Configuration Manual

MSc Research Project
MSc Cyber Security

Muhammad Usman Sarafarz
Student ID: X23160667

School of Computing
National College of Ireland

Supervisor: Liam McCabe

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. **Muhammad Usman Sarafarz** ……………………

Student ID: **X23160667** ……………………

Programme: **MSc Cyber Security** …………… **Year:** **2023** ……….

Module: **Thesis** ……………………

Lecturer: **Liam McCabe** ……………………

Submission Due Date: **12/10/2024** ……………………

Project Title: **Enhancing Real-Time Threat Detection In Data Centre Firewalls Through Deep Learning & Machine Learning Techniques** ……………………

Word Count: **2500** …………… **Page Count:** **5 Pages** ……………

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: **Muhammad Usman Sarfaraz** ……………………

Date: **12/10/2024** ……………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Muhammad Usman Sarfaraz
Student ID: X23160667

1 Introduction

This comprehensive configuration manual will guide you through installing, configuring, and managing a network firewall system. It is designed to equip system administrators, network engineers, and IT specialists with the knowledge and skills to set up the firewall and implement configuration best practices effectively. By following this manual, you will be well-prepared to ensure maximum protection against potential threats and risks. It also covers the installation and configuration, including basic and advanced firewall manipulation techniques. It targets an audience that already knows about network security and has a minimum of experience with network equipment and software.

As a guideline, the reader is advised to go through the prerequisites and systems requirements, which are essential for the solution's configuration. It was established earlier that this manual is useful in helping an organisation acquire a more secure and strong network platform that will be able to address network threats.

2 System overview

2.1 Architecture

The network firewall system is designed with a flexible architecture that adapts to your organisation's needs. It can be best described as layered in terms of its hardware and software, which are integrated to enhance the entire system's security. The architecture constitutes a perimeter firewall that monitors and filters incoming and outgoing traffic based on the security parameters set. Internal firewalls are also implemented in the organisational internal network to prevent internal threats to reaching confidential information and other important organisational assets. The system also includes intrusion detection and prevention systems (IDPS) to detect and prevent potential security threats as they are being executed. The build and structure of the system are malleable, allowing you to organically add to existing network structures and further develop the system as needed.

2.2 Hardware & Software requirements

The technical requirements of the hardware and software used in the network firewall system are selected to deliver the best and most reliable results achieved in the paper. A high-performance network firewall appliance with at least a 2-core CPU and preferably with a multiple-core processor. The need to have a 5 GHz clock speed to meet the required processing when filtering and efficiently inspecting the networks in real time cannot be understated. The minimum 8 GB of RAM is enough to supply the firewall software and any extra security programs with enough memory; the 500 GB SSD guarantees enough storage for the logs, configurations, and updates for fast and efficient read/write and data access. Multiple network connections and segments are made possible by at least four Gigabit Ethernet ports, which improve the defined traffic flow and increase the system's security by creating different network layers. The chassis unit must have a redundant power supply since power failures are inevitable, and without protection, availability is doomed to suffer significant downtime.

On the software side, it is suggested that a Linux-based firewall operating system like pfSense or IPFire be used due to its efficiency, security functions, and many supporters. The availability of the latest release of the selected firewall software enables one to defend against current threats, which tend to be more frequent and sophisticated. A web-based management console to administratively configure and manage the firewall is the most convenient feature available in this firewall. Information logging and monitoring technologies are primary instruments for security occurrences and system function tracking, aiming to assess threats immediately. Integrating IDPS software with anti-virus software is useful because the former works proactively by recognising and preventing threats as they happen. Last but not least, VPN support is required for remote connectivity – a user can connect to the LAN securely from outside the organisation. Altogether, the listed hardware and software components provide consistent, effective, and secure firewall solutions that safeguard the network from cyber threats.

Component	Specification
Firewall Appliance	High-performance network firewall appliance
Processor	Multi-core CPU with at least 2.5 GHz clock speed
Memory	Minimum 8 GB RAM
Storage	Minimum 500 GB SSD
Network Interfaces	At least 4 Gigabit Ethernet ports
Power Supply	Redundant power supply for high availability
Operating System	Linux-based firewall OS (e.g., pfSense, IPFire)
Firewall Software	Latest stable release of the chosen firewall software
Management Console	Web-based management interface
Logging and Monitoring	Integrated logging and monitoring tools
IDPS Software	Intrusion Detection and Prevention System (IDPS) software
VPN Support	Virtual Private Network (VPN) support for secure remote access

3 Installation

3.1 Pre-installation

As much as installing the network firewall system is necessary, a few prerequisites must be fulfilled before starting the process. First, ensure that all the specified electrical and computing assembly elements, such as the firewall appliance, processor, memory, storage, network connections, and power, meet the company's standards. Ensure the hardware is also well configured and interconnected in the network platform. It is also necessary to acquire the updated version of the chosen Linux-based firewall operating system and required elements, including IDPS and VPN support tools. Save the current network configuration and data before proceeding with the installation in case anything is lost. Furthermore, examine the organization's network security policy to understand how the Firewall settings should be to meet the organisation's security regimes.

3.2 Installation procedure

The defining installation process encompasses the following steps that will enable the implementation of the firewall system. Starting with this operating system, you must introduce the Linux-based firewall operating system to the specific firewall appliance. This is usually done by starting the computer from an installation media like a USB disk or CD and following on-screen instructions to finish the process. After the installation of the operating system, go on to install the firewall software; use the current stable version. The firewall interface address, subnet masks, and default gateways are basic network settings that must be designed.

After that, configure the management console so firefighters can manage and monitor the firewall over the Internet. This step involves specifying users' rights, creating system, operator and other administrative user accounts, and setting up passwords. Integrating and setting up the Intrusion Detection and Prevention System (IDPS) to strengthen the firewall's defence is also recommended. Ensure that the IDPS is well configured with the firewall application it is coordinated with and that the different characteristics of the IDPS to maintain alert for network packets and be ready to handle threats as and when they arise are correctly configured. Then, set up a VPN to secure connections with the network, even if made remotely. This entails establishing the VPN server properties, defining users, and distributing User Connect Scripts to only those with permission to access the VPN.

3.3 Model integration with firewall

Originally, the firewall, in particular, required an upgrade by installing the exported trained machine learning model and the firewall. This procedure usually ranges from several steps. First, preparing the environment will require the right machine-learning environment installed on the firewall appliance. This may include other sub-dependencies like Python, TensorFlow if the model requires it or PyTorch, among others. After that, the trained model file can be safely copied to the firewall appliance through secure means, such as SCP or SFTP. When transferred, use the model by copying it to the proper directory so that the firewall software can reach it. Prepare the model’s path for evaluation in the firewall and incorporate it into the threat detection process. Last but not least, set up the options for machine learning within the firewall software that relate to the steps taken to apply the model and the patterns it should look for in the network traffic.

The load balancer becomes integrated into the system to solve the problem of an overload of the firewall. This way, the load balancer will share the connection and traffic loads going through the network among the several firewalls so that no firewall gets overwhelmed with loads of connections coming through the network. The framework of the integration process is as follows: First, you can choose probably one of the most used software load balancer solutions, which is HA-Proxy or NGINX, or you can consider a hardware load balancer. To implement the selected load balancer, one is supposed to run the software on a dedicated appliance or a server as prescribed by the installation guidelines of the software in question. After installation, you need to set the load balancer to accept incoming connections, properly direct the connections to the available firewalls, and configure checkpoints or health checks to verify the health status of the firewalls in order not to send traffic to a sick instance. Finally, change the network setting in the traffic flow path so that all the traffic is directed to the load balancer before being sent to the firewalls. This setup means that the firewall and the related operations are balanced in the procedure, and it remains a secure work for the network.

3.4 Post-installation

Following the installation procedure, several tests and settings shall be done to ensure that the firewall system functions correctly and has optimal functionality. First, one should do a system test and ensure that all the system's perceived components are functioning correctly. This includes verifying the network connection, firewall configurations, IDPS features, and VPN connectivity. Check and enhance the firewall settings to meet the organisation’s security policy requirements and ensure all the required rules and policies exist.

Moreover, logging and monitoring devices should be set up for system performance and security occurrences. This involves putting in place the policies and disparities of the retention of the log, defining the alert thresholds, and archiving and researching the logs. Attend a security audit that would potentially check for the drawbacks or loopholes in the firewall settings. Last, configuration records should be made, including settings, users placed on the system, and the security policies set for the system in case of future support and repair. Thus, the outlined steps will help administrators establish the network firewall system and achieve the proper security level for the network and its devices.

4 Configuration

4.1 Initial Configuration

Subsequently, the first stage of the network firewall system can be implemented for use and must be set up to correspond to the organizational security policies. First, launch your Hitachi digital platform's secure web-based management console. Using the account created during installation, log in to the Third–Party Management portal using the administrative account. The first process of configuring is the network interface setup. Type the correct IP addresses, subnet masks, and gateway for each interface assigned according to the network's design layout. Configuring routing on the default gateway is necessary so that every packet goes through the firewall.

4.2 Advanced Configuration

Secured configuration focuses on the creation of intricate security measures and parameters as a way of enhancing the protection of the network. The first step is to set up rules for the firewall concerning incoming and outgoing traffic. These rules should determine which types of traffic are allowed or denied based on conditions like a source IP address, destination IP address, ports, and protocol. Activate rules for NAT, if necessary, for internal organization of the IP addresses and to have an external connection. Set up IDPS according to the possible threats that may occur and monitor the system to prevent them. This would require defining rule sets to alert the system of improper actions. Appropriate measures, such as notifying the administrators or filtering the traffic, should be taken when a threat is detected. Ensure there are records of all events and possible threats to enhance the visibility of all actions. Define log retention policy to define rules for when and how long logs should be saved and when they should be deleted.

4.3 Integrating the Trained Model

To incorporate the trained machine learning model with the firewall, go to the firewall management console's model configuration space. Enter the model file's path and ensure the firewall software you use can locate it.

The choices made regarding model settings define how and when this model will be used to analysis traffic in the given network. This often requires specifying the level of deviation that would be considered abnormal and defining the actions to be taken about the detected threats.

4.4 Load Balancer Configuration

Set up the load balancing pattern to generate traffic correctly in multiple firewall instances. Login to the management interface of the load balancer and configure the backend servers, commonly referred to as the firewall instances. It is necessary to organise health checks to determine the status of each firewall and block traffic to non-functioning instances. Set rules for load balancing to ensure traffic is well distributed, whereby the options include using round-robin and least connection. Last, change the network configuration to forward all traffic to the load balancer, enabling them to balance traffic loads in the network.

5 Glossary

1. Firewall: An organisation security system responsible for implementing and maintaining security rules defining what is allowed to enter and exit through a network.
2. IDPS is an intrusion detection and prevention system that scans the network's traffic and attempts to prohibit intrusion.
3. NAT: Network Address Translation is a technique used to convert an internal IP address privately to an external IP address.
4. VPN: A Virtual Private Network is a procedure that lets an individual or two or more devices communicate securely over the Internet.
5. Load Balancer: A load-balancing device regulates a network's traffic so as not to overload individual servers or firewalls.

5.1 Acronyms

a. ACL: Access Control List
b. CPU: Central Processing Unit
c. GB: Gigabyte
d. IDPS: Intrusion Detection and Prevention System
e. IP: Internet Protocol
f. NAT: Network Address Translation
g. OS: Operating System
h. RAM: Random Access Memory
i. SCP: Secure Copy Protocol
j. SFTP: Secure File Transfer Protocol
k. SSD: Solid State Drive
l. TCP: Transmission Control Protocol
m. UDP: User Datagram Protocol
n. VPN: Virtual Private Network

6 References

Netgate. (n.d.). pfSense documentation. Netgate. https://docs.netgate.com/pfsense/en/latest/
IPFire. (n.d.). Firewall configuration documentation. IPFire. https://www.ipfire.org/docs/configuration/firewall
TensorFlow. (n.d.). TensorFlow tutorials. TensorFlow. https://www.tensorflow.org/tutorials
Canonical Ltd. (n.d.). Ubuntu Server documentation. Ubuntu. https://ubuntu.com/server/docs