Implementing Stateful vs. Stateless Firewalls: Choosing the Right Approach for Modern Network Security

Nikhil Bhagat

Principal Network Engineer, Independent Scholar, Network Engineering
nikhil.bhagat90@gmail.com

Abstract:
Rapid growth of threats to network security through ever-evolving cyber technology has given rise to the need for stronger, more flexible security systems in today's IT infrastructure. Firewalls are the core part of network security as they are responsible for protecting systems from unauthorized access, virus, malware, and other types of attacks. These firewalls are divided into stateless and stateful, which both offer different operating models and features. Stateless firewalls scan packets on pre-defined rules without keeping record of the connection state between the packets, making it faster and easier to control. Stateful firewalls on the other hand protect against advanced attacks by continuously monitoring the state of connections. As Stateful firewalls are connection aware, they offer more detailed traffic analysis and protection from advanced attacks. This paper outlines a detailed discussion on stateless and stateful firewalls, their architecture, operational practices, strengths, and weaknesses. Further, the paper identifies cases where an organization should choose one firewall type or the other based on its security needs, network complexity and performance. It also provides important design considerations to help organizations select the right firewall architecture, ensuring optimal network security while balancing performance and resource efficiency in the ever-evolving digital age.

Keywords: Stateless firewalls, Stateful firewalls, cost optimization, session tracking, best practices.

1. Introduction

Organizations today are under pressure from cybersecurity breaches, which are more common than ever in our hyperconnected digital age. Firewalls, the foundational element of network security, can act as an interface between secure internal networks and unsafe outside networks. They operate by inspecting and managing traffic both inbound and outbound according to established security policy. Stateless firewalls and stateful firewalls are two primary types. Each type has its own strengths and weaknesses, and fits different network setups.

Stateless firewalls are easier, faster, and operate at the packet level, mainly considering IP addresses and ports, without maintaining a record of the state of a connection. Stateful firewalls, however, are more granular and observe the state of connections to the internet, and can therefore make better-informed choices about whether to accept or reject traffic.

The primary purpose of this paper is to present a comparison of stateless and stateful firewalls, discuss what each type provides in terms of features and drawbacks, and give recommendations when both types would be the best option. This will help IT experts and network administrators to determine for themselves which kind of firewall would be most appropriate for their organization's security needs.

I. STATELESS FIREWALL ARCHITECTURE AND OPERATION

A. Architecture

Stateless firewalls are designed to examine individual packets without knowing any context for a connection or session. They do not keep track of the connected connections so they make their decisions entirely based on the packet headers (source/destination IP addresses, port numbers, protocols). It's easier and faster to set up stateless firewalls as opposed to stateful ones.

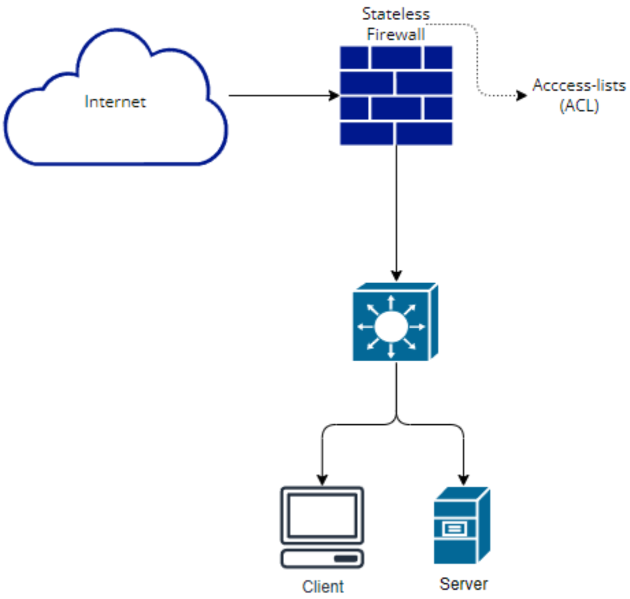

Fig. 1 Stateless Firewall Implementation

B. Key Components

- Filtering Rules: Stateless firewalls have a set of filter rules which are used on every packet. Such rules define whether a given traffic should be allowed or blocked based on features such as IP address, ports and protocols.
- Header Inspection: The stateless firewall only checks the header of the packet. It doesn't examine the packet's message or observe whether the packet is connected to an active session.
- No State Table: Stateless firewalls don't have a state table or connection logs, in contrast to stateful firewalls. All packets are unique, and no past data is cached other than the packet being processed.

C. Operation

Stateless firewalls or "packet filtering" firewalls work by analyzing every packet of data moving through the network. They analyze packets according to only default rules (usually including IP addresses, ports, and protocols). Each packet is examined individually, independent of whether any current or existing network connections are involved.

The packet that comes into the firewall is filtered using a number of rules to decide if the packet should be allowed or denied. Those rules are generally based on input parameters like source IP address, destination IP address, source port, destination port, and protocol (e.g., TCP, UDP, ICMP). When the packet matches a rule, firewall does the appropriate thing (allow or block). When packets don't match any rule they are usually dropped default.

This packet-by-packet analysis makes stateless firewalls very quick and easy. However, they do not track the state of network sessions, which means they can't make more granular security decisions. Since stateless firewalls are unable to track connection states, it’s becomes challenging for them to distinguish between legitimate traffic belonging to an existing connection, and potentially malicious traffic replicating the connection.

2. Advantages of Stateless Firewalls

A. Performance

Performance is one of the greatest benefits of stateless firewalls. Since they don’t require the monitoring of network connections, they can take care of packets faster than stateful firewalls. This makes them ideally suited for high throughput applications where speed is essential.

B. Simpler configuration

Stateless firewalls work on simple filters. This simplicity can be useful in a situations when a simple traffic management is needed. Stateless firewall rules are easy to set up and maintain, and ideal for networks with low security needs.

C. Low Resource Utilization

Stateless firewalls do not draw any system resources like RAM and CPU as they do not have to store connections state tables. This can result in less hardware expenditures and less burden on network devices, which can be great for small networks or applications with limited budgets.

D. Easy to Scale

Stateless firewalls can also be used in large distributed networks, where scalability is important. Since they do not need to hold the state of connections, they are able to support larger traffics without compromising on the performance.

3. Challenges with Stateless Firewalls

A. Lack of higher OSI layer Awareness

Stateless firewalls analyze each packet individually and disregard the context of the connection. They’re less capable of identifying the difference between legitimate traffic and malicious traffic that tries to exploit a loophole in a connection. Stateless firewalls are therefore at risk for certain attacks, including spoofing and replay attacks.

B. Limited Control over Stateful Protocols

Stateless firewalls also face a challenge with protocols that depend on the state of a connection (for example, TCP), in which packets are part of a current session. As stateless firewalls do not track the state of the connection, these firewalls are ineffective at managing TCP sessions and will likely drop connections or miss the legitimate traffic.

C. Complexity in Managing Rulesets

Keeping the stateless firewall's rulesets under control can become a challenge endeavor with evolving and growing network. Since each rule needs to take into consideration the packet attributes without connection tracking, it can lead to multiple detailed and complicated rulesets.

D. Lower Defense Against Matured Attacks

Stateless firewalls are poorly positioned to respond to today’s advanced attacks that exploit the connection states. It is difficult for a stateless firewall to discover and block modern advanced attacks like session hijacking, where the attacker steals an existing session.

4. Stateful firewall architecture and operation

A. Architecture

Stateful firewalls are more complex than stateless firewalls as they incorporate advance features. They inspect each packet’s state within a larger context of the communication. They also track the state of the connection i.e they can monitor whether a packet is in an established, new or closing session. It's has a granular packet inspection and security control architecture.

B. Key Components

- State Table: This is the key part of a stateful firewall setup where the state table stores all the connected instances. For each connection, the state table holds the source/destination IP addresses, port numbers, sequence numbers and the current state of the connection (e.g. SYN_SENT, ESTABLISHED, FIN_WAIT).
- Session Tracking: Stateful firewalls monitor all levels of a connection, particularly for stateful protocols such as TCP. They do this to enable packets that belong to a current session without having to repeat the whole filter rules for each upcoming packet.
- Inspection Process: When a packet arrives, the firewall looks into the state table to see whether or not it is part of a current session. If it does, the packet is released without further inspection. Otherwise, the packet goes through the inspection process where it is determined whether the packet can start a new session.
- Deep Packet Inspection (DPI): Most stateful firewalls today do deep packet inspection i.e. they examine both the headers and the packet itself. This enables stateful firewalls to identify and stop attacks that target the higher layers of the protocol stack (application-layer attacks, etc.).

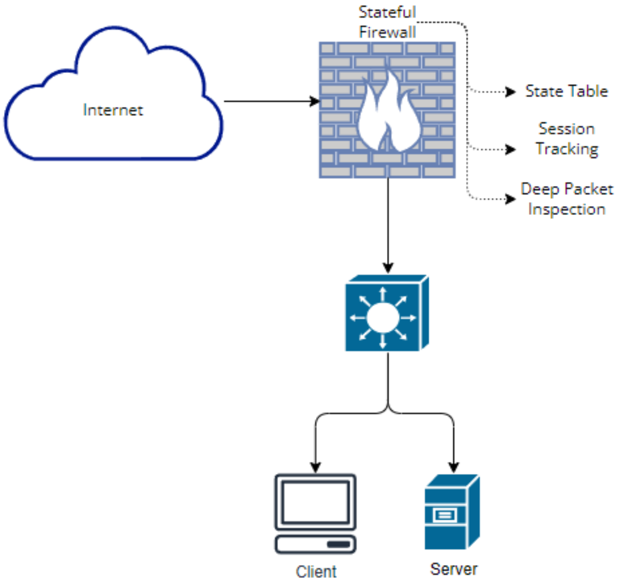

Fig. 2 Stateful Firewall Implementation

C. Operation

Stateful firewalls, in contrast to stateless firewalls, collect and store details about connected connections status as data packets travel through the network. They work at packet and session level, and trace traffic over time to detect the context of the exchange between source and destination.

When a data packet arrives in a stateful firewall, the firewall accesses its connection state table and determines if the packet belongs to an existing, previously approved connection. In the case it is, the packet goes through without any further examination. If not, then the packet is checked against the firewall security policy to see if it's allowed to make a new connection.

Stateful firewalls are best suited for handling sophisticated protocols like TCP, which need a stream of packets to connect to the internet. They can keep track of the different points in a connection state (e.g., SYN, SYN-ACK, ACK) and verify that packets are legitimate. This context persistence allows stateful firewalls to offer more extensive protection against attacks based on utilizing the state of a connection.

5. Advantages of Stateful Firewalls

a. Higher Layer Awareness

Stateful firewalls make a connection more secure, because they're constantly aware of the state of the connection. That allows them to recognize and block attacks that exploit the state of network sessions (session hijacking and man-in-the-middle attacks).

b. Efficient Handling of Stateful Protocols

Stateful firewalls are ideal for encapsulating stateful protocol like TCP. They track connection states, allowing sessions to be managed effectively and enabling packets belonging to a connection to flow through without further inspection.

c. Simpler Rules to Manage

Since stateful firewalls store connection states, they require less individual rules to process traffic. Users do not need to create different rules for each packet type, simplifying firewall rules thus avoiding the possibility of implementation errors.

d. Protection Against Modern, Advanced Attacks

The stateful firewalls are better suited for advanced, sophisticated attacks. With the ability to check for connection states, they can detect malicious traffic, which may try to take advantage of weak connections or even trick the firewall by imitating normal traffic.

6. Key Differences between Stateless and Stateful firewall architechtures

Feature	Stateful Firewall	Stateless Firewall
Operation	Operates at Layer 3 and Layer 4 of the OSI model	Operates at Layer 3, Layer 4, Layer 5 and Layer 7 of the OSI model
Connection Tracking	Tracks and maintains connection state	No connection state tracking; operates per-packet
Inspection Depth	Analyzes both headers and content (Supports Deep Packet Inspection)	Inspects only packet headers
State Table	Uses a state table to track ongoing sessions	No state table; each packet is independent
Rule Complexity	Rules are simple as state table is maintained	Rules can get complex as sessions are not tracked
Performance	Relatively lower performance in terms of latency when compared to stateless firewalls	Higher performance in latency sensitive, high-performance environments
Security	Provides higher security, due to its deep packet inspection mechanism	Provides IP and Port level security (not an effective solution for Layer 7 attacks)
Resource Consumption	Higher resource consumption	Low resource consumption
Implementation example	Access-Lists	Firewalls with deep packet inspection and other features
Cost	Price depends on the features but typically more expensive to implement and operate	Less expensive to implement and maintain

7. Scenarios Where Organizations Should Prefer Stateless Firewalls

a. High-Performance and Low Latency Environments

If there are high throughput and low latency requirements, like in massive datacenters or backbone networks, stateless firewalls might be the better option due to their faster packet-processing capabilities.

b. Predictable Traffic Flow

Stateless firewalls can provide adequate security for networks with restricted internet exposure and predictable traffic flow patterns such as networks with limited external visibility or internal networks with minimal endpoint exposure.

c. Budget constraints

Stateless firewalls can be cheap to deploy and maintain, which make them an attractive solution for businesses with smaller budgets or resources, especially if their networks are part of a restricted, well monitored environment.

d. Edge Networks

Stateless firewalls work well at the edge of a network to rapidly reject inbound traffic by IP address, port, and protocol before it gets into the inside network. They can also be combined with other security technologies for multi-layer protection.

8. Scenarios Where Organizations Should Prefer Stateful Firewalls

a. Complex, Dynamic Networks

In networks with complex and dynamic traffic patterns, like cloud infrastructures or data centers with multiple applications, stateful firewalls offer the flexibility and management needed to control the traffic.

b. Environments with High-Security requirements

Stateful firewalls are more robust against sophisticated attacks and connection state exploit attacks in scenarios where security is a paramount concern, such as financial institutions, hospitals, and government organizations.

c. Networks with Sensitive Information

For organizations that deal with proprietary or sensitive information, like personal data, intellectual property, or financial transactions, you need to have stateful firewalls that secure all connections and keep an eye on attacks.

d. Remote Access

Stateful firewalls are more suitable for remote access and VPN connections. As they maintain the status of the connection, they can make to allow legitimate traffic and reject unauthorized connections.

9. Design Considerations When Implementing Stateless vs. Stateful Firewalls

When it comes to choosing between stateless and stateful firewalls, organizations need to weigh performance, security and network complexity among others. Here are some key design considerations:

a. b

Stateless firewalls are typically faster and best-suited for highly trafficked and low latency applications. However, in an environment where traffic is more diverse and safety is a high priority, stateful inspection can be worth the additional cost.

b. Type of Network

Stateless firewalls, with no stateful inspection, can be adequate to defend low level static networks. On the other hand, complex networks with non-predictable traffic pattern with multiple applications may demand the additional adaptability and control of stateful firewalls.

c. Security Requirements

For organizations with heavy security requirements such as organizations that process sensitive data or are required by regulatory regulations, the top consideration will be for stateful firewalls which are highly resistant to sophisticated attackers.

d. Resource Consumption

A stateful firewall typically consumes additional system resources, including memory and processing power to store connections. Organizations with low spending budgets might struggle to balance security with hardware and budget limits.

e. Cost vs the Use-case

Stateful firewalls are more secure, but they're also generally more expensive to setup and maintain. While deciding on a firewall solution, businesses should consider the costs of operating and maintain a stateful firewalls with the amount of security protection it provides.

10. Conclusion

Stateless and stateful firewalls have distinct advantages and disadvantages in network security. Stateless firewalls, as they are simple and fast, are well-suited for environments with well-defined predictable traffic patterns and lower security requirements. Stateful firewalls, on the other hand, offer more advanced security by keeping track of network connections, making them desirable for high-security, complex scenarios.

Choosing the right firewall depends on the company's specific needs in terms of network complexity, speed, security, and cost. In many scenarios, both firewalls can be used together to achieve a balanced approach, with stateless firewalls providing perimeter defense and stateful firewalls securing internal network and critical systems.

By analyzing these parameters and making sure they are aligned with organizational requirements, companies can select the optimal firewall model to protect and defend their networks from emerging cyber threats while maximizing the efficiency and performance of their resources.

References

1. S. K. Majhi and P. Bera, "Designing an adaptive firewall for enterprise cloud," Proc. 2021 Int. Conf. Cloud Computing (ICCC), 2021.
2. J. P. Wack, K. Cutler, and J. Pole, "Guidelines on firewalls and firewall policy," NIST Special Publication 800-41, National Institute of Standards and Technology (NIST), 2002.
3. [19] Cisco Systems, "The next-generation firewall: The future of firewalling," Cisco White Paper, 2019. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/firewalls/ngfw-futureoffirewalling-wp.html
4. W. M. Eddy, "TCP SYN flooding attacks and common mitigations," Internet Engineering Task Force (IETF), RFC 4987, 2007. [Online]. Available: https://www.ietf.org
5. A. Stubblefield, "Firewall manipulation," Black Hat USA 2007, Las Vegas, NV, USA, 2007.
6. D. Brent Chapman and E. D. Zwicky, Building Internet Firewalls, 2nd ed. Sebastopol, CA, USA: O'Reilly Media, 2000.
7. S. Bellovin, "Security problems in the TCP/IP protocol suite," ACM SIGCOMM Computer Communication Review, vol. 19, no. 2, pp. 32-48, Apr. 1989.
8. E. W. Fulp and R. Farley, "A function-parallel architecture for high-speed firewalls," IEEE Trans. Parallel Distrib. Syst., vol. 14, no. 12, pp. 1266-1276, Dec. 2003.
9. P. Gupta and N. McKeown, "Packet classification on multiple fields," in Proc. SIGCOMM '99, Cambridge, MA, USA, 1999, pp. 147-160.
10. A. Yaar, A. Perrig, and D. Song, "SIFF: A stateless internet flow filter to mitigate DDoS flooding attacks," in Proc. 2004 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2004, pp. 130-143.
11. S. Charp and D. Hines, "A primer on campus networks," Tech Directions, vol. 62, no. 5, pp. 23-28, Jan. 2003.

12. Y. Chang and T. Lin, "Cloud-clustered firewall with distributed SDN devices," 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 2018, pp. 1-5, doi: 10.1109/WCNC.2018.8377305.
13. W. Liu, M. Ermini, and F. Gont, "Requirements for IPv6 enterprise firewalls," Internet Engineering Task Force (IETF), RFC 8504, 2019. [Online]. Available: https://www.ietf.org
14. Cisco Systems, "Getting started with application layer protocol inspection," Cisco Documentation, 2014. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/firewall/asdm_71_firewall_config/inspect_overview.html
15. F. A. Guenane, M. Nogueira, and G. Pujolle, "Reducing DDoS attacks impact using a hybrid cloud-based firewalling architecture," IEEE Trans. Cloud Comput., vol. 9, no. 4, pp. 1110-1122, Dec. 2021.
16. A. Mayer, A. Wool, and E. Ziskind, "Offline firewall analysis," Int. J. Inf. Security, vol. 5, no. 3, pp. 125-144, Aug. 2006.
17. A. K. Sahoo, A. Das, and M. Tiwary, "Firewall engine based on graphics processing unit," in Proc. 2018 IEEE Int. Conf. Cloud Computing in Emerging Markets, Bangalore, India, 2018, pp. 65-72.
18. P. A. Henry, "Firewall considerations for the IT manager," IEEE IT Professional, vol. 17, no. 6, pp. 56-61, Nov.-Dec. 2015.