Global Information Assurance Certification Paper

Citrix Secure Gateway: Improving Remote Access

Vincent R. Streiff
May 16, 2003
GSEC Practical Assignment Version 1.4b, Option #1

Abstract:

This paper is intended to serve as a concise explanation of how Citrix ICA clients communicate with Citrix MetaFrame XP servers, and how best to provide clients secure access over an untrusted network such as the Internet. I will review the major security concerns, and explain how to address them. While not exactly a step-by-step "Howto," it is my hope this paper will provide both the incentive and the foundation needed to successfully deploy Citrix Secure Gateway.

I will also discuss some of the major issues you may encounter while installing and configuring the Citrix NFuse Web server and the Citrix Secure Gateway (CSG) proxy. These products are both included free with Citrix MetaFrame, so no additional purchases are necessary other than the hardware to run them on, assuming you don't have any unused servers lying around available for use.

Why Citrix:

I won't spend too much time on this subject, as I assume if you're reading this you're already using Citrix MetaFrame and simply want to secure your remote access implementation. For those still wondering whether using Citrix for remote access is a good idea, however, I'll touch on the basic issues.

The answer is, of course, "It depends." One of the main advantages to using Citrix for remote access is the relative lack of training required; users don't need to know much more than how to use a browser, and they can access the same programs—even have the same desktop—as when they're sitting at their desk. Indeed, for this very reason many organizations simply train users to access Citrix MetaFrame via a Web browser using Java even when in the office, as everything is then identical whether users are in the office, at home, or at an Internet kiosk at the airport. (Note that entering username and password information at a totally untrusted kiosk is not necessarily a good idea, as there's no way of knowing what has been compromised or what is being monitored; it's entirely possible keystrokes are recorded. You have been warned.)

Another advantage is performance; because very little information is crossing the wire, applications that are otherwise impossible to use over a high-latency connection will work just as in the office. Legacy database applications are a good example. Another example is Microsoft Outlook, which is notorious for being painfully slow at synchronizing over slow links. Because with Citrix MetaFrame the applications are still running on the LAN, synchronization is no longer an issue.

This does point out, however, the primary drawback to using Citrix as a remote access solution: it only works when there's a connection. That may not sound like a problem, as making a connection is after all the whole point of remote access. However, consider the above Outlook scenario. It works wonderfully for the telecommuter sitting at home, but does not help the salespeople sitting on airplanes who need to work off-line. Citrix can transfer files to and from the local client PC, but it does not provide for synchronization or other more efficient means of off-line storage. If you need access to any significant amount of data offline, you'll probably still need a more traditional VPN solution. The two are not mutually exclusive, though; remote users may prefer to access programs via Citrix first to see if they can simply transfer a few select items rather than take the time to perform a full synchronization. A VPN implementation may make some of the work detailed in this paper unnecessary as well; since your VPN is presumably a secured connection, further encrypting the Citrix sessions may be unnecessary. However, using Citrix as outlined here does have the advantage of not requiring any special client software installed or configured.

In short, particularly if you already have Citrix MetaFrame deployed, there can be significant benefits to using Citrix as a remote access solution. If you're still debating whether or not to deploy Citrix at all, many of the same benefits to using it for remote access apply to internal use as well or even better. It provides for centralized administration, and you can use pretty much anything for clients, whether "thin" terminals, old Windows PC's, or even Linux or BSD clients booting off of a CD. Eliminating the "fat" PC clients can significantly improve your security; there's no longer a hard drive for attackers to compromise or to install programs onto. You do still have to address security issues for the Citrix servers themselves, of course, and any remaining "fat" clients—including users at home—still need just as much securing with Citrix as they do without it.

Citrix MetaFrame runs on top of, and extends, Windows Terminal Services. This means you need to harden the underlying Windows operating system as best as possible, and lock down the user permissions to ensure enforcement of a policy of least required access. This gets rather tricky, as users need the "Log on locally" permission on the server to use Citrix MetaFrame, and these servers frequently have a wide variety of software installed on them. John B. "Bill" Evrigenis, Jr. has written a good summary of what's required to secure the Windows Terminal Services side.[1] For a thorough explanation of all the steps needed in securing your Citrix environment, see Madden, Chapter 15.

[1] Evrigenis, John B. "Bill" Jr., "Secure Remote Server Administration of the Windows Server Family using Windows Terminal Services," Jan. 12, 2003, http://www.giac.org/practical/GSEC/Bill_Evrigenis_GSEC.pdf (May 8, 2003).

NFuse: The more "traditional" Remote Access model for Citrix

The first assumption this paper makes is that Citrix MetaFrame XP[2] is already up and running; worrying about remote access before local access functions properly is pointless. Installing and configuring Citrix MetaFrame is well beyond the scope of this paper, however, so if you're still at that stage I suggest either starting with a few training courses or hiring someone already qualified.

As I write this, Citrix MetaFrame XP is at Feature Release 2, NFuse Classic is at version 1.7, and Citrix Secure Gateway is at version 1.1. I will therefore use these versions in this paper, even though they may change with Feature Release 3 (which will have been released by the time you read this paper) as I do not yet have experience with FR3, and the fundamentals are not changing significantly in any event[3].

The standard model for providing remote access to Citrix MetaFrame application servers is to install and configure a Citrix NFuse Web server in an isolated service network, sometimes referred to as a De-Militarized Zone (DMZ).[4] This method is diagramed below, in *Figure 1*.

[2] Citrix MetaFrame XP comes in three separate "flavors," XP_s, XP_a, and XP_e. The techniques described here will work with all three. References to NFuse indicate NFuse Classic, unless otherwise noted.

[3] The names of the products will be changing, though. NFuse will now simply be called the web interface, and Citrix Secure Gateway will simply be called secure gateway. See Citrix Systems, Inc., "Packaging, Pricing & Availability," http://www.citrix.com/site/PS/products/QA.asp?familyID=19&productID=186&faqID=3876&featureID=QAP.

[4] There are differing opinions on just what and where a DMZ really is; some consider it to be the network between the border router and firewall, others consider it either a separate network off of the firewall or a network between two firewalls. It could also be referred to as a perimeter network. (See Zwicky, pp. 103, 129.) In any case, to avoid confusion I will simply refer to our isolated subnet as a service network, since it's a network dedicated to providing services. As shown in the diagrams, it is behind the primary firewall, on a dedicated subnet.

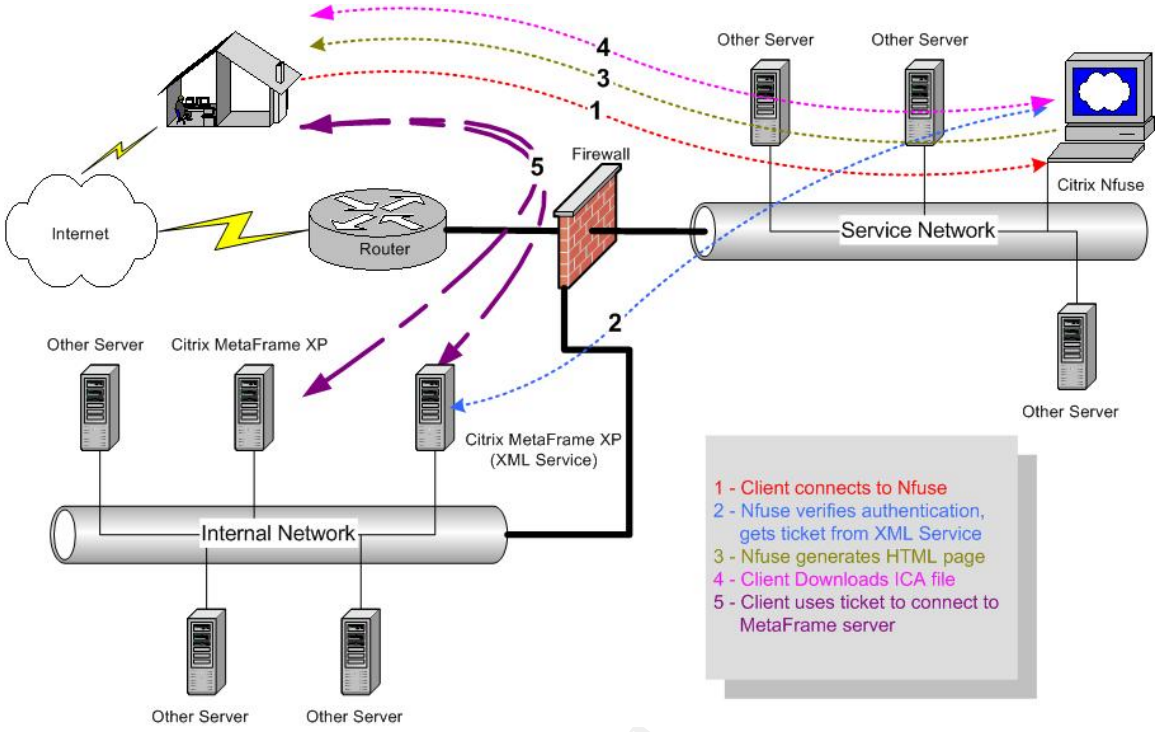

Figure 1

Let's take a step-by-step look at the actual processes going on here. First, the client connects to the Citrix NFuse Web server (Step 1 in *Figure 1*); this is generally done via TCP port 80 or, if SSL/TLS is used, TCP port 443.[5] Since for some strange reason we'd prefer not to send our usernames and passwords across the Internet in plain text, we'll use SSL and port 443 in this paper. Note that Citrix can also use TLS, but we'll stick with SSL for the moment because some of our users are using older PC's and we aren't positive their browsers are all modern enough to use TLS. Does that weaken our security? Not really, since for our purposes the differences between SSL and TLS aren't significant[6]; our efforts can probably be better spent doing something else that makes more of a difference. Also note that the encryption level we use here only needs to be strong enough to take longer to crack than the session itself lasts; using 3DES would probably be overkill here, and would only add unnecessary overhead to the connection. This may change as hardware continues to improve, however; once DES only takes a few hours to crack, it will no longer be sufficient for us.

Once the user has entered his or her login credentials, the NFuse server communicates with the Citrix MetaFrame Data Store server via the XML Service

[5] This paper assumes familiarity with TCP/IP. For a better understanding of how TCP/IP works, readers are encouraged to see Stevens, *TCP/IP Illustrated, Volume 1*.

[6] For information on TLS, see TLS Working Group, "Transport Layer Security (tls)," January 14, 2003, http://www.ietf.org/html.charters/tls-charter.html (May 5, 2003), and for the SSLv3 specifications see TLS Working Group, "The SSL Protocol Version 3.0," November 18, 1996, http://wp.netscape.com/eng/ssl3/draft302.txt (May 5, 2003).

(Step 2). The XML Service can be configured to use any port, but uses 80 by default. Because this is authentication traffic, and because it's still traversing a service network—which must be assumed will be compromised—this communication is often secured by using the Citrix SSL Relay, which acts as a proxy and secures the traffic over the wire via SSL or TLS, and is normally configured to use port 443.

The third step is for the Data Store server, via the XML Service, to reply to the NFuse Web server with the list of applications available to the user that has logged on. The NFuse server then dynamically generates an HTML page for the client with links to those applications (Step 3 in *Figure 1*).

When the user clicks on one of the application links, the Web browser downloads the associated ICA file (Step 4). This communication, too, will be done via TCP port 443, as we want to prevent eavesdroppers from being able to hijack our session now that we've logged in (more on this later). This ICA file is passed on to the local ICA Client software.

The ICA files are simply plain-text files, as shown in the example below for launching MS Outlook:

```
[Encoding]
InputEncoding=ISO8859_1

[WFClient]
Version=2
ClientName=-v-streiff-jxknd

RemoveICAFile=yes

[ApplicationServers]
MS Outlook=

[MS Outlook]
Address=10.20.13.219:1494
InitialProgram=#MS Outlook
LongCommandLine=""
DesiredColor=2
TransportDriver=TCP/IP
WinStationDriver=ICA 3.0

AutologonAllowed=ON
Username=v-streiff@example.com
Domain=\C1CF3BD2658ECAE7
ClearPassword=5ECBF8DABD7F43

DesiredHRES=800
DesiredVRES=600
TWIMode=On

SessionsharingKey=2-basic-none—v-streiff@example.com-CitrixFarm
```

```
[EncRC5-0]
DriverNameWin16=pdc0w.dll
DriverNameWin32=pdc0n.dll

[EncRC5-40]
DriverNameWin16=pdc40w.dll
DriverNameWin32=pdc40n.dll

[EncRC5-56]
DriverNameWin16=pdc56w.dll
DriverNameWin32=pdc56n.dll

[EncRC5-128]
DriverNameWin16=pdc128w.dll
DriverNameWin32=pdc128n.dll

[Compress]
DriverNameWin16=pdcompw.dll
DriverNameWin32=pdcompn.dll
```

Readers familiar with Windows .INI files should feel right at home here, as that's essentially what it is. A lot can be done to modify the properties of the session by editing the associated ICA file; for example, we could change the size of the window we see by altering the `DesiredHRES` and `DesiredVRES` settings. For a more detailed explanation of ICA files, see the nice analysis of them on Douglas A. Brown's site.[7]

Finally, the ICA Client uses the information contained in the ICA file to connect to the Citrix MetaFrame server to launch the application (Step 5). This is done via TCP port 1494, directly to the Citrix MetaFrame server.

This remote access method works quite well, and can be fairly secure by utilizing the encryption capabilities included natively within Citrix MetaFrame XP now that RSA encryption is included at no additional charge[8]. However, this "traditional" method does have a couple of weaknesses. If the ICA file is not transmitted in a secure fashion, there is a risk of "hijacking" an ICA session. Also, and perhaps more importantly, this scenario requires opening TCP port 1494 on the firewall for traffic inbound from the Internet directly to the Citrix MetaFrame servers.

The first weakness mentioned, the possibility of an attacker intercepting an ICA file and launching an application as the user, could best be described as "hijacking" an ICA session. It is actually quite easy to mimic in a controlled environment. If you want to have a little fun, log onto two different computers on a shared network; they'll both need the ICA client installed.[9] Just to show this

[7] Brown, Douglas A., "ICA File Explained," http://www.dabcc.com/NFuse/Docs/ica_file_explained.htm (May 8, 2003).
[8] See RSA Security Inc., "RSA Security and Citrix Systems Provide Stronger Security for the Virtual Workplace," April 10, 2002, http://www.rsasecurity.com/company/news/releases/pr.asp?doc_id=1264.
[9] There are ICA clients available for most popular operating systems today, though not all have the same features. See Citrix Systems, Inc., "Clients Downloads,"

could work in the real world, be sure to log on using two different user accounts. Then, log into your NFuse server; instead of just opening an application, right-click on the link and choose "save to file" or whatever the equivalent choice is with your browser. Save the file to a location accessible to both computers and users. Next, switch to the other computer and simply open up the saved ICA file with the ICA Client; on Windows computers, all you have to do is double-click. The application will launch without hesitation, running in the context of the user who logged on at the other machine.

In the real world, an attack of this sort is certainly more complex; the attacker would not only have to intercept and recognize the traffic for the ICA file after the link was clicked, but also launch the file before the ticket expires (200 seconds, by default). Neither of these is a trivial task—but if the ICA file is sent in clear text, they are not impossible either. It is therefore important to encrypt *all* of the traffic between the NFuse Web server and the client, not just the initial logon credentials. Implementing this attack has been made even more difficult with more recent versions of NFuse, including 1.7, now that by default tickets are sent to the client instead of the actual user logon credentials. These tickets are one-time use only. You can change how long the ticket is valid by editing the NFuse.conf file; edit the following line to indicate the number of seconds the tickets should be valid: `SessionField.NFuse_TicketTimeToLive=200`.

The more serious security concern with this scenario, however, is the exposure of the Citrix MetaFrame servers to direct access from the Internet. This opening in the firewall is not trivial, because the Citrix MetaFrame servers are usually, out of necessity, located on the internal LAN. Note also that that's "servers," plural; direct access must be granted to each and every Citrix MetaFrame server housing applications. This can also be troublesome for organizations using NAT with a small number of available public addresses, as a separate public address is required for each internal Citrix MetaFrame server.

Opening ports to the internal network is naturally a concern; any vulnerability in the Citrix MetaFrame ICA server would be unprotected. In addition, anyone scanning the network from the Internet will see TCP port 1494 open and know instantly that you're running Citrix MetaFrame. Are you completely confident that there are no buffer overflows in the programming exposed and listening on port 1494? Are you positive malformed ICA traffic can't and won't adversely affect your Citrix MetaFrame server farm? Me neither.

Citrix Secure Gateway: The new model

Citrix Secure Gateway addresses these concerns. It is essentially a proxy for the ICA protocol; instead of communicating directly with the back-end Citrix MetaFrame servers, remote clients communicate with the CSG. The CSG then

---

http://www.citrix.com/site/SS/downloads/downloads.asp?dID=2755 (May 16, 2003) for details and to download the client software.

gets the information from the Citrix MetaFrame servers, and passes it along to the clients. In this way, the back-end MetaFrame servers are not directly exposed to the Internet, and invalid or malformed traffic should be caught and stopped rather than being passed on to those servers. In addition, because only port 443 is opened on the Internet-facing interface of the firewall, there is no obvious indication to automated scanners that Citrix is in use.

This new configuration can be seen below in *Figure 2*.

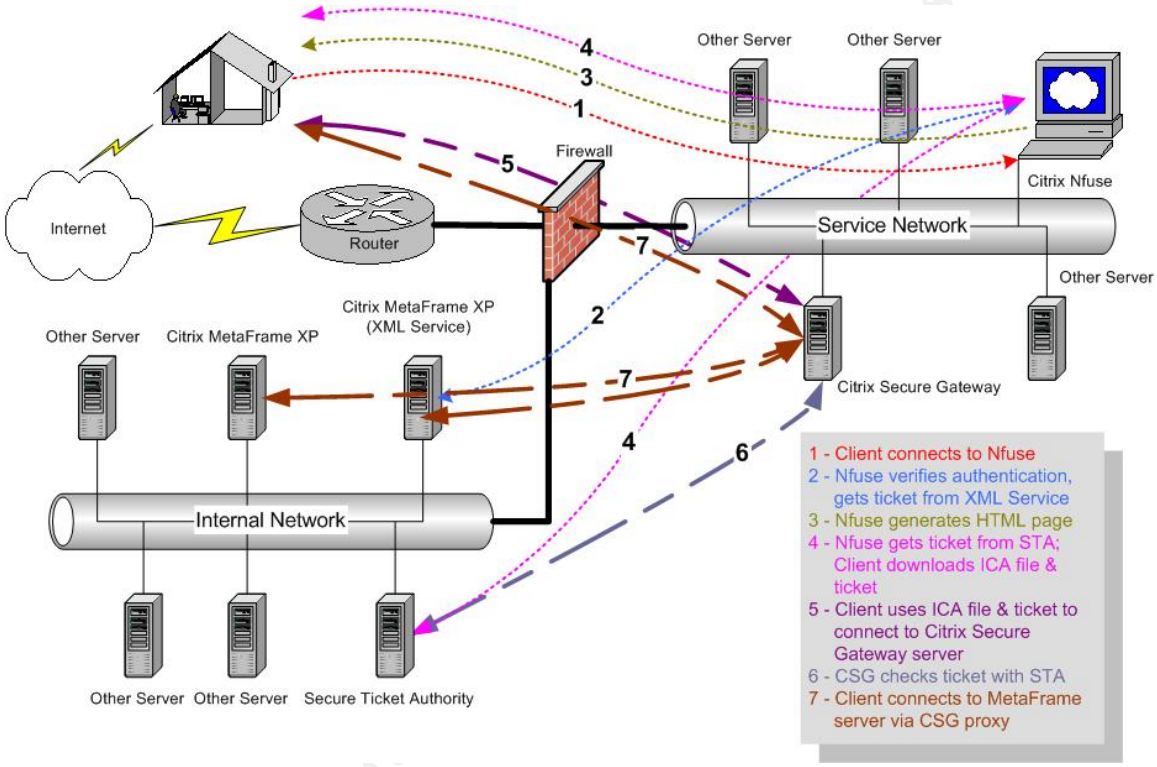

Figure 2

The first several steps are essentially the same in this scenario as they are without the Citrix Secure Gateway. The remote client connects to the NFuse server and enters the appropriate credentials (Step 1 in *Figure 2*); the NFuse server then forwards those credentials on to the Citrix XML Service (Step 2), and gets back a list of available applications. The NFuse server generates a custom HTML page for the client with links to ICA files for those applications (Step 3), and the client launches the applications by clicking on the links to download the appropriate ICA files and hand them over to the ICA client software (Step 4).

There is a little bit more going on behind the scenes here, however. In particular, when the client clicks on the link to an application, the NFuse server sends the IP address of the Citrix MetaFrame server the client should use to the Secure Ticket Authority (STA) as part of a request for a ticket for the client (Step 4). The STA issues the ticket to NFuse, and records the IP address of the Citrix MetaFrame

server for later reference. The ICA file generated by NFuse for the client then contains the ticket from the STA. Instead of containing the IP address of the Citrix MetaFrame server as in the "traditional" method shown in *Figure 1*, however, the ICA file this time simply contains the fully qualified domain name (FQDN) of the Citrix Secure Gateway.

The client then connects to the CSG using SSL or TLS, over TCP port 443 (Step 5). The CSG checks the ticket from the ICA client, and validates it with the STA (Step 6). This communication, like the other XML Service communications in this scenario, uses TCP port 80 by default. If the ticket is not OK, then the CSG sends an error message back to the client. If the ticket is successfully validated, the STA informs the CSG of the IP address of the appropriate Citrix MetaFrame server (established in Step 4).

The CSG then establishes a connection to the MetaFrame server, and acts as a proxy for the ICA client (Step 7).

Note that it is possible to use CSG without the STA; the CSG server simply acts as a proxy for the MetaFrame servers, accepting incoming authentication and ICA connections. Citrix refers to this as "Relay Mode," and while it avoids the need for the STA or even NFuse, it is less secure. I therefore won't cover configuring Citrix Secure Gateway to use Relay Mode.

Configuration Basics: What you need to do this

As mentioned before, the first thing you need is a functioning Citrix MetaFrame XP server farm. That's enough on that…

Next, we will configure the Citrix NFuse server. Obviously, this NFuse server needs to be very well hardened and secured. NFuse can run on either IIS or Apache, though NFuse is only supported on a limited number of operating systems:[10]

Microsoft OS's:
Windows NT 4 (doesn't support NFuse Classic Admin tool, and requires IIS 4)
Windows 2000 (IIS 5)

Unix (and Unix-like) OS's running Apache, Tomcat, iPlanet, or IBM WebSphere:
Solaris 7
Solaris 8
Redhat 6.2
Redhat 7.1

[10] Citrix Systems, Inc., "Administrator's Guide: Citrix NFuse Classic Version 1.7," September 2002, http://support.citrix.com/servlet/KbServlet/download/137-102-7739/NFuse_Guide.pdf , p. 27-28.

You may also be able to get it running on another operating system, such as OpenBSD with Linux emulation. Citrix doesn't support this, however, so if you do so, you're on your own.

This paper will focus primarily on running NFuse on IIS, though the fundamentals are the same regardless of Web server or operating system.[11] There are of course significant steps you need to take to adequately harden the machine, since it's exposed to the Internet. Securing IIS is certainly beyond the scope of this paper, but that doesn't mean you can ignore it. I do want to mention one rather common "gotcha," which is that the installation process for NFuse doesn't ask you where you want to install it; it just places the Web site files in the default Windows location on the boot drive (normally the C: drive.) You can not simply move them and change the pointers to the site in the IIS configuration, however. You also need to update the registry and the IIS Metabase; fortunately, Citrix is aware of the problem and has published a script to help you with the task. See Citrix Knowledge Base document CTX875451, "NFuse Classic 1.7 Error: Blank page at redirect.asp after moving web pages."[12] Personally, I think it would have been better and easier to simply ask us where to put it, but I digress.

Also note that NFuse is rather finicky about permissions needed for its various files; in particular, the `IUSR_<machinename>` account needs write access to the NFuseIcons folder, because NFuse generates HTML pages dynamically. Hardening simply by limiting everything to read-only access, or putting all of your Web site's files on a CD, will leave you with a server that can't show any icons for the application links. (The links will still work without the pretty graphics, of course, so this may be acceptable for you.) Also note that this server does not need to be a member of an Active Directory domain. Unless your organization's policies require doing so for Group Policy implementation and enforcement, it would probably be best to configure this as a stand-alone server. Security templates can and should still be implemented on the machine locally. Keeping the server out of your domain simply adds an additional layer, in conjunction with a good "defense in depth" strategy.

It's also a good idea to configure the SSL Relay on the MetaFrame servers so the authentication traffic between the NFuse server and the Citrix XML Service is encrypted. A sample configuration for a small network of 3 servers is shown below in *Figure 3*. The SSL Relay will work whether or not you're using CSG. Optionally, you could skip all of the extra application configuration and certificate

[11] For a nice step-by-step explanation of how to configure NFuse on Red Hat Linux 7.2, see Lutz, Joshua & O'Mahony, Brian, ESI Enterprises, Inc., "Procedure to Install and Configure NFuse on RedHat Linux 7.2 with Apache and/or Tomcat (Including Integration with Citrix Secure Gateway)," July 19, 2002, http://www.esient.com/WhitePaper-NFuse.pdf (May 8, 2003). It refers to NFuse 1.6, rather than the newer 1.7, but the steps should still work.

[12] Citrix Systems, Inc., "NFuse Classic 1.7 Error: Blank page at redirect.asp after moving web pages," April 23, 2003, http://support.citrix.com/kb/entry!default.jspa?categoryID=135&entryID=2232&fromSearchPage=true (May 5, 2003).

generation, which requires having digital certificates for each and every server, and just secure these back-end communications via IPSec.

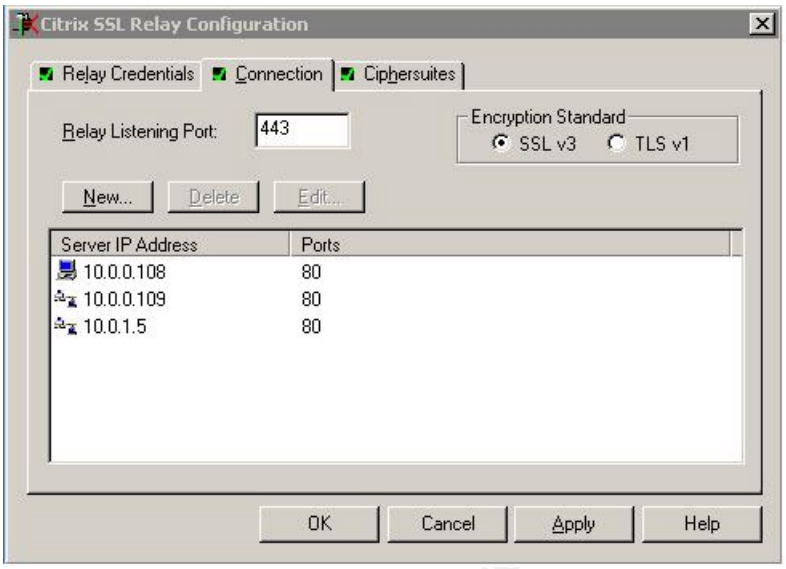

Figure 3[13]

The NFuse Web site can, of course, be customized with corporate graphics, legal disclaimers, etc. The functionality of the site, however, is primarily controlled through the NFuse.conf file. This can either be modified directly, or via the Administrative Web site, accessible at https://<YourServer'sURL>/NFuseAdmin shown in *Figure 4* below. Particularly for NFuse "newbies," the admin site can make initial setup a much less painful experience. Be sure to severely restrict access to this site; you don't want the entire world able to modify your configuration! As with any remote access configuration, be careful making administrative changes remotely; this is a good way to shoot yourself in the foot, so to speak, and you may find yourself climbing into your car instead of your bed.

[13] Snapshot taken from the Citrix SSL Relay Configuration screens.

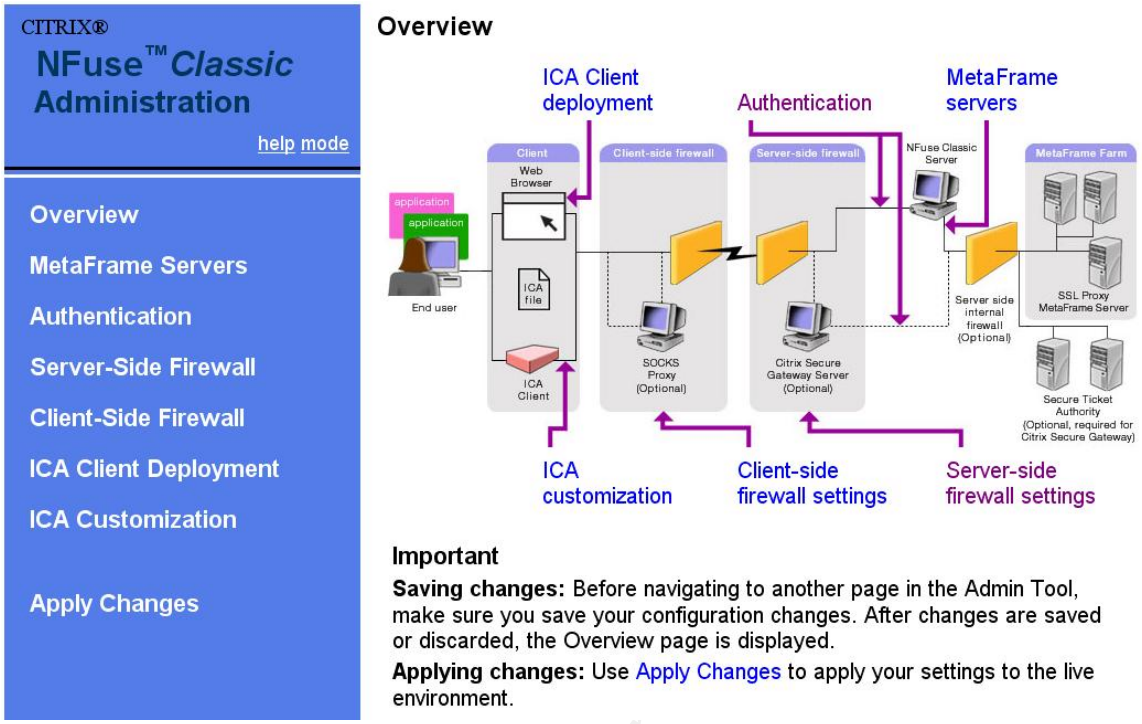

Figure 4[14]

Don't forget to acquire and install a certificate from a trusted Certificate Authority to enable the use of SSL to secure the communications with the NFuse Web server. Note that this does not necessarily need to be a certificate from a big, public firm; a certificate from a private CA can often work fine here, as long as you can properly train your users to configure their machines to trust certificates from your private CA—or else configure the machines for them.

For a nice checklist for hardening the NFuse server, see Knight, "Best Practices for Securing a Citrix Secure Gateway Deployment."[15]

One more aspect of NFuse configuration we should touch on is Network Address Translation. If you're using NAT of any sort for your connection with the Internet, with the "traditional" method you need to tell both NFuse and the MetaFrame servers. The easiest way to do this on the MetaFrame servers is to simply open a command prompt and type `ALTADDR /SET <PUBLIC-IP-ADDRESS>`. Naturally, since this is a Windows box, this won't take effect until you reboot. For NFuse, you can enter this information in the administrative site or, of course, edit the NFuse.conf file directly. The NFuse Administration Tool walks you through it quite nicely; you simply enter the private address for each MetaFrame server, the

[14] Screenshot taken from the Citrix NFuse Classic Admin Tool default page.
[15] Knight, Toby, Citrix Systems, Inc., "Best Practices for Securing a Citrix Secure Gateway Deployment," March, 2002, http://www.fgagne.org/Doc/csg/Best_Practices_Securing_a_Citrix_Secure_Gateway_Deployment.pdf (May 6, 2003).

corresponding public address, and click on the "Add" button to add it to the list of translation mappings. Note that you need a mapping for each and every MetaFrame server that clients may try to contact, or else they won't be able to reach it.

With Citrix Secure Gateway implemented, NFuse sends the client a ticket from the STA, and the FQDN of the CSG; the IP addresses for MetaFrame servers are hidden from the clients entirely. Assuming the CSG and STA are in a service network behind the NAT device, they will simply use the "real," private addresses of the MetaFrame servers. No alternate addresses are needed in this case. You do, however, need a "split brain" DNS configuration: the FQDN of the CSG must have a public DNS entry that resolves to a public IP address, and it must have a different private DNS entry for the private network that resolves to its private address.

Before we move on to configuring the CSG, however, we need to have a Secure Ticket Authority (STA) configured. This is fairly simple. In very small environments, this could be installed on a MetaFrame server, but again, the whole idea here is to maximize our security; the STA should be on a separate machine.

All that's needed for the STA is Windows 2000 with IIS installed. Naturally, everything should be hardened and have all of the latest service packs and hotfixes applied. Aside from that hardening, the installation of the Secure Ticket Authority is about as easy as software installation gets; you just need to know the location of your IIS server's scripts folder, and the installation copies a dll into that folder.[16] The STA configuration tool will then launch; all you really have to do is tell it what name to use for its ID, which needs to be 16 or fewer alpha-numeric characters. You can have multiple STA's to provide load balancing, but each STA needs a unique ID. You can have up to 256 STA's, "in case you want a really redundant environment."[17] Other options you can configure if you want are the timeout value for the tickets, which defaults to 100 seconds, and the maximum number of concurrent tickets, which defaults to 100,000. I'm guessing the majority of people reading this paper won't have that many sessions active at one time, so I recommend reducing that number.

Now we're ready to move on to the Citrix Secure Gateway. CSG can be installed on the same box as NFuse, but this is not recommended because of both the added workload and the reduced security. There are some extra configuration steps as well if you combine them, because IIS wants to bind to 443 on all adapters. If you really need to combine the two onto a single machine, though, you can.[18]

---

[16] Madden, p. 675.
[17] Madden, p. 678.
[18] See Citrix Systems Inc., "Running Citrix Secure Gateway and IIS/NFuse on the same server," Document ID CTX799332, April 23, 2003, http://support.citrix.com/kb/entry.jspa?entryID=1737 (May 5, 2003) and

For better security, however—which, after all, is the whole point of doing all of this work—the CSG should be on a dedicated machine. Aside from the fringe benefits of easier configuration and better performance, the real advantage to this is that the Citrix Secure Gateway does not need IIS or Apache installed to function properly. This makes hardening the CSG much, much easier. Again, hardening servers is beyond the scope of this document.

Citrix Secure Gateway can run on either Windows or Solaris; we'll cover the Windows installation here. As mentioned above, it does not require a Web server. It does, however, require a certificate from a trusted Certificate Authority. This, too, can naturally be from a private CA. Installation is fairly straightforward; Citrix even provides a simple checklist[19] for you to fill out before starting to make sure you have all of the details and prerequisites ready. Once you have answers to all of the items on this checklist, installation and configuration are very easy.

The majority of the default settings should be fine. Settings you should pay particular attention to relate to logging; you can exclude IP addresses if you want, but more importantly make sure your Windows Event Log is configured to handle all of the logging. Since we've made this a dedicated server, we can safely set the Event Log to a very large size without worrying about the hard drive space it will occupy. This is done by opening Event Viewer and editing the "Maximum log size" property; you should probably set these to something approaching 100 MB at least.

Now that all of the parts are in place, we can change the NFuse configuration to take advantage of our improved architecture. Again, the Web-based Administration Tool makes this very simple; on the Server-Side Firewall page, simply check the boxes telling NFuse to use CSG, enter the FQDN of the CSG and the TCP port to use, enter the URL to the CTXSTA.DLL on the STA Web server(s), and save and apply the changes. They will take effect as soon as you restart the Web server service. The only confusing aspect of all of this is whether or not you need to use alternate addressing; chances are you don't, but it's simple enough to change if it doesn't work when you test.

Traffic Summary:

In the hopes of making your life a little easier, here is a list of the default openings you'll need to make in your firewall to get Citrix to work with NFuse, Citrix Secure Gateway, and the Secure Ticket Authority. These ports are of course not set in stone; depending on how you've configured your servers, your

---

(cont.) Microsoft Knowledge Base Article 238131, "How to Disable Socket Pooling," April 22, 2003, http://support.microsoft.com/default.aspx?scid=kb;EN-US;q238131 (May 5, 2003).

[19] Citrix Systems, Inc., "Installation Checklist: Citrix Secure Gateway Version 1.1," April 19, 2002, http://support.citrix.com/servlet/KbServlet/download/147-102-7749/Citrix_Secure_Gateway_Checklist.pdf (May 6, 2003).

mileage may vary. If you've altered any ports, though, then you presumably know what you've done and can make the requisite adjustments.

Traffic inbound from the clients on the Internet to the service network:
TCP ports 80 and 443 to the NFuse server
TCP port 443 to the CSG server

Traffic from the NFuse server to the Citrix MetaFrame servers:
TCP port 80 or 443, depending on whether or not you're using the SSL Relay.

Traffic from the NFuse server to the STA:
TCP port 80 (can secure using IPSec if desired)

Traffic from the NFuse server to the CSG:
None!

Traffic from the STA to the Citrix MetaFrame servers:
None!

Traffic from the CSG to the Citrix MetaFrame servers:
TCP port 1494 (could be secured using RSA encryption, or use IPSec if you prefer.)

Traffic from the clients on the Internet to the Citrix MetaFrame servers:
None!

Note that if you use IPSec across the firewall, you'll have to configure it to pass that traffic as well, in both directions:[20]
ISAKMP / IKE: UDP port 500
ESP: IP Protocol 50
AH: IP Protocol 51 (if used)

Conclusion:

Citrix MetaFrame XP, when used in conjunction with Citrix NFuse, the Citrix Secure Gateway, and the Secure Ticket Authority, can provide an excellent, securely proxied remote access solution. What's more, because NFuse, the CSG, and the STA are all included with Citrix MetaFrame XP, the only costs involved for those who have already implemented Citrix MetaFrame XP are a little hardware and a little time. Hopefully, I've enabled you to reduce that time even further.

[20] See Microsoft Knowledge Base Article 233256, "How to Enable IPSec Traffic Through a Firewall," October 10, 2002 at http://support.microsoft.com/?kbid=233256 (May 2003).

Resources:

Brown, Douglas A., "DABCC.COM - Citrix Secure Gateway 1.1," August 20, 2002, http://www.dabcc.com/thinsol/csg/csghome.htm (April 23, 2003).

Brown, Douglas A., "ICA File Explained," http://www.dabcc.com/NFuse/Docs/ica_file_explained.htm (May 8, 2003).

Carpe Diem, "Citrix Secure Gateway," March 10, 2003, http://www.carpediem.de/products/citrix/csg.html (April 21, 2003) [Note: Site is in German].

Citrix Systems, Inc., "Administrator's Guide: Citrix NFuse Classic Version 1.7," September 2002, http://support.citrix.com/servlet/KbServlet/download/137-102-7739/NFuse_Guide.pdf (May 8, 2003).

Citrix Systems, Inc., "Citrix NFuse Technical Whitepaper," March 31, 2000, www.thethin.net/whitepapers/NFUSE15/NFuseWP.doc (April 23, 2003).

Citrix Systems, Inc., "Citrix Secure Gateway: Technical Presentation, February 2002," http://download2.citrix.com/ctxlibrary/Products/ppt/CSG_Techical_Presentation022002.ppt (May 5, 2003).

Citrix Systems, Inc., "Clients Downloads," http://www.citrix.com/site/SS/downloads/downloads.asp?dID=2755 (May 16, 2003).

Citrix Systems, Inc., "Installation Checklist: Citrix Secure Gateway Version 1.1," April 19, 2002, http://support.citrix.com/servlet/KbServlet/download/147-102-7749/Citrix_Secure_Gateway_Checklist.pdf (May 6, 2003).

Citrix Systems, Inc., "NFuse Classic 1.7 Error: Blank page at redirect.asp after moving web pages," April 23, 2003, http://support.citrix.com/kb/entry!default.jspa?categoryID=135&entryID=2232&fromSearchPage=true (May 5, 2003).

Citrix Systems, Inc., "Packaging, Pricing & Availability," http://www.citrix.com/site/PS/products/QA.asp?familyID=19&productID=186&faqID=3876&featureID=QAP (May 8, 2003).

Citrix Systems Inc., "Running Citrix Secure Gateway and IIS/NFuse on the same server," Document ID CTX799332, April 23, 2003, http://support.citrix.com/kb/entry.jspa?entryID=1737 (May 5, 2003).

Citrix Systems, Inc., “Technical Considerations for Secure Gateway,” http://www.citrix.com/site/PS/products/QA.asp?familyID=19&productID=186&faqID=3339&featureID=QAP (May 6, 2003).

Evrigenis, John B. “Bill” Jr., “Secure Remote Server Administration of the Windows Server Family using Windows Terminal Services,” Jan. 12, 2003, http://www.giac.org/practical/GSEC/Bill_Evrigenis_GSEC.pdf (May 8, 2003).

Harwood, Ted, “Providing Access to Citrix MetaFrame Through a Firewall,” May 1, 2002, http://www.informit.com/isapi/product_id~%7B4663909B-C195-4095-BBC5-0A81B12C47DC%7D/content/index.asp (April 23, 2003).

Knight, Toby, Citrix Systems, Inc., “Best Practices for Securing a Citrix Secure Gateway Deployment,” March, 2002, http://www.fgagne.org/Doc/csg/Best_Practices_Securing_a_Citrix_Secure_Gateway_Deployment.pdf (May 6, 2003).

Lutz, Joshua & O’Mahony, Brian, ESI Enterprises, Inc., “Procedure to Install and Configure NFuse on RedHat Linux 7.2 with Apache and/or Tomcat (Including Integration with Citrix Secure Gateway),” July 19, 2002, http://www.esient.com/WhitePaper-NFuse.pdf (May 8, 2003).

Madden, Brian S., *Citrix MetaFrame XP: Advanced Technical Design Guide, Including Feature Release 2,* Washington, D.C., BrianMadden.com Publishing, November 2002.

Microsoft Knowledge Base Article 233256, “How to Enable IPSec Traffic Through a Firewall,” October 10, 2002 at http://support.microsoft.com/?kbid=233256 (May 8, 2003).

Microsoft Knowledge Base Article 238131, “How to Disable Socket Pooling,” April 22, 2003, http://support.microsoft.com/default.aspx?scid=kb;EN-US;q238131 (May 5, 2003).

Montgomery, Phil, “Citrix Secure Gateway v1.1: Technical Presentation,” August 2002 Citrix Systems, Inc., http://www.dabcc.com/thinsol/csg/Docs/CSG%20Technical%20Presentation%20v1.1.ppt.

Ogle, Ron, “RE: Securing Citrix NFuse and IIS 5,” October 22, 2002 (posted to focus-ms@securityfocus.com), http://archives.neohapsis.com/archives/sf/ms/2002-q4/0032.html (May 8, 2003).

RSA Security Inc., “RSA Security and Citrix Systems Provide Stronger Security for the Virtual Workplace,” April 10, 2002, http://www.rsasecurity.com/company/news/releases/pr.asp?doc_id=1264 (May 6, 2003).

Stevens, W. Richard, *TCP/IP Illustrated, Volume 1: The Protocols,* New York, Addison Wesley, October 2000.

Thethin.net, “Frequently Asked Terminal Services Questions!” 2003, http://www.thethin.net/faqs.cfm?category=2&sortby=date (May 9, 2003).

TLS Working Group, “The SSL Protocol Version 3.0,” November 18, 1996, http://wp.netscape.com/eng/ssl3/draft302.txt (May 5, 2003).

TLS Working Group, “Transport Layer Security (tls),” January 14, 2003, http://www.ietf.org/html.charters/tls-charter.html (May 5, 2003).

TweakCitrix.com, http://www.tweakcitrix.com.

Vistorm Ltd., “Citrix Secure Gateway,” 2003, http://www.vistorm.com/content/sbc/products/citrix/secure_gateway.asp (April 21, 2003).

Warren, Steven, “Set up a Citrix NFuse portal in a load-balanced cluster,” May 1, 2003, http://www.techrepublic.com/article.jhtml?id=r00220030501wrr01.htm&fromtm=e102-2 (May 5, 2003) [Note: site requires free registration.]

Zwicky, Elizabeth D. et al, *Building Internet Firewalls,* Sebastopol, CA, O’Reilly & Associates, Inc., June 2000.