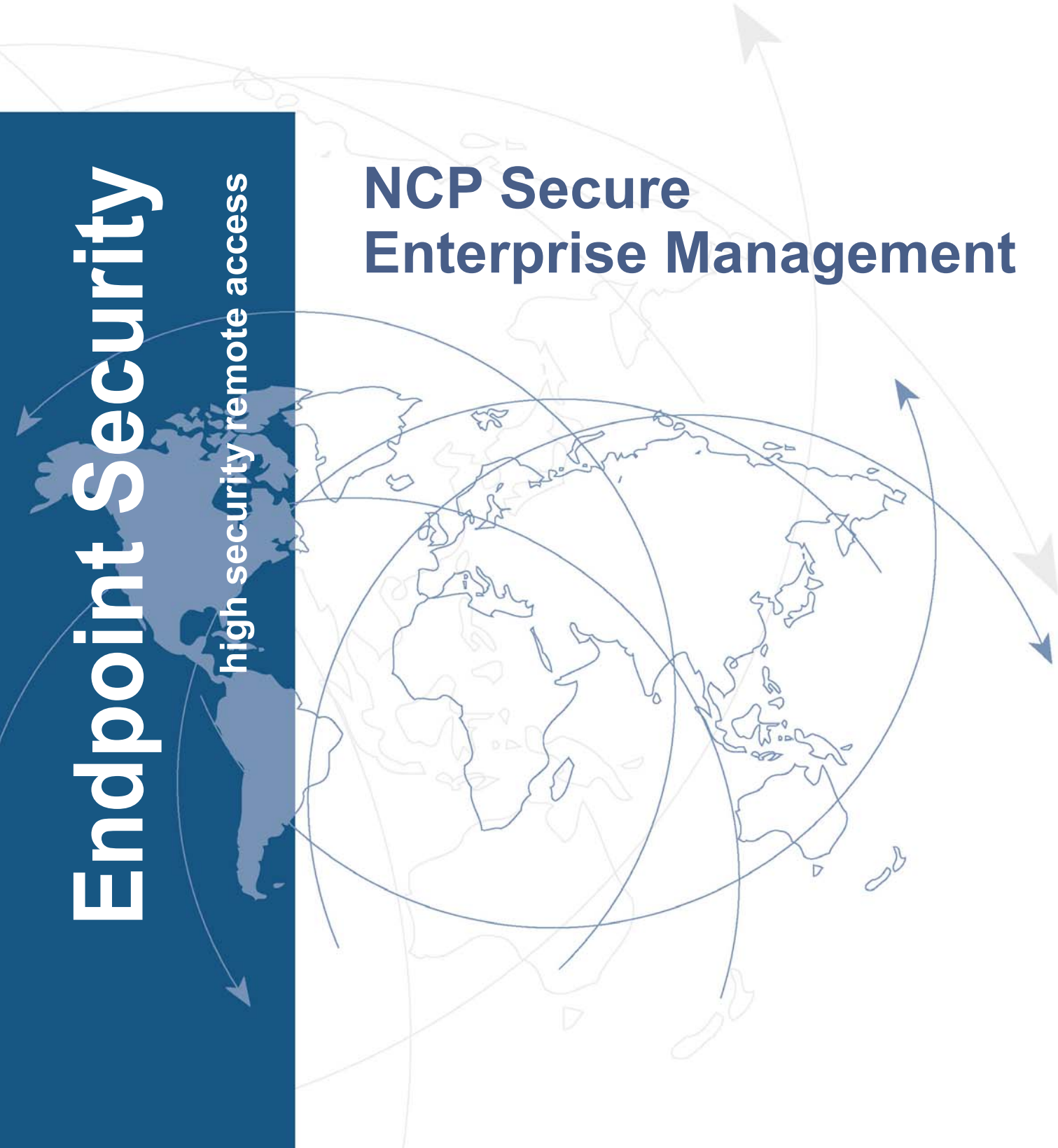
NCP
SECURE COMMUNICATIONS

Endpoint Security

high security remote access

# NCP Secure Enterprise Management



NCP SECURE COMMUNICATIONS

# Secure Enterprise Management

## Endpoint Security

Sie erreichen unsere NCP Experten unter folgenden Hotlines:

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

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

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

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

Network
Communications
Products engineering GmbH

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

## Copyright

# Endpoint Policy Enforcement Plug-in

**Dieses Dokument beschreibt wie die Funktion der Endpoint Security in der NCP Secure Enterprise Lösung arbeitet und liefert einen Leitfaden für eine schrittweise onfiguration. Die Endpoint Security kann mit folgenden Produkten eingesetzt werden:**

– NCP Secure Server ab Version 7.0

– NCP Secure Enterprise Client ab Version 9.0

– NCP Secure Management Server ab Version 1.04

## Einrichten der Kommunikationsbeziehungen

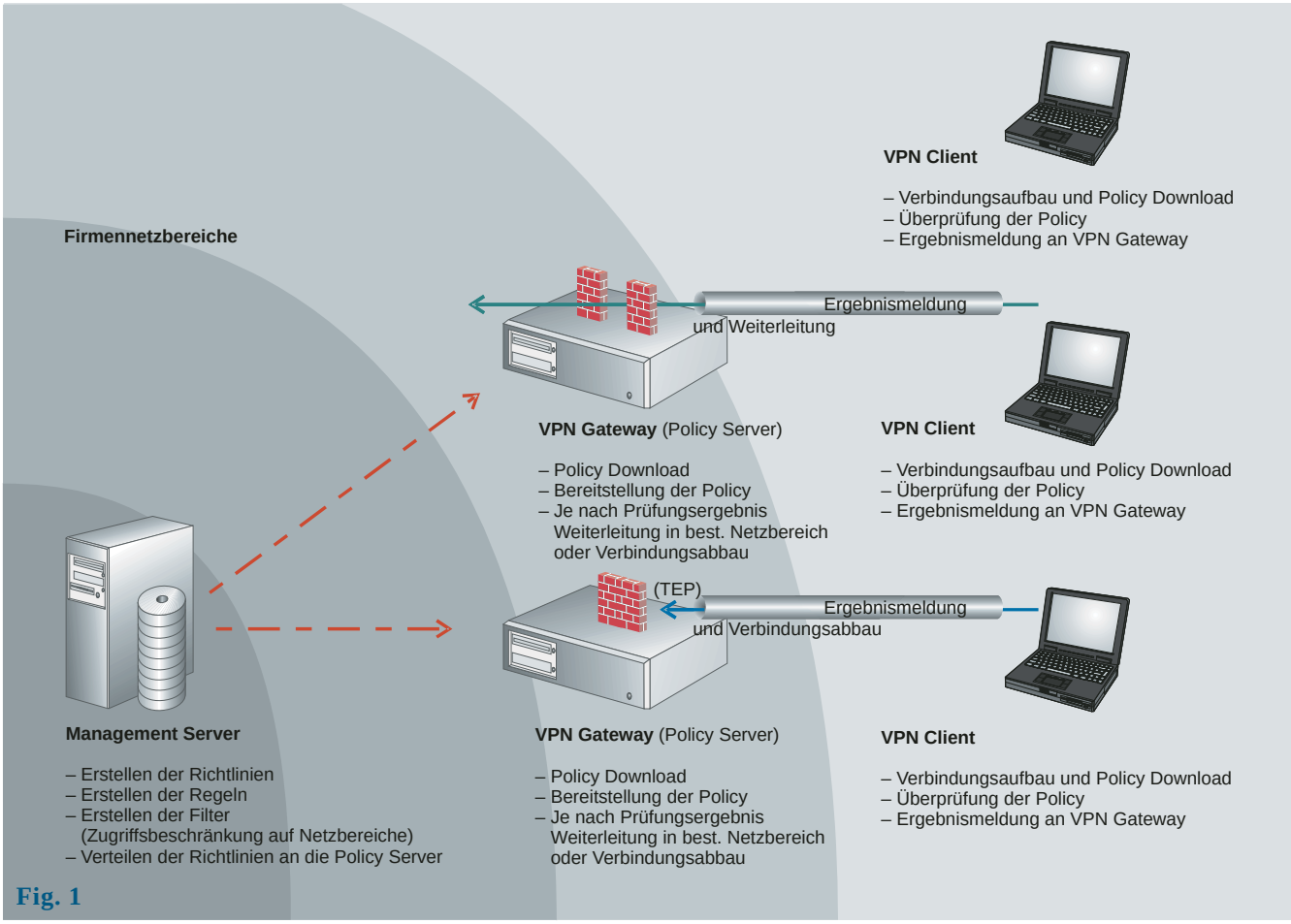



Fig. 1

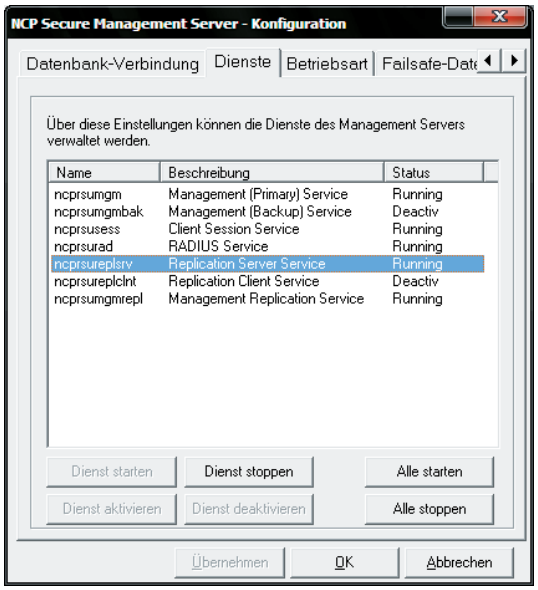
Figur 1 gibt einen Überblick über die Kommunikation der beteiligten Komponenten. So werden auf dem Management Server die benötigten Policies mittels Management Console erstellt bzw. editiert, anschließend durch den Replikations-Dienst auf die NCP Secure Server (VPN Gateways) übermittelt und schließlich den VPN-Clients beim Herstellen der VPN-Verbindung zugeordnet.

Es können mehrere Richtlinien erstellt und verwendet werden, z. B. für verschiedene Gruppen wie Administratoren, VIPs, Standardbenutzer, Außendienst oder externe Zugänge.

Werden die Regeln der “Endpoint Security”, die in den Sicherheits-Richtlinien vom Secure Enterprise Management zentralseitig festgelegt wurden, von der Remote-Seite nicht erfüllt, so wird der Netz-Zugang definitionsgemäß eingeschränkt oder gesperrt.

# Verteilung an die VPN Gateways (Policy Server)

Zunächst muss sichergestellt werden, dass die erzeugten Richtlinien der Endpoint Security an die vorgesehenen NCP Secure Server verteilt werden können. Dazu muss zwischen den NCP Secure Server(n) und dem NCP Secure Management Server der Verbindungsaufbau über Port TCP 12506 möglich sein. Über diesen Port bezieht der Secure Server die aktuellen Richtlinien. Secure Server und Management Server müssen entsprechend konfiguriert werden, so muss auf dem Management Server der Dienst “Replication Server Service” aktiviert und gestartet werden, sofern es nicht bereits geschehen ist. Dies geschieht, indem Sie auf dem Management Server das Menü “Start / Programme / NCP Management Server” öffnen und die Anwendung “Configuration” starten. Über den Reiter “Dienste” können Sie die benötigten Dienste aktivieren und starten. (Abb. unten)



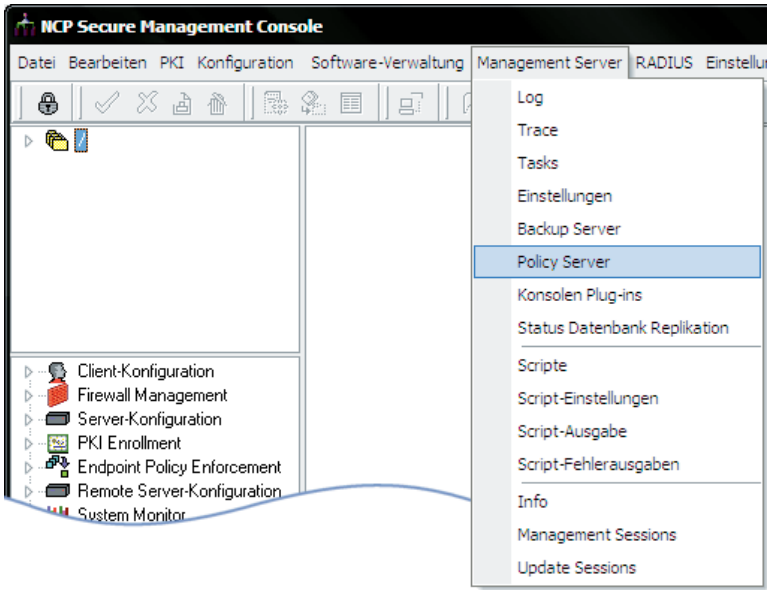

Wenn Sie den Management Server unter Linux betreiben ist der Service automatisch aktiviert, überprüfen lässt sich dies auf dem Management Server durch den Aufruf:

```
/usr/local/ncp/mgmsrv/ncpmgmsrv status
```

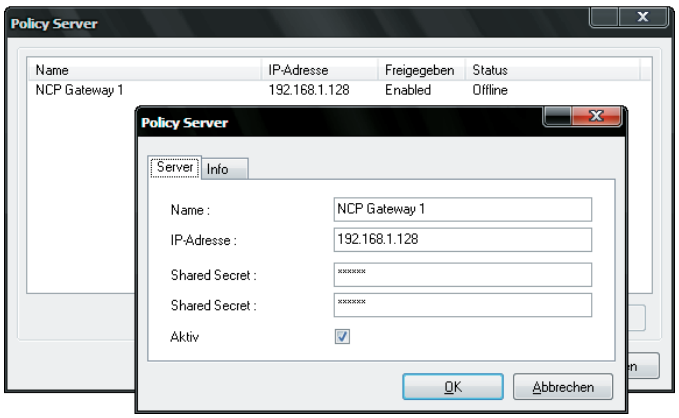
Im nächsten Schritt müssen Sie die Kommunikationsbeziehung zwischen Management Server und Secure Server konfigurieren, dazu starten Sie die Management Console und melden sich am Management Server an. Sie benötigen Berechtigungen, um die Server-Konfiguration zu verändern, sollten Sie nicht über die notwendigen Rechte verfügen, so müssen Sie sich diese von Ihrem System-Administrator über dir Rechteverwaltung des Management Servers zuweisen lassen.

(Beachten Sie dazu auch das PDF **Plug-in-Konzept und Gruppenstruktur**)

Über den Menüpunkt “Management Server/ Policy Server” gelangen Sie zur Konfigurationsoberfläche, in der Sie die beteiligten NCP Secure Server eintragen können. (Abb. unten)




In dem erscheinenden Konfigurations-Fenster tragen Sie die Parameter für die jeweiligen Secure Server (VPN Gateways) ein (Beschreibung nächste Seite):



### Name / Beschreibung

Der Name kann beliebig vergeben werden, sollte aber der Übersichtlichkeit wegen mit dem Namen des entsprechenden Secure Servers korrespondieren.

### IP−Adresse des Secure Servers

Die hier einzutragende IP-Adresse (darf nicht 127.0.0.1 lauten) ist die IP-Adresse des Secure Servers (Policy Servers).

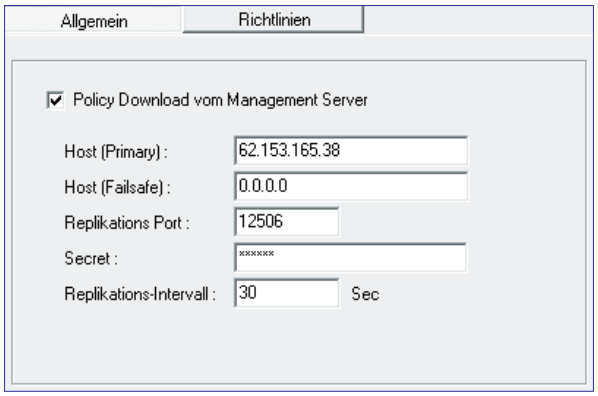
### Shared Secret

Das Shared Secret kann frei gewählt werden, es muss jedoch mit dem am Secure Server übereinstimmen.

## Konfiguration der Secure Server

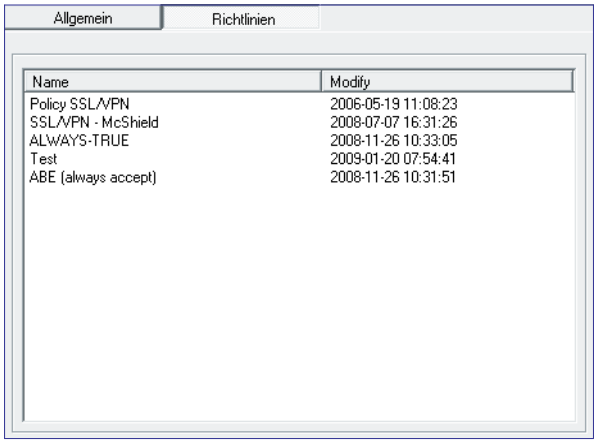
Im Anschluss daran werden die Secure Server für die Kommunikation konfiguriert. Hierfür starten Sie das Web-Interface des Secure Servers (Version >= 8.0) oder den Secure Server Manager (Version < 8.0) oder in der Management Console (Version >= 2.02) das Server Configuration Plug-in.

Um den Secure Server konfigurieren zu können (Version >= 8.0) muss im Konfigurationsbereich der Abschnitt “Lokales System / Client-Richtlinie” geöffnet werden. (Bei älteren Versionen als 8.0 muss im Konfigurationsbaum “Client Policy Enforcement” geöffnet werden).




Im Parameterfeld “Allgemein” (Abb. links) wird eingestellt ob und wie oft die Richtlinie vom Management Server heruntergeladen werden soll. Dazu muss die IP-Adresse des Management Servers (Host) angegeben werden und der Policy Download vom Management Server aktiviert werden. Der hier einzutragende Replikations-Port muss mit dem Port für den Replikationsdienst am Management Server übereinstimmen (Standard: 12506). Das Shared Secret muss mit dem am Management Server konfigurierten übereinstimmen (siehe oben).

Mit dem Replikations-Intervall bestimmen Sie den zeitlichen Abstand, innerhalb dessen der Secure Server die Client Policy am Management Server auf Aktualität prüft und gegebenenfalls die neueste Version herunterlädt. Das Intervall wird in Sekunden angegeben (Standard ist 30 sec).




Die heruntergeladenen Richtlinien werden im benachbarten Fenster namentlich und mit einem Zeitstempel versehen aufgeführt.

Da bei einem Download vom Management Server prinzipiell alle Richtlinien repliziert werden, die dort erstellt wurden, sollte durch die Namensgebung der Richtlinien (Policy Name) bei Erstellung am Management Server kenntlich gemacht werden, um welche Art der Regeln es sich dabei handelt.

# Regeln der Endpoint Policy

Mit dem NCP Secure Enterprise Management (SEM), der zentralen Verwaltungs-Einheit, kann das Regelwerk zur Einhaltung von Sicherheits-Richtlinien (Policy Rules) konfiguriert und den eingesetzten Komponenten übergeben werden.

Die Sicherheits-Richtlinien beinhalten Vorgaben von der zentralen Administrations-Komponente (SEM) an die Komponente, die sich mit dem Firmennetz verbindet, d. h. für den Secure Client oder den Anwender von SSL/VPN. Diese Vorgaben müssen vom entfernten System erfüllt sein, um einen bestimmten Zugriff auf das zentrale Firmennetz zu erhalten. Dabei spielt die Verbindungsart und das eingesetzte Tunneling-Verfahren des Clients keine Rolle.

Die Sicherheits-Richtlinien werden durch den Administrator vorgegeben, wobei die jeweilige Architektur des Firmennetzes, sowie auch die Verantwortlichkeit der Benutzer von Bedeutung sein können.

Mit diesen Sicherheits-Richtlinien wird die Netzwerksicherheit dergestalt erhöht, als sie den Zugriff des Clients auf Ressourcen hinter dem Tunnel-Endpunkt des Secure Servers regeln, bzw. mittels bestimmter Filter einen benutzerspezifisch zu definierenden Netzwerkbereich nach Erfüllung der Vorgaben freigeben.

Die Einhaltung der vorgegebenen Sicherheits-Richtlinien ist für den Benutzer zwingend und kann weder umgangen werden, noch sind die Richtlinien manipulierbar.

Nach dem Verbindungsaufbau des entfernten PCs zum zentralen Gateway können unter anderem folgende, den Client-PC betreffende Parameter überprüft werden:

– Betriebssystem-Informationen (z. B. Version, Hotfix-Stand)

– Software-Stand des Secure Enterprise Clients

– Dienste-Informationen

– Datei-Informationen

– Status eines Viren-Scanners

– Inhalte bestimmter Registry-Werte

– Inhalte von Zertifikaten (Benutzer-und Hardware-Zertifikat)

## Richtlinien

Die möglichen Vorgaben der Richtlinien beziehen sich unter anderem auf die Rechner-Konfiguration der Remote-Seite, wobei Umgebungs-Variablen und Software-Versionen auch unabhängig von der NCP Software abgefragt werden können.

Prinzipiell können sowohl für die SSL/VPN-Anwender-PCs als auch für die PCs der Secure Clients die gleichen Sicherheits-Richtlinien zum Einsatz kommen. Je nach installiertem Betriebssystem auf dem Anwender-PC und der installierten Client-Komponente (Secure Client) können jedoch nur die Werte und Parameter abgefragt und verglichen werden, auf die ein Zugriff am PC möglich ist. Diese Zugriffsmöglichkeiten sind auf dem PC eines SSL/VPN-Anwenders für gewöhnlich durch die Rechtestruktur des Betriebssystems stärker eingeschränkt.

## Abgleich mit den vorgegebenen Sicherheits-Richtlinien

Bei jeder Verbindung eines Remote-Systems mit dem zentralen Gateway (Secure Server) wird die jeweils gültige Endpoint Policy heruntergeladen und abgeglichen. Bei Nichterfüllung der Vorgaben können unterschiedliche Meldungen oder Aktionen erfolgen, je nachdem ob SSL/VPN genutzt wird oder der Secure Client im Einsatz ist.

### SSL/VPN

Policy Rules für SSL/VPN-Anwender-PCs erhalten vom Management-System den Wert für einen Security Level, der einer SSL/VPN-Anwendung zugeordnet werden kann. Entsprechend erhält das Remote-System je nach Regelerfüllung einen Security-Wert, der die entsprechende(n) Anwendung(en) zur Verwendung freischaltet, d. h. auf der Startseite des Browsers darstellt. (Siehe dazu weiter unten “Security Level der Sicherheits-Richtlinien”)

### Secure Client

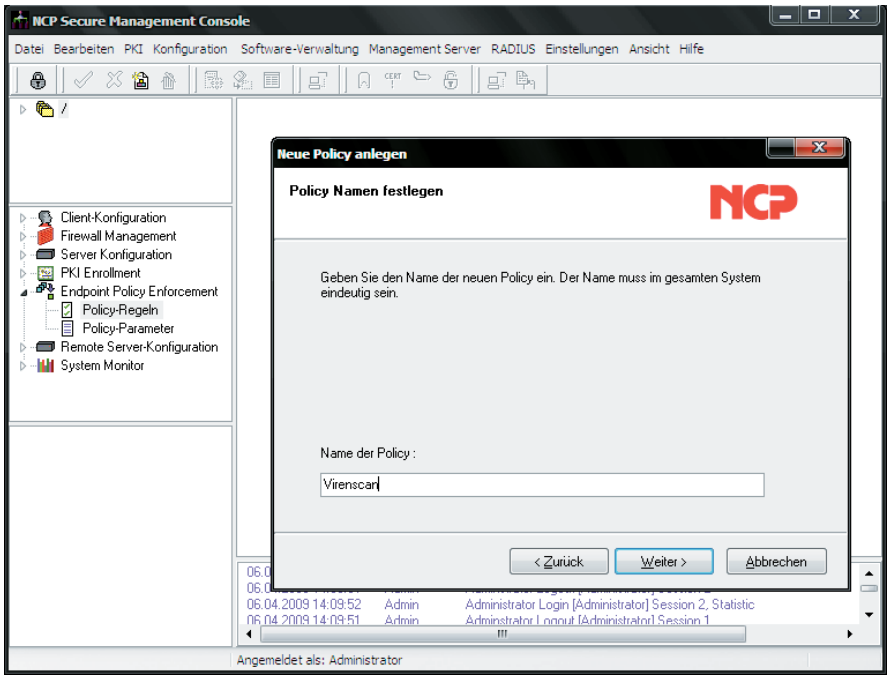
Der Secure Client verfügt über eine Statusanzeige zur Endpoint Security. Während der Prüfung der Policy, nachdem die Verbindung aufgebaut wurde, erscheint es in gelber, wenn die Richtlinien erfüllt werden in grüner Farbe, wenn die Richtlinien nicht erfüllt werden in roter Farbe, wonach konfigurationsabhängig die Verbindung zum Gateway wieder abgebaut wird.

Abweichungen am PC des Secure Clients von den Sollvorgaben werden protokolliert und können unterschiedliche Meldungen bzw. Aktionen auslösen. Diese sind:

– Anzeige einer Meldung am Client (ab Client-Version 9.0)
– Ausgabe einer Meldung im Log des Monitors
– Senden einer Meldung zum Management Server
– Senden einer Meldung zu einem Syslog Server
– Trennung der VPN-Verbindung
– Einschränkung auf einen Netzbereich

Zum Beispiel 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 “Client Policy” 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.

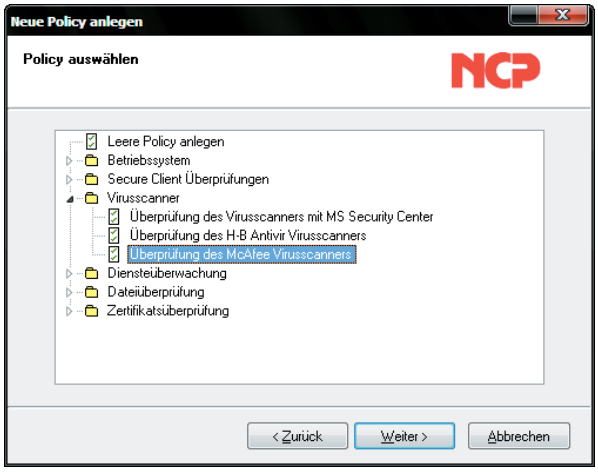
# Erstellen der Richtlinien (Policies)



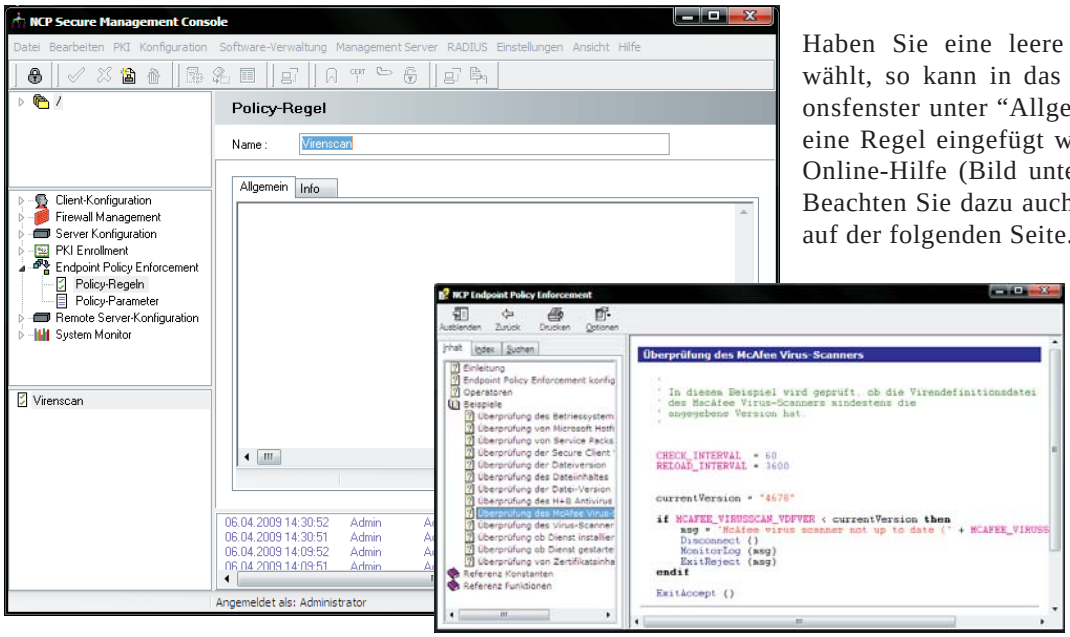

Die Policies werden an der Secure Management Console ebenso gruppenbezogen erstellt wie die Client-Konfigurationen. D. h. nachdem die gewünschte Gruppe bzw. Firma im Gruppenbereich der Console markiert wurde, kann für diese Gruppe eine Policy erstellt werden.

Im Plug-in-Bereich öffnen Sie den Konfigurationsknoten “Endpoint Policy Enforcement” und klicken die “Policy-Regeln” an. Eine neue Policy wird nun mit Hilfe eines Assistenten angelegt, indem ein “Neuer Eintrag” aus dem Bearbeiten-Menü selektiert wird.

Der Assistent fragt zunächst nach dem Namen für die neue Richtlinie (Policy). Bei Namensvergabe ist darauf zu achten, dass über diesen Namen die Richtlinie für ein bestimmtes Link-Profil am Server Manager selektiert werden kann. (Hier in der Abbildung soll der Name der Funktion entsprechen den Virenscanner zu überprüfen, z. B. Virenscan.)




Anschließend kann alternativ eine leere Policy angelegt werden, worin im nächsten Schritt die Regeln eingetragen werden, oder aus der angebotenen Liste der Beispiele wird eine vordefinierte Regel selektiert und mittels [Weiter]-Button in die Richtlinie eingefügt. (Hier in der Abbildung z. B. eine Regel, die den Virenscanner betrifft.)




Haben Sie eine leere Richtlinie ausgewählt, so kann in das leere Konfigurationsfenster unter “Allgemein” (Bild links) eine Regel eingefügt werden, die aus der Online-Hilfe (Bild unten) kopiert wurde. Beachten Sie dazu auch die Beschreibung auf der folgenden Seite.

## Erstellen der Regeln mit der Online-Hilfe

Zur Erstellung der Regeln kann die Online-Hilfe genutzt werden, die sich mit [F1] öffnet, nachdem Sie den Text-Cursor in das Konfigurationsfenster gesetzt haben. Aus den Beispielen oder der Referenzliste kann eine Funktion bzw. Regel ausgewählt und mit Copy&Paste in das Konfigurationsfenster eingetragen werden.

Da die Funktionen und Konstanten, die mit der Online-Hilfe des Endpoint Security PlugIns zur Verfügung gestellt werden, nicht auf allen Betriebssystemplattformen gleichermaßen angewendet werden können und möglicherweise von der eingesetzten Version des Policy Clients am remote PC nicht unterstützt werden, wird in deren Beschreibung das jeweilige Betriebssystem genannt, für das sie eingesetzt werden können, sowie auf die Version des Policy Clients verwiesen. Wenn nicht ausdrücklich gekennzeichnet (z. B. nur für Windows CE), sind die Konstanten für alle Betriebssystemplattformen verwendbar.

Unter “Betriebssystem” wird aufgeführt, unter welchem Betriebssystem der NCP Enterprise Client aktuell installiert sein muss, bzw. unter welchem der SSL/VPN remote PC betrieben wird, damit diese Funktion für die Endpoint Security ausgewertet werden kann. Wird ein hiervon abweichendes Betriebssystem eingesetzt, so werden bei der Prüfung der Security-Richtlinie entweder leere Zeichenketten (statt eines Return Strings) oder eine Null (statt eines Zahlenwertes) erzeugt und eine Verbindung vom Client zum Server abgewiesen.

“Version” beschreibt, welche Version der Policy Client besitzen muss, damit diese Funktion ausgeführt werden kann. Die Version des Policy Clients kann im Logfile abgelesen werden, sofern Endpoint Security eingesetzt wird. Die erste ausgelieferte Version ist 1.0.0.0.

Die Referenzlisten der Konstanten und Funktionen sind geordnet nach Gruppen der Funktionalität. Z. B. sind nach “FileExists” (der Abfrage nach dem Vorhandensein einer Datei) die Abfragen nach Eigenschaften einer Datei sortiert, wie “GetFileSize”, “GetFileVersion” oder “GetFileSha1Hash”.

## Eintragen der Regeln in das Konfigurationsfenster der Richtlinie

Es gibt verschiedene Möglichkeiten, Regeln in das Konfigurationsfenster “Allgemein” einzutragen:

– Ein Klick auf die rechte Maustaste öffnet das Kontextmenü. Selektieren Sie “Neue Regel hinzufügen” und wählen Sie aus dem Assistenten eine Regel aus.

– Setzen Sie den Text-Cursor in das Konfigurationsfenster und öffnen Sie mit [F1] die Online-Hilfe. Wählen Sie aus den Beispielen eine Regel aus und fügen Sie sie mit Copy&Paste in das Konfigurationsfenster ein.

– Schreiben Sie eine Regel gemäß der Policy-Syntax in das Konfigurationsfeld und drükken Sie [F1]. Entspricht die eingegebene Buchstabenkombination einem Begriff in der Online-Hilfe, so wird das entsprechende Kommando angezeigt. Ist die Buchstabenkombination nicht in der Hilfe vorhanden, wird die Hilfe in der vollen Übersicht geöffnet.

– Geben Sie den Anfangsbuchstaben einer Funktion oder eines Befehls ein und drücken Sie die Tasten [Strg] + [Leertaste], so erhalten Sie eine Liste aller Befehle und Funktionen, die mit diesem Buchstaben beginnen.

– Schreiben Sie eine Regel korrekt in das Konfigurationsfenster, so werden alle Befehle, die das System kennt, entsprechend eingefärbt dargestellt:

blau = Konstanten

rot = Texte

**fett = Funktionen**

braun = (feste) Werte

Als Variable können alle Begriffe verwendet werden, die nicht als Schlüsselworte für Funktions-und Konstantennamen verwendet werden. (Ein zulässiger Begriff für eine Variable ist daran erkennbar, dass sich seine Farbe und sein Textformat nach dem Eintrag im Konfigurationsfenster nicht ändert.)

– In der Online-Hilfe sind eine Reihe von Beispielen vorrätig, die einfach übernommen und gegebenenfalls ergänzt oder mit den vordefinierten Konstanten oder Funktionen modifiziert werden können.

## Interne Variablen zur Regel-Prüfung

Nach Übertragung der Sicherheits-Richtlinie an den Client, ist eine darin enthaltene Regel unmittelbar ab diesem Zeitpunkt wirksam, d. h. sie wird zu diesem Zeitpunkt zum ersten Mal geprüft. Die Zeitspanne des Prüf-Intervalls (CHECK_INTERVAL) wie auch die des Intervalls bis zum nächsten Herunterladen (RELOAD_INTERVAL) einer Richtlinie wird ab der ersten Prüfung gemessen. (Beide Werte werden durch die Policy vorgegeben.)

Allgemein gilt, dass bei Nichterfüllung einer Regel die Reaktion erfolgt, die innerhalb der Regel zwischen den Operatoren “if” und “endif” angegeben wird, normalerweise ein Verbindungsabbau.

### CHECK_INTERVAL

Zeitintervall in Sekunden in dem die Überprüfungen durchgeführt werden sollen. Standard = 10 s. Ist ‘0’ angegeben, wird die Überprüfung nicht zyklisch wiederholt. Die Widerholung der Prüfung stellt sicher, dass Veränderungen am Benutzer-PC auch während der Online-Zeit/Verbindung wahrgenommen werden können.

### RELOAD_INTERVAL

Zeitintervall in Sekunden in dem die Policy vom Server erneut heruntergeladen wird. Dieser Parameter darf nicht kleiner als Check-Intervall gewählt werden. Ausnahme ist die Standardeinstellung ‘0’, die besagt, dass die Richtlinie nicht zyklisch heruntergeladen wird.

Jede wiederholt heruntergeladene Policy wird als neue Policy geprüft, die zum ersten Mal heruntergeladen wurde, sodass das Check-Intervall neu angezählt wird.

Das Reload-Intervall sollte größer sein als das Replikations-Intervall am Secure Server. (Vergleichen Sie dazu das “Replikations-Intervall”, das am Secure Server eingestellt werden kann, womit das Zeitintervall für das Herunterladen der Richtlinien vom Management Server definiert wird. Siehe auch weiter unten “Download der Policies”.)

### ISFIRSTCHECK

Flag, das nur bei der ersten Überprüfung nach einem neuen Verbindungsaufbau TRUE ist. Bei weiteren Überprüfungen ist dieses Flag FALSE.

### WAS_ACCEPTED

TRUE, wenn in der vorherigen Überprüfung während derselben Verbindung ‘ExitAccept’ aufgegeben wurde.

### FILTERGROUPNAME

Name der Filtergruppe, die nach dem Accept verwendet werden soll. Ist diese Variable nicht zugewiesen, wird die konfigurierte Filtergruppe aus dem Link-Profil verwendet.

### SECURITY_LEVEL

Der Wert dieser Variable bestimmt, ob eine Konfiguration in SSL/VPN verwendet werden soll. In der SSL/VPN-Konfiguration kann sowohl in den WEB Proxy-Anwendungen als auch bei den Port Forwarding-Einstellungen der Security Level angegeben werden, ab dem die Anwendung dem Benutzer zur Verfügung gestellt werden soll. Beachten Sie zur Funktionsweise des Security Levels den Abschnitt weiter unten “Endpoint Security mit SSL/VPN-Benutzern”, sowie das Handbuch zum SSL/VPN Server.

### SSLVPN_DELCLNTAFTERDISCONN

Wird diese Variable auf TRUE gesetzt, wird nach dem SSL/VPN Verbindungsabbau der SSL/VPN Client gelöscht.

### SSLVPN_DELAPPLSAFTERDISCONN

Wird diese Variable auf TRUE gesetzt, werden nach dem SSL/VPN Verbindungsabbau die heruntergeladenen Applikationen gelöscht.

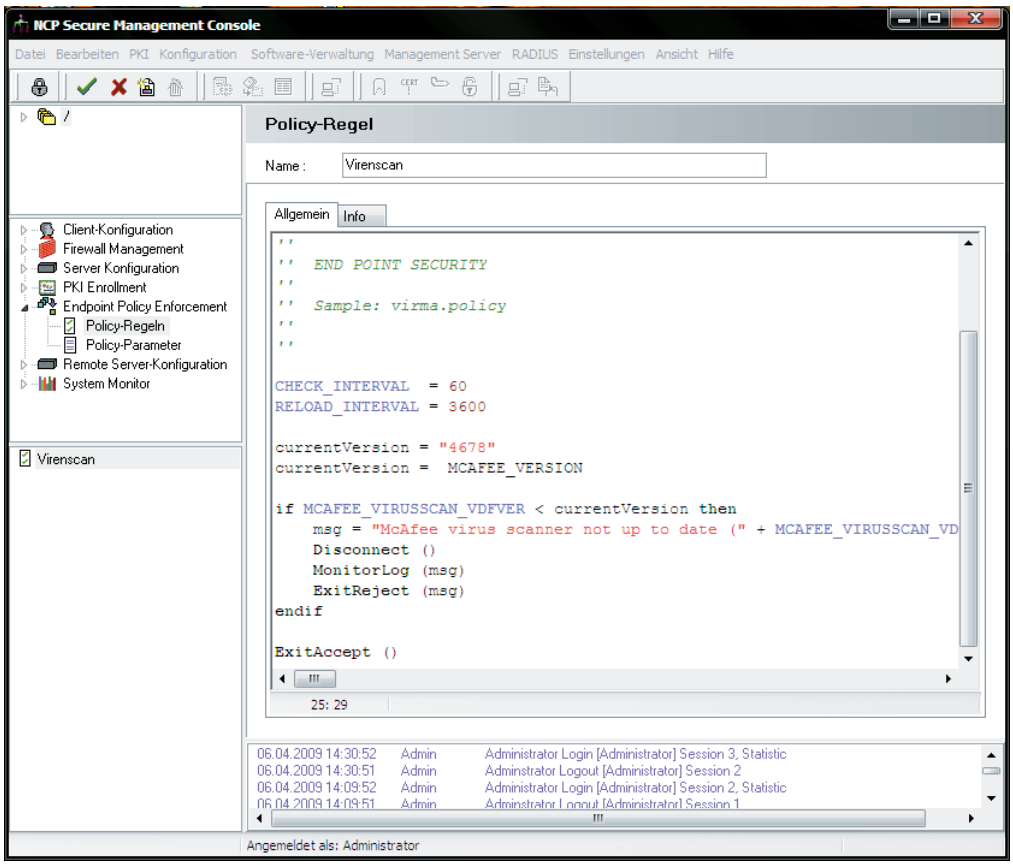
## Operatoren

| Operator | Beschreibung |
|---|---|
| NOT | Negierung des Ergebnisses |
| OR | logische Oder-Verknüpfung |
| AND | logische Und-Verknüpfung |
| = | ist gleich |
| <> | ist ungleich |
| > | ist größer |
| >= | ist größer oder gleich |
| < | ist kleiner |
| <= | ist kleiner oder gleich |

## Anpassen der Regeln

Das Konfigurationsfenster der Policy wird geöffnet, indem die Policy im Vorlagen-Bereich selektiert wird. Unter “Allgemein” werden die Regeln der Richtlinie angegeben bzw. bereits vorhandene angepasst. (Hier in der Abbildung wurde die Regel “Sample: virma.policy” kopiert.)

Die Regel muss nun so editiert werden, dass entweder die aktuelle Version (currentVersion =) als fester Wert in Anführungszeichen als Zahl z. B. “4678" angegeben wird, oder als Variable eines Parameters.




Je nachdem, ob die Version des Viren-Scanners am Client mit dem festen Wert oder mit dem dynamisch eingelesenen Wert des Parameters MCAFEE_VERSION verglichen werden soll, muss die eine oder andere Zeile der “currentVersion” gelöscht werden.

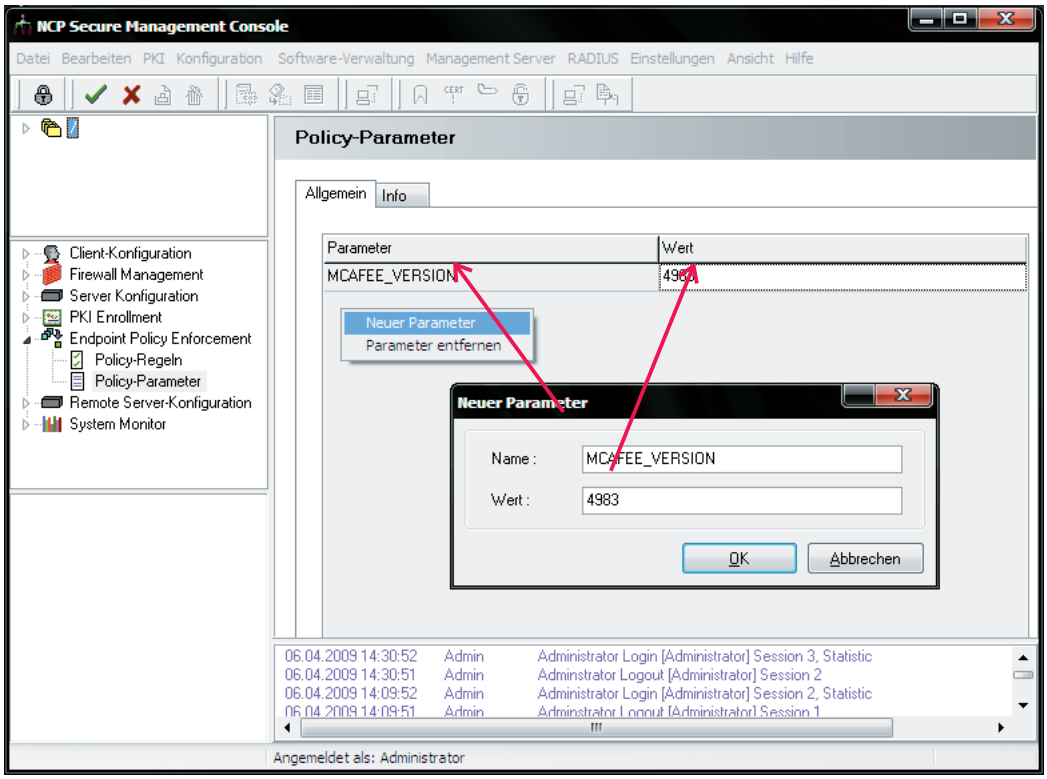
```
''
''  _   _ ____ ____
''  | \ | |/ ___|  _ \
''  |  \| | |   | |_) |
''  | |\  | |___|  __/
''  |_| \_|\____|_|    engineering GmbH
''
''  END POINT SECURITY
''
''  Sample: virma.policy
''

CHECK_INTERVAL  = 60
RELOAD_INTERVAL = 3600

currentVersion =  MCAFEE_VERSION

if MCAFEE_VIRUSSCAN_VDFVER < currentVersion then
    msg = "McAfee virus scanner not up to date ("+ MCAFEE_VIRUSSCAN_VDFVER +")"
    Disconnect ()
    MonitorLog (msg)
    ExitReject (msg)
endif

ExitAccept ()
```

Soll statt eines festen Werts der Wert der Variablen eingelesen werden, so muss die Regel zum Beispiel wie in unten stehender Abbildung aussehen. In diesem Beispiel wird geprüft, ob die Virendefinitionsdatei des McAfee Virus-Sanners mindestens die eingelesene aktuelle Version “currentVersion” hat.

Werden selbstdefinierte Parameter statt fester Werte in einer Regel verwendet, so können über ein Script die Werte in vorgegebenen Zyklen automatisch aktualisiert werden. Dazu muss jedoch zunächst der Parameter als solcher für die Endpoint Policy definiert werden.

## Selbstdefinierte Parameter

Um einen neuen Parameter einzuführen, öffnen Sie im Plug-in-Bereich den Konfigurationsknoten “Endpoint Policy Enforcement” und klicken die “Policy-Parameter” an.




Im Konfigurationsbereich können Sie nach Klick auf die rechte Maustaste “Neuer Parameter” selektieren und “Name” sowie “Wert” dieses Parameters eintragen. Der Name kann beliebig sein, muss aber sein identisch mit dem Parameter-Namen, der in der “currentVersion”-Zeile der Regel eingetragen ist, in der Abbildung hier: MCAFEE_VERSION (siehe vorige Seite).

Als Variable können alle Begriffe verwendet werden, die nicht als Schlüsselworte für Funktions-und Konstantennamen verwendet werden. (Ein zulässiger Begriff für eine Variable ist daran erkennbar, dass sich seine Farbe und sein Textformat nach dem Eintrag im Konfigurationsfenster nicht ändert.) Der Wert ist lediglich Startwert, sofern er durch die nächste Aktualisierung mittels Script überschrieben wird.

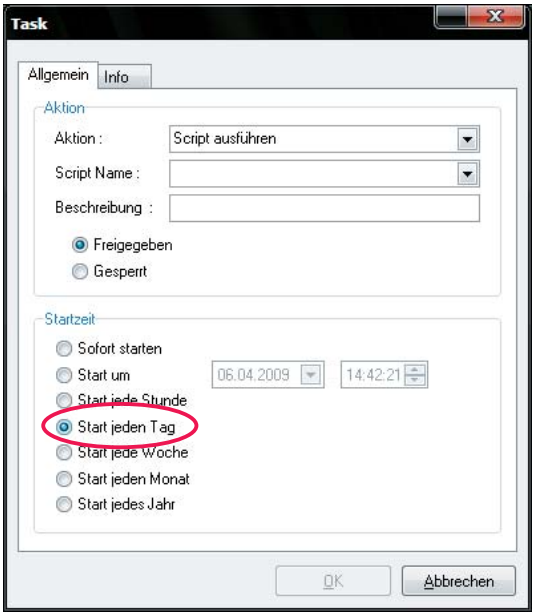
Mit der in diesem Beispiel eingesetzten Regel soll geprüft werden, ob der Client über die jeweils aktuellste Viren-Definitionsdatei verfügt, um eine Viren-Übertragung ausschließen zu können.

Dazu wurde zunächst eine Regel erstellt, mit der die “currentVersion” des McAfee Viren-Scanners am Client überprüft wird. Da sich die Version ständig erneuert, wurde, statt einen festen Versions-Wert einzusetzen, der Parameter “MCAFEE_VERSION” definiert, dessen Variable nach Ausführen eines Scripts durch den Wert für die jeweils aktuellste Version ersetzt wird.

## Beispiel-Script

Im folgenden muss ein Script erstellt werden, worüber z. B. die Viren-Definitionsdatei von einem FTP-Server heruntergeladen werden kann und der Wert für den Parameter MCAFEE_VERSION in die Regel am Management Server eingesetzt werden kann. Das Script muss am Rechner des Management Servers verfügbar sein und über die Management Console ausgeführt werden können. Es könnte wie folgt beschaffen sein:

```
'------------------------------------------------------------------------
' Informationen der Viren-Definitionsdatei werden über FTP heruntergeladen
' und der Wert für den Parameter MCAFEE_VERSION des Management Servers
' wird neu gesetzt.
'------------------------------------------------------------------------

const MGMSRV_HOST           = "181.10.13.10"
const MGMSRV_ADMIN          = "Administrator"
const MGMSRV_PASSWORD       = "passwort"
const MGMSRV_GROUPNAME  = "/Firma1.de"

    const FTPHOST               = "ftp.nai.com"
    const FTPPATH               = "/pub/antivirus/datfiles/4.x"
    const FTPFILE               = "update.ini"

sess = new CRsuSession
if sess.Connect (MGMSRV_HOST, MGMSRV_ADMIN, MGMSRV_PASSWORD) = 0 then
            print "Connect failed "; sess.GetErrorStr
            Halt (1)
    endif

print "SEM Connect ok"
    grp = sess.GetGroupByName (MGMSRV_GROUPNAME)
    if grp = 0 then
        print "Group not found"
        Halt (1)
    end if

    ftp  = new CFtpClient
    if ftp.Connect (FTPHOST) = false then
            print "Connect failed"
            Halt(0)
    end if
    print "FTP Connect ok"

    if ftp.Login ("Anonymous", " ") = false then
            print "Login failed"
            Halt(0)
    end if
    print "FTP Login ok"

    if ftp.ChDir (FTPPATH) = false then
            print "ChDir failed"
            Halt(0)
    end if
    print "FTP ChDir ok"

    if ftp.Get (FTPFILE, FTPFILE) = false then
            print "Get failed"
            Halt(0)
    end if
    print "FTP Get ok"

    version = IniFileGetValue (FTPFILE, "SuperDat-IA32", "DATVersion")

    print "New Version : " ; version

param = grp.GetPolicyParam ()
if param then
   oldVersion = param.GetValue ("MCAFEE_VERSION")
   print "MGM Version : " ; oldVersion
   if oldVersion <> version then

      param.SetValue ("MCAFEE_VERSION", version)
      grp.UpdatePolicyParam (param)

      msg = "McAfee Versions Update -> " + version
      grp.log (msg)
      print (msg)

   end if
end if
```



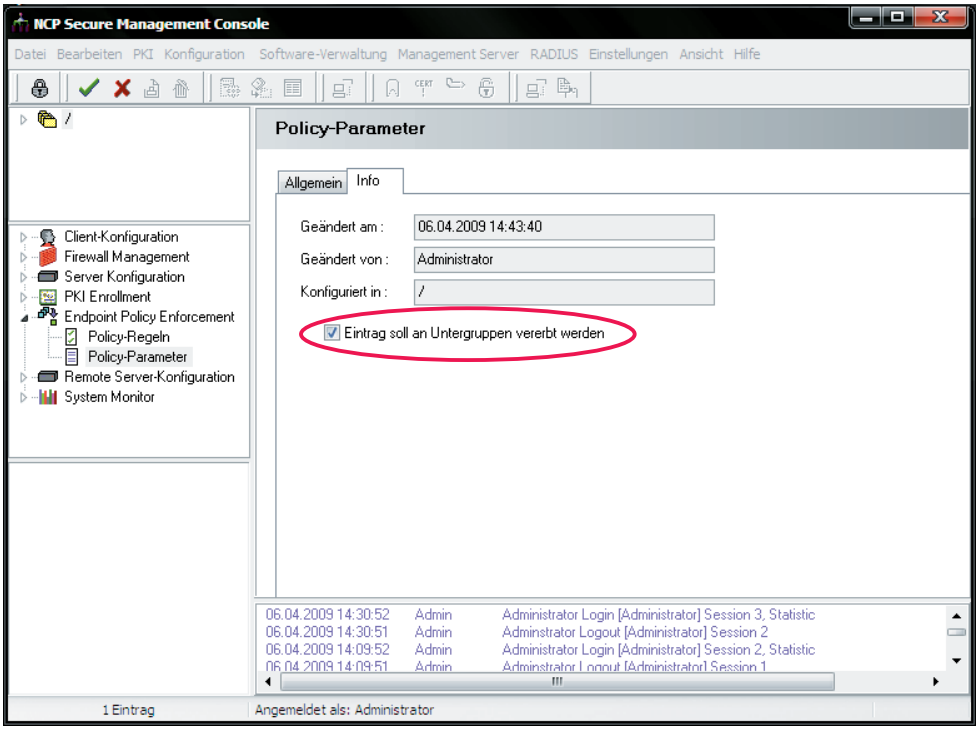

Das Script muss am Rechner des Management Servers verfügbar sein und über die Management Console aufgerufen werden. Über das Task-Fenster unter dem Menüpunkt “Management Server / Tasks” der Management Console können Sie außerdem den Zyklus der Aktualisierung bestimmen.

In nebenstehender Abbildung wird “jeden Tag” die aktuellste Version des Viren-Scanners abgefragt.

# Abschließen und Speichern einer Policy

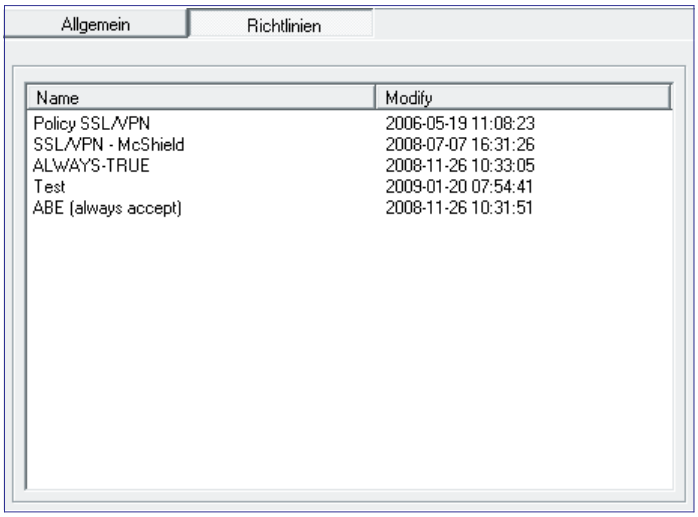
Bitte beachten Sie, dass eine Policy nur mit einem “ExitAccept” abgeschlossen ist, das nach Erfüllung der Richtlinie an den Secure Server geschickt wird, der daraufhin den Netzzugang für den Client freischaltet.

Eine Policy muss erst vom Management System übernommen worden sein, damit sie eingesetzt werden kann. Wählen Sie dazu, nachdem die Policy abgefasst wurde, im Hauptmenü “Bearbeiten / Übernehmen” oder betätigen Sie den Button mit dem grünen Haken in der Werkzeugleiste der Management Console.




Zunächst müssen die Richtlinien zu einem Policy Server (Bestandteil des Secure Servers) übertragen werden, d. h. der Policy Server muss vom Enterprise Management angesprochen werden können.

Im Info-Fenster des Konfigurations-Bereichs der Policy-Regeln kann die Policy auch an Untergruppen weitervererbt werden.

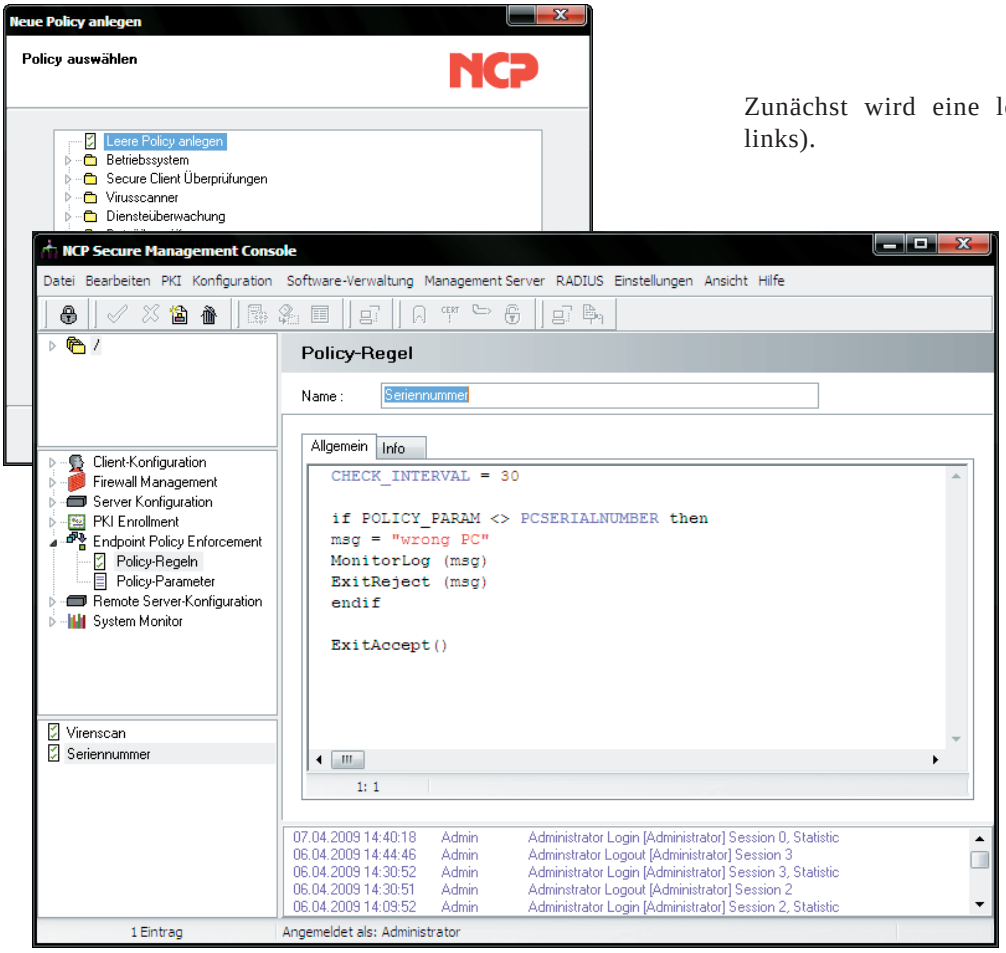



Wenn Sie die erstellte und bearbeitete Richtlinie abspeichern und im Anschluss daran in der Konfiguration des Secure Servers unter “Endpoint Policy Enforcement / Policy Rules” nachsehen, so finden Sie dort einen Eintrag zu der gerade erstellten Richtlinie. (Beachten Sie dazu oben den Abschnitt **Konfiguration der Secure Server**.)

Die heruntergeladenen Richtlinien werden im benachbarten Fenster namentlich und mit einem Zeitstempel versehen aufgeführt.

# Richtlinien mit einem benutzerspezifischen Policy-Parameter

Policy-Parameter werden am Management Server für eine komplette Organisationsgruppe konfiguriert. Soll nun z. B. der benutzerspezifische Wert der PC-Seriennummer eines jeden Benutzers überprüft werden, so kann die PC-Seriennummer allgemein als “POLICY_PARAM1" definiert werden.




Zunächst wird eine leere Policy geöffnet (Abb. links).

Um die Richtlinie zum Abprüfen der Seriennummer zu erstellen, wird der POLICY_PARAM1 über einen Operator-Vergleich auf Ungleichheit (<>) mit der vordefinierten Konstanten PCSERIALNUMBER verknüpft:

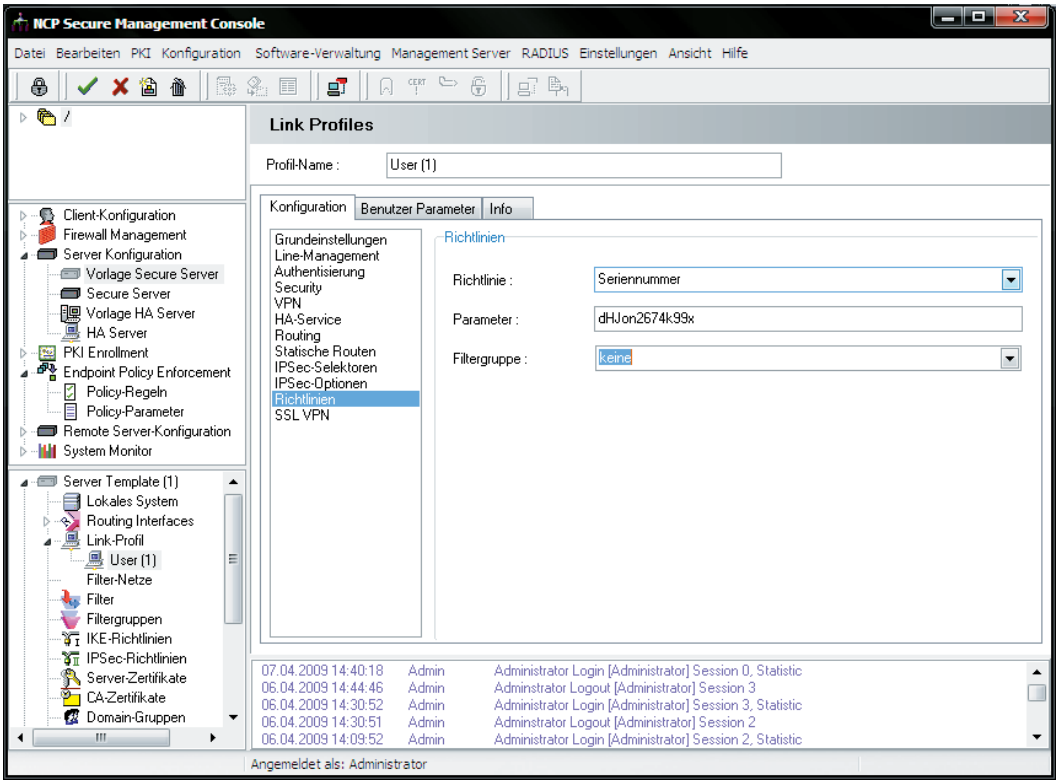
```
if POLICY_PARAM1 <> PCSERIALNUMBER then
```

PCSERIALNUMBER ist eine der vordefinierten Konstanten, die sich in der Online-Hilfe zur Endpoint Policy Enforcement finden: Seriennummer des Rechners (nur unter Windows verfügbar) PokketPC Device ID bei PocketPC bzw. Windows Mobile.

POLICY_PARAM1 ist in der Online-Hilfe ebenfalls unter den vordefinieren Konstanten zu finden. Sofern eine Regel diese Konstante enthält, beschreibt sie den 1. Parameter der Benutzer-Konfiguration, der vom Secure Server aus der Policy gelesen wird. Den Wert zu dieser Konstanten fragt der Secure Server zunächst aus der lokalen Link-Konfiguration ab. Ist der Wert hier nicht eingetragen, wird er über die definierte Schnittstelle abgefragt, z. B. Radius (siehe weiter unten).

# Einsatz der Richtlinien am Secure Server

Über den Server Manager oder die Management Conole können die Policies am Secure Server für den Secure Client wirksam geschaltet werden. Dazu wird im Server Manager das Parameterfeld “Client Richtlinien” im Konfigurationszweig “Link-Profile” geöffnet. Dort wählt der Administrator eine der Richtlinien des Policy Servers nach ihrem Namen aus (Policy Name). Wird keine Policy ausgewählt, so ist das Endpoint Policy Enforcement nicht wirksam.




Beachten Sie dazu, dass je nach Regelinhalt der Richtlinie gegebenenfalls der Wert eines Policy-Parameters abgefragt wird, wie im obigen Beispiel.

In der Abbildung oben wurde die Policy “Seriennummer” gewählt, die eine Regel zur Seriennummer des Benutzers enthält.

Wird eine Policy ausgewählt, die eine Regel mit einer vordefinierten Konstanten beinhaltet, die auf einen jeweils benutzerspezifischen Wert verweist, wie z. B. die Seriennummer des Benutzer-PCs, so muss der generalisierte Policy-Parameter, in diesem Fall PCSERIALNUMBER, für dieses Link-Profil personalisiert werden.

Im Konfigurationsfeld des Server Managers (Link-Profile / Client Policy) muss in das Feld “Policy Parameter” für diese vordefinierte Konstante PCSERIALNUMBER ein realer Wert eingetragen werden. Im Beispiel obiger Abbildung wurde die Konstante für diesen Link personalisiert, indem die Seriennummer des Client PCs eingetragen wurde.

# Personalisierte Richtlinien über RADIUS-Konfiguration

Wurde ein RADIUS Server in der Systemumgebung definiert, so erhält der Secure Server (Policy Server) von ihm die Link-Konfiguration einschließlich der Sicherheits-Richtlinien, deren Regeln samt personalisierter Parameter.

Im Management-System müssen für die benutzerspezifische Zuordnung der Richtlinie folgende Einstellungen vorgenommen werden:

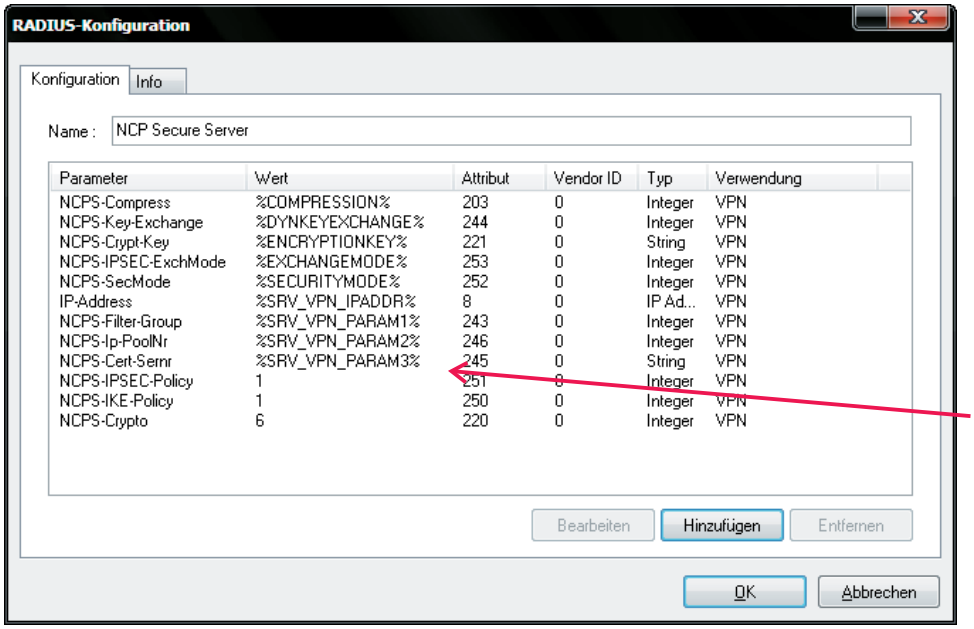
Zunächst wird die Richtlinie “Seriennummer”, wie oben beschrieben, mit einem benutzerspezifischen Policy-Parameter erstellt:

```
if POLICY_PARAM1 <> PCSERIALNUMBER then
msg = "Wrong PC"
MonitorLog (msg)
ExitReject (msg)
endif
ExitAccept ()
```

An den RADIUS Server muss der Name der Policy und die Bezeichnung für den Policy-Parameter übergeben werden. Um dies zu bewerkstelligen, müssen die entsprechenden Attribute aus dem RADIUS Dictionary (servdict.txt) in die RADIUS-Konfiguration am Management-System übernommen werden. (Vergleichen Sie dazu in diesem Handbuch auch den Abschnitt 14.3.2 Beispiele für Parameterwerte und Platzhalter in der RADIUS-Konfiguration.)

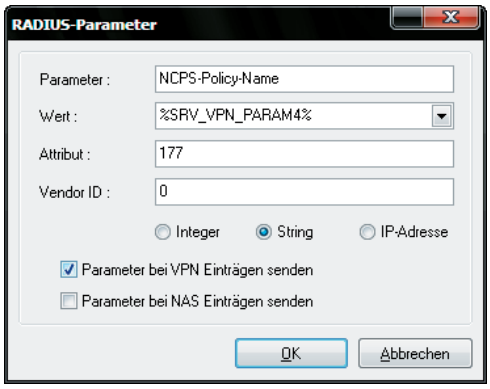
Die entsprechenden Attribute aus dem RADIUS Dictionary lauten:

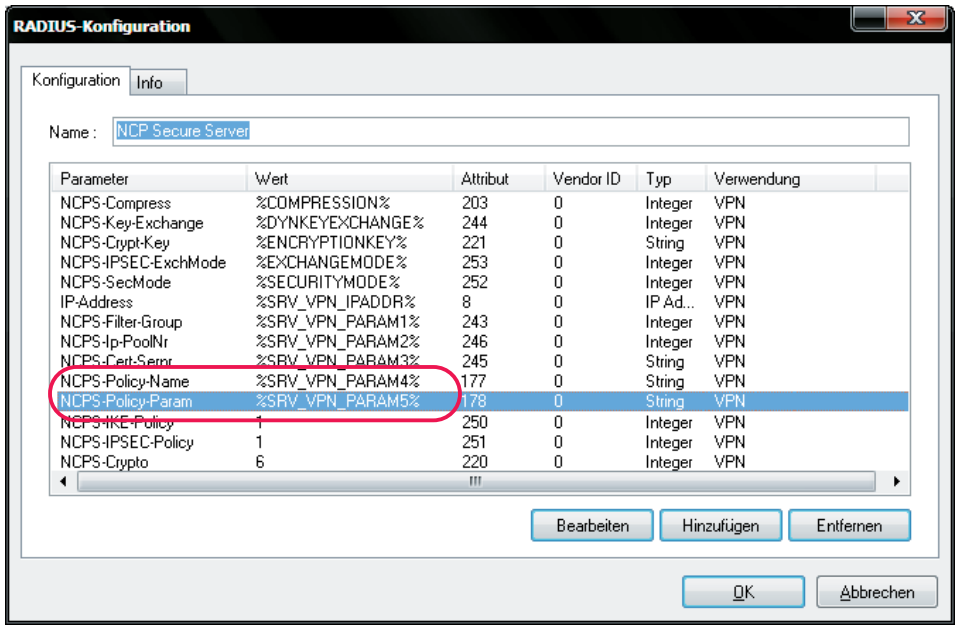
```
ATTRIBUTE NCPS-Policy-Name 177 string
ATTRIBUTE NCPS-Policy-Param 178 string
```




Über die Management Console öffnen Sie die RADIUS-Konfiguration und prüfen, welche Server-Parameter für die Link-Konfiguration noch zur Verfügung stehen. Im obigen Beispiel sind dies %SVR_VPN_PARAM4% und %SVR_VPN_PARAM5%.

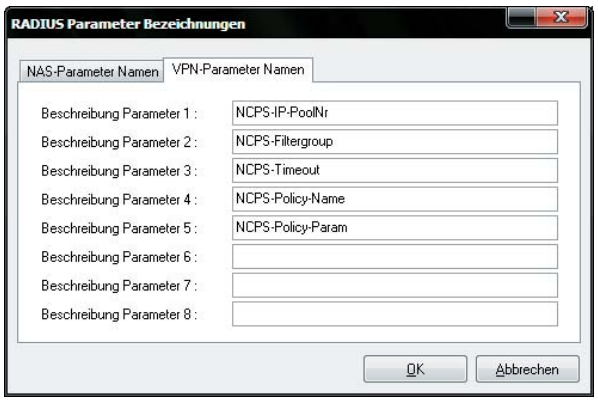
Anschließend werden die neuen Parameter gemäß der Attributliste des RADIUS Dictionarys der RADIUS-Konfiguration hinzugefügt. (Abb. unten)




Wenn die Attribute aus dem RADIUS Dictionary in der RADIUS-Konfiguration vorhanden sind (siehe Abbildung oben), ist die Konfiguration fertiggestellt und kann mit “OK” geschlossen werden.

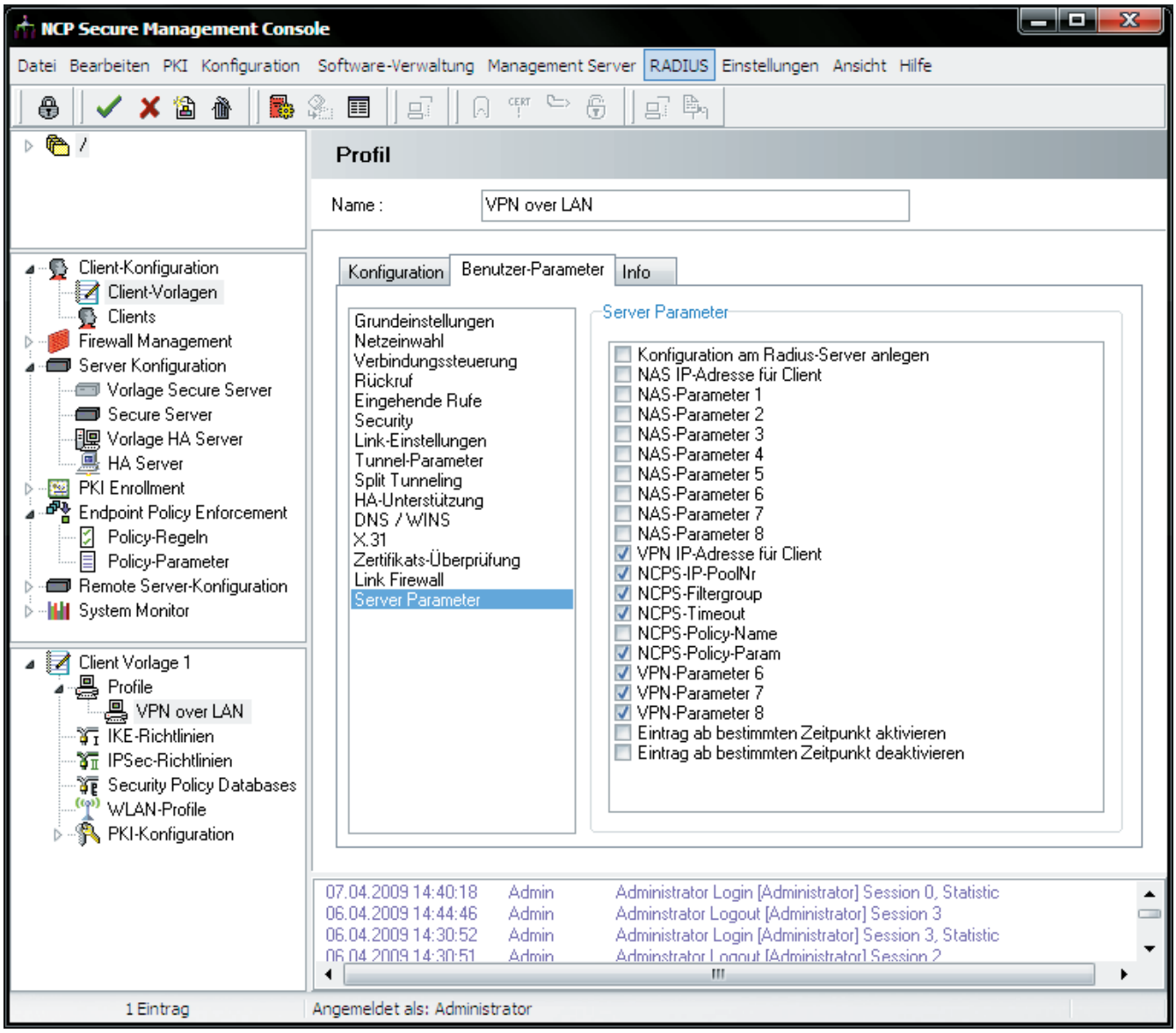
Anschließend müssen die Parameter der RADIUS-Konfiguration als zusätzliche Parameter an die Vorlage für die Client-Konfiguration übergeben werden. Dazu erhalten die RADIUS-Parameter Bezeichnungen, unter denen sie als zusätzliche Konfigurations-Parameter in der Vorlage erscheinen.



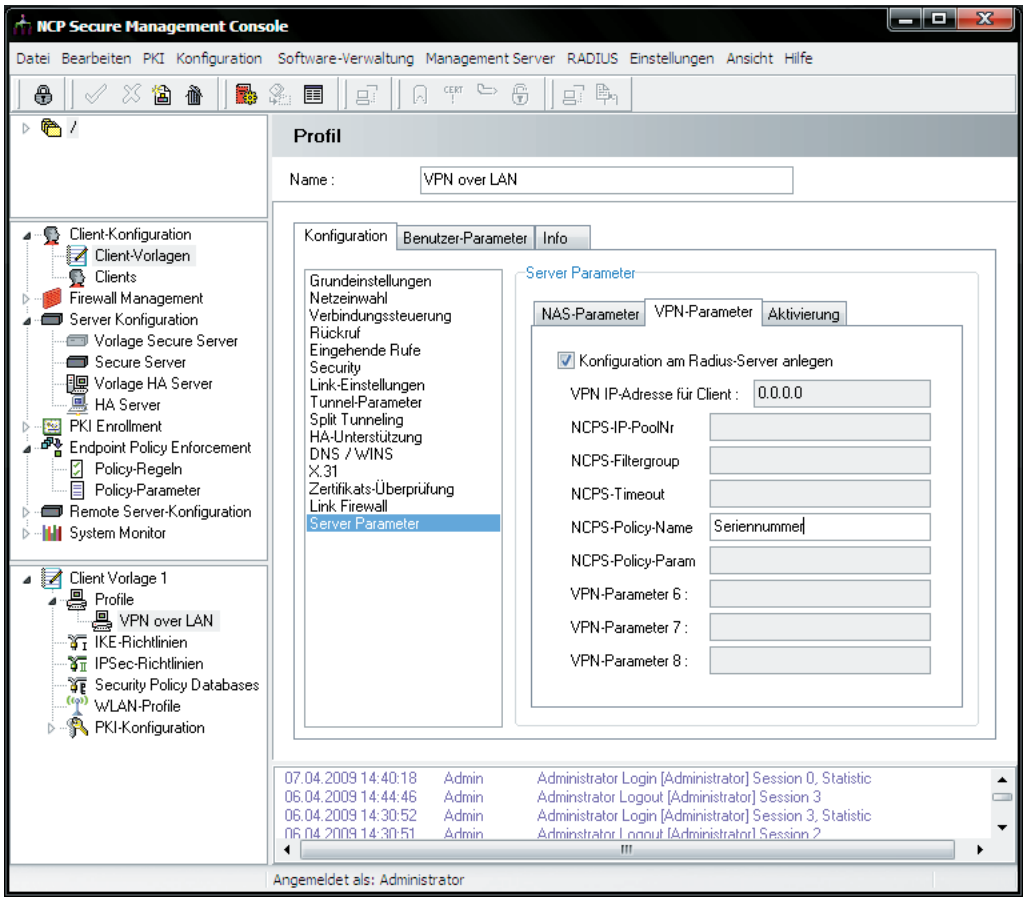

Dazu wird im RADIUS-Menü der Console das Feld “RADIUS Parameter-Bezeichnungen ” geöffnet und eine Bezeichnung eingetragen. Dabei empfiehlt sich, als Beschreibung die gleiche Bezeichnung zu verwenden, unter der der Parameter in der RADIUS-Konfiguration geführt wird, um eine eindeutige Zuordnung sicher zu stellen. Demnach entspricht in diesem Beispiel:

```
NCPS-Policy-Name: %SVR_VPN_PARAM4%: Beschreibung Parameter 4
NCPS-Policy-Param: %SVR_VPN_PARAM5%: Beschreibung Parameter 5
```

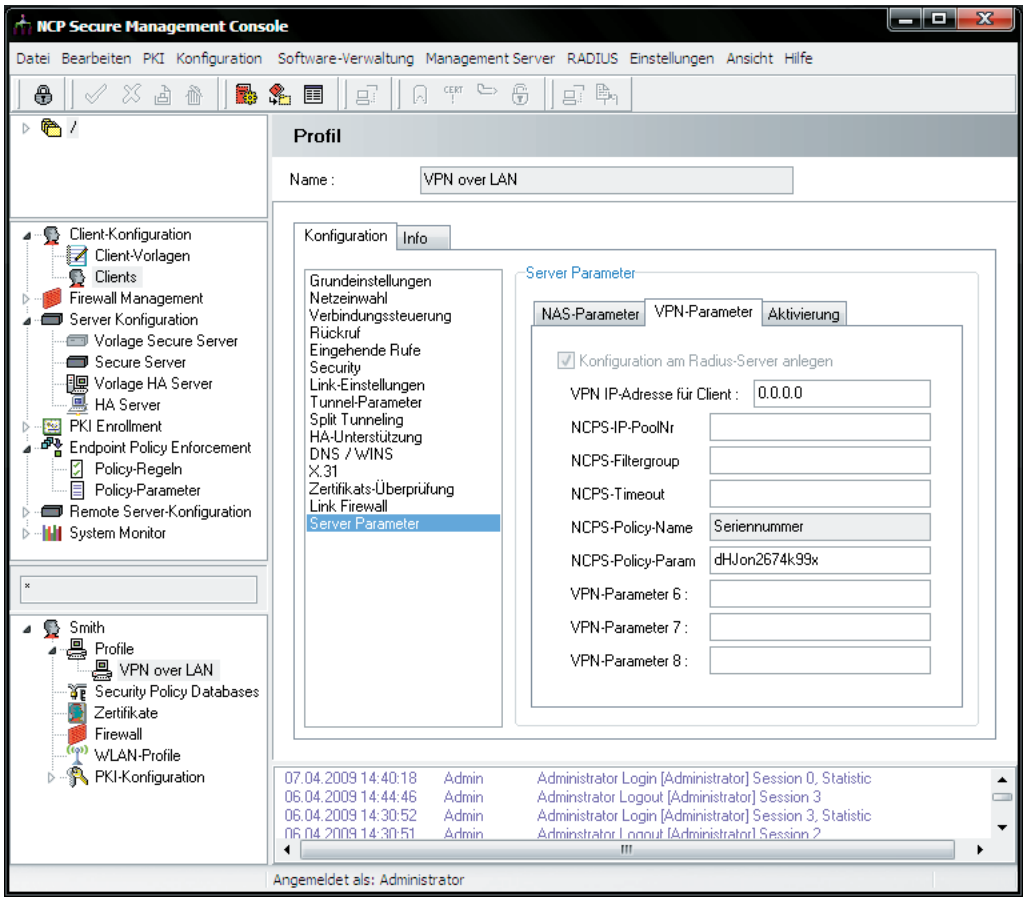
Anschließend wird die Vorlage geöffnet und unter “Benutzer-Parameter” festgelegt welche der neuen Server-Parameter für die Benutzer der gruppenspezifischen Vorlage gleich sein sollen (hier: NCPS-Policy-Name) und welche client-spezifisch in der Benutzer-Konfiguration eingegeben werden müssen (hier: NCPS-Policy-Param). (Abb. unten)




**Weiter auf der nächsten Seite**




Entsprechend muss im Konfigurationsfeld die genaue Bezeichnung der Richtlinie eingegeben werden (im obigen Beispiel “Seriennummer”).



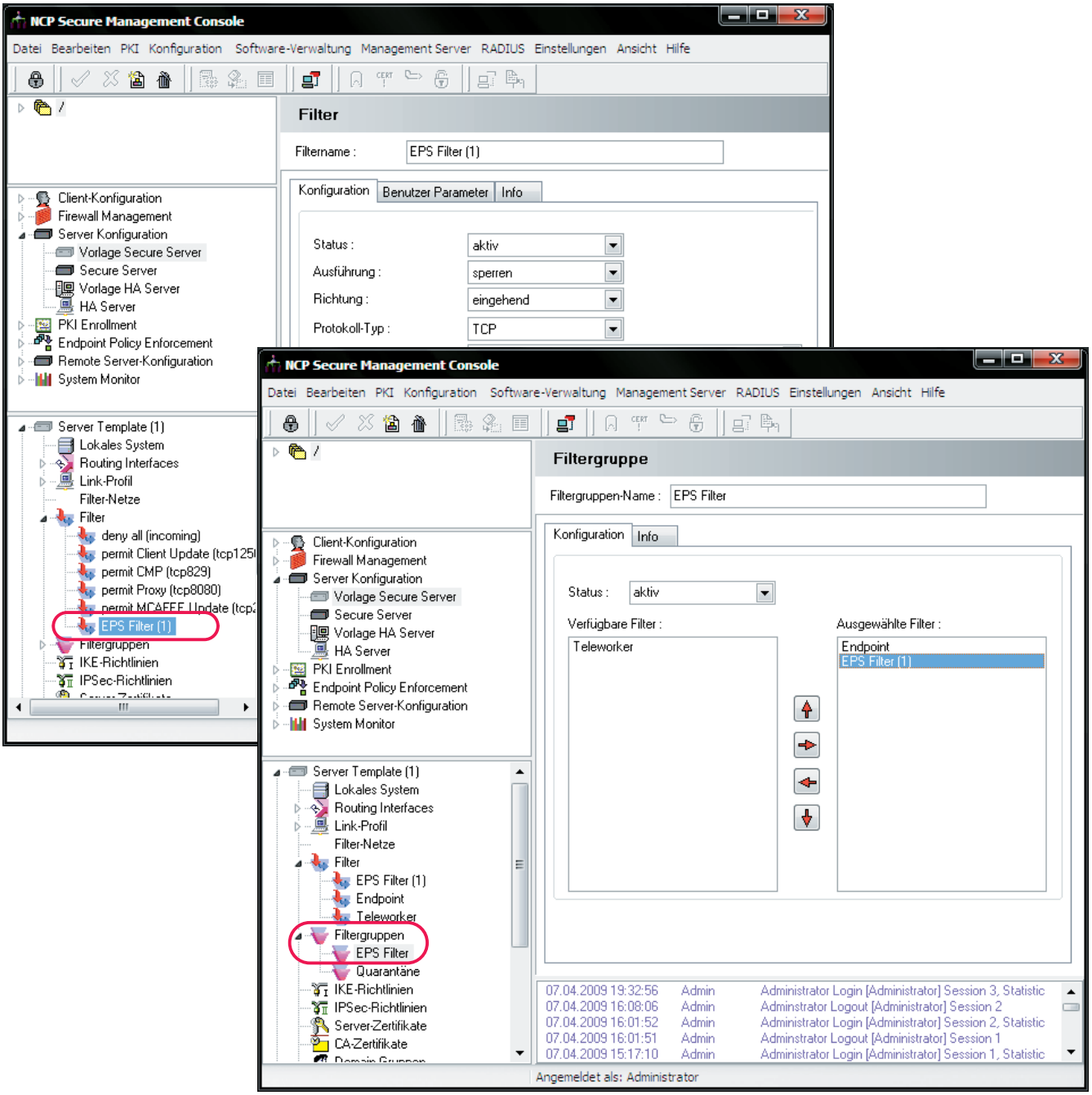

Die Personalisierung der Richtlinienregel erfolgt anschließend in der Benutzer-Konfiguration, indem die Seriennummer des PCs eingetragen wird.

Wird das Link-Profil am Secure Server inaktiv gestellt, und ist ein RADIUS Server konfiguriert und aktiv, so schickt der Server beim Verbindungsaufbau eines Remote-Systems einen RADIUS Request und erhält vom RADIUS Server die Benutzer-Konfiguration, einschließlich der Sicherheits-Richtlinien und personalisierten Parameter, die dort vom Management Server abgelegt wurde.

Das Link-Profil wird über den Server Manager unter “Link-Profile / Grundeinstellungen” inaktiv geschaltet. Eine lokale Konfiguration wie unter **Einsatz der Richtlinien am Secure Server** beschrieben, ist dann überflüssig.

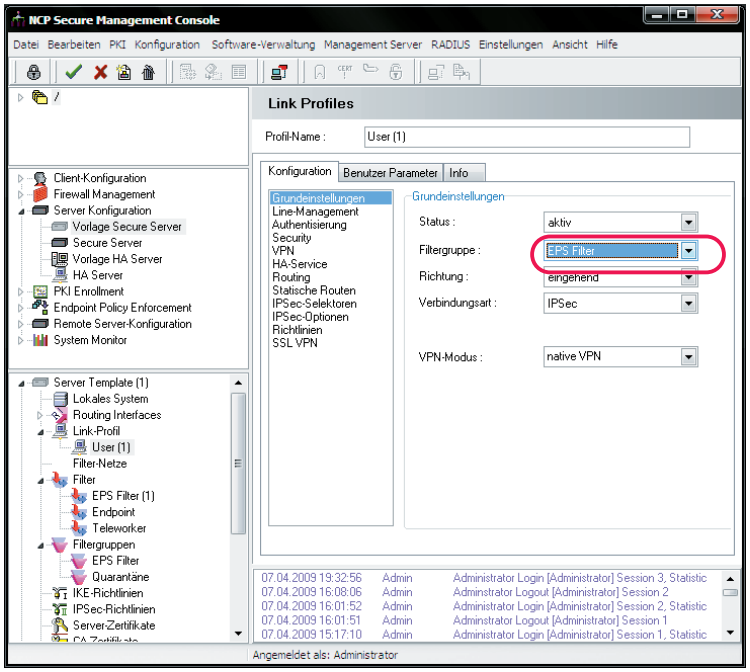
## Nichterfüllung einer Richtlinie

Bei Nichterfüllung der Regelvorgaben einer Richtlinie können unterschiedliche Meldungen oder Aktionen erfolgen. Z. B. kann dem Client der Zugang zum Firmennetz völlig verwehrt werden, oder der Zugriff auf einen bestimmten Bereich eingeschränkt werden, sodass es einem Client mit falscher Versionsnummer nur möglich ist, ein Update herunterzuladen, um anschließend mit der richtigen Software-Version Zugriff auf seinen kompletten Netzbereich zu erhalten.



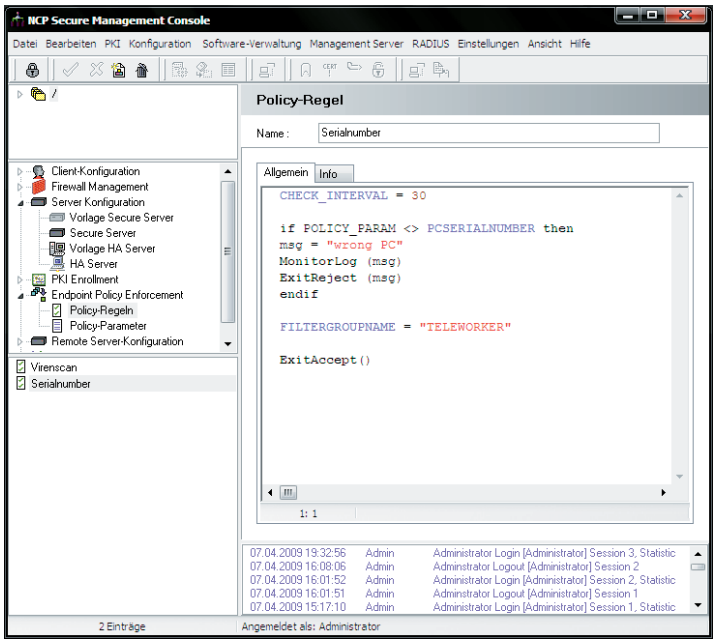

Diese Steuerung des potenziellen Netzwerkzugriffs wird über Filter und Filtergruppen bewerkstelligt, die am Secure Server definiert wurden. (Siehe obige Abbildungen.)

Die Zuordnung der Filtergruppe erfolgt mit der Konfiguration des Link-Profils unter “Link-Profile / Grundeinstellungen” und unter “Link-Profile / Client Policy”. Dabei werden für Erfüllung und Nichterfüllung der Richtlinie unterschiedliche Filtergruppen genutzt.




**1. Die Filtergruppe, die im Konfigurationszweig “Link-Profile / Grundeinstellungen”** (Bild oben) selektiert wurde, ist dann wirksam, wenn kein Endpoint Policy Enforcement eingesetzt wird, d. h. wenn keine Policy wie oben beschrieben selektiert wurde, und sie ist auch wirksam, wenn die Policy vom Client erfüllt wurde. Somit wird über diese Filtergruppe für eingehende Links der jeweils **maximale Netzbereich** definiert.

**2. Die Filtergruppe, die im Konfigurationszweig “Link-Profile / Client Policy”** (Bild oben) selektiert wurde, ist immer wirksam ab dem VPN-Verbindungsaufbau von Client zu Server solange die Policy-Prüfung durchgeführt wird und darüber hinaus, wenn die Policy nicht erfüllt wird. Somit wird über diese Filtergruppe **der jeweils kleinste Netzbereich** definiert oder der Zugriff verweigert.




**3.** Sollen aufgrund unterschiedlicher Charakteristiken der Richtlinien auch unterschiedliche **Filtergruppen pro Policy** verwendet werden, so kann die Filtergruppe auch mit der Richtlinie übergeben werden (Bild oben). In diesem Fall wird die im Link-Profil konfigurierte Filtergruppe ignoriert und die in der Policy angegebene für den Netzzugang verwendet. Diese Filtergruppe muss gleichwohl am Secure Server unter “Filtergruppen” angelegt worden sein.

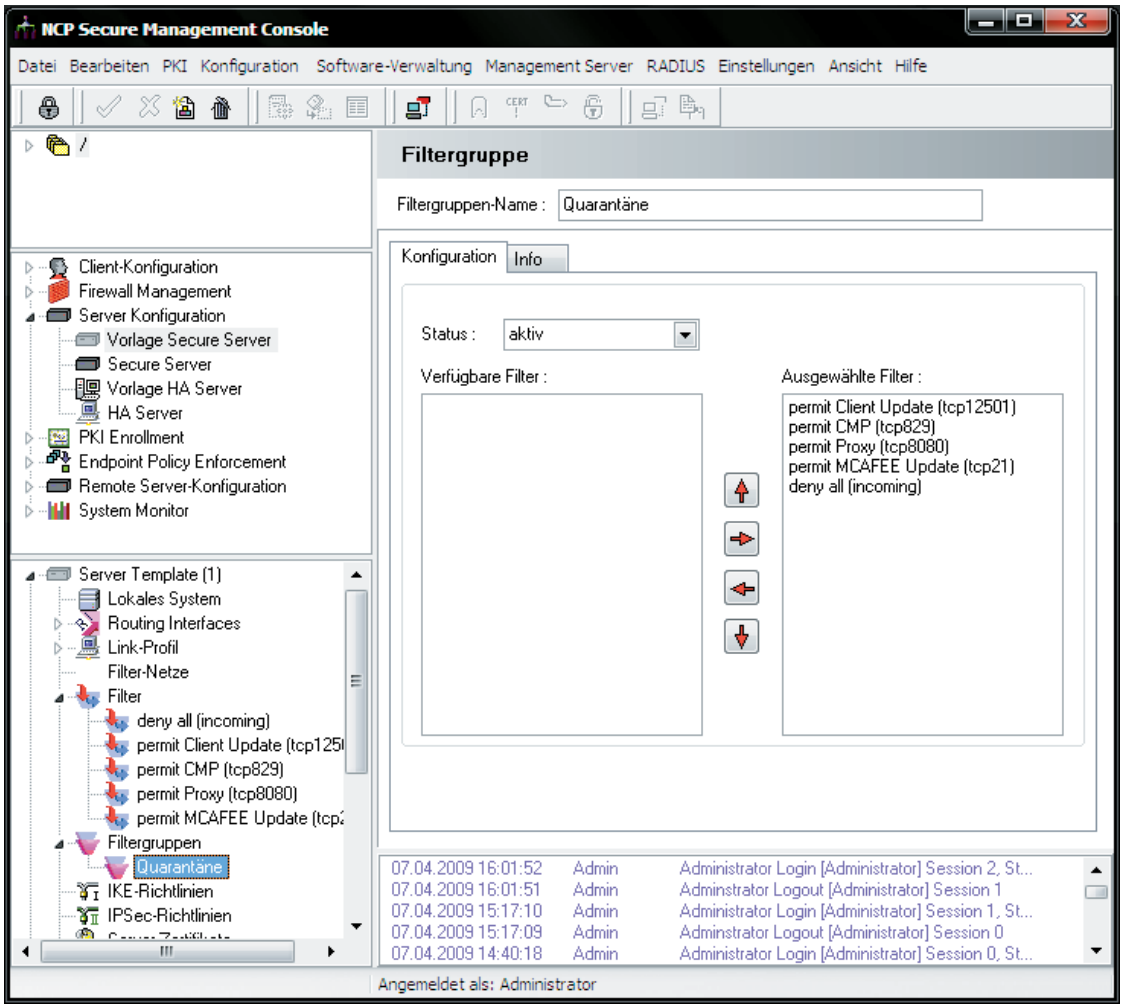
# Einrichten einer Quarantäne Zone

Um dem Benutzer während der Überprüfung der Policy und bei Nichterfüllung der Policy keinen produktiven Zugriff auf das Netzwerk zu ermöglichen ist der NCP Secure Server in der Lage, den Client in einer “Quarantäne-Zone” zu halten. Um die Quarantäne-Zone korrekt definieren zu können, müssen zunächst die erlaubten Zugriffe bestimmt werden. So soll der Client z.B. eine Verbindung zu folgenden Diensten herstellen dürfen:

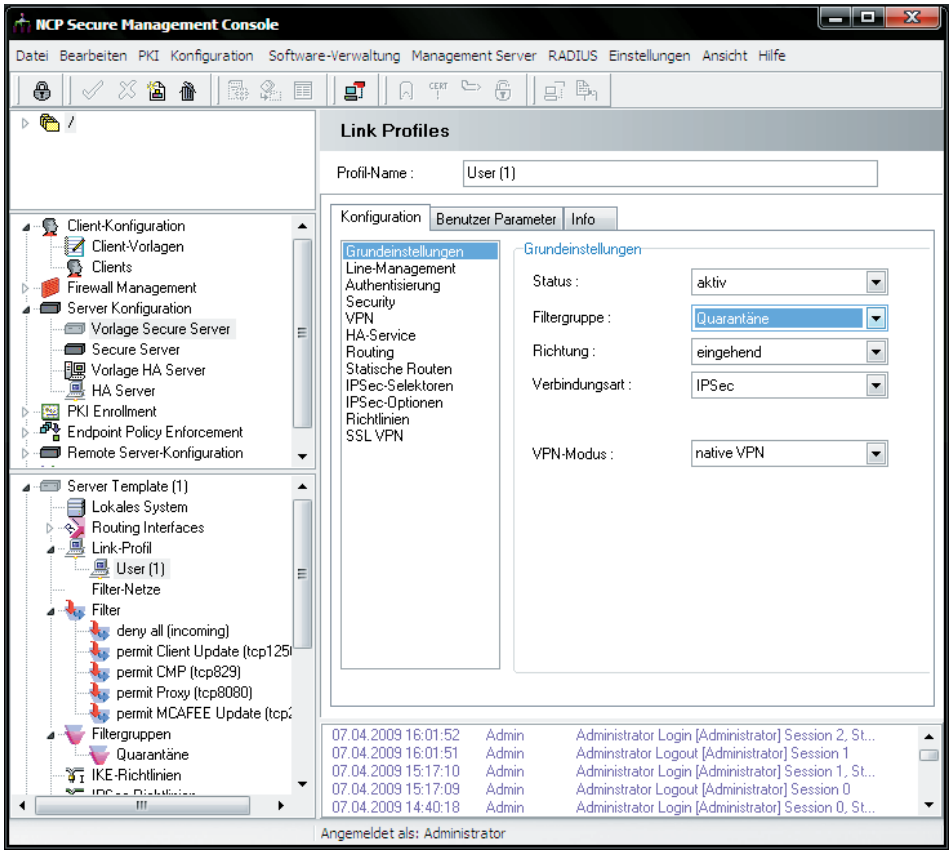
– Endpoint Policy Server (tcp 12511)
– Management Server für Client Update (tcp 12501)
– Management Server für Client Update (tcp 829)
– http-Proxy (tcp 8080)
– Update-Server des Virenscanner-Herstellers per ftp (tcp 21)

Jede andere Kommunikation soll blockiert werden.

Die “Quarantäne-Zone” wird über die Filterregeln bzw. Filtergruppen des NCP Secure Servers eingerichtet, alle notwendigen Kommunikationsbeziehungen werden als Filter erstellt und in einer Filtergruppe zusammengefasst, die dann einzelnen Benutzern zugewiesen werden kann.

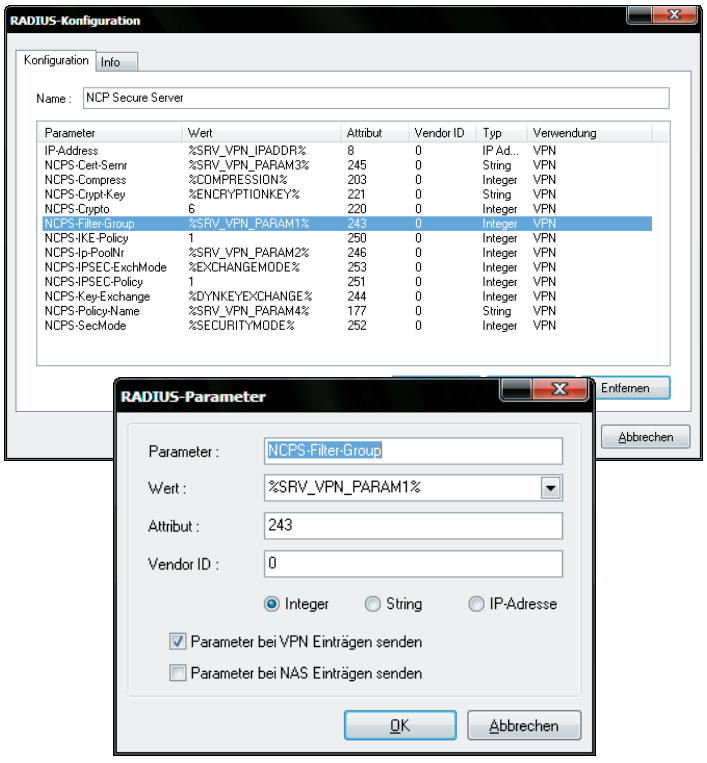


Die Quarantäne-Filtergruppe muss nun, genau wie der Policy-Name, den Benutzern zugewiesen werden. Dies erfolgt bei lokal angelegten Benutzern im Secure Server. Dort wird pro Benutzer im Bereich “Client Policy” der Parameter “Filtergruppe” auf den gewünschten Wert gesetzt. (Abb. unten)




Bei RADIUS-Benutzern erfolgt die Zuweisung wieder mittels RADIUS-Attribut, dieses lautet “NCPS-Policy-Filtgrp”, und bei LDAP-Benutzern ist das Attribut “ncpmprWANLinkPolicyFilterGroup” zu setzen.

Bei der Zuweisung der Filtergruppe mittels RADIUS muss ein Integer-Wert angegeben werden, der auf die Filtergruppe im NCP Secure Server referenziert. Der Wert, der angegeben werden muss, berechnet sich aus dem Index, der im Secure Server Manager für die Filtergruppe angezeigt wird, abzüglich “1". In unserem Beispiel wird für die Filtergruppe ”(0) Quarantäne" der Index “1" angezeigt, demnach muss im RADIUS-Server ”1-1=0" der Wert “0" eingetragen werden. (Abb. rechts)

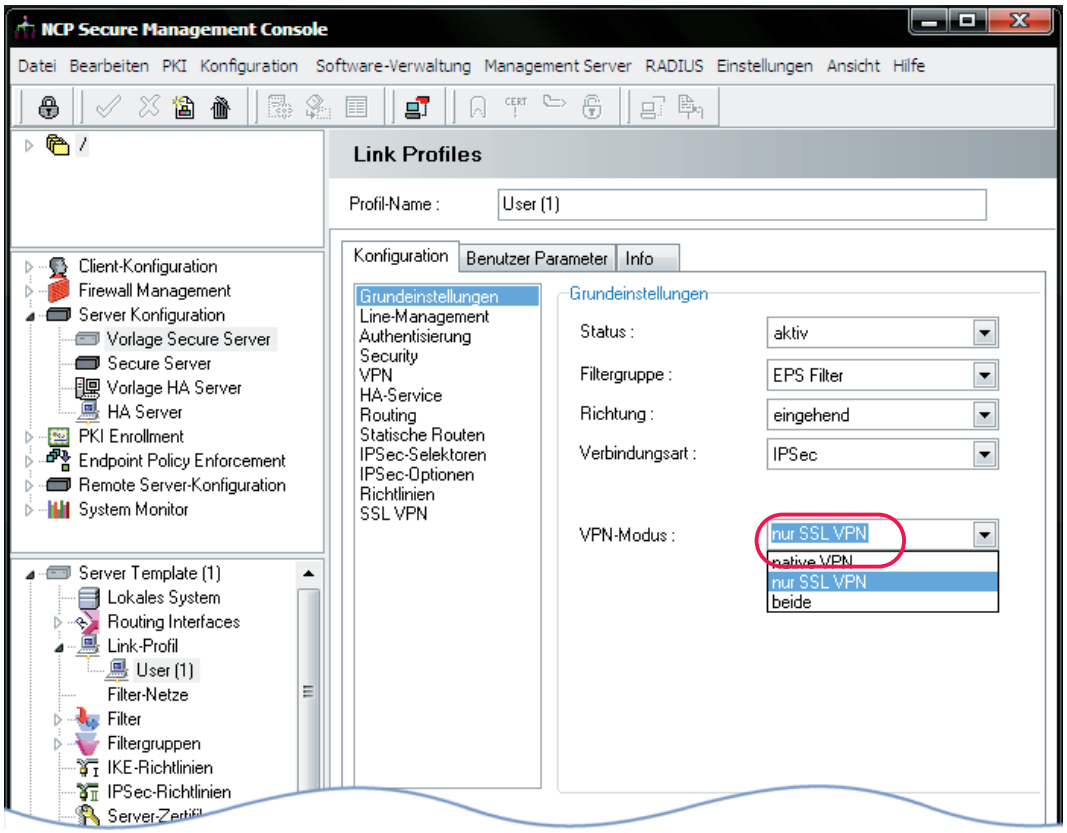



Wurden diese Einstellungen übernommen, so sorgt der NCP Secure Server nach dem Verbindungsaufbau eines Clients dafür, dass dieser erst dann Zugang zum Produktiv-Netzwerk erhält, wenn er die in der Richtlinie vorgegebenen Regeln entsprechend positiv erfüllt. Während der Überprüfung und sofern das Regelwerk nicht erfolgreich abgearbeitet werden kann, wird die mögliche Kommunikation des Clients auf die in der Filtergruppe angegebenen Adressen und Ports beschränkt. Diese Einschränkung gilt auch, wenn ein Client eingesetzt wird, der Endpoint Security nicht unterstützt.

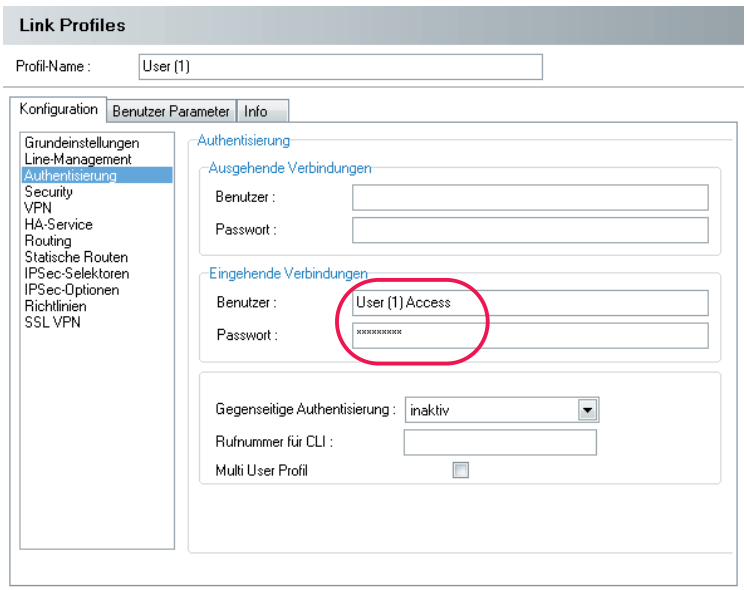
# Endpoint Security mit SSL/VPN-Benutzern

Für den folgenden Abschnitt beachten Sie bitte auch die Beschreibung im Handbuch zum **SSL/VPN-Server**.

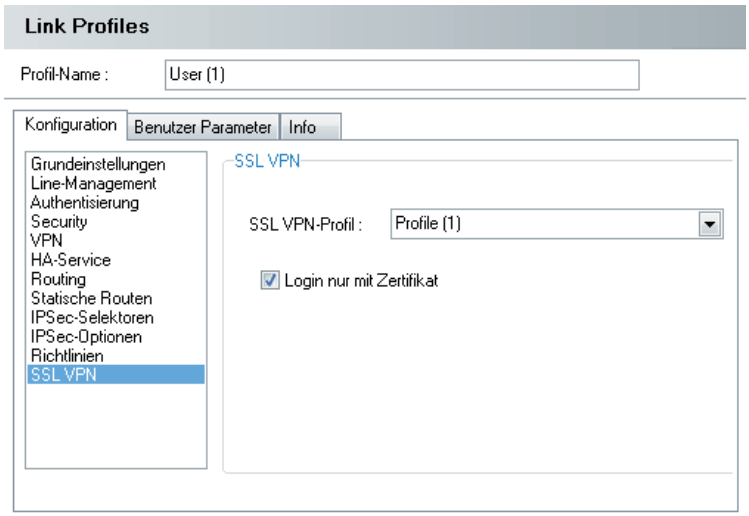
## Zur Konfiguration eines SSL/VPN-Benutzers am Server




Im Konfigurationsbaum des Server Managers wurde ein Link-Profil für SSL/VPN-Anwendungen angelegt. In den Grundeinstellungen dieses Link-Profils wurde dazu der Parameter “VPN-Modus” auf “Nur SSL/VPN” oder, wenn IPSec mit benutzt werden soll, auf “IPSec + SSL/VPN” gestellt. (Bild links)

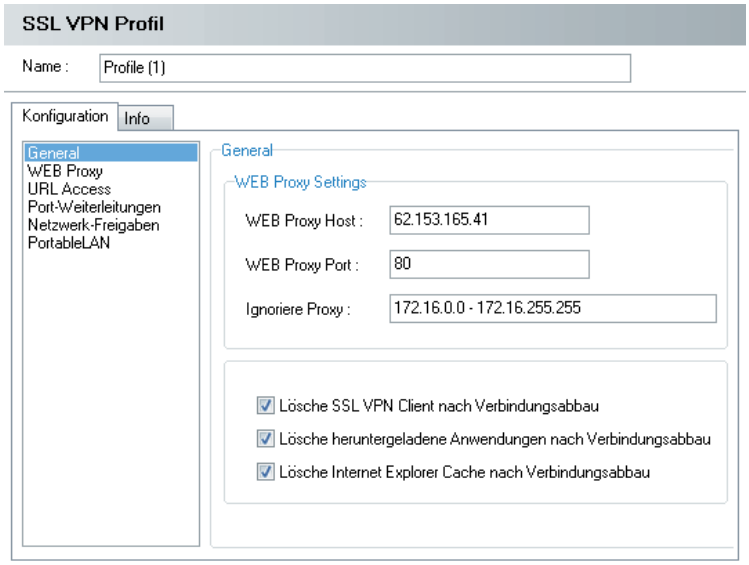



Im Parameterfeld “Authentisierung” (Bild links) wurde unter “Eingehende Verbindungen” die Art der Authentisierung für den SSL/VPN-Anwender definiert. Wurde für den Anwender keine zertifikatsbasierte Authentisierung konfiguriert, so muss er die hier eingetragenen Zugangsdaten auf der Login-Seite des Browsers eingeben, um eine Verbindung zum Gateway herstellen zu können.

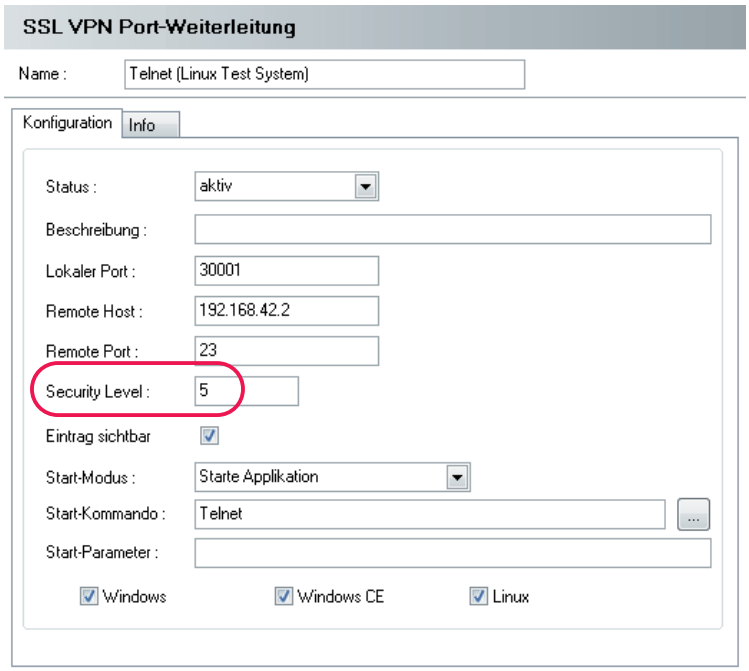



Soll sich der Benutzer über Zertifikat authentisieren, so kann dies benutzerspezifisch in der Link-Konfiguration unter "SSL/VPN" eingestellt werden. Die Aktivierung dieser Funktion hat nur Bedeutung, wenn in der Listener-Konfiguration keine zertifikatsbasierte Authentisierung eingestellt wurde.

Wenn die zertifikatsbasierte Authentisierung in der Listener-Konfiguration aktiviert wurde, so gilt sie für alle SSL/VPN-Anwender. Das Zertifikat muss dann am Browser des remote PCs eingespielt worden sein. (Dabei kann das PKCS#11-Modul des Browsers verwendet werden.) Dieses Zertifikat wird für die SSL-Verhandlung herangezogen und kann mit demjenigen identisch sein, das ein NCP Secure Client verwendet. (Beachten Sie die Konfigurationsbeschreibung im Handbuch zum SSL/VPN Server!)




In der SSL/VPN-Konfiguration dieses Link-Profils wurde sodann mit einem SSL/VPNProfil-Namen (Bild oben) festgelegt, welche Web Proxy- und Port-Forwarding-Anwendungen und welche Network Sharings für dieses Link-Profil, das den Benutzer-Zugang zum Gateway regelt, nutzbar sein sollen.




Dabei konnten für diese Anwendungen Security Level gesetzt werden. (Im Bild oben eine Port Forwarding-Anwendung mit Security Level 5). Was diese Level für die Endpoint Security bedeuten und bewirken wird im folgenden kurz beschrieben.

## Security Policy Level am Server

Prinzipiell können sowohl für die SSL/VPN-Anwender-PCs als auch für die PCs der Secure Clients die gleichen Sicherheits-Richtlinien zum Einsatz kommen. Je nach installiertem Betriebssystem auf dem Anwender-PC und dem installierten Secure Client können jedoch nur die Werte und Parameter abgefragt und verglichen werden, auf die ein Zugriff am jeweiligen PC möglich ist. Diese Zugriffsmöglichkeiten sind auf dem PC eines SSL/VPN-Anwenders für gewöhnlich durch die Rechtestruktur des Betriebssystems stärker eingeschränkt. Entscheidend für die Regel einer SSL/VPN-Richtlinie ist der Eintrag eines Security Levels.

Über den Security Level wird mittels Security-Richtlinie, die am Management-System erstellt wird, die Bereitstellung der jeweiligen Anwendung für die SSL/VPN-Benutzer gesteuert.

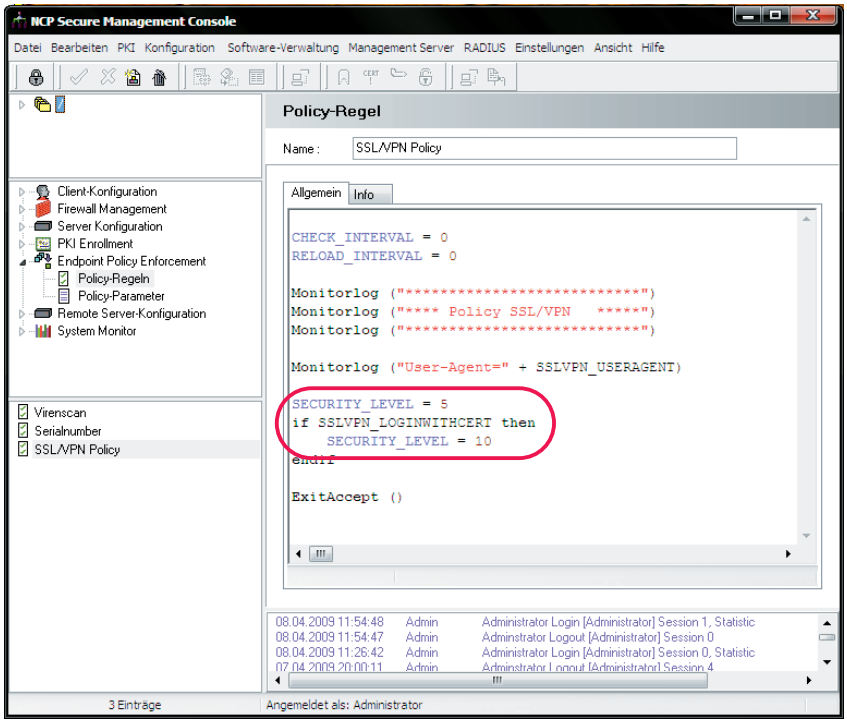
Der Security Level bezeichnet den Wert eines Regelwerks, das mindestens erfüllt sein muss, damit diese Anwendung im Start-Menü erscheint. Der hier einzutragende ganzzahlige Wert muss mit den Definitionen der Sicherheits-Richtlinien im Secure Enterprise Manager abgestimmt sein.

## Security Level im Management System

Policy Rules für SSL/VPN-Anwender-PCs erhalten vom Management-System den Wert für einen Security Level, der einer SSL/VPN-Anwendung zugeordnet werden kann. Die interne Variable SECURITY_LEVEL kann dabei aus der Online-Hilfe des Management-Systems übernommen werden.

Bei Einsatz des Endpoint Policy Enforcements erhält der SSL/VPN-Anwender je nach Regelerfüllung einen Security-Wert, der die entsprechende(n) Anwendung(en) zur Verwendung freischaltet, d. h. auf der Startseite des Browsers darstellt.

Zahlenwerte ausgedrückt. Je höher der Zahlenwert, desto stärker die Regel, d. h. desto strenger die Sicherheitsanforderungen. Die Regeln werden im Endpoint Policy Enforcement Plug-in als Wenn-Dann-Bedingungen formuliert. Die Werteskala ist nach oben offen und kann nach Belieben skaliert werden. In obiger Abbildung wird ein Login-Vorgang mit Zertifikat mit dem Security Level ”10" bewertet. Das Vorhandensein eines Virenscanners kann z. B. mit (5) bewertet werden und das installierte Betriebssystem Windows 2000 mit “2".




Die fertiggestellten Policy Rules (Regelwerk) werden nach dem Gruppenprinzip des Secure Enterprise Managements einer Benutzergruppe zugeordnet (im Bild oben der Root-Gruppe). In einer der Client-Vorlagen dieser Gruppe werden die Policies unter “Server-Parameter / VPN” eingebunden.

Nach Anlegen eines Benutzers mit der entsprechenden Vorlage kann unter “Server-Parameter / VPN” die Regel (individuell) eingetragen werden. Anschließend werden am Server Manager die Client-Konfigurationen erzeugt und am Management Server abgelegt.

Um den Überblick darüber zu behalten, welche Sicherheitsanforderungen an die zugehörigen Client PCs gestellt werden, sollte eine Tabelle mit Zahlenwerten des Security Levels erstellt werden. Z. B.:

Security Levels werden zentral über das Management System definiert. Nur der Level “1" ist dabei fest definiert als der kleinste Level, d. h. ohne Policy-Regel. Alle weiteren Levels werden durch

| Endpoint Security-Tabelle | |
|---|---|
| Anwender-PC | Security Level |
| Betriebssystem Windows 2000 | 2 |
| Virenscanner | 5 |
| Hash-Datei | 10 |

## Zum Ablauf der Richtlinien-Prüfung

Am Gateway (Secure Server) findet eine Zwischenspeicherung der Konfigurationen einschließlich der Policies statt. Beim Verbindungsaufbau eines Anwender-PCs zum Gateway werden Software- und Policy-Versionen automatisch abgeglichen, im Fall einer SSL/VPN-Verbindung über Browser wird bei Bedarf der Thin SSL/VPN Client mit den Policy-Informationen aktualisiert.

Die Web Proxy-oder Port Forwarding-Anwendungen, sowie die Network Sharings werden wie oben beschrieben mittels Server Manager am Gateway konfiguriert. (Beachten Sie dazu auch das Handbuch zum SSL/VPN-Server). Dabei ist darauf zu achten, dass der Wert des Security Levels in einem praktikablen Verhältnis zu den Werten in der Endpoint Security-Tabelle steht.

Nach Maßgabe der Policy wird die Umgebung des Anwender-PCs geprüft. Nur wenn die Sicherheits-Anforderungen vom Anwender-PC erfüllt werden, die der Secrity-Level für die auf der Menü-Seite gelisteten Anwendungen verlangt, wird die jeweilige Anwendung auf der Menü-Seite auch dargestellt.

D. h. gelangt ein Anwender (nach obigem Beispiel) von seinem PC aus über den Browser auf die Menü-Seite, nachdem er sich auf der Login-Seite mit Zertifikat authentisiert hat, so kann er von dort alle Applikationen nutzen, deren Security Level nicht größer als “10" ist.

## Skalierung und Auswertung der Regel

Das Regelwerk kann auf verschiedene Arten abgefasst werden. Unter anderem
- mit einer Einzelregel, der ein Wert zugeordnet ist. In diesem Fall ist der Wert der Regel gleich dem Wert des Security Levels, sofern der PC die Bedingung erfüllt.
- mit einer Regelverkettung, bei der der höchste Regel-Wert dem maximal erreichbaren Security Level entspricht. In obigem Beispiel sind die jeweiligen Werte:

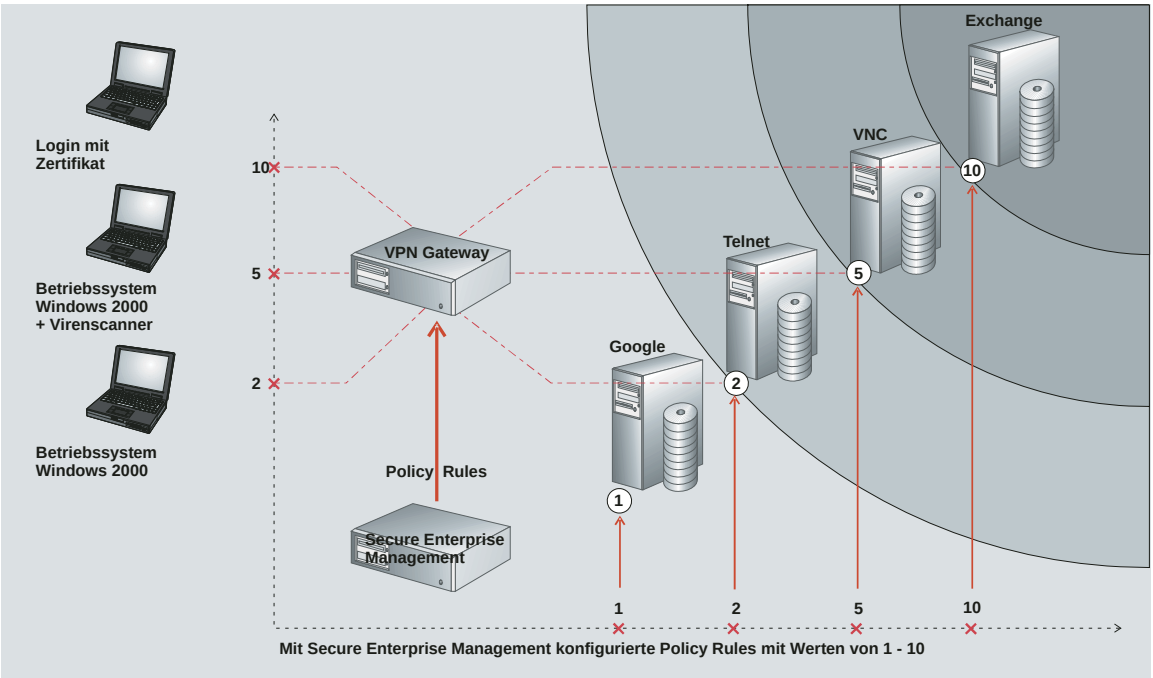
```
Betriebssystem Windows 2000   |  2
Virenscanner                  |  5
Hash-Datei                    | 10
```

Die Verkettung kann so definiert werden, dass stufenweise alle Regeln erfüllt sein müssen, um den Level “10" zu erreichen. Wird eine der Regeln nicht erfüllt, wird die Anwendung nicht frei gegeben.

Die Verkettung kann auch so definiert werden, dass aus der Liste der Regeln die Werte der erfüllten Regeln addiert werden, gleich in welcher Reihenfolge und unabhäng davon, welche Regel nicht erfüllt wird. Der addierte Wert wird dann verglichen mit dem Security Level der Anwendung.

Weitere Mischformen sind möglich; etwa, dass nur ein höchster Wert einer erfüllten Regel mit dem Security Level der Anwendung verglichen wird.

Entscheidend ist, dass der Wert, der sich aus dem Regelwerk ergibt immer mit dem Security Level der Anwendung verglichen wird. Alle Anwendungen mit Level (x) können nur genutzt werden, wenn der Security-Wert des Anwender-PCs einen Level größer oder gleich dem Level (x) besitzt.



Mit Secure Enterprise Management konfigurierte Policy Rules mit Werten von 1 - 10

# Die Meldung am Secure Client

Bei jeder Verbindung eines Remote-Systems fragt der Secure Server ab, ob der Client die Endpoint Policy erfüllt.

## Bei Erfüllung einer Richtlinie

Bei Erfüllung der Richtlinien wird der Netzbereich freigeschaltet, auf den der Client im regulären Betrieb Zugriff benötigt. Dieser Netzbereich wird, wie oben beschrieben (Nichterfüllung einer Richtlinie), über die Filtergruppe für eingehende Links definiert, die im Konfigurationszweig “Link-Profile / Grundeinstellungen” selektiert wurde. Im Client Monitor ist unter der aufgebauten VPN-Verbindung ein Schreibtischsymbol für die mit grüner Farbe als “ok” abgehakten Richtlinien zu erkennen.


Werden die Richtlinien erfüllt, wird das Symbol für Endpoint Security grün dargestellt (oben).

## Bei Nicherfüllung einer Richtlinie

Bei Nichterfüllung der Richtlinien wird die VPN-Verbindung zunächst ebenso zum Secure Server aufgebaut. Das Schreibtischsymbol erscheint jedoch mit rot abgehakten Richtlinien, als Zeichen für deren Nichterfüllung.


Werden die Richtlinien nicht erfüllt, wird das Symbol für Endpoint Security rot dargestellt (oben).

Je nach vorher am Management System festgelegter Policy können im weiteren Verlauf unterschiedliche Aktionen erfolgen. Z. B.:

– kann die Verbindung abgewiesen werden
– kann die Verbindung auf einen Netzbereich eingeschränkt werden, der durch eine Filtergruppe definiert wird (siehe oben **Nichterfüllung einer Richtlinie**).

Allgemein gilt, dass bei Nichterfüllung der Policy die Reaktion erfolgt, die in der Policy zwischen den Operatoren “if” und “endif” steht.

### Beispiel

Zum Beispiel wird die Meldung “McAfee Virus Scanner is not up to date (xxxx)” im Fenster des Log-Buchs ausgegeben, wenn die Version des Virenscanners nicht den Erfordernissen der Regel entspricht und in der Richtlinie die Ausgabe dieser Meldung als MonitorLog definiert wurde.

Diese Meldung kann, wie im Beispiel unten, mit der Variablen “msg =” definiert werden, sodass für das Kommando “MonitorLog” nur die Variable “(msg)” gesetzt werden muss.

Statt der Variablen kann aber auch eine Meldung im Klartext hinter dem Kommando eingegeben werden. Im Beispiel unten wird durch das Kommando “MonitorMessage” der Text ausgegeben, der in den Klammern zwischen den Anführungszeichen steht.

```
CHECK_INTERVAL  = 60
RELOAD_INTERVAL = 3600

currentVersion = MCAFEE_VERSION

if MCAFEE_VIRUSSCAN_VDFVER < currentVersion then
   msg = "McAfee Virus Scanner is not up to date
         ("+ MCAFEE_VIRUSSCAN_VDFVER +")"

" Disconnect ()
   MonitorLog (msg)
   MonitorMessage ("virus scanner has old signatures")
   ExitReject (msg)
endif

ExitAccept ()
```

(Die Verbindung zum Firmen-Gateway wird nur getrennt, wenn das Hochkomma zum Disconnect-Befehl in obiger Regel entfernt wird.)

### MonitorLog

Mit diesem Kommando wird eine Meldung im Log-Fenster des Client-Monitors ausgegeben. Die Meldung kann als Variable (msg) in der Richtlinie definiert werden oder als Klartext zwischen den Anführungszeichen in den Klammern.

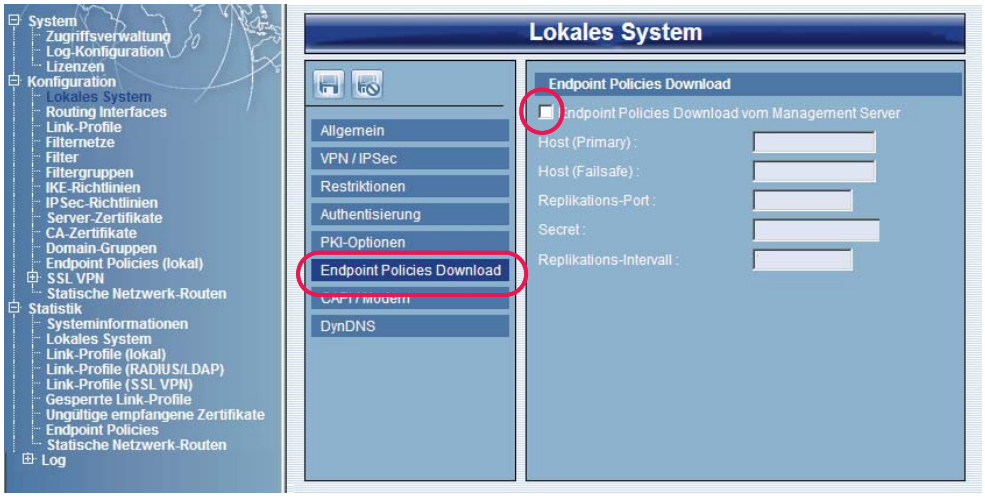
### MonitorMessage

Mit diesem Kommando wird eine Messagebox über dem Client-Monitor geöffnet, die eine Information enthält. Die Information kann als Variable (msg) in der Richtlinie definiert werden oder als Klartext zwischen den Anführungszeichen in den Klammern.

# Konfiguration der Endpoint Policies am Server

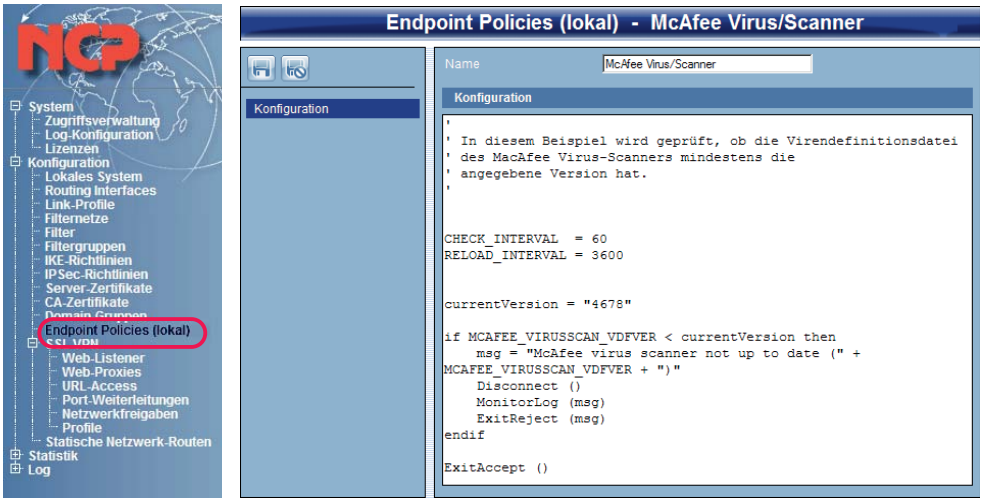
Eine ausführliche Beschreibung zu den im folgenden abgebildeten Parameterfenstern und Parametern des Web-Interfaces finden Sie im PDF **SES-Parameter-d**.

Ab der Secure Enterprise Server Version 8.0 können Endpoint Policies wahlweise entweder am Secure Enterprise Server oder mit dem Management-System angelegt werden.




**1.** Das entsprechende Auswahlfenster befindet sich im Konfigurationsbaum des Web-Interfaces unter **Lokales System / Endpoint Policies Download**. (Abb. links)

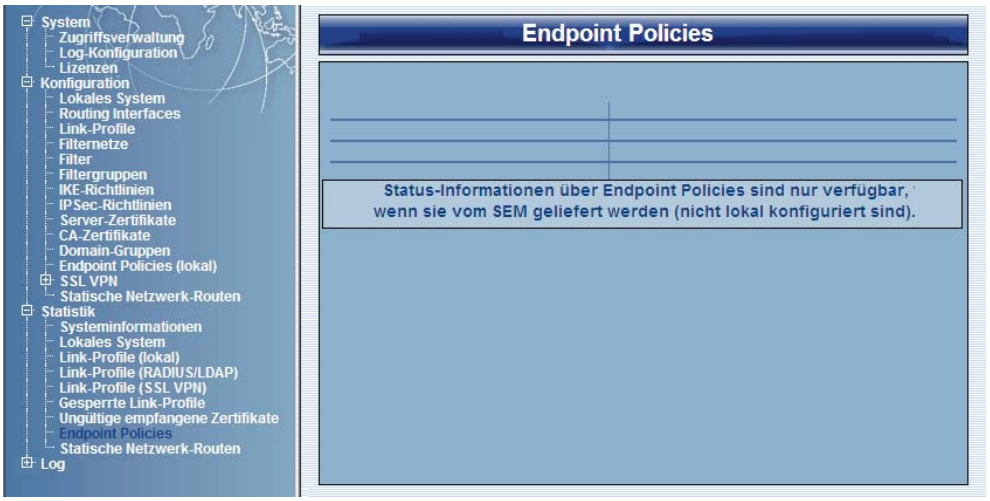
Ist ein Download vom Management Server wie in der Abbildung links ausgeschaltet, so können Policies am Server angelegt werden.




**2.** Die Konfiguration der Richtlinie erfolgt im Konfigurationsbaum des Web-Interfaces unter **Endpoint Policies (lokal)**. Dabei kann ebenso wie im Management-System die Online-Hilfe der Endpoint Security verwendet werden. Daraus kann z. B. eine Richtlinie wie in nebenstehender Abblidung kopiert und in das Konfigurationsfenster eingefügt werden.

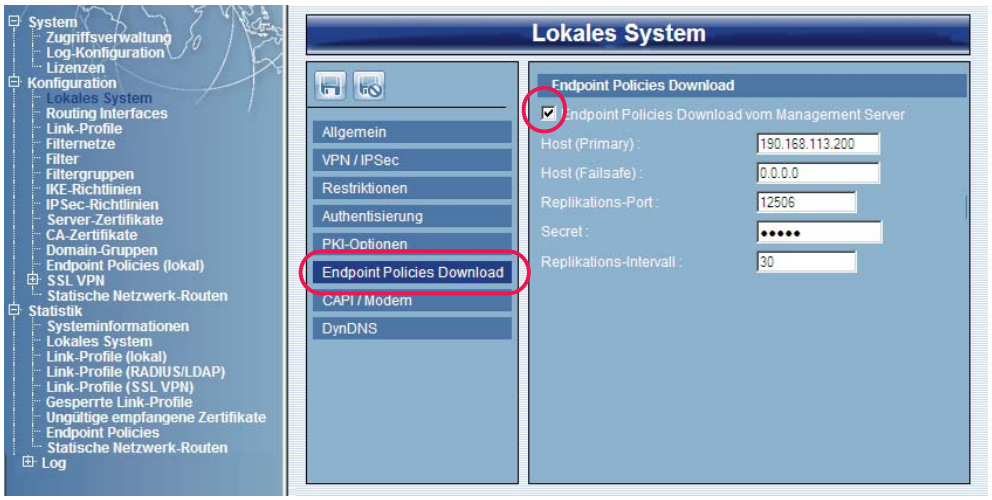

**3.** Nachdem die Richtlinie unter einem eigenen Namen gespeichert wurde, kann sie an diesem Server eingesetzt werden.

Dazu wird im Konfigurationsbaum unter **Link-Profile / Endpoint Policy** die gewünschte Policy selektiert.

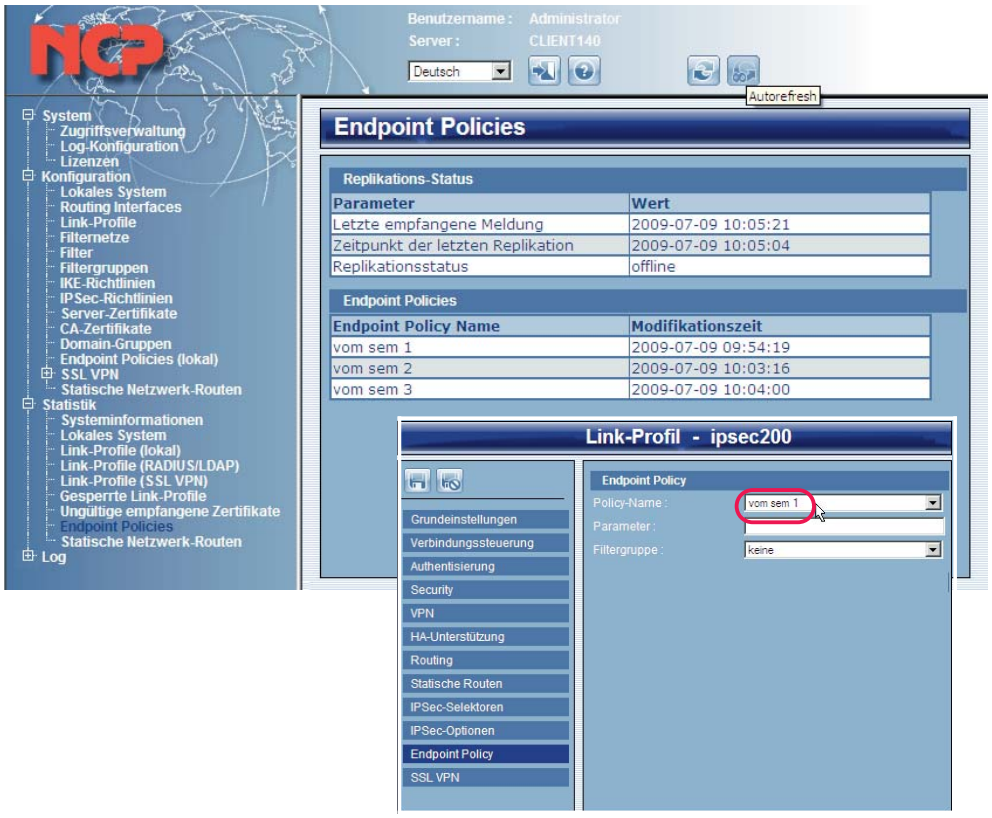



**4.** Statusinformationen stehen für lokal konfigurierte Richtlinien nicht zur Verfügung.

## Endpoint Policies Download von Management Server




Wird ein Download vom Management Server aktiviert, müssen die Zugangsdaten zum SEM eingegeben werden. Das hier einzugebende Secret muss mit dem Shared Secret am SEM übereinstimmen (siehe oben **Verteilung an die VPN Gateways** und **Konfiguration der Secure Server**). Zur Konfiguration mit dem Web-Interface gehen Sie zu **Endpoint Policies Download**.




Die heruntergeladenen Richtlinien werden in der Statistik unter Endpoint Policies namentlich und mit einem Zeitstempel versehen angezeigt wie in nebenstehendem Bild.

(Vergessen Sie nicht, den Refresh-Button zu drücken.)

Sobald eine Richtlinie heruntergeladne wurde, kann sie für ein Link-Profil selektiert werden (Abb. links unten).

*(Download ausschalten – nächste Seite)*

## Download ausschalten

Wird der **Endpoint Policies Download von Management Server** in der Konfiguration über das Web-Interface des Servers nach einer gewissen Betriebsdauer wieder ausgeschaltet, so werden die vormals heruntergeladenen Richtlinien gelöscht!

Stattdessen werden die vorher am Server konfigurierten Endpoint Policies wieder hergestellt, sodass sie in den Link-Profilen wieder selektiert werden können (siehe oben).