Payment Card Industry and Citrix XenApp and XenDesktop Deployment Scenarios

Overview

Citrix XenApp, XenDesktop and NetScaler are commonly used in the creation of Payment Card Industry (PCI), Data Security Standard (DSS) compliant data processing systems. This document describes common PCI designs and provides vendor guidance to the construction of secure data processing systems based on Citrix remoting technologies.

Through the use of network separation, server based computing and display remoting protocols, sensitive credit card data is restricted to a PCI data processing backend, with data accessing applications hosted on Citrix XenApp or XenDesktop and the screen and keyboard user experience delivered to the user, always on remote networks, via Citrix Independent Computing Architecture (ICA) display remoting protocol. The PCI data processing backend is firewalled and separated from the main corporate network; all user interaction is remote, across gateways, with no VPN and no direct network connectivity between the user computer and the protected applications.

The only applications which can interact with the secure data are the ones specifically included in the administrator defined PCI backend and all user view of the protected data is via remote execution of the approved applications and systems.

By enabling centralized data processing and restricting PCI data access to only the approved components specifically included inside the protected environment, the scope of PCI evaluation is greatly reduced and security is greatly improved compared to making the protected systems and data accessible from all user devices. Data centralization is a core reason that Citrix technologies are often a primary component of a PCI Compliant data processing system.

Revision History

2016-06-30	1.3	PCI DSS 3.2 updates, encryption details and admin multi-factor authentication
2014-09-04	1.2	Clarified that double hop network configuration is partner or remote office
2014-02-26	1.1	Changed nomenclature describing NetScaler Gateway and Web App Firewall to clarify that these are modules running on NetScaler rather than included in all revisions
2013-12-10	1.0	First release

PCI Introduction

Payment Card Industry (PCI) Data Security Standard (DSS) is a credit card industry standard which defines a required level of computer system security that must exist when processing credit card data. PCI DSS applies to merchants, processors, financial institutions, and service providers, as well as all other entities that store, process, or transmit cardholder data. PCI DSS certification is ultimately an agreement that a specified level of security is required, and certification that it exists.

PCI Compliance is a certification given to a PCI data processing environment; there is no PCI Certification for Citrix XenApp or XenDesktop, but it is very common for PCI compliant data processing systems to include Citrix hosted execution systems in their design.

PCI Tiers

The required level of security will often grow as a merchant's business grows and as their PCI tier changes. The specific requirements of a certification will vary based upon the requirements of the issuing bank and the Qualified Security Assessor (QSA) and these may include expanded or reduced requirements compared to those presented in this paper.

Citrix XenApp and XenDesktop Introduction

Citrix XenApp and XenDesktop are server based computing systems whose design goes back to the founding of Citrix in 1989. The technology has gone by many names including WinFrame, MetaFrame, Presentation Server and XenApp and XenDesktop.

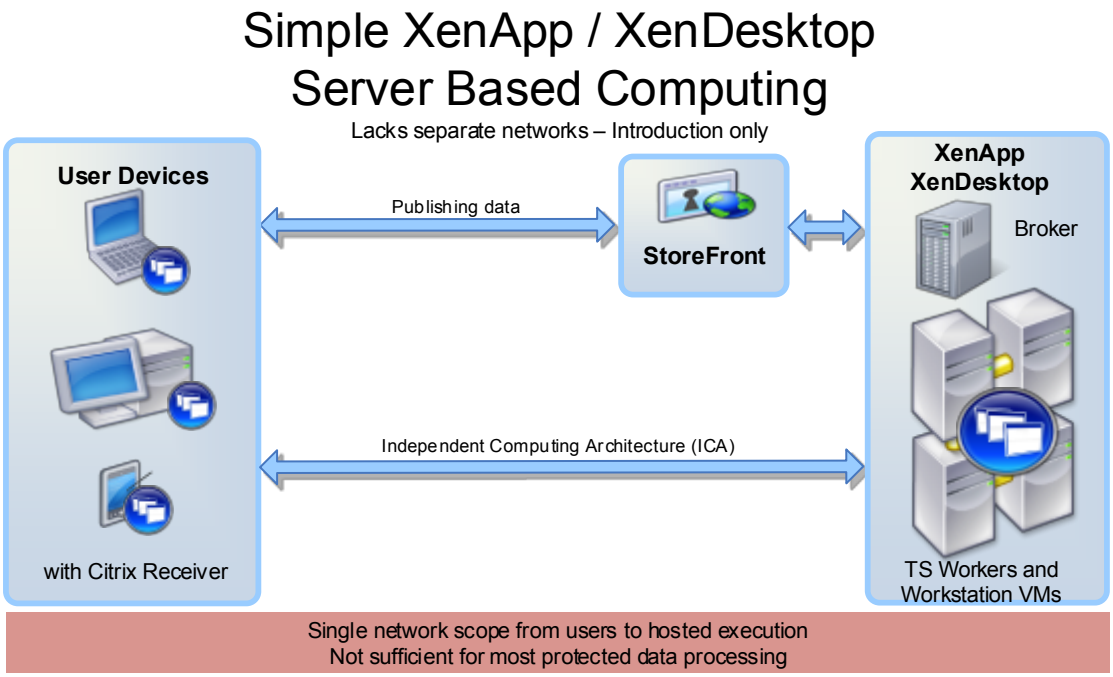
Applications are run on a Windows session sharing Terminal Server system (XenApp) or a desktop Windows operating system (XenDesktop) and are delivered via remote execution. In both XenApp and XenDesktop, the execution workload runs on computers inside of a data center and users are physically remote compared to the hosting computers. The screen, keyboard and other user experience items are delivered to the user via the Citrix Receiver (terminal application) which presents the remote execution of Windows applications and desktops to the user as though the execution is occurring locally.

While the computing is central, the user view is that computing is on their end-user device. Individual remote applications (plural) can be overlaid onto the user's main desktop screen as if they are local applications (XenApp), or an entire separate desktop operating system can be run and reflected onto the user's computing device (XenDesktop). Whether remoting applications or remoting desktops, the user experience and remote delivery are the same; the execution and data are inside the central data center and the screen and keyboard interaction are delivered to the user computer via the Receiver application.

With the addition of Citrix NetScaler and the NetScaler ICA Proxy Module, it is possible to completely separate the user computer network from the protected network and eliminate the need for a traditional IP layer VPN. The ICA Proxy relays screen and keyboard information across the boundary of the protected PCI space to the user computer networks, permitting the user to do their work, but at the same time enhancing security by maintaining IP network separation between the user computer and the protected network. No applications on the user computer can "see" the protected environment as there is no IP level network connectivity from the user machines.

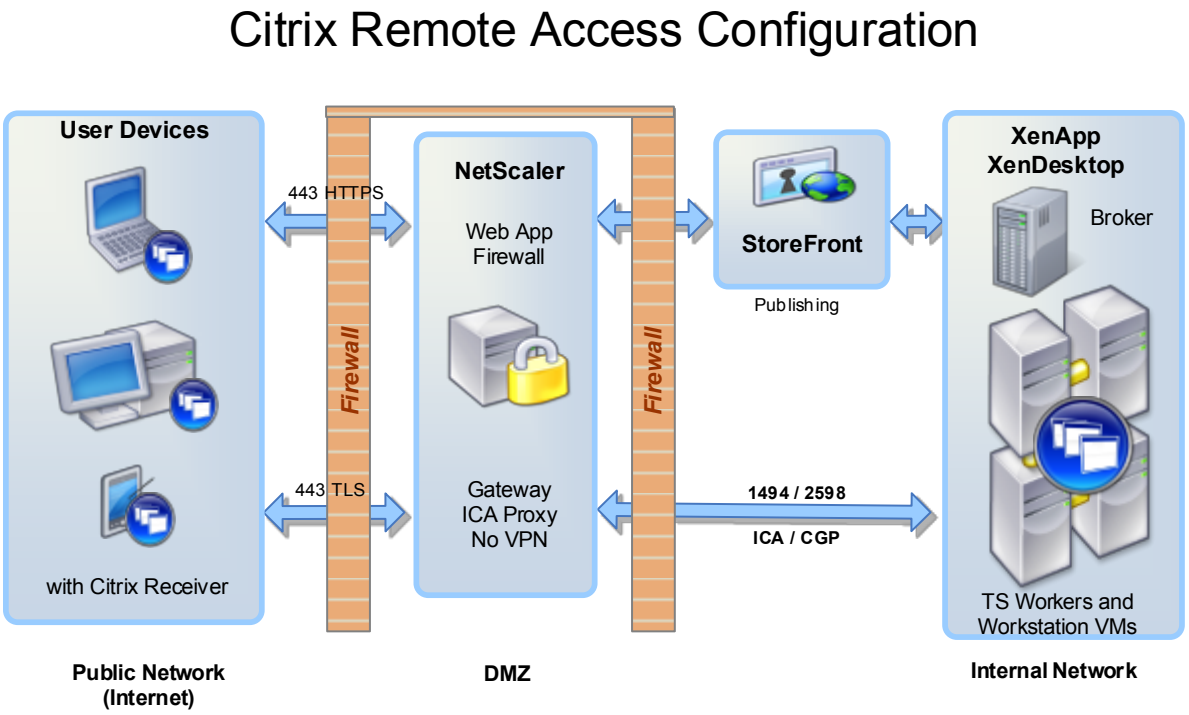
The diagrams that follow show example Citrix deployments, starting with a simple non-PCI XenApp / XenDesktop configuration and then growing that to a configuration suitable for PCI and eventually a double-hop PCI configuration which includes wide area accessibility from partner companies.

Simple XenApp / XenDesktop



Remote Access using XenApp and XenDesktop

The diagram below shows a XenApp / XenDesktop farm with the added ability to get to corporate applications from both inside the company as well as access from the internet via Citrix Receiver and NetScaler Gateway module. This is a classic "remote access" configuration for Citrix XenApp and XenDesktop. This diagram omits drawing internal user computers; these are common in a remote access farm architecture, but are not suitable for PCI.



Whether a user is local or remote, they get the same experience of hosted application and desktop execution. It is common that authentication from outside of the company requires two-factor authentication and access from inside the network requires only username and password.

Publishing and Application Launch

The starting point for a user launching an application is using the Citrix Receiver or a web browser to logon to StoreFront. StoreFront is a Microsoft IIS web server running the Citrix StoreFront application. StoreFront will enumerate the applications and desktops available to the user, providing a list of application names and icons back to the Receiver application or web browser. The user will ultimately request an application or desktop launch by clicking on an icon representing the application or desktop. Whether initiated from a web browser visiting the StoreFront website to list available application, or initiated from the Receiver giving the user icons to select, the launch process is the same and is described in detail below.

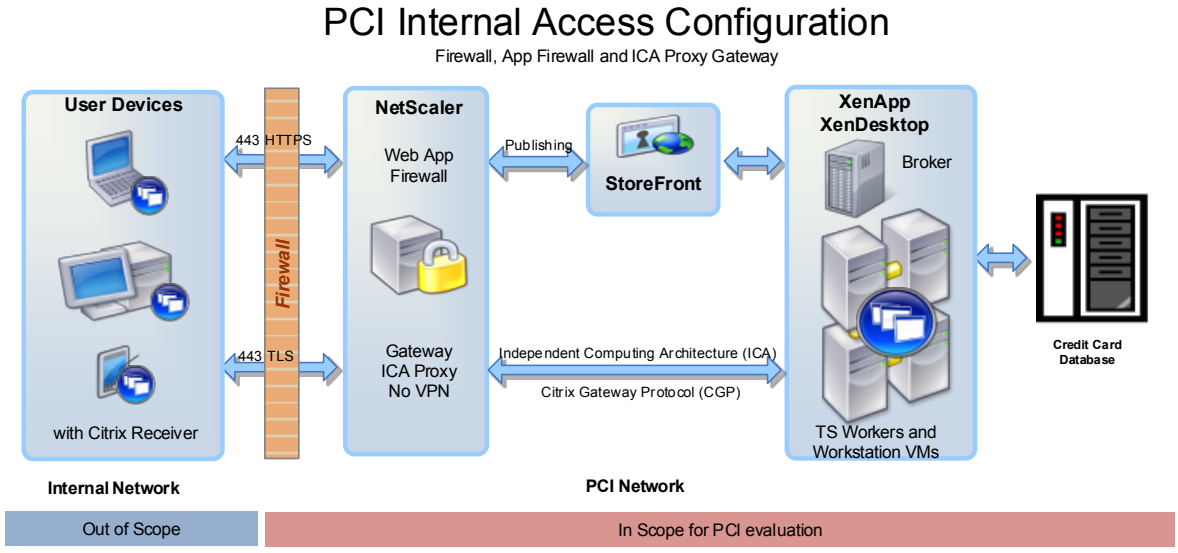
Application enumeration and launch via Citrix Receiver or Web Browser:

1. User uses a web browser or Citrix Receiver to view the StoreFront login page
    a. StoreFront is a web service, running on top of Microsoft IIS
    b. User authenticates
2. StoreFront queries published applications and desktops for this user
    a. Application names, desktop names and icons are gathered based upon publishing information stored in the Citrix Desktop Delivery Controller (DDC)
    b. A web page is constructed and provided to the user's browser or equivalent information is provided to the Receiver application
    c. Program launch icons are constructed on the endpoint browser or application system
3. User clicks an icon, starting the process of remote application launch
4. Request is sent to StoreFront to retrieve the ICA (Independent Computing Architecture) file for the selected application or desktop. The ".ica" file is a text file which contains publishing information needed to tell the Citrix Receiver how to connect to the server based execution of the application or desktop. The .ica file is constructed by StoreFront at runtime based up communication with the Desktop Delivery Controller / publishing back end
    a. StoreFront contacts DDC and requests a TS server or workstation assignment. Note it is this point where XenApp and XenDesktop can spread users across servers and desktops and manages load and scale
    b. For local network execution cases (user machine is inside the corporate network, not PCI), the ICA file includes the server assignment by name. This does not apply for the PCI case because all execution in the PCI configuration is "remote", going through the NetScaler Gateway Module with ICA proxy
    c. For remote execution (All PCI), ICA file includes
        i. NetScaler fully-qualified domain name. The ICA file does not contain any information regarding the internal network addresses or server assignment
        ii. A Secure Ticket Authority launch ticket is created (STA Ticket) and is included in the .ica file

5. Citrix Receiver on the client machine or web browser agent launches the Citrix ICA client (wfica32.exe). It connects to the assigned server, or in the remote case, to the NetScaler Gateway and provides the STA ticket given from StoreFront
    a. The connection uses TLS to ensure data confidentiality and integrity is maintained
    b. NetScaler Gateway contacts the Secure Ticket Authority server in the DDC and provides STA ticket
    c. The Secure Ticket Authority validates the STA ticket and returns to the gateway the stored IP address of the Server or workstation that contains the requested application or desktop. The endpoint computer remains unaware of the internal network assignment
6. The NetScaler Gateway initiates an ICA session with that server / workstation.
7. User computer has an ICA session between itself and the Gateway
8. NetScaler Gateway Module acts as ICA proxy between the networks
    a. From end user Receiver view, the ICA Proxy gateway is the “server”
    b. From server view, the gateway is the “user”
    c. Keyboard and Screen data are relayed by the NetScaler Gateway
    d. No direct network connection exists from user network to protected network
9. Eventually the application or desktop terminates and the connection is closed
10. The session may also be “disconnected” and the applications will continue to run. On next application launch, the user is reconnected with their existing session

PCI Implementation – Internal Network Only

When a merchant’s quantity of PCI transactions grows, the Issuing Bank may require improvements to data processing security so that credit card data processing occurs in a space that is separate from the main corporate network. If no existing XenApp or XenDesktop environment exists and if remote access is not required, the following solution can provide an effective separation of the primary corporate network and the PCI space. This has advantage of limiting vision to the PCI data to only the applications and systems in the PCI back-end, keeping the majority of the existing corporate network out of scope for PCI.



Observe that “remote access” is used “inside”. All users are “external”. The value of using this configuration is that the PCI applications can be separated from the non-PCI applications. It is common that there will be a XenApp / XenDesktop configuration just for PCI applications even if the corporate environment already has one or more Citrix infrastructures. The key is that only PCI applications are present in the validated space. The main corporate network is separate from the PCI space.

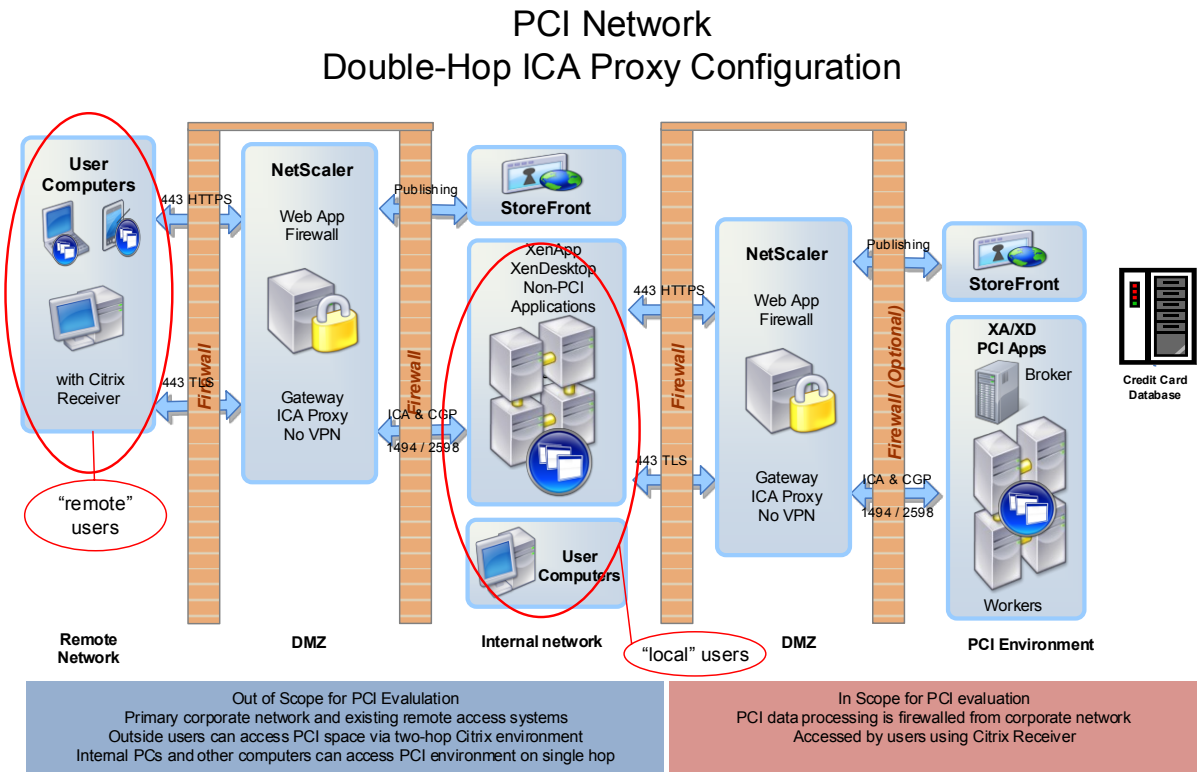
PCI – With Remote Access (XenApp and XenDesktop)

Achieving PCI data separation with remote access from a partner company utilizes two-hops. The first hop gets the remote user into the company internal network; the second hop provides access to the PCI applications.

The diagram below is effectively equal to the XenApp/XenDesktop remote access configuration combined with the simple PCI internal-only deployment earlier in this document. In this configuration, the users will be

1) Internal; shown in the diagram as “User Computers” or
2) External; shown in the diagram on left as User Computers with Citrix Receiver”

In both cases, the user view of the applications is the same, though in the external case, an additional “hop” is required to get to the protected data as these are published only to internal resources.



Access to PCI published components is restricted to internal resources. User sessions running on the internal network XenApp/XenDesktop cannot themselves see the PCI protected applications, but

they can remotely execute the applications running on the protected PCI back-end. Remote users (partner companies) will first logon to a hosted desktop in the Internal Network and then run a PCI application on the PCI network.

Internal users can access the PCI space directly via the PCI environment remoting to their computers. Some customers prefer to limit all access to PCI space to exclusively double-hop configurations, even for internal users.

Firewalls

In the diagrams, many firewalls are shown, often on both sides of the NetScaler in the DMZ. Installed firewalls should follow the firewall vendor guidance for configuration with a minimum of ports open to access the protected systems. In most external spaces, only TLS port 443 must be open. Internally, TLS and ICA ports are opened to the NetScaler Gateway.

NetScaler Gateway - ICA Proxy

The NetScaler Gateway module provides ICA Proxy to connect hosted application and desktop execution to the Citrix Receivers on user systems. The gateway relays ICA data to/from specific endpoints. There is no traditional VPN between the protected and non-protected spaces and specifically there is no IP level network connectivity, the end user computer has no IP level network connectivity to the PCI space.

NetScaler Gateway – Web Application Firewall

NetScaler Platinum Edition provides the Web Application Firewall that is placed in front of the IIS web server hosting StoreFront. In this configuration, the NetScaler can provide this web access control as well as the ICA Proxy functions required for display remoting across networks.

NetScaler Gateway – Endpoint analysis

NetScaler Platinum Edition provides the ability to inspect Receiver machines to query a number of factors required for launch. Importantly, the NetScaler Platinum Edition can be configured to block all connections from IP address ranges outside a defined set. In this configuration, the PCI space NetScaler can restrict all access to the double hop space. The Gateway can also be configured to permit connections from the double hop space and a possible subset of the internal corporate network.

Multi-factor authentication for remote access

PCI DSS version 3.2 section 8.3 requires multi-factor authentication for “all individual non-console administrative access and all remote access”. Citrix XenApp, XenDesktop and NetScaler support multi-factor authentication via a variety of techniques and a variety of partner companies. The “Citrix Ready” website is a starting point for selecting suitable products. Popular solutions for multi-factor user authentication include FOB tokens from RSA and Symantec. Smart Card solutions are also available for user access though these are more commonly used for administration functions in PCI.

Consider in PCI DSS that the definition of “remote” varies compared to an enterprise work from home scenario. In PCI case, two levels of Gateway may be used, users traveling through only one gateway are “local” and users passing through double hop are “remote”. This means that key fob

plus username and password authentication would normally be required for users accessing from a remote partner company, but use of a key FOB would not be required for users accessing via local resources.

Though multi-factor is only required in remote access configuration, it is a security advantage to require multi-factor authentication in all scenarios and the QSA may provide guidance to the value/cost of this configuration for any specific implementation.

Multi-factor authentication for administration

Multi-factor authentication for administration is also supported. Citrix XenApp and XenDesktop are managed via two primary applications, the Citrix Studio and Desktop Director. Studio is the primary application for configuring a Citrix XenApp/XenDesktop environment; this is where applications are published and where specific user groups are granted access to published resources. Citrix Studio is a Windows application hosted on a server and run by administrators, normally via local logon to that server, but also possible via published application to the server that hosts the application which is Studio.

Administrators must be able to logon to Windows before the Studio application can be executed and Studio leverages Windows integrated authentication to restrict administration to only privileged administrator systems. It is expected in this configuration that XenApp and XenDestkop administrative users on the domain will be configured to require smart card for authentication to the domain. Once logged on, the administrative user can execute Citrix studio, who will validate administrator rights for configuring the XenApp and XenDesktop environment.

The Citrix Desktop Director is the "level 1" help desk system. Compared to Studio, Director is "less powerful". Director is implemented as a Windows IIS hosted web application and administrator authentication into Director is performed as a user authentication to IIS website. Director is designed for quick vision to end user running application sessions and hosted desktops, providing the level 1 help desk administrator the ability to force logoff and evaluate logon time performance metrics or other parameters of end user running sessions.

As an IIS application, Windows techniques for restricting access as with Studio can be used though it is common that Desktop Director itself is delivered to help desk administrators as a Citrix published application. Here, the same key FOB tools used for delivering PCI applications to end users can also be used to deliver Desktop Directory to help desk administrators.

Encryption of data in motion

PCI DSS requirement 4, states that "*Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals*". In the PCI configurations described in this paper, all Citrix traffic crossing over networks easily accessible to malicious individuals is encapsulated inside of TLS and HTTPS encrypted channels. The endpoint communication to StoreFront is always HTTPS and the ICA communication for remote display protocol is encapsulated inside of TLS.

All components support the PCI DSS 3.2 required TLS 1.1 as well as the not required TLS 1.2. The administrator can configure the ciphers on the StoreFront and NetScaler Gateway. Beyond product

documentation, a 1-hour presentation on configuring ciphers with NetScaler and Citrix Receivers was presented at Citrix Synergy 2016 and is a useful reference, SYN262 link.

The PCI space is not "easily accessed by malicious individuals". The ICA traffic "inside" will normally not be TLS encrypted and will instead be encrypted with the one of the older Citrix ICA encryption methods.

Encryption algorithms in Citrix ICA

The encrypted delivery of the ICA display remoting protocol has undergone change over time. There are 3 primary levels of encryption.

	Description
Basic	XOR – scramble data from view of network analysers
SecureICA	Diffie Hellman key exchange and RC5 128-bit cipher. Not FIPS Compliant.
TLS	Industry standard FIPS 140-2 compliant cryptography

With view of PCI DSS requirement 4 (encryption), the guidance in this document considers Basic and SecureICA to be "clear text" and TLS to be encrypted. This definition is consistent with guidance from USA NIST where data encrypted with non-FIPS algorithms is considered not encrypted.

In spaces normally accessible to attackers (outside the NetScaler Gateway), all ICA traffic travels inside of TLS secured communication. Inside the PCI space, it is common that Basic or SecureICA are used as the PCI network is IP separated from non-PCI network and is normally not accessible to attackers.

If required, the ICA communication inside the PCI space can also be encrypted with TLS; this requires additional administration to distribute per-server TLS certificates. Consult Citrix XenApp and XenDesktop FIPS Compliance documents for details, link.

Conclusion

Data centralization and server based computing provide significant value in security and also in audit. By restricting PCI data to only a small protected space, that space can be audited more completely and efficiently than attempting to certify an entire corporate internal network.

Data centralization, firewalls and remote execution provide an environment for protecting data from unauthorized access, while enabling access to that data for authorized users from a variety of end user locations. End user access to hosted applications can be via a variety of computing devices running a myriad of operation systems. Since the Citrix Receiver is logically a "terminal", the quantity of data that leaves the protected space, to be shown to or entered by the user, is small compared to the quantity of data that exists in the back end.

Server based computing with Citrix provides the ability to protect payment card data and the tools to get that data to authorized users.

Supporting documents

Overview of NetScaler Web Application Firewall module and PCI DSS

http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/pci-dss-success-achieving-compliance-and-increasing-web-application-availability.pdf

Common Criteria Certifications and Security Targets for XenApp, XenDesktop and NetScaler

http://www.citrix.com/support/security-compliance/common-criteria.html

FIPS Compliance documents and lockdown guidance

http://citrix.com/security

https://www.citrix.com/content/dam/citrix/en_us/documents/about/citrix-xenapp-and-xendesktop-76-fips-140-2-sample-deployments.pdf