Dynamic Firewall Decomposition and Composition in the Cloud

E. Madhorubagan[1], Abhiekrrishnan.J[2], Balu.K[3], Chinnaiyan.M[4]
[1] *Assistant Professor, M.E., Department of Computer Science and Engineering, Mahendra Engineering College, Tamilnadu, India*
[2,3,4] *UG Students, Department of Computer Science and Engineering, Mahendra Engineering College, Tamilnadu, India*

Abstract **- Firewalls filter malicious traffic and provide the network with a satisfying level of security. Thus, their performance is critical for the whole network. Rule-based firewalls are the most widely deployed among traditional ones. However, as the size of the rule list of a firewall increases, lookup latency increases significantly. One main solution to enhance the performance of a firewall is to reorder rules based on traffic characteristics to obtain the minimum number of packet matches. The optimal firewall rule ordering problem (ORO) is NP-Complete. Therefore, setting up a centralized firewall for a whole network is infeasible. Our proposed solution dynamically scales in and out firewalls across multiple administrative domains for more efficient rules optimization, filtering, and better attack response. The proposed solution, in this paper, outsources the firewall functions into micro firewalls, which are located in different places and have their configurations. Therefore, traffic is treated locally and in a distributed way. The experimental results show that our proposed solution is scalable regarding the organization's network requirements. Moreover, the central firewall is relaxed executing rules optimization algorithms in consecutive time intervals, inefficient.**

OBJECTIVE

Enhance the performance of a firewall is to reorder rules based on traffic characteristics to obtain the minimum number of packet matches. The optimal firewall rule ordering problem (ORO) is NP-Complete. Therefore, setting up a centralized firewall for a whole network is infeasible. Our proposed solution dynamically scales in and out firewalls across multiple administrative domains for more efficient rules optimization, filtering, and better attack response

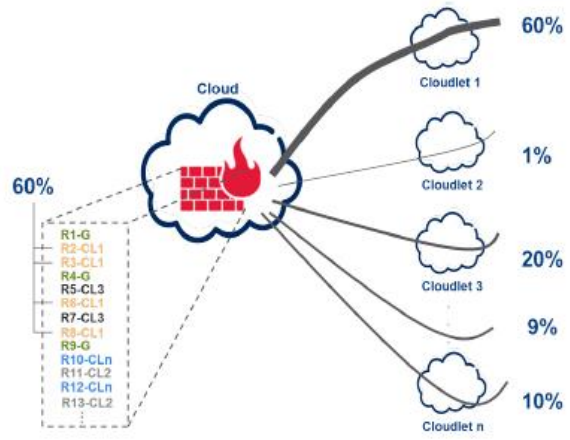
OVER VIEW OF THE PROJECT

Rule-based firewalls are the most widely deployed among traditional firewalls and an improper rule ordering can become a performance bottleneck since the rarely triggered rules are checked unnecessarily frequently. Thus, the traffic characteristics should be analyzed to figure out which rules are outdated or have not been used for a long time. Consequently, firewall rules need to be ordered adaptively to obtain the minimum number of packet matches and avoid serious performance degradation due to the traffic anomaly.

INTRODUCTION

Firewalls have been widely deployed for securing networks and are the first line of defense against malicious traffic [1]. A firewall checks each incoming or outgoing packet to decide whether to accept or reject the packet based on its policy. The efficiency of firewalls depends on two factors as follows: 1) Rules Optimization: Rule-based firewalls are the most widely deployed among traditional firewalls [2] and an improper rule ordering can become a performance bottleneck since the rarely triggered rules are checked unnecessarily frequently. Thus, the traffic characteristics should be analyzed to figure out which rules are outdated or have not been used for a long time [3], [4]. Consequently, firewall rules need to be ordered adaptively to obtain the minimum number of packet matches and avoid serious performance degradation due to the traffic anomaly. The optimal rule ordering problem (ORO) with rule dependency constraints is proven to be NP-Complete. The proof is presented in [3]. Therefore, it is costly to update the rule ordering dynamically concerning the traffic loads. 2) Scalability Architecture: The deployment of centralized firewalls leads to performance bottleneck

for heavy traffic (e.g., DDoS) and it is hard to guarantee QoS requirement for all other normal traffic [5], [6]. Besides, distributed architecture with physical firewalls is neither rational nor cost-effective, since it needs a high level of traffic directed toward the appropriate firewall at the appropriate time. Thus, techniques must be provided for the firewalls to treat the traffic at any time without introducing any noticeable delay and cost.



Initial rule ordering configuration

MODULES

- A Super-Peer Protocol for Job Submission
- Dynamic Caching
- Performance Evaluation
- Redundant Scalability Analysis

MODULES DESCRIPTION:

A SUPER-PEER PROTOCOL FOR JOB SUBMISSION

A data-intensive Grid application can require the distributed execution of a large number of jobs with the goal to analyze a set of data files. Data can be analyzed in parallel by a number of Grid nodes to speed up computation and keep the pace with data production. A single job consists of the comparison of the input data file with a number of templates, and in general it must be executed multiple times in order to assure a given statistical accuracy. This kind of application is usually managed through a centralized framework, in which one server assigns jobs to workers, sends them input data, and then collects results; however this approach clearly limits scalability.

DYNAMIC CACHING

Dynamic caching allows for the replication of input data files on multiple data cachers. This leads to well known advantages such as increased degree of data availability and improved fault tolerance. Moreover, dynamic caching allows for a significant saving of time in the data download phase, because data queries have a greater chance to find an available data center, and most workers can download data from a neighbor data cacher instead of a remote data source.

PERFORMANCE EVALUATION

It is assumed that all the jobs have similar characteristics and can be executed by any worker. Workers can disconnect and reconnect to the network at any time. This implies that a job execution fails upon the disconnection of the corresponding worker. This is a new feature with respect to the basic protocol presented in. The overall execution time, Texec, is crucial to determine the rate at which data files can be retrieved from the data source in order to guarantee that the workers are able to keep the pace with data. which is defined as the fraction of time that a data center is actually utilized, i.e., the fraction of time in which at least one download connection, from a worker or a data cacher, is active with this data center.

REDUNDANT SCALABILITY ANALYSIS

Two different scenarios were tested: when only one data source is available, regardless of the network size; and when the number of data sources is proportional to the network size. It is interesting to note that the overall execution time may be decreased by using a larger number of workers. Furthermore, it can be noticed that the reduction of the execution time is obtained only if the Machine Time to Live (MTL) is larger than a threshold. Indeed, if MTL is low, it is likely that a considerable percentage of jobs are assigned to workers that are distant from the data source(s); the larger is the network, the longer are download times, and therefore the overall execution time.

SOFTWARE ENVIRONMENT

NetBeans is an integrated development environment (IDE) for Java. NetBeans allows applications to be

developed from a set of modular software components called modules. NetBeans runs on Windows, macOS, Linux and Solaris. In addition to Java development, it has extensions for other languages like PHP, C, C++, HTML5, and JavaScript. Applications based on NetBeans, including the NetBeans IDE, can be extended by third party developers.

The NetBeans Platform is a framework for simplifying the development of Java Swing desktop applications. The NetBeans IDE bundle for Java SE contains what is needed to start developing NetBeans plugins and NetBeans Platform based applications; no additional SDK is required.

Applications can install modules dynamically. Any application can include the Update Center module to allow users of the application to download digitally signed upgrades and new features directly into the running application. Reinstalling an upgrade or a new release does not force users to download the entire application again.

The platform offers reusable services common to desktop applications, allowing developers to focus on the logic specific to their application. Among the features of the platform are:

- User interface management (e.g. menus and toolbars)
- User settings management
- Storage management (carries out efficient storage)
- Window management
- Wizard framework (supports step-by-step dialogs)
- NetBeans Visual Library
- Integrated development tools

NetBeans IDE

NetBeans IDE is an open-source integrated development environment. NetBeans IDE supports development of all Java application types (Java SE (including JavaFX), Java ME, web, EJB and mobile applications) out of the box. Among other features are an Ant-based project system, Maven support, refactorings, version control (supporting CVS, Subversion, Git, Mercurial and Clearcase).

This tutorial provides a very simple and quick introduction to the NetBeans IDE workflow by walking you through the creation of a simple "Hello World" Java console application. Once you are done with this tutorial, you will have a general knowledge of how to create and run applications in the IDE. This tutorial takes less than 10 minutes to complete.

After you finish this tutorial, you can move on to the learning trails, which are linked from the Documentation, Training & Support page. The learning trails provide comprehensive tutorials that highlight a wider range of IDE features and programming techniques for a variety of application types. If you do not want to do a "Hello World" application, you can skip this tutorial and jump straight to the learning trails.

NetBeans IDE Bundle for Web and Java EE

The NetBeans IDE Bundle for Web & Java EE provides complete tools for all the latest Java EE 6 standards, including the new Java EE 6 Web Profile, Enterprise Java Beans (EJBs), servlets, Java Persistence API, web services, and annotations. NetBeans also supports the JSF 2.0 (Facelets), JavaServer Pages (JSP), Hibernate, Spring, and Struts frameworks, and the Java EE 5 and J2EE 1.4 platforms. It includes GlassFish and Apache Tomcat. Some of its features with javaEE includes

- ❖ Improved support for CDI, REST services and Java Persistence
- ❖ New support for Bean Validation
- ❖ Support for JSF component libraries, including bundled PrimeFaces library
- ❖ Improved editing for Expression Language in JSF, including code completion, refactoring and hints

These modules are part of the NetBeans IDE:

The **NetBeans Profiler** is a tool for the monitoring of Java applications: It helps developers find memory leaks and optimize speed. Formerly downloaded separately, it is integrated into the core IDE since version 6.0. The Profiler is based on a Sun Laboratories research project that was named JFluid.

That research uncovered specific techniques that can be used to lower the overhead of profiling a Java application. One of those techniques is dynamic bytecode instrumentation, which is particularly useful for profiling large Java applications. Using dynamic bytecode instrumentation and additional algorithms, the NetBeans Profiler is able to obtain runtime information on applications that are too large or complex for other profilers. NetBeans also support Profiling Points that let you profile precise points of execution and measure execution time.

GUI design tool

- Formerly known as *project Matisse*, the GUI design-tool enables developers to prototype and design Swing GUIs by dragging and positioning GUI components.
- The GUI builder has built-in support for JSR 295 (Beans Binding technology), but the support for JSR 296 (Swing Application Framework) was removed in 7.1.

NETBEANS JAVASCRIPT EDITOR

The NetBeans JavaScript editor provides extended support for JavaScript, Ajax, and CSS.

JavaScript editor features comprise syntax highlighting, refactoring, code completion for native objects and functions, generation of JavaScript class skeletons, generation of Ajax callbacks from a template; and automatic browser compatibility checks.

CSS editor features comprise code completion for styles names, quick navigation through the navigator panel, displaying the CSS rule declaration in a List View and file structure in a Tree View, sorting the outline view by name, type or declaration order (List & Tree), creating rule declarations (Tree only), refactoring a part of a rule name (Tree only).

No other Java development tool on the market today combines the ease of use of NetBeans 4.1 with this level of comprehensive support for J2EE application development," said Jeff Jackson, Vice President of Java Development and platform engineering for Sun Microsystems. "The search, download, test and assemble cycle that is required by other open source development offerings cannot even approximate what NetBeans provides out-of-the-box for free."

- ✓ The NetBeans IDE enhances developer workflow with its more intuitive interface, integrated Ant-based project management build environment and productivity tools that support agile development processes. NetBeans' acclaimed advanced code editor, with built-in refactoring, helps developers code more accurately and more quickly. Mobile development support is augmented in this version with visual drag-and-drop MIDP authoring and a Wireless Connection Wizard for building end-to-end mobile applications.
- ✓ "eBay Web Services makes a variety of tools and resources available to its Developers Program members to encourage the creation of new, innovative applications," said Greg Isaacs, director of the eBay Developers Program. "The rich set of features and proven performance of the NetBeans IDE are two reasons the eBay SDK has been enabled to support this development environment."
- ✓ NetBeans 4.1 IDE supports the broadest array of Java technology-based solutions, from Java Web Services, to mobile Java applications, to applications deployments on the industry's most advanced desktop environments. With the Sun Java System Application Server Platform Edition 8.1 deployment runtime integrated at no additional cost., NetBeans offers the industry's most cost effective IDE for building web services.
- ✓ Advanced features in NetBeans guide the developer and automatically build the underlying J2EE application infrastructure, making it easier than ever to develop J2EE platform 1.4 applications. To further assist the developer, the Java BluePrints Solutions Catalog and an updated performance profiler are also available. The profiler enables memory profiling, leak detection, CPU performance profiling, low-overhead profiling, task-based profiling and tight integration into the IDE workflow.
- ✓ The NetBeans platform is a 100 percent Java technology-based IDE and runs on any operating system with a Java 2 technology-compatible Java Virtual Machine. This includes the Solaris Operating System, Windows, Linux and Macintosh platforms. NetBeans is also the foundation for Sun's Java development tools offerings, including the award winning Sun Java Studio Enterprise and Sun Java Studio Creator.

NetBeans IDE Complete Bundle

Oracle also releases a version of NetBeans that includes all of the features of the above bundles. This bundle **includes:**

- NetBeans Base IDE
- Java SE, JavaFX
- Web and Java EE
- Java ME
- C/C++
- PHP (Version 5.5 and later)
- Apache Groovy
- GlassFish
- Apache Tomcat

About NetBeans IDE

NetBeans IDE is a free, open source, integrated development environment (IDE) that enables you to develop desktop, mobile and web applications. The IDE supports application development in various languages, including Java, HTML5, PHP and C++. The IDE provides integrated support for the complete development cycle, from project creation through debugging, profiling and deployment. The IDE runs on Windows, Linux, Mac OS X, and other UNIX-based systems.

The IDE provides comprehensive support for JDK 7 technologies and the most recent Java enhancements. It is the first IDE that provides support for JDK 7, Java EE 7, and JavaFX 2.

NetBeans IDE Bundle for PHP

NetBeans supports PHP since version 6.5. The bundle for PHP includes:

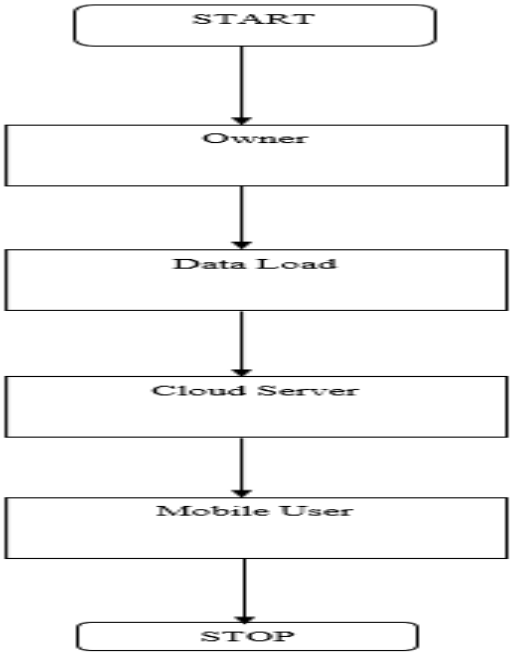
- ✓ syntax highlighting, code completion, occurrence highlighting, error highlighting, CVS version control
- ✓ semantic analysis with highlighting of parameters and unused local variables
- ✓ PHP code debugging with xdebug
- ✓ PHP Unit testing with PHPUnit and Selenium
- ✓ Code coverage
- ✓ Symfony framework support (since version 6.8)
- ✓ Zend Framework support (since version 6.9)
- ✓ Yii Framework support (since version 7.3)
- ✓ PHP 5.3 namespace and closure support (since version 6.8)
- ✓ Code Folding for Control Structures (since version 7.2 dev

SYSTEM DESIGN

DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

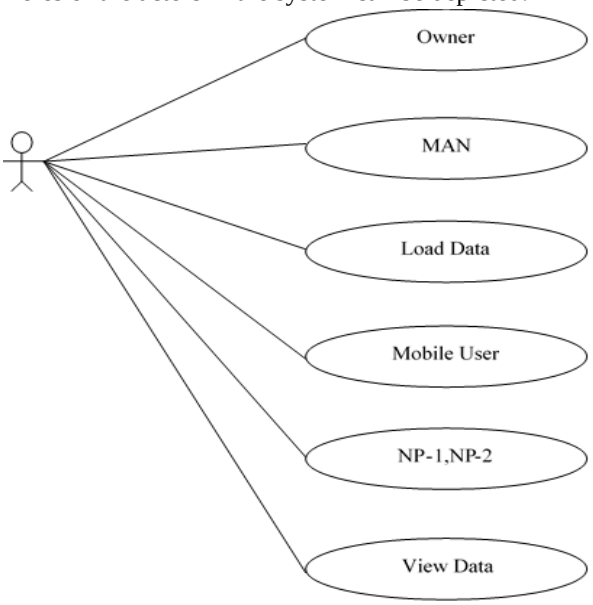
DATA FLOW DIAGRAM:



USE CASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases.

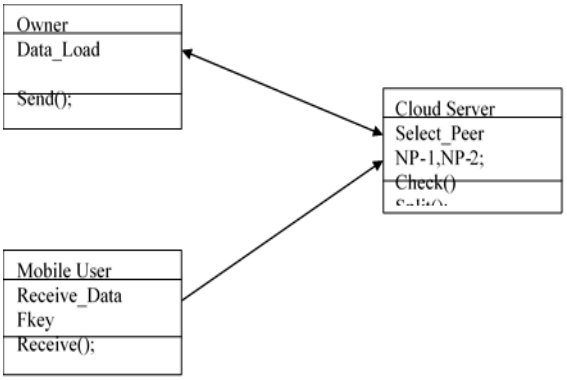
The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.



CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods)

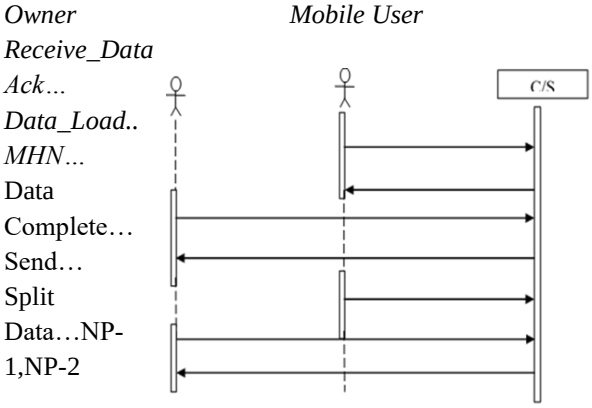
and the relationships among the classes. It explains which class contains information.



SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart.

Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.



LITERATURE SURVEY

FIREWALL FINGERPRINTING AND DENIAL OF FIREWALLING ATTACKS

AUTHORS: Alex X. Liu, Amir R. Khakpour and Joshua W. Hulst

Firewalls are critical security devices handling all traffic in and out of a network. Firewalls, like other software and hardware network devices, have vulnerabilities, which can be exploited by motivated attackers. However, just like any other networking and computing devices, firewalls often have vulnerabilities that can be exploited by attackers. In this paper, first, we investigate some possible firewall fingerprinting methods and surprisingly found that these methods can achieve quite high accuracy. Second, we study what we call denial of firewalling (DoF) attacks, where attackers use carefully crafted traffic to effectively overload a firewall. To the best of our knowledge, this paper represents the first study of firewall fingerprinting and DoF attacks.

PERFORMANCE MODELING AND ANALYSIS OF NETWORK FIREWALLS

AUTHORS: Khaled Salah, Khalid Elbadawi and Raouf Boutaba.

Network firewalls act as the first line of defense against unwanted and malicious traffic targeting Internet servers. Predicting the overall firewall

performance is crucial to network security engineers and designers in assessing the effectiveness and resiliency of network firewalls against DDoS (Distributed Denial of Service) attacks as those commonly launched by today's Botnets. In this paper, we present an analytical queueing model based on the embedded Markov chain to study and analyze the performance of rule-based firewalls when subjected to normal traffic flows as well as DoS attack flows targeting different rule positions. We derive equations for key features and performance measures of engineering and design significance. These features and measures include throughput, packet loss, packet delay, and firewall's CPU utilization. In addition, we verify and validate our analytical model using simulation and real experimental measurements.

DYNAMIC RULE-ORDERING OPTIMIZATION FOR HIGH-SPEED FIREWALL FILTERING

AUTHORS: Hazem H Hamed and Ehab Salem Al-Shaer

Packet filtering plays a critical role in many of the current high speed network technologies such as firewalls and IPSec devices. The optimization of firewall policies is critically important to provide high performance packet filtering particularly for high speed network security. Current packet filtering techniques exploit the characteristics of the filtering policies, but they do not consider the traffic behavior in optimizing their search data structures. This results in impractically high space complexity, which undermines the performance gain offered by these techniques. Also, these techniques offer upper bounds for the worst case search times; nevertheless, average case scenarios are not necessarily optimized. Moreover, the types of packet filtering fields used in most of these techniques are limited to IP header fields and cannot be generalized to cover transport and application layer filtering.In this paper, we present a novel technique that utilizes Internet traffic characteristics to optimize firewall filtering policies. The proposed technique timely adapts to the traffic conditions using actively calculated statistics to dynamically optimize the ordering of packet filtering rules. The rule importance in traffic matching as well as its dependency on other rules are both considered in our optimization algorithm. Through extensive evaluation experiments using simulated and real Internet traffic traces, the proposed mechanism is shown to be efficient and easy to deploy in practical firewall implementations.

AN INTELLIGENT SECURITY ARCHITECTURE FOR DISTRIBUTED FIREWALLING ENVIRONMENTS

AUTHORS: Aniello Castiglione, Ugo Fiore and Francesco Palmieri.

Due to the increasing threat of attacks and malicious activities, the use of firewall technology is an important milestone toward making networks of any complexity and size secure. Unfortunately, the inherent difficulties in designing and managing firewall policies within modern highly distributed, dynamic and heterogeneous environments might greatly limit the effectiveness of firewall security. It is therefore desirable to automate as much as possible the firewall configuration process. Accordingly,
this work presents a new more active and scalable firewalling architecture based on dynamic and adaptive policy management facilities, thus enabling the automatic generation of new rules and policies to ensure a timely response in detecting unusual traffic activity as well as identify unknown potential attacks (zero-day). The proposed scheme, with a multi-stage modular structure, can be easily applied to a distributed security environment and does not depend on any specific security solutions or hardware/software packages.

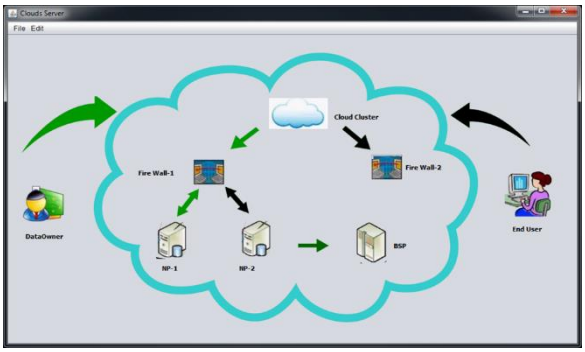
A DECENTRALIZED CLOUD FIREWALL FRAMEWORK WITH RESOURCES PROVISIONING COST OPTIMIZATION.

AUTHORS: Meng Liu, Wanchun Dou and Zhensheng Zhang.

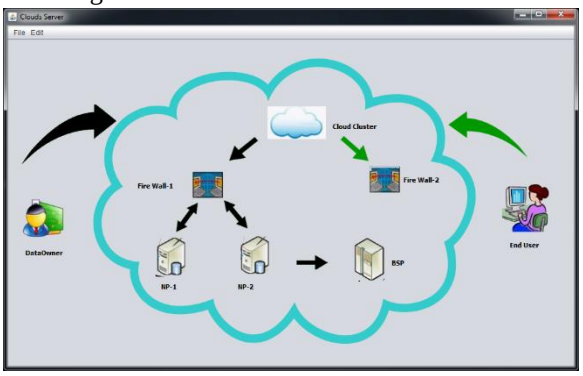
Cloud computing is becoming popular as the next infrastructure of computing platform. Despite the promising model and hype surrounding, security has become the major concern that people hesitate to transfer their applications to clouds. Concretely, cloud platform is under numerous attacks. As a result, it is definitely expected to establish a firewall to protect cloud from these attacks. However, setting up a centralized firewall for a whole cloud data center is infeasible from both performance and financial aspects. In this paper, we propose a decentralized cloud firewall framework for individual cloud customers. We investigate how to dynamically allocate resources to optimize resources provisioning

cost, while satisfying QoS requirement specified by individual customers simultaneously. Moreover, we establish novel queuing theory based model M/Geo/1 and M/Geo/m for quantitative system analysis, where the service times follow a geometric distribution. By employing Z-transform and embedded Markov chain techniques, we obtain a closed-form expression of mean packet response time. Through extensive simulations and experiments, we conclude that an M/Geo/1 model reflects the cloud firewall real system much better than a traditional M/M/1 model. Our numerical results also indicate that we are able to set up cloud firewall with affordable cost to cloud customers.

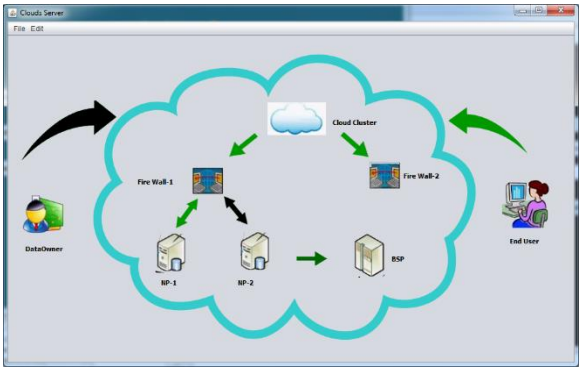
File Store on Cloudlet Platform:



User Login Firewall Authentication:



Firewall Access:



EXISTING SYSTEM

The conventional ORO is a NP Complete problem. A DoS attack can target the bottom rules and increase their matching frequency intentionally. Subsequently, ORO has to regularly move the rules up and down causing a great computational cost, delay, and less QoS for legitimate traffic. Thus, running the conventional ORO not only suffers the NP-Complete problem but also cannot handle the attacked rule problem in the ordering process. Therefore, by dynamically decomposing the macro-FW, not only the ORO challenges are solved but also every cloudlet has its customized rules, treating the traffic locally, without other cloudlets intervention.

DISADVANTAGE

- Difficult to establish trust for data providers in the network; that is, it is difficult to stop people acting as rogue providers.
- Low FireWall Security.
- Serve false data across the network or disrupt the network in some way.

FUTURE WORK

Enhance up the firewall packet processing time up to 95% compared to the conventional solutions, only after four firewall decomposition operations. Moreover, we have been able to show that CODO is able to adaptively scale in/out firewalls with traffic deviation while preserving firewall rules integrity.

CONCLUSION

Firewall rules can be ordered adaptively to avoid performance degradation due to traffic changes. This is commonly referred to as the optimal rule ordering (ORO) problem. Updating the rule ordering dynamically can be costly with respect to the new traffic characteristics. Conventional ORO approaches consider the rule set as constant, or static in a particular firewall. Besides, the rule set may be duplicated and shared in a distributed firewall environment. Typically, it is assumed that firewall policies cannot be shared across domains due to containing confidential information. Accordingly, conventional approaches do not consider cross-domain traffic to export sets or subsets of rules outside the firewall. This

can limit the extensibility of their approach to modern networks employing Network Functions Virtualization (NFV) and software defined networking (SDN).

REFERENCES

[1] AX. Liu, AR. Khakpour, JW. Hulst, Z. Ge, D. Pei, and J. Wang," Firewall fingerprinting and denial of firewalling attacks," IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1699-1712, 2017.

[2] K. Salah, K. Elbadawi, and R. Boutaba," Performance modeling and analysis of network firewalls," IEEE Transactions on Network and Service Management, vol. 9, no. 1, pp. 12-21, 2012.

[3] H. Hamed and E. Al-Shaer," Dynamic rule-ordering optimization for high-speed firewall filtering," In Proceedings of the 2006 ACM Symposium on Information, computer and communications security, pp. 332- 342, 2006.

[4] A. De Santis, A. Castiglione, U. Fiore, and F. Palmieri," An intelligent security architecture for distributed firewalling environments," Journal of Ambient Intelligence and Humanized Computing, vol. 4, no. 2, pp. 223- 234, 2013.

[5] P. Manuel," A trust model of cloud computing based on Quality of Service," Annals of Operations Research, vol. 233, no. 1, pp. 281-92, 2015.

[6] Q. Duan and E. Al-Shaer," Traffic-aware dynamic firewall policy management: techniques and applications," IEEE Communications Magazine, vol. 51, no. 7, pp. 73-79, 2013.

[7] A. Shameli-Sendi, Y. Jarray, D. Migault, M. Pourzandi, and M. Cheriet," Firewall Rule Set Composition and Decomposition," U.S. Patent Application No. 16/488,469., 2019.

[8] M. Liu, W. Dou, S. Yu, and Z. Zhang," A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 3, pp. 621-631, 2015.

[9] K. Salah, P. Calyam, and R. Boutaba," Analytical model for elastic scaling of cloud-based firewalls," IEEE Transactions on Network and Service Management, vol. 14, no. 1, pp. 136-46, 2016.

[10] B. Varghese, R. Buyya," Next generation cloud computing: New trends and research directions," Future Generation Computer Systems, vol. 79, pp. 849-61, 2018