Enhancing Exchange Mobile Device Security with the F5 BIG-IP Platform

As the use of mobile devices in the workplace continues to grow, the risk to corporate assets, and the need to mitigate these risks, increases as well. For many organizations, providing remote mobile device access to corporate assets such as Microsoft Exchange is not just a luxury but also a business requirement. Therefore administrators must find ways to balance the requirements of a mobile workforce with the need to secure corporate assets. Fortunately, F5® BIG-IP® Application Delivery Controllers (ADCs) can help.

White Paper
by the F5 business development team for the Microsoft Global Alliance

Introduction

As the use of mobile devices in the workplace continues to grow, the risk to corporate assets, and the need to mitigate these risks, increases as well. For many organizations, providing remote mobile device access to corporate assets such as Microsoft Exchange is not just a luxury but also a business requirement. Therefore administrators must find ways to balance the requirements of a mobile workforce with the need to secure corporate assets. Fortunately, F5 BIG-IP Application Delivery Controllers (ADCs) can help.

This document provides guidance for utilizing BIG-IP Access Policy Manager (APM) and BIG-IP Application Security Manager (ASM) to significantly enhance Exchange 2010 mobile device security.

Disclaimer and assumptions

While this guidance presents functional and tested solutions for securing mobile devices in an Exchange 2010 environment, it by no means represents the entirety of options available. One of the greatest strengths of the BIG-IP product line (including BIG-IP LTM, APM, ASM, and more) is its flexibility. The primary goal of this technical brief is to not only provide practical guidance but also to illustrate the power and flexibility of BIG-IP products. The reader is assumed to have general administrative knowledge of BIG-IP Local Traffic Manager (LTM) and familiarity with BIG-IP APM and ASM modules.

The following BIG-IP products and software were utilized for purposes of configuration and testing of guidance presented in this brief.

Product	Versions
BIG-IP Local Traffic Manager (LTM)	Versions 11.1 and 11.2
BIG-IP Access Policy Manager (APM)	Versions 11.1 and 11.2
BIG-IP Application Security Manager (ASM)	Versions 11.1 and 11.2
Apple iPhone 4 and 4S	iOS version 5.1.1
Windows Phone 7 - Dell Venue Pro	OS version 7.0.7392.212

Additional Documentation

- Microsoft Exchange Server 2010 (BIG-IP v11: LTM, APM, Edge Gateway) deployment guide: http://www.f5.com/pdf/deployment-guides/microsoft-exchange2010-iapp-dg.pdf

- BIG-IP Product Family Overview: http://www.f5.com/products/big-ip/

BIG-IP Access Policy Manager and ActiveSync

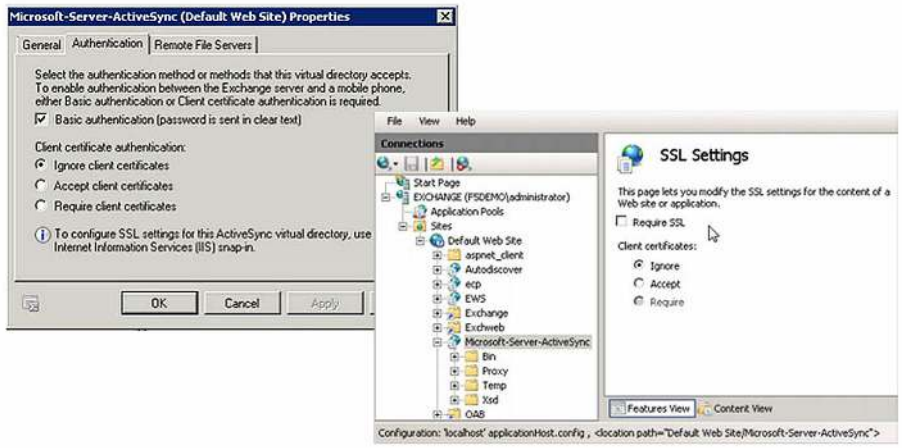
The client access server role (CAS) functions as the access point for all client traffic (including mobile devices), in Exchange 2010. More specifically, a majority of mobile devices make use of Exchange ActiveSync to access mailbox information. Allowing access into the corporate environment from mobile devices that can be easily compromised poses a significant risk. Therefore, deploying a multifactor solution that authenticates and authorizes not only the user but the device as well is crucial.

Working hand-in-hand with the reverse-proxy functionality of BIG-IP LTM, the BIG-IP APM module resides on the BIG-IP system and provides secure pre-authentication (including end-point inspection) to business-critical applications. Traffic management decisions can be made and enforced at the network perimeter on a group or individual basis. The following section utilizes the BIG-IP APM module to provide access based on username and password, device ID, and client certificates, while still allowing for the use of built-in Exchange security functionality such as ActiveSync policies and remote device wipe.

Username and Password Authentication- "Something You Know"

Exchange 2010 CAS Configuration

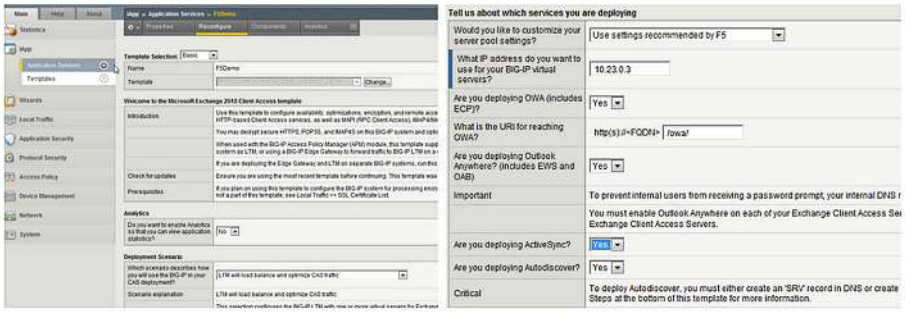
To facilitate SSL offloading to the BIG-IP system (as well as pre-authentication), the Exchange ActiveSync configuration and policy utilizes the default settings.



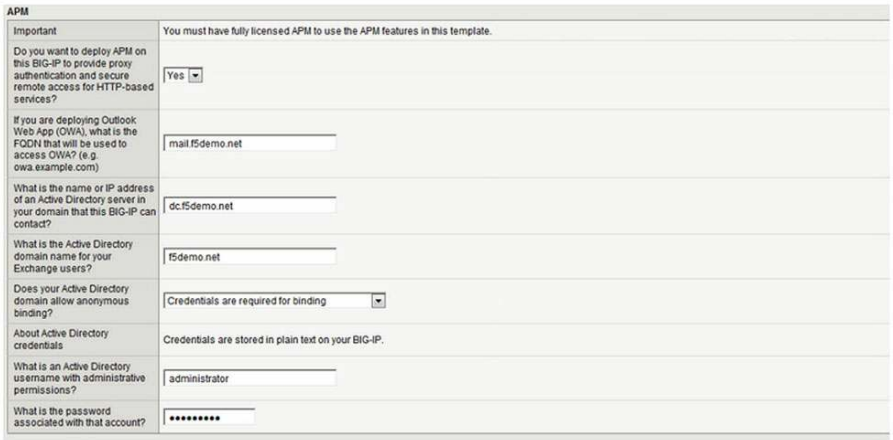
Initial iApps Configuration

Successfully configuring and deploying BIG-IP APM starts with the F5 iApps. First made available with version 11.0, iApps (F5 iApps: Moving Application Delivery Beyond the Network) provide an efficient and user-friendly means to quickly deploy business-critical applications onto the network.

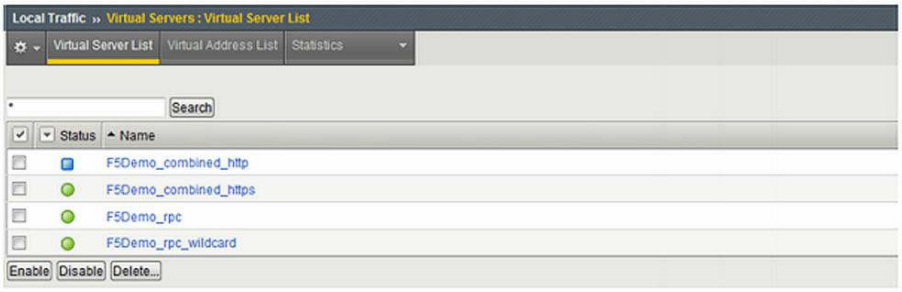
Illustrated below, as a starting point of this guidance, the Exchange environment will be deployed via the Exchange 2010 iApp. Utilizing a menu-drive configuration screen, the base iApp configures access to the Exchange 2010 CAS environment, including access to Exchange ActiveSync.

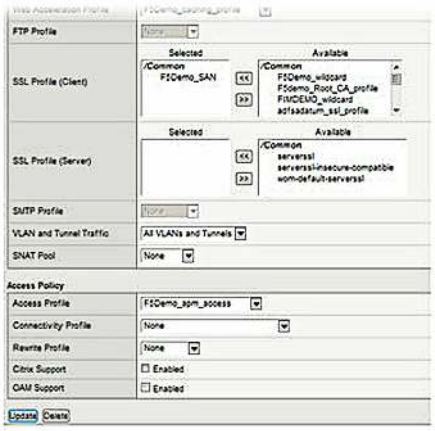


BIG-IP APM configuration is performed via the iApp.



A completed deployment is illustrated below.





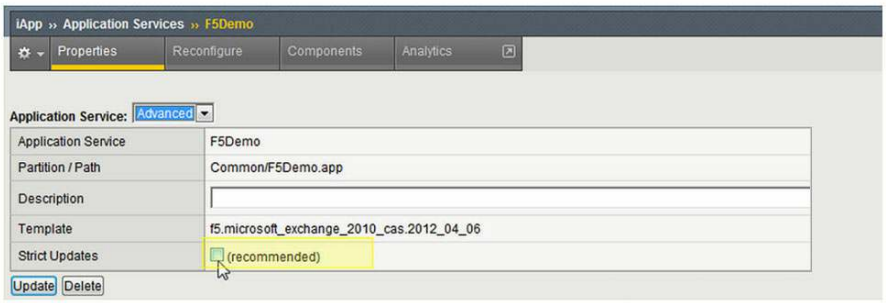
This basic configuration of the BIG-IP system provides advanced traffic management and optimization functionality including load balancing, compression, caching, and session persistence. In addition, pre-authentication is provided for all web-based traffic, including traffic from Outlook Web Access, Outlook Anywhere, and Exchange ActiveSync. Credentials (username and password) are requested by and delivered to the BIG-IP system, which in turn authenticates the user against Active Directory. Only properly authenticated users are allowed access into the organization's internal environment.

Device ID Validation-"Something You Have"

To further enhance the security posture, many organizations wish to restrict access to corporate email from only pre-approved mobile devices. These approved devices may be assigned to a specific user or may be included in a pool of devices that can be provided to users on an as-needed basis. Utilizing the flexibility of BIG-IP APM and the unique device IDs associated with mobile devices, the previously configured Exchange deployment can be easily modified to enforce access based on both username and password, as well as the physical device.

Modifying the iApp-Created Deployment

Before modifying the BIG-IP configuration, the iApp-created configuration needs to be set to allow for non-iApp updates. This is done by modifying the properties of the specific application service (see below).

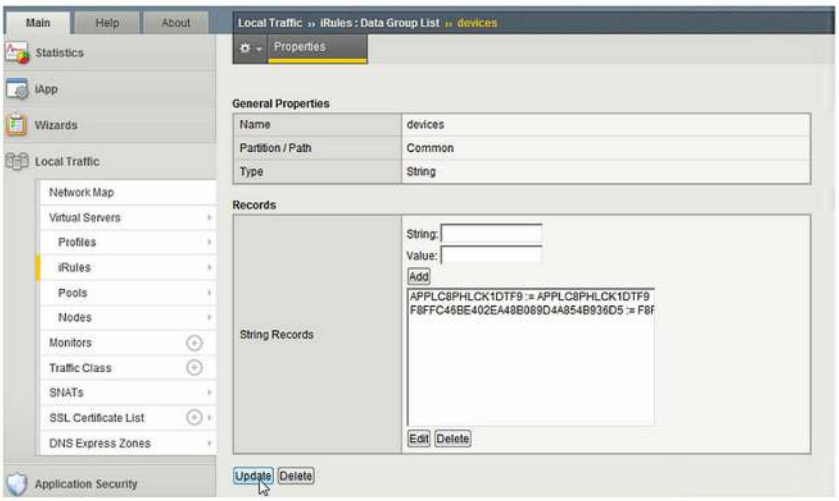


Device Validation Method 1-"Organization Device Pool"

The BIG-IP system can be configured to use a pool of approved devices in the authentication process. Only authenticated users with approved devices (devices that are included in the shared pool) will be granted mobile access to the Exchange environment. This method utilizes centralized pool of acceptable devices and allows administrators the flexibility to "check out" devices to individual end-users on an as-needed basis.

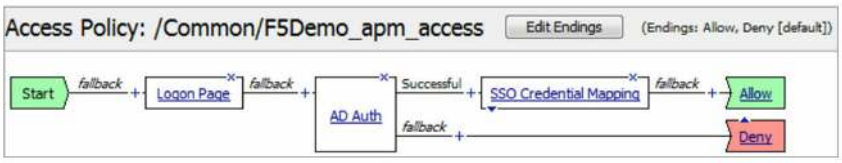
The following steps are performed on the current BIG-IP deployment.

1. Create a Data Group List that includes all relevant device IDs.

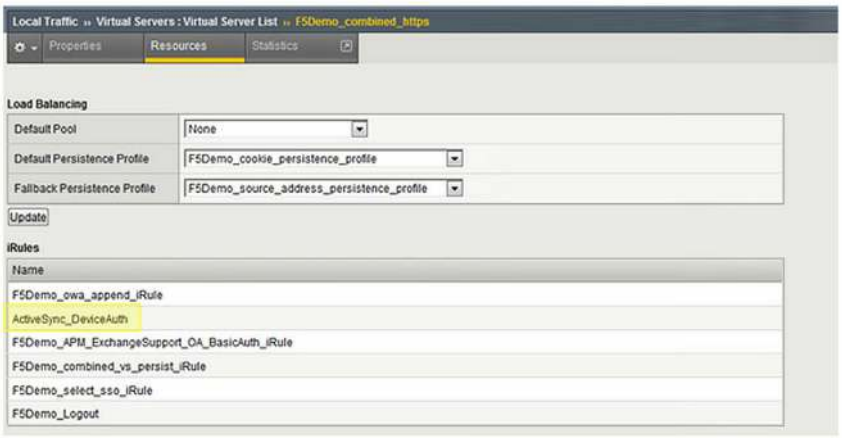


As an alternative to entering device IDs into the BIG-IP web GUI, reference an external file using the iFile capability of the BIG-IP system. Details are provided on DevCentral website: https://devcentral.f5.com/Tutorials/TechTips/tabid/63/articleType/ArticleView/articleId/1086514/v111ndashExternal-File-Access-from-iRules-via-iFiles.aspx

2. The existing access policy is utilized.



3. An F5 iRule is created and associated with the Exchange HTTPS virtual server. The iRule compares the device ID of the client connection (contained in the HTTP query) with the device IDs stored in the previously created Data Group List. If the device ID is not in the list of acceptable devices, the session is terminated and access is denied.



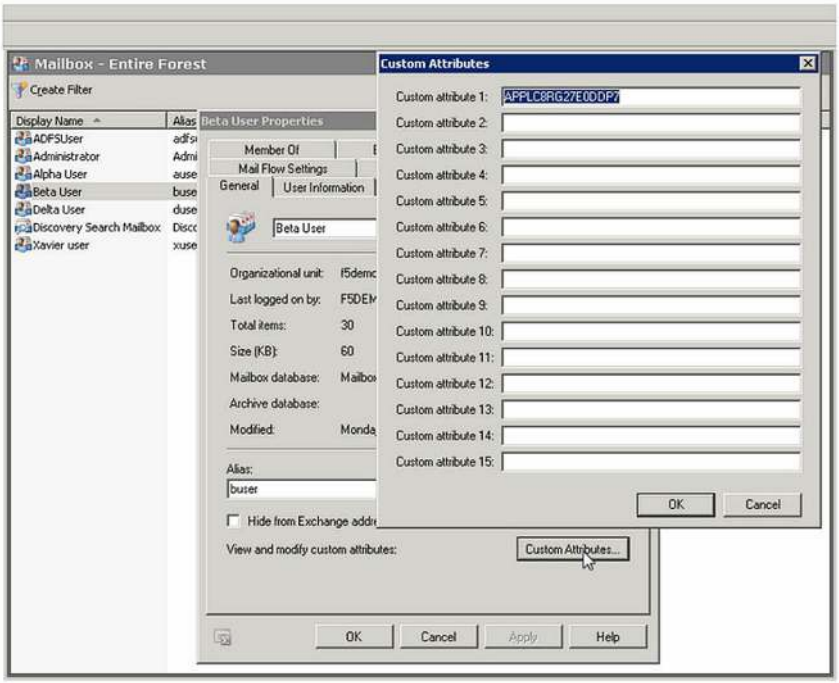
A note on Base64 encoding: The method and extent to which different mobile OS vendors (for example Apple iOS, Android, and Windows Phone) access ActiveSync may differ. Some devices, such as Windows Phone 7, use Base64 encoding, which must be decoded to identify the device ID. The iRule referenced above will determine if the HTTP query is encoded and decoded as needed.

Device Validation Method 2-"Individual User/Device Validation"

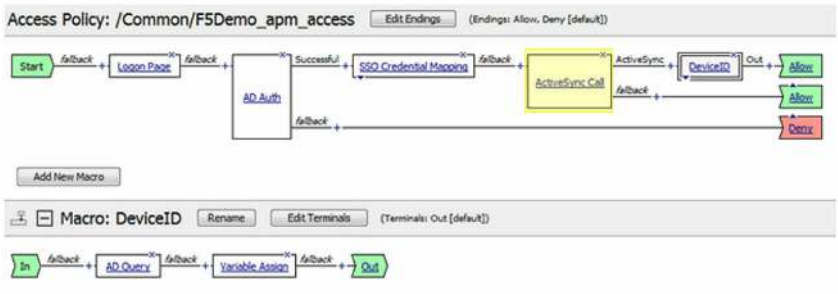
While not as straightforward as the previous example, the BIG-IP APM can be used to query user attributes in Active Directory. To facilitate user-to-device mapping for access security, the Exchange 2010 custom attributes can be utilized to store acceptable device IDs on a per-user basis. Subsequently, during the authentication process, BIG-IP APM can query these user attributes to enforce mobile device access.

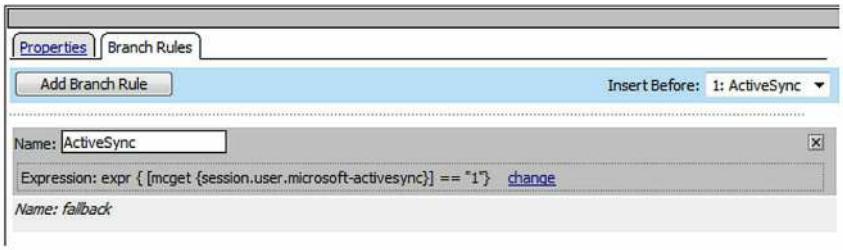
The following steps are performed on the existing Exchange 2010/BIG-IP deployment.

1. The custom attributes of the user mailbox are populated with acceptable device ID(s) for the specific user. For purposes of the following example, three devices may be assigned to a particular mailbox. Device IDs can be stored in "Custom attribute" 1, 2, and 3.

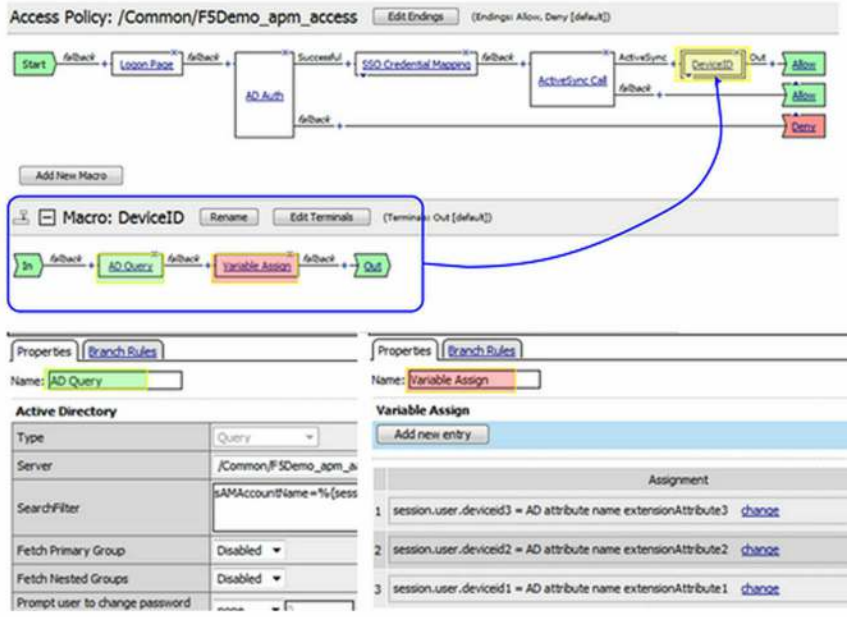


2. The existing BIG-IP APM access policy is modified. An empty element is configured to determine that the current session is ActiveSync.

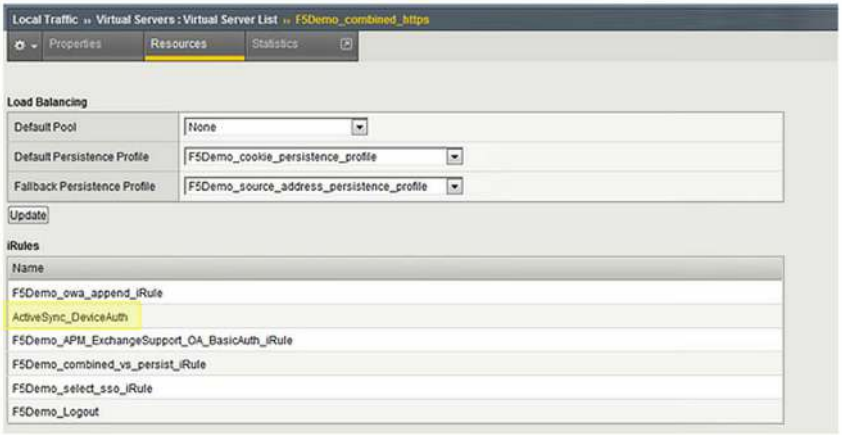




3. If the session is ActiveSync, a macro is utilized that performs an AD Query of the user's attributes, and captures the Device IDs as session variables.



4. An iRule is created and associated with the Exchange HTTPS virtual server. The iRule compares the device ID of the client connection (contained in the HTTP query) with the session variable(s). If the client device ID does not match one of the devices previously assigned to the user, the session is terminated and access is denied.

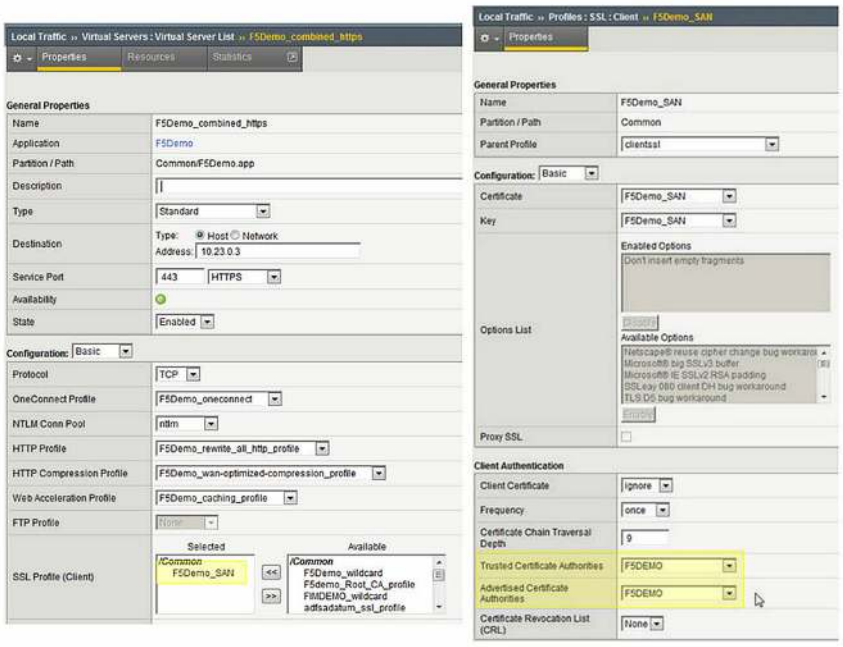


Device ID Validation-"Something You Have"

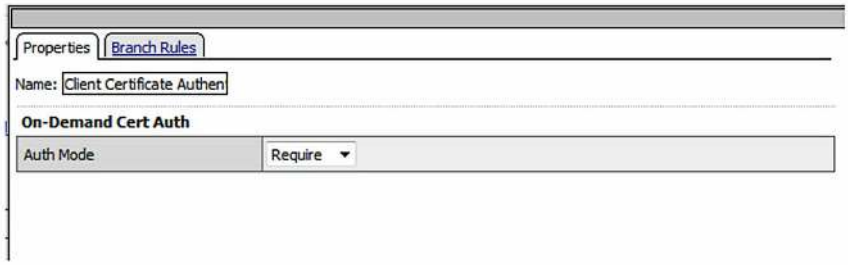
Perhaps one of the most challenging (and therefore seldom used) methods for securing mobile devices is the use of client-side certificates. In the native Exchange implementation, individual certificates must be created, stored in Active Directory, and distributed to devices. In addition, to enable this type of authentication to the CAS array, traffic arriving at the CAS server must be encrypted.

The BIG-IP system has the ability to re-encrypt traffic destined for the internal CAS server farm as well as acting as an SSL proxy for client-side certificate authentication. However, BIG-IP APM provides a means to require and validate client-side certificates while still offloading SSL processing from the CAS array. The following example demonstrates how to implement certificate-based validation along with username and password authentication.

1. The current Client SSL Profile is modified to include a trusted certificate authority (CA) with a CA certificate previously imported into the BIG-IP system. In this example, the trusted CA is "F5DEMO."



2. The existing BIG-IP APM access policy is modified. An "On-Demand Cert Auth" element is included. Once users have successfully authenticated with their credentials (username and password), BIG-IP APM will perform an SSL re-handshake and validate the client certificate against the trusted CA above. If validation fails, the session is terminated and access is denied.



Combining Authentication Methods-"Multifactor Authentication"

The previous examples have shown how the BIG-IP APM can authenticate mobile devices via usernames and passwords, device IDs, and client certificates. By combining these various methods into a single multifactor authentication solution, BIG-IP APM can provide secure and easily managed access to Exchange ActiveSync. The illustration below shows a typical authentication flow that combines the previously discussed methods, as well as a decision based upon the device type.

1. User is pre-authenticated to Active Directory with username and password.
2. If the session is utilizing ActiveSync, the device ID is compared against the user's attributes and a list of acceptable devices.
3. The device type is checked.
4. If the device type is an iPhone, a valid certificate is required.

BIG-IP Application Security Manager and ActiveSync

Implementing appropriate security controls for Exchange mobile device access does not end with authentication and authorization. To further enhance the organization's security posture, the traffic flow (including traffic from authenticated sources) needs to be effectively monitored and managed. Since most traffic from external sources flows through traditional Layer 3 firewalls into the corporate network, an application layer firewall or WAF should be implemented. WAFs, such as BIG-IP Application Security Manager (ASM), operate at the application layer, analyzing and acting upon HTTP payloads to further protect corporate assets.

The BIG-IP ASM module resides on the BIG-IP system and can be used to protect the Exchange environment against numerous threats, including but not limited to Layer 7 DoS and DDoS, SQL injection, and cross-site scripting.

The following section illustrates how to configure BIG-IP ASM modules for use with Exchange ActiveSync.

The ActiveSync Security Policy

BIG-IP ASM is an extremely robust application and as such can be rather time-consuming to deploy. Fortunately, F5 has developed a number of preconfigured templates to drastically reduce the time and effort required. This is the case with Exchange ActiveSync. The following steps are required to implement BIG-IP ASM for Exchange ActiveSync.

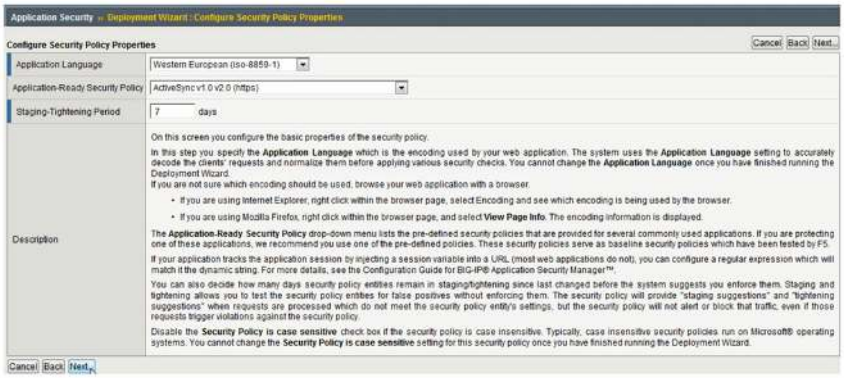
1. From the Application Security menu, select "Security Policies" and create a new policy.

2. Select "Existing Virtual Server" and "Next."

3. Select "HTTPS," the existing Exchange virtual server, and "Next."

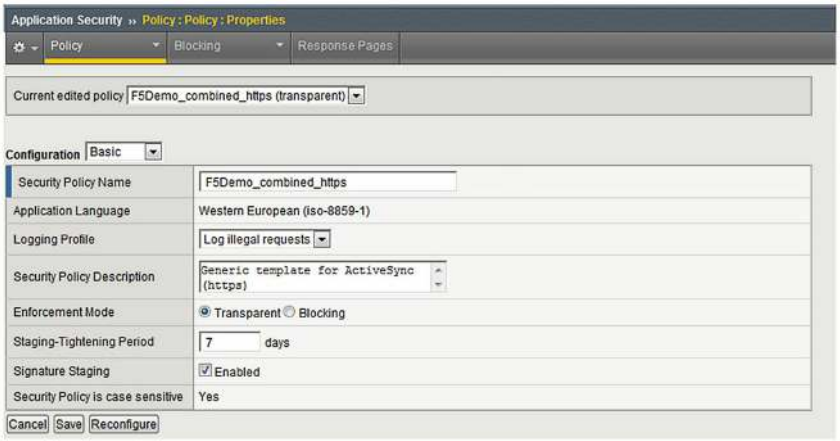
4. Select "Create a policy manually or use templates (advanced)," and "Next."

5. Select the policy language, which is typically Western European (iso-8859-1). Then select "ActiveSync v1.0 v2.0 (https)" and "Next."

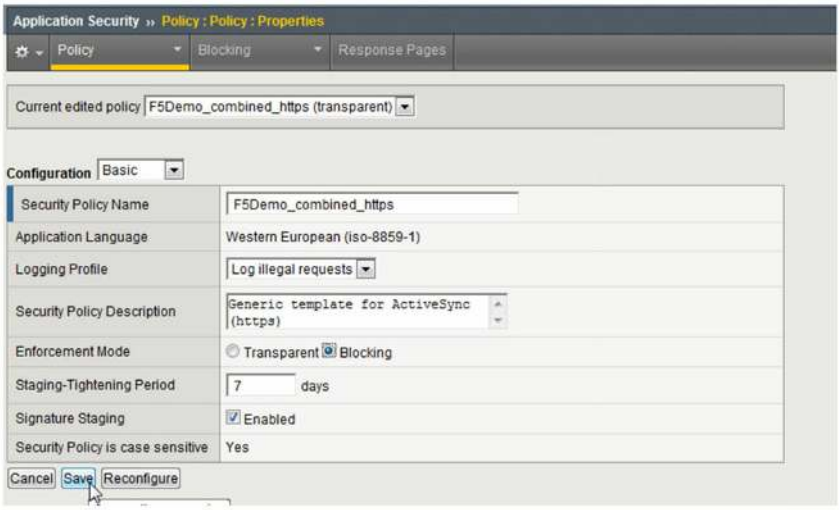


6. Select "Finish."

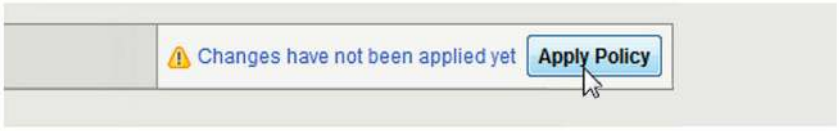
At this point the security policy has been created and applied to the Exchange virtual server. However, by design, the policy is implemented in a "Transparent" enforcement mode. The policy is monitoring traffic (both ingress and egress), but will not take any action. This enables the administrator to tune the policy without affecting users.

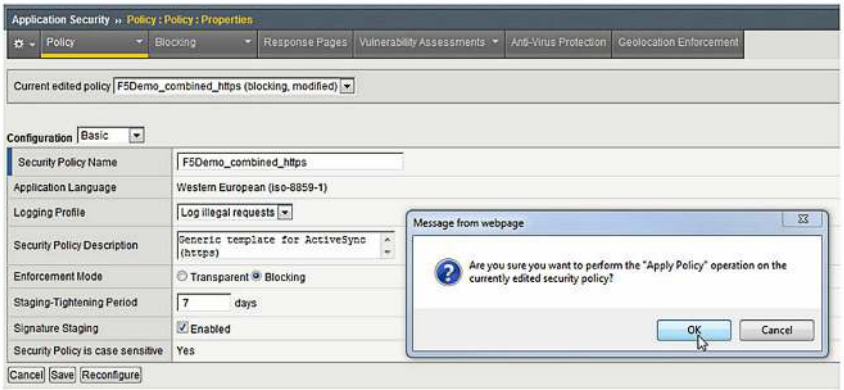


7. Once the policy has been tuned to an acceptable level, the policy should be switched from "Transparent" to "Blocking." Select the radial option of "Blocking," and "Save."



8. Select "Apply Policy" to commit the changes.





The BIG-IP ASM policy is now operating in "Blocking" mode.

Conclusion

Providing application access to an increasingly mobile workforce is quickly becoming a business requirement for many organizations. Ensuring these applications are both highly available and secure is absolutely critical. The BIG-IP Access Policy Manager (APM) and Application Security Manager (ASM) Application Delivery Controllers are designed to provide a highly available and secure deployment of business-critical applications. Specifically, superior Exchange mobile device security can be achieved by combining the multifactor authentication mechanisms of BIG-IP APM along with the robust Layer 7 firewall functionality of BIG-IP ASM.

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