KEMP | APPLICATION DELIVERY

White Paper

LoadMaster Powering the Internet of Things (IoT)

Introduction

The promises of greater efficiency, agility, and cost-savings are driving an increasing number of enterprises toward cloud computing. Today's technology now allows these enterprises to extend the benefits of cloud computing to their emerging Internet of Things (IoT) workloads.

Research shows that the IoT is disrupting markets and IT organizations worldwide. This revolution, in turn, is changing the economics and agility in many markets. With this change comes growth in IoT device data, analysis, and integration with back-end systems, along with the subsequent IoT feedback and control that will improve business outcomes and quality of life in general.

Leading technology research company Gartner predicts:

- By 2020, there will be 25 billion connected IoT devices, with a compound annual growth rate of 35% (see "Forecast: Internet of Things, Endpoints and Associated Services, Worldwide, 2014").
- By 2018, the number of new connections for IoT devices will exceed all other new connections for interoperability and integration combined (see "Predicts 2015: Digital Business and Internet of Things Add Formidable Integration Challenges").

Despite these benefits, the business and technical challenges of managing and capitalizing on the proliferation of IoT adoption remain daunting to many IT organizations. Moreover, the challenges in designing and deploying large-scale IoT solutions are enormous due to the rigidity, poor elasticity, and limited dependability of traditional products.

Consider that:

- Traditional IoT solutions are rigid and inflexible because they are tailored specifically to solve a problem and are not designed for flexible customization, utility-oriented delivery, and granular consumption.
- IoT devices are not built to scale dynamically to respond to varying loads.
- The general measure of availability, reliability, and maintainability of traditional IoT solutions is poor.

- The dynamic heterogeneity and geographical distribution of large-scale IoT solutions disrupt traditional security and management tools, rendering them ineffective.

As the recognized leader in the load balancing arena, KEMP Technologies recognizes that traditional load balancers are not suited for environments that include IoT deployments. KEMP has investigated these challenges thoroughly. From this research, KEMP created a suite of virtual products and application delivery tools uniquely suited for today's IoT workloads.

KEMP Solutions for the IoT

KEMP Virtual LoadMasters (VLMs) abstract application delivery services from the physical networks and deliver virtual services that can be attached to IoT workloads. KEMP VLMs can be provisioned dynamically to deliver proactive performance management.

To enhance reliability and availability, KEMP VLMs include L4-7 load balancing and GEO load balancing. These features ensure that IoT sessions are always processed by the most highly available server. GEO load balancing also ensures that IoT sessions are always sent to the application server closest to the IoT device.

Complementing KEMP VLMs is the KEMP 360™ Central application delivery framework. This framework offers a single point for control, analysis, and diagnosis of key application metrics that enable customers to make smarter decisions about managing capacity adaptively. Advanced monitoring and analytics engines allow changes in device behavior to be visualized and remedial actions to be taken before a catastrophic failure occurs.

To improve security, KEMP Web Application Firewall (WAF) secures IoT applications dynamically. By enabling SSL or IPSec encryption, IoT data is protected during transfer from the enterprise edge to the cloud. And with KEMP Edge Security Pack (ESP), IoT devices can be authenticated and authorized.

IoT Architecture

To appreciate the benefits of the KEMP solutions, it is important to understand the IoT architecture. Most IoT solutions include endpoints, platforms, and business solutions. IoT endpoints are a combination of real-world sensors and some form of hardware and/or software that detects or

causes a change in the state (or "event") of those sensors.

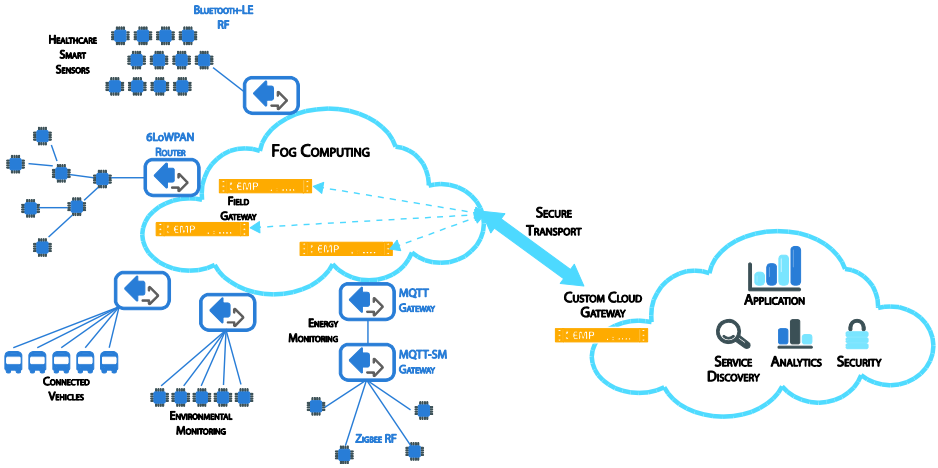

Figure 1 IoT Architecture

IoT platforms leverage gateways to monitor and manage IoT endpoints and their software, and to aggregate and analyze IoT endpoint data. An IoT gateway can be:

- A physical router, application delivery controller, or server with an IoT agent, or
- A virtual solution that resides in the cloud as a Platform as a Service (PaaS).

Whether physical or virtual, the goal of the IoT gateway is the same: to provide aggregated edge device management and connectivity. The IoT platform may have agents located on the IoT endpoints that connect either directly to the IoT back end or indirectly through IoT gateways.

IoT business applications use the data collected from sensors and endpoints to improve operational intelligence, produce better business outcomes, and improve the quality of life for businesses and consumers alike.

Powerful Solutions for the Challenges of IoT

Reliability and Availability of IoT Solutions

The Challenge

Most IoT solutions involve thousands of endpoints that generate and process data across multiple networks. The time and effort required to provision new services and transfer data reliably to IoT applications in the cloud is a challenge for most IT organizations. In particular, organizations running traditional IoT systems are often locked into a rigid framework and cannot respond fast enough to changing demands of IoT solutions.

The Solution

KEMP VLMs abstract application delivery services like load balancing and web application firewalls, and delivers them through virtual services. These services can be deployed and attached to IoT applications automatically on demand.

KEMP VLMs boast high-performance L4/7 server load balancing to ensure that each user receives the best application experience possible. By distributing incoming IoT sessions to the most highly available application server KEMP VLMs accelerate processing time. And by integrating with SDN controllers, KEMP VLMs configure network bandwidth dynamically and direct network traffic to least loaded network paths. This translates into more efficient load balancing, accelerated application delivery, and improved Quality of Experience (QoE) for end users.

In addition, KEMP VLMs support multiple hypervisors, including:

- VMware vSphere
- OpenStack load balancing as a Service (LBaaS) plugin
- Microsoft Hyper V
- RedHat KVM

This wide-ranging support slashes the time required to deliver IoT solutions.

KEMP VLMs operate as an active/hot-standby configuration, with stateful failover that delivers superior high-availability for mission-critical IoT solutions and removes single points of failure. With server hardware and application health checking, user requests go to the most "available" servers and applications.

To ensure optimum user experiences, KEMP Multi-Site GEO LoadMasters (GSLB) are designed from the ground up to optimize and increase availability and continuity for IoT workloads across multiple datacenters and hybrid clouds. KEMP GEO LoadMasters ensure that when a primary site goes down, traffic is diverted to the disaster recovery site automatically. In this way, clients connect to their fastest performing and geographically closest datacenter seamlessly.

Perimeter Protection for Preventing Breaches on IoT Solutions

The Challenge

Enterprise IT professionals and analysts agree that securing the network only at the perimeter is sorely inadequate for IoT solutions. Modern attacks can exploit a perimeter-centric defense in no time. After the malware enters the data center, it can move easily from sensor to sensor within the data center by compromising just one authorized sensor or using other nefarious methods. Recent, attacks for example, used an army of hijacked security cameras and video recorders to launch several massive Internet attacks on a web hosting provider in France.

A stricter, micro-granular security model effectively points to the need for unique firewalling of each individual IoT workload. Until now, this approach has been cost-prohibitive and operationally infeasible.

The Solution

KEMP VLMs boast a unique "defense-in-depth" architecture for securing IoT applications and data. This architecture allows IT teams to bring security closer to the IoT workloads and protect IoT data.

To protect IoT data transfer from the data center edge to cloud gateways, KEMP VLMs implement IPsec VPN tunnels. IPsec is an industry standard that is offered as a secure connectivity option on cloud services from Microsoft, Amazon, and Google.

KEMP VLMs also protect against Distributed Denial of Service (DDoS) attacks that hijack IoT devices and flood the network with unnecessary traffic until systems are rendered unavailable. By validating network connections and checking for protocol correctness (header, URL, HTTP version, method) while proxying connections, KEMP VLMs protect against SYN flood attacks, TCP reset attacks, ICMP attacks, UDP storm attacks, and many other application layer attacks.

KEMP Application Firewall Pack

KEMP's WAF combines Layer 7 Web Application Firewall protection with other application-delivery services that include intelligent load balancing, intrusion detection, intrusion prevention, and edge security and authentication. By integrating one of the world's most deployed Open Source Web Application Firewall engines, ModSecurity, augmented by threat intelligence and research from information security provider Trustwave, KEMP WAF provides ongoing protection against known and evolving vulnerabilities in IoT solutions.

KEMP Edge Security Pack

With KEMP Edge Security Pack, you can authenticate devices using certificates before accessing the IoT application servers. Active directory group membership can restrict access to IoT published applications. Installing certificates on devices can authenticate them with validation using the Online Certificate Status Protocol (OCSP).

For enhanced protection of private key material required to support a TLS (SSL) handshake, KEMP LoadMasters support network-attached Hardware Security Modules (HSMs) that executes cryptographic functions, such as encryption (signing) and decryption.

Management and Orchestration

The Challenge

Most IoT solutions follow distributed models that include many devices. Provisioning and continuously monitoring these devices presents a big challenge.

These configurations require analytics to make the IoT solutions intelligent and responsive. By processing event data from sensors in real time, and combining the data with historical data, insights can be obtained that deliver predictive and adaptive solutions that reduce operational cost and accelerate productivity. For example, a worldwide supplier of manufacturing

equipment can differentiate its solution by installing telematics in each piece of equipment to monitor performance and predict problems in advance.

The Solution

KEMP offers a number of solutions for simplifying IoT infrastructures.

The KEMP 360 framework includes KEMP 360 Central™, a single pane of glass for managing application delivery infrastructures.

KEMP 360 Vision™ service delivers proactive alerting and diagnosis to minimize or even eliminate the impact of issues in the IoT application delivery infrastructure. It collects key application availability, reachability, and performance metrics continuously. If a defined limit being breached initiates a notification and remediation process.

KEMP 360 Vision™ also provides an easily digestible snapshot of incidents, issues, events, and workload availability, along with consolidated reporting across IoT application workloads. The service can consolidate performance and availability metrics from multiple IoT solutions using KEMP VLMs – including public cloud, on premise, and hosted environments–into a single point of notification and escalation.

Conclusion

Industry analysts agree that the proliferation of connected devices is disrupting IT organizations. The dramatic increase in the number of connected things is forcing IT organization to evolve and consider new architectures to address security, privacy, cost, ease of access, agility, and performance.

KEMP Technologies offers powerful, real-world solutions to address these issues (see **Error! Reference source not found.**). KEMP VLMs accelerate and optimize data transfer, while protecting applications and data with a Defense-in-Depth architecture. KEMP 360 and Vision make managing the IoT infrastructure management a snap.

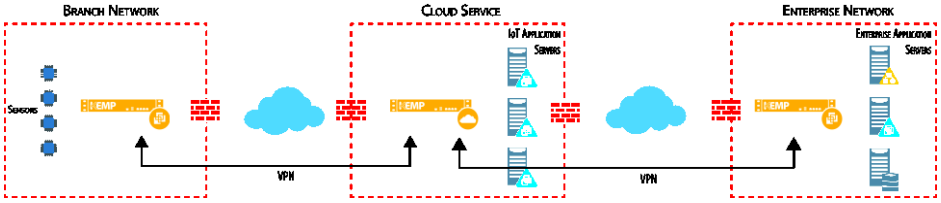

Figure 2 Defense in Depth Architecture