Planning Network based-firewalls

Team number: 3

Team Members:

2010030046: E.Pravallika

2010030168: Tahseen Begum

2010030445: P.Keerthana

Question And Answers

1. Explain What is Firewall?

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices that is configured to permit or deny computer applications based upon a set of rules and other criteria.

Firewalls can be implemented in either hardware or software or a combination of both.

1. How does a firewall protect data?

Data transmitted over the internet has several categories of metadata associated with it. An individual packet has a source IP address and a destination IP address, which says where it's coming from and where it's going. It's also directed toward one of many ports, each of which is meant for different purposes.

Firewalls inspect this metadata and either block or allow it. For example, firewalls may be used to block a device from receiving any traffic originating from an external network, block off unused ports, or block all traffic except packets coming from a list of pre-approved IP addresses.

1. What are the types of firewalls?

Four Types of Firewalls

Packet filtering firewalls. Packet filtering firewalls are the oldest, most basic type of firewalls. ...

Circuit-level gateways. ...

Stateful inspection firewalls. ...

Application-level gateways (proxy firewalls)

1. What is the main function of a firewall?

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

1. How do firewalls block traffic?

Firewalls rely on either Stateful Packet Inspection (SPI) or Deep Packet Inspection (DPI) to analyze whether data packets passing through a network contain benign or malicious content. Traditional firewalls relied on a database of known threat signatures to spot potential threats, but modern firewalls use machine learning & AI to determine if a data packet’s behavior is consistent with the behavior of known cyber threats - allowing them to catch never before seen exploits.

1. Do firewalls stop hackers?

Firewalls close off many of the potential backdoors & security vulnerabilities that hackers use to breach networks. However, firewalls cannot stop users from clicking malicious links, prevent physical network breaches, or stop insider attacks. Firewall appliances play a major role in thwarting hackers but should be part of a layered network security posture.

1. At which OSI layers do firewalls work?

Firewalls work at layers 3 (network), 4 (transport), and 7 (application).

1. What information does the Stateful Firewall maintain?

A Stateful Firewall maintains the following information in its state table:

Source IP address

Destination IP address

IP protocol, like TCP or UDP

IP protocol information such as TCP/UDP port numbers, TCP sequence numbers, and TCP Flags

1. What is Proxy?

A software agent that acts on behalf of a user. Typical proxies accept a connection from a user, decide as to whether or not the user or client IP address is permitted to use the proxy, perhaps do additional authentication, and then complete a connection on behalf of the user to a remote destination.

1. What is Access Router?

A router that connects your network to the external Internet. Typically, this is your first line of defense against attackers from the outside Internet. By enabling access control lists on this router, you'll be able to provide a level of protection for all of the hosts `behind' that router, effectively making that network a DMZ instead of an unprotected external LAN.

Case study and Implementation of Geometric Efficient Matching Algorithm for Firewalls

Abstract

A firewall is a device that controls the flow of communications across networks of computers by examining their source, destination, and type – and comparing these with predetermined lists of allowed and disallowed transactions. Packet matching in firewalls involves matching on many fields from the TCP and IP packet header. At least five fields (protocol number, source, and destination IP addresses, and ports) are involved in the decision which rule applies to a given packet. With available bandwidth increasing rapidly, effective matching algorithms need to be deployed in modern firewalls to ensure that the firewall does not become a bottleneck, Since firewalls need to filter all the traffic crossing the network perimeter, they should be able to sustain a very high throughput. In this paper, we consider a classical algorithm that we adapted to the firewall domain. We call the resulting algorithm “Geometric Efficient Matching”. The Geometric Efficient Matching algorithm enjoys a logarithmic matching time performance. However, the algorithm’s theoretical worst-case space complexity is O (n4) for a rule-base with n rules. Based on statistics from real firewall rule-bases, we created a perimeter rules model that generates random, but non-uniform, rule bases. We evaluated the Geometric Efficient Matching algorithm via extensive simulation using the perimeter rules model. Geometric Efficient Matching algorithm speed is far better than the naïve linear search algorithms, and it can increase the throughput by an order of magnitude.

1. Introduction

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting outward communication. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria. Firewalls 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, especially intranets. From the fig1 all messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria

1.1 Types of Firewalls:

The International Standards Organization (ISO) Open Systems Interconnect (OSI) model for networking defines seven layers, where each layer provides services that ``higher-level'' layers depend on. In order from the bottom, these layers are physical, datalink, network, transport, session, presentation, and application. The important thing to recognize is that

the lower-level the forwarding mechanism, the less examination the firewall can perform. Generally speaking, lower-level firewalls are faster but are easier to fool into doing the wrong thing. The different firewalls can be developed based on the functionality and requirement.

1.2.1 Packet-filtering firewall

Typically, is a router with the capability to filter some packet content, such as Layer 3 and sometimes Layer 4 information.

1.2.2 Application gateway firewall (proxy firewall)

A firewall that filters information at Layers 3, 4, 5, and 7 of the OSI reference model. Most of the firewall control and filtering are done in software.

1.2.3 Address-translation firewall

A firewall that expands the number of IP addresses available and hides network addressing design.

1.2.4 Host-based (server and personal) firewall

A PC or server with firewall software running on it.

1.2.5 Transparent firewall

A firewall that filters IP traffic between a pair of bridged interfaces.

1.2.6 Hybrid firewall

A firewall is a combination of the various firewalls types.

1.3 Case Study on Network layer and application layer Firewalls

For example, an application inspection firewall combines a stateful firewall with an application gateway firewall. Conceptually, there are two types of firewalls: one is Network layer firewalls and the second is Application layer firewalls. They are not as different as you might think, and the latest technologies are blurring the distinction to the point where it's no longer clear if either one is ``better'' or ``worse.'' As always, you need to be careful to pick the type that meets your needs. It depends on what mechanisms the firewall uses to pass traffic from one security zone to another.

1.3.1 Network layer Firewalls

These generally make their decisions based on the source, destination addresses, and ports in individual IP packets. A simple router is the ``traditional network layer firewall since it is not able to make particularly sophisticated decisions about what a packet is talking to or where it came from. Modern network layer firewalls have become increasingly sophisticated, and now maintain internal information about the state of connections passing through them, the contents of some of the data streams, and so on. One thing that's an important distinction about many network layer firewalls is that they route traffic directly through them, so to use one you either need to have a validly assigned IP address block or to use a ``private internet'' address block Network layer firewalls tend to be very fast and tend to be very transparent to users. a network layer firewall called a screened host firewall'' is represented. In a screened host firewall, access to and from a single host is controlled using a router operating at a network layer. The single host is a highly-defended and secured strong-point that (hopefully) can resist attack.

1.3.2 Application layer Firewalls

These generally are hosts running proxy servers, which permit no traffic directly between networks, and which perform elaborate logging and auditing of traffic passing through them. Since the proxy applications are software components running on the firewall, it is a good place to do lots of logging and access control. Application layer firewalls can be used as network address translators since traffic goes in one ``side'' and out the other, after having passed through an application that effectively masks the origin of the initiating connection. Having an application in the way in some cases may impact performance and may make the firewall less transparent. Modern application layer firewalls are often fully transparent. Application layer firewalls tend to provide more detailed audit reports and tend to enforce more conservative security models than network layer firewalls

1.4 Different Firewall Techniques:

1.4.1 Packet filters:

Look at each packet entering or leaving the network and accept or reject 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. Packet-filtering firewalls work primarily at the Network Layer of the OSI model. Firewalls are generally considered Layer 3 constructs. However, they permit or deny traffic based on Layer 4information such as protocol, and source and destination port numbers. Packet filtering uses ACLs to determine whether to permit or deny traffic, based on source and destination IP addresses, protocol, source, and destination port numbers, and packet type. Packet-filtering firewalls are usually part of a router firewall.

1.4.2 Application gateway:

Applies security mechanisms to specific applications, such as FTP and telnet servers. This is very effective but can impose a performance degradation.

1.4.3 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.

1.4.4. Proxy server:

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

2. Existing Algorithms

Most modern firewalls are stateful. This means that after the first packet in a network, flow is allowed to cross the firewall, all subsequent packets belonging to that flow, and especially the return traffic, are also allowed through the firewall. This statefulness has two advantages. First, the administrator does not need to write explicit rules for return traffic—and such return-traffic rules are inherently insecure since they rely on source-port filtering. So stateful firewalls are fundamentally more secure than simpler, stateless, packet filters. Second, state lookup algorithms are typically simpler and faster than rule match algorithms, so statefulness potentially offers important performance advantages. Firewall statefulness is commonly implemented by two separate search mechanisms: (i) a slow algorithm that implements the ―first match‖ semantics and compares a packet to all the rules, and (ii) a fast state lookup mechanism that checks whether a packet belongs to an existing open flow. In many firewalls, the slow algorithm is a naive linear search of the rule base, while the state lookup mechanism uses a hash table or a search tree. There are strong indications that commercial firewalls use linear search for the slow rule-match as well. Moreover, the standard advice for improving firewall performance, for all vendors is to place the most popular rules near the top of the rule base. This advice doesn‘t make much sense if the firewall rearranges the rules into a complex search data structure. Note that a stateful firewall‘s two-part design provides its highest performance on long TCP connections, for which the fast state lookup mechanism handles most of the packets. However, connectionless UDP and ICMP traffic and short TCP flows, like those produced in extremely high volume by Distributed Denial of Service attacks, only activate the ―slow‖ algorithm, making it a significant bottleneck. Our main result is that the ―slow‖ algorithm does not need to be slow, even in a software-only implementation running on a general-purpose operating system. Existing algorithms implement the ―longest prefix match‖ semantics, using several different approaches. The IPL algorithm, which is based on results, divides the search space into elementary intervals by different prefixes for each dimension and finds the best (longest) match for each such interval. The note to be made regarding the existing algorithms, there is no security when the packet sending and time-consuming are high.

Conclusions

We conclude that the GEM algorithm is an efficient and practical algorithm for firewall packet matching. We implemented it successfully and tested its packet-matching speeds on live traffic with realistic large rule-bases. GEM’s matching speed is far better than the naive linear search, and it can increase the throughput of IP tables by an order of magnitude. On rule-bases generated according to realistic statistics, GEM’s pace complexity is well within the capabilities of modern hardware. As for GEM itself, we would like to explore the algorithm’s behaviour when using more than four fields, e.g., matching on the TCP flags, metadata, interfaces, etc