F5 White Paper

Maximizing the Strategic Point of Control in the Application Delivery Network

Improve performance, implement security procedures, and institute server redundancy that is invisible to the user by leveraging the strategic point of control that exists between the servers in the data center and the Internet.

by Don MacVittie
Technical Marketing Manager

Contents

Introduction

Three major factors in the perception of a corporate website and the performance of applications can be summarized as "secure, fast, and available." If applications are secure, the systems are highly available, and users experience fast access—which can never be perceived as too speedy—then those users will perceive web applications as acceptable and feel comfortable with the level of security protection implemented for those applications.

Given the wide variety of services performed by most Internet connections today, administrators must watch throughput and take steps to guarantee bandwidth for the most critical applications, while ensuring that those with lower business value do not take over the available connection space. Administrators and IT managers need to:

- Drive context-based security into the network.
- Secure and optimize point-to-point connections.
- Ensure that systems are highly available at all times.

Connecting data centers through a WAN connection is the best way to keep them up to date and failover-ready, but unless a given data center has multiple Internet connections, this strategy also places a drag on the connection customers use to communicate with an organization's websites.

There is a point at the edge of the network, however, between public-facing applications and the world, where data center administrators have access to a wealth of control and information. That point is where F5® BIG-IP® Local Traffic Manager™ (LTM) Application Delivery Controller resides, monitoring application/server availability and directing connections to the appropriate servers while maintaining information about connections between applications and users. BIG-IP LTM ensures that Internet-served solutions are available to users as long as those users can get to the data center network.

This strategic point of control is also a leverage point for other critical functionality. F5 BIG-IP® Access Policy Manager® (APM) is an access and security product that can reside on the same device as BIG-IP LTM. From this location between users and applications, it can handle security issues with calls to all of the major authentication and access control products on the market today. BIG-IP APM maintains the context of the security information while keeping unauthorized users from ever reaching a server.

From this same control location, the data center WAN connection can also can be optimized and secured. F5 BIG-IP® WAN Optimization Manager™ (WOM) is an acceleration tool for data center-to-data center communications that encrypts, compresses, and deduplicates data before it is placed on the wire, sending less traffic and securing that traffic with state-of-the-art encryption.

Working together, BIG-IP LTM, APM, and WOM give data center administrators maximum influence at the strategic point of control to deliver a website and applications that meet the secure, fast, and available ideal.

Regardless of the industry being served, the data center of the future depends on the ability to secure applications and traffic while providing high availability and sophisticated traffic routing and redirection.

55% of IT organizations reported that the ability to redirect, split, or rate-shape application traffic between multiple data centers i valuable when choosing a cloud provider.

Source: TechValidate Survey
TVID: 3D4-C64-27A

Secure, Fast, Available. One Platform.

The number of devices between users and applications is important. Each device creates latency and introduces another point of failure, another chance for a given "solution" to become the problem. Placing as much advanced Application Delivery Controller (ADC) functionality into one place as possible reduces the number of devices in the communications path and enables a single pair of redundant devices to maintain availability in an emergency. Advanced F5 ADC products offer the most integrated approach to maximizing the strategic point of control in the data center network.

- BIG-IP LTM provides load balancing, server monitoring, and traffic direction capabilities.
- BIG-IP APM is a product module that can run on BIG-IP LTM to control authentication, authorization, and accounting (AAA) where users enter the network.
- BIG-IP WOM is a product module that can run on BIG-IP LTM to provide encryption, compression, and deduplication for communication between data centers.

Individually, these F5 products can improve the overall network and server environment by increasing uptime, security, and utilization of WAN bandwidth. Taken together, they can be utilized to provide all authorized users outside the data center with communications that are secure, fast, and available.

- By improving data center-to-data center communications, BIG-IP WOM clears network bandwidth for other use.

- By providing centralized AAA where users enter the data center network, BIG-IP APM taps the best of the available authentication services to help set highly granular access to corporate resources.
- By monitoring servers, re-routing traffic, and balancing loads, BIG-IP LTM makes web applications more resilient without having to change the applications or code.

Expand the power of BIG-IP LTM with BIG-IP WOM and BIG-IP APM

When the data center's Internet connection acts as a strategic point of control, data center administrators and IT managers gain the ability to drive traffic and adapt to dynamic circumstances while maintaining context-aware security and high resilience.

Achieve flexible control with BIG-IP LTM

BIG-IP LTM creates pools of servers, with each server capable of handling requests coming in over the wire. Those pools can then be monitored, as can each server in a pool. Traffic can be routed in a variety of ways, from the use of application templates—which tell BIG-IP devices how best to deal with known applications and their protocols—to the creation of F5 iRules® scripts that can redirect users from the access URL to one with more availability.

With BIG-IP LTM in place, IT staff have the tools to scale applications, take on more users, and tackle upgrades with confidence, knowing everything will be handled smoothly and efficiently from a strategic point of control that virtualizes IP access. The IP address represents a BIG-IP entry point, but how any given request is handled beyond that entry is dictated solely by the needs of the IT organization. That's because the application and its IP address are separated at the strategic point of control, giving IT staff the ability to insert monitoring and management or even redirect the user to a different locale.

Optimize bandwidth with BIG-IP WOM

Unlike BIG-IP LTM, BIG-IP WOM does not deal directly with users. Instead, it concerns itself with the back end of the application and data center puzzle. How can IT staff make the most of the data center WAN connection, which for most organizations is the same gateway through which users access the website? BIG-IP WOM specializes in answering that question.

Layering increased WAN optimization functionality on top of BIG-IP LTM, BIG-IP WOM offers deduplication, compression, and encryption while utilizing the rate shaping, TCP optimizations, and other "one sided" functionality of the BIG-IP device. Focusing on tasks that must be undone on the other end—such as encryption and deduplication—BIG-IP WOM calls on BIG-IP LTM to manage one-way tasks, which won't later be undone and thus are better handled from a single point. BIG-IP WOM is a symmetric product. Installing BIG-IP WOM in a data center implies that a second BIG-IP WOM will also need to be installed at the other end of the WAN connection, but the opportunity to improve bandwidth use by as much as 48 times saves costly WAN connection upgrades and more than justifies that need. Plus, once a BIG-IP WOM exists at a backup data center or other remote location, BIG-IP LTM also resides there, meaning all of the benefits of BIG-IP LTM are at both locations, and the network staff can now do things like construct tunnels to send overflow traffic to the remote data center without users even knowing they're being redirected.

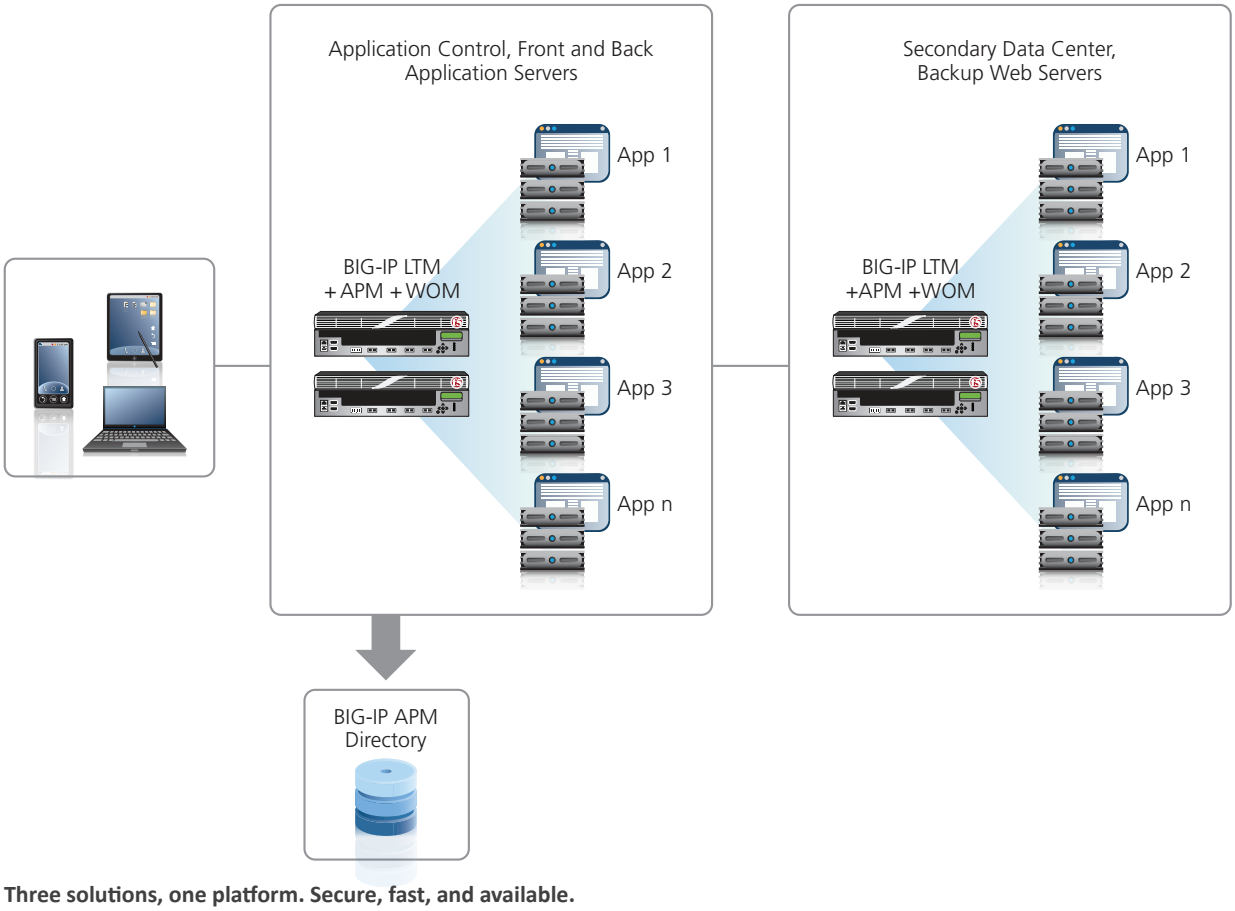
Strengthen security with BIG-IP APM

In this integrated approach, BIG-IP APM handles access at the network's strategic point of control in a manner that both increases the security of web applications and enables seamless extension of existing AAA infrastructure to remote users. Because BIG-IP APM resides on BIG-IP LTM hardware, it validates users—both for access and authorization—simultaneously with their routing by BIG-IP LTM. This allows the extension of security to layers 4-7 and connects into LDAP and administrative desktop services (ADS) so access to an application or a part of an application can be managed and determined based on group membership or other rights and attributes.

The complementary access and authorization facets of BIG-IP APM provide a stronger overall security architecture. When customers come randomly from the Internet to browse an internally hosted site, access can be determined and controlled before such users ever reach a web server, thus protecting against attacks that seek a software weakness. When employees come in through the Internet, BIG-IP APM can validate their authorization to access their desired applications, again protecting data center systems from rogue hackers. BIG-IP APM can even be configured to force checks on the client for assurance that valid users are not carrying viruses over the Internet and into the data center.

Using application profiles and a UI-based access control system, IT staff can readily create access statements such as, "This is Microsoft Exchange 2010, and this group

of ADS users should be granted access." With that information, BIG-IP APM will allow the authorized group access and deny any other users. A GUI-based access control list makes it easy to later add authorized users or modify rights.



Three solutions, one platform. Secure, fast, and available.

The Power of Three

All of this traffic management, WAN optimization and AAA functionality is powerful in the individual products, but when all three are deployed together, administrators have the tools to create a secure, fast, and available ecosystem that's aligned with business priorities and that makes the lives of IT staff easier while keeping costs down.

Each of these BIG-IP products capitalizes on the functionality of the other two, making the most of their integration. For instance, the ability of BIG-IP LTM to

route and manage traffic is useful to BIG-IP APM when security dictates that a user be denied access to a resource. In that case, BIG-IP LTM can be directed to present an unauthorized user with a login page, send the user to a specialized page with a message that indicates why the user was denied, or even to simply reject the connection.

Similarly, BIG-IP LTM enhances BIG-IP WOM by combining TCP optimization with WAN acceleration, which largely mitigates the effects of latency, even before compression and deduplication are applied to the data streams. Most customers find the encryption capability of BIG-IP LTM truly effective in keeping their hardware costs down, since it helps them to offload a lot of work from servers and place it into a specialized subsystem—hardware on a hardware platform, software on a virtual machine—that's optimized for encryption. With each server relieved of encryption duties, resource consumption goes down and the servers are doing less work, so more tasks can be assigned to them. This encryption engine can also be applied to BIG-IP WOM on the way out of the building to secure communications over the Internet.

BIG-IP WOM does not increase actual available bandwidth, but it increases apparent bandwidth by reducing the amount of data transferred over the connection so more data can be sent over existing connections. This data reduction means that replication—always a difficult prospect over the WAN—might well become possible with BIG-IP WOM. Similarly, by reducing the bandwidth required for all applications, BIG-IP WOM increases the perceived performance of any applications with a remote element—whether a front-end user or a back-end system—because there's less congestion on the line.

In the extreme case where a connection is still near maximum utilization, the rate shaping of BIG-IP LTM can help prioritize the traffic being transferred. This means assured completion of mission-critical applications, whether the application is a complex web application or the day's replication task, while less critical connections may be rate limited or dropped, according to the organization's IT policies.

Meanwhile, BIG-IP APM delivers access to critical resources under the umbrella of overall security policy simply by connecting applications to an organization's internal AAA servers. When it is positioned in the strategic point of control, BIG-IP APM can call these internal resources without exposing them to the world, and then use the results to control access to other internal applications. With the security capabilities of BIG-IP LTM as an underlying framework, BIG-IP APM can encrypt when necessary, taking advantage of TCP optimizations, DDoS resistance, and other functionality built into the system by BIG-IP LTM.

F5 devices allow us to rapidly deploy application access to a wide range of users, from customers and consultants to employees, with minimal configuration and support requirements.

Source: TechValidate Survey
TVID: 487-29B-0C1

For an example of this integrated power, suppose user Bob wants to access the internal corporate web portal hosted on Microsoft SharePoint from his Apple iPad while headed to work on public transit. He'll make a request to a public-facing URL residing behind a BIG-IP platform. The BIG-IP platform will understand that the IP it presents at that URL is protected and will tell the BIG-IP APM module to apply the security policy from the template for that URL (which may be the built-in SharePoint template). Bob will be asked to log in, since that's what the template requires. When he does so, his credentials will be compared to those of authorized users in Microsoft Exchange, and if his username is in the list, he will be redirected to the actual application over a secured connection, his authentication already established. Meanwhile, any changes he makes to documents or other files residing on the company intranet will be replicated to the redundant data center via BIG-IP WOM with little or no impact on his ability to continue using the SharePoint server.

Conclusion

Given the ever-increasing use of Internet connections, the corporate network needs to be locked down. Applications must be more reliable and resilient, and the performance and stability of WAN connections enhanced. BIG-IP LTM, BIG-IP APM, and BIG-IP WOM can work together to achieve all of those goals and better align IT systems and infrastructure to organizational needs. Deployed together, this powerful triumvirate makes systems secure, fast, and available, using one of the network's strategic points of control to insert critical functionality between services and service consumers. By offloading security functions, bandwidth management, and WAN optimization from core systems, these three complementary products can therefore enable those systems to focus on business challenges and free IT staff to concentrate on helping the overall organization achieve its goals.

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

CS01-00051 0511