

Proposal

by Faiz Khalid Khan

Submission date: 21-Oct-2024 01:27PM (UTC+0100)

Submission ID: 240762088

File name: 58091_Faiz_Khan_Proposal_586419_2050981499.docx (42.89K)

Word count: 1539

Character count: 9240

Test-bed security utilities Firewalls and ACLs

Research Proposal

Faiz Khan 2221958

1.introduction.....	3
2.Background to the Proposed Research.....	3
3.research Problem Statement	5
4.research Aim & Objectives	5
5. Methodology	5
5.1 Methods	5
5.2 Materials.....	6
6.Project Plan	6
7.References.....	6
Bibliography	6

1.introduction

Network security is a critical concern in today's digital world, where cyber threats are rapidly increasing. Business organizations are relying on various security services such as firewalls and Access Control Lists ACLs to protect their network frameworks. The firewalls will act as a barrier which will control the flow of data traffic based on pre-defined security rules. While Access Control Lists offer a more infiltrated control by managing access at the router and switches levels based on IP addresses, ports and protocols. [1]" As stated by Daniele Brighenti he says, that their main limitation is that they cannot configure Firewalls from scratch, since they are approaches for fixing firewall misconfigurations. For this reason, they do not achieve full automation, but they require that someone provides and initial rule set." So, this text shows that firewalls will have to be maintained by the administrator and require somebody to control them.

[2]" As stated by Yamini Kannan she says, However, their effectiveness relies heavily on the correct ordering of rules within the list, prudent placement on the network, and ongoing management of the ACL Itself. In conclusion, ACLs play a pivotal role in managing and securing networks access." So, this shows that ACLs will also have to be managed so they can secure the network by shielding against DDos attacks. By inspecting both Firewalls and ACLs, the project will supply relative investigations of their performance, ease of use and usefulness for various network frameworks. Similar understanding is important for network administrators looking to enhance their security configuration while reducing the risks for networking threats. [3] "As stated by Michael Alicea and Izzat Alsmadi they say, that Since Networks are much larger and have many more devices and services than in the past, a firewall rule list is much larger on average. There is also now the consideration that there are several firewalls on a network with anomaly detection needing to be checked between different components." Therefore, this shows firewall anomaly detection help administrators assess security risks and helps the devices to stay protected on the network.

2.Background to the Proposed Research

The field of network security has seen fast evolution in recent years. Standard Firewalls, which usually depend on packet filtering has advanced into more cultivated next generation firewalls which are able to do deep packet check-up and threat judgement integration. Likewise, ACLs have increased in size from simple IP-based filtering to more complex operations which serve various network domains, plus cloud and virtualized systems. [4] " As stated by Hanane Aznaoui and Canan Batur Sahin they say, the configuration of a firewall is more important than the

configuration of other computer systems.” This is because firewalls are a barrier to keep threats out of the network system and they protect the computer systems from any threats.

While both Firewalls and ACLs play a vital role in network security but there is little research comparing their success across different network planning. Previous Studies have focused essentially on independent performance benchmarks but have often abandoned a thorough view which reviews real world frameworks and effective network conditions. This testing will address this gap by designing a test bed which replicates many network conditions to balance these two systems.

The aim is to recognize certain configuration where each utility excels, therefore, assisting network administrators in designing well-informed decisions. [5]" As stated by Yamini Kannan she says that ACLs provide a first line defense against possible network security threats. By restricting network traffic flow, they can help stop threats from propagating within the network, thereby limiting potential damage." So, this shows that ACLs will stop threats from getting in the network which have sensitive information.

[6] "As stated by Yamini Kannan she says, Moreover, from a performance perspective, ACLs are boon as they help control the flow of unnecessary traffic, thereby optimizing overall network performance. By discarding unwanted traffic at the network's edge, ACLs reduce load on network devices deeper within the infrastructure, conserving valuable system resources and enhancing network efficiency." So, this shows that ACLs will provide instructions to the devices which will be connected to the network. ACLs will guide the devices which will allow traffic in the network. The other benefit of a ACLs is that it will prevent unwanted users and traffic from getting in a network. This will protect the network from getting attacked by unwanted users.

[7] "As stated by Yamini Kannan she says, that improperly configured ACLs can have severe implications. From a security standpoint, misconfigured ACLs can create vulnerabilities that attackers could exploit to gain unauthorized access to network resources, potentially leading to data theft or sabotage. A common exploit would be allowing traffic from untrusted sources, creating an opportunity for malicious entity to perform a network attack." So, this ACLs lists should be configured properly as if they are not configured properly then this can cause many issues like DDos attacks to the network or even data theft.

[8] "As stated by Michael Alicea and Izzat Alsmadi they say, an autonomous firewall would have to generate rules dynamically, based on traffic that it deems normal and traffic that it deems malicious. When adding a new rule into the existing ruleset, the device would have to ensure the new rule does not conflict with the existing ones." So, this shows that if the firewall rules that are set dynamically it could change conditions to the network like the time or traffic

in the network. The other thing the dynamic firewall could do is that it can give automatically add bad IP addresses to the devices. This could cause major issues to any organizations because the network administrator would have set up the static firewall and add IP address to all the devices.

3.research Problem Statement

This plan will address the challenges of directing the valid layout and usage of Firewalls and ACLs for different network frameworks. Particularly, it seeks to assess their advantages and identifies frameworks where one might surpass the other in terms of security performance and serviceability.

4.research Aim & Objectives

The Aim is to assess the advantages of Firewalls and ACLs in protecting networks by managing a relative analysis within a simulated environment.

- Developing a simulation/ test bed environment for carrying out testing's for Firewalls and ACLs.
- Investigate the performance of Firewalls and ACLs over multiple network frameworks.
- Analyze common misconfigurations and their effects on security.
- Laying out guidance for valid use cases and configurations established on findings.

5. Methodology

5.1 Methods

This project will engage an assessable research approach. Planning test practices to assess Firewalls and ACLs performance. The simulation environment will be set up in Cisco Packet Tracer concentrating on benchmarks like latency packet loss and output.

The testing plan is experimental, requiring a series of tests plans to simulate possible cyber threats and assess how each service responds. For the information analysis, statistical implements like Python will be used to exercise performance data and create relative insights. This approach is fitting given the need to quantify and investigate analytical data objectively.

5.2 Materials

The main data source will be simulated network traffic. As the software which will be used for testbed will be Cisco Packet Tracer, PfSense for Firewall execution and Python for data investigation. The ethical reflection for this project is minimum due to the use of simulated data. Therefore, data privacy and security measures will be maintained all round.

6. Project Plan

A present timeline for the projects covers:

- November – December 2024: Start off with the simulation environment and describe test frameworks.
- January – February 2025: The performance start tests and collects data on Firewalls and ACLs performance.
- March 2025: Looking at investigating data, completing the report, prepare for the presentation.
- April 2025: Complete and submit the project.

7. References

Bibliography

- [D. Bringhent, "Automated Firewall Configuration," IEEE Xplore, 17 March 2023. [Online].
1 Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9737389>. [Accessed
] Thursday 10/10/2024 2024].
- [Y. Kannan, "Access control list (ACL) Compliance Verification and Alarm Systems:
2 Strengthening Network Security," Authorea, 10 March 2024. [Online]. Available:
] <https://essopenarchive.org/doi/full/10.22541/au.171011477.72357180>. [Accessed Thursday
10/10/2024 2024].
- [M. A. a. I. Alsmadi, "Misconfiguration in Firewalls and Network Access Controls:," MDPI,
3 Saturday October 2021. [Online]. Available: <https://www.mdpi.com/1999-5903/13/11/283>.
] [Accessed Thursday October 2024].
- [H. A. a. C. B. Şahin, "A Virtual Data Center Comparison Of Different Firewalls' Performance,"
4 Journal of Avancement in Computing , Tuesday April 2023. [Online]. Available:
] <https://journalsriuf.com/index.php/JAC/article/view/46/61>. [Accessed Friday October
2024].
- [Y. Kannan, "Access control list (ACL) Compliance Verification and Alarm Systems:
5 Strengthening Network Security," Authorea , 10 March 2024. [Online]. Available:
] [https://d197for5662m48.cloudfront.net/documents/publicationstatus/199481/preprint_pdf
f/dc0a655e6f1ef537b031067c61004d67.pdf](https://d197for5662m48.cloudfront.net/documents/publicationstatus/199481/preprint_pdf/dc0a655e6f1ef537b031067c61004d67.pdf). [Accessed Friday October 2024].
- [Y. Kannan, "Access control list (ACL) Compliance Verification and Alarm Systems:
6 Strengthening Network Security," Authorea , Sunday March 2024. [Online]. Available:
] <https://essopenarchive.org/doi/full/10.22541/au.171011477.72357180>. [Accessed Friday
October 2024].
- [Y. Kannan, "Access control list (ACL) Compliance Verification and Alarm Systems:
7 Strengthening Network Security," Authorea , Sunday March 2024. [Online]. Available:
] <https://essopenarchive.org/doi/full/10.22541/au.171011477.72357180>. [Accessed Friday
October 2024].
- [M. A. a. I. Alsmadi, "Misconfiguration in Firewalls and Network Access Controls:," MDPI,
8 Saturday October 2021. [Online]. Available: [https://www.mdpi.com/1999-
\] 5903/13/11/283#B11-futureinternet-13-00283](https://www.mdpi.com/1999-5903/13/11/283#B11-futureinternet-13-00283). [Accessed Friday October 2024].

Proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

53/100

PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT

Student: Faiz Khan

Mark: 53

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 Introduction was mainly on ACL, it would be good to include firewall. The aim would need to be more focus.	20	12
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 It would be good to highlight some related work rather than discuss generically. Can	20	12

be improved.		
Ethical issues not discussed		
Project Design (500 words)		
Clear statement of which development methods are to be used and why 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 This was done but need to be improved, address briefly.	30	13
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices	15	7

No diagram provide, just bullet point stating period. A Gantt chart can improve this section.		
Document Presentation		
Correct spelling, grammar and punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with bibliography; Strict word limit Writing style and presentation can be improved. Be consistent with your formatting.	15	9
TOTAL	100	53

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5
