Best Practices for Securing a Citrix Secure Gateway Deployment

By Citrix Consulting Services

Citrix Systems, Inc.
Notice

The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

This publication contains information protected by copyright. Except for internal distribution, no part of this publication may be photocopied or reproduced in any form without prior written consent from Citrix.

The exclusive warranty for Citrix products, if any, is stated in the product documentation accompanying such products. Citrix does not warrant products other than its own.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Copyright © 2002 Citrix Systems, Inc., 851 West Cypress Creek Road, Ft. Lauderdale, Florida 33309-2009 U.S.A. All rights reserved.
# Table of Contents

**TABLE OF CONTENTS** .................................................................................................................. III

**INTRODUCTION** ................................................................................................................................. 1

- Document Overview .......................................................................................................................... 1
- What is the Citrix Secure Gateway? .................................................................................................. 1
- Benefits of a CSG Deployment ........................................................................................................ 1
- Further Enhancing Security in a CSG Environment ......................................................................... 2
- Pre-requisites ........................................................................................................................................ 2

**STANDARD IMPLEMENTATION OF THE CSG** ............................................................................... 3

- CSG Typical Network Interaction ................................................................................................... 3
- Order .................................................................................................................................................. 4
- Action ................................................................................................................................................. 4
- Event .................................................................................................................................................. 4
- Comments .......................................................................................................................................... 4

**Citrix Secure Gateway Components** ............................................................................................ 5

- Secure Gateway ............................................................................................................................... 5
- Citrix NFuse ....................................................................................................................................... 5
- Secure Ticketing Authority (STA) ..................................................................................................... 6

**Securing Citrix Secure Gateway – Best Practices** ......................................................................... 7

**BEST PRACTICES SUMMARY** ......................................................................................................... 7

**BEST PRACTICES DETAIL** ............................................................................................................... 9

- File System ....................................................................................................................................... 9
- Sample Code ...................................................................................................................................... 9
- Authentication .................................................................................................................................... 10
- User Accounts ................................................................................................................................. 11
- IIS Anonymous Access User Account ........................................................................................... 13
- Disable Unused Services ..................................................................................................................... 16
- Remove Windows Components ......................................................................................................... 18
- Hot Fixes and Service Packs ............................................................................................................. 21
- Remove Unused File Associations ..................................................................................................... 22
Introduction

Document Overview

All implementations of computing technology exposed to the Internet are subject to the potential threat of malicious use. This document has been written to provide best practices for securing the implementation of CSG. This document focuses on locking down the Microsoft 2000 Server and IIS 5.0 components.

This document outlines the following:

• Standard Implementation of Citrix Secure Gateway
• Securing Citrix Secure Gateway – Best Practices

This document assumes the reader has some knowledge of NFuse and the Citrix Secure Gateway, and briefly discusses them.

What is the Citrix Secure Gateway?

The Citrix Secure Gateway (CSG) functions as a secure Internet-ready gateway for Citrix Independent Computing Architecture (ICA) traffic between MetaFrame servers and Secure Sockets Layer (SSL)-enabled ICA client workstations. All data traversing the Internet, between the client workstation and the CSG server, is encrypted, ensuring privacy and integrity of information flow.

CSG provides a single point of entry and secures access to Citrix server farms. SSL technology is used for encryption, allowing secure transfer of data across public networks. CSG is also designed to make firewall traversal with MetaFrame solutions easier.

CSG is an enterprise-wide solution that protects a customer’s investment in Citrix MetaFrame infrastructure and business applications. It is completely transparent to both application programs and network devices, eliminating the need for any program modifications or equipment upgrades.

Benefits of a CSG Deployment

CSG removes the need to publish the addresses of every Citrix server, simplifies server certificate management, and allows a single point of encryption and access into the Citrix servers. It does this by providing a gateway that is separate from the MetaFrame servers and reduces the issues for firewall traversal to a widely accepted port for ICA traffic in and out of firewalls. The following benefits are achieved:

• Strong encryption (SSL V3 128-bit)
• Authentication (achieved through NFuse)
• Hidden internal network addresses for Citrix servers
• Firewall traversal through a widely accepted port
• Certificates are only required on the CSG gateway, and not on every MetaFrame server.
• Easy support for a large number of servers
• No requirement for separate client software (the standard ICA Win32 client is sufficient)
Further Enhancing Security in a CSG Environment

The CSG has three components: the Secure Ticket Authority (STA), NFuse and Secure Gateway. In some implementations, the last two components may be exposed to Internet users. Since the availability of a correctly configured firewall is often beyond the scope of a CCS engagement, all of the security considerations detailed in this document should be applied to the CSG infrastructure.

Although CSG can be used in conjunction with any NFuse v1.61 (or higher) supported platform, on NFuse v1.60 and v1.51 implementation of CSG requires the use of Microsoft Internet Information Server (IIS). The first release of this document will therefore provide security best practices for CSG implemented with Microsoft IIS 5.0 and installed on the Windows 2000 Server family.

Pre-requisites

Before proceeding with this document the reader should complete the following prerequisites.

- Read and understand the CSG Administrators Guide
- Download the latest version of the CSG software. Version 1.01 contains a number of security Hot Fixes for the STA component.
Standard Implementation of the CSG

This section outlines the basic configuration of a standard CSG implementation. The section also describes the components and the basic network traffic interaction of the different components.

CSG Typical Network Interaction

Figure 1 - CSG Typical Network Interaction

1. A remote user launches a Web browser and connects to an NFuse Web server on port 80 (HTTP) or port 443 (HTTPS). The NFuse Web portal requires the user to authenticate using valid user credentials.

2. NFuse uses the user credentials to contact the Citrix XML Service, on port 80, running on a MetaFrame server and obtains a list of applications that the user is authorized to access. NFuse populates the Web portal page with the list of published applications that the user is authorized to access. The communications so far are the normal sequence of events that occur when an NFuse Web server is deployed to provide ICA client users with access to published applications.

3. When the user clicks on a link for a published application, NFuse sends the IP address for the requested MetaFrame server to the STA and requests a Secure Gateway ticket for the user. The STA saves the IP address and issues the requested Secure Gateway ticket to NFuse.

4. NFuse generates an ICA file containing the ticket issued by the STA, and then sends it to the client browser. Note that the ICA file generated by NFuse contains only the IP address of the Secure Gateway server. The address of the MetaFrame server(s) that the ICA client eventually connects to is not exposed.

5. The browser passes the ICA file to the ICA client, which launches an SSL connection to the Secure Gateway server. Initial SSL handshaking is performed to establish the identity of the Secure Gateway server.
6. The Secure Gateway server accepts the ticket from the ICA client and uses information contained in the Secure Gateway ticket to identify and contact the STA for ticket validation. If the STA is able to validate the ticket, it returns the IP address of the MetaFrame server on which the requested application resides. If the ticket is invalid or has expired, the STA informs the Secure Gateway server, and an error message is displayed on the ICA client device.

7. On receipt of the IP address for the MetaFrame server, the Secure Gateway server establishes an ICA connection to the MetaFrame server. After the ICA connection is established, the Secure Gateway server monitors ICA data flowing through the connection, and encrypts and decrypts client-server communications.

The table below details a typical CSG connection sequence:

<table>
<thead>
<tr>
<th>Order</th>
<th>Action</th>
<th>Event</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Client enters public IP address in web browser and is connected to non-secured website on HTTP port 80.</td>
<td>Firewall passes request to web server in DMZ and presents specified web page to client using HTTP port 80.</td>
<td>The connection is unsecured at this point. The initial Web page should be designed to redirect client automatically to a secure page. This ensures that password and user ID do not traverse the network unencrypted.</td>
</tr>
<tr>
<td>2</td>
<td>Server redirects client to secure web page on HTTPS port 443.</td>
<td>Web server presents specified web page using HTTPS port 443 (on the NFuse server) – presenting server certificate at this time.</td>
<td>Begin setup of SSL v3.0 tunneled session. If certificate server is not a public CA, the root certificate (server) must first be registered with the client – this provides the client with the CA’s public key.</td>
</tr>
<tr>
<td>3</td>
<td>Client web browser checks certificate presented against known certificate authorities (CAs).</td>
<td>If CA is reliable, SSL session on HTTPS port 443 is established – using private keys stored in RAM only. NFuse server presents authentication credentials challenge. This may take the form of a standard NFuse page or a customized authentication page to capture extended credentials (i.e., RSA Secure ID token).</td>
<td>Extended login credentials (NFuse login info + token info) may be collected using a DLL-based authentication agent. If extended credentials are collected, a secure cookie is placed on the client device with NFuse authentication credentials. Upon successful presentation and acceptance by NFuse the secure cookie is destroyed. This cookie removal process follows extended authentication. NOTE: During this process an agent can also trigger the opening of specified firewall ports for redirection of SSL.</td>
</tr>
<tr>
<td>4</td>
<td>Client provides authentication credentials – user ID/password and/or token.</td>
<td>User is authenticated against backend user database (on internal network) – checking extended credentials if required. NFuse presents enumerated application list based on user group membership (or other pre-defined values).</td>
<td>MetaFrame server returns enumerated list of applications via XML (HTTP port 80) – standard NFuse application enumeration. This link can be secured with VPN (server to server).</td>
</tr>
</tbody>
</table>
5 User selects application from the NFuse web page. NFuse server contacts STA to request generated ticket information. NFuse server presents client with an ICA file containing the CSG ticket information. CSG ticket is delivered to CSG server as the part of SOCKS inside SSL information. The ticket format is: 10;STAID:xxxxxxxxxxxxxxxxxxxxxxxxxxxx. The ‘xxx’ field represents a random hex address used to index the MetaFrame address stored by the STA. The ticket is only used once and destroyed (for each session).

6 Upon receiving the ICA file from NFuse, the ICA client contacts the CSG (via HTTPS port 443) to establish an ICA session to the specified application. CSG compares the ticket information, and if valid, proxies the client request to the MetaFrame server on the protected network (via TCP port 1494). CSG checks with Secure Ticket Authority (STA) to verify that the user was in fact authenticated by NFuse and not coming directly to the CSG. A firewall rule must be established that allows (DMZ to/from internal) network communications to the STA. This link can be secured with VPN (server to server).

7 CSG contacts target MetaFrame server via Port 1494 to establish ICA session and proxies information to ICA client on HTTPS port 443. User establishes server based application session. This session is tunneled via port 443 until it is closed. After which the SSL session is torn down, and the process must be repeated to establish a new ICA session.

Citrix Secure Gateway Components
There are always at least three primary components in a CSG environment:

- Citrix Secure Gateway
- Citrix NFuse
- Citrix Secure Ticketing Authority (STA)

Secure Gateway
The Secure Gateway acts as a SSL Gateway for ICA network traffic that services requests between the ICA client and the MetaFrame XP server. This is a NT service and must run on a Windows 2000 Server.

Citrix NFuse
The Citrix NFuse application portal allows organizations and application service providers (ASPs) to publish unmodified interactive applications to a standard Web browser. Customers can integrate and publish interactive applications into any standard Web browser. Administrators retain all the robust features and benefits of Citrix MetaFrame while getting business and productivity applications across the Web to users quickly and cost-effectively.

NFuse has the following benefits:

- Improved application management
- Faster deployment
- Reduced administrative costs
- Leverage of existing infrastructure
- Increased user productivity
- Security (SSL, encryption, ticketing)

On the client side, users benefit from the ease of using a familiar Web browser as their central interface to all published applications, as well as other portal content, tools and resources. With NFuse, all these systems can be viewed and interacted with as if they were a single system. Furthermore, NFuse can accommodate any level of personalization from a presentation (look) standpoint to an organization (feel) standpoint.

On the server side, Citrix MetaFrame provides single-point control, allowing applications and application content to be customized by user or by group. Application management is centralized through the deployment of applications in a controlled and monitored server environment as opposed to individual desktop deployments.

This document addresses Citrix NFuse installed on Microsoft IIS 5.0.

**Secure Ticketing Authority (STA)**

The STA is an Internet Server Application Program Interface (ISAPI) DLL that is installed on a Microsoft IIS 5.0 server. IIS 5.0 calls the DLL when a ticket is requested. The primary purpose of the STA is to generate and validate tickets for access to MetaFrame XP published applications.
Securing Citrix Secure Gateway – Best Practices

This section highlights the security considerations that need to be addressed in a CSG environment in respect to the NFuse and CSG implementation, as well as outlining a possible solution. The best practices are intended to be a guideline and may need to be customized for a particular site. Each best practice will be ranked with the level of importance (for example, Mandatory or More Secure).

**Best Practices Summary**

The table below gives a high level overview of the best practices and there importance.

<table>
<thead>
<tr>
<th>Legend</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mandatory</strong></td>
<td>This step must be completed.</td>
</tr>
<tr>
<td><strong>More Secure</strong></td>
<td>These steps should be completed unless there is a good reason not to implement them, by doing so, the CSG infrastructure will be more impenetrable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NFuse Server</th>
<th>Securing the File System</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Remove Sample Code</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>User Account</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>IIS Anonymous Access User Account</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Disable Unused Services</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Remove Windows Components</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Hot Fixes and Service Packs</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Remove Unused File Associations</td>
<td>More Secure</td>
</tr>
<tr>
<td></td>
<td>IIS Security</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Auditing</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>NetBIOS</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Information Leakage via NULL Sessions</td>
<td>More Secure</td>
</tr>
<tr>
<td></td>
<td>Port Filtering</td>
<td>More Secure</td>
</tr>
<tr>
<td></td>
<td>Denial of Service Registry Entries</td>
<td>More Secure</td>
</tr>
<tr>
<td></td>
<td>Disable Internet Printing</td>
<td>More Secure</td>
</tr>
</tbody>
</table>

Best Practices for Securing a Citrix Secure Gateway Deployment
<table>
<thead>
<tr>
<th></th>
<th>STA</th>
<th>NFuse Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Securing the File System</td>
<td>Securing the File System</td>
</tr>
<tr>
<td></td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Remove Sample Code</td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>User Account</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>IIS Anonymous Access User Account</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Disable Unused Services</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Remove Windows Components</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Hot Fixes and Service Packs</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Remove Unused File Associations</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>More Secure</td>
<td>More Secure</td>
</tr>
<tr>
<td></td>
<td>IIS Security</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Auditing</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>NetBIOS</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Information Leakage via NULL Sessions</td>
<td>More Secure</td>
</tr>
<tr>
<td></td>
<td>More Secure</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Port Filtering</td>
<td>More Secure</td>
</tr>
<tr>
<td></td>
<td>More Secure</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Denial of Service Registry Entries</td>
<td>More Secure</td>
</tr>
<tr>
<td></td>
<td>More Secure</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Disable Internet Printing</td>
<td>More Secure</td>
</tr>
<tr>
<td></td>
<td>More Secure</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>STA TCP/IP Filtering</td>
<td>More Secure</td>
</tr>
<tr>
<td></td>
<td>More Secure</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Best Practices Detail

This section outlines each of the best practices in detail. The best practices are divided into four points, description, solution, components and importance. The **description** is used to detail the best practice and its potential security vulnerability. The **solution** details what steps can be taken to reduce the security vulnerability. The **components** section details which parts of the CSG infrastructure is at potential risk and as a result of this which CSG components that the best practice solution should be applied. The **importance** point is provided as an indicator of the potential threat and vulnerability that this security consideration has on the security of a CSG implementation.

### File System

**Description**

The file system on each of the CSG components detailed below should be secured so that the Everyone group in particular does not have Write and Execute permissions for particular directories. The Windows 2000 system directories should also be secured so that the Everyone group does not have access to the server’s system files. Another important configuration change that should be made is preventing the user’s ability to traverse directories.

**Solution**

The file system is secured by modifying the ACLs on the relevant areas of the NTFS file system.

**Components**

STA, NFuse and Secure Gateway (system directories only)

**Importance**

Mandatory

### Sample Code

**Description**

During the installation of IIS 5.0 a number of sample applications are installed. These are a security hole because malicious users will know the default installation directories of the samples. A malicious user could use these samples to violate the IIS server.

**Solution**

The following directories and virtual directories should be removed if they are present.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Virtual Directory</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>IIS Samples</td>
<td>IISSamples</td>
<td>c:\inetpub\iissamples</td>
</tr>
<tr>
<td>IIS Documentation</td>
<td>IISHelp</td>
<td>c:\winnt\help\iishelp</td>
</tr>
<tr>
<td>Data Access</td>
<td>MSADC</td>
<td>c:\program files\common files\system\msadc</td>
</tr>
</tbody>
</table>

**Components**

STA and NFuse

**Importance**

Mandatory
Authentication

Description

Authentication is a critical component of CSG security. The recommended method for authentication is using some form of certificate-based authentication (such as two-factor authentication using SecurID). If using Windows NT LAN Manager (NTLM) for authentication, it is recommended that a local or group policy be implemented that only accepts NTLMv2 authentication. The reason is that a simple hash algorithm, which performs basic encryption, is used for NTLM and there are numerous utilities available that can decrypt the passwords that are stored in the Windows NT Storage Account Management (SAM) database.

If a certificate is used during authentication, it is important that a Certificate Trust List (CTL) be configured on the IIS server so that malicious users do not use unknown Certificate Authorities.

Solution

1. Within the Microsoft Management Console (MMC), load the Security Templates and Security Configuration and Analysis snap-ins.
2. Copy the template securews and call it secure_ccs.
3. Select Local Policies\Security Options\LAN Manager Authentication Level.
4. Modify this setting to “Send NTLMv2 responses only, refuse LM and NTLM” as shown in the figure below.

![Figure 2 - Configure Authentication Level](image)
Components
NFuse and STA

Importance
Mandatory

User Accounts

Description
User accounts can be a major weakness in a Windows 2000 environment; an important consideration is the prevention of malicious access to the environment using brute-force password-related attacks. These can be made much more difficult by implementing a security policy. The following settings must be implemented:

- Password History – 7 Passwords remembered
- Maximum Password Age – 180 days or less
- Minimum Password Age – 1 day or more
- Minimum Password Length – 8 characters
- Passwords must meet complexity requirements – Enabled
- Reverse Encryption – Disabled
- Account Lockout duration – 3 minutes or more
- Account Lockout Threshold - 3

All unused local user accounts must be disabled. These include the following:

- IUSR_MYPC
- Guest

Solution
1. Within the MMC, load the Security Templates and Security Configuration and Analysis snap-ins
2. Copy the template securews and call it secure_ccs
3. Select Account Policy\Password Policy and configure as shown in the figure below:
Components

NFUSE, Secure Gateway and STA

Importance

Mandatory
IIS Anonymous Access User Account

Description

To allow anonymous access to an IIS 5.0 server, the default IIS 5.0 installation creates a user name called IUSR_SERVERNAME. Since this is a well-known account it provides a malicious user with potential security vulnerability. The password of this account is randomly generated. This user account needs to be disabled. A new user account needs to be created only if anonymous user access is required. Leaving the default account there adds a decoy account that can be used in conjunction with system auditing to detect if an attempt has been made to gain access to the server.

Solution

1. Start Computer Management and select Local Users and Groups
2. Select IUSR_COMPUTERNAME and disable this account

![Figure 4 - Disable Default IIS Anonymous Account](image)

3. Create a new account called CCS_ANON with a strong password. A strong password is at least 10 characters long and has a combination of alphanumeric characters. The passwords should not contain natural language words.
4. Within Computer Management select IIS
5. Right-click Default Web Site
6. Select the Directory Security tab
7. Click on the Edit button for Anonymous access and authentication Control
8. Modify the User Name as in the figure below:

![Figure 6 - Modify Anonymous Account Within IIS 5.0 part 1](image)

Components

NFuse and STA

Importance

Mandatory
Disable Unused Services

Description

All Windows 2000 services provide a level of vulnerability, so it is important to disable the services that are not needed. The following is a list of services that need to be disabled:

- Application Management
- Clipbook
- Computer Browser
- DHCP
- DFS
- DNS Server
- Fax Service
- File Replication Service
- Index Service
- Internet Connection Sharing
- Intersite Messaging
- Messenger
- Net Meeting Remote Desktop Sharing
- Network DDE
- Network DDE DSDM
- Performance Logs and Alerts
- Print Spooler
- QoS RSVP
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Registry Service
- RunAs Service
- SMTP
- Smart Card
- Smart Card Helper
Solution

1. Start Computer Management and select Services
2. Highlight the service and select properties
3. Disable each of the services listed above as depicted in the figure below:

![Indexing Service Properties (Local Computer)](image)

**Figure 8 - Disable Unused Services**

**Components**

NFuse, Secure Gateway and STA

**Importance**

Mandatory
Remove Windows Components

Description
During an installation of Windows 2000 Server a number of windows components are installed by default. These are not necessary and only increase security vulnerability. An example of this would be the FTP or Telnet server components within the IIS installation options.

Solution
1. Start Control Panel and select Add/Remove Programs

2. Deselect all Windows Components except Internet Information Services
3. Within the IIS options deselect everything except Common Files, Internet Information Services Snap-In and World Wide Web Server.
Components

NFuse, Secure Gateway and STA

Importance

Mandatory
Hot Fixes and Service Packs

Description

The Internet is a dynamic environment, and new security vulnerabilities are discovered everyday. It is very important that all Microsoft security hot fixes are installed when they become available.

Solution

Microsoft has developed a tool called HFNETCHK.EXE, which is available at www.microsoft.com/technet. This tool uses XML to compare the server against a list of currently released security hot fixes. Below is an example of that output from the utility. The output of the utility is a list of hot fixes that have not been applied, as well as a reference to a TechNet Q article explaining the security vulnerability that the hot fix applies to.

Figure 13: Check Microsoft for Latest Security Hot Fixes

Once the utility has been run, the Hot Fixes can to be downloaded from www.microsoft.com and installed on the server.

Components

NFuse, Secure Gateway and STA

Importance

Mandatory
Remove Unused File Associations

Description

IIS uses file associations to map a file type to a specific program. This program is run when the file type is encountered. A malicious user may substitute the original program with a substitute program and use that to breach the security of the system. Remove the following file associations:

| .printer | .asa |
| .htw     | .htr |
| .ida     | .idc |
| .idg     | .stm |
| .cdf     |     |

Solution

1. Within Computer Management, select IIS
2. Right-click Default Web Site
3. Select the Home Directory tab
4. Under Application Settings, select Configuration
5. Remove the Unused File Associations Listed above as depicted in the figure below:

![Figure 14 - Remove Unused File Associations](image)

Components

NFuse and STA

Importance

More Secure
IIS Security

Description
Permissions on folders should be as restrictive as possible. The NFuse and STA scripts will be located in a script folder with Execute permissions set to Scripts only and with no Read or Write permissions set. All other directories should have no Execute Permissions and be set to Read only. Directory browsing should always be off. IP address and domain name restrictions should be set to duplicate your firewall rules. This adds another layer of security.

Solution
Configure the permissions using the MMC and use the Internet Information Server snap-in.

Components
NFuse and STA

Importance
Mandatory

Auditing

Description
Auditing is an essential security consideration. Without auditing it may be hard to detect that a user has infiltrated the system or has attempted to do so. The size of the event log also needs to be increased to 500MB and needs to be backed up weekly. It is essential that the following objects be audited:

- Account management
- Logon events
- Policy change

Solution
1. Within the MMC, load the Security Templates and Security Configuration and Analysis snap-ins.
2. Copy the template securews and call it secure_ccs
3. Select Local Policies\Audit Policy and configure as in the figure below:
Figure 15 - Configure Auditing Policy

Components

NFuse, Secure Gateway and STA

Importance

Mandatory
NetBIOS

Description

The Server Message Block (SMB) protocol, also known as the Common Internet File System (CIFS), enables file sharing over networks. Improper configuration can expose critical system files or give full file system access to any hostile party connected to the Internet. Access to administrative shares like ADMIN$, C$ etc should be disabled. On the NFuse Server depending on the authentication method used, if the server is part of an NT domain and NTLMv2 authentication is used, then Client for Microsoft Networks will need to be enabled. NTLMv2 authentication uses NetBIOS application calls to authenticate to a Microsoft NT 4.0 compatible domain controller. This also affects Windows 2000 networks running in mixed mode.

Solution

1. Stop sharing the default administrator shares & unbind NETBIOS from the adapter.
2. Right-click My Network Places
3. Highlight each network adapter and right click with your mouse
4. Select the Properties of each Network Adapter
5. Deselect Client for Microsoft Networks and File and Print Sharing for Microsoft Networks

![Figure 16 - Disable NetBIOS](image)

6. Select TCP/IP click on Properties
7. Click on Advanced select WINS
8. Click on Disable NetBIOS over TCP/IP

Components

NFuse, Secure Gateway and STA

Importance

Mandatory
Information Leakage via NULL Sessions

Description

If NetBIOS must be enabled, you can limit the amount of information returned to users via a NULL session. Windows 2000 Server uses NULL sessions for the browser service to return a server’s list of shares or local users. A registry key can be set to minimize the amount of information that is returned by these requests. If you can connect to the server with the following command, then NULL sessions are available: net use \w.x.y.z\ipc$ " /user:""

Solution

1. Start REGEDT32.EXE
2. Set the following registry value:
   HKLM/System/CurrentControlSet/Control/LSA/RestrictAnonymous=2
3. This will bar all anonymous access to NULL sessions. By setting this value to 1 the information returned is restricted.

Components

NFuse, Secure Gateway and STA

Importance

More Secure
Port Filtering

Description

Enabling port filtering on each network card will add an extra level of security to the CSG infrastructure. Port filtering allows access to specific IP ports. We need to limit this to the ports used by CSG. On the NFuse server the ports that need to be enabled are the following:

- HTTP and XML Port 80
- HTTPS Port 443

On the Secure Gateway, the ports that need to be enabled are the following:

- SSL Port 443
- ICA Port 1494
- XML Port 80

The STA needs the following ports available:

- XML Port 80

Solution

On each of the servers:
1. Right-click My Network Places
2. Select TCP/IP and click Properties
3. Click Advanced
4. Select TCP/IP filtering and select Properties
5. On the TCP Ports, select Permit Only
6. Add the ports listed above for the server you are configuring

Components

NFuse, Secure Gateway and STA

Importance

More Secure
STA TCP/IP Filtering

Description

The STA should only accept TCP/IP connections from the NFuse server and also the CSG server. This is to stop other servers impersonating these components. It is possible that the STA can allocate a secure ticket to an invalid host giving a malicious user the potential to access to published applications.

Solution

On the STA:

1. Right-click My Network Places
2. Right Click on the network adapter
3. Select TCP/IP and click Properties
4. Click Advanced
5. Select TCP/IP filtering and select Properties
6. On the TCP Protocol, select Permit Only
7. Add the TCP/IP addresses of the NFuse server and the CSG server

Components

STA

Importance

More Secure
Denial of Service Registry Entries

Description

The following registry entries need to be applied in HKLM\System\CurrentControlSet\Services to help guard against denial-of-service registry attacks.

| Key: Tcpip\Parameters Value: SynAttackProtect Value Type: REG_DWORD Parameter: 2 |
| Key: Tcpip\Parameters Value: EnableDeadGWDetect Value Type: REG_DWORD Parameter: 0 |
| Key: Tcpip\Parameters Value: TcpMaxHalfOpen Value Type: REG_DWORD Parameter: 100 |
| Key: Tcpip\Parameters Value: KeepAliveTime Value Type: REG_DWORD Parameter: 300000 |
| Key: Tcpip\Parameters Value: TcpMaxHalfOpenRetried Value Type: REG_DWORD Parameter: 80 |
| Key: Tcpip\Parameters Value: EnableICMPRedirect Value Type: REG_DWORD Parameter: 0 |
| Key: Tcpip\Parameters Value: EnablePMTUDiscovery Value Type: REG_DWORD Parameter: 0 |
| Key: Netbt\Parameters Value: NoNameReleaseOnDemand Value Type: REG_DWORD Parameter: 1 |

Solution

1. Start REGEDT32.EXE
2. Set the registry values detailed above

Components

NFuse, Secure Gateway

Importance

More Secure
Disable Internet Printing

Description
Windows 2000 provides the ability to print from the Internet; this functionality should be disabled. Printers are attached to the server by means of a Web page; administration of these printers is also accessed from a Web page. This creates a large hole through which your server can be attacked. Many times Internet printing is disabled from the Internet Service Manager, but after you reboot or log out, the Group Policy object that enables Internet printing will restart this functionality. Make sure that it is not in your Group Policy object before deploying the server.

The registry setting below will disable Internet printing.

HKLM\Software\Policies\Microsoft\Windows NT\Printers
Key: DisableWebPrinting
Value: DisableWebPrinting
Value Type: REG_DWORD
Parameter: 1

Solution
1. Start REGEDT32.EXE
2. Set the registry value detailed above

Components
NFuse, Secure Gateway

Importance
More Secure
Appendix: More Information

For more information on these security topics, please see the following websites.

http://rr.sans.org/win2000/sec_win2k.php
http://nsa2.www.conxion.com/win2k/
http://rr.sans.org/win2000/vulnerabilities.php
http://rr.sans.org/win2000/sec_IIS.php
http://rr.sans.org/win2000/5threats.php
http://www.microsoft.com/technet/security/iis5chk.asp