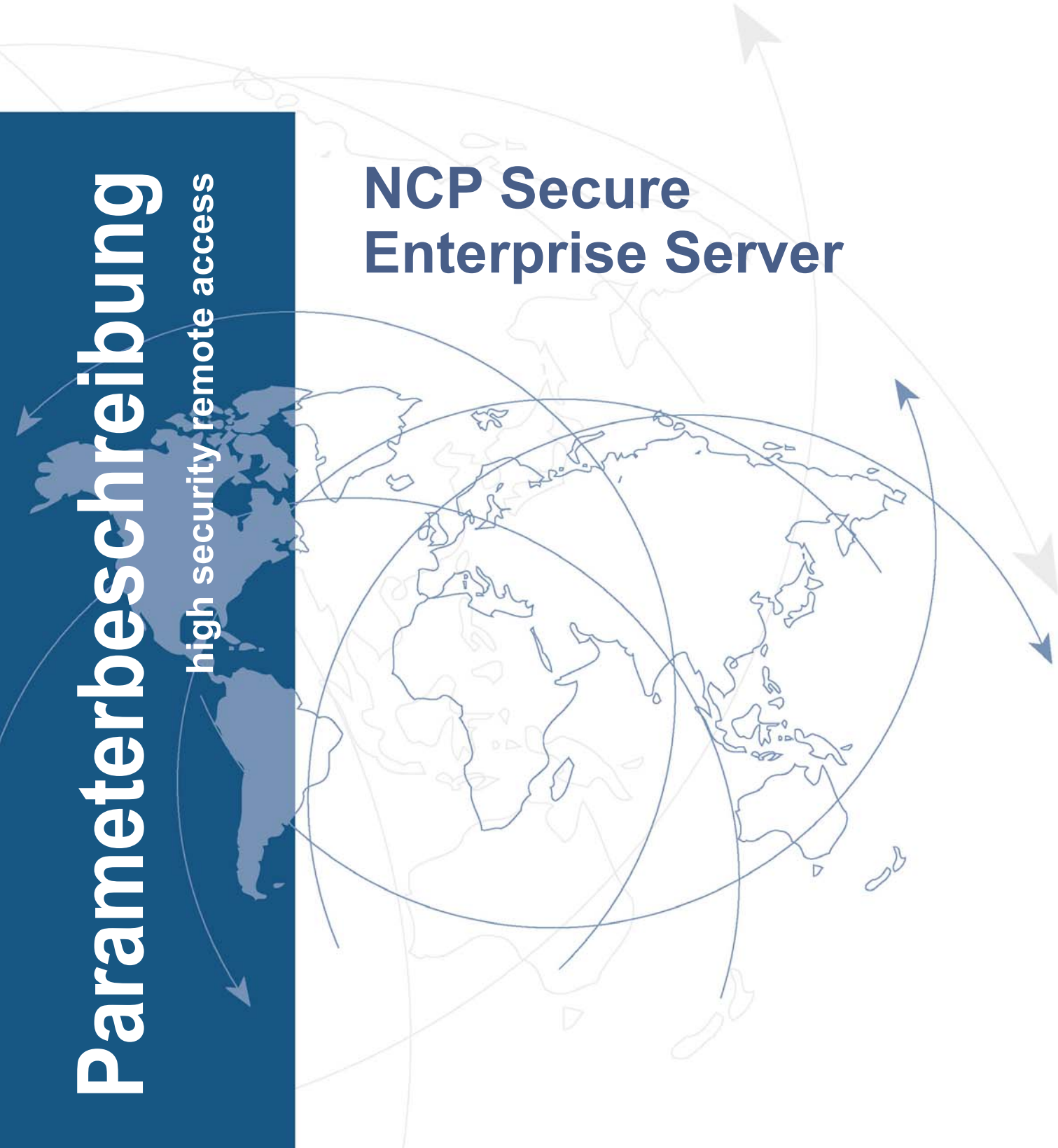
NCP
SECURE COMMUNICATIONS

Parameterbeschreibung

high security remote access

NCP Secure Enterprise Server



Secure Enterprise Server

Parameterbeschreibung

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

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

Server-Parameter

Diese Dokumentation beschreibt die Web-Oberfläche und die Parameter des Secure Servers 8.0, die darüber konfiguriert werden können.

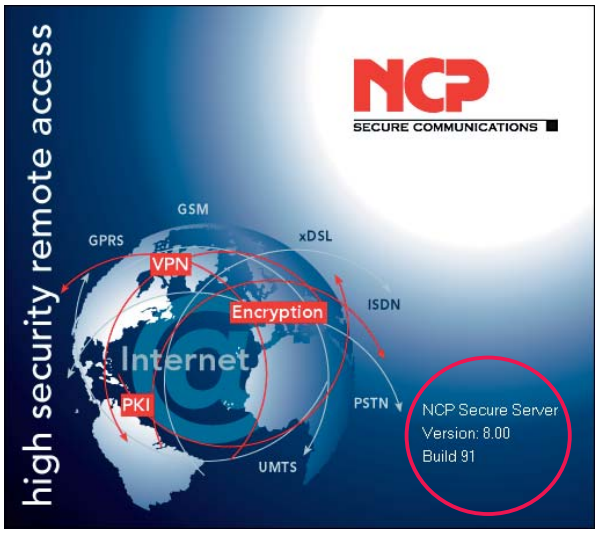
Voraussetzung für den Einsatz des Web-Interface ist die Installation eines Browsers und ein aktives Java Script.

Weitere Informationen zu Ausbaustufen und Produktvarianten erhalten Sie auf der NCP Website: http://www.ncp-e.com

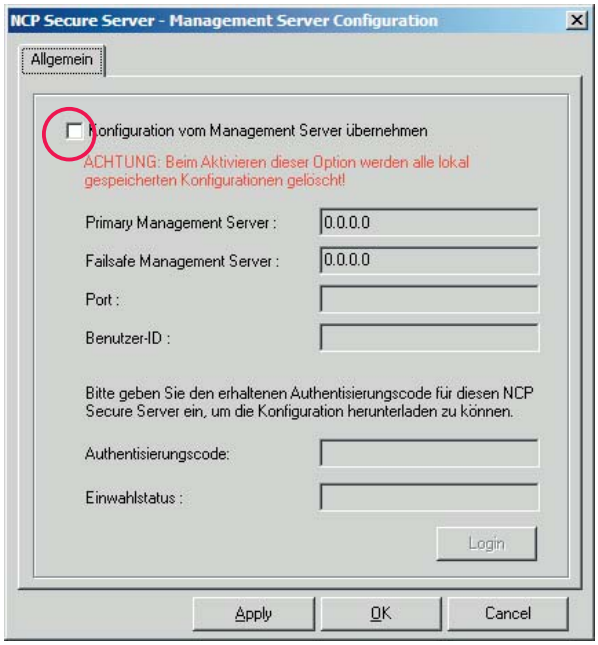
Server-Konfiguration

Nach der **Installation des Secure Servers** finden Sie in der Windows Programmgruppe drei Programme zum NCP Secure Enterprise Server (Abb. unten):

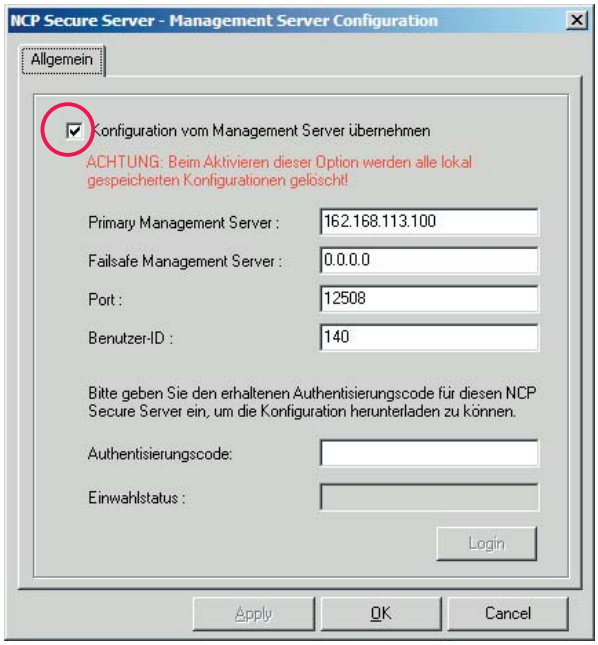
Das **Secure Server Popup** zeigt Versions- und Build-Nummer der Software (Abb. unten):



Über **Configuration SEM** legen Sie fest, ob die Konfiguration des Servers über das **Web-Interface** – wie in der Standardeinstellung nach der Installation erfolgen soll (Abb. unten)



– oder ob die Server-Konfiguration vom **Secure Enterprise Management (SEM)** heruntergeladen werden soll. In letzterem Fall muss die Funktion in unten stehender Abbildung aktiviert werden. Danach werden IP-Adresse und Port eingetragen. Die **Benutzer-ID** entspricht der **ID für Konfiguration** im Server Plug-in. Der **Authentisierungscode** wird in der Server-Konfiguration am SEM erzeugt*.



Der Authentisierungscode muss beim ersten Verbindungsaufbau zwischen Server und Management-System eingegeben werden. Durch Drücken des Login-Buttons wird die Verbindung hergestellt und die Konfiguration vom Management-System herunter geladen.

Wenn diese Art der Konfiguration durchgeführt wird, können über das Web-Interface keine Konfigurations-Einstellung vorgenommen werden! Die Administratoren haben nur Leserechte!

Wird die Konfiguration über das Web-Interface durchgeführt und zu einem späteren Zeitpunkt eine Konfiguration vom SEM heruntergeladen, geht die manuell über das Web-Interface gemachte Konfiguration verloren! Sie wird gelöscht!**

** Im Abschnitt **Server Plug-in** ist beschrieben wo sich diese Benutzer-ID befindet und wo der Authentisierungscode erzeugt wird.*
*** Eine Ausnahme bilden die **Endpoint Policies** und die **Routing Interfaces**.*

Web-Interface

Die Server-Konfiguration kann über das Web-Interface erfolgen, wenn nach der Installation des Servers in der Windows-Programmgruppe “NCP Secure Enterprise Server” die **Configuration** angeklickt wird.

Um zu verhindern, dass der Browser beim ersten Verbindungsaufbau zum Web-Interface das Server-Zertifikat als nicht vertrauenswürdig einstuft, sollte jedoch zuerst das Server-Zertifikat eingerichtet werden.

Einrichten des Server-Zertifikats

Nach der **Installation des Secure Servers** sollte das mitgelieferte Server-Zertifikat durch Ihr eigenes Server-Zertifikat ausgetauscht werden und dieses von Ihrem Browser importiert werden, solange dies noch nicht geschehen ist.

Das mitgelieferte Server-Zertifikat, das für das Web-Interface unmittelbar nach der Installation verwendet wird, befindet sich im Programmverzeichnis unter:
`NCP\NCPweb\websrv.p12`

Löschen Sie dieses Zertifikat und spielen Sie das Zertifikat ein, das vom Browser für das Web-Interface verwendet werden soll. (Dabei kann es sich auch um das Server-Zertifikat handeln, das in Ihrem PKI-Umfeld für IPSec / L2Sec-Verbindungen benutzt wird. Beachten Sie dazu die Beschreibung zu **Server-Zertifikate / Konfiguration**.)

Anschließend editieren Sie die Datei ncpweb.conf* indem Sie Pfad und Name des neuen Zertifikats eintragen.

** Die Konfigurationsdatei ncpweb.conf dient dazu, die Verbindung zwischen Browser und Secure Server zu definieren. Mögliche Änderungen der Datei sind unter* **Editieren von ncpweb.conf** *beschrieben. Bitte beachten Sie, dass das System neu gestartet werden muss, nachdem diese Datei bearbeitet wurde! (Dies kann im Web-Interface mit einem Restart-Button erfolgen unter “Statistik / Systeminformationen”.*

Verbindung zum lokalen Web-Interface

Mit einem Browser auf dem Installationsrechner kann unmittelbar nach der Installation das Web-Interface lokal über die Windows Startleiste “NCP Secure Enterprise Server / Configuration” gestartet werden. Mit Klick auf das “Configuration”-Programm wird der vorhandene Standard-Browser automatisch gestartet mit der URL:
`https://127.0.0.1:20112`

Die IP-Adresse 127.0.0.1 ist die lokale Adresse für den integrierten Web Server, 20112 bezeichnet den Port für den integrierten Web Server des Web-Interfaces. Dieser vorgegebene Port kann über die Konfigurationsdatei **ncpweb.conf** gegebenenfalls geändert werden.

https-Verbindung zum Web-Interface

Um eine erste Verbindung über das Internet aufbauen zu können, muss vorher unbedingt die offizielle IP-Adresse des Secure Servers festgelegt werden. Sie wird in den Netzwerkeinstellungen des Secure Server-Adapters des Betriebssystems eingegeben. In der Konfiguration des Secure Servers kann sie abgelesen werden unter “Routing Interfaces / Secure Server Adapter / IP-Adresse”. Diese IP-Adresse muss mit der im Browser einzugebenden übereinstimmen.

Nach dem Browser-Start geben Sie als URL ein:
– die IP-Adresse des Secure Servers-Adapters mit Doppelpunkt und
– den Port; z. B.:
`https://121.23.122.10:20112`

https = Damit bestimmen Sie in der Adressleiste des Browsers, dass die Verbindung über https durchgeführt wird.

Port = Die Angabe des Ports nach der Web-Adresse mit Doppelpunkt ist erforderlich, da nicht der Standard-Port (443) für https verwendet wird, sondern Port 20112. Dieser vorgegebene Port kann über die Konfigurationsdatei **ncpweb.conf** gegebenenfalls geändert werden.

Zugriff

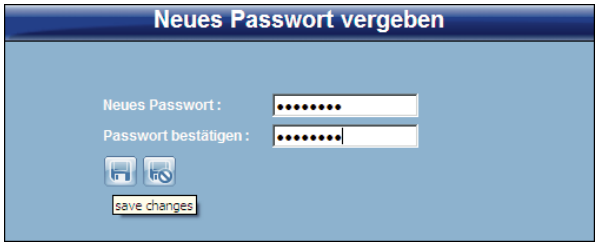
Nach dem Verbindungsaufbau wird Benutzername und Passwort abgefragt.

Erstes Login

Die erste Anmeldung erfolgt immer mit dem Benutzernamen “Administrator” (sofern es durch das **Plug-in** nicht anders vorgegeben wurde). Das Passwort ist frei wählbar. (Abb. unten)

Wird die Konfiguration des Servers vom Management-System herunter geladen, so muss ein Administrator das Passwort übernehmen, das am SEM erzeugt wurde. Dieses Passwort kann nicht verändert werden! (Siehe **Server Plug-in**)

Im zweiten Login-Fenster muss dieses Passwort erneut eingegeben und bestätigt werden. (Abb. unten)

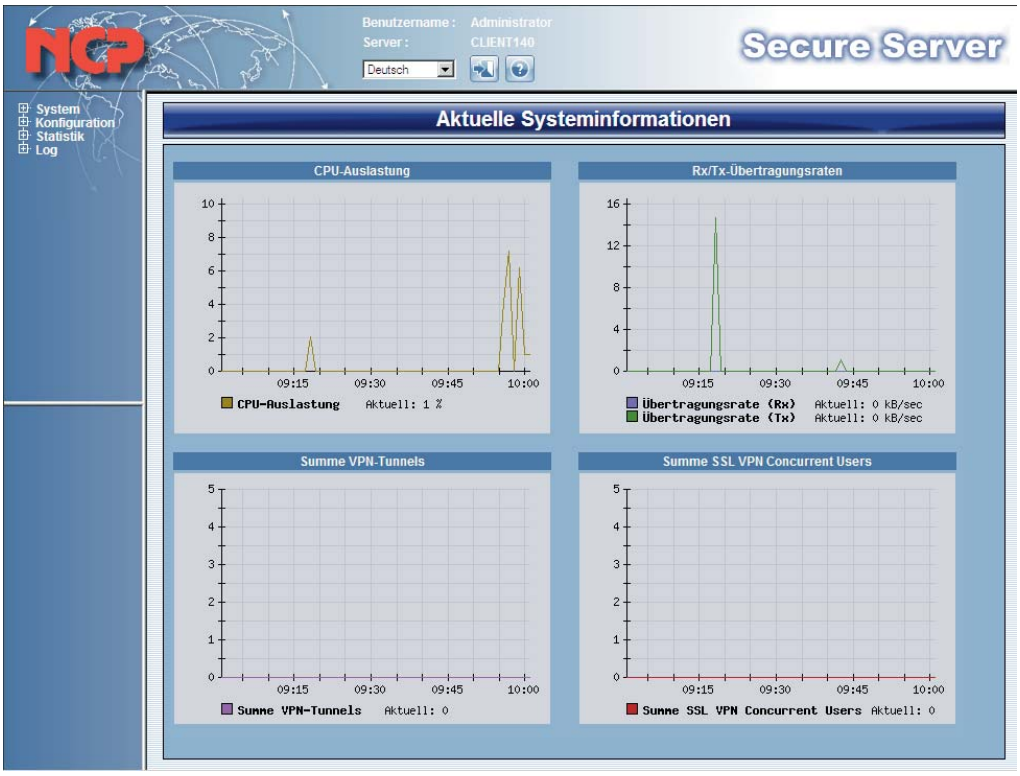


Bei einem folgenden Login kann das Passwort gespeichert werden.

Der erste Systemadministrator verfügt über alle Rechte. Auch kann er neue Administratoren (im folgenden “Manager” genannt) anlegen. Beachten Sie dazu den Abschnitt **Zugriffsverwaltung / Allgemein**.

Nach dem ersten Login

Nach dem ersten Login öffnet sich die Konfigurationsoberfläche des Web-Interface mit den aktuellen Systeminformationen (Abb. links unten).



Die Beschreibung der Schaltknöpfe in der Web-Oberfläche und weitere Bedienungshinweise finden Sie im Abschnitt **Web-Oberfläche** (per Mausklick auf den Begriff).

Auf den folgenden Seiten sind die Konfigurationsparameter beschrieben.

Parameter-Übersicht

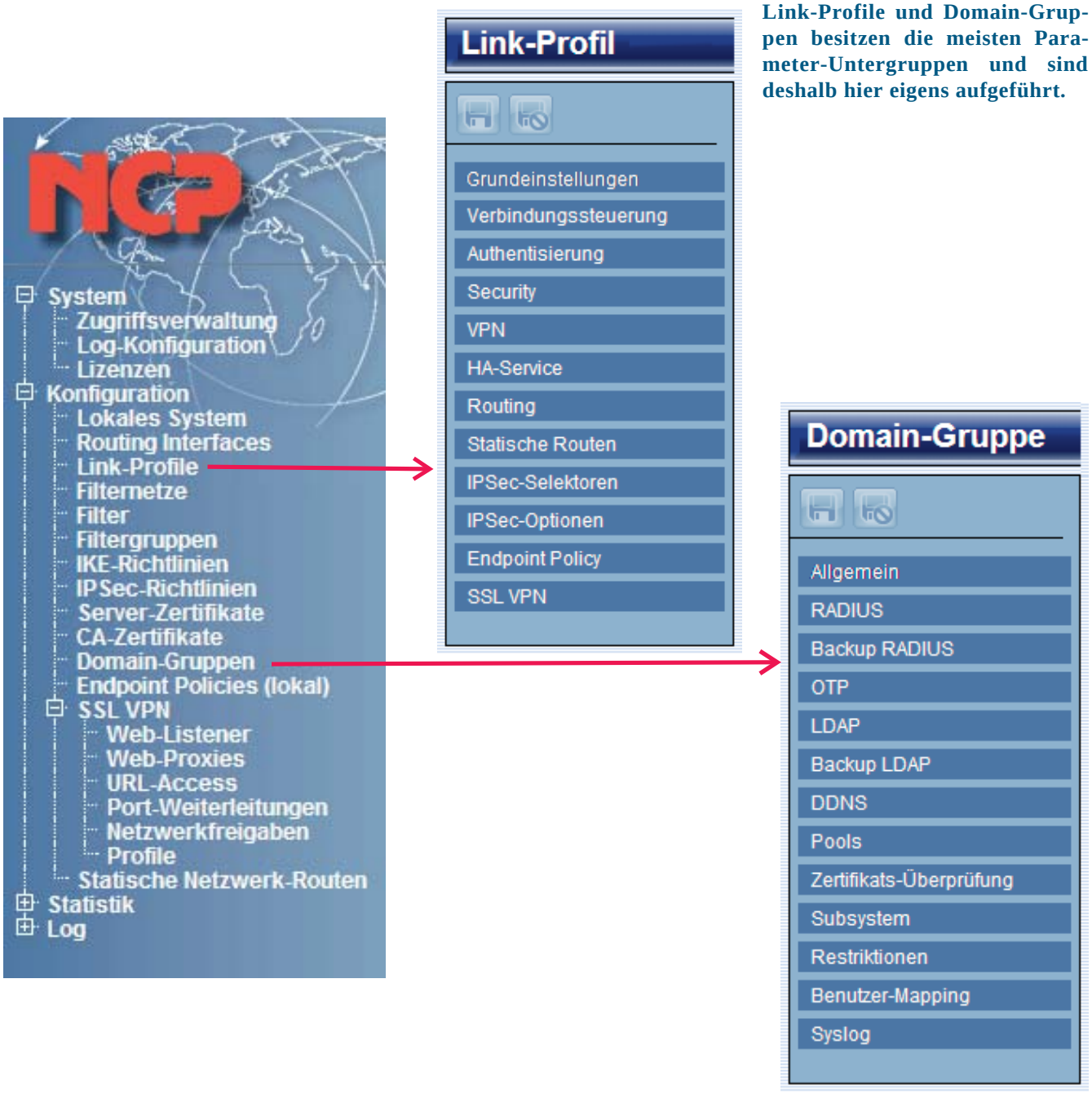
In diesem Abschnitt sind alle Parameterbeschreibungen in der Reihenfolge aufgeführt in der sie im Konfigurationsbaum der Web-Oberfläche angeordnet sind.

Ebenso wie Sie in der Web-Oberfläche mit Mausklick auf einen der Begriffe ein Konfigurationsfeld bzw. einen Konfigurationszweig öffnen, gelangen Sie auch in dieser Dokumentation per Mausklick auf den Begriff in den Abbildungen unten auf die Seite mit der entsprechenden Beschreibung.

Suchen Sie ein bestimmtes Konfigurationsfeld, gelangen Sie mit Klick auf das Web-Icon (links) immer auf diese Übersichtsseite zurück. Suchen Sie einzelne Parameter, so benutzen Sie bitte den alphabetischen **Index** am Ende dieses PDFs!

Querverweise sind mit fetter roter Schrift markiert und können mit Mausklick darauf angesprungen werden. Verweise auf andere Dokumente sind ebenso mit fettroter Schrift gedruckt und mit dem PDF-Icon (links) versehen.

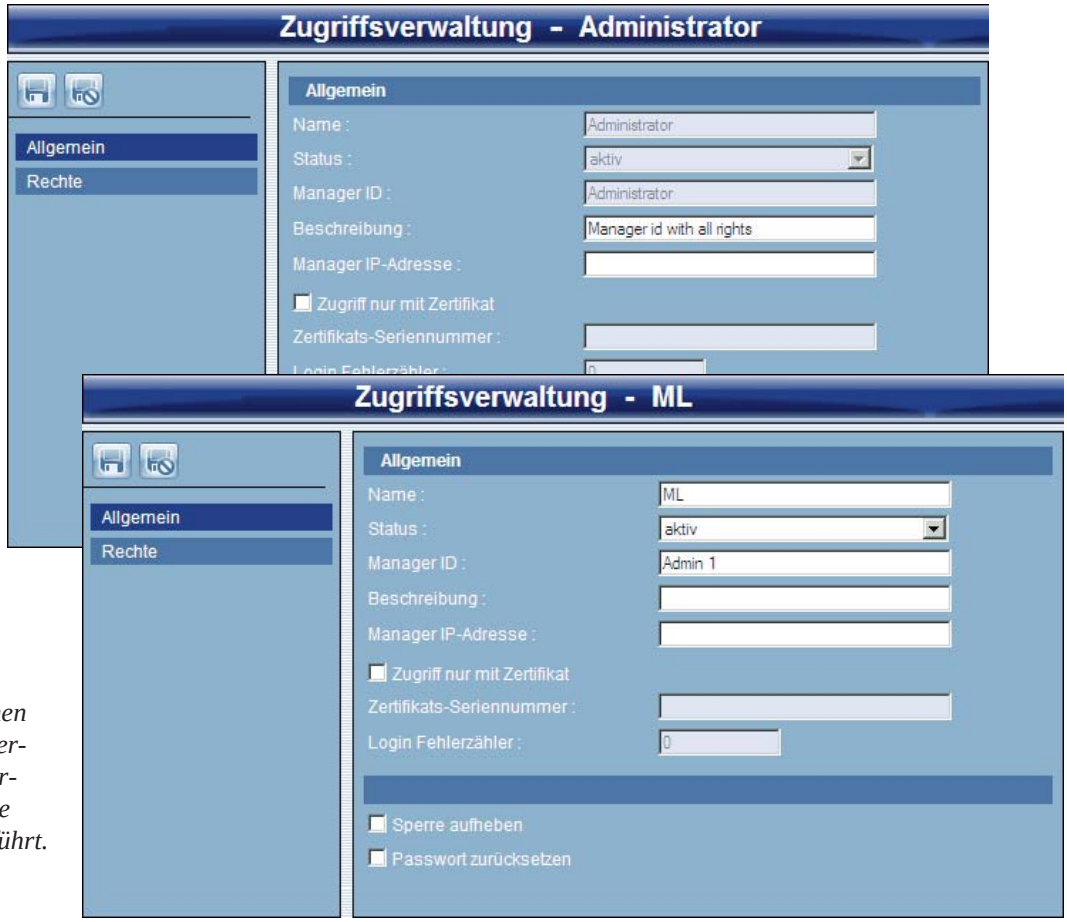
Link-Profile und Domain-Gruppen besitzen die meisten Parameter-Untergruppen und sind deshalb hier eigens aufgeführt.



System

Im Management-System wird die Verwaltungsstruktur für Administratoren (Manager) und die Rechtestruktur für die Systemzugriffe festgelegt.

Nach dem ersten Login wird automatisch der “System”-Administrator erzeugt, der alle Rechte besitzt (Manager ID with all rights) Abb. rechts oben.



Zugriffsverwaltung / Allgemein

Mit der Zugriffsverwaltung können bis zu 25 weitere Manager mit verschiedenen Rechten angelegt werden. Die Überprüfung der Rechte wird am Secure Server durchgeführt.

Anlegen eines neuen Administrators (Managers)

Zunächst kann nur der System-Administrator neue Manager-Profile festlegen. Pro Klick auf den Plus-Button wird ein neues Konfigurationsfeld für einen neuen Administrator (Manager) geöffnet (Admin 1, Admin 2, etc.)

Sollen mehrere System-Manager mit unterschiedlichen Administratorrechten Zugriff auf das System erhalten, so erfolgt dies über den Konfigurationsbaum “System / Zugriffsverwaltung / Allgemein”, wobei die Rechte pro Manager unter “System / Zugriffsverwaltung / **Rechte**” zugewiesen werden.

Ändern Sie in der Zugriffsverwaltung unbedingt die Standardeinstellung des Benutzernamens (Admin 1, etc.) und vergeben Sie für jeden Administrator ein eigenes Passwort, um unerlaubte Zugriffe ausschließen zu können.

Name

Der Name bezeichnet den Manager. Er wird in der Liste der vom Administrator angelegten Manager geführt. Der Administrator kann einen Manager in dieser Liste selektieren (Bild rechts unten ML) und z. B. seine Rechte definieren.

Status

Der Status kann vom Systemadministrator von “aktiv” auf “inaktiv” oder umgekehrt geschaltet werden. Bei inaktivem Status ist ein Zugriff auf die Server-Konfiguration nicht möglich.

Manager ID

Ist der Benutzername des jeweiligen Managers in der Anmeldemaske und kann dort selektiert werden (siehe oben **Zugriff**).

Beschreibung

Die Beschreibung dient als Feld für freie Benutzereingaben.

Manager IP-Adresse

Dies ist die IP-Adresse desjenigen Rechners im Firmennetz, über den via Browser der Server verwaltet wird.

Durch Angabe von Adressbereichen (125.0.0.1 - 125.255.255.255) können die Rechner eines Netzbereichs gefiltert werden.

Zugriff nur mit Zertifikat

Soll der Zugriff des selektierten Administrators (Abb. oben “ML”) nur mit dem Zertifikat des Browser-Zertifikats-Stores erlaubt sein, so muss die Datei **ncpweb.conf** editiert werden und diese Option aktiviert sein.

In der Datei ncpweb.conf muss der Parameter “require certificate” auf “1" gesetzt werden. Der Zugriff ist dann nur mit Zertifikat (am Browser) gestattet. Neben dem Server-Zertifikat ist auch das signierte Benutzer-Zertifikat für diesen Administrator nach X.509.3 nötig. Dies ermöglicht die Authentisierung des Administratores gegenüber dem Server.

Wird diese Funktion aktiviert, so muss sich der Administrator mit seinem Benutzer-Zertifikat ausweisen. Das zum Benutzer-Zertifikat des Administrators gehörige Aussteller-Zertifikat muss am Secure Server unter:
`<programme>\ncp\CA-Certs`
hinterlegt sein und muss für den Verwendungszweck “Authentisierung von Web-Konfiguration” zugelassen sein (siehe: CA-Zertifikate / Verwendungszweck).

Zertifikats-Seriennummer

Zusätzlich kann die Sereinummer des Benutzer-Zertifikats ausgewertet werden, wenn sie hier eingetragen wird.

Login-Fehlerzähler

Erfolgt bei einem neu angelegten Manager zum 5. Mal ein Login-Fehler, so wird der Zugriff für diesen Manager gesperrt.

Sperre aufheben

Die Zugriffssperre ist erst dann aufgehoben wenn der Haken vom Administrator gesetzt wurde und der Status auf aktiv steht und diese Einstellung gespeichert wurde.

Passwort zurücksetzen

Das Passwort ist erst dann zurückgestzt wenn der Haken vom Administrator gesetzt wurde und diese Einstellung gespeichert wurde. Der Manager muss beim nächsten Login ein neues Passwort eingeben und bestätigen.

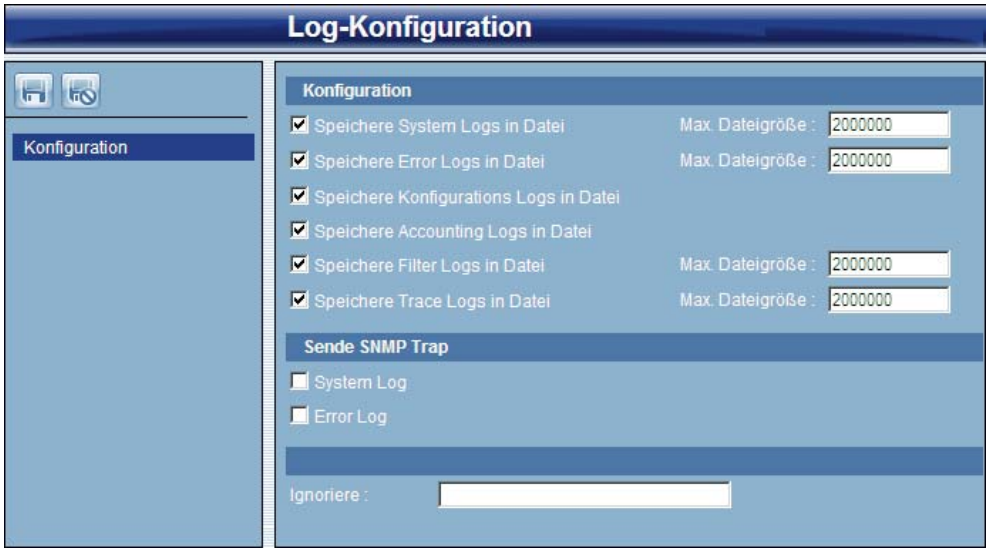
Zugriffsverwaltung / Rechte

Für jeden Manager kann der Administrator gesondert Rechte vergeben. In der Standard-Einstellung werden alle Konfigurationen angezeigt. Konfigurationsberechtigungen sind noch nicht verliehen (Abb. unten).

Log-Konfiguration

Log-Meldungen können für Statisken ausgewertet oder zur Fehlersuche verwendet werden.

In der Log-Konfiguration kann angeben werden, welche Log-Meldungen in einer Datei gespeichert werden sollen. In der Standard-Einstellung werden alle als Datei gespeichert, wobei mit Ausnahme der Konfigurations- und Accounting-Logs die jeweilige max. Dateigröße in Byte angegeben werden kann (Standard 2 MB).



Erreicht eine Log-Datei die max. Dateigröße, wird sie als *.old gesichert und eine neue Log-Datei wird geöffnet.

Konfigurations- und Account-Logs werden monatlich als account- bzw. configYYMM.log gesichert.

Alle Log-Dateien werden im TSV-Format (Tabulator Seperated Value) geschrieben und im Installationsverzeichnis (Programs, bzw. Program Files) unter NCP\SecureServer\Logfiles gespeichert. Sie können von jeder Datenbank- oder Spreadsheet-Anwendung gelesen und statistisch ausgewertet werden.

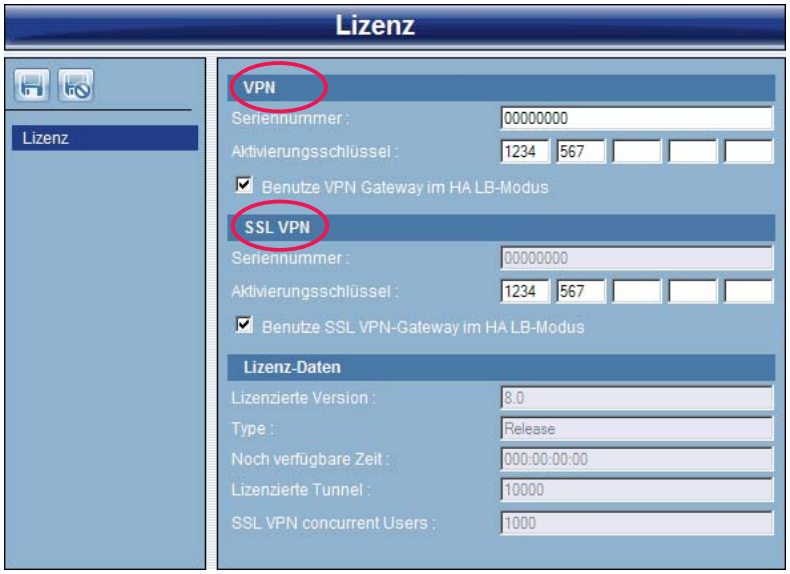
Unabhängig von der Log-Datei können die letzten Reports im Konfigurationsbaum des Secure Servers unter “Log” betrachtet werden.

Abb. oben: Fenster des aktuellen Konfigurations-Log mit Konfigurationsverlauf.

Lizenzen

Für den Secure Server stehen verschiedene Lizenzmodalitäten zur Verfügung:

– VPN-Lizenz und SSL VPN-Lizenz
– VPN-Lizenzierung des Secure Servers
– Benutze VPN Gateway im HA LB Modus
– Lizenzierung der SSL VPN-Funktionalität



VPN-Lizenz und SSL VPN-Lizenz

Im Lizenz-Fenster kann abgelesen werden, ob diese Version eine Vollversion oder eine Testversion ist, wie lange letztere noch gültig ist und wieviele Tunnels zur Verfügung stehen bzw. wieviele gleichzeitige SSL VPN-Nutzer (Concurrent Users) sich mit dem Server verbinden können.

VPN-Lizenzierung des Secure Servers

Die Testversion eines Secure Servers wird mit 5 IPSec-Tunnels ausgeliefert. Zur Lizenzierung der Server Software geben Sie im Linzenz-Fenster die Seriennummer und den Aktivierungsschlüssel ein. Nehmen Sie eine Tunnelerweiterung vor, muss der Aktivierungsschlüssel entsprechend abgeändert werden.

Bitte beachten Sie, dass nach der Lizenzierung die Dienste erneut gestartet werden müssen!

Drücken Sie dazu den Restart-Button unter “Statistik / Systeminformationen”!

Benutze VPN Gateway im HA LB Modus

Wird diese Option genutzt, so wird das VPN Gateway beim nächsten Start mit der Maximalen Tunnelanzahl (1000) hochgefahren. Ein Tunnelaufbau ist erst nach einer Verbindung mit dem HA Server möglich. Die Tunnellizenzen werden in diesem Fall vom HA Server verwaltet. Ist die maximale Anzahl der Tunnellizenzen erreicht, so sperrt der HA Server alle vorhandenen Gateways für weitere Tunnelverbindungen.

Lizenzierung der SSL VPN-Funktionalität

Die Testversion eines Secure Servers wird mit 5 SSL VPN-Tunnels ausgeliefert. Ein SSL VPN-Tunnel entspricht einem SSL VPN-Nutzer (Concurrent User). In der Testversion läuft die SSL VPN-Funktionalität mit den Modulen Endpoint Security, Port Forwarding und Portable LAN. Zur Lizenzierung der SSL VPN-Funktionalität wird der Aktivierungsschlüssel eingegeben. Die Seriennummer muss der Seriennummer des VPN Gateways entsprechen, das mit einem neuen Aktivierungsschlüssel um die SSL VPN-Funktionalität erweitert wird.

Wird die SSL VPN-Funktionalität mit den Modulen Endpoint Security, Port Forwarding und Portable LAN lizenziert, so werden die Test-Konfigurationen dazu übernommen.

Wird die SSL VPN-Funktionalität nicht lizenziert, sondern ausschließlich das VPN Gateway, so verlieren die SSL VPN-Tunnels und die zugehörige Konfiguration bzw. die beiden Concurrent Users der Testversion ihre Funktionalität. D. h. nach der Lizenzierung des VPN Gateways entfällt die SSL VPN-Funktionalität.

Konfiguration

Die Parameter, nach denen das Server-System spezifiziert wird, sind in folgenden Zweigen des Konfigurationsbaums dargestellt:

Jeder Konfigurationszweig ist in verschiedene Parameterfelder unterteilt.

Auf den folgenden Seiten werden pro Konfigurationszweig alle Parameterfelder aufgelistet.

Per Mausklick können Konfigurationszweige und Parameterfelder direkt angesprungen werden.

Lokales System

Allgemein

In diesem Feld werden Authentisierungsparameter eingegeben, das Verbindungsmedium ins WAN und das Tunnel-Protokoll bestimmt.

Benutzer (System)

Diese ID gilt für alle von dieser Maschine abgehenden Rufe, wenn im Parameterfeld “Link-Profile” keine andere Link-spezifische ID eingetragen wurde (siehe: Link-Profile). Baut diese Maschine eine Verbindung auf, meldet sie sich mit dieser Benutzer-ID bei der Gegenstelle an. Diese PPP-ID wird entsprechend der RFC-Spezifikationen für das CHAP-Protokoll verwendet und muss von der Gegenstelle erkannt werden.

Sie wird nur bei gegenseitiger (bidirectional) Authentisierung benötigt oder wenn dieser Maschine gestattet ist, sich an die Remote-Seite anzuwählen (z. B. bei einem Rückruf).

Wird auf der Remote-Seite die Client Software eingesetzt, so muss diese ID übereinstimmen mit **Benutzer der Gegenstelle** im Parameterfeld “Eingehende Rufe”.

Die ID kann bis zu 253 Zeichen lang sein.

Passwort (System)

Dieses Passwort gilt für alle von dieser Maschine abgehenden Rufe, wenn im Parameterfeld “Link-Profile” kein anderes Link-spezifisches Passwort eingetragen wurde (siehe: Link-Profile). Baut diese Maschine eine Verbindung auf, weist sie sich mit diesem Passwort bei der Gegenstelle aus. Dieses PPP-Passwort wird entsprechend der RFC-Spezifikationen für das CHAP-Protokoll verwendet und muss von der Gegenstelle erkannt werden.

Es wird nur bei gegenseitiger (bidirectional) Authentisierung benötigt oder wenn dieser Maschine gestattet ist, sich an die Remote-Seite anzuwählen (z. B. bei einem Rückruf).

Wird auf der Remote-Seite die Client Software eingesetzt, so muss dieses Passwort übereinstimmen mit “Passwort der Gegenstelle” im Parameterfeld “Eingehende Rufe”.

Das Passwort kann bis zu 253 Zeichen lang sein.

Rufablehnung

Die Rufablehnung wird nur aktiviert vor Wartungsarbeiten, bzw. wenn das System kurzzeitig abgeschaltet werden soll. Ist die Rufablehnung aktiviert, wird verhindert, dass sich außer den Benutzern, die sich bereits angewählt haben, noch weitere anwählen können. Wenn keine Verbindungen mehr aktiv sind, kann das System abgeschaltet werden.

Benutze DNS / WINS Proxy

Wird das Gateway als Client Gateway zwischen lokalem Filialnetz und entferntem Secure Server genutzt, so kann es für die Workstations im LAN mit dieser Funktion als DNS / WINS Proxy Server fungieren.

Die DNS-Anfrage des LAN Clients leitet das Filial Gateway dann weiter an den DNS Server im entfernten Netz.

Verfügbare Verbindungsmedien

Hier klicken Sie die Verbindungsmedien an, über die abgehende WAN-Verbindungen hergestellt werden sollen. Entsprechend des gewählten Verbindungsmediums muss auch der zugehörige Adapter installiert und sein Treiber geladen worden sein. Nach Ihrer Auswahl werden die Schnittstellenmodule für die Maschine geladen.

Für jedes gewählte Verbindungsmedium wird ein virtueller Controller vom System erzeugt (siehe: Controller).

Folgende Verbindungsmedien stehen zur Verfügung:

	Schnittstelle	**WAN**
ISDN:	ISDN-Adapter	ISDN
Digitale Modems:	Asynchrones digitales Modem	PSTN
GSM:	ISDN Adapter mit V.110	GSM
PPPoE:	Ethernet-Adapter mit xDSL-Modem und Splitter	xDSL

Wichtig: Nach jeder Änderung des Verbindungsmediums müssen die Dienste neu gestartet werden!

Drücken Sie dazu den Restart-Button unter “Statistik / Systeminformationen”!

VPN-Protokolle

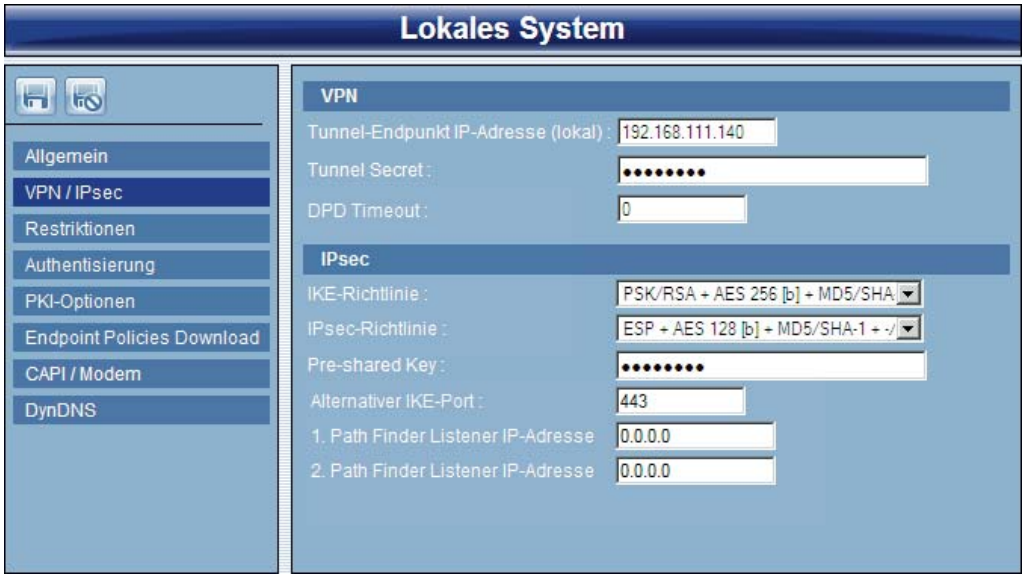
An dieser Stelle bestimmen Sie, welche Tunneling-Protokolle genutzt werden können. Aktivieren Sie ein VPN-Protokoll, so können so viele Tunnels aufgebaut werden, bis die volle Anzahl der lizenzierten Tunnels erreicht ist. Ohne VPN-Protokoll wird zwischen dem VPN Gateway und dem Zielsystem kein Tunnel aufgebaut.

Zur Wahl stehen L2TP (Layer 2 Tunneling Protokoll) und IPSec. Die IKE / IPSec-Richtlinien und der statische Schlüssel werden unter **IKE-Richtlinien** und **IPSec-Richtlinien** eingestellt.

Soll ein abgehender IPSec-Link mit XAUTH und ConfigMode hergestellt werden, so muss zusätzlich im Link-Profil die Verbindungart “IPSec” eingestellt werden.

VPN / IPsec

In diesem Feld werden die Tunnel-Parameter für IPsec oder L2TP am lokalen System global für alle eingehenden Verbindungen eingestellt. Die Tunnel-Parameter des Clients müssen diesen Werten entsprechen, um eine Verbindung vom Client zu diesem VPN Gateway aufbauen zu können.



VPN

Tunnel-Endpunkt IP-Adresse (lokal)

Dies ist die offizielle IP-Adresse (im Internet) des Tunnel-Endpunkts am VPN Gateway (siehe auch: Link-Profile, VPN, Tunnel-Endpunkt IP-Adresse (Ziel)). Über diese offizielle IP-Adresse erreicht der Client das VPN Gateway.

Tunnel Secret

“Tunnel Secret” ist ein Passwort, das für den Tunnelaufbau benötigt wird. Nur wenn dieses Passwort beim VPN Gateway und an der Gegenseite (Client Software) übereinstimmt, wird der Tunnel aufgebaut. Das Passwort kann bis zu 16 Zeichen lang sein. (siehe: **Link-Profile / VPN**)

L2TP DPD Timeout

Der eingetragene Wert gibt die Zeit in Sekunden an, wann die L2TP-Tunnelüberwachung einsetzt. Ist der Wert auf “0" gesetzt erfolgt keine Tunnelüberwachung.

Das Gateway prüft bei einer Layer-2-Tunnelverbindung mit Polling, ob die Gegenstelle noch aktiv ist. Bleibt eine Antwort aus, so wird die Verbindung getrennt. Das Polling wird dann aktiv, wenn keine Daten mehr vom Client empfangen werden und wird in den angegebenen Zeitintervallen ausgeführt. Dieses Verfahren hat keinen Einfluss auf die Einstellungen des Timeouts.

IPsec [Lokales System]

IKE-Richtlinie

Sie wählen aus der Listbox der vorkonfigurierten IKE-Richtlinien diejenige aus, nach der der Kontrollkanal aufgebaut werden soll.

In der Listbox werden alle IKE-Richtlinien aufgeführt, die Sie im Konfigurationsbaum unter der Verzweigung “IKE-Richtlinie” und “IPsec-Richtlinie” angelegt haben. Die IKE-Richtlinien erscheinen in der Box mit dem Namen, den sie bei der Konfiguration vergeben haben.

Funktional unterscheiden sich zwei IKE-Richtlinien, die standardmäßig vorkonfiguriert mit der Software ausgeliefert werden. Sie finden sie unter dem Konfigurationsknoten “IKE-Richtlinie / PRE Shared Key” und “RSA-Signatur”.

IPsec-Richtlinie

Sie wählen aus der Listbox der vorkonfigurierten IPsec-Richtlinien diejenige aus, nach der in der Phase 2 die Datenverschlüsselung erfolgen soll.

In der Listbox werden die IPsec-Richtlinien aufgeführt. Sie erscheinen in der Box mit dem Namen, den sie bei der Konfiguration vergeben haben.

Da der IPsec-Modus mit AH-Sicherung für flexiblen Remote Access ungeeignet ist, wird nur eine IPsec-Richtlinie mit ESP-Protokoll standardmäßig vorkonfiguriert mit der Software ausgeliefert. Sie finden sie unter dem Konfigurationsknoten “IPsec-Richtlinie” als “ESP AES-3DES-MD5".

Pre-shared Key

Ein Pre-shared Key kann zur Authentisierung in der IKE-Verhandlung verwendet werden (siehe: IKE-Richtlinien). An beiden Endpunkten der Kommunikation muss der gleiche Pre-shared Schlüssel verwendet werden. (Der Pre-shared Key für eine dynamische SPD wird unter “Link-Profile / Security” eingegeben.)

Alternativer IKE-Port [Lokales System]

Sind z. B. an der zentralen Firewall die Standard-Ports für die IPsec-Kommunikation bereits für andere IPsec-Lösungen freigeschaltet (IPsec mit UDP: Port 4500, für IPsec ohne UDP: Port 500), so kann für die NCP IPsec-Lösung mit dieser Option ein beliebig anderer Port für die IPsec-Kommunikation definiert werden, wenn UDP (User Datagram Protocol) Encapsulation genutzt wird.

Dieser Port wird dann für die Phase-1- und Phase-2-Verhandlung der IPsec-Kommunikation verwendet, wenn in der Konfiguration der Link-Profile unter “IPsec-Optionen” die Funktion **Benutze UDP-Encapsulation** aktiviert wurde und der gleiche Port auch in der Client-Konfiguration in den Profil-Einstellungen unter **Erweiterte IPsec-Optionen** eingetragen wurde.

NCP Path Finder

Mit dem Protokoll NCP Path Finder wird TCP Encapsulation als Fallback über den HTTPS Port 443 unterstützt, falls IPsec nicht möglich ist.

Diese Funktion ist dann aktiviert, wenn als alternativer Port der Port 443 eingestellt wird. Der Secure Server kann dann Datenpakete sowohl über den IPsec Port als auch über den Port 443 empfangen.

Dies ist dann von Bedeutung, wenn für den Client nur der HTTPS Port 443 zur Verfügung steht und eine reine IPsec-Verbindung nicht möglich ist.

Am Client ist der NCP Path Finder aktiv, wenn in den Profil-Einstellungen unter “Erweiterte IPsec-Optionen” der entsprechende **IPsec-Modus** eingestellt wurde.

Path Finder Listener IP-Adresse

IPsec-Verbindungen mit Path Finder-Protokoll nutzen zum VPN Gateway den Port 443 (siehe oben “Alternativer IKE-Port [Lokales System]”).

Auch SSL VPN-Verbindungen nutzen den Port 443 (siehe “SSL VPN / Listener”).

Sollen beide Verbindungsarten zu einem VPN Gateway möglich sein, so muss dem Client für die IPsec-Verbindung über Path Finder zusätzlich zum alternativen IKE-Port 443 eine eigene IP-Adresse mitgegeben werden.

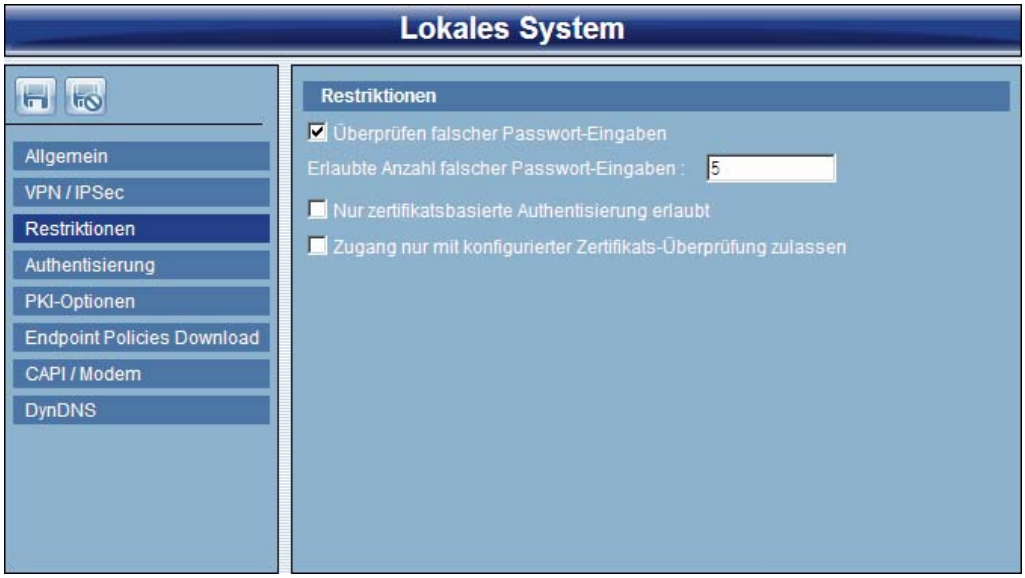
Diese IP-Adresse ist am Client als “Gateway (Tunnel-Endpunkt)” unter “Tunnel-Parameter” einzutragen.

Am Gateway wird sie als “Path Finder Listener (IP-Adresse)” eingetragen.

Restriktionen [Lokales System]

Mit Restriktionen wird unerlaubter Zugriff auf das System noch weiter erschwert. Wiederholtes Ausprobieren von Passwörtern kann hier unterbunden werden.

Die Restriktionen können nur für lokal konfigurierte Link-Profile (aus dem Konfigurationsbaum) zur Anwendung kommen, nicht für Link-Profile, die über LDAP oder RADIUS verwaltet werden.



Überprüfen falscher Passwort-Eingaben

Wenn diese Checkbox angeklickt ist, werden falsche Passwort-Eingaben überprüft, bis die erlaubte Anzahl (siehe: unten) erreicht ist. Das heißt in der Link-Statistk des Systems wird für dieses Link-Profil ein Zähler gesetzt, der auch die erlaubten falschen Passwort-Eingaben mitzählt.

Erlaubte Anzahl falscher Passwort-Eingaben

Geben Sie an dieser Stelle die erlaubte Anzahl der falschen Passwort-Eingaben ein. Wird die erlaubte Anzahl überschritten, so wird der Benutzer gesperrt. Auch wenn nach der erlaubten Anzahl der falschen Eingaben eine richtige erfolgt, gelangt der Benutzer nicht mehr auf dieses System.

Das Link-Profil eines gesperrten Benutzers wird automatisch inaktiviert (siehe: Link-Profil / Grundeinstellungen). Eine WAN-Verbindung über dieses Link-Profil ist damit nicht mehr möglich! Der Status ist in der Link-Statistik des Systems für dieses Link-Profil ablesbar.

Der Status des Link-Profils muss nach der Sperre erst wieder auf aktiv gestellt werden, wenn sich ein Benutzer über das WAN an das System anmelden will!

Zugang nur mit konfigurierter Zertifikats-Überprüfung zulassen

Wenn Zertifikate für die Kommunikation eingesetzt werden, aktivieren Sie unbedingt diese Funktion!

Bitte beachten Sie, dass im Link-Profil ein Inhalt für die Zertifikats-Überprüfung (Common Name, E-Mail oder Seriennummer) angegeben sein muss!

Ist diese Funktion aktiv und im Link-Profil kein Inhalt für die Zertifikats-Überprüfung angegeben, wird die Verbindungswunsch abgewiesen und eine Trap-Meldung gesendet. Ist das Link-Profil in einem RADIUS oder LDAP Server abgelegt, müssen auch hier die entsprechenden Parameter oder Attribute angegeben sein.

(Siehe auch:
Link-Profile / Zertifikats-Überprüfung)

Nur zertifikatsbasierte Authentisierung erlaubt

Der Einsatz von Zertifikaten kann für alle eingehenden Verbindungen erzwungen werden. Dazu wird die Funktion “nur zertifikatsbasierte Authentisierung erlaubt” aktiviert.

Eine Zertifikats-Überprüfung muss in diesem Fall nicht zwingend stattfinden. Damit kann jedoch ausgeschlossen werden, dass sich Benutzer ohne gültiges Zertifikat am Gateway anmelden.

Authentisierung

Authentisierungsprotokoll

Die Einstellungen in diesem Feld definieren wie die NCP Security Features für diese Verbindung genutzt werden.

Die Server Software unterstützt sowohl Authentisierungsverfahren nach CHAP (Challenge Handshake Authentication Protocol) als auch nach PAP (Password Authentication Protocol). Die Security-Verhandlungen erfolgen jeweils automatisch und hängen davon ab, welche Methode hier eingestellt wird.

Dabei ist CHAP, die am häufigsten eingesetzte Methode, sicherer als PAP, da das Passwort verschlüsselt übertragen wird. PAP überträgt das Passwort in Klartext.

RADIUS-Konfiguration für ausgehende Verbindungen

Damit ist es möglich das zugehörige Link-Profil zu einer Ziel-IP-Adresse eines Clients vom RADIUS Server abzufragen. Diese Funktionalität ist nur mit dem Secure Enterprise Management-System gegeben.

LDAP-Konfiguration für ausgehende Verbindungen

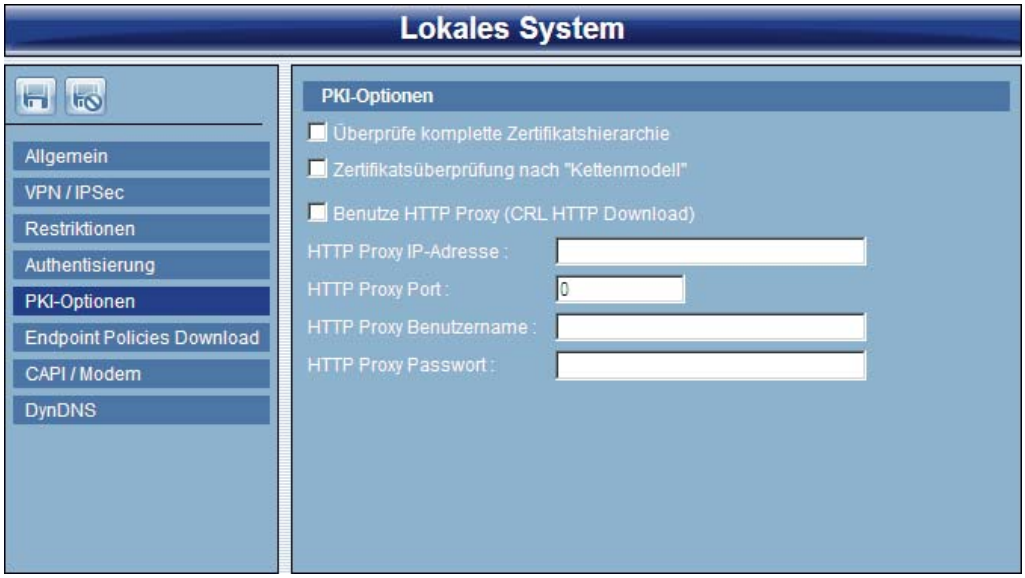
Diese Funktion hat nur Bedeutung, wenn ein Link-Profil für eine ausgehende Verbindung auf einem LDAP-Server abgelegt ist. (Normalerweise sind Link-Profile für ausgehende Verbindungen lokal gespeichert.)

Wird diese Funktion aktiviert, so kann die Konfiguration des Link-Profils aus LDAP abgefragt werden. Suchkriterium ist die IP-Adresse.

Dabei ist zu beachten, dass der LDAP-Server so konfiguriert sein muss, dass über das Attribut, welchem der Wert “IP-Adresse” zugeordnet ist, die IP-Adresse gefunden werden kann.

PKI-Optionen

Unter den PKI-Optionen kann festgelegt werden, welche Bedingungen die Gültigkeitszeiträume der Zertifikate entlang des Zertifizierungspfades erfüllen sollen und bis zu welcher Höhe der Zertifizierungspfad geprüft werden soll.



Überprüfe komplette Zertifikatshierarchie

Bei Aktivierung dieser Funktion wird die Vollständigkeit der eingespielten CA-Zertifikate bis zum Root-Zertifikat überprüft. Bei Unstimmigkeit eines Zertifikats-Inhalts oder Fehlen eines der Zertifikate in der Hierarchie wird ein Trap erzeugt und die Benutzer werden abgewiesen.

Zertifikatsüberprüfung nach “Kettenmodell”

Wird diese Funktion aktiviert, so werden die Zertifikate nach dem “Kettenmodell” geprüft. Danach kann ein Benutzer sich auch nach Ablauf der Gültigkeit des CA-Zertifikats noch am Secure Server einwählen. Nach dem Kettenmodell ist ein Zertifikat gültig, wenn das ausstellende Zertifikat zum Zeitpunkt der Signaturerstellung gültig war.

Wird diese Funktion nicht aktiviert, so werden die Zertifikate nach dem “Schalenmodell” geprüft. Die Gültigkeitsdauer eines Aussteller-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Ist die Gültigkeitsdauer des CA-Zertifikats abgelaufen, so wird der Benutzer abgewiesen.

Benutze HTTP Proxy (CRL HTTP Download)

Wird ein Proxy-Server im System verwendet, so muss diese Funktion aktiviert werden, damit ein HTTP-Download der Widerrufsliste erfolgen kann. Folgende Eingaben müssen dazu gemacht werden:

HTTP Proxy IP-Adresse:
IP-Adresse des Proxy-Servers im Netz

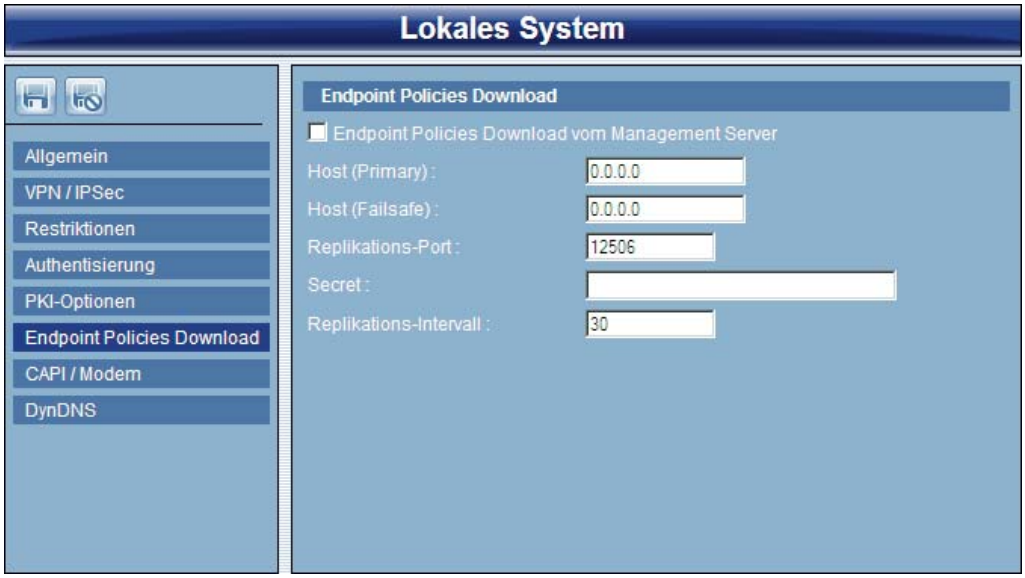
HTTP Proxy Port:
(Der Proxy-Port ist standardmäßig 80)

HTTP Proxy-Benutzername:
Benutzername für den Proxy-Server

HTTP Proxy-Passwort:
Passwort für den Proxy-Server

Endpoint Policies Download

Die Einhaltung von Endpoint Sicherheits-Richtlinien (Endpoint Policy Enforcement) kann alternativ vom Secure Server oder vom Secure Enterprise Management erzwungen werden. Sollen die Richtlinien am Secure Server erstellt werden, so darf der Richtlinien-Download vom Management Server nicht aktiviert sein! Die Richtlinien können dann unter "Konfiguration / Richtlinien" erstellt werden.



Die Sicherheits-Richtlinien beinhalten sicherheitsrelevante Vorgaben vom Secure Enterprise Management. Bei jeder Anwahl eines Clients wird die Endpoint Policy heruntergeladen. Bei Nichterfüllung der Vorgaben können unterschiedliche Meldungen oder Aktionen erfolgen, z. B. kann die Verbindung auf einen Netzbereich eingeschränkt werden, der durch eine Filtergruppe für die Link-Profile definiert wird. Die entsprechende Einstellung kann in der Konfiguration eines Link-Profils in der Rubrik **Endpoint Policies (lokal)** vorgenommen werden. Bei Erfüllung der Sicherheits-Richtlinien wird der komplette Netzbereich für den Client-Zugriff freigeschaltet, der durch die Filtergruppe für eingehende Links definiert wurde.

Endpoint Policies Download von Management Server

Mit dieser Funktion erfolgt die Aktivierung des Downloads der Endpoint Sicherheits-Richtlinien vom Management Server. Mit dem zentralen Enterprise Management können die Sicherheits-Richtlinien allen Endpunkten der eingesetzten Komponenten gleichermaßen zugeteilt werden.

Ist diese Funktion aktiviert und werden Policies vom Management-System heruntergeladen, so können lokal keine Policies angelegt werden (siehe weiter unten **Endpoint Policies (lokal)**!

Host (Primary / Failsafe)

Hier muss die IP-Adresse des Management Servers eingetragen werden.

Replikations-Port

Der hier eingetragene Port muss mit dem Port für den Replikationsdienst am Management Server übereinstimmen. Standard: 12506

Secret

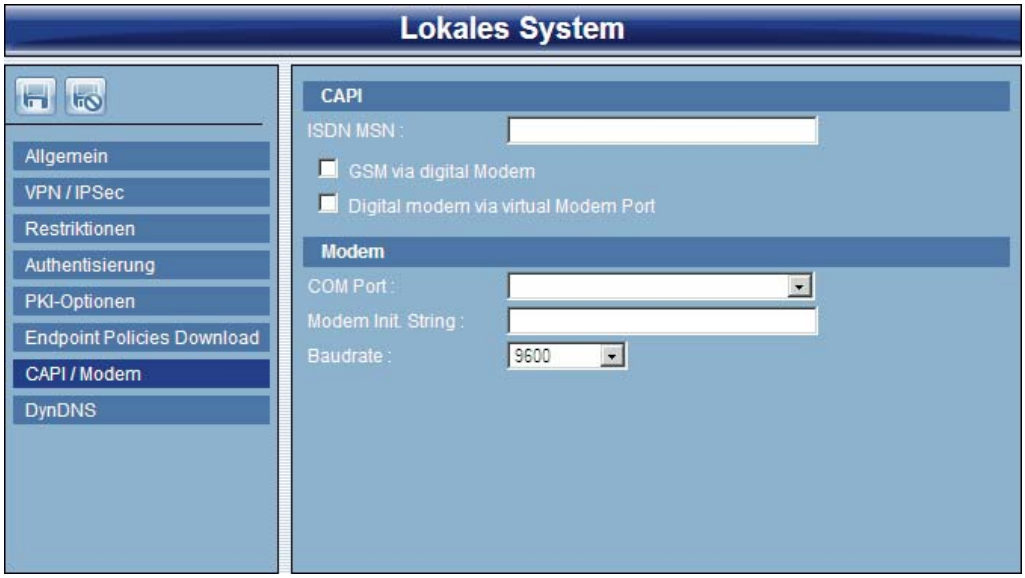
Nur wenn es mit dem am Management Server konfigurierten "Shared Secret" übereinstimmt, wird die Client Policy korrekt übertragen.
(Siehe **SEM-Endpoint-Security**)

Replikations-Intervall

Hier bestimmen Sie den zeitlichen Abstand, in dem das Gateway die Client Policy vom Management Server herunterlädt. Das Intervall wird in Sekunden angegeben. Standard ist 30 sec.

CAPI / Modem

Wenn für ausgehende Verbindungen ein Verbindungsmedium über GSM oder Digitale Modems genutzt werden soll, können alternativ zum Capi 2.0 Kernel Mode virtuelle Modem-Ports der Adapter-Hersteller genutzt werden.



ISDN MSN

Mit der MSN kann ein anderes Gateway für eine Direktverbindung über ISDN mit DSS1 adressiert werden. Die MSN des jeweiligen Gateways wird in der Konfiguration unter “Lokales System / VPN/IPsec” eingegeben. Das andere Gateway muss diese MSN der Rufnummer anhängen.

Capi-Alternativen

Die Windows-Treiber für die virtuellen Modem-Ports werden bei der Installation des Adapters (für GSM oder Digitale Modems) mit installiert.

Folgende Alternativen stehen zur Verfügung:

– GSM über virtuelle Modem-Ports

– Digitale Modems über virtuelle Modem-Ports

Modem

Unter der Konfigurationsgruppe “Modem” können die Parameter für ein analoges Modem eingegeben werden, das an dieses System angeschlossen ist. Entsprechend kann für ein Link-Profil im Parameterfeld “Grundeinstellungen” das Verbindungsmedium “Modem” selektiert werden.

COM Port

An dieser Stelle muss der Com Port für das analoge Modem angegeben werden. Der Port wird bei korrekter Installation automatisch bestimmt. Bei Unstimmigkeiten können die COM Ports 1-4 gezielt angesteuert werden.

Modem Init. String

Sofern Ihr Modem korrekt im Windows-System installiert ist, wird der entsprechende “Modem Init. String” automatisch in dieses Feld übernommen. In Ausnahmefällen kann der String mit (Hayes-) Befehlen erweitert werden.

Baudrate

Die Baudrate beschreibt die Übertragungsgeschwindigkeit zwischen Com Port und Modem. Wenn Ihr Modem z.b. mit 14.4 Kbits übertragen kann, sollten sie die nächsthöhere Baudrate 19200 wählen. Folgende Baudraten können gewählt werden: 1200, 2400, 4800, 9600, 19200, 38400, 57600 und 115200

DynDNS

Zur Funktion "Dynamic DNS"

Das VPN Gateway benötigt keine feste offizielle IP-Adresse, sodass auch die Einrichtung einer Internet-Festverbindung entfallen kann. Das Gateway erhält bei jeder Verbindung mit dem Internet eine neue IP-Adresse vom Internet Service Provider. Da vom ISP bei jeder erneuten Einwahl seitens des Gateways eine andere Adresse vergeben wird, kann die eindeutige Identifikation durch den Secure Client nicht mehr über eine im Telefonbuch des Clients fest zu konfigurierende IP-Adresse erfolgen.

Statt dessen wird dem VPN Gateway vom Administrator ein Name zugeordnet (DNS Name), der am Dyn DNS Server bei der Registrierung mit Benutzername (User ID) und Passwort gespeichert wird. Auf Seiten des Clients wird nun statt der (festen) IP-Adresse für den Tunnel-Endpunkts dieser, beim Dyn DNS Service Provider hinterlegte Name des Gateways eingetragen (DNS Name).

Vor dem Tunnelaufbau vom Client zum Gateway findet nun ein DNS Request statt, über den eine Auflösung des DNS Namens erfolgt. Damit erhält der Client die jeweils aktuelle IP-Adresse des Gateways, und der Tunnelaufbau zum Gateway kann erfolgen.

Beachten Sie bitte, dass eine Verbindung vom Client zum Gateway natürlich nur stattfinden kann, solange das Gateway eine Verbindung zum Internet unterhält (z. B. über DSL Flatrate).

Konfiguration am Server

Die Verbindung vom Gateway zum ISP wird als ausgehender Link konfiguriert. Der Wert für den Parameter "Dyn DNS-Hostname", der im Parameterfeld "Routing" eingegeben wird, ist der Name des Gateways, der auch bei der Registrierung des Gateways beim Dyn DNS Service Provider und am Client im Telefonbuch unter "Tunnel-Parameter" eingegeben wurde (z. B. test.dyndns.org; siehe unten).

In der neuen Hauptgruppe des Konfigurationsbaums "DynDNS" wird der Zugang zum Dynamic DNS Server konfiguriert, indem dessen Server Name "Hostname DynDNS Server" (z. B. members.dyndns.org) und die Zugangsdaten, die bei der Registrierung als Benutzer-Name (User ID) und Passwort verwendet wurden, eingegeben werden. Die Funktion "Benutze DynDNS" wird "aktiv" geschaltet.

Automatische Einrichtung für DynDNS Client

(nächste Seite):

Automatische Einrichtung für DynDNS Client

Nach den eingegebenen Werten, inklusive der vom ISP zugewiesenen IP-Adresse, wird die Batch-Datei NCPDDNS.BAT automatisch wie folgt generiert und gestartet:

Die Batch-Datei enthält alle nötigen Parameter für den NCP-DynDNS Client. Wird ein anderer DynDNS Client verwendet, so kann die Batch-Datei nach Bedarf abgeändert werden.

```
rem the input to this batchfile is as follows
rem ncpddns members.dyndns.org test test 172.16.15.52 test.dyndns.org
rem %1 = members.dyndns.org : This is the Name of the DDNS provider.
rem %2 = test               : This is the UserID to the DDNS provider.
rem %3 = test               : This is the Password to the DDNS provider.
rem %4 = 172.16.15.52       : This is the IPAddress to be assigned.
rem %5 = test.dyndns.org    : This is the Name of the IP address above.

rem The NCP DDNS client is called by default
rem 1. -h DynDNSServer
rem 2. -u UserID
rem 3. -w Password
rem 4. -i IPAddress
rem 5. -n DNSName
rem -p Port              Default HTTP:80, HTTPS:443
rem -x Proxy Ip Address  Default none
rem -y Proxy Port        Default 80
rem -s Use HTTPS

e:\win2000s\ncprtr\ncpdnscl -h %1 -u %2 -w %3 -i %4 -n %5 -s
```

Benutze DynDNS

inaktiv: Das Gateway nutzt die Funktion eines DynDNS Servers nicht.

aktiv: Das Gateway nutzt die Funktion eines DynDNS Servers und benötigt dafür weitere Eingaben.

DynDNS Hostname

Für den Zugang zum Dynamic DNS Server wird der Hostname DynDNS Server benötigt (z.B. members.dyndns.org).

Benutzer [DynDNS]

Bei der Registrierung am DynDNS Server wurde der hier einzugebende Benutzer-Name festgelegt.

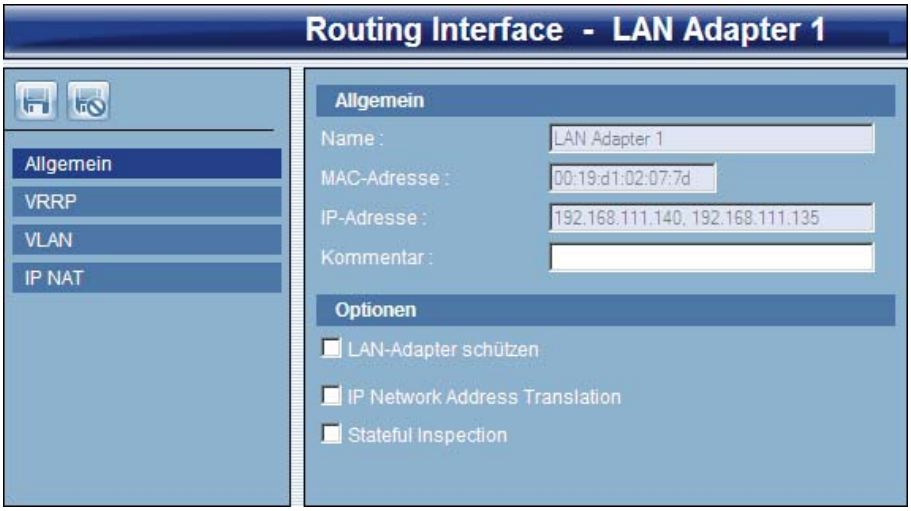
Passwort [DynDNS]

Bei der Registrierung am DynDNS Server wurde das hier einzugebende Passwort festgelegt.

Routing Interfaces

Allgemein

Mit der Konfiguration einer Routing-Schnittstelle wird das Wide Area Network (WAN) als IP-Netz eingerichtet. Sie können hier die im System integrierten Netzwerk-Adapter als Routing-Schnittstellen einrichten, denen verschiedene Links zugeordnet werden können.



Bitte beachten Sie, dass die Dienste neu gestartet werden müssen, nachdem eine Routing-Schnittstelle konfiguriert oder modifiziert wurde!

Drücken Sie dazu den Restart-Button unter “Statistik / Systeminformationen”!

Anzeige des Secure Server Adapters

Die virtuelle IP-Adresse des Secure Servers, der als LAN-Adapter installiert wird, wird bei seiner benutzerdefinierten Installation festgelegt. Dort vergeben Sie eine gültige IP-Adresse aus Ihrem Netzbereich.

In der Standardinstallation wird die Adresse 172.16.119.8 vorgegeben.

Die virtuelle IP-Adresse des Secure Servers wird hier angezeigt. Sie kann nur in in den Netzwerkeinstellungen des Betriebssystems geändert werden!

Name [Routing Interfaces]

Der Name der Routing-Schnittstelle wird hier nur angezeigt. Er wird automatisch generiert (LAN Adapter 1, LAN Adapter 2, etc.) und kann über das Web-Interface nicht geändert werden.

Mit dem Secure Enterprise Management (SEM) kann in der Vorlage für den Secure Server ein Name eingegeben werden. Dieser Name wird mit der Server-Konfiguration vom SEM an den Server übertragen, wenn in den lokalen Server-Einstellungen festgelegt wurde, dass die Konfiguration vom SEM übernommen wird (siehe oben **Server-Konfiguration**). Dieser Name bleibt auch dann erhalten, wenn zu einem späteren Zeitpunkt die Konfiguration nicht mehr vom SEM übernommen wird.

MAC-Adresse [Routing Interfaces]

Hier wird die lokale MAC-Adresse dieses LAN-Adapters, die er in den Netzwerkeinstellungen des Systems besitzt, angezeigt.

Mit dem Secure Enterprise Management (SEM) kann in der Server-Konfiguration unter “Routing Interface / Allgemein” für einen selektierten Adapter-Namen ein Fenster mit der Darstellung der Netzwerk-Konfiguration am Secure Server geöffnet werden. (Eine Verbindung zwischen SEM und Server muss über die Einstellung am Server, siehe oben **Server-Konfiguration**, hergestellt worden sein.) In diesem Fenster kann eine Adapter-Konfiguration vorgenommen werden, indem dem selektierten Adapter-Namen die IP- und MAC-Adressen eines anderen LAN-Adapters zugeordnet werden. (Siehe **Server Plug-in**)

Diese Konfiguration wird an den Server übertragen, wenn in den lokalen Server-Einstellungen festgelegt wurde, dass die Konfiguration vom SEM übernommen wird (siehe oben **Server-Konfiguration**). Diese Konfiguration bleibt auch dann erhalten, wenn zu einem späteren Zeitpunkt die Konfiguration nicht mehr vom SEM übernommen wird.

Die MAC-Adresse besteht aus 6 hexadezimalen Zahlen, die durch einen Punkt “.” getrennt sind. Die Standardadresse ist 00.00.00.00.00.00

IP-Adresse [Routing Interfaces]

Hier wird die IP-Adresse dieses LAN-Adapters, die er in den Netzwerkeinstellungen des Systems besitzt, angezeigt. Sie ist die WAN-seitige IP-Adresse des VPN Gateways. Diese Adresse darf keiner anderen Schnittstelle zugeordnet werden. Sie können dieser Schnittstelle jedoch auch mehrere IP-Adressen zuordnen. Mit dieser Adresse wird dem Routing Interface ein logisches Netzwerk (subnet) zugeordnet.

Mit dem Secure Enterprise Management (SEM) kann in der Server-Konfiguration unter “Routing Interface / Allgemein” für einen selektierten Adapter-Namen ein Fenster mit der Darstellung der Netzwerk-Konfiguration am Secure Server geöffnet werden. (Eine Verbindung zwischen SEM und Server muss über die Einstellung am Server, siehe oben **Server-Konfiguration**, hergestellt worden sein.) In diesem Fenster kann eine Adapter-Konfiguration vorgenommen werden, indem dem selektierten Adapter-Namen die IP- und MAC-Adressen eines anderen LAN-Adapters zugeordnet werden.

Diese Konfiguration wird an den Server übertragen, wenn in den lokalen Server-Einstellungen festgelegt wurde, dass die Konfiguration vom SEM übernommen wird (siehe oben **Server-Konfiguration**). Diese Konfiguration bleibt auch dann erhalten, wenn zu einem späteren Zeitpunkt die Konfiguration nicht mehr vom SEM übernommen wird.

Kommentar [Routing Interfaces]

Hier kann ein Kommentar zu dieser Routing-Schnittstelle eingegeben werden.

Optionen [Routing Interfaces]

In dieser Rubrik können Schutzmechanismen für Netzwerkadapter eingestellt werden.

LAN-Adapter schützen [Routing Interfaces]

Der Parameter “LAN-Adapter schützen” hat nur Bedeutung, wenn der PC über mindestens zwei Netzwerkkarten verfügt. Dieser Adapter lässt dann nur noch ein- und ausgehende Tunnel-Frames passieren. Ist die Funktion aktiv, betrifft sie alle Netzwerkkarten des PCs und sie sind gegen den Zugriff von anderen LAN-Benutzern im gleichen LAN gesperrt.

IP Network Address Translation [Routing Interfaces]

Wenn Sie IP Network Address Translation nutzen, wird jede VPN-IP-Adresse in eine systemeigene des lokalen LANs oder LAN-Adapters übersetzt. Die Adressen können im letzten Konfigurationsfeld “IP NAT” eingegeben werden.

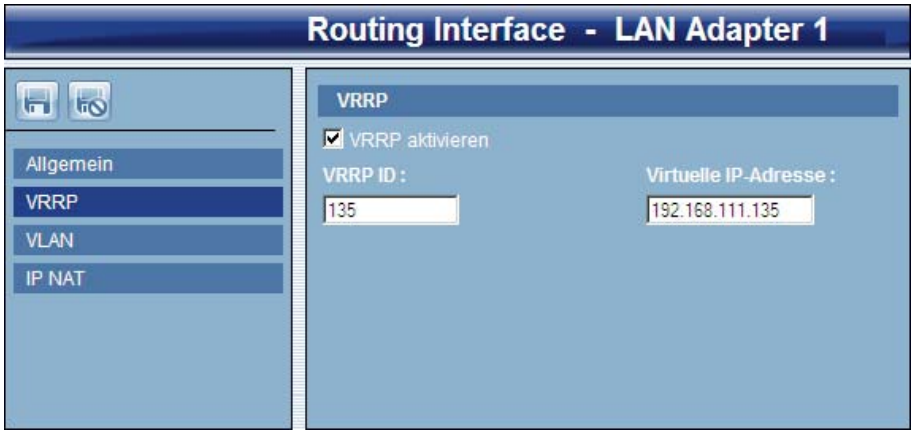
Stateful Inspection [Routing Interfaces]

Mit dieser Funktion wird Stateful Inspection für diese Netzwerkkarte eingeschaltet.

Stateful Inspection ist eine neue Firewall-Technologie und bietet den derzeit höchstmöglichen Sicherheitsstandard für Internet-Verbindungen und somit das Firmennetz. Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen verhindert diese Funktionalität den unbefugten Zugriff auf Daten und Ressourcen im zentralen Datennetz. Zum anderen überwacht sie als Kontrollinstanz den jeweiligen Status aller bestehenden Internet-Verbindungen.

VRRP [Routing Interfaces]

Das VRRP (Virtual Router Redundancy Protocol) wird zur Steigerung der Verfügbarkeit wichtiger Gateways in lokalen Netzen genutzt. Voraussetzung für den Einsatz des VRRP ist die Konfiguration eines HA-Systems im Failsafe- oder Load Balancing-Modus.



Kommt im Backup-Fall der Secondary Server im Failsafe-Modus zum Einsatz, so müssen bei Einsatz des VRRP keine Routing-Anpassungen des Standard-Routers mehr vorgenommen werden, da beide Gateways, die im Failsafe-Modus arbeiten, über eine gemeinsame IP-Adresse angesprochen werden können. (Beachten Sie dazu die PDF-Datei **HA-Szenarien**.*)*

VRRP aktivieren

Die beiden VPN Gateways (Failsafe oder Load Balancing Server) stehen innerhalb einer DMZ und besitzen je einen LAN-Adapter in Richtung Internet und einen in Richtung internes Firmennetz. Jeweils die LAN-Adapter der beiden Gateways in Richtung Internet, wie auch die LAN-Adapter in Richtung internes Firmennetz können unter Nutzung von VRRP eine gemeinsame virtuelle IP-Adresse und eine gemeinsame VRRP ID erhalten.

Erst im Anschluss daran kann die gemeinsame virtuelle IP-Adresse jeweils an die entsprechenden Adapter der Gateways gebunden werden.

Halten Sie sich bitte unbedingt an diese Reihenfolge, sonst kann diese Funktionalität nicht genutzt werden.

Zum Eintragen der gemeinsamen IP-Adressen öffnen Sie jeweils die Eigenschaften der Netzwerkadapter und fügen in den erweiterten TCP/IP-Einstellungen zusätzlich zur ersten IP-Adresse die gemeinsame hinzu.

Im Anschluss daran müssen die Dienste der beiden Gateways neu gestartet werden. Drücken Sie dazu den Restart-Button unter “Statistik / Systeminformationen”!

VRRP unter Linux

Am NCP Secure Server für Linux sind die beiden Scripte “dve_up” und “dve_down” hinterlegt. Sie befinden sich im Verzeichnis:
`/usr/local/ncp/ses/`

Diese Scripte werden vom NCP Secure Server dann aufgerufen, wenn er durch den HA-Server in den Betriebs-Modus FS_Master (dve_up) bzw. zum FS_Secondary (dve_down) geschaltet wird.

In diesen Beispielscripten (dve_up.sam und dve_down.sam) wird die Verwendung von arptables empfohlen. Arptables blockiert eingehende arp-Anfragen auf dem Backup Gateway (Secondary), während auf dem Master Gateway (Primary) diese Anfragen durchgelassen werden.

Arptables ist als zusätzliches Paket für viele Linux Distributionen erhältlich. Sollte die Verwendung von arptables nicht möglich sein, muss der Netzadapter gemäß der Beispiele aktiviert bzw. deaktiviert werden.

VRRP ID

Die ID ist frei wählbar zwischen 1 und 254. Die VRRP ID muss jeweils für das Paar der Gateways identisch sein, die als Master und Backup bzw. Primary und Secondary Gateway fungieren. Entsprechend muss diese ID auch auf dem Routing Interface zugewiesen sein, an das die gemeinsame virtuelle IP-Adresse gebunden wird.

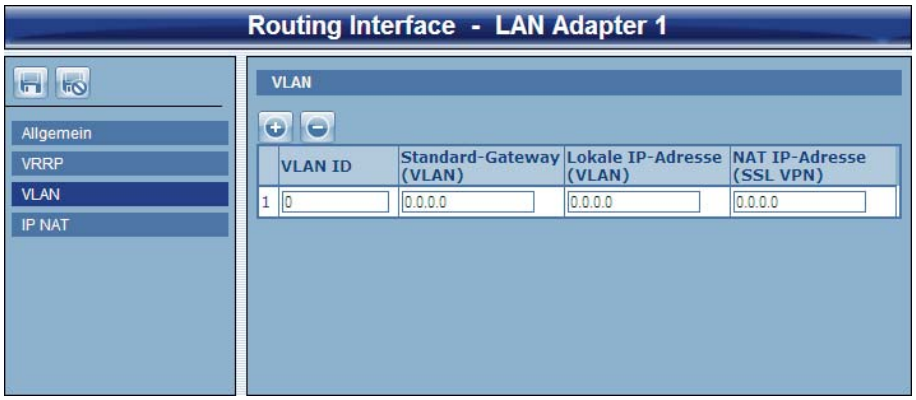
Virtuelle IP-Adresse

Über die virtuelle IP-Adresse werden zwei Gateways mit unterschiedlichen IP-Adressen zu einem virtuellen Router zusammengeschlossen. Die virtuelle IP-Adresse besitzen beide Gateways gemeinsam und muss deshalb jeweils für den externen bzw. internen LAN-Adapter eines Primary (Master) Gateways und eines Secondary (Backup) Gateways, die im VRRP-Modus stehen identisch sein.

VLAN [Routing Interfaces]

VLAN (Virtuelles LAN) ist neben GRE und VPN eine weitere Art der Tunnelweiterleitung für die Mitglieder einer bestimmten Domain-Gruppe. Ein VLAN wird nur dazu eingerichtet, die IP-Pakete der definierten Gruppe (zu einem anderen VLAN-fähigen Gateway) weiterzuleiten.

Nach drücken auf die Buttons "+ / -" können VLANs eingerichtet oder gelöscht werden.



Eine SSL VPN-Weiterleitung im VLAN ist nur unter Windows-Betriebssystemen möglich.

Das VLAN wird als Routing-Schnittstelle auf einem LAN-Adapter ins Firmennetz aufgesetzt. Pro LAN-Adapter können maximal 256 VLANs definiert werden. Von welcher Domain-Gruppe welches VLAN genutzt wird, wird dabei über die VLAN ID festgelegt.

VLAN ID [Routing Interfaces]

Jedem VLAN wird eine eindeutige Nummer zugeordnet, die VLAN ID.

Mit der VLAN ID wird eine bestimmte Domain-Gruppe einem bestimmten VLAN zugewiesen, d. h. die IP-Pakete der Mitglieder der Domain-Gruppe, die für die Weiterleitung die gleiche VLAN ID hat, werden über das VLAN mit dieser ID geschickt. Beachten Sie daher, dass der hier gesetzte Wert der ID auch in der entsprechenden Domain-Gruppe unter "Allgemein / Weiterleitung" eingetragen werden muss.

Die VLAN ID kann einen beliebigen Wert von 1 bis 4094 annehmen.

Standard-Gateway (VLAN)

Das VLAN wird zwischen diesem Secure Server und einem VLAN-fähigem Gateway im physikalischen Netz, dem "VLAN Default Gateway", hergestellt. Hier geben Sie dessen IP-Adresse an.

Vom VLAN Default Gateway werden die IP-Pakete weitergeleitet.

Lokale IP-Adresse (VLAN)

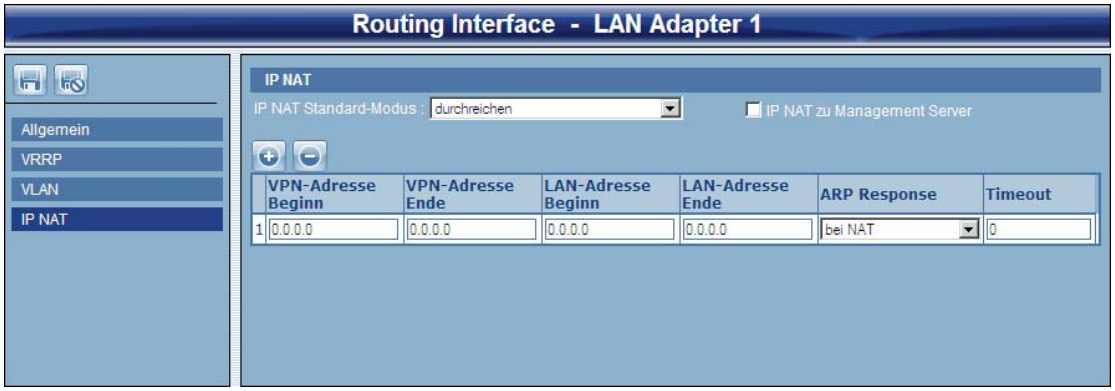
Dies ist die vom Administrator zu bestimmende Netz-Adresse des VLANs.

NAT IP-Adresse (SSL VPN)

IP-Pakete von SSL VPN-Benutzern werden mit dieser Quell-IP-Adresse über VLAN weitergeleitet.

Eine SSL VPN-Weiterleitung im VLAN ist nur unter Windows-Betriebssystemen möglich.

IP NAT [Routing Interfaces]



Wenn Sie für diesen Adapter IP NAT aktiviert haben (siehe oben: **Routing Interface / IP Nat aktivieren***) können Sie in diesem Feld weitere Einstellungen für IP NAT vornehmen.*

Dazu konfigurieren Sie eine Tabelle für IP NAT. Darin ist beschrieben, welche VPN-Adresse in welche LAN-Adresse übersetzt wird, wie lange diese Zuordnung beibehalten wird (Timeout) und wann eine Rückübersetzung bei einem ARP Request erfolgen soll (ARP Response).

IP NAT Standard-Modus

Dieser Modus bestimmt, wie mit VPN-Adressen verfahren wird, die nicht im Bereich der konfigurierten Tabelle liegen.

– durchreichen: die VPN-Adresse wird nicht in eine LAN-Adresse übersetzt
– IP NAT: die VPN-Adresse wird auf die LAN IP-Adresse des Gateways umgesetzt

IP NAT zu Management Server

Die Management Server-Requests des Clients werden auf die interne LAN-Adresse des Gateways gemappt.

VPN-Adresse (Beginn / Ende)

Dies ist die IP-Adresse, mit der sich der Client (nach Erhalt seiner IP-Adresse aus dem Firmennetz, siehe auch: **IP-Pool**) mit dem VPN Gateway verbindet.

LAN-Adresse (Beginn / Ende)

Dies ist die IP-Adresse mit der der Client nach Network Address Translation im LAN erscheint.

ARP Response

Die ARP Response gibt an, wann eine Rückübersetzung der LAN IP-Adresse bei einem ARP Request erfolgen soll:

– bei NAT
– bei Connect
– immer

Timeout

Dies ist ein Inactivity Timeout, der ab dem Moment angezählt wird, ab dem keine Nutzdaten fließen. Wird die hier eingetragene Zeitspanne erreicht, wird die Zuordnung VPN / LAN IP-Adresse aus der IP NAT-Tabelle aufgelöst.

Bei neuerlichem Datenaufkommen wird der VPN-Adresse wieder eine LAN-Adresse aus der IP NAT-Tabelle zugeordnet.

Standardwert ist 0 = der Timeout wird nicht angezählt.

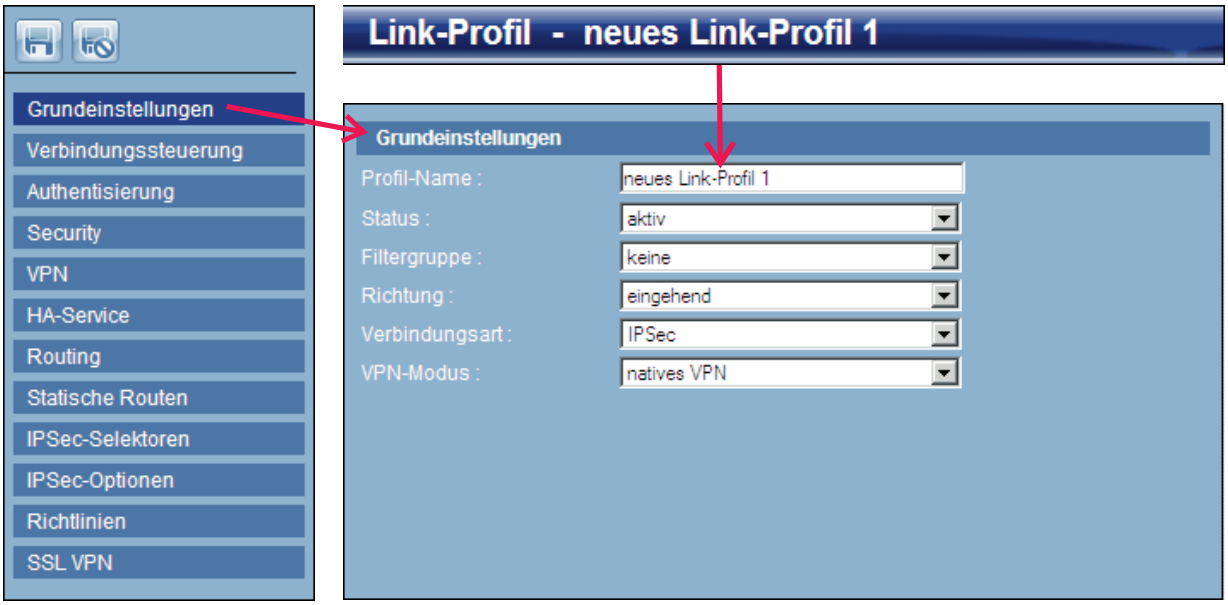
Link-Profile

Die Konfiguration der Link-Profile erfolgt dynamisch. D. h. das NCP Server-System braucht nach dem Einrichten oder Modifizieren eines Link-Profils weder abgeschaltet noch neu gestartet zu werden.

Ein neues Link-Profil legen Sie über das Hauptmenü mit Mausklick auf den Insert-Button an. Sie löschen ein Link-Profil per Mausklick auf den Remove-Button.

Bitte beachten Sie, dass Link-Profile, die Sie über das Web-Interface erstellt haben, komplett gelöscht werden, wenn Sie die Server-Konfiguration vom Secure Enterprise Management (SEM) herunterladen! (Siehe dazu oben **Server-Konfiguration**)

Grundeinstellungen



Profilname [Link-Profile]

Der Name für das Link-Profil wird zunächst automatisch generiert (neues Link-Profil 1, neues Link-Profil 2, etc.). Er ist frei editierbar.

Status [Link-Profile]

Mit dem Status wird bestimmt, ob eine Verbindung über das WAN möglich sein soll oder nicht. Wenn Sie den Status auf “aktiv” setzen, kann ein Link hergestellt werden, wenn Sie ihn auf “inaktiv” setzen, kann keine WAN-Verbindung hergestellt werden.

Der Status sollte auf “inaktiv” gestellt sein, während Sie die Konfiguration dieser WAN-Verbindung ändern und wenn ein weiterer aktiver Link dieselbe IP-Adresse benutzt.

Filtergruppe [Link-Profile]

Mit dem Listbutton wählen Sie eine von Ihnen definierte Filtergruppe (siehe: **Link-Filter, Filtergruppen**) aus und ordnen sie dieser logischen Verbindung zu. Diese bedeutet, dass kein Rechner in diesem Netzwerk, der ein Protokoll aus dieser Filtergruppe nutzt eine Verbindung zu einem Partner über diese WAN-Strecke herstellen kann.

Filter werden gesetzt, um Broadcasts zu unterbinden. Broadcasts werden normalerweise von Netzwerkteilnehmern gesendet, um Partnerstationen im Netz aufzuspüren oder um sich als möglicher Netzpartner zu erkennen zu geben. Diese Broascasts können auch den Inactivity Timeout verhindern und so zu hohen Gebühren in Wählnetzen führen. Deshalb wird empfohlen auf jedenfall Filter bzw. Filtergruppen zu setzen, um Verbindungskosten zu sparen. Dies sollte jedoch gut geplant durchgeführt werden.

Richtung [Link-Profile]

Mit der “Richtung” legen Sie fest, ob eine Verbindung auch von einem “eingehenden” (incoming, WAN -> LAN) Ruf aufgebaut werden kann oder nur von einem “abgehenden” (outgoing, LAN -> WAN), oder von beiden “bidirektional” (bidirectional).

Verbindungsart [Link-Profile]

Hier können Sie aus der Listbox das Verbindungsmedium per Mausklick auswählen, die für dieses Link-Profil genutzt werden soll (Standard ist IPSec). Die entsprechenden Adapter oder Tunnel-Protokolle müssen für das lokale System eingerichtet sein (siehe: **Lokales System**).

VPN-Modus [Link-Profile]

Je nach Lizenzierung kann dem mobilen Benutzer gestattet werden mit dem gleichen Benutzernamen und Passwort (siehe unten) verschiedene VPN-Kommunikationen zu nutzen.

Der oder die entsprechenden Lizenzschlüssel werden im Web Interface unter “System” als **Lizenz** oder auch als **SSL VPN-Lizenz** eingetragen. Wird nur der SSL VPN-Lizenzschlüssel für die Web-orientierte SSL VPN-Kommunikation eingetragen, so kann die IPSec-Kommunikation nicht genutzt werden. Ohne diesen Lizenzschlüssel kann die VPN SSL-Kommunikation nicht genutzt werden. Werden beide Lizenzschlüssel eingetragen, so kann ein mobiler Benutzer gegebenenfalls aus einem Internet-Café mit einem fremden Rechner ohne VPN Client über SSL VPN auf das Firmennetz mit dem gleichen Passwort/Benutzer-Paar zugreifen wie von seinem eigenen Rechner über einen VPN CLient. Die Schalterstellung ist im letzten Fall auf “beide” einzustellen, ansonsten entsprechend auf “Native VPN” (für IPSec- und L2TP-Tunneling) oder auf “Nur SSL VPN” (für SSL-Tunneling).

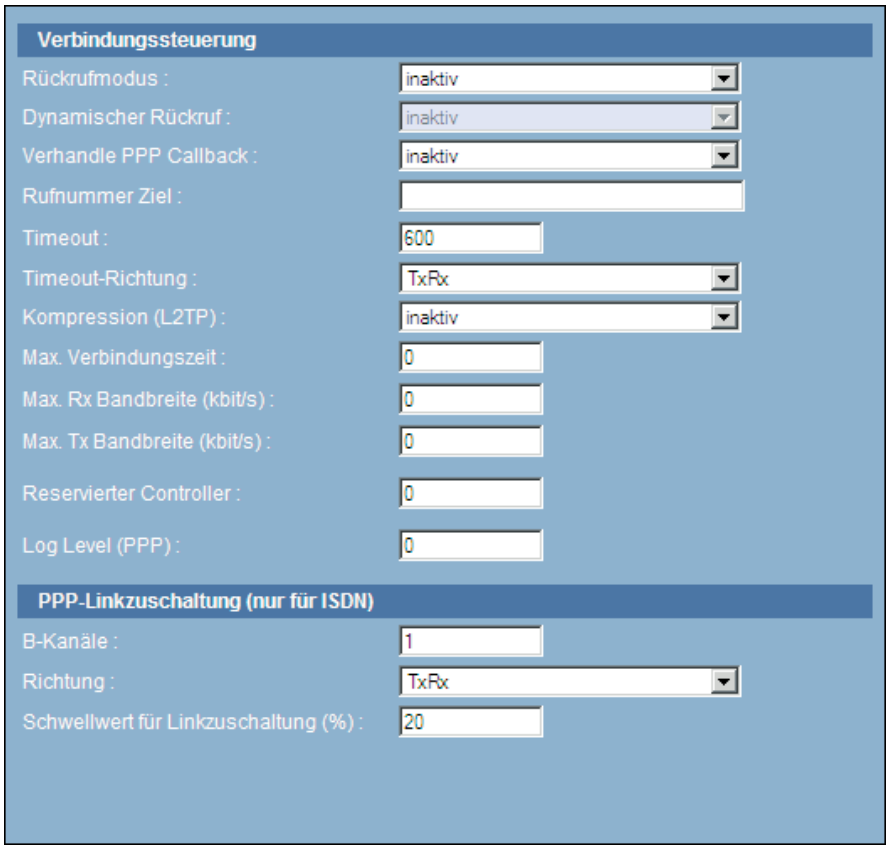
Benutzername und Passwort, die für die VPN-Kommunikation notwendig sind, werden über das Web-Interface unter dem entsprechenden Link-Profil unter “Authentisierung / Eingehende Verbindungen / **Benutzer**, **Passwort**” eingetragen.

Verbindungssteuerung

In diesem Parameterfeld kann ein Rückrufmodus festgelegt werden. Der Rückruf wird z. B. dann eingesetzt, wenn der Client vom Server per **Lock-ruf** *informiert wird, dass Daten für ihn bereit stehen. Der Client kann dann einen automatischen Rückruf ausführen und die Daten werden zwischen zentralem Gateway und Client übertragen.*

Sie stellen hier auch die Timeout-Werte ein und können Kompression (L2TP) aktivieren. Mit "Kompression" kann der Datendurchsatz um den Faktor 3 bis 5 erhöht werden, je nachdem um welche Daten es sich handelt.

Wenn Sie die Workstation in der "Verbindungsart" "ISDN" betreiben, können Sie in diesem Parameterfeld auch eine Kanalbündelung aktivieren. Bitte beachten Sie dabei, dass die Kanalbündelung nur funktionieren kann, wenn sowohl der Secure Client als auch der Server über gleich viele mögliche B-Kanäle verfügen.



Rückrufmodus [Link-Profile]

Die Möglichkeit eines Rückrufs kann nur mit einer Wählverbindung genutzt werden.

Der Rückruf von einem Server an eine Remote Workstation oder eine andere Remote-Maschine wird durch die Remote-Seite angestoßen. Von dort wird zunächst eine Verbindung aufgebaut, anschließend eine PPP-Verhandlung durchgeführt, danach die Verbindung abgebaut und schließlich die Verbindung vom Server an die Remote-Seite mit der konfigurierten Telefonnummer aufgebaut.

a) Wenn der **Rückruf vom Server** abgehen soll (outgoing call) wird einer der am Server eingestellten Rückrufmodi automatisch abgehandelt. Folgende Voraussetzungen müssen dazu an der Gegenstelle erfüllt sein:

Sie stellen den Rückrufmodus auf "aus". Mit dem Verbindungsaufbau (Hinauswählen) von der Remote-Seite (Workstation) zum Server wird der Server dazu angeregt, automatisch einen Rückruf auszuführen. Der vom Server verwendete Rückrufmodus muss von der Gegenseite unterstützt werden, darf jedoch nicht eingestellt werden! (Rückrufmodus = aus!).

Bitte beachten Sie, dass der automatische Rückruf nur stattfinden kann, wenn der Client und der Server für diese Verbindung folgende Bedingungen erfüllen (siehe: Eingehende Rufe):

– Der Client muss den Server anwählen können und eingehende Rufe (wie den Rückruf) zulassen, d.h. in dessen Profil-Einstellung muss im Fenster für **Eingehende Rufe** die "Richtung" auf "bidirektional" gestellt sein.

– Der Server muss die Rufnummer für den Rückruf wählen, die am Client im Fenster für **Eingehende Rufe** unter "Rufnummer lokal" eingetragen wurde. Dies muss die Rufnummer (Durchwahl) des PCs sein. Vergewissern Sie sich bitte, dass die im ISDN übermittelte Rufnummer genau der konfigurierten Nummer entspricht. Ziehen Sie im Zweifelsfall Ihren Internet Provider oder Systemadministrator zu Rate.

– Der Server muss sich mit "Benutzer" und "Passwort" beim Client anmelden, die im Fenster für **Eingehende Rufe** unter "Benutzer lokal" und "Passwort lokal" eingetragen wurden. Sind an dieser Stelle keine Code-Namen eingetragen, kann sich die Remote-Seite (Server) auch ohne Benutzer und Passwort anwählen.

b) Wenn der **Rückruf vom Client an den Server** erfolgen soll (incoming call):

Am Client wird einer der drei möglichen Rückrufmodi gewählt. Nachdem sich der Server an den Client angewählt hat, wird der Rückruf vom CLient an den Server im eingestellten Modus durchgeführt.

Bitte beachten Sie, dass der automatische Rückruf nur stattfinden kann, wenn der Client und der Server für diese Verbindung folgende Bedingungen erfüllen (siehe: Eingehende Rufe bei der Remote Workstation):

– Der Client muss den Server anwählen können und eingehende Rufe (wie den Rückruf) zulassen, d.h. in dessen Profil-Einstellung muss im Fenster für **Eingehende Rufe** die “Richtung” auf “bidirektional” gestellt sein.

– Der Client wählt die Rufnummer für den Rückruf, die in der Profil-Einstellung unter **Netzeinwahl** eingetragen wurde. Dies muss die Rufnummer (Durchwahl) des Servers sein. Vergewissern Sie sich bitte, dass die im ISDN übermittelte Rufnummer genau der konfigurierten Nummer entspricht. Ziehen Sie im Zweifelsfall Ihren Internet Provider oder Systemadministrator zu Rate.

– Der Client meldet sich mit “Benutzer” und “Passwort” beim Server an, die in der Profil-Einstellung unter **Netzeinwahl** von Ihnen eingetragen wurden. Diese Code-Namen müssen mit denen am Server übereinstimmen.

Rückrufmodi:

Aus (Disabled) = (standard)

PPP = (RFC 1570 konform) wird via B-Kanal nach dem Point-to-Point Protocol (PPP) abgehandelt; wird von den meisten Network Access Servern unterstützt

NCP = (NCP-spezifisch) wird via B-Kanal nach dem NCP Callback Control Protocol (CBCP) abgehandelt; kann nur mit NCP-Systemen eingesetzt werden

COSO = (Charge-One-Side-Only) auch Low-Level- oder D-Kanal-Rückruf; für den ISDN D-Kanal fallen keine (lokalen) Gebühren für Ihre Workstation an; COSO ist auch Cisco-kompatibel;

Wichtig: Für COSO-Rückruf muss eine CLI-Rufnummer zur Rufnummernauswertung konfiguriert werden (siehe: Authentisierung / Security). COSO-Rückruf kann nur ausgeführt werden, wenn RADIUS-Support nicht aktiviert ist (siehe: RADIUS).

Dynamischer Rückruf [Link-Profile]

Wenn dynamischer Rückruf für diese Verbindung eingestellt ist, wird jede Rufnummer, die sich hier einwählt vom Server zurückgerufen. (Am Client muss dazu unter “Rückruf” die jeweils gültige “Rückrufnummer” eingetragen werden.)

Verhandle PPP Callback [Link-Profile]

Sie aktivieren die PPP Callback-Verhandlung nur, wenn ein Rückruf von der Remote-Seite erfolgen soll und die Remote-Seite den Rückrufmodus PPP Callback verwendet.

Rufnummer Ziel [Link-Profile]

Solange dieses Feld leer bleibt, kann keine abgehende Verbindung aufgebaut werden.

Für eine abgehende Festverbindung muss die Null “0" eingetragen werden.

Für eine abgehende Wählverbindung muss hier die Rufnummer des Ziels eingetragen werden.

Diese Rufnummer muss genauso eingetragen werden, als würden Sie diese Telefonnummer per Hand wählen. D. h. Sie müssen alle notwendigen Vorwahlziffern berücksichtigen: Landesvorwahl, Ortsvorwahl, Durchwahlziffern, etc... vergessen Sie auch nicht die Amtsholung wenn Sie an einer Nebenstellenanlage angeschlossen sind!

Beispiel: Sie wollen eine Verbindung von Deutschland nach England herstellen:

00 (für die internationale Verbindung, wenn Sie von Deutschland aus wählen)
44 (dies ist die landesspezifische Vorwahl für England)
171 (Vorwahl für London)
1234567 (die Nummer, die Sie zu erreichen wünschen)

Insgesamt wird nach diesem Beispiel folgende Nummer im Telefonbuch gespeichert und für die Anwahl verwendet: 00441711234567

Die Rufnummer des Ziels kann bis zu 30 Ziffern beinhalten.

Hinweis: Wenn vom Server ein Rückruf ausgeführt werden soll, muss hier die Rufnummer des Client-Systems eingetragen werden.

Timeout [Link-Profile]

Mit diesem Parameter wird der Zeitraum festgelegt, der nach der letzten Datenbewegung (Empfang oder Versenden) verstreichen muss, bevor automatisch ein Verbindungsabbau erfolgt. Der Wert wird in Sekunden zwischen 1 und 65356 angegeben. Der Standardwert ist “40".

Hinweis: Um den Timeout zu aktivieren, ist es nötig, einen Wert zwischen 1 und 65356 einzutragen. Mit dem Wert “0" wird der automatische Timeout (Verbindungsabbau) nicht ausgeführt. Der Wert ”0" bedeutet, dass das Trennen der Verbindung manuell durchgeführt werden muss.

Wichtig: Der Timer für das gewählte Zeitintervall läuft erst dann an, wenn keine Datenbewegung oder Handshake mehr auf der Leitung stattfindet. Um den Timeout auch für Bridging (802.2- und NetBIOS-Daten) effektiv einsetzen zu können, ist es nötig “Local Termination” zu aktivieren.

Timeout-Richtung [Link-Profile]

Mit diesem Parameter bestimmen Sie, für welche Übertragungsrichtung der Timeout gelten soll. Drei verschiedene Einstellungen sind möglich:

TxRx
(standard) in diesem Fall achtet die Workstation sowohl auf das Ende der gesendeten (out) als auch der empfangenen (in) Daten, bevor der Timer angestoßen wird.

Tx
nur die Senderichtung (out) wird beobachtet.

Rx
nur die Empfangsrichtung (in) wird beobachtet.

Hinweis: Um die Timeout-Richtung zur Geltung kommen zu lassen, muss der Wert für den Timeout zwischen 1 und 65356 gewählt sein.

Kompression (L2TP) [Link-Profile]

Mit diesem Parameter bestimmen Sie den Typ der Kompression. Drei Einstellungen sind möglich:

Aus (standard), d.h. ohne Kompression

STAC (without History)

STAC mit History Cisco-kompatibel

Wichtig: Der hier gewählte Typ der Kompression muss auch von der Gegenstelle unterstützt werden.

Mit Kompression kann der Datendurchsatz um den Faktor 3 bis 5 erhöht werden, je nachdem um welche Daten es sich handelt.

Wichtig: Nutzen Sie nicht gleichzeitig “Stac mit History” und “Kanalbündelung”. Dies drückt die Übertragungsrate.

Maximale Verbindungszeit [Link-Profile]

In dieses Parameterfeld kann eine Zeitspanne in Sekunden eingetragen werden (Null besitzt keine Gültigkeit). Diese Zeitspanne bestimmt die maximale Verweildauer für den Benutzer im Firmennetz. Unabhängig davon ob eine Datenübertragung stattfindet oder nicht, wird die Verbindung abgebaut, sobald die maximale Verbindungszeit erreicht ist.

Die maximale Verbindungszeit kann auf drei Ebenen eingestellt werden:

– linkspezifisch hier (gilt nur für den jeweiligen Benutzer)

– gruppenspezifisch unter **Domain-Gruppen / Allgemein** (gilt für alle Benutzer der jeweiligen Gruppe)

– global für dieses Gateway unter **Lokales System / Restriktionen** (gilt für alle Benutzer)

Auf allen drei Ebenen kann eine jeweils unterschiedliche maximale Verbindungszeit eingestellt werden. Für den aktuell ins Firmennetz eingewählten Benutzer wird immer nur die Verweildauer gestattet, die die höchste Priorität hat. Dabei hat die linkspezifische Konfiguration Priorität vor der gruppenspezifischen und diese vor der globalen.

Bitte beachten Sie, dass die Timeout-Funktion nur wirksam werden kann, wenn die eingetragene Zeitspanne kleiner ist als die maximale Verbindungszeit, gleich auf welcher Ebene sie gesetzt wurde.

Maximale Bandbreite (kbit/s) [Link-Profile]

Mit diesem Parameter kann die maximal zur Verfügung stehende Bandbreite pro Benutzer in kBits/sec eingetragen werden (Null besitzt keine Gültigkeit). Damit kann unabhängig vom Verbindungsmedium der entfernten Clients die zentralseitig verfügbare Bandbreite für alle Benutzer gleich-

mäßig zugeteilt werden. Dabei wird unterschieden, ob die Bandbreite für ausgehenden (Tx) oder eingehenden (Rx) Datenverkehr genutzt wird.

Beachten Sie, dass die Zentralseite die Bandbreite unabhängig von der Richtung des Datenaufkommens zur Verfügung stellt. Ist die Bandbreite ausgeschöpft, kann kein weiterer Datenverkehr stattfinden.

Die Bandbreitenbeschränkung kann nur für TCP-Anwendungen genutzt werden.

Die maximale Bandbreite kann auf drei Ebenen eingestellt werden:
– linkspezifisch unter **Link-Profile / Verbindungssteuerung** (gilt nur für den jeweiligen Benutzer)
– gruppenspezifisch unter **Domain-Gruppen / Allgemein** (gilt für alle Benutzer der jeweiligen Gruppe)
– global für dieses Gateway unter **Lokales System / Restriktionen** (gilt für alle Benutzer)

Auf allen drei Ebenen kann eine jeweils unterschiedliche maximale Bandbreite eingestellt werden. Für den aktuell ins Firmennetz eingewählten Benutzer wird immer nur die Bandbreite gestattet, die die höchste Priorität hat. Dabei hat die linkspezifische Konfiguration Priorität vor der gruppenspezifischen und diese vor der globalen.

Reservierter Controller [Link-Profile]

Wenn mehrere Controller für ein Verbindungsmedium im System zur Verfügung stehen, kann für ein Link-Profil für ausgehende Rufe ein Controller mit Hilfe seiner Ordnungsziffer reserviert werden. (Eingehende Rufe nehmen den Weg über den Controller, der ihnen über die Rufnummer für das jeweilige Verbindungsmedium zugewiesen wird.)

Einen Controller zu reservieren kann zweckmäßig sein, wenn viele Rückrufe ausgelöst werden. In diesem Fall können alle Rückrufe über den reservierten Controller abgewickelt werden. Allerdings muss dabei das Verbindungsmedium berücksichtigt werden (ein Modem kann nicht über einen ISDN-Controller zurück gerufen werden.)

Ein Controller muss reserviert werden, wenn ISDN-Festverbindungen genutzt werden, da im Konfigurationsbaum nicht unterschieden werden kann zwischen ISDN-Wählverbindung und ISDN-Festverbindung. Zudem können verschiedene Zielsysteme über verschiedene Controller, d.h. verschiedene Festverbindungen, erreichbar sein. Alle Link-Profile für eines dieser bestimmten Zielsysteme müssen dann den richtigen Controller für eine der ISDN-Festverbindungen nutzen. Zudem dürfen abgehende ISDN-Wählverbindungen oder Modem-Verbindungen die Controller für Festverbindungen nicht nutzen. Bei einer derartigen Mischkonfiguration muss deshalb auch für die abgehenden Wählverbindungen ein definierter Controller zugeordnet werden.

Wenn im System keine Festverbindungen konfiguriert wurden, wird mit dem Eintrag “0" unter ”Link-Profile, Allgemein" sichergestellt, dass für ausgehende Rufe der nächstfreie dem Verbindungsmedium entsprechende Controller genommen wird.

Log Level [Link-Profile]

Der Debug Level hat keinen Einfluss auf die Funktion. Er dient nur der technischen Diagnose. Die Tiefe der Diagnose-Schichten sollte im normalen Betrieb immer auf “0" eingestellt sein, da sonst die automatisch geführten Log-Dateien ständig überlaufen.

Debug Levels sollten nur vom Personal des technischen Supports gesetzt werden. Um einen Störfall zu analysieren, werden die Debug Levels vor dem Start des fehlerhaften Systems hochgesetzt. Mit einem hiernach erstellten Hex Dump (TRACE.*) kann der NCP Support eine Fehlerauswertung vornehmen.

PPP-Linkzuschaltung (nur für ISDN) [Link-Profile]

In diesem Parameterfeld nehmen Sie Einstellungen für die Linkzuschaltung vor. Mit dynamischer Linkzuschaltung können bis zu 8 ISDN B-Kanäle gebündelt werden. Um diese Funktion in vollem Umfang nutzen zu können, muss allerdings diese Maschine wie auch die Gegenstelle mit der nötigen Anzahl von So-Schnittstellen (4) ausgestattet sein. Linkzuschaltung funktioniert auch bei ungleicher Anzahl von So-Schnittstellen auf beiden Seiten und nutzt dann maximal die Anzahl der ISDN-B-Kanäle, die auf der Seite mit weniger So-Schnittstellen zur Verfügung stehene.

Mit dynamischer Linkzuschaltung erhöhen sich zwar die Kosten für jeden zugeschalteten B-Kanal, gleichzeitig verringern sie sich jedoch in höhererm Maße, weil sich die Übertragungsdauer entsprechend verkürzt!

B-Kanäle [Link-Profile]

Die hier angegebenen Kanäle (2-8) müssen mit denen in der ISDN-Konfiguration übereinstimmen. Mit “1" ist die Kanalbündelung ausgeschaltet.

Dynamische Linkzuschaltung [Link-Profile]

Mit diesem Parameter bestimmen Sie, wie die Linkzuschaltung erfolgen soll. Drei Möglichkeiten stehen zur Auswahl:

Aus
(standard)

Tx
Links werden zugeschaltet, wenn der Schwellwert durch die Bitrate der von hier aus gesendeten Daten überschritten wird

Rx
Links werden zugeschaltet, wenn der Schwellwert durch die Bitrate der hier empfangenen Daten überschritten wird

TxRx
Links werden zugeschaltet, wenn der Schwellwert durch die Bitrate der übertragenen (gesendeten oder empfangenen) Daten überschritten wird

Schwellwert für Linkzuschaltung [Link-Profile]

Der Schwellwert für Linkzuschaltung (Channel on Demand) teilt dem Server die Bitrate mit, ab der ein weiterer Kanal zugeschaltet werden soll. Er entspricht einem Prozentsatz der maximalen Bitrate. Mögliche Werte sind von 1 bis 100 (Prozent). Standardwert ist “20".

Die Kanäle werden wieder geschlossen, wenn die Bitrate unter den kritischen Wert der Zuschaltung sinkt oder wenn der Timeout eintritt.

Diese Einstellung kommt nur zum Tragen, wenn die Linkzuschaltung bei Sender und Empfänger aktiviert wurde. Dabei sollte der Schwellwert bei Sender und Empfänger unterschiedlich sein (z.B. “20" und ”90). Das Öffnen und Schließen eines Kanals wird von der Seite initiiert, auf der der niedrigere Schwellwert gesetzt ist.

Beispiel:
Wird der Schwellwert auf “50" gesetzt und wird zu Beginn eines Datentransfers nur ein ISDN-B-Kanal genutzt (64 kBit/s), so wird ein zweiter Kanal zugeschaltet, sobald 32 kBit/s erreichet werden. Damit erhöht sich die maximale Bitrate auf 128 kBit/s, so dass ein dritter Kanal erst zugeschaltet wird, wenn 64 kBit/s erreicht werden. Der zweite Kanal wird wieder abgebaut, sobald 32 kBit unterschritten werden.

Authentisierung

Die Einstellungen in diesem Feld definieren wie die NCP Security Features für diese Verbindung genutzt werden.

Die Server Software unterstützt sowohl Authentisierungsverfahren nach CHAP (Challenge Handshake Authentication Protocol) als auch nach PAP (Password Authentication Protocol). Die Security-Verhandlungen erfolgen jeweils automatisch und hängen von der Methode ab, die die Remote-Seite verwendet.

Dabei ist CHAP, die am häufigsten eingesetzte Methode, sicherer als PAP, da das Passwort verschlüsselt übertragen wird. PAP überträgt das Passwort in Klartext.

Beachten Sie zu den Authentisieungs-Einstellungen in den Link-Profilen auch die Einstellungen im Abschnitt **Lokales System / Authentisierung** .

Benutzer (Ausgehende Verbindung) [Link-Profile]

Diese Benutzer-ID ist optional. Wird an dieser Stelle keine ID eingetragen, so wird statt dessen die ID “Benutzer (System)” aus den Einstellungen zu **Lokales System / Allgemein** ausgewertet. Diese ID gilt nur für abgehende Rufe unter Nutzung dieser speziellen Link-Konfiguration. Baut diese Maschine eine Verbindung über diesen Link auf, meldet sie sich mit “Benutzer (Ausgehende Verbindung)” bei der Gegenstelle an.

Diese PPP-ID wird entsprechend den RFC-Spezifikationen für das CHAP-Protokoll abgearbeitet und muss von der Gegenstelle erkannt werden. Wird auf der Remote-Seite die NCP Client Software eingesetzt, so muss diese ID übereinstimmen mit “Benutzer lokal” im Parameterfeld **Eingehende Rufe**.

Die ID kann bis zu 253 Zeichen lang sein.

Wichtig: Bitte beachten Sie unbedingt weiter unten die Beschreibung zur gegenseitigen Authentisierung!

Passwort (Ausgehende Verbindung) [Link-Profile]

Dieses Passwort ist optional. Wird an dieser Stelle kein Passwort eingetragen, so wird statt dessen das “Passwort (System)” aus aus den Einstellungen zu **Lokales System / Allgemein** ausgewertet.

Dieses Passwort gilt nur für abgehende Rufe unter Nutzung dieser speziellen Link-Konfiguration. Baut diese Maschine eine Verbindung über diesen Link auf, weist sie sich mit diesem Passwort bei der Gegenstelle aus.

Dieses PPP-Passwort wird entsprechend den RFC-Spezifikationen für das CHAP-Protokoll abgearbeitet und muss von der Gegenstelle erkannt werden. Wird auf der Remote-Seite die NCP Client Software eingesetzt, so muss dieses Passwort übereinstimmen mit “Passwort lokal” im Parameterfeld **Eingehende Rufe**.

Das Passwort kann bis zu 253 Zeichen lang sein.

Wichtig: Bitte beachten Sie unbedingt weiter unten die Beschreibung zur gegenseitigen Authentisierung!

Benutzer (Eingehende Verbindung) [Link-Profile]

Diese Benutzer-ID ist für eingehende Rufe unter Nutzung dieser speziellen Link-Konfiguration zwingend erforderlich.

Diese PPP-ID wird entsprechend den RFC-Spezifikationen für das CHAP-Protokoll von dieser Maschine abgehandelt. Will die Remote-Seite (NAS, RADIUS Server oder NCP Client) eine Verbindung zu dieser Maschine über diesen Link aufbauen, muss sie sich mit dieser Benutzer-ID anmelden, sonst wird der Verbindungswunsch von dieser Maschine abgewiesen.

Wird auf der Remote-Seite die NCP Client Software eingesetzt, so muss diese ID übereinstimmen mit “Benutzer” im Parameterfeld “Netzeinwahl”.

Die ID kann bis zu 253 Zeichen lang sein. Da die ID linkspezifisch ist, darf sie nur einmal im System vorkommen.

Wichtig: Wichtig: Bitte beachten Sie unbedingt weiter unten die Beschreibung zur gegenseitigen Authentisierung!

Benutzer und Passwort bei SSL VPN-Verbindungen

Im Parameterfeld “Authentisierung” vergeben Sie unter “Eingehende Verbindungen” den Benutzernamen und das Passwort für den Anwender. Mit diesen Zugangsdaten wird der Anwender immer authentisiert.

Wurde für den Anwender keine zertifikatsbasierte Authentisierung konfiguriert, muss er diese Zugangsdaten auf der Login-Seite des Browsers eingeben, um eine Verbindung zum Gateway herstellen zu können.

Wurde eine zertifikatsbasierte Authentisierung für den Anwender festgelegt, so ist zu unterscheiden, ob diese Art der Authentisierung in der Listener- (siehe: SSL VPN) oder in der Link-Konfiguration (an dieser Stelle) gemacht wird.

Wurde die zertifikatsbasierte Authentisierung in der Listener-Konfiguration festgelegt, so gilt sie für alle SSL VPN-Anwender, unabhängig davon, ob in der Link-Konfiguration unter “SSL VPN” (siehe unten) ein Login nur mit Zertifikat zugelassen wird oder nicht.

Außerdem ist darauf zu achten, ob der Benutzername aus einem Zertifikatsinhalt gebildet wird oder nicht. Benutzername und Passwort sind frei wählbar, wenn kein Zertifikatsinhalt zugrunde liegt. Im anderen Fall müssen Benutzername und Passwort gleich sein und genau dem Zertifikatsinhalt entsprechen, auf den in der Listener-Konfiguration verwiesen wird.

Passwort (Eingehende Verbindung) [Link-Profile]

Dieses Passwort ist für eingehende Rufe unter Nutzung dieser speziellen Link-Konfiguration zwingend erforderlich.

Dieses PPP-Passwort wird entsprechend den RFC-Spezifikationen für das CHAP-Protokoll von dieser Maschine abgehandelt. Will die Remote-Seite (NAS, RADIUS Server oder NCP Client) eine Verbindung zu dieser Maschine über diesen Link aufbauen, muss sie sich mit diesem Passwort anmelden, sonst wird der Verbindungswunsch von dieser Maschine abgewiesen.

Wird auf der Remote-Seite die NCP Client Software eingesetzt, so muss dieses Passwort übereinstimmen mit “Passwort” im Parameterfeld “Netzeinwahl”.

Das Passwort kann bis zu 253 Zeichen lang sein. Da das Passwort linkspezifisch ist, darf es nur einmal im System vorkommen.

Wichtig: Bitte beachten Sie unbedingt weiter unten die Beschreibung zur gegenseitigen Authentisierung!

Gegenseitige Authentisierung [Link-Profile]

Diese Funktion kann für eine erweiterte Zugriffskontrolle verwendet werden. Wenn die Funktion “Gegenseitige Authentisierung” aktiviert ist, müssen sich beide Kommunikationspartner immer gegenseitig per CHAP oder PAP identifizieren, bevor eine Verbindung durchgeschaltet wird.

Zunächst muss sich der Kommunikationspartner ausweisen, der beabsichtigt eine Verbindung herzustellen. Nachdem dies erfolgt ist und ihn der Partner der Zielseite erkannt hat, muss sich auch dieser Partner auf der Zielseite ausweisen. Erst nachdem auch dieser Partner von der Gegenseite erkannt wurde, wird die Verbindung aufgebaut.

1. Beabsichtigt der Router eine Verbindung zu einem Remote-Partner herzustellen, so kann er eine definierte Link-Konfiguration für einen abgehen-

den Ruf zu diesem Partner nutzen. D.h. zur Authentisierung wird die ID und das Passwort für nur diese spezielle Link-Konfiguration genutzt. Dies sind in diesem Fall “Benutzer” und “Passwort” für abgehende Verbindung (siehe oben).

Handelt es sich bei der Remote-Seite um einen NCP Client, so muss Link-spezifischer “Benutzer” und “Passwort” des Servers mit “Benutzer (lokal)” und “Passwort (lokal)” im Parameterfeld “Eingehende Rufe” auf Seiten des Clients übereinstimmen.

Ist die Gegenstelle ein NCP Server, so muss Link-spezifischer “Benutzer” und “Passwort” mit “Benutzer (System)” und “Passwort (System)” auf der Gegenseite übereinstimmen.

2. Beabsichtigt die Remote-Seite eine Verbindung zum Server herzustellen, so kann vom Server keine definierte Link-Konfiguration für diesen eingehenden Ruf genutzt werden. Wüsste der Server, wem gegenüber er sich ausweisen muss, könnten zur Authentisierung die Parameter einer definierten Link-Konfiguration genutzt werden. Da der Server aber zunächst nicht weiß, wem gegenüber er sich ausweisen muss, nutzt er in diesem Fall die nicht link-spezifischen Parameter “Benutzer (System)” und “Passwort (System)” aus dem Parameterfeld “Lokales System / Allgemein”.

Handelt es sich bei der Remote-Seite um einen NCP Client, so muss System-spezifischer “Benutzer (System)” und “Passwort (System)” des Servers mit “Benutzer lokal” und “Passwort lokal” im Parameterfeld “Eingehende Rufe” auf Seiten des Clients übereinstimmen.

Ist die Gegenstelle ein NCP Server, so muss System-spezifischer “Benutzer (System)” und “Passwort (System)” mit “Benutzer” und “Passwort” auf der Gegenseite übereinstimmen.

(siehe: **Lokales System / Authentisierung**)

Rufnummer für CLI [Link-Profile]

Die Rufnummer für CLI (Calling Line Identifikation/Rufnummernauswertung) muss immer dann eingesetzt werden, wenn Low Level Callback (COSO) für diese Link-Konfiguration definiert wurde (siehe: Rückrufmodus" unter “Link-Profile, Verbindungssteuerung). Ansonsten ist die Rufnummernauswertung optional und kann als Zugangsbeschränkung genutzt werden.

Die Rufnummernauswertung ist ausschließlich ein ISDN-Leistungsmerkmal. Wenn Sie genutzt wird, ist der Zugriff auf diesen NAS nur von dem ISDN-Anschluss möglich, der durch die hier eingegebene Rufnummer bestimmt wird.

Mit dieser Funktion kann die komplette Rufnummer oder nur ein Teil von ihr ausgewertet werden. Bei der Auswertung werden die Ziffern der Rufnummer von rechts nach links berücksichtigt. Wenn zum Beispiel die bei der Einwahl im ISDN-B-Kanal mitgegebene Anschlussnummer der Gegenseite 49-911-578361-2073 lautet und an dieser Stelle zur Rufnummernauswertung 2073 eingegeben wird, so wird der Ruf entgegen genommen.

Maximal können 30 Stellen zur Rufnummernauswertung eingegeben werden.

(siehe: **Lokales System / Authentisierung**)

Multi User-Profil [Link-Profile]

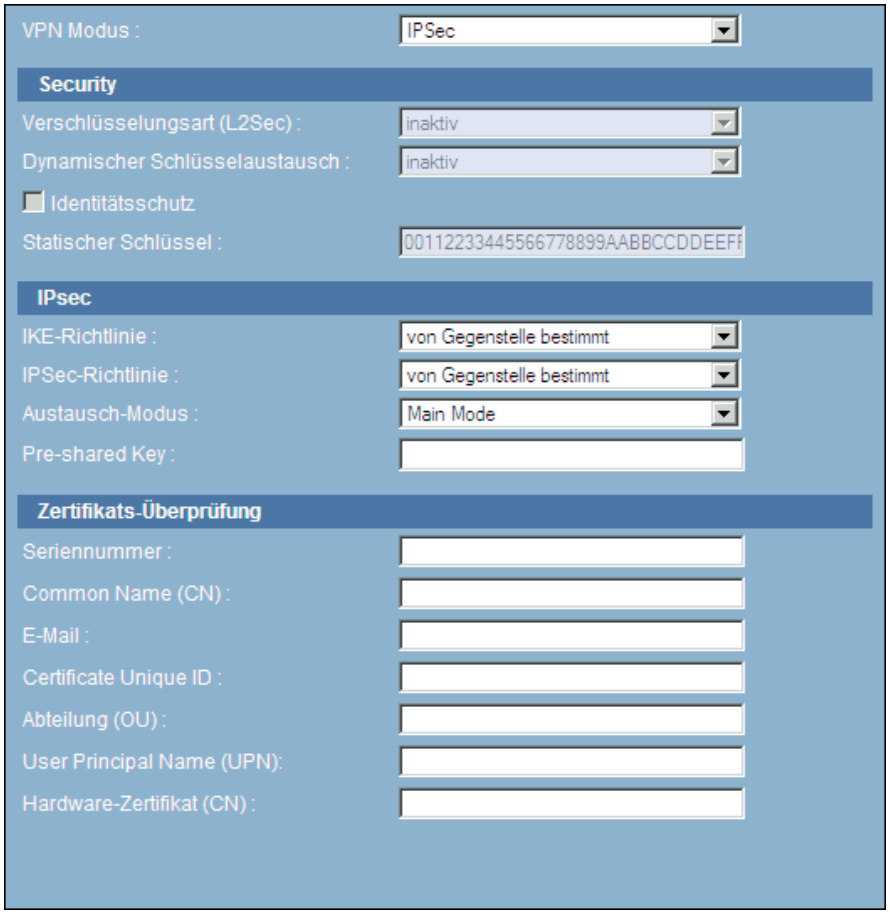
Mit diesem Parameter ist es möglich, dass sich mehrere Benutzer mit dem selben Paar “Benutzer” und “Passwort” am VPN-Gateway einwählen können. (Die Statistik wird unter RADIUS/LDAP angezeigt.) Dies wird benötigt, damit bei einem Rollout für viele Benutzer gleichzeitig die Verbindung zum Management Server hergestellt werden kann. Vom Management Server erhalten die Benutzer ihre erste Konfiguration.

[Link Profile, Authentisierung, Benutzer, Passwort]

Security

Im Parameterfeld "Security" sind die Konfigurationsparameter zu den Security-Modi L2Sec und IPSec für den Einsatz in Remote Access-Umgebungen gesammelt. Je nach eingestelltem Sicherheits-Modus, L2Sec oder IPSec, kann eine weitergehende Parametrisierung vorgenommen werden.

IPSec kann sowohl in einem L2TP-Tunnel (over L2TP) als auch ohne L2TP-Tunnel (native IPSec, auch IPSec-Tunneling) gefahren werden.



Security-Modus [Link-Profile]

Hier legen Sie fest, nach welchem Sicherheits-Standard, IPSec oder L2Sec, eine Verbindung zugelassen wird.

inaktiv = Verschlüsselung und Authentisierung sind ausgeschaltet

L2Sec = Alle Sicherheits-Verhandlungen erfolgen verschlüsselt und sicher in einem End to End-Tunnel (Layer 2) zwischen Client und Secure Server.

IPSec = Mit dieser Option kann über jeden Layer-2-Provider-Medientyp (siehe: Grundeinstellung / Verbindungsmedium), wie ISDN oder L2TP, zwischen Client und Server der Standard IPSec im Tunnel-Modus (Layer 3) eingesetzt werden.

Der Security-Modus IPSec ist dann fest eingestellt, wenn in den Grundeinstellungen als Verbindungsmedium das VPN-Protokoll IPSec gewählt wurde.

Verschlüsselungsart (L2Sec) [Link-Profile]

Wenn Sie als Modus L2Sec gewählt haben, können Sie hier entscheiden, ob eine Verschlüsselung eingesetzt werden soll und welche Art der Verschlüsselung verwendet werden soll. Bitte beachten Sie dabei, dass die Verschlüsselung der Daten nur möglich ist, wenn auf der Gegenseite eine entsprechende Verschlüsselungsart eingestellt wurde.

Aus = Verschlüsselung nicht aktiv (standard)

DES = Die Verschlüsselung erfolgt nach dem DES-Standard mit 128 Bit. (Nutzt die Gegenstelle eine NCP Client Software, so muss dort im Parameterfeld "Verschlüsselung" eingegeben werden "Von Gegenstelle bestimmt".)

Triple DES = Die Verschlüsselung erfolgt nach dem Triple DES-Standard mit 128 Bit. (Nutzt die Gegenstelle eine NCP Client Software, so muss dort im Parameterfeld "Verschlüsselung" eingegeben werden "Von Gegenstelle bestimmt".)

Blowfish = Die Verschlüsselung erfolgt nach dem Blowfish-Standard mit 128/448 Bit. (Ist die Gegen-

stelle eine NCP Client Software, so muss dort im Parameterfeld “Verschlüsselung” eingegeben werden “Von Gegenstelle bestimmt”.)

AES = Die Verschlüsselung erfolgt nach dem Advanced Encryption Standard mit 128, 192 oder 256 Bit. (Ist die Gegenstelle eine NCP Client Software, so muss dort im Parameterfeld “Verschlüsselung” eingegeben werden “Von Gegenstelle bestimmt”.)

Dynamischer Schlüsselaustausch [Link-Profile]

Der dynamische Schlüsselaustausch gemäß dem SSL-Protokoll (Secure Socket Layer) kann nur aktiviert und konfiguriert werden, wenn vorher Verschlüsselung aktiviert wurde.

Deaktiviert = Dynamischer Schlüsselaustausch ist ausgeschaltet, standard

SSL = Der dynamische Schlüsselaustausch nach SSL-Protokoll wird aktiviert. Beim Booten werden dabei zwei Schlüssel generiert, ein Private Key und ein Public Key. Beide Schlüssel sind systemgeschützt und können nicht eingesehen werden. Mit Hilfe dieser beiden Schlüssel wird für jede Session ein neuer Session Key generiert, der via SSL-Protokoll übertragen wird. (Ist die Gegenstelle ein NCP Client, so muss dort im Parameterfeld “Verschlüsselung” “Von Gegenstelle bestimmt” eingegeben werden.)

SSL mit Zertifikat = Mit dieser Verschlüsselung, dynamischer Schlüsselaustausch gemäß SSL-Protokoll, ist ein Verbindungsaufbau nur möglich, wenn vorher an der Gegenstelle eine gültige PIN eingegeben wurde. Der Remote-Zugriff wird also erst nach Prüfung des Zertifikats auf der Chipkarte oder in einer PKCS#12-Datei der Gegenstelle zugelassen. (Ist die Gegenstelle ein NCP Client, so muss dort im Parameterfeld “Verschlüsselung” “SSL mit Zertifikat” eingegeben werden.)

Wenn die Verbindung aufgrund unkorrekter SSL-Authentisierung abgelehnt wird, wird eine Fehlermeldung erzeugt, die in der Trap-Datei eingesehen werden kann.

Identitätsschutz

Wenn im Security-Modus L2Sec ein dynamischer Schlüsselaustausch mit Zertifikatsprüfung (SSL mit Zertifikat) durchgeführt wird, wird der Client durch Aktivierung dieser Funktion dazu veranlasst, das Zertifikat, bzw. die Benutzerdaten darauf, verschlüsselt zu übertragen. Auf diese Weise ist der Identitätsschutz (Identity Protection Mode) auch für die SSL-Verhandlung gewährleistet (Vergleiche auch: Austausch-Modus, Main Mode).

Statischer Schlüssel [Link-Profile]

Der statische Schlüssel kann nur eingegeben werden, wenn vorher die Verschlüsselung aktiviert wurde. Der statische Schlüssel muss auf beiden Seiten der Verbindung identisch sein.

Mit dem statischen Schlüssel werden die Daten auf beiden Seiten der Verbindung gleichermaßen ent- und verschlüsselt. Der statische Schlüssel ist ein String mit 16 hexadezimalen Zahlen, die durch einen Punkt (.) getrennt sind.

Standard ist:

```
00.11.22.33.44.55.66.77.88.99.AA.BB.CC.DD.EE.FF
```

Ändern sie die Standardeinstellung auf beiden Seiten der Verbindung gleichermaßen ab.

IKE-Richtlinie [Link-Profile]

Die IKE-Richtlinie wird aus der Listbox selektiert. (Vorkonfiguriert befinden sich dort: “Pre-shared Key” und “RSA-Signatur”). In der Listbox werden namentlich alle IKE-Richtlinien aufgeführt, die bei der IPSec-Konfiguration angelegt wurden (siehe: Konfiguration / IKE-Richtlinie)

automatischer Modus: In diesem Fall kann die Konfiguration der IKE-Richtlinie über die IPSec-Konfiguration entfallen.

Pre-shared Key: Diese vorkonfigurierte Richtlinie kann ohne PKI-Unterstützung genutzt werden (Access Server / VPN Gateway). Beidseitig wird der gleiche Pre-shared Key verwendet.

RSA-Signatur: Diese vorkonfigurierte Richtlinie kann nur mit PKI-Unterstützung eingesetzt werden (Secure Server). Als zusätzliche, verstärkte Authentisierung ist der Einsatz der RSA-Signatur nur sinnvoll unter Verwendung einer Smart Card oder eines Soft-Zertifikats.

IPSec-Richtlinie [Link-Profile]

Die IPSec-Richtlinie wird aus der Listbox selektiert. (Vorkonfiguriert befinden sich dort: “ESP AES-3DES-MD5"). In der Listbox werden nament-

lich alle IPSec-Richtlinien aufgeführt, die bei der IPSec-Konfiguration angelegt wurden (siehe: **Konfiguration / IPSec-Richtlinie**)

automatischer Modus: In diesem Fall kann die Konfiguration der IKE-Richtlinie über die IPSec-Konfiguration entfallen.

Austausch-Modus [Link-Profile]

Der Austausch-Modus bestimmt wie der Internet Key Exchange vonstatten gehen soll. Zwei unterschiedliche Modi stehen zur Verfügung, der Main Mode, auch Identity Protection Mode und der Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch deren Verschlüsselung.

Main Mode: Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden – daher auch Identity Protection Mode.

Aggressive Mode: Im Aggressive Mode gehen nur drei Meldungen über den Kontrollkanal, wobei nichts verschlüsselt wird.

Zertifikats-Überprüfung [Link-Profile]

Die Zertifikats-Überprüfung ist nur dann wirksam, wenn sie für das lokale System des Secure Servers eingestellt wurde!

Aktivieren Sie im Konfigurationsbaum unter “Lokales System / Restriktionen” unbedingt die Funktion **Zugang nur mit konfigurierter Zertifikats-Überprüfung zulassen**, wenn Zertifikate für die Kommunikation eingesetzt werden.

Pro Link-Profil des Secure Servers kann vorgegeben werden, welche Einträge in einem von der Gegenstelle (Secure Client) eingehenden Zertifikat vorhanden sein müssen.

Nur wenn die hier definierten Einträge mit den Einträgen des eingehenden Zertifikats übereinstimmen, wird das Zertifikat mit dem Link-Profil gekoppelt und der Benutzer dieses Zertifikats erhält Zugang zum Secure Server.

Konventionen:

– Der Name kann mit einer Wildcard abgeschlossen werden. z. B. “nc*.
– Es können mehrere Einträge pro Zertifikatsinhalt angegeben werden. Trennzeichen ist das Semikolon “;”. Z. B. “Vertieb;support” oder “vertr*;supp*”
– Groß- und Kleinschreibung werden unterschieden.

Je nach PKI-Umgebung können eindeutige Einträge des eingehenden Zertifikats ausgewählt bzw. kombiniert werden. Folgende Zertifikatseinträge werden angeboten, um mit der Zertifikats-Überprüfung jeweils eindeutig ein einzelnes Zertifikat zu filtern – oder aber die Benutzer von Zertifikaten (auch mehrere) diesem Link-Profil zuzuordnen:

Seriennummer [Link-Profile]

Optional kann zusätzlich zum dynamischen Schlüsselaustausch die Seriennummer des Zertifikats der Gegenstelle bei Session-Beginn abgefragt werden. Tragen Sie dazu die Seriennummer des Zertifikats der Gegenstelle hier ein. Bitte achten Sie dabei unbedingt auf Groß-, Kleinschreibung und Kommasetzung.

Die Zertifikats-Seriennummer kann direkt von einer Chipkarte eingelesen werden. Hinter dem Eingabefeld “Zertifikats-Seriennummer” befindet sich ein Button. Dieser öffnet einen Dialog, der den Kartenleser und die Zertifikatsnummer abfragt. Wird daraufhin der “Weiter” Button betätigt, wird das Zertifikat ausgelesen und anschließend die Seriennummer im Eingabefeld eingetragen.

Hat ein Benutzer mehrere Zertifikate oder ein verlängertes Zertifikat, so können die zugehörigen Seriennummern durch Semikolon “;” getrennt per Hand angegeben werden. Auf diese Weise kann der Benutzer alle seine Zertifikate einsetzen.

Wenn das Feld leer bleibt, wird die Seriennummer ignoriert und alle Zertifikate werden akzeptiert.

Die Inhalte von Zertifikaten, die bei der Authentisierung abgelehnt wurden, werden in der Statistik unter “Ungültige empfangene Zertifikate” angezeigt.

Common Name (CN) [Link-Profile]

Werden mehrere Common Names durch Semikolon “;” getrennt angegeben, und kein weiteres eindeutiges Zertifikatsmerkmal, so kann das Link-Profil von allen jeweiligen Benutzern der angegebenen Common Names genutzt werden. Die Attributtypen für Zertifikatseinträge werden ohne das Kürzel (cn=) eingetragen.

E-Mail [Link-Profile]

Mehrere E-Mail-Adressen können durch Semikolon ";" getrennt angegeben werden. Wird ohne das Kürzel (email=) der Attributtypen für Zertifikatseinträge eingetragen.

Certificate Unique ID [Link-Profile]

Dies ist eine Zertifikats-Erweiterung, die von der Zertifizierungsstelle auf Anfrage vergeben wird und absolut eindeutig für ein Zertifikat ist. Mehrere dieser Erweiterungen können durch Semikolon ";" getrennt angegeben werden, sodass mehrere Zertifikate mit diesem Link gekoppelt werden.

Abteilung (OU) [Link-Profile]

Bezeichnet die Firmenabteilung (ou= Organisation Unit) des Zertifikatsinhabers und wird ohne das Kürzel (ou=) der Attributtypen für Zertifikatseinträge eingetragen.

Bei mehreren "ou-Einträgen" im Zertifikat, wird der letzte Eintrag zur Verifikation herangezogen.

User Principal Name (UPN)

Der User Principal Name besteht aus Anmeldename@Domain-Name.

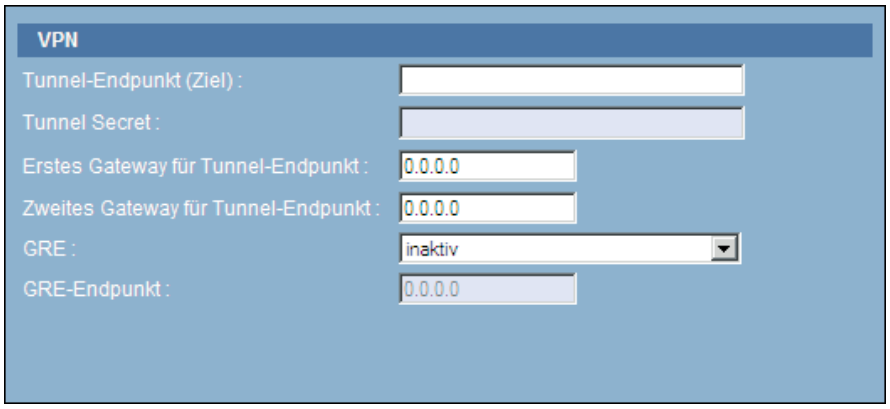
Hardware-Zertifikat (CN) [Link-Profile]

Findet die Einwahl an das Gateway von einem Rechner aus statt, der über ein Hardware-Zertifikat identifiziert wird, so kann hier der Common Name dieses Hardware-Zertifikats eingetragen werden, um erst nach seiner Überprüfung einen Verbindungsaufbau von diesem Rechner zu diesem Gateway zuzulassen oder gegebenenfalls abzulehnen.

Wird der Common Name des Hardware-Zertifikats nicht eingetragen, so hat es keinen Einfluss auf die Authentisierung.

VPN [Link-Profile]

Diese Parameter werden benötigt, wenn zwischen der Gegenstelle und dem VPN Gateway ein Tunnel (VPN) mit diesem Link-Profil aufgebaut werden soll.



Tunnel-Endpunkt (Ziel) [Link-Profile]

Dies ist die IP-Adresse des Tunnel-Endpunkts auf der Remote-Seite, wenn dieses VPN Gateway die Verbindung zum remote VPN Gateway aufbaut (siehe auch: Lokales System / VPN / Tunnel-Endpunkt (lokal)).

Für eingehende Verbindungen kann die Standardeinstellung “0.0.0.0" beibehalten oder die IP-Adresse gelöscht werden.

Ist dieses Gateway Teil eines HA-Systems, das einen dynamischen VPN-Endpunkt (DVE) nutzt, so kann hier keine IP-Adresse eingegeben werden.

Tunnel Secret [Link-Profile]

“Tunnel Secret” ist ein Passwort, das für den L2TP-Tunnelaufbau benötigt wird. Nur wenn dieses Passwort beim VPN Gateway und der Gegenseite übereinstimmt, wird der Tunnel aufgebaut.

Das Passwort kann bis zu 16 Zeichen lang sein.

Erstes / Zweites Gateway für Tunnel-Endpunkt [Link-Profile]

Dieser Parameter hat nur Bedeutung für ausgehende Verbindungen von Client Gateways. Es wird laufend überprüft, ob der Tunnel-Endpunkt über die LAN-Verbindung erreichbar ist. Ist dies nicht der Fall, wird über einen Backup Link die Verbindung zum Internet hergestellt. Ist der Tunnel-Endpunkt wieder über LAN erreichbar, wird der Backup Link wieder abgeschaltet.

Hier tragen Sie die IP-Adresse des Gateways (next Hop Router) ein, worüber der konfigurierte Tunnel-Endpunkt im Backup-Fall geroutet werden soll. Dieser Hop Router kann sowohl im LAN als auch im Internet (z. B. ISP Gateway) vorgeschaltet sein.

GRE [Link-Profile]

Die Generic Router Encapsulation (GRE) kann nur genutzt werden, wenn die Gegenstelle ebenfalls GRE unterstützt. Hier bestimmen Sie, ob für dieses Link-Profil GRE genutzt werden soll (aktiv) oder nicht (nicht aktiv).

Das IP-Packet wird vor dem Senden mit einem GRE-Header verpackt, am GRE-Endpunkt wieder entpackt und erst dann “normal” weiter geroutet.

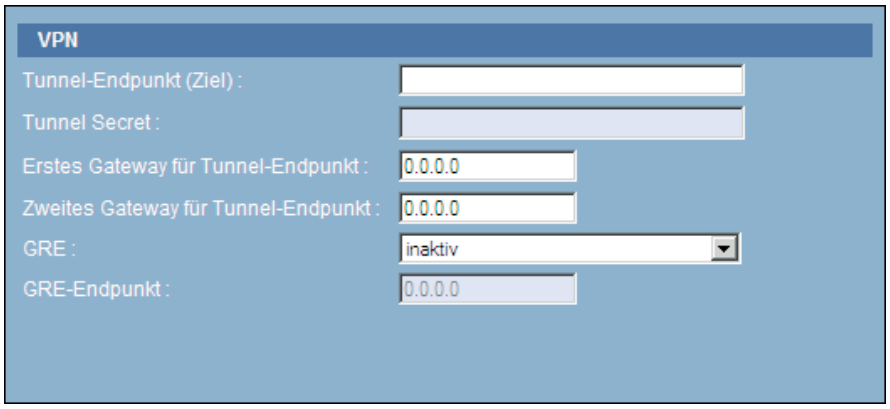
GRE-Endpunkt [Link-Profile]

Sofern GRE genutzt wird können Sie die IP-Adresse des GRE-Endpunkts der Gegenstelle hier eintragen.

Belassen Sie die Standard-Einstellung “0.0.0.0", so wird für dieses Link-Profil automatisch der GRE-Endpunkt aus den Einstellungen zu ”Lokales System / VPN" genutzt.

HA-Unterstützung [Link-Profile]

Die NCP HA Services arbeiten mit einem DVE (Dynamic VPN Endpoint). Sie können zum Lastausgleich (Loadbalancing) oder zur Ausfallsicherung (Failsafe) eines Virtual Private Networks mit zwei VPN Gateways genutzt werden. Mit DVE wird, je nach Konfiguration im DVE Manager, sichergestellt, dass kein Engpass beim Tunnelaufbau auftritt. Je nach Lastaufkommen wird zum Tunnelaufbau zwischen zwei Tunnel-Endpunkten gewechselt.



Um einen DVE nutzen zu können, benötigen Sie zwei VPN Gateways, ausgestattet mit HA Server Software. Die HA Server müssen offizielle IP-Adressen besitzen.

Da die IP-Adresse des Tunnel-Endpunkts dynamisch ermittelt wird, braucht der lokale Tunnel-Endpunkt in der Konfiguration des VPN Gateways nicht eingetragen zu werden. (Siehe: Link-Profile / VPN)

DVE (Dynamischer VPN-Endunkt) [Link-Profile]

Um einen DVE nutzen zu können, muss die Funktion hier aktiviert werden und ein Tunneling-Protokoll für dieses Link-Profil definiert sein. Standardeinstellung ist “inaktiv”.

Erster / Zweiter HA-Server [Link-Profile]

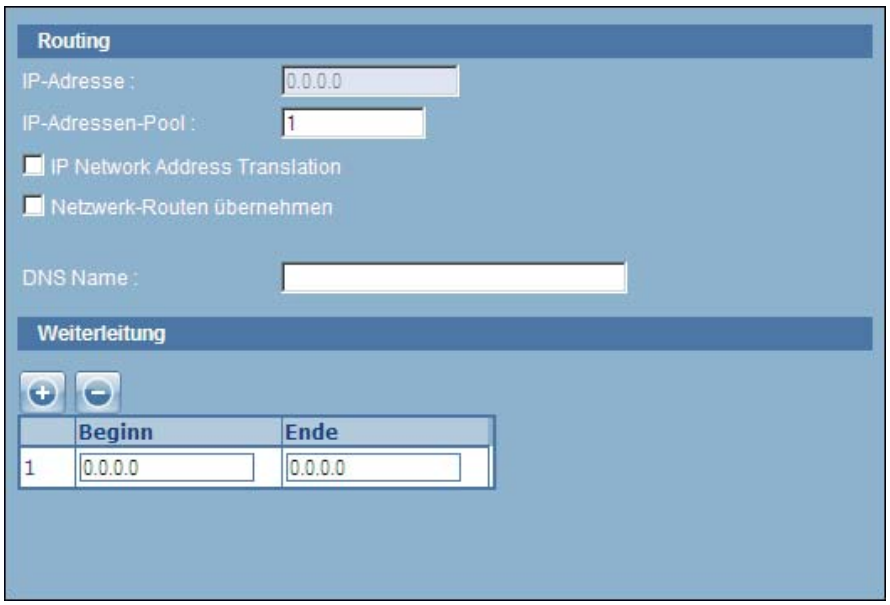
Geben Sie hier die offiziellen IP-Adressen oder die DNS-Namen der HA Server ein.

DVE Secret [Link-Profile]

“DVE Secret” ist ein Passwort, das für die Verbindung zwischen einem DVE Client und HA-Server benötigt wird. Nur wenn dieses Passwort bei beiden HA-Servern und dem Client übereinstimmt, wird die Verbindung aufgebaut. Wenn Sie das Passwort hier eintragen, stimmt es bei beiden HA Servern überein. Das Passwort kann bis zu 16 Zeichen lang sein.

Routing [Link-Profile]

In diesem Parameterfeld werden die link-spezifischen Einstellungen für das Routing vorgenommen.



IP-Adresse [Link-Profile]

Bei eingehenden Verbindungen ist dies die (WAN) IP-Adresse der über diesen Link kommunizierenden Remote-Seite. Diese IP-Adresse wird der Gegenstelle in der PPP-Verhandlung übermittelt.

Bei abgehenden Verbindungen ist dies die (WAN) IP-Adresse der Gegenstelle. (Bei wechselnden, unbekannten IP-Adressen muss IP Network Address Translation eingestellt sein, siehe unten).

(Zu eingehenden und abgehenden Verbindungen beachten Sie bitte die “Richtung”, bestimmt unter “Link-Profile / Grundeinstellungen”.)

Wenn eine feste IP-Adresse genutzt werden soll, muss diese Adresse mit der auf der Remote-Seite übereinstimmen.

Bitte beachten Sie, dass diese Adresse aus dem Adress-Bereich des WAN stammen muss und nur einmal vorkommen darf, d. h. jeder Link benötigt eine eigene IP-Adresse. Auch darf diese IP-Adresse nicht aus dem Adress-Bereich der Pools stammen.

IP Adressen-Pool [Link-Profile]

Sie können statt einer festen IP-Adresse dem Link-Profil auch einen IP Adressen-Pool zuweisen. Diesen Pool müssen Sie vorher definiert haben (siehe: Konfiguration / Domain-Gruppen). Hier tragen Sie die Nummer des IP-Adressen-Pools ein.

IP Network Address Translation [Link-Profile]

Die meisten Internet Service Provider nutzen die Network Address Translation zur Kommunikation. Wenn IP Network Address Translation aktiviert ist, werden alle übertragenen Frames mit der ausgehandelten (PPP) IP-Adresse verschickt. Wenn Sie IP Network Address Translation nutzen, können Sie jede beliebige IP-Adresse in Ihren Systemeinstellungen konfigurieren, da die Software die ausgehandelte (PPP) IP-Adresse in ihre systemeigene übersetzt. Die DHCP-Wartezeit wird in diesem Fall ignoriert.

Wenn die Checkbox angeklickt ist, wird Network Address Translation für diesen Link aktiviert.

Netzwerk-Routen übernehmen [Link-Profile]

IP-Netz-Adressen, die sich hinter einem Filial-Router befinden, der sich zu diesem Gateway verbindet, werden automatisch ausgewertet, wenn diese Funktion aktiviert wird. Das heißt, für diesen Gateway-Gateway-Link müssen keine statischen Routen mehr gesetzt werden, da die Netzwerk-Routen automatisch übernommen werden.

Bitte beachten Sie, dass dieser Parameter nur bei IPSec-Verbindungen funktionsfähig ist.

DNS Name [Link-Profile]

Die Funktion des hier einzutragenden Namens ist Richtungsabhängig!

Bei ausgehenden Verbindungen für Provider-Benutzer wird dieser Name des Gateways an einen DynDNS Server zur Namensauflösung geschickt. Dies ist dann der Fall, wenn das VPN Gateway keine feste offizielle IP-Adresse besitzt. Das Gateway erhält bei jeder Einwahl eine neue IP-Adresse vom Internet Service Provider. Die eindeutige Identifikation durch den Secure Client kann nicht mehr über eine im Telefonbuch des Clients fest zu konfigurierende IP-Adresse erfolgen. Statt dessen wird dem VPN Gateway vom Administrator hier der DNS Name zugeordnet, der am Dyn DNS Server in die jeweils aktuelle IP-Adresse aufgelöst wird. Auf Seiten des Clients wird statt der (festen) IP-Adresse für den Tunnel-Endpunkt (siehe am Client: Profil-Einstellungen / Tunnel-Parameter) dieser, beim Dyn DNS Service Provider hinterlegte DNS Name eingetragen (siehe: Konfiguration / Lokales System / DynDNS).

Bei eingehenden Verbindungen für VPN-Benutzer ist dies der für den Client zu vergebende Name, der mit der jeweils aktuellen IP-Adresse, die der Client aus dem Firmennetz erhält, an den DDNS Server zur Namensauflösung weitergeleitet wird (siehe: Konfiguration / Domain-Gruppen / DDNS).

Weiterleitung [Link-Profile]

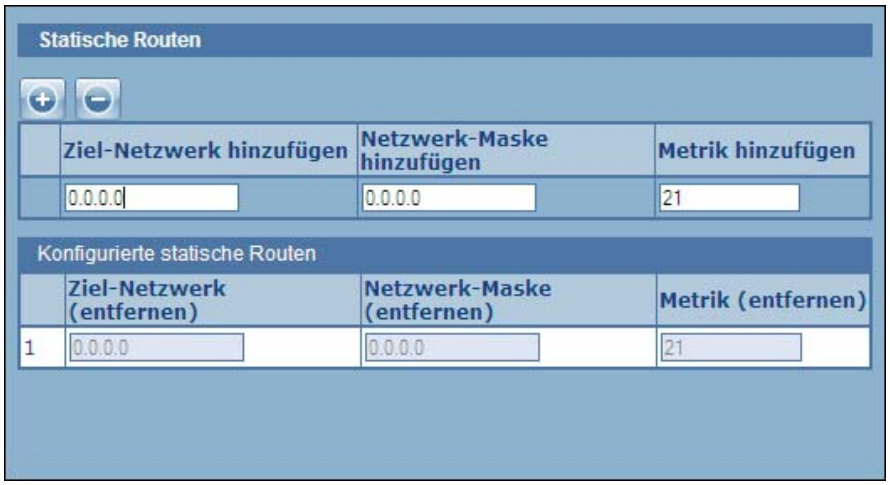
Nach Klick auf den Plus-Button können die Source IP-Adressen, für die diese linkspezifische Weiterleitung ausgeführt werden soll, eingetragen werden. Diese linkspezifische Tunnelweiterleitung erfolgt zu der Zieladresse, die mit diesem ausgehenden Link unter “VPN” konfiguriert wurde.

Eine gruppenbezogene Weiterleitung wird in der Konfigurationsgruppe “Domain-Gruppen” unter “Allgemein” als ausgehender Link konfiguriert.

Bitte beachten Sie, dass die linkspezifische Weiterleitung automatisch mit höherer Priorität behandelt wird, sofern gleichzeitig eine gruppenspezifische Weiterleitung konfiguriert sein sollte.

Statische Routen [Link-Profile]

Statische Routen werden immer dann gesetzt, wenn das bestimmte Zielnetz nicht über das Default-Gateway erreicht werden kann. Statische Routen werden nur für ausgehende Verbindungen genutzt. Dabei muss die IP-Adresse des für diese Verbindung genutzten Links eine feste IP-Adresse sein (siehe: **Link-Profile / Routing / IP-Adresse**).



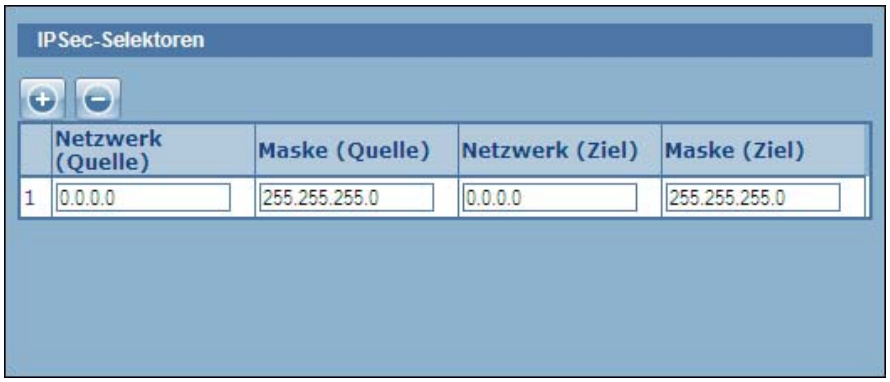
Konfiguration [Statische Routen]

Wenn Sie eine feste IP-Adresse für dieses Link-Profil unter “Link-Profile / Routing” eingegeben haben, können Sie hier das Ziel-Netzwerk, die Netzwerk-Maske und die Metrik eintragen.

Mit Klick auf den Plus-Button werden die Daten in die Liste der konfigurierten statischen Routen übernommen.

Wird eine konfigurierte statische Route markiert, kann sie mit dem Minus-Button gelöscht werden.

IPSec-Selektoren



Konfiguration bei Gateway-Gateway-Kopplungen über IPSec

Für Gateway-Gateway-Kopplungen über IPSec, wobei hinter dem Gateway für ausgehende Verbindungen (GW1) und hinter dem Gateway für eingehende Verbindungen (GW2) mehrere Netze installiert sind, ist bei der Konfiguration für GW1 folgendes zu beachten:

– Unter Link-Profile muss ein neuer Link für ausgehende Verbindungen angelegt werden. In den “Grundeinstellungen” der “Link-Profile” muss der Status auf “aktiv” gestellt sei, als Richtung muss “ausgehend” definiert und als Verbindungsmedium muss “IPSec” gewählt sein.

– Je nach den Erfordernissen der IPSec-Verbindungen werden unter Link-Profile die Parameter gesetzt.

– Im Link-Profil unter “VPN” muss der “Tunnel-Endpunkt (Ziel)” mit der “IP-Adresse IPSec Gateway” unter “IPSec Optionen” übereinstimmen.

– Sollen mehrere bestimmte Netze hinter GW1 und GW2 miteinander gekoppelt werden, so können die Netzwerk-Parameter als IPSec-Selektoren eingegeben werden.

Netzwerk (Quelle) [IPSec-Selektoren]

Dieses Parameterfeld ist nur von Bedeutung, wenn die Gegenstelle ein IPSec Gateway (Secure Server) ist und sich hinter diesem Filial-Gateway genau zu bestimmende Netze befinden, von denen aus der Zugriff auf die Gegenstelle stattfinden soll. Sollen alle Netze zugelassen werden, so kann die Netz-Adresse 0.0.0.0 belassen werden.

Soll nur ein bestimmtes Netz zugelassen werden, so muss hier dessen IP-Adresse eingetragen werden.

Maske (Quelle) [IPSec-Selektoren]

Dieses Parameterfeld ist nur von Bedeutung, wenn die Gegenstelle ein IPSec Gateway (Secure Server) ist und sich hinter diesem Filial-Gateway genau zu bestimmende Netze befinden, von denen aus der Zugriff auf die Gegenstelle stattfinden soll. Sollen alle Netze zugelassen werden, so kann die Netz-Adresse 0.0.0.0 belassen werden.

Soll nur ein bestimmtes Netz zugelassen werden, so muss hier dessen Netz-Maske als 255.255.255.255 (Standard-Maske für private IP-Netze) eingetragen werden.

Netzwerk (Ziel) [IPSec-Selektoren]

Dieses Parameterfeld ist nur von Bedeutung, wenn die Gegenstelle ein IPSec Gateway (Secure Server) ist, hinter dem sich dezidiert zu erreichende Netze befinden. Sollen alle Netze erreicht werden, so kann die Netz-Adresse 0.0.0.0 belassen werden.

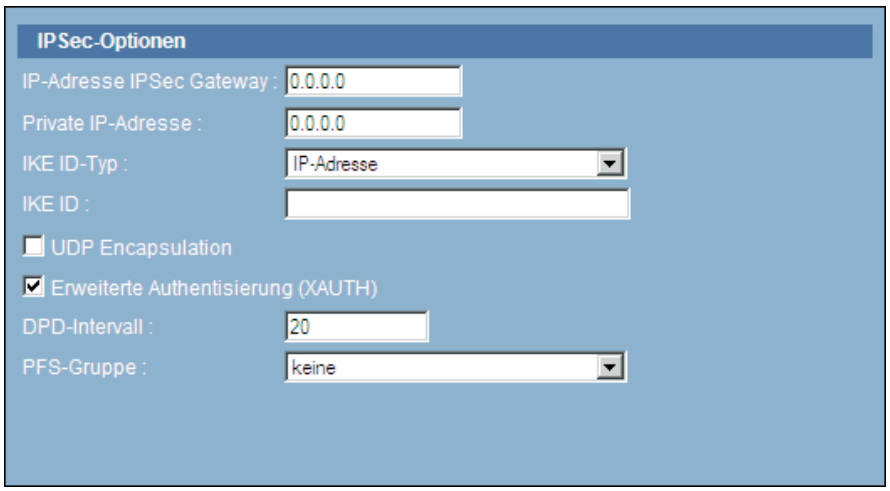
Soll ein bestimmtes Netz erreicht werden, so muss hier dessen IP-Adresse eingetragen werden.

Maske (Ziel) [IPSec-Selektoren]

Dieses Parameterfeld ist nur von Bedeutung, wenn die Gegenstelle ein IPSec Gateway (Secure Server) ist, hinter dem sich dezidiert zu erreichende Netze befinden. Sollen alle Netze erreicht werden, so kann die Netz-Adresse 0.0.0.0 belassen werden.

Soll ein bestimmtes Netz erreicht werden, so muss hier dessen Netz-Maske als 255.255.255.255 (Standard-Maske für private IP-Netze) eingetragen werden.

IPSec-Optionen



Zieladresse IPSec Gateway [IPSec-Optionen]

Dieses Parameterfeld ist nur von Bedeutung, wenn eine IPSec-Verbindung über L2TP-Tunneling konfiguriert wurde und das IPSec Gateway der Gegenstelle (hinter dem sich die zu addressierenden Netze befinden) eine andere IP-Adresse besitzt als das VPN Ziel-Gateway für die darunter liegende L2TP-Verbindung. Dessen IP-Adresse wird unter Link-Profile im Parameterfeld “VPN” als “Tunnel-Endpunkt (Ziel)” eingetragen.

Vergleiche auch die Beschreibung unter:

Konfiguration bei Gateway-Gateway-Kopplungen über IPSec

Private IP-Adresse

Dieser Parameter ist nur bei einer Gateway-Gateway-Koppelung über IPSec von Bedeutung.

Viele IPSec Gateways haben die Möglichkeit, der Gegenstelle eine private IP-Adresse zuzuweisen. Mit dieser Adresse erscheint die Gegenstelle dem IPSec Gateway im Firmennetz. Diese private IP-Adresse kann der Gegenstelle während der IKE-Verhandlung auch dynamisch zugewiesen werden, wenn sie den IKE-Konfigurations-Modus (Config Mode) unterstützt. Unterstützt die Gegenstelle den IKE-Konfigurations-Modus (Config Mode) nicht, muss diese Adresse statisch konfiguriert werden. Wenn ein Gateway die Nutzung privater IP-Adressen nicht unterstützt, muss die private mit der offiziellen IP-Adresse übereinstimmen.

Folgende Einträge sind möglich:

– 255.255.255.255
(Standard bei GW-GW-Kopplung)
In diesem Fall wird die vom ISP zugewiesene IP-Adresse als private IP-Adresse ohne Einschränkung akzeptiert. Das Ziel-Gateway muss den IKE-Konfigurations-Modus (Config Mode) nicht unterstützten.

– 0.0.0.0
In diesem Fall erwartet der Client, dass ihm vom Gateway eine private IP-Adresse dynamisch zugewiesen wird und versucht sie über den IKE-Config Mode zu erhalten. Dies kann nur funktionieren, wenn das IPSec Gateway den IKE-Config Mode unterstützt.

– Andere Werte
In diesem Fall verwendet das Gateway die konfigurierte IP-Adresse (ohne IKE-Config Mode).

IKE ID-Typ

Bei “IPSec-Tunneling” (native IPSec) müssen diese Parameter “IKE ID-Typ” und “IKE ID” mit denen der Gegenstelle übereinstimmen. Für den “IKE ID-Typ” stehen folgende Alternativen zur Auswahl:

– IP Address
– Fully Qualified Domain Name
– Fully Qualified Username
– IP Subnet Address
– ASN1 Distinguished Name
– ASN1 Group Name
– Free String used to identify Groups

IKE ID

Entsprechend dem “IKE ID-Typ” muss die zugehörige “IKE ID” als String eingetragen werden.

UDP Encapsulation

Sind z. B. an der zentralen Firewall die Standard-Ports für die IPSec-Kommunikation bereits für andere IPSec-Lösungen freigeschaltet (IPSec mit UDP: Port 4500, für IPSec ohne UDP: Port 500), so kann für die NCP IPSec-Lösung mit dieser Option ein beliebig anderer Port für die IPSec-Kommunikation definiert werden, wenn UDP (User Datagram Protocol) Encapsulation genutzt wird.

Diese Funktion ist nur für ausgehende Verbindungen eines Client Gateways nutzbar.

Global wird der Port definiert unter “Konfiguration / Lokales System / VPN / **Alternativer IKE-Port**”. Dieser Port wird mit UDP Encapsulation sowohl für die IKE-Verhandlung als auch für die IPSec-Verhandlung genutzt und muss in der Client-Konfiguration im Telefonbuch unter “IPSec-Optionen / **Benutze UDP Encapsulaion**” ebenso konfiguriert sein.

Ebenso muss dieser Port dann an der Firewall freigeschaltet werden.

Erweiterte Authentisierung (XAUTH)

Wird für eine ausgehende Verbindung “IPSec-Tunneling” genutzt, so kann die Authentisierung über Extended Authentication (XAUTH Protokoll, Draft 6) erfolgen. Ist dies der Fall, so können zusätzlich zum pre-shared Key noch folgende Parameter gesetzt werden:

Benutzer = Benutzername des IPSec-Benutzers

Passwort = Kennwort des IPSec-Benutzers

Siehe dazu **Benutzer und Passwort für ausgehende Verbindungen** unter “Authentisierung”.

DPD-Intervall

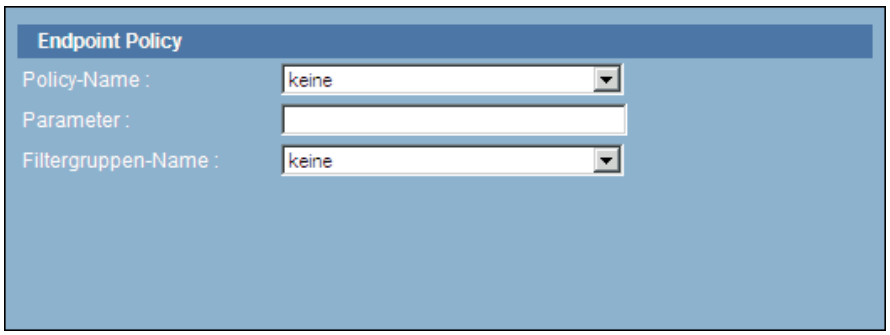
DPD (Dead Peer Detection) wird automatisch im Hintergrund ausgeführt, sofern dies die Gegenstelle unterstützt. Mit DPD (Dead Peer Detection) wird die Gegenstelle aktiv (nach eingestelltem Zeitintervall in Sekunden) unabhängig vom tatsächlichen Nutzdatenverkehr “angepingt” und der Tunnel abgebaut, wenn keine Antwort erfolgt oder der Timeout abgelaufen ist (unabhängig vom Datenaufkommen).

Mit einem größeren Intervall werden weniger häufig Pakete geschickt, die prüfen ob die Gegenstelle noch erreichbar ist und das Datenaufkommen verringert.

PFS-Gruppe

Mit Auswahl einer der angebotenen Diffie-Hellman-Gruppen wird für die ausgehende IPSec-Verbindung festgelegt, ob ein kompletter Diffie-Hellman-Schlüsselaustausch (PFS, Perfect Forward Secrecy) in Phase 2 zusätzlich zur SA-Verhandlung stattfinden soll. Standard ist “keine”.

Endpoint Policy [Link-Profile]



Policy-Name [Link-Profile]

Wählen Sie aus der Liste der Policy Rules (siehe auch: Lokales System / Endpoint Policies) den Namen der Policy, die für diesen Link gelten soll.

Wird in dieses Feld kein Name eingetragen, so wird keine Endpoint Policy ausgeführt.

Parameter [Link-Profile]

Hier kann eine Konstante für diesen Link individualisiert werden, indem (z. B.) die Seriennummer des Client PCs eingetragen wird. Diese allgemeine Konstante wird mit der Richtlinie zur Verfügung gestellt und muss als “POLICY_PARAM1" im Policy Script verwendet werden bzw. enthalten sein.

Beispiel:

```
if PCSERIALNUMBER = POLICY_PARAM1 then ...
```

Filtergruppe [Link-Profile]

Hier wird die Filtergruppe gewählt, die gelten soll, wenn die Policy eingeschaltet ist. Diese Filtergruppe schränkt den Bereich ein, auf den der Client Zugriff haben soll (z. B. auf einen Bereich, auf dem nur ein Update zur Verfügung gestellt wird).

Wird die Policy vom Client erfüllt, so wird der komplette Bereich freigeschaltet, der durch die Filtergruppe definiert wurde, deren Name in den Grundeinstellungen für die Link-Profile angegeben wurde. Siehe “Konfiguration / Link-Profile / Grundeinstellungen / **Filtergruppe**”.

SSL VPN [Link-Profile]

Die linkspezifische SSL VPN-Konfiguration hängt von der Konfiguration des SSL VPN Gateways ab. Dessen Einstellungen werden im Konfigurationszweig **SSL VPN** (siehe weiter unten) festgelegt.

SSL VPN-Profil

Mit dem Profil-Namen definieren Sie, welche Web Proxy- und welche Port-Forwarding-Anwendungen für dieses Link-Profil, das den Benutzer-Zugang zum Gateway regelt, nutzbar sein sollen.

Login nur mit Zertifikat

An dieser Stelle wird die zertifikatsbasierte Authentisierung linkspezifisch (pro Anwender) eingestellt. Die Aktivierung dieser Funktion hat nur Bedeutung, wenn in der Listener-Konfiguration keine zertifikatsbasierte Authentisierung eingestellt wurde.

Filternetze

Hier können IP-Netze oder Netzbereiche zusammengestellt werden, für die der gleiche Filter gelten soll.

Konfiguration der Filternetze

Die hier definierten Filternetze können unter Konfiguration / Filter selektiert werden.

Name [Filternetze]

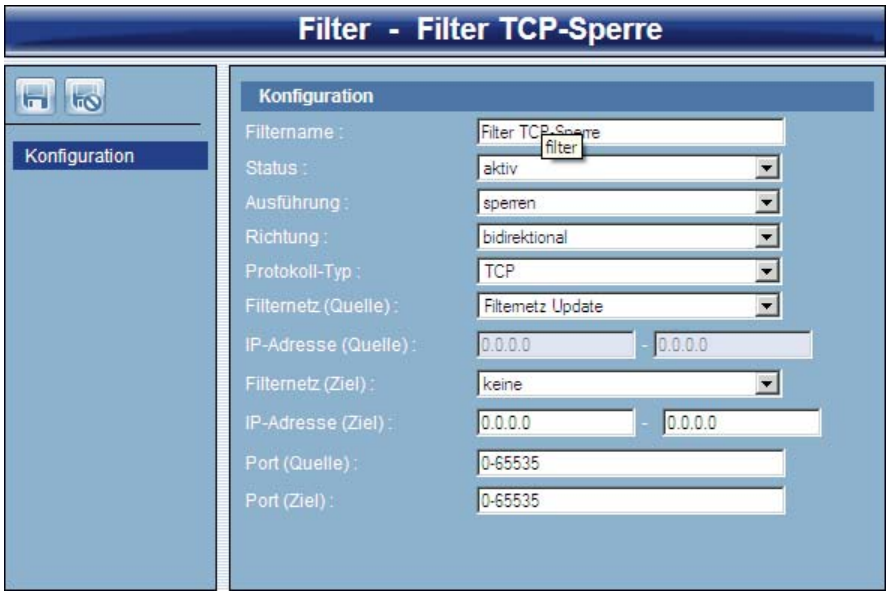
Jedes Filternetz erhält einen eigenen Namen, unter dem es in der Filter-Konfiguration ausgewählt werden kann.

Bereich [Filternetze]

Anstatt pro Netzbereich jeweils eine Filtertregel erstellen zu müssen, können diese unter einem gemeinsamen Namen zusammengestellten “Filternetze” alternativ als “Filternetz (Quelle oder Ziel)” in einem einzigen Filter selektiert werden.

Filter

Filter die hier konfiguriert werden, können anschließend in einer Filtergruppe kombiniert werden.



Konfiguration der Filter

Die Link-Filter können für jeden IP-Protokoll-Typ dynamisch konfiguriert werden, d. h. ein Anhalten der Server Software oder ein Neustart der Dienste ist nicht nötig.

Filtername [Filter]

Die hier konfigurierten Filter werden später über die Zusammenstellung der “Filtergruppe” (siehe: unten) über ihren Filternamen einem Link zugeordnet.

Tragen Sie den gewünschten Filternamen ein.

Status [Filter]

Mit dem Status, “aktiviert” oder “nicht aktiviert”, bestimmen Sie, ob der Filter für einen Link genutzt wird oder nicht.

Ausführung [Filter]

Je nach Ausführung des Filters können die Frames zur Übertragung über das WAN zugelassen werden oder von der Übertragung ausgeschlossen werden.

zulassen: Die Frames, die durch die weiteren Einstellung beschrieben werden, werden zur Übertragung über den Link, der diesem Filter zugeordnet wird, zugelassen.

ausschließen: Die Frames, die durch die weiteren Einstellung beschrieben werden, werden von der Übertragung über den Link, der diesem Filter zugeordnet wird, ausgeschlossen.

Richtung [Filter]

Der Filter kann für eingehende oder abgehende Verbindungen und deren Datenstrom wirksam sein.

ausgehend: Dieser Filter ist nur wirksam für die Frames, die durch die weiteren Einstellungen beschrieben werden und vom lokalen Netz (LAN) über den NAS in das WAN übertragen werden.

eingehend: Dieser Filter ist nur wirksam für die Frames, die durch die weiteren Einstellungen beschrieben werden und vom WAN über den NAS in das lokale Netz (LAN) übertragen werden sollen.

Aus Sicherheitsgründen sind die meisten Filter nur für eingehende Frames wirksam.

Protokoll-Typ [Filter]

Mit Hilfe der Einstellungen eines flexiblen IP-Filters wird der Notwendigkeit Rechnung getragen, wichtige LAN-Datenbestände vor ungewünschtem Zugriff zu bewahren oder sie im Netzwerk zu verstecken. Der IP-Filter kann auf bestimmte IP-Protokoll-Typen eingestellt werden:

alle: alle IP-Protokoll-Typen

ICMP: Internet Control Message Protocol

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

ESP: Encapsulating Security Payload

Filternetz (Quelle)

Wurden über die “Filternetze” mehrere Netzbereiche unter einem gemeinsamen Namen zusammengefasst, so kann diesem Filter durch Selektion des Filternetz-Namens dieser Netzbereich als Quell-IP-Adresse zugeeordnet werden.

IP-Adresse (Quelle) [Filter]

Je nachdem, worauf der Filter angewendet werden soll, können Sie die Adresse eines Source Hosts oder den Adress-Bereich eines Netzwerks, aus dem der zu routende Frame stammt, spezifizieren. Dabei ist die IP-Adresse (Quelle) immer die IP-Adresse, die dem Router über die Herkunft des zu routenden Frames Auskunft gibt.

Soll der Filter auf mehrere Netzbereiche angewendet werden, so können diese unter “Filternetze” konfiguriert werden.

Alle Adressen: Wenn Sie die Standard-Adresse “0.0.0.0" belassen, wird der Filter auf alle IP-Adressen angewendet.

Adress-Bereich: Den Adress-Bereich, worauf der Filter angewendet werden soll, bestimmen Sie mit der ersten (von) und der letzten (bis) IP-Adresse dieses Bereichs.

Einzelne IP-Adresse: Die einzelne IP-Adresse, worauf der Filter angewendet werden soll, bestimmen Sie, indem Sie die gewünschte Adresse in beide Felder der Source IP-Adresse (von, bis) eintragen.

Port (Quelle) [Filter]

Dieser Eintrag spezifiziert den IP-Port (Service) der Herkunfts-Adresse, die Sie unter IP-Adresse (Quelle) definiert haben.

Für einen bestimmten Service-Typ geben Sie die Nummer nach RFC 1340 ein.

Für alle Services belassen Sie den Standardeintrag “0".

Mit Klick auf den Auswahl-Button erhalten Sie eine Übersicht über die Standard-Ports.

Statt eines einzelnen Ports können auch Port-Bereiche (max. 32) oder mehrere Ports angegeben werden. Z. B.: 22,80,44,1024-65535 (ohne Leerzeichen)

Filternetz (Ziel)

Wurden über die “Filternetze” mehrere Netzbereiche unter einem gemeinsamen Namen zusammengefasst, so kann diesem Filter durch Selektion des Filter-Netz-Namens dieser Netzbereich als Ziel-IP-Adresse zugeordnet werden.

IP-Adresse (Ziel) [Filter]

Je nachdem, worauf der Filter angewendet werden soll, können Sie als Ziel-Adresse einen Destination Host oder den Adress-Bereich eines Netzwerks, wohin der Frame geroutet werden soll, spezifizieren. Dabei ist die IP-Adresse (Ziel) immer die IP-Adresse, die dem Router über das Ziel des zu routenden Frames Auskunft gibt.

Soll der Filter auf mehrere Netzbereiche angewendet werden, so können diese unter “Filternetze” konfiguriert werden.

Alle Adressen: Wenn Sie die Standard-Adresse “0.0.0.0" belassen, wird der Filter auf alle IP-Adressen angewendet.

Adress-Bereich: Den Adress-Bereich, worauf der Filter angewendet werden soll, bestimmen Sie mit der ersten (von) und der letzten (bis) IP-Adresse dieses Bereichs.

Einzelne IP-Adresse: Die einzelne IP-Adresse, worauf der Filter angewendet werden soll, bestimmen Sie, indem Sie die gewünschte Adresse in beide Felder der Destination IP-Adresse (von, bis) eintragen.

Port (Ziel) [Filter]

Dieser Eintrag spezifiziert den IP-Port (Service) der Ziel-Adresse, die Sie unter IP-Adresse (Ziel) definiert haben.

Für einen bestimmten Service-Typ geben Sie die Nummer nach RFC 1340 ein.

Für alle Services belassen Sie den Standardeintrag “0".

Mit Klick auf den Auswahl-Button erhalten Sie eine Übersicht über die Standard-Ports.

Statt eines einzelnen Ports können auch Port-Bereiche (max. 32) oder mehrere Ports angegeben werden. Z. B.: 22,80,44,1024-65535 (ohne Leerzeichen)

Filtergruppen

Konfiguration der Filtergruppen

Allgemeine Vorgehensweise

Im Konfigurationsbaum können Sie unter Filtergruppe so viele Filter kombinieren, wie Sie benötigen. Die Filtergruppe speichern Sie unter einem eigenen Namen. Maximal können 1024 Filtergruppen angelegt werden. Die Filtergruppe ordnen Sie einem Link-Profil in den Grundeinstellungen zu. Eine Filtergruppe kann auch verschiedenen Links zugeordnet werden. Beachten Sie jedoch, dass einem Link nur eine Filtergruppe zugeordnet werden kann.

Funktionsweise von Filtergruppen, die einzelne Frames ausschließen

Wenn Sie einige wenige Frames vom Routing ausschließen wollen, werden Sie für diese Frames Filter anlegen, die aufgrund der darin definierten Eigenschaft des Frames, das Routing über diesen Link ausschließen. Diese Filter haben Sie unter einem jeweils eigenen Namen im Konfigurationsbaum unter “Filter” gespeichert. (Ihre Funktion ist das Zulassen oder Verweigern von Protokollen und Adressen. Normalerweise ist die Einstellung der Filter “Deny”.)

In der Filtergruppe sortieren Sie die Filter nach deren Restriktionen. Der Filter, der vorraussichtlich die meisten Frames vom Routing ausschließt, sollte an erster Stelle der Reihenfolge stehen, usw.

Wenn ein Frame das Gateway erreicht, durchläuft er die Liste der Filtergruppe für diesen Link sequentiell von oben nach unten. D. h. der erste Filter, der abgearbeitet wird, ist der der im Fenster “Ausgewählte Filter” in der ersten Zeile der Filtergruppe steht. Der nächste Filter, der aktiv wird, ist der in der zweiten Zeile, usw.

Der erste Filter in dieser Reihenfolge, der zu diesem Frame passt, wird angewendet. Alle in der Reihenfolge innerhalb der Filtergruppe nachgeordneten Filter werden im folgenden gar nicht mehr abgearbeitet und die Liste der Filtergruppe wird verlassen.

Nur wenn keiner der Filter auf den Frame passt, so dass er von keinem der Filter vom Routing ausgeschlossen wird, wird der Frame geroutet.

Eine neue Filtergruppe zusammenstellen

– Wählen Sie im Konfigurationsfenster “Filtergruppe” den Button “Neu / Einfügen”
– Vergeben Sie eine Bezeichnung als Filtergruppen-Name
– Belassen Sie den Status auf “aktiv”
– Markieren Sie einzeln per Maus, in der für die Filtergruppe gewünschten Reihenfolge, die Filter aus dem Fenster für “Verfügbare Filter”, die Sie der Filtergruppe zuordnen möchten: Ist der erste Filter markiert, klicken Sie ihn mit der Pfeiltaste “->” in das Fenster der selektierten Filter. Danach markieren Sie den zweiten Filter usf., bis zum letzten
– (Vergessen Sie nach der Kombination von “Permit”-Filtern nicht den letzten “Deny all”)
– Die Reihenfolge für “Ausgewählte Filter” können Sie noch korrigieren, wenn der in falscher Reihenfolge befindliche Filter markiert ist und Sie die Tasten mit Pfeil-auf und Pfeil-ab klicken. Aus der Filtergruppe können Sie einen Filter entfernen, indem Sie ihn in der Liste für “Ausgewählte Filter” markieren und die Pfeiltaste “<-” drücken.
– Speichern Sie die Filtergruppe

IKE-Richtlinien

Um die IPSec-Konfiguration für Clients zu erleichtern, wurden neue Optionen geschaffen, die es ermöglichen IPSec zu fahren ohne eine IKE- (Phase 1) oder IPSec-Richtlinie (Phase 2) vorzudefinieren.

Sobald am Client eingegeben wurde IKE-Richtlinie und/oder IPSec-Richtlinie "automatischer Modus", akzeptiert der Client die Richtlinie, die vom Gateway geschickt wird. Auf diese Weise wird IPSec genauso gehandhabt wie L2Sec: die Gegenstelle (VPN Gateway) legt die Parameter fest, die vom Initiator (Client) akzeptiert werden müssen.

Ist ein VPN Gateway ein Initiator (Client Gateway) gegenüber einem anderen VPN Gateway (aufbauendes Gateway), muss beim Initiator-Gateway des IPSec-Prozesses die entsprechende Einstellung vorgenommen werden. Diese Einstellungsmöglichkeiten befinden sich in den "Link-Profilen" unter "Security" (**Security-Modus IPSec**) bei den Parametern "IKE-Richtlinie und/oder IPSec-Richtlinie".

Konfiguration [IKE-Richtlinien]

Die Parameter in diesem Feld beziehen sich auf die Phase 1 des Internet Key Exchange (IKE) mit dem der Kontrollkanal für die SA-Verhandlung aufgebaut wird. Den IKE-Modus (Austausch-Modus / Exchange Mode), Main Mode oder Aggressive Mode, bestimmen Sie in den Parameterfeldern "Security" unter "Link-Profile".

Alle IKE-Richtlinien, die während der IPSec-Konfiguration angelegt werden, werden namentlich in einer Listbox aufgeführt.

Sofern IPSec für Remote Access eingesetzt wird, ordnen sie eine der IKE-Richtlinien im Parameterfeld "Security" unter "Link-Profile" dem jeweiligen Link zu.

Funktional unterscheiden sich zwei IKE-Richtlinien, die standardmäßig vorkonfiguriert mit der Software ausgeliefert werden als "Preshared Key" und "RSA-Signatur".

Inhalt und Name dieser Richtlinien können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf, d. h. eine Richtlinie kann aus mehreren Vorschlägen bestehen.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D. h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Mit den Plus/Minus-Buttons erweitern Sie die Liste der Vorschläge oder löschen einen Vorschlag aus der Liste der Richtlinie.

Richtlinienname [IKE-Richtlinien]

Geben Sie dieser Richtlinie einen Namen, über den sie später einer SPD zugeordnet werden kann.

Art der Gültigkeit [IKE-Richtlinien]

... bestimmt nach welchen Kriterien die Art der Schlüsselgültigkeit festgelegt wird, nach Dauer, nach übertragenen kBytes oder nach beiden. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt.

Dauer [IKE-Richtlinien]

Die Menge der kBytes oder die Größe der Zeitspanne kann eigens eingestellt werden.

kBytes [IKE-Richtlinien]

Die Menge der kBytes oder die Größe der Zeitspanne kann eigens eingestellt werden.

Authentisierung [IKE-Richtlinien]

Bevor der Kontrollkanal für die Phase 1-Verhandlung (IKE Security Association) aufgebaut werden kann, muss beidseitig eine Authentisierung stattgefunden haben.

Preshared Key = Zur gegenseitigen Authentisierung wird ein (allen) gemeinsamer statischer Schlüssel verwendet. Diesen Schlüssel definieren Sie in den Security-Parameterfeldern (siehe: Link-Profile / Security).

RSA Signature = Zur gegenseitigen Authentisierung wird das Zertifikat verwendet, das Sie für die “Erweiterte Authentisierung” konfiguriert haben (siehe: Server-Zertifikate). Im Main Mode wird das Zertifikat zusätzlich verschlüsselt.

Verschlüsselung [IKE-Richtlinien]

Nach einem der optionalen Verschlüsselungsalgorithmen erfolgt die symmetrische Verschlüsselung der Messages 5 und 6 im Kontrollkanal (siehe: Beispiele und Erklärungen, IKE-Modi), sofern der Main Mode (Identity Protection Mode) gefahren wird. Zur Wahl stehen: DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

Hash [IKE-Richtlinien]

Modus, wie der Hash-Wert über die ID bzw. das Zertifikat der Messages im Kontrollkanal gebildet wird (siehe: Beispiele und Erklärungen, IKE-Modi).

Zur Wahl stehen:

– MD5 (Message Digest, Version 5)

– SHA 256 (Secure Hash Alogrithm)

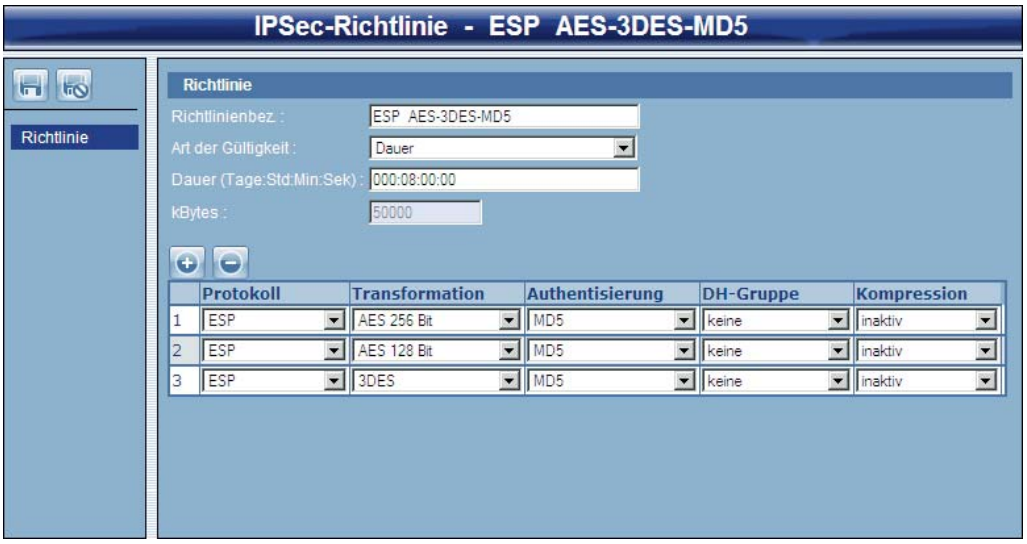
– SHA 384

– SHA 512

DH-Gruppe [IKE-Richtlinien]

Mit der Wahl einer der angebotenen Diffie-Hellmann-Gruppen wird festgelegt, wie sicher der Key Exchange im Kontrollkanal erfolgen soll, nach dem der spätere symmetrische Schlüssel erzeugt wird. Je höher die DH Group desto sicherer ist der Key Exchange.

IPSec-Richtlinien



Um die IPSec-Konfiguration für Clients zu erleichtern, wurden neue Optionen geschaffen, die es ermöglichen IPSec zu fahren ohne eine IKE- (Phase 1) oder IPSec-Richtlinie (Phase 2) vorzudefinieren.

Sobald am Client eingegeben wurde IKE-Richtlinie und/oder IPSec-Richtlinie "von Gegenstelle bestimmt", akzeptiert der Client die Richtlinie, die vom Gateway geschickt wird. Auf diese Weise wird IPSec genauso gehandhabt wie L2Sec: die Gegenstelle (VPN Gateway) legt die Parameter fest, die vom Initiator (Client) akzeptiert werden müssen.

Ist ein VPN Gateway ein Initiator (Client Gateway) gegenüber einem anderen VPN Gateway (aufbauendes Gateway), muss beim Initiator-Gateway des IPSec-Prozesses die entsprechende Einstellung vorgenommen werden. Diese Einstellungsmöglichkeiten befinden sich in den "Link-Profilen" unter "Security" (Security-Modus IPSec) bei den Parametern "IKE-Richtlinie und/oder IPSec-Richtlinie".

Konfiguration [IPSec-Richtlinien]

Die IPSec-Richtlinien (Phase-2-Parameter), die Sie hier konfigurieren, werden zur Auswahl für die SPD gelistet.

Sofern IPSec für Remote Access eingesetzt wird, ordnen sie eine der IPSec-Richtlinien im Parameterfeld "Security" unter "Link-Profile" dem jeweiligen Link zu.

Eine IPSec-Richtlinie mit ESP-Protokoll ist standardmäßig vorkonfiguriert mit der Software ausgeliefert.

Inhalt und Name dieser Richtlinie können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu IPSec-Protokoll und Authentisierung auf, d. h. eine Richtlinie kann aus mehreren Vorschlägen bestehen.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D. h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Mit den Plus/Minus-Buttons erweitern Sie die Liste der Vorschläge oder löschen einen Vorschlag aus der Liste der Richtlinie.

Richtlinienname [IPSec-Richtlinien]

Geben Sie dieser Richtlinie einen Namen, über den Sie sie später einer SPD zuordnen können.

Art der Gültigkeit [IPSec-Richtlinien]

Bestimmt nach welchen Kriterien die Art der Schlüsselgültigkeit festgelegt wird, nach Dauer, nach übertragenen kBytes oder nach beiden. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt.

Dauer [IPSec-Richtlinien]

Dauer und kBytes können eigens festgelegt werden.

kBytes [IPSec-Richtlinien]

Dauer und kBytes können eigens festgelegt werden.

Protokoll [IPSec-Richtlinien]

Die IPSec-Richtlinien sind im Wesentlichen nach den beiden Sicherheitsprotokollen unterschieden, AH oder ESP, die sich im Tunnelmodus gegenseitig ausschließen. Standard ist ESP.

Transformation [IPSec-Richtlinien]

Wenn das Sicherheitsprotokoll ESP eingestellt wurde, kann hier definiert werden wie mit ESP verschlüsselt werden soll. Zur Wahl stehen die gleichen Verschlüsselungsalgorithmen wie für Layer 2:

DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

Authentisierung [IPSec-Richtlinien]

Für das Sicherheitsprotokoll ESP kann der Modus der Authentisierung eigens eingestellt werden. Zur Wahl stehen:

– MD5(Message Digest, Version 5)

– SHA 256 (Secure Hash Alogrithm)

– SHA 384

– SHA 512

– DES

DH-Gruppe [IPSec-Richtlinien]

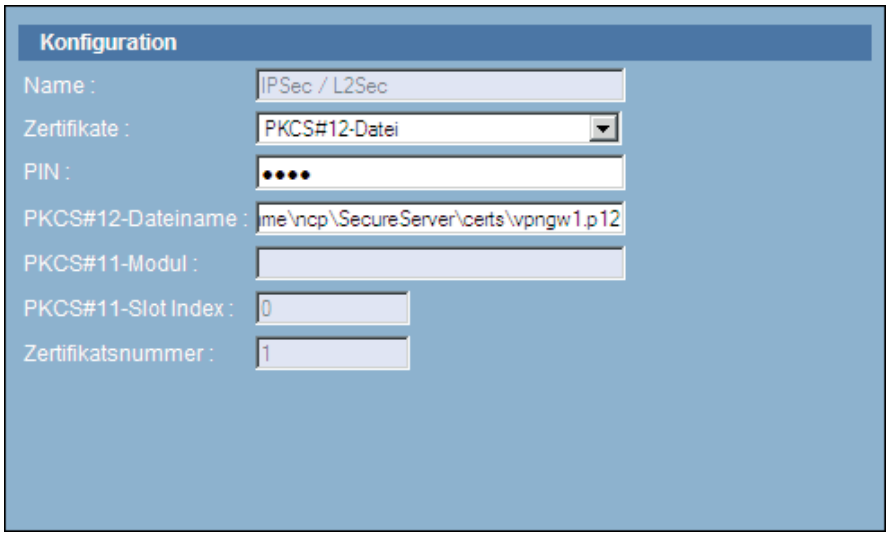
Mit der Wahl einer der angebotenen Diffie-Hellmann-Gruppen wird festgelegt, dass zusätzlich in Phase 2 mit der SA-Verhandlung ein kompletter Schlüsselaustausch (PFS) stattfinden soll. Standard ist inaktiv.

Kompression [IPSec-Richtlinien]

Die Datenübertragung kann mit IPSec ebenso komprimiert werden wie ein Transfer ohne IPSec. Dies ermöglicht eine Steigerung des Durchsatzes um maximal das 3-fache. Die Einstellung dazu muss beidseitig am Client und am Server vorgenommen werden.

Server-Zertifikate

Für IPSec- und L2Sec-Verbindungen ist ein Test-Zertifikat von NCP in Form einer PKCS#12-Datei vorkonfiguriert.



Diese Zertifikats-Konfiguration heißt "IPSec / L2Sec". Sie ist eine Grundkonfiguration, die sich abändern lässt aber nicht gelöscht werden kann.

Konfiguration [Server-Zertifikate]

Max. 128 Server-Zertifikate bzw. Konfigurationen von Server-Zertifikaten können abgespeichert werden. Das in dieser Konfiguration aktive Server-Zertifikat wird bei IPSec- und L2Sec-Verbindungen des Servers zur Authentisierung genutzt.

In der SSL VPN-Konfiguration kann dasselbe Server-Zertifikat durch Selektion dieser Konfiguration genutzt werden, sofern es als PKCS#12-Datei vorliegt (siehe: **SSL VPN / Web-Listener**). PKCS#11-Module können als Server-Zertifikate für den Web-Listener nicht eingesetzt werden.

Name [Server-Zertifikate]

Über den hier eingetragenen Namen der Konfiguration wird das zugehörige Server-Zertifikat dem Web-Listener zugeordnet.

Zertifikat [Server-Zertifikate]

Wählen Sie die Einstellung "ohne", so wird kein Zertifikat ausgewertet und die "Erweiterte Authentisierung" findet nicht statt.

Wählen Sie "PKCS#12-Datei", so wird das Server-Zertifikat aus einer Datei auf der Festplatte Ihres Rechners gelesen. In diesem Fall muss zusätzlich Pfad und Dateiname der PKCS#12-Datei eingegeben werden (siehe: PKCS#12-Dateiname).

Wählen Sie "PKCS#11-Modul", so wird das Server-Zertifikat von einem USB-Token gelesen. In diesem Fall muss Pfad und Dateiname des PKCS#11-Moduls und der Slot-Index eingegeben werden.

PIN [Server-Zertifikate]

Die PIN (Personal Identification Number) muss eingegeben werden, wenn Zertifizierung eingesetzt wird, gleich ob dabei eine PKCS#12-Datei oder ein PKCS#11-Modul genutzt wird. Die PIN besteht aus mindestens 4 Ziffern.

PKCS#12-Dateiname [Server-Zertifikate]

Wenn Sie die PKCS#12-Datei nutzen, muss der Dateiname, einschließlich des kompletten Pfades, angegeben werden.

PKCS#11-Modul [Server-Zertifikate]

Wählen Sie "aus PKCS#11-Modul" aus der Listbox, so werden bei der erweiterten Authentisierung die Zertifikate aus einem Token über ein PKCS#11 Modul gelesen.

Nutzen Sie das PKCS#11-Format, so erhalten Sie eine DLL vom Hersteller, die auf der Festplatte Ihres Rechners eingespielt werden muss. Tragen Sie Pfad und Namen dieser DLL in das Feld für das PKCS#11-Modul ein.

PKCS#11-Slot Index [Server-Zertifikate]

Der PKCS#11-Slot Index hängt vom Hersteller der DLL ab. Diesen Slot-Index tragen Sie hier ein.

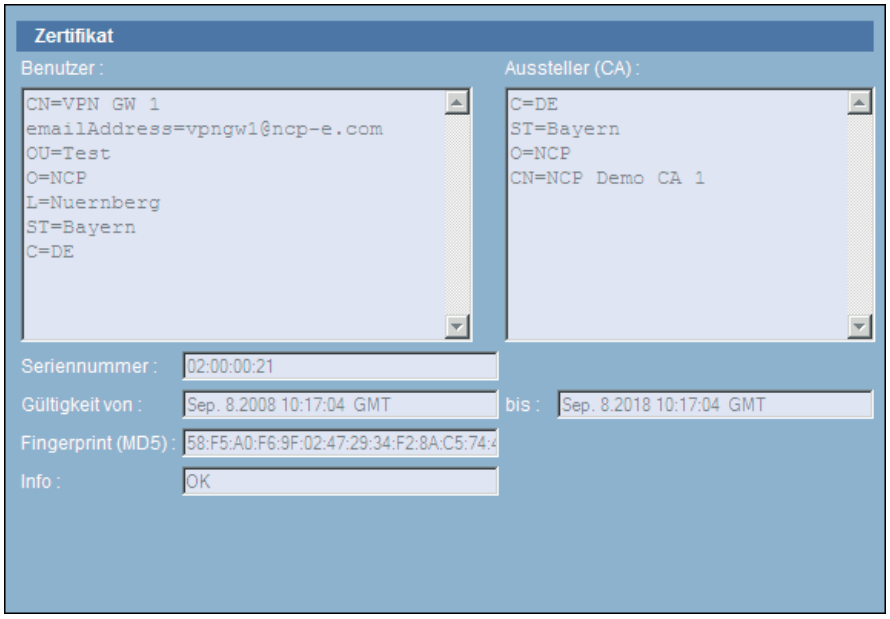
Zertifikats-Auswahl [Server-Zertifikate]

Wählen Sie aus welches Zertifikat aus welchem Slot selektiert werden soll.

Zertifikat [Server-Zertifikate]

Der Inhalt des aktiven Server-Zertifikats wird mit folgenden Größen angezeigt:

– Benutzer
– Aussteller
– Seriennummer
– Gültigkeit
– Fingerprint (MD5)
– Info



Benutzer [Server-Zertifikate]

Wenn Sie sich Ihr Benutzer-Zertifikat anzeigen lassen, können Sie sehen, welche Merkmale zur Erstellung des Zertifikats genutzt wurden, z. B. die eindeutige E-Mail-Adresse.

Aussteller [Server-Zertifikate]

Der Aussteller Ihres Server-Zertifikats muss mit dem Aussteller des CA-Zertifikats identisch sein.

Seriennummer [Server-Zertifikate]

Nach der Seriennummer werden die Zertifikate mit den in der Sperrliste der Certification Authority gehaltenen verglichen.

Gültigkeit [Server-Zertifikate]

Das Gültigkeitsintervall des Zertifikats wird in GMT (Greenwich Mean Time) angezeigt. Die Gültigkeitsdauer eines Aussteller-Zertifikats ist in aller Regel länger als die eines Server- oder Benutzer-Zertifikats. Mit dem Erlöschen der Gültigkeit des Aussteller-Zertifikats erlischt automatisch die Gültigkeit eines vom gleichen Aussteller ausgestellten Benutzer-Zertifikates.

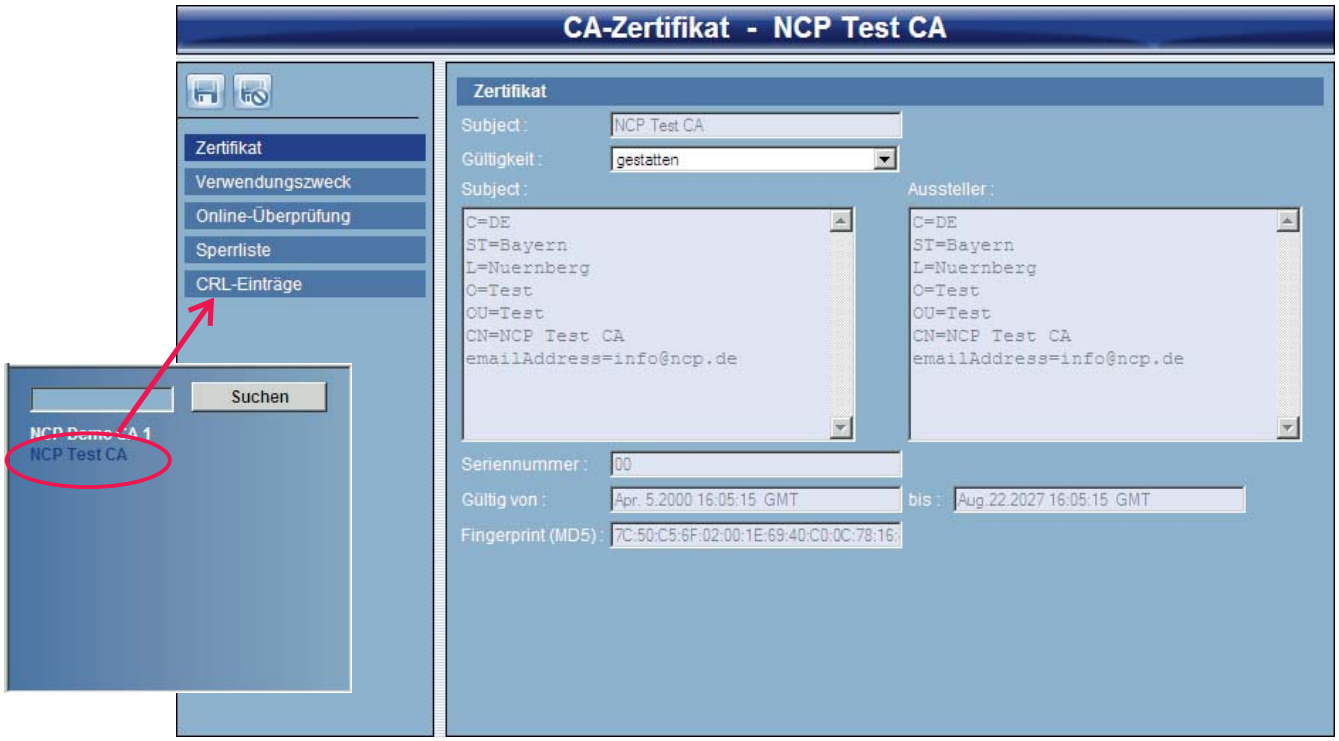
Fingerprint (MD5) [Server-Zertifikate]

Der Fingerprint ist ein Hash-Wert. Der mit dem Private Key der CA verschlüsselte Hash-Wert ist die Signatur des Zertifikats.

Info [Server-Zertifikate]

In diesem Feld werden mögliche Mängel eines Zertifikats angezeigt, die es ungültig machen, wie z. B. der Ablauf der Gültigkeit oder die Registrierung in einer CRL.

CA-Zertifikate



Die Software untestützt zwei Formate für ein CA-Zertifikat: *.pem und *.crt.

Nach der Installation des Servers sind immer zwei CA-Zertifikate zum Test eingerichtet (Abb. oben):

NCP Demo CA 1 (ncpdemoca1a.crt)

NCP Test CA (ncpsupportca.pem)

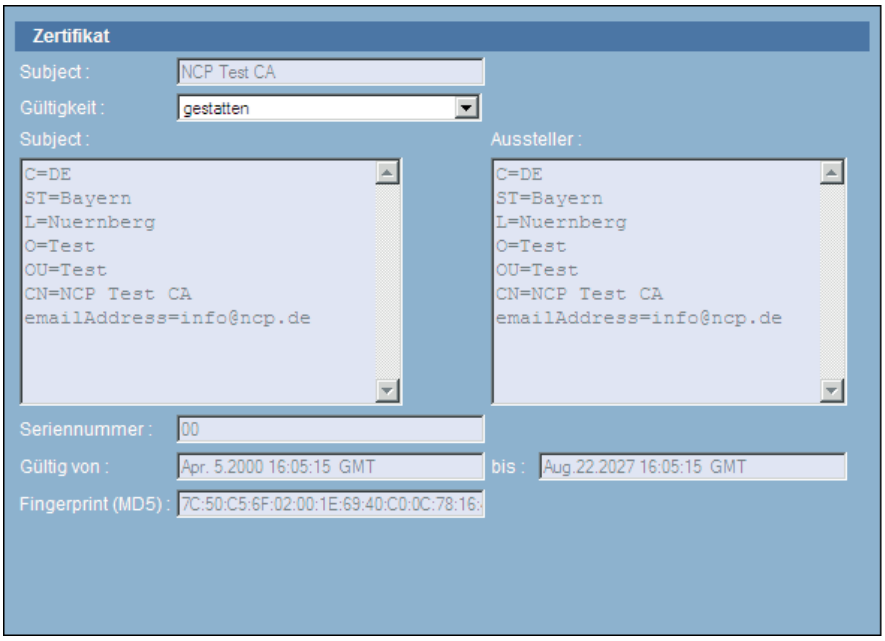
Diese CA-Zertifikate befinden sich im Installationsverzeichnis unter `<ncp\secureserver\certs>`.

Ihr eigenes CA-Zertifikat spielen Sie dort ein. Sie können es in die Konfiguration laden, indem Sie unter “CA-Zertifikate / Zertifikat” den Plus-Button drücken und Ihr CA-Zertifikat im Unterverzeichnis <cacerts> selektieren.

Für das jeweils markierte CA-Zertifikat werden fünf Konfigurationsfelder eingeblendet (Abb. oben).

Zertifikat [CA-Zertifikate]

Das erste Konfigurationsfeld dient der Anzeige des CA-Zertifikats bzw. des Subjects.



Subject [CA-Zertifikate]

Ein bezeichnendes Feld aus dem Subject wird explizit angezeigt (CN, E-Mail-Adresse, etc.), nicht der komplette String.

Gültigkeit [CA-Zertifikate]

Die Gültigkeit eines Aussteller-Zertifikats (CA-Zertifikat) kann an dieser Stelle unabhängig von der ausgestellten Gültigkeitsdauer eingeschränkt werden. So kann der Administrator z. B. in einem Korruptionsfall den Zugang für alle Clients verhindern, welche sich über dieses CA-Zertifikat authentisieren, indem er das CA-Zertifikat sperrt.

Allerdings kann die Gültigkeit nur verweigert oder erteilt werden, wenn das Zertifikat aus einer Datei auf der Festplatte des Rechners gelesen wird (siehe: Zertifikat aus Datei). Wenn das Aussteller-Zertifikat über einen LDAP Server ausgewertet wird, ist dieses Feld nicht editierbar.

sperren = Das CA-Zertifikat kann nicht mehr zur Authentisierung von Clients verwendet werden, sodass für Clients mit diesem CA-Zertifikat der Zugang gesperrt ist.

gestatten = Das CA-Zertifikat wird zur Authentisierung genutzt. Clients mit diesem CA-Zertifikat erhalten Zugang zum Gateway.

Subject / Aussteller [CA-Zertifikate]

Subject und Aussteller eines CA-Zertifikats – hier die Zertifikatsinhalte – sind für gewöhnlich identisch (selfsigned certificate).

Seriennummer [CA-Zertifikate]

Nach der Seriennummer werden die Zertifikate z. B. mit den in der Sperrliste der Certification Authority gehaltenen verglichen.

Gültigkeitsdauer [CA-Zertifikate]

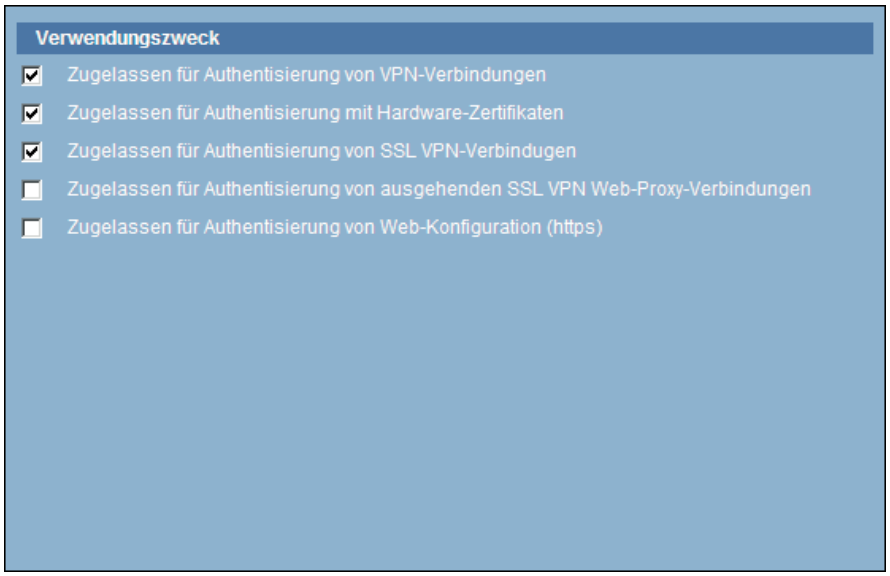
Das Gültigkeitsintervall des Zertifikats wird in GMT (Greenwich Mean Time) angezeigt. Die Gültigkeitsdauer eines Aussteller-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Mit dem Erlöschen der Gültigkeit des Aussteller-Zertifikats erlischt automatisch die Gültigkeit eines vom gleichen Aussteller ausgestellten Benutzer-Zertifikates.

Fingerprint (MD5) [CA-Zertifikate]

Der Fingerprint ist ein Hash-Wert. Der mit dem Private Key der CA verschlüsselte Hash-Wert ist die Signatur des Zertifikats.

Verwendungszweck [CA-Zertifikate]

Das CA-Zertifikat kann für verschiedene Verwendungszwecke zugelassen werden.



Auswahl des Verwendungszwecks

– für Authentisierung von VPN-Verbindungen

– für Authentisierung mit Hardware-Zertifikaten

– für Authentisierung von SSL VPN-Verbindungen

– für Authentisierung von ausgehenden SSL VPN Web-Proxy-Verbindungen

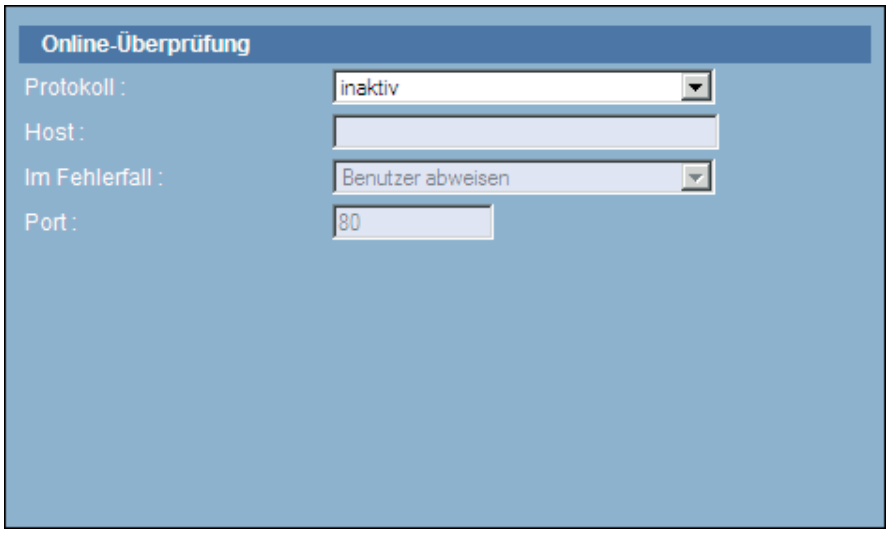
[Soll über den Secure Server eine SSL-Verbindung zu einem Anwendungs-Server wie z. B. einem Web-Server (zugewiesen durch die URL) weitergeführt werden, so muss das Aussteller-Zertifikat des Web-Servers am Secure Server eingespielt werden und die Gültigkeit des CA-Zertifikats auf “SSL VPN Web-Proxy-Verbindungen” gesetzt werden.]

– für Authentisierung von Web-Konfiguration (https)

[Wurde in der Zugriffsverwaltung des Systems für Administratoren der “Zugriff nur mit Zertifikat” erlaubt, so muss das Aussteller-Zertifikat des Servers vorhanden sein und die Gültigkeit des CA-Zertifikats für die Web-Konfiguration aktiviert sein.]

Online-Prüfung [CA-Zertifikate]

Beachten Sie zu diesem Konfigurationsfeld auch die Beschreibungen zu anderen “Zertifikats-Überprüfungen”.



Protokoll [Online-Prüfung]

Als Protokoll für die Online-Prüfung können Sie OCSP (Online Certificate Status Protocol) für binäre Übertragung oder OCSP (HTTP) mit dem HTTP-Übertragungsprotokoll wählen.

Host [Online-Prüfung]

Je nach gewähltem Protokoll geben Sie hier die Host IP-Adresse des OCSP-Servers ein.

Im Fehlerfall [Online-Prüfung]

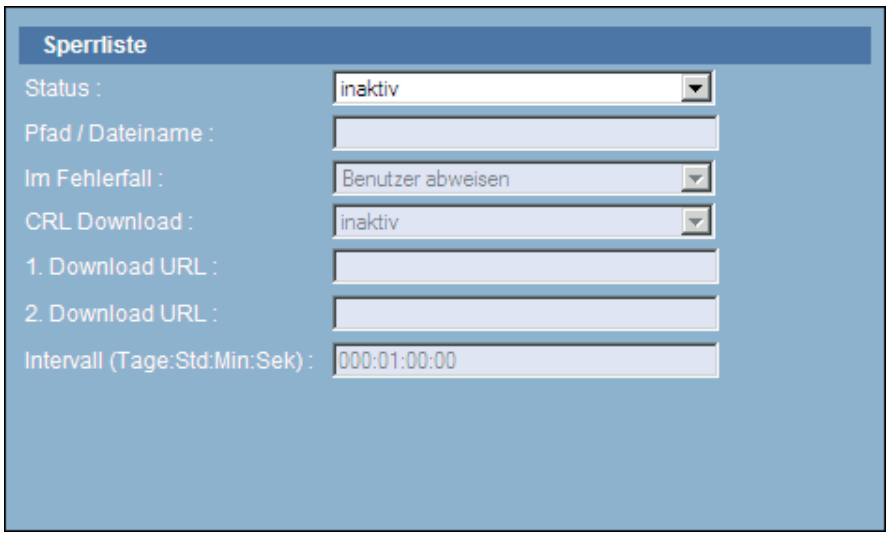
Wenn keine Verbindung zum OCSP-Server zustande kommt, können Sie trotzdem Benutzer ohne Online-Prüfung “zulassen”. Sie können die Benutzer dann aber auch “abweisen”.

Port [Online-Prüfung]

Die Port-Nummer des OSCP-Servers. Ändern Sie diesen Wert nur, wenn der Server unter einer anderen Port-Nummer als der hier angegeben Standard-Nummer (80) läuft.

Sperrliste [CA-Zertifikate]

Jede Certification Authority führt ihre eigene Revocation List (Sperrliste). In der Sperrliste werden alle gesperrten Benutzer-Zertifikate geführt. Gesperrt werden sie zum Beipsiel, wenn der Benutzer den Verlust seiner Chipkarte meldet. (Zertifikate, deren Gültigkeitsdauer abgelaufen ist, werden hier nicht gehalten.) Die Sperrliste wird in definierten Abständen auf den aktuellsten Stand gebracht.



Um lückenlose Sicherheit zu gewährleisten, ist es unbedingt notwendig, die aktuellste Revocation List (Sperrliste) der jeweiligen CA zu benutzen. Bitte achten Sie auch darauf, dass Sie die Sperrliste dem richtigen CA-Zertifikat zuordnen (siehe: CRL-Einträge / Fehler).

Status [Sperrliste]

Mit dem Status bestimmen Sie ob eine Sperrliste “genutzt” oder “ungenutzt” wird.

Pfad / Dateiname [Sperrliste]

Hier geben Sie Pfad und Dateiname der Sperrliste an, die Sie für Clients der CA nutzen, die oben unter “Benutzer” angezeigt wird. Achten Sie bitte darauf, dass die Sperrliste nur begrenzte Zeit Gültigkeit hat, und dass sie nach entsprechenden Zeitintervallen erneuert werden muss. Pfad und Dateiname der mitgelieferten Sperrliste ist im Installationsverzeichnis unter
`<NCP\SecureServer\certs\crl.crl>`

Die CRL kann in zwei Dateiformaten gelesen werden: PEM (Textfile Base 64 encoded) und CRL (binär).

Wenn CRL abgelaufen [Sperrliste]

Wenn die Sperrliste (Sperrliste) veraltet ist, können Sie trotzdem Benutzer ohne Online-Prüfung “zulassen”. Sie können die Benutzer dann aber auch “abweisen”.

“Benutzer zulassen” bedeutet: Trotz veralteter Sperrliste können Benutzer, die nicht darin eingetragen sind, eine Verbindung herstellen.

“Benutzer abweisen” bedeutet: Kein Benutzer kann eine Verbindung herstellen, bis die CRL aktualisiert wurde.

CRL Download [Sperrliste]

In der Sperrliste (Sperrliste, CRL) werden die gesperrten Benutzer-Zertifikate geführt. Sie wird von der Certification Authority in definierten Zeitabständen auf den aktuellsten Stand gebracht.

Der automatische Download wird mit dem Parameter “Benutze CRL Download” aktiv geschaltet.

Download URL [Sperrliste]

Je nachdem, wo die CA ihre Sperrliste ablegt, kann der “Download URL” der Sperrliste auf den Secure Server über HTTP (Web Server), HTTPS oder LDAP (LDAP Server) erfolgen.

Eine alternative zweite Adresse für den Download kann angegeben werden.

Die CRL kann nun in zwei Dateiformaten gelesen werden: PEM (Textfile Base 64 encoded) und CRL (binär), wobei das CRL-Format schneller ausgewertet werden kann und nicht konvertiert werden muss. Die Endung des Dateinamens (CRL oder PEM) muss mit der Endung der CRL-Datei auf dem Server übereinstimmen. Die Dateinamen der URL und der konfigurierten CRL-Dateien brauchen nicht übereinzustimmen.

HTTP

Erfolgt der Download von einem Web Server, so muss die Web-Adresse mit dem Dateinamen (http://web server/filename) angegeben werden.

Beispiel für HTTP
URL: http://62.152.164.36/crl.crl

LDAP

Über LDAP muss als Suchkriterium die LDAP Base DN angegeben werden. Stimmt der Aussteller der Sperrliste mit dem Subject des CA-Zertifikats nicht überein, so wird der Download bei LDAP abgebrochen.

Beispiel für LDAP
URL: ldap://62.152.164.36/o=ncp,c=de

HTTPS

Soll eine CRL über HTTPS vom Web Server heruntergeladen werden, muss das Protokoll “https:\\” angegeben werden.

Intervall [Sperrliste]

Hier können Sie eine bestimmte Zeitspanne als Intervall des Downloads eingeben.

Bei der ersten Konfiguration braucht nur ein Dateiname der CRL angegeben zu werden. Die Datei muss nicht auf dem Secure Server vorhanden sein. Nach dem Speichern der Konfiguration wird der Download zum ersten Mal durchgeführt und die CRL in der angegebenen Datei gespeichert.

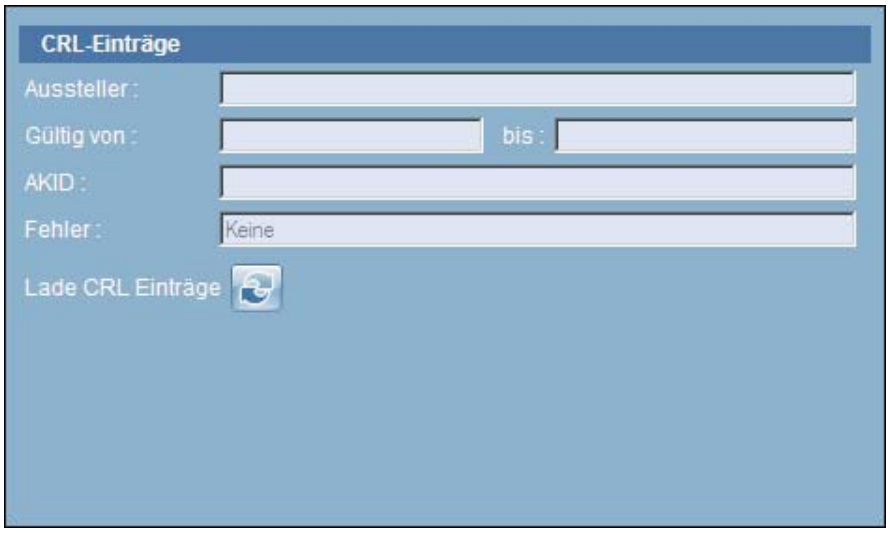
Der Download wird im angegebenen Zeitintervall wiederholt und beginnt immer ca. 20 Sekunden nach dem Start des SNMP-Dienstes. Wird die Konfiguration des CA-Zertifikats geändert, so wird der Download nach ca. 5 Sekunden wiederholt.

CRL-Einträge [CA-Zertifikate]

Unter diesem Menüpunkt können Sie die signifikanten Einträge der Revocation List (Sperrliste) betrachten und gegebenenfalls zu Entscheidungen bezüglich zulässiger Zugriffe auf Ihr System heranziehen.

Bitte beachten Sie, dass das Auslesen dieser Informationen nur sinnvoll ist, wenn Sie die neusten Sperrlisten (Revocation Lists) im Installations-Verzeichnis unter

<NCP\SecureServer\Certs> vorliegen haben – bzw. in dem von Ihnen dafür vorgesehenen Verzeichnis (siehe: Pfad / Dateiname, Sperrliste).



Aussteller [CRL-Einträge]

Der Aussteller der Sperrliste kann in diesem Feld abgelesen werden.

Aussteller einer Sperrliste (Revocation List) ist in der Regel die Stelle, der der Verlust oder der Verfall eines gültigen Zertifikats gemeldet wird. Meist ist es die Registrierungsstelle (Registration Authority), die auch die Daten für die Beantragung eines Zertifikats entgegen nimmt.

Die CRL kann auch von einem anderen Aussteller übernommen werden. Dazu muss vom Secure Server auch das Aussteller-Zertifikat der CA importiert worden sein, die die zu nutzende CRL erzeugt hat. Nur dann kann die Signatur der CRL überprüft werden. Zusätzlich muss für die jeweiligen CA-Zertifikate, für die diese CRL gültig sein soll, im Parameterfeld “Sperrliste” unter “CA-Zertifikate” die gleiche CRL konfiguriert werden, d. h. Pfad und Dateiname müssen für alle CA-Zertifikate gleich eingestellt sein.

Gültigkeitsdauer [CRL-Einträge]

Sie können hier ablesen von wann bis wann eine Sperrliste gültig ist und sie gegebenenfalls austauschen, wenn ein Fehler abgelesen wird (siehe unten: im Fehlerfall).

Die Sperrliste (Revocation List) wird für gewöhnlich in regelmäßigen (täglichen) Abständen erneuert, unabhängig davon wieviele Zertifikate innerhalb eines Erneuerungsintervalls in die Liste aufgenommen wurden.

AKID [CRL-Einträge]

Ist in einem Benutzer-Zertifikat die Erweiterung “Authority Key Identifier” (AKID) vorhanden, so wird diese hier angezeigt.

Fehler [CRL-Einträge]

Die Sperrliste kann falsch eingesetzt werden. Folgende Fehlermeldungen sind möglich:

noch nicht gültig = Es gibt ein eindeutiges Datum, ab dem das Intervall der Gültigkeitsdauer beginnt. Dieses Datum ist noch nicht eingetreten.

abgelaufen = Die Gültigkeitsdauer der Sperrliste ist abgelaufen (siehe: CRL-Einträge, Gültigkeitsdauer).

falscher Aussteller = Sperrliste und CA-Zertifikat haben unterschiedliche Aussteller. Dieser Fehler kann durch Korrektur von Pfad/Dateiname der Sperrliste behoben werden (siehe: Sperrliste, Pfad/Dateiname).

keiner = Die Sperrliste ist gültig.

Seriennummer [CRL-Einträge]

Hier werden die Seriennummern der widerrufenen, gesperrten Zertifikate angezeigt. Versucht ein Benutzer sich mit einem widerrufenen Zertifikat gegenüber diesem Server zu authentisieren, so wird die Verbindung vom Server nicht hergestellt. Über Traps kann zu einem späteren Zeitpunkt ausgelesen werden, was die Ursache der Verbindungsablehnung war.

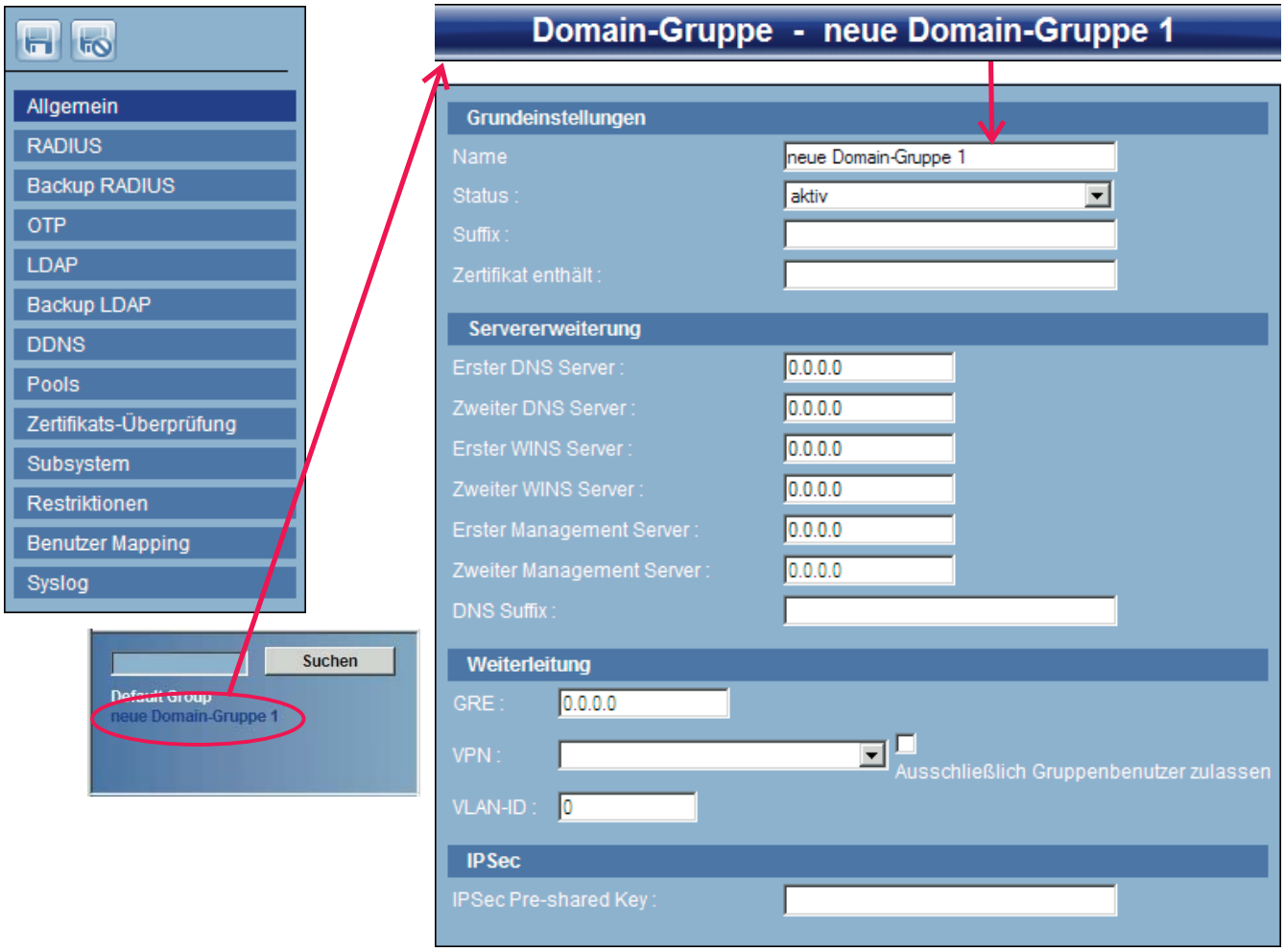
Datum / Zeit [CRL-Einträge]

Datum und Zeit zeigen an, seit wann die Zertifikate der Sperrliste gesperrt sind. Für gewöhnlich werden die Sperrlisten ständig ergänzt, das heißt neuerlich ungültig gewordene Zertifikate werden aufgenommen. Ungültig gewordene Zertifikate können erst aus der Liste entfallen, wenn ihr Gültigkeitszeitraum bereits abgelaufen ist.

Domain-Gruppen

Die Standard-Gruppe (Default Group) ist in der Server-Konfiguration immer vorhanden. Klicken Sie auf den Plus-Button, kann eine neue Domain-Gruppe angelegt werden.

Wird eine Gruppe angelegt, so kann die Server-Umgebung und die Adress-Zuordnung für diese Gruppe definiert werden, indem mindestens ein RADIUS- oder LDAP-Server mit den E-Mail-Adressen der Benutzer dieser Gruppe aktiviert wird. Alle anderen Server-Erweiterungen oder Adress-Zuordnungen sind optional.



Allgemein [Domain-Gruppen]

Maximal können 1024 Gruppen angelegt werden, die nach Bedarf “aktiv” geschaltet werden können.

Status [Allgemein / Domain-Gruppen]

Jede Gruppe kann einzeln “aktiv” oder “inaktiv” gesetzt werden. Mitglieder einer inaktiven Gruppe können sich nicht über den Gruppenzugang mit dem Secure Server verbinden.

Suffix [Allgemein / Domain-Gruppen]

Eine Gruppe unterscheidet sich von einer anderen durch mindestens ein Merkmal, über das alle Gruppenmitglieder gleichermaßen verfügen.

Dieses Merkmal wird aus der Benutzerkennung “Benutzer (VPN)” (VPN User ID) des Clients gewonnen, indem in der Konfiguration des Secure Clients unter “Tunnelparameter” dem Benutzernamen im Feld für “Benutzer (VPN)” ein Suffix mit einem @-Zeichen angehängt wird (z. B. @firma2). Dieser Suffix ist in der Client-Konfiguration frei wählbar.

Als Suffix kann auch die Domain der E-Mail-Adresse gewählt werden, indem in der Client-Konfiguration unter “Tunnelparameter” die Einstellung “Benutze Zugangsdaten von Zertifikat” gewählt und dafür die E-Mail-Adresse bestimmt wird. Dieser Suffix wird hier eingetragen.

Die Benutzer, die einer Gruppe angehören sollen, müssen mit diesem Suffix lokal oder auf einem RADIUS-/ LDAP-Server angelegt worden sein.

Eine zusätzliche gruppenspezifische Differenzierung kann über weitere Inhalte und die ausstellende Zertifizierungstelle der Benutzer-Zertifikate erfolgen (siehe: Zertifikats-Überprüfung [Domain-Gruppen]).

Kann ein Benutzer weder über Suffix noch Zertifikatsinhalt einer bestimmten Domain-Gruppe zugewiesen werden, wird er zur “Standard-Gruppe” gerechnet.

Zertifikat enthält [Allgemein / Domain-Gruppen]

Bei Verwendung von IPSec native kann die Gruppe alternativ zum Benutzer-Suffix auch anhand von Zertifikatsinhalten erkannt werden.

Zum Abgleich von Zertifikatsinhalten mit Gruppeneigenschaften können bestimmte Ausdrücke (expressions) mit Inhalten (contents), Operatoren (operation) und Werten (values) nach folgender Syntax gebildet werden:
`contents operation value`

Folgende Operatoren können eingesetzt werden:
`expression AND expression`
`expression OR expression`
`NOT expression`
`(expression)`

Folgende Operationen (Operations) können durchgeführt werden:
`= <> >= <= > <`

Einträge in Listen (z. B. Policies) können verglichen werden:
`~ (enthält Eintrag in Liste)`
Z. B.: POLICY ~ 1.3.6

Folgende Werte (Values) können in Anführungszeichen abgefragt werden:
Zeichenkette mit “ am Anfang und am Ende

Folgende Inhalte (contents) können ausgelesen werden:
```
S_CN Common Name im Subject
S_EMAIL EMail im Subject
S_SN Name im Subject
S_GN Vorname im Subject
S_OU3 3. Organisation Unit im Subject
S_OU2 2. Organisation Unit im Subject
S_OU 1. Organisation Unit im Subject
S_O2 2. Organisation im Subject
S_O 1. Organisation im Subject
S_L Location in Subject
S_ST State/Province in Subject
S_C Country im Subject
I_CN Common Name im Issuer
I_EMAIL EMail im Issuer
I_SN Name im Issuer
I_GN Vorname im Issuer
I_OU3 3. Organisation Unit im Issuer
I_OU2 2. Organisation Unit im Issuer
I_OU 1. Organisation Unit im Issuer
I_O2 2. Organisation im Issuer
I_O 1. Organisation im Issuer
I_L Location in IssuerI_ST State/Province in Issuer
I_C Country im Issuer
POLICY Certificate Policy Info
```

Erster / Zweiter DNS Server [Allgemein / Domain-Gruppen]

Der zuerst eingetragene DNS Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt. Der zweite DNS Server dient als Backup-DNS Server.

Dazu muss in den Netzwerk-Einstellungen des Betriebssystems der DNS-Modus eingestellt sein.

Erster / Zweiter WINS Server [Allgemein / Domain-Gruppen]

Der zuerst eingetragene WINS Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt. Der zweite WINS Server dient als Backup-WINS Server.

Hinweis: Je nach Anwendung können Sie ein oder zwei DNS- oder WINS Server eintragen. Genutzt wird immer der jeweils erste. Wird kein alternativer zweiter Server eingetragen, wird der Server genutzt, der über PPP zugewiesen wird.

Dazu muss in den Netzwerk-Einstellungen des Betriebssystems der DNS-Modus eingestellt sein.

Erster / Zweiter Management Server [Allgemein / Domain-Gruppen]

IP-Adresse des Management Servers aus dem Firmennetz, die vom Secure Server an den Secure Client übermittelt wird.

DNS Suffix [Allgemein / Domain-Gruppen]

Entfernte VPN Clients bekommen beim Verbindungsaufbau über DHCP den hier eingetragenen gruppenspezifischen DNS Suffix zugewiesen.

SSL VPN DNS Suffix [Allgemein / Domain-Gruppen]

Entfernte SSL VPN Clients bekommen beim Verbindungsaufbau über DHCP den hier eingetragenen gruppenspezifischen DNS Suffix zugewiesen.

GRE [Allgemein / Domain-Gruppen]

Die Generic Router Encapsulation (GRE) kann nur genutzt werden, wenn die Gegenstelle ebenfalls GRE unterstützt.

An dieser Stelle tragen Sie die IP-Adresse des GRE-Endpunkts der Gegenstelle ein.

Das IP-Packet wird vor dem Senden mit einem GRE-Header verpackt, am GRE-Endpunkt wieder entpackt und erst dann “normal” weiter geroutet.

GRE kann für jedes **Link-Profil** einzeln konfiguriert werden. Wird im Link-Profil kein GRE-Endpunkt angegeben, so wird automatisch der hier eingegebene angenommen.

Achten Sie außerdem darauf, dass nur eine der drei Weiterleitungsarten aktiviert ist!

Ausschließlich Gruppenbenutzer zulassen

Nur die Datenpakete dieser Domain-Gruppe werden über den VPN-Tunnel weitergeleitet.

VPN [Allgemein / Domain-Gruppen]

Datenpakete von Mitgliedern einer Domain-Gruppe können vom zentralen VPN Gateway, das bei einem Application Service Provider betrieben wird, über Tunnel an das entfernte Ziel-Gateway weitergeleitet werden. Dazu wird für die entsprechende Domain-Gruppe im Parameterfeld “Allgemein” ein jeweils zu konfigurierendes Link-Profil für eine ausgehende Verbindung zugeordnet, über welches der Tunnel zum gewünschten Ziel-Gateway hergestellt (bzw. initiiert) wird. Der Name dieses Link-Profils muss hier eingetragen werden.

Verfügt das Ziel-Gateway nicht über eine feste IP-Adresse, so erfolgt via ISDN vom ASP Gateway ein **Lockruf** an das Ziel-Gateway, womit ein Tunnelaufbau vom Ziel-Gateway zum ASP initiiert wird.

Achten Sie außerdem darauf, dass nur eine der drei Weiterleitungsarten aktiviert ist!

VLAN ID [Allgemein / Domain-Gruppen]

Die hier eingetragene VLAN ID muss mit der VLAN ID übereinstimmen, die den LAN-Adapter unter “Routing Interfaces” für die Weiterleitung der Datenpakete zu dieser Domain-Gruppe festlegt. Die VLAN ID kann Werte von 1 bis 4094 annehmen.

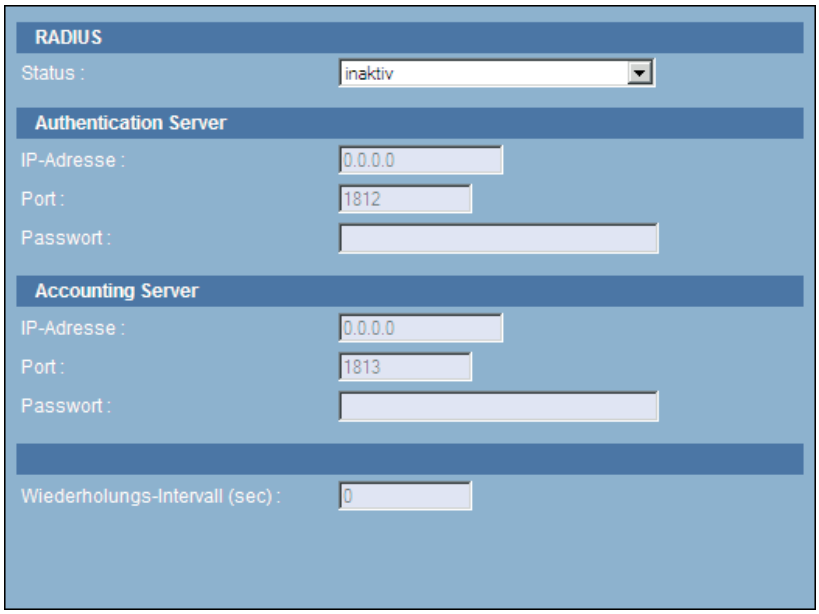
(Siehe: **Routing Interfaces / LAN-Adapter**)

Achten Sie außerdem darauf, dass nur eine der drei Weiterleitungsarten aktiviert ist!

IPSec Pre-shared Key [Allgemein / Domain-Gruppen]

Ist der Pre-Shared Key nicht benutzerspezifisch im Link-Profil konfiguriert (siehe: Link-Profile / Security), so wird der hier eingegebene gruppenspezifische Pre-Shared Key für die IPSec-Verbindung herangezogen.

RADIUS [Domain-Gruppen]



Mit RADIUS-Datenbanken kann die Benutzerverwaltung sehr komfortabel gestaltet werden. Daher ermöglicht der NCP Router den Zugriff auf RADIUS (Remote Authentication Dial In User Service). Alle Benutzer-Daten sind zentral auf dem RADIUS Server gespeichert.

In LANs mit mehreren Routern, kann jeder Router auf den Datenbestand des RADIUS Servers zugreifen. Dies bedeutet, dass Benutzer aus dem WAN immer mit der gleichen Sicherheits-Konfiguration, gleich über welchen dieser Router, auf das LAN zugreifen können.

Für die RADIUS-Konfiguration stehen zwei Parameterfelder zur Verfügung, “RADIUS Server” und “Backup RADIUS Server”. Die Parameter beider Parameterfelder sind identisch, wobei diejenigen für den Backup RADIUS Server nur einzutragen sind, wenn sich in Ihrem LAN ein zweiter RADIUS Server befindet.

Wichtig: Nachdem Sie die RADIUS-Konfiguration durchgeführt haben, müssen die Dienste neu gestartet werden.

Drücken Sie dazu den Restart-Button unter “Statistik / Systeminformationen”!

Status [RADIUS / Domain-Gruppen]

Mit dem Status bestimmen Sie, ob ein RADIUS Server für die Zugriffssteuerung genutzt wird (aktiv) oder nicht (nicht aktiv).

Wichtig: Wenn der Low Level Callback COSO (Charge one Side only) genutzt wird, können die Dienste des RADIUS Servers nicht genutzt werden. In diesem Fall muss der Status auf “nicht aktiv” geschaltet werden. (Siehe: Link-Profile / Line Management / Rückrufmodus).

Authentication Server [RADIUS/Domain-Gruppen]

Der RADIUS Authentication Server beinhaltet die Konfigurationsdaten für RADIUS-Zugriff. Die hier eingetragenen Daten berechtigen den Server, die Authentisierungs-Dienste des RADIUS Servers zu nutzen.

IP-Adresse: Die IP-Adresse des RADIUS Authentisierungs-Servers

Port: Die Port-Nummer des RADIUS Authentisierungs-Servers. Ändern Sie diesen Wert nur, wenn der RADIUS Server unter einer anderen Port-Nummer als der hier angegeben Standard-Nummer läuft.

Passwort: Passwort für den RADIUS Authentisierungs-Server.

Accounting Server [RADIUS / Domain-Gruppen]

Der RADIUS Accounting Server führt die Konten des RADIUS-Zugriffs, zum Beispiel Dauer der Verbindungszeit. Die hier eingetragenen Daten berechtigen den NAS, die Accounting-Dienste des RADIUS Servers zu nutzen.

IP-Adresse: Die IP-Adresse des RADIUS Accounting Servers

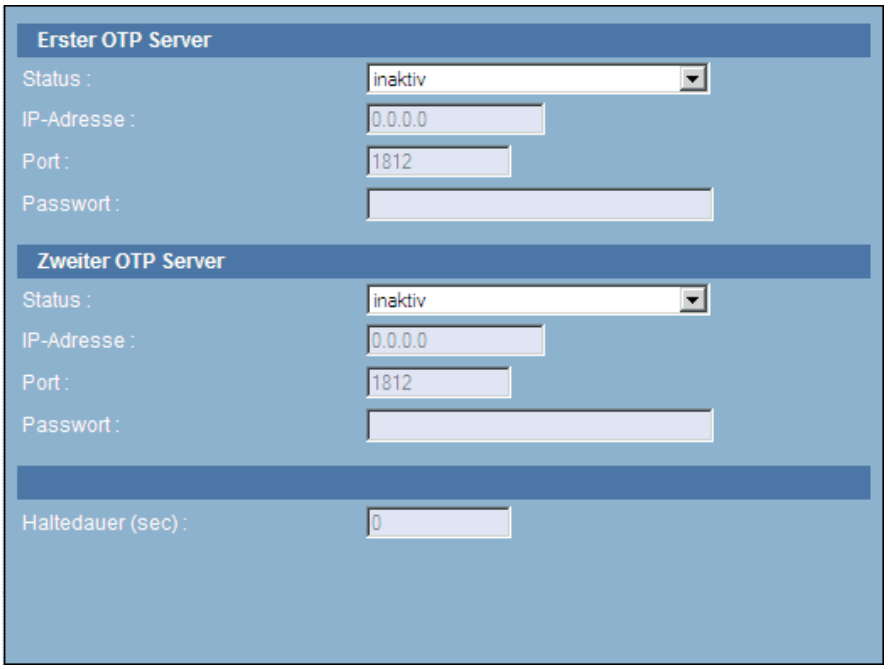
Port: Die Port-Nummer des RADIUS Accounting Servers. Ändern Sie diesen Wert nur, wenn der RADIUS Server unter einer anderen Port-Nummer als der hier angegeben Standard-Nummer läuft.

Passwort: Passwort für den RADIUS Accounting Server.

Wiederholungs-Intervall [RADIUS / Domain-Gruppen]

Der Zeitabstand in Sekunden, in denen Anfragen an den RADIUS Server bei Nichtbeantwortung wiederholt werden.

OTP [Domain-Gruppen]



Wird ein OTP-Token verwendet, so kann statt “Benutzer” und “Passwort” für die Einwahl an einem NAS oder VPN Gateway PIN und Passwort des Tokens eingegeben werden. (Wofür der OTP-Token genutzt wird, wird im Telefonbuch des Clients unter “Verbindungssteuerung” angegeben.)

Funktionsweise:

Für das VPN Gateway können zwei Arten des RADIUS Servers unterschieden werden:

– Interner RADIUS Accounting Server zur Client-Konfiguration im VPN Gateway

– Externer (Internet) oder interner OTP Server zur Client-Authentisierung (= RADIUS Authentisierungs-Server)

Der Client baut die Verbindung zum Gateway auf und leitet die Authentisierungsphase ein. Ein Authentisierungsantrag (Request) wird an den OTP Server (RADIUS Authentisierungs-Server) geschickt. Die IP-Adresse des OTP Servers hängt vom Benutzer-Suffix ab (z.B. @firma2). Nach der Authentisierungsphase wird ein zweiter Antrag, diesmal an den internen RADIUS Server gesendet. Auf dem internen RADIUS Server wird das Passwort für die Benutzerprofile identisch zur Benutzerkennung vergeben, da die Authentisierung bereits vom OTP Server durchgeführt wurde.

Status: Der Status des OTP Servers kann aktiv oder inaktiv geschaltet werden.

IP-Adresse: Die IP-Adresse des OTP Servers

Port: Der Port des OTP Servers

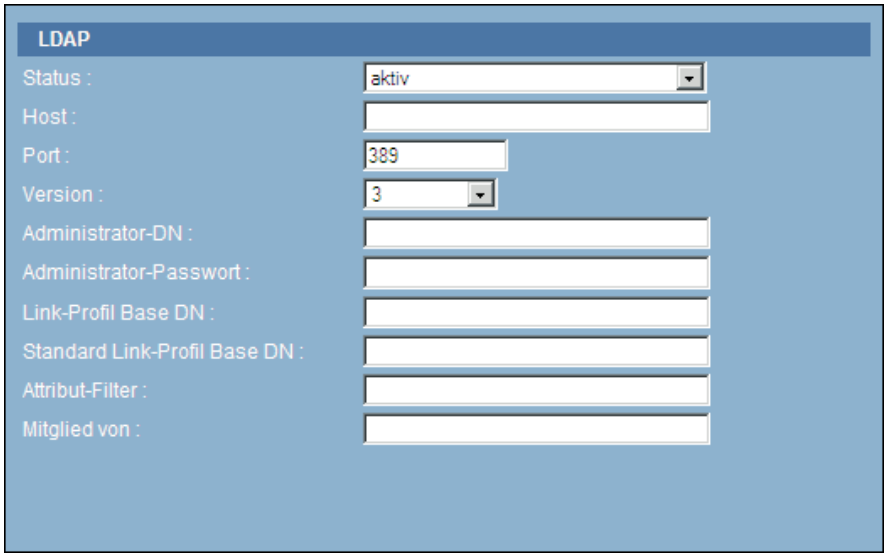
Passwort: Das Passwort für diesen OTP Server

OTP-Haltedauer (sec) [OTP / Domain-Gruppen]

Falls gewünscht wird, dass das One-Time-Passwort für eine zu bestimmende Zeitdauer seine Gültigkeit behält, so kann dieses Zeitintervall als “OTP-Haltedauer (sec)” konfiguriert werden. Die in Sekunden zu bestimmende Haltedauer läuft ab dem Zeitpunkt der Ersteinwahl ab.

Aus Sicherheitsgründen wird die gesamte PAP Verhandlung verschlüsselt übertragen. Dabei wird ein gemeinsames Passwort (shared secret) über Zufallstahlen generiert, das erneut abgefragt wird, wenn der Client sich innerhalb des Intervalls erneut einwählt.

LDAP [Domain-Gruppen]



Mit LDAP-Datenbanken kann die Benutzerverwaltung sehr komfortabel gestaltet werden. LDAP Server sind speziell zur zentralen Verwaltung einer großen Anzahl von Hosts eingerichtet und an RFC-Protokoll-Standards orientiert.

LDAP-Datenbanken werden auf einem Server gehalten, d. h. alle Benutzer-Daten sind zentral auf dem LDAP Server gespeichert.

In LANs mit mehreren Routern, kann jeder Router auf den Datenbestand des LDAP Servers zugreifen. Dies bedeutet, dass Benutzer aus dem WAN immer mit der gleichen ID und dem gleichen Passwort, egal über welchen dieser Router, auf jeden Host und jede Applikation dieses LANs zugreifen können.

Für die LDAP-Konfiguration stehen zwei Parameterfelder zur Verfügung, “LDAP Server” und “Backup LDAP Server”. Die Parameter beider Parameterfelder sind identisch, wobei diejenigen für den Backup LDAP Server nur einzutragen sind, wenn sich in Ihrem LAN ein zweiter LDAP Server befindet.

Wichtig: Nachdem Sie die LDAP-Konfiguration durchgeführt haben, müssen die Dienste neu gestartet werden.

Status [LDAP Server / Domain-Gruppen]

Mit dem Status bestimmen Sie, ob ein LDAP Server für die Zugriffssteuerung genutzt wird (aktiv) oder nicht (nicht aktiv).

Host [LDAP Server / Domain-Gruppen]

Dies ist die IP-Adresse des Hosts vom LDAP Server. Statt der IP-Adresse kann auch der symbolische Namen des Hosts eingegeben werden, wie er vom Domain Name Server kommt.

Port [LDAP Server / Domain-Gruppen]

Die Port-Nummer des LDAP Servers. Ändern Sie diesen Wert nur, wenn der LDAP Server unter einer anderen Port-Nummer als der hier angegeben Standard-Nummer (LDAP 389) läuft.

Version [LDAP Server / Domain-Gruppen]

Wählen Sie hier die LDAP-Version, mit der der LDAP Server läuft. Standard ist 2.

Administrator-DN [LDAP Server / Domain-Gruppen]

Dieser Distinguished Name (DN) gibt an, wo sich die Konfiguration für den Administrator auf dem LDAP Server befindet.

Zur Syntax von Distinguished Names: Distinguished Names werden von rechts nach links gelesen. Mögliche Einträge sind:

c= Country Code, z. B. DE für Deutschland

o= Organisation, z. B. NCP

cn= Gruppe, z. B. Filter. Die Anzahl der Gruppen ist unbegrenzt. Tragen Sie alle Gruppen ein, die zur Identifikation des Distinguished Names nötig sind.

Administrator-Passwort [LDAP Server / Domain-Gruppen]

Das Passwort des Administrators, um auf den LDAP Server zugreifen zu können.

Link-Profile Base DN [LDAP Server / Domain-Gruppen]

Suchpfad, unter dem die benutzer-spezifischen Konfigurationen der Link-Profile für diesen Network Access Server auf dem LDAP Server zu finden sind.

Zur Syntax von Distinguished Names: Distinguished Names werden von rechts nach links gelesen. Mögliche Einträge sind:

c= Country Code, z. B. DE für Deutschland

o= Organisation, z. B. NCP

cn= Gruppe, z. B. Filter. Die Anzahl der Gruppen ist unbegrenzt. Tragen Sie alle Gruppen ein, die zur Identifikation des Distinguished Names nötig sind.

Standard Link-Profil Base DN [LDAP Server / Domain-Gruppen]

Standard-Suchpfad, unter dem die Parameter der Link-Profile zu finden sind, die für alle Benutzer gleich sind.

Zur Syntax von Distinguished Names: Distinguished Names werden von rechts nach links gelesen. Mögliche Einträge sind:

c= Country Code, z. B. DE für Deutschland

o= Organisation, z. B. NCP

cn= Gruppe, z. B. Filter. Die Anzahl der Gruppen ist unbegrenzt. Tragen Sie alle Gruppen ein, die zur Identifikation des Distinguished Names nötig sind.

Bitte beachten Sie:

Die Verzeichnisstrukturen für die Konfigurationen der Link-Profile werden nach folgender Priorität ausgelesen:

1. “Link-Profil Base DN”, wenn keine Konfigurationsdaten gefunden werden,

dann:

2. “Standard Link-Profil Base DN”, wenn keine Konfigurationsdaten gefunden werden,

dann:

3. Standard-Konfiguration (wie in Attribut-Datei ncprtr\ldap\mpr.at.ncp.conf beschrieben)

Attribut-Filter

Der Filter dient der Einschränkung bei der LDAP-Suche. Mit ihm werden zusätzliche Bedingungen für die LDAP-Abfrage definiert.

Nur Benutzer, die dieses Attribut besitzen, bekommen VPN-Zugang.

Ist kein LDAP-Attribut gesetzt, ist der Filter nicht aktiv, d. h. alle LDAP-Benutzer bekommen VPN-Zugang.

Die Syntax entspricht der LDAP-Spezifikation. Beispiel:

```
(attr1=TRUE) oder
(&(attr1=TRUE)(attr2=2))
```

Mitglied von

Der hier eingegebene String wird mit dem Inhalt des Attributs "Memberof" im Active Directory Server verglichen. Bei Übereinstimmung bekommt der Benutzer aus dem ADS VPN-Zugang.

Ist kein String eingegeben, ist der Filter nicht aktiv, d. h. alle Benutzer aus dem ADS bekommen VPN-Zugang.

Syntax-Beispiele:

Übereinstimmung mit vollen Namen:

```
cn=VPN Gruppe, dc=myCommany, dc=de
```

Bei Verwendung von Wildcards und Übereinstimmung mit Namensanfang:

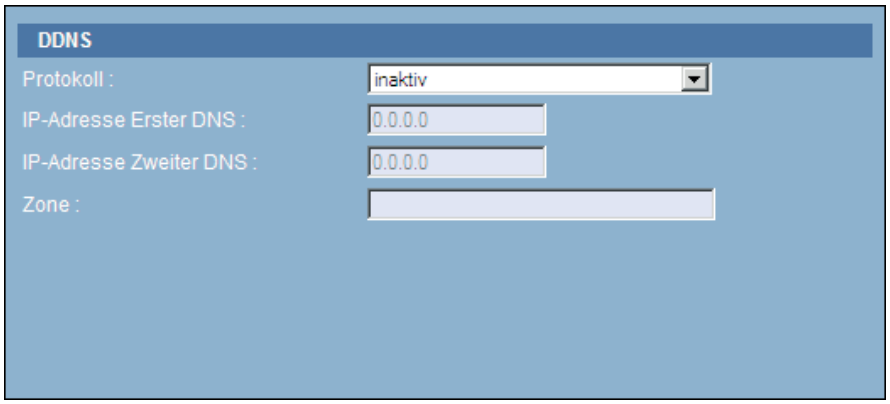
```
cn=VPN Gruppe*
```

Bei Verwendung von Wildcards und Übereinstimmung mit einer Zeichenfolge innerhalb des Namens:

```
*VPN*
```

DDNS [Domain-Gruppen]

DDNS beschreibt das dynamische Update eines DNS Servers. Über das DDNS-Protokoll wird das dynamische Update des DNS-Servers abgewickelt: Nachdem sich ein Benutzer mit dem VPN Gateway verbunden hat und eine IP-Adresse erhalten hat, wird diese an den DNS-Server inklusive DNS-Name und Domäne (Zone) übermittelt. Bei einem Verbindungsabbau (Disconnect) wird die Adresse dort wieder gelöscht.



Protokoll [DDNS / Domain-Gruppen]

Hier wählen Sie das DDNS-Protokoll.

DDNS = dynamisches DNS-Protokoll (standard)

inaktiv = das dynamische Update des DNS Servers ist ausgeschaltet

IP-Adresse erster / zweiter DNS Server [DDNS / Domain-Gruppen]

Tragen Sie hier die IP-Adressen des oder der DNS Server ein, für die das dynamische Update gelten soll.

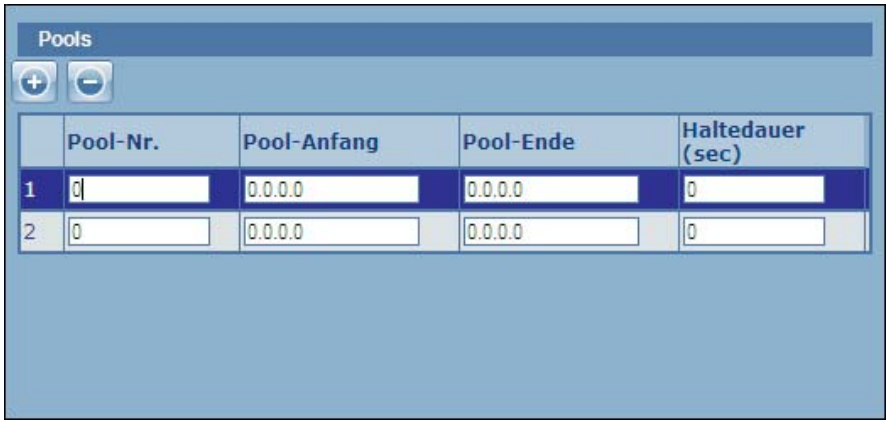
Zone [DDNS / Domain-Gruppen]

Anhand der hier eingetragenen Zone erkennt der Domain Name Server, dass er für die gleiche Zone zuständig ist. Die Zone beschreibt einen Adressbereich (Domäne), in dem sich der DNS Server und das VPN Gateway befinden, zum Beispiel “ncp.de”.

Pools [Domain-Gruppen]

Das VPN Gateway kann jedem Client, der sich zu ihm verbindet, automatisch eine freie IP-Adresse für eine Session aus einem Pool zuweisen.

Ob für den Link eine feste IP-Adresse oder ein bestimmter Pool verwendet werden soll, definieren Sie unter “Link-Profile / Routing”. Dort geben Sie die entsprechende Pool-Nr. an.



Pool-Nr. [Pools / Domain-Gruppen]

Über die Pool-Nummer wird dem Link-Profil unter “Routing” der entsprechende IP-Adress-Adressbereich zugewiesen.

Pool-Beginn / Ende [Pools / Domain-Gruppen]

Bitte beachten Sie:

– dass die Adress-Bereiche der Pools sich nicht überschneiden dürfen

– dass alle IP-Adressen im Bereich des IP-Netzes (WAN) liegen müssen

– dass auch feste IP-Adressen der Link-Profile nicht im Bereich eines Pools liegen dürfen

Haltedauer [Pools / Domain-Gruppen]

Ist für ein Link-Profil ein IP-Adressen-Pool unter “Link-Profile / Routing” selektiert und wird ein HA-Server mit Load Balancing verwendet, sollte der Client immer zu dem Gateway verbunden werden, aus dessen IP-Pool er seine IP-Adresse erhalten hat. Um dies zu gewährleisten kann in den Profil-Einstellungen des Clients unter “HA-Unterstützung” der Parameter “Zuletzt zugewiesenes Gateway benutzen” aktiviert werden. Wird diese Option genutzt, muss an dieser Stelle am Gateway die Haltedauer definiert werden.

Mit der Haltedauer ist es möglich, eine IP-Adresse aus einem Pool für einen bestimmten Benutzer zu reservieren. Die Zeitspanne für die Reservierung wird hier bestimmt. Für jeden Pool kann eine bestimmte Haltedauer eingestellt werden. Wählt sich ein Benutzer innerhalb der Haltedauer erneut ein, wird ihm dieselbe IP-Adresse zugewiesen.

Zertifikats-Überprüfung [Domain-Gruppen]

Eine Gruppe definiert sich über den “Suffix”, über den alle Gruppenmitglieder gleichermaßen verfügen (siehe: Domain-Gruppen / Allgemein). Eine zusätzliche gruppenspezifische Differenzierung kann hier über weitere Inhalte und die ausstellende Zertifizierungstelle (CA) der Benutzer-Zertifikate erfolgen.

Zertifikatsinhalte [Zertifikats-Überprüfung / Domain-Gruppen]

Land (C)

Bundesland (ST)

Ort (L)

Firma (O)

Abteilung (OU)

Domain Component (DC)

Alle Eintragungen, die zu diesen Zertifikatsinhalten gemacht werden, müssen im eingehenden Benutzer-Zertifikat eines Gruppenmitglieds enthalten sein, sonst erhält der Benutzer keinen Zugang.

Nur wenn die hier definierten Einträge mit den Einträgen des eingehenden Zertifikats übereinstimmen, wird das Zertifikat mit dem Gruppen-Profil gekoppelt und der Benutzer dieses Zertifikats erhält Zugang zum Secure Server.

Ungültige eingehende Zertifikate werden in der Statistik angezeigt.

Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

```
CN    = Common Name / Name
S     = Surname / Nachname
G     = Given name / Vorname
T     = Title / Titel
O     = Organisation / Firma
OU    = Organisation Unit / Abteilung
C     = Country / Land
ST    = State / Staat, RegionL     =
Location / Stadt, Ort
email = E-mail
DC    = Domain Component
```

Konventionen für die Einträge:

– Je nach PKI-Umgebung und Hierarchie der angelegten Gruppen können die für die Gruppe eindeutigen Zertifikatsinhalte ausgewählt bzw. kombiniert werden.

– Die Inhalte müssen ohne das Kürzel und das Gleichheitszeichen (x=) vor dem Inhaltstext eingetragen werden. Z. B. bei “st= Bayern” wird zu Bundesland (st) nur eingetragen: Bayern.

– Mehrere Inhalte zu einer Rubrik können mit Semikolon “;” getrennt hintereinander eingetragen werden.

– Die Einträge können mit Wildcards “*” abgekürzt werden.

– Sind mehrere gleiche Einträge im Zertifikat vorhanden, so müssen alle Einträge durch “ AND ” getrennt, angegeben werden. z. B. “xxx AND yyy”

CA-Zertifikate [Zertifikats-Überprüfung / Domain-Gruppen]

– Erlaube alle CA-Zertifikate

Ist diese Einstellung aktiv, können die eingehenden Benutzer-Zertifikate von einer der CAs sein, deren Aussteller-Zertifikat am Server eingespielt ist.

– Erlaube nur die ausgestellten Zertifikate

Nach Klick auf diesen Auswahl-Button werden die am Secure Server gehaltenen CA-Zertifikate gezeigt. Hier kann durch Markierung der gewünschten CA-Zertifikate eingestellt werden, von welchen CAs die eingehenden Benutzer-Zertifikate ausgestellt sein müssen, damit das entsprechende Mitglied dieser Gruppe Zugang erhält.

Erfüllen z. B. die Zertifikatsinhalte alle Kriterien der Gruppenzugehörigkeit, ist das Zertifikat aber von einer CA ausgestellt, die für diese Gruppe nicht zuständig ist, erhält das Gruppenmitglied keinen Zugang.

Verbindung nur mit Hardware-Zertifikat erlaubt [Zertifikats-Überprüfung / Domain-Gruppen]

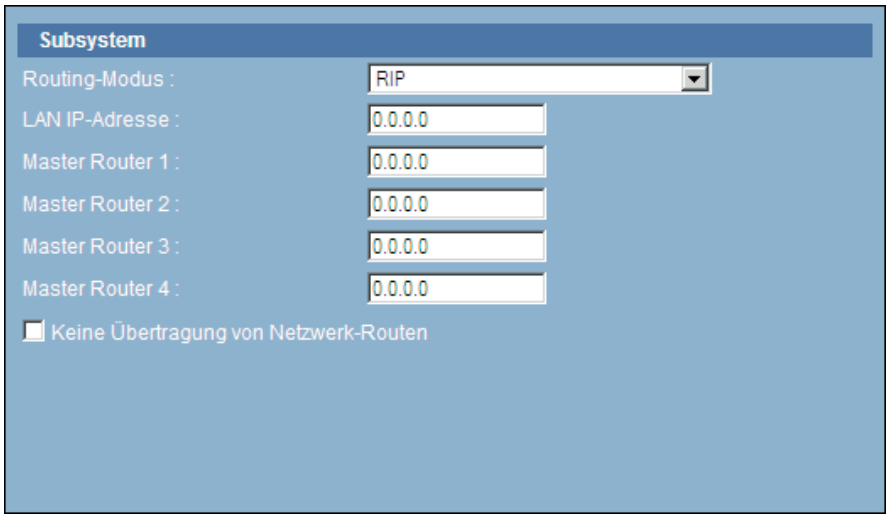
Bitte beachten Sie, dass das Hardware-Zertifikat nur bei IPSec-Verbindungen ausgewertet werden kann. Bei anderen Verbindungen wird ein eventuell konfiguriertes Hardware-Zertifikat ignoriert.

Die Benutzer (Mitglieder) einer Domain-Gruppe können dazu veranlasst werden jeweils ein Hardware-Zertifikat einzusetzen, indem dieser Schalter gesetzt wird, der die “Verbindung nur mit Hardware-Zertifikat erlaubt”. Ist dieser Parameter eingeschaltet, so muss in der IKE-Verhandlung ein Hardware-Zertifikat übertragen werden.

Subsystem [Domain-Gruppen]

Mit dem Subsystem wird hohes eintreffendes Datenaufkommen effizient weitergeleitet. Mehrere Network Access Server mit gleicher WAN IP-Adresse und identischen Benutzer-Konfigurationen (gleiche Link-Profile oder Nutzung gleicher LDAP / RADIUS Server) sind in diesem Subsystem gekoppelt und leiten die Datenströme der eingehenden Verbindungen weiter an einen dahinter liegenden Master Router, der die Daten im LAN verteilt.

Der Master Router auf der WAN-Seite muss die Routing-Modi ICMP redirect oder RIP unterstützen.



Routing-Modus [Subsystem / Domain-Gruppen]

Der Routing-Modus, ICMP Redirect oder RIP, der hier eingestellt wird, muss auch WAN-seitig vom Master Router unterstützt werden. (siehe: Subsystem)

Wenn ein VLAN zur Weiterleitung der Daten genutzt werden soll, muss als Routing-Modus “RIP” gesetzt werden.

LAN IP-Adresse [Subsystem / Domain-Gruppen]

Dies ist die LAN-seitige IP-Adresse des NCP Network Access Servers, der mit identischer Benutzer-Konfiguration parallel zu einem zweiten oder weiteren VPN Gateway zwischen WAN und Master Router gekoppelt ist. Er leitet die Daten eingehender Verbindungen weiter zum Master Router.

Um die Weiterleitung über VLAN nutzen zu können, muss hier die Adresse eines Netzes für VLAN eingetragen werden. Die Adresse wird vom Netz-Administrator vorgegeben.

Master Router [Subsystem / Domain-Gruppen]

Dies ist die WAN-seitige IP-Adresse des Master Routers. Der Master Router leitet die Daten der VPN Gateways weiter ins LAN.

Um die Weiterleitung über VLAN nutzen zu können, muss hier die Adresse des Master Router 1 eingetragen werden.

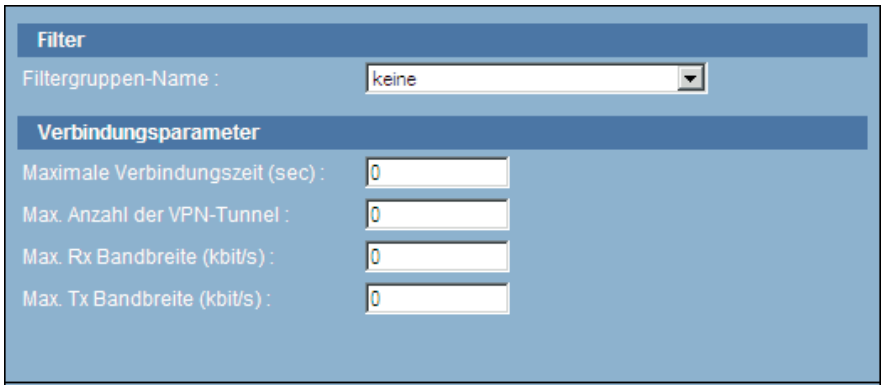
Keine Übertragung von Netzwerk-Routen

Wird diese Funktion eingeschaltet, so werden keine Netzwerk-Broadcasts von Remote-Netzen übertragen (RIP-Informationen).

Restriktionen [Domain-Gruppen]

Filtergruppen-Name [Restriktionen / Domain-Gruppen]

Anstatt Filter bzw. Filtergruppen den Mitgliedern einer Domain-Gruppe einzeln zuzuordnen, kann hier eine Filtergruppe ausgewählt werden, die für alle Mitglieder der Domain-Gruppe gelten soll.



Max. Verbindungszeit (sec) [Restriktionen / Domain-Gruppen]

In dieses Parameterfeld kann eine Zeitspanne in Sekunden eingetragen werden (Null besitzt keine Gültigkeit). Diese Zeitspanne bestimmt die maximale Verweildauer für den Benutzer im Firmennetz. Unabhängig davon ob eine Datenübertragung stattfindet oder nicht, wird die Verbindung abgebaut, sobald die maximale Verbindungszeit erreicht ist.

Die maximale Verbindungszeit kann auf drei Ebenen eingestellt werden:

– linkspezifisch unter **Link-Profile / Verbindungssteuerung** (gilt nur für den jeweiligen Benutzer)
– gruppenspezifisch unter **Domain-Gruppen / Allgemein** (gilt für alle Benutzer der jeweiligen Gruppe)
– global für dieses Gateway unter **Lokales System / Restriktionen** (gilt für alle Benutzer)

Auf allen drei Ebenen kann eine jeweils unterschiedliche maximale Verbindungszeit eingestellt werden. Für den aktuell ins Firmennetz eingewählten Benutzer wird immer nur die Verweildauer gestattet, die die höchste Priorität hat. Dabei hat die linkspezifische Konfiguration Priorität vor der gruppenspezifischen und diese vor der globalen.

Bitte beachten Sie, dass die Timeout-Funktion unter “Link-Profile / Line-Management” nur wirksam werden kann, wenn die dort eingetragene Zeitspanne kleiner ist als die maximale Verbindungszeit, gleich auf welcher Ebene sie gesetzt wurde.

Maximale Anzahl der VPN-Tunnels [Restriktionen / Domain-Gruppen]

Mit diesem Parameter kann die Anzahl der für die jeweils konfigurierte Domain-Gruppe gleichzeitig genutzten VPN-Tunnels begrenzt werden.

Maximale Bandbreite (kbit/s) [Restriktionen / Domain-Gruppen]

Mit diesem Parameter kann die maximal zur Verfügung stehende Bandbreite pro Benutzer in kBits/sec eingetragen werden (Null besitzt keine Gültigkeit). Damit kann unabhängig vom Verbindungsmedium der entfernten Clients die zentralseitig verfügbare Bandbreite für alle Benutzer gleichmäßig zugeteilt werden. Dabei wird unterschieden, ob die Bandbreite für ausgehenden (Tx) oder eingehenden (Rx) Datenverkehr genutzt wird.

Beachten Sie, dass die Zentralseite die Bandbreite unabhängig von der Richtung des Datenaufkommens zur Verfügung stellt. Ist die Bandbreite ausgeschöpft, kann kein weiterer Datenverkehr stattfinden.

Die Bandbreitenbeschränkung kann nur für TCP-Anwendungen genutzt werden.

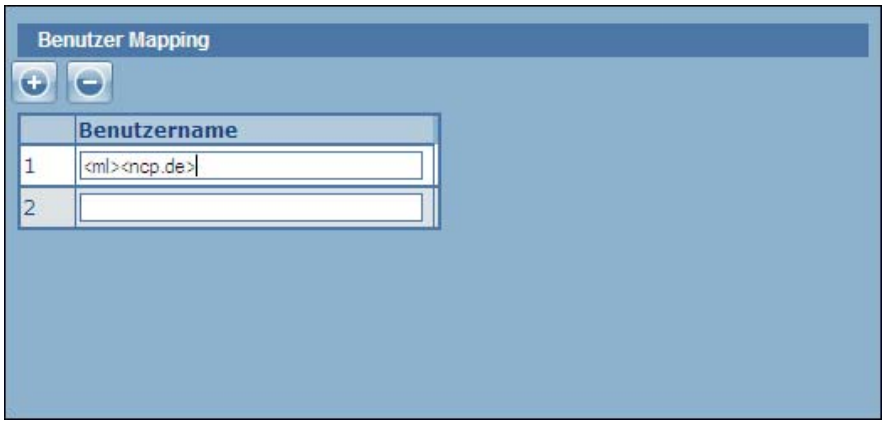
Die maximale Bandbreite kann auf drei Ebenen eingestellt werden:

– linkspezifisch unter **Link-Profile / Verbindungssteuerung** (gilt nur für den jeweiligen Benutzer)
– gruppenspezifisch unter **Domain-Gruppen / Allgemein** (gilt für alle Benutzer der jeweiligen Gruppe)
– global für dieses Gateway unter **Lokales System / Restriktionen** (gilt für alle Benutzer)

Auf allen drei Ebenen kann eine jeweils unterschiedliche maximale Bandbreite eingestellt werden. Für den aktuell ins Firmennetz eingewählten Benutzer wird immer nur die Bandbreite gestattet, die die höchste Priorität hat. Dabei hat die linkspezifische Konfiguration Priorität vor der gruppenspezifischen und diese vor der globalen.

Benutzer-Mapping [Domain-Gruppen]

Unabhängig vom Gruppen-Suffix der in der Client-Konfiguration (siehe: Domain-Gruppen / Allgemein / Suffix) festgelegt wurde, kann mit dem Benutzer-Mapping die Gruppenzugehörigkeit geändert werden. Dies erfolgt dynamisch ohne Restart der Dienste.



Benutzername [Domain-Gruppen]

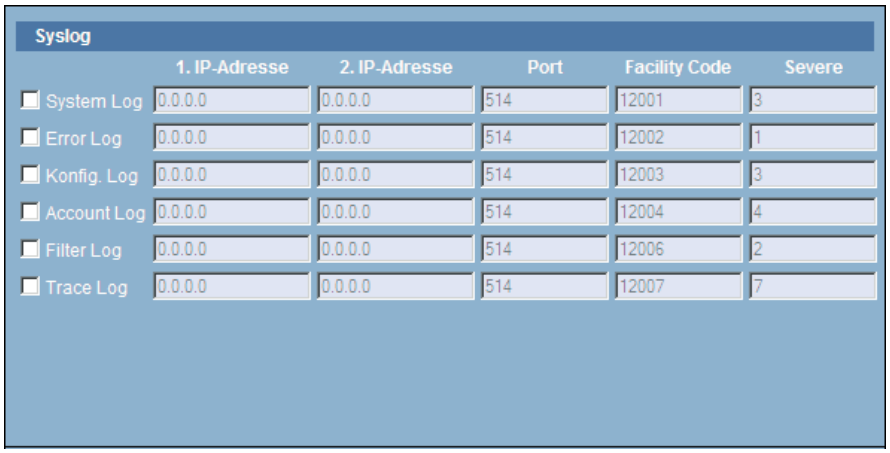
Tragen Sie VPN-Benutzername und Gruppen-Suffix in spitzen Klammern ein, dann wird der Benutzer der Gruppe mit dem eingetragenen Suffix zugeordnet.

```
<Name> <Gruppen-Suffix>
```

Achten Sie auf Groß- und Kleinschreibung!

Syslog [Domain-Gruppen]

Nach Konfiguration dieses Parameterfelds werden Log-Meldungen an einen Syslog Server Ihrer Wahl übertragen. Auf Syslog Servern (Unix) werden alle systemrelevanten Meldungen verwaltet.



Log-Meldungen

Wenn Sie Log-Meldungen an einen Syslog Server senden wollen, setzen Sie einen Haken hinter die entsprechende Log-Datei.

Log-Ausgaben können gruppenspezifische Syslog Server verwenden.

Trace Log kann nur in der Standard-Gruppe (Default Group) konfiguriert werden.

IP-Adresse (Syslog Server)

Mit der IP-Adresse wird der Syslog Server angesprochen.

Port (Syslog Server)

Standardmäßig wird der Syslog Server über den UDP Port 514 angesprochen.

Facility Code

Über den Facility Code wird die Log-Datei am Syslog Server identifiziert.

Severity

Die eingetragene Zahl bestimmt ob bereits leichte Fehler (kleine Zahl) oder erst schwerwiegende Fehler (große Zahl) übertragen werden.

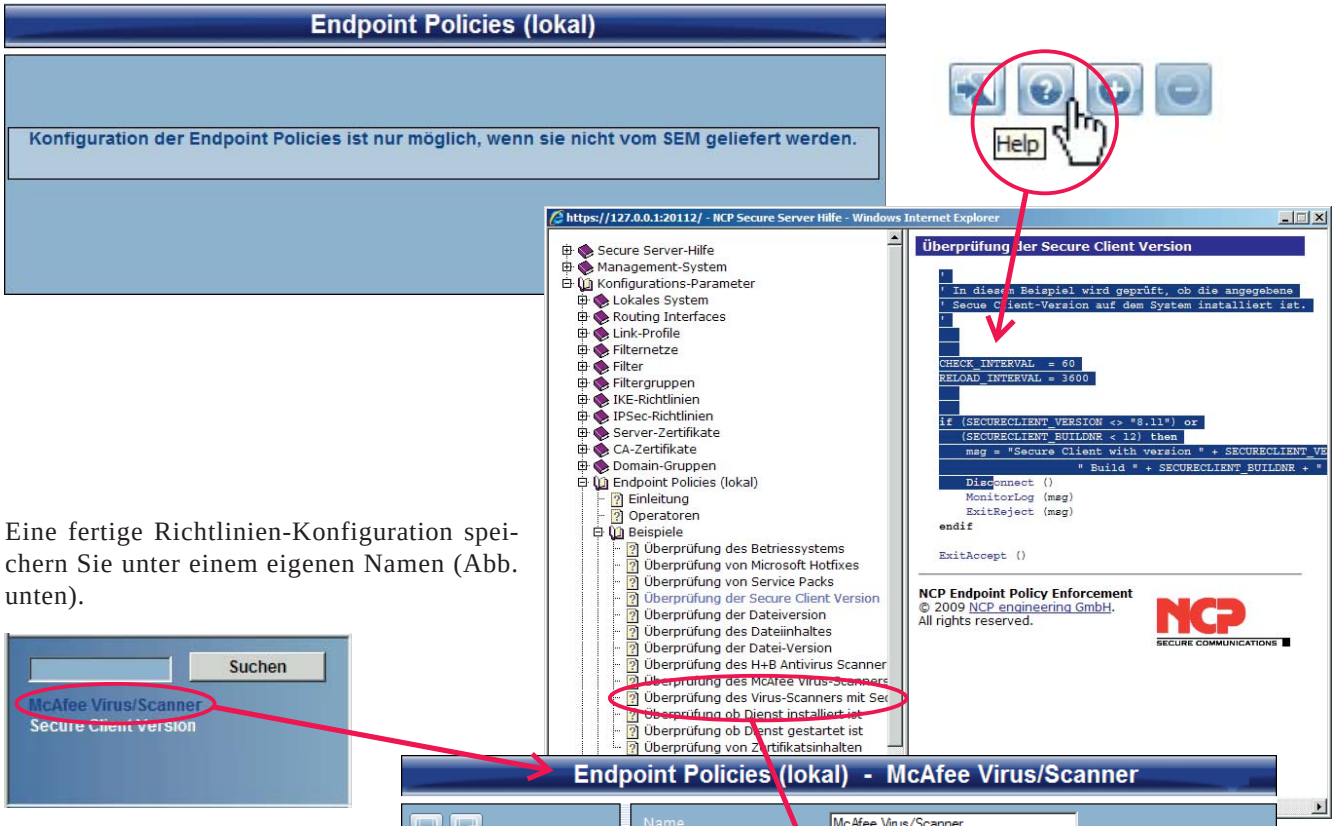
Endpoint Policies (lokal)

Wenn Sie die Richtlinien für die Endpoint Security vom Management Server übernehmen, können lokal keine Policies angelegt werden (Abb. unten links)!

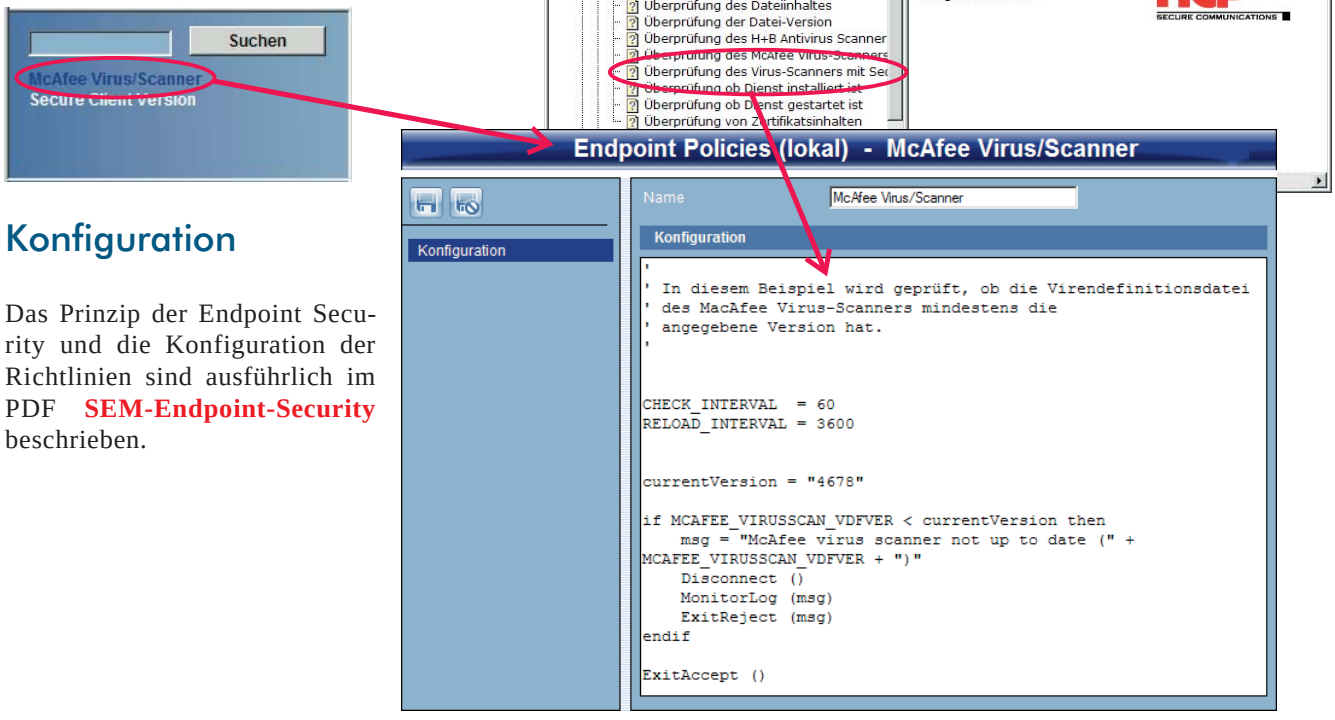
Nur wenn die Funktion **Endpoint Policies Download** unter “Lokales System” deaktiviert ist, können hier Policies konfiguriert werden werden!

Wenn Sie eine neue lokale Richtlinie anlegen möchten, öffnen Sie die Online-Hilfe mittels Button (Abb. unten rechts).

Aus der Online-Hilfe können Beispiele, Konstante etc. entnommen und in die Server-Konfiguration kopiert werden.



Eine fertige Richtlinien-Konfiguration speichern Sie unter einem eigenen Namen (Abb. unten).



Konfiguration

Das Prinzip der Endpoint Security und die Konfiguration der Richtlinien sind ausführlich im PDF **SEM-Endpoint-Security** beschrieben.

SSL VPN

Das NCP Gateway stellt die SSL VPN-Funktionalität zur Verfügung. Am Benutzer-PC muss, um diese Funktionalität nutzen zu können, keine VPN Client-Software installiert werden. Voraussetzung am Anwender-PC ist lediglich ein SSL-fähiger Browser mit Java-Installation.

Prinzip der SSL VPN-Verbindung

Der Anwender-PC verbindet sich mit dem Browser über HTTPS zum Firmen-Gateway und gelangt über die Gateway-Adresse auf eine Login-Seite, wo sich der Benutzer mit Passwort und Benutzername authentisieren muss.

Passwort und Benutzername können die gleichen sein, wie für einen optional zusätzlich zu installierenden VPN Client. Auch kann die Authentisierung über Zertifikat erfolgen, das dann am Browser eingespielt worden sein muss.

Wie die Authentisierung stattzufinden hat, wird am Firmen-Gateway konfiguriert, wo auch wie bisher die weitere Parametrisierung zur Rechtestruktur für den Zugriff auf das Firmennetzwerk stattfindet.

Das Aussehen der Login-Seite kann firmenspezifisch gestaltet werden, wobei die von NCP vorgegebenen Eingabefelder (für Passwort und Benutzername) beibehalten werden müssen.

Nach der erfolgreichen Authentisierung öffnet sich im Browser eine Menü-Seite (Portal), über die der Anwender aus einer (über das Gateway zu konfigurierenden Liste) die gewünschte Anwendung auswählen kann.

Je nach gewählter Anwendung wird (für den Anwender im Hintergrund) vom Gateway eine Verbindung hergestellt (z. B. zu Web-Server, Terminal-Server, File-Server) und die entsprechende Applikation über die Browser-Oberfläche gestartet.

Anwendungen für SSL VPN

Dem Benutzer öffnet sich nach der Authentisierung eine Menü-Seite mit verschiedenen möglichen Anwendungen. Die grafische Gestaltung der Menü-Seite kann firmenspezifisch verändert werden, nicht aber die Funktionsfelder. Welche Anwendungen dem Benutzer auf der Menü-Seite zur Verfügung gestellt werden, kann in der Gateway-Konfiguration des Listeners, der die Verbindungen von den Browsern über IP-Adresse und Port entgegen nimmt, definiert werden. Prinzipiell können drei Anwendungsbereiche unterschieden werden.

Web-Proxy (Anwendung in Browser-Fenster)

Statt direkt über HTTP auf den Web-Server zuzugreifen, wählt sich der remote PC im SSL-Tunnel über HTTP am Gateway an und erhält nach der Authentisierung eine Menü-Seite im Browser, die verschiedene Web-basierte Applikationen zur Wahl stellt (z.B. Internet Banking, Intranet). Das Gateway stellt die Verbindung zum firmeninternen Web-Server über HTTPS her. Web-Proxy-Anwendungen können u.a. genutzt werden für: Intra-Web, Nagios, Web-Interfaces zur Administration, Surfen über die Firmen-Firewall, Web-E-Mail.

Port-Weiterleitung (Anwendung in DOS-Box oder eigenem Anwendungs-Fenster)

Über die Technik des Port-Forwarding können im SSL-Tunnel auch TCP-Verbindungen z.B. zu einem SSH- oder Terminal-Server hergestellt werden. In der Gateway-Konfiguration erfolgt die Zuordnung eines Ports zum Ziel-Port und der Ziel-Adresse am Server. Dies erfolgt durch den Download eines Applets und die Installation eines SSL VPN Thin Clients. Port-Forwarding-Anwendungen können u.a. genutzt werden für: E-Mail Clients, SSH, Telnet, FTP.

Remote File Access (Anwendung in eigenem Anwendungs-Fenster)

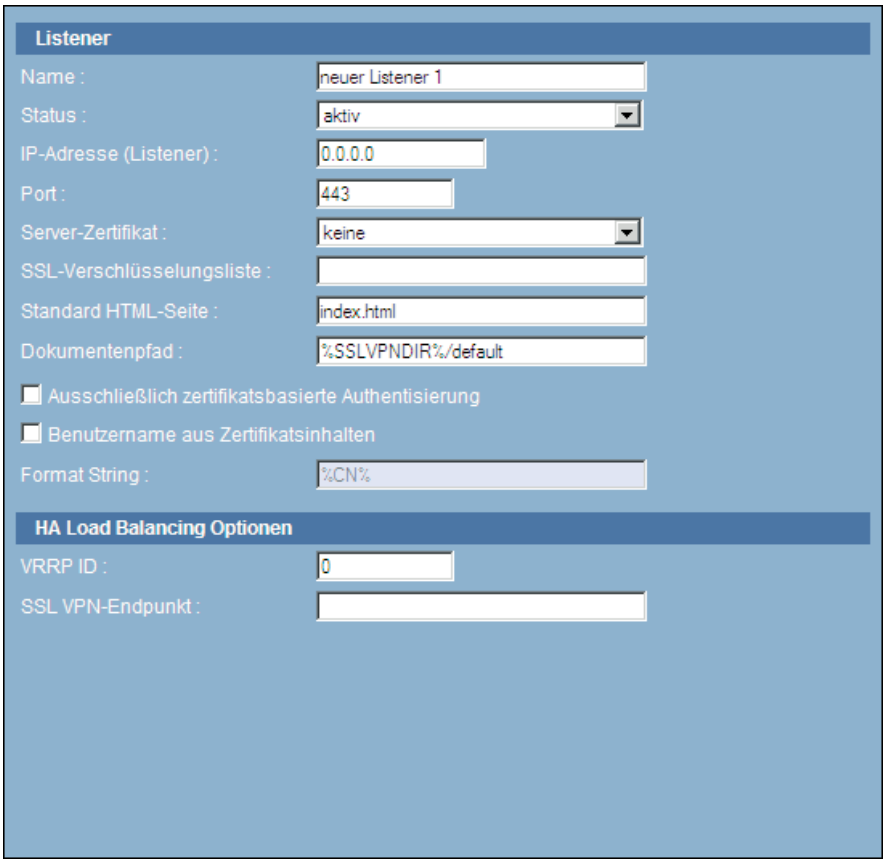
Um über den SSL-Tunnel auf einen File-Server zugreifen und dabei die Funktionen des Datei-Handlings eines “Explorers” nutzen zu können, wird im Web-Browser eine entsprechende Oberfläche emuliert, die die Datei-Struktur der File-Server-Seite zeigt. Über diese Oberfläche ist ein File-Transfer von und zum Server im Firmennetz möglich.Dateioperationen, wie Anzeigen, Herunterladen, Hochladen und Anlegen von Verzeichnissen, sind möglich.

SSL VPN-Konfiguration

Im folgenden werden die zur SSL VPN-Funktionalität wesentlichen Parameter beschrieben.

Listener

Der Listener nimmt die Verbindungen von den Browsern über IP-Adresse und Port entgegen, die bei der Einwahl mit dem Browser als URL in der Form “hostname:port” eingegeben werden.



Nach Verbindungsaufbau und anschließender Authentisierung auf der Login-Seite, stellt der Listener dem Anwender die Applikationen auf der jeweils zu konfigurierenden Menü-Seite zur Verfügung. Je nach Gateway-Konfiguration können bis zu 32 IP-Adressen bei gleichem (Standard-) Port für (32) verschiedene Listener genutzt werden. Jeder dieser Listener kann dem Anwender eine andere, z.B. firmenspezifische Menü-Seite öffnen, so dass die Mandantenfähigkeit auch für die SSL VPN-Funktionalität des Gateways gewährleistet ist. Die Anzahl der Listener bzw. der Menü-Seiten kann durch Änderung des Ports noch erhöht werden (siehe dazu weiter unten “Port”). Die mitgelieferte Menü-Seite kann über den hier zu konfigurierenden Listener hinsichtlich der Anzahl der Anwendungen verändert werden, wie auch grafisch so modifiziert werden, dass sie der Corporate Identity einer Benutzer- oder Mandantengruppe entspricht (siehe unten “Default Document Path”). Zur Konfiguration selektieren Sie den Standard-Listener 443 im Konfigurationsbaum.

Name [Listener]

Der Name des Listeners ist beliebig modifizierbar.

Status [Listener]

Der Status muss “aktiv” geschaltet sein, damit die Verbindung von Browser zu Gateway hergestellt werden kann. Die Funktion kann dynamisch eingesetzt werden. Das Gateway muss nicht neu gebootet werden.

IP-Adresse (Listener)

Je nachdem wieviele IP-Adressen dem Gateway zur Verfügung stehen und welcher Port dem Anwender für seine URL mitgeteilt wurde, kann mit der Konfiguration die Zuteilung von Menü-Seiten erfolgen.

0.0.0.0

Der Listener hört auf alle IP-Adressen, die für dieses Gateway zur Verfügung stehen, wenn gleichzeitig der Port in der URL des Browsers mit dem unten konfigurierten Port übereinstimmt.

n.n.n.n

Der Listener hört nur auf die genau zutreffend konfigurierte IP-Adresse einschließlich unten konfiguriertem Port. D. h. die im Browser des remote PCs eingegebene URL muss genau mit IP-Adresse und Port in diesem Parameterfeld übereinstimmen, dann erhält der Anwender die hier hinterlegte Menü-Seite.

Port [Listener]

Der Standard-Port 443 muss nicht eigens im Browser angegeben werden. Er kann jedoch nur verwendet werden, wenn er frei ist. In einer DOS-Box kann mit dem Kommando

```
netstat -a -n
```

geprüft werden, ob der SSL-Port 443 für SSL VPN noch frei ist.

Ist dieser Port nicht frei, so muss genau der Dienst beendet werden, der diesen Port benutzt. Alternativ

kann aber auch ein anderer freier Port verwendet werden, der dann jedoch im Browser des remote PCs bei der URL hinter dem Hostnamen explizit angegeben werden muss:
`https://hostname:port`

Server-Zertifikat [Listener]

Selektieren Sie hier eines der Server-Zertifikate, die in der Konfiguration bereitgestellt wurden (siehe: Konfiguration / Server-Zertifikat).

Bitte achten Sie darauf, dass der Common Name des Server-Zertifikats mit dem Hostnamen bzw. der IP-Adresse des SSL VPN Gateways übereinstimmt, da der Web Browser bei Nichtübereinstimmung einen Fehlerfall meldet. Das Fehlerprotokoll befindet sich im Trap.log. Pro IP-Adresse (max. 32) muss Common Name und Hostname unterschieden werden.

SSL-Verschlüsselungsliste [Listener]

Mit der SSL-Verschlüsselungsliste kann definiert werden, welche Algorithmen zur SSL-Verschlüsselung in welcher Weise genutzt werden sollen.

Die Zeichenfolge besteht aus einer Reihe optionaler Regeln zur SSL/TLS-Verschlüsselung, die mit der remote Seite in der SSL/TLS-Verhandlung ausgehandelt wird. Sie kann aus einem oder mehreren Strings bestehen, die durch Doppelpunkt (auch Komma oder Leerzeichen) getrennt sind. Unterstützt die remote Seite eine der hier verlangten Verschlüsselungen nicht, so kommt keine Verbindung zum Gateway zustande.

Die Zeichenfolge für die Verschlüsselungsregeln kann verschiedene Formen annehmen. Sie kann aus einer einzigen Ziffernfolge bestehen, wie RC4-SHA (Regeln, die RC4 und SHA1 benutzen, siehe unten “Erlaubte Zeichenfolgen und ihre Bedeutung”).

Sie kann aber auch aus einer Reihe von Ziffernfolgen bestehen, die einen bestimmten Algorithmus beschreiben oder einen bestimmten Typ repräsentieren. Z.B. repräsentiert SHA1 alle Schlüsselfolgen, die sich aus diesem Algorithmus ergeben, SSLv3 repräsentiert alle SSL v3-Algorithmen. Nur “TLSv1" bedeutet, dass nur mit TLS Version 1 verschlüsselt wird.

Reihen zu Verschlüsselungsregeln und einzelne Strings können operational und logisch mit dem Zeichen “+” kombiniert werden. Zum Beispiel beinhaltet SHA1+DES alle Verschlüsselungsoptionen der SHA1- und DES-Algorithmen.

Optional kann allen Ziffernfolgen das Zeichen “!”, das Zeichen “-” oder das Zeichen “+” vorangestellt werden.

Mit “!” werden die Verschlüsselungsregeln dauerhaft aus der Liste gelöscht. Sie können nur dann wieder in der Liste erscheinen, wenn sie explizit festgelegt werden.

Mit “-” werden die Regeln zwar aus der Liste gelöscht, sie können jedoch zu späteren Einsätzen wieder hinzugefügt werden.

Mit “+” werden die Regeln an das Ende der Liste gesetzt.

Wird keines dieser Zeichen verwendet, wird der String nur als Liste von Verschlüsselungen interpretiert, die der aktuell präferierten Liste angehängt wird. Verschlüsselungsoptionen, die bereits einmal in der Liste aufgeführt wurden, werden ignoriert.

Zusätzlich kann mit dem String @STRENGTH, gleich an welcher Stelle eingefügt, die Regelliste nach der Schlüssellänge der jeweiligen Algorithmen sortiert werden.

Erlaubte Zeichenfolgen und ihre Bedeutung:

DEFAULT: Die Standard-Regelliste. Um Zeit zu sparen, kann von dieser Zeichenfolge ausgegangen und die Regeln angepasst werden. Sie besteht aus: ALL:!ADH:RC4+RSA:+SSLv2:@STRENGTH.

COMPLEMENTOFDEFAULT: Ist enthalten in ALL aber nicht standardmäßig aktiviert. Aktuell ist dies ADH. Beachten Sie, dass diese Regel nicht eNULL abdeckt, die nicht in ALL enthalten ist (benutzen Sie COMPLEMENTOFALL wenn nötig).

ALL: Gültig sind alle Verschlüsselungsoptionen außer eNULL, welche explizit aktiviert werden muss.

COMPLEMENTOFALL: Gültig sind alle Verschlüsselungsoptionen die nicht mit ALL aktiviert werden, in der Regel nur eNULL.

HIGH: “High” Encryption Verschlüsselungsoptionen. Damit werden Verschlüsselungen mit mehr als 128 Bits verwendet.

MEDIUM: “Medium” Encryption Verschlüsselungsoptionen. Damit werden Verschlüsselungen mit 128 Bits verwendet.

LOW: “Low” Encryption Verschlüsselungsoptionen. Damit werden Verschlüsselungen mit 56 oder

64 Bits verwendet ausgenommen Export-Algorithmen.

EXP, EXPORT: Export Verschlüsselungs-Algorithmen. Beinhalten Algorithmen mit 40 und 56 Bits.

EXPORT40: 40 Bit Export Verschlüsselungs-Algorithmen.

EXPORT56: 56 Bit Export Verschlüsselungs-Algorithmen.

eNULL, NULL: Mit der Zeichenfolge “NULL” wird keine Verschlüsselung angeboten. Da hiermit keine Verschlüsselung eingesetzt wird und somit ein Sicherheitsrisiko besteht, ist dieser String solange nicht aktiv bis er explizit eingefügt wird.

aNULL: Hiermit wird keine Authentisierung angeboten, wie im anonymen DH-Algorithmus. Diese Verschlüsselungen sind durch eine “Man in the Middle”-Attacke angreifbar und werden deshalb normalerweise nicht eingesetzt.

kRSA, RSA: Verschlüsselungsoptionen, die RSA-Schlüsselaustausch nutzen.

kEDH: Verschlüsselungsoptionen, die ein vorübergehendes DH Key Agreement nutzen.

kDHr, kDHd: Verschlüsselungsoptionen, die DH Key Agreement und DH-Zertifikate nutzen, die von CAs mit RSA- und DSS-Schlüsseln gezeichnet sind. Nicht implementiert.

aRSA: Verschlüsselungsoptionen, die RSA-Authentisierung nutzen, z.B. RSA-Schlüssel tragende Zertifikate.

aDSS, DSS: Verschlüsselungsoptionen, die DSS-Authentisierung nutzen, z.B. DSS-Schlüssel tragende Zertifikate.

aDH: Verschlüsselungsoptionen, die DH-Authentisierung nutzen, z.B. DH-Schlüssel tragende Zertifikate. Nicht implementiert.

kFZA, aFZA, eFZA, FZA: Verschlüsselungsoptionen, die FORTEZZA Schlüsselaustausch, Authentisierung, Verschlüsselung oder auch alle FORTEZZA Algorithmen nutzen. Nicht implementiert.

TLSv1, SSLv3, SSLv2: TLS v1.0, SSL v3.0 oder SSL v2.0 Verschlüsselungsalgorithmen in dieser Reihenfolge.

DH: Regeln, die DH nutzen, inklusive anomymes DH.

ADH: Regeln, die anonymes DH nutzen.

AES: Regeln, die AES nutzen.

3DES: Regeln, die triple DES nutzen.

DES: Regeln, die DES nutzen (außer triple DES).

RC4: Regeln, die RC4 nutzen.

RC2: Regeln, die RC2 nutzen.

IDEA: Regeln, die IDEA nutzen.

MD5: Regeln, die MD5 nutzen.

SHA1, SHA: Regeln, die SHA1 nutzen.

Standard HTML-Seite [Listener]

Diese Seite erscheint, wenn in der URL keine weitere Seite angegeben ist. Sie verweist standardmäßig auf die Login-Seite. Diese Seite kann jedoch auch nach Bedarf modifiziert werden. Sie befindet sich im Installationsverzeihnis unter:
`<SecureServer\sslvpn\default\wwwroot\index.html>`
Bitte beachten Sie, dass die Originale aller Seiten, die Sie editieren, gesichert werden sollten. Außerdem sollten Ihre modifizierten Seiten ebenso an anderer Stelle gesichert sein, da diese Seiten bei jeder Neuinstallation und jedem Update von den unbearbeiteten Originalen überschrieben werden.

Dokumentenpfad [Listener]

Unter diesem Pfad befinden sich Script-, HTML- und Bilddateien, die von Ihnen nach Bedarf angepasst werden können:
`<SecureServer\sslvpn\default\def>`

Bitte beachten Sie, dass die Originale aller Seiten, die Sie editieren, gesichert werden sollten. Außerdem sollten Ihre modifizierten Seiten ebenso an anderer Stelle gesichert sein, da diese Seiten bei jeder Neuinstallation und jedem Update von den unbearbeiteten Originalen überschrieben werden.

Ausschließlich zertifikatsbasierte Authentisierung [Listener]

Wenn Sie nur eine zertifikatsbasierte Authentisierung zulassen, muss das Zertifikat am Browser des remote PCs eingespielt worden sein. (Dabei kann das PKCS#11-Modul des Browsers verwendet werden.) Dieses Zertifikat kann mit demjenigen identisch sein, das ein NCP Secure Client verwendet. Dieses Zertifikat wird für die SSL-Verhandlung herangezogen. (Benutzername und Passwort werden sind aus der Konfiguration des Link-Profils).

Zertifikate verwenden [Listener]

Zusätzlich kann ein Zertifikatsinhalt die Zugangsdaten Benutzername und Passwort ersetzen. Bei diesem Inhalt kann es sich um einen festen Wert (String aus Zeichen, die genau so im Zertifikat vorkommen) oder um einen Platzhalter für standardisierte Inhalte wie Name, Firma oder Land handeln. Wird diese Option genutzt, so entfällt die Login-Seite zur Eingabe von Benutzername und Passwort beim Verbindungsaufbau mit dem Browser.

Format String [Listener]

Der String des Zertifikatsinhalts wird als Variable eingetragen oder als fester Wert. Mögliche Variable sind:

```
%CN%          Common Name
%EMAIL%       E-Mail-Adresse%SURNAME%
Nachname
%GIVENNAME%   Vorname
%ORGUNIT3%    Organisation / Gruppe
%ORGUNIT2%    Organisation / Abteilung
%ORGUNIT%     Organisation
%ORG2%        Firmenname
%ORG%         Firmenname
%LOCATION%    Stadt / Ort
%STATE%       Bundesland / Provinz
%COUNTRY%     Land
%SERIALNR%    Seriennummer
```

Wird kein Format String konfiguriert, so muss beim Verbindungsaufbau Benutzername und Passwort eingegeben werden.

Ist ein String konfiguriert, so wird dieser beim Verbindungsaufbau verwendet.

HA Load Balancing-Optionen

Die Verbindungen von SSL VPN Clients können von einem HA-System entsprechend der aktuellen Auslastung verteilt werden. Dies erfolgt mittels einer vituellen IP-Adresse.

VRRP ID

Die ID ist frei wählbar zwischen 1 und 254. Die VRRP ID muss jeweils für das Paar der Gateways identisch sein, die als Master und Backup bzw. Primary und Secondary Gateway in einem HA-System fungieren. Entsprechend muss diese ID hier auch auf dem Routing Interface zugewiesen sein, an die die gemeinsame virtuelle IP-Adresse gebunden wird (siehe “Routing Interface / LAN-Adapter”).

SSL VPN-Endpunkt

Zum Load Balancing von SSL VPN-Verbindungen über eine VRRP-Adresse benötigen Sie zwei Listener-Konfigurationen pro Gateway. Die IP-Adresse des ersten Listeners ist die virtuelle VRRP-Adresse, die IP-Adresse des zweiten Listeners ist die physikalische Adresse des LAN-Adapters, die später auch Tunnel terminiert.

Als SSL VPN-Endpunkt tragen Sie nichts ein, wenn die IP-Adresse des Listeners die virtuelle VRRP-Adresse ist.

Als SSL VPN-Endpunkt tragen Sie die IP-Adresse des Listeners ein, die der physikalischen IP-Adresse des Gateways entspricht.

Der SSL VPN-Endpunkt gibt an, wie der Browser bei Einsatz des Load Balancing-Modus zu dem Listener eines Gateways mit der physikalischen IP-Adresse kommt. Sind die “HA Load Balancing-Optionen” per Lizenzschlüssel aktiv geschaltet, so erhält der Browser nach Anwahl an die virtuelle IP-Adresse vom Master Gateway per HTTPS Redirect die IP-Adresse des SSL VPN-Endpunkts die am Gateway mit der geringsten Auslastung hier eingetragen ist.

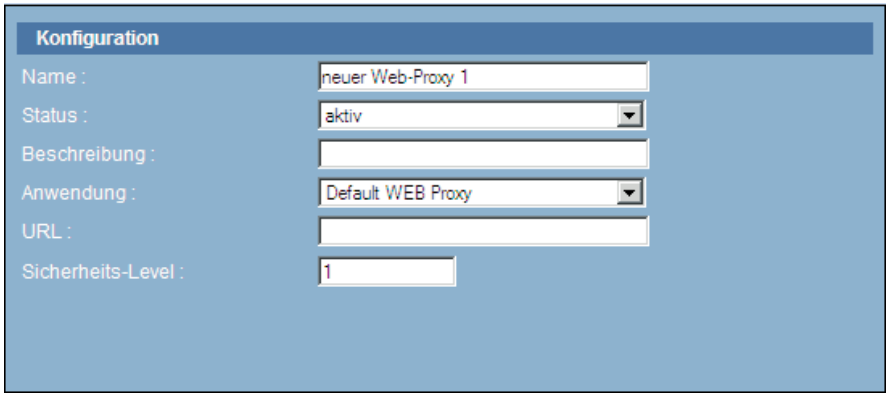
Dies gilt auch dann, wenn außer Master- und Backup Gateway weitere Gateways über den HA Manager für den Load Balancing-Modus konfiguriert wurden. Von diesen zusätzlichen Gateways wird kein VRRP-Modus benötigt, sondern nur der VPN-Modus (“Nur SSL VPN” oder “beide”) die VRRP-ID und die (physikalische) IP-Adresse. Unter Master- und Backup Gateway wird pro zusätzlichem Gateway jeweils ein weiterer Listener angelegt, der diese VRRP-ID und diese (physikalische) IP-Adresse bzw. diesen SSL VPN-Endpunkt als HA Load Balancing-Option enthält.

Der HA Server ist über die aktuelle Auslastung der LB Gateways informiert, die diese VRRP-ID besitzen. Er sucht unter den zugehörigen Gateways das mit der niedrigsten Auslastung aus und veranlasst das Master Gateway zu einem HTTPS Redirect, mit welchem dem Browser die Adresse des SSL VPN-Endpunkts übergeben wird, die zu dem Gateway mit genau dieser VRRP-ID und der geringsten Auslastung passt.

Der SSL VPN-Tunnel-Endpunkt ist in der Regel immer die offizielle physikalische IP-Adresse des Gateways, wenn es sich im Internet befindet. Wird die Verbindung über eine Firewall hergestellt, dann wird hier die Adresse eingetragen, die im Browser eingegeben werden muss, um das Gateway über die Firewall zu erreichen.

Web Proxies

Um eine Web Proxy-Anwendung zu konfigurieren, muss unter “SSL VPN” der Zweig “Web Proxies” selektiert und zunächst ein neuer Eintrag angelegt werden.



Soll über den Secure Server eine SSL-Verbindung zu einem Ziel-Web-Server (zugewiesen durch die URL) weitergeführt werden, so muss das Aussteller-Zertifikat des Web-Servers am Secure Server eingespielt werden (siehe: Konfiguration / Zertifikat, Verwendungszweck) und der Verwendungszweck für ausgehende SSL VPN Web-Proxy-Verbindungen erlaubt sein.

Name [Web Proxies]

Unter “Name” geben Sie einen Namen für diese Anwendung an. Dieser Name erscheint später als Applikation auf der Menüseite des Browser am Benutzer-PC.

Status [Web Proxies]

Der Status muss “aktiv” geschaltet sein, damit die Anwendung genutzt werden kann. Wird der Status auf “inaktiv” geschaltet, verschwindet diese Anwendung für Benutzer, die eine neue Verbindung zum Gateway herstellen, von der Menü-Seite. Die Verbindung für aktuelle Anwender bleibt bestehen.

Beschreibung [Web Proxies]

Diese Beschreibung erscheint im Browser hinter dem Namen der Applikation.

Anwendung [Web Proxies]

Eine Auswahl von Anwendungskonfigurationen ist als Datei im Installationsverzeichnis unter <Secure-Server\SSLVPN\WebProxy> mitgegeben. Die Konfigurationen können benutzerspezifisch modifiziert oder erweitert werden.

- Default Web Proxy
- Citrix Web Interface 4.5
- NCP Secure Server
- Microsoft Outlook Web Access 2007

URL [Web Proxies]

Hier wird die URL (Uniform Resource Locator) mit Protokoll, Hostname, Port und ggf. der Datei angegeben, die angezeigt werden soll, wenn später der Benutzer im Browser die entsprechende Applikation anklickt. Z. B.:
`http://172.16.15.46/exchange`

Sicherheits-Level [Web Proxies]

Der Security Level bezeichnet den Wert eines Regelwerks, das mindestens erfüllt sein muss, damit diese Anwendung im Start-Menü erscheint. Der hier einzutragende ganzzahlige Wert muss mit den Definitionen der Sicherheits-Richtlinien im Secure Enterprise Manager abgestimmt sein.

Single Sign-on

Single Sign-on kann dann eingesetzt werden, wenn die Web Server-Anwendung die gleichen Zugangsdaten benötigt wie der SSL VPN Client.

inaktiv: Normalerweise erfolgt die Anmeldung am Web Server über HTTP, wobei Benutzername und Passwort eingegeben werden müssen.

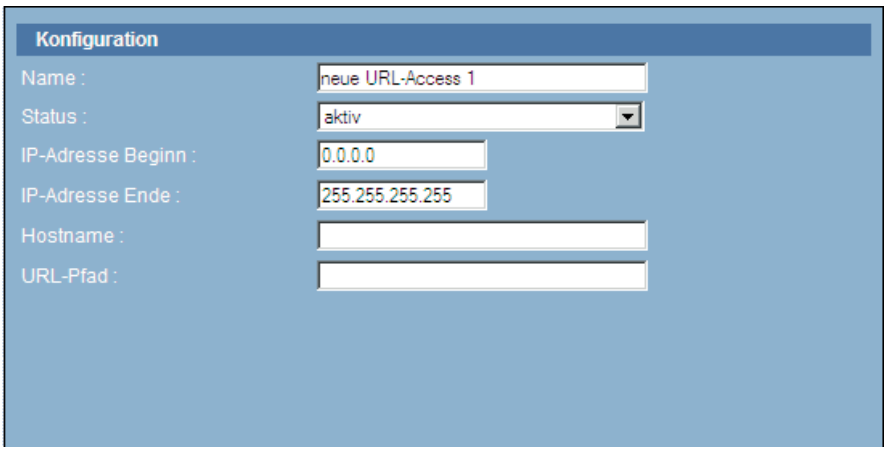
HTTP-Authentisierung: Wird Single Sign-on mit HTTP-Authentisierung aktiv geschaltet, so wird im Hintergrund SSL VPN Benutzername / Passwort zur Authentisierung verwendet.

Derzeit werden als Authentisierungsmethoden “digest” und “basic” unterstützt.

URL Access

Ein URL Access erweitert den Zugriffsbereich auf Web-Seiten, die durch die Web Proxy-Konfiguration vorgegeben wurden. Gelangt ein Benutzer auf eine HTML-Seite, die nicht im freigegebenen Bereich liegt, so erscheint ein entsprechender Fehlertext.

Um einen URL Access zu konfigurieren, muss unter “SSL VPN” der Zweig “URL Access” selektiert und zunächst ein neuer Eintrag angelegt werden.



Name [URL Access]

Unter “Name” geben Sie einen Namen für diesen Filter an. Dieser Name erscheint später in einer Liste der URL Access, wenn Sie ein SSL VPN-Profil zusammenstellen.

Status [URL Access]

Um dieses Feature nutzen zu können, muss der Status “aktiv” geschaltet sein. Wird der Status auf “inaktiv” geschaltet, so wird der URL Access temporär ausgeschaltet, ohne gelöscht zu werden.

IP-Adressbereich [URL Access]

Über den IP-Adressbereich kann die Anzahl der möglichen Web-Server eingeschränkt werden (z.B. um die Darstellung bestimmter Bild- oder Textdaten auszuschließen). In der Standardeinstellung (0.0.0.0 bis 255.255.255.255) ist keine Einschränkung vorgenommen.

Hostname [URL Access]

Die Adresse des Web-Servers wird hier als Hostname oder als IP- oder Web-Adresse angegeben und muss mit der URL übereinstimmen, die in der Web Proxy-Konfiguration vorgenommen wurde.

Wenn Sie den Hostnamen verwenden, beachten Sie bitte, dass ein DNS Server für die Namensauflösung installiert sein muss. Der DNS Server wird unter “Lokales System / DNS/WINS” konfiguriert.

URL-Pfad [URL Access]

Hier wird der Web-Zugriff erweitert. Wird in der Web Proxy-Konfiguration definiert, dass ein Zugriff maximal bis zur letzten angegebenen Dokumentenseite erfolgen darf, z.B.:

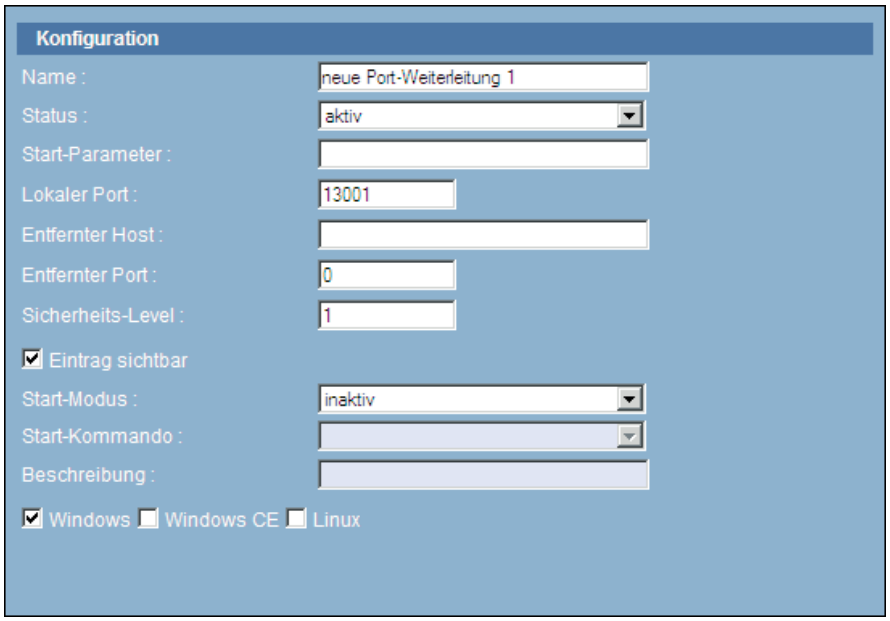
/deutsch/index.html

- so gestattet der Eintrag eines Slash “/” den Zugriff auf alle Web-Seiten, die nach dem ersten Slash in der URL folgen.

Die Pfadeingabe muss immer mit einem “/” beginnen. Es darf kein Hostname oder Protokoll angegeben werden.

Port-Weiterleitungen

Für jede TCP Verbindung muss ein Port Weiterleitungs-Eintrag angelegt werden. Dazu wird unter “SSL VPN” die “Port-Weiterleitung” selektiert und zunächst ein neuer Eintrag angelegt.



Name [Port-Weiterleitungen]

Unter “Name” geben Sie einen Namen für diese Anwendung an. Dieser Name erscheint später als Applikation auf der Menüseite des Browser am Benutzer-PC.

Status [Port-Weiterleitungen]

Der Status muss “aktiv” geschaltet sein, damit die Anwendung genutzt werden kann. Wird der Status auf “inaktiv” geschaltet, verschwindet diese Anwendung für Benutzer, die eine neue Verbindung zum Gateway herstellen, von der Menü-Seite. Die Verbindung für aktuelle Anwender bleibt bestehen.

Beschreibung [Port-Weiterleitungen]

Diese Beschreibung erscheint im Browser hinter dem Namen der Applikation.

Lokaler Port [Port-Weiterleitungen]

Als Lokaler Port muss ein freier Port am Rechner der Benutzer angegeben werden, zu dem die Applikation die TCP-Verbindung herstellen soll. z.B. Port 13002.

Entfernter Host [Port-Weiterleitungen]

Hier geben Sie die IP-Adresse oder den Host-Namen des Servers an, der die Anwendung zur Verfügung stellt und zu dem die TCP-Verbindung hergestellt werden soll.

Entfernter Port [Port-Weiterleitungen]

Hier geben Sie den Port des Server-Dienstes an. Z.B. für SSH = 22.

Sicherheits-Level [Port-Weiterleitungen]

Der Sicherheits-Level bezeichnet den Wert eines Regelwerks, das mindestens erfüllt sein muss, damit diese Anwendung im Start-Menü erscheint. Der hier einzutragende ganzzahlige Wert muss mit den Definitionen der Sicherheits-Richtlinien im Secure Enterprise Manager abgestimmt sein.

Eintrag sichtbar [Port-Weiterleitungen]

Mit dieser Funktion kann die Anwendung auf der Menü-Seite des Browsers sichtbar oder unsichtbar geschaltet werden.

Start-Modus [Port-Weiterleitungen]

Wird der Start-Modus auf “inaktiv” gesetzt, so kann die Applikation nicht aus der Menü-Seite des Browsers gestartet werden. Mit der Einstellung “Starte Applikation” können bestimmte Applikationen aus der Menü-Seite direkt gestartet werden. Andere Applikationen können über Script gestartet werden (z.B: Telnet oder SSH). Das Script wird unter “Start-Kommando” ausgewählt.

Start-Parameter [Port-Weiterleitungen]

Im Installationsverzeichnis befinden sich Original-Scripte von NCP zu jenen Anwendungen, die mit der Erstinstallation des Gateways eingespielt werden. Sie liegen unter:
`[WINDIR]\ncprtr\sslvpn\applications`

Diese Scripte können modifiziert werden. So kann eine Applikation z.B. zuerst heruntergeladen, entpackt und dann gestartet werden. Mit welchen Funktionen eine dieser Script-Dateien erweitert werden kann, zeigt eine Funktionsliste dlcmds.txt, die sich in dem gleichen Verzeichnis befindet.

Bitte beachten Sie, dass die Originale aller Scripte, die Sie editieren, gesichert werden sollten. Außerdem sollten Ihre modifizierten Scripte ebenso an anderer Stelle gesichert sein, da diese Seiten bei jeder Neuinstallation und jedem Update von den Originaldateien überschrieben werden. Die von Ihnen für den Einsatz editierten Script-Dateien müssen in den gleichen Verzeichnissen gespeichert werden wie die Originale.

Mit Klick auf den Auswahl- Button des Start-Kommandos öffnet sich nebenstehendes Fenster, das die aktuell zur Verfügung stehenden Start- Scripte für die jeweilige Anwendung (mit Version) zeigt. Hier kann für die selektierte Anwendung Ihr Script mit Klick auf “OK” als Start-Kommando eingefügt werden.

Wurden neue Scripte hinzugefügt oder editiert, so sollte zunächst der Button “Neu laden” angeklickt werden.

Im folgenden die Verzeichnisse für die SVS-Script-Dateien, daneben der Script-Titel, der über den Auswahl-Button [...] als Start-Kommando selektiert werden kann, und daneben der Browser-Menütitel, mit dem die Applikation im Menü-Fenster erscheint:

```
Verzeichnis / Script-Titel            / Browser-Menütitel
Telnet      / Telnet                  / Telnet (Linux Test System)
SSH         / Putty SSH (Windows)     / SSH (Linux Test System)
TightVNC    / Tight VNC (Java)        / VNC (Windows Test System)
MsRdpClient / Remote Desktop (Win32) / Terminal Server (Windows Test System)
```

Die möglichen Start-Parameter sind applikationsspezifisch und werden in den entsprechenden Scripten mitgeliefert.

Betriebssystem-Schalter [Port-Weiterleitungen]

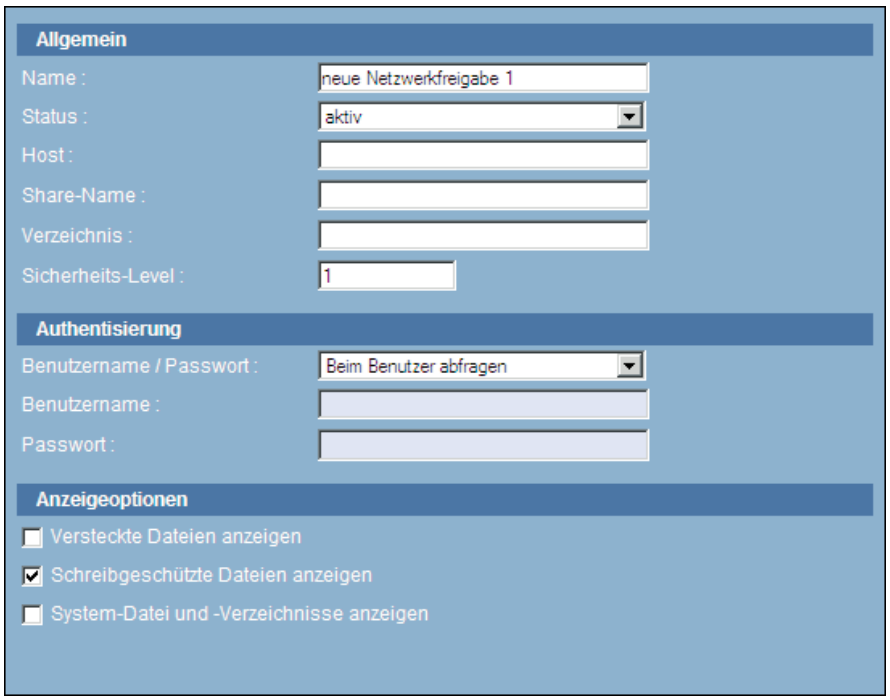
Je nachdem, unter welchem Betriebssystem eine Anwendung nicht einsetzbar ist, kann dieses Betriebssystem (Windows, Windows CE oder Linux) hier selektiert werden, so dass diese Applikation auf der Menü-Seite dieses Betriebsystems gar nicht erscheint.

Netzwerkfreigaben

Allgemein

Mit Network Sharing kann ein Laufwerk auf einem File Server freigegeben werden. Der Benutzer erhält über den Datei-Explorer seines Browsers darauf Zugriff. Für die Verbindung zum File Server wird das Microsoft SMP-Protokoll verwendet, für das, bei Einsatz einer Firewall zwischen VPN Gateway und File Server der TCP Port 445 freigeschaltet sein muss.

Um den Zugriff auf ein Laufwerk und die darunter liegende Ordnerstruktur eines File Servers konfigurieren zu können, muss im Konfigurationsbaum unter “SSL VPN” das “Network Sharing” selektiert und zunächst ein neuer Eintrag angelegt werden.



Name [Netzwerkfreigaben]

Unter “Name” geben Sie einen Namen für das freizugebende Laufwerk an. Dieser Name erscheint im Datei-Explorer des Browsers als Laufwerksname der obersten Ebene der Ordnerstruktur.

Status [Netzwerkfreigaben]

Der Status muss “aktiv” geschaltet sein, damit das Laufwerk und der darunter liegende Verzeichnisbaum im Datei-Explorer erscheint. Wird der Status auf “inaktiv” geschaltet, verschwindet dieses Laufwerk aus dem Datei-Explorer.

Host [Netzwerkfreigaben]

Hier wird der Hostname oder die IP-Adresse des File Servers eingetragen. Wenn Sie den Hostnamen verwenden, beachten Sie bitte, dass ein DNS Server für die Namensauflösung installiert sein muss. Der DNS Server wird unter “Lokales System / DNS/WINS” konfiguriert.

Share-Name [Netzwerkfreigaben]

Als Share-Name wird der Name (ohne Backslashs) eingetragen, mit dem dieses Laufwerk in der Netzwerkkonfiguration freigegeben wurde.

Verzeichnis [Netzwerkfreigaben]

Mit dem hier eingetragenen Verzeichnispfad kann festgelegt werden, ab welcher Verzeichnistiefe die Ordner im Datei-Explorer dargestellt werden. Verzeichnisebenen, die sich über dem hier eingetragenen Verzeichnispfad befinden, sind im Datei-Explorer nicht sichtbar.

Sicherheits-Level [Netzwerkfreigaben]

Der Sicherheits-Level bezeichnet den Wert eines Regelwerks, das mindestens erfüllt sein muss, damit dieses freigegebene Laufwerk im Datei-Explorer erscheint. Der hier einzutragende ganzzahlige Wert muss mit den Definitionen der Sicherheits-Richtlinien im Secure Enterprise Manager abgestimmt sein.

Authentisierung [Netzwerkfreigaben]

Die Authentisierung am File Server kann auf drei Arten erfolgen. Wählen Sie dazu eine Option unter Benutzername / Passwort nach Klick auf den Auswahl-Button.

Benutzername / Passwort [Netzwerkfreigaben]

Wird Benutzername und Passwort beim Benutzer abgefragt, so erhält der Benutzer eine Eingabemas-

ke für das Netzwerk-Login, in die er die Login-Daten, die er von seinem Administrator erhalten hat eingibt.

Sollen SSL VPN Benutzername und Passwort verwendet werden, so müssen diese mit den Login-Daten für das Netzwerk übereinstimmen. Beim Netzwerkzugriff auf dieses Laufwerk mit dem Datei-Explorer im Browser erfolgt dann keine weitere Abfrage.

Wird der konfigurierte Benutzername und Passwort verwendet, so müssen diese Login-Daten in die unteren Felder eingetragen werden, um sie automatisch beim Netzwerkzugriff auf dieses Laufwerk übergeben zu können.

Anzeige der Dateien in der Benutzeroberfläche [Netzwerkfreigaben]

Welche Dateien im Datei-Explorer angezeigt werden, kann eigens selektiert werden:

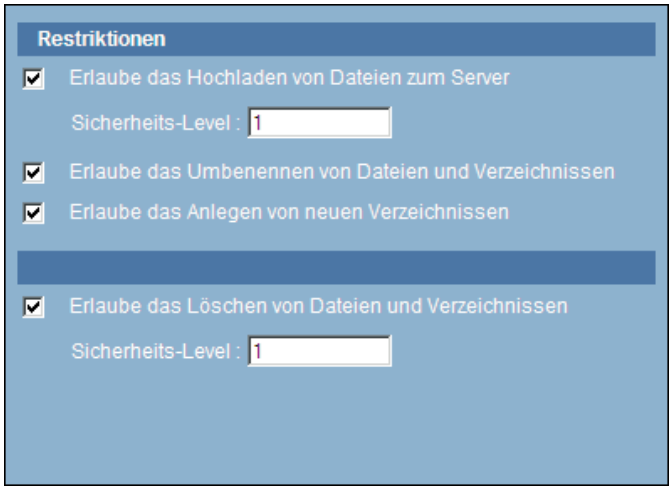
- Versteckte Dateien anzeigen

- Schreibgeschützte Dateien anzeigen

- System- Dateien und Verzeichnisse anzeigen

Restriktionen [Netzwerkfreigaben]

Mit den Restriktionen werden die Datei-Operationen festgelegt, die gestattet oder nicht erlaubt sind. Die entsprechenden Funktions-Buttons im Datei-Explorer werden aktiv oder inaktiv (grau) geschaltet, sobald ein Ordner oder eine Datei im Verzeichnisbaum markiert ist.



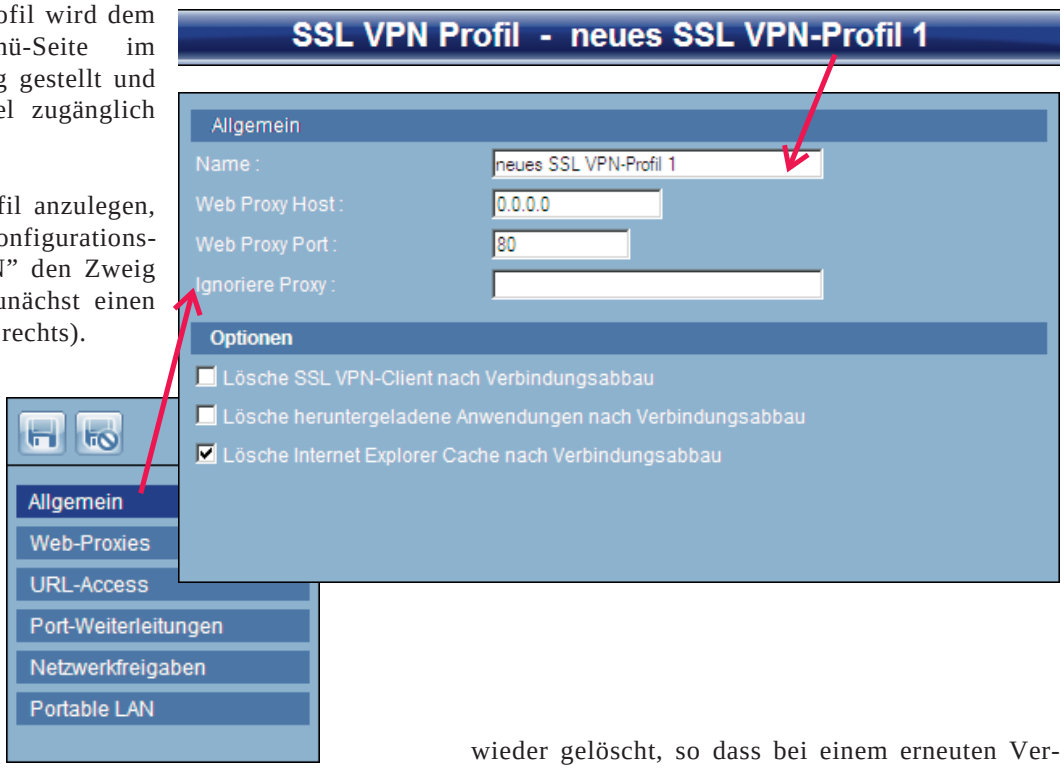
Sicherheits-Level (Restriktionen) [Netzwerkfreigaben]

Der Sicherheits-Level bezeichnet den Wert eines Regelwerks, das mindestens erfüllt sein muss, damit dieses freigegebene Laufwerk im Datei-Explorer erscheint. Der hier einzutragende ganzzahlige Wert muss mit den Definitionen der Sicherheits-Richtlinien im Secure Enterprise Manager abgestimmt sein.

Profile / Allgemein

Über das SSL VPN-Profil wird dem Anwender die Menü-Seite im Browser zur Verfügung gestellt und je nach Security Level zugänglich gemacht.

Um ein SSL VPN-Profil anzulegen, selektieren Sie im Konfigurationsbaum unter “SSL VPN” den Zweig “Profile” und legen zunächst einen neuen Eintrag an (Abb. rechts).



Im allgemeinen Bereich werden die Zugriffe für Intra Web-Anwendungen über einen Proxy-Server und der Umgang mit evtl. heruntergeladenen Anwendungen geregelt.

Name [Profile]

Mit dem hier hinterlegten Namen wird später dieses SSL VPN-Profil dem Link-Profil zugeordnet, das den Benutzer-Zugang zum Gateway regelt.

Web Proxy Host / Web Proxy Port [Profile]

Sofern der Anwender über das Firmennetz auch auf externe Web-Seiten zugreift (z. B. Google) und im Firmennetz ein Proxy-Server installiert ist, muss hier die IP-Adresse des Proxy-Servers mit dem Web Proxy Port angegeben werden.

Ignoriere Proxy [Profile]

Intra Web-Anwendungen, die über den internen Web-Server dargestellt werden, benötigen keinen Proxy-Server. Für diese Anwendungen wird der Proxy-Server ignoriert, indem ihre IP-Adresse hier eingetragen wird, entweder als einzelne IP-Adresse(n), getrennt mit Semikolon oder als Adressbereich des Firmennetzes von IP-Adresse “-” IP-Adresse.

Lösche SSL VPN Client nach Verbindungsabbau [Profile]

Wird diese Funktion aktiv geschaltet, so wird nach einem Verbindungsabbau der Thin SSL VPN Client wieder gelöscht, so dass bei einem erneuten Verbindungsaufbau die Software erneut heruntergeladen und wieder initialisiert werden muss. Dies ist insbesondere dann zu empfehlen, wenn der Anwender an einem Fremd-PC arbeitet (z.B. Internet Café).

Die Software für den Thin SSL VPN Client wird auch dann erneut heruntergeladen, wenn am Gateway eine neuere Version vorliegt.

Lösche heruntergeladene Anwendungen nach Verbindungsabbau [Profile]

Applikationen, die über Script heruntergeladen und installiert wurden, können nach einem Verbindungsabbau wieder gelöscht werden, so dass bei einem erneuten Verbindungsaufbau die Software erneut heruntergeladen und wieder initialisiert werden muss. Dies ist insbesondere dann zu empfehlen, wenn der Anwender an einem Fremd-PC arbeitet (z.B. Internet Café).

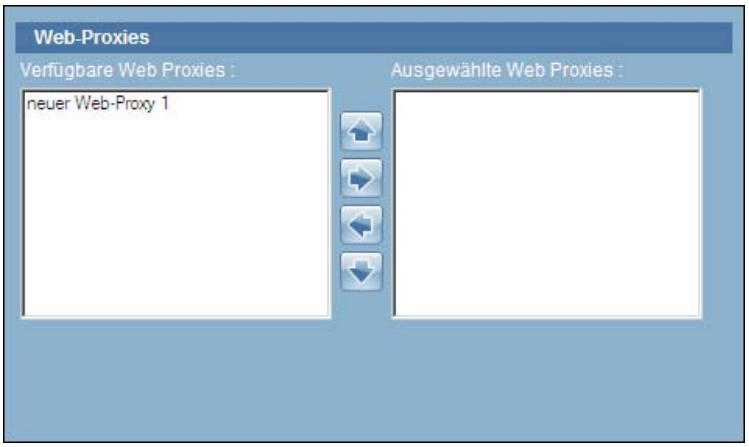
Die Software wird auch dann erneut heruntergeladen, wenn am Gateway eine neuere Version vorliegt.

Lösche Internet Explorer Cache nach Verbindungsabbau [Profile]

Mit dieser Funktion kann der Internet Explorer Cache des Benutzer-PCs gelöscht werden.

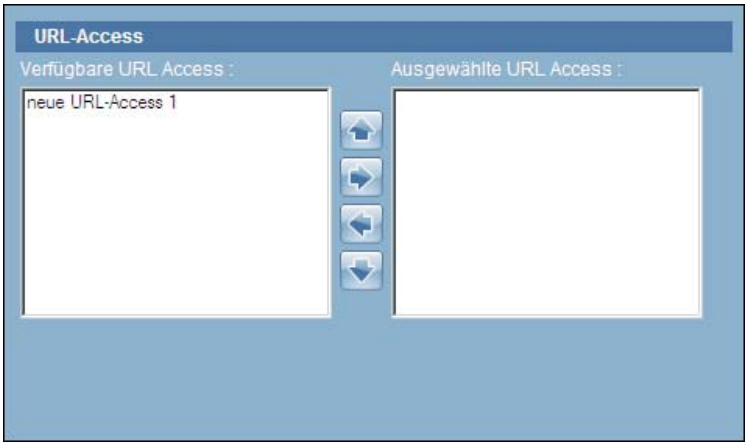
Web Proxy [Profile]

Im Register “Web Proxy” wählen Sie aus den verfügbaren Proxies, die Sie in einer eigenen Gruppe oben konfiguriert haben, die gewünschten aus und schieben sie mit dem Pfeil-Button auf die Seite “Ausgewählte Web Proxies”.



URL Access [Profile]

Hier kann der Bereich möglicher Web-Adressen eingegrenzt werden. Dazu wählen Sie aus den verfügbaren URL-Zugriffen (URL Access), die Sie oben in einer eigenen Gruppe konfiguriert haben, die gewünschten aus und schieben sie mit dem Pfeil-Button auf die Seite “Ausgewählte URL Access”.

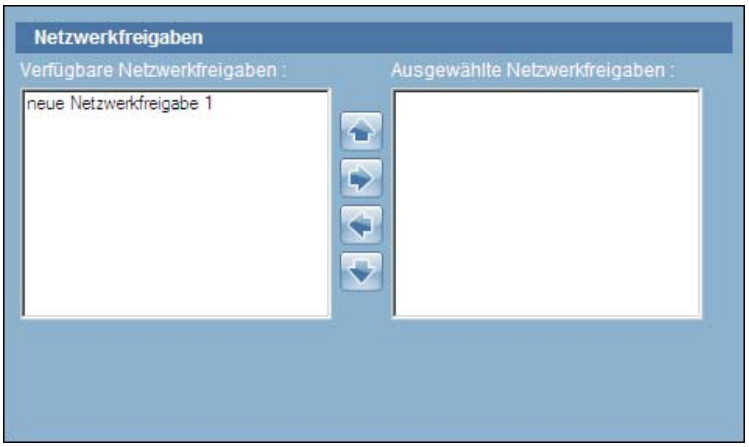


Port-Weiterleitung [Profile]

Im Register “Port-Weiterleitung”, wählen Sie aus den verfügbaren Port-Weiterleitungen, die Sie in einer eigenen Gruppe oben konfiguriert haben, die gewünschten aus und schieben sie mit dem Pfeil-Button auf die Seite “Ausgewählte Port-Weiterleitungen”.

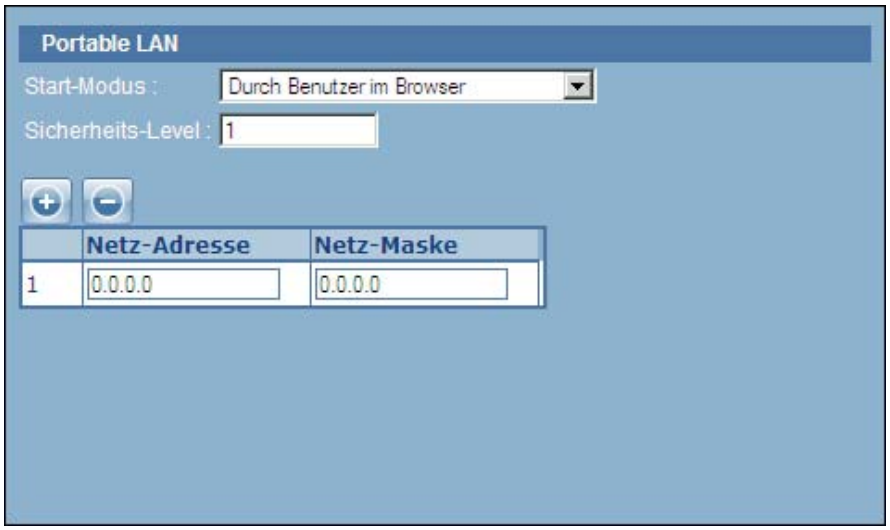
Netzwerkfreigaben [Profile]

Hier kann ausgewählt werden, welche Netzwerk-Zugriffe über den Browser des Benutzers möglich sein sollen. Die Netzwerkfreigaben wurden oben in einer eigenen Gruppe konfiguriert.



PortableLAN [Profile]

Das SSL VPN Gateway unterstützt (ab lizenzierter Version 7.0) mit dem PortableLAN-Modul die Netzanbindung von NCP Secure Enterprise Clients (Windows XP 32/64 Bits, Vista 32/64 Bits) über SSL VPN. Remote Access über SSL VPN kommt insbesondere dann zum Einsatz, wenn eine Verbindung über IPSec nicht möglich ist, z. B. von Hotels, die nur HTTP- oder HTTPS-Verbindungen zulassen.



Start-Modus

inaktiv: Für dieses Profil wird der NCP portableLAN-Adapter nicht genutzt.

durch Benutzer im Browser: Nach dem Verbindungsaufbau über den Browser zum Web Server öffnet sich die Login-Seite. Dort wird nach Klick auf das Icon für den Netzzugang die SSL VPN-Verbindung hergestellt.

automatisch: Nach Anmeldung über SSL VPN wird automatisch der portableLAN Adapter mit Benutzeroberfläche aktiviert.

Sicherheits-Level [Profile / PortableLAN]

Der Sicherheits-Level bezeichnet den Wert eines Regelwerks, das mindestens erfüllt sein muss, damit die SSL VPN-Verbindung hergestellt werden kann. Der hier einzutragende ganzzahlige Wert muss mit den Definitionen der Sicherheits-Richtlinien im Secure Enterprise Manager abgestimmt sein.

VPN-Netzwerke

Hier können genau die IP-Netze definiert werden, über die der Client via SSL VPN-Tunnel kommunizieren kann. Wenn Tunneling genutzt wird und hier keine Einträge erfolgen, so können alle VPN-Netze genutzt werden.

Statische Netzwerk-Routen

Diese statischen Netzwerk-Routen gelten global für alle ausgehenden Verbindungen. Sie werden nur durch eine statische Route die in einem Link-Profil angelegt wurde überschrieben.

Die statische Netzwerk-Route wird immer dann gesetzt, wenn das bestimmte Zielnetz nicht über das Default-Gateway erreicht werden kann. Statische Routen werden nur für ausgehende Verbindungen von Clients oder Filial-Gateways genutzt.

Alle statischen Routen müssen in dieser Konfiguration eingetragen werden.

Beim Starten des Secure Servers erfolgt ein Abgleich zwischen den hier in der Konfiguration eingetragenen und den am System-Rechner eingetragenen statischen Routen. Dabei werden Routen die in der Konfiguration nicht eingetragen wurden aus dem System gelöscht und Routen die in der Konfiguration eingetragen wurden hinzugefügt.

Die Default Route wird nicht verändert.

Konfiguration der statischen Routen

Mit Klick auf den Plus-Button werden die Daten in die Liste der konfigurierten statischen Routen übernommen.

Wird eine konfigurierte statische Route markiert, kann sie mit dem Minus-Button gelöscht werden.

Server Plug-in

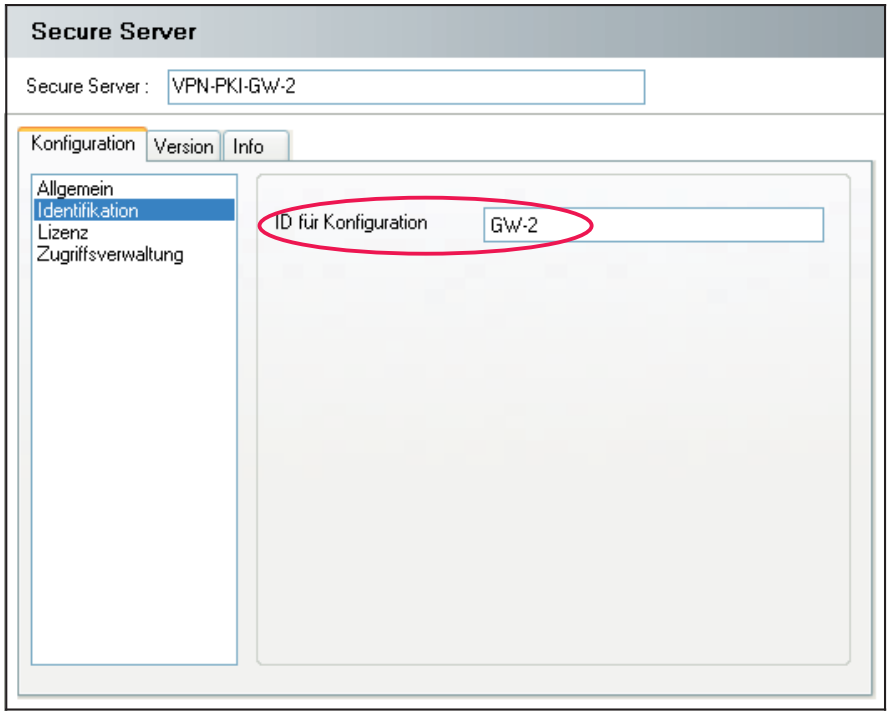
Der Konfigurationsbaum des Server Plug-ins im Secure Enterprise Management (SEM) ist mit wenigen Ausnahmen genauso aufgebaut wie der Konfigurationsbaum im Web-Interface, sodass Sie bei Erstellung einer Konfiguration / Vorlage mit dem SEM die Online-Hilfe oder diese Parameterbeschreibung in der gleichen Weise verwenden können.

Die Ausnahmen beziehen insbesondere auf Eingabefelder, die zur Übertragung der Konfiguration aun einen entfernten Secure Server bzw. für einen Konfigurations-Download vom Secure Server nötig sind.

Mit einem Mausklick auf den roten Begriff gelangen Sie zum Konfigurationsbaum.

Übertragen der Konfiguration

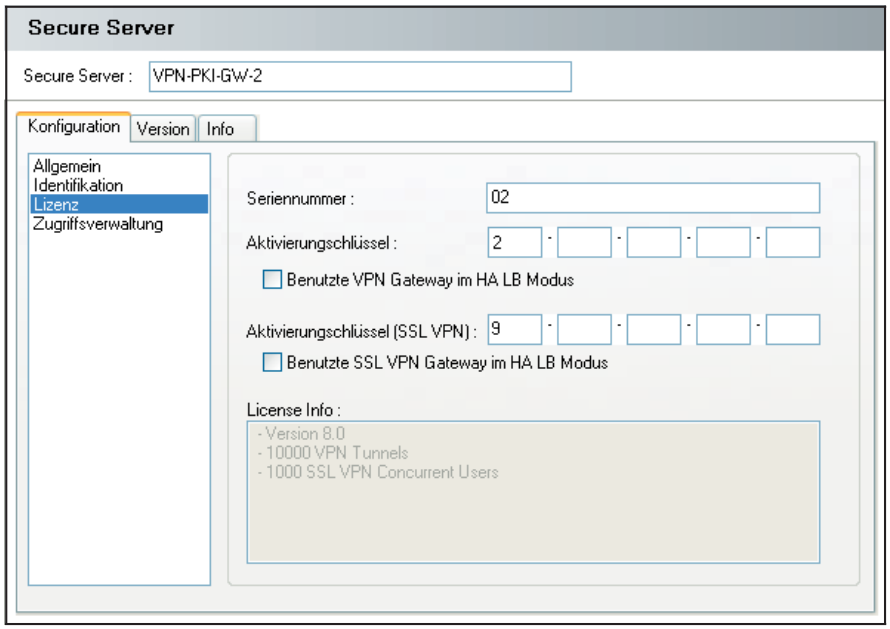
Die Konfiguration, die mit dem Server Plug-in erzeugt wurde, kann nur an den entfernten Server übertragen werden, wenn dort die **Server-Konfiguration** wie oben beschrieben vorgenommen wurde.



ID für Konfiguration (Plug-in)

Die ID für Konfiguration wird dafür benutzt, dass der Server eine bestimmte Konfiguration vom Management-System herunterladen kann.

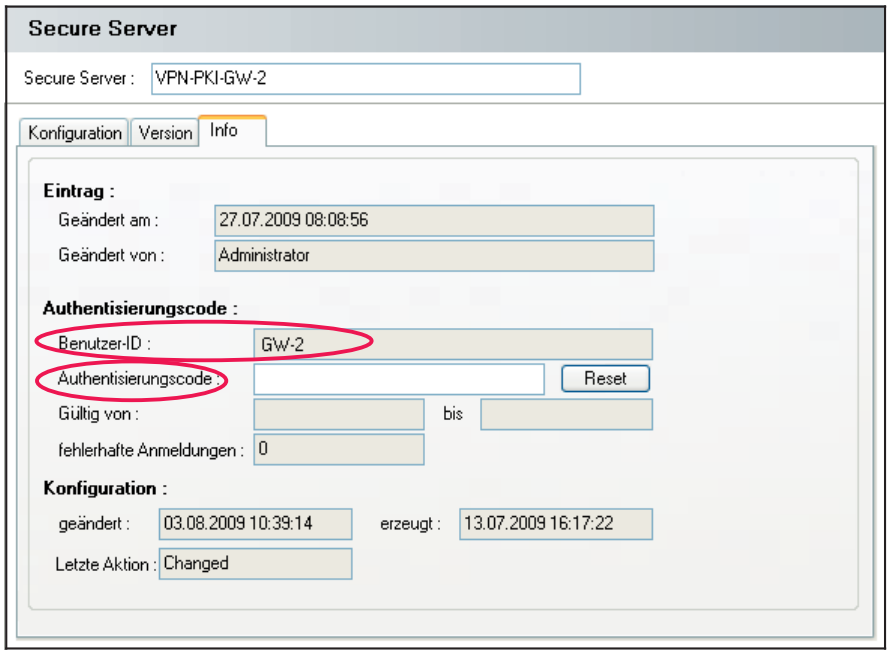
Sie wird am Plug-in für den jeweiligen Server unter “Konfiguration / Identifikation” eingegeben (Abb. links) und muss ebenso in der Server-Konfiguration eingetragen werden, wo sie **Benutzer-ID** heißt wie auch im Info-Fenster der Server-Konfiguration (Abb. nächste Seite)..



Lizenz (Plug-in)

Die Lizenz wird am Plug-in für den jeweiligen Server unter “Konfiguration / Lizenz” eingetragen (Abb. links).

Im Konfigurationsbaum des Web-Interfaces werden die Lizenzdaten unter “System / Lizenz” eingetragen. Eine Beschreibung finden Sie unter **Lizenzen**.



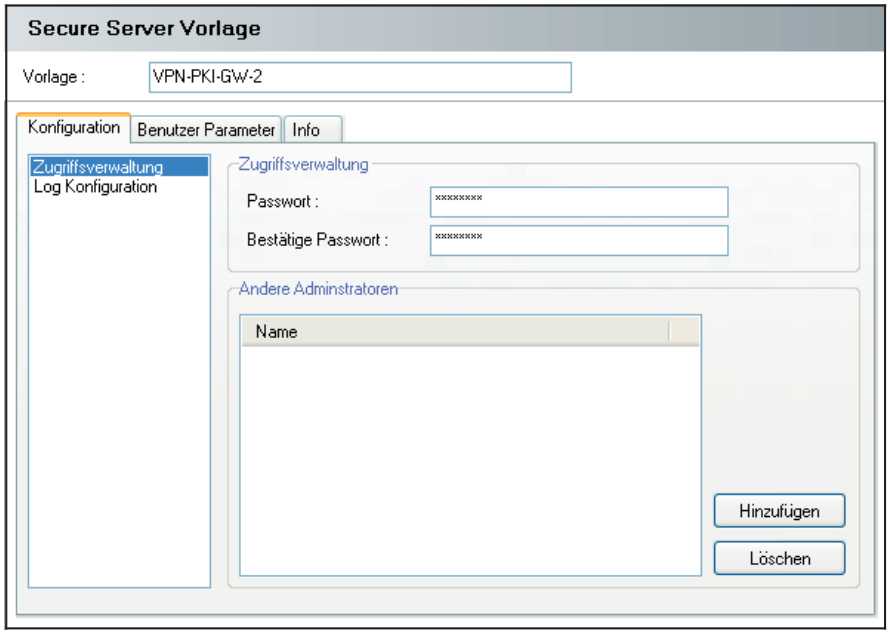
Benutzer-ID (Plug-in)

Die Benutzer-ID zeigt die **ID für Konfiguration** aus dem Konfigurationsfenster des Servers an.

Sie muss am Secure Server eingetragen werden, um die Server-Konfiguration vom SEM herunterladen zu können (siehe **Server-Konfiguration**).

Authentisierungscode (Plug-in)

Der hier erzeugte Authentisierungscode muss in der Server-Konfiguration für die erste Verbindung zwischen Server und Management-System eingegeben werden.



Zugriffsverwaltung (Plug-in)

Die Zugriffsdaten werden am Plug-in in der Vorlage unter “Konfiguration / Zugriffsverwaltung” eingetragen (Abb. links).

Wird die Konfiguration an den Server übertragen, so muss von einem Administrator immer dieses Passwort verwendet werden (siehe **Zugriff**). Administratoren, die hier (Abb. links) über das Server Plug-in angelegt werden, besitzen nur Leserechte über das Web-Interface. Sind sie in der Rechtestruktur des SEM bereits angelegt, wird für den Server das gleiche Passwort genutzt wie für den SEM.

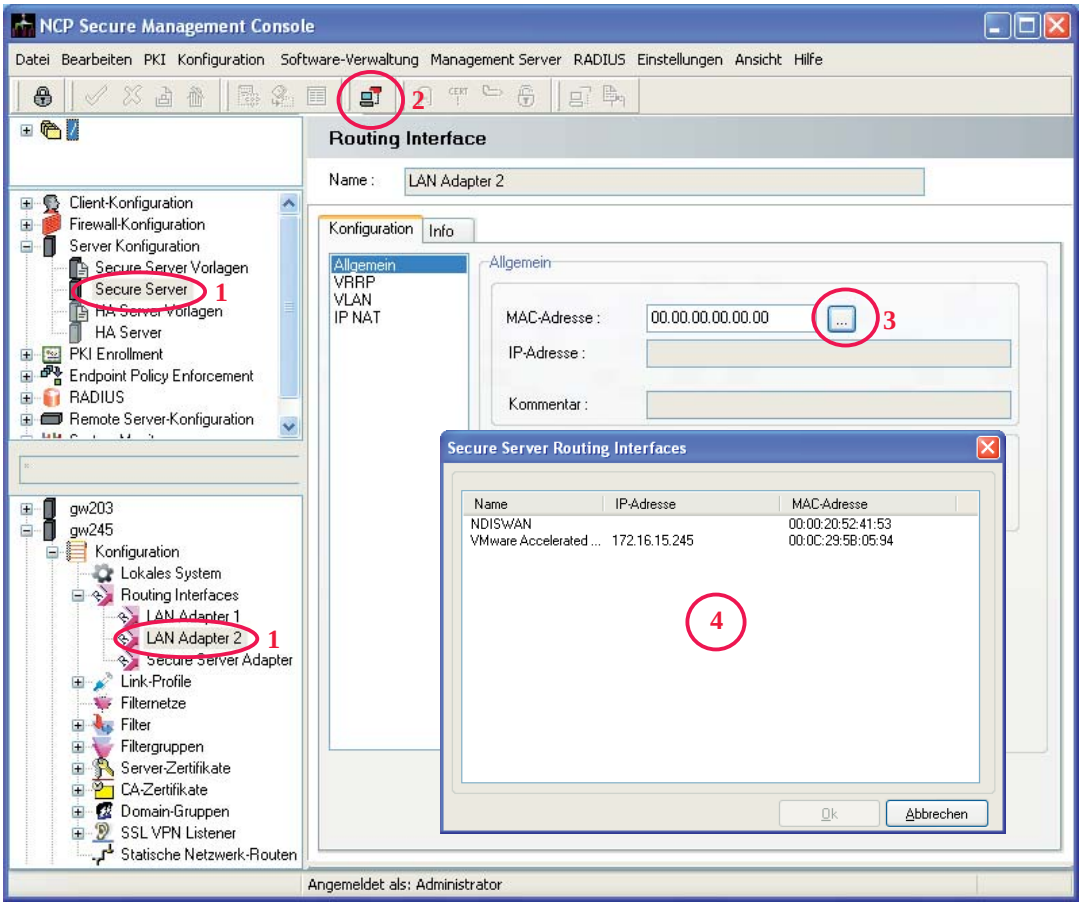
Routing Interfaces (Plug-in)

Mit dem Secure Enterprise Management (SEM) kann in der Server-Konfiguration unter “Routing Interface / Allgemein” für einen selektierten Adapter (Abb. unten 1) eine Konfiguration des Routing Interfaces vorgenommen werden.

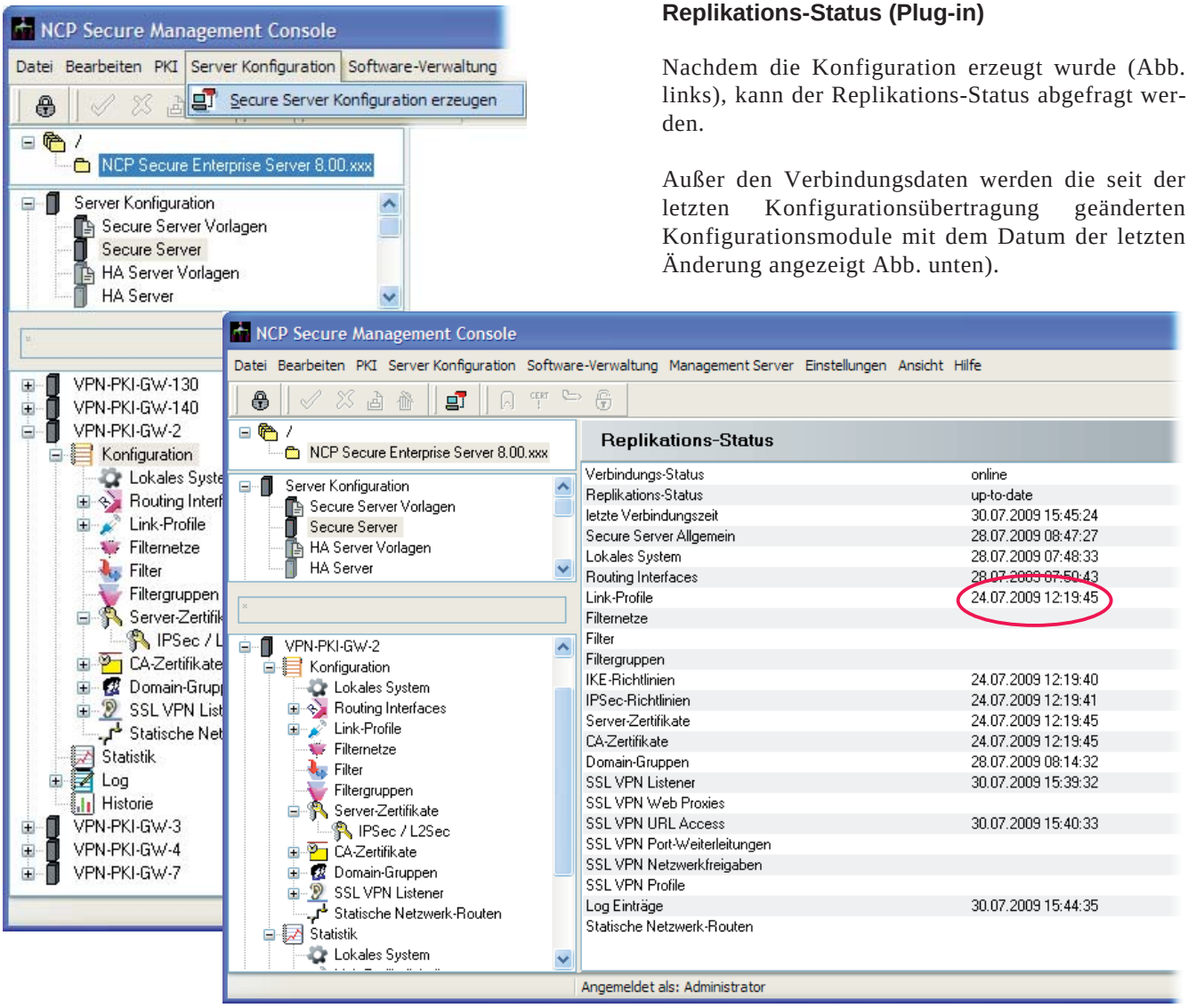
Eine Verbindung zwischen SEM und Server muss über die Einstellung am Server, siehe oben **Server-Konfiguration**, hergestellt worden sein, d. h. die Konfiguration muss vom Management-System übertragen worden sein (Abb. unten 2).

In diesem Fenster kann die Adapter-Konfiguration vorgenommen werden, indem dem selektierten Adapter die **IP-** und **MAC-Adresse** eines anderen LAN-Adapters zugeordnet werden, außerdem ein **Name** für den LAN-Adapter eingegeben werden kann.

Diese Konfiguration bleibt auch dann erhalten, wenn zu einem späteren Zeitpunkt die Konfiguration nicht mehr vom SEM übernommen wird.



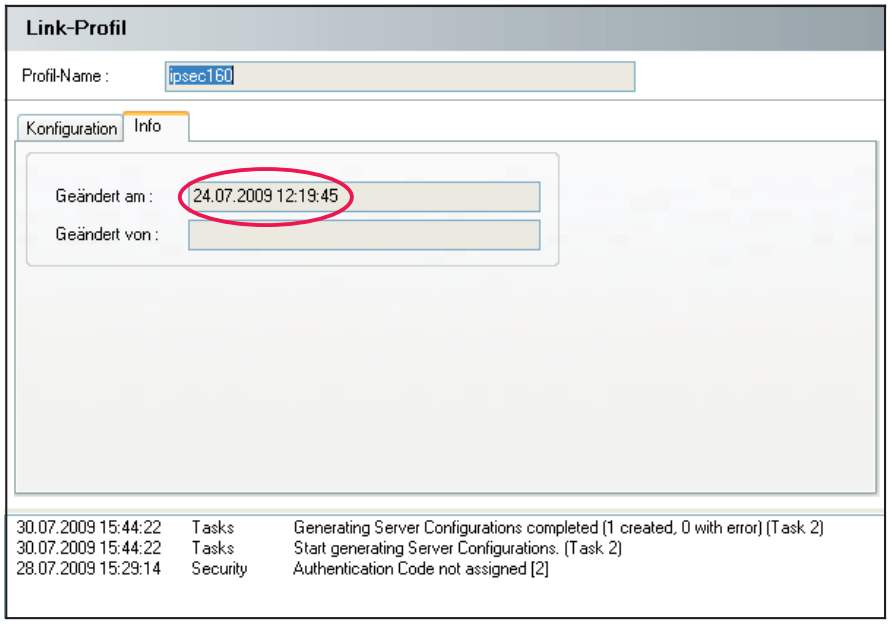
Während der Online-Dauer kann im Konfigurationsfeld für den selektierten LAN-Adapter über den Auswahl-Button (Abb. oben 3) ein Fenster mit der Darstellung der Netzwerk-Konfiguration am Secure Server geöffnet werden (Abb. oben 4).



Replikations-Status (Plug-in)

Nachdem die Konfiguration erzeugt wurde (Abb. links), kann der Replikations-Status abgefragt werden.

Außer den Verbindungsdaten werden die seit der letzten Konfigurationsübertragung geänderten Konfigurationsmodule mit dem Datum der letzten Änderung angezeigt Abb. unten).



Die letzten erfolgreich übertragenen Konfigurationsänderungen können auch in den Konfigurationsmodulen direkt abgelesen werden.

Abbildung links und oben: Der Zeitstempel zeigt die letzte Konfigurations-Änderung in einem Link-Profil, die der Server übernommen hat.

Importieren der Konfiguration

Ebenso wie eine Konfiguration vom Management-System an einen Server übertragen werden kann, kann eine Konfiguration von einem entfernten Server (Version >= 8.0) mithilfe seiner Konfigurationsdatei auch importiert und anschließend vom zentralen Management-System verwaltet werden. Der Import der Konfiguration kann jederzeit ohne Voreinstellung am Server erfolgen.

Voraussetzung
Secure Server der Version 7.xx müssen auf die Version 8.0 aktualisiert werden.

Konfigurationsdatei und Installationsverzeichnis

Ab der Version 8.0 heißt das Installationsverzeichnis **unter Windows** der Server Software:
`<Programme>\ncp\SecureServer`

Alle Konfigurationsdateien, CA-Zertifikate und Dateien, die vorher unter `\ncprtr\certs` gespeichert waren, werden im Verzeichnis
`<Programme>\ncp\SecureServer \backups\updateFromNcprtr`
gesichert.

Beim Update werden alle Dateien unter `\ncprtr` gelöscht. Die bestehende Konfiguration wird beim Update in das neue XML-Format konvertiert.

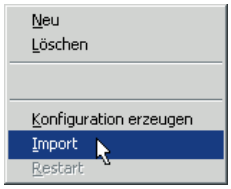
Das Installationsverzeichnis heißt **unter Linux**:
`/usr/local/ncp/ses`
Backup-Verzeichnis:
`/var/adm/backup/ncp/ses /deinst-yymmdd[-1]`
Alte zu löschende Dateien in:
`/usr/local/ncp/ses und /etc/ncp`
Konfigurationsdateien:
`/etc/ncp/ses`
Log-Dateien: /var/log/ncp

Die **Konfigurationsdatei** beinhaltet die gesamte Konfiguration im XML-Format. Sie befindet sich **unter Windows** im Verzeichnis:
`<Programme>\ncp\SecureServer \config\srvwin.conf`
unter Linux im Verzeichnis:
`/etc/ncp/srvlx.conf`

Die Konfigurationsdatei wird automatisch ca. 30 Sekunden nach der letzten Konfigurationsänderung am Secure Server gespeichert.

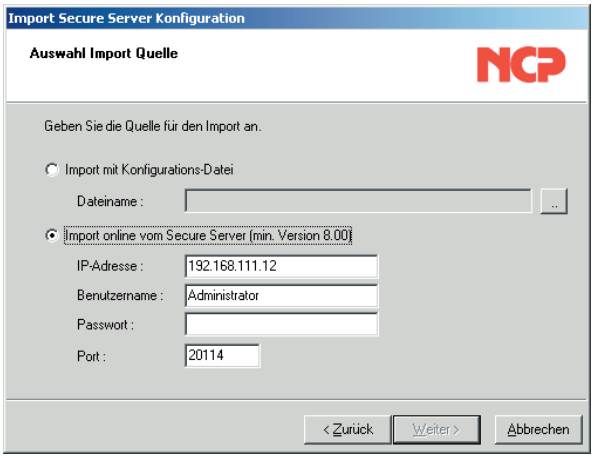
Darin enthalten sind neben der Konfiguration server- und gerätespezifische Angaben für:
– Aussteller Zertifikate: Diese werden jetzt direkt über die Web-Oberfläche importiert.
– Lizenz
– Statische Routen:
Sind diese in der Konfiguration nicht eingetragen, werden alle nicht konfigurierten Statischen Routen beim Einlesen der Konfiguration im System gelöscht! (Auch wenn diese unter Windows als permanent im System eingetragen sind). Beachten Sie dazu **Statische Netzwerk-Routen**!

Import der Konfigurationsdatei



Die Konfigurationsdatei wird vom SEM eingelesen nachdem Sie die Import-Funktion im Menü der rechten Maustaste selectiert haben (Abb. links).

Die Konfigurationsdatei kann nach Drücken des Auswahl-Buttons lokal eingelesen werden oder online vom Secure Server (Abb. unten).

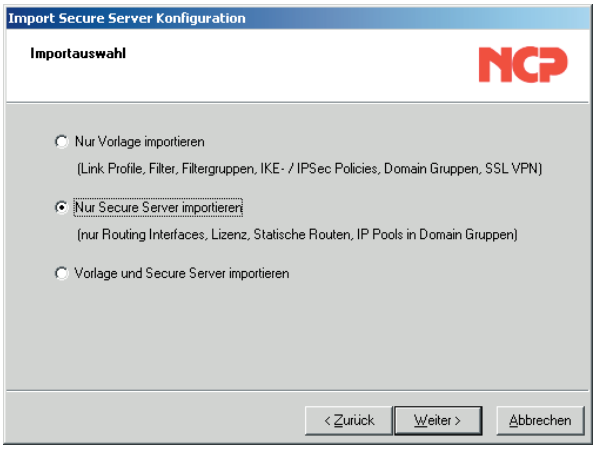


Geben Sie dazu folgende Daten ein:

IP-Adresse (Import)
ist die IP-Adresse über die der Secure Server im LAN erreicht wird, in der Regel die des Web-Interfaces.

Benutzername und Passwort (Import)
ist identisch mit Benutzername und Passwort beim Login am Web-Interface (siehe **Zugriff**).

Port (Import)
ist auf den Standard 20114 voreingestellt.

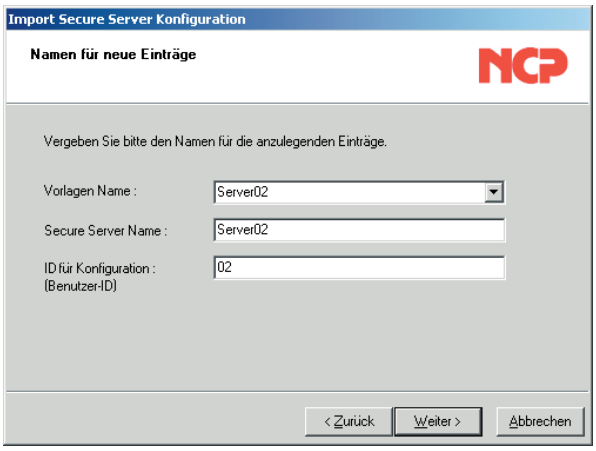


In der Importauswahl (Abb. oben) wird unterschieden, ob nur die Vorlage, nur server- und gerätespezifische Daten oder beides importiert werden soll.

Wird die Vorlage mit dem Secure Server importiert, so wird die komplette Konfiguration importiert und im SEM eine Vorlage und ein Server zu dieser Vorrlage generiert. Dieses Vorgehen wird bei einzelnen unterschiedlichen Servern empfohlen.

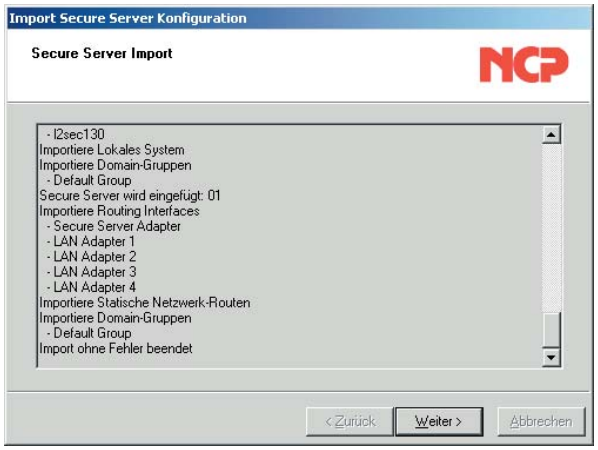
Nur die server- und gerätespezifischen Daten zu importieren wird dann empfohlen, wenn die Konfigurationen von weitgehend identischen Servern, die z. B. im HA Load Balancing-Modus arbeiten, im SEM angelegt werden sollen. In diesem Fall wird vom ersten LB Server die komplette Konfiguration importiert. Vom zweiten LB Server nur die Server-Daten, wobei die Vorlage des ersten LB Servers übernommen wird.

Diese Vorlagen-Zuordnung erfolgt im nächsten Fenster der Import-Funktion (Abb. unten).

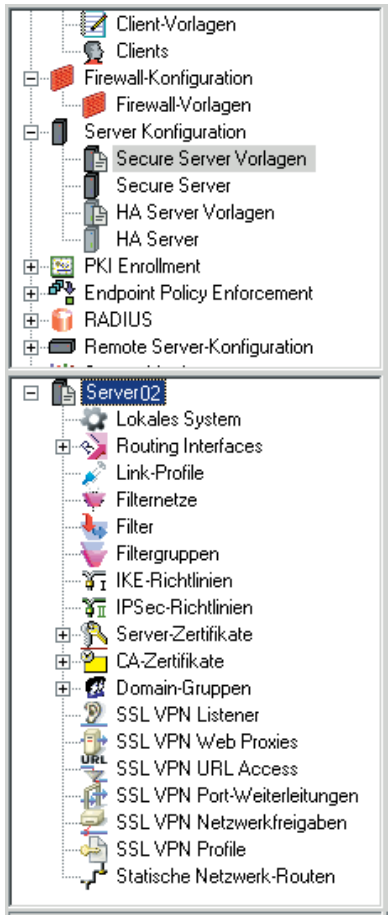


Die ID für Konfiguration ist frei wählbar und kann ggf. später in der Server-Konfiguration am SEM unter Identifikation wie oben beschrieben geändert werden (siehe **Übertragen der Konfiguration**). Anhand dieser ID wird eine am SEM gehaltene oder erzeugte Konfiguration dem entfernten Server zugeordnet (siehe **Server-Konfiguration**).

Klicken Sie auf weiter, so wird die Konfiguration nach Ihren Vorgaben importiert. (Abb. unten)



Nach einem fehlerfreien Import wird der Konfigurationsbaum des Servers und/oder der Server-Vorlage in der Oberfläche des SEM dargestellt (Abb. unten).



Web-Oberfläche

Das Web-Interface des Secure Servers wird über einen Browser erreicht, indem Sie die Internet-Adresse oder URL des Servers in Form von Hostname oder IP-Adresse mit der nachfolgenden Port-Nummer 20112 in die Adressleiste eingeben. Zum Beispiel:
`https://hostname:20112`

Im folgenden sind die Schaltknöpfe der Web-Oberfläche beschrieben:


Abmelden: Damit beenden Sie diese Session


Hilfe: Hiermit kann eine Online-Hilfe aufgerufen werden


Deutsch: Schaltet die Sprache der Oberfläche und der Online-Hilfe auf deutsch um


English: Schaltet die Sprache der Oberfläche und der Online-Hilfe auf englisch um


Neuen Eintrag hinzufügen: Unter diesem Menupunkt kann zu den Konfigurationsgruppen “Link-Profile”, “Filter” und “Filtergruppen” eine neue Komponente hinzugefugt werden. Je nachdem, welche dieser Gruppen markiert ist, wird eine neue Komponentemit den Standardparametern im Konfigurationsbaum erzeugt. Die neue Komponente wird im Konfigurationsbaum unter den bereits bestehenden aufgenommen und erhält als Name die fortlaufende Index-Nummer der Komponenten.


Ausgewählten Eintrag löschen: Unter diesem Menüpunkt kann eine im Konfigurationsbaum markierte Komponente aus den Konfigurationsgruppen “Link-Profile”, “Filter” und “Filtergruppen” entfernt werden.


Refresh: Mit einem Klick auf diesen Button wird die Anzeige aufgefrischt
Betrifft die Anzeige statistischer Werte während des laufenden Betriebs


Autorefresh: Mit einem Klick auf diesen Button wird die Anzeige in kurzen Intervallen automatisch aufgefrischt (betrifft die Anzeige statistischer Werte während des laufenden Betriebs)


Connect: Wird in der Statistik ein Link-Eintrag ausgewählt und auf diesen Button geklickt, so wird eine Verbindung hergestellt


Disconnect: Wird in der Statistik ein Link-Eintrag ausgewählt zu dem eine Verbindung hergestellt ist und auf diesen Button geklickt, so wird die Verbindung abgebaut

NCPWEB.CONF editieren

Die Konfigurationsdatei ncpweb.conf dient dazu, die Verbindung zwischen Browser und Secure Server zu definieren. Die Datei befindet sich auf dem Server-Rechner im Programmverzeichnis unter:
`<systemroot>\ncpweb\ncpweb.conf`

Bitte beachten Sie, dass die Server-Dienste nach einer Bearbeitung der Konfigurationsdatei am Secure Server neu gestartet werden müssen.

Drücken Sie dazu den Restart-Button unter “Statistik / Systeminformationen”!

Editierbare Parameter

Die Konfigurationsdatei ist in mehrere Kapitel gegliedert, die in eckigen Klammern überschrieben sind. Unter den Überschriften sind die Parameter in der Standardeinstellung angeordnet. Nur wenige dieser Parameter dürfen geändert werden! Mit einer Raute# können die Parameter und ihre Werte auskommentiert werden, d. h. sie werden mit der Raute# auf die Standardeinstellung zurück gesetzt.

Bitte belassen Sie die im folgenden nicht beschriebenen Parameter unverändert!

Die editierbaren Parameter sind im folgenden nach den Kapiteln mit ihren Standardeinstellungen aufgelistet und den jeweiligen Änderungsmöglichkeiten beschrieben:

```
[General]
CertificateFile   = ./vpngw.p12
PIN               = 1234
CAPath            = ./rootcerts
```

CertificateFile (ncpweb.conf)

Hier geben Sie Pfad und Dateinamen des Sever-Zertifikats an, wenn Sie SSL mit Zertifikat nutzen wollen. In der Standardeinstellung wird das mitinstallierte Testzertifikat genutzt:
`<systemroot>\ncpweb\vpngw.p12`

Dieses Zertifikat müssen Sie gegen Ihr eigenes austauschen.

PIN (ncpweb.conf)

In der Standardeinstellung ist dies “1234", die PIN des mitgelieferten Server-Zertifikats (hier des mitgelieferten Test-Zertifikats vpngw.p12). Geben Sie die PIN Ihres Server-Zertifikats hier ein.

CAPath (CertificateFile) (ncpweb.conf)

Dies ist der Pfadname zum Aussteller-Zertifikat des oder der Benutzer-Zertifikate für Server und Benutzer (Administrator). In der Standardeinstellung ist dies:
`<systemroot>\ncpweb\rootcerts`

Dieses Aussteller-Zertifikat muss am Server hinterlegt sein, um das Benutzer-Zertifikat des Administrators gegenprüfen zu können. Geben Sie hier

den Pfad zu ihrem CA-Zertifikat an. Gegebenenfalls können dort auch mehrere CA-Zertifikate abgelegt werden.

```
[Log]
LogPath                 = ./log
```

LogPath (ncpweb.conf)

Hier bestimmen Sie das Verzeichnis am Server, in das die Log-Ausgaben für das Web-Interface geschrieben werden.

```
[VirtualDir SecureServerCfg]
SessionTimeOut      = 300
```

SessionTimeOut (ncpweb.conf)

Der Standardwert für den Session Timeout beträgt 600 Sekunden. Nach jeder Bestätigung eines Konfigurationswerts und nach jedem Blättern in den Konfigurationsseiten beginnt der Timeout abzulaufen. Ist die zugewiesene Session-Zeit erreicht, findet ein automatisches Logout statt. Unbestätigte Konfigurationseingaben gehen verloren. Der Timeout wird in Sekunden eingestellt.

```
[Listen SesCfg]
ListenAddress       = 0.0.0.0
Port                = 20112
UseSSL              = 1
RequireCertificate= 0
#PKISerialAccess   = 01:00:02
IpAddrAccess       = 0.0.0.0-
255.255.255.255
```

ListenAddress (ncpweb.conf)

Die Standardeinstellung ist 0.0.0.0, d. h. alle Adressen, die für dieses Gateway zur Verfügung stehen, sind zulässig. Alternativ kann auch eine einzelne IP-Adresse eingegeben werden. Der Listener hört dann nur auf die genau zutreffend konfigurierte IP-Adresse, die genau der am Browser eingegebenen URL entsprechen muss.

Port (ncpweb.conf)

In der Standardeinstellung ist dies für das Web-Interface Port 20112. Sollte dieser Port von einer anderen Anwendung belegt sein, muss er hier und in der URL für die Einwahl entsprechend geändert werden. Folgender Befehl am Kommandprompt zeigt die belegten Ports am Server an:

```
netstat -a -n
```

UseSSL (ncpweb.conf)

1 = Server-seitig wird ausschließlich https zugelassen. Mit der Standardeinstellung “1" wird demnach für die Verbindung von Browser zu Web-Interface eine SSL-Verbindung genutzt. Am Browser muss dazu eine https-Adresse mit Port-Nummer angegeben werden. https ist weitgehend identisch mit http, die zusätzliche Verschlüsselung der Daten geschieht mittels SSL/TLS. Unter Verwendung des SSL-Handshake-Protokolls findet zunächst eine geschützte Identifikation und Authentisierung der Kommunikationspartner statt. Anschließend wird mit Hilfe asymmetrischer Verschlüsselung oder des Diffie-Hellman-Schlüsselaustauschs ein gemeinsamer symmetrischer Sitzungsschlüssel ausgetauscht. Dieser wird schließlich zur Verschlüsselung der Nutzdaten verwendet.

0 = Wird SSL nicht genutzt, so kann zur Anwahl der Web-Site auch eine http-Adresse am Browser angegeben werden. Die geschützte Identifikation und Authentisierung entfällt dann jedoch, und auch die Übertragung der Login-Seite an den Browser findet ungeschützt statt.

Require Certificate (ncpweb.conf)

1 = Der Zugriff ist nur über SSL mit Zertifikat (am Browser) gestattet. Neben den Server-Zertifikaten sind auch signierte Benutzer-Zertifikate für die Administratoren nach X.509.3 nötig. Dies ermöglicht die Authentisierung der Administratoren gegenüber dem Server. Wird diese Funktion aktiviert, so müssen sich alle Administratoren mit ihrem Benutzer-Zertifikat ausweisen. Zusätzlich muss der Administrator Benutzername und Passwort in der Login-Maske eingeben. Das zum Benutzer-Zertifikat des Administrators gehörige Aussteller-Zertifikat muss am Web-Interface hinterlegt sein (siehe oben -> CAPath).

0 = In der Standardeinstellung ist der Zugriff über SSL ohne Zertifikat gestattet; Benutzername und Passwort müssen eingegeben werden.

Wurde am Browser das Aussteller-Zertifikat des Server-Zertifikats noch nicht als vertrauenswürdig eingestuft oder importiert, so erscheint zunächst eine Sicherheitsabfrage, da das Server-Zertifikat nicht verifiziert werden kann. In dieser Sicherheitsabfrage kann das Server-Zertifikat angezeigt werden. Die Sicherheitsabfrage erscheint nicht, wenn das Aussteller-Zertifikat des Server-Zertifikats am Browser importiert wurde.

(Mit dem neueren Internet Explorer 7 hat Microsoft die Warnung bei nicht eingetragenen Zertifikaten verschärft: Erschien vorher nur ein Popup “Sicher-

heitshinweis", so wird nun statt der Webseite eine Warnung über das ganze Fenster angezeigt, mit der Empfehlung, die Seite nicht zu benutzen. Sollte dieser Empfehlung Folge geleistet werden, so kann das Web-Interface nicht verwendet werden.)

PKISerialAccess (ncpweb.conf)

Zusätzlich zur Zertifikats-Anforderung (siehe oben -> Require Certificate) kann mit diesem Parameter die Seriennummer des eingehenden Zertifikats des Administrators abgefragt werden, wobei die Seriennummer in hexadezimaler Schreibweise angegeben wird (siehe Beispiel unten). In der Standardeinstellung ist dieser Parameter auskommentiert, d. h. die Seriennummer wird nicht abgefragt.

Sollen mehrere Seriennummern abgefragt werden, so muss die Zeile entsprechend oft untereinander mit den zugelassenen bzw. erforderlichen Seriennummern wiederholt werden. Zum Beipiel:

```
PKISerialAccess = 01:00:02:01
PKISerialAccess = 01:00:02:12
PKISerialAccess = 01:00:02:AA:9B:F4
```

IpAddrAccess (ncpweb.conf) = 0.0.0.0-255.255.255.255

Mit diesem Parameter kann der Zugriff von Browsern auf das Web-Interface eingeschränkt werden. Zugriff erhalten nur die Browser mit Quell-IP-Adressen, die in dem hier angegebenen Bereich liegen. (Die Standard-Einstellung ist ohne Einschränkung.)

Sollen mehrere eingeschränkte Adress-Bereiche möglich sein oder nur bestimmte IP-Adressen zugelassen werden, so muss die Zeile entsprechend oft untereinander wiederholt werden. Z. B.:

```
IpAddrAccess = 192.168.1.1-
192.168.1.255
IpAddrAccess = 172.16.15.44
IpAddrAccess = 172.16.15.47
```

Index