MAINTAINING THE INTEGRITY OF EFFECTIVE COMMUNICTION BASED ON PROXY FIREWALL

PHASE 1 REPORT

Submitted by

PRAVEENKUMAR A (RCAS2021MCS210)

in partial fulfillment for the award of the degree of

MASTER OF SCIENCE
SPECIALIZATION IN
INFORMATION SECUIRTY AND CYBER FORENSICS

DEPARTMENT OF COMPUTER SCIENCE

RATHINAM COLLEGE OF ARTS AND SCIENCE

(AUTONOMOUS)

COIMBATORE - 641021 (INDIA)

DECEMBER-2022

RATHINAM COLLEGE OF ARTS AND SCIENCE
(AUTONOMOUS)
COIMBATORE - 641021

BONAFIDE CERTIFICATE

This is to certify that the Phase I Report entitled **MAINTAINING THE INTEGRITY OF EFFECTIVE COMMUNICTION BASED ON PROXY FIREWALL** submitted by **PRAVEENKUMAR A** , for the Degree of Master in Computer Science specialization in **"INFORMATION SECUIRTY AND CYBER FORENSICS"** is a bonafide record of the work carried out by him/her under my guidance and supervision at Rathinam College of Arts and Science, Coimbatore

Dr.Mohamed Mallick
Supervisor

Mr.P.Sivaprakash
Mentor

Submitted for the University Examination held on 02.12.2022

INTERNAL EXAMINER

EXTERNAL EXAMINER

RATHINAM COLLEGE OF ARTS AND SCIENCE

(AUTONOMOUS)

COIMBATORE - 641021

DECLARATION

I, **PRAVEENKUMAR A** , hereby declare that this Phase I Report entitled **" MAINTAINING THE INTEGRITY OF EFFECTIVE COMMUNICTION BASED ON PROXY FIREWALL",** is the record of the original work done by us under the guidance of **Dr.Mohamed Mallick, M.E., Ph.D**, Faculty Rathinam college of arts and science, Coimbatore. To the best of my knowledge this work has not formed the basis for the award of any degree/diploma/ associateship/fellowship/or a similar award to any candidate in any University.

Signature of the Student

PRAVEENKUMAR A

Place: Coimbatore

Date: 02.12.2022

COUNTERSIGNED

Dr.Mohamed Mallick, M.E., Ph.D

Contents

Acknowledgement

On successful completion for project look back to thank who made in possible. First and foremost, thank **"THE ALMIGHTY"** for this blessing on us without which we could have not successfully our project.I am extremely grateful to **Dr.Madan.A. Sendhil, M.S., Ph.D.,** Chairman, Rathinam Group of Institutions, Coimbatore and **Dr. R.Manickam MCA., M.Phil., Ph.D.,** Secretary, Rathinam Group of Institutions, Coimbatore for giving me opportunity to study in this college. I am extremely grateful to **Dr.R.Muralidharan, M.Sc., M.Phil., M.C.A., Ph.D.,** Principal Rathinam College of Arts and Science(Autonomous), Coimbatore.Extend deep sense of valuation to **Mr.A.Uthiramoorthy, M.C.A., M.Phil., (Ph.D),** Rathinam College of Arts and Science (Autonomous) who has permitted to undergo the project.

Unequally I thank **Mr.P.Sivaprakash, MTech., (Ph.D).,** Mentor and **Dr.Mohamed Mallick, M.E., Ph.D.,** Project Coordinator, and all the Faculty members of the Department - iNurture Education Solution Pvt Ltd for their constructive suggestions, advice during the course of study. I convey special thanks, to the supervisor **Dr.Mohamed Mallick, M.E., Ph.D.,** who offered their inestimable support, guidance, valuable suggestion, motivations, helps given for the completion of the project.

I dedicated sincere respect to my parents for their moral motivation in completing the project.

List of Figures

List of Abbreviations

FW	FirewallIT
IT	Information Technology
OT	operation Technology
DCN	Digital Communication Networks
REDIAL	RulE DIstribution ALgorithm
ABE	Attribute Based Encryption
PHR	Personal Health Records
TKQ	Top-K Query
AAL	Ambient Assisted iving

Abstract

A technical solution that can adapt to momentary changes in the network is the dynamic redistribution of filtering rules between firewalls that are situated inside the same network.

The amount of traffic that the firewalls process. This project introduces a novel formal model that may be used to enable the transfer of a set of rules from a firewall to its downstream neighbours when changes in the input traffic profile indicate doing so. The model is applicable to networks with many cascaded firewalls. In contrast to other solutions reported in the literature, a formal approach permits the computation of theoretical bounds for the anticipated performance prior to the proposed scheme being actually implemented in the target network, in addition to offering clear specifications and mathematical proofs of correctness.

Chapter 1

Introduction

TODAY, digital communication networks (DCNs) in all application areas require security and appropriate management are recognised critical features that are garnering growing attention even in fields that were not previously especially sensitive to security challenges. Network automation systems, factory networks, and distributed critical infrastructures are typical examples, which have become increasingly vulnerable to cyber-attacks since they began to migrate from proprietary communication technologies to more open, Internet-based solutions, and where awareness for improved security guarantees is constantly growing .

Filtering devices in general, and firewalls in particular, are widely used hardware (h/w) and software (s/w) components They are commonly used in digital networks a) to prevent undesired traffic from being sent to any destination, b) to prevent malicious communications from reaching their intended recipients to put countermeasures in place against cyberspace assaults . As networks become more complex, due in part to powerfully emerging paradigms such as edge and fog computing , Industrial IoT , the number of firewalls they include grows, and hierarchies of (cascaded) h/w and/or

s/w FWs can be found in real systems more frequently.

To address this issue, many methods may be implemented, which either function within a single FW (intra-firewall techniques) or rely on acceptable network-level procedures incorporating numerous FWs (inter-firewall approaches). Intra-firewall contributions in the literature have included (optimal) rule ordering, firewall compression, and rule analysis.

Inter-firewall alternatives are typically built on specialised architectures such as parallel firewalls]; another way makes use of the transmission of filtering rules between firewalls in the same network.In this research, we offer a formal method and an algorithm based on rule redistribution between cascaded firewalls to avoid performance loss.When an FW becomes overwhelmed with the flow of packets it must filter, it experiences a decrease in packet processing rate.

In comparison to previous strategies described in the literature, our solution requires no changes to the original routing of packets, as well as their forms and data. On the one hand, this is especially crucial in circumstances where the underlying communication infrastructure is not flexible enough to handle dynamic re-configurations, such as many factory, automation, and process control networks. reducing the efficacy of the control mechanism Similarly, neither the introduction of new h/w FWs nor

In these cases, dynamic instantiation of virtual FWs is possible since the system must frequently operate around the clock and cannot be halted or modified on the fly. As a result, installed FWs might become bottlenecks under high traffic load situations.

The approach presented in this study, on the other hand, does not rely on the

availability of specific h/w. As a result, the key contributions of this study are the following:

1] A network formal model that can deal with several cascaded firewalls and can be used to represent most systems seen in real-world applications.

2] A RulE DIstribution ALgorithm (REDIAL) to shift rules from a specific FW to downstream firewalls and minimise the average number of rules examined per packet, hence reducing packet processing activity by the FW of interest. The suggested technique's correctness is also explicitly confirmed and validated through simulation.

3] A simple model for forecasting the performance gain feasible with the FW transformation before implementing the proposed approach in the target network. The firewall's achievable benefit in terms of packet processing rate is given lower and upper constraints.

4] The performance results obtained by modelling our approach in a variety of settings indicate its benefits and strong agreement with the theoretical model.

5] Experiment performance data acquired by running the suggested method through a basic but realistic laboratory test-bed.

Our solution presupposes the presence of an orchestrator/supervisor with full view of the network's security settings and the capacity to coordinate and supervise the filtering activities of several firewalls.

The reader should be reminded that this requirement, which is also present in other authors' proposals, may incur some implementation costs. However, this type of assistance and products are not unusual, since they have been available in proprietary

technologies for quite some time, i.e., [29], [30], but they frequently necessitate the adoption of s/w and h/w devices from the same vendor (s).

Moving rules between multiple FWs may be challenging in general due to the existence of disparate administrative domains and authority. However, in the application areas covered in this study, this is seldom an issue because industrial/enterprise networks are frequently under the control of a few coordinated organisations (i.e., the information technology (IT) and operation technology (OT) departments) within the same organisation.

The remainder of the paper is structured as follows: Sect. II explains the adopted nomenclature and our model, whereas Sect. III describes the suggested approach in depth, including the REDI AL algorithm and the formal demonstration that the network's security integrity is preserved. Sect. IV deals with the determination of performance bounds for our method and displays the simulation results. This section also includes experimental performance numbers. Sect. V analyses several analogous studies that have emerged in the literature, highlighting parallels and differences with respect to our approach, and Sect. VI derives some conclusions.

1.1 Objective of the project

Moving rules between multiple FWs may be challenging in general due to the existence of disparate administrative domains and authority. However, in the application areas covered in this study, this is rarely an issue since industrial/enterprise networks are frequently controlled by a few coordinated organisations (i.e., the information technology

(IT) and operation technology (OT) departments) inside the same organisation.

1.2 Existing System

The approach suggested in this research does not rely on the availability of specialised hardware or software. Advanced FWs, for example, employ content-addressable memory (CAMs) or even ternary CAMs (TCAMs) to accelerate their operations. They are, however, uncommon in industrial devices, which are often rather basic and equipped with relatively low-power processing resources, as their design prioritises (mechanical) durability above performance. The penalty for improving the target FW's load filtering capabilities is an increase in communication bandwidth utilisation for links linking the FW to its downstream neighbours.

Chapter 2

Literature Survey

2.1 Encryption Based on Anonymous Hierarchical Identity

In this project, [1] Xavier Boyen proposes an identity-based cryptosystem with fully anonymous ciphertexts and hierarchical key delegation. Based on the moderate Decision Linear complexity assumption in bilinear groups, we provide a demonstration of security in the standard model. The system is efficient and practical, with short ciphertexts of linear size in the hierarchy's depth. Applications include encrypted data search, entirely private conversation, and so forth. Our findings address two outstanding issues in anonymous identity-based encryption, since our approach is the first to provide verifiable anonymity in the standard model, as well as the first to achieve fully anonymous at all levels of the hierarchy.

2.2 Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings

Ming Li has developed an online personal health record (PHR) that allows individuals to maintain their own medical information in a centralised manner, considerably facilitating the storing, access, and sharing of personal health data in this work work [2].

With the rise of cloud computing, it is becoming more appealing for PHR service providers to move their PHR apps and storage to the cloud in order to benefit from elastic resources while lowering operational costs.However, by storing PHRs in the cloud, individuals lose physical control over their personal health data, necessitating encryption of each patient's PHR data before uploading to cloud servers.It is difficult to provide fine-grained access control to PHR data using encryption in a scalable and efficient manner.

The PHR data for each patient should be encrypted such that it scales with the number of people that have access to it. Furthermore, because there are several owners (patients) in a PHR system, and each owner encrypts her PHR files with a separate set of cryptographic keys, it is critical to decrease key distribution complexity in such multi-owner scenarios.In this paper, we present a unique architecture for controlling access to PHRs in a cloud computing context. We use attribute-based encryption (ABE) approaches to encrypt each patient's PHR data to provide fine-grained and scalable access control for PHRs.To simplify the complexity of key distribution, we divide the

system into many security domains, each of which maintains just a fraction of the users.

As a result, each patient has complete control over her own privacy, and the complexity of key management is greatly decreased. Our suggested approach is also adaptable, since it allows for rapid and on-demand revocation of user access permissions, as well as break-glass access in emergency situations. Personal health records (PHR) have evolved as a patient-centric paradigm of health information interchange in recent years.

2.3 Identity-Based Proxy Re-Encryption

Matthew Green has proposed in this work work [4] A semi-trusted proxy turns a ciphertext for Alice into a ciphertext for Bob without seeing the underlying plaintext in a proxy re-encryption process. In the public-key setting, several solutions have been offered. We address the topic of Identity-Based proxy re-encryption in this paper, in which ciphertexts are changed from one identity to another. Our schemes are compatible with existing IBE deployments and do not necessitate any additional effort on the side of the IBE trusted-party key generator. Furthermore, they are non-interactive, and one of them allows for numerous re-encryptions. The random oracle model's security is based on a standard assumption.(DBDH).

A proxy can transform an encryption computed using Alice's public key into an encryption designed for Bob in a proxy re-encryption method. Alice can use such a method to temporarily pass encrypted messages to Bob without disclosing her secret key. The basic aspect of proxy re-encryption systems is that the proxy is not completely trusted; that is, it does not know Alice or Bob's secret keys and does not learn the

plaintext during the conversion. However, because the proxy and Bob are not permitted to cooperate, it is commonly presumed that at least one of them is telling the truth or that their cooperation is prevented or detectable through other ways.

2.4 A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks

Linke Guo has proposed in this work work [6] Because of attractive qualities such as universal accessibility, high accuracy, and cheap cost, electronic healthcare (eHealth) systems have largely supplanted work-based medical systems. Mobile healthcare (mHealth) is a fundamental component of eHealth systems that uses mobile devices such as smartphones and tablets to enable patient-to-physician and patient-to-patient conversations for improved healthcare and quality of life (QoL). Unfortunately, patients' fears about potential leakage of personal health information (PHRs) remain the most significant impediment.

Patients' medical records are often connected with a set of features such as existing symptoms and treatments in contemporary eHealth/mHealth networks based on information obtained from portable devices. PHRs should be verified in order to ensure the legitimacy of such qualities. Existing mHealth solutions, however, fail to protect patient identity privacy while providing medical services due to the linkability between identities and PHRs. To address this issue, we offer a decentralised system that uses verifiable qualities of users to authenticate each other while protecting attribute and identity privacy.

Furthermore, in diverse interactions among involved organisations, we create authentication systems with increasing privacy constraints. Finally, we conducted comprehensive simulations and tests to properly analyse the security and computational overheads of our suggested systems. WIDELY DEPLOYED electronic healthcare (eHealth) systems have enhanced people's everyday lives as compared to traditional work-based systems because of its exceptional benefits, such as higher efficiency, better accuracy, and broader availability. Furthermore, mobile healthcare (mHealth) systems use portable devices to simplify the use of eHealth systems, allowing users to collect personal health data more rapidly and effectively and gain better medical services.

2.5 Top-k Queries for Categorized RFID Systems

In this paper, [9] Xiulong Liu suggested This study investigates the practically essential topic of top-k queries for categorised RFID systems, which is to determine the top-k smallest and (or) top-k biggest categories, as well as the sizes of such categories. In this paper, we present a Top-k Query (TKQ) protocol as well as two supplemental strategies for enhancing TKQ: segmented perfect hashing (SPH) and switching to framed slotted aloha (STA). To begin, TKQ allows each tag to select a time window in which to answer to the reader with a single geometric string utilising the ON-OFF Keying modulation. To estimate the matching category size, TKQ uses the length of the continuous leading 1 s in the combined signal.

TKQ can swiftly reject most categories with sizes that differ considerably from the top-k border, and it only needs to do accurate prediction on a small number of categories

that may be within the top-k set. We do extensive analysis to ensure that the query results meet the set accuracy limits. Second, we suggest the SPH approach to enhance TKQ's average frame utilisation from 36.8To reduce total time costs, we improve the critical parameter that balances communication and calculation costs.

Third, the simulation traces show that TKQ+SPH spends the majority of its execution time querying a small number of remaining categories with sizes near to the top-k threshold, which occasionally surpasses the time cost of accurately identifying these remaining tags. Motivated by this discovery, we suggest the STA method to dynamically identify when we should stop TKQ+SPH and transition to FSA to complete the rest of the top-k query. The experimental findings reveal that TKQ+SPH+STA not only meets the needed accuracy limits, but it also runs many times quicker than the previous methods.

2.6 Fool Me If You Can: Mimicking Attacks and Anti-attacks in Cyberspace

In this work work [13] Shui Yu, has proposed Botnets have become major engines for malicious activities in cyberspace nowadays. To sustain their botnets and disguise their malicious actions, botnet owners are mimicking legitimate cyber behavior to fly under the radar. This poses a critical challenge in anomaly detection. In this work, we use web browsing on popular web sites as an example to tackle this problem. First of all, we establish a semi-Markov model for browsing behavior.

Based on this approach, we conclude that detecting imitating assaults based on

statistics is difficult if the number of active bots in the attacking botnet is sufficiently big (no less than the number of active legitimate users). However, we found that most of the time, botnet owners struggle to meet the criterion required to carry out a mimicking assault. We infer from this novel observation that imitating attacks may be distinguished from actual flash crowds using second order statistical indicators. We define a new fine correntropy metric and demonstrate its efficacy in comparison to others.

Our investigations and simulations using real-world data sets back up our theoretical claims. Furthermore, the findings have broad applicability to comparable circumstances in other scientific domains. In this paper, we aim to address the question: can we recognise genuine cyber activities imitating large-scale botnet attacks? The short answer is that it depends. We first establish this by demonstrating that genuine cyber behaviour may be successfully imitated; hence, statistical approaches cannot distinguish between imitating assaults and actual cyber activities. To do this, attackers must meet one essential condition: they must have a sufficiently big number of active bots, with no less than the number of active genuine users of the simulated events.

By active bots, we mean bots that botnet owners can manage when they launch assaults. Botnets are the primary motivators behind cyber assaults such as distributed denial of service (DDoS), information phishing, and email spamming. These assaults are common on the Internet and can result in significant financial loss. Attackers find it desirable to create complex botnets for use as attack tools when they are motivated by large financial or political rewards. Botnets of several varieties exist in cyberspace, in-

cluding DSNXbot, evilbot, G-Sysbot, sdbot, and Spybot. On the one hand, researchers have investigated botnets from a variety of angles, including botnet probing events, Internet connections, scale, and domain fluxing.

2.7 LDPA: A Local Data Processing Architecture in Ambient Assisted Living Communications

The author of this article, Kun Wang, has proposed How the living conditions of the elderly can be effectively assessed using the information gathered by ambient sensors is one of the most problematic issues in ambient assisted living. Environmental factors should be appropriately taken into account to resolve this issue. Some researchers have suggested using dispersed environmental sensors to collect data completely, but they neglected how the vast amounts of data would be evaluated and delivered. In this paper, we provide a local server-based data processing architecture for analysing gathered data. The data gathering layer of this three-layer design stores the most recent data that has been received.

A data filtering layer then evaluates the effectiveness of the data. Additionally, this layer divides the incoming data into streams of real-time data that indicate quality of life and static data that reflect the state of the sensors. The real-time data stream is separated into levels, and static data is directly recorded in a database. A data analysis layer uses these levels as a foundation to reorganise the data into a neighbourhood structure we'll refer to as RDAA. Only abnormal data will be provided to a healthcare provider when its risk factor is greater than a predetermined threshold. RDAA returns

a risk factor. The effort of the distant healthcare practitioner is reduced as a result of LDAP's ability to distribute the strain of remote centralised processing and data storage.

For instance, multiple sensors in a home can communicate living status and sleep regularity to a remote health care provider Through a variety of intelligent services, ambient assisted living (AAL) improves the senior population's capacity for independent living, hence lowering the need for on-site or off-site direct care.

Applications offered by AAL include reminding older individuals to take their medications, keeping tabs on their health to prevent illness, and identifying and analysing physiological features to assure their safety and wellness. Real-time communications that keep the elderly in touch with their relatives can also be facilitated by AAL technologies.

2.8 Mobile Big Data Fault-Tolerant Processing for eHealth Networks

In this work work [8] Kun Wang, has proposed In daily life, people tend to use mobile networks for more accurate overall data. With intelligent mobile devices, almost all kinds of data can be collected automatically, which contributes directly to the blooming of eHealth. However, large amounts of data are also leading us into the era of big data, in which new data collection, transmission, and processing techniques are required. To ensure ubiquitous data collection, the scale of mobile eHealth networks has to be expanded. Also, networks will face more pressure to transmit large amounts of eHealth data. In addition, because the processing time increases with data volume, even powerful processors cannot always be regarded as efficient for big data. To solve these problems, in this article, an interests-based reduced variable neighborhood search (RVNS) queue architecture (IRQA) is proposed. In this three-layer architecture, a fault-tolerant mechanism based on interests matching is designed to ensure the completeness of eHealth data in the data gathering layer. Then the data integrating layer checks the accuracy of data, and also prepares for data processing. In the end, an RVNS queue is adopted for rapid data processing in the data analyzing layer. After processing with relevant rules, only valuable data will be reported to health care providers, which saves their effort to identify these data. Simulation shows that IRQA is steady and fast enough to process large amounts of data. Traditional health care services can hardly meet the needs of the growing population because hospital capacity and medical

workers are limited in terms of the continuously increasing treatment requests. On this background, a new kind of eHealth service using intelligent device to monitor people's lives is developing rapidly with the benefits of big data technique. In this era of big data, large amount of data has been transmitted on the Internet, stored in servers and clouds, and even collected around people's life by mobile networks. Characterized by their volume, velocity, variability, and veracity, mobile big data networks are used to describe those extremely large or complex data sets in the network for which traditional processing methods are inadequate. Specifically, data collected by mobile eHealth networks are becoming more ubiquitous with the development of hardware, and a group of collecting nodes are required to get more overall data. Meanwhile, the number of collecting nodes in a network tends to increase, and each collecting node tends to have higher sampling frequency. Some typical types of sensors (e.g., brain sensors) will generate huge amounts of data, the size of which can even grow to the terabyte level. Also, the size of records of a clinic agency easily grows to the exabyte level. All the factors mentioned above increase the scale of a network, as well as the data volume transmitted in an eHealth network.

Chapter 3

Methodology

3.1 Multiple Firewall Architecture Modelling

Stremed Topology

The model under consideration can officially define real architectures and topology types while simplifying and improving the presentation of the suggested approach. We are particularly interested in networks that incorporate three main types of devices:

• Filtering Devices (i.e., firewalls): these elements have one input and one output port and can pass (some subset of) packets received from their input to their output. A sufficient set of rules underpins the filtering function.

• Routing Devices (i.e., switches and routers): these elements often have multiple input/output ports and can appropriately pass packets from an input to one or more outputs on the pathways to their intended destinations.

• End Devices (PCs, servers, and special-purpose computing nodes): these are the origin(s) and/or destination(s) of packets. To receive and

transfer data, they need an input/output network interface. A entire subnetwork can be encased into an appropriate end device for modelling purposes if its building blocks and connections are not of interest, obscuring the subnetwork underlying architecture and superfluous features.

Similarly, actual devices can be modelled by combining one or more logical components (for example, a personal computer with two or more network interfaces and a software firewall can be described by combining one filtering element with one route and end device pair). This option allows for the seamless translation of sophisticated and fine-grained designs into smaller systems To keep the notation simple, RST device names are used in the following to remember the sets of linked IP addresses. 1) The IP address d0 for the tree's root is known in advance. 2) The preceding set d2,i for each leaf I is known. 3) All root and leaf sets are distinct (not overlapped) and not interleaved. 4) Each routing device's set is the union of the sets for each subtree rooted in it, for example, d1 = N i=1 d2,i. This set may be calculated in general as the union of all sets in each subtree via a postorder visit that yields the set for each reached node, where firewalls are considered as simple connections.

3.2 Firewalls

We focus on IP-layer firewalls, which have filtering fields that include source and destination IP addresses, source and destination port addresses, and protocol number. However, the criteria below are broad enough to be applied to firewalls functioning at any network level.

A d-tuple of ranges is defined in Definition 1. F = (f1,..., fd) is a tuple of d non-negative integer finite ranges, fi N0 I [1, d]. As an example, we can define F to represent all of the filtering fields considered by a firewall and, as a result, the corresponding fields in network packets: F = ([0, 232 1], [0, 232 1], [0, 216 1], [0, 216 1], [0, 28 1], representing source and destination IPv4 addresses, source and destination port addresses, and protocol number, respectively.

Definition 2: Given a d-tuple of ranges F = (f1,..., fd), define a packet P across F as P = (p1,..., pd), with each pi fi.

Definition 3: Given a d-tuple of ranges, P is the set of all feasible packets across F, i.e. P = P = (p1,..., pd) where each pi fi and its cardinality is —P— = I — fi—, where — fi— stands for the cardinality of fi, i.e. the breadth of its corresponding range.

Definition 4: Given a d-tuple of ranges F = (f1,..., fd), construct a condition C over F as follows: C = (c1,..., cd) where each ci fi.

Definition 5: A condition C over P defines PC P where PC = (p1,..., pd)

P and its cardinality is —PC— = I —ci——p— Definition 6: A firewall f w is a finite sequence of rules.

f w = (r1,r2,...,r— f w—), where the number of rules — f w— is referred to as the firewall cardinality.

Each rule is specified as r = (C, action), where action varies within a limited set of all conceivable firewall actions. Definition 7: Given a packet P and a rule r = (C, action), we say that P matches r .

Definition 5: A condition C over P defines PC P where PC = (p1,..., pd) P and its cardinality is —PC— = I —ci——p— Definition 6: A firewall f w is a finite sequence of rules.

Definition 6 : f w = (r1,r2,...,r— f w—), where the number of rules — f w— is referred to as the firewall cardinality. Each rule is specified as r = (C, action), where action varies within a limited set of all conceivable firewall actions.

Definition 7: Given a packet P and a rule r = (C, action), we say that P matches r if PC.

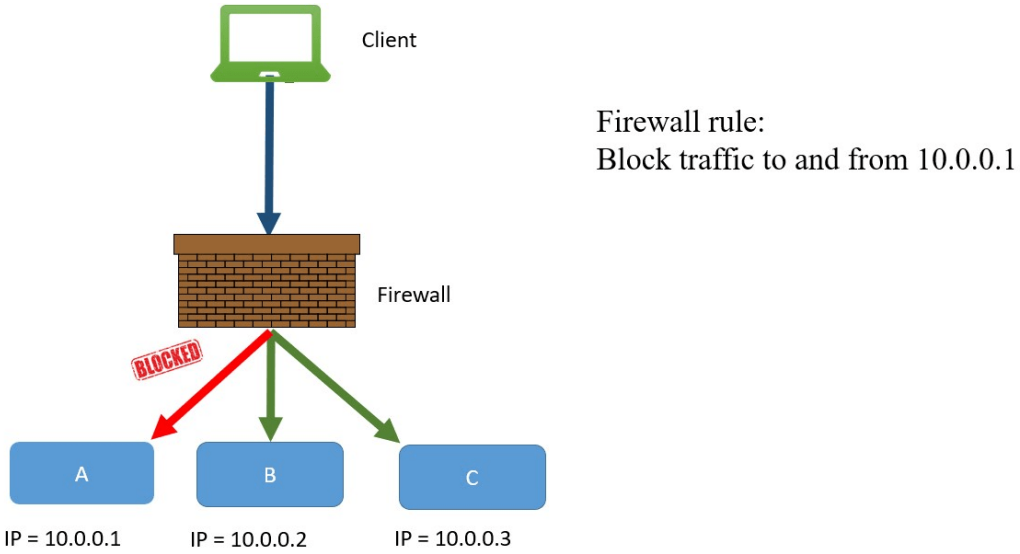

Figure 3.1: implementation of Firewall

3.3 Advantages

• It uncovers problems quickly because the specification language syntax enforces correctness. It promotes problem-free software because each step is verified or validated along the way. •They help disambiguate system specifications and articulate implicit assumptions. •They also expose flaws in system requirements, and their rigor enables a better understanding of the problem. •Incrementally grows in effective solution after each iteration. •This model does not involve high complexity rate.

3.4 System Design

I present the entire system in this part, including system setup, key generation, encryption, re-encryption, authentication, and decryption. The settings are first set up, and the secret keys are created. The data is encrypted and converted into ciphertext. The production of re-encryption keys is then completed. Following that, the data receivers' qualities are validated, and only receivers with particular attributes have access to the re-encryption keys and can re-encrypt the ciphertexts. Finally, the decryption of re-encrypted ciphertexts is demonstrated. Privacy-preserving Personal information may be exposed since PKE cannot ensure the anonymity of the people sending and receiving the ciphertext in this module.

If an opponent obtains the ciphertext, he may determine whose key the ciphertext is encrypted with, hence determining the owner of the ciphertext. To circumvent this limitation, several anonymous encryption schemes, such as the anonymous mechanism, have been developed. They accomplish anonymity by disassociating the data from the identity. Identities are separated into two randomised complimentary components that conceal the receivers' identities behind some randomness.

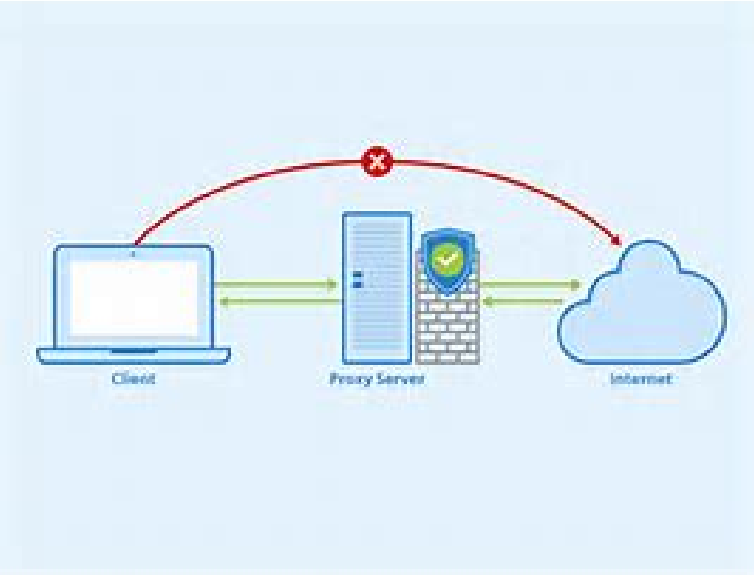

Figure 3.2: proxyFirewall

3.5 authentication

This module may aim to distribute data exclusively with recipients who meet particular criteria. To ensure that data and identities are not compromised, data providers and receivers must authenticate each other's authenticity. The traits must also be safeguarded. presented a system for verifying the legitimacy of users' characteristics

Using this strategy, we propose a mechanism termed the pre-authentication approach to proxy re-encryption. Data providers can use our system to validate the identity of receivers. If the qualities of the receiver do not fulfil the requirements, the provider will no longer contact with him and he will be unable to acquire the data.

Chapter 4

Experimental Setup

4.1 proxy re-encryption

When results are compared when data is on disc vs in cache, disc throughput limits IB-speed DPDP's when accessing all blocks. I/O and challenge computation happen in parallel, with the exception of the initial blocks of a file. Thus, Proxy-Conditional-Re-Encryption creates proofs quicker than the disc can transmit data: 1.0 second for a 64 MB file against 1.8 seconds for a disc. No protocol can surpass Proxy-Conditional-Re-Encryption by more than the beginning costs since I/O limits performance. While quicker, multiple-disk storage may eliminate the I/O constraint for the time being. Processor speeds will eventually outpace disc bandwidth, and the I/O bound will hold. Sampling disrupts the linear scaling relationship between the amount of time required to establish proof of data possession and the size of the file.

4.2 Implementation of proxy firewall

The basic network layout represented in Fig. 4 was subsequently chosen for the test-bed, and timing data was gathered using appropriate traffic access points (TAPs) and cards supporting hardware timestamps. Figure 7 depicts the test-bed configuration, which includes: • The traffic generator G (d0) is an Apple iMac with an Intel® CoreTM 2 Extreme X7900 CPU @ 2.80GHz, 4 GB of RAM, and the 20.04 LTS Ubuntu Linux distribution. • The firewalls FW1 and FW2 are personal computers with an Intel® CoreTM 2 Duo E6750 CPU @ 2.66GHz, 4GB of RAM, and two identical Realtek Semiconductor NICs (ICSs RTL-8139). They use the 18.04 LTS Ubuntu Linux distribution, which includes the iptables firewall configurator.

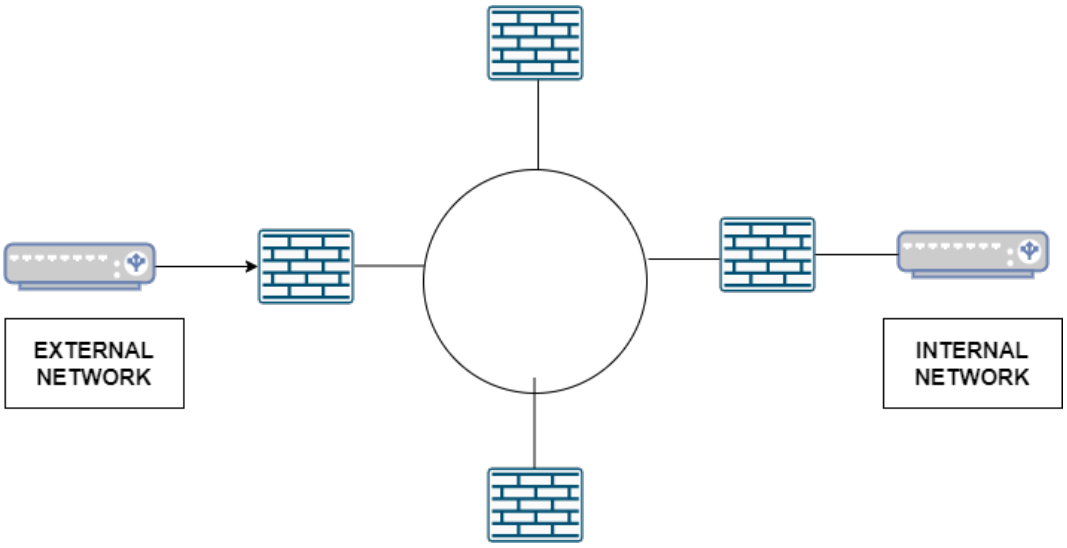

Figure 4.1: Flow work

4.3 CLIENT/SERVER:

A server is anything that has some resource that can be shared. There are compute servers, which provide computing power; print servers, which manage a collection of printers; disk servers, which provide networked disk space; and web servers, which store web pages. A client is simply any other entity that wants to gain access to a particular server.

A server process is said to "listen" to a port until a client connects to it. A server is allowed to accept multiple clients connected to the same port number, although each session is unique. To manage multiple client connections, a server process must be multithreaded or have some other means of multiplexing the simultaneous I/O.

Chapter 5

Conclusion

The (re)distribution of filtering rules between multiple firewalls in the same network is a technological difficulty that is critical not only during the design phase of a new system, but also during the network's real-time operation and administration. Of course, this would not be feasible without rigorous coordination of firewall actions, but solutions are now available from well-tested paradigms such as SDN and NFV, which provide the necessary levels of flexibility and monitoring. In this study, a unique approach for reducing packet processing cost in overload scenarios, such as transient traffic surges or DoS assaults, is proposed.

My method necessitates no changes to the routing architecture or packet modification, such as the use of additional bit fields, and is highly compatible with devices and network equipment often found in industrial and automation systems. To shift rules across various FWs, a transformation method was devised, and its accuracy and ability to maintain network security were explicitly established and tested by simulation.

5.1 Future Works

Simulation results obtained in a number of experiments by varying the traffic and firewall characteristics confirm the validity of the proposed approach and a very good accordance with the theoretical model. Measures collected, by deploying the proposed solution in a purposely developed testbed, show that the expected performance gain determined both theoretically and through simulation is close to the actual improvements achievable in realistic conditions can be done in future .

References

1. **X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption (without random oracles(lecture notes in computer science)," Advances in Cryptology, vol. 4117, pp. 290–307, Aug 2006.**

2. **K. R. M. Li, S. Yu and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," Security and Privacy in Communication Networks -, Iternational ICST Conference, SECURECOMM, pp. 89–106, 2010.**

3. **E. H. J. Benaloh, M. Chase and K. Lauter, "Patient controlled encryption: Ensuring privacy of electronic medical records," ACM Cloud Computing Security Workshop, pp. 103–114, 2009.**

4. **M.Green and G. Ateniese, "Identity-based proxy re-encryption," Applied Cryptography and Network Security (Lecture Notes in Computer Science), vol. 4521, pp. 288–306, 2007.**

5. **W. S. K. Liang and J. Liu, "Privacy-preserving ciphertext multisharing control for big data storage," IEEE Transaction on Information Forensics and Security, vol. 10, no. 8, Aug 2015.**

6. **J. S. L. Guo, C. Zhang and Y. Fang, "A privacy-preserving attribute-based authentication system for mobile health networks," IEEE Transaction on Mobile Computing, vol. 13, no. 9, Sep 2014.**

7. **K. Wang, Y. Shao, L. Shu, G. Han, and C. Zhu, "Ldpa: A local data processing architecture in ambient assisted living communications," IEEE Communications Magazine, vol. 53, no. 1, pp. 56–63, Jan 2015.**

8. **K. Wang, Y. Shao, L. Shu, Y. Zhang, and C. Zhu, "Mobile big data fault-tolerant processing for ehealth networks," IEEE Network, vol. 30, no. 1, pp. 1–7, Jan 2017.**

9. **X. Liu, K. Li, J. Wu, A. X. Liu, X. Xie, C. Zhu, and W. Xue, "TOP-k Queries for Multi-category RFID Systems," Proc. of IEEE INFOCOM, 2016.**

10. **K. Wang, M. Du, Y. Sun, A. Vinel, and Y. Zhang, "Attack detection and distributed forensics in machine-to-machine networks," IEEE Network, vol. 30, no. 6, pp. 49–55, Nov 2016.**

11. **L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. Vasilakos,**

"Security and privacy for storage and computation in cloud computing," Information Sciences, vol. 258, pp. 371–386, Feb 2014.

12. H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-toltrant networks," IEEE Transaction on Parallel and Distributed Systems, vol. 25, no. 1, pp. 22–32, Jan 2014.