Citrix XenApp and XenDesktop 7.15 LTSR FIPS 140-2 Sample Deployments

Contents

Introduction 2

Audience 2

Security features introduced in XenApp and XenDesktop 7.15 LTSR 2

FIPS 140-2 with XenApp and XenDesktop 3

Sample deployments 4

XenApp (internal network) 7

How the components interact 7

XenApp using NetScaler Gateway MPX FIPS (external access) 9

How the components interact 10

XenDesktop (internal network) 11

How the components interact 11

XenDesktop using NetScaler Gateway MPX FIPS (external access) 13

How the components interact 14

Finding more information 15

Introduction

When deploying XenApp and XenDesktop within large organizations, particularly in government environments, security standards are an important consideration. Many government bodies specify a preference or requirement for applications to be compliant with Federal Information Processing Standards 140-2 (FIPS 140-2).

The document provides an overview of the security features that apply to XenApp and XenDesktop, with an emphasis on FIPS 140-2. Sample deployments are shown, providing guidance on FIPS 140-2 compliance. For more information regarding details of the individual security features, refer to the relevant product or component documentation.

Audience

This document is designed to meet the needs of security specialists, systems integrators, and consultants, particularly those working with government organizations worldwide.

Security features introduced in XenApp and XenDesktop 7.15 LTSR

The new security features and enhancements in XenApp and XenDesktop 7.15 LTSR, since the previous Long Term Service Release, provide a more streamlined route to deploy Citrix products securely and in accordance with FIPS 140-2. The new features provide the following benefits:

- More communications paths between XenApp and XenDesktop components can take advantage of the TLS 1.2 protocol. Refer to the white paper “End to End Encryption with XenApp and XenDesktop” for details.
- There is a broader choice of TLS 1.2 cipher suites, including ECDHE and AES GCM cipher suites.

FIPS 140-2 with XenApp and XenDesktop

FIPS 140-2 is a U.S. federal government standard that details a benchmark for implementing cryptographic software. The Cryptographic Module Validation Program (CMVP), that is administered by the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE), allows encryption product vendors to demonstrate the extent to which they comply with the standard and thus, the trustworthiness of their implementation.

Some U.S. government organizations restrict purchases of products and use of services from suppliers and nonfederal organizations.

The security community at large values products that follow the guidelines detailed in FIPS 140-2 and the use of FIPS 140-2-validated cryptographic modules.

To facilitate implementing secure application server access and to meet the FIPS requirements, Citrix products can use cryptographic modules that are FIPS 140-2-validated for implementations of secure TLS connections.

The following Citrix products and components included in the sample deployments can use cryptographic modules that are FIPS 140-validated:

- Citrix XenApp 7.15 LTSR
- Citrix XenDesktop 7.15 LTSR
- NetScaler Gateway MPX FIPS edition hardware appliance 12.0
- StoreFront 3.12
- Citrix Receiver for Windows 4.9

When using these products with the TLS connections enabled, the cryptographic modules that are used are FIPS 140-2-validated. Citrix XenApp and XenDesktop, StoreFront and Receiver, use cryptographic modules provided by the Microsoft Windows operating system. NetScaler uses the FIPS 140-2-validated Cavium cryptographic module.

Sample deployments

To ensure XenApp and/or XenDesktop deployments are FIPS 140-2 compliant, you need to consider each communication channel within the deployment. The following sample deployments show how users can connect and access resources on XenApp and XenDesktop with different configurations of components and firewalls. In particular, the samples provide general guidance on how to make each communication channel secure using TLS so that the system as a whole is FIPS 140-2 compliant.

The following sample deployments are shown:

Product	Deployment
XenApp	Direct internal access [LAN] External remote access [via Internet]
XenDesktop	Direct internal access [LAN] External remote access [via Internet]

These deployment scenarios utilize the following components to secure data communications using the TLS protocol. TLS provides server authentication, encryption of the data stream, and message integrity checks.

The NetScaler Gateway MPX FIPS hardware appliance is deployed in the DMZ to provide secure remote access to XenApp and XenDesktop environments. It provides FIPS 140-2 Level 2 TLS encryption of traffic to encrypt and secure communication between:

- Citrix Receiver and the NetScaler Gateway MPX FIPS hardware appliance
- The NetScaler Gateway MPX FIPS hardware appliance and Storefront, Delivery Controller, and VDA

StoreFront provides TLS encryption and secure communication between:

- Citrix Receiver and the XenApp and XenDesktop VDA (for the internal access deployment scenarios)
- Citrix Receiver and StoreFront (for the remote access deployment scenarios)
- Delivery Controller and StoreFront

Virtual Desktop Agent (VDA) runs on XenApp and XenDesktop and provides encryption and secure communication between:

- Citrix Receiver and the XenApp and XenDesktop VDA (for the internal access deployment scenarios)
- NetScaler Gateway MPX FIPS hardware appliance and the XenApp and/or XenDesktop VDA (for the remote access deployment scenarios)

XenApp, XenDesktop, and Storefront can be configured to use government approved cryptography to protect data by using the applicable cipher suites:

- TLS_ECHDE_RSA_WITH_AES_256_GCM_SHA384 supports ECDHE key agreement and 256-bit keys in GCM mode for TLS connections, as defined in FIPS 197 and RFC 5289.
- TLS_ECHDE_RSA_WITH_AES_128_GCM_SHA256 supports ECDHE key agreement and 128-bit keys in GCM mode for TLS connections, as defined in FIPS 197 and RFC 5289.
- TLS_ECHDE_RSA_WITH_AES_256_CBC_SHA384 supports ECDHE key agreement and 256-bit keys for TLS connections, as defined in FIPS 197 and RFC 5289.
- TLS_ECHDE_RSA_WITH_AES_128_CBC_SHA256 supports ECDHE key agreement and 128-bit keys for TLS connections, as defined in FIPS 197 and RFC 5289.
- TLS_RSA_WITH_AES_256_CBC_SHA supports RSA key exchange with AES and 256-bit keys forTLS connections, as defined in FIPS 197 and RFC 3268.
- TLS_RSA_WITH_AES_128_CBC_SHA supports RSA key exchange with Advanced Encryption Standard (AES) and 128-bit keys for TLS connections, as defined in FIPS 197 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf and Internet RFC 3268 (http://www.ietf.org/rfc/rfc3268.txt). For more information about AES, see http://csrc.nist.gov/cryptval/des.htm.
- TLS_RSA_WITH_3DES_EDE_CBC_SHA supports RSA key exchange and TripleDES encryption, as defined in Internet RFC 2246 (http://www.ietf.org/rfc/rfc2246.txt). Note that this cipher suite has been deprecated by NIST.

NetScaler Gateway MPX FIPS hardware appliances can be configured to use government-approved cryptography to protect data by using the applicable cipher suites:

- Cipher Name: SSL3-DES-CBC3-SHA [TLS_RSA_WITH_3DES_EDE_CBC_SHA]
- Cipher Name: TLS1-AES-256-CBC-SHA [TLS_RSA_WITH_AES_256_CBC_SHA]
- Cipher Name: TLS1-AES-128-CBC-SHA [TLS_RSA_WITH_AES_128_CBC_SHA]Cipher Name: TLS-1.2-ECDHE-RSA-AES-128-SHA256 [TLS_ECHDE_RSA_WITH_AES_128_CBC_SHA256]
- Cipher Name: TLS-1.2-ECDHE-RSA-AES-256-SHA384 [TLS_ECHDE_RSA_WITH_AES_256_CBC_SHA384]
- Cipher Name: TLS-1.2-ECDHE-RSA-AES-128-GCM-SHA256 [TLS_ECHDE_RSA_WITH_AES_128_GCM_SHA256]
- Cipher Name: TLS-1.2-ECDHE-RSA-AES-256-GCM-SHA384 [TLS_ECHDE_RSA_WITH_AES_256_GCM_SHA384]
- Note that 'SSL3-DES-CBC3-SHA' is relevant to TLS encryption (despite the reference to SSL3 in the cipher name).

Components of XenApp, XenDesktop, StoreFront, and NetScaler may support other cipher suites with government approved cryptography. These are not described in these deployment scenarios.

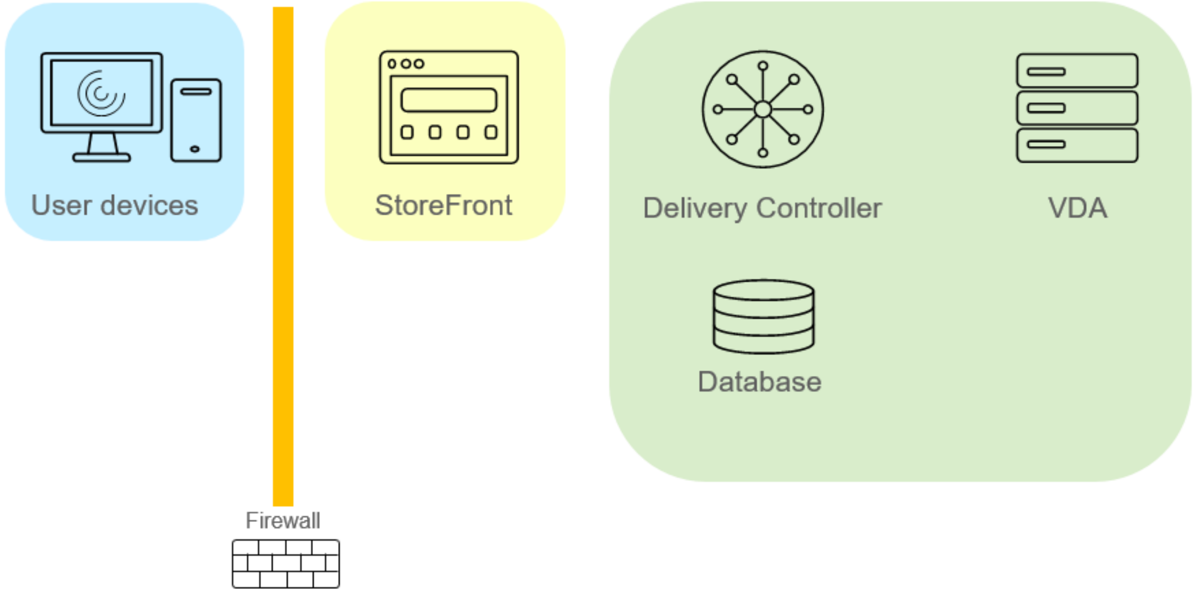
The following features and components are not within the scope of these FIPS 140-2 sample deployments:

- UDP-based features: UDP audio, FrameHawk, and Enlightened Data Transport (EDT)
- Linux VDA
- Federated Authentication Service (FAS)
- VMware SSL thumbprint

For more information and support regarding these deployment scenarios, including the operating system requirements, contact Technical Support or your Citrix partner.

XenApp (internal network)

This deployment provides end-to-end TLS encryption between the user device and the applications hosted on XenApp. The deployment includes Citrix Receiver, StoreFront, the Delivery Controller and the VDA.



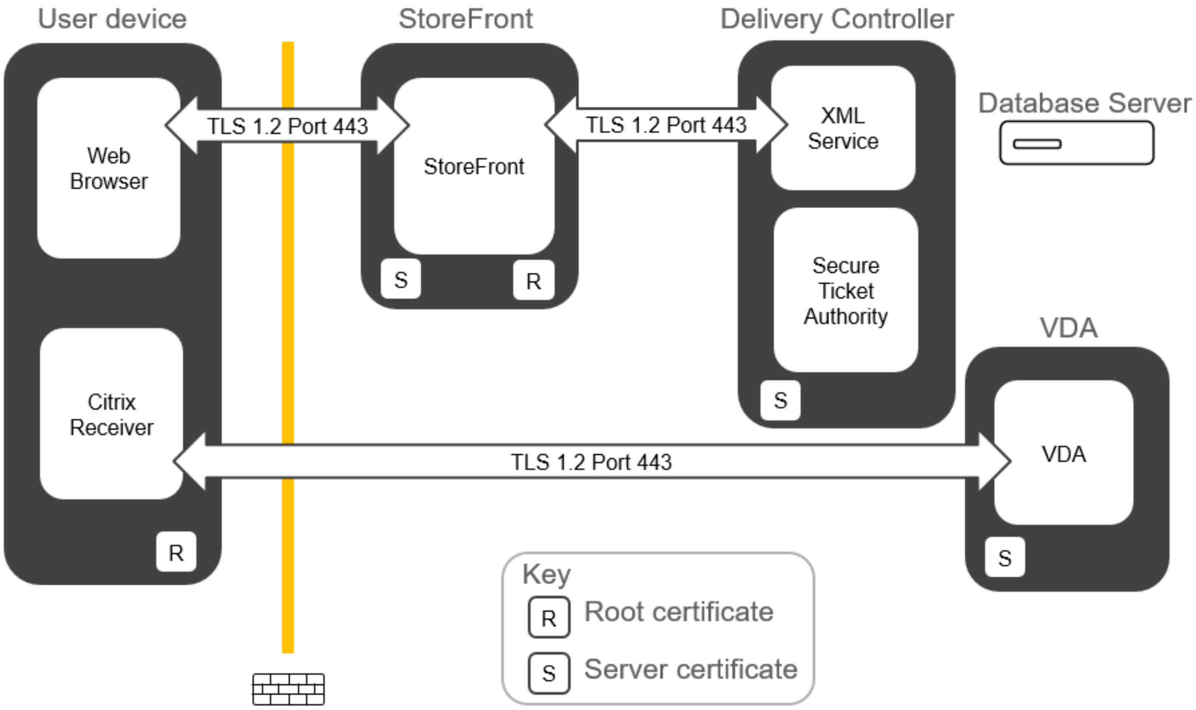
The following table lists the components of the deployment and the operating systems required for the servers and user devices.

	Product/Components	Operating System
XenApp	Delivery Controller (Secure Ticket Authority is part of the Desktop Controller)	Windows Server 2016
	XenApp VDA	Windows Server 2016
StoreFront	StoreFront 3.12	Windows Server 2016
User Devices	Citrix Receiver for Windows 4.9 TLS-enabled web browser	Windows 10 x64

How the components interact

Traffic between the web browser on the user device and StoreFront is secured using HTTPS. All other traffic is secured using TLS.

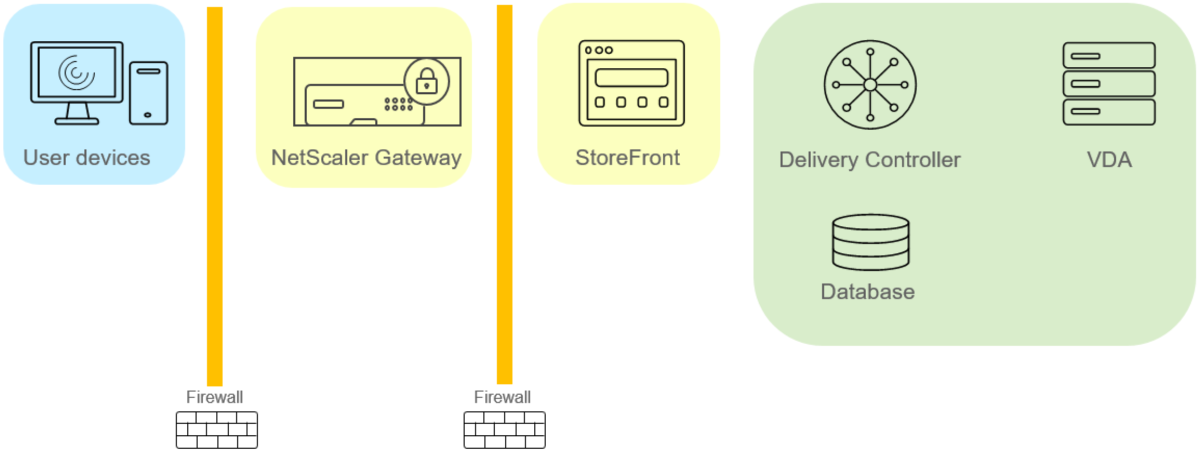
The diagram below shows a detailed view of the deployment including the components and certificates on each server, plus the communication and port settings.



The MS SQL database must be hosted on a dedicated server, and the connection between the database and Delivery Controller must be secured. For details regarding securing this link, see http://support.citrix.com/article/CTX137556.

XenApp using NetScaler Gateway MPX FIPS (external access)

The deployment includes Citrix Receiver, NetScaler Gateway MPX FIPS appliance, StoreFront, the Delivery Controller, and the VDA. The NetScaler Gateway MPX FIPS hardware appliance terminates the TLS/HTTPS connections from the user device (browser and Citrix Receiver). Traffic from the NetScaler Gateway MPX FIPS appliance through StoreFront, the Delivery Controller, and the VDA is secured using TLS.



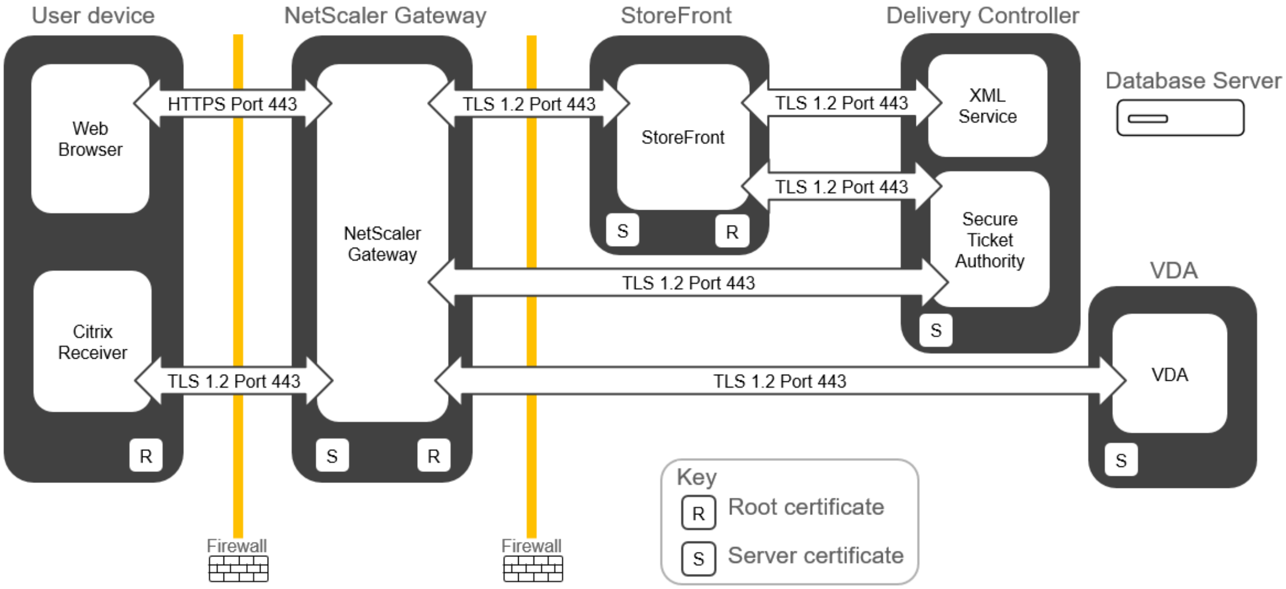
The following table lists the components of the deployment and the operating systems required for the servers and client devices.

Product/Components		Operating System
XenApp	Delivery Controller (Secure Ticket Authority is part of the Desktop Controller)	Windows Server 2016
	XenApp VDA	Windows Server 2016
NetScaler Gateway	NetScaler Gateway MPX FIPS hardware appliance 12	
StoreFront	StoreFront 3.12	Windows Server 2016
User Devices	Citrix Receiver for Windows 4.9 TLS-enabled web browser	Windows 10

How the components interact

Traffic between the web browser on the user device and NetScaler Gateway is secured using HTTPS. All other traffic is secured using TLS.

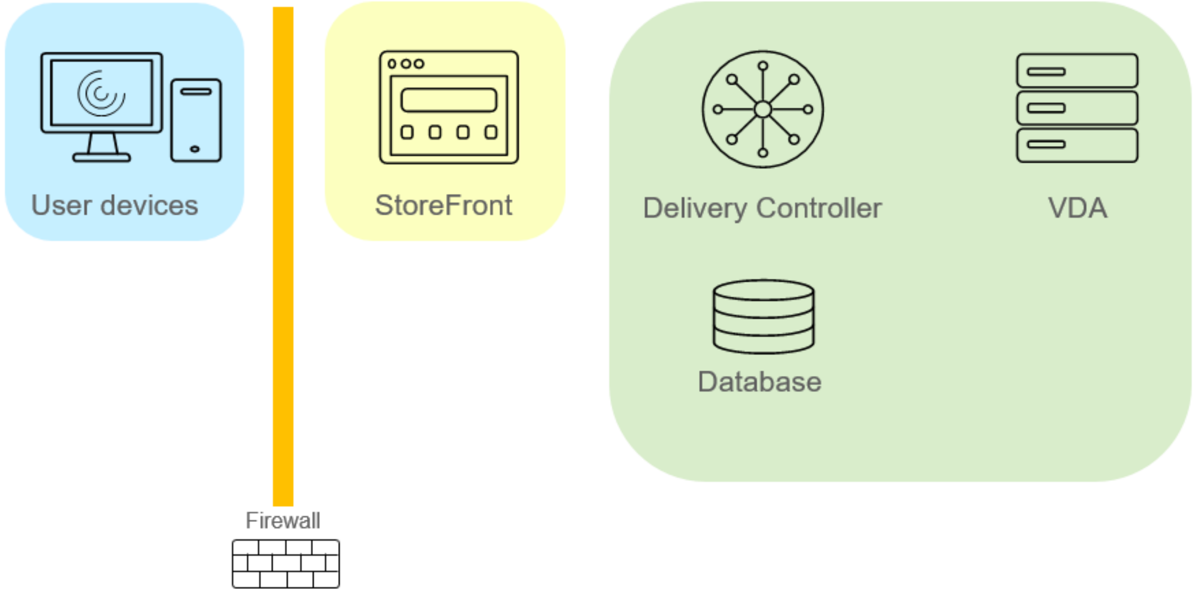
This diagram shows a detailed view of the deployment including the components and certificates on each server, plus the communication and port settings.



The MS SQL database must be hosted on a dedicated server, and the connection between the database and Delivery Controller must be secured. For details regarding securing this link, see http://support.citrix.com/article/CTX137556.

XenDesktop (internal network)

This deployment provides end-to-end TLS encryption between the user device and the resources hosted on XenDesktop. The deployment includes Citrix Receiver, StoreFront, the Delivery Controller, and the VDA.



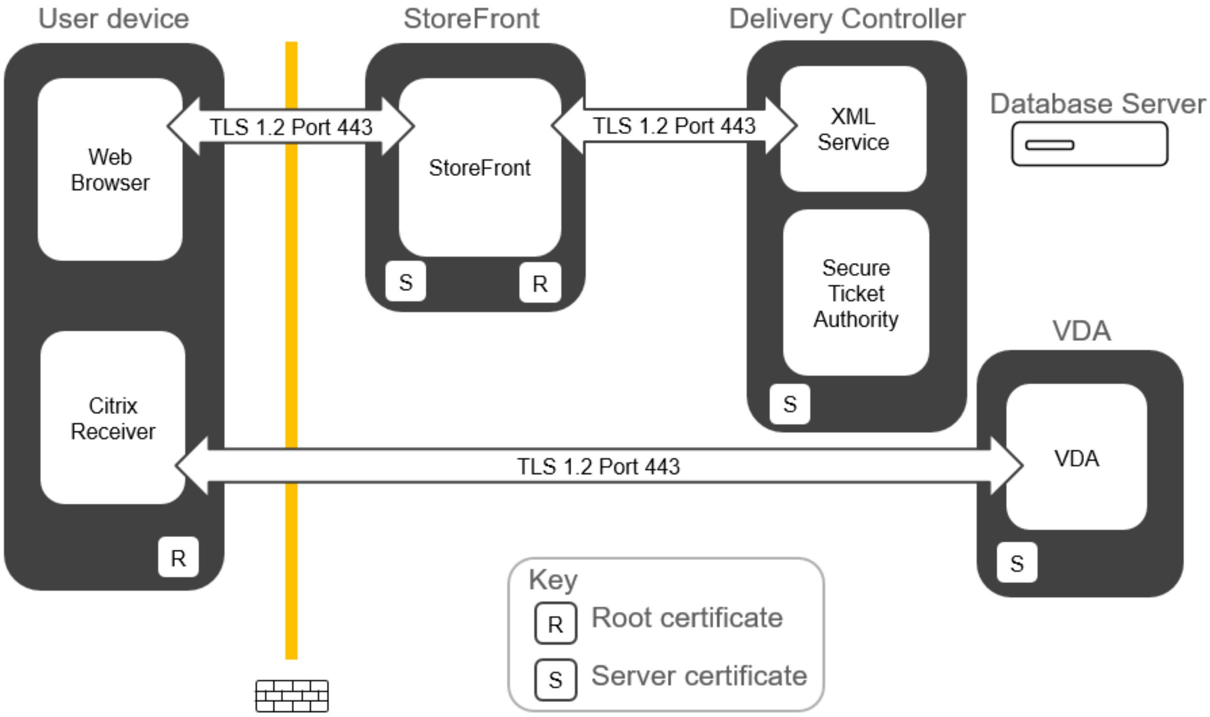
The following table lists the components of the deployment and the operating systems required for the servers and client devices.

	Product/Components	Operating System
XenDesktop	Delivery Controller (Secure Ticket Authority is part of the Desktop Controller) XenDesktop VDA	Windows Server 2016 Windows 10
StoreFront	StoreFront 3.12	Windows Server 2016
User Devices	Citrix Receiver for Windows 4.9 TLS-enabled web browser	Windows 10

How the components interact

Traffic between the web browser on the user device and StoreFront is secured using HTTPS. All other traffic is secured using TLS.

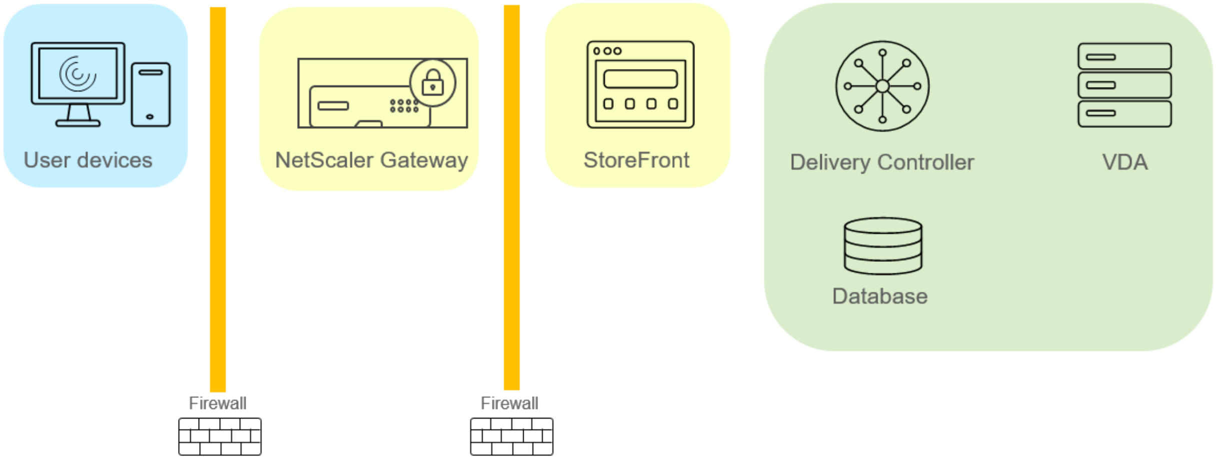
This diagram shows a detailed view of the deployment including the components and certificates on each server, plus the communication and port settings.



The MS SQL database must be hosted on a dedicated server and the connection between the database and Delivery Controller must be secured. For details regarding securing this link, see http://support.citrix.com/article/CTX137556.

XenDesktop using NetScaler Gateway MPX FIPS (external access)

The deployment includes Citrix Receiver, NetScaler Gateway MPX FIPS hardware appliance, StoreFront, the Delivery Controller, and the VDA. NetScaler Gateway terminates the TLS/HTTPS connections from the user device (browser and Citrix Receiver). Traffic from NetScaler Gateway through StoreFront, the Delivery Controller, and the VDA is secured using TLS.



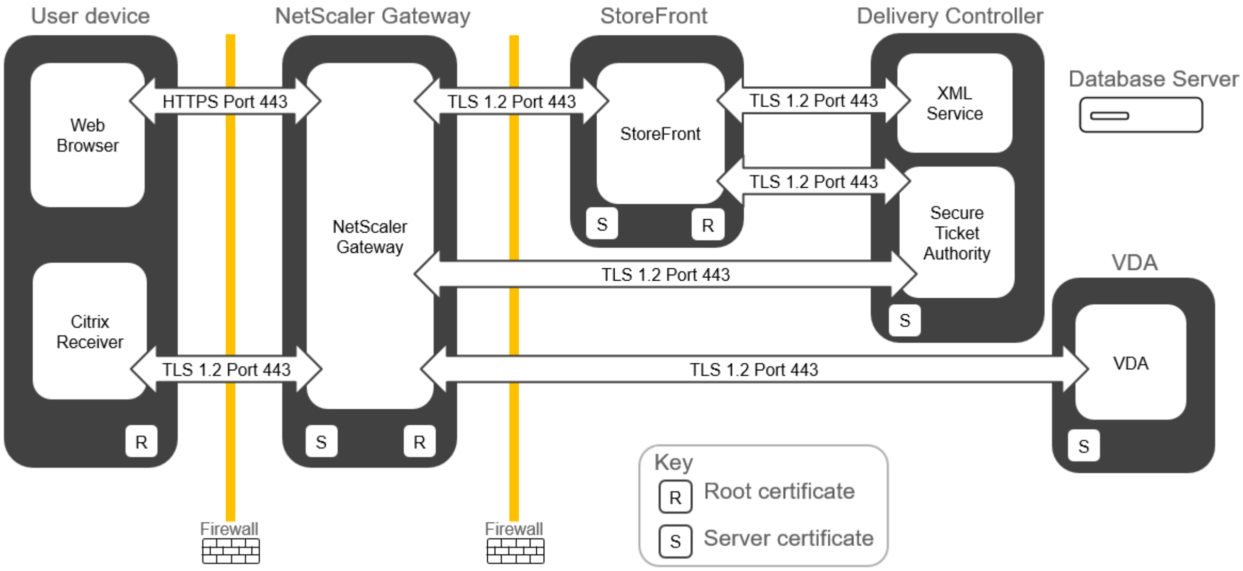
The following table lists the components of the deployment and the operating systems required for the servers and user devices.

	Product/Components	Operating System
XenDesktop	Delivery Controller (Secure Ticket Authority is part of the Desktop Controller)	Windows Server 2016
	XenDesktop VDA	Windows 10
NetScaler Gateway	NetScaler Gateway MPX FIPS hardware appliance 12.0	
StoreFront	StoreFront 3.12	Windows Server 2016
User Devices	Citrix Receiver for Windows 4.9 TLS-enabled web browser	Windows 10

How the components interact

Traffic between the web browser on the user device and NetScaler Gateway is secured using HTTPS. All other traffic is secured using TLS.

This diagram shows a detailed view of the deployment including where the components and certificates on each server, plus the communication and port settings.



The MS SQL database must be hosted on a dedicated server, and the connection between the database and Delivery Controller must be secured. For details regarding securing this link, see http://support.citrix.com/article/CTX137556.

Finding more information

For more information regarding the products, requirements, and specific procedures, please see:

- Product-specific content at the Citrix product documentation site (https://docs.citrix.com/).
- For more information about secure NetScaler Gateway deployments, see http://support.citrix.com/article/CTX129514.
- For more information regarding the XenApp and XenDesktop 7.15 LTSR FIPS support and features, see http://blogs.citrix.com/2014/10/16/xenapp-and-xendesktop-7-6-security-fips-140-2-and-ssl-to-vda/.
- For additional guidance regarding certificate management, see http://blogs.citrix.com/2014/12/11/how-to-secure-ica-connections-in-xenapp-and-xendesktop-7-6- using-ssl/ .
- The white paper “End to End Encryption with XenApp and XenDesktop” is available at https://www.citrix.com/content/dam/citrix/en_us/documents/white-paper/end-to-end-encryption-with-xenapp-and-xendesktop.pdf.

Product Documentation
docs.citrix.com

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale,
FL 33309, United States Silicon Valley | 4988 Great America
Parkway Santa Clara, CA 95054, United States