Global Information Assurance Certification Paper

Secure Remote Access with Citrix Secure Gateway and Microsoft RDP

Brian Robertson
GIAC Security Essentials Certification (GSEC)
Version 1.4b
Option 1
March 30, 2004

ABSTRACT

Providing secure remote access to network resources while incorporating a multitude of application sets to end users is an increasingly complex challenge for IT workers. According to a recent study sponsored by AT&T, there are 16.5 million regularly employed teleworkers that telework at least one day a month.[1] In addition to regular telecommuters, typical organizations also have remote salespeople and corporate employees that need access to their applications away from the office.

Throughout this practical, Citrix Secure Gateway and Microsoft Windows technologies will be discussed. The primary scope will examine how an IT department can provide both secure remote access and provide users with the same application sets that are in use in the corporate office by implementing Citrix Secure Gateway and Microsoft Windows Remote Desktop Protocol. The initial installation of a Citrix MetaFrame XP farm is beyond the scope of this assignment. This practical will focus on the installation, configuration and securing of Microsoft Internet Information Services servers and Microsoft Remote Desktop Protocol services.

Citrix MetaFrame XP Presentation Server Overview

Citrix MetaFrame XP Presentation Server is an extension to the existing Terminal Services that are provided with Microsoft Windows servers. Citrix provides remote users access to centralized enterprise applications installed on MetaFrame servers. Applications are published on the servers and made available to end users by the Citrix administrator. In addition to publishing applications, this paper will demonstrate how you can publish a Remote Desktop Protocol profile of a Windows XP machine that will allow a user secure remote access to their corporate workstation that is loaded up with their appropriate application sets.

The diagram below (Figure 1) illustrates the placement within the network of the various pieces that make up an implementation of Citrix Secure gateway.

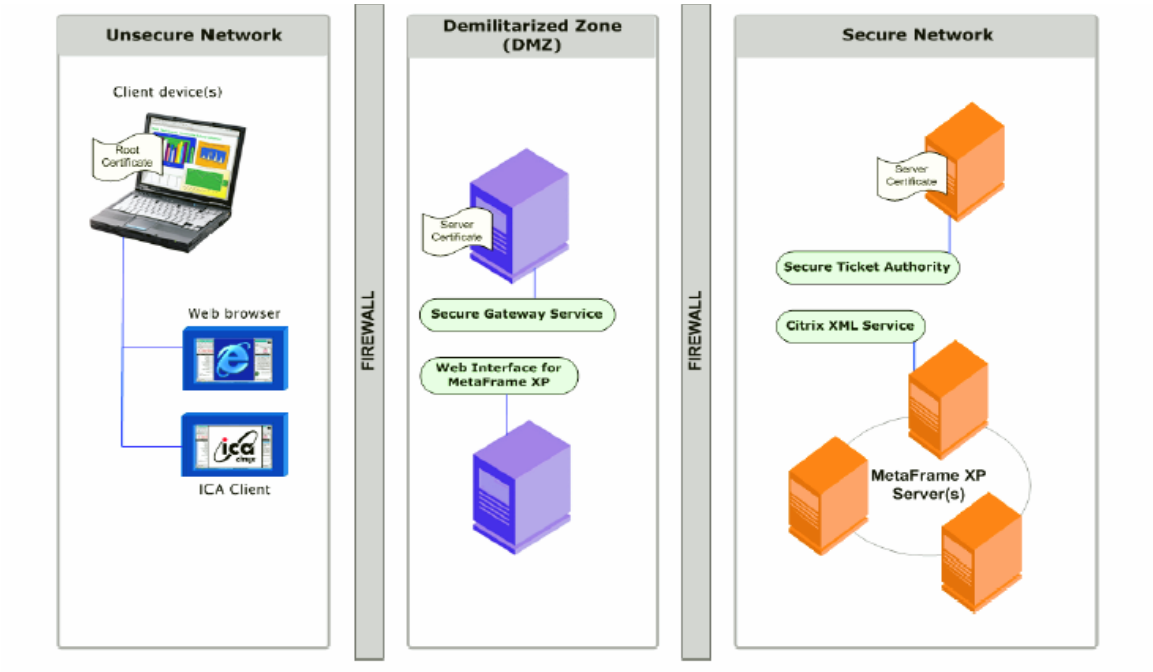


Figure 1 [2]

Secure Network (Internal Network)

The internal network contains the Citrix MetaFrame XP farm and the Citrix Secure Ticket Authority. In order to deploy the Secure Gateway product you must have a MetaFrame XP farm. The MetaFrame farm consists of one or more Microsoft NT/2000 Servers running Terminal Services. The servers in the farm have applications installed on them that are provided to network users. Any server within the farm may be designated to host the Citrix XML service. The Citrix XML service holds a listing of all installed applications within the farm and their respective locations within the farm. When a user accesses the web interface, the web server contacts the XML service to provide a list of applications the user is granted access.

The internal network is additionally comprised of the Citrix Secure Ticket Authority (STA). The STA is installed on a Windows 2000 Server running Internet Information Services (IIS) 5.0. The Secure Ticket Authority is responsible for issuing “session” tickets to clients who are requesting access to published resources. The requests themselves are forwarded from the Secure Gateway server in the DMZ. In order to secure communications between the Secure Gateway server and the Secure Ticket Authority server a server certificate from a commercial certificate authority needs to be installed on this server.

The Demilitarized Zone (DMZ)

Next is to install and configure the components that will reside in the Demilitarized Zone (DMZ). These servers are accessible from the unsecured

public network and increased care must be taken in the configuration and maintenance to ensure their availability and integrity.

The Web Interface for MetaFrame XP Server provides just what its name implies, the graphical user interface (GUI) that the user receives when they enter the address of the Secure Gateway Server into their internet browser. This server provides the interface for logging into the Citrix MetaFrame XP server farm as captured below (figure 2).

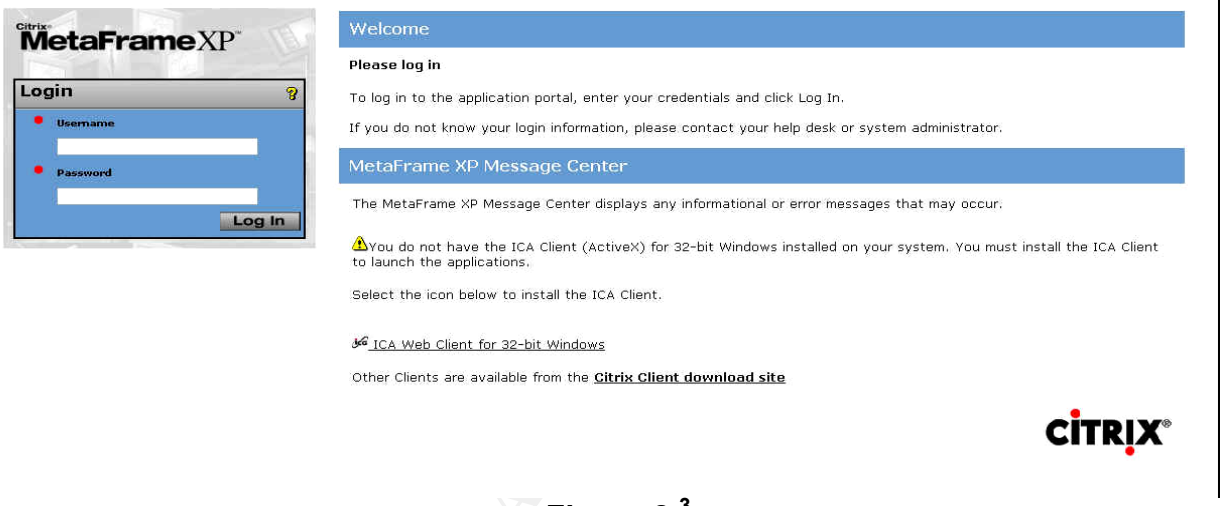


Figure 2 [3]

The last piece of this configuration that resides in the DMZ is the Secure Gateway Server. This server provides the Secure Sockets Layer (SSL) or Transport Layer Session (TLS) protocol encrypted session with the end users browser. The Secure Gateway Server provides 128 bit encryption through the use of digital server certificates from a commercial certificate authority. The use of the Secure Gateway allows for a single point of entry into the server farm that is encrypted. Data between the client and secure gateway resides on TCP ports 80 and 443 which are typically open on firewalls in most corporate networks.

End User's Workstation (Internet)

The end users workstation will need the Citrix ICA web client in order to access published resources via the Citrix Secure Gateway. The web client will install on Internet Explorer 5.0 or later, Netscape Navigator or Communicator version 4.78, 6.2, or later. The operating system requirements are Windows 9X, Windows 2000, and Windows XP[4]. The latest Citrix web clients can be downloaded at www.citrix.com or a download can be made from the Web Interface Server during the initial login.

Configure the Servers

With an understanding of the basic architecture, it is now time to cover configuration details for the needed servers. With the exception of the servers that hold the actual applications in the Citrix server farm, three Windows 2000 servers running Internet Information Services 5.0 (IIS) web servers will be needed.

Building a secure Windows server running IIS is a daunting task. IIS servers have been a preferred target of malicious code writers and hackers alike for several years now. The following steps should be taken to secure your IIS servers. Citrix Consulting Services has compiled an excellent reference paper titled “Best Practices for Securing a Citrix Secure Gateway” that details steps you should take to harden your deployment. Another excellent reference for assistance when configuring a secure web server is from the National Security Agency titled “Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0”. The following steps will add significant security posture to your deployment, though they do not by any means guarantee the systems will not be compromised by a determined attacker. An administrator should consult with his/hers companies’ policy to determine their requirements. The idea here is not to provide “low hanging fruit” to a potential attacker and hope they will find more inviting targets elsewhere.

Operating System Installation

There are two fundamental steps to increase security at the point of operating system installation. The first step is to choose an installation directory other than the default, C:\WINNT. Creating an alternate directory will render malicious scripts that look for system files in the default directory useless against your server.

The second step is to install on a partition formatted with the NTFS file system. Unlike the FAT file system, NTFS allows setting specific individual permissions on files and directories alike. NTFS also allows for us to audit events on the file system.

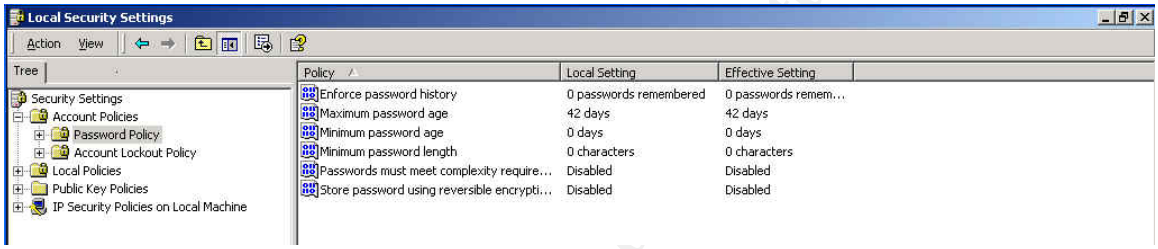
Post Operating System Installation

Both the Secure Gateway and Web Interface Server will be located in the Demilitarized Zone. They will be installed as standalone servers and will require the security and auditing policies to be setup locally on each server. The Secure Ticket Authority Server will be installed as a member server of the internal domain so the policies can be applied from the domain level.
The following are important steps one should take from a local policy perspective.

User Account Policies

The following steps should be applied to user accounts and passwords.

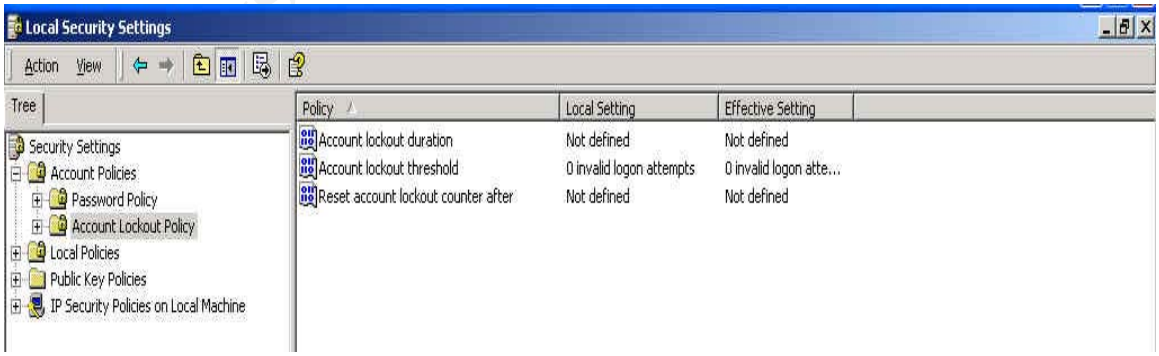
1. Rename the administrator account. A strong password should have been given to the administrator account during installation.
2. Check to make sure the Guest account is disabled. This account is disabled by default, never hurts to check.
3. Set the minimum password length to 8 characters.
4. Set account password age to 30 days.
5. Password must meet complexity requirements. Policy should be set to require a strong password made up of upper and lower case as well as characters and numbers.



Account Lockout Policies

Dictionary and brute force attacks are used to try and “generate” a correct password in order to access a system. There are two major changes one can make to their account lockout policies that will dramatically lower the chances that one of the attacks will be successful against your server.

1. Account lockout duration should be set to 60 minutes at a minimum.
2. Account lockout thresholds determine how many unsuccessful login attempts a user can have before the account is locked out. This number should be no higher than 3.

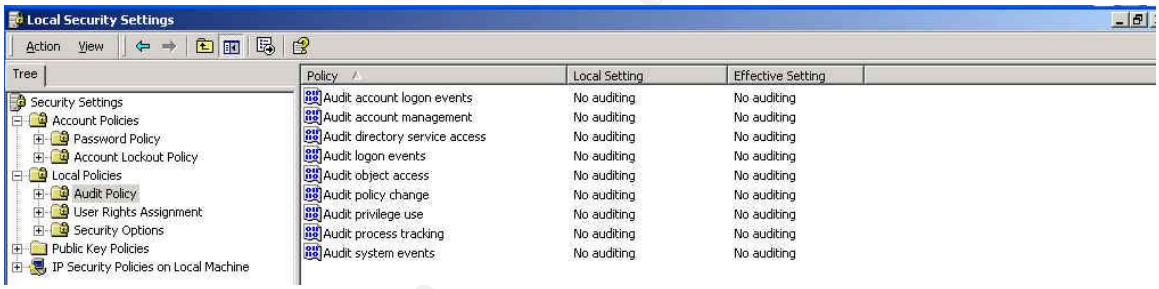


Auditing Policies

Audit policies allow an administrator to have a log of all audited system events over a period of time. Auditing is disabled by default and should be enabled to track events made by either an application or a user on the system. Security related events are kept in the security log and should be checked time to time for suspicious activity. The following are some of the major audit policies that are recommended.

1. Audit logon events. Both success and failure.
2. Audit account management. Both success and failure
3. Audit policy change. Both success and failure.
4. Audit system events. Both success and failure.

The default log settings should also be changed from their default size of 512k to allow for an effective amount of data to be held within. Application, System, and Security log file sizes should all be changed to accommodate at least 50MB before they start to overwrite events. Permissions to access the logs should also be set to only allow administrators access to them.



Service Packs and HotFixes

Microsoft releases updates to its applications and operating systems in the form of service packs. Service packs include all hotfix releases and other code fixes up to the date of their release. At the time of this writing service pack four has been released for Windows 2000. It is absolutely critical to install the latest service pack for both the operating system and other installed Microsoft applications before putting servers in production. After installing the latest service pack, download and run the Microsoft Baseline Security Analyzer (MBSA) and install whatever other hotfixes the MBSA scan finds that are missing.

Disable Services

A default installation of Windows 2000 Server installs and enables a number of services that are not needed. All installed services provide a potential weakness

if vulnerabilities are discovered that exploit that particular service. Here are the steps to take to remove unnecessary services.

- From a command line, type services.msc, this will bring up a window listing all your installed services.
- Right click the service name and choose properties.
- Drop down the startup type list box and select disable.

Here is a list of the services to be set to “disabled” in alphabetical order.

- Application Management
- Computer Browser
- DHCP Client
- Fax Service
- Index Service
- Internet Connection Sharing
- Intersite Messaging
- Messenger
- Net Meeting Remote Desktop Sharing
- Network DDE
- Performance Logs and Alerts
- Print Spooler
- QoS RSVP
- Remote Access Auto Configuration Manager
- Remote Access Connection Manager
- Remote Registry Service
- RunAs Service
- Smart Card
- Smart Card Helper
- TCP/IP NetBIOS Helper Service
- Telephony
- Telnet
- Terminal Services
- Windows installer
- WINS

Locking Down IIS

A default installation of Microsoft IIS can by no means be considered a secure web server. IIS by default installs with minimal file-system permissions as well as sample scripts and default file handlers that have been easily exploited by malicious users in the past.[5]

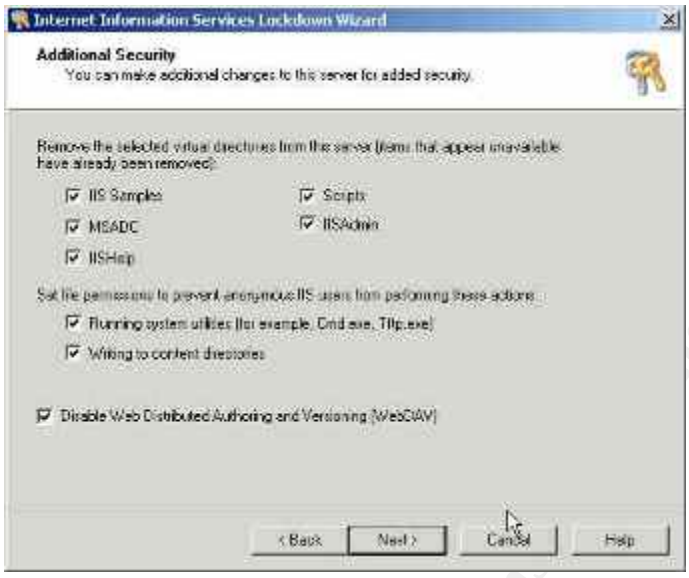
Microsoft provides a free download named IIS lockdown tool to aid an administrator in securing an installation of IIS. This tool provides a GUI interface to perform many tasks that used to have to be done manually. These tasks

include disabling unused web services, un-mapping default file handlers, un-mapping sample directories and scripts, modifying file permissions, and modifying WebDAV permissions.

The first step to take to secure the server is to disable or remove and unused services installed by the web server. A full install of IIS will install not only the Web Service (HTTP) but also File Transfer Protocol service (FTP), Simple Mail Transport Protocol service (SMTP) and Network News Transfer Protocol (NNTP). An implementation of Citrix Secure Gateway only requires the web service, so the other services should be removed altogether.

IIS provides many default file extension associations that allow it to provide functionality for many different application types. The mappings that will not be used on the server should be “un-mapped” with the IIS lockdown tool if unused. The .dll files used by these mappings have been exploited by buffer overflow attacks. A Secure Gateway Server implementation uses ASP pages so that mapping should be left in place. The IIS lockdown tool does not delete the files but simply un-maps them so they can easily be replaced if needed by running the tool again.

Microsoft IIS installs sample scripts and applications by default to demonstrate the capabilities of the web server.[6] They have been found to have several vulnerabilities and have been widely exploited. The IIS Lockdown tool can be used to disable the mappings of these samples and can be easily restored to their original functionality if needed, though this is unlikely.



IIS 5 supports the use of Web Distributed Authoring and Versioning, or as it is most commonly known WebDAV. WebDAV allows an authorized user the ability to manage a web site remotely. This added functionality also comes with many well documented exploits. Check the box within IIS Lockdown that will disable this feature.

File permissions are modified on the web servers root directory located at Inetpub\wwwroot. The tool explicitly denies an anonymous user the ability to create or delete files, alter data, or modify permission settings on files located in the root directory. By default IIS also creates a user account to allow anonymous access to the web servers. This user account name is IUSR_*Computername.* This account is given permissions to log on as a batch job should be disabled. A new user account with limited privileges should be created and IIS can be configured to use this account for anonymous connections to the server.

- An implementation of Citrix Secure Gateway requires the following user account privileges in order to operate correctly.
- Web Interface Server- The account created for anonymous access should have Read/Write access to the Web Interface Folder located in IIS.
- Secure Ticket Authority Server- The account given anonymous access permissions should have Modify access to the scripts folder. Any other accounts should be set to Read Only.
- Secure Gateway Server – Anonymous user account must have read access to web directories.

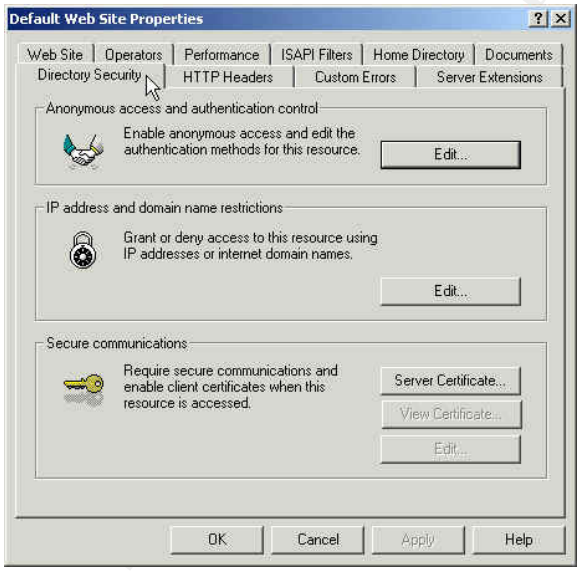
Installing SSL Certificates

All communications between the clients' web browser and the Secure Gateway Server will be over the public internet and needs to be encrypted.

Secure Gateway supports the use of unencrypted communications over TCP port 80 but this is not recommended. By installing a Secure Sockets Layer (SSL) digital certificate, all transmissions between a client and the web server will benefit from the security 128-bit encryption.

The following steps are necessary to acquire an SSL digital certificate from a trusted third part certificate authority and install on your server.

- From the Internet Services manager located in Administrative tools, right click default web site and select properties.
- From the Directory Security Tab, select the server certificate button near the bottom of the window.



- This will launch the Welcome to the Web Server Certificate Wizard

- The wizard will ask for information about your organization and the server that will be hosting the certificate. After inputting this information, the wizard will create a text file with the answers. Send this text file to a third party certificate authority such as Verisign.
- The third party certificate authority will then run through the necessary steps of validating the organization and will then issue a certificate to install on the web servers.
- Once the certificate has been received, the Web Server Certificate Wizard can be run again to install the certificate on the server.
- To apply the certificate to the website, open the Internet Services Manager, right click the web site, and choose properties. Select the Directory Security tab.
- Click edit from within secure communications. From here require secure channel should be checked as well as require 128-bit encryption. If require 128-bit encryption is not checked some older browsers will connect using 40-bit encryption, which can be defeated.

Additional Security Measures

The Secure Ticket Authority server will only need to accept connections from the Web Interface and Secure Gateway servers. TCP/IP filtering can be enabled on the Secure Ticket Authority server in order to prevent an unauthorized host from receiving a valid session ticket and potentially have access to published resources. To enable TCP/IP filter on a Windows 2000 Server.

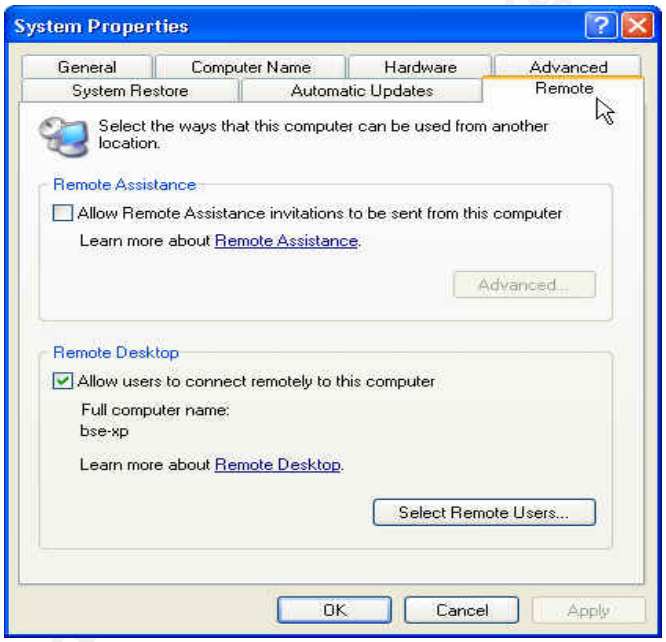
- Start , settings, network connections
- Right click the network connection, choose properties
- Select TCP/IP and click properties
- Select TCP/IP Filtering, TCP Protocol Permit only
- Input IP addresses of Web Interface and Secure Gateway

The Secure Ticket Authority will now only respond to connection requests from the two servers IP addresses that were entered.

A Citrix Secure Gateway can also be used in conjunction with RSA SecurID to provide two-factor user authentication[7]. SecurID tokens are assigned to users and generate a different code every 60 seconds. When a user attempts to login to the Secure Gateway server they will need to provide something they have, the RSA token, and something they know, a password. This implementation provides a greater degree of security against unauthorized access because simply knowing a valid password will not be enough to grant you access to published applications.

Remote Desktop Configuration

Microsoft Windows XP Professional provides a feature named Remote Desktop. Remote Desktop can be thought of as a light version of Windows Terminal Server, because Windows XP Remote Desktop only supports one remote session at a time. An XP computer will refuse any further connections from the same user account after one session has initiated, if another authorized user tries to connect to a Windows XP computer that already has an active remote session, it will prompt that it will log off the current user if proceeding. To begin using Remote Desktop, you have to configure the XP computer to accept remote connections; by default this is not enabled.

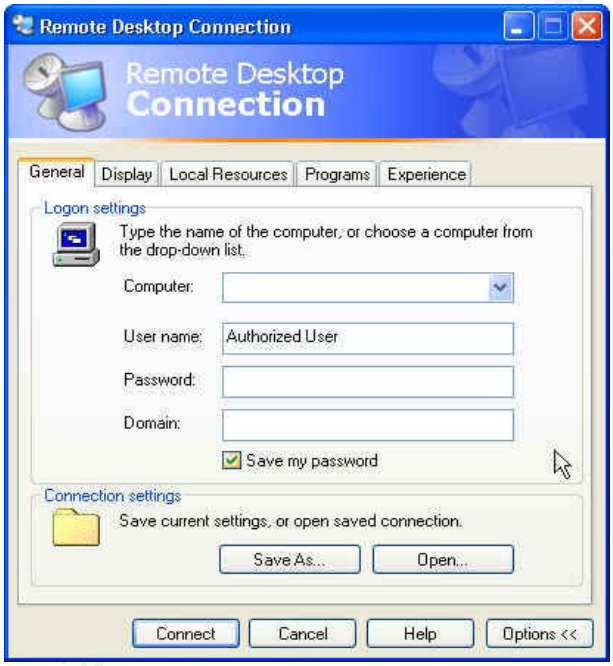


- Right click My Computer to bring up the system properties window
- Select the remote tab and check the box “allow users to connect remotely to this computer”
- Click select remote users and add the appropriate user accounts.

Completing the above steps is necessary to enable Remote Desktop on a Windows XP Professional computer. Any Windows client from Windows 95 and later will connect to a remote XP computer if the Remote Desktop Connection client software is loaded on it. At the time of this writing, Remote Desktop Connection for Windows 5.2.3790 is the latest version of the client and can be downloaded for free at www.microsoft.com/downloads. After the client is installed, simply input the name or IP address of the remote server and a connection will be made. If proper authentication is met, a desktop of the remote machine will be presented. Data between the client and the remote host will be encrypted with a 128-bit algorithm.

Windows Remote Desktop Connection software has many configuration settings that can be saved in a remote session profile to be used each time a connection is made. This allows an administrator to pre-configure a session profile that meets the performance and security requirements of their organization and makes it easier for the end user to initiate sessions to the remote computer.

To configure a Remote Desktop Connection profile, launch the client and complete the following steps.



- Input the computer name or IP address of the remote host.
- Enter username, password, and Domain name. Uncheck the “save my password” box for added security.
- Configure desktop size and color depth under Display tab
- Configure local resources
    - Remote computer sound, select do not play
    - Keyboard, select full screen only
    - Local Devices, for usability purposes, select disk drives, printers, and serial ports
- Programs, leave unchecked
- Experience- Choose custom and only check bitmap caching for added performance.
- Return to the General tab and select save as, and save the profile. The profile can now to be double clicked to initiate a remote session with the settings that were configured before.

The saved session can now be advertised out to selected users from within the Citrix farm. When the user connects to the Secure Gateway Server

and enters the proper credentials, the Remote Desktop Connection profile will be available for he or she to select when published by the Citrix administrator. They will again be prompted for authentication, but this time to the remote Windows XP computer they are initiating a remote session with. If the credentials are authorized the user will be presented with the XP desktop that has all the applications they use in the office.

Conclusion

There are many solutions available today for providing remote access to employees. Clearly, some are more complex than others. Citrix Secure Gateway is a logical choice if an organization is already deploying MetaFrame XP servers as Secure Gateway is licensed with the initial purchase. Secure Gateway offers simplified firewall management through the use of ports that are commonly open on today's corporate networks. Encryption of the data streams is achieved using industry standard 128 bit SSL. An implementation of Citrix Secure Gateway in conjunction with Microsoft XP Remote Desktop Protocol offers remote users secure access to their application sets installed on their corporate computers. Users are not burdened by complex VPN clients and configurations. A user simply needs a reliable connection to the internet and a one time install of the Citrix web client to enjoy the access they are accustomed to in the office.

The scope of this practical was to offer some insight into how Citrix Secure Gateway is implemented and how to secure the web servers that make up the deployment. The security steps outlined may not meet the requirements of different organizations but will go a long way in avoiding being "low hanging fruit" to an opportunistic attacker.

References

1. Citrix Secure Gateway 1.1 for Windows Administrator's Guide – English http://support.citrix.com/servlet/KbServlet/download/134-102-7736/Windows_Secure_Gateway_Guide.pdf

2. Secure Gateway for MetaFrame Administrator's Guide http://support.citrix.com/servlet/KbServlet/download/2373-102-8730/Windows_Secure_Gateway_Guide.pdf

3. Telework America, Behavior Research Center study (July 2000) http://www.workingfromanywhere.org/pdf/ITACTeleworkAmerica2000KeyFindings.pdf

4. Administrator's Guide - Citrix® ICA® Win32 Clients - Version 7.0 – English http://support.citrix.com/servlet/KbServlet/download/169-102-8767/ICA_Win32_Guide.pdf

5. Getting Started with Windows XP http://www.microsoft.com/windowsxp/pro/using/howto/gomobile/remotedesktop/default.asp

6. William E Walker, Sheila M Chrisman: Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0. http://www.nsa.gov/snac/os/win2k/iis_5_v1_4.pdf

7. Nishchal Bhalla and Rohyt Belani IIS Lockdown and URLScan, (January 5 2003) http://www.securityfocus.com/infocus/1755

8. Owen R McGovern and Julia M Haney Guide to Securing Microsoft Windows 2000 File and Disk Resources, (April 19, 2001) http://www.nsa.gov/snac/os/win2k/w2k_file_disk_resource.pdf

9. Savage, Marcia (Nov 2003) Peace of Mind in Remote Use SC Magazine

10. Secure Internet Information Services 5 Checklist, Microsoft Corporation http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/tips/iis5chk.mspx

11. Citrix Consulting Services, Best Practices for Securing a Citrix Secure Gateway Deployment (March 2002) http://www.go-eol.com/seminars/presentations/BestPracSecCSG.pdf

[1] Telework America, Behavior Research Center study (July 2000)
[2] Secure Gateway for MetaFrame Administrator's Guide
[3] Secure Gateway for MetaFrame Administrator's Guide
[4] Administrators Guide Citrix WIN32 Clients
[5] IIS Lockdown and URLSCAN
[6] IIS Lockdown and URLSCAN
[7] Peace of Mind in Remote Use