NCP
SECURE COMMUNICATIONS

Funktionsbeschreibung und Konfiguration

high security remote access

Personal Firewall und Friendly Net Detection

Personal Firewall und Friendly Net Detection

NCP Hotline auf Abruf

Sie erreichen unsere NCP Experten unter folgenden Hotlines:

Kunden mit Hotline Service Vertrag
Sie erhalten sofortigen Support unter der vertraglich angegebenen Rufnummer.
Ihnen steht das komplette Serviceportfolio zur Verfügung.

Kunden ohne Hotline Service Vertrag
Sie können wählen zwischen:
Kostenpflichtige Service-Rufnummer 09001996800 (-,80 Euro / Minute)
E-Mail an support@ncp-e.com oder Telefax an 0911 99 68 458
(ohne feste Reaktionszeiten)

Dienstleistungsauftrag (Berechnung nach Aufwand)
mit festen Reaktionszeiten und Zusatzservices.
Bitte nutzen Sie zur Anfrage das NCP Service-Formular von der Website
http://www.ncp-e.com/de/service-support/support.html

Sie möchten mehr über den NCP Hotline Service Vertrag wissen?
Bitte senden Sie eine E-Mail an:
vertrieb@ncp-e.com

Network
Communications
Products engineering GmbH

Dombühler Str.2
D-90449 Nürnberg
Tel.: 0911 / 99 68-0
Fax: 0911 / 99 68-299
internet http:// www.ncp-e.com
E-mail: info@ncp-e.com

Copyright

Die Firewall des Secure Clients

Diese Dokumentation beschreibt im ersten Teil die Funktionalität der Personal Firewall sowie die besonderen Leistungsmerkmale Friendly Net Detection und Stateful Boot Option.

Im zweiten Teil sind Konfigurationsbeispiele zur Aktivierung der Firewall und zu Friendly Net Detection dargestellt, sowie alle Parameter des Firewallmenüs beschrieben.

Im dritten Teil sind Installation und Konfiguration des Friendly Net Detection Servers beschrieben.

Der vierte Teil der Dokumentation beschreibt die Besonderheiten der Dynamic Personal Firewall.

Inhaltsübersicht

Auf spezielle Firewall-Einstellungen für **Mobile Computing** wird in der gleichnamigen Dokumentation verwiesen.

Am komfortabelsten erhalten Sie die gewünschten Informationen über die **Enterprise Suite Navigation**. In dieser PDF-Datei sind alle aktuell verfügbaren Dokumente zu Ihrem Produkt verzeichnet.

Vom Navigator aus können Sie alle relevanten Dokumente direkt anspringen und – falls sie noch nicht in Ihrem Navigatorverzeichnis gespeichert sind – von der NCP Website herunterladen.

Funktionalität der Firewall

Alle Firewall-Mechanismen sind optimiert für Remote Access-Anwendungen und können bereits beim Start des Rechners aktiviert werden. Im Gegensatz zu VPN-Lösungen mit eigenständiger Firewall ist der Telearbeitsplatz bereits vor der eigentlichen VPN-Nutzung gegen Angriffe geschützt.

Die Firewall ist gemäß ihrer Konfiguration für den gesamten IP-Datenverkehr des Rechners aktiv.* Sie ist “global” wirksam, unabhängig vom Standort des Rechners und dem jeweils aktuell selektierten Profil des Clients.**

Die Firewall arbeitet nach dem Prinzip der Paketfilterung in Verbindung mit Stateful Packet Inspection (SPI). Dabei prüft sie alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis des konfigurierten Regelwerks, ob ein Datenpaket weitergeleitet oder verworfen wird.

Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen wird der unbefugte Zugriff auf Daten und Ressourcen im zentralen Datennetz verhindert. Zum anderen wird mittels Stateful Inspection der jeweilige Status bestehender Verbindungen überwacht. Die Firewall kann darüber hinaus erkennen, ob eine Verbindung “Tochterverbindungen” geöffnet hat - wie beispielsweise bei FTP oder Netmeeting - deren Pakete ebenfalls weitergeleitet werden müssen. Wird eine Regel für eine ausgehende Verbindung definiert, die einen Zugriff erlaubt, so gilt die Regel automatisch für entsprechende Rückpakete. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für den Datenaustausch nach den vereinbarten Regeln genutzt werden darf.

** Bei aktiver Firewall ist ggf. auch die IP-Kommunikation mit einem Netzwerk-Drucker nicht möglich.*

*** Entgegen der Personal Firewall wird die Einstellung der Link Firewall, die in den Profil-Einstellungen des Monitors vorgenommen werden kann, nur für das dazu gehörende Profil aktiviert.*
Um Konflikte zwischen den Regeln der verbindungsorientierten Link Firewall in den Profil-Einstellungen und der Personal Firewall zu vermeiden, wird empfohlen, die Link Firewall auszuschalten wenn die erweiterte Firewall eingesetzt wird. Setzen Sie dann die IP-Adressen des jeweiligen Links zum Ziel-Gateway in den Filterregeln der Personal Firewall ein.
Sollte der Einsatz der Link Firewall zusätzlich zur Personal Firewall unumgänglich sein, dann beachten Sie bitte, dass die link-bezogenen Firewall-Einstellungen bei Aktivierung immer Vorrang haben. Ist z. B. die Link-Firewall auf “immer” und “Ausschließlich Kommunikation im Tunnel zulassen” eingestellt, kann trotz eventuell anders lautender Regeln der Personal Firewall nur über einen VPN-Tunnel kommuniziert werden. Jeglicher anderer Verkehr wird von der Link-Firewall verworfen.

**** Der Administrator kann alle Firewall-Regeln vorgeben und deren Einhaltung erzwingen. Dazu müssen die* **Parametersperren** *des Clients entsprechend eingestellt werden. Voraussetzung für die zentrale Administration von Enterprise Clients ist das NCP Secure Enterprise Management.*

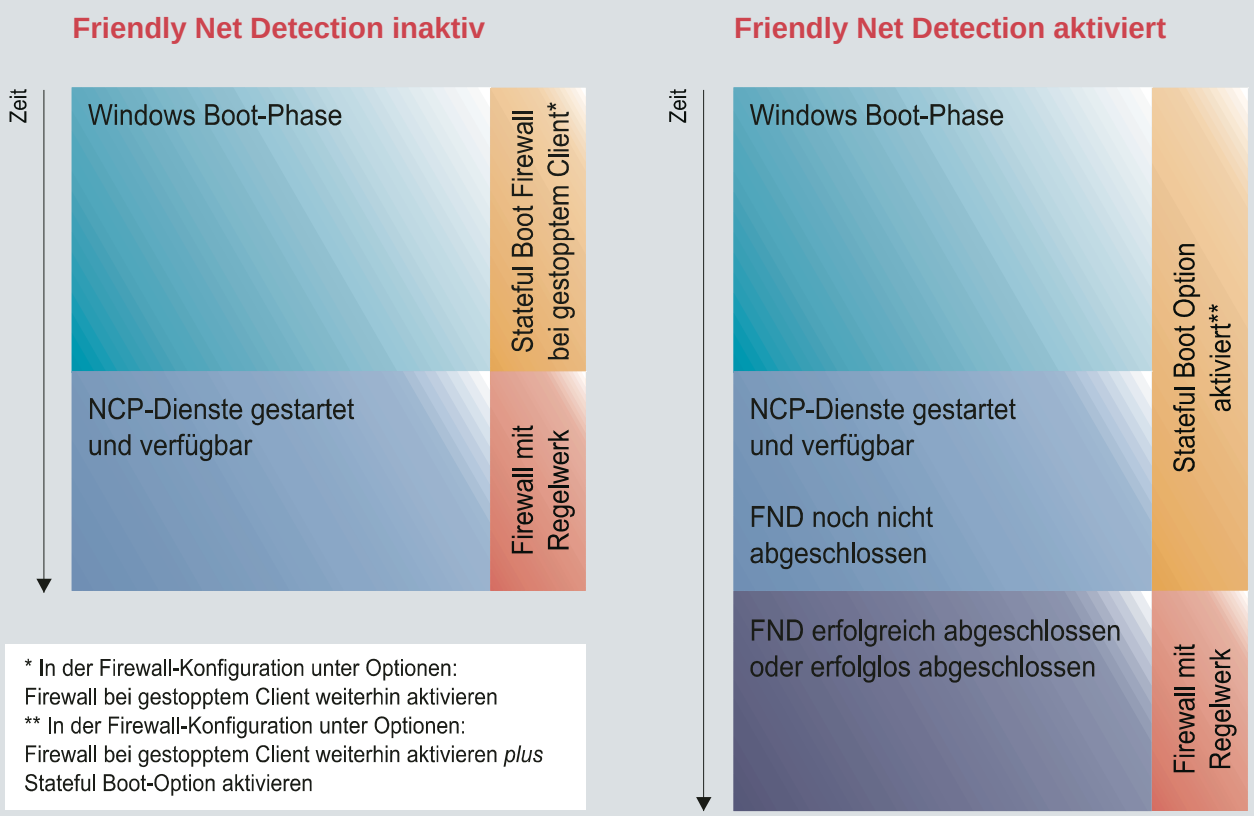
Friendly Net Detection und Stateful Boot-Option

Ein weiteres bedeutendes Leistungsmerkmal der NCP Secure Client Software für den universellen Einsatz in beliebigen Remote Access- und Kommunikations-Umgebungen ist **Friendly Net Detection**. Die Regeln der integrierten Personal Firewall werden dabei vom Administrator (zentral*) vorgegeben und sind vom Anwender nicht manipulier- bzw. abschaltbar. Der Anwender kann in jeder Situation hochsicher und transparent auf das Firmennetz zugreifen.

Die Firewall bietet auch “bei gestopptem Client” (bei nicht gestartetem Dienst) vollen Schutz des Endgeräts wenn diese Einstellung in der Firewall unter **Optionen** vorgenommen wurde. Während des Systemstarts tauscht Microsoft Windows verschiedene Gruppen- und Sicherheits-Richtlinien zwischen dem Client und dem Domain Controller aus. Diese Richtlinien werden verworfen wenn die Firewall bei gestopptem Client unabhängig von einem gestarteten NCP-Dienst aktiv ist.

Die “Stateful Boot Option” (Firewall-Einstellung unter **Optionen**) erweitert die Personal Firewall zu einer Stateful Packet Inspection Firewall auf Treiber-Ebene, die den Richtlinien-Austausch und die Kommunikation zwischen Windows Workstations in der Boot-Phase gestattet, während das Rechnersystem gleichzeitig gegen Angriffe von außen geschützt ist.

NCP Firewall mit Stateful Boot Option



Firewall-Einstellungen

Die Firewall-Regeln können dynamisch konfiguriert werden, das heißt ein Anhalten der Software oder ein Neustart ist nicht nötig.

Die Firewall-Einstellungen im Konfigurationsmenü des Client-Monitors erlauben eine genaue Spezifikation von Firewall-Filterregeln. Diese können sowohl anwendungsbezogen als auch zusätzlich adressorientiert oder umgekehrt gebildet werden. Außerdem können sie speziell bekannten oder unbekannten Netzen, aber auch VPN-Verbindungen zugewiesen werden (Firewall-Einstellungen, Firewall-Regeln).

Wie bekannte oder unbekannte Netze ggf. automatisch vom Client erkannt werden können und jeweils konsequent entsprechende Firewall-Filterregeln zugeordnet werden können, ist weiter unten im Abschnitt **Friendly Net Detection** beschrieben.

Anzeige der Firewall-Einstellungen

Die Grundeinstellungen der Firewall werden bei einem Tool-Tip auf das System Tray Icon als Quick-Info angezeigt, sodass schnell erkennbar ist, ob die Personal Firewall (FW) aktiv oder inaktiv ist und ob sich der Client in einem bekannten oder unbekannten Netz befindet. (Die Mauer einer aktiven Firewall im unbekannten Netz ist rot, im Friendly Net grün; siehe Abb. unten). Im PDF zum Client-Monitor sind die **Symbole** der Client-Oberfläche ausführlich beschrieben.

Anzeige der Firewall im Popup des Tray Icons

Funktionsweise der Friendly Net Detection

Außendienstmitarbeiter, die sowohl in der Firma arbeiten als auch von Unterwegs oder von zu Hause Zugriff auf das Internet und auf das Firmennetz über VPN benötigen, haben besondere Anforderungen an ihre Personal Firewall.

Zum einen muss deren Notebook unterwegs vor Angriffen geschützt sein und unerlaubte Kommunikation unterbinden. Zum anderen soll in der Firma die Anmeldung an die Domäne und der Zugriff auf verschiedenste Server im Firmennetz problemlos möglich sein. Auch könnte dem mobilen Anwender nur erlaubt sein, seine E-Mails vom Firmen-Server herunterzuladen, während ihm das Internet-Surfen untersagt ist. Im zentralen Datennetz dagegen befindet er sich in einer geschützten Umgebung (mit Virenscanner und Firewall), wo eine Personal Firewall überflüssig ist und er eine Client-Server-Anwendung über definierte TCP/IP- bzw. UPD-Ports nutzen möchte.

Bei Verwendung einer statischen Firewall müsste der Benutzer selbständig die Einstellungen seiner Personal Firewall, die für den mobilen Einsatz konfiguriert wurde, um- oder ausschalten - je nach Sicherheitsrichtlinie und Netzwerkumgebung (Zentrale oder Filiale).

Dieses manuelle Umschalten wird überflüssig und automatisiert durch die Technik der Friendly Net Detection (FND), die zwischen “bekannten”, friendly Networks wie dem Firmennetz, und allen “unbekannten” Netzen unterscheiden kann.

Sicherheitsrichtlinie

In einer Sicherheitsrichtlinie werden vom Administrator Kriterien zusammengefasst, wonach die Rechte eines Anwenders in einem Netzwerk (z. B. Intranet, zentrales Datennetz, Firmen-Netzwerk, Internet usw.) definiert werden. Entsprechend gestalten sich das Firewall-Regelwerk, das vom Administrator festgelegt wird und das den Sicherheitsanforderungen der unterschiedlichen Netzwerke, Friendly Net oder Unfriendly Net, gerecht werden muss (Firewall-Einstellungen, **Firewall-Regeln**). Schließlich ist in der Sicherheitsrichtlinie* auch zusammengefasst, welche Netze als “bekannte” Netze gelten und welche nicht.

Um nun Firewall-Regeln zu definieren, die abhängig vom Standort bzw. dem aktuellen Netzwerk des Anwenders sind, bieten die NCP Secure Clients die Möglichkeit einer dieser Gruppen von “bekannten” oder “unbekannten” Netzen eine Firewall-Regel zuzuordnen. Dadurch wird die entsprechende Regel nur dann automatisch aktiv gesetzt, wenn sich der Anwender in einer der Netzwerkgruppen befindet.

** Damit ein Anwender diese Security Policy nicht umgehen, d. h. Firewall-Regeln deaktivieren, löschen oder ändern kann, ermöglicht der NCP Secure Client ein Sperren des Zugriffs auf diese Konfigurationsparameter. Dies gilt auch für Benutzer mit Administrator-Berechtigungen, d. h. unabhängig von den Rechten der Systemumgebung (siehe **Parameter-Sperren**).*

Definition des bekannten Netzes (Friendly Net)

Über die Firewall-Einstellungen können dem Client bekannte Netze manuell oder automatisch mitgeteilt werden. In beiden Fällen definiert der Administrator Firewall-Regeln nur einmal für die gesamte System-Landschaft.

Die manuelle Konfiguration eines bekannten Netzes in den Firewall-Einstellungen erfordert die Eingabe der Netzwerkdaten (**Firewall-Einstellungen**, Bekannte Netze, **Manuell**). Dabei steht der Administrator vor der Aufgabe, die Liste der Friendly Networks permanent aktuell zu halten und die Einhaltung der Firewall-Regeln in sich ständig ändernden Kommunikationsumgebungen sicherzustellen.

Dabei muss darauf geachtet werden, dass nicht jede Firma einen IP-Adressenbereich aus dem öffentlichen IP-Adressraum besitzt. Viele verwenden private IP-Adressen wie 10.x.x.x/8, 172.16.x.x/16 oder 192.168.x.x/24 und setzen dann auf NAT-Devices (Network Addess Translation) bzw. Proxy-Server, ohne zu bedenken, dass in fest konfigurierten FNs ein Mitarbeiter mit den gleichen Netzwerk-Adressen in seinem Heimnetzwerk arbeitet, wie im Friendly Net. Umgekehrt kann ein Außendienstmitarbeiter sein Notebook in einem unbekannten Netzwerk anschließen, das den gleichen IP-Adressraum verwendet wie das Firmen-Netzwerk. Beide Male wird die Sicherheitsrichtlinie aufgehoben und Firewall-Regeln, welche den Client in unbekannten Netzen schützen sollten werden deaktiviert.

Damit weder der Benutzer noch der Administrator mit dem Pflegen einer Liste von bekannten Netzen beschäftigt ist und Authentisierungsmechanismen eine eindeutige Erkennung eines bekannten Netzes

ermöglichen, sollte die **automatische Konfiguration** mit Friendly Net Detection eingesetzt werden.

Die automatische Konfiguration, eines der Leistungsmerkmale der dynamischen Personal Firewall, ermöglicht dem Client automatisch zu erkennen ob er sich in einem bekannten Netz befindet, völlig transparent und ohne das Einspielen einer neuen Konfiguration.

Prinzip der Friendly Net Detection

Die FND ist eine Client-Server-Anwendung. Da es sich bei dem Server (**FNDS**) um einen separat zu installierenden Dienst handelt, der vollkommen unabhängig vom VPN-Gateway ist, kann er auf einem beliebigen Rechner innerhalb des Netzwerkes, welches als FN deklariert werden soll, installiert werden.

Die Funktionsweise der FND basiert auf etablierten Standards. Dies gewährleistet die Sicherheit des Systems und schützt vor Fehlern, wie sie bei proprietären Lösungen häufiger vorkommen.

Nach der Installation des Friendly Net Detection Servers in einem Netzwerk, welches als Friendly Net deklariert wurde und nach dem **Start des NCPFND-Dienstes** (siehe weiter unten beim FND Server), muss dieser Dienst von allen Anschlüssen des Netzwerks erreichbar sein, d. h. es müssen gegebenenfalls Änderungen an den Firewall-Regeln vorgenommen werden.

Betreibt ein Mitarbeiter sein Endgerät am Firmen-Netzwerk, so versucht der FND-Client den konfigurierten FND-Server zu kontaktieren. Wird dieser erreicht und authentisiert, so ist bestätigt, dass sich der Rechner in einem bekannten Netz befindet und die entsprechenden, für dieses Netz vorkonfigurierten Firewall-Regeln werden automatisch aktiviert.

Die Authentisierung

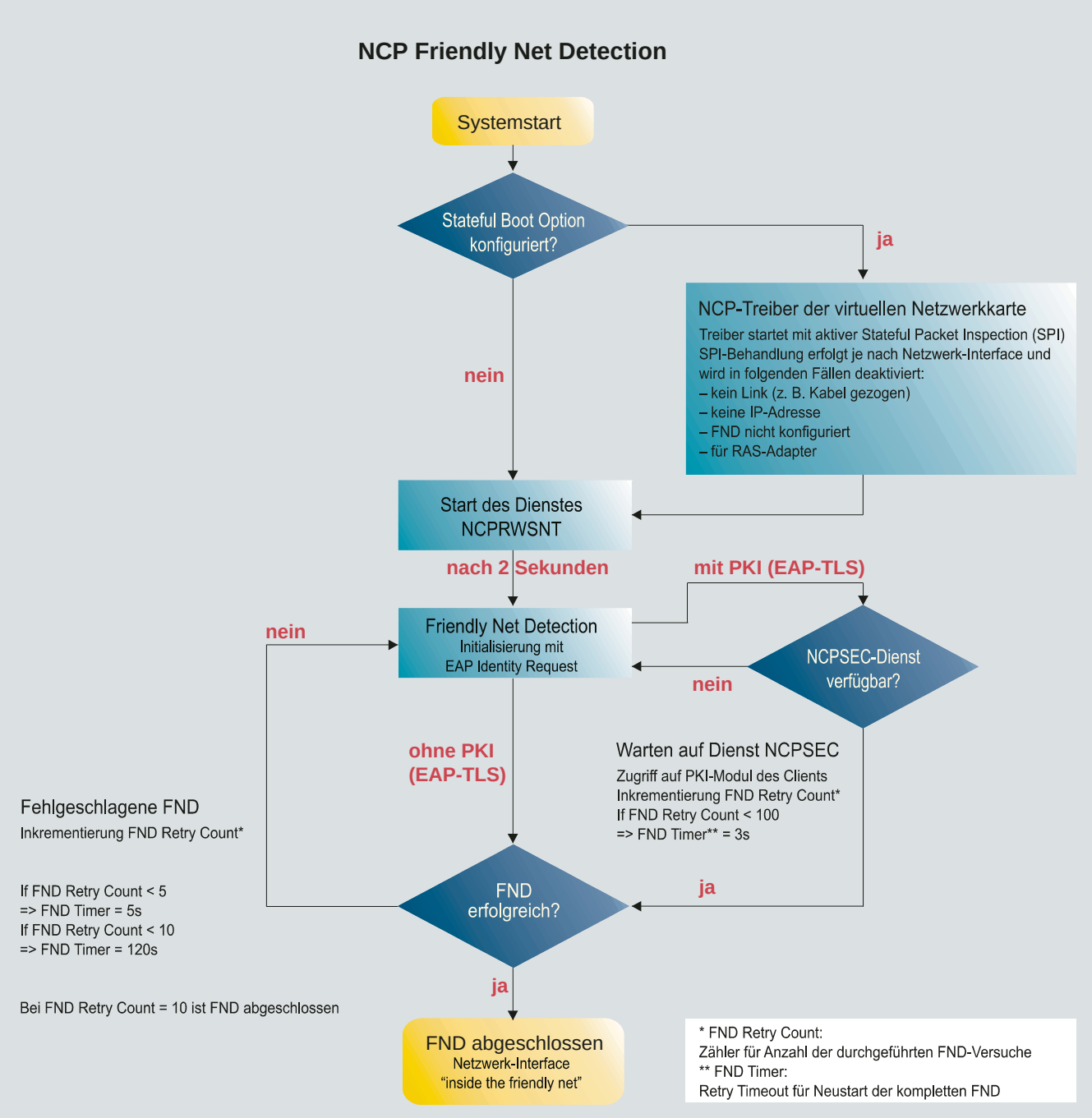
Die Konfigurationsbeschreibung zur folgenden Ausführung finden Sie im Abschnitt “Automatische Erkennung der bekannten Netze”.

Zur Authentisierung dienen Benutzername und Passwort (in den **Firewall-Einstellungen**) in den standardisierten Authentisierungs-Protokollen MD5 (RFC2284) und TLS (RFC2716), wobei nur der Server vom Client authentisiert wird.

Im Falle von **EAP-MD5** wird am Server Benutzername und Passwort hinterlegt, welche zur Prüfung auch im Client hinterlegt werden müssen. Diese Vorgehensweise ermöglicht auch eine **Gruppenbildung** von Clients (Definition gruppenspezifischer FNs). Siehe auch **Authentisierung mit MD5 und TLS**.

Bei **EAP-TLS** muss das Aussteller-Zertifikat bzw. alle Zertifikate, die für die Validierung des FNDS-Zertifikates notwendig sind, am Client zur Verfügung stehen. Weiter kann am Client der Fingerprint des Aussteller-Zertifikats und das Subject des FNDS-Zertifikats konfiguriert werden. Damit wird der mögliche “Nachbau” eines eines Friendly Nets ausgeschlossen. Siehe auch **Authentisierung mit MD5 und TLS**.

Nachdem alle Informationen für die Authentisierung konfiguriert wurden, muss hinterlegt werden, unter welcher **IP-Adresse** (alternativ auch Host-Name) der FNDS erreichbar ist. Maximal können zwei durch Komma getrennt angegeben werden.



Friendly Net Detection ist ein bedeutendes Leistungsmerkmal der NCP Secure Client Software für den universellen Einsatz in beliebigen Remote Access- und Kommunikations-Umgebungen. Die Regeln der integrierten Personal Firewall werden vom Administrator zentral* vorgegeben und sind vom Anwender nicht manipulier- bzw. abschaltbar. Der Anwender kann in jeder Situation hochsicher und transparent auf das Firmennetz zugreifen.

** Für zentral gesteuerte Veränderungen an den Konfigurationsparametern des NCP Secure Enterprise Clients, bietet NCP optional das Secure Enterprise Management (SEM) als “Single Point of Administration” .*

Konfigurationsmenü der Personal Firewall und Beispiele

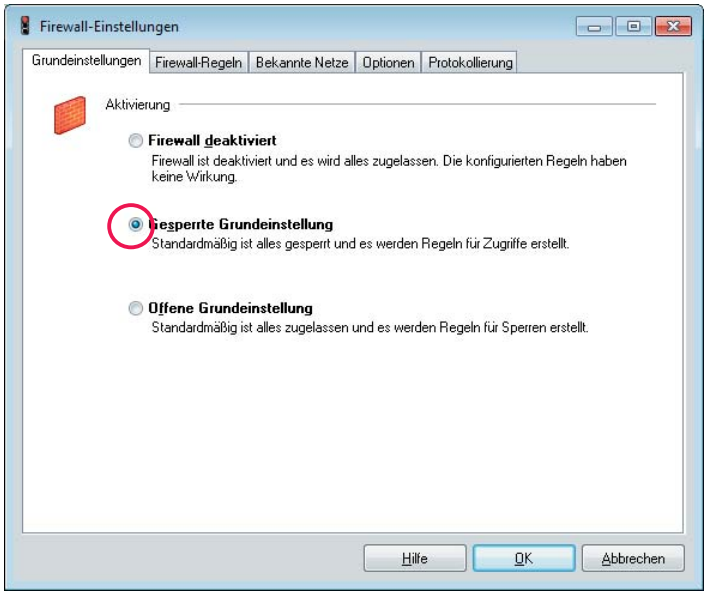


Abb. 1

Beispiel: Client-Firewall mit anwendungsbezogener Regel

Der Secure Client besitzt eine Personal Firewall, die Sie für verschiedene Umgebungen und Anwendungen vorkonfigurieren können. Diese Firewall ist auch denn aktiv wenn der Client-Monitor nicht gestartet ist.

Die Firewall aktivieren Sie über das Konfigurations-Menü unter “Firewall” mit den gesperrten Grundeinstellungen (Abb. 1). Damit wird der komplette IP-Datenverkehr blockiert.

Anschließend erstellen Sie Regeln, die die Firewall, je nachdem in welchem Netz (bekanntes, unbekanntes oder VPN-Netz) sich der Client befindet, für IP-Verkehr öffnet.

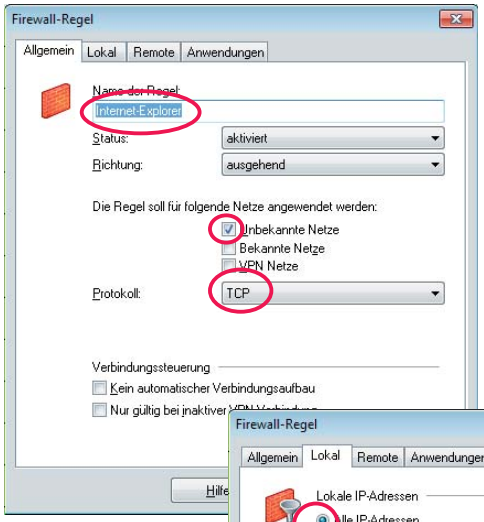


Abb. 2

Beispiel: Sie wollen mit dem Internet Explorer surfen

Unter der Rubrik “Allgemein” vergeben Sie einen Namen für diese Regel und legen die ausgehende Richtung fest. Diese Regel soll außerdem nur für unbekannte Netze und TCP-Pakete gelten (Abb. 2).

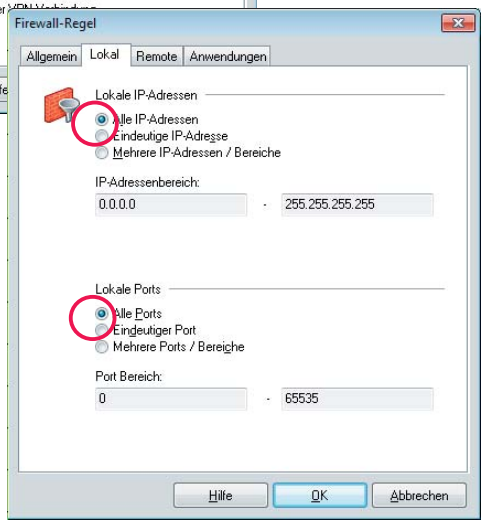


Abb. 3

Unter der Rubrik “Lokal” stellen Sie ein, dass alle IP-Pakete nach außen durchgelassen werden, unabhängig davon, welche IP-Adresse oder welchen Port die IP-Pakete verwenden (Abb. 3).

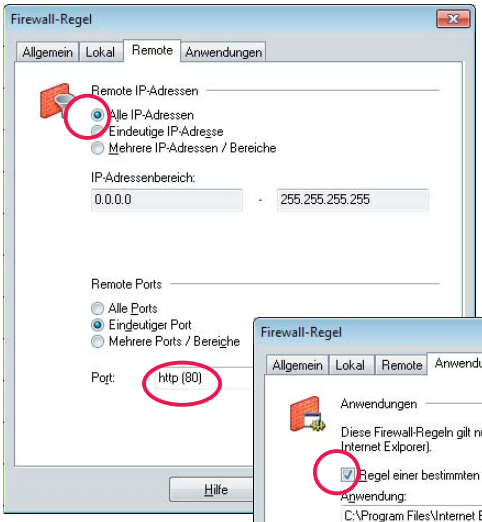


Abb. 4

Unter der Rubrik “Remote” öffnen Sie die Firewall für die Kommunikation mit allen IP-Adressen und legen fest ob Port 80 (für HTTP) und / oder Port 443 (für HTTPS) geöffnet wird (Abb. 4).

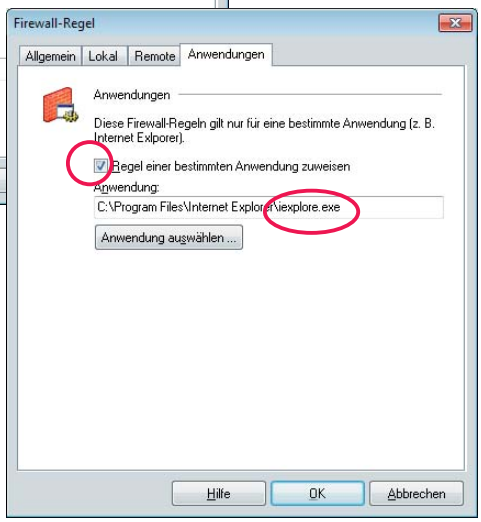


Abb. 5

Unter “Anwendungen” weisen Sie diese Regel einer Anwendung zu, indem Sie die entsprechende EXE-Datei für den Internet Explorer auswählen (Abb. 5).

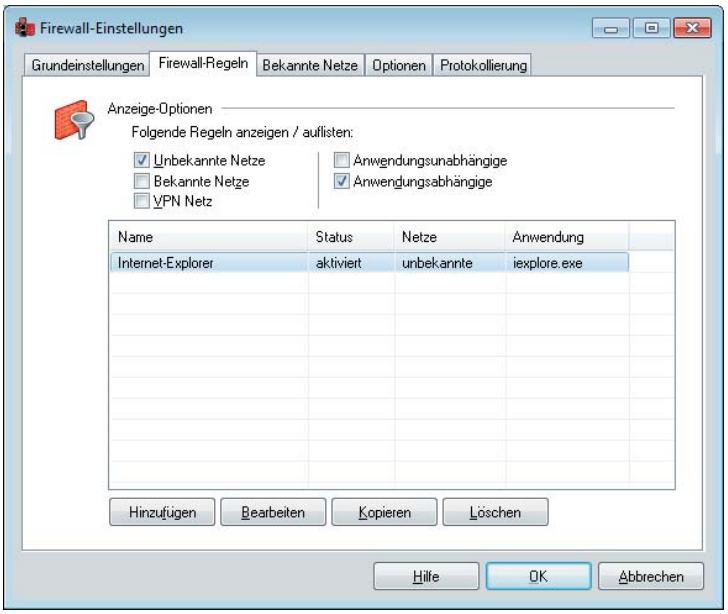


Abb. 6

In der Liste der Firewall-Regeln können Sie nach Netztypen getrennt die vorhandenen Firewall-Regeln ablesen (Abb. 6).

Beachten Sie zu anwendungsbezogenen Reglen die Einschränkung auf Seite 22!

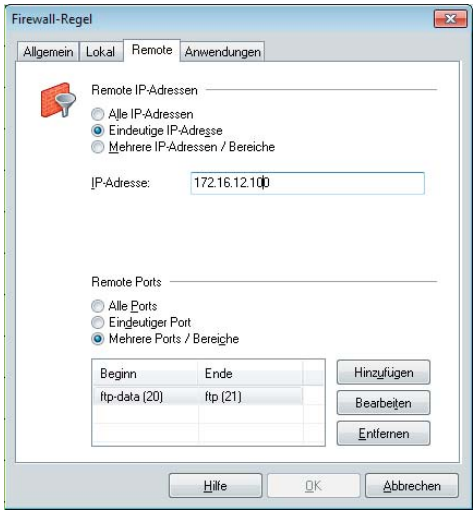


Abb. 1

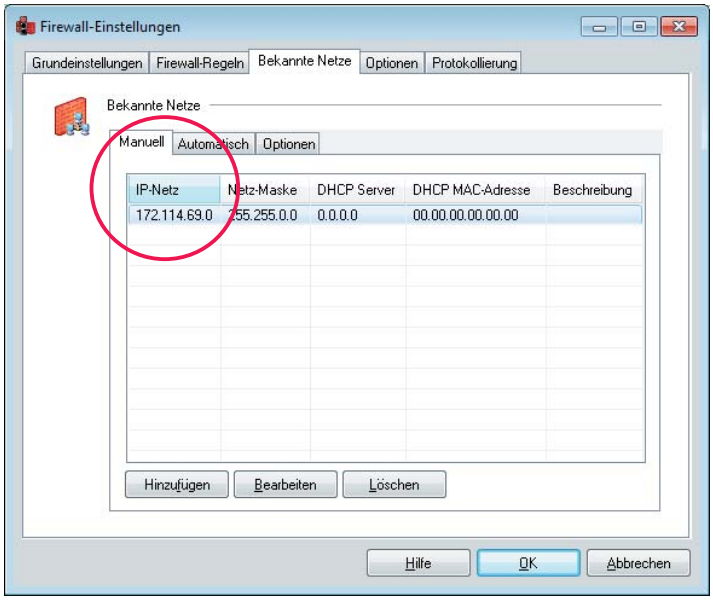


Abb. 2

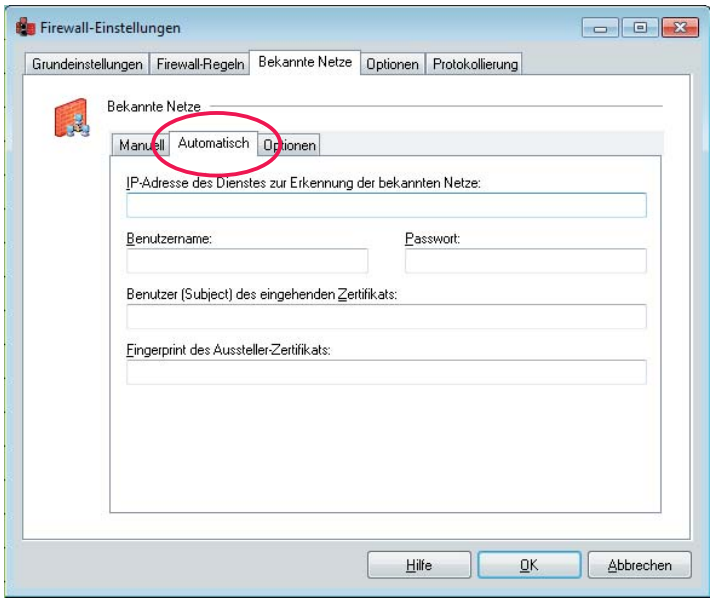


Abb. 3

Beispiel: Automatische Anpassung der Firewall-Regeln in bekannten Netzen

Der Client verfügt über eine Personal Firewall, die gestattet, Regeln für drei unterschiedliche Netztypen zu erstellen. Dabei wird nach VPN-Netzen (Daten im VPN-Tunnel), bekannten Netzen (z. B. das Firmen- oder Heimnetzwerk) und unbekannten Netzen (alle anderen) unterschieden. Neue Regeln werden über das Konfigurations-Menü “Firewall” durch Hinzufügen der “Firewall-Regeln” erstellt (Abb. 1).

Sobald eine Netzwerkverbindung jeglicher Art hergestellt wird, erkennt der Client selbständig in welcher Art des Netzes er sich befindet.

Bekannte Netze

Manuell können dem Client ein oder mehrere Parameter mitgeteilt werden, anhand denen er erkennt, ob er sich im bekannten Netz (Friendly Net) der Firma oder z. B. in einem unbekannten WLAN an einem Hotspot befindet. Diese Parameter werden im Konfigurations-Menü unter “Firewall / Bekannte Netze / Manuell” eingegeben (Abb. 2):

– IP-Netz / Netz-Maske

– IP-Adresse des DHCP Servers

– MAC-Adresse des DHCP Servers

Automatisch kann die Erkennung der bekannten Netze dann erfolgen, wenn ein **Friendly Net Detection Server** (FND Server) eingesetzt wird. Über die “IP-Adresse (oder den DNS-Namen) des Dienstes zur Erkennung der bekannten Netze” muss der FND Server vom Client über IP erreichbar sein. Am FND Server sind Benutzername, Passwort und ggf. ein Zertifikat hinterlegt, die mit den hier einzutragenden Werten übereinstimmen müssen (Beachten Sie hierzu die Online-Hilfe) (Abb. 3). Erreicht der Client einen FND Server und ist die Authentisierung erfolgreich, befindet sich der Netzwerkadapter im Friendly Net.

Erstellen einer Regel

Um eine Regel für bekannte Netze zu erstellen, aktivieren Sie zunächst die “Gesperrte Grundeinstellung” im Konfigurations-Menü des Monitors unter “Firewall”. Damit ist zunächst jeder IP-Verkehr blockiert.

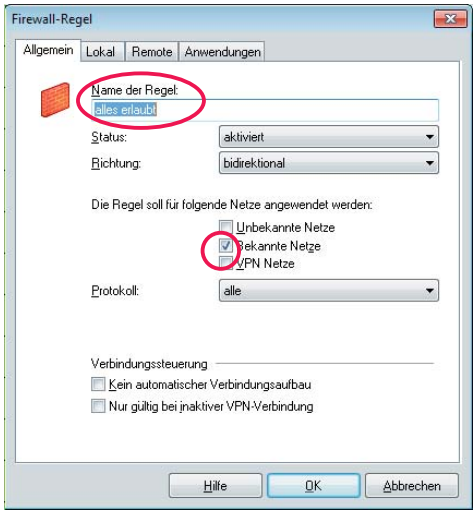
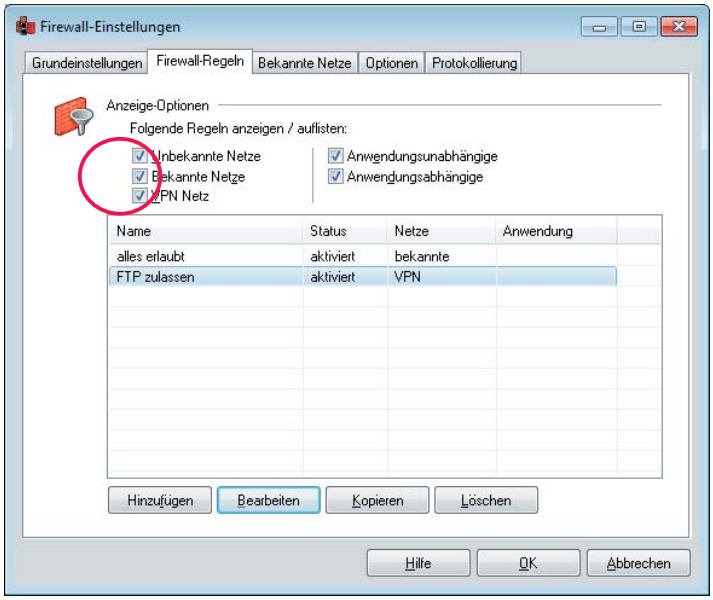


Abb. 4

In den Firewall-Einstellungen unter “Firewall-Regeln” fügen Sie eine Regel hinzu (Abb. 4). Geben Sie der Regel einen Namen und definieren Sie mit den angegebenen Parametern, welche Aktionen erlaubt sein sollen (siehe dazu Online-Hilfe). Markieren Sie schließlich, dass diese Regel nur für bekannte Netze angewendet werden soll.

Abb. 5



Nach dem Speichern der Regel mit Klick auf “Ok” sehen Sie in der Liste der Firewall-Regeln, welche Regeln für welche Netz-Typen angewendet werden (Abb. 5).

Friendly Net im Monitor

Ob sich der Client in einem Friendly Net befindet, können Sie im Monitor bzw. am Tray Icon des Clients erkennen, wenn sich das Firewall-Symbol grün färbt (Abb. links).

Konfigurationsmenü der Personal Firewall

Die Parameter für die Firewall-Einstellungen werden auf fünf Konfigurationsfeldern, zum Teil mit untergeordneten Registerkarten, eingestellt:

Grundeinstellungen

Firewall-Regeln

- **Allgemein**
- **Lokal**
- **Remote**
- **Anwendungen**

Bekannte Netze

- **Manuell**
- **Automatisch**
- **Optionen**

Optionen

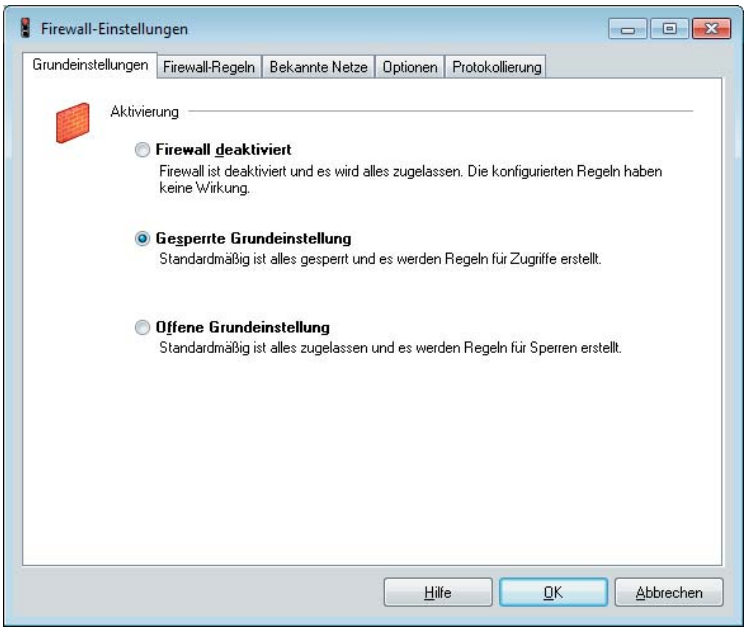
- **Allgemein**
- **Kommandos**

Protokollierung

Per Mausklick auf einen der Begriffe gelangen Sie direkt dorthin. Mit Mausklick auf das Info-Icon gelangen Sie wieder zurück zu dieser Übersicht.

Die Firewall-Einstellungen bzw. das Konfigurationsmenü der Firewall wird über das Konfigurationsmenü des Client-Monitors geöffnet (Abb. links).

Konfigurationsfeld Grundeinstellungen



In den Grundeinstellungen wird festgelegt, mit welcher Basis-Richtlinie die Firewall arbeiten soll.

Firewall deaktiviert

Wird die erweiterte Firewall deaktiviert, so wird in diesem Kompatibilitätsmodus nur die in den Profil-Einstellungen konfigurierte **Link-Firewall** genutzt. Dies bedeutet, dass alle Datenpakete nur über die Sicherheitsmechanismen dieser verbindungsorientierten Firewall abgearbeitet werden.

Gesperrte Grundeinstellung (empfohlen)

Wird diese Einstellung gewählt, so sind die Sicherheitsmechanismen der Firewall immer aktiv. D. h. ohne zusätzlich konfigurierte Regeln wird jeglicher IP-Datenverkehr unterbunden.

Ausgenommen sind die Datenpakete, die durch eigens erstellte, aktive Firewall-Regeln gestattet (durchgelassen) werden (Permit Filter). Trifft eine der Eigenschaften eines Datenpakets auf die Definition einer Firewall-Regel zu, wird an dieser Stelle die Abarbeitung der Filterregeln beendet und das IP-Paket weitergeleitet.

Im Modus der gesperrten Grundeinstellung kann auf komfortable Weise eine IPsec-Tunnelkommunikation freigeschaltet werden.

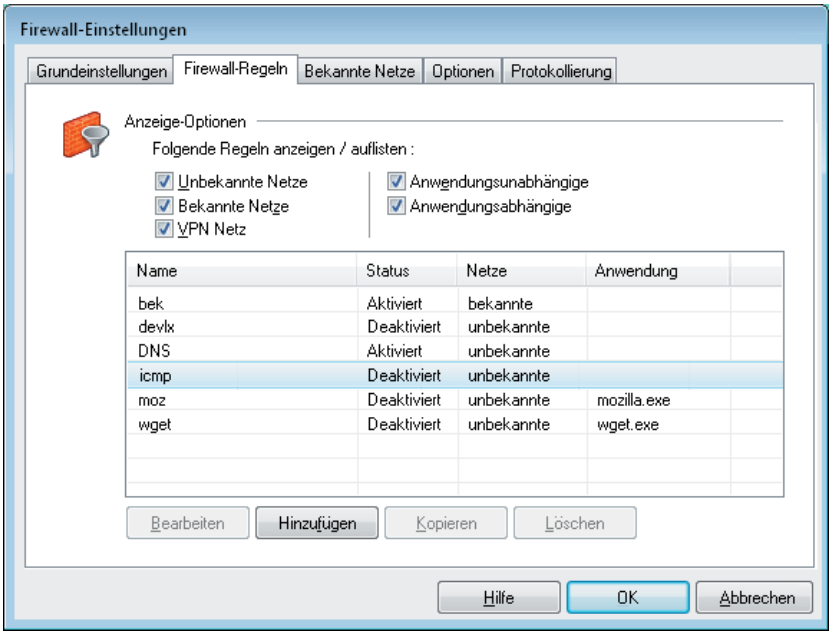
Dazu kann im Konfigurationsfeld **Optionen** der Datenverkehr über IPsec-Protokolle und VPN-Path Finder global zugelassen werden.

Offene Grundeinstellung

In der offenen Grundeinstellung sind zunächst alle IP-Pakete zugelassen. Ohne weitere Filterregeln werden alle IP-Pakete weitergeleitet.

Ausgenommen sind die Datenpakete, die durch eigens erstellte, aktive Firewall-Regeln ausgefiltert (nicht durchgelassen) werden (Deny Filter). Trifft eine der Eigenschaften eines beim Server/Client ankommenden IP-Pakets auf die Definition eines Deny-Filters zu, wird an dieser Stelle die sequentielle Abarbeitung der Filterregeln beendet und das IP-Paket von der Weiterleitung ausgeschlossen. Daten-Pakete, die auf keinen passenden Deny-Filter treffen, werden weitergeleitet.

Konfigurationsfeld Firewall-Regeln



In diesem Konfigurationsfenster werden die Regeln für die Firewall zusammengestellt. Die Anzeige-Optionen sind standardmäßig alle aktiv. Mittels dieser wird eingestellt, welche Regeln in Abhängigkeit ihrer Zuordnung in der Übersicht angezeigt werden:

– unbekannte Netze
– bekannte Netze
– VPN-Netze
– anwendungsabhängi
– unabhängig

Diese Auswahlfelder für die Anzeigen der Regeln dienen nur der Übersichtlichkeit und haben keine Auswirkung auf die Anwendung einer Filterregel. Für jede definierte Regel werden die wichtigsten Eigenschaften gezeigt:

– Name
– Status
– Netz
– Anwendung

Durch Klick auf diese Eigenschafts-Buttons können die eingeblendeten Regeln sortiert werden.

Erstellen einer Firewall-Regel

Über die Buttons unterhalb der Anzeigezeilen werden die Regeln erzeugt oder bearbeitet. Um eine Firewall-Regel zu erstellen, klicken Sie auf “Hinzufügen”. Die Erstellung einer Filterregel erfolgt über vier Konfigurationsschritte bzw. Registerkarten:

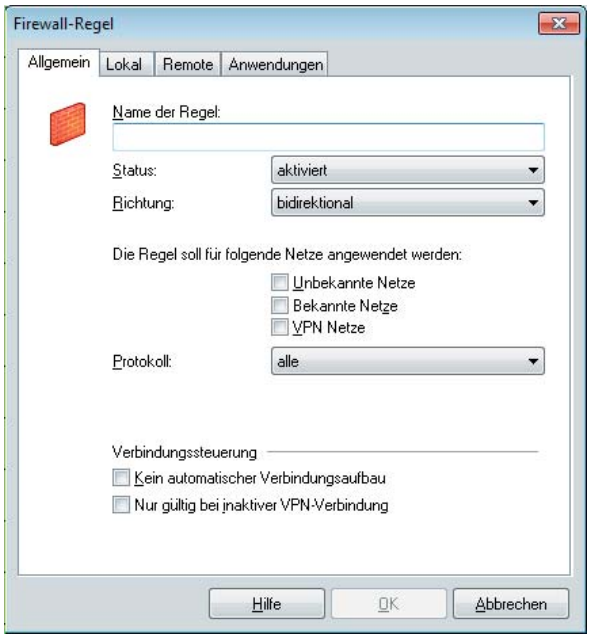
– Allgemein: In diesem Konfigurationsfeld wird festgelegt für welche Netze und welches Protokoll die Regel gelten soll.

– Lokal: In diesem Konfigurationsfeld werden die Werte der lokalen Ports und IP-Adressen eingetragen.

– Remote: Im Remote-Feld werden die Port-und Adress-Werte der Gegenseite eingetragen.

– Anwendungen: In diesem Konfigurationsfeld kann die Regel einer oder mehrerer Anwendungen zugeordnet werden.

Firewall-Regel / Allgemein



Einzelregeln stellen immer Ausnahmen von der Grundeinstellung dar.

Name der Regel

Mit diesem Namen erscheint die Regel in der Anzeigeliste.

Status

Die Regel wird nur dann auf Datenpakete angewendet, wenn der Status “aktiv” ist.

Richtung

Mit der Richtung geben Sie an, ob diese Regel für eingehende oder ausgehende Datenpakete gelten soll. Wird die Richtung auf ausgehend gesetzt, wird nach dem Prinzip von Stateful Inspection gearbeitet. Stateful Inspection wird jedoch nur für die Protokolle UDP und TCP angewendet. Auf “eingehend” kann z.B. dann geschaltet werden, wenn von Remote-Seite eine Verbindung aufgebaut werden soll (z. B. für “eingehende Rufe” oder Administrator-Zugriffe). Die Einstellung “bidirektional” ist nur sinnvoll, wenn Stateful Inspection nicht zur Verfügung steht, z. B. für das ICMP-Protokoll (bei einem Ping).

Die Regel soll für folgende Netze angewendet werden

Beim Neuanlegen einer Regel ist diese zunächst keinem Netz zugeordnet. Eine Regel kann erst dann gespeichert werden, wenn die gewünschte Zuordnung erfolgt ist und ein Name vorgegeben wurde.

Unbekannte Netze
– sind alle Netze (IP-Netzwerkschnittstellen), die weder einem bekannten noch einem VPN-Netz zugeordnet werden können. Darunter fallen z.B. Verbindungen über das DFÜ-Netzwerk von Microsoft oder auch direkte und unverschlüsselte Verbindungen mit dem integrierten Dialer des Clients, wie auch HotSpot WLAN-Verbindungen. Soll eine Regel für unbekannte Netze gelten, so muss diese Option aktiviert werden.

Bekannte Netze
– werden im gleichnamigen Register im Fenster “Firewall-Einstellungen” definiert. Soll eine Regel für bekannte Netze gelten, muss diese Option aktiviert werden.

VPN-Netze
– sind alle IPsec-Verbindungen in aufgebautem Zustand. Darüber hinaus fallen unter diese Gruppe auch alle verschlüsselten Direkteinwahlverbindungen über den integrierten Dialer des Clients. Soll eine Regel für VPN-Netze gelten, so muss diese Option aktiviert werden.

Protokoll

Je nach Anwendung oder Art der Verbindung ist das entsprechende Protokoll zu wählen:

TCP, UDP, ICMP, GRE, ESP, AH, IGRP, RSVP, IPv6 oder IPv4, Alle

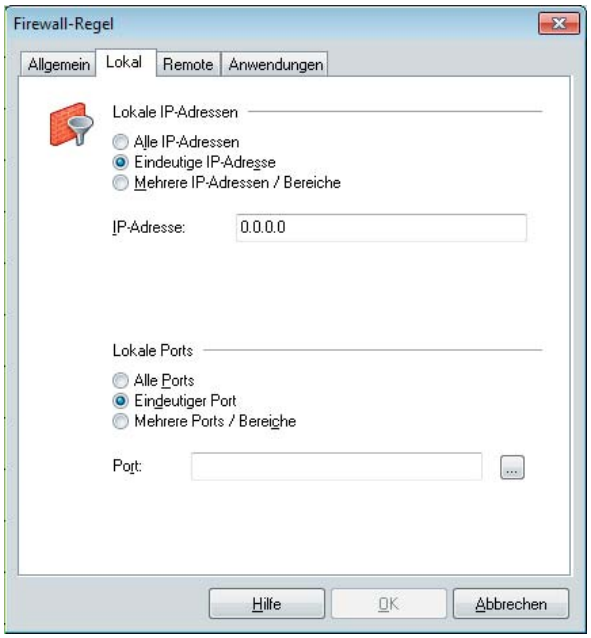
Verbindungssteuerung

Über diese Parameter wird die Art der Verbindung beeinflusst.

Sie wählen z.B. die Option, dass die hier konfigurierte Regel “nur gültig bei inaktiver VPN-Verbindung” ist, wenn Sie wünschen, dass z.B. eine Internet-Verbindung bei gleichzeitig bestehender VPN-Verbindung ausgeschlossen wird, ansonsten aber Internet-Verbindungen zu unbekannten Netzen zugelassen sein sollen. Dazu muss diese Regel für “unbekannte Netze” angewendet werden, d.h. diese Regel muss den Zugang zu unbekannten Netzen zulassen.

Die Option “kein automatischer Verbindungsaufbau” steht nur bei gesperrter Grundeinstellung zur Verfügung. Sie ist nur sinnvoll, wenn im Telefonbuch im Parameterfeld “Verbindungssteuerung” der Verbindungsaufbau auf “automatisch” gestellt wurde. Für die über diese Regel definierten Datenpakete findet bei Aktivierung dieser Funktion kein automatischer Verbindungsaufbau statt, für andere Datenpakete schon.

Firewall-Regel / Lokal



Auf dieser Registerkarte werden die Filter für die lokalen IP-Adressen und IP-Ports eingestellt.

Lokale IP-Adressen

Bei gesperrter Grundeinstellung werden diejenigen Datenpakete von der Firewall nach außen durchgelassen, deren Quelladresse (Source Address) mit der unter “Lokale IP-Adressen” übereinstimmt oder im Gültigkeitsbereich liegt. Von den eingehenden Datenpaketen werden diejenigen durchgelassen, deren Zieladresse (Destination Address) mit der unter “Lokale IP-Adressen” übereinstimmt oder im Gültigkeitsbereich liegt.

Alle IP-Adressen
– umfasst alle Quell-IP-Adressen abgehender bzw. Ziel-IP-Adressen eingehender Pakete, unabhängig vom lokalen Netzwerkadapter.

Eindeutige IP-Adresse
– ist die für den lokalen Netzwerkadapter definierte IP-Adresse. Sie kann je nach Verbindung z.B. der Adresse der Ethernet-Karte, der WLAN-Karte oder auch dem VPN-Adapter zugeordnet sein.

Mehrere IP-Adressen
– bezeichnet einen Adressbereich oder Pool. Z.B. kann dies der IP-Adress-Pool sein, aus dem die vom DHCP Server an den Client zugewiesene Adresse stammt.

Lokale Ports

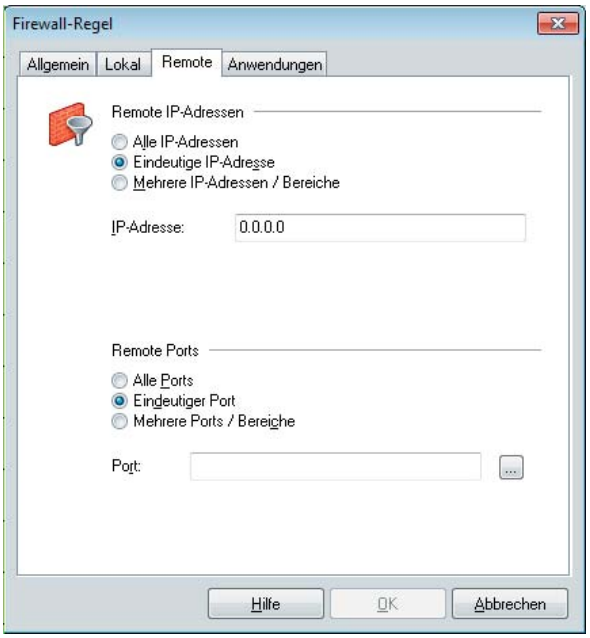
Ebenso verhält es sich bei gesperrter Grundeinstellung mit den IP-Ports. Diejenigen Datenpakete werden nach außen gelassen, deren Quell-Port (Source Port) unter die Definition der lokalen Ports fällt. Von den eingehenden Datenpaketen werden die durchgelassen, deren Ziel-Port (Destination Port) unter die Definition der lokalen Ports fällt.

Alle Ports
– erlaubt Kommunikation über alle Quellports bei ausgehenden und Ziel-Ports bei eingehenden Paketen.

Eindeutiger Port
– diese Einstellung sollte nur dann verwendet werden, wenn dieses System einen Server-Dienst zur Verfügung stellt (z.B. Remote Desktop auf Port 3389).

Mehrere Ports
– diese Einstellung sollte nur dann verwendet werden, wenn sich die lokalen Ports zu einem Bereich zusammenfassen lassen, die von einem Dienst benötigt werden, der auf diesem System zur Verfügung gestellt wird (z. B. FTP Ports 20/21).

Firewall-Regel / Remote



Auf dieser Registerkarte werden die Filter für die remote IP-Adressen und IP-Ports eingestellt.

Remote IP-Adressen

Bei gesperrter Grundeinstellung werden diejenigen Datenpakete von der Firewall nach außen durchgelassen, deren Zieladresse (Destination Address) mit der unter “Remote IP-Adressen” übereinstimmt oder im Gültigkeitsbereich liegt. Von den eingehenden Datenpaketen werden diejenigen durchgelassen, deren Quelladresse (Source Address) mit der unter “Remote IP-Adressen” übereinstimmt oder im Gültigkeitsbereich liegt.

Mit den Einstellungen unter Remote-IP-Adressen lässt sich festlegen, mit welchen entfernten IP-Adressen das System kommunizieren darf.

Alle IP-Adressen
– erlaubt die Kommunikation mit beliebigen IP-Adressen der Gegenseite, ohne Einschränkung.

Eindeutige IP-Adresse
– lässt nur Kommunikation mit der hier angegebenen IP-Adresse auf der Gegenseite zu.

Mehrere IP-Adressen /-Bereiche
– gestattet die Kommunikation mit verschiedenen IP-Adressen auf der Gegenseite entsprechend der Einträge.

Remote Ports

Ebenso verhält es sich bei gesperrter Grundeinstellung mit den IP-Ports. Diejenigen Datenpakete werden von der Firewall nach außen gelassen, deren Ziel-Port (Destination Port) unter die Definition der remote Ports fällt. Von den eingehenden Datenpaketen werden die durchgelassen, deren Quell-Port (Source Port) unter die Definition der remote Ports fällt.

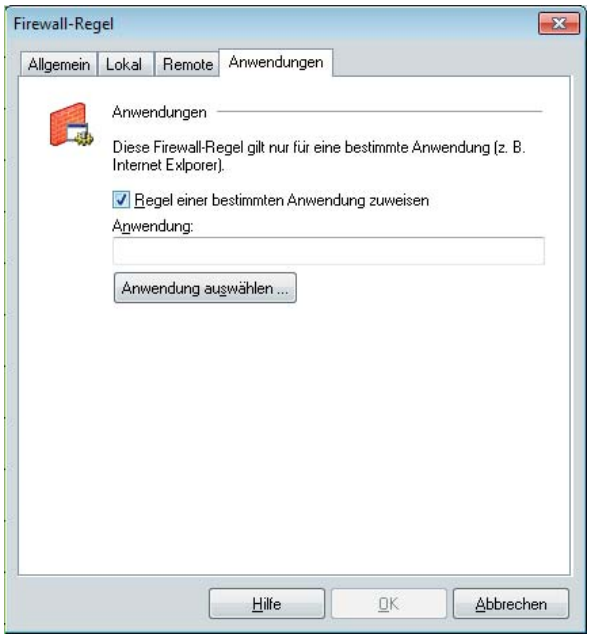
Mit den Einstellungen unter Remote Ports lässt sich festlegen, über welche Ports mit entfernten Systemen kommuniziert werden darf.

Alle Ports
– setzt keinerlei Beschränkungen hinsichtlich Ziel-Port bei abgehenden bzw. Quell-Port bei eingehenden Paketen.

Eindeutiger Port
– lässt nur eine Kommunikation über den angegebenen Port zu, wenn dieser als Ziel-Port im abgehenden bzw. als Quell-Port im eingehenden Paket vorkommt. Soll z.B. eine Regel nur Telnet zu einem anderen System zulassen, ist hier Port 23 einzutragen.

Mehrere Ports / Bereiche
– können verwendet werden, wenn mehrere Ports für eine Regel verwendet werden sollen (z. B. FTP Port 20/21).

Firewall-Regel / Anwendungen



Regel einer bestimmten Anwendung zuweisen

– besagt, dass (bei gesperrter Grundeinstellung) für diese Anwendung eine Verbindung möglich ist. Wird über den Button “Anwendung auswählen” eine lokal installierte Anwendung, wie z. B. ping.exe, selektiert, so kann nur diese Applikation kommunizieren. In diesem Fall dürfen nach dieser Regel nur Pings ausgeführt werden.

In diesem Beispiel sollte dann auch beachtet werden, dass vom **Protokoll** her ICMP zugelassen ist. (Abb. rechts oben)

Beachten Sie, dass auch der zugehörige **Port** selektiert sein muss. Für eine E-Mail-Anwendung (80). (Abb. rechts unten)

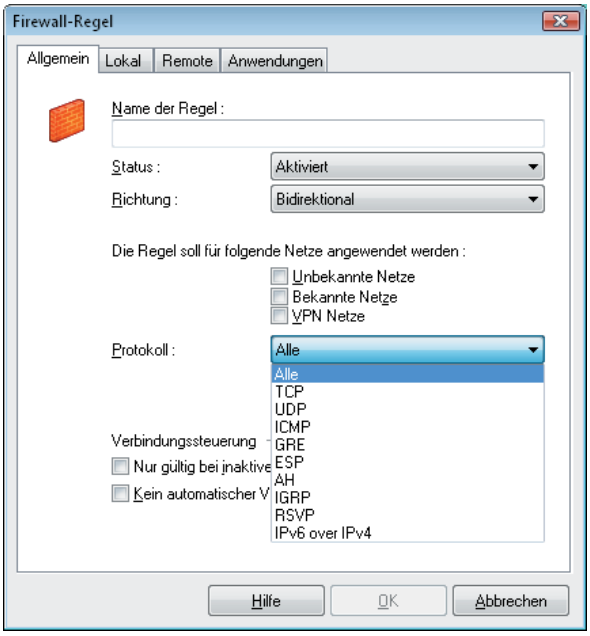
Einschränkung

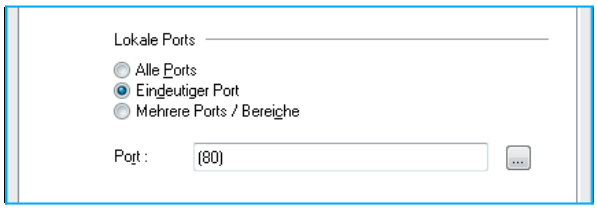
Die Kommunikation über eine Anwendung (Browser, Port 80) kann von der Firewall geblockt werden, wenn:

1. ein Virenscanner aktiv ist der nach dem Prinzip der Content Security arbeitet.
2. in der Firewall eine anwendungsabhängige Regel für einen Browser über Port 80 eingerichtet wurde und

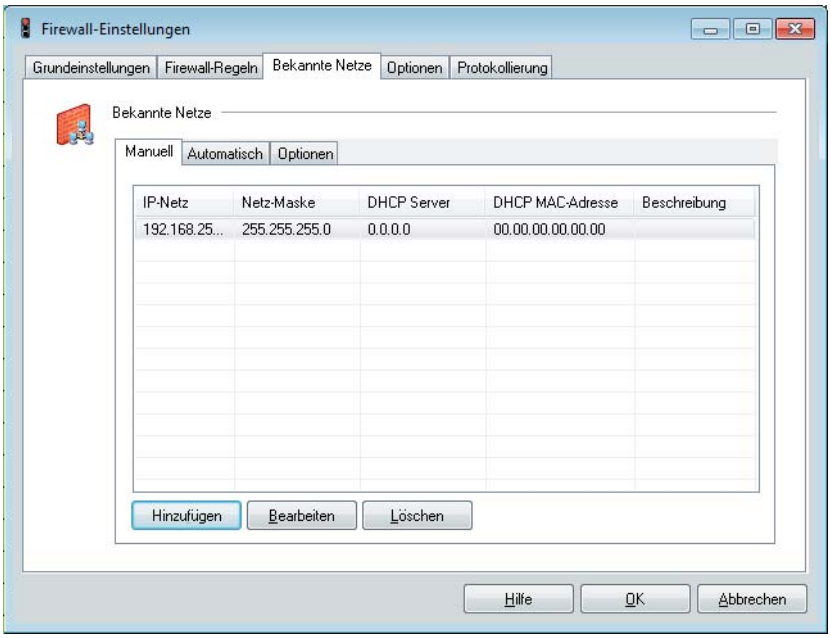
Abhilfe:

1. Virenscanner deaktivieren.
2. Bei Verwendung von nur einem Browser kann die Aktivität des Virenscanners gestattet werden, indem seine Exe-Datei in der anwendungsabhängigen Regel eingetragen wird. (Über diese Regel wird jeder Browser berechtigt, eine Internet-Verbindung aufzubauen.)





Konfigurationsfeld Bekannte Netze



Wurde im Konfigurationsfeld “Firewall-Regeln” definiert, dass eine Regel auf Verbindungen mit bekannten Netzen (Friendly Nets) anzuwenden ist, so wird diese Regel immer dann angewendet, wenn ein Netz nach den hier anzugebenden Kriterien als Friendly Net identifiziert werden kann, also der LAN-Adapter sich in einem Friendly Net befindet.

Was ein Friendly Net ist, wird vom Administrator zentral verbindlich festgelegt. Dies kann erfolgen durch eine manuelle Konfiguration oder mittels des Automatismus über Friendly Net Detection.

Die manuelle Definition eines bekannten Netzes durch den Administrator und die automatische Erkennung eines bekannten Netzes mittels Friendly Net Detection schließen sich nicht aus, sondern können gleichzeitig eingesetzt und über die Registerkarten “Manuell” und “Automatisch” konfiguriert werden.

Die Signalisierung eines Friendly Net erfolgt im Monitor durch das Firewall-Symbol, das sich grün färbt, sobald sich der Client in ein Friendly Net eingewählt hat.

Bekannte Netze / Manuell

Wurde im Konfigurationsfeld “Firewall-Regeln” definiert, dass eine Regel auf Verbindungen mit bekannten Netzen (Friendly Nets) anzuwenden ist, so wird diese Regel immer angewendet, wenn ein Netz nach den hier anzugebenden Kriterien als Friendly Net identifiziert werden kann, bzw. der LAN-Adapter sich in einem Friendly Net befindet.

Der LAN-Adapter des Clients befindet sich dann in einem Friendly Net wenn:

IP-Netze und Netzmaske

– die IP-Adresse des LAN-Adapters aus dem angegebenen Netzbereich stammt. Ist z. B. das IP-Netz 192.168.254.0 mit der Maske 255.255.255.0 angegeben, so würde die Adresse 192.168.254.10 auf dem Adapter eine Zuordnung zum bekannten Netz bewirken.

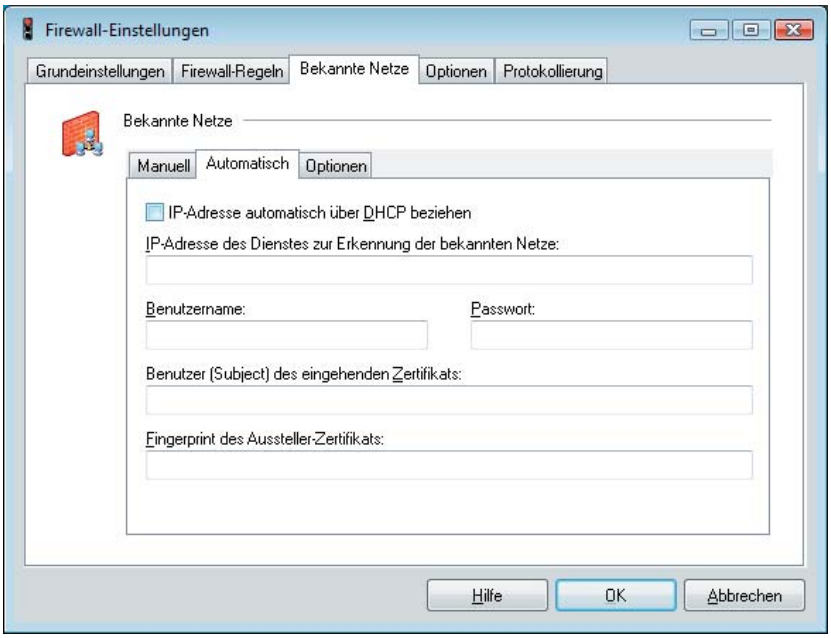
DHCP Server

– diese IP-Adresse von dem DHCP Server zugewiesen wurde, der die hier angegebene IP-Adresse besitzt;

DHCP MAC-Adresse

– wenn dieser DHCP Server die hier angegebene MAC-Adresse besitzt. Diese Option kann nur dann verwendet werden, wenn sich der DHCP Server im selben IP-Subnet befindet wie der DHCP Client. Je mehr dieser Bedingungen erfüllt werden, desto präziser ist der Nachweis, dass es sich um ein vertrautes Netz handelt. Die Zuordnung eines Adapters zu unbekannten oder bekannten Netzen wird automatisch protokolliert im Log-Fenster des Client-Monitors und in der Log-Datei der Firewall (siehe **Protokollierung**), wenn dieser DHCP Server die hier angegebene MAC-Adresse besitzt.

Bekannte Netze / Automatisch



Was ein Friendly Net ist, wird vom Administrator zentral verbindlich festgelegt. Die Signalisierung eines Friendly Net erfolgt im Monitor durch das Firewall-Symbol, das sich grün färbt, sobald sich der Client in ein Friendly Net eingewählt hat.

Für die automatische Erkennung ist ein Friendly Net Detection Server (FNDS) erforderlich, d. h. eine Softwarekomponente, die in einem als "Friendly Net" definierten Netz installiert und über IP erreichbar sein muss.

IP-Adresse automatisch über DHCP beziehen

Mit dieser Option erhält der Client automatisch die IP-Adresse des FND Servers über DHCP.

Voraussetzung ist, dass über den LAN-Adapter des Clients eine DHCP-Verhandlung angestoßen wird, um die IP-Adresse für den LAN-Adapter automatisch von einem DHCP Server zu beziehen. (Dies ist die Standard-Konfiguration in den Netzwerkeinstellungen des Betriebssystems.)

Am DHCP Server des Firmennetzes muss eine DHCP-Standardoption hinzugefügt werden, die den Code 159 und die IP-Adresse des FND Servers erhält, die dann automatisch mit der DHCP-Verhandlung verteilt wird.

IP-Adresse des Dienstes zur Erkennung der bekannten Netze

Erforderlich ist ein **Friendly Net Detection Server** (FNDS), d. h. eine Softwarekomponente von NCP, die in einem als "Friendly Net" definierten Netz installiert werden muss. Dieser Friendly Net Detection Server muss über IP erreichbar sein und seine IP-Adresse muss hier eingetragen werden. Maximal können die IP-Adressen (oder Host-Namen) von zwei FDNS, durch Komma getrennt, eingetragen werden.

Benutzername, Passwort (FNDS)

Die Authentisierung des FND Servers erfolgt über MD5 oder TLS. Hier einzutragender Benutzername und Passwort müssen mit jenen am **FNDS** hinterlegten übereinstimmen. Siehe auch **Authentisierung mit MD5 und TLS**.

Benutzer (Subject) des eingehenden Zertifikats

Das eingehende Zertifikat des FNDS wird auf diesen String hin geprüft. Nur bei Gleichheit handelt es sich um ein Friendly Net.

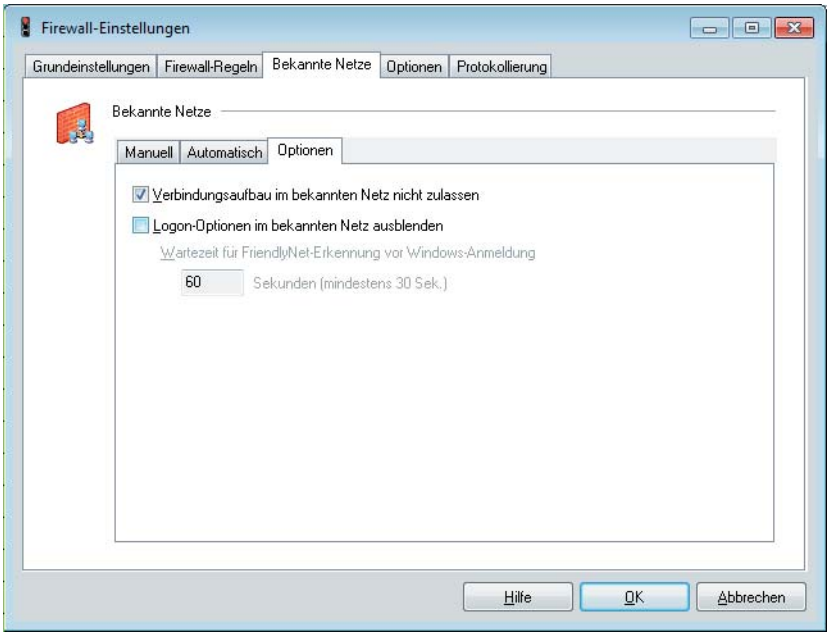
Fingerprint des Aussteller-Zertifikats

Um ein Höchstmaß an Fälschungssicherheit bieten zu können, muss der Fingerprint des Aussteller-Zertifikats überprüft werden können. Er muss mit dem hier eingegebenen Hash-Wert übereinstimmen.

Friendly Net Detection mittels TLS

Soll die Friendly Net Detection mittels TLS erfolgen (einschließlich einer Authentisierung über den Fingerprint des Aussteller-Zertifikats), so muss sich im Installationsverzeichnis \CaCerts dieses Aussteller-Zertifikat befinden und dessen Fingerprint muss mit dem hier konfigurierten übereinstimmen. Siehe auch **Authentisierung mit MD5 und TLS**.

Bekannte Netze / Optionen



Optional können bestimmte Funktionen für Clients, die sich bereits im bekannten Netz befinden, ausgeblendet werden.

Verbindungaufbau im bekannten Netz nicht zulassen

Ist diese Option eingeschaltet, so ist kein zusätzlicher VPN-Tunnelaufbau mehr möglich, wenn sich der Client bereits im bekannten Netz befindet. Der Button für den Verbindungsaufbau (bzw. der Menüpunkt) im Client-Monitor wird deaktiviert. Eine bereits bestehende VPN-Verbindung, die möglicherweise durch eine andere Anwendung hergestellt wurde, kann jedoch getrennt werden.

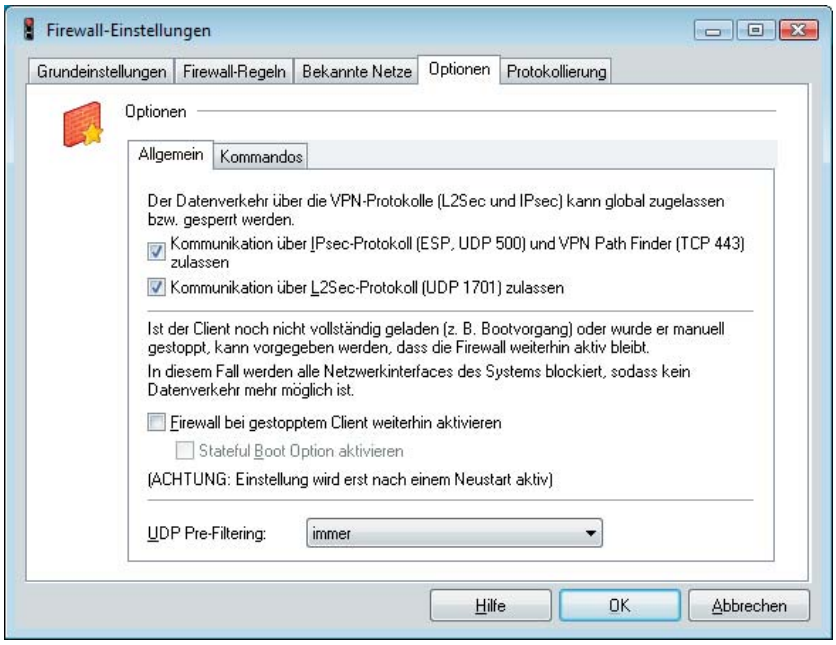
Logon-Optionen im bekannten Netz ausblenden

Für den Fall, dass sich der Client bereits im bekannten Netz befindet, können die Logon-Optionen zur Domänen-Anmeldung hier ausgeblendet werden.

Wartezeit für Friendly Net-Erkennung vor Windows-Anmeldung

Die Zeitspanne für die automatische Friendly Net Detection kann unabhängig vom Timeout-Wert eingegeben werden. Der Wert für die Zeit der Netzsuche muss mindestens 30 Sekunden sein. (Standard sind 60 Sekunden).

Konfigurationsfeld Optionen



Optionen / Allgemein

Bei gesperrter Grundeinstellung kann der Aufbau von VPN-Verbindungen über das Register "Allgemein" global zugelassen werden. Im Register "Kommandos" können Passwort und Zeitspanne hinterlegt werden, um die Firewall temporär von der Kommandozeile aus zu öffnen.

Kommunikation über IPsec und Pathfinder global zulassen

Bei gesperrter Grundeinstellung kann der Aufbau von VPN-Verbindungen über dieses Register global zugelassen werden. Folgende für den Tunnelaufbau benötigten Protokolle und Ports werden per automatisch generierter Filter **für IPsec** freigegeben:
UDP 500 (IKE ISAKMP),
IP-Protokoll 50 (ESP),
UDP 4500 (NAT-T),
UDP 67 (DHCPS),
UDP 68 (DHCPC),
TCP 443 (Pathfinder, falls konfiguriert)
Diese Protokolle werden **für L2sec** freigegeben:
UDP 1701 (L2TP),
UDP 67 (DHCPS),
UDP 68 (DHCPC)

Diese globale Definition erspart die Einrichtung von Einzelregeln für die jeweilige VPN-Variante.

Darüber hinaus wird bei Aktivierung dieser Option auch DHCP (UDP 68) zugelassen, um automatisch IP-Adressen auf angeschlossenen Adaptern beziehen zu können.

Bitte beachten Sie, dass dadurch lediglich der Tunnelaufbau ermöglicht wird. Existieren keine weiteren Regeln für VPN-Netze, die eine Kommunikation im Tunnel zulassen, kann über die VPN-Verbindung kein Datenaustausch erfolgen.

Firewall bei gestopptem Client weiterhin aktivieren

Die Firewall kann auch bei gestopptem Client aktiv sein, wenn diese Funktion selektiert wird. In diesem Zustand wird jedoch jede Kommunikation unterbunden, so dass keinerlei Datenverkehr möglich ist, solange der Client deaktiviert ist. Wird oben genannte Funktion nicht genutzt und der Client gestoppt, so wird auch die Firewall deaktiviert.

Stateful Boot-Option aktivieren

Ist die Firewall auch bei gestopptem Client aktiv geschaltet, so kann mit dieser Funktion Stateful Inspection eingeschaltet werden. Damit ist die Kommunication von diesem PC in eine anderes Netz möglich.

Diese Einstellung wird erst nach einem Neustart des Dienstes (Reboot) aktiv.

UDP Pre-Filtering

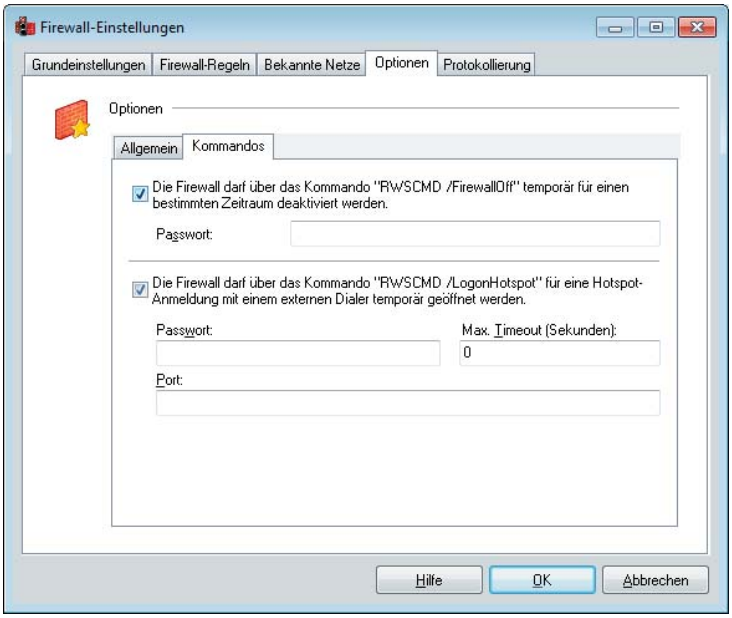
In der Standardeinstellung werden bei gestartetem Client (unabhängig von der Firewall) DP-Pakete ausgefiltert, so dass eine Verbindung von außen zum Client PC nicht möglich ist. Ist auf dem Client PC eine Anwendung mit Server-Funktion gestartet, die auf UDP-Datentransfer basiert (wie z. B. Terminalanwendungen oder NTP), kann sich diese Standardeinstellung störend auf die Datenkommunikation auswirken. Daher kann diese Standardeinstellung ausgeschaltet oder auf die UDP-Pakete unbekannter Netze beschränkt werden.

immer
Standardeinstellung. In dieser Schalterstellung gelangen bei gestartetem Client keine UDP-Pakete auf den Client PC.

nur bei unbekannten Netzen
In dieser Schalterstellung wirkt der UDP-Filter nur auf Pakete, die über Adapter unbekannter Netze eintreffen.

aus
Wird der Filter ausgeschaltet, gelangen alle UDP-Pakete auf den Client PC. Diese Einstellung sollte nur verwendet werden, wenn Probleme mit einer Anwendung auftreten.

Optionen / Kommandos



Die Firewall darf über das Kommando "RWSCMD /Firewalloff" temporär für einen bestimmten Zeitraum deaktiviert werden.

Soll das temporäre Öffnen der Firewall über die Kommandozeile möglich sein, muss diese Funktion hier aktiviert werden.

Die Eingabe eines Passworts ist optional. Wird hier ein Passwort eingegeben, muss dieses Passwort auch in der Kommandozeile wiederholt werden.

Das Kommando lautet:
`rwscmd /firewalloff [Passwort] [Timeout]`

Ein Timeout kann in der Kommandozeile ganzzahlig in Sekunden angegeben.

Die Firewall wird wieder aktiv wenn der Timeout abgelaufen ist oder nach dem Kommando:
`rwscmd /firewallon`

Die Firewall darf über das Kommando "RWSCMD /LogonHotspot" für eine Hotspot-Anmeldung mit einem externen Dialer temporär geöffnet werden.

Soll die Firewall für die Hotspot-Anmeldung mit externem Dialer geöffnet werden, muss diese Funktion hier aktiviert werden.

Die Eingabe eines Passworts ist optional. Wird hier ein Passwort eingegeben, muss dieses Passwort auch in der Kommandozeile wiederholt werden.

Die Eingabe des "Max. Timeouts" ist optional. Ein hier eingetragener Wert dient nur der Begrenzung des Timeouts, der in der Kommandozeile eingegeben werden muss.

Zusätzliche Ports zu den Standard-Ports 80 und 443, die automatisch zur Hotspot-Anmeldung geöffnet werden, werden dann geöffnet, wenn sie hier eingetragen werden. Mehrere Ports werden mit einem Komma getrennt.

Das Kommando lautet:
`rwscmd /logonhotspot [Passwort] [Timeout]`

Dabei kann der vom Benutzer eingegebene Timeout nie länger sein als der in den Kommando-Einstellungen der Firewall gespeicherte.

Die Firewall wird wieder aktiv wenn der Timeout abgelaufen ist oder nach dem Kommando:
`rwscmd /firewallon`

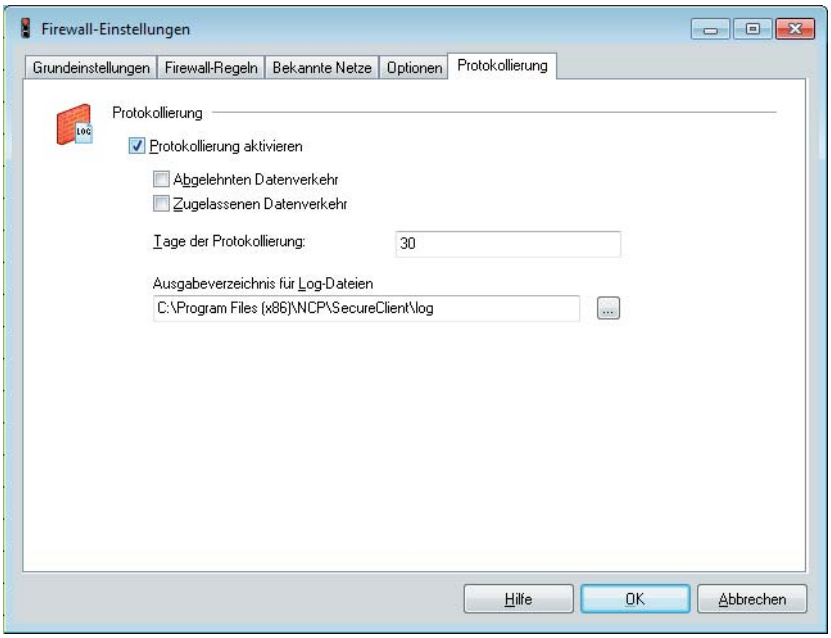
Hotspot-Anmeldung für externe Dialer zulassen

Wenn diese Funktion aktiviert ist, kann über einen externen Dialer eine Hotspot-Anmeldung erfolgen. Dazu wird die Kommandozeilen-Schnittstelle rwscmd.exe aufgerufen. Mit dem Befehl
`rwscmd /logonhotspot [Timeout]`
wird die Firewall für die Ports 80 (HTTP) und 443 (HTTPS) freigeschaltet. Damit wird eine dynamische Regel erzeugt, die den Datenverkehr zulässt, bis der übergebene Timeout (in Sekunden) abgelaufen ist.

Ports

Durch Komma getrennt, können weitere Ports (bis zu 10) hinzugefügt werden, welche für die Hotspot-Anmeldung zusätzlich zu Port 80 und 443 geöffnet werden sollen.

Konfigurationsfeld Protokollierung



Protokollierung aktivieren

Die Aktivitäten der Firewall werden je nach Einstellung in eine Log-Datei geschrieben. Das "Ausgabeverzeichnis für Log-Dateien" befindet sich standardmäßig im Installationsverzeichnis unter LOG\.

Die Log-Dateien für die Firewall sind im reinen Textformat geschrieben und benannt als Firewall-lyymmdd.log. Sie beinhalten eine Beschreibung vom "abgelehnten Datenverkehr" und/oder "zugelassenen Datenverkehr". Wurde keine dieser Optionen selektiert, so werden nur Statusinformationen zur Firewall hinterlegt.

Die Log-Dateien werden bei jedem Start der Firewall geschrieben. Maximal werden davon so viele im Log-Verzeichnis gehalten, wie als Anzahl der "Tage der Protokollierung" eingegeben wurde.

Bitte beachten Sie, dass es bei aktivierter Protokollierung zu Performance-Einbußen kommen kann, da für jedes Paket, für welches diese Einstellung gilt, ein entsprechender Protokolltext ausgegeben werden muss.

Installation und Konfiguration des FND-Servers

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

Sie besteht aus fünf Dateien, die Sie in ein beliebiges Verzeichnis eines PCs kopieren, der sich in dem als Friendly Net zu definierenden Netzwerk befindet.

Die Dateien haben folgende Funktionen:

`ncpfnd.exe`
Dienstprogramm (Friendly Net Detection Server)

`fndtest.exe`
Test-Client

`ncpfnd.conf`
Konfigurationsdatei

`vpngw.p12`
PKCS#12-Datei (Soft-Zertifikat)

`readme.txt`
Kommandobeschreibung

Nach dem Kopieren der Dateien kann der Dienst installiert werden. Dazu wechseln Sie in das Installationsverzeichnis und verwenden das Kommando:

```
ncpfnd -install
```

Nach einer erfolgreichen Installation erscheint die Meldung:

```
Service successfully installed
```

Konfiguration des FND Servers

Die Konfiguration des FND Servers erfolgt durch die Editierung der Konfigurationsdatei ncpfnd.conf, die in verschiedene Kapitel unterteilt ist.

[General]

In diesem Kapitel werden die wichtigsten Parameter für den Dienst FNDS festgelegt.

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

LogLevel

Der LogLevel ist normalerweise auf “O” gesetzt, so dass keine Log-Meldungen geschrieben werden. Log-Meldungen werden nur für Wartungszwecke benötigt.

LogPath

Der LogPath ist das aktuelle Verzeichnis der FNDS Software. Er wird nur für Wartungszwecke benötigt.

Port

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

LocalIPAdress

LocalIpAddr, 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. 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 (siehe unten “Konfiguration des Clients”). D. h. 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 (für SSL oder TLS) benötigt. Das Soft-Zertifikat vpngw.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 Aussteller-Zertifikat am Client in das Installationsverzeichnis unter \CaCerts eingespielt werden muss. Das Aussteller-Zertifikat für Testzwecke, das standardmäßig mit der Client Software ausgeliefert wird, befindet sich im Installationsverzeichnis der NCP Software und hat den Namen ncpsupportca.pem. Beide NCP-Zertifikate, vpngw.p12 und ncpsupportca.pem, dienen nur Testzwecken.

PKCS12Pin

Als Pkcs12Pin wird die PIN des hier gespeicherten Zertifikats fest eingegeben. Die PIN “1234" gilt nur für das NCP-Testzertifikat.

[SysLog]

Nach Konfiguration dieses Kapitels können Log-Meldungen an einen Syslog Server übertragen werden.

```
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.

[FND-USER 1]

Dieses Kapitel in der Beispiel-Konfiguration legt als Authentisierungs-Protokoll MD5 fest. Das heißt, 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”.

Password

“Password” entspricht dem Parameter **Passwort** in den Firewall-Einstellungen des Clients unter der Rubrik “Bekannte Netze”.

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 der Konfigurationsdatei [FND-USER 1] 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.

[FND-USER 2]

Dieses Kapitel in der Beispiel-Konfiguration legt als Authentisierungs-Protokoll TLS fest. Das heißt, 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 FNDS-Zertifikats notwendig sind, am Client zur Verfügung stehen. Außerdem kann am Client der Fingerprint des Aussteller-Zertifikats und der Benutzer (Subject) des FNDS-Zertifikats konfiguriert werden. Damit wird der mögliche “Nachbau” eines eines Friendly Nets ausgeschlossen (siehe weiter unten “Konfiguration am 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

“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”.

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.

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 dann von allen Anschlüssen des Netzwerks erreichbar sein, d. h. es müssen gegebenenfalls Änderungen an den Firewall-Regeln vorgenommen werden.

Betreibt ein Mitarbeiter sein Endgerät direkt am Firmen-Netzwerk, 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, so ist bestätigt, dass sich der Rechner in einem bekannten Netz befindet und die entsprechenden, für dieses Netz vorkonfigurierten, Firewall-Regeln werden automatisch aktiviert.

Zur folgenden Beschreibung beachten Sie auch Beispiel: **Automatische Anpassung der Firewall-Regeln in bekannten Netzen**.

Grundeinstellung

Die integrierte Personal Firewall des NCP Secure Clients ermöglicht eine sehr flexible Gestaltung von Firewall-Regeln. So besteht die Möglichkeit Regeln zu definieren, die von einer gesperrten Grundeinstellung (es ist alles verboten, was nicht erlaubt ist.) bzw. offene Grundeinstellung (es ist alles erlaubt, was nicht verboten ist) ausgehen. Normalerweise wird die “Gesperrte Grundeinstellung” eingestellt. (Siehe oben **Konfigurationsfeld Grundeinstellung**).

Filterregeln

Abhängig von der Grundeinstellung können Netzwerkpakete nach bestimmten Kriterien gefiltert werden. (Siehe oben **Konfigurationsfeld Firewall-Regeln**).

Die Kriterien, die in der Security Policy festgeschrieben sind, definieren sehr genau was ein Anwender von seinem Rechner aus in einem Netzwerk z. B. Intranet, zentrales Datennetz (Firmen-Netzwerk), Internet usw. darf und was nicht. Die Security Policy wird in der Regel vom Netzwerkadministrator erstellt und gepflegt.

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** die entsprechende Funktion.

Auf der Abbildung unten ist eine MD5-Konfiguration dargestellt. Vergleichen Sie dazu die Beschreibung zum Konfigurationskapitel **[FND-USER 1]**.

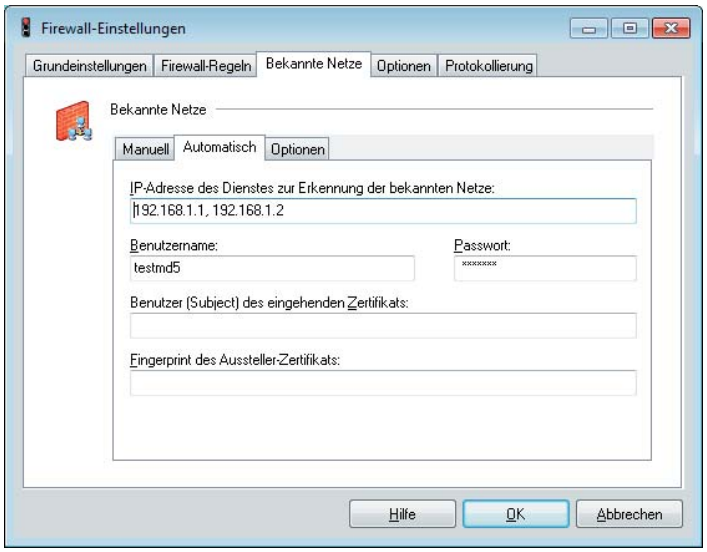
IP-Adresse des Dienstes zur Erkennung der bekannten Netze

Dies ist die IP-Adresse des Friendly Net Detection Server (FNDS), die der **LocalIpAddr** im Kapitel “General” der Konfigurationsdatei ncpfnd.conf entspricht.

Zur Erhöhung der Redundanz kann die IP-Adresse 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, so versucht er dreimal im Abstand von 3 Sekunden den ersten FND Server zu erreichen. Kann kein Kontakt hergestellt werden, wird die zweite IP-Adresse angewählt. (Siehe **NCP Friendly Net Detection**).

MD5-Konfiguration



Benutzername, Passwort (FNDS)

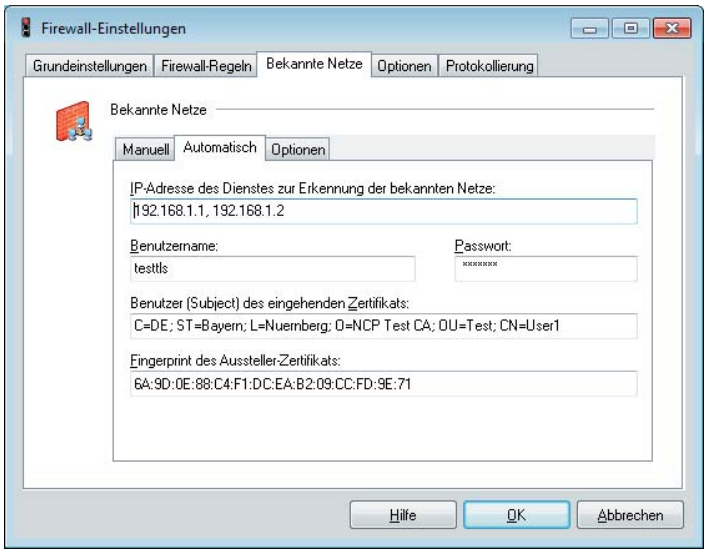
Die Authentisierung des Friendly Net Detection Servers erfolgt über MD5 oder TLS*. Hier einzutragender Benutzername und Passwort müssen mit jenen am FNDS hinterlegten übereinstimmen. Bei Einsatz von MD5 findet die Authentisierung über “Benutzername” und “Passwort” statt. Bei Einsatz von TLS kann das Passwort entfallen.

** Bei Friendly Net Detection wird immer EAP over UDP eingesetzt, sowohl bei MD5 als auch bei TLS.*

"Benutzername" und "Passwort" entsprechen **User-Name** und **Password** in den Kapiteln "FND-USER 1" und "FND-USER 2" in der Konfigurationsdatei ncpfnd.conf.

Auf der Abbildung unten ist eine TLS-Konfiguration dargestellt. Vergleichen Sie dazu die Beschreibung zum Konfigurationskapitel **[FND-USER 2]** des Servers.

TLS-Konfiguration



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 FNDS-Zertifikats nötig sind, müssen am Client im Installationsverzeichnis unter \CaCerts 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.

Start des NCPFND-Dienstes

Der Dienst NCPFND muss in der Dienste-Verwaltung des Systems als Autostarttyp "Automatisch" aufgenommen sein, dann wird er nach einem Boot-Vorgang des PCs automatisch gestartet.

Der Dienst kann auch manuell gestartet und gestoppt werden mit den Kommandos:

```
net start ncpfnd
```

und

```
net stop ncpfnd
```

Test

Mit dem Programm fndtest.exe kann der jeweilige Authentisierungstyp, der in der Konfigurationsdatei gesetzt wurde, getestet werden, ohne einen Client installieren zu müssen.

Dazu wird nach dem Kommando der Authentisierungstyp angegeben und die Client-Parameter wie oben beschrieben. Folgende Syntax wird verwendet:

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

Deinstallation

Um den Dienst zu deinstallieren, muss das Kommando eingegeben werden:

```
ncpfnd -remove
```

Dynamic Personal Firewall

Anwender die die Vorteile einer zentral administrierbaren Firewall inkl. friendly Net Detection nutzen möchten, jedoch keine VPN Funktionalität benötigen, können die Produktvariante der Dynamic Personal Firewall ohne VPN Client nutzen.

Mittels der Personal Firewall können Regelwerke und Applikationen definiert werde für: Ports, IP-Adressen und Segmente. Ein weiteres Sicherheitskriterium ist **Friendly Net Detection**, d. h. die automatische Erkennung von sicheren und unsicheren Netzen. In Abhängigkeit davon werden die entsprechenden Firewall-Regeln aktiviert bzw. deaktiviert.

Die lizenzierte Dynamic Personal Firewall erscheint zunächst nur im **Tray Icon**. Der Monitor muss über das Menü der Firewall im Tray Icon eigens eingeblendet werden. Anschließend können die Features der Firewall auch über das Ansichtmenü angezeigt werden. Nach der Installation sind Firewall und EAP als Standard-Features aktiviert. Nach Bedarf lönnen alle Features ein- oder ausgeblendet werden:

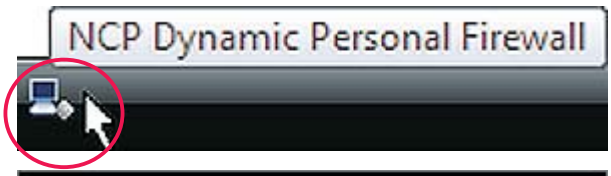
– Dialer für Internet-Einwahl (zusätzl. ext. Dialer)
– WLAN (auch Hotspot-Anmeldung)
– EAP (erweiterte Authentisierung in LAN / WLAN)
– Personal Firewall

Die NCP Dynamic Personal Firewall besitzt bis auf die VPN-Funktionalität alle Funktionalitäten der Software und ist wie der Secure Enterprise Client ebenso mit dem Secure Enterprise Management zentral via Update über LAN administrierbar.

Ein späteres Upgrade auf den Secure Enterprise Client ist mit dem entsprechenden Lizenzschlüssel jederzeit möglich.

Konfigurationsoberfläche der Dynamic Personal Firewall

Firewall in der Tray-Leiste

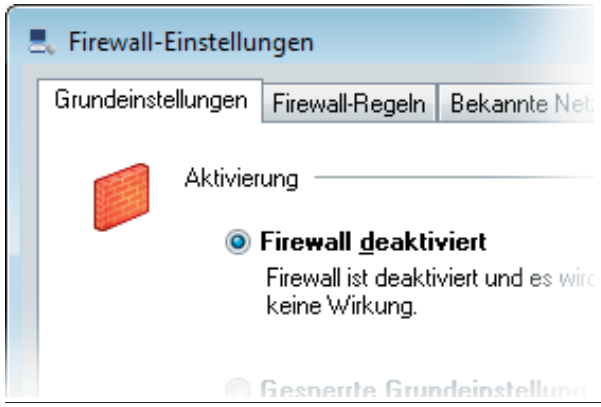


Nach der Installation (bzw. Lizenzierung) der Dynamic Personal Firewall erscheint sie zunächst nur im Tray Icon mit EAP-Option (Punkt rechts neben dem Symbol).

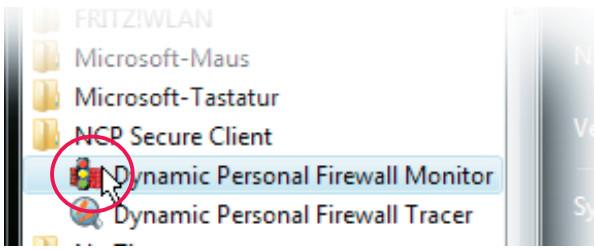
Nach einer Mausberührung erkennen Sie, dass sie noch deaktiviert ist.

Nach einem Mausklick auf das Tray-Icon öffnen Sie das Menü der Dynamic Personal Firewall:

– mit Klick auf “Firewall” gelangen Sie in das **Konfigurationsmenü der Personal Firewall** wie ab Seite 16 dieser Dokumentation beschrieben (Abb. unten links).

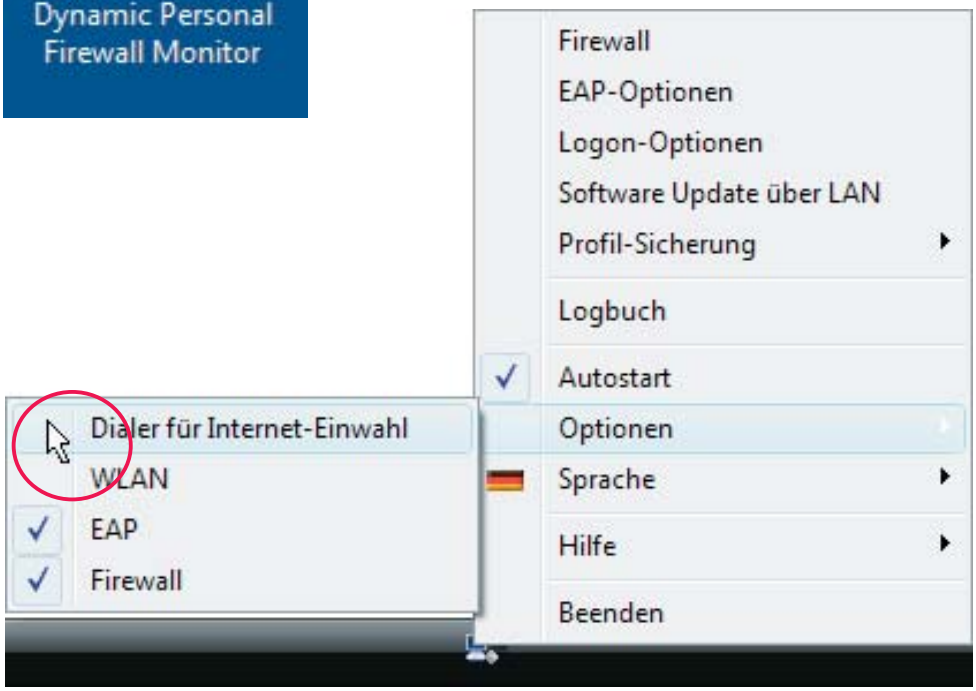


– die Autostart-Option ist in der Standardeinstellung aktiv. (Ohne die aktive Autostartoption ist die Firewall auch in der Tray-Leiste nicht mehr sichtbar und muss über das Windows-Startmenü als Tray-Icon gestartet werden, Abb. ganz unten rechts.)



Firewall-Monitor auf dem Desktop

Um die Konfigurationsoberfläche bequem auf dem Desktop erreichbar abzulegen, kann zunächst bei der benutzerdefinierten Installation das **Icon auf dem Desktop** angelegt werden (Abb. links).



Nach Abschluss der Installation muss zunächst über das Menü des Tray-Icons der Dialer für die Internet-Einwahl aktiviert werden, da der Dynamic Personal Firewall Monitor Bestandteil dieses Dialers ist.

Anschließend kann der Monitor der Firewall (Abb. links) über das Deskzop-Icon geöffnet und geschlossen werden.

– mit Klick auf “Firewall” gelangen Sie in das **Konfigurationsmenü der Personal Firewall** wie ab Seite 16 dieser Dokumentation beschrieben (Abb. unten links).

Aktivierung der Firewall

Um die Firewall zu aktivieren und nach Bedarf zu konfigurieren, gehen Sie vor wie in dieser Dokumentation ab Abschnitt **Konfigurationsmenü der Personal Firewall** beschrieben.

In der Oberfläche erkennen Sie die aktivierte Firewall an ihrem Symbol im Monitor oder in der Tray-Leiste (Abbildungen links) wie folgt:

Das Firewall-Symbol ist nur dann sichtbar, wenn die Firewall aktiviert ist. Ist die Personal Firewall mit definierten Regeln aktiv, so wird das Symbol in der Farbe Rot dargestellt.

Wurde ein Friendly Net (Friendly Net Detection) festgelegt, und befindet sich der LAN-Adapter darin, so wird das Firewall-Symbol in der Farbe Grün dargestellt.

Weitere Konfigurationen

Zu weiteren Konfigurationsmöglichkeiten der Software, sowie zu Profil-Sicherung und Update über LAN beachten Sie die Online-Hilfe und insbesondere folgende PDF-Dokumente:

Enterprise-Cl-Monitor

Enterprise-Cl-Parameter

Enterprise-Cl-Mobile-Computing

Index