F5 PARTNERSHIP SOLUTION GUIDE

F5 and Microsoft

Exchange Security Solutions

Deploying a service-oriented perimeter for Microsoft Exchange

WHAT'S INSIDE

Go Beyond Network Firewalls to Protect Microsoft Exchange

Business need and user demand for access to email anytime, anywhere, and from any device has created challenges for IT departments to keep this business-critical application secure, fast, available, and compliant.

Extending your security perimeter outward can improve security and availability for Microsoft Exchange email services published over the Internet (Outlook Web App, Exchange ActiveSync, Outlook Anywhere, and Exchange Web Services). F5® Application Delivery Controllers (ADCs) offer an ICSA Labs certified network and application firewall solution that creates a service-oriented perimeter for Exchange. With intelligent monitoring of traffic, pre-authentication, and access control for mobile devices, F5 helps you deploy highly available and secure email services.

Pre-Authentication

Avert threats before they reach the data center interior

KEY BENEFITS

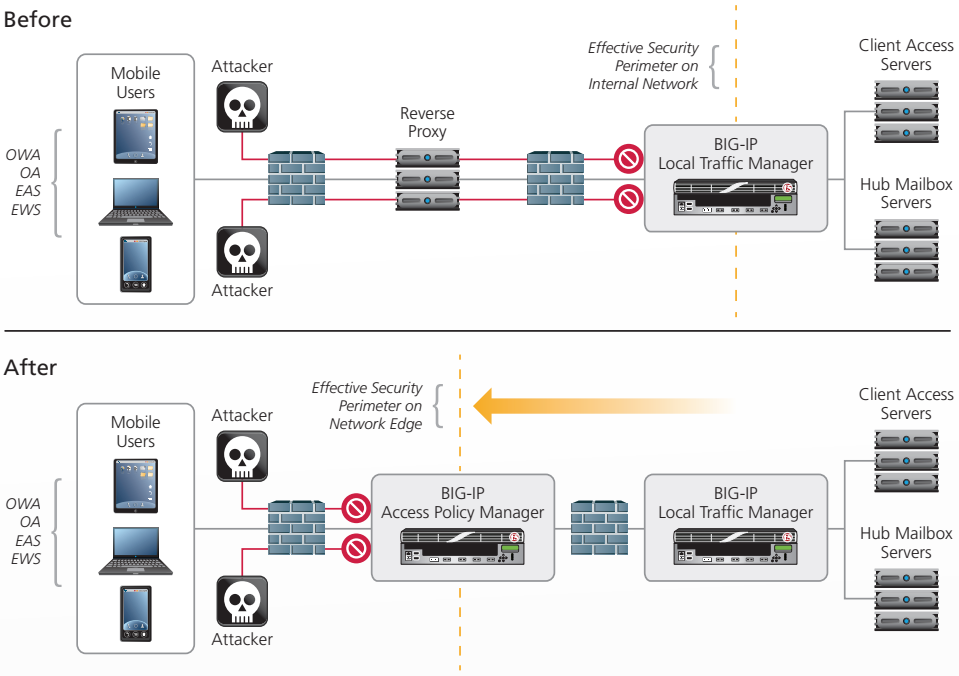
- Improve your security posture
- Ensure only authorized traffic reaches Exchange servers
- Reduce cost to operate and maintain security infrastructure

THE CHALLENGES

Preventing invalid and potentially malicious traffic from entering your data center can be challenging. Traditional network firewalls are designed to perform a basic level of filtering based on port, but are not designed to inspect and enforce highly intelligent security policies using surrounding contextual knowledge about the user, the application service being requested, or the device being used.

In fact, SSL encrypted application traffic needs to pass through the network firewall and on to another device near or on an internal data center network for termination—usually a hardware load balancer or even a specific application server itself. The challenge lies in enforcing effective security measures before the traffic reaches the internal network when the information needed to make access decisions is encrypted.

Relying on your servers to process the unnecessary and potentially malicious requests wastes valuable resources, slows performance, and leaves your business vulnerable to attacks, so the next choice is the hardware load balancer.



THE SOLUTION

F5 BIG-IP® Access Policy Manager® (APM) extends your security perimeter so that threats are eliminated before they reach your data center. BIG-IP APM is certified by ICSA Labs as a firewall device, but it is different from traditional network firewalls because it can intelligently inspect traffic for information about users, devices, and applications to increase security.

For Microsoft email services, including Outlook Web App (OWA), Exchange ActiveSync (EAS), and Outlook Anywhere (OA), BIG-IP APM prevents invalid traffic from ever reaching Exchange Server through pre-authentication, authorization, and device access control. User credentials are cached by BIG-IP APM, which proxies connections to Windows Active Directory and the Exchange Client Access server (CAS) array. These connections are made up of a set of customized verifications. For example, user name and password are used to prove the authenticity of the user. This user account can then be used to determine whether permissions are granted to access a given corporate resource such as Microsoft Exchange. Pre-authentication ensures that only authenticated and authorized traffic reaches the internal network where Exchange Client Access servers are located. Since only necessary traffic enters that network, processing load on servers is reduced, which helps their performance.

Using BIG-IP APM Visual Policy Editor, a workflow-like access path can be designed with forked logic and causal relationships to exactly represent corporate constraints for approved access and customized responses for validation failures. BIG-IP APM provides support for dozens of types of queries out of the box, such as collecting different types of logon information from users and performing queries into Microsoft Active Directory to verify specific information about users, security group memberships, and profile settings.

Provide secure access to email from mobile devices

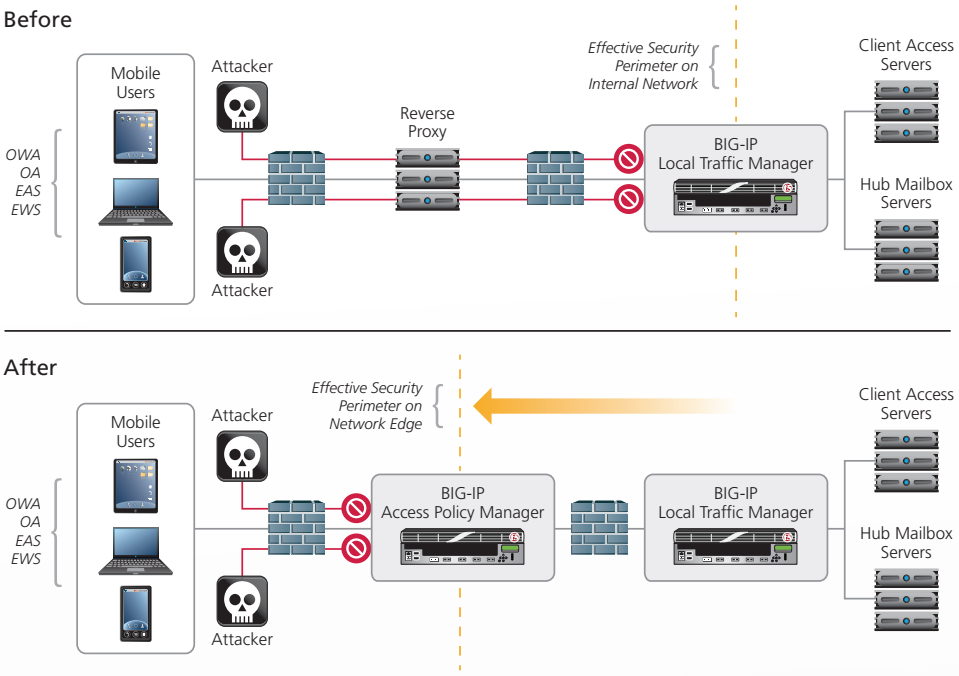
KEY BENEFITS

- Seamlessly support access to corporate resources from various types of mobile devices
- Implement advanced multi-factor authentication

THE CHALLENGES

The consumerization of IT and bring-your-own-device (BYOD) work policies have created a huge increase in access to corporate email from mobile devices. In today's world, email must be accessible to known trusted devices as well as an ever increasing assortment of unknown and untrusted devices.

According to a 2011 CIO.com report, network security breaches, possible loss of customer enterprise data, potential theft of intellectual property, and difficulty meeting compliance requirements are among the top concerns IT departments have about employees using personal devices for work.



THE SOLUTION

F5 BIG-IP Access Policy Manager (APM) provides a strategic point of control in the data center, supporting a variety of approaches for granting or denying email access to mobile devices. Building on its user authentication and authorization capabilities, BIG-IP APM also supports the use of user and device security certificates, Exchange ActiveSync User Policy settings, and other information stored in Active Directory, as well as device information provided in the packet flow, such as device type and device ID, to enforce multi-factor validation.

In Exchange Server, the Client Access server (CAS) role functions as the access point for all client traffic, including mobile devices that use the Exchange ActiveSync (EAS) protocol to access mailbox information over HTTPS. Using BIG-IP APM, traffic management decisions can be made and enforced at the network perimeter on a group and or individual basis while still allowing for the use of built-in Exchange security functionality such as ActiveSync policies and remote device wipe.

BIG-IP APM enables customers to enforce a customized security policy for Exchange access by mobile devices using a flexible set of pre-defined actions that represent their organizations' requirements for access approval—even from devices employees bring from home.

Simplify compliance and protect sensitive data

KEY BENEFITS

- Implement cost-effective PCI compliance and reporting
- Provide continual protection and built-in remediation
- Reduce OpEx by using the ADC platform

THE CHALLENGES

Network-level attacks are highly visible and disruptive, but application-level attacks are what threaten the core of a business. According to Gartner, 95 percent of security investments are focused on the network while 75 percent of attacks happen at the application level. These attacks can leave sensitive data—such as employee records, confidential information, intellectual property, and financial records—vulnerable to theft.

In addition, resolving application-level breaches can be time-consuming and expensive. According to a WhiteHat security report, the top 10 application attacks are cross-site scripting, information leakage, content spoofing, insufficient authorization, SQL injects, predictable resource location, session fixation, cross-site request forgery, insufficient authentication, and HTTP response splitting. The average time reported to resolve these vulnerabilities is 77 days. During those weeks or months, a business must take down the application or risk its security being compromised.

The prevalence of application-layer attacks against critical business applications makes securing those applications and verifying compliance with security and privacy regulations of paramount importance. Even those organizations that employ dedicated staff to review compliance and the security posture of applications prefer deploying solutions that automatically and continually provide compliance and reporting over manual human activity to achieve the same results.

THE SOLUTION

F5 BIG-IP® Application Security Manager™ (ASM) offers advanced, built-in security protection and remote auditing to help you comply with industry security standards, including PCI DSS, HIPAA, Basel II, and SOX. The system can be deployed in "Learning" mode and then switched to "Enforcement," where it provides continual protection.

The deployment, configuration, and operation of BIG-IP ASM delivers compliance in a cost-effective way—without requiring multiple appliances, application changes, or rewrites. Detailed PCI reporting determines if PCI DSS compliance is being met, and it guides you through the necessary steps to become compliant.

LEARN MORE

To learn more about F5 solutions for Microsoft, please visit **www.f5.com/microsoft**.

Tech tips, discussion forums, free samples, and more can be found on DevCentral,™ F5's global technical community, by visiting **devcentral.f5.com/microsoft**.

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

Microsoft Partner Network