AirWatch/F5 Solution for Enterprise Mobility

Comprehensive, Consolidated Enterprise Mobility Management and Application Access and Security

Contents

Introduction

F5 Networks provides strategic points of control throughout IT infrastructure, enabling organizations to scale, adapt, and align with their fast-changing business demands, and to drive business forward on a solid foundation of agility.

F5's BIG-IP® Access Policy Manager® (APM) is a flexible, high-performance access and security solution that unifies global access to applications and networks. BIG-IP APM converges and consolidates remote access, LAN access, web access, and wireless connections within a single management interface, and enables the development, application, administration, and management of access policies. BIG-IP APM delivers a simplified, central point of control at the perimeter and/or within the data center to manage access to applications and websites through the dynamic enforcement of context-aware policies.

When deployed together, AirWatch and F5 work in concert to help organizations successfully address Enterprise Mobility Management (EMM). The AirWatch/F5 solution enables organizations to define and implement comprehensive, granular bring-your-own-device (BYOD) policies. It also ensures the safety and security of corporate assets, while increasing employee satisfaction and productivity. The AirWatch/F5 solution consolidates and manages application access and security through F5 BIG-IP Access Policy Manager (APM), which integrates with the AirWatch solution to enable flexibility and granularity in the creation and enforcement of corporate access policies for mobile devices, as well as mobile and cloud-based applications. The advanced Visual Policy Editor (VPE) in BIG-IP APM allows for the simple creation of granular network and application access policies that integrate mobile device data and status gathered by AirWatch. F5 BIG-IP APM augments existing access gateways, delivering a robust, easily scalable mobile proxy environment that enables additional services including high-availability (HA), high-performance SSL, complex and legacy authN schema integration, and enhanced Microsoft ActiveSync support, to name a few.

The AirWatch/F5 solution is well-suited for mid- to large-sized enterprise organizations with on-premise or cloud-based deployments, and can support BYOD, corporate, or a hybrid approach to Enterprise Mobility Management. By addressing critical mobility and security use cases, the AirWatch/F5 solution is appropriate for all industries and vertical markets.

Use Case – Streamlined, Secure EMM/BYOx Deployment

The AirWatch/F5 APM solution simplifies the deployment and implementation of Enterprise Mobility Management (EMM) and Bring Your Own (BYOx). The joint solution delivers high-availability (HA). The solution leverages a security- and application-centric optimized and directory-integrated access infrastructure. The AirWatch/F5 APM solution leverages existing authentication (Active Directory, LDAP, WLAN, NAC, etc.) and existing critical application systems, simplifying and securing the speedy rollout of mobile apps. Together, AirWatch and F5 effectively manage email, web and native apps, and ERP access for all mobile devices, from any location, over any network. The comprehensive, simple policy development capabilities of BIG-IP APM – via its VPE – enhance and simplify the enforcement and management of how mobile users access network, cloud, and Web applications. This is accomplished via APM's granular, context-aware access control policies, which leverage the mobile device data and status, and mobile app and content information gathered by and through AirWatch. Coupled with the identity federation and single sign-on (SSO) capabilities available within F5 BIG-IP APM, the AirWatch/F5 APM solution streamlines and secures EMM/BYOx deployments for organizations while simplifying and protecting application access and data, regardless of where the application and its content are located. Additionally, F5 APM leverages the AirWatch Push API, allowing messages to be pushed from F5

APM to a user via the AirWatch client. For instance, the F5 APM can inform a user why they are unable to access an app, providing an enhanced user experience.

Use Case – Secure, Context-based Mobility

Through the simple and centralized creation and management of access and security policies in the F5 BIG-IP APM, the joint AirWatch/F5 APM solution enables secure, context-aware mobility for enterprise organizations. The joint solution allows for the customization of user access flows based on specific mobile configurations. By using the mobile device configuration and status, context-based authorization delivers organizations secure, policy-based control over a mobile device and its user's navigation. An access profile may be defined for all connections launched from the user's mobile device; or, multiple access profiles may be created for each connection or connection type, each with a different, unique access policy. By integrating the device data and status captured by AirWatch, the joint solution can deliver dynamic access authentication. And, if defined by policy, or if a mobile device did not comply with appropriate policies as defined, per application VPN tunnels can deliver access to specific applications, without opening risk to the entire network.

Use Case – Corporate Mobile Apps and Files Services Security

The AirWatch/F5 APM solution enables and delivers data protection at rest, between apps, and in transit via per app VPN and Layer 3 VPN. AirWatch policy invokes the secure mobile app VPN tunnel in F5 BIG-IP APM for Android or Windows, and uses native iOS per app VPN capabilities to achieve the same security posture. F5 BIG-IP APM ensures any mobile device seen by a corporate Wi-Fi network does not pose a security risk when it initially attempts to connect to the network by gathering available data about the device and end user in order to assess whether to allow or prevent network access based on that information. When AirWatch and BIG-IP APM are integrated, the solution automatically prompts any unmanaged device attempting to connect to the network to enroll in AirWatch in order to successfully connect. When the end user enrolls their device in order to gain access, the required agent and/or profiles are immediately pushed to the device and installed, initiating an additional layer of security.

	AirWatch	F5 BIG-IP APM
Mobile Device Management	✓	✗
Mobile App Management	✓	✗
Basic Mobile Gateway Services	✓	✓
Enhanced Gateway Services	✗	✓
Unified Access Policy Controls	✗	✓
SSL L3 & 4 VPN Client	✗	✓
Single-Sign-On & SAML	✓	✓
Authentication Proxy Services	✓	✓
Secure Web Gateway	✓	✓
Mobile/Web App Firewall	✗	✓

Figure 1: The features and functionality found in the standalone AirWatch and F5 BIG-IP APM offerings.

Process

The AirWatch/F5 enterprise mobility solution creates a secure method of access for anyone attempting to join a corporate network and access applications on a network, cloud or the Web. F5 BIG-IP APM is easily provisioned and configured by both AirWatch MDM for the F5 Layer 3 VPN client, as well as for per app VPN. Via a simple F5 iApp template on the F5 BIG-IP APM, integration is achieved between F5 APM and AirWatch for MDM to Access Controller API and directory integration.

When F5 BIG-IP APM receives a request for application access, it instantly queries and loads all applicable user and mobile device context from AirWatch as session variables. It then applies the appropriate policy enforcement for the application or asset requested. For example: Sally from HR requests access to an internal time keeping application. F5 BIG-IP APM determines Sally is a member of the HR Management Group within Active Directory, and her device is enrolled in AirWatch, is currently assessed by AirWatch as being compliant with device security policies, and has not been jail-broken. Therefore, Sally and her iOS device are granted access to all applications and resources she is authorized to access, including Microsoft Exchange, HRMS services, internal portal, SharePlus App access, and so on. However, if BIG-IP APM determines that Sally is outside of corporate Wi-Fi range, has a compromised device, has a jail-broken device, or learned from AirWatch that a device-level security setting has been removed, the policy verification at BIG-IP APM will deny her session access to ERP and Executive portal applications. The AirWatch/F5 APM solution can also recognize if Sally is off corporate Wi-Fi, and require a per app VPN policy session be established through F5 BIG-IP APM for her SharePlus mobile app to gain appropriate SharePoint access.

When on-boarding personal or corporate-issued personally enabled (COPE) devices to enable BYOD, once F5 BIG-IP APM receives an access request, and an AirWatch query indicates that the user's device is currently unmanaged, the AirWatch/F5 APM solution redirects the device to the previously configured enrollment URL. Once enrolled, the device automatically receives the above session treatment.

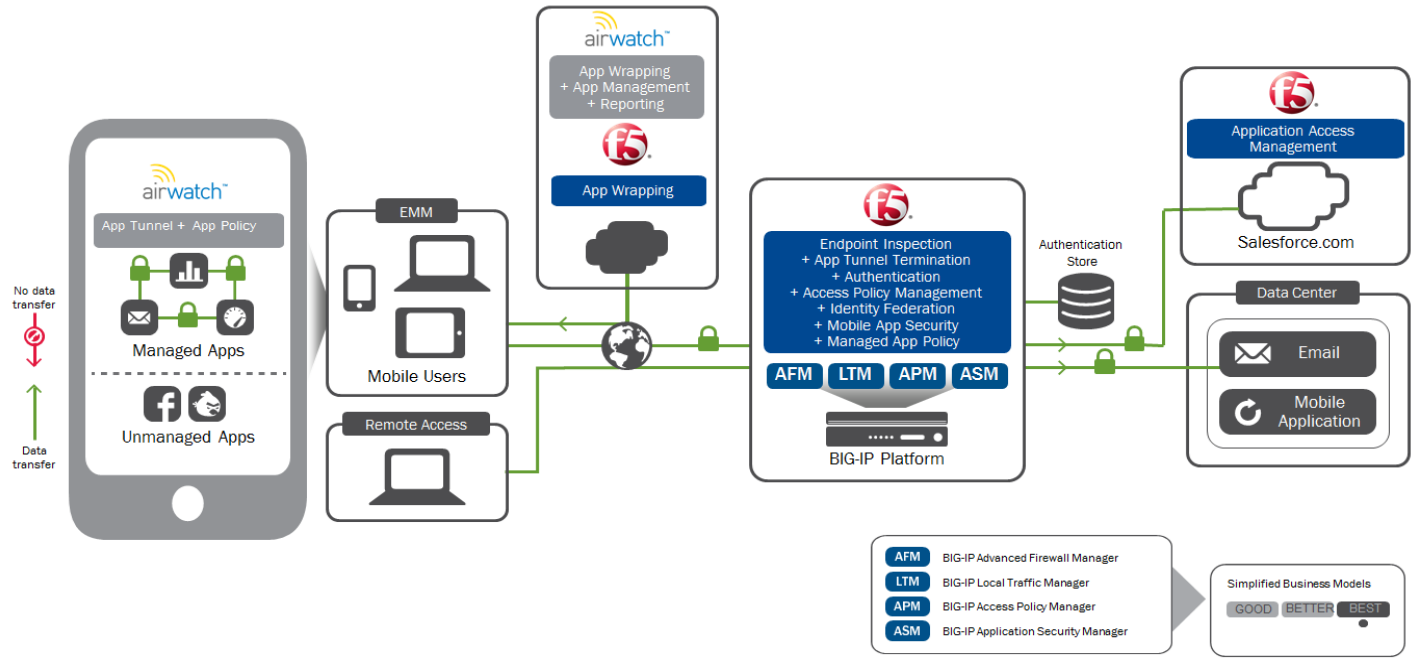

Figure 2: AirWatch and F5 Secure Enterprise Mobility

What Are the Benefits of an AirWatch/F5 Solution?

Among the many benefits an organization can enjoy with an integrated AirWatch/F5 BIG-IP APM solution are:

- Simplified deployment for Enterprise Mobility Management (EMM) and BYOx (Bring Your Own Device, Bring Your Own Apps, etc.)
- Centralized control and management for all security and access policies to networks and applications, regardless if the location of the apps (network, cloud, or Web)
- Reduced total cost of ownership (TCO) and deployment time for mobile app rollouts
- The ability to use and maintain existing apps, infrastructure and processes, once again saving deployment time and expense
- A rich, layered and enhanced user experience
- A robust, highly-scalable mobile proxy environment that enables services including high-availability (HA), high-performance SSL, complex and legacy authN schema integration, and enhanced Microsoft ActiveSync support
- Comprehensive, layered, end-to-end security, from the mobile device through to applications

Who Can Benefit from the AirWatch/F5 Solution?

While the AirWatch/F5 solution is appropriate for all industries and vertical markets to address critical mobility and security use cases, there are specific use cases and scenarios in which the integrated AirWatch/F5 solution is best suited, including:

Enterprises Desiring Agent/Profile Mobile Device Management (MDM)

If a company desires on-device Mobile Device Management (MDM) security controls, but currently relies only on outward looking NAC appliances to manage automated network access, the potential for sensitive data loss remains high. If sensitive corporate content is accessed and retrieved from inside the network by a managed, yet unsecured device, it can be compromised or distributed without warning. Installing AirWatch MDM and applying restrictions using profiles and compliance policies, leveraging F5 BIG-IP APM on managed devices dramatically increases network and application security and lowers the potential for sensitive data loss and malicious attacks on networks and applications.

Enterprises Desiring Context-based Access Control

A properly configured agent/profile based MDM strategy such as AirWatch is extremely effective at restricting managed devices and securing networks and applications against unauthorized mobile access. But, implementing a comprehensive role-/policy-based and context-aware access control solution, such as F5 BIG-IP APM, in conjunction with AirWatch, adds a necessary layer of security and automates tasks associated with determining network and/or application access to a specific mobile device and/or user. A comprehensive network and application access control solution like F5 APM can address a use case where previously unseen, unmanaged, and unauthorized mobile devices without MDM controls in place, such as personal mobile devices, may be vetted based on available context prior to being granted network or application access.

Enterprises Desiring Per App VPN or Developing Apps with Secure Transport Methods

In this mobile world, it is imperative communications to and from mobile apps and enterprise networks and clouds are secure. One of the most effective ways to ensure security for data-in-transit is via a virtual private network (VPN). While Layer 3 VPNs can ensure mobile device connectivity, they also ensure that any personal information accessed or downloaded by a mobile user, especially in a BYOD environment, also flows through the corporate network. This raises serious privacy and legal issues for an organization. A per app VPN ensures only specific mobile apps and their data remain secure and protected, and only data relevant to the app is sent to the corporate network. With the per app VPN capabilities of the AirWatch/F5 BIG-IP APM solution, enterprise organizations can be sure only authenticated, authorized mobile users may access and send data from approved mobile apps, or from a mobile container, to the organization.

Enterprises Desiring Additional Access Scalability

Enterprises that require added scalability and robustness in addition to superior enterprise mobility management capabilities need the AirWatch/F5 solution. AirWatch's market-leading ability and reputation to address Enterprise Mobility Management (EMM) is well known and highly regarded. When coupled with the highly scalable, robust security and access capabilities of F5 APM, the AirWatch/F5 solution delivers a comprehensive, powerful end-to-end mobile access, security, and management solution.

Requirements

To take advantage of the enhanced mobile device security provided by the AirWatch-F5 integrated solution, ensure you have the following resources available:

- AirWatch version 6.2 or higher.
- F5 BIG-IP APM version 11.5 or higher, with AirWatch API Integration activated.
- F5 Edge Client 2.0.1 for Layer 3 and per app VPN.

To ensure an environment is compatible and to get started with the AirWatch/F5 integration, contact your F5 Networks representative and AirWatch Support.