Safeguards Technical Assistance Memorandum
Protecting Federal Tax Information (FTI) In a Virtual Desktop Environment

Introduction

Virtual Desktop Infrastructure (VDI) is the practice of hosting a desktop operating system within a virtual machine (VM) running on a centralized server. A VDI provides users access to enterprise resources, including a virtual desktop from locations both internal to and external to the agency's networks. In a VDI environment a user can access FTI by connecting to their virtual workstation via a vendor specific agent, connection client or through an Internet browser from practically any mobile device with Internet access. This can offer significant savings to agencies from a cost perspective and also from a management perspective, allowing agencies to largely centralize patch management and deploy standard desktop configurations.

There are several vendors who offer a variety of VDI solutions, including Citrix, VMware, and Microsoft. This technical memo does not compare the features or security options offered among the above products, nor does it provide an opinion of one product over another. Each agency should carefully select the desktop virtualization solution that best fits to their operational environment and end user needs, while ensuring security of FTI received, stored, processed or transmitted in a virtual desktop environment. This technical memo provides the IRS mandatory security requirements should an agency choose to use virtual desktop technologies.

This technical memo is applicable to VDI environments in which agency-owned, non-agency owned and personally owned equipment may be used as the client for the virtual desktop. Additional security requirements apply to an agency that is approved by IRS to use non-agency owned and personally owned equipment to access FTI through a VDI environment. The agency must demonstrate that despite the operational location of the client, FTI remains subject to the safeguard requirements and the highest level of attainable security. Please reference IRS Publication 1075, Section 7.4.5 *Non-Agency-Owned Information Systems* for the detailed requirements and the approval process for obtaining approval for the use of non-agency computers to access FTI.

Virtual Desktop Components and Architecture

A typical virtual desktop deployment consists of four tiers: the Client Tier, Access Tier, Virtual Desktop Tier, and Client Application Tier.

1. **Client Tier includes the thin client devices (laptops, desktops, etc.) the end user** employs to access their desktop within the virtual desktop tier.

2. **Access Tier** consists of entry points to the virtual environment. Access Tier devices include gateways, web interfaces, authentication servers and session manager. This tier brokers connections between Client Tier devices and Virtual Desktop Tier components.

3. **Virtual Desktop Tier** contains the virtual desktop images residing on servers in the data center. Other components within the Virtual Desktop Tier include management consoles, databases, virtualization components that publish virtualization resources, and the hypervisor that handles the execution of the virtual environment. A virtual desktop is built using a modular approach where each component layers on top of another component to give the end-user a customized desktop environment.

   Client Application Tier (not pictured) includes the applications that are delivered to the end user via the virtual desktop. This tier will not be addressed in this memo as it is application level.

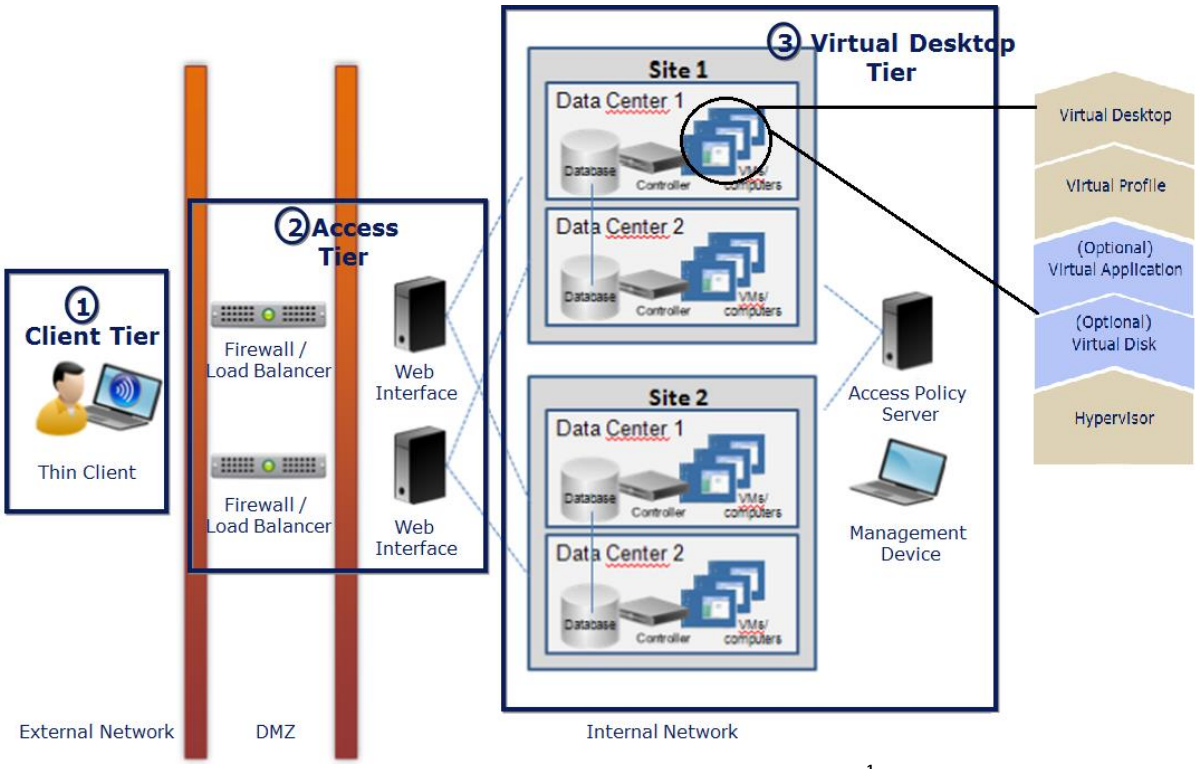

Figure 1. Virtual Desktop Components and Architecture[1]

Unique Security Challenges to Virtual Desktop

Virtual Desktops allow users to remotely access their desktop from a variety of locations. The following risks are unique to a virtual desktop environment and can jeopardize the confidentiality, integrity and availability of FTI if protection is inadequate:

- Risk 1: Client Tier devices can be operated from a remote location, such as a public space, where physical security controls are inadequate.

[1] http://support.citrix.com/proddocs/topic/xendesktop/cds-library-wrapper-rho.html

- Risk 2: Sensitive information traverses over networks where the agency cannot control security.

- Risk 3: Users can potentially store FTI locally on the thin client or on removable media by escaping the confinement of the virtual desktop using guest-to-host operations. FTI can also be printed locally if the virtual environment is not securely configured.

- Risk 4: Virtual desktops are prone to virtualization specific attacks such as hyperjacking, in addition to the traditional threats such as viruses, Trojans, man-in-the-middle attacks, key loggers, root kits and client-side attacks that targeted against Client Tier devices.

- Risk 5: Security event auditing is more complex and cumbersome in the virtual environment. Log correlation can be difficult to accomplish leading to undetected security incidents.

- Risk 6: Internal resources that were not previously accessible from external networks are vulnerable to new threats from untrusted client devices and networks.

Mandatory Requirements for FTI in a Virtual Desktop Environment
To utilize Virtual Desktop that provides FTI to a customer, the agency must meet the following mandatory requirements to lower the residual risk of the potential weaknesses identified in the section above:

1. **Environment segregation**: Virtual Desktop components should be segregated so that boundary protections can be implemented and access controls are granulized.

2. **Access Control**: An access control system must be specifically configured to address the complicated nature of the environment. Ensure only authorized clients that conform to agency security policy are permitted access to the VDI.

3. **Securely Configure Components within the Virtual Desktop Tier and Access Tier**: Configure the hypervisor, management consoles and other virtual desktop components using the secure configuration guidelines provided by the vendor.

4. **Managing User Privileges**: The least privilege principle must be strictly enforced in a virtualized environment.

5. **Limit Functionality Provided by the Virtual Desktop**: Configure the virtualized desktop to provide the functionalities only required for operations. Non-essential functionality or components must be removed or prohibited.

6. **Multi-factor Authentication**: Users who access FTI remotely must use multi-factor authentication to validate their identity.

7. **Audit All Privileged and Administrative Functions:** Privileged and administrative functions must be recorded by the system. Security events must be reviewed regularly, at least on a weekly basis, by security personnel.

8. **Session Confidentiality and Integrity:** FTI must be transmitted securely using end-to-end encryption.

These requirements are explained in detail in the sections below.

#1 Environment Segregation
Major VDI components such as databases, application servers and management software must be installed on dedicated platforms to prevent unauthorized access. If a design validation farm or a pilot farm exists, there must be adequate separation for each environment. If the agency supports more than one virtual environment, each virtual environment must be independent from each other to prevent single point of failure. The Virtual Desktop Tier must be protected in a logical enclave so that VDI resources are protected and segregated from other enterprise IT resources. Devices that have access to FTI must be further segregated into a logical enclave to provide the most granular protection for FTI.

External facing Access Tier components such as web servers and interface servers must be placed behind filtering devices in a Demilitarized Zone (DMZ).

#2 Access Control
All devices (laptops, computing platforms) must be evaluated for compliance (patches, anti-virus) prior to being allowed to attempt connection to the VDI. For example, in XenDesktop Application Access Control implements this requirement. The agency should ensure that following access controls are implemented in the VDI:

- Access to each resource must be granted explicitly to prevent unauthorized access.
- Anonymous and public access must be disabled.
- Ensure that administrative and monitoring traffic originate from authorized IP address ranges.
- Administrative consoles must be restricted to authorized personnel only.
- Implement Network Access Control (NAC) or device authentication to ensure only authorized thin client devices are permitted to access the virtual desktop environment.

#3 Securely Configure Components within the Virtual Desktop Tier and Access Tier
The virtual desktop environment must be securely configured, patched for security vulnerabilities and supported by the vendor. The underlying OS must be securely configured as published by the IRS Office of Safeguards via the Safeguard Computer Security Evaluation Matrices (SCSEM).

Additionally, there are several configurations which may need to be adjusted in order to become compliant including:

- Install anti-virus software on all platforms supporting the virtual environment.
- Repositioning of an existing firewall, or adding additional boundary protection so that internal resources are adequately protected.
- For web interfaces used by the virtual environment, change the default ports of the web server and remove any sample sites installed by the web server. All web interfaces must be encrypted using HTTPS to ensure the confidentiality and integrity of web traffic. Ensure that SSL certificates are current and that all encryption mechanisms are FIPS 140-2 compliant.

#4 Managing User Privileges

While it is important to manage user privileges in a traditional client-server environment, it is equally important to limit the permissions of virtual desktop administrators and the permissions given to end users on their virtual desktop. Implement Role-Based Access Control (RBAC) to effectively manage user privileges. Additionally, system administrators should not be able to authenticate directly as root and must "sudo". Within the VDI environment, users must be restricted from installing software on the virtual environment to prevent the use of unauthorized and malicious software. Unless a business justification is documented and approved by management, only allow end users to have permissions sufficient for daily business operations.

Configuration files, log files and automated scripts that are placed on the virtual machine must be restricted to virtual desktop administrators only. Access control list must be in place to prevent unauthorized access from end users. Virtual machine files, snapshots and roll back files must be protected from unauthorized access. These files can recreate the user session and sensitive information can be disclosed.

#5 Limit Functionality Provided by the Virtual Desktop

FTI must be protected and remain under the agency control at all times. There are a number of common parameters/options that can enhance the security of the virtual desktop. Some of these parameters also prevent users transferring FTI from their virtual desktop to Client Tier devices:

1. Client clipboard redirection allows a user to copy information from the virtualization environment to the local workstation's clipboard. Copy and clipboard functions such as the "Client clipboard redirection" must be disabled to prevent unauthorized access and disclosure of FTI.

2. Disable client drive mapping to prevent users from storing data on their local devices or on the virtual workstation. File transfer to local device and USB support must be disabled to ensure FTI cannot be stored or transferred either locally or onto a removable media.

3. For virtual desktop solution that supports shadowing, disable shadowing to ensure sensitive data are limited to authorized users only. The shadowing

feature is designed to provide remote assistance and allows an administrator to have unobstructed access to an active user session.

4. Unnecessary functionality such as the capability to deliver multimedia information and support of collaboration devices such as webcam and microphones must be disabled.

5. Disable printer configuration so that FTI cannot be printed locally.

6. The virtual desktop must be configured to prompt the user for credentials before attempting to resume the disconnected session after network disruption.

7. Anonymous or public user accounts must be removed from the virtual environment. Published resources must be restricted to authorized users only.

8. Snapshots and roll back functionality must be disabled if they are not required.

#6 Multi-factor Authentication
Remote access and virtualization technologies allow a user to access FTI from a remote location. However, the threats of shoulder surfing, network sniffing and password cracking decrease the assurance level of user identity. Traditional challenge response based authentication mechanisms are no longer sufficient to proof the identity of remote users. In accordance with IRS Publication 1075, Section 9.3.1.12, multi-factor authentication must be implemented for remote access of FTI to ensure only authorized users have access to FTI.

#7 Audit All Privileged and Administrative Functions
Configure the virtual desktop environment to record all privileged and administrative functions. For a list of security events that must be recorded by the virtual environment, please reference IRS Publication 1075, Section 9.3.3.3, Audit Events.

#8 Session Confidentiality and Integrity
FTI must be encrypted in transit using strong encryption. Enable encryption for traffic with FTI as well as management traffic and between Client Tier communications to the virtual desktop. All encryption must be FIPS 140-2 compliant.

References
Additional information can be found in the following documents:

1. IRS Publication 1075, Tax Information Security guidelines for Federal, State and Local Agencies and Entities
2. Citrix XenDesktop Implementation: A Practical Guide for IT Professionals, Gareth R. James, 2010.
3. XenDesktop online documentation by Citrix
4. Common Criteria Documents for XenDesktop 4.0 by Citrix

5. NIST Special Publication 800-46, Guide to Enterprise Telework and Remote Access Security
6. Defense Information Systems Agency, Secure Remote Computing Security Technical Implementation Guide.
7. Defense Information Systems Agency, XenApp Security Technical Implementation Guide.
8. VMware View Security online documentation by VMware
9. An insider's look at a security strategy centered around desktop virtualization. How Citrix leverages technology and best practices to minimize risk and protect the organization.