# Global Information Assurance Certification Paper

# Capitol SANS Practical

**By Alan McClelland**
**Lucent Technologies**

# Securing Windows 2000 on the Internet

# Securing Windows 2000 running IIS5

This paper will explain how to secure a Windows 2000 server running IIS 5 on the Internet. There will be four sections to this document: System location, Installing Windows 2000, Securing 2000 Server and Securing IIS 5. There are many other products that can also be installed onto a Windows 2000 server accessible from the Internet, which are outside the scope of this document.

**System Location:**

The first step in securing your system is to allow the traffic that your system requires and restrict all other traffic. It is recommended that the Windows 2000 servers be installed into a DMZ (Demilitarized Zone) or a specially designed Web hosting center.

A DMZ as defined by http://whatis.techtarget.com

In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. (The term comes from the geographic buffer zone that was set up between North Korea and South Korea following the war in the early 1950s.) A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.
In a typical DMZ configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests on the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested. Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages so these could be served to the outside world. However, the DMZ provides access to no other company data. In the event that an outside user penetrated the DMZ host's security, the Web pages might be corrupted but no other company information would be exposed. Cisco, the leading maker of router, is one company that sells products designed for setting up a DMZ.

A typical DMZ configuration is shown in Figure 1.1

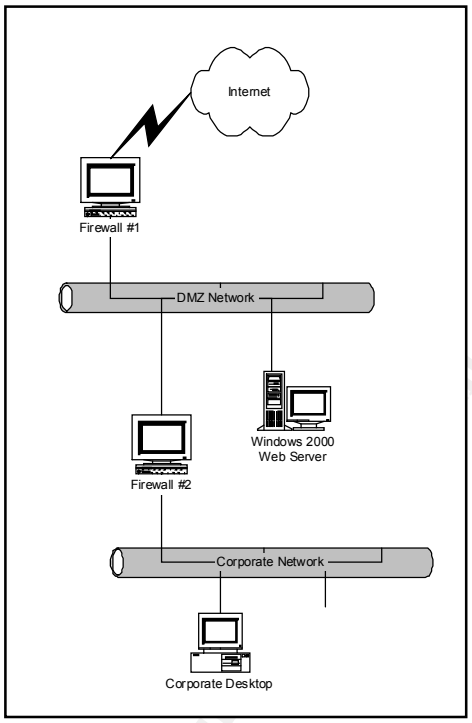



Figure 1.1

This DMZ configuration could also be accomplished with one Firewall that has multiple network interfaces in it; however, this is less secure because only one box would need to be compromised for full access to the corporate network.

This network configuration allows traffic from the Internet to get to the Windows 2000 Web Server's through Firewall #1 but this inbound traffic will be filtered at Firewall #2. A good rule of thumb is to setup both firewalls to deny all traffic and then open only the specific ports that are needed. For example: configure the Firewall #1 to allow port 80 (HTTP) and then deny anything else for inbound traffic. If other ports are needed then these could be opened individually. Firewall #2 should then be configured to allow only the corporate IP address through to the Internet and the DMZ on the specific ports needed. Of course for this to allow traffic from the Corporate network to the Internet then Firewall #1 would then need to be configured to allow the corporate IP addresses through as well. Firewall #1 should be set up as state-aware firewall that will keep track of the corporate connection that traverse through it and allow a response back automatically. This automatic state-aware configuration should only be configured for corporate traffic coming from the corporate LAN.

If cost is an issue then two routers with ACL's (Access Control Lists) applied can be configured to provide security similar to the same configuration as the two firewalls. A router configured in this manner is referred to as a Choke Router. This configuration is not as manageable as the firewalls.

Most corporate run Hosting Centers have either choke routers or firewalls isolating their networks from the Internet and you as a customer can request specific access control lists for your servers. If you are deciding on a Hosting Center to host your server then make

sure they have either a choke router or firewall. It is important to check the hosting center's policy on the internal network ACL's so that your system is protected from another customer's system located with in the same hosting center. This security is often overlooked.

When it comes to the location of the servers in relation to the Internet it is important to isolate them as much as possible from your corporate users and regulate the type of traffic getting to your system. Using a DMZ or Hosting Center solution will provide this isolation with minimal impact to both your corporate users and customers from the Internet. No matter which solution you decide on it is recommended that you allow only specific ports and deny all others.

**Installation of Windows 2000 Server**

After deciding on the location the server can then be loaded. It is recommended that the server be disconnected from the Internet before starting the installation. This is important to keep people from exploiting the server before it has been secured. You can load this server while connected to your corporate network but make sure that it is not Internet accessible. Since this server will be a web server then it is recommended that it be striped down to support only web hosting. We will install only applications that are needed to run the web server.

Simple outline of the installation process is:

1) Install the server with a minimal configuration.
2) Install the Service Pack & Hotfixes
3) Install the applications needed for the server.
4) Re-Install the Service Packs & Hotfixes

Each of these install processes will be explained in more detail.

*Installing with Minimal installation:*

Start with a clean system making sure all old operating systems are cleaned off. Install the OS with the minimal configuration and do not install any other applications during the install phase. Applications should be added later but since Internet Information Server 5.0(IIS) is integrated with the 2000 install it should be installed at this time with the OS. Do not create a dual boot with any other OS. Install the operation system to a NTFS partition only and do not create any FAT partitions. NTFS will be needed later when we make changes to the file permissions.

At the Windows 2000 components, deselect all except for Internet Information Server (IIS). Select IIS and click on Details the select only the following components: Common Files, Documentation, Internet Information Server Snap-in and WorldWide Web Server: As shown in the figure 2-1. If FTP is going to be used it to can be selected however for the rest of this document it will not be discussed.

TCP/IP and "Client for Microsoft Networks" should be installed. This can be accomplished by clicking on Custom Settings and checking only the two required services. To make this server more secure it is recommended to unbind "Client for Microsoft Networks" from all interfaces. "Client for Microsoft Networks" is needed for IIS to function but doesn't need to be bound to any interface. Delete File & Printer sharing for Microsoft Networks. Do not install any other protocol because they can't be used on the Internet any way. Disable NetBIOS over TCP/IP from the TCP/IP properties dialog box. Other network services will not be needed and should not be installed. These services include DNS, WINS, DHCP, TCP/IP Printing, etc.

This server should be setup as a stand-a-lone server and not participate in a Domain. This will keep the Corporate Domain separate from the server in the DMZ incase the server in the DMZ is compromised.

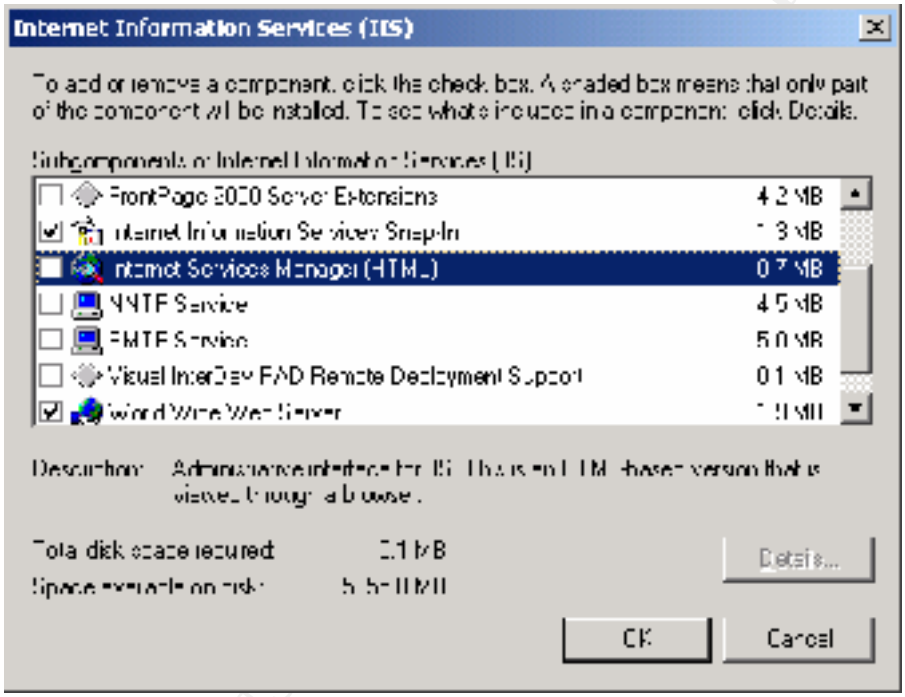


Figure 2-1

*Installing Service Pack & Hotfixes:*

The Service Pack(SP) should be installed at this point because some applications require a specific level of a Service Pack before they can be installed. It is recommended to download the latest service pack from http://www.microsoft.com/windows2000/downloads/default.asp. Always install the latest version that has been tested in a Lab or on a Quality Control server. Test these Service Packs on a mirror image of your production server to get an accurate test. After installing the Service Pack reboot the server.

Hotfixes are intermediate patches between Service Packs that Microsoft publishes. Of course only apply the Hotfixes that are needed for the system. For example if there is a Hotfix that patches DNS then this is not needed on the server because DNS is not installed. Installing a Hotfix for a system that doesn't need it would just put critical files on that server that could be used for an exploit. Hotfixes can be found at http://www.microsoft.com/windows2000/downloads/default.asp. It is important to install Hotfixes in the correct order because one Hotfix could over write a file from another Hotfix. This can be done by looking at the Hotfix web site and checking when the Hotfix was released. After noting the release dates of the Hotfixes start installing them latest to earliest. This is the safest way to install Hotfixes.

There is also another feature of Windows 2000 called Windows Update. This is on the Start Menu and will check with Microsoft's Web site for the latest patches or fixes automatically. This could be used after you apply all the SP & Hotfixes to check if the system is up to date. Shown in figure 2-2 is an example of the website for the Windows Update feature.

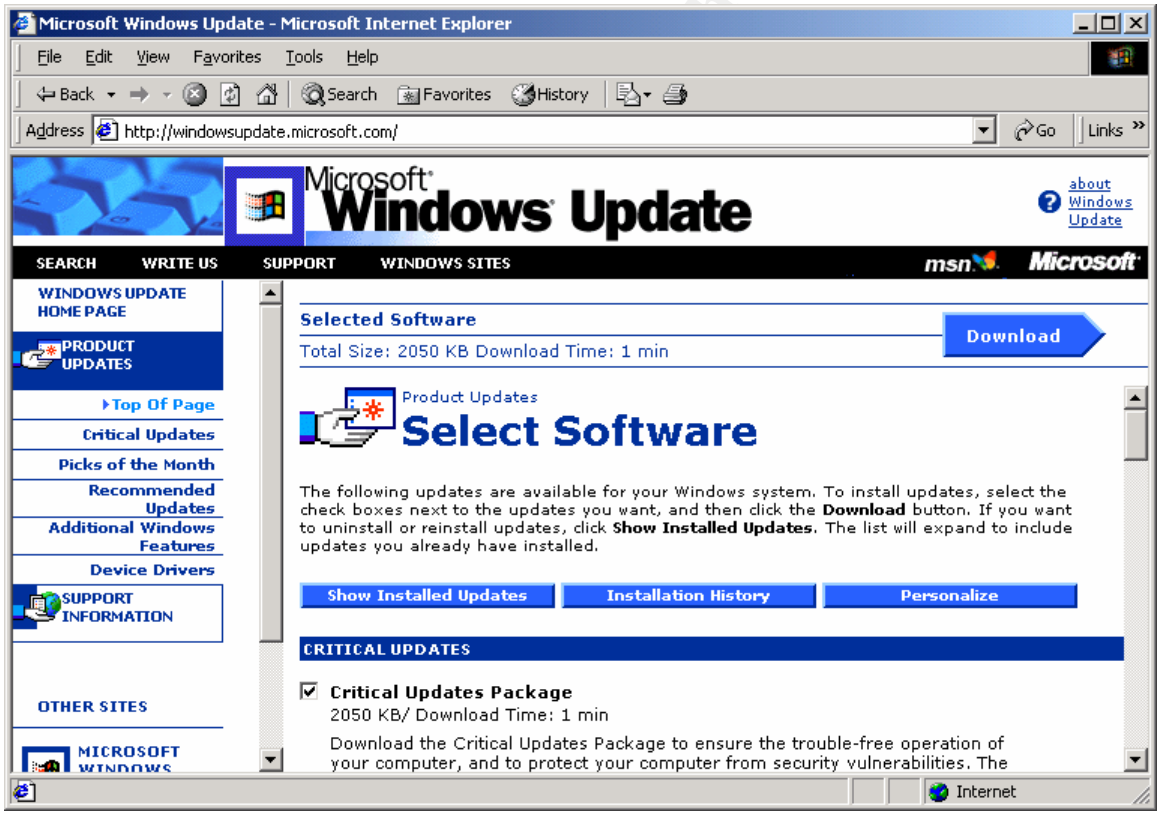


Figure 2-2

*Installing Applications:*

Since the server that this document covers will be a Web server then this section will discuss the installation of Internet Information Server (IIS). Since the IIS 5.0 install for Windows 2000 comes on the default CD then this was installed during the OS install. If another application is to be installed then it would be installed at this point. Install the

applications selecting only the needed options. Do not perform a FULL install for an application because this will install executable that will not be used.

*Re-installing the Service Packs & Hotfixes:*

It is recommended to reinstall the Service Packs(SP) and any Hotfixes after any applications have been installed. The reason that this needs to be done is because the SPs fix application problems along with OS problems. If you install an application after applying a SP then it might over write a file that the SP could have installed. It is also possible for the SP not to upgrade a file because the application was not on the system during the SP install. Any time in the future that an application is installed or files are copied from the original Windows 2000 CD then the SP should be re-applied. This is usually overlooked and can cause problems or security issues.

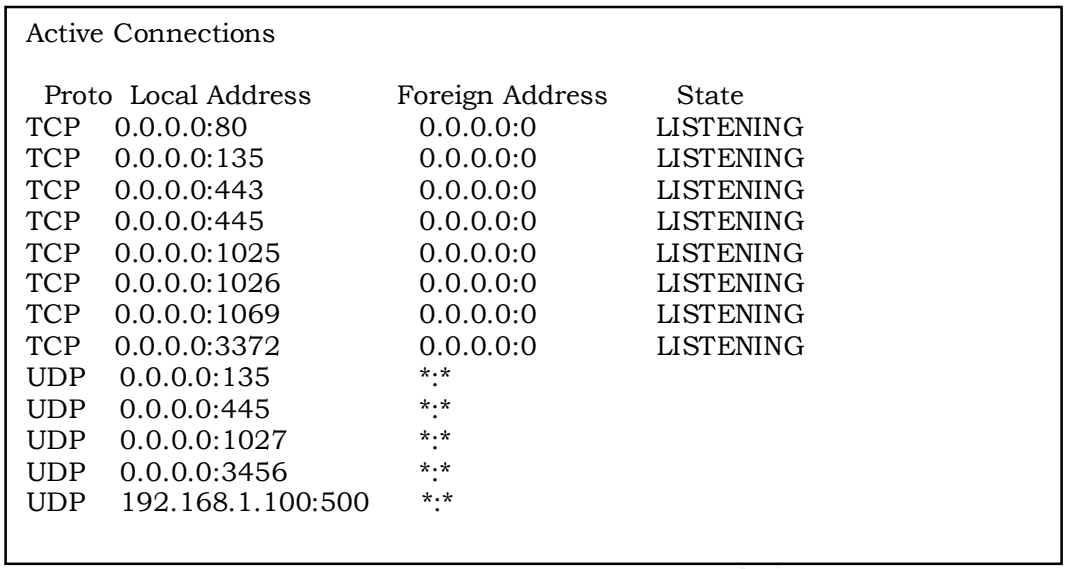
Hotfixes should also be re-applied after the applications have been installed. Hotfixes must always be reapplied after the Service Packs because they are post Service Pack patches. Check Microsoft's web site to make sure there are no Hotfixes for the application that was just applied. If there are Hotfixes for that application then apply these as well. Of course apply the patches earliest to latest based on release date.

**Securing 2000 Server:**

Topics that will be covered in this section include Services & Programs, Traffic filtering, File Permissions and Security Policies. We will discuss each topic in the next four sections. Making these changes will secure our base install of 2000 from the previous section.

*Removing or Disabling Services & Programs:*

The figure 3-1 shows the default ports that are open on this machines to this point. This section will explain how to tighten this server even more by removing unwanted ports.



Active Connections

| Proto | Local Address | Foreign Address | State |
|---|---|---|---|
| TCP | 0.0.0.0:80 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:135 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:443 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:445 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:1025 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:1026 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:1069 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:3372 | 0.0.0.0:0 | LISTENING |
| UDP | 0.0.0.0:135 | *:* | |
| UDP | 0.0.0.0:445 | *:* | |
| UDP | 0.0.0.0:1027 | *:* | |
| UDP | 0.0.0.0:3456 | *:* | |
| UDP | 192.168.1.100:500 | *:* | |

Figure 3-1 (Default ports figure)

Here is a break down of these ports:

:80 HTTP Web Server
:135 RPC Port
:443 SSL Port
:445 Direct Host (Replaces 139)
:1025, 1026 RPC Listener ports (Opened by RPC)
:1069 Distributed Transaction Coordinator
:3372 Distributed Transaction Coordinator
UDP:135 Messenger Service
UDP:445 Direct Host
UDP:1027 Messenger Service
UDP:3456 IIS Port
UDP:500 IPSec (IKE)

RPC opens 3 ports for it's operations it would be good if we could disable this service however IIS requires RPC to function and it RPC is not running IIS will not start. The way RPC works is by opening ports in order from 1025 and depending on when the service start determines which port get assigned to that service. So your ports might not match these exactly. We can clean up a few of the other ports by removing some unused services. The figure 3-2 shows the default services that the 2000 system installed by default:

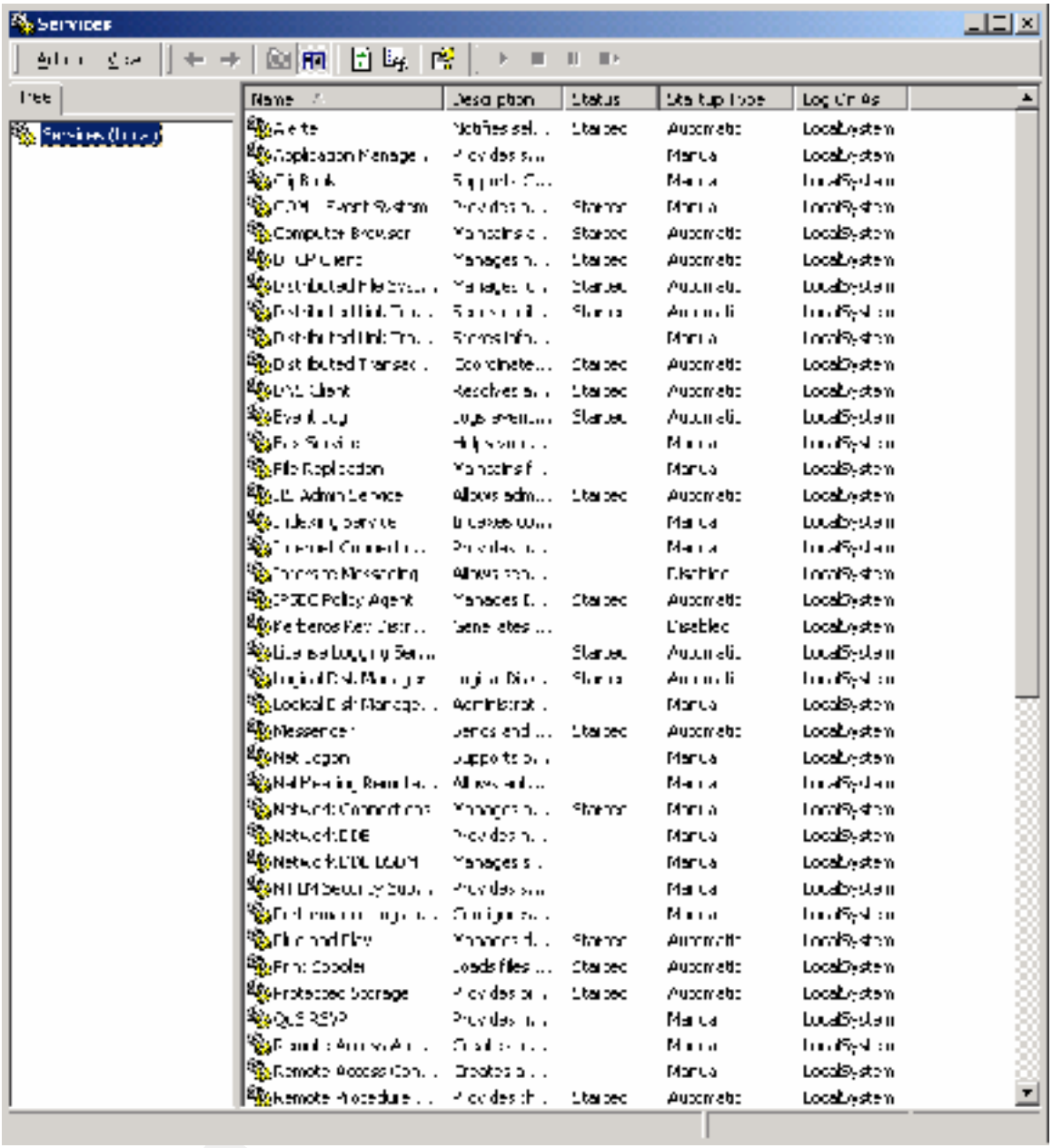


Figure 3-2 (Default Services)

Even a default system with no Windows components except for IIS has a lot of services running. In fact there were so many running that this figure is not complete. The follow lists the services that should be set to automatic start.

DNS Client
Event Log
IIS Admin Service
IPSEC Policy agent
Logical Disk Manager
Plug & Play

Protected Storage
Remote Procedure Calls (RPC)
RunAs Service
Security Account Management
System Events Notifications
Task Scheduler
Windows Management Instrumentation
World Wide Web Publishing

All the rest of the services should be set to Manual Start.

So your services should look something like the figure 3-3

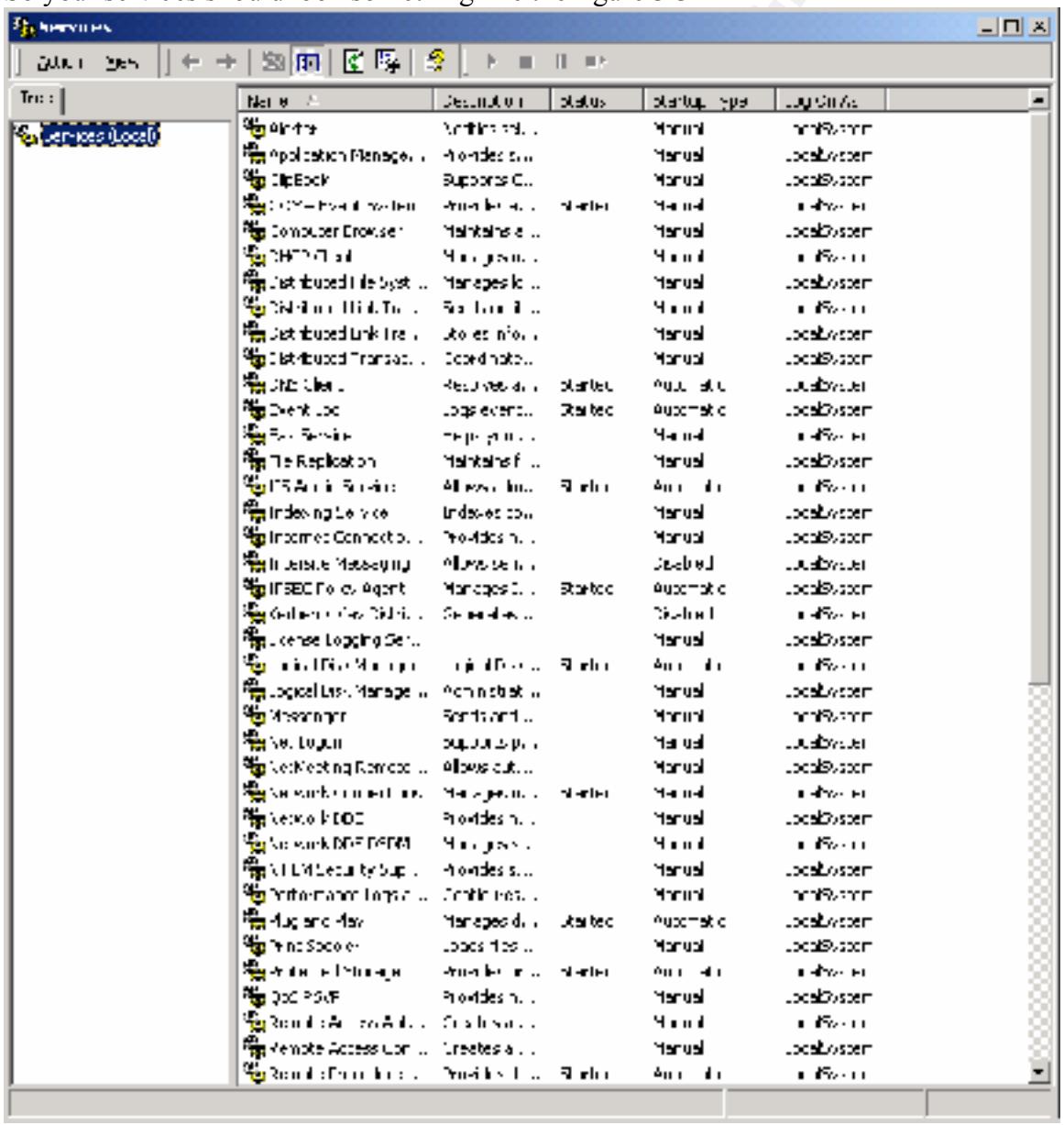


Figure 3-3 (New Service Settings)

Of course this is an incomplete list because of size limitations.

After these services have been disabled. Reboot the system. Figure 3-4 below is a list of the ports open after disabling these services.

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:80           127.0.0.1:1037         TIME_WAIT
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:3456           *:*
  UDP    192.168.1.99:500       *:*
```

Figure 3-4 (Ports open after disabling ports)

As you can see this removed 3 ports from the open list. Two of the ports are for the web server and we can't disable them because then our customers won't be able to access our server. However we still have the pesky RPC ports, in fact we have 6 of them and disabling RPC will kill our IIS server. The :500 port is our IPSEC which we will discuss later. This secures the ports as well as we can get it on the system but we can protect these open ports by using a port filter.

*Traffic Filtering*

There are three port filters built into Windows 2000, TCP/IP Filtering, IPSEC, and RRAS. It is recommended to use TCP/IP Filtering but if more security is needed then use IPSEC. It is not recommended to use RRAS because it requires the Workstation and Server service, which we want disabled and did so in the last section. The next two sections will explain how to filter ports using TCP/IP filtering and then using IPSEC filtering. Which filtering program to use will be based on what requirement are needed. IPSEC is more configurable but TCP/IP Filtering is more easier to use.

TCP/IP Filtering

TCP/IP filtering is only an inbound filter and should not be substituted for a firewall. To configure TCP/IP filtering go to the Network application in the Control Panel under Network and Dial-up Connections under Local Area Connection (name of the network connection) Properties under TCP/IP under Advanced under Options under TCP/IP Filtering.

In every situation all ports that are not need should be blocked. For our example we will block everything except for port 80, port 443 on TCP. In some situation ICMP might also be left open. All UDP ports will be blocked. This is shown in Figure 3-5 below. This should not be used in place of a firewall but used to supplement a firewall's security.

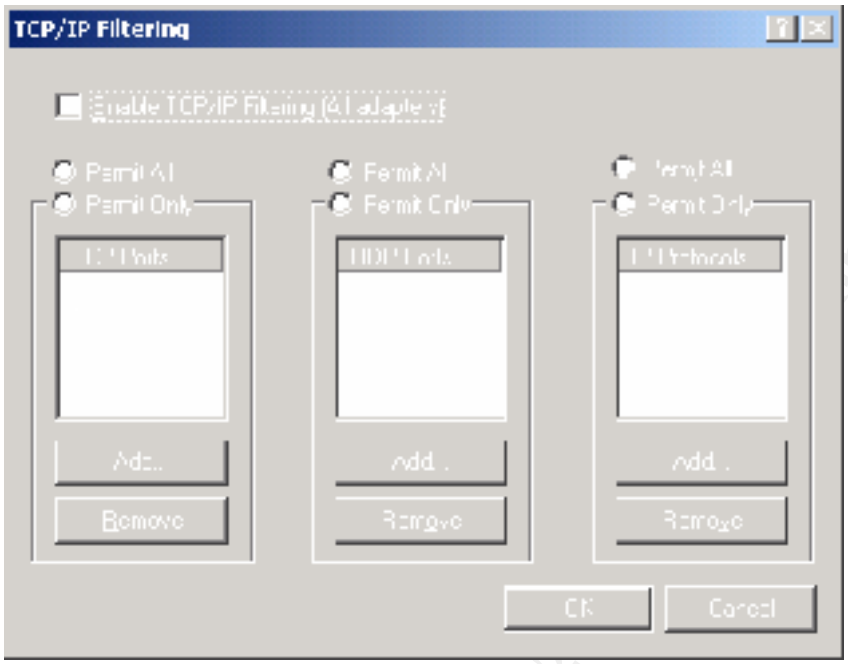


Figure 3-4 (TCP Filter Ports)

IPSEC

IPSEC does more then just filter IP ports it also supports secure communications between machines using encryption. This type of configuration can be used to require encryption from a Web server to a Database server. Using IPSEC this can be configured to require the encryption otherwise the connection will fail. IPSEC is more configurable and robust then TCP/IP. If planning to manage this server from another machine located in your corporate network then it is recommended to set this up using IPSEC secure communications requiring encryption.

This document will cover filtering only and not encryption. IPSEC is configured by using Microsoft Management Console.

The IPSEC filters match on one or more of the following properties:

- Source Address
- TCP/UDP Source Port
- Destination Address
- TCP/UDP Destination Port
- IP Protocol Number

Remember in TCP/IP filters we could only filter on Destination Port (or Inbound). In IPSEC you can filter traffic Inbound and Outbound.

Both IPSEC filter and TCP/IP filter can be used together but it is recommended to settle on one or the other.

There are default rules on the server that allow any client on any port on any protocol in to any IP on this server. Not to secure. We will remove this rule and specify only the ports that we will need.

There is another rule defined by default that allows ICMP protocol access to this server. We will remove this rule also.

To create a new filter follow the steps

1) Open the Local Security Policy MMC snap-in from the Administrative Tools menu.
2) Click on IP Security Policies on Local Machine.
3) Remove the three default policies located in the right panel as showing in Figure 3-5.

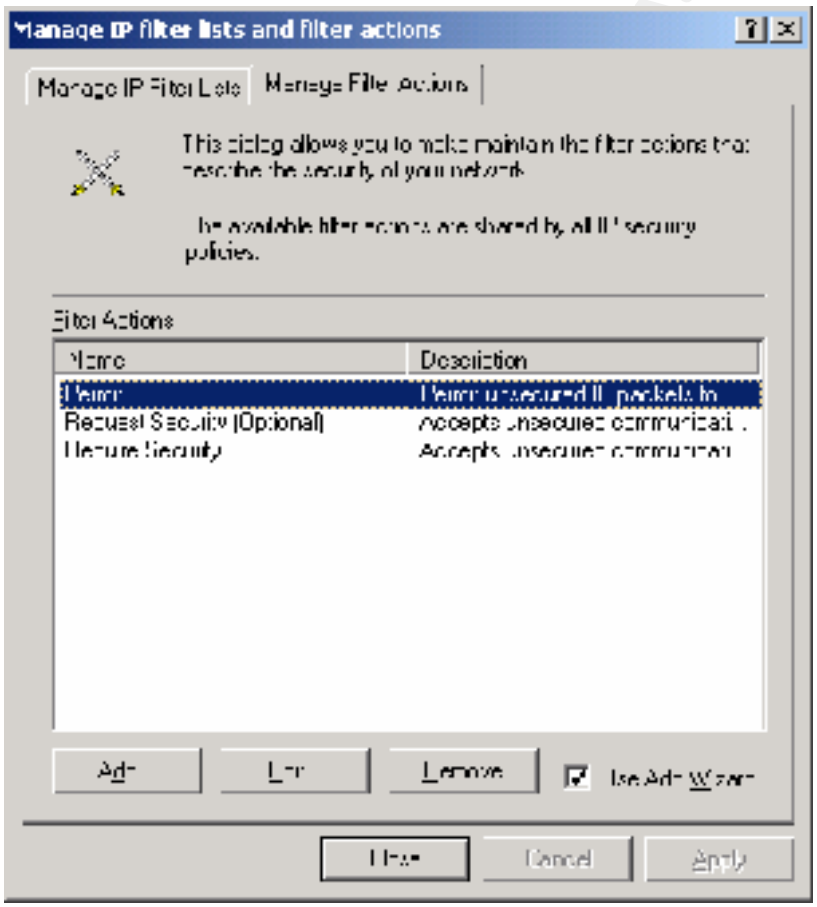


Figure 3-5

4) Right-click in the right pane and choose “Manage IP filter lists and filter actions” Remove the default filter lists and filter actions.
5) There will be two filter actions defined one called Block and one called Permit. It is recommended not to use the Wizard. After selecting Permit click on the General tab and enter Permit in the Name field. Repeat this for the Block Action also. As shown in Figure 3-6.

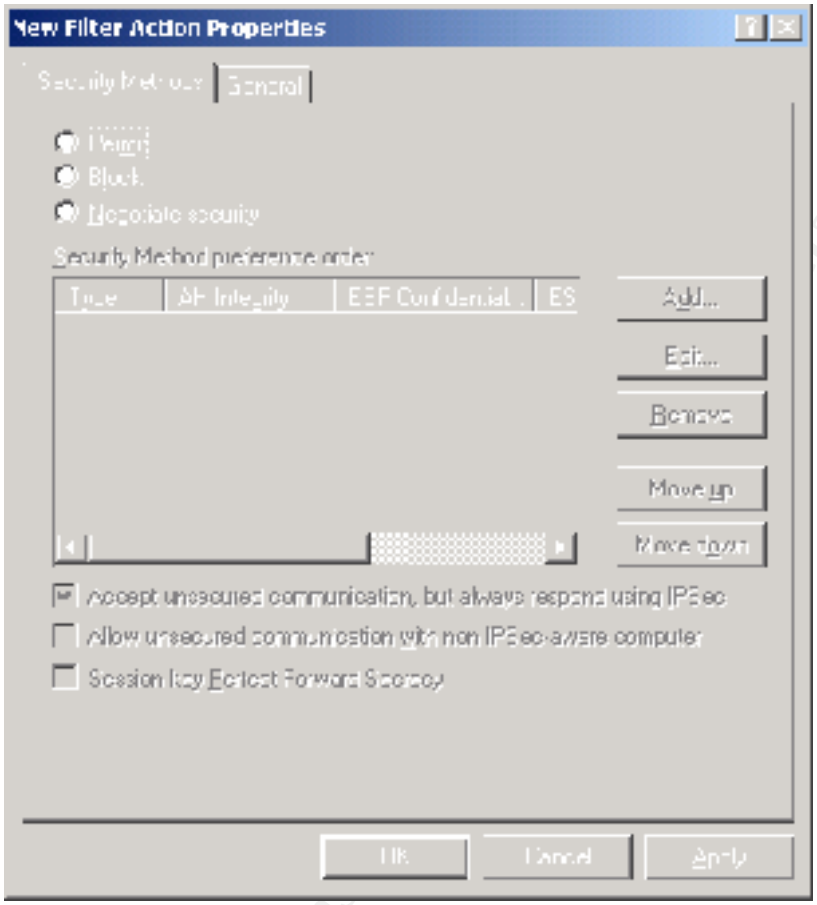


Figure 3-6

6) Create an IP filter list (Again don’t use the Wizard) called “all” that has the default settings which will match all traffic. Just take the defaults for the configuration.
7) Create an IP filter list (again don’t use the Wizard) called “Web server” that follows the list below for ports and IP address access.

| FILTER #1 | |
|---|---|
| Source Address | Any IP Address |
| Destination Address | My IP Address |
| Mirrored | Yes |
| Protocol | TCP |
| From Port | Any |
| To Port | 80 |

| FILTER #2 | |
|---|---|
| Source Address | Any IP Address |
| Destination Address | My IP Address |
| Mirrored | Yes |
| Protocol | TCP |
| From Port | Any |
| To Port | 443 |

OK lets explain what this does because more might be needed depending on the servers role.

The "Source Address" is the IP address of the source packet. IE: a machine on the Internet. "Destination Address" is the IP address of the web server. This is after all the machine we want to protect. This is configured as "My IP Address". This make changing an IP address on a server much easier if needed. "Mirrored" is yes because we want this rule to allow traffic back out the way it came in. If we don't set the mirror to yes then we will only be able to receive the request and nothing will go back out. "Protocol" is the protocol of the packet. In our case it is TCP. "From Port" is set to any. This is because some machines will random the "From port" for web access. The "To Port" is set to 80 and 443 in these rules. This is relatively straightforward.

8) Create a new IPSEC policy called "Web Server" No not activate the default response rule.
9) To create a default-deny rule for then system called "Any" and use the "All" Filter that was created in the previous step and use the Block Filter Action on it. This will block everything.
10) Of course you don't want to block everything but that is the best place to start. Now create a rule called "Web Access" and use the "Web Server" filter with the Permit Filter Action on it. Just like it shows in Figure 3-7.

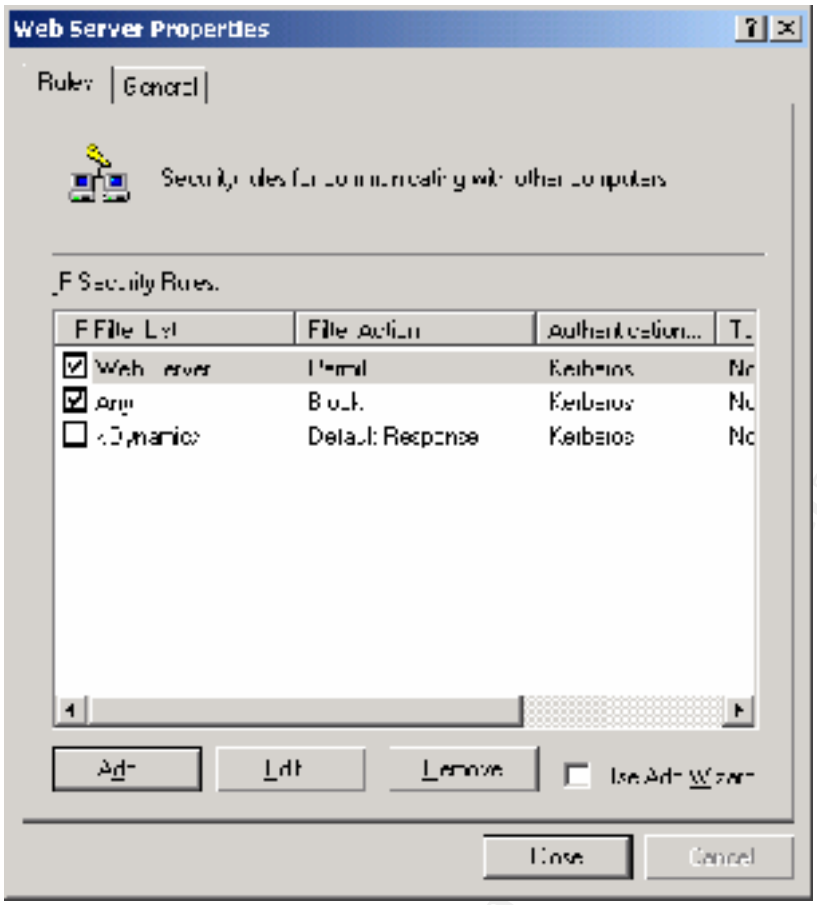


Figure 3-7

11) Apply the policy by right clicking on the policy and choosing Apply.
12) Test the policy.

When you complete the steps up to this point then the system from the Internet will only have two ports open: Port 80 and Port 443. This makes your system secure from the network standpoint however the system should also have file access control lists (FACL) and Security Policy's installed incase there is a bug or other problem that would give someone access by mistake. The next two sections will discuss these two steps.

*File Permissions*

ACLs are permissions assigned to the individual files. We will discuss just a few key practices for ACLs because this topic is a complete paper by itself.

The default permissions on a freshly installed machine are as follow:

Root of C Drive Everyone has Full rights.
Remove Everyone and add Administrators Group/Power Users Group/Backup Users Group – Full. Add the IUSR-SystemName (Web Anonymous) user with Read and

execute rights to c:/Inetpub because removing everyone from the root of the C Drive renders the web server usless. As shown in the Figure 3-8.

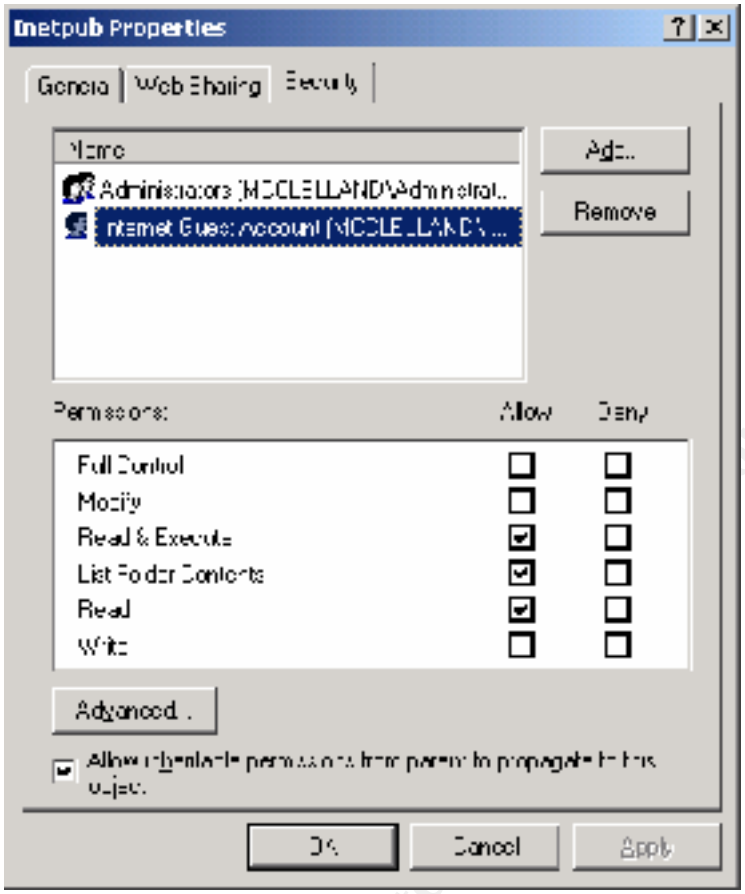


Figure 3-8

C:\WINNT Everyone has Read & Execute/Users group has Read & Execute
Remove Everyone
C:\WINNT\SYSTEM32 Everyone has Read & Execute/Users group has Read & Execute. Remove Everyone

Another key folder is the C:\Windows\Repair folder should only have Administrator group assigned to it and no one else.

This will secure the critical components of the operating system from the Everyone group. FACLs need to be changed and tested on a case by case basis but the above changes are a good starting point.

*Security Policies*

Windows 2000 has a good built in Security configuration editor that can be used to secure a system with very little effort. These are predefined policies that are applied

simply by loading them into the system. Microsoft has supplied predefined policies in several different configurations below is a list of these and a brief descriptions of them. There are 100's of setting that each of these change which it too many to list here but these can be viewed and changed after these policies are loaded. These default settings can also be modified before applying and saved for use later.

Security Policies:

- Basicwk.inf – For computers running Windows 2000 Professional
- Basicsv.inf – For computers running Windows 2000 Server
- Basicdc.inf – For domain controllers running Windows 2000 Server
- Compatws.inf – For Workstations and Servers to allow users to run more applications without being power users.
- Securews.inf – Provides a secure configuration for Workstations & Servers
- Securedc.inf – Provides a secure configuration for Domain Controllers
- Hisecws.inf – For Workstations and Servers for High Security
- Hisecdc.inf – For Domain controllers for High Security

To load up the Configuration Editor click on Local Security Policy from the Administrator Tools menu. If IPSEC was setup before this dialog box might look familiar as shown in Figure 3-8. Anything that is loaded using the Local Security Policy will not affect what was previously done in the IP Security Policy.

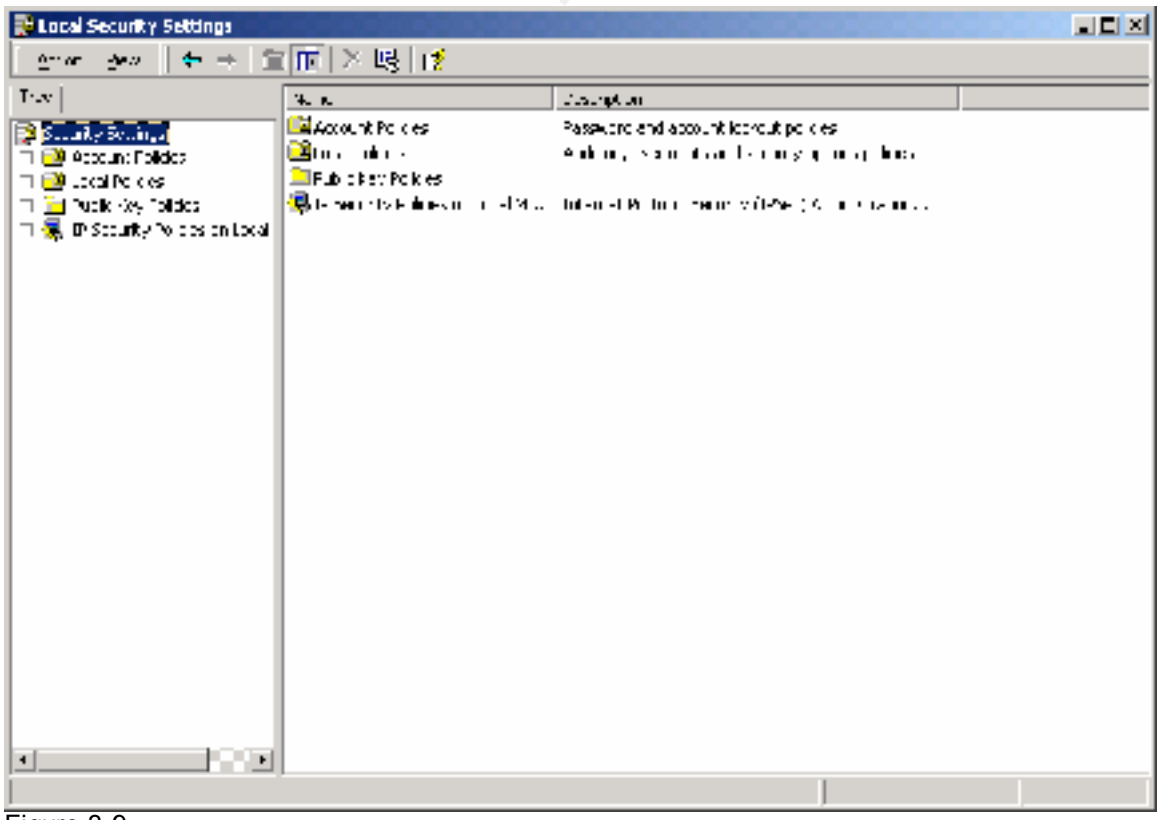


Figure 3-9

There are four policies that can be modified here. Account Policies, Local Policies, Public Key Policies and IP Security which we have already discussed. We will not discuss Public Key Policies.

Account policies control the passwords and account lockout policies. These can be used to set the limitations on the user accounts.

Local Policies are used to setup Auditing, User rights and security options.

Public Key Policies place restrictions on Certificate Keys.

To load up the policies click on Security Settings and then Click on Action. Click on Import Policy. There will be a list of the available policies on this system.

Click on HISECWS and click Open. This will install and apply the HISECWS policies. Shown in Figure 3-10 is the new policy for the Password Policy. You can see the restrictions on the accounts.

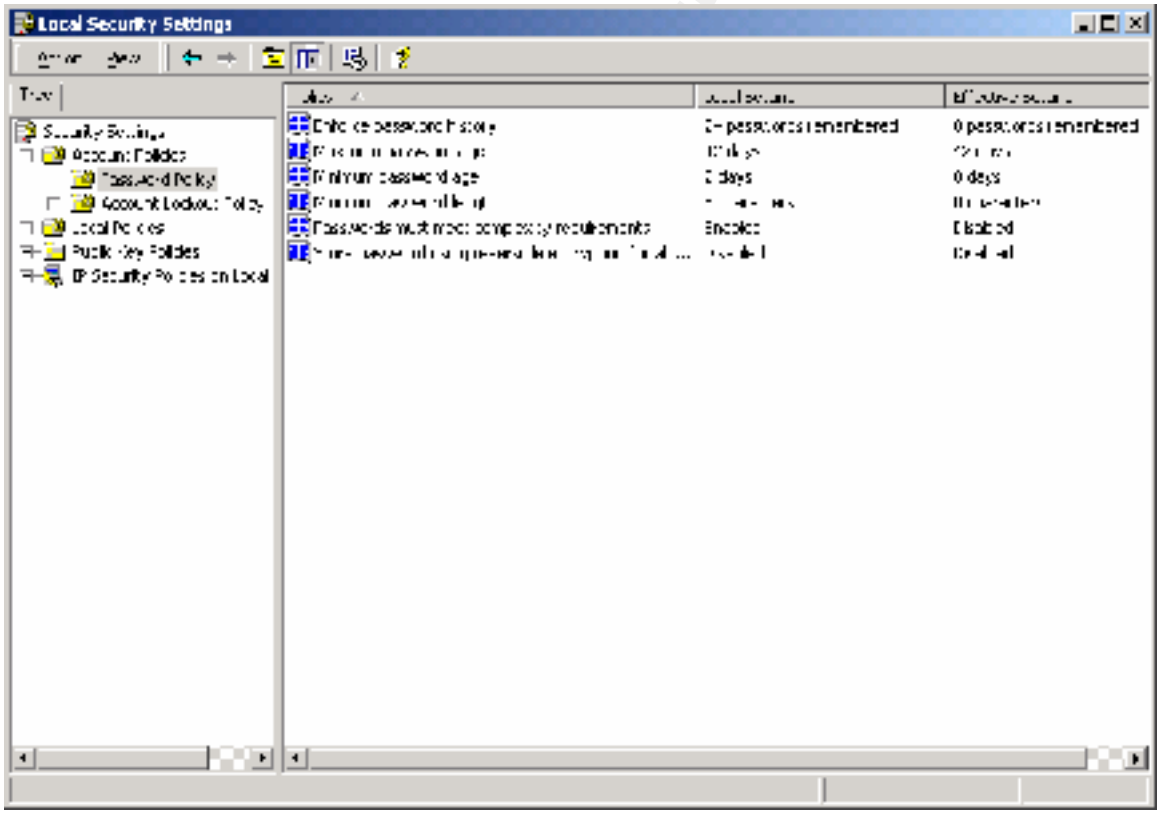



Figure 3-10

You can see that we are now auditing most everything including success and failures. As shown in Figure 3-11

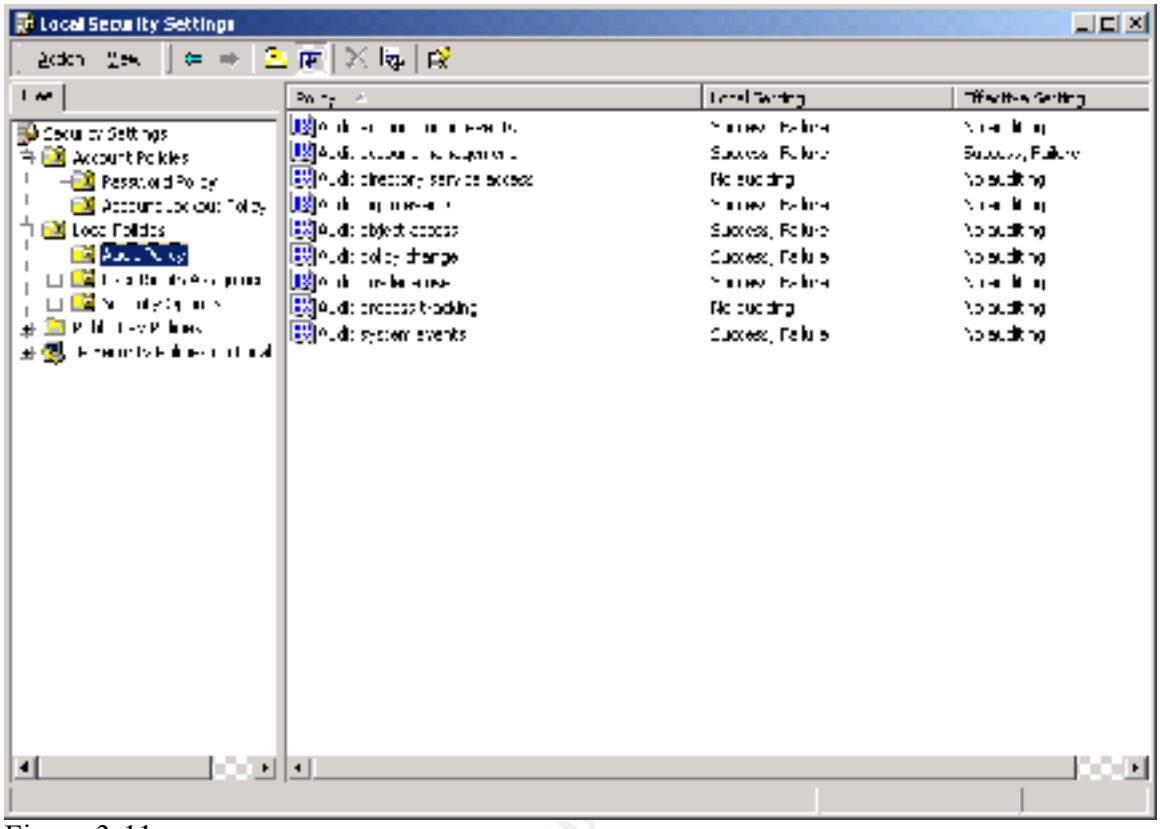


Figure 3-11

Of course any of these modifications can be changed after applying the policies. We are going to leave the defaults.

This completes the securing of the Windows 2000 OS. In the next section we will make changes to the IIS server to secure it.

There are 2 additional Microsoft Management Console (MMC) snap-ins that should be added to help on the Security Policies. These two are called Security Templates and Security Configuration and Analysis.

The Security Templates allows you to make changes to the templates. The default templates can also be loaded and changed then saved under a new name. These then can be copied to and used on another system. This is a convenient way replicate a security policy to all other machines.

The Security Configuration and Analysis add in is a tools that will analysis the current system for problems based on the loaded policy. This is used to make sure that the current policy is applied correctly. If it is not applied correctly you can then apply it from this add-in also. These two add-ins are supplied on the Windows 2000 CD and are installed by default onto the system. You add theseby clicking on Add Snap-ins from the MMC console.

**Securing IIS5.0**

We will now start the lock down of the IIS server because during the install the system basically did a complete install of IIS server from the application stand point.

We will start by removing any scripts or programs that could be used against the machine in the event of a compromise. We will also discuss the location of the scripts and what permissions we should apply to them.

Make sure that there are no additional files loaded on the Web server that can be used. For example don't load up the Internet Information Server Resource Kit.

There is a folder located in the INETpub folder called IISadmpwd which has scripts for changing passwords. These are rarely used and should be removed. Not only should this be removed from the file system but removed also from Internet Service Manager.

There is another folder in the Inetpub folder called iissamples which should be removed. If there are files located in \Program Files\Common Files\System\msadc\Samples then these too should be deleted. Internet Service Manager will have an entry for these Sample scripts also so these too will need to be removed.

There are five permissions that can be applied to a web page. Script Source Access, Read, Write, Directory Browsing and Execute. It is important to apply these permissions correctly to the folder to keep users from acquiring data incorrectly. Here is a brief description on what each one does.

Script Source Access: This permission is used with the Distributed Authoring and Versioning extensions to allow HTTP to manage files. If Script Source Access and Read are applied to a folder then the user can download the ASP code and other scripts. This is not a good thing to allow a user to download your code.

Read: Allows downloading of the files.

Write: Allows a user to upload files.

Directory Browsing: Allows users to see a list of all files in a folder.

Execute: Three levels – None which will not allow a user to download a script or executable. Scripts Only – Will allow downloading of script & script engines only. Script & Executables – Allows downloading of scripts & executables.

ISAPI extensions

ISAPI extensions is any programs that are launched by IIS because that program was associated with a specific file extension. There are known exploits using some of these

ISAPI extensions and precautions should be taken to protect the system. The best way to protect the system is to remove the unused ISAPI extensions.

These extensions are removed and added from the Properties menu of the website, Home Directory tab, Configuration button and Apps Mappings tab. At least it is recommended that the .htr, .printer, .bat, and .cmd extensions be removed. The .htr extension is used to change passwords on the system and we don't need or want that. The .printer extension is used to print from the web server and in our particular setup we don't need. The .bat extension are used to execute .bat files using a command interpreter (the .cmd extension). It is recommended that all ISAPI filters that are not needed be removed. Here is a list of these filters:

| | |
|---|---|
| .asa | Asp files to declare scripts/objects |
| .asp | Active Server Pages |
| .bat | Batch scripts interpreted by CMD.EXE |
| .cdx | Scripts to create Channel Definitions Files. |
| .cer | Scripts to handle Digital Certificates |
| .cmd | Batch Scripts interpreted by CMD |
| .htr | Remote Password change scripts |
| .htw | Index Server hit highlighting |
| .ida | Index Server performance monitoring |
| .idx | Internet Database Connector file |
| .idq | Index Server Query |
| .printer | Support for Internet Printing |
| .shtm | Server side Includes |
| .shtml | Server side Includes |
| .stm | Server side Includes |

Keep in mind that if one of these extensions is needed later then it can be added back in using the same dialog box. As shown in the Figure 3-12.

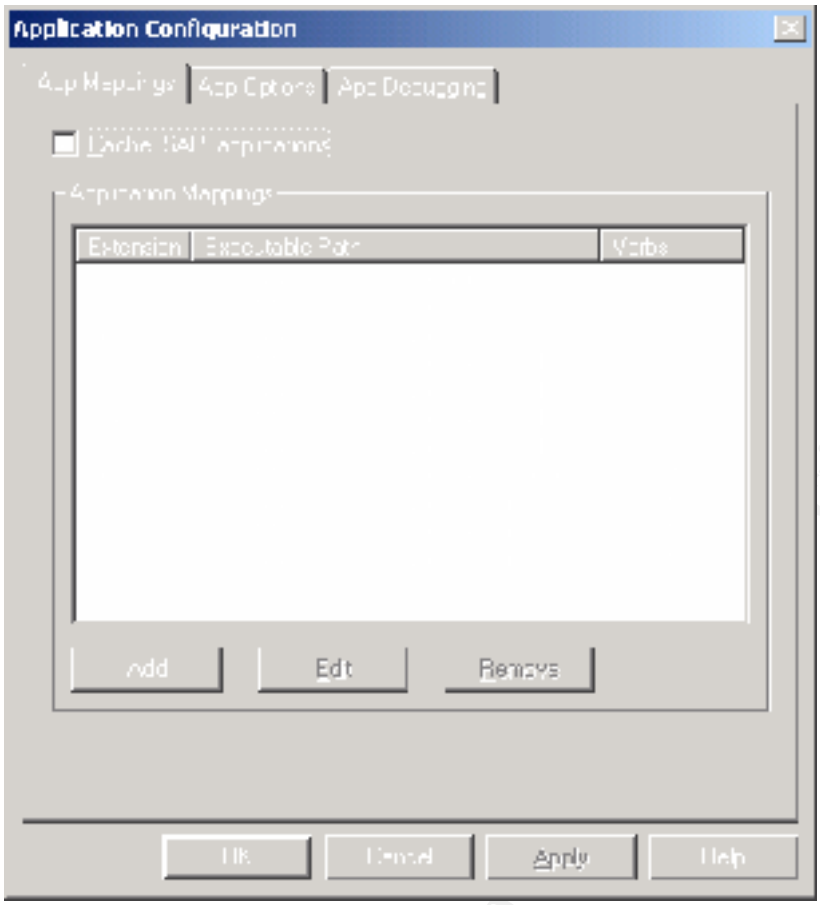


Figure 3-12

If Index server is not going to be used for this server then it is recommended to disable the service from the Services dialog box.

Following these guidelines it should create a fairly secure Web Server running on Windows 2000. Security of this server starts with the placement of this server in relation to the Internet and Corporate networks. Placing a Firewall between the Internet and the Web server and one between the Web server and the Corporate network will provide the maximum protection. Of course some companies use a single Firewall to handle both functions. Loading the Windows 2000 server correctly is critical when dealing with Security. Windows 2000 server can perform many functions but when trying to secure a server it is recommended that the server only perform a single role. For example if logon accounts are not needed for the web server then it doesn't make since to add this server to Active Directory. Doing so only opens more security holes to the Corporate network. After the server has been loaded then the system needs to be hardened. This is done by removing services, adding IP filters, changing file permissions, removing unused applications, changing security settings and changing settings from the Internet Information Server. After all these changes from the Internet only ports 80 and 443 will

be open, even ICMP or PING packets will not get into the server and the system will be more secured from users on the internet.

RESOURCES used:


'Securing Windows NT/2000 Servers for the Internet' O'Reilly Press by Stefan Norberg

'Step by Step Guide to Using the Security Configuration Tool Set" Microsoft web site
http://www.microsoft.com/WINDOWS2000/library/planning/security/secconfsteps.asp

'Hacking Exposed' Osborne by Scanbray, Mcclure, Kurtz

'Windows 2000 Security Technical Overview' Microsoft web Site
http://www.microsoft.com/WINDOWS2000/library/howitworks/security/sectech.asp

'Windows 2000 Seccurity' Microsoft web Site
http://www.microsoft.com/TechNet/Win2000/seconfig.asp