Research on Firewall Implementation Principles and Application Deployment (Postprint)

Authors: Wang Baoshi

Date: 2023-10-08T00:00:00+00:00

Abstract

Firewall technology constitutes a critical component of network security protection. This paper analyzes and compares the implementation principles and deployment methods of mainstream firewall technologies in the current cybersecurity domain, systematically reviews the key firewall metrics that merit attention, proposes recommendations for evaluation criteria, and investigates the development trends of next-generation firewalls, which can serve as a reference for the construction of network security protection systems.

Full Text

Abstract

Firewall technology represents a critical component of cybersecurity defense. This paper analyzes and compares the implementation principles and deployment methods of mainstream firewall technologies in the current cybersecurity landscape, systematically reviews key firewall metrics that warrant attention, proposes recommendations for evaluation criteria, and examines the development trends of next-generation firewalls. The findings can serve as a reference for constructing cybersecurity defense systems.

Keywords: Information Security, Firewall
CLC Number: TP309.5
Document Code: A
Article ID: 1671-0134(2019)01-107-04
DOI: 10.19483/j.cnki.11-4653/n.2019.01.029
Author: Wang Baoshi

Introduction

Deployed at network entry and exit points, firewalls inspect incoming and outgoing data packets based on their characteristics, permitting those that comply

with security policies while discarding those that do not. Consequently, firewalls are often referred to as "security gateways." Firewalls constitute an indispensable element in network application deployment, essential for both internet-facing network architectures and internal network infrastructures within defense-in-depth frameworks. They serve to isolate security threats from external networks while simultaneously preventing the leakage of sensitive information from internal networks to external ones, thereby protecting network assets from compromise.

Firewall technology first emerged in the 1980s [1]. With the continuous evolution of cybersecurity technologies, firewall capabilities have undergone ongoing refinement and enhancement. To achieve comprehensive and scientifically sound network protection through synchronized security design and planning during network construction, a thorough understanding of firewalls—the most critical component in cybersecurity defense—becomes imperative.

1. Firewall Operating Principles

The primary function of a firewall is to achieve logical isolation from external networks, preventing external attackers from infiltrating internal networks ("keep unauthorized out") while protecting internal sensitive information resources and preventing internal data leakage ("prevent unauthorized access").

[Figure 1: see original paper] illustrates a typical network topology for an information system connected to the internet. The internal system is divided into a DMZ zone hosting services and a user zone, with a firewall deployed at the network exit to connect with the external internet. The firewall blocks "unwanted" external access along traffic path 1, while preventing internal users from accessing "prohibited" destinations along traffic path 2. Firewalls operate without concern for specific content details, functioning instead by filtering data traffic.

1.1 ACL Rules

Firewalls establish rules for evaluating data packets through Access Control Lists (ACLs). During packet evaluation, firewalls query these rules to determine appropriate actions. [Figure 2: see original paper] demonstrates the operational principle of firewalls using access control policies to manage data packets.

The syntax for a standard IP access control list is:

```
access-list [list number] [permit | deny] [source-address] [wildcard-mask]
[log]
```

The following example configures firewall policies using a standard IP access control list:

```
access-list 1 deny 172.16.4.13 0.0.0.0
access-list 2 permit 172.16.0.0 0.0.255.255
access-list 3 permit 0.0.0.0 255.255.255.255
```

The first ACL denies all traffic from host 172.16.4.13; the second permits all data traffic from the 172.16 network segment; the third permits data traffic from any address.

Standard IP access control lists are limited to controlling source addresses only, lacking the ability to manage traffic destinations or protocols. To achieve more flexible and powerful control capabilities, extended IP access control lists were developed.

The syntax for an extended IP access control list is:

```
access-list [list number] [permit | deny] [protocol] [source-address]
[source-mask] [source-port] [destination-address] [destination-mask]
[destination-port] [log] [option]
```

The following example configures firewall policies using an extended IP access control list:

```
access-list 150 permit tcp any host 192.168.50.10 eq smtp
access-list 151 permit tcp any host 192.168.50.20 eq www
```

The first ACL permits TCP packets from any source address to destination 192.168.50.10 using the SMTP protocol; the second permits TCP packets from any source address to destination 192.168.50.20 using the WWW protocol.

Thus, access control lists essentially implement the function of determining "who can access what services where."

1.2 ACL Rule Matching Principles

In practical applications, a complete information system provides multiple services with diverse incoming and outgoing data traffic patterns, necessitating multiple ACLs on firewalls. Firewalls employ specific matching mechanisms to evaluate traffic against these rules, which can be summarized as follows:

Firewall security rules follow a top-down matching principle. Once a packet matches a rule, it is processed according to that rule' s action, with remaining ACLs no longer evaluated. Consequently, ACL ordering is critically important. If no rules match, the packet is discarded. Security filtering rules primarily encompass source and destination addresses and ports, TCP flags, time-of-day, and advanced filtering options.

1.3 Implementation Methods

1.3.1 Packet Filtering Packet filtering represents the earliest supported firewall method [2]. Firewalls deployed on links that data traffic must traverse match each passing packet against ACLs sequentially until a matching rule determines the appropriate action. This approach does not establish content buffers or examine transmission content. Its advantages include simplicity and fast processing speeds; however, it evaluates packets individually, examining only packet headers without establishing logical relationships between preceding

and subsequent packets. This limitation prevents detection of inserted, missing, or spoofed packets during communication. For example, in TCP' s three-way handshake, packet-filtering firewalls do not verify whether the sequence of transmitted packets is legitimate, making them vulnerable to DoS attacks.

1.3.2 Stateful Inspection To address inherent weaknesses in packet-filtering firewalls, stateful inspection firewalls emerged, performing protocol detection on packets according to TCP standard protocol rules. Stateful inspection firewalls build upon packet inspection while simultaneously establishing protocol state tracking for each data connection, discarding packets when state mismatches are detected. [Figure 3: see original paper] illustrates the operational principle of stateful inspection firewalls.

When a data packet enters the firewall, the firewall first checks whether it matches a configured state inspection list. If matched, the packet is forwarded; if not matched, it undergoes packet-filtering security inspection—forwarded if matched, discarded if not. Stateful inspection extends packet-filtering functionality, enabling both security policy compliance checks and packet state verification, thereby defending against attacks that exploit packet state vulnerabilities (such as DoS attacks).

Stateful inspection firewalls perform state detection on every packet, requiring buffer space for incoming packets. As packet volume through the firewall increases, hardware resources are heavily consumed, potentially degrading data forwarding performance and impacting normal business operations.

1.3.3 Application Proxy Application proxy firewalls operate by establishing multiple application proxies on the firewall, with each proxy requiring a distinct application process or background service program. For each new application, a corresponding service program must be added; otherwise, the service cannot be used—traffic for non-proxied applications cannot pass through. Application proxy firewalls collect user request packets, reconstruct them into application-level requests, process these requests according to rules, and then forward them to servers, effectively interrupting direct user-to-server connections.

The advantage of application proxy firewalls lies in their role as intermediaries between users and services, interrupting direct connections and preventing direct server intrusion. However, they must be used in conjunction with packet-filtering and stateful inspection technologies, and suffer from long buffering times, slow speeds, and high latency.

2. Firewall Deployment Modes

Firewalls are hardware devices deployed within networks to enhance cybersecurity defense capabilities, with several common deployment modes including bridge mode, gateway mode, and NAT mode.

2.1 Bridge Mode

Bridge mode, also known as transparent mode, involves the simplest network consisting of clients and servers on the same network segment. For security purposes, a firewall device is inserted between clients and servers to control passing traffic. Normal client requests pass through the firewall to reach servers, and server responses return to clients without users perceiving the intermediate device's presence. Firewalls operating in bridge mode lack IP addresses, enabling network expansion without reconfiguring network addresses, though at the cost of sacrificing routing and VPN functionalities.

2.2 Gateway Mode

Gateway mode applies when internal and external networks reside on different network segments. The firewall is configured with gateway addresses to implement router functionality, forwarding traffic between different network segments. Gateway mode offers higher security compared to bridge mode, achieving security isolation alongside access control and providing certain privacy protections.

2.3 NAT Mode

NAT (Network Address Translation) technology enables firewalls to translate internal network IP addresses, replacing internal source addresses with the firewall' s IP address when sending data to external networks. When response traffic returns from external networks, the firewall replaces the destination address with the internal network' s source address. NAT mode prevents external networks from directly viewing internal network IP addresses, further enhancing internal network security protection. Additionally, internal networks can use private addresses in NAT mode, conserving limited IP address resources.

When external network access to internal services is required in NAT mode, address/port mapping (MAP) technology can be employed. By configuring address/port mapping on the firewall, external user requests are mapped to internal servers; when internal servers return data, the firewall forwards it to external networks. This mapping technology enables external users to access internal services while preventing them from seeing the internal server' s real address—only the firewall' s address is visible—thereby enhancing internal server security.

2.4 High Reliability Design

Firewalls deployed at network entry and exit points serve as the gateway for network communications, necessitating high reliability in their deployment. Typical IT equipment is designed for a 3-5 year lifespan; when single-point devices fail, redundancy technologies ensure reliability, such as Virtual Router Redundancy Protocol (VRRP) for active-standby redundancy. Currently, mainstream network equipment supports high reliability design, with [Figure 4: see original

paper] illustrating a typical high-reliability network architecture design for backbone network exits.

4. Firewall Performance Metrics

Regardless of the data filtering method employed, firewall performance relies on hardware resources, directly impacting user experience and even system security. The most critical performance metrics include throughput, latency, packet loss rate, concurrent connections, and new connection establishment rate.

Throughput refers to data forwarding capacity. According to Ethernet packet encapsulation rules, a gigabit firewall' s throughput should be:

$$64/(64 + 8 + 12) \times 1000\text{Mbps} \times 1.024 \approx 780.2\text{Mbps}$$

Irrespective of operating mode, firewalls must process passing data, which is slower than data transmission through fiber optics. The internet comprises numerous network devices, and data latency from source to destination represents the sum of delays across all traversed devices. Firewall latency should generally be controlled at the millisecond level.

During packet processing, firewalls may lose some packets due to errors or delays. This packet loss excludes packets discarded for failing ACL policy checks; any additional packet loss indicates firewall problems.

When traffic through the firewall involves numerous concurrent and newly established connections, the firewall must track these connection states. Whether hardware resources such as CPU can support the resource consumption from these connections can be assessed through connection count metrics.

4.2 Virtualization and Policy Hardware Acceleration

Firewall technology represents both the earliest and most widely applied technology in cybersecurity. As cybersecurity demands continue growing, firewall technology advances continuously, with improvements in processing speed, intelligent detection capabilities, and diverse deployment modes addressing evolving security requirements. Firewalls will remain among the most important devices in cybersecurity applications.

From an architectural perspective, firewalls impose high hardware requirements. With network upgrades, gigabit, 10-gigabit, and even 100G switches are now deployed, placing greater demands on firewall performance in high-throughput networks. Several architectural designs address high-throughput network applications.

Virtualization [3] involves designing firewalls with multiple port groups, enabling a single hardware firewall to function as multiple virtual firewalls through software configuration. However, virtualization still relies on CPU-executed algorithms for traffic filtering, with processing speeds limited by CPU capabilities.

Policy hardware acceleration moves beyond CPU-based algorithmic processing for each ACL match, instead encapsulating each policy within FPGA chips for packet processing. When large volumes of packets pass through, hardware rule tables composed of multiple FPGA chips filter packets, substantially increasing data processing speeds.

References

[1] Zhang Yan. *Firewall Product Principles and Applications* [M]. Beijing: Publishing House of Electronics Industry, 2016, 1(1).

[2] Chen Bo. *Firewall Technology and Applications* [M]. Beijing: China Machine Press, 2016, 1(1).

[3] Xie Zhenglan, Zhang Jie. *New Generation Firewall Technology and Applications* [M]. Xi' an: Xidian University Press, 2018, 5(1).

(Author Affiliation: National Radio and Television Administration Monitoring Center)

Note: Figure translations are in progress. See original paper for figures.