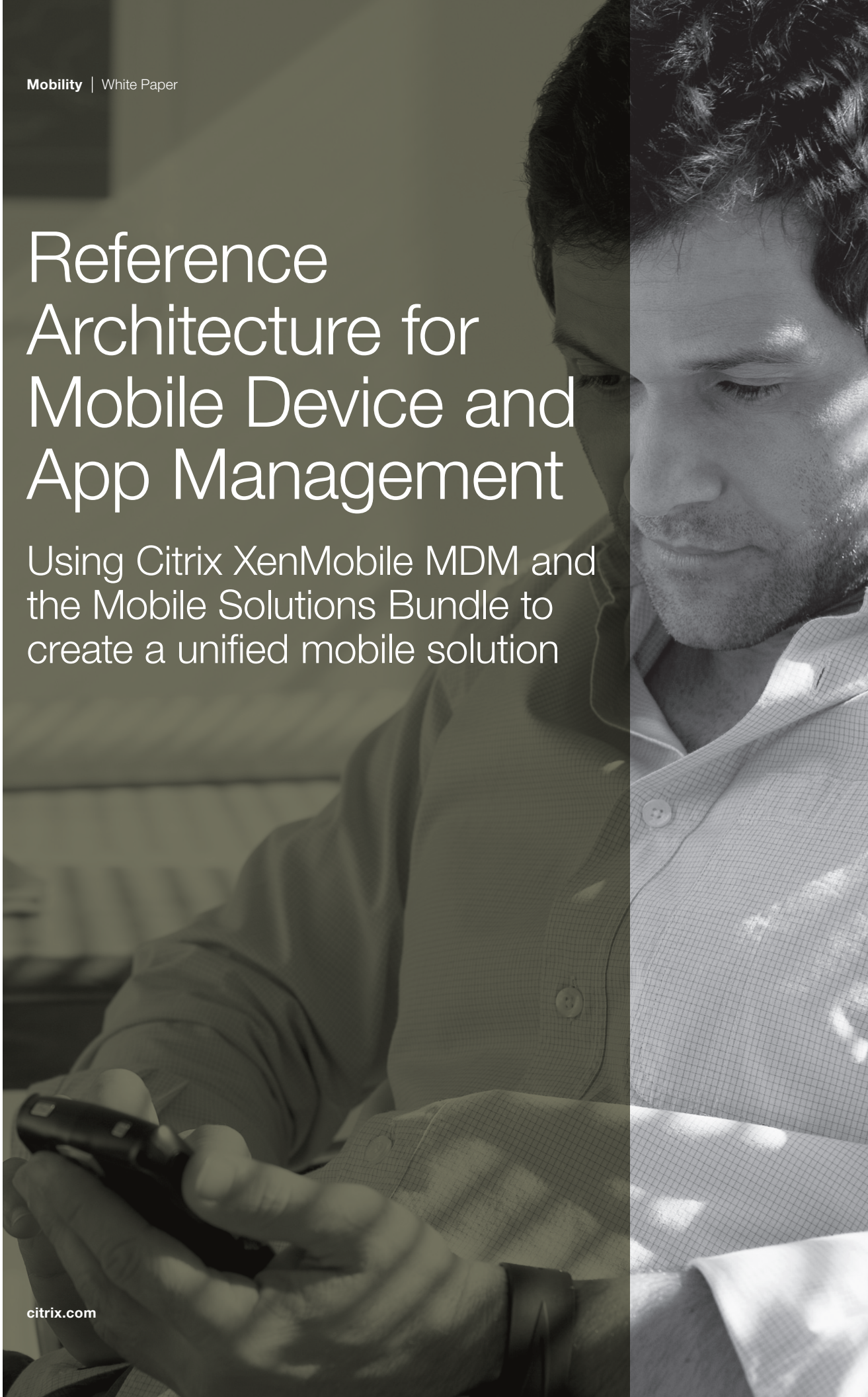


Mobility | White Paper

Reference Architecture for Mobile Device and App Management

Using Citrix XenMobile MDM and the Mobile Solutions Bundle to create a unified mobile solution

CITRIX®

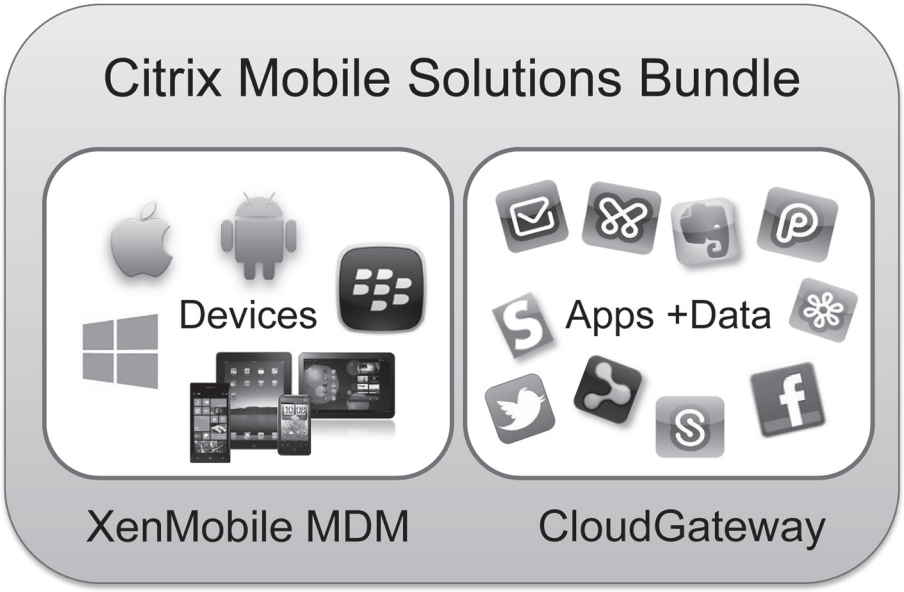
citrix.com

The Citrix *Reference Architecture for Mobile Device and App Management* guides architects in designing the next generation of mobile device and application management services. These services allow IT organizations to gain control over the proliferation of mobile devices in the enterprise. The Mobile Solutions Bundle provides a solution that securely delivers mobile, web, Windows apps, and data to all devices in the enterprise. The Mobile Solutions Bundle is the first step in making mobility a strategic advantage rather than a security liability. This document is for IT architects looking to implement and manage their mobility infrastructure. Each of these validated architectures has been certified by Citrix to perform and scale to the most demanding enterprise requirements.

Mobile Solutions Bundle

The Mobile Solutions Bundle combines XenMobile™ MDM, security and management of mobile end-points with CloudGateway™, a self-service enterprise app store for business apps, and data to provide a complete mobile solution. Each of these components includes infrastructure components that will be described in detail in the following sections.

- XenMobile MDM
  - XenMobile Device Manager
  - XenMobile SMG
  - XenMobile SharePoint DLP
- CloudGateway
  - AppController
  - Access Gateway
  - StoreFront (Windows® Desktops and Apps)



XenMobile Device Manager (MDM)

XenMobile MDM offers advanced mobile device management capabilities like provisioning, automated compliance, and features that make mobile apps "business-ready". With a "one-click" dashboard, simple administrative console, and real-time integration with Microsoft Active Directory XenMobile MDM simplifies device administration across the enterprise.

XenMobile MDM provides the ability to manage the device lifecycle across every major platform, including iPhone, iPad, Android, BlackBerry, Symbian, and Microsoft Windows 8. It offers out-of-the-box support for BYOD programs or corporate mobile initiatives.

XenMobile SMG

XenMobile Secure Mobile Gateway (SMG) provides the ability to protect mobile email with MDM policies. It lets mobile users view encrypted attachments in a secure viewer and keeps sensitive corporate data from leaking outside of enterprise control on iOS and Android devices.

XenMobile SharePoint DLP

XenMobile SharePoint DLP (Data Leak Prevention) provides SharePoint access to mobile devices via MDM policies. This feature gives IT administrators control over the devices that have access to SharePoint data while the native mobile app, Citrix® Mobile Connect, provides the interface and security to view the documents.

CloudGateway

Citrix CloudGateway is an enterprise mobility management solution that securely delivers mobile, web, Software as a Service (SaaS), Windows apps, and data to any device. It empowers employees with a self-service enterprise app store that provides access to business apps and data, leveraging the consistent, rich user experience of Citrix Receiver™.

AppController

AppController provides access to web, SaaS, mobile apps, and ShareFile®. This component allows IT to protect enterprise apps and data with policy-based controls, such as restriction of application access to authorized users, automatic account de-provisioning for terminated employees and remote wipe for data and apps stored on lost devices.

Access Gateway

NetScaler Access Gateway™ provides secure remote access from outside the corporate network while maintaining the highest level of protection for sensitive corporate data.

StoreFront

StoreFront, the next-generation of Web Interface, provides a set of services used by Receiver to enable access to AppController and XenDesktop®.

ShareFile

Citrix ShareFile is a cloud based follow-me-data solution. ShareFile enables users to securely store, sync and share data, both within and outside the organization. Using ShareFile with CloudGateway provides IT with enterprise directory integration capabilities for easy, enterprise-wide provisioning and deployment of user accounts.

Reference Environments

This document will guide IT administrators through proven architectures based on the enterprises mobile device and application management requirements. The following environments have been validated as reference architectures.

- XenMobile MDM
- XenMobile MDM – Secure Proxy
- Mobile Solutions Bundle
- Mobile Solutions Bundle – XenDesktop (XD) integration
- Mobile Solutions Bundle – Multi-Store
- Mobile Solutions Bundle – High Availability
- Mobile Solutions Bundle – NetScaler® as proxy

Determining the correct architecture will be based on the device or app management requirements of the enterprise. The components of the bundle are modular and build upon each other. The following table displays architectures based on the mobile technologies. Before making a decision it is important to determine the following:

- What level of management is required, App vs. Device or both?
- What types of apps need to be managed and deployed?
- What data strategy is required, SharePoint or ShareFile?

	XenMobile MDM	Mobile Solutions Bundle	Mobile Solutions Bundle XD Integration
Device Security Control	X	X	X
Device Provisioning	X	X	X
Native App Delivery	X	X	X
SharePoint Integration	X	X	X
Web/SaaS App Delivery		X	X
Mobile MDX Apps		X	X
ShareFile Integration		X	X
Mobile App Policies		X	X
Mobile App Mgmt.		X	X
Win Apps/Desktops			X

XenMobile MDM

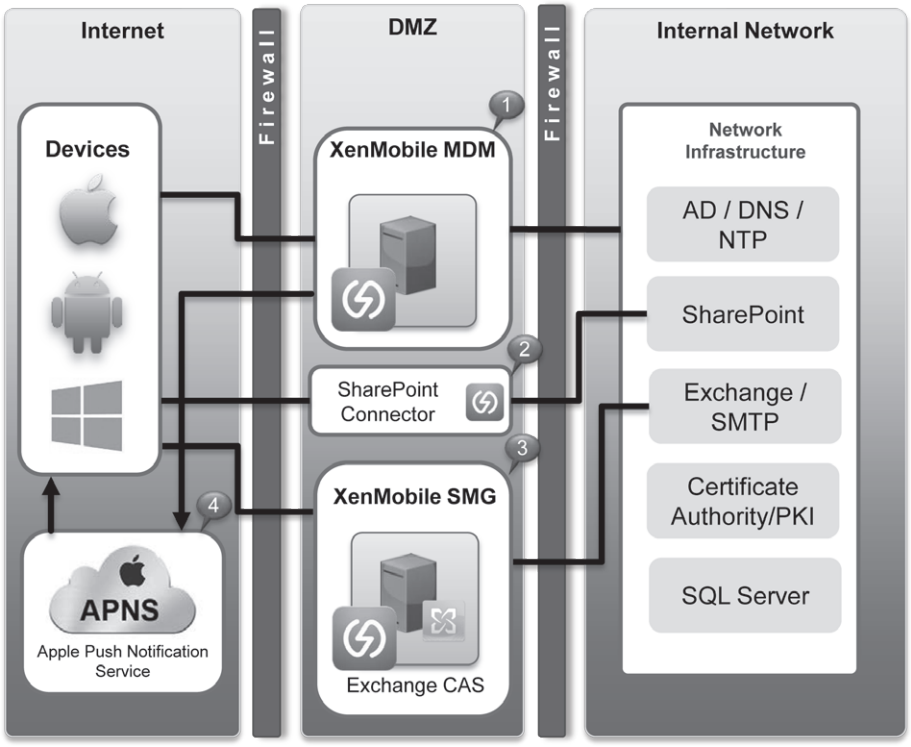


Figure 1 – XenMobile MDM Reference Architecture

1. **XenMobile Device Manager (MDM)** is the central server for MDM that combines policies, devices, and users to create deployments to manage the corporate mobile strategy.

- Devices connect to MDM over ports 80, 443, and 8443 (only during device enrollment for iOS).
- MDM runs on a Windows Server 2008 R2. It is recommended to follow the Microsoft security best practices for Windows Servers in the DMZ.
- The MDM Server requires connections to backend infrastructure components like, Active Directory, DNS, SMTP, SQL Server, and a certificate authority.
- MDM also requires a PKI service like Microsoft Certificate Authority or it can use its own PKI service hosted on the MDM Server that gets installed with Device Manager. Device Manager will use this service to push out client certificates to devices for client certification authentication to MDM. Client certificates are deployed automatically during device enrollment.
- It is recommended to use SQL Server, Express, Standard, or Enterprise for a production environment. Reference the following link for supported Windows and SQL versions.

2. The **SharePoint connector** is an optional component of XenMobile MDM that provides access to SharePoint sites. This requires external access to your SharePoint server by either placing the SharePoint server in the DMZ or utilizing a load balancer in the DMZ with access to the SharePoint server. This functionality can be configured in a MDM policy allowing the Citrix Mobile Connect app to host the SharePoint data in a secure viewer on the mobile device.
3. **XenMobile Secure Mobile Gateway (SMG)** provides protected mobile email through MDM policies. This can be installed on an Exchange Client Access Server (CAS) or in the DMZ on a Microsoft Forefront or Threat Management Gateway (TMG) server. Basic operation requires access to Exchange, MDM, and mobile devices over HTTPS (443). SMG will query the MDM Server to check policies for user and device access.
4. The **Apple Push Notification Service (APNS)** is used by MDM to push notifications to iOS devices for configuration and policy updates. This is service provided by Apple and is only required for iOS devices. Non-iOS devices have their own push implementation.

Note: A special APNS certificate that is signed by Citrix and issued by Apple is required before installing MDM. Please see installation instructions.

MDM Firewall Ports

The following ports need to be open to allow MDM to communicate with internal and external resources.

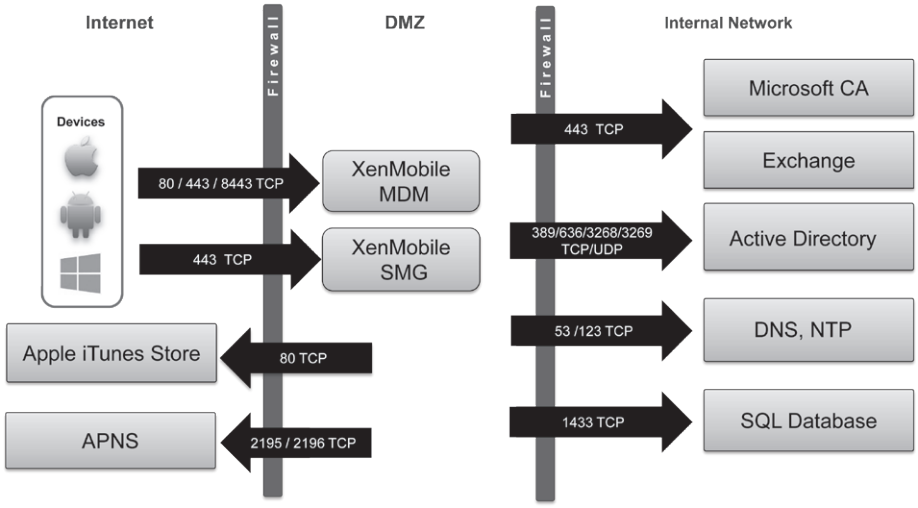


Figure 2 – XenMobile MDM Communication Paths

MDM Server Specifications

All components of the MDM architecture can be installed on physical or virtual machines. The following table describes the resource requirements to support 5000 devices for each of the components in the MDM architecture.

Virtual Machine	vCPU	Memory (GB)	Disk Space (GB)
XM Device Manager	2 – 4	4	24
Secure Mobile Gateway	2	2	24
XM SQL Server	2	6	24

Enterprises requiring scalability greater than 5,000 devices will need to adjust server specifications to match the parameters in the table below.

Devices	XenMobile MDM Server	SQL Server
5,000	2 vCPU, 4 GB RAM	2 vCPU, 6 GB RAM
10,000	4 vCPU, 8 GB RAM	4 vCPU, 16 GB RAM
20,000	8 vCPU, 16 GB RAM	16 vCPU, 24 GB RAM
40,000	16 vCPU, 32 GB RAM	32 vCPU, 64 GB RAM

The MDM and database servers can be clustered for high availability, please reference the High Availability section for more details on clustering the MDM components. Database backup and recovery should be performed according to the organization's data center policy.

Tomcat TCP connections also need to be taken into consideration:

Devices	Port 443	Port 8443	Port 80	PortMax Threads
Up to 10,000	400	30	20	12
Over 10,000	750	50	50	20

If the TCP connections are getting close to 750, then consider clustering the MDM Server.

XenMobile MDM with NetScaler option

An alternative and more secure deployment for MDM is to use a hardware load balancer like NetScaler in front of all the MDM components. In the architecture, the NetScaler is load balancing all HTTP and HTTPS traffic to MDM, SMG, and SharePoint.

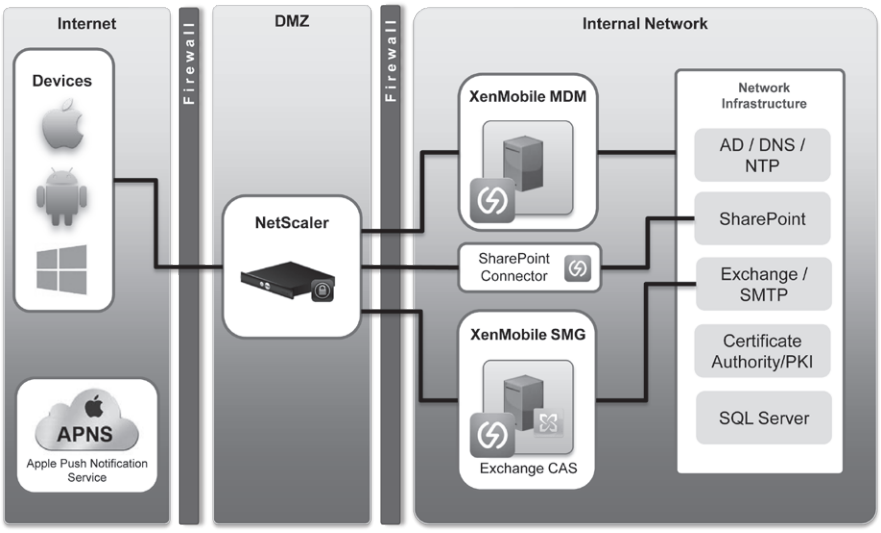


Figure 3 – XenMobile MDM with NetScaler

There are several reasons to do this:

- Limit exposure to Windows Servers in the DMZ
- Easily scale out by adding more servers behind NetScaler in the future
- Additional NetScaler features can be enabled to further increase security (e.g., application firewalls)

Configuration Tip: On the NetScaler device ensure SSL persistence is enabled and set to SSLSESSION for the HTTPS load balancing virtual servers (443 and 8443).

Mobile Solutions Bundle

CloudGateway, a component of the Mobile Solutions Bundle, includes Access Gateway, AppController, and optionally, StoreFront (for XenDesktop and XenApp® integration). The following components are highlighted in this architecture:

- AppController
- Access Gateway

In this environment, MDM and CloudGateway are installed side-by-side, complementing each other. MDM provides the device management and control with policies while CloudGateway provides MDX capabilities and secure remote access to enterprise resources. The following diagram highlights the CloudGateway infrastructure components.

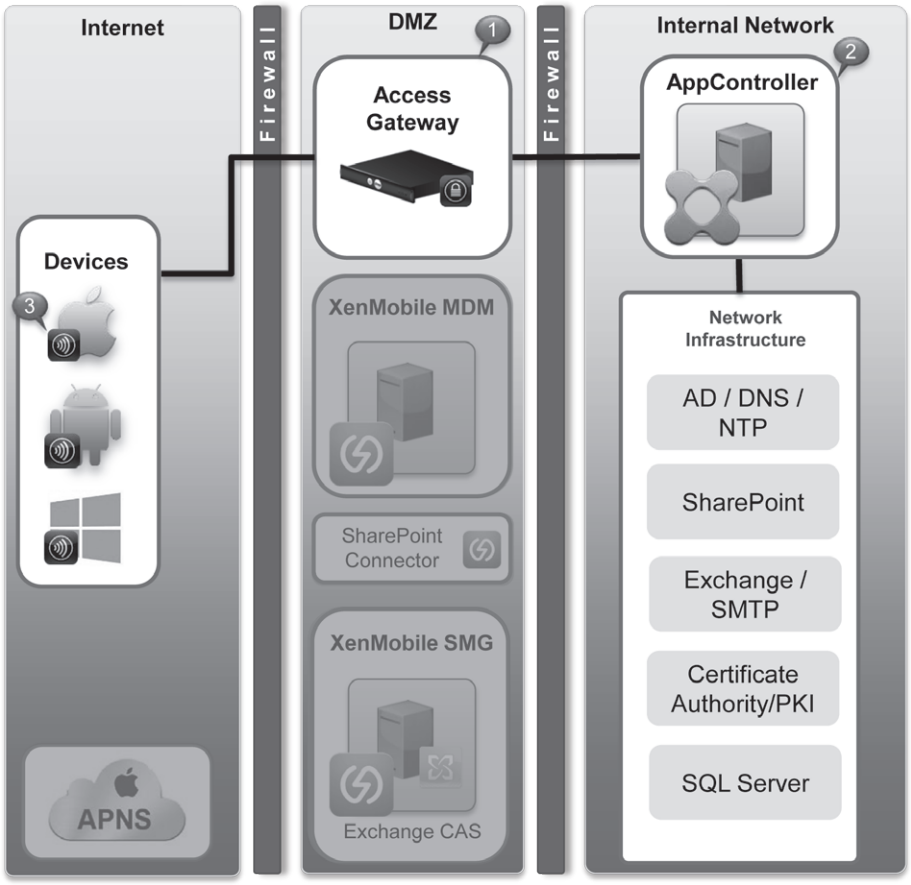


Figure 4 – Mobile Solutions Bundle Reference Architecture

1. **Access Gateway** – NetScaler Access Gateway is used for remote access and can be installed in the form of a NetScaler hardware appliance (MPX or SDX) or a VPX (virtual appliance that runs on XenServer®, VMware, or Hyper-V). This infrastructure component resides in the DMZ and is the central access point into the enterprise network. For extra security, two-factor authentication using RADIUS as a secondary authentication method is supported for services such as like RSA SecurID or Symantec VIP products.

2. **AppController** – AppController is a Linux-based hardened VPX appliance that can be deployed on XenServer or VMware. In this configuration, remote access is available using Access Gateway, but internal users can access AppController directly with the Receiver or Receiver for Web. AppController includes a version of Receiver for Web on the same server to allow mobile and desktop receivers to access apps without the addition of a StoreFront server. AppController requires connections to LDAP, DNS, NTP, and SMTP servers. SMTP is required for workflow approval through email notification.

   AppController integrates with ShareFile (ShareFile account with SSO enabled is required) by provisioning Active Directory users to the ShareFile cloud service, providing Single Sign-on (SSO) to the data service using SAML authentication.

3. **Citrix Receiver** – Citrix Receiver is client software that lets you access your data, applications, and desktops from any device including smartphones, tablets and PCs. Receiver can be downloaded from the device's app store or pushed to the device from XenMobile MDM.

CloudGateway Firewall Ports

In addition to the XenMobile MDM firewall ports in the previous environment, the following ports need to be opened for the CloudGateway infrastructure components. Ports 1494 and 2598 will only need to be opened if XenDesktop or XenApp is integrated (shown in next environment).

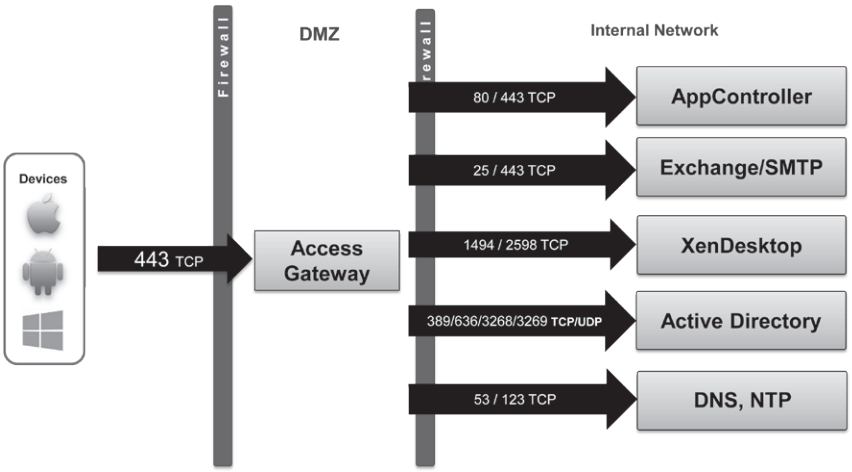


Figure 5 – CloudGateway Firewall Ports

CloudGateway Server Specifications

All components of CloudGateway can be configured and hosted as virtual machines. The AppController virtual machine (VM) is a virtual appliance that runs on XenServer and VMware ESXi. Access Gateway VPX is a virtual appliance that delivers the same features and functionality as the MPX physical appliance. Access Gateway VPX is a virtual workload that is deployed on its own hardware. The following table details the minimum resource requirements.

	vCPU	Memory (MB)	Disk Space (GB)
Access Gateway VPX	2	4096	20
App Controller	2	4096	50

CloudGateway Enterprise Scalability

CloudGateway can support enterprises with thousands of users by selecting the appropriate NetScaler Access Gateway hardware appliance. As the number of users authenticating, using mail and web resources and app activity through MicroVPN increase (Figure 6) the power of the NetScaler Access Gateway infrastructure component will need to be increased. Please refer to the figure below to select the appropriate configuration for your environment. These results are based on an AES encryption algorithm with a 1024bit key size. Scalability results will differ based on encryption algorithm and key sizes.

Sample user profile used for results below:

- Single connection per user
- Using only @WorkMail™ app
- Traffic usage is approximately 2.5 MB/min per user

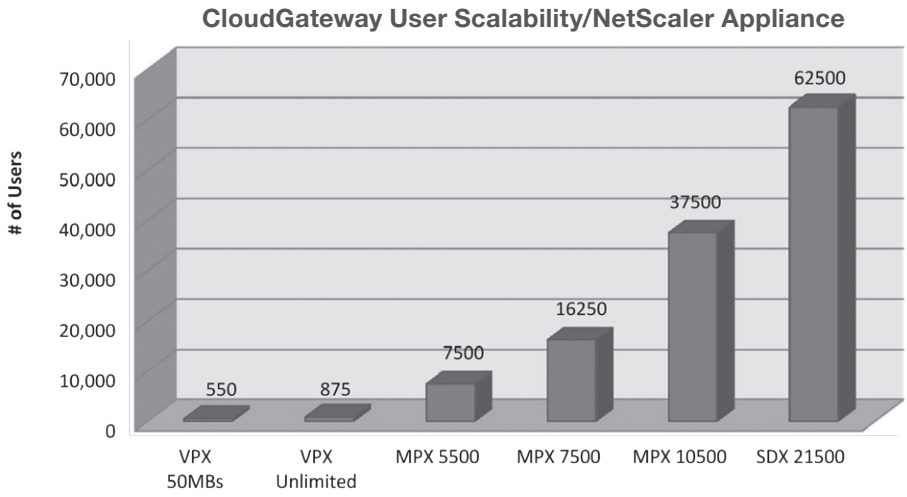


Figure 6 – CloudGateway User Scalability (@WorkMail)

For more information on the NetScaler hardware appliances used in these tests please refer to the following knowledgebase article.

CloudGateway – XenDesktop Integration

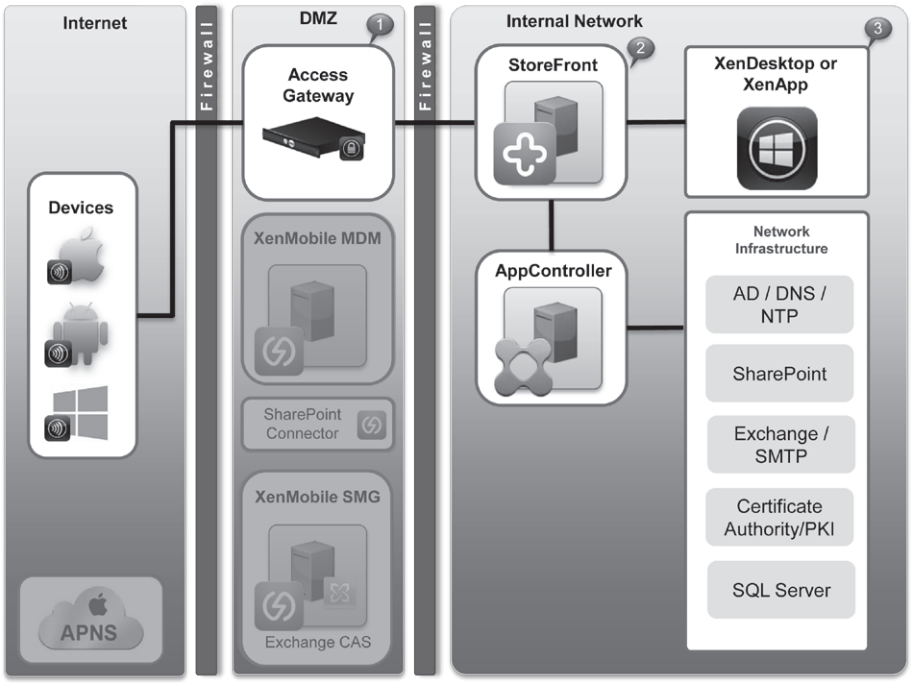


Figure 7 – CloudGateway - XenDesktop integration

1. **Access Gateway** – Access Gateway provides access to XenDesktop/XenApp HDX sessions, access to web/SaaS and mobile apps are delivered from the AppController. The additional configuration needed for this setup of Access Gateway is providing the Secure Ticket Authority (STA) URLs for XenDesktop/XenApp to the Access Gateway. This will allow pass-through authentication to Windows desktops and apps. TCP ports 1494 and 2598 need to be opened for ICA/CGP traffic between AG and XenDesktop/XenApp.

2. **StoreFront** – For access to Windows desktops and apps, StoreFront needs to be placed in front of the AppController and XenDesktop components. StoreFront provides resource aggregation. It will enumerate apps from XenDesktop, XenApp, and AppController to show the user one consolidated list of resources: Windows apps, desktops, mobile apps, web/SaaS apps, and data. In this configuration, Storefront needs to know how to pass device-specific information to AppController like device enrollment information and key management. These services need to be configured in the web.config file for proper communication between all three servers. Please follow these instructions for proper configuration.

3. **XenDesktop** – Link the XenDesktop broker or XenApp XML service to complete the integration with CloudGateway.

CloudGateway – Multi-Store Option

An alternative deployment option exists for organizations that have not yet consolidated Windows desktops and apps using StoreFront. In this scenario, Access Gateway is upgraded to version 10 and a separate Access Gateway virtual server is created to support the Mobile Solutions Bundle. If that is not possible yet, another configuration is to setup a separate Access Gateway 10 server for AppController and leave the older AG setup untouched. Either configuration requires Citrix Receiver to have two stores configured, one for XenDesktop/ XenApp using PN Agent Server and one for AppController. Citrix Receiver has been enhanced to easily switch between the two stores without having to re-authenticate each time. You will only have to authenticate once for each store.

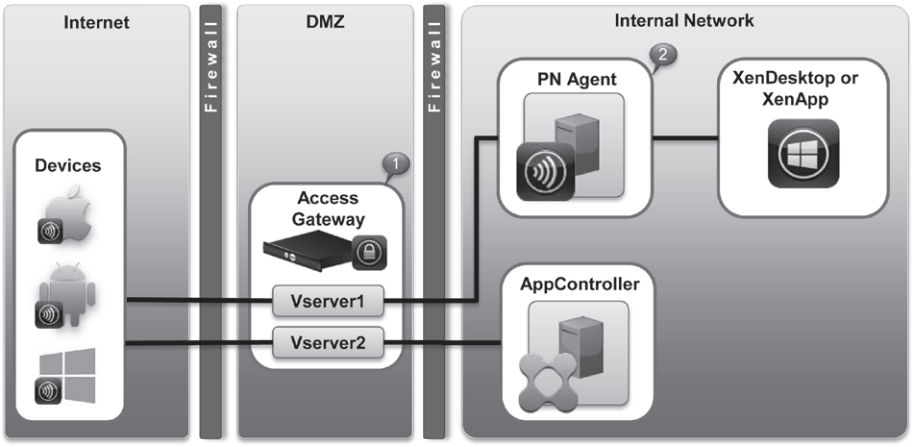


Figure 8 – CloudGateway – Multi Store Option

1. **Access Gateway** has to be upgraded first to v10.0.71.6014e or later. Creating a second AG virtual server will require a separate public URL, public IP, and certificate.

2. **Web Interface/PN Agent Server** – There are no changes required for PN Agent Server in this environment. Web Interface Server v5.4 is the only version supported.

High Availability – XenMobile MDM + CloudGateway

This architecture provides a fully redundant XenMobile MDM and CloudGateway environment.

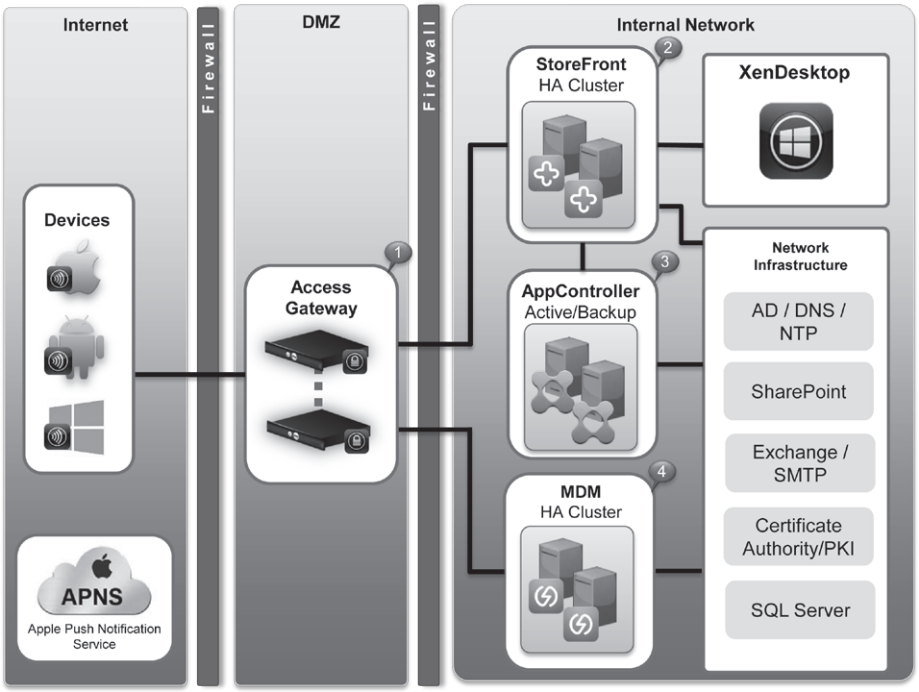


Figure 9 – High Availability – XenMobile MDM + CloudGateway

1. **Access Gateway HA Mode** – In this environment NetScaler devices are configured in high availability mode. A high availability (HA) deployment of two NetScaler appliances can provide uninterrupted operation in any transaction. With one appliance configured as the primary node and the other as the secondary node, the primary node accepts connections and manages servers while the secondary node monitors the primary node. If, for any reason, the primary node is unable to accept connections, the secondary node takes over. For more information, please follow this link.

2. **StoreFront HA Mode** – StoreFront HA mode is similar to the MDM server setup. It requires a separate SQL server (SQL server should have its own clustered environment) and a hardware load balancer like NetScaler. Ports 80 and 443 will need to be configured on the load balancer with SSL session persistence turned on for SSL connections. It is recommended to have multiple connection broker URLs and STA URLs for XenDesktop/XenApp connections. For more information, please follow this link.

3. **AppController** – Two AppController VMs can be deployed in a high availability configuration. The first AppController on which high availability is configured is called the primary, and the other instance is called the secondary. In this deployment, the primary AppController listens for requests, serves

user requests, and synchronizes its data with the data on the secondary AppController. The two VMs work as an active-passive pair, in which only one VM is active at a time. If the primary AppController stops responding for any reason, the secondary AppController takes over, becoming the active VM and begins to service user requests. As the active VM, the secondary AppController also synchronizes system and database information by using a client-server mechanism. A client on the active AppController VM shares the necessary information to a virtual server on the passive AppController as a series of requests. The virtual server parses the requests and performs the necessary action. A virtual IP is required; this will be the FQDN AppController address used when configuring StoreFront and Access Gateway in a CloudGateway deployment. For more information, please follow this link.

4. **XenMobile MDM HA Mode** – XenMobile MDM can be configured with multiple servers load-balanced behind a NetScaler appliance or another hardware load-balancing solution. In this environment, ports 80, 443, and 8443 are load-balanced. For SSL connections (ports 443 and 8443), make sure to turn on SSL session persistence in the load balancing rules. MDM requires a shared SQL server and NTP configured on each server.

Note: This configuration is more secure as the MDM servers are located in the internal network behind the Access Gateway.

Mobile Solutions Bundle with NetScaler

This environment shows NetScaler being a transparent proxy for all MDM components as well as enabling Access Gateway for the CloudGateway components. This is an alternative to having multiple servers in the DMZ.

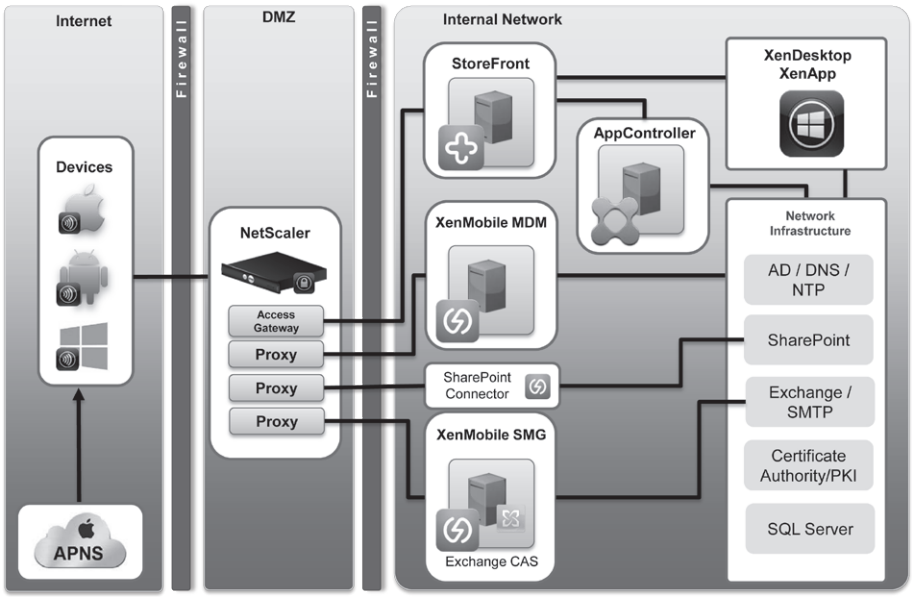


Figure 10 – Mobile Solutions Bundle with NetScaler

In the NetScaler configuration, Load Balancing is used as a proxy for each component. In this case, only one server is used for each balancer. Here is a sample configuration for a component server:

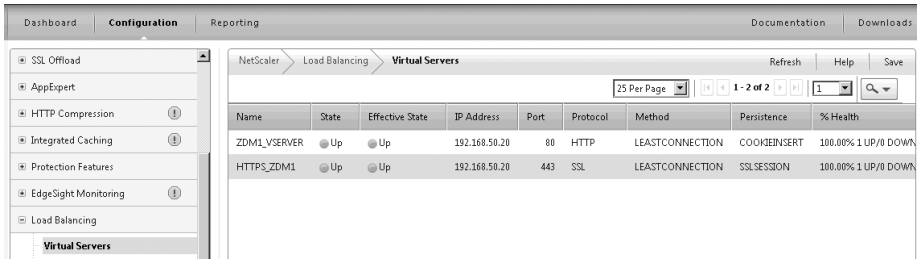


Figure 11 – NetScaler Load Balancing Configuration

Reference Environment Infrastructure

In the XenMobile and CloudGateway reference architectures; there are many supporting servers and services that are required for operation in an enterprise environment. The following section details the common infrastructure components (storage, virtualization environment, servers, networking equipment, etc.) and how the XenMobile and CloudGateway reference architectures integrate with them.

Network Layout

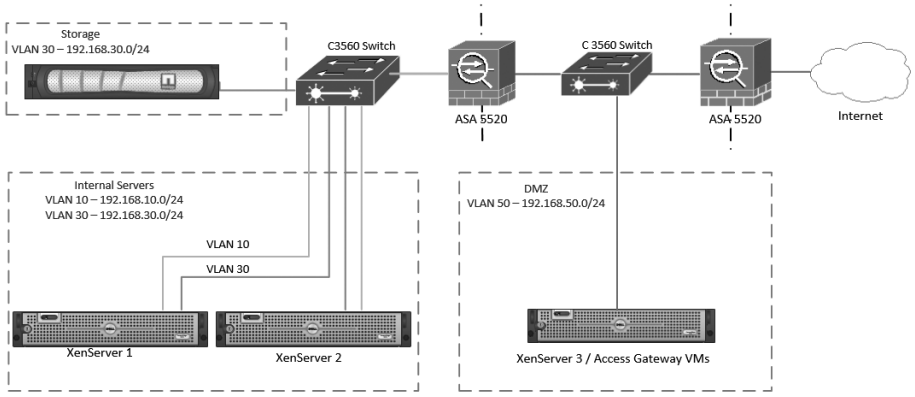


Figure 12 – Network Layout for Reference Environments

Server Hardware

XenServer Hosts	**Dell PowerEdge C6100** The Dell C6100 contains 4 physical servers enclosed in a 2U form factor with each server having the hardware specifications listed below: • 2 – Intel Xeon E5620 Processors • 64GB RAM • 500GB HDD • 2 – physical machines configured in HA (High Availability) mode • 2 – 1Gb Ethernet Adapters
XenServer Configuration	• 2 – servers configured in a virtualization pool for HA (High Availability) • XenServer version 6.1.0-59235p • Three separate VLANs configured: – VLAN 30 – Storage VLAN configured for 9000 MTU for fast connectivity to backend NFS storage. – VLAN 10 – User/Management traffic VLAN configured for standard 1500 MTU. Please note that it is best practice for XenServer to further segregate User and Management traffic by creating additional VLANs in high traffic implementations. – VLAN 50 – DMZ VLAN to provide access from outside the enterprise network.
Storage	**NetApp 2240-2** • 7.2TB total configurable storage • Active/Active Controller configuration • 4.5TB NFS configured storage volume • ~250GB used for complete virtualized environment • 2 – 10Gb Ethernet (10GbE) Adapters
Network	Cisco C3560X Cisco ASA 5520

Authentication

Active Directory running on Windows Server 2008 R2 was used for all reference architecture environments. Active Directory, or LDAP, support is different for each product. Both AppController and XenMobile MDM do not support users in nested groups. Another limitation for AppController is that it only supports a single forest environment. Please check each product's documentation for full support requirements.

The reference environments also make use of two factor authentication configured on Access Gateway to provide secure access to the internal corporate resources using RADIUS authentication from Symantec Validation and ID Protection. Using two-factor authentication will require an extra port to be opened on the firewall (typically UDP/1812) from DMZ (AG) to the RADIUS server (internal).

More information on configuring two-factor authentication can be found here.

Certificates

Wildcard and SAN certificates are supported for all Citrix products. In most deployments, only two wildcard or SAN server certificates are required:

1. External – *.extcompany.com
2. Internal – *.intdomain.net

The following table shows the certificates required and format needed for each component. A simple utility like OpenSSL can be used to convert certificate formats. A separate SAML Certificate will be needed depending on the SAML authentication enabled apps that are published in AppController.

	Certificate format	Certificates Required	Location
Access Gateway	PEM	Server*, root CA	External
AppController	PEM or PFX (PKCS#12)	Server, SAML, root CA	Internal
StoreFront	PFX (PKCS#12)	Server, root CA	Internal
XenMobile MDM	PFX (PKCS#12)	APNS, server. MDM will create its own PKI service or use Microsoft CA for client certificates.	External
XenMobile SMG	PFX (PKCS#12)	Server, root CA	External

*It is recommended to make this a public (3rd party) cert so mobile devices won't need to download the company's private root CA first.

DNS

It is recommended to use static IPs for all servers in the environment. As configured in the reference environment the following records were added to the DNS server.

Server	DNS Location	Record
XenMobile MDM	Internal and External	Host (A)
Access Gateway " (AG Vserver IP address)	Internal and External	Host (A)
AppController	Internal	Host (A)
StoreFront	Internal	Host (A)
XenMobile SMG	Internal and External	Host (A) and Mail (MX)
SharePoint DLP	Internal and External	Host (A)

Configuration Tip: Make sure that the FQDN of every server from every other server, especially Access Gateway can be resolved and pinged.

SQL Server

SQL server (Express, Standard, and Enterprise) are supported for all the products in the Mobile Solutions Bundle. It is important to plan accordingly and size the SQL server based on number of devices, applications and users that will be using the environment. The same SQL Server may be used for the different products. It is recommended to size the SQL server based on the MDM requirements. The impact of StoreFront on SQL is minimal. Please refer to the individual architectures for sizing recommendations.

Exchange Server and XenMobile Secure Mobile Gateway

In the reference environment, a Microsoft Exchange 2010 server was used to provide access to secure mail from XenMobile Secure Mobile Gateway. A full exchange server 2010 implementation includes 5 roles; there are 3 main roles that need to be configured:

- The Mailbox Server which is the backend server that hosts mailboxes.
- The Hub Transport server that routes mail and handles mail flow.
- The Client Access Server (CAS) which is an edge server that accepts connections to Exchange server from a variety of clients.

Although all 3 roles mentioned above are required as per the reference design, more details on the CAS role are included here as the physical placement of this role on a server in the topology, and the integration with XenMobile SMG is important.

XenMobile SMG is installed on the CAS and works to manage policy based device access to email by intercepting ActiveSync traffic using the built-in ISAPI filters provided by the CAS server. The CAS role is a middle-tier server that accepts connections to Exchange server from a variety of clients. This server hosts the protocols used by all clients when checking messages. On the local network, Outlook MAPI clients are connected directly to the Client Access server to check mail. Remote users can check their mail over the Internet by using Outlook Anywhere, Outlook Web App, Exchange ActiveSync, POP3, or IMAP4. While the CAS role placement is usually dictated by the placement of the Exchange Server Mailbox server, it is recommended as per the reference architecture that the CAS role be installed on a stand-alone server that is separate from the Exchange mailbox server and it resides in the DMZ. Having the CAS server placed in the DMZ adds an additional layer of security to the implementation by avoiding the need to place the mailbox server in the DMZ. Instead the CAS server can communicate with the Exchange server residing on the internal network over secure communications.

Conclusion

The Citrix Mobile Solutions Bundle is an enterprise mobility management solution that enables complete and secure mobile device, app and data freedom. Employees gain quick, single-click access to all their mobile, web, datacenter and Windows apps from a unified app store, including beautiful productivity apps that seamlessly integrate to offer a great user experience. The solution provides identity-based provisioning and control for all apps, data and devices, policy-based controls, such as restriction of application access to authorized users, automatic account de-provisioning for terminated employees and selective wipe of apps and data stored on lost, stolen or out-of-compliance devices. With the Mobile Solutions Bundle, IT can meet users' desire for device choice while preventing data leakage and protecting the internal network from mobile threats.

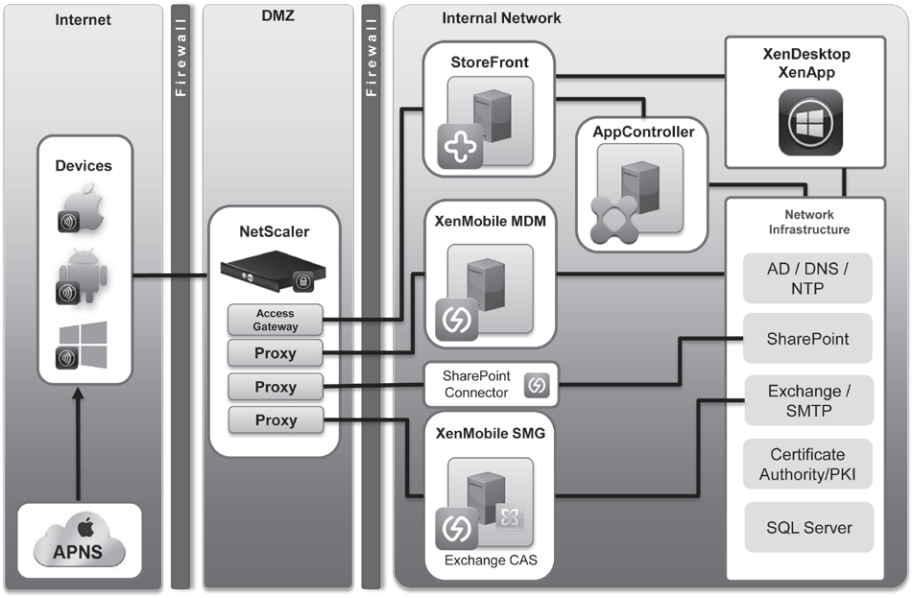


Figure 13 – Citrix Mobile Solutions Bundle Reference Architecture

Appendix A – Reference Documents

Storefront 1.2

http://support.citrix.com/proddocs/topic/dws-storefront-12/dws-version-wrapper.html

Netscaler 10.0

http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler10-wrapper-con.html

Access Gateway:

http://support.citrix.com/proddocs/topic/access-gateway/ag-edocs-landing.html

AppController 2.5

http://support.citrix.com/proddocs/topic/appcontroller-25/clg-appc-landing-page-d-con.html

XenMobile Device Manager

http://kb1.zenprise.com/Zenprise_Device_Manager

Secure Mobile Gateway (AKA Active-Synch Controller)

http://kb1.zenprise.com/Zenprise_Device_Manager/Zenprise_Device_Manager/Secure_Mobile_Gateway

Installation guide – Microsoft Client Access Server

http://technet.microsoft.com/en-us/library/ff622319(v=exchg.141).aspx

Microsoft Client Access Reference for Exchange 2010

http://technet.microsoft.com/en-us/library/ff622319(v=exchg.141).aspx

Microsoft Exchange 2010 Installation Guide Download
(Includes instructions for all required roles)

http://www.microsoft.com/en-us/download/details.aspx?id=17206

Appendix B - Firewall port requirements

XenMobile MDM

TCP Port	Description	Source	Destination
25	By default, the MDM SMTP configuration of the Notification Service uses port 25. However, if your corporate SMTP server uses a different port, make sure that your corporate firewall does not block that port.	XenMobile MDM	Corporate SMTP Server
80	Over-the-Air (OTA) Enrollment and Agent Setup *(Android and Windows Mobile)*	Internet	XenMobile Device Manager Server
	Over-the-Air (OTA) Enrollment and Agent Setup *(Android and Windows Mobile)*, MDM Web Console, MDM Remote Support Client	Corporate LAN and Wi-Fi	
	MDM Server Enterprise App Store connection to Apple iTunes App Store (ax.itunes.apple.com). Used for publishing recommended iTunes App Store apps from the available iOS applications within the Web Console and iOS Mobile Connect App	XenMobile MDM	Apple iTunes App Store (ax.itunes.apple.com)
80 or 443	XenMobile Device Manager Nexmo SMS Notification Relay outbound connection	XenMobile MDM	Nexmo SMS Relay server
389 or 636	LDAP/LDAPS connection from MDM Server to Directory Service Host (Active Directory Global Catalog server or equivalent LDAP directory service host)	XenMobile MDM	LDAP / Active Directory Services
443	SSL OTA Enrollment/Agent Setup *(Android and Windows Mobile)*, All Device-related traffic and data connections *(iOS, Android and Windows Mobile)*	Internet	XenMobile MDM
	SSL OTA Enrollment/Agent Setup *(Android and Windows Mobile)*, All Device-related traffic and data connections *(iOS, Android and Windows Mobile)*, MDM Web Console	Corporate LAN and Wi-Fi	
1433	Remote database server connection to separate SQL Server (Optional)	XenMobile MDM	SQL Server
2195	Apple APNS (Push Notification Service) outbound connection to **gateway.push.apple.com**, used for iOS device notifications and device policy push	XenMobile MDM	Internet (Apple APNS Service Hosts on public IP network17.0.0.0/8)
2196	Apple APNS (Push Notification Service) outbound connection to feedback.push.apple.com, used for iOS device notifications and device policy push		
5223	Apple APNS (Push Notification Service) outbound connection from iOS devices connected via Wi-Fi network to ***.push.apple.com**	iOS device on Wi-Fi network service	
8443	Over-the-Air (OTA) Enrollment for iOS Devices only	Internet	XenMobile MDM
		Corporate LAN and Wi-Fi	

1 Corporate LAN traffic outbound to DMZ and the Internet is assumed to be allowed

CloudGateway

TCP Port	Description	Source	Destination
80	Mobile Application download	Access Gateway	AppController
443	Connections to Storefront Services for Enterprise edition access to We, Mobile, SaaS and Desktop Applications	Access Gateway	StoreFront
	Connections to AppController for Web, Mobile and SaaS application delivery	Access Gateway	AppController
	Secure Ticket Authority (STA)	Access Gateway	Citrix XD / XA Servers
389, 636 or 3268	LDAP/LDAPS connection from NetScaler AG to Directory Service Host (Active Directory Global Catalog server or equivalent LDAP directory service host)	Access Gateway	LDAP / Active Directory Services
53	DNS	Access Gateway	DNS Server
123	NTP Services	Access Gateway	NTP Server
1494	Citrix ICA Protocol	Access Gateway	Citrix XD / XA Servers
2598	Citrix ICA/CGP Protocol When Session Reliability is enabled, TCP port 2598 replaces port 1494	Access Gateway	Citrix XD / XA Servers

1 Corporate LAN traffic outbound to DMZ and the Internet is assumed to be allowed

Corporate Headquarters
Fort Lauderdale, FL, USA

India Development Center
Bangalore, India

Latin America Headquarters
Coral Gables, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

Online Division Headquarters
Santa Barbara, CA, USA

UK Development Center
Chalfont, United Kingdom

EMEA Headquarters
Schaffhausen, Switzerland

Pacific Headquarters
Hong Kong, China

About Citrix
Citrix (NASDAQ:CTXS) is the cloud computing company that enables mobile workstyles—empowering people to work and collaborate from anywhere, accessing apps and data on any of the latest devices, as easily as they would in their own office—simply and securely. Citrix cloud computing solutions help IT and service providers build both private and public clouds—leveraging virtualization and networking technologies to deliver high-performance, elastic and cost-effective services for mobile workstyles. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations of all sizes achieve the kind of speed and agility necessary to succeed in an increasingly mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at www.citrix.com.