Unit-V

Securing the Storage Infrastructure, Managing the Storage Infrastructure: Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementations in Storage Networking Monitoring the Storage Infrastructure, Storage Management Activities, Storage Infrastructure Management Challenges, Developing an Ideal Solution.

Key Concepts:

- Storage Security Framework
- The Risk Triad
- Denial of Service
- Security Domain
- Infrastructure Right Management
- Access Control

This chapter describes a framework for storage security that is designed to mitigate security threats that may arise and to combat malicious attacks on the storage infrastructure.

In addition, this chapter describes basic storage security implementations, such as the security architecture and protection mechanisms in SAN, NAS, and IP-SAN.

15.1 Storage Security Framework

The basic security framework is built around the four primary services of security: accountability, confidentiality, integrity, and availability. This framework incorporates all security measures required to mitigate threats to these four primary security attributes:

- □ **Accountability service:** Refers to accounting for all the events and operations that takes place in data center infrastructure. The accountability service maintains a log of events that can be audited or traced later for the purpose of security.

- □ **Confidentiality service:** Provides the required secrecy of information and ensures that only authorized users have access to data. This service authenticates users who need to access information and typically covers both data in transit (data transmitted over cables), or data at rest (data on a backup media or in the archives).

- ❑ **Integrity service:** Ensures that the information is unaltered. The objective of the service is to detect and protect against unauthorized alteration or deletion of information. Similar to confidentiality services, integrity services work in collaboration with accountability services to identify and authenticate the users. Integrity services stipulate measures for both in-transit data and at-rest data.

- ❑ **Availability service:** This ensures that authorized users have reliable and timely access to data. These services enable users to access the required computer systems, data, and applications residing on these systems. Availability services are also implemented on communication systems used to transmit information among computers that may reside at different locations. This ensures availability of information if a failure in one particular location occurs. These services must be implemented for both electronic data and physical data.

15.2 Risk Triad

Risk triad defines the risk in terms of threats, assets, and vulnerabilities. Risk arises when a threat agent (an attacker) seeks to access assets by exploiting an existing vulnerability. The severity of an adverse event is estimated by the impact that it may have on critical business activities. Based on this analysis, a relative value of criticality and sensitivity can be assigned to IT assets and resources. For example, a particular IT system component may be assigned a high-criticality value if an attack on this particular component can cause a complete termination of mission-critical services.

15.2.1 Assets

Information is one of the most important *assets* for any organization. Other assets include hardware, software, and the network infrastructure required to access this information. To protect these assets, organizations must develop a set of parameters to ensure the availability of the resources to authorized users and trusted networks. These parameters apply to storage resources, the network infrastructure, and organizational policies.

Several factors need to be considered when planning for asset security.

Security methods have two objectives.

First objective is to ensure that the network is easily accessible to authorized users.

It should also be reliable and stable under disparate environmental conditions and volumes of usage.

Second objective is to make it very difficult for potential attackers to access and compromise the system.

These methods should provide adequate protection against unauthorized access to resources, viruses, worms, Trojans and other malicious software programs.

Security measures should also encrypt critical data an disable unused services to minimize the number of potential security gaps.

15.2.2 Threats

Threats are the potential attacks that can be carried out on an IT infrastructure.

These attacks can be classified as active or passive. *Passive* attacks are attempts to gain unauthorized access into the system. They pose threats to confidentiality of information.

Active attacks include data modification, Denial of Service (DoS), and repudiation attacks. They pose threats to data integrity and availability.

In a *modification* attack, the unauthorized user attempts to modify information for malicious purposes.

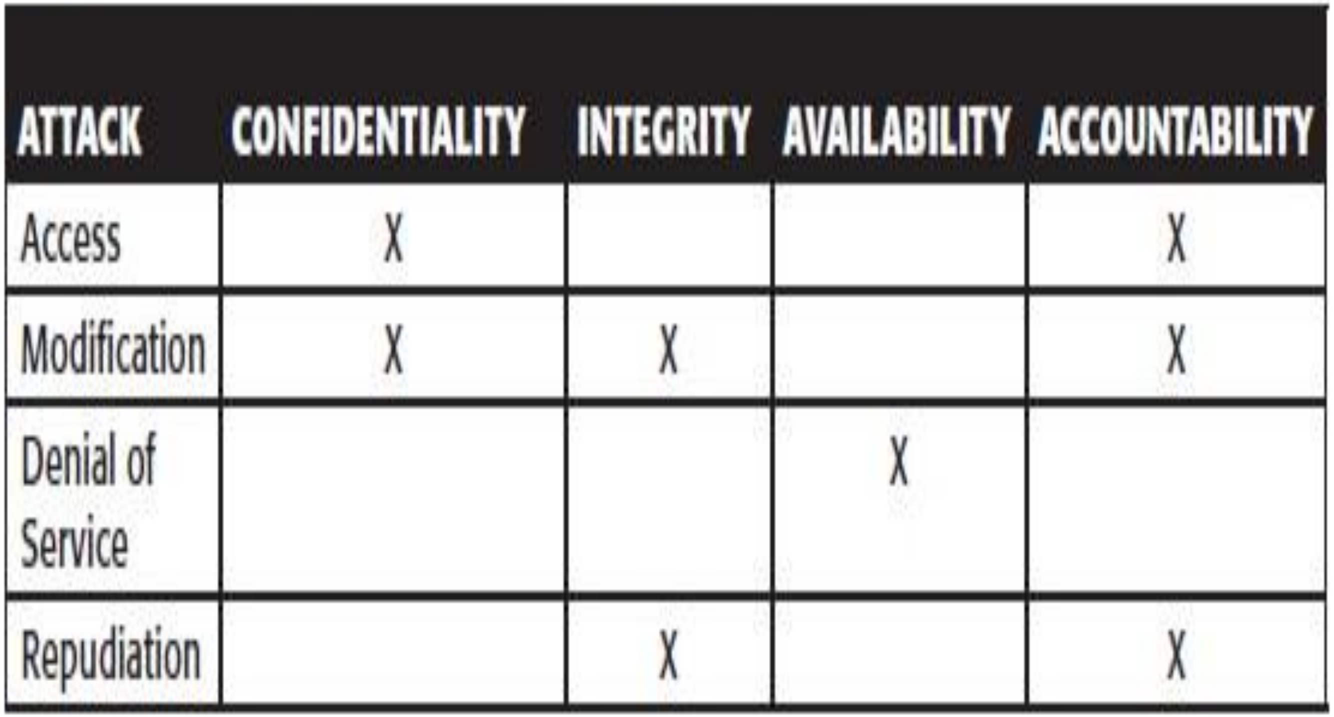
A modification attack can target data at rest or data in transit. These attacks pose a threat to data integrity.

Denial of Service (DoS) attacks denies the use of resources to legitimate users.

These attacks generally do not involve access to or modification of information on the computer system. Instead, they pose a threat to data availability.

The intentional flooding of a network or website to prevent legitimate access to authorized users is one example of a DoS attack.

Table 15-1: Security Services for Various Types of Attacks



ATTACK	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	ACCOUNTABILITY
Access	X			X
Modification	X	X		X
Denial of Service			X	
Repudiation		X		X

15.2.3 Vulnerability

The paths that provide access to information are the most vulnerable to potential attacks. Each of these paths may contain various access points, each of which provides different levels of access to the storage resources. It is very important to implement adequate security controls at *all* the access points on an access path. Implementing security controls at each access point of every access path is termed as *defense in depth*.

Attack surface, *attack vector*, and *work factor* are the three factors to consider when assessing the extent to which an environment is vulnerable to security threats. *Attack surface* refers to the various entry points that an attacker can use to launch an attack. Each component of a storage network is a source of potential vulnerability. All of the external interfaces supported by that component, such as the hardware interfaces, the supported protocols, and the management and administrative interfaces, can be used by an attacker to execute various attacks. These interfaces form the attack surface for the attacker. Even unused network services, if enabled, can become a part of the attack surface.

15.3 Storage Security Domains

Storage devices that are not connected to a storage network are less vulnerable because they are not exposed to security threats via networks. However, with increasing use of networking in storage environments, storage devices are becoming highly exposed to security threats from a variety of sources. Specific controls must be implemented to secure a storage networking environment.

If each component within the storage network is considered a potential access point, one must analyze the attack surface that each of these access points provides and identify the associated vulnerability. In order to identify the threats that apply to a storage network, access paths to data storage can be categorized into three security domains: *application access*, *management access*, and *BURA (backup, recovery, and archive)*. Figure 15-1 depicts the three security domains of a storage system environment.

To secure the storage networking environment, identify the existing threats within each of the security domains and classify the threats based on the type of security services-availability, confidentiality, integrity, and accountability.

The next step is to select and implement various controls as countermeasures to the threats.

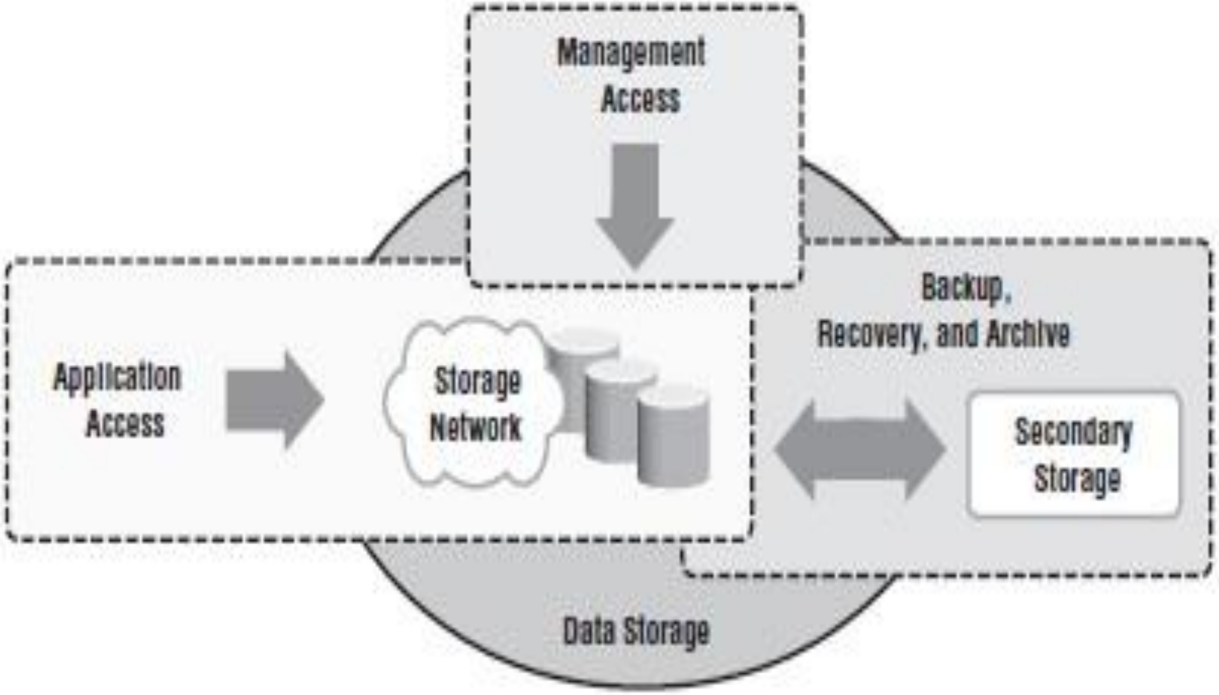


Figure 15-1: Three security domains of data storage

15.3.1 Securing the Application Access Domain

The application access domain may include only those applications that access the data through the file system or a database interface. Figure 15-2 shows application access in a storage networking environment. Host A can access all V1 volumes; host B can access all V2 volumes. These volumes are classified according to access level, such as confidential, restricted, and public.

Some of the possible threat in this scenario could be host A spoofing the identity or elevating the privileges of host B to gain access to host B's resources.

Another threat could be an unauthorized host gain access to the network; the attacker on this host may try to spoof the identity of another host and tamper with data, snoop the network, or execute a DoS attack.

Also any form of media theft could also compromise security.

These threats can pose several serious challenges to the network security, hence they need to be addressed.

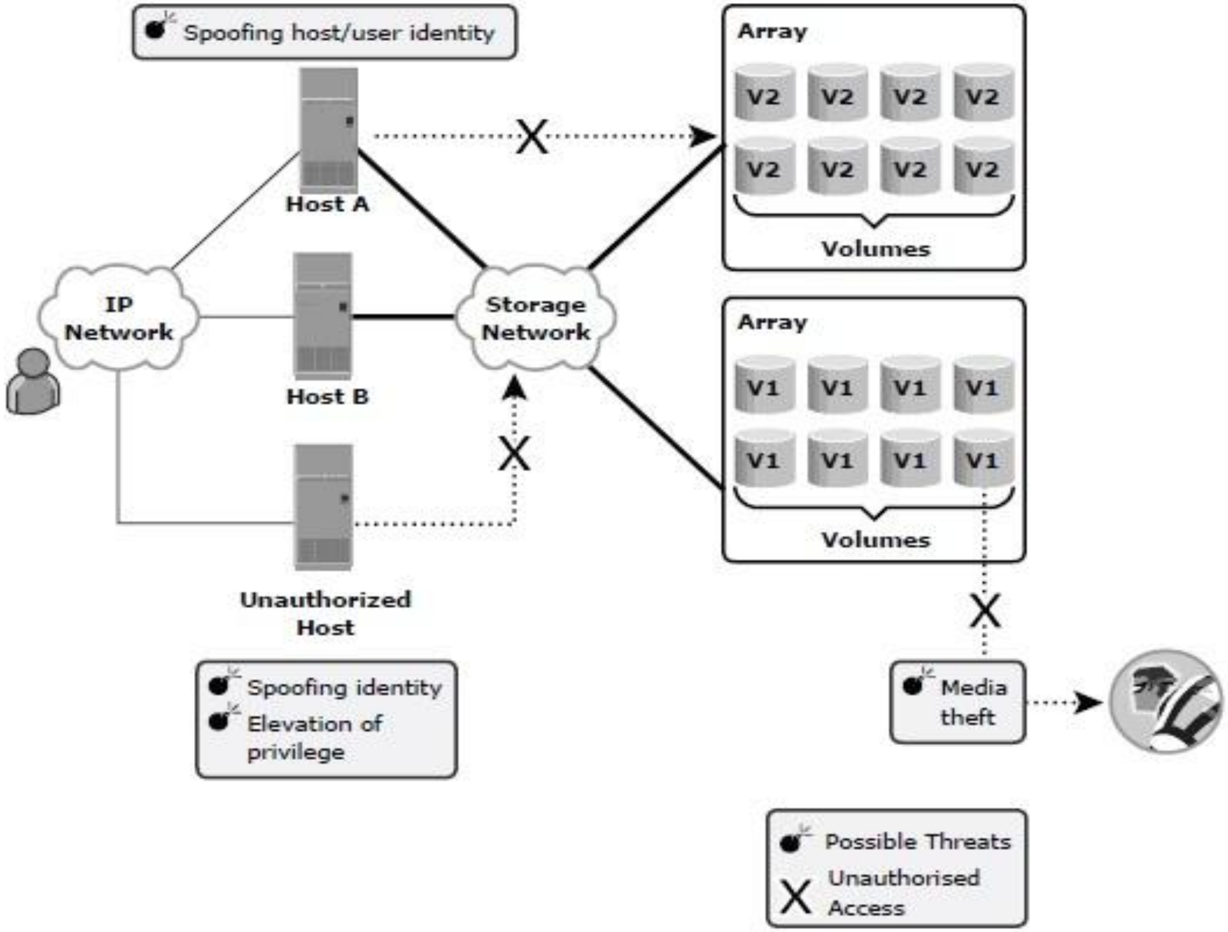


Figure 15-2: Security threats in application access domain

Controlling User Access to Data

Technical control in the form of user authentication and administrative control in the form of user authorization are the two access control mechanisms used in application access control.

These mechanisms may lie outside the boundaries of the storage network and require various systems to interconnect with other enterprise identity management and authentication systems—for example, systems that provide strong authentication and authorization to secure user identities against spoofing.

Protecting the Storage Infrastructure

Securing the storage infrastructure from unauthorized access involves protecting all the elements of the infrastructure.

Security controls for protecting the storage infrastructure address the threats of unauthorized tampering of data in transit that leads to a loss of data integrity, denial of service that compromises availability, and network snooping that may result in a loss of confidentiality.

The security controls for protecting the network fall into two general categories: *connectivity infrastructure integrity* and *storage network encryption*.

Controls for ensuring the infrastructure integrity include a fabric switch function to ensure fabric integrity.

This is achieved by preventing a host from being added to the SAN fabric without proper authorization. Storage network encryption methods include the use of IP Sec, for protecting IP-based storage networks, and FC-SP, for protecting FC networks.

Data Encryption

The most important aspect of securing data is protecting data held inside the storage arrays. Threats at this level include tampering with data, which violates data integrity, and media theft, which compromises data availability and confidentiality.

Data should be encrypted as close to its origin as possible.

If it is not possible to perform encryption on the host device, an encryption appliance can be used for encrypting data at the point of entry into the storage network.

Encryption devices can be implemented on the fabric that encrypts data between the host and the storage media.

These mechanisms can protect both the data at rest on the destination device and data in transit.

15.3.2 Securing the Management Access Domain

Management access, whether monitoring, provisioning, or managing storage resources, is associated with every device within the storage network.

Most management software supports some form of CLI, system management console, or a web-based interface.

It is very important to implement appropriate controls for securing storage management applications because the damage that can be caused to the storage system by using these applications can be far more extensive than that caused by vulnerability in a server.

Figure 15-3 depicts a storage networking environment in which production hosts are connected to a SAN fabric and are accessing storage Array A, which is connected to storage Array B for replication purposes.

Further, this configuration has a storage management platform on Host B and a monitoring console on Host A.

All these hosts are interconnected through an IP network.

Some of the possible threats in this system are, unauthorized host may spoof the user or host identity to manage the storage arrays or network.

For example, Host A may gain management access to array B. Remote console support for the management software also increases the attack surface.

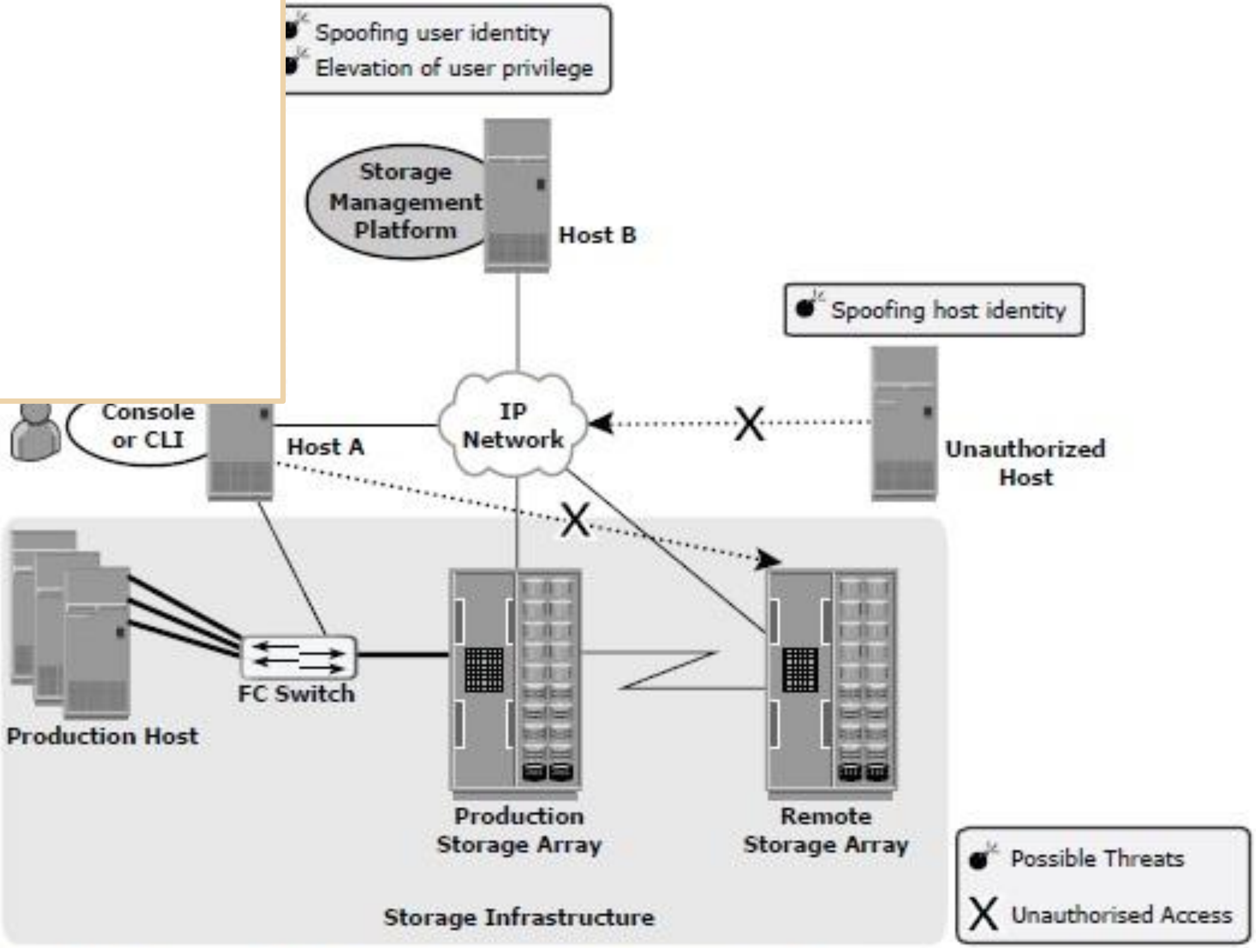


Figure 15-3: Security threats in management access domain

The storage management platform must be validated for available security controls and ensures that these controls are adequate to secure the overall storage environment.

The administrator's identity and role should be secured against any spoofing attempts so an attacker cannot manipulate the entire storage array and cause intolerable data loss by reformatting storage media or making data resources unavailable.

Controlling Administrative Access

Controlling administrative access to storage aims to safeguard against the threats of an attacker spoofing an administrator's identity or elevating another user's identity and privileges to gain administrative access.

Both of these threats affect the integrity of data and devices.

To protect against these threats, administrative access regulation and various auditing techniques are used to enforce accountability.

Every storage component should provide access control.

Protecting the Management Infrastructure

Protecting the management network infrastructure is also necessary.

Controls to protect the management network infrastructure include encrypting management traffic, enforcing management access controls, and applying IP network security best practices.

These best practices include the use of IP routers and Ethernet switches to restrict traffic to certain devices and management protocols.

SAN Security Architecture

Storage networking environments are a potential target for unauthorized access, theft, and misuse because of the vastness and complexity of these environments.

Therefore, security strategies are based on the *defense in depth* concept, which recommends multiple integrated layers of security.

This ensures that the failure of one security control will not compromise the assets under protection.

Figure 15-5 illustrates various levels (zones) of a storage networking environment that must be secured and the security measures that can be deployed.

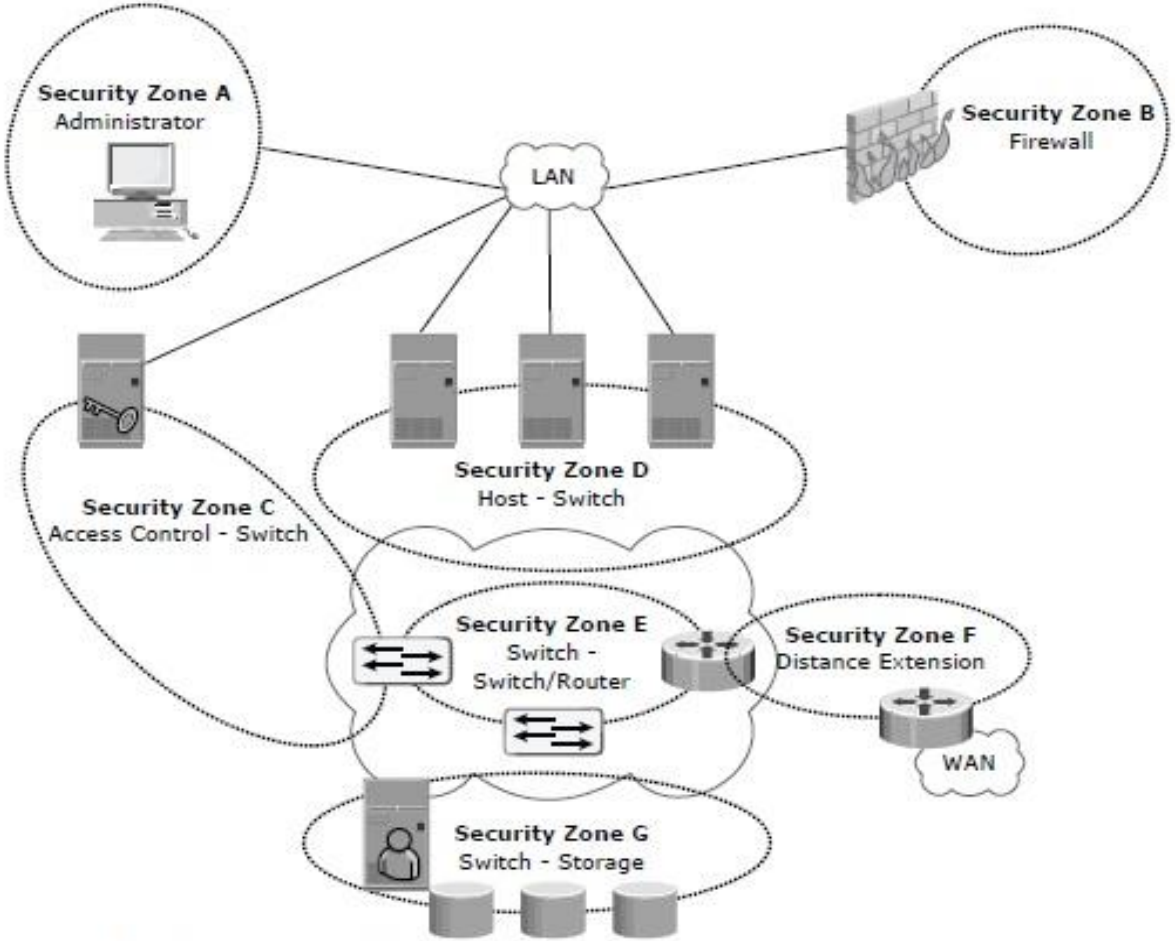


Figure 15-5: SAN security architecture

Table 15-2 provides a comprehensive list of protection strategies that must be implemented in various security zones.

Note that some of the security mechanisms listed in Table 15-2 are not specific to SAN, but are commonly used data center techniques.

For example, two-factor authentication is implemented widely; in a simple implementation it requires the use of a user name/password and an additional security component such as a smart card for authentication.

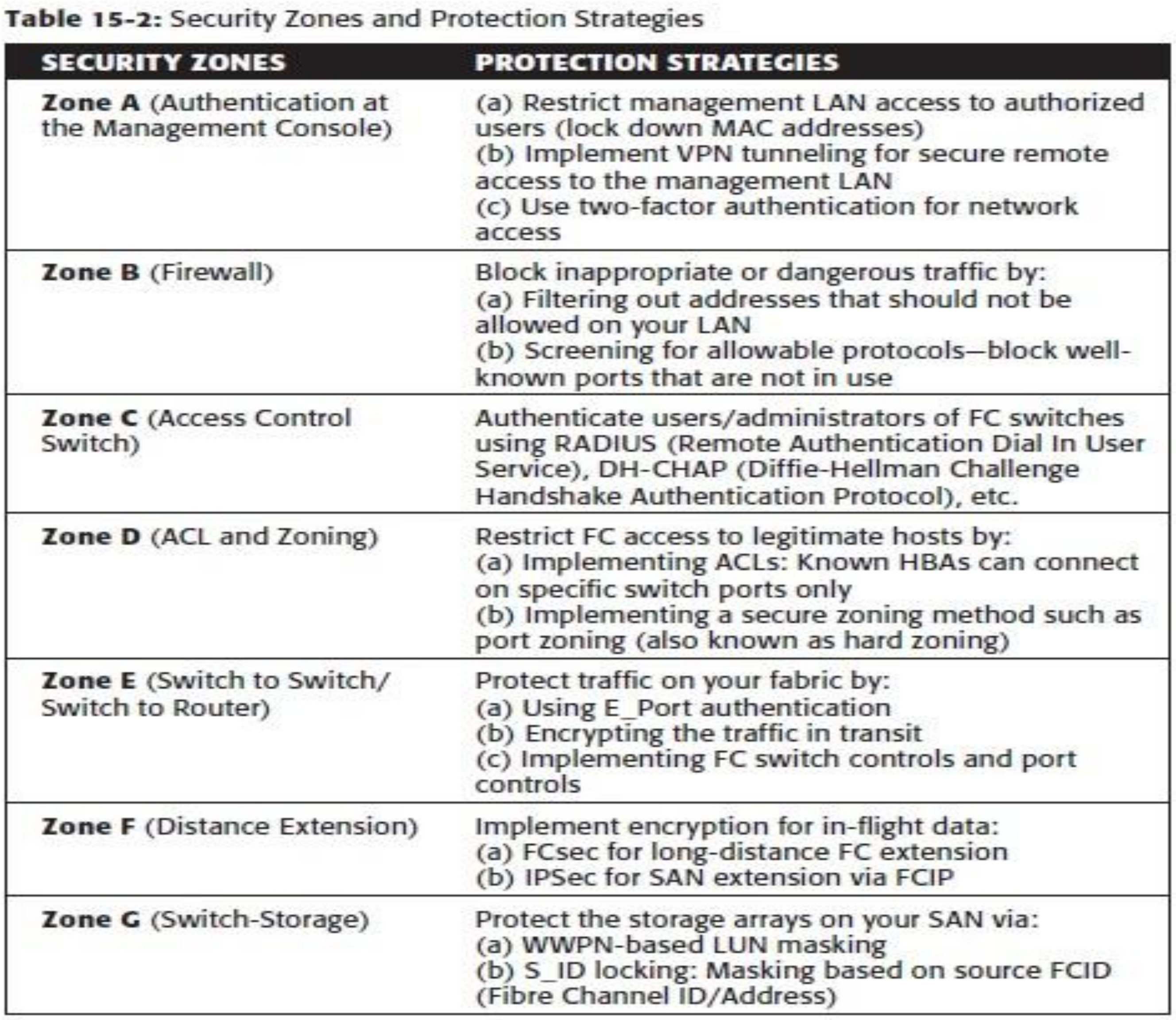


Table 15-2: Security Zones and Protection Strategies

SECURITY ZONES	PROTECTION STRATEGIES
Zone A (Authentication at the Management Console)	(a) Restrict management LAN access to authorized users (lock down MAC addresses) (b) Implement VPN tunneling for secure remote access to the management LAN (c) Use two-factor authentication for network access
Zone B (Firewall)	Block inappropriate or dangerous traffic by: (a) Filtering out addresses that should not be allowed on your LAN (b) Screening for allowable protocols—block well-known ports that are not in use
Zone C (Access Control Switch)	Authenticate users/administrators of FC switches using RADIUS (Remote Authentication Dial In User Service), DH-CHAP (Diffie-Hellman Challenge Handshake Authentication Protocol), etc.
Zone D (ACL and Zoning)	Restrict FC access to legitimate hosts by: (a) Implementing ACLs: Known HBAs can connect on specific switch ports only (b) Implementing a secure zoning method such as port zoning (also known as hard zoning)
Zone E (Switch to Switch/ Switch to Router)	Protect traffic on your fabric by: (a) Using E_Port authentication (b) Encrypting the traffic in transit (c) Implementing FC switch controls and port controls
Zone F (Distance Extension)	Implement encryption for in-flight data: (a) FCsec for long-distance FC extension (b) IPSec for SAN extension via FCIP
Zone G (Switch-Storage)	Protect the storage arrays on your SAN via: (a) WWPN-based LUN masking (b) S_ID locking: Masking based on source FCID (Fibre Channel ID/Address)

Basic SAN Security Mechanisms

LUN masking and zoning, switch-wide and fabric-wide access control, RBAC, and logical partitioning of a fabric (Virtual SAN) are the most commonly used SAN security methods.

LUN Masking and Zoning

LUN masking and zoning are the basic SAN security mechanisms used to protect against unauthorized access to storage.

LUN masking and zoning were detailed earlier in Chapter 4 and Chapter 6. Standard implementations of storage arrays mask the LUNs that are presented to a front-end storage port, based on the WWPNs of the source HBAs.

A stronger variant of LUN masking may sometimes be offered whereby masking can be done on the basis of source FCIDs.

Note that the FCID typically changes if the HBA is relocated across ports in the fabric.

Switch-wide and Fabric-wide Access Control

As organizations grow their SANs locally or over longer distances there is a greater need to effectively manage SAN security.

Network security can be configured on the FC switch by using *access control lists (ACLs)* and on the fabric by using fabric binding.

Fabric binding prevents an unauthorized switch from joining any existing switch in the fabric.

It ensures that authorized membership data exists on every switch and that any attempt to connect two switches by using an ISL causes the fabric to segment.

Role-based access control provides additional security to a SAN by preventing unauthorized management activity on the fabric for management operations.

Logical Partitioning of a Fabric: Virtual SAN

Zoning should be done for each VSAN to secure the entire physical SAN.

Each managed VSAN can have only one active zone set at a time.

As depicted in the figure, VSAN 1 is the active zone set.

The SAN administrator can create distinct VSANs other than VSAN 1 and populate each of them with switch ports.

In the example, the switch ports are distributed over three VSANs: 1, 2, and 3—for the IT, Engineering, and HR divisions, respectively.

A zone set is defined for each VSAN, providing connectivity for HBAs and storage ports logged into the VSAN.

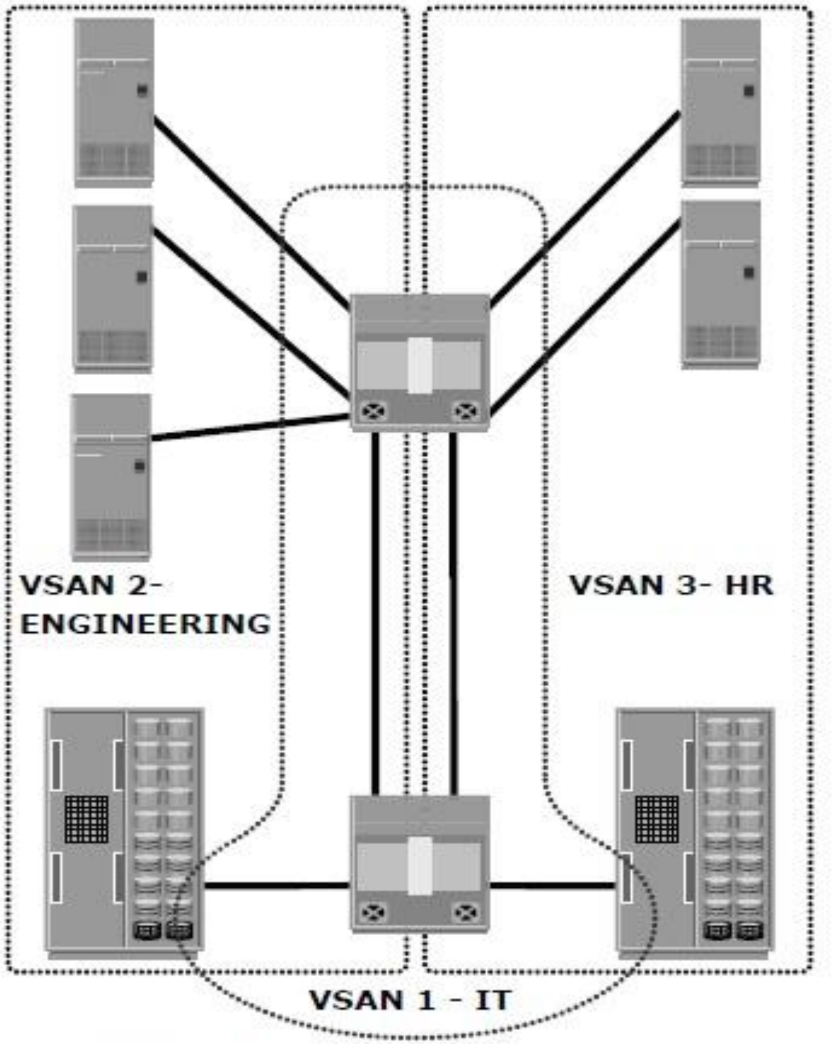


Figure 15-6: Securing SAN with VSAN

15.4.2 NAS

NAS is open to multiple exploits, including viruses, worms, unauthorized access, snooping, and data tampering.

Various security mechanisms are implemented in NAS to secure data and the storage networking infrastructure.

Permissions and ACLs form the first level of protection to NAS resources by restricting accessibility and sharing.

These permissions are deployed over and above the default behaviors and attributes associated with files and folders.

In addition, various other authentication and authorization mechanisms, such as Kerberos and directory services, are implemented to verify the identity of network users and define their privileges.

NAS File Sharing: Windows ACLs

In addition to these ACLs, Windows also supports the concept of object ownership.

The owner of an object has hard-coded rights to that object, and these rights do not have to be explicitly granted in the SACL.

The owner, SACL, and DACL are all statically held as an attribute of each object.

Windows also offers the functionality to inherit permissions, which allows the child objects existing within a parent object to automatically inherit the ACLs of the parent object.

NAS File Sharing: UNIX Permissions

For the UNIX operating system, a *user* is an abstraction that denotes a logical entity for assignment of ownership and operation privileges for the system.

A user can be either a person or a system operation.

A UNIX system is only aware of the privileges of the user to perform specific operations on the system, and identifies each user by a user ID (UID) and a user name, regardless of whether it is a person, a system operation, or a device.

Authentication and Authorization

Authentication requires verifying the identity of a network user and therefore involves a login credential lookup on a Network Information System (NIS) server in a UNIX environment. Similarly, a Windows client is authenticated by a Windows domain controller that houses the Active Directory.

The Active Directory uses LDAP to access information about network objects in the directory, and Kerberos for network security.

NAS devices use the same authentication techniques to validate network user credentials.

Active Directory, LDAP, and Kerberos are discussed later in this chapter.

Figure 15-7 depicts the authentication process in a NAS environment.

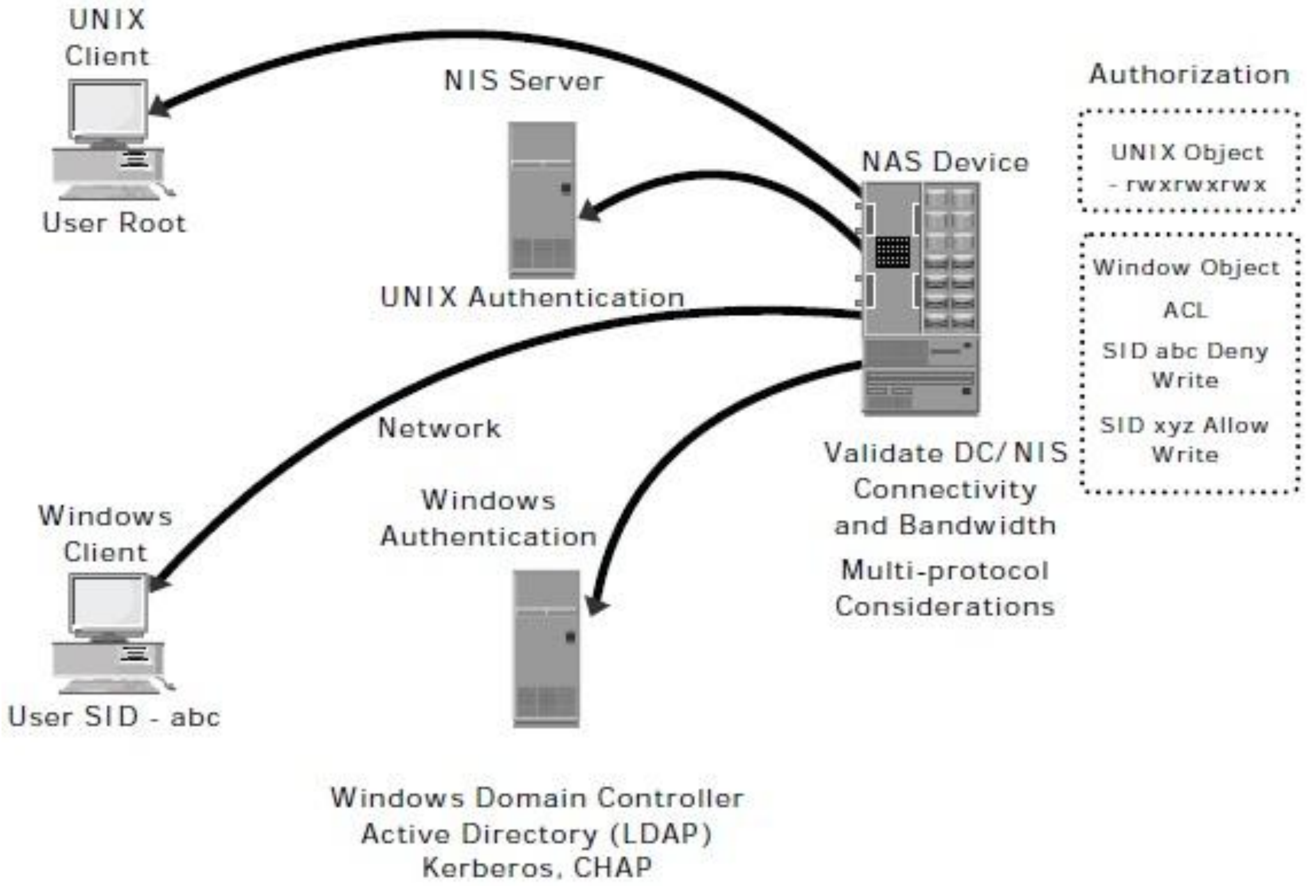


Figure 15-7: Securing user access in a NAS environment

Authorization defines user privileges in a network.

The authorization techniques for UNIX users and Windows users are quite different.

UNIX files use mode bits to define access rights granted to owners, groups, and other users, whereas Windows uses an ACL to allow or deny specific rights to a particular user for a particular file.

Kerberos

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It uses cryptography so that a client and server can prove their identity to each other across an insecure network connection. After the client and server have proven their identity, they can choose to encrypt all of their communications to ensure privacy and data integrity.

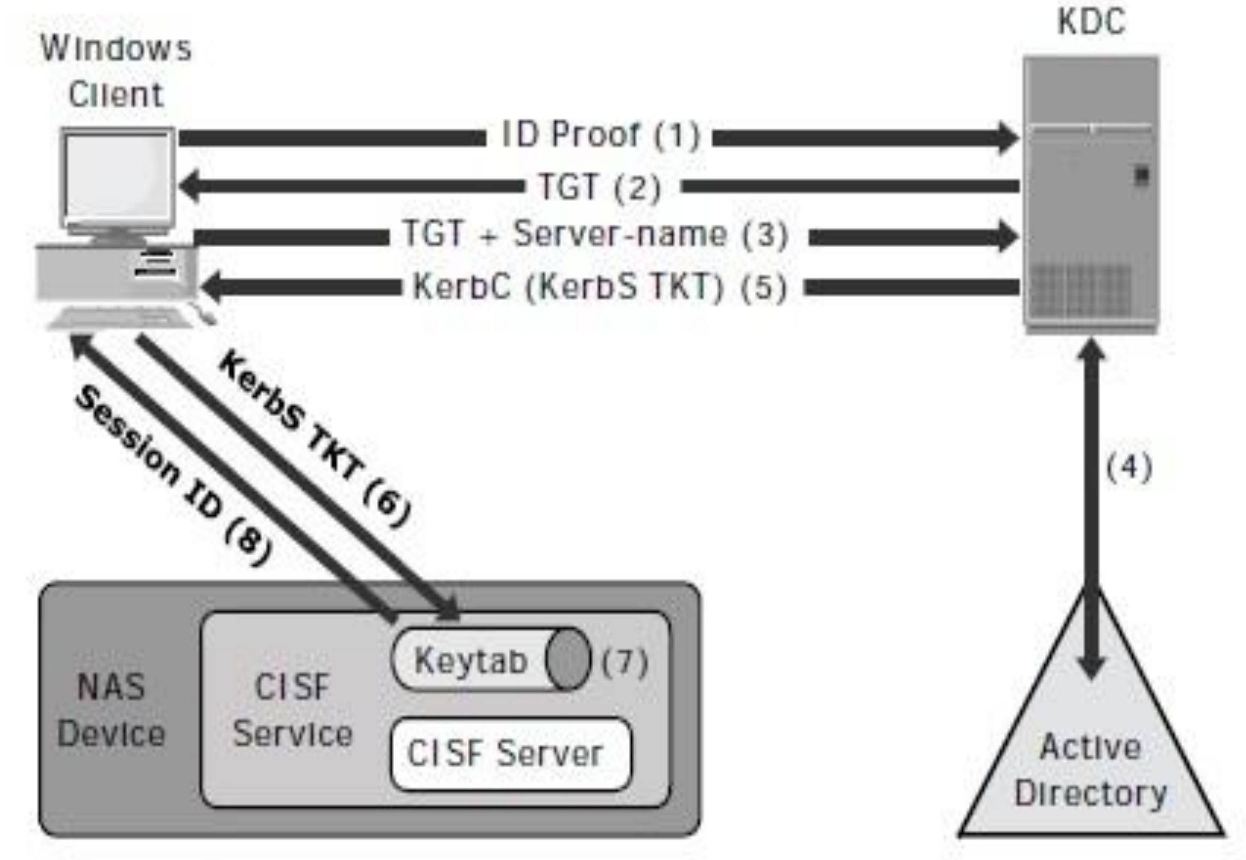


Figure 15-8: Kerberos authorization

Network-Layer Firewalls

Because NAS devices utilize the IP protocol stack, they are vulnerable to various attacks initiated through the public IP network.

Network layer firewalls are implemented in NAS environments to protect the NAS devices from these security threats.

These network-layer firewalls are capable of examining network packets and comparing them to a set of configured security rules.

Packets that are not authorized by a security rule are dropped and not allowed to continue to the requested destination.

Figure 15-9 depicts a typical firewall implementation. Demilitarized zone (DMZ) is commonly used in networking environments.

A DMZ provides a means of securing internal assets while allowing Internet-based access to various resources.

In a DMZ environment, servers that need to be accessed through the Internet are placed between two sets of firewalls.

Application-specific ports, such as HTTP or FTP, are allowed through the firewall to the DMZ servers.

However, no Internet-based traffic is allowed to penetrate the second set of firewalls and gain access to the internal network.

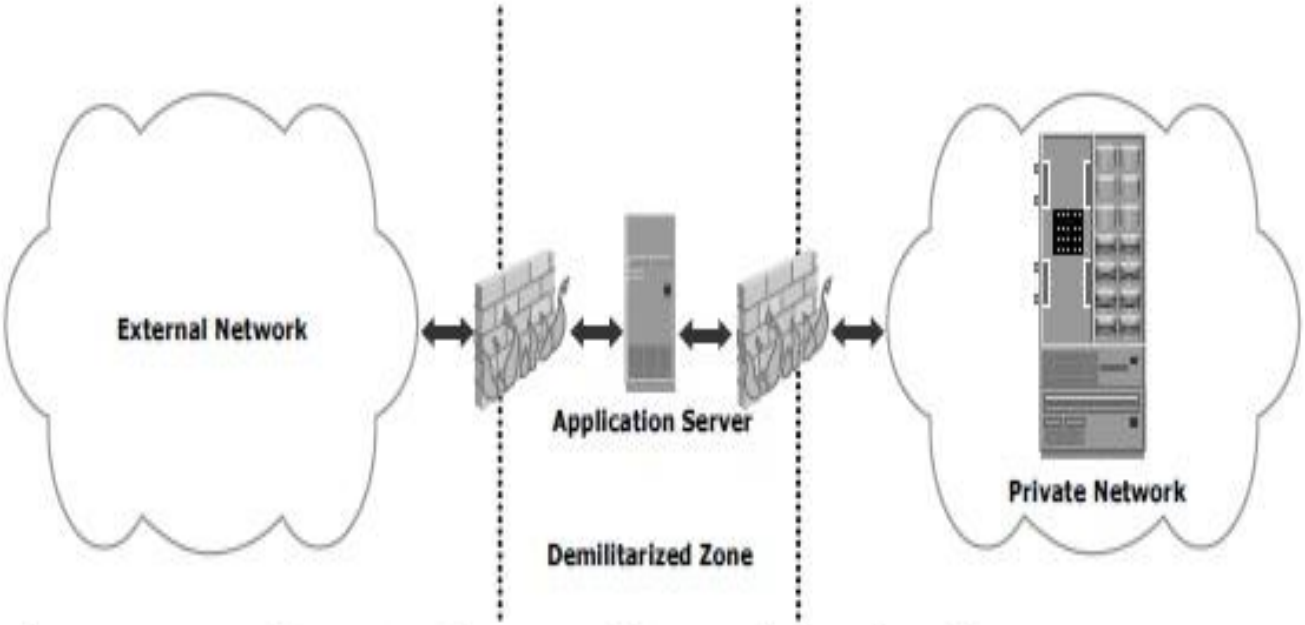


Figure 15-9: Securing NAS environment with network-layer firewall

15.4.3 IP SAN

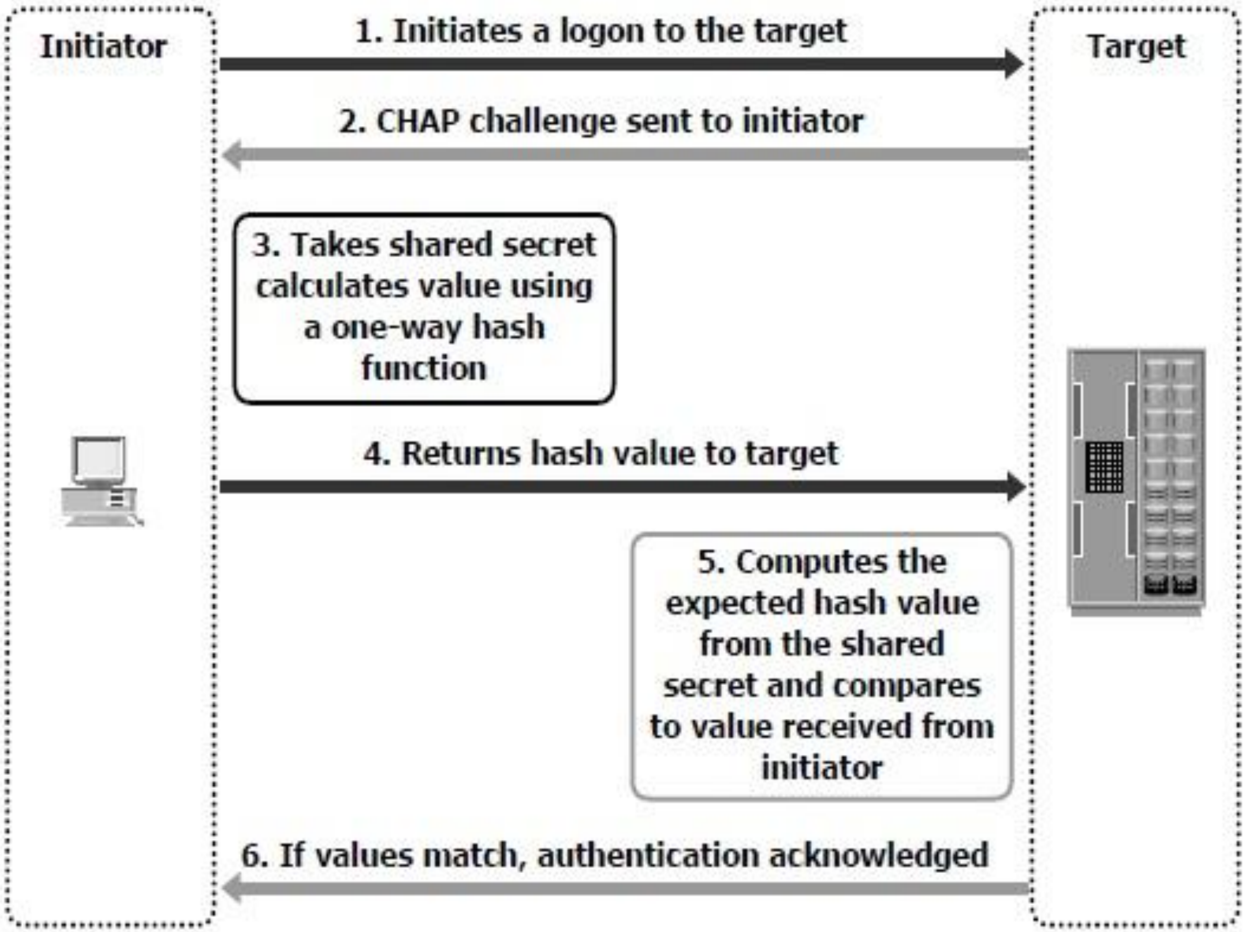
The *Challenge-Handshake Authentication Protocol (CHAP)* is a basic authentication mechanism that has been widely adopted by network devices and hosts.

CHAP provides a method for initiators and targets to authenticate each other by utilizing a secret code or password.

CHAP secrets are usually random secrets of 12 to 128 characters.

The secret is never exchanged directly over the wire; rather, a one-way hash function converts it into a hash value, which is then exchanged.

Figure 15-10 depicts the CHAP authentication process.



Initiator

Target

1. Initiates a logon to the target

2. CHAP challenge sent to initiator

3. Takes shared secret calculates value using a one-way hash function

4. Returns hash value to target

5. Computes the expected hash value from the shared secret and compares to value received from initiator

6. If values match, authentication acknowledged

Figure 15-10: Securing IPSAN with CHAP authentication

iSNS discovery domains function in the same way as FC zones.

Discovery domains provide functional groupings of devices in an IP-SAN.

In order for devices to communicate with one another, they must be configured in the same discovery domain.

State change notifications (SCNs) tell the iSNS server when devices are added or removed from a discovery domain.

Figure 15-11 depicts the discovery domains in iSNS.

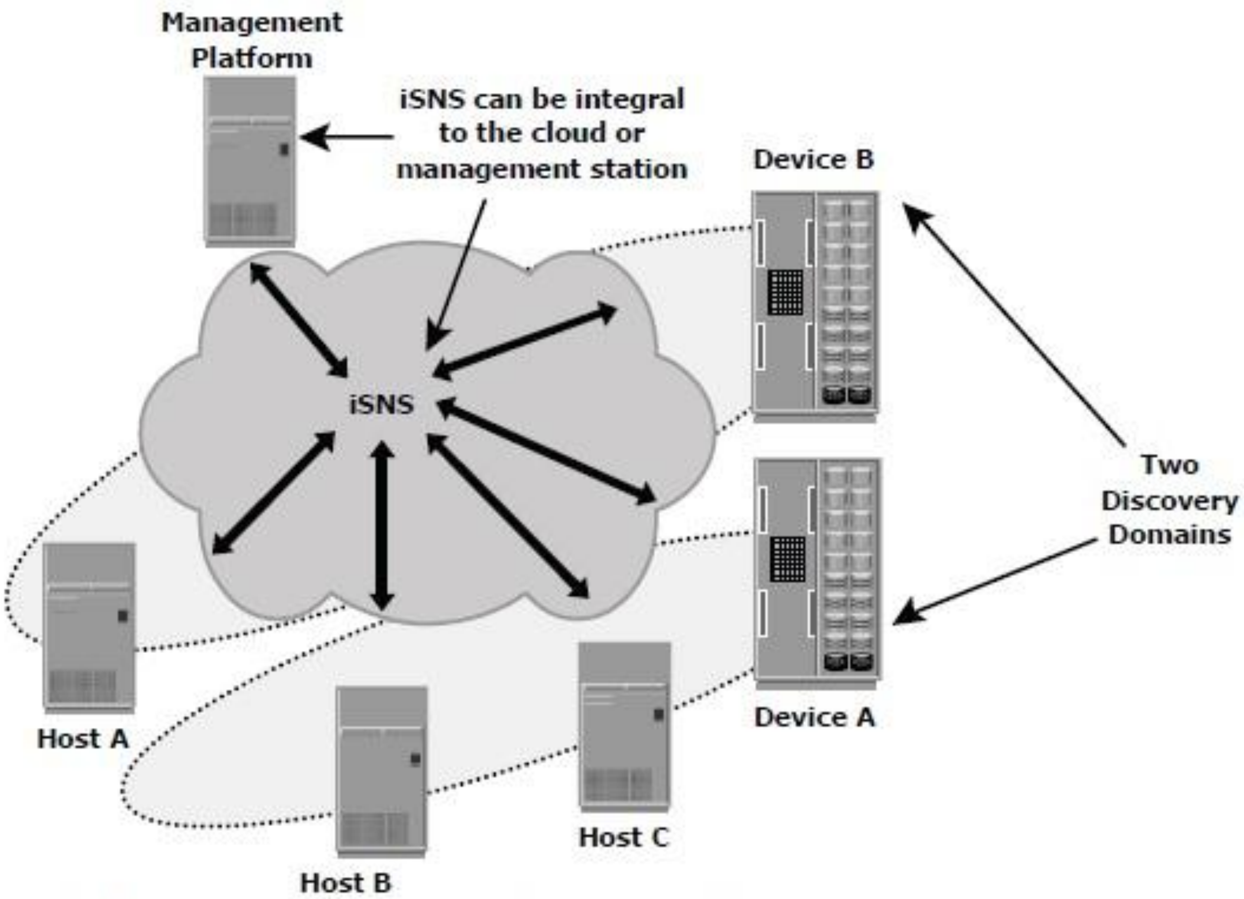


Figure 15-11: Securing IPSAN with iSNS discovery domains

Summary

The continuing expansion of the storage network has exposed data center resources and storage infrastructures to new vulnerabilities.

The delineation between a back-end data center and a front-end network perimeter has become less clear.

IP-based storage networking has exposed storage resources to traditional network vulnerabilities.

Data aggregation has also increased the potential impact of a security breach.

In addition to these security challenges, compliance regulations continue to expand and have become more complex.

Data center managers are faced with addressing the threat of security breaches from both within and outside the organization.

This chapter detailed a framework for storage security and provided mitigation methods that can be deployed against identified threats in a storage networking environment.

It also detailed the security architecture and protection mechanisms in SAN, NAS, and IP-SAN environments.

Security has become an integral component of storage management, and it is the key parameter monitored for all data center components.

The following chapter focuses on management of a storage infrastructure.

Section 4 : Storage Security and Management

Managing the Storage Infrastructure

EMC Education Services

Chapter 16

EMC Proven Professional

The #1 Certification Program in the information storage and management industry

Storage Infrastructure Management

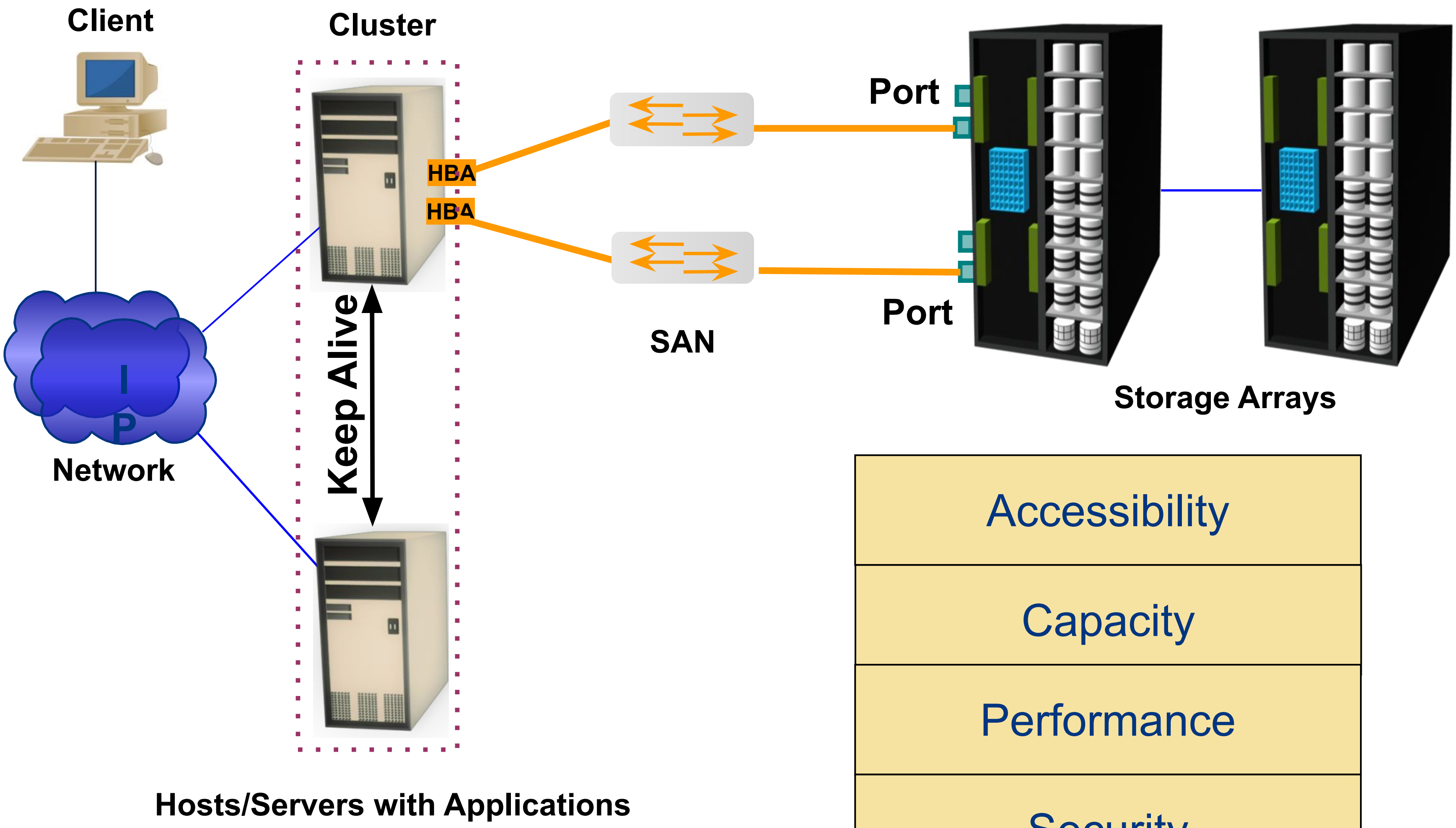
- Managing storage infrastructure is a key to ensure continuity of business
- Establishing management processes and implementing appropriate tools is essential to meeting service levels proactively
- Management activities include availability, capacity, performance, and security management
- Monitoring is the most important aspects that forms the basis for storage management
- Continuous monitoring enables availability and scalability by taking proactive measures

Lesson: Monitoring the Storage Infrastructure

Upon completion of this lesson, you will be able to:

- Discuss the major storage infrastructure components that should be monitored
- Describe what is to be monitored for the various storage infrastructure components
- Discuss alerting of events

Monitoring Storage Infrastructure



- Accessibility
- Capacity
- Performance
- Security

Parameters Monitored – Accessibility

- Accessibility refers to the availability of a component to perform a desired operation
- Why monitor accessibility of different components?
  - Failure of any hardware/software component can lead to outage of a number of different components
    - Example: HBA failure could cause degraded access to a number of devices in multi-path environment or loss of data access in single path environment
- Monitoring accessibility involves
  - Checking availability status of the hardware or software components through predefined alerts

Parameters Monitored – Capacity

- Capacity refers to the amount of storage infrastructure resources available
- Why monitor capacity?
  - Capacity monitoring prevents outages before they can occur
    - Inadequate capacity may lead to degraded performance or affect application/service availability
  - More preventive and predictive in nature
    - Report indicates 90% of all the ports have been utilized in SAN, a new switch must be added if more arrays/servers are to be added

Parameters Monitored – Performance

- Performance monitoring evaluates how efficiently different components are performing
- Why monitor Performance metrics?
  - Want all data center components to work efficiently/optimally
  - Helps to identify performance bottlenecks
  - Measures and analyzes the ability to perform at a certain predefined level
- Examples
  - Number of I/Os to disks
  - Application response time
  - Network utilization
  - Server CPU utilization

Parameters Monitored – Security

- Monitoring security helps to track and prevent unauthorized access
- Why monitor security?
  - Need to be protected for confidentiality, integrity and availability
  - To meet regulatory compliance
- Examples
  - Tracking and reporting changes made to zoning configurations
  - Physical security through badge readers, scanners and cameras

> - Monitoring Environmental parameters
>   - Temperature, humidity, airflow, hazards (water, smoke, etc.)
>   - Voltage – power supply

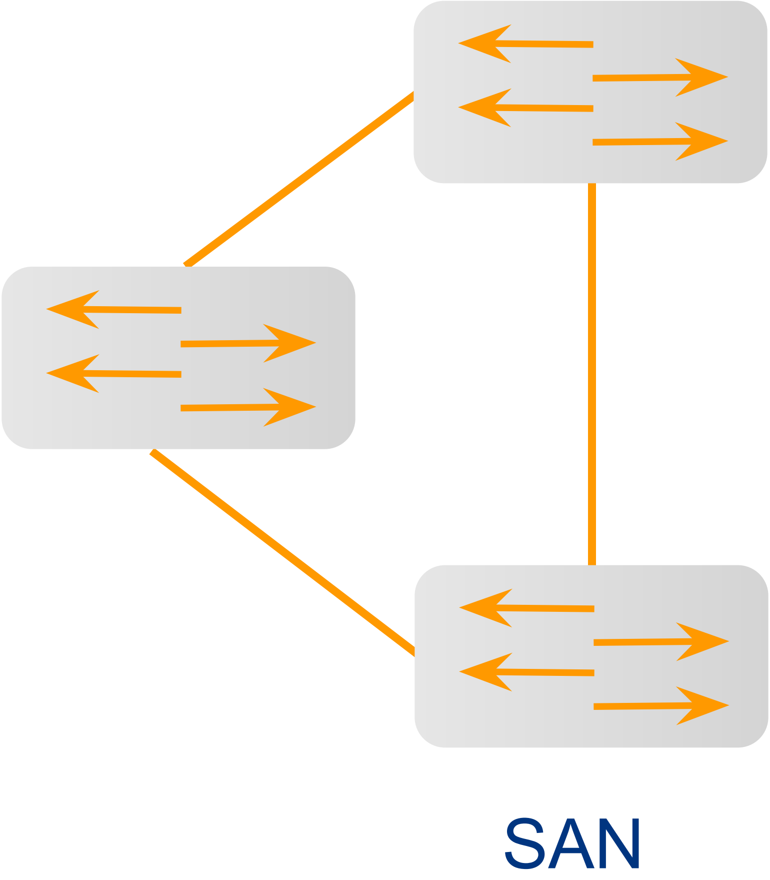
Monitoring Hosts

- Accessibility
  - Hardware components: HBA, NIC, graphic card, internal disk
  - Status of various processes/applications
- Capacity
  - File system utilization
  - Database: Table space/log space utilization
  - User quota
- Performance
  - CPU and memory utilization
  - Transaction response times
- Security
  - Login and authorization
  - Physical security (Data center access)

Host

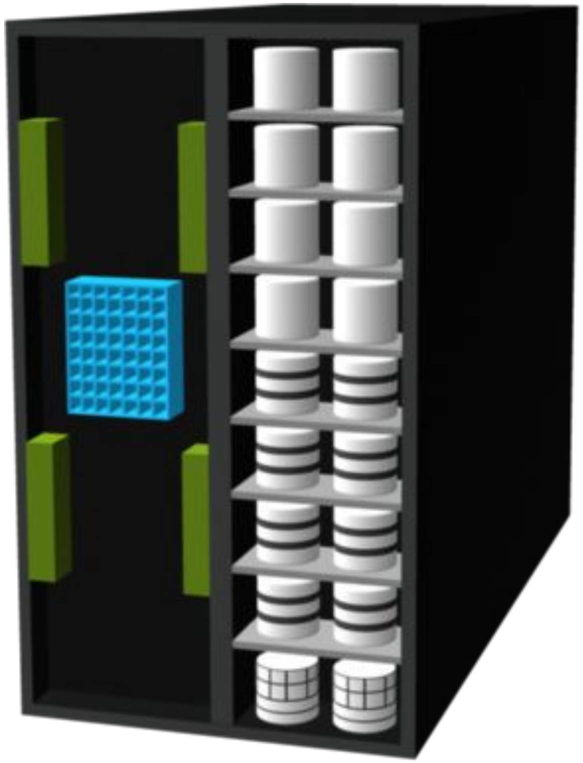
Monitoring the SAN

- Accessibility
  - Fabric errors, zoning errors, GBIC failure
  - Device status/attribute change
  - Processor cards, fans, power supplies
- Capacity
  - ISL (inter-switch link) and port utilization
- Performance
  - Connectivity ports
    - Link failures, loss of signal, link utilization
  - Connectivity devices
    - Port statistics
- Security
  - Zoning and LUN Masking
  - Administrative tasks and physical security
    - Authorized access, strict passwords



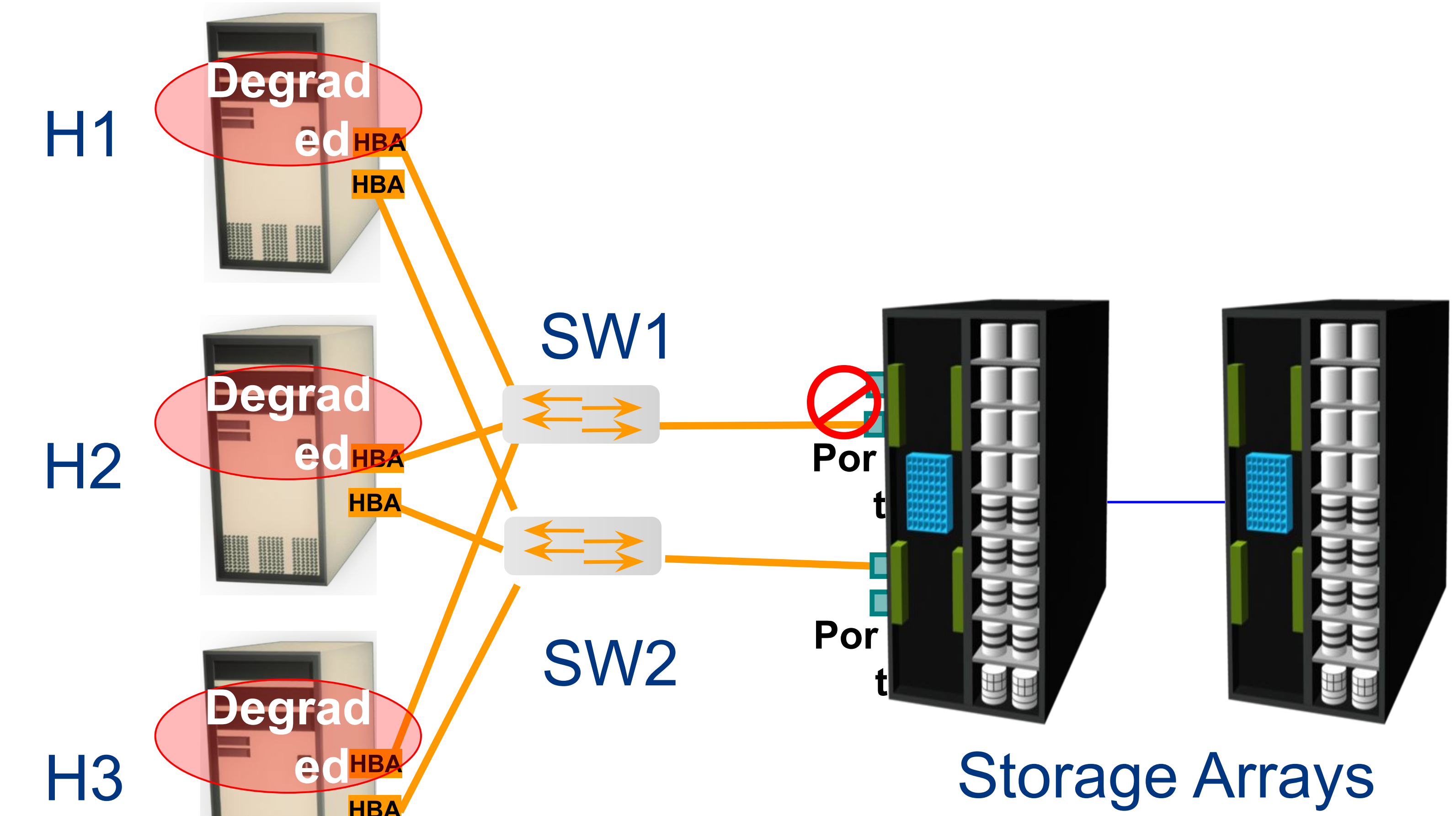
Monitoring Storage Arrays

- Accessibility
  - All Hardware components
  - Array Operating Environment
    - RAID processes
    - Environmental sensors
    - Replication processes
- Capacity
  - Configured/un-configured capacity
  - Allocated/unallocated storage
  - Fan-in/fan-out ratios
- Performance
  - FE (front-end) and BE (back-end) utilization/throughput
  - I/O profile, response time, cache metrics
- Security
  - Physical and administrative security



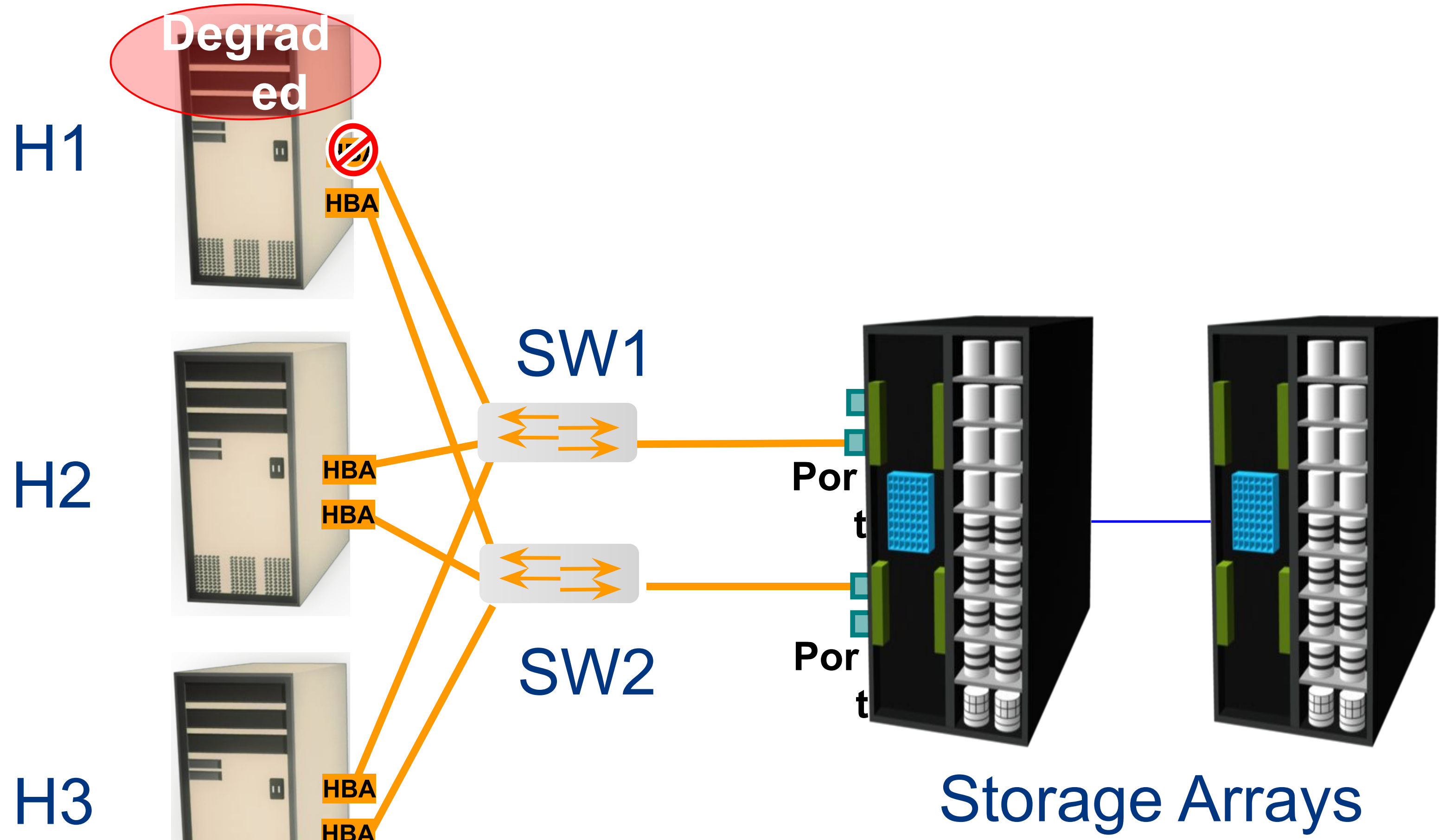
Storage Array

Accessibility Monitoring Example: Array Port Failure



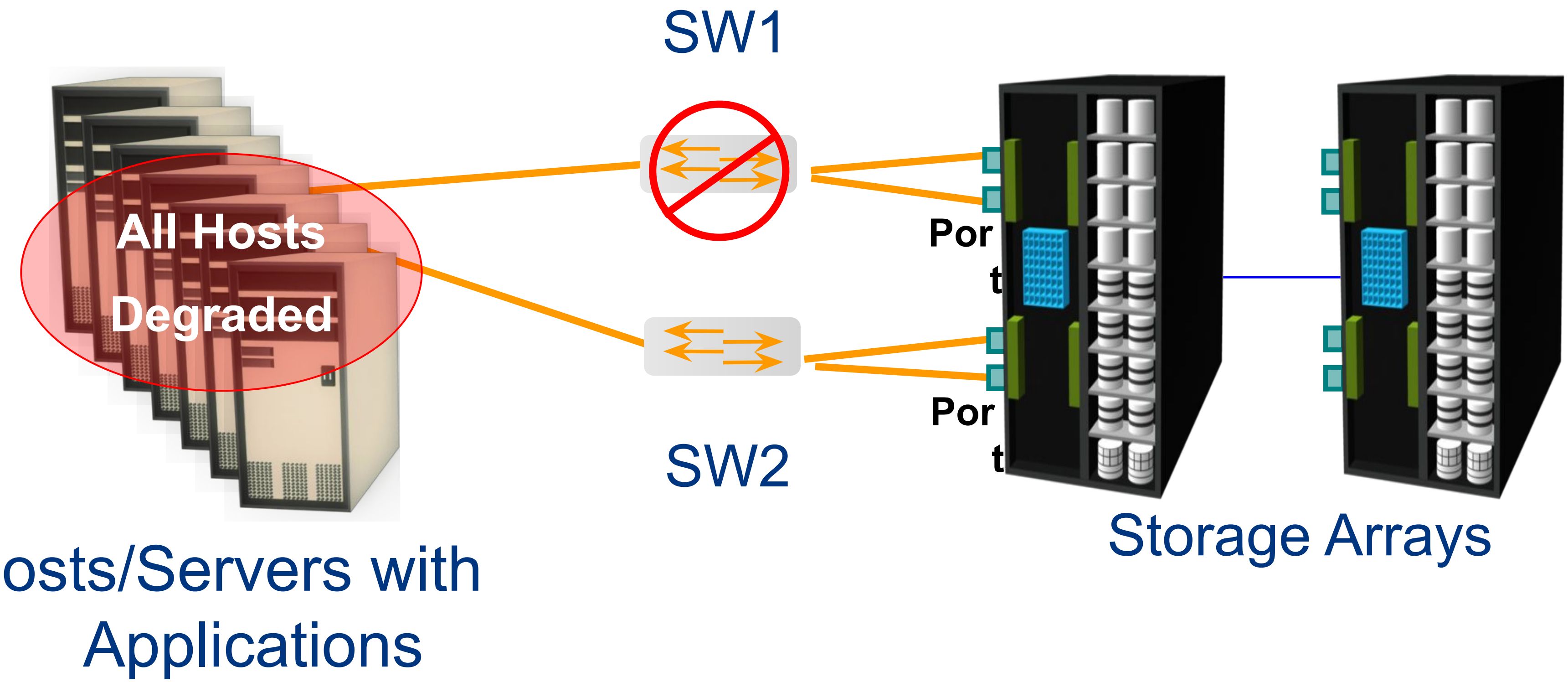
Hosts/Servers with Applications

Accessibility Monitoring Example: HBA Failure

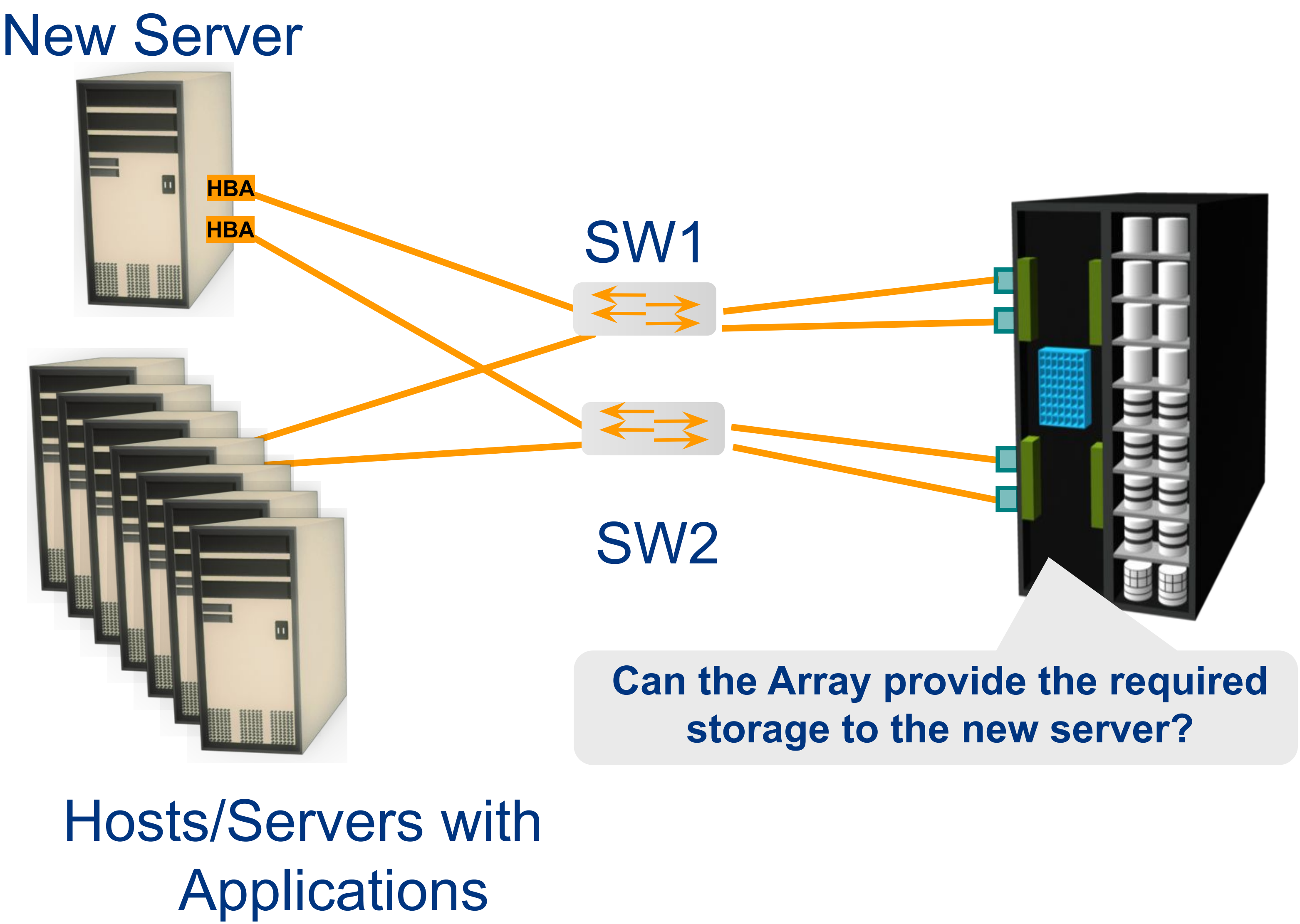


Hosts/Servers with Applications

Accessibility Monitoring Example: Switch Failure

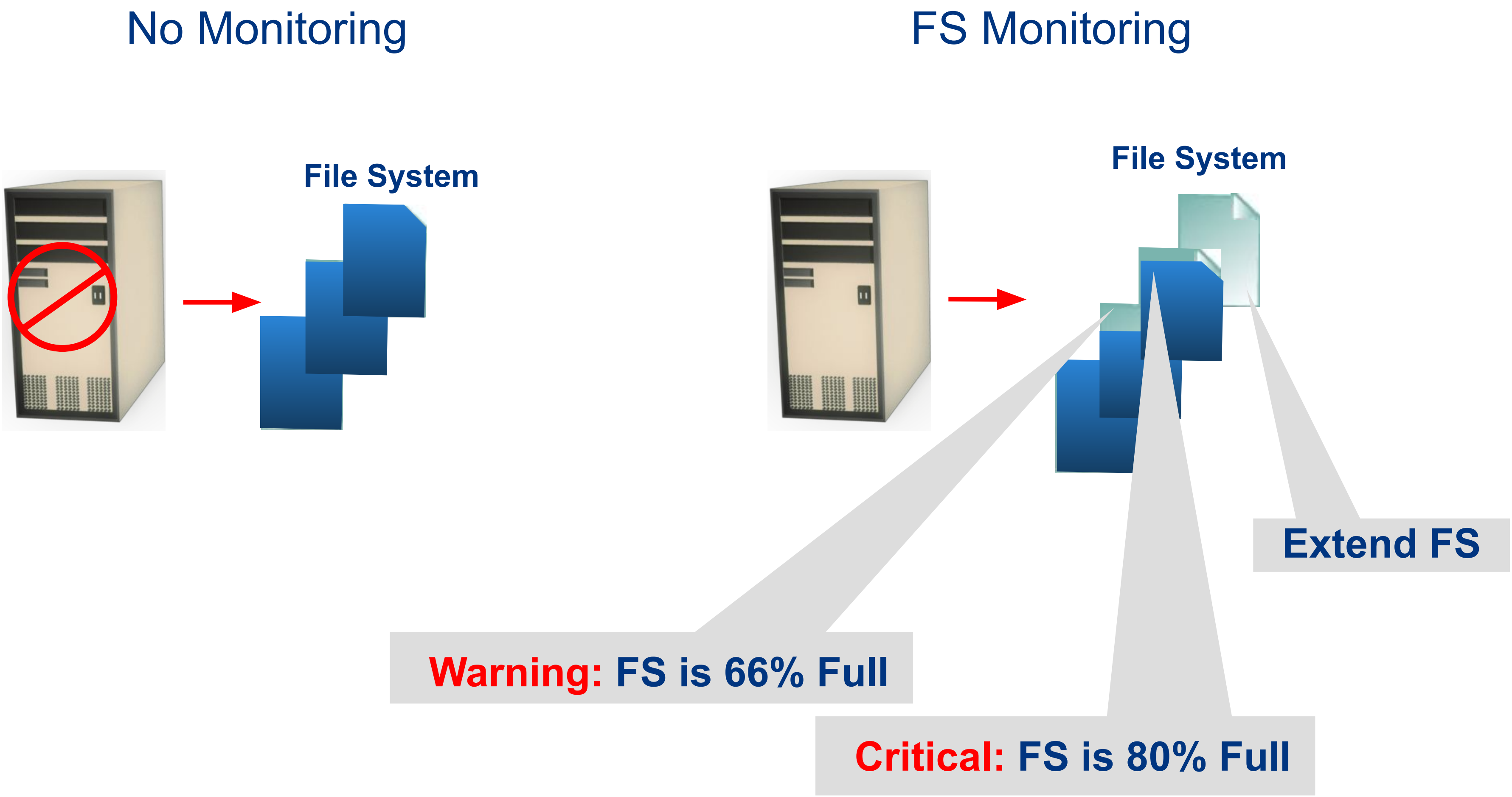


Capacity Monitoring Example: Storage Array



Can the Array provide the required storage to the new server?

Capacity Monitoring Example: File System Space



No Monitoring

File System

FS Monitoring

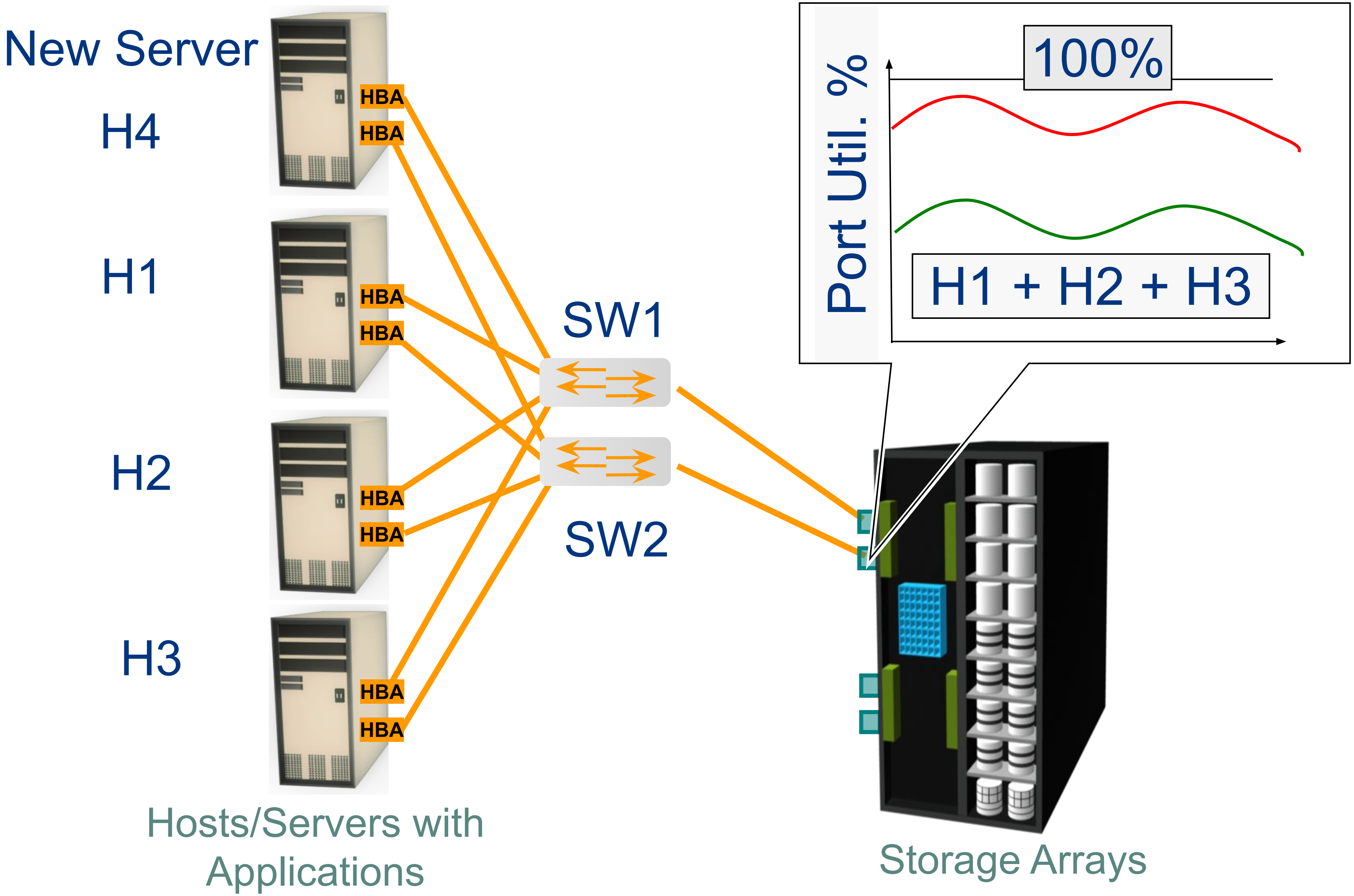
File System

Extend FS

Warning: FS is 66% Full

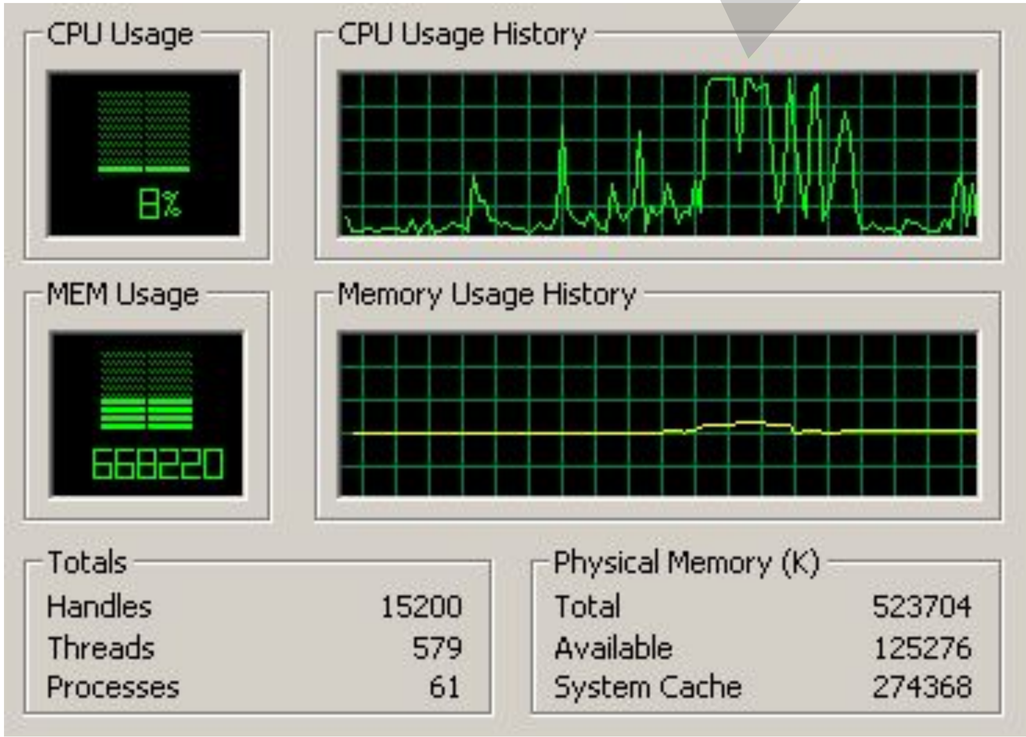
Critical: FS is 80% Full

Performance Monitoring Example: Array Port Utilization



Performance Monitoring Example: Servers CPU Utilization

Critical: CPU Usage above 90% for the last 90 minutes



CPU Usage

8%

CPU Usage History

MEM Usage

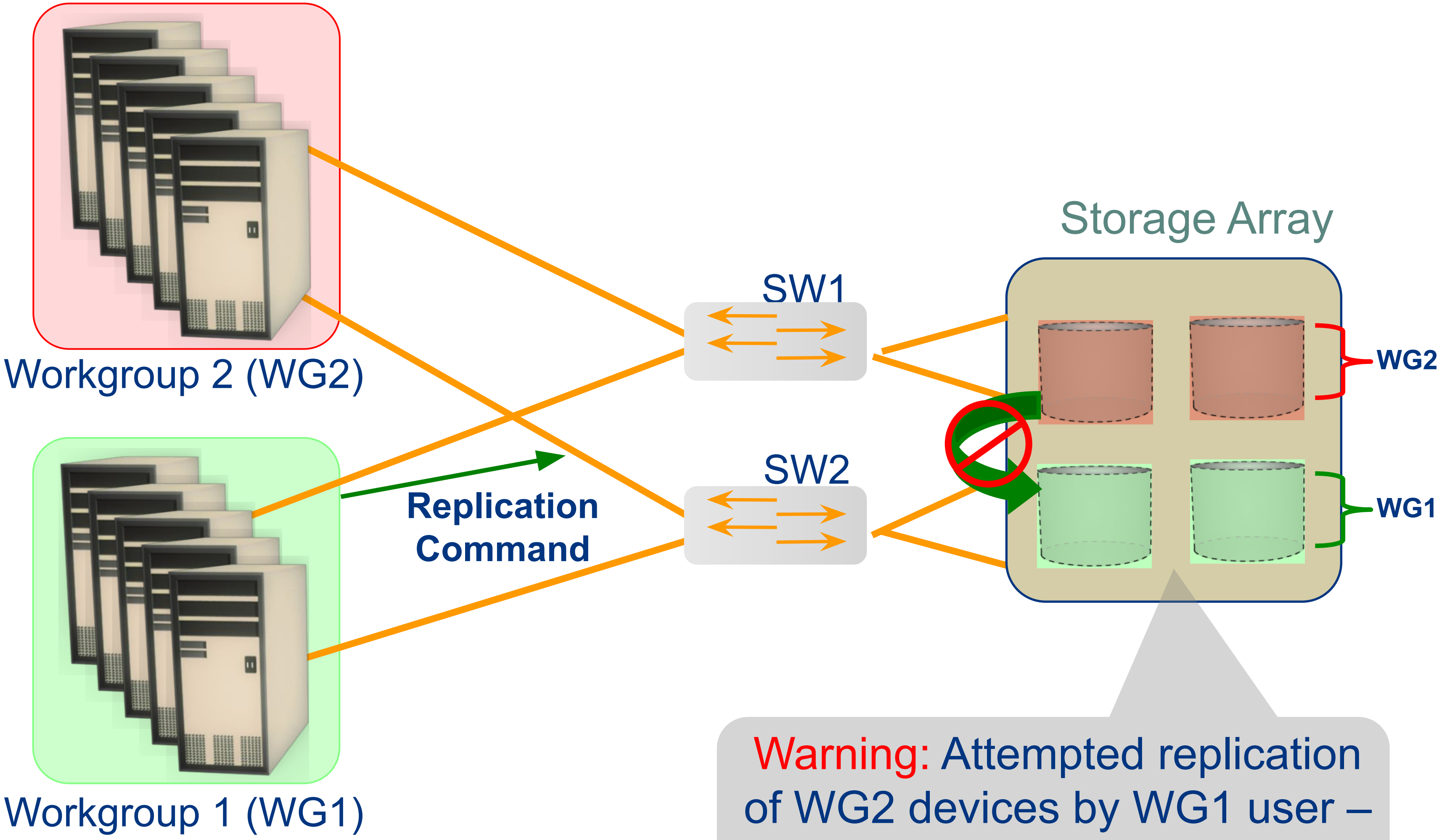
668220

Memory Usage History

Totals	
Handles	15200
Threads	579
Processes	61

Physical Memory (K)	
Total	523704
Available	125276
System Cache	274368

Security Monitoring Example: Storage Array



Warning: Attempted replication of WG2 devices by WG1 user – Access denied

Alerting of Events

- Alerting is an integral part of monitoring
- Monitoring tools enables administrators to assign different severity levels for different events
- Level of alerts based on severity
  - **Information alert**: Provide useful information and may not require administrator intervention
    - Creation of zone or LUN
  - **Warning alerts**: Require administrative attention
    - File systems becoming full/Soft media errors
  - **Fatal alert**: Require immediate administrative attention
    - Power failures/Disk failures/Memory failures/Switch failures

Lesson Summary

Key concepts covered in this module are:

- Storage infrastructure components that should be monitored
- Parameters of monitoring:
  - Accessibility
  - Capacity
  - Performance
  - Security
- Monitoring examples

Additional Task

Research on key requirements of a data center

Storage Management Activities

- All the management tasks in a storage infrastructure can be broadly categorized into:
  - Availability management
  - Capacity management
  - Performance management
  - Security management
  - Reporting

Availability Management

- Establishing a proper guideline for all configurations to ensure availability based on service levels.
- Example: When a server is deployed to support a critical business function, the highest availability standard is required. This involved deploying the following components:
  - Two or more HBAs
  - Multipathing software
  - Server clustering
  - Two independent fibre channel switches
  - RAID protection
  - Backup
  - Local and remove replication

Capacity Management

- Ensure adequate availability of resources for all services based on their service level requirements
- Capacity management provides:
  - Capacity analysis – compare allocated storage to forecasted storage on a regular basis
  - Trend analysis – actual utilization of allocated storage and rate of consumption
- Example 1: Storage provisioning
  - Device configuration and LUN masking on storage arrays
  - Zoning configuration on SAN and HBA components
- Example 2: Estimating future needs of resources
  - Gather and analyze related information to come up with estimates

Performance Management

- Ensures the optimal operational efficiencies of all components
- Performance analysis is performed on existing storage infrastructure components
  - Provides information whether a component is meeting expected performance levels
- When a new application or server is to be deployed, every components involved must be validated for adequate performance capabilities as defined by the service levels.
  - Server: volume configuration, database design, application layout on multiple HBAs, multipathing software
  - SAN: designing sufficient ISLs in a multi-switch fabric with adequate bandwidth
  - Storage arrays: selecting appropriate RAID type and LUN layout, front-end and back-end ports, LUN masking

Security Management

- Prevents unauthorized access and configuration of storage infrastructure components
- Example: When deploying a new application or server
  - Managing user accounts and access policies
  - Zoning configuration in the SAN
  - LUN masking

Reporting

- Keeping track and gathering information from various components / processes
- This information is compiled to generate reports for:
  - Trend analysis and capacity planning – current and historic information about utilization of storage, file system, database tablespace, ports
  - Configuration or asset management – device allocation, local and remote replicas, fabric configuration, list of equipment with details such as their value, purchase date, lease status and maintenance record
  - Chargeback – allocation and utilization of storage infrastructure components by various departments / user groups.
  - Performance – performance of various storage infrastructure components

Storage Infrastructure Management Challenges

- Large number and variety of storage arrays, networks, servers, databases and applications
- Variety of storage devices varying in capacity, performance and protection methodologies
- Deployment of both SAN and IP networks for storage devices
- Servers with different operating systems: UNIX, LINUX, Windows, mainframe
- Interoperability issues between devices from multiple vendors
- Multiple vendor-specific tools to monitor devices from different vendors