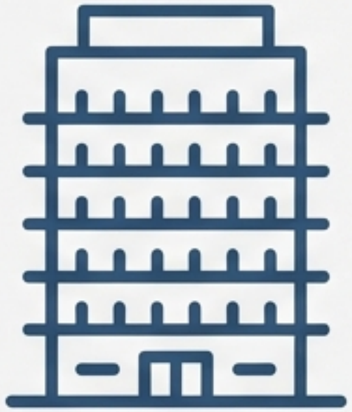
Theta Company: Architecting a Resilient & Secure Infrastructure

A Strategic Proposal for a Future-Proof Foundation

120 Users

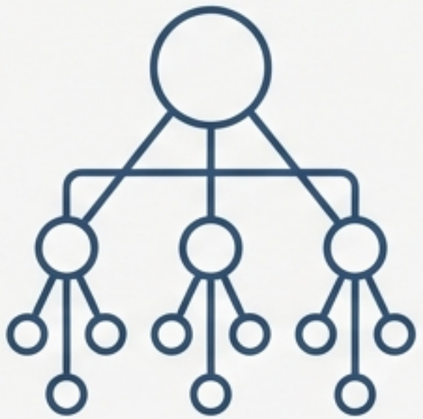


6 Floors

Defense in Depth Security Model

A Turnkey Infrastructure for €226,000

We propose a comprehensive infrastructure overhaul designed to support Theta Company's operational needs and meet rigorous security requirements. The investment is built on three core pillars:



Modern Architecture

A hierarchical, segmented network designed for scalability and performance across 6 floors.

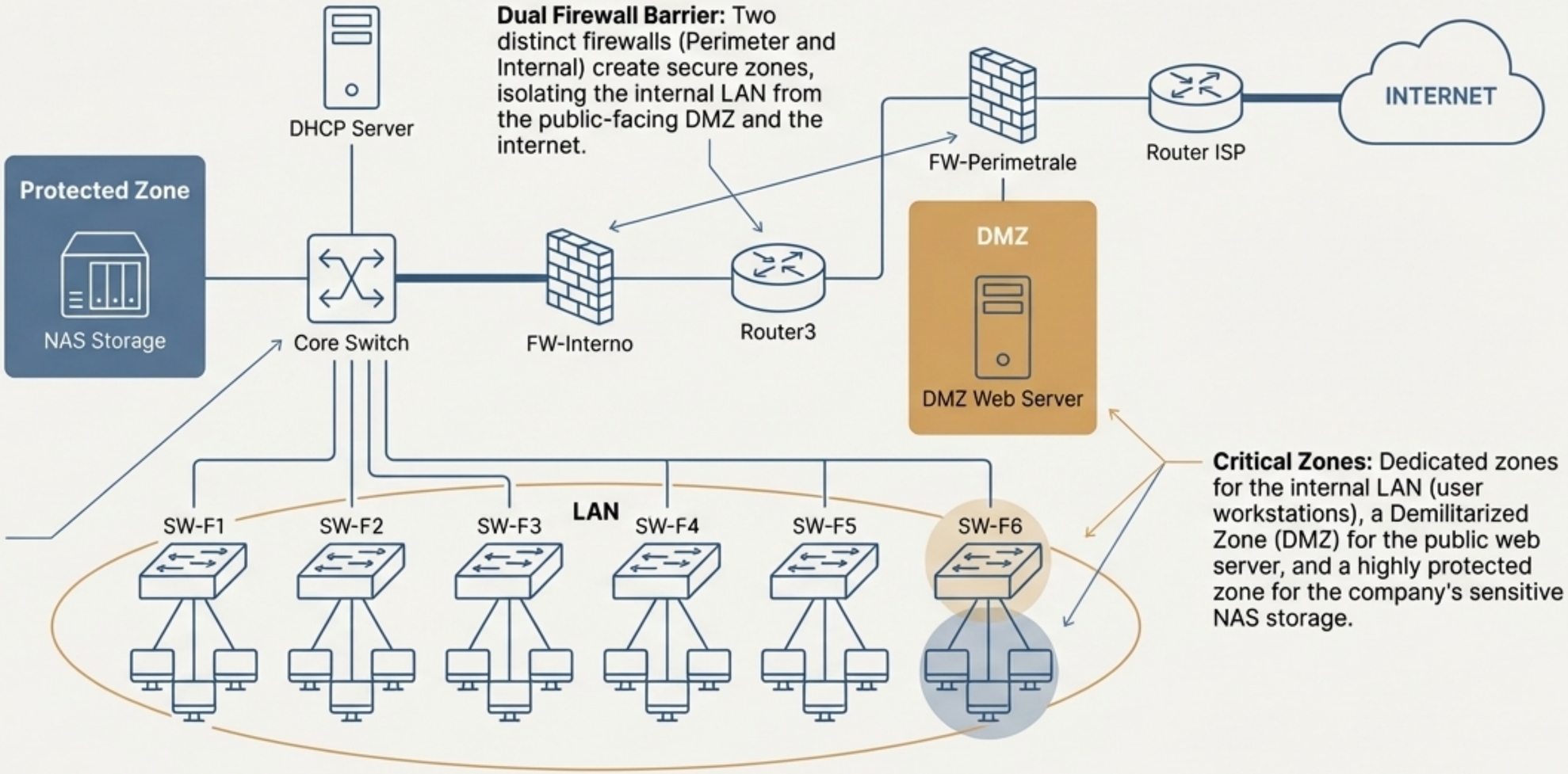
Tiered Hardware

Performance-optimized hardware, from the network core to user workstations, tailored to specific roles to balance cost and capability.

In-Depth Security

A multi-layered defense strategy, validated by rigorous engineering and custom-developed auditing tools.

The Architectural Blueprint: A Hierarchical and Segmented Design

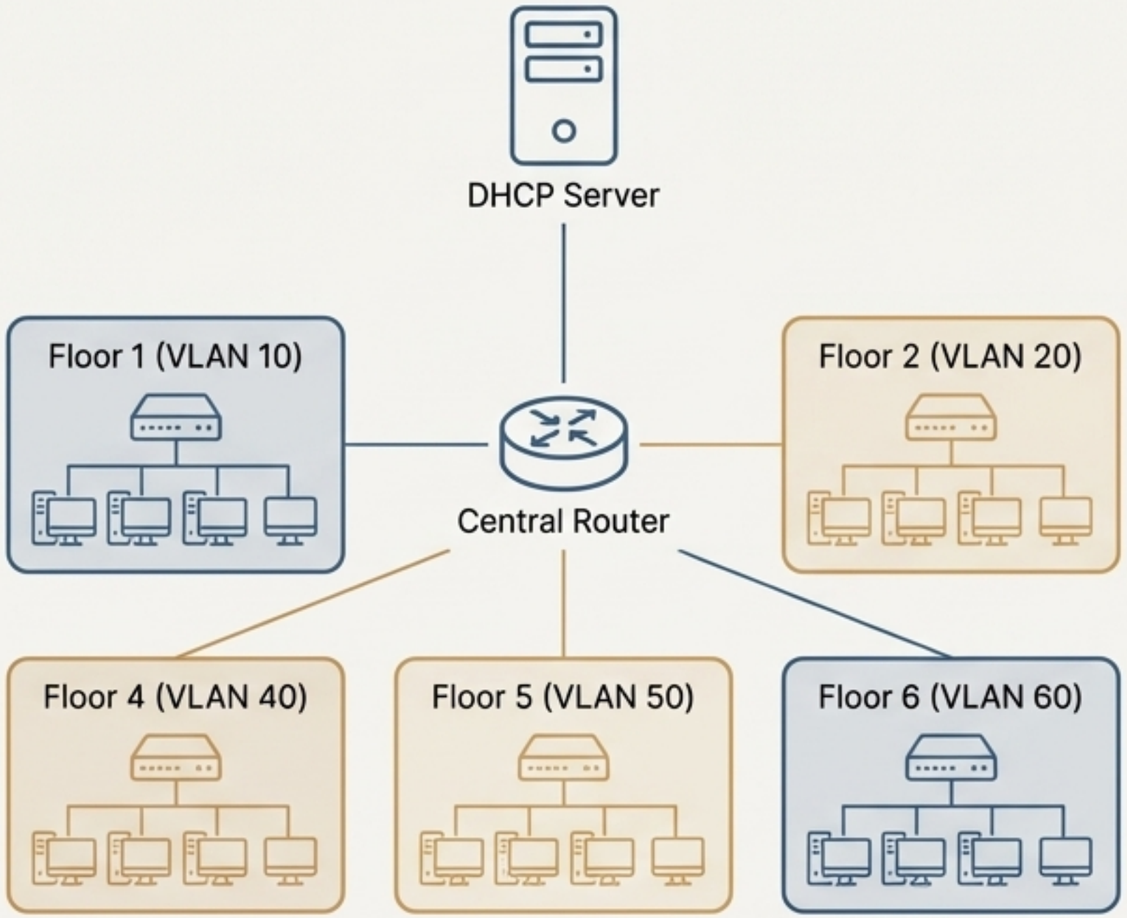


Hierarchical Model (Core/Access): A central Core Switch aggregates traffic from 6 Access Layer switches (one per floor), ensuring scalability and simplified fault management.

Critical Zones: Dedicated zones for the internal LAN (user workstations), a Demilitarized Zone (DMZ) for the public web server, and a highly protected zone for the company's sensitive NAS storage.

Logical Segmentation Supports 120 Users Across 6 Floors

The network is logically divided to enhance security and performance.



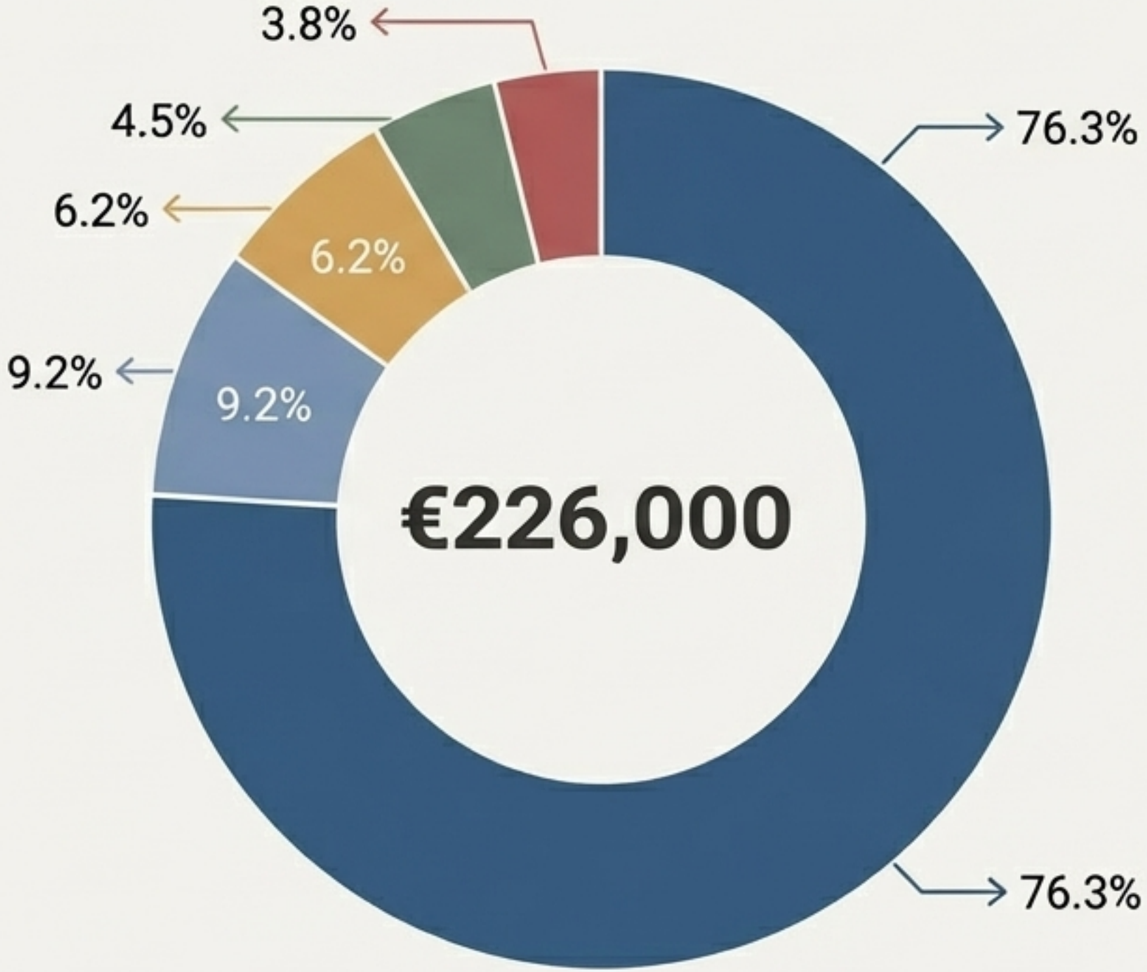
VLANs for Isolation

Each of the 6 floors is assigned a dedicated VLAN (e.g., VLAN 10, 20, 30...). This isolates broadcast traffic, improving performance and containing potential security issues within a single floor.

Centralized DHCP Management

A single, dedicated DHCP Server manages IP address assignment for all 120 hosts across all VLANs. The `ip helper-address` command on the router ensures seamless, automated configuration for every user.

Justifying the €226,000 Investment: A Breakdown



- Flotta PC (Workstations): €172,500
- Network & Security: €20,800
- Manodopera (Labor): €14,000
- Server Farm: €10,200
- Licenze & Supporto (Licenses & Support): €8,500

Key Insight

The majority of the investment is allocated to user workstations, directly impacting employee productivity. The network, security, and server components represent a calibrated 'Business Standard' (Tier 2) selection, avoiding both underpowered and overpriced solutions.

A Tailored Approach to Workstations: The Right Tool for Every Role

TIER 1: Low-End

Users: 20 (Amministrazione, HR, Segreteria)

Specs: Dell OptiPlex / HP Pro (i5, 16GB RAM, 512GB SSD)

Total Cost: €15,000 **(€750/unit)**

TIER 2: Mid-Range

Users: 75 (Consulenti, PM, Sales)

Specs: Dell Latitude / HP EliteBook (i7, 32GB RAM, 1TB SSD)

Total Cost: €97,500 **(€1,300/unit)**

TIER 3: High-End

Users: 25 (Sviluppatori, DevOps)

Specs: Dell Precision / Lenovo P-Series (i9/Xeon, 64GB RAM, Dedicated GPU)

Total Cost: €60,000 **(€2,400/unit)**

By segmenting the 120 workstations based on actual job requirements, we optimize the **€172,500 fleet cost**, ensuring technical staff have the necessary power while containing expenses for administrative roles.

Security in Practice: Implementing the Principle of Least Privilege

The pfSense firewall's LAN interface rules are configured to control all outbound traffic, ensuring that only necessary communication is allowed. The rules are processed top-down.

Admin SSH to DMZ

PASS

Rule Number: 2
Source: 192.168.50.151 (Admin Host)
Destination: 192.168.51.10 (DMZ Server)
Port: TCP 22

Restricts server management access to a single, authorized administrative workstation, preventing unauthorized access from other internal devices.

Corporate Web Access

PASS

Rule Number: 3
Source: LAN Subnets
Destination: 192.168.51.10 (DMZ Server)
Port: TCP 80

Allows all employees to access the corporate web service, but strictly limits access to the web port only, blocking other potentially vulnerable services.

Reject All Other LAN to DMZ

REJECT

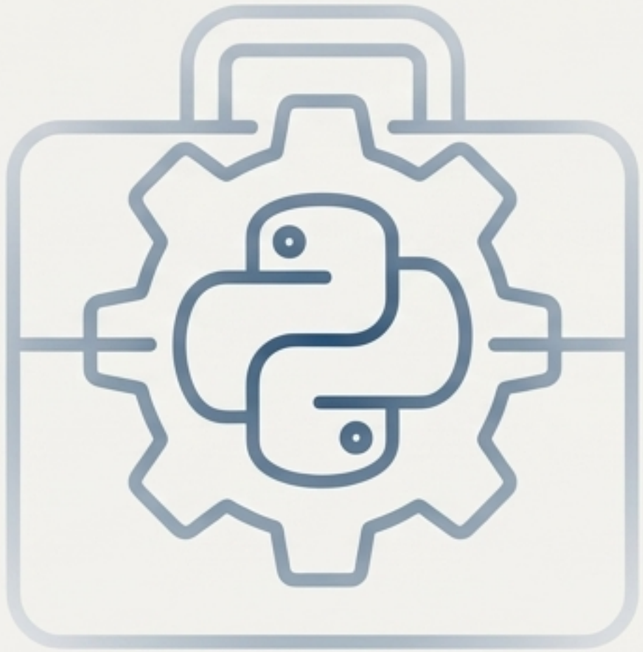
Rule Number: 4
Source: LAN Subnets
Destination: DMZ Subnet
Port: ANY

The cornerstone of internal security. This rule explicitly blocks all other traffic, preventing lateral movement from a compromised PC on the LAN to the DMZ and stopping network scanning attempts.

Proving Security: Custom Tooling for Validation & Auditing

To meet Theta Company's strict audit requirements, we were prohibited from using off-the-shelf scanning software like Nmap. We therefore developed a suite of proprietary Python tools to perform a deep, compliant validation of the network's security posture.

- **Full Compliance**: Adherence to project-specific security guidelines.
- **Granular Control**: Precise, targeted testing of network services and configurations.
- **Demonstrable Expertise**: Proof of deep network and software engineering capabilities.



Tool 1: Port Scanner — Mapping the Attack Surface

Purpose

To verify firewall rules are correctly applied and to identify all exposed services on a target device, as required by the audit.

Core Logic

```
# Use non-blocking connect_ex() to get an OS error code
status = sock.connect_ex((target, port))

if status == 0:
    # TCP Handshake successful -> Port is OPEN
elif status == 111:
    # Connection actively refused -> Port is CLOSED
elif status == 110 or status == 11:
    # Connection timed out -> Port is FILTERED (by
firewall)
```

Proof of Concept: Results from scanning the Web Server (192.168.50.101)

```
Scanning IP 192.168.50.101 from port 10 to 100
Port 21: OPEN
Port 22: OPEN
Port 23: OPEN
Port 25: OPEN
Port 53: OPEN
Port 80: OPEN
Full scan log saved to: scan_192.168.50.101_10-100.log
```

Log File View

```
[2025-12-17 08:48:27] Port 21 -> OPEN
[2025-12-17 08:48:27] Port 22 -> OPEN
[2025-12-17 08:48:27] Port 23 -> OPEN
[2025-12-17 08:48:27] Port 24 -> CLOSED
```

Tool 2: Packet Sniffer — Achieving Layer 2 Traffic Visibility

Purpose

To capture and analyze raw network packets for deep traffic analysis, essential for verifying IDS/IPS placement and understanding data flows.

Core Logic

```
# Create a raw socket to capture at Layer 2 (Ethernet)
sock = socket.socket(socket.AF_PACKET, socket.SOCK_RAW,
        socket.ntohs(0x0003))

# Unpack the binary IP header into a readable format
iph = struct.unpack("!BBHHHBBH4s4s", ip_header)
```

This code allows us to listen directly to the network card driver (AF_PACKET) and decode the binary data of each packet to extract source/destination IPs.

Proof of Concept: Example Capture

```
[+] Filtering packets for IP: 192.168.1.101

Packet 1 (Outgoing Traffic)
  Source IP:       192.168.1.101
  Destination IP:  20.42.65.93

Packet 2 (Incoming Response)
  Source IP:       20.42.65.93
  Destination IP:  192.168.1.101
```

Insight: This demonstrates the ability to monitor conversations at the packet level, confirming traffic is flowing as expected and providing data for security analysis.

Tool 3: HTTP Verb Scanner — Auditing Web Application Security

Purpose

To assess the security configuration of the public-facing web server in the DMZ by testing which HTTP methods (verbs) it allows.

Core Logic

The script uses the Python `requests` library to loop through a list of methods (`OPTIONS`, `GET`, `POST`, `PUT`, `DELETE`) for a target URL, recording the server's response code for each.

Proof of Concept: Results from scanning the DMZ Web Server

Method	Result
OPTIONS	200 OK (Allow=GET, HEAD, POST, OPTIONS, TRACE)
GET	200 OK
POST	200 OK
PUT	405 Method Not Allowed
DELETE	405 Method Not Allowed

The scan confirms a secure baseline configuration. The server correctly allows standard web methods but rejects potentially dangerous ones like PUT and DELETE, preventing unauthorized content modification.

A Turnkey, Resilient Foundation for Theta Company

The proposed investment delivers a complete solution where design principles translate directly into business value.

From Design...

Hierarchical model, VLANs, Centralized DHCP

...To a Scalable & Organized Network

Ready for future growth and easy to manage.

From Hardware...

Tiered Aruba/Dell equipment, tailored workstations

...To a High-Performance User Experience

Empowering every employee with the right tools.

From Security Engineering...

Dual firewalls, 'Least Privilege' rules, custom validation tools

...To a Resilient 'Defense in Depth' Posture

Proven to protect critical company assets.

The €226,000 investment provides Theta Company with a comprehensive, secure, and future-proof infrastructure, delivered and validated with proven engineering expertise.