PulseSecure

White Paper

A DAY IN THE LIFE OF THE MOBILE WORKER

Pulse Secure and the MAG Series Gateways Enable Fast, Secure Network, Cloud, and Application Access

Table of Contents

Executive Summary

Today's IT leaders face a difficult situation in handling mobile device security and policy compliance, particularly given the Bring Your Own Device, or BYOD, trend. The Consumerization of IT is driving end-user demand for ubiquitous access—to networks, to clouds, to applications, to everything—from any device, anywhere, at any time. Meanwhile, IT faces an overwhelming challenge as it attempts to provide a consistent end user experience across inconsistent platforms, while maintaining corporate and regulatory policy compliance.

In this white paper, we will consider the difficulty of managing mobile security and policy today. We will consider the issues faced by IT when managing different operating systems across a myriad of endpoints and point products, some of which are user-owned. Finally, we will look at how Pulse Secure addresses a broad spectrum of security and end-user experience issues, as we step through a day in the life of a mobile worker.

Introduction—Creating a Unified User Experience in a Fragmented IT World

The workforce has changed dramatically in the last five years, both in terms of where people work and how they work. The number of worldwide remote workers is growing exponentially, while some analysts have estimated that mobile workers will account for almost half of the workforce in the next few years. The ability to accommodate remote and mobile workers allows enterprises to select the best employees regardless of their proximity to the corporate HQ. This not only saves relocation costs, time, etc., but also increases employee satisfaction and decreases churn. Mobility is clearly a compelling benefit for workers and for the enterprise itself, but it also introduces a new paradigm to IT.

The Bring Your Own Device (BYOD) trend has complicated IT issues exponentially. A recent Pulse Secure survey reports that almost 44 percent of respondents use their mobile devices for both personal and business purposes, while fewer than 4 percent use them strictly for business. If business IT leaders think they can keep personal devices off of their networks and out of their resources, consider that 81 percent of respondents admitted to using their devices to access their employer's network without their employer's knowledge or permission—and 58 percent do so every single day.

These new issues complicate the use of technologies borne of more "mainstream" remote or mobile initiatives, including IPsec and SSL VPN, network access control (NAC) and endpoint security. The growing focus on BYOD policies stretches these applications over a wide variety of devices, many of which are not managed by corporate IT. The growth in remote and mobile workers, combined with the BYOD trend, would effectively multiply management complexity even if the support technologies worked seamlessly and identically over all devices.

Unfortunately, however, these technologies do not work seamlessly or identically over different devices and operating platforms. This means that enterprise IT departments are presented with the nearly impossible task of managing up to five different pieces of client software on up to five different devices per user. This task would be daunting even if all devices were running identical corporate images, but that is seldom the case, and the adoption of the BYOD model makes it all the more unlikely in the future.

The issue of upgrading software clients complicates matters even further. While an upgrade might function perfectly on one device type or operating system, it may break down completely on another. At best, upgrades may be applied inconsistently and at worst "opposing" vendors end up pointing fingers at each other as the reason for a breakdown, with no solution in sight.

The sheer variety of possible outcomes illustrates the issue. As an example, consider any number of Microsoft Windows applications that use dynamic link libraries (DLLs), or shared libraries. An application upgrade might change an element in a DLL that is common between several applications. So, while an upgrade might work for a single application, others that use that common element will break. The result is the opposite of what the upgrade is designed to do. Instead of making the application run faster or enabling additional features, IT is deluged with helpdesk calls complaining of broken applications and, in some cases, on more than one device per user.

Still another issue to be considered is simple day-to-day desktop or device management. IT must now manage up to five different packages of client software per user, over several operating systems and a myriad of images that may differ significantly from the current corporate image. The larger the number of clients and user desktops, the bigger this issue becomes. Not only is this unwieldy to manage, but it can also seriously impact device performance.

And IT is not the only victim of the battle of many different client software elements vs. myriad devices. Users are affected as well. Many pieces of client software available today require end user interaction to function properly. The end user must know which client to activate in order to get the desired experience. For example, if a user usually works from a NAC-enabled corporate office, the user may not understand why that client does not work when trying to access the network from home, where a VPN would be needed. If the end user typically works remotely over a VPN using a client on a corporate laptop, the user may not be aware that the client will not be available on another device.

While such decisions may seem trivial to IT, they can be baffling to the typical nontechnical end user who simply expects an endpoint device—regardless of whether it is corporate issued or personal—to be a tool, not a vocation. Not only do these issues erode productivity, they come with a substantial cost in the form of helpdesk calls. And when the end user decides to become noncompliant, this can lead to huge ramifications for overall network security, privacy, and data integrity, as well as the potential for regulatory noncompliance, data breaches, and even loss of corporate reputation.

Remote and mobile workforces, with their proliferation of devices, operating systems, and corporate images, are here to stay. These trends yield significant benefits to businesses by lowering costs, raising productivity, and increasing employee satisfaction. This means that IT organizations must find a way to bring disparate client software elements and their functionality together in a way that delivers the desired experience across the plethora of devices and operating platforms. At the same time, they must remove the burden of network or software knowledge from the end user in order for these benefits to be realized.

Solution Requirements

IT began this journey by adopting a variety of point products, each with its own, distinct client software. As the number of clients and operating systems grew, however, the point product model quickly became unwieldy. Each platform ended up with a different set of clients, each of which might interact negatively with the others or with the underlying OS, many times in unpredictable and dangerous ways. Most enterprises today have more than one corporate image, adding still another level of complexity. Upgrades and additions are nearly impossible, given the number of variables created. Finally, and perhaps most significantly, service delivery depends heavily on the end user knowing which client to use in which situation—knowledge that requires an understanding of the underlying network infrastructure and technology.

With this backdrop, Pulse Secure approached the development of a single client, designed to simplify service delivery for both IT and the end user. The first goal was to build a single piece of enabling software that addressed:

- Secure remote access from any device, including mobile devices
- Network or LAN-based access control
- Endpoint security, including mobile device security and management
- Overall device performance by reducing the number of clients required for complete functionality

Finally, the solution had to "just work," delivering users safe, secure, ubiquitous access to data and applications. The product had to provide this access based upon the user's identity, role in the organization, location, device type, and the underlying security of the device—while minimizing end user intervention and interaction. And finally, the solution needed to automatically answer the following questions:

- Does the user's device have a current version of the corporate mandated endpoint security applications?
  - If not, can the device be remediated, and how?
- Is the user allowed access to the requested resource? If so, is user access allowed from this device? From this location?
- Does the user need to activate different clients when moving, for example, from a remote connection into the corporate network? Can a single client be used regardless of connectivity (wireless or wired)?
- Can a nontechnical user get needed access from any device, anywhere, without any understanding of technology and the underlying network configuration?
- Can a remote user make the most of "heavy" data laden or rich media applications?

Pulse Secure—a Single Unified Enabler

Wrapped in an extremely user-friendly package, Pulse Secure is a highly complex piece of software that securely connects users to networks and dynamically enables the appropriate network and security services on the endpoint. Users are not distracted from their work activities to figure out what network they are on or what service to enable. With Pulse Secure, the connection just works, helping to deliver the productivity promised by mobile devices. And, dynamic access control seamlessly switches between remote (SSL VPN) and local (UAC) access control services, enabling additional functionality such as endpoint assessment, and remediation when needed.

With Pulse Secure, endpoint security is assessed through an automatic host check, ensuring that the device meets the corporation's security and access policy requirements before network access is granted. If a computing device is out of compliance, remediation for the device can be handled automatically, many times without user or helpdesk intervention. And Pulse Secure works seamlessly across Windows, Mac OS, Android, iOS, and other operating systems.

With Pulse Secure, regardless of device or OS type, the result is the same: For the end user, the connection process is simple, fast, and easy to use, requiring minimal interaction or intervention. In the data center, Pulse Secure enables comprehensive, location-aware, identity-enabled, federated network and application access and security across a myriad of platforms.

The Pulse Secure solution includes a simple yet sophisticated client interface, purpose-built software services, and scalable, centralized gateways. For mobile devices, Pulse Secure is a quick, easy download from any major mobile OS app store. For laptops and nonmobile devices, enterprises may choose to push the Pulse Secure client to users themselves, or to post it on an intranet or corporate app store.

The Pulse Secure MAG Series Pulse Secure Gateways, located in the enterprise, can be enabled to run the following services:

- **Pulse Connect Secure**, which provides secure SSL VPN access to corporate resources and web- and cloud-based applications for remote and mobile users
- **Pulse Policy Secure (UAC),** which provides identity-based access control for mobile and remote users within the corporate environment
- **Both of these Pulse Secure services** simultaneously through service modules within a MAG Series gateway chassis.

The Pulse Secure User Experience

The best way to describe how Pulse Secure helps IT and end users is to follow a typical user through several daily scenarios. We'll look at both what the user experiences and what is actually happening "under the covers."

Home Access from a Remote Corporate Laptop

Our typical user begins his day at home. He wants to check his Microsoft Outlook e-mail on his corporate Windows laptop. When the laptop PC "wakes up," the user is prompted for his username and password, requiring his SecurID token, which is the multi-factor authentication scheme his company has deployed. He clicks on the "Connect" button when prompted. Even though he is on a slower network and Outlook is a fairly heavy application, the user doesn't notice any significant delay in how the application performs. He checks his e-mail, puts his laptop into hibernation mode, and leaves for the office.

Under the Covers

When the corporate laptop woke up, the Pulse Secure client detected that the user was not on the corporate network. Pulse Secure's Location Awareness feature recognized the device's location and enabled the correct and appropriate connection without requiring any end user intervention. For example, if Pulse Secure had been started in a remote location, it would automatically connect to the appropriate MAG Series gateway running Pulse Connect Secure. Using the Pulse Secure Location Awareness feature, that same client will automatically connect to Pulse Policy Secure as soon as the user is on the corporate network.

The following location awareness example includes two connections. The first connection is a Pulse Policy Secure connection that resolves to "TRUE" when the endpoint is connected on the corporate LAN. The second connection is a Pulse Connect Secure connection that resolves to "TRUE" when the endpoint is located in a remote location.

- Pulse Policy Secure connection: If the Domain Name System (DNS) server that is reachable on the endpoint's physical network interface is one of your organization's internal DNS servers, then establish the connection.
- Pulse Connect Secure connection: If the DNS server that is reachable on the endpoint's physical network interface is not one of your organization's internal DNS servers, and the DNS name of your Pulse Connect Secure device resolves to the external-facing IP address of the Pulse Connect Secure device, then establish the connection.

In the latter case, Pulse Secure connects to the SSL VPN gateway, and the user is asked to log in. Pulse Secure automatically checks the user's endpoint for corporate defined security and access policy status, and finds that the device's security stance is in compliance with corporate policy. If the device were not compliant, the situation could have been remediated automatically.

In our example, the user was presented with a login page. He entered his credentials, which were sent via encrypted tunnel to the SSL VPN gateway. The gateway checked the user via whatever authentication scheme was enabled by corporate IT, including multi-factor or biometrics, confirming the user's identity as well as determining the user's role and therefore his access permissions for this session.

Access from a Corporate Laptop on Campus

Our user arrives at his office and wakes up his hibernating laptop. It does not matter if the user is in his office on the corporate campus wired into his laptop's docking station, or if he is roaming the corporate campus, wirelessly connected from a conference room in a meeting. Either way, Pulse Secure is automatically connected, and has determined that the user is connected directly to the corporate network. So now he's off and running with his day. The user doesn't have to switch clients or even log in again.

Under the Covers

After the laptop came out of hibernation, Pulse Secure—which was still active on the user's laptop—determined that the user was now connected directly to his corporate office and network. In this case, Pulse Secure saw that the user was attaching to an 802.1X-enabled WLAN, according to the location awareness rules set by the corporation's IT team. Remote access was no longer applicable, so Pulse Secure switched from SSL VPN access to Unified Access Control (UAC) network access control, and ended the remote access connection automatically.

One notable fact is that the user did not have to login again because of Pulse Secure's Session Migration feature. Location Awareness and Session Migration are similar because they both simplify connectivity for the user, but they do so under different conditions. With Location Awareness, Pulse Secure makes a decision about how and where to connect the user and device when the device login occurs. Session Migration occurs when the user puts the device into a standby or hibernation mode without first logging off of the network, and then opens that device in a different network environment. Session Migration enables the appropriate Pulse Secure gateways and services to intelligently migrate an existing session and the associated session data. While switching connection from SSL VPN to UAC, the user does not need to be prompted for credentials

Session Migration is enabled using the Interface for Metadata Access Point (IF-MAP), a standard protocol from the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) Work Group. IF-MAP was designed to support standardized, dynamic data interchange among a wide variety of networking and security components, and it is a standard client/server protocol for accessing a metadata access point such as an IF-MAP server. The Pulse Secure services to which a user authenticates will publish session information to the IF-MAP server, which is part of Pulse Policy Secure. When a user session is migrated to another service and service module or gateway, the new service and service module or gateway consults the IF-MAP server, and imports information about the preexisting session to automatically establish a new session for the user. The original gateway then terminates the prior (pre-migration) session. More details on IF-MAP can be found on the TNC website at: **www.trustedcomputinggroup.org/developers/trusted_network_connect**.

In our example, Pulse Policy Secure queried the IF-MAP server and found that the user had already been authenticated to Pulse Connect Secure, and that the previous session was still valid. The user's session was then migrated to Pulse Policy Secure with no requirement for additional sign-in or network authentication by the user.

Access from a Personal Mobile Device

Our user's flight lands at a connecting city, and he has some time during the layover to check e-mail and do some work via his iPad. From his tablet, he launches Pulse Secure, enters his network username and password, and clicks "Connect". Regardless of the connection type (Wi-Fi, 3G, 4G, etc.), he is able to access all of the networked and cloud-based resources and applications he has been authorized for, just as if he were working from his corporate issued laptop.

Under the Covers

To start working from his personal tablet, our user needed to launch Pulse Secure, which is available for Apple iOS, Google Android, and several other mobile operating systems. Before being granted network access, Pulse Secure assessed the endpoint to determine its security posture. For example, Pulse Secure can determine whether a device has been "jail-broken" or "rooted," and it can also determine whether or not Pulse Secure Mobile Security Suite is operational on the device. Once compliance has been confirmed, our user entered his username and password, multi-factor authentication or biometrics, and Pulse Secure made the connection via the appropriate MAG Series gateway running Pulse Connect Secure. If the user is attempting to access third-party cloud- or web-based applications, the MAG Series gateway serving as SSL VPN will generate a SAML assertion (including authentication statements to the Web/cloud resource), automatically authenticating our user. After logging into Pulse Secure via single sign-on (SSO), the user was not required to log in again to any Web- or cloud-based application that has been set up to work with this feature on the MAG Series gateway running Pulse Connect Secure. IT administrators can choose to make the presence of Pulse Secure Mobile Security Suite mandatory to ensure security on the user's personal mobile device and mitigate risks posed by a BYOD policy.

Conclusion

Today's IT manager is faced with a host of challenges, including the need to enable users with fast, secure network, cloud, and application access from any device and any location. This requirement has forced the deployment of many different pieces of client software, and these often differ by operating system and version of corporate image. The new trend toward BYOD has multiplied these challenges exponentially, adding layers of complexity and making even simple deployments or updates virtually impossible. Nontechnical users should not be expected to be able to navigate the intricacies of today's network access.

Enter Pulse Secure, which enables users to just click and connect for fast, secure network, cloud, and application access—anytime, anywhere. Pulse Secure delivers simplicity for the user, security for the IT Administrator, and peace of mind for all, automatically.

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
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net

WP001 Aug 2014