System and Network Infrastructure Design and Implementation Report for BankSO

Summary

- Overview
- Timeline
- Tasks
- Company Organizational Chart
- Statement Of Work
- Equipment Used
- Network Topology
- Proposed Solutions
- Project Objectives
- Expected Results
- Gantt Chart
- Areas For Improvements
- ANSSI Recommendations
- Communication Matrix
- Cisco Packet Tracer
- Documentations

Overview

Project name: INFRA BANKSO	**Due date:** Apr 4, 2025

Goal: Design and implement a secure and high-performance systems and network infrastructure for BankSO, enabling the company to meet its needs in terms of data management, security, and communication.

Group members

Name	Role	Contact
Samuel DECARNELLE	Project manager / Technician	07 11 11 11 11
Julien PESCE	Technician	07 22 22 22 22
Sasha DANIEL	Technician	07 33 33 33 33
Maxence GALOPIN	Technician	07 44 44 44 44
Marc VANCAPPEL	Technician	07 55 55 55 55
Gabrielius VANDERHAGHEN	Technician	07 66 66 66 66

Project overview

Objective	Success Criteria
This project aims to design and implement a secure systems and network infrastructure for BankSO.	□ **Secure infrastructure**: The implementation of a secure systems and network infrastructure, compliant with industry security standards.
The objective is to create a robust and efficient infrastructure that meets the company's data management, security, and communication needs.	□ **Optimal performance** : Systems and networks must function efficiently, with minimal latency and maximum availability.
	□ **Timeline adherence** : The project must be completed within the allotted 4-6 week timeline.
The project scope includes network configuration, security measures, and system implementation, with deliverables due within a 4 day timeline.	□ **Quality of deliverables** : Deliverables must meet the needs and expectations of BankSO.
	□ **Client satisfaction** : BankSO's satisfaction with the quality and performance of the implemented infrastructure.

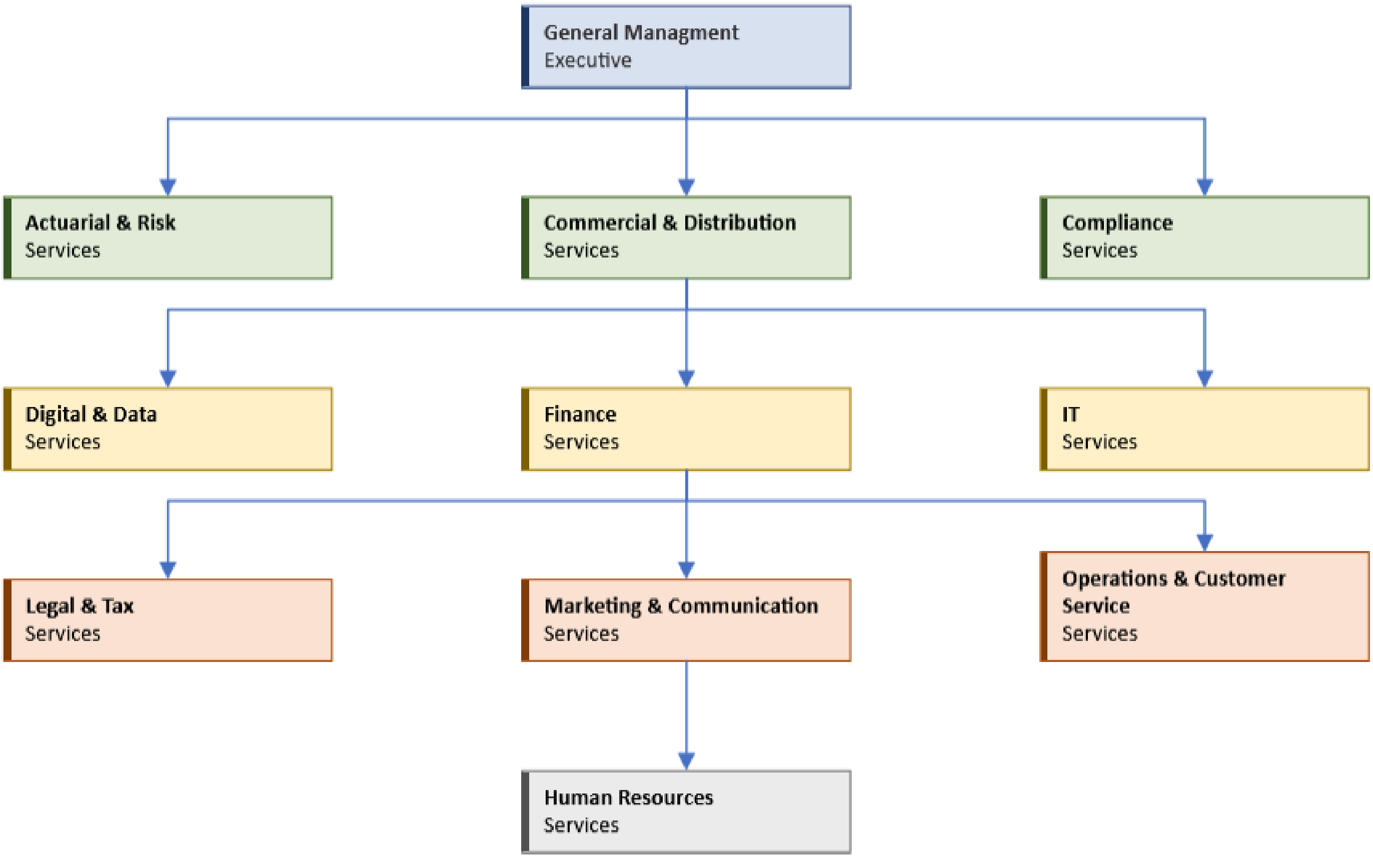
Timeline

<table>
<tr><th>Day 1</th><th>Day 2</th><th>Day 3</th><th>Day 4</th></tr>
<tr><td><b>Coordination</b>
<b>Roles distribution</b></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Early Phase Development</td><td></td><td></td></tr>
<tr><td></td><td>First team gathering</td><td></td><td></td></tr>
<tr><td></td><td colspan="2">Testing, further development</td><td></td></tr>
<tr><td></td><td></td><td>Second team gathering</td><td></td></tr>
<tr><td></td><td></td><td colspan="2">Final touch, assembly</td></tr>
<tr><td></td><td></td><td></td><td><b>Network Rollout</b></td></tr>
</table>

Tasks

Group member	Task
Samuel DECARNELLE	Web Server, phpmyadmin, fail2ban, SSL, reverse proxy
Julien PESCE	Windows Server : ADDS DHCP DNS WDS, File sharing
Sasha DANIEL	ADDS, WDS, VPN attempt, Gantt Chart
Maxence GALOPIN	Windows Server : ADDS, DHCP, DNS, WDS
Marc VANCAPPEL	IoDraw, Network Map, CISCO, GNS3 implementation attempt, firewall (pfSense),
Gabrielius VANDERHAGHEN	Documentation (PDF, Company Organizational Chart), BankSO website, VPN attempt

Company Organizational Chart



Statement of Work

Functional and Technical Requirements

Security Requirements

1. Implementation of SSL certification for secure, encrypted connections between internal systems and external resources
2. Establishment of a centralized file sharing system with appropriate access controls
3. Deployment of machine security system for continuous device monitoring and threat detection
4. Implementation of port closure system to secure unnecessary ports and reduce attack surface
5. Configuration of Fail2ban to prevent brute-force attacks and unauthorized access attempts
6. VPN implementation for secure remote connections for employees working outside the office
7. Installation and configuration of reverse proxy to protect the internal network from external threats
8. Deployment of pfSense firewall with properly configured security rules and policies

9. Implementation of regular security updates and patches for all systems as per ANSSI recommendations
10. Data encryption for sensitive information at rest and in transit

Performance Requirements

1. Systems and networks must operate efficiently with minimal latency (response time < 100ms)
2. Network infrastructure must support high availability (99.9% uptime)
3. Implementation of load balancing mechanisms to distribute traffic evenly
4. Server resources must be optimized to handle peak usage periods
5. Bandwidth allocation must be configured to prioritize critical business applications
6. Implementation of performance monitoring tools to identify and address bottlenecks
7. Scalable architecture to accommodate future growth in users and applications
8. Backup systems must operate without impacting production environment performance

Communication Requirements

1. Implementation of Active Directory Domain Services (ADDS) for centralized authentication and user management
2. Configuration of ADCS (Active Directory Certificate Services) for certificate-based authentication
3. Deployment of DHCP server for automatic IP address assignment and network configuration
4. Implementation of DNS services for domain name resolution and service discovery
5. Configuration of WDS (Windows Deployment Services) for centralized OS deployment
6. Secure email communication system with encryption and spam filtering
7. Implementation of internal messaging platform for team collaboration
8. Configuration of secure file transfer protocols for external communications
9. Network segmentation to control communication flow between different departments
10. Implementation of logging and monitoring for all communication channels

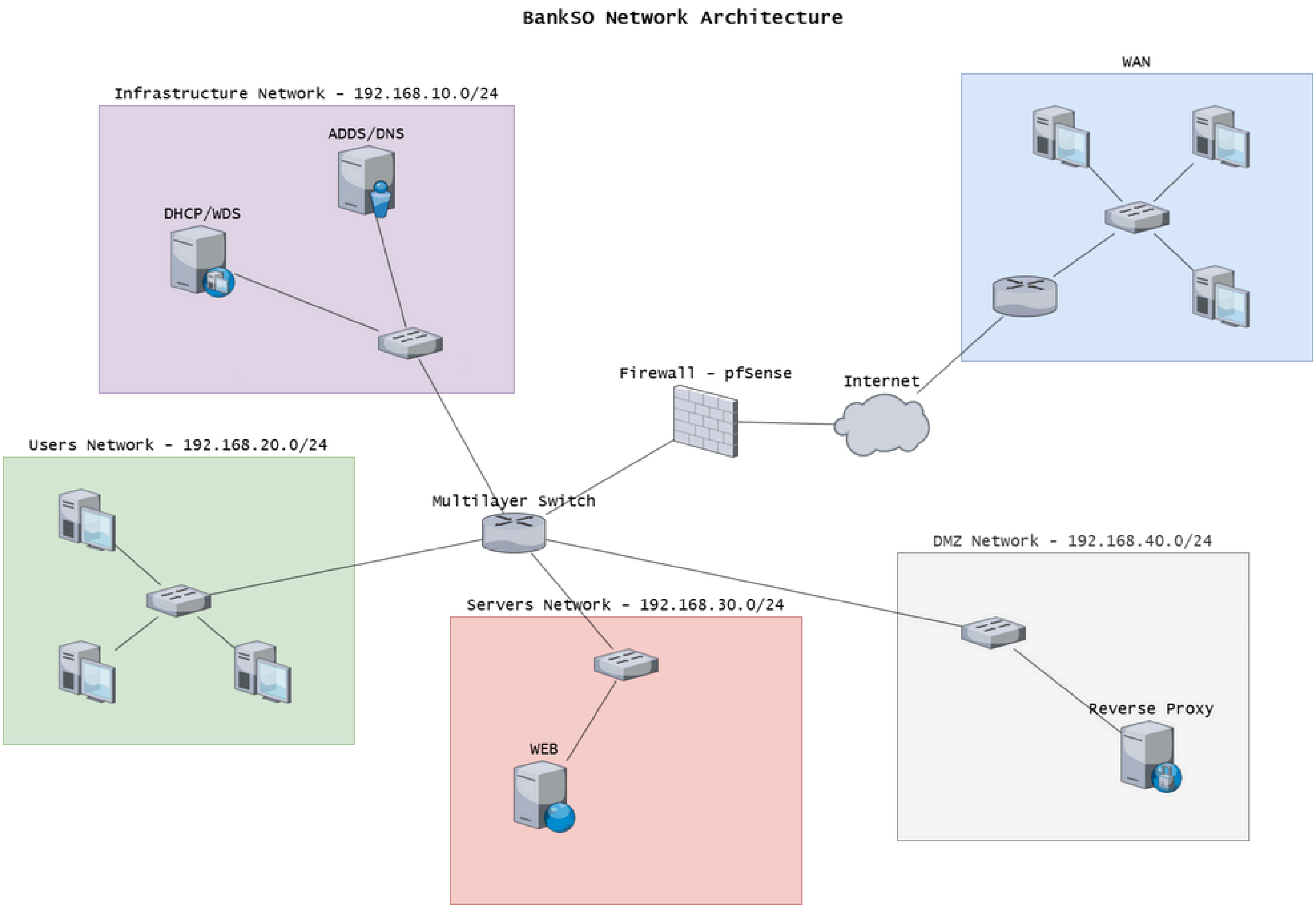
Company-Specific Needs

1. Banking website infrastructure with secure client portal access
2. Integration with existing banking applications and databases
3. Compliance with financial industry security standards and regulations
4. Support for multi-factor authentication for critical systems access
5. Disaster recovery capabilities with minimal data loss and downtime
6. Audit logging for all system and user activities for compliance purposes
7. Secure workstation environments for customer service representatives
8. Protected environment for financial transaction processing
9. Secure infrastructure for mobile banking services
10. Role-based access controls aligned with organizational structure

Equipment Used

Equipment	Description	Quantity
Personal Computer	Workspace	6
VMWare Workstation Pro	Workspace	1
VM Client	Windows 10 Pro, for testing	4
VM Windows Server	Windows Server 2022, to manage a virtual server	2
Web Server	Linux Mint Cinemon, to manage the WEB server with Apache2	1
Reverse Proxy	Linux Mint Cinnamon, to manage the Reverse Proxy with Nginx	1

Network Topology


BankSO Network Architecture
Infrastructure Network - 192.168.10.0/24
ADDS/DNS
DHCP/WDS
WAN
Firewall - pfSense
Internet
Users Network - 192.168.20.0/24
Multilayer Switch
DMZ Network - 192.168.40.0/24
Servers Network - 192.168.30.0/24
Reverse Proxy
WEB

Proposed Solutions

Equipment	Description
Reverse proxy	A reverse proxy will be implemented to protect the internal network from external attacks and to ensure that all incoming traffic is filtered and authenticated before reaching the internal servers. The reverse proxy will be configured to only allow authorized traffic and will block all other traffic by default. The reverse proxy will force the HTTP to HTTPS to ensure the security.
WEB Server	The WEB Server will be onto a local network only and will receive the 443 traffic from the Reverse Proxy.
Firewall (pfsense)	A firewall will be implemented using pfsense to protect the internal network from external attacks and to ensure that all incoming and outgoing traffic is filtered and authenticated. The firewall will be configured to only allow authorized traffic and will block all other traffic by default.
ADDS (Active Directory Domain Services)	An Active Directory Domain Services (ADDS) will be implemented to provide a centralized authentication and authorization system for all users and computers on the network. This will ensure that all users and computers are properly authenticated and authorized before accessing network resources.
ADCS	The ADCS implementation will integrate seamlessly with the existing Active Directory infrastructure, providing automated certificate enrollment for domain-joined devices and enabling certificate-based authentication for critical systems.
DHCP (Dynamic Host Configuration Protocol)	A DHCP server will be implemented to automatically assign IP addresses and other network settings to devices on the network. This will ensure that all devices on the network are properly configured and can communicate with each other.

WDS (Windows Deployment Services)	A Windows Deployment Services (WDS) server will be implemented to provide a centralized deployment system for all Windows-based devices on the network. This will ensure that all devices on the network are properly configured and up-to-date with the latest software and security patches.
DNS (Domain Name System)	A DNS server will be implemented to provide a centralized system for resolving domain names and IP addresses on the network. This will ensure that all devices on the network can communicate with each other and access external resources.
SSL certification	An SSL certificate will be implemented to provide a secure and encrypted connection between the internal network and external resources. This will ensure that all data transmitted between the internal network and external resources is properly encrypted and secure.
File sharing	A file sharing system will be implemented to provide a centralized system for sharing files and resources on the network. This will ensure that all users on the network can access and share files and resources in a secure and controlled manner.
Machine security	A machine security system will be implemented to provide a centralized system for securing and monitoring all devices on the network. This will ensure that all devices on the network are properly secured and up-to-date with the latest security patches.
Port closure	A port closure system will be implemented to ensure that all unnecessary ports on the network are closed and secured. This will prevent unauthorized access to the network and ensure that all devices on the network are properly secured.
Fail2ban setup	A Fail2ban setup will be implemented to provide a centralized system for detecting and preventing brute-force attacks on the network. This will ensure that all devices on the network are properly secured and protected from unauthorized access.

Project Objectives

Primary Objective

To design and implement a secure systems and network infrastructure for BankSO that meets the company's needs for data management, security, and communication.

Success Criteria

1. **Secure Infrastructure**: Implementation of a secure infrastructure compliant with industry security standards
2. **Optimal Performance**: Systems and networks functioning efficiently with minimal latency and maximum availability
3. **Timeline Adherence**: Project completion within the 4-day timeline
4. **Quality of Deliverables**: All deliverables meeting BankSO's needs and expectations
5. **Client Satisfaction**: BankSO's satisfaction with the quality and performance of the implemented infrastructure

Security Implementation Components

- SSL certification for secure, encrypted connections
- Centralized file sharing system
- Machine security system for device monitoring
- Port closure system to secure unnecessary ports
- Fail2ban setup to prevent brute-force attacks
- VPN implementation for secure remote connections
- Reverse proxy to protect internal network
- pfSense firewall configuration
- Active Directory Domain Services (ADDS) for centralized authentication
- ADCS for certificate services
- DHCP, DNS, and WDS implementation

The project scope includes network configuration, security measures, and system implementation in accordance with ANSSI recommendations for secure information systems.

Expected Results

Security Enhancements

1. **Encrypted Communications**: All data transmitted between internal network and external resources will be properly encrypted through SSL certification
2. **Protected Network Access**: Unauthorized access prevented through port closure system and firewall implementation
3. **Attack Prevention**: Reduced security incidents through Fail2ban implementation to detect and prevent brute-force attacks

Infrastructure Improvements

1. **Centralized Management**: Fully functional Active Directory infrastructure providing centralized authentication and authorization
2. **Automated Network Configuration**: DHCP server successfully assigning IP addresses and network settings to all devices
3. **Streamlined Resource Sharing**: Centralized file sharing system enabling secure and controlled file access
4. **Efficient Domain Resolution**: DNS server properly resolving domain names and IP addresses across the network
5. **Simplified Deployment**: Windows Deployment Services enabling standardized deployment of Windows-based devices

Operational Benefits

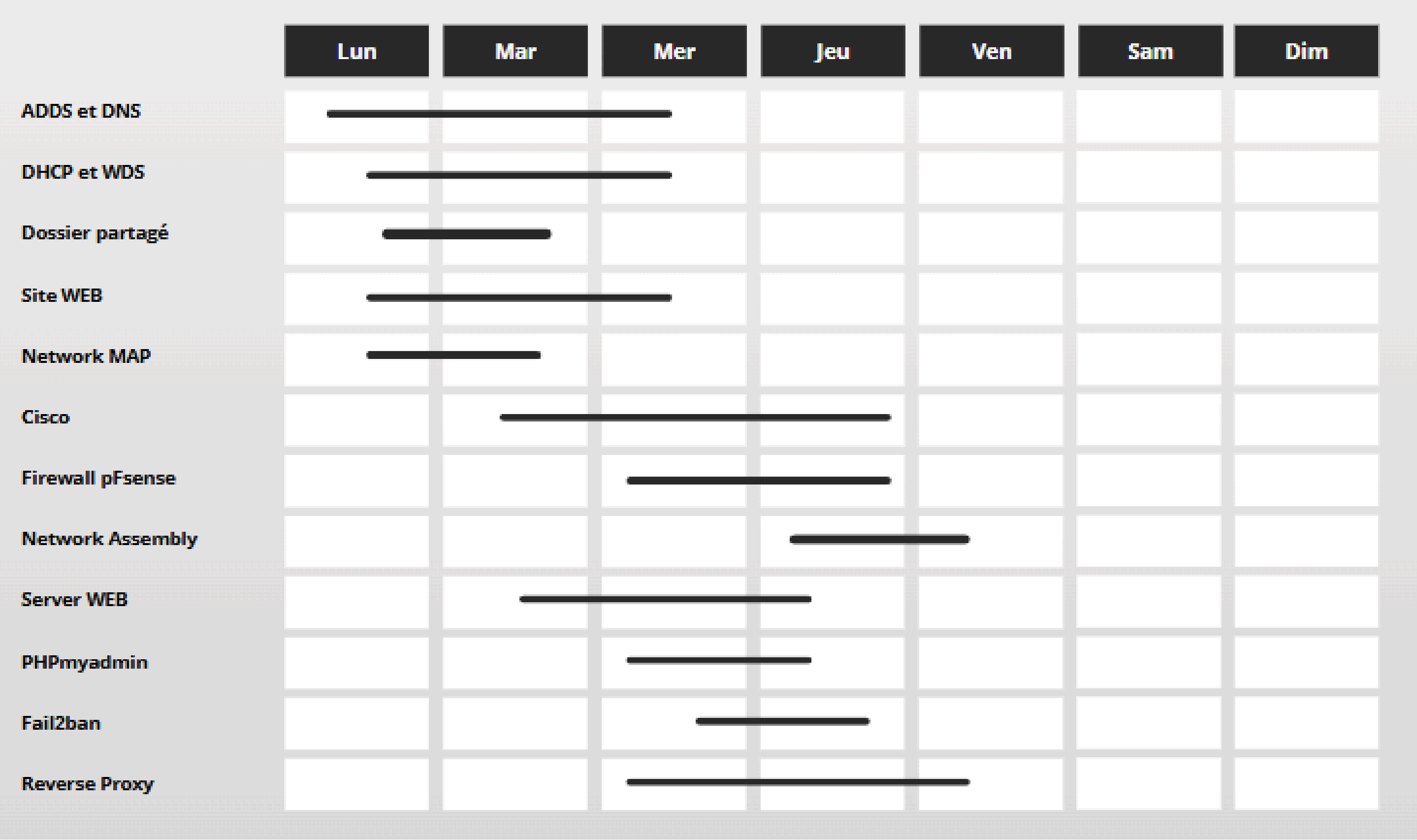
1. **Improved System Security**: All devices properly secured and up-to-date with latest security patches
2. **Enhanced Compliance**: Network configuration aligning with ANSSI security recommendations
3. **Optimized Performance**: Network and systems operating at peak efficiency with minimal latency
4. **Simplified Administration**: Centralized management of security policies, users, and devices
5. **Increased Reliability**: Stable infrastructure with high availability for business operations

Documentation Deliverables

1. **Comprehensive Network Topology**: Detailed documentation of network segments, servers, and devices
2. **Implementation Guides**: Step-by-step configuration documentation for all implemented services
3. **Security Protocols**: Documentation of security measures and best practices adopted

The infrastructure will be delivered as a complete, functional system ready to support BankSO's business operations with enhanced security and performance.

Gantt Chart



Areas for Improvement

For the Web Server:

Others LAN Or WAN website - We can, in the future implement others website if the company have the need for it.

For the Reverse-Proxy:

Redirection for Others services that need an WAN access - We can implement more services inside the DMZ and/or redirect more services to the WAN.

For the Fail2Ban:

Email notifications for ban events - Our company can easily configure the reverse proxy to send e-mails to notified to the IT services if the reverse proxy ban users or bot. This implementation make the process way more easy for the IT of your company.

Whitelist configuration for trusted IPs - We can easily implement some trusted IP address so the Fail2ban don't ban the IT service for example.

Geo-blocking integration for high-risk regions - We can integrate a Geo-blocking, so the high-risk regions are block by default.

Custom actions for persistent attackers - We can make some customs actions for persistent attackers.

Integration with centralized security monitoring - Our company can developpe a tools to centralized the security monitoring.

For the All the services:

Multi-Factor Authentication (MFA) - Enhancing the authentication system beyond passwords to provide an additional layer of security for accessing critical systems and data.

Penetration Testing Schedule - Establishing a regular schedule for security assessments and penetration testing to proactively identify vulnerabilities.

Network Performance Monitoring - Implementing tools to continuously monitor network performance, identify bottlenecks, and optimize resource usage.

Comprehensive Backup Solution - Implementation of an automated backup and disaster recovery system to ensure business continuity in case of data loss or system failure.

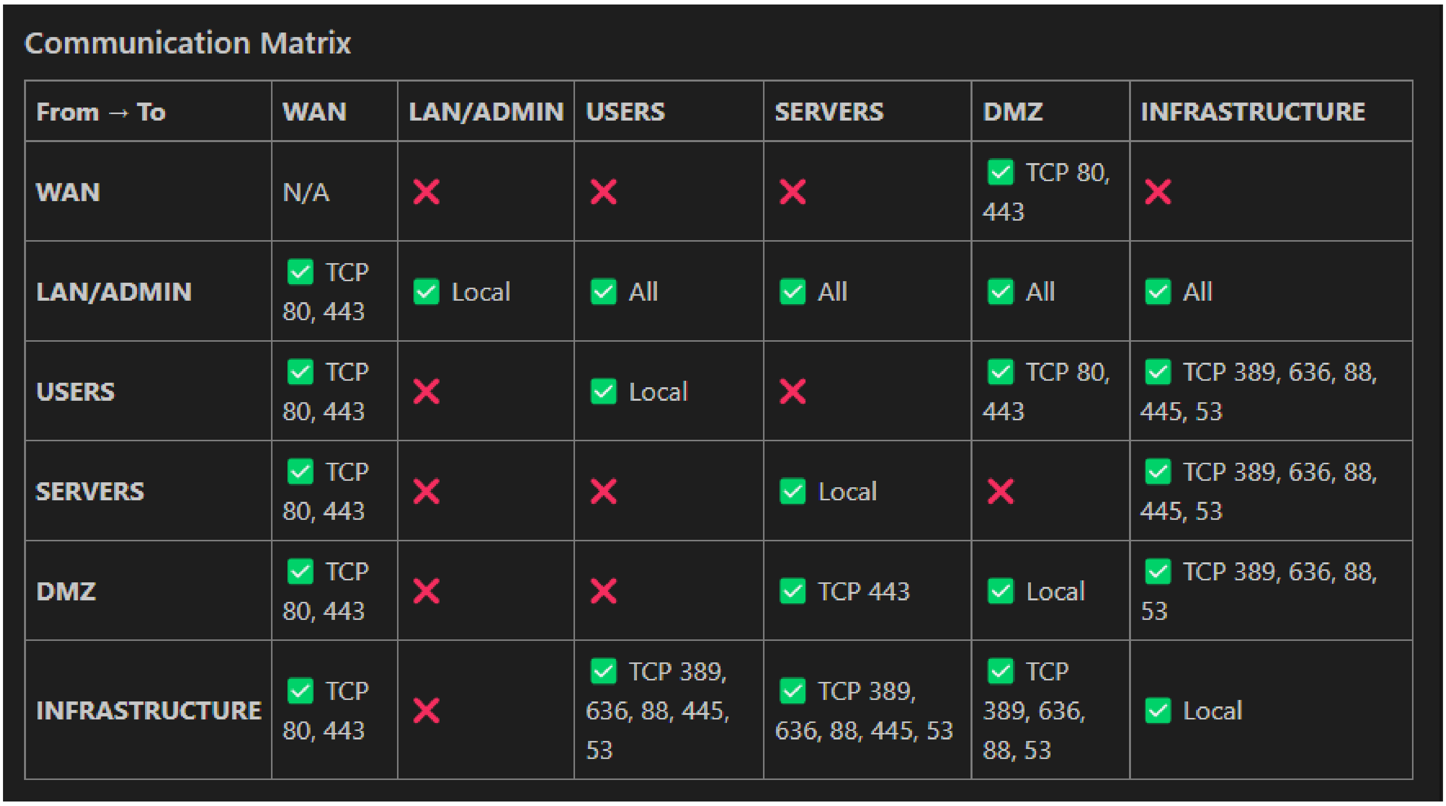
Documentation Improvement - Creating more detailed technical documentation and standard operating procedures for system maintenance and troubleshooting.

ANSSI Recommendations

The ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) is a French government agency responsible for ensuring the security of information systems. Here are some of the ANSSI recommendations that have been implemented to the BankSO project:

1. **Password management**: ANSSI recommends implementing strong password policies, including password length, complexity, and rotation.
2. **Firewall configuration**: ANSSI recommends configuring firewalls to only allow necessary traffic, and to block all other traffic by default.
3. **Network segmentation**: ANSSI recommends segmenting the network into different zones, each with its own access controls and security measures.
4. **Secure protocols**: ANSSI recommends using secure communication protocols, such as HTTPS, SSH, and SFTP, instead of insecure protocols like HTTP, FTP, and Telnet.
5. **Regular updates and patches**: ANSSI recommends regularly updating and patching all systems, including operating systems, applications, and firmware.
6. **Access control**: ANSSI recommends implementing strict access controls, including role-based access control (RBAC) and attribute-based access control (ABAC).

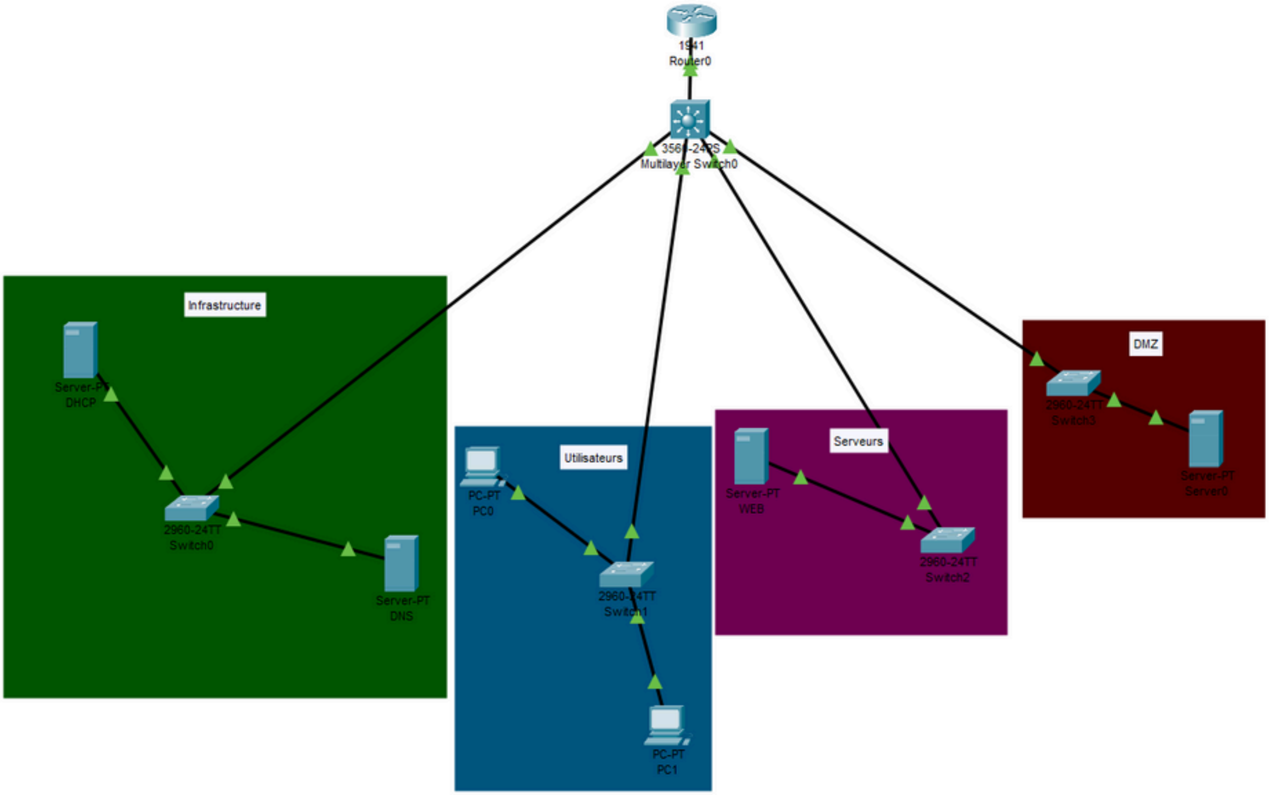
Communication Matrix



Communication Matrix

From → To	WAN	LAN/ADMIN	USERS	SERVERS	DMZ	INFRASTRUCTURE
WAN	N/A	❌	❌	❌	✅ TCP 80, 443	❌
LAN/ADMIN	✅ TCP 80, 443	✅ Local	✅ All	✅ All	✅ All	✅ All
USERS	✅ TCP 80, 443	❌	✅ Local	❌	✅ TCP 80, 443	✅ TCP 389, 636, 88, 445, 53
SERVERS	✅ TCP 80, 443	❌	❌	✅ Local	❌	✅ TCP 389, 636, 88, 445, 53
DMZ	✅ TCP 80, 443	❌	❌	✅ TCP 443	✅ Local	✅ TCP 389, 636, 88, 53
INFRASTRUCTURE	✅ TCP 80, 443	❌	✅ TCP 389, 636, 88, 445, 53	✅ TCP 389, 636, 88, 445, 53	✅ TCP 389, 636, 88, 53	✅ Local

Cisco Packet Tracer



Documentation

Here you can discover in detail the configuration, the maintenance procedures and some good practices:

- Web Server Configuration & Good Practice Link
- Reverse-Proxy Configuration & Good Practice Link
- Firewall Configuration & Good Practice Link