DDefender® Solution Overview

Preventing Distributed Denial-of-Service (DDoS) attacks

Contents

1. Introduction

The goal of a Denial-of-Service (DoS) attack is to overload or flood the target device with requests and thus prevent its intended use. Overloading the network protections may also cause them to function incorrectly or poorly, which allows the DoS attacker to get through the compromised protection. DoS attacks pose a significant threat to online services, causing disruptions, financial losses, and reputational damage.

Distributed Denial of Service (DDoS) is a distributed version of the DoS attack, where the target receives data from multiple sources. DDoS attacks can be implemented with botnets, which consist of several infected network devices that are under the control of malware. Often the owner of the network device does not even know that the device has been infected and that a bot - an automated software program - is running in the background. The attacker sends instructions to the bots remotely through infected controller devices, as illustrated below in Figure 1. Large bot networks can be used for targeted DDoS attacks, and since the last few years, bot-driven attacks have become the most dominant form of DDoS.

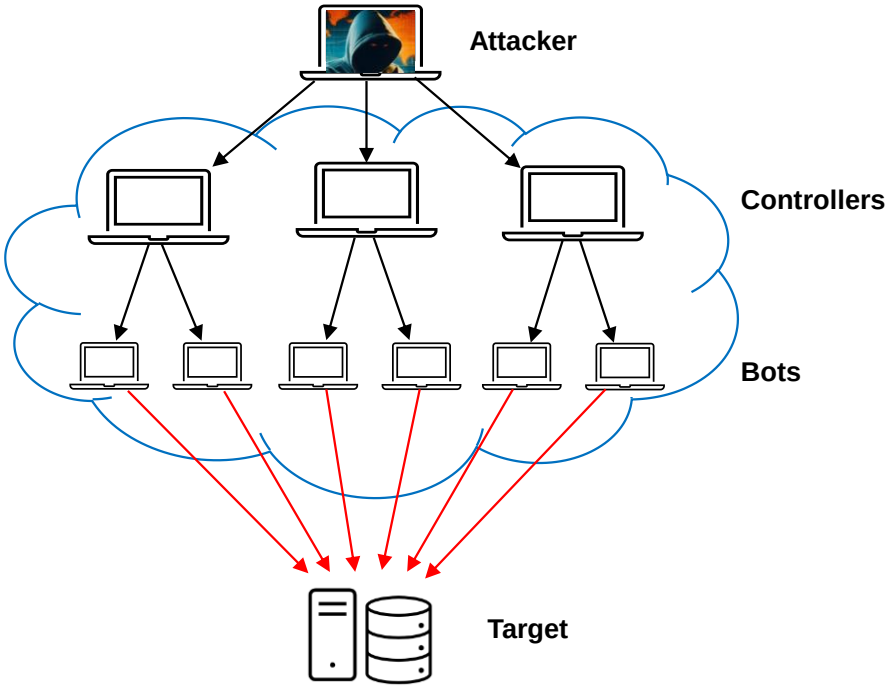

Figure 1. A DDoS attack using a bot network

Common DDoS attack types include Volumetric attacks, Protocol attacks and Application layer attacks. Volumetric attacks aim to congest the target network by sending massive amounts of data. Protocol attacks utilize weaknesses in OSI layers 3 and 4 protocols (network and transport layers) in order to overload network resources with a large number of connection or service requests. Application layer attacks, also known as layer 7 attacks, aim to overload services with connection openings and/or with service requests.

Attackers often use IP spoofing, i.e. modifying the source IP address, in order to hide the identity of the sender and to amplify the impact of the attack. For example, the attacker can amplify the attack by making requests to open DNS servers with a spoofed IP address of the victim, causing the servers to route their responses to the victim.

This Solution Overview describes how DDoS attacks can be eliminated with DDefender software tools. This document is intended for IT decision makers and security engineers who are familiar with the basic concepts of networking and security.

2. Impact of DDoS Attacks

The consequences of DDoS attacks can be quite significant for businesses and services:

- DDoS attacks can take down websites or services, leading to loss of availability for users and customers.
- The downtime caused by an attack can result in direct financial loss due to lost sales or transactions.
- Repeated attacks can harm a company's reputation, leading to loss of customer trust and potentially driving users to competitors.
- Responding to and mitigating DDoS attacks can consume significant IT resources and time.
- While a DDoS attack is ongoing, security teams may be distracted, potentially leaving other areas vulnerable to intrusion.

Figure 2. DDoS attackers often have financial, political or philosophical motivations.

3. Solution Overview

DDefender is a real-time network traffic monitoring system that is able to detect malicious traffic using protocol rules and features. The DDefender software can be deployed on industry standard devices in various kinds of local and cloud network environments. It works alongside the network to be protected, as depicted in Figure 3. The network traffic does not pass through DDefender but the analysis is done on the traffic copied through a mirror port, therefore the system does not cause any delays in the data transfer.

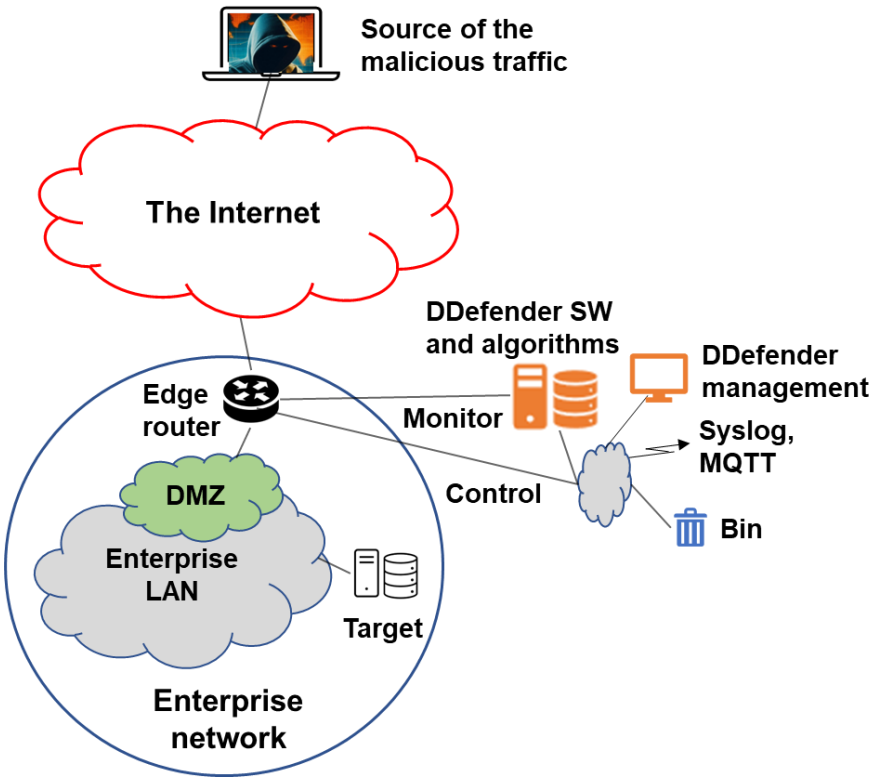

Figure 3. DDefender solution architecture

DDefender provides efficient tools to combat malicious network traffic and eliminate cyber-attacks quickly. All monitoring and analysis are based on IP protocol frames and protocol properties, which makes the system efficient and secure. The user data content is not processed in any way, and data security is never compromised. The DDefender tools are based on protocol manipulation and enable the attacks to be extinguished immediately at their source. The tools are particularly effective against DDoS attacks.

DDefender monitors both incoming and outgoing traffic and produces a real-time snapshot of the traffic profile. The snapshot shows the current load level of the monitored node, reports any malicious traffic and indicates network attacks. The DDefender monitoring and prevention tools are completely invisible to the protected network and to the Internet, therefore it is not possible for the attacker to disable the DDefender protection.

The network status can be monitored and defense measures activated easily through a browser-based management interface. It is also possible to transfer alarms and logs through standard Syslog and MQTT interfaces to third party management systems for further processing and analysis.

Figure 4 shows the key functions of the DDefender solution. The core of the solution is an algorithm-based protocol analysis engine. It checks the protocol frames of L2-L4 network traffic flows and identifies malicious traffic based on pre-defined algorithms and default network parameters. The Session Control function monitors UDP/TCP ports and sessions, it is able to identify malfunctioning applications and malfunctioning connections. The APP Layer 7 function detects application layer attacks as well as snooping and sniffing attempts. Other key functions include the Volumetric Attack Detection function, Thread Sources Identification function, and Security Processes function.

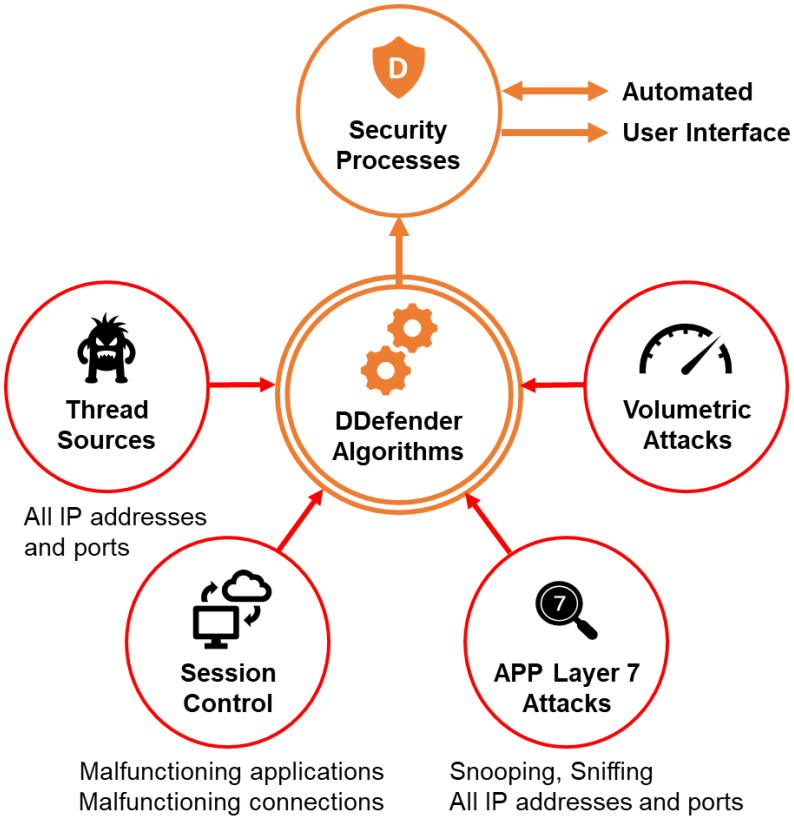

Figure 4. Key functions of the DDefender solution

A summary of the DDefender protection tools is shown in Table 1.

DDefender tool	Description
GameGUI®	Offers a unique graphical view of the organization's Internet data traffic and malicious data flows. The administrator can monitor the network status and initiate defensive actions through the GameGUI.
Turnpoint®	Session-control tool for monitoring data flows, identifying malicious traffic and eliminating DDoS attacks by bouncing the malicious traffic back to the attacker.
Red Button®	Tool for discarding outgoing or/and incoming malicious data traffic immediately, e.g. during volumetric DDoS attacks.
DLatenator®	Latency control software for slowing down malicious connection-oriented TCP data traffic, thus releasing bandwidth for the legitimate traffic.
Syslog or MQTT	Interface to 3rd party managements systems for further processing of alarms and logs.

Table 1. DDefender tools

4. How It Works

This section describes the step-by-step process of how the DDefender solution detects and mitigates DDoS attacks. We discuss the various types of DDoS attacks, including connection-oriented and connectionless attacks. Additionally, we explore spoofed attacks and their implications.

While traditional defense methods rely on traffic filtering, DDefender supports multiple defensive actions:

- Preventing the attacking devices from sending additional malicious traffic
- Slowing down the malicious traffic to release capacity for the legitimate traffic
- Discarding the malicious traffic
- Completely isolating the local network from the Internet

The innovative DDefender solution is able to block the DDoS attacker completely by bouncing the malicious traffic back to the attacker. As a result, the attacking device itself stops sending malicious traffic. Here’s a typical course of actions:

1. DDefender monitors and analyzes network traffic at the L2-L5 levels.
2. DDefender detects malicious traffic.
3. DDefender analyzes the characteristics of the malicious traffic.
4. DDefender exchanges source and destination addresses and sends the packet to the edge router.
5. The edge router sends the packet back to the sender.

6. The sender's network driver receives its own packet as a transmission acknowledgment.
7. The sender's driver interprets the received data packet as a communication error and enters the time-out mode.
8. In case of connection-oriented protocols (TCP), the time-out is typically a few seconds (e.g. Microsoft default is 3 seconds) at the first time and then doubled after each time-out. The data transfer will be terminated after approximately 10 attempts.
9. In case of connectionless protocols (UDP), the attacking application has to interpret the content of the data packets it gets back. This loads the application process and slows down the attack. Depending on the implementation of the malware, the attacking computer may get stuck temporarily.

This defense method works against both connection-oriented and connectionless protocols. It can eliminate attacks from any source, including botnets and Tor. Figure 5 shows how DDefender blocks the DDoS attack.

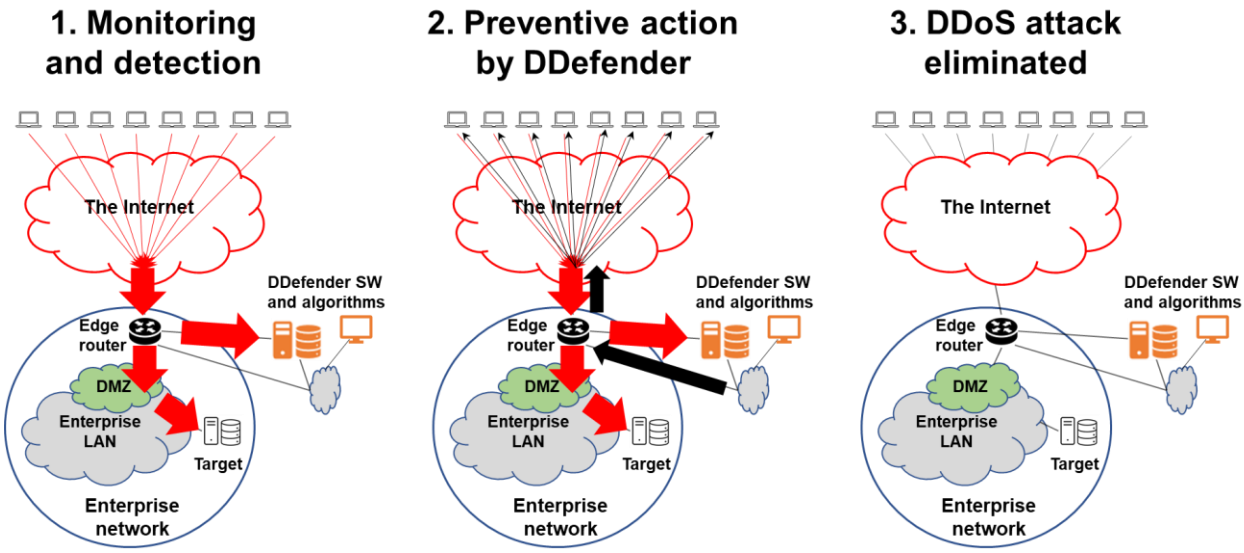

Figure 5. An example of how DDefender blocks the attacker

DDefender has also the ability to detect a spoofed DDoS attack. A short response is sent to the attacking address and the effect of the response is analyzed. If the attack is coming from a spoofed address, DDefender can hijack the DDoS traffic from the router and direct it to the bin. This terminates the network connection between the attacking device and the local network as long as the hijacking is kept active.

In volumetric DDoS attacks, DDefender detects the overloading malicious traffic and generates an alarm. The network administrator can use DDefender to send a slow-down command to the overloading device. This slows down the malicious traffic and releases network capacity for the legitimate traffic.

In an emergency situation like a sudden volumetric DDoS attack with snooping attempts, DDefender can completely isolate the local network from the Internet. DDefender can activate this mode through control messages to an existing network switch or router, it does not require additional network security devices.

5. Benefits

The DDefender system ensures business continuity and protects reputation by identifying unwanted traffic and eliminating DDoS attacks. DDefender monitors network traffic and analyses IP network protocols in real time. The intelligent algorithms of DDefender eliminate DDoS attacks by using protocol rules and features. DDefender runs on standard hardware and is invisible to the monitored network and to the Internet. The revolutionary DDefender system does not require packet filtering used in traditional firewalls or shield services.

Traditional DDoS protection methods include:

- over-dimensioning the capacity of the network and services in order to withstand an attack,
- using firewalls to reduce the attack surface,
- using Web Application Firewalls to configure blacklists and/or whitelists, and
- using shield services to analyze network traffic and filter out malicious packets.

A weakness of all these traditional methods is that the DDoS attack is not eliminated from the network.

While traditional protection solutions are location dependent, DDefender can be deployed where the protection is needed either locally or in the cloud. A single DDefender system can support multiple subnetworks.

Table 2 shows a comparison of the DDefender solution versus traditional DDoS protection methods.

DDefender	Traditional DDoS protection
The monitoring view shows the situation of both traffic directions	Usually only one direction is shown
Works also on encrypted network traffic (https, ftps, etc.)	Encrypted network traffic often causes difficulties
Analysis done on mirrored traffic	The traffic often passes through an active online security device
Not connected to the Internet	Usually requires a connection to the Internet
Easy to monitor traffic between protected networks	Often difficult and expensive to install in an internal network
Analyzes protocol frames, does not process data content	Often also the data content is analyzed, user data security can be compromised
Invisible to the Internet	An internet address is usually needed
The attack is eliminated and the load on the network is removed	Prevents the attack from reaching the target, the network load does not go away
Instant recovery from an attack	Recovery only when the attacker stops the attack
Treats the "disease" and its symptoms	Treats the symptom, not the "disease"
Easy and quick to deploy	May require extensive system knowledge and laborious maintenance of filtering rules and network configurations
Cost-effective additional protection for network data security	Often expensive and heavy solutions

Table 2. Benefits of DDefender vs. traditional DDoS protection

6. Case Study

This section provides an example of successful prevention of DoS attacks in a real-world customer network of Helsinki City Transport. Empirical tests were carried out in the customer network as part of this study.

During the monitoring period, DDefender detected occasional spying attempts on external network ports and external network scans. In addition, DDefender discovered a security issue in the customer's firewall configuration, and a corrective action was taken to fix the issue.

External DoS test attacks were carried out with the open-source Low Orbit Ion Cannon (LOIC) tool. For example, a User Datagram Protocol (UDP) flood attack was launched, sending a large number of UDP packets to random destination ports on the target

network, which can exhaust the network capacity on the target. When DDefender was activated to prevent the malicious traffic, the DoS attack stopped within few seconds.

More information on this case study is available from BouncePoint upon request.

7. Conclusion

DDefender provides you with the necessary tools and services to prevent DDoS attacks, helping you to ensure high availability, security and resiliency of your network. DDefender includes control tools for real-time monitoring and for quick and effective protection against cyberattacks.

The DDefender system is able to detect any type of malicious traffic and the protection is effective also for encrypted traffic.

Alarms and logs from the DDefender system can be transferred to other management systems if needed.

DDefender is based on unique, innovative and patented technology (over 15 patents).

DDefender complements traditional cybersecurity methods and can even replace them. DDefender safeguards your network against all kinds of DDoS attacks.

8. Contact information

We are always happy to help you with network analytics and DDoS protection. You can reach us at:

BouncePoint Ltd, Viikinkaari 6, 00790 Helsinki, Finland

Email: getit@bouncepoint.fi

www.bouncepoint.fi

BOUNCEPOINT

YOUR KEY TO

NETWORK SECURITY