White Paper

Security *and* Speed

Security is an intrusive mechanism that is often seen to interfere with normal business operations. Nonetheless, security is essential to the normal operation of the business, and the right security mechanisms and approaches can minimize performance degradation.

by Don MacVittie
Technical Marketing Manager

Contents

Introduction

Information security is not an option in the modern enterprise. Hiding behind the supposed anonymity of the Internet, attackers come from all directions, including, at most organizations, from within. Yet in many respects, security can be seen as a burden to an enterprise. While the "intrusiveness" of security procedures will always be debated and the performance impacts of security measures will always be questioned, there are ways to minimize issues, both maintaining performance and raising the overall security posture of the organization. It is not possible to completely eliminate the performance degradation that active security solutions such as web application firewalls (WAFs) introduce. Rather, the goal is to minimize the performance degradation and then look elsewhere in the network for performance improvements to counter any remaining effects.

The problem of security implications for performance is growing as the number of devices or procedures deployed between the user and applications continues to grow. Firewalls, WAFs, encryption, SSL VPN, and intrusion prevention systems all reduce the perceived performance of web applications, and all exist solely to secure those applications. As virtualization of web application servers has progressed, so have concerns about encryption, as it is not only one application utilizing an encryption procedure, but one (or more) applications per virtual machine, all utilizing the same hardware.

All of this security comes with overhead—overhead that must be accounted for. Of course, rolling back security so that applications perform better is not an option, but when performance starts to degrade, competitive organizations require a solution that cuts the security overhead dramatically while optimizing application delivery to mitigate any remaining reductions in performance.

The Enterprise Network Today

Today, most organizations have a large number of devices sitting between users and the applications they need to access. It doesn't matter if those users are employees or customers; the layers of security in place slow access with the latency they introduce and the bandwidth throttling that some security provisions invoke.

Typical security measures may include:

- **Encryption on the server**—which protects data, but entails a large CPU overhead that does nothing but grow, since multiple virtual machines often reside on a single physical server and encryption keys keep getting larger.
- **Traditional firewalls**—which protect the network from known network layer intrusions and denial-of-service (DoS) attacks, but create latency as rules are tested and scans are performed on the connection data.
- **Web application firewalls**—which protect against common application-layer attacks, but also introduce latency as rules are tested and scans performed on the application layer data.
- **VPN connections**—which allow employees or trusted partners and customers direct access to the network, but perform notoriously slowly compared to local area network (LAN) connections.
- **Intrusion prevention systems (IPSs)**—which detect and disconnect attacks that do make it to the network, generally without introducing latency as they run transparently on the network, but which increase network traffic and can cause congestion when a large number of resets are sent.

All of these systems together make for a solid security posture, but they do not make for astounding performance. The total effect of these systems on performance depends upon vendors, architectural implementation details, and the environment, but it is not negligible.

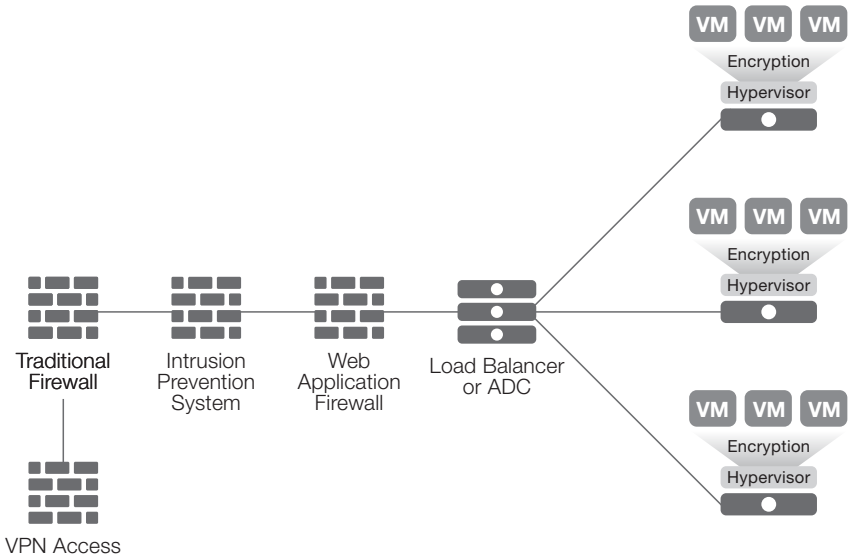

Figure 1: Existing enterprise security architectures are typically complex and slow.

Given users' demands for high performance web applications—a challenge aggravated by the trend toward access via slower networks such as cell phone systems—the total performance reduction caused by these security devices is less and less acceptable. If an organization doesn't have a problem with performance today, it will soon—particularly if access to its website is growing, since more traffic compounds latency problems.

In some enterprises, turning off or never implementing certain security devices is an option for a subset of applications and/or network segments. That helps those who do not need the services in question, but it does not improve performance for those who do need them.

The Case of DDoS

In 2011 and 2012, a wide range of companies faced an increase in sophisticated distributed denial-of-service (DDoS) attacks. In many cases, traditional firewalls were unable to cope with the volume and variety of the attacks and thus failed—making the DDoS successful by rejecting valid customer connections because the firewall was too busy dealing with attacker connections.

Not all of these attacks were successful, though. Some organizations had a more sophisticated device to fall back upon, one that could handle volume, detect malicious connections, and route them to neverland.

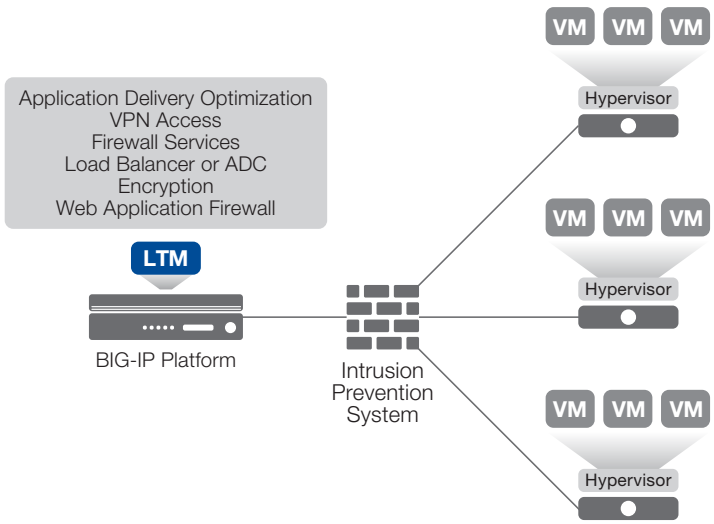

Figure 2: A secure, fast, and available network can be managed by the F5 BIG-IP system.

These organizations made good use of an F5® BIG-IP® Application Delivery Controller (ADC), such as BIG-IP® Local Traffic Manager™ (LTM), as part of their networks. If connections coming in to the load balancing/firewall services device are deemed to be part of an incoming attack (a DDoS attack, for example), they can be routed to a page outside of the production network instead of past the IPS to production servers. The strength of this methodology is in the design of the F5® TMOS® architecture and F5 hardware. With high-performance routing and manipulation engines facilitated by custom hardware, the BIG-IP device is able to handle far more traffic than traditional firewalls in a DoS scenario. At the same time, valid connections are routed through the other features of the BIG-IP ADC to connect valid users with the applications they need. Accelerating those valid connections means that the overall perceived performance at valid client machines is high, while attackers are sent to a custom page denying them access to critical infrastructure.

Speeding Applications, Securing the Perimeter

While DDoS protection is important, it is just the tip of the iceberg. DDoS is an occasional, if horrifying, attack, but for those average days without DDoS activity, the performance of web applications is enhanced by the F5 architecture with a variety of improvements to data communications and processing.

- **SSL offload** improves the overall performance of web applications by freeing server CPU to handle connection requests.
- **Web application firewall** services improve the security posture for all web applications, whether purchased or developed internally.
- **TCP optimizations** make the overhead of TCP connections—particularly on a lossy network—considerably less.
- **Compression** reduces the number of bytes being sent over the wire for clients that support it, improving perceived performance.
- **SPDY** improves performance in the same way that Unix TAR files save disk space: by eliminating the overhead of multiple connections just as TAR eliminates the wasted space of multiple files.
- **Deduplication** further reduces the amount of data sent over the wire when two data centers need to pass data between them, as is the case in replication and other forms of backup. This ensures space on Internet connections for customers to connect to applications.

Fast Access Anywhere

"BIG-IP or FirePass solutions for remote access to applications and networks gives us secure and fast access to mission critical applications from anywhere in the world. It enables users to become more productive, increase communication, publish and share information faster; all while lowering costs."

—Project Manager, Small Business Telecommunications Services Company

Source: TechValidate
TVID: 7F2-385-BD9

- **Image optimization** reduces the overhead of images being transferred by reducing file size through elimination of unnecessary metadata and through compression, if the image is not already compressed.

Organizations today are driven to improve utilization of network resources by as much as virtualization improved the utilization of server resources. By minimizing the amount of data being transferred and enhancing the responsiveness of the servers accepting connections, IT departments help users feel as if applications are better performing, while saving on the cost of additional servers and upgraded Internet connections to handle more volume.

Conclusion

Load balancers allowed organizations to service many more incoming connections by distributing those connections across many servers. The evolution of the ADC enabled additional functionality such as request rewriting and content-based routing. Today that continuing evolution allows for a much more sweeping change to application architectures. Internet attackers have found a fundamental weakness in traditional firewalls that ADCs are more than capable of dealing with, while the use of add-ons such as web application firewalls increases security without introducing even more devices between applications and clients. F5 Application Delivery Optimization improves the performance of web applications by reducing the number of round trips and the amount of data transferred over a connection. Simultaneously, SSL offloading improves the actual performance of application servers by allowing customized hardware to handle incoming connections.

And all of this can be achieved from a single point of control within the network. Adding on SSL VPN provides trusted entities, such as employees and business partners, secure access to the internal network with an organization's preferred credential provider as the source for authentication. Tracking problems with the infrastructure in this environment is much more readily accomplished because the connection stream is only touched once—at the strategic point of control. Add advanced reporting that can graph CPU usage, network throughput, connections rejected, and a host of other variables, and you have a complete, optimized, Application Delivery Network (ADN) capable of handling both the worst attacks and the day-to-day interactions seamlessly.

F5 secures network traffic and enables rapid deployment

"With the F5 LTM's we deployed, we were able to further secure our traffic – verify it was coming from allowable sources; we were able to quickly deploy multiple lab environments without a lot of complexities, and with iControl we are able to register dynamic virtual machines that come up on our network and register themselves with the F5 as valid application servers ready to take customer traffic without any manual reconfiguration."

—Ben Weldon,
Senior IT Architect,
Tangent Information Systems

Source: TechValidate
TVID: B0E-6DF-820

F5 is the provider of choice for most organizations' ADN plans and architectures, with BIG-IP LTM managing the core of the network. Additional performance gains to offset increased security can be achieved with other modules, including BIG-IP® Application Security Manager™ (ASM) for web application firewalling, BIG-IP® Application Acceleration Manager™ (AAM) for handling symmetric communications for backup and recovery, or for web application performance enhancements. In addition, the F5 application delivery firewall solution fulfills the role of traditional firewalls. An ADN built from these building blocks will carry a corporate network into the future, with additional functionality to improve cloud-hosted or cloud bursting and multiple data center functionality.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com