DDoS Protection Method for Servers

V Kh Fedorov¹, E G Balenko¹, E V Vershennik², P V Zakalkin²

¹Federal State Budgetary Educational Institution of Higher Education DON STATE AGRARIAN UNIVERSITY
pos. Persianovsky, 346493, Russian Federation
²FGKVOU VPO "Military Academy of communications named after Marshal of the Soviet Union S. M. Budyonny», St. Petersburg, 143900, Russian Federation

E-mail: balenko2008@mail.ru, Yelena.Vershennik@mail.ru

Abstract. Cyberspace, a global artificial space, has emerged and become part of all human activities, which exposes communication network elements, in particular service servers, to attacks, whether from individual hackers and cyberterrorists or from organized communities. Denial-of-service or DDoS attacks are the most common type. These are intended solely to cause a denial of service in various information systems, including service servers. This paper presents a method that can improve protection of servers that provide various resources (services) by reasonable management of filter rules and IP address lists.

1. Introduction
Today’s development of information and telecommunication networks (ITCN) focuses on:

- extensive adaptability to any physical infrastructure;
- use of distributed computing to enable flexible access to information and computational resources.

However, numerous groups of hackers and cyberterrorists continue to improve their methods of malware attacks, and they do it faster than data protection methods could adapt.

Distributed denial of service (DDoS) is a common type of such attacks. Importantly, the percentage of DDoS attacks in the totality of malware attacks (MA) has been on the rise, and some of such attacks have been significant in scale [1].

2. Statement of problem
The existing approaches to protection design cannot guarantee full DDoS protection due to the substantial time required to bring network elements back online. Besides, they do not implement complementary analysis of service data, which means that data does not get necessary updates. As a result, the existing DDoS protection solutions are ineffective [2-7].

Thus, a fundamentally novel DDoS protection method adapted to make the best use of protection functionality is objectively the most suitable solution.

3. Prepare input data
The proposed method uses the following data for input:
– network traffic filter rules;
– maximum performance of the service server;

In addition to that:
– create a control module to use whitelists and blacklists of IP addresses to adjust the filter rules: preset the whitelists and generate blacklists in Block 11.
– create a backup service server and an additional alert server to send service commands to switch to the backup server. The alert server can be a mail server, an SMS server, etc.
– connect the backup service server and the additional alert server to the communication network via an independent channel.

4. Theory
Figure 1 explains the implementation of the method. Once inputs are at hand, and all the required extra elements are set up, monitor network traffic and collect data on the server’s active connections. Make an inventory of the connections, write recipient’s / sender’s IP addresses and how many packets are being sent.

Use this data to calculate the current load on the server. Server load is number of connected users times user-sent data:

\[ R_{\text{ss}} = N_{a} \cdot V_{a} \]

where \( R_{\text{ss}} \) is the total load on the service server; \( N_{a} \) is the number of users; \( V_{a} \) is the amount of user-transmitted data.

![Flowchart diagram](image)
Figure 1. DDoS protection algorithm.

Given the load that MAs create, total load on the server is the normal host load + attack-induced load:

\[ R_{cy} = \sum_{i=1}^{j} R_{inf}^{yi} + R_{att}^{'}, \]

where \( R_{cy} \) is the total load on the service server; \( R_{inf}^{yi} \) is load from the communication nodes connected to the server; \( R_{att}^{'} \) is the load attributable to a DDoS attack.

Now verify the condition \( R_{cy} \geq R_{max}^{ip} \). If all conditions are true, go to Block 7; else, go to Block 3 and proceed to monitor network traffic.

In Block 8, log all the servers attempting to connect to the main server except the whitelisted IP addresses. In query logs, isolate non-whitelisted IP addresses that the server was accessed from, write them to the memory array \( M_{i} \).

In Block 9, reset all the connections to the whitelisted IP addresses, reboot the service server.

Proceed to monitor the network traffic of the main server. Process query logs and aggregate the data. When processing query logs, isolate IP addresses that attempted to but did not establish a connection.
In Block 11, isolate IP addresses that attempted to connect, write them to the memory array $M_2$. Compare $M_1$ and $M_2$ and write matching IP addresses to the memory array $M$. This new array is the blacklist of IP addresses. An IP address only found in either array is not a threat and need not be blacklisted.

Update the filter rules for the updated blacklist.

If the attack is not over yet, keep the whitelisted IP addresses connected to the backup server; otherwise, send service commands to reconnect them to the main server. Proceed to operate the service server with the updated blacklist.

Once the whitelisted nodes are reconnected to the main server, validate the received packets against the whitelist of IP addresses. Process packets received from whitelisted IP addresses. Should a packet be received from a non-whitelisted IP address, search for it in the blacklist. Forward packets received from blacklisted IP addresses to the cleanup.

The proposed method was tested for effectiveness as follows. An average DDoS attack lasts about 5 hours and overloads the server beyond the capacity, which causes a denial of service to legitimate users; besides, restoring the server back to its normal functioning takes time. Thus, the server will not be able to provide services to its users for the entire duration of a DDoS attack and post-attack recovery.

where $t_{oy}$ is the average time of denial of service; $t_a$ is the average recovery time.

As a DDoS attack begins, the proposed method reconnects all the currently connected users to the backup server over the time $t_1$, then processes network traffic over the time $t_2$ and generates an updated blacklist of IP addresses, then spends the time $t_3$ to reboot the server and the time $t_4$ to restore it back to normal operation as affected by the updated blacklist:

\[ t_{oy} = t_1 + t_2 + t_3 + t_4. \]  (4)

On average, reconnecting all the currently connected users to the backup server can take up to 10 minutes (including time to send the command to reconnect the whitelisted nodes to the backup server), traffic processing can take up to 20 minutes, reboot up to 15 minutes, and post-reboot recovery up to 40 minutes. Thus, the server will be fully back online in 1 hour and 25 minutes. This is a 4 times shorter denial of service compared to the prototype method.

5. Conclusions
The proposed method makes a blacklist of IP addresses during an attack; therefore, the blacklist is up-to-date for each specific attack. It updates in real time, eliminating the need to query blacklist providers.

Thus, the developed method improves server security by continuously servicing whitelisted IP addresses and running additional analysis of their blacklisted counterparts.

6. References
[1] Grechishnikov E V, Dobryshin M M 2015 Evaluation of the effectiveness of destructive software influences on communication networks Control, communication and security systems 2 pp 135-146
[2] Grechishnikov E V, Dobryshin M M, Zakalkin P V 2016 Model of a VPN access node as an object of network and streaming computer intelligence and DDoS attacks Cybersecurity Issues 3(16) pp 4-12
[3] Begaev A N, Grechishnikov E V, Dobryshin M M, Zakalkin P V 2018 Proposal for assessing the ability of a computer network node to function in conditions of information and technical influences Issues of cybersecurity 3(27) pp 2-8
[4] Starodubtsev Yu I, Brechko A A 2019 Modeling of communication networks operating in conditions of destructive program influences *Problems of defense technology Series 16: Technical means of countering terrorism* 1-2(127-128) pp 21-28

[5] Begaev A N, Dobryshin M M, Zakalkin P V, Reformat A N, Rautkin Yu V 2018 Complex algorithm for monitoring the protection of VPN nodes from computer intelligence and DDoS attacks *Elektrosvyaz* 7 pp 46-52

[6] Kotsynyak M A, Lauta O S, Ivanov D A, Lukina O M 2019 Model of the Impact of a Targeted Cyber Attack on an Information and Telecommunication Network *Problems of Defense Technology. Series 16: Technical means of countering terrorism* 3-4(129-130) pp 58-65

[7] Kotsynyak M A, Lauta O S, Nechepurenko A P 2019 Model of the system of influence on the information and telecommunication system of special purpose in the conditions of information confrontation *Questions of defense technology. Series 16: Technical means of countering terrorism* 3-4 (129-130) pp 40-44