

# Better Provisioning of the Web Infrastructure through Device Consolidation

Today, small and medium-sized businesses (SMBs) are often challenged when provisioning multiple disparate, but necessary components when upgrading existing web infrastructure. These problems relate to complexity, cost, and disparate performance capabilities, but can be solved through device consolidation and management. While this can affect any IT organization, SMBs are especially sensitive to these issues due to cost and resource considerations.

### Disparate Capabilities

The rule of lowest common denominator applies to device and capability purchases. If you purchase a firewall that is capable of handling 50 Mbps of traffic and a load balancer capable of handling 150 Mbps, then you paid 100 Mbps too much for your load balancer. Add in several other types of devices, such as an application firewall, caching device, and anything else you might need, and whatever can handle the least amount of traffic makes what you paid for the other devices too much.

Ideally, devices should match each other fairly closely in terms of capacity. But that rarely happens, even when the devices are from the same vendor. There are just too many variables (types of traffic, how the device is used, etc.) to accurately match device capability. In a less than perfect world, companies need to find solutions that balance device functionality, price and interoperability.

### Complexity

Larger enterprises may enjoy the staffing and technical expertise of an expansive team of talented engineers, while SMBs typically make do with much more limited staffing. Simplicity is always an advantage to any deployment, but this is critical for the SMB with limited manpower resources to expend.

Complexity comes in the form of interconnecting devices in a web traffic flow. Most web infrastructure devices need to be within the flow of traffic. Chaining together a load balancer, SSL accelerator, caching device, application firewall, and traditional

firewall together on a redundant Layer 2 switching infrastructure can create an absolute nightmare in redundant cross-connections, with more cabling connections between these devices than there are server connections.

Not only do the devices need to be chained in such a way that they're in the flow of traffic, but it must be done in such a way that if any of the elements were to fail, the traffic flows would be diverted to the partner unit, without disrupting upstream or downstream flows from the failover layer. While this can be done in a number of ways, such as dual-homing interfaces, NIC teaming, NAT, floating IP address schemes, and so forth, it can be far from straight forward and difficult to troubleshoot.

### Pricing It All Out

When adding up the cost of several types of devices, SMBs often find installing multiple devices is a budget-buster. Because of this budget crunch, an SMB might be forced to choose between a device that's inexpensive, yet very limited in functionality, or functionally highly effective, yet expensive. For example, an SMB can purchase a simple Layer 4 firewall, sometimes for a few hundred dollars, at the local consumer electronics store. It will provide a stateful packet filter, perhaps some rudimentary NATing, and usually not much else. At the other end of the spectrum, an application firewall will prevent against a greater number of attacks, but with a higher price tag.

While a Layer 4 firewall will prevent attacks against services that aren't meant to be exposed to the public (for instance, preventing access to the Common Internet File System (CIFS) services of a Windows server), it will provide no protection for attacks that reside inside requests to the web application, such as SQL injection.

An application firewall, on the other hand, will help prevent against attacks that are based on HTTP and the underlying web application. However, these devices are expensive, and only just beginning to appear on the SMB market. Like most technology,

**By combining the functionality of several typically stand-alone devices into a single device, an SMB's IT organization can solve the problems of complexity, over-provisioning, and cost all at the same time.**

the larger enterprises enjoy the benefits first, with the technology trickling down to the SMBs a few years later.

### **Device Consolidation: Boon to the SMB**

One solution to the problem of over-provisioning and complexity is device consolidation. By combining the functionality of several typically stand-alone devices into a single device, an SMB's IT organization can solve the problems of complexity, over-provisioning, and cost all at the same time. Device consolidation is nothing new, and has been used in many areas of IT for some time, but for the SMB and web infrastructure it has been especially beneficial.

Take the example of the marriage of SSL accelerators and load balancers. At one point in the late 90s, load balancers and SSL accelerators existed as separate devices, yet they were increasingly being deployed in tandem. They both provided necessary services to a web infrastructure, with the load balancer providing scaling and high-availability by distributing traffic among servers, and the SSL accelerator providing the offloading of SSL operations from the servers, giving a web application both security and scalability.

It wasn't long before load balancing vendors started to integrate the features of SSL acceleration into their devices. This greatly simplified the deployment of both SSL and load balancing, as there was only one redundant system to configure, and managing the traffic flows was much easier.

Cost was greatly reduced with this combination as well, as adding SSL acceleration was often a simple matter of adding a PCI expansion card and purchasing the requisite feature license. The cost associated with this was usually far less than a stand-alone appliance. Today, you would be hard-pressed to find an installation that used a stand-alone SSL accelerator.

This consolidation continues even today. Caching devices, which once enjoyed a rapid popularity in the datacenter, quickly disappeared from the scene. While they were useful, the benefit typically didn't make up for the cost and complexity associated with their deployment. With the advent of horizontal scaling, adding inexpensive servers is often a more cost-effective way to add capacity. For example, an SMB wants to add capacity by deploying a \$20,000 caching appliance. However, adding two more \$2,500 servers expands capacity by the same amount, giving the same benefit for one-quarter the cost, and it's much simpler since no additional skill sets are needed to deploy two more of the same type of servers.

Today, the industry is seeing a renewed interest in caching, but not as a stand-alone device. Instead, caching is being added as functionality to ADCs (Application Delivery Controllers). After all, caching can help reduce the number of servers needed, as well as increase a site's responsiveness. By adding caching into an existing device, the cost of caching is greatly reduced.

This caching functionality, along with load balancing, SSL, application security, and other tasks are being combined into a single device called an Application Delivery Controller (ADC). By having one device, many of the equipment issues faced by the SMB are often solved. Complexity-wise, it's much easier to manage traffic flows and redundancy with a single pair of devices, than several pairs of disparate appliances.

Provisioning is much simpler too, since there is only one device to take into account. With one device's performance to manage, there's less concern over paying for capabilities that are going to be throttled by the lower capacity of another device in the traffic flow.

Vendors can offer additional features typically included for free, or available as a licensed option for what is almost always far less expensive than a separate device doing the same function. The vendors can offer these features at lower cost because they save on hardware costs. For example, SSL acceleration is usually just the cost of an additional SSL card, instead of paying for a whole host system. Moreover, vendors don't need to charge the money that would be necessary to support an entire product line.

### Security Requirements of a Web Gateway Device

While ADCs have long provided security by offloading the CPU-intensive SSL operations from servers, they are now being equipped with application level security, beyond that of traditional firewall. In addition to Layer 4 protection they can also provide Layer 7 application-level protection for HTTP. Since they are an SSL termination point, ADCs can inspect encrypted HTTP sessions.


The security requirements for a web infrastructure gateway device are far different from an edge or core security device. With core and (non-web) edge devices, they need to be aware of many protocols, whereas a web gateway needs to be aware of the application protocols that the web infrastructure services, which is generally HTTP/HTTPS.

A web gateway device also does not need to have complicated Layer 4 firewalling rules in place, nor does it require the ability to perform complex NAT configurations. Instead, a web gateway needs to be fluent in HTTP/HTTPS, and be able to provide security for both Layer 4 and Layer 7.

### The All-In-One Solution

By integrating SSL, load balancing, application security, caching, and other functionality into one device, many issues facing the SMB are solved in one neat package. An SMB can benefit from an all-in-one ADC device by saving both time and money, and while ADCs have been available to the enterprise market for some time, companies like KEMP Technologies are leading the adoption of these features and benefits to the SMB with ever increasing feature sets. They save time by dealing with a much simpler network deployment, and the cost savings of device consolidation allow the SMB to provide more services to their customers with less attention to network details.

## SMBs Need Complete Solutions

<b>High Availability</b>	<b>Layer 7 Persistence</b>	<b>Layer 4 Persistence</b>	<b>Resource Load Balancing</b>
<b>Layer 4 Load Balancing</b>	 <b>Application Delivery Controller</b>		<b>HTTP Compression</b>
<b>Layer 7 Content Switching</b>			<b>HTTP Caching</b>
<b>SSL Offload</b>	<b>SSL Acceleration</b>	<b>Persistence with SSL</b>	<b>Intrusion Prevention</b>

### Complete ADC Solution

KEMP Technologies, Inc.  
 12 Old Dock Road  
 Yaphank, NY 11980  
 Tel: (631) 345-5292  
[Info@KEMPtechnologies.com](mailto:Info@KEMPtechnologies.com)  
[KEMPtechnologies.com](http://KEMPtechnologies.com)