Global Information Assurance Certification Paper

Table of Contents 1
Robert_Rounsavall_GCWN.doc 2

Windows Security Challenge
Allowing vendors in to mission critical systems for remote maintenance and administration

GIAC Certified Windows Security Administrator (GCWN)
Practical Assignment Version 5.0 Option 1

Abstract

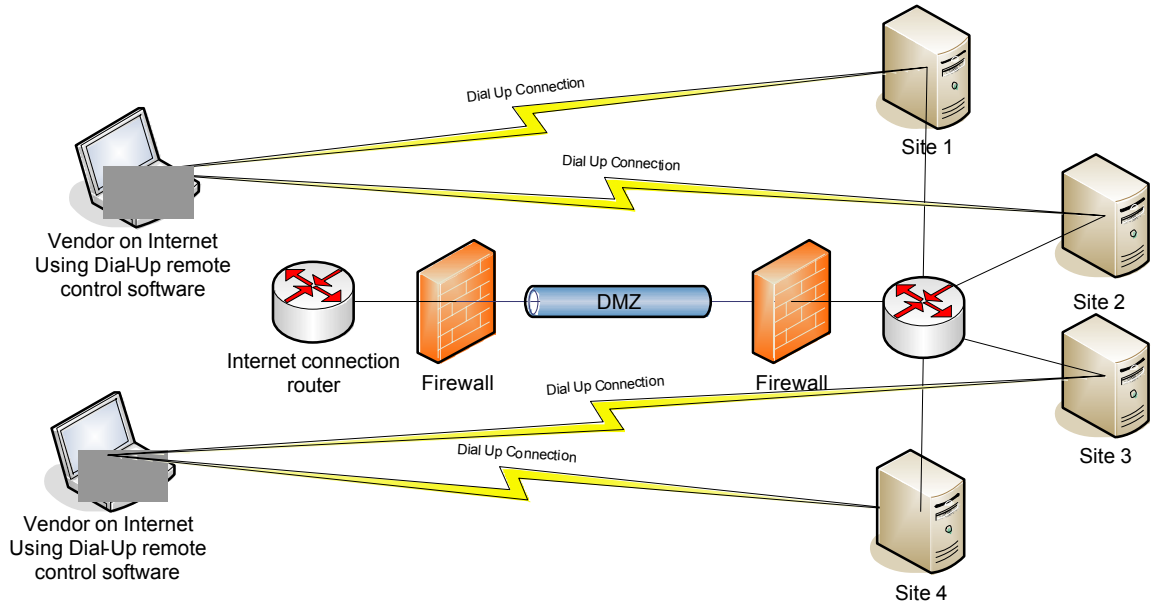
A major Windows security issue today is an extremely common one, and one that there are no real easy or good answers to. How do you allow vendors to securely access your internal networks for remote maintenance and administration? Just the words remote administration and control bring security administrators to their knees and keep them awake at night. This is because of the combination of phrases here, the first being "remote administration" and the second one being "vendor". Any good security administrator knows that you never let your employees use remote administration software to get into computers to work or to fix servers in the middle of the night, much less a vendor. Someone would have to give most of them some sort of mind altering illegal substance to get them to allow such a thing.

Let's assume your company has a manufacturing facility, or several of them on a large corporate WAN. In those manufacturing facilities there are machines that make things that keep you in business, such as computer chips, or parts for airplanes, or whatever it may be. These machines all happen to be controlled by Windows PCs running some sort of proprietary software. If these machines fail, or something happens to them, you could lose hundreds of thousands of dollars in revenue if you can't keep that proprietary software running correctly.

You have just been informed by your CEO that you MUST allow the vendors in remotely to service the machines, and it's your job to find a secure solution for remote access. They must be allowed into the internal network because they are a small office in New York, and your company has facilities all over the country. In situations where their proprietary software fails, they will need access instantly to fix the problem. After grumbling a few things under your breath about proprietary software, and the fact that the CEO was an idiot for buying that brand of machines in the first place, you decide its time to get to work.

Part 1: Solving a Windows Problem

You have concluded that this is not a convenience issue because you have no choice but to let the vendors in remotely. The issue cannot be solved by doing anything locally. Hiring and training staff on this software is not an option, and typically the computers are located in physically secure areas where most employees don't have access, and especially not vendors. If you do nothing, your CEO is going to listen to the vendor and put a modem at each site, and have the same username and password on each one so the vendors can dial in whenever they want. If you sit back and do nothing, the situation might look something like the following diagram:



In the above scenario, the un-trusted vendors are simply bypassing every security measure that you have put in place. They are dialing directly into machines in different locations, and preparing to put you into a state of panic. You have taken precious time and care to put in place a patch management system, and your antivirus updates are handled with care, but now you are just open to machines that you have no idea what is installed on them. As you start thinking about how to take care of this problem, a couple of products and solutions come to mind that can address this problem, and securely allow your vendors to come into the network and administer and troubleshoot these machines.

The ideal tool would be a tool that gives the vendor secure access to the internal desktop without bypassing the firewall. It would also be easy for the vendor to understand and configure. Finally it would not do what a VPN does and give someone out in the un-trusted world an internal network address.

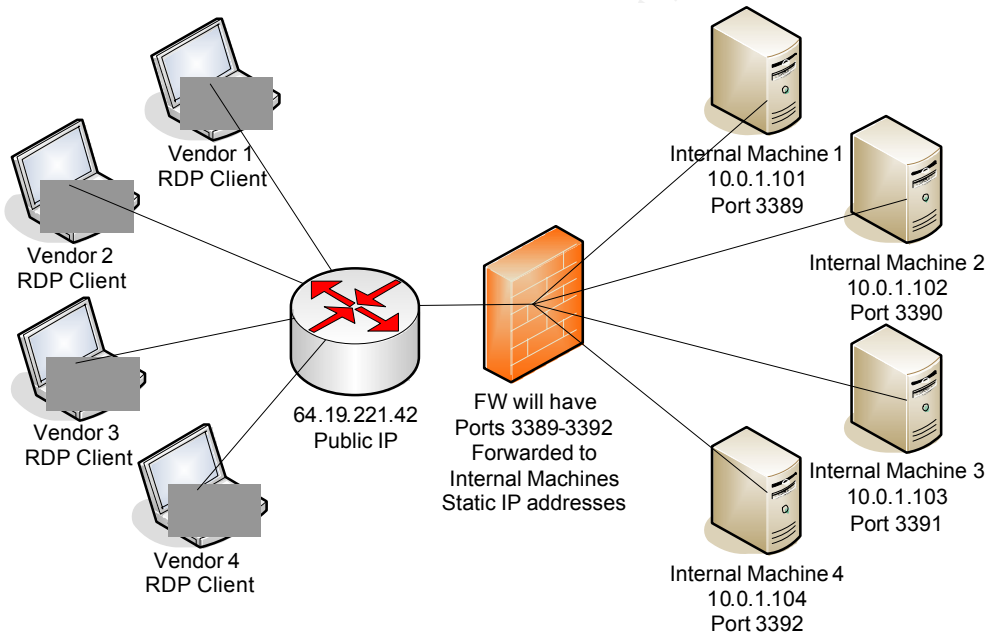
You have decided that you want to use a 3rd party remote control product to administer the machines, but your CIO heard that there was a built in Microsoft Remote Control that would do the same thing. You have decided to evaluate Microsoft Remote Desktop and NetOp Remote Control based on internet research, product reviews, computer security tradeshows such as SANS, RSA, and GOVSEC as well as recommendations from several co-workers.

Part 2: Product Evaluation

Product 1: Microsoft Remote Desktop. Microsoft Remote Desktop[1] is a Microsoft built-in product that comes with Windows XP Professional. It allows a Terminal Server type connection to a remote PC for system administration and

maintenance. On a Windows XP PC, this access can be enabled by right clicking **My Computer, Properties, Remote**. Put a check in the box that says **"Allow users to connect remotely to this computer"**. At this point, you can add a username and password for each user who wishes to connect to this computer. This means that a local user account has to be created for each vendor, or you could do what smart security people don't do and create a single account for all your vendors to use. This will throw all auditing capabilities out the window.

Now that you have enabled the Remote Desktop, and created an account for each of your vendors, here is where the challenge comes in again. How do you safely and securely let them into your network? If they already are in your network this is not a problem, but with Remote Desktop, in order to connect over the Internet, you either need a VPN, or it will be necessary to open and forward many different ports on your firewall. Your company does not allow external VPN connections, especially from un-trusted vendors, so you will have to set it up some different way. The following diagram shows how this can be done with Remote Desktop.

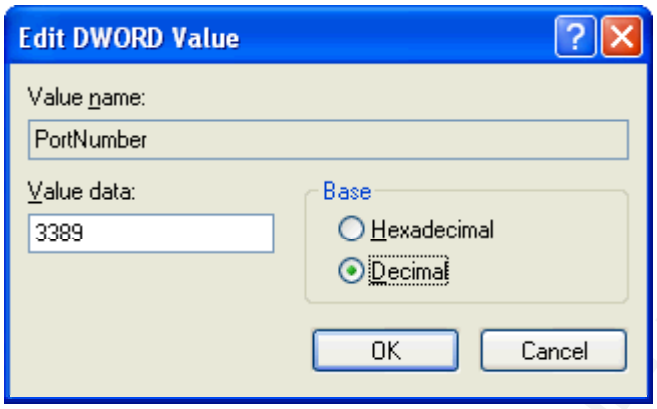


The above scenario makes it somewhat easy on the vendor, because all they have to do is have the Remote Desktop Client, an account on the internal machine, and know the public IP address and port number. All you had to do was assign a static IP address to each internal machine, assign a different port number for the Remote Desktop Connection, and forward ports in your firewall or firewalls.

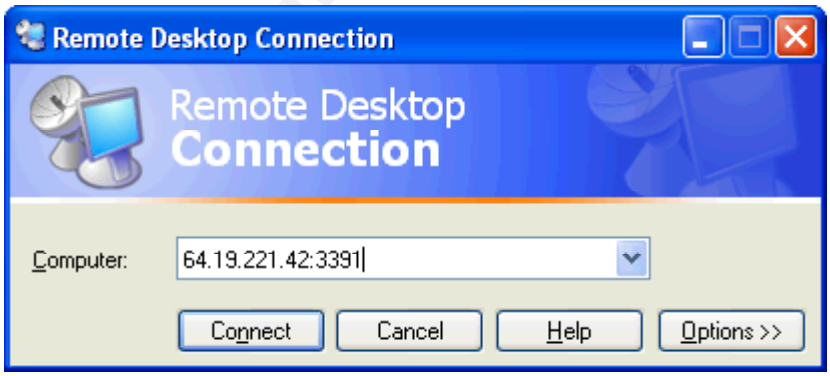
Changing the port number on the internal machines can be done in the following registry key:[2]

\HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp.

Just double click on the PortNumber value to change the default port number. The window is shown below:



Now that you have enabled the connections, and changed port numbers in order to connect to different machines, what does the vendor have to do? Going back to the above diagram, lets assume vendor 1 wants to connect to machine 3. All they have to do is fire up their remote desktop connection by clicking **Start > All Programs > Accessories > Communication > Remote Desktop Connection.** The user then types in the IP address and the port number of machine 3, and they are connected and prompted for their Username and Password. After typing that in, they are at the desktop of the remote machine, and can perform whatever maintenance is necessary to get the job done.



This looks somewhat simple and straight forward, and might work if you only have a few machines that need to be connected to, and one firewall, but what happens when these machines are behind several layers of firewalls, and there

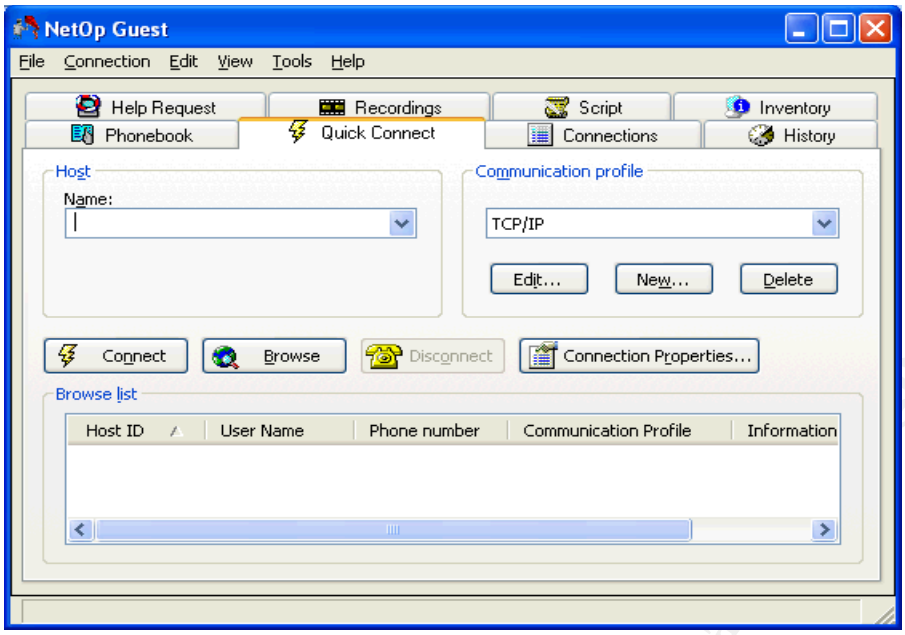
are many of them at each location on the corporate WAN? This solution also will not work if your machines are anything other than Windows XP Professional, Windows 2000 Server, or Windows 2003 Server. The administrative overhead can outweigh the benefit of making it easy on the vendor. There are a few reasons that companies and systems administrators implement solutions like this. The company name might not be Wal-Mart, or Coca-Cola, and therefore does not have the sheer financial power to tell the vendor that they absolutely must install the VPN client software of its choosing, or the company might have a security policy that says absolutely no VPN connections are allowed, especially for outside vendors. Everyone has Remote Desktop, or can easily install the software. In summary, this solution would only be realistic in smaller, Windows XP only environments where legacy machines are not used.

Product 2: NetOp Remote Control. NetOp Remote Control[3] is an enterprise wide remote control product. Similar products in this category are PCAnywhere[4] from Symantec, and NetSupport Manager[5]. With this product an administrator can connect to a distant PC, and have keyboard, video, and mouse control of that particular machine. CrossTec Corporation is the North American distributor for NetOp Remote Control. Please see the following URLs for more information:

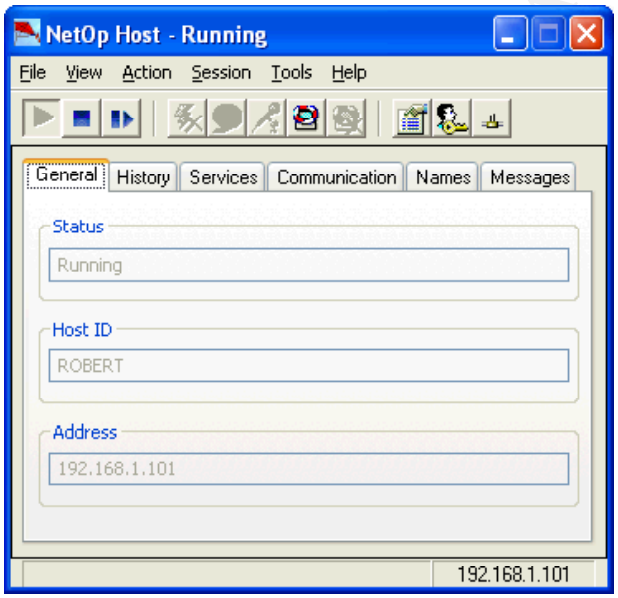
www.crossteccorp.com Contains general information.
www.crossteccorp.com/tryit Contains form to request a trial version.
www.crossteccorp.com/whitepapers Contains implementation guides and security whitepapers.

There are several pieces that we are going to look at with NetOp Remote Control and they are defined below.

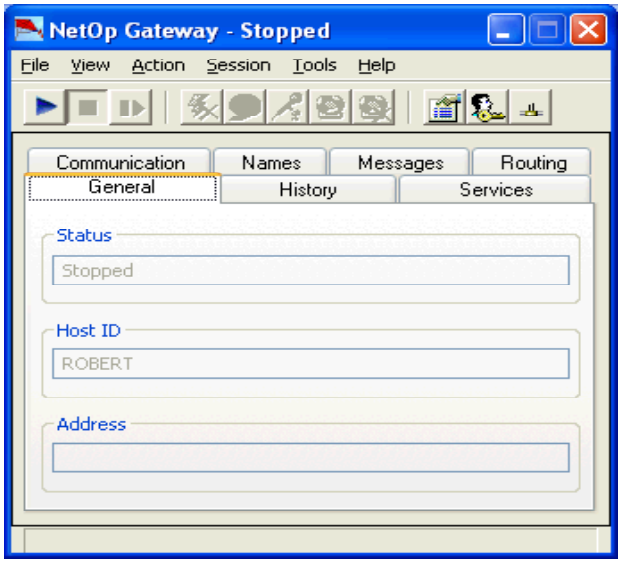
NetOp Guest: Referred to as just "Guest" for the remainder of this paper. The Guest is the piece of software that is used to connect to the distant PC.



NetOp Host: Referred to as "Host" for the rest of this paper. This is the piece of software that will reside on the machine that the vendor needs to access for remote administration and maintenance. If someone wants to connect to a remote machine, at minimum they need a Guest and a Host.

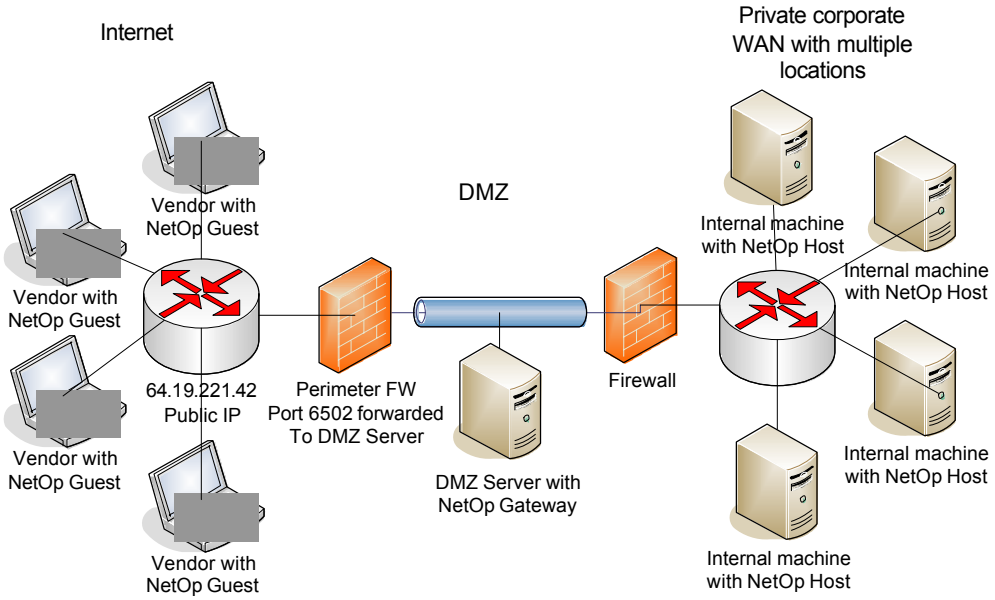


NetOp Gateway: The Gateway is a modified NetOp Host that acts as a router for Remote Control traffic and sessions. It also allows multiple remote control connections through a single port, which eliminates the need to have multiple ports open to the Internet. The Gateway is installed on a machine with a static IP, and a port is forwarded from the Router/Firewall to that machine. Once configured, a Guest can connect to all the Hosts on the internal network.



NetOp Remote Control works on every Windows platform from 3.1 to 2003 Server as well as Linux and Solaris, so if there are legacy machines on the internal network, a vendor can still connect to them through the NetOp Gateway from the Internet. NetOp Remote Control also offers a high level of encryption (256 bit AES) and the ability to log, and or record each remote control session that takes place, and that is extremely important when outsiders are accessing your most important internal machines. As far as installation and deployment, NetOp Hosts can be deployed in several ways. They can be deployed individually, just like each remote desktop client, or they can be deployed with a utility called the NetOp Deployment Utility across a LAN or WAN. This requires administrative privileges, and assumes the OS is Windows NT or later and the ability to connect remotely to a network drive. This can be tested using the NET USE command.

The following diagram details what a typical NetOp Remote Control solution looks like:



Vendors have the NetOp Guest, they connect to the NetOp Host through the NetOp Gateway, and everything works nice and smooth, and fast and secure. Well that is at least the thought or hope. There is an issue here, which brings up the same issue as when you are trying to force vendors to use a VPN. How do you get them to properly install the software? Are you going to support them? Do you trust them to properly install the software?

Remote Desktop is convenient for the Vendor. They have to do minimal work, but the systems administrator has to do a ton of internal configuration as well as open up multiple ports on the firewall. At this time, it is not realistic to think that in most situations, internal machines will all be running Windows XP Professional, especially when these machines are out on manufacturing floors and have been in production for some time.

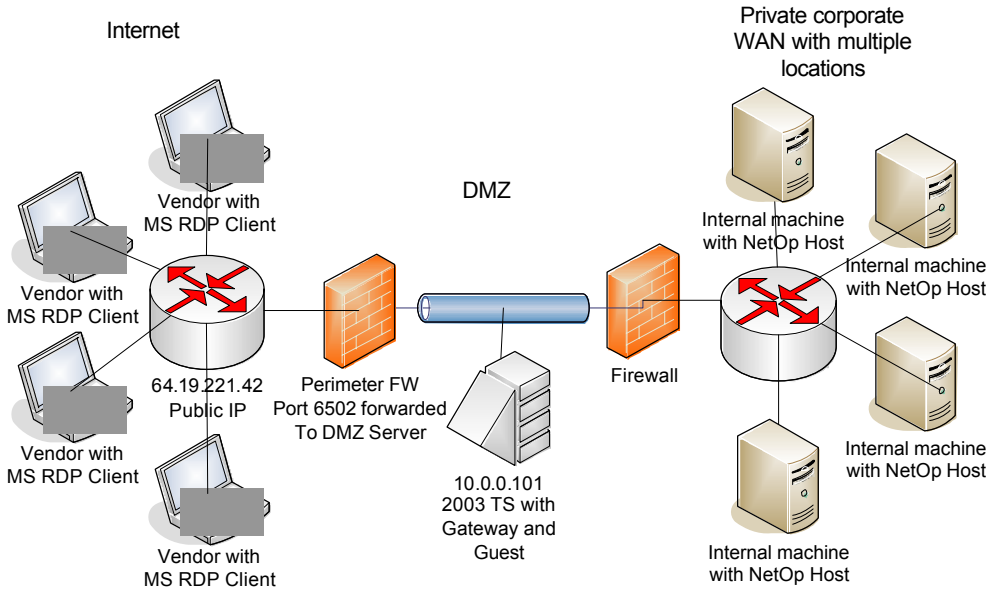
NetOp Remote Control will meet the needs for other operating systems, as well as the ability to log and record which vendor is accessing what machine, and it doesn't open up multiple ports, however it falls short of the requirement of making it easy for the vendor to use because it requires that the vendors install a 3rd party remote control product.

Proposed solution:

After testing each product and finding that they both came up short in a couple of areas, a combination of the two products was decided on. It would be nice to have the ease of use of Remote Desktop, yet the platform support and auditing capabilities of NetOp Remote Control. It was found that NetOp Remote Control works quite well on Microsoft Terminal Services, and the NetOp Gateway would let Terminal Service clients use NetOp Remote Control to connect to machines on the internal network and not in the terminal session. Logging could be set up, and the solution could be hardened to a point that gave a reasonable level of

comfort with the risk of letting the vendors in. The solution works as follows:

A secure, internet facing terminal server would be installed in the DMZ. The NetOp Guest and Gateway program will be installed on the Terminal Server. The NetOp Hosts will be installed on the internal machines. The vendors will use Remote Desktop to connect to the secure terminal server. They will then use NetOp to connect only to the machines in which they are authorized. All remote control activity will be logged giving the security administrator the ability to audit each remote control session. The proposed solution is shown in the diagram below:



Part 3: Implementation Guide

Step 1: Install the Terminal Server
Step 2: Install the NetOp Gateway and Guest on the Terminal Server
Step 3: Configure the NetOp Gateway on the Terminal Server
Step 4: Configure the Host on the internal machine
Step 5: Configure the NetOp Guest on the Terminal Server
Step 6: Test the solution

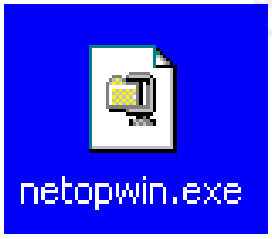
Step 1. Install and harden the Terminal Server: From the diagram above, you can see that we decided to put a terminal server in the DMZ which will be accessed from the internet. After much searching and testing, I decided that it was too much of a pain to try and use the local security policy in order to harden

the server. If I harden it as much as I want, I will lock out the administrative account, and won't be able to do the things that I want to with the machine. The other thought is to have an internal domain controller and make the server a member server in the domain, and use GPOs to harden the server as well. Trying to do this basically eliminates the DMZ, and as was so nicely put in one Microsoft article "Turns your firewall into Swiss cheese"[6].
One might as well just put the server on the internal network. This is perfect justification for a DMZ specifically for this solution and a domain controller with the sole purpose of hardening the terminal server or servers. This domain has no interaction or connection to the internal network. At this point I configured a Windows 2003 Server to act as my DC. I then created a hardened OU for my Terminal Server computer and users, and then enabled loop back processing on the GPO so that anything that connects to that server will have the settings applied. For simplified administration, I can simply move the computer out of the hardened OU and into a different OU to make any changes that need to be made. By doing this, none of the users can log onto the terminal server from the outside while maintenance is performed. When finished, I simply put it back into the hardened OU and then I am ready to roll!

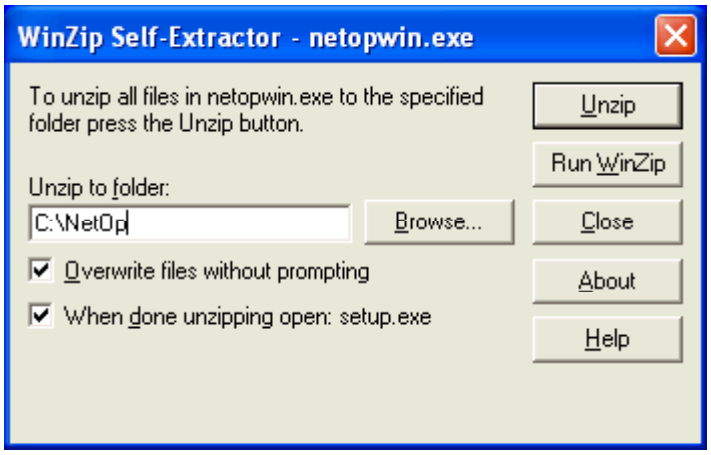
Step 2. Install the NetOp Guest and Gateway on the Terminal Server:

An evaluation version of NetOp Remote Control including all of the modules previously mentioned can be obtained from www.NetOpUSA.com The NetOp Gateway is a modified NetOp Host which will allow the vendor to get from the terminal session to the internal network by routing NetOp Remote Control traffic. Once installed and configured, the Vendors will not know that the Gateway is running. They will only interact with the Guest program which allows them to connect to a Host program running on the internal machine that they need access to.

To install the Guest and Gateway, download the software from the vendor. The file is called netopwin.exe.



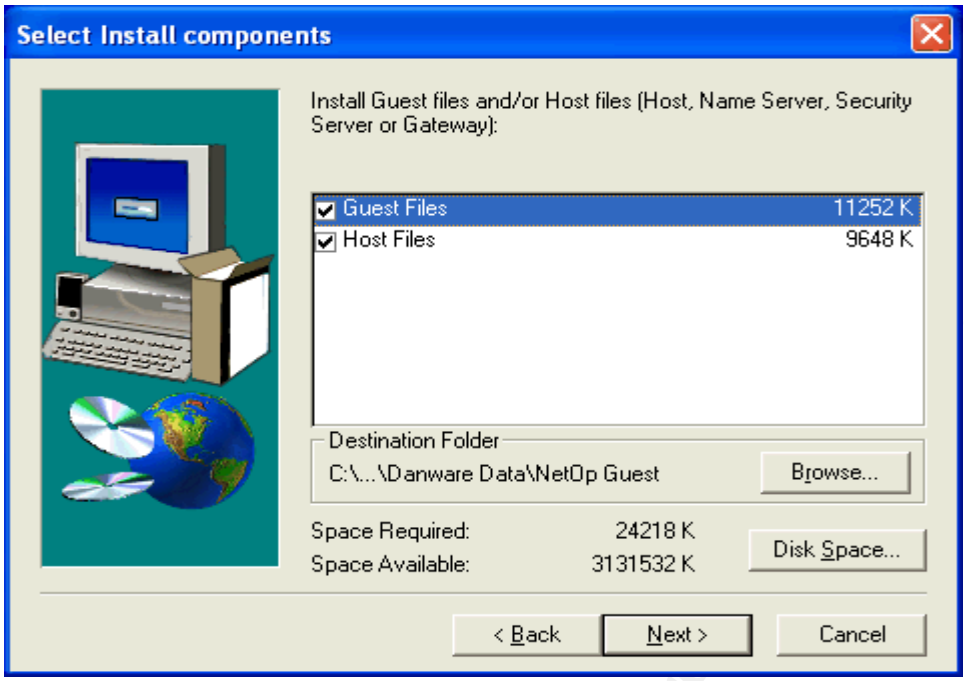
Double click the file and you will be prompted with the following window:



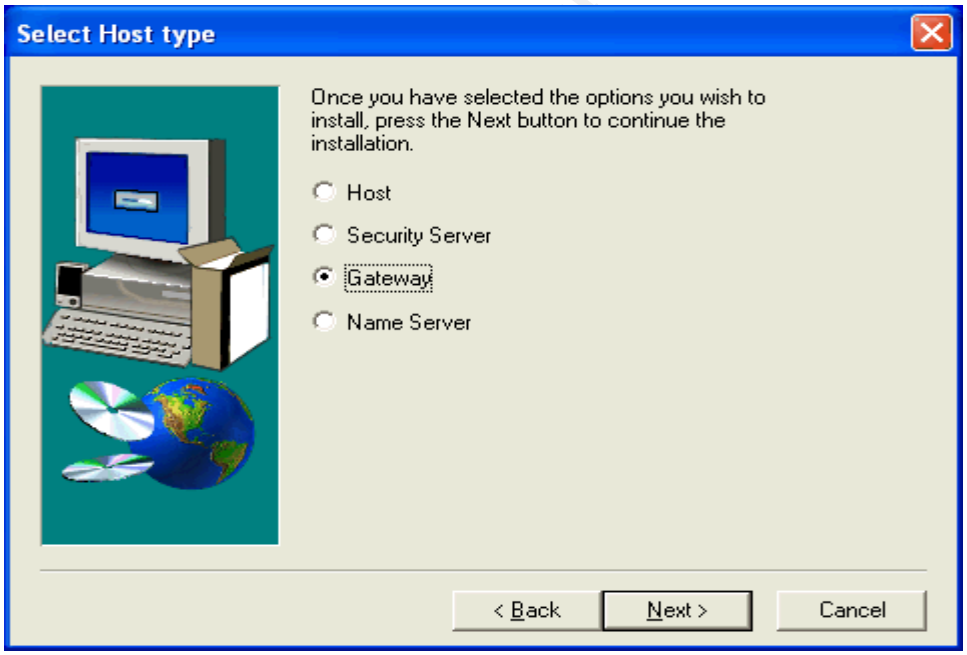
By default, the files are extracted to a temporary folder. You should create a folder in the location of your choosing and then click Unzip. You will then be prompted for the password supplied by the vendor.

The setup will automatically launch after the files are extracted and you click Ok.

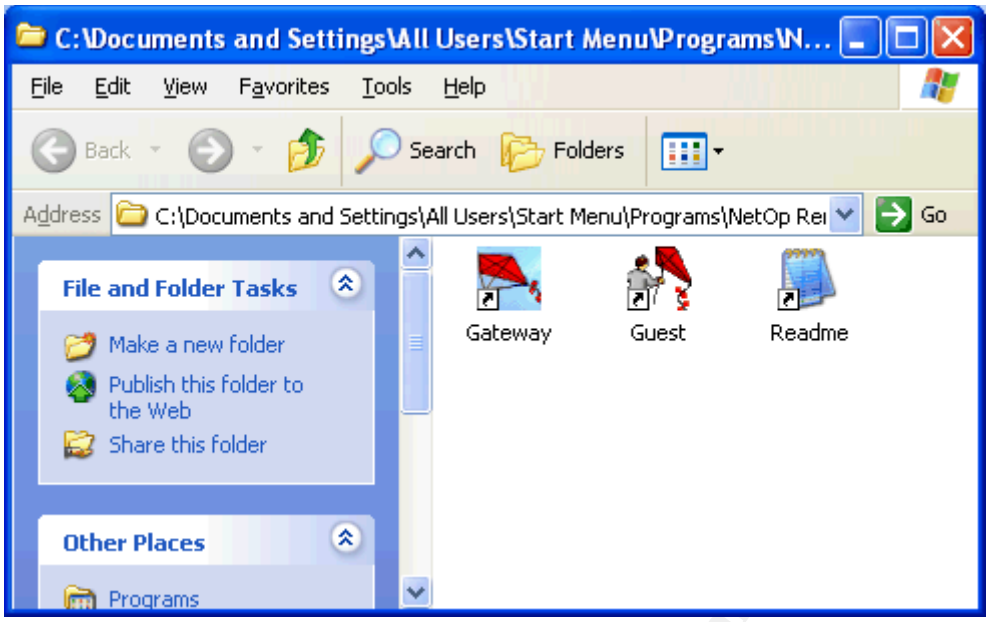
Click Next until you arrive at the following window:



By default both Guest and Host are selected. This is ok since we are installing both of them on our Terminal Server. Click Next.



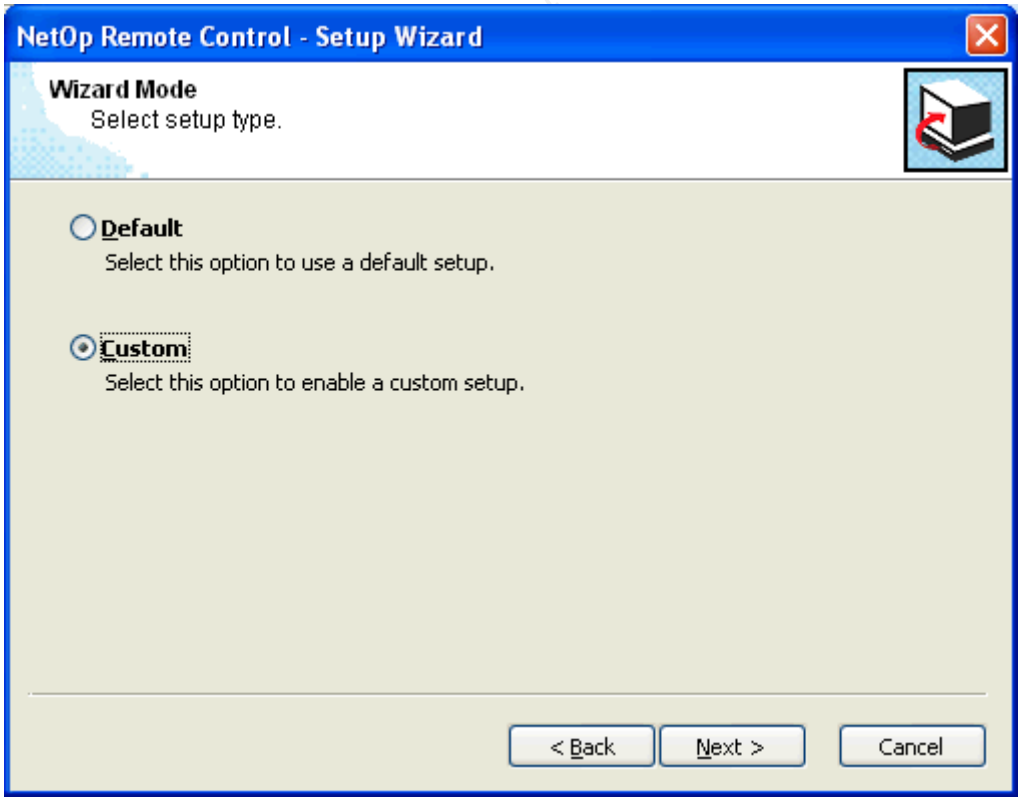
Select Gateway instead of Host since we want to install the Gateway.
Click Next all the way through the rest of the installation.
Upon completion, you will be presented with the following folder with the Guest and Gateway icons, as well as a readme. The readme file contains information about NetOp including each file associated with NetOp and its purpose.



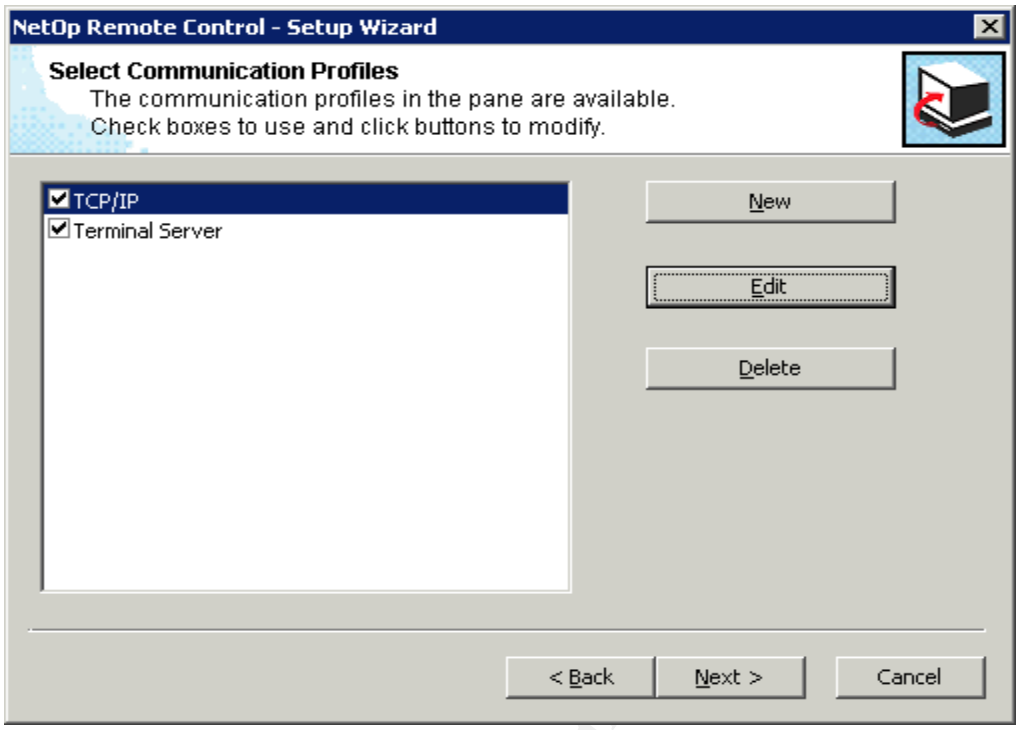
Double Click the Gateway icon to launch the Gateway and the SetUp Wizard.

Step 3: Configure the Gateway on the Terminal Server

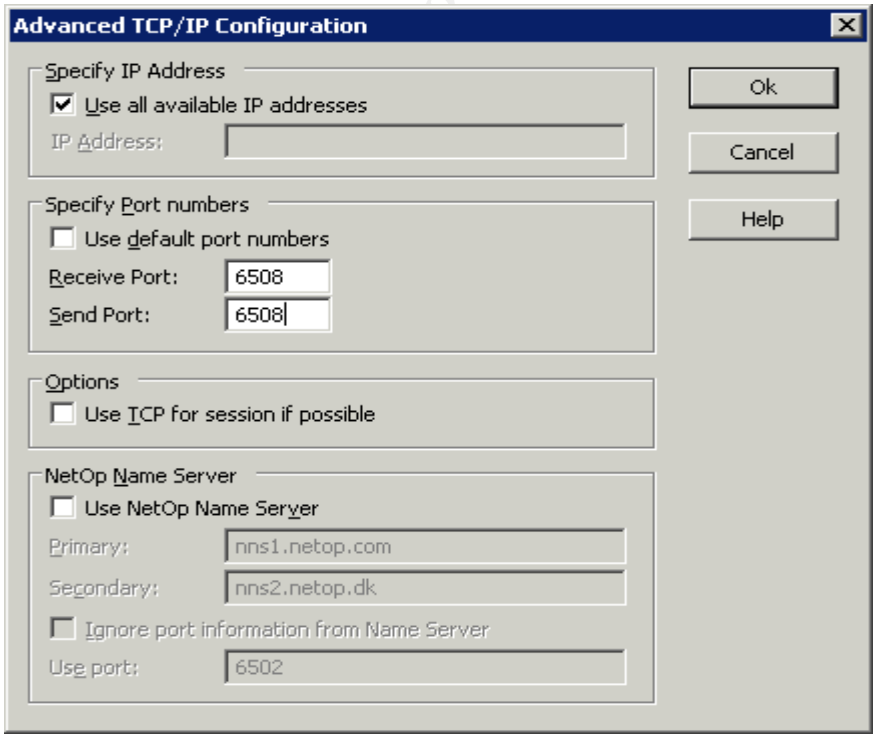
When starting the Host after installation, a setup wizard will be launched.



Click the custom button to show all of the communication profiles.

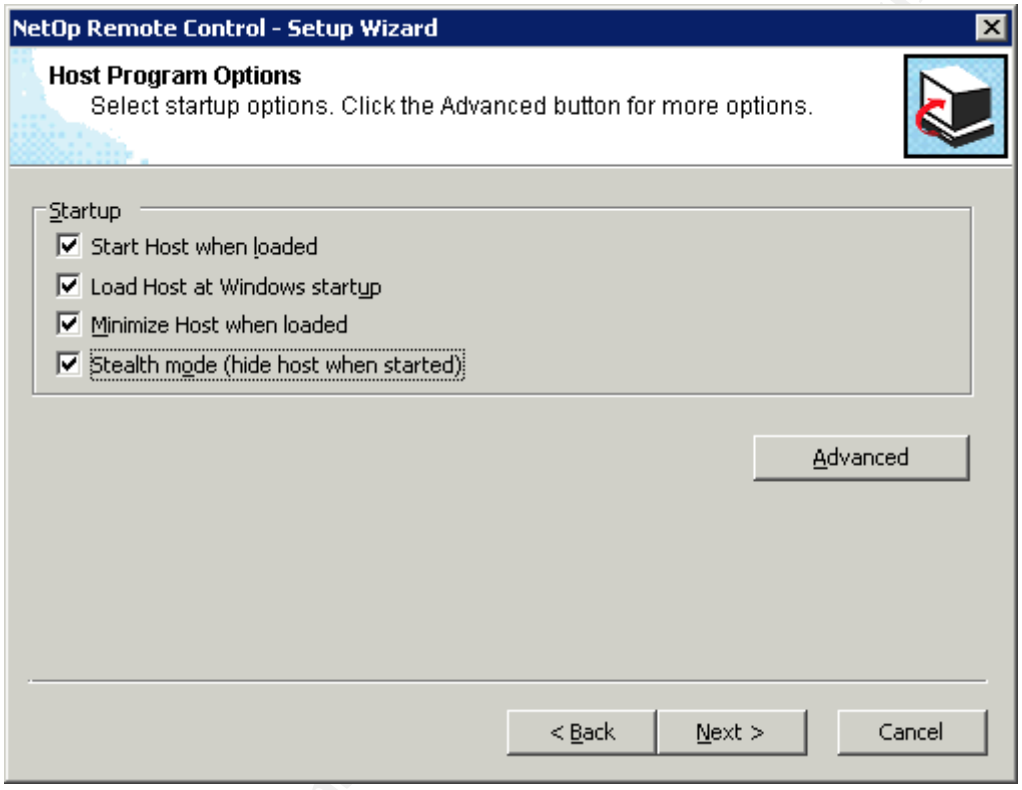


Delete every communication profile except for **TCP/IP** and **Terminal Server**.
Click **TCP/IP**, and then click **Edit**.
Click the **Advanced** button to show the following window:



The default NetOp Port is 6502. Tools like NMAP know that NetOp runs on port 6502.

Uncheck the use Default port number box and change the port number to a different port number. We will use 6508 for the purpose of this paper.
Uncheck Use TCP for session if possible.
Click **OK** twice to exit the menu, then click **Next**.

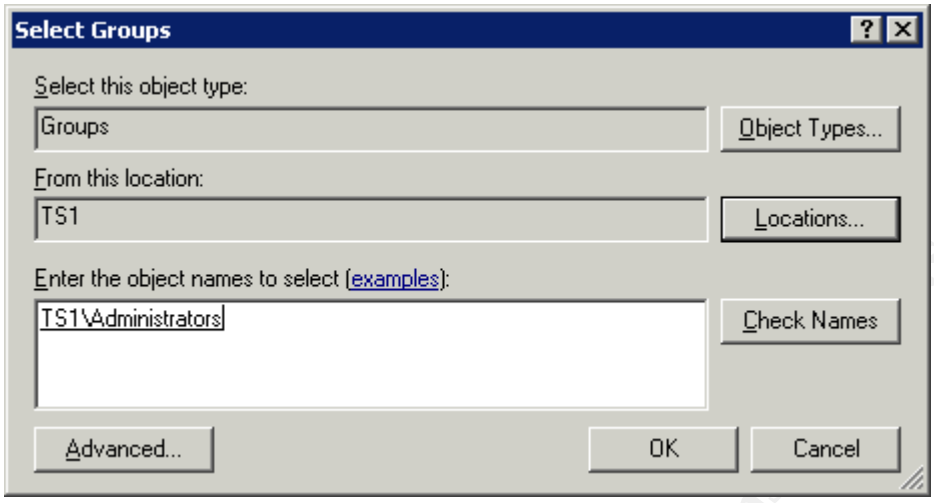


By default the first three options are selected. Put a check in the bottom box called **Stealth mode**. This make the program run invisible, so users logging on to the local system will not see NetOp running.
Click **Next**

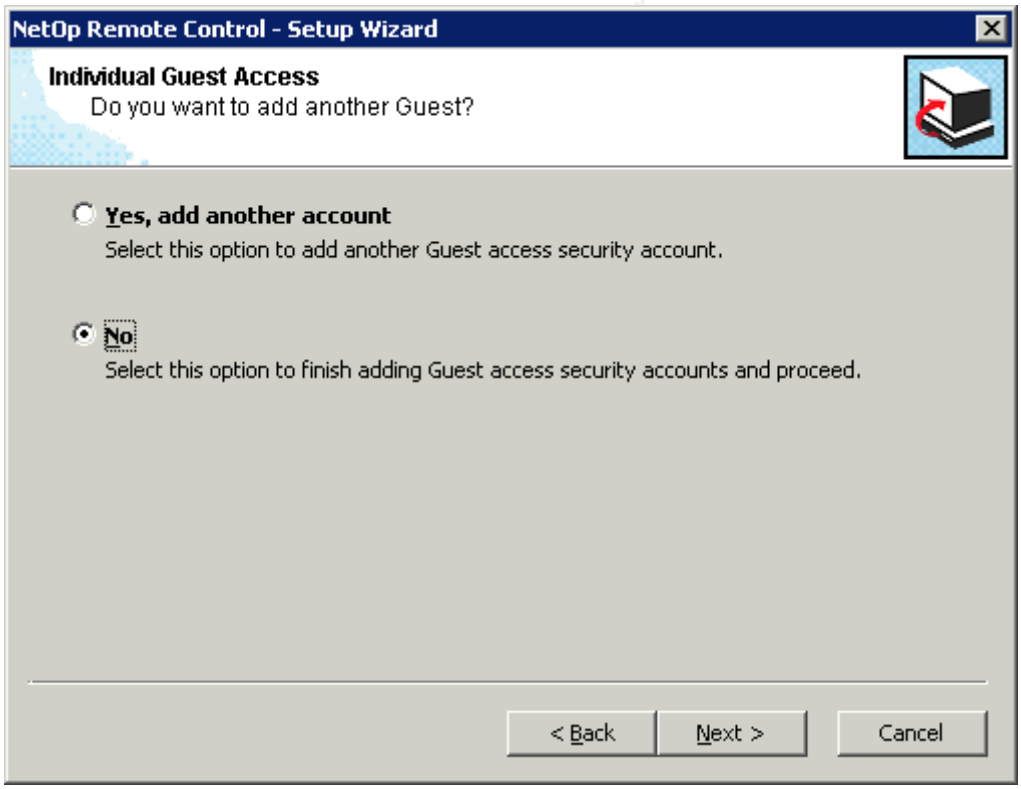
Click **Use Windows Security Management**, then click **Next**.

Click **Yes, add a Windows group**, then click **Next**.

Click **Locations** and select the local computer, TS1 in this case.



Type in **administrators**, and click **Check Names**.
Click **Ok** to return to the wizard.



Click **No**, then **Next**, then click **Finish**.

By installing the Gateway on the terminal server, and enabling the port 6508, we

have set it up so that we can connect from the terminal session with the Guest to a host that is not in a terminal session via port 6508. We now just need to open port 6508 on the interior firewall to connect to machines on the internal network. Next we are going to set up the hosts on the internal network

Step 5: Install the NetOp Hosts on the internal machines.
Now that we have the Gateway and Guests installed on the Terminal Server it is time to install NetOp Hosts on the internal machines. NetOp supports all Windows Operating Systems from 3.1 to 2k3 Server. For the purpose of this paper, we will assume that Windows NT is being used. Remember, we can't upgrade because our CEO bought that custom application 5 years ago and it is now not used or supported by normal means. Before the Host is installed, it is important that a local account for the vendors be set up on the machine with permission only to do what they need to do. For example, if they need to just maintain an application as a user, then create a local user account for them. Each vendor can have their own unique username and password, which will help in determining who is connected when. Many organizations have a single username and password that all of their vendors use to connect to the same machines. Once the accounts are created, the Hosts can be installed.

The install for the Host on the internal machine is almost exactly the same as the Gateway. It is very simple. Unzip the evaluation files, and run through the installation by clicking Next. This time, uncheck the part where it says to install the Guest. Everything else will remain with defaults.

After the installation, when the Host program is launched, you will get the same setup wizard that came up with the NetOp Gateway. All of the configuration that can be done with the wizard can also be done from the Tools menu on the Host but we will stick with the wizard for now. Do the following when the wizard launches.

Click **Next**, then click **Custom**, then **Next** again.

NOTE: This opens the same window that would open when clicking **Tools, Communication Profiles** if not in the setup wizard.

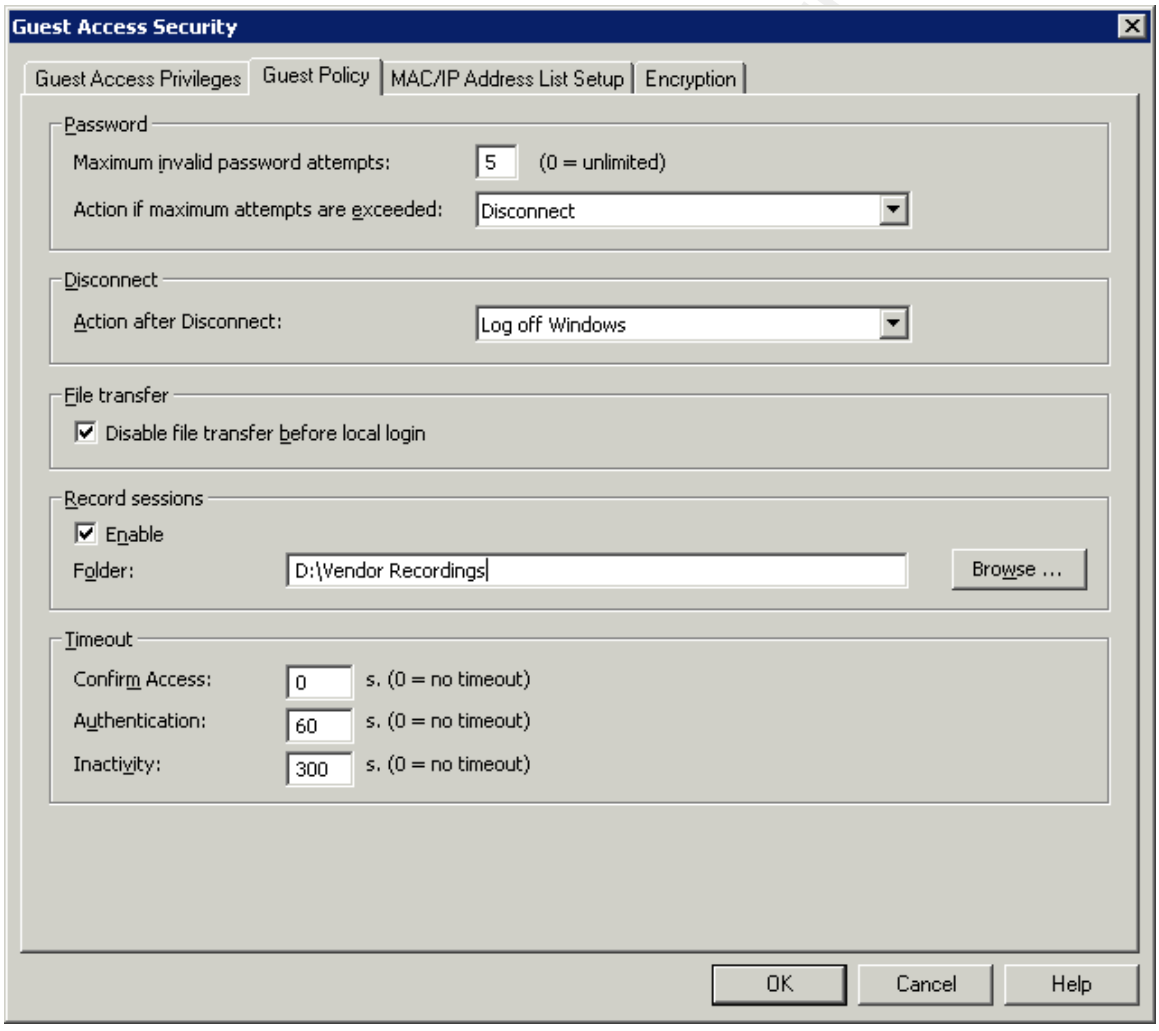
Delete all except **TCP/IP** which is checked. Click **Edit** then **Advanced** on TCP/IP.
Uncheck **Use default port numbers** and change to **6508**.
Uncheck **Use TCP for session if possible**. Click OK twice to return to the wizard, then click **Next**.
Click **Stealth mode (hide host when started)** and click **Advanced**.

NOTE: This opens the same window that would open when clicking **Tools**, then **Program Options** if not using the setup wizard.

Uncheck the **Public Host name** and click **OK**. Click **Next**.
Click on **Windows Security Management** and click **Configure**.

NOTE: This opens the same window that would open when clicking **Tools**, then **Guest Access Security** if not using the setup wizard.

Click **Add User**, and add your vendor user accounts to the Hosts.
Click the **Guest Policy tab**.



Set the maximum password attempts to **5**.
Check **Disable file transfer before local login**.
Check **Enable** record sessions.
Create a folder where you can store local recordings, and click the **Browse** button to locate the folder. Recordings are about 1 mb per minute of activity.

Depending on the frequency of expected connections and how long vendors will connect determine how often you need to audit or clear out the folder, but you will have a recording of every single thing that the vendor does (or attempts to do!) while logged into the machine.
Set the **Authentication** to **60** seconds to time out. There is no reason that authentication should take more than 60 seconds.
Set the **Inactivity** to **300** seconds (5 minutes). This will disconnect the remote control session if there is inactivity for that long.

Click the **Encryption** Tab.
Uncheck everything except for **Very High**. This forces 256 bit AES encryption.
Selecting **Very High** and clicking **Details** shows the details of the Encryption as shown in the screenshot below.

Click **OK** to close the above window and **OK** again to return to the wizard.

Click **Next,** then Click **No** and proceed without adding a Windows user account and click **Next**, then **Finish**.

Your Host is now configured with your vendor's user accounts and ready to go. These same steps will be taken on each internal machine that will be set up for vendor access. All of these settings can be pre-configured using the NetOp Deployment Utility and deployed to many machines as well.

Step 5. Configure the NetOp Guest on the Terminal Server.
We installed the Guest on the Terminal Server earlier, but never launched it. There are a couple of things that we want to do prior to this to make life a bit

easier for us and the vendors. Typically the Guest configuration files are stored in each user profile, so each Vendor has their own configuration. The only problem with that is that as each vendor logged in to the Terminal Server, they would have to launch the Guest and run the setup wizard and configure the Guest. We are going to make it so that when they authenticate and open up a Terminal Server session, they have an icon on their desktop to connect to their machine. Take the following steps before logging launching the Guest program.

Log in to the terminal server and create a local folder called NetOp. It is always better to put these types of folders somewhere other than the system drive, so we will create a folder on another drive besides the system drive. This is where the configuration files will be stored.

Now we must edit a configuration file so that the Guest knows to create and look for the configuration files in that folder.

Locate the **NetOp.ini** folder in the system drive (C:\Windows)

Add the following entries to the **[GUEST]** section.

[GUEST]
DataPath=D:\NetOp
DisableLocalFileTransfer=1

The **DataPath=** entry obviously points to that shared folder.
The **DisableLocalFileTransfer=** entry disables a feature on the Guest which allows a user to view files on the local hard drive. The last thing we want vendors to do is try to explore files on our local terminal server.

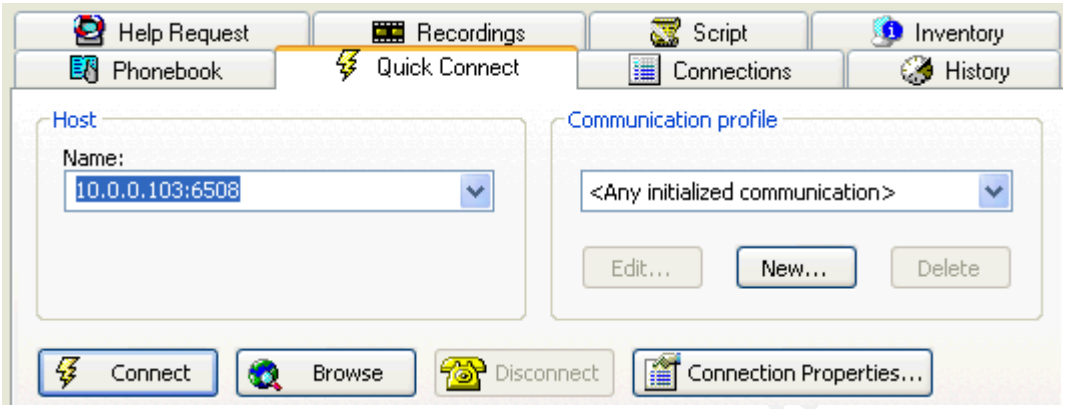
Now that that is configured, open the Guest program by clicking **Start, All Programs, NetOp Remote Control, Guest**. The setup wizard will launch the first time the program is run. Keep all the default setting and click **Next** all the way through the wizard.

Because we are running the Guest on a Terminal Server, we need to make a small change to the communication profile.

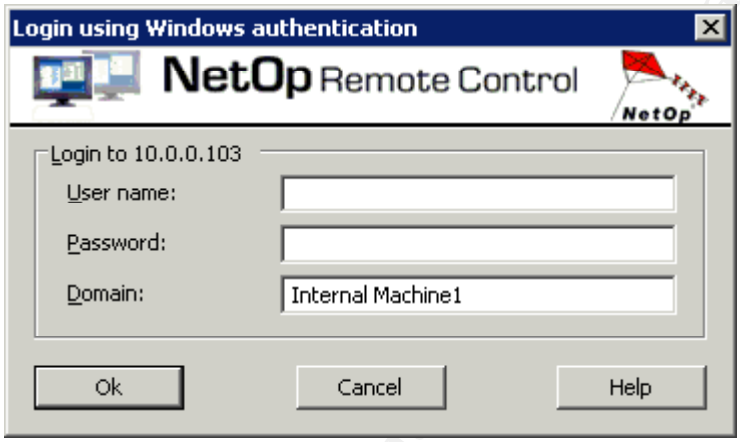
Click **Tools**, **then Communication profiles** on the Guest program.
Put a check mark in the box next to **Terminal Services**.
Delete all other communication profiles.
Click **Ok**, then restart the Guest.

When the Guest comes up, in the **Quick Connect** tab, click the drop down arrow in **Communication profile**, and change it to **<Any initialized communication>**. The first thing we want to do is test and make sure we can

connect to our internal computer from the Guest. Type in the IP address of the internal machine and click the **Connect** button as shown in the screenshot below.



You should get a login prompt as shown below:



At this point you know that the NetOp Host is responding to you. Enter the name and password for one of your vendor accounts start a remote control session.

I will point out a few of the relevant buttons on the above remote control session window.

 These two small locks indicate that the communication is using the Very High encryption, which is what we wanted.

 This icon is the Disconnect icon. Click it to disconnect from the remote control session.

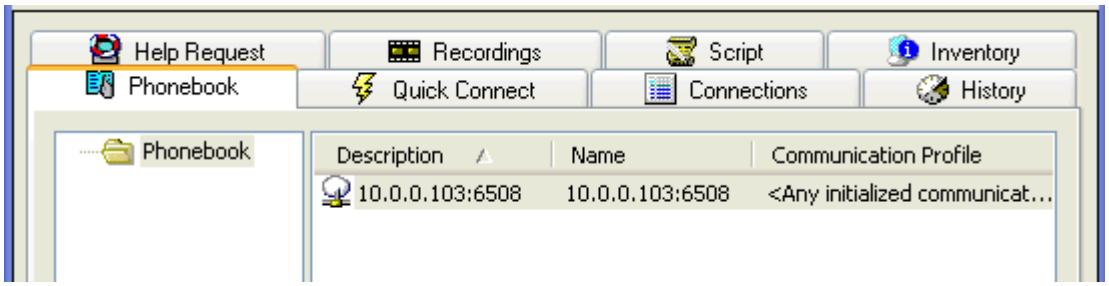
 This button is the send Ctrl+Alt+Del button so you can log into the computer.

 This icon lets you go from full screen to a Window

Now that we have successfully connected to the internal machine, we are going to make it very clean for the vendor by using a phone book entry.

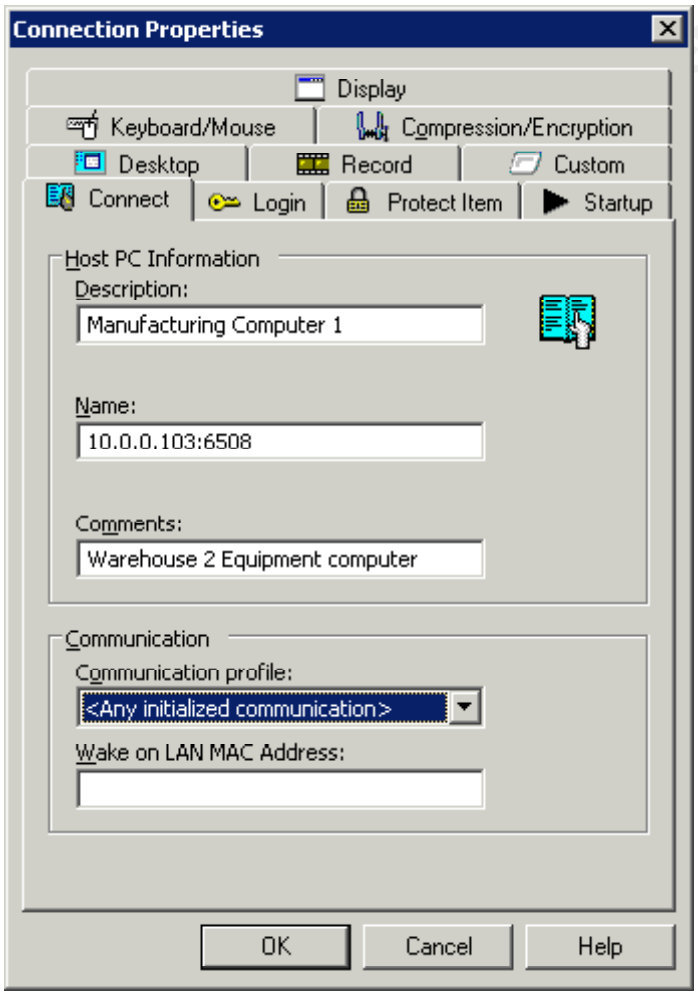
Click the **Disconnect** Icon to end the remote control session.

On the Guest Program, click the **History** tab and you will see the connection that you just made.
Right click the connection, then **Copy** and **Paste** the connection into the **Phonebook** Tab.



Right click the Phonebook entry and click **Connection Properties**. Currently the Description has the IP address. Change this to something that will identify the machine to the vendor, such as Manufacturing 1, or whatever is easily recognizable. If you have several machines, name them accordingly. You can also use the comments field to put something such as location, or anything else you want.

See the screenshot below.



At this time I will cover the other relevant options that are important in the **Connection Properties** window.

Protect Item: Enter a strong password here to protect the phonebook entry. The vendor will not be able to modify any of the settings made in here.

Record: This is the same as the record feature we enabled on the Host security section. By default our recordings will go to a folder called record in where the configuration files are located. In this case they will go to D:\NetOp\Record. If you want to enable this setting, you can place the recordings in another location with a NetOp.ini entry in the **[Guest]** section of **RecordPath=\\SERVERNAME\Share name**. Using this feature, if your vendor is controlling some sort of lift and accidentally makes it drive over and crush your computer out on the manufacturing floor, you still have a recording here on your terminal server. At the same time you still have to remember the space considerations.

Startup: Click the **Full Screen** radio button. This will force the Remote Control session to launch full screen in the terminal server session.
Compression/Encryption: Click the Drop down at the bottom and select **Very High** for **Preferred Encryption Type**.

Click **Ok** to close the phonebook entry.

Double Click your phonebook entry and test the connection again to make sure it works, and then disconnect.

At this point we are almost finished. We now only have a few things to do on the Guest program, then we will set it up so that it will launch automatically for the vendor. On the Guest we will remove all the tabs so that the vendor only sees the Phonebook tab, enable logging, and set up a maintenance password.

Remove all tabs except for the Phonebook tab:
Click **Tools**, then **Program Options**, then the **Layout** tab.
In the **Tab Layout** section, uncheck everything except **Phonebook.**
Click Ok

Doing this will make it so that the vendor has no access to other tabs such as quick connect, inventory, or scripting.

Enable Logging:
Click **Tools**, then **Log Setup**. There are several different ways to log including a **Local Log file, Windows Event Log, NetOp Log Server**, and **SNMP Traps**. For the Windows event log, you can log locally, remotely or both. Depending on your paranoia and how you currently log and audit your network will depend on what you want to do.

For the purpose of this paper I am going to show how to set up a local log to a log file and to the Windows Event Log.

On the **Log Setup Menu**, click **Log Locally**, and **Log to Windows Event Log**. There are tabs for each of these. There are several different types of events that can be logged. All of the events can be viewed from the Log Setup window. I am going to make some suggestions on which ones to log.

Connection events:
Connect to Host
Disconnect Host
Connection lost
User Authenticated

Sesion Events:
Remote Control Started
Remote Control Stopped

Action Events:
Host Rebooted

Security Events:
Password Rejected

Configuration Events:
Local Logging turned on
Local Logging turned off
Local Logging filename changed
Windows Event Logging turned on
Windows Event Logging turned off

Set up the Maintenance Password:
Click **Tools**, then **Maintenance password**, and enter a complex password. This will prevent your vendors from making any configuration changes to the Guest program.

We are now done with the Guest. Time to make it so the Guest program loads automatically for the vendor when they logs in to the terminal session. The easiest way to accomplish this is through your GPO. Enable the following entry:

User Configuration, Administrative Templates, System, Logon, Run these programs at logon.

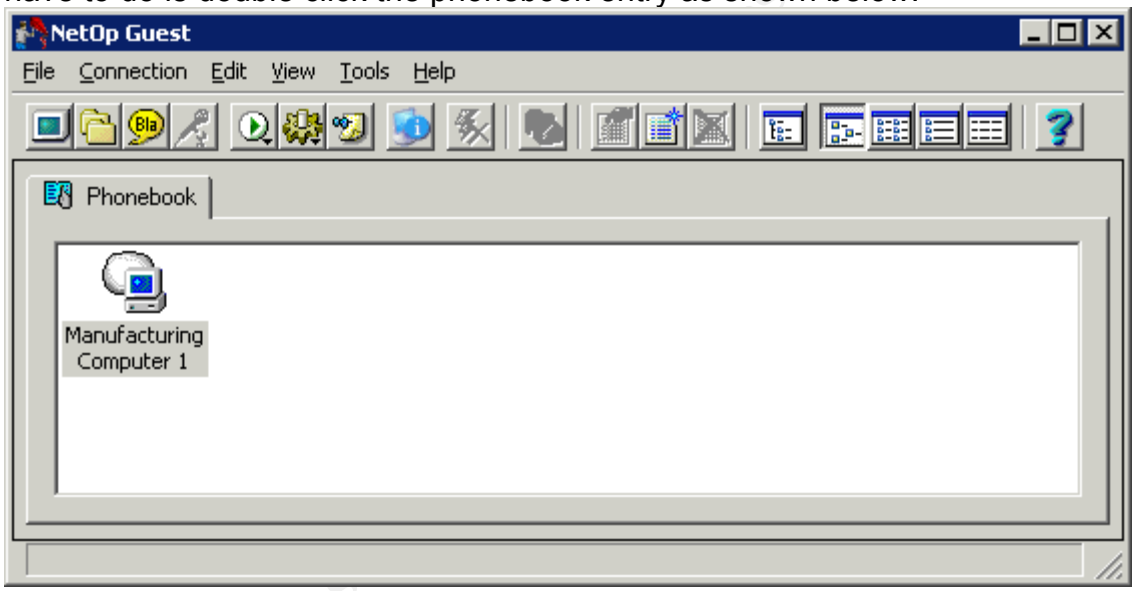
Add the following executable:

C:\Program files\Danware Data\NetOp Remote Control\Guest\Ngstw32.exe.

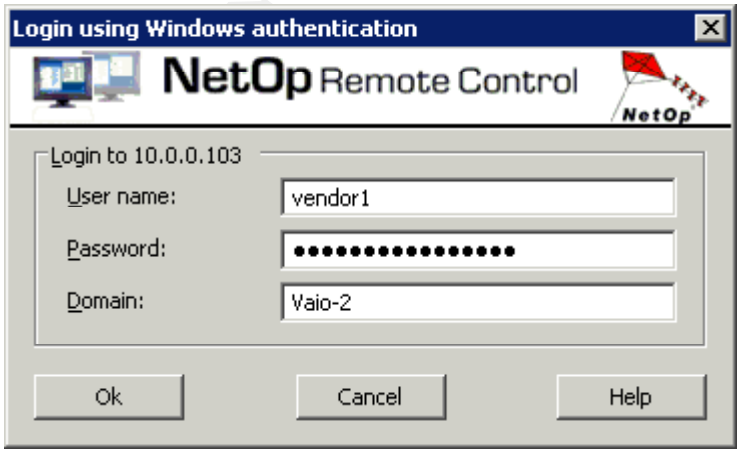
This will cause the Guest program to launch when the vendor logs in to the Terminal Server. At that point they can just double click on their phone book entry, enter their credentials and go to work. They will then be presented with the Windows Login Screen, and they can log in and go to work!

Step 6: Test the Solution

From an external Windows XP machine, fire up your remote desktop connection, and connect to the public IP address. Click **OK** on the warning banner you placed in there that states that all activity may be monitored and recorded, then just enter your Active Directory user credentials to log into the Terminal Server, and the Guest will launch automatically. At this time all you have to do is double click the phonebook entry as shown below:



You will be prompted with your username and password.



After clicking OK, you will be at the full screen of your workstation, and ready to log in and work!

Conclusion:

In this paper we have looked at what companies are currently doing to let their vendors into their network, which is use modems, or remote access programs with no way to audit or log what is going on. They also are using solutions that make it extremely difficult for the vendors or outsiders who need access to the internal network. We looked at different ways to take care of this gaping security hole, as well as give a tolerable ease of use to the vendors. The products that we looked at were Windows Remote Desktop and NetOp Remote Control. We found that both of them had limitations, specifically, Remote Desktop had platform limitations, as well as forcing companies to open up more ports on their firewall than they wanted to. NetOp Remote control, while satisfactory in that it allowed only one port to be opened, was not what we were looking for because we did not have the ability to force the vendor to install the software, and some vendors did not have the technical ability to do so. To solve this problem, we decided to go with a combination of both technologies using the RDP connection on a Terminal Server as a point of entry to the network, then using NetOp to go from the DMZ to the internal machines. This allowed ease of use for the vendor, but also allowed strong authentication via AD on the terminal server and on the local internal machine, as well as the ability to audit, log, and record everything that the vendor did from multiple locations. By implementing this solution, a company can raise their level of security and lower their paranoia about remote control access from outside vendors.

References:

[1] Microsoft. Remote Desktop information.
http://www.microsoft.com/windowsxp/using/mobility/default.mspx

[2] Microsoft HOWTO: Changing the default port in Terminal Services.
http://support.microsoft.com/default.aspx/kb/187623 (June 24, 2004)

[3] CrossTec Corporation. NetOp Remote Control Information.
www.NetOpUSA.com

[4] Symantec Corporation. PCAnywhere.
http://sea.symantec.com/content/product.cfm?productid=16

[5] NetSupport Inc. NetSupport Manager
http://www.netsupport-inc.com/nsm/netsupport_manager_overview.htm

[6] Riley, Steve. “Active Directory Replication over Firewalls” 15 March 2004

http://www.microsoft.com/serviceproviders/columns/config_ipsec_P63623.asp