicate with each other within the group

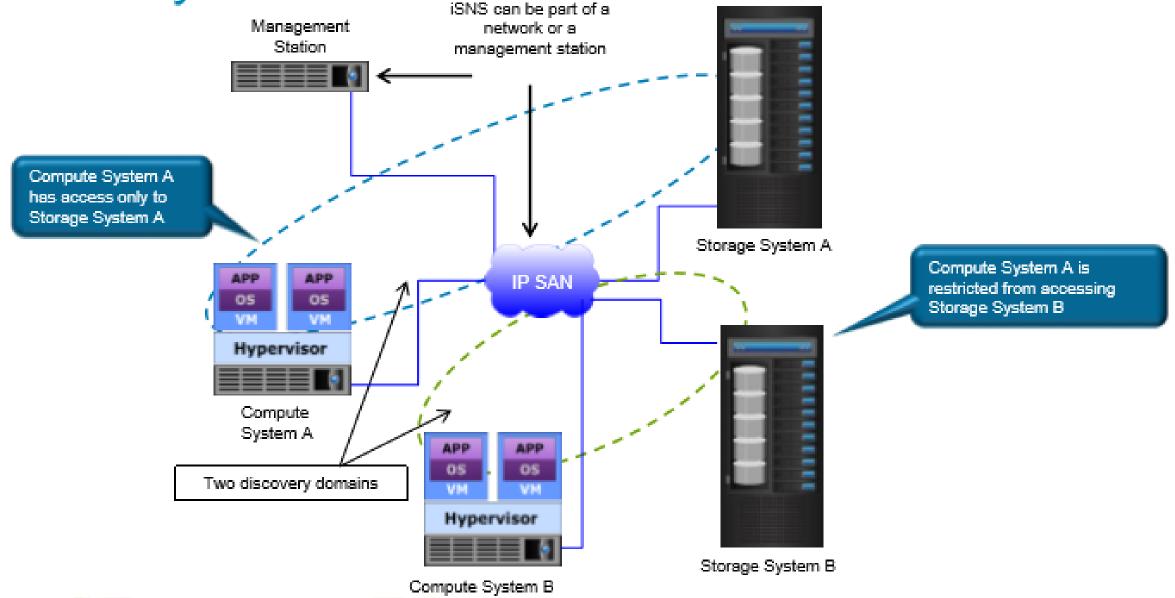


LUN Masking

Refers to the assignment of LUNs to specific host bus adapter worldwide names



Discovery Domain



Key Security Controls



Physical security

Identity and access management

Role-based access control

Firewall

Intrusion detection and prevention system

Virtual private network

Virtual LAN and virtual SAN

Zoning

LUN Masking

Discovery domair

Securing hypervisor

Securing management server

VM, OS, and application hardening

Malware protection software

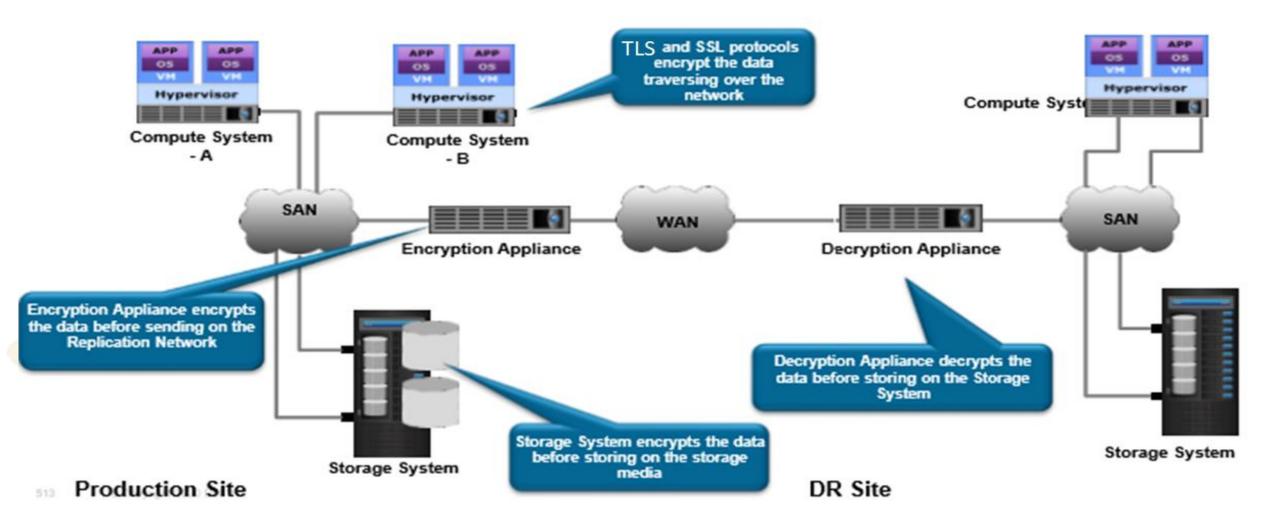
Mobile device management

Data encryption

Data shredding

Data Encryption

A cryptographic technique in which data is encoded and made indecipherable to eavesdroppers or hackers.



Discussion



Do a google search and explain in detail the following big data security technologies

- 1. Encryption
- 2. Use access control
- 3. Physical Security
- 4. Centralized Key Management
- 5. Intrusion Detection and Prevention System
- 6. Zoning
- 7. LUN Masking

Question and answer session

Q&A