Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Understanding and Implementing Microsoft Terminal Services & Citrix MetaFrame

Technology has become an important part of our society and corporations are finding that they need a way to provide employees with access to corporate data and various applications from remote sites, even an employee's home. There are several ways in which to provide this access, however this paper will focus on the implementing a combination of Microsoft Windows Terminal Services and Citrix MetaFrame. The combination of these two technologies has proven to be an attractive way for corporations to operate server-based ...

Copyright SANS Institute

Author Retains Full Rights

AD

Understanding and Implementing

Microsoft Terminal Services

&

Citrix MetaFrame

Chris Johnson
GSEC Practical Assignment
Version 1.2f (amended August 13, 2001)
Submitted 10 DEC 01

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Abstract

Technology has become an important part of our corporations are finding that they need away to provide employees with access to corporate data and various applications from remote sites, to include an employee's home. There are several ways in which to provide this access, however this paper will focus on the implementing a combination of Microsoft Windows Terminal Services and Citrix MetaFrame. The combination of these two technologies has proven and attractive way for corporations to operate server based application software.

Understanding Microsoft Windows Terminal Services (TS)

The information presented here will be based on MS Windows TS for Windows 2000 Server, Advanced Server and Windows 2000 Datacenter Server operating systems. With these operating systems TS is available with the base operating system, however, if you are still running MS NT 4.0 servers, TS is available to you as a separate package to be purchased separately. Terminal server will allow a corporation to place 32 bit Windows based applications in a central location, such as on a Windows 2000 server and to give their employees access to execute those applications from the server. Why is this important? Well if we look at the cost of maintaining personal computers both hardware and software we see that it becomes very expensive for the company and the home PC owner. If you have a number of remote uses, say 10,000 then you don't have to upgrade all 10,000 personal/notebook computers. Instead you run Terminal Services on the Windows 2000 server and have you employees' access the applications from the server regardless of the operating systems the remote users may be using.

Terminal services use the Remote Desktop Protocol (RDP). This protocol is based on the International Telecommunications Union (ITU) T.120 protocol. A few drawbacks of the RDP protocol are that it only supports using TCP/IP for transporting data between the server and client. More importantly is the limitation of encryption standards that RDP has the capability of using. A more important limitation is that of the encryption available to TS, which provides the following:

- Low encryption: encrypts only packets going from the client to the terminal server with a 40-bit RC4 encryption standard.
- Medium encryption: encrypts all packets (both directions) with 40-bit RC4.
- High encryption: encrypts all packets (both directions) with 128-bit RC4.

There is little documentation and third-party verification of the RDP protocol. As such, people in the security field are cautious to say that the most this protocol supports effective security this protocol provides is basic security, with no evidence of showing that the protocol is protected against such intrusions as Man In The Middle. There is a better way – and that would be using Citrix MetaFrame in addition to TS.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

History Behind Citrix MetaFrame

Citrix Systems, Inc. was started in 1989. Citrix started with a product called Citrix WinFrame. With the introduction of this server-based computing application, Citrix introduced the server based computing model and two technologies as well. The first is Citrix Independent Computing Architecture (ICA). ICA is a protocol adding features not supported by RDP, such as sound, higher color allowance, better handling at lower bandwidths (such as a 56K modem), and encryption. The second is Citrix MultiWin, which allows many users to run applications at the same time on one server. These technologies have carried over to MetaFrame. The latest version of MetaFrame is XP. However, do not confuse this with Microsoft XP implementations.

A look into Citrix's ICA Protocol

Before we look at how to configure a Citrix MetaFrame environment we must look at a few concepts that Citrix follows in its development strategies. The strength behind Citrix is it ability to use a Thin Client on a variety of operating system platforms. Lets take a look at what a definition of a thin client.

Thin client provides the ability for almost any computer system to access either Microsoft Windows based or Unix based applications over the Internet or better yet over a corporate Intranet. Lets assume you have a server running a thin client computing software like Citrix MetaFrame. You could have any Windows 32-bit application running on the server, for example Microsoft Office Professional. You would simply give that employee the ICA Client to load on their home personal computer and with some instructions they could now access MS Office Professional, their files and continue to work. One of Citrix's strong points is the ability to run a single application from a web page directly.

The strongest feature of using thin client server based software is that all the processing for an application is done at the server level. This allows people in remote sites to enjoy the processing power of these servers and gives managers an opportunity to show just why it was so important to spend the money on some powerful servers. Another nice feature is that the only traffic that passes to the workstation from the workstation is keyboard, mouse, screen information, sound, file sharing and printing.

The ICA protocol "has a layered architecture, which allows the insertion of a dedicated encryption protocol driver into its network stack." (http://www.nue.et-inf.uni-siegen.de/~schmidt/tcsecurity/protocols.html) This is important because it means that you can use any third party encryption that you prefer. Of course, Citrix does offer their own layer of encryption, aptly called Secure ICA. Which was an add-on for older versions of MetaFrame, but now comes packaged with the current versions of MetaFrame.

Why consider using the Citrix Client

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The following when making you decision about using the Citrix ICA client over another companies client.

⇒ Compatible with Windows 9x, NT, and 2000
⇒ Excellent ability to customize the interface

- Placing application icons in the Start menu
- Placing applications directly on the desktop based on group membership

⇒ Various ICA clients available

- ICA 32 bit Client
- ICA 16 bit Client
- ICA ActiveX Client
- Java ICA Client
- ICA DOS Client
- ICA Unix Clients
- ICA Windows CE Client
- ICA Macintosh Client

Source: www.thin-world.com/thindefined.htm

With all these advantages in mind, let us not forget the fact that ICA "has become the de facto industry standard for delivering corporate applications across the broadest variety of desktop platforms and networks." (http://www.sac-computer.com/CitrixFeatures.htm)

Why add MetaFrame to Windows Terminal Services

The time will come when you'll have to justify to upper management that there is a real benefit to using MetaFrame. Many business are now concerned with scalability. Managers do not like to be presented with a solution at one time that costs $200,000.00 and then within a week the same person comes back in and asks for another $100,000.00 because they forgot something or the solution was not designed for future growth. The combination of TS and MetaFrame allows for growth, enterprise application management, easy deployment of costly applications such as MS Office 2000 Professional, and allows employees to access these applications over the Internet from virtually anywhere regardless of hardware or software available at the remote site.

MetaFrame was designed and is continually being upgraded with security in mind. There are some security implications that you should be aware of. If the Citrix server is compromised, many users' "desktops" are compromised as well, and possibly take out of service while law enforcement agencies investigates. Single point of failure is the main argument against TS and Citrix, as well as the relatively outrageous hardware requirements to support a large number of users.

Implementing a Citrix MetaFrame Solution

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Now that we have looked at the benefits of using a combination of Microsoft and Citrix technologies the table below will outline what you will need to get started. In order to determine the necessary requirements I have decided to use the following as a guideline:

Project Outline

Scope: The purpose of the Citrix project is to provide employees of a government agency the ability to access data files from inside the protected network and run Microsoft Office 2000 Professional from a central server so that copies do not have to be purchased for each employee working form home.

Specifics: The government agency has about 300 employees, but right now only 15 will be allowed to access the Citrix server at one time. Based on past statistics gathered from the Information Systems Group when remote connectivity was offered a few years back only 3-5 people were logged on to the server concurrently.

Hardware: With further research and discussion with upper management it was discovered that the government agency requires that all servers to be used will be Hewlett Packard. The server must be rack mounted.

Pricing: The estimated costs provided in the tables below were obtained through web resources and several vendors. They represent the government's cost and as such the actual retail cost may be more.

Software Required

Item	Estimated Cost
Microsoft Windows 2000 Server,	$760.00
Microsoft Windows 2000 Usage CAL	$621.00 (for 20 users)
Microsoft Terminal Services CAL	$1,679.00 (for 20 users)
Microsoft Office XP Professional	$500.00
Citrix MetaFrame XP for Windows 2000 Servers	$4,995.00 (for 20 concurrent users)
Total Software Cost (Estimated)	**$8,555.00**

Hardware Required

Item	Estimated Cost
HP PIII/1.26 GHz Dual processor	$4,237.00
HP SDRAM (total of 2 gig RAM)	$2,584.00
HP NetRAID Controller	$865.00
Hard Drives SCSI-3 73.4 GB (2 drives)	$3,804.00
Total Hardware Cost (Estimated)	**$11,490.00**

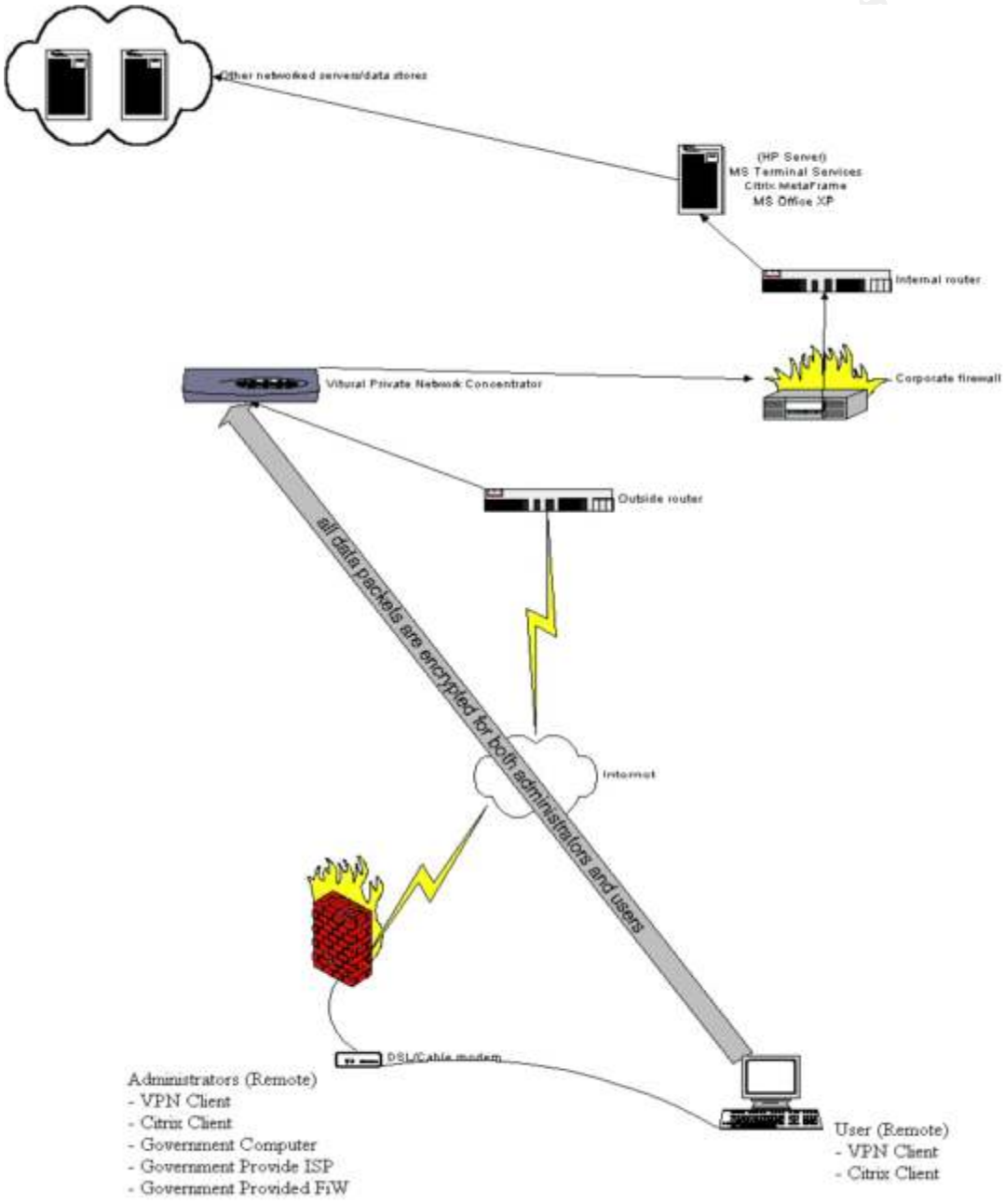
Approval: Now with actual costs associated with the project this can be presented to management for approval. Keep in mind that this cost is only for hardware

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

and software. The cost of personnel to install and maintain the system will be determined based on if the personnel are on staff or outsourced.

What will the network design look like?

With the backing of management and necessary budget lets take a look at how Terminal Services and MetaFrame will integrated into the existing network. Below is the diagram of how I would suggest the network look after implementation.



© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Basically as the diagram above shows you can break the remote access community down into two groups (administrators and users). The requirements for each are listed. The requirements for administrators are much more based upon the type of work they will be performing from a remote location.

Developed with security in mind

Within the solution proposed there is a layered approach to keeping the information that flows from the government network to the remote offices.

Corporate Firewall: this is a hardware device on the government's end that is used to permit/deny network traffic based upon Access Control Lists. Limitations can be set based upon network IP address or specific protocols. Modifications will have to be made to allow the appropriate VPN Client and Citrix Client software to pass through.

Virtual Private Network Concentrator: this is a hardware device controlled by the government, which will allow the remote workstations to create encrypted tunnels from the workstation to the concentrator.

Personal Firewall: this can be hardware or software based. Administrators should have a hardware firewall that is configured and controlled by the government. Normal remote users should have a firewall, but not maintained by the government since they will be using and ISP and computer that they have purchased.

DSL/Cable/Dial-Up; Administrators, where possible will be issued DSL connectivity with a static IP address. This measure limits the number of open connections necessary through the VPNC and Firewall devices.

The incorporation of all these devices is a necessary step to ensure the integrity of the governments data and limit the exposure to external threats.

Conclusion

The deployment of Microsoft Terminal Server and Citrix MetaFrame for use as a way in which employees and administrators to remotely gain access to a corporate or government network needs to be carefully planned out with upper management, security professionals, network administrators and the end users. Remote network connectivity is a must for a businesses survival. Hopefully you now have a better idea of what resources are available to you and how to implement a plan in which you can come up with a compromise between security and functionality.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References

About Citrix Systems, Inc., URL: http://www.citrix.com/company/

Gonce, Fred. Planning an Implementation of Citrix MetaFrame XP on Dell PowerEdge Servers, July 2001, URL: http://www.dell.com/downloads/us/pedge/citrix.doc

SAC Computer Solutions, Inc., Citrix Features, URL: http://www.sac-computer.com/CitrixFeatures.htm

SAC Computer Solutions, Inc., Citrix MetaFrame FAQ, URL: http://www.sac-computer.com/CitrixFAQ.htm

Citrix Support Solutions, SecureICA Option Pack, URL: http://www.citrix.com/support/solution/SOL00044.htm

Schmidt. Protocol Analysis, URL: http://www.nue.et-inf.uni-siegen.de/~schmidt/tcsecurity/protocols.html

Jacobs, April. Thin Clients A simple, money-saving options for users with limited needs. Computerworld, August 3, 1998, URL: http://careers.computerworld.com/home/features.nsf/all/980803qs

Kaplan, Steve and Mangus, Marc, Citrix Metaframe for Windows Terminal Services, Chapter 9, March 2000, URL: http://www.books.mcgraw-hill.com/betabooks/mar00/Kaplan/chap09.html

Microsoft Support Bulletin (Q232514), Securing Terminal Server Communications Between Client and Server, URL: http://support.Microsoft.com/default.aspx?scid=kb;EN-US;q232514

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced