kemp

WHITEPAPER

Key Considerations for US Federal Agencies

Application Load Balancing

OVERVIEW

Mission accomplishment by US federal agencies depends on the performance, availability, and security of IT applications. The primary technology deployed to meet these requirements is called an application delivery controller (ADC) more commonly known as a load balancer. There are several key issues to consider when comparing top load balancer manufacturers for federal government use and ownership strategy that can significantly impact Total Cost of Ownership (TCO) and Return on Investment (ROI).

Load balancers enable the security, availability and performance of network-based applications by providing a combination of application proxy, authentication proxy, Web Application Firewall, application load balancing, content-based steering, global load balancing and distributed denial of service (DDOS) mitigation services. These services ensure the application server is protected from bad actors while at the same time addressing application performance and availability to ensure users receive the best possible application experience (AX).

Application proxy addresses the security and enhances the performance of application servers. Authentication proxy protects authentication servers from bad actors while providing application users a rich single sign on (SSO) experience. Web Application Firewall (WAF) protects websites from application level cyber-attacks. Application load balancing provides advanced scheduling, persistence, application heath checking, and content steering algorithms to ensure that clients can connect to the correct application instance and, if necessary, reconnect to the same application instance. Global load balancing addresses multiple data centers or cloud hosting environments to ensure users are connected to locations providing the best application experience while health checking these locations and automating the process of continuity of automation in the event of site level failures. DDOS and Intrusion Prevention Services (IPS) mitigate protocol based (network based) attacks to ensure application services are available in hostile network environments.

The US government model of doing business can be very different from how traditional private enterprises work. Governmental organizations are not profit driven; instead they are mission driven and must deliver required services, often with constricted budgets and manpower. For these organizations, finding solutions to meet their operational requirements that are easy to operate and affordable are critical to their sustainable success.

US FEDERAL ADC VENDORS

The US Federal government ADC load balancer market is dominated by four manufacturers: F5 Networks (F5), Citrix Netscaler, A10, and Kemp Technologies (Kemp). Only these four manufacturers of ADCs are certified by the US Joint Interoperability Test Center (JITC) and listed on the US Department of Defense (DoD) DODIN Approved Product List (DODIN APL) under the Cyber Security Tools category. Each has strengths and weaknesses, and all have implemented required US Federal specific features to varying degrees. There are cloud service providers that have varying load balancer functionality offerings, but none have passed the rigors of JITC certification, nor do they provide for on-premise and hybrid cloud architectures. They are therefore dependent on the principle load balancer manufacturers for most federal use cases.

A comparison of F5 and Kemp LoadMaster provides good examples of contrasting approaches by top federal ADC manufacturers.

F5 Networks entered the ADC market in 1997 with their custom hardware appliance, the BIG-IP Local Traffic Manager. F5 has added additional custom hardware models and functionality to their BIG-IP platform and is currently rated as the world-wide leader in ADC sales. F5 is reshaping its BIG-IP into a platform for other security services, with options for a full stateful inspection firewall, content filtering forward proxy, and remote access VPN concentrator. F5 includes the iRules programming language and allows end users to write additional code to extend the functionality of the BIG-IP platform. The upside of these feature enhancements has resulted in F5's ability to address a broader range of use cases. The downside is the creation of a highly complex and manpower intensive solution that includes the requirement for customer creation and maintenance of custom software (iRules). F5's custom hardware focus and extensive list of optional components results in high development and support costs, which is reflected in the high cost of F5 appliances. Many governmental agencies adopted F5 in part because they were the initial manufacturer to offer federally mandated encryption (FIPS 140-2). Today, operational complexity and total costs of ownership of F5 has become its most vulnerable exposure to competitive alternatives.

Kemp Technologies entered the ADC market in 2003 with the LoadMaster (application proxy and load balancer). Since its introduction, Kemp has added the Edge Security Pack (authentication proxy with Single Sign On), Geographical Server Load Balancing – GSLB (global load balancer), Web Application Firewall – WAF (application firewall) and enhanced content rules and matching services along with DDOS and Intrusion Prevention Services. Kemp has focused on the technologies needed to ensure an always-on application experience. Kemp's design philosophy is centered around ease of use and affordability and as a result, LoadMaster is considered the easiest to operate and most affordable enterprise class advanced load balancer in the industry. Kemp grew out of the small/medium business (SMB) market where economical cost and ease of use are competitive mandates and incorporated this philosophy into its enterprise product development. In response to government market requirements, Kemp included FIPS 140-2 encryption in its core LoadMaster Operating System (LMOS), along with other key features including Kerberos for federal identity smartcard management, and DNS security (DNSSEC) in its global load balancing functionality. Today Kemp market share expansion is in part at the expense of F5.

The competition between Kemp and F5 has emerged as a disruptive technology change away from complex application load balancing solutions to ownership strategies that consider other important factors which play a significant role in procurement criteria and selection.

LOAD BALANCING FOR FEDERAL AGENCIES

There are several factors that organizations need to consider when deciding upon and implementing technical solutions that also apply specifically to application load balancing sourcing decisions.

OPERATIONAL REQUIREMENTS

It is necessary and critical to understand operational requirements before purchasing any product or service and the same applies to load balancing technology. Well defined operational requirements in solicitations enable manufacturers to assess the requirements against their capabilities and provide accurate bid responses. Good clear requirements enable multiple manufacturers to compete for the business, which is in the best interest of the purchaser. When this approach is not followed, the result can be influence by an individual manufacturer that restricts competition at taxpayer expense.

Using the specification for one manufacturer and/or allowing manufacturers to input to requirements for solicitations can create unfair advantage and usually results in purchases of capabilities that are not utilized. Manufacturers may add optional features that only they provide, even when there is no operational need, to “spec out” other manufacturers. Validation of the technical requirements for projects based on the design and functional use is a best practice.

FAIR AND OPEN COMPETITION

Historically a high percentage of US federal agencies have standardized their application load balancing solutions on a single vendor which introduces both benefits and risks. Vendor exclusivity is often a circumstance that is inherited from previous procurement decisions. If the need arises to change vendors, the ability to accurately assess the risk of changing often becomes a hurdle to the migration decision. Organizations that use vendor unique features or vendor proprietary standards run the risk of becoming dependent on that one manufacturer, a situation known as “vendor lock”. The use of brand name justification (BNJ) in procurements often indicates vendor lock. While it can be difficult for an organization to break a proprietary technology dependency, with proactive planning the risks can be mitigated. The use of brand name or equivalent solicitations fosters competition for the incumbent manufacturer and surfaces potential valid alternatives. Standardizing on application load balancer technology rather than vendor specific solutions supports diversified sourcing strategies and reduces critical application experience risks. The US Federal Acquisition Regulation (FAR) encourages and in most cases requires full and open competition for affordable solutions that use open standards by applying “technically acceptable least expense” selection criteria.

EASE OF USE

Technology design and procurement decisions should consider the length of time the organization will utilize the solution, and the resource requirements the solution will impose. Assessing manpower and training requirements before the purchase can be difficult to do accurately but is essential in load balancing. Many organizations suffer the circumstance of purchasing what they perceive is the most advanced solutions, only to later realize the full impacts including costs of sustainment. Purchase decisions based on which product has the most features can result in buying the most complex and expensive solution available. While training may be included in the purchase, load balancing proficiency requirements can vary considerably between manufacturers. The more complex the solution, the higher the requirement is for experienced personnel to install and operate it. This can drive up Total Cost of Ownership (TCO) if additional professional services become necessary beyond on-hand staffing. Retention of personnel for complex solutions is also a factor that can dramatically impact on total costs. Many federal load balancing deployments are of a nature that the technical personnel have multiple functions to perform in stressful environments. These factors favor load balancing solutions that focus on ease of use as a primary characteristic.

CO-EXISTANCE

Incorporating multiple load balancer manufacturer solutions into an organizational architecture can be a valuable technique to aid in avoiding the pitfalls of vendor lock. Adding manufacturer diversity reduces the dependency on a single solution, which in turn reduces risk for application security and performance and mitigates concerns about replacing one manufacturer for another. Customers may have legacy load balancers that are fit-for-purpose which are not cost effective or practical to replace immediately. Per-application load balancing is a term used to describe the ability to deploy load balancers on an as needed basis as new application "workload" requirements emerge and/or change. A solution like Kemp's 360 Central provides a "single pane of glass" ADC management system which has the unique ability to provide ADC visibility and control across multiple platforms (on-premise and cloud) and multiple load balancing vendors. Using solutions like Kemp 360 empowers manufacturer diversity which is especially important for agencies that find themselves in a vendor lock circumstance.

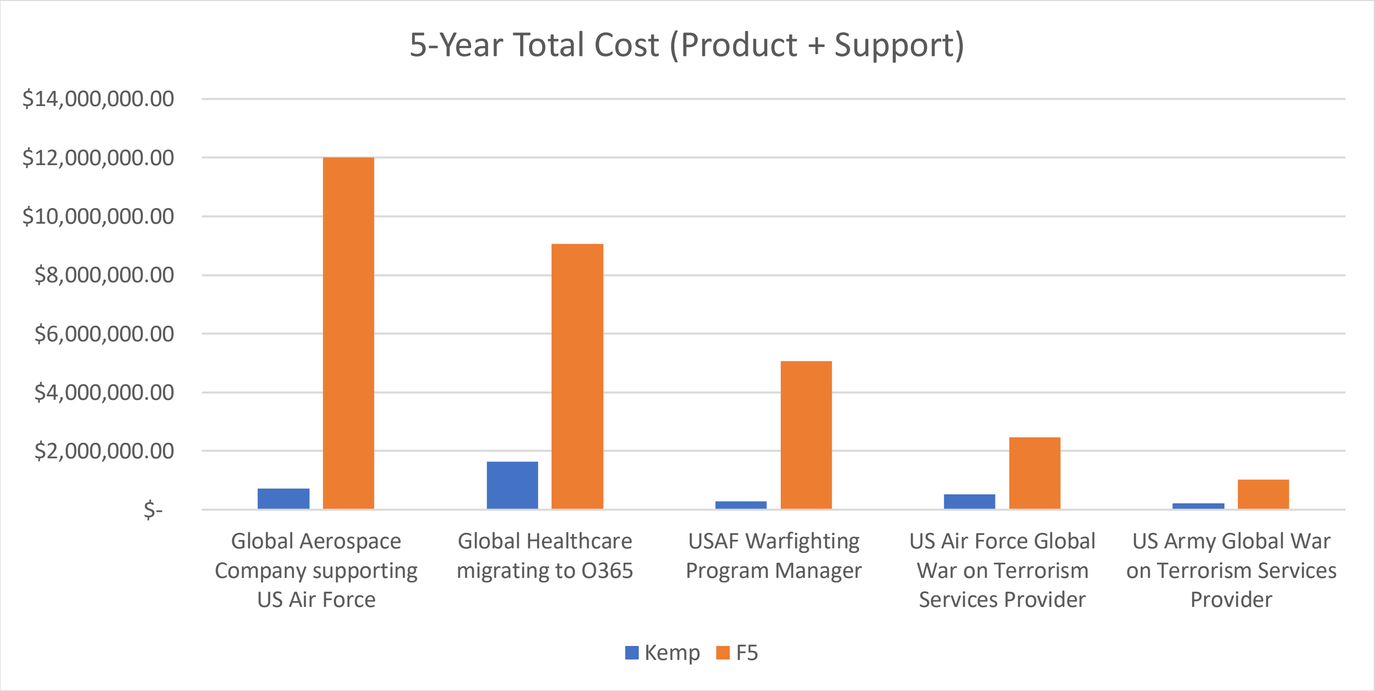
VENDOR MIGRATION

If the need arises to change out load balancer manufacturers, there are best practices that can help reduce the risks. Proactively engaging in product purchasing decisions that diversify vendor dependencies helps. The investment in planning is key in these circumstances. Replicating the current operating environment in an evaluation/assessment lab that includes the legacy load balancer provides the ability to introduce the new target load balancer and assess the mechanics of the migration. Inevitably the goal is to activate the new target load balancer and retire the legacy. The evaluation lab not only allows the ability to isolate the vendor specific features/functions to determine whether they can be satisfied by a different manufacturer with other more desired characteristics (such as ease of use and lower total costs of ownership), but it also provides the ability to confirm what the true organization load balancing requirements are and insure vendor capabilities are not driving procurement decisions.

TOTAL COST OF OWNERSHIP (TCO)

Arguably one of the most important purchase decision planning actions is to conduct a Total Cost of Ownership (TCO) analysis of the primary load balancer manufacturers identified during market research/RFI (Request for Information) and at the time of Request for Quotes (RFQ) before award. This analysis is more effective when the period of ownership is calculated for at least 3 years and better for a 5-year period.

Here is an example of a comparison of five recent use cases of large Federal programs that required highly available load balancing solutions utilizing server load balancing (SLB) and global server load balancing (GSLB). All five use cases needed globally distributed load balancers with centralized management to support their application infrastructure. The customers required that products offered be tested and listed on the DoD Information Network Approved Products List (DoDIN APL) and contain independently validated FIPS 140-2 certified cryptography. Using current MSRP pricing, TCO calculations show that on average the load balancing costs for these five programs was 89% less when using the selected vendor Kemp over a 5-year period.



To better demonstrate the cost advantages, the below table breaks out the comparison for the Global Health Care Provider. The requirement was to host 750,000 Microsoft Exchange users in 4 data centers with any one data center capable of hosting all 750,000 users in a worst-case scenario. Microsoft calculated that to meet this requirement, the load balancers needed to support up to 3 million concurrent layer 7 (application level) connections. The design was to provide N+1 high availability. Kemp provided the LM-8020M, a single device capable of 3 million layer 7 concurrent connections. At the time of this program, the top end F5 appliance supported around 800,000 L7 concurrent connections so to meet the requirement of N+1, it would have taken 5 F5 appliances per data center. Kemp bid 2 appliances per data center and was selected for this effort.

Model	L7 Concurrent Connections' (Required)	Quantity of Devices Required	Product Cost per Device	Support Cost per Device	Cost per Device	Total Cost (Year 1)	Total Cost (5 Years)
					Cost	Total	Total
LM-8020M	12,000,000	8	$ 60,000.00	$ 28,800.00	$ 88,800.00	$ 710,400.00	$ 1,632,000.00
LTM-10350V-F	12,000,000	20	$ 244,995.00	$ 41,649.00	$ 286,644.00	$ 5,732,880.00	$ 9,064,800.00
Savings						**$ 5,022,480.00**	**$ 7,432,800.00**
4 Data Centers, each capable of hosting 750,000 MS Exchange users with an average of 4 connections per user.							
Design to provide high availability (no single points of failure)							

FEATURE COMPARISON

There is a common set of core features that define a product as a load balancer/application delivery controller and will be found in all major manufacturer models in varying degrees. A subset of those features determines the differences in capacity which are relatively straightforward to compare. Load Balancer manufacturer features vary in that some are integrated into the product, while others separate features and sell them as add-ons. Example:

FEATURE COMPARISON (Common Load Balancer features)	Kemp (Module)	F5 (Module)
Application Load Balancer	LoadMaster	LTM
Global Load Balancer	GSLB	GTM
Application Proxy	LoadMaster	APM
Authentication Proxy (SSO, Kerberos, CAC)	ESP	ASM
Certified Encryption (FIPS 140-2)	LoadMaster	Full Box FIPS
HTTP Caching, Compression, Multiplexing	LoadMaster	AAM
HTTP2 Support	LoadMaster	LTM
API Support (REST)	LoadMaster	LTM
Content Rules	LoadMaster	LTM
Web Application Firewall (WAF)	AFP	AFM

LoadMaster – Kemp - L4/L7 load balancer
LTM – F5 Local Traffic Manager- L4/L7 load balancer
GSLB – Kemp Global Server Load Balancer – global load balancer
GTM – F5 Global Traffic Manager – global Load Balancer
ESP – Kemp Edge Security Pack – authentication proxy and SSO
ASM – F5 Application Security Manager – authentication proxy and SSO
AFP – Kemp Application Firewall Pack – web application firewall
AFM – F5 Application Firewall Manager – web application firewall

Federal specific features common to the ADC vendors include Kerberos integration for federal smartcard authentication management, DNS Security (DNSSEC), and FIPS 140-2 encryption. Federal Information Processing Standards (FIPS) is a feature that has had significant impacts on the federal load balancing market which is mandated under US Public Law (100-235 and 104-106). FIPS 140-2 is the mandatory standard associated with encryption of unclassified information required in load balancers used in US Federal agencies. There are two basic approaches to achieving compliance with FIPS 140-2. FIPS 140-2

Level 1 can be achieved by incorporating a software-based certified encryption module. FIPS 140-2 Level 2 and higher levels can be achieved by incorporating an embedded hardware based certified encryption module. Initially load balancers with FIPS 140-2 compliance were only available in select hardware models with FIPS 140-2 level 2. These models have historically been the most expensive higher capacity load balancer models sold in US Federal. Many agencies invested into these load balancers to meet the FIPS 140-2 mandate, even though the capacity exceeded their requirements resulting in technical and financial sustainment challenges.

Competitive equivalents and alternatives are now available that offer FIPS 140-2 level 1 compliance in virtual, hardware, and cloud load balancers. Federal users have gradually realized that the physical security requirement for FIPS 140-2 level 2 is not required for most federal use cases, and the additional costs do not justify the expense especially given the availability of the FIPS 140-2 level 1 alternative.

SUMMARY

The federal load balancer market has changed considerably in recent years, driven by increasing competition which has put pressure on pricing and improved usability while expanding support for virtualization and cloud constructs. As federal organizations go through load balancer technology refresh, the opportunity exists to reduce costs, complexity, and manpower requirements while benefiting from increasingly simple yet sophisticated features and functions. Personnel with load balancer experience are in high demand putting pressure on retention, and their skills are better positioned to administer load balancing technology from multiple vendors. These advances increasingly reduce the hurdles to vendor transition which fosters competition and opportunity to the benefit of federal load balancer ownership.

ABOUT KEMP

Kemp Technologies application delivery controllers deliver easy to operate, cost effective solutions, to ensure critical applications will be delivered securely, reliably and without interruption.

Kemp builds to US Federal standards. FIPS 140-2 certified encryption is included in all LoadMaster products and architectures and certified by the US Joint Interoperability Test Center (JITC).

Included in all Kemp LoadMaster models:

- Multifactor authentication including Common Access Card (CAC) and Personal Identity Verification (PIV) certificate-based access
- Advanced L4/L7 application load balancing
- Advanced geographic server load balancing
- Application proxy services to ensuring no one can directly connect to your servers
- Authentication proxy with integrated single sign on services is included to protect your authentication servers
- Web Application Firewall to mitigate application level attacks

Kemp LoadMaster ADCs are listed on the US DoD DoDIN Approved Products List under the Cybersecurity Tools (CST) section.

Learn more about Kemp Technologies at: http://KempTechnologies.com

Kemp Federal Compliance

- US Government validated cryptography (FIPS 140-2)
- US DoD validated security (DoDIN Approved Product List)
- DNS Security (DNSSEC) client and server
- Authenticated Network Time Service (NTPv3)
- Intelligence Community Directive Number 503
- VPAT/Section 508 compliant
- Trade Agreement Act (TAA) compliant
- Buy American Act (BAA) compliant

CONTACT US

Michael Bomba, Solutions Architect
+1 520-457-8507
mbomba@kemptechnologies.com

Jim Justice, Federal Business Manager
+1 202-359-2669
jjustice@kemptechnologies.com

MORE KEMP RESOURCES

- Free Trial Download - Virtual Load Balancer
- KEMP Solutions for US Government

http://KempTechnologies.com