
kemp
Averistar
2020
Summit
US Department of Justice Deployment Presentation
Kemp LoadMaster Security & DDoS Prevention
Frankie Cotto, Enterprise Engineer

Table of Contents

kemp

About Kemp

25,000+
customers

100,000+
deployments

115
countries

New York City

Limerick

Munich

Hannover

Singapore

Kemps mission is to provide invisible technology with a visible impact, making it easy for our customers to power an always-on application experience.

US Department of Justice Deployment Requirements

Intelligent Application Server Load Balancing

Intelligent Application Server health checking

Server Token Server Side Authentication

BroadWorks SAML Integration with Okta IDP

Appliance & Site to Site Redundancy

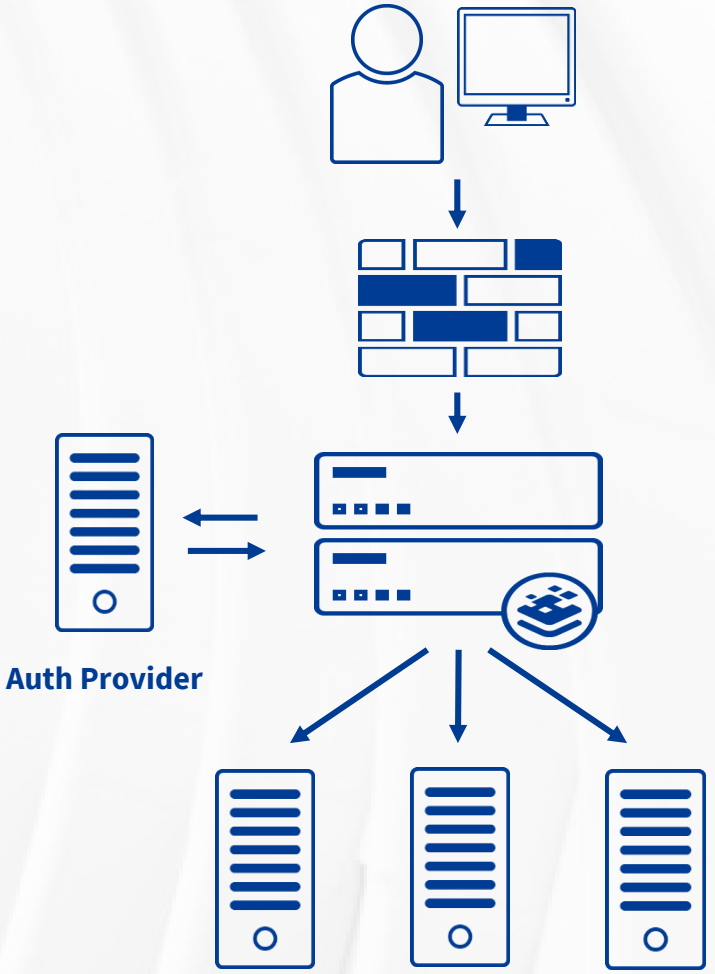
Application Security & Intrusion prevention

kemp

Edge Security Pack (ESP)

The Kemp ESP offers the following key features:

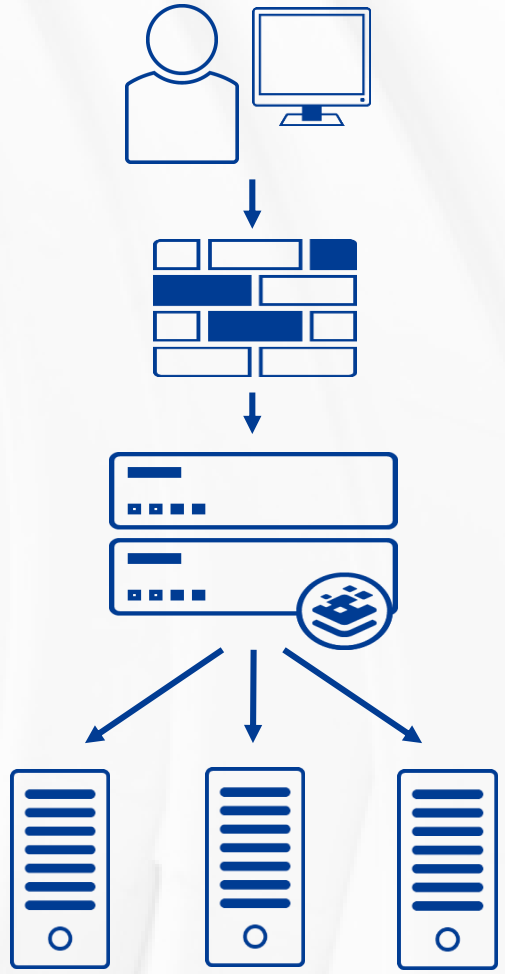
- End point authentication for pre-authentication.
- Persistent logging and reporting for user, connection, & security logging.
- Single Sign-On (SSO) across Virtual Services load balancing different workloads.
- Dual-factor authentication.
- Custom forms based authentication SSO image sets.
- Allowed virtual hosts and directory access limiting.



For more details see the Kemp Edge Security Pack feature description article.

High Availability (HA)

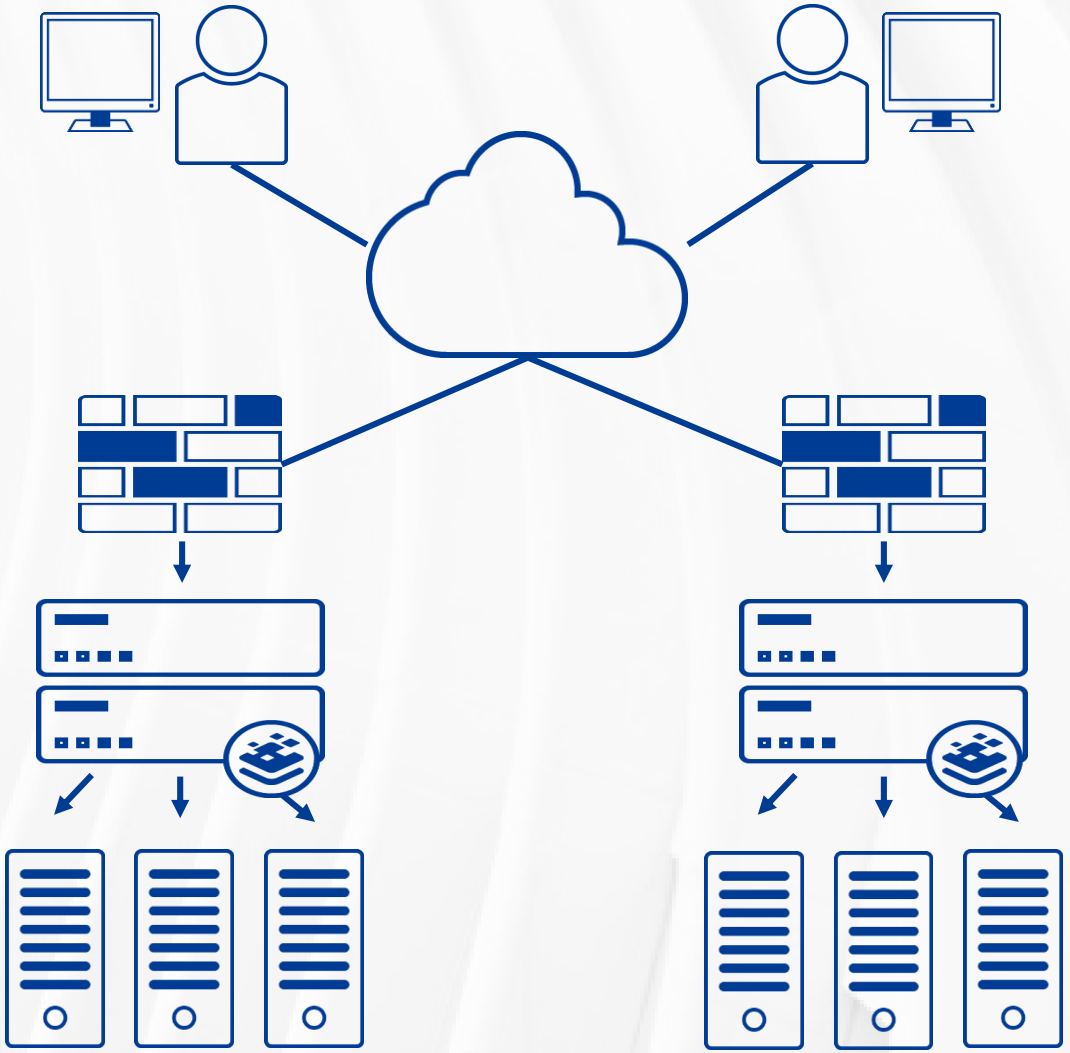
- The High Availability (HA) feature of the LoadMaster guarantees the availability of your server farm.
- HA is achieved by a hot-standby, failover mechanism.
- Two identical LoadMaster units are integrated into the network as a cluster.
- One machine serves as the active LoadMaster and the second one remains in a standby, idle state - always prepared to take over the activities from the active server.
- This cluster appears as a single logical unit to the internet side and to the server farm side connections.



For more details see the Kemp High Availability feature description article.

Global Server Load Balancing (GEO)

- Intelligently distributes traffic across server arrays or data centers.
- Reduces the need for increasingly larger and more expensive servers to accommodate increases in network traffic.
- Enables many distributed application servers to function as a single, virtual server.
- Reduces the risks of having all application resources deployed at a single geographical location.



For more details see the Kemp GEO feature description article.

kemp

Security & DDoS Prevention

Attackers use a number DDoS attack methods in order to slow down or shut down voice networks , infect systems with worms and viruses, and gain access to configurations files that contain user sensitive data.

The LoadMaster can help mitigate the below categories of DDoS attacks via its intrusion prevention system, client limiting, web application firewall engine and subscription rules, whitelists/blacklists, high capacity connection ability, content switching, SSL/TLS termination, and SSL/TLS validation.

Infrastructure (Network & Session) Layer Attacks

SYN Flood Attack

ICMP Attack

TCP Reset Attack

UDP Storm Attack

Application Layer Attacks

Slow Loris

POST Flood Attack

GET Flood and Recursive GET Flood

kemp

Web Application Firewall

When WAF is enabled, the WAF engine scans every incoming HTTP packet - running through each assigned rule individually and deciding what action to take if a rule is matched. The rules can be run on requests and responses.

In addition to protecting against DDoS attacks, WAF can protect your applications against the following attack categories and vulnerabilities.

OWASPs Top Ten Vulnerabilities

Cross-Site Scripting (XSS)

Unvalidated redirects and forwards

Missing function-level access control

Sensitive data exposure

Injection (SQL Injection Attacks)

Broken authentication and session management

XML External Entities (XEE)

DDOS Attacks

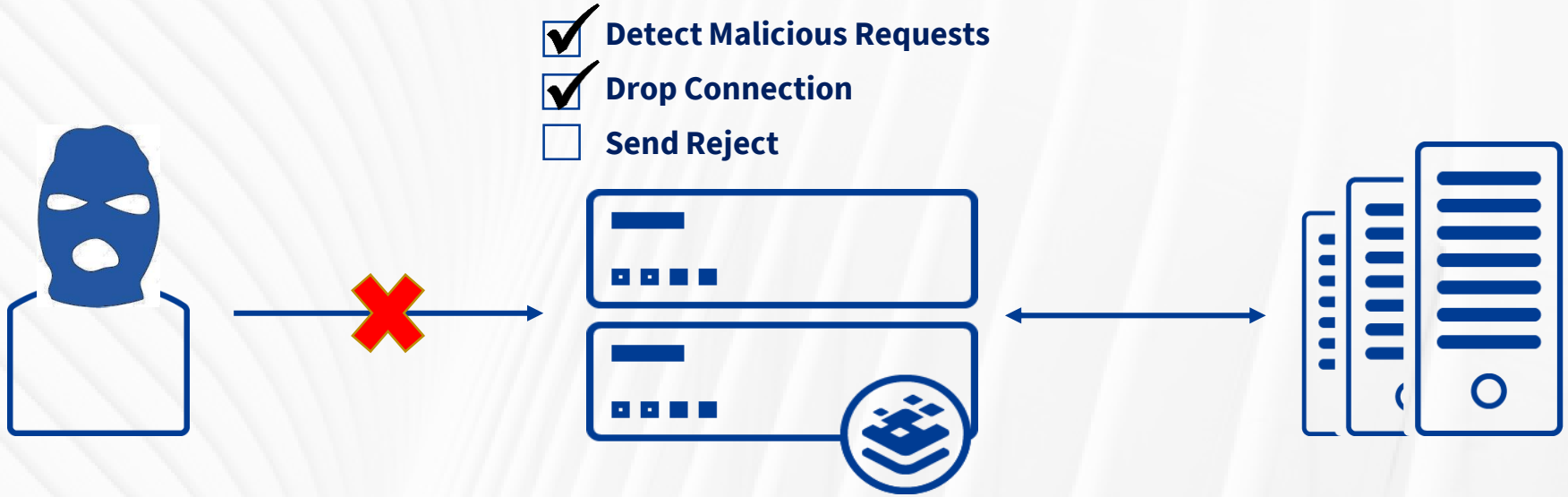
Security misconfiguration

For more details see the Kemp Web Application Firewall feature description article.

kemp

Intrusion Prevention System

- The Kemp Intrusion Prevention System is powered by SNORT. SNORT rules can be imported to the LoadMaster and applied to HTTP/HTTPS service type virtual services.
- SNORT rules can be custom created and edited to fit your application security needs.
- False positive handling, customer detection levels, and intrusion logging
- Global per host connection per second client limiting



Content Switching & Access Lists

Kemp Content Switching enables you to leverage Content Rules in order to:

- Add, replace, or delete HTTP headers.
- Modify request/response URLs sent to and from your application servers.
- Strip out sensitive server information.
- Match on URLs, HTTP headers, Source IPs, or request bodies in order to force connections to close.
- Use replace HTTP header rules to Secure cookies set by your application servers.

Kemp also offers the ability to set global or per virtual service whitelists or blacklists preventing access from individual IP addresses or entire subnets.

kemp

Why Kemp?

- Kemp is the industry application server load balancing price/performance leader. 4x the throughput per $ compared to F5/Citrix.
- Proven technology at an affordable price.
- Appliance availability - software, hardware or cloud.
- Multiple licensing options - permanent, subscription or consumption.
- Unmatched industry leading always-on global support.

For more information or to learn more about how Kemp can meet your application delivery needs, please feel free to contact us:

Timothy Quinn
Director, Partner Development
Kemp
T: +1 (631) 418-7733
E: tquinn@kemp.ax

Frankie Cotto
Enterprise Engineer
Kemp
T: +1 (631) 259-4711
E: fcotto@kemp.ax

kemp

References

Protection from DDoS Attacks –
https://support.kemptechnologies.com/hc/en-us/articles/208758696-Protecting-from-DDoS-Attacks

Kemp Web Application Firewall (WAF) –
https://support.kemptechnologies.com/hc/en-us/articles/203128369-Web-Application-Firewall-WAF-Feature-Description

Kemp High Availability (HA) –
https://support.kemptechnologies.com/hc/en-us/articles/203125199-High-Availability-HA-

Kemp Global Server Load Balancing (GEO) –
https://support.kemptechnologies.com/hc/en-us/articles/203125189-GEO-Feature-Description

Kemp Edge Security Pack (ESP) –
https://support.kemptechnologies.com/hc/en-us/articles/203125029-Edge-Security-Pack-ESP-

Kemp Content Rules –
https://support.kemptechnologies.com/hc/en-us/articles/203125019-Content-Rules

kemp