A Firewall Architecture to Enhance Performance of Enterprise Network

Hailu Tegenaw
HiLCoE, Computer Science Programme, Ethiopia
Commercial Bank of Ethiopia, Ethiopia
hailutegenaw@yahoo.com

Mesfin Kifle
HiLCoE, Ethiopia
Department of Computer Science, Addis Ababa University, Ethiopia
kiflemestir95@gmail.com

Abstract

The performance of an enterprise network is affected not only by its protocol specification, its communication channel, design capacity and architecture of the firewall but also by its implementation and traffic management. Firewall is a perimeter security solution that is useful for addressing network traffic. It introduces a single point through which all traffic passes and as a result it creates performance bottleneck on enterprise network by increasing latency, reducing bandwidth and throughput.

The challenges of firewall architecture on enterprise network performance and the proposed solution to enhance it are presented in this paper. Literature review and simulated experiment are employed to study the practice in firewall configuration and management, firewall security and network performance. The stateful firewall architecture is studied and redesigned into three layers or modules: The application identification and control module, content awareness and filtering module, and enforcement module integrated with traffic optimization to accommodate the applications performance and security requirement of the enterprise network.

The application identification features is tested using OPNET for efficient application identification. Its performance is then compared with a sample firewall system based on scenarios to meet the temporal quality of service requirement under DDoS envision. We have achieved firewall performance improvements of 94.4% on CPU utilization, 98.9% on throughput, and 69.20% on queue delay against the base scenario. We also achieved performance improvement of 49.23% on servers task processing and 54.35% on DB query response against the base scenario.

Keywords: Application Identification; Emerging Applications; Perimeter; Optimization; Performance

1. Introduction

Performance degradation of a firewall adversely affects service level and quality of enterprise network. Firewalls have become crucial network elements and have evolved over the last couple of decades from simple packet filtering as add-ons to the stateful packet filtering firewall [6]. It controls access and traffic between networks employing different security [1, 2, 3]. Firewalls use service control, direction control, user control, and behavior control to control access and enforce security policy. Enterprise Firewalls technology is classified into three types. These are Packet-filtering firewalls, Application-level gateways, and stateful packet filtering.

Literature reviewed and domain experts asserted that the sources of firewall performance degradations are the quality of firewall policy configured the number and order of the rule which are implemented, increased level of security requirements, methodology in implementing the firewall in the enterprise network, emerging attack vectors, TCP/IP packet overhead, the underlying hardware and software architecture.

The solution proposed intents that the above mentioned challenges can be best taken care of and solved by using firewall architecture that manages users and applications rather than port. Unlike the stateful firewall architecture that is mainly on port

based traffic classification, the proposed architecture provides policy based visibility and control over the application. It will use multifactor approach where the policy check determines how to treat the application and related functions. Therefore, designing a firewall architecture that has application identification and control, optimization traffic, and manages bandwidth based on policy rule sets are worth considered to enhance the performance of a firewall.

The methodology used in order to verify critical problems and to validate the solution were literature review, interview, questionnaires and experimenting the proposed architecture using OPNET simulation.

2. Background

The explosive growth of the Internet, computing dynamics and emergent enterprise applications, coupled with the increasing sophistication of attacks, are introducing two main problems in enterprise networks in general and stringent demand on firewall performance in particular [4, 9].

The first problem is due to a change in posture of the security perimeter. The perimeter security model was the dominant security model for almost two decades. The concept of a "perimeter" is becoming more difficult to define when the concepts of inside and outside change rapidly and fluidly.

The IT perimeter is diluted from a well-defined set of points to a mesh of undetectable devices accessing and penetrating corporate network. The perimeter is now becoming fuzzy. Any sort of computing device may become the perimeter itself [5, 8].

The traditional security perimeter model is becoming more difficult to apply. As an integral part of enterprise infrastructure, firewalls are strongly affected by the development and deployment of new communication paradigm and applications. In recent times there has been a rise in the use of various emerging applications which differ in many aspects from known applications.

The second problem is enterprise firewalls are not fully application aware. Existing firewalls are not able to support the performance requirement of the existing and emerging applications as the trend of the security perimeter is transformed to system perimeter. A firewall is still positive security model and yet unaware of its enterprise applications [5, 7].

The preliminary literature survey and domain experts experience demonstrate that the existing firewall suffers from several shortcomings and has negative impact on performance. Unlike the stateful firewall architecture that is mainly on port based traffic classification methods, the proposed architecture provides policy based visibility and control over the application.

3. Related Work

Over the course of this research, there has been not much resource available that emphasizes the architectural aspect of the firewall. There have been some works done that dictate the trends of the current firewall evolutions.

Pohlmann and Cothers [6] presented the basic elements of a firewall system. It explains how technical security mechanism is implemented for firewall elements, what options for assuring security exist, how those options work and their limitations. The firewall architecture proposed by the authors consists of the following modules: Active Integration and Enforcement, Analysis, Decision, Processing for security related events, Authentication, Rule set, and Logbook Security Management System. Further the authors stated that a firewall should be designed and implemented with maximum performance in mind and it is not a one time issue.

Young [7] proposed a definition for next generation firewall based on a review of the traditional firewall such as the packet filtering, application proxies and stateful packet filtering challenges and found out that:

- The current firewall is not intelligent enough to be fully application aware to protect breaches and attacks happening over the network.
- Firewall rules are not permanent and need frequent updates which are carried out manually and become cumbersome activities.

- The position of the rule in the rule set can have an impact on the performance of the firewall under denial of services (DoS) type of attacks.

4. The Proposed Firewall Architecture

The proposed firewall architecture is shown in Figure 1. It shows the conceptual model that indicates the whole participating components. Thus it consists of three modules: the application identification module, content filtering and enforcement modules.

4.1 Application Identification Module

It consists of application policy detection and encryption, application protocol decoding, application signature and heuristics classification. It uses multifactor approaches to determine the identity of the application on the network regardless of ports and protocols using application protocol detection and decryption, application protocol decoding, application signature and behavioral analysis.

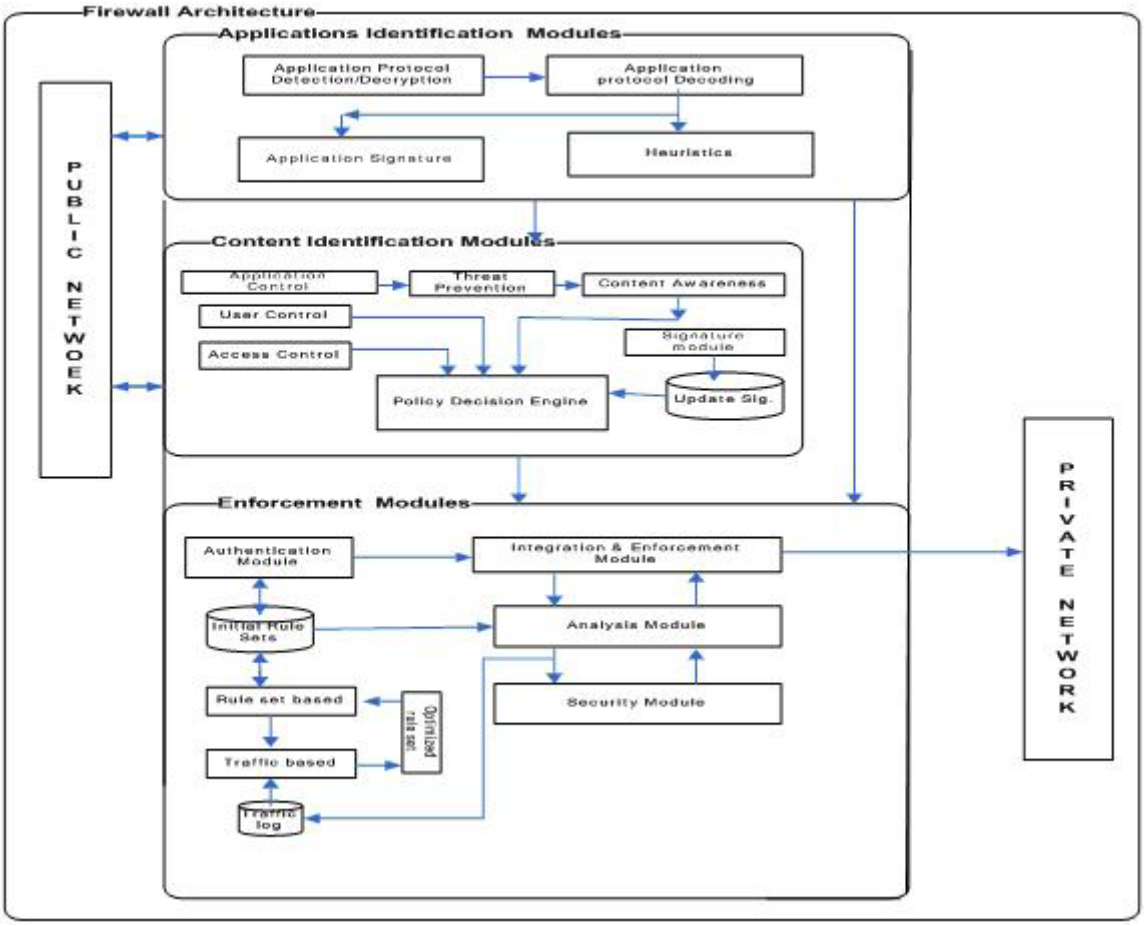

Figure 1: The Proposed Conceptual Firewall Architecture

4.2 Content Awareness Module

It is used to prevent real-time threat regardless of the application traffic. It determines what information is contained in a specific file, folder, application or other data store, whether that information is in use or in transit. It provides granular control on application usage and behavior and it gives control of what leaves and enters to enterprise network on applications and users rather than traditional methods of port and protocol. The content awareness also applies new sources of intelligence to existing techniques such as correlation, context and content.

The proposed data flow and packet inspection engine (Figure 2), which is part of the policy decision, has been designed with a feature to process packets for signature, heuristic and encryption and decryption for application. It is unlike the traditional firewall data flow and inspection engine that uses IP address and

port numbers as a way of enforcing policies. Application signature mapping is a precise method of identifying the application that issued traffic on the network. Signature mapping operates at application layer and inspects the actual content of the payload. Known applications are mapped to specific patterns in the application identification database. The payload of the first few packets is compared to the content of the database. If the payload contains the same patterns as an entry in the database, the application of the traffic is identified as the application mapped to that pattern in the database entry.

4.3 Enforcement Module

It is used to manage the various services required of the firewall including, the rule sets, authentication, analysis, security and traffic optimization.

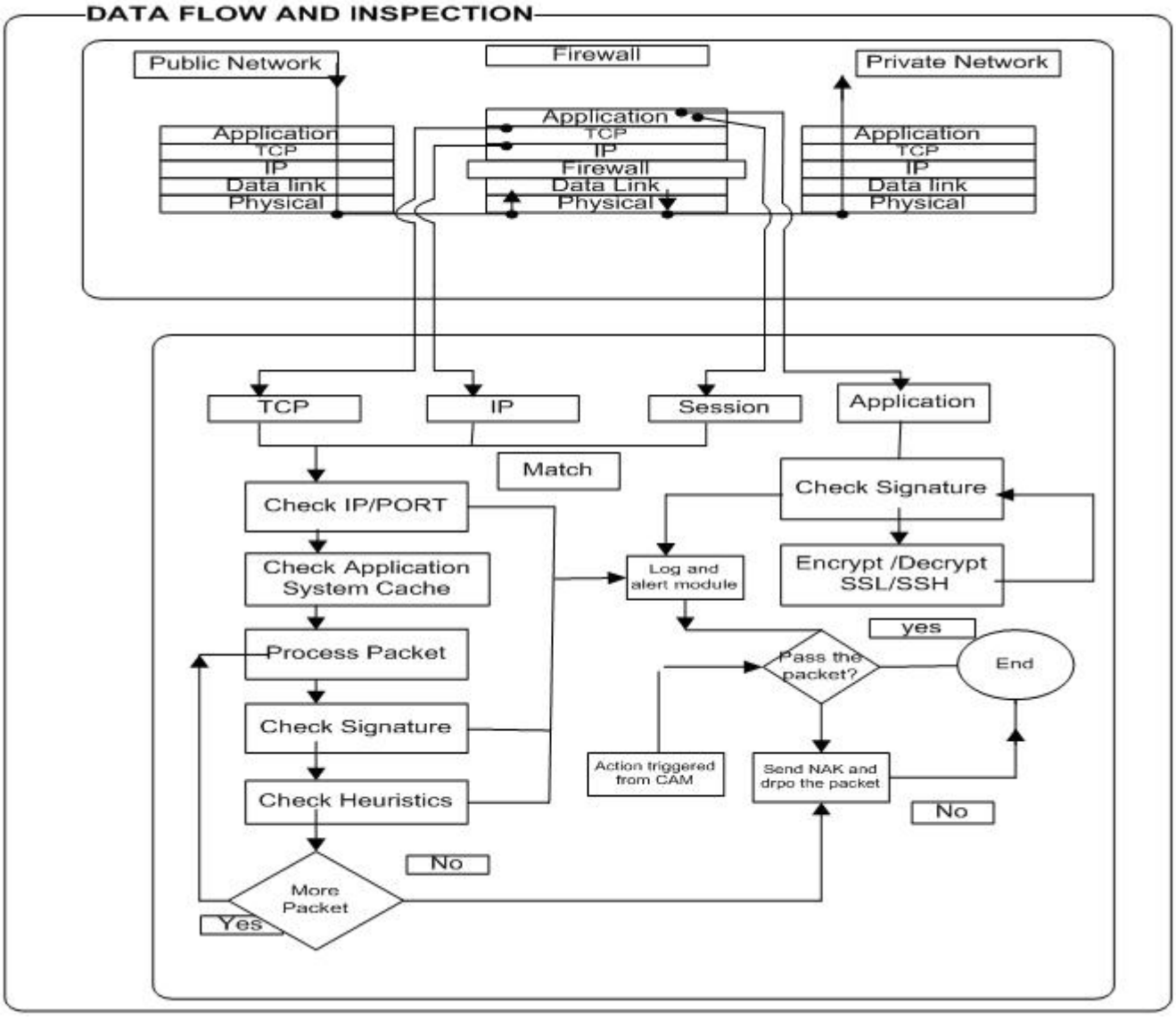

Figure 2: Packet Inspection Engine for Conceptual Firewall Architecture

5. Implementation

To test some features of the proposed architecture we used a simulated environment using Optimized Network Engineering Tools (OPENT). OPNET is a comprehensive tool capable of simulating large communications networks with detail protocol modeling and performance analysis. For the implementation we run three scenarios: the base scenario, attack scenario and application identification scenario.

5.1 Base Scenario

A base scenario is considered as shown in Figure 3. We have server setups at one end with Database Server, Email Server, FTP Server and Web Server, and on one side of the network we have 25 LAN users. The LAN users are configured with 100BaseT settings and it is terminated at the LAN router, In addition to this, we also have a group of 25 remote users.

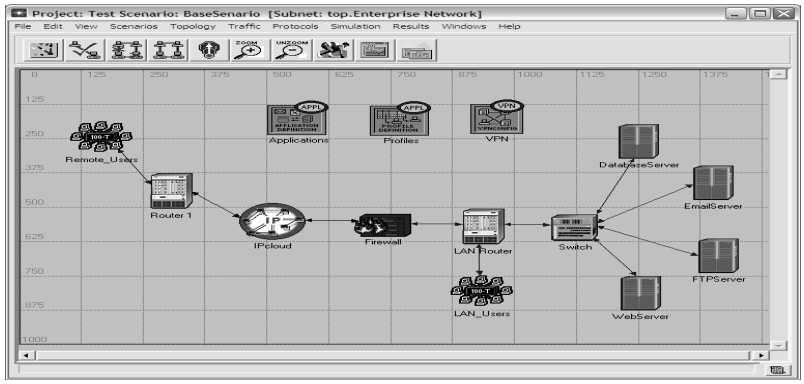

Figure 3: Base Scenario

5.2 Attack Scenario

In attack scenario (Figure 4), all configurations remain the same as they are in the baseline scenario. In addition to this we assume that 50,100 and 200 attackers have got control of a botnet and succeeded to pass through the firewall. It is out of the scope of this analysis how the attackers get success in controlling the botnet and penetrating the firewall. Ultimately, the attacker launches DDoS attacks on the Database Server.

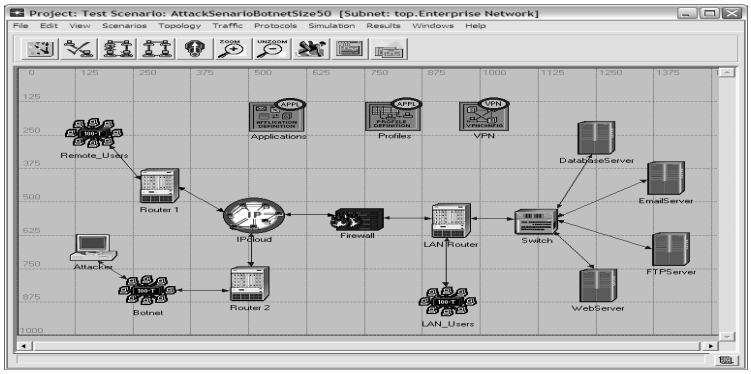

Figure 4: Attack Scenario: Botnet Size 50

5.3 Application Identification Scenario

In Application Identification Scenario (Figure 5), all configurations remain the same as they are in the Attack Scenario. In addition to this we assume that load balancer - f5-BIGip has a feature to identify application traffic and succeeded to control application identification that passes through it. The load balancer is assumed to be part of the firewall even if it is not integrated.

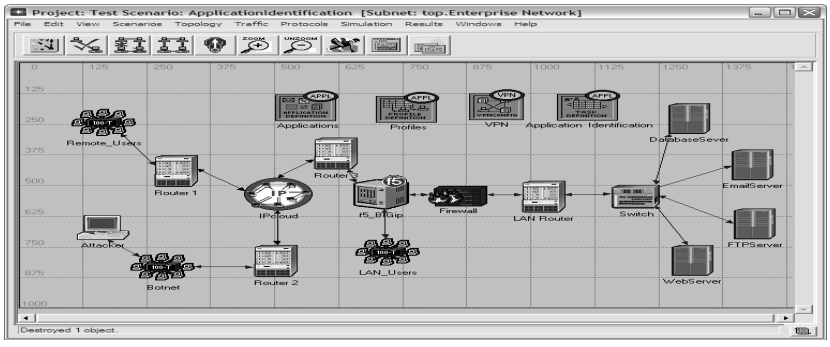

Figure 5: Application Identification Scenario

6. Results and Discussion

In our simulation analysis, we considered a few performance metrics in analyzing the network traffic, its flow and aggregations. As described below, we also obtained firewall and server side parameters to analyze the effect on performance. In order to observe the effect, 50, 100 and 200 botnets sizes are considered. We observed the parameters with respect to simulation time of one hour.

6.1 Firewall Performance

The firewall performance is assessed in terms of CPU utilization (%), throughput (packet/sec), TCP delay (sec), and Queuing delay (sec).

In analyzing CPU utilization, it is observed that the CPU utilization is minimal in the Application identification scenario, whereas it increases manifold under attack scenario.

Moreover, it is found that increasing botnet size has proportional effect on the CPU utilization, i.e., CPU utilization is also increased. This is because as more traffic is sent by the attacker to exhaust the service, more processing is required to process incoming requests by the firewall. As a result, the firewall is incapable to effectively responding to the legitimate requests. In this analysis, CPU utilization of the firewall has increased more than 50 times (percentage utilization) at peak value when the server is under DDoS attack with 50 botnets as compared to the application identification scenario.

Additionally, we found that the CPU utilization of 1.5% is experienced by the firewall under attack scenario with 200 botnets as compared to 0.25% and 0.01% under baseline scenario and application identification scenario, hence showing 6 and 150 times increase in the CPU utilization respectively.

While evaluating *throughput (packet/sec),* for botnet size 50, the firewall interface throughput is not very high when legitimate or allowed applications communicate under the application identification scenario. On the other hand, under the attack scenario, it is a shot on the load with increased connection request. Hence, we inferred that the botnet size creates more impact on the firewall.

TCP active delay is also analyzed for various scenarios. The TCP traffic on the interface of the firewall continued to grow as the number of attack botnets are growing. The application identification scenario still exhibits the least TCP delay.

Having analyzed the point to point queuing delay of the firewall interface for the three scenarios, it was observed that, the queuing delay is less under the application identification scenario and this indicates that the performance of the firewall due to queue delay is improved by 69.20% under the application identification.

6.2 Server Performance

The server performance is assessed in terms of *task processing time and response time.*

In the experiment we conducted on the web server's performance, the task processing time greatly increased under attack scenario as compared to the baseline scenario and it shows minimum task processing under application identification scenario. The server is exhausted by sending huge amount of attack traffic for which it has to perform requested tasks. As a result the average processing time per task increased degrading services for legitimate requests.

Similarly the response time of the mail server is not very high when legitimate users communicate under base scenario. On the other hand, when botnet attack strikes under Attack Scenario, we observed a shoot on the response time with an increase in request. It is found that the increased botnet size makes greater impact on the server's load. However, the response time has been improved by 50% under the application identification scenario that allows legitimate applications and users.

7. Conclusion and Future Work

In this paper, we have presented a novel firewall architecture that bases on the new feature application identification and incorporates modules that the stateful firewall architecture does not constitute.

The conceptual firewall architecture is built with a center of performance requirement on the enterprise network for the emerging application. The performance test of the firewall architecture shows that the firewall and enterprise server has exhibited performance improvement.

In general, the proposed firewall architecture enables:

- Application Identification: the architecture is proven to have accurate traffic identification through task definitions and load balancer features successfully maintained.
- Performance improvement on Firewall: the performance requirement of the applications is achieved through application identification and control, CPU utilization, throughput, task processing and memory queue delay has improved.
- Performance improvement on servers: There is an improvement on the database query response time and email download.

In the future the prototype can be modified by introducing more modules and/or upgrading existing ones in the conceptual firewall architecture to support:

- Content Awareness: the module that encompasses the intrusion prevention system may be further studied for advanced persistent threat mitigation and appropriate intrusion detection engine or algorithms and other modules may be built.
- Application Identification and Control Technology: another possible extension is also to consider efficient application and its signature identification technology.
- Integration methodology for Rules set Optimization: better integration of the rule set on the existing firewall architecture as a firmware and developing integration methodology may be considered as future improvement on the firewall performance.
- Firewall Hardware Platform: better hardware platforms and network processor design can be studied to further enhance and accommodate the performance and security requirement of the proposed conceptual firewall architecture to support the emerging application performance and security requirements.

References

[1] Richard E. Smith, “Internet Cryptography”, 2000.

[2] Paul Ferguson and Geoff Huston, “Quality of Service Delivering on the Internet and in Corporate Networks”, 1998.

[3] John Sherwood, Andrew Clark, and David Lynas, “Enterprise Security Architecture”, White Paper.

[4] Diana Keley, “Next-Generation Firewall: From Business Problem to Technical Solution”, White paper, 2013.

[5] IBM Systems, IPS-evolving-to-remain relevant, http://www.techrepublic.com/resource library/ Webcasts/ips-evolving-to remain relevant/, 2013.

[6] Norbert Pohlmann and Tim Cothers, “Firewall Architecture for the Enterprise”, 2004.

[7] Greg Young, “Defining the Next Generation Firewall”, White Paper, 2009.

[8] William Stallings, “Cryptography and Network Security”, Fourth Edition, 2012.

[9] John Day, “Patterns in Network Architecture”, 2008.