

# Project 10:

## Designing and Securing a Corporate Data Center Network

### Prepared by:

1. Khaled Elawady Elgamal
2. Abdalrahman Saad Hamed (Team Leader)
3. Gena Esbergen
4. Sama Mostafa
5. Rowaida Abdelnasser
6. George Hany

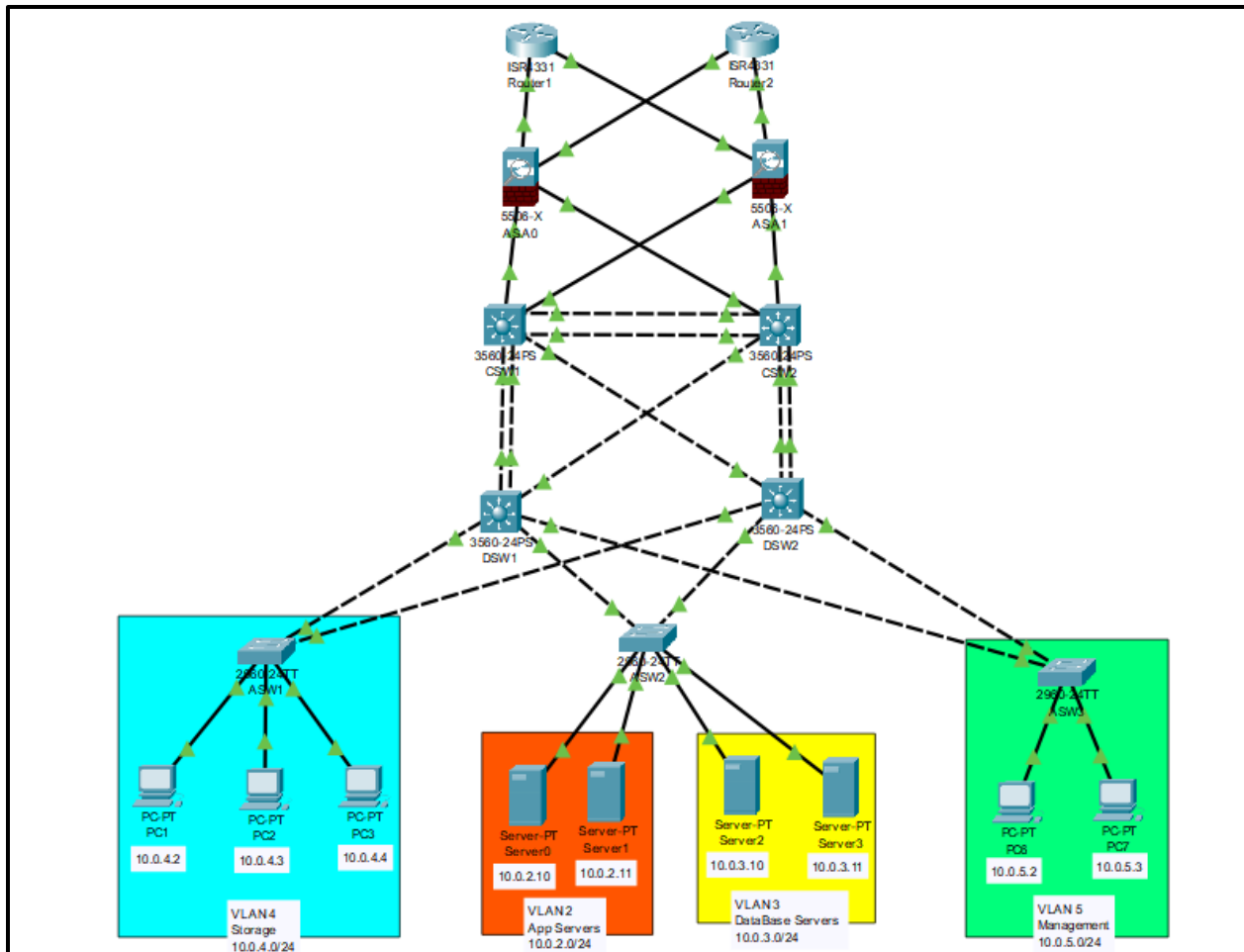
### Network Topology Design:

The data center uses a three-tier hierarchical model (core layer, aggregation/distribution layer, access layer) to balance performance, scalability and manageability. **The core layer** acts as the backbone, interconnecting all parts of the network; it uses powerful cisco switches and routers with redundant links to eliminate single points of failure. **The Distribution layer** sits between core and access enforcing policies. It connects access switches to the core, performs VLAN routing/segmentation, and filters traffic. **The Access layer** provides network access to servers, storage devices and management team.

- **Core Layer:** Central backbone with high-speed, low-latency switches and routers. Implemented as a redundant pair of core switches with

high throughput. Redundant uplinks and backup devices ensure continuity if one core unit fails.

- **Aggregation (Distribution) Layer:** Aggregates multiple access switches and uplinks them to the core. Implements inter-VLAN routing and enforces security/quality policies. Usually consists of dual (redundant) distribution switches with multilayer (L3) capability. Traffic is load-balanced across them and VLANs are segmented at this layer.
- **Access Layer:** Entry point for servers and storage devices. Composed of rack switches providing connectivity to hosts. Supports port security and access controls. Access switches are dual homed to the aggregation layer for resiliency.



Device roles in this topology include:

- **Switches:** Connect hosts and interconnect other switches. Data center switches form each layer of the hierarchy and carry VLAN traffic. They ensure efficient data flow and implement features like VLAN tagging and link aggregation.
- **Routers:** Provide L3 connectivity. Core routers manage traffic between the data center and external networks and route between VLAN subnets. Routers at distribution may handle inter-VLAN routing if core is purely switching.
- **Firewalls:** Deployed at the network edge and between tiers to enforce security. They filter traffic entering and leaving the data center (north-

south) and can also segment trust zones internally (east-west).  
Firewalls monitor and block unauthorized flows.

- **Servers/Hosts:** Application, database, and storage servers connect at the access layer. They host corporate applications, data services and connect over the network via their top-of-rack switch.

**Redundancy** is built into every layer to avoid single points of failure. Core and distribution switches are deployed in pairs in an active/standby configuration with equal-cost paths. Access switches typically have dual uplinks to aggregation switches using EtherChannel so that any single link or switch failure still leaves alternate paths. **Spanning Tree Protocol (STP)** runs on switches to allow these redundant links without loops.

## VLANs:

VLANs are essential in modern data center networks as they allow logical segmentation of devices and traffic without requiring separate physical infrastructure. By isolating different types of network traffic into separate VLANs, we enhance **performance**, **security**, and **manageability**.

In this project, VLANs were implemented to logically separate functions within the data center. Each VLAN represents a unique service or group of devices (e.g., application servers, database servers, storage systems). This segmentation helps:

- **Limit broadcast traffic**, improving overall network efficiency.
- **Enhance security** by isolating sensitive traffic (e.g., database and storage VLANs) from general application or management traffic.
- **Simplify access control** and policy enforcement, as rules can be applied at the VLAN or inter-VLAN routing level.

- **Support high availability and scalability** by allowing network administrators to manage and expand services independently.

VLAN ID	VLAN Name	IP Subnet	Associated Devices/Services
5	Management	10.0.5.0/24	Switch/server management (SSH, SNMP); OOB management interfaces
2	Application	10.0.2.0/24	Application/web servers
3	Database	10.0.3.0/24	Database servers
4	Storage	10.0.4.0/24	Backup

The chosen segmentation — such as separate VLANs for management, applications, databases, and storage — reflects best practices for separating roles and minimizing attack surfaces. For instance, the management VLAN isolates device management interfaces from user traffic, while the storage VLAN ensures storage protocols do not compete with application traffic for bandwidth.

## IP Addressing Scheme:

Each VLAN is assigned a unique subnet to clearly distinguish traffic types and support routing, ACLs, and segmentation policies. This approach minimizes confusion, simplifies troubleshooting, and aligns with best practices for enterprise network design.

Subnets were allocated as follows:

- Each VLAN was given a /24 subnet to support up to 254 usable hosts.
- For Vlan 4 & 5 we developed a **DHCP** to automatically assign IPs.

- IP addresses were assigned to servers and devices based on their roles within each VLAN.
- Gateways are implied to be at .1 for consistency.

VLAN ID	VLAN Name	Subnet	Assigned IPs	Devices / Purpose
VLAN 2	App Servers	10.0.2.0/24	10.0.2.10, 10.0.2.11	Server0, Server1 (App Servers)
VLAN 3	Database Servers	10.0.3.0/24	10.0.3.10, 10.0.3.11	Server2, Server3 (DB Servers)
VLAN 4	Storage	10.0.4.0/24	DHCP	PC0, PC1, PC2 (Storage Devices)
VLAN 5	Management	10.0.5.0/24	DHCP	PC6, PC7 (Admin)

## High Availability Planning

To minimize downtime and ensure fault tolerance, we implemented first-hop redundancy protocols and loop-avoidance protocols across the network. Key elements include:

**Router Redundancy (HSRP):** It's configured on the distribution layer switches dividing the traffic of the vlans on the two switches as the DSW1 is **active** for **vlan 4 & 2** and **standby** for **vlan 3 & 5**, The DSW2 is **active** mode for **vlan 3 & 5** and **standby** for **vlan 4 & 2**. They share a virtual IP address the default gateway for hosts. If the active layer 3 switch fails, the standby immediately takes over, preserving host connectivity.

### DSW1 Standby Table:

Interface	Group	Priority	State	Active	Standby	Virtual IP
Vlan 2	2	105	Active	Local	10.0.2.1	10.0.2.50

Vlan 3	3	95	Standby	10.0.3.1	Local	10.0.3.50
Vlan 4	4	105	Active	Local	10.0.4.1	10.0.4.50
Vlan 5	5	95	Standby	10.0.5.1	Local	10.0.5.50

### **DSW2 Standby Table:**

Interface	Group	Priority	State	Active	Standby	Virtual IP
Vlan 2	2	95	Standby	10.0.2.1	Local	10.0.2.50
Vlan 3	3	105	Active	Local	10.0.3.1	10.0.3.50
Vlan 4	4	95	Standby	10.0.4.1	Local	10.0.4.50
Vlan 5	5	105	Active	Local	10.0.5.1	10.0.5.50

- **Switch Redundancy (STP):** All redundant L2 links use Spanning Tree Protocol to prevent loops. We designate one core switch as the STP root bridge (primary) and the other as secondary, ensuring predictable path selection. When links or switches fail, STP reconverges to unblock alternate paths so that uplinks remain available. STP settings (root priorities, port costs) are tuned so that traffic normally flows symmetrically, and failover is quick.
- **Link Aggregation:** Critical links between switches are bundled into EtherChannel so that physical interface failures do not interrupt the logical connection. Aggregated ports between core and aggregation increase throughput and provide path redundancy.

These measures ensure that the data center network remains operational under faults, maintaining continuous connectivity and quick recovery of services. The combination of HSRP, STP and redundant links provides the high availability required for corporate data center operations.

## **OSPF Routing:**

- OSPF is implemented as the primary routing protocol to facilitate dynamic routing within the data center.
- Configuration includes defining OSPF areas, network types, and router IDs on core and distribution layer devices.
- OSPF ensures efficient path determination and automatic rerouting in case of link failures, enhancing network resilience.
- Parameters are tuned to optimize convergence time and minimize routing overhead.

**Security Implementation:** Initial security measures are implemented, with a focus on secure management access.

- **SSH Configuration:**

- SSH is configured as the primary protocol for secure remote access to network devices, replacing Telnet.
- Configuration involves generating SSH keys, securing access with strong passwords or key-based authentication, and disabling insecure protocols.
- Access control list is used to restrict SSH access to management VLAN administrator workstations.



- Firewalls, IDS, and IPS systems are initially set up with basic configurations to provide fundamental security. Further detailed configuration and tuning will occur in subsequent phases.
- Network access control is implemented to start defining policies for device and user access, focusing on initial segmentation and restricting unnecessary access.

---

## MLS2 ACL Configuration Documentation

📍 **Device: MLS2 (Multilayer Switch 2)**

🎯 **Purpose: Apply VLAN-specific access control for zone-based network segmentation and security.**

# Least Privilege ACL

## 1. VLAN 2 – Application Servers (APP\_LIMIT)









**Access List Name:** APP\_LIMIT

**Interface Applied:** vlan 2 (Inbound)

**Purpose:**

- Allow secure HTTPS access from public clients.
- Limit monitoring and management access to MGMT VLAN only.
- Allow SQL communication from DB to App.

**Rules:**

-  Allow **HTTPS** from public (any) to App servers (10.0.2.0/24) on port 443.
-  Allow **ICMP** from 10.0.5.100 (MGMT host) to App servers.
-  Allow **SNMP & Syslog** from App to MGMT (10.0.5.0/24).
-  Allow **Zabbix Monitoring** (TCP port 10050) from MGMT to App.
-  Allow **NTP** (UDP 123) from MGMT to App.
-  Allow **SQL** (TCP 1433) between App servers and DB (10.0.3.0/24).
-  Allow **SSH/RDP** access from MGMT to App.
-  Block all other **ICMP**, **SSH (22)**, **RDP (3389)**, and unspecified traffic.

## 2. VLAN 3 – Database Servers (DB\_LIMIT)








**Access List Name:** DB\_LIMIT

**Interface Applied:** vlan 3 (Inbound)

**Purpose:**

- Control access to the DB zone.
- Allow necessary App, MGMT, and Storage communication.
- Secure the database zone from unauthorized traffic.

#### Rules:

-  Allow **ICMP** from 10.0.5.100 (MGMT) to DB.
-  Allow **SNMP & Syslog** from DB to MGMT.
-  Allow **SQL** communication between App and DB servers.
-  Allow **Zabbix Monitoring** and **NTP** from MGMT.
-  Allow **Storage Access** using NFS, SMB (TCP 2049/445, UDP 137/138).
-  Allow **SSH/RDP** access from MGMT to DB servers.
-  Deny all other **ICMP, SSH, RDP**, and unspecified traffic with logging.

### 3. VLAN 4 – Storage Servers (STORAGE\_LIMIT)






**Access List Name:** STORAGE\_LIMIT

**Interface Applied:** vlan 4 (Inbound)

#### Purpose:

- Restrict Storage VLAN communication.
- Allow only approved protocols and services.

#### Rules:

-  Allow **ICMP** from 10.0.5.100 (MGMT) to Storage.
-  Allow **NFS & SMB** communication from Storage to DB zone.
-  Allow **SNMP & Syslog** from Storage to MGMT.
-  Block **SSH/RDP** traffic to/from Storage.
-  Block all other outgoing traffic from Storage VLAN.

### 4. VLAN 5 – Management Zone (MGMT\_FULL\_ACCESS)


**Access List Name:** MGMT\_FULL\_ACCESS

**Interface Applied:** vlan 5 (Outbound)

#### Purpose:

- Grant unrestricted full access to MGMT VLAN for administrative operations and monitoring.

#### Rules:

-  Permit **all traffic** from MGMT zone (10.0.5.0/24) to any destination.

#### Notes:

- All ACLs are **applied inbound** on their respective VLAN interfaces, except MGMT which is **outbound** to allow admin access to other zones.
- Logging is enabled for denied traffic where applicable.
- Protocol-specific ports are chosen based on common enterprise standards:
  - **HTTPS**: 443
  - **SQL Server**: 1433
  - **NFS**: 2049
  - **SMB**: 445 (TCP), 137/138 (UDP)
  - **SNMP**: 161
  - **Syslog**: 514
  - **Zabbix Agent**: 10050
  - **NTP**: 123
  - **SSH**: 22
  - **RDP**: 3389

# ASA Firewall ACL Documentation

## ACL Name: INSIDE\_IN

**Interface Applied On:** inside

**Direction:** inbound

### ACL Rules Breakdown:

#### ☒ Allow HTTPS to App Servers

```
access-list INSIDE_IN extended permit tcp any 100.0.2.0 255.255.255.0  
eq 443
```

#### ☒ Allow App → DB SQL

```
access-list INSIDE_IN extended permit tcp 100.0.2.0 255.255.255.0  
100.0.3.0 255.255.255.0 eq 1433
```

#### ☒ Allow Storage → DB NFS & SMB

```
access-list INSIDE_IN extended permit tcp 100.0.4.0 255.255.255.0  
100.0.3.0 255.255.255.0 eq 2049  
access-list INSIDE_IN extended permit tcp 100.0.4.0 255.255.255.0  
100.0.3.0 255.255.255.0 eq 445  
access-list INSIDE_IN extended permit udp 100.0.4.0 255.255.255.0  
100.0.3.0 255.255.255.0 eq 137
```

```
access-list INSIDE_IN extended permit udp 100.0.4.0 255.255.255.0  
100.0.3.0 255.255.255.0 eq 138
```

### ☒ **Allow Management Host (10.0.5.100) → Any**

```
access-list INSIDE_IN extended permit icmp host 10.0.5.100 any echo  
access-list INSIDE_IN extended permit tcp host 10.0.5.100 any eq 22  
access-list INSIDE_IN extended permit tcp host 10.0.5.100 any eq 3389  
access-list INSIDE_IN extended permit tcp 10.0.5.0 255.255.255.0 any  
eq 10050  
access-list INSIDE_IN extended permit udp 10.0.5.0 255.255.255.0 any  
eq 123
```

### ☒ **Allow Monitoring → MGMT VLAN**

```
access-list INSIDE_IN extended permit udp 100.0.3.0 255.255.255.0  
10.0.5.0 255.255.255.0 eq 161  
access-list INSIDE_IN extended permit udp 100.0.3.0 255.255.255.0  
10.0.5.0 255.255.255.0 eq 514  
access-list INSIDE_IN extended permit udp 100.0.2.0 255.255.255.0  
10.0.5.0 255.255.255.0 eq 161  
access-list INSIDE_IN extended permit udp 100.0.2.0 255.255.255.0  
10.0.5.0 255.255.255.0 eq 514
```

### ☒ **Deny all other traffic (with logging)**

```
access-list INSIDE_IN extended deny ip any any log
```

## **Apply ACL to Inside Interface:**

```
access-group INSIDE_IN in interface inside
```

## Summary of Effects

NETWORK	ALLOWED TRAFFIC
App Servers	Public HTTPS allowed
DB Servers	Accept only App SQL and Storage NFS/SMB.
Storage	NFS/SMB to DB only.
Management	ICMP, SSH, RDP, Zabbix, NTP anywhere
Monitoring	SNMP & Syslog allowed
All other	Dropped and logged

# Baseline Monitoring Setup

## 1. Syslog Server Setup (PC in VLAN5 - 10.0.5.100)

- **IP Configuration:**
  - IP: 10.0.5.100
  - Subnet: 255.255.255.0
  - Gateway: 10.0.5.1
- **Enable Syslog Service:**

- Services > Syslog > Enable (default settings)

## 2. MLS2 & ASA Syslog Configuration

```
logging 10.0.5.100      # Syslog server IP
logging trap debugging  # Severity level
service timestamps log datetime msec
```

- **Severity Levels:** Critical(2), Warning(4), Informational(6), Debugging(7)

## 3. SNMPv2c Setup (Router & MLS)

```
snmp-server community SECURE_COMMUNITY ro
```

- Replace SECURE\_COMMUNITY with a strong community string for security.

## 4. Monitoring Tool Simulation (PC in VLAN5)

- Use the Syslog Server PC as a simulated monitoring system (e.g., Zabbix).
- Collects Syslog and SNMP data from Router & MLS switches.

## 5. Testing Steps

1. On Router:

```
debug ip icmp
```

2. Ping Router from another device.
3. Verify logs on Syslog Server (10.0.5.100).



## Summary

Item	Details
Syslog Server IP	10.0.5.100
SNMP Devices	Router, MLS1, MLS2
Logging Level	Informational
SNMP Community	SECURE_COMMUNITY (RO)
Monitoring Tool	Simulated (PC acting as Zabbix)

This config enables secure logging and performance monitoring via Syslog and SNMP, documented for future reference.