Secure Mobile Access to Corporate Applications

The way corporations operate around mobile devices is currently shifting—employees are starting to use their own devices for business purposes, rather than company-owned devices. With no direct control of the endpoints, IT departments have generally had to prohibit this or risk insecure access inside the firewall. But as more mobile devices appear on the corporate network, mobile device management has become a key IT initiative.

White Paper
by Peter Silva

Introduction

Mobile devices have become computers in their own right, with a huge array of applications, significant processing capacity, and the ability to handle high bandwidth connections. They are the primary communications device for many, for both personal and business purposes.

Many IT executives are planning to make internal business applications available to employees from their smartphones or mobile devices. This goes beyond email and includes CRM applications, ERP systems, and even proprietary in-house applications. Because personal mobile devices are so prevalent, many organizations are moving from corporate ownership of devices to allowing employees to use their own devices for business purposes. Some companies view this as a cost-saving measure, but identifying these personal devices as legitimate endpoints is still a challenge, especially when it comes to security and compliance. In addition to smartphones, tablet devices like the Apple iPad and a whole new array of computing devices are requesting access to corporate resources.

The 2007 launch of the iPhone and the 2008 release of Android changed the way people perceive and use mobile devices. These devices aren't just for the tech-savvy —parents, celebrities, retailers, and everyone in between love to use their smartphones for personal purposes and for work. The first iPhone was missing a few important features that would have made it a business-capable device. But as new generations hit the market and iOS matured, the iPhone became a viable business device; plus, more and more consumers are choosing Android devices. This, combined with the trending 'bring-your-own-device' model in business, means more secure apps and ways to access content are a necessity.

Getting Down to Business

IT infrastructure and helpdesk staff have been inundated with requests to support both managed and unmanaged Apple iPads and iPhones and Android devices in the corporate environment. With no direct control of the endpoints, IT has had to turn these requests away to avoid risking insecure access inside the firewall. Mobile devices, personal or not, have always presented a challenge to IT. Provisioning a mobile device and determining which applications and services are allowed/enabled can be daunting. Despite impressive computing power, a mobile device is not a traditional laptop or desktop, and functionality can differ greatly. Even mobile device capabilities vary based on make, model, and OS. Many IT organizations have solved some of their security and compliance issues and now allow personal home computers to access business resources; providing access to personal mobile devices is the next piece of the puzzle.

Technologies like SSL VPN have made it easier for organizations to inspect the host, know its security posture, and allow a certain level of access based on those checks. With mobile platforms, it can be hard to determine if the latest patches are up to date, if it is free of malware, if it is free of otherwise unauthorized programs, and if it abides by the corporate access policy. Different security policies may apply to mobile computing devices than to traditional devices. Can the corporation disable the personal device if it is compromised and contains sensitive information?

If VPN access is allowed, IT must ensure the authentication and authorization mechanisms are configured properly. There may also be issues with usage tracking, license compliance, and session persistence as users roam among various mobile networks. Many companies also use portals, proxies, and IDS/IPS to control access. Even GPS data could pose a risk to an organization, especially for government and military deployments. Increased network traffic also needs to be monitored. As more employee-owned mobile devices appear on the corporate network, IT departments must make mobile device management a key initiative.

iOS and Android Devices with the BIG-IP System

Business users are increasingly looking to take advantage of both Apple iOS and Android devices in the corporate environment, and accordingly, IT organizations are looking for ways to allow access without compromising security or losing endpoint control. Many IT departments that have been slow to accept personal mobile devices are now looking for a remote access solution to balance the need for mobile access and user productivity with the ability to keep corporate resources secure.

F5 BIG-IP Edge Apps

F5 created two apps for Apple iOS and Android mobile devices: F5® BIG-IP® Edge Portal® and BIG-IP® Edge Client®. The iOS versions of BIG-IP Edge Client and BIG-IP Edge Portal are available at the Apple App Store, and the Android versions are available at Google Android Marketplace (North America) and the Samsung App Store (international). There is also a version of the client for all Android 4.0 (Ice Cream Sandwich) devices.

BIG-IP Edge Portal

The BIG-IP Edge Portal app for iOS and Android devices streamlines secure mobile access to corporate web applications that reside behind BIG-IP® Access Policy Manager™ (APM) and BIG-IP Edge Gateway.™ With the BIG-IP Edge Portal app, users can access internal web pages and web applications securely.

Mobile Workforce Increasing

According to IDC, the worldwide mobile worker population is set to increase from 919.4 million in 2008, accounting for 29 percent of the worldwide workforce, to 1.19 billion in 2013, accounting for 34.9 percent of the workforce.1

BIG-IP Edge Portal, in combination with customers' existing BIG-IP Edge Gateway and BIG-IP APM or FirePass SSL VPN deployments, provides portal access to internal web applications such as intranet sites, wikis, and Microsoft SharePoint. This portal access provides a launch pad that IT administrators can use to allow mobile access to specific web resources, but without risking full network access connections from unmanaged, unknown devices. Mobile users can sync their email, calendar, and contacts directly to the corporate Microsoft Exchange Server via the ActiveSync protocol. This solution also enables corporate IT to grant secure mobile access to web-based resources.

IT administrators can also create and manage layer 7 access control lists (ACLs) to limit access to certain resources. For instance, administrators can specifically create white lists or blacklists of sites that users can access. Administrators can even specify a particular path within a web application, like /contractors or /partners. Based on the device check and the authenticated user group, a user on that device would only be able to navigate to those assigned resource paths. Even if a contractor happens to guess the partner path, if he or she tries to navigate to it, access is denied. Administrators can also configure BIG-IP Edge Gateway to provide and push policies to the client, such as allowing a user to save credentials on the device.

If the system is configured to require a client certificate, iOS users can add BIG-IP Edge Client from a web location or through iTunes. The Android version supports certificates that have been copied to the SD memory on the device, or that are available externally via a URL—users simply import or download the certificate when prompted. Users of both platforms can add bookmarks to save sites they want to connect to again and specify a keyword to open a page. For example, users can specify the keyword "intra" to go to the company's intranet page. If users specify a keyword when they bookmark a site, they can later launch that bookmarked site by typing the keyword in the BIG-IP Edge Portal address bar.

The BIG-IP Edge Portal app allows users to access internal web applications securely and offers the following features:

- User name/password authentication
- Client certificate support
- Saving credentials and sessions (iOS)
- SSO capability with BIG-IP APM for various corporate web applications
- Saving local bookmarks and favorites
- Accessing bookmarks with keywords
- Display of all file types supported by native Mobile Safari and native Android browser

figure 1: BIG-IP Edge Portal on Apple iPhone

BIG-IP Edge Client

Assuming a smartphone is a trusted device and/or that network access from a mobile device is allowed, then the BIG-IP Edge Client app offers all the BIG-IP Edge Portal features listed above, plus the ability to create an encrypted, optimized SSL VPN tunnel to the corporate network. BIG-IP Edge Client offers a complete network access connection to corporate resources from an iOS or Android device — a comprehensive VPN solution for both iOS and Android. With full VPN access, mobile users can run supported applications such as RDP, SSH, Citrix, VMware View, VoIP/SIP, and other enterprise applications.

BIG-IP Edge Client and Edge Portal work in tandem with BIG-IP Edge Gateway and FirePass® to drive managed access to corporate resources and applications, and to centralize application access control for mobile users. Enabling access to corporate resources is key to user productivity, which is central to F5's dynamic services model that delivers on-demand IT.

For Apple iOS devices, a VPN connection can be user-initiated, either explicitly through BIG-IP Edge Client or implicitly through iOS's VPN-On-Demand functionality. For example, administrators can configure a connection to be automatically triggered whenever a certain domain or hostname pattern is matched. VPN-On-Demand configuration is allowed if the client certificate authentication type is used. A user name and password can be used along with the client certificate, but they are optional. No user intervention is necessary for connections initiated by VPN-On-Demand (for example, a connection will fail if a password is not supplied in the configuration but is needed for authentication). For Android devices, BIG-IP Edge Client is supported on version 2.2 and later (most Android devices are supported).

Figure 2: BIG-IP Edge Client on Android

The BIG-IP Edge Gateway controller optimizes and accelerates client traffic between gateways and data centers. With the addition of the BIG-IP Edge Client app, that optimization is extended to the mobile device, improving mobile user performance with accelerated client access. BIG-IP Edge Client, when used in tandem with BIG-IP Edge Gateway, provides secure and optimized application access to iOS and Android devices. If a user is on a high-latency mobile network and needs to download a file from the corporate infrastructure, the unique, adaptable compression algorithms ensure the file arrives quickly. Now users experience secure LAN-like performance, even when they are mobile.

BIG-IP Edge Client, like the BIG-IP Edge Portal app, also adheres to the ACLs limiting access to certain resources, as well as access polices defined by the administrator such as credential caching. For BIG-IP Edge Client, administrators can create both layer 7 and layer 3/4 ACLs. Even if the iPhone is a trusted device and IT has allowed network access from that device, IT might still want to restrict those users to certain subnets within the infrastructure based on organization, role, or other criteria. If there are compliance requirements for corporate access and when user access and application logging is required, BIG-IP APM and BIG-IP Edge Gateway provide detailed logging and accounting, so IT can meet regulatory requirements even when applications are accessed from unmanaged devices not owned by IT.

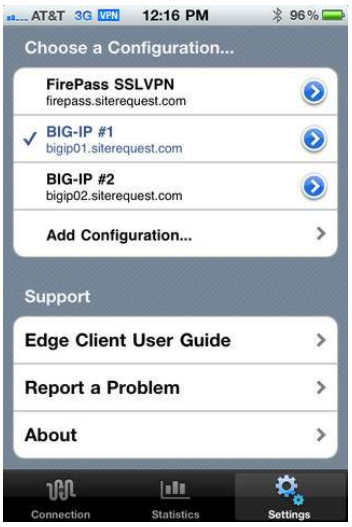

Figure 3: BIG-IP Edge Client configuration page on iOS and Android devices

Administrators can create and manage access control policies using F5's unique Visual Policy Editor (VPE). With the advanced VPE, administrators can easily create secure, granular access control policies on an individual or group basis. The flowchart-like GUI gives administrators point-and-click control to seamlessly add iOS or Android devices to an existing system or to create a new macro policy exclusively for both devices.

BIG-IP Edge Client offers additional features such as Smart Reconnect, which enhances mobility when there are network outages, when users roam from one network to another (like going from a mobile to WiFi connection), or when a device comes out of hibernate/standby mode. Split tunneling mode is also supported, which allows users to access the Internet and internal resources simultaneously.

Users can easily add any of their corporate BIG-IP access controllers (BIG-IP APM, BIG-IP Edge Gateway) or FirePass SSL VPN as a secure gateway on their mobile device. To minimize helpdesk calls, adding user credentials is as easy as typing the user name and password, and then clicking Save and Done.

Figure 4: BIG-IP Edge Client on Apple iPad

Conclusion

The BIG-IP Edge Portal app for Android and iOS mobile devices provides simple, streamlined access to web applications that reside behind BIG-IP APM, without requiring full VPN access, to simplify login for users and provide a new layer of control for administrators. Using BIG-IP Edge Portal, users can access internal web pages and web applications securely, and administrators can seamlessly add iOS and Android mobile device management to their already existing BIG-IP infrastructure.

The BIG-IP Edge Client app provides not only full SSL VPN access from iOS and Android devices, but also accelerated application performance when it's used with BIG-IP Edge Gateway. Administrators can maintain granular control with F5's Visual Policy Editor, and users experience fast downloads and quick web access with the integrated optimization and acceleration technologies built into BIG-IP Edge Gateway. IT no longer has to provision and manage multiple units to ensure their corporate applications are available, fast, and secure to iOS and Android users.

[1]Worldwide Mobile Worker Population 2009–2013 Forecast. IDC Doc #221309, December 2009.

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

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS01-00082 0113