# NCP Friendly Net Detection Server

## Administrationshandbuch



Version 4


Next Generation Network
Access Technology

www.ncp-e.com

## Kontakt

Wenn Sie weitere Informationen wünschen oder Fragen zu NCP-Produkten und Service-Leistungen haben:


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

**USA, North America**
NCP engineering, Inc.
601 Cleveland Street
Suite 501-25
Clearwater, FL 33755
Phone: +1 (650) 316-6273


**Support per E-Mail:**

support@ncp-e.com (deutsch)
helpdesk@ncp-e.com (englisch)

**Support Hotline:**

0900 / 1 99 68 00
(nur aus Deutschland erreichbar, 80 Cent / Minute)
Unsere Supportzeiten sind von Mo - Fr von 08:00 - 17:00 Uhr.

Bei einer Support-Anfrage benötigen wir folgende Informationen:
- Genauer Produktname
- Seriennummer
- Versionsnummer
- Genaue Problembeschreibung
- Fehlermeldung

# NCP Friendly Net Detection Server

# Inhaltsverzeichnis


Friendly Net Detection Server 5

Installation des FND-Servers 5

Konfiguration des FND-Servers 5

- Authentisierungs-Protokoll MD5 ..... 8
- Authentisierungs-Protokoll TLS ..... 9
- Authentisierungs-Protokoll TCP-TLS ..... 10
- Authentisierung mit MD5 und TLS ..... 11
- Konfiguration am Client ..... 12

Verwaltung des NCPFND-Dienstes 12

# Friendly Net Detection Server

Friendly Net Detection ist ein Leistungsmerkmal der NCP Secure Client Software für den universellen Einsatz in Remote Access- und Kommunikations-Umgebungen. Hierbei lassen sich einzelne Firewall-Regeln der Personal Firewall des NCP Secure Enterprise VPN Clients für verschiedene Netzzustände aktivieren. Firewallregeln können so konfiguriert werden, dass sie nur, in als "bekannt" definierten Netzen, angewandt werden. Die Erkennung bekannter Netze erfolgt entweder per fester Definition in der Client-konfiguration, oder automatisch per Kommunikation mit einem Friendly Net Detection Server (FND-Server).

Die FND ist eine Client-Server-Anwendung. Da es sich bei dem FND-Server um einen separat zu installierenden Dienst handelt, der vollkommen unabhängig vom VPN-Gateway ist, kann er auf einem beliebigen, dauerhaft erreichbaren, Rechner innerhalb des Netzwerkes installiert werden.

# Installation des FND-Servers

## Voraussetzungen

Der FND-Server für Linux funktioniert auf gängigen Linux-Distributionen. Eine Übersicht der offiziell getesteten und freigegebenen Betriebssysteme findet sich in den aktuellen Release Notes des FND-Servers.

## Installation unter Linux

Siehe NCP Linux Admin Guide.

**Die Software für den NCP Friendly Net Detection Server kann auf Anfrage vom NCP Support kostenfrei bezogen werden.**

# Konfiguration des FND-Servers

**Hinweis:** Beachten Sie, dass für die unterschiedlichen Authentisierungsprotkolle unterschiedliche Parameter gelten.

LocalIpAddr: EAP-MD5, EAP-TLS

Zertifikatskonfiguration: EAP-TLS, TCP-TLS

Listen: TCP-TLS

Wird der Parameter *Listen* zur Ermittlung des FND-Servers verwendet, ist es notwendig in der FND-Serverkonfiguration die Parametergruppe *Protokoll* mit den Parametern *eap* und *tls* einzufügen. Je nach dem welches Protokoll verwendet werden soll, müssen diese Parameter auf *1*" gesetzt werden.

Siehe ncpfnd.sam.

[Protocol]

eap=1 # [für EAP-MD5 und EAP-TLS]

tls=1 # [für TCP-TLS]

Die Konfiguration des FND-Servers erfolgt durch die Editierung der Konfigurationsdatei ncpfnd.conf, die sich im Installationsverzeichnis befindet. Sie ist in verschiedene Abschnitte unterteilt.

**Beachten Sie, dass in der Konfigurationsdatei das Zeichen "#" zum auskommentieren verwendet wird und daher nicht in den Parameterwerten vorkommen darf. Um Änderungen in der Konfigurationsdatei in den aktiven Betrieb zu übernehmen, müssen diese gespeichert und der FND-Dienst neu gestartet werden.**

**Hinweis:** Nach Verbindungsaufbau werden werdem vom FND-Server unterschiedliche Log-Datein geschrieben.

Unter Windows finden Sie die Log-Datein beispielsweise hier:

```
C:\Program Files (x86)\NCP\FndServer\log\
```

Unter Linux finden Sie die Log-Datein beispielsweise hier:

```
/var/log/ncp/fnd/
```

**[General]**

In diesem Abschnitt werden generelle Parameter und Einstellungen für den FND-Server festgelegt.

```
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**

Der LogLevel ist standardmäßig auf 10 gesetzt, so dass grundlegende Log-Meldungen geschrieben werden. Log-Meldungen werden nur für Wartungszwecke benötigt.

**LogPath**

Der LogPath legt das Verzeichnis fest in dem die Log-Files des FND-Servers abgelegt werden.

**Port**

Port 12521 (UDP) ist als Standard-Port für den FND-Dienst voreingestellt und sollte nicht verändert werden.

**LocalIPAdress**

Die lokale IP-Adresse muss nur dann eingetragen werden, wenn der Rechner über mehrere IP-Adressen verfügt und er nur auf die eingetragene hören soll. In der Standardeinstellung ist die IP-Adresse mit "#" auskommentiert, wodurch der Server auf alle IP-Adressen hört. Wird eine IP-Adresse hier eingetragen, so muss diese mit einer der IP-Adressen übereinstimmen, die in den Firewall-Einstellungen des Clients unter "Bekannte Netze" als die "IP-Adresse des Dienstes zur Erkennung der bekannten Netze" eingesetzt wurde. Mit der in der Client-Konfiguration angegebenen IP-Adresse muss dieser FND Server erreichbar sein.

**PKCS12FileName**

PKCS12FileName ist der Dateiname des Soft-Zertifikats (PKCS12-Zertifikat) mit Pfadangabe. Das Zertifikat wird zur Schlüsselerzeugung benötigt. Das Soft-Zertifikat *server1-rsa-2050.p12* dient nur Testzwecken, wird mit der Software ausgeliefert und befindet sich im Installationsverzeichnis. Es sollte durch ein eigenes Zertifikat ausgetauscht werden. Dabei ist darauf zu achten, dass auch das passende Ausstellerzertifikat am Client in das Installationsverzeichnis unter \CaCerts eingespielt werden muss. Das Ausstellerzertifikat für Testzwecke, das standardmäßig mit der Client Software ausgeliefert wird, befindet sich im Installationsverzeichnis der NCP Software.

**Pkcs12Pin**

Hier muss die zum Zugriff auf den Zertifikatsinhalt der p12-Datei notwendige PIN eingetragen werden. Die PIN wird in der Konfigurationsdatei abgespeichert. Beim Einlesen der Konfigurationsdatei durch den FND-Dienst wird die PIN verschlüsselt. Eine verschlüsselte PIN ist durch den vorangestellten Tag `crypt:` gekennzeichnet.

**[SysLog]**

Dieser Abschnitt legt fest, ob Log-Meldungen an einen Syslog-Server geschickt werden sollen.

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

Standardmäßig wird der Syslog Server (mit der angegebenen IP-Adresse) über den UDP Port 514 angesprochen. Die Meldungen werden erzeugt, wenn LogEnabled und/oder TraceEnabled auf "1" gesetzt werden. Über LogFacility / TraceFacility werden die Log-Dateien am Syslog Server identifiziert.

# Authentisierungs-Protokoll MD5

**[FND-User 1]**

Dieses Kapitel in der Beispiel-Konfiguration legt als Authentisierungs-Protokoll MD5 fest. In den Firewall-Einstellungen des Clients müssen Benutzername und Passwort mit den hier eingetragenen UserName und Password übereinstimmen.

```
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**

"Enabled" (eingeschaltet) wird die Authentisierung mittels MD5 indem die "1" gesetzt wird. Mit "0" wird die Authentisierung mittels MD5 für dieses Kapitel ausgeschaltet.

**UserName**

"UserName" entspricht dem Parameter Benutzername in den Firewall-Einstellungen des Clients unter der Rubrik "Bekannte Netze" im Reiter "automatisch".

**Password**

"Password" entspricht dem Parameter Passwort in den Firewall-Einstellungen des Clients unter der Rubrik "Bekannte Netze" im Reiter "automatisch".

**EAP-Type**

Als "EAP-Type" kann zwischen den Authentisierungs-Protokollen MD5 und TLS gewählt werden. Wird als EAP-Type das Protokoll MD5 gewählt, muss, wie oben beschrieben, UserName (Benutzername) und Password (Passwort) eingetragen sein.

Gruppenbildung

Eine Gruppenbildung kann vorgenommen werden mittels einer Übereinstimmung von User-Name und Password mit den Parametern in den Firewall-Einstellungen des Clients. Dies geschieht dadurch, dass obiges Kapitel 8 der Konfigurationsdatei dupliziert wird, wobei in dem duplizierten Kapitel andere Platzhalter für UserName und Password eingetragen werden, die dann entsprechend auch in den Konfigurationen der Clients für diese Gruppe übernommen werden müssen.

**IP-Range**

Die IP-Range beschreibt die IP-Adressen, die der FND Server entgegen nimmt. Dies können einzelne IP-Adressen oder Adress-Bereiche sein. Werden diese Bereiche mit "#" auskommentiert, so werden alle Adressen aus dem LAN zugelassen.

## Authentisierungs-Protokoll TLS

**[FND-User 2]**

**Dieses Kapitel in der Beispiel-Konfiguration legt als Authentisierungs-Protokoll TLS fest. In den Firewall-Einstellungen des Clients muss ein Benutzername mit dem hier eingetragenen UserName übereinstimmen. Das Passwort kann entfallen.**

Zusätzlich muss bei einer Authentisierung über TLS das Aussteller-Zertifikat bzw. alle Zertifikate, die für die Validierung des FND-Zertifikats notwendig sind, am Client zur Verfügung stehen. Außerdem kann am Client der Fingerprint des Aussteller-Zertifikats und der Benutzer (Subject) des FND-Zertifikats konfiguriert werden. Damit wird der mögliche “Nachbau” eines eines Friendly Nets ausgeschlossen.

**Hinweis**: Ab Version 4 erscheint in der Konfigurationsdatei der Parameter *Listen*.

```
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**

"Enabled" (eingeschaltet) wird die Authentisierung mittels TLS indem die "1" gesetzt wird. Mit "0" wird die Authentisierung mittels TLS für dieses Kapitel ausgeschaltet.

**UserName**

"UserName" entspricht dem Parameter "Benutzername" in den Firewall-Einstellungen des Clients unter der Rubrik "Bekannte Netze" im Reiter "automatisch".

**EAP-Type**

Als "EAP-Type" kann zwischen den Authentisierungs-Protokollen MD5 und TLS gewählt werden. Wird als EAP-Type das Protokoll TLS gewählt, so genügt es, wie oben beschrieben, einen UserName (Benutzernamen) einzutragen.

**IP-Range**

Die IP-Range beschreibt die IP-Adressen, die der FND Server entgegen nimmt. Dies können einzelne IP-Adressen oder Adress-Bereiche sein. Werden diese Bereiche mit "#" auskommentiert, so werden alle Adressen aus dem LAN zugelassen.

## Authentisierungs-Protokoll TCP-TLS

Hier erhalten Sie Hinweise darüber, wie sich das Authentisierungsprotokoll *TCP-TLS* bei unterschiedlichen Parametereingaben verhält.

- Bei einem Update ist EAP standardmäßig aktiviert, TCP-TLS ist standardmäßig nicht aktiviert. Bei einer Neuinstallation sind beide aktiviert.
- Wird `Listen` als Parameter gesetzt, wird eine Liste von IPv4- und IPv6-Adressen angesprochen. **Hinweis:** Es können mehrere IP-Adressen angegeben und durch einen Leerschritt, Semikolon oder Komma getrennt werden.
- Wird `Listen` nicht als Parameter gesetzt, wird der EAP-Paramter `LocalIPAddr` verwendet. **Hinweis:** Hierbei kann nur eine IP-Adresse angegeben werden. Dieser Parameter wird ebenfalls von den EAP-Protokollen verwendet.
- Das Protokoll TLS spricht standardmäßig alle IPv4-Adressen an, falls der Parameter `LocalIpAddr` ebenfalls nicht gesetzt ist.
- Die Versionsnummer kann über `-h` abgefragt werden. Hierbei werden *ncpfndd* bzw. *ncpfnd.exe* aufgerufen. Die Versionsnummer erscheint im Hilfetext.

**Hinweis:** Ein Update des *FND-Servers* von der Version 3 auf die Version 4.00 wird keine zusätzlichen Ports öffnen. Die vorherigen Einstellungen werden übernommen.

# Authentisierung mit MD5 und TLS

Um die "Automatische Erkennung der bekannten Netze aktivieren" zu können, selektieren Sie in den Firewall-Einstellungen unter der Rubrik Bekannte Netze im Reiter "automatisch" die entsprechende Funktion. Vergleichen Sie dazu die Beschreibung zum Konfigurationskapitel Authentisierungsprotokoll MD5 8.

**IP-Adresse des Dienstes zur Erkennung der bekannten Netze**

Als Backup kann die IP-Adresse bzw. der DNS-Name eines zweiten FND Servers nach einem Komma eingetragen werden. Achten Sie in diesem Fall darauf, dass am zweiten FND Server auch die entsprechende Konfigurationsdatei ncpfnd.conf vorhanden ist.

Befindet sich der Client im bekannten Netz, wird einmalig versucht den FND Server zu erreichen. Kann kein Kontakt hergestellt werden, wird die zweite IP-Adresse (oder DNS-Name) angewählt.

**Benutzername, Passwort (FND)**

Die Authentisierung des Friendly Net Detection Servers erfolgt über MD5 oder TLS. Bei Friendly Net Detection wird immer EAP over UDP eingesetzt, sowohl bei MD5 als auch bei TLS. Hier einzutragender Benutzername und Passwort müssen mit jenen am FNDS hinterlegten übereinstimmen. Bei Einsatz von MD5 findet die Authentisierung über "Benutzername" und "Passwort" statt. Bei Einsatz von TLS kann das Passwort entfallen.

**Benutzer (Subject) des eingehenden Zertifikats**

Das eingehende Zertifikat des FND Servers wird auf den String bzw. den Abschnitt des Strings hin geprüft, der hier eingegeben wird. Diese Zeichenkette darf nicht mit Semikolon ";" abgeschlossen werden! Nur bei Gleichheit wird das angeschlossene Netz als bekanntes Netz anerkannt. Das entsprechende Aussteller-Zertifikat bzw. alle Zertifikate, die für die Validierung des eingehenden FND-Zertifikats nötig sind, müssen am Client zur Verfügung stehen.

**Fingerprint des Aussteller-Zertifikats**

Um ein Höchstmaß an Fälschungssicherheit bieten zu können, kann eingestellt werden, dass der Fingerprint des Aussteller-Zertifikats, das sich im Installationsverzeichnis des Clients unter \CaCerts befinden muss, überprüft werden muss. Er muss mit dem hier eingegebenen Hash-Wert übereinstimmen.

# Konfiguration am Client

Voraussetzung für die Nutzung von Friendly Net Detection ist die Installation des FND Servers in einem Netzwerk, welches als Friendly Net (bekanntes Netz) deklariert wurde. Dieser Dienst muss von allen Anschlüssen des Netzwerks erreichbar sein. Es müssen gegebenenfalls Änderungen an den Firewall-Regeln vorgenommen werden.

Betreibt ein Mitarbeiter sein Endgerät direkt am Firmennetzwerk, so versucht der Secure Client, der für die automatische Erkennung der bekannten Netze konfiguriert wurde, den FND Server zu kontaktieren. Wird dieser erreicht und authentisiert, ist bestätigt, dass sich der Rechner in einem bekannten Netz befindet. Dadurch werden die entsprechenden, für dieses Netz vorkonfigurierten, Firewall-Regeln automatisch aktiviert.

# Verwaltung des NCPFND-Dienstes

**Hinweis:** Die hier beschriebenen Informationen beziehen sich auf die Protokolle EAP-TLS und EAP-MD5.

## Unter Linux

Siehe NCP Linux Admin Guide.