Citrix Presentation Server
Security Standards and Deployment Scenarios
Including Common Criteria Information

Citrix Presentation Server™ 4.5

Copyright and Trademark Notice

Trademark Acknowledgements

Document Code: August 20, 2007 (SC)

Contents

Introduction

About this Document

Citrix products offer the security specialist a wide range of features for securing a Citrix Presentation Server system.

When deploying Citrix Presentation Server 4.5 for Windows within large organizations and government environments, security standards are an important consideration. This document addresses common issues related to such environments.

This document provides an overview of the process of securing communications across a range of deployment models. Details of the individual security features are explained in the relevant product documentation.

Target Audience

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

Country-Specific Government Information

Sections of this document are of particular importance and relevance to certain countries as shown in the table below. If your country is not listed, contact your local Citrix representative.

Country	**Topic**	**See**
United States	FIPS 140 TLS Smart card support Smart card: Common Access Card Kerberos authentication	page 10 page 13 page 14 page 15 page 15

Country	Topic	See
Canada	FIPS 140 TLS Smart card support Kerberos authentication ITS Pre-qualified Product List (IPPL)	page 10 page 13 page 14 page 15 page 6
United Kingdom	FIPS 140 TLS Smart card support Kerberos authentication	page 10 page 13 page 14 page 15
Australia	FIPS 140 TLS Smart card support Kerberos authentication	page 10 page 13 page 14 page 15

For further information concerning issues specific to your country, contact your local Citrix representative.

Government of Canada ITS Pre-qualified Product List. Citrix Presentation Server 4.5 and 4.0, and MetaFrame XP with Feature Release 3 are pre-qualified by the Canadian Communications Security Establishment (CSE) under the Information Technology Security (ITS) Product Pre-qualification Program (IPPP).

The program is relevant to the Government of Canada procurement process and the Canadian Common Criteria Scheme. The program pre-qualifies ITS products for use within the Government of Canada and facilitates the procurement of ITS products by government departments.

Contact your Citrix representative for further details.

Finding More Information

For assistance with securing a Citrix Presentation Server deployment, the following documentation is available from the Citrix Knowledge Center. To find the Knowledge Center, go to the Support area of the Citrix Web site at http://www.citrix.com/.

- The *Citrix Presentation Server Administrator’s Guide* explains how to install and configure Citrix Presentation Server on Windows servers. Included in this documentation is information about publishing applications, configuring the Citrix XML Service, and configuring the Citrix SSL Relay to provide TLS/SSL-based communications.

- The *Web Interface Administrator's Guide* explains how to install and configure the Web Interface and provides information about securing Web Interface deployments using TLS/SSL-based communications.
- The *Secure Gateway for Windows Administrator's Guide* explains how to install and configure Secure Gateway to provide a secure Internet gateway for ICA traffic traveling into and out of servers in a farm running Citrix Presentation Server.
- The *Clients for Windows Administrator's Guide* explains how to install, configure, and deploy Citrix Presentation Server Clients for Windows. The guide includes a chapter about client security measures and features.
- The *Citrix Password Manager Administrator's Guide* explains how to install, configure and deploy Password Manager with Presentation Server. It includes details of enterprise security features such as integration with smart cards, Kerberos, and Federated Environment Support (ADFS and SAML).

What's New

Security features and enhancements included in Citrix Presentation Server 4.5 for Windows are described in the following sections.

Advanced Encryption Standard Support

Advanced Encryption Standard (AES) is a Federal Information Processing Standard (FIPS), specifically, FIPS Publication 197, that specifies a cryptographic algorithm for use by US Government organizations to protect sensitive, unclassified information.The Clients for Windows now support the AES cipher for connections using TLS.

Citrix Password Manager

Password Manager provides single sign-on access to any number of password-protected Windows-, Web-, and host-based applications published on computers running Presentation Server. Password Manager is included in the Platinum Edition of Presentation Server.

The Common Criteria target of evaluation for Presentation Server 4.5 includes Citrix Password Manager 4.5, Enterprise Edition. Throughout this guide, references are made to Password Manager where appropriate.

Security Considerations in a Citrix Presentation Server Deployment

Citrix Presentation Server provides server-based computing to local and remote users through the Independent Computing Architecture (ICA) developed by Citrix.

ICA is the communication protocol by which servers and client devices exchange data in a Citrix Presentation Server environment. ICA is optimized to enhance the delivery and performance of this exchange, even on low-bandwidth connections.

The ICA protocol transports an application's screens (and audio where relevant) from the server it is running on to the user's client device, and returns the user's input to the application on the server. As an application runs on a server, Citrix Presentation Server intercepts the application's display data and uses the ICA protocol to send this data (on standard network protocols) to the client software running on the user's client device.

When the user types on the keyboard or moves and clicks the mouse, the client software sends this data to the application on the server. ICA requires minimal client workstation capabilities and includes error detection and recovery, encryption, and data compression.

A server farm is a grouping of computers running Citrix Presentation Server that you can manage as a unit, similar in principle to a network domain. When designing server farms, you should keep in mind the goal of providing users with the fastest possible application access while achieving the degree of centralized administration and network security that you need.

In a Citrix Presentation Server deployment including the Web Interface, communication is conducted using both the ICA and HTTP protocols, among three different points: the computer running Citrix Presentation Server, a server running the Web Interface, and a client device with a Web browser and client.

In a Citrix Presentation Server deployment, you can configure encryption using either of the following:

- Citrix SSL Relay
- Secure Gateway

The Citrix SSL Relay component is integrated into Citrix Presentation Sever. The Secure Gateway is provided on the Citrix Presentation Server Components CD.

Common Criteria

Common Criteria certification is an internationally recognized standard for evaluating the security of IT products and systems. Common Criteria certification provides assurance that products were thoroughly and independently tested and validated against a set of requirements established by the worldwide International Standards Organization to ensure IT security.

For customers, especially US Federal and international government agencies, Common Criteria certification is an important requirement when procuring IT products and systems. Common Criteria certification is also applicable to private sector industries such as healthcare and financial.

Citrix Presentation Server 4.5 for Windows, Platinum Edition, and Citrix Password Manager 4.5 were evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL2.

For further details, see:

http://www.citrix.com/English/SS/supportThird.asp?slID=162512&tlID=162515

The following documents are available on the Web site:

- *Security Target for Citrix Presentation Server 4.5 for Windows*

  This document specifies the functional, environmental, and assurance evaluation requirements for Presentation Server 4.5.

- *Common Criteria Evaluated Configuration Guide, Citrix Presentation Server 4.5 for Windows*

  This document describes the requirements and procedures for installing and configuring Presentation Server in accordance with the Common Criteria-evaluated deployment.

  The Common Criteria-evaluated configuration is similar to sample deployment B.2 shown on page 27.

- *Common Criteria Certification Report, Citrix Presentation Server 4.5 for Windows*

  This report, prepared by the certification body (UK IT Security Evaluation and Certification Scheme Certification Body, CESG), states the outcome of the Common Criteria security evaluation.

- *Security Target for Citrix Password Manager 4.5*

  This document specifies the functional, environmental, and assurance evaluation requirements for Password Manager 4.5.

- *Common Criteria Evaluated Configuration Guide for Citrix Password Manager 4.5*

  This document explains how to install and configure Citrix Password Manager for use with the Common Criteria evaluated deployment. The procedures relating to Presentation Server 4.0 in this document are also valid for Presentation Server 4.5.

- *Common Criteria Certification Report, Citrix Password Manager 4.5*

  This report, prepared by the certification body (UK IT Security Evaluation and Certification Scheme Certification Body, CESG), states the outcome of the Common Criteria security evaluation.

FIPS 140 and Citrix Presentation Server

Federal Information Processing Standard 140 (FIPS 140) is a US federal government standard that details a benchmark for implementing cryptographic software. It provides best practices for using cryptographic algorithms, managing key elements and data buffers, and interacting with the operating system. An evaluation process that is administered by the National Institute of Standards and Technology's (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) allows encryption product vendors to demonstrate the extent to which they comply with the standard, and thus, the trustworthiness of their implementation.

Some US government organizations restrict purchases of products that contain cryptography to those that have FIPS 140-validated modules.

In the UK, according to CESG published guidance at http://www.cesg.gov.uk, where the required use is for information below RESTRICTED, but still sensitive; that is, PRIVATE, CESG recommends the use of FIPS 140-approved products.

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

To facilitate implementing secure application server access and to meet the FIPS 140 requirements, Citrix products can use cryptographic modules that are FIPS 140-validated in Windows 32-bit implementations of secure SSL/TLS connections.

The following Citrix Presentation Server components can use cryptographic modules that are FIPS 140-validated:

- Citrix Presentation Server Clients for Windows (including Program Neighborhood, Program Neighborhood Agent, and the Web Client)
- Secure Gateway for Windows
- Citrix Presentation Server
- Citrix SSL Relay
- Citrix Web Interface

When using the client and server components listed above with the SSL/TLS connection enabled, the cryptographic modules that are used are FIPS 140-validated. The cryptographic modules used are those provided by the Microsoft Windows operating system.

One government ciphersuite is RSA_WITH_3DES_EDE_CBC_SHA. As defined in Internet RFC 2246 http://www.ietf.org/rfc/rfc2246.txt, this ciphersuite uses RSA key exchange and TripleDES encryption.

This is achieved as follows. The information below is correct at the time of writing; see the Microsoft documents referred to below for more recent updates:

- According to the Microsoft information concerning the cryptographic provider types in the document http://msdn2.microsoft.com/en-us/library/aa380244.aspx, the only cryptographic provider type supporting RSA key exchange and TripleDES encryption is the PROV_RSA_SCHANNEL (Type 012) cryptographic provider type.
- By inspection of a particular configuration, the only cryptographic provider of this type is the Microsoft RSA Schannel Cryptographic Provider that is hosted in rsaenh.dll.
- According to the Microsoft document FIPS 140 Evaluation http://www.microsoft.com/technet/archive/security/topics/issues/fipseval.mspx, the protocols whose cryptographic processing take advantage of the components that completed FIPS-140-1 evaluation include the SSL protocol that is used between a Web browser (Internet Explorer) and a Web server (Internet Information Server);

- The Microsoft document lists the following supported and FIPS-validated cryptographic algorithm implementations of Microsoft Windows operating system platforms:

FIPS-46-3 DES (ECB, CBC)	Windows XP, Server 2003 rsaenh.dll and dssenh.dll, Windows XP, Server 2003 fips.sys
FIPS-46-3 3DES (ECB, CBC)	Windows XP, Server 2003 rsaenh.dll and dssenh.dll, Windows XP, Server 2003 fips.sys
FIPS-197 AES-128, -192, -256 (ECB, CBC)	Windows XP SP1, Windows Server 2003 rsaenh.dll
FIPS-186-2 DSA	Windows XP, Server 2003 dssenh.dll
FIPS-186-2 RSA	Windows XP, Server 2003 rsaenh.dll
FIPS-180-2 SHA-1	Windows XP, Server 2003 rsaenh.dll and dssenh.dll, Windows XP, Server 2003 fips.sys
FIPS-198 HMAC-SHA-1	Windows XP, Server 2003 rsaenh.dll, Windows XP, Server 2003 fips.sys

Given the accuracy of the above statements and assuming the system is configured as described above, the resulting Citrix configuration would use FIPS 140-validated cryptomodules.

For a list of currently validated FIPS 140 modules, see the NIST Web site at: http://csrc.nist.gov/cryptval/140-1/1401val.htm.

For additional details regarding FIPS 140 and NIST, visit the NIST site at: http://csrc.nist.gov/cryptval/.

Alternatively, for TLS connections, you can use AES as defined in FIPS 197. The government ciphersuites are RSA_WITH_AES_128_CBC_SHA for 128-bit keys, or RSA_WITH_AES_256_CBC_SHA for 256-bit keys. As defined in Internet RFC 3268 http://www.ietf.org/rfc/rfc3268.txt, these ciphersuites use RSA key exchange and AES encryption. For further information on AES, visit the NIST WEb site at http://csrc.nist.gov/cryptval/des.htm.

TLS/SSL

Secure Socket Layer (SSL) is an open, nonproprietary protocol that provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. Where SSL is used to secure communications between clients and servers within the server farm, the Citrix SSL Relay is required at each server within each farm. Alternatively, you can use the Secure Gateway. Both solutions are discussed in this document.

Transport Layer Security (TLS) is the latest, standardized version of the SSL protocol. TLS is an open standard and like SSL, TLS provides server authentication, encryption of the data stream, and message integrity checks. The Citrix SSL Relay, described above, supports TLS and you can configure the SSL Relay, the Secure Gateway, and the Web Interface to use TLS. Support for TLS Version 1.0 is included in Citrix Presentation Server 4.5 for Windows and in Citrix Password Manager 4.5.

Because there are only minor differences between SSL and TLS, the server certificates in your installation can be used for both SSL and TLS purposes.

Government Ciphersuites

You can configure Citrix Presentation Server, the Web Interface, and the Secure Gateway to use government-approved cryptography to protect “sensitive but unclassified” data.

For RSA key exchange and TripleDES encryption, the government ciphersuite is RSA_WITH_3DES_EDE_CBC_SHA.

Alternatively, for TLS connections, you can use AES as defined in FIPS 197. The government ciphersuites are RSA_WITH_AES_128_CBC_SHA for 128-bit keys, or RSA_WITH_AES_256_CBC_SHA for 256-bit keys.

IP Security

IP Security (IPSec) is a set of standard extensions to the Internet Protocol (IP) that provides authenticated and encrypted communications with data integrity and replay protection. IPSec is a network-layer protocol set, so higher level protocols such as Citrix ICA can use it without modification.

Although such deployment scenarios are not within the scope of this document, you can use IPSec to secure a Citrix Presentation Server deployment within a virtual private network (VPN) environment.

IPSec is described in Internet RFC 2401.

Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Server 2003, and Microsoft Windows Vista have built-in support for IPSec.

Smart Cards

You can use smart cards with Presentation Server, supported Presentation Server Clients, the Web Interface, and Password Manager, to provide secure access to applications and data. Using smart cards simplifies the authentication process while enhancing logon security. Presentation Server supports smart card authentication to published applications, including “smart card enabled” applications such as Microsoft Outlook.

In a business network, smart cards are an effective implementation of public-key technology and can be used to:

- Authenticate users to networks and computers
- Secure channel communications over a network
- Use digital signatures for securing content

If you are using smart cards for secure network authentication, your users can authenticate to applications and content published on your server farms. In addition, smart card functionality within these published applications is also supported.

For example, a published Microsoft Outlook application can be configured to require that users insert a smart card into a smart card reader attached to the client device to log on to a computer running Citrix Presentation Server. After users are authenticated to the application, they can digitally sign email using certificates stored on their smart cards.

Citrix supports the use of Personal Computer Smart Card (PC/SC) based cryptographic smart cards. These cards include support for cryptographic operations such as digital signatures and encryption. Cryptographic cards are designed to allow secure storage of private keys such as those used in Public Key Infrastructure (PKI) security systems. These cards perform the actual cryptographic functions on the smart card itself, meaning the private key and digital certificates never leave the card. In addition, you can use two-factor authentication for increased security. Instead of merely presenting the smart card (one factor) to conduct a transaction, a user-defined PIN (a second factor), known only to the user, is used to prove that the cardholder is the rightful owner of the smart card.

Smart Card Support

Citrix continues testing various smart cards to address smart card usage and compatibility issues with Citrix Presentation Server.

Citrix Presentation Server fully supports the Common Access Card in a deployment that includes the Clients for Windows. Contact your Common Access Card vendor or Citrix representative about supported versions of Common Access Card hardware and software.

Citrix tests smart cards using certificates from common certificate authorities such as those supported by Microsoft. If you have any concerns regarding your certificate authority and compatibility with Citrix Presentation Server, contact your local Citrix representative.

Kerberos Authentication

Kerberos is an authentication protocol. Version 5 of this protocol is standardized as Internet RFC 1510. Many operating systems, including Microsoft Windows 2000 and later, support Kerberos as a standard feature.

Citrix Presentation Server extends the use of Kerberos. After users log on to a client device, they can connect to Citrix Presentation Server without needing to authenticate again. The user's password is not transmitted to Presentation Server; instead, authentication tokens are exchanged using the Generic Security Services API (GSSAPI) standardized in Internet RFC 1509.

This authentication exchange is performed within a Citrix ICA virtual channel and does not require any additional protocols or ports. The authentication exchange is independent of the logon method, so it can be used with passwords, smart cards, or biometrics.

To use Kerberos authentication with Citrix Presentation Server, client and server must be appropriately configured. You can also use Microsoft Active Directory Group Policy selectively to disable Kerberos authentication for specific users and servers.

Citrix Presentation Server Clients

Users access applications running on server farms using Citrix Presentation Server Client software installed on their client devices. ICA lets virtually any type of client device access applications over any type of network connection, including LAN, WAN, dial-up, and direct asynchronous connections. Because ICA does not download applications to client devices (as in the Network Computing architecture), application performance is not limited by bandwidth or device performance.

Citrix Presentation Server Clients are available for Windows, Macintosh, UNIX, Linux, Symbian, Windows CE, DOS, and Java operating systems. Additionally, you can use the Web Client (Win32) with Web browsers that support ActiveX controls or Netscape plug-ins.

As described earlier, Citrix Presentation Server Clients for Windows use cryptographic modules provided by the Microsoft Windows operating system. Other clients, including the Citrix Presentation Server Client for Java, contain their own cryptographic modules. The Client for Java can, therefore, be used on older Microsoft Windows operating systems that are not upgraded to support strong encryption.

The following table lists the latest versions of the available clients and details whether or not each client is FIPS 140-compliant, supports TLS, includes smart card support, uses government ciphersuites, supports certificate revocation checking, and supports Kerberos authentication. Note that certificate revocation checking is applicable to clients running on Windows 2000 and Windows XP only. Where the latest version of a client does not completely supersede a previous version (for example, a particular operating system may be supported only by an earlier client version), the earlier version of the client is also listed.

Certificates

	FIPS 140	TLS support	Government Ciphersuite (TripleDES)	Government Ciphersuite (AES)	Certificate revocation checking	Smart card support	Kerberos authentication support
Program Neighborhood (Win32) Version 10.*x*	▶	▶	▶	▶	▶	▶	▶
Program Neighborhood Agent (Win32) Version 10.*x*	▶	▶	▶	▶	▶	▶	
Web Client (Win32) Version 10.*x*	▶	▶	▶	▶	▶	▶	▶
Client for Windows CE WBT Version 10.*x*		▶	▶			▶	
Client for Pocket PC Version 10.*x*		▶	▶			▶	
Client for Java Version 9.*x* [1]		▶	▶	▶	▶		▶
Client for Macintosh Version 7.0 (for Mac OS 10.2)		▶	▶				
Client for Macintosh Version 8.*x*		▶	▶			▶	▶
Client for Win16 Version 6.20							
Client for Linux Version 10.*x*		▶	▶			▶	
Client for UNIX (Sun Solaris) Version 8.*x*		▶	▶			▶	
Client for UNIX (IBM AIX) Version 6.30		▶	▶			▶	
Client for UNIX (SGI IRIX) Version 6.0							
Client for UNIX (HP-UX) Version 6.30		▶	▶				
Client for OS/2 Version 6.012							
Client for Nokia 9200 Series Communicator							
Client for FOMA M1000, Version 4.*x*		▶					
Client for Symbian Series 60 3rd Edition, Version 4.*x*		▶					
Client for Symbian Series 80, Version 4.*x*		▶					

[1] Kerberos authentication is not supported when the Client for Java is running on Mac OS X client devices

The table below details the certificate source for clients that support at least one of the security features shown in the table above.

	Root certificate source (OS or Client)
Program Neighborhood (Win32) Version 10.*x*	OS
Program Neighborhood Agent (Win32) Version 10.*x*	OS
Web Client (Win32) Version 10.*x*	OS
Client for Windows CE WBT Client Version 10.*x*	OS
Client for Pocket PC Version 10.*x*	OS
Client for Java Version 8.*x*	Client (or JRE)
Client for Java Version 9.*x*	JRE when using JRE 1.4.*x* JRE or OS when using JRE 1.5.*x* or later versions of the JRE
Client for Macintosh Version 7.0	Client
Client for Macintosh Version 8.*x*	OS
Client for Linux Version 10.*x*	Client
Client for UNIX (Sun Solaris) Version 8.*x*	Client
Client for UNIX (IBM AIX) Version 6.30	Client
Client for UNIX (HP-UX) Version 6.30	Client
Client for FOMA M1000, Version 4.*x*	OS
Client for Symbian Series 60 3rd Edition, Version 4.*x*	OS
Client for Symbian Series 80, Version 4.*x*	OS

Clients marked with OS use certificates stored in the operating system certificate store. Clients marked with Client use certificates bundled with the client. Clients include native support for the following certificate authorities:

- VeriSign, Inc., http://www.verisign.com/
- Cybertrust, http://www.cybertrust.com/

Government organizations may use a different certificate authority. If so, you must install the root certificate for the certificate authority on each client device.

The root certificates used by the Client for Java depend on the environment. When running in the Microsoft JVM environment, the client uses root certificates bundled with the client or root certificates provided by the archive file on the Web server.

Note The Microsoft JVM environment is supported by the Client for Java Version 8.*x*, but not by subsequent versions.

When running in the Java 2 environment, the client uses root certificates in the Java Runtime Environment (JRE) Java keystore.

Virtual Channels

Note that this section relates only to Presentation Server, not to Password Manager.

The following table illustrates which ICA virtual channels or combination of virtual channels can be used for authentication and application signing/encryption methods.

	Smart card virtual channel	**Kerberos virtual channel**	**Core ICA protocol (no virtual channel)**
Authentication method			
Smart card	▶	▶	
Biometric		▶ *	
Password		▶	▶
Application signing/encryption	▶		

* Third party equipment is required for biometric authentication.

Additional Citrix Presentation Server Security Features

All the security features described in this section, apart from Secure Computing SafeWord, support both Presentation Server and Password Manager. However, they are not discussed in this document and are not included in any of the example deployment scenarios. For details concerning these features, see the relevant product documentation.

Web Interface RSA SecurID Authentication

You can use RSA SecurID as an authentication method for the Web Interface running on Windows servers. If enabled, users must log on using their credentials (user name, password, and domain) plus their PASSCODE. The PASSCODE comprises a PIN (Personal Identification Number) followed by the RSA SecurID tokencode (the number displayed on the RSA SecurID token).

Web Interface Secure Computing SafeWord Authentication

You can use Secure Computing SafeWord as an authentication method for the Web Interface running on Windows servers. If enabled, users must log on using their credentials (user name, password, and domain) plus their SafeWord passcode. The passcode comprises the code displayed on their SafeWord token plus (optionally) a PIN (Personal Identification Number).

Note SafeWord does not support Password Manager.

ICA Encryption (SecureICA)

ICA encryption (SecureICA) is integrated into Citrix Presentation Server. You can use SecureICA (128-bit encryption) to protect the information sent between a computer running Citrix Presentation Server and clients.

SecureICA does not use FIPS 140-compliant algorithms. You can configure clients and computers running Citrix Presentation Server to avoid using SecureICA.

Sample Deployments

Both Citrix SSL Relay and Secure Gateway are capable of supporting TLS-based and SSL-based encryption. Selection is largely a matter of deciding which topology best meets the needs of the organization's security policies. Each approach has its own advantages and the relative merits of the two are best illustrated by considering the following sample deployment models:

Sample Deployment A. Using Citrix SSL Relay to provide end-to-end TLS/SSL encryption between a computer running Citrix Presentation Server and a client device.

Sample Deployment B. Using Secure Gateway in the single-hop deployment to provide TLS/SSL encryption between a secure Internet gateway server and an SSL-enabled client, combined with encryption of the HTTP communication between the Web browser and the Web server. Additionally, you can secure ICA traffic within the internal network using IPSec.

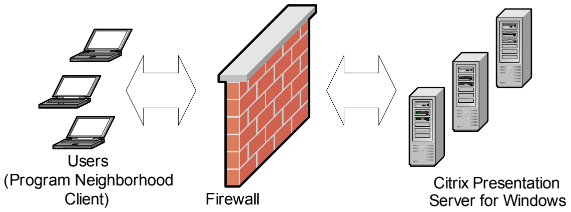
Sample Deployment C. Using Secure Gateway in the double-hop deployment to provide TLS/SSL encryption between a secure Internet gateway server and an SSL-enabled client, combined with encryption of the HTTP communication between the Web browser, Web Interface, and Secure Gateway proxy. Additionally, you can secure ICA traffic within the internal network using IPSec.

Sample Deployment D. Using SSL Relay with the Web Interface to encrypt the ICA and HTTP communication between the computer running Citrix Presentation Server and the server running the Web Interface, combined with encryption of the HTTP communication between the Web browser and the Web server.

Sample Deployment E. Using Password Manager and Secure Gateway in the single-hop deployment to enable single sign-on and TLS/SSL encryption between a secure Internet gateway server and an SSL-enabled client, combined with encryption of the HTTP communication between the Web browser and the Web server. Additionally, you can secure ICA traffic within the internal network using IPSec.

Sample Deployment A - Using SSL Relay

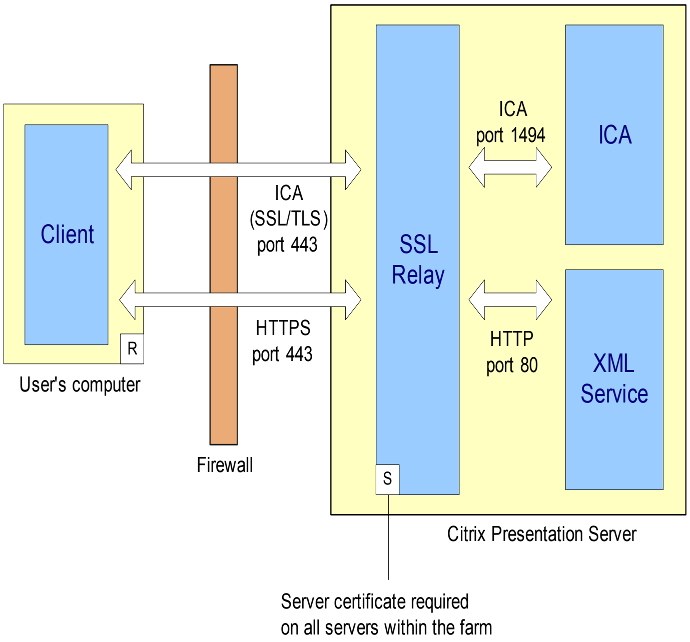
The computers running Citrix Presentation Server in sample deployment A comprise Citrix Presentation Server 4.5 for Windows on Microsoft Windows Server 2003 with Terminal Services. Users in deployment A are running the Program Neighborhood Client (32-bit Windows, Version 10.*x*).



This diagram shows Sample Deployment A using SSL Relay

How the Components Interact

You use TLS/SSL to secure the connection between a client and the computer running Citrix Presentation Server. To do this, you deploy TLS/SSL-enabled clients and configure SSL Relay on the computer running Citrix Presentation Server.



This diagram shows a detailed view of Sample Deployment A

This deployment provides end-to-end encryption of the communication between the client and the server. Both SSL Relay and the appropriate server certificate must be installed and configured on each server within the server farm.

The SSL Relay operates as an intermediary in the communications between the client and the XML Service at each server. Each client authenticates the SSL Relay by checking the SSL Relay's server certificate against a list of trusted certificate authorities. After this authentication, the client and SSL Relay negotiate requests in encrypted form. The SSL Relay decrypts the requests and passes them to the server. When returning the information to the client, the server sends all information through the SSL Relay, which encrypts the data and forwards it to the client to be decrypted. Message integrity checks verify each communication was not tampered with.

FIPS 140 Validation

In sample deployment A, the SSL Relay uses the Microsoft Cryptographic Service Providers (CSPs) and associated cryptographic algorithms available in the Microsoft Windows CryptoAPI to encrypt/decrypt communication between client and server. Direct questions regarding the FIPS 140 validation of the CSPs to Microsoft Corporation.

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL support and supported ciphersuites can also be controlled by the following Microsoft security option:

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing. Refer to Microsoft product documentation for details.

TLS/SSL Support

You can configure Citrix Presentation Server to use either the Transport Layer Security (TLS) protocol 1.0 or the Secure Sockets Layer (SSL) protocol 3.0. In sample deployment A, the components are configured for TLS. For details about configuring TLS, see the:

- *Citrix Presentation Server Administrator's Guide* and the online application help for the SSL Relay Configuration tool. When using the SSL Relay Configuration tool, ensure that **TLS** is selected at the **Connection** tab.
- *Client for Windows Administrator's Guide*

Supported Ciphersuites

In sample deployment A, you configure Citrix Presentation Server to use government-approved cryptography to protect "sensitive but unclassified" data. One government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

- *Citrix Presentation Server Administrator's Guide* and the online application help for the SSL Relay Configuration tool. When using the SSL Relay Configuration tool, ensure that only **GOV** is selected at the **Ciphersuite** tab.
- *Client for Windows Administrator's Guide*

Alternatively, for TLS connections, you can use AES as defined in FIPS 197. The government ciphersuites are RSA_WITH_AES_128_CBC_SHA for 128-bit keys, or RSA_WITH_AES_256_CBC_SHA for 256-bit keys. As defined in Internet RFC 3268 http://www.ietf.org/rfc/rfc3268.txt, these ciphersuites use RSA key exchange and AES encryption. For further information on AES, visit the NIST WEb site at http://csrc.nist.gov/cryptval/des.htm.

Certificates and Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment A, you configure a separate server certificate for each server on which you use the SSL Relay. A root certificate is required for each client. For further details, see the *Citrix Presentation Server Administrator's Guide*.

Smart Card Support

In sample deployment A, you can configure Citrix Presentation Server to provide smart card authentication. To do this, you must configure authentication using the Microsoft Active Directory and use the Microsoft Certificate Authority.

For more information, see the latest version of the *Advanced Concepts Guide for Citrix Presentation Server*, available from the Citrix Web site.

Clients

The Program Neighborhood Client is used in sample deployment A. For details concerning the security features and capabilities of Citrix Presentation Server Clients, see “Citrix Presentation Server Clients” on page 16.

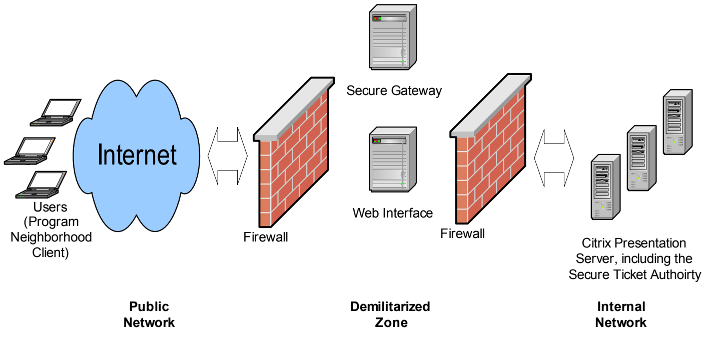
Sample Deployment B - Using Secure Gateway (Single-Hop)

The computers running Citrix Presentation Server in sample deployment B comprise Citrix Presentation Server 4.5 for Windows on Microsoft Windows Server 2003 with Terminal Services. Citrix SSL Relay is enabled. The Secure Ticket Authority (STA) is automatically installed on the server running Citrix Presentation Server.

The server running the Web Interface in sample deployment B comprises the Citrix Web Interface on Microsoft Windows Server 2003, with Microsoft Internet Information Services Version 6.0 or later.

The Secure Gateway and the Secure Ticket Authority in sample deployment B are both running on Microsoft Windows Server 2003.

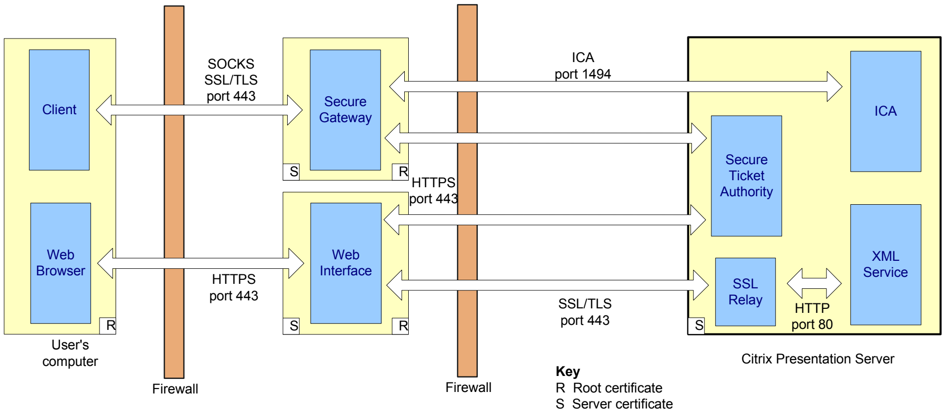
Users in deployment B are running a TLS-enabled Web browser and the Program Neighborhood Client (32-bit Windows, Version 10.*x*).


Internet
Users (Program Neighborhood Client)
Firewall
Secure Gateway
Web Interface
Firewall
Citrix Presentation Server, including the Secure Ticket Authoirty
Public Network
Demilitarized Zone
Internal Network

This diagram shows Sample Deployment B using the Secure Gateway

How the Components Interact

You use TLS to secure the connection between a client and the Secure Gateway. To do this, you deploy TLS/SSL-enabled clients and deploy the Secure Gateway at the network perimeter, typically in a demilitarized zone (DMZ). You secure the connection between the Web browser and the Web Interface using HTTPS. Additionally, you secure communication between the Web Interface and Citrix Presentation Server using TLS.



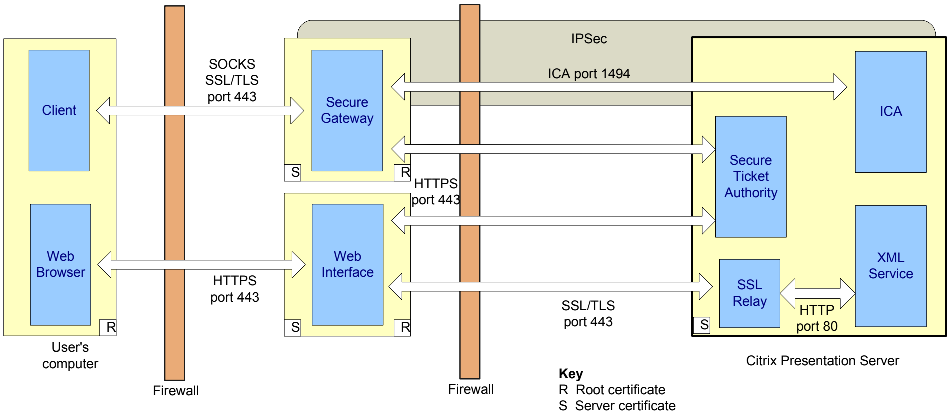
This diagram shows a detailed view of Sample Deployment B.1, which uses SSL Relay

In sample deployment B, the Secure Gateway removes the need to publish the addresses of every computer running Citrix Presentation Server, and allows a single point of encryption and access to the Citrix servers. It does this by providing a gateway that is separate from the computers running Citrix Presentation Server and reduces the issues for firewall traversal to a widely accepted port for ICA traffic in and out of firewalls.

Set against the increased scalability of sample deployment B is the fact that ICA communication is encrypted only between the client and the gateway. ICA communication between the gateway and Citrix Presentation Server is not encrypted.

Note that the SSL Relay in sample deployment B.1 is used to encrypt communication between the Web Interface and the XML Service running on Citrix Presentation Server. The Secure Gateway communicates with Citrix Presentation Server directly (the SSL Relay is not used for Secure Gateway to Citrix Presentation Server communication).

To achieve FIPS 140, you can secure the communication between the Secure Gateway and Citrix Presentation Server using IPSec. This is illustrated in the next diagram.



This diagram shows a detailed view of Sample Deployment B.2, which uses IPSec

IPSec

To enable IPSec to secure communication between the Secure Gateway and the computers running Citrix Presentation Server, you must configure IPSec for the following servers:

- Secure Gateway
- All the computers running Citrix Presentation Server

IPSec is configured using the Local Security Settings (IP Security Policies) for each server. In deployment B.2, IPSec is enabled on the required servers and the security method is configured for 3DES encryption and SHA-1 integrity to meet FIPS 140 requirements.

FIPS 140 Validation

In sample deployment B, the Citrix SSL Relay uses the Microsoft Cryptographic Service Providers (CSPs) and associated cryptographic algorithms available in the Microsoft Windows CryptoAPI to encrypt/decrypt communication between client and server. Direct questions regarding the FIPS 140 validation of the CSPs to Microsoft Corporation.

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL support and supported ciphersuites can also be controlled by the following Microsoft security option:

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing. Refer to Microsoft product documentation for details.

TLS/SSL Support

In sample deployment B, you can configure Secure Gateway and the Web Interface to use either the Transport Layer Security (TLS) protocol 1.0 or the Secure Sockets Layer (SSL) protocol 3.0. In sample deployment B, the components are configured for TLS.

For details about configuring TLS, see the:

- *Web Interface Administrator's Guide*
- *Secure Gateway for Windows Administrator's Guide*
- *Clients for Windows Administrator's Guide*

Supported Ciphersuites

In sample deployment B, you configure Secure Gateway and the Web Interface to use government-approved cryptography to protect "sensitive but unclassified" data. One government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

- *Secure Gateway for Windows Administrator's Guide*
- *Clients for Windows Administrator's Guide*

Alternatively, for TLS connections, you can use AES as defined in FIPS 197. The government ciphersuites are RSA_WITH_AES_128_CBC_SHA for 128-bit keys, or RSA_WITH_AES_256_CBC_SHA for 256-bit keys. As defined in Internet RFC 3268 http://www.ietf.org/rfc/rfc3268.txt, these ciphersuites use RSA key exchange and AES encryption. For further information on AES, visit the NIST WEb site at http://csrc.nist.gov/cryptval/des.htm.

Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment B, you configure one server certificate on the Secure Gateway, and one on the Web Interface. You also configure a certificate on each computer running Citrix Presentation Server. For further details, see the relevant Administrator's Guides.

Smart Card Logon

In sample deployment B, you can configure Citrix Presentation Server to provide smart card authentication. To do this, you must configure authentication using the Microsoft Active Directory and use the Microsoft Certificate Authority.

For more information, see the latest version of the *Advanced Concepts Guide for Citrix Presentation Server* available from the Citrix Web site.

Clients

The Program Neighborhood Client is used in sample deployment B.

For details about the security features and capabilities of Citrix Presentation Server Clients, see “Citrix Presentation Server Clients” on page 16.

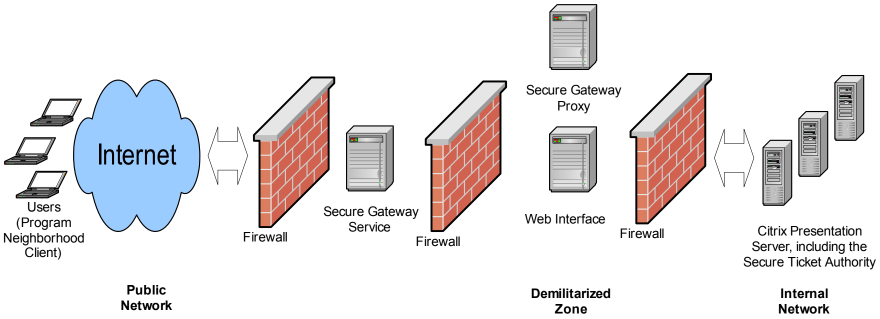
Sample Deployment C - Using Secure Gateway (Double-Hop)

The computers running Citrix Presentation Server in sample deployment C comprise Citrix Presentation Server 4.5 for Windows on Microsoft Windows Server 2003 with Terminal Services. Citrix SSL Relay is enabled. The STA is automatically installed on the server running Citrix Presentation Server.

The server running the Web Interface in sample deployment C comprises the Web Interface for Citrix Presentation Server, on Microsoft Windows Server 2003, with Microsoft Internet Information Services Version 6.0 or later.

The Secure Gateway Service and the Secure Gateway proxy in sample deployment C are running on Microsoft Windows Server 2003.

Users in deployment C are running a TLS-enabled Web browser and the Program Neighborhood Client (32-bit Windows, Version 10.*x*).

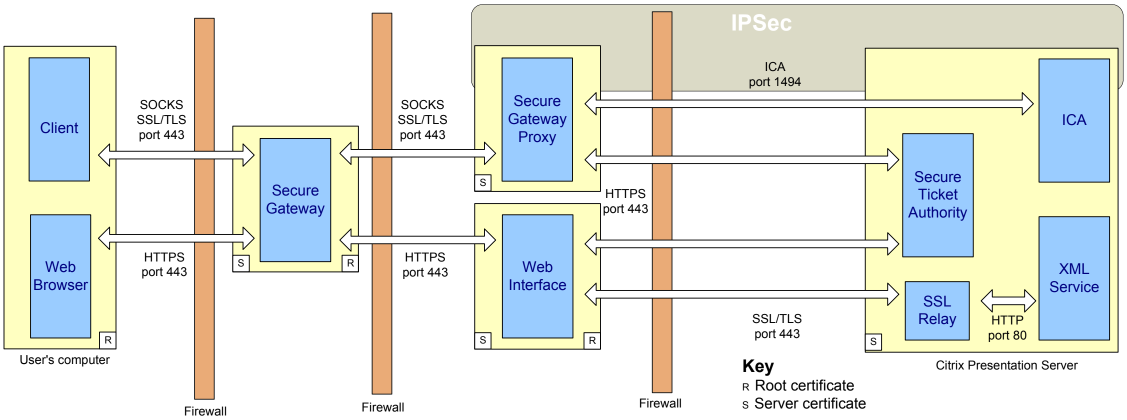


This diagram shows Sample Deployment C, which uses Secure Gateway (double hop) and IPSec

How the Components Interact

In sample deployment C, the demilitarized zone (DMZ) is divided into two segments. The Secure Gateway Service is located in the first hop of the DMZ. The Web Interface and Secure Gateway proxy are located in the second hop of the DMZ. Users connect to the Secure Gateway server in the first hop DMZ.

You use TLS to secure the connection between a client and the Secure Gateway. To do this, you deploy TLS/SSL-enabled clients and deploy the Secure Gateway at the network perimeter, typically in a DMZ.



This diagram shows a detailed view of Sample Deployment C

In sample deployment C, the Secure Gateway removes the need to publish the addresses of every computer running Citrix Presentation Server and allows a single point of encryption and access to the Citrix servers. It does this by providing a gateway that is separate from the computers running Citrix Presentation Server and reduces the issues for firewall traversal to a widely accepted port for ICA traffic in and out of firewalls.

To achieve FIPS 140, you can secure communication between the Secure Gateway proxy and computers running Citrix Presentation Server using IPSec.

IPSec

To enable IPSec to secure communication between the Secure Gateway proxy and computers running Citrix Presentation Server, you must configure IPSec for the following servers:

- Secure Gateway proxy
- All computers running Citrix Presentation Server

IPSec is configured using the Local Security Settings (IP Security Policies) for each server. In deployment C, IPSec is enabled on the required servers and the security method is configured for 3DES encryption and SHA-1 integrity to meet FIPS 140 requirements.

FIPS 140 Validation

In sample deployment C, the Citrix SSL Relay uses the Microsoft Cryptographic Service Providers (CSPs) and associated cryptographic algorithms available in the Microsoft Windows CryptoAPI to encrypt/decrypt communication between client and server. Direct questions regarding the FIPS 140 validation of the CSPs to Microsoft Corporation.

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL support and supported ciphersuites can also be controlled by the following Microsoft security option:

System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing. Refer to Microsoft product documentation for details.

TLS/SSL Support

In sample deployment C, you can configure Secure Gateway and the Web Interface to use either the Transport Layer Security (TLS) protocol 1.0 or the Secure Sockets Layer (SSL) protocol 3.0. The components are configured for TLS.

For details about configuring TLS, see the:

- *Web Interface Administrator's Guide*
- *Secure Gateway for Windows Administrator's Guide*
- *Clients Windows Administrator's Guide*

Supported Ciphersuites

In sample deployment C, you configure Secure Gateway, Secure Gateway proxy, and the Web Interface to use government-approved cryptography to protect "sensitive but unclassified" data. One government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

- *Web Interface Administrator's Guide*
- *Secure Gateway for Windows Administrator's Guide*
- *Clients for Windows Administrator's Guide*

Alternatively, for TLS connections, you can use AES as defined in FIPS 197. The government ciphersuites are RSA_WITH_AES_128_CBC_SHA for 128-bit keys, or RSA_WITH_AES_256_CBC_SHA for 256-bit keys. As defined in Internet RFC 3268 http://www.ietf.org/rfc/rfc3268.txt, these ciphersuites use RSA key exchange and AES encryption. For further information on AES, visit the NIST WEb site at http://csrc.nist.gov/cryptval/des.htm.

Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment C, you configure one server certificate on the Secure Gateway, one on the Secure Gateway Proxy, and one on the Web Interface. You also configure a certificate on each computer running Citrix Presentation Server. For further details, see the relevant Administrator's Guides.

Smart Card Logon

Smart card authentication is not supported in deployment C. It is not possible to configure smart card support where the Secure Gateway is positioned between the clients and the Web Interface.

For more information, see the *Secure Gateway for Windows Administrator's Guid*e.

Clients

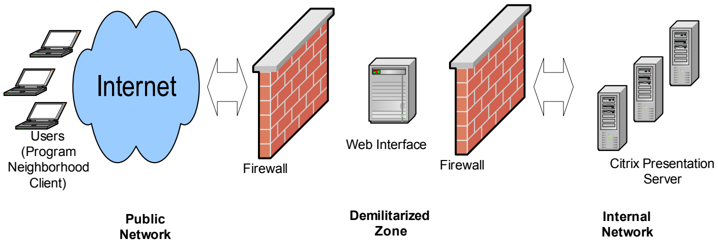
The Program Neighborhood Client is used in sample deployment C. For details about the security features and capabilities of Citrix Presentation Server Clients, see "Citrix Presentation Server Clients" on page 16.

Sample Deployment D - Using SSL Relay and the Web Interface

The computers running Citrix Presentation Server in sample deployment D comprise Citrix Presentation Server 4.5 for Windows on Microsoft Windows Server 2003 with Terminal Services. Citrix SSL Relay is enabled.

The server running the Web Interface in sample deployment D comprises the Web Interface for Citrix Presentation Server on Microsoft Windows Server 2003, with Microsoft Internet Information Services Version 6.0 or later.

Users in deployment D are running a TLS-enabled Web browser and the Program Neighborhood Client (32-bit Windows, Version 10.*x*).



This diagram shows Sample Deployment D using SSL Relay and the Web Interface

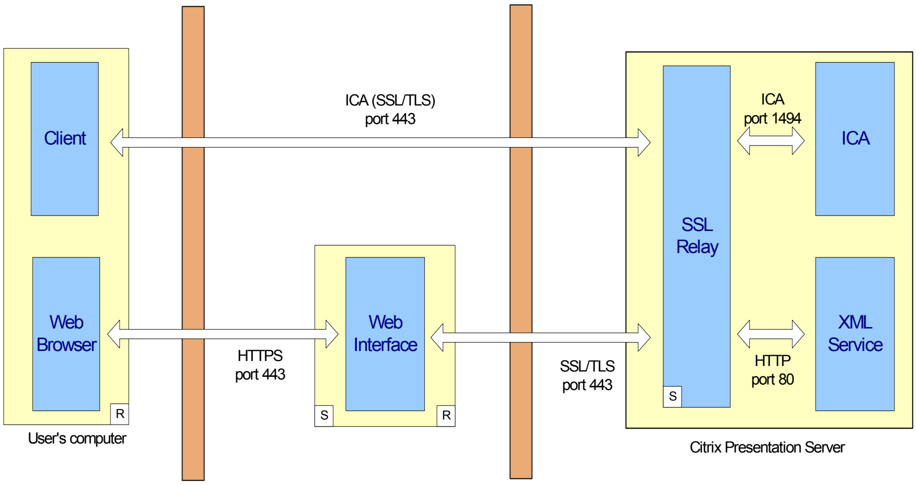
How the Components Interact

In sample deployment D, you secure the connection between the user's Web browser and the Web Interface using HTTPS. You secure the connection between the Web Interface and the Citrix SSL Relay using TLS.

The connection between the client device and the Citrix SSL Relay is secured using TLS.

The SSL Relay operates as an intermediary in the communications between the clients, the Web Interface, and the XML Service at each computer running Citrix Presentation Server. Each client authenticates the SSL Relay by checking the SSL Relay's server certificate against a list of trusted certificate authorities. After this authentication, the client and SSL Relay negotiate requests in encrypted form. The SSL Relay decrypts the requests and passes them to the computer running Citrix Presentation Server. When returning the information to the client, the server sends all information through the SSL Relay, which encrypts the data and forwards it to the client to be decrypted. Message integrity checks verify each communication was not tampered with.

The following diagram shows the interaction of these components:



This diagram shows a detailed view of Sample Deployment D

FIPS 140 Validation

In sample deployment D, the Citrix SSL Relay uses the Microsoft Cryptographic Service Providers (CSPs) and associated cryptographic algorithms available in the Microsoft Windows CryptoAPI to encrypt/decrypt communication between client and server. Direct questions regarding the FIPS 140 validation of the CSPs to Microsoft Corporation.

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL support and supported ciphersuites can also be controlled by the following Microsoft security option:

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing. Refer to Microsoft product documentation for details.

TLS/SSL Support

In sample deployment D, you can configure the Citrix SSL Relay and the Web Interface to use either the Transport Layer Security (TLS) protocol 1.0 or the Secure Sockets Layer (SSL) protocol 3.0. In sample deployment D, the components are configured for TLS.

For details about configuring TLS, see the:

- *Citrix Presentation Server Administrator's Guide* and the online application help for the SSL Relay Configuration tool. When using the SSL Relay Configuration tool, ensure that **TLS** is selected at the **Connection** tab.

- *Web Interface Administrator's Guide*
- *Clients for Windows Administrator's Guide*

Supported Ciphersuites

In sample deployment D, you configure the Citrix SSL Relay and the Web Interface to use government-approved cryptography to protect “sensitive but unclassified” data. One government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

- *Citrix Presentation Server Administrator's Guide* and the online application help for the SSL Relay Configuration tool. When you use the SSL Relay Configuration tool, ensure that only **GOV** is selected at the **Ciphersuite** tab.
- *Web Interface Administrator's Guide*
- *Clients for Windows Administrator's Guide*

Alternatively, for TLS connections, you can use AES as defined in FIPS 197. The government ciphersuites are RSA_WITH_AES_128_CBC_SHA for 128-bit keys, or RSA_WITH_AES_256_CBC_SHA for 256-bit keys. As defined in Internet RFC 3268 http://www.ietf.org/rfc/rfc3268.txt, these ciphersuites use RSA key exchange and AES encryption. For further information on AES, visit the NIST WEb site at http://csrc.nist.gov/cryptval/des.htm.

Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment D, you configure a separate server certificate for each computer running Citrix Presentation Server on which you use the SSL Relay. For further details, see the *Citrix Presentation Server Administrator's Guide*.

Smart Card Logon

In sample deployment D, you can configure Citrix Presentation Server to provide smart card authentication. To do this, you must configure authentication using the Microsoft Active Directory and use the Microsoft Certificate Authority.

For more information, see the latest version of the *Advanced Concepts Guide for Citrix Presentation Server* available from the Citrix Web site.

Clients

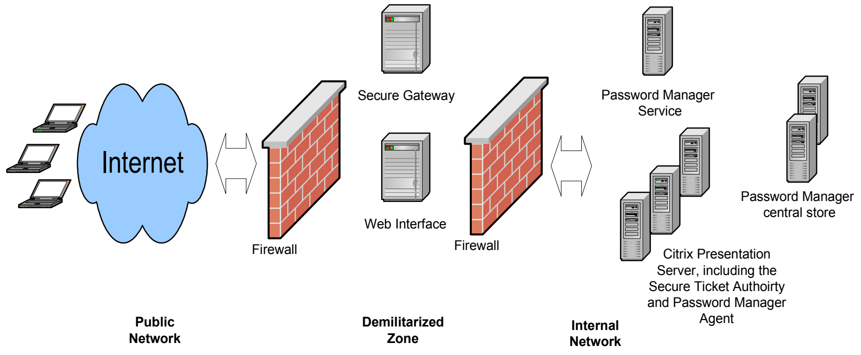
The Program Neighborhood Client is used in sample deployment D. For details about the security features and capabilities of Citrix Presentation Server Clients, see "Citrix Presentation Server Clients" on page 16.

Sample Deployment E - Using Password Manager and Secure Gateway (Single-Hop)

The computers running Presentation Server and Password Manager in sample deployment E comprise:

- Presentation Server 4.5 for Windows, Platinum Edition, on Microsoft Windows Server 2003 with Terminal Services, Service Pack 1 or later, 32-bit version. SSL Relay is not enabled. Platinum Edition incorporates Password Manager, and the Password Manager Agent runs on the computer running Presentation Server.
- The Secure Gateway and the Secure Ticket Authority (STA) are both running on Microsoft Windows 2003. STA is automatically installed on the computer running Presentation Server.
- The server running the Web Interface comprises the Web Interface on Microsoft Windows Server 2003, with Microsoft Internet Information Services Version 6.0 or later.
- The Password Manager Service is running on Microsoft Windows Server 2003, Service Pack 1 or later, 32-bit version, with Microsoft .NET Framework 2.0 installed.
- The Password Manager central store is hosted on two servers (a primary server and a secondary server) both running Active Directory on Microsoft Windows Server 2003, Service Pack 1 or later, 32-bit version. The sole purpose of the secondary server is to provide failover for the primary server.
- Users are running a TLS-enabled Web browser and the Program Neighborhood Client (32-bit Windows, Version 10.*x*).

For further details of the Password Manager components in this deployment, see the *Citrix Password Manager Administrator's Guide*.



This diagram shows deployment E, using Password Manager and the Secure Gateway

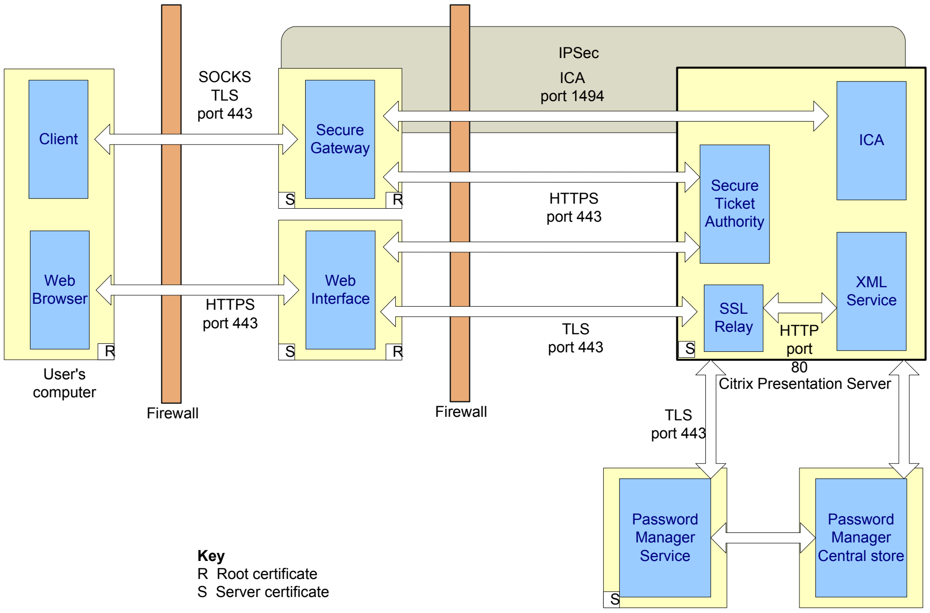
How the Components Interact

You use TLS to secure the connection between a client and the Secure Gateway. To do this, you deploy TLS/SSL-enabled clients and deploy the Secure Gateway at the network perimeter, typically in a demilitarized zone (DMZ). You secure the connection between the Web browser and the Web Interface using HTTPS. Additionally, you use TLS to secure communication between the Web Interface and Citrix Presentation Server, and between Citrix Presentation Server and the Password Manager central store and service.

In sample deployment E, the Secure Gateway removes the need to publish the addresses of every computer running Citrix Presentation Server, and allows a single point of encryption and access to the Citrix servers. It does this by providing a gateway that is separate from the computers running Citrix Presentation Server and reduces the issues for firewall traversal to a widely accepted port for ICA traffic in and out of firewalls.

Set against the high level of scalability of sample deployment E is the fact that ICA communication is encrypted only between the client and the gateway. ICA communication between the gateway and Citrix Presentation Server is not encrypted.

To achieve FIPS 140, you secure the communication between the Secure Gateway and Citrix Presentation Server using IPSec. This is illustrated in the next diagram.



This diagram shows a detailed view of Sample Deployment E

IPSec

To enable IPSec to secure communication between the Secure Gateway and the computers running Citrix Presentation Server, you must configure IPSec for the following servers:

- Secure Gateway
- All the computers running Citrix Presentation Server

IPSec is configured using the Local Security Settings (IP Security Policies) for each server. In deployment B.2, IPSec is enabled on the required servers and the security method is configured for 3DES encryption and SHA-1 integrity to meet FIPS 140 requirements.

FIPS 140 Validation

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL support and supported ciphersuites can be controlled by the following Microsoft security option:

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing. Refer to Microsoft product documentation for details.

TLS/SSL Support

In sample deployment E, you configure Secure Gateway and the Web Interface to use the Transport Layer Security (TLS) protocol 1.0.

For details about configuring TLS, see the:

- *Web Interface Administrator's Guide*
- *Secure Gateway for Windows Administrator's Guide*
- *Clients for Windows Administrator's Guide*
- *Citrix Password Manager Administrator's Guide*

Supported Ciphersuites

In sample deployment E, you configure Secure Gateway and the Web Interface to use government-approved cryptography to protect "sensitive but unclassified" data. One government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

- *Secure Gateway for Windows Administrator's Guide*
- *Clients for Windows Administrator's Guide*

Alternatively, for TLS connections, you can use AES as defined in FIPS 197. The government ciphersuites are RSA_WITH_AES_128_CBC_SHA for 128-bit keys, or RSA_WITH_AES_256_CBC_SHA for 256-bit keys. As defined in Internet RFC 3268 http://www.ietf.org/rfc/rfc3268.txt, these ciphersuites use RSA key exchange and AES encryption. For further information on AES, visit the NIST WEb site at http://csrc.nist.gov/cryptval/des.htm.

Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment E, you configure one server certificate on the Secure Gateway, and one on the Web Interface. You also configure a certificate on each computer running Citrix Presentation Server and on the computer running the Password Manager Service. For further details, see the relevant Administrator's Guides.

Smart Card Logon

In sample deployment E, you can configure Citrix Presentation Server to provide smart card authentication. To do this, you must configure authentication using the Microsoft Active Directory and use the Microsoft Certificate Authority.

For more information, see the latest version of the *Advanced Concepts Guide for Citrix Presentation Server* available from the Citrix Web site.

Clients

The Program Neighborhood Client is used in sample deployment E.

For details about the security features and capabilities of Citrix Presentation Server Clients, see "Citrix Presentation Server Clients" on page 16.