Securing a Process to Synchronize Field Data with a Central Database

GIAC Certified Windows Security Administrator (GCWN) Practical (v.3.2)
Option 2

Mark Winder
December 19, 2003

Abstract

This paper discusses how Windows security can be used to secure a commercial software system that collects data from geographically remote locations.

As this software, which will be referred to as the **Program**, is a commercial closed-source application, some details of its internal security will not be covered. The focus will be on presenting Windows security topics that can be applied to protect the data synchronization process. Examples will demonstrate the application of Windows security in specific (but sometimes hypothetical) cases[1].

Some background information is required to fully understand the security problems. Where possible, supporting information will be relegated to Appendices to keep the security discussion in the body of the paper. This does not mean the Appendices are optional reading. For example, Appendix A contains a background of the operating and business environment that is required to fully understand the security challenges.

The Data Synchronization process starts in a Field environment that often consists of seasonal, transient, and non-technical workforce running the Program Client on outdated, unmanaged laptops communicating over slow, unreliable connections. At the other extreme, and far more uncommon, the Field environment can consist of highly-managed laptops on a high-speed WAN. This range provides the opportunity to discuss a broad range of Windows security topics.

The Data Synchronization process ends at the central Database Server; located at a head office there is security infrastructure and, usually, trained and dedicated people responsible for the Enterprise's security. Data Synchronization must happen in as secure an environment as possible between the endpoints.

One theme to come out of this paper is there are many ways Windows Security can be applied to a real-life system! Most involve tradeoffs (for example, one

[1] It was my intention to make this paper a complete "Practical" guide for IT staff trying to securely implement the Program, in addition to meet the GCWN Practical requirements. However, to cover each topic in breadth, and then in depth, along with a demonstration of my applied knowledge, would mean an encyclopedia sized paper and a permanent home in the looney bin. I hope I have provided a suitable balance between providing security facts and showing how security can be applied.

group of tradeoffs is between security, cost, and ease of use[2]). It is ultimately up to each company to decide on the process that works best in their environment.

[2] See "Which Technology Decision Triangle". URL: http://www.signify.co.uk/services/cost_conv_security_triange.asp, (23 Nov. 2003).

Table Of Contents

Overview of the Program's Data Synchronization Process

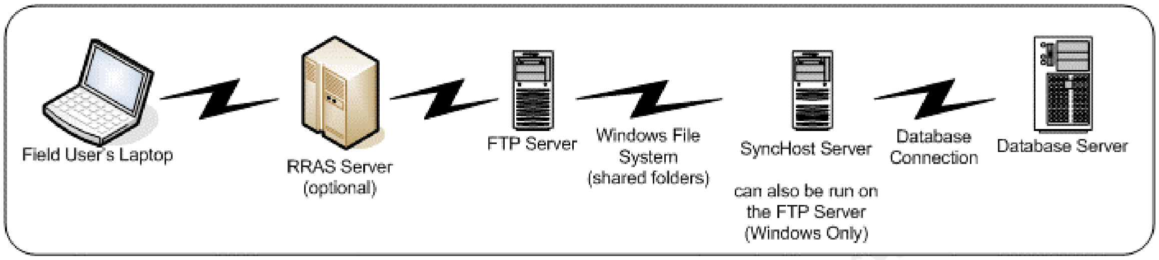


Figure 1 - Data Synchronization process

A high level view of the Data Synchronization Process (Data Sync) is shown above.

Laptop (Program Client)

The Program Client is a graphical 32-bit Windows application that updates a local Access database of well information. Most field users run the Program Client on laptops running Windows 98 or later.

The goal of the Data Sync Process is to synchronize the field data in the local Access database with a central Database Server at a head office. The data is entered locally without requiring a connection to the Database Server. The synchronization process can be two-way; data is sent from the client to update the central database and changed values can be sent from the central database back to the client.

To synchronize, the field user provides:

FTP Username
FTP Server Address
FTP SyncHost Root Directory
Database Username
Database Password
RAS Connection

This data is all stored in the registry except the database password (which must be typed on each synchronization attempt). The FTP Username and FTP Password are stored encrypted in the HKEY_CURRENT_USER hive of the registry. If multiple profiles are used on the Program Client, these settings will have to be entered for each user.

RRAS Server (optional)

A company may choose to manage the Laptop's network connection and provide a Routing and Remote Access Server (or a similar product from a third party).

Laptop to FTP Server Communications

The Program Client contains a built-in FTP Client. The Program Client can dial a RAS Dial-up Networking configuration (actually it can dial two, allowing for a VPN connection) or use an existing network connection.

The Program Client uses Passive FTP and the port is hard-coded 21.

FTP Server

The Program Client sends and retrieves data through an FTP Server. The FTP server is usually managed by a Company's IT department and located at a branch or head office.

Any FTP server software that supports Passive (PASV) client connections can be used. Both read and write permissions are required on the server (the FTP folder structure and detailed permissions are covered later). There is no requirement that the FTP Server run on Windows; however, the host OS must support Windows File Sharing to communicate with the SyncHost Server.

FTP Server to SyncHost Server Communications

The FTP Server and SyncHost Server share a common directory structure on the file system.

If the SyncHost Server and FTP Server are on separate computers, a secure alternative to setting up a file system share is a firewall-friendly directory synchronization product. IPSec can further be used to encrypt network traffic between the two servers.

SyncHost Server

The SyncHost Server is a graphical 32-bit Windows executable. Like the FTP Server, this server is usually under the control of a company's head office IT Department.

SyncHost Server monitors a Windows file system (or file share) for file changes (files arriving from the client via the FTP Server). When files appear, SyncHost Server decodes them, performs requested actions on the Database Server using the Client’s embedded database credentials, and provides results back to the Program Client (by creating new files for the client to download through the FTP Server).

The SyncHost Server is a standalone application (not a service). When running standalone, a user must be logged in to start SyncHost Server. From a security standpoint, it is important that this user have limited permissions, the server be physically secure, and the system be locked (password-protected screen saver or OS lock) when unattended. SyncHost Server can be set up to run as a service using an unsupported Microsoft tool called Srvany.exe. This is covered in Appendix F.

SyncHost Server to Database Server Communications

The SyncHost Server connects to the database server using a TCP/IP connection and authenticates using the database credentials passed in by the Program Client. The SyncHost Server does not impersonate the field user (it is not a SQL Trusted connection).

A firewall or proxy should be set up between the SyncHost Server and Database Server. They can be set up to communicate over non-standard ports, and firewall rules can be used to limit the database connection to/from the SyncHost server only. IPSec or SSL can be set up to encrypt traffic between the servers.

Database Server

The corporate Database Server usually is Oracle (version 8 or later) or MS SQL Server (version 7 or later).

The Database Server usually lives in a secure corporate environment accessible by the administrative staff. One of the challenges of the Database Server is user maintenance. The Program does require that each field user have his or her own unique database login if data is to be audited in the application (a requirement for the majority of companies).

Firewalls Overview

This paper assumes a technical audience that is familiar with firewalls. Readers unfamiliar with firewalls may want to refer to a book[3] or article[4] for some background knowledge. Firewalls are a big part of securing Field Data Transfer.

Here is the simplest setup for data synchronization:

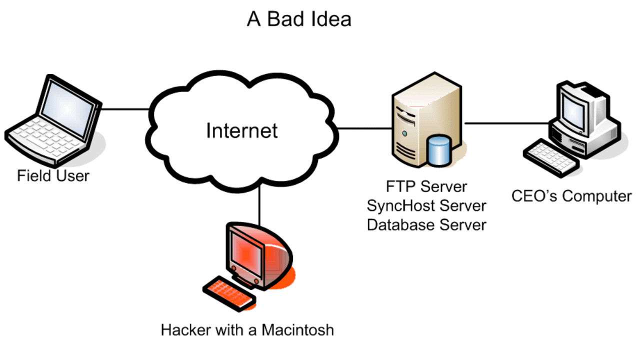


Figure 2 - No Firewalls

Although the configuration in Figure 2 - No Firewalls has the advantage of simplicity and cost savings, connecting a computer to the internet without a hardware firewall is a high-risk activity. The FTP Server could be hardened[5] but some ports will have to be exposed (port 21 must be exposed for instance). If the wily Mac Hacker manages to compromise the server through FTP there is nothing stopping him or her from undoing the security improvements and, in time, draining the CEO's bank account.

It would be better to use firewalls:

[3] There are many great books. A classic is “Firewalls and Internet Security, Repelling the Wily Hacker” by Cheswick and Bellovin.

[4] There are many articles on the internet as well. For example, “Firewalls Explained” on TechTV's web site. URL: http://www.techtv.com/callforhelp/answerstips/story/0,24330,2436994,00.html, (23 Nov. 2003).

[5] Stefan Norberg. “Building a Windows NT Bastion Host in Practice”. URL: http://www.blacksheepnetworks.com/security/info/nt/ntbastion/, (23 Nov. 2003).

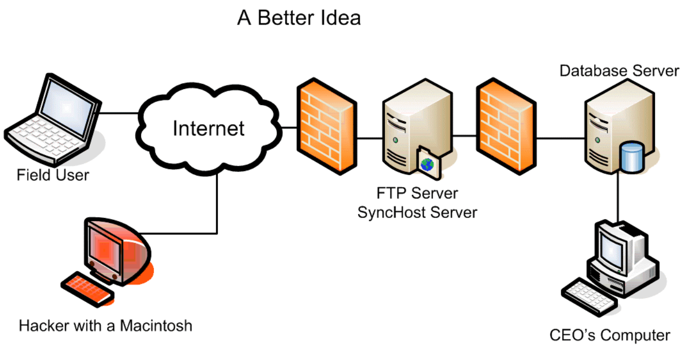


Figure 3 - Using Firewalls

In this example a hardware firewall will ensure only FTP traffic reaches (or leaves) the FTP server. If the firewall includes an FTP proxy, incoming connections can be checked for validity and unused FTP commands can be rejected. This makes it harder for the Mac Hacker to exploit the FTP Server with a buffer overrun or malformed command. In turn, the Database Server is protected with a firewall rule that only allows connections from the SyncHost Server.

While this configuration is popular with smaller companies, a larger company's security team would probably be uncomfortable with the risk of exposing a database connection to the FTP Server. The CEO's bank account may be relatively safe, but a Mac Hacker who manages to manipulate the FTP server could retrieve all the data from the Database Server.

One solution is to add more firewalls:

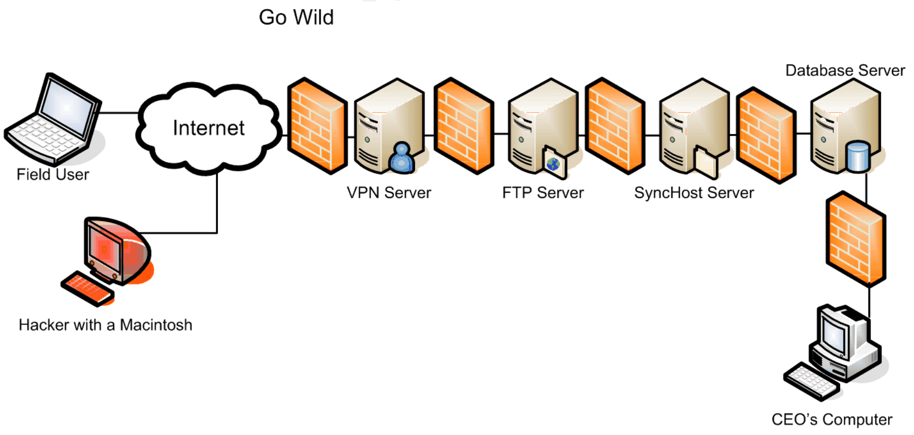


Figure 4 - Defense in Depth

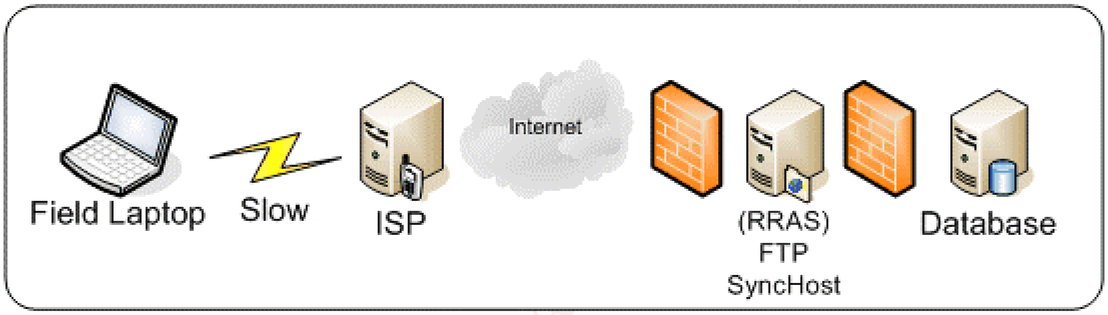
It now becomes much more difficult for the Mac Hacker. Please note that although there are five firewalls shown in the example Figure 4 - Defense in Depth, this could be implemented with one firewall that has six interfaces.

Architecture Overview

This paper discusses Windows Security topics and how they can be applied to three typical data synchronization scenarios. To cover each scenario in depth is far too much material. Rather, examples throughout the paper will cover specific security concerns of these scenarios and demonstrate best practices.

Case 1 - Unmanaged

This scenario is the most common in the field today. This architecture is usually implemented by small companies with a limited budget, often with part time or inexperienced IT staff.



The field laptops are not managed by a central IT group. They are personally owned by the field users and include a variety of hardware brands, Windows versions, and pre-existing problems.

Field users have analog bag phones, digital cell, or older (9600 baud) satellite connections to dial a nearby rural ISP. Experience has shown better network connections by dialing a rural Internet Service Provider (ISP) over a company hosted dial-up (RRAS for instance)[6] with unmanaged laptops.

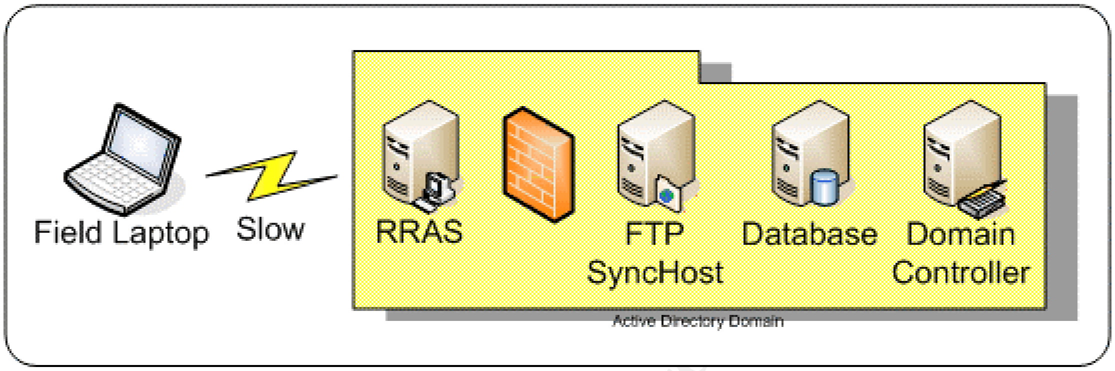
The company configures a firewall (often with outside help) and a single internet-connected server running FTP and SyncHost. The company may also install Routing and Remote Access (RRAS) for a PPTP-based VPN so field laptops can connect to the FTP Server securely. Active Directory is not used in the DMZ and no Certificate Authority is available.

A second firewall is placed between this server and the database server.

[6] Although no data is shown to prove the statement, historical experience would show this is true. The most likely explanation is that in rural locations the cell provider and local ISP are the usually same company. Another possibility is that an ISP may invest in more tolerant equipment and have more robust, tested modem configurations.

User Authentication is required for the FTP Server and the Database Server. A single (but not anonymous) FTP login is added to the local SAM database for all field users[7]. However, a unique login for each field user is required for the database. An outside company is hired for database administration. Once the logins are created, they are seldom changed.

Case 2 – Semi-Managed



In this scenario a mid-sized company with a dedicated IT staff manages a pool of laptops that are assigned to field users. Before going out into the field they are ghosted with a Windows 2000 image, complete with the current service pack and relevant hot-fixes, anti-virus software with current definitions, and Windows Script Host. The laptops are also members of the internal Active Directory domain.

Once in the field, the laptops connect with digital cell phones (with boosters) or CPDC (1X) to the corporate Routing and RAS Server. Because of the slow network speeds the laptops cannot fully participate in Active Directory Group Policy from the field[8], but they are authenticated to RRAS using their Active Directory authentication.

The FTP Server logins are also authenticated on a per user basis and managed using Active Directory.

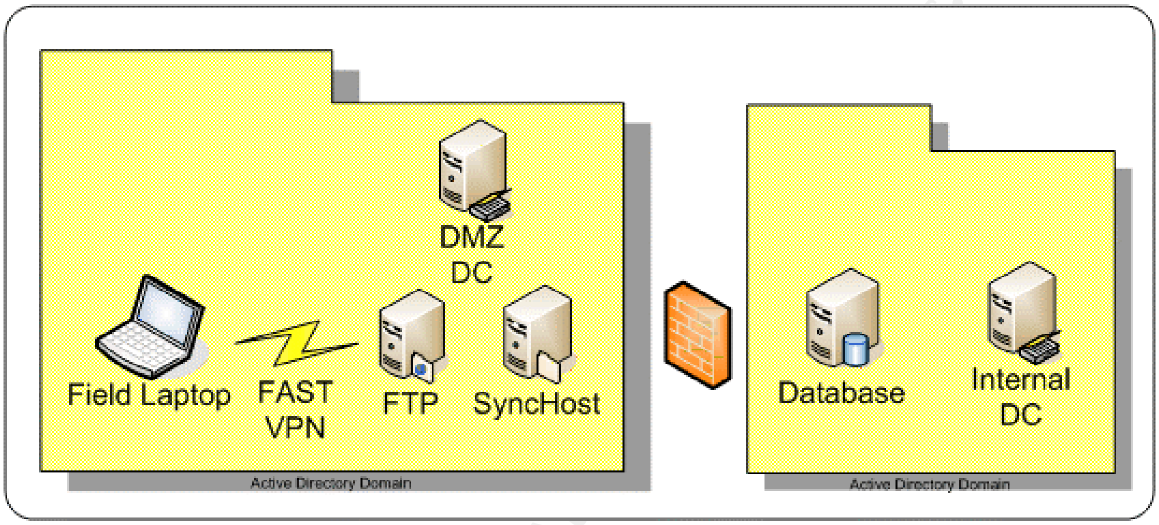
[7] Poor security practice, but this happens when the company lacks process and tools to manage the FTP accounts in the DMZ and/or the project lacks a long-term admin resource. In other cases, passwords are rarely changed because of the difficulty of communicating to the field and the field users' novice computer skills in changing the FTP password in the Program Client.

[8] Both the user configuration and computer configuration of Group Policy have a bandwidth threshold to define a slow link (default is 500Kbps). Under this limit, as the field laptops will be, only the security settings, registry settings, EFS Recovery Policy, and IPSec policy will be applied (by default). Some settings can be overridden.

The database logins are not Active Directory integrated (SyncHost does not support trusted SQL Server logins).

The laptops are returned to head office on a regular schedule for maintenance and upgrading.

Case 3 – Managed



In this environment a large company has invested significant resources to build a satellite WAN to all rig sites. IP traffic on the WAN is encrypted with Cisco networking equipment. Although this case is uncommon, the Oil & Gas industry is currently enjoying great prosperity and fast network infrastructure is quickly becoming accessible to even the most remote locations.

An Active Directory domain has been created for the WAN that is completely isolated from the internal AD domain. Field employee accounts are maintained in the WAN Active Directory (of which the FTP Server and SyncHost Server are also members). Field laptops are built by IT department to participate in the WAN AD and are connected with a fast 1 Mb connection 24 hours/day.

The Database server lies behind a firewall and accounts are not Active Directory integrated (as per the SyncHost requirement). The diagram is not meant to imply the machines in the DMZ are not protected by firewalls as well.

Case 4 – Citrix/Terminal Server

If field laptops are unmanaged, a solution like Citrix MetaFrame[9] provides a secure and effective way to access the Program client. Citrix is only an option when a sustained bandwidth of 20Kb is available[10] (in practice 30Kb is more practical).

There are many obvious administrative advantages of using Citrix. Especially on unmanaged laptops, the IT department regains control of the client desktop and only has to get the Citrix client running opposed to the Program Client, OS updates, patches, etc. (all in an often hostile already misconfigured windows installation).

However, one disadvantage is the inability to work offline if a network connection is not available. It will also result in longer network connections.

[9] "Citrix MetaFrame Access Suite". URL: http://www.citrix.com/, (23 Nov. 2003).

[10] As mentioned at URL: http://www.tushaus.com/Sol/Communications/RemoteAccess/Citrix.asp, (23 Nov. 2003).

Laptop

The Field laptop is the most challenging to secure, especially when the laptops are unmanaged and on slow dial-up network connections.

Communicating Expectations

A written policy explaining the IT group's security expectations and guidelines should be communicated to users, especially if the laptops are on slow connections and are not remotely managed.

A company may want to consult a lawyer to discuss legal ramifications of new policies before implementing them. Policies can cover acceptable use, virus scanning, and use of VPN/Dial-up for example. The SANS Security Policy Project contains a library of example policies[11]. Many universities have published laptop guidelines[12] that can be used as a reference as well.

If update media is provided to clients with slow network connections, the installation procedures should be well documented.

Program Client Installation and Updates

The Program Client is usually provided as a self-extracting InstallShield installer (non-MSI) about 40Mb in size (compressed). Local Administrative rights are required to install.

The confidentiality of the install varies from client to client. Large customers that have custom versions of the software and/or provide initial data (see the following section on seeding the Program Client's local Access Database) may need to prevent other people from accessing the installation media. A standard install would not contain sensitive information.

The program vendor does not provide application patches or updates. New installs will automatically upgrade and patch existing installs. So a patch is also 40Mb!

[11] "The Sans Security Policy Project", URL: http://www.sans.org/resources/policies/, (12 Dec. 2003).

[12] An example made by Indiana University can be seen at http://www.itso.iu.edu/howto/laptop/, (23 Nov. 2003).

Physical Media

Field users with slow network connections will likely install with physical media.

Most installations are done using a CD or USB Key prior to the field user traveling to the remote field site. It is also common for the software vendor to visit users in the Field and perform the installation and initial configuration.

The install can be customized and scripted to help novice field users successfully install on their laptops.

If confidential, after the software is copied to the laptop the physical media should be stored in a safe place or destroyed[13] before being discarded.

Example: Create a Custom CD silent Install

The Program Client can be uncompressed into a temporary folder with the command:

```
setup.exe /extract_all:C:\Temp
```

Where C:\Temp is the folder the setup files will be placed in. The files extracted to C:\Temp make up the CD Image of the program install. One of the files in the directory is named “setup.iss”. This file is a recorded script that will complete the prompts and paths in order to do an unattended install.

A new script can be recorded by running setup from C:\Temp with a /r parameter:

```
setup.exe /r
```

This will walk the administrator through an install. All the keystrokes and install selections are recorded to %windir%\setup.iss. When the installation is complete the administrator will copy the “setup.iss” script from %windir% to C:\Temp, overwriting the default script already there.

The setup can now be run silently with the command:

```
setup.exe /s
```

[13] Really really destroyed. No sense allowing someone to take your database out of the garbage.

The CD can also include an “autorun.inf” file that will run commands when the CD is placed in the drive[14]. To automatically run the setup program silently the “autorun.inf” file only needs to include:

```
[autorun]
open=”setup.exe /s”
```

If additional work needs to be done before installation, the “autorun.inf” file can run a script or batch file that performs some initial actions and then runs the setup file. The advantage of a batch file is it will run on any Windows version without additional software. This can be a factor in an environment with a large number of uniquely configured unmanaged laptops.

A batch file to remove an existing report directory (something the update feature of the install is unable to do) before installation would look like this:

```
@ECHO OFF

REM  Check for the OS
If "%OS%" == "Windows_NT" goto WINNT2KXP
goto WIN9X

:WINNT2KXP
REM ==================================================
REM STEP 1:  Remove the existing folders and reports
REM ==================================================
ECHO Removing Reports Directory
RMDIR /S /Q “C:\Program Files\reports\Default"
goto END

: WIN9X
REM ==================================================
REM STEP 1:  Remove the existing folders and reports
REM ==================================================
ECHO Moving Default Reports Directory to reports.bak
CD “C:\Program Files\reports”
MOVE /Y Default Default.bak
CLS

:END

ECHO Run the Setup
D:\setup.exe
```

[14] This feature can be disabled (or enabled) with the registry value NoDriveAutoRun and/or NoDriveTypeAutoRun in HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer. Clearing the values of both will enable autorun.

Be aware that some DOS commands have different parameters between Windows versions (and some are not available). In the above example Windows 9x uses the MOVE command because the Windows 9x version of RMDIR cannot be run without user interaction.

The advantage of a scripting language, like vbscript, is that more powerful functions can be created (like finding the install location of a program from the registry for instance). The disadvantage is the scripting language may not be installed on all laptops.

One solution is to include the scripting language installs on the distribution CD. In the case of Microsoft Windows Script Host (WSH provides vbscript), there are two installs; one for Windows 2000 and XP and a separate install for NT 4, Windows 9x, and ME. A batch file can check to see if the Windows Script Host is installed and install the correct one:

Example: Install Windows Script Host (Case 1, 2)

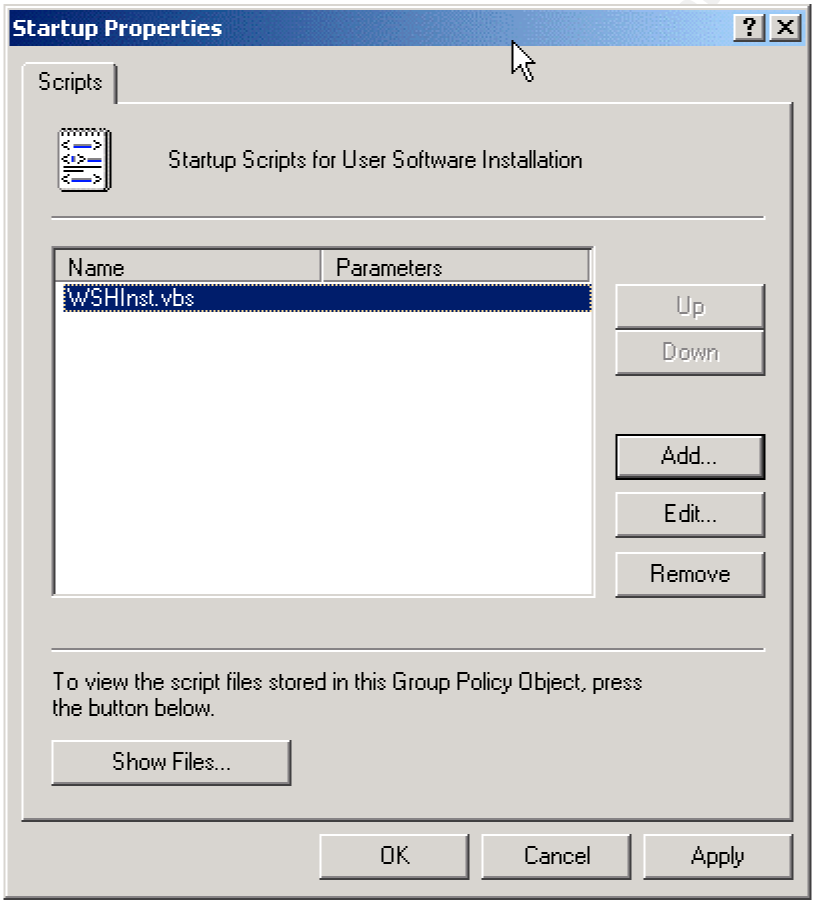
One of the challenges of this script is to determine if the OS is Windows NT or 2000/XP. This can be done with the “gettype.exe” utility from the Windows 2000 Resource Kit.

```
@ECHO OFF

REM  Check for the OS
If "%OS%" == "Windows_NT" goto WIN2KXP
goto WINNT9X

:WIN2KXP
REM ================================================
REM Gettype.exe from the Windows 2000 Resource Kit
REM ================================================
gettype.exe

if ERRORLEVEL=9 goto GETTYPERR
if ERRORLEVEL=1 goto WINNT9X

REM ================================================
REM test if the wscript.exe file is present (assumes default location)
REM if not run the 2K/XP version of WSH (scripten.exe)
REM ================================================
IF NOT EXIST %windir%/system32/wscript.exe scripten.exe
goto END

: WINNT9X
REM ================================================
REM test if the wscript.exe file is present (assumes default location)
REM if not run the NT/9X version of WSH (scr56en.exe)
REM ================================================
IF NOT EXIST %windir%/wscript.exe scr56en.exe
goto END

:GETTYPERR
echo gettype.exe not found.
goto END

:END
```

Example: Publish Script in GPO (Case 3)

If the laptop is a member of Active Directory, the script can be pushed out though Group Policy. In this example I push it out with a computer startup script.

From the Group Policy mmc I open Computer Configuration > Windows Settings > Scripts (Startup/Shutdown). I right-click on the Startup scripts and pick “Properties”.


Startup Properties

Startup Scripts for User Software Installation

Name	Parameters
WSHInst.vbs	

To view the script files stored in this Group Policy Object, press the button below.

Figure 5 - Adding a script to a Group Policy

By selecting “Add…” I open a dialog to select the script and add command-line parameters.

After the Group Policy is complete, it can link to a Site, Domain or OU in the Group Policy Management snap-in (right-click the root policy name > properties > Link tab).

Startup scripts run in the context of the System user and will run before regular user logon scripts. In Case 2, where the laptops no longer have access to the Domain Controller, the scripts are not accessible and do not run.

Electronic Distribution

The install file(s) can also be transferred electronically. How this is done depends on the network connectivity and management infrastructure. Keep in mind that the compressed 40Mb install takes over 2 hours to download over a 36Kb modem connection.

Email (Case 1, 2, 3)

For unmanaged field laptops with a fast enough connection this often means email. If confidential, the file should be encrypted (perhaps in a password protected Zip file) before being transmitted and removed from any servers and/or the email program’s Deleted Items after it has been used (if one exists).

There are many software packages that will bundle a directory into a self-extracting executable, password-protect it, and automatically run a selected file in the archive when it is uncompressed (pkzip, winzip, winrar, etc.).

ZAP Package (Case 3)

In an Active Directory environment the program install can be pushed to Windows Clients (including Windows 98) using a ZAP package. This will place an icon in the “Add/Remove Programs” applet of the control panel that can be used to install the software. In order to use this technology, the client must have a high-speed connection to the software share point (it does not have to be permanent, but ideally would be created on demand).

Example: Create a ZAP package and Distribute with Group Policy

A ZAP file that installs the software with an unattended script would look like:

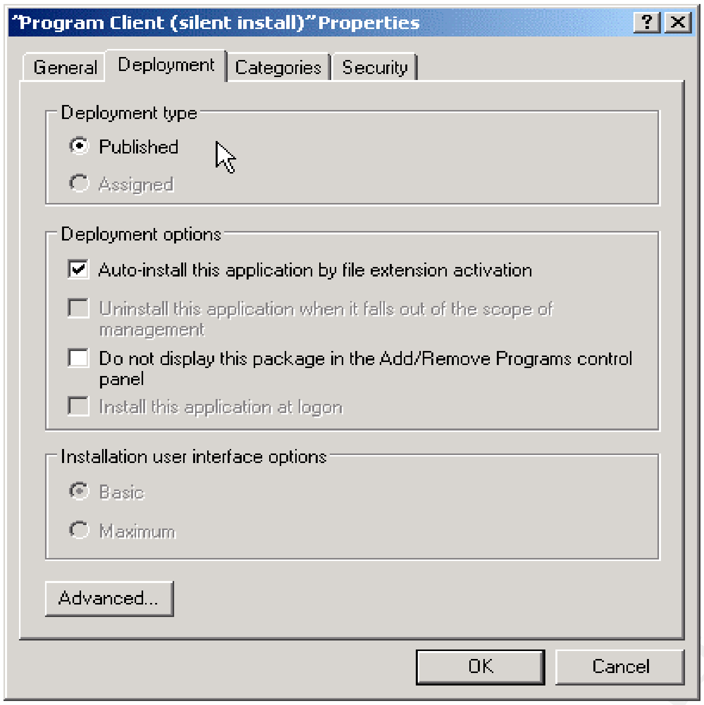
```
[Application]
FriendlyName=”Program Client (silent install)”
SetupCommand=”\\server\share\install\setup.exe” /s
```

I start by creating the network share \\server\share (with read file and share permissions for the field users) and make an install folder in it. Next, I place the program install (setup.exe) in this folder and save the ZAP file there as well (called clientinstall.zap).

I then create a Group Policy called “User Software Installation” to hold the zap package. To do this I start the Group Policy Management mmc snap-in, right-click Group Policy Objects and pick New to create the GPO. After it is created I right-click on the new policy and pick Edit. Zap packages are installed per user, so I go to User Configuration > Software Settings > Software Installation. I right-click it and pick New > Package…

A dialog appears asking to open the .msi file. This example uses a zap package so I change the file type to “ZAW Down-Level Application Packages (*.zap)” and point to the zap file I placed on the network share. The install type is Advanced or Published (with Published you can still set the advanced properties later). I choose Advanced.

The advanced options allow the name to be changed as displayed in Add/Remove programs, to auto-install based on file extension (uncheck, it is not required for the Program Client), whether the package is displayed, and assigned categories. Security can also be set to fine-tune the user’s access to the install.



"Program Client (silent install)" Properties

General | Deployment | Categories | Security

Deployment type

● Published

○ Assigned

Deployment options

☑ Auto-install this application by file extension activation

□ Uninstall this application when it falls out of the scope of management

□ Do not display this package in the Add/Remove Programs control panel

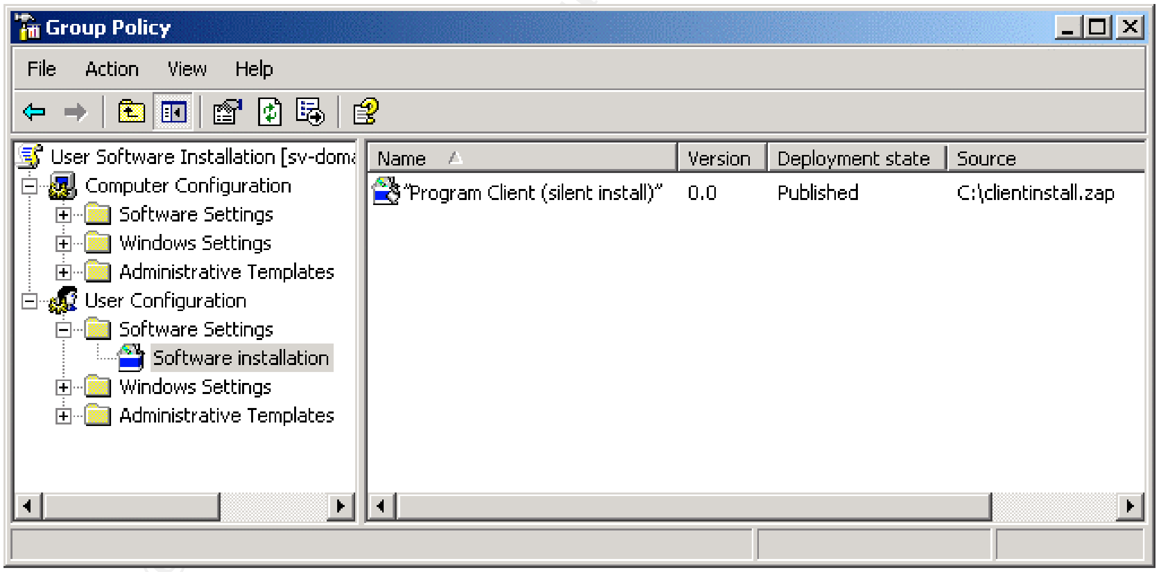
□ Install this application at logon

Installation user interface options

● Basic

○ Maximum

Figure 6 - GPO Zap Install Options



Group Policy

- User Software Installation [sv-dom
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - User Configuration
    - Software Settings
      - Software installation
    - Windows Settings
    - Administrative Templates

Name	Version	Deployment state	Source
"Program Client (silent install)"	0.0	Published	C:\clientinstall.zap

Figure 7 - GPO - Completed Zap Setup

Now that it has been completed, the Group Policy can be linked to domains, OUs, and sites in the Group Policy Management snap-in.

Note that the user requires Administrator or local Power User privileges to install the Program Client and that it can only be applied under the User Configuration of the GPO (not per computer).

MSI Repackage

Although the Program Client install is not an MSI package, it can be repackaged[15] into an MSI installer. Stock Windows 98 and NT computers need the latest MSI installation software before an MSI file can be installed on them. Other software may already have installed MSI, but with unmanaged laptops that cannot be assumed.

Although an MSI package can be run by the user (right-clicking an MSI file will give Install, Repair, and Uninstall options for example) or run by a script, it can also be pushed out using Group Policy to Active Directory integrated laptops.

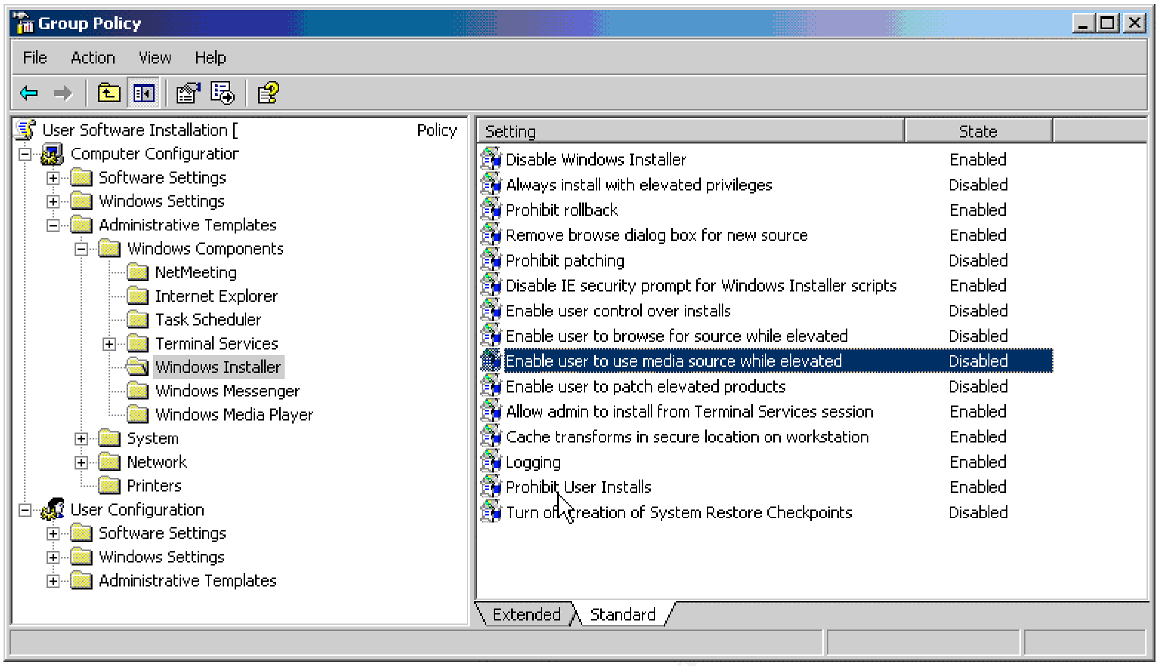
There are several GPO options that are unique to MSI files. The first is you can Assign MSI files to computers as well as users. Assigning to computers is advantageous because users cannot uninstall them and they can be set to install silently and automatically (if the MSI file allows these features).

The security options of MSI itself can be managed. One functional advantage of MSI is it can elevate its privileges so a user can install software that he/she would not normally have permissions to. The down-side is hackers can potentially exploit these privileges. MSI options in the registry can be set to mitigate this risk. They can be managed by Group Policy but they can also be set by Security Templates or ".reg" files on non-Active Directory machines (if permissions allow).

Example: MSI Registry Settings

Many MSI security options can be set through Group Policy. In Case 2 they can be set on the laptops before they are released to the field. In Case 3 they can be pushed out in real time.

[15] See the article "Repackaging Applications for Distribution" at http://appdeploy.com/articles/repack.shtml for pros and cons of repackaging and a link to a list of repackaging tools.



Setting	State
Disable Windows Installer	Enabled
Always install with elevated privileges	Disabled
Prohibit rollback	Enabled
Remove browse dialog box for new source	Enabled
Prohibit patching	Disabled
Disable IE security prompt for Windows Installer scripts	Enabled
Enable user control over installs	Disabled
Enable user to browse for source while elevated	Disabled
Enable user to use media source while elevated	Disabled
Enable user to patch elevated products	Disabled
Allow admin to install from Terminal Services session	Enabled
Cache transforms in secure location on workstation	Enabled
Logging	Enabled
Prohibit User Installs	Enabled
Turn off creation of System Restore Checkpoints	Disabled

Figure 8 - Setting Windows Installer Security Options in Group Policy

The Extended Tab view of each setting includes a description and, in some cases, recommended values. The settings shown in Figure 8 - Setting Windows Installer Security Options in Group Policy provide for improved security (although they should be tested before being released).

For clients that cannot participate in Group Policy, a Security Template or ".reg" file can be created to set the same settings. MSI registry keys are located under the HKEY_LOCAL_MACHINE hive in \Software\Policies\Microsoft\Windows\Installer. Security Templates are covered in a following section.

For example, "Disable Windows Installer" is the DWORD value name "DisableMSI" and has values of 0 (default), 1 (admin only), or 2 (disabled).

A complete list can be pulled from the Administrative Template "system.adm" (found in %windir%\Inf).

Third Party

The Program Client can also be rebundled and distributed through enterprise tools such as Novell's ZENworks for Desktops, Microsoft SMS, or Symantec Ghost. In general these tools require a fast network connection to the client, but in some cases they can be placed on a CD and scripted to run when inserted into the field user's laptop.

Seeding the Program Client's Local Access Database

To begin the synchronization process, the Program Client must select a well (or wells) to synchronize with the Database Server. The first time the program is run, the field user has no wells to select unless the initial data is provided with the Program Install.

Wells are usually created at head office and populated with administrative data (which can still be confidential). Then the well or wells are assigned to a Field User and sent to him/her as required. As with the Installation, the task is to securely distribute this data and safely store it afterwards. In addition to the methods previously described, the data itself can be sent as a password-protected import/export file or a complete Access database (also password-protected).

Wells can also be selected and downloaded through the Sync Process itself (well retrieval) if enabled on the SyncHost Server. If this is allowed (again, it can be disabled on the SyncHost) extra care should be taken in setting up application-level database security so field users can only download wells they are responsible for.

Securing the Client Laptop

No matter how the laptop is managed or connected to the network, once proprietary data is on the laptop it is important to protect it!

Physical Security

With laptops being light and easy to steal, it is imperative that the laptop itself is physically protected.

Laptop Locks

Most laptops have a Universal Security Slot (USS) where a standard security lock can be attached. Those that do not can still be secured with a special adapter. Laptop security locks are keyed or have a combination and are simple to install. As many field users run their laptops from their vehicle or a small high-traffic shack, a laptop lock is one of the simplest and least expensive security options.

Personal Asset Security

There are many products that provide additional security to the laptop including login devices based on biometrics (such as iris and fingerprints[16]) and products that disable the laptop when the owner is too far away[17].

BIOS Protect the Laptop Hard Drive

Most modern laptop BIOSs allow the user to set a boot and a hard drive password. Boot passwords (the password typed when the computer is turned on) can be defeated by clearing the BIOS. The instructions on how to do this for most laptops are easy to find.

The hard drive password is advantageous in that if the BIOS is reset or the hard drive is placed in another computer the data is still encrypted. There is nothing keeping the hard drive from being formatted, however. There are commercial services and products that can remove hard drive passwords[18].

Tracking and Recovery

Special software and hardware are available to monitor the physical location of a laptop and/or report back to a central server if it connects to the internet after being stolen. The web site http://www.stolenlaptop.com/ lists many vendors.

Data Security

Anti-Virus Software

File attachments can be transmitted through the Sync process. Therefore, it is very important client laptops have a commercial anti-virus software package installed with current anti-virus definitions. Obtaining current anti-virus definitions can be an issue for poorly connected remote laptops.

[16] Some examples can be seen at Securenet Solutions. URL: http://www.securenetsol.com/bs_biometric_products.html, (23 Nov. 2003).

[17] See “How XyLoc works”, Ensure Technologies, URL: http://www.xyloc.com/products/technology/technology.html#HowXyLocWorks, (23 Nov. 2003).

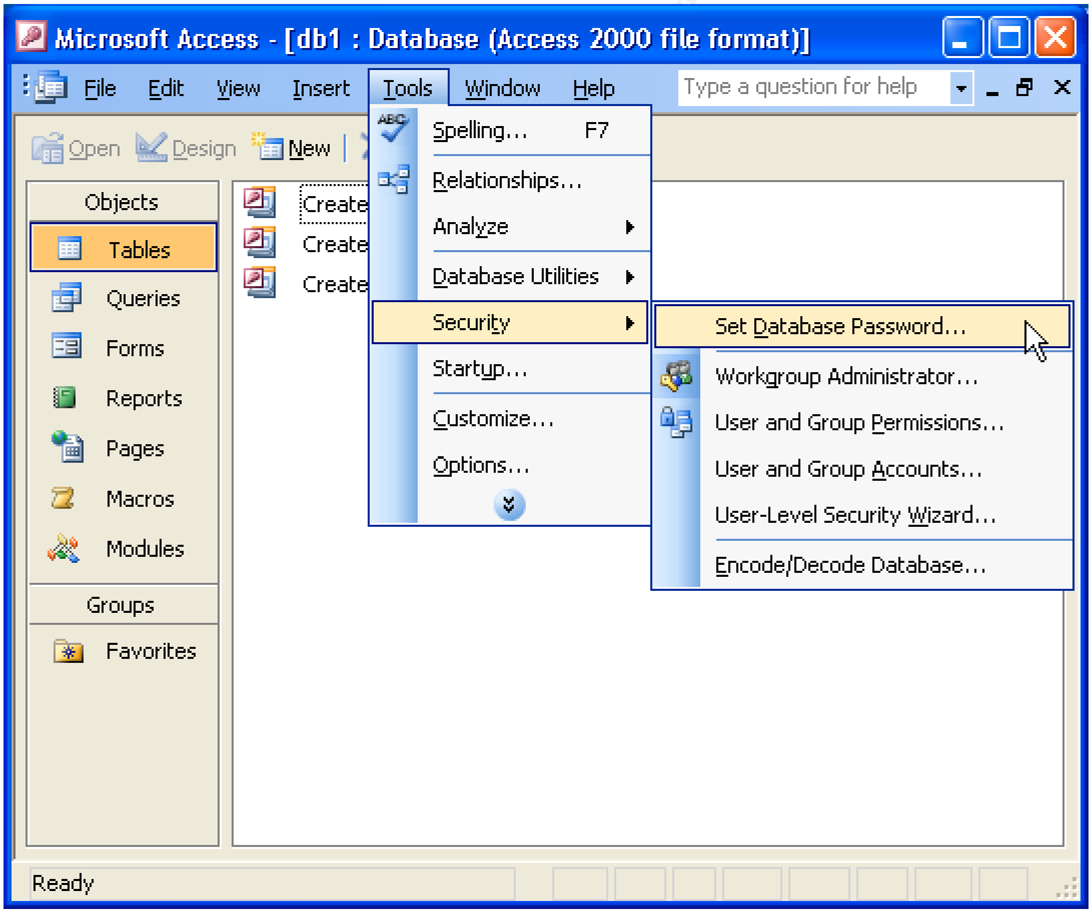
[18] Vogon International claims to have a password cracker pod that can remove and reapply hard drive passwords in 7 – 60 minutes. URL: http://www.vogon-computer-evidence.com/password-cracker-solution.htm, (23 Nov. 2003).

Since attachments are compressed and encrypted, there is no opportunity to scan them until after they are placed in the database. This can be a dangerous backdoor though a company’s virus barriers. A free tool is provided by the software vendor to analyze the central Database and copy the embedded file attachments to a file system so they can be scanned. However, this is done AFTER the data is synchronized.

As with the install program, getting anti-virus updates can be a challenge in the Field. If download speeds are too slow, a distribution method such as update CDs should be considered. If corporate IT has no control over Field Laptops, anti-virus updates should be required by policy (to be applied when possible).

Password Protect the Local Access Database

In Access, the database can (and should) be password-protected. A copy of Microsoft Access[19] is required to set the password.



[19] The version of Access must be later than the current version of the mdb file.

The dialog will only request a password (with verification). The username is "Admin". Be aware that password cracking programs are available[20].

Backup

In the remote rough-and-tumble field environment, it would be convenient to have a backup of the laptop should data be lost or the OS damaged. Most companies synchronize data to head office daily, which in itself is a form of backup.

But there are many laptop backup solutions available that could save hours should the laptop need to be restored (providing the laptop is still working).

Backups should be protected as seriously as the laptop; it is easier to walk away with a tape or CD-R than a laptop. Wise backup advice says:

> Back up all your data.
>
> Back up frequently.
>
> Take some backups offsite.
>
> Keep some old backups.
>
> Test your backups.
>
> Secure your backups.
>
> Perform Integrity Checking[21].

Encrypting File System

If the laptop is running Windows 2000 or XP Professional and NTFS, the user can use the Encrypting File System (EFS) on files to encrypt them. This does not affect the files from the user's point-of-view. The user does not have to enter extra passwords to decrypt files.

[20] "Advanced Office XP Password Recovery". Elcomsoft Proactive Software. URL: http://www.crackpassword.com/products/prs/integpack/officexp/, (23 Nov. 2003).

[21] Ross Williams. "The Tao of Backup". URL: http://www.taobackup.com, (23 Nov. 2003).

There are some issues. When using SMB or FTP to transmit EFS-encrypted files, they are first decrypted and sent in cleartext[22]. On a Windows 2000 stand-alone field laptop, the default recovery agent is the local Administrator account; thus a private key that can decrypt any EFS file on the laptop's hard drive[23] can potentially be retrieved by a hacker. The private key can be exported and removed from the computer with Certificates mmc snap-in.

Since the program client creates temporary files in %TEMP% it is recommended that it be set to use EFS (if EFS is chosen to be used). The Program Client's database folder should also be protected.

The command-line utility CIPHER.EXE can be used as well as the GUI to encrypt and decrypt files. CIPHER.EXE can also be used to create a recovery agent (Windows XP Pro does not have one by default) and re-encrypt EFS files.

Example: EFS on Windows XP Professional

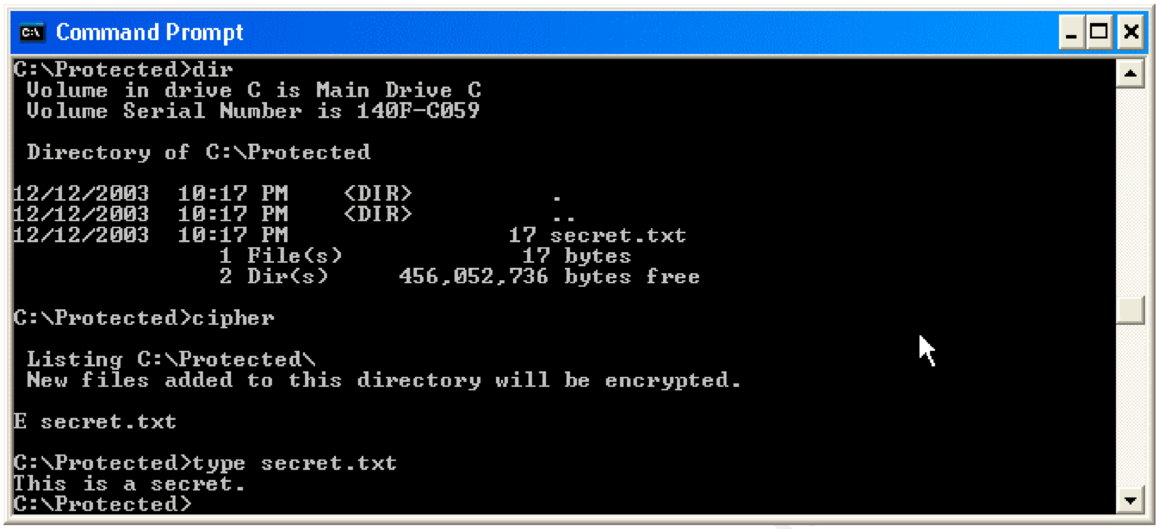
In this example a directory name C:\Protected is created, a file named secret.txt added to it, and the directory and file EFS protected:

```
cipher /e /a C:\Protected
```

Checking the files:

[22] Jason Fossen. Windows 2000 PKI, Smart Cards, and the Encrypting File System. SANS Institute, version 7.2 (2002). 133.

[23] William Boswell, "EFS Best Practices". URL: http://www.informit.com/content/index.asp?product_id=%7BA762B6C0%2D2D1C%2D470D%2DBE7C%2DB78103711CAD%7D, (23 Nov. 2003).



```
C:\Protected>dir
 Volume in drive C is Main Drive C
 Volume Serial Number is 140F-C059

 Directory of C:\Protected

12/12/2003  10:17 PM    <DIR>          .
12/12/2003  10:17 PM    <DIR>          ..
12/12/2003  10:17 PM                17 secret.txt
               1 File(s)             17 bytes
               2 Dir(s)     456,052,736 bytes free

C:\Protected>cipher

 Listing C:\Protected\
 New files added to this directory will be encrypted.

E secret.txt

C:\Protected>type secret.txt
This is a secret.
C:\Protected>
```

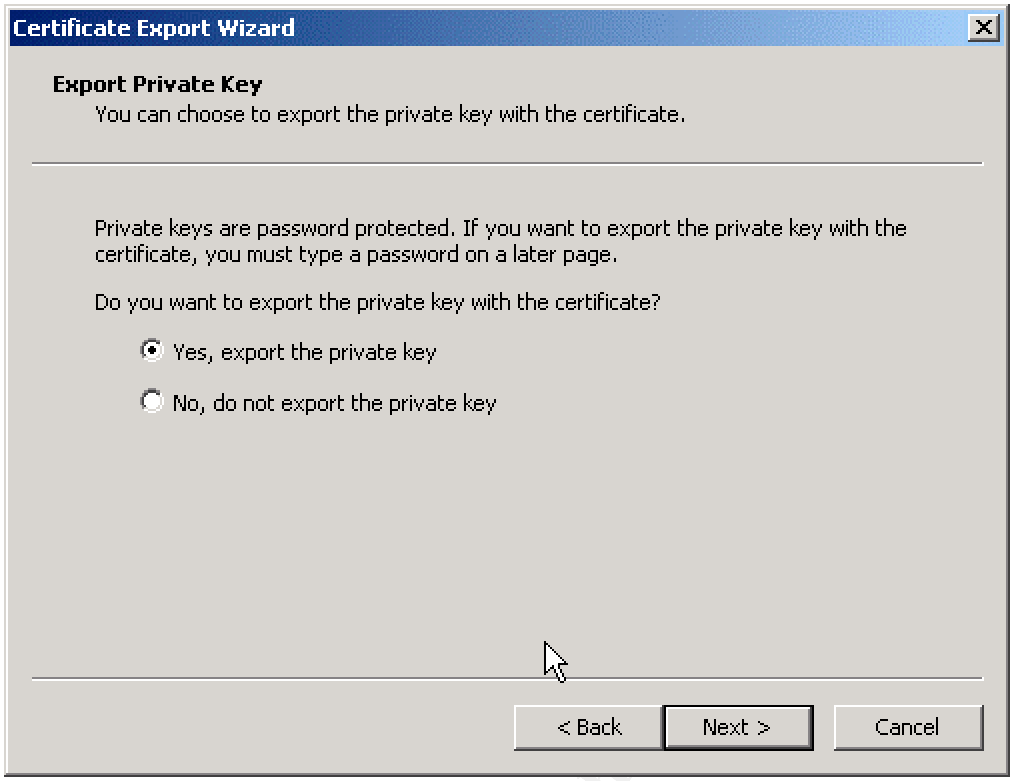
Figure 9 - An Encrypted File with the Certificate Present

The E indicates that secret.txt is protected. I looked at the contents to ensure I could still read it.

The next step is to remove my EFS Certificates to show that without it secret.txt could not be read.

The EFS Certificates are removed by creating a Certificates mmc snap-in for the current user. Under Personal > Certificates I find my EFS certificate and back it up:

I right-clicked the certificate > All Tasks > Export… The Certificate Export Wizard starts and I click Next to see the following:



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

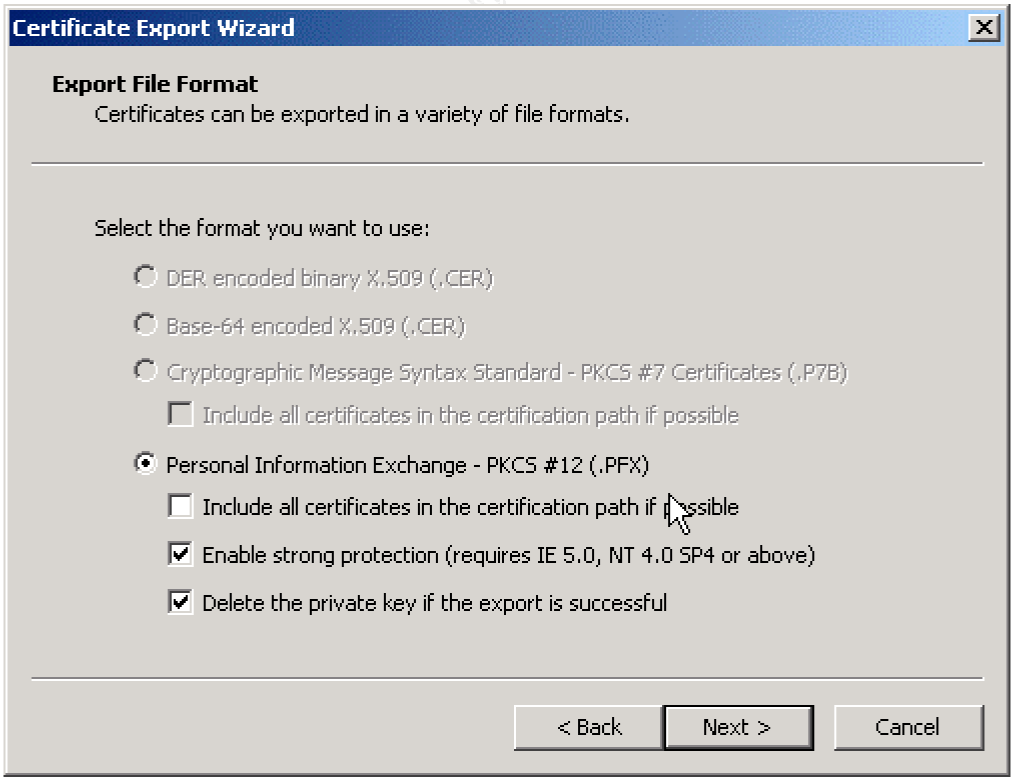
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

In this Example I want to export the private key because I plan to delete the certificate to prove I can not view the EFS protected files without it.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

☑ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

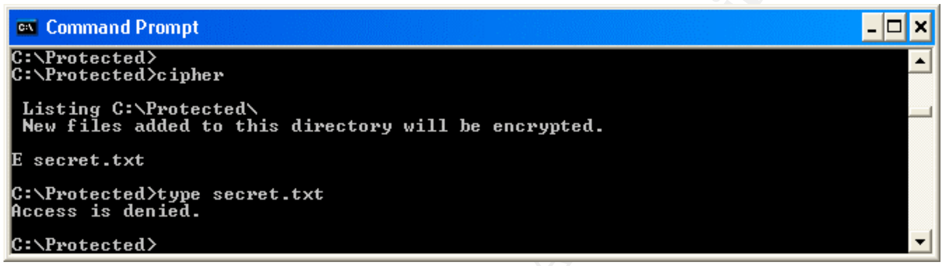
☑ Delete the private key if the export is successful

I choose to delete the private key. If I intend to import on another machine, I would also select “Include all certificates in the certification path if possible”. Click Next.

I enter a good password (see the password section) and pick a file name to store the key. In high-security environments I would store the key on removable media, like a floppy disk.

Then I remove my EFS Certificate by right-clicking on it in the Certificates snap-in and picking Delete.

Now I come to a small snag. Even though I removed the certificate, it is still cached and I can view the contents of secret.txt even though the EFS Certificate is removed. However, when I log off and back on I see the following:

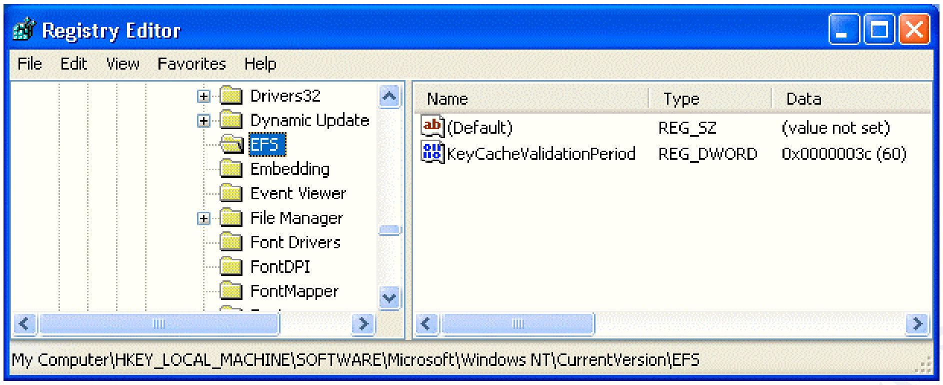


```
C:\Protected>
C:\Protected>cipher

 Listing C:\Protected\
 New files added to this directory will be encrypted.

E secret.txt

C:\Protected>type secret.txt
Access is denied.

C:\Protected>
```

Figure 10 - An Encrypted File Without the Key

To improve performance Windows XP caches EFS Certificates for 60 minutes. The one hour EFS certificate cache can be configured[24]. The lower the time, the more responsive the system is to certificate changes. But this is at the expense of performance. The value in seconds can be entered in the registry:

[24] “Registry Tip #8: XP registry values to tune EFS caching”. URL: http://is-it-true.org/nt/xp/registry/rtips8.shtml, (12 Dec. 2003).



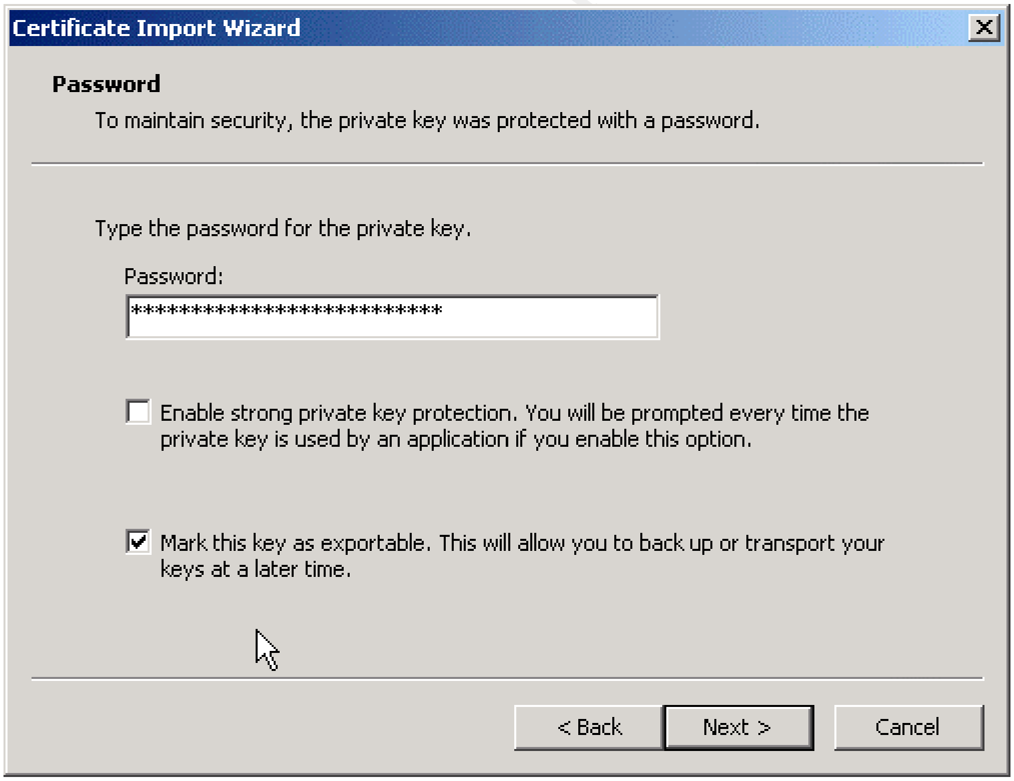
Name	Type	Data
(Default)	REG_SZ	(value not set)
KeyCacheValidationPeriod	REG_DWORD	0x0000003c (60)

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS

Figure 11 - The "sounds good but doesn't work" KeyCacheValidationPeriod Key

However, my attempts to get this to work failed. My default cache period was many hours and changing the registry value seemed to have no effect (even after rebooting). I've shown the key in Figure 11, perhaps you'll have better luck.

Restoring the key allowed me to access the file again instantly. When restoring the certificate I was sure not to check "Enable strong private key protection" or I would have had to enter the certificate password each time it is used:



Password
To maintain security, the private key was protected with a password.

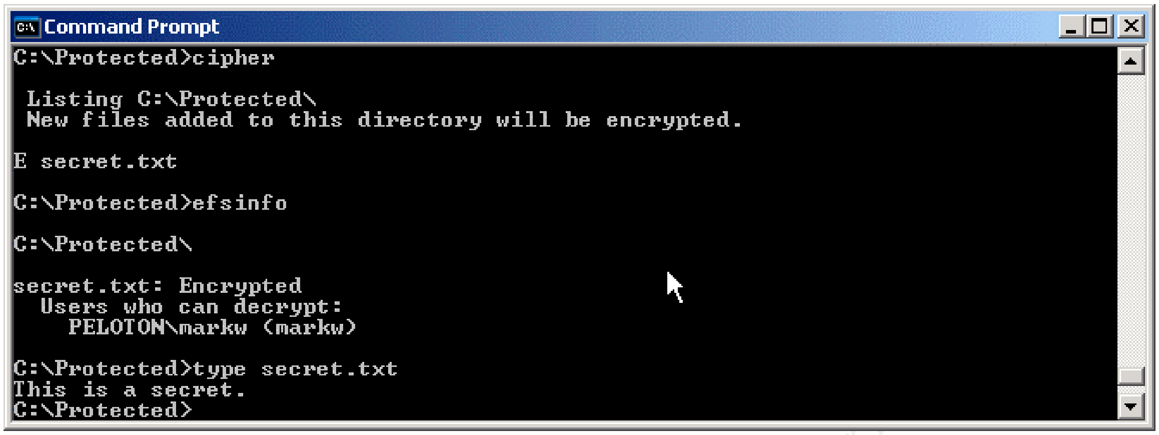
Type the password for the private key.

Password:
****

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

After importing the file can be viewed again:



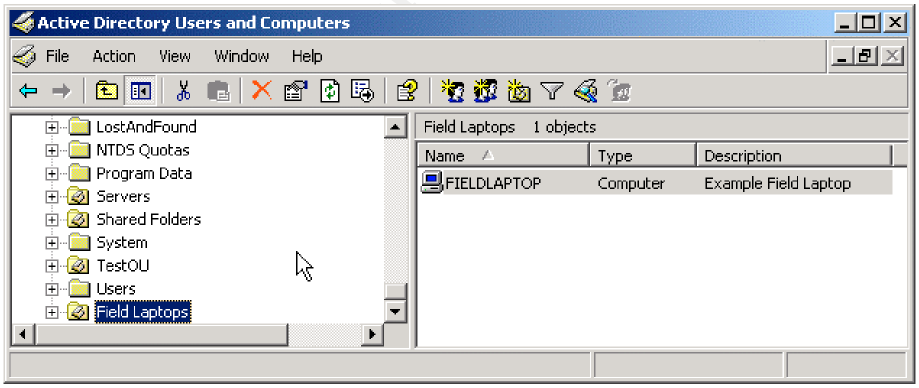
```
C:\Protected>cipher

 Listing C:\Protected\
 New files added to this directory will be encrypted.

E secret.txt

C:\Protected>efsinfo

C:\Protected\

secret.txt: Encrypted
  Users who can decrypt:
    PELOTON\markw (markw)

C:\Protected>type secret.txt
This is a secret.
C:\Protected>
```

Example: Adding Recovery Agents with Group Policy

Managed laptops that are members of Active Directory (Case 3), even if temporarily so (Case 2), can have recovery agent(s) added through Group Policy.

If field users are encouraged to use EFS, it is only a matter of time before something happens so the field user cannot decrypt an important file. So it is the wise Administrator who adds known EFS Recovery Keys to the laptops before they are sent to the field.

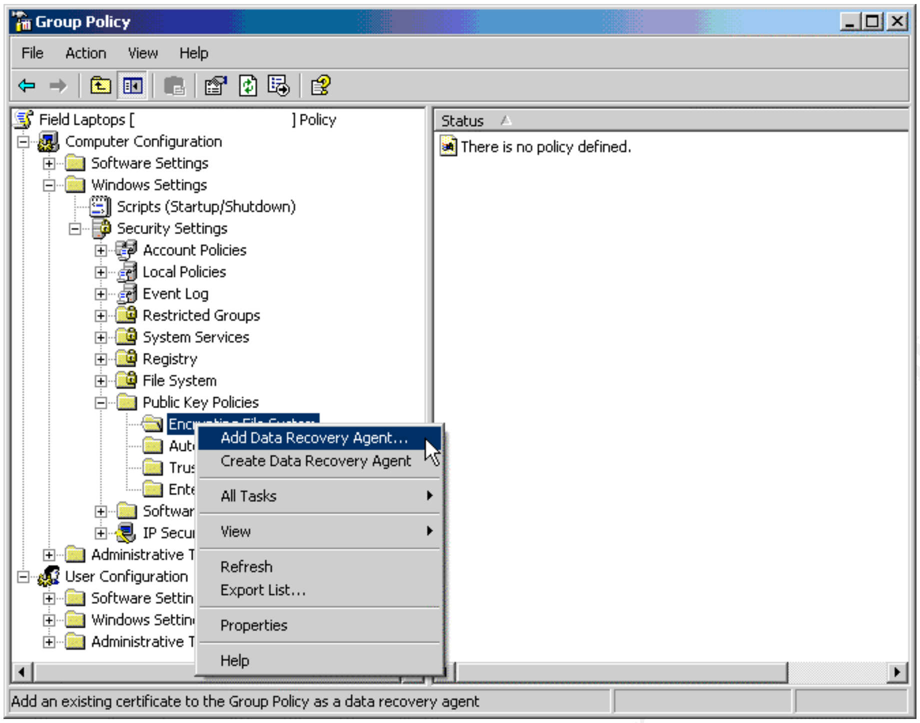
Taking Case 2, a group of laptops are imaged and prepared for release to the field. They are all Active Directory domain members and have been placed in an OU called Field Laptops.



Field Laptops 1 objects

Name	Type	Description
FIELDLAPTOP	Computer	Example Field Laptop

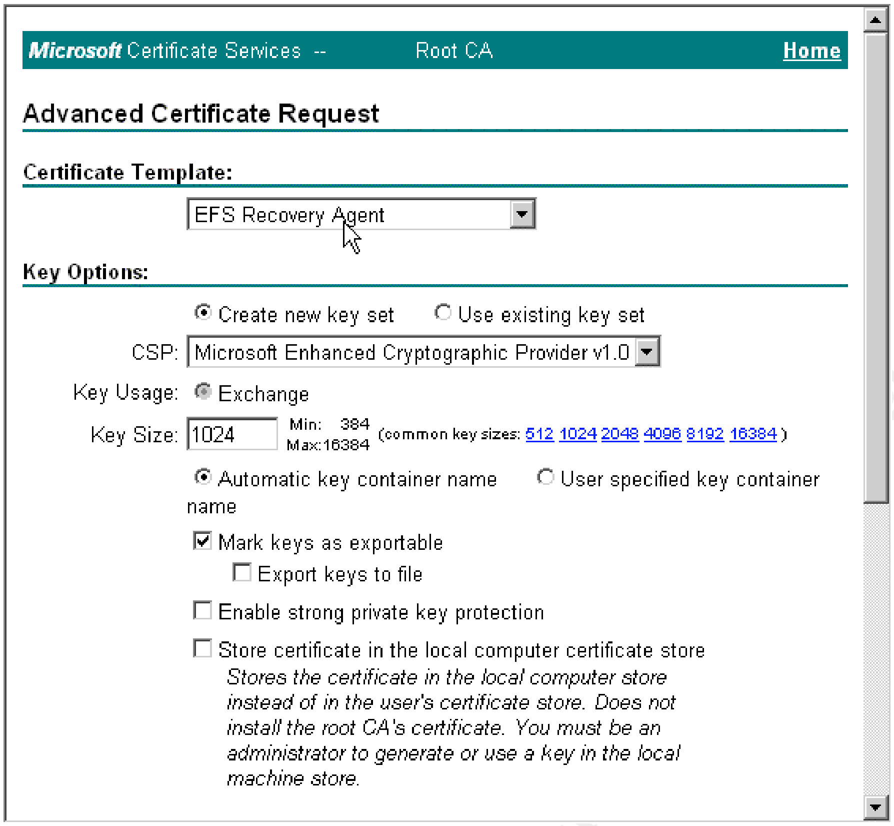
A Group Policy is created to add new data recovery agents:



There is no policy defined.

Add an existing certificate to the Group Policy as a data recovery agent

If a Certificate Authority is available, a new data recovery agent can be created with “Create Data Recovery Agent”. In this example, we do it the long way and request a key first.



Microsoft Certificate Services -- Root CA **Home**

Advanced Certificate Request

Certificate Template:

EFS Recovery Agent

Key Options:

● Create new key set ○ Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: ● Exchange

Key Size: 1024 Min: 384 Max:16384 (common key sizes: 512 1024 2048 4096 8192 16384)

● Automatic key container name ○ User specified key container name

☑ Mark keys as exportable

□ Export keys to file

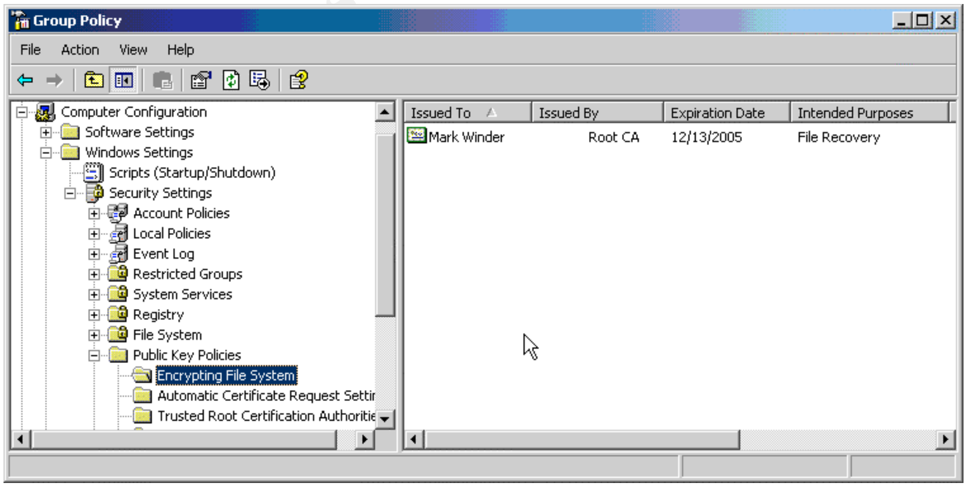
□ Enable strong private key protection

□ Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Request a new EFS Recovery Agent from the CA. In this example, we'll select "Export keys to file" and save them on a floppy with a filename of efs.cer.

Next, select Add Data Recovery Agent… and start the wizard. Pick Browse Folders and select efs.cer from the floppy. After importing, we see the new EFS Recovery certificate has been added:

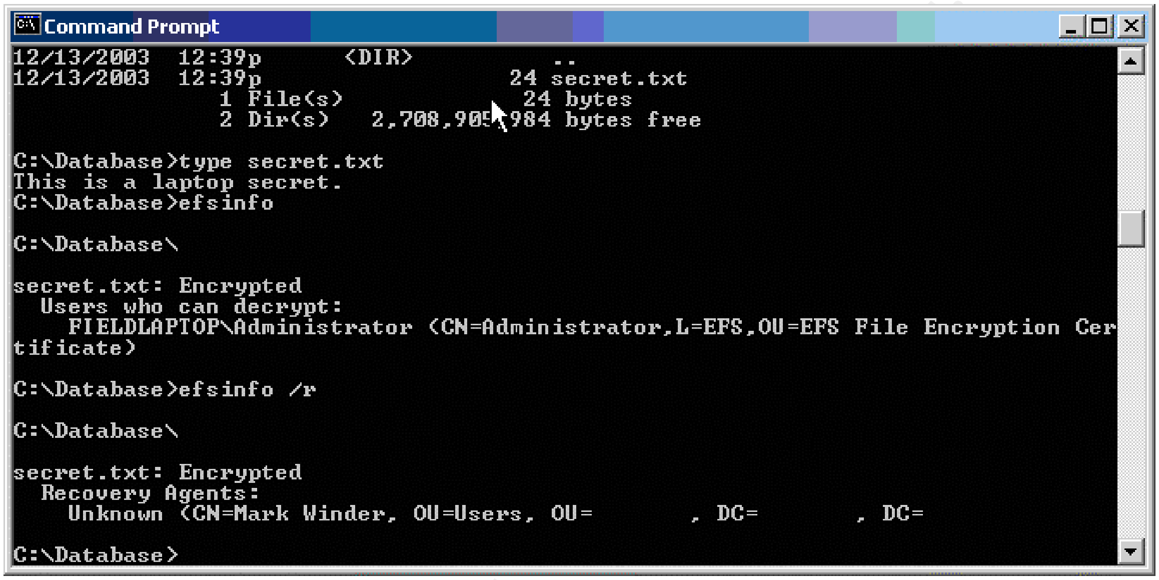


Computer Configuration
- Software Settings
- Windows Settings
  - Scripts (Startup/Shutdown)
  - Security Settings
    - Account Policies
    - Local Policies
    - Event Log
    - Restricted Groups
    - System Services
    - Registry
    - File System
    - Public Key Policies
      - Encrypting File System
      - Automatic Certificate Request Settir
      - Trusted Root Certification Authoritie

Issued To	Issued By	Expiration Date	Intended Purposes
Mark Winder	Root CA	12/13/2005	File Recovery

In the Group Policy Management mmc snap-in, we next link this Group Policy to the Field Laptops OU.

After the group policy has propagated (60 to 120 minutes) the laptops are taken into the field. In this example, a disconnected user has enabled EFS on the Database folder and made a text file. To prove the recovery agent was applied, the EFSINFO.EXE utility is used (/r shows the recovery agents):



```
12/13/2003  12:39p      <DIR>          ..
12/13/2003  12:39p                  24 secret.txt
               1 File(s)             24 bytes
               2 Dir(s)   2,708,905,984 bytes free

C:\Database>type secret.txt
This is a laptop secret.
C:\Database>efsinfo

C:\Database\

secret.txt: Encrypted
  Users who can decrypt:
    FIELDLAPTOP\Administrator (CN=Administrator,L=EFS,OU=EFS File Encryption Cer
tificate)

C:\Database>efsinfo /r

C:\Database\

secret.txt: Encrypted
  Recovery Agents:
    Unknown (CN=Mark Winder, OU=Users, OU=       , DC=        , DC=

C:\Database>
```

Windows Security

OS Security is somewhat dependent on the Windows Operating System version. Later versions have more security features and are supported by Microsoft. Although the Program Client runs on Windows 98, from a security standpoint Windows 2000 or later is recommended.

Lock Unattended Laptop

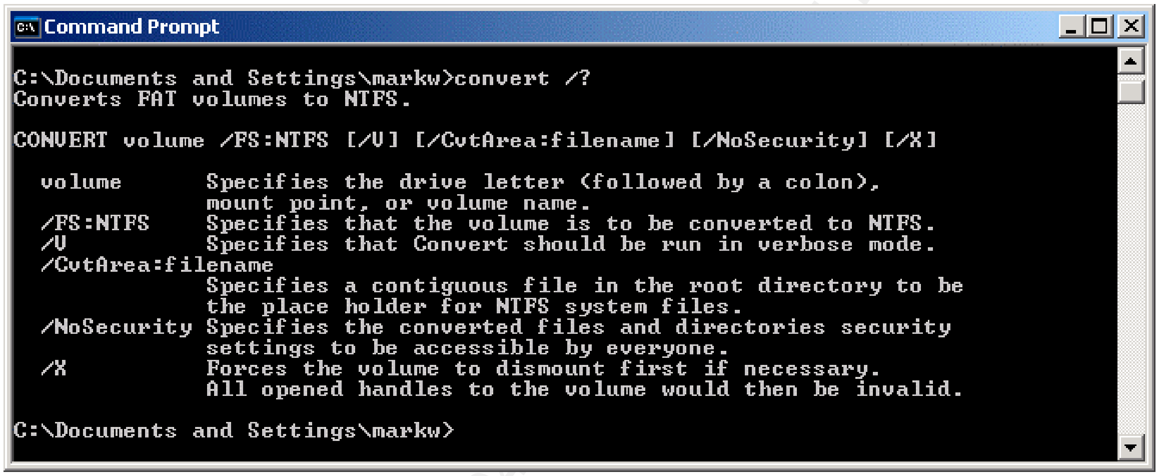
If a laptop is left unattended, it should be locked (ctrl-alt-del in 2000, windows-L in XP) or disabled in some way so another person cannot use the laptop with the logged-in user's credentials.

Setting up a password-protected screen saver with a short timeout helps forgetful users.

Use NTFS

Laptops running Windows NT, 2000, and XP should use NTFS and protect the files, especially the local database, with Access Control Lists (ACLs) that limit permissions on the database folder. The Program's user requires read and write permissions to the database folder. If the database is backed up, the backup user requires read access.

To update a FAT system to NTFS, the command is "convert" (available on Windows OSs that support NTFS). In Windows NT and 2000, the resultant NTFS drive initially gives Full Control rights to the Everyone group.



```
C:\Documents and Settings\markw>convert /?
Converts FAT volumes to NTFS.

CONVERT volume /FS:NTFS [/V] [/CvtArea:filename] [/NoSecurity] [/X]

  volume      Specifies the drive letter (followed by a colon),
              mount point, or volume name.
  /FS:NTFS    Specifies that the volume is to be converted to NTFS.
  /V          Specifies that Convert should be run in verbose mode.
  /CvtArea:filename
              Specifies a contiguous file in the root directory to be
              the place holder for NTFS system files.
  /NoSecurity Specifies the converted files and directories security
              settings to be accessible by everyone.
  /X          Forces the volume to dismount first if necessary.
              All opened handles to the volume would then be invalid.

C:\Documents and Settings\markw>
```

Use Good Passwords

Selecting a good password helps secure files (including the local database) that are protected with NTFS File System permissions. If a FAT file system is used, a good OS login password is meaningless—FAT does not support file permissions.

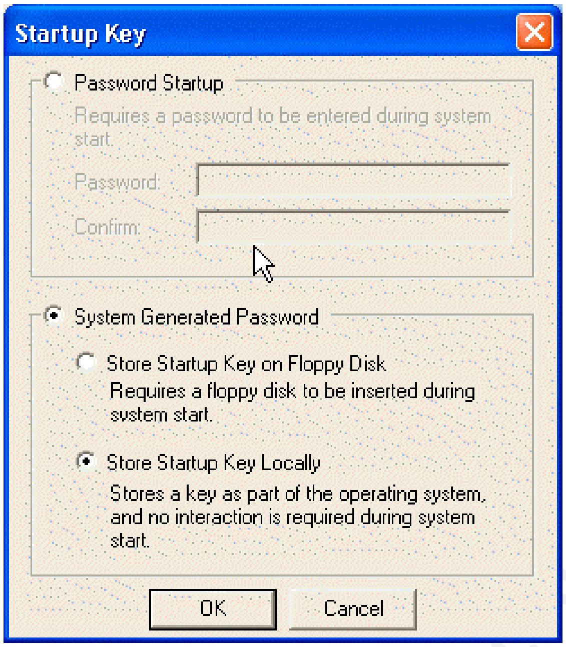
Long passwords (or passphrases) with some complexity (include numbers or symbols) are ideal. It is recommended that an 8+ character password be used for medium security and a password 14+ characters long be used for high security[25].

It is extremely important that field users understand they should not share passwords, even at the expense of convenience!

[25] Jason Fossen. DNS and Group Policy. SANS Institute, version 1.1 (2002). 83.

Protect the System Key

The system key is a 128-bit RC4 key used to protect account databases (local or Active Directory), the registry's "LSA Secrets", and other keys. SYSKEY.EXE is available for Windows NT 4 (SP3+), 2000, XP, and .Net. When this utility is run and Update is pressed, the following dialog is shown:



Startup Key

○ Password Startup

Requires a password to be entered during system start.

Password:

Confirm:

● System Generated Password

○ Store Startup Key on Floppy Disk

Requires a floppy disk to be inserted during system start.

● Store Startup Key Locally

Stores a key as part of the operating system, and no interaction is required during system start.

By selecting Password Startup the operating system does not boot until the password has been entered. This makes remote management of the laptop more difficult, but adds another layer of security.

The Startup Key can also be stored on a floppy. If the BIOS boot order is set right (boot off Hard Drive), the floppy can be left in the drive for convenience or removed for security. It can also be backed up. If a floppy disk is lost or compromised, the Startup Key can be reset by changing to password protection and back.

Security Templates

Many security settings can be configured and applied at once with Security Templates. Security templates can be managed with an mmc snap-in named "Security and Configuration Analysis" or with a command-line tool named secedit.exe.

Security Templates can be applied to machines that are not part of an Active Directory (but if they are, Security Templates can be applied through Group Policy). Windows NT (SP 4+), 2000 or XP running NTFS is a requirement.

Security Templates can be combined on a machine (if there are conflicts the last Template applied wins).

Extreme care should be taken in installing a Security Template on an unmanaged laptop. Security Templates set many policies, permissions, and settings; this could cause a mismanaged laptop to run poorly, applications to crash, or worse. However, on a managed laptop the IT department can use Security Templates to quickly and safely set these same settings. The Windows XP version of secedit.exe has a command-line parameter named /generaterollback that is run before applying a new template. It creates a template of the current settings so the new template can be backed out if there are problems with it.

Templates can be loaded into the Security Configuration and Analysis tool, an mmc snap-in.

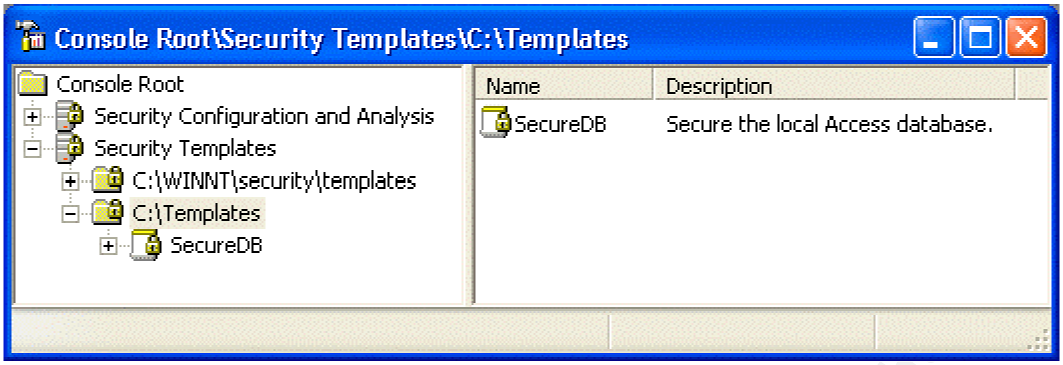
There are many publicly available tested Security Templates[26]. It is important to look carefully at these templates before applying them; the high security templates may actually remove desired functionality.

Example: Creating a Security Template to Set NTFS Permissions

A simple Security Template can be created to change the file permission on the database (Database.mdb) so only a local Administrator or Power User has access.

I start in the Security Templates mmc snap-in:

[26] For example, "Security Recommendation Guidelines", URL: http://www.nsa.gov/snac/index.html, (Dec 10, 2003).



Console Root\Security Templates\C:\Templates

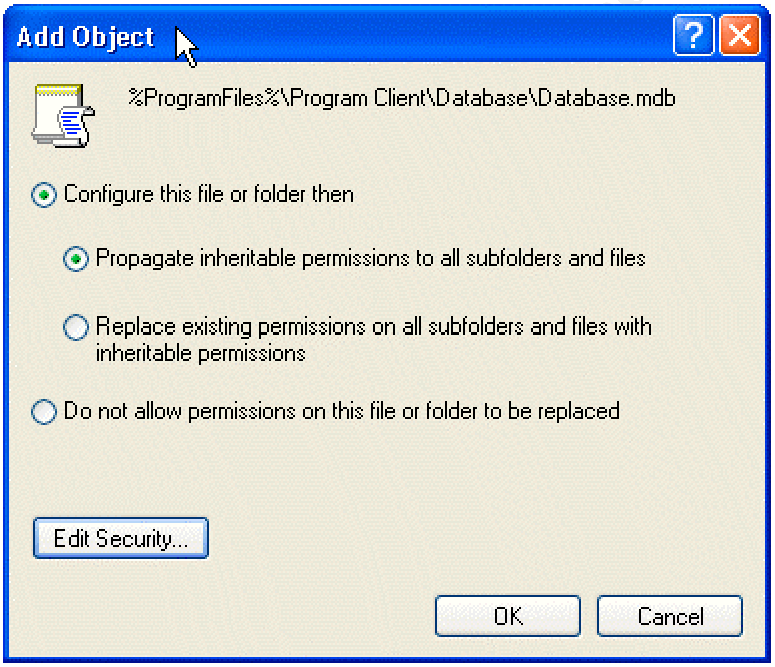
- Console Root
  - Security Configuration and Analysis
  - Security Templates
    - C:\WINNT\security\templates
    - C:\Templates
      - SecureDB

Name	Description
SecureDB	Secure the local Access database.

Figure 12 - Security Template mmc

“C:\Templates” is a new repository I add by right-clicking Security Templates and picking “New Template Search Path”. Then I right-click “C:\Templates” and pick New Template. I name the Template “SecureDB.inf”.

I expand SecureDB and right-click File System > Add File… to choose the database folder that contains the Database:



Add Object

%ProgramFiles%\Program Client\Database\Database.mdb

● Configure this file or folder then

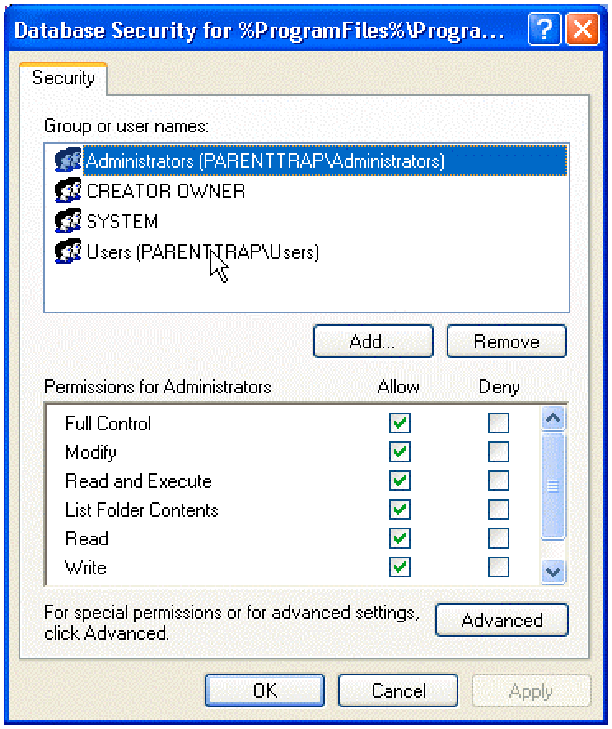
● Propagate inheritable permissions to all subfolders and files

○ Replace existing permissions on all subfolders and files with inheritable permissions

○ Do not allow permissions on this file or folder to be replaced

Figure 13 - Configuring Permission Propagation

I am choosing to propagate the permissions I set in case I add new databases to the database directory in the future.



Database Security for %ProgramFiles%\Progra...

Group or user names:

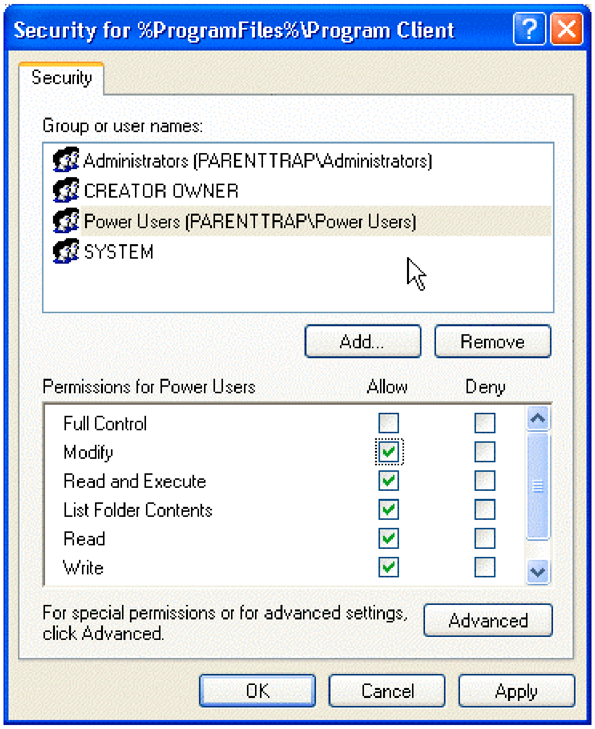
- Administrators (PARENTTRAP\Administrators)
- CREATOR OWNER
- SYSTEM
- Users (PARENTTRAP\Users)

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read and Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

Figure 14 - Current OS Permissions

I want to change these permissions to:



Group or user names:

- Administrators (PARENTTRAP\Administrators)
- CREATOR OWNER
- Power Users (PARENTTRAP\Power Users)
- SYSTEM

Permissions for Power Users	Allow	Deny
Full Control	☐	☐
Modify	☑	☐
Read and Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☑	☐

For special permissions or for advanced settings, click Advanced.

Figure 15 - Security Template Permissions

And save the template.

Next I go into the Security Configuration and Analysis Tool, right-click the title and pick Open Database…

I select a new database called SetPerms.sdb and right-click the title again to pick Import Template…

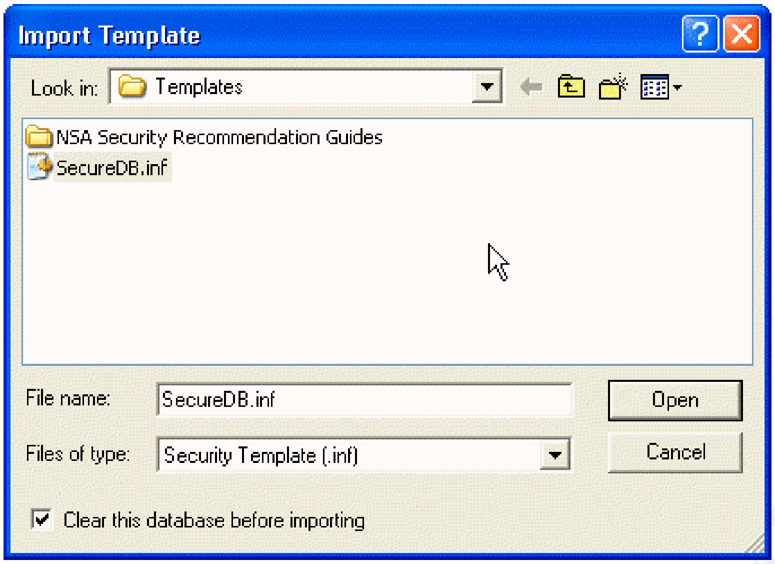


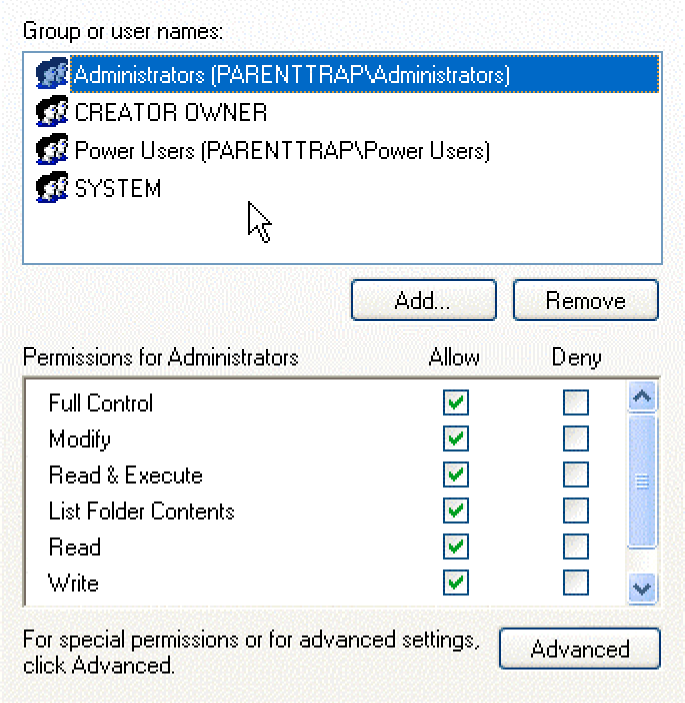
Figure 16 - Importing a Template

I select the SecureDB.inf template just created, and check the "Clear this database before importing" because if the sdb database did have existing data, it should be cleared (we're not merging templates in this example).

I right-click the title once again and pick Analyze Computer Now… After completion, I expand the File System section to view the database folder and see the red x on the icon shows the folders did not match.

However, after selecting Configure Computer Now… the changes are applied and the icon on the database folder turned into a green checkbox.

By looking at the actual permissions on the file system, I see they changed after the Template was applied:



Group or user names:

- Administrators (PARENTTRAP\Administrators)
- CREATOR OWNER
- Power Users (PARENTTRAP\Power Users)
- SYSTEM

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

Figure 17 - Resulting File Permissions

Example: Scripting Security Templates

This next example shows how Security Templates can be used to pre-populate keys used in the Program Client. This is a small challenge as the Program Client stores keys in HKEY_CURRENT_USER. Security Templates provide only direct assess to HKEY_USERS. Fortunately, HKEY_CURRENT_USER is a child of HKEY_USERS, but it is not named HKEY_CURRENT_USER. Rather, it is named with the current user's SID.

This example assumes the user running the script is the same user who will run the Program Client and the script runs under that user's context. It uses the utility SECEDIT.EXE to install the Security Template to the machine.

Although there are many (better) ways of reaching the same goal, this exercise demonstrates how Templates can be dynamically generated and installed using a script.

The keys we would like to set are:

> HKEY_CURRENT_USER\Software\Company\Program Client\DB\Client\SendInclude\attachment

And

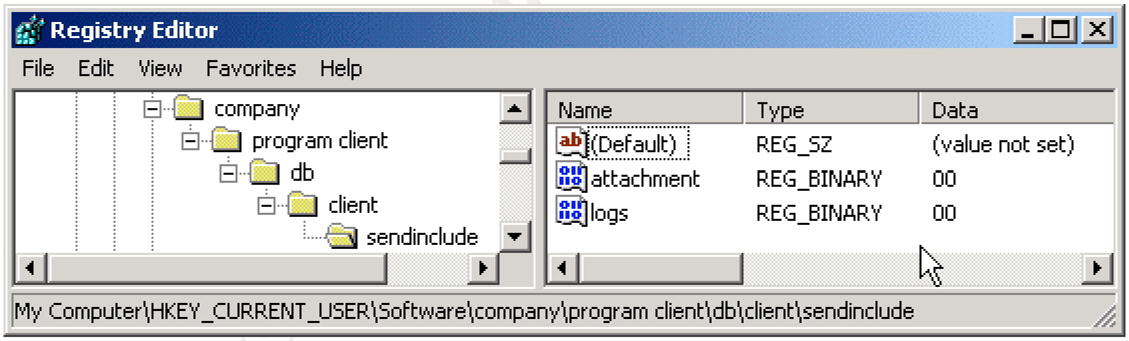
```
HKEY_CURRENT_USER\Software\Company\Program
Client\DB\Client\SendInclude\logs
```

Both these values are Boolean and should be set to 0 to prevent users from uploading attachments with their wells. The script looks like this:

```
' ================================================
' This vbscript creates a template for the current
' user (or the user the script is running as) and
' applies it using SECEDIT.EXE.
' ================================================
Dim sTempFolder
Dim sTemplateName
Dim sSid

' get the current user's SID
sSid = sGetSid
‘ if the sid is found…
if sSid <> “” then
  ' a text stream
  Dim tsTemplate

  sTempFolder = "C:\Temp"
  sTemplatePath = sTempFolder & "\" & "ClientTemplate.inf"
  sDatabasePath = sTempFolder & "\" & "ClientTemplate.sdb"
  sLogPath = sTempFolder & "\" & "ClientTemplateLog.txt"

  Dim ofs
  set ofs = CreateObject("Scripting.FileSystemObject")

  ' create the temp folder if it doesn't exist
  If Not (ofs.FolderExists(sTempFolder)) Then
     ofs.CreateFolder (sTempFolder)
  End If
  Set tsTemplate = ofs.CreateTextFile( sTemplatePath, True)

  ' write the template
  tsTemplate.WriteLine "[Unicode]"
  tsTemplate.WriteLine "Unicode = yes"
  tsTemplate.WriteLine "[Version]"
  tsTemplate.WriteLine "signature = ""$CHICAGO$"""
  tsTemplate.WriteLine "Revision = 1"
  tsTemplate.WriteLine "[Registry Values]"
  tsTemplate.WriteLine "USERS\" & sSid & "\Software\Company\Program
Client\DB\Client\SendInclude\attachment=3,0"
  tsTemplate.WriteLine "USERS\" & sSid & "\Software\Company\Program
Client\DB\Client\SendInclude\logs=3,0"
  tsTemplate.WriteLine "[Profile Description]"
  tsTemplate.WriteLine "Description = Program Client Registry Set"
  tsTemplate.Close

  ' run secedit to import
  Dim oShell
  Set oShell = CreateObject("Wscript.Shell")
  oShell.Run ("%comspec% /c secedit /configure /db """ & sDatabasePath & """ /cfg """ &
sTemplatePath & """ /overwrite /log """ & sLogPath & """ /quiet"), 1, True
```

```
End If

' ==============================================
' SID code lifted from a question by "Ruben" on a wrox forum -
' http://p2p.wrox.com/topic.asp?TOPIC_ID=4490
' ==============================================
Function sGetSid
        Set WSHNetwork = Wscript.CreateObject("Wscript.Network")
        username = WSHNetwork.UserName

        Set wmi = GetObject("winmgmts:root/CIMV2")
        wql = "Select SID from Win32_UserAccount Where Name='" & username &"'"
        Set result = wmi.ExecQuery(wql)

        For each rec in result
                sid = rec.SID
        Next

        If sid <> "" then
                sGetSid = sid
        else
                sGetSid = ""
        end If
End Function
```

After running the script, a quick check of the registry shows both values have been created and set correctly:



```
company
  program client
    db
      client
        sendinclude
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
attachment	REG_BINARY	00
logs	REG_BINARY	00

My Computer\HKEY_CURRENT_USER\Software\company\program client\db\client\sendinclude

OS Patches

OS patches can be distributed in a number of ways, depending on the network speeds and whether the laptop is Active Directory Integrated. To take Case 1 as an example, the laptops connect directly to the internet. Many exploits and viruses work at slow speeds.

For the poorly connected laptops of Case 1 and 2, an IT department can provide CD media that includes the latest service packs and required hotfixes. There may be (legal) risk in providing update software (in Case 1 the laptops are not owned by the company); on a wide variety of laptops and configurations there are bound to be issues such as blue-screens-of-death and unbootable paperweights. On the other hand, this is a way to improve the security of the laptops and the Synchronization process in general. The same means used to distribute OS Patches could also be used to distribute and install Program updates, Anti-Virus updates, Security Templates, etc.

Microsoft service packs and patches can be combined with the OS Install to create a single install. This is called a "slipstreamed" installation. Third party packages, such as Ghost, perform similar functions.

For laptops that are occasionally connected to broadband, the Windows Update Service (or if connected to a corporate network as in Case 3, Microsoft's Software Update Services[27]) can be set up to automatically download and install for the field users. The Windows Update Service uses the Background Intelligent Transfer Service (BITS) to slowly stream down updates if automatic downloads are requested.

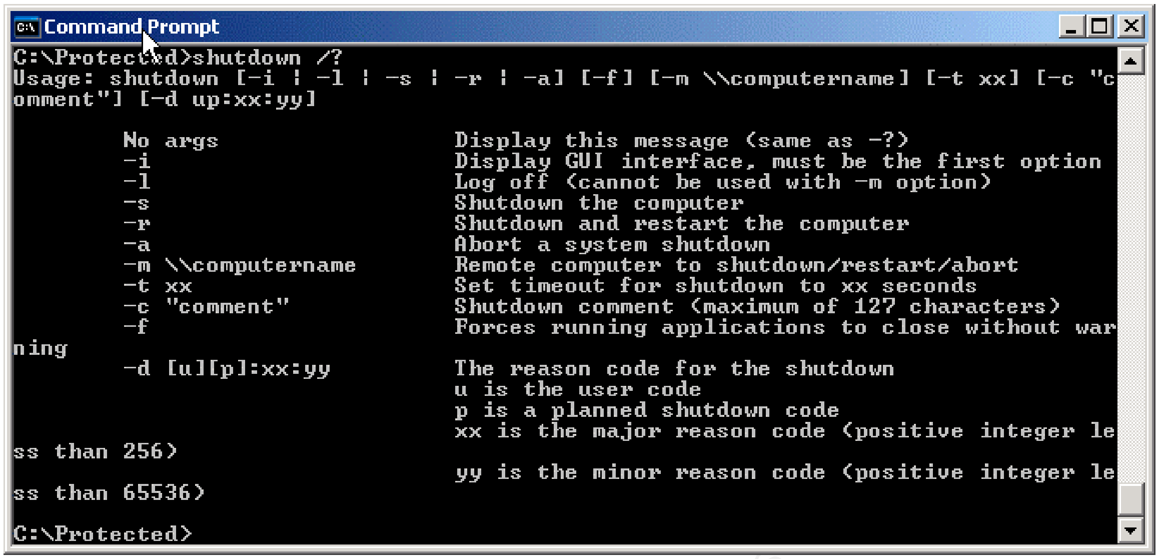
Microsoft Hotfixes can be installed from script with:

```
Hotfix1.exe –m –z
Hotfix2.exe –m –z
qchain.exe
```

Where –m is "unattended mode" and –z is "do not reboot". Many hotfixes require reboots; in order to ensure the hotfixes are applied in the correct order the utility QCHAIN.EXE[28] should be run after the hotfixes. The machine should be rebooted afterwards. The utility shutdown.exe can be scripted to do this:

[27] "Software Update Services". URL: http://www.microsoft.com/windowsserversystem/sus/default.mspx, (23 Nov. 2003).

[28] qchain.exe can be downloaded from http://www.microsoft.com/downloads/details.aspx?FamilyID=a85c9cfa-e84c-4723-9c28-f66859060f5d&displaylang=en



```
C:\Protected>shutdown /?
Usage: shutdown [-i | -l | -s | -r | -a] [-f] [-m \\computername] [-t xx] [-c "c
omment"] [-d up:xx:yy]

        No args                 Display this message (same as -?)
        -i                      Display GUI interface, must be the first option
        -l                      Log off (cannot be used with -m option)
        -s                      Shutdown the computer
        -r                      Shutdown and restart the computer
        -a                      Abort a system shutdown
        -m \\computername       Remote computer to shutdown/restart/abort
        -t xx                   Set timeout for shutdown to xx seconds
        -c "comment"            Shutdown comment (maximum of 127 characters)
        -f                      Forces running applications to close without war
ning
        -d [u][p]:xx:yy         The reason code for the shutdown
                                u is the user code
                                p is a planned shutdown code
                                xx is the major reason code (positive integer le
ss than 256)
                                yy is the minor reason code (positive integer le
ss than 65536)

C:\Protected>
```

QCHAIN is only available for Windows NT 4 and later. Windows 9x users have to install one hotfix at a time, rebooting as required.

Example: Forcing the Windows Update Client to Install Critical Patches

In this example we are assuming that the critical updates (and only the critical updates) that Microsoft releases should be patched immediately and there is no danger of side-effects[29].

Nevertheless, the Windows Update Client can be configured to automatically download and install critical patches[30].

The registry entry would look like this:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]
"NoAutoUpdate"=dword:00000000
"AUOptions"=dword:00000004
"ScheduledInstallDay"=dword:00000000
"ScheduledInstallTime"=dword:00000003
"UseWUServer"=dword:00000000
"RescheduleWaitTime"=dword:00000005
"NoAutoRebootWithLoggedOnUsers"=dword:00000001
```

[29] We can also assume I'm good looking and rich.

[30] "How to Configure Automatic Updates by Using Group Policy or Registry Settings". Microsoft Knowledge Base. URL: http://support.microsoft.com/default.aspx?kbid=328010, (23 Nov. 2003).

The AuOptions value of 4 means “Automatically download and install”.

Using Group Policy the same settings can be changed through the Group Policy mmc snap-in under Computer Configuration > Administrative Templates > Windows Components > Windows Update.

If this branch is not available it can be added with the wuau.adm administrative template (right-click Administrative Templates and choose Add/Remove Templates). If wuau.adm is not in the %windir%\Inf folder it can be downloaded from Microsoft’s web site.

Network Security

Firewalls

In Case 1, a field user may run a firewall on the laptop (software) or use an external device, such as a SOHO router with NAT capabilities (hardware). In Case 3, field users are probably firewalled without even knowing it.

A hardware firewall has the advantage of not taking processing power from the laptop. Although there are hardware firewalls that support dial-up connections[31], most are made for high-speed connections and only include an analog port for failover (if at all). However, that does not mean the failover analog ports on them cannot be used.

Software firewalls include programs like ZoneAlarm and Black Ice. There are many others, many of which are certified by standards[32] and government organizations[33]. Windows XP even has a built-in software firewall[34].

NAT firewalls at the client can interfere with network communications, especially L2TP.

[31] “ISDNLink INET Router”. URL: http://www.asuscom.com.tw/product/inet8xx.html, (23 Nov. 2003).

[32] “ICSA Labs’ Firewall Community”. ICSA Labs. URL:http://www.icsalabs.com/html/communities/firewalls/index.shtml, (23 Nov. 2003).

[33] “Validated Product List”. The Common Criteria Evaluation and Validation Scheme. URL: http://niap.nist.gov/cc-scheme/ValidatedProducts.html#def-firewalls, (23 Nov. 2003).

[34] “How to Manually Open Ports in Internet Connection Firewall in Windows XP”. URL: http://support.microsoft.com/default.aspx?kbid=308127, (23 Nov. 2003).

Securing the Program Client Connection to the FTP Server

Network Connections

Once the field user has a device to make a connection with, the next step is to create a TCP/IP network connection through it to the FTP Server. There are many options, but this paper will discuss three:

1. Case 1 – Leverage off of rural Internet Service Provider (ISP) Points of Presence (POPs) and the internet. Optionally VPN to a RRAS Server.

2. Case 2 – Dial direct to a corporate dial-up RRAS server.

3. Case 3 – Pay a satellite carrier for a secure WAN.

An excellent in-depth resource on the planning and setup of RRAS for Cases 1 and 2 is Chapter 6 of “Expanding and Securing Remote Client Access” in the Windows 2000 Network Deployment Guide[35].

Case 3, a secure WAN from a satellite vendor, is a very expensive but convenient option. The network aspects of this case will not be discussed.

Port Settings

The Program Client uses passive FTP to connect to an FTP Server. Passive FTP is advantageous from the laptop’s point of view as the FTP command and data socket connections both originate at the laptop and more likely work through a NAT firewall (see Appendix D for details on Passive FTP). To enable Passive FTP at the field side through a packet filtering firewall, outgoing traffic must be allowed on port 21 and ports > 1024. The packets of the established connections on ports > 1024 must be allowed back in.

While it is possible to change to use a port other than 21, these changes require editing a client-side dll with a hex editor. This is **not supported** by the software vendor and makes future upgrades tricky. However, for those who can’t take a

[35] “Windows 2000 Server Resource Kit”. Network Deployment Guide, Chapter 6 - Expanding and Securing Remote Client Access. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/Default.asp, (23 Nov. 2003).

hint, the process could be automated with one of many patching programs, including Gnu Software's patch program[36].

Port Forwarding and Proxy Servers

Although the Program Client itself does not support technologies such as SSL, there are products that can be installed on the laptop to broker a secure connection to the FTP server.

For example, the client could run a program like SSH[37] (Secure Shell) with FTP forwarding (FTP forwarding contains knowledge of the passive FTP protocol and additional logic over generic port forwarding[38]). Note that this is different than SFTP, which is an FTP Client with built-in understanding of SSH and is not supported in the Program Client.

The SSH Client would first connect to a Secure Shell Server and broker FTP traffic to and from the FTP Server (so this assumes the SSH Server and FTP server can communicate—or are the same box). To the Program Client it appears it is talking to an FTP Server running on the same laptop (the FTP server would be listed in the Program Client as "localhost" or "127.0.0.1".)

The software for FTP forwarding contains logic to monitor for the returned data port number from the FTP server. It then dynamically changes the port forwarding to include the data traffic through the tunnel. The SSH Client would need to be running before the synchronization process is started (perhaps manually or as a post connect step in a RAS connection).

Another option is an FTP Proxy like SafeTP[39]. This particular proxy uses an uncommon security protocol (X-SafeTP1[40]) that must be supported at the Server for secure communications. However, other proxies are available that support other methods of secure communications, including SSL.

[36] "patch". Gnu Software. URL: http://www.gnu.org/software/patch/patch.html, (23 Nov. 2003).

[37] "SSH Manual Page". OpenBSD Reference Manual. URL: http://www.openbsd.org/cgi-bin/man.cgi?query=ssh&sektion=1, (23 Nov. 2003).

[38] "Port Forwarding". SSH Admin Guide. URL: http://www.ssh.com/support/documentation/online/ssh/adminguide/32/Port_Forwarding.html, (23 Nov. 2003).

[39] "SafeTP Transparent FTP Security Software". URL: http://safetp.cs.berkeley.edu/, (23 Nov. 2003).

[40] Described in URL: http://safetp.cs.berkeley.edu/protocol.txt, (23 Nov. 2003).

Transmission Methods

Here are some of the transmission methods available from the Field:

Connect Type	Speed (bps)	Coverage	Reliability	Cost	Security
Land Line	~33,600	Poor	Great	Great	Great
Digital Cell	14,400	Poor	Poor	Good	Good
Bag Phone	4,800	Good	Good	Good	Poor
Satellite Phone	2,400 - 1 Mbs	Great	Good	Poor	Great
CDPC (Cellular Digital Packet Data) (1x)	19,200	Poor	Good	Good	Great

With the exception of land line connections, which are rare in the wilderness, all these connect types involved some sort of through-the-air transmission. As such, there is an opportunity for the transmission to be intercepted.

Bag Phones are still commonly used in the Field. Until recently they were the only options in some remote areas. A Bag phone uses analog cell infrastructure but has a more powerful transmitter and receiver (a cell phone is typically .7-1 watt while a bag phone is 3-8 watts). Bag phone transmissions are not secure. Bag phones use standard analog cell phone technology and can easily be intercepted by amateurs with off-the-shelf equipment. This is especially easy considering the high power broadcast required to reach cell towers from remote locations.

Digital cell is more secure, but quoting a letter from Bruce Schneier (Countpane Labs) to the CTIA:

> Certainly, digital cellular is harder to eavesdrop on than analog cellular. The latter just requires a scanner tuned to the correct frequencies. Digital cellular voice security can be broken in real time by anyone with a little bit of budget, expertise, and desire.[41]

CDPC is also more secure than analog cell, but is subject to man-in-the-middle attacks and uses CMEA (like digital cell) and ORYX encryption algorithms; both of which have been successfully broken[42].

Digital cell and CDPC are quickly replacing Bag Phones in the field. Most rural cell towers have been upgraded for digital, and signal boosters can be used to increase the phone range.

Satellite phones vary in their capabilities depending on the satellite system used and phone model. Some phones are as slow as 2400 baud. Others have speeds up to 1Mbs down and 153Kb up[43] (in practice speeds are lower). The satellite transmission itself can be very secure. In the case of Infosat's HSI product, communications are 128 bit encrypted[44]. Not all satellite systems have coverage in Northern areas, however. Some satellite providers only offer internet connectivity while others offer complete WAN and VPN services to the enterprise.

Hardware Settings

Compression and Error Correction

Because the data rates are so slow, most modems negotiate a compression algorithm during the connection handshake. Error correction schemes can also be negotiated to better handle noisy lines. These are usually set in Windows modem (or other device) connect string settings. They can also be stored in many modem's non-volatile memory.

It is important to note that while compression and error correction algorithms do not provide much in the way of security, they can significantly affect the data transmission speeds, which in turn does have an impact on what security methods can be used.

[41] "Counterpane's reply to the CTIA". URL: http://www.schneier.com/cmea-response.html, (23 Nov. 2003).

[42] "Thin Client Security Homepage". URL: http://www.nue.et-inf.uni-siegen.de/~schmidt/tcsecurity/protocols.html, (23 Nov. 2003).

[43] For example, URL: http://www.infosat.com/services/hsi/index.html, (23 Nov. 2003).

[44] Khosa Amardeep. InfoSat. Interview. 21 Nov. 2003.

Modem compression algorithms such as MNP-5 actually provide worse performance if the data is already compressed[45]. Some error compression algorithms[46] purposely slow down the transmission on a noisy line, introduce delays[47], or repeat part of the transmission. Sometimes the error correction algorithms do not provide optimal throughput on a noisy line[48].

For optimum connection, the modems at both the laptop end and the RAS Server end should be optimally configured and tested in a variety of environments.

PPTP vs. L2TP – A Tale of Two Protocols

Purely for security, L2TP is the better choice. L2TP requires the use of certificates (pre-shared keys are allowed, but not suggested[52] below).

In Case 1, the network does not have a Certificate Authority, and even if it did, distribution of certificates and use of older Windows versions would make L2TP a challenge; PPTP is more attractive despite the security shortcomings. However, in Case 2, L2TP is the best choice.

L2TP/IPSec and PPTP differ in several ways.

- Authentication Levels: L2TP/IPSec requires two levels of authentication - computer authentication (either certificate or pre-shared key) through IPSec and L2TP to authenticate the user. PPTP performs only user-level authentication.

- Encryption Algorithms: L2TP/IPSec uses DES. PPTP uses MPPE.

- L2TP/IPSec encrypts the authentication process. PPTP does not.

[45] "Data Compression". URL: http://www.modem.com/glossary/glos2.html, (23 Nov. 2003).

[46] Chen, Patrick. "Modem Tutorial – Error correction Protocols". URL: http://www.sfn.saskatoon.sk.ca/Help/ModemTutorial/MT-Error.html, (23 Nov. 2003).

[47] Interleaving for example: URL: http://www.moseleysb.com/OptPerf1.html, (23 Nov. 2003).

[48] If you're looking for a better system, check here: URL: http://www.nsa.gov/programs/tech/factshts/modem.html, (23 Nov. 2003).

PPTP

In its initial implementation, PPTP was not very secure[49]. Version 2 is more secure, but is still vulnerable to password guessing tools[50].

If PPTP is used, it is important that the newest Dial-up Networking (DUN) clients are installed along with the latest OS patches (especially for older Windows versions).

PPTP is compatible with most NAT routers.

L2TP/IPSec

L2TP is supported natively in Windows 2000 and later. Earlier versions of Windows (98, ME, and NT) have to install a newer VPN Client[51].

L2TP/IPSec is a more secure VPN technology then PPTP. There may be issues using it through a local NAT firewall. Many SOHO DSL or Cable routers are IPSec friendly now (or have options to be).

To authenticate machines, the laptop requires a certificate or a pre-shared key[52]. Distribution and installation can be such a challenge in field environments that PPTP may be more effective overall to implement. If certificates are used, a PKI infrastructure (including a Certificate Authority) must be set up. It is unlikely field laptops will be able to participate in a domain where certificate transfer can be automated (unless we're talking about Case 3).

Encryption and Network Overhead at Slow Speeds

The major hurdle to encryption is the slow connect speeds. A VPN does introduce overhead. The exact amount varies with many factors, but 10-30% is common.

[49] In a very unfavorable paper: Schneier, Bruce and Mudge. "Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)". URL: http://www.schneier.com/paper-pptp.html, (23 Nov. 2003).

[50] According to Counterpane and friends: URL: http://www.schneier.com/pptp.html, (23 Nov. 2003).

[51] Available at http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp

[52] Microsoft does not actually support the use of pre-shared keys to a VPN client (but you can do it). See "How to Configure a L2TP/IPSec Connection Using Pre-shared Key Authentication". URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q240262, (23 Nov. 2003).

Also of note, at slow speeds Windows chooses a smaller IP Packet and MTU size[53]. Dial-up connections of 128kbps and below start at 576 and range up to 1500 for LAN connections.

Routing and Remote Access (RRAS) Server

RRAS is Microsoft's VPN and dial-up access server. It is available on Windows 2000 Server and .Net Server.

A RRAS Server is described as being optional in Case 1. Without it, field users make an internet connection and directly access an FTP Server. While this does have the advantage of simplicity, and it provides a connection with the least amount of overhead, the network traffic is not encrypted in any way. The FTP protocol is not secure and the username and password are transmitted in plain text. If anyone is able to capture packets on or between the laptop and FTP server, it is very simple to view the login information. Although the Program Client encrypts application data before sending it, it is possible for a hacker to collect vast amounts of data over time to aid in his/her cracking efforts.

What field users need to do after making an internet connection is create a Virtual Private Network (VPN) to the network where the FTP Server is located (in the example of Case 1, it's the same machine).

One instance where a VPN may not be practical is in the very worse-case scenario of an extremely slow and unreliable modem connection. If the impact of the VPN is such that a connection to the server is no longer viable, it may be worth the risk to connect without it.

In Case 2, field users dial into a private bank of modems. The quality and reliability of a direct RAS connection is very dependent on hardware compatibility and modem options. This approach requires some real-world field testing and informed hardware purchases.

A direct RAS connection can minimize one security risk of the internet; packets will not be traveling through a public infrastructure. However, as dial-up RAS is usually used in the field with boosted analog and cell phones, these packets are broadcast over a large area through the air and should be encrypted. However, if the transmission medium is considered "safe", dial-up RAS without encryption will provide a more efficient connection for slow (2400 baud for example) devices.

[53] Lynn Larrow. "Dial-up and Home Networking Troubleshooting Reference". 1 June 2003, http://www.internetweekly.org/llarrow/mtumss.html, (23 Nov. 2003).

Client Setup

RAS phone book entries can be configured and distributed as a small install package using Microsoft's Connection Manager Administration Kit[54].

The Connection Manager can also be used with tools like the Phone Book Server[55] to provide a list of corporate dial-up access numbers.

This is very convenient for Case 1 laptops where an IT group has not had the opportunity to pre-configure Dial-up Networking entries for a VPN. Field users will already have a Dial-up Networking connection to their local ISP. The Connection Manager package installs a connection for the VPN. It is worth checking that the ISP permits and/or supports VPN connections.

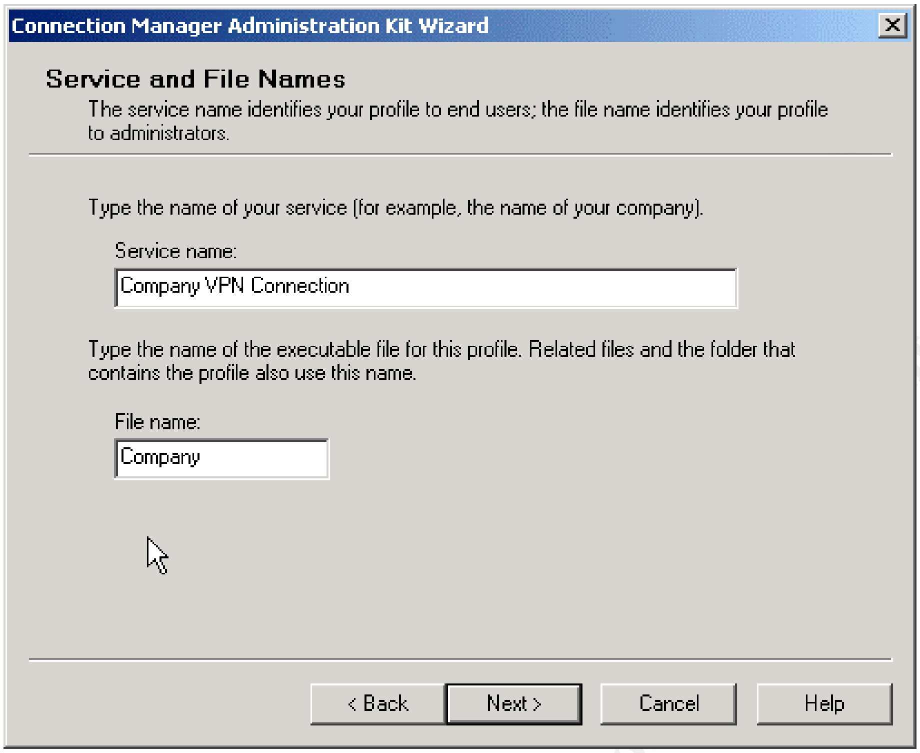
The Program Client does allow up to 2 RAS connections; it automatically dials the ISP and, if the connection succeeds, dials the VPN before trying to make an FTP connection.

Example: Creating a Client VPN Install using Connection Manager (Case 1)

When the Connection Manager Administration Kit (CMAK) Wizard is run, the first useful screen will ask to create a New profile or use an Existing profile. Select New:

[54] See "Before you start: Understanding Connection Manager and the Administration Kit". URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/cmak_ops_03.asp, (23 Nov. 2003).

[55] See "Microsoft Connection Manager". URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=4981, (23 Nov. 2003).



Service and File Names

The service name identifies your profile to end users; the file name identifies your profile to administrators.

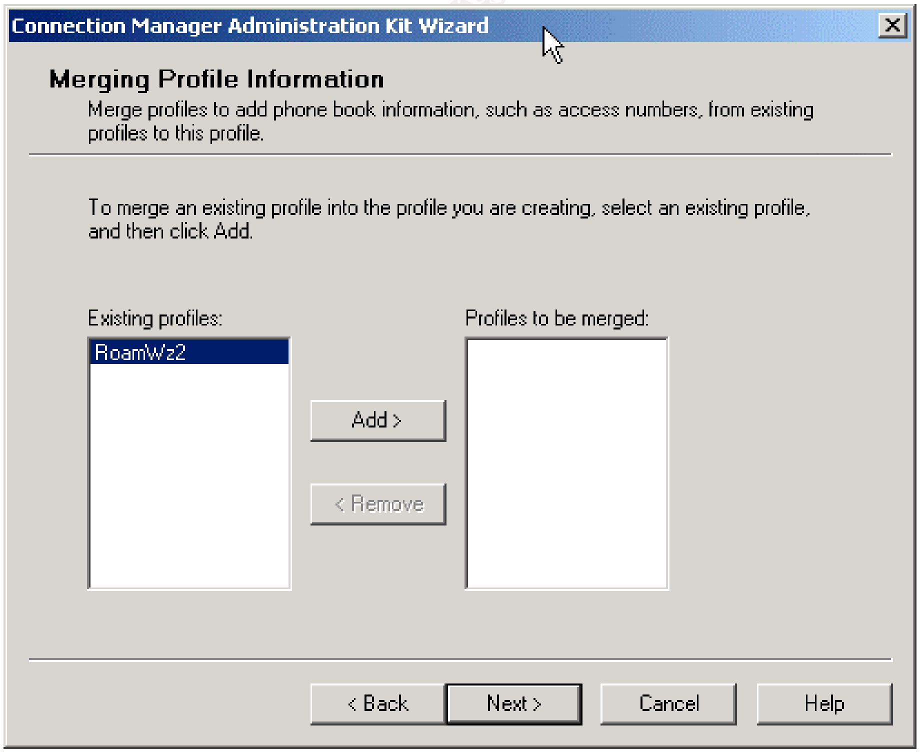
Type the name of your service (for example, the name of your company).

Service name: Company VPN Connection

Type the name of the executable file for this profile. Related files and the folder that contains the profile also use this name.

File name: Company

The File name is limited to eight characters. The next dialog asks for a Realm Name. Since in Case 1 all the users will be local users on the RRAS/FTP server a realm name is not required. Click Next.



Merging Profile Information

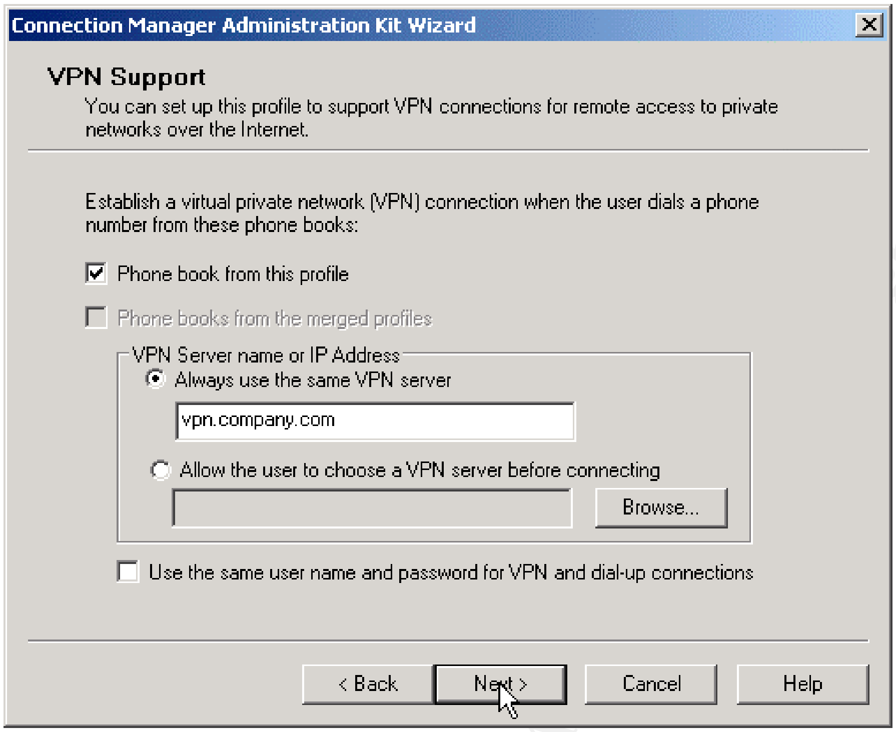
Merge profiles to add phone book information, such as access numbers, from existing profiles to this profile.

To merge an existing profile into the profile you are creating, select an existing profile, and then click Add.

Existing profiles: RoamWz2

Profiles to be merged:

If a profile already exists on the machine that settings should be merged from, pick Add. In this case we click Next.



Connection Manager Administration Kit Wizard

VPN Support

You can set up this profile to support VPN connections for remote access to private networks over the Internet.

Establish a virtual private network (VPN) connection when the user dials a phone number from these phone books:

☑ Phone book from this profile

□ Phone books from the merged profiles

VPN Server name or IP Address

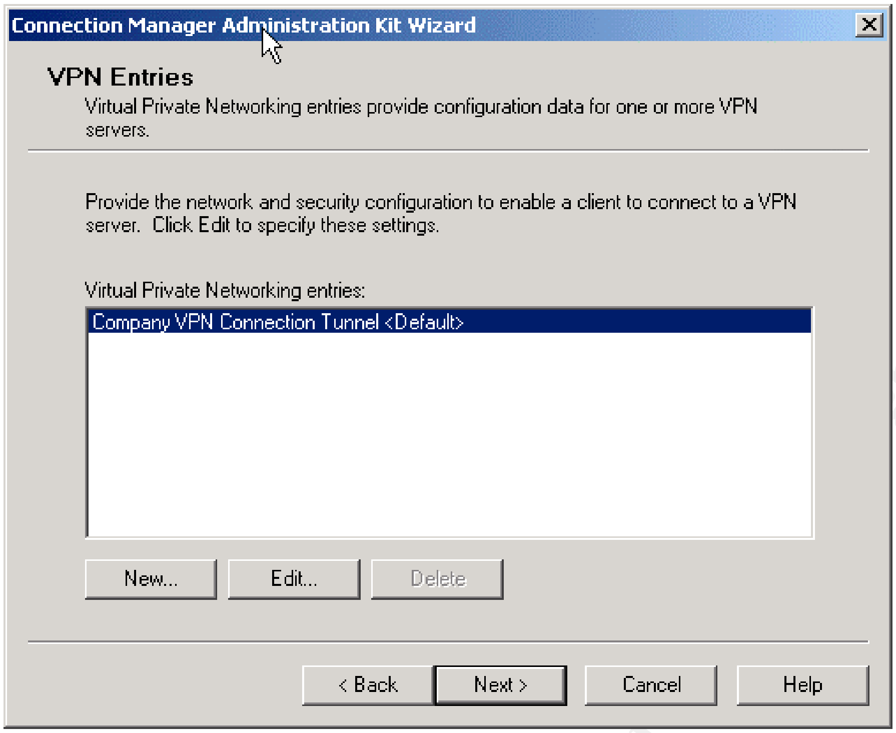
● Always use the same VPN server

vpn.company.com

○ Allow the user to choose a VPN server before connecting

□ Use the same user name and password for VPN and dial-up connections

Add the IP address or DNS name of the internet available VPN server and click Next.



VPN Entries

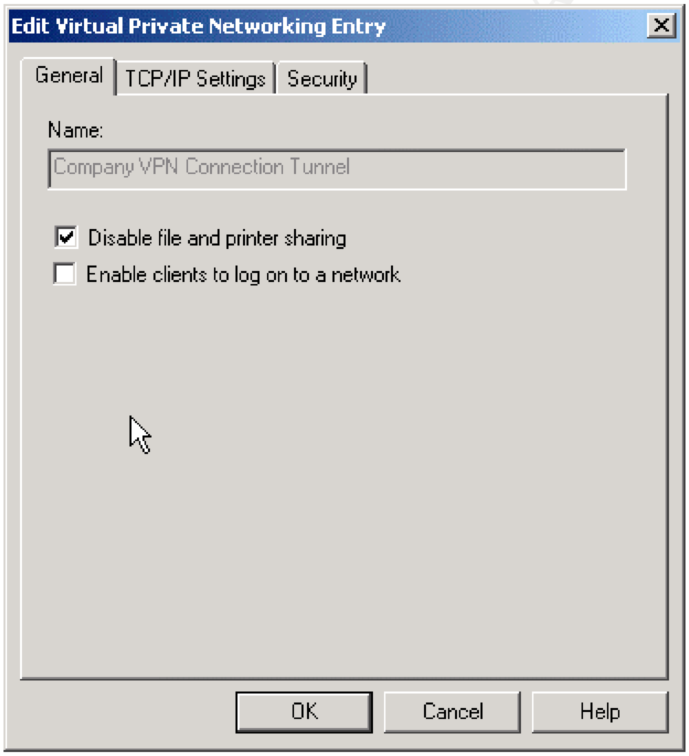
Virtual Private Networking entries provide configuration data for one or more VPN servers.

Provide the network and security configuration to enable a client to connect to a VPN server. Click Edit to specify these settings.

Virtual Private Networking entries:

Company VPN Connection Tunnel <Default>

Pick Edit… to set the VPN Options:

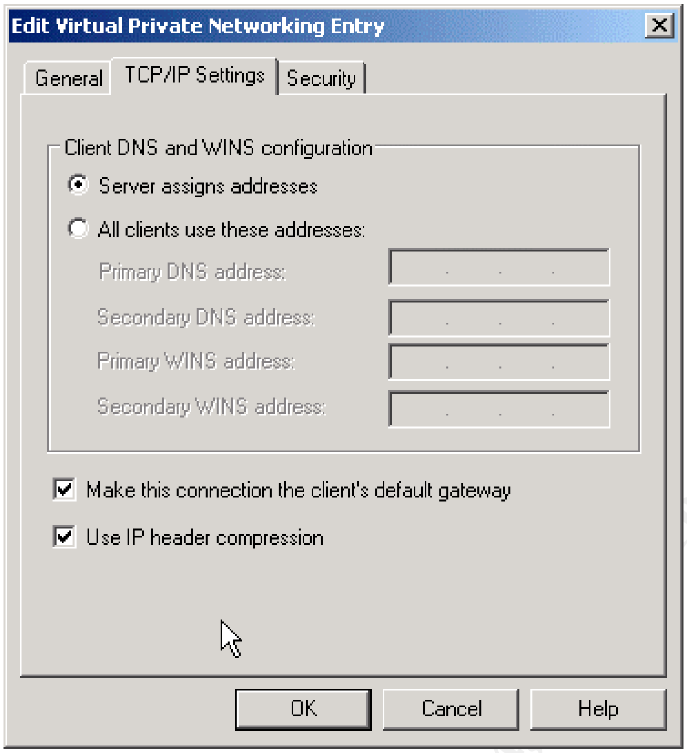


Name: Company VPN Connection Tunnel

☑ Disable file and printer sharing

□ Enable clients to log on to a network

“Disable file and printer sharing” affects only Windows NT 4 and later OS’s. It’s been disabled because it is not required. Similarly, “Enable clients to log on to a network" applies only to Windows 9x and ME. Program Clients do not require network access as, in Case 1, the FTP server is on the same machine. The next tab, "TCP/IP Settings" displays:



Client DNS and WINS configuration

● Server assigns addresses

○ All clients use these addresses:

Primary DNS address: . . .

Secondary DNS address: . . .

Primary WINS address: . . .

Secondary WINS address: . . .

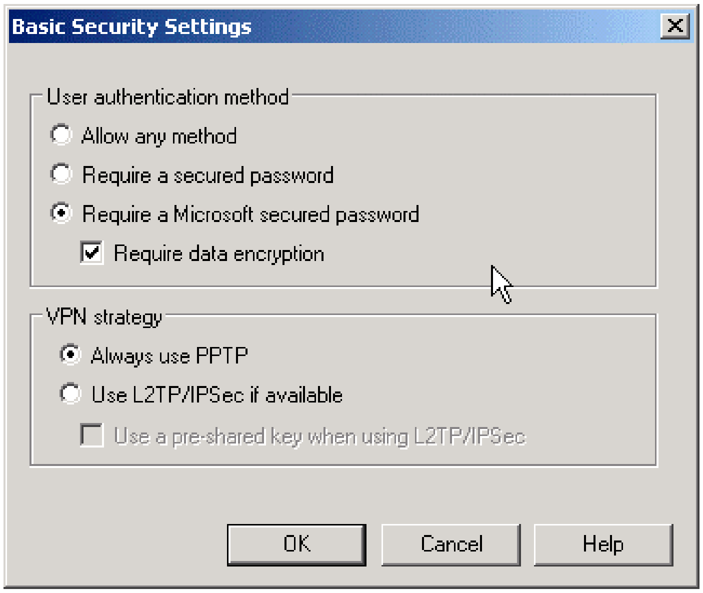
☑ Make this connection the client's default gateway

☑ Use IP header compression

Of most importance is the "Make this connection the client's default gateway". It is extremely risky turning this off.

The laptop must already have an internet connection to establish the VPN. If the laptop has been compromised and the VPN is NOT the default gateway, a hacker has a clear route from his/her internet location, to the laptop, and on through the VPN. The disadvantage of turning this option on is all the user's internet traffic goes to the RRAS server. If the RRAS server does not allow, say, http packets out, the user cannot browse the web while the VPN connection is active. But this is a small inconvenience considering the security risk.

The final tab is Security. It contains buttons for both Basic and Advanced security. The Basic button displays:



Basic Security Settings

User authentication method

○ Allow any method

○ Require a secured password

● Require a Microsoft secured password

☑ Require data encryption

VPN strategy

● Always use PPTP

○ Use L2TP/IPSec if available

□ Use a pre-shared key when using L2TP/IPSec

Obviously "Require data encryption" is critical in protecting the network traffic. In this example for Case 1, the VPN protocol chosen is PPTP because there is no Certificate Authority available for L2TP to be used.

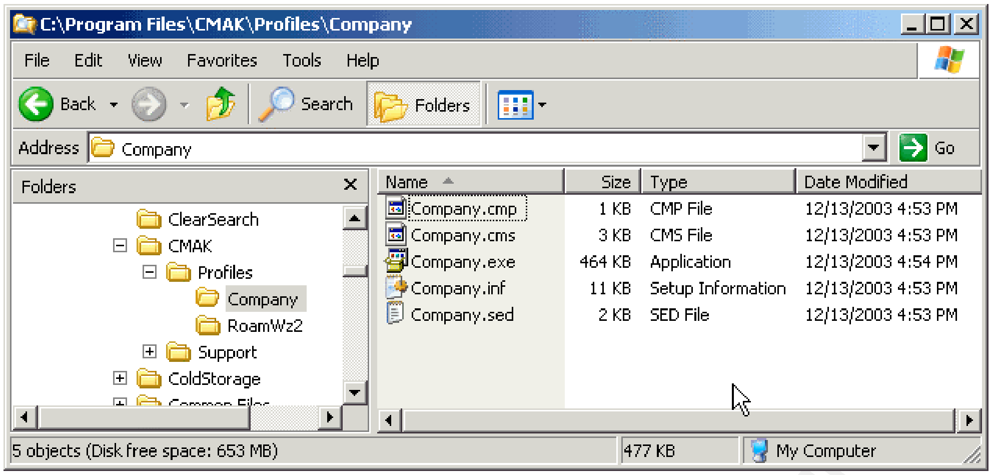
The default Advanced settings were used (Require Encryption, **Authenticate with MS-CHAP version 2**, and to Try PPTP Protocol First). MS-CHAP version 1 is not secure enough to be used over the internet. Version 2 is only available on Windows 9x with the latest Dial-up Networking software (for VPN use).

Going back to the main Wizard dialog and pressing Next asks about the Phone Book entries. In Case 1 we are not using Phone Books; uncheck "Automatically download phone book Updates" and press Next.

The Dial-up Networking Entries information does not need to be changed. Press Next. The Routing Table also does not need to be changed. Press Next. Proxy settings do not need to be changed. Press Next. Custom Actions are not required. Press Next. The Logon Bitmap can be standard. Press Next. Leave defaults for the Phone Book Bitmap and the Icons that follow. Next. Next.

The Notification Area Shortcut Menu can be added if desired. Next. A custom help file would be a nice touch, but the default is fine for now. Next. Enter the phone number of someone you don't like. Next. Finally, select to install Connection Manager 1.3 with the service. Press Next past the License Agreement. Press Next past Additional files.

Press Next one last time to build the install.



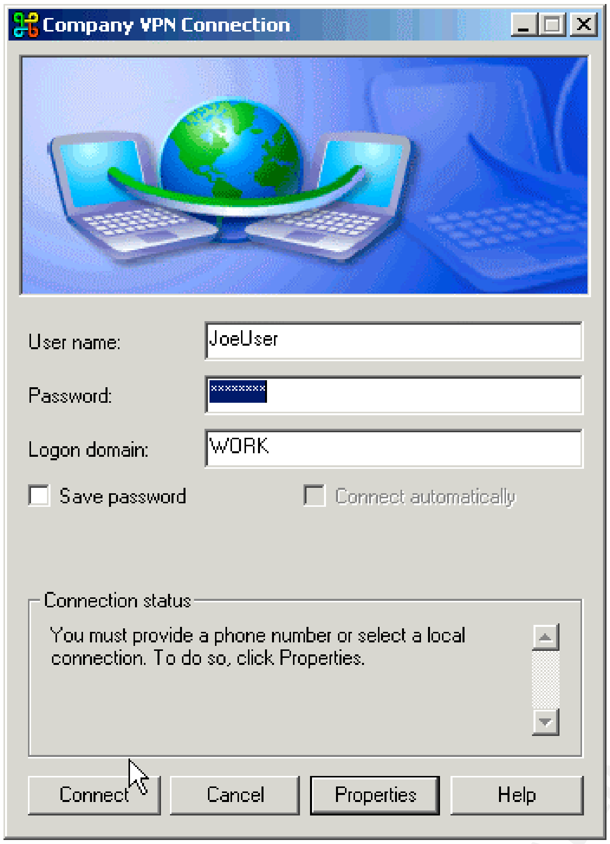
Name	Size	Type	Date Modified
Company.cmp	1 KB	CMP File	12/13/2003 4:53 PM
Company.cms	3 KB	CMS File	12/13/2003 4:53 PM
Company.exe	464 KB	Application	12/13/2003 4:54 PM
Company.inf	11 KB	Setup Information	12/13/2003 4:53 PM
Company.sed	2 KB	SED File	12/13/2003 4:53 PM

5 objects (Disk free space: 653 MB) 477 KB My Computer

Figure 18 - The completed CMAK install

As seen above, the install files easily fit on a floppy.

Once the distribution media has been sent to the field users, they run the exe (Company.exe in this case), and select if they want all laptop users to see the connection and if they want a shortcut on the desktop. Selecting the desktop shortcut of the entry from Network and Dial-up Connections displays the following:



User name: JoeUser

Password: ********

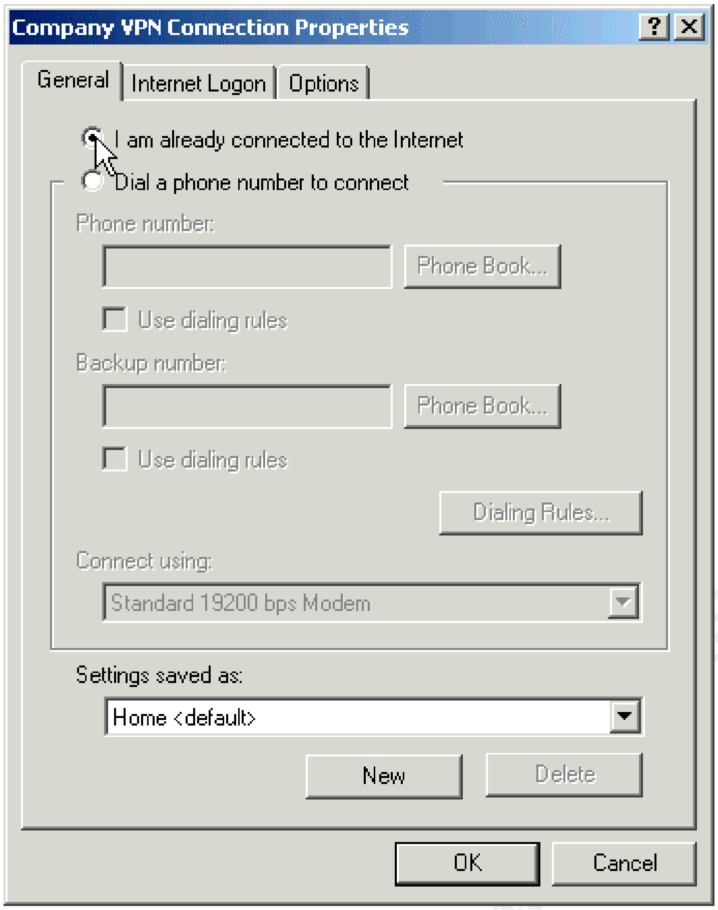
Logon domain: WORK

☐ Save password ☐ Connect automatically

Connection status

You must provide a phone number or select a local connection. To do so, click Properties.

Because this connection was built to include only a VPN connection (in Case 1 laptop users may have many different ISP dial-ups), the first time the user tries to connect he/she is asked to select a phone number in Properties. Selecting Properties gives you the following:



Company VPN Connection Properties

General | Internet Logon | Options

● I am already connected to the Internet

○ Dial a phone number to connect

Phone number:

□ Use dialing rules

Backup number:

□ Use dialing rules

Connect using: Standard 19200 bps Modem

Settings saved as: Home <default>

The user should pick "I am already connected to the Internet". The Program Client dials the ISP RAS connection first, and then the VPN (if configured correctly).

Server Setup

A RRAS server requires a bank of (properly configured) modems and the Routing and Remote Access service (there are other hardware and software products that provide the same functionality).

There is a great deal of information on Microsoft's web site on the proper planning and configuration of a Routing and Remote Access Server.

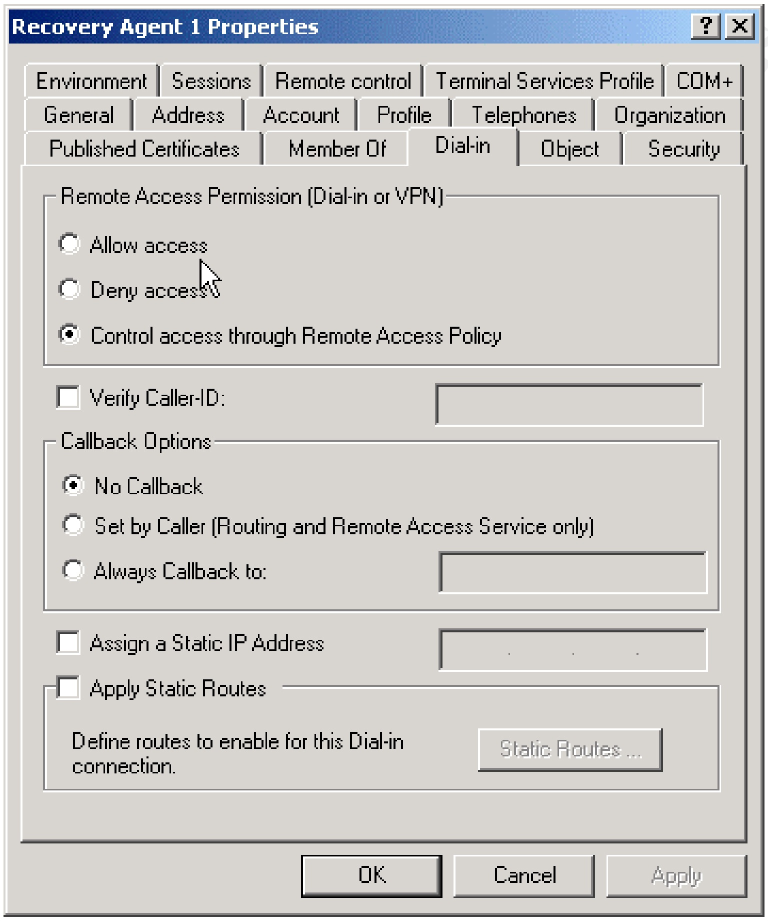
From a security angle the RRAS Server should be protected by its environment, it should limit the traffic that can travel on its interfaces as well as the RRAS traffic it allows. The server should also be configured securely, as should the RRAS Service.

Example: Configuring RRAS (Case 2)

In Case 2, the RRAS Server only has one network card. It also has a bank of modems that field users dial in to. The RRAS Server is a member of the Active Directory domain and the field users authenticate with their domain logins.

Because the laptops were configured by the IT group, they have been given certificates to use the more secure L2TP tunneling protocol (more on this later). PPTP will not be allowed by policy.

Field user's remote access permissions will not be controlled through their Active Directory Users and Computers user property sheets.



Remote Access Permission (Dial-in or VPN)

○ Allow access

○ Deny access

● Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

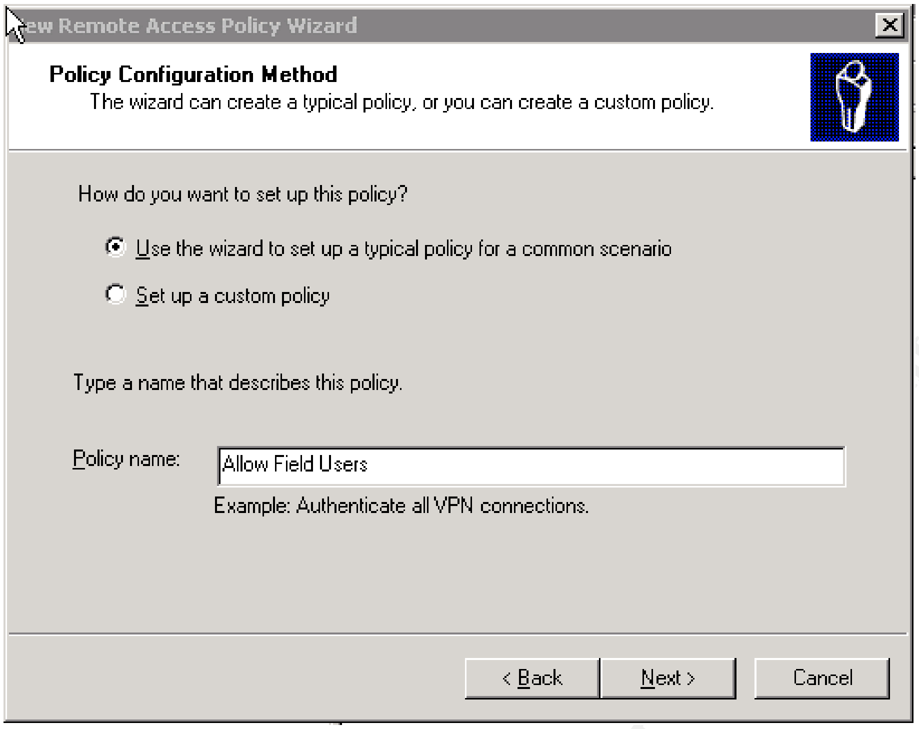
□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

Rather, the user object defers to the RRAS Remote access policy to control dial-up access.

I begin by creating a RRAS Policy. I open the Routing and Remote Access mmc snap-in, right-click "Remote Access Policies" and select New Remote Access Policy to start the Wizard:



Policy Configuration Method

The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

● Use the wizard to set up a typical policy for a common scenario

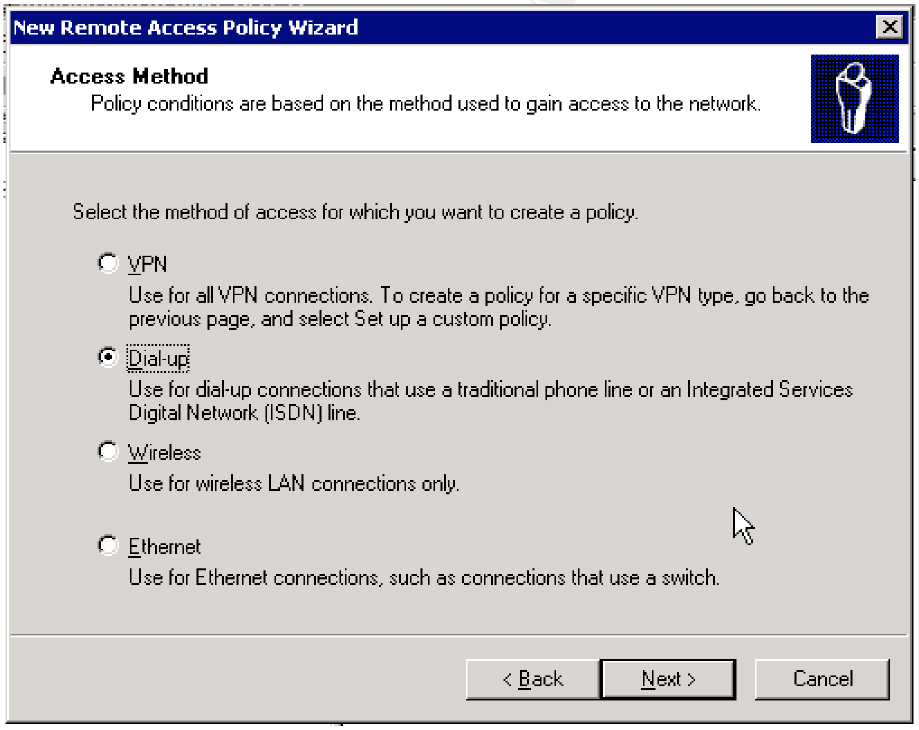
○ Set up a custom policy

Type a name that describes this policy.

Policy name: Allow Field Users

Example: Authenticate all VPN connections.

Next,



Access Method

Policy conditions are based on the method used to gain access to the network.

Select the method of access for which you want to create a policy.

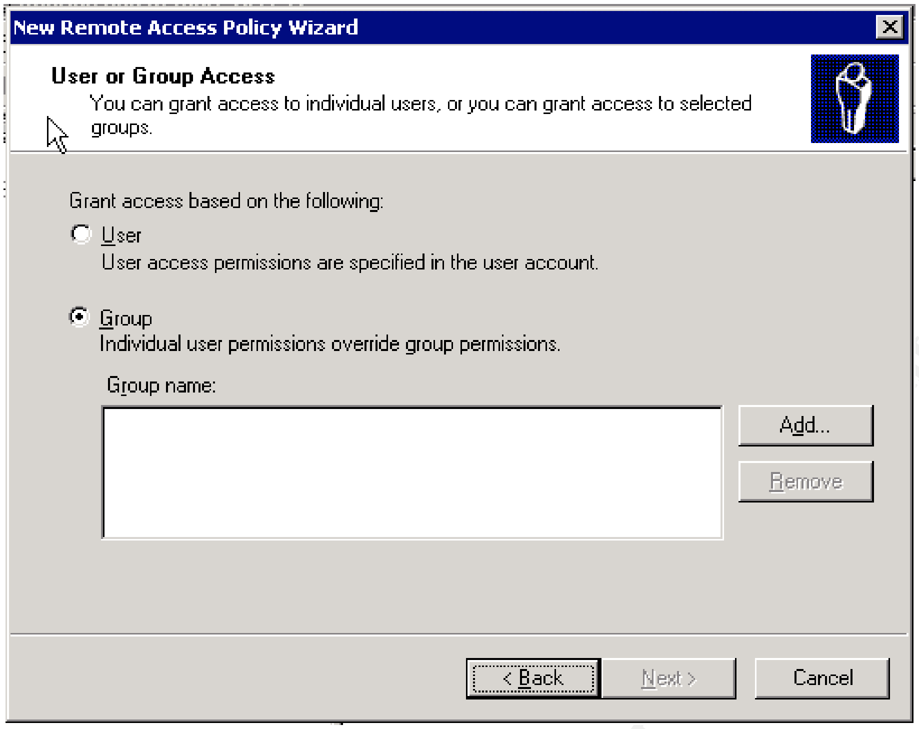
○ VPN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.

● Dial-up
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.

○ Wireless
Use for wireless LAN connections only.

○ Ethernet
Use for Ethernet connections, such as connections that use a switch.

Next,



New Remote Access Policy Wizard

User or Group Access

You can grant access to individual users, or you can grant access to selected groups.

Grant access based on the following:

○ User

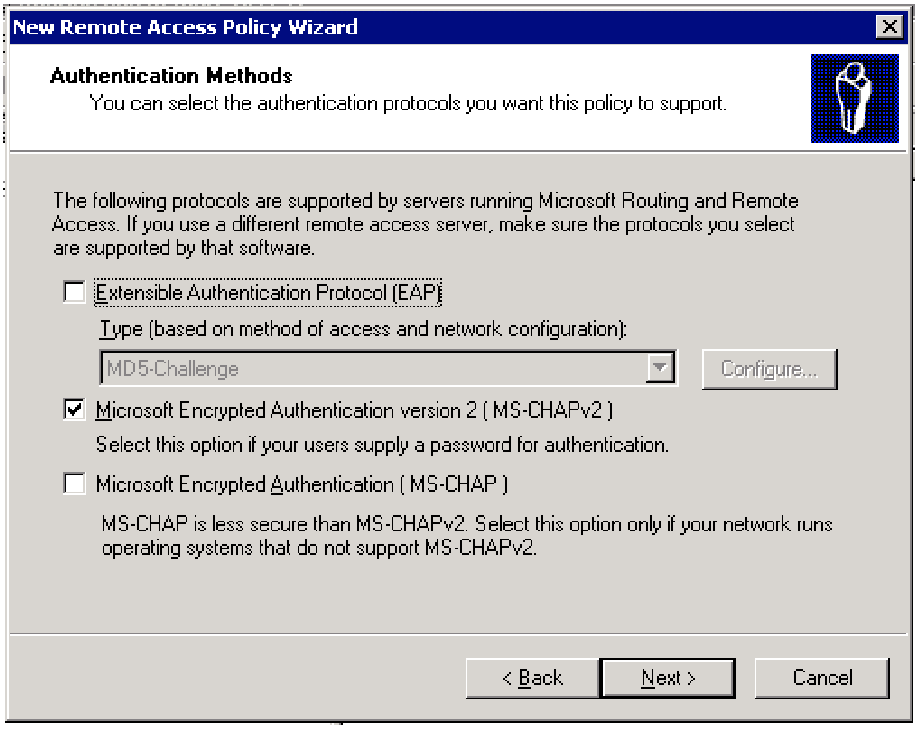
User access permissions are specified in the user account.

● Group

Individual user permissions override group permissions.

Group name:

I add a Domain Security Group named Field Users that contains each of the remote access field users as a member. Next,



New Remote Access Policy Wizard

Authentication Methods

You can select the authentication protocols you want this policy to support.

The following protocols are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the protocols you select are supported by that software.

□ Extensible Authentication Protocol (EAP)

Type (based on method of access and network configuration):

MD5-Challenge

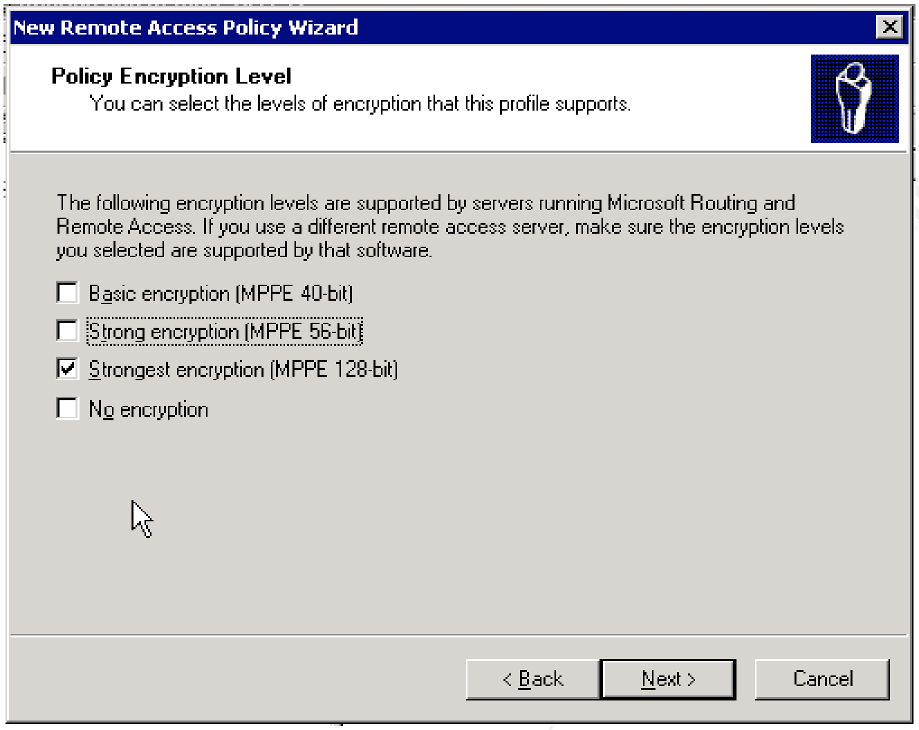
☑ Microsoft Encrypted Authentication version 2 (MS-CHAPv2)

Select this option if your users supply a password for authentication.

□ Microsoft Encrypted Authentication (MS-CHAP)

MS-CHAP is less secure than MS-CHAPv2. Select this option only if your network runs operating systems that do not support MS-CHAPv2.

EAP can be used for smart card and other third party authentication methods. In the example of Case 2, security tokens were not cost effective (too many field users were using them as bottle openers and breaking them). Next,



Policy Encryption Level

You can select the levels of encryption that this profile supports.

The following encryption levels are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the encryption levels you selected are supported by that software.

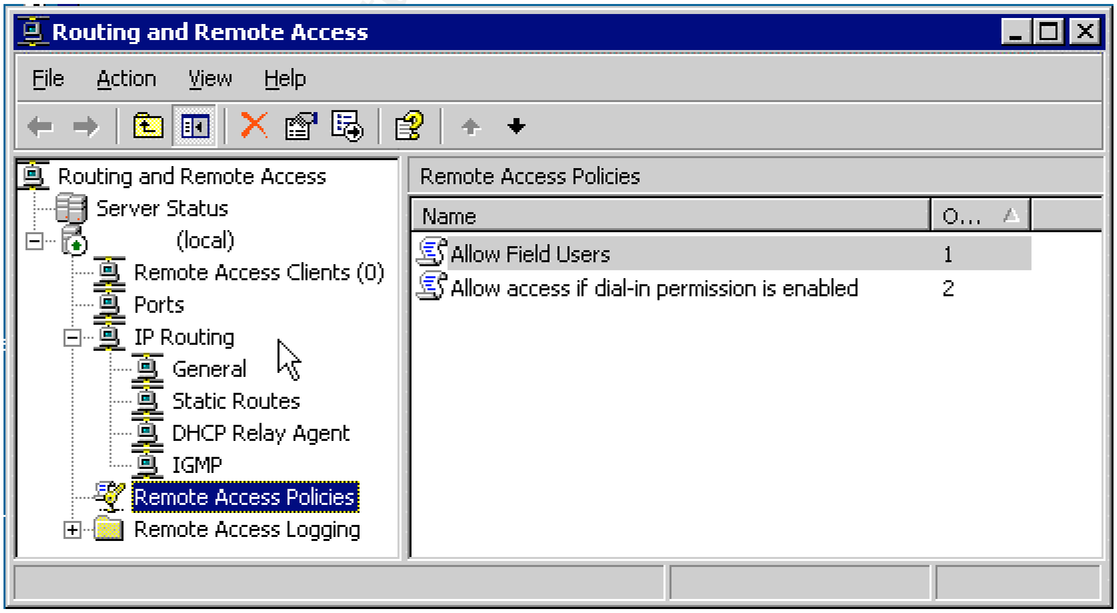
☐ Basic encryption (MPPE 40-bit)

☐ Strong encryption (MPPE 56-bit)

☑ Strongest encryption (MPPE 128-bit)

☐ No encryption

As the clients are all running Windows 2000, I can require the strongest encryption. Basic and Strong encryption (40 and 56 bit) are not considered secure. I click Next to complete the wizard:

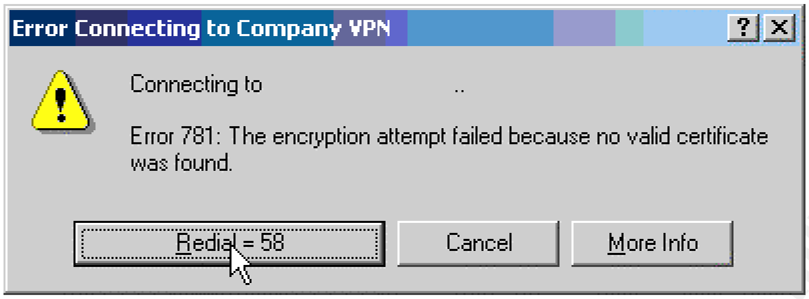


Remote Access Policies

Name	O...
Allow Field Users	1
Allow access if dial-in permission is enabled	2

The Remote Access Policy is complete.

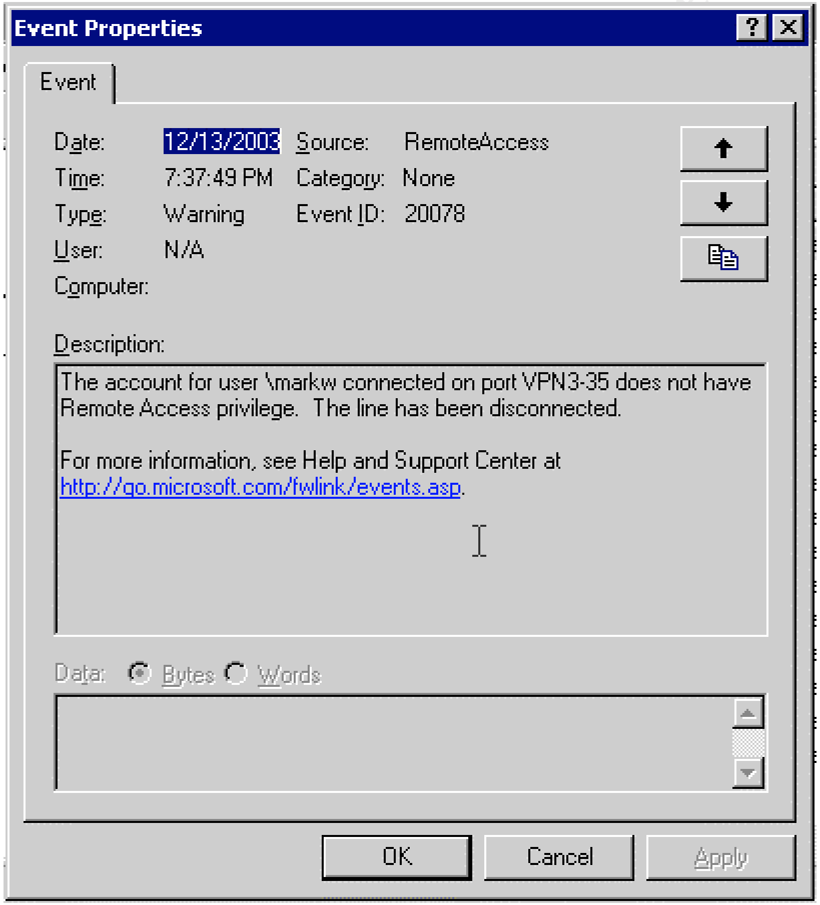
Finally, I'll perform a quick test: A user in the Field Users group tries to connect via PPTP rather than L2TP (as required by the Allow Field Users Policy). The results:


Error Connecting to Company VPN

Connecting to ..

Error 781: The encryption attempt failed because no valid certificate was found.

And the Server:


Event Properties

Date: 12/13/2003 Source: RemoteAccess
Time: 7:37:49 PM Category: None
Type: Warning Event ID: 20078
User: N/A
Computer:

Description:

The account for user \markw connected on port VPN3-35 does not have Remote Access privilege. The line has been disconnected.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

This brings us to the next example:

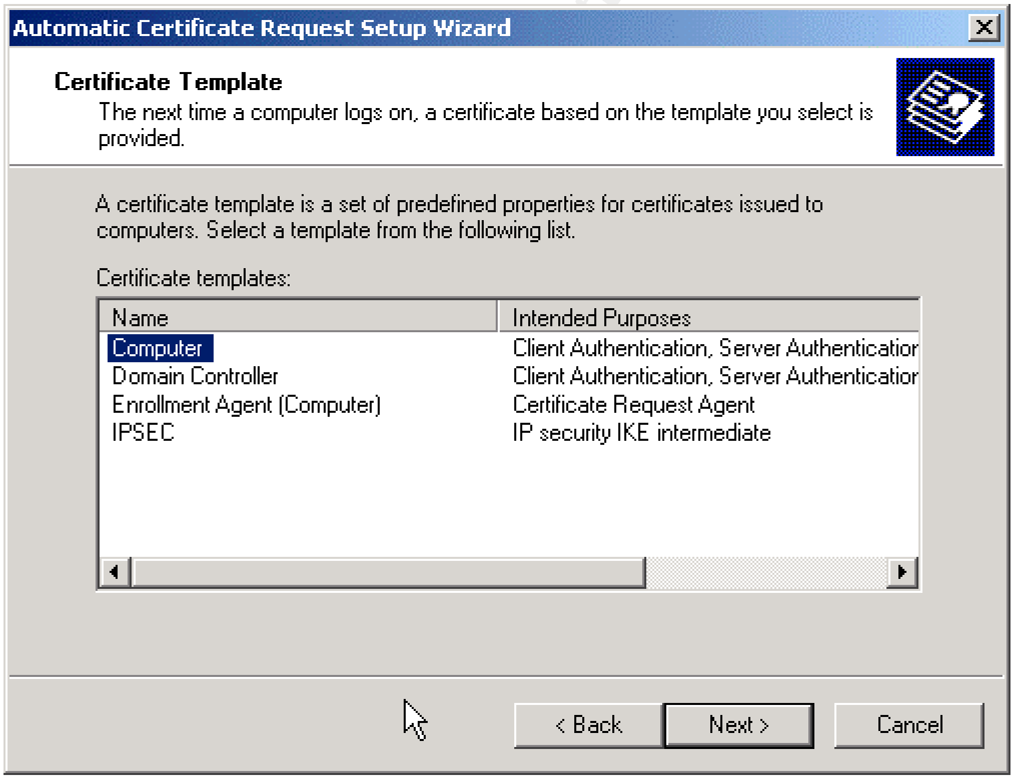
Example: Creating a RRAS Computer Certificate for L2TP

The diagram in Case 2 shows a firewall between the RRAS Server and the rest of the network. The RRAS server is, however, a domain member and is managed by Active Directory Group Policy (firewall configuration is covered later).

The RRAS Server will require certificates as will the VPN clients to authenticate using L2TP. The assumption is made that an Enterprise CA is on-line, it is available over the network, and computer auto-enrollment is configured.

I'll begin by creating a Group Policy for the RRAS Server to get the required certificates from the CA. I start by creating a new group policy for the RRAS Server in the Group Policy Management mmc snap-in and editing it. Then, in the Group Policy mmc I expand Computer Configuration > Windows Settings > Security Settings > Public Key Policies > Automatic Certificate Request Settings.

I right-click Automatic Certificate Request and choose New… > Automatic Certificate request. A wizard starts:



Certificate Template

The next time a computer logs on, a certificate based on the template you select is provided.

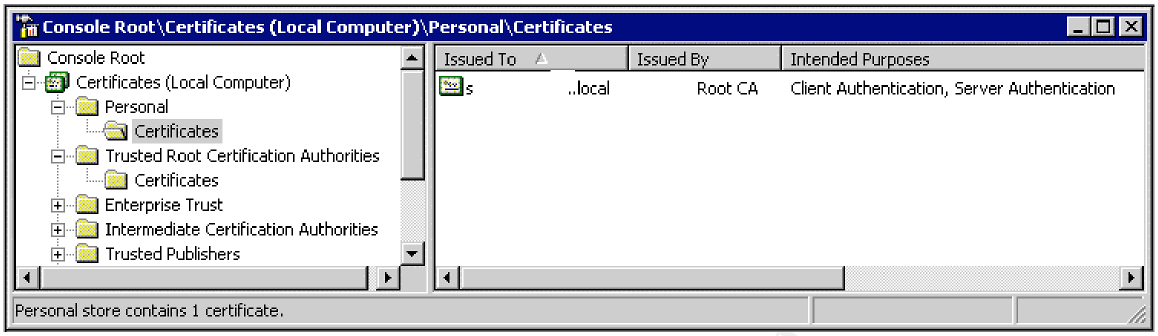
A certificate template is a set of predefined properties for certificates issued to computers. Select a template from the following list.

Certificate templates:

Name	Intended Purposes
Computer	Client Authentication, Server Authenticatior
Domain Controller	Client Authentication, Server Authenticatior
Enrollment Agent (Computer)	Certificate Request Agent
IPSEC	IP security IKE intermediate

I would like the RRAS server to keep both a Computer (for this example) and an IPSEC certificate (for later). I add a Computer Certificate Template and run the wizard again so I can add IPSEC.

Next, I link the GPO to the RRAS Server's OU in the Group Policy Management mmc, go to the RRAS Server, and gpupdate (Windows .Net) to refresh its group policies. I next open the Certificates mmc snap-in on the RRAS Server to verify the computer certificate has been installed:


Console Root\Certificates (Local Computer)\Personal\Certificates

Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers

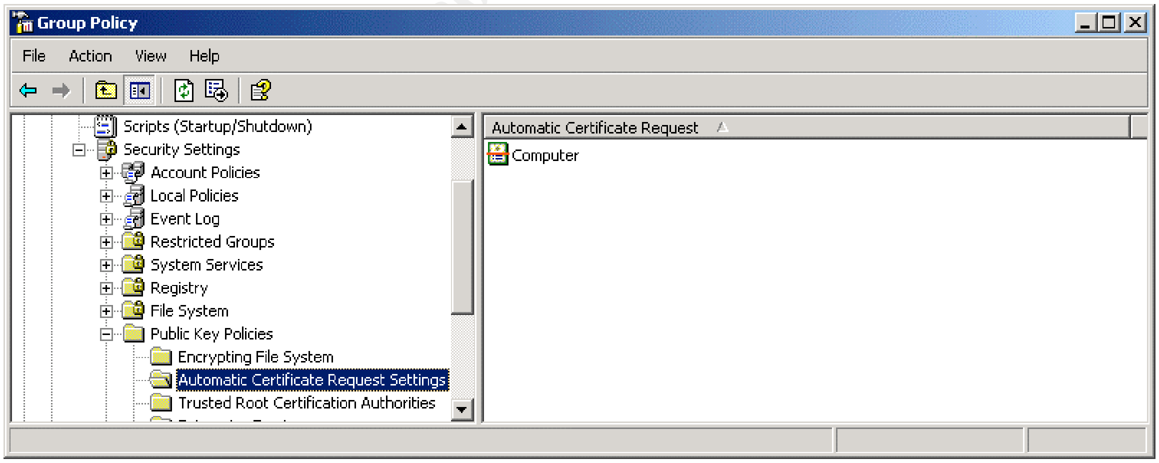
Issued To	Issued By	Intended Purposes
s ..local	Root CA	Client Authentication, Server Authentication

Personal store contains 1 certificate.

Example: Creating VPN Client Certificates Through Group Policy (Case 2)

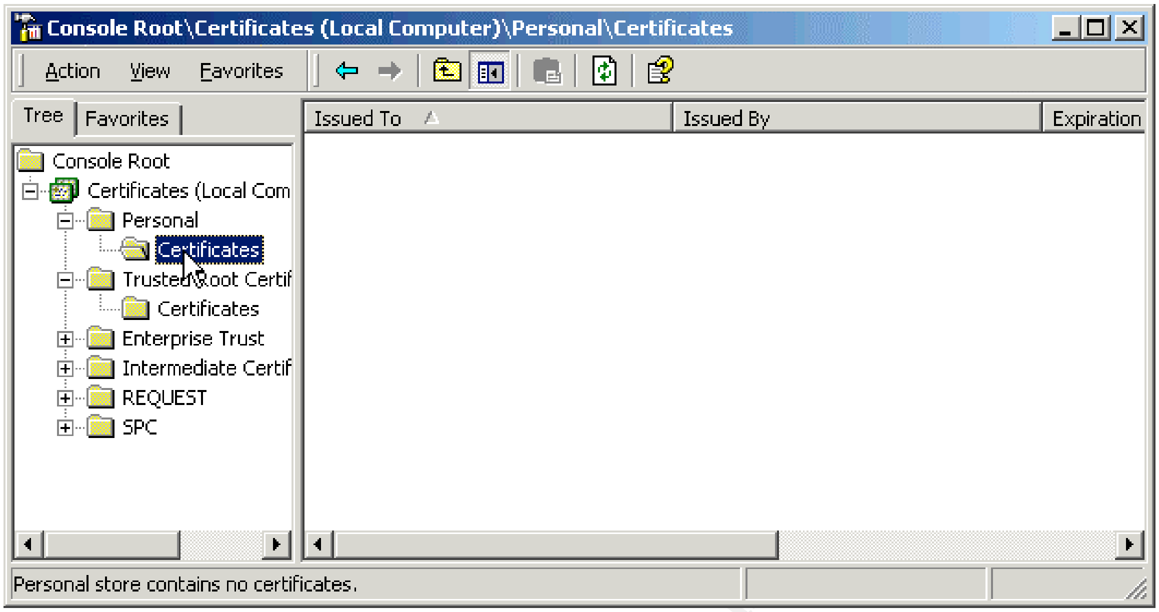
While the field laptops are in head office, it is an opportune time to push out certificates so the VPN clients can do L2TP.

I start with the existing Field Laptops Group Policy in the Group Policy mmc snap-in. As with the RRAS Server I go to Computer Configuration > Windows Settings > Security Settings > Public Key Polices > Automatic Certificate Request Settings and I request a new Computer certificate. When complete:


Group Policy

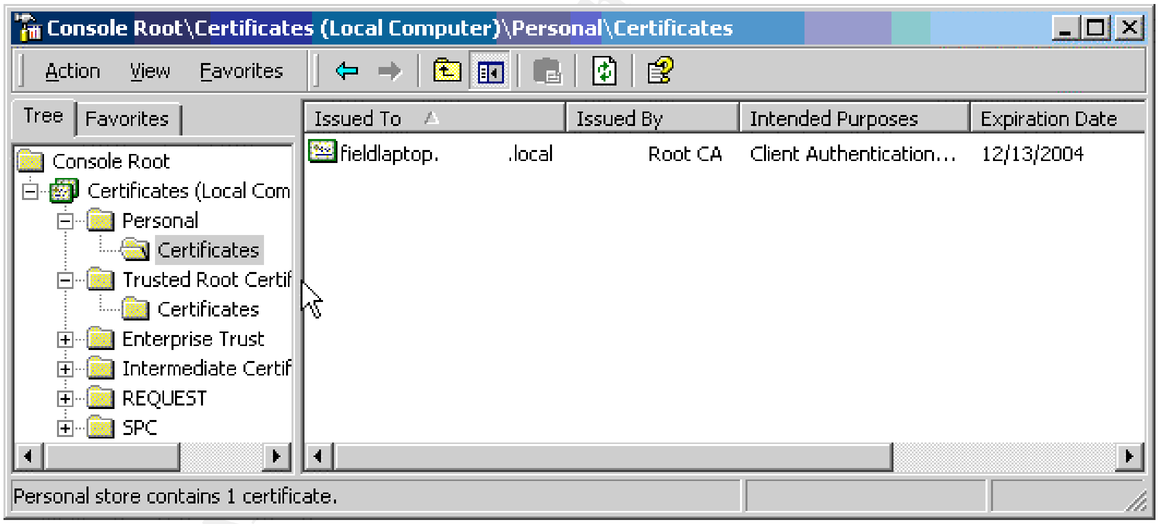
Automatic Certificate Request
Computer

I then go to the Windows 2000 laptop and open the Certificates mmc snap-in for the local machine. I check for the certificate:



Personal store contains no certificates.

Hmmm. Not there yet. The laptops are Windows 2000, so I type “secedit /refreshpolicy”, wait a few seconds, and refresh:



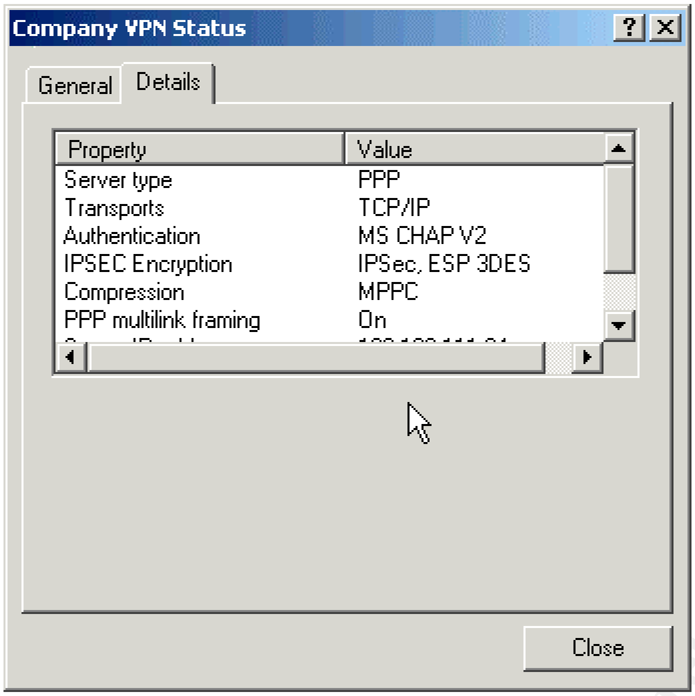
Issued To	Issued By	Intended Purposes	Expiration Date
fieldlaptop. .local	Root CA	Client Authentication...	12/13/2004

Personal store contains 1 certificate.

This also adds a certificate for the Enterprise CA in the Trusted Root Certificates > Certificates folder.

But does it work?

I disconnect from the network, and attempt the L2TP connection now. It works!



Property	Value
Server type	PPP
Transports	TCP/IP
Authentication	MS CHAP V2
IPSEC Encryption	IPSec, ESP 3DES
Compression	MPPC
PPP multilink framing	On

Figure 19 - A successful L2TP connection!

Security Templates

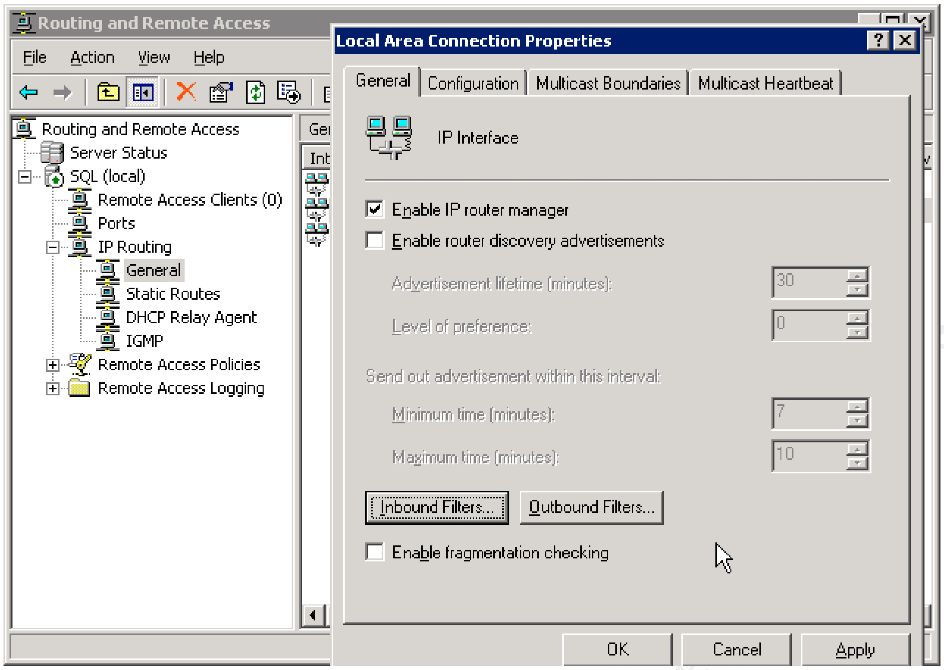
The RRAS server should be hardened on a variety of fronts. The most effective way of doing this is finding a good security template, customizing it for the environment, and applying it (possibly as part of Group Policy).

An example of selecting and applying security templates is covered in the FTP Server section.

RRAS Filters

RRAS Filters deserve a security mention (and an example!).

To further protect the destination network packet filters can be installed on real and virtual interfaces in the RRAS mmc snap-in:



☑ Enable IP router manager

□ Enable router discovery advertisements

Advertisement lifetime (minutes): 30

Level of preference: 0

Send out advertisement within this interval:

Minimum time (minutes): 7

Maximum time (minutes): 10

□ Enable fragmentation checking

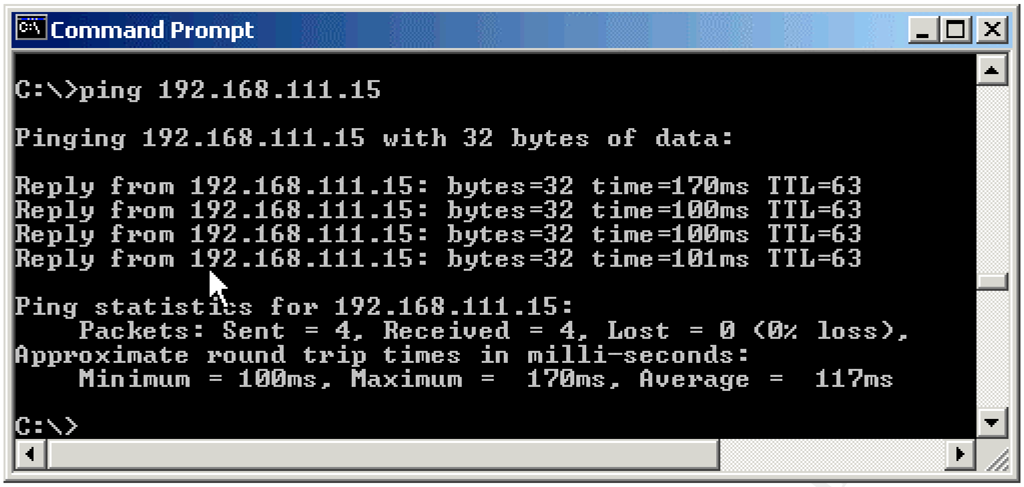
Figure 20 - RRAS Interface Filters

Example: Configuring RRAS Filters to Allow Access Only to the FTP Server

Filters for a complete interface can be seen above in Figure 20 - RRAS Interface Filters. This dialog can be reached through IP Routing > General and by right-clicking the interface and picking Properties. One disadvantage of applying filters here is they apply for all traffic on the interface. If you apply a filter to the lone Ethernet card, for example, it applies to all traffic going and coming from the server.

In this example, I chose to apply filters to the Field User Remote Access policy I created earlier. By doing this, I can make the filter apply only to the Field Users. The filter is simple: only allow field users access to the FTP Server.

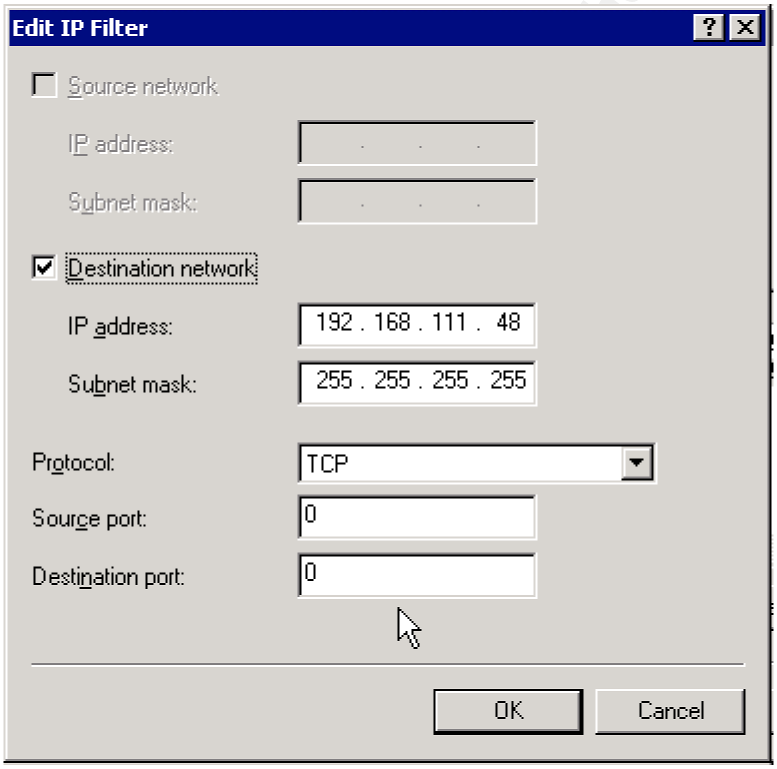
First I make a connection with my client and ping the database server (192.168.111.15) and the FTP server (192.168.111.48).



```
C:\>ping 192.168.111.15

Pinging 192.168.111.15 with 32 bytes of data:

Reply from 192.168.111.15: bytes=32 time=170ms TTL=63
Reply from 192.168.111.15: bytes=32 time=100ms TTL=63
Reply from 192.168.111.15: bytes=32 time=100ms TTL=63
Reply from 192.168.111.15: bytes=32 time=101ms TTL=63

Ping statistics for 192.168.111.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 100ms, Maximum =  170ms, Average =  117ms

C:\>
```

Next, I write my packet filters. I select the "Allow Field Users" Policy from Remote Access Policies in the Routing and Remote Access mmc snap-in.

Then I pick Edit Profile… and the IP tab. Input… and Output… buttons are available. I select input first and create a Permit only rule:



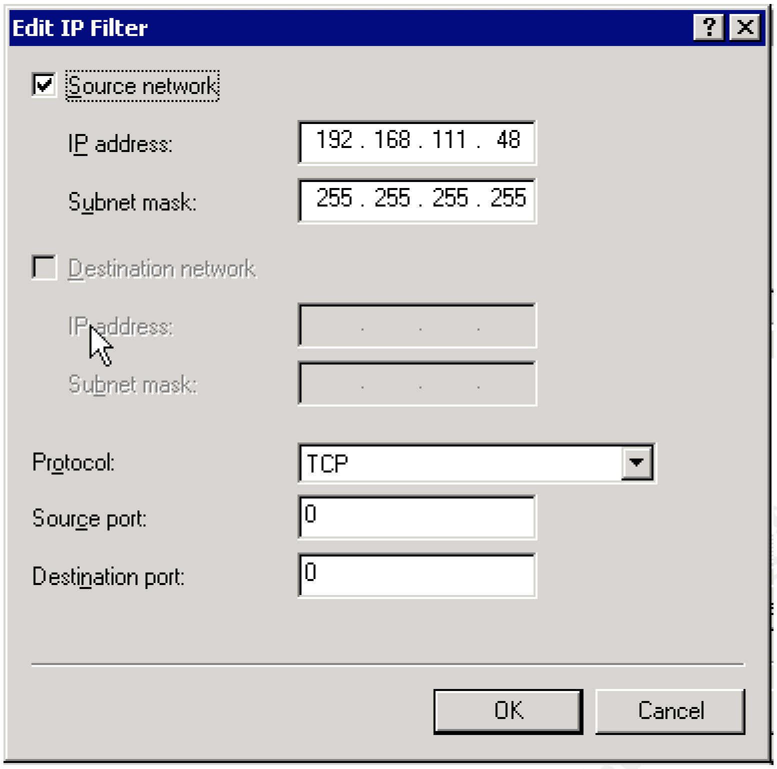
□ Source network

IP address:	. . .
Subnet mask:	. . .

☑ Destination network

IP address:	192 . 168 . 111 . 48
Subnet mask:	255 . 255 . 255 . 255
Protocol:	TCP
Source port:	0
Destination port:	0

I also want the FTP server to be the only server that can access the Field users while they are logged in (I don't want other employees, or viruses, to access the laptops while they are logged in), so I make an Output filter as well:



☑ Source network

IP address: 192 . 168 . 111 . 48

Subnet mask: 255 . 255 . 255 . 255

□ Destination network

IP address:

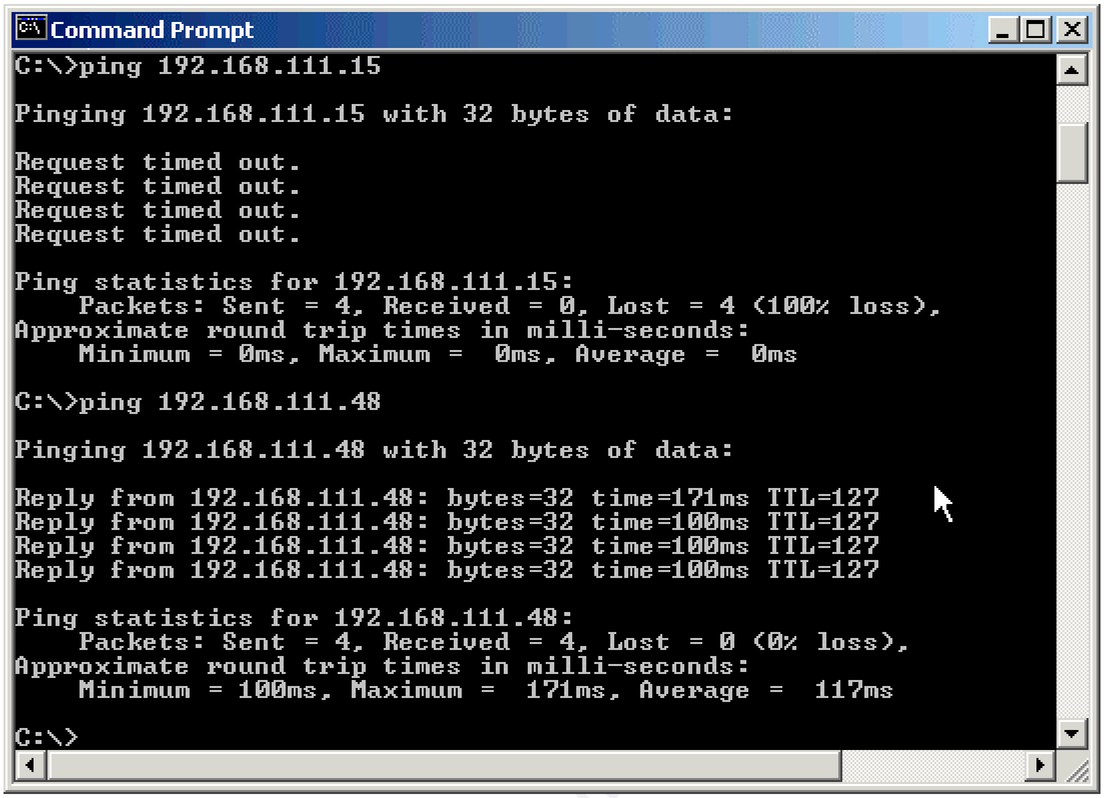
Subnet mask:

Protocol: TCP

Source port: 0

Destination port: 0

I save my changes and restart RRAS. Now when I dial in:



```
C:\>ping 192.168.111.15

Pinging 192.168.111.15 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.111.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping 192.168.111.48

Pinging 192.168.111.48 with 32 bytes of data:

Reply from 192.168.111.48: bytes=32 time=171ms TTL=127
Reply from 192.168.111.48: bytes=32 time=100ms TTL=127
Reply from 192.168.111.48: bytes=32 time=100ms TTL=127
Reply from 192.168.111.48: bytes=32 time=100ms TTL=127

Ping statistics for 192.168.111.48:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 100ms, Maximum =  171ms, Average =  117ms

C:\>
```

I can no longer access the database server, but the FTP server is still available. The RRAS filters are working.

IPSec Filters

IPSec filters can be used in conjunction with RRAS filters. They operate at a lower level in the stack. Windows 2000 Service Pack 1 or later must be installed if both are to be used together.

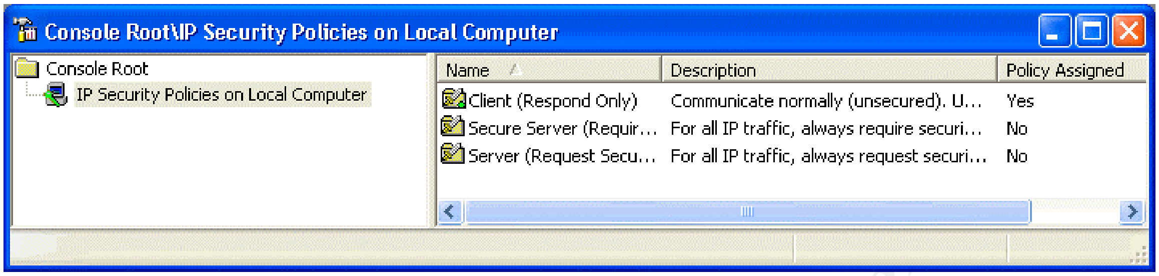
An IPSec Filter can be used to encrypt traffic from the RRAS Server to the FTP Server.

Example: Encrypting Traffic from RRAS to the FTP Server (Case 2)

To encrypt the packets between the two servers, both will require IPSec Policies. For this example, the RRAS server is at 192.168.111.6 and the FTP Server is at 192.168.111.66.

I'll start on both computers with the IP Security Policy Management mmc snap-in.

The FTP Server will be a simple example. I run the IP Security Policy Management tool on the local computer, and turn on the Client (Respond Only) rule. This allows the FTP Server to participate in an IPSec connection. I could also have pushed it to the FTP Server through Group Policy.

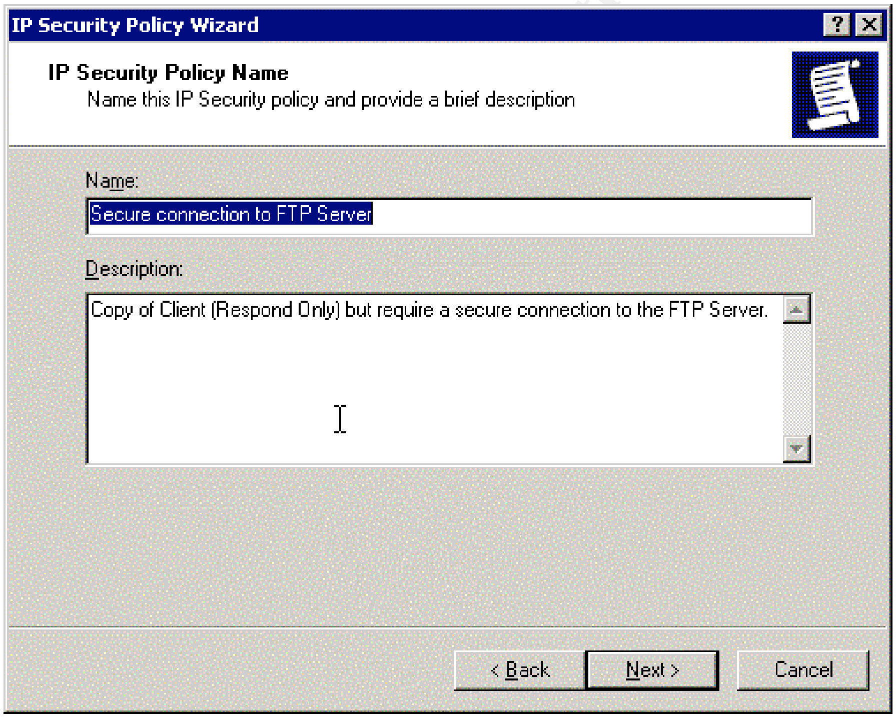


Console Root\IP Security Policies on Local Computer

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecured). U…	Yes
Secure Server (Requir…	For all IP traffic, always require securi…	No
Server (Request Secu…	For all IP traffic, always request securi…	No

The RRAS Server has a more complicated filter. I want a policy on the Ethernet card that enforces all IP traffic to the FTP server to be encrypted, but all other traffic need not be.

I run the IP Security Policy Management snap-in on the RRAS server. It is recommended not to modify the default rules, but to create a new rule (GUID problems). So I right-click on IP Security Policies to Create IP Security Policy… This starts the wizard.



IP Security Policy Wizard

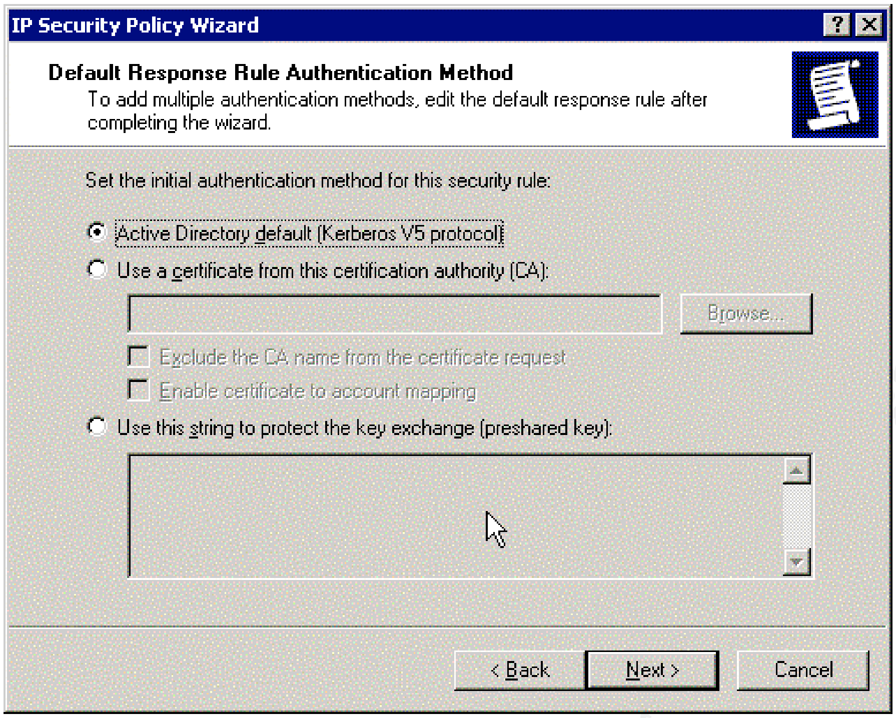
IP Security Policy Name

Name this IP Security policy and provide a brief description

Name: Secure connection to FTP Server

Description: Copy of Client (Respond Only) but require a secure connection to the FTP Server.

Then I check the Active the Default Response Rule.



IP Security Policy Wizard

Default Response Rule Authentication Method

To add multiple authentication methods, edit the default response rule after completing the wizard.

Set the initial authentication method for this security rule:

● Active Directory default (Kerberos V5 protocol)

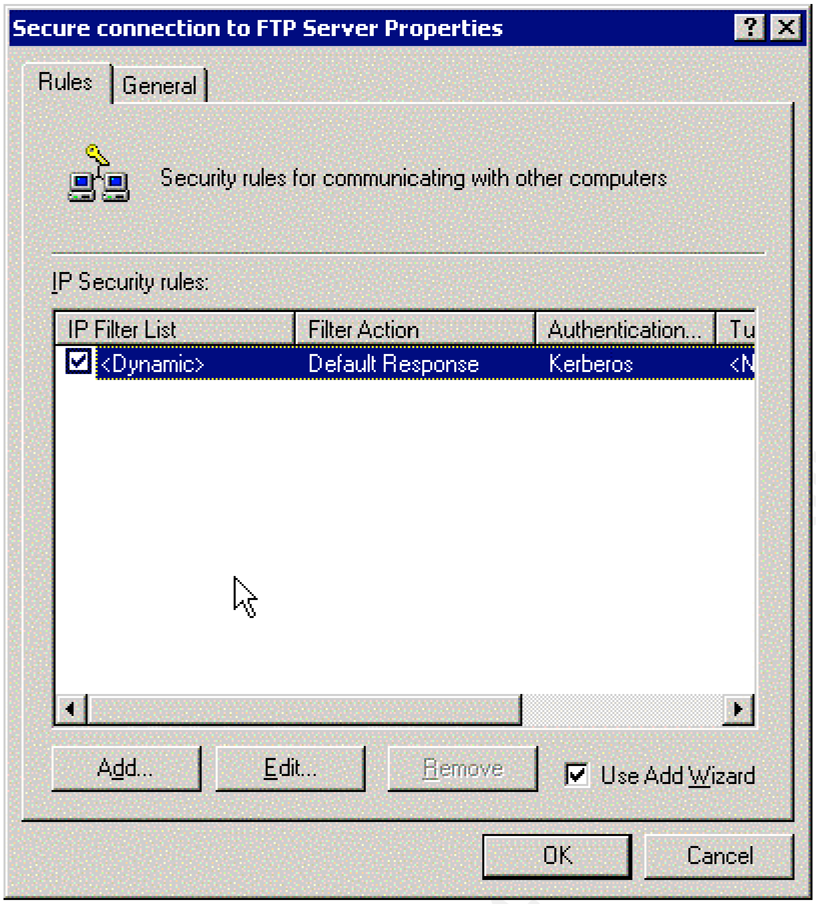
○ Use a certificate from this certification authority (CA):

□ Exclude the CA name from the certificate request

□ Enable certificate to account mapping

○ Use this string to protect the key exchange (preshared key):

Both machines are able to use Kerberos to authenticate.



Secure connection to FTP Server Properties

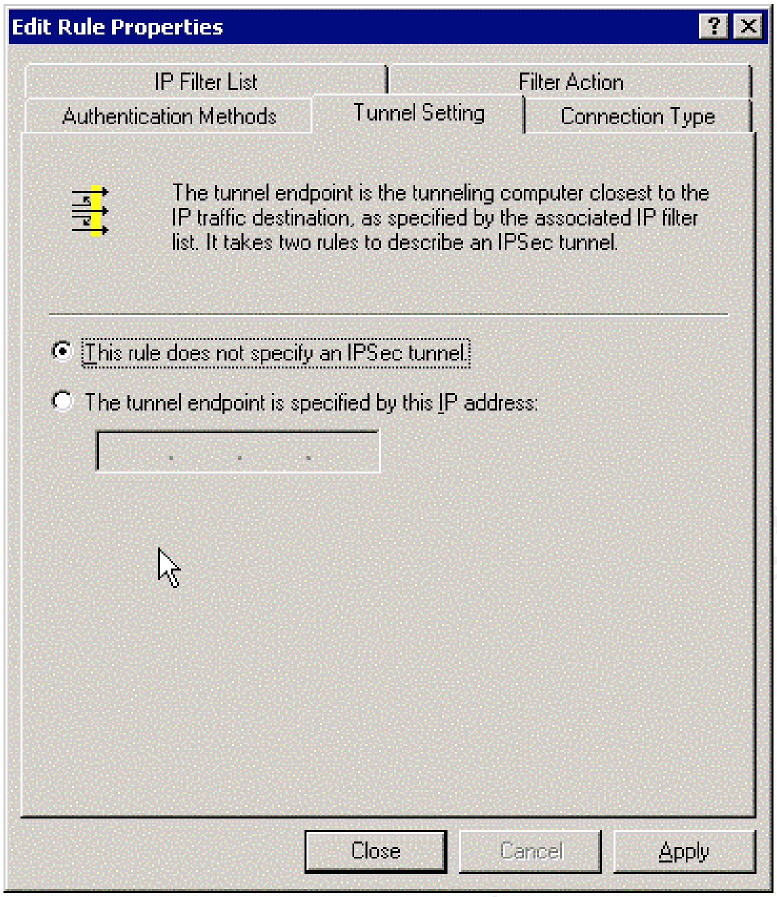
Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ <Dynamic>	Default Response	Kerberos	<N

☑ Use Add Wizard

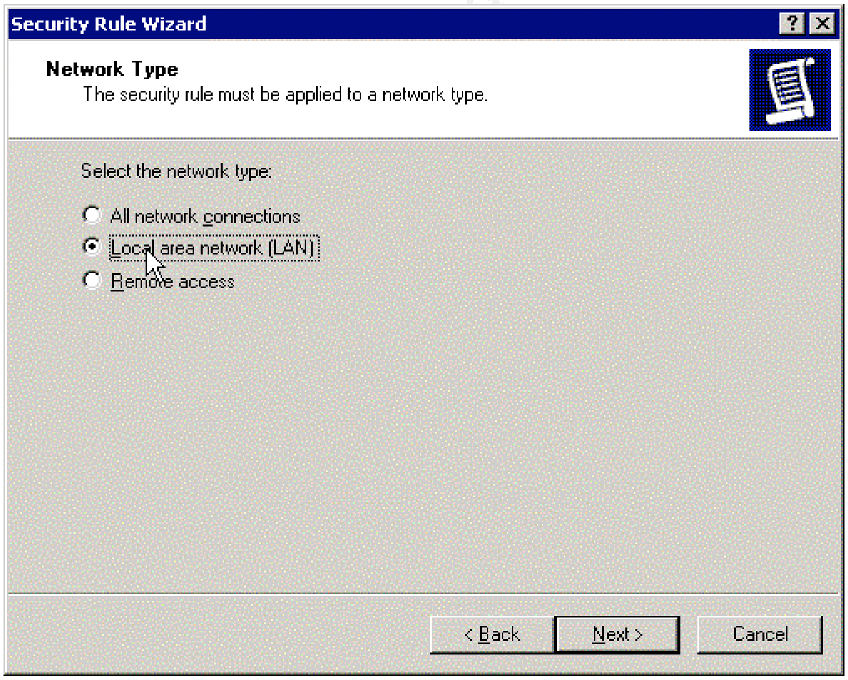
And we are shown the default rule. I now add a rule to encrypt traffic to 192.168.111.66. I pick Add…



The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

● This rule does not specify an IPSec tunnel.

○ The tunnel endpoint is specified by this IP address:



Network Type

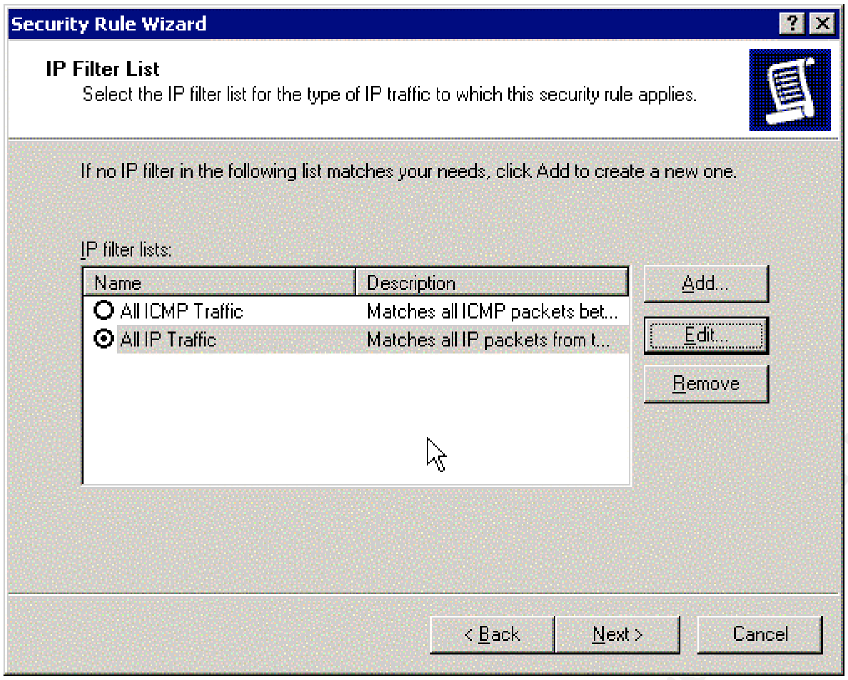
The security rule must be applied to a network type.

Select the network type:

○ All network connections

● Local area network (LAN)

○ Remote access



IP Filter List

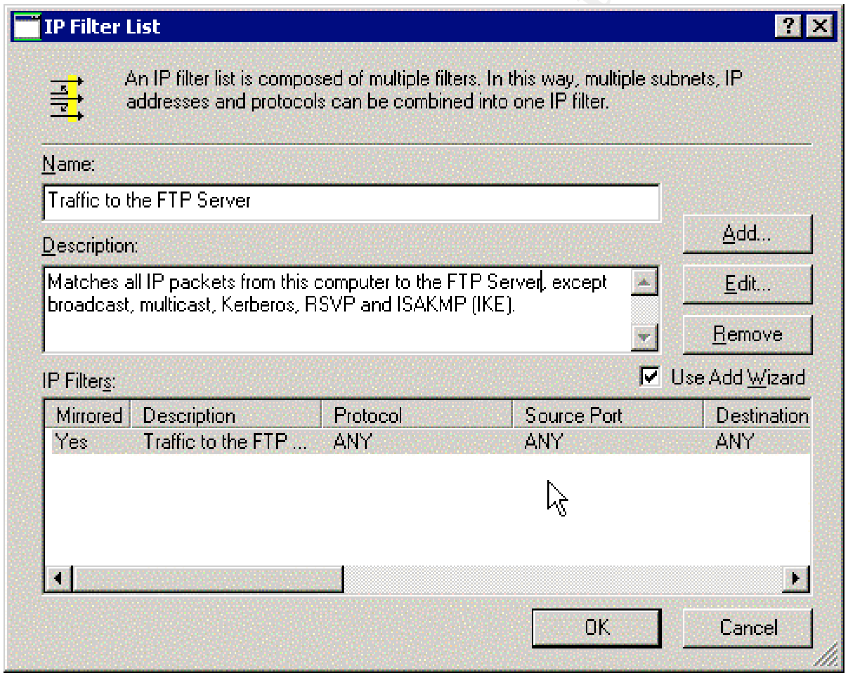
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
● All IP Traffic	Matches all IP packets from t...

Here I want to add a new Filter List. Click Add…



An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

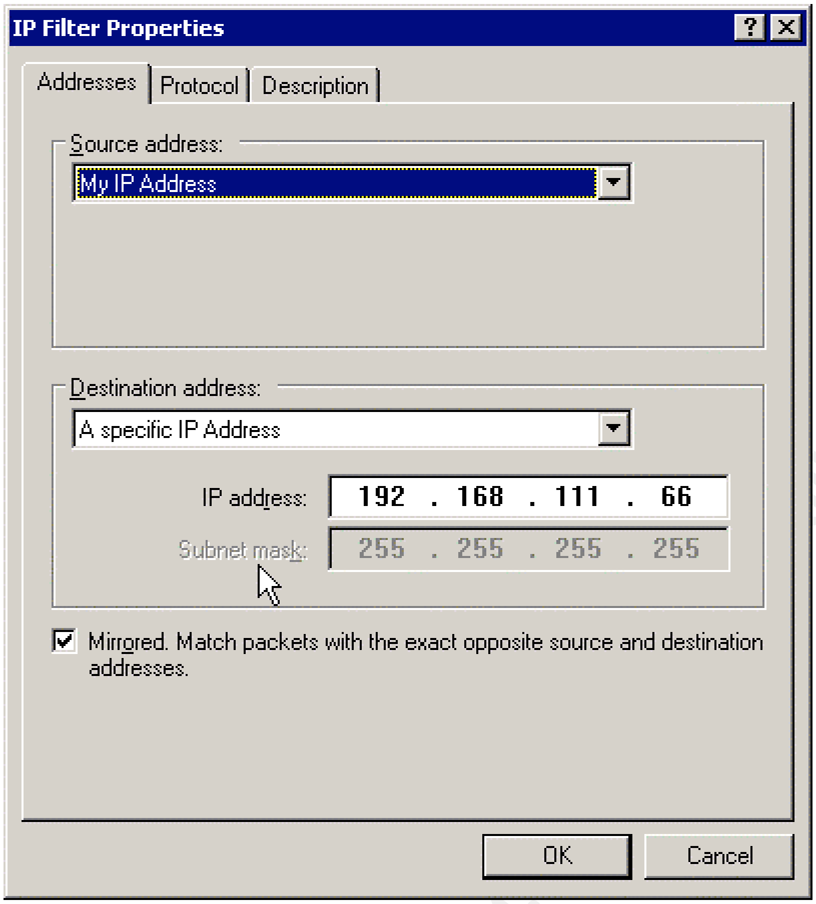
Name: Traffic to the FTP Server

Description: Matches all IP packets from this computer to the FTP Server, except broadcast, multicast, Kerberos, RSVP and ISAKMP (IKE).

☑ Use Add Wizard

IP Filters:

Mirrored	Description	Protocol	Source Port	Destination
Yes	Traffic to the FTP ...	ANY	ANY	ANY



IP Filter Properties

Source address:
My IP Address

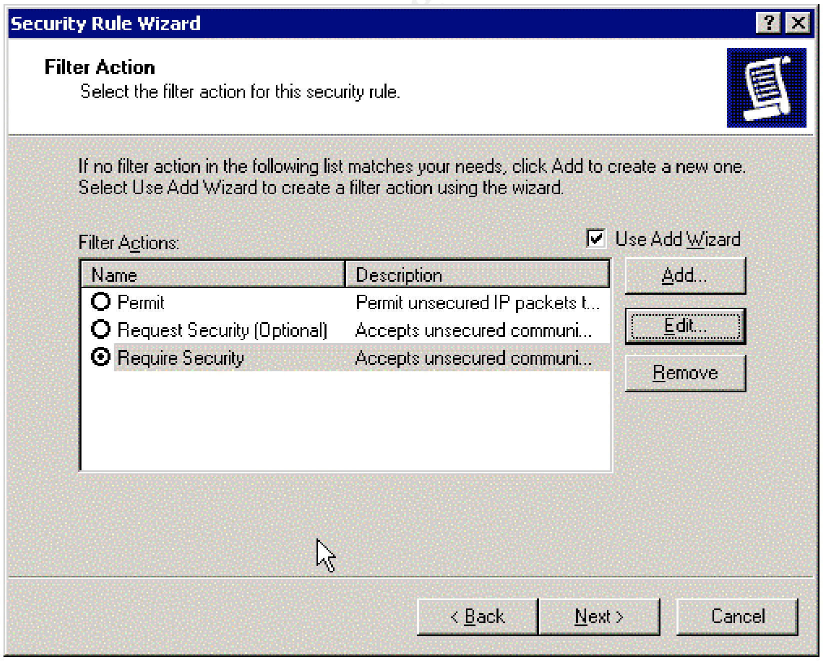
Destination address:
A specific IP Address

IP address: 192 . 168 . 111 . 66

Subnet mask: 255 . 255 . 255 . 255

☑ Mirrored. Match packets with the exact opposite source and destination addresses.

Once the filter is made, I need an action. Matching packets must be encrypted:



Security Rule Wizard

Filter Action

Select the filter action for this security rule.

If no filter action in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action using the wizard.

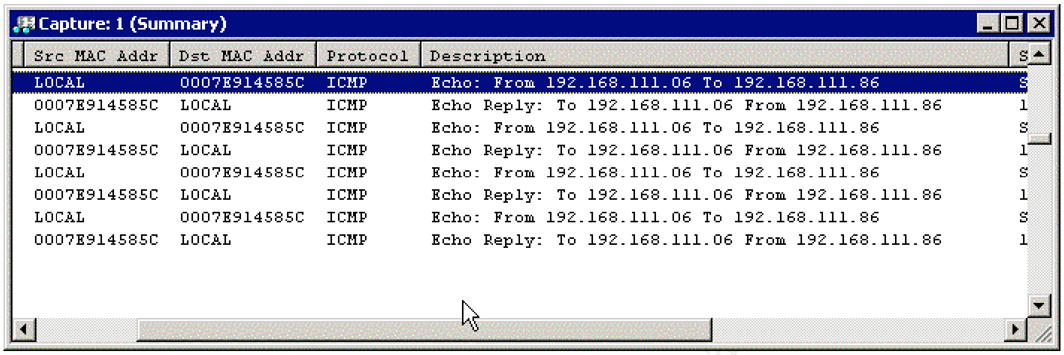
Filter Actions:

☑ Use Add Wizard

Name	Description
○ Permit	Permit unsecured IP packets t...
○ Request Security (Optional)	Accepts unsecured communi...
● Require Security	Accepts unsecured communi...

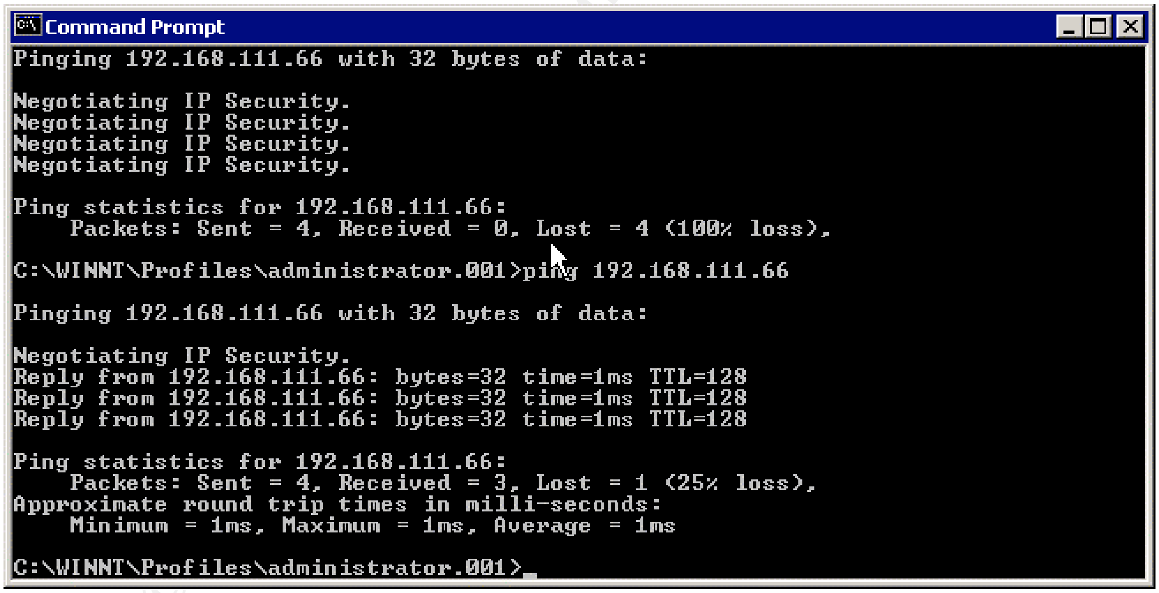
Once the new rules are done, the next step is to Assign them so they become active (only one policy can be active at a time). Right-click on the policy and pick Assign.

Now to test, from the RRAS server I pinged a random, but existing, machine on the network. It responded fine. The packet trace:



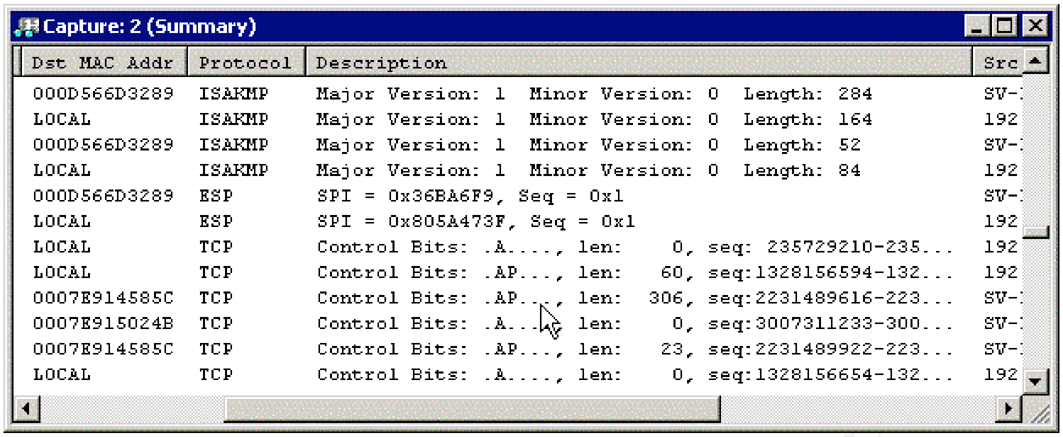
Src MAC Addr	Dst MAC Addr	Protocol	Description	S
LOCAL	0007E914585C	ICMP	Echo: From 192.168.111.06 To 192.168.111.86	S
0007E914585C	LOCAL	ICMP	Echo Reply: To 192.168.111.06 From 192.168.111.86	1
LOCAL	0007E914585C	ICMP	Echo: From 192.168.111.06 To 192.168.111.86	S
0007E914585C	LOCAL	ICMP	Echo Reply: To 192.168.111.06 From 192.168.111.86	1
LOCAL	0007E914585C	ICMP	Echo: From 192.168.111.06 To 192.168.111.86	S
0007E914585C	LOCAL	ICMP	Echo Reply: To 192.168.111.06 From 192.168.111.86	1
LOCAL	0007E914585C	ICMP	Echo: From 192.168.111.06 To 192.168.111.86	S
0007E914585C	LOCAL	ICMP	Echo Reply: To 192.168.111.06 From 192.168.111.86	1

Traffic is not encrypted. Next I pinged the FTP Server, 192.168.111.66 and we can see the IPSec connection is negotiated and finally completes:



```
Pinging 192.168.111.66 with 32 bytes of data:

Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.

Ping statistics for 192.168.111.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\WINNT\Profiles\administrator.001>ping 192.168.111.66

Pinging 192.168.111.66 with 32 bytes of data:

Negotiating IP Security.
Reply from 192.168.111.66: bytes=32 time=1ms TTL=128
Reply from 192.168.111.66: bytes=32 time=1ms TTL=128
Reply from 192.168.111.66: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.111.66:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\WINNT\Profiles\administrator.001>_
```

Figure 21 - Establishing an IPSec Connection

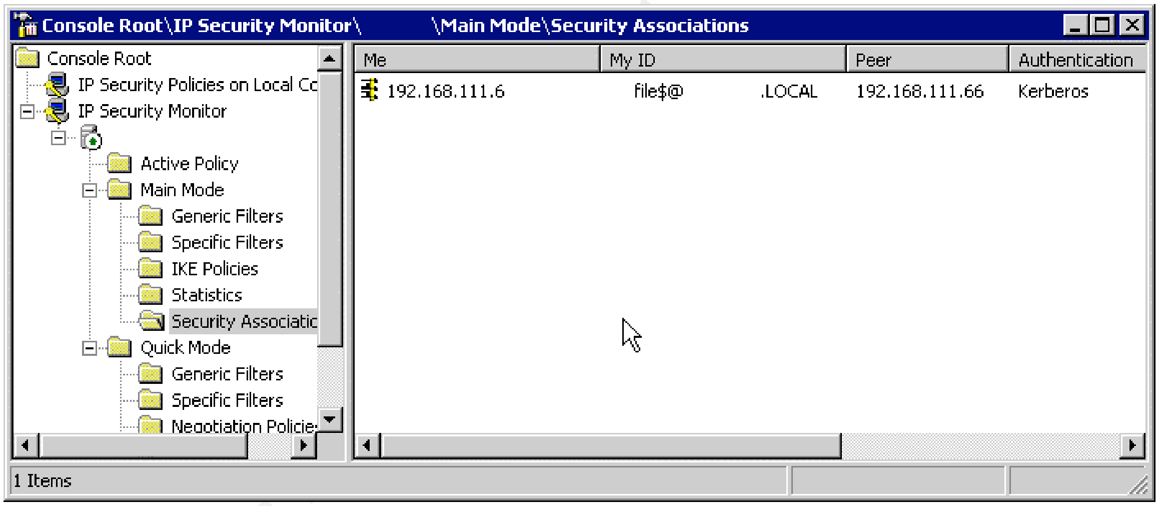


Capture: 2 (Summary)

```
Dst MAC Addr   Protocol  Description                                     Src
000D566D3289   ISAKMP    Major Version: 1  Minor Version: 0  Length: 284  SV-1
LOCAL          ISAKMP    Major Version: 1  Minor Version: 0  Length: 164  192
000D566D3289   ISAKMP    Major Version: 1  Minor Version: 0  Length: 52   SV-1
LOCAL          ISAKMP    Major Version: 1  Minor Version: 0  Length: 84   192
000D566D3289   ESP       SPI = 0x36BA6F9, Seq = 0x1                       SV-1
LOCAL          ESP       SPI = 0x805A473F, Seq = 0x1                      192
LOCAL          TCP       Control Bits: .A...., len:    0, seq: 235729210-235...  192
LOCAL          TCP       Control Bits: .AP..., len:   60, seq:1328156594-132...  192
0007E914585C   TCP       Control Bits: .AP..., len:  306, seq:2231489616-223...  SV-1
0007E915024B   TCP       Control Bits: .A...., len:    0, seq:3007311233-300...  SV-1
0007E914585C   TCP       Control Bits: .AP..., len:   23, seq:2231489922-223...  SV-1
LOCAL          TCP       Control Bits: .A...., len:    0, seq:1328156654-132...  192
```

Figure 22 - Packet Trace of IPSec Connection

You can see the key exchange and some IPSec Packets in Figure 22. No ICMP packets were found in the packet dump. Looking at the IP Security Monitor on RRAS:



Console Root\IP Security Monitor\   \Main Mode\Security Associations

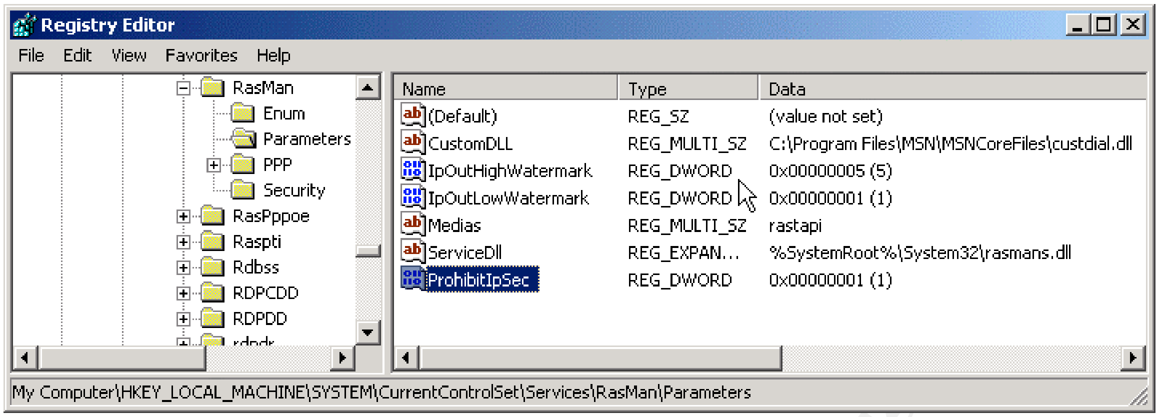
Me	My ID	Peer	Authentication
192.168.111.6	file$@ .LOCAL	192.168.111.66	Kerberos

1 Items

We can see a secure connection was made to the FTP Server.

L2TP Dynamic IPSec Policies

It is a security concern that RRAS automatically injects a dynamically generated IPSec policy (if it injected no policy, for example, the L2TP traffic would not be encrypted). To ensure this is working correctly, an IPSec policy can be assigned to the RRAS Server through group policy and the default injection behavior disabled through a registry setting. The registry setting is:



Name	Type	Data
(Default)	REG_SZ	(value not set)
CustomDLL	REG_MULTI_SZ	C:\Program Files\MSN\MSNCoreFiles\custdial.dll
IpOutHighWatermark	REG_DWORD	0x00000005 (5)
IpOutLowWatermark	REG_DWORD	0x00000001 (1)
Medias	REG_MULTI_SZ	rastapi
ServiceDll	REG_EXPAN...	%SystemRoot%\System32\rasmans.dll
ProhibitIpSec	REG_DWORD	0x00000001 (1)

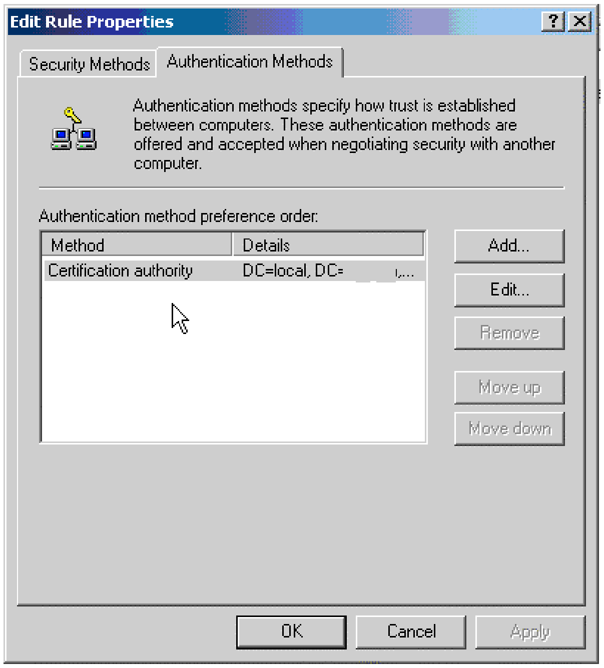
My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters

Figure 23 - ProhibitIpSec Registry Entry

The next stop is to add a new IPSec Security Policy. To do this through Group Policy, open it in Group Policy Manager and go to Computer Configuration > Windows Settings > Security Settings > IP Security Policies on Active Directory. Right-Click to “Create IP Security Policy…”.

For the sake of brevity, I can’t cover all the steps in this paper. The detailed instructions are available on Microsoft Knowledge Base (Q240262)[56]. The only difference is Step 10: rather then selecting a pre-shared key, select your certificate authority instead:

[56] “How to Configure a L2TP/IPSec Connection Using Pre-shared Key Authentication”, URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;240262, (14 Dec. 2003).



Edit Rule Properties

Security Methods | Authentication Methods

Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Certification authority	DC=local, DC=[redacted],...

FTP Server

The FTP Server needs to be placed in a secure environment, the server itself needs to be hardened, the FTP Service needs to be protected, and the application folders themselves must be locked down.

Secure the Environment

The computer that will be providing FTP Services should be placed in a secure environment. This includes physical security as well as network security.

Firewall Configuration

The FTP server should be placed behind a firewall(s). A packet filtering firewall needs to allow connections from the internet (unless the Program Clients are in a known IP space) to port 21 and all ports > 1024 (as explained in Appendix D).

As this is a rather large hole, it may be wise to protect the FTP server with a firewall that supports stateful packet inspection[57] (SPI) rather than packet filtering alone. This gives the firewall some knowledge of how the passive FTP protocol works and the ability to better recognize legitimate initiated FTP traffic.

Even more secure would be to use an FTP Proxy. The proxy accepts connections from the Program client and route them to the real FTP server. The FTP Proxy is able to restrict unnecessary FTP commands and check the validity of requests before they are passed to the FTP server (which helps protect against buffer overrun attacks). The commands required are:

PASS
USER
TYPE
PWD
PASV
DELE
APPE
MKD
STOR
RETR

[57] See http://www.webopedia.com/TERM/S/stateful_inspection.html for a complete definition.

LIST
QUIT

All others can be blocked. See Appendix E for a typical FTP session.

The Program Client connects to the FTP server with a single username and password. A second login at the FTP proxy could be used as long as the logins can be chained together so, from the client's point-of-view, there is still a single login. For example, the login would need to be proxyftpuser@proxypassword:ftpuser to pass through another level of authentication at a Check Point Firewall 1 FTP Proxy[58].

Secure the Server

Ideally the server will only be used for the FTP Service (as in Case 2), but that is not true in smaller companies (Case 1). No matter how tight the budget, however, it is not recommended to put the database on the same server unless the data has no value.

It is extremely important to have the latest Service Packs installed. There have been numerous FTP bugs fixed in Service Packs.

Windows should be hardened to the point where only the required software is running, and that software is protected as much as possible. As the details of creating a bastion host would fill a book[59], an important step in securing the FTP server will be the use of Security Templates.

The choice of security template will depend on the FTP Server's roles. In Case 1 the FTP Server is also running RRAS and the SyncHost server. In Cases 2 and 3 the FTP Server is standalone, but it is required to Authenticate users with the domain controller and share a filesystem with the SyncHost Server. It may also be a requirement that the server be managed with Group Policy.

A good place to start for templates is the Center for Internet Security Benchmarks and Scoring Tools[60]. The chance of finding a template that perfectly

[58] From the Check Point Firewall 1 Guide pages 169-170

[59] "Securing Windows NT/2000 Servers for the Internet" by Stefan Norberg for example.

[60] "Windows 2000 Benchmarks", Oct. 2003, URL: http://www.cisecurity.org/bench_win2000.html, (14 Dec. 2003).

fits a security problem is small. However, there are well-tested templates that will provide a good starting point.

One such IIS template is the HISECWEB.INF file from Microsoft (see Appendix B). In its original form HISECWEB.INF is not recommended for Domain Controllers or RRAS Servers (it turns off two services that may be required for the Routing and Remote Access service to start).

Example: Securing a Windows 2000 FTP Server

I start with IIS 5 running on Windows 2000 Server with a fresh install of the FTP Service. To install FTP, I went to Add/Remove Programs in the Control Panel > Add/Remove Windows Components > Application Server > Details > Internet Information Service (IIS) > Details and selected File Transfer Protocol (FTP) Service. This automatically selected Common Files and the IIS Manager as well, but I unchecked web server services. I then installed all the latest critical updates from Microsoft's Update Site (http://windowsupdate.microsoft.com).

After installation, the Internet Information Services (IIS) Manager is available under Start > Administrative Tools. This is the GUI configuration tool for the FTP Server.

I will be applying this example to Case 2. The FTP Server is in an Active Directory domain. Windows Authentication (accounts from the Active Directory) is used to log field users into the FTP Server. As well, the FTP Server is sharing the "D:\Sync" folder to the SyncHost Server. The server is managed through Terminal Services in Remote Administration mode.

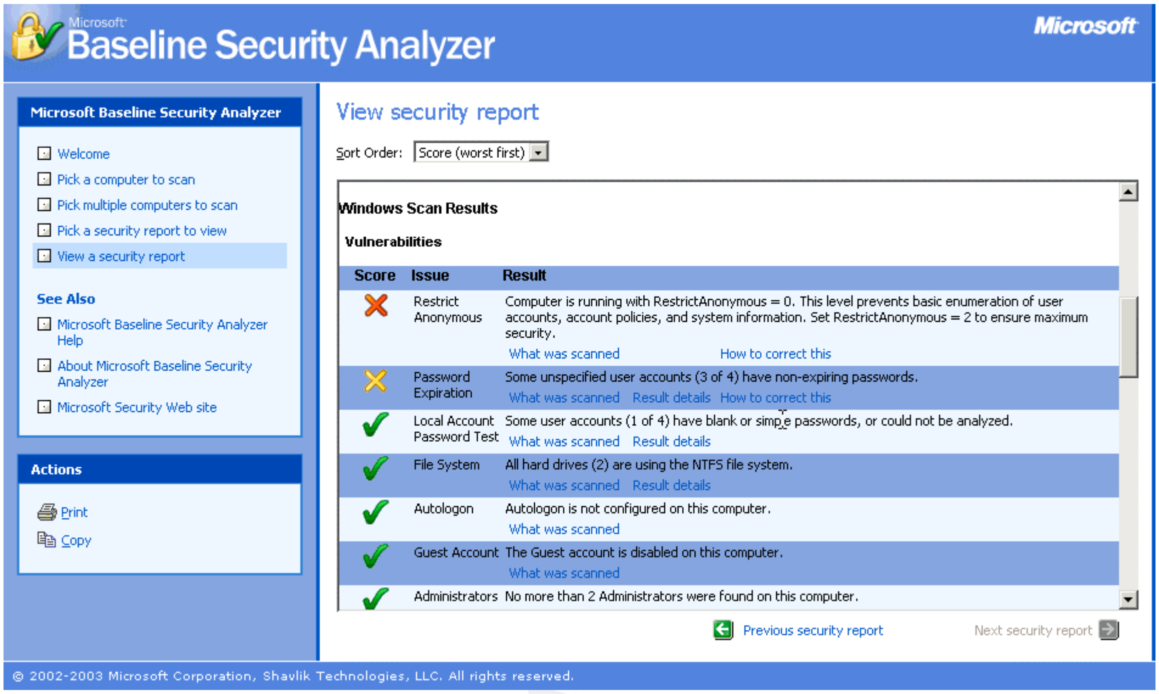
With these requirements in mind I need to build a security template for Windows that will lock it down as much as possible while still allowing these services.

I decided to start with Microsoft's hisecweb.inf Security Template. I needed to make a couple modifications:

- I want administrators to be able to log in over the network
- I want Terminal Services to be turned on.
- I changed the logon legal notice text.

To that end I edited hiseweb.inf as shown in Appendix B. The template assumes a static IP address (DHCP is disabled).

I ran Microsoft's Baseline Security Analyzer to get an idea of where I was starting. This isn't necessarily the best tool[61], but it is free and supported by Microsoft.


Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Actions
Print
Copy
Previous security report
Next security report
© 2002-2003 Microsoft Corporation, Shavlik Technologies, LLC. All rights reserved.

View security report

Sort Order: Score (worst first)

Windows Scan Results

Vulnerabilities

Score	Issue	Result
✗	Restrict Anonymous	Computer is running with RestrictAnonymous = 0. This level prevents basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security. What was scanned How to correct this
✗	Password Expiration	Some unspecified user accounts (3 of 4) have non-expiring passwords. What was scanned Result details How to correct this
✓	Local Account Password Test	Some user accounts (1 of 4) have blank or simple passwords, or could not be analyzed. What was scanned Result details
✓	File System	All hard drives (2) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Administrators	No more than 2 Administrators were found on this computer.

Figure 24 - The Initial Baseline Report on the FTP Server

I start the Security Information and Analysis mmc snap-in, right-click to Open a Database… and select a new database name, FTPDB.sdb. I then select my modified hisecweb.inf file.

Before applying the template I pick Analyze Computer Now… and store a log file of the changes. This will be handy later when I try to figure out why the server stops working after the template is applied.

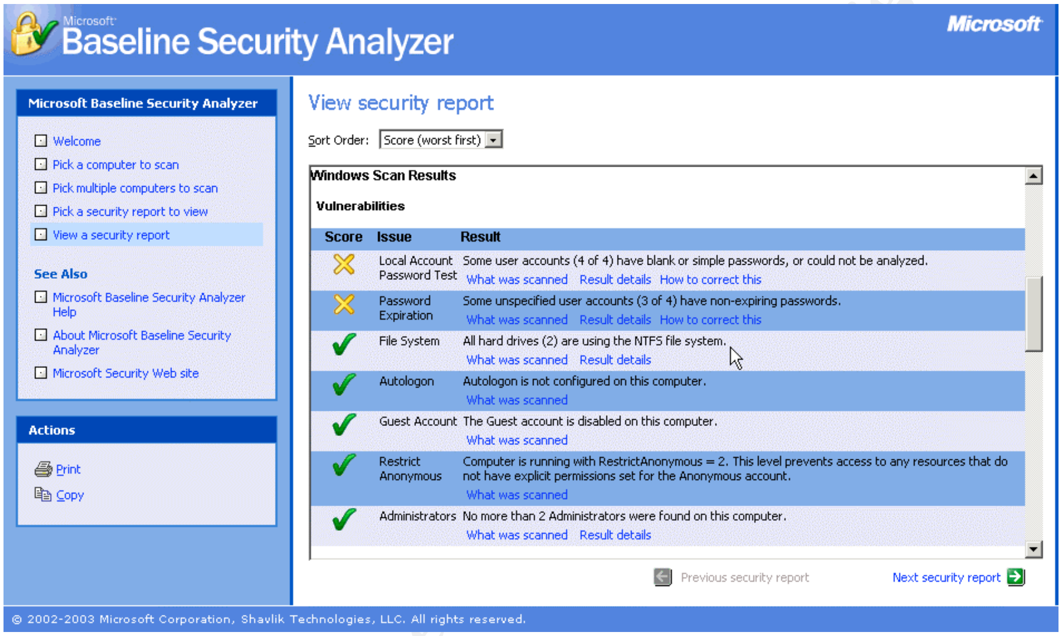
Here's a tip: if you can, test templates on test machines, not production machines. If the FTP Server is Windows XP I would also run secedit.exe with the /generaterollback parameter so I have a template of the original values.

[61] There are many tools, both for pay and free, that will perform security analysis of a computer. Most are available from your favorite hacking site.

I the apply the template with Configure Computer Now and reboot for good measure. After rebooting I see the legal notice text, so the template definitely was applied.

I check that I can still FTP to the server and that an administrator group member has access to the sync network share. I also test that I can still Terminal Server into the machine.

I then run the Baseline Security Analyzer again:


Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Actions
Print
Copy
Previous security report
Next security report
© 2002-2003 Microsoft Corporation, Shavlik Technologies, LLC. All rights reserved.

View security report

Sort Order: Score (worst first)

Windows Scan Results

Vulnerabilities

Score	Issue	Result
✗	Local Account Password Test	Some user accounts (4 of 4) have blank or simple passwords, or could not be analyzed. What was scanned Result details How to correct this
✗	Password Expiration	Some unspecified user accounts (3 of 4) have non-expiring passwords. What was scanned Result details How to correct this
✓	File System	All hard drives (2) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is running with RestrictAnonymous = 2. This level prevents access to any resources that do not have explicit permissions set for the Anonymous account. What was scanned
✓	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details

Figure 25 - Baseline Report after Applying the Security Template

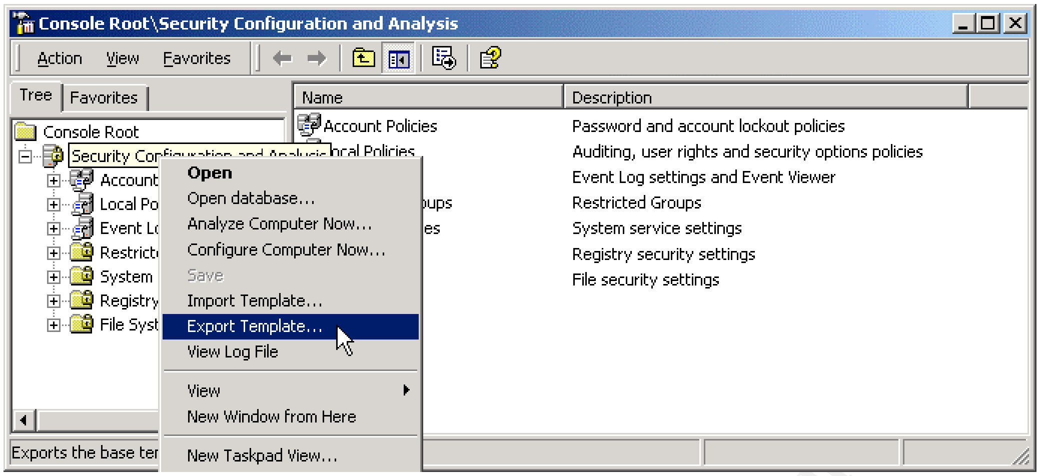
This is a slight improvement over the first run.

I now go through all the errors and ensured they are acceptable.

As a further step I decide to analyze my configuration against another high security template. The intention isn't to apply the template, but to see what options the template suggested that I might be able to turn on.

Once again, I used Analyze Computer Now… and save a log file. I also back everything up again first.

I will conclude this example here as several more iterations can be made. As the database's settings are improved a new template can be exported from it (Export Template…



Secure the FTP Service

The Data Synchronization Process supports any FTP Server that accepts Passive (PASV) FTP connections[62].

Microsoft's FTP (MSFTP) Server component of IIS is a common choice among small clients. The advantages of MSFTP are the price (it's free, providing whatever Microsoft licensing scheme the server is under is being adhered to[63]) and it integrates with the OS for tasks such as authentication and user management.

Some versions of Windows impose a ten-connection limit on the OS and therefore the FTP Server! [64]

MSFTP, however, does not provide best-of-breed security features. Third party products such as WS_FTP Server[65] and Serv-U[66], provide a number of valuable security features including:

[62] The discussions that follow assume an FTP server dedicated for the data synchronization process.

[63] Some licensing programs require client accesses to be licensed!

[64] "Inbound Connections Limit in Windows". Microsoft Knowledge Base. 6 May 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;122920, (23 Nov. 2003).

[65] "WS_FTP Server". URL: http://www.ipswitch.com/products/ws_ftp-server/whatsnew.html, (23 Nov. 2003).

[66] "Serv-U Home Page", URL: http://www.serv-u.com/, (11 Dec. 2003).

- file type restriction: The sync process uses only two file extensions, ".command" and ".data". Only allowing files of these types will help prevent the FTP Server from being used for other purposes.

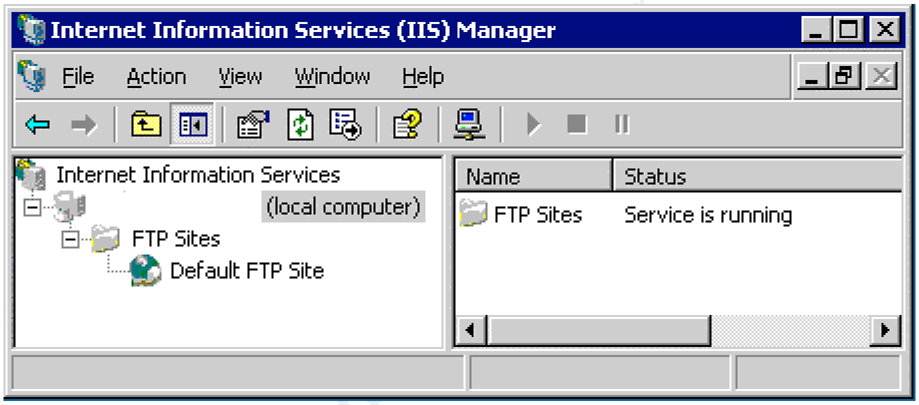
- IP based access: For environments where Program Clients come from known address spaces.

- Event triggers: processes can run when a file is uploaded (including moving the file to a new folder).

- Passive range setup: FTP manager can set up a range of ports the FTP server can accept data channels on.

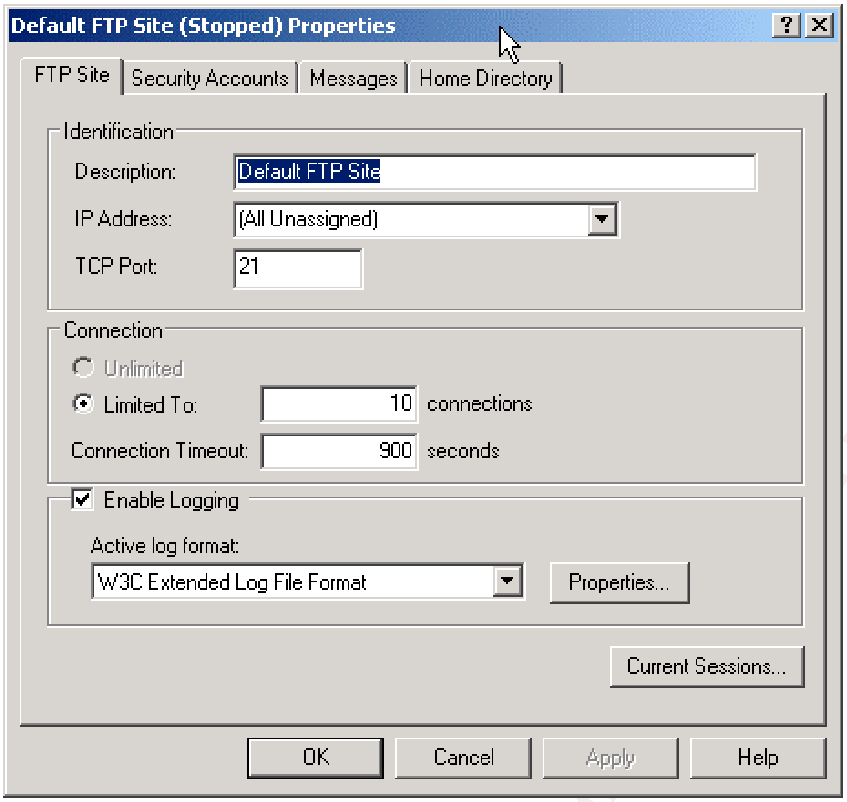
Securing IIS FTP

The FTP Server can be configured initially through the GUI or command line. Opening the Internet Information Services (IIS) Manager will show:


Internet Information Services (IIS) Manager
File
Action
View
Window
Help
Internet Information Services
(local computer)
FTP Sites
Default FTP Site

Name	Status
FTP Sites	Service is running

If the computer is selected, global defaults for all child FTP Sites (including the default site) can be set. By right-clicking the Default FTP Site and picking Properties, each of the FTP property dialogs can be explained:


Default FTP Site (Stopped) Properties

Identification

Description: Default FTP Site

IP Address: (All Unassigned)

TCP Port: 21

Connection

○ Unlimited

● Limited To: 10 connections

Connection Timeout: 900 seconds

☑ Enable Logging

Active log format: W3C Extended Log File Format

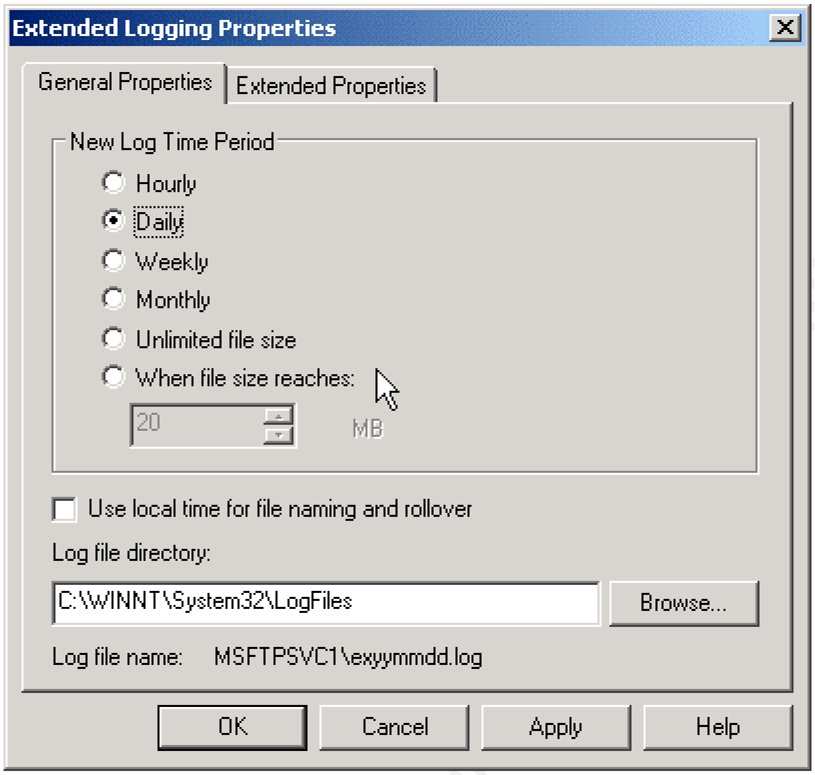
If the FTP Server is multi-homed (it has multiple IP addresses and/or multiple network cards) only one address should be listed under IP Address (the address the Field Laptops will be connecting to—or the address the firewall will be redirecting traffic to) unless the FTP server needs to be accessible on multiple IP addresses for other reasons.

The TCP Port can be changed to improve security, although it is not supported by the Program Client. However, if there is a firewall in front of the FTP Server capable of port mapping, the Program Client can connect to the FTP Server on port 21 and the firewall can connect to the FTP Server on a different port. This may be slightly advantageous if other machines in the DMZ have access to the server.

A connect limit of 10 is a pretty good indication the FTP Server is running on a Workstation version of Windows or a crippled demo/MSDN version. The Windows 2000 Server default is 100,000. The number should be at least the number of field users connecting. If a long timeout is used, two or three times the max possible connection is even better (for most companies that number is still less than 1000).

A long connection timeout may be desirable if users are on slow connections. However, a timeout of more than ten minutes is not required; anything longer and the connection at the Program Client will have timed out and disconnected.

Logging should also be enabled. Log files should be stored on their own physical hard drive and protected with NTFS permissions (full control for Administrator and System). NTFS auditing should also be used on the log files to detect failed access (at minimum).



Extended Logging Properties

New Log Time Period

○ Hourly
● Daily
○ Weekly
○ Monthly
○ Unlimited file size
○ When file size reaches:

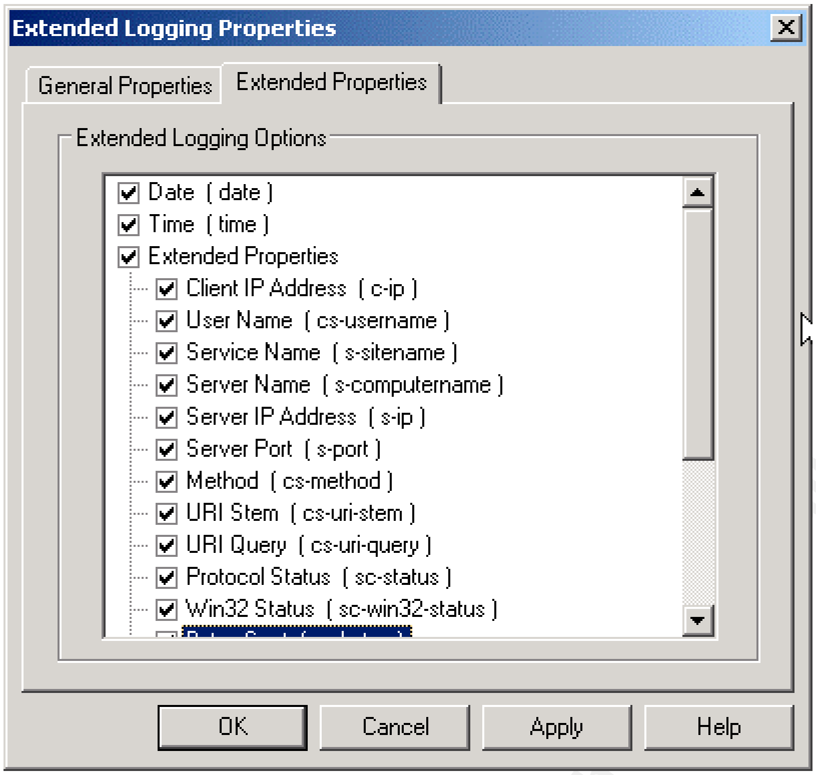
20 MB

□ Use local time for file naming and rollover

Log file directory: C:\WINNT\System32\LogFiles

Log file name: MSFTPSVC1\exyymmdd.log

A lot of information that can be stored in the log files is not stored by default. These extra fields can be selected in the Extended Properties tab.



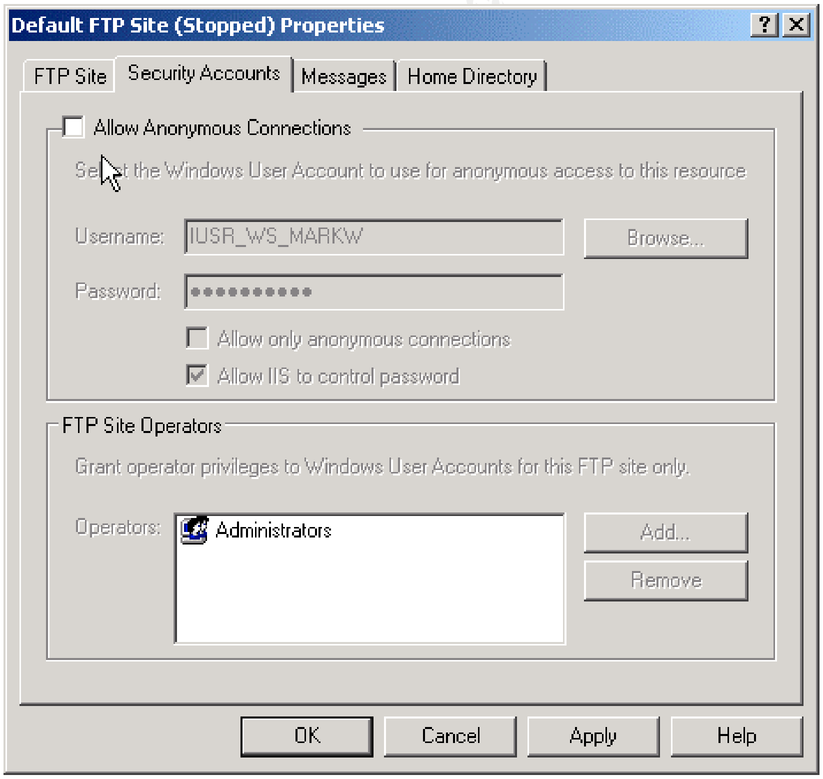
Extended Logging Properties

General Properties | Extended Properties

Extended Logging Options

- ☑ Date (date)
- ☑ Time (time)
- ☑ Extended Properties
  - ☑ Client IP Address (c-ip)
  - ☑ User Name (cs-username)
  - ☑ Service Name (s-sitename)
  - ☑ Server Name (s-computername)
  - ☑ Server IP Address (s-ip)
  - ☑ Server Port (s-port)
  - ☑ Method (cs-method)
  - ☑ URI Stem (cs-uri-stem)
  - ☑ URI Query (cs-uri-query)
  - ☑ Protocol Status (sc-status)
  - ☑ Win32 Status (sc-win32-status)

Unless there is a performance concern turning on a property, enable logging for it.



Default FTP Site (Stopped) Properties

FTP Site | Security Accounts | Messages | Home Directory

☐ Allow Anonymous Connections

Select the Windows User Account to use for anonymous access to this resource

Username: IUSR_WS_MARKW

Password: ●●●●●●●●●●

☐ Allow only anonymous connections

☑ Allow IIS to control password

FTP Site Operators

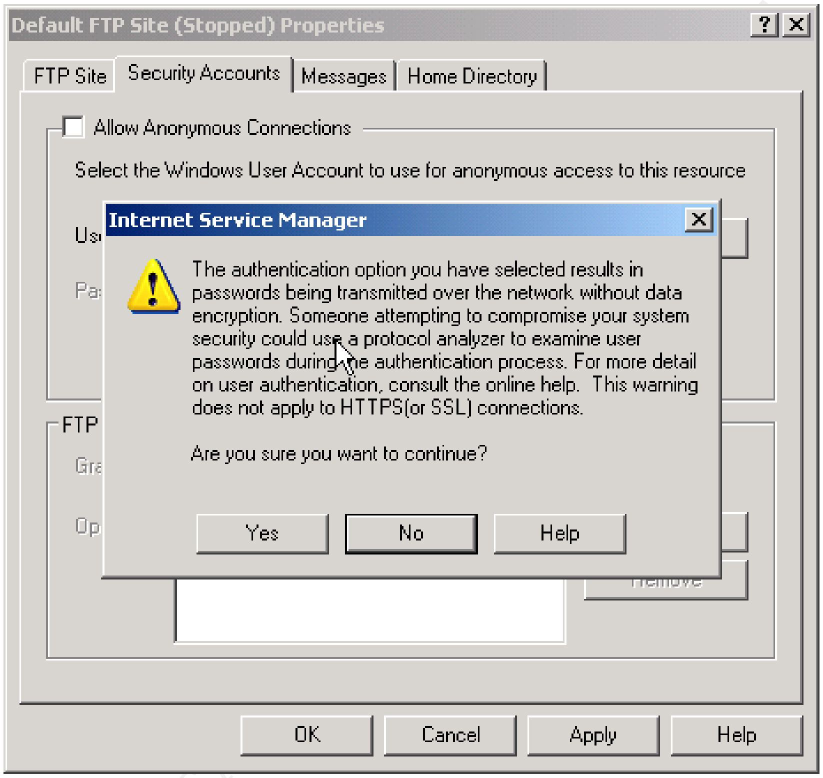
Grant operator privileges to Windows User Accounts for this FTP site only.

Operators: Administrators

The next property tab is Security Accounts. There is no reason to allow anonymous connections in the Data Synchronization process. The Program Client should always use a local or domain account to connect, even if that account is shared among all the field users (which is not recommended of course).

A closely related topic is the Guest account. If the local guest account is enabled and has a blank password, and the NTFS permissions on the Home Directory allow Guest at least Read access, then an FTP user can log in with an empty username and password. And the user they connect as is Guest! Most security templates disable the guest account. This is mandatory!

When Anonymous Connections are turned off, the following warning appears:



Select the Windows User Account to use for anonymous access to this resource

The authentication option you have selected results in passwords being transmitted over the network without data encryption. Someone attempting to compromise your system security could use a protocol analyzer to examine user passwords during the authentication process. For more detail on user authentication, consult the online help. This warning does not apply to HTTPS(or SSL) connections.

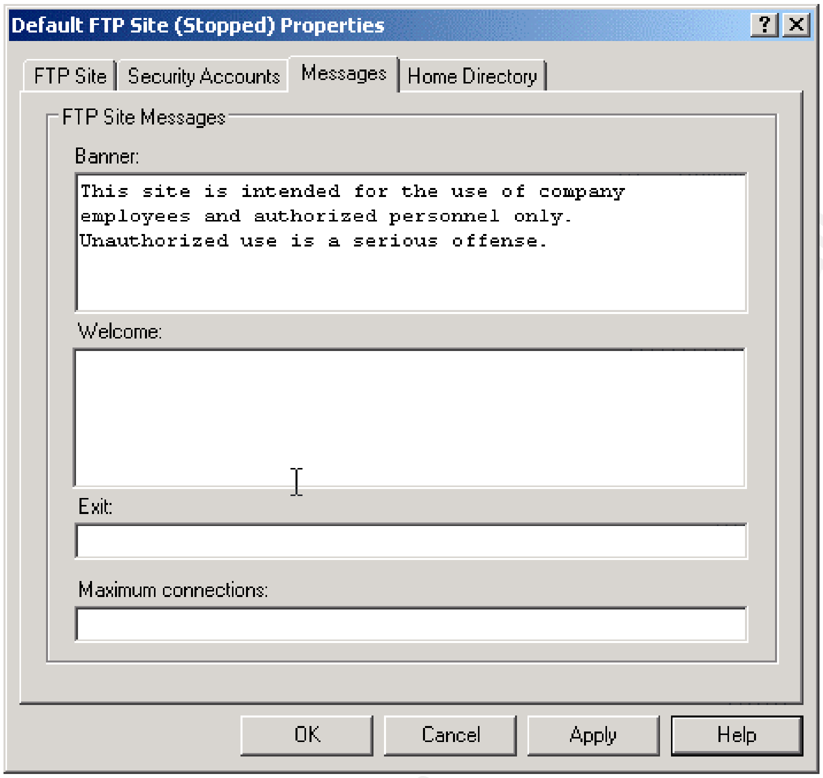
Are you sure you want to continue?

This is a good reason to make FTP connections through a VPN.

The FTP Site Operators are users who are allowed to manage this FTP Site. This does not give them access to manage the FTP Server, only this site. The option is not available in the IIS 6 Version of FTP—permissions are set by right-clicking the site and picking Permissions.

The next Properties tab allows the messages that appear when an FTP client connects to the FTP Server (banner), when a user logs in (welcome), when a user exits (exit), and the error message that appears when the maximum number of allowed connections is exceeded (maximum connections).

It may be wise to consult legal counsel and enter messages that will maximize the potential to succeed in a legal case against a hacker (who has been caught).



Banner:

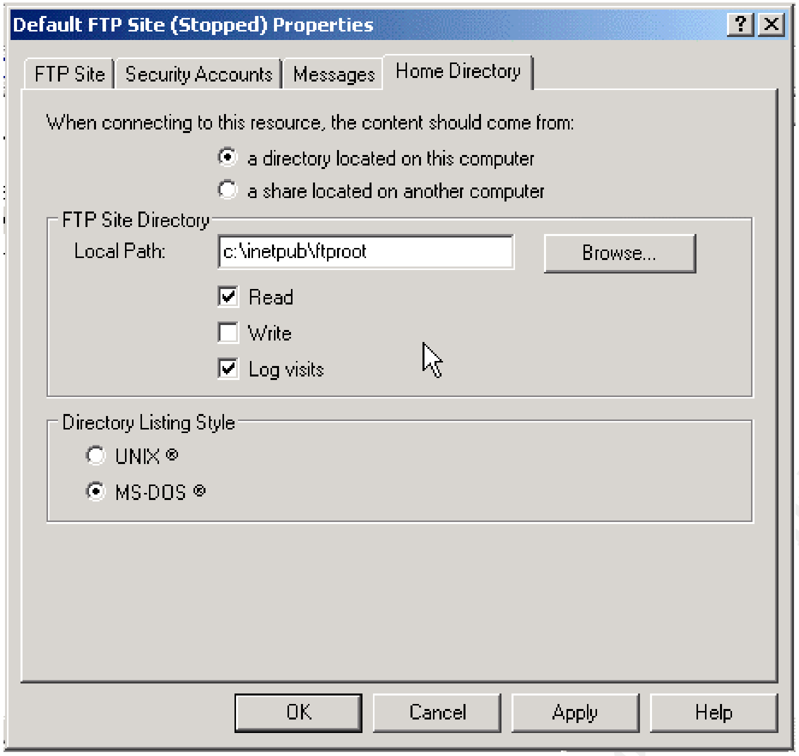
This site is intended for the use of company employees and authorized personnel only.
Unauthorized use is a serious offense.

Welcome:

Exit:

Maximum connections:

The Home Directory tab follows:



When connecting to this resource, the content should come from:

● a directory located on this computer
○ a share located on another computer

FTP Site Directory

Local Path: c:\inetpub\ftproot

☑ Read
□ Write
☑ Log visits

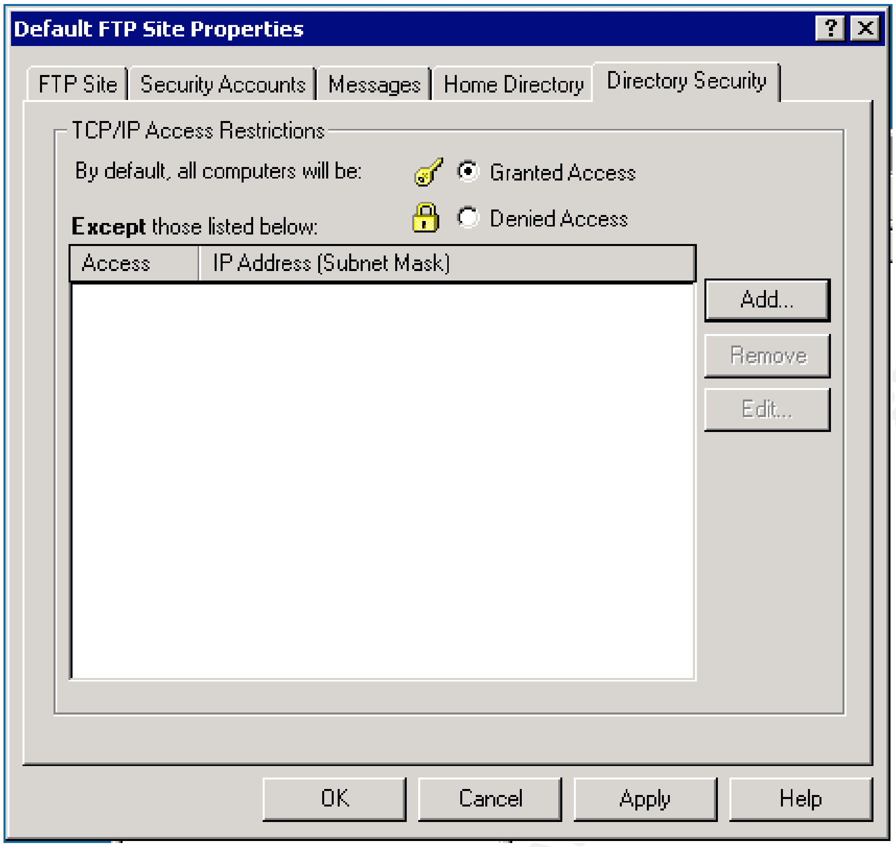
Directory Listing Style

○ UNIX ®
● MS-DOS ®

The Directory Listing Style should be set to MS-DOS, although the Program Client will also work with Unix-style directory listings.

The FTP Site Directory is preferable to have on a different volume than Windows and the Log files. The Sync folder can be added as a Virtual directory (see the “Secure the Sync FTP Site” section that follows). The Home Directory, therefore, is not used as part of the Synchronization process and can be locked down and audited for suspicious behavior. The Home Directory should never allow Write permission.

The actual Home directory should only allow NTFS Read access to the group containing the field users. Auditing should be enabled for failed privilege use.



TCP/IP Access Restrictions

By default, all computers will be: ● Granted Access ○ Denied Access

Except those listed below:

Access	IP Address (Subnet Mask)

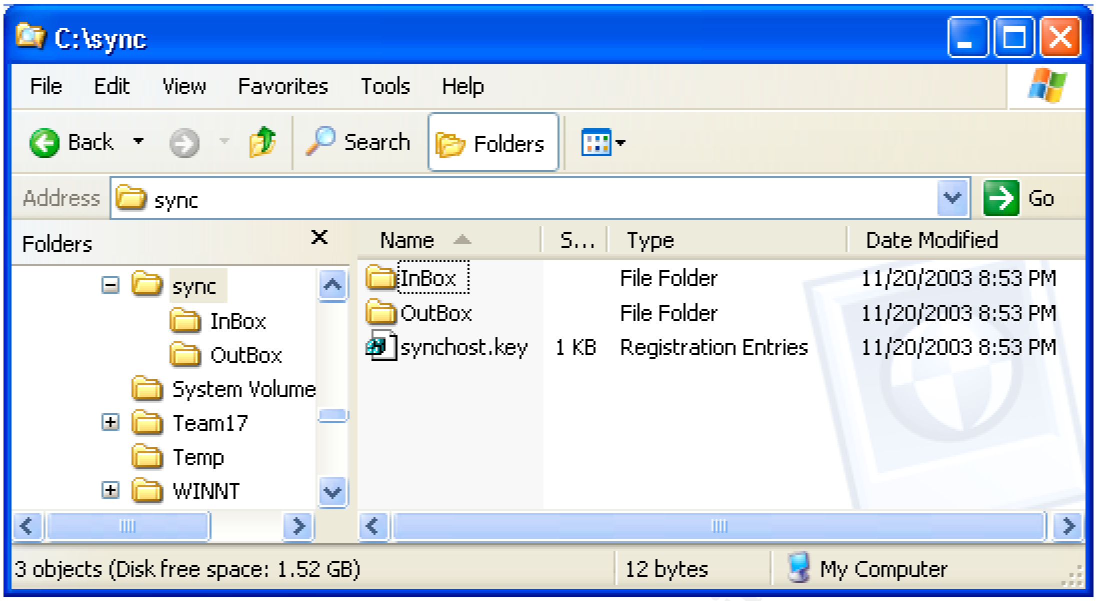
The final tab is Directory Security. An IP address or Range of addresses can be granted or denied access.

The Add… dialog allows DNS lookups, but be aware that after the lookup is done only the IP address is stored (not the DNS name). If the IP address changes at a later date, the FTP Site will be unaware; the lookup is only done when the entry is added.

Secure the Sync FTP Site

The FTP Server needs mappings from the FTP root (or a virtual FTP directory) to the Sync Folder.

If, for example, the Program Client has “\Sync” entered as the Sync FTP Folder the FTP server needs to create a virtual directory named “Sync” to the sync folder on the file system. The FTP user requires read access on this folder. For example, if the sync folder is “C:\Sync”.



Name	S...	Type	Date Modified
InBox		File Folder	11/20/2003 8:53 PM
OutBox		File Folder	11/20/2003 8:53 PM
synchost.key	1 KB	Registration Entries	11/20/2003 8:53 PM

3 objects (Disk free space: 1.52 GB) 12 bytes My Computer

Figure 26 - Sync Folder Structure

The FTP user requires read access to the root, write access to the InBox and both read and write to the OutBox subfolders.

Example: Creating a Sync FTP Site

I will make another FTP Site using the GUI wizard of the Internet Information Services tool. I right-click the FTP Server and pick New > FTP Site.

I enter:

Description: Data Sync FTP Site
IP Address: 192.168.5.102
TCP Port: 21
Path: D:\Sync
Read: checked
Write: checked

And I finish the wizard. I the pick the properties and ensure:

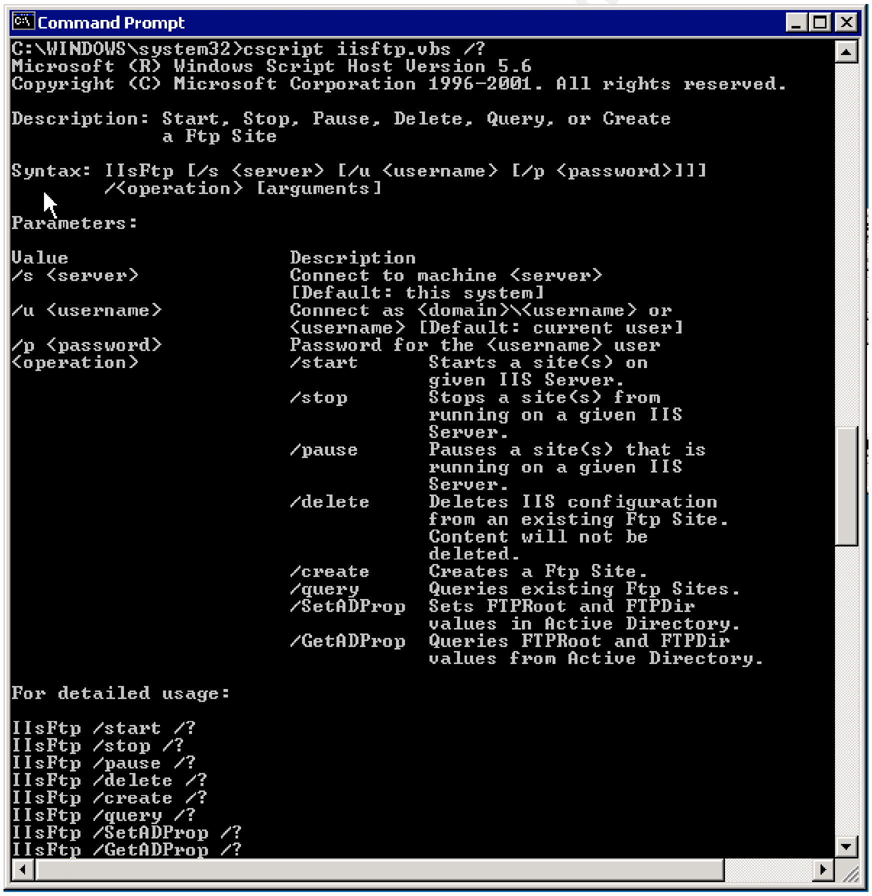
Connections: 1000
Logging: enabled with all fields selected
Allow Anonymous Connections: unchecked
FTP Site Operators: will be the Administrators group in this example
Welcome message: scary legalese and dire warnings

Exit message: Bye!
Maximum connections message: Too many!
Home directory: is a directory based on the computer
FTP Site Directory: D:\Sync
Read: checked
Write: checked
Log visits: checked
Directory Listing Style: MS-DOS
Directory Security: All computers granted access

Script Tools

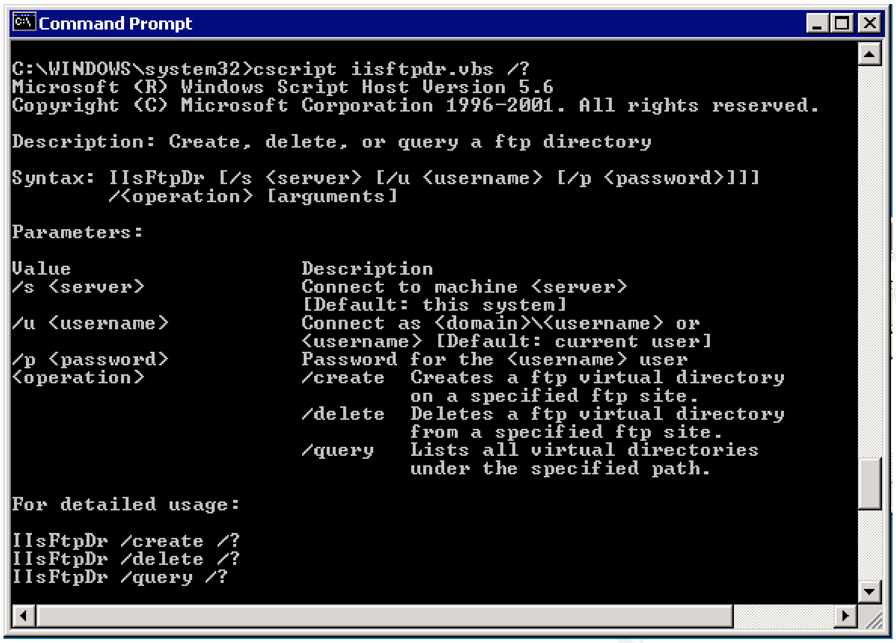
IIS 5 can use script tools such as adsutil.vbs to set metabase values from the command line. IIS 6 introduces two new script tools for managing the FTP Server from the command line; iisftp.vbs and iisftpdr.vbs. These scripts can both be used to connect to remote servers.

iisftp.vbs is used to query, manage, and control a local or remote IIS 6 FTP Server. It has the following parameters:



```
C:\WINDOWS\system32>cscript iisftp.vbs /?
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Description: Start, Stop, Pause, Delete, Query, or Create
             a Ftp Site

Syntax: IIsFtp [/s <server> [/u <username> [/p <password>]]]
        /<operation> [arguments]

Parameters:

Value                       Description
/s <server>                 Connect to machine <server>
                            [Default: this system]
/u <username>               Connect as <domain>\<username> or
                            <username> [Default: current user]
/p <password>               Password for the <username> user
<operation>                 /start      Starts a site(s) on
                                        given IIS Server.
                            /stop       Stops a site(s) from
                                        running on a given IIS
                                        Server.
                            /pause      Pauses a site(s) that is
                                        running on a given IIS
                                        Server.
                            /delete     Deletes IIS configuration
                                        from an existing Ftp Site.
                                        Content will not be
                                        deleted.
                            /create     Creates a Ftp Site.
                            /query      Queries existing Ftp Sites.
                            /SetADProp  Sets FTPRoot and FTPDir
                                        values in Active Directory.
                            /GetADProp  Queries FTPRoot and FTPDir
                                        values from Active Directory.

For detailed usage:

IIsFtp /start /?
IIsFtp /stop /?
IIsFtp /pause /?
IIsFtp /delete /?
IIsFtp /create /?
IIsFtp /query /?
IIsFtp /SetADProp /?
IIsFtp /GetADProp /?
```

Likewise, iisftpdr.vbs is used to create, delete, and query IIS 6.0 Virtual FTP directories:



```
C:\WINDOWS\system32>cscript iisftpdr.vbs /?
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Description: Create, delete, or query a ftp directory

Syntax: IIsFtpDr [/s <server> [/u <username> [/p <password>]]]
        /<operation> [arguments]

Parameters:

Value                   Description
/s <server>             Connect to machine <server>
                        [Default: this system]
/u <username>           Connect as <domain>\<username> or
                        <username> [Default: current user]
/p <password>           Password for the <username> user
<operation>             /create   Creates a ftp virtual directory
                                  on a specified ftp site.
                        /delete   Deletes a ftp virtual directory
                                  from a specified ftp site.
                        /query    Lists all virtual directories
                                  under the specified path.

For detailed usage:

IIsFtpDr /create /?
IIsFtpDr /delete /?
IIsFtpDr /query /?
```

Registry Entries

FTP shares many registry entries with IIS and the other Internet services. It also has a few of its own under HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ MSFTPSVC\ Parameters.

EnablePortAttack set to 0

From Microsoft's knowledge base (note the year of 1999):

> Recently there was a security hole discovered in FTP service with passive connection support. The hole is in the FTP protocol specification. By default, the FTP service allows passive connections to be established based on the port address given by client. This can enable some hackers to use this facility to execute malicious commands off the FTP service. The problem occurs when we request FTP service to connect to a port other than FTP Data port (20) and port number is less than IP_PORT_RESERVED (1024). This flag controls if such an attack should be allowed. By default, the service does not make any connections to ports less than IP_PORT_RESERVED (other than 20). If someone deliberately wants the old behavior then this flag should be enabled.[67]

[67] "IIS FTP Registry Parameters", Microsoft Knowledge Base. 4 Apr. 1999. URL: http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q147/6/21.asp&NoWebContent=1, (14 Dec., 2003).

AllowGuestAccess set to 0

Guest access should NOT be allowed (and the guest user should be disabled anyway).

FTP Metabase

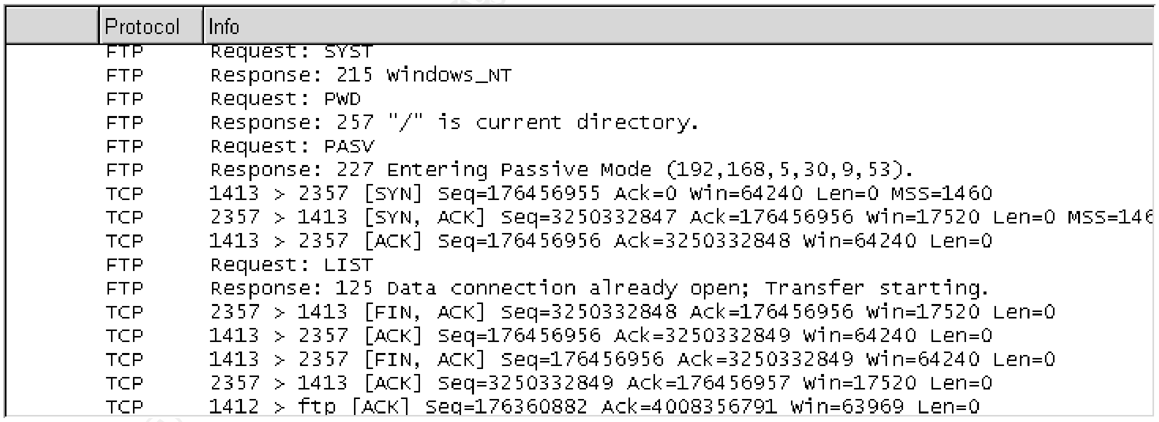
Most settings in IIS 5 and 6 have been moved from the registry to the Metabase. In IIS 6 the metabase is an XML file and can be edited with an XML editor, or even Notepad! The metabase file is in %windir%/system32/inetsrv and is called metabase.xml.

In IIS 5 the preferred tool is METAEDIT.EXE, the metabase editor. The tool can be downloaded from Microsoft. The metabase can also be edited using WMI and ADSI, either from the command line or via a script.

Many useful IIS 6 Metabase keys can be found in Appendix C.

Example: Setting the PassivePortRange in IIS 6

By default, IIS 6 will offer Passive Data ports in the range 1025 to 5000. Making a connection to a standard IIS 6 FTP Server confirms this:

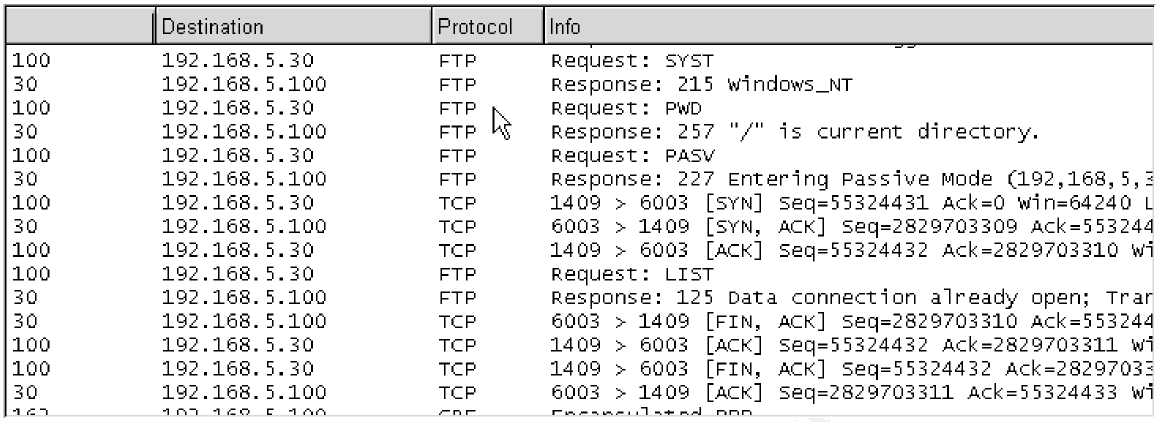


```
          Protocol  Info
          FTP       Request: SYST
          FTP       Response: 215 Windows_NT
          FTP       Request: PWD
          FTP       Response: 257 "/" is current directory.
          FTP       Request: PASV
          FTP       Response: 227 Entering Passive Mode (192,168,5,30,9,53).
          TCP       1413 > 2357 [SYN] Seq=176456955 Ack=0 Win=64240 Len=0 MSS=1460
          TCP       2357 > 1413 [SYN, ACK] Seq=3250332847 Ack=176456956 Win=17520 Len=0 MSS=146
          TCP       1413 > 2357 [ACK] Seq=176456956 Ack=3250332848 Win=64240 Len=0
          FTP       Request: LIST
          FTP       Response: 125 Data connection already open; Transfer starting.
          TCP       2357 > 1413 [FIN, ACK] Seq=3250332848 Ack=176456956 Win=17520 Len=0
          TCP       1413 > 2357 [ACK] Seq=176456956 Ack=3250332849 Win=64240 Len=0
          TCP       1413 > 2357 [FIN, ACK] Seq=176456956 Ack=3250332849 Win=64240 Len=0
          TCP       2357 > 1413 [ACK] Seq=3250332849 Ack=176456957 Win=17520 Len=0
          TCP       1412 > ftp [ACK] Seq=176360882 Ack=4008356791 Win=63969 Len=0
```

In this case the port selected was 2357. In this example I want to change the data port to use the range 6000 to 8000, so I set the PassivePortRange key on the IIS 6 server with this script (ADSI):

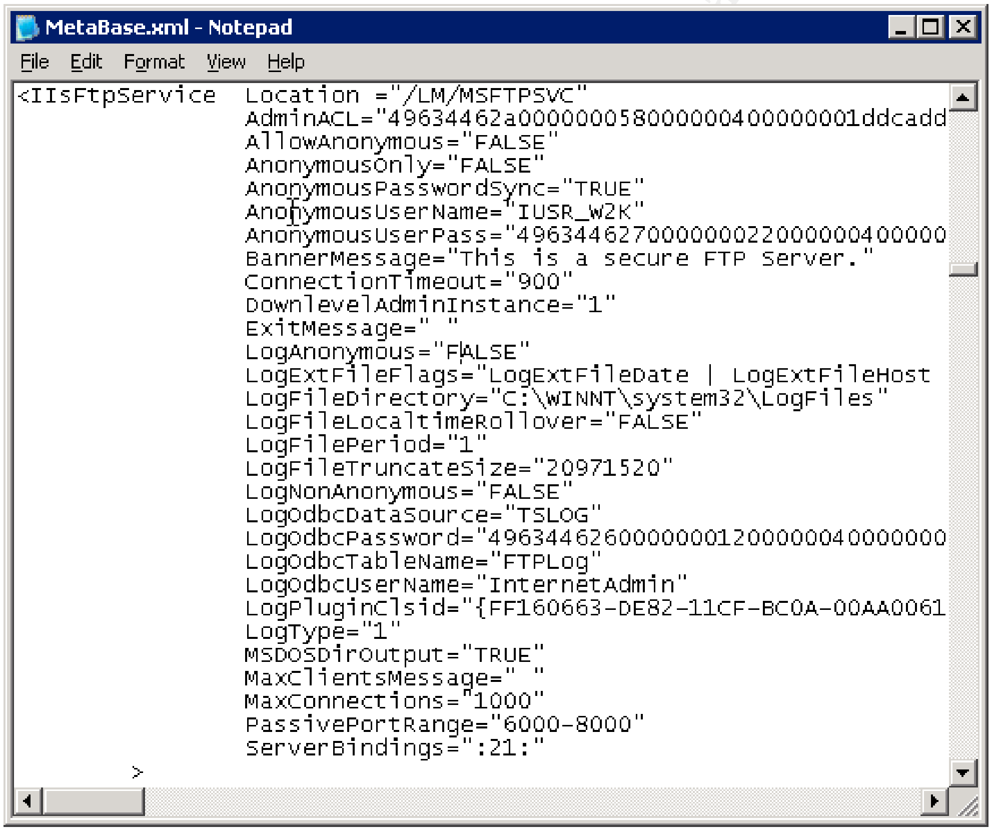
```
set vdirObj=GetObject("IIS://localhost/MSFTPSVC")
vdirObj.Put "PassivePortRange", "6000-8000"
vdirObj.SetInfo
```

and restart the server. I make a reconnection with my client (a couple times):



```
           Destination      Protocol  Info
100        192.168.5.30     FTP       Request: SYST
30         192.168.5.100    FTP       Response: 215 Windows_NT
100        192.168.5.30     FTP       Request: PWD
30         192.168.5.100    FTP       Response: 257 "/" is current directory.
100        192.168.5.30     FTP       Request: PASV
30         192.168.5.100    FTP       Response: 227 Entering Passive Mode (192,168,5,3
100        192.168.5.30     TCP       1409 > 6003 [SYN] Seq=55324431 Ack=0 Win=64240 L
30         192.168.5.100    TCP       6003 > 1409 [SYN, ACK] Seq=2829703309 Ack=553244
100        192.168.5.30     TCP       1409 > 6003 [ACK] Seq=55324432 Ack=2829703310 Wi
100        192.168.5.30     FTP       Request: LIST
30         192.168.5.100    FTP       Response: 125 Data connection already open; Trar
30         192.168.5.100    TCP       6003 > 1409 [FIN, ACK] Seq=2829703310 Ack=553244
100        192.168.5.30     TCP       1409 > 6003 [ACK] Seq=55324432 Ack=2829703311 Wi
100        192.168.5.30     TCP       1409 > 6003 [FIN, ACK] Seq=55324432 Ack=28297033
30         192.168.5.100    TCP       6003 > 1409 [ACK] Seq=2829703311 Ack=55324433 Wi
```

And the data port is changed to 6003. I also check the metabase.xml file:



```
<IIsFtpService   Location ="/LM/MSFTPSVC"
                 AdminACL="49634462a0000000580000004000000001ddcadd
                 AllowAnonymous="FALSE"
                 AnonymousOnly="FALSE"
                 AnonymousPasswordSync="TRUE"
                 AnonymousUserName="IUSR_W2K"
                 AnonymousUserPass="4963446270000000220000004000000
                 BannerMessage="This is a secure FTP Server."
                 ConnectionTimeout="900"
                 DownlevelAdminInstance="1"
                 ExitMessage=" "
                 LogAnonymous="FALSE"
                 LogExtFileFlags="LogExtFileDate | LogExtFileHost
                 LogFileDirectory="C:\WINNT\system32\LogFiles"
                 LogFileLocaltimeRollover="FALSE"
                 LogFilePeriod="1"
                 LogFileTruncateSize="20971520"
                 LogNonAnonymous="FALSE"
                 LogOdbcDataSource="TSLOG"
                 LogOdbcPassword="49634462600000001200000040000000
                 LogOdbcTableName="FTPLog"
                 LogOdbcUserName="InternetAdmin"
                 LogPluginClsid="{FF160663-DE82-11CF-BC0A-00AA0061
                 LogType="1"
                 MSDOSDirOutput="TRUE"
                 MaxClientsMessage=" "
                 MaxConnections="1000"
                 PassivePortRange="6000-8000"
                 ServerBindings=":21:"
        >
```

To see that the PassivePortRange is added.

Backing Up the FTP Site and the Metabase

The IIS 5, the Metabase can be backed up through METAEDIT.EXE. The Metabase menu contains an item Backup/Restore… that will let you create and restore backups. An FTP site can also be exported.

In IIS 6, the metabase is a file and can be backed up. FTP Site configurations can be saved (and encrypted with a password) through the IIS Manager.

User Management

The Program Client logs into the FTP server with a single username and password. This introduces the issue of managing of FTP logins.

The FTP Server can use Active Directory domain logins, or local users.

A more secure method would be to give each field user their own login. If a field user changes companies, the login can be revoked. This assumes that the process of FTP user management is tied into the HR process. In practice, many companies do not have real-time HR information available. There have been cases of a field user being fired from a drilling group and re-hired with a different drilling group in the same day (and both groups are in the same company!).

Some companies may already have a user management tool and field user accounts available to the DMZ from related projects. These companies may expose a portion of the Active Directory (AD) tree to the DMZ or run a Domain Controller with a separate AD Forest in the DMZ. An excellent paper on setting up Active Directory through firewalls is entitled Active Directory in Network Segmented by Firewalls[68].

Having a good process to communicate to the field users will help inform them of password changes. Password changes can also be set at head office (with a utility provided by the vendor) and distributed in a .reg file or script:

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Program Client\DB\Client]
"FTPUserName"="3B1A932DD333153947235543323483227373 1952"
"FTPPassword"="341193223232335354723215433648 3AA7373D952"
```

[68] "Active Directory in Networks Segmented by Firewalls". URL: http://www.microsoft.com/windows2000/docs/adsegmented.doc, (23 Nov. 2003)

Performance Monitor

Perfmon can be used to monitor many aspects of the FTP Server, including Bytes Received, Bytes Sent, Logon attempts, Current Connections, Total files transferred, and many more, both for the FTP Service as a whole or for individual FTP Sites.

Securing FTP Server to SyncHost Server Transmission

The SyncHost Server and FTP Server communicate through a shared file system. If the two servers are on the same machine there should be no transmission issues once the proper file permissions are set. However, there are good security reasons for putting the FTP Server, which may be exposed to the internet at considerable risk, and the SyncHost Server, which requires a direct connection to the Database Server containing millions of dollars of confidential data, on different sides of a firewall.

One means of communication between the servers is a Windows network share. The sync folder on the FTP Server can be shared to the SyncHost Server as a mapped drive or UNC name. Likewise, the FTP Server can map to a share of the SyncHost's sync folder.

It is better to put the fileshare on the FTP Server. If the FTP server was compromised it would be good that the FTP Server had one less way to connect to the SyncHost server. In theory, a hacker would have to compromise the FTP Server before he/she could get to the SyncHost Server. If the SyncHost server could be compromised and controlled by data passed through the FTP server this need not be true, but for the sake of argument it is less likely.

There is an opportunity to use IPSec to encrypt the packets between the two machines. This could involve authentication though Kerberos (UDP 500), sharing certificates (a manual task if the machines are not in the same domain), or a pre-shared key[69]. An example of an IPSec connection is covered in the RRAS section.

Another option is to install two-way real-time mirroring software on both the FTP Server and the SyncHost Server. This software communicates on a defined port (probably > 1024) and synchronizes the sync folder (and subfolders) on the two machines.

[69] See cited work "How to Enable IPSec Traffic Through a Firewall". Microsoft Knowledge Base. 21 Nov. 2003. URL: http://support.microsoft.com/default.aspx?kbid=233256, (23 Nov. 2003).

There are many software packages that will synchronize folders[70]. It would be a good time to understand the fine details of the Sync process. The requirements for this application are:

- Two-way synchronization: Inbox Files need to be replicated from the FTP Server to the SyncHost. When they are deleted by the SyncHost Server they need to be removed from the FTP Server. OutBox Files need to be replicated from the SyncHost side to the FTP Server. When they are deleted by the Program Client at the FTP side they need to be removed from the SyncHost Server. The sync folder itself only needs one-way replication from the SyncHost Server to the FTP Server.

- Communication through a port: preferably through a high port (> 1024).

- Run as a service.

- Encrypt data during transmission.

- Manage NTFS permissions correctly. Both the FTP Server and SyncHost server will need the correct permissions on their respective sides.

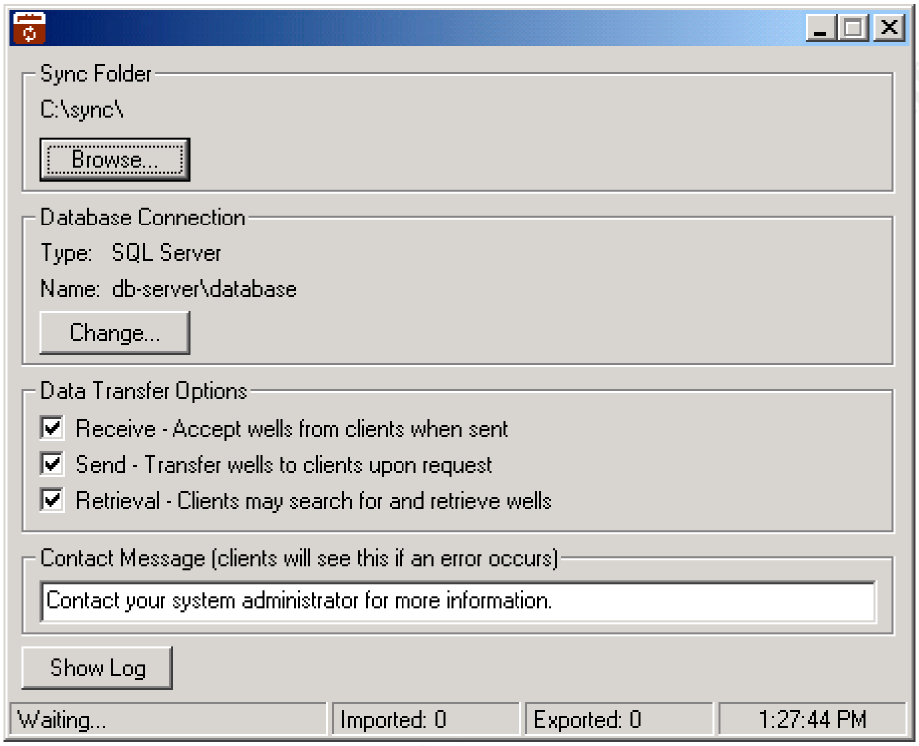
- The files must appear in the same order on both sides of the firewall.

The last requirement is particularly challenging for third party software. The SyncHost server is a single threaded application. It processes the files that appear in the InBox one at a time on a first-come first-served basis. The Program Client uploads a large ".data" file and immediately follows with the much smaller corresponding ".command" file. It is only when the ".command" file appears that the SyncHost Server will process the ".data" file. The problem arises in that most directory synchronization software is multi-threaded. In a worse case scenario the directory synchronization software can still be transferring the large ".data" file while the small ".command" file arrives and is mirrored to the SyncHost Server. The SyncHost Server processes the ".command" file but the ".data" file is not completely copied and the synchronization fails!

[70] A huge list of products has been compiled by Folder Match at http://www.foldermatch.com/fmcompetitors.htm

SyncHost Server Configuration

The SyncHost Server is installed on a server with a self-extracting Windows installer, usually by an IT Administrator. Once installed the SyncHost Server runs as a windows application, displaying:



Sync Folder

C:\sync\

Database Connection

Type: SQL Server

Name: db-server\database

Data Transfer Options

☑ Receive - Accept wells from clients when sent

☑ Send - Transfer wells to clients upon request

☑ Retrieval - Clients may search for and retrieve wells

Contact Message (clients will see this if an error occurs)

Contact your system administrator for more information.

Waiting... | Imported: 0 | Exported: 0 | 1:27:44 PM

Figure 27 - SyncHost Server Main Dialog

The Sync Folder is a directory that contains two subfolders, InBox and the OutBox as shown in Figure 26 - Sync Folder Structure. The Sync Folder must be a local directory or a network share on the FTP Server. If a file system that supports file permissions is used (NTFS is recommended), the user the SyncHost Server is running under requires read and write permissions to the Sync Folder and its subfolders.

The database connection is selected with the Change… button. If, for example, the Database Server is Oracle, the SyncHost Server would have to have a correctly configured Oracle Client (SQL*Net, Net8) installed with a tested connection to the database. The TNS connection name would be the only input required in this case.

The SyncHost Server can limit what operations a Program Client can request. In particular the Retrieval function should not be checked if you do not want field users to request well download lists (and well downloads!).

Securing the Server

As with the RRAS and FTP Servers, the SyncHost Server should be locked down using Security Templates. If the SyncHost server is part of an Active Directory Domain the Templates can be distributed through Group Policy.

Running the SyncHost Server as a Service

The SyncHost Server is a windows executable and is run by a user logging in. The user has to remain logged in; this is an inconvenience to the IT staff and a potential security issue.

The server can be run as a windows service with the unsupported Microsoft utility Srvany.exe that can be found in the Windows 2000 and 2003 resource kits (See Appendix F).

The SyncHost Server stores its configuration data in the registry under HKEY_LOCAL_USER. When SyncHost is initially set up, the configuration information is stored in the registry of the user who was logged in at the time. When SyncHost runs as a service, however, it is common to run the service in the context of LocalSystem. Unfortunately LocalSystem does not have access to the configuration info in the registry (and network shares if applicable) and SyncHost appears to do nothing when it is run. Run the service as the user who configured it. Create a local user for the task and set the permissions appropriately (file system permissions and "Log on as a Service" right).

NTFS and Temporary Files Issue

When the SyncHost Server communicates back to the Program client it assembles an encrypted and compressed file to be placed in the OutBox folder.

The contents of this file are assembled in the Temp folder of the user SyncHost Server is running under. The completed file is then moved to the OutBox. If the Temp folder and the Sync Folder are on the same NTFS Volume, the file permissions of this file will move with the file[71] (so they match the permissions of the current user's Temp folder). The file does not inherit the permissions of the OutBox as is required.

[71] See "How Permissions are Handled When You Copy and Move Files and Folders". URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;310316, (23 Nov. 2003).

Securing the SyncHost Server to Database Server Transmission

The SyncHost Server communicates to the Database Server through a port. The well-known port for Oracle is 1521 while Microsoft's SQL Server (SQL Server) is 1433, although both can be changed.

To connect to an Oracle database the Oracle Client must be installed on the SyncHost Server. Oracle version 8 (9 and later recommended[72]) supports encrypted connections to the database[73]. There are many configuration options that can be set in an Oracle Client or Server that can change the ports, the method of establishing the connection, and the forms of encryption used. This in turn effects how the firewall needs to be set up. Keep in mind that unless the connection is encrypted in some way, either through native Oracle features or through an external tunnel, the data is sent in cleartext. Although Oracle connections can be difficult to tunnel[74] there is internet documentation available[75].

SQL Server can use IPSec[76] or SSL[77] to encrypt traffic to/from the SyncHost Server. A secure connection can be required by SQL Server, in which case only clients that use SSL can connect, or it can be left up to the client to choose to connect securely or not.

To enable SSL encryption on the SyncHost server, the database connect string in the registry must be manually edited:

```
[HKEY_CURRENT_USER\Software\Synchronization\Host]
```

[72] See a University of Missouri how-to: "Enabling Encryption". URL: https://www.umsystem.edu/umdw_upgrade/encryption.html, (23 Nov. 2003).

[73] See cited work "Oracle Advanced Networking Option Administrator's Guide".

[74] "Protecting Oracle Connections". URL: http://www.stunnel.org/examples/oracle.html, (23 Nov. 2003).

[75] Roger Schrag. "Securing Oracle Network Traffic". URL: http://www.dbspecialists.com/presentations/net8_security.html, (23 Nov. 2003).

[76] See cited work Meier, J.D. et.al. "How To: Use IPSec to Provide Secure Communication Between Two Servers". Microsoft Patterns and Practices. Nov. 2002. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/SecNetHT18.asp, (23 Nov. 2003).

[77] See cited work "How To: Use SSL to Secure Communication with SQL Server 2000 Building Secure ASP.NET Applications: Authentication, Authorization, and Secure Communication".

"Host DB Connection String"="provider=SQLOLEDB;data source=db-server;database=database;password=<PASSWORD>;user id=<USERID>;"

Add the string “Use Encryption for Data=True;” to force an encrypted client connection. To change the port number from 1433, add a comma and the port number after the server name (Data Source=ServerName,PortNumber)

Example: Securing a SQL Server Connection with SSL (Case 3)

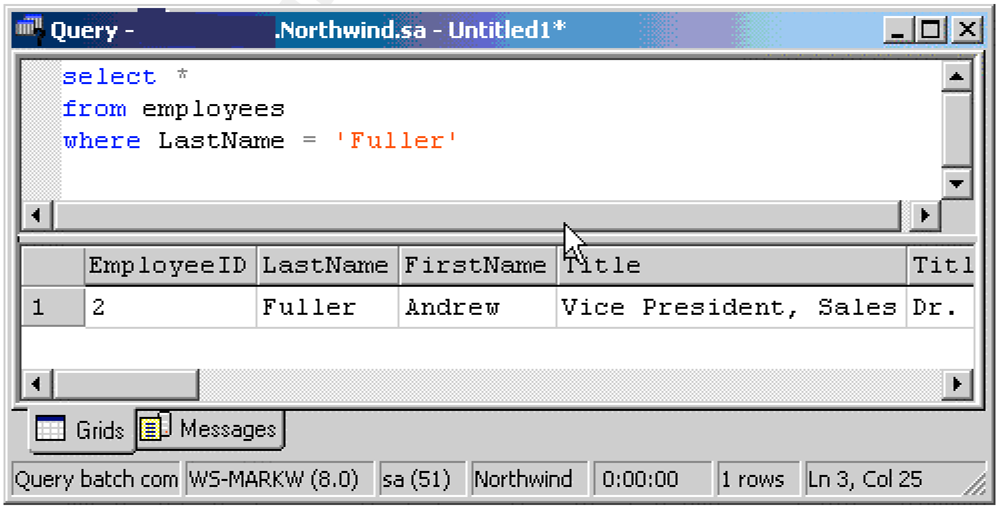
In this example I will be discussing Case 3. The well data starts at the laptop, it is encrypted by the Program Client, and it is sent over an encrypted VPN to the FTP server. The SyncHost server pulls the encrypted data files from the FTP server’s network share via an encrypted IPSec connection. The SyncHost server then decrypts the information.

At this point the data has made is safely all the way from the Field Laptop to the SyncHost server. The data is now in plain text and ready to add to the database. If the database connection is not encrypted, all the work done so far may be for naught.

While I could show another secure IPSec connection to the Database, in Case 3 the SyncHost server and Database server are in different (and isolated) domains. That makes Kerberos authentication somewhat challenging, so let’s try SSL instead.

So in this example I will demonstrate an SSL connection to Microsoft SQL Server 2000. I’ll start by showing what a simple SQL query looks like when it is unprotected.

First, the query:



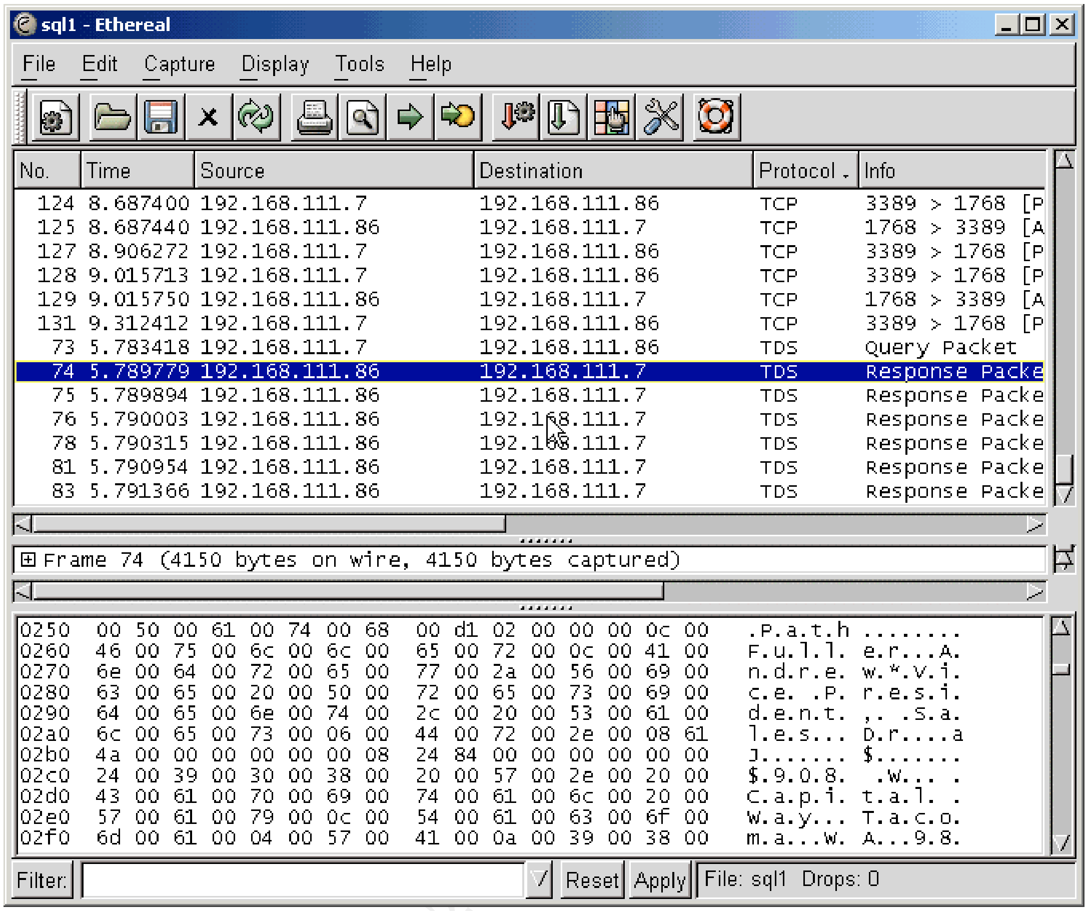
Query - [redacted] .Northwind.sa - Untitled1*

```
select *
from employees
where LastName = 'Fuller'
```

	EmployeeID	LastName	FirstName	Title	Titl
1	2	Fuller	Andrew	Vice President, Sales	Dr.

Query batch com | WS-MARKW (8.0) | sa (51) | Northwind | 0:00:00 | 1 rows | Ln 3, Col 25

And how it looks on the network (the reply packet is shown):



```
No.  Time     Source          Destination     Protocol  Info
124 8.687400 192.168.111.7   192.168.111.86  TCP       3389 > 1768 [P
125 8.687440 192.168.111.86  192.168.111.7   TCP       1768 > 3389 [A
127 8.906272 192.168.111.7   192.168.111.86  TCP       3389 > 1768 [P
128 9.015713 192.168.111.7   192.168.111.86  TCP       3389 > 1768 [P
129 9.015750 192.168.111.86  192.168.111.7   TCP       1768 > 3389 [A
131 9.312412 192.168.111.7   192.168.111.86  TCP       3389 > 1768 [P
 73 5.783418 192.168.111.7   192.168.111.86  TDS       Query Packet
 74 5.789779 192.168.111.86  192.168.111.7   TDS       Response Packe
 75 5.789894 192.168.111.86  192.168.111.7   TDS       Response Packe
 76 5.790003 192.168.111.86  192.168.111.7   TDS       Response Packe
 78 5.790315 192.168.111.86  192.168.111.7   TDS       Response Packe
 81 5.790954 192.168.111.86  192.168.111.7   TDS       Response Packe
 83 5.791366 192.168.111.86  192.168.111.7   TDS       Response Packe
```

```
⊞ Frame 74 (4150 bytes on wire, 4150 bytes captured)
```

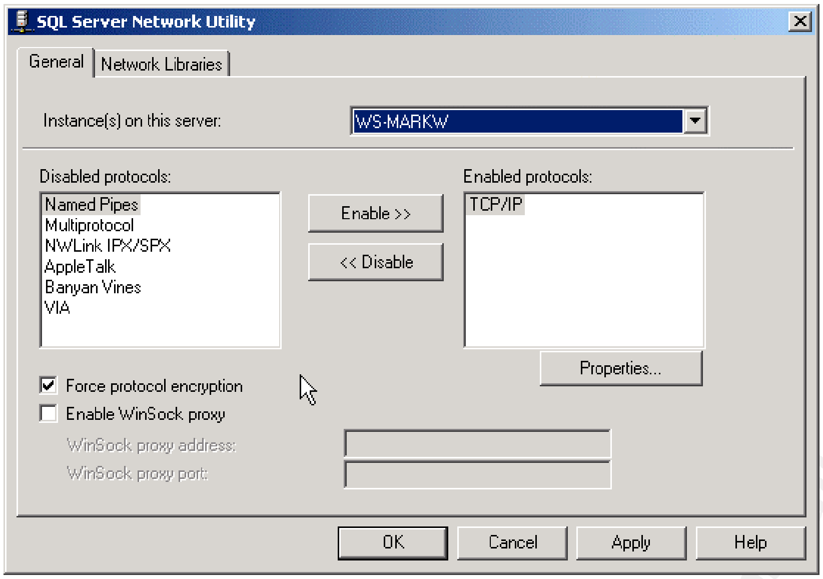
```
0250  00 50 00 61 00 74 00 68  00 d1 02 00 00 00 0c 00   .P.a.t.h ........
0260  46 00 75 00 6c 00 6c 00  65 00 72 00 0c 00 41 00   F.u.l.l. e.r...A.
0270  6e 00 64 00 72 00 65 00  77 00 2a 00 56 00 69 00   n.d.r.e. w.*.V.i.
0280  63 00 65 00 20 00 50 00  72 00 65 00 73 00 69 00   c.e. .P. r.e.s.i.
0290  64 00 65 00 6e 00 74 00  2c 00 20 00 53 00 61 00   d.e.n.t. ,. .S.a.
02a0  6c 00 65 00 73 00 06 00  44 00 72 00 2e 00 08 61   l.e.s... D.r....a
02b0  4a 00 00 00 00 00 00 08  24 84 00 00 00 00 00 00   J....... $.......
02c0  24 00 39 00 30 00 38 00  20 00 57 00 2e 00 20 00   $.9.0.8.  .W... .
02d0  43 00 61 00 70 00 69 00  74 00 61 00 6c 00 20 00   C.a.p.i. t.a.l. .
02e0  57 00 61 00 79 00 0c 00  54 00 61 00 63 00 6f 00   W.a.y... T.a.c.o.
02f0  6d 00 61 00 04 00 57 00  41 00 0a 00 39 00 38 00   m.a...W. A...9.8.
```

As you can see, it’s pretty easy to see the data. So the next step is to set SQL Server 2000 to require SSL encrypted connections. The SQL Server requires a certificate[78]:

To add a certificate to the SQL Server I open the Certificate mmc snap-in for the local computer (on the SQL Server), select Personal > All Tasks… > Request New Certificate, and request a computer certificate. The certificate for the computer appeared in the certificates subfolder.

The SQL Client in my example already trusts the Root CA. So the next step is to require secure connections on the SQL Server:

[78] Be sure to add the certificate before turning on Force Protocol Encryption. See http://support.microsoft.com/default.aspx?scid=kb;EN-US;319349.



SQL Server Network Utility

General | Network Libraries

Instance(s) on this server: WS-MARKW

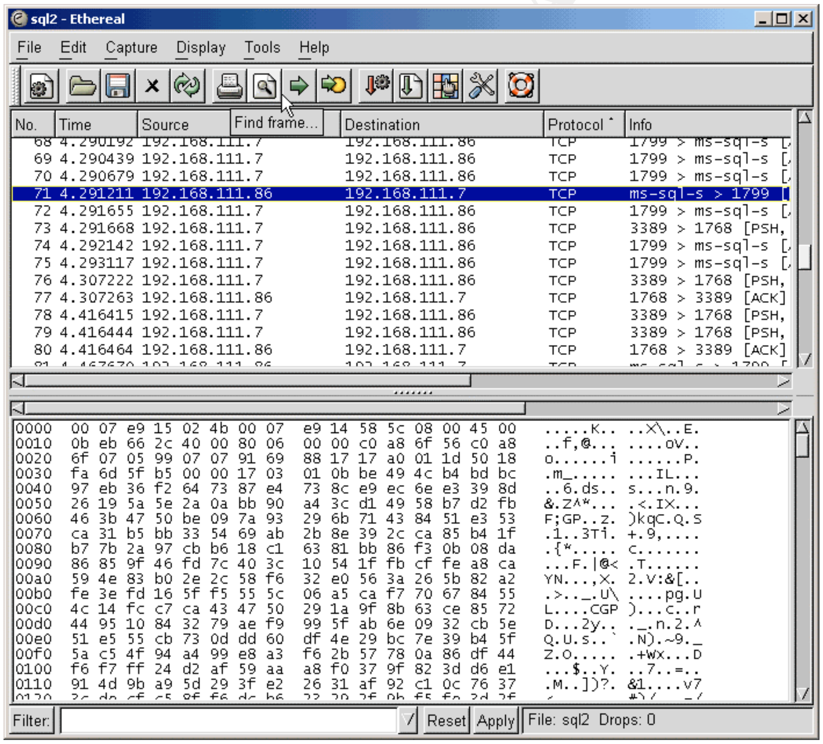
Disabled protocols:
Named Pipes
Multiprotocol
NWLink IPX/SPX
AppleTalk
Banyan Vines
VIA

Enabled protocols:
TCP/IP

☑ Force protocol encryption
□ Enable WinSock proxy
WinSock proxy address:
WinSock proxy port:

Figure 28 - Forcing Encryption in the SQL Network Utility

As you can see I checked “Force protocol encryption”. I then restart the SQL service and reconnect the Client’s Query Analyzer to the server. I run the query and it returns the same results. But a packet trace now shows:



sql2 - Ethereal

```
No. Time     Source          Destination     Protocol Info
 68 4.290192 192.168.111.7   192.168.111.86  TCP      1799 > ms-sql-s [
 69 4.290439 192.168.111.7   192.168.111.86  TCP      1799 > ms-sql-s [
 70 4.290679 192.168.111.7   192.168.111.86  TCP      1799 > ms-sql-s [
 71 4.291211 192.168.111.86  192.168.111.7   TCP      ms-sql-s > 1799 [
 72 4.291655 192.168.111.7   192.168.111.86  TCP      1799 > ms-sql-s [
 73 4.291668 192.168.111.7   192.168.111.86  TCP      3389 > 1768 [PSH,
 74 4.292142 192.168.111.7   192.168.111.86  TCP      1799 > ms-sql-s [
 75 4.293117 192.168.111.7   192.168.111.86  TCP      1799 > ms-sql-s [
 76 4.307222 192.168.111.7   192.168.111.86  TCP      3389 > 1768 [PSH,
 77 4.307263 192.168.111.86  192.168.111.7   TCP      1768 > 3389 [ACK]
 78 4.416415 192.168.111.7   192.168.111.86  TCP      3389 > 1768 [PSH,
 79 4.416444 192.168.111.7   192.168.111.86  TCP      3389 > 1768 [PSH,
 80 4.416464 192.168.111.86  192.168.111.7   TCP      1768 > 3389 [ACK]
```

```
0000  00 07 e9 15 02 4b 00 07  e9 14 58 5c 08 00 45 00   ......K.. ..X\..E.
0010  0b eb 66 2c 40 00 80 06  00 00 c0 a8 6f 56 c0 a8   ..f,@... ....oV..
0020  6f 07 05 99 07 07 91 69  88 17 17 a0 01 1d 50 18   o......i ......P.
0030  fa 6d 5f b5 00 00 17 03  01 0b be 49 4c b4 bd bc   .m_..... ...IL...
0040  97 eb 36 f2 64 73 87 e4  73 8c e9 ec 6e e3 39 8d   ..6.ds.. s...n.9.
0050  26 19 5a 5e 2a 0a bb 90  a4 3c d1 49 58 b7 d2 fb   &.Z^*... .<.IX...
0060  46 3b 47 50 be 09 7a 93  29 6b 71 43 84 51 e3 53   F;GP..z. )kqC.Q.S
0070  ca 31 b5 bb 33 54 69 ab  2b 8e 39 2c ca 85 b4 1f   .1..3Ti. +.9,....
0080  b7 7b 2a 97 cb b6 18 c1  63 81 bb 86 f3 0b 08 da   .{*..... c.......
0090  86 85 9f 46 fd 7c 40 3c  10 54 1f fb cf fe a8 ca   ...F.|@< .T......
00a0  59 4e 83 b0 2e 2c 58 f6  32 e0 56 3a 26 5b 82 a2   YN...,X. 2.V:&[..
00b0  fe 3e fd 16 5f f5 55 5c  06 a5 ca f7 70 67 84 55   .>.._.U\ ....pg.U
00c0  4c 14 fc c7 ca 43 47 50  29 1a 9f 8b 63 ce 85 72   L....CGP )...c..r
00d0  44 95 10 84 32 79 ae f9  99 5f ab 6e 09 32 cb 5e   D...2y.. ._.n.2.^
00e0  51 e5 55 cb 73 0d dd 60  df 4e 29 bc 7e 39 b4 5f   Q.U.s..` .N).~9._
00f0  5a c5 4f 94 a4 99 e8 a3  f6 2b 57 78 0a 86 df 44   Z.O..... .+Wx...D
0100  f6 f7 ff 24 d2 af 59 aa  a8 f0 37 9f 82 3d d6 e1   ...$..Y. ..7..=..
0110  91 4d 9b a9 5d 29 3f e2  26 31 af 92 c1 0c 76 37   .M..])?. &1....v7
```

Filter: File: sql2 Drops: 0

Figure 29 - Encrypted SQL traffic

Where ms-sql-s packets contain the encrypted data. No plain text in any of the packets!

Securing the Database Server

The topic of securing a database server is one for another paper. Different databases have different features, risks, and management tools. There are, however, some common security points that should be mentioned[79]:

- Change the database administrator's password.
- Allow only encrypted connections[80] (if possible).
- Follow good backup practices.
- Monitor (and patch) database vulnerabilities.

The Application enforces database security on the record and field, based on the user credentials that are passed from the SyncHost Server. Application security is set up with a security editor provided by the software vendor.

[79] A detailed list can be found in an article by Neil Boyle. "SQL Server Security Checklist". URL: http://www.databasejournal.com/features/mssql/article.php/2221471, (23 Nov. 2003).

[80] Screen shots of the SQL Server configuration to require SSL connections can be found at URL: http://www.atstake.com/research/reports/eval_ms_ibm/analysis/2.9.2.html, (23 Nov. 2003).

Firewalls Part II

The diagrams in Cases 2 and 3 do not show firewalls between the RRAS, FTP, SyncHost Server, domain controllers, backup servers, etc. In a secure environment it makes sense to protect the servers with external firewalls as well as with internal IPSec filters.

The ports that need to be opened depend on the services that the server is offering and requires from other servers. It also depends on whether the server(s) communicates through IPSec (if all the required traffic is transmitted through IPSec, only the IPSec ports need to be opened!).

The following list was pruned from an excellent web page from Microsoft entitled “Port Requirements for the Microsoft Windows Server System” at http://support.microsoft.com/default.aspx?scid=kb;en-us;832017.

Service	**Application protocol**	**Protocol**	**Ports**
Certificate Services	Randomly allocated high TCP ports	TCP	*random port number*
Computer Browser	NetBIOS Datagram Service	UDP	138
Computer Browser	NetBIOS Name Resolution	UDP	137
Computer Browser	NetBIOS Name Resolution	TCP	137
Computer Browser	NetBIOS Session Service	TCP	139
DHCP Server	DHCP Server	UDP	67
DHCP Server	MADCAP	UDP	2535
DNS	DNS	UDP	53
DNS	DNS	UDP	53
FTP	FTP control	TCP	21

Service	Application protocol	Protocol	Ports
FTP	FTP default data	TCP	20
FTP	Randomly allocated high TCP ports	TCP	*random port number*
IPSec (AH)	IPSec Authentication Header	IP	51
IPSec (ESP)	IPSec Encapsulating Security Payload	IP	50
IPSec Services	IPSec	ISAKMP	500
Kerberos	Kerberos	TCP	88
Kerberos	Kerberos	UDP	88
LSA	Global Catalog Server	TCP	3269
LSA	Global Catalog Server	TCP	3268
LSA	LDAP Server	TCP	389
LSA	LDAP Server	UDP	389
LSA	LDAP SSL	TCP	636
LSA	LDAP SSL	UDP	636
LSA	Randomly allocated high TCP ports	TCP	*random port number*
SQL Server	SQL over TCP	TCP	1433
SQL Server	SQL Probe	UDP	1434
Net Logon	NetBIOS Datagram Service	UDP	138
Net Logon	NetBIOS Name	TCP	137

Service	Application protocol	Protoco l	Ports
	Resolution		
Net Logon	NetBIOS Name Resolution	UDP	137
Net Logon	NetBIOS Session Service	TCP	139
Net Logon	SMB	TCP	445
Net Logon	SMB	UDP	445
RRAS	GRE (IP protocol 47)	GRE	n/a
RRAS	IPSec AH (IP protocol 51)	AH	n/a
RRAS	IPSec ESP (IP protocol 50)	ESP	n/a
RRAS	L2TP	UDP	1701
RRAS	NAT-T	UDP	4500
RRAS	PPTP	TCP	1723
Server	NetBIOS Datagram Service	UDP	138
Server	NetBIOS Name Resolution	TCP	137
Server	NetBIOS Name Resolution	UDP	137
Server	NetBIOS Session Service	TCP	139
Server	SMB	TCP	445
Server	SMB	UDP	445

Service	Application protocol	Protoco l	Ports
Terminal Services	Terminal Services	TCP	3389

Appendix A - Background

The Program is run by Oil & Gas companies to manage and send data from remote rig sites to their corporate head offices. The data is gathered often, typically on a predefined schedule, and in some cases is extremely confidential. Head offices are usually located in large urban centers. The rig sites, which I'll call the **Field**, are where the new oil and gas wells are actually being drilled and can be anywhere in the country, even offshore.

The data is very valuable; well and drilling information can be worth millions of dollars. Security is a primary requirement as industrial spying is somewhat accepted in the industry. Professional "scouts" are employed to gather information on competitors' drilling activity. Scouts employ methods ranging from low-tech (binoculars and social engineering for example) to high-tech spy gadgets.

Drilling in the Far North presents the most challenging conditions for secure operations. Because Northern Canada is a large bog, drilling is seasonal. The drilling season starts in the fall when the ground freezes and heavy equipment can be driven to the Field. The drilling season ends in the spring when the ground thaws. It is common for rig workers to change companies throughout the drilling season. Generally, oil workers do not have a reputation as a computer skilled workforce.

To make matters slightly worse, it is common for companies to pay field users to supply their own laptops; the employer provides only the Program and basic training. Many Field workers pocket their computer stipend and run outdated laptops and old Windows versions. Some corporate IT departments never see the laptops that they allow to pass data into their central database.

A further challenge is the remote locations make network communications difficult. In the vast areas outside of cell coverage, satellite and bag phones provide data connections as low as 2400 baud. Even when faster connections are possible, they are often unreliable.

Appendix B – Modified HiSecWeb.Inf

```
; (c) Microsoft Corporation 1997-2000

;

; Security Configuration Template for Security Configuration Editor

;

; Template Name:        HiSecWeb.INF

; Template Version:     05.00.HB.0000

;

; ------------------------------------------------------------------

; Revision History

; ------------------------------------------------------------------

; Date            Comment

; 03-Sep-1999     Original, based on the following assumptions:

;                 Machine is a not a Domain Controller

;                 DC's should not be web-servers

;                 Machine is a standalone server

;                 - If machine is joined to a domain,

;                   then domain-level policies may (or may not)

;                   overwrite these settings.

;                 - If machine is joined to a domain,

;                   it should be in it's own OU, and you would
;                   apply this template at the OU level.

;                 Machine is a dedicated web-server and physically
protected

;                 Machine has the Windows 2000 clean-install defaults

;                 - No modifications have been made to ACLs, User
Rights etc.

;                 No one is allowed to log on locally to the machine
accept an admin

;                 Admins are not allowed to log on over

;                 the network (they have to go to the Web server to
administer it)

;                 Admin\Guest accounts are not renamed via this
template

; 24-Jan-2000     Updated registry entries

; 23-May-2000     Updated to reduce SMB/Secure channel signing
requirements.

; 17-Dec-2003     MW – Allow network logon for Administrators,

;                 enable Terminal Service, change logon message

; -------------------------------------------------------------------



[version]

signature="$CHICAGO$"

Revision=1



[System Access]

MinimumPasswordAge = 2
```

```
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = -1
RequireLogonToChangePassword = 0
ClearTextPassword = 0

[System Log]
RestrictGuestAccess = 1

[Security Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1

[Application Log]
RestrictGuestAccess = 1

;----------------------------------------------------------------------
```

```
;     Local Policies\Audit Policy
;----------------------------------------------------------------------
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 3
AuditPolicyChange = 3
AuditAccountManage = 3
AuditAccountLogon = 3

[Strings]
SceInfAdministrator = Administrator
SceInfAdmins = Administrators
SceInfAcountOp = Account Operators
SceInfAuthUsers = Authenticated Users
SceInfBackupOp = Backup Operators
SceInfDomainAdmins = Domain Admins
SceInfDomainGuests = Domain Guests
SceInfDomainUsers = Domain Users
SceInfEveryone = Everyone
SceInfGuests = Guests
```

```
SceInfGuest = Guest

SceInfPowerUsers = Power Users

SceInfPrintOp = Print Operators

SceInfReplicator = Replicator

SceInfServerOp = Server Operators

SceInfUsers = Users



[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\SeCEdit\Reg
Values\MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/SynAt
tackProtect]

"ValueType"=dword:00000004

"DisplayType"=dword:00000000

"DisplayName"="TCPIP: Syn Attack Protection"



[Privilege Rights]

SeNetworkLogonRight = *S-1-5-32-544

[Group Membership]

*S-1-5-32-547__Memberof =

*S-1-5-32-547__Members =

[Service General Setting]

Alerter,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

ClipSrv,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

```
Browser,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Dhcp,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLC
SWRPWPDTLOCRSDRCWDWO;;;WD)"

Fax,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;WD)"

SharedAccess,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;F
A;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Messenger,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;C
CDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

mnmsrvc,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Spooler,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

RasAuto,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

RasMan,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDC
LCSWRPWPDTLOCRSDRCWDWO;;;WD)"

RemoteRegistry,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU
;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Schedule,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CC
DCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

TapiSrv,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

;TermService,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;F
A;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

PolicyAgent,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC
;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"

W3SVC,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"

IISADMIN,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;
IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
```

```
Irmon,4,"D:AR(A;;RPWPDTRC;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;AU)(A;;
CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"

[Registry Values]

MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,2

MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown=4,1

MACHINE\System\CurrentControlSet\Control\Session
Manager\ProtectionMode=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\Enabl
eSecuritySignature=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\Enabl
eForcedLogOff=4,1

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\
EnableSecuritySignature=4,1

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\
EnablePlainTextPassword=4,0

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePa
sswordChange=4,0

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecur
eChannel=4,1

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecur
eChannel=4,1

MACHINE\Software\Microsoft\Driver Signing\Policy=3,2

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Disab
leCAD=4,0

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontD
isplayLastUserName=4,1
```

```
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shutd
ownWithoutLogon=4,0

MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1

MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AllocateDASD=1,0

MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AllocateFloppies=1,1

MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\Printers\DisableWebPrinting=4,1

MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3Nam
eCreation=4,1

MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoS
hareServer=4,0

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRe
direct=4,0

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableSecuri
tyFilters=4,1

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackPro
tect=4,1

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGW
Detect=4,0

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDi
scovery=4,0

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTim
e=4,300000

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSou
rceRouting=4,1

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnec
tResponseRetransmissions=4,2

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRe
transmissions=4,3
```

```
MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\NoNameReleas
eOnDemand=4,1

MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\DynamicBacklog
GrowthDelta=4,10

MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\EnableDynamicB
acklog=4,1

MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MinimumDynamic
Backlog=4,20

MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MaximumDynamic
Backlog=4,20000

MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,1

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Legal
NoticeText=1,This is a private computer system.

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Legal
NoticeCaption=1,A T T E N T I O N !
```

Appendix C – FTP Metabase

A complete list of Metabase keys can be found in Microsoft's "Metabase Property Reference", URL: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/ref_mb_aambref.asp

The following keys are particularly relevant, although most only apply to IIS 6. They are copied directly from the Microsoft site and are listed for convenience. For a full list, check out the link above.

PassivePortRange

The **PassivePortRange** property specifies the range of data ports to be used by the FTP service in response to PASV commands.

PASV FTP requires the server to open a data port for the client to make a second connection. This is a separate connection than the typical port 21 that is used for the control channel. The second connection is used when data files are transferred back to the client. By configuring the port range, you can write firewall and router rules to allow external clients access only to the ports they need and reduce the attack surface available to malicious users. In other words, if you have applications other than FTP that are using the default port range of 1025-5000, and do not want to expose these ports through your firewall in order to enable PASV FTP, you can use this value to change the range that you must open through your firewall. If this value is not specified, or is set to an empty string, the default value of 1025-5000, as specified by Winsock, is used. If this property is specified, the valid range that FTP will validate is from 5001 to 65535 (see **StartingNumber** and **EndingNumber** below), and may be a range or a single number.

This property can be set only at the service level. In order to make the changes effective, the service must be restarted. If the value is invalid, the service will invalidate it and will not restart.

AllowAnonymous

The **AllowAnonymous** property specifies whether the FTP server will allow anonymous access. The default is true.

DontLog

The **DontLog** property specifies whether client requests are written to the log file. By default, requests are written to the log file. You can set this value to **true** to turn logging off.

LogFileDirectory

The **LogFileDirectory** property specifies the default logging directory, where the log file and logging-related support files are stored. The specified log-file directory must be on the local computer.

IPSecurity

The **IPSecurity** property specifies the IP access restrictions for a URL. This property can be used to assign or deny access to browsers, based on either their IP address or DNS host name.

GreetingMessage

The **GreetingMessage** contains a greeting message that can be sent to new clients from an FTP server.

MaxClientsMessage

The **MaxClientsMessage** property contains a string that is displayed to an FTP client when there are too many FTP clients accessing the server. You can configure the maximum number of FTP clients by using the **MaxConnections** property.

ExitMessage

The **ExitMessage** property specifies the message text an FTP server transmits to a client, when the client sends a **quit** command.

Path

The **Path** property specifies the physical path associated with a virtual directory.

FtpDirBrowseShowLongDate

The **FtpDirBrowseShowLongDate** indicates whether to display two-digit or four-digit years when browsing directories. The **MSDOSDirOutput** property allows UNIX-style directory browsing, and if set to **false**, **FtpDirBrowseShowLongDate** will have no effect. **FtpDirBrowseShowLongDate** is valid only when **MSDOSDirOutput**=true, which sets the directory output to MS-DOS format .

MSDOSDirOutput

The **MSDOSDirOutput** property specifies the style of directory output for a **list** operation request from an FTP client. If the value is **true**, the format is in MS-DOS® style, if **false**, it is produced in UNIX style.

ServerSize

The **ServerSize** property specifies the general size of the server, in terms of the number of client requests processed per day. A value of 0 (zero) indicates a small Web site that expects to receive fewer than 10,000 requests per day; a value of 1 indicates a medium site handling between 10,000 and 100,000 requests per day; and a value of 2 designates a large site, processing more than 100,000 requests a day. The value of this property is used in calculating the value for the ServerListenBacklog property.

ServerListenTimeout

The **ServerListenTimeout** property specifies the amount of time (in seconds) the server waits for a client to send data. After the allotted amount of time passes, the server disconnects the client. The default is 120.

ServerListenBacklog

The **ServerListenBacklog** property specifies the number of outstanding sockets that can be queued. The value is based on the *AcceptEx* operating system parameter, and the server size specified in the ServerSize property. Valid values for this property range from 5 to 500. The default is 40.

MaxConnections

The **MaxConnections** property specifies the maximum number of simultaneous connections to a server. The valid range is 0 to 4294967295 (unlimited). The MaxClientsMessage property can be used to send a message to clients when this value has been exceeded.

MaxEndpointConnections

The **MaxEndpointConnections** property specifies the maximum number of "listen" sockets that will be aggregated on a network endpoint. For example, if this value is set to 15, then a maximum of 15 total connections can be made to a single port, even if more than one domain is bound to the port.

The metabase represents unlimited as the DWORD value of 4294967295 (0xFFFFFFFF); however, VBScript represents unlimited in hexadecimal format as &HFFFFFFFF. Previous versions of IIS represented unlimited as -1.

ConnectionTimeout

The **ConnectionTimeout** property specifies the amount of time (in seconds) that the server waits before disconnecting an inactive connection. (default 120)

ServerBindings

The **ServerBindings** property specifies a string that IIS uses to determine which network endpoints are used by the server instance. The string format is *IP*:*Port*:*Hostname*.

The following Metabase keys can be used to set up virtual directories based on what user logging in.

UserIsolationMode

The **UserIsolationMode** property defines the isolation type desired on the corresponding FTP site.

If **UserIsolationMode** is set to 0, there is no user isolation. This setting is the default and is backwards-compatible.

If the property is set to 1, a client authenticates using local or domain accounts, then is sent to a folder under the root matching the user name. This setting is known as "Isolated (Locally)", and supports users who do not want to use Active Directory (AD).

If the property is set to 2, user isolation is dependent on Active Directory. This setting is known as "Isolated (Active Directory)" and is primarily of use to Internet service providers (ISPs) and other customers who want to set up large numbers of FTP accounts.

If you set this property to 2, you should also set DefaultLogonDomain, ADConnectionsPassword, and ADConnectionsUserName.

DefaultLogonDomain

The **DefaultLogonDomain** property is used to specify the default domain that the server uses to authenticate users. If the value of **DefaultLogonDomain** is not specified, the default domain will be the domain name controlled by the computer, if the computer is a domain controller. If the computer is not a domain controller, the default domain will be the computer name.

In the case of FTP, IIS uses this domain name to query the corresponding Active Directory (AD) for the two properties required for each user in the Web hosting scenario: msIIS-FTPRoot and msIIS-FTPDir.

ADConnectionsPassword

The **ADConnectionsPassword** property is used when the FTP property, UserIsolationMode, is set to 2, which makes FTP user isolation dependent upon the Active Directory® directory service. Set **ADConnectionsUserName** to the user name that has access to the domain controller, and set **ADConnectionsPassword** to the corresponding password.

ADConnectionsUserName

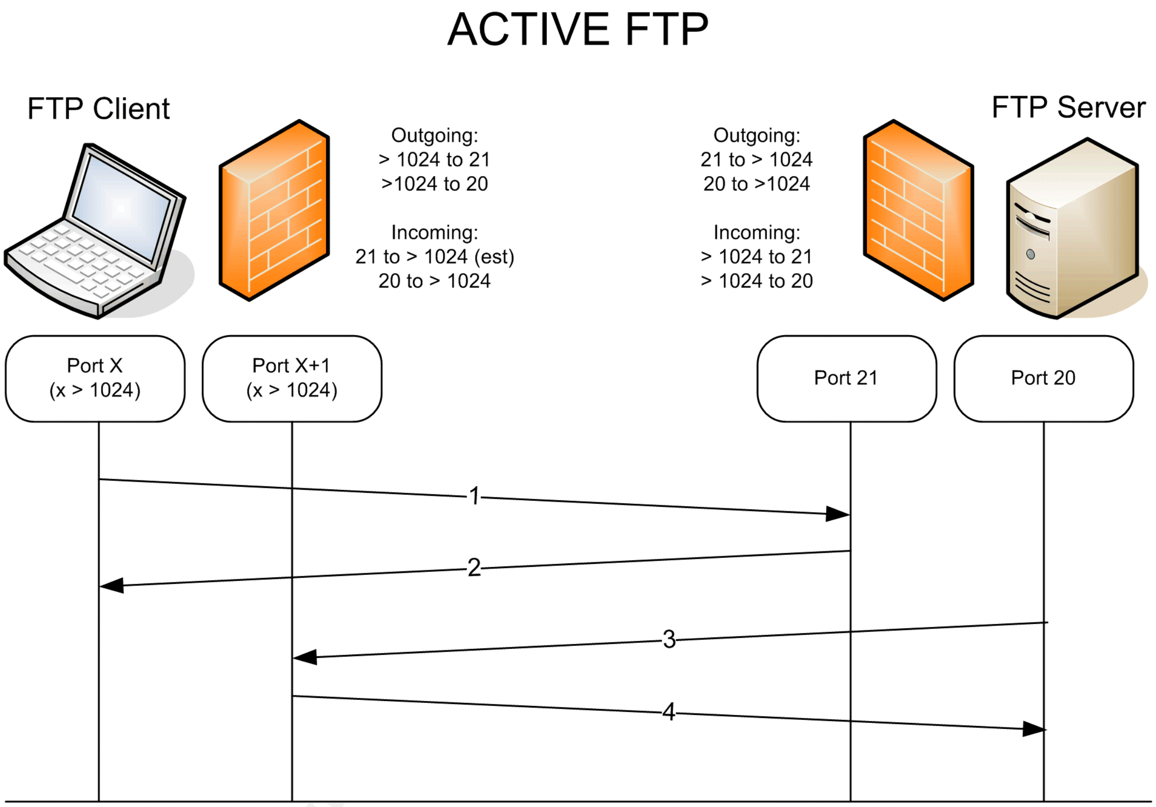
The **ADConnectionsUserName** property is used when the FTP property, UserIsolationMode, is set to 2, which makes FTP user isolation dependent upon Active Directory®. Set **ADConnectionsUserName** to the user name that has access to the domain controller, and set **ADConnectionsPassword** to the corresponding password.

ADConnectionsUserName must be in the *domain\user* format.

Appendix D – Active vs. Passive FTP

The Program Client is hard-coded to use Passive FTP.

The FTP protocol requires two ports, the command port and the data port. Passive FTP differs from Active FTP in that the client initiates both the command and data connections.



1. The FTP Client connects from a high port (> 1024) to the FTP Server's port 21 (command channel). The FTP Client tells the FTP Server what port it is listening on for the data connection.

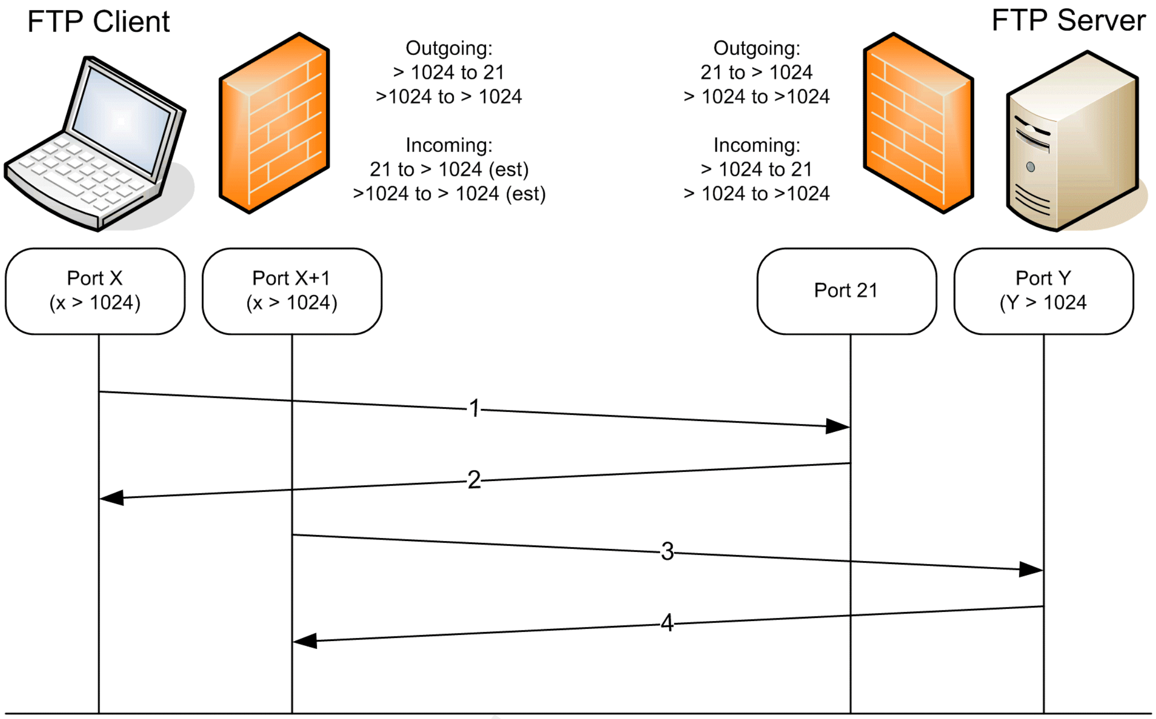
2. The FTP Server acknowledges on the command channel.

3. The FTP Server connects the data channel from port 20 to the listening channel on the FTP Client.

4. The Client acknowledges.

5. The data and command channels are open for file transfer!

Passive FTP



1. The FTP Client connects from a high port (> 1024) to the FTP Server's port 21.

2. The FTP Server acknowledges back with the port number of its data channel.

3. The FTP Client connects from a high port (> 1024 + 1) to the FTP Server's listening data port.

4. The FTP Server acknowledges.

5. The data and command channels are open for file transfer!

Passive FTP is advantageous from the Program Client's point of view as the FTP command and data connections both originate from the client and will more likely work through a local firewall.

Passive FTP is not nice for the FTP Server’s firewall as it has to allow all incoming packets to ports greater than 1024. For a firewall that does packet filtering only, this is a big hole.

Appendix E – Program Client FTP Trace

You may note that there are some MKD commands and corresponding errors. This is a “feature” of the 3rd party FTP control used in the Program Client…

```
Response: 220-<FTP Server> ready...
Response: 220 welcome to <company>.com
Request: USER <user>
Response: 331 user name okay, need password.
Request: PASS <password>
Response: 230 user logged in, proceed.
Request: PWD
Response: 257 "/" is current directory.
Request: TYPE I
Response: 200 Type set to I.
Request: PASV
Response: 227 Entering Passive Mode (142,56,1,27,16,105)
Request: RETR /sync/synchost.key
Response: 150 opening BINARY mode data connection for synchost.key (338 bytes).
Response: 226 Transfer complete.
Request: TYPE A
Response: 200 Type set to A.
Request: PASV
Response: 227 Entering Passive Mode (142,56,1,27,16,106)
Request: LIST /sync/inbox/B915822965554DA78C4EF868BDF898A2.data
Response: 150 opening ASCII mode data connection for /bin/ls.
Response: 226 Transfer complete.
Request: TYPE I
Response: 200 Type set to I.
Request: MKD /sync
Response: 550 /sync: failed to create.
Request: MKD /sync/inbox
Response: 550 /sync/inbox: failed to create.
Request: PASV
Response: 227 Entering Passive Mode (142,56,1,27,16,107)
Request: STOR /sync/inbox/B915822965554DA78C4EF868BDF898A2.data
Response: 150 opening BINARY mode data connection for
B915822965554DA78C4EF868BDF898A2.data
Response: 226 Transfer complete.
Request: TYPE A
Response: 200 Type set to A.
Request: PASV
Response: 227 Entering Passive Mode (142,56,1,27,16,108)
Request: LIST /sync/inbox/B915822965554DA78C4EF868BDF898A2.command
Response: 150 opening ASCII mode data connection for /bin/ls.
Response: 226 Transfer complete.
Request: TYPE I
Response: 200 Type set to I. Request: MKD /sync
Response: 550 /sync: failed to create.
Request: MKD /sync/inbox
Response: 550 /sync/inbox: failed to create.
Request: PASV
Response: 227 Entering Passive Mode (142,56,1,27,16,109)
Request: STOR /sync/inbox/8915822965554DA78C4EF868BDF898A2.command
```

```
Response: 150 opening BINARY mode data connection for
B915822965554DA78C4EF868BDF898A2.v
Response: 226 Transfer complete.
Request: TYPE A
Response: 200 Type set to A.
Request: PASV
Response: 227 Entering Passive Mode (142,56,1,27,16,110)
Request: LIST /sync/outbox/8915822965554DA78C4EF868BDF898A2.command
Response: 150 opening ASCII mode data connection for /bin/ls.
Response: 226 Transfer complete.
Request: TYPE A
Response: 200 Type set to A.
Request: PASV
Response: 227 Entering Passive Mode (142,56,1,27,16,111)
Request: LIST /sync/outbox/8915822965554DA78C4EF868BDF898A2.command
Response: 150 opening ASCII mode data connection for /bin/ls.
Response: 226 Transfer complete.
Request: TYPE I
Response: 200 Type set to I.
Request: PASV
Response: 227 Entering Passive Mode (142,56,1,27,16,112)
Request: RETR /sync/outbox/8915822965554DA78C4EF868BDF898A2.command
Response: 150 opening BINARY mode data connection for
B915822965554DA78C4EF868BDF898A2.command
Response: 226 Transfer complete.
Request: TYPE I
Response: 200 Type set to I.
Request: PASV
Response: 227 Entering Passive Mode (142,56,1,27,16,113)
Request: RETR /sync/outbox/8915822965554DA78C4EF868BDF898A2.data
Response: 150 Opening BINARY mode data connection for
8915822965554DA78C4EF868BDF898A2.data
Response: 226 Transfer complete.
Request: DELE /sync/outbox/8915822965554DA78C4EF868BDF898A2.data
Response: 250 DELE command successful.
Request: DELE /sync/outbox/8915822965554DA78C4EF868BDF898A2.command
Response: 250 DELE command successful.
Request: DELE /sync/outbox/B915822965554DA78C4EF868BDF898A2.data
Response: 550 /sync/outbox/B915822965554DA78C4EF868BDF898A2.data: No such file or
dir
Request: QUIT
Response: 221 Goodbye!
```

Appendix F – Running a Win32 Exe as a Service

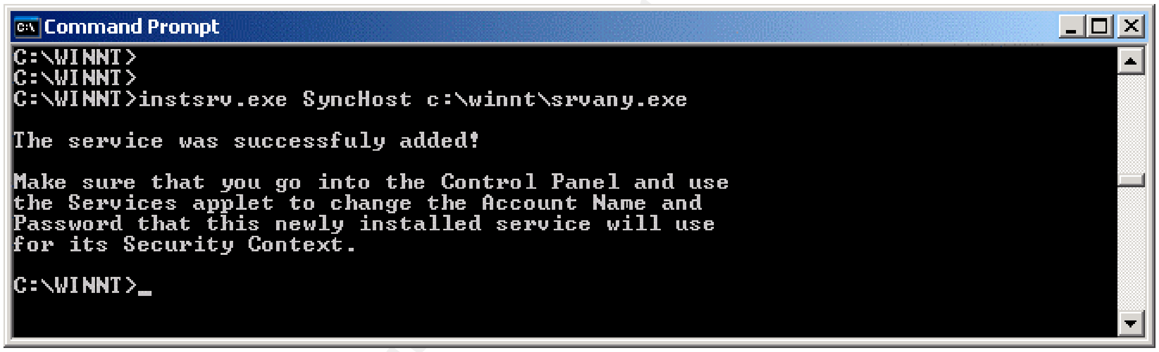
The Windows NT Resource Kit provides two utilities that can be used to create a service from a windows executable (not batch files though).

The Instrsrv.exe program is used to add and remove services from the Windows system services list (the list you see in the Control Panel's Services applet). The Srvany.exe utility is used to actually run the program as a service.

To install a service:

C:\><path>INSTSRV.EXE SyncHost <path>\SRVANY.EXE

Where <path> is the drive and folder that contains the two utilities.



```
C:\WINNT>
C:\WINNT>
C:\WINNT>instsrv.exe SyncHost c:\winnt\srvany.exe

The service was successfuly added!

Make sure that you go into the Control Panel and use
the Services applet to change the Account Name and
Password that this newly installed service will use
for its Security Context.

C:\WINNT>_
```

The next step is to edit the registry with Regedt32.exe:

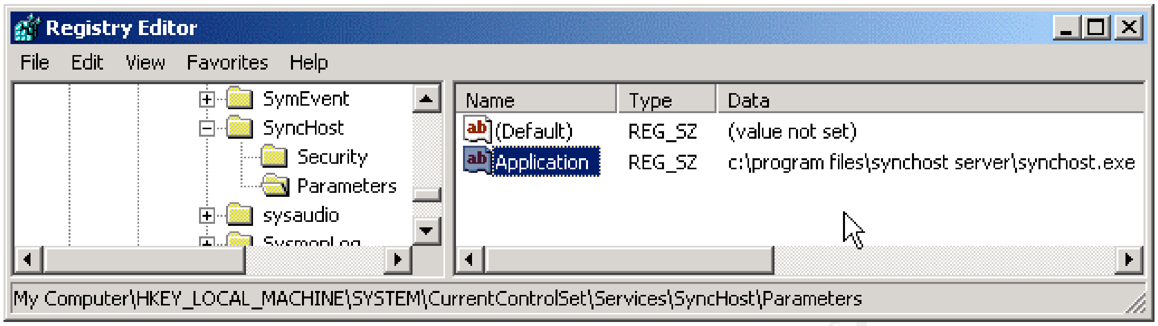
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SyncHost

From the Edit menu, click Add Key and enter:

Key Name: Parameters
Class: <leave blank>

Next, select the Parameters key just created and click New String Value from the Edit menu:

Value Name: Application
Data Type: REG_SZ
String : <path>\synchost.exe



Name	Type	Data
(Default)	REG_SZ	(value not set)
Application	REG_SZ	c:\program files\synchost server\synchost.exe

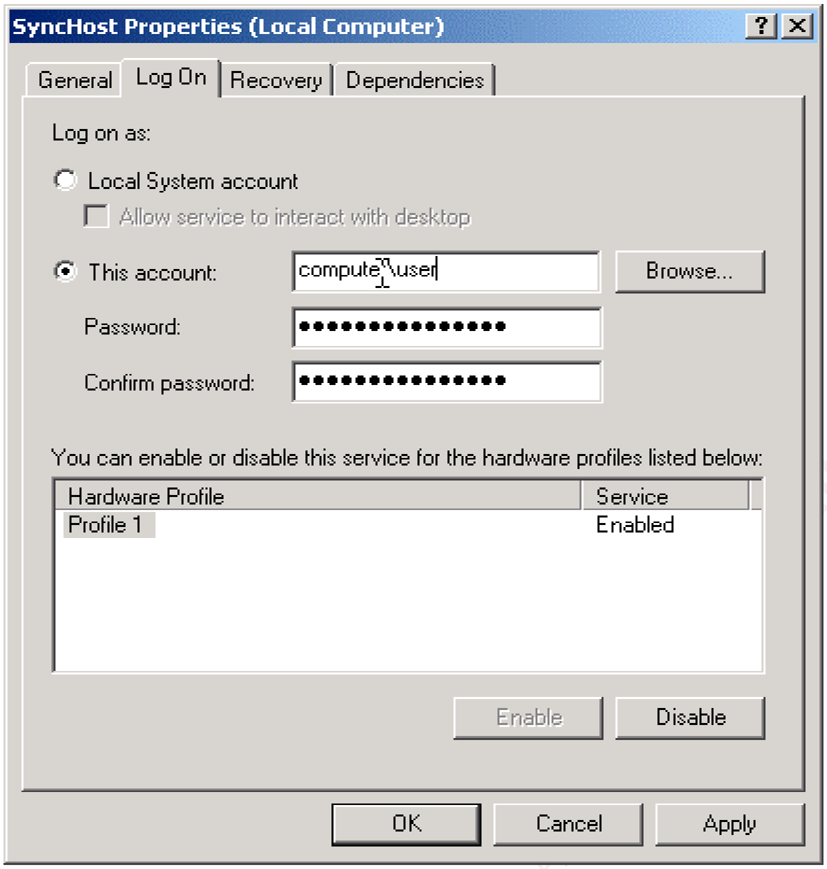
My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SyncHost\Parameters

By default, a newly created service is configured to run Automatically when the system is restarted. The service also defaults to run as the Local System Account.

To change settings, run the Services applet from Control Panel (or Manage Computer on XP).

The SyncHost server needs to be run in the security context of the user who configured it. If run as the default LocalSystem, the application will not have access to the registry area that contains its configuration or mapped drives.

In the Services applet go to the Log On tab and change the Account the service runs as:



SyncHost Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: computer\user

Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Profile 1	Enabled

Works Cited

"Active directory in networks segmented by firewalls". July 2002. URL: www.microsoft.com/windows2000/docs/adsegmented.doc, (18 Nov. 2003).

"Active FTP vs. Passive FTP, a Definitive Explanation". URL: http://slacksite.com/other/ftp.html, (2 Sept. 2003).

"Administrator's Guide to Microsoft L2TP/IPSec VPN Client". June 2002. URL: http://www.microsoft.com/windows2000/docs/VPNClient_AdminGuide.doc, (16 Nov. 2003).

"Advance Office XP Password Recovery". Elcomsoft Proactive Software. URL: http://www.crackpassword.com/products/prs/integpack/officexp/, (23 Nov. 2003).

"Before you start: Understanding Connection Manager and the Administration Kit". URL: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/cmak_ops_03.asp, (23 Nov. 2003).

Boswell, William. "EFS Best Practices". 10 Mar. 2000. URL: http://www.informit.com/content/index.asp?product_id=%7BA762B6C0%2D2D1C%2D470D%2DBE7C%2DB78103711CAD%7D, (23 Nov. 2003).

Boyle, Neil. "SQL Server Security Checklist". URL: http://www.databasejournal.com/features/mssql/article.php/2221471, (23 Nov. 2003).

"CDPC – Sierra Wireless Aircard 555 Frequently Asked Questions". 7 May 2003. URL: http://www.sierrawireless.com/SupportDownload/faq_ac555.asp, (19 Nov. 2003).

"Check Point Firewall 1 Guide" (2001): 169 -170

Chen, Patrick. "Modem Tutorial – Error correction Protocols". 1991. URL: http://www.sfn.saskatoon.sk.ca/Help/ModemTutorial/MT-Error.html, (23 Nov. 2003).

Cheswick, William and Steven Bellovin. Firewalls and Internet Security, Repelling the Wily Hacker. Reading: Addison-Wesley, 1994.

"Citrix MetaFrame Access Suite". Citrix. URL: http://www.citrix.com/site/PS/products/family.asp?familyID=19, (23 Nov. 2003).

"Comprehensive List of File and Folder Comparison and Synchronization Tools". 2 Aug 2002. URL: http://www.foldermatch.com/fmcompetitors.htm, (23 Nov. 2003).

"Computer Forensic Services and Systems". Vogon. URL: http://www.vogon-computer-evidence.com/, (23 Nov. 2003).

"Counterpane's reply to the CTIA", URL: http://www.schneier.com/cmea-response.html , (23 Nov. 2003).

"Data Compression". URL: http://www.modem.com/glossary/glos2.html, (23 Nov. 2003).

Den Beste, Steven. “Can I use a normal modem with my CDMA cell phone?”. CDMA FAQ. May 1999. URL: http://home.san.rr.com/denbeste/modem.html, (20 Nov. 2003).

“Enabling Encryption”. URL: https://www.umsystem.edu/umdw_upgrade/encryption.html, (23 Nov. 2003).

“End-to-End Security”. Deploying Network Services, http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/dnsbj_ips_grdc.asp, (23 Nov. 2003).

“Expanding and Securing Remote Client Access “. Windows 2000 Server Resource Kit, Network Deployment Guide. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/reskit/deploy/netdepl/ndgch07.asp, (23 Nov. 2003).

“Firewalls Explained”. TechTV. 18 Nov. 2002. URL: http://www.techtv.com/callforhelp/answerstips/story/0,24330,2436994,00.html , (23 Nov. 2003).

Fossen, Jason. Windows 2000 PKI, Smart Cards, and the Encrypting File System. SANS Institute, version 7.2 (2002). 133.

Fossen, Jason. DNS and Group Policy. SANS Institute, version 1.1 (2002). 83.

“High-Speed Broadband Internet Satellite Access (Hsi) for Business”. Infosat Telecommunications. URL: http://www.infosat.com/services/hsi/index.html, (23 Nov. 2003).

"How Permissions are Handled When You Copy and Move Files and Folders", Microsoft Knowledge Base. 6 June 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;310316, (23 Nov. 2003).

"How To: Create a User-Defined Service". Microsoft Knowledge Base. 7 May 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;137890, (19 Nov. 2003).

"How To: Use SSL to Secure Communication with SQL Server 2000". Building Secure ASP.NET Applications: Authentication, Authorization, and Secure Communication. Nov 2002. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/secnetht19.asp, (23 Nov. 2003).

"How to Configure a L2TP/IPSec Connection Using Pre-shared Key Authentication". URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q240262, (22 Nov. 2003).

"How to Configure Automatic Updates by Using Group Policy or Registry Settings". Microsoft Knowledge Base. 4 Nov. 2003. URL: http://support.microsoft.com/default.aspx?kbid=328010, (23 Nov. 2003).

"How to Determine the OS Type in a login Script". Microsoft Knowledge Base. 9 Nov. 2003. URL: http://support.microsoft.com:80/support/kb/articles/q190/8/99.asp&NoWebContent=1&NoWebContent=1, (11 Dec. 2003).

"How to Enable IPSec Traffic Through a Firewall". Microsoft Knowledge Base. 21 Nov. 2003. URL: http://support.microsoft.com/default.aspx?kbid=233256, (23 Nov. 2003).

"How to Manually Open Ports in Internet Connection Firewall in Windows XP". Microsoft Knowledge Base. 3 Nov. 2003, URL: http://support.microsoft.com/default.aspx?kbid=308127, (23 Nov. 2003).

"How XyLoc works". Ensure Technologies. URL: http://www.xyloc.com/products/technology/technology.html#HowXyLocWorks, (23 Nov. 2003).

"ICSA Labs' Firewall Community", ICSA Labs, 5 Dec. 2002. URL: http://www.icsalabs.com/html/communities/firewalls/index.shtml, (23 Nov. 2003).

"IIS FTP Registry Paramters", Microsoft Knowledge Base. 30 Apr. 1999. URL: http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q147/6/21.asp&NoWebContent=1, (14 Dec. 2003).

"Inbound Connections Limit in Windows", Microsoft Knowledge Base. 6 May 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;122920, (23 Nov. 2003).

"ISDNLink INET Router", 20 Dec. 2001. URL: http://www.asuscom.com.tw/product/inet8xx.html, (20 Nov. 2003).

"IP Security Protocol (ipsec)". 16 Oct. 2003. URL: http://www.ietf.org/html.charters/ipsec-charter.html, (23 Nov. 2003)

Khosa, Amardeep. InfoSat. Interview. 21 Nov. 2003.

Larrow, Lynn. "Dial-up and Home Networking Troubleshooting Reference". 1 June 2003, http://www.internetweekly.org/llarrow/mtumss.html, (23 Nov. 2003).

Meier, J.D., Alex Mackman, Michael Dunner, Srinath Vasireddy. "How To: Use IPSec to Provide Secure Communication Between Two Servers". URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/SecNetHT18.asp, (23 Nov. 2003).

"Metabase Property Reference", Microsoft Technet, URL: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/ref_mb_aambref.asp, (16 Dec. 2003).

"Microsoft Connection Manager". URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=4981, (23 Nov. 2003).

Norberg, Stefan. "Building a Windows NT Bastion Host in Practice". Version 1.01. http://www.blacksheepnetworks.com/security/info/nt/ntbastion/, (23 Nov. 2003).

Norberg, Stefan. Securing Windows NT/2000 Servers for the Internet, California: O'Reilly, 2001.

"Optimizing Radio Performance for Hostile Environments". URL: http://www.moseleysb.com/OptPerf1.html, (23 Nov. 2003).

"Oracle Advanced Networking Option Administrator's Guide". Release 8.0. URL: http://sunsite.eunnet.net/documentation/oracle.8.0.4/network.804/a58229/toc.htm, (23 Nov. 2003).

Paynter, Bill. "Laptop Security". URL: http://www.asis119.org/articles.php?artid=5, (18 Nov. 2003).

"patch". Gnu Software. 27 June 2000. URL: http://www.gnu.org/software/patch/patch.html, (23 Nov. 2003).

"Port Forwarding", SSH Admin Guide. URL: http://www.ssh.com/support/documentation/online/ssh/adminguide/32/Port_Forwarding.html, (23 Nov. 2003).

"Port Requirements for the Microsoft Windows Server System", 24 Nov. 2003. Microsoft Knowledge Base, URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;832017, (16 Dec. 2003).

"Protecting Oracle Connections". URL: http://www.stunnel.org/examples/oracle.html, (23 Nov. 2003).

"Protecting your laptop computer", 3 Jan. 2003. URL: http://www.itso.iu.edu/howto/laptop, (23 Nov., 2003).

"protocol.txt [definition of X-SafeTP1]". URL: http://safetp.cs.berkeley.edu/protocol.txt, (23 Nov. 2003).

"Protocol Analysis". Thin Client Security Homepage, URL: http://www.nue.et-inf.uni-siegen.de/~schmidt/tcsecurity/protocols.html, (23 Nov. 2003).

Ray. “Configuring and using and FTP Proxy”. 16 Nov. 2002. URL: http://librenix.com/?inode=2465, (23 Nov. 2003).

“Registry Tip #8: XP registry values to tune EFS caching”. URL: http://is-it-true.org/nt/xp/registry/rtips8.shtml, (12 Dec. 2003).

“Remote Access”. Solutions. URL: http://www.tushaus.com/Sol/Communications/RemoteAccess/Citrix.asp, (23 Nov. 2003).

“Repackaging Applications for Distribution”, URL: http://appdeploy.com/articles/repack.shtml, (10 Dec. 2003).

“SafeTP Transparent FTP Security Software”, URL: http://safetp.cs.berkeley.edu/, (23 Nov. 2003).

Schneier, Bruce and Mudge. “Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)”. URL: http://www.schneier.com/paper-pptp.html, (23 Nov. 2003).

Schrag, Roger. “Securing Oracle Network Traffic”. URL: http://www.dbspecialists.com/presentations/net8_security.html, (23 Nov. 2003).

“Security Evaluation Windows Server 2003 with .NET Framework and IBM Websphere”. URL: http://www.atstake.com/research/reports/eval_ms_ibm/analysis/2.9.2.html, (23 Nov. 2003).

"Security Recommendation Guidelines", National Security Agency, 24 Nov. 2003. URL: http://www.nsa.gov/snac/index.html, (10 Dec. 2003).

"Serv-U Home Page", URL: http://www.serv-u.com/, (11 Dec. 2003)

"SSH man page". OpenBSD Reference Manual. 5 Sept. 1999. URL: http://www.openbsd.org/cgi-bin/man.cgi?query=ssh&sektion=1, (23 Nov. 2003).

"Symantec Ghost Corporate Edition", URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=3&EID=0, (10 Dec. 2003).

"The National Security Agency Technology Transfer". 1998. URL: http://www.nsa.gov/programs/tech/factshts/modem.html, (23 Nov. 2003).

"The SANS Security Policy Project". URL: http://www.sans.org/resources/policies/, (12 Dec. 2003).

"Validated Product List (byType)". The Common Criteria Evaluation and Validation Scheme. 23 Nov. 2003. URL: http://niap.nist.gov/cc-scheme/ValidatedProducts.html#def-firewalls, (23 Nov. 2003).

"Which Technology Decision Triangle". Signify. URL: http://www.signify.co.uk/services/cost_conv_security_triange.asp, (23 Nov. 2003).

Williams, Ross. "The Tao of Backup". URL: http://www.taobackup.com, (23 Nov. 2003).

"Windows 2000 Benchmarks", Oct. 2003. URL: http://www.cisecurity.org/bench_win2000.html, (14 Dec. 2003).

Wingert, Christopher and Mullaguru Naidu. "CDMA 1xRTT Security Overview". Aug. 2002. URL: http://www.cdg.org/technology/cdma_technology/white_papers/cdma_1x_security_overview.pdf, (19 Nov. 2003).

"Wireless Data". URL: http://www.modem.com/glossary/glos22.html, (20 Nov. 2003).

"WS_FTP Server". URL: http://www.ipswitch.com/products/ws_ftp-server/whatsnew.html, (23 Nov. 2003).

"ZENworks for Desktops", URL: http://www.novell.com/products/zenworks/desktops/, (10 Dec. 2003).