Global Information Assurance Certification Paper

Windows 2000 Small Business Security Guide

Preface

This guide is written to aid small and growing businesses in their effort to provide file, print, security and other services to their employees. While Windows 2000 (Win2K) excels in corporate environments where thousands of users and objects exist, it has also been found to excel in the small office environment as well. Out of the box, Win2K includes tools and templates to quickly and effectively perform system tasks. Often in small office environments, there is no dedicated IT administrator to support the infrastructure. For this often underpaid and overworked computer 'expert' this guide is written.

This guide focuses on aiding smaller-sized domain administrators in their efforts to integrate Win2K into their current infrastructure. Section 1 outlines high-level tasks necessary to bring a Win2K environment from the manufacturer's box to a living and breathing support and protection service. Sections 2 through 4 outline the basic purposes and security steps for Templates, Group, Security Policies as well as IP Security. Each section outlines the purpose, importance of and directions for implementing security settings.

Environmental Issues

At our example small business, Solar Systems, there are currently only two employees that would perform administrator-type duties, Bill and Ted. Bill performs the day-to-day administration duties and Ted is learning and takes care of business when Bill, the primary administrator is out of the office. Bill is therefore a member of the Administrator group and Ted is a member of the Server Operators built-in group. Obviously, in a large organization the system settings can allow many different groups and teams perform different functions, but here at Solar Systems Bill and Ted are in charge. Another assumption of this paper is that the server has already been promoted and is acting as the domain controller for SolarSystems.net.

To this end, let us begin.

Section 1: Windows 2000 Deployment Checklist

Step A: Corporate Security Policy

The first step in creating a security system for your company lies in creating an adequate security policy. Ideally, a secure computer system is one that is locked in a safe and can only be accessed by an administrator using a retinal scan and voiceprint technologies. This computer, however, is not readily usable by the organization that it supports, nor is this type of technology within the grasp of, or practical for any small business. Technology not withstanding, the most important component of any security system are the policies that define what kinds of activities will be allowed by your infrastructure.

Policies *are* the most important aspect of any security system, however they are the most tedious and overlooked portions of security. Security policies are relatively easy to write after you answer these questions:

- What kinds of business processes will my Win2K server be supporting?
- What kinds of services do I not want to let my employees have access to?
- What kinds of data will be available on this server, and is it sensitive?
- How much security is adequate, and how much will restrict my employees unnecessarily?

The last question is probably the hardest to answer since many small businesses do not have any security implemented. Many do not require their users to have a password, let alone change it every sixty to ninety days or implement one of any possibly irritating security restrictions imposed on them. Some of the questions will be easier and some will be harder to answer. As you do so, your corporate security policy will develop. This is one of our goals, to develop a security policy that will translate into a system security posture that is both sound and as transparent to your employees as possible. A good security policy leads to good system security, and so on.

If you do not currently have a corporate security policy, consider viewing the request for comments (RFC) concentrating on writing network security policies found in RFC 2196 at http://www.ietf.org/rfc/rfc2196.txt. Another good place to look is to view preexisting security policies from other companies that are performing the same types of services that yours does. For example, a law office might have different services from an architecture firm, however the services that the computer infrastructure serves in both instances are pretty similar in nature. In addition to the RFC, there are more references on security policies located in the references section of this document. The security settings used in this guide are developed from personal experience, research and industry best practices while working in various security and infrastructure consulting engagements. In each section, an explanation of what the security setting accomplishes will be outlined.

Step B: Implementing System Security

Once your policy has been written, it is time to implement the corporate policy and turn the written word into system settings. System setting translation is one of the more difficult tasks to accomplish, however using tips from RFC 2196 and other security sites will enable you to make the correlation between written policy and security settings. For a baseline of system security settings, use the ones presented in this text, modifying them as needed.

Step C: Maintenance and Auditing

Just like anything worthwhile in life, your system's security requires a checkup and look over every once in a while. For high-profile companies that have

security staff that monitor system security on an hourly basis, maintaining and auditing occurs very frequently. For the small business, maintenance and auditing are just as important as they are in a large corporation. The difference lies in that maintenance and auditing have to be performed in a way that maximizes your productivity in your primary occupation and is also manageable for your secondary occupation…the upkeep of the server.

System maintenance includes several different actions, none of which should be overlooked. By maintaining your security system, you ensure that it stays up to date and secure. One of the most important things an administrator can do is stay up to date on current exploits (loopholes that attackers use to circumvent your security system) and patches. See the references section for a small cross-section of relevant websites that can provide you with the 9 o'clock news when it comes to computer security. There are even mailing lists that you can subscribe to that provide you with weekly updates on current Win2K exploits. Many of these sites will include information on how to fix these loopholes by modifying certain system settings, applying third-party vendor solutions or loading Hot Fixes from Microsoft. Hot Fixes and Service Packs are an administrator's best friend since they can help you ensure that attackers are unable to find loopholes in your system. Most network attacks are enabled from exploits that are six or more months, if not several years old. Keeping your system up to date is arguably one of the best ways to keep it secure.

Whenever anyone says the word 'Audit' people get nervous and think about the IRS. Auditing your security system should not be thought of in this way. An audit of your system is a very important aspect to any security plan. The best audits occur often and identify loopholes and problems with security before they happen. Section 3, Security Configuration and Analysis contains the details on how we will set up a livable audit and logging trail to help keep your system yours.

Section 2: Security Templates

One of the features that has been integrated into Win2K is security templates. Imagine that you have forty employees at two different sites, and each site has three different departments, two of which are common to both sites and one that isn't. Now imagine that you have to set up each person's security settings individually. In the small (and large) business, one of the biggest stumbling blocks for security is factoring in security administration. This is where security templates can help you (more) easily define and manage your company's security. Not only will templates assist you in easing management tasks, but they will also ensure that your security changes are applied across the entire organization equally and that nobody will be left out. In information security, system security is only as strong as the weakest link.

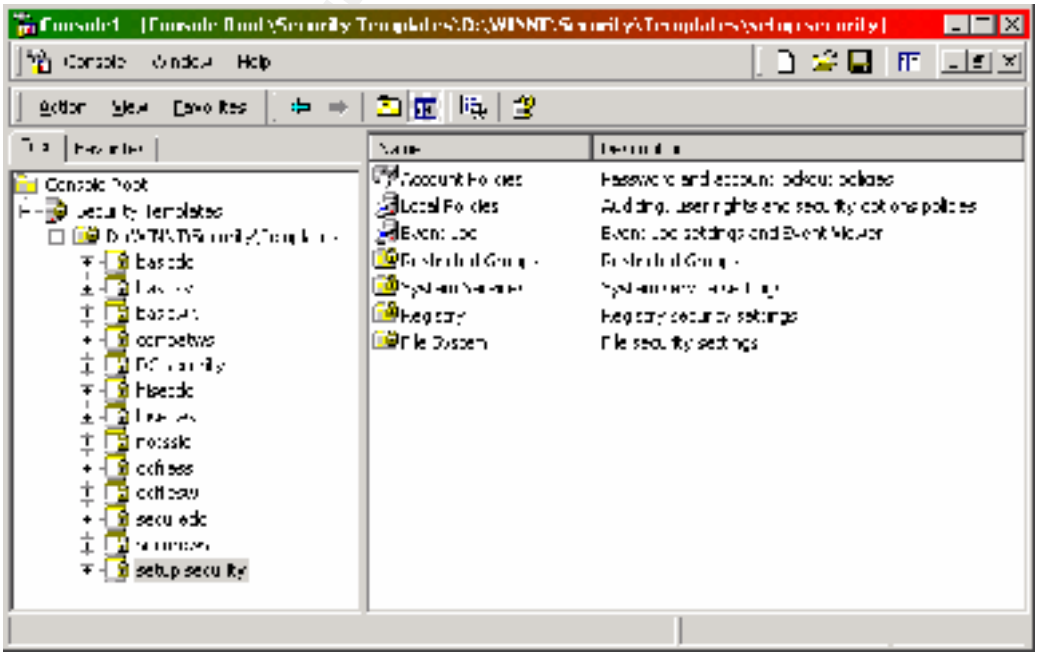
The Windows 2000 Server Administrator's Companion defines security templates as a "configuration file for all of the security attributes of a system." Security

templates can be applied to your servers and also be imported into a *Group Policy Object*, explained further in Section 4: Group Policy. When a template is placed into a Group Policy Object, the attributes of that template will affect all objects defined by that group policy.

Security Template Snap-in

Security templates are an integrated feature of Win2K and can be accessed through the Microsoft Management Console (MMC). The MMC is not installed out of the box with the Security Templates functionality built in, so we will have to install the snap-in. To add the snap-in to the MMC, go to the Start menu and from the Run dialog box run the mmc.exe executable. From the Console menu, select Add/Remove Snap-in. Once the Snap-in window appears, click on the Add button on the Standalone tab and select the Security Templates Snap-in from the list. Click Add, noticing that the Security Template snap-in has been added to the previous window. Click the Close button on the list window, and OK on the Add/Remove Snap-in window. You will notice that the snap-in has been added to the Console Root folder in the MMC.

The default templates that are standard include security settings at varying levels for different types of Win2K platforms. Templates are basically abbreviated with the security level first, followed by the type of platform. The template basicwk defines the basic or default (basic) workstation (wk) security settings. The security levels can be ordered in increasing levels of security by following this progression: DC/Setup security (out of the box), basic (default), compat (compatible), secure (secure), and hisec (highly secure). The platforms are denoted by the following abbreviations: workstation (wk), server (sv), and domain controller (dc). While each default security template predefines an array of security settings, we will concentrate on making our own template and explaining the settings as we go.



Expand the Security Templates and the Security\Templates folder to look at the default templates that are included with Win2K. Each of these templates affects the following security areas:

- Account Policies: An area that defines computer user policies.
- Local Policies: An area that defines policies that govern who has network or local access to the computer, and how events are logged.
- Event Log: An area that contains attributes that define how the security, application and system event logs function.
- Restricted Groups: Settings that define how users are added to user groups that have high levels of system access.
- System Services: An area that contains security attributes of all system services on the local computer to include file, print and networking services.
- Registry: An area that controls security settings, access, and auditing of existing registry keys.
- File System: Settings that configures access rights and permissions for local files and volumes on the system.

Creating a Security Template

To create a template, first right-click on the \Security\Templates folder and select the New Template menu item. Name the template something meaningful for your company (I have chosen smallbusinessserver) and include the current month and year in the description. Expand and view the contents of your new policy. You will notice that all of the policies will be present, however none of the individual policies will be defined. In order to define them, you will have to double click (right-clicking and selecting Security also works) on the policy in question and the settings window will appear. Inside this window, there will be a checkbox that will enable the settings, and other controls that will define the setting further.

Account Policy Security Settings

The first template policy we will visit is the Account Policy. Included in this policy are password, account lockout and Kerberos security settings. Each of the policies within the Account Policy container are detailed in the sections below.

Password Policy

Policies defined in the password section define how users are allowed to access the system using a password authentication sequence. Username/password authentication schemes are a very important step in setting and keeping a system secure. In the password policy section, we will make the following changes to our blank policy. Note: Remember to double-click on the policy in question to change the settings.

Policy	Enabled/Disabled	Setting
Enforce Password History	Enabled	5
Maximum Password Age	Enabled	60 days
Minimum Password Age	Enabled	0 days
Minimum Password Length	Enabled	7 characters
Password Complexity	Enabled	
Reversible Encryption	Disabled	

Account Lockout Policy

Policies defined in the account lockout section define how many attempts users are given before the account is locked out, and restrictions imposed on a locked account. Using the account lockout policy correctly, you can better protect your system from being compromised from a brute-force style of attack. This type of attack uses computer scripts to guess passwords very quickly, thereby circumventing system security. The following table defines how we will set our account lockout policies:

Policy	Enabled/Disabled	Setting
Account Lockout Duration	Enabled	0 minutes
Account Lockout Threshold	Enabled	5
Reset Lockout Counter After	Enabled	60 minutes

Note: Setting the account lockout duration to 0 will require an administrator to reset the account. If this is not desired, choose a value from your corporate security policy (Industry standard: 15 minutes). Also note that the counter's reset time must be equal to or less than the lockout duration.

Kerberos Policy

Many authors have explained what Kerberos is and how it works in an entire manual, so at an extremely high level, Kerberos is an authentication security protocol used by Microsoft Windows NT and now, Win2K. It is designed to provide both the end user and network resource with a source of identification over an often-insecure network connection. The following table will define how Kerberos tickets will be used on our system:

Policy	Enabled/Disabled	Setting
Enforce User Logon Restrictions	Enabled	
Maximum Service Ticket Lifetime	Enabled	90 minutes
Maximum User Ticket Lifetime	Enabled	4 hours
Maximum User Ticket Renewal	Enabled	10 days
Maximum Tolerance	Enabled	30 minutes

Local Policy Security Settings

The Local Policies area contains policies that govern the auditing of system events (Audit Policy), how users' rights are assigned (User Rights Assignment), and Security Options. A script of the settings we will enable is listed below.

Audit Policy

The policies outlined in this section dictate how strict or lenient the actions of your server and users are logged. Logging each and every single action will flood your system logs with data, possibly masking anomalous events. Not logging enough actions, or not logging business critical actions is just as ineffective. By using these settings, we will attempt to strike a balance between the two. Like in previous sections, double-click on the policy in question and the settings window will appear. Make the following changes to the Audit Policy settings:

Policy	Enabled/Disabled	Setting
Audit Account Logon Events	Enabled	Success, Failure
Audit Account Management	Enabled	Success, Failure
Audit Directory Service Access	Enabled	Failure
Audit Logon Events	Enabled	Failure
Audit Object Access	Enabled	No Auditing
Audit Policy Change	Enabled	Success, Failure
Audit Privilege Use	Enabled	Failure
Audit Process Tracking	Enabled	No Auditing
Audit System Events	Enabled	Success, Failure

Note: To enable the no auditing feature, double-click the policy in question, and mark the checkbox to define the policy settings and leave the success/failure sections blank.

User Rights Management

This policy is one of the larger policies, but it is the most important. An interesting security loophole or feature of running Win2K in mixed mode (having backwards compatibility with WinNT) is that initially, the Everyone Group is given full access to almost everything. While this makes the daily duties of your users easy, it is also an interesting loophole that internal and external unauthorized users are using to gain access to critical business systems. The dialog windows

to set these security settings are slightly different from those used earlier. In order to enable the setting, mark the checkbox to define the security settings in the template and click Add. To easily add users and groups to your list, click browse. Select the group you desire and click the Add button. Once you are done selecting the appropriate users and groups, then click OK. This last window will allow you to select who you want to have certain access rights. Make the following changes to the User Rights Management settings:

Policy	Enabled/Disabled	Setting
Network Access	Enabled	Server Operators, Administrators
Act as Part of the OS	Enabled	Administrators
Add Workstations to the Domain	Enabled	Administrators
Back up Files and Directories	Enabled	Server Operators, Administrators
Bypass Traverse Checking	Not Defined	
Change the System Time	Enabled	Administrators
Create a Pagefile	Not Defined	
Create a Token Object	Not Defined	
Create Permanent Shared Objects	Enabled	Administrators
Debug Programs	Not Defined	
Deny Access from the Network	Enabled	Guests, Anonymous Logon
Deny Logon as a Batch Job	Not Defined	
Deny Logon as a Service	Not Defined	
Deny Logon Locally	Enabled	Users, Guests, Anonymous Logon
Enable Trust for Delegation	Not Defined	
Force Shutdown Remotely	Enabled	Administrators
Generate Security Audits	Enabled	Administrators
Increase Quotas	Enabled	Administrators, Server Operators
Increase Scheduling Priority	Enabled	Administrators
Load and Unload Device Drivers	Enabled	Administrators
Lock Pages in Memory	Not Defined	
Log on as a Batch Job	Not Defined	
Log on as a Service	Not Defined	
Log on Locally	Enabled	Administrators, Server Operators
Manage Auditing and Security Log	Enabled	Administrators
Modify Firmware Environment	Enabled	Administrators
Profile Single Process	Not Defined	
Profile System Performance	Enabled	Administrators

Policy	Enabled/Disabled	Setting
Remove Computer from Docking	Not Defined	
Replace a Process Level Token	Not Defined	
Restore Files and Directories	Enabled	Administrators
Shut Down the System	Enabled	Administrators
Synchronize Directory Service Data	Not Defined	
Take Ownership of Files	Enabled	Administrators

Note: This user rights management scheme assumes that there are one, or possibly two people (one Administrator and possibly a backup who would be a member of the Server Operator group) in the organization that will be performing administrative duties. Many of the rights assigned here would not be adequate and/or appropriate in a large organization where there is a dedicated staff for user management.

Security Options

The security options section of your template defines a large number of system security settings that do not easily fit into any particular group. As a result, this section is rather large but it is also one of the more important sections of your security template. Make the following changes to the Security Options settings:

Policy	Enabled/Disabled	Setting
Additional Restrictions	Enabled	Do not Allow Enumeration
Server Task Scheduler	Disabled	
Shut Down w/o Logon	Disabled	
Eject NTFS Media	Enabled	Administrators
Session Idle	Enabled	15 minutes
Global System Objects Auditing	Enabled	
Backup and Restore Auditing	Enabled	
Logoff of Users	Enabled	
Logoff of Users (Locally)	Enabled	
Clear Virtual Memory	Disabled	
Sign Digital Client (Always)	Disabled	
Sign Digital Client (When Possible)	Enabled	
Sign Digital Server (Always)	Disabled	
Sign Digital Server (When Possible)	Enabled	
Disable CTRL + ALT + DEL	Disabled	
Last Username Display	Enabled	
LAN Manager Authentication	Enabled	NTLM Response Only

Policy	Enabled/Disabled	Setting
Message Text Logon	Enabled	<Choose your Message>
Message Text Title	Enabled	<Choose your Title>
Cache Previous Logons	Enabled	10 logons
System Maintenance of Password	Disabled	
Prevent Printer Driver Installation	Enabled	
Password Change Notice	Enabled	7 days
Recovery: Automatic Logon	Disabled	
Recovery: Allow Copy and Access	Disabled	
Rename Administrator Account	Enabled	<Choose Name>
Rename Guest Account	Enabled	<Choose Name>
Restrict CD-ROM to Local User	Enabled	
Restrict Floppy to Local User	Enabled	
Encrypt Channel Data (Always)	Disabled	
Encrypt Channel Data (When Possible)	Enabled	
Sign Channel Data (When Possible)	Enabled	
Require post Win2K Session Key	Disabled	
Secure System Partition	Not Defined	
Send Unencrypted Passwords	Disabled	
Shut Down if Unable to Log Audits	Disabled	
Smart Card Removal Behavior	Enabled	Lock Workstation
Strengthen Permissions for Global	Enabled	
Unsigned Driver Installation	Enabled	Do Not Allow
Unsigned Non-Driver Installation	Enabled	Warn but Allow

Event Log Security Settings

The settings that control the event, security and application logs are contained in this policy. Although not as large or descriptive as other policy sections, these settings are important because if something happens to your system, and the log files are not saved and accessed correctly, then the real events might not be able to be viewed. Make the following changes to the Event Log settings:

Policy	Enabled/Disabled	Setting
Maximum Application Log Size	Enabled	1024 Kbytes
Maximum Security Log Size	Enabled	1024 Kbytes
Maximum System Log Size	Enabled	1024 Kbytes
Restrict Guest Access to Application Log	Enabled	
Restrict Guest Access to Security Log	Enabled	
Restrict Guest Access to System Log	Enabled	

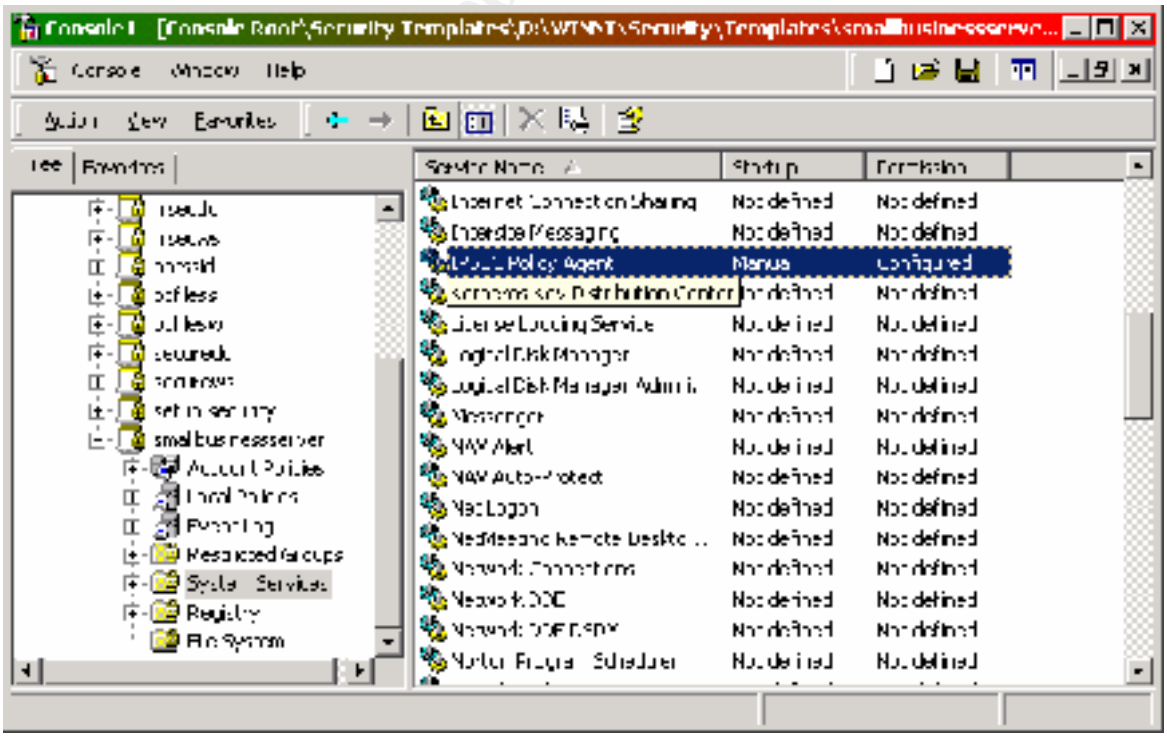
Policy	Enabled/Disabled	Setting
Retain Application Log	Enabled	7 days
Retain Security Log	Enabled	14 days
Retain System Log	Enabled	7 days
Retention Method for Application Log	Enabled	By days
Retention Method for Security Log	Enabled	By days
Retention Method for System Log	Enabled	By days
Shut Down if Logs are Full	Disabled	

Restricted Groups Security Settings

As mentioned previously, the Restricted Groups policy will allow you to administer built in user groups and also user-defined groups. Often, there are times when someone is given permissions or added to a built-in group on an ad-hoc basis. Eventually, these unregulated users can create security loopholes. All of the built-in groups are already members of the restricted 'club', so add user-defined groups to this setting if they contain users with high-level privileges.

System Services Security Settings

System Services policy settings control two different aspects of any services that are running on your server. In the System Services container, all of the services that are available to your server will be listed. These security settings will allow you to control what user or group account has permission to read, write, delete or execute, as well as define inheritance settings, auditing and ownership permissions.

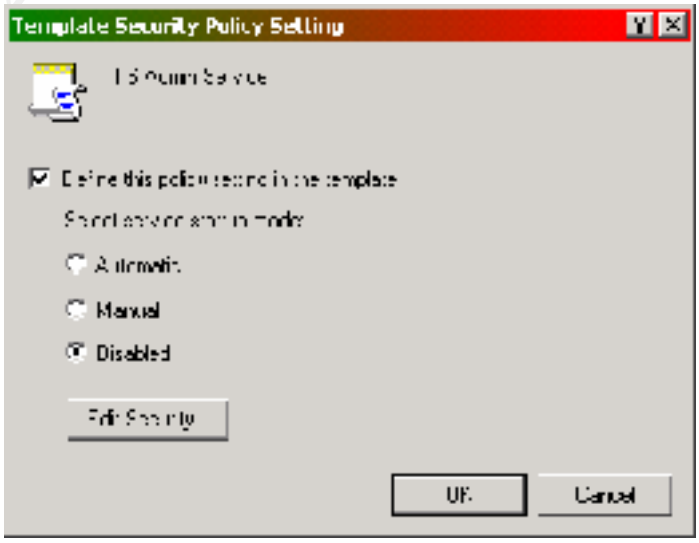


The first aspect or setting is what the service will do when the server is started. These settings are displayed in the appropriately named Startup column. The three startup modes are Automatic, Manual and Disabled. If you select Automatic, then the service will be loaded automatically; Manual will require some user intervention to start the service, and disabled will not allow the service to load upon startup. Disabling services at the boot of the computer can protect it from misuse and ensure that the server is performing services in accordance with its purpose. We will be disabling many services here that do not adhere to the purpose of the small business server and have high potential for abuse.

The second aspect or setting for System Services are the permissions. These permissions allow you to define what groups or users have the ability to perform changes to system services. Furthermore, the advanced settings will allow you to control how the auditing of this system setting is performed. We will be setting permissions for services that are sensitive in nature and can alter how security is managed on your server, and we will be auditing services to determine when users have accessed them. We are concentrating on these services to ensure that we cover the security-critical ones at this time. It is usually a safe bet to have all services audited when they are started and stopped, and to have all unnecessary services disabled on any server. We will be identifying the ones we are changing in this section, and showing an example of how to change the settings.

Modifying Startup Settings

To modify the Startup settings, double-click on the service in question and the Template Security Policy Setting window will appear. Once you mark the checkbox, the security settings window will automatically appear. After you have changed the permissions, you can set the startup mode for the service by clicking on the appropriate radio button. In the example to the right, we are disabling the IIS Admin service.



Modifying Permissions

The default permissions list for any service is to allow the Everyone group full access to the service. While this allows the most flexibility, it will also allow unauthorized users access to your most vital services. The first step when setting the permissions is probably to remove the Everyone group first. To do this, highlight the Everyone group and click on the Remove button. Then to add a group, click on the Add button and the standard Users, Computers and Groups window selection window will appear. Once you have selected all of the entities

desired, click on the OK button and then assign permissions as needed. Note: Keep in mind that these permissions will override other security permissions and that to Deny permissions will override any other Allow permission. To change damaging permissions settings later, see the General Comments portion of this section for details.

Advanced Permissions

To set the advanced permissions, click on the Advanced button on the Security for (service) window. This window contains two tabs, one for advanced permissions and another for auditing. To view and set the advanced permissions, click on the View/Edit button and a listing of the advanced permissions is shown. The permissions listed here enable an administrator to control more than just a few aspects of permission authorization.

Enabling Auditing

To enable auditing in the various system, security and event logs, then click on the Advanced button on the Security for (service) window. Click on the Auditing tab and select the user or user group desired and click on the View/Edit button. The list for auditing is the same to the previous section, and allows you to select what actions are audited, and if they will be audited when they pass or fail.

Services to be modified from the default settings are listed in the following table:

Name	Startup Type	Control	Audit
Alerter	Automatic	Administrators: Full	Yes, Full
ClipBook	Disabled		
COM+ Event System	Disabled		
Distributed File System	Disabled		
Distributed Link Tracking Client and Server	Automatic	Administrators: Full	Yes, Full
Event Log	Automatic	Administrators: Full Server Operators: Read	Yes, Full
FTP Publishing Service	Disabled		Yes, Fails only
IIS Admin Service	Disabled		Yes, Fails only
IPSEC Policy Agent	Automatic	Administrators: Full	Yes, Full
Kerberos KDC	Automatic	Administrators: Full	Yes, Fails only
Messenger	Automatic	Administrators: Full	Yes, Full
Net Logon	Automatic	Administrators: Full	Yes, Full
NetMeeting Remote Desktop Sharing	Disabled		Yes, Fails only
Performance Logs and Alerts	Automatic	Administrators: Full Server Operators: Read	Yes, Full

Name	Startup Type	Control	Audit
Routing and Remote Access	Automatic	Administrators: Full	Yes, Full
Security Accounts Manager	Automatic	Administrators: Full	Yes, Full
Simple Mail Transport Protocol	Disabled		Yes, Fail only
System Event Notification	Automatic	Administrators: Full	Yes, Full
Task Scheduler	Automatic	Administrators: Full	Yes, Full
Telnet	Disabled		Yes, Fail only
World Wide Web Publishing Service	Disabled		Yes, Fail only

Note: Ensure that after you make Service setting changes that other Services are not dependant on each other. Use the Event Viewer after startup to see if any Services failed.

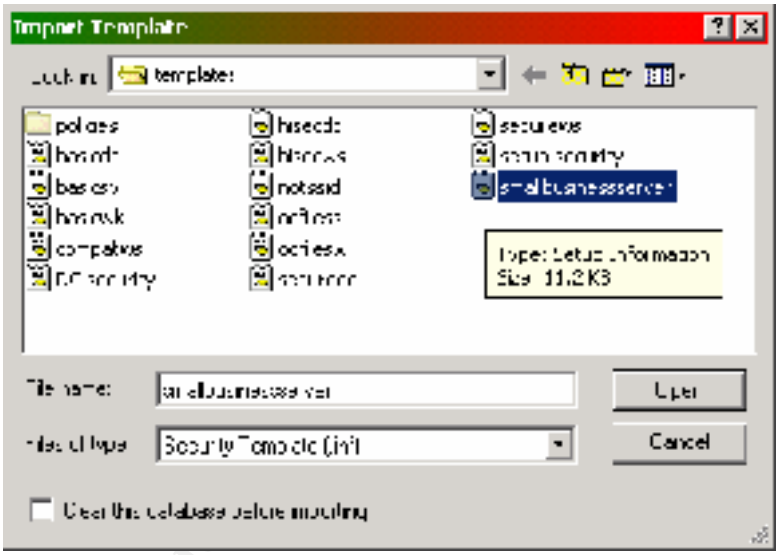
Template Considerations

Win2K templates, when used properly can help system administrators perform security and permission tasks quickly and easily. Changing settings in your server's Local Security Policy and Local Domain Policy interfaces can effectively change all of the settings we set in this section. The power of templates is that you can create templates for different organizational units, servers, and users and import those policies into Group Policy. Templates can be layered within an organization and the subordinate organizational units to easily manage your infrastructure. Templates are also an easy way to quickly reset system security to the default levels by applying the 'Setup Security' template to your organization. Traditionally, administrators will apply a template on the computers within a Group Policy Object (GPO) and another template onto the users within the GPO. This is useful because often users might wander from computer to computer within an organization, and you want their user rights and security restrictions to follow them.

Section 3: Security Configuration and Analysis

The Security Configuration and Analysis snap-in "allows an administrator to check the state of a system's security against one or more security templates and make appropriate modifications." Like the Templates snap-in, the Security Configuration and Analysis snap-in must be added to the Microsoft Management Console (MMC). To add the snap-in to the MMC, go to the Start menu and from the Run dialog box run the mmc.exe executable. From the Console menu, select Add/Remove Snap-in. Once the Snap-in window appears, click on the Add button on the Standalone tab and select the Security Configuration and Analysis Snap-in from the list. Click Add, noticing that the Security Configuration and Analysis snap-in has been added to the previous window. Click the Close button

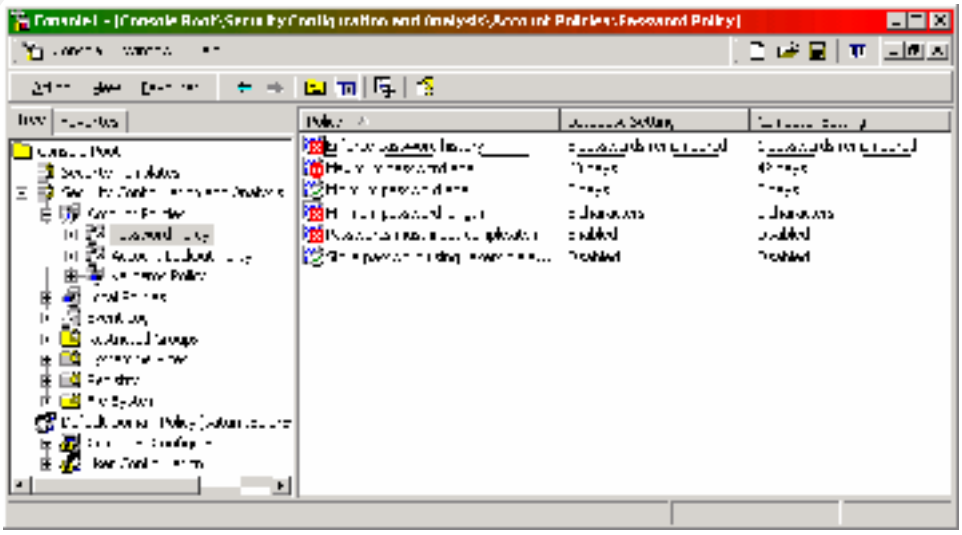
on the list window, and OK on the Add/Remove Snap-in window. You will notice that the snap-in has been added to the Console Root folder in the MMC.



This snap-in allows us to perform two very important functions, Configuration and Analysis of your server. To perform analysis of your computer, right click on the Security Configuration and Analysis (SCA) container. Click the Open database menu item and name your database. Since we are creating a new database, we will be checking our domain against the current settings within a security template. Select the security template you created before and click the Open button. In the right-hand window of the MMC you will see instructions on how to carry out analysis and configuration tasks.

To analyze your computer, right click on the SCA container and click on the Analyze Computer Now menu item. You can rename your log file if you wish, as the default value will match your database name. Click OK. Your computer will now perform the analysis, comparing the items set on your computer with the items specified in your template. Once the analysis is complete, you will notice that your SCA container now has subordinate containers that look very similar to the base template security policy areas.

To check to see how your domain stacks up against your template, expand one of the policies and select one of the lowest-level policies. Our example shows the elements of the Password Policy and you can see that the minimum password age policy met standards. As a result, a check mark notifies you that the current settings meet the standards set in the template. A red x notifies you that there is a discrepancy between the settings.



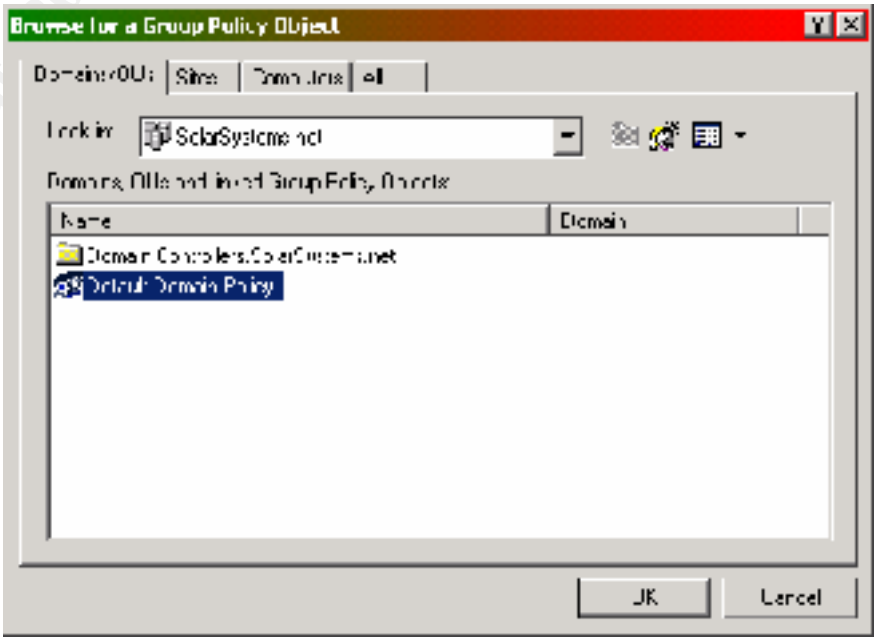
In instances where the current settings exceed the standard, a red x will still appear.

Looking through your current policy, you might notice that there are a lot of discrepancies. The reason that there are discrepancies is because your Windows 2000 server has different security settings than the template that we tested against. There are a few ways to solve these discrepancies and secure your server. One is to use the SCA snap-in Configure your Computer menu item. We will not be performing this action, because we will be applying our template in Section 4: Group Policy. In the vent that you want to do this, right click on the SCA container and select Configure Computer Now. Follow the instructions and the configuration editor will perform all tasks to ensure that your computer is now configured in compliance with your template. The main difference between importing a template into Group Policy and running the configuration editor is that these settings will be applied to this computer only, and will not be applied to the Group Policy Object.

Section 4: Group Policy

Group Policy has grown up from Windows NT Security Configuration Editor and System Policy and has become one of the most important features included in Windows 2000. Group Policy, according to Jason Fossen has been expanded to allow an administrator to control "the configuration of computers and user preferences automatically, no matter how many computers or users exist in your organization."

Group Policy Snap-in



The first task in securing Group Policy is to apply our template to the Group Policy. Following the same procedure as earlier, we will add the Group Policy snap-in to the Microsoft Management Console. Once you have select the Group Policy snap-in, click Add. A Group Policy Object wizard will appear and ask GPO you would like to load into the snap-in. Click Browse. The window seen to the right shows the default GPO browsing window. Depending on the number of organizations and organizational units within your organization, you will have the ability to load the Group Policy editor

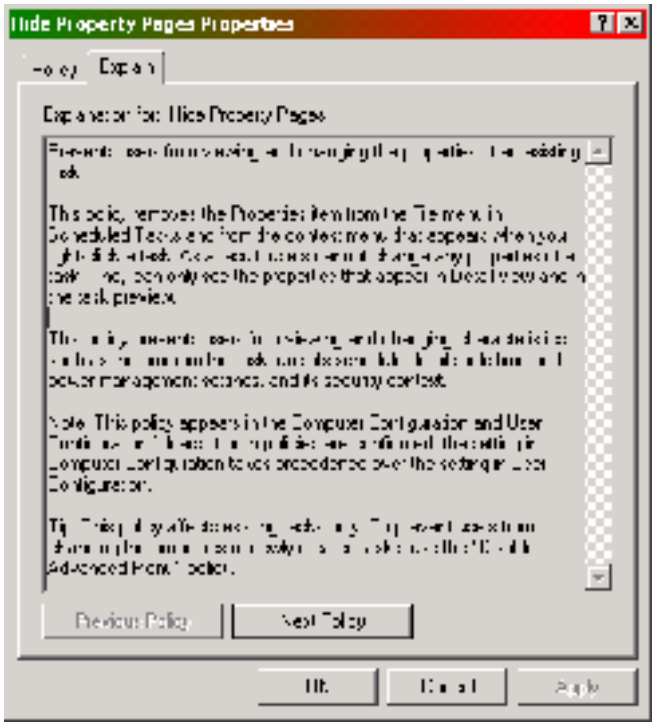
for each one of these. I chose the Default Domain Policy since at Solar Systems there are not any organizational units. After you close the snap-in windows, the MMC will display the policy you loaded with the Computer and User Configuration containers. Expanding the Computer Configuration > Windows Settings > Security Settings container, you will see some of the same Policy Containers that we defined during template set up. Expand some of the other containers and look to see what kinds of policies are included in your Group Policy. As you can see, Group Policy if properly configured, is arguably one of the most powerful enhancements to Win2K.

Applying Templates to Group Policy

To apply your Template to the Group Policy Object (GPO), expand the Computer Configuration > Windows Settings container and right click on the Security Settings container. Select Import Policy and a standard file dialog box will appear. Choose the template you wish to apply to the GPO and click Open. Once you perform this action, the Template you selected will be applied to the GPO, however it won't actually be enforced until you reboot the server twice. This is a documented and tested (I had to try it myself) function that enables Win2K to make policy changes in a phased approach. Before you reboot your system, ensure that you can recall the newly renamed Administrator account, if you changed it during the Template set up. After the second reboot, all changes will be applied and any renamed accounts can only be accessed through their new names.

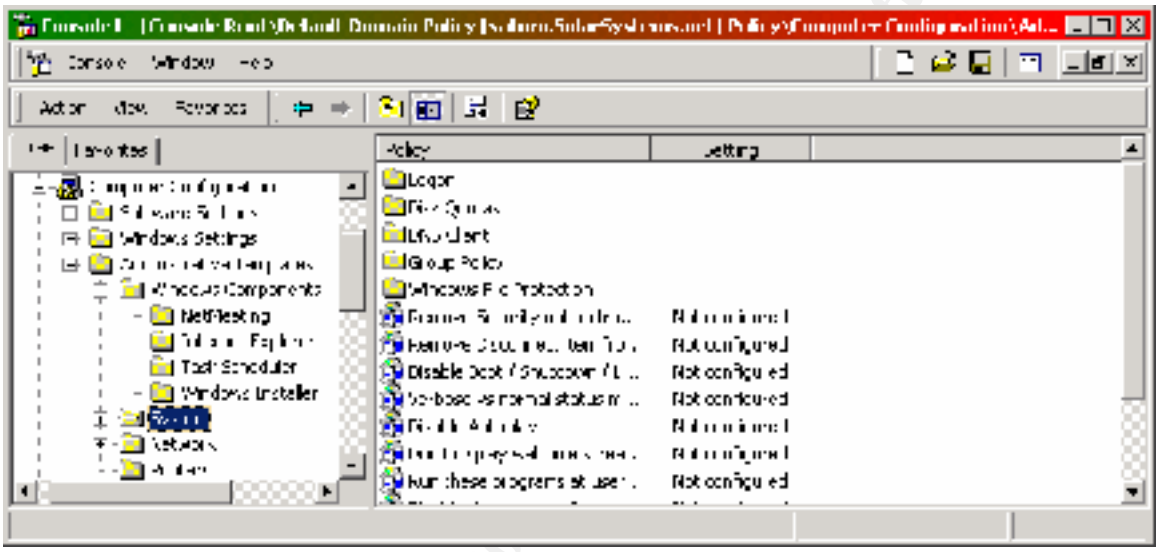
Configuring Other Group Policy Settings

As was already noted, there are more settings in Group Policy than what the Security Templates can set. All of these settings are customizable and there are extensive explanations of each and every Group Policy setting within the GPO.



To configure the setting for the GPO, double-click the policy in question, or right-click it and select Properties. On the policy tab, three radio buttons with accompanying setting levels will be present: Not Configured, Enabled and Disabled. The setting levels, coupled with the wording of some of the settings can be somewhat confusing. Remember that you Enable/Disable a setting, and that setting performs some action. If you Enable a setting that Disables control of a Windows 2000 feature, then you have *disabled that Windows 2000 feature.* Do not look at the

actual feature and insert the setting level into the sentence. For an explanation of the feature, you can click on the Explain tab. The explanations within the Group Policy are probably the best online documentation available and they come standard in Windows 2000. Another thing to consider is that you will notice that there are duplicate settings for certain resources in both the Computer and User containers. It is important to note that Computer configurations will override User configurations every time. When troubleshooting problems with a user or group that has the appropriate permissions, this is a good area to check for discrepancies.



Make security changes to the Group Policy containers listed below. Note: Settings that are omitted from this table should remain at default levels.

Container	Policy	Setting	Advanced Setting
Computer Configuration > Administrative Templates > Windows Components			
Netmeeting	Desktop Sharing	Enabled	
Task Scheduler	New Task Creation	Enabled	
Computer Configuration > Administrative Templates > System			
Disk Quotas	Enable Quotas	Enabled	
Disk Quotas	Enforce Limits	Enabled	
Disk Quotas	Default Quota	Enabled	See Note a
Disk Quotas	Log Quota Exceeded Events	Enabled	
Computer Configuration > Administrative Templates > Network			
Offline Files	Enabled	Disabled	
Network and Dial-up Connections	Connection Sharing	Enabled	
Computer Configuration > Administrative Templates > Printers			
Printers	Web-Based Printing	Enabled	

Container	Policy	Setting	Advanced Setting
User Configuration > Administrative Templates > Windows Components			
Netmeeting > Application Sharing	Prevent Sharing	Enabled	See Note b
Netmeeting > Application Sharing	Prevent Desktop Sharing	Enabled	
Netmeeting > Application Sharing	Prevent Sharing Command Prompts	Enabled	
Netmeeting > Application Sharing	Prevent Sharing Explorer Windows	Enabled	
Netmeeting > Application Sharing	Prevent Control	Enabled	
Netmeeting	Set Call Security	Enabled	Required
Netmeeting	Automatic Acceptance	Enabled	
Netmeeting	Sending Files	Enabled	
Netmeeting	Receiving Files	Enabled	
Windows Explorer	Do Not Request Alternate Credentials	Disabled	
Windows Explorer	Request Credentials for Network Installs	Enabled	
Task Scheduler	Disable Task Creation	Enabled	
Computer Configuration > Administrative Templates > Network			
Network and Dial-up Connections	Prevent Configuration of Sharing	Enabled	

Notes:

a) Disk Quotas are not normally thought of as security items, however if a malicious attacker (or greedy employee) uses all of the hard disk resources on your computer, problems will occur.
b) Netmeeting security values have been set in this section assuming that the users and computers within this GPO are not allowed to use Netmeeting.

Section 5: Internet Protocol Security Policies

Win2K comes standard with two separate approaches to securing network data, tunneling and Internet Protocol Security Policies (IPSec). Where tunneling masks the actual contents of the message and provides some measure of confidentiality, IPSec provides system users with confidentiality, integrity and authentication. IPSec basically works by creating and activating a policy that contains certain security requirements at each end of a network connection. Just like any other protocol, once a handshake is done to ensure authentication, secure transmittal of data is possible. IPSec is flexible in that it allows systems to use Kerberos authentication, and/or various public/private and symmetric key

algorithms. Before we establish a secure channel between two Win2K servers that are not in the same domain, here is a brief explanation of IPSec policy components:

- IP Filter: Network traffic defined by IP address, transport protocol and port. This item tells the IPSec driver what traffic should be secured.
- IP Filter List: A grouping of one or more IP filters which is used to define network ranges.
- Filter Action: What methods the IPSec driver should secure the transmissions.
- Security Method: Defines the type of authentication and process for key exchange.
- Tunnel Setting: If using IPSec Tunneling, defines the end point of the tunnel.
- Connection Type: The type of connection, LAN, remote access or all.
- Rule: The combination of all of the components that create a policy. If necessary a single policy can have several rules to secure each channel uniquely.

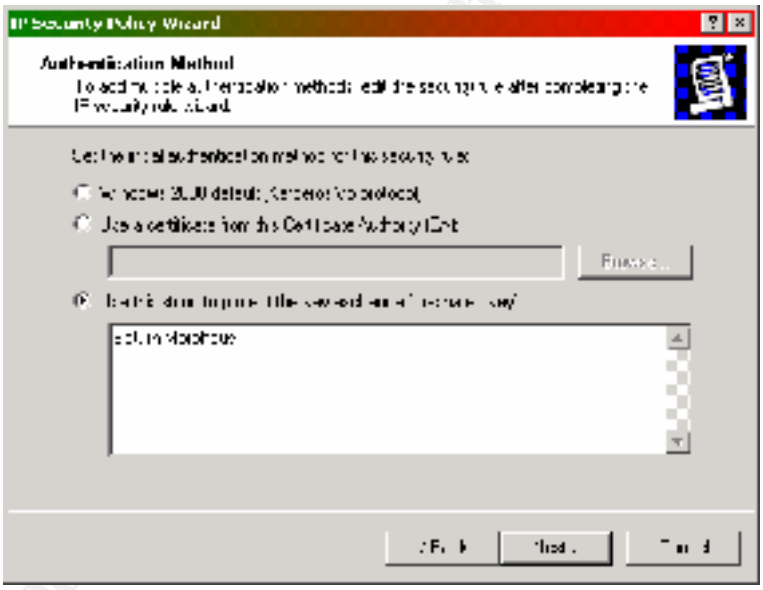
Creating IPSec Policies

This section will outline how to create a secure channel between two Win2K systems using IPSec. In our environment, we have connected our home server (Saturn) with the remote server (Morpheus). Since both servers should follow the same procedure (Task Lists A and B), once you have performed these functions on one server, repeat them on the opposite server, and then proceed to Task List C.

Task List A: Creating an IPSec Policy

1. Start the MMC (using procedures found in earlier sections) and load the IP Security Policy Management snap-in. When prompted for the scope of the policy, click the radio button for Local Computer and click Finish.
2. Right-click on the IP Security Policies on Local Machine container, and select Create IP Security Policy.
3. Once the next window loads, click Next.
4. Type the name of the policy and add a comment if needed. Note: Using the end connection server names helps when troubleshooting and identifying policies. Example: Saturn-Morpheus.
5. Un-mark the checkbox labeled Activate the default response rule, and click Next.
6. Ensure that the Edit Properties checkbox is marked, and click Finish.
7. On the properties window of your policy (it will carry the name that you assigned it on the title bar), ensure that the checkbox in the IP Filter List is unmarked, and that the Use Add Wizard checkbox is marked. Click Add.
8. Once the next window loads, click Next.

9. Since we will not be using tunneling, click on the radio button, not specifying a tunnel endpoint. Click Next.
10. Click on the LAN radio button. Click Next.
11. Depending on what services you have available, there will be a difference in what selections you make on the Authentication Method Window. If you choose to use the Windows 2000 Default (Kerberos V5 protocol), then select that radio button. If you have a CA (certificate authority) in your enterprise, you can select the radio button and fill in the CA's DNS name. In the example, we chose the third radio button to use a pre-shared symmetric key, which is protected (hashed) by a string. Whichever method you use, you must use the same authentication method on both ends of the connection. Ensure that you write down or remember the string, if you select that option (case sensitive) to ensure that the other server uses the same value. Note: In the caption below, we selected to use a pre-shared key. Click Next.

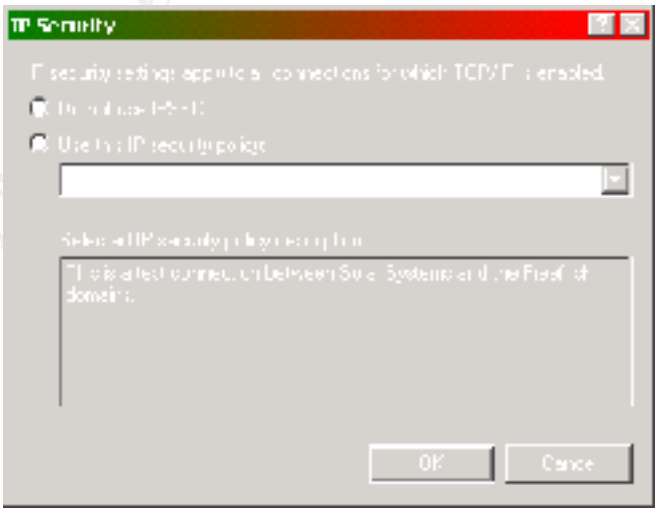


12. At the next window, click Add.
13. Choose a name and a meaningful description and ensure that the Use Add Wizard checkbox is marked. Click Add.
14. At the next window, click Next.
15. Select My IP Address from the drop-down box. Click Next.
16. Select A Specific IP Address from the drop-down box. Enter in the remote IP address and click Next.
17. Select Any from the drop-down box. Click Next.
18. At the next window, ensure that the Edit Properties checkbox is unmarked. Click Finish.
19. At the next window, click Close.
20. Click on the radio button next to your new IP filter. Click Next.
21. Ensure that the Use Add Wizard checkbox is marked. Click Add.
22. At the next window, click Next.
23. Choose a name and a meaningful description and ensure that the Use Add Wizard checkbox is marked. Click Next.
24. Click on the Negotiate Security radio button. Click Next.
25. Ensure that the radio button is clicked that selects not to communicate with computers that do not support IPSec. Click Next.
26. Ensure that the High (Encapsulated Secure Payload) radio button is selected. Click Next.

27. At the next window, ensure that the Edit Properties checkbox is unmarked. Click Finish.
28. Click on the radio button next to your new IP filter action. Click Next.
29. At the next window, ensure that the Edit Properties checkbox is unmarked. Click Finish.
30. On your IPSec policy properties window, ensure that your new filter is selected. Click Close.

Task List B: Configuring Adapters and Services

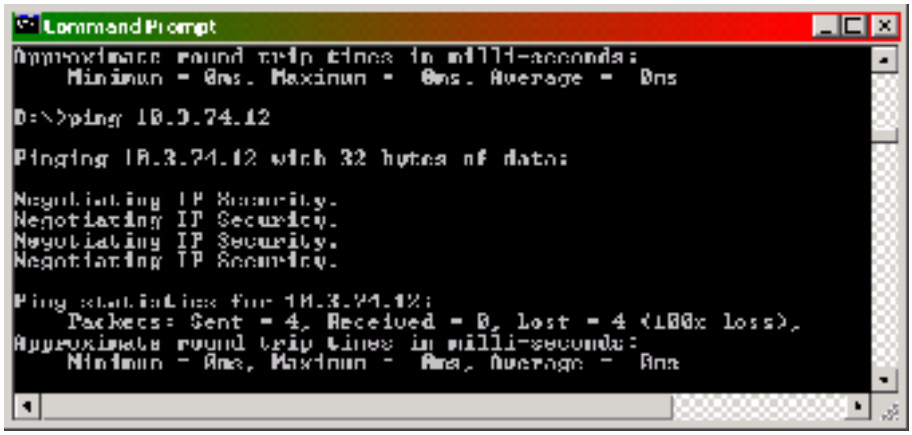
1. Right-click on your Network Neighborhood icon. Click on properties.
2. Right-click on your network device that will be connected to your remote computer and secure the channel. Click on properties.
3. Scroll down in the components window, select the Internet Protocol (TCP/IP) and click on the Properties button.
4. On the properties window, click on the Advanced button.
5. On the settings window, click on the Options tab. Select IP Security and click on the Properties button.
6. On the IP Security, click on the radio button to specify an IPSec Policy and select yours from the drop-down box. Click OK.
7. Click OK until you have left the configuration windows for your network adapter.



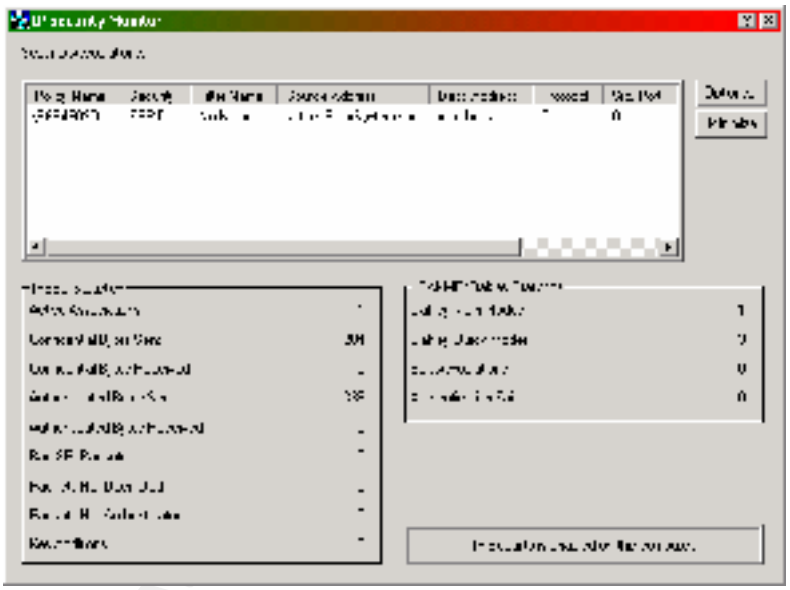
8. Start the Services Console by navigating: Start Menu > Programs > Admininistrative Tools > Services.
9. Start and Stop the IPSec Policy Agent to ensure that the new IPSec Policy is loaded.

Task List C: Connecting Servers

Once both servers have completed both Task Lists A and B, at either system open up a command prompt and ping the other system, ensuring that you use the IP address. You will notice that instead of the traditional ping responses, the 'Negotiating IP Security' string will be shown.



The action of pinging the host opens the secure channel (one way, not both ways yet) between the two servers. Perform a ping from the remote system to complete the transaction.



Once you have completed this, you can monitor any IPSec Policy-secured transmissions by using the ipsecmon command from the Run menu. The IP Security Monitor will show all current connections, as well as show statistics on the number of bytes sent and received and others.

Troubleshooting

While IPSec is a very powerful tool provided with Win2K, it is a very fragile method of securing data. To track the success and failure of key exchanges between servers, enable logon and logoff auditing (the template in section 2 already has this enabled) and load the Event Viewer. Look for event ID's 541, 542 and 543. These events will outline successful and unsuccessful attempts of IPSec to establish and maintain channels. Often protocols are enabled and the initial exchange of credentials is successful, but network problems cause the channel to lose connection. According to Zubair Ahmad, on network segments with high levels of traffic, or slow connection speeds, it may be necessary to "[use] a number of re-keys greater than 50MB and a key lifetime value of greater than 5 minutes."

Ending Comments

While Microsoft and the Windows 2000 product provides system administrators with a host of tools and training, security seems to always be the least thought of task. With a great majority of the businesses in the world fitting into the 'small office' classification, a proliferation of security essentials must be passed onto administrators in order to raise the security environment as a whole. Out of the box, Win2K offers an impressive array of tools, and loopholes that unauthorized users can utilize to make your Win2K server…their Win2K server.

References and Credits

Note: The section title of the book precedes the MLA to make the references more informative.

Section 1:

Hernandez, Ernest D. "Network Security Policy - A Manager's Perspective". http://www.sans.org/infosecFAQ/policy/netsec_policy.htm. November 2000 (25 February 2001).

"Request For Comments 2196".
http://www.cis.ohio-state.edu/htbin/rfc/rfc2196.html. September 1997. (1 March 2001).
"Security Websites"; 4th Edition Sans Institute Roadmap.
Bugtraq: http://www.ntbugtraq.com
Packetstorm: http://www.packetstorm.securify.com
SANS: http://www.sans.org/giac.html
L0pht Heavy Industries: http://www.l0pht.com
"Security Mailing Lists" 4th Edition Sans Institute Roadmap.
(Type "suscribe <listname>" in the body of the message)
SANS Security Alert Consensus: sans@sans.org
SANS Newsbites: sans@sans.org
SANS Windows Security Digest: sans@sans.org
Bugtraq Full Disclosure List: listserv@securityfocus.com
NT Bugtraq: listserv@listserv.ntbugtraq.com

Section 2:

"Using Templates to Implement Security Policies". C. Russel & S. Crawford; Microsoft Windows 2000 Server - Administrator's Guide. Redmond: Penguin Books, 2000. pp 629-638.
"Microsoft Management Console Help", Windows 2000 Online Help.

Section 3:

"Using Security Configuration and Analysis". C. Russel & S. Crawford; Microsoft Windows 2000 Server - Administrator's Guide. Redmond: Penguin Books, 2000. pp 636-641.
"Using the Security Configuration and Analysis Tool Set", October 2000, Roberta Bragg; Windows 2000 Security, pp 216, 218-225.

Section 4:

"Group Policy". Fossen, Jason. Windows 2000: Active Directory and Group Policy. SANS Institute, July 2000. pp 106-138.
"Group Policy". Bragg, Roberta. Windows 2000 Security. Indianapolis: New Riders, October 2000. pp 216, 225-230.
"Managing Local Security Settings with Group Policy". Bragg, Roberta. Windows 2000 Security. Indianapolis: New Riders, October 2000. pp 216, 260-275.

Section 5:

"Using Internet Protocol Security Policies". C. Russel & S. Crawford; Microsoft Windows 2000 Server - Administrator's Guide. Redmond: Penguin Books, 2000. pp 655-664.
Sharick, Paula. "Use IPSec to Protect Your LAN Resources", Windows2000 Magazine. Vol. 6 No. 11 (2000): pp 71-74.
Ahmad, Zubair "Troubleshooting IP Security Problems". http://www.win2000mag.com InstantDoc ID# 7831. December 1999 (20 February 2001).

Last Updated: July 27th, 2017

Upcoming Training

SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC505: Securing Windows and PowerShell Automation	SEC505 - 201709,	Sep 18, 2017 - Nov 13, 2017	vLive
Secure DevOps Summit & Training	Denver, CO	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced