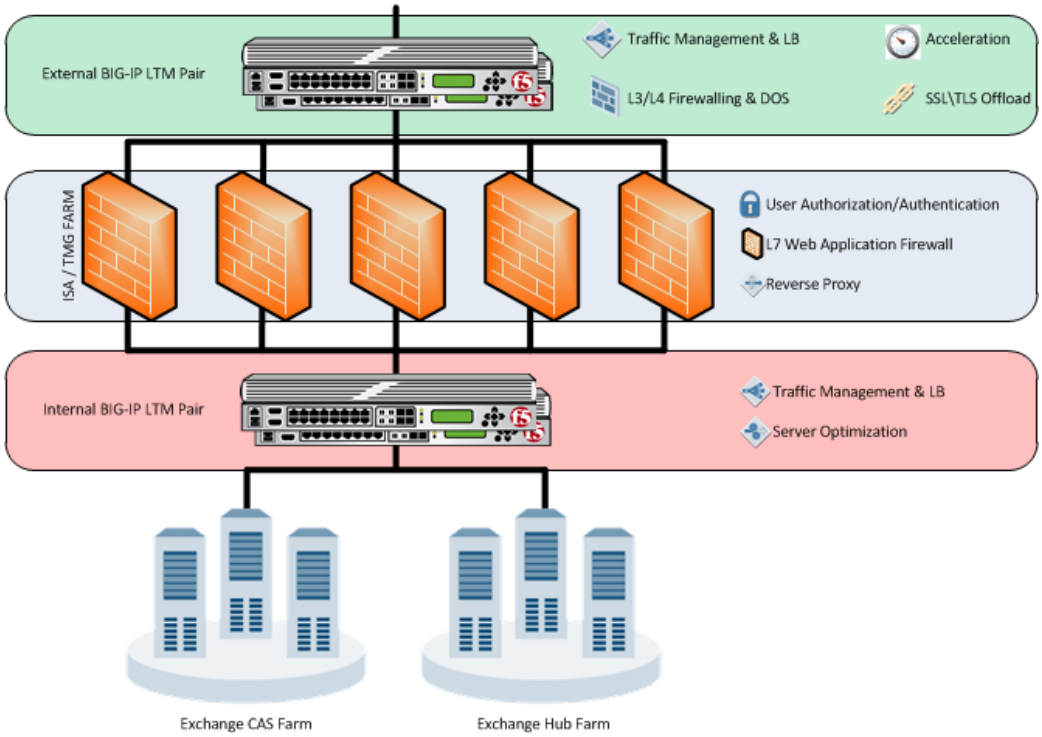
TMG2F5 Series: Publishing Microsoft Exchange Using F5

Ryan Korock, 2012-21-09

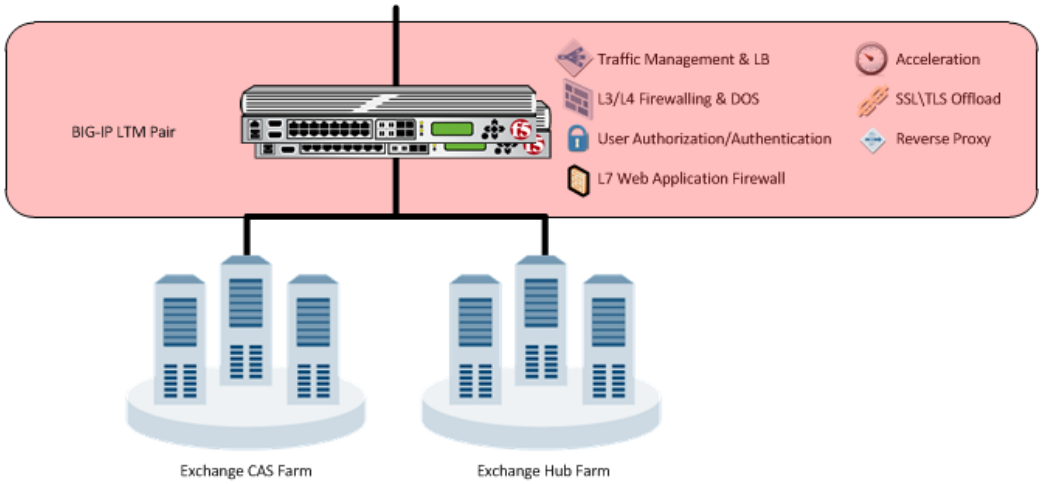
Although predicted by some, Microsoft caused quite a stir last week by formally announcing the discontinuation of Forefront Threat Management Gateway. One of the primary use cases of TMG has been to externally publish Microsoft applications, and F5 has often co-existed in these environments. With the sunset of the TMG line, it's time to look at alternative technologies to replace the responsibilities of TMG, and the F5 gear that you already have in the network may be the best solution. I am putting together a 3 part blog series on leveraging F5 as a suitable (dare I say, better?) TMG replacement for your Exchange, Lync, and SharePoint deployments. This is the first post of the series, and will focus on using F5 to securely publish Exchange services.

Architecture

One of the most significant benefits of leveraging F5 to publish Exchange services is the consolidation of devices & simplification of the architecture. Enterprise customers leveraging TMG for publishing applications are often using F5 to provide the traffic management control to the TMG & application services, which means multiple devices and a tiered network. In a traditional F5/TMG deployment, traffic management and security responsibilities have often been split amongst devices like below….



As you can see, there are several tiers in the architecture, which leads to complexities in configuration and troubleshooting. By onboarding the publishing responsibilities onto the BIG-IP, customers can simplify the architecture by reducing the network segments and consolidating into an HA pair of BIG-IP devices. And more importantly, all without losing significant functionality.



Now that we have a basic understanding of the architectural benefits of using F5, let's dive deeper into some of the features and functionality that F5 will be providing when being used to publish Exchange Server.

Traffic Management

Yes, TMG does have basic server load balancing capabilities, however this has never been functionality that has met the needs of the enterprise customer. Even in the heyday of TMG, most enterprise customers opted to leverage a 3rd party technology, such as the BIG-IP LTM, to handle this workload. BIG-IP has been designed from the ground up (both hardware and software) to handle traffic management, and honestly, you won't find similar performance nor features in any other solution. A critical piece of the Exchange network solution is providing high availability and scalability through load balancing, and the BIG-IPs application health awareness & load distribution engines deliver on the promise of making sure users & mail are consistently sent to Exchange servers that are alive and performing optimally. As enterprises move to multi-datacenter Exchange deployments, F5's Global Traffic Manager (GTM) can provide the same load balancing and resiliency intelligence, but at the wide area level.

Layer 3-7 Firewalling

With roots in the firewall space, TMG has a history of providing layer 3/4 security, and over the last few years Microsoft added in application firewalling as well. BIG-IP LTM, an ICSA certified firewall, is a default-deny platform coupled with an advanced DDOS mitigation engine, making it extremely well suited to provide the layer3/4 defense perimeter. BIG-IP LTM also ships with content inspection & iRules, that allow administrators write basic filters to stop well known application layer attacks. Enterprises looking for a more advanced Web Application Firewall for Exchange can activate the Application Security Module (ASM), which ships with pre-built security policies for Outlook WebApp and ActiveSync.

Server Optimization

I hate to see this significant benefit of the solution overlooked, primarily because of the dividends it pays. Exchange Server makes use of SSL/TLS for a majority of the client access protocols, including Outlook Anywhere, Outlook WebApp, and Activesync. The server CPU cost of negotiating these SSL transactions is significant, and by offloading the SSL responsibilities to the BIG-IP LTM, enterprises can leave their Exchange servers to do what they do best, serve content. BIG-IP LTM also includes TCP optimizations and content caching which can significant decrease the load on the servers. By leveraging the optimization & offloading features in BIG-IP LTM, customers can decrease the load on the servers, allowing them to perform faster, and also possibly allowing them to go with a smaller farm of servers to serve the same amount of users.

Perimeter Security

Let's face it, exposing domain joined servers (CAS, Hub) to anonymous connections is a bad idea, and this is probably one of the most compelling reasons to put TMG in front of your Exchange architecture. The good news is that F5's Access Policy Manager (APM), which is a software module for BIG-IP LTM, can provide an enhanced perimeter of security by making sure no user or connection reaches the CAS server until it has been authenticated and authorized. The APM engine is incredibly powerful and flexible, and new customer use cases are brought to our attention constantly. Client side certificate support, AD FS integration, client interrogation, single sign on, Active Directory attribute enforcement, are all features that APM supports in making sure the right level of privileges are granted the users that are authenticated before being sent to the CAS services. The Active Directory awareness that APM also provides has been instrumental in helping enterprises seamlessly upgrade from Exchange 2007 to Exchange 2010 without making any client side modifications at all.

Acceleration

Native BIG-IP LTM includes a set of acceleration technologies, such as caching and compression that provide benefit for Exchange deployments. Enterprises have the option of going a step further and leveraging advanced acceleration of Exchange by enabling the WebAccelerater Module (WAM) on top of their BIG-IP LTM to reach new levels of performance. WAM provides a set of acceleration technologies, such as browser optimization, deduplication & intelligent client side caching that enterprises with a large remote workforce, or multiple branch offices will want to take a look at.

Administration

10+ network and access protocols can make it a challenge to deploy Exchange with the network optimally configured. Many of these protocols have different persistence, security, and acceleration profiles, and a configuration that may end up 'working' is still not the optimal solution. BIG-IP LTM's wizard driven configuration menu, known as 'iApp', is designed to request the most basic system information from the Exchange administrator (Server IP addresses, hostnames, etc) and dynamically build the configuration on their behalf. The result is an optimal configuration that was simple and fast build, and much less prone to human error.

Hardware

Yes, the diagram above shows consolidating 5 TMG servers down to a single failover pair of BIG-IPs; and Yes, this is what we have often seen customers be able to do. To be honest, we've even seen customers go from much larger numbers of TMG servers to a single pair of BIG-IPs. BIG-IP is a special purpose platform with custom hardware built to provide advanced network services. Dedicated layer 2/3 chipsets, SSL and compression hardware, and specialized multi-core processing FPGAs are some of the pieces that allow BIG-IP LTM to manage and process network traffic at speeds and complexities not seen in typical server hardware.

The others….

There are numerous other reasons to use F5 to publish Exchange, including

1. Single URL access, which gives the ability for Exchange administrators to give a single URL to all users, regardless of which device they will be using, or what protocol they will be connecting with.

2. Advanced Hosted & Hybrid Exchange deployment integration, that includes support for advertising a single point of client access and silently directing those users to their appropriate mail system. For customers migrating to/from hosted Exchange or Office 365, or moving forward with a long term hybrid solution, this removes the need to maintain different access URLs for the different mail systems. All of this integrates well with ADFS.

3. Integration with 3rd party monitoring Solutions, including System Center Operations Manager, that in conjunction with BIG-IP provide fine grain detail about the Exchange system and user access.

4. Open APIs that allow for management & automation through tools such as PowerShell and System Center Orchestrator.

5. Multi-application support, which allows customers to leverage the same F5 investment across multiple application environments. The BIG-IPs providing publishing for Exchange can also provide the same benefits for SharePoint, Oracle, VMWare, etc…..

I hope this post gives you some insight as to the benefits of using F5 to publish Exchange services. In light of the recent announcement regarding the future of TMG it's time to consider alternatives, and F5 fits in well as a solution to provide network security, acceleration, and availability. All of the features described above are available in a lab edition of our virtual platform, allowing for customers to test the solution by running the BIG-IP as a virtual machine. Reach out to your F5 sales rep or F5 partner for information on access. If you want more information on F5's solution for Exchange, check out our solution page.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | 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