Protecting Applications from DDoS Attacks

Technical Note

UPDATED: 22 March 2021

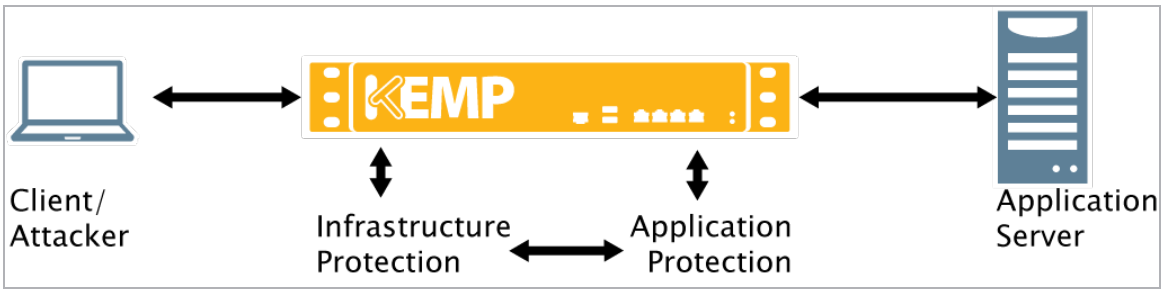
Copyright Notices

Table of Contents

1 Introduction

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks leverage stolen computing power from infected endpoints to flood target networks and web applications with malicious or spurious traffic. By consuming available network bandwidth or server resources, DoS attacks disrupt the online operations of target organizations. These attacks reduce the amount of computing resources available to legitimate end users and can cause massive economic and reputation impact.

In general, any organization that has a significant online presence - such as finance, retail, healthcare, entertainment and technology companies - are likely targets. DDoS attackers have typically focused on infrastructure (network and session) level attacks, but application-centric attacks are becoming more common.



The Kemp LoadMaster network processing engine provides protection against common infrastructure attacks. The Kemp Web Application Firewall (WAF) augments our network processing engine by preventing application-specific attacks. The LoadMaster also includes additional security controls to stop, shape, steer, secure, and manage traffic to limit the likelihood and impact of DDoS attacks. The Kemp LoadMaster should be thought of as a part of a comprehensive defense in depth strategy – providing another layer of defense against skilled and organized attackers.

Please note that DoS and DDoS are used interchangeably in this document with the main difference being scale of attack – the mitigation strategies are the same.

1.1 Document Purpose

This document seeks to summarize our DoS/DDoS protections at a high level. Please contact Kemp for additional information and detailed guidance.

1.2 Intended Audience

This document is intended to be most useful for security architects, network engineers, and enterprise IT managers. Kemp welcomes questions and feedback.

1.3 Related Firmware Version

Published with LMOS version 7.2.48.3 LTS. This document has not required substantial changes since 7.2.48.3 LTS. However, the content is in sync with the latest LoadMaster LTS firmware.

1.4 DDoS Overview

DDoS attacks are growing in frequency – in a recent study by Akamai, they found that the number of DDoS attacks increased by 116% in Q1 2015, compared to Q1 2014. They also found that the application layer attacks increased by 59%, while infrastructure layer attacks increased by 125%.

DDoS attacks are increasing in magnitude - There is an increase in Amplification attacks. These attacks involve sending small requests to servers that return a significantly larger response. In 2013, hackers used a DNS reflection attack to generate a peak of 300 Gbps of attack traffic.

DDoS attacks are growing in sophistication – traditionally attackers used TCP and UDP floods to consume network bandwidth. More recently, attackers are targeting application layer protocols and services with greater frequency. A few examples are:

- Hackers leverage application-layer attacks by sending Hyper Text Transfer Protocol (HTTP) “GET” method requests for large Portable Document Format (PDF) files, thereby successfully exhausting server resources with few requests.
- Hackers create significant latency by targeting “heavy URLs” that require complex database queries.
- Hackers blend network and application-layer attack techniques to generate large amounts of traffic that consume significant bandwidth and, execute complex transactions that consume server resources.

2 Types of DDoS Attacks

Refer to the below sections for further information on some DDoS attack types.

2.1 Infrastructure (Network & Session) Layer Attacks

Infrastructure layer (Layer 2 to 4) DoS attacks flood the network with unnecessary traffic until systems become unavailable. The Kemp LoadMaster network processing engine validates connections and checks for protocol correctness (header, URL, HTTP version, method) while proxying and protecting the Real Servers.

The LoadMaster can help mitigate the below categories of attacks via the:

- Network processing engine
- WAF engine and subscription rules
- Whitelist/blacklists
- High capacity connection ability
- Content switching
- SSL/TLS termination and SSL/TLS validation

2.1.1 SYN Flood Attack

The attackers use half-open TCP connections to cause the server to exhaust its resource by keeping the information describing all pending connections. This results in a system crash or system failure.

2.1.2 TCP Reset Attack

By listening to the TCP connections of the victim, the attacker sends a fake TCP RESET packet to the victim. This causes the victim to inadvertently terminate its TCP connection.

2.1.3 ICMP Attack

The attacker broadcasts a large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP to the network. Most devices on the network will (by default) respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes

impossible to work. ICMP datagram can also be used to start an attack via ping. Attackers use the ping command to construct oversized ICMP datagram to launch the attack.

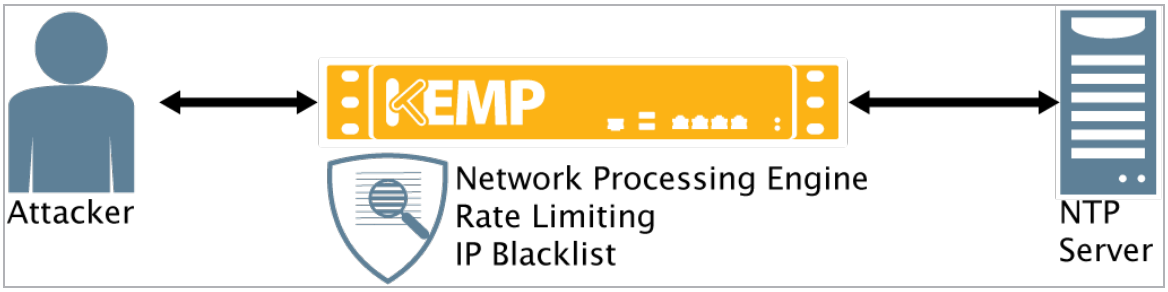
2.1.4 UDP Storm Attack

This kind of attack impairs the host's services and congests or slows down the prevailing network. In this attack, a connection is established between two UDP services, each of which produces a very huge number of packets.

2.1.5 Reflected request (DNS/NTP) attack

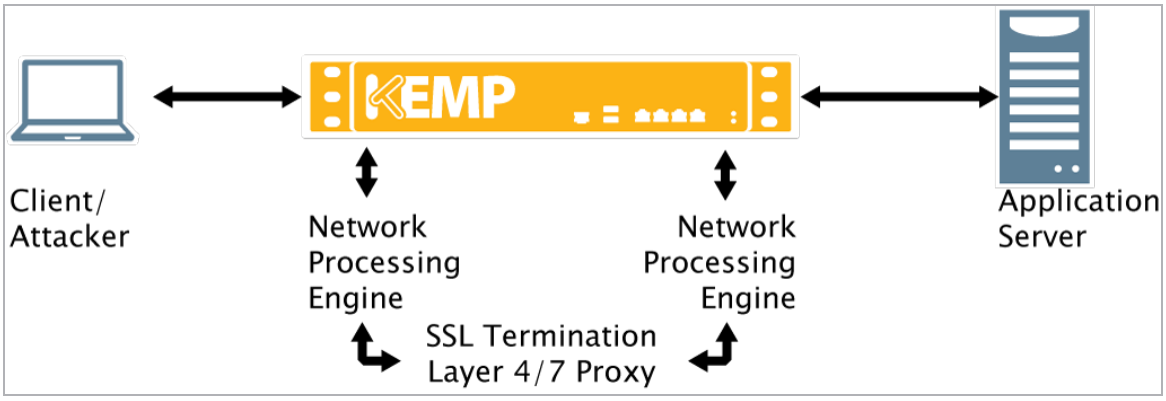
In this attack scenario, the attacker sends a large number of UDP-based requests to a name server or NTP server using a spoofed source IP address. Then the server, acting as an intermediate party in the attack, responds by sending information back to the spoofed IP address which is the victim. Because of the amplification effect of an unproportional response, it can cause serious bandwidth shortage. For example, a reflected NTP attack can amplify 556 times the amount of traffic as used to create the attack making it easy for attackers to force multiple their stolen resources.

The below figure show some mechanisms on how a Kemp LoadMaster can mitigate NTP servers being from being part of a NTP amplification attack.



2.2 Application Layer Attacks

An application layer DDoS attack overloads specific functions or features of a website with the intent to disable them, crash the application or take the site down. Infrastructure layer based attacks account for a large share of DDoS activity. In Q1 2015, application layer DDoS attacks accounted for less than 10% of all activity, while the infrastructure layer experienced 90% of DDoS attacks. However, the use of attack scripts that leverage open proxies on the Internet may pave the way to an increase in application-based DDoS attacks going forward.



Application layer attacks are hard to prevent and protect against with edge security devices, as application context is generally required for appropriate mitigation. LoadMasters that are in the critical data path and have knowledge of the application and network are well suited to provide application centric DDoS/DoS protection, due to the following features:

- Network processing engine
- WAF engine and subscription rules
- Whitelist/blacklists
- High capacity connection ability
- Content switching
- SSL/TLS termination and SSL/TLS validation
- Global Server Load Balancing (GSLB)
- HTTP/HTTPS proxying

2.2.1 GET Flood and Recursive GET Flood

The attack repeatedly requests a specific HTTP URL or all of the URLs in a web application. This can have a massive performance impact on the targeted server.

2.2.2 POST Flood

This attack generates HTTP POST requests, which are generally handled directly by the targeted Real Server causing a significant performance impact.

2.2.3 Slow Loris

The attacker opens connections to the target web server and keeps sending partial requests. Periodically, it will send subsequent HTTP headers, to keep the connection open. The affected

servers will fill up their maximum concurrent connection pool and deny additional connection attempts from clients.

References

References are listed below:

US patent application publication, Application number - US 13/458,129 - System and method for mitigating application layer distributed denial of service attacks using human behavior analysis

https://www.google.com/patents/US20130291107

Akamai's [state of the internet] / security - Q1 2015 State of the Internet — Security Report

Analysis of the Global Distributed Denial of Service (DDoS) Mitigation Market - Frost & Sullivan's Global DDoS Mitigation Market Research Report, July, 2014

2015 Data Breach Investigations Report – Verizon

Last Updated Date

This document was last updated on 22 March 2021.