Building Theta Company's Secure Digital Foundation

A Strategic Investment in Performance, Security, and Scalability

---

Project Reference: Comprehensive Infrastructure & Security Overhaul
Total Proposed Investment: €226,000
Date: 16/12/2025

The €226,000 Investment Delivers a Turnkey ‘Defense in Depth’ Infrastructure

Key Deliverables

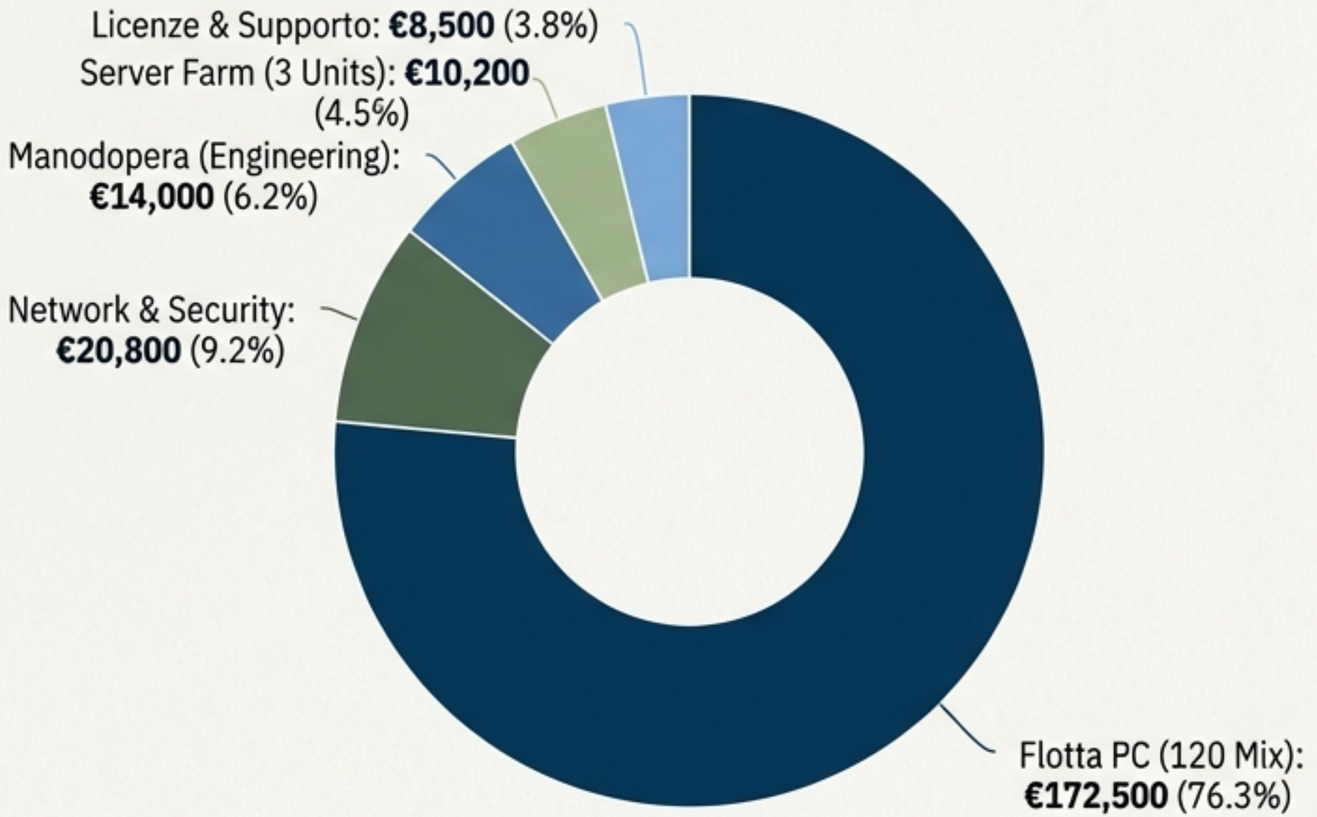
A high-performance network supporting **120 users** across **6 floors**.

A resilient, multi-layered security architecture featuring **dual firewalls**, **network segmentation**, and **3 dedicated IDS/IPS systems**.

A modernized, role-based fleet of **120 workstations** to maximize workforce productivity.

22 man-days of high-end engineering, from architectural design to security validation.

Investment Allocation: €226,000



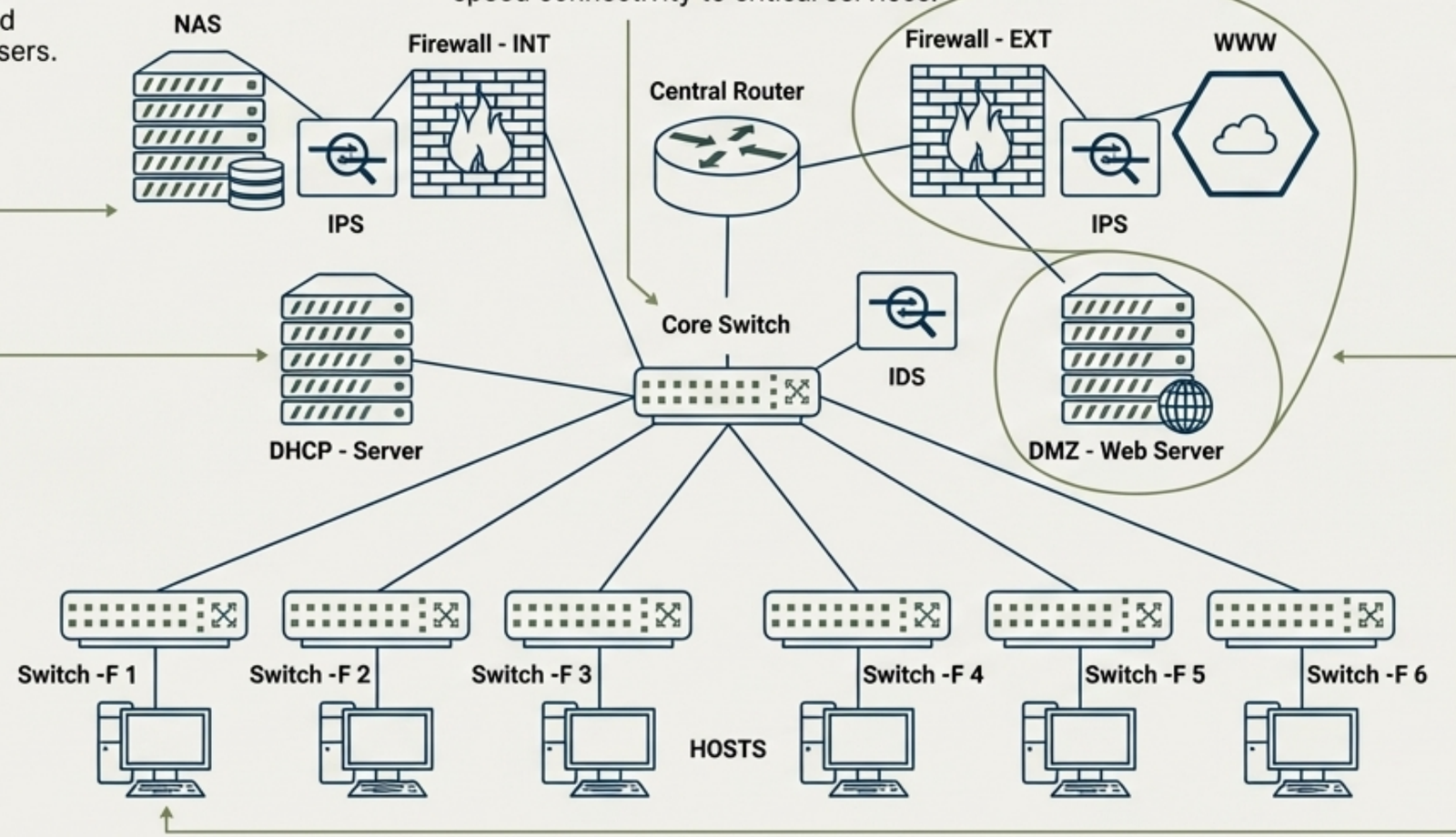
Our Architectural Blueprint: A Resilient, Hierarchical Design

1. **Access Layer**: 6 dedicated switches, one for each floor, ensuring localized performance for 120 users.

2. **Core Layer**: A central Core Switch aggregates all traffic, providing high-speed connectivity to critical services.

3. **Security Zones**: Distinct security zones (Inside, DMZ, Outside) are enforced by a dual-firewall architecture, creating a robust 'Defense in Depth' posture.

4. **Critical Services:** Dedicated servers for DHCP, NAS, and the public-facing DMZ Web Server are strategically placed and protected.



Investing in a High-Performance Network & Security Core (€31,000)

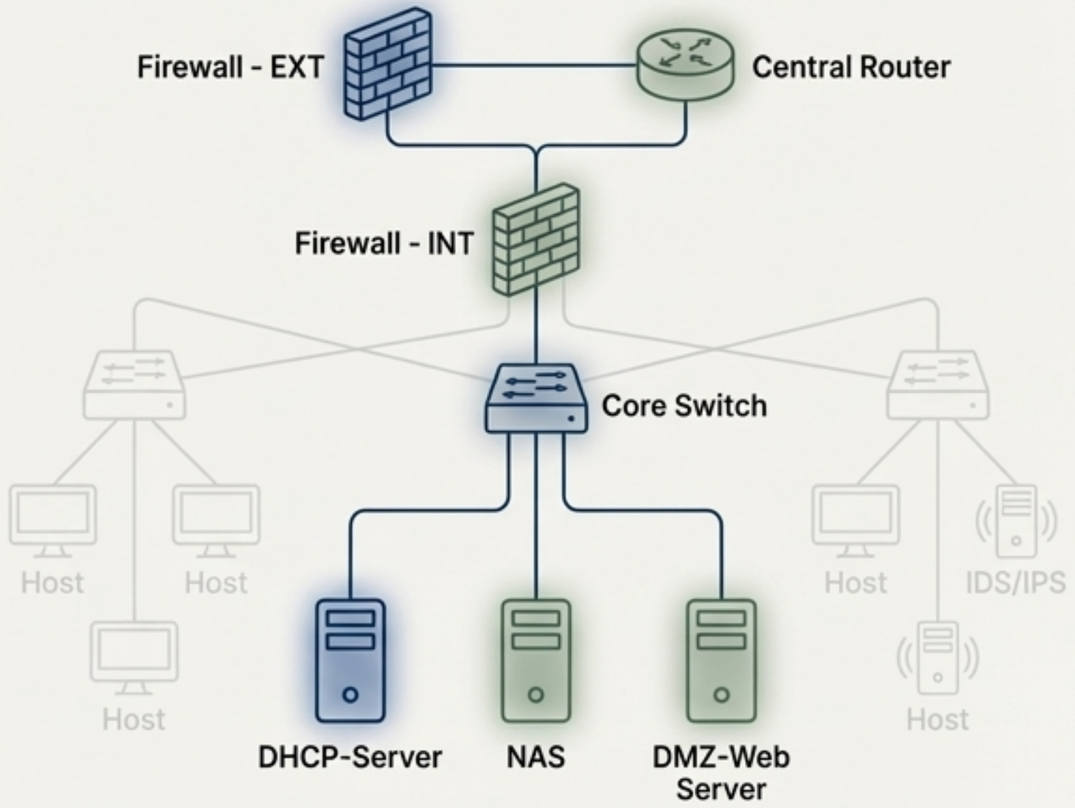
We selected the 'Tier 2: Business Standard" (Aruba/Fortinet) to provide the necessary throughput and features for a modern security strategy, avoiding underpowered SMB gear and oversized Enterprise costs.

Networking Core (Aruba/Fortinet): €20,800

- Supports the hierarchical model (Core + 6 Access Switches).
- Enables a dual-firewall topology (Perimeter & Internal).
- Provides the necessary throughput for real-time traffic analysis by 3 IDS/IPS systems.

Server Farm (Dell PowerEdge/QNAP): €10,200

- **DHCP Server:** Centralized IP management across all floor VLANs.
- **NAS Storage:** Secure, isolated file server for sensitive corporate data.
- **DMZ Host:** Dedicated, hardened server for public services, ensuring internal network is not exposed.



A Rationalized Fleet for a Modern Workforce (€172,500)

A ‘one-size-fits-all’ approach is inefficient. We segmented the 120 workstations based on real-world departmental needs to maximize value and productivity.

TIER 2: Mid-Range (75 Users)

Target: Consultants, PMs, Sales
Specs: i7, 32GB RAM, 1TB SSD, QHD Monitor
Rationale: For intensive multitasking, CRM, and analytics.

Total Cost: €97,500

TIER 3: High-End (25 Users)

Target: Developers, DevOps, Data Scientists
Specs: i9/Xeon, 64GB RAM, Dedicated GPU, Dual 4K Monitors
Rationale: Essential for virtualization, coding, and rendering workloads.

Total Cost: €60,000

TIER 1: Low-End (20 Users)

Target: Administration, HR, Back Office
Specs: i5, 16GB RAM, 512GB SSD, FHD Monitor
Rationale: Cost–effective solution for Office, ERP, and web–based tasks.

Total Cost: €15,000

More Than Installation: The Value of High-End Engineering (€14,000)

The 22-day project timeline is driven by complex configuration and security hardening, not just racking and stacking hardware.

1. Engineering & Design

Site survey, L2/L3 logical design, VLAN and IP addressing plan for 6 floors.

(3 days - €1,800)

→

2. Network & Security Setup

Critical Phase. Physical install, core routing, and granular configuration of firewall ACLs and the 3 IDS/IPS systems.

(5 days - €3,200)

→

3. Server Farm Configuration

DHCP scope setup, NAS RAID/ACL configuration, and OS hardening for the exposed DMZ host.

(4 days - €2,500)

→

4. Mass Client Deployment

Logistics for 120 workstations across 6 floors, including imaging, domain join, and cable management.

(8 days - €5,000)

→

5. Testing & Handover

Network stress testing, DMZ isolation verification, and creation of 'As-Built' documentation.

(2 days - €1,500)

Enforcing Zero Trust: A Granular Look at Firewall Policy

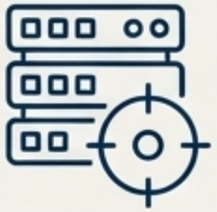
The firewall operates on the Principle of Least Privilege. We move beyond a simple 'allow/deny' to a stateful policy that isolates roles and contains threats.

Top-Down Execution

Rule	From	To	Security Justification
Rule 2: Admin Access (PASS) ✓	192.168.50.151 (Admin PC)	192.168.51.10 (DMZ Server) on Port 22 (SSH)	Restricts server management to a single, authorized host, preventing unauthorized access from other internal devices.
Rule 3: Corporate Services (PASS) ✓	LAN Subnet	DMZ Server on Port 80 (HTTP)	Allows employees to access the web service while implicitly blocking access to other potentially vulnerable ports on the server.
Rule 4: Isolate DMZ (REJECT) ✗	LAN Subnet	DMZ Subnet (Any Port)	**The cornerstone of internal security.** Prevents lateral movement from a compromised LAN device attempting to scan or attack the DMZ, effectively containing threats.
Rule 5: Internet Access (PASS) ✓	LAN Subnet	ANY	Standard rule allowing general internet access for business operations.

Beyond Off-the-Shelf: Verifying Security with a Custom Toolkit

Project guidelines required a deep-dive network audit but explicitly forbade the use of standard automated tools like Nmap. To meet this requirement, we developed a proprietary suite of Python-based tools for network reconnaissance and validation.



Attack Surface Mapping

A custom Port Scanner to identify open, closed, and filtered services without relying on third-party software.

Low-Level Traffic Analysis

A bespoke Packet Sniffer to capture and decode raw network data for forensic investigation.

Web Application Auditing

An automated HTTP Verb Checker to probe web server configurations for security weaknesses.

This demonstrates our ability to not only implement but also rigorously validate the security of the infrastructure we build.

Tool Deep Dive 1: The Custom Port Scanner

The Logic

- **Requirement:** Map the network's attack surface without using Nmap.
- **Our Solution:** `portscnRange.py`, a Python tool using low-level socket connections.
- **Technical Advantage:** Utilizes `socket.connect_ex()` to analyze OS return codes, providing a more granular diagnosis than a simple connection test.
  - `Status 0`: Port is **OPEN**.
  - `Status 111` (ECONNREFUSED): Port is definitively **CLOSED**.
  - `Status 110/11` (Timeout): Port is **FILTERED** (e.g., by a firewall), indicating a dropped packet.

Proof of Concept: Scanning the DMZ Web Server

Terminal Input

```
IP to scan: 192.168.50.101
Ports range (Es. 20-100): 10-100
```

Terminal Output

```
Port 21: OPEN
Port 22: OPEN
Port 23: OPEN
Port 25: OPEN
Port 53: OPEN
Port 80: OPEN
```

Log File Snippet

```
[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 24 -> CLOSED
...
Open ports: [21, 22, 23, 25, 53, 80]
```

Tool Deep Dive 2: The Raw Packet Sniffer

The Purpose

- **Objective:** Capture and analyze raw network packets directly from the network interface for deep traffic inspection.
- **Core Functionality:**
  - Binds to the network card at a low level (`socket.AF_PACKET`) to intercept all traffic.
  - Decodes the Ethernet and IPv4 headers using the `struct library to interpret the binary data.
  - Filters traffic to isolate conversations involving a specific target IP.

Captured Traffic Analysis

```
$ sudo python SocketReteperRelazione.py
[+] Filtering packets for IP: 192.168.1.101

Packet 1
  Source IP     : 192.168.1.101
  Destination IP: 20.42.65.93
  Length        : 66 bytes

Packet 2
  Source IP     : 20.42.65.93
  Destination IP: 192.168.1.101
  Length        : 66 bytes
```

Packet 1 (Outbound): Shows a small packet originating from our network, likely a TCP control packet or DNS query.

Packet 2 (Inbound): Shows the corresponding response from the external server, confirming a successful two-way communication.

Tool Deep Dive 3: The HTTP Verb Auditor

The Goal

- **Objective:** Automatically discover which HTTP methods (GET, POST, PUT, DELETE, etc.) a web server allows on a specific URL.
- **Methodology:**
  1. Sends an `OPTIONS` request for initial reconnaissance, which often reveals the `Allow` header.
  2. Systematically cycles through a list of common methods (`GET`, `POST`, `PUT`, `DELETE`).
  3. Analyzes the HTTP status code of the response. A `405 (Method Not Allowed)` response indicates the method is disabled; other codes (like `200 OK`) suggest it is handled.

Auditing a Web Resource

```
Target: http://192.168.1.102/phpMyAdmin/.../logo_right.png
------------------------------------------------------------------
OPTIONS -> 200 Allow=GET, HEAD, POST, OPTIONS, TRACE Server=Apache...
GET     -> 200 Server=Apache...
POST    -> 200 Server=Apache...
PUT     -> 405 Allow=GET, HEAD, POST, OPTIONS, TRACE Server=Apache...
DELETE  -> 405 Allow=GET, HEAD, POST, OPTIONS, TRACE Server=Apache...

Likely handled/enabled methods: OPTIONS, GET, POST
```

Security Insight

The audit confirms that potentially dangerous methods like `PUT` and `DELETE` are correctly disabled on this resource, preventing unauthorized content modification or deletion.

A Resilient, Validated, and Performance-Tuned Infrastructure

The €226,000 investment delivers a comprehensive, ‘Chiavi in Mano’ (Turnkey) solution that secures Theta Company’s digital operations and empowers its workforce.

- **Functional Needs Met:** Supports 120 users across 6 floors with segmented, high-performance VLANs.
- **Resilient Security Implemented:** A multi-layered “Defense in Depth” strategy protects critical assets like the company NAS and isolates public services in a DMZ.
- **Expertise Verified:** The architecture has been rigorously tested and validated using proprietary tools, demonstrating a level of care and technical skill beyond standard implementation.