Chapter 11
Implementing Security Policy

Prescriptive Architecture Guide

Abstract
After the required servers for the base architecture and any additional components and applications have been installed in the Microsoft® Systems Architecture (MSA) Internet Data Center (IDC), the security policies are applied. This chapter describes the implementation of the Internet Data Center security and authentication solutions. This chapter also explains the implementation of various policies and discusses the detailed steps for securing servers in the perimeter network.
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>Strategic Technology Protection Program</td>
<td>1</td>
</tr>
<tr>
<td>Design Considerations</td>
<td>1</td>
</tr>
<tr>
<td>Resource Requirements</td>
<td>2</td>
</tr>
<tr>
<td>IMPLEMENTING SECURITY POLICIES</td>
<td>3</td>
</tr>
<tr>
<td>Policy Design</td>
<td>3</td>
</tr>
<tr>
<td>Applying Policies</td>
<td>3</td>
</tr>
<tr>
<td>Applying Security to Servers</td>
<td>4</td>
</tr>
<tr>
<td>Forcing Domain Controller Replication</td>
<td>5</td>
</tr>
<tr>
<td>Implementing Security in the Internet Data Center</td>
<td>5</td>
</tr>
<tr>
<td>Architecture</td>
<td>5</td>
</tr>
<tr>
<td>Backing Up the System State</td>
<td>7</td>
</tr>
<tr>
<td>Creating Custom Security Templates for Each Server Class</td>
<td>7</td>
</tr>
<tr>
<td>Creating and Installing the Domain Policy</td>
<td>9</td>
</tr>
<tr>
<td>Creating and Installing the Domain Controller Policy</td>
<td>10</td>
</tr>
<tr>
<td>Creating Organizational Units for Each Class of Server</td>
<td>11</td>
</tr>
<tr>
<td>IIS Servers</td>
<td>11</td>
</tr>
<tr>
<td>External DNS Servers</td>
<td>11</td>
</tr>
<tr>
<td>Management Servers</td>
<td>11</td>
</tr>
<tr>
<td>SQL Server 2000 Clusters</td>
<td>11</td>
</tr>
<tr>
<td>Importing Security Templates for Each Organizational Unit</td>
<td>12</td>
</tr>
<tr>
<td>IMPLEMENTING IP PACKET FILTERS BY USING IPSEC</td>
<td>14</td>
</tr>
<tr>
<td>DISABLING NETBIOS AND SMB ON DMZ SERVERS</td>
<td>18</td>
</tr>
<tr>
<td>SECURING AN IIS 5.0 WEB SERVER</td>
<td>19</td>
</tr>
<tr>
<td>Removing Nonessential Folders</td>
<td>19</td>
</tr>
<tr>
<td>Disabling Nonessential IIS Services</td>
<td>19</td>
</tr>
<tr>
<td>Removing Script Mapped ISAPI Extensions</td>
<td>20</td>
</tr>
<tr>
<td>Disabling WebDAV</td>
<td>21</td>
</tr>
<tr>
<td>Securing IIS Defaults</td>
<td>21</td>
</tr>
<tr>
<td>Disabling Parent Paths</td>
<td>22</td>
</tr>
<tr>
<td>Enabling Auditing</td>
<td>23</td>
</tr>
<tr>
<td>Installing Security Hot Fixes</td>
<td>24</td>
</tr>
<tr>
<td>ADDITIONAL SECURITY SETTINGS FOR ALL SERVERS</td>
<td>25</td>
</tr>
<tr>
<td>Restricting Default NTFS Permissions</td>
<td>25</td>
</tr>
<tr>
<td>Securing the Administrator Account on Member Servers</td>
<td>27</td>
</tr>
<tr>
<td>Securing the Administrator Account on Domain Controllers</td>
<td>28</td>
</tr>
<tr>
<td>Service Accounts</td>
<td>28</td>
</tr>
<tr>
<td>IMPORTANT ISSUES AND RECOMMENDATIONS</td>
<td>29</td>
</tr>
</tbody>
</table>
SUMMARY ........................................................................................................30
  Additional Information ..................................................................................30

APPENDIXES ..................................................................................................31
  Appendix 11.1 – Security Template for DMZ Servers ..................................31
  Appendix 11.2 – Security Template for Management Servers ......................31
  Appendix 11.3 – Security Template for SQL Server .....................................31
  Appendix 11.4 – Security Template for Domain Controllers .......................31
  Appendix 11.5 – Security Template for the Domain ....................................31
  Appendix 11.6 – Enhanced File Security Batch File ....................................32
INTRODUCTION

Security is a major consideration for all networks, but it is crucial for e-commerce networks, which conduct financial transactions and store sensitive information, and thus become targets for malicious attacks mounted over the Internet. Security breaches can range from minor intrusions and embarrassing infiltrations, to serious, costly, and disastrous events. The effects of a security breach can result in reduced customer confidence and a substantial loss of business.

This chapter discusses the steps for installing and configuring the components used to implement security and authentication in the Internet Data Center base architecture. The application of security to some Internet Data Center additional components, such as database and management servers, is also included.

Strategic Technology Protection Program

The Strategic Technology Protection Program (STPP) provides information, tools, and services to help ensure that systems can be made secure in a simple manner, and can then be kept secure in the future with minimal time and effort.

To ensure that the security issues faced by the Internet Data Center architecture, many of which are addressed by the STTP, are completely understood, this document details these steps without the help of many of the tools and services provided by this program.

After you fully understand the secure issues faced in the configuration of the Internet Data Center architecture, implementing the STTP will ensure that your environment will "get secure" and "stay secure."

For details about the most recent developments with the Strategic Technology Protection Program initiative and all Microsoft-related security issues, go to:

http://www.microsoft.com/security

Design Considerations

The Internet Data Center architecture is based on known security methodologies, real-world experiences, and best practices. Implementing network security is a complicated process that is susceptible to human error, particularly when you have to configure many different servers. The Internet Data Center implementation simplifies the process of applying security by providing an architecture that is based on Microsoft Active Directory™ directory service, organizational units, and policies, which will help automate many of the tasks.
Resource Requirements
To fully implement the Internet Data Center security model, you need to have an in-depth knowledge of Microsoft® Windows® 2000, Active Directory, and registry configuration. It is imperative that the IT professionals who implement security have a thorough understanding of networking technologies and devices (such as firewalls, routers, switches, protocols, and ports).
Securing a large e-commerce network for live Internet access is a complex process. A firewall is not enough to ensure that the servers are secure. You need to follow numerous configuration procedures for securing servers before placing them on the active connection to the Internet. Though the Microsoft Internet Information Services (IIS) servers and Domain Name System (DNS) servers are the only servers exposed to the Internet directly, you still need to protect the domain controllers and all other servers that reside in the internal network.

The following sections describe the procedure for deploying security from Active Directory by using Group Policy objects (GPOs). This method automatically applies security to the servers that belong in the domain. This section assumes that you are already familiar with managing GPOs and that you understand the ramifications of changing security settings within the GPO. You can find more information about group policies at the following Web site:


**Important:** Test policies thoroughly on servers within a test environment that simulates the production environment. Incorrect configuration changes applied to production servers could disable the server to the point where it must be rebuilt.

**Policy Design**

The Internet Data Center architecture partitions the policy implementation as follows:

- **Domain-wide policy.** Implemented to address the common security requirements, such as account policies and audit policies, that must be enforced for all servers in the perimeter network.

- **Organizational unit policies.** Implemented to address specific server security requirements that are not common to all the servers in the network. For example, the security requirements for the IIS servers differ from those for servers running Microsoft SQL Server™ 2000. To address this, separate organizational unit policies are configured to meet the specific needs of each of these roles. The servers are then configured to receive the specific policy that applies to their role in addition to the domain-wide policy.

**Applying Policies**

This section describes the steps taken to implement security policies and to apply security to the servers in the Internet Data Center architecture. As with any production environment, it is important to test fully the results of a policy change before applying security to all servers. It is recommended that these tests be carried out in a test lab prior to release, but if that is not practical you can apply security as follows:
1. Select one server in each group (one of the IIS servers, for example).

2. Apply the security policy to it.

3. Test that the server performs all its required functions and is able to communicate successfully with other servers.

4. Check the Event Log service for any outstanding error messages.

5. Restart the server to ensure that it starts properly, because the policy will disable certain services that are not required.

6. After you are satisfied that the server is functioning properly, apply security to the rest of the servers within the same group and test each one again.

Applying Security to Servers
After you implement security to the domain and all the organizational units, the member servers in the domain will receive only the domain-wide policy until they are manually moved within Active Directory to their correct destination organizational unit. When servers are first created and joined to the domain, they are automatically placed in the computer’s container within Active Directory. To apply all the security settings, they still need to be moved to the destination organizational unit. Before moving the server into the organizational unit, check Event Log to see the errors that occurred before security was applied so they are known. After the server is moved into the organizational unit, you can immediately download the policy to the server. To do this at the server, at a command prompt, run the **Secedit /refreshpolicy machine_policy** command.

The **Secedit /refreshpolicy machine_policy** command tells the server to check Active Directory for any updates to the policy and, if there are any, to download them immediately. If the policy is downloaded successfully, an Event Log message with the following information appears:

- Type: Information
- SourceID: SceCli
- Event ID: 1704
- Message String: Security policy in the Group Policy objects are applied successfully

It may take a few minutes for this message to appear. If you do not receive the successful Event Log message, you need to restart the server to force the server to download the policy. Check Event Log again after the restart to verify the successful download of the policy. You may want to restart the server a number of times to ensure that it is stable.
Another method for verifying that the policy has been applied successfully is to review the effective policy setting on the local server.

**To verify the effective policy settings:**

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Local Security Policy**.
2. Under **Security Settings**, click **Local Policies**, and then click **Security Options**.
3. In the right pane, view the **Effective Settings** column to verify that the correct security settings have been applied.

**Forcing Domain Controller Replication**

After any Active Directory changes are made on one domain controller, the other domain controller must wait for the default replication cycle to expire (usually five minutes) to receive any updates. Before applying security to any server in the Internet Data Center architecture by using Group Policy objects, ensure that the two domain controllers are fully synchronized. Otherwise, the server being secured may contact the domain controller that has not yet received the update and, therefore, not get the new or updated policy. To ensure replication between the two domain controllers, you can force each of the domain controllers to replicate to the other domain controller.

**To force domain controller replication:**

1. Open **Active Directory Sites and Services**, expand **Default-First-Site-Name**, expand **Servers**, expand both **MSADC1** and **MSADC2** and then, for each server, click **NTDS Settings**.
2. In the right pane, right-click the default name and select **Replicate Now**. This will force replication immediately between both domain controllers.

**Implementing Security in the Internet Data Center Architecture**

The steps for applying security to all the servers in the Internet Data Center architecture are as follows. (For specific details about implementing each step, see the sections that follow.)

1. Back up each server prior to applying security. Make sure the system state is included in the backup, because this is where the registry data is kept.
2. Create and install the domain policy and verify that the policy is being distributed to all servers in the domain. After the policy is implemented, check the local policy of one of the member servers in the domain to verify that the password, account, and audit policies have been applied.
3. Back up the system state of both domain controllers. This will also back up all the objects in Active Directory for each controller. Create and install the domain controller policy in the Domain Controller organizational unit and import the domain controller security template into the GPO. After applying the security template to the Domain Controller organizational unit, force replication between each domain controller using the Active Directory Sites and Services management console. Use the `secedit` command line utility as follows on each domain controller to download and apply the new policy: `Secedit /refreshpolicy machine_policy`

Restart each domain controller to ensure that it starts successfully.

4. Create organizational units for each class of server. The following are example organizational units used within the Internet Data Center architecture:
   - IIS Cluster1 Servers
   - IIS Cluster2 Servers
   - External DNS Servers
   - SQL Servers (additional components built on top of the base architecture)
   - Management Servers (additional components built on top of the base architecture)

5. For each organizational unit, create a new Group Policy object (GPO) and import the appropriate security template into the newly defined object. Select one of the servers from the computer's container and move it into the appropriate organizational unit to apply security to it. Force replication between the domain controllers and then, from the server that is to have security applied, download the policy by using the `secedit` command. Verify in Event Log that the policy was downloaded successfully and that the server can communicate with the domain controllers and with other servers in the domain. After successfully testing one server in the organizational unit, move the remaining servers in the organizational unit and then apply security. Use the `secedit` command line utility as follows on each server to download and apply the new policy: `Secedit /refreshpolicy machine_policy`

Restart the servers after the policy is applied to ensure that all security settings are currently configured. Check the Event Logs.

6. Implement IPSec packet filtering for the IIS servers. From each IIS Cluster organizational unit, install filtering into the IPSec policy of the GPO to permit only port 80 traffic through to the IIS servers' Internet facing interface.
7. For each IIS server and DNS server, disable NetBIOS on the Internet facing interface.

8. Secure the Web sites for each IIS server by using the IIS 5.0 lockdown steps discussed later in this chapter.

9. For each server in the domain, apply additional security. For further information, refer to the "Additional Security Settings for All Servers" section later in this chapter.

**Backing Up the System State**

Before applying policy and security changes to each server, take backups of the Windows 2000 server system state by using the backup utility provided with Windows 2000. Make sure you back up the system state as described in the following steps. (When backing up the system state on the domain controllers, all objects in Active Directory are included in the backup, including Group Policy objects.)

**To run the backup utility:**

1. Click **Start**, point to **Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.

2. On the **Backup** tab, click **Browse**, and then enter the path to which you want to save the backup file on the local hard drive.

3. Select the **System State** check box, and then click **Start Backup**.

4. Accept the default settings in the **Backup Job Information** dialog box by clicking **Start Backup**.

**Creating Custom Security Templates for Each Server Class**

Each type of server may require different security configurations. Although the differences are minor, automating management is best served by creating a distinct security template for each server type. Table 1 lists the templates used on each class of server (both base architecture and additional components) in the Internet Data Center architecture; copies of these templates are provided in Appendixes 11.1 to 11.6 see the Appendixes section at the end of this chapter for more details.
Table 11.1 Security Templates

<table>
<thead>
<tr>
<th>Security Template</th>
<th>GPO Container</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDCDMZ.inf</td>
<td>IIS Cluster1 Servers and Cluster2 Servers organizational units and External DNS Servers organization unit</td>
</tr>
<tr>
<td>IDLCMMgmt.inf</td>
<td>Management Servers organizational unit (additional component)</td>
</tr>
<tr>
<td>IDCSQL.inf</td>
<td>SQL Servers organizational unit (additional component)</td>
</tr>
<tr>
<td>IDCDC.inf</td>
<td>Domain Controller organizational unit</td>
</tr>
<tr>
<td>IDCDomain.inf</td>
<td>Domain container</td>
</tr>
</tbody>
</table>

If you need to make changes to the security policies, first edit the template files. These new template files must then be imported into the GPO to update the Group Policy with the changes. The new template files must be copied to both domain controllers to maintain consistency.

To review or make modifications to the policy template file from the domain controller:

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type **MMC**, and then press **ENTER**.
3. In the **Secure Templates** MMC snap-in, click **Console**, and then **Add/Remove Snap-in**.
4. Click **Add**, click **Security Templates**, and then click **Add**.
5. Click **Close**.
6. Click **OK** to load the snap-in into the console window.
7. Expand the `%systemroot%\Security\Templates` folder.
8. Select a template to view its current configuration. To make changes, double-click a policy setting within the template, and then make the appropriate changes.
9. To save the template, right-click the template name, (for example, **IISPolicy**), and click **Save** to replace the configuration or **Save As** to create a new template.
10. Make sure the template is copied to the other domain controller for consistency.
Creating and Installing the Domain Policy
To implement changes to the default domain policy in the Internet Data Center architecture, create a new Group Policy object and link it above the default domain policy. After this GPO is enabled, it overrides the specific settings in the default domain policy that are configured when the domain is initially built.

The changes to the domain policy are made in the Active Directory Users and Computers management console.

To make changes to the domain policy:
1. Click Start, point to Programs, point to Administrative Tools, and then click Active Directory Users And Computers.
2. Right-click the domain name for which you want to change the domain policy, and then click Properties.
3. On the Group Policy tab, click New to add a new Group Policy. Give it a name such as "Domain Override." Make sure the new policy is displayed above the default domain policy so it will override the default settings. To do this, select the new policy, and then click the Up button to move the new policy above the default domain policy.

The domain policy security template enforces password restrictions, account lockouts, and detailed audit logging for all servers in the domain.

The next step is to import the IDCDomain.inf security template into the Domain Override GPO.

To import the IDCDomain.inf template:
1. Select the Group Policy that you have created, and then click Edit.
2. Expand Computer Configuration, expand Windows Settings, and then right-click Security Settings.
3. Click Import Policy, and then click IDCDomain.inf.
4. Select the Clear the database before importing check box.
5. Click Open, and then click OK.
6. Force replication between both domain controllers, according to the steps outlined earlier in this chapter.
Creating and Installing the Domain Controller Policy

A domain controller resides in its own organizational unit, which is created when the Windows 2000 domain is created. The domain policy will not override certain settings on a domain controller, such as the auditing policies. These settings will need to be configured in the domain controller policy. Similar to the domain policy, a new domain controller policy is created and linked above the default domain controller policy to override its default settings.

In the Internet Data Center architecture, a domain controller security template was created to store the configuration changes to be applied to the policy.

To install the IDCDC.inf template into the domain controller policy:

1. Click Start, point to Programs, point to Administrative Tools, and then click Active Directory Users And Computers.
2. Select the Domain Controller organizational unit for which you want to create a new policy, and then click Properties.
3. On the Group Policy tab, click New to add a new Group Policy. Give it a name such as "DC Override." Make sure the new policy is above the default domain controller policy so it will override the default settings. To do this, select the new policy, and then click the Up button to move the DC Override policy above the default domain controller policy.

To import the IDCDC.inf security template:

1. Select the policy that you have just created, and then click Edit.
2. Expand Computer Configuration, expand Windows Settings, and then right-click Security Settings.
3. Click Import Policy, and then click IDCDC.inf.
4. Select the Clear the database before importing check box.
5. Click Open and then click OK.
6. Force replication for both of the domain controllers so the second controller will get the policy object in its database immediately. Use the Active Directory Sites and Services management console to trigger immediate replication.

Note After the domain controller policy is updated, the domain controllers will receive the changes every five minutes with their default replication cycle.
Creating Organizational Units for Each Class of Server
Organizational units are containers that allow you to group objects within Active Directory. You can then set specific configurations that are applied only to the objects that are in the organizational unit container. The Internet Data Center architecture uses Group Policy objects defined in each organizational unit to apply common security settings to the servers that are in that organizational unit. Custom security templates can be imported into the GPO without affecting servers in other organizational units. After the GPO is assigned to the organizational unit and the security template is imported into the GPO, security policies are applied automatically to all servers that are in the organizational unit.

Domain controllers are automatically created and assigned to the Domain Controller organizational unit when the domain is created. In the Internet Data Center architecture, you create additional organizational units for the different classes of servers (for example, IIS servers and DNS servers). You also create them for any additional components installed on top of the base architecture, such as Management servers and SQL Server cluster servers.

IIS Servers
IIS servers need the highest security that can be applied, because they are on the front line of the perimeter network. The security model created for IIS servers enforces strong security. This includes hardening of the TCP/IP stack, disabling services not required, securing NTFS default permissions, and overriding the default security options of Group Policy with enforced restrictions.

External DNS Servers
The external DNS servers are grouped into their own organizational unit and assigned the same security template as the IIS servers, because they are also located in the demilitarized zone (DMZ) and need the highest security applied.

Management Servers
It is recommended that you use the same settings for the management servers as those applied to the IIS Servers. However, you need to use the additional registry settings implemented to protect IIS from misuse of TCP/IP and to disable some of the additional services.

SQL Server 2000 Clusters
When building SQL Server 2000 clusters onto the base architecture, it is important to note that these cluster servers are very sensitive to policy changes. One difference between the SQL Server 2000 cluster security model and the model used in the rest of the organizational units is with the LMCompatibilitymode policy setting. The SQL Servers 2000 cluster’s LMCompatibilitymode is configured for LM and NTLM, while all other servers in the domain are configured to only use NTLMv2. The
Cluster service does not function properly when configured to use NTLMv2 authentication. If NTLMv2 is implemented by using either a local security policy or by using a domain security policy, a cluster can be formed, but a cluster node cannot be joined. The details of this problem and resolution can be found in the Microsoft Knowledge Base article Q272129. However, due to time limitations, this latest solution was not tested in the Internet Data Center lab and, therefore, the SQL Server policy was configured to use LM and NTLM authentication.

**Importing Security Templates for Each Organizational Unit**

After you have created the organizational units described in the previous section, you can create a new Group Policy for each organizational unit. The security templates (.inf file) for each group of servers can then be imported into the newly created policy.

**To create a new security policy and import the security template for each organizational unit:**

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users And Computers**.

2. Select the organizational unit for which you want to create a new policy, such as the External DNS Servers organization unit, and then click **Properties**.

3. On the **Group Policy** tab, click **New**, and then enter a meaningful name for the new policy, such as "External DNS Servers Policies."

4. Select the new policy, and then click **Edit**.

5. Expand **Computer Configuration**, expand **Windows Settings**, and then right-click **Security Settings**.

6. Click **Import Policy**, and then click the security template created in the previous section. For the external DNS servers, IDCDMZ.inf was the security template imported into the group policy object.

7. Select the **Clear the database before importing** check box.

8. Click **Open** and then click **OK**.

9. Repeat steps 2 through 8 for each of the organizational units that require a security policy.

Now that the policy has been created and loaded with the correct security template, the servers can be moved into the appropriate organizational unit.
To move the server to the appropriate organizational unit:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users And Computers**.
2. Click the Computer organizational unit.
3. Right-click the server that needs to be moved.
4. Click **Move operation**, and then click the organizational unit to which you want the server moved.
You can improve security by permitting only the required TCP/IP ports to access the server’s external network adapter card that connects to the Internet. If the firewall were to become compromised by an attacker, applying packet filtering to the Internet-facing interfaces for servers in the DMZ would provide another level of defense. For the Internet Data Center architecture, IP security is implemented using Group Policy objects to automate the application of filters to each server in the DMZ. For the IIS servers, only TCP port 80 traffic is permitted; all other ports are blocked.

Group Policies were created in the previous section for the IIS organizational units. After the IPSec policy is activated within the organizational unit, all IIS servers that belong to the organizational unit will be able to apply the policy to their Internet facing interface. Only Hypertext Transfer Protocol (HTTP) traffic will be allowed to the IIS servers from the Internet. Other protocols and ports such as PING will no longer function on the IIS server’s Internet facing interface.

To implement the IPSec filter for each IIS server, two filters were created and applied to each policy. The first filter only permits port 80 traffic to the IIS servers and the second filter denies all other traffic to the IIS servers on the Internet facing interface. These filters are implemented in the organizational units by modifying the Group Policy objects. Note - The names and numbers of servers and VLANs in your IDC may vary.

The following IP security filters and policies were manually created in the group policy object within the organizational unit:

**To implement IPSec for IIS servers:**

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users And Computers**.
2. Select the **IIS Servers** organizational unit and then click **Properties**.
3. On the **Group Policy** tab, click **Edit**, expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.
4. Right click **IP Security Policies on Active Directory** and then select **Manage IP filter lists and filter actions**.

**To create a block filter:**

1. On the **Manage Filter Actions** tab, click **Add** and then click **Next**.
2. For **Filter Action Name**, type **Block** and then click **Next** to continue.
3. For **Filter Action General Options**, select **Block**, then click **Next** and click **Finish** to end the wizard.
To create the HTTP traffic filter:

1. On the **Manage IP Filter List** tab, click **Add** to add a new filter and assign a name. Give it a description such as “Permit HTTP traffic to Web servers”

2. Click **Add** to start the IP Filter Wizard and then click **Next**.

3. In the **Source Address** drop-down list, select **Any IP Address** and then click **Next**.

4. In the **Destination Address** drop-down list, select **A Specific IP Subnet**. Then, assign the VLAN subnet address and subnet mask (192.168.16.0 and 255.255.255.0). Click **Next**.

5. In the **IP Protocol Type** drop-down list, select **TCP** and then click **Next**.

6. In the **IP Protocol Port** screen, select **From Any Port** and select **To this port** and then assign **80** for the value to this port.

7. Click **Next**, click **Finish**, and then click **Close** to close the **IP Filter List** dialog box.

To create all other traffic filters:

1. On the **Manage IP Filter List** tab, click **Add** to add a new filter, assign it a name, then give it a description, such as **Block all other traffic to web servers**.

2. Click **Add** to invoke the IP Filter Wizard and then click **Next**.

3. In the **Source Address** drop-down list, select **Any IP Address** and then click **Next**.

4. In the **Destination Address** drop-down list, select **A Specific IP Subnet**, assign the VLAN subnet address and subnet mask (192.168.16.0 and 255.255.255.0). Click **Next**.

5. In the **IP Protocol Type** drop-down list, leave the default setting, which is **Any**, and click **Next**.

6. Click **Finish**, and then click **Close** to close the **IP Filter List** dialog box.

7. Click **Close** again to close the **Manage IP filter lists and filter actions** dialog box.
To create the IP security policy:
When you have defined the filters for Web server VLAN, create an IPSec policy and then apply the new filters as follows:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users And Computers**.
2. Select the **IIS Servers** organizational unit, and then click **Properties**.
3. On the **Group Policy** tab, click **Edit**, expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.
4. Right-click **IP Security Policies on Active Directory**, select **Create IP Security Policy** to start the IP Security Policy Wizard, and then click **Next** to continue.
5. Assign a new name, such as “IIS VLAN Policy,” to the policy and then click **Next**.
6. Clear the **Activate the default response rule** check box, click **Next**, and then click **Finish** to bring up the **Properties** dialog box for this new policy.

To add a HTTP traffic filter:

1. Click **Add** to start the Security Rule Wizard and then click **Next**.
2. For **Tunnel Endpoint**, leave the default setting **This rule does not specify a tunnel**, and then click **Next**.
3. For **Network Type**, leave the default setting **All network connections**, and then click **Next**.
4. For **Authentication Method**, leave the default setting **Windows 2000 default (Kerberos V5 protocol)**, and then click **Next**.
5. For **IP Filter List**, select the filter “Permit HTTP Traffic” that you previously created and then click **Next**.
6. For **Filter Action**, select **Permit**, click **Next**, clear the **Edit Properties** check box, and then click **Finish** to complete the wizard.
To add all other traffic filters:

1. The **IIS VLAN Policy Properties** dialog box will still be displayed. Click **Add** to start the Security Rule Wizard, and then click **Next**.

2. For **Tunnel Endpoint**, leave the default setting **This rule does not specify a tunnel**, and then click **Next**.

3. For **Network Type**, leave the default setting **All network connections**, and then click **Next**.

4. For **Authentication Method**, leave the default setting **Windows 2000 default (Kerberos V5 protocol)**, and then click **Next**.

5. For **IP Filter List**, select the filter “**All Other VLAN Traffic**” that was previously created and then click **Next**.

6. For **Filter Action**, select **Block**, click **Next**, clear the **Edit Properties** check box, and then click **Finish** to complete the wizard.

7. Click **Close** to end the policy configuration.
The Internet Data Center environment is a Windows 2000 environment that has no requirement for NetBIOS on the Internet facing interfaces of the IIS and DNS servers in the DMZ. It is important to disable NetBIOS traffic completely on these exposed interfaces because it poses a serious security risk. There are two areas within the network card configuration that require modifying to remove NetBIOS completely from a specific network interface. The first area is to disable NetBIOS over TCP/IP, which prevents the computer listening on NetBIOS ports (137,138,139) on the network interface on which it was disabled. The second area within the network card configuration is to disable “Client for Microsoft Networks” and “File and Printer Sharing,” which will stop the server from listening to TCP port 445 on the interface on which it was disabled. TCP port 445, which is sometimes referred to as Direct Host, uses the Server Message Block (SMB) protocol for sharing files and printers, along with other communication processes between servers. Therefore, intruders cannot determine the security configuration of your perimeter network by responding to NBTSTAT or other NetBIOS queries. The steps necessary to disable NetBIOS completely on the Internet facing interface on all servers in the DMZ are listed below. Perform these steps only if NetBIOS was not disabled using the Post-OS installation steps listed in Chapter 4.

**To disable NetBIOS over TCP/IP from the external network card:**

1. Right-click My Network Places, and then click Properties.
2. Right-click the Local Area Connection for the external network adapter card.
3. Right-click Properties.
4. Click Internet Protocol (TCP/IP), and then click Properties.
5. Click Advanced.
6. On the WINS tab, clear the Enable LMHOSTS lookup check box.
7. Select the Disable NetBIOS over TCP/IP option.
8. To accept changes, click OK until all dialog boxes are closed.
9. When an Empty database message appears, click Yes to continue.

**To disable direct host SMB (TCP Port 445) from advanced network settings:**

1. Right-click My Network Places, and then click Properties.
2. Click the Advanced menu and then select Advanced Settings.
3. Highlight the external network card and clear the check boxes for both File and Printer Sharing for Microsoft Networks and Client for Microsoft Networks.
4. Click OK to close the dialog box.

Repeat these steps for all servers situated in the DMZ.
This section shows how to secure an IIS 5.0 Web server. As a general precaution, always back up your computer configuration before applying new settings. Part of this section disables IIS functionality; you should always check with the customer before disabling functionality. You can reduce the risk of an attack, or limit its potential damage, as follows:

1. Remove default folders that are not required.
2. Disable nonessential IIS services.
4. Disable parent paths.
5. Enable auditing.
6. Install security hot fixes.

**Note** You can also download a free utility called IIS Lockdown from Microsoft’s site which will perform many of the below steps upon installation.

### Removing Nonessential Folders
By default, IIS installs folders with the default Web site that are not required by most applications and can create potential security issues. Remove these folders to further secure the Web site.

**To delete nonessential folders:**

1. To open Internet Information Services Manager, click **Start**, click **Run**, and then type `inetmgr.exe`.
2. Expand the **Computer Name** folder.
3. Expand the folder for the default Web site.
4. Right-click each of the following folders and then click **Delete**:
   - **IISSamples**
   - **IISHelp**
   - **MSADC**
   - **Scripts**

### Disabling Nonessential IIS Services
It is imperative to disable nonessential IIS services to prevent hackers from gaining access to your system. For the Internet Data Center environment, services that are disabled are outlined in the proper security policy.
Removing Script Mapped ISAPI Extensions
The default installation of IIS is designed to enable as much functionality as possible. However, hackers have demonstrated that most people do not change these defaults, which makes their IIS servers vulnerable.

To remove script processor mapped ISAPI extensions:

1. Open the IIS snap-in (Click Start, click Run, and then type inetmgr.exe.).
2. Right-click the default Web site, and click Properties.
3. Click the Home Directory tab, and then click Configuration. The Application Configuration dialog box appears. The Application Configuration dialog box shows the ISAPI DLLs that are mapped to certain file types. You can determine which mappings need to be removed for each feature from the following table:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Remove Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index Server</td>
<td>.ida, .idq, .htw</td>
</tr>
<tr>
<td>Internet Data</td>
<td>.idc</td>
</tr>
<tr>
<td>Connector</td>
<td></td>
</tr>
<tr>
<td>Server-side includes</td>
<td>.shtml, .stm, .shtm</td>
</tr>
<tr>
<td>HTR files</td>
<td>.htr</td>
</tr>
<tr>
<td>Internet printing</td>
<td>.printer</td>
</tr>
</tbody>
</table>

Table 11.1 ISAPI DLL Mappings to Remove

4. For each feature listed in the table, select the mappings for the feature and then click Remove.

Removing the printer mapping does not completely remove printer extensions. This functionality is enabled because of a Group Policy setting. Users can still print from their desktop and server; this only affects printing over HTTP. The steps to take to disable the Group Policy setting completely are as follows:

5. To open the Group Policy snap-in, click Start, click Run, and then type gpedit.msc
6. Click Computer Configuration, click Administrative Templates, and then click Printers.
7. In the right pane, right-click Web-based printing, and then click Properties.
8. On the Policy tab, select the Disabled option.
Disabling WebDAV
Web Distributed Authoring and Versioning (WebDAV) is an extension to the HTTP protocol that allows remote authoring and management of Web content. IIS performs initial processing of all WebDAV requests, and then forwards the appropriate commands to the WebDAV DLL. Because relatively few customers use WebDAV, the easiest and safest strategy is to disable it. You cannot remove WebDAV with a configuration setting or by removing the WebDAV DLL, because it is system-file protected. You must use access control lists (ACLs) to disable WebDAV, which prevents IIS from loading it.

To disable WebDAV:
1. Stop the IIS Web service by typing the following at the command prompt:
   ```plaintext
   net stop iisadmin /y
   ```
2. Deny access to the WebDAV DLL for the group **Everyone**, by typing at the command prompt:
   ```plaintext
   CACLS %windir%\system32\inetsrv\httpext.dll /D Everyone
   ```
3. Start the Web server by typing at the command prompt:
   ```plaintext
   net start w3svc
   ```

Securing IIS Defaults
It is important to secure the following IIS defaults to prevent a hacker from taking advantage of a set of known exploits. In particular, it is important to:

- Limit the ability of hackers to execute command-line tools from the IIS Anonymous Account and IIS Out-of-Process (OOP) Account. When hackers have access to the command line, they can traverse into other folders, such as System32.

- Limit the ability of hackers to overwrite content for the IIS Anonymous Account that enables them to edit customer Web sites at will.

The following procedures show how to secure IIS defaults.

To limit the ability to execute command-line tools, remove permissions for the IIS anonymous account to these tools.
To remove permissions for the IIS anonymous account to execute command-line tools:

1. At the command prompt, execute NET USER to find out the name of the IIS Anonymous Account. The Anonymous Account will show as IUSR_servername, where servername is the name of the computer, and the Out-of-Process Account will show as IWAM_servername.

2. At the command prompt, type the following line to write the appropriate ACLs to all executables in the System32 directory:

   ```
   CACLS %windir%\system32\*.exe /E /D servername \IUSR_servername
   ```

To limit the ability of hackers to overwrite content of a Web site using the IIS Anonymous Account, modify the permissions on the Web root folder.

To place a read-only access control entry on the files in the c:\inetpub\wwwroot folder:

At the command prompt, enter the following CACLS commands:

   ```
   CACLS c:\inetpub\wwwroot\*.* /C /P Administrators:F
   CACLS c:\inetpub\wwwroot\*.* /C /E /G servername \IWAM_servername:R
   ```

Disabling Parent Paths

The parent paths option allows a Uniform Resource Locator (URL) to use “..” in calls to functions. By default, this option is enabled, but it must be disabled.

To disable Parent Paths:

1. Open the Internet Information Services Manager: click Start, click Run, and then type inetmgr.exe.

2. Right-click the default Web site and then click Properties.

3. Click the Home Directory tab.

4. Click the Configuration button.

5. Click the App Options tab.


7. Click OK to close the Application Configuration dialog box. You may be prompted to disable child nodes Parent Paths. Click Select All, and then click OK.

8. Click OK to close the Default Web Site Properties dialog box.
**Enabling Auditing**

Logging is paramount when you want to determine whether your server is being attacked.

**To use the W3C Extended Logging format to determine whether your server is under attack:**

1. Open the Internet Information Services Manager, click **Start**, click **Run**, and then type `inetmgr.exe`.
2. Right-click the default Web site and then click **Properties**.
3. Click the **Web Site** tab.
4. Check the **Enable Logging** check box.
5. Choose **W3C Extended Log File Format** from the **Active Log Format** drop-down list.
6. Click **Properties**.
7. Click the **Extended Properties** tab and then set the following properties:
   - Client IP Address
   - User Name
   - Method
   - URI Stem
   - Win32 Status
   - User Agent
   - Server IP Address
   - Server Port

The latter two properties are useful only if you host multiple Web servers on a single computer. The Win32 Status property is useful for debugging purposes. When you examine the log, look out for error 5, which means access denied. You can find out what other Win32 errors mean by typing `net helpmsg err` on the command line, where `err` is the error number that you are interested in.
Installing Security Hot Fixes
It is essential to stay up to date with all the latest hot fixes. The IIS product team has created the following tools and resources to make it easy for you to install hot fixes and receive notifications of new patches as soon as they are available:

- **QChain.exe.** QChain.exe enables you to install multiple hot fixes with only one restart. This tool is located at:

- **TechNet security Web site.** All IIS security bulletins released after MS01-026 are cumulative, so installing the latest patch gives you all the IIS 5.0 patches with one installation. This is also available for IIS 4.0 patches. Security bulletins are available from:

- **HFCheck.** You can run HFCheck to verify that your servers are up to date with all IIS security patches. It is available from the following Web site:

- **Microsoft Security Notification Service.** You can receive future security bulletins automatically by subscribing to the Microsoft Security Notification Service. To subscribe, go to the following Web page:
This section discusses additional security settings that are applied to all servers in the Internet Data Center Active Directory domain. These settings are not implemented as part of the GPO and must be made manually.

**Restricting Default NTFS Permissions**
Enhancing network security requires additional restrictions to Windows 2000 files and folders. Applying access control lists to files and folders can be automated to some extent by executing a batch job. A template of this batch job is provided in Appendix 11.7. Save this file to your preferred path. This job uses the xcacls program to apply the changes. This xcacls utility, which stands for Extended Change Access Control List, is included in the *Windows 2000 Resource Kit*.

**Caution** Remember that many files and folders receive their permissions through inheritance. Therefore, when you think you are changing only one folder, you may be changing many more.

**To apply the required directory permission settings on each server:**

1. Install the `xcacls` utility and specify the location to be the System32 folder in your root directory.
2. Copy the `acl.cmd` batch file to a directory on the server.
3. Open the command prompt and execute the `acl.cmd` batch job from the directory path used in step 2. This command file changes permission settings for directories (Table 11.2), files (Table 11.3), and programs (Table 11.4):

<table>
<thead>
<tr>
<th>Directories Secured</th>
<th>Permissions Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td>Administrators: Full control</td>
</tr>
<tr>
<td></td>
<td>SYSTEM: Full control</td>
</tr>
<tr>
<td></td>
<td>Users: Read and Execute</td>
</tr>
<tr>
<td>%SystemRoot%\Repair</td>
<td>Administrators: Full control</td>
</tr>
<tr>
<td>%SystemRoot%\Security</td>
<td>SYSTEM: Full control</td>
</tr>
<tr>
<td>%SystemRoot%\Temp</td>
<td>CREATOR OWNER: Full control</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Config</td>
<td>SYSTEM: Full control</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Logfiles</td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%\Inetpub</td>
<td>Administrators: Full control</td>
</tr>
<tr>
<td></td>
<td>SYSTEM: Full control</td>
</tr>
<tr>
<td></td>
<td>Everyone: Read and Execute</td>
</tr>
</tbody>
</table>

Table 11.3 Directory Permission Settings
<table>
<thead>
<tr>
<th>Files Secured</th>
<th>Permissions Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>%SystemDrive%\Boot.ini</td>
<td>Administrators: Full control</td>
</tr>
<tr>
<td>%SystemDrive%\Ntdetect.com</td>
<td>System: Full control</td>
</tr>
<tr>
<td>%SystemDrive%\Ntldr</td>
<td></td>
</tr>
<tr>
<td>%SystemDrive%\Io.sys</td>
<td></td>
</tr>
<tr>
<td>%SystemDrive%\Autoexec.bat</td>
<td>Administrators: Full control</td>
</tr>
<tr>
<td>%SystemDrive%\Config.sys</td>
<td>System: Full control</td>
</tr>
<tr>
<td></td>
<td>Users: Read and Execute</td>
</tr>
</tbody>
</table>

**Table 11.4 Permissions to be Applied to Files Under Root Directory**

The following list shows the programs that can be run from a command prompt. The NTFS permissions are modified by `acl.cmd` so only users that belong to the administrators group can execute them.

<table>
<thead>
<tr>
<th>Programs Secured</th>
<th>Programs Secured</th>
</tr>
</thead>
<tbody>
<tr>
<td>%SystemRoot%\system32\Append.exe</td>
<td>%SystemRoot%\system32\Regedt32.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\At.exe</td>
<td>%SystemRoot%\system32\Regini.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Attrib.exe</td>
<td>%SystemRoot%\system32\Regsvr32.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Cacls.exe</td>
<td>%SystemRoot%\system32\Rexec.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Cmd.exe</td>
<td>%SystemRoot%\system32\Route.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Command.com</td>
<td>%SystemRoot%\system32\Routemon.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Cscript.exe</td>
<td>%SystemRoot%\system32\Router.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Debug.exe</td>
<td>%SystemRoot%\system32\Rsh.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Exe2bin.exe</td>
<td>%SystemRoot%\system32\Runas.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Finger.exe</td>
<td>%SystemRoot%\system32\Runonce.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Ftp.exe</td>
<td>%SystemRoot%\system32\Secedit.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Hostname.exe</td>
<td>%SystemRoot%\system32\Share.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Immc.exe</td>
<td>%SystemRoot%\system32\Telnet.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Ipconfig.exe</td>
<td>%SystemRoot%\system32\Termsrv.exe</td>
</tr>
<tr>
<td>%SystemRoot%\system32\Mmc.exe</td>
<td></td>
</tr>
</tbody>
</table>
Securing the Administrator Account on Member Servers

Apply the following changes to the Administrator account to all member servers in the domain.

1. Rename the Administrator account on each member server. Do not use the same name for the account for all member servers. Use different names to reference the Administrator account, such as IISAdmin for the IIS servers or SQLAdmin for the servers running SQL Server. Set a strong password of at least 15 characters for this account.

2. Create a fake Administrator account that has no rights. After creating the account, remove any memberships to global groups to which it belongs by default. In addition, give this account a very strong password of at least 15 characters using a combination of special characters, upper and lower case characters, and numbers.
Securing the Administrator Account on Domain Controllers
Before renaming the Administrator account, as a precaution, copy the Administrator account assigning it a new name. This will copy all the permissions associated with the default administrator account and will provide a backup of it. Now, rename the original Administrator account assigning it a new name that does not have “admin” as part of the name. Make sure that the Full Name and User Logon Name fields match the new assigned name and remove the default description. Give the copied Administrator and renamed Administrator accounts a strong password of at least 15 characters using a combination of special characters, upper and lower case characters, and numbers.

Service Accounts
Windows 2000 services typically run under the Local System account, but they can also be configured to run under a domain user account. Local accounts should be used whenever possible in preference to domain user accounts for both domain controllers and servers. If a domain user account is used and shared between domain controllers services and servers services a single compromised account on a server could also be used to compromise the domain controller.

If a domain user account is required for a application service that runs on both servers and domain controllers then a domain user account should be assigned to the service on the servers and a different domain user account should be assigned to the service on the domain controllers.
This section describes issues and recommendations for a production perimeter network.

- Remember, whenever changes are made to a GPO, or computers are moved between organizational units, or a security ACL is applied to an Active Directory object, these changes should be made on a single domain controller and then let Active Directory replication apply the changes to the other domain controller.
- If you are having problems downloading a policy to a member server or you are unable to view the Group Policy Objects on the domain controllers, verify that the “TCP/IP NetBIOS Helper” service is running and not disabled on the domain controllers and the member servers.
- If the print spooler is disabled, the Windows Management Interface (WMI) may produce an Event ID 36 or 37 error message in the application Event Log. To correct this error message, disable the performance counters for the spooler service in the registry. Create the REG_DWORD name `Disable Performance Counters`. Assign it a value of 1 and place it in the following registry location:

```
HKLM\System\CurrentControlSet\Services\Spooler\Performance\`
```
- Auditing for the domain controllers must be configured in the domain controller security template and applied to the domain controller policy. The domain policy will not override the auditing and, therefore, must be implemented in the domain controller policy.
- If you are experiencing problems with IPSec policies that have been assigned to the IIS Servers and you need to disable their functionality, you can disable the policy without affecting the security that has been applied to the server using the security templates. You go into the policy and change the Policy Assigned value to `No`. You must then reapply the policy to the server using the `secedit` command.
- If you disable NetBIOS completely on all the network adapters for the server, the following Event Log errors may occur:
  - SMTPSVC, W3SVC, FTPSVC, LDAPSVC EventID 105 means that the server was unable to register the administrator tool discovery information. If this error occurs, the administrator tool may not be able to see the server. See Microsoft Knowledge Base article Q254525 for details.
  - On the domain controller, EventID 5781 – Netlogon failure – Dynamic registration or deregistration of one or more DNS records failed, because no DNS servers are available. This happens when the domain controller is restarted, and the DNS server service has not yet started while the NETLOGON service has. See Microsoft Knowledge Base article Q259277 for details.
Security is a very important aspect of any e-commerce network. The Internet Data Center architecture provides high-level security by implementing various security policies. These policies are applied and tested before any part of the system is exposed to the Internet. It is also important to review their effectiveness continually. You must not consider security as a “set and forget” configuration. New hacker and system defense techniques are being developed all the time. Therefore, it is important to keep your security policies under review to ensure your system stays secure.

Now that you have seen and understood the type of security issues facing the Internet Data Center architecture, integrating the Strategic Technology Protection Program components will help to ensure that your implementation of this infrastructure is kept up to date with the latest security configurations.

**Additional Information**

For information on the Strategic Technology Protection Program and general Windows 2000 Security information, refer to the following Microsoft Web sites:


For more information on Windows 2000 Group Policy and troubleshooting, refer to the following Microsoft Web sites:

This section provides details of the appendix files that are provided as part of the Internet Data Center architecture documentation

Appendix 11.1 – Security Template for DMZ Servers
This appendix provides an example of a security template designed to apply security settings to all servers on the Internet Data Center DMZ network. A security template has been created called IDCDMZ.inf, this appendix file contains example settings that can be used for your deployment project. This template must be copied to the %systemroot%\Security\Templates folder on both domain controllers and must then be applied to the following organizational units:

- IIS Servers
- External DNS Servers

Appendix 11.2 – Security Template for Management Servers
This appendix provides an example of a security template designed to apply security settings to all servers in the Management Servers organizational unit. The IDCManagement.inf appendix file contains example settings that can be used for your deployment project. This template must be copied to the %systemroot%\Security\Templates folder on both domain controllers and must then be applied to the Management Servers organizational unit.

Appendix 11.3 – Security Template for SQL Server
This appendix provides an example of a security template designed to apply security settings to all servers in the SQL Server organizational unit. The IDCSQL.inf appendix file contains example settings that can be used for your deployment project. This template must be copied to the %systemroot%\Security\Templates folder on both domain controllers and must then be applied to the SQL Servers organizational unit.

Appendix 11.4 – Security Template for Domain Controllers
This appendix provides an example of a security template designed to apply security settings to all servers in the Domain Controllers organizational unit. The IDCDC.inf appendix file contains example settings that can be used for your deployment project. This template must be copied to the %systemroot%\Security\Templates folder on both domain controllers and must then be applied to the Domain Controllers organizational unit.

Appendix 11.5 – Security Template for the Domain
This appendix provides an example of a security template designed to
apply security settings to all servers in the Domain. The IDCDomain.inf appendix file contains example settings that can be used for your deployment project. This template must be copied to the %systemroot%\Security\Templates folder on both domain controllers and must then be applied to the Domain.

**Appendix 11.6 – Enhanced File Security Batch File**
This appendix is a batch file that will enhance security by applying additional restrictions to Windows 2000 files and folders. The template batch file called acl.cmd should be saved to your preferred path and checked before it is executed. This file requires the xcacls program, which is included in the Windows 2000 Resource Kit.