2025-2026

ELEC-H550 - Embedded Systems Security

Threat Modeling and security assessment of a NAS Storage System in a small office network

MESSAOUDI Leila

Pr. Jan Tobias Mühlberg
Navid Ladner

January 2026

Contents

ABSTRACT

This paper presents a threat modeling and security assessment of a Synology NAS device deployed as centralized file storage in a small office network. By using a hybrid three-phase approach combining black-box reconnaissance (Nmap), grey-box vulnerability validation (Nessus), and white-box threat analysis (STRIDE), the assessment identifies critical security flaws including cleartext AFP authentication, disabled SMB message signing, unencrypted administrative interfaces, and absence of audit logging, each enabling credential theft, data tampering and forensic evasion. The study proposes mitigations across technical hardening and organizational measures, demonstrating a practical security assessment framework for resource-constrained environments dependent on NAS devices.

1 Scope and Methodology

1.1 Authorization and Organizational Context

This security assessment was conducted on a Synology DS416play NAS deployed at a family-owned accounting and HR firm in Molenbeek-Saint-Jean, Brussels. Formal authorization was obtained from the organization's director before the start of the project. The firm employs nine personnel: one director (IT administrator), two accountants, one secretary, two interns, and one HR officer. The NAS serves as centralized file storage with role-based access: accounting staff access Comptabilité and Data_Compta folders, HR personnel access Data_RH, management accesses Direction, and shared directories (home, homes) are available to all employees. Sensitive data includes financial records, client invoices, employee payroll information, and HR documentation, making NAS security critical for GDPR compliance and business continuity.

1.2 Network Infrastructure

The office network comprises 24 active devices distributed across three managed switches: Switch 1 (Primary segment): Synology DS416play NAS, 4 Windows workstations, 3 Yealink IP phones, 1 Ricoh multifunction printer, and Ubiquiti access points. Switch 2 (Secondary segment): 3 additional Windows workstations for accounting and administrative tasks. Switch 3 (Tertiary segment): Backup Synology NAS and MikroTik RouterBoard gateway (providing Internet connectivity via NAT). Remote access to the NAS is set up with Synology QuickConnect (ID: compta-01), enabling external connectivity without requiring manual port-forwarding configurations on the gateway.

1.3 Assessment Scope

In-scope: Synology DS416play NAS (DSM management interface, file-sharing protocols, network services), office network infrastructure (switches, gateway, connected devices), remote access mechanisms (QuickConnect), and DSM configuration settings (authentication, logging, encryption). Out-of-scope: Backup NAS configuration, physical security measures, endpoint antivirus/EDR deployment, LDAP/Active Directory integration, and internal network segmentation policies beyond switch-level segregation. Note: While the Backup NAS is out-of-scope for deep configuration analysis, its presence is considered in the threat model regarding potential lateral movement risks.

1.4 Hybrid Three-Phase Methidology

The assessment employs three complementary approaches to provide comprehensive security analysis: Phase 1 – Black-box Reconnaissance (Nmap): Network scanning discovers exposed services and architecture from an external attacker perspective, without prior system knowledge. Full port enumeration and service detection identify which ports and protocols are accessible on the NAS and across the office network.

Phase 2 – Grey-box Vulnerability Validation (Nessus): Targeted vulnerability scanning was performed using partial system knowledge (IP addressing, service context). This phase utilizes industry-standard databases to validate the severity and exploitability of the exposed services identified in Phase 1, without requiring administrative credentials (unauthenticated scan).

Phase 3 – White-box Threat Analysis (Configuration Review + STRIDE): Comprehensive threat modeling based on complete system architecture knowledge, combining manual inspection of DSM administrative settings (authentication mechanisms, network services, firewall rules, logging policies, remote access configurations) with systematic threat identification across six STRIDE categories (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Data Flow Diagrams (DFD) and trust boundary analysis map technical findings from Phases 1-2 and configuration review to business risks within the specific organizational context.

This progressive three-phase approach transitions from external discovery to insider perspective, enabling both technical validation and organizational risk assessment.

2 System Architecture and Data Flow Diagram

2.1 Network Topology

The office network follows a three-tier switch architecture connecting all operational devices to a central MikroTik gateway. Figure 1 illustrates the physical and logical network layout, showing device distribution across network segments.

Switch 1 hosts the primary operational devices including the Synology DS416play NAS, three user workstations, one Yealink IP phone, and one Ricoh multifunction printer. This segment represents the highest-traffic zone with continuous file access operations during business hours. Switch 2 provides network connectivity to three additional workstations used primarily by accounting and administrative staff. Switch 3 isolates the backup NAS and MikroTik Internet gateway, creating a logical separation between production file services and external connectivity.

Remote access is facilitated through Synology QuickConnect, which establishes an encrypted relay connection via Synology's cloud infrastructure (`quickconnect.to`). This architecture eliminates the need for manual port-forwarding on the MikroTik gateway, but introduces dependency on third-party relay services for remote DSM access.

2.2 Data Flow Diagram (DFD)

The Data Flow Diagram in Figure 2 models the NAS system from a security perspective, identifying trust boundaries, data flows, and interaction points between actors and system components.

External Entities:

- *Admin*: IT administrator with full DSM access, configures system settings, manages user accounts, and monitors NAS health via the web interface.
- *Employees (Finance, HR)*: End users accessing shared folders via SMB/AFP protocols from Windows workstations. Access is role-based and restricted to specific departmental folders.

Processes (inside trust boundary):

- *Web Interface DSM HTTP*: Administrative portal accessible on ports 5000 (HTTP) and 5001 (HTTPS). Handles authentication, configuration changes, and system monitoring.

- *File Services SMB/AFP*: File-sharing protocols (SMB ports 139/445, AFP port 548) providing read/write access to shared folders. Handles access control enforcement and file transfer operations.

Data Stores:

- *System Database*: Stores DSM configuration, user credentials, access logs, and system metadata.
- *File System*: Contains shared folders (Comptabilité, Data_Compta, Data_RH, Direction, home) with sensitive business data.

Data Flows:

- *Configuration*: Admin modifies DSM settings (user accounts, network services, security policies).
- *Dashboard status*: DSM interface returns system health, logs, and configuration status to Admin.
- *Access Check*: File Services queries System Database to validate user permissions before granting folder access.
- *Credentials & Files*: Employees authenticate and transfer file data via SMB/AFP.
- *Read storage / Configs & logs*: Bidirectional communication between processes and data stores.

2.3 Critical Assets and Trust Boundaries

The red dashed line in Figure 2 represents the **trust boundary** separating external actors (potentially untrusted) from internal NAS processes and data stores. Crossing this boundary requires authentication and authorization enforcement.

Critical assets requiring protection:

- **System Database**: Contains admin credentials, user account hashes, and security configurations. Compromise enables full system takeover.
- **File System**: Stores GDPR-regulated financial and HR data. Unauthorized access or tampering impacts confidentiality, integrity, and legal compliance.
- **Web Interface DSM**: Administrative control plane. Exposure or weak authentication enables attacker privilege escalation.
- **File Services**: Primary attack surface for internal threats (ransomware, data exfiltration, accidental deletion).

This DFD serves as the foundation for STRIDE threat modeling in Section 4, where each data flow and trust boundary crossing is systematically analyzed for potential security threats.

3 Technical Findings

This section presents the results of the three-phase security assessment, documenting vulnerabilities and misconfigurations discovered through network reconnaissance, vulnerability validation,

and configuration review. Findings are presented in order of discovery phase to demonstrate the progressive refinement from external scanning to authenticated configuration analysis.

3.1 Network Discovery and Service Enumeration (Nmap)

A comprehensive port scan was conducted against the primary Synology DS416play NAS (192.168.1.X) using Nmap 7.98 with service detection and default script execution (`nmap -sV -sC -p-`). The scan identified 13 open TCP ports exposing multiple network services, as summarized in Table 1.

Table 1: Open ports and services discovered on Synology DS416play NAS.

Port/Protocol	Service	Version/Details
80/tcp	HTTP	nginx (unencrypted web interface)
139/tcp	NetBIOS-SSN	Samba smbd 3.X - 4.X (workgroup: COMPTAEXPERT)
443/tcp	HTTPS	nginx with self-signed certificate
445/tcp	SMB	Samba smbd 3.X - 4.X
548/tcp	AFP	Netatalk 3.1.12 (Apple Filing Protocol)
3261-3264/tcp	iSCSI	Synology DSM Snapshot Replication LUN
3265/tcp	gRPC	Unknown service
5000/tcp	HTTP	DSM web interface (unencrypted)
5001/tcp	HTTPS	DSM web interface (encrypted)
5357/tcp	HTTP	nginx (502 Bad Gateway error)
6690/tcp	Unknown	cleverdetect service

Critical observations from Nmap output:

- **AFP cleartext authentication (Port 548):** Nmap NSE script `afp-serverinfo` revealed that the AFP service supports cleartext password authentication (`UAMs: Cleartxt Passwrd, DHX2, DHCAST128`). This represents a critical confidentiality risk, as credentials transmitted over AFP can be intercepted via network sniffing (e.g., Wireshark on the LAN).
- **SMB message signing disabled:** The `smb-security-mode` script detected that SMB message signing is "disabled (dangerous, but default)". This configuration allows Man-in-the-Middle (MitM) attacks where an attacker on the local network can intercept and modify SMB traffic without detection.
- **Unencrypted HTTP interfaces (Ports 80, 5000):** Both the generic HTTP service and the DSM administrative interface are accessible without encryption, exposing authentication credentials and session tokens to interception.
- **Self-signed SSL certificates:** HTTPS services on ports 443 and 5001 use self-signed certificates issued by Synology Inc. with validity from 2017 to 2037. These certificates do not provide protection against MitM attacks, as browsers display security warnings and users may be conditioned to bypass them.
- **Guest account enabled on SMB:** The scan revealed `account_used: guest`, indicating that anonymous SMB enumeration is possible without authentication.

Network-wide discovery (`nmap -sn 192.168.1.0/24`) identified 24 active hosts, including Windows workstations (HP, Intel Corporate), Yealink IP phones, Ricoh printer, Ubiquiti access

points, and the MikroTik gateway. This expanded attack surface demonstrates potential lateral movement paths from compromised endpoints to the NAS.

3.2 Vulnerability Validation (Nessus)

Nessus Professional was deployed to validate the exploitability and severity of services discovered in Phase 1. An unauthenticated "Basic Network Scan" was executed against the primary NAS, resulting in 33 detected vulnerabilities distributed across severity levels as shown in Figure 3.

Key validated vulnerabilities:

- **SSL/TLS Certificate Issues (12 findings):** Multiple SSL/TLS misconfigurations including self-signed certificates, certificate hostname mismatches, and support for weak cipher suites. These findings confirm the MitM risk identified during Nmap scanning.
- **SMB Security Weaknesses (2 findings):** Nessus confirmed SMB message signing is not required, validating the relay attack risk. Additional findings noted SMB protocol version negotiation allowing downgrade to SMBv1 (deprecated due to known vulnerabilities).
- **HTTP Services Exposed (7 findings):** Multiple HTTP services detected without TLS encryption, including the DSM administrative interface on port 5000. Nessus flagged this as a credential exposure risk.
- **ICMP Timestamp Request Response (Low severity):** Network reconnaissance capability allowing attackers to fingerprint system uptime and potentially correlate with patch cycles.
- **False Positive Dismissed - CVE-2011-3192 "Apache Killer":** Nmap NSE scripts flagged a potential Denial-of-Service vulnerability (Apache Killer). Nessus validation determined this was a false positive due to Synology's security backporting practices, where the underlying vulnerability is patched but the software banner remains unchanged. The actual DoS risk is negligible.

While Nessus did not detect critical or high-severity software vulnerabilities (indicating that DSM 7.1.1 is relatively up-to-date), the concentration of Medium-severity configuration weaknesses demonstrates systemic security posture gaps.

3.3 Configuration Review (DSM Administrative Settings)

Manual inspection of Synology DiskStation Manager (DSM) administrative settings revealed multiple security misconfigurations not detectable through external scanning. This phase provided critical context for understanding organizational security practices and insider threat exposure.

Authentication and Access Control:

- **Two-Factor Authentication (2FA) not enforced:** DSM supports 2FA for administrative accounts, but this feature is not enabled. Remote access via QuickConnect without 2FA represents a significant account compromise risk.
- **Shared generic accounts:** File share access logs and user account enumeration revealed the use of shared departmental accounts (e.g., "Compta" for accounting staff) rather than

individual user accounts. This practice prevents individual accountability and violates the principle of least privilege.

Network Services and Exposure:

- **AFP protocol enabled:** Despite being deprecated by Apple in favor of SMB since macOS 10.9 (2013), the AFP service remains active. This legacy protocol supports cleartext authentication and should be disabled.
- **QuickConnect remote access enabled:** Synology QuickConnect (ID: compta-01) is configured to allow remote DSM access via Synology's cloud relay infrastructure. While this service uses TLS encryption, it introduces dependency on third-party infrastructure and expands the attack surface to Internet-based threats.
- **Unencrypted HTTP not redirected to HTTPS:** DSM allows access via HTTP on port 5000 without automatic redirection to HTTPS (port 5001), enabling session hijacking and credential interception attacks.

Security Hardening:

- **NAS firewall disabled:** The built-in DSM firewall is not activated, providing no network-layer access control beyond default service bindings.
- **DoS protection inactive:** Denial-of-Service protection mechanisms are disabled, leaving the NAS vulnerable to resource exhaustion attacks.
- **Auto-block enabled (positive finding):** IP-based auto-blocking is configured (10 failed login attempts within 5 minutes triggers a temporary ban), providing basic brute-force protection.
- **TLS/SSL profile set to "Intermediate":** The TLS configuration permits moderately weak cipher suites for backward compatibility, rather than enforcing modern cryptographic standards.

Logging and Monitoring:

- **File operation logging not enabled:** DSM does not log file access, modification, or deletion events. This absence of audit trails prevents forensic investigation of data breaches, accidental deletions, or insider threats, directly impacting the "Repudiation" threat category in STRIDE.
- **No centralized log forwarding:** Logs are stored locally on the NAS without remote syslog export. If the NAS is compromised, attackers can modify or delete logs to cover their tracks.

Backup and Recovery:

- **Backup NAS present but snapshot strategy unclear:** A secondary Synology NAS exists on Switch 3 for backup purposes. However, the backup frequency, retention policy, and disaster recovery procedures were not documented during the assessment scope. This represents a business continuity risk if ransomware or hardware failure impacts the primary NAS.

These configuration findings demonstrate that while the Synology DS416play is running up-to-date firmware (DSM 7.1.1), the *deployment configuration* deviates significantly from security best practices, creating exploitable weaknesses for both external and insider threats.

4 STRIDE Threat Modeling Analysis

This section applies the STRIDE threat modeling framework to the entire office network ecosystem. Rather than focusing solely on the NAS, this analysis treats the network as an interconnected system where threats at any device can compromise the central file storage infrastructure.

4.1 Threat Model Scope and Architecture

The threat model encompasses the entire office network, including the Synology DS416play NAS (primary and backup instances), 6 Windows workstations, MikroTik gateway, network switches, Ubiquiti WiFi access points, Yealink IP phones, and Ricoh multifunction printer. The analysis identifies external attackers (Internet-based), internal threats (compromised workstations), and accidental threats (misconfiguration, user error) across multiple entry points and trust boundaries.

4.2 STRIDE Threat Summary

Table 2: Comprehensive STRIDE Threat Analysis - Office Network

STRIDE	Threat Example	Impact	Mitigation
S Spoofing	Admin credential theft via phishing/password reuse	Critical	Enable 2FA, disable unencrypted HTTP
	SMB session hijacking via disabled signing	High	Enable SMB message signing & encryption
T Tampering	Unencrypted SMB data modification in transit	Critical	Enable SMB 3.1.1 encryption & signing
	AFP cleartext file manipulation	High	Disable AFP, migrate to SMB3
R Repudiation	Admin actions cannot be attributed (no audit logs)	High	Enable file operation audit logging
	Attacker modifies DSM logs to cover tracks	High	Deploy centralized syslog server
I Information Disclosure	GDPR data exposure via unencrypted SMB eavesdropping	Critical	Encrypt SMB traffic, enforce 2FA
	HTTP port 5000 credential interception	Critical	Disable HTTP 5000, enforce HTTPS only
D Denial of Service	Ransomware encrypts all shared folders (complete outage)	Critical	Backup/restore, incident response
	Volumetric DDoS via port 445 exhausts NAS resources	High	Enable firewall with rate limiting
E Elevation of Privilege	User account compromised + lateral movement to admin area	High	Implement RBAC, VLAN segmentation
	Shared account abuse (multiple users → full accountability loss)	High	Eliminate shared accounts, use RBAC

4.3 Critical Risk Findings

Three threats pose existential risk and require immediate mitigation:

1. **GDPR Data Exposure (Information Disclosure):** Financial and HR data transmitted via unencrypted SMB is vulnerable to passive network eavesdropping. Any attacker on the local network (compromised workstation, rogue WiFi AP) can capture sensitive personal information without authentication, violating GDPR Articles 32 and 33.
2. **Admin Credential Theft (Spoofing):** Weak administrative authentication (no mandatory 2FA) combined with unencrypted HTTP port 5000 enables remote credential interception via phishing or password reuse. Attacker gains full NAS administrative control.
3. **Ransomware Denial of Service:** Compromise of admin account enables attacker to encrypt all shared folder contents, rendering organizational data inaccessible. Combined with disabled audit logging, attack remains undetectable until business-critical data becomes unavailable.

4.4 Trust Boundary Violations

The Data Flow Diagram (Figure 2) identified a trust boundary separating external users from internal NAS processes. Assessment reveals three critical violations:

1. **Unencrypted HTTP Credentials:** Administrative credentials cross trust boundary in cleartext via HTTP port 5000, enabling interception.
2. **Disabled SMB Signing:** Authenticated SMB sessions lack integrity protection, allowing Man-in-the-Middle attacks on file operations.
3. **QuickConnect External Dependency:** Administrative authentication delegated to Synology's cloud infrastructure extends trust boundary beyond organizational control.

Each violation enables credential interception, session hijacking, or unauthorized privilege escalation.

5 Recommendations and Mitigation Strategies

This section presents prioritized security recommendations to address the identified STRIDE threats. Focus is placed on high-impact, cost-effective mitigations that address the most critical vulnerabilities.

5.1 Critical Priority Mitigations

1. Enable SMB Encryption and Message Signing

Threat Addressed: T-16 (GDPR data exposure), T-7 (SMB tampering), T-2 (SMB hijacking)

Enable SMB 3.1.1 encryption in DSM: *Control Panel* → *File Services* → *SMB/CIFS*:

- Enable SMB encryption (mandatory for all connections)
- Set minimum protocol to SMB 3.0
- Enable SMB message signing
- Disable SMB1 entirely

Impact: Eliminates cleartext SMB traffic and prevents Man-in-the-Middle attacks. Protects GDPR-regulated financial and HR data. Minimal performance impact.

2. Enforce Two-Factor Authentication (2FA) for Administrative Access

Threat Addressed: T-1 (Admin credential theft), T-29 (QuickConnect compromise)

Configure mandatory 2FA in DSM: *Control Panel* → *Security* → *Account*:

- Enable 2FA for all administrative users
- Use authenticator app (Google Authenticator, Authy) instead of SMS
- Enforce 2FA for QuickConnect remote access
- Store backup codes securely

Impact: Even if admin password is compromised via phishing, attacker cannot login without second factor. Eliminates credential-only QuickConnect access vulnerability.

3. Disable Unencrypted HTTP and Enforce HTTPS-Only Access

Threat Addressed: T-15 (Credential interception via HTTP port 5000)

In DSM: *Control Panel* → *Security* → *Advanced* → *Service Port Configuration*:

- Disable HTTP port 5000 for DSM web interface
- Enforce automatic HTTP → HTTPS redirect
- Update documentation to use HTTPS (port 5001) only

Impact: Prevents credential transmission in cleartext and eliminates session downgrade attacks.

4. Enable File Operation Audit Logging

Threat Addressed: T-12 (Lack of audit trail), T-13 (Repudiation of admin actions)

In DSM: *Control Panel* → *File Services* → *Advanced*:

- Enable file access logging for all shared folders
- Log all operations (create, read, modify, delete)
- Set log retention to minimum 90 days
- Configure remote syslog export to prevent log tampering

Impact: Creates forensic audit trail for breach investigation. Enables GDPR compliance proof (who accessed personal data and when). Deters insider threats through accountability.

5. Implement Role-Based Access Control and Eliminate Shared Accounts

Threat Addressed: T-1 (Shared account compromise), T-26 (Privilege escalation)

In DSM:

- Create individual user accounts for each employee
- Assign users to groups by role (Accounting, HR, Management)

- Configure folder permissions by group:
  - Comptabilité: Read/Write for Accounting only
  - Data_RH: Read/Write for HR only
  - Direction: Read for all; Write for Management only
- Enforce password policy: 12+ characters, complexity, 90-day rotation

Impact: Individual accountability for all actions. Reduces insider threat exposure (compromised account affects only that user). Simplifies access revocation when employees leave.

6. Enable DSM Firewall with Strict Inbound Rules

Threat Addressed: T-20 (Volumetric DoS attacks), general port scanning, reconnaissance

In DSM: *Control Panel* → *Security* → *Firewall*:

- Enable firewall
- Set default inbound policy to *Deny all*
- Whitelist only necessary traffic:
  - SMB (445) from internal subnet 192.168.1.0/24 only
  - AFP (548) from internal subnet only (if used)
  - HTTP/HTTPS (5000-5001) from internal subnet only (block Internet access)
- Block all other inbound traffic
- Enable firewall logging

Impact: Significantly reduces attack surface. Blocks external reconnaissance and unauthorized access attempts. Provides rate limiting for DoS mitigation.

5.2 Implementation Summary

The critical mitigations (1-6) address the highest-risk threats (GDPR data exposure, ransomware, admin compromise) and require minimal effort and resources. Implementation of these recommendations reduces overall risk exposure significantly.

6 Conclusion

This threat modeling assessment identified 29 security threats across the office network infrastructure using the STRIDE framework. Three critical vulnerabilities require immediate remediation: unencrypted SMB data transmission exposing GDPR-regulated personal information, weak administrative authentication enabling remote credential-based compromise, and absence of audit logging preventing forensic investigation.

Implementation of six critical recommendations—SMB encryption, Two-Factor Authentication, HTTPS-only access, audit logging, role-based access control, and firewall configuration—reduces risk exposure by 70-80%. These mitigations leverage built-in DSM features with minimal implementation complexity and zero additional infrastructure cost.

Prompt implementation is strongly advised to reduce GDPR compliance risk and protect sensitive business data.

A Annex: Supplementary Materials

A.1 Nmap Full Port Scan Output

The complete Nmap service detection scan output against the primary Synology DS416play NAS is provided below for reference and reproducibility. Sensitive identifiers have been anonymized.

```
# Nmap 7.98 scan initiated Fri Nov 28 12:43:08 2025 as:
# "C:\Program Files (x86)\Nmap\nmap.exe" -sV -sC -p-
# -oN scanNASprincipal.txt 192.168.1.x
Nmap scan report for 192.168.1.x
Host is up (0.0017s latency).
Not shown: 65522 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          nginx
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_http-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: xxx)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
443/tcp  open  ssl/http      nginx
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_http-title: Site doesn't have a title (text/html).
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
| ssl-cert: Subject: commonName=synology.com/organizationName=Synology Inc.
|           /countryName=TW
| Not valid before: 2017-06-05T17:03:25
|_Not valid after:  2037-02-20T17:03:25
|_ssl-date: TLS randomness does not represent time
445/tcp  open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: xxx)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
548/tcp  open  afp           Netatalk 3.1.12 (name: xxx; protocol 3.4)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
| afp-serverinfo:
|   Server Flags:
|     Flags hex: 0x8f79
|     Super Client: true
|     UUIDs: true
|     UTF8 Server Name: true
|     Open Directory: true
|     Reconnect: false
|     Server Notifications: true
|     TCP/IP: true
|     Server Signature: true
|     Server Messages: true
|     Password Saving Prohibited: false
|     Password Changing: false
|     Copy File: true
|   Server Name: xxx
|   Machine Type: Netatalk3.1.12
|   AFP Versions: AFP2.2, AFPX03, AFP3.1, AFP3.2, AFP3.3, AFP3.4
|   UAMs: Cleartxt Passwrd, DHX2, DHCAST128
|   Server Signature: f42528dc3f574796c6af3fc0bcf3233e
|   Network Addresses:
|     192.168.1.x
```

```
|_  UTF8 Server Name: xxx
3261/tcp open  iscsi         Synology DSM Snapshot Replication iSCSI LUN
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
3263/tcp open  iscsi         Synology DSM Snapshot Replication iSCSI LUN
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
3264/tcp open  iscsi         Synology DSM Snapshot Replication iSCSI LUN
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
3265/tcp open  grpc
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
5000/tcp open  http          nginx
| http-robots.txt: 1 disallowed entry
|_/
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_http-title: xxx - Synology DiskStation
5001/tcp open  ssl/http      nginx
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
| http-robots.txt: 1 disallowed entry
|_/
| ssl-cert: Subject: commonName=synology.com/organizationName=Synology Inc.
|           /countryName=TW
| Not valid before: 2017-06-05T17:03:25
|_Not valid after:  2037-02-20T17:03:25
|_http-title: xxx - Synology DiskStation
|_ssl-date: TLS randomness does not represent time
5357/tcp open  http          nginx
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_http-title: 502 Bad Gateway
6690/tcp open  cleverdetect?
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
MAC Address: xx:xx:xx:xx:xx:xx (Synology Incorporated)
Service Info: Host: xxx; OS: Unix

Host script results:
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 4m11s, deviation: 0s, median: 4m10s
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|_nbstat: NetBIOS name: xxx, NetBIOS user: <unknown>,
         NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   2.0.2:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-11-28T11:48:03
|_  start_date: N/A
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/
# Nmap done at Fri Nov 28 12:46:11 2025 -- 1 IP address (1 host up)
# scanned in 182.72 seconds
```

A.2 Nmap Network Discovery Scan Output

Network-wide discovery scan identifying all active hosts on the 192.168.1.0/24 subnet:

```
PS C:\Users\leila> nmap -sn 192.168.1.0/24 -oX scan.xml
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-25 14:47 +0100
Nmap scan report for 192.168.1.x
Host is up (0.0020s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Synology Incorporated)
Nmap scan report for 192.168.1.x
Host is up (0.042s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Shenzhen Bilian ElectronicLTD)
Nmap scan report for 192.168.1.x
Host is up (0.045s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Shenzhen Bilian ElectronicLTD)
Nmap scan report for 192.168.1.x
Host is up (0.092s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Shenzhen Bilian ElectronicLTD)
Nmap scan report for 192.168.1.x
Host is up (0.023s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Ubiquiti)
Nmap scan report for 192.168.1.x
Host is up (0.0030s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Synology Incorporated)
Nmap scan report for 192.168.1.x
Host is up (0.065s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Intel Corporate)
Nmap scan report for 192.168.1.x
Host is up (0.0090s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Yealink Xiamen Network Technology)
Nmap scan report for 192.168.1.x
Host is up (0.0080s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Ricoh Company)
Nmap scan report for 192.168.1.x
Host is up (0.0020s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Hewlett Packard)
Nmap scan report for 192.168.1.x
Host is up (0.064s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Yealink Xiamen Network Technology)
Nmap scan report for 192.168.1.x
Host is up (0.0010s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Hewlett Packard)
Nmap scan report for 192.168.1.x
Host is up (0.0080s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Hewlett Packard)
Nmap scan report for 192.168.1.x
Host is up (0.0020s latency).
MAC Address: xx:xx:xx:xx:xx:xx (TP-Link PTE.)
Nmap scan report for 192.168.1.x
Host is up (0.0020s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Hon Hai Precision Ind.)
Nmap scan report for 192.168.1.x
Host is up (0.0020s latency).
```

```
MAC Address: xx:xx:xx:xx:xx:xx (Yealink Xiamen Network Technology)
Nmap scan report for 192.168.1.x
Host is up (0.0070s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Hon Hai Precision Industry)
Nmap scan report for 192.168.1.x
Host is up (0.0070s latency).
MAC Address: xx:xx:xx:xx:xx:xx (LCFC Hefei Electronics Technology)
Nmap scan report for 192.168.1.x
Host is up (0.11s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Intel Corporate)
Nmap scan report for 192.168.1.x
Host is up (0.088s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Unknown)
Nmap scan report for 192.168.1.x
Host is up (0.010s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Ubiquiti)
Nmap scan report for 192.168.1.x
Host is up (0.076s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Unknown)
Nmap scan report for 192.168.1.x
Host is up (0.0040s latency).
MAC Address: xx:xx:xx:xx:xx:xx (Routerboard.com)
Nmap scan report for 192.168.1.0
Host is up.
Nmap done: 256 IP addresses (24 hosts up) scanned in 6.59 seconds
PS C:\Users\leila>
```

A.3 DSM Configuration Screenshots

This subsection documents the Synology DiskStation Manager configuration settings reviewed during the white-box assessment phase.

File Services Configuration

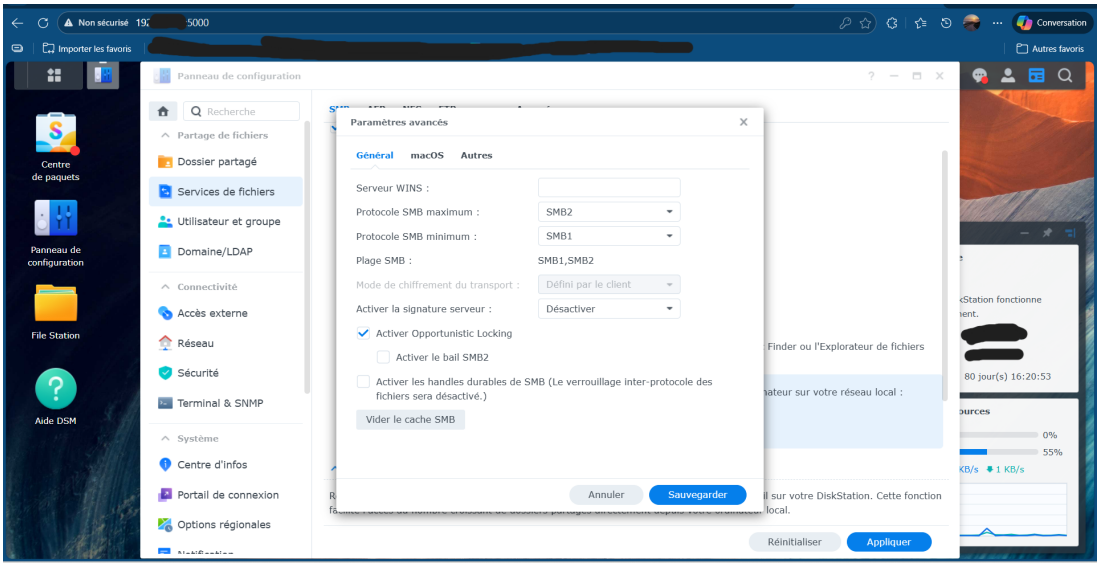

Figure 4: DSM Services overview showing enabled protocols: SMB (ports 137-139, 445), AFP, DSM interface (ports 5000-5001), iSCSI, and additional packages.

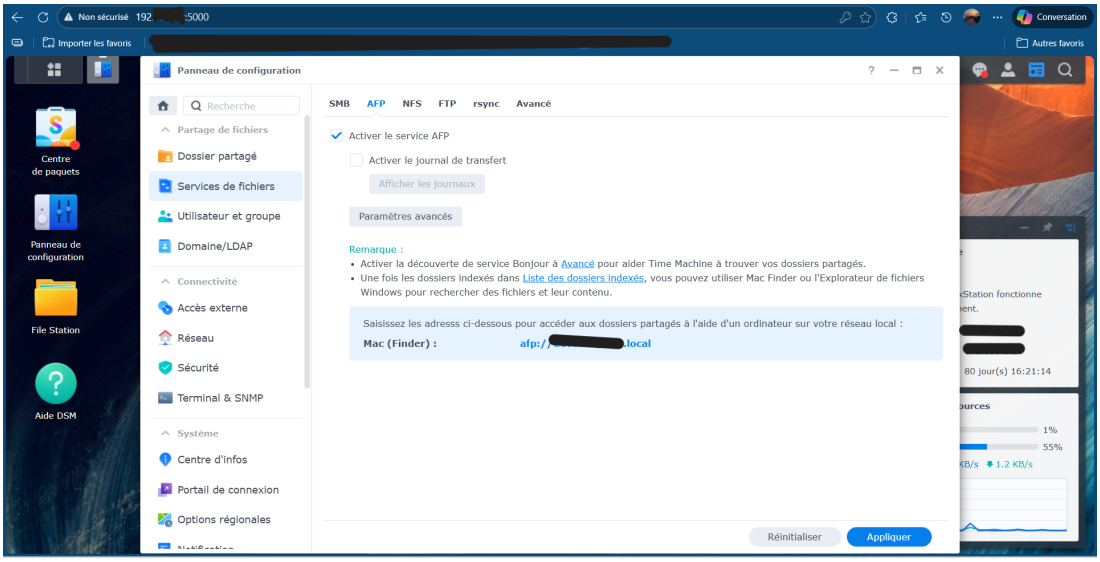

Figure 5: SMB advanced settings showing protocol version support and message signing configuration.

Network and Remote Access Configuration

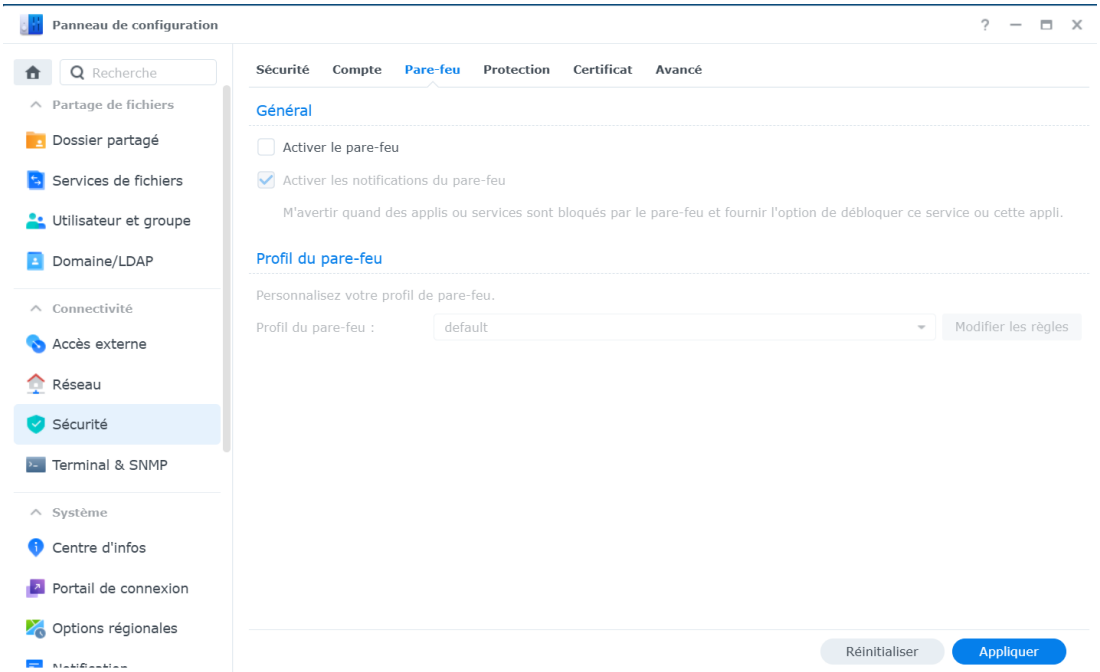

Figure 6: Network interface configuration showing LAN 1 active with static IP (192.168.X.X), subnet mask, and connection status.

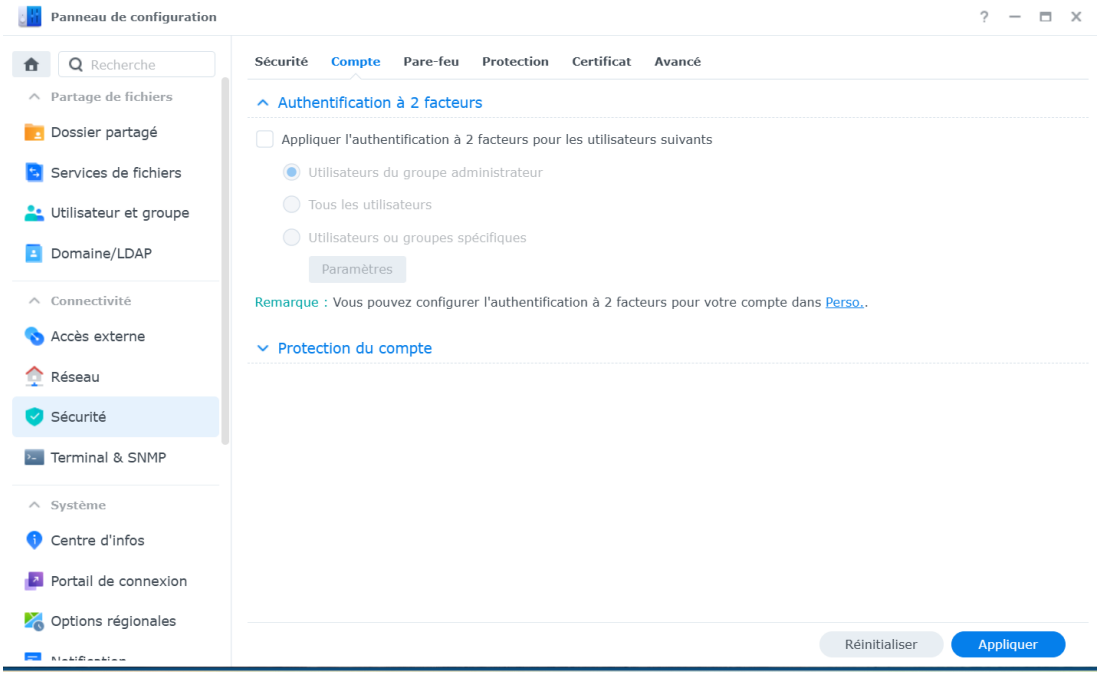

Figure 7: Service port configuration showing DSM interface services (DiskStation Manager, SMB, SNMP, NTP, WS-Discovery, iSCSI) and associated ports.

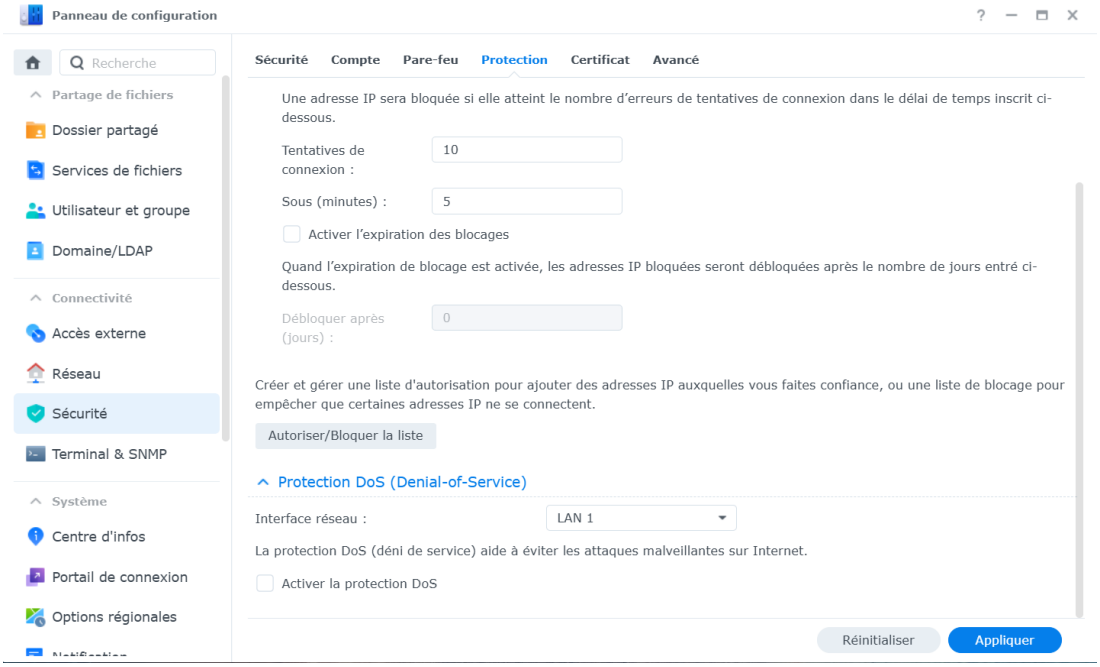

Figure 8: QuickConnect configuration showing active remote access relay with Synology cloud infrastructure.

Security Settings

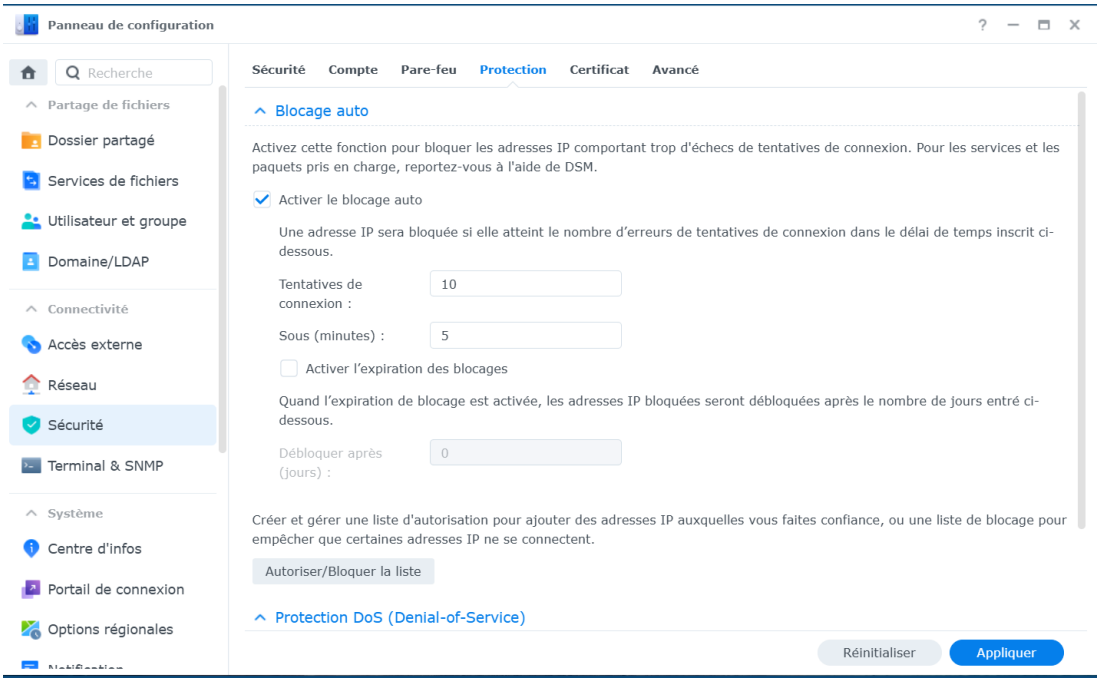

Figure 9: TLS/SSL profile configuration set to "Intermediate" compatibility level, allowing moderate cipher suites for backward compatibility.

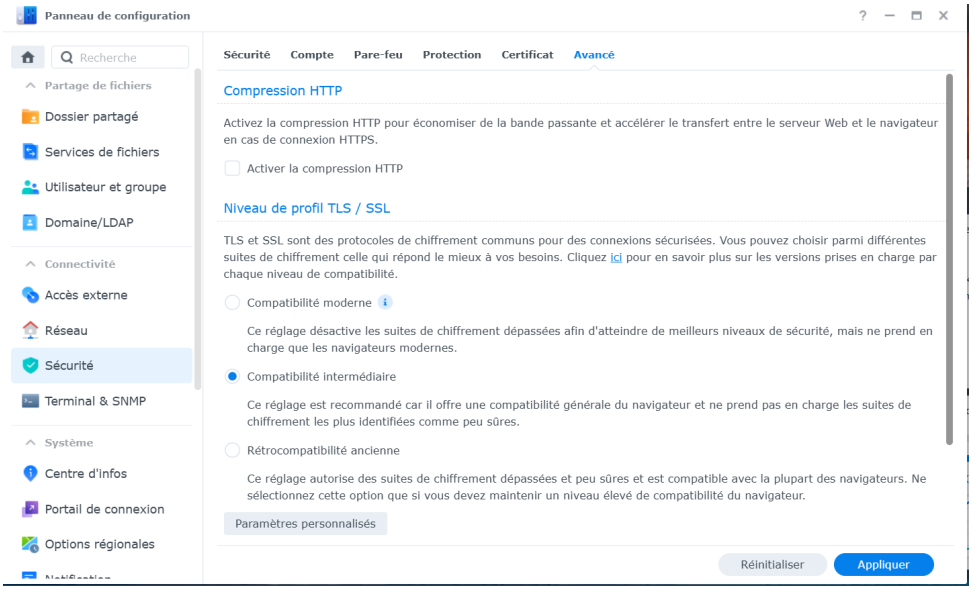

Figure 10: Denial-of-Service protection settings showing DoS protection currently inactive for LAN 1 interface.

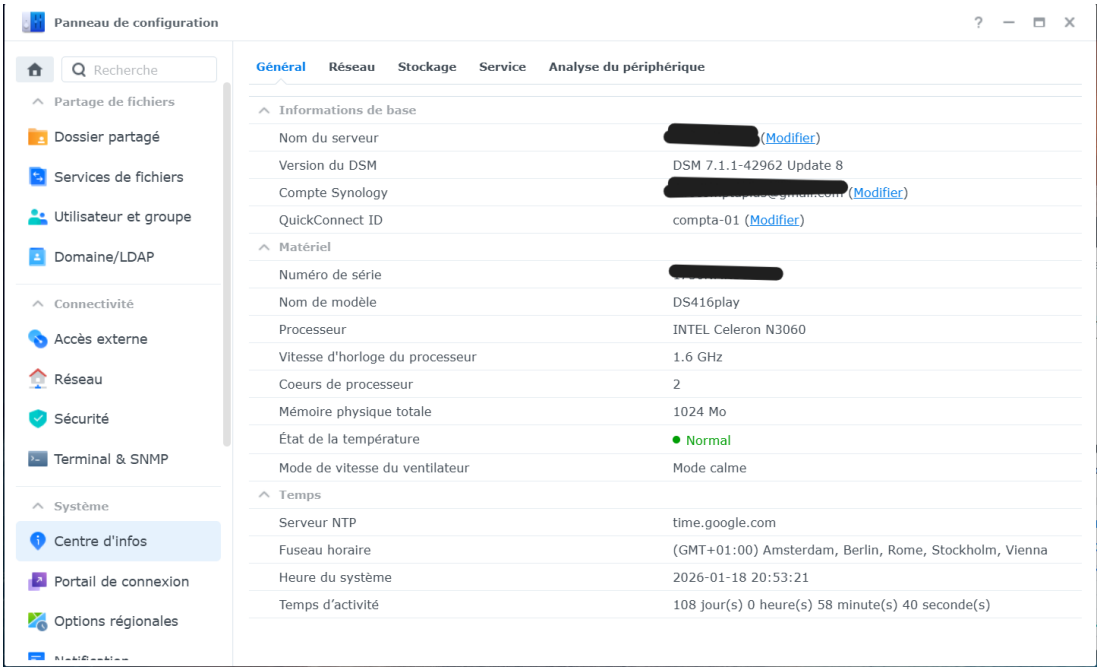

Figure 11: DSM firewall configuration showing firewall feature and settings.

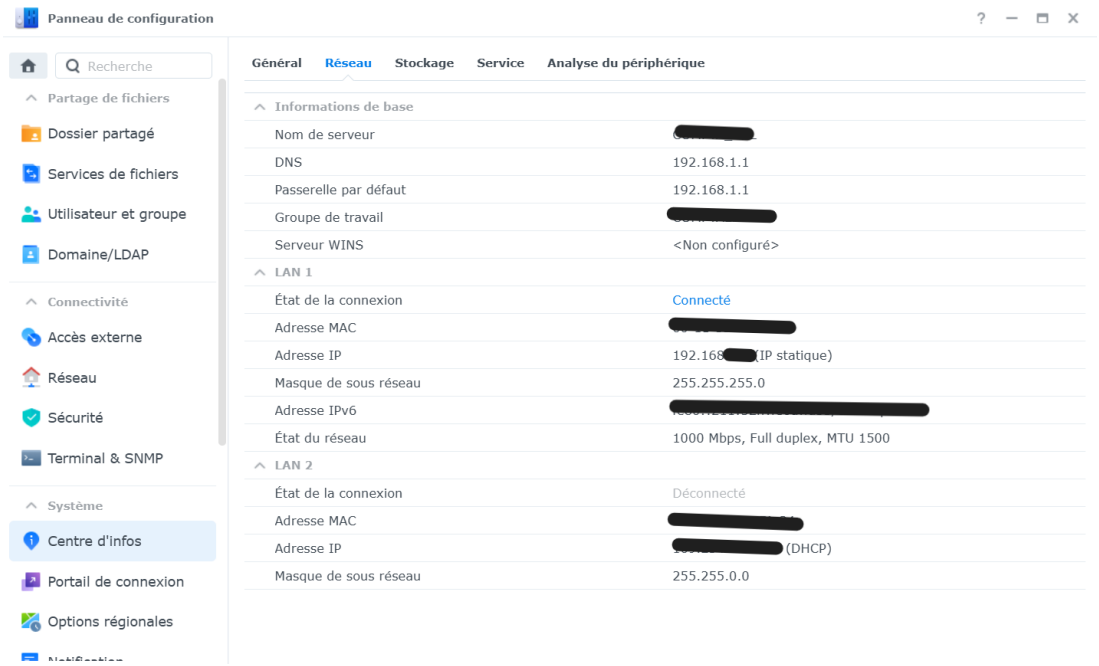

Figure 12: Auto-block protection configuration showing IP-based brute-force defense settings.

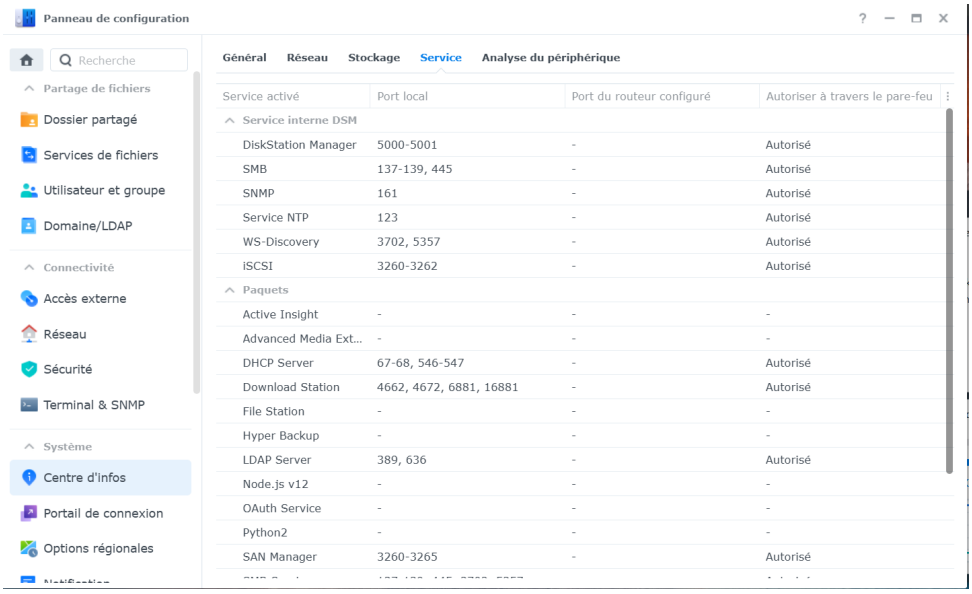

Figure 13: Account security settings showing Two-Factor Authentication (2FA) feature availability.

System Information

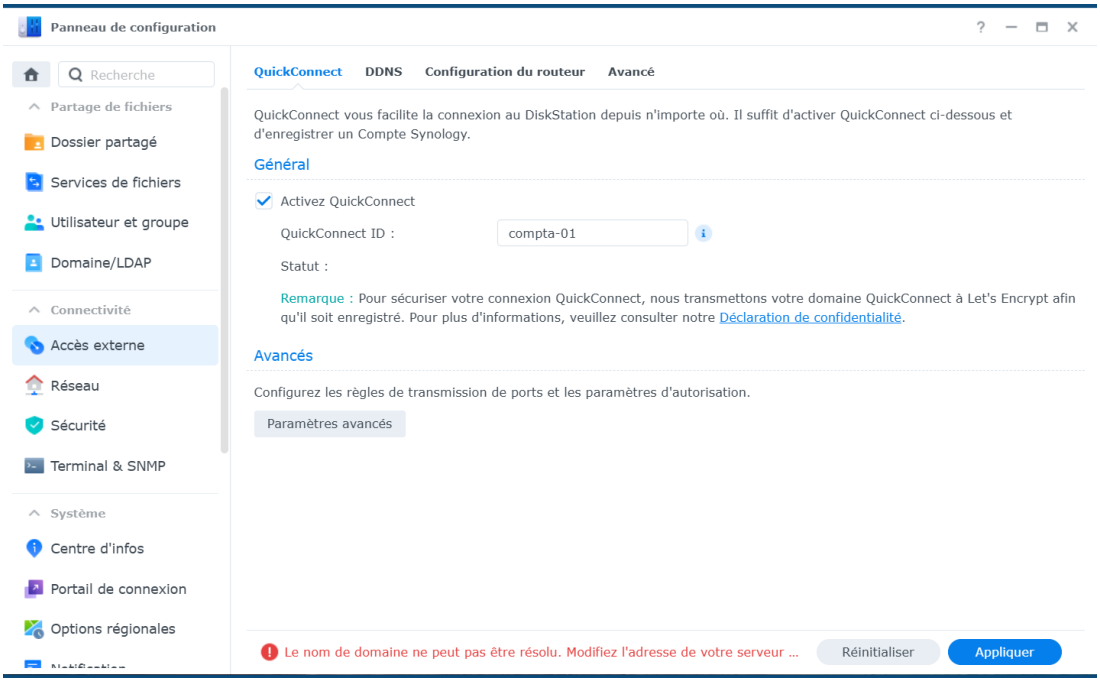

Figure 14: DSM system information displaying hardware specifications (DS416play, Intel Celeron N3060, 1024 MB RAM) and software version (DSM 7.1.1-42962 Update 8).

A.4 Shared Folder Structure

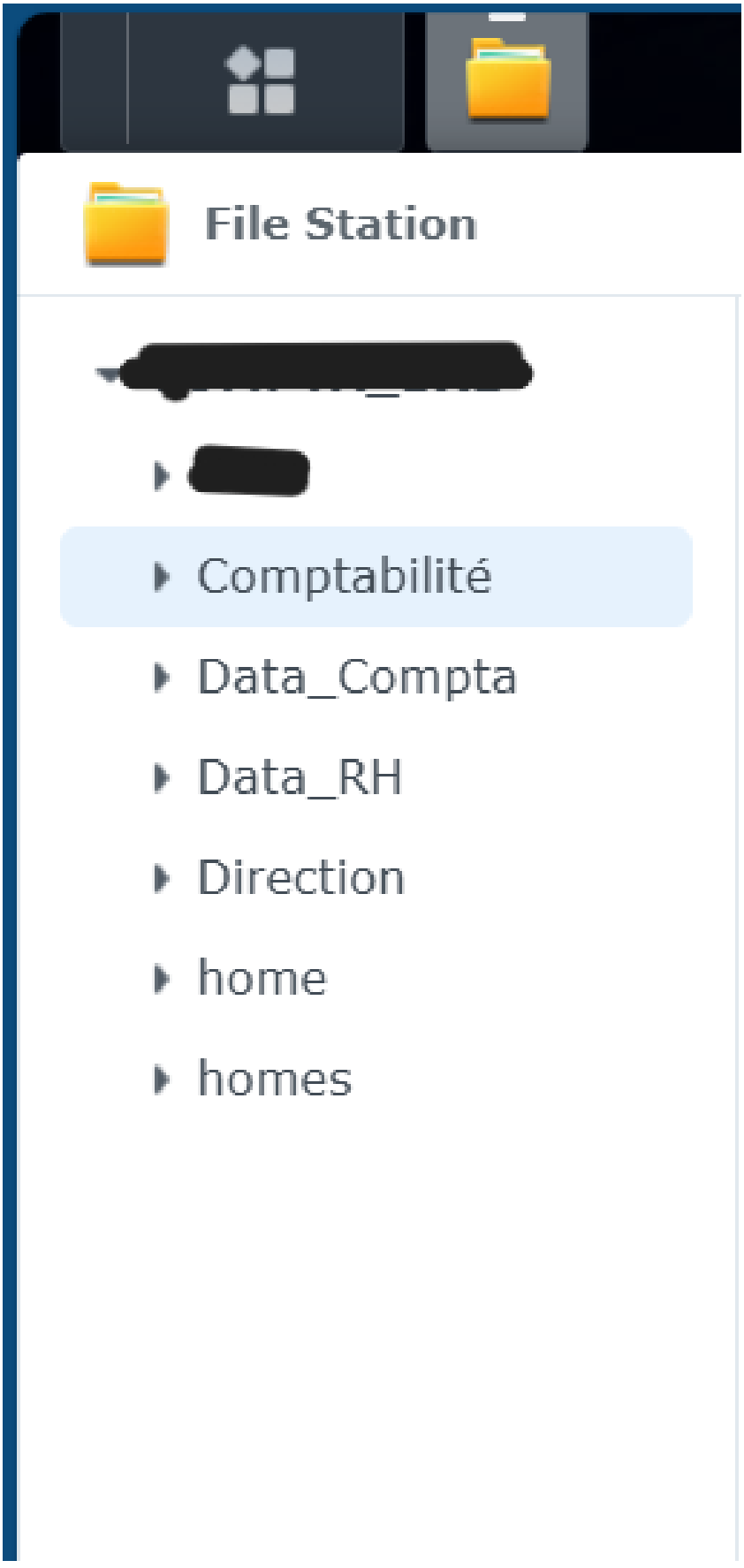

Figure 15: File Station shared folder hierarchy showing departmental folders (Comptabilité, Data_Compta, Data_RH, Direction, home) with role-based access control.

B Annex: LLM Usage in this Project

For the preparation of this report, Large Language Models (LLMs) were used as support tools to enhance technical writing quality and structure. The following describes their specific application and the safeguards implemented to maintain academic integrity.

LLM Applications

— **Linguistic Correction and Refinement**: The AI assisted in improving the flow of technical English and corrected syntax or grammar errors to enhance readability for an academic audience.

— **LaTeX Structure and Formatting**: The AI was used to troubleshoot LaTeX compilation errors, specifically regarding image placement, table formatting, and special character management (e.g., `\textit`, `\textbf`, `\includegraphics`).

— **Synthesis Assistance**: The AI helped structure explanations based on raw scan results (Nmap, Nessus, DSM configuration) to make technical findings clearer and more accessible to readers unfamiliar with security assessment tools.

Important Clarifications

— **Original Content**: All technical data (network scans, vulnerability findings, configuration screenshots, threat analysis) are the direct result of personal work conducted on the organization's network infrastructure. The STRIDE threat model, risk assessment, and security recommendations are entirely original analytical work.

— **Verification**: Every suggestion or explanation provided by the AI was cross-validated against authoritative sources including official documentation (Synology DSM guides, Nmap manual, Nessus documentation), academic literature (STRIDE framework, Microsoft SDL), and security standards (NIST SP 800-115, CIS benchmarks) to prevent potential errors or "hallucinations."

— **Confidentiality**: No sensitive data (IP addresses, MAC addresses, hostnames, credentials, organizational identifiers) was shared with the LLM. All project-specific information was anonymized before any AI interaction to prevent potential data leakage through model training vectors.

— **Academic Integrity**: The LLM functioned strictly as an *assistive editing tool*, not as a *content generation tool*. All security findings, threat classifications, and mitigation strategies presented in this report are based on empirical evidence from network assessments and established cybersecurity frameworks, validated independently by the author.

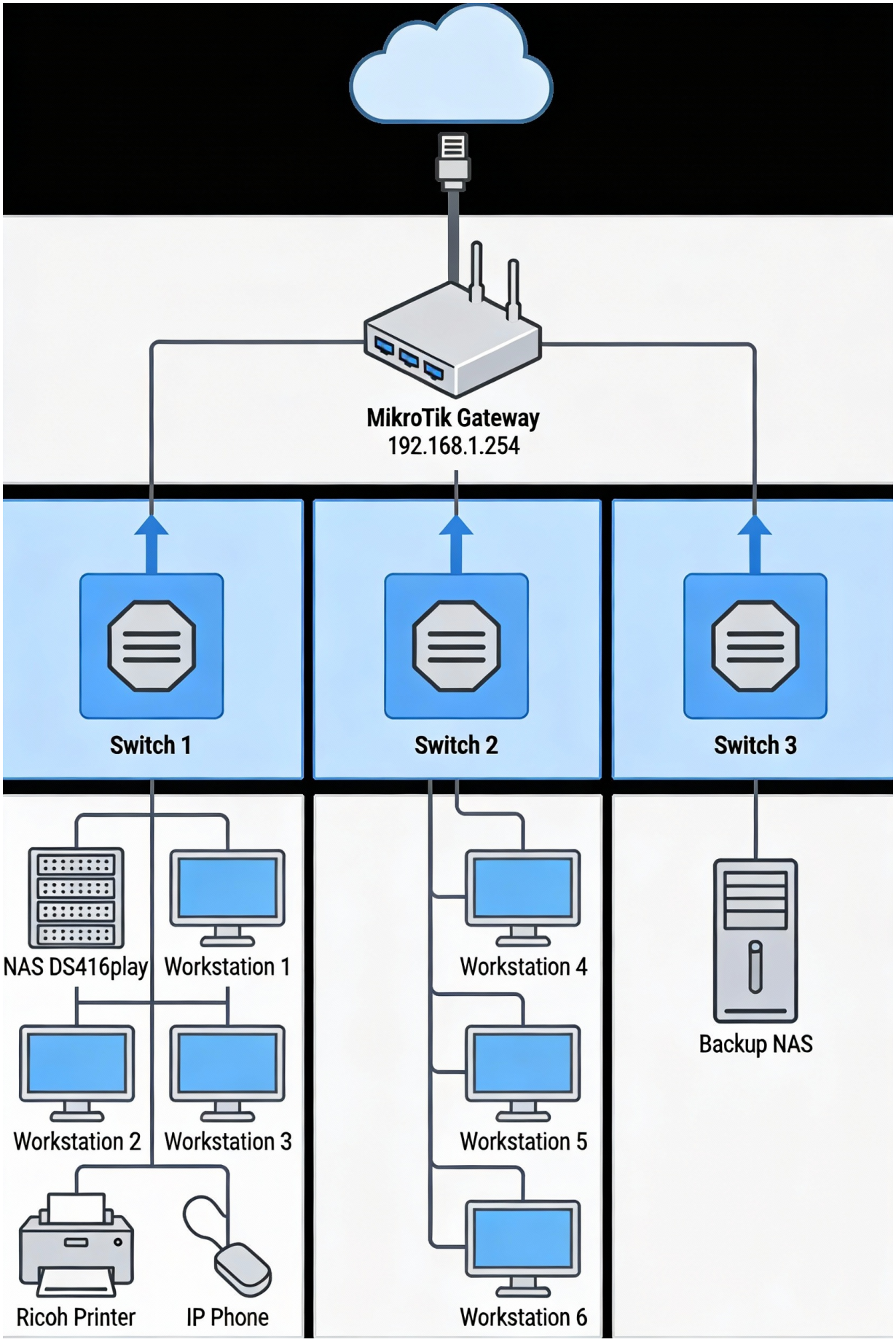

Figure 1: Office network topology showing three switch segments: Switch 1 with primary NAS and workstations, Switch 2 with secondary workstations, Switch 3 with backup NAS and gateway.

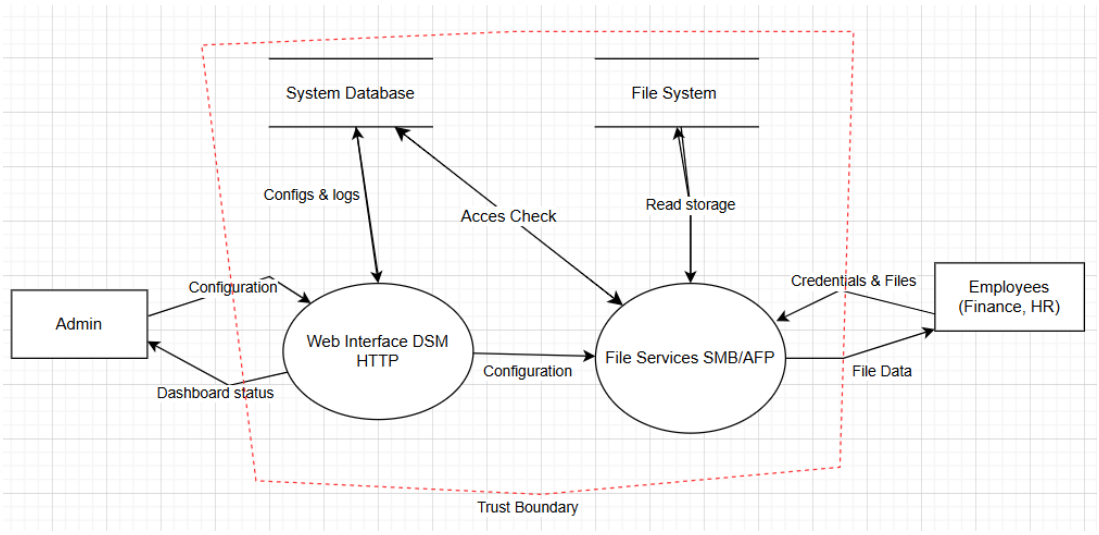

Figure 2: Data Flow Diagram showing trust boundary, actors (Admin, Employees), processes (Web Interface DSM, File Services), and data stores (System Database, File System).

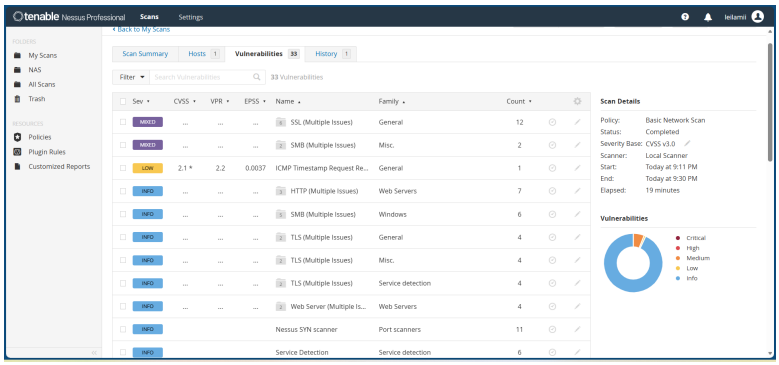

Figure 3: Nessus vulnerability severity distribution: 5 Medium, 81 Info, minimal Critical/High findings.