Post-TMG: Securely Delivering Microsoft Applications

Microsoft Forefront Threat Management Gateway customers need an alternative to secure their Internet-facing Microsoft applications. F5 BIG-IP Application Delivery Controllers provide the advanced features necessary to fill the gap.

White Paper

by Gregory Coward

Introduction

With the recently announced departure of Microsoft Forefront Threat Management Gateway (TMG), many organizations currently using or considering TMG face a dilemma: How, or more importantly, what will administrators use to secure their Internet-facing Microsoft applications such as Exchange, SharePoint, and Lync?

Securely deploying an application to the Internet requires a combination of technologies, including a reverse proxy with pre-authentication, a web application firewall, and a traditional network layer firewall. These security layers may be delivered separately along the deployment data path or from one central point of control, such as with TMG and F5 BIG-IP solutions. Regardless of which way security is delivered, administrators and decision-makers need to take a holistic approach when publishing Microsoft applications to the Internet.

This document provides a brief overview of the features and benefits provided by the aforementioned technologies, and details how BIG-IP Application Delivery Controllers (ADCs) can more than fill the gap left by TMG.

Reverse Proxy/Pre-Authentication

Using an ADC for reverse proxy with pre-authentication at the network perimeter provides a critical layer of security. Much like a nightclub bouncer working the door, the ADC isolates internal resources from external access, allowing only authenticated and authorized users to enter the corporate LAN and use internal resources.

A reverse proxy terminates external connections at the perimeter and, upon successful authentication and authorization, establishes a proxy connection into the organization's LAN. In addition to supporting these basic functions, ADCs can further secure organizational assets with the following additional functionality.

A Strategic Point of Control for Application Delivery

A reverse proxy with pre-authentication provides a central point from which to administer access to multiple applications. Without this central management point solution, access must be configured and managed separately at each internal resource, such as Exchange and SharePoint. All too often, different individuals and groups administer these internal resources, and this independent access control makes it challenging to apply corporate security policy. In contrast, implementing ADCs provides a strategic point of control where corporate applications can be deployed more securely and consistently.

Endpoint Inspection

Some remote access solutions make it possible to identify and evaluate the client endpoint as part of the authentication and authorization process. For example, with BIG-IP Access Policy Manager (APM), administrators can manage access to corporate resources based upon the device that is trying to connect. Administrators can also ensure that the approved device adheres to corporate policies for AV status, OS versions, patch levels, and more.

Multifactor Authentication

Remote access solutions provide a much more secure authentication mechanism than what can be found natively on most applications. This is especially critical when considering the vast and ever-growing number of devices for which organizations need to provide access.

TMG provides for some multifactor authentication integration, including RSA SecurID, RADIUS OTP, and client-side certificates. BIG-IP APM can also be integrated with these authentication types. Using the flexibility of the BIG-IP APM Visual Policy Editor (see below) and F5 iRules, administrators can integrate with a variety of authentication providers and technologies.

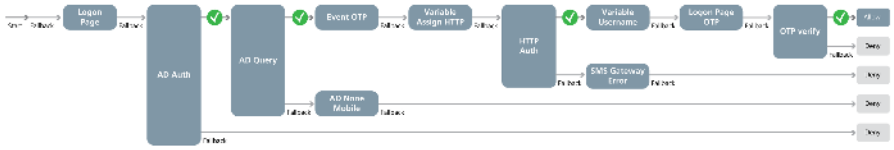

Figure 1: BIG-IP APM Visual Policy Editor.

Securing Internal Assets with BIG-IP ADCs

BIG-IP ADCs include advanced features that provide organizations with the critical security they need. These features include:

Pre-authentication

BIG-IP ADCs support authentication of users against a wide array of providers, including Active Directory, LDAP, RADIUS, RADIUS OTP, and RSA SecurID. BIG-IP ADCs also enable dynamic application of authentication methods, including multifactor. For example, Outlook Web Access, ActiveSync, and Outlook Anywhere (RPC over HTTP) can be published on the same IP/port while using different authentication methods.

Advanced authorization

Access is not always a yes-or-no decision. Approval may depend upon a host of factors such as where users are attempting to access resources and whether they are accessing from an approved device. BIG-IP APM can query Active Directory for user attributes such as AD group membership, assigned mailbox database, and device IDs. These attributes, along with deep packet inspection, can then be used to dynamically apply policy, which further enhances device security.

Single sign-on

After signing into one application, such as Outlook Web Access, BIG-IP ADC users can seamlessly access on-premise applications such as SharePoint, as well as hosted applications such as Microsoft Office 365.

Endpoint inspection

BIG-IP APM makes it possible to manage access to corporate resources based upon the device that is trying to connect. The solution also ensures that the approved device adheres to corporate policies for AV status, OS versions, patch levels, and more.

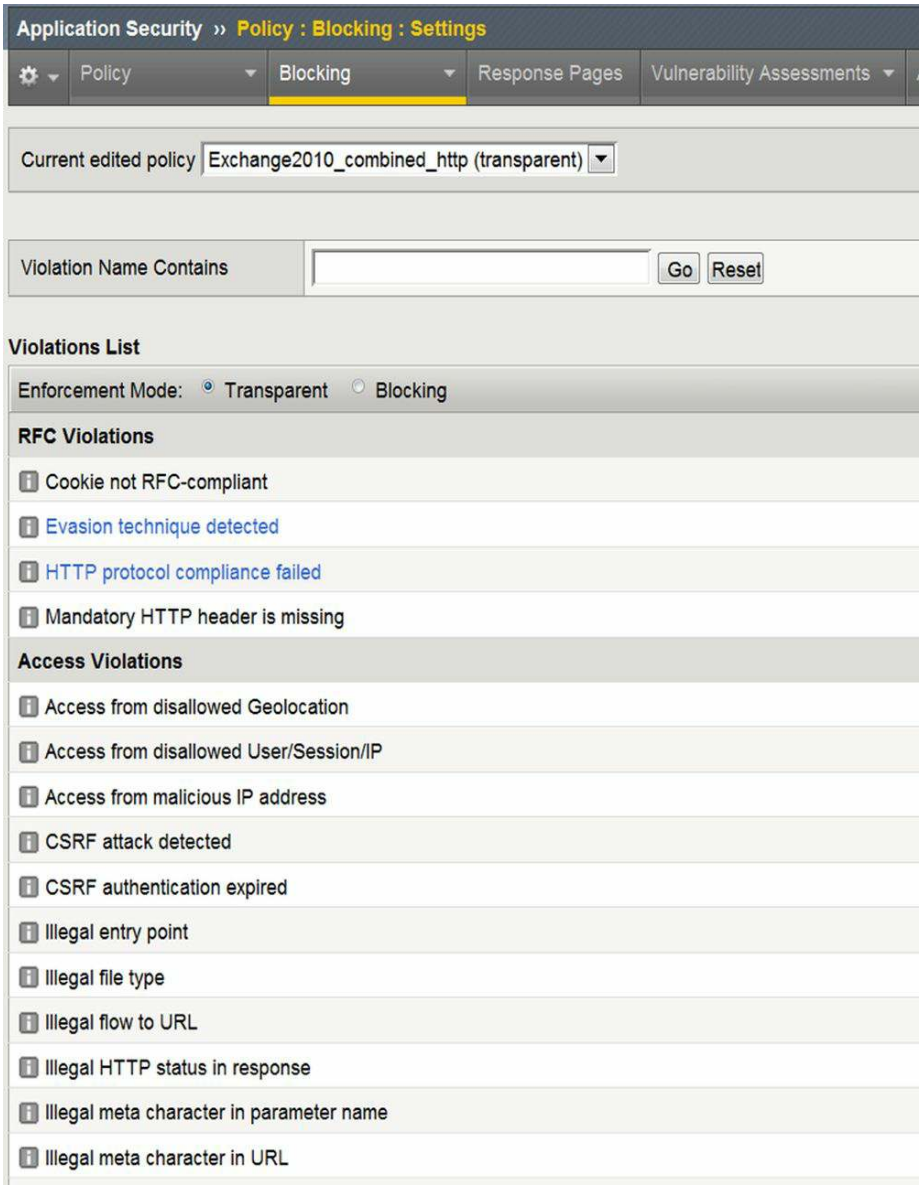

Figure 2: BIG-IP ASM.

The Web Application Firewall: Securing Layer 7

While a network firewall works at and secures traffic at Layers 3 and 4, a web application firewall (WAF) analyzes and secures application traffic at Layer 7. WAFs protect web servers from malicious traffic, and are designed to combat attacks such as cross-site scripting, SQL injection, and cookie poisoning.

In contrast to TMG's signature-based, negative model filtering, BIG-IP Application Security Manager™ (ASM) module uses both a positive and negative security model to protect against Layer 7 distributed denial-of-service (DDoS) attacks, SQL injection, and OWASP Top Ten attacks, and to secure the latest interactive AJAX applications and JSON payloads.

BIG-IP ASM first analyzes internal applications such as SharePoint and Exchange ActiveSync in "learning mode" to identify legitimate traffic. After the learning period is complete, traffic that does not adhere to the application's standard traffic patterns can be isolated and blocked. This positive security model provides a high level of protection against unknown or "zero-day" attacks.

The Network Firewall: Securing Layers 3 and 4

To ensure network security, organizations that expose internal resources to the Internet rely on a network (Layers 3 and 4) firewall. A network firewall works as a packet filter and uses access rules to control access to and from the organization.

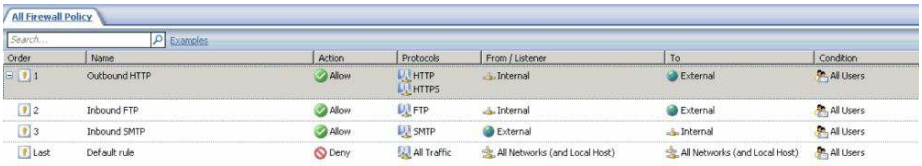

Figure 3: TMG firewall policy.

In addition, a network firewall can be "stateful," meaning it is aware of and can act upon the state of a given connection. Stateful firewalls, such as TMG and BIG-IP solutions, further enhance security by granting access only to traffic that is part of an established connection.

Securing the Network with BIG-IP ASM

BIG-IP ASM operates on a platform that consolidates an application delivery firewall solution with network and application access control. The solution secures web applications in traditional, virtual, and private cloud environments with features including:

- ICSA-certified network and application firewall: BIG-IP Local Traffic Manager™ (LTM), together with BIG-IP ASM, is an ICSA Labs certified L3-L7 firewall that can handle eight times more traffic than its closest competitor.
- Positive and negative model WAF: BIG-IP ASM uses both positive and negative security models to provide a high level of protection against unknown and zero-day attacks, as well as well-known application layer attacks.
- Predefined application templates: BIG-IP ASM includes a number of

preconfigured, application-specific security templates, including templates from Exchange OWA, ActiveSync, and SharePoint. These predefined templates greatly decrease the time and effort required to safely deploy a variety of web-based applications.

- Third-party integration: BIG-IP ASM integrates with a number of third-party vulnerability assessment providers, including WhiteHat and Cenzic.

Streamlining Application Delivery

One of the most significant yet least considered factors when deciding upon a suitable reverse proxy solution is the effect on the organization's network infrastructure. Scalability, availability, and overall performance are important factors that must be accounted for when deploying mission-critical applications such as Microsoft Exchange, SharePoint, and Lync.

The level to which scalability, availability, and performance are addressed varies greatly between a software-based solution such as TMG and hardware-based BIG-IP ADCs. For example, due to its limited scalability and simplistic load balancing technology, TMG servers are often deployed in an array. The TMG array can be load balanced with native network load balancing or, more commonly, deployed between a pair of hardware load balancers (see below).

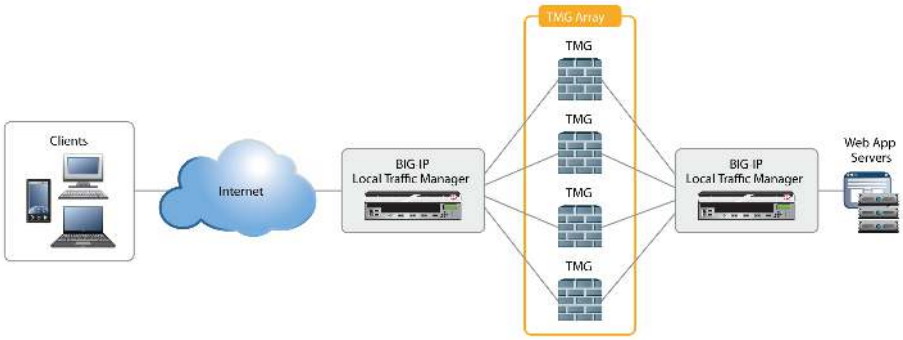

Figure 4: Load balancing the TMG array with BIG-IP LTM.

While this design satisfies the requirements for strong scalability, availability, and performance, it is not nearly as efficient as using the full features available on BIG-IP ADCs. Implementing BIG-IP APM and BIG-IP ASM can significantly streamline the network infrastructure required to deploy applications to the Internet (see below). The purpose-built, high-performance platforms of BIG-IP ADCs can handle substantially greater amounts of application traffic than TMG or, for that matter, other hardware-based competitors.

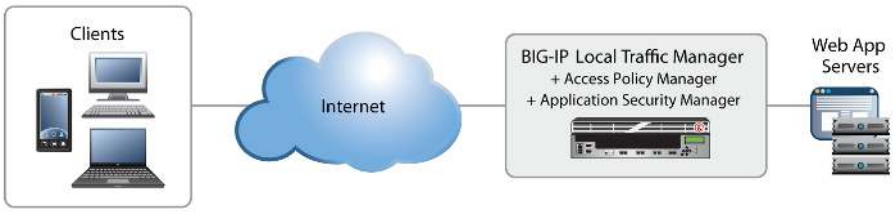

Figure 5: Replacing TMG with BIG-IP ADC and security modules.

Features	Microsoft Forefront Threat Management Gateway 2010	BIG-IP Solution
Reverse Proxy/ Pre-Authentication	Software-based SSL offload	High-performance, hardware-based SSL offload
	Authentication: Forms-based, basic, integrated, and certificates	Authentication: Multiple pre-authentication methods, including forms-based, HTTP Basic, Kerberos, and certificates. Authentication (including multifactor) can be dynamically applied.
	Multifactor authentication: Client certificates, RSA SecurID, and RADIUS OTP	Multifactor authentication: Client certificates, RSA SecurID, RADIUS OTP, SMS, and integration with multiple third-party vendors
Load Balancing	Load balancing method: Round Robin	Load balancing method: Variety of methods include Least Connections, Ratio, Dynamic Ratio, Observed, and Round Robin
	Persistence: Cookie-based, source IP	Persistence: Cookie-based, destination IP, source IP, SSL Session, Hash, and MSRDP
	Health monitoring: Limited to one of three options (HTTP GET, PING request, or TCP connection)	Health monitoring: Variety of customizable service-level health monitors for specific applications. Additionally, BIG-IP LTM has the ability to perform synthetic transactions to determine service availability.
Scalability/ High Availability	Windows-based software deployment	Purpose-built hardware platform built on proprietary architecture (TMOS)
	Primarily designed for small and medium businesses, a TMG array can scale out to a maximum of 50 array members* (requires a load balancing solution)	Variety of platforms (including virtual editions) available to accommodate organizations from small and medium businesses to enterprises and service providers
	Load balancing: Either WNLB (up to 8 TMG members) or third-party hardware-based solutions such as BIG-IP LTM	All-in-one, modular ADC encompassing security, scalability, high availability, and performance
Firewall Security	Stateful Layer 3 and 4 firewall	ICSA-certified stateful network firewall
	Network inspection: Negative security model, with hardcoded, protocol-specific application filters	Web application firewall (L7) with both positive and negative security model
		ICAP integration capability
		Integration with third-party vulnerability assessment providers

* Applicable to EMS-managed environment.

Figure 6: Side-by-side comparison: TMG vs. BIG-IP solution

Conclusion

To fill the gap left by TMG, administrators and decision-makers must consider numerous factors to determine the best way to deploy applications to the Internet. BIG-IP ADCs offer a compelling alternative to TMG that delivers the advanced security, availability, performance, and scalability organizations demand. Whether the need is for a secure reverse proxy, a Layer 3–7 firewall, a high-performance load balancer, or all three, BIG-IP ADCs provide a comprehensive solution to secure application delivery.

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

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com