CHAPTER 1

Introduction

May 14, 2014

Historically the workplace defined the workspace, but trends in mobility have impacted both. Ten years ago, Cisco published a CVD that expanded the workplace to include the home office, which allowed employees to join the corporate network securely, allowing them to remain productive even when not physically on campus. This transformed the workplace, but the devices limited the solution. Often the employee would carry the same laptop back and forth between the campus and the home office out of necessity. While the expanded network kept the devices connected, the data (e.g., an Office document, email, etc.) physically resided on a hard drive in the device. Corporate policy required that only a specific device could be trusted for use by a specific employee.

This Cisco Mobile Workspace Solution with Citrix design guide finally addresses that limitation. A single device no longer binds a user to their work. Instead the device is a tool or a conduit that allows employees to interact with their content. In the ever-continuing effort to maximize productivity gains, organizations are responding by removing restrictions that limit how a user interacts with data, yet still recognize that this content represents intellectual property and is a corporate asset that must be protected. When thinking about productivity, work is user interaction with data. This interaction has context. For example, creating a spreadsheet is a different activity than looking up data in a spreadsheet. The data itself should not be bound by the application, which is especially true in organizations that have developed legacy in-house applications that now must be extended to additional mobile platforms. This design guide explores how users can better interact with data by abstracting the layers that separate them. Conceptually this is accomplished with a mobile workspace. The term is dual purpose: first, the workspace is accessible on mobile devices but, more importantly, the workspace is not tied to any single device or platform. Users can interact with their work securely from any device, anytime, anywhere.

The CVD is broken into several sections that cover on-campus and remote devices using both native applications and virtualized desktops, however these are not mutually-exclusive deployment models. A comprehensive solution includes a range of components to enable a truly fluid mobile experience while securing both the network and the device without compromising the user experience. Cisco and Citrix offer a unique solution that leverages a full range of products that can now integrate together in ways not previously possible. For example, Citrix XenMobile Device Manager and Cisco Identity Services Engine (ISE) can integrate over an API to ensure that network policy and device policy complement one another. The device manager is responsible for establishing mobile policy on hand-held compute devices such as smartphones and tablets. XenMobile device manager is also capable of establishing policy on MacBooks and limited policy on Window devices, although they are not the focus of this guide.

Cisco ISE sets network policy with respect to what level of access a particular device has on the corporate network and the compliance conditions that must be met prior to gaining network connectivity. Cisco ISE can enforce device policy by restricting access to the corporate network, ensuring that mobile devices do not pose a security threat to corporate resources. This is accomplished by setting access appropriate for both the user's role and asset class of the networked device. Active Directory group

membership defines the users role, while the ownership of the device sets the asset class. The CVD builds on concepts introduced in the BYOD design guide and covers employee-owned and corporate-owned devices. The same user in AD does not get the same access level on their personal device as they do on their corporate device. This is true both on campus as well as for remote users that attach to a VPN head-end device. Remote access is covered in a later section.

Citrix XenMobile is a comprehensive solution to manage mobile applications, data, and devices. Users have single-click access to all of their apps from a unified corporate app store and IT can easily configure, secure, and support mobile devices. With XenMobile, IT can meet their compliance and control requirements while giving users the freedom to experience work and life their way.

Citrix is a leading provider of enterprise mobility management (EMM) software used to establish and enforce device policy on hand-held endpoints, which might include corporate- and employee-owned phones and tablets. Devices manufactured by all the major equipment providers are supported at some level. Apple and Android devices are the primary focus, but XenMobile also supports Blackberry and Windows 8 mobile devices.

Enterprise mobility management is a relatively new phenomenon and is in a constant state of expansion. Features can be thought of in several categories:

- Device Restrictions—There are two common types of restrictions. Either some feature of the device is disabled, such as the camera, or there are additional requirements for basic usage, such as a PIN lock or storage encryption. When a restriction is in place, the user is not offered the choice of non-compliance. Restrictions are used to reduce security risks to the enterprise.
- Device Compliance—This may also be referred to as posture enforcement. The XenMobile Device Manager checks the attributes of the device against a list of acceptable operational conditions. Compliance checks can be enforced based on their severity. For example, an email could be sent to the user if they are running a software version known to contain a vulnerability or XenMobile can automatically issue a selective wipe if the device has been compromised. A compliance check is different from a restriction because the user can become out of compliance. XenMobile uses automatic actions to respond to non-compliant devices. Compliance can be used to increase security and reduce operational costs.
- Content Distribution—Bookmarks, Web Clips, and other content can be pushed to devices in the background without user intervention or made available on demand. Content distribution is used to increase productivity. XenMobile can push content to Android devices natively. Both Apple and Android can leverage Citrix's ShareFile to distribute content from on-premise or cloud-based data repositories. Web Clips are HTML bookmarks that are displayed as application icons on an Apple mobile device.
- Application Distribution—The XenMobile Device Manager can offer a company catalog of available software or in the case of Apple devices, push required software to the device. The software can come from public repositories or can be corporate-developed applications. Application distribution has both security and productivity gains. Security is enhanced because any software distributed by the XenMobile Device Manager or AppController, including local storage associated to the software, can be removed as part of a corporate wipe. This is not true if the user installs the same software from Apple's App Store, Google Play, or any Android marketplace. The XenMobile Device Manager can also inventory devices for installed software. AppController has the additional advantage of integration with Store Front to offer virtualized applications that are offered through Citrix Receiver.

Citrix XenMobile consists of two core function, XenMobile Device Manager and XenMobile Application Controller. Together they are known as XenMobile Enterprise Edition. The XenMobile Device Manage provides MDM functionality, including traditional device management through the use of policy profiles. XenMobile AppController is a full application life cycle management tool that can integrate into Citrix StoreFront and, by extension, XenDesktop. Citrix offers XenMobile Mobile Device

Manager Edition and XenMobile App edition to allow enterprises to customize their deployment to meet their needs. This CVD incorporates device and application management and requires XenMobile Enterprise edition, which includes both components.

Beyond these, there are additional components for enterprise integration, such as WorxMail for secure email, WorxWeb for secure Web browsing, and ShareFile for secure collaboration. Together these components integrate to form a comprehensive mobile policy framework that enables the mobile workforce.

Until recently, many organizations may have simply chosen to grant restricted access to the network and allow only communications between the mobile device and a virtual desktop infrastructure. In doing so, the organization can be sure that access to corporate applications and sensitive data can only be accomplished through the use of a secured, unalterable virtual desktop environment with no data stored locally. When considering this approach, the XenDesktop family of products is the leading solutions in Desktop Virtualization. When combined with WAN Optimization technologies such as Cisco WAAS, protocol enhancements through "Citrix HDX" and Citrix Receiver, the user experience from mobile devices even over slower Internet connections is greatly enhanced.

Overview

This CVD brings together components from Cisco with those from Citrix and details how the complementary mobility offerings can work together to provide a flexible and customizable solution that can meet the full set of requirements needed for a successful mobile workspace program. The CVD presents several use cases to further illustrate the application of this solution to likely business needs. The following use cases are covered:

- Corporate-owned device with full access
- Employee-owned device with full access
- Employee-owned device with partial access
- Contractor-owned device with restricted project access

These use cases generally extend those presented in the most recent version of the Cisco BYOD CVD (http://www.cisco.com/c/en/us/solutions/enterprise/data-center-designs-cloud-computing/own_device.html). The intent of the use cases is to illustrate the flexibility of the system and is not meant to restrict how the features of the system can be configured. Within solution design, there is often a trade-off between an extremely secure system and those that deliver a very open user experience. Specific use cases have been chosen to explore how a balance can be achieved by weighing corporate risk against employee productivity.

Although the system is composed of products from both Cisco and Citrix, the foundation is built from the Cisco BYOD CVD, which describes how to provide secure network access to a wide variety of devices, both wired and wireless. A REST API that is supported between the system components makes the integration between Cisco ISE and the XenMobile Device Manager possible. The device manager responds to requests from ISE with respect to a device's operational parameters, including for example the presence of a PIN Lock on the device and the version of the OS. ISE uses this information to establish the level of network access to which the device and user are entitled. In addition, ISE can request that the device manager execute several tasks on the behalf of ISE, such as removing all corporate data from the device or locking the device.

There is a focus on mobile productivity. Users want to interact with their work from a wide range of device, including smartphones and tablets. With the exception of images and video, most smartphones consume data. Mobile devices are unique because they are always connected either via LTE or WiFi and can be used almost instantly without lengthy boot-up times. They also have ready-to-use video, GPS location, accelerometers, piezo compasses, and a range of other physical sensors they may be attached

via Bluetooth. These attributes make mobile devices a compelling platform for a range of new business applications that were not possible on legacy devices such as laptops. Mobile applications offer context around data that is unique. This context has the potential to deliver large productivity gains when fully leveraged, usually through the use of in-house-developed mobile applications. For example, an insurance company could create a claims application that allowed adjusters to include high-resolution pictures or video, GPS location information, or the customer's verbal statement could be attached to a claim that is filed from the field in real-time. Other companies may already have a Windows-based application that is installed on laptops mounted in the adjuster's car and may want to port those applications quickly onto a new mobile tablet. The Cisco Mobile Workspace Solution with Citrix enables both scenarios.

Cisco Mobile Workspace Solution with Citrix Components

There are several components required to enable Cisco Mobile Workspace Solution with Citrix. Some components described here could be replaced or substituted with similar products that provide equivalent functionality, such as a Certificate Store. Other components are core to this solution, for example ISE and the WorkHome client. In addition, there is some product overlap between Cisco and Citrix and there may be more than one way to accomplish a specific goal. Not all possible configurations are presented here. In addition, some essential components are not discussed that are a prerequisite for the solution, including DHCP Servers, DNS, NTP, route protocols, and other fundamental network services.

Cisco Components

The following Cisco products are used in this solution.

Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) is a core component of the Cisco Mobile Workspace (CMW) solution architecture. It delivers the necessary services required by enterprise networks, such as Authentication, Authorization, and Accounting (AAA), profiling, posture, and guest management on a common platform. The ISE provides a unified policy platform that ties organizational security policies to business components.

The ISE also empowers the user to be in charge of on-boarding their device through a self-registration portal in line with CMW policies defined by IT. Users have more flexibility to bring their devices to their network with features such as sponsor-driven guest access, device classification, CMW on-boarding, and device registration.

Cisco Integrated Services Routers

Cisco Integrated Services Routers (ISR), including the ISR 2900 and ISR 3900 families, provide WAN and LAN connectivity for branch and home offices. The LAN includes both wired and wireless access. In addition, ISRs may provide direct connectivity to the Internet and cloud services, application and WAN optimization services, and may also serve as termination points for VPN connections by mobile devices.

Cisco Wireless LAN Controllers (WLC)

The WLC automates wireless configuration and management functions and provides visibility and control of the WLAN. The WLC extends the same access policy and security from the wired network core to the wireless edge while providing centralized access point configuration. The WLC interacts with the Cisco Identity Services Engine (ISE) to enforce authentication and authorization policies across device endpoints. Multiple WLCs may be managed and monitored by Cisco Prime Infrastructure. Wireless LAN controller functionality can be within standalone appliances, integrated within Catalyst switch products, or run virtually on Cisco Unified Computing System (UCS).

Cisco Aggregation Services Routers

Cisco Aggregation Services Routers (ASR), available in various configurations, provide aggregate WAN connectivity at the campus WAN edge. In addition, ASRs may provide direct connectivity to the Internet and cloud services and may also serve as a firewall. The ASR runs Cisco IOS XE software and offers Flexible Packet Matching (FPM) and Application Visibility and Control (AVC).

Cisco Catalyst Switches

Cisco Catalyst® switches, including the Catalyst 3000, Catalyst 4000, and Catalyst 6000 families, provide wired access to the network and handle authentication requests to the network via 802.1X. In addition, when deployed as access switches, they provide power-over-Ethernet (PoE) for devices such as thin client workstations, IP phones, and access points.

Cisco Nexus Series Switches

Cisco Nexus switches, including the Cisco Nexus 7000 and 5000 families, serve as the data center switches within the CVD. The Cisco Nexus 7000 switches provide 10GE Layer 3 connectivity between the Campus Core, Data Center Core, and Aggregation Layers and 10GE Layer 2 connectivity, utilizing VPC, for the Cisco Nexus 5000 switches in the Data Center Access Layer to which all servers are attached.

Citrix Components

The following Citrix products are used in Cisco Mobile Workspace Solution with Citrix.

Citrix XenMobile

Citrix XenMobile is a comprehensive solution to manage mobile devices, apps, and data. Users have single-click access to all of their mobile, SaaS, and Windows apps from a unified corporate app store, including seamlessly-integrated email, browser, data sharing, and support apps. IT gains control over mobile devices with full configuration, security, provisioning, and support capabilities. Flexible deployment options give IT the choice to manage XenMobile in the cloud or on-premise. In addition, XenMobile securely delivers Worx Mobile Apps, mobile apps built for businesses using the Worx App SDK and found through the Worx App Gallery.

- XenMobile Device Manager—The device manager is responsible for setting and enforcing device policy. Policy can include device restrictions or requirements. The device manager can also provision some aspects of the base services provided on the device such as email settings, VPN settings, or WiFi settings. Once installed on the device, the device manager can dynamically update

the configuration on the device without user intervention. Furthermore, it can collect information about the device such as installed applications, PIN Lock enabled, or Cell plan usage. It interfaces with the device through a combination of agent software and built-in MDM APIs. It can also integrate with LDAP for user account information.

- XenMobile AppController—The AppController provides enterprise and public app management on mobile devices. It sets corporate policy around application distribution. It interfaces with the WorxHome client on the mobile device to offer users a central location to manage their work place applications. AppController can interface with the device manager to provide additional services. AppController can also provide authentication services to other components of the solution. For example, Citrix ShareFile can authenticate against AppController. XenMobile AppController should not be confused with XenApp, which is a separate product used to virtualized Windows applications.

Citrix Unified App Store

Unified App Store together with XenMobile AppController provide applications services to both Citrix Receiver and WorkHome Mobile Applications for Windows-based virtual application support. Storefront maintains a list of application subscriptions and can synchronize this between devices.

Citrix WorxHome

WorxHome is the mobile client that runs on the hand-held device. It provides access to XenMobile AppController and also works in conjunction with the XenMobile Device Manager. The Android version of WorxHome interfaces with the device administrator APIs found on Android devices. The iOS version augments the built in MDM protocol found in Apple devices. WorxHome is the user portal into the solution.

Citrix Receiver

The Receiver application provides access to virtualized applications and desktop hosted on XenDesktop and is the primary user interface for all hosted applications. Installed on user devices, Citrix Receiver provides users with quick, secure, self-service access to applications, desktops, and data from any of the user's devices, including smartphones, tablets, and PCs. Receiver provides on-demand access to Windows, Web, and Software as a Service (SaaS) applications. Receiver integrates directly with AppController and WorxHome.

Citrix XenDesktop 7.0

Citrix XenDesktop delivers Windows apps and desktops as secure mobile services. With XenDesktop, IT can mobilize the business, while reducing costs by centralizing control and security for intellectual property. Incorporating the full power of XenApp, XenDesktop can deliver full desktops or just the apps to any device. HDX technologies enable XenDesktop to deliver a native touch-enabled look-and-feel that is optimized for the type of device, as well as the network.

- Director—Director is a web-based tool that enables IT support and help desk teams to monitor an environment, troubleshoot issues before they become system-critical, and perform support tasks for end users. You can also view and interact with a user's sessions using Microsoft Remote Assistance.
- StoreFront—StoreFront authenticates users to sites hosting resources and manages stores of desktops and applications that users access.

- Studio—Studio is the management console that enables IT to configure and manage the XenDesktop deployment, eliminating the need for separate management consoles for managing delivery of applications and desktops. Studio provides various wizards to guide administrators through the process of setting up theXenDesktop environment, creating workloads to host applications and desktops, and assigning applications and desktops to users.
- Delivery Controller—Installed on servers in the data center, the Delivery Controller consists of services that communicate with the hypervisor to distribute applications and desktops, authenticate and manage user access, and broker connections between users and their virtual desktops and applications. The Controller manages the state of the desktops, starting and stopping them based on demand and administrative configuration. In some editions, the Controller allows you to install Profile management to manage user personalization settings in virtualized or physical Windows environments. Each site has one or more Delivery Controllers.
- Virtual Delivery Agent (VDA)—Installed on server or workstation operating systems, the VDA enables connections for desktops and apps.
- Machine Creation Services (MCS)—A collection of services that work together to create virtual servers and desktops from a master image on demand, optimizing storage utilization and providing a pristine virtual machine to users every time they log on. Machine Creation Services is fully integrated and administrated in Citrix Studio.
- Windows Server OS machines—VMs or physical machines based on Windows Server operating system used for delivering applications or hosted shared desktops to users. Also known as Hosted Shared Desktops, this is the deployment method that is followed in Cisco Mobile Workspace Solution with Citrix.
- Secure delivery—When users connect from outside the corporate firewall, the Cisco AnyConnect Client is used to establish a secure VPN Tunnel to an ASA firewall located at the Internet edge. Optionally, this release can use Citrix NetScaler Gateway (formerly Access Gateway) technology to secure these connections as well. NetScaler Gateway or NetScaler VPX virtual appliance is an SSL VPN appliance that is deployed in the demilitarized zone (DMZ) to provide a single secure point of access through the corporate firewall. Both methods are examined, however only the ASA is discussed in Cisco Mobile Workspace Solution with Citrix.
- Citrix XenApp—Citrix XenApp technology has been integrated in XenDesktop 7.Citrix XenApp delivers Windows apps as secure mobile services as well as the Hosted Shared Server OS-based desktop virtualization used in this CVD. Users can self-select apps from an easy-to-use app store that is accessible from tablets, smartphones, PCs, Macs, and thin clients. HDX technologies enable XenApp to deliver a native touch-enabled look-and-feel that is optimized for the type of device, as well as network conditions. XenApp is built on the same FlexCast management architecture as XenDesktop offering simple, powerful configuration and operations management and cloud-style automation and scalability.

Citrix ShareFile

ShareFile is a secure and robust enterprise data synchronization and sharing service solution that empowers users to share data with anyone and synchronize data across all of their devices. ShareFile seamlessly integrates with workflow tools and provides a rich user experience on any device to enhance productivity.

Additional Partner Components

In addition to Cisco and Citrix, the solution depends on a number of products from other market leaders.

Microsoft Certificate Authority

The solution uses Microsoft's CA server to distribute user certificates. These certificates are used to authenticate users for both WiFi using EAP-TLS and remote access using Cisco AnyConnect. Other CA servers could be used although only Microsoft's has been validated in this CVD.

Microsoft Active Directory

Microsoft Active Directory (AD) is a core component of the solution. It binds together policy and is set up on various components of the system. Users are placed in various AD groups that define the user's role within the enterprise. All policy decisions are tied to these roles through LDAP integration. These roles constitute the various use cases covered within the CVD.

Apple Push Notification Service

Push services are required for MDM functionality with Apple products. Push serves as a middle-man between the MDM and the devices. The only configuration requirement is to install an APNS certificate on the MDM to allow it access to this service.

Apple iOS Mobile Devices

Although somewhat obvious, mobile hand-held devices are a core component of the solution. Like the other components, mobile devices require minimum software levels and appropriate configuration settings to be fully functional. The mobile device provides the user experience. Apple software includes a device management stack as an integral component of the operating system.

Android Based Mobile Devices

As is the case with iOS device, Android devices are also a core component. Android represents a unique challenge because of the wide range of devices and software levels found in the field. Complicating matter somewhat, users are not always able to update the software on their phone and are dependent on their carrier. This can present a unique challenge if a defect is discovered that could compromise the device's security. Android, which is owned by Google, also has a push service but is not required for device management.