NCP Friendly Net Detection Server

Administration Guide

Next Generation Network
Access Technology

www.ncp-e.com

Contact

For more information or questions about NCP products and services:

Germany
NCP engineering GmbH
Dombühlerstraße 2
D-90449 Nürnberg
Tel.: +49 (911) 9968 0
Homepage: http://www.ncp-e.com
Mail: info@ncp-e.com

E-Mail Support:
support@ncp-e.com (german)
helpdesk@ncp-e.com (english)

Contact USA, North American HQ
NCP engineering, Inc.
678 Georgia Ave.
Sunnyvale, CA 94085
Phone: +1 (650) 316-6273

East Coast Office
601 Cleveland Street, Suite 501-25
Clearwater, FL 33755

Support Hotline:
0900 / 1 99 68 00
(only available from Germany, 80 Cent / per minute)
Our support times are from monday to friday from 08:00 am to 17:00 pm.

For a support request we need the following information:
- exact product name
- serial number
- version number
- precise description of the problem
- any error message(s)

NCP Friendly Net Detection Server

While considerable care has been taken in the preparation and publication of this manual, errors in content, typo-graphical or otherwise, may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP. 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 suitability of use for any particular purpose.
Furthermore, NCP reserves the right to revise this publication and to make amendments to the contents, at any time, without obligation to notify any person or entity of such revisions or 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. All trademarks or registered trademarks appearing in this manual belong to their respective owners.

Table of contents

Friendly Net Detection Server

Friendly Net Detection is a feature of the NCP Secure Client Software for the universal use in any remote acces and communication environment. Individual firewall rules of the personal firewall of the NCP Secure Enterprise VPN Client can be activated for different network states. Firewall rules can be configured so that they are only applied in networks defined as "known". The detection of known networks is performed by definition in the client configuration or automatically by communication with a Friendly Net Detection Server (FND server).

The FND is a client-server application. Since the FND server is a service to be installed separately, which is completely independent of the VPN gateway, it can be installed on any permanently accessible computer within the network.

Installation of the FND Server

Requirements

The FND server for Linux works on common Linux distributions. An overview of the officially tested and released operating systems can be found in the current release notes of the FND server.

Linux Installation

See NCP Linux Admin Guide.

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

Configuration of the FND Server

Configure the FND Server by editing the configuration file ncpfnd.conf which is divided into different sections.

Commenting out with "#" is possible in the configuration file, but note that it can't be used for parameter values. The editings in the configuration file will be active after a reboot of the FND services.

[General]

The most important parameters for the FND service are described in this section.

```
LogLevel          = 10
LogPath           = /var/log/ncp/fnd
Port              = 12521
#LocalIpAddr            = 192.168.1.1
```

```
# either an absolute path or a path relative to the directory where this file resides
Pkcs12FileName     = server1-rsa-2050.p12
Pkcs12Pin          = crypt:d40d17329a977f93
```

LogLevel

Usually the LogLevel is set to "10" so that no log texts are written. Log messages are only required for maintenance purposes.

LogPath

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

Port

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

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 commented out with "#", the server is set to listen on all IP addresses. 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". 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. The soft certificate "*server1-rsa-2050.p12*" is only used for test purposes only. It is delivered with the software and is located in the installation directory. It should be replaced by a company specific certificate. Please note that a matching issuer certificate has to be available on the client side. The test issuer certificate which comes with the Client Software is located in the installation directory of the NCP software and is named "ncpsupportca.pem".

PKCS12Pin

This specifies the PIN required to access the certificate information of the p12 file. The PIN is saved in the configuration file. As soon as the FND service loads the configuration the PIN is encrypted. A crypted PIN is visualized by the `crypt:` tag.

[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.

Authentication Protocol MD5

[FND User 1]

This section in the sample configuration specifies the authentication protocol MD5. This means that user name and password in the firewall settings of the client have to agree with the user name 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.

UserName

"UserName" corresponds to the parameter Username in the firewall settings of the client under the tab "Friendly Networks" under "automatic".

Password

"Password" corresponds to the parameter Password in the firewall settings of the client under the tab "Friendly Networks" under "automatic".

EAP-Type

You can choose between the authentication protocols MD5 and TLS as "EAP type". If the MD5 protocol is selected as EAP type, user name and password have to be entered as described above.

Forming Groups

Group formation can be carried out via the correspondence of user name and password with those in the firewall settings of the client. This is done by duplication of the section above 6 of the configuration file and by entering other placeholders in the duplicated section for user name 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 addresses that the FND Server accepts. These can be individual IP addresses or address ranges. If these ranges are replaced with "#", all addresses from the LAN are allowed.

Authentication Protocol TLS

[FND User 2]

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

In addition, for authentication via TLS the issuer certificate or all certificates, necessary for validation of the FND certificate, have to be available to the client. Moreover the fingerprint of the issuer certificate and the subject of the FND certificate can be configured. This prevents a hostile re-creation of the friendly network.

```
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.

UserName

"UserName" corresponds to the parameter "User-Name" in the firewall settings of the client under the tab "Friendly Networks" under "automatic".

EAP-Type

You can choose between the authentication protocols, MD5 and TLS, as "EAP type". If the TLS protocol is selected as EAP type, it suffices to enter a user name, as described above.

IP Range

The IP range describes the IP address that the server accepts. This can be individual IP addresses or address ranges. If these ranges are replaced with "#", all addresses from the LAN are accepted.

Configuration at 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. 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.

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.

IP address for friendly network detection service

The IP address of a second FND server can be entered as a back-up after a comma. In this case make sure that the corresponding configuration file ncpfnd.conf is also available at the second FND server.

If the client is located in the friendly network, it attempts to reach the first FND server once. If no contact can be established, the second IP address will be selected.

User Name, Password (FND)

The friendly net detection server is authenticated via MD5 or TLS. The user name and password, entered here, have to agree with those stored on the FND. When using MD5, authentication occurs via "UserName" and "password". When using TLS a password is not required.

Subject of the Incoming Certificate

The incoming certificate of the FND server is checked for this string or the section of the string entered here. This string of characters must not end on a semi-colon ";". Only if there is agreement, the connected network is recognized as a friendly network. The appropriate issuer certificate or all certificates necessary for validation of the incoming FND 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. The fingerprint has to agree with the hash value entered here.

Starting the NCPFND Service

Under Linux

See NCP Linux Admin Guide.