

SoAC Project Proposal

by Abdullah Azhar Cassim

Submission date: 19-Oct-2023 08:45PM (UTC+0100)

Submission ID: 213732973

File name: 50548_Abdullah_Azhar_Cassim_SoAC_Project_Proposal_508662_723271255.docx (35.79K)

Word count: 2456

Character count: 14431

Firewall Configuration and Optimization

Research Proposal

Abdullah Azhar Cassim

Munyaradzi Nicholas Murira

2332

Contents

Contents

Contents.....	2
Figures.....	3
Tables.....	3
1. Introduction	4
2. Background to the Proposed Research.....	5
3. Aims & Objectives	7
4. Methodology.....	8
4.1 Research Methodology	8
4.1.1 Philosophy.....	8
4.1.2 Approach.....	8
4.1.3 Strategies	8
4.1.4 Risks & Limitations	8
4.1.5 Ethical Issues	9
4.1.6 Validity, Reliability & Generalisability.....	9
4.1.7 Data Evaluation Methods	9
4.2 Development Methodology.....	10
4.2.1 Software Development Methodology OR Other Relevant Major Methodology.....	10
5 Resources and Planning	11
5.1 Hardware Resources	11
5.2 Software Resources	11
5.3 (Optional) Information Resources	11
5.4 (Optional) Human Resources	11
5.5 Project Plan	11
6. Reference List.....	12
References	12

Figures

Tables

1. Introduction

This project's context mainly involves setting up a firewall and testing it under different configurations. There is no industrial partner in this project. Me having done an HND in Network Engineering and now a 3rd year direct entry into the cyber security and computer networks degree here at UWTSD, I figured this project is the perfect combination of both networking and cyber security, my current skillset would be enough to configure a basic firewall, this project would encourage me to dive deeper into ethical hacking and other security aspects. Ultimately this project is aligned to my future career goals.



2. Background to the Proposed Research

The need for network security is constantly increasing, as there is a growing demand for measures to prevent attacks, data loss, and any kind of threat. Firewalls play a role, in ensuring network security by preventing cyber-attacks safeguarding valuable data and upholding the privacy and integrity of computer systems and networks. [1]

Firewalls, commonly referred to as Packet Filter Firewalls or first-generation firewalls have been around since 1987. Their primary purpose is to regulate the flow of connections by examining network and transport layer protocol details. Initially these firewalls proved effective, in safeguarding against access, by blocking IP addresses and port numbers. However, as the internet evolved and advanced web applications emerged it became evident that these traditional firewalls had limitations in coping with the network landscape. [2]

Whereas the New Generation Firewall's (NGFW), which were initially introduced by Palo Alto Networks in 2010 are an upgraded version of firewall technologies. They come with capabilities that primarily focus on packet inspection. Deep packet inspection involves the ability of the network technology solution to analyse the underlying layers of traffic that are transmitted over transport layer protocols. NGFWs include all the functions found in firewalls, like packet filtering, network and port address translation (NAT) stateful inspection and support for virtual private networks (VPN). However, they also offer features such as identifying applications at high-speed detecting anomalies and the capability, to decrypt and re encrypt SSL traffic. [2] [3]

When comparing firewalls to NGFWs we can identify key distinctions. Traditional firewalls offer protection based on ports, state and protocols. They filter traffic according to set rules. On the hand NGFWs have the ability to recognize applications irrespective of port, protocol, evasive tactics or SSL encryption. They provide real time defence, against zero-day attacks. Can collaborate with user roles to restrict access within an organization. NGFWs outperform firewalls in detecting and preventing attacks due, to their nature. This allows them to thoroughly examine connection requests by comparing them with established connections characteristics. Consequently they are able to detect requests even if they are structured differently or originate from computers. [1] [4] [5]

For this project I have selected the NGFW to be the Cisco Adaptive Security Appliances (ASA) 5500 firewall, but Cisco has announced the end-of-life and end-of-sale notices for the Cisco ASA 5500 series since there were multiple vulnerabilities found and published in 2012. Due to the limitations in resources the only firewall available in the university lab were the ASA 5500 series firewall. Now the firewall itself is a network device that offers strong defence against different types of cyber threats. Numerous research papers, case studies and technical documents delve into the performance, setup and security capabilities of this firewall regardless of the minor vulnerabilities that were found later. [6]

According to Cisco there were multiple vulnerabilities that were found in the ASA firewalls. One of them was the "DHCP Memory Allocation Denial of Service Vulnerability". DHCP is a protocol that automatically configures settings for devices, such, as an IP address, subnet mask, default gateway, DNS server and WINS server IP address. The Cisco ASA Software has the capability to act as a server or a DHCP client. When functioning as a server the Cisco ASA Software provides network configuration settings to clients. However there is a flaw in the implementation of the Dynamic Host Configuration Protocol (DHCP) Server feature. This vulnerability could be exploited by an attacker leading to a reboot of the affected device. The vulnerability occurs due to memory allocation, for a

DHCP data structure when receiving manipulated DHCP packets. To exploit this vulnerability an attacker can send manipulated packets to the targeted system. If either feature is enabled on the Cisco ASA Software there is potential for this vulnerability to be present. [6]

At the Cyprus University of Technology there was a case study that showcased how the Cisco ASA 5500 series firewall was utilized. The purpose of implementing this firewall was to ensure the security and safety of both students and staff members. This case study effectively demonstrated how this device proved to be beneficial, in an environment. [6] Apart, from the case study mentioned earlier Cisco offers a manual on how to monitor and resolve performance related problems, with the Cisco Adaptive Security Appliance (ASA) 5500 series firewall. The manual states commands that help the user in monitoring the firewalls performance and troubleshooting any issues that might occur. [7]

In conclusion although the Cisco ASA 5500 series firewall may not be the choice, for industry applications due to its performance limitations and the availability of advanced alternatives it still holds value as a tool for learning and experimentation in my final year project. Its wide range of configuration options and robust set of features make it an excellent firewall to test and understand how firewalls operate and grasp network security principles. Additionally conducting penetration testing on the ASA 5500 series can offer insights, into the process of identifying and exploiting vulnerabilities. Furthermore studying known vulnerabilities can serve as practical case studies to gain an understanding of security issues and effective ways to address them.

Keywords: (NGFW: New Generation Firewall), (NAT: Network and port Address Translation), (SSL: Secure Sockets Layer), (ASA: Adaptive Security Appliances).

3. Aims & Objectives

- Basic firewall configuration.
- Set up ACL's and security policies.
- Network Integration and Test.
- Monitoring/ Analyse traffic for optimization.
- Clear documentation of all the above work.

4. Methodology

4.1 Research Methodology

Configuring a firewall and testing seems easy said than done, first a lot of planning would be needed to be done along with set requirements and the final expectations. Configuration of the firewall would be the next step, this includes the essential configurations including hostname, passwords, management interfaces, defining security policies, access control rules and user authentication methods. Next would be integrating the firewall into the lab environment along with Network Address Translation rules for internal and external traffic for proper connectivity. Following up with thorough testing of security policies and access controls using test scenarios, simulated attacks and real traffic. Thereafter I'd have to set up and use different monitoring tools for logging and alerting to capture firewall events and anomalies, preferably using different tools to see the difference in results and maybe compare them. All the while creating a detailed documentation that includes network diagrams, configuration files and testing results to conclude.

4.1.1 Philosophy

For this project I'll be using a Positivist philosophy, since this is an experiment with the collection of quantitative data I believe it can benefit from a positivist philosophy approach. For example, the network traffic patterns, data transfer rates, the number of rules, access control lists or firewall policies, all these provide objective, numerical data that can show a clear insight into the firewall's performance and under different configurations its effectiveness.

4.1.2 Approach

For this project I have decided on a deductive approach, a deductive approach would provide me with a structured and rigorous framework to conduct the controlled experiments in testing the specific hypotheses. It would also allow me to be efficient by helping me to focus research efforts on the most important parts of the firewall and test accordingly with the specific configurations. Since deductive approach aligns with the evidence available, it would make it easier to draw valid conclusions.

4.1.3 Strategies

4.1.3.1 Literature Review

4.1.3.2 <Strategy 2>

4.1.3.3 <Strategy 3>

4.1.4 Risks & Limitations

Risks:

- Misconfigurations. Human errors may lead to an ineffective firewall or sometimes security vulnerabilities.
- Inadequate testing. Vulnerabilities may go undetected if the firewall isn't thoroughly tested in a number of scenarios.
- Resource constraints like in a lab environment resource limitations may affect the realism of the tests, the lab setup would not fully replicate the complexity of a real world network

- False Positives or Negatives. Intrusion detection and prevention systems might generate false positives/negatives which would be ineffective.
- Lack of real world threats which would also affect the accuracy of security assessments.

Limitations:

- A lab environment may not scale well enough to emulate a large network like in real life.
- Time constraints. Lab testing would be time consuming and it won't be possible to replicate all the real world threat scenarios.
- Lab environment would lack the diversity of devices and software that would be found in the real world networks which would limit my testing coverage.

To mitigate these risks, I would have to take a step by step and cautious approach while conducting thorough testing while maintaining proper documentation. Additionally I would have to invite third party penetration testers to get valuable insights into the security and effectiveness of the firewall configuration.

4.1.5 Ethical Issues

No ethical issues since the project would be carried out under a controlled lab environment

4.1.6 Validity, Reliability & Generalisability

4.1.6.1 Validity

Ultimately it depends on how it's aligned with the network objectives, supported by comprehensive documentation of configurations, test results and findings.

4.1.6.2 Reliability

It comes down to how the lab environment is reproduced, if it is consistent and well controlled with no big changes or variations even with the testing scenarios it's more likely that the obtained results would be similar.

4.1.6.3 Generalisability

The end results from my project could be valuable to similar problems that involve firewall configuration and security testing in lab environments. If for example an organization decides to configure and test the Cisco ASA 5500 firewall. In regard to data sets, if the results that I obtain have similar data characteristics, the data might be applicable to a company or projects that involve testing the Cisco ASA 5500 firewall's performance under different configurations.

4.1.7 Data Evaluation Methods

4.1.7.1 Data Collection

- Configuration data: CLI commands during the initial firewall configurations, network layout, IP addresses, routing tables and VLAN configurations
- Test Data: Captures of network traffic logs, packet flow analysis, intrusion attempt logs, anomalies and other security events that would be detected by the firewall.
- Security Policy Data: Services that are allowed/denied by the firewall, applications that are blocked or permitted by the firewall, login information's.

4.1.7.2 Data Evaluation

- Configuration data: Document the firewall configuration commands using screenshots of the CLI, network layout documented on a network diagram. IP addresses and routing tables would be stored and displayed on a table.
- Test Data: For incoming/outgoing network traffic, intrusion logs and intrusion attempts techniques like data clustering or anomaly detection can be implemented to identify unusual patterns in the network traffic

Some hypotheses for this project could be:

- Testing the firewall against DDoS attacks- "As the volume of the attack traffic increases, the firewall's ability to handle DDoS attacks will decrease"
- Testing the firewall to detect and prevent intrusion: "the ability to detect and prevent intrusion attempts would increase with the complexity of the intrusion attempt"

4.2 Development Methodology

4.2.1 Software Development Methodology OR Other Relevant Major Methodology

1. Project Planning: identifying the timeline/ configurations to be tested/ testing scenarios/ identifying resources.
2. Preparing and Firewall Configuration: Setting up lab environment/ network topology and end devices.
3. Test scenario planning: A set of test scenarios that are close to real-world threats.
4. Data collection: Firewall logs/ Network traffic.
5. Testing and performance evaluation: Test the firewall with different types of real world attacks and collect the data on firewall performance metrics, security incidents and vulnerabilities detected.
6. Data analysis: Analyse the collected data to understand the firewall's performance and security effectiveness using tools and monitoring software's like SIEM tools, wireshark for traffic analysis, etc.
7. Documentation: A comprehensive documentation of the above steps.

5 Resources and Planning

5.1 Hardware Resources

- Cisco ASA 5500 Firewall.
- Cisco switches/ routers.
- Workstations.
- Cables.

5.2 Software Resources

- Cisco ASDM: firewall configuration management software.
- Wireshark: Network traffic analyser.
- iPerf / D-ITG: To generate network traffic patterns.
- Nessus: To perform vulnerability assessments/ security weakness.
- Virtualbox: when working with virtualized firewall instances.
- Nmap/ Metasploit and other security assessment tools: Specialized tools to conduct pen testing/ firewall testing.

5.3 (Optional) Information Resources

If you need external data for your project, where will that data come from?

5.4 (Optional) Human Resources

- Third party pen tester to get insights from another perspective and perhaps uncover more vulnerabilities.

5.5 Project Plan

6. Reference List

References

- [1] M. K. Kumawat, "Traditional Firewall vs Next Generation Firewall (NGF)," *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, vol. 5, no. 2, p. 5, 2021.
- [2] J. Heino, A. Hakkala and S. Virtanen, "Study of methods for endpoint aware inspection in a next generation firewall," *Cybersecurity*, vol. 5, no. 1, p. 25, 2022.
- [3] J. Surana, K. Singh, N. Bairagi, N. Mehto and N. Jaiswal, "Survey on Next Generation Firewall," *Information Technology*, vol. 5, no. 2, p. 5, 2017.
- [4] A. Makhdoomi, N. Jan, P. and N. Goel, "Conventional and next generation firewalls in network security and its applications," in *International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Greater Noida, India, 2022.
- [5] J. Metzler, "The Next Generation Firewall The policy and Security Control Point," *Kubernan*, vol. 1, no. 6, p. 6, 2007.
- [6] "Multiple Vulnerabilities in Cisco ASA 5500 Series Adaptive Security Appliances and Cisco Catalyst 6500 Series ASA Services Module," Cisco, 10 10 2012. [Online]. Available: <https://www.cisco.com/c/dam/en/us/support/docs/csa/cisco-sa-20121010-asa.html>. [Accessed 2023 10 19].
- [7] "Cyprus - Customer Story - Services (CX)," Cisco, 10 07 2023. [Online]. Available: https://www.cisco.com/c/m/en_us/customer-experience/customer-stories/cyprus.html. [Accessed 19 10 2023].
- [8] "Cisco ASA 5500-X Series Firewalls - Configuration Examples and TechNotes," Cisco, 22 11 2015. [Online]. Available: <https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-configuration-examples-list.html>. [Accessed 19 10 2023].

SoAC Project Proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

65/100

PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT

Student [2306801](#)(Abdullah Azhar Cassim).
Mark **65**

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project	20	13
- Objectives Not SAMRT		
- The introduction could be improved by providing a more compelling opening statement or anecdote to draw readers in. It should also mention the project's significance in the		

broader context of cybersecurity.		
Background to the Project / Literature Review (400 words)		
Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8 journal papers and book chapters rather than just websites; Selection of relevant models & concepts - The section references relevant literature, such as the case study at Cyprus University of Technology and Cisco's documentation, to support the choice of the ASA 5500 series firewall. This adds credibility to the project. - While the background is informative, it could benefit from a more critical analysis of the state of the field and how this project fits into existing research. Additionally, the section could be more concise.	20	14
Project Design (500 words)		
Clear statement of which development methods are to be used and why	30	20

they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will be analysed - To improve, the author should provide more detailed hypotheses and scenarios they plan to test. This will make it clear how the project contributes to the field of network security. The Aim and Objectives are lacking - While it's a common approach, the specific experiments and hypotheses are not detailed, making it difficult to assess the novelty.		
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices - The section could be improved by explaining why each resource is chosen and how it contributes to the project. Additionally, it could include a	15	8

timeline or project plan for better project management.		
Document Presentation		
Correct spelling, grammar and punctuation; Flow of narrative/fluency; Coherence; Word processed; Correct use of referencing with bibliography; Strict word limit - While it's clear and coherent, there's room for improvement in the narrative's flow. The structure could be optimized to make the document more reader-friendly. Additionally, the section labeled "Strategies" under the research methodology is incomplete and should be elaborated upon.	15	10
TOTAL	100	65

PAGE 1
PAGE 2
PAGE 3
PAGE 4



Comment 1

no comment

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12
