Securing Legacy Applications

Security Use Cases for Kemp Loadmaster

Pavel Minarik . Chief Technology Officer

Cyber Security Facts and Figures

18,362

The number of vulnerabilities published in 2020 by the US Government National Security Database

32%

The percentage of vulnerabilities in internet facing applications that are high or critical severity according to Edgescan's 2021 Vulernability Report

1 in 4

The number of companies still vulnerable to the WannCry ransomware because they haven't patched their systems yet according to research by Positive Technologies

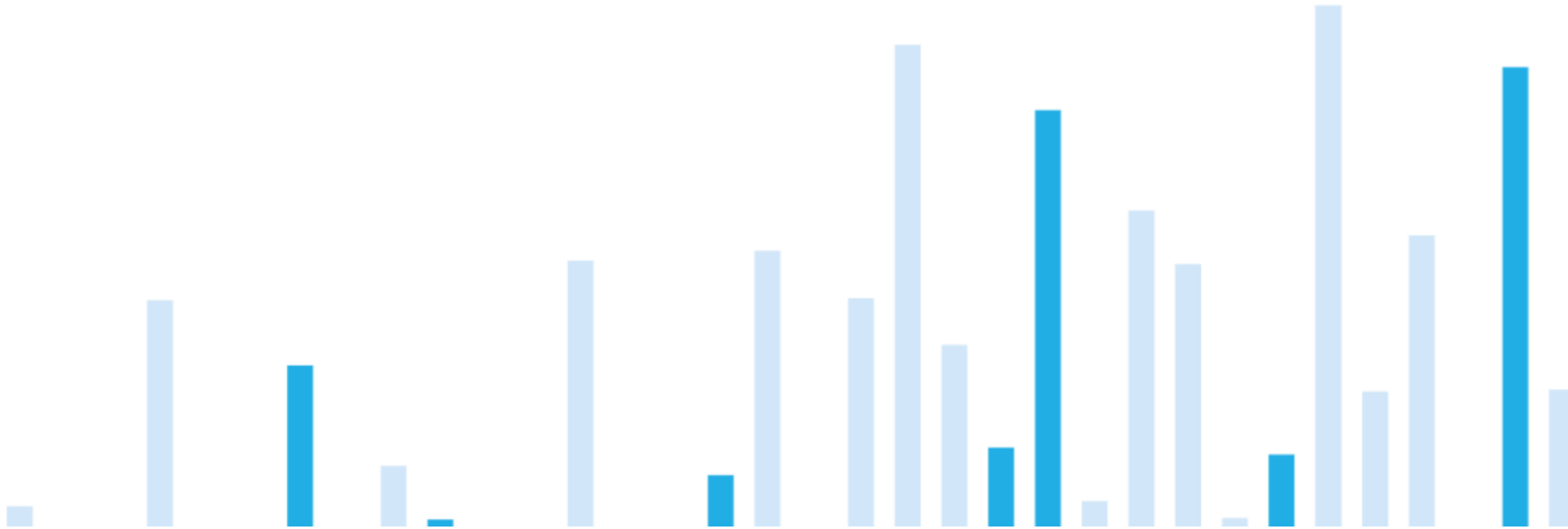
75%

The percentage of applications that contain at least one vulnerability according to Veracode's 2020 State of Software Security report

kemp

Kybernetické incidenty pohledem NÚKIB

Srpen 2021



kemp

Nejpoužívanější technika měsíce: Zneužití aplikací otevřených do internetu [5]

Útočníci v srpnových incidentech nejčastěji zneužívali aplikací otevřených do internetu (Exploit public-facing application). Do systémů obětí pronikli skrze nedostatečně zabezpečené webové servery, VPN nebo Remote Desktop Protocol (RDP), který se používá pro vzdálenou správu počítače.[6]

Exploit public-facing application je technika, kterou útočníci zneužívají slabých míst v systémech otevřených do internetu. Takovým slabým místem může být například nevhodné nastavení zabezpečení ze strany oběti nebo chyba, která vznikla při psaní programu.

MITRE ID: T1190

Mitigace: Organizace mohou zmírnit riziko úspěšného zneužití této techniky tím, že do in-

Challenges of Legacy Applications

Encryption. Does the application use encryption? Is it configured to use the latest secure encryption standards and cipher suites?

Vulnerabilities. Is the application vulnerable to common attacks? How does it protect itself against OWASP Top 10 attacks?

Authentication. Is authentication enforced prior to any interaction with the application? Are best practices such as SSO or MFA implemented?

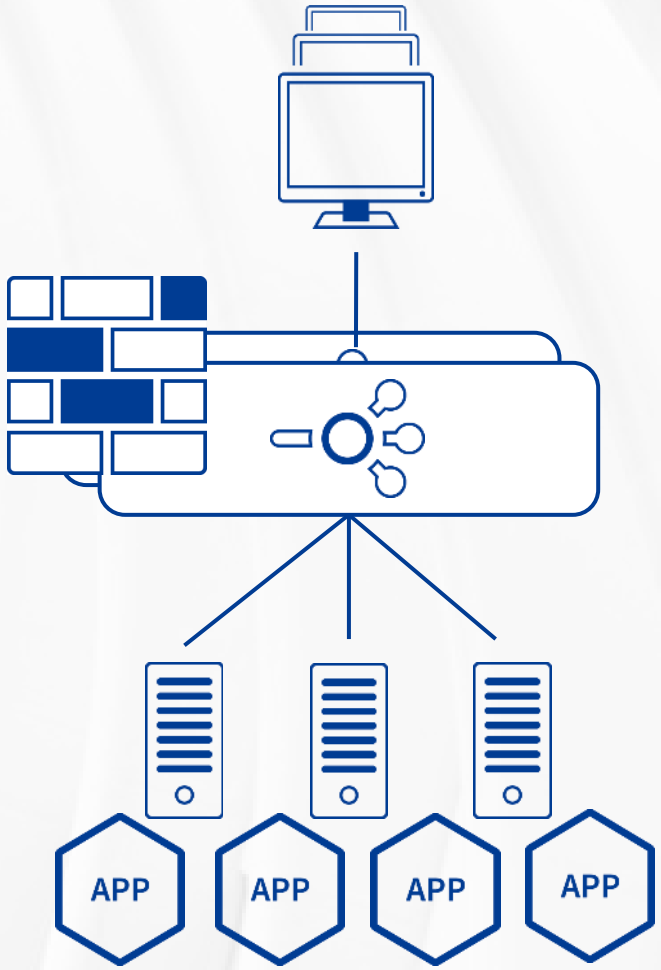
Regulatory requirements. Mandate certain level of security compliance for regulated industries.

We all have legacy applications. It is difficult to decommission them due to the business value they deliver. A lot of technical debt is carried over. Modernization is a long, painful and expensive process.

Load Balancers Isolate Applications

Load Balancer function	OSI Layer
• Hide server network as reverse proxy	**Layer 1/2**
• Hide server IP with Virtual IP	**Layer 3**
• Only allow specific TCP/UDP ports	**Layer 4**
• Advanced content rules	**Layer 7**

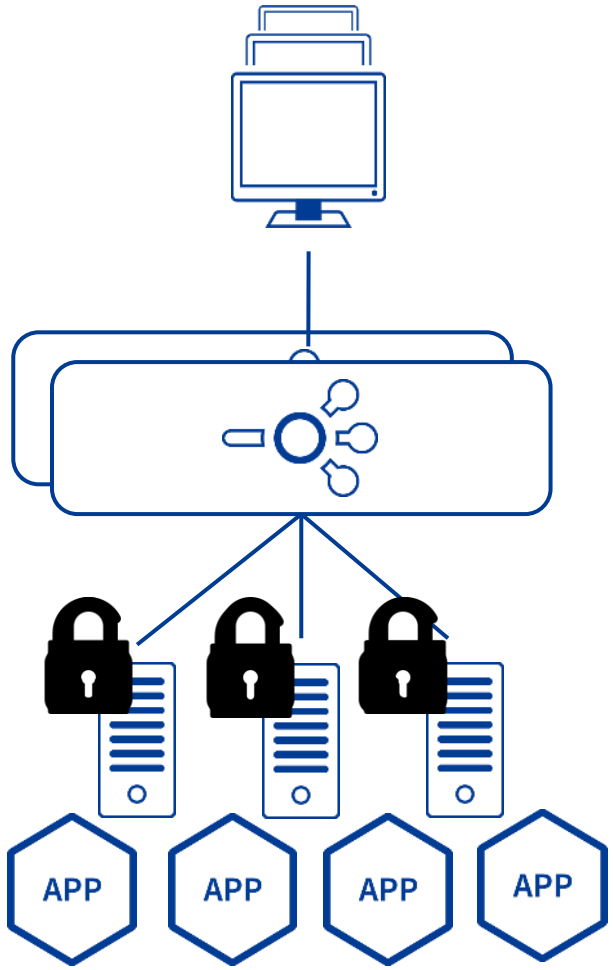
Load Balancers perform the same functions as a traditional firewall!



kemp

Offload Encryption

- Move SSL/TLS encryption processing to the load balancer
  - Eliminates server overhead
- Centralize certificates
- Use consistent and current algorithms
- Enforce proper security levels
  - ECC, TLS 1.3, etc.



kemp

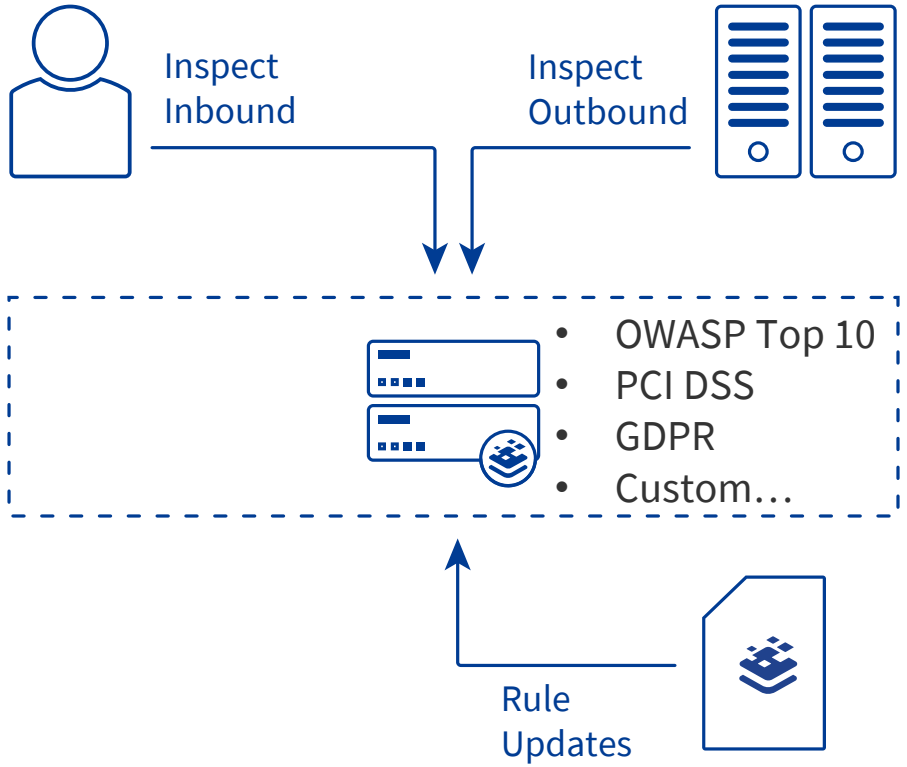
Content Validation

Web Application Firewall (WAF)

- Real-time threat protection for packaged & custom applications
- Mitigation of the OWASP Top 10 common vulnerabilities

Content rules

- Specific policy to enforce application clients
  - Operating system and version
  - Browser and version
- Custom content rules



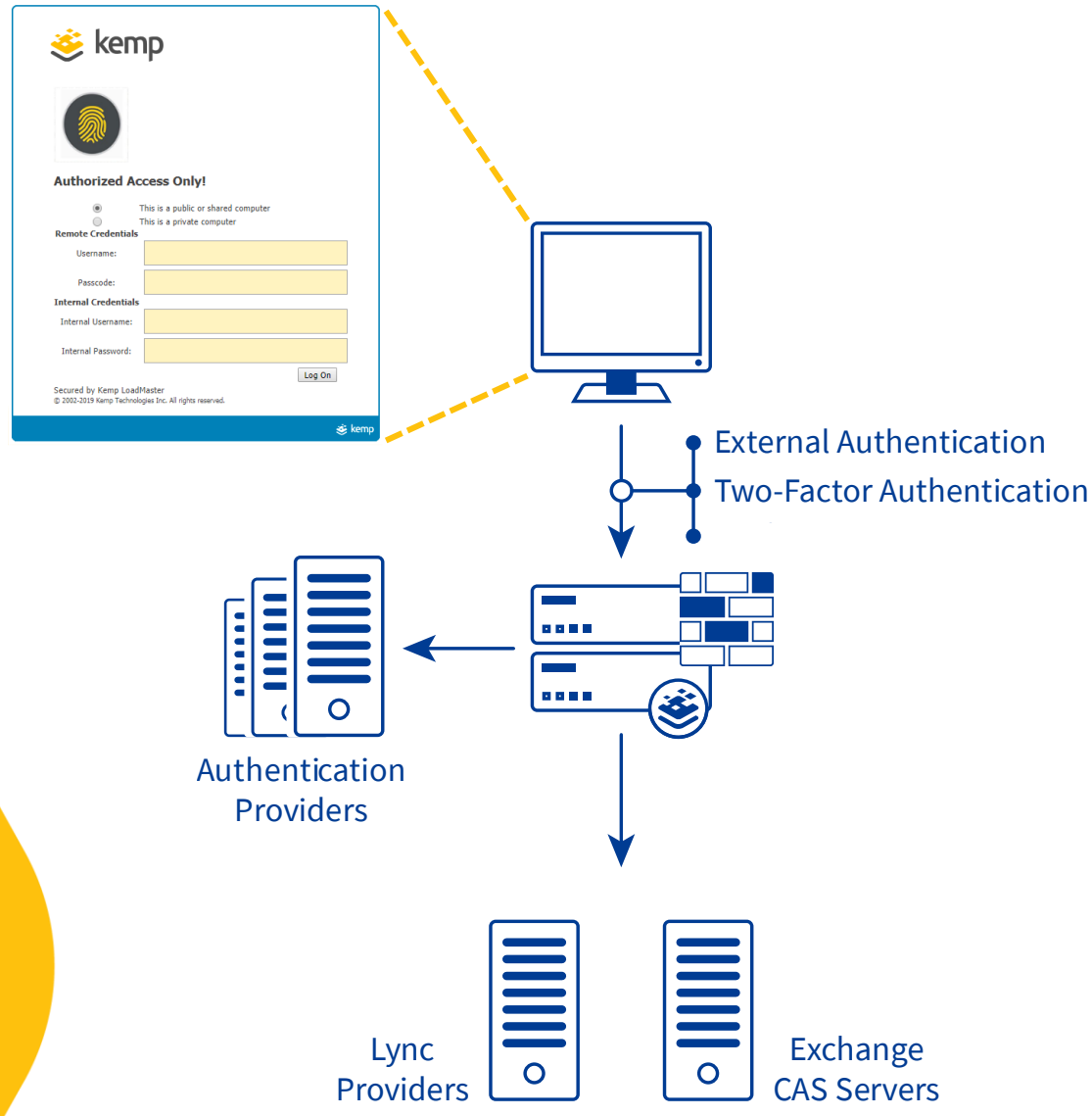
kemp

Edge Authentication

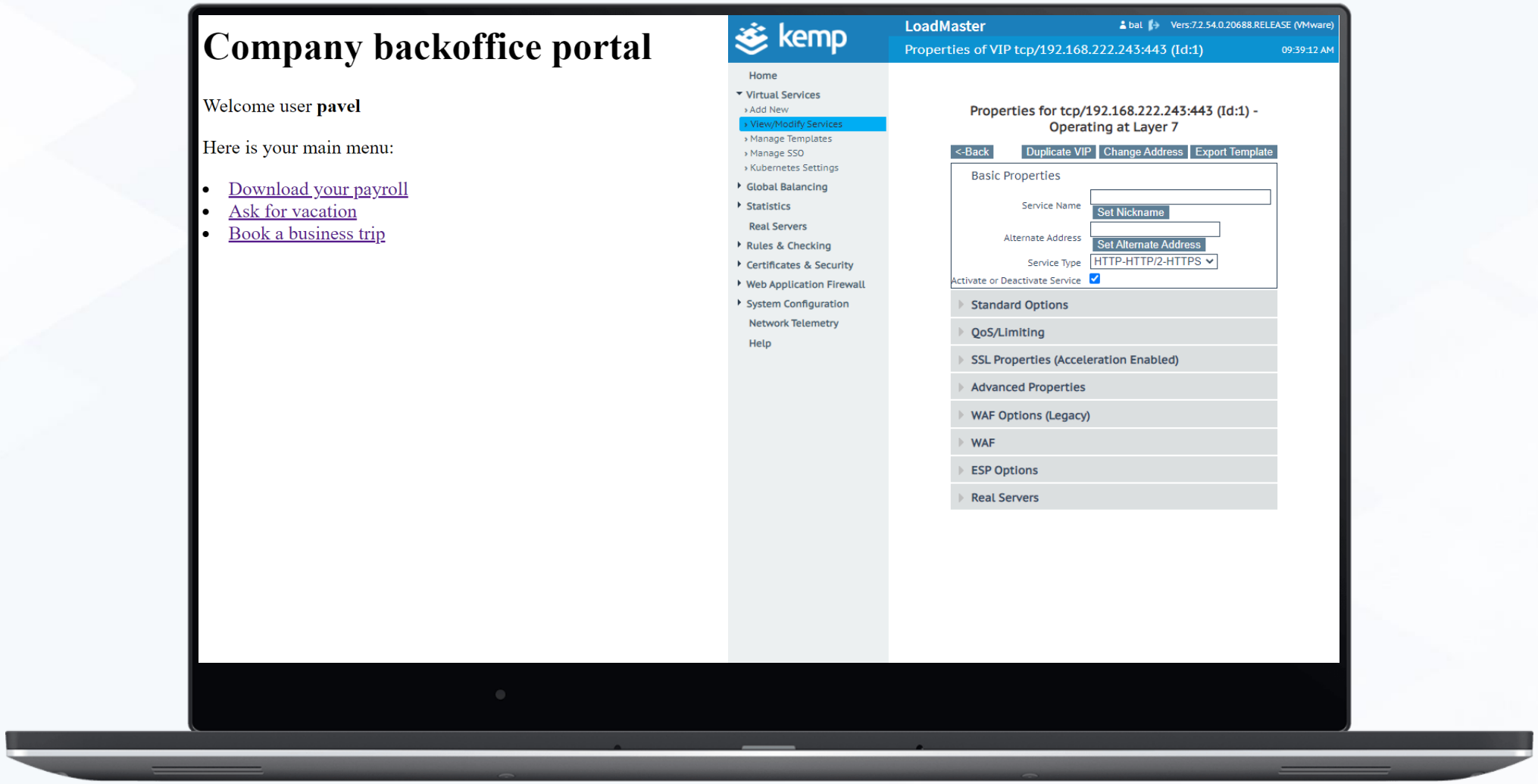
Advanced client authentication

- 2 factor authentication (2FA)
  - Token, SMS, etc.
- Multiple authentication data sources
  - Active Directory, LDAP, RADIUS, etc.
- Single Sign On (SSO)

Nobody is allowed to access the application while not authenticated properly > **Zero Trust**



Live Demo: Securing a legacy application

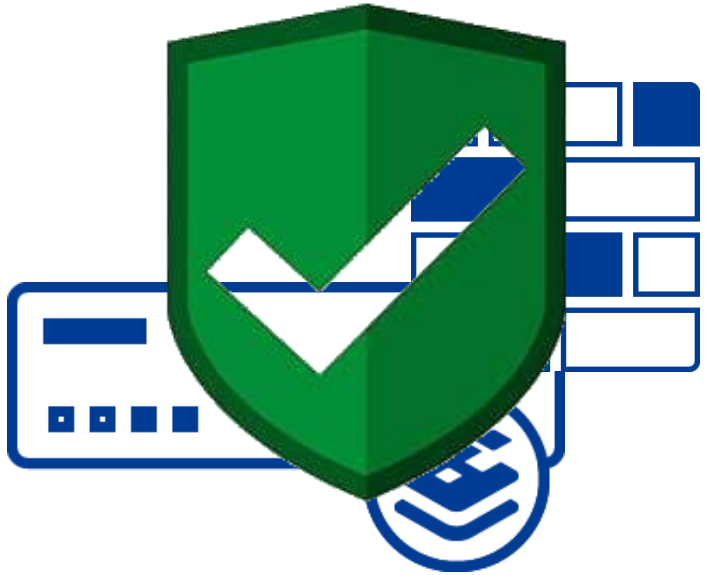


kemp

Summary

- Achieved by combining current functionalities
  - Load balancer (reverse proxy) as such
  - SSL offloading
  - WAF and content rules for policy enforcement
  - ESP for authentication
- Use cases
  - Securing a legacy application
  - Publishing an application without VPN access

Zero Trust Access Gateway



kemp

Further Reading

- Understanding Load Balancing Essentials [BLOG]
- Publishing & Securing Legacy Applications [BLOG]
- Global Site Load Balancing Explained [BLOG]
- User Identity Awareness with LoadMaster ESP and Flowmon [BLOG]
- Kemp Zero Trust Access Gateway [Overview]
- Getting Started with LoadMaster Network Telemetry [BLOG]

kemp

Thank You

kemp.ax