Future Firewall Security Enhancements

K. K. C. D Rathnayake¹, N. H. De Silva ² & D. J Amarasinghe³
Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

Abstract - Firewalls protect your office and home computers or network systems from outsiders. This paper contains about network security implementations. Firewalls protect you from dangerous softwares that can intrude your systems or from advanced hackers. Nowadays online security is concerned as top priority of the computer users. Firewalls provide you the necessary safety protection for devices. Application proxy firewall is a form of computer network packet filtering searches the data part of packet when it passes as a point. It searches for protocol non-compliance, spam and viruses for the validations. Firewall understands certain protocols. Therefore signatures or rules can specifically be addressed. Stateful Firewall is also a computer network which keeps track of the state of network connections and is able to hold significant attributes of each connection in firewalls. By keeping track of the connection state, Stateful firewalls provide the efficiency in terms of packet inspection. This analysis is also broader than common technologies because it combines techniques such as protocol anomaly detection and signature scanning, traditionally available in virus protections.

Keywords: Application Proxy Firewall, Stateful Firewall, Connection state, Packet Inspection

I.INTRODUCTION

When designing a network, network security will be considered mainly to protect the network from threats and viruses and network will be protected from unauthorized users. More firewalls that are sophisticated block traffic from outside to the inside, but this permits users to communicate with outside.

Network firewalls are devices or systems that control the flow of traffic between networks working in different security. The network traffic flow is controlled according to a firewall policy. The filtering decision is based on a firewall policy defined by network administrator. For each type of network traffic, there are one or more different rules. Every network packet, which arrives at firewall, must be checked against defined rules until first matching rule is found. The packet will either be allowed or banned access to the network, depending on the action which is taken in matching.

Figure 1: An illustration of how firewall works

Application Proxy Firewall

Application proxy Firewall is a next generation technology that protects network resources by filtering messages at the application layer. Just like a proxy server or cache server, a proxy firewall acts as an intermediary between in-house clients and servers on the Internet. The difference is that in addition to intercepting Internet requests and responses, a proxy firewall also monitors incoming traffic for layer 7 protocols, such as HTTP and FTP. In addition to determining which traffic is allowed and which is denied, a proxy firewall uses Stateful inspection technology and deep packet inspection to analyze incoming traffic for signs of attack. Proxy firewalls are considered to be the most secure type of firewall.
because they prevent direct network contact with other systems.

Due to proxy firewall has its own IP address; an outside network connection will never receive packets from the sending network directly. Having the ability to examine the entire network packet rather than just the network address and port number also means that a proxy firewall will have extensive logging capabilities. They are valuable resource for security administrators who are dealing with security incidents [2].

Application proxy firewalls function by determining whether a process should accept any given connection and accomplish their function by getting into sockets to filter the connections between the application layer and the lower layers of the OSI model. Application proxy firewalls that getting into socket are also referred to as socket filters. Application proxy firewalls work much like a packet filter but application filters apply filtering rules to allow or block on a per process basis instead of filtering connections on a per port basis. Generally, prompts are used to define rules for processes that have not yet received a connection. It is rare to find application firewalls not combined or used in conjunction with a packet filter. Further filter connections by examining the process ID of data packets against a set for the local process involved in the data transmission. The extent of the filtering that occurs is defined by the provided rules. Given the variety of software that exists application proxy firewalls only have more complex rule for the standard services, such as sharing services. These per process rules have limited power in filtering every possible association that may occur with other processes [3].

The goal of the proxy approach is to create a single point that allows a security to assess threat levels represented by application protocols and put error detection, attack detection and validity checking in place. The added security offered by a proxy firewall has its drawbacks, however. Because a proxy firewall establishes an additional connection for each outgoing and incoming packet, the firewall can become a bottleneck, causing a degradation of performance or becoming a single point of failure. Additionally, proxy firewalls may only support certain popular network protocols, thereby limiting which applications the network can support.

Figure 2: Diagram of Application Proxy Firewall

The benefits of Application Proxy Firewall

The best way to describe the benefits of application proxy firewalls is to look at the shortcomings of other firewall technologies. There are three general classes of firewall:

- Packet filtering firewalls
- Stateful inspection firewalls
- Proxy firewalls or application-level

All three analyzed packets against a rule base and decide to block or allow packets through based upon those rules but it is the level of analysis that differentiates them. Packet filter, or network layer, firewalls operate at Layer 3 of the OSI (Open System Interconnection Reference) model and separate an organization's network from other domains by standing between incoming and outgoing network traffic.

- The firewall inspects each packet’s header information and blocks or allows it through by comparing its source and destination addresses, network ports, and protocol type against a set of rules.

These firewalls make a decision for each packet based on the information contained in that individual packet and are not aware of any traffic patterns or data flows. This makes them susceptible to masking attacks and other network protocol-based attacks. In order to evaluate an individual packet in the larger context of a network communications session

- Application Proxy Firewalls record all connections passing through them by operating at Layer 5 of the OSI model. By keeping track of the state of network connections they have much more complete information and can reject packets that don’t match a known connection state.
While Stateful firewalls can block many types of attacks at the network protocol level, they cannot inspect the actual load contained in each packet as it travels between the application and its users. This allows malformed or unexpected data to reach and exploit vulnerabilities in a particular application such as a buffer overflow or SQL injection. Enter application proxy firewalls, which operate at Layer 7 of the OSI model and have advanced inspection capabilities. These firewalls do not allow any packets to directly pass between an application and the user. Instead all traffic is intercepted and passed through a proxy connection. This means that there are then two connections in place: one between the user and the proxy server and another between the proxy server and the application with the proxy receiving, inspecting, and forwarding all traffic bi-directionally between the client and application.

This places the firewall in the middle of the logical Connection and allows it to examine the traffic, including its load, for any signs of malicious activity at the application level.

- Unlike a packet filter an application proxy understands the application it is protecting and can block forbidden commands such as dangerous SQL commands or malformed requests such as attempts to cause a buffer overflow.

However, data leaving the network can be analyzed and any sensitive data intercepted before it is output to the user. All this detailed knowledge of network traffic headers and loads can also be logged to provide better auditing.

- New threats to an application can be tackled by changes to the firewall’s rule set.
- Direct Connections between internal and external hosts are disallowed
- User level authentication is supported
- The application commands are analyzed inside the payload portion of the data packets [4].

This is far quicker and easier than making changes to the application itself. Other advantages include providing anonymity for systems behind the firewall while isolating security checks in a separate process and memory space. This level of filtering provides an extra layer of security to protect data, business logic and applications from flaws in their design [5].

Stateful Inspection Firewall

In computing, a type of firewall that attempts to track the state of network connections when filtering packets. The Stateful firewall’s capabilities are somewhat of a cross between the functions of a packet filter and the additional application-level protocol intelligence of a proxy. Stateful inspection, also known as dynamic packet filtering, is a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall [6].

Stateful inspection has largely replaced an older technology, static packet filtering. In static packet filtering, only the headers of packets are checked, which means that an attacker can sometimes get information through the firewall simply by indicating "reply" in the header. Stateful inspection, on the other hand, analyzes packets down to the application layer. By recording session information such as IP addresses and port numbers, a dynamic packet filter can implement a much tighter security posture than a static packet filter can. Stateful inspection monitors communications packets over a period of time and examines both incoming and outgoing packets. Outgoing packets that request specific types of incoming packets are tracked and only those incoming packets constituting a proper response are allowed through the firewall. In a firewall that uses Stateful inspection, the network admin can set the parameters to meet specific needs [7].

Figure 3: Diagram shows how Stateful Firewall works
How Stateful Firewall works

With a Stateful firewall these long lines of configuration can be replaced by a firewall that is able to maintain the state of every connection coming through the firewall. Operationally, traffic that needs to go through a firewall is first matched against a firewall rules list If the packet type is allowed through the firewall then the Stateful part of the process begins [8].

The easiest example of a Stateful firewall utilizes Traffic that is using the Transport Control Protocol (TCP). This is because TCP is Stateful to begin with. TCP keeps track of its connections through the use of source and destination address, Port number and IP flags. A connection will begin with a three way handshake (SYN, SYN-ACK, ACK) and typically end with a two way exchange (FIN, ACK). For a Stateful firewall this makes keeping track of the state of a connection rather simple.

An initial request for a connection comes in from an inside host (SYN). This will initiate an entry in the firewall's state table. If the destination host returns a packet to set up the connection (SYN, ACK) then the state table reflects this. Finally, the initial host will send the final packet in the connection setup (ACK). This will finalize the State to establish. Once a connection is maintained as established communication is freely able to occur between hosts. With TCP, this state entry in the table is maintained as long as the connection remains established (no FIN, ACK exchange) or until a timeout occurs. The harder part of the operation of a Stateful firewall is how it deals with User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP).

This is because neither of these protocols are connection-based like TCP. With UDP, the firewall must track state by only using the source and destination address and source and destination port numbers. Of course this is not quite as secure as the state tracking that is possible with TCP but does offer a mechanism that is easier to use and maintain with than ACLs. UDP and ICMP also bring some additional state tracking complications.

This is because UDP utilizes ICMP for connection assistance (error handling) and ICMP is inherently one way with many of its operations. ICMP itself can only be truly tracked within a state table for a couple of Operations. These operations have built in reply packets, for example, echo and echo-reply. For its other one way operations the firewall must maintain a state of related. This state is used when an ICMP packet is returned in response to an existing UDP state table entry. The Stateful Firewall spends most of its examining packet information in transport layer and lower. However, it offers more advanced capabilities by targeting vital packets for layer 7 (application layer) [9].

Advantages of Stateful Firewall

- These will typically offer much higher performance than
- Communication session. Therefore, a higher level of protection proxies,
- Stateful Inspection provides a greater level of security control by enforcing security policies at the "application socket" or port layer as well as the protocol and address level.

Incoming traffic can be blocked. However, all the incomings can be blocked, yet still have replies to requests from the client come in without the complex rule sets that need for a static packet filter. This is where Stateful technology wins over static packet filters. Stateful Firewall can provide much more granularity in securing a network. Just by issuing several simple sanity checks we can offload a great deal of unnecessary work that our flow-based firewall would have had to do. In addition the ability to track sessions can also allow us to track unusual activity, such as a system making hundreds of connections unexpectedly. This is useful for determining things such as virus outbreaks or unauthorized access/attempts to a system [10].

II. BACKGROUND AND RELATED WORKS

A firewall can prevent unauthorized access to a network and it can be either a hardware or software device. They can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All data entering or leaving the Intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria. Generally, firewalls are configured to protect against unauthenticated interactive logins from the outside world. This helps prevent hackers from logging into machines on the network. Application Proxy Firewall and Stateful Firewall provides more security that other functions, often they provide summaries to the administrator about the type of traffic that has gone through. Therefore there is a certainty that a pure packet comes in.
Firewall Techniques

1. **Proxy server**: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

2. **Packet filters**: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

3. **Application gateway**: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.

4. **Circuit-level gateway**: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking [11].

### III. Solution

A certain protocol or packet can either be blocked or allowed due to the process, which is not good due to no certainty that the packet goes in. From the perspective of the port number, a data read message looks like a firmware update message. If the date read messages are allowed to pass through a traditional firewall which means programming messages will be allowed to pass through. This is a serious security issue. Clearly the firewall needs to dig deeper into the protocols, packets to understand exactly what the protocol is being used for and that is exactly what Application Proxy Firewall does. After the traditional firewall rules are applied, the firewall inspects the content of the contained messages and applies more detailed rules for example, Application proxy firewall determines if the Modbus message is a read or a write message and then drops all write messages. Good firewalls can also sanity check traffic for strangely formatted messages or unusual behaviors. These sorts of abnormal messages can indicate traffic created by a hacker trying to intrude, these things can be avoided in Application Proxy Firewall and Stateful Firewall if have been applied as functions. There is a guarantee that a safe packet goes through without any virus and infections and destructive intruders who are trying to hack the system will be restricted. Especially Application Proxy Firewall provides more security that other Firewalls which controls traffic and allows or blocks network packets passing to the network. This prevents direct connections between systems on either sides and make it harder for the attackers to find out where the network is [12].

### IV. Conclusion

Firewalls are being asked to fill a larger and more varied role in network security these days than several years ago. One of the more recent innovations in firewall technology is the application of deep packet inspection or DPI. Deep Packet Inspection can be seen as the integration of Intrusion Detection (IDS) and Intrusion Prevention (IPS) capabilities with traditional state-full firewall technology. And also firewall clustering explain expanding of the firewall in a synchronized manner. Backup firewall system will be implemented in case of unexpected firewall crash.

### V. Future Work

Internet security has become a major concern as many businesses now make their transactions online. Our team is planning to develop a new security firewall with specific features included and mainly concerned about security and speed. Therefore the internet must be secured in networks for the business to be done. The use of firewalls in network systems as a result cannot be accessed. Large organizations and companies can now prevent hackers and unrestricted access to their database or some important information by the use of firewall.

### VI. Acknowledgment

This research was supported by Sri Lanka Institute of Information Technology (SLIIT) and the Lecturer Mr.Dhishan Dhammearatichi. We would like to express our very great appreciation and gratitude to Mr.Dhishan Dhammearatchi for his valuable and innovative suggestions during the planning and development of this research work. His willingness to give his time so generously has been very much appreciated. We would also like to thank our colleagues K.K.C.D Rathnayake, N.H De Silva, D.J Amarasinghe who provided their best to complete the research.
REFERENCES


