GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Kevin C. Teaff
March 11, 2004

SANS

Securing Citrix Metaframe XP and Citrix Nfuse Classic 1.7 in a Windows Environment

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Table of Contents 1

Abstract 2

Overview 2

Ports used by Citrix and Nfuse 4

Nfuse/IIS Placement and Citrix Server Placement 5

Reasons for separating Nfuse/IIS and Citrix 5

Pre-Installation and Configuration of Nfuse/IIS box 6

Nfuse 1.7 software installation 6

How to move Nfuse to a new web site 7

Baseline Security Analyzer 7

Running IIS Lockdown with Nfuse 1.7 8

URLSCAN 10

NfuseAdmin/Nfuse.Conf 11

Misc. Security elements impacting Nfuse and Citrix 12

- Web Page Timeout 12
- Passwords and Two-Factor Authentication 13
- Ticketing 13
- SSL 13
- SSL Relay 14
- Secure ICA 14
- VPN 14

Securing Citrix at the Connection level 15

- Some suggestions for securing Citrix Connections 15

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Conclusion 17

References 18

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Abstract

With the release of Citrix Nfuse, companies are now able to deliver their Citrix-based applications not just to LAN/WAN clients, but to users over the internet. When delivering business applications over the internet, security is the key consideration.

There are two software components discussed in this paper, Citrix Nfuse Classic 1.7 and Citrix Metaframe XP. We will treat both of these as separate products which can be secured using different strategies, depending on the environment in which they are implemented.

This paper will focus on securing these products using four main strategies. First, securing the base Operating System. Second, securing Microsoft Internet Information Server. Third, making configuration changes to Citrix products that enhance security.

Within this document I will attempt to provide a basic overview of the Citrix Nfuse 1.7 product with strategies and options for securing it. This document will also cover various elements of the Citrix Metaframe XP product suite that can have an impact on security.

This paper will focus on Citrix Metaframe XP for Windows 2000, Windows-based Clients, and Nfuse Classic 1.7 for IIS (Internet Information Server) 5.x on Windows 2000 Server.

Overview

Citrix MetaFrame is a popular thin-client solution for delivering business applications. Primary benefits of this product include; one, the ability to deliver critical business apps (email, ERP, CRM, etc) to users in disparate locations regardless of bandwidth and desktop hardware/software and, two, the reduction of the costs of delivering complex business applications.

Citrix has been around for some time, with the majority of early implementations revolving around using Citrix in a LAN/WAN/Dialup environment to deliver applications. With the advent of the Citrix Nfuse product, companies are now able to use Citrix not just for internal LAN/WAN implementations, but also for delivering Citrix-hosted applications over the Internet. Essentially, any user with an Internet connection and a web-browser could access their business applications.

© SANS Institute 2000 - 2005 Author retains full rights.

Nfuse has provided businesses with a powerful tool for delivering applications. However, any time critical business applications and data are delivered over the Internet, security concerns become paramount.

Implementing and successfully securing Nfuse also requires expanding the skillset of many Citrix Administrators. Prior to Nfuse, Citrix Administrators were mainly focused on getting their applications to reliably work on Citrix and protecting Citrix servers from accidental user error. For many Citrix Administrators, implementing Nfuse was their first experience with exposed production web-servers.

So what is Nfuse? It's essentially a web-based version of the old Citrix "Program Neighborhood" client, or at least provides the same functions.

Nfuse is a series of web pages that allows a user to:

1. Enter a userid and password
2. Receive a list of published applications
3. Initialize a Citrix session and access a published application

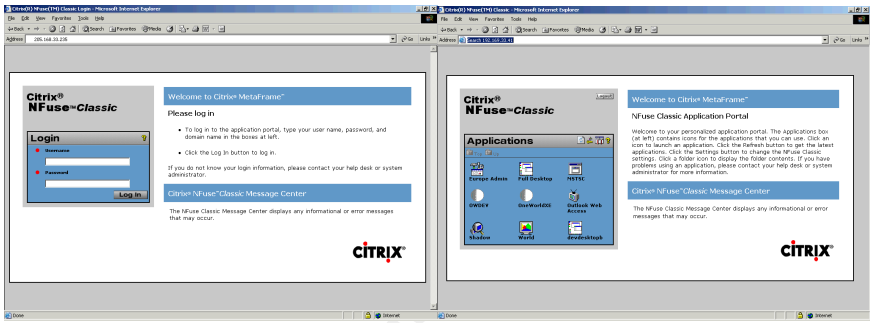
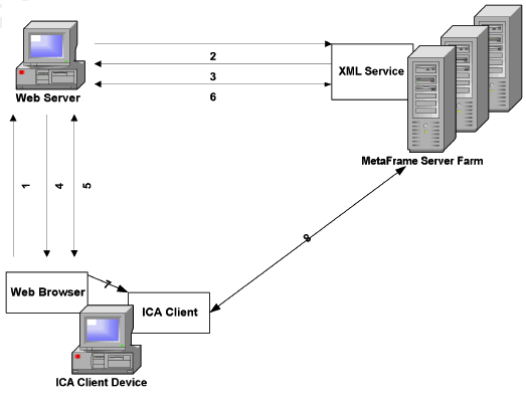


Figure 1. Nfuse 1.7 Classic's Login.ASP and Frameset.ASP

Nfuse does require some variation of the "Citrix Client" installed on the users workstation. For Windows users, the web-client, PN-agent, and full PN client all provide the functionality for a user to access an Nfuse site successfully.

How does Nfuse 1.7 work? The Nfuse 1.7 Administrators guide (P. 20) provides a good overview:



© SANS Institute 2000 - 2005
Author retains full rights.

Figure 2. Nfuse Administrator's guide p. 20.

1. An ICA Client device user utilizes a Web browser to view the NFuse Classic Login page and enters his or her user credentials. The credentials are sent as a standard HTTP request over the default HTTP port 80.
2. The Web server reads the user™s information and uses the NFuse Classic Java
objects to forward the information to the Citrix XML Service on a MetaFrame server in the server farm. The designated server acts as a broker between the Web server and the MetaFrame server farm.
The Citrix XML Service on the designated server then retrieves from the farm a list of applications that the user can access. These applications comprise the user™s *application se*t. In MetaFrame XP and MetaFrame 1.8 server farms, the XML Service retrieves the application set from the Independent Management Architecture (IMA) system and Program Neighborhood Service, respectively.
In a MetaFrame for UNIX Operating Systems farm, the Citrix XML Service on the designated MetaFrame server uses information gathered from the ICA Browser and the local NFuse configuration file to determine which applications the user can access.
The Citrix XML Service then forwards the user™s application set information to the NFuse Classic Java objects running on the Web server.
4. The Web server uses the NFuse Classic Java objects to generate an HTML page
containing links to the applications in the user™s application set. Each hyperlink in the HTML page points to a template file stored on the Web server. This file serves as a template from which NFuse Classic can dynamically generate ICA files. *ICA files* are text files containing parameters that configure ICA session properties such as the application to run in the session, the address of the server that will execute the application, and the properties of the window in which to display the application. ICA files are written in .Ini file format and have an .Ica extension.
5. The user initiates the next step by clicking one of the hyperlinks in the HTML page. The Web browser sends a request to the Web server to retrieve an ICA file
for the selected application.
The Web server passes this request to the NFuse Classic Java objects, which retrieve the template ICA file. The template file contains substitution tags. The Java objects replace the substitution tags in the template ICA file with information specific to the user and desired application. The Java objects then send the customized ICA file to the Web browser.
6. The Citrix XML Service is contacted to locate the least-busy MetaFrame server in the farm.
7. The Web browser receives the ICA file and passes it to the ICA Client device.
8. The ICA Client receives the ICA file and initiates an ICA session with a MetaFrame server according to the ICA file™s connection information.

Ports used by Citrix and Nfuse

Citrix and Nfuse use a number of TCP/IP port assignments for a variety of functions (CTX184502):

© SANS Institute 2000 - 2005 Author retains full rights.

- Port 1494 (TCP) This is the actual port used to initialize a Citrix Session. Generally, this port is opened inbound to the Citrix Servers.
- Port 80 (TCP) Besides being the default port assignment for HTTP traffic, this is also the default port setting used for XML traffic to pass credentials and published application data between the Nfuse/IIS server and the Citrix Server. This port is opened inbound and outbound between the Nfuse/IIS server and the Citrix Server(s). This port configuration can be changed for security and network auditing purposes (Madden, 637).
- Port 1023 and above (UDP and TCP) outbound from the Citrix Servers. These high-ports are randomly assigned.

NOTE: Port 1604 for UDP is often referenced in Citrix documentation, this port is used by the Program Neighborhood Client to communicate published application information between the Citrix Farm and Program Neighborhood. This port is not needed in an Nfuse/IIS implementation.

Nfuse/IIS Placement and Citrix Server Placement

Where you place your Nfuse/IIS server and Citrix server(s) is a key element in securing your Citrix/Nfuse implementation. While there are a number of approaches to delivering Citrix apps over the internet, a de-facto standard has evolved whereby the Nfuse/IIS server resides in a DMZ and the Citrix Server(s) reside behind a firewall. This approach seems to balance the competing desires of security versus functionality, as well as limiting the amount of open inbound ports on the firewall (Madden, 634).

Another approach is to place both the Nfuse/IIS server and Citrix server(s) behind the firewall. This approach is best for LAN/WAN implementations and is not recommended for users accessing Citrix over the Internet, as it potentially opens port 80 inbound to your entire internal network (Madden, 635).

Some Citrix Administrators are choosing to run Nfuse/IIS and Citrix on the same server. Again, for the reasons stated above, this approach is best for LAN/WAN implementations and is not recommended for users accessing Citrix over the Internet.

Reasons for separating Nfuse/IIS and Citrix

Microsoft patches for IIS and other Microsoft components have a tendency to break Citrix Metaframe components. Keeping Nfuse and Citrix separate allows you to aggressively patch your Nfuse/IIS Server while taking a more structured approach to patching your Citrix Server, giving you time to research the impact of the patch on a Citrix Server (CTX102523).

Citrix servers generally need high-performance hardware to host applications

© SANS Institute 2000 - 2005 Author retains full rights.

effectively while Nfuse/IIS does not require near the same level of hardware (Microsoft, 3).

Due to the configuration of the NFUSE.CONF file, a single instance of Nfuse on IIS will not be able to host applications to both internal users and external users (CTX103197).

Pre-Installation and Configuration of Nfuse/IIS box

The task of securing Nfuse 1.7 is primarily done by securing Internet Information Server (IIS) and Windows. By installing your operating system and configuring IIS with security in mind, you have gone a long way to securing Nfuse. It is beyond the scope of this paper to cover the details of securing Windows 2000 or IIS, but there are a variety instruction guides and templates which are freely available which cover the process of securing these products.

Below are some references to suggested guides and templates:

http://www.cisecurity.org/bench_win2000.html

http://www.nsa.gov/snac/win2k/index.html

http://www.microsoft.com/security/guidance/topics/ServerSecurity.mspx

Prior to installing Nfuse, a recommended strategy would be to do a secure installation and configuration of Windows 2003 (standalone server, no DC, minimal components, disables services, ntfs, etc), then do a secure installation and configuration of IIS (disable default page, remove helps, remove sample site, etc) and then install Nfuse. After the installation of Nfuse 1.7 (and moving pages to a new web site) you should test the basic functionality of Nfuse before further securing the box. Then it becomes a matter of further securing the server and testing the functionality of Nfuse. Using this step-wise model, it should be easy to track down what secured component broke Nfuse and be able to recover accordingly.

It is often recommended to disable the “default web site” or “Default Page” that comes pre-configured with IIS (SANS, 1326). Note that Nfuse 1.7 assumes you will be using the Default Page and installs many Nfuse components into wwwroot. In order to migrate Nfuse 1.7 to another web site, you will need to complete a few additional steps after the installation, which will be covered later in this document.

© SANS Institute 2000 - 2005 Author retains full rights.

Nfuse 1.7 software installation

For the most part, the install of Nfuse itself is pretty much a "Next, Next, I agree, Finish" install. But, there are a couple of key steps worth mentioning.

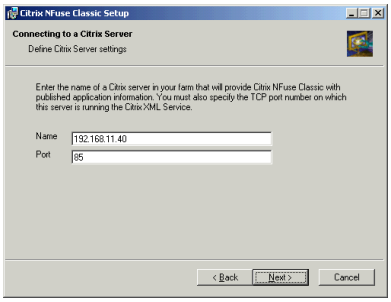


Figure 3. Nfuse 1.7 Classic Setup.

Notice the installation is asking for a computer name, in many DMZ environments, you may not be able to enter a NETBIOS-based computer name for a machine that is on the internal network; an IP address will work fine. Also notice that you are asked to enter a port number, it defaults to 80, but you have the option to change it.

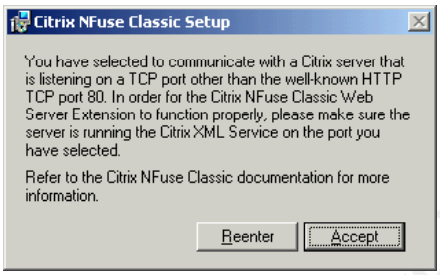


Figure 4. Nfuse 1.7 Classic Setup.

If you do change the default port setting for Nfuse XML traffic, you will be prompted to confirm the change.

How to move Nfuse to a new web site

First, you'll need to create a new web site. Create a new directory to store the new web site. Then, within Internet Information Services MMC, create a new web site using the "Web Site Wizard"; in most cases you can use the defaults. After you have created the new web site, copy the Nfuse pages from wwwroot. Finally, according to Douglas Brown (Citrix Systems Engineer) "Right-click the NFuse17 folder in IIS Manager, view its properties and on the Directory tab in the Application Settings area and click 'Create'". This step should allow Nfuse to function properly in the new web site. You will also have to modify the NFUSE.CONF file to reflect the new location of the web site. The NFUSE.CONF file will be discussed further later in this document.

© SANS Institute 2000 - 2005 Author retains full rights.

At this point, you should check the basic functionality of Nfuse. You should be able to login to Nfuse, receive a list of published apps, and initialize a Citrix session.

Baseline Security Analyzer

Now is probably a good time to run Microsoft Baseline Security Analyzer. There are no particular issues with running it against an instance of Nfuse, just remember to check the appropriate options. After running the Security Analyzer, apply the recommended patches and configuration changes and re-test the basic functionality of Nfuse.

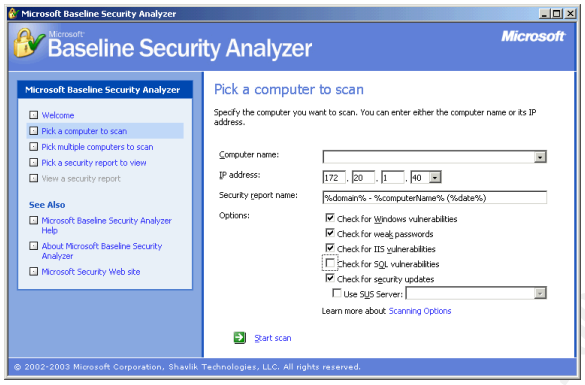
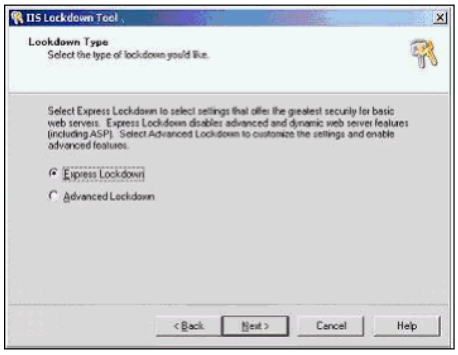


Figure 5. Microsoft Baseline Security Analyzer.

Running IIS Lockdown with Nfuse 1.7

The next step would be to run IIS Lockdown. Beware, according to Citrix Knowledge Base document CTX101778, running IIS lockdown in “Express Mode” will “render Nfuse inoperable”. Make sure to select the “Advanced Lockdown” option.



Then, de-select the option “Disable support for Active Server Pages”

© SANS Institute 2000 - 2005
Author retains full rights.

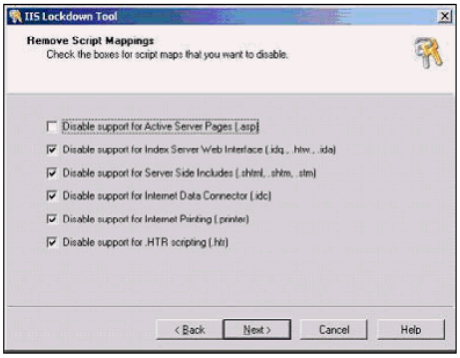


Figure 7. IIS Lockdown Setup.

Next, make sure to select "Dynamic Web Server" (ASP enabled) and select "View template settings"

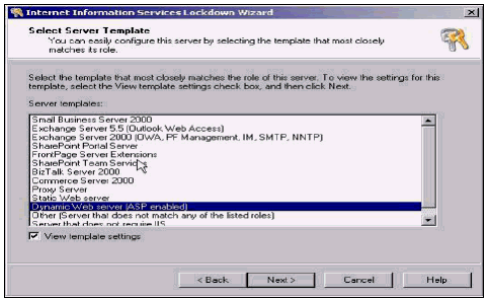


Figure 8. IIS Lockdown Setup.

If you are only using HTTP, de-select all unused web services.

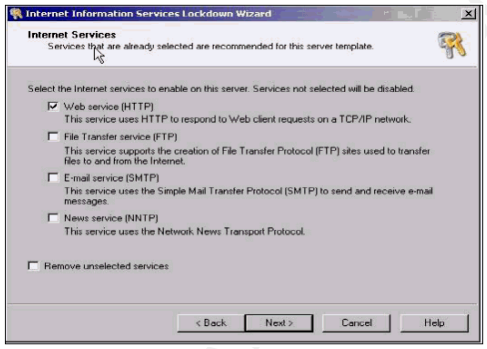


Figure 9. IIS Lockdown Setup.

When you get to the section on "Script Maps", make sure to un-"check" "Active Server Pages"

© SANS Institute 2000 - 2005 Author retains full rights.

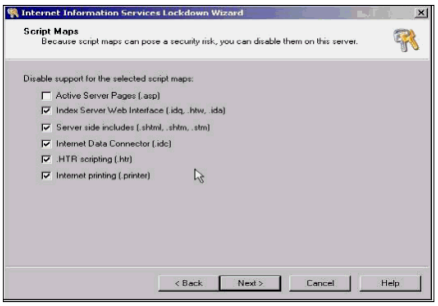


Figure 10. IIS Lockdown Setup.

Finally, make sure to de-select the "Writing to Content Directories" as this will break the Nfuse icons embedded in the page.

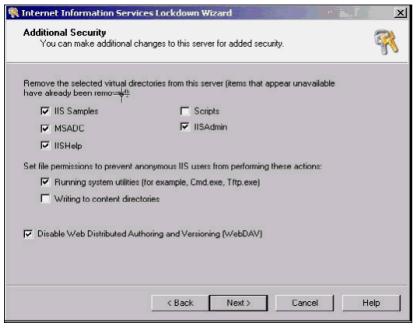


Figure 11. IIS Lockdown Setup.

It is important to note that in some instances IIS Lockdown will still create problems with what are called "NfuseIcons" (the application Icons that appear in the Nfuse web page). If you experience a problem with your Nfuse Icons on the page, modify the file and directory permissions manually on the NfuseIcons folder (CTX890678).

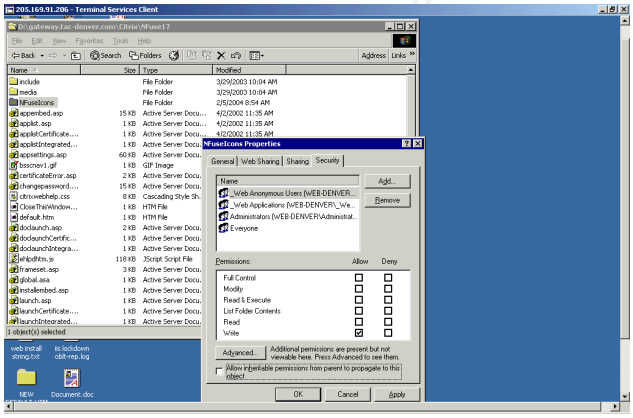


Figure 12. Windows 2000 File and Directory Security Dialog Box.

URLSCAN

UrlScan.ini is a web filter which screens incoming requests to the IIS server. It is an option that's installed with IIS Lockdown. You filter certain URL request by modifying the content of the URLSCAN.INI file. Installing URLSCAN will not

© SANS Institute 2000 - 2005 Author retains full rights.

negatively impact Nfuse 1.7, unless you are implementing the "Automated Citrix Client Install" feature of Nfuse 1.7. If you are using the automated install feature, you need to remark out the reference to .exe under the "Deny Executables that could run on the server" section (CTX101778).

; Deny executables that could run on the server
;.exe
.bat
.cmd
.com

At this point, re-test the functionality of Nfuse to assure proper functionality.

NfuseAdmin/Nfuse.Conf

Many configuration options are available by modifying the NFUSE.CONF file. This can be done either by using the NfuseAdmin web site (web pages that come installed with Nfuse), or you can modify the NFUSE.CONF file directly. After making changes to Nfuse.conf, you will need to restart IIS for thIS setting to take effect. From the Nfuse 1.7 Administrators guide (P. 93), here are some elements of the NFUSE.CONF that relate to security:

> **AllowUserPassword Change** never Specifies whether users are permitted to change their logon passwords
> within an NFuse Classic session. The options are:
> never users cannot change their logon password within NFuse Classic
> always users can change their password as often as they want in NFuse Classic. When you enable this option, the change password icon appears on the user™s screen. When users click on this icon, the change password dialog box appears, where users can enter a new password.
> **expired-only** users can change their password only when the password expires. When a user fails to log on to NFuse Classic due to an expired password, the user is automatically redirected to the change password dialog. After changing the password, the user is automatically logged on to NFuse Classic using the new password.
>
> **AuthenticationMethods** Explicit Specifies the ways in which users can authenticate to NFuse Classic.
> Authentication to NFuse Classic occurs when a user initially logs on to NFuse Classic, either using the Login dialog or by another authentication method.The options are:
> **Explicit** Users must have a user account and must supply a username and password to log on to NFuse Classic.
> **Guest** Enables guest users to log on to NFuse Classic using the Guest User option displayed in the user Login page. Guest users do not have to supply a username or password, and can access applications that the MetaFrame administrator has published for anonymous use.
> **Integrated** Enables Desktop Credential Pass-Through. This allows users to authenticate to NFuse Classic using the credentials they provided when

© SANS Institute 2000 - 2005 Author retains full rights.

they logged on to their Windows desktop. Users do not need to enter credentials at the NFuse Classic Login page and their NFuse Classic application set is automatically displayed. For this feature to work, NFuse Classic must be running on IIS and users must be running Internet Explorer Version 5.0 or later, on Windows 2000 or later.
Certificate Allows users to authenticate to NFuse Classic by inserting a smart card in a smart-card reader attached to the client device. Smart cards eliminate the need for users to remember multiple sign on processes, user ids, and passwords. This feature is available only on Windows/IIS and users must be running Internet Explorer Version 5.0 or later on Windows 2000 or later.
To specify more than one authentication method, use commas to separate the list for example: **Explicit,Guest**
ForceLoginDomain none When using Microsoft domain-based authentication, you can force all users
to log on to a specific domain by specifying the domain as the value. By default, this parameter is commented out by a pound symbol or hash mark (#) at the beginning of the line. When commented out, users must type the name of the domain in the NFuse Classic Login page. When a value is specified, the domain is not displayed to users on the NFuse Classic Login page.
When using ADS authentication, you can force users to type their user principal name (UPN) in the user name box by removing the pound symbol (#) at the beginning of the line and defining this parameter with a blank value.

AlternateAddress off Specifies whether to replace the address of the specified MetaFrame server
with its alternate address in the .Ica files sent to client devices to launch ICA sessions. The options are:
on The external address of MetaFrame servers is included in .Ica files generated by NFuse Classic.
Off No alternate address translation is performed.
Mapped The address depends upon the mappings you set in **ClientAddressMap**.
The external address of MetaFrame servers is configured with the ALTADDR command. For more information, see the description for the ALTADDR command in Appendix A of the *MetaFrame XP Administrator™s Guide* or the ctxalt command in the *MetaFrame for UNIX Operating Systems Administrator™s Guide*.

Misc. Security elements impacting Nfuse and Citrix

Web Page Timeout

Another configuration change that can greatly improve the security of Nfuse is to implement web-page timeouts for the Nfuse site (Madden, 597). The concern here is that a user can login to Nfuse, receive a list of applications and then walk away from their desktop letting someone else initialize a published application. To rectify this, change the default timeout value from 20 minutes to something less. Go to Internet Service Manager | Right-click the website hosting

© SANS Institute 2000 - 2005 Author retains full rights.

Nfuse| Properties | Home Directory Tab | Configuration Button | App Options Tab | Session Timeout .

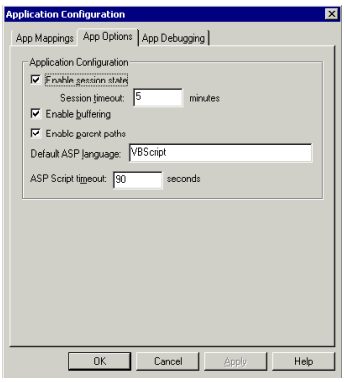


Figure 13. IIS 5.0 Internet Service Manager.

Passwords and Two-Factor Authentication

A strong password policy is imperative in securing an Nfuse/Citrix implementation. In a Windows 2000 Active Directory environment, this would normally be configured via a Group Policy. Turning on the "password complexity" feature of Windows 2000 would also be recommended.

Citrix Nfuse 1.7 also supports two-factor authentication (smart-cards, securID, etc) and is certainly a viable and recommended way to strengthen passwords.

Ticketing

When a user signs on to Nfuse and double-clicks one of the published applications, a small file called LAUNCH.ICA is copied to the users hard drive. This file is used to initialize a specified Citrix application. In earlier versions of Nfuse, the file contained all the necessary information for a user to start a Citrix session. A user could potentially copy the file and distribute it to other users. That user could then bypass Nfuse altogether and initialize Citrix sessions just by double-clicking the file. Citrix's response to this security issue is the "Ticketing" feature available in Nfuse. With Ticketing, the Nfuse server keeps the user ID and password on the server and associates a random 30-character "ticket" with the user ID. The "ticket" then goes into the LAUNCH.ICA file. This ticket is good for only one Citrix session and has a default expiration of 200 seconds. To confirm that Ticketing is enabled, you need to check two files on your Nfuse server (Madden, 648).

In the Nfuse.Conf file, look for the

SessionField.NFuse_TicketTimeToLive=200

and in the template.ica look for the following 2 parameters:

© SANS Institute 2000 - 2005 Author retains full rights.

AutoLogonAllowed=On

[NFuse_ticket]

SSL

Another frequently suggested way to improve login security with Nfuse is to implement SSL encryption on your Nfuse sign on page. By default, the user ID and password are transmitted in clear text. SSL encryption would severely limit the ability of someone to capture the userid and password from the Nfuse sign on page. SSL encryption will require the purchase of an x.509 certificate, but it does increase the security of Nfuse (Madden, 616).

SSL Relay

Another communication channel that can be secured via SSL is the Nfuse-to-XML data transfer. When a user enters their user ID and password on the Nfuse sign on page those credentials are passed in clear text to the Citrix server/s running the XML service. While this can enhance the security of this data channel, it is usually not necessary as this data is transmitted between private, secured lines. But if for some reason, this data is being transmitted across unsecured networks, this option becomes more useful (Madden, 631).

Secure ICA

SecureICA (or SecureICA extensions) is Citrix's proprietary method for encrypting Citrix ICA session traffic. It is built into Citrix Metaframe XP and all Citrix clients above version 6.01. SecureICA uses RSA RC5 encryption and supports 40-bit, 56-bit, and 128-bit encryption; there is also support for 128-bit encryption for only logon. SecureICA encryption can be applied at the connection-level, the application level or initiated from the Citrix client itself (Madden, 621).

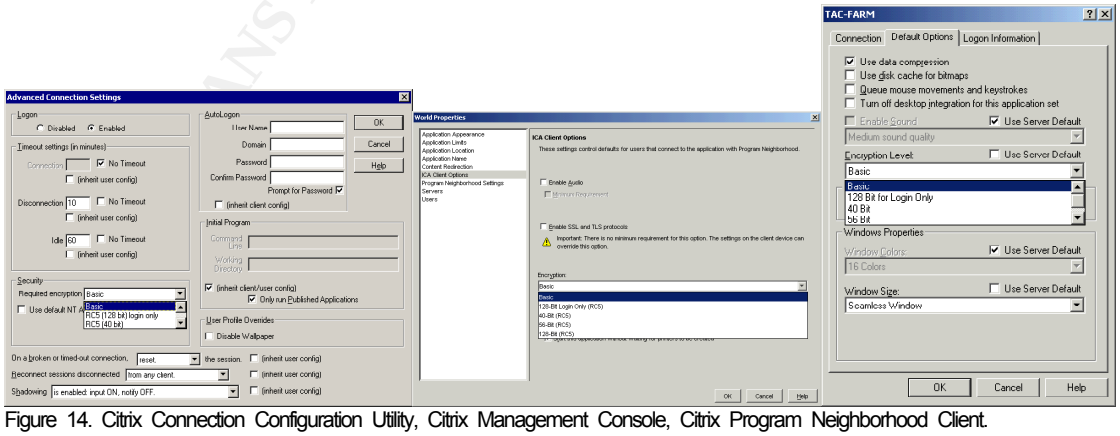


Figure 14. Citrix Connection Configuration Utility, Citrix Management Console, Citrix Program Neighborhood Client.

SecureICA when used in conjunction with Nfuse, is seamless and requires no

© SANS Institute 2000 - 2005 Author retains full rights.

user configuration. Overhead with SecureICA is minimal, with a small amount of increased processor load on the server and client. One interesting encryption option is the "128-login" only, which encrypts only the login information. Since Citrix session traffic data is primarily "keyboard-video-mouse" information, there may be value in just encrypting the logon credentials.

VPN

Another approach for encrypting Citrix ICA traffic would be to run your Citrix session through a VPN tunnel. This has the advantages of being very secure and an industry standard. Often, a VPN has already been implemented on the network. Since connecting via VPN is similar to being on the local network, you would probably want to move your Nfuse server behind the firewall and make it available to internal users; or remove Nfuse altogether. The disadvantages of this approach are that it will require VPN software configured on every device that will connect in this manner, making it somewhat inflexible. VPN also opens up your entire network to VPN users, which may not acceptable if your Citrix users are not employees or regular LAN users (as in an ASP), or when customers access specific applications via Citrix. Nfuse in a dmz environment allows you to easily deliver applications without opening up your entire network. Another approach would be to use Nfuse for external users and VPN for internal remote users (Madden, 619).

Securing Citrix at the Connection level

Citrix provides a powerful tool for securing communications with Metaframe servers; it is called the "Citrix Connection Configuration" utility.

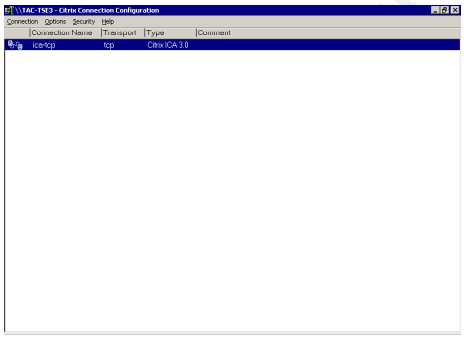


Figure 15. Citrix Connection Configuration Utility.

While this utility seems relatively simple, this application controls how communications occur with a Citrix server and has some configuration options that can greatly improve security. It is important to note that any configuration changes made using this utility will have preference over any conflicting changes made somewhere else on the server (Madden, 609).

Some suggestions for securing Citrix Connections

© SANS Institute 2000 - 2005 Author retains full rights.

Delete or Disable RDP connections. RDP is the communication protocol used in Microsoft Terminal Services, and as such, isn't used in a Citrix environment (which uses the ICA protocol). Having multiple "active" connections means you have manage and secure two thin-client protocols instead of one.

Don't "inherit user config" don't "inherit client config" . If you right-click on the "ica-tcp" connection within the Citrix Connection Configuration utility, select "Edit" and then select "Advanced" button, you'll see the following screen

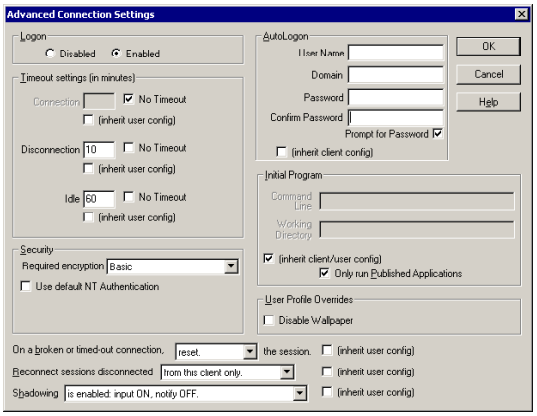


Figure 16. Citrix Connection Config Utility, Advanced Settings.

By default, the majority of these options are set to either "inherit user config" or "inherit client config" which basically means "let the user decide". If you do nothing else in this utility, change these to something other than "inherit user config". A few recommended changes in this utility include:

Idle Timeout: Setting an idle timeout means that a user will be logged off an idle Citrix session when the Idle Timeout setting has lapsed. This has the benefit of closing Citrix sessions when a user forgets to signoff.

Only run Published Applications: Enabling this option will force users to only run published applications and not initialize "Full Desktop" sessions. This option brings up an often-overlooked security issue with Citrix, whereby users, by default, have the ability to setup full-desktop Citrix sessions on their own.

Required Encryption: This will set the encryption level for all Citrix ICA communication on this server.

Securing Citrix Clients

A common theme when securing systems is to limit the ability of the user to change something that may impact security. With Citrix, one area where users can have more control than they should; is with the Citrix Client and Citrix Connections (Madden, 644).

Without going into to much detail regarding all the different Citrix clients, it is

© SANS Institute 2000 - 2005 Author retains full rights.

generally agreed that the Citrix PN Agent and Citrix Web Client allow users to change very little and as such provides better security than the Full Program Neighborhood Client, which is a very flexible Citrix client, and by default gives users a number of configurable options.

However, the Full Program Neighborhood Client may be required in some cases, especially when users connect to Citrix via a number of communication mediums, especially dial-up via RAS. There is a "grey" version of the full PN client, which has all the user configurable options "greyed" out and maybe a viable way to secure the full PN client for users that require it (Madden, 645).

Conclusion

In conclusion, when securing Nfuse 1.7 and Citrix Metaframe XP, stay focused on three key areas. First, install your Operating System and key software components in a secure manner. Second, use commonly available software tools and add-on components to enhance security. Third, configure Nfuse and Citrix Metaframe in a manner that enhances security.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

References

Madden, Brian S. Citrix Metaframe XP Advanced Technical Design Guide. Washington, D.C.: BrianMadden.com publishing Group, Jan 2002. (212,597,600,605,608,610,616-618,619-622,631-632,633-636 ,637,644-645,648-651)

Cole, Fossen, Northcutt, Pomeranz. SANS Security Essentials with CISSP CBK. The SANS Institute. Feb. 2003. (1326)

Citrix Systems Inc. CTX101778- Runing IIS Lockdown on an IIS server running Nfuse or Web Interface. CTX101778. Sept. 8, 2003. Url:
http://support.citrix.com/kb/entry!default.jspa?categoryID=135&entryID=2469&fromSearchPage=true

Citrix Systems Inc. CTX103197- Web Interface and multiple sites on same IIS server. CTX103197. Jan 12, 2004. Url:
http://support.citrix.com/kb/entry!default.jspa?categoryID=242&entryID=3670&fromSearchPage=true

Citrix Systems Inc. CTX102523- Current known issues with Windows 2000 Server with Service Pack 4. CTX102523. Oct. 29, 2003. Url:
http://support.citrix.com/kb/entry!default.jspa?categoryID=118&entryID=3038&fromSearchPage=true

Citrix Systems Inc. CTX184502- Using Firewalls With MetaFrame. CTX184502. Apr. 23, 2003. Url:
http://support.citrix.com/kb/entry!default.jspa?categoryID=118&entryID=2075&fromSearchPage=true

Microsoft Inc. Windows 2000 Server Datasheet. Sept. 25, 2001. Url:
http://www.microsoft.com/windows2000/server/evaluation/business/overview/datasheet.asp

Brown, Douglas Email interview. Jan. 29,2003.

Citrix Systems Inc. CTX890678-Application names appear but icons do not display on Nfuse web page . CTX890678. Apr. 23, 2003. Url:
http://support.citrix.com/kb/entry!default.jspa?categoryID=135&entryID=1839&fromSearchPage=true

Microsoft Inc. About URLScan.ini Url:
http://www.microsoft.com/resources/documentation/isa/2000/enterprise/proddocs/en-us/urlscan/vp_urlscanini.mspx

Citrix Systems Inc. Administrator's Guide: Citrix Nfuse Classic Version 1.7 (93,)Url:
http://support.citrix.com/kb/entry!default.jspa?categoryID=136&entryID=137&fromSearchPage=true

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.