White Paper

Unified Enterprise Mobility with the F5 BIG-IP System

Enterprises need to unify mobility with their existing corporate access and security policies. Combining F5 BIG-IP Access Policy Manager (APM) with mobile device management (MDM) solutions, the latest mobile OS controls from Apple, Android, and virtual desktops, reduces enterprise mobility deployment costs and minimizes complexity while bringing unparalleled scale, security, and control.

by Lori MacVittie
Senior Technical Marketing Manager

Contents

Introduction

If consumers are overwhelmed by the dizzying array of choices in the mobile device market, IT is exhausted by it. From ensuring that organizations can safeguard against rogue attacks, to troubleshooting issues before they occur, to users demanding access to information from anywhere, IT organizations are under intense pressure to support mobile devices in the same way as traditional enterprise computing devices.

Adding to this pressure is the demand for IT to support multiple devices for each user spread across multiple device types. Organizational attempts to "standardize" on a single operating system or device type are met with disdain from users and are ultimately unenforceable as employees are quickly adopting the bring-your-own-device model. This necessitates multiple mobile device management (MDM) solutions—technologies that enable IT to apply policies to mobile devices in the same way they would apply policies to corporate desktop devices. However each MDM solution comes with its own infrastructure and administrative overhead, increasing both OpEx and complexity, and MDM doesn't solve the difficulty of applying optimization, scale, and security policies during application delivery for different users on different devices.

Enterprises need a simpler, more comprehensive solution to answer the challenge of mobility and device creep and sprawl. In response to this, IT organizations are demanding simpler deployments, end-to-end security, and effective and broad control and management.

Security First

One of IT's biggest challenges is to secure corporate resources against a variety of potential risks, including theft, unauthorized access, and infection stemming from the spread of malware. While infection is not nearly as prevalent on mobile platforms as it is on the desktop, there is a growing concerted effort by miscreants to exploit the exploding popularity of mobile devices both to generally access web-based applications, and to interact with corporate resources.

This makes IT's primary challenge to enforce access control on corporate networks and resources, including the very difficult task of verifying compliance with various regulations such as OFAC, PCI, HIPAA, and FIPS. These regulations often mandate that certain policies be met not only internally, but on end points as well, which requires an end-to-end, deployable solution for any device. In terms of managing

security and compliance, traditional desktops have long been a problem area for IT organizations. However new, easy-to-manage desktop solutions such as virtual desktop infrastructure (VDI) aim to help solve both fixed and mobile desktop end points. Although VDI does help IT maintain control over the desktop, it simply extends the reach of the desktop through a laundry list of mobile device support. It also expands IT management issues to include securing access from devices to remote desktops; securely authenticating and managing users from any device; and even adding new components such as separate authentication and authorization elements for VDI that don't integrate with the rest of the infrastructure.

Managing a Sea of Devices

Given the variety in the mobile platform market today, this lack of integration can be problematic. Historically, users were satisfied with an IT-provided desktop or laptop for work functions, but the consumerization of IT has drastically changed this model. Users are blurring the lines between devices solely used for work and personal devices, and are forcing IT to create solutions that allow them to use their iPads at home for gaming, checking work email, and accessing their corporate desktop all at the same time. The most obvious solution is to restrict the devices allowed, but this approach is rarely acceptable to users.

A second but just as problematic approach is to deploy multiple MDM solutions on each device. This introduces additional complexity and integration challenges, as IT must then cobble together a set of operationally disjointed solutions to address device scale, secure remote access, access management, acceleration and optimization, secure transport, and more across many different and unique devices. Such a mish-mash of solutions—especially in light of the devices and servers required to support solutions like VDI, Exchange Active Sync, and integration with other enterprise-class systems—results in a fragile and very costly architecture. As new devices enter the organization, the complexity increases as does the cost to maintain the overall solution set.

Further adding to this complexity is increasing pressure to support IPv6. Service providers can only bear the strain of maintaining IPv4 support as a means to not "break the Internet" for so long before IPv6 becomes, as has been predicted, the Y2K threat for the network. The ability to deliver applications to mobile devices will soon require support for IPv6, but will not yet obviate the need to support IPv4. A dual stack approach will be required during the transition period, again putting delivery infrastructure front and center in the battle to deploy and support applications for mobile devices.

A disconnected multi-device approach is unsustainable in terms of OpEx, reliability, and scalability. This approach is reminiscent of the early days of the Internet when differences in browser capabilities resulted in excessive client-scripting or outright non-support as a means to address users who chose to use non-standard browsers based on personal preference or because they had unique needs. This situation has always left users frustrated and IT overwhelmed. A new approach, one that is less operationally disconnected and more able to adapt as new devices are introduced, is required to successfully meet this challenge now and in the future.

Unified Enterprise Mobility

There is no question that users are going to continue to access IT resources on new devices that challenge the standard desktop model—but IT can begin managing all users with BIG-IP® Access Policy Manager™ (APM). BIG-IP APM is a unified application mobility security and management module that enables organizations to leverage strategic points of control to deploy scalable, adaptable policies across the IT infrastructure and into the public cloud.

As part of F5's Application Delivery Networking (ADN) solutions, BIG-IP APM helps integrate disparate technologies such as MDM, VPN access, and VDI to provide greater control of the entire infrastructure. This improves application delivery and data management while also meeting the needs of users for seamless, secure, and fast access to applications from corporate desktops as well as mobile devices.

Simplified Mobile Architecture

BIG-IP APM integrates with multiple VDI and MDM solutions to consolidate and unify disparate mobile technologies. This integration and collaboration eliminates the need for multiple, disconnected solutions to address user management and operational risk within the data center. Security, performance, and availability services are all equally manageable, and ultimately more scalable, when deployed on the BIG-IP platform. BIG-IP APM provides greater control of mobile infrastructure, which enables IT to enforce security policies (including end point inspection) that can be as broad or granular as necessary to meet business and operational security needs.

Working together, BIG-IP® Local Traffic Manager™ (LTM) and BIG-IP APM help IT scale infrastructure to support new devices on the front end and scale applications

on the back end. As new devices come into the enterprise, BIG-IP APM authenticates each device individually as it accesses corporate resources, and then passes the user onto BIG-IP LTM for managing application delivery, specifically for the particular device. Together, BIG-IP LTM and BIG-IP APM can elastically scale up and out across BIG-IP hardware and software platforms such as VIPRION—a chassis-based BIG-IP hardware platform—and across multiple virtual instances of BIG-IP LTM and BIG-IP APM with virtual Clustered Multiprocessing (vCMP). Scaling VDI services in the data center, for example, have long been a challenge for IT when users are accessing single desktop images from multiple devices. BIG-IP LTM scales the VDI infrastructure up and out so it can grow as mobile device demand increases.

Simplification through consolidation dramatically reduces the cost and complexity of designing and deploying access and security policies, while achieving higher performance and resiliency for services—two paramount concerns with a disconnected, mobile workforce.

End-to-End Control

A unified solution with BIG-IP APM further provides critical security data points through its ability to monitor and log events to enterprise compliance systems. Verifying regulatory compliance with HIPAA, FIPS, PCI, and OFAC is only possible with a solution that has end-to-end controls in place, from the mobile device OS—and through the desktop in the case of VDI—to the application being accessed. BIG-IP APM provides those controls for the leading desktop, virtualization, mobile OS, and handset vendors including Apple, Android, Microsoft, VMware, Citrix, and others.

End-to-end control also enables organizations to deliver valuable services such as acceleration, split tunneling for secure web gateway, single sign-on, and VPN on-demand. These services enhance application performance and improve productivity in addition to providing a firm foundation of security services.

BIG-IP APM offers real-time control over mobile devices through its integration with MDM solutions. Organizations can leverage the advanced Visual Policy Editor (VPE) in BIG-IP APM to create, deploy, and manage device policies, as well as the F5 iRules® scripting language, to interact in real time with MDM solutions to verify mobile device registrations. Using F5 iControl®, an open, standards-based API, real-time publications from MDM solutions can be received and acted upon, ensuring that administrators can revoke user access automatically and immediately as policies or access rights change.

Flexibility to support a variety of authentication mechanisms is the foundation for architectural solutions that address the challenge of integrating cloud-based resources with traditional enterprise applications, whether delivered via VDI or natively to mobile clients. For example, BIG-IP APM can broker authentication between users and cloud-based resources such as Salesforce.com, regardless of client platform.

Support for IPv6

Support for IPv6 is a key consideration when designing a scalable, mobile-supporting infrastructure because of where access and security solutions are within the data center network. These solutions typically reside at the perimeter, interfacing directly with clients and mediating for corporate resources such as virtual desktops and applications. Because of this location, they must simultaneously support IPv4 and IPv6 if they are to scale to accommodate the growing mobile user base. The BIG-IP platform is fully IPv6-compliant, and can support all three primary IPv6 transition architectures: dual stack, tunneling, and translation.

This comprehensive support for IPv6 in the core BIG-IP platform is inherited automatically by BIG-IP APM, making it the first secure remote access solution to fully support IPv6. This enables organizations to transition strategically to IPv6 while maintaining support for IPv4 applications and clients, including mobile devices. Using client applications for desktops, laptops, mobile phones, and tablets, BIG-IP APM supports a mixed IPv4 and IPv6 environment from the data center all the way down to the device, so IT can manage IPv4 and IPv6 devices together in one central location. IPv6 support for new devices allows IT to future-proof for network growth, support new operating systems like Windows 8, and continue to allow mobile users to bring any device to the enterprise.

Conclusion

As enterprise employees use more personal technology solutions for work purposes—such as bringing their own laptops for IT-supported VDI images and demanding support for different mobile platforms for app-based access and connectivity—IT will need to support them while scaling the application infrastructure and continuing to provide the same level of security and control traditionally applied to the standard corporate desktop. Standard desktop management technologies and policies aren't enough in a multi-device mobile world: IT must look at unifying security and management across the entire user experience as users move from device to device, while also being able to scale for massive device adoption.

Working in parity with VDI, MDM, and user access policies throughout the enterprise, BIG-IP APM provides a true consolidated and unified access management and optimization solution for users in any location and on any device. By focusing on user access and application delivery, the BIG-IP system becomes a single policy

management and scale solution with which IT organizations can manage remote users at one location as part of the entire application delivery lifecycle; in this way, it supports all users as they move around and beyond the enterprise.

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

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com