Secure iPhone Access to Corporate Web 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 changed the way people perceive and use mobile devices. The iPhone isn't just for the tech-savvy—parents, celebrities, retailers, and everyone in between love to use the iPhone 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. iOS 4 is compatible with Microsoft Exchange ActiveSync accounts and Exchange Server, so users can configure multiple email accounts for secure access on their iPhones. Business apps like Documents To Go enable iPhone users to not only view Microsoft Word and Excel documents, but to create and edit them as well. Companies like Salesforce, SAP, and Oracle have released general business apps and business intelligence and HR apps.

Getting Down to Business

IT infrastructure and helpdesk staff have been inundated with requests to support both managed and unmanaged Apple iPads and iPhones 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 capabilities among the various mobile devices differ 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?

Mobile Worforce Increasing

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

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.

iPhone and BIG-IP

Business users are increasingly looking to take advantage of Apple iOS 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 the iPhone 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.

The F5 BIG-IP Edge Apps

F5 has created two apps for the iPhone and iPad: F5 BIG-IP Edge Portal and BIG-IP Edge Client.

The BIG-IP Edge Portal

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

BIG-IP Edge Portal, in combination with customers' existing BIG-IP Edge Gateway and BIG-IP APM or FirePass SSL VPN solutions, provides portal access to internal web applications such as intranet sites, wikis, and Microsoft SharePoint. This portal access provides a launchpad that IT administrators can use to allow mobile access to specific web resources, but without risking full network access connections from unmanaged, unknown devices. iPhone users can sync their email, calendar, and contacts directly to the corporate Microsoft Exchange Server via FirePass and the ActiveSync protocol. This solution also enables corporate IT to grant secure iPhone and iPad 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, 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, users can add it from a web location or through iTunes. Users 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 bookmark 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
- SSO capability with BIG-IP APM for various corporate web applications
- Saving local bookmarks and favorites
- Accessing bookmarks with keywords
- Embedded web viewer
- Display of all file types supported by native Mobile Safari

The F5 BIG-IP Edge Client

Assuming an iPhone is a trusted device and/or network access from an iPhone/iPad 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 device—a comprehensive VPN solution for both the iPhone and iPad. With full VPN access, iPhone/iPad users can run 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 SSL VPN solutions 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.

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 host name 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).

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 iOS 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 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.

Like the BIG-IP Edge Portal app, BIG-IP Edge Client also adheres to the ACLs limiting access to certain resources, as well as access polices defined by the administrator like 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.

Policy and access management are created and controlled by F5's unique Visual Policy Editor (VPE). Using 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 iPhone and iPad devices to an existing system or to create a new macro policy exclusively for iOS devices.

Figure 1: BIG-IP Edge Portal on Apple iPhone

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

Users can easily add any of their corporate BIG-IP access controllers (BIG-IP APM, Edge Gateway) or FirePass SSL VPN as a secure gateway on their iOS device. A user simply starts BIG-IP Edge Client and in the Server field, types the IP address or fully qualified domain name of a FirePass SSL VPN controller, a BIG-IP APM, or BIG-IP Edge Gateway. They can also type a name for this server in the Description field to make it easier to locate. To minimize helpdesk calls, adding user credentials is as easy as typing the user name and password, and then clicking Save and Done.

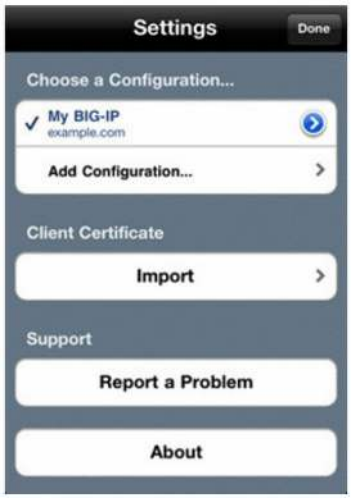

Figure 2: BIG-IP Edge Portal configuration page on Apple iPhone

Conclusion

The BIG-IP Edge Portal app for iOS 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 iPhone and iPad mobile device management to their already existing BIG-IP infrastructure.

The BIG-IP Edge Client app provides not only full SSL VPN access from iPhones and iPads, 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 iPhone and iPad users.

Figure 3: BIG-IP Edge Client on Apple iPad

[1] http://www.idc.com/research/viewdocsynopsis.jsp?containerId=221309§ionId=null&elementId=null&pageType=SYNOPSIS

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