Project: METAL SNAKE

Requirements Document

Project Sponsor: Brendan Gasparin

Project Manager: Brendan Gasparin

Date of Project Approval: 14/08/2024

Commencement Date: 29/07/2024

Estimated Completion Date: 24/10/2024

Estimated Project Duration: 17 Weeks

Version: 1.0 (2024-08-24)

1. Executive Summary

1.1. Introduction

Project: METAL SNAKE involves the creation of an on-premises cybersecurity lab with a server for hosting business infrastructure (including a website), and cloud infrastructure to host client sites and a SIEM cybersecurity system.

1.2. Purpose of the Requirements Document

The purpose of the Requirements Document is to capture and define all the functional and non-functional requirements for Project: METAL SNAKE. This document will guide the development of the on-premises cybersecurity lab and web server, including the setup of network infrastructure

1.3. Project Objectives

The overall objectives of Project: METAL SNAKE are:

- Reducing reliance on expensive cloud hosting services for the business website.
- Provision of a cybersecurity lab for increased security posture and staff training.
- Thorough public documentation to make the process replicable for learners.

1.4. Scope

Project: METAL SNAKE aims to create a secure, cost-effective on-premises infrastructure for web hosting and cybersecurity, integrated with cloud-based services. The requirements in this document cover the setup and configuration of hardware, software, and network components, as well as security and performance standards.

Table of Contents

2. Introduction

2.1. Project Overview

Project: METAL SNAKE is the construction of an on-premises cybersecurity lab using Raspberry Pi devices to reduce reliance on cloud hosting. The project include the installation of a LAMP stack web server with Mautic email automation, and integration with cloud services for reliable client web hosting and security monitoring. The processes will be thoroughly documented to allow replication by others.

2.2. Stakeholders

The following stakeholders may have an interest in the project requirements:

Stakeholder	Title/Position	Interest in Project	Additional Notes
Brendan Gasparin	Sole proprietor	Project Sponsor / Project Manager	
[redacted]	Premises owner	Premises owner	
	Premises owner	Premises owner	
	Intern	Education, experience, fun	
Vendors	N/A	Supplier	
Clients	Varies	Internet services	
Users	Varies	End-user	

2.3. Document Structure

The Requirements Document is broken down into sections covering functional requirements, non-functional requirements, assumptions and constraints, and approval details. It also includes a Requirements Traceability Matrix to map each requirement to its source and corresponding test cases.

3. Functional Requirements

ID #	Description	Rationale	Acceptance Criteria	Dependencies
FR-001	The ISP modem must be setup and configured.	Provides access to the Internet.	The ISP modem allows devices to connect to the Internet via Ethernet.	None
FR-002	The LAMP stack must be installed and configured on a Raspberry Pi to host the business website.	Provides local hosting for the business website, reducing cloud hosting costs	The website is accessible, and all necessary services (e.g. Apache, MySQL, HTTPS) are running properly.	FR-001
FR-003	A cloud-based web server must be set up to provide hosting for client websites.	Ensures business continuity during residential Internet outages.	The cloud-based server remains operational during on-premises outages and has minimal downtime.	FR-001
FR-004	The Raspberry Pi firewall must be configured with predefined security rules to filter inbound and outbound traffic.	Protects the network from unauthorized access and threats.	The firewall successfully blocks unauthorized traffic, and security tests confirm effectiveness.	FR-001
FR-005	The Raspberry Pi router must be configured to allow Internet access through an ISP modem in bridged mode.	Ensures the network can access the Internet for business and residential users.	Internet access is confirmed, and the network configuration is stable.	FR-001
FR-006	The Raspberry Pi wireless access point must be configured to allow Internet access to business and residential users.	Ensures wireless devices can access the Internet for business and residential users.	Internet access is confirmed for all devices, and the network configuration is stable.	FR-005
FR-007	The network needs to be assembled to complete the lab.	Ensures the network functions.	Connectivity and necessary functions between Raspberry Pis, ISP modem, and external network are confirmed.	FR-001, FR-002, FR-003, FR-004, FR-005, FR-006
FR-008	The cloud-based SIEM system must be configured to monitor and collect logs from the on-premises network.	Enhances network security by providing real-time monitoring and alerts for potential threats.	The SIEM system receives logs and generates alerts as expected.	FR-004, FR-007

FR-009	Mautic is installed and configured to run automated emails and email campaigns.	Allows for automated email capabilities.	Mautic is tested and validated with both automated email and automated email campaign functionality.	FR-002
FR-010	Regular backups of the web servers and Mautic data must be scheduled and stored securely.	Protects against data loss due to system failures or attacks.	Backups are completed as scheduled, and data recovery is successfully tested.	FR-002, FR-003
FR-011	User access controls must be implemented to restrict access to network devices and the web server based on role and necessity.	Limits access to critical systems and protects against unauthorized changes.	Access control policies are enforced, and only authorized users can make changes.	FR-002, FR-003, FR-007
FR-012	Comprehensive documentation for the installation, setup, and maintenance of all network components, servers, and software must be created.	Ensures that the project can be replicated by others and maintained over time.	Documentation is complete, clear, and published on GitHub.	FR-001, FR-002, FR-003, FR-004, FR-005, FR-006, FR-007, FR-008, FR-009, FR-010, FR-011
FR-013	User-friendly operating manuals must be created for staff training on the new infrastructure.	Facilitates easy handover and ongoing operation by the Operations Team.	Staff successfully follow the operating manuals to complete routine tasks.	FR-001, FR-002, FR-003, FR-004, FR-005, FR-006, FR-007, FR-008, FR-009, FR-010, FR-0011

4. Non-Functional Requirements

4.1. Performance Requirements

ID #	Description	Rationale	Acceptance Criteria
NFR-001	The on-premises network must support a minimum throughput of 100Mbps for business-critical services.	Ensures that network performance is sufficient for daily operations.	Network speed tests confirm a minimum throughput of 100 Mbps.
NFR-002	The LAMP stack web servers must handle at least 50 concurrent connections with a response time of no more than 500 milliseconds.	Ensures the web servers can handle typical traffic loads without performance degradation	Load testing confirms the server meets the specified performance criteria.

4.2. Reliability and Availability Requirements

ID #	Description	Rationale	Acceptance Criteria
NFR-003	The on-premises network must maintain a minimum uptime of 99.9% for business-critical services.	Minimizes downtime and ensures continuous availability of business services.	Monitoring data confirms 99.9% uptime over a defined period.
NFR-004	The cloud-based web server must provide failover support to ensure continuity of service during on-premises outages.	Protects against service disruptions caused by local network issues and residential Internet outages.	Failover tests confirm that the cloud server remains operational during local outages.

4.2. Security Requirements

ID #	Description	Rationale	Acceptance Criteria
NFR-005	All data transmitted between the on-premises network and the cloud must be encrypted using TLS 1.2 or higher.	Protects sensitive data from interception during transmission.	Network tests confirm that all data is encrypted during transmission.
NFR-006	The system must undergo regular security audits and vulnerability assessments.	Ensures that the infrastructure remains secure over time and that any vulnerabilities are addressed promptly.	Security audit reports confirm compliance with best security practice.

4.3. Usability Requirements

ID #	Description	Rationale	Acceptance Criteria
NFR-007	The system's administrative interface must be user-friendly and intuitive,	Simplifies system management for the IT and Operations Teams.	Usability tests with the IT and Operations Teams

	allowing for easy management of network and server settings.		confirm that the interface is easy to use.

4.5. Maintainability

ID #	Description	Rationale	Acceptance Criteria
NFR-008	All system configurations and setups must be documented in a way that facilitates easy maintenance and future upgrades.	Ensures that the system can be maintained efficiently over time.	Maintenance tasks are performed successfully using the provided documentation.

4.6. Compliance Requirements

ID #	Description	Rationale	Acceptance Criteria
NFR-009	The system must adhere to relevant cybersecurity standards and data protection regulations.	Ensures legal and regulatory compliance.	Compliance checks confirm adherence to applicable regulations (e.g. GDPR, Australian Privacy Act).

5. Assumptions and Constraints

5.1. Project Assumptions

- All necessary hardware components (e.g. Raspberry Pis, network switches) will be available for procurement within the planned timeline.
- The cloud infrastructure (web server and SIEM) will remain stable and accessible throughout the project.
- Residential users will not interfere with the business network or security configurations
- Key project personnel will be available as scheduled to complete their assigned tasks.

5.2. Time Constraints

- The project must be completed within the 3-month timeline, with specific milestones being met on time to ensure overall project success.

5.3. Budget Constraints

- The project is limited by a fixed budget for hardware, software, and personnel costs.

5.4. Resource Constraints

- Limited availability of personnel, which may affect the scheduling of certain tasks.

6. Dependencies

- The completion of the network configuration depends on the setup of the Raspberry Pi devices and the ISP modem in bridged mode.
- The installation and configuration of the SIEM is dependent on the setup of the on-premises network.
- The installation and configuration of Mautic is dependent on the setup of the Rapsberry Pi server.
- Security testing and configurations depend on the successful setup of the network and server infrastructure.

7. Requirements Traceability Matrix

This table maps each requirement to its source, related requirements, and the specific test case(s) that will verify it. This ensures that all requirements are tracked throughout the project lifecycle.

ID #	Req. Description	Source	Dependencies	Test Case(s)	Status
FR-001	The ISP modem must be setup and configured.		None	TC-001	Pending
FR-002	The LAMP stack must be installed and configured on a Raspberry Pi to host the business website.		FR-001	TC-002	Pending
FR-003	A cloud-based web server must be set up to provide hosting for client websites.		FR-001	TC-003	Pending
FR-004	The Raspberry Pi firewall must be configured with predefined security rules to filter inbound and outbound traffic.		FR-001	TC-004	Pending
FR-005	The Raspberry Pi router must be configured to allow Internet access through an ISP modem in bridged mode.		FR-001	TC-005	Pending
FR-006	The Raspberry Pi wireless access point must be configured to allow Internet access to business and residential users.		FR-005	TC-006	Pending
FR-007	The network needs to be assembled to complete the lab.		FR-001, FR-002, FR-003, FR-004, FR-005, FR-006	TC-007	Pending
FR-008	The cloud-based SIEM system must be configured to monitor and collect logs from the on-premises network.		FR-004, FR-007	TC-008	Pending
FR-009	Mautic is installed and configured to run automated emails and email campaigns.		FR-002	TC-009	Pending
FR-010	Regular backups of the web servers and Mautic data must be scheduled and stored securely.		FR-002, FR-003	TC-010	Pending
FR-011	User access controls must be implemented to		FR-002, FR-003, FR-007	TC-011	Pending

	restrict access to network devices and the web server based on role and necessity.				
FR-012	Comprehensive documentation for the installation, setup, and maintenance of all network components, servers, and software must be created.		FR-001, FR-002, FR-003, FR-004, FR-005, FR-006, FR-007, FR-008, FR-009, FR-010, FR-011	TC-012	Pending
FR-013	User-friendly operating manuals must be created for staff training on the new infrastructure.		FR-001, FR-002, FR-003, FR-004, FR-005, FR-006, FR-007, FR-008, FR-009, FR-010, FR-0011	TC-013	Pending
NFR-001	The on-premises network must support a minimum throughput of 100Mbps for business-critical services.		FR-001, FR-002, FR-003, FR-004, FR-005, FR-006, FR-007, FR-008, FR-009, FR-010, FR-0011	TC-014	Pending
NFR-002	The LAMP stack web servers must handle at least 50 concurrent connections with a response time of no more than 500 milliseconds.		FR-001, FR-002, FR-003	TC-015	Pending
NFR-003	The on-premises network must maintain a minimum uptime of 99.9% for business-critical services.		FR-001, FR-002, FR-003, FR-004, FR-005, FR-006, FR-007, FR-008, FR-009, FR-010, FR-0011	TC-016	Pending
NFR-004	The cloud-based web server must provide failover support to ensure continuity of service during on-premises outages.		FR-001, FR-002, FR-003	TC-017	Pending
NFR-005	All data transmitted between the on-premises network and the cloud must be encrypted using TLS 1.2 or higher.		FR-001, FR-002, FR-003, FR-004, FR-005, FR-006, FR-007, FR-008, FR-009, FR-010, FR-0011	TC-018	Pending
NFR-006	The system must undergo regular security audits and vulnerability assessments.		FR-001, FR-002, FR-003, FR-004, FR-005, FR-006, FR-007, FR-008,	TC-019	Pending

			FR-009, FR-010, FR-0011		
NFR-007	The system's administrative interface must be user-friendly and intuitive, allowing for easy management of network and server settings.		FR-001, FR-002, FR-003, FR-004, FR-005, FR-006, FR-007, FR-008, FR-009, FR-010, FR-0011	TC-020	Pending
NFR-008	All system configurations and setups must be documented in a way that facilitates easy maintenance and future upgrades.		FR-001, FR-002, FR-003, FR-004, FR-005, FR-006, FR-007, FR-008, FR-009, FR-010, FR-011, FR-012, FR-013	TC-021	Pending
NFR-009	The system must adhere to relevant cybersecurity standards and data protection regulations.		FR-001, FR-002, FR-003, FR-004, FR-005, FR-006, FR-007, FR-008, FR-009, FR-010, FR-011, FR-012, FR-013	TC-022	Pending

9. Approval and Sign-Off

[Agreement between project manager acknowledging and accepting the assignment, and any stakeholders.]

Project Manager:

Brendan Gasparin

X _____

(Signature)

X _____

(Date)

Premises Owner:

[redacted]

X _____

(Signature)

X _____

(Date)

Premises Owner:

[redacted]

X _____

(Signature)

X _____

(Date)