Howto für das Praktikum NWS

Notizen

1. Einleitung

Im Praktikum des Fachs NWS sollen sie die Administration des Firewall-Systems der Firma Compumatica erlernen. Das Firewall-System besteht aus den folgenden Komponenten.

**Security Management Station (SMS) -
zentrale Verwaltung Ihres Firewall-Systems**

Die Security Management Station (SMS) ermöglicht die zentrale Verwaltung der Hauptelemente Ihres Firewall-Systems. Mit der SMS definieren Sie die Filterregeln für CryptoGuard VPN, steuern den Proxy-Einsatz auf der CryptoBastion und kontrollieren die kryptografisch gesicherten Verbindungen. Hier gehen Alarm- und Zustandsmeldungen (Spontane Meldungen) der einzelnen Komponenten ein. Die Kommunikation der SMS mit den anderen Komponenten kann verschlüsselt geschehen, wodurch ein typischer Angriffspunkt von Firewall-Systemen eliminiert wird. Bei der SMS handelt es sich um einen Standard PC mit dem Linux-Betriebssystem Suse 8.2.

CryptoBastion - Application Gateway für sicheren Zugang zum Internet

Die CryptoBastion trennt Ihr privates Netz logisch und physikalisch vom unsicheren öffentlichen Netz. Der gesamte Datenverkehr zum Internet läuft ausschließlich über diesen Rechner. Proxies stellen gezielt die Verbindung für bestimmte Dienste und Protokolle (HTTP, FTP, Telnet, ESMTP, NNTP usw.) her. Dadurch wird jeder unmittelbare externe Zugriff auf Ihre Systeme verhindert und die Struktur Ihres internen Netzes bleibt nach außen hin unsichtbar (address hiding). Die CryptoBastion prüft die Zugangsberechtigung jedes externen Benutzers und arbeitet nach erfolgreicher Authentikation transparent.

CryptoGuard VPN (CG-VPN) - Paketfilter und Datenverschlüsselung

CryptoGuard VPN ist eine Hardware-Box für Paketfilterung und transparente Datenverschlüsselung. Der Paketfilter kontrolliert den durchgehenden Datenstrom nach den Regeln, die Sie definieren, z.B. IP/ Benutzer-Adresse, Wochentag, Protokollen, Diensten und anderen Kategorien. Mit dieser Funktion von CryptoGuard VPN können Sie Netze oder Strukturen von Teilnetzwerken mit differenzierten Zugangsbedingungen absichern. Beim Einsatz von CryptoGuardVPN schützt die starke Verschlüsselung zudem die Vertraulichkeit Ihrer Kommunikation - auch über das öffentliche Netz hinweg. So schaffen Sie Virtual Private Networks (VPNs).

Client

Als IPSec Clients werden IPSec-fähige Endgeräte (z.B. SafeGuard VPN 2.50) bezeichnet. Diese Geräte können zwar in der Security Management Station aufgenommen, aber nicht mit ihr über das Netzwerk administriert werden. Die Administration erfolgt über das Erzeugen von Konfigurationsdateien, die auf eine Diskette exportiert werden. Die auf der Diskette enthaltenen Dateien können dann in das IPSec-fähige Gerät übertragen werden.
Der IPSec Client SafeGuard VPN 2.50 ist mit dem KryptoGuard PC vergleichbar, der ebenfalls Endgerät und Security-Komponente vereint.

Notizen

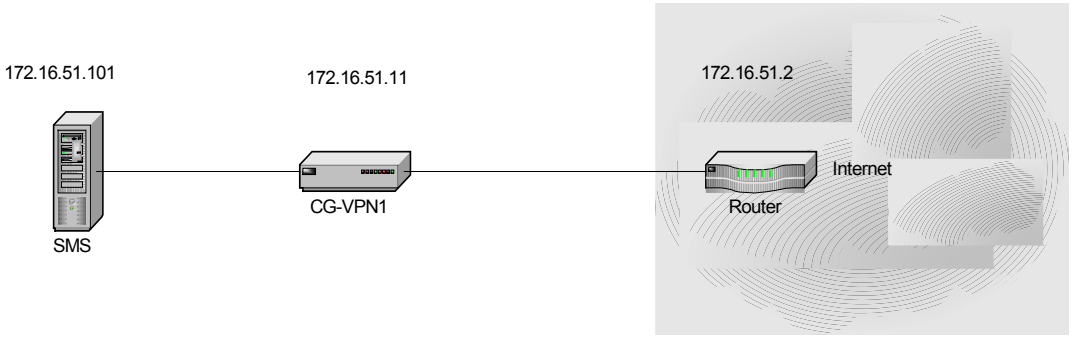
Gateway

Der Ausdruck „Gateway“ wird im Rahmen der SMS zur Zusammenfassung der Geräte CryptoGuard VPN, CryptoGuard VPN IPSec, und IPSec-Gateway verwendet.

IPSec Gateway

Als IPSec Gateway werden IPSec-fähige Geräte anderer Hersteller (z.B. Router) bezeichnet. Diese Geräte können zwar in der Security Management Station aufgenommen, aber nicht mit ihr über das Netzwerk administriert werden. Die Administration erfolgt über das Erzeugen von Konfigurationsdateien. Die auf eine Diskette exportiert werden. Die auf der Diskette enthaltenen Dateien können dann in das IPSecfähige Gerät übertragen werden.

2. Erstes Szenario



In diesem Szenario sollen Sie Administration eines CG-VPN erlernen. Eine verschlüsselte Datenverbindung ist zwischen zwei CG-VPN s möglich. Da in diesem Szenario nur ein CG-VPN verwendet wird, wird hier das CG-VPN als Packetfilter bzw. Packetfirewall verwendet. Sie sollen das CG-VPN 1 so Konfigurieren, das nur die Protokolle DNS und HTTP von der SMS in das Internet möglich sind. Alle anderen Protokolle bzw. Datenverbindungen sollen vom CG-VPN 1 unterbunden werden.

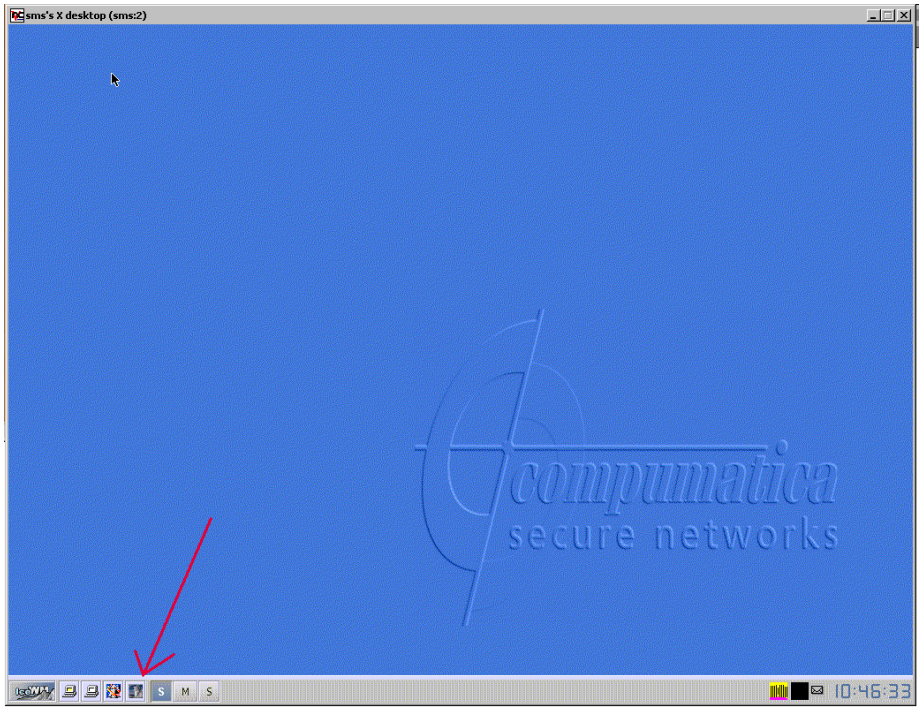
2.1 Vorbereitung

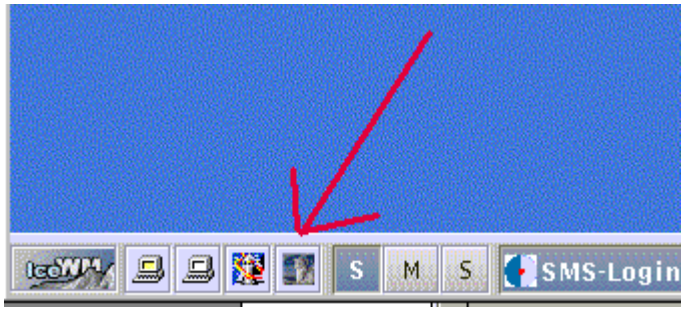
- Schalten Sie die SMS ein
- Schalten Sie den CG-VPN1 ein
- Verbinden Sie die Netzwerkkarte der SMS mit der Plain-Netzwerkkarte des CG-VPN 1. Verwenden Sie hierzu ein Crosslink Kabel.
- Verbinden Sie Cipher-Netzwerkkarte mit dem Switch1
- Verbinden Sie den Switch1 mit der Netzwerkanschluss 33 am Kabelkanal
- Verbinden Sie den Seriellport Com1 des SMS mit dem
- Serviceport von CG-VPN1.Verwenden Sie hierzu das Nullmodemkabel.

2.2 Starten der SMS-Software

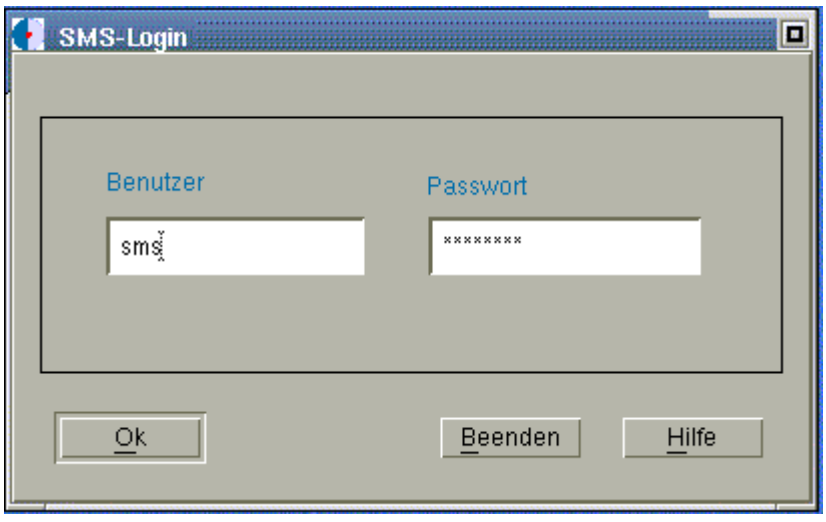
Notizen

- Wenn der Bootvorgang, der SMS beendet ist, loggen Sie sich mit dem Usernamen **sms** und dem Passwort **sms123** . Sie bekommen die folgende Oberfläche angezeigt.





- Starten Sie die SMS-Software indem Sie den Button betätigen auf dem der rote Pfeil zeigt.
- Anschließend erwartet die SMS-Software das Sie sich authentifizieren. Geben Sie im folgenden Dialogfenster für den Benutzer **sms** und für das Passwort **1q2w3e4r** ein.



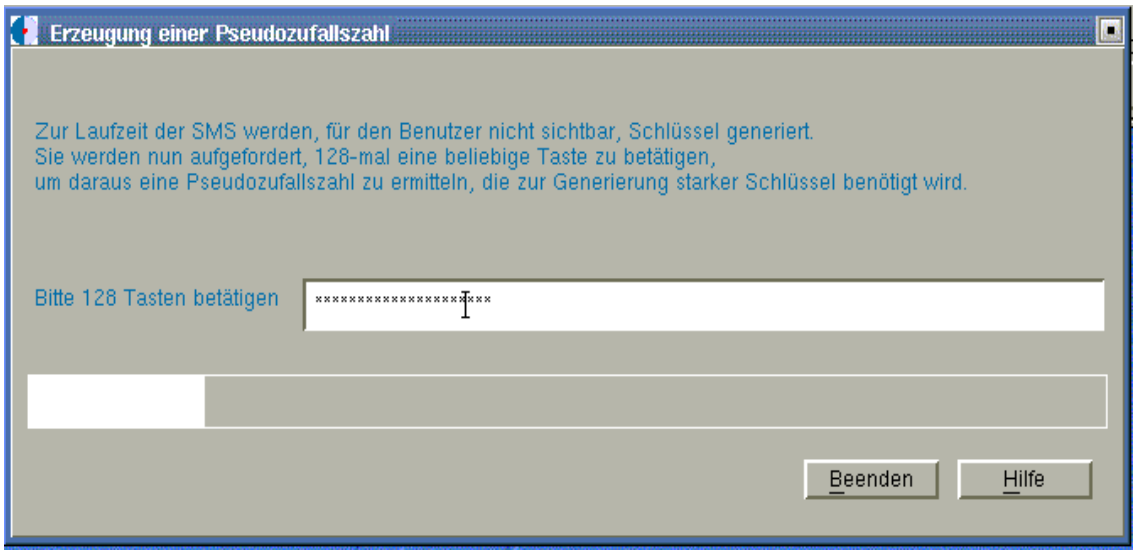
Notizen

Der Zugang zur SMS wird Ihnen nicht gestattet, wenn:

- die maximale Anzahl fehlerhafter Logins erreicht wurde
- die Gültigkeitsdauer Ihres Passworts abgelaufen ist
- Sie durch den SMS-Administrator gesperrt wurden

Erfolglose Authentikationsversuche werden protokolliert und dem Benutzer durch eine entsprechende Meldung angezeigt. Im Falle einer Zugangsverweigerung wenden Sie sich bitte an den SMS-Administrator.

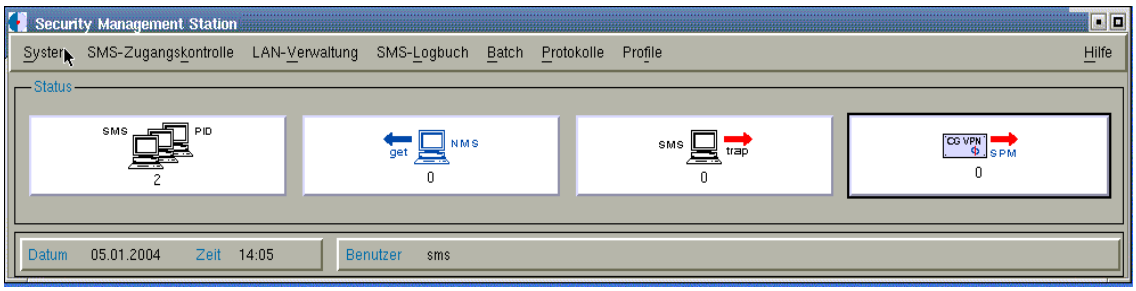
Nach erfolgreichen Login werden Sie aufgefordert, eine Pseudozufallszahl zu erzeugen.



- Betätigen Sie 128-mal eine beliebige Taste.

Verwenden Sie nur Tasten, die druckbare Zeichen generieren. Eine Balkenanzeige zeigt den Fortschritt der Aktion. Sobald die erforderliche Anzahl an Eingaben erfolgt ist, wird die SMS gestartet.
Dieser Vorgang muss bei jedem Neustart wiederholt werden

Nach erfolgreichen Start erscheint das Hauptfenster der SMS



Hilfe zum SMS-Hauptfenster im Anhang A1

2.3 CG-VPN1 zurücksetzen

Notizen

Bevor Sie versuchen einen CG-VPN zu konfigurieren sollten Sie ihn in den Auslieferungszustand (Manufacturing Status) zurücksetzen.

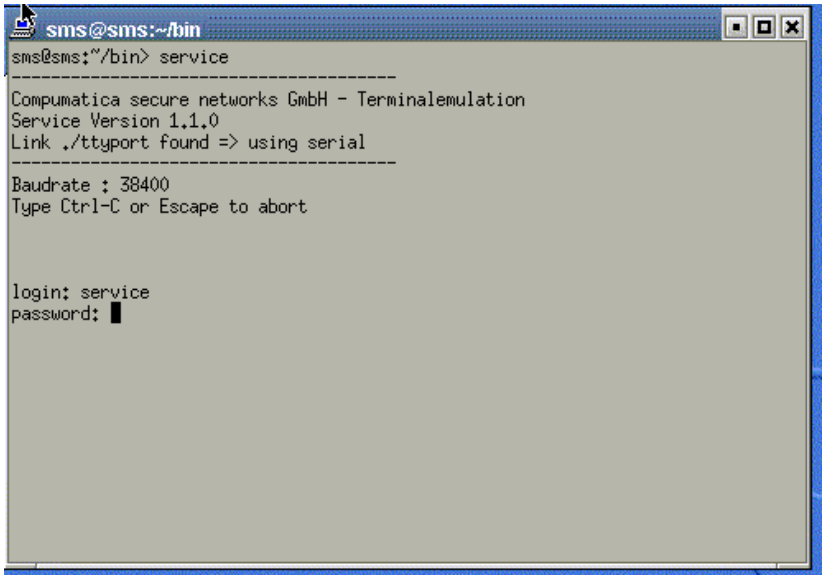
Das Terminalprogramm *service*

Mithilfe des Terminalprogramms ***service*** ist es möglich, über den Serviceport eine direkte Kommunikation zwischen der SMS und einem CryptoGuard VPN herzustellen. Dies wird zum Beispiel erforderlich, wenn Sie einen CryptoGuard VPN in den Manufacturing Status zurückversetzen möchten.

- Um das Terminalprogramm aufzurufen, klicken Sie im Menü ***System*** auf ***Shell***.

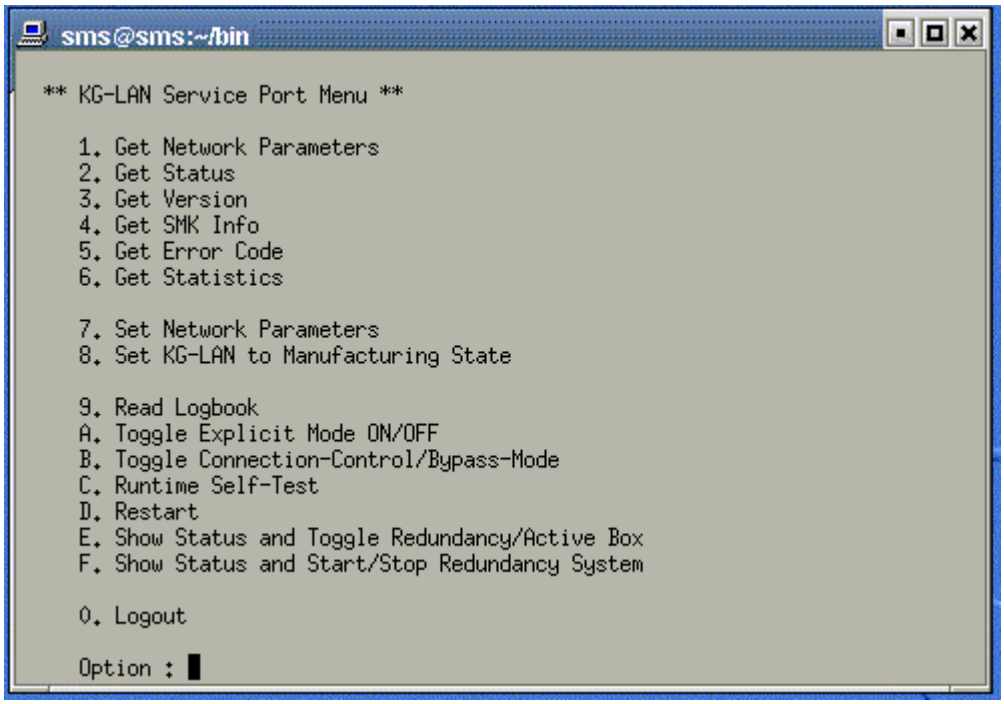
Eine UNIX-Shell öffnet sich.

- Tippen Sie den Befehl ***service*** ein. Der
- Loginname lautet **service**, das standardmäßige Passwort **serpwd01**.

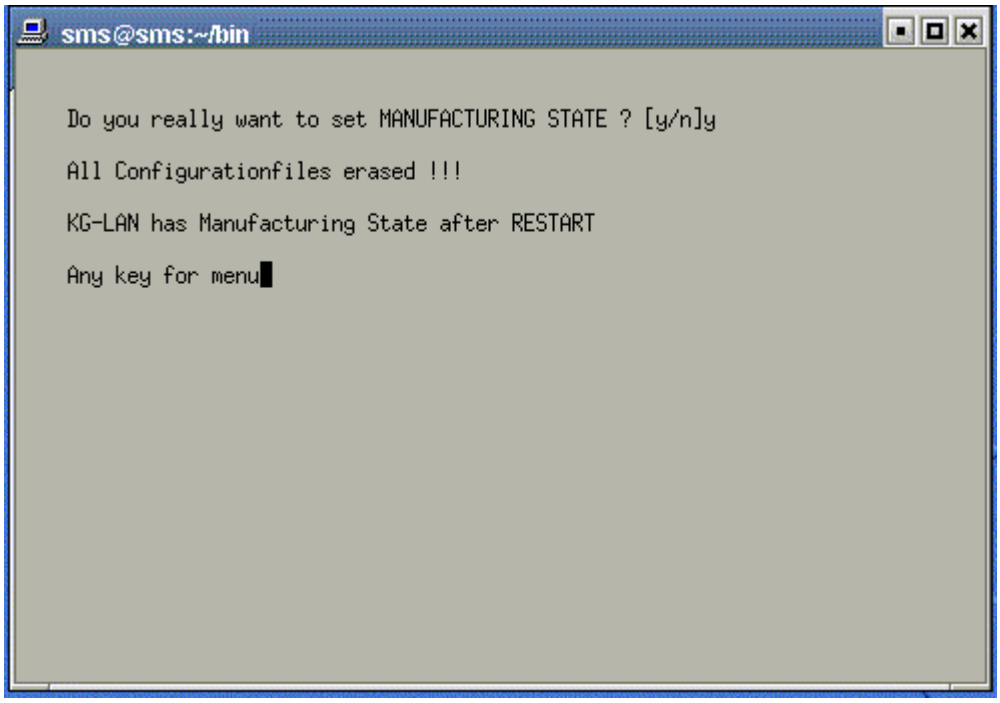


Das daraufhin erscheinende Menü bietet Ihnen eine Vielzahl an Optionen, mit denen Sie die Daten des CryptoGuard VPN abfragen bzw. verändern können.

Notizen



- Setzen Sie den *CG-VPN1* zurück indem Sie den ***Punkt 8*** auswählen und die anschließende Frage mit **y** beantworten.

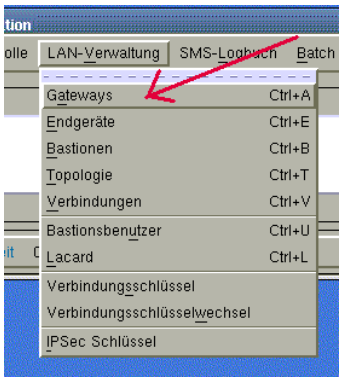


- Jetzt müssen Sie die Option ***D*** auswählen damit der *CG-VPN1* neu gestartet wird.
- Sie beenden das Terminalprogramm mit der Tastenkombination ***Ctrl+C*** und dem Befehl ***exit***

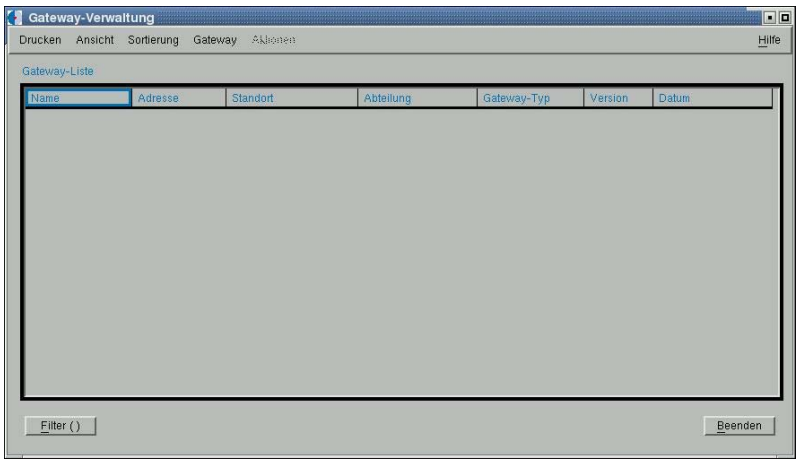
2.4 Ein CG-VPN (Gateway) hinzufügen.

Notizen

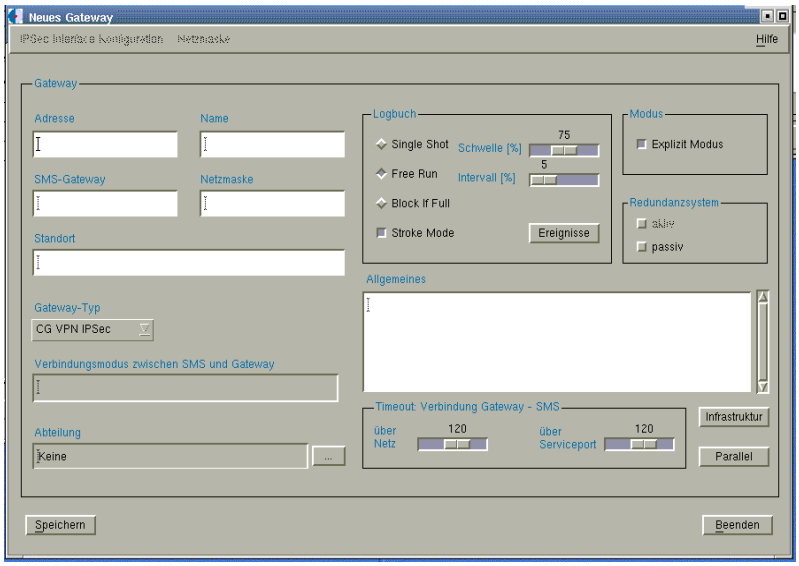
- Um ein neues Gateway zur Datenbank der SMS hinzuzufügen, klicken Sie das Menu ***LAN-Verwaltung*** an und wählen Sie den Menüpunkt ***Gateways*** aus.



Mit dem sich öffnenden Fenster können die Gateways (CG-VPNs) verwaltet werden.



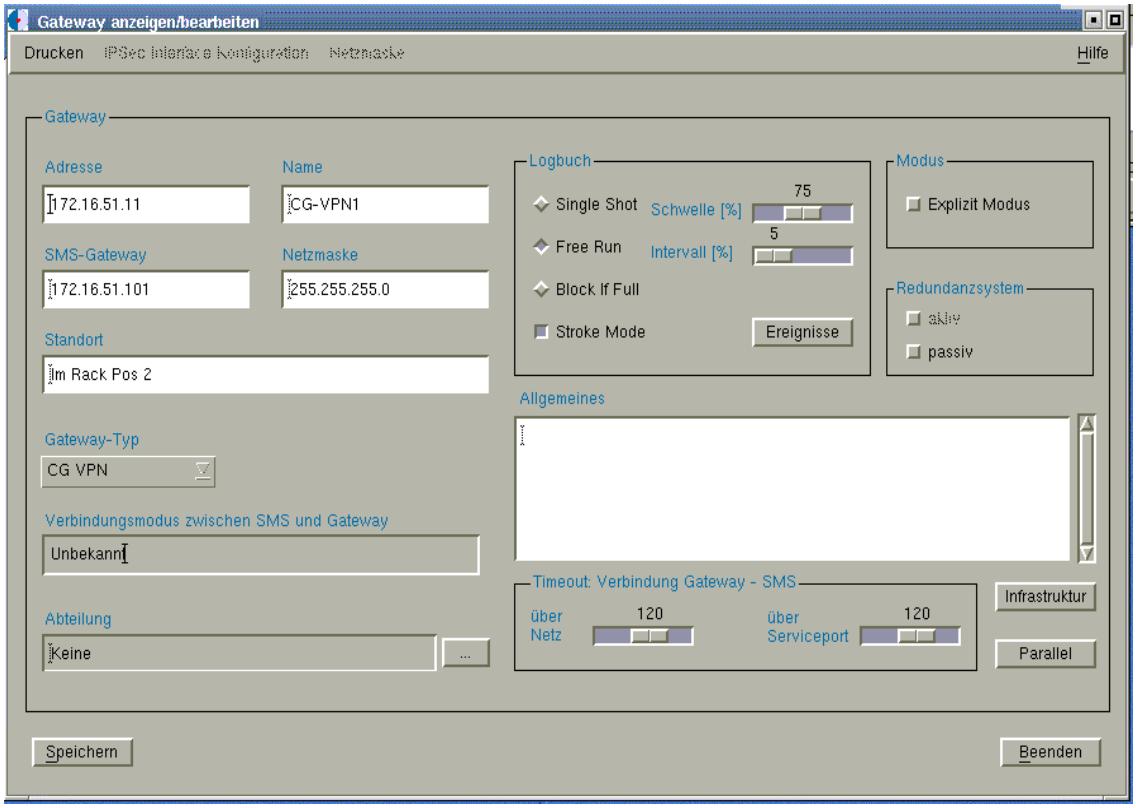
- Klicken Sie im Menü ***Gateway*** auf den Menüpunkt ***Neu***. Es öffnet sich das Fenster ***Neues Gateway***.



In diesem Fenster geben Sie alle relevanten Daten ein, die für das Anlegen eines neuen Gateway-Datensatzes erforderlich sind. Alle Eingaben werden erst auf das Gateway übertragen, wenn Sie den Arbeitsschritt ***Konfiguration*** ausführen.

*Hilfe zum Fenster **Neues Gateway** im Anhang A2*

- Füllen Sie die Eingabemaske wie folgt aus.
  Adresse: 172.16.51.11
  Name: CG-VPN1
  SMS-Gateway: 172.16.51.101
  Netzmaske 255.255.255.0
  Standort: Im Rack Pos 2
  Explizit Modus: off



- Schließen Sie das Fenster ***Gateway anzeigen/bearbeiten*** in dem Sie den Button ***Speichern*** betätigen

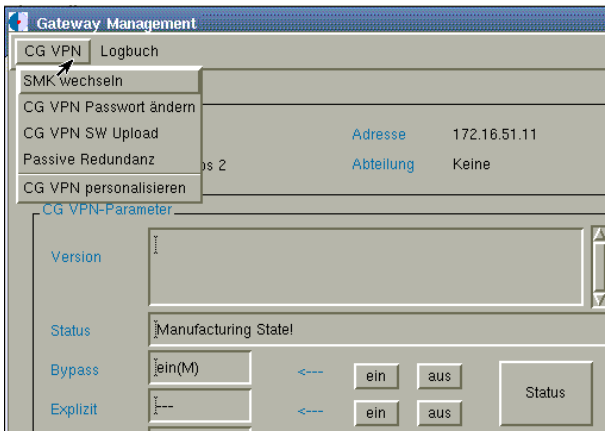
Notizen

2.5 CG-VPN1 personalisieren

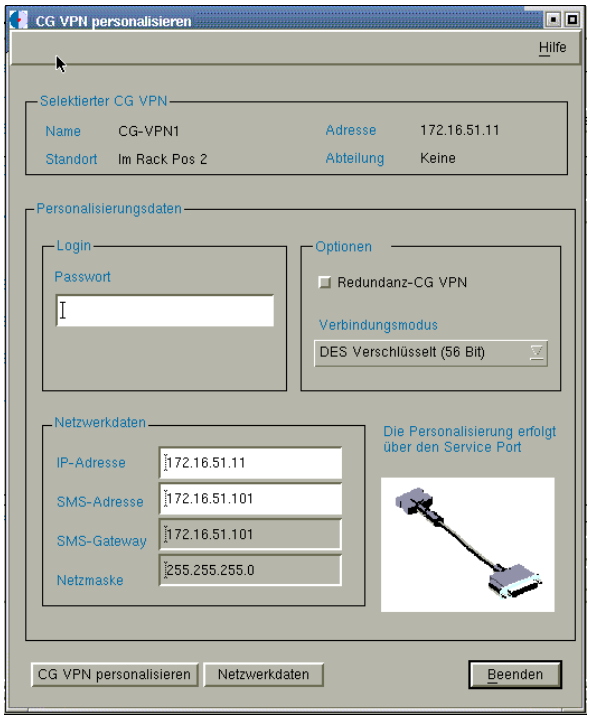
Notizen

Die Personalisierung eines CryptoGuard VPN ist ein initialer Vorgang und wird über den Serviceport des CryptoGuard VPN durchgeführt. Mit der Personalisierung erhält der CryptoGuard VPN seine Netzwerkparameter, den System-Master-Key-Satz sowie Personalisierungsattribute und ist anschließend von der SMS über das Netz ansprechbar. Um einen CryptoGuard VPN zu personalisieren, gehen Sie wie folgt vor.

- Markieren Sie diesen im Fenster ***Gateway-Verwaltung*** und klicken Sie im Menü ***Aktionen*** auf den Menüpunkt ***CG VPN Management***. Es öffnet sich das Fenster ***CG VPN Management***. Klicken Sie dort im Menü ***CG VPN*** auf den Menüpunkt ***CG VPN personalisieren***.



Es öffnet sich das Fenster 'CG VPN personalisieren'.



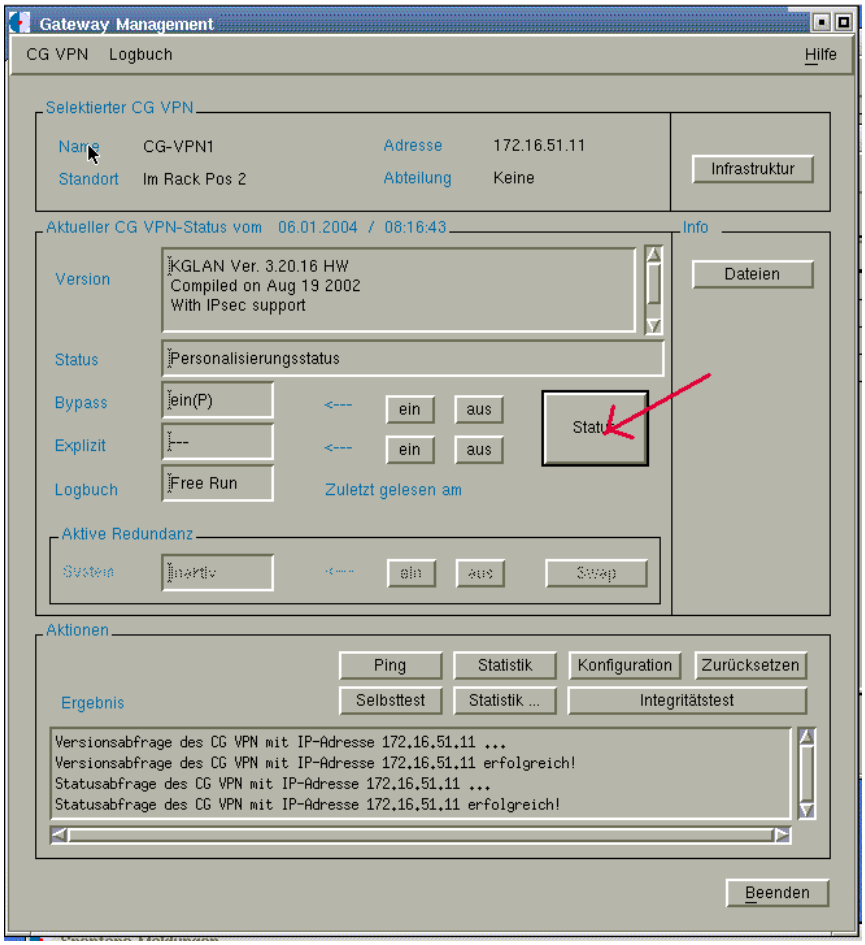
*Hilfe zum Fenster **CG VPN personalisieren** im Anhang A3*

Notizen

- Wählen Sie als Verbindungsmodus ***DES-verschlüsselt (112) Bit)***, geben als Passwort ***smspwd01*** ein und klicken Sie auf den Button ***CG VPN personalisieren***, um den selektierten CryptoGuard VPN zu personalisieren.

Der CryptoGuard VPN erhält hierdurch seine Netzwerkparameter IP-Adresse, Gateway--Adresse, Netzmaske, IP-Adresse der SMS und den System-Master-Key-Satz.

- Mithilfe des Buttons ***Status*** können Sie Informationen über das *CG-VPN1* abfragen.



Sie können erkennen das sich *CG-VPN1* noch im Bypass-Modus befindet. Das heißt der *CG-VPN1* verhält sich wie ein Stück Netzwerkkabel und beeinflusst die Netzwerkkommunikation nicht.

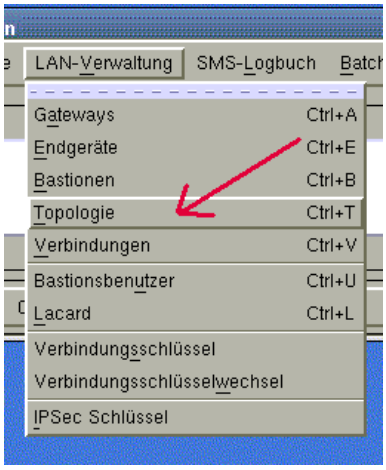
Hilfe zum Bypass Mode und Expizit Modus finden Sie im Anhang A4

2.6 Topologie verwalten

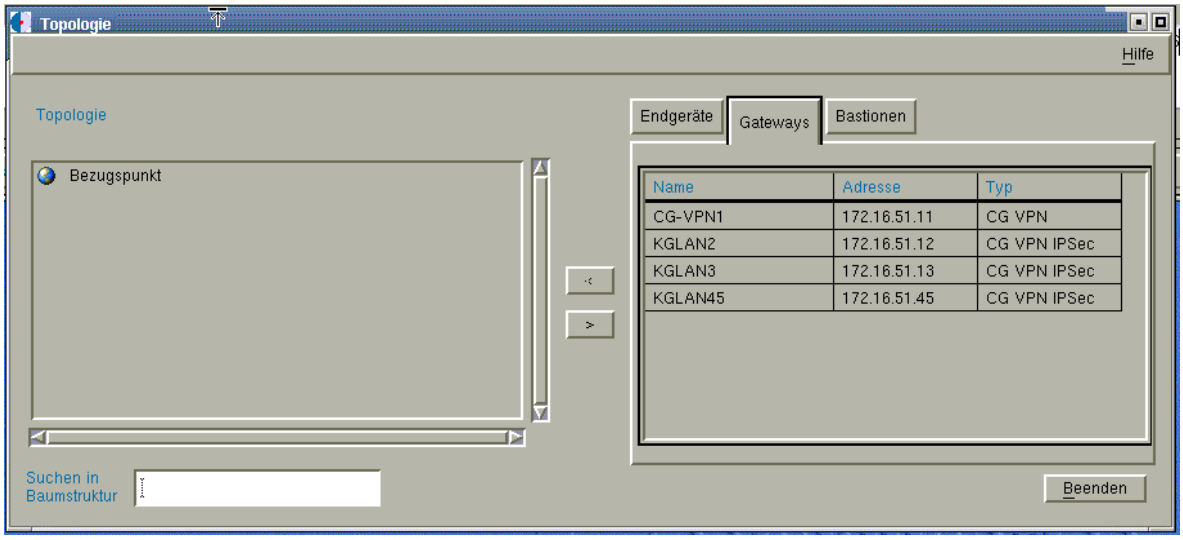
Notizen

Im Topologiefenster wird die real vorhandene Netzstruktur grafisch abgebildet und damit der SMS bekannt gemacht.

- Klicken Sie im SMS-Hauptfenster im Menü ***LAN-Verwaltung*** auf den Menüpunkt ***Topologie***.



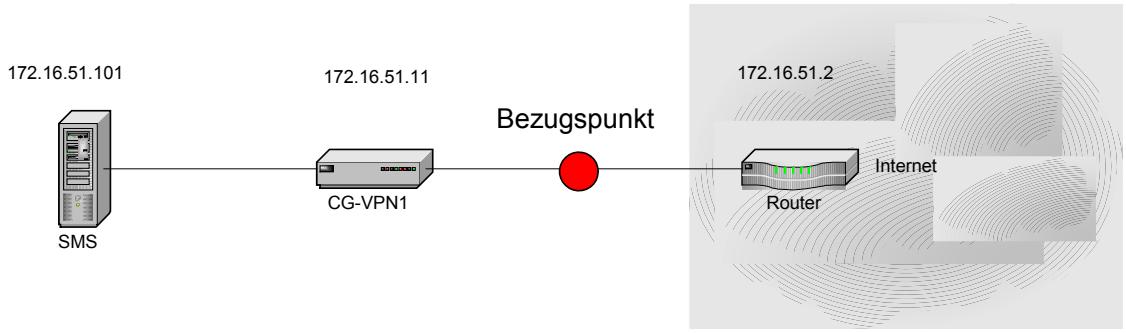
Es öffnet sich das Topologiefenster.



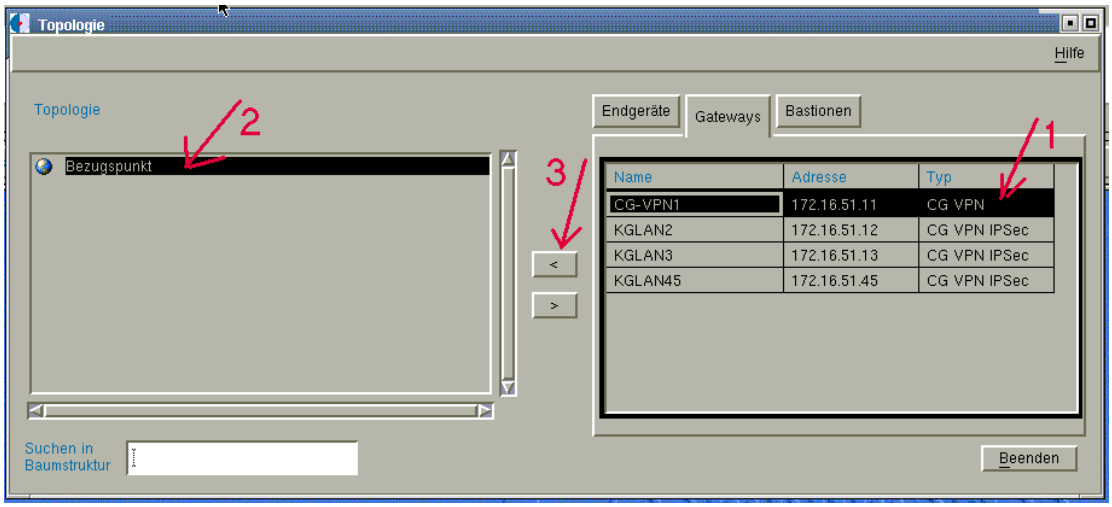
Hilfe zum Fenster Topologie finden Sie im Anhang A5

CG-VPN1 und die SMS zur Topologie hinzufügen

Damit sie die Realwelt in der Topologie der SMS abbilden können müssen Sie einen Bezugspunkt wählen. Von diesen Bezugspunkt ausgehend beschreiben Sie, wie die einzelnen Endgeräte, Gateways und Bastionen miteinander verbunden sind. Wählen Sie als Bezugspunkt die Verbindung zwischen CG-VPN1 und dem Internet.

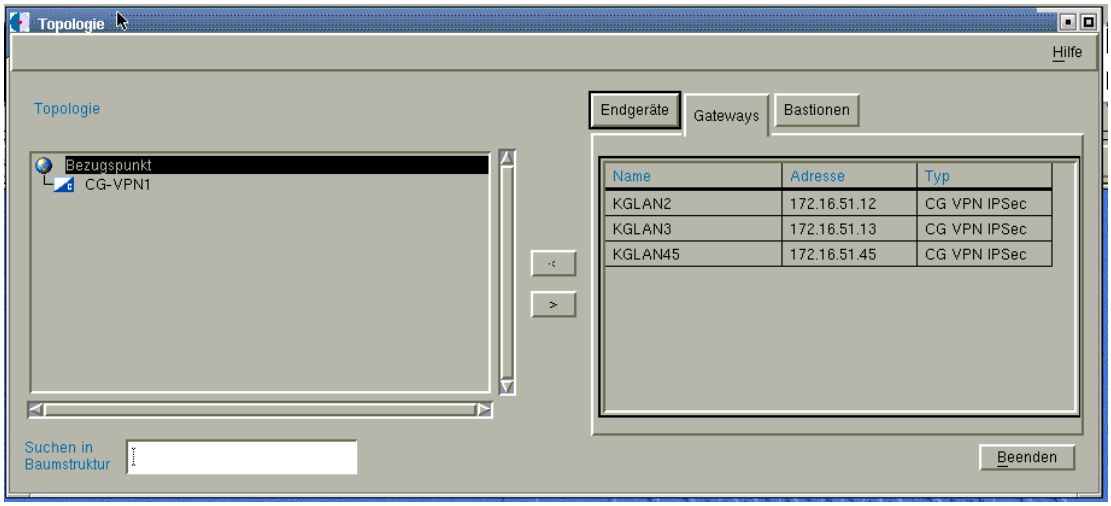


- Wählen Sie den Register Gateways aus und markieren Sie den Eintrag *CG-VPN1* **(1)**
- In der Topologie wählen Sie den Bezugspunkt aus. **(2)**
- Mit dem Button **<** verschieben Sie *CG-VPN1* in die Topologie **(3)**



Der CG-VPN1 wird anschließend in der Topologie angezeigt.

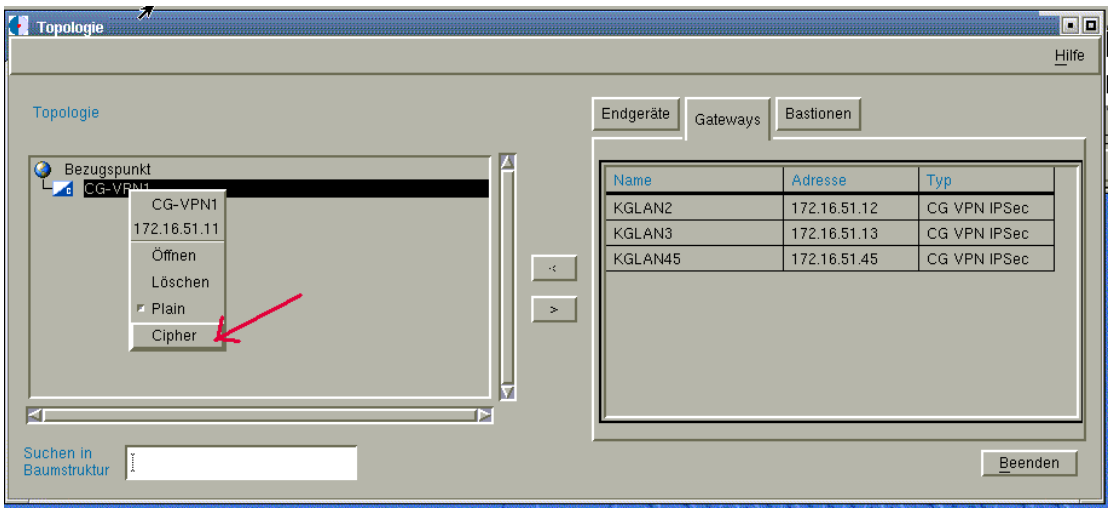
Notizen



Man kann anhand des Icons erkennen, wohin Cipher (verschlüsselt) und Plain des *CG-VPN1* zeigen. Im Augenblick zeigt die Plain Seite zum Bezugspunkt. Sie haben aber die Plainseite physikalisch mit der SMS verbunden und nicht mit dem Bezugspunkt. Daher müssen Sie das Icon umdrehen.

- Markieren Sie hierzu *CG-VPN1* mit der linken Maustaste und öffnen Sie mit der rechten Maustaste das Menü. Dort wählen Sie den Menüpunkt Cipher aus.

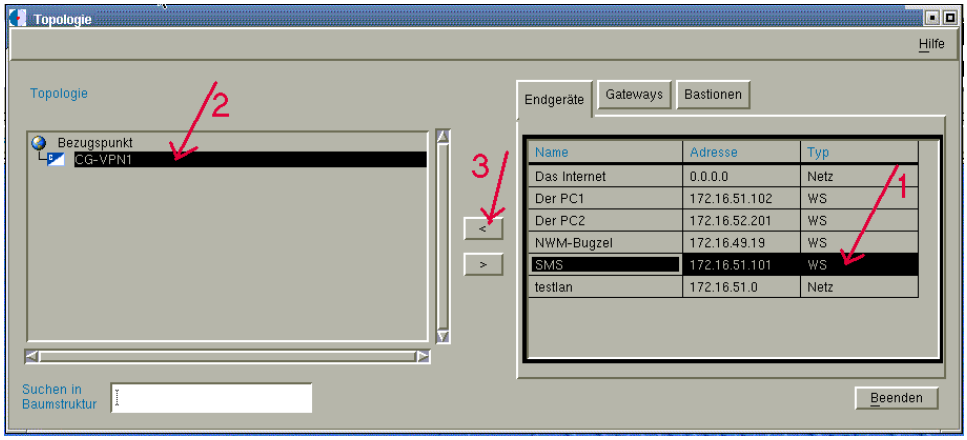
Jetzt wird das Icon von CG-VPN1 umgedreht und entspricht jetzt der Realwelt.



SMS zur Topologie hinzufügen

- Wählen sie den Register Endgeräte aus und markieren Sie den Eintrag SMS **(1)**
- Markieren Sie in der Topologie den CG-VPN1 **(2)**
- Mit den Button „<“ fügen Sie den CG-VPN1 in die Topologie ein **(3)**

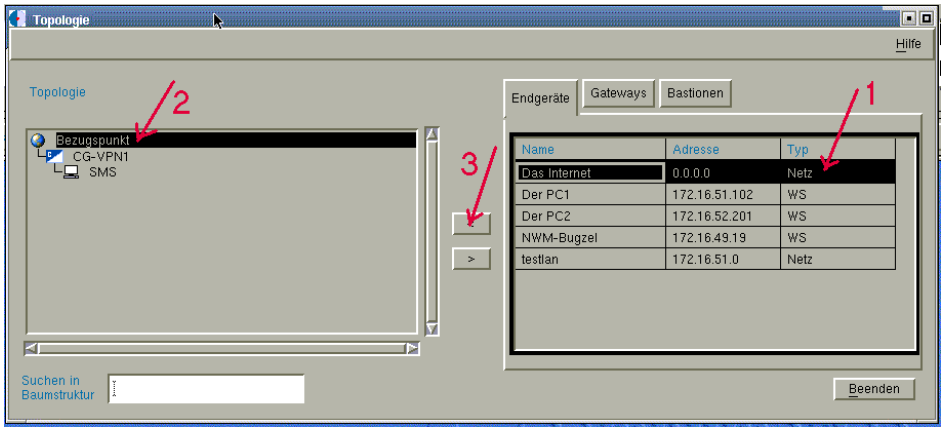
Notizen



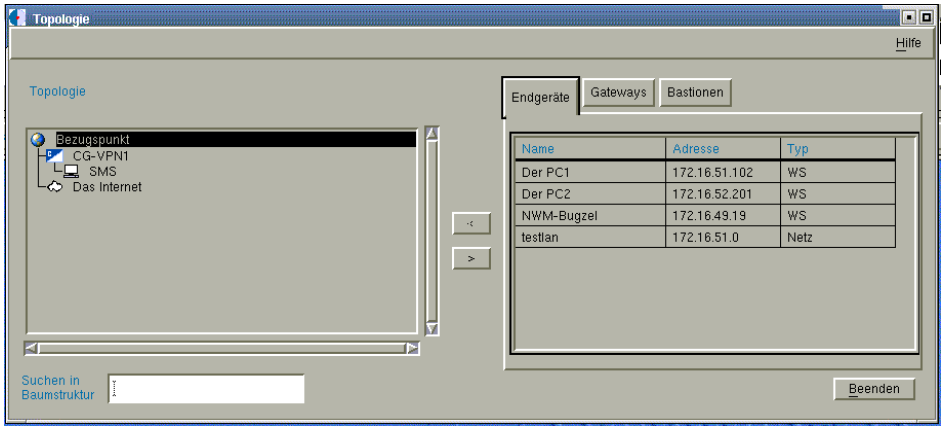
Die SMS wird nicht sofort in der Topologie angezeigt. Erst wenn sie auf das Icon des CG-VPN1 klicken wird die SMS angezeigt.

Internet zur Topologie hinzufügen

- Wählen Sie im Register Endgeräte den Eintrag Internet aus **(1)**
- Markieren Sie in der Topologie den Bezugspunkt **(2)**
- Mit den Button **<** fügen Sie das Internet in die Topologie ein **(3)**



Das Internet wird anschließend in der Topologie angezeigt



- Schließen Sie das Fenster *Topologie*

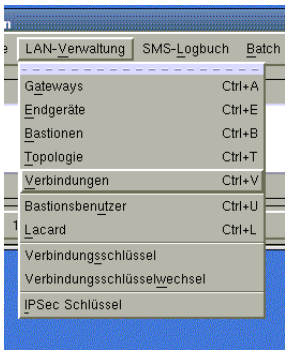
Notizen

2.7 Eine Verbindung erstellen

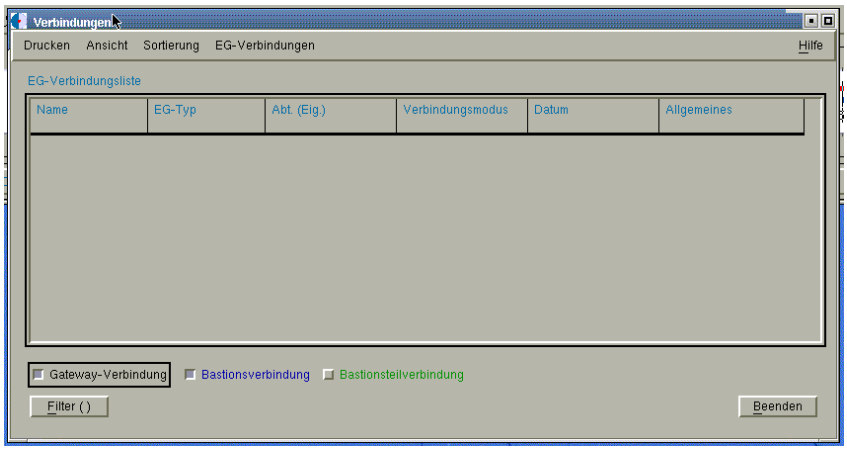
Notizen

Nachfolgend wird Ihnen gezeigt wie Sie eine Verbindung definieren die es der SMS erlaubt DNS- und http-Datenverbindungen in das Internet aufzubauen.

- Klicken Sie im Menü ***LAN-Verwaltung*** auf den Menüpunkt ***Verbindungen***.



Es öffnet sich das Fenster *Verbindungen*. Darin können Sie Endgeräte-Verbindungen einrichten und administrieren.

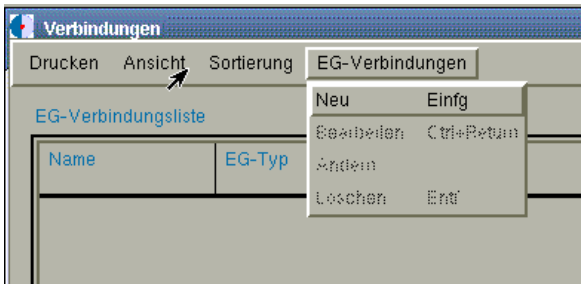


Hilfe zum Fenster EG-Verbindungliste finden Sie im Anhang A6

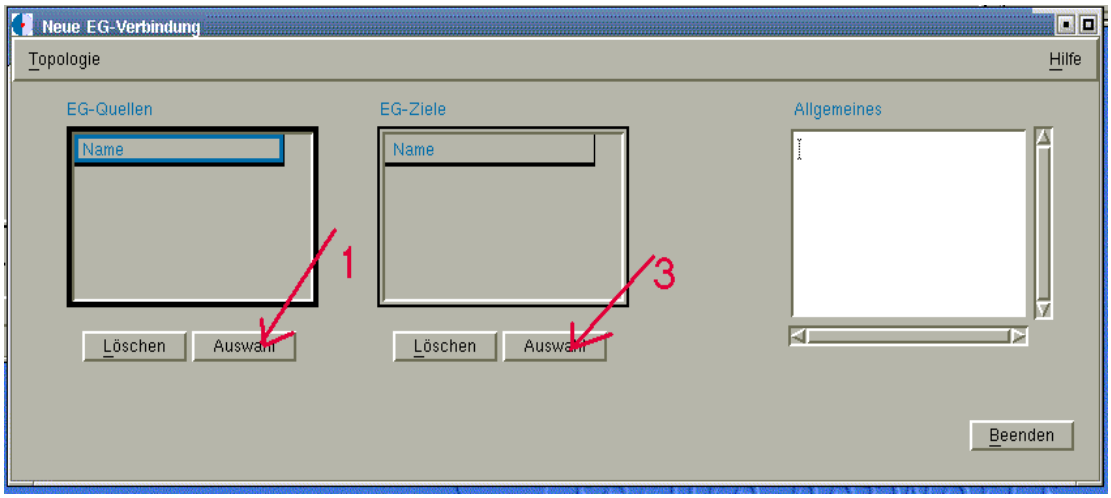
Notizen

Neue Endgeräte-Verbindung anlegen

- Um eine neue Endgeräte-Verbindung anzulegen, klicken Sie im Fenster ***Verbindungen*** im Menü ***EG-Verbindungen*** auf den Menüpunkt ***Neu***.



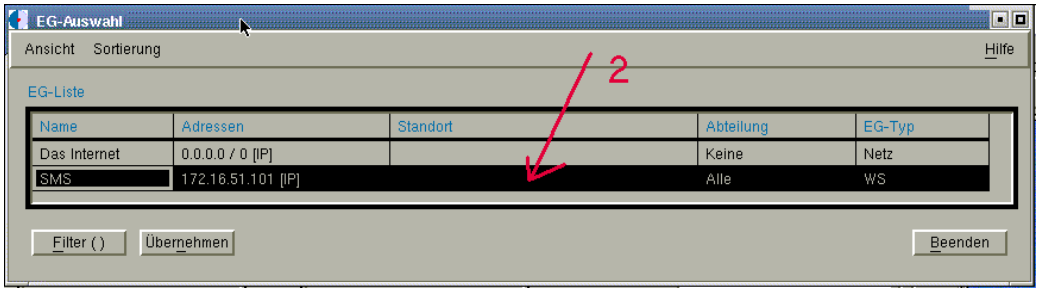
Es öffnet sich das Fenster ***Neue EG-Verbindung***.



Dieses Fenster verändert seinen Aufbau während des Bedienablaufs, abhängig von der Verbindungsart. Sie können Bastionsverbindungen oder Gateway-Verbindungen einrichten. Im ersten Schritt wählen Sie die zu verbindenden Endgeräte aus, danach legen Sie das zugehörige Dienst- oder Protokollprofil fest.

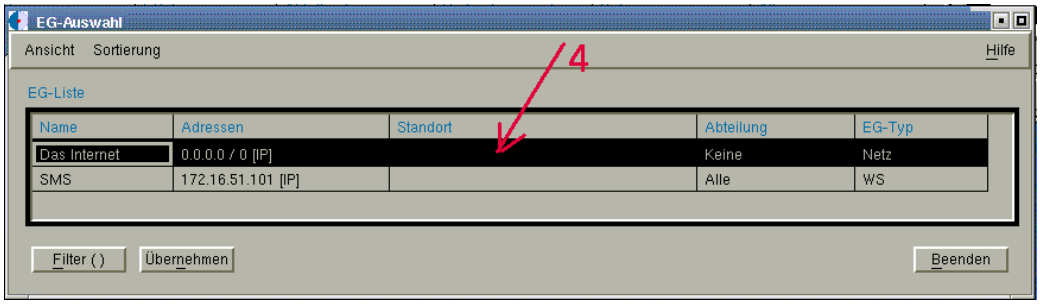
Hilfe zum Fenster Neue EG-Verbindung finden Sie im Anhang A7

- Betätigen Sie den Button *Auswahl* der EG-Quellen . Es öffnet sich das Fenster *EG-Auswahl* (1)

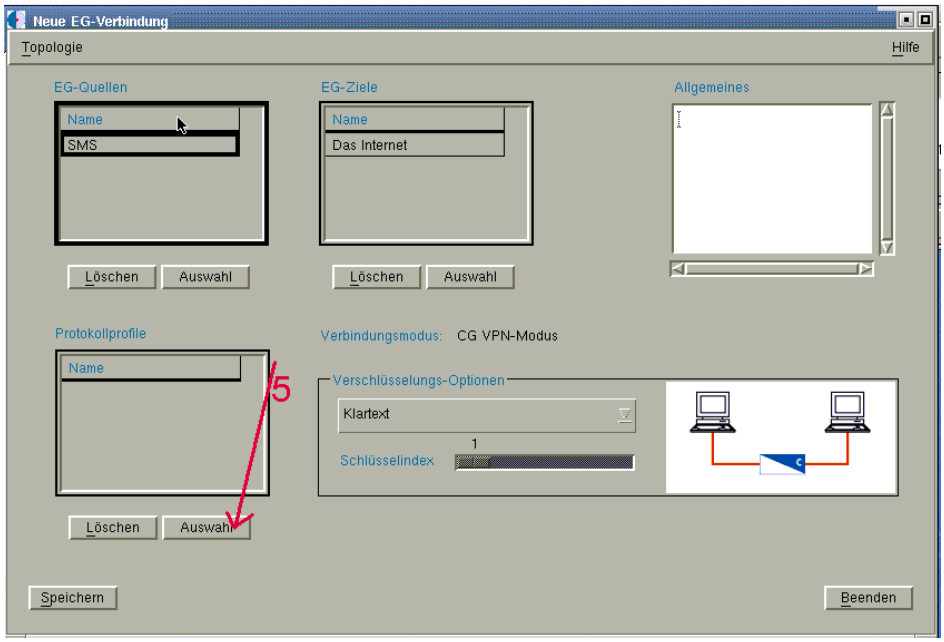


- Markieren Sie den Eintrag ***SMS*** und schließen Sie das Fenster indem Sie den Button ***Übernehmen*** betätigen **(2)**
- Betätigen Sie den Button ***Auswahl*** der EG-Ziele . Es öffnet sich das Fenster ***EG-Auswahl*** **(3)**

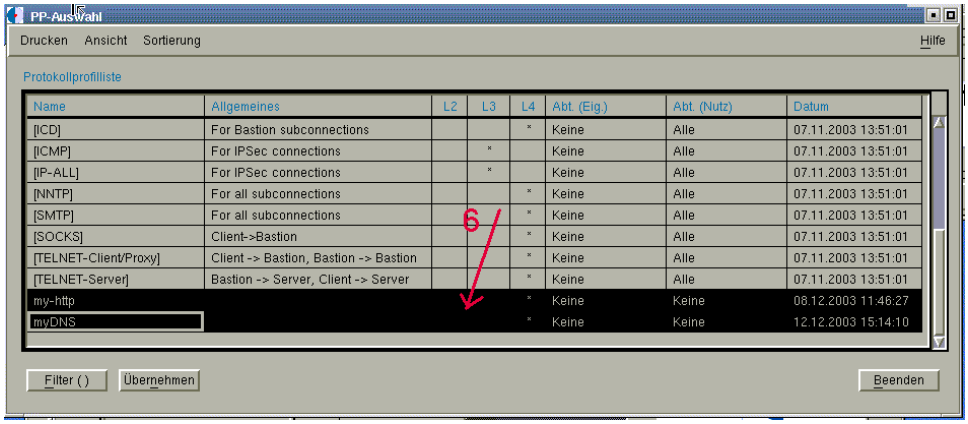
- Markieren Sie den Eintrag ***Das Internet*** und schließen Sie das Fenster indem Sie den Button ***Übernehmen*** betätigen **(4)**



- Betätigen Sie den Button ***Auswahl*** der Protokollprofile. Es öffnet sich das Fenster ***EG-Auswahl*** **(5)**



- Markieren Sie die Einträge ***my-http*** und ***myDNS*** und schließen Sie das Fenster indem Sie den Button ***Übernehmen*** betätigen **(6)**

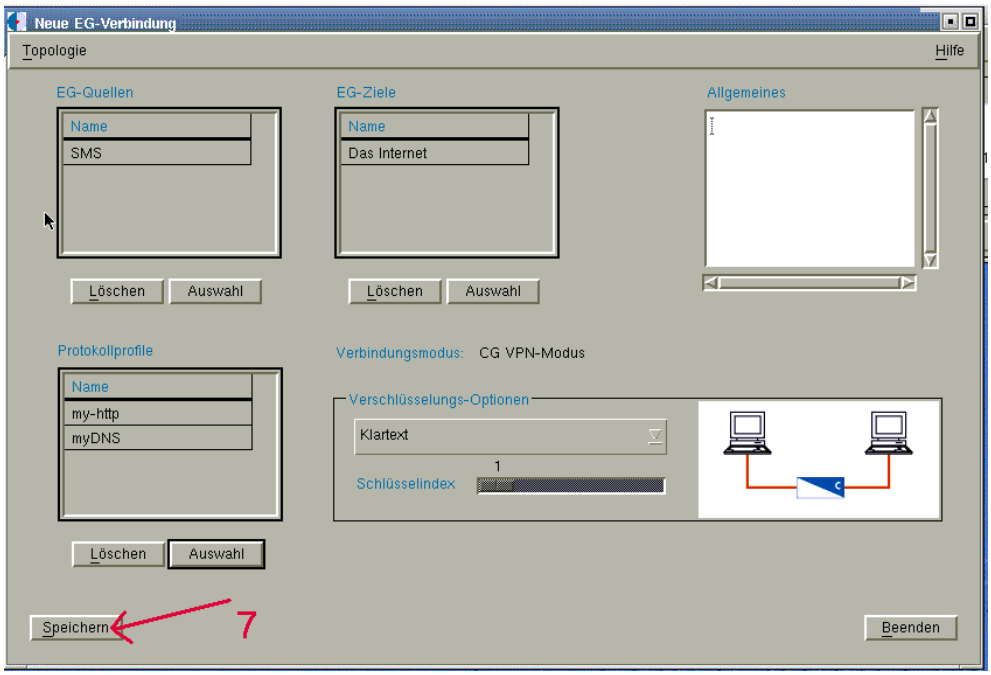


Eine Verschlüsselung kann nicht genutzt werden da bei dieser Verbindung nur ein CG-VPN verwendet wird. Es werden bei den „Verschlüsselungs-Optionen“ die Einträge „Klartext“ und „Geblockt“ angeboten. Wenn Sie anstatt „Klartext“ den Eintrag „Geblockt“

Notizen

verwenden, würden DNS- und http-Verbindungen unterdrückt werden und alle anderen Verbindungen würden im „Expliziet-Off“ Modus erlaubt sein.

Notizen



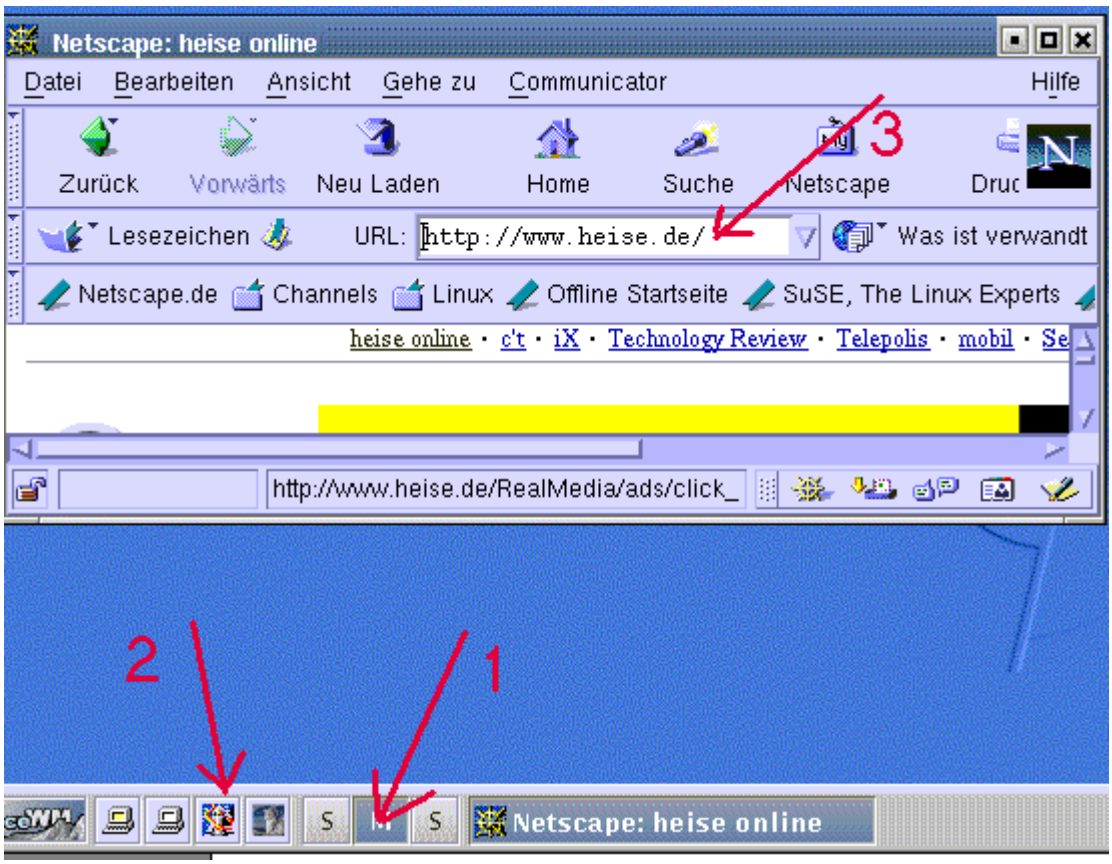
- Das Fenster ***EG-Verbindungen*** schließen Sie indem Sie den Button ***Speichern*** betätigen **(7)**

2.8 Konfiguration übertragen

Die Verbindung die Sie definiert haben muss jetzt zum *CG-VPN1* übertragen werden. Vorher sollten Sie überprüfen das bis jetzt jede Kommunikation, von der SMS in das Internet möglich ist.

Notizen

Kommunikation testen



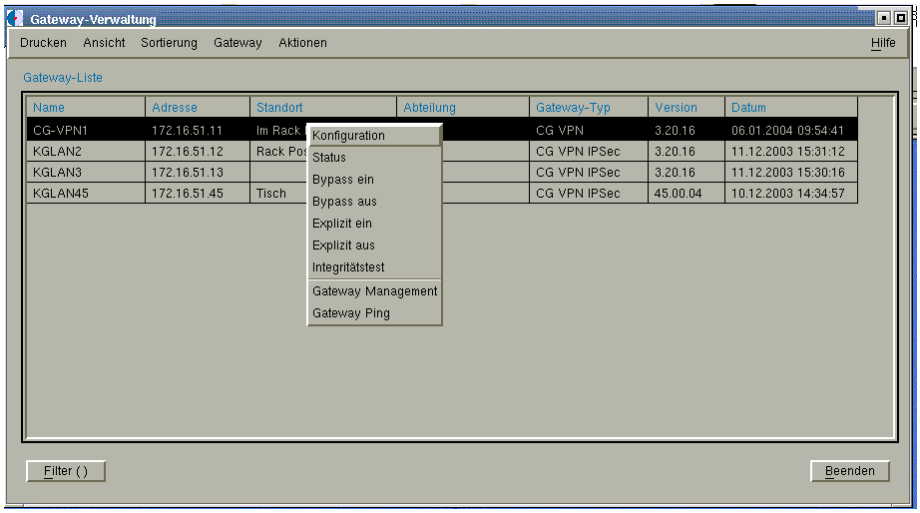
- Wählen Sie hierzu in eine andere Arbeitsfläche **(1)**
- Starten Sie den Netscape-Browser **(2)**
- Rufen Sie z.B. die Seite **http://www.heise.de** . Hierdurch sehen Sie das zurzeit DNS- und HTTP-Datenverbindungen möglich sind. **(3)**
- Rufen Sie z.B. die Seite **https://www.gmx.de** auf. Hierdurch sehen Sie das zurzeit auch HTTPS-Datenverbindungen möglich sind. Nach der Übertragung der Verbindung (Konfiguration) zum *CG-VPN1* darf diese Kommunikation nicht mehr möglich sein.

Notizen

Konfiguration übertragen

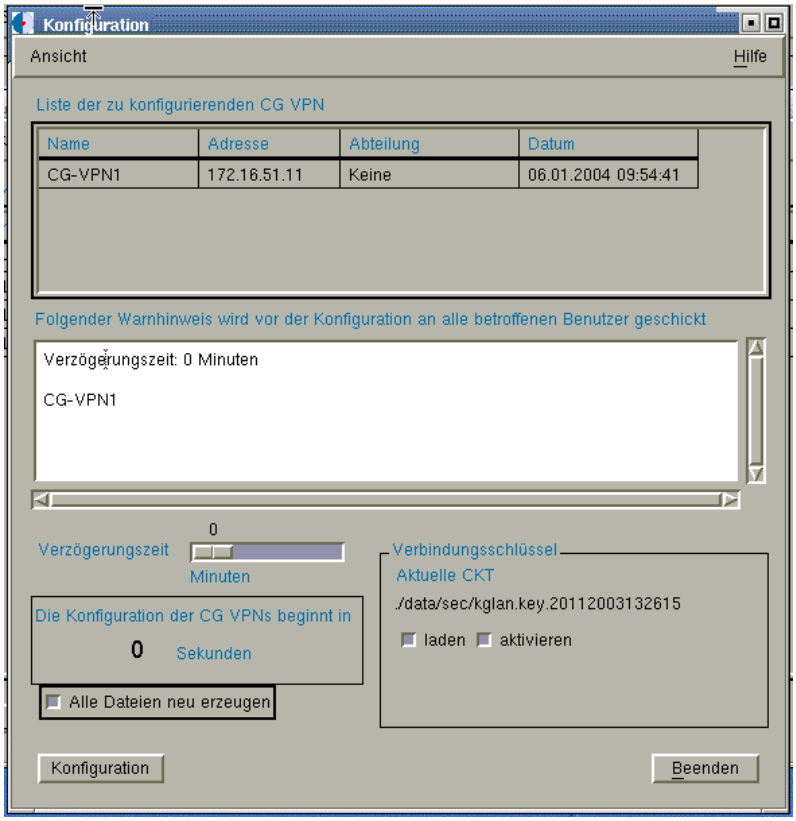
- Klicken Sie im Menü ***LAN-Verwaltung*** auf den Menüpunkt ***Gateways***.

Es öffnet sich das Fenster Gateway-Verwaltung.



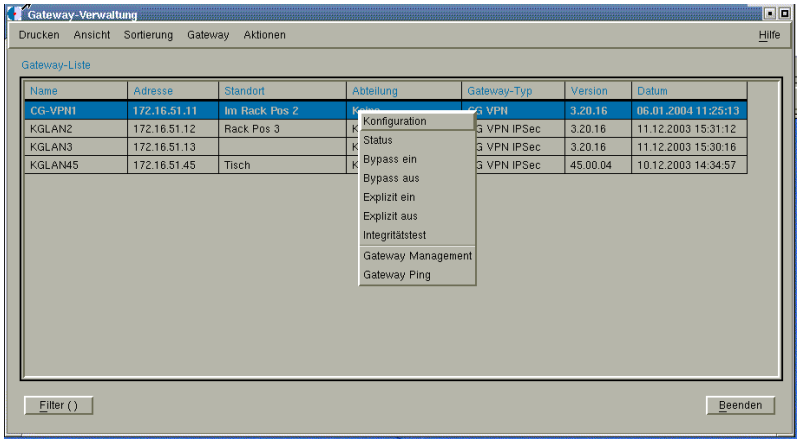
- In diesem Fenster wählen Sie mit der linken Maustaste den Eintrag ***CG-VPN1*** aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet



- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN1* übertragen.

Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den CG-VPN1 in der Gatewayliste blau angezeigt.

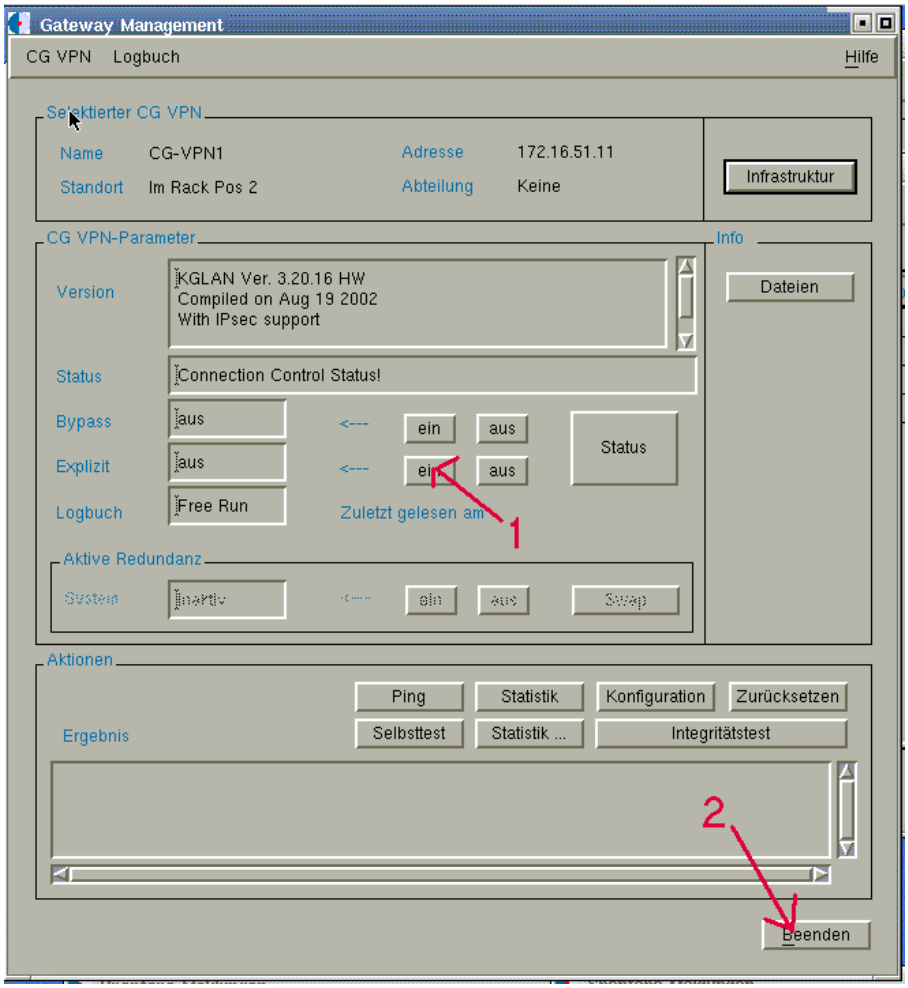


Bis jetzt kann die SMS aber immer noch ohne Einschränkungen mit dem Internet kommunizieren. Das liegt daran das der *CG-VPN1* im Modus ***Expliziet-Off*** arbeitet und alle Datenverbindungen für die keine Verbindung (Regel) definiert wurde im Klartext überträgt und nicht blockt. Darum müssen Sie jetzt noch den CG-VPN1 in den Modus ***Expliziet-ON*** setzen.

- Wählen sie den Eintrag des *CG-VPN1* mit der linken Maustaste aus und öffnen mit der rechten Maustaste das Menü. Dort wählen Sie den Menüpunkt ***Gateway-Management*** aus.

Das Fenster ***Gateway-Management*** wird geöffnet.

Notizen



- Schalten Sie Explizit ein, indem Sie den Button ***ein*** betätigen. **(1)**
- Schließen Sie das Fenster, indem Sie den Button Beenden betätigen. **(2)**

Kommunikation überprüfen

Wenn Sie jetzt mit dem Netscape-Browser versuchen die Seite **https://www.gmx.de** aufzurufen, wir die Datenübertragung vom CG-VPN1 unterbunden. Es ist nur noch DNS- und HTTP-Datenübertragung von der *SMS* in das Internet möglich. Jede andere Datenübertragung wird vom *CG-VPN1* unterdrückt.

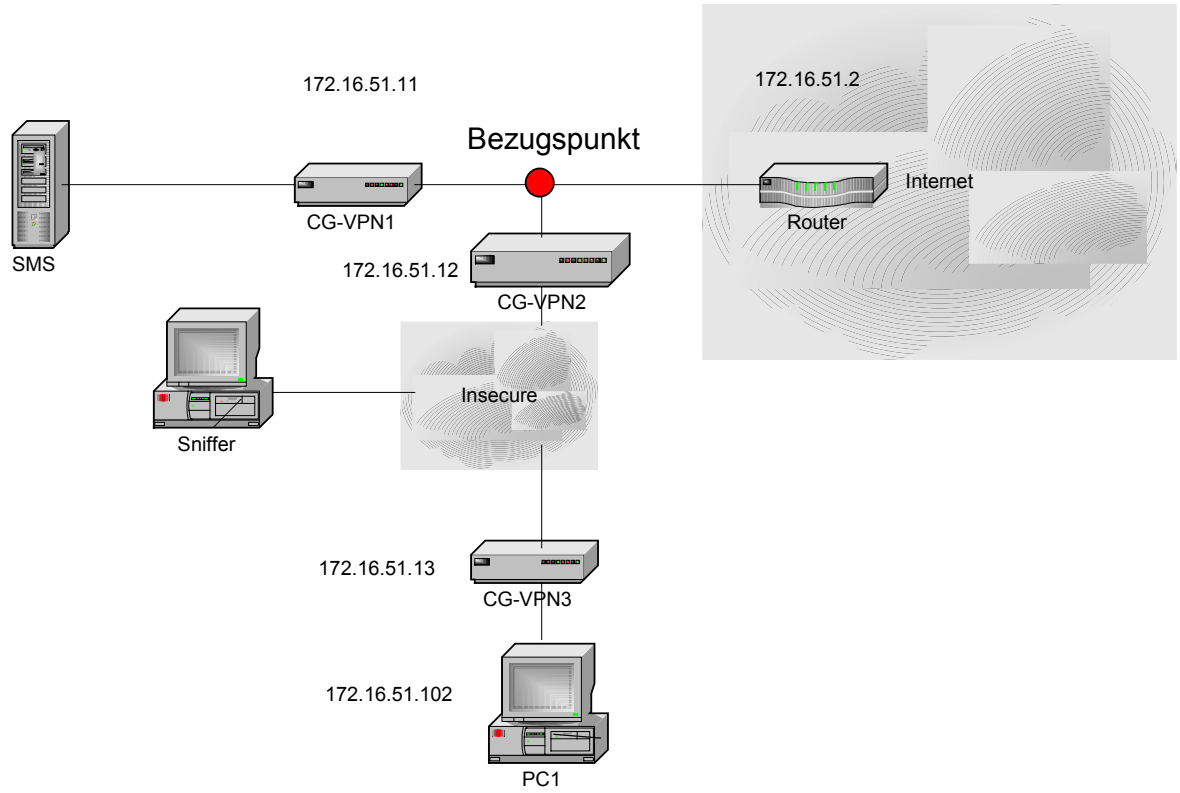
2.8 Fazit

Das Hauptanwendungsgebiet von CG-VPNs ist die Datenverschlüsselung, diese Funktion haben Sie noch nicht eingesetzt. Sie haben aber gelernt das man die Geräte aber auch als Packetfirewall einsetzen kann. Dies kann in bestimmten Einsatzszenarien aber auch eine benötigtes Leistungsmerkmal sein. Sie haben im ersten Szenario gelernt, wie man CG-VPNs in den Auslieferungszustand zurücksetz, sie personalisiert und mit Verbindungsinformationen konfiguriert. Diese Arbeitsschritte benötigen Sie auch in den nachfolgenden Szenarien.

Notizen

Notizen

3 Zweites Szenario



Im zweiten Szenario sollen Sie die Verwaltung von verschlüsselten Datenverbindungen erlernen hierzu verwenden Sie zwei weitere CG-VPNs. Der Sniffer dient zum Protokollmitschnitt.
Im folgenden Howto werden Sie die Verschlüsselungsarten ***KryptoGuard-Mode, IPSec - Main – Mode*** und ***IPSec - Aggressive Mode*** verwenden.
Alle vier Kommunikationen (Klartext, KryptoGuard-Mode, IPSec - Main - Mode und IPSec - Aggressive Mode) sollen mit Ethereal mitgeschnitten werden.

Danach sollen Sie eine Ausarbeitung machen, die folgende Aspekte berücksichtigen soll:

- Auswertung der Aufzeichnungen
  Zeigen Sie den Unterschied zwischen der Klartextkommunikation und der verschlüsselten Kommunikation auf.
- Machen Sie eine Analyse der unterschiedlichen Verschlüsselungsmethoden bezüglich
- Performance (Anzahl der Bytes, die ausgetauscht werden und der Handshakes, usw.)
- Sicherheit
- Diskutieren Sie die Vor- und Nachteile der verschiedenen Modies.

3.1 Vorbereitung

Notizen

- Verbinden Sie die Plain-Netzwerkkarte des CG-VPN2 mit dem Switch1
- Verbinden Sie die Cipher-Netzwerkkarte des CG-VPN2 mit dem Hub1
- Verbinden Sie die Cipher-Netzwerkkarte des CG-VPN3 mit dem Hub1
- Verbinden Sie die Plain-Netzwerkkarte des CG-VPN3 mit dem PC1
  Verwenden Sie hierzu ein Crosslink Kabel
- Verbinden Sie den Sniffer-PC mit dem Hub1
- Schalten Sie den Sniffer-PC ein
- Schalten Sie den PC1 ein

3.2 Administration von CG-VPN2

- Verbinden Sie COM1 der SMS mit dem Serviceport von CG-VPN2.
  Verwenden Sie hierzu das Nullmodemkabel

Den CG-VPN2 zurücksetzen.

- Um das Terminalprogramm aufzurufen, klicken Sie im Menü ***System*** auf ***Shell***.

Eine UNIX-Shell öffnet sich.

- Tippen Sie den Befehl ***service*** ein. Der Login-Name lautet **service**, das standardmäßige Passwort **serpwd01**.

- Setzen Sie den CG-VPN zurück indem Sie den ***Punkt 8*** auswählen und die anschließende Frage mit ***y*** beantworten.

- Jetzt müssen Sie die Option ***D*** auswählen damit der CG-VPN2 neu gestartet wird.

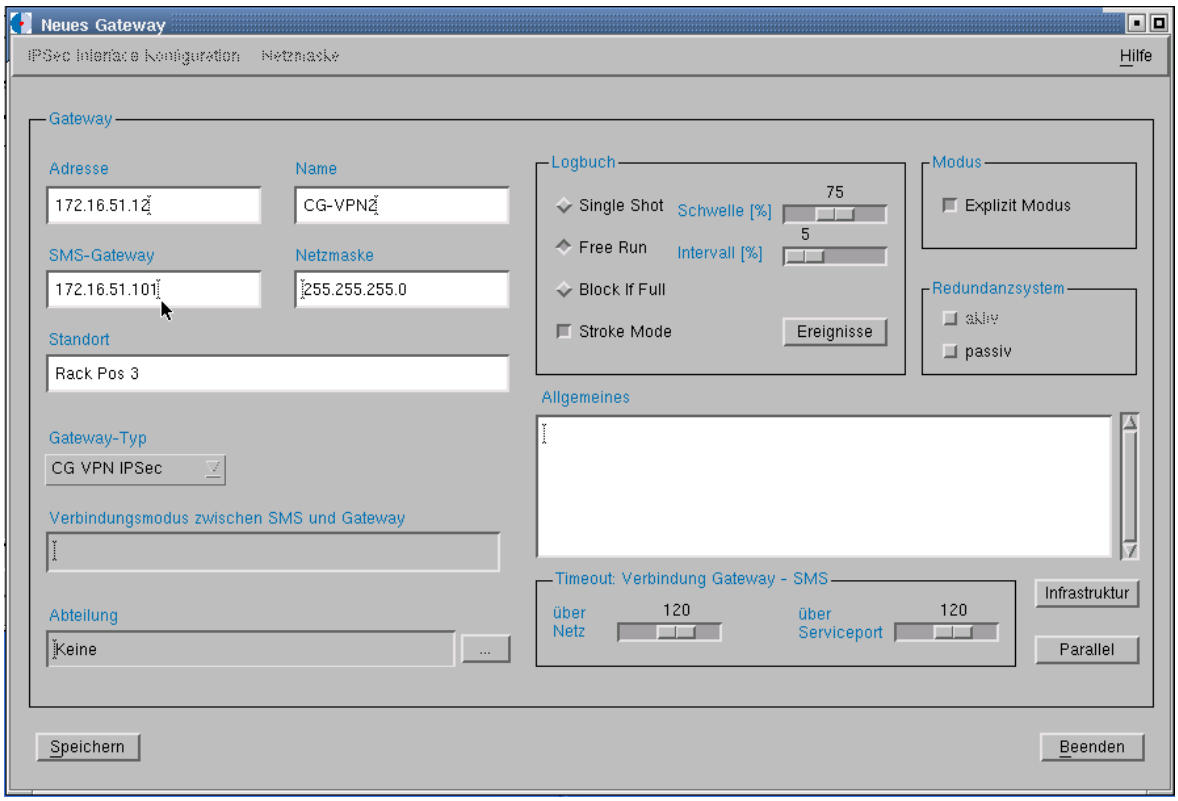
- Sie beenden das Terminalprogramm mit der Tastenkombination ***Ctrl+C*** und dem Befehl ***exit***

CG-VPN2 zum SMS-System hinzufügen.

- Um ein neues Gateway zur Datenbank der SMS hinzuzufügen, klicken Sie das Menu ***LAN-Verwaltung*** an und wählen Sie den Menüpunkt ***Gateways*** aus.

- Klicken Sie im Menü ***Gateway*** auf den Menüpunkt ***Neu***. Es öffnet sich das Fenster ***Neues Gateway***.

- Füllen Sie die Eingabemaske, wie folgt aus.
  Adresse: 172.16.51.12
  Name: CG-VPN2
  SMS-Gateway: 172.16.51.101
  Netzmaske 255.255.255.0
  Standort: Im Rack Pos 3
  Explizit Modus: on



- Schließen Sie das Fenster ***Neues Gateway, indem Sie den Button Speichern betätigen***

CG-VPN2 personalisieren

- Markieren Sie den Eintrag ***CG-VPN2*** im Fenster ***Gateway-Verwaltung*** und klicken Sie im Menü ***Aktionen*** auf den Menüpunkt ***Gateway Management***.

Es öffnet sich das Fenster ***Gateway Management***.

- Klicken Sie dort im Menü ***CG VPN*** auf den Menüpunkt ***CG VPN personalisieren***.

- Wählen Sie als Verbindungsmodus ***DES-verschlüsselt (112) Bit)***, geben als Passwort ***smspwd01*** ein und klicken Sie auf den Button ***CG VPN personalisieren***, um den selektierten CryptoGuard VPN zu personalisieren.

Der CryptoGuard VPN erhält hierdurch seine Netzwerkparameter IP-Adresse, Gatewayadresse, Netzmaske, IP-Adresse der SMS und den System-Master-Key-Satz.

Notizen

3.3 Administration von CG-VPN3

Notizen

- Verbinden Sie COM1 der SMS mit dem Serviceport von CG-VPN3.
  Verwenden Sie hierzu das Nullmodemkabel

Den CG-VPN3 zurücksetzen.

- Um das Terminalprogramm aufzurufen, klicken Sie im Menü ***System*** auf ***Shell***.

Eine UNIX-Shell öffnet sich.

- Tippen Sie den Befehl ***service*** ein. Der Login-Name lautet **service**, das standardmäßige Passwort **serpwd01**.

- Setzen Sie den CG-VPN3 zurück indem Sie den ***Punkt 8*** auswählen und die anschließende Frage mit ***y*** beantworten.

- Jetzt müssen Sie die Option ***D*** auswählen damit der *CG-VPN3* neu gestartet wird.

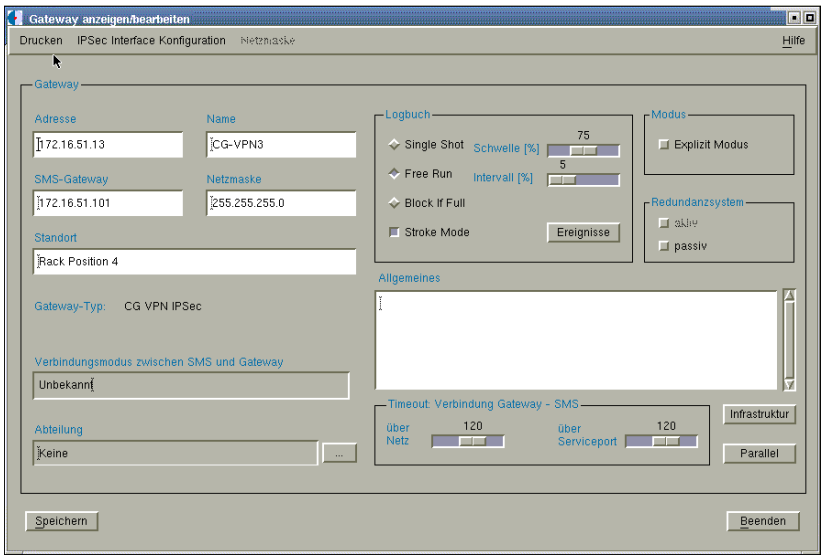
- Sie beenden das Terminalprogramm mit der Tastenkombination ***Ctrl+C*** und dem Befehl ***exit***

CG-VPN3 zum SMS-System hinzufügen.

- Um ein neues Gateway zur Datenbank der *SMS* hinzuzufügen, klicken Sie das Menu ***LAN-Verwaltung*** an und wählen Sie den Menüpunkt ***Gateways*** aus.

- Klicken Sie im Menü ***Gateway*** auf den Menüpunkt ***Neu***. Es öffnet sich das Fenster ***Neues Gateway***.

- Füllen Sie die Eingabemaske wie folgt aus.
  Adresse: 172.16.51.13
  Name: CG-VPN3
  SMS-Gateway: 172.16.51.101
  Netzmaske 255.255.255.0
  Standort: Im Rack Pos 4
  Explizit Modus: on



Notizen

- Schließen Sie das Fenster ***Neues Gateway, indem Sie den Button Speichern betätigen***

CG-VPN3 personalisieren

- Markieren Sie den Eintrag ***CG-VPN2*** im Fenster ***Gateway-Verwaltung*** und klicken Sie im Menü ***Aktionen*** auf den Menüpunkt ***Gateway Management***. Es öffnet sich das Fenster ***Gateway Management***. Klicken Sie dort im Menü ***CG VPN*** auf den Menüpunkt ***CG VPN personalisieren***.

- Wählen Sie als Verbindungsmodus ***DES-verschlüsselt (112) Bit)***, geben als Passwort ***smspwd01*** ein und klicken Sie auf den Button ***CG VPN personalisieren***, um den selektierten CryptoGuard VPN zu personalisieren.

Der CryptoGuard VPN erhält hierdurch seine Netzwerkparameter IP-Adresse, Gatewayadresse, Netzmaske, IP-Adresse der SMS und den System-Master-Key-Satz.

Notizen

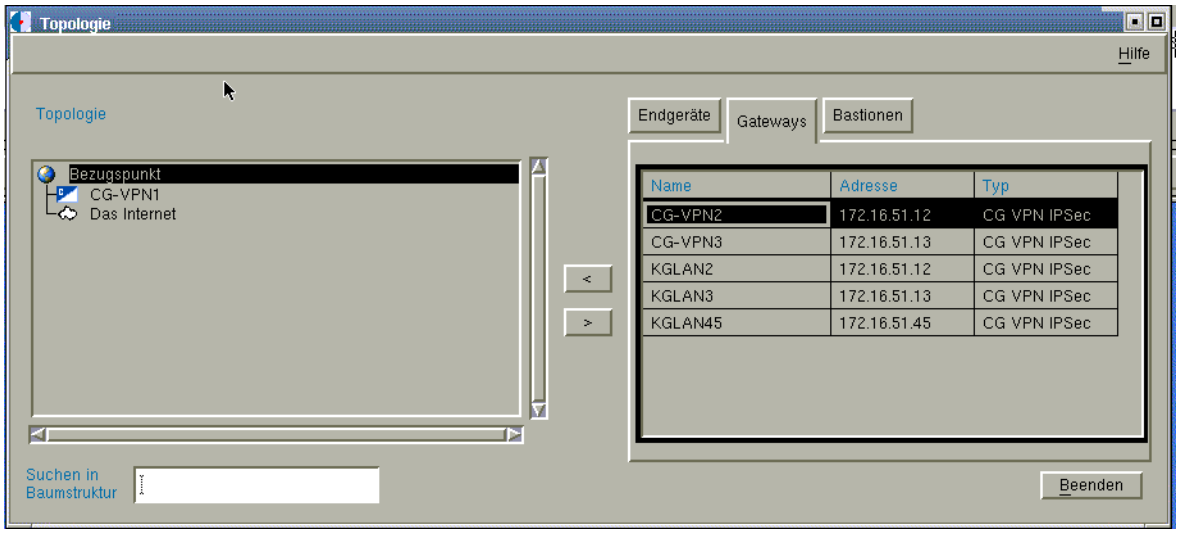
CG-VPN2, CG-VPN3 und PC1 zur Topologie hinzufügen

- Klicken Sie im SMS-Hauptfenster im Menü ***LAN-Verwaltung*** auf den Menüpunkt ***Topologie***.

Es öffnet sich das Topologiefenster.

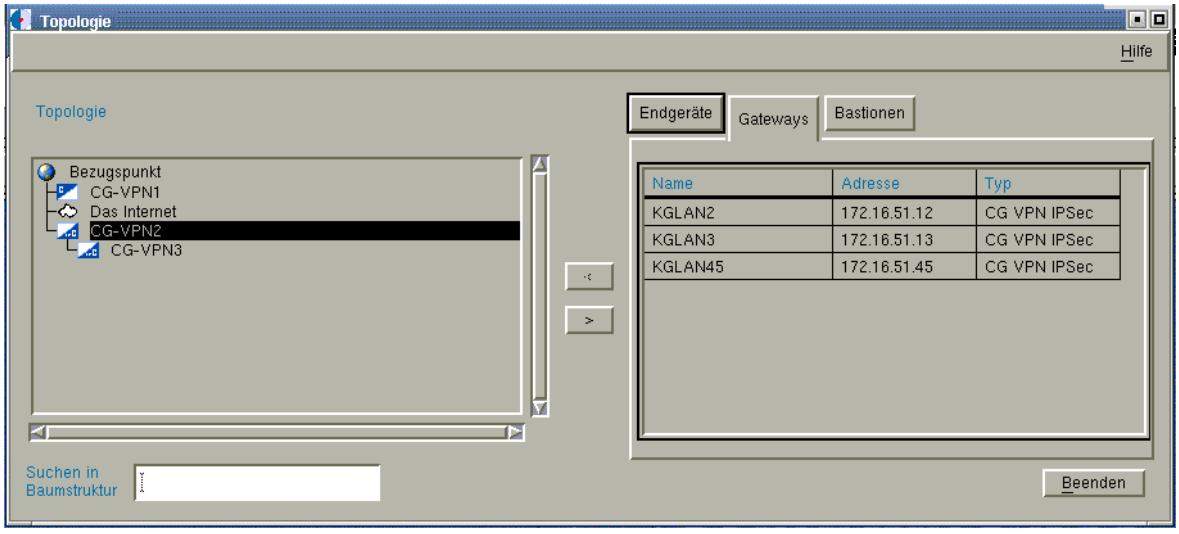
- Wählen Sie den ***Register Gateways*** aus und markieren Sie den Eintrag ***CG-VPN2***
- In der Topologie wählen Sie den Bezugspunkt aus.
- Mit dem Button **<** verschieben Sie ***CG-VPN2*** in die Topologie

Der CG-VPN1 wird anschließend in der Topologie angezeigt.



- Wählen Sie den ***Register Gateways*** aus und markieren Sie den Eintrag ***CG-VPN3***
- In der Topologie wählen Sie ***CG-VPN2*** aus.
- Mit dem Button **<** verschieben Sie ***CG-VPN3*** in die Topologie

Der CG-VPN3 wird nicht sofort in der Topologie angezeigt. Erst wenn sie auf das Icon des CG-VPN2 klicken wird der CG-VPN3 angezeigt



Notizen

Man kann anhand des Icons erkennen, wohin Cipher (verschlüsselt) und Plain des CG-VPN3 zeigen. Im Augenblick zeigt die Plain Seite zum CG-VPN2. Sie haben aber die Cipherseite physikalisch mit dem CG-VPN2 verbunden. Daher müssen Sie das Icon umdrehen.

- Markieren Sie hierzu *CG-VPN3* mit der linken Maustaste und öffnen Sie mit der rechten Maustaste das Menü. Dort wählen Sie den Menüpunkt ***Cipher*** aus. Jetzt wird das Icon von *CG-VPN3* umgedreht und entspricht jetzt der Realwelt.

- Wählen Sie den Register ***Endgeräte*** aus und markieren Sie den Eintrag *PC1*
- In der Topologie wählen Sie *CG-VPN3* aus.
- Mit dem Button **<** verschieben Sie *PC1* in die Topologie

Der PC1 wird nicht sofort in der Topologie angezeigt. Erst wenn sie auf das Icon des CG-VPN3 klicken wird der PC1 angezeigt

Notizen

Eine Verbindung vom PC1 in das Internet erstellen

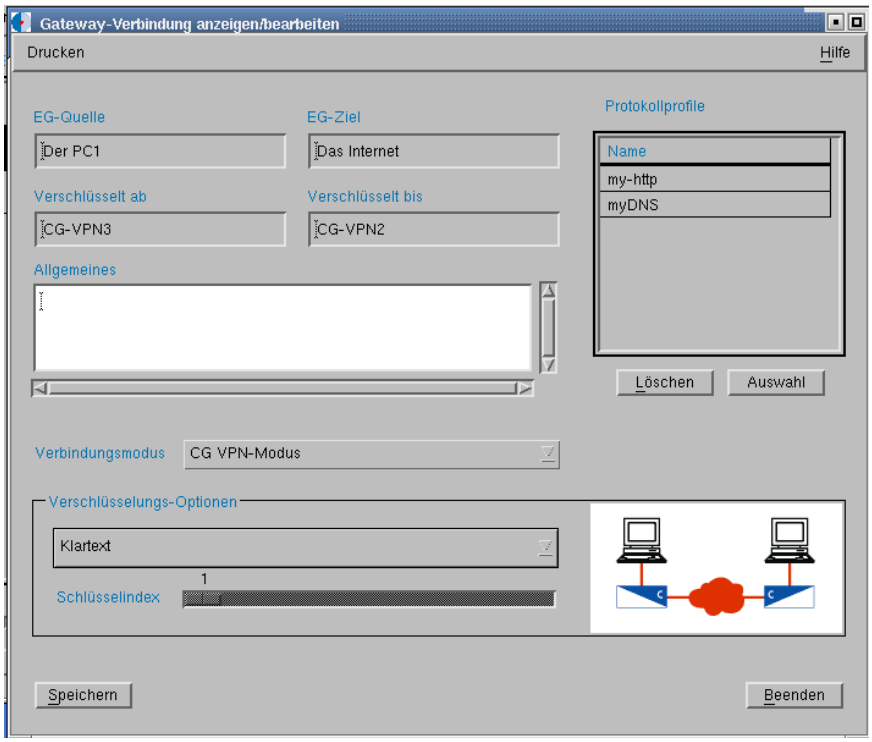
- Klicken Sie im Menü ***LAN-Verwaltung*** auf den Menüpunkt ***Verbindungen***.

Es öffnet sich das Fenster ***Verbindungen***. Darin können Sie Endgeräte-Verbindungen einrichten und administrieren.

- Um eine neue Endgeräte-Verbindung anzulegen, klicken Sie im Fenster ***Verbindungen*** im Menü ***EG-Verbindungen*** auf den Menüpunkt ***Neu***.

Es öffnet sich das Fenster ***Neue EG-Verbindung***.

- Betätigen Sie den Button ***Auswahl*** der EG-Quellen . Es öffnet sich das Fenster ***EG-Auswahl***
- Markieren Sie den Eintrag *PC1* und schließen Sie das Fenster, indem Sie den Button Übernehmen betätigen
- Betätigen Sie den Button ***Auswahl*** der EG-Ziele . Es öffnet sich das Fenster ***EG-Auswahl***
- Markieren Sie den Eintrag ***Das Internet*** und schließen Sie das Fenster, indem Sie den Button Übernehmen betätigen
- Betätigen Sie den Button ***Auswahl*** der Protokollprofile. Es öffnet sich das Fenster ***PP-Auswahl***
- Markieren Sie die Einträge ***my-http*** und ***myDNS*** und schließen Sie das Fenster, indem Sie den Button Übernehmen betätigen
- Wählen Sie als Verschlüsselungs-Option ***Klartext***



- Das Fenster ***EG-Verbindungen*** schließen Sie, indem Sie den Button Speichern betätigen

Notizen

Konfiguration Übertragen

- Wählen Sie im SMS Hauptfenster im Menü ***LAN-Verwaltung*** den Menüpunkt ***Gateways*** aus

Es öffnet sich das Fenster Gateway-Verwaltung.

- In diesem Fenster wählen Sie mit der linken Maustaste den Eintrag *CG-VPN3* aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet

- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN3* übertragen.

Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den *CG-VPN3* in der Gatewayliste blau angezeigt.

- Wählen Sie jetzt den Eintrag *CG-VPN2* aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet

- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN2* übertragen.

Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den *CG-VPN2* in der Gatewayliste blau angezeigt.

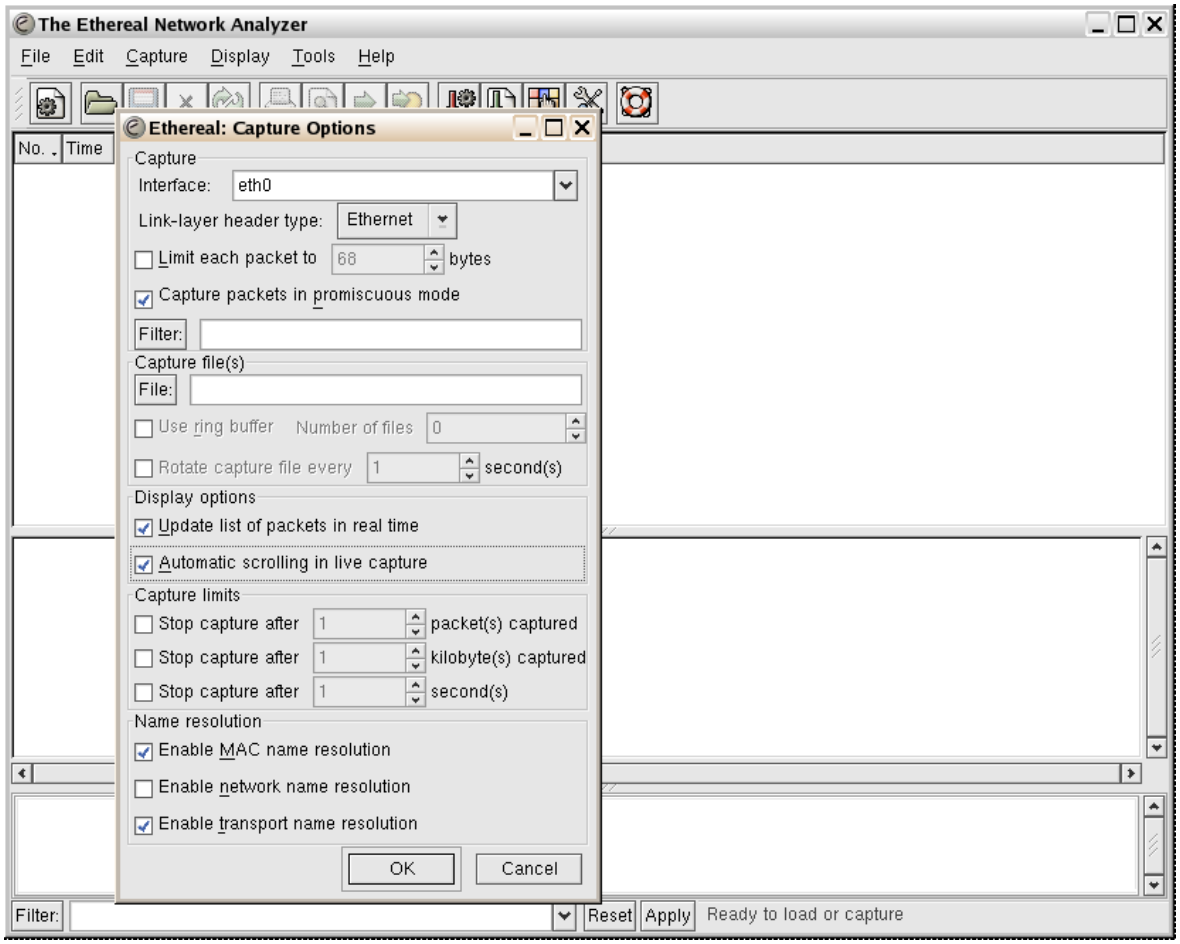
Klartextkommunikation testen und mitschneiden

PC1 vorbereiten

- Loggen Sie sich auf dem PC1 als User **root** mit dem Passwort **nwsnws** ein
- Starten Sie die grafische Benutzeroberfläche, indem Sie den Befehl startx eingeben
- Starten Sie den Webbrowser *Mozilla*

Sniffer vorbereiten

- Loggen Sie sich auf dem *Sniffer* als User **root** mit dem Passwort **nwsnws** ein
- Starten Sie die grafische Benutzeroberfläche, indem Sie den Befehl startx eingeben
- Starten Sie die Sniffersoftware, indem Sie im Terminalfenster den Befehl ethereal eingeben
- Wählen Sie im Menü ***Capture*** den Menüpunkt ***Start*** aus. Es wird ein Fenster geöffnet indem Sie die Parameter für das sniffen festlegen können.



- Ändern Sie die ***Display Options*** so dass ***Update list of packets in real time*** und ***Automatic scrolling in live capture*** aktiviert sind.

- Starten Sie den Capturevorgang, indem Sie den Button OK betätigen
- Auf dem PC1 rufen Sie mit dem Webbrowser eine einfache Webseite aus dem Internet auf, z.B. www.google.de

Im Etherealfenster können sie die gecapturten Datenpackete sehen.

- Beenden Sie das Capturen und speichern Sie die Daten ab, indem Sie im Menü File den Menüpunkt Save as auswählen. Als Speicherort wählen Sie das Verzeichnis /tmp. Den Dateinamen können Sie frei wählen.

Notizen

Kommunikation im CG-VPN Modus mitschneiden

Notizen

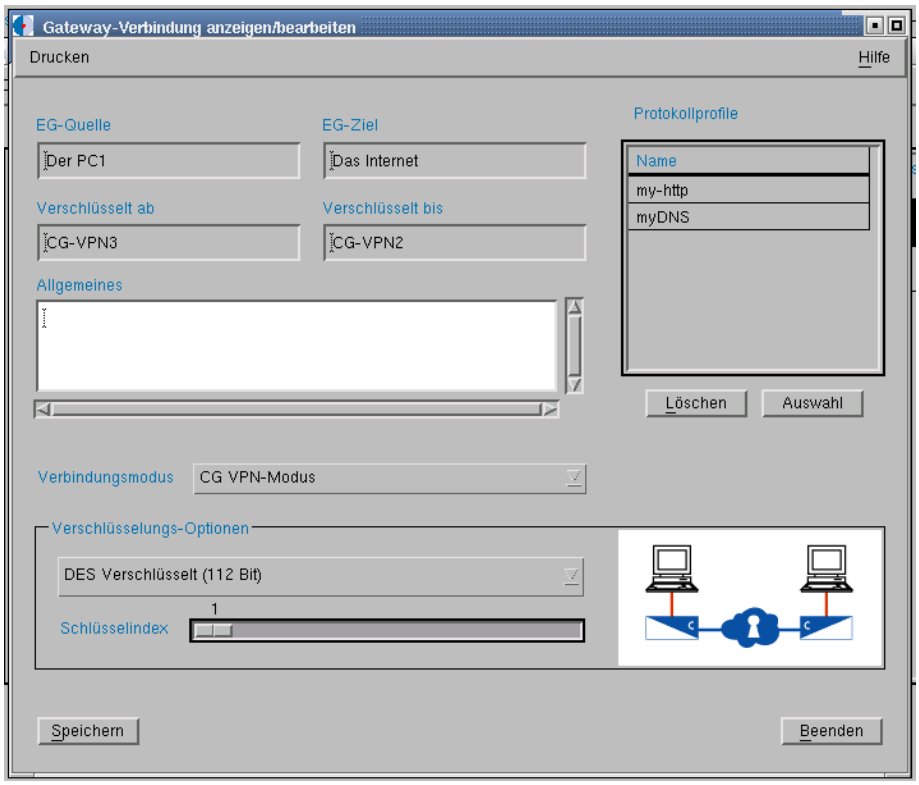
- Wählen Sie im SMS Hauptfenster im Menü ***LAN-Verwaltung*** den Menüpunkt ***Verbindungen*** aus.

Das Fenster *Verbindungen* wird geöffnet.

- Markieren Sie die Verbindung Der PC1 Das Internet und wählen im Menü EG-Verbindungen den Menüpunkt Bearbeiten aus.

Das Fenster *Gateway Verbindungen anzeigen/bearbeiten* wird geöffnet.

- Als Verschlüsselungsoption wählen Sie DES Verschlüsselt (112 Bit) aus.



- Das Fenster Gateway Verbindung anzeigen/bearbeiten schließen Sie, indem Sie den Button Speichern betätigen.

Konfiguration Übertragen

- Wählen Sie im SMS Hauptfenster im Menü ***LAN-Verwaltung*** den Menüpunkt ***Gateways*** aus.

Es öffnet sich das Fenster Gateway-Verwaltung.

- In diesem Fenster wählen Sie mit der linken Maustaste den Eintrag *CG-VPN3* aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet

- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN3* übertragen.

Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den *CG-VPN3* in der Gatewayliste blau angezeigt.

- Wählen Sie jetzt den Eintrag *CG-VPN2* aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet

- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN2* übertragen.

Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den *CG-VPN2* in der Gatewayliste blau angezeigt.

- Starten Sie am Sniffer-PC einen neuen Capture. Wählen Sie hierzu im Menü ***Capture*** den Menüpunkt ***Start*** aus.

- Starten Sie den Capturevorgang, indem Sie den Button OK betätigen

- Am *PC1* rufen Sie mit die Webseite erneut auf, indem Sie den Button Reload des Webbrowsers betätigen.

Im Etherealfenster können sie die gecapturten Datenpackete sehen.

- Beenden Sie das Capturen und speichern Sie die Daten ab, indem Sie im Menü File den Menüpunkt Save as auswählen. Als Speicherort wählen Sie das Verzeichnis /tmp. Den Dateinamen können Sie frei wählen.

Notizen

Kommunikation im Ipsec Mainmode mitschneiden

Notizen

- Wählen Sie im SMS Hauptfenster im Menü ***LAN-Verwaltung*** den Menüpunkt ***Verbindungen*** aus.

Es öffnet sich das Fenster ***Verbindungen***.

- Markieren Sein den Eintrag für die Verbindung *Der PC1 Das Internet* und löschen sie die Verbindung, indem sie im Menü EG-Verbindungen den Menüpunkt Löschen wählen

- Schließen Sie das Fenster Verbindungen

Jetzt muss die Konfiguration an CG-VPN3 und CG-VPN2 übertragen werden.

- Wählen Sie im SMS Hauptfenster im Menü ***LAN-Verwaltung*** den Menüpunkt ***Gateways*** aus

Es öffnet sich das Fenster Gateway-Verwaltung.

- In diesem Fenster wählen Sie mit der linken Maustaste den Eintrag *CG-VPN3* aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet

- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN3* übertragen.

Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den *CG-VPN3* in der Gatewayliste blau angezeigt.

- Wählen Sie jetzt den Eintrag *CG-VPN2* aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet

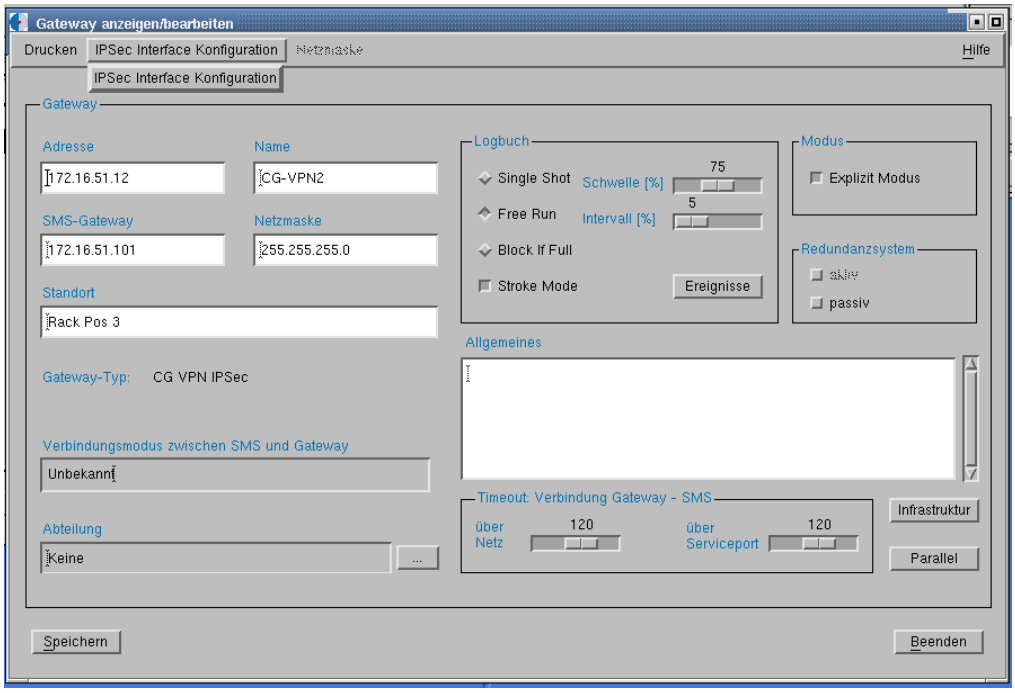
- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN2* übertragen.

Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den *CG-VPN2* in der Gatewayliste blau angezeigt.

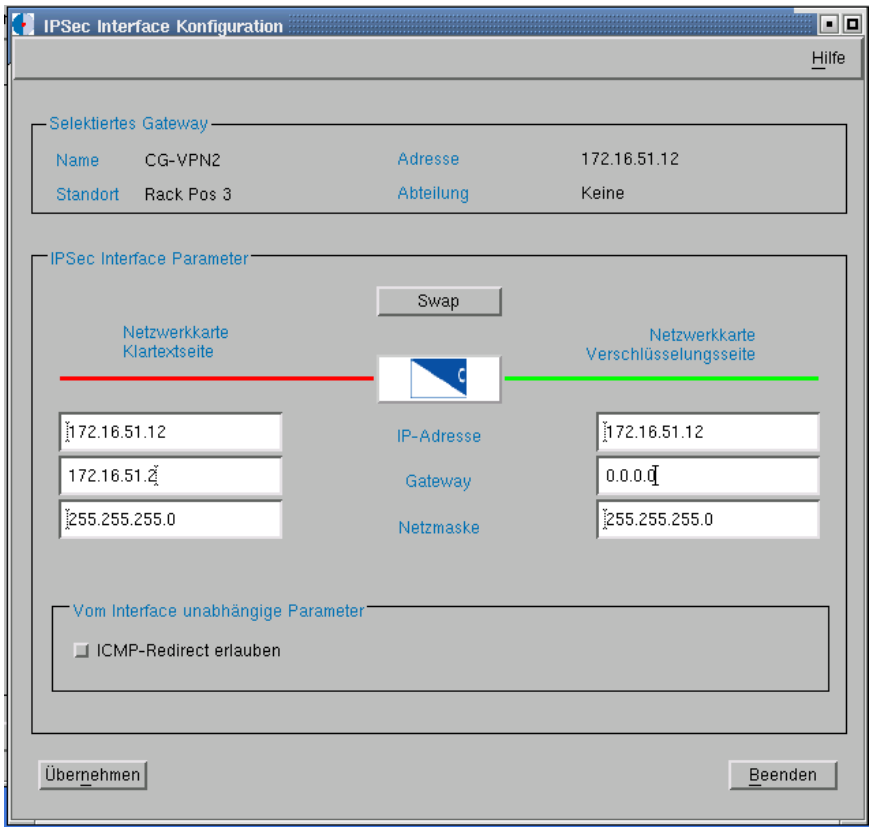
IPSec Interface Konfiguration von CG-VPN2 bearbeiten

- Im Fenster ***Gateway Verwaltung*** markieren Sie den Eintrag für das *CG-VPN2* und wählen anschließend im Menü ***Gateway*** den Menüpunkt ***Bearbeiten*** aus.

- Im Fenster ***Gateway bearbeiten/anzeigen*** wählen Sie jetzt das Menü ***IPSec Interface Konfiguration*** und den Menüpunkt ***IPSec Interface Konfiguration*** aus.



- Im Fenster ***IPSec Interface Konfiguration*** passen Sie die IP-Adressen für die Gateways auf der Klartext und der Verschlüsselungsseite an
  Gateway Klartextseite: 172.16.51.2
  Gateway Verschlüsselungsseite: 0.0.0.0



Notizen

- Schließen Sie das Fenster ***IPSec Interface Konfiguration, indem Sie den Button Übernehmen betätigen.***

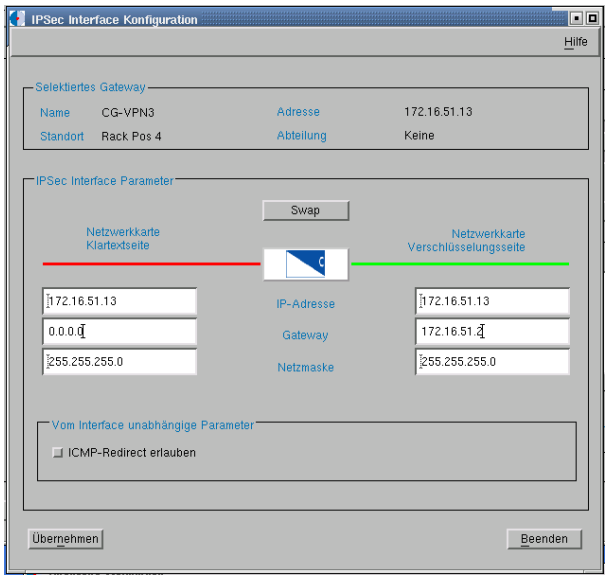
Notizen

IPSec Interface Konfiguration von CG-VPN3 bearbeiten

- Im Fenster ***Gateway Verwaltung*** markieren Sie den Eintrag für das *CG-VPN3* und wählen anschließend im Menü ***Gateway*** den Menüpunkt ***Bearbeiten*** aus.

- Im Fenster ***Gateway bearbeiten/anzeigen*** wählen Sie jetzt das Menü ***IPSec Interface Konfiguration*** und den Menüpunkt ***IPSec Interface Konfiguration*** aus.

- Im Fenster ***IPSec Interface Konfiguration*** passen Sie die IP-Adressen für die Gateways auf der Klartext und der Verschlüsselungsseite an
  Gateway Klartextseite: 0.0.0.0
  Gateway Verschlüsselungsseite: 172.16.51.2



- Schließen Sie das Fenster ***IPSec Interface Konfiguration, indem Sie den Button Übernehmen betätigen.***

Geänderte Konfiguration übertragen

- Im Fenster ***Gateway Verwaltung*** wählen Sie mit der linken Maustaste den Eintrag *CG-VPN3* aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet

- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN3* übertragen.

Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den *CG-VPN3* in der Gatewayliste blau angezeigt.

- Wählen Sie jetzt den Eintrag *CG-VPN2* aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet

- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN2* übertragen.

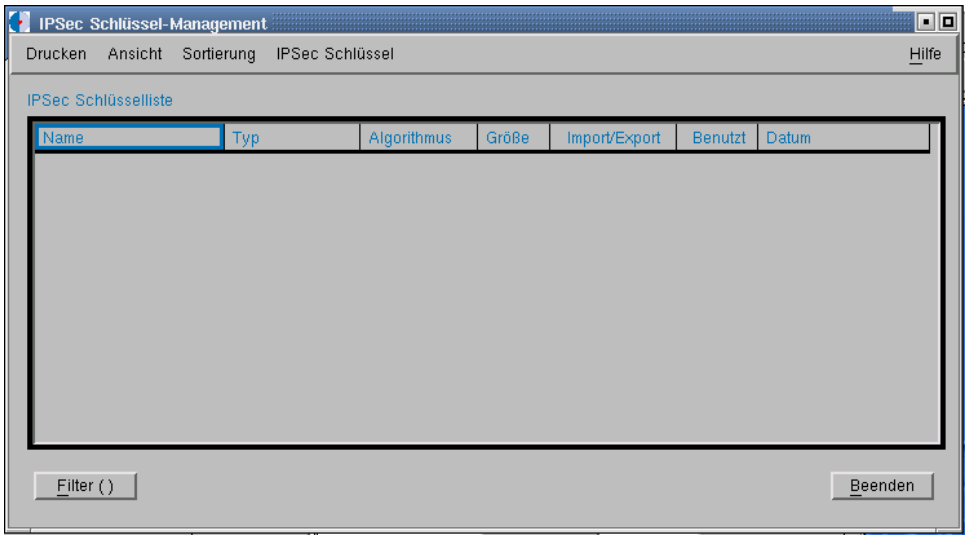
Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den *CG-VPN2* in der Gatewayliste blau angezeigt.

Notizen

IPSec Schlüssel erstellen

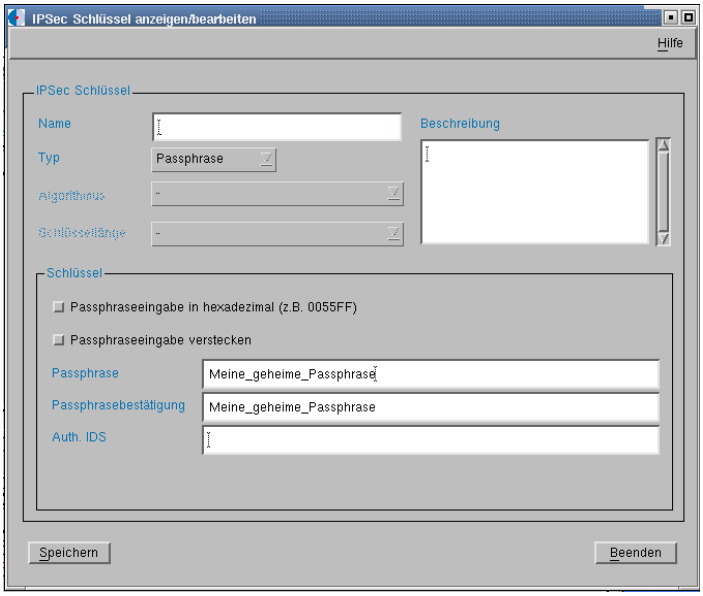
Wählen Sie im SMS Hauptfenster im Menü ***LAN-Verwaltung*** den Menüpunkt IPsec Schlüssel aus.

Das Fenster Ipsec Schlüssel-Management wird geöffnet



- Wählen Sie im Menü ***IPSec Schlüssel*** den Menüpunkt ***Neu*** aus

Das Fenster *IPSec Schlüssel anzeigen/bearbeiten* wird angezeigt



- Geben Sie im Feld ***Name*** einen beliebigen Name für Ihren Schlüssel ein

- Als Typ für den IPSec Schlüssel wählen Sie ***Passphrase*** aus. Geben sie in den Feldern Passphrase und Passphrasebestätigung einen beliebigen Text ein.

Achtung:Geben Sie im Feld Auth. IDS keine Daten ein

- Schließen Sie das Fenster *IPSec Schlüssel anzeigen/bearbeiten* indem sie den Button ***Speichern*** betätigen.

Notizen

Notizen

Eine IPSEc-Verbindung erstellen

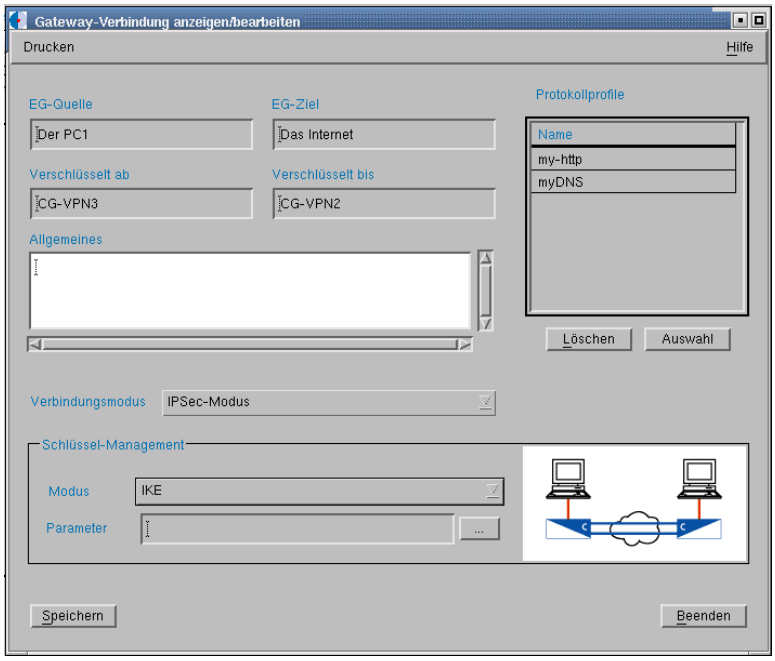
- Wählen Sie im SMS Hauptfenster im Menü ***LAN-Verwaltung*** den Menüpunkt ***Verbindungen*** aus.

Es öffnet sich das Fenster ***Verbindungen***. Darin können Sie Endgeräte-Verbindungen einrichten und administrieren.

- Um eine neue Endgeräte-Verbindung anzulegen, klicken Sie im Fenster ***Verbindungen*** im Menü ***EG-Verbindungen*** auf den Menüpunkt ***Neu***.

Es öffnet sich das Fenster ***Neue EG-Verbindung***.

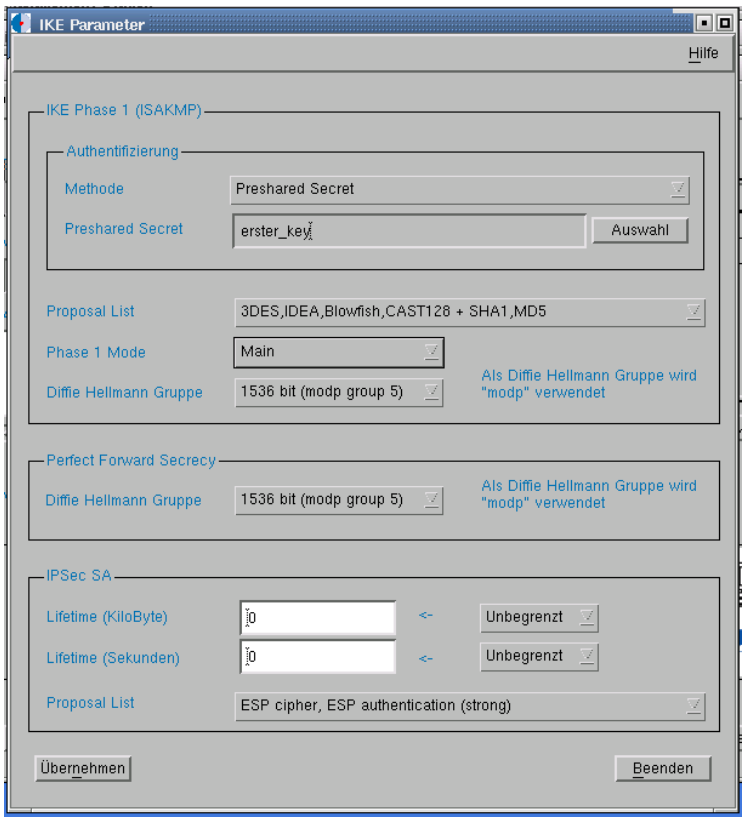
- Betätigen Sie den Button ***Auswahl*** der EG-Quellen . Es öffnet sich das Fenster ***EG-Auswahl***
- Markieren Sie den Eintrag *PC1* und schließen Sie das Fenster, indem Sie den Button Übernehmen betätigen
- Betätigen Sie den Button ***Auswahl*** der EG-Ziele . Es öffnet sich das Fenster ***EG-Auswahl***
- Markieren Sie den Eintrag ***Das Internet*** und schließen Sie das Fenster, indem Sie den Button Übernehmen betätigen
- Betätigen Sie den Button ***Auswahl*** der Protokollprofile. Es öffnet sich das Fenster ***PP-Auswahl***
- Markieren Sie die Einträge ***my-http*** und ***myDNS*** und schließen Sie das Fenster, indem Sie den Button Übernehmen betätigen
- Als Verbindungsmodus wählen Sie ***IPSec-Modus*** aus
- Als Modus wählen Sie IKE aus.



- Betätigen Sie den Button „...“

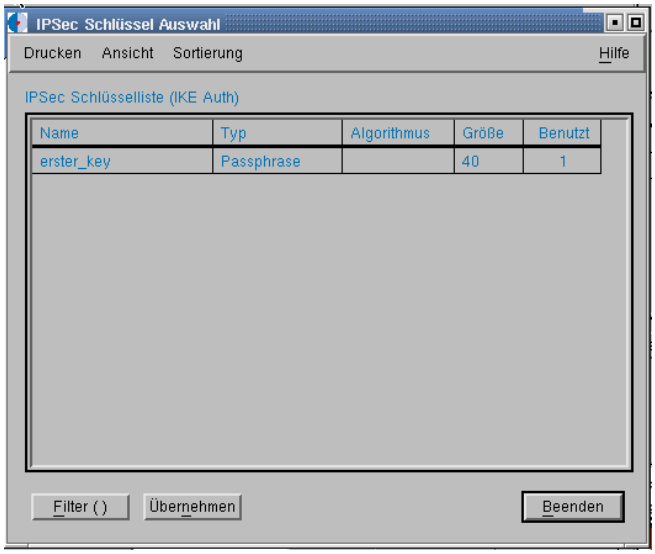
Notizen

Es wird das Fenster IKE Parameter geöffnet



- Wählen sie ein Preshared Secret aus, indem sie den Button Auswahl betätigen.

Es wird das Fenster IPSec Schlüssel Auswahl geöffnet



- Wählen Sie in diesem Fenster mit der linken Maustaste den von Ihnen erstellten IPSec-Schlüssel aus.

- Schließen Sie das Fenster, indem Sie den Button Übernehmen betätigen
- Schließen Sie das Fenster *IKE Parameter*

- Das Fenster *Gateway Verbindung anzeigen/bearbeiten* schließen Sie, indem Sie den Button Speichern betätigen.

Notizen

Konfiguration Übertragen

- Wählen Sie im SMS Hauptfenster im Menü ***LAN-Verwaltung*** den Menüpunkt ***Gateways*** aus.

Es öffnet sich das Fenster Gateway-Verwaltung.

- In diesem Fenster wählen Sie mit der linken Maustaste den Eintrag *CG-VPN3* aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet

- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN3* übertragen.

Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den *CG-VPN3* in der Gatewayliste blau angezeigt.

- Wählen Sie jetzt den Eintrag *CG-VPN2* aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet

- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN2* übertragen.

Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den *CG-VPN2* in der Gatewayliste blau angezeigt.

- Starten Sie am Sniffer-PC einen neuen Capture. Wählen Sie hierzu im Menü ***Capture*** den Menüpunkt ***Start*** aus.

- Starten Sie den Capturevorgang, indem Sie den Button OK betätigen

- Am *PC1* rufen Sie mit die Webseite erneut auf, indem Sie den Button Reload des Webbrowsers betätigen.

Im Etherealfenster können sie die gecapturten Datenpackete sehen.

- Beenden Sie das Capturen und speichern Sie die Daten ab, indem Sie im Menü File den Menüpunkt Save as auswählen. Als Speicherort wählen Sie das Verzeichnis /tmp. Den Dateinamen können Sie frei wählen.

Notizen

Kommunikation im Ipsec Aggressivemode mitschneiden

- Wählen Sie im SMS Hauptfenster im Menü ***LAN-Verwaltung*** den Menüpunkt ***Verbindungen*** aus.

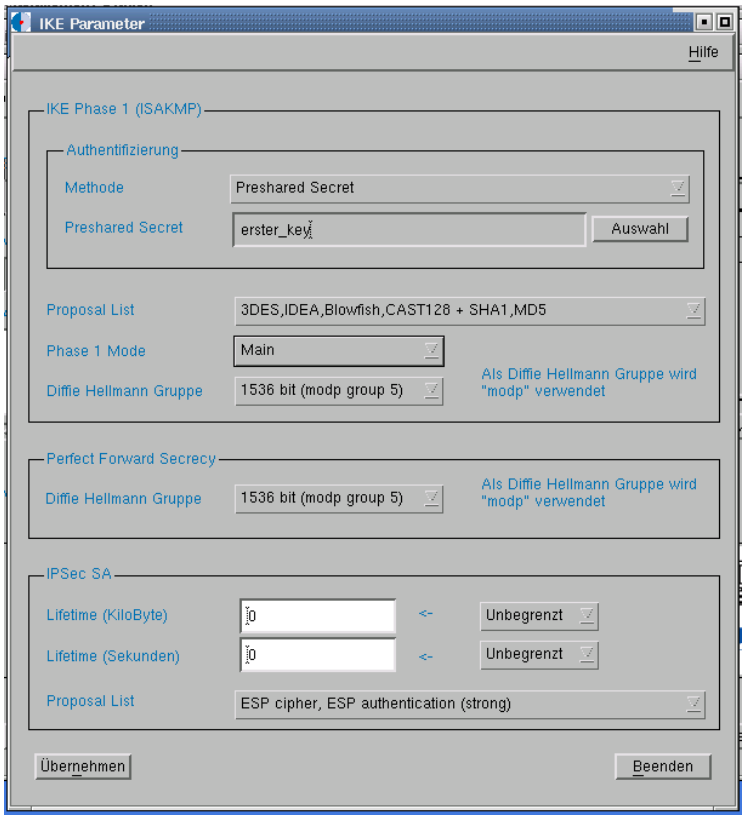
Das Fenster *Verbindungen* wird geöffnet.

- Markieren Sie die Verbindung Der PC1 Das Internet und wählen im Menü EG-Verbindungen den Menüpunkt Bearbeiten aus.

Das Fenster *Gateway Verbindungen anzeigen/bearbeiten* wird geöffnet.

- Betätigen Sie den Button „...“

Es wird das Fenster IKE Parameter geöffnet



- Wählen sie für den ***Phase 1 Mode*** den ***Aggressive Mode***

- Schließen Sie das Fenster *IKE Parameter*

- Das Fenster *Gateway Verbindung anzeigen/bearbeiten* schließen Sie, indem Sie den Button Speichern betätigen.

Notizen

Konfiguration Übertragen

- Wählen Sie im SMS Hauptfenster im Menü ***LAN-Verwaltung*** den Menüpunkt ***Gateways*** aus.

Es öffnet sich das Fenster Gateway-Verwaltung.

- In diesem Fenster wählen Sie mit der linken Maustaste den Eintrag *CG-VPN3* aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet

- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN3* übertragen.

Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den *CG-VPN3* in der Gatewayliste blau angezeigt.

- Wählen Sie jetzt den Eintrag *CG-VPN2* aus und öffnen mit der rechten Maustaste das Menü und wählen den Menüpunkt ***Konfiguration*** aus.

Das Fenster Konfiguration wird geöffnet

- Indem Sie den Button Konfiguration betätigen, wird die Konfiguration an den *CG-VPN2* übertragen.

Nach erfolgreicher Übertragung der Konfiguration wird der Eintrag für den *CG-VPN2* in der Gatewayliste blau angezeigt.

- Starten Sie am Sniffer-PC einen neuen Capture. Wählen Sie hierzu im Menü ***Capture*** den Menüpunkt ***Start*** aus.

- Starten Sie den Capturevorgang, indem Sie den Button OK betätigen

- Am *PC1* rufen Sie mit die Webseite erneut auf, indem Sie den Button Reload des Webbrowsers betätigen.

Im Etherealfenster können sie die gecapturten Datenpackete sehen.

- Beenden Sie das Capturen und speichern Sie die Daten ab, indem Sie im Menü File den Menüpunkt Save as auswählen. Als Speicherort wählen Sie das Verzeichnis /tmp. Den Dateinamen können Sie frei wählen.

Hausaufgabe:

Notizen

Kopieren Sie die vier Etherealmitschnitte auf Diskette, damit Sie die Daten zu Hause mithilfe der Software Ethereal betrachten können.
Erstellen Sie eine Ausarbeitung, die folgende Aspekte berücksichtigen soll:

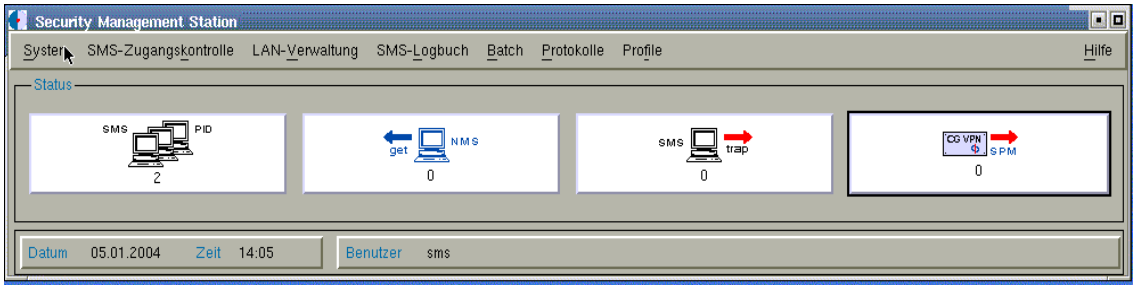
- Auswertung der Aufzeichnungen
  Zeigen Sie den Unterschied zwischen der Klartextkommunikation und der verschlüsselten Kommunikation auf.
- Machen Sie eine Analyse der unterschiedlichen Verschlüsselungsmethoden bezüglich
- Performance (Anzahl der Bytes, die ausgetauscht werden und der Handshakes, usw.)
- Sicherheit
- Diskutieren Sie die Vor- und Nachteile der verschiedenen Modies.

Die Software Ethereal ist Freeware und z.B. für die Betriebssysteme Linux und Windows erhältlich.

Anhang

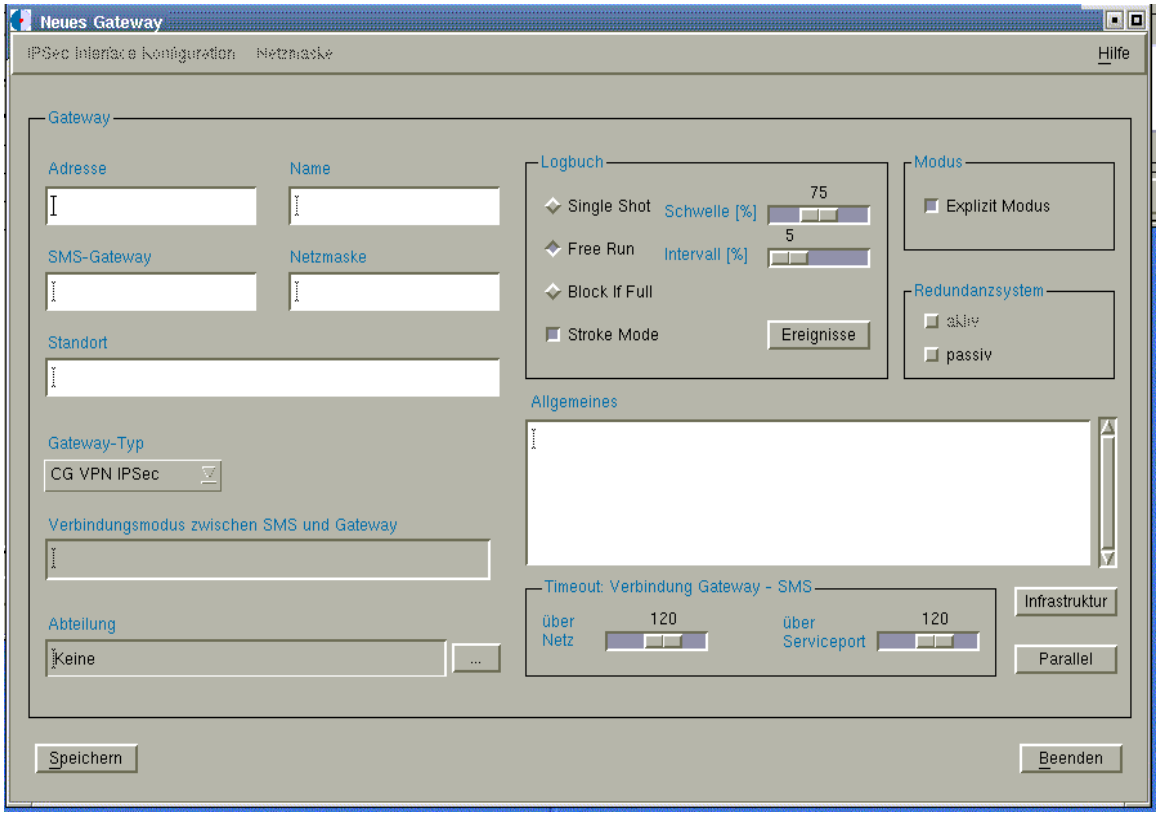
Notizen

A1 SMS-Hauptfenster



Menü	Funktionen
System	Verwaltung der SMS-Systemdaten sowie der Konfigurationsdatei, Lizenzmanagement, UNIX-Shell
SMS Zugangskontrolle	Verwaltung des SMS-Administrationspersonals (Benutzer) sowie der diesem Personal zugewiesenen Rollen und Administrationsbereiche, SMS-Zertifikaterstellung, Login/Logout, SMS-Passwörter ändern
LAN- Verwaltung	Verwaltung von Gateways, IPSec Gateways, CryptoGuardVPN, CryptoGuard VPN IPSec, IPSec Clients, Endgeräten, Bastionen, Netzwerktopologie, Verbindungen, Benutzern, kryptographischen Schlüsseln, IPSecSchlüssel Management
Batch	Automatische Ausführung von Prozeduren
Protokolle	Verwaltung von Netzwerk-, Transport- und Applikationsprotokollen
Profile	Verwaltung von Zeit-, Protokoll- und Dienstprofilen

A2 Neues Gateway



Gruppenfeld Gateway

Adresse Geben Sie hier die IP-Adresse des Gateway ein.

Name Hier wird der logische Name des Gateway eingegeben. Er dient ausschließlich Verwaltungszwecken, z.B.: 'Gateway intern 01'. Erlaubt sind bis zu 50 Zeichen. Geben Sie hier bitte ein, ob es sich um einen CG VPN, eine CG VPN IPSec oder um einen Gateway handelt.

SMS-Gateway Hier ist die IP-Adresse des Gateway einzutragen, über welches ein Gateway die SMS erreichen kann, z.B. die IP-Adresse des zur SMS führenden Routers. Befinden sich SMS und Gateway im gleichen Netz, wird die IP-Adresse der SMS eingegeben.

Netzmaske Geben Sie hier die Netzmaske des Netzes ein, in dem sich der Gateway befindet. Wenn Sie mit der rechten Maustaste in das Feld klicken, öffnet sich ein Kontextmenü, das Ihnen die Einstellung erleichtert. Wenn sich die Einfügemarke im Feld befindet, dann können Sie über die rechte Maustaste das Menü 'Netzmaske' aufrufen.

Standort Geben Sie hier den Standort ein, an dem sich der CryptoGuardVPN befindet. Erlaubt sind bis zu 50 Zeichen.

Gateway-Typ Wählen Sie hier den Gateway-Typ aus. Möglich sind: CG VPN, CG VPN IPSec und IPSec Gateway

Verbind... In diesem Infofeld wird der Verbindungsmodus zwischen Gateway und SMS angezeigt. Wenn Sie ein neues Gateway anlegen ist dieses Infofeld leer.

Abteilung Mit diesem Feld weisen Sie dem Gateway einen Administrationsbereich zu. Klicken Sie auf den Button '...'. Es öffnet sich das Fenster 'Administrationsbereiche'. Markieren Sie einen Bereich/Abteilung und klicken Sie auf 'Übernehmen'. Sie gelangen daraufhin ins Fenster 'Neues Gateway' zurück.

Allgemeines In dieses Feld können Sie weitere Informationen eintragen. Bis zu 255 Zeichen sind möglich.

Gruppenfeld Logbuch

Notizen

In diesem Gruppenfeld legen Sie die Logbuch-Strategie fest. Einerseits konfigurieren Sie, wie sich der CryptoGuardVPN verhalten soll, falls das Logbuch überläuft oder überzulaufen droht. Andererseits haben Sie durch Anwendung des 'Stroke Modes' die Möglichkeit, einen Überlauf durch zweckmäßige Einstellung von 'Schwelle' und 'Intervall' zu vermeiden.

Um das Überlaufverhalten zu konfigurieren, ist einer der folgenden Buttons zu betätigen:

Single Shot	Betätigen Sie diesen Checkbutton, wenn bei einem Überlauf des Logbuchs keine weiteren Logbucheinträge mehr übernommen werden sollen.
Free Run	Betätigen Sie diesen Checkbutton, wenn Sie einen Überlauf des Logbuchs dadurch vermeiden möchten, dass vor jedem neuen Eintrag der jeweils älteste gelöscht wird.
Block if Full	Betätigen Sie diesen Checkbutton, wenn bei einem Überlauf des Logbuchs alle Frames durch den CryptoGuardVPN geblockt werden sollen. Die Kommunikation zwischen CG VPN und SMS bleibt erhalten.

Um die Logbucheinträge zyklisch von der SMS abholen zu lassen, betätigen Sie den Button **'Stroke Mode':**

Schwelle	Betätigen Sie diesen Schieber, um den prozentualen Füllstand des Logbuches einzustellen, ab dem der CryptoGuardVPN eine Spontane Meldung an die SMS sendet, um die vorhandenen Logbucheinträge abholen zu lassen.
Intervall	Betätigen Sie diesen Schieber, um den sekundengenauen Abstand einzustellen, in dem der CryptoGuardVPN wiederholt eine Spontane Meldung an die SMS sendet, um die vorhandenen Logbucheinträge abholen zu lassen.

Ereignisse

Mit diesem Button öffnen Sie das 'Ereignis'-Fenster. Dort können Sie festlegen, wie der CryptoGuardVPN auf generierte Ereignisse reagieren soll: einen Logbucheintrag erzeugen oder Spontane Meldungen bzw. Traps generieren.

Gruppenfeld Modus

Diese Einstellungen sind nur für den CG VPN und den CG VPN IPsec möglich.
Bringen Sie den Button 'Explizit Modus' in die gedrückte Stellung, um ausschließlich die in der Verbindungsliste (CCT) definierten Regeln wirksam werden zu lassen.

Explizit Modus aktiviert	Alle nicht definierten Verbindungen werden gesperrt.
Explizit Modus nicht aktiviert	Alle nicht definierten Verbindungen werden im Klartext durchgereicht.

Gruppenfeld Redundanzsystem

Diese Einstellungen sind nur für den CG VPN und den CG VPN IPsec möglich.
In diesem Gruppenfeld wird angezeigt, ob der CryptoGuard VPN einem aktiven oder passiven Redundanzsystem angehört. Der Button 'aktiv' ist selektierbar, wenn zuvor ein redundantes System in der CG VPN-Liste ausgewählt wurde.

Infrastruktur
Mit diesem Button öffnen Sie das Fenster 'Infrastruktur', in dem das hinter dem Gateway befindliche System beschrieben wird. Für den Eintrag stehen Ihnen maximal 1024 Zeichen zur Verfügung.

Beispiel: Der Gateway steht in Haus A, 3. Etage, Raum 3 bei Frau Mustermann. Der Schlüssel befindet sich beim Hausmeister im Raum 17, der von 9-17:30 Uhr besetzt ist (Telefon: 123/456789).

Notizen

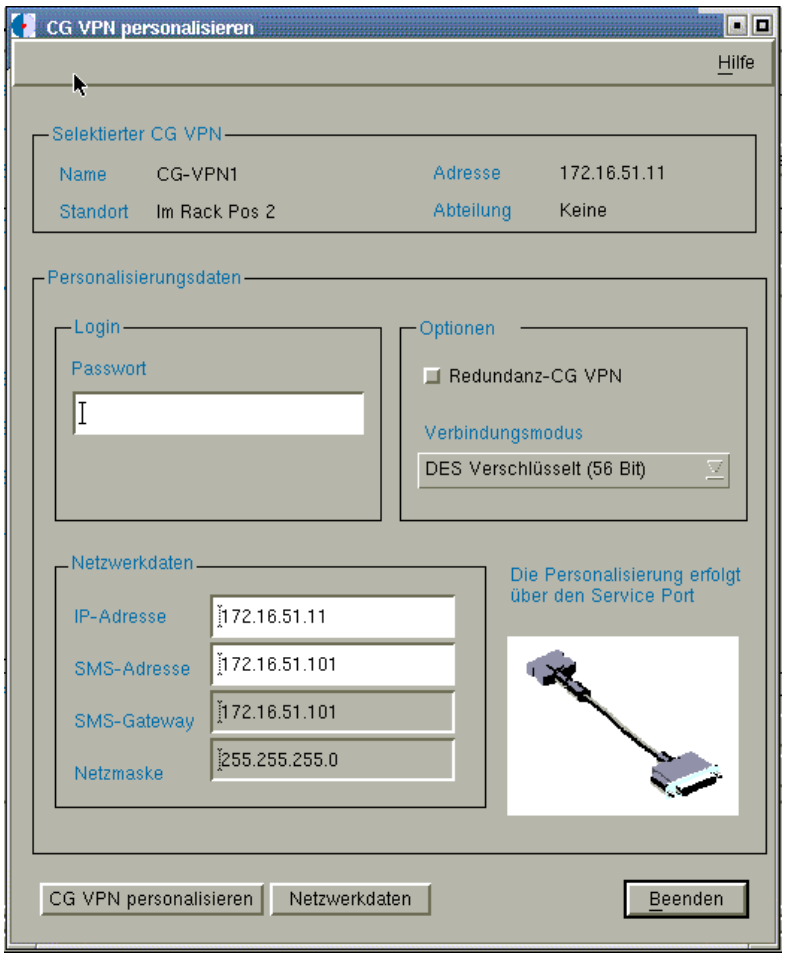
Parallel
Mit diesem Button öffnen Sie das Fenster 'Parallele CG VPN'. Dort können Sie zwei CryptoGuardVPN parallel schalten. Dies hat zur Folge, dass jeder CryptoGuardVPN die Filterregeln des parallel geschalteten Geräts erhält, alle anderen Daten (z.B. IP-Adresse, SMK) jedoch differieren. Diese Betriebsart eignet sich zur Lastverteilung zwischen zwei oder mehreren CryptoGuardVPN, die beispielsweise zwischen zwei Netze geschaltet wurden.

Gruppenfeld Timeout

Diese Funktion ist für die Personalisierung und Konfiguration eines CryptoGuardVPN von Bedeutung. Im Gruppenfeld 'Timeout ....' wird die Anzahl der Sekunden angegeben, nach denen die Verbindung zwischen SMS und CryptoGuardVPN abgebrochen wird, falls in diesem Zeitraum keine Eingabe erfolgte.

über Netz Verzögerungszeit nach der eine über das Netzwerk aufgebaute Verbindung abgebrochen wird.
über Serviceport Verzögerungszeit nach der eine über den Serviceport aufgebaute Verbindung abgebrochen wird.

A3 CG VPN personalisieren



Selektierter CG VPN
In diesem Gruppenfeld werden die Stammdaten des CryptoGuard VPN angezeigt: **Login**

Notizen

Notizen

Passwort In dieses Editierfeld geben Sie das Passwort „smspwd01“ zur Personalisierung des CryptoGuard VPN ein; es umfasst 8 alphanumerische Zeichen. Änderungen des Passworts führen Sie im Fenster 'CG VPN-Passwort ändern' durch

Optionen

Redundanz-CryptoGuard VPN	Bringen Sie diese Taste in die gedrückte Stellung, um den selektierten CryptoGuard VPN als Passiven CryptoGuard VPN eines aktiven Redundanzsystems zu deklarieren. Beim aktiven Redundanzsystem sind zwei CryptoGuard VPN über den Redundanzport mit einem Nullmodemkabel miteinander verbunden.
Verbindungsmodus	Mit dieser Taste wählen Sie den Verschlüsselungsmodus: • DES-verschlüsselt (56Bit) • DES-verschlüsselt (112 Bit)

Netzwerkdaten
In den nachfolgenden Infofeldern sind die in der Datenbank enthaltenen Netzwerkparameter des selektierten CryptoGuard VPN eingeblendet. Über den Button 'Netzwerkdaten' können Sie die aktuelle Netzwerk-Konfiguration in die Infofelder laden. Diese Daten werden über das Netzwerk aus dem CryptoGuard VPN ausgelesen. Diese Funktion kann nur dann ausgeführt werden, wenn der CryptoGuard VPN bereits personalisiert und in das Netzwerk integriert wurde.

A4 Bypass Mode und Expliziet Modus

Bypass Modus

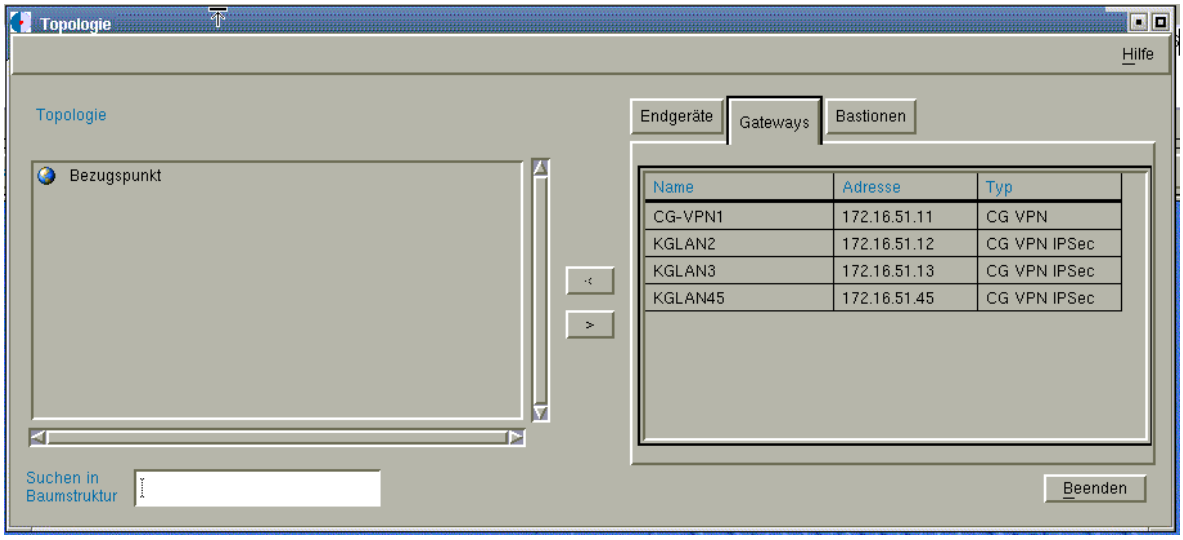
Falls erforderlich, kann der eingehende Datenstrom an den Kontroll-Mechanismen des Paketfilters sowie dem Verschlüsselungsmodul vorbei geleitet werden (Bypass Mode). Besonders in der Einrichtphase oder während einer evtl. notwendigen Fehleranalyse des Sicherheitssystems kann es notwendig sein, den CryptoGuardVPN und seine Restriktionen zu umgehen. Zu diesem Zweck kann ein CryptoGuardVPN in den BypassModus geschaltet werden.

	Bypass Mode OFF	**Bypass Mode ON**
Explizit Modus aktiviert	Befindet sich die Verbindung in der Access-Liste, wird sie entsprechend dem gesetzten Attribut (clear, ciphered, blocked) bearbeitet. Befindet sich die Verbindung nicht in der Access Liste, wird sie geblockt.	Die Access-Liste wird nicht bearbeitet, die Kommunikation wird im Klartext geführt.

Explizit Modus deaktiviert	Befindet sich die Verbindung in der Access-Liste, wird sie entsprechend dem gesetzten Attribut (clear, ciphered, blocked) geführt. Befindet sich die Verbindung nicht in der Access Liste, wird die Kommunikation im Klartext geführt.	Die Access-Liste wird nicht bearbeitet, die Kommunikation wird im Klartext geführt.

Notizen

A5 Topologiefenster



Netzwerk-Komponenten, wie CryptoBastionen, Gateways und Endgeräte werden per Mausklick in das Grafikfeld 'Topologie' übernommen.

Liste aller ... Endgeräte... Gateways... Bastionen

Klicken Sie diesen Wahl-Button an, um im darunter liegenden Listenfeld die der SMS bekannten Endgeräte, Gateways oder Bastionen einblenden zu lassen.

Name Namen der Netzwerk-Komponenten, die in die Bastions-, Endgeräte- oder Gateway-Verwaltung eingegeben wurden und somit der SMS bekannt sind.

Adresse Adressen der Netzwerk-Komponenten, die in die Bastions-, Endgeräteoder Gateway-Verwaltung eingegeben wurden und somit der SMS bekannt sind. Es werden sowohl IP- als auch IPX-, MAC- und OSI-IPAdressen angezeigt.

Typ Typen der Netzwerk-Komponenten, die in der Endgeräte- oder GatewayVerwaltung eingegeben wurden und somit der SMS bekannt sind.

Die Tasten '<' und '>'

Durch Anklicken des Buttons '<' übertragen Sie eine vorher im rechten Listenfeld selektierte Netzwerk-Komponente in das linke Grafikfeld 'Topologie'.
Durch Anklicken des Buttons '>' übertragen Sie eine vorher selektierte NetzwerkKomponente aus dem Grafikfeld 'Topologie' in das rechte Listenfeld.

Grafikfeld: Topologie

Folgende Netzwerk-Komponenten können zur Zeit in Form einer Baumstruktur graphisch abgebildet werden.

- Bastionen
- Gateways
  - CryptoGuardVPN
  - CryptoGuard VPN IPSec
  - IPSec Gateway
- Endgeäte
  - KryptoGuard PC
  - IPSec Client
  - Netzwerke
  - Workstations

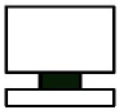
Dabei besitzen die Elemente Bastion und Gateway bipolaren Charakter: Eine Bastion verfügt über ein internes und ein externes Interface, ein Gateway besitzt einen KlartextAnschluss (Plain Side) sowie einen Verschlüsselungs-Anschluss (Cipher Side).
Die im Grafikfeld verwendeten Symbole sind, mit Ausnahme des selbsterklärenden Bezugspunktes, nachstehend erklärt.

Die Zugbrücke zeigt das externe Interface der Bastion an. Ein Wechsel der Seiten können Sie über das Kontextmenü durchführen.
Die Zugbrücke zeigt das interne Interface der Bastion an. Ein Wechsel der Seiten können Sie über das Kontextmenü durchführen.

Notizen

Notizen


Endgeräte-Typen Workstation und Server. Endgeräte-


Typ Netz.

'C' kennzeichnet die aktuelle Verschlüsselungsseite (Cipher Side) eines in das Grafikfeld 'Topologie' integrierten CryptoGuardVPN. Über das Kontextmenü können Sie zwischen Plain- und Cipherside wechseln.

CG VPN IPSec

KGPC (KryptoGuard-PC).

IPSec Client.

IPSec Gateway (cipher)


IPSec Gateway (plain)


Beachten Sie bitte, dass sich der Statuswechsel bei Bastionen und Gateways nur durchführen lässt, wenn diese Komponenten nicht Teil einer Verbindung sind.

Linke und rechte Maustaste

Mit der linken Maustaste selektieren bzw. markieren Sie Einträge sowohl im Grafikfeld wie im Listenfeld. Mit der rechten Maustaste öffnen Sie im Grafikfeld das Kontextmenü.

Einfügen einer Netzwerk-Komponente in das Grafikfeld 'Topologie'

- Wenn das Grafikfeld noch keine Netzwerk-Komponenten enthält: Markieren Sie den Bezugspunkt. Selektieren Sie danach im rechten Listenfeld die gewünschte NetzwerkKomponente und integrieren Sie diese mit dem Button '<' in die Topologie.
- Wenn das Grafikfeld bereits Netzwerk-Komponenten enthält: Markieren Sie den Bezugspunkt oder die Komponente, an die Sie weitere Komponenten angliedern möchten. Selektieren Sie danach im rechten Listenfeld die Komponente und integrieren Sie diese mit dem Button '<' in die Topologie.

Ansehen der topographischen Struktur

- Gesamtüberblick: Markieren Sie den Bezugspunkt und aktivieren im Kontextmenü den Menüpunkt 'Öffnen'.
- Teilzweige ansehen: Markieren Sie die Netzwerk-Komponente, deren weitere Verzweigung Sie ansehen möchten. Bei Benutzung der linken Maustaste gelangen Sie bis zum nächsten CryptoGuardVPN oder zur nächsten Bastion, bei Benutzung des Kontextmenüs (rechte Maustaste) mit dem Menüpunkt 'Öffnen' bis zum Ende des Zweiges.

Suchen in der Baumstruktur

Sie können besonders bei großen, unübersichtlichen Baumstrukturen nach einzelnen Komponenten suchen.
Geben Sie dazu Zeichen in das Editierfeld ein, die vom Anfangsbuchstaben bis zur vollen Zeichenkette des Suchbegriffs reichen können. Erlaubt sind Buchstaben und Zahlen. Groß- und Kleinschreibung sind kein Selektionskriterium, Platzhalter können nicht verwendet werden. Starten Sie die Suche mit Return.

Kontextmenü

Durch Betätigen der rechten Maustaste öffnen Sie das Kontextmenü. Gültig ist das Kontextmenü für genau die Zeile, in der sich der Mauszeiger befindet.

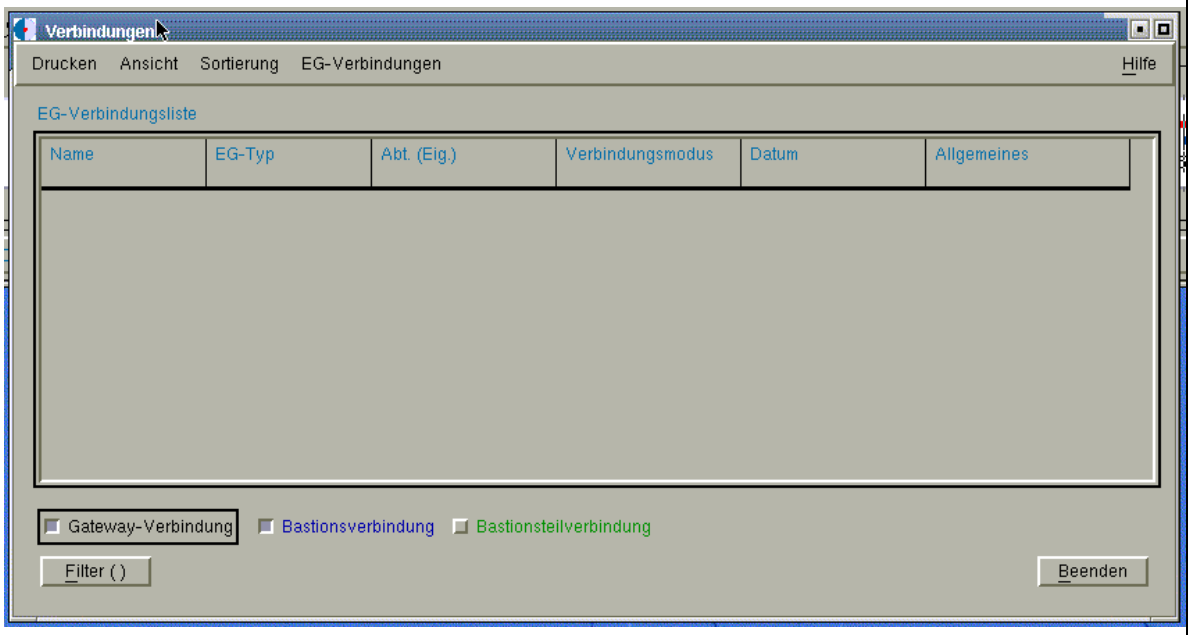
Name	Name der in die Topologie integrierten NetzwerkKomponente
Adresse	Adresse der in die Topologie integrierten NetzwerkKomponente
Öffnen (Bastion/ CG VPN)	Mit diesem Menüpunkt lassen Sie sich den aktuellen Teilzweig anzeigen
Löschen	Mit diesem Menüpunkt entfernen Sie eine Komponente aus dem Grafikfeld
Intern/ Extern (Bastion)	Mit diesen Menüpunkten können Sie die Interfaces der Bastion in der Topologie vertauschen. Klicken Sie im geöffneten Kontextmenü mit der linken Maustaste 'intern' oder 'extern' an um das Interface
Plain / Cipher (CG VPN)	Mit diesen Menüpunkten können Sie die Klartextseite (Plain Side) und die Verschlüsselungsseite (Cipher Side) des CG VPN oder des IPSec Gateway vertauschen. Wählen Sie dazu bei geöffnetem Kontextmenü mit der linken Maustaste die gewünschte Anschlussseite aus

Beachten Sie bitte, dass sich der Statuswechsel bei Bastion und CG VPN nur durchführen lässt, wenn diese Komponenten nicht Teil einer Verbindung sind.

Notizen

A6 EG-Verbindungsliste

Notizen



EG-Verbindungsliste

In der 'EG-Verbindungsliste' werden alle bereits bestehenden Verbindungen zwischen Endgeräten angezeigt. Die Bedeutung der Spalten kann der nachfolgenden Tabelle entnommen werden.

Name Namen der miteinander verbundenen Endgeräte.

IP-Adresse IP-Adressen der an den Verbindungen beteiligten Endgeräte.

EG Typ Typenbezeichnungen der verbundenen Endgeräte:

- KGPC (KryptoGuard-PC)
- IPSec Client (IPSec-fähiges Endgerät)
- Netz (Netzwerk)
- WS (Workstation)
- BI (Bastions-Interface)

Abteilung Administrationsbereiche, denen die jeweiligen Endgeräte zugeordnet wurden.

Verbindungsmodus Der gezeigte Modus wurde der betreffenden EndgeräteVerbindung zugewiesen:

- Klartext
- verschlüsselt
- geblockt
- IPSec (Manul Keying oder IKE)

Der Verbindungsmodus wird nur bei den Verbindungsarten CG VPN-Verbindung und Bastionsteilverbindung angezeigt. Bei Bastionsverbindungen ist das Feld leer.

Datum Letztes Änderungsdatum eines Verbindungsparameters

Notizen

Allgemeines Allgemeine Informationen.

Gateway-Verbindung, Bastionsverbindung, Bastionsteilverbindung anzeigen:

Mit den unter dem Listenfeld befindlichen Buttons können Sie die Art der angezeigten Verbindungen auswählen. Die Verbindungsarten werden in unterschiedlichen Farben dargestellt. Gateway-Verbindungen (schwarz) sind stets bastionslose Verbindungen. Bastionsverbindungen (blau) sind Verbindungen die über eine Bastion gehen. Bastionsteilverbindungen (grün) sind automatisiert generierte Verbindungen und bestehen zwischen einem Endgerät und einer Bastion, können aber auch, sofern eine Verbindung über mehrere Bastionen angelegt wurde, zwischen mehreren Bastionen bestehen.
Wenn Sie beispielsweise nur Bastionsverbindungen anzeigen lassen wollen, bringen sie nur den zugehörigen Button in die gedrückte Position.

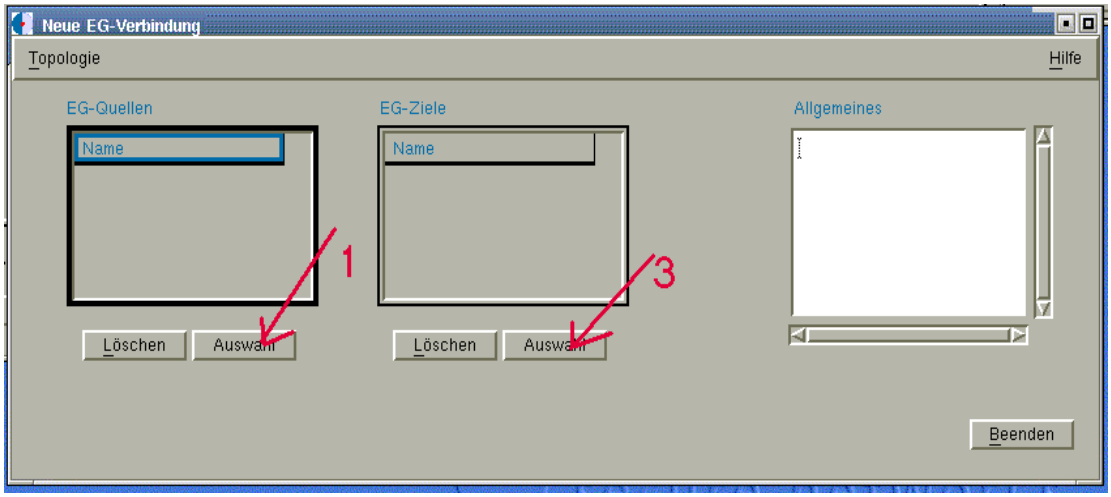
Abhängige Verbindungen auflisten

Mit der rechten Maustaste können Sie eine vorher selektierte Bastionsverbindung anklicken, um die von ihr abhängigen Bastionsteilverbindungen auflisten zu lassen.

Mit 'Tabelle zurücksetzen' setzen Sie die Tabelle wieder in den Ursprungszustand zurück. Diese beiden

Kontextmenüpunkte sind auch über das Menü 'Ansicht' verfügbar.

A7 Fenster Neue EG-Verbindung



EG-Quellen

In diesem Listenfeld erscheint das ausgewählte Quell-Endgerät. Es können auch mehrere Endgeräte, die mit einem Ziel verbunden werden sollen, ausgewählt werden.

Auswahl Mit diesem Button öffnen Sie das Fenster 'EG-Auswahl', um daraus das gewünschte Quell-Endgerät zu übernehmen.

Löschen Mit diesem Button löschen Sie das vorher im Listenfeld selektierte Endgerät.

EG-Ziele

In diesem Listenfeld erscheint das ausgewählte Ziel-Endgerät. Es können auch mehrere Endgeräte, die mit einer Quelle verbunden werden sollen, ausgewählt werden.

Auswahl Mit diesem Button öffnen Sie das Fenster 'EG-Auswahl', um daraus das gewünschte Ziel-Endgerät zu übernehmen.

Löschen Mit diesem Button löschen Sie das vorher im Listenfeld selektierte Endgerät.

Allgemeines

In dieses Editierfeld können Sie Informationen zur Verbindung eingeben.

Das Menü 'Topologie'

Ein Klick auf diesen Menüpunkt öffnet das Topologiefenster, mit dessen Hilfe Sie leicht überprüfen können, wie die ausgewählten Endgeräte in das Netzwerk integriert wurden.

Notizen