NetOp®

Process Control

NetOp Process Control Quick Guide

Document Revision: 2007205
Please send any comments to:
Danware Data A/S
Bregnerodvej 127
DK-3460 Birkerod
Denmark
Tel: +45 45 90 25 25
Fax: +45 45 90 25 26
E-mail: info@netop.com
Internet: http://www.netop.com

NetOp Process Control Quick Guide

Warranty

Danware Data A/S warrants the quality of the physical material of the user package, that is manual and CD-ROM. If these items are defective, we will exchange them at no cost within 60 days of purchase from Danware Data.

Disclaimer

Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of any faults with the enclosed programs and/or documentation.

Licence

Trademarks

Publisher
Danware Data A/S
Technical Editors
Lars Lyhne
Team Coordinator
Allan Iskov

Table of Contents

1 Welcome

Welcome to NetOp Process Control, a Danware Data security software.

This quick guide will lead you through a default installation and startup of NetOp Process Control. Additionally it will present examples of how to configure programs to work with the firewall.

Available options are explained in the NetOp Process Control User's Manual which you can find in the install directory or as an online help system which can be activated by pressing the F1 button or by clicking the Help-button.

Furthermore, it is possible to find information on our KnowledgeBase on the NetOp homepage, or using the Support form.

The NetOp Product Services Team

1.1 Introduction

The NetOp Process Control is an extremely powerful tool that offers process control and dynamic packet filtering.

Process control gives you the ability to deny any program (process) to run at all, allow communication, only allow communication of a trusted network or prevent any communication.

Packet Filtering is used for restricting the computer's inbound and outbound traffic based on IP addresses, ports and protocols.

Packet Log and **Traffic Matrix** are two built-in tools used for displaying real-time network activity details such as which IP addresses, ports and protocols a program is trying to use for communication. Make use of this information to configure the firewall.

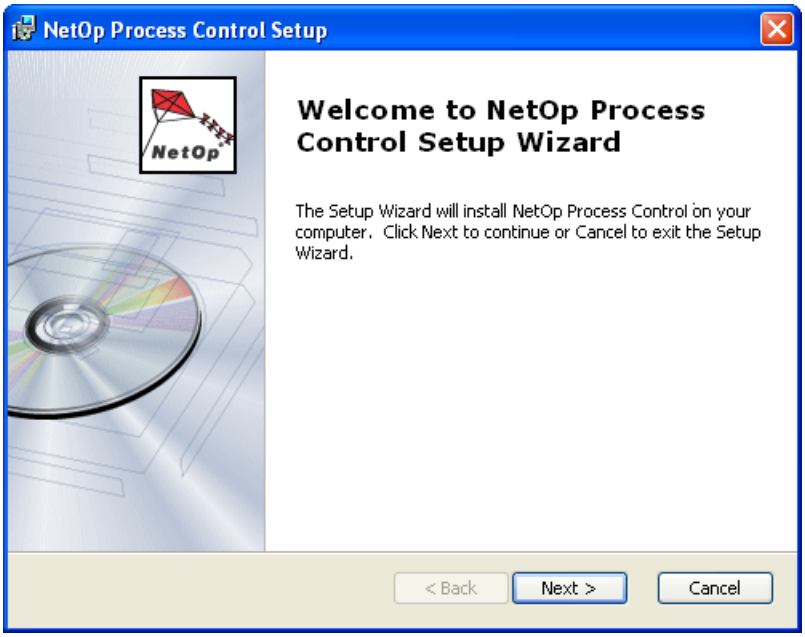
Note: The NetOp Process Control configuration can either be managed locally on each computer or centralized by the optional **NetOp Policy Server**. For fault tolerance and load distribution the NetOp Policy Server has been implemented with a **Master Server** and multiple **Replica Servers** ensuring maximum system availability.

1.2 Before you install

1. **Read the NDFReadMe.txt file that resides in the root directory of the CD.**
2. Remove any installed firewall.
3. Scan your computer with an updated anti virus product.
4. Save all data and shut down all running Windows applications.
5. Make sure that the computer is connected to the Internet. If connected to the Internet by a dial-up connection, the dial-up connection must be running.

1.3 Installation

Once you have downloaded the installation file, click Run and follow the on-screen instructions.



Remember to have all required information ready at hand.

After installing, choose *Yes* to restart the computer and complete the installation, optionally choose *No* to postpone the restart.

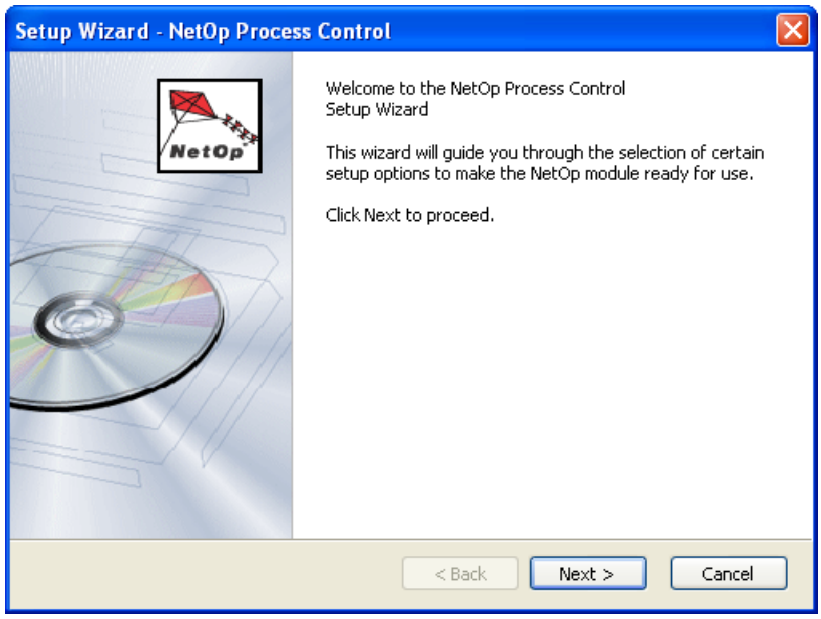
Note: NetOp Process Control will not be running until the computer has been restarted

1.4 Setup

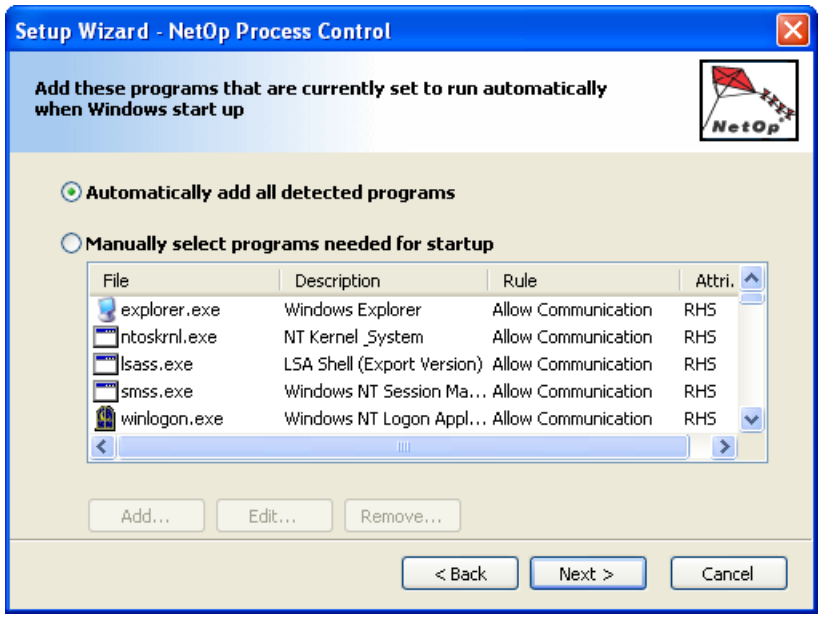
When the computer has been restarted, the Setup Wizard will automatically be loaded. The Setup Wizard assists you in creating a NetOp Process Control (NPC) setup for your current computer environment.

To create a default setup, accept the Setup Wizard suggestions.

In the window shown below, click Next > to continue.



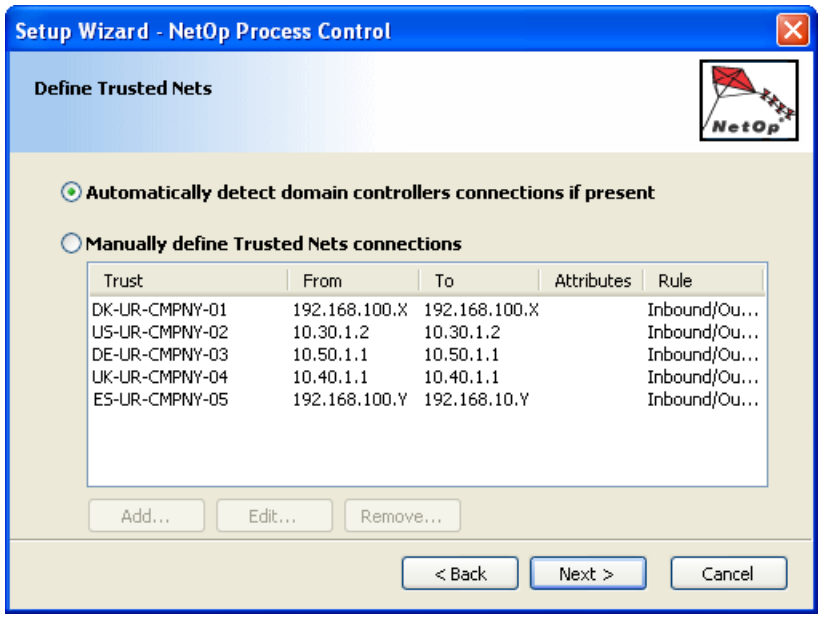
NPC makes an initial detection of which programs and services are running after you logged on to your computer. The wizard assumes that these are mandatory for your system to function correctly and lists them in the window below.



To edit to the list of detected programs, select Manually select programs needed for startup.

In general it is not recommended to make any changes to the automatically detected programs, since it may cause malfunction of your system.

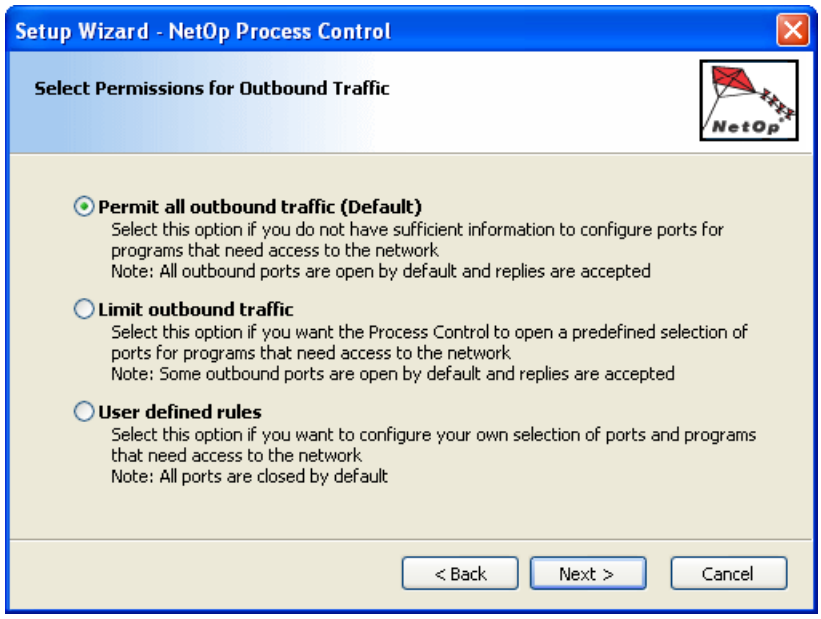
Click Next > to continue



NPC automatically detects the domain controllers of the domain that you are currently logged on to. This enables you to set up a trust for these, securing that your communication with the Local Area Network will not be blocked. The list is empty, if you are presently not logged on to a domain, or if no domain controller is present.

To edit the list of detected domains, select Manually define Local Area Network.

Click Next > to continue.



Initially, NPC allows traffic that is necessary for your programs to function smoothly. This means that the programs will be allowed to communicate with e.g. the Internet and accept replies to this specific communication. Your computer will still be blocked for undesired incoming traffic.

It is recommended at this time to keep the default.

Click Next > to continue.

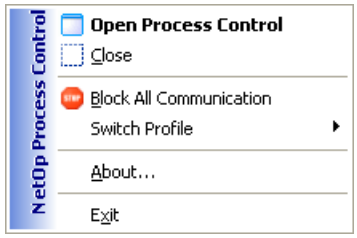
Click Finish to leave the setup wizard.

NetOp Process Control is now set up and running.

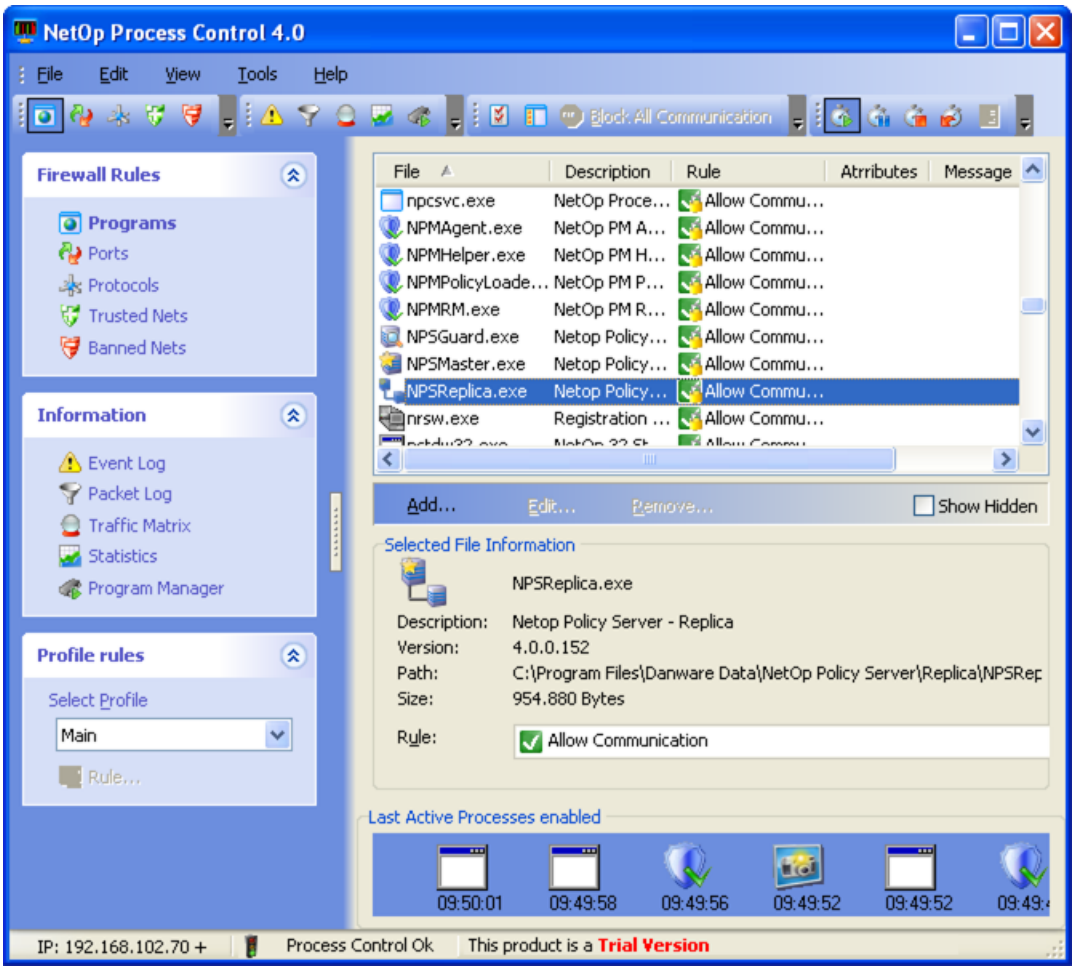
2 Configuration of NPC

When NetOp Process Controlis installed on a computer, this button will by default appear in the notification area in the lower right corner of the screen:

Right-click this button to display this menu:



The Open Process Control provides access to the NetOp Process Control window.



This is the NetOp Process Control main user interface that specifies Firewall Rules, accesses Information utilities and specifies Profiles.

2.1 Firewall Rules

This section allows the user to configure rules for program execution and communication.

For each *Program* a specific rule can be applied to decide whether the program may run and if communication is allowed.

As a general setting for all programs *Ports* and *Protocols* can be used to restrict communication.

Trusted Nets and *Banned Nets* are used for controlling which IP addresses the computer can communicate with.

2.2 Information

This section displays historic event information and real-time details about network traffic.

The *Event Log* gives information about e.g. programs starting and stopping, changes in your networking environment and results of unknown programs requesting network access.

The *Packet Log*, the *Traffic Matrix* and *Statistics* give a real-time picture of the actual networking

activity and is a valuable tool for deciding if a firewall rule should be modified to block or allow communication.

To get a list of currently running programs and processes, access the *Program Manager*. From here you can stop a program or you can add it to the database for later editing.

2.3 Profiles

A *Profile* is a complete set of firewall rules that can be used on a specific network. All of the rules that are created, will affect the *Main Profile* until you actually decide to create new profiles.

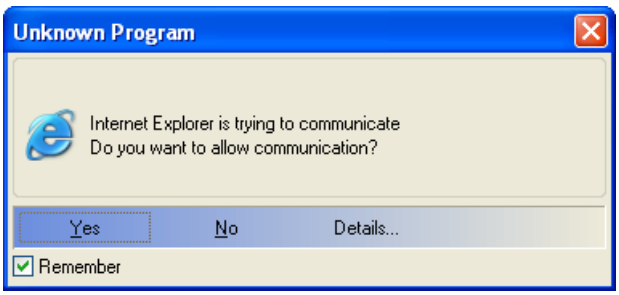
When creating a new profile an exact copy of the *Main Profile* is used as template for the new definition.

3 Configuring the Process Control

3.1 Allowing outbound communication for a program

While working on your computer, programs may need to communicate with other networked computers to execute their tasks.

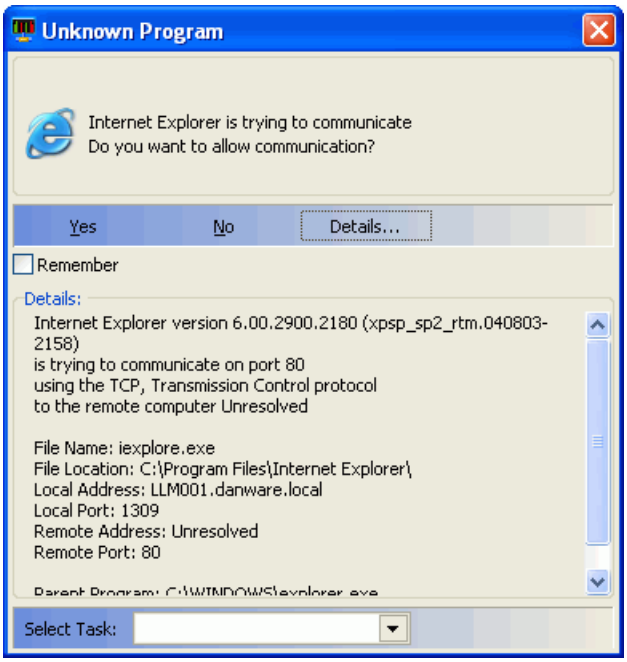
For programs not listed and approved during the initial setup wizard, NetOp Process Control will display this window when a program tries to communicate with other computers:



In this example Microsoft Internet Explorer is trying to start outbound communication with a web-server. This is OK, if you just launched this internet browser and entered a web address to visit. Outbound communication means that the communication is initiated from your own computer going out through your firewall.

In case you do not want to be prompted each time the program tries to communicate, check Remember.

If the program name does not seem familiar, you can optionally select the Details... button to display a lower extension of the window with details on the communication attempted by the program and additional program firewall rule options. Based on this information, you have a better chance of deciding whether or not the program should be allowed to communicate.



By clicking Yes this program will be added to the database with the firewall rule Allow Communication. The next time Internet Explorer is being launched, the user will not be prompted for a decision.

3.2 Denying outbound communication for a program

Today, many programs by default establish a connection to the Internet to e.g. check for updates, even though it is not necessary for the program to function correctly.

In these situations you may not wish to allow programs and services to communicate with other networked computers, that could cause superfluous network traffic.

In the above example Windows Media Player is trying to communicate to e.g. retrieve media information from the Internet.

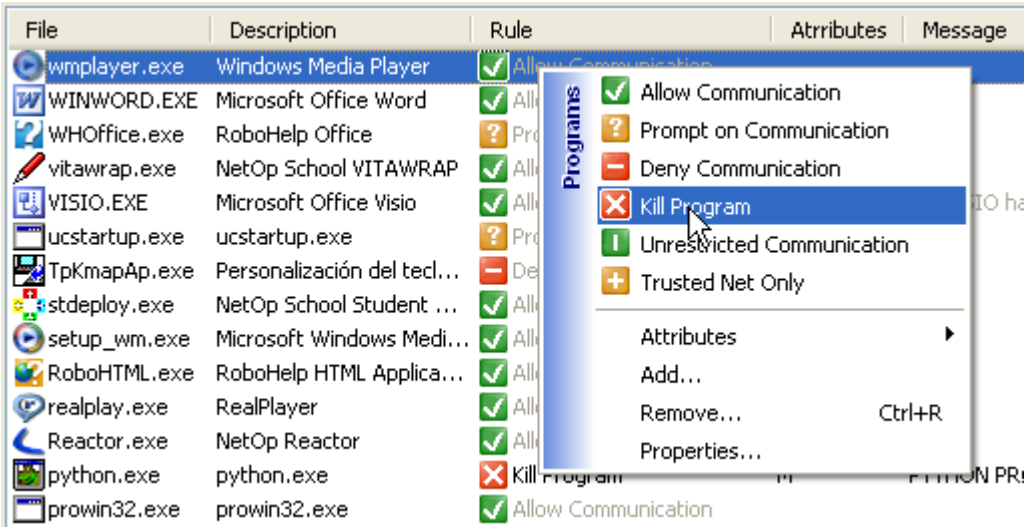
If you wish to play only local media files, there is no need for the Media Player to contact the Internet. In this case you may wish to *Deny Communication*. The firewall will then prevent any communication regardless of the settings in the Media Player Options.

By checking *Remember* and clicking *No*, this program will be added to the database with the firewall rule *Deny Communication*. Thus you will not be prompted the next time Media Player tries to communicate.

In case you want to be prompted each time the program tries to communicate, leave *Remember*

unchecked. This enables you to change your decision the next time Windows Media Player tries to communicate.

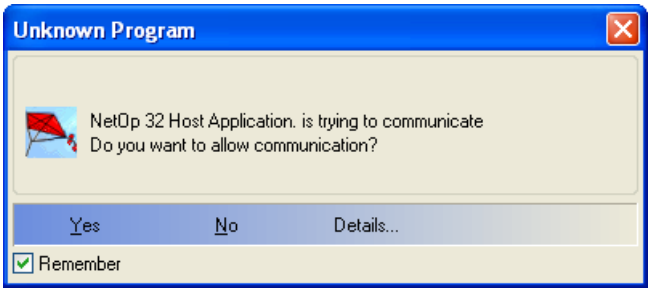
To change the current rule for Windows Media Player, select Firewall Rules/Programs. Locate the file Windows Media Player file called wmplayer.exe, right-click it and choose between the options below:



3.3 Allowing inbound communication for a program

Certain computers offer networking services and may need to allow inbound communication, coming from other networked computers. Examples of these services are web, file, database and computer management services, like remote control.

Inbound communication means that the communication is initiated from other computers coming in through NPC.



In this example NetOp Host tries to communicate with the network during the initial startup using outbound communication. As such, NPC prompts the user to allow this program to communicate. By checking *Remember* and clicking Yes, this program will be added to the database with the firewall rule Allow Communication.

From a user point-of-view this program should now be ready for communication. However, when trying to communicate with the NetOp Host using TCP from other computers on the network, no connection can be established because NPC by default is not open for inbound communication.

The NetOp Host is the server part of a remote control program and as such requires an inbound port to be open in order to work properly.

To configure the *Firewall Rules* correctly for this program, use the *Packet Log* to observe

information about the blocked inbound communication:

Process Name	Protocol De...	Remote IP Address	Remote Port	Local IP Address	Local Port
Nhstw32.exe	TCP, Transmi...	192.168.109.52	1654	192.168.103.61	6502
Nhstw32.exe	TCP, Transmi...	192.168.109.52	1654	192.168.103.61	6502

Look for Nhstw32.exe, which is the NetOp Host file name and locate the *Local Port* number. In this case you need to open Port 6502 to allow inbound communication from the NetOp Guest that is the client part of the remote control program.

To change the current rule for Port 6502, select *Firewall Rules/Ports*. Locate NetOp Remote Control and change the rule in the drop-down list at the bottom to *Inbound/Outbound Traffic*.

NPC is now configured correctly to let the NetOp Host be remotely controlled. You can also see the effect of the changed setting in the the Packet Log:

Process Name	Protocol De...	Remote IP Address	Remote Port	Local IP Address	Local Por
Nhstw32.exe	TCP, Transmi...	192.168.109.52	1682	192.168.103.61	6502
Nhstw32.exe	TCP, Transmi...	192.168.109.52	1682	192.168.103.61	6502
Nhstw32.exe	TCP, Transmi...	192.168.109.52	1682	192.168.103.61	6502
Nhstw32.exe	TCP, Transmi...	192.168.109.52	1682	192.168.103.61	6502
Nhstw32.exe	TCP, Transmi...	192.168.109.52	1682	192.168.103.61	6502
Nhstw32.exe	TCP, Transmi...	192.168.109.52	1682	192.168.103.61	6502
Nhstw32.exe	TCP, Transmi...	192.168.109.52	1682	192.168.103.61	6502
Nhstw32.exe	TCP, Transmi...	192.168.109.52	1682	192.168.103.61	6502

3.4 Working with other computers on your LAN

By default NPC will not allow inbound communication from other computers on your Local Area Network.

This may not be convenient for your daily office routines, like e.g. sharing folders and printers. You will receive an error message like this:

At this point the *Setup Wizard* has already detected the domain controllers of the domain (if present) that you are currently logged on to, and added a Trust with these. This secures that your communication with the Windows Domain will not be blocked.

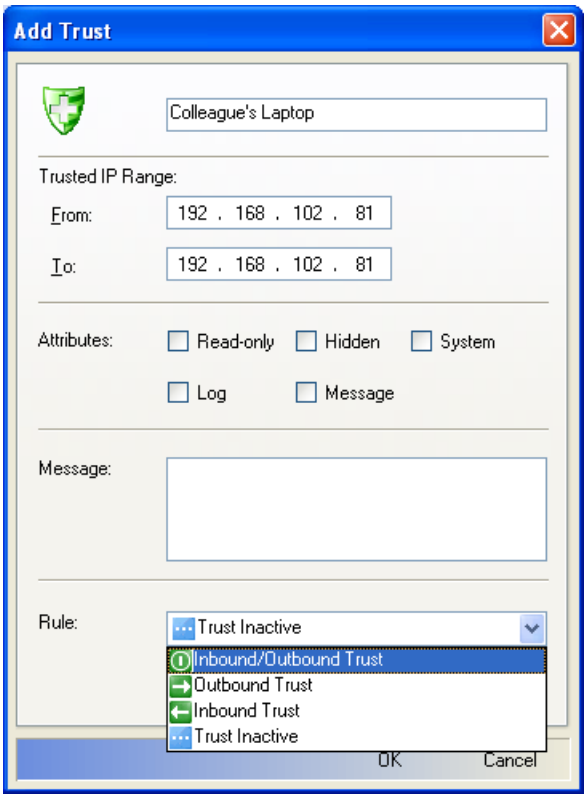
However, this is still not enough to e.g. share files with a specific computer, like your colleague's laptop. First you must configure NPC to use a *Trust* between your computer and the laptop.

A *Trust* allows communication with the specified computer's IP address on all ports and protocols. The *Trust* can be in one or both directions.

While the *Trust* is not established, the *Packet Log* will show blocked traffic from your colleague's laptop:

Process Name	Protocol De...	Remote IP Address	Remote Port	Local IP Address	Local Port
Ntoskrnl.exe	TCP, Transmi...	192.168.102.81	2954	192.168.103.61	445
Ntoskrnl.exe	TCP, Transmi...	192.168.102.81	2955	192.168.103.61	139
Ntoskrnl.exe	ICMP, Interne...	192.168.102.81	0	192.168.103.61	0
Ntoskrnl.exe	ICMP, Interne...	192.168.102.81	0	192.168.103.61	0
Ntoskrnl.exe	TCP, Transmi...	192.168.102.81	2955	192.168.103.61	139

To add your colleague's laptop to the the *Trusted Nets*, open *Firewall Rules/Trusted Nets* and click *Add*... Enter the laptop's IP address and select *Inbound/Outbound Trust*:



Now your colleague can access your shared folders and printers. The *Packet Log* will look like this:

Process Name	Protocol De...	Remote IP Address	Remote Port	Local IP Address	Local Port
Ntoskrnl.exe	TCP, Transmi...	192.168.102.81	2994	192.168.103.61	139
Ntoskrnl.exe	TCP, Transmi...	192.168.102.81	2994	192.168.103.61	139
Ntoskrnl.exe	TCP, Transmi...	192.168.102.81	2994	192.168.103.61	139
Ntoskrnl.exe	TCP, Transmi...	192.168.102.81	2994	192.168.103.61	139