

Functional Description and Configuration

high security remote access

Personal Firewall and Friendly Net Detection





Personal Firewall and Friendly Net Detection

Support

NCP offers support for all international users by means of Fax and Internet Mail.

Fax Hotline Number

+49 911 99 68 458

Internet Mail Address

support@ncp-e.com

When contacting NCP with your problems or queries please include the following information:

- exact product name
- serial number
- Version number
- Accurate description of your problem
- Any error message(s)

NCP will do its best to respond as soon as possible, but we do not guarantee a fixed response period.



Network
Communications
Products engineering GmbH

GERMANY
Headquarters:
Dombühler Straße 2
D-90449 Nürnberg
Tel.: +49-911-99680
Fax: +49 - 911 - 9968 299
Internet <http://www.ncp-e.com>
E-mail: info@ncp-e.com

Copyright

Considerable care has been taken in the preparation and publication of this manual, errors in content, typographical or otherwise may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP as desired.

NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or use for any particular purpose. Furthermore NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and changes.

This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH, Dombühler Str. 2, D - 90449 Nürnberg, Germany.

All trademarks or registered trademarks appearing in this manual belong to their respective owners.

© NCP engineering, March 2012

The Firewall of the Secure Client	5
Overview of Contents	5
Functions of the Firewall	6
Friendly Net Detection and Stateful Boot Option	7
Firewall Settings	8
Display of the Firewall Settings	8
Security Policy	9
Mode of Operation of Friendly Net Detection	9
Definition of Friendly Networks	9
Principle of Friendly Net Detection	10
Authentication	10
Configuration Menu of the Personal Firewall and Examples	12
Example: Client Firewall with Application Dependent Rule	12
Example: Automatic Adaption of a Rule to a Friendly Network	14
Creating a Rule	14
Friendly Network	15
Automatic Detection of Friendly Networks	15
Friendly Network Display on the Monitor	15
Configuration Menu of the Personal Firewall	16
Basic Settings and predefined NCP Rules	17
NCP Rules for test connection	17
NCP Rule for DNS Request	17
NCP Rules for Web Browser	17
NCP Rule for FTP	17
NCP Rule for Ping (IP communications)	18
All connections outgoing (IPv4)	18
All connections (friendly network)	18
All connections (VPN)	18
Internet access via webbrowser	18
Rule for Remote Desktop (RDP access)	18
Permit IPsec-protocol	18
Permit L2Sec protocol (UDP 1701)	19
Editing Rules	19
Restrictions for Application Specific Firewall Rules	21
Configuration Folder Friendly Networks / Manual	22
Configuration Folder Friendly Networks / Automatic	23
Friendly Net Detection via TLS	23
Configuration Folder Friendly Networks / Options	24
Configuration Folder Friendly Networks / Actions	25
Configuration Folder Options / General	26
Configuration Folder Options / Commands	28
Configuration Folder Logging	29
Installation and Configuration of the FND Server	30
Configuration of the FND Server	31
[General]	31
[SysLog]	31
[FND-USER 1]	32
[FND-USER 2]	32
Configuration of the Client	33
Basic Settings	33
Filter Rules	33
Authentication with MD5 and TLS	33
MD5 Configuration	33
TLS Configuration	34
Starting the NCPFND Service	34
Test	34
Uninstalling	34
Index	35

The Firewall of the Secure Client



The first part of this document describes the functions of the personal firewall as well as the special features Friendly Net Detection and Stateful Boot Option.

The second part features configuration examples for activation of the firewall and friendly net detection and it describes all parameters of the firewall configuration menus.

The third part describes installation and configuration of the friendly net detection server.

Contents

- **Functions of the Firewall**
- **Friendly Net Detection and Stateful Boot Option**
- **Firewall Settings**
- **Mode of Operation of Friendly Net Detection**
- **Example: Application Dependent Rule**
- **Example: Friendly Net Detection**
- **Configuration Menue of the Personal Firewall**
- **Installation and Configuration of the FND Server**
- **Authentication with MD5 and TLS**
- **Index**



The firewall settings for mobile computing are described in the manual **Mobile Computing**.



The **Enterprise Suite Navigation** is a very convenient way to access the desired information. This pdf file contains links to all manuals currently available for your product.

You can directly access all relevant manuals via the navigator. If a manual has not yet been stored in your navigator's directory, it can be downloaded from the NCP website.

Functions of the Firewall

All firewall mechanisms are optimized for remote access applications and are activated as soon as the computer is started. This means that in contrast to VPN solutions with an autonomous firewall, the mobile computer is already protected against attacks before the VPN is actually used.

Dependent on how the firewall is configured, it is active for all IP traffic to and from the computer.* It is globally effective, independent of the location of the computer or the currently selected profile of the Client.**

The firewall uses packet filtering techniques in connection with Stateful Packet Inspection (SPI). The firewall checks all incoming and outgoing data packets, and on the basis of the configured rules, it decides whether a packet should be forwarded or rejected.

Security is insured in two ways: Unauthorized access to data and resources in the central data network is prevented. The current status of existing connections is monitored via stateful inspection. In addition, the firewall also detects whether a connection has opened “spawned connections”, as is the case with FTP or Netmeeting for example, whose packets likewise have to be forwarded. If a rule is defined which permits an outgoing connection, then the rule automatically applies to the corresponding return packets. For the communication partner a stateful inspection connection is represented as a direct line which can only be used for the exchange of data that complies with the stipulated rules.

** If the firewall is activated, IP communication with a network printer might not be possible.*

*** In contrast to the personal firewall, the link firewall, which can be set up in the profile settings of the monitor, is only activated for the affiliated profile.*

To avoid conflicts between the rules of the connection-orientated link firewall of the profile settings and the personal firewall it is advisable to disable the link firewall when using the personal firewall. Enter the IP addresses of the links to the destination gateway in the personal firewall's filter rules.

If the link firewall has to be used parallel to the personal firewall, please note that the link-orientated firewall settings always have priority during activation. For example, if the link firewall is set to “always” and “only tunneling permitted” has also been activated, communication can only take place via a VPN tunnel, even if there are different rules defined for the personal firewall. All other traffic is rejected by the link firewall.



**** The administrator can define all firewall rules and force their compliance. For this, set the appropriate **Parameter Locks** of the Entry Client. Prerequisite for the central administration of the Enterprise Client is the NCP Secure Enterprise Management.*

Friendly Net Detection and Stateful Boot Option

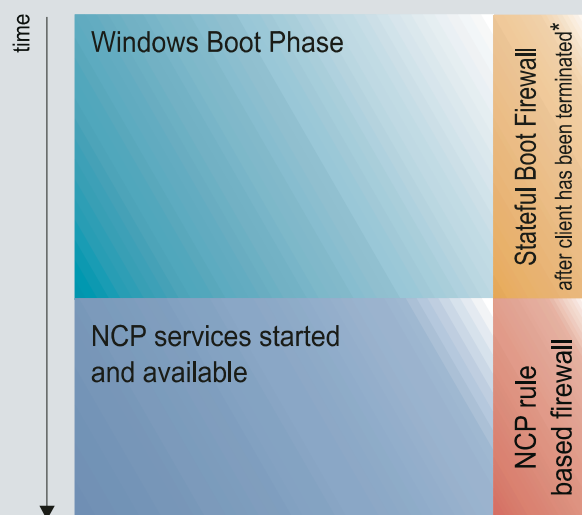
Another important feature of the NCP Secure Client software is **Friendly Net Detection**, which enables the client to be used universally, in any remote access and communication environment. The rules of the integrated personal firewall are set (centrally*) by the administrator and can neither be manipulated nor switched off by the user. At all times, the user can access the corporate network highly secure and with a maximum of transparency.

The feature “keep firewall active after Client has been terminated” ensures full protection of the computer, even if the Client is not running - provided this feature has been activated in the firewall under **Options**. During system startup, Microsoft Windows exchanges various group and security policies between Client and domain controller. These policies are discarded if the NCP personal firewall is active when the Client is stopped, even if the NCP service has been terminated.

The “Stateful Boot Option” (Firewall settings under **Options**) expands the personal firewall to a stateful packet inspection firewall at driver level. This allows policies to be exchanged as well as communication between other Windows workstations during the boot phase. At the same time, the system is protected from attacks from the outside.

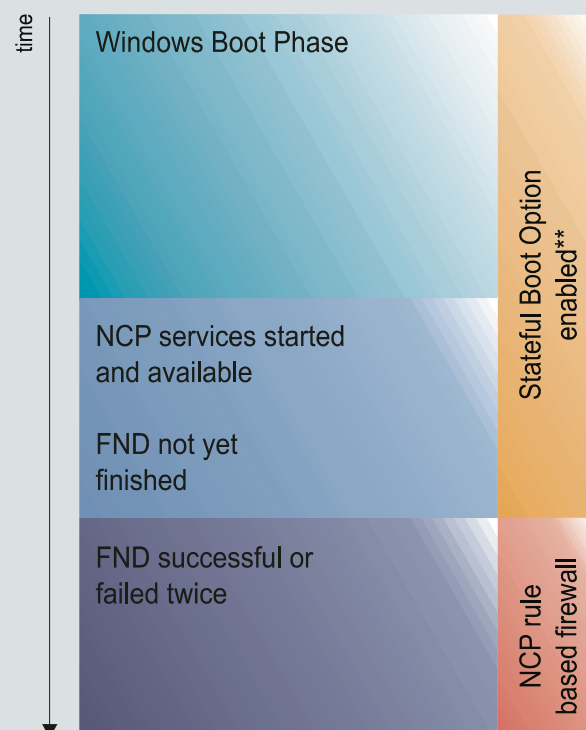
NCP Firewall with Stateful Boot Option

Friendly Net Detection disabled



* In firewall configuration under options:
Active Firewall after Client has been terminated
** In firewall configuration under options:
Active Firewall after Client has been terminated *plus*
Activate Stateful Boot Option

Friendly Net Detection enabled



Firewall Settings

The firewall rules can be configured dynamically, which means that it is not necessary to stop the software or restart it.

Specific firewall filter rules are defined using the Client monitor's configuration menu. They can be created as either application dependent and additionally address dependent or vice versa. In addition, they can be specially assigned to friendly networks as well as unknown networks or VPN connections (Firewall settings, Firewall rules).

The section **Friendly Net Detection** describes how friendly or unknown networks can be detected by the Client and how respective firewall filter rules can be assigned.

Display of the Firewall Settings

The basic settings of the firewall are displayed in a tool tip of the system tray icon, making it easy to see whether the personal firewall is enabled or disabled or whether the Client is in a friendly or in an unknown network. (The wall icon of an active firewall is red when in an unknown network and green when in a friendly network; see illustration below). The **Symbols** of the Client monitor are described in detail in the PDF "Client Monitor".



Display of the firewall in the popup of the icon tray.

Mode of Operation of Friendly Net Detection

Mobile workers who need access to the Internet and the corporate network via VPN from their office in the corporate headquarters as well as from their home office place special demands on their personal firewall.

When “on the road” the laptop must be protected against attacks and must reject all prohibited communications. In the corporate office, on the other hand, registration on the domain and subsequent connection to all servers of the corporate network should be swift and easy. It could also be that the mobile user, when “on the road”, should only be allowed to download e-mails from the corporate server, and not be allowed to surf the Internet. On the other hand, if linked to the corporate network, the laptop is in a protected environment (with virus scan software and firewall), making a personal firewall superfluous if the user wants to use a client / server application via defined TCP/IP or UDP ports.

If a static firewall, configured for mobile use, were used, the user would have to change the settings of his personal firewall manually, dependent on security policy and network environment (headquarters or branch office).

The need to manually change the settings is obviated by the Friendly Net Detection (FND) technology which can distinguish between friendly networks, such as the corporate network, and unknown networks, and then automatically change the firewall settings.

Security Policy

A security policy comprises all criteria set by the administrator, defining the user's rights in a network (e.g. Intranet, central data network, corporate network, Internet, etc.). The rules for the firewall, also set by the administrator, are created in the same manner. The firewall rules have to meet the demands of the security requirements of the various networks, i.e. friendly networks or unknown networks (Firewall Settings, **Firewall Rules**). The security policy* contains all information about which networks are defined as friendly networks and which are defined as unknown networks.

In order to define firewall rules which are location or network dependent, the NCP Secure Client includes the capability to assign one or more firewall

rules to either a group of friendly networks or to a group of unknown networks. This enables a rule to be only automatically activated when the user moves to one of the network groups.



** In order to avoid users bypassing this security policy, i.e. deactivating, deleting or changing firewall rules, the NCP Secure Client supports the capability to lock configuration parameters. This is also possible for users with administrator rights i.e. it is independent of the rights of the system environment (see **Parameter Locks**).*

Definition of Friendly Networks

ÜThe Client can be notified about friendly network status either manually or automatically, dependent on firewall settings. In both cases, the administrator has to define the firewall rules only once for the entire system environment.

Manual configuration of a friendly network requires entering the relevant network data (**Firewall Settings**, friendly networks, **Manual**). The administrator must keep the list of friendly networks permanently up-to-date and secure compliance to the firewall rules in the constantly changing communication environments.

One constraint is that not every company has an IP address range from the public IP address range. Many companies use private IP addresses such as 10.x.x.x/8, 172.16.x.x/16 or 192.168.x.x/24 and use NAT-Devices (Network Address Translation) or a proxy server, but without considering that with statically configured friendly networks, a member of staff will have to work with the same IP address in both the home network as the friendly network. A teleworker, conversely, could then be able to access an unknown network which uses the same IP address range as the corporate network. In both cases the security policy is nullified and firewall rules, designed to protect the Client in unknown networks, deactivated.

For users and administrators, the task of keeping the list of friendly networks up to date becomes superfluous if **Automatic Configuration** with friendly net detection is used. This feature also allows for authentication mechanisms to unambiguously detect a friendly network.

Automatic configuration is one of the features of the dynamic personal firewall. Completely transparent and without the need to import a new configuration, it enables the Client to automatically detect a friendly network.

Friendly Net Detection

FND is a client / server application. Since the Friendly Net Detection Server (**FNDS**) is a service which has to be installed separately and which is completely independent of the VPN gateway, it can be installed on any computer within the network to be declared as FN.

The FND's operation is based on established standards. This guarantees system security and prevents the errors frequently found in custom-made solutions.

After installation of the NCP FNDS in the network defined as a "Friendly Network", the **NCPFND Service has to be started** (see section FND). This service must be reachable from all points on the network, i.e. firewall rules may have to be changed.

Regardless of where user is working, the FND Client in the Client computer attempts to contact the configured FND server. If the FND server is reached and authenticated, it confirms that the user is located within a friendly network and all firewall rules pre-configured for this "friendly network" are activated automatically. Failure to reach the FND indicates that the user is located in an "Unknown network" and the corresponding rules are automatically set.

Authentication

The configuration description associated with the following explanation is located in section "Automatic Detection of Friendly Networks".

User ID and password are used for authentication (in the **Firewall Settings**) in the standardized authentication protocols MD5 (RFC2284) and TLS (RFC2716), in which only the server is authenticated by the client.

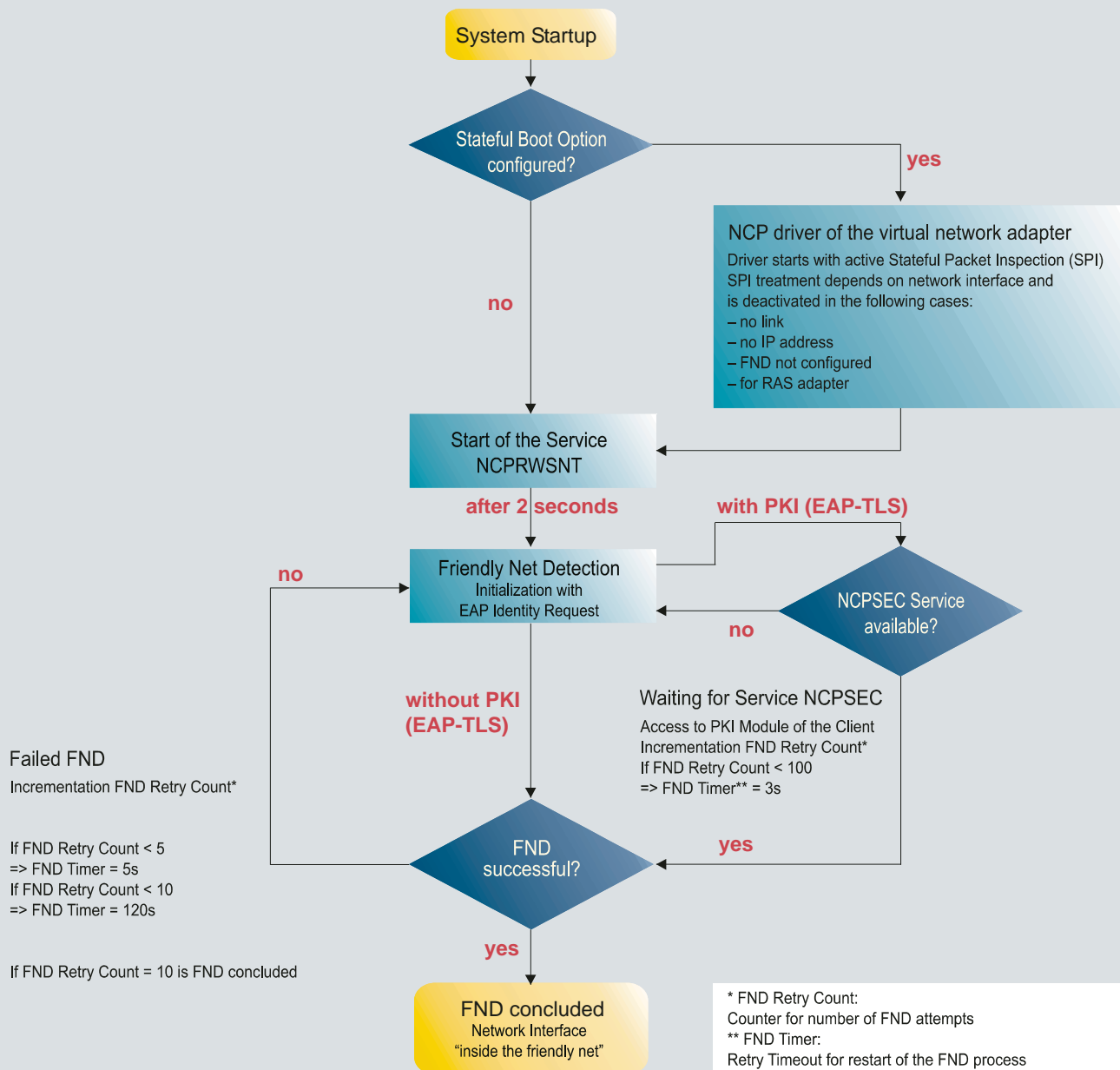
In the case of **EAP-MD5**, user ID and password have to be stored on the server as well as on the Client to allow authentication. This also opens up the possibility to **create groups** of Clients (defini-

tion of group specific FNs). Please also refer to the section **Authentication with MD5 and TLS**.

Using **EAP-TLS** the issuer certificate or all certificates which are necessary for validating the FNDS certificate have to be available on the Client. Furthermore, the fingerprint of the issuer certificate and the subject of the FNDS certificate can be configured at the Client. This excludes a hostile recreation of the friendly network. Please also refer to the section **Authentication with MD5 and TLS**.

After all information for authentication have been configured, the **IP Address** (or hostname) of the FNDS has to be defined. The maximum number IP addresses or hostnames is two and they have to be separated by commas.

NCP Friendly Net Detection



Friendly net detection is an important feature of the NCP Secure Client Software for universal use in any remote access and communication environment. The rules for the integrated personal firewall can be set centrally* by the administrator and cannot be manipulated or switched off by the user. At all times, the user can access the corporate network highly secure and with a maximum of transparency.

* For centrally managed changes to the NCP Secure Enterprise Client's configuration parameter, NCP offers the Secure Enterprise Management (SEM) System as "Single Point of Administration".

Configuration Menu of the Personal Firewall and Examples

Example: Firewall with application dependent rule

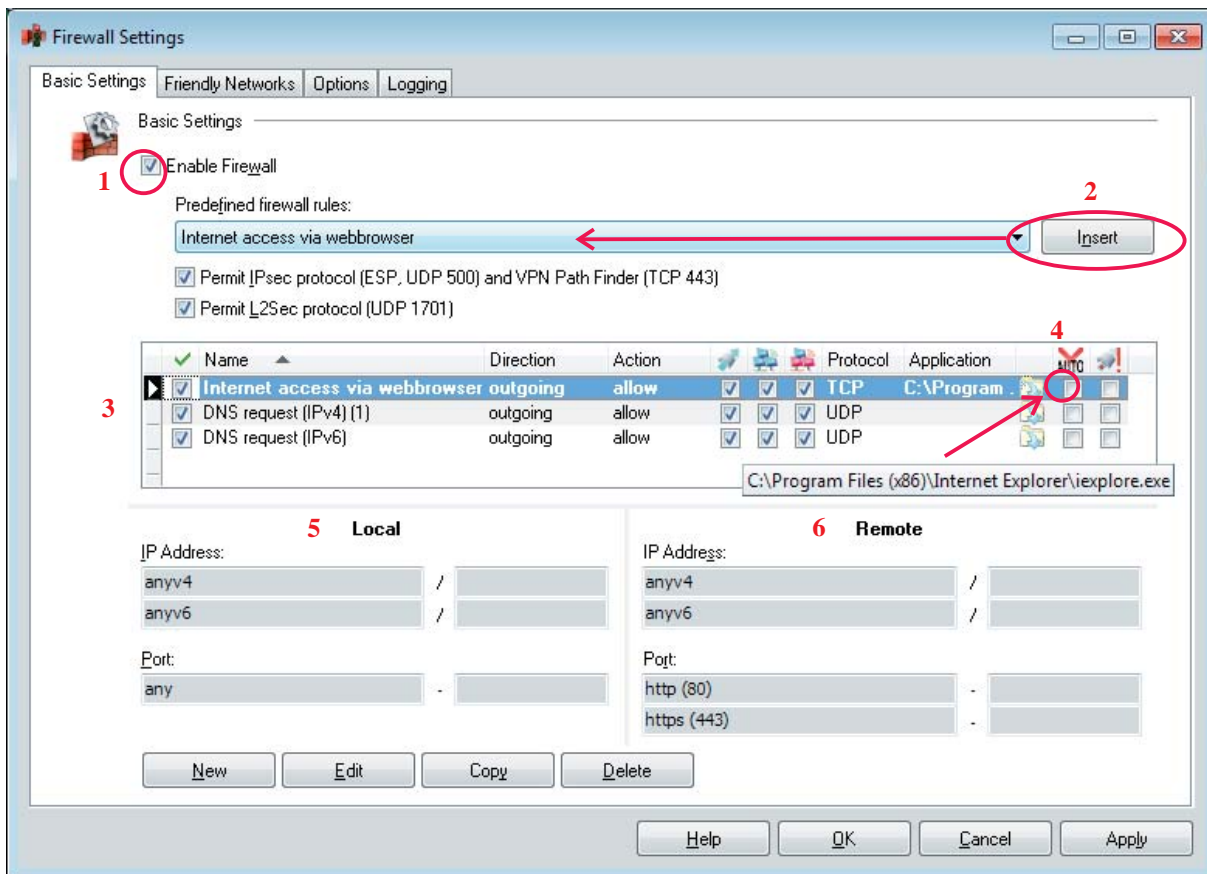


fig. 1

The predefined firewall rules can be rapidly adapted for different environments and applications

To enable the firewall, select the menu item “Firewall” from the Client Monitor’s Configuration Menu, then, in the Basic Settings displayed, click on the “Enable Firewall” option. (fig. 1 above)

As soon as the firewall is enabled, a symbol is displayed in the Client Monitor indicating that all IP communication in the network (LAN, printers, etc.) is blocked, regardless of whether it is IPv4 or IPv6 or whether incoming or outgoing. This happens when no explicit firewall rules have been created or enabled.

Next select a preconfigured rule or create your own rule which will open the firewall for IP data traffic, depending on the network the computer is connected to: friendly, unfriendly or VPN network.

Example: Surfing the Internet with Internet Explorer

Select the “Internet access via webbrowser” and click on “Insert” (2); the three lines illustrated above are inserted into the list of rules (3)

Internet access is now enabled for outgoing connections in friendly and unknown networks. In addition this rule only allows TCP packets to pass through the firewall. In the application field, use the browse function to define the path to the Internet Explorer .exe file.

Under the “Local” heading, specify that all outgoing IP packets will be allowed, independent of the IP address or port the IP packets are using (5).

Under the “Remote” heading, specify that the firewall is open for all IP addresses and that it allows connections via port 80 (for HTTP) and port 443 (HTTPS) (6).

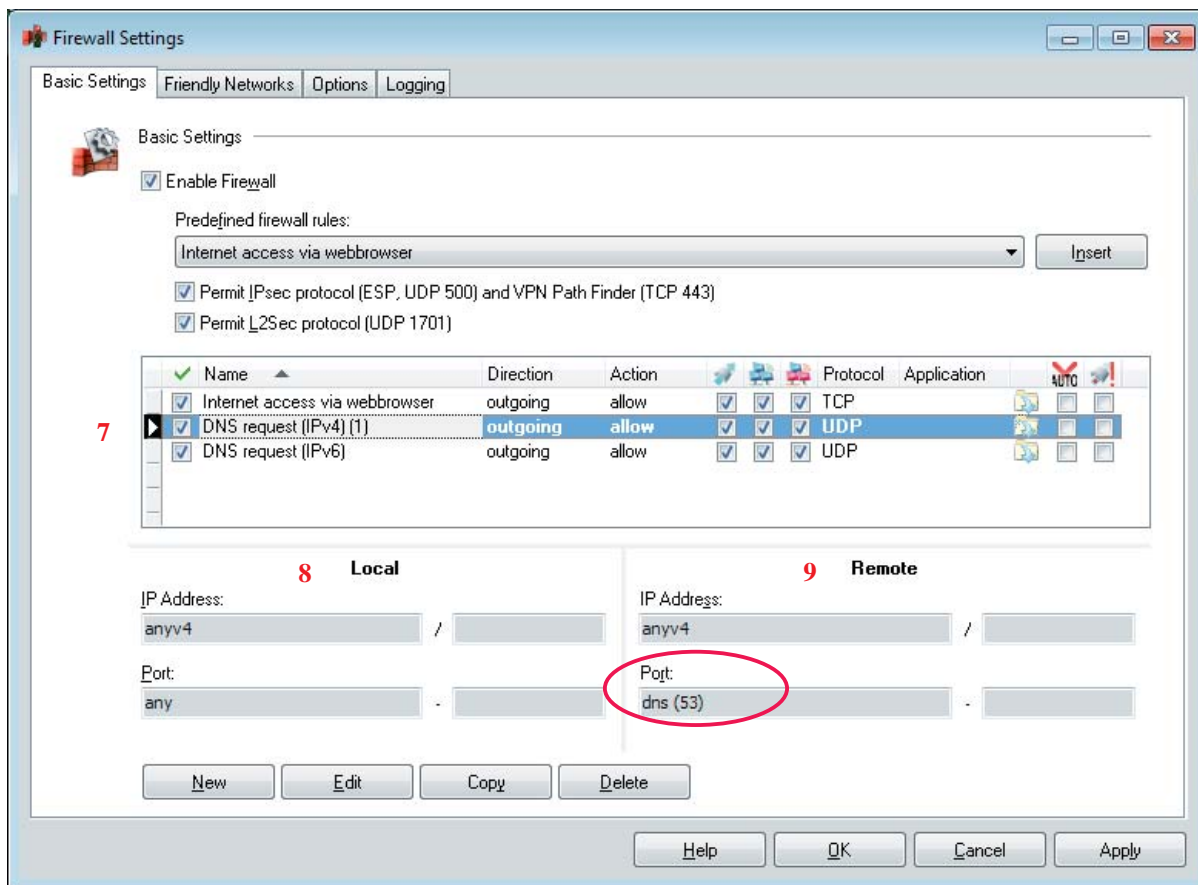


fig. 2

Rules for DNS Requests (7)

The rules for DNS requests (IPv4 and IPv6) can be adopted unchanged. (fig. 2 above)

Local Ports and IP Addresses (8)

Data packets that are to be allowed through the firewall must have a source address that corresponds to the address or address range defined here.

anyv4: allows communication with any IPv4 address from the local side (source address), without restriction.

Similarly for IP ports. Data packets that are to be allowed through the firewall must have a source port corresponding to a port or ports defined here.

Remote Ports and IP Addresses (9)

Data packets that are to be allowed through the firewall must have a destination address that corresponds to the address or address range defined here.

anyv4: allows communication with any IPv4 address at the destination.

Similarly for IP ports. Data packets that are to be allowed through the firewall must have a destination port corresponding to a port or ports defined here. Note: port 53 is required for DNS requests.

Regarding IPv4 and IPv4 address notations, see the descriptions of the individual **Configuration Fields** or the Online Help.



Note, in addition to the application dependent rules, the restrictions on page 22.

Example: Automatic adaptation of a rule to a friendly network

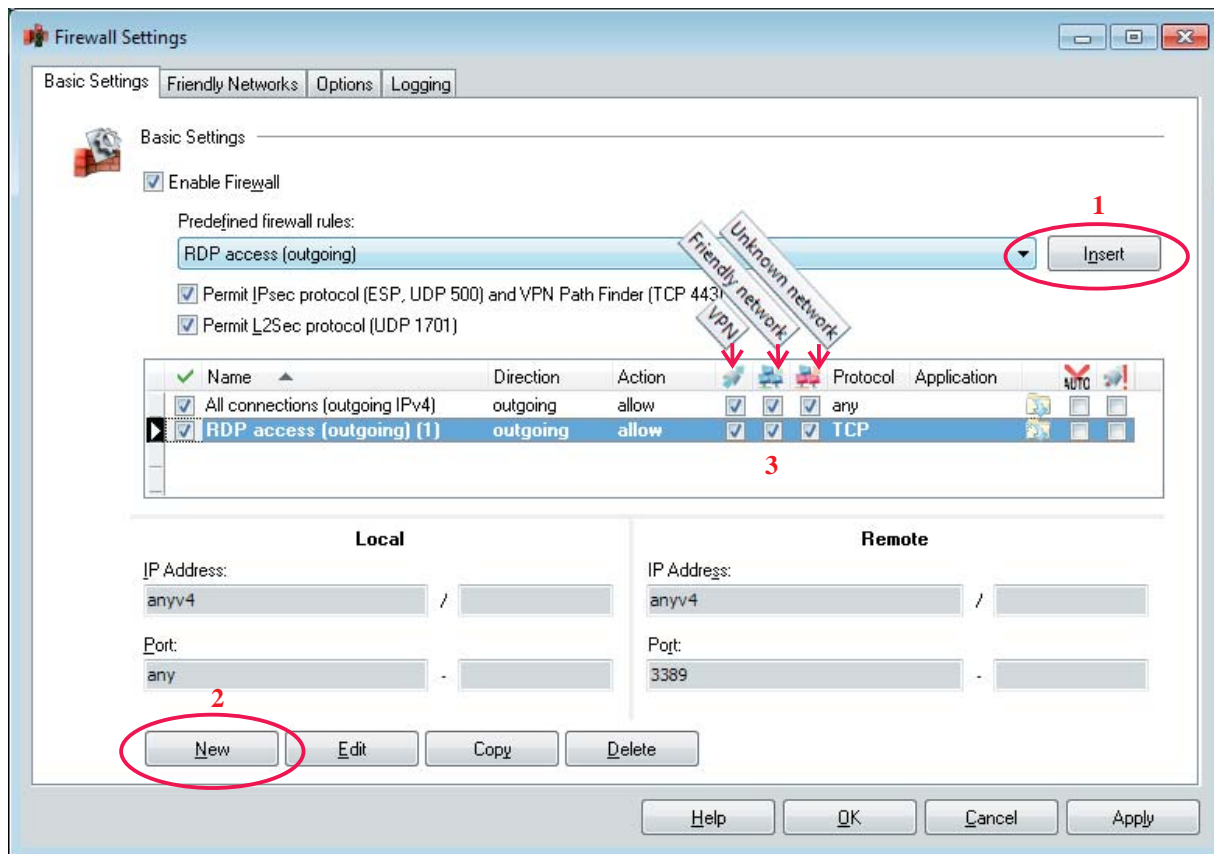


fig. 1

The Personal Firewall enables rule for various types of networks to be inserted (fig. 1, 1) or created (2). This enables the difference to be made between friendly networks (e.g. the company or home network) and unknown networks (all others). (3).

As soon as a network connection using any available media is established, the Client automatically detects the type of network to which it is connected.

Creating a Rule

In order to create a rule for a friendly network, first enable the firewall. This blocks all IP traffic for the time being.

Next, insert the rule (1) and define the direction in which actions will be allowed. Then mark the network to which the rule will apply (3), and finally, store the rule using "Apply" or "OK".

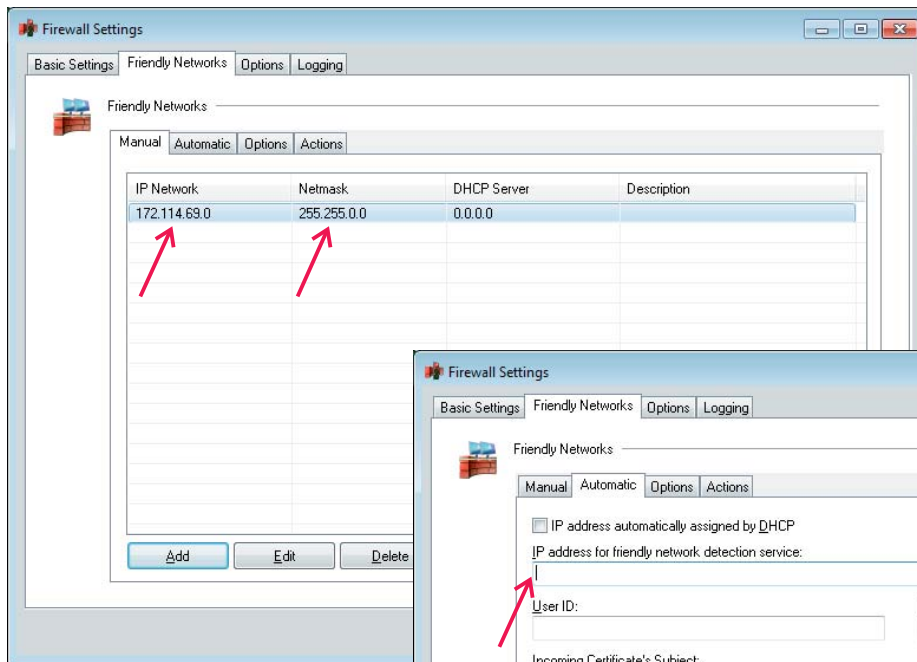


fig. 2

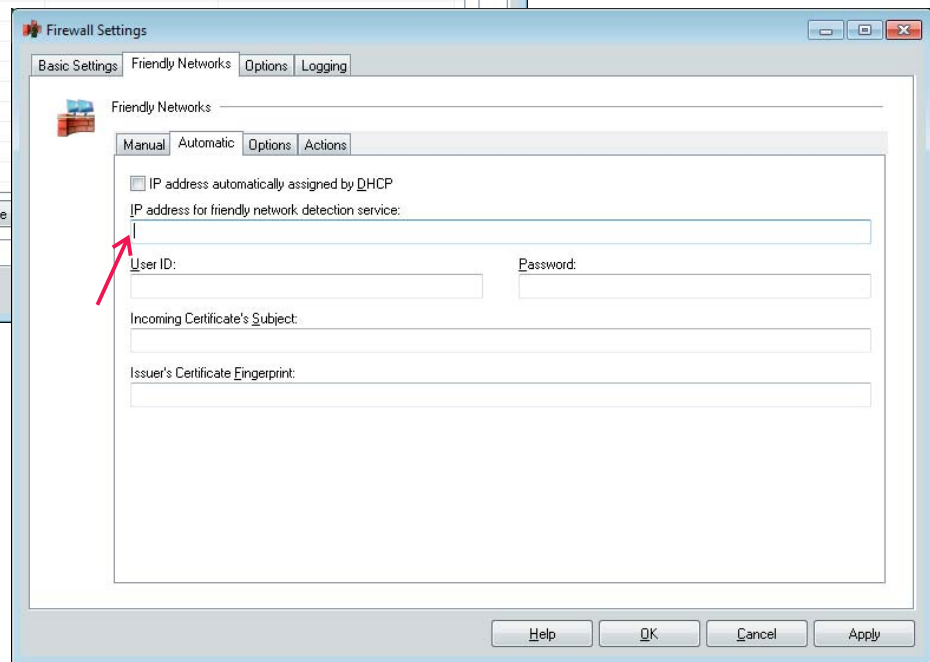


fig. 3

Friendly Network

A friendly network can be defined manually in the Client via either the friendly network's IP address with mask or the IP address of the DHCP server. The Client will then use either of these to detect when it is connected to the friendly network. These parameters are entered in the configuration menu item under "Firewall / Friendly Networks / Manual" (fig. 2).

Automatic Detection of Friendly Networks

Detection of friendly networks can be carried out automatically if a **Friendly Network Detection Server** (FND server) is being used. The FND Server must be accessible from the Client via the "IP address for friendly net detection service", or its DNS name (fig. 3). User-ID, password and, where appropriate, a certificate are stored in the FND server and these must correspond to the values entered here (fig. 3). If the Client can communicate with the FND Server and is authenticated successfully, the network adapter is said to be in the Friendly Network.

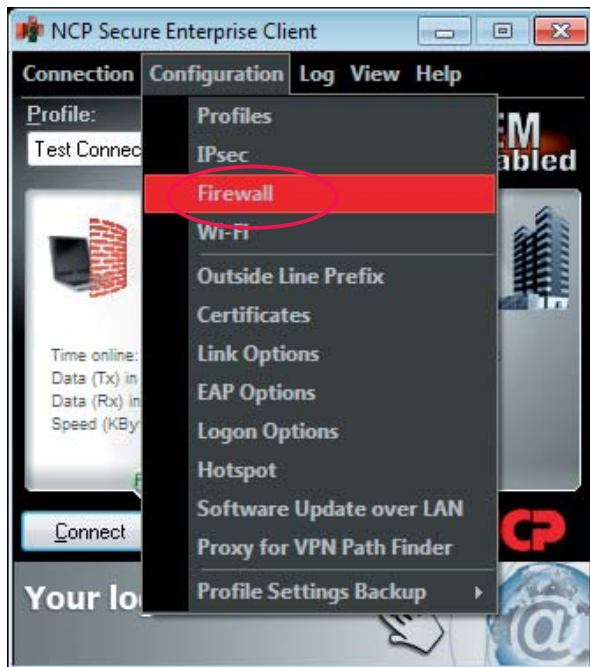
Friendly Network Display in the Monitor



The current location of the Client, i.e. whether or not it is located in a friendly network, is displayed in the monitor and in the Client's tray icon - the firewall symbol is green when located in a friendly network. (fig. left).

Configuration Menu of the Personal Firewall

Open the firewall settings or configuration menu from the Client monitor (see fig. below).



The parameter for the firewall settings are set on four configuration folders some of which feature further tabs:

Basic Settings with predefined Firewall Rules

Creating and Editing the Rules Table

Friendly Networks

Manual Configuration

Automatic Friendly Net Detection

Options

Actions

Options

General

Commands

Logging



Clicking on one of the terms takes you to the corresponding chapter. Clicking on the info icon takes you back to this overview.

All firewall mechanisms are optimized for remote access applications and activated during the computer's boot process.

When the Client's firewall is enabled, the status is recorded in the Windows Vista Security Center or the Windows 7 Action Center. (Windows Vista requires Service Pack 1 as a minimum.) In contrast to VPN solutions with a standalone firewall, the mobile workplace is protected from attack before the VPN connection has been established. Even when the Client software is deactivated, the firewall still fully protects the computer.

All firewall rules can be centrally predefined by the administrator and compliance with them made mandatory. Prerequisite here is the central NCP Secure Enterprise Management (SEM), where the configuration is specified - a configuration that cannot be changed by the user.

Note that firewall settings are global, and therefore applicable to all profiles.

Firewall rules can be changed at any time, it is not necessary to restart the software or reboot the computer.

The firewall settings in the Client monitor's configuration menu enable a precise specification of either application specific or address oriented firewall filter rules in connection with unknown / friendly networks.

When the Client software is updated, any previous firewall settings remain in operation.

When the Client software is installed for the first time on a machine, i.e. a new installation, the firewall will not yet be enabled after the first start of the Client, and no predefined rules will have been selected.

NCP recommendation:

Use the Personal Firewall's global filter capabilities to meet your firewall requirements.

A combination of the global Personal Firewall and the link dependent Firewall (in the link profile **parameter settings**) can be useful in specific scenarios; however, should only be configured by an expert.



Basic Settings and predefined NCP Rules for Test Connections

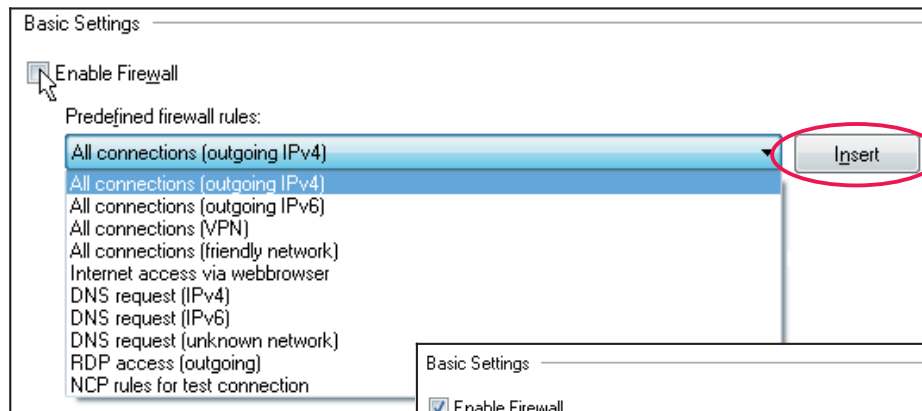


fig. 1

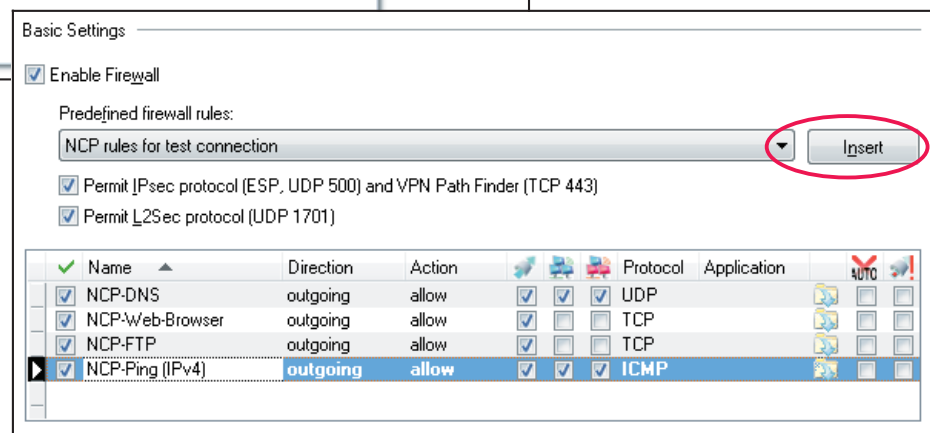


fig. 2



The firewall is enabled by putting a ticking “Enable Firewall”.



As soon as the firewall has been enabled, all IP communication (LAN, printer etc) in the network will be blocked. This happens when no explicit firewall rules have been created or enabled.

Predefined firewall rules can be inserted into the list of rules, as required, using the “Insert” button. The following is a description of the functions of the most important rules

NCP rules for test connection

If, during the installation of the software, the opportunity is taken to setup a test connection (Test Connection IPsec Native), a connection can be established even when the firewall is enabled by inserting the “Predefined firewall rule” “NCP rules for test connection”.

When all the rules for the test connection have been activated and the firewall configuration closed with OK, the profile for the test connection can be used to establish a connection to NCP’s VPN gateway.

Using the predefined rules for test connection, the individual rules illustrated above are inserted into the list (ill. 2).

NCP Rule for DNS Request

The Test Connection profile, automatically created during the installation, contains a Tunnel Endpoint defined with the DNS name “vpntest.ncp-e.com”. Establishment of a tunnel will fail if the NCP-DNS firewall rule is not enabled as the attempt to contact the DNS name server to resolve the DNS name “vpntest.ncp-e.com” will fail.

In order to enable name resolution and allow DNS requests, the following rules are available for use unchanged:

- DNS request (IPv4)
- DNS request (IPv6)
- DNS request (unknown network).

NCP Rules for Web Browser

The NCP rule for web browsers only allows access to the web server via a VPN tunnel to the VPN test gateway (remote IP address 172.16.12.100). In addition, only HTTP (remote port 80) websites are supported, websites with server verification (remote port HTTPS, 443) are not supported. The rule only applies to IPv4 addresses

An additional rule for Internet access via web browser allows access via all networks, also allows HTTPS and applies for both IPv4 and IPv6.

NCP Rule for FTP

The NCP rule for FTP access only allows the connection via a VPN tunnel to the NCP test gateway (remote IP Address 172.16.12.100) via remote ports 20 and 21.

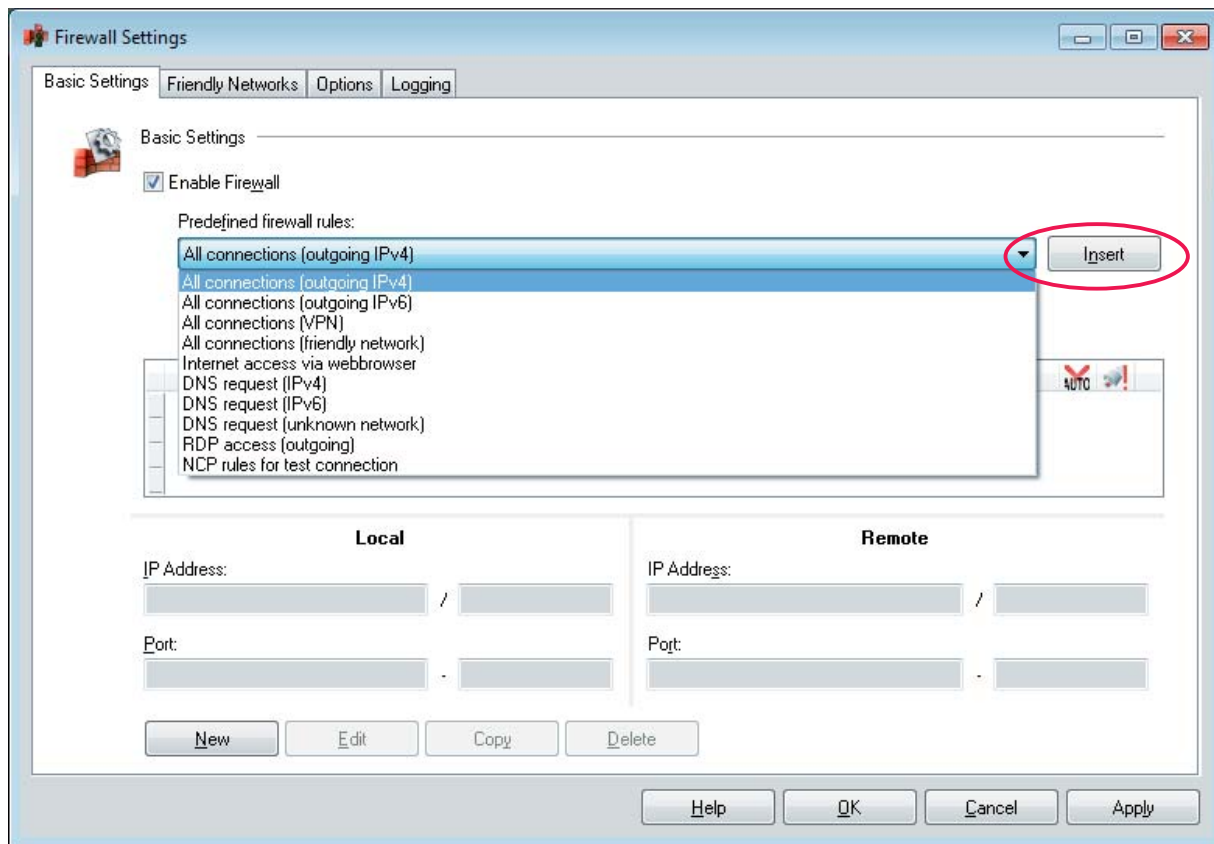


fig. 3

NCP Rule for Ping (IP communications) for Network Diagnosis

If an attempt is made to use network diagnostics to ping the ip address of google.de (74.125.39.106) without an additional firewall rule, this will fail with a timeout (in the Network Diagnostics Information window).

If either of the rules “All connections (outgoing IPv4)” or “NCP-Ping (IPv4)” are activated, an answer will be received from the Internet.



Other predefined firewall rules can be selected as necessary, inserted into the list of firewall rules using the “Insert” button and then edited. (ill. 3 above)

All connections outgoing (IPv4)

Using this rule allows all outgoing connections (IPv4 or IPv6 respectively) from this computer, both via a VPN and in friendly or unknown networks.

All connections (friendly network)

Using this rule, all connections from the computer to and from a friendly network are allowed. In this case access to the computer from the friendly network is also allowed.

All connections (VPN)

Using this rule all connections via the VPN are allowed. In this case access to the computer from the VPN is also allowed!

Internet access via webbrowser



See **the application specific rule example** on page 12.

Rule for Remote Desktop (RDP access)

The firewall rules that allow access to a remote computer (RDP access) is preconfigured for remote port 3389.



The following functions are always active in the default settings, enabling VPN tunnel establishment globally.

Permit IPsec-protocol (ESP, UDP 6) and VPN Path Finder (TCP: 500)

The following protocols and ports, required for tunnel establishment, are enabled via the automatically generated IPsec filter:

- UDP 500 (IKE SAKMP),
- IP protocol 50 (ESP),
- UDP 4500 (NAT-T),
- UDP 67 (DHCPs),
- UDP 68 (DHCPc),
- TCP 443 (VPN Path Finder, when configured)

Creating and Editing the Rules Table

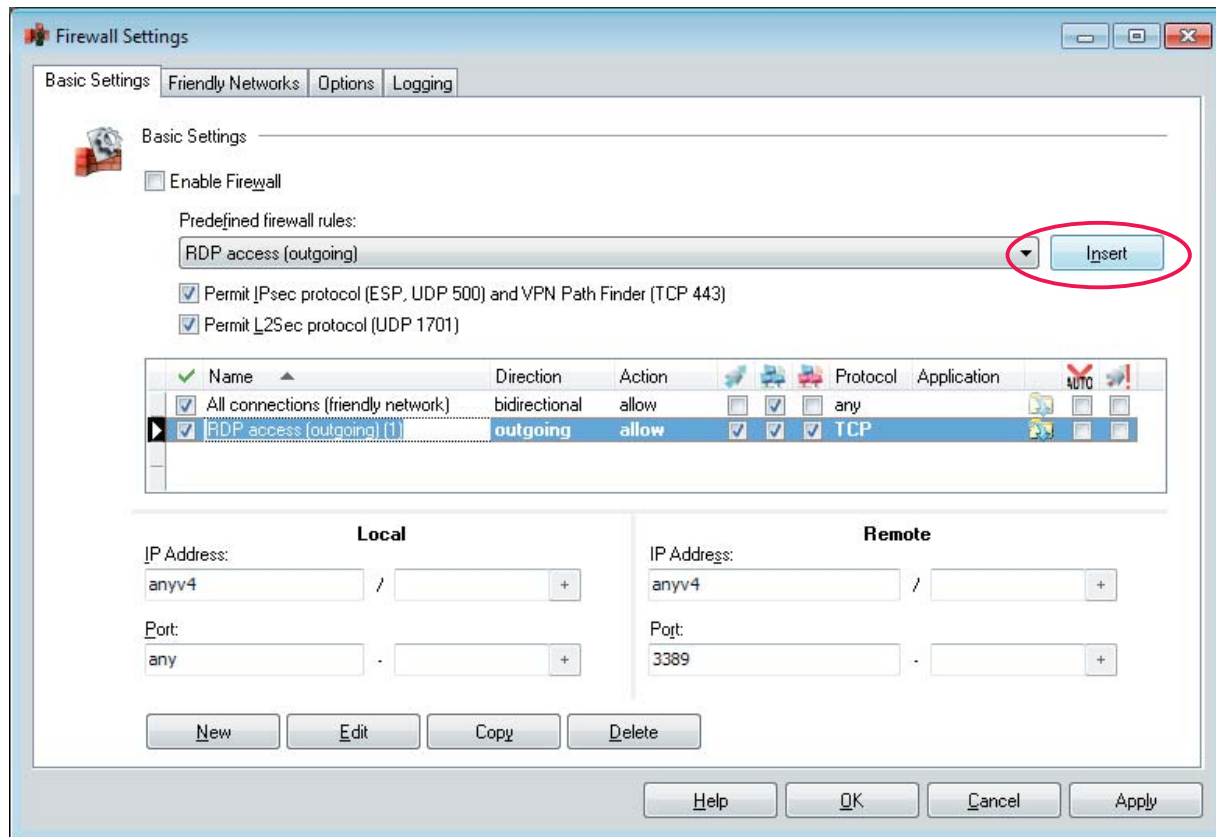


Abb. 4

Permit L2Sec protocol (UDP 1701)

These protocols are enabled for L2Sec:

UDP 1701 (L2TP),
UDP 67 (DHCP),
UDP 68 (DHCP)

Activating this function avoids having to configure individual rules for the respective VPN variants.



Note: This only enables tunnel establishment. If there are no other rules defined for the VPN network and that enable communication in the tunnel, data cannot be transferred through the tunnel.

Editing Rules



In order to create a firewall rule, click on “New” or “Copy”, on “Edit” to change a rule, and on “Delete” to delete a rule.

The edit mode can be switched on either by a double click on the parameter field or on the rule in the table to be edited. Use the tab key to jump from field to field in the rule being edited.

Predefined rules that are inserted into the table are automatically activated. Newly created rules must be enabled manually.

Click on a column heading or symbol to sort the listed rules accordingly.

If a rule is added or changed after the firewall configuration is opened, the “Apply” button is activated. Use “Apply” to transfer the new settings in their entirety to the firewall’s rules database, rather than leaving the firewall configuration by pressing “OK” and then having to re-open the firewall configuration..

The following gives an overview of the column headings and symbols in the rules table, working from left to right. (See: Ill. above from “Name” to “Application”)

Enable

Rules that have been inserted from the predefined list are automatically enabled. Newly created rules must be enabled manually. A rule is only applied to a data packet after that rule has been enabled.

Name

A rule’s name can be changed at any time.

Direction

Use direction to specify whether a rule applies for incoming or outgoing data packets. If the direction is set to outgoing, stateful inspection is used. Stateful inspection is only used for UDP and TCP protocols.

“Incoming” should only be set when connections should be established from the remote side (e.g. for administrator access).

The “bi-directional” setting is only practical if stateful inspection is not available, e.g. for the ICMP protocol (for a ping).

Action

Action is normally set to “allow”.

Only in special cases should action be set to “drop”; such as when in a rule the admissibility for an IP address range or port range has been defined and a second rule defines, for example that an individual address or port should be denied inside that first range. In such a case the second rule for the individual address or port would be set to “drop”.

Friendly network / Unknown network

When creating a rule, at first it is not assigned to any network.

Unknown networks are all networks that cannot be assigned to the categories Friendly. These include for example connections via the Microsoft remote data transmission network, direct or unencrypted connections with the integrated dialer of the Client, as well as hotspot Wi-Fi connections. If a rule must apply for unfriendly networks, this option must be activated.

Friendly networks must be defined under the **Friendly Networks** if this option is to be enabled.

VPN networks are all established L2Sec or IPsec connections. Apart from that, this group covers all encrypted direct dial-in connections via the Client’s integrated dialer. If this rule is to apply for VPN networks this option has to be activated.

No Automatic Connection Establishment

Not active in the default settings (only relevant for dial-up type connections such as GPRS / 3G with automatic connection establishment in the current profile)

This option is only appropriate when, in the profile parameter folder “Line Management”, the connection establishment is set to “automatic”. When this function is

set for a particular rule, automatic connection establishment does not take place for the data packets defined by the rule, however, it does for other data packets.

only valid when the VPN connection is not established

Select this option for the associated rule when, for example, an Internet connection is not allowed to be established over an already established VPN connection, but allowed when in an unfriendly network. In addition, this rule must be used for the “unknown network”, i.e. the rule must allow access to the unknown network.

Protocol

Select the corresponding protocol, dependent on the application or type of connection: TCP, UDP, ICMP, GRE, ESP, AH, IGRP, RSVP, IPv6 over IPv4, ICMPv6, all

Application

Click on the directory symbol to browse to the appropriate directory and select the application that will be used to create the connection. Only this locally installed application, for example Internet Explorer, can communicate. Note the **restrictions**.



Local ports and IP addresses

Those data packets will be allowed through the firewall, whose source address matches the address or address range defined in “Local IP addresses”.

Similarly for IP ports. Data packets that are to be allowed through the firewall must have a source port corresponding to a port or ports defined here.

IP addresses

Under the Local IP address field(s), define which IP address(s) of outgoing packets should be allowed by the firewall. The following entries are valid:

anyv4: allows communication with any IPv4 address from the local side (source address), without restriction.

anyv6: allows communication with any IPv6 address from the local side (source address), without restriction.

specific address: individual addresses can be entered, one under the next, after pressing the “+” button, (different protocol version addresses can also be mixed in the list).

The layout conventions are:

```
123.10.62.1 / 32 (for IPv4)
fd00:6e93:5063:37de:12:16:8005:7a /
128
(for IPv6)
```

Address ranges: two different notations can be used for address ranges.

For IPv4, 32-, 24-, 16-, 8- or other bit masks between 1 and 32 can represent a range to be masked out:

```
123.10.62.1 / 24
correspond to the range (from - to)
123.10.62.0 - 123.10.62.255
```

In the same way, IPv2 address with bit masks between 6 and 1 can represent an area to be masked out:

```
fd00:6e93:5063:37de:12:2c35:987c:2450 / 64
correspond to the range (from - to)
fd00:6e93:5063:37de:: - ...
```

Ports

Under the Local Port entry or entries, define which port(s) can be used on the local system. The following entries are valid:

any: allows communication via all source ports for outgoing packets and all destination ports for incoming packets.

specific port: the ability to define a specific port can be useful when a machine must make a server service available (e.g. Remote Desktop on port: 3389).

port range: can be used when multiple ports are required for a particular rule (e.g. FTP port: 20/21).

Remote ports and IP addresses

Those data packets will be allowed through the firewall, whose source address matches the address or address range defined in "Remote IP addresses".

Similarly for IP ports. The outgoing data packets those are permitted through whose destination port falls under the definition of the remote port.

IP addresses

Under the Remote IP address entry, define which remote IP addresses the system should be allowed to communicate with. The following entries are valid:

anyv4: allows communication with any destination IPv4 address, without restriction.

anyv6: allows communication with any destination IPv6 address, without restriction.

specific address: individual addresses can be entered, one under the next, after pressing the "+" button, (different protocol version addresses can also be mixed in the list).

The notations are:

```
123.10.62.1 / 32 (for IPv4)
fd00:6e93:5063:37de:12:16:8005:7a / 128
(for IPv6)
```

Address range: two different notations can be used for address ranges.

For IPv4, 32-, 24-, 16-, 8- or other bit masks between 1 and 32 can represent a range to be masked out.

```
123.10.62.1 / 24
represents the range (from - to)
123.10.62.0 - 123.10.62.255
```

In the same way, IPv6 address with bit masks between 1 and 125 can represent an area to be masked out:

```
fd00:6e93:5063:37de:12:2c35:987c:2450
/ 64
represent the range (from - to)
fd00:6e93:5063:37de:: - ...
```

Restrictions for Application Specific Firewall Rules



Communication via an application (Browser, Port 80) may be blocked by the firewall if:

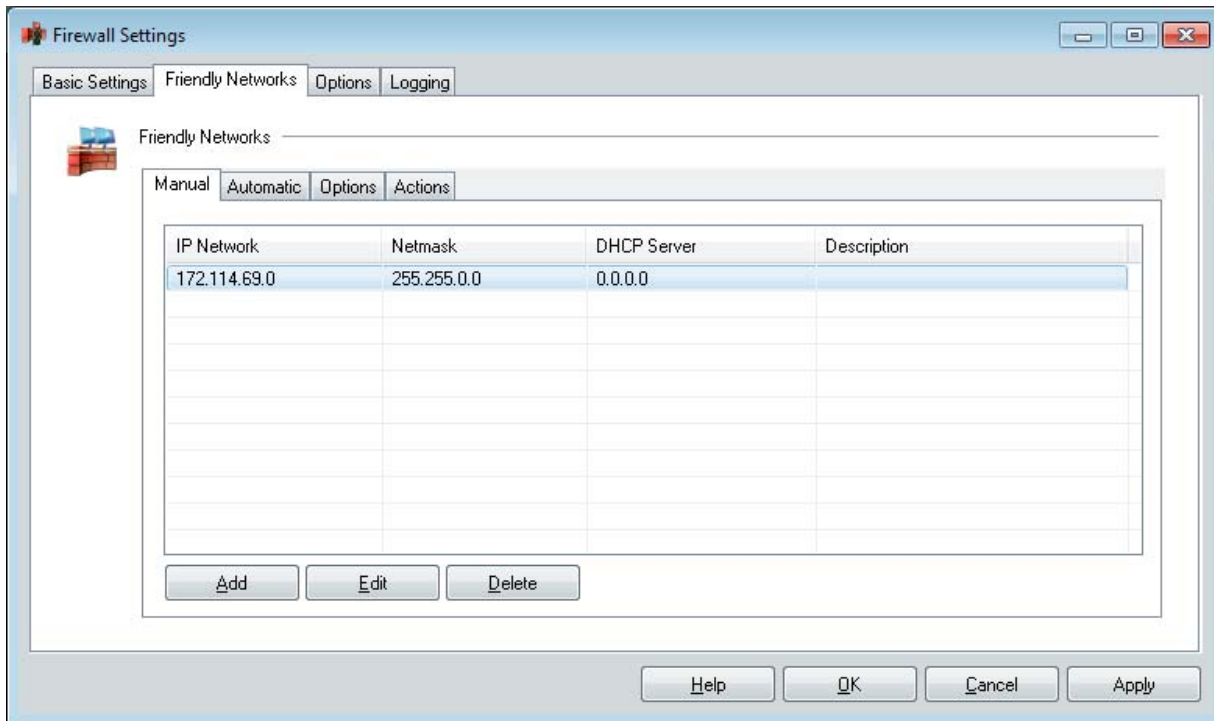
1. A virus scanner is active, working according to the principle of content security.
2. A firewall rule for an application has been configured for a browser via port 80.

Solution:



1. Deactivate virus scanner
2. If only a single browser is used, the virus scanner may remain active provided its exe file is entered in the rule for the respective application. (This rule allows every browser to set up an Internet connection.)

Manual Configuration of Friendly Networks



If a rule is defined in the rule table and that rule is specified for use for communications in a friendly network, that rule will always be used when a network is detected that matches the criteria used to define a friendly network, i.e. the LAN adapter is located in the friendly network.

The administrator centrally defines the friendly networks. This can either be done via manual configuration or via the friendly net detection automatism.

The manual definition of a known network by the administrator and the automatic detection of a known network via friendly net detection are not mutually exclusive, rather they can be used concurrently and they can be configured via the “manual” and “automatic” tabs.

A friendly network is indicated in the monitor by the firewall icon, which changes to green as soon as the Client detects it is located in a friendly network.

In addition, selected actions can be started as soon as the Client detects a friendly net or when friendly net detection fails.

The Client's LAN adapter is located in the friendly net when:

IP Network and Network Mask

- the IP address of the LAN adapter originates from the specified network range. If for example IP network 192.168.254.0 with mask 255.255.255.0 is entered, address 192.168.254.10 will be detected as matching a friendly networks.

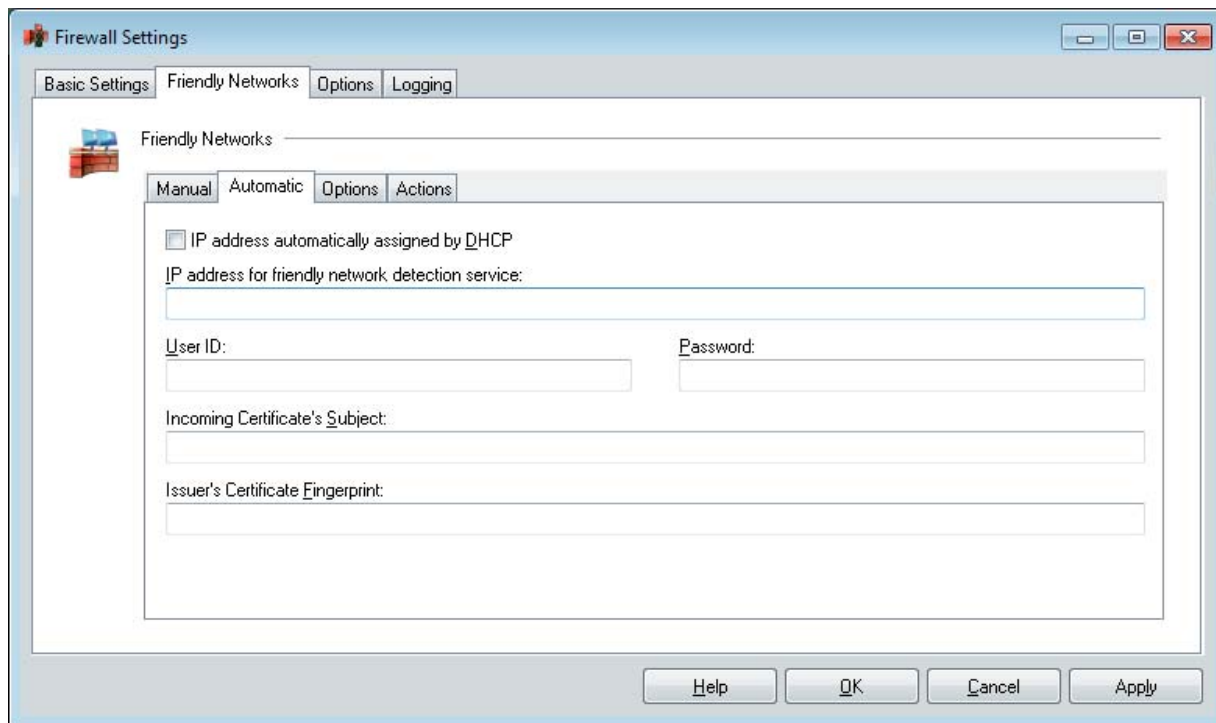
DHCP Server

- the IP address has been assigned by the DHCP server that has the IP address specified here;

The more of these conditions fulfilled, the more precise is the verification that the detected network is a friendly network.

The allocation of an adapter to an unknown or friendly network is automatically logged in the log window of the Client monitor and in the log file of the firewall (see **Logging**), provided this DHCP server has the MAC address entered here.

Activate automatic Friendly Network Detection



What constitutes a friendly net is defined centrally by the administrator. A friendly net is signaled in the Client monitor by the firewall symbol: this is green when the Client is located in a friendly net.

For automatic detection a **Friendly Net Detection Server** is required, located in the network defined as the “Friendly Net” and reachable via IP.

IP address automatically over DHCP assigned

Set this option if the Client will automatically receive the IP address of the FND server via DHCP. It is a prerequisite that a DHCP negotiation has been triggered via the LAN adapter of the Client, in order to automatically receive the IP address for the LAN adapter from the DHCP server. (Default in the operating system’s network settings.)

At the corporate DHCP server a DHCP standard option must be introduced that contains the code 159 and the IP address of the FND server. This option is then distributed via DHCP.

IP address for friendly network detection service

A **Friendly Net Detection Server** is required, reachable via IP. Its IP address must be entered here. The maximum number FNDS IP addresses or hostnames is two and they must be separated by commas.

User-ID, Password (FNDS)

The friendly net detection server is authenticated via MD5 or TLS. The user ID and password entered here have to agree with those that have been stored on the **FNDS**. See also **Authentication with MD5 and TLS**.

Incoming Certificate’s Subject (user)

The incoming certificate of the FNDS is checked for this string. It is considered a friendly network only if there is agreement.

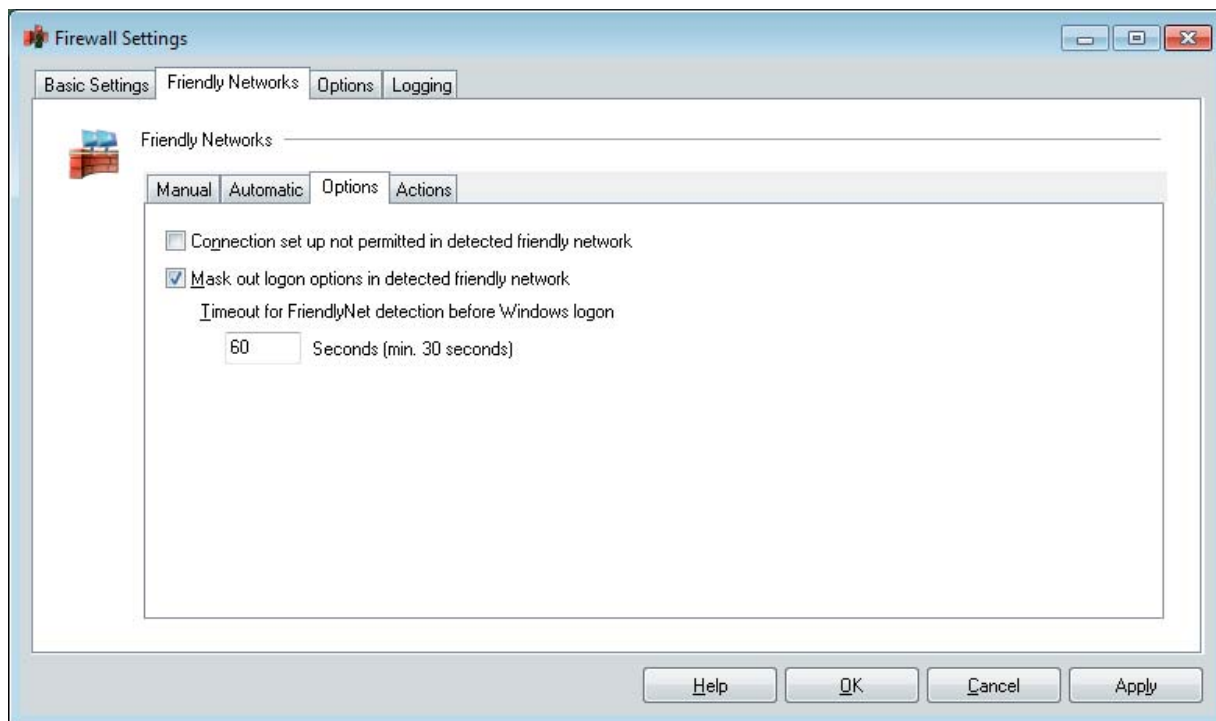
Issuer Certificate Fingerprint

In order to provide the maximum security against counterfeiting, the fingerprint of the issuer certificate has to be verified. It must match the hash value entered here.

Friendly Net Detection via TLS

If the friendly network is to be detected via TLS, (including authentication via the issuer certificate fingerprint), this issuer certificate has to be located in the \CaCerts program directory and its fingerprint has to match the fingerprint configured here. See also **Authentication with MD5 and TLS**.

Friendly Networks / Options



Optionally certain function of a Client, already located in a friendly network, can be grayed out.

Connection set-up not permitted in detected friendly network

By checking this option, you can specify that no additional VPN tunnel can be established when the Client is already connected to a friendly network; the button for connection set-up (or the menu item) in the Client Monitor is deactivated. However, any existing VPN connection, perhaps established by a different application, can be disconnected.

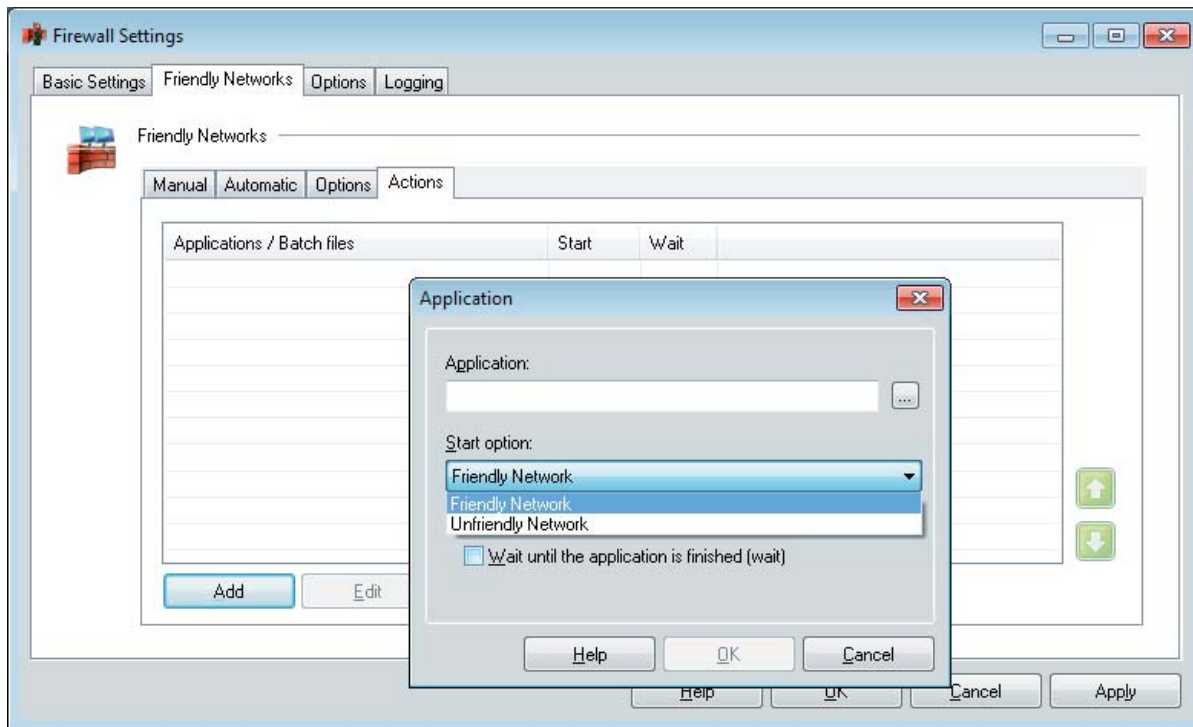
Mask out logon options in detected friendly network

If the Client is already connected to a friendly network the logon options for domain logon can be hidden.

Timeout for Friendly Network Detection before Windows Logon

The time span for automatic friendly net detection can be entered independently from the timeout value. The value for the network search time has to be at least 30 seconds. (The default value is 60 seconds.)

Friendly Networks / Actions



As soon as a Client detects the change from friendly to unknown network (or vice-versa), a dependent action can be started. For example, an external program or batch file could be started that changes the Windows system proxy settings.

Application / Batch file

Click “Add” and then select either an application or a batch file (*.com, *.exe, *.bat).

Start option

The application / batch file can be started when the Client has detected a friendly network or the network adapter is located in a friendly network.

The selected application / batch file could also be started when the Client can not detect a friendly network or the network adapter is not located in a friendly network.

Wait until the application has run to completion and terminated (wait)

The applications and batch files will be started, dependent on the start option, in the sequence in which they are listed in the actions overview table, i.e. the sequence of those for a friendly network or for an unfriendly/unknown network.

The execution of applications (*.com and *.exe) in the corresponding sequence can be halted with the Wait function, i.e. the next application will only be started when the action marked with the Wait function has been deliberately terminated by the user.



Please note the following when creating batch files:

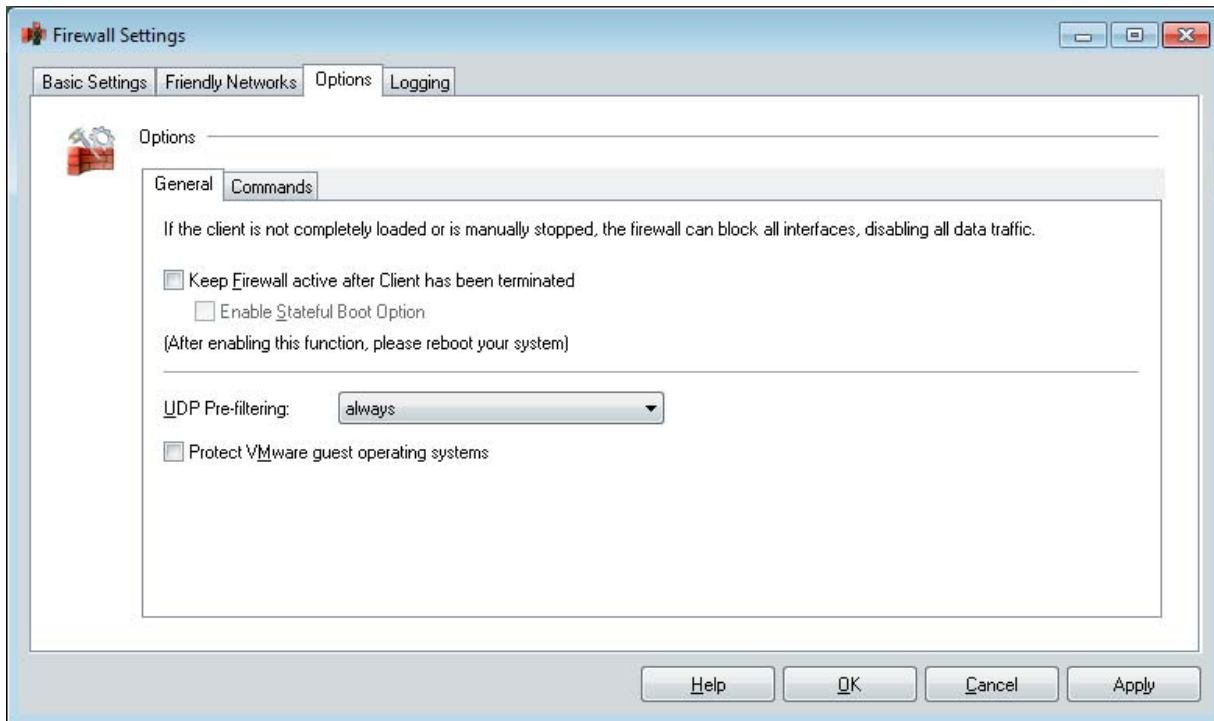
The Wait function will only work with a batch file when that batch file has an error, e.g. halts prematurely, that makes it unable to correctly execute all the commands in the batch file. If, in this case, the Wait function is set, then the batch file must first be manually terminated before the subsequent application/batch file in the list will be started. In such a case, the user must be informed by suitable feedback from the batch file.

Overview table for Applications / Batch files

Initially, actions are listed in the overview table in the sequence in which they were created. Use the green arrows at the bottom RH border to alter the sequence of the actions.

In order to improve the overview, group all the actions together, one after the other, according to whether they will be started on detection of friendly or unknown (unfriendly) networks.

Options / General



Under the “General” tab, the firewall can also be enabled when the Client has not been started.

Keep Firewall active after Client has been terminated

Enable this option if the firewall is to be kept active even when the Client is stopped. In this state each incoming and outgoing communication is suppressed and no data can be communicated, as long as the Client is stopped. If this function is not enabled when the Client is stopped, the firewall will also be deactivated.

Enable Stateful Boot Option

If the firewall is to be kept enabled, even when the Client is stopped, Stateful Inspection can be switched on using this function, enabling communication between the computer and another network.



This setting is only activated after a restart of the services (reboot).

UDP Pre-Filtering

In the default setting, when the Client is running (independent of the firewall) UDP packets are filtered out and so that a connection to the Client computer from the outside is disabled. If a server type application that uses UDP data transfer (e. g. terminal applications or NTP) has been started on the Client computer, this default setting has a disruptive effect on data communication. Consequently this default setting can be switched off or it can be limited to UDP packets from unknown networks.

always

Default setting. No UDP packets reach the Client PC.

only for unknown networks

UDP filtering discards all packets from unknown networks.

off

If the filter is switched off, all UDP packets reach the Client PC. This setting should only be used if problems occur with an application.

Protect VMware guest operating systems



A VMware guest system can be protected by a Client installed in the host system, if the firewall is activated. This means that the firewall of the Client has to be active in the “Basic Locked Settings” or that at least one firewall rule is active in the “Basic Open Settings”. The guest system cannot then receive incoming connections. VMware supports various networking modes for the guest system:

Bridged, NAT and Host Only. If Host Only Mode is used then, independent of the firewall, the guest can always communicate bidirectionally with the host system.

Bridged Mode

When in bridged mode and with the option “Protect VMware guest operating systems” enabled, the guest system is completely sealed off. Communication between the guest system and the Internet is blocked, this includes DHCP requests.

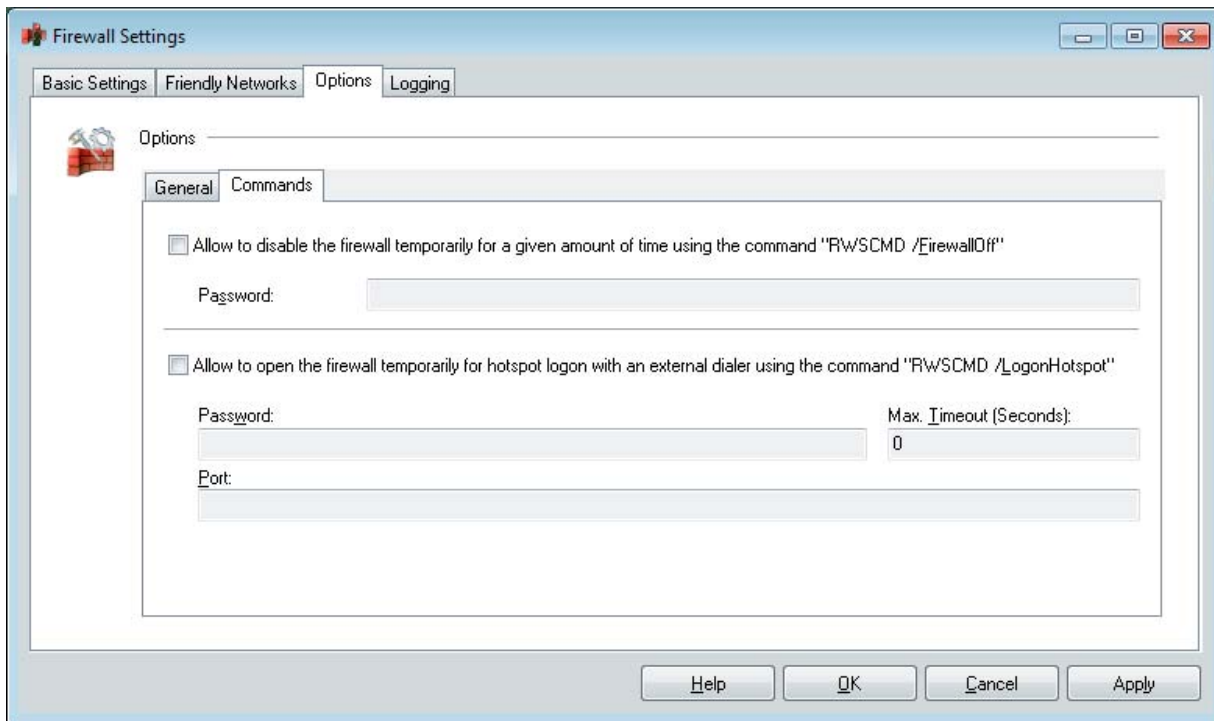
When enabled, bidirectional communication between guest system and host system will still be possible.

Nat Mode

When in NAT mode and with the option “Protect VMware guest operating systems” enabled, the configurable firewall rules apply to outgoing connections. Incoming connections cannot, however, be established.

When enabled, bidirectional communication between guest system and host system will still be possible.

Options / General



The firewall can be temporarily disabled for a period of time.

If it is to be possible to temporarily open the firewall via the command line, this function has to be activated. In this case, entering a password is optional. If a password has been entered it has to be repeated in the command line. The command is:

```
rwscmd /firewalloff [Passwort] [Timeout]
```

A timeout can be set in the command line in seconds (whole-numbers). The firewall is enabled again if either the timeout has been counted down or after the command:

```
rwscmd /firewallon
```

The firewall can be opened temporarily for hotspot login with an external dialer.

If the firewall is to be opened with an external dialer this function has to be activated in this tab. In this case, entering a password is optional. If it is entered, it must also be entered at the command line.

Input of the "Max. Timeouts" is optional. The value entered in this field is for limiting the timeout which has to be set in the command line.

Further ports, apart from the default ports 80 and 443 which are automatically opened for hotspot login, are opened if they are entered in this field. Several ports are separated from each other by using a comma. The command is:

```
rwscmd /logonhotspot [Passwort] [Timeout]
```

The timeout set by the user can never exceed the timeout set in the command settings of the firewall.

The firewall is enabled again if either the timeout has been counted down or after the command:

```
rwscmd /firewallon
```

Allow Hotspot Logon with External Dialer

If this function is activated, then hotspot logon can be executed via an external dialer. You have to call the command line interface `rwscmd.exe` for this. With the command

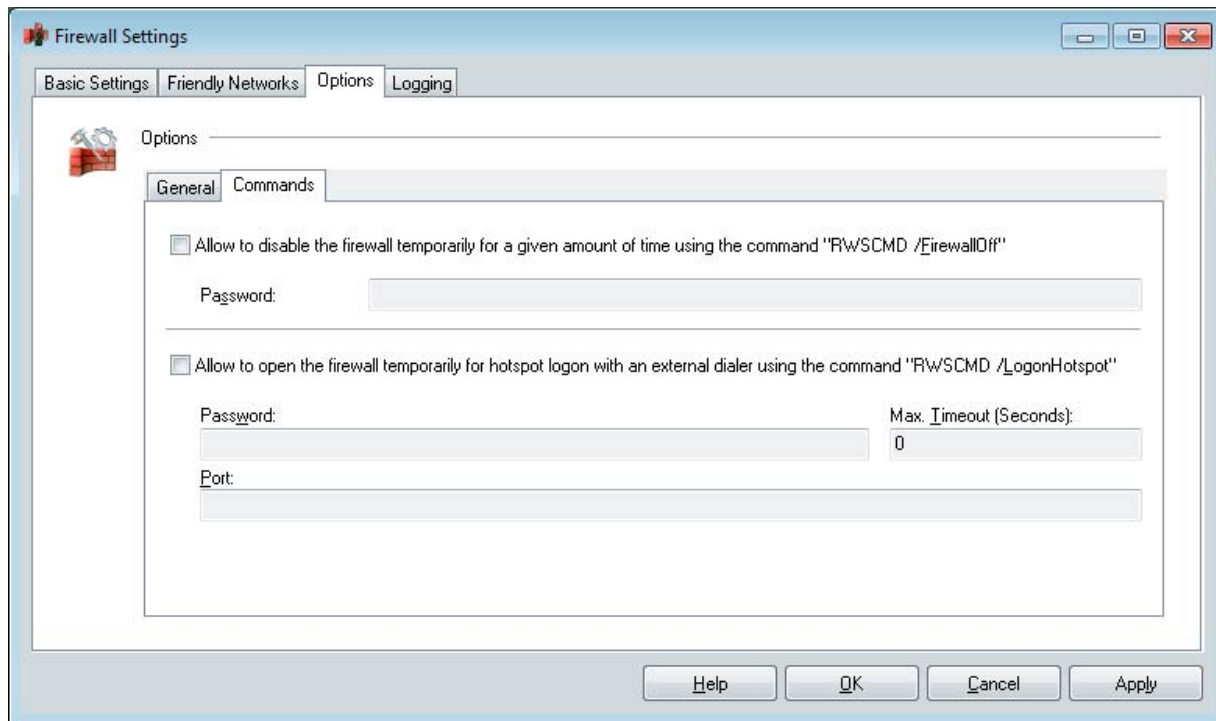
```
rwscmd /logonhotspot [Timeout]
```

the firewall is released for ports 80 (HTTP) and 443 (HTTPS). This generates a dynamic rule that allows data traffic until the transferred timeout (in seconds) has elapsed.

Ports

Separated by commas, further ports (up to 10) can be added. They will be opened for hotspot logon additionally to the ports 80 and 443.

Logging



Enable firewall log



The activities of the firewall are written to log file depending on the setting. The default location of the log files is in the installation directory under log\.

The log files for the firewall are written in pure text format and are named Firewallymmdd.log. They contain a description of “rejected data traffic” and/or “permitted data traffic”. If neither of these options has been selected, only status information on the firewall is logged.

The log files are written at each start of the firewall. The maximum number is maintained in the log directory, as has been entered in “days of logging”.

Please note that active logging decreases the performance, because for each packet corresponding to this setting a log text has to be written.

Installation and Configuration of the FND Server

The free of charge software for the NCP Friendly Net Detection Server can be received upon request from the NCP support.

The NCP FND Server for Windows can be installed under Microsoft Windows Server 2003 or Windows Server 2008.

Prerequisite: administrator rights are required for installation, operating and deinstallation.

Installation: The software is installed by executing the file

```
NCP_FndSrv_Win32_100_004.exe
```

The program files are copied to

```
<program>ncp\FndServe
```

The NCP FND Server is installed in the Windows system as NCP Secure Friendly Net Detection Service (ncpfnd) and started immediately. The FND is then started automatically after every reboot.

The NCP FND Server for Linux can be installed under either SuSe or Red Hat (but NOT under Ubuntu or Debian).

Prerequisite: The user must have root privileges (for installation, operation and deinstallation).

Installation: Call the self-extracting install script (set execute permission on the file as appropriate):

```
./ncp_fnd_linux_100_001.i386.sh [u]
```

During an unattended installation, i.e. with the “u” option, the installation is carried out without user intervention and files are copied to /usr/local/fnd:

The daemon is integrated into the SysV init process.

In this standard configuration the daemon is always started automatically after a reboot.

If the install script is not started with the unattended installation option, the user must respond to various prompts during the installation. Also, the FND server must be started manually after every reboot:

```
rcncpfnd start
```

Configuration of the FND Server

The FND server is configured via entries in the file `ncpfnd.conf`, located in the installation directory. It is split into various sections

[General]

The most important parameters for the FNDS are defined in this section.

```
LogLevel = 0
LogPath = .\log
Port = 12521
#LocalIpAddress = 192.168.1.1
Pkcs12FileName = .\vpngw.p12
Pkcs12Pin = 1234
```

LogLevel

Usually the LogLevel is set to "0" so that no log texts are written. Log messages are only required for maintenance purposes.

LogPath

The LogPath is the current directory of the FNDS software. It is only required for maintenance purposes.

Port

Port 12521 is pre-set as default port for the FND service and should not be changed.

LocalIPAddress

LocalIpAddress, the local IP address does only have to be entered if the computer has multiple IP addresses and it should only respond to the entered IP address. In the default setting the IP address is replaced with "#". If an IP address is entered here, it has to agree with one of the IP addresses that have been used in the firewall setting of the Client under "Friendly Networks" as the "IP address of the service for detection of friendly networks" (see below "configuration of the Client"). This means that this FND server needs to be reached with the IP address specified in the Client configuration.

PKCS12FileName

Pkcs12FileName is the filename and path of the soft certificate (PKCS12 Certificate). This certificate is used for key generation purposes (SSL or

TLS). The soft certificate "vpngw.p12" is only used for test purposes, is delivered with the software and is located in the installation directory. It should be replaced by a company specific certificate. Please note that the issuer certificate has to be imported into the Client's installation directory under \CaCerts. The test issuer-certificate which comes standard with the Client Software is located in the installation directory of the NCP software and is named ncpsupportca.pem. Both NCP certificates, vpngw.p12 and ncpsupportca.pem, are only for test purposes.

PKCS12Pin

Pkcs12Pin has to be entered as the PIN of the certificate stored here. The PIN "1234" only applies for the NCP test certificate.

[SysLog]

After configuration of this section, log messages can be transferred to a Syslog server.

```
Host = 192.168.1.1
Port = 514
LogEnabled = 0
LogFacility = 24001
TraceEnabled = 0
TraceFacility = 24002
```

As default, the Syslog Server (with the specified IP address) is addressed via the UDP port 514. The messages are generated if LogEnabled and / or TraceEnabled are set to "1". The log files are identified on the Syslog Server via LogFacility / Trace Facility.

[FND-USER 1]

This section in the sample configuration specifies the authentication protocol MD5. This means that User ID and Password in the firewall settings of the Client have to agree with the user ID and password entered here.

```
Enabled = 1
UserName = testmd5
Password = testmd5
EAP-TYPE = MD5
#IP-Range1 = 192.168.1.2-192.168.1.127
#IP-Range2 = 192.168.1.128-192.168.1.254
```

Enabled

Authentication is “Enabled” (switched on) via MD5 by setting “1”. With “0” authentication is switched off for this section via MD5.

User-ID

“User ID” corresponds to the parameter **User ID** in the firewall settings of the Client under the tab “Friendly Networks”.

Password

“Password” corresponds to the parameter **Password** in the firewall settings of the Client under the tab “Friendly Networks”.

EAP-Type

Choose either of the authentication protocols, MD5 and TLS, as “EAP type”. If the MD5 protocol is selected as EAP type, user ID and password have to be entered as described above.

Forming Groups

Group formation can be carried out via the correspondence of user ID and password with those in the firewall settings of the Client. This is done by duplication of the section above of the configuration file [FND-USER 1] and by entering other placeholders in the duplicated section for user ID and password, which then also have to be transferred accordingly into the configurations of the Clients in this group.

**IP range**

The IP range describes the IP address that the FND server will accept. This can be individual IP addresses or address ranges. If these ranges commented out with “#”, all addresses from the LAN are accepted.

[FND-USER 2]

This section in the sample configuration specifies TLS as the authentication protocol. This means that the user ID in the firewall settings of the Client has to agree with the user ID entered here. The password is not required.

In addition, for authentication via TLS the issuer certificate or all certificates, necessary for validation of the FNDS certificate, have to be available to the Client. Moreover the fingerprint of the issuer certificate and the subject of the FNDS certificate can be configured. This prevents a hostile recreation of the friendly network (see below “Configuration on the Client”).

```
Enabled = 1
UserName = testtls
EAP-TYPE = TLS
#IP-Range1 = 192.168.1.2-192.168.1.127
#IP-Range2 = 192.168.1.128-192.168.1.254
```

Enabled

The authentication is “enabled” via TLS by setting the “1”. Setting “0” the authentication is disabled for this section.

User-ID

“User ID” corresponds to the parameter “User ID” in the firewall settings of the Client under the header “Friendly Networks”.

EAP-Type

Choose either of the authentication protocols, MD5 and TLS, as “EAP type”. If the TLS protocol is selected as EAP type, simply enter a user ID, as described above.

IP range

The IP range describes the IP address that the FND server will accept. This can be individual IP addresses or address ranges. If these ranges commented out with “#”, all addresses from the LAN are accepted.

Configuration of the Client

The prerequisite for the use of friendly net detection is installation of the FND Server in a network that has been declared as a friendly network. This service has to be reachable from all ports of the network, i.e. firewall rules may have to be changed.

If an employee operates his end device directly on the corporate network, the Secure Client (that has been configured for automatic friendly net detection) attempts to contact the configured FND Server. If the FND server is reached and authenticated, the system confirms that the computer is located in a friendly network and the appropriate firewall rules, pre-configured for this network, are activated automatically.

For the description below, please also refer to the configuration example **Automatic Adaption of Firewall Rules in Friendly Networks**.

Basic Settings

The NCP Secure Client's integrated Personal Firewall facilitates an extremely flexible organization of firewall rules. If the firewall is enabled in the **Basic Settings** all IP communication with the network is inhibited.

Filter Rules

Using **predefined or individually defined rules**, the firewall can be opened for communication with certain subnets. In all cases, blocking rules (e.g. port 80) can not be overwritten by unblocking rules (e.g. ports 60 - 180), i.e. made inactive.

The criteria that are specified in the security policy precisely define what a user is authorized or not authorized to do from the computer in a network e.g. Intranet, central data network (corporate network), Internet etc. The Security Policy is usually created and maintained by the network administrator.

Authentication with MD5 and TLS

In order to activate "Automatic Friendly Net Detection", select the appropriate function in the firewall settings under the header **Friendly Networks**.

The illustration below shows an MD5 configuration. Please also compare the section **[FND USER 1]** for server configuration.

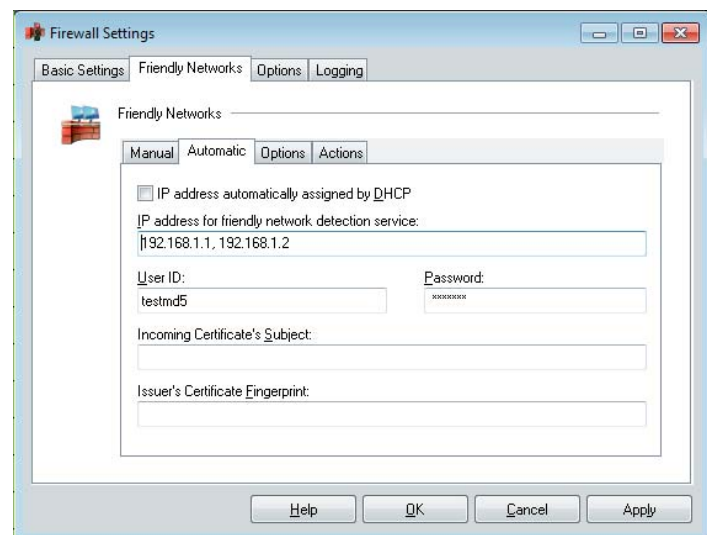
IP address for friendly network detection service

The IP address of the Friendly Net Detection Server (FNDS) corresponds to the **LocalIpAddress** in the section "General" of the configuration file `ncpfnd.conf`.

To increase redundancy the IP address of a second FND server can be entered after a comma. In this case, ensure that the appropriate configuration file `ncpfnd.conf` is also available on the second FND Server.

If the Client is located in the friendly network, it attempts to reach the first FND server, three times in 3-second intervals. If contact cannot be established, the second IP address is selected (See **NCP Friendly Net Detection**).

MD5 Configuration



User-ID, Password (FNDS)

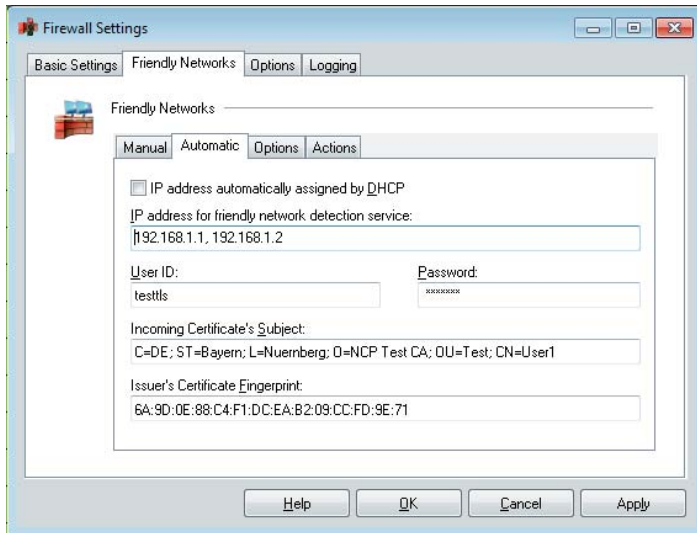
The friendly net detection server is authenticated using MD5 or TLS*. The user ID and password entered here, have to agree with those stored on the FNDS. When using MD5, authentication is carried out against "User ID" and "Password". When using TLS a password is not required.

* Using Friendly Net Detection, EAP over UDP is used for MD5 as well as TLS.

“User ID” and “Password” correspond to **User ID** and **Password** in the sections “FND User 1” and “FND User 2” in the configuration file, ncpfnd.conf.

The illustration below shows a TLS configuration. Please also compare the section **[FND USER 2]** for server configuration.

TLS Configuration



Incoming Certificate's Subject (user)

The incoming certificate of the FNDS server is checked for this string or the section of the string entered here. This string of characters must not end on a semicolon “;”.



Only if there is agreement, the connected network is detected as a friendly network. The appropriate issuer certificate or all certificates necessary for validation of the incoming FNDS certificate have to be available on the Client in the installation directory under “CaCerts”.

Issuer Certificate Fingerprint

In order to offer maximum security against counterfeiting, you can specify that the fingerprint of the issuer certificate, located in the installation directory of the Client under \CaCerts, has to be checked. It must match the hash value entered here.

Starting the NCPFND Service

Under Windows

The NCPFND service has to be listed in the “Services” administration of the system as auto start type “Automatic”. Then it starts automatically after a boot process of the PC.

The service can also be started and stopped manually with the commands:

```
net start ncpfnd
and
net stop ncpfnd
```

Deinstallation

To deinstall the service, use the command:

```
ncpfnd -remove
```

Under Linux

If the install script is not started with the unattended installation option, the user must respond to various prompts during the installation. Also, the FND server must be started manually after every reboot.

start the daemon manually:

```
rcncpfnd start
```

stop the daemon manually:

```
rcncpfnd stop
```

display status of the daemon:

```
rcncpfnd status
```

Deinstallation

To deinstall the service, use the command:

```
ncpfnddeinstall
```

Test

Use the program fndtest.exe to test the respective type of authentication that has been set in the configuration file, without having to install a Secure Client.

For this specify the authentication type after the command, and specify the Client parameters as described above. The following syntax is used:

```
fndtest md5 [Username] [Password] [FND Server]
fndtest tls [Username] [FND Server]
```

Index

Action	20	Friendly Network / Unknown Network	20
All Connections (outgoing) / Rule for Ping (IP Communication) for Network Diagnostics	18	Friendly Networks / Actions	25
Allow All Connections in Friendly Network	18	Friendly Networks / Automatic	23
Allow all Outgoing Connections	18	Friendly Networks / Manual	22
Allow Hotspot Logon with External Dialer	28	Friendly Networks	15
Application	20	Functions of the Firewall	6
Applications / Batch Files	25	Incoming Certificate's Subject (user)	23
Apply Rule to Following Networks	20	Internet Access via Webbrowser	18
Authentication with MD5 and TLS	32	IP address automatically assigned by DHCP	23
Authentication	10	IP address for friendly network detection service	33
Automatically Friendly Net Detection	15	IP addresses	20
Basic Settings and predefined rules	17	IP Network and Network Mask	22
Batch File	24	IP-Range	32
Commands	28	Issuer's Certificate Fingerprint	23, 34
Configuration Folder Friendly Networks / Actions	25	Keep Firewall active after Client has been terminated	26
Configuration Folder Friendly Networks / Automatic	23	Line Management	20
Configuration Folder Friendly Networks / Manual	22	Local IP Addresses	20
Configuration Folder Logging	29	Local Ports	20
Configuration Folder Options / Commands	28	LocalIPAddress	31
Configuration Folder Options / General	26	LogLevel	31
Configuration Menu of the Personal Firewall	16	LogPath	31
Configuration of the FND Server	31	MD5 Configuration	33
Creating a Firewall Rule	18	Mode of Operation of Friendly Net Detection	9
Definition of Friendly Networks	9	NCP Dynamic Net Guard	5
DHCP Server	22	Password	32
Direction	18	PKCS12FileName	31
Display of the Firewall Settings	8	PKCS12Pin	31
DNS Request (unknown Network) / Rule for DNS Requests for Network Diagnostics	17	Port	31
EAP-Type	32	Ports	21
Enable Firewall	17	Predifined Rules	17
Enable Firewall Log	29	Principle of Friendly Net Detection	10
Enable Stateful Boot Option	26	Protect VMware guest operating systems	27
Example: Adapting automatically firewall rules in friendly networks	14	Protocol	21
Example: Client Firewall with application dependent rule	12	RDP Access / Rule for Remote Desktop	18
Example: How to surf the Internet by using the Internet Explorer	12	Remote IP Addresses	21
Filter Rules	33	Remote Ports	21
Firewall Settings	8	Restriction	21
Friendly Networks	15	Rule Name	19
Friendly Net Detection and Stateful Boot Option	7	Security Policy	9
Friendly Net Detection via TLS	23	Setting up a Rule	14
Friendly Network Display on the Monitor	15	Starting the NCPFND Service	34
		Subject of the Incoming Certificate	34
		Test	34
		TLS Configuration	34
		UDP Pre-Filtering	26
		Uninstalling	34
		User ID, Password (FNDS)	23, 33
		UserName	32
		Wait Function	2 5