BETTER BYOD WITH PULSE SECURE AND MDM PARTNERS

Integrated VPN, Access Control, and Mobile Device Management Solutions Deliver Network Security and BYOD Productivity

Challenge

When organizations allow their employees and guests to use any device to access the network, they gain in productivity and user satisfaction, but this freedom comes with significant security risks.

Solution

Together with its partners, Pulse Secure has overcome these challenges by integrating Pulse Secure's Connect Secure and Policy Secure gateway solutions with MDM solutions such as MobileIron and Airwatch—bringing the productivity and flexibility of BYOD, without compromising security or increasing management complexity.

Benefits

- Remote connectivity
- Seamless onboarding and admission control
- Zero-touch application configuration
- Flexibility with security

Over the last decade, network access control has established itself as the preferred approach to selectively connecting devices to private networks. NAC, which ensures that only authorized users and devices gain network access, also makes sure that each user and device can only access what's allowed. The more information NAC can leverage, the more intelligent and granular an NAC policy can be. A policy that controls SSL VPN remote access, for example, can leverage geolocation or other telemetry to regulate access, and to restrict access where or when needed.

Pulse Secure Policy Secure is an industry leading NAC solution that controls and protects cloud and network access for remote and LAN-based mobile and nonmobile devices. Pulse Policy Secure delivers granular, secure, identity-based, location-aware, granular access control for LANs, as well as public and private networks and their applications. This enables safe, protected cloud and network access to a variety of devices, including Windows and Mac Laptops, Apple iOS, and Google Android devices.

The Challenge

There are significant security risks that come with the very real benefits and liberating effects of allowing employees and guests to use any device. And there is no single panacea for addressing these risks. However, when network access control (NAC) user policies leverage mobile device management (MDM) device-based information, the result is more intelligent security, simplified management, and increased mobile worker productivity.

When it comes to noncorporate managed devices entering the network, finding a way to balance security with easy user and device access can be a challenge. This is especially relevant with the bring-your-own-device (BYOD) trend and the proliferation of personal mobile phones and tablets. Provisioning BYOD devices to ensure secure access to the network, enforce policy, and protect the enterprise can be a complex multivendor undertaking. In any large organization, there will be numerous users attempting to connect their devices to the corporate network. In order to deliver the flexible access that users expect, enterprises must intelligently manage these new devices, their apps, and all of the data they interact with.

The Pulse Secure BYOD Solution

Mobile Device Management

Together with its partners, Pulse Secure has overcome these challenges by integrating the Connect Secure and Policy Secure gateways with MDM solutions such as MobileIron and Airwatch.

With mobile devices becoming ubiquitous, mobile management is growing in importance. Relatively new on the scene, and complementary to NAC, is the advent of mobile device management (MDM) solutions, which deliver centralized management control of mobile devices; both those privately owned by company employees and those owned by the enterprise. By controlling and protecting the data and configuration settings for all mobile devices in the network, MDM reduces support costs and business risks. MDM optimizes the functionality and security of a mobile communications network, while minimizing cost and downtime, especially when combined with NAC solutions.

Industry leading MDM solutions, including MobileIron and Airwatch, combine traditional mobile device management with comprehensive security and app management. This enables the mobile IT administrator to manage the lifecycle of devices and apps, from registration to retirement, and quickly get mobile operations under control.

A Better Way to BYOD: Pulse Secure and Partner MDM Solutions

The most effective means to efficiently and effectively protect the BYOD-enabled enterprise requires cooperation between NAC and MDM technologies. Once integrated, MDMs can inform smarter NAC policies. For example, MDM integration can enable organizations to check and block a jail-broken or rooted device before it can compromise network security. It can also set policy that will prevent employees from downloading unapproved applications, or applications that could contain malware and compromise network security.

Solution Workflow

The BYOD workflow in Figure 1 shows how a partnership between MDM and the Connect Secure or Policy Secure gateway work together to grant a new user remote access to a secured network. With this integration, the MDM acts as a device authorization server, and MDM record attributes are used as the basis for assigning role-based policy:

1. The user first onboards an MDM client to the mobile device. In many scenarios, this will have already occurred via a public or private app store. Once the MDM client is installed, the user initiates registration with the MDM server.
2. Once registered, the device connects with the MDM. Remote access credentials are provisioned and the device configuration may be modified to comply with policy.
3. The client connects through a Web browser to the Pulse Connect Secure gateway.
4. The gateway identifies the device and queries the MDM for device attributes. Roles are assigned and a custom message is sent to the MDM.
5. That message is then passed to the phone via the MDM informing the user of connection success or failure.

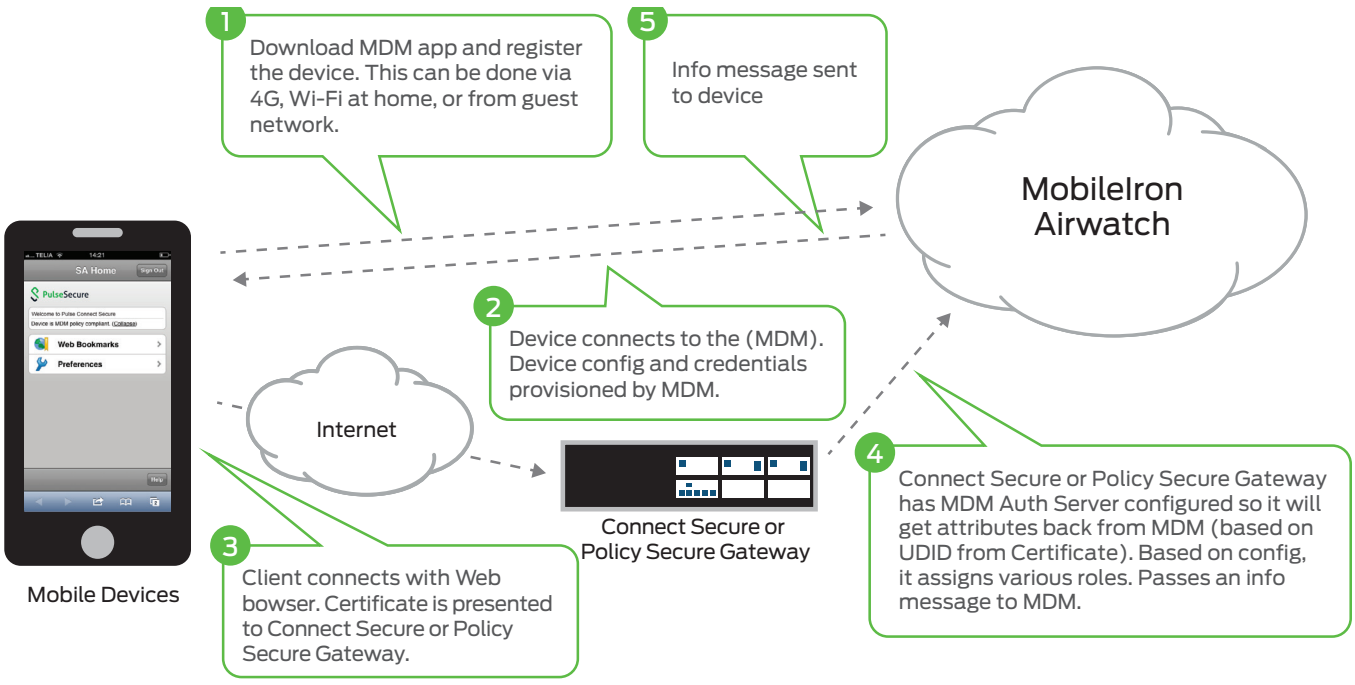

Figure 1: Pulse Secure and MobileIron or Airwatch MDM onboarding workflow

Features and Benefits

Advantages of an integrated NAC/MDM/remote access solution include more intelligent security, simplified management, and increased mobile worker productivity. The Pulse Secure/partner BYOD/MDM solution also enables:

- Remote connectivity
- Seamless onboarding
- Admission control
- Zero-touch application configuration
- Automated application deployment

Summary

With a fully integrated solution, end users can gain secure remote access capabilities via SSL VPN connectivity that are regulated by NAC policy, which in turn is informed by the MDM. The combined system can configure remote devices through the MobileIron or Airwatch MDM solutions—granting employees and employers transparent flexibility to access any networked device securely from any location without adding complexity to the end-user experience. Management also becomes easier as shared information can be consolidated into a confluent IT management experience.

The BYOD movement is transforming the workplace, and Pulse Secure and leading MDM product partners are transforming the way employees and IT benefit from the productivity and flexibility of BYOD—without compromising security or increasing management complexity.

About Pulse Secure, LLC

Pulse Secure, LLC is a leading provider of access and mobile security solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize the company's Pulse virtual private network (VPN), network access control and mobile security products to enable end user mobility securely and seamlessly in their organizations. Pulse Secure's mission is to enable open, integrated enterprise system solutions that empower business productivity through seamless mobility.

Corporate and Sales Headquarters

Pulse Secure LLC
address
address
Phone: xxx-xxx-xxxx
Fax: xxx-xxx-xxxx
www.xxxxxxx.com

SB00x Aug 2014