Denial of Firewalling Attacks (DoF): Detection, Defense and Challege

1st Liang Liu
Civil Aviation University of China
Tianjin, China
liul@cauc.edu.cn

2nd Tong Wang
Civil Aviation University of China
Tianjin, China
2021021023@cauc.edu.cn

3rd Zhijun Wu
Civil Aviation University of China
Tianjin, China
zjwu@cauc.edu.cn

Abstract—Firewalls are network security systems positioned between internal and external networks to isolate them. Their fundamental functions include zone isolation, access control, attack protection, and redundancy design. However, firewalls also face numerous security challenges, with Distributed Denial of Service (DDoS) attacks being a major concern, particularly the Denial of Firewalling (DoF) attacks targeting firewalls. Despite extensive research on DDoS attacks against traditional networks, relatively fewer studies focus on DoF attacks. To comprehensively understand the latest research progress and inspire the development of new solutions to counter DoF attacks, this paper conducts an extensive survey of existing research progress and forms a review. Firstly, we analyze the principles of DDoS attacks against firewalls, as well as the security risks of new firewall technologies, and classify them based on attack rates and target components of firewalls. Secondly, we analyze and evaluate existing DoF attack detection technologies. Next, we summarize existing DoF attack mitigation techniques. Finally, we discuss current challenges and open issues. It is hoped that this research work will assist relevant researchers in effectively addressing DoF attacks.

Index Terms—Denial of Firewalling attacks, attack classification, attack detection, attack mitigation

I. Introduction

In recent years, DDoS attacks have been widely recognized as a major security threat in the field of the Internet [1]. Such attacks not only cause severe disruptions to network infrastructure, rendering legitimate users' normal requests ineffective, but also generate significant negative impacts on the nation and society. Traditional DDoS attacks exploit vulnerabilities in the target user systems through technical means, infiltrating a large number of puppet machines to construct a zombie network. Subsequently, the attacker employs hosts within this network to launch massive DDoS attacks against the target server. The primary objectives of attackers are focused on network bandwidth resources and system resources, ultimately leading to the incapacitation of legitimate user requests [2].Some notable DDoS attack incidents, such as the large-scale Internet outage in the eastern United States in 2016, significantly affected the security of major regions, including prominent websites like Twitter, Github, and The New York Times. The root cause of this incident was a DDoS attack on Dyn Inc.'s servers, preventing legitimate users from accessing websites and causing widespread disruption [1].

Firewalls are deployed at the network edge, serving as the first line of defense to protect network resources and servers. Their primary responsibility is to filter traffic entering and leaving the network, inspect data packets based on predefined filtering rules, and make decisions on whether to allow passage [3]. The first generation of firewalls, namely packet filtering firewalls, primarily achieves filtering of incoming and outgoing network data packets through the configuration of Access Control Lists (ACLs). The filtering process is based on information such as source IP address, destination IP address, source port, destination port, IP identification, and packet transmission direction. Today, stateful firewalls have become the most widely adopted type of firewall. In contrast to the first-generation firewall, stateful firewalls introduce session tables, employing dynamically set packet filtering rules to improve system transmission efficiency while enhancing system security [4].

While firewalls play a critical role in safeguarding networks and services, they themselves are susceptible to becoming targets of DDoS attacks. DoF attacks exploit firewall resources, inducing an overload that disrupts the normal access of legitimate users to the network. Attackers achieve this by inundating the firewall with a massive volume of malicious traffic, utilizing redundant data packets. Additionally, attackers can inflict a more persistent impact on the firewall by sending small volumes of specifically crafted malicious packets [4].

Mitigating DoF attacks has long been a focal point in academia. This paper aims to comprehensively review existing research achievements from a technical perspective, outlining the detection, defense, and challenges posed by DoF attacks. The intent is to provide insights and assistance to scholars and experts in related fields. The primary contributions of this paper are as follows:

(1) Analyzing the security vulnerabilities of firewall technology and categorizing DDoS attack techniques utilized by attackers targeting firewalls. (2) Analyzing, summarizing, and comparing detection and mitigation techniques for DoS attacks. (3) Exploring the issues present in current defense mechanisms against DoS attacks.

*

The structure of the remaining sections in this paper is as follows: Section 2 discusses the relevant technologies of firewalls and reveals the security vulnerabilities they present. Section 3 categorically reviews DoF attack techniques. Section 4 summarizes and compares existing DoF attack detection schemes and mitigation techniques. Section 5 concludes the current research issues. Section 6 provides an overall summary of the paper.

II. Analysis of Vulnerabilities to DDoS Attacks in Firewalls

With the rapid development of Internet technology, the number of cybercrimes has sharply increased, resulting in an urgent demand for individuals and enterprises to protect their data. Despite the challenges in implementing effective security measures, firewalls, as a security tool, can effectively safeguard networks and devices from various attacks. However, certain features of firewalls also expose certain security vulnerabilities, thereby providing an opportunity for the proliferation of DDoS attacks.

A. Packet Filtering

Packet filtering is one of the fundamental functions of a firewall, operating at the network layer. It determines whether to allow a data packet through the firewall by inspecting information such as the source address, destination address, and port number of the packet. This filtering can be based on a predefined set of rules, such as allowing specific IP addresses or ports, or it can be adjusted according to dynamic security policies. Packet filtering technology examines each incoming packet and matches it against each rule in the rule set until a match is found with the information in the packet. Otherwise, the packet is discarded using default rules. The process of matching packets to the rule set often consumes a significant amount of time. If an attacker crafts packets specifically to match all default rules, it can severely deplete system resources, making it a potential target for DDoS attackers.

B. Stateful Inspection

Stateful inspection represents a more sophisticated firewall technique that goes beyond examining individual data packets by tracking the state of network connections, also known as dynamic packet filtering. The firewall maintains a connection state table, recording pertinent information such as source and destination addresses, and ports for all connections passing through it. This enables the firewall to scrutinize incoming data packets to determine if they belong to established legitimate connections, thereby enhancing security. However, configuring stateful inspection is highly complex and can result in decreased network speeds. Additionally, the state table has a fixed capacity limit, and when the number of real-time connections exceeds this threshold, the firewall begins to discard new connections. Malicious actors conducting DDoS attacks can exploit this characteristic to congest the firewall's state table, thereby impeding the processing of legitimate user requests.

C. Proxy Services

Proxy services act as intermediaries between clients and servers. They receive requests from clients, establish new connections between clients and servers, and forward data between the two. Through proxy services, firewalls can conceal internal network structures, thereby enhancing network security and privacy. However, when the proxy server of a firewall becomes a target of attack, attackers can overwhelm its resources through flood attacks, causing it to fail or become ineffective in forwarding traffic, thereby bypassing the firewall and directly targeting end users.

D. Network Address Translation

The fundamental principle of Network Address Translation (NAT) in firewalls is to map private IP addresses from internal networks to public IP addresses in external networks, thereby achieving isolation between internal and external networks. It effectively conceals the true structure of the internal network and also addresses the issue of IPv4 address exhaustion, significantly enhancing the security of internal networks. However, it also introduces certain security vulnerabilities. NAT technology conceals the real IP addresses of internal networks, making all outbound traffic appear to originate from a single public IP address. Attackers can exploit this characteristic to spoof IP addresses, making DDoS attacks more difficult to trace and mitigate. Additionally, attackers can utilize legitimate NAT traversal techniques to bypass network filtering, making it more challenging to detect and filter attack traffic.

In addition to the aforementioned basic principles, modern firewalls incorporate various other technologies such as deep packet inspection, Virtual Private Networks (VPNs), and Intrusion Detection Systems (IDS). Deep packet inspection involves thorough analysis of packet contents to identify malicious code and attack behaviors. However, deploying a firewall for deep packet inspection can introduce a single point of failure. In the event of a DDoS attack causing the failure of this firewall, the entire system may be compromised. VPN technology ensures secure transmission of data over public networks through encryption and tunneling techniques. Nevertheless, a single point of failure in the network, such as all VPN connections routed through a single server or device, can render the VPN service unavailable if targeted by attackers. IDS systems monitor network traffic to detect and prevent potential intrusion attempts. Attackers may disguise their malicious traffic as legitimate data packets, making it challenging for IDS systems to accurately detect DDoS attacks.

The security vulnerabilities mentioned above are summarized in Table I. Attackers can exploit these vulner-

abilities to launch various types of DDoS attacks using different techniques.

III. DoF attack techniques

Over recent years, the frequency, scale, and sophistication of DDoS attacks have continued to escalate. However, the characteristics of DDoS attacks remain unchanged: the attack tools are freely available, online services are inexpensive, and anyone can launch an attack via the internet. Currently, DDoS attacks against firewalls exhibit two main trends. Firstly, traditional DDoS attacks primarily rely on brute force to increase attack traffic, aiming to overwhelm firewall resources with redundant data packets, thereby keeping the firewall busy dealing with the current attack traffic and preventing legitimate user access, consequently lowering its performance. Secondly, novel attack methods involve attackers sending a small number of specially crafted attack packets to precisely target critical components of the firewall, continuously affecting its operation and making it difficult to withstand the load.

The common classification of DDoS attacks is typically based on protocol perspectives. However, this article adopts a classification approach based on attack rates and targeted components of firewalls. The rationale behind this choice lies in two aspects: firstly, attackers can opt for either flood-based or low-rate attacks when launching Denial of Firewalling attacks. These two attack methods have distinct principles and impacts, thus prompting varied detection and mitigation strategies by defenders. Secondly, firewalls primarily operate through packet filtering and state monitoring mechanisms, achieved via configuring access control lists and maintaining session tables to inspect and filter incoming and outgoing packets. Consequently, attackers may target these firewall components to disrupt the firewall's ability to process legitimate packets effectively. Therefore, basing the classification on the primary targeted components of firewalls holds reasonable validity.

From the perspective of attack rate, attacks can be classified into two main categories: traditional flooding attacks and low-rate attacks.

A. Flooding attack

Traditional DDoS attacks, such as ICMP flooding attacks, inundate the firewall with a large volume of ICMP echo request packets [Type: 8, Code: 0], thereby reducing the performance of packet filtering firewalls and impeding their ability to handle legitimate traffic. Stateful inspection firewalls extend packet filtering techniques by primarily examining data packets passing through the firewall based on connection state. Their operation treats each data packet as an independent unit and considers the historical correlation between preceding and succeeding packets. Stateful inspection firewalls utilize various session tables to track activated TCP sessions and UDP pseudo-sessions, determining which sessions to establish based on access control lists, and only forwarding packets associated with established sessions. Consequently, attackers can exploit the aforementioned principles to launch various transport layer flooding attacks against targets, such as UDP flooding, SYN flooding, SYN/ACK flooding, and ACK reflection attacks.

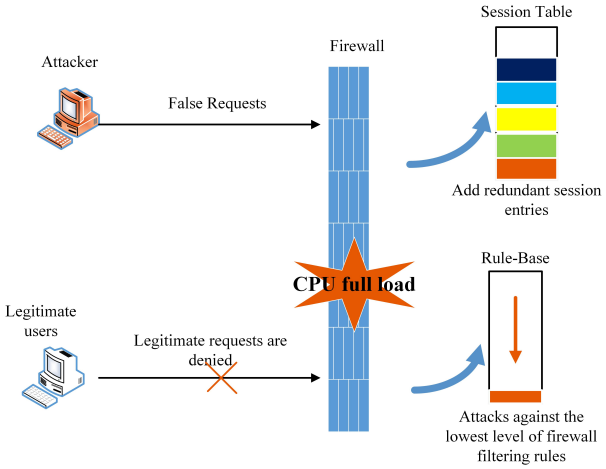

Fig. 1. BlackNurse attack model.

B. Low-rate attacks

In addition to the aforementioned flooding attacks, various Low-rate DoF attacks are also becoming increasingly prevalent. Attackers can easily evade intrusion detection systems and intrusion prevention systems' defense techniques by designing special low-rate attack packets, causing prolonged harm to the targeted systems. This section will primarily introduce the BlackNurse attack and EDoS attack.

1) BlackNurse Attack: BlackNurse attack is a specialized type of ICMP attack, which involves launching an assault on firewalls by sending low-rate ICMP traffic with [Type: 3, Code: 3] to the target server. The attack principle relies on sending response requests to specific ports on the target host. However, since the target ports are inactive, they fail to deliver response packets to the requesting user and generate ICMP Destination Unreachable and Port Unreachable error messages. Consequently, firewalls analyze and process these ICMP error messages, consuming a significant amount of firewall resources. This process leads to a sharp increase in CPU load, thereby impeding the normal processing of legitimate user requests. The attack model is depicted in Figure 1.

Experts from the TDC SOC (Security Operations Center) in Denmark have stated that launching a BlackNurse attack requires only a laptop. By sending 40,000 to 50,000 ICMP packets per second, all with Type and Code set to 3, this attack can generate ICMP error messages that consume 15 Mbps to 18 Mbps of bandwidth.

TABLE I
Security Vulnerabilities of Firewalls

Firewall Technology	Summary Description
Packet Filtering	The attacker crafts specialized data packets to match the default rules at the lowest level of the rule library, resulting in resource depletion.
Stateful Inspection	By examining the capacity of the congestion state table through data packets.
Proxy Services	The attacker inundates the proxy service's resources with a flooding attack, rendering it incapable of properly forwarding traffic.
Network Address Translation	Forging IP addresses to make attacks difficult to trace and mitigate.
Deep Packet Inspection	Single Point of Failure
Virtual Private Networks	If all VPN connections are routed through a single server or device, attackers can focus their efforts on exploiting this central point of concentration
Intrusion Detection Systems	Attackers masquerade as legitimate traffic, potentially rendering IDS systems unable to discern such traffic.

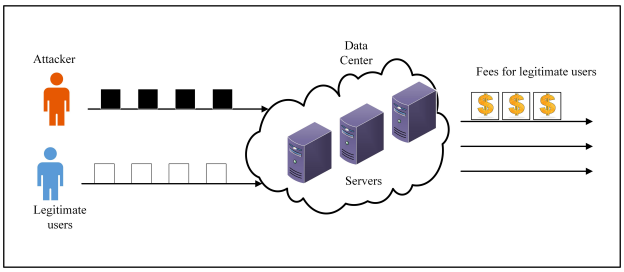

Fig. 2. FRC attack model.

2) EDoS attacks: For cloud firewall, attackers have devised a novel economic denial-of-sustainability attack [24]. This represents a new form of DDoS attack, primarily leveraging the pay-as-you-go billing model of cloud firewalls and the utility computing model of infrastructure. Its objective is to induce users into unlimited additional payments for virtual software, causing economic loss. The characteristic of this attack traffic is 'small and slow', which not only consumes resources of data centers but also can deceive legitimate users into incurring expenses. The main attack technique is FRC attack, whose attack model is illustrated in Figure 2.

Attacks against firewall components can be classified into DoF attacks targeting firewall filtering rules and DoF attacks targeting the firewall session table. This is because firewalls have limited resources, implying constraints on their simultaneous traffic processing capacity and the number of sessions they can establish. Attackers exploit this vulnerability to launch assaults against firewalls. The impact of such attacks is primarily manifested in increased packet filtering times, elevated CPU usage of the firewall, an increase in the number of allocated sessions in the session table, and unresponsive handling of legitimate user requests.

C. DoF attacks targeting firewall Rule-Base

The firewall filtering rules are defined by Access Control Lists (ACLs), and the firewall examines each rule until a match is found between the information in the packet and a rule in the rule set. Otherwise, default rules are applied. Typically, the default rule requires the firewall to discard the packet.

In the context of DoF attacks targeting firewall rule sets, attackers craft specialized types of data packets

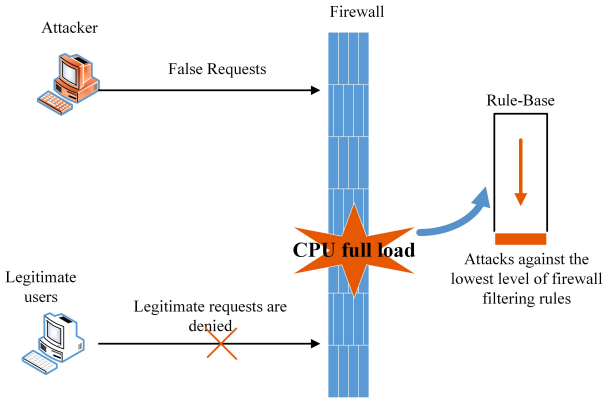

Fig. 3. DoF attacks targeting firewall Rule-Base model.

that do not match any rules in the rule set, ultimately leading to rejection by default rules or acceptance by the bottom rules of the firewall. This matching process, being the longest path, consumes time for the firewall to filter packets, thereby degrading firewall performance. The attack model is illustrated in Figure 3.

The firewall rule set deployed by large and medium-sized enterprises or businesses can reach up to 10,000 rules, and some large firewalls can even reach a quantity of 50,000 rules. The default rules or the rules that match last are typically located at the bottom of the rule set. Once attackers detect these rules and trigger them with specially crafted attack packets, the firewall's CPU usage will significantly increase in a short period, requiring a substantial amount of processing time. This results in legitimate user packets being unable to be processed normally.

D. DoF attack targeting firewall session table

The session table is the core of a stateful firewall, used to record entries of TCP, UDP, ICMP, and other protocol connection states. It serves as a crucial basis for the firewall to forward packets. The principle behind packet filtering by a stateful firewall involves inspecting only the initial or a small number of packets entering or exiting the firewall to establish a state. Subsequent packets are then controlled based on the established connection state. This mechanism significantly enhances the efficiency of the firewall in inspecting and forwarding past packets.

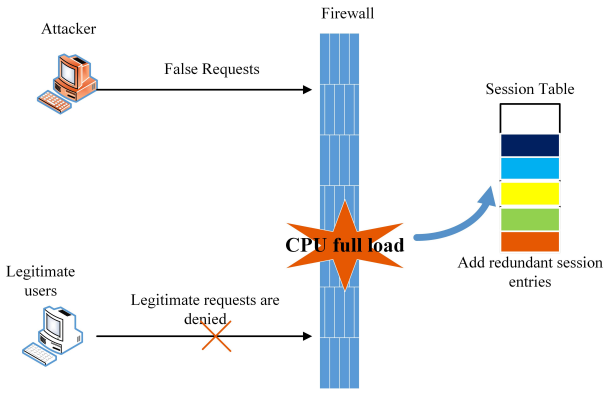

Fig. 4. DoF attacks against the firewall session table model.

However, attackers can increase the firewall's redundant session entries by sending a large number of false requests until the session table is filled, thereby blocking legitimate connection requests. Additionally, attackers can send a small number of specially crafted packets, ensuring that the destination host's target port is closed, prompting the destination host to return an error message. The firewall parses these error messages to identify the cause of the error. If this process takes too long or if there are too many packets awaiting analysis, it may result in the firewall being unable to handle new sessions and starting to discard new connection requests. The objective of both attack methods is to force the firewall to add new session entries until the firewall's session table becomes overwhelmed, rendering it incapable of handling legitimate user connection requests. The attack model is illustrated in Figure 4.

The above categorization of current DoF attacks is based on attack rate and target components against firewalls. It can be observed that traditional DDoS attacks remain effective when launched against firewalls, and novel DoF attacks pose challenges to experts and scholars in related fields. With the continuous emergence of new DoF attacks and the expansion of attack traffic scale, the upgrading and replacement of firewalls are facing severe challenges.

IV. Defense Techniques against DoF Attacks

A. Detection Techniques for DoF Attacks

Attack detection serves as the primary step in defense when attacks occur, necessitating defenders to promptly and accurately identify the targets. Currently, research on detection techniques for DoF attacks is relatively scarce, primarily classified into two major categories: anomaly detection and feature detection.

1) Anomaly-based DoF attack detection: Anomaly-based detection primarily involves modeling using statistical knowledge to identify differences between attack traffic and normal traffic.

Attackers can use probing techniques to understand firewall policies and then launch DoS attacks by flooding the firewall with crafted traffic that exploits vulnerabilities in these policies. Al-Haidari et al. [8]proposed a countermeasure that enables firewalls to withstand such attacks without denying service to legitimate clients. The goal of this work is to utilize an entropy-based approach to distinguish between legitimate and attack traffic. Subsequently, legitimate traffic is prioritized over attack traffic in the queue. Results indicate that this approach enhances firewall performance in terms of throughput, delay, and availability during DoS attacks. Results demonstrate that this approach enhances the firewall's performance in terms of throughput, latency, and availability during DoS attacks.

2) Feature-based DoF detection: Feature-based detection refers to the process of extracting attack traffic, analyzing and comparing the characteristic differences between attack traffic and legitimate traffic, and summarizing features such as attack rate, traffic size, duration, and attack period of attack traffic. The objective of feature-based detection is to accurately detect attacks in the early stages.

Firewall rejection attacks involve flooding the firewall effectively with specific traffic by attackers, causing it to become overloaded. Subsequently, data packets are discarded without inspecting the firewall rules. Following the initiation of firewall rejection attacks, Khakpour et al. [9] proposed a decision-making method for sequences of TCP data packets with abnormal flags based on firewall features, which can be utilized for firewall fingerprinting. Additionally, they employed machine learning techniques to validate that different firewalls are susceptible to different attacks. Regarding firewall rejection attacks, they suggested designing a defense mechanism to conceal firewall information to prevent attackers from obtaining it.

Nevertheless, similar to other network and computing devices, firewalls frequently possess vulnerabilities that can be exploited by attackers. Initially, Liu et al. [12] investigated DoF attacks, where attackers employ meticulously designed traffic to overwhelm the firewall. Additionally, they introduced several potential firewall fingerprinting techniques and discovered, somewhat surprisingly, that these methods can achieve high accuracy in identifying DoF attacks.Table II compares the above DoF attack detection techniques.

B. Alleviation of DoF attacks

Currently, most proposed mitigation strategies for DoF attacks are adaptations of conventional DDoS defense mechanisms. These defense strategies aim to upgrade firewall session tables or filtering rules to filter and cleanse attack traffic as effectively as possible. This article categorizes attack defense based on the rate of attack traffic: burst traffic, low-rate traffic, and high-rate traffic.

TABLE II
Security Vulnerabilities of Firewalls

Detection Method	Advantages and disadvantages	Scope of application
Based on entropy [8]	Ability to differentiate attack traffic and improve firewall performance	Based on firewall policies and rules
Fingerprint recognition [9], [10]	Identify DoF with high accuracy	Based on firewall features and vulnerabilities

1) DoF attack mitigation for bursts traffic: Firewalls are deployed at the forefront of networks to defend against external threats, capable of preventing unauthorized access to cloud resources by malicious users [11], [12]. However, they may be inundated by DDoS attackers using large-scale data packets, thereby reducing the firewall's speed in filtering packets. To better understand the behavior and characteristics of firewalls, it is necessary to further model and analyze their performance under legitimate traffic and DDoS attacks. Cloud firewalls can protect infrastructure from DDoS attacks. By comparing Poisson and IPP attacks, cloud firewalls are vulnerable to burstiness-aware attacks that affect their operation. Considering the complete characteristics of the system and workload, such as the correlation and burstiness of malicious and legitimate data traffic, Glaucio et al. [13] propose a multidimensional continuous-time Markov chain model for cloud firewalls. By adopting Interrupted Poisson Processes and Markov Modulated Poisson Processes (MMPP), the workload conditions under which cloud firewalls may become unavailable are identified. Finally, an elastic cloud firewall is designed by separating the MMPP arrival process to meet Service Level Agreement (SLA) latency specifications, ensuring a more secure cloud environment..

In order to effectively handle the large burst traffic loads against traditional firewalls, Trabelsi et al. [14] propose a method that leverages packet matching rule histograms and non-matching rule field histograms. This method aims to enhance firewall packet filtering rules by optimizing the sequence of firewall rule fields for early packet acceptance and rejection. These histograms can monitor firewall performance in real-time and predict packet filtering patterns based on the sequence and order of rule fields.

2) DoF attack mitigation for High-rates ttaffic: Stateful firewalls remain susceptible to DoF attacks, which can lead to significant damage and the exhaustion of all firewall resources, particularly the firewall's session table [15], [16], and [17]. A typical mitigation strategy for DoF attacks targeting the firewall session table involves threshold-based mechanisms, such as the Screen feature employed by Juniper Networks [17]. However, if the activation threshold is set too high, it permits attack traffic to evade firewall filtering and deplete firewall system resources. Additionally, most threshold-based mechanisms are often disabled, and when they are enabled, they substantially increase the firewall's CPU usage and session table utilization, as seen with the TCP SYN flooding mechanism [18].

3) DoF attack mitigation for Low-rate traffic: Mechanisms used for packet filtering and session handling play a crucial role in determining the performance of stateful firewalls, allowing them to track the state of network connections. Combining the use of octree firewalls, Trabelsi et al. [19] proposed a method to defend against denial of service attacks targeting stateful firewalls by introducing a stateful session table structure. By employing a one-level vertical expansion session hash table with a hash slot for each connection, the proposed stateful session table architecture enhances firewall concurrency, reduces hash computations, and saves memory space. This method simplifies the complexity of threshold mechanisms and provides defense against Denial of Service (DoS) attacks that target session tables. By leveraging the intrinsic properties of octree firewalls and a session table architecture that separates session attributes, this mechanism efficiently manages the costly timeout attributes. On the other hand, BlackNurse attacks are challenging to detect and handle. This difficulty arises because firewalls treat the ICMP destination unreachable messages, which are used in BlackNurse attacks, as legitimate session packets. Consequently, all firewalls must inspect these packets and correlate them with their respective session tables, if applicable.

Another issue is that BlackNurse attacks utilize low-volume traffic, making it challenging for firewalls to detect and classify them as legitimate traffic. Furthermore, all available BlackNurse attack mitigation measures have their own limitations. It is worth mentioning that iptables by default limit the rate of ICMP destination unreachable messages. This explains why products based on iptables are not affected by BlackNurse attacks [20]. Additionally, as noted in [20], BlackNurse attacks significantly degrade the performance of numerous widely-used firewalls and routers. Nevertheless, products utilizing iptables are resistant to BlackNurse attacks. Generally, a firewall's vulnerability to BlackNurse attacks is determined by its device architecture and protocol stack implementation. Several mitigation strategies can be employed to reduce the impact of BlackNurse attacks.

① Drop ICMP packets that reach the WAN interface of the firewall. This may lead to issues, as internal hosts attempting to check server availability using the ping command will not receive responses.②The recommendation in [20] advises denying ICMP type 3 messages sent to the firewall's WAN interface. However, rejecting ICMP unreachable messages disables ICMP Path MTU Discovery, which can disrupt IPSec and PPTP traffic. To ensure normal Path MTU Discovery operation, ICMP type 3 code 4 packets should be allowed to pass through.③Create a trusted source host list for ICMP packets and implement

rate limiting on incoming ICMP traffic.

Due to the fact that the BlackNurse attack primarily affects firewalls with a single CPU, another mitigation strategy involves upgrading to firewalls with multiple CPU cores. Research shows that multi-core firewalls are relatively less affected by the BlackNurse attack. Trabelsi et al. [21] categorized DoF attacks based on the targeted firewall segments, the nature of the traffic, and the potential effects of the attacks. In response to the BlackNurse attack, they proposed an innovative defense mechanism that relies on early denial rules. These rules are specifically designed to activate only during a BlackNurse attack, addressing the limitations of existing mitigation mechanisms, such as iptables, which do not distinguish between false and legitimate destination unreachable messages. Additionally, the proposed rules feature a dynamic defense time, estimated using current and historical attack data along with severity parameters..

Low-rate Distributed Denial of Service (LDDoS) attacks present a particularly challenging threat to network security devices and services due to their subtle nature and difficulty in detection and mitigation. In these attacks, attackers use minimal amounts of malicious traffic that mimic legitimate traffic, allowing them to infiltrate networks stealthily. Despite their low rate, LDDoS attacks can significantly disrupt network services, deplete system resources, and reduce network speeds, making them one of the most destructive types of attacks. LDDoS can manifest in various forms, such as those targeting application servers or employing ICMP error messages. To address this threat, Hayawi et al. [22] proposed a mechanism to mitigate low-rate ICMP error message attacks aimed at firewalls and other security devices. This mechanism generates an early rejection rule, formatted as <ICMP(x, y), TTD>, which identifies the specific ICMP error message attack type and code values. The rule remains active for a duration TTD, determined by assessing the current and past attack severity and relevant statistical parameters. The proposed mechanism includes an easily implementable algorithm designed to balance the trade-off between the activation time of firewall rules and legitimate packet loss, thus preventing a significant increase in legitimate packet loss due to low-rate attacks by avoiding incremental cycles that could unnecessarily extend the active time for rejection rules.

Due to the unique characteristics of internet traffic that cannot be captured by traditional queuing models, Shahsavari et al. [23] proposed a novel model based on rule-based firewall performance modeling and analysis, considering the burstiness of incoming traffic and the correlation between arriving packets, utilizing discrete-time queuing systems. The performance of the proposed model is evaluated using metrics such as firewall CPU utilization, latency, packet loss, and throughput. They also initiated a potential DoS attack with extremely low speed against firewalls with different burst factors. To defend against this attack, they proposed a method based on assigning weights to rules based on previous matching counts and periodically reordering these weights.

TABLE III
Comparison of DoF defense techniques

Attack classification	Defense Technology	Scope of Adaptation
Burst attacks	Multidimensional continuous-time Markov chain model [13]	For cloud firewall performance
	Based on the computation of packet matching rule histogram and packet mismatch rule field histogram [14]	For firewall rules
Low-rate Attack	Based on generating an early rejection rule [22], [4]	For firewall rules
	Based on discrete-time queuing system [23]	
	Stateful session table based architecture [19]	For session tables

Table III compares the above DoF attack defense techniques.

V. Problems and Prospects

At present, there are still many challenges in the detection and defense against DDoS attacks on firewalls, which presents both opportunities and challenges for experts and scholars. In this section, we analyze from a technical perspective the numerous issues currently facing DoF defense, while also looking ahead to future research trends.

With the advancement of technology and the rapid evolution of information, attackers continuously upgrade their attack methods, rendering no single universal solution capable of completely mitigating such attacks. Therefore, the attack and defense against firewalls will remain a long-term issue requiring in-depth research. The prompt and efficient detection of attacks in their early stages, as well as subsequent mitigation processes, still necessitate exploration by experts and scholars. Several specific issues merit particular attention.

A. The escalating form of DoF attacks

DoF attacks are advancing towards characteristics such as stealthiness, low rate, distributed nature, and diversification, presenting defenders with increasingly complex challenges. Defenders are required to detect and filter out attack traffic at the source in the early stages of an attack. The success of attackers in launching attacks and causing harm to enterprise security implies the existence of vulnerabilities in firewalls themselves. Therefore, the updating and upgrading of firewalls cannot be ignored.

B. Data collection and analysis

Low-rate DoF attacks pose significant challenges to attack detection and defense due to their inherent stealthiness. Traditional feature-based detection methods have certain limitations, such as the correct extraction of

normal and abnormal traffic features. It is essential to analyze abnormal traffic features to further identify attack patterns and other pertinent information. Data collection and analysis are prerequisite steps in determining detection and mitigation models.

C. Algorithm selection and deployment

Through an investigation of relevant literature on DoS attacks, only a limited number of studies have proposed defense mechanisms against such attacks. Traditional solutions involve the construction of attack detection and defense models using techniques such as deep learning, statistics, software-defined networking, and blockchain. However, no single algorithm can be universally applicable to all types of DDoS attacks, and its effectiveness is constrained by specific network environments. Therefore, the deployment of algorithms needs to consider factors such as cost, types of attacks, network environments, and efficiency.

VI. Summary

As a barrier between local and external networks, a firewall serves to filter traffic, isolate risks, and protect the local network from external attacks. With the continuous escalation of DDoS attacks, firewalls themselves have become targets of such attacks. Attackers can migrate traditional flooding attacks to the firewall. Similarly, with the continuous improvement of attackers' professional levels, various new forms of DoF attacks targeting firewall rule libraries and session tables have emerged, causing financial losses to enterprises and individuals.

This article first provides a brief introduction to DDoS attacks and firewall technology, thereby introducing DoF attacks. Subsequently, this paper summarizes existing forms of DoF attacks from two perspectives: attack rate and attackers' targeting of firewall components. In addition to traditional flooding attacks, DoF attacks targeting firewalls also exhibit diversified characteristics, with many new attack methods emerging. Then, this paper evaluates and compares existing DoF attack detection and mitigation from two perspectives: attack detection and mitigation. However, existing anti-DoF attack technologies are insufficient, lacking in timeliness and adaptability to different network environments.Finally, this paper discusses typical problems existing in current research, hoping that the work done in this paper can provide some assistance to researchers in related fields and expand research ideas.

References

[1] M. Yue, H. Y. Wang ,Z. J. Wu ,and L. Liu, "A review of research on DDoS attack and defense techniques in cloud computing," Journal of Computer Science, vol. 43, no. 12, pp. 2315–2336, 2020.

[2] M. E. Tao, "Research and system implementation of SDN-oriented DDoS attack defense technology," Beijing University of Posts and Telecommunications, 2019.

[3] K. Salah, K. Elbadawi, and R. Boutaba, "Performance Modeling and Analysis of Network Firewalls," IEEE Transactions on Network and Service Management, vol. 9, no. 1, pp. 12-21, March 2012.

[4] Z. Trabelsi, S. Zeidan, and K. Hayawi, "Denial of Firewalling Attacks (DoF): The Case Study of the Emerging BlackNurse Attack," IEEE Access, vol. 7, pp. 61596-61609, 2019.

[5] C. C. Zhang, M. Winslett, and C.A. Gunter, "On the Safety and Efficiency of Firewall Policy Deployment," Proceedings of IEEE Symposium on Security and Privacy, May 2007.

[6] A. X. Liu, and M.G. Gouda, "Removing Redundancy from Packet Classifiers," Proceedings of ACM SIGCOMM, Portland, Oregon, August 2004.

[7] M. K. Yoon, S. Chen, and Z. Zhang, "Reducing the Size of Rule Set in a Firewall," Proceedings of IEEE International Conference on Communications, ICC'07, Glasgow, pp. 1247-1279, June 2007.

[8] F. Al-Haidari, M. Sqalli, K. Salah, and J. Hamodi, "An Entropy-Based Countermeasure against Intelligent DoS Attacks Targeting Firewalls," 2009 IEEE International Symposium on Policies for Distributed Systems and Networks, pp. 41-44, 2009.

[9] A. R. Khakpour, J. W. Hulst, Z. Ge, A. X. Liu, D. Pei, and J. Wang, "Denial of Firewalling," Citeseer, 2012.

[10] A. X. Liu, A. R. Khakpour, J. W. Hulst, Z. Ge, D. Pei, and J. Wang, "Firewall Fingerprinting and Denial of Firewalling Attacks," IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1699-1712, July 2017.

[11] K. Salah, P. Calyam, and R. Boutaba, "Analytical Model for Elastic Scaling of Cloud-Based Firewalls," IEEE Transactions on Network and Service Management, vol. 14, no. 1, pp. 136-146, March 2017.

[12] M. Liu, W. Dou, S. Yu, and Z. Zhang, "A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 3, pp. 621-631, March 1 2015.

[13] G. H. S. Carvalho, I. Woungang, and A. Anpalagan, "Cloud Firewall Under Bursty and Correlated Data Traffic: A Theoretical Analysis," IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 1620-1633, 1 July-Sept. 2022.

[14] Z. Trabelsi, L. Zhang, and S. Zeidan, "Dynamic rule and rule-field optimization for improving firewall performance and security," IET Information Security, vol. 8, no. 4, pp. 250–257, Jul. 2014.

[15] L. Alex, K. Amir, H. Joshua, G. Zihui, P . Dan, and W. Jia, "Firewall fingerprinting and denial of firewalling attacks," IEEE Transactions on information forensics and security, vol. 12, no. 7, pp. 1699–1712, Jul. 2017.

[16] P. A. Jishiya, A. James, and K. P. Swaraj, "Survey on various DDoS attacks on firewall and study on emerging DoF attacks," AIP Conference Proceedings, AIP Publishing, 2023, 2773(1).

[17] R. S. Yadav, and P. Likhar, "Firewall: A Vital Constituent of Network Security," Information Technology Security: Modern Trends and Challenges, Singapore: Springer Nature Singapore, no.47–67, 2024.

[18] P. A. Jishiya, A. James, and K. P. Swaraj, "Survey on various DDoS attacks on firewall and study on emerging DoF attacks," AIP Conference Proceedings, AIP Publishing, vol. 2773, no. 1, 2023.

[19] Z. Trabelsi, S. Zeidan, K. Shuaib, and K. Salah, "Improved session table architecture for denial of stateful firewall attacks," IEEE Access, vol. 6, pp. 35528–35543, 2018.

[20] L. Hansson, P. Hogh, B. Bachmann, K. Jor-gensen, and D. Rand, "The BlackNurse Attack, TDC Security Operation Center," Available: http://soc.tdc.dkl/blacknurse/blacknurse.pdf, 2016.

[21] Z. Trabelsi, and S. Zeidan, "Resilence of Network Stateful Firewalls against Emerging DoS Attacks: A Case Study of the BlackNurse Attack," 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1-8, 2019.

[22] K. Hayawi, Z. Trabelsi, S. Zeidan, and M. M. Masud, "Thwarting ICMP Low-Rate Attacks Against Firewalls While Minimizing Legitimate Traffic Loss," IEEE Access, vol. 8, pp. 78029-78043, 2020.

[23] Y. Shahsavari, H. Shahhoseini, K. Zhang, and H. Elbiaze, "A Theoretical Model for Analysis of Firewalls Under Bursty Traffic Flows," IEEE Access, vol. 7, pp. 183311-183321, 2019.
[24] J. Idziorek, M. Tannian and D. Jacobson, "Attribution of Fraudulent Resource Consumption in the Cloud," 2012 IEEE Fifth International Conference on Cloud Computing, Honolulu, HI, USA, 2012, pp. 99-106.