

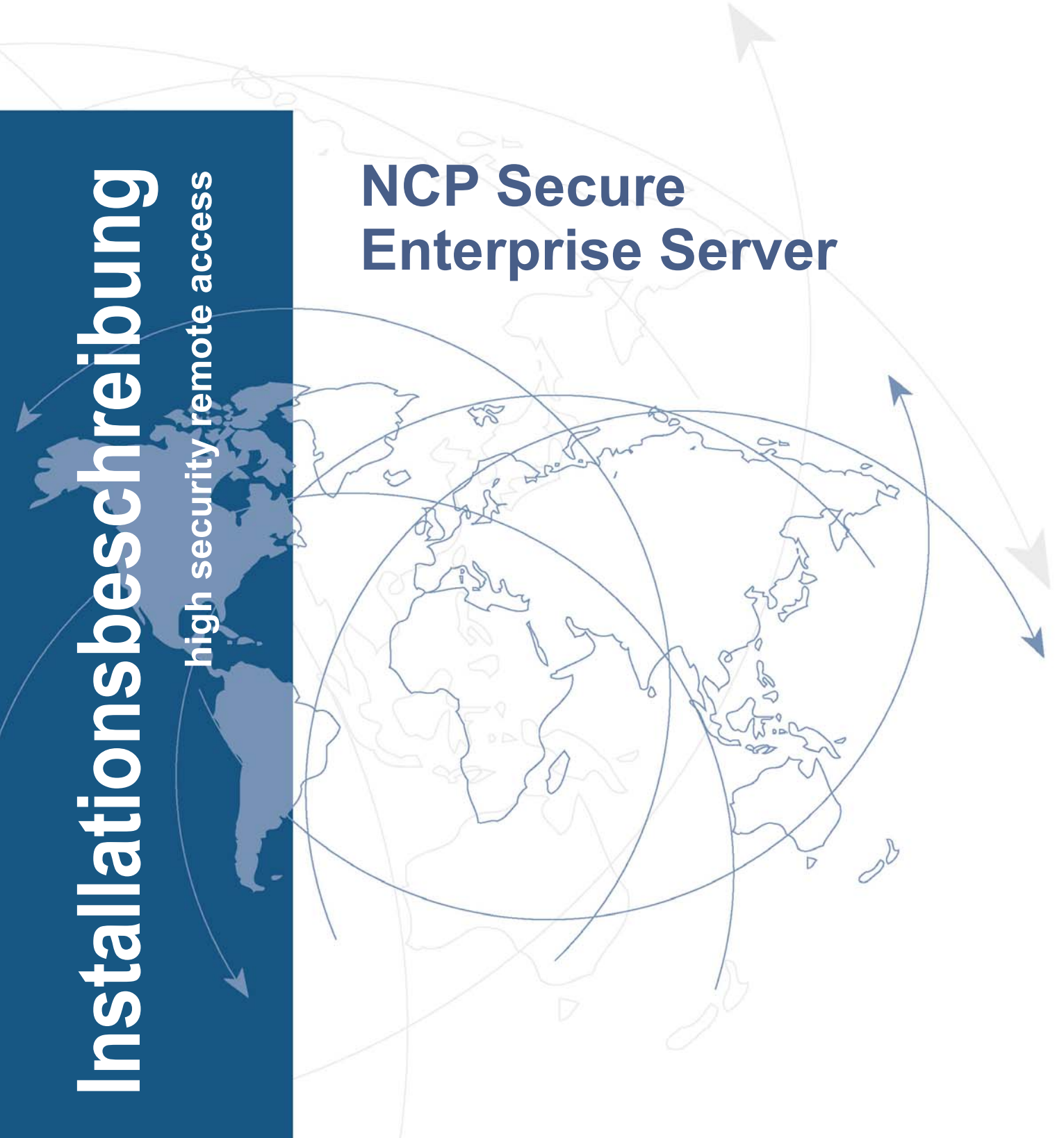


SECURE COMMUNICATIONS ■

# Installationsbeschreibung

high security remote access

## NCP Secure Enterprise Server





# **Secure Server**

## **Installationsbeschreibung**



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](http://www.ncp-e.com)  
E-mail: [info@ncp-e.com](mailto:info@ncp-e.com)

### Copyright

*Alle Programme und diese Beschreibung wurden mit größter Sorgfalt erstellt und nach dem Stand der Technik auf Korrektheit überprüft. Alle Haftungsansprüche infolge direkter oder indirekter Fehler, oder Zerstörungen, die im Zusammenhang mit den Programmen stehen, sind ausdrücklich ausgeschlossen.*

*Die in diesem Handbuch enthaltene Information kann ohne Vorankündigung geändert werden und stellt keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.*

*Ohne ausdrückliche schriftliche Erlaubnis von NCP engineering GmbH darf kein Teil dieser Beschreibung für irgendwelche Zwecke oder in irgendeiner Form elektronisch oder mechanisch, reproduziert oder übertragen werden.*

*Microsoft® und Windows® sind eingetragene Warenzeichen der Microsoft Corporation in den USA und/oder anderen Ländern. Alle anderen genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.*

© NCP engineering, Juli 2009

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](mailto: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](mailto:vertrieb@ncp-e.com)

<b>Systemvoraussetzungen (Windows)</b>	<b>7</b>
Adressen und Telefonnummern	7
LAN-Adapter	7
ISDN (nur für Direkteinwahl)	7
SNMP-Installation	7
<b>Installation unter Windows</b>	<b>9</b>
<b>Starten der Konfiguration</b>	<b>12</b>
<b>Update und Deinstallation</b>	<b>13</b>
Neues Installationsverzeichnis und Konvertierung bei Update auf V. 8.0	13
Neue Konfigurations-Datei bei Update auf Version 8.0	13
Neue RADIUS-Attribute für Filtergruppe in der Version 8.0	13
 <b>Systemvoraussetzungen (Linux)</b>	 <b>14</b>
Adressen und Telefonnummern	14
LAN-Adapter	14
ISDN (nur für Direkteinwahl)	14
SNMP-Modul	14
<b>Installation (Linux)</b>	<b>16</b>
Script-gesteuerte Installation	16
Installationsroutinen	16
Neuinstallation	17
Installation abschließen	17
<b>Update und Deinstallation (Linux)</b>	<b>18</b>
Neues Installationsverzeichnis und Konvertierung bei Update auf V. 8.0	18
Neue Konfigurations-Datei bei Update auf Version 8.0	18
Neue RADIUS-Attribute für Filtergruppe in der Version 8.0	18
<b>Start des Secure Servers Linux</b>	<b>19</b>
Dienste vom Start ausschließen	19
Script-Unterstützung im HA-Verbund	19

# Installationsbeschreibung

Diese Dokumentation beschreibt die Installation des NCP Secure Enterprise Servers einschließlich der Administrationskomponente Web-Interface.



Die **Lizenzierung** der Software ist im PDF **SES-Parameter-d** beschrieben.

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

## Systemvoraussetzungen (Windows)

Bevor Sie die Software installieren, beachten Sie die Daten zu folgenden Systemkomponenten:

### CPU

empfohlen Dual Core

### Taktung

pro 150 MHz bei einer Single Core CPU kann ein Datendurchsatz von ca. 4,5 Mbit/s. realisiert werden (incl. symmetrischer Verschlüsselung), pro 150 MHz bei einer Dual/Quad Core CPU kann ein Datendurchsatz von ca. 9 Mbit/s realisiert werden (incl. symmetrischer Verschlüsselung)

### Arbeitsspeicher

min. 1 GB

### Festplattenspeicher

ca. 400 MB freier Speicher auf der Festplatte

### 32-Bit Betriebssystem

Windows 2003 Standard / Enterprise Server Edition R2 SP2, Windows Server 2008 Enterprise SP2.

### 64-Bit Betriebssystem

Windows Server 2008 Enterprise SP2

### Hinweise



Halten Sie für die Dauer der Installation die CD mit der Betriebssystem-Software bereit. Es können Einspielungen von der Betriebssystem-Software nötig sein.



Achten Sie bei einer Installation unter Windows 2003 darauf, dass der Dienst "IPSec Driver" deaktiviert ist.

### Adressen und Telefonnummern

Notieren Sie sich vor der Installation unbedingt folgende Adressen und Telefonnummern:

- IP-Adresse und Netzwerk-Adresse (Subnet Mask) für den virtuellen NCP Netzwerk-Adapter. (Diese Adressen werden während der Installation eingegeben und vom Betriebssystem übernommen. Sie erscheinen anschließend im Konfigurationsbaum des Secure Server Managers als IP-Adresse und IP-Netzmaske des "Secure Sever Adapters" unter "Routing Intefaces".)

- ISDN Telefonnummer(n)
- MSN (Multiple Subscriber Number)

## LAN-Adapter

Ethernet: Alle gängigen LAN-Adapter für Windows 2003 / 2008 werden unterstützt. Installieren Sie die Hardware und vergeben Sie eine feste IP-Adresse für die Netzwerk-Karte in den Netzwerkeinstellungen des Betriebssystems. (Diese Adressen erscheinen anschließend im Konfigurationsbaum des Secure Server Managers als IP-Adresse und IP-Netzmaske unter "Routing Interfaces / LAN Adapter".)

## ISDN (nur für Direkteinwahl)

Die Einrichtung einer ISDN-Schnittstelle ist nicht nötig, wenn der Secure Server als VPN Gateway ohne Routing-Funktionalität eingesetzt wird.

Die ISDN-Schnittstelle muss eingerichtet und der ISDN-Adapter funktionsfähig sein, wenn die Routing-Funktionalität des Secure Servers genutzt werden soll. Der ISDN-Adapter muss mit dem ISDN über die Schnittstelle So oder S2m verbunden sein. Der zugehörige Treiber muss installiert sein.

Der ISDN-Adapter muss die Common ISDN API Version 2.0 unterstützen (CAPI). Die Server Software unterstützt den CAPI 2.0 Standard und läuft mit allen handelsüblichen ISDN-Adaptern, die ebenfalls diesen Standard unterstützen.

Prüfen Sie ob die ISDN-Verbindung über eine Festverbindung (DDV) oder eine Wählleitung (NT1) hergestellt wird.

## SNMP-Installation

Installieren Sie SNMP auf dem Rechner (über Systemsteuerung / Software / klicken Sie die Windows-Komponente "Verwaltungs- und Überwachungsprogramme" an und selektieren unter "Details" "SNMP (Simple Network Management Protocol)" für die Installation.)

Anschließend können Sie die "Eigenschaften von SNMP-Dienst" über die Systemsteuerung unter "Dienste / SNMP-Dienst" konfigurieren.

In das Feld mit "Agent" tragen Sie einen "Kontakt Namen" und einen "Standort" für den Secure Server ein. Die Check-Boxen unter "Dienst" können unverändert bleiben.

Öffnen Sie in den "Eigenschaften von Microsoft SNMP" das Feld "Traps". SNMP stellt Informationen zu wichtigen Server-Ereignissen zur Verfügung, die Traps genannt werden. Um Gebrauch von diesen Informationen machen zu können, müssen

die hier erwähnten Parameter entsprechend eingestellt werden. (Weitere Informationen zu Traps und deren Konfiguration erhalten Sie in der Microsoft Windows-Dokumentation.) Wenn keine Traps empfangen werden sollen, verlassen Sie das Trap-Feld unverändert. Die Adressen der Trap-Ziele können als IP- oder Web-Adressen eingetragen werden. Zum Beispiel 191.63.22.134 oder Manager1.ncp.de. Um mehrere Adressen einzugeben, wiederholen Sie die Prozedur.

Öffnen Sie in den “Eigenschaften von Microsoft SNMP” das Feld “Sicherheit”. Klicken Sie die Box “Echtheitsbestätigungs-Trap senden” (Send Authentication Trap) an, wenn ein Trap bei einem Login mit falschem Passwort gesendet werden soll.

Tragen Sie alle “Community Namen” (community names) ein, die Lese- und Schreibrechte besitzen sollen, zum Beispiel die Administrator(en)-Passwort(e), die nötig sind, um Werte erhalten oder ändern zu können.

### Wichtig



Lassen Sie aus Sicherheitsgründen den Standardeintrag “Public” unter “Community Names” nicht unverändert! Die hier eingetragenen Passwörter müssen mit SNMP-Passwort (Leserecht) und SNMP-Passwort (Schreibrecht) in der SNMP-Konfiguration des Secure Server Managers übereinstimmen. Nur dann kann der Secure Server über SNMP erreicht und gegebenenfalls konfiguriert werden.

Um die Anzahl der Rechner (Hosts) zu begrenzen, von denen SNMP-Pakete akzeptiert werden sollen, klicken Sie “SNMP-Pakete von diesen Hosts annehmen” an und fügen die IP-Adresse dieser Rechner hinzu. Klicken Sie auf “Übernehmen” (Apply) um die vorgenommen Einstellungen für den SNMP-Dienst anzunehmen.

Nachdem Sie die Einstellungen für die SNMP-Eigenschaften vorgenommen haben, klicken Sie auf “OK” und starten Sie den SNMP-Dienst neu.



## Installation unter Windows

Die Installation der Server Software erfolgt komfortabel über Setup. Der Installationsablauf ist für alle Versionen des Secure Servers identisch. Im folgenden ist die Installation unter Windows 2003/2008 beschrieben.

Die Server Software kann von CD oder Festplatte installiert werden. Sollten Sie bereits eine ältere Version der Software installiert haben, beachten Sie bitte das Kapitel "Update und Deinstallation der Server Software".

Mit der Server Software wird automatisch das Web-Interface und das Modul für die SSL VPN-Funktionalität installiert.

Die Server Software wird immer als Testversion installiert und über das Web-Interface lizenziert. Zur

**Lizenzierung** der Server Software und des SSL VPN-Moduls beachten Sie das PDF **SES-Parameter-d**.



Die Server Software wird unter Windows als virtueller LAN-Adapter installiert. Dieser LAN-Adapter wird bei der Installation automatisch in das System übernommen, einschließlich IP-Adresse und Microsoft SNMP. Im Konfigurationsbaum des Secure Server Managers erscheint der virtuelle LAN-Adapter später unter "Routing Interfaces" mit dem Namen "Secure Server Adapter".

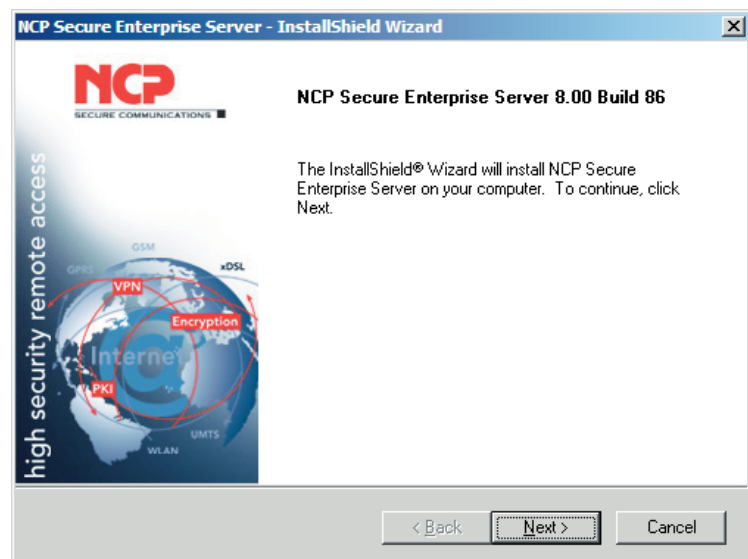
## Installation von der Festplatte

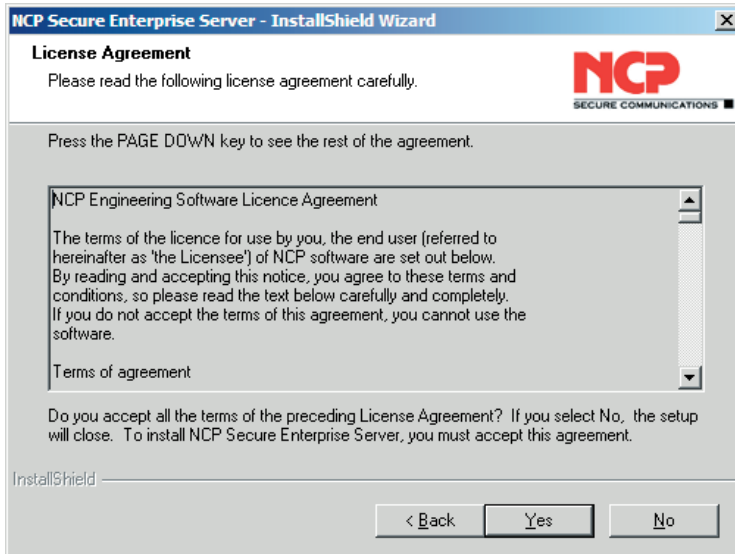
Wenn Sie die Software nach einem Download installieren möchten, entpacken Sie die Zip-Datei in einem neuen Verzeichnis. Wählen Sie mit dem Explorer das Verzeichnis "Disk1" und aktivieren Sie "SETUP.EXE" mit Doppelklick. Daraufhin startet der Install Shield-Assistent und führt Sie durch die Installation. (Die Installationssprache ist dabei immer English.) Für alle weiteren Installationsschritte folgen Sie den Anweisungen auf dem Bildschirm und den nachfolgenden Textabschnitten. Nach dem "Welcome Window" verläuft die Installation so wie unter "Installation von CD" beschrieben.

## Installation von CD

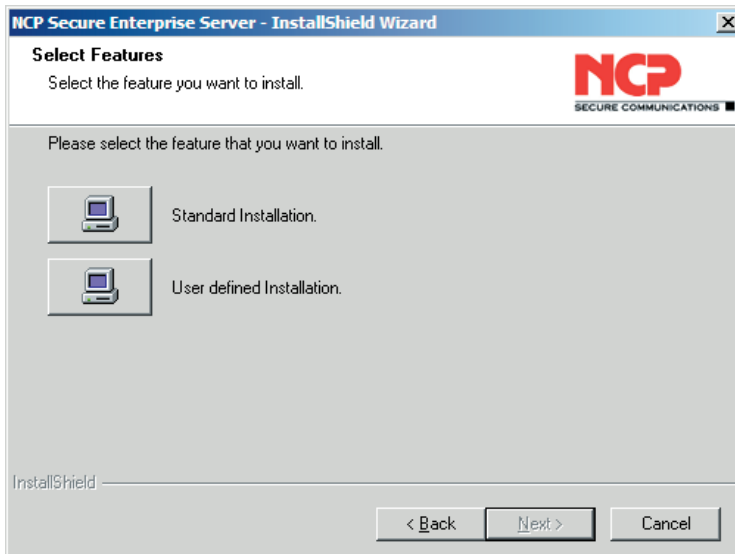
Nachdem Sie die CD in das Laufwerk Ihres Computers eingelegt haben, erscheint nach einigen Sekunden automatisch die NCP-Begrüßungsmaske auf Ihrem Monitor. Sie wählen mit einem Mausklick "Produkte installieren" und mit einem weiteren Klick die gewünschte Version. Anschließend bereitet das Setup-Programm den Install-Shield Assistenten vor, mit dessen Hilfe die Installation fortgesetzt wird.

Lesen Sie die Hinweise im Welcome-Fenster des Setup-Programms, bevor Sie auf "Next" klicken. (Abb. unten)





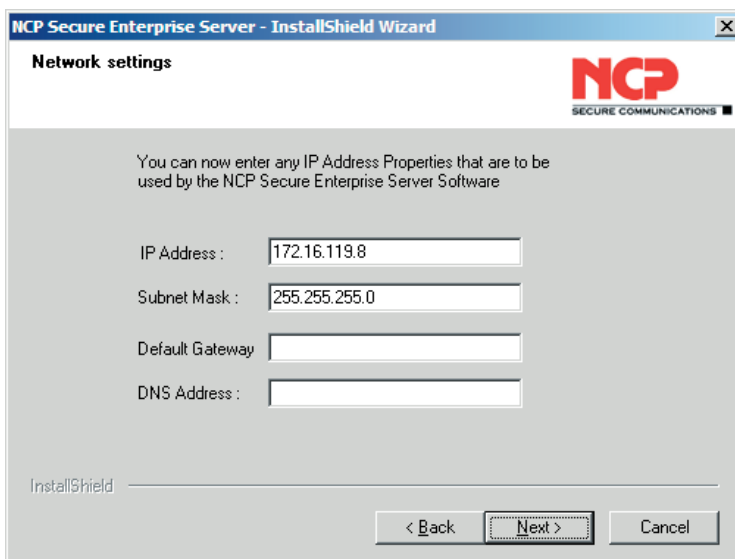
Anschließend werden die Lizenzbedingungen gezeigt. Wollen Sie die Software später lizenzieren (Software License Agreement), so stimmen Sie dem Vertrag mit “Yes” (Ja) zu. (Mit “No” (Nein) wird die Installation abgebrochen.)



Im folgenden Fenster können Sie zwischen “Standard Installation” und “User-Defined Installation” wählen.

1. In der “Standard Installation” werden IP-Adresse und Netzmaske des virtuellen NCP Netzwerk-Adapters automatisch eingetragen. Die Installation ist damit beendet und Sie werden aufgefordert das System zu booten.

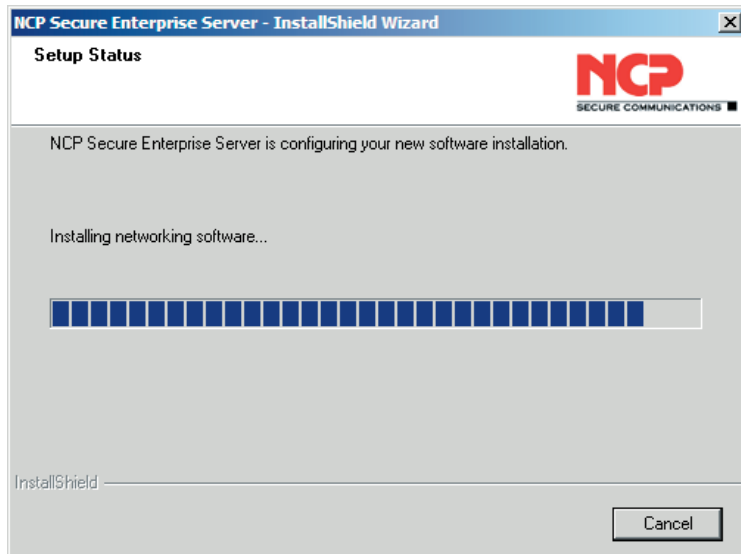
2. Um andere Werte entsprechend Ihrer Netzwerk-Umgebung eintragen zu können, wählen Sie “User Defined Installation”.



Im Fenster für “Network Settings” geben Sie folgende Adressen ein:

- IP-Adresse des Secure Servers (IP Address)
- Netzmaske (Subnet Mask)
- Default Gateway (Wenn die Software auf einem PC mit LAN-Anschluss installiert wird, darf keine Adresse für ein Default Gateway eingetragen werden! Andernfalls wird Ihr System ständig versuchen Verbindungen über das LAN aufzubauen anstatt über den Secure Server)
- Domain Name Server (DNS Address)

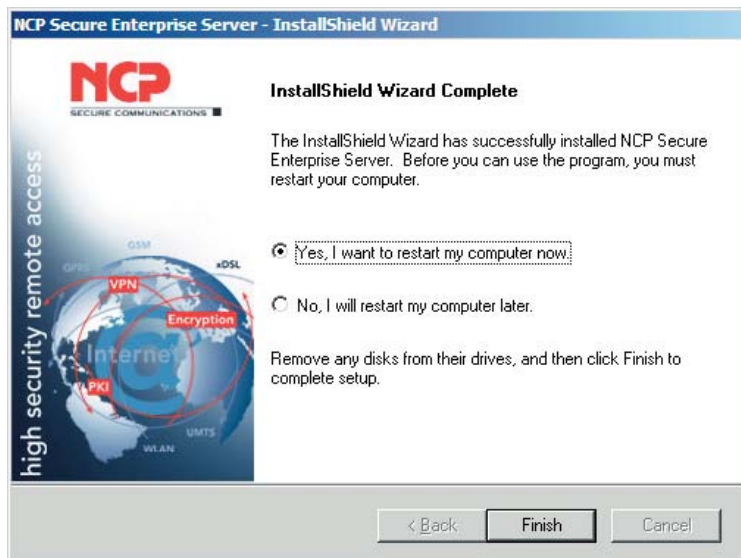
Nachdem Sie die Einträge vorgenommen haben, klicken Sie auf “Next”.



Legen Sie nun die CD mit dem Betriebssystem in das CD ROM-Laufwerk, damit das Setup-Programm verschiedene Dateien auf den PC kopieren kann. (Bei Updates ist dies nicht nötig!). Diese Dateien befinden sich im Verzeichnis \i386 auf der CD. Geben Sie den Pfad für dieses Verzeichnis an.

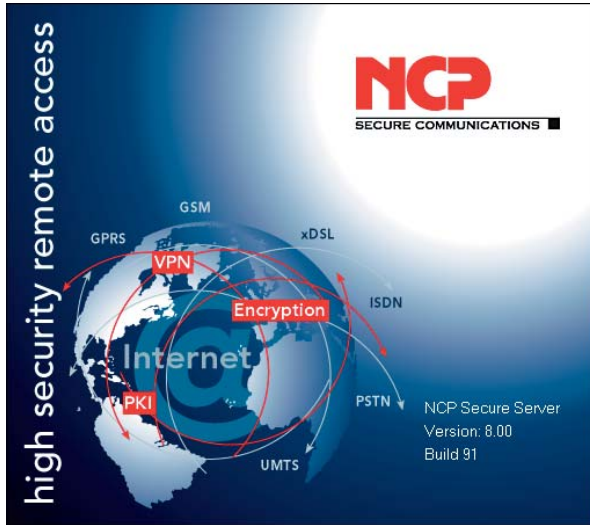
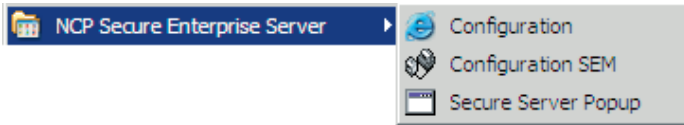
Windows stoppt nun die Dienste (stopping Services). Das Setup-Programm kopiert nun die benötigten System-Dateien und spielt die Server Software ein.

Nachdem die Software installiert wurde, werden die Programmgruppe und die Icons dafür angelegt.



Klicken Sie auf "Finish" (Beenden) und booten Sie den Rechner.

## Starten der Konfiguration



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

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

Über **Configuration SEM** legen Sie fest, ob die Konfiguration des Servers über das NCP Secure Enterprise Management, kurz SEM, und das dortige Server-Plug-in oder über das **Web-Interface** erfolgen soll.

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.



Die **Server-Konfiguration** und die **Konfigurationsparameter** sind im PDF **SES-Parameter-d** beschrieben.

## Update und Deinstallation

Wenn bei der Installation eine ältere Version der Server Software gefunden wird, haben Sie die Möglichkeit, ein Update durchzuführen. Link-Profil und die sonstige Konfiguration bleiben dabei erhalten.

Statt eines Updates kann auch eine Deinstallation der älteren Software durchgeführt und danach die neuere Software installiert werden. Auch in diesem Fall bleiben Link-Profil und die sonstige Konfiguration erhalten.

### Neues Installationsverzeichnis und Konvertierung bei Update auf Version 8.0

Installationsverzeichnis ist jetzt  
`<Programme>\ncp\SecureServer`

Alle Konfigurationsdateien, CA-Zertifikate und Dateien, die vorher unter `\ncprtr\certs` gespeichert waren, werden gesichert im Verzeichnis  
`<Programme>\ncp\SecureServer  
 \backups\updateFromNcprtr`

Beim Update werden alle Dateien unter `<WIN-DIR>\ncprtr` gelöscht. Die bestehende Konfiguration wird beim Update automatisch in das neue Format konvertiert.

### Neue Konfigurations-Datei bei Update auf Version 8.0

Die gesamte Konfiguration befindet sich in einer Datei mit XML-Format. Sie befindet sich unter Windows unter:

`<Programme>\ncp\SecureServer  
 \config\srwin.conf`

Darin enthalten sind neben der eigentlichen Konfiguration:

- 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).

Die Konfigurationsdatei wird automatisch ca. 30 Sekunden nach der letzten Konfigurationsänderung gespeichert.

### Neue RADIUS-Attribute für Filtergruppe in der Version 8.0

In älteren Server-Versionen wurde für die Filtergruppen im RADIUS der Index konfiguriert. Dieses Attribut wurde ersetzt durch ein RADIUS-Attribut für den Filtergruppennamen. Werden ältere und neue Gateways parallel betrieben, sollte eine neue RADIUS-Konfiguration für den neuen Secure Server angelegt werden.



Attribute mit Filtergruppen-Index sind im Secure Server 8.0 nicht mehr gültig! Sollte ein ungültiger Filtergruppennamen oder ein Filtergruppen-Index konfiguriert sein, wird der Benutzer abgelehnt!

## Systemvoraussetzungen (Linux)

Bevor Sie die Software installieren, beachten Sie die Daten zu folgenden Systemkomponenten:

### CPU

empfohlen Dual Core

### Taktung

pro 150 MHz bei einer Single Core CPU kann ein Datendurchsatz von ca. 4,5 Mbit/s. realisiert werden (incl. symmetrischer Verschlüsselung), pro 150 MHz bei einer Dual/Quad Core CPU kann ein Datendurchsatz von ca. 9 Mbit/s realisiert werden (incl. symmetrischer Verschlüsselung)

### Arbeitsspeicher

min. 1 GB

### Festplattenspeicher

Ca. 400 MB freier Speicher auf der Festplatte

### Betriebssystem

SUSE Linux Enterprise Server 10 SP 1,  
Kernel Version: 2.6.16.46-0.12-smp;  
openSUSE 11.0 (i586), Kernel 2.6.25-1.1-pae i686;  
openSUSE 11.1 (i586), Kernel 2.6.27.7-9-pae i686;  
Red Hat Enterprise Linux Server 5, Kernel 2.6.18-8.el5;  
Ubuntu 9.04 Server, Kernel 2.6.28-11-server



### Hinweise

Voraussetzung für das Paket-Handling bei VPN-Verbindungen ist das installierte Netfilterpaket iptables.

Bitte beachten Sie unbedingt zur Netzwerkeinrichtung:

Ab Linux SuSe Version 10.0 werden im Yast-Menü bei Installation der NCP Linux Software und Einrichtung der Netzwerkkarte zwei Methoden zur Auswahl gestellt:

- Benutzergesteuerte Methode mit Hilfe des Network Managers
- Traditionelle Methode mit ifup (interface up)

Bitte benutzen Sie die traditionelle Methode, da es ansonsten vorkommen kann, dass das eth-device (für Ethernet) von der NCP Software nicht erkannt wird.

## Adressen und Telefonnummern

Notieren Sie sich vor der Installation unbedingt folgende Adressen und Telefonnummern:

- IP-Adresse und Netzwerk-Adresse (Subnet Mask) für den virtuellen NCP Netzwerk-Adapter. (Diese Adressen werden während der Installation eingegeben und vom Betriebssystem übernommen. Sie erscheinen anschließend im Konfigurationsbaum des Secure Server Managers als IP-Adresse und IP-Netzmaske des "Secure Sever Adapters" unter "Routing Intefaces".)
- ISDN Telefonnummer(n)
- MSN (Multiple Subscriber Number)

## LAN-Adapter

Im Linux System muss mindestens ein Ethernet LAN-Adapter sowie das Netzwerk-Protokoll TCP/IP installiert und konfiguriert sein. [Weitere Kommunikationshardware (DSL, ISDN, Modem) entsprechend dem gewünschtem Einsatzprofil.] Desweiteren muss ein tap-Device (ethertap - älter, oder tuntap - neuer) entweder in den Kernel kompiliert oder als Modul vorhanden sein. Dieses Modul setzt den netlink-Support im Kernel voraus.

## ISDN (nur für Direkteinwahl)

Die Einrichtung einer ISDN-Schnittstelle ist nicht nötig, wenn der Secure Server als VPN Gateway ohne Routing-Funktionalität eingesetzt wird.

Die ISDN-Schnittstelle muss eingerichtet und der ISDN-Adapter funktionsfähig sein, wenn die Routing-Funktionalität des Secure Servers genutzt werden soll. Der ISDN-Adapter muss mit dem ISDN über die Schnittstelle So oder S2m verbunden sein.

Die ISDN-Verbindung kann sowohl über CAPI als auch über Modem-Emulation genutzt werden. Beachten Sie bitte, falls Sie die CAPI-Verbindung nutzen wollen, das auf ihrem System ein Link auf die CAPI-Library gesetzt ist /usr/lib/libcapi20.so oder /usr/lib/libcapi20.so.x.

## SNMP-Modul

Die gesamte Konfiguration des Servers erfolgt über das Web-Interface. Das SNMP-Modul wird nur genutzt, um Konfigurationsdaten zu betrachten. Das dafür benötigte Tool ist in dem Software-Paket mit enthalten.

Konfiguriert wird das SNMP-Modul über die Konfigurationsdatei `snmpd.conf`, die in `/etc/ncp/snmp` zu finden ist.

Diese Datei ist mit folgenden Einstellungen vorbelegt:

```
rocommunity      public
trapcommunity    public
syslocation      ""
syscontact       ""
syssservices     72
```



Aus Sicherheitsgründen sollten Sie die Community-Namen grundsätzlich ändern. Ein entsprechender Dialog wird während der Installation aufgerufen.

Bei der unbeaufsichtigten Installation werden die Defaulteinstellungen beibehalten. Sie sollten in diesem Fall möglichst schnell die entsprechenden Einträge manuell ändern.



## Installation (Linux)

Mit der Server Software wird automatisch Modul für die SSL VPN-Funktionalität installiert.

Die Server Software wird immer als Testversion installiert und über das Web-Interface lizenziert. Zur **Lizenzierung** der Server Software und des SSL VPN-Moduls beachten Sie das PDF **SES-Parameter-d**.



In der weiteren Beschreibung werden für die Versionsbezeichnung folgenden Platzhalter verwendet:  
 vvv . Versionsbezeichnung (z. B. 8.00)  
 bbb . Buildnummer (z. B. 009)

Sie erhalten die Software für den Secure Enterprise Server Linux auf einer CD oder als Download. Das Installationsscript befindet sich in dem Verzeichnis:

`Products/SecSvr/Bin/Linux/vvv.`



Beachten Sie bitte, dass Sie dem Installationsscript vor dem Start Ausführungsrechte vergeben müssen (`chmod +x ncp_ses_linux_vvv_bbb.i586.sh`).

### Script-gesteuerte Installation

Install-Script aufrufen:

```
- ./ ncp_ses_linux_vvv_bbb.i586.sh [u]
```

– Option u ... unattended installation

Unbeaufsichtigte Installation - die Installation erfolgt ohne Benutzereingaben.

Das Installations-Script wird abgearbeitet:

- entpackt das integrierte Archiv in das Verzeichnis `./ncpinst`
- wechselt in dieses Verzeichnis
- testet verschiedene Voraussetzungen für die Installation (s. u.)
- kopiert die zu installierenden Dateien in ihre Zielverzeichnisse und
- ermöglicht Grundeinstellungen für den Secure Server vorzunehmen (nur bei nicht unbeaufsichtigter Installation)

### Installationsroutinen

Drei mögliche Routinen können unterschieden werden. Die Abarbeitung des Scripts ist immer gleich:

#### Neuinstallation

Vor der Installation war kein Secure Server installiert bzw. er wurde vorher komplett deinstalliert.

#### Update

Eine Version des Secure Servers ist bereits installiert.

#### Unbeaufsichtigte Installation (Option “u”)

Die Installation erfolgt ohne Benutzereingaben. Es werden Standardwerte für Konfigurationsparameter eingesetzt. Im Falle eines Updates werden die bisherigen Einstellungen übernommen. Diese Installationsart kann sowohl bei Neuinstallation als auch bei Update gewählt werden.

Ein Sonderfall tritt ein, wenn bereits ein NCP HA Server auf dem System installiert ist. In diesem Fall werden gemeinsame Parametereinstellungen übernommen.

Das Installationsscript prüft als erstes verschiedene Installationsvoraussetzungen und Systemeinstellungen wie:

- ist der User als root angemeldet,
- ist die Kernel-Version größer gleich 2.6.25,
- ist eines der VPN-Device-Module installiert (tun oder ethertap),
- ist das Module iptables installiert,
- ist eine Version des NCP Secure Servers bereits installiert,
- ist gerade ein NCP Secure Server oder ein NCP HA Server gestartet. (Ist einer der beiden Server gestartet, wird dieser als erstes gestoppt.)





## Neuinstallation

Hier kopiert die Installationsroutine die benötigten Dateien (Anhang) in die entsprechenden Verzeichnisse und fragt interaktiv benötigte Konfigurationsparameter ab.

1. Schritt: Die Lizenzvereinbarung wird eingeblendet. Dieser muss zugestimmt werden, soll die Installation fortgesetzt werden. Innerhalb des Lizenztextes kann mittels der Tasten "Leertaste", "Enter", "Shift Page-Up", "Shift Page-Down" navigiert werden.
2. Schritt: Die IP-Adresse und die Netzmaske des VPN-Adapters manuell eingegeben werden. Wird keine Adresse angegeben, werden nach [Enter] die Standardwerte übernommen.
3. Schritt: SNMP Community Namen können eingegeben bzw. verändert werden.
4. Schritt: In der nun folgenden Eingabe wird entschieden, ob der Secure Server nach jedem Bootvorgang automatisch gestartet wird. Diese Möglichkeit ist nur für die Linux-Distributionen von SuSE und RedHat vorgesehen. Für alle anderen Distributionen sind die notwendigen Einträge in den Initscripts manuell vorzunehmen.
5. Schritt: Als letztes steht zur Auswahl den Secure Server sofort zu starten.



Ist bereits ein NCP HA Server installiert, werden Konfigurationseinstellungen, die von beiden gemeinsam genutzt werden, übernommen. Das betrifft:

- die SNMP Community Namen und
- die Behandlung des Initscripts.

Beide Parameter können im nachhinein noch geändert werden.

- die SNMP Community Namen durch editieren der `/etc/ncp/snmp/ncpsnmpd.conf` und
- die Aktivität des Initscripts mittels `/usr/local/ncp/sbin/ncpinststartup`.

Darüber hinaus werden Dateien, die von beiden Produkten gemeinsam verwendet werden und von dem das Erstellungsdatum des bereits installierten Produkts jünger ist, in das Verzeichnis

```
/var/adm/backup/ncp/ses/deinst-  
yymmdd[-1]
```

gesichert. Damit ist jederzeit möglich, die ursprüngliche Datei zurück zu sichern.

## Installation abschließen

Die Installation endet mit dem Start des Secure Servers. Das Installationsscript löscht automatisch das temporäre Installationsverzeichnis und beendet sich anschließend.

## Update und Deinstallation (Linux)

Wenn bei der Installation eine ältere Version der Server Software gefunden wird, wird die aktuell installierte Version angezeigt und gefragt, ob diese Version ersetzt werden soll. Bei der Antwort "nein" bleibt alles beim alten.

### Neues Installationsverzeichnis und Konvertierung bei Update auf Version 8.0

Bei einem Update auf Version 8.0 werden die Dateien wie folgt verschoben:

```
Installationsverzeichnis:
/usr/local/ncp/ses
Backup-Verzeichnis:
/var/adm/backup
/ncp/ses/deinst-ymmdd[-1]
Alte zu löschende Dateien in:
/usr/local/ncp/ses und
/etc/ncp
Konfigurationsdateien:
/etc/ncp/ses
Log-Dateien:
/var/log/ncp
```

Die bestehende Konfiguration wird beim Update automatisch in das neue Format konvertiert. Die einzige Entscheidung die zu treffen ist, ist ob der Server sofort gestartet werden soll.

Möchten Sie die Software noch einmal komplett neu installieren oder komplett entfernen, so starten Sie das Script "ncpsesdeinstall". Damit wird die gesamte Installation des Secure Servers von Ihrem System entfernt. Sie erhalten allerdings während der Deinstallation die Möglichkeit zu entscheiden, ob Sie die Konfigurations- und Logdateien oder auch alle zuvor installierten Dateien gesichert haben möchten.

Auch wenn Sie sich entscheiden, alles komplett von ihrem System zu entfernen, werden die Konfigurations- und Logdateien vorsichtshalber nach  
`/var/adm/backup/ncp/ses/deinst-ymmdd[-1]`  
 gerettet. Diese Dateien können, wenn nicht mehr benötigt, manuell entfernt werden.

### Neue Konfigurations-Datei bei Update auf Version 8.0

Die gesamte Konfiguration befindet sich in einer Datei mit XML-Format. Sie befindet sich unter Linux unter:  
`/etc/ncp/ses`

Darin enthalten sind neben der eigentlichen Konfiguration:

- 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).

Die Konfigurationsdatei wird automatisch ca. 30 Sekunden nach der letzten Konfigurationsänderung gespeichert.

### Neue RADIUS-Attribute für Filtergruppe in der Version 8.0

In älteren Server-Versionen wurde für die Filtergruppen im RADIUS der Index konfiguriert. Dieses Attribut wurde ersetzt durch ein RADIUS-Attribut für den Filtergruppennamen. Werden ältere und neue Gateways parallel betrieben, sollte eine neue RADIUS-Konfiguration für den neuen Secure Server angelegt werden.



Attribute mit Filtergruppen-Index sind im Secure Server 8.0 nicht mehr gültig! Sollte ein ungültiger Filtergruppennamen oder ein Filtergruppen-Index konfiguriert sein, wird der Benutzer abgelehnt!

## Start des Secure Servers Linux

Wurde bei der Installation der automatische Start des Servers gewählt (Standard-Einstellung, nur SuSE und RedHat), so ist er nach dem Hochfahren des Systems sofort betriebsbereit. Ungeachtet dessen kann der Server jederzeit gestoppt und wieder gestartet werden. Die Kommandos dazu lauten:

```
rcncpses start
rcncpses stop
rcncpses restart
```

(Startet den Server nach dem Stoppen)

```
rcncpses try-restart
```

(Startet den Server nachdem er erfolgreich gestoppt wurde)

Mit dem Kommando "rcncpses status" kann der aktuelle Ausführungsstatus des Servers abgefragt werden. Dazu muss der User root-Rechte besitzen und die Umgebungsvariable PATH muss das Verzeichnis "/usr/local/ses" eingetragen sein. Falls nicht der automatische Start des Secure Servers gewählt wurde, kann man mit diesen Kommandos den Server auch manuell steuern.

Mit Hilfe des Scripts "ncpinststartup" kann die Einstellung, ob der Server automatisch beim Boot des Systems geladen werden soll oder nicht geändert werden. Das Script im Verzeichnis "/usr/local/ncp/ses/" muss mit folgenden Optionen gestartet werden:

```
/usr/local/ncp/ses/ncpinststartup y|n
```

**y:** Das Startupsript des Secure Servers wird aktiviert, d.h. der Server wird während des nächsten Hochfahrens des Systems gestartet.

**n:** Das Startupsript des Secure Servers wird wieder deaktiviert.

## Dienste vom Start ausschließen

Bestimmte Dienste können vom Start ausgeschlossen werden. Dazu stehen bestimmte Parameter zur Verfügung in der Datei:

```
/usr/local/ncp/ses/sesstart
```

Wird der jeweilige Parameter auf "1" gesetzt, wird der Dienst gestartet, mit "0" wird er vom Start ausgeschlossen.

Parameter	Beschreibung	Dienst
POLSRV	Policy Server	ncppolsrzd
SSLVPN	SSL/VPN Server	ncpsslvpnd
WEBCFG	Web-Interface	ncpwebd

## Script-Unterstützung im HA-Verbund

Für die Umschaltung zwischen Master- und Backup-Server in einem HA-Verbund werden zwei Leer-Scripte mit installiert, dve\_up und dve\_down. Mit Hilfe dieser Scripte kann der Benutzer beliebige Aktionen ausführen lassen (z. B. Interface aktivieren / deaktivieren).

Die Scripte werden mit der Extension "sam" installiert, um bereits angelegte Scripte nicht zu überschreiben. D. h. um diese Scripte einsetzen zu können, müssen sie zunächst umbenannt werden:

```
dve_up.sam -> dve_up
dve_down.sam -> dve_down
```

