Diego Raúl Roldán Urueña

LAB TASK 4

NETWORK SYSTEMS AND SECURITY

FACHHOCHSCHULE KIEL
University of Applied Sciences

Environment

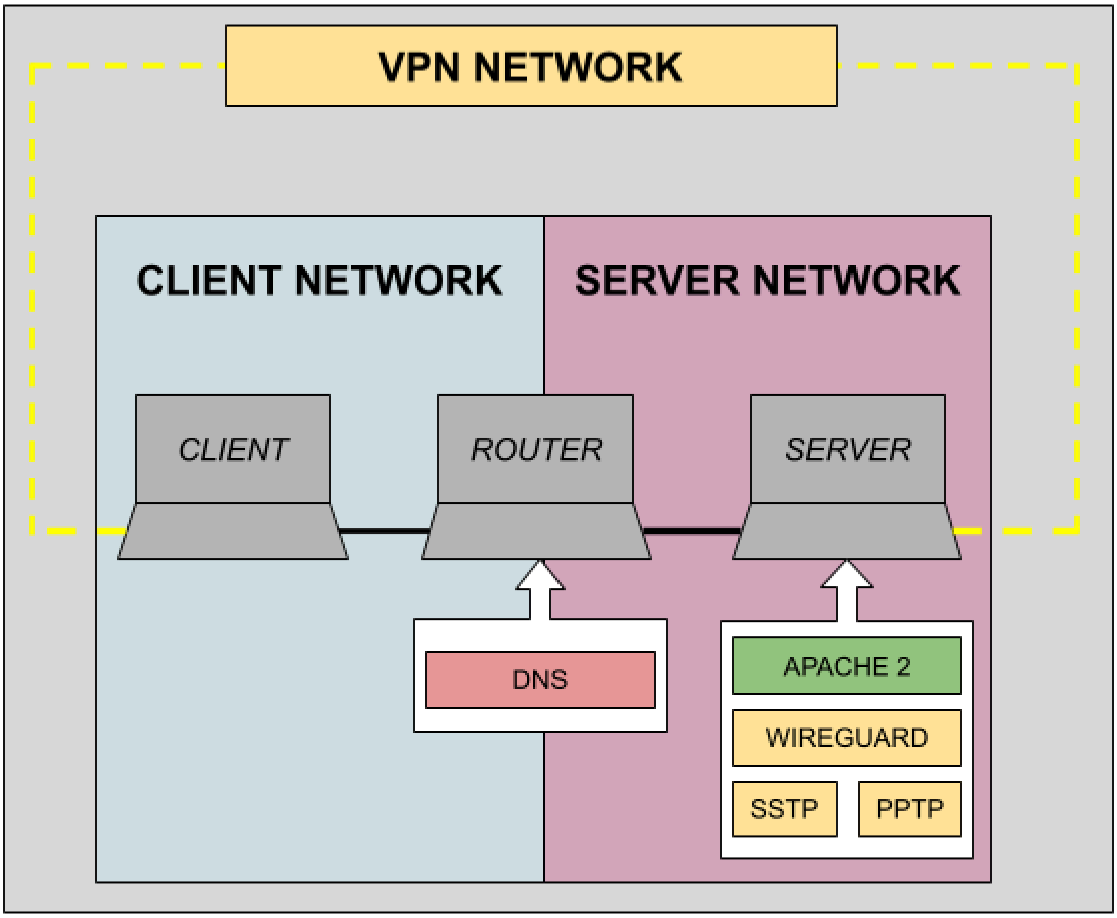
In words

This network is made up of 2 different internal private networks. Each of them has 2 machines on it, one of them will be the router which is connected to both networks and the other one will be client on one network and server on the other. So, in total we have 2 machines in different networks which are available between each other via the router which is connected to both networks.

The router provides a DNS server which is used by client and server.

The server provides a web server and a VPN server. Both can be accessible by the client via router.

In a drawing



Locating in the standard

This file has been used https://www.itref.ir/uploads/editor/42890b.pdf.

Requirements

4 - Context of the Organization

- Identify Internal and External Issues:
  - Internal: Network topology, role of each machine (router, client server).
  - External: Threats like unauthorized access, data interception, or misuse of DNS services.

6.1 - Information Security Risk Assessment

- Identify risks like threats to DNS, web server and VPN vulnerabilities, or router/server misconfiguration.

6.2 - Information Security Objectives

- Ensure secure and uninterrupted access to the web server, VPN and DNS services.
- Ensure encrypted communication for VPN traffic.

7 - Support

- Competence: Make sure that administrators are trained in securing DNS, web servers, and VPNs.
- Awareness: Users should understand how to safely use VPNs.

8 - Operational Controls

- Document configuration changes in the router, DNS server, and VPN server.

9 - Performance Evaluation

- Regularly test VPN connectivity and web server availability from the client network.

Checklists

Area	Checklist Item	Implemented (Y/N)
A.5	Context of the Organization	
A.5.1.1	Policies for information security	
A.6	Organization of information security	
A.6.1.1	Information security roles and responsibilities	
A.8	Asset management	
A.8.2.1	Classification of information	
A.9	Access control	
A.9.1.1	Access control policy	
A.9.1.2	Access to networks and network services	
A.9.2.4	Management of secret authentication information of users	
A.9.3.1	Use of secret authentication information	
A.10	Cryptography	
A.10.1.2	Key management	
A.12	Operations security	
A.12.1.1	Documented operating procedures	
A.13	Communications security	
A.13.1.1	Network controls	
A.13.1.2	Security of network services	
A.13.1.3	Segregation in networks	

Security guidelines for Private Environment

This document outlines the security requirements for implementing ISO 27001 in a network consisting of two private internal networks connected via a router, ensuring the correctness of the DNS server, VPN server, and web server.

1. Network Segmentation and Routing

- The router shall enforce strict firewall rules to allow only necessary traffic between the networks.
- The server shall enforce firewall rules to allow only necessary traffic.
- Traffic between the client and server networks shall be monitored and logged on the router.

2. DNS

- The server shall only allow queries from authorized machines in the private networks.
- DNS logs shall be stored securely and monitored for anomalies.

3. VPN

- Split-tunneling shall be employed to route only necessary traffic through the VPN.
- The server shall implement strict access control to allow only authorized client devices to connect.
- The server shall be configured to log all connection attempts securely.

4. Web Server

- The server shall be secured with a valid TLS/SSL certificate to encrypt all packages
- The server shall use firewall rules to restrict access to specific IP ranges (e.g., the client network).

5. System

- All systems (router, server, client) shall:
  - Disable unused services and ports.
  - Apply least privilege principles for all users and services.
  - Regularly update software to fix vulnerabilities.

6. Authentication and Access Control

- Strong passwords or certificates shall be required for all users accessing the VPN and web server.
- Administrative access to the router, VPN, and web server shall be restricted to specific IP addresses.

7. Backup and Recovery

- Configuration backups of the router, DNS server, and VPN server shall be performed regularly.