Introduction

Citrix Systems offers enhanced functionality for MS Windows Terminal Server (WTS). WTS provides the capabilities to run Windows applications from remote clients, independent of the client operating system. The Citrix product Metaframe extends this functionality to a wider range of clients and a larger set of features. For added functionality, customers may decide to use Nfuse, a Citrix product that installs on their local Web server. By utilizing Nfuse, customers can provide connectivity to applications through a centralized Web page to clients on the Intranet or Internet.

Allowing connectivity to internal applications from external clients poses obvious security risks. Properly securing the connections requires up-front planning to insure the integrity of the system. This paper will examine the basic functionality of the Nfuse system and some simple steps that can be taken to mitigate the associated risks.

System Overview

The base operating system of the application server is Windows NT or Windows 2000 with terminal services enabled. Enabling terminal services creates the multi-user environment, which permits simultaneous remote logins to the server. Concurrently logged in clients run applications in separate, protected sessions from a single application server.

Layered on top of the base operating system will be Citrix Metaframe. Metaframe incorporates the proprietary independent computing architecture (ICA) protocol. ICA is a remote presentation protocol that separates an application's logic from its user interface. This means only keystrokes, mouse clicks, and screen updates have to traverse the network.[1] ICA supports most standard network protocols including TCP/IP, PPP, IPX/SPX and NetBEUI as well as common network transport implementations such as asynchronous, dial-up, ISDN, frame relay, and ATM.

For customers operating Nfuse, clients connect to the Web server to receive a list of applications available to them. The communication between the clients and the Web server can be made through standard HyperText Transfer Protocol (HTTP) or HTTP encrypted with the Secure Sockets Layer (SSL).[2] Following are the required steps for authentication as outlined in figure 1.

1) The Client visits a login page and enters user credentials. Credentials can be transmitted either standard HTTP or securely with SSL. The Web browser sends an HTTP request containing the credentials to the Web server.
2) The Web server reads the user's information and uses the Nfuse Java objects to

[1] "Rapid Application Deployment White Paper", Citrix Systems. June 1999. http://www.citrix.com
[2] "Security Guidelines for Nfuse 1.0", Citrix Solutions Knowledgebase. http://knowledgebase.citrix.com

forward that information to the Citrix XML Service on a designated Citrix server in the server farm across HTTP port 80. This designated server acts as a broker between the Web server and the Citrix server farm.

3) 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. The Citrix XML Service then forwards the user's application set information to the Nfuse Java objects running on the Web server.
4) The Web server uses the Nfuse Java HTML 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 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 to display the application in. ICA files are written in .Ini file format and have an .Ica extension.

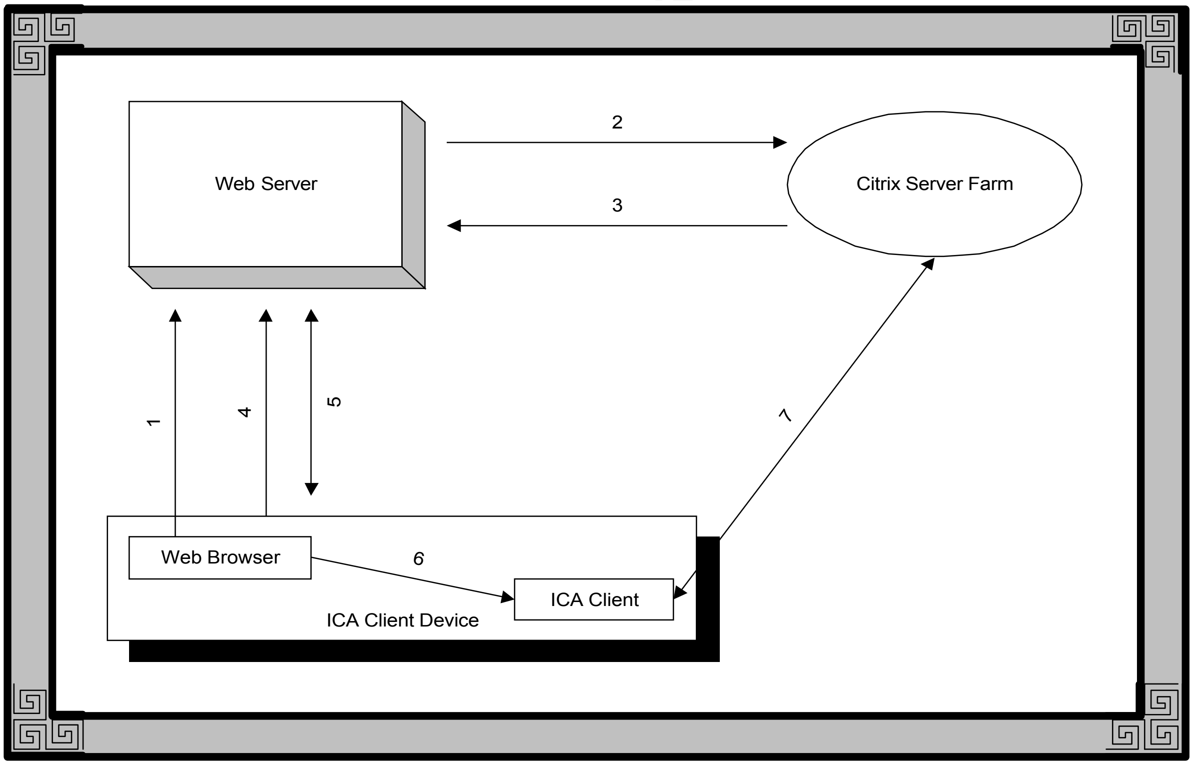

Figure 1 Web-Based Authentication Steps[3]

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 Java objects, which retrieve the template ICA file. The template file contains substitution tags. The Java objects replace the substitution tags in the template

[3] Citrix Systems, "Nfuse Administrators Guide", http://www.citrix.com/support. January 2001

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 Web browser receives the ICA file and passes it to the client device's ICA Client.
7) The ICA Client receives the ICA file and initiates an ICA session with a Citrix server according to the ICA file's connection information. All communications directly between the client and the server occur through TCP port 1494.

Securing Client - Server Communications

In securing a system for Citrix connectivity, the first thing to do is require SSL for all communications between the client and the Web server. Configuring this option resolves two security issues. The two issues are client authentication and client-side cookies.

Client authentication must be specified on the server to explicitly require clients to login before accessing any applications. Not configuring explicit logins allows anonymous users to run applications. On pages requiring explicit logins, the user credentials are transmitted across the network in plain text. Enabling SSL prevents the information from being passed in plain text.

The second issue is client-side cookies. Once authenticated, the client receives a cookie containing their logon credentials. Whenever the client issues a GET statement for the Nfuse server, the information in the cookie is retransmitted so the client does not have to re-authenticate with each request. The cookie is not stored on the user's hard drive and expires when the session is closed. Enabling SSL prevents the information in the cookie from being stored in plain text.

During an established client session, all communication occurs directly between the client and the application server without the need for further intervention on the part of the Web server. It is possible to increase security for the client – server communication by specifying an RC5 key length of up to 128 bits.[4]

Securing Server – Server Communications

The client authentication process requires the Nfuse Web server to forward the client credentials to the Metaframe server. These communications are handled with the XML protocol. The server-to-server communications are all clear text, however, the client passwords are encrypted using a Citrix proprietary algorithm. For increased security of server-to-server communications, it is recommended establishing a Virtual Private Network (VPN) to transport traffic between the servers.[5]

[4] "ICA Basic Encryption FAQ", Citrix Solutions Knowledge Base. http://knowledgebase.citrix.com
[5] "Security Guidelines for Nfuse 1.0", Citrix Solutions Knowledge Base. http://knowledgebase.citrix.com

Another area of vulnerability is the Web server itself. All variables posted from standard HTML forms, such as user credentials, are available on the server. This is true even if SSL is enabled. An insecure server, or an unscrupulous administrator, could allow the information to become insecure. Independent auditing of the server and maintenance of software patches is a must to protect user credentials.

Communications Through a Firewall

All communications to the Internet should be through a firewall. The firewall should be configured with Network Address Translation (NAT). Using NAT, all external communications are translated to an internal IP address. The external clients have no knowledge of the internal IP addresses. The firewall handles translation between the public and private IP addresses.

When clients connect to a redundant Metaframe server farm, the Citrix master browser returns the IP address of the available application server. When an external client attempts the same connectivity through a NAT enabled firewall, the client receives the internal address of the application server. When the client attempts to use that address, it is stopped at the firewall.

Correcting this problem is a two-step process.[6] The first step requires the use of a command line utility to set the external address on the Metaframe server. After the address has been set, the Metaframe server informs the Citrix master browser of the address. The master browser then returns the external address of the Metaframe server whenever external clients request services.

The second half of the process requires specifying the alternate address on the Nfuse Web server. To do this, simply modify the template file used to create the dynamic client connections. Once this is done the Web server will return connections specifying the correct address.

Conclusion

Nfuse offers a simplified method for administrators to provide a Web based front end for their Citrix-enabled clients. Careful planning on the administrator's part can help provide a secure environment in which to allow clients access to their applications.

The planning should include client to Web server communications, server-to-server communications, and external communications through a firewall. In addition to this, basic security auditing of the physical systems should be implemented in order to reduce

[6] Mathers, Todd W. "Windows NT/2000 Thin Client solutions." Macmillan Technical Publishing, 2000

the risk of penetration by undesired sources.

References

"Rapid Application Deployment White Paper", Citrix Systems. June 1999. http://www.citrix.com

"Security Guidelines for Nfuse 1.0", Citrix Solutions Knowledge Base. http://knowledgebase.citrix.com

"Nfuse Administrators Guide", Citrix Systems. http://www.citrix.com/support. January 2001

Mathers, Todd W. "Windows NT/2000 Thin Client solutions." Macmillan Technical Publishing, 2000

"ICA Basic Encryption FAQ", Citrix Solution Guide. Document ID # CTX155541, http://www.citrix.com