ViPNet Coordinator HW/VA 3.2

Referenzhandbuch

ViPNet Virtual Private Network

infotecs

Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Konfiguration von ViPNet Produkten. Für die neuesten Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Upgrade zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind immer zu finden unter http://www.infotecs.de

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Der Hersteller haftet nur im Umfang seiner Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für ViPNet Produkte finden Sie unter http://www.infotecs.de. Der Hersteller übernimmt keine Verantwortung für Datenverlust und Schäden, die durch den unsachgemäßen Betrieb des Produkts entstanden sind.

Copyright

1991–2014 Infotecs GmbH, Berlin

Version: 00079-05 90 01 DEU

Dieses Dokument ist Teil des Softwarepaketes und unterliegt daher denselben Lizenzbestimmungen wie das Softwareprodukt.

Dieses Dokument oder Teile davon dürfen nicht ohne die vorherige schriftliche Zustimmung der Infotecs GmbH verändert, kopiert, weitergegeben etc. werden.

ViPNet ist ein registriertes Warenzeichen des Softwareherstellers Infotecs GmbH.

Marken

Alle genannten Markennamen sind Eigentum der jeweiligen Hersteller.

Wie Sie Infotecs erreichen

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

Tel.: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

WWW: http://www.infotecs.de

E-Mail: support@infotecs.biz

Inhalt

Einführung

Über dieses Dokument

Dieses Dokument bildet den Anhang zum Hauptdokument „ViPNet Coordinator HW/VA. Administratorhandbuch“ und enthält Beschreibungen und Beispiele für Befehle, die durch Befehlszeilenschnittstelle für Konfiguration des ViPNet Coordinator HW/VA angegeben werden sollen. Für die erfolgreiche Arbeit mit diesem Dokument ist es empfehlenswert, dass der Leser über Grundlagenwissen in Netzwerktechnologie sowie über erste Einblicke in die ViPNet-Technologie verfügt. Ausführliche Informationen über ViPNet-Netzwerke s. Dokumente „ViPNet VPN. Benutzerhandbuch“ und „Die Technologie von ViPNet. Allgemeine Informationen“.

Zielgruppe

Dieses Dokument ist für Administratoren der ViPNet VPN-Netzwerke bestimmt, die für Installation und Konfiguration von ViPNet Coordinator HW/VA zuständig sind.

Verwendete Konventionen

Weiter unten sind Konventionen aufgeführt, die im gegebenen Dokument zur Kennzeichnung wichtiger Informationen verwendet werden.

Tabelle 1. Symbole, die für Anmerkungen benutzt werden

Symbol	Beschreibung
	**Achtung!** Dieses Symbol weist auf einen Vorgang hin, der für die Daten- oder Systemsicherheit wichtig ist.
	**Hinweis.** Dieses Symbol weist auf einen Vorgang hin, der es Ihnen ermöglicht, Ihre Arbeit mit dem Programm zu optimieren.
	**Tipp.** Dieses Symbol weist auf zusätzliche Informationen hin.

Tabelle 2. Notationen, die zur Kennzeichnung von Informationen im Text verwendet werden

Notation	Beschreibung
Name	Namen von Elementen der Benutzeroberfläche. Beispiele: Fensterüberschriften, Feldnamen, Schaltflächen oder Tasten.
Taste+Taste	Tastenkombinationen. Zum Betätigen von Tastenkombinationen sollte zunächst die erste Taste gedrückt und dann, ohne die erste Taste zu lösen, die zweite Taste gedrückt werden.
Menü > **Untermenü** > **Befehl**	Hierarchische Abfolge von Elementen. Beispiele: Menüeinträge oder Bereiche der Navigationsleiste.
`Code`	Dateinamen, Pfade, Fragmente von Textdateien und Codeabschnitten oder Befehle, die aus der Befehlszeile ausgeführt werden.

Für die Beschreibung der Befehle werden in diesem Dokument folgende Konventionen verwendet:

- Befehle, die aussschließlich im Administratormodus ausgeführt werden können, werden in roter Farbe hervorgehoben. Beispiel:

  ```
  Befehl
  ```

- Parameter, die vom Benutzer festgelegt werden sollen, werden in Pfeilklammern eingeschlossen angezeigt. Beispiel:

  ```
  Befehl <Parameter>
  ```

- Optionale Parameter werden durch eckige Klammern begrenzt angezeigt. Beispiel:

  ```
  Befehl <obligatorischer Parameter> [optionaler Parameter]
  ```

- Wenn bei der Befehlseingabe ein Parameter aus mehreren möglichen Parameteroptionen ausgewählt werden soll, werden die Parameteroptionen in geschwungenen Klammern durch Strich getrennt angezeigt. Beispiel:

  ```
  Befehl {Option-1 | Option-2}
  ```

Kontakt

FAQ und andere Hilfsinformation

Informationen über ViPNet-Produkte und Lösungen, gängige Fragen und andere nützliche Hinweise sind auf der Webseite von „InfoTeCS“ zusammengefasst. Unter den aufgeführten Links können Sie zahlreiche Antworten auf mögliche während des Produktbetriebs auftretenden Fragen finden.

- Allgemeine Geschäftsbedingungen http://www.infotecs.de/about/terms.php
- ViPNet-Lösungen im Überblick http://www.infotecs.de/solutions/
- Frequently Asked Questions
  http://www.infotecs.biz/doc_vipnet/DEU/index.htm#2_11572.htm
- ViPNet-Wissensdatenbank
  http://www.infotecs.biz/doc_vipnet/DEU/index.htm#1_main.htm

Kontakt

Bei Fragen zur Nutzung von ViPNet-Software sowie möglichen Wünschen und Anregungen nehmen Sie Kontakt mit den Fachleuten der Firma „InfoTeCS“ auf. Für die Lösung aufgetretener Problemfälle wenden Sie sich an den technischen Support.

- E-Mail: support@infotecs.biz.
- Anfrage an den technischen Support via Internetseite http://infotecs.de/support/
- Support Hotline +49 (0) 30 206 43 66 0 (Tel.); +49 (0) 30 206 43 66 66 (Fax).

1

Grundparameter für ViPNet Coordinator HW/VA einstellen

Konfiguration der Systemparameter

Datum und Uhrzeit einstellen

Damit ein Computer mit installiertem ViPNet Coordinator HW/VA ordnungsgemäß mit anderen Anwendungen und geschützten ViPNet Knoten kommunizieren kann, sollten Systemdatum und -uhrzeit richtig konfiguriert werden.

Achtung! Wenn das Systemdatum und die Systemuhrzeit nicht richtig eingestellt sind, können abgesicherte Verbindungen zu anderen ViPNet Knoten blockiert werden.

Es wird empfohlen, die Synchronisation der Systemzeit über das NTP-Protokoll einzustellen (s. Parameter des NTP-Servers einstellen auf S. 29).

Führen Sie die folgenden Befehle aus, um Systemdatum und –uhrzeit einzustellen:

1. Zum Anzeigen der aktuellen Systemzeit führen Sie den folgenden Befehl aus:

   `machine show date`

2. Wenn die Zeitzone geändert werden soll, führen Sie die folgenden Schritte aus:
   - Führen Sie den Befehl `machine set timezone` aus.
   - Sobald Ihnen die Kontinente zur Auswahl stehen („`Please select a continent or ocean`“), geben Sie die Ihrem Kontinent entsprechende Nummer ein und drücken **Eingabe**.
   - Sobald Ihnen die Länder zur Auswahl stehen („`Please select a country`“), geben Sie die Ihrem Land entsprechende Nummer ein und drücken **Eingabe**.
   - Sobald Ihnen die Zeitzonen zur Auswahl stehen („`Please select one of the following time zone regions`“), geben Sie die richtige Nummer ein und drücken **Eingabe**.
   - Die dem angegebenen Standort entsprechende Zeitzone wird auf dem Bildschirm angezeigt. Um diese Zeitzone zu übernehmen, geben Sie „`1`“ („`Yes`“) ein. Um den Standort neu zu definieren, geben Sie „`2`“ („`No`“) ein. Drücken Sie **Eingabe**.
   - Nachdem die Zeitzone angenommen wurde, wird die Systemzeit angezeigt.
     - Um die Systemzeit zu übernehmen, drücken Sie **Eingabe**.

- Um die Zeit zu ändern, geben Sie Datum und Zeit an und drücken **Eingabe**. Bitte halten Sie sich an dieses Format: JJJJ-MM-TT hh:mm:ss.

3 Falls erforderlich, ändern Sie die Systemzeit mit Hilfe des folgenden Befehls:

```
machine set date <Datum>
```

Datum und Uhrzeit werden im Format MMTThhmm[JJJJ] eingegeben.

Konfiguration der Auslagerungsdatei

Führen Sie die folgenden Schritte aus, um die Parameter der Auslagerungsdatei zu konfigurieren:

- Benutzen Sie den folgenden Befehl, um die maximale Größe der Auslagerungsdatei festzulegen:

  ```
  machine swap set <Größe in MB>
  ```

  Wenn die festgelegte Größe der Auslagerungsdatei den zur Verfügung stehenden freien Speicherplatz auf dem Laufwerk übersteigt, wird eine entsprechende Meldung angezeigt.

Achtung! Nachdem die Größe der Auslagerungsdatei festgelegt wurde, sollten auf dem Laufwerk noch mindestens 256 MB freier Speicherplatz verbleiben.

- Benutzen Sie den folgenden Befehl, um die Verwendung der Auslagerungsdatei zu aktivieren:

  ```
  machine swap mode on
  ```

- Führen Sie den folgenden Befehl aus, um Informationen über die Speicherverwendung und die Auslagerungsdatei anzuzeigen:

  ```
  machine show memory
  ```

- Benutzen Sie den folgenden Befehl, um die Verwendung der Auslagerungsdatei zu deaktivieren:

  ```
  machine swap mode off
  ```

  Nach Ausführung dieses Befehls wird die Auslagerungsdatei gelöscht.

Parameter für Systemprotokoll einstellen

Benutzen Sie die folgenden Befehle, um mit dem Ereignisprotokoll zu arbeiten:

- Führen Sie den folgenden Befehl aus, um den Knoten anzugeben, auf dem das Ereignisprotokoll gespeichert werden soll, oder um das Ereignisprotokoll zu deaktivieren:

  ```
  machine set loghost {local | <IP-Adresse> | null}
  ```

  Geben Sie einen der folgenden Werte an, um den Knoten zu definieren:

  - `local` – lokales Laufwerk von ViPNet Coordinator HW/VA,
  - `IP-Adresse` – IP-Adresse des Knotens, an welchen Daten über Systemereignisse gesendet werden sollen,
  - `null` – Ereignisprotokoll nicht speichern.

- Wenn das Ereignisprotokoll auf dem lokalen Laufwerk gespeichert wird, dann führen Sie den folgenden Befehl aus, um das Log anzuzeigen:

  ```
  machine show logs
  ```

- Ereignisprotokolle, die auf dem lokalen Laufwerk gespeichert werden, können auf einen abnehmbaren USB-Datenträger mit Dateisystem FAT32 oder ext2 exportiert werden. Schließen Sie dazu den USB-Datenträger an den Computer an und führen Sie den folgenden Befehl aus:

  ```
  admin export logs usb
  ```

- Führen Sie den folgenden Befehl aus, um das Ereignisprotokoll auf dem lokalen Laufwerk zu löschen:

  ```
  admin remove logs
  ```

ViPNet Coordinator HW/VA zum Netzwerk verbinden

Verbindung zum Ethernet-Netzwerk herstellen

Den im System installierten Ethernet-Netzwerkadaptern werden die Bezeichnungen `eth0`, `eth1` usw. zugeordnet (je nach Anzahl der Adapter im System). Damit Verbindungen zum Ethernet-Netzwerk hergestellt werden können, sollten Sie die Parameter der Netzwerkadapter einstellen. Wechseln Sie dazu in den Administratormodus und führen Sie die folgenden Schritte aus:

- Führen Sie den folgenden Befehl aus, um einen Netzwerkadapter ein- oder auszuschalten:

  ```
  inet ifconfig eth0 {up | down}
  ```

  

  Hinweis. Hier und im Folgenden sollte statt `eth0` der Name des benötigten Netzwerkadapters angegeben werden.

- Führen Sie den folgenden Befehl aus, um auf dem Netzwerkadapter den automatischen Bezug von Parametern vom DHCP-Server zu aktivieren:

  ```
  inet ifconfig eth0 dhcp
  ```

- Führen Sie den folgenden Befehl aus, um dem Netzwerkadapter eine statische IP-Adresse zuzuordnen:

  ```
  inet ifconfig eth0 address <IP-Adresse> netmask <Netzmaske>
  ```

  Wenn der Adapter über eine dynamische IP-Adresse verfügte, dann gehen die Daten auf dem DNS- und NTP-Server, die über das DHCP-Protokoll bezogen wurden, nach dem Setzen einer statischen IP-Adresse verloren.

- Wenn Sie den Alias für einen Netzwerkadapter mit einer statischen Adresse festlegen möchten, dann führen Sie den folgenden Befehl aus:

  ```
  inet ifconfig eth0 address add <IP-Adresse> netmask <Netzmaske>
  ```

  Für die zusätzliche statische IP-Adresse, spielt es keine Rolle, ob die erste IP-Adresse statisch oder dynamisch ist.

- Wenn Sie alle Einstellungen auf einem Adapter zurücksetzen möchten, dann führen Sie den folgenden Befehl aus:

  ```
  inet ifconfig eth0 reset
  ```

  Beim Ausführen dieses Befehls werden alle Einstellungen des Adapters zurückgesetzt und der Adapter selbst wird deaktiviert (sein Status wird auf down gesetzt).

  Wenn Sie die Einstellungen für alle Adapter eines Computers zurücksetzen möchten, dann führen Sie den folgenden Befehl aus:

  ```
  inet ifconfig all reset
  ```

- Führen Sie den folgenden Befehl aus, um eine Adresse des DNS-Servers hinzuzufügen oder zu löschen:

  ```
  inet dns {add | delete} <IP-Adresse>
  ```

  Wenn die Adressen der DNS-Server vom DHCP-Server bezogen wurden, ist das manuelle Hinzufügen oder Löschen der DNS-Server nicht möglich.

- Führen Sie den folgenden Befehl aus, um eine Adresse des NTP-Servers hinzuzufügen oder zu löschen:

  ```
  inet ntp {add | delete} <IP-Adresse | DNS-Name>
  ```

  Wenn die Adressen der NTP-Server vom DHCP-Server bezogen wurden, ist das manuelle Hinzufügen oder Löschen der NTP-Server nicht möglich.

Beispiele für Befehle:

```
inet ifconfig eth0 address 10.0.8.79 netmask 255.255.255.0
inet route add default gw 10.0.8.1
inet dns add 10.0.2.3
```

Verbindung zum Wi-Fi-Netzwerk herstellen

Wenn der Computer über einen Wi-Fi-Adapter verfügt (wird als Adapter mit dem Namen wlan0 aufgeführt), dann kann ViPNet Coordinator HW/VA im Wi-Fi-Netzwerk in einem der zwei Modi eingesetzt werden:

- Client: für Verbindungen zu beliebigen Wi-Fi-Netzwerken.
- Zugriffspunkt (s. Parameter des Wi-Fi-Zugriffspunkts einstellen auf S. 26): für Verbindungen drahtloser Wi-Fi-Geräte zum ViPNet Coordinator HW/VA.

Die Funktion des Clients und die Funktion des Zugriffspunkts können dabei nicht gleichzeitig ausgeübt werden.

Führen Sie die folgenden Befehle aus, um die Verbindung von ViPNet Coordinator HW/VA zum Wi-Fi-Netzwerk als Client einzurichten:

1. Schalten Sie den Netzwerkadapter wlan0 mit Hilfe des folgenden Befehls in den Client-Modus um:

   ```
   inet wifi role client
   ```

2. Führen Sie den folgenden Befehl aus, um eine Liste verfügbarer Wi-Fi-Netzwerke anzuzeigen:

   ```
   inet wifi scan
   ```

3. Geben Sie den Namen des Wi-Fi-Netzwerks, zu dem Sie sich verbinden wollen, sowie den Authentisierungsmodus an. Benutzen Sie dazu einen der folgenden Befehle:

   - Wenn keine Authentifizierung im Netzwerk erforderlich ist, führen Sie den folgenden Befehl aus:

     ```
     inet wifi client ssid <Netzwerkname> authentication open
     ```

   - Wenn für die Authentifizierung der Modus WPA-PSK oder WPA2-PSK verwendet wird, dann muss ein Passwort eingegeben werden. Führen Sie dazu den folgenden Befehl aus:

     ```
     inet wifi client ssid <Netzwerkname> authentication {wpa-psk | wpa2-psk} passphrase <Passwort>
     ```

     Das Passwort können Sie beim Administrator des Wi-Fi-Netzwerks, zu dem Sie sich verbinden, anfordern.

4. Aktivieren Sie den Netzwerkadapter wlan0 mit Hilfe des Befehls:

   ```
   inet wifi mode on
   ```

5. Führen Sie den folgenden Befehl aus, um die Verbindungsparameter für das Wi-Fi-Netzwerk zu überprüfen:

   ```
   inet show wifi
   ```

Beispiele für Befehle:

```
inet wifi ssid mynetwork authentication wpa-psk passphrase qwerty
inet wifi mode on
```

Verbindung zum 3G-Mobilfunknetz herstellen

ViPNet Coordinator HW/VA kann sich über 3G-Mobilfunknetze mit Hilfe eines eingebauten oder externen Modems zum Internet verbinden. Im System wird ein 3G-Modem als Netzwerkadapter mit dem Namen ppp0 abgebildet.

Für Verbindungen zum Internet können die Dienste eines beliebigen Mobilfunkanbieters genutzt werden. Dazu sind die Anschaffung einer SIM-Karte und die Aktivierung entsprechender Dienste (falls nötig) erforderlich. Ausführliche Informationen über die Bedingungen eines Internet-Anschlusses können Sie bei Ihrem Mobilfunkanbieter anfordern.

Für die Funknetzbetreiber Verizon und Vodafone können Sie die vorkonfigurierten Internet-Verbindungseinstellungen verwenden. Andere Betreiber können, wenn nötig, wie weiter unten beschrieben hinzugefügt werden.

Führen Sie die folgenden Schritte aus, um die Verbindung zum Internet über ein 3G-Mobilfunknetz einzurichten:

1 Wenn ein Mobilfunkanbieter, der nicht in der Standardliste enthalten ist, neu hinzugefügt werden soll, dann führen Sie die folgenden Schritte aus:

- Geben Sie den Namen des Anbieters mit Hilfe des folgenden Befehls an:

  ```
  inet usb-modem add provider <Anbietername>
  ```

Hinweis. Wenn Sie einen neuen Provider hinzufügen, wird dieser automatisch als der Standard-Provider festgelegt.

- Geben Sie die IP-Adresse oder den DNS-Namen des Zugriffspunkts mit Hilfe des folgenden Befehls an:

  ```
  inet usb-modem set connection address <IP-Adresse | DNS-Name>
  ```

- Legen Sie die Telefonnummer (im USSD-Befehlsformat) des Internet Access Point mit Hilfe des folgenden Befehls fest:

  ```
  inet usb-modem set phone *99***1#
  ```

- Wenn nötig, geben Sie den Namen des Benutzers mit Hilfe des folgenden Befehls an:

  ```
  inet usb-modem set user <Benutzername>
  ```

- Wenn nötig, geben Sie das Passwort für den Anschluss mit Hilfe des folgenden Befehls an:

  ```
  inet usb-modem set password <Passwort>
  ```

  Zugriffspunktadresse, Benutzername und Passwort erhalten Sie bei Ihrem Mobilfunkanbieter.

2 Wählen Sie aus der Liste vorgegebener Mobilfunkanbieter den Betreiber aus, mit dessen Hilfe der Zugang zum Internet erfolgen soll. Führen Sie dazu den folgenden Befehl aus:

```
inet usb-modem set provider <Anbietername>
```

Als Anbieternamen können Sie Folgendes angeben:

- Namen der Anbieter, die standardmäßig definiert sind: `vodafone`, `verizon`.
- Namen der Anbieter, die manuell hinzugefügt wurden.

3 Wenn die SIM-Karte durch eine PIN geschützt ist, geben Sie die PIN mit Hilfe des folgenden Befehls an:

```
inet usb-modem set pin <PIN>
```

Um Verwenden der PIN abzubrechen, benutzen Sie den Befehl:

```
inet usb-modem reset pin
```

4 Um das Internet über ein mobiles Netzwerk zuzugreifen, verbinden Sie das 3G-Modem an den USB Port des Computers nach BIOS geladen wurde.

Hinweis. Bei Verwendung einiger Modelle von 3G-Modems können ab dem Zeitpunkt des Modem-Anschlusses bis zum Aufbau einer aktiven Verbindung einige Minuten vergehen.

Beispiele für Befehle:

```
inet usb-modem add provider xtelecom
inet usb-modem set connection address internet.xtelecom.ru
inet usb-modem set phone *99***1#
inet usb-modem set user xtelecom
inet usb-modem set password xtelecom
inet usb-modem set pin 1234

inet usb-modem mode on
```

Statusinformationen über ViPNet Coordinator HW/VA anzeigen

Benutzen Sie die folgenden Befehle, um den Status und die unterschiedlichen Komponenten von ViPNet Coordinator HW/VA zu überprüfen und die Logdateien anzuzeigen:

- Verwenden Sie zum Anzeigen von Informationen über die Nutzung des Arbeitsspeichers den Befehl:

  ```
  machine show memory
  ```

- Zum Anzeigen der Parameter der Netzwerkadapter führen Sie den folgenden Befehl aus:

  ```
  inet show interface
  ```

- Zum Anzeigen der Konfigurationsdatei des Netzwerkadapters führen Sie den folgenden Befehl aus:

  ```
  iplir show config <Name des Netzwerkadapters>
  ```

- Zum Überprüfen der Verbindung zu einem offenen Knoten führen Sie den folgenden Befehl aus:

  ```
  inet ping <IP-Adresse>
  ```

- Zum Überprüfen der Verbindung zu einem geschützten ViPNet Knoten führen Sie den folgenden Befehl aus:

  ```
  iplir ping <ViPNet Netzwerkknoten-ID>
  ```

  Bei der Eingabe der ID stehen dem Benutzer die Features Autovervollständigung und Tipps zur Seite. Tipp-Daten werden aus der Verbindungsliste des ViPNet Coordinator HW/VA-Knotens bezogen.

- Zum Anzeigen der Konfigurationsdatei der Firewall führen Sie den folgenden Befehl aus:

  ```
  iplir show config firewall
  ```

- Führen Sie zum Anzeigen der Logdatei registrierter IP-Pakete den folgenden Befehl aus:

  ```
  iplir view
  ```

- Verwenden Sie zum Anzeigen des Systemprotokolls (s. Parameter für Systemprotokoll einstellen auf S. 12), der sich auf dem lokalen Laufwerk befindet, den Befehl: `machine show logs`

2

Stabilerer Zugang zu Netzwerkressourcen durch Verwendung alternativer Datenübertragungskanäle

Über Verwendung alternativer Datenübertragungskanäle

Wenn Sie den Zugang zu einem Netzwerk oder zu einer Webressource verbessern möchten, können Sie zwei unabhängige Kanäle einrichten, die sich im Fall von Störungen gegenseitig dublieren oder einen Lastenausgleich des Traffics durchführen können. Sie können z. B. zwei Anbieter für den Internetzugang verwenden, um mögliche Verbindungsstaus und Ausfälle zu reduzieren. Dieser Ansatz ermöglicht es, eine gleichmäßige Verteilung des Traffics durchzuführen und einen zusätzlichen Reservekanal für Internetverbindungen zu verwenden. Die Verwendung alternativer Kanäle wird vom *loadbalancer* gesteuert.

Hinweis. Alternative Kanäle können ausschließlich für nicht verschlüsselte (nicht-VPN) Verbindungen verwendet werden. Gegenwärtig unterstützt der Dienst zwei alternative Kanäle vom Typ Ethernet.

Die Verwendung alternativer Kanäle kann in den folgenden Modi aktiviert werden:

- Kanalwechselmodus: in diesem Fall wird einer der zwei Kanäle als Primärkanal festgelegt. Wenn dieser Kanal ausfällt, dann wird der Traffic über den alternativen Kanal weitergeleitet. In diesem Fall wird die Verbindung über den Primärkanal regelmäßig überprüft. Sobald der Primärkanal wieder betriebsbereit ist, wird der Traffic wieder zu diesem Kanal umgeleitet.

- Traffic-Lastenausgleichsmodus. In diesem Fall wird der Traffic gemäß den von Ihnen festgelegten Prioritäten auf die zwei Kanäle aufgeteilt. Sie können z. B. für einen der Kanäle eine Traffic-Rate von 80 % definieren. Der Rest des Traffics wird über den anderen Kanal weitergeleitet. Wenn einer der Kanäle ausfällt, wird der Traffic zu 100 % über den störungsfreien Kanal solange weitergeleitet, bis der gestörte Kanal wieder betriebsbereit ist.

Wenn die Verwendung alternativer Kanäle aktiviert ist, überprüft der Dienst *loadbalancer* regelmäßig die Verfügbarkeit der beiden Kanäle, indem er versucht, auf die Test-IP-Adresse zuzugreifen. Der Dienst versucht dabei, mit Hilfe einer ICMP-Anfrage auf die Testadresse eines der beiden Kanäle abwechselnd zuzugreifen. Wenn der Zugriff auf die Testadresse über einen bestimmten Kanal erfolgreich verläuft, dann bedeutet das, dass der entsprechende Kanal aktiv ist. Wenn der Zugriff fehlschlägt, dann wird der entsprechende Kanal als fehlerhaft eingestuft. Wenn beide Kanäle ausfallen, dann setzt der Dienst seine regelmäßigen Überprüfungen

trotzdem fort. Sobald einer der Kanäle wieder betriebsbereit ist, wird der Traffic automatisch über diesen Kanal weitergeleitet.

Beim Konfigurieren des Dienstes *loadbalancer* müssen Sie eine Test-IP-Adresse festlegen, die über beide Kanäle erreichbar sein sollte, sobald diese Kanäle verfügbar sind.

Befehle zum Steuern des Dienstes loadbalancer

Alle Befehle, die zum Steuern des Dienstes *loadbalancer* zur Verfügung stehen, sind nachfolgend aufgeführt:

```
service loadbalancer
```

- start startet den Dienst *loadbalancer*.
- stop stoppt den Dienst *loadbalancer*.
- `mode [on|off]` aktiviert oder deaktiviert den automatischen Start des Dienstes während des Betriebssystemstarts.
- `add provider <Kanalname>` fügt einen neuen Kanal (Provider) mit dem angegebenen Namen hinzu.
- `delete provider <Kanalname>` entfernt den angegebenen Kanal (Provider).
- `set`
  - `mode [failover|balancing]` legt fest, ob der Dienst *loadbalancer* im Kanalwechselmodus oder im Traffic-Lastenausgleichsmodus arbeitet (s. Über Verwendung alternativer Datenübertragungskanäle auf S. 21).
  - `provider <Kanalname> gateway <IP-Adresse>` legt die IP-Adresse des Standardgateways beim Verwenden des angegebenen Kanals fest.
  - `provider <Kanalname> interface <Netzwerkadapter>` legt den Netzwerkadapter des Knotens ViPNet Coordinator HW/VA beim Verwenden des angegebenen Kanals fest.
  - `provider <Kanalname> weight <Lastgewicht>` legt das Lastgewicht des entsprechenden Kanals fest. Dieses Lastgewicht (ganzzahliger Wert zwischen 1 und 10) wird im Traffic-Lastenausgleichsmodus verwendet und bestimmt den jeweiligen Anteil jedes Kanals am gesamten weitergeleiteten Traffic.

    Das Verhältnis der Lastgewichte der beiden Kanäle bestimmt ihren jeweiligen Anteil am übermittelten Traffic. Wenn Sie den beiden Kanälen z. B. die Gewichte 2 und 4 zuweisen, dann wird ein Drittel des Traffics über den ersten Kanal und der Rest über den zweiten Kanal geleitet. Wenn Sie die Gewichte 3 und 6 zuweisen, bleibt das Verhältnis der Lastenverteilung gleich, d. h. ein Drittel zu zwei Drittel.

- `testip <IP-Adresse>` legt die Test-IP-Adresse (s. Über Verwendung alternativer Datenübertragungskanäle auf S. 21) fest.
- `polltime <Zeit>` legt das Abrufintervall (zwischen 10 und 600 Sekunden) für die Testadresse fest. Das Standardintervall beträgt 10 Sekunden.
- `provider <Kanalname>` default legt den Standardkanal fest. Dieser Befehl wird im Kanalwechselmodus verwendet. Wenn der Standardkanal verfügbar ist, wird der gesamte Traffic über diesen Kanal geleitet.

- `show` zeigt den Status, den Modus, die Kanaleigenschaften und andere Einstellungen des Lastenausgleichsdienstes an.

- `nat`
  - `add localnet <Netzwerk_1,Netzwerk_2,...>` legt die Liste der internen Netzwerke fest, für welche der Knoten ViPNet Coordinator HW/VA Adressenübersetzung (NAT) durchführen wird. Die Netzwerke werden durch das Angeben ihrer IP-Adressen im CIDR-Format hinzugefügt (z. B. 192.168.0.0/24).
  - `delete localnet <Netzwerk_1,Netzwerk_2,...>` deaktiviert NAT für die angegebenen internen Netzwerke.

3

Konfiguration der integrierten Dienste

Parameter für Netzwerkdienste einstellen

Auf einem Computer mit ViPNet Coordinator HW/VA können mehrere Netzwerkdienste ausgeführt werden, die in einem lokalen Netzwerk von Nutzen sind und den Betrieb eines kleinen Firmennetzwerks erleichtern.

Parameter des Wi-Fi-Zugriffspunkts einstellen

Wenn der Computer über einen Wi-Fi-Adapter verfügt (wird als Netzwerkadapter mit dem Namen `wlan0` aufgelistet), kann ViPNet Coordinator HW/VA als Wi-Fi-Zugriffspunkt verwendet werden.

Wenn der Wi-Fi-Zugriffspunkt aktiviert ist, wird dem Netzwerkadapter wlan0 automatisch die IP-Adresse 192.168.20.1 zugewiesen. Auf diesem Adapter wird ein DHCP-Server gestartet. Der DHCP-Server verfügt über fixe Parameter, die nicht vom Benutzer geändert werden können:

- Bereich der zu verteilenden IP-Adressen: 192.168.20.2–192.168.20.20.
- Adresse des DNS- und NTP-Servers: 192.168.20.1 (Adresse des Netzwerkadapters wlan0).

Hinweis. Wenn die Möglichkeit von Verbindungen zwischen Geräten, die mit dem Wi-Fi-Netzwerk verbunden sind, und Computern, die an das Ethernet-Netzwerk angeschlossen sind, sichergestellt werden soll, dann sollten in der Konfigurationsdatei der ViPNet Coordinator HW/VA-Firewall Transitregeln definiert werden, die den Durchlass von IP-Paketen zwischen diesen beiden Netzwerken erlauben.

Führen Sie die folgenden Schritte aus, um ViPNet Coordinator HW/VA als Wi-Fi-Zugriffspunkt einzustellen:

1. Schalten Sie den Netzwerkadapter wlan0 mit Hilfe des folgenden Befehls in den Zugriffspunkt-Modus um (ist standardmäßig eingestellt):

   ```
   inet wifi role access-point
   ```

2. Geben Sie den Namen Ihres Wi-Fi-Netzwerks und den Authentisierungsmodus für die Netzwerkbenutzer an. Benutzen Sie dazu einen der folgenden Befehle:

- Wenn keine Authentifizierung im Netzwerk erforderlich ist, führen Sie den folgenden Befehl aus:

  ```
  inet wifi access-point ssid <Netzwerkname> authentication open
  ```

- Wenn für die Authentifizierung ein Passwort verwendet werden soll, dann wählen Sie den Authentifizierungsmodus WPA-PSK oder WPA2-PSK und definieren Sie ein Passwort. Führen Sie dazu den folgenden Befehl aus:

  ```
  inet wifi access-point ssid <Netzwerkname> authentication {wpa-psk |
  wpa2-psk} passphrase <Passwort>
  ```

  Das angegebene Passwort sollte allen Benutzern, die sich zu Ihrem Wi-Fi-Netzwerk verbinden, mitgeteilt werden.

3 Wenn für Ihr Wi-Fi-Netzwerk ein Funknetzwerk-Standard festgelegt werden soll, führen Sie den folgenden Befehl aus:

```
net wifi server hwmode {a | b | g}
```

Es werden folgende Standards unterstützt:

- a – IEEE 802.11a — 5 GHz, Verbindungsgeschwindigkeit bis 4 MBit/s.
- b – IEEE 802.11b — 2,4 GHz, Verbindungsgeschwindigkeit bis 11 MBit/s.
- g – IEEE 802.11g — 2,4 GHz, Verbindungsgeschwindigkeit bis 54 MBit/s (standardmäßig eingestellt).

4 Wenn die Nummer des verwendeten Wi-Fi-Kanals angegeben werden soll, führen Sie den folgenden Befehl aus:

```
inet wifi server channel <Kanalnummer>
```

Standardmäßig wird Kanal Nummer 1 verwendet, zulässig sind Nummern von 1 bis 14.

5 Aktivieren oder deaktivieren Sie den Netzwerkadapter wlan0 mit Hilfe des folgenden Befehls:

```
inet wifi mode {on | off}
```

Parameter des DHCP-Servers einstellen

ViPNet Coordinator HW/VA kann im lokalen Netzwerk als DHCP-Server auftreten (s. DHCP-Server auf S. 84). Wenn der Netzwerkknoten mit installiertem ViPNet Coordinator HW/VA als Wi-Fi-Zugriffspunkt eingesetzt wird (s. Parameter des Wi-Fi-Zugriffspunkts einstellen auf S. 26), oder wenn sich zu diesem Netzwerkknoten Geräte über das Bluetooth-Protokoll verbinden, dann wird auf dem entsprechenden Netzwerkadapter automatisch ein DHCP-Server gestartet, dessen Parameter nicht vom Benutzer geändert werden können.

Hinweis. Wenn Sie den integrierten DHCP-Relay in ViPNet Coordinator HW/VA aktivieren möchten, wenden Sie sich an den Abschnitt Parameter des DHCP Relay einstellen.

Wenn der DHCP-Server auf einem der Ethernet-Netzwerkadapter gestartet werden soll, müssen die Parameter dieses Servers manuell konfiguriert werden. Führen Sie dazu die folgenden Schritte aus:

1. Geben Sie den Ethernet-Netzwerkadapter, auf welchem der DHCP-Server laufen soll, mit Hilfe des folgenden Befehls an:

   ```
   inet dhcp interface <Netzwerkadaptername>
   ```

2. Geben Sie den IP-Adressbereich für die Verteilung durch den Server mit Hilfe des folgenden Befehls an:

   ```
   inet dhcp range <Start-IP-Adresse> <End-IP-Adresse>
   ```

3. Führen Sie den folgenden Befehl aus, um die IP-Adresse des Standardgateways anzugeben:

   ```
   inet dhcp router <IP-Adresse>
   ```

4. Führen Sie den folgenden Befehl aus, um den automatischen Start des DHCP-Servers beim Laden von ViPNet Coordinator HW/VA zu (de-) aktivieren:

   ```
   inet dhcp mode {on | off}
   ```

   Standardmäßig ist der automatische Start des DHCP-Servers deaktiviert.

   Hinweis. Bevor Sie den DHCP-Server aktivieren oder starten, stellen Sie sicher, dass der DHCP-Relaydienst deaktiviert und gestoppt ist.

5. Führen Sie den folgenden Befehl aus, um den DHCP-Server zu starten bzw. zu stoppen:

   ```
   inet dhcp {start | stop}
   ```

6. Führen Sie den folgenden Befehl aus, um die aktuellen Parameter des DHCP-Servers anzuzeigen:

   ```
   inet show dhcp
   ```

Parameter des DNS-Servers einstellen

ViPNet Coordinator HW/VA kann im lokalen Netzwerk als DNS-Server auftreten (s. DNS-Server auf S. 84). Der eingebaute DNS-Server von ViPNet Coordinator HW/VA leitet die

eingehenden DNS-Anfragen an den übergeordneten DNS-Server um und übermittelt die erhaltenen Antworten an die Clients.

Führen Sie die folgenden Schritte aus, um die Parameter des DNS-Servers einzustellen:

1. Führen Sie den folgenden Befehl aus, um die IP-Adresse des DNS-Servers hinzuzufügen, an welchen ViPNet Coordinator HW/VA die DNS-Anfragen weiterleiten soll:

   ```
   inet dns add <IP-Adresse>
   ```

   Standardmäßig werden die Clientanfragen an die Stamm-DNS-Server umgeleitet.

2. Führen Sie den folgenden Befehl aus, um die Adresse des DNS-Servers aus der Liste zu löschen:

   ```
   inet dns delete <IP-Adresse>
   ```

3. Führen Sie den folgenden Befehl aus, um den automatischen Start des DNS-Servers beim Laden von ViPNet Coordinator HW/VA zu (de-) aktivieren:

   ```
   inet dns mode {on | off}
   ```

   Standardmäßig ist der automatische Start des DNS-Servers aktiviert.

4. Führen Sie den folgenden Befehl aus, um der DNS-Server zu starten oder zu stoppen:

   ```
   inet dns {start | stop}
   ```

5. Führen Sie den folgenden Befehl aus, um die aktuellen Parameter des DNS-Servers anzuzeigen:

   ```
   inet show dns
   ```

Parameter des NTP-Servers einstellen

ViPNet Coordinator HW/VA kann im lokalen Netzwerk als NTP-Server auftreten (s. NTP-Server auf S. 86). Der eingebaute NTP-Server synchronisiert automatisch die Systemzeit mit der Weltzeit, um Clients mit korrekten Zeitwerten versorgen zu können.

Führen Sie die folgenden Schritte aus, um die Parameter des NTP-Servers einzustellen:

1. Führen Sie den folgenden Befehl aus, um die IP-Adresse des NTP-Servers für die Synchronisation der Systemzeit von ViPNet Coordinator HW/VA hinzuzufügen:

   ```
   inet ntp add {IP-Adresse | DNS-Name}
   ```

   Standardmäßig wird für die Synchronisation der Server pool.ntp.org verwendet.

2. Führen Sie den folgenden Befehl aus, um die Adresse des NTP-Servers aus der Liste zu löschen:

   ```
   inet ntp delete {IP-Adresse | DNS-Name}
   ```

3 Führen Sie den folgenden Befehl aus, um den automatischen Start des NTP-Servers beim Laden von ViPNet Coordinator HW/VA zu (de-) aktivieren:

```
inet ntp mode {on | off}
```

Standardmäßig ist der automatische Start des NTP-Servers aktiviert.

4 Führen Sie den folgenden Befehl aus, um der NTP-Server zu starten oder zu stoppen:

```
inet ntp {start | stop}
```

5 Führen Sie den folgenden Befehl aus, um die aktuellen Parameter des NTP-Servers anzuzeigen:

```
inet show ntp
```

Parameter des Bluetooth-Zugangspunkt einstellen

Falls der Computer mit installierter ViPNet Coordinator HW/VA-Software über einen Bluetooth-Adapter verfügt, dann können an diesen Computer unterschiedliche Bluetooth-Geräte angeschlossen werden. Die Tunnelung dieser Geräte ist ebenfalls möglich.

Bei der Anbindung des Geräts wird eine PIN benötigt, die standardmäßig den Wert 4321 hat. Zum Ändern der PIN kann der folgende Befehl benutzt werden:

```
inet bluetooth pin <neuer PIN-Wert>
```

Zum Zeitpunkt der Verbindung wird im System ein Netzwerkadapter mit dem Namen bnep0 erstellt, dem die IP-Adresse 192.168.10.1 zugeordnet wird. Auf diesem Netzwerkadapter wird automatisch ein DHCP-Server gestartet. Der DHCP-Server besitzt fest eingestellte Parameter, die vom Benutzer nicht geändert werden können:

- Bereich der zu verteilenden IP-Adressen: 192.168.10.2–192.168.10.10.
- DNS- und NTP-Server-IP-Adresse: 192.168.10.1 (Adresse des Netzwerkadapters bnep0).

Es kann sich nur jeweils ein Bluetooth-Gerät gleichzeitig mit Hilfe von ViPNet Coordinator HW/VA zum Netzwerk verbinden.

Hinweis. Wenn Verbindungen zwischen Geräten, die über das Bluetooth-Protokoll an ViPNet Coordinator HW/VA angeschlossen sind, und Computern, die an andere Netzwerkadapter angebunden sind, möglich sein sollen, dann müssen in der Konfigurationsdatei der ViPNet Coordinator HW/VA-Firewall Transitregeln erstellt werden, die den Durchlass von IP-Paketen zwischen den betroffenen Netzwerken erlauben.

Proxyserver-Parameter einstellen

Wenn Sie den Internetzugang für Ihre lokalen Benutzer absichern möchten, indem Sie den integrierten Proxyserver aktivieren, dann sollten Sie zunächst die allgemeinen Parameter des Proxyservers konfigurieren. Optional können Sie Inhaltsfilter einstellen und den Antivirusschutz aktivieren. Weitere Informationen dazu s. Inhaltskontrolle konfigurieren (auf S. 33) und Antivirus konfigurieren (auf S. 36).

Die Konfiguration der Basisparameter besteht darin, den externen Netzwerkadapter des Servers, die abzuhörende IP-Adresse und die IP-Adressen der lokalen Netzwerke, die den Proxyserver verwenden sollen, zu definieren. Zusätzlich können Sie den transparenten Modus auf dem Proxyserver aktivieren.

Wenn der Proxyserver als „nicht transparenter“ Proxy auftritt (d. h. der transparente Modus ist deaktiviert), sollten Sie die IP-Adresse und den Port des Proxyservers in Benutzerprogrammen (Webbrowser) aktivieren.

Wenn der Proxyserver im transparenten Modus funktioniert, sind erweiterte Konfigurationen in den Benutzerprogrammen nicht erforderlich. Die Benutzer werden in diesem Fall gezwungen, den Proxyserver zu verwenden. Legen Sie auf Benutzercomputern die IP-Adresse des Proxyservers (ViPNet Coordinator HW/VA-Knoten) als das Standardgateway fest.

Konfiguration der allgemeinen Einstellungen

Führen Sie die folgenden Schritte aus, um die grundlegenden Parameter des Proxyserver einzustellen:

1. Geben Sie die IP-Adressen und Ports an, die vom Proxyserver für den Empfang von Benutzeranfragen verwendet werden:
   - Führen Sie den folgenden Befehl aus, um eine IP-Adresse und einen Port hinzuzufügen:

     ```
     service http-proxy listen-address add <address> <port>
     ```
   - Führen Sie den folgenden Befehl aus, um die Liste der festgelegten IP-Adressen und Ports anzuzeigen:

     ```
     service http-proxy listen-address list
     ```
   - Führen Sie den folgenden Befehl aus, um eine IP-Adresse mitsamt Port wieder zu entfernen:

```
service http-proxy listen-address delete <address> <port>
```

Achtung! Für den Empfang von Anfragen sollten Netzwerkadapter mit statischen IP-Adressen verwendet werden. Bei Änderungen von IP-Adressen der Netzwerkadapter sollte der Proxyserverdienst gestoppt, die aktuellen IP-Adressen als Adressen für Verbindungen festgelegt und der Proxyserver erneut gestartet werden.

2 Geben Sie die externe IP-Adresse von ViPNet Coordinator HW/VA an, die für den Zugang zum Internet verwendet wird. Führen Sie dazu den folgenden Befehl aus:

```
service http-proxy external-address set <IP-адрес>
```

Führen Sie den folgenden Befehl aus, um die festgelegte externe IP-Adresse anzuzeigen:

```
service http-proxy external-address show
```

3 Definieren Sie die Liste der Netzwerke, für welche die Benutzung des Proxyservers erlaubt werden soll. Standardmäßig wird die Verwendung des Proxyservers für alle privaten Netzwerke (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) erlaubt.

- Führen Sie den folgenden Befehl aus, um die IP-Adresse eines Netzwerks hinzuzufügen:

  ```
  service http-proxy allow network add <Netzwerkadresse>/<Subnetz-Präfixlänge >
  ```

  Beispiel:

  ```
  service http-proxy allow network add 192.168.10.0/24
  ```

- Führen Sie den folgenden Befehl aus, um die Liste der festgelegten Netzwerke anzuzeigen:

  ```
  service http-proxy allow network list
  ```

- Führen Sie den folgenden Befehl aus, um die IP-Adresse eines Netzwerks wieder aus der Liste zu löschen:

  ```
  service http-proxy allow network delete <Netzwerkadresse>
  ```

4 Falls erforderlich, legen Sie die Cache-Größe des Proxyservers mit Hilfe des folgenden Befehls fest:

```
service http-proxy cache <Größe>
```

Die Cache-Größe wird in Megabytes angegeben, der Standardwert beträgt 256 MB. Der Cache wird für die Speicherung von Daten verwendet, die von den Benutzern häufig angefragt werden.

5 Führen Sie den folgenden Befehl aus, um den Betrieb des Proxyservers im transparenten Modus zu (de-)aktivieren:

```
service http-proxy transparent mode {on | off}
```

Achtung! Beim Aktivieren des transparenten Modus werden in der Konfigurationsdatei der Firewall automatisch Regeln der statischen Adressenübersetzung erstellt. Beim Deaktivieren des transparenten Modus werden diese Regeln wieder automatisch entfernt.

Wenn Sie eigene Regeln der Adressenübersetzung definiert haben, dann sollten Sie nach der Deaktivierung des transparenten Modus sicherstellen, dass die von Ihnen angelegten Regeln noch intakt sind.

6 Führen Sie den folgenden Befehl aus, um den automatischen Start des Proxyservers beim Laden von ViPNet Coordinator HW/VA zu (de-) aktivieren:

```
service http-proxy mode {on | off}
```

7 Führen Sie den folgenden Befehl aus, um den Proxyserver-Dienst umgehend zu starten:

```
service http-proxy start
```

Hinweis. Vor dem Start des Proxyservers sollten die IP-Adresse und der Port für den Empfang von Benutzer-Verbindungsanfragen sowie die externe IP-Adresse von ViPNet Coordinator HW/VA definiert werden.

Führen Sie den folgenden Befehl aus, um den Proxyserver-Dienst zu stoppen:

```
service http-proxy stop
```

Hinweis. Damit für offene Knoten der Zugang zum Internet über den Proxyserver sichergestellt wird, konfigurieren Sie entsprechende Traffic-Verarbeitungsregeln.

Inhaltskontrolle konfigurieren

Durch Inhaltskontrolle kann der Zugang zu unerwünschten Webressourcen blockiert werden. Eine URL-Datenbank wird dazu verwendet, den Inhalt von Webressourcen zu filtern. Sie können diese Datenbank im Internet oder von einem anderen ViPNet Coordinator HW/VA-Knoten, der als Server für die URL-Datenbank verwendet wird, abrufen.

Die URLs in der Datenbank können unterschiedlichen Inhaltsklassen zugeordnet werden, zum Beispiel „Glücksspiele“, „Shopping“, „Soziale Netzwerke“, u. s. w. Der Webfilter kann den Zugriff auf Webressourcen dieser Inhaltsklassen (unabhängig voneinander) verhindern. Wenn der Benutzer eine URL anfordert, die dem Muster einer verbotenen URL entspricht, wird die

Anforderung abgelehnt und der Benutzer wird darüber informiert, dass die Webseite nicht angezeigt werden kann.

Führen Sie die folgenden Schritte aus, um die Parameter der Inhaltskontrolle zu konfigurieren:

- Führen Sie den folgenden Befehl aus, um die Funktion der Inhaltskontrolle zu (de-)aktivieren:

  ```
  service http-proxy redirector mode{on | off}
  ```

- Geben Sie die Quelle der Adressendatenbank und die Rolle von ViPNet Coordinator HW/VA mit Hilfe des folgenden Befehls an:

  ```
  service http-proxy redirector role {server | client}
  ```

  Wenn als Rolle server definiert ist, wird die Adressendatenbank aus dem Internet geladen. ViPNet Coordinator HW/VA übernimmt dabei die Rolle des Servers, von dem andere ViPNet Coordinator HW/VA-Knoten die Datenbank laden können.

  Wenn als Rolle client definiert ist, dann wird die Adressendatenbank von einem anderen ViPNet Coordinator HW/VA-Knoten geladen. Dieser Knoten übernimmt die Rolle des Servers und aktualisiert die Datenbank mit Daten aus dem Internet.

- Wenn für ViPNet Coordinator HW/VA die Rolle des Adressendatenbank-Clients festgelegt wurde, geben Sie einen anderen ViPNet Coordinator HW/VA-Knoten an, der als Server auftreten soll. Führen Sie dazu den folgenden Befehl aus:

  ```
  service http-proxy redirector client server-address <Adresse von ViPNet Coordinator HW/VA>
  ```

  Sie können einen der nachfolgenden Parameter verwenden, um die Adresse des ViPNet Coordinator HW/VA-Knotens zu definieren:

  - IP-Adresse,
  - Hexadezimal-Id des ViPNet Netzwerkknotens im Format `0xAAAAAAAA`.

- Führen Sie den folgenden Befehl aus, um die Adressendatenbank umgehend zu laden:

  ```
  service http-proxy redirector fetch
  ```

  Die Größe der Datenbank beträgt ungefähr 100 MB.

- Benutzen Sie den folgenden Befehl, um die automatische Aktualisierung der Adressdatenbank einzustellen:

  ```
  service http-proxy redirector schedule fetch <Update-Intervall>
  ```

  Geben Sie einen der folgenden Werte an, um das Update-Intervall für die Datenbank zu bestimmen:

  - `none` – die automatische Aktualisierung wird deaktiviert.

- Zahl von 1 bis 5 – die Datenbank wird ein- bis fünfmal innerhalb von 24 Stunden aktualisiert. Das Update wird dabei in gleichmäßigen Intervallen durchgeführt.

  Wenn Sie das Update so einstellen, dass die Datenbank einmal täglich aktualisiert wird, dann wird das Update täglich um 00.00 Uhr durchgeführt. Wenn Sie das Update so einstellen, dass die Datenbank dreimal innerhalb von 24 Stunden aktualisiert wird, dann wird das Update täglich um 0.00, 8.00 und 16.00 Uhr gestartet.

  Zum Beisiel: `service http-proxy redirector schedule fetch 3`

  Führen Sie zum Anzeigen des Zeitplans für automatische Updates den folgenden Befehl aus:

  ```
  service http-proxy redirector schedule fetch list
  ```

- Legen Sie die Kategorien von Internetobjekten fest, die vom Proxyserver blockiert werden sollen. Führen Sie dazu die nachfolgenden Aktionen aus:

  - Führen Sie den folgenden Befehl aus, um eine Liste aller Kategorien von Internetobjekten anzuzeigen:

    ```
    service http-proxy redirector category list
    ```

    Auf dem Bildschirm wird eine Liste blockierter (Blocked) und erlaubter (Available) Kategorien im folgenden Format angezeigt:

    ```
    Blocked: jobsearch, drugs, violence...
    Available: adv, aggressive, alcohol, anonvpn, automobile/bikes...
    ```

  - Führen Sie den folgenden Befehl aus, um eine Kategorie in der Liste blockierter Kategorien hinzuzufügen:

    ```
    service http-proxy redirector category add <Kategorie>
    ```

  - Führen Sie den folgenden Befehl aus, um eine Kategorie aus der Liste blockierter Kategorien zu entfernen:

    ```
    service http-proxy redirector category delete <Kategorie>
    ```

- Wenn nötig, legen Sie eine Liste von Ausnahmen fest. Dazu gehören Knoten, für welche keine Inhaltskontrolle durchgeführt werden soll. Führen Sie dazu die folgenden Aktionen aus:

  - Führen Sie den folgenden Befehl aus, um eine IP-Adresse in der Liste der Ausnahmen hinzuzufügen:

    ```
    service http-proxy redirector exception add <IP-Adresse>
    ```

  - Führen Sie den folgenden Befehl aus, um die festgelegte Liste der Ausnahmen anzuzeigen:

    ```
    service http-proxy redirector exception list
    ```

  - Führen Sie den folgenden Befehl aus, um eine IP-Adresse aus der Liste der Ausnahmen zu entfernen:

```
service http-proxy redirector exception delete <IP-Adresse>
```

Antivirus konfigurieren

Wenn Sie ViPNet Coordinator HW/VA als Proxeserver verwenden, können Sie Antivirus-Prüfung der Daten, die über das HTTP-Protokoll in beide Richtungen (sowohl in Richtung Benutzer als auch in Richtung Internet, zum Beispiel das Hinzufügen von Anlagen in E-Mail-Nachrichten über die Webschnittstelle) weitergeleitet werden, aktivieren.

Für die Antiviren-Überprüfung des Inhalts von Internetobjekten auf dem Proxyserver kann eines der zwei Programme verwendet werden:

- „Kaspersky Anti-Virus für Proxy Server“: Software, die von der Firma „Kaspersky Lab“ entwickelt wird http://www.kaspersky.com/de/anti-virus_proxy_server. Für den Einsatz von „Kaspersky Anti-Virus für Proxy Server“ sollte eine Lizenz (s. Lizenzdatei für „Kaspersky Anti-Virus“ installieren auf S. 37) erworben und installiert werden.
- Clam Antivirus: frei verfügbare Software (Freeware), die von der Firma Sourcefire entwickelt wird.

Führen Sie die nachfolgenden Aktionen aus, um die Parameter der Antivirus-Prüfung zu konfigurieren:

- Führen Sie den folgenden Befehl aus, um die Antivirus-Datenbank unverzüglich zu laden:

  ```
  service http-proxy antivirus {kav | clamav} fetch
  ```

  Die Größe der Datenbank beträgt ungefähr 100 MB.

- Führen Sie den folgenden Befehl aus, um die automatische Aktualisierung der Datenbank des gewählten Antivirenprogramms zu konfigurieren:

  ```
  service http-proxy antivirus {kav | clamav} schedule fetch <Update-Intervall>
  ```

  Geben Sie einen der folgenden Werte an, um das Update-Intervall für die Datenbank zu bestimmen:

  - `none` – die automatische Aktualisierung wird deaktiviert.
  - Zahl von 1 bis 5 – die Datenbank wird ein- bis fünfmal innerhalb von 24 Stunden aktualisiert. Das Update wird dabei in gleichmäßigen Intervallen durchgeführt.

  Wenn Sie das Update so einstellen, dass die Datenbank einmal täglich aktualisiert wird, dann wird das Update täglich um 00.00 Uhr durchgeführt. Wenn Sie das Update so einstellen, dass die Datenbank dreimal innerhalb von 24 Stunden aktualisiert wird, dann wird das Update täglich um 0.00, 8.00 und 16.00 Uhr gestartet.

Zum Beispiel: `service http-proxy antivirus clamav schedule fetch 3`

Benutzen Sie zum Anzeigen des Zeitplans für automatische Updates den folgenden Befehl:

```
service http-proxy antivirus {kav | clamav} schedule fetch list
```

- Führen Sie den folgenden Befehl aus, um die Antivirus-Prüfung des Inhalts zu aktivieren:

  ```
  service http-proxy antivirus {kav | clamav} mode on
  ```

  Geben Sie zum Auswählen des Antivirenprogramms, das für die Prüfung verwendet wird, einen der folgenden Werte an:

  - `kav` – „Kaspersky Anti-Virus für Proxy Server“.
  - `clamav` – Clam Antivirus.

  Es können keine zwei Antivirenprogramme gleichzeitig aktiv sein. Wenn eines der Antivirenprogramme aktiviert ist, wird beim Versuch, das andere Programm zu starten, eine entsprechende Fehlermeldung angezeigt.

- Verwenden Sie den folgenden Befehl, um das aktuell aktive Antivirusprogramm zu deaktivieren:

  ```
  service http-proxy antivirus {kav | clamav} mode off
  ```

Lizenzdatei für „Kaspersky Anti-Virus“ installieren

Damit „Kaspersky Anti-Virus für Proxy Server“ auf dem Proxyserver verwendet werden kann, sollte die entsprechende Programmlizenz erworben und installiert werden.

Installieren Sie vor Beginn der Nutzung von „Kaspersky Anti-Virus für Proxy Server“ die dazugehörige Lizenzdatei. Führen Sie dazu die folgenden Schritte aus:

1. Erwerben Sie die Lizenzdatei und kopieren Sie diese auf einen USB-Datenträger.
2. Schließen Sie den USB-Datenträger mit der Lizenzdatei an den Computer an.
3. Führen Sie den folgenden Befehl aus:

   ```
   service http-proxy antivirus key install
   ```

   Auf dem Bildschirm wird eine Liste verfügbarer Lizenzdateien ausgegeben.
4. Geben Sie die Nummer der benötigten Lizenzdatei ein und drücken Sie die **Eingabe**-Taste. Die ausgewährte Lizenzdatei wird nun installiert.
5. Führen Sie den folgenden Befehl aus, um Informationen über die Lizenz anzuzeigen:

   ```
   service http-proxy antivirus key show
   ```

Hinweis. Damit Informationen über die Lizenz angezeigt werden können, sollte die Antivirus-Datenbank geladen sein. Wenn die Datenbank nicht geladen ist, benutzen Sie den Befehl `service http-proxy antivirus fetch`.

6 Führen Sie den folgenden Befehl aus, um die Lizenzdatei wieder zu entfernen:

```
service http-proxy antivirus key delete
```

Konfiguration des VoIP-Servers

Die Software ViPNet Coordinator HW/VA besitzt einen eingebauten VoIP-Server, mit dessen Hilfe Sie ein firmeninternes IP-Telefoniesystem einrichten können.

Wenn Sie verschlüsselte Sprachkommunikation zwischen mehreren Firmenniederlassungen gewährleisten möchten, installieren Sie in jeder Niederlassung einen VoIP-Server auf Basis von ViPNet Coordinator HW/VA und bauen Sie Verbindungskanäle zwischen diesen Servern auf. Es können auch Trunks für beliebige Drittanbieter-VoIP-Server erstellt werden. Trunks ermöglichen es den Benutzern unterschiedlicher VoIP-Server, sich gegenseitig anzurufen.

Der VoIP-Server unterstützt das SIP-Protokoll, weswegen für Verbindungen zum Server beliebige softwarebasierte SIP-Clients oder SIP-Telefongeräte verwendet werden können. Dabei sollten folgende Bedingungen beachtet werden:

- Softwarebasierte SIP-Clients sollten auf geschützten oder getunnelten Knoten installiert werden.
- SIP-Telefongeräte sollten vom ViPNet Coordinator HW/VA-Knoten getunnelt werden.
- Damit SIP-Clients, die vom ViPNet Coordinator HW/VA-Knoten getunnelt werden, Verbindungen zum Server aufbauen können, sollten Filterregeln für den offenen Traffic konfiguriert werden (s. Konfiguration der Filterregeln für offene IP-Pakete auf S. 61), die eingehende Verbindungen von getunnelten SIP-Clients über das TCP- und UDP-Protokoll auf Port 5060 erlauben.
- Getunnelte SIP-Clients und geschützte SIP-Clients sollten unterschiedliche Netzwerkadapter von ViPNet Coordinator HW/VA benutzen.

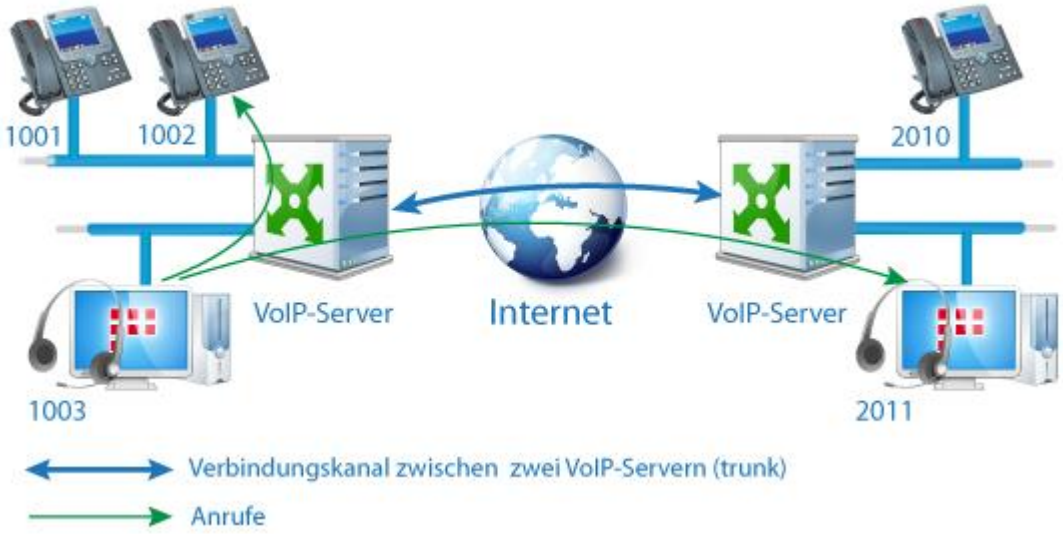

Abbildung 1: Verwendung des integrierten VoIP-Servers

Führen Sie die folgenden Schritte aus, um VoIP-Serverparameter zu konfigurieren:

1. Wechseln Sie zur Konfiguration der VoIP-Serverparameter in den Administratormodus. Führen Sie dazu den Befehl `enable` aus und geben Sie das Passwort des Netzwerkknoten-Administrators ein.

2. Geben Sie den Netzwerkadapter von ViPNet Coordinator HW/VA an, zu dem sich SIP-Clients verbinden sollen. Führen Sie dazu den folgenden Befehl aus:

   ```
   service sip listen internal <Netzwerkadaptername>
   ```

   Hinweis. Führen Sie zum Anzeigen einer Liste aller Netzwerkadapter von ViPNet Coordinator HW/VA den folgenden Befehl aus, ohne den Adapternamen anzugeben: `service sip listen internal`.

   Wenn der angegebene Netzwerkadapter über keine IP-Adresse verfügt, wird eine Fehlermeldung angezeigt. Wenn der VoIP-Serverdienst gestartet ist, sollte er nach dem Ausführen dieses Befehls neu gestartet werden.

3. Registrieren Sie die Telefonnummern der Benutzer auf dem Server:

   - Zum Hinzufügen einer Telefonnummer führen Sie den folgenden Befehl aus:

     ```
     service sip phone add number <Telefonnummer> name <Vorname> surname <Nachname> password <Passwort>
     ```

     Die Telefonnummer sollte aus vier Ziffern bestehen. Zum Beispiel:

```
service sip phone add number 1015 name Max surname Mustermann password
qwerty
```

Wenn die Nummer, die Sie hinzufügen möchten, bereits existiert, wird eine Meldung mit dem Vorschlag angezeigt, die Daten des entsprechenden Benutzers entweder zu ersetzen oder unverändert zu lassen.

- Zum Löschen einer Telefonnummer führen Sie den folgenden Befehl aus:

```
service sip phone delete <Telefonnummer>
```

4 Wenn nötig, definieren Sie die Kanäle für Verbindungen mit anderen VoIP-Servern:

- Geben Sie den Netzwerkadapter von ViPNet Coordinator HW/VA an, zu dem sich entfernte VoIP-Server verbinden sollen. Führen Sie dazu den folgenden Befehl aus:

```
service sip listen external <Adaptername>
```

Hinweis. Führen Sie zum Anzeigen einer Liste aller Netzwerkadapter von ViPNet Coordinator HW/VA den folgenden Befehl aus, ohne den Adapternamen anzugeben: `service sip listen external`.

Wenn der angegebene Netzwerkadapter über keine IP-Adresse verfügt, wird eine Fehlermeldung angezeigt. Wenn der VoIP-Serverdienst gestartet ist, sollte er nach dem Ausführen dieses Befehls neu gestartet werden.

- Führen Sie den folgenden Befehl aus, um ein Verbindungskanal zu einem Remote-VoIP-Server zu erstellen:

```
service sip trunk add name <Servername> address <IP-Adresse des
Servers> local <lokale Nummern> remote <Remote-Nummern>
```

Lokale Nummern repräsentieren hier Telefonnummern, die auf Ihrem VoIP-Server registriert sind und für Benutzer des Remote-Servers zugänglich sein sollen. Remote-Nummern stellen Telefonnummern dar, die auf dem Remote-VoIP-Server registriert sind und für Benutzer Ihres Servers zugänglich sein sollen.

Die Telefonnummern sollten mit Hilfe einer Maske angegeben werden, zum Beispiel:

```
service sip trunk add name RemoteVoIP address 214.56.112.47 local 1XXX
remote 2XXX
```

- Führen Sie den folgenden Befehl aus, um das Verbindungskanal zum Remote-Server zu löschen:

```
service sip trunk delete <Servername>
```

5 Führen Sie den folgenden Befehl aus, um das automatische Starten des VoIP-Servers beim Laden von ViPNet Coordinator HW/VA zu (de-)aktivieren:

```
service sip mode {on | off}
```

6 Wenn Sie den VoIP-Serverdienst umgehend starten möchten, benutzen Sie den Befehl:

```
service sip start
```

Verwenden Sie zum Stoppen des Proxyserver-Dienstes den Befehl:

```
service sip stop
```

Benutzen Sie die folgenden Befehle, um VoIP-Serverparameter anzuzeigen:

- Geben Sie den folgenden Befehl ein, um Informationen über den Status des VoIP-Dienstes anzuzeigen:

  ```
  service show sip
  ```

- Geben Sie den folgenden Befehl ein, um eine Liste aller zu diesem Zeitpunkt verbundenen Benutzer anzuzeigen:

  ```
  service sip phone active
  ```

- Geben Sie den folgenden Befehl ein, um eine Liste aller auf dem Server registrierten Telefonnummern anzuzeigen:

  ```
  service sip phone list
  ```

- Geben Sie den folgenden Befehl ein, um eine Liste aller konfigurierten Verbindungskanäle zu Remote-Servern anzuzeigen:

  ```
  service sip trunk list
  ```

Konfiguration des IPsec-Gateways

In Unternehmensnetzwerken ist es oft erforderlich, die Verbindungen zu Remotenetzwerken oder -Knoten zu schützen. Beispiel: im Unternehmensnetzwerk ist ein Anwendungsserver installiert, der über einen abgesicherten Kanal aus dem Internet zugänglich sein soll. Diese Aufgabe kann nicht immer mit Hilfe der ViPNet Technologie gelöst werden. Es ist zum Beispiel nicht möglich, ViPNet Software auf mobile Geräte zu installieren.

Bei Verwendung von ViPNet Coordinator HW/VA kann der Traffic mittels Verschlüsselung über das IPsec-Protokoll geschützt werden. In diesem Fall tritt ViPNet Coordinator HW/VA als ein ViPNet IPsec-Gateway auf. ViPNet Coordinator HW/VA unterstützt zwei Typen von IPsec-Verbindungen: Site-to-Site (s. Verbindungen über einen geschützten IPsec-Kanal auf S. 44) und Client-to-Site (s. Einrichtung des Zugangs mobiler Geräte zu Unternehmensressourcen über einen geschützten IPsec-Kanal auf S. 49). In beiden Fällen unterstützt ViPNet Coordinator HW/VA die Authentifizierung über Pre-Shared Key (PSK) oder über ein Zertifikat (RSA).

Achtung! Wenn Sie einen ViPNet Coordinator HW/VA als IPsec-Gateway verwenden, dann sollte eine öffentliche statische IP-Adresse zur Verfügung stehen. Deswegen kann ein ViPNet Coordinator HW/VA nicht als IPsec-Gateway bereitgestellt werden, wenn er sich hinter einer dynamischen NAT befindet.

Wenn Sie PSK-Authentifizierung verwenden möchten, empfehlen wir ausdrücklich, IPsec-Verbindungseinstellungen in ViPNet Network Manager zu konfigurieren (s. Dokument „ViPNet Coordinator HW/VA. Administratorhandbuch“). RSA-Authentifizierung wird in ViPNet Network Manager nicht unterstützt.

Achtung! Wenn Sie sich dafür entscheiden, IPsec-Verbindungen mit Hilfe der Befehlszeile von ViPNet Coordinator HW/VA zu konfigurieren, dann sollten Sie keine Änderungen an den IPsec-Einstellungen des betroffenen Knotens in ViPNet Network Manager vornehmen. Anderenfalls gehen die in der Befehlszeile vorgenommenen Änderungen an den Einstellungen verloren, sobald Sie die Schlüssel an den ViPNet Coordinator HW/VA-Knoten absenden.

Gehen Sie wie folgt vor, um eine IPsec-Verbindung über die Befehlszeilenschnittstelle von ViPNet Coordinator HW/VA zu konfigurieren:

1. Stellen Sie sicher, dass die IPsec-Gateway-Funktion für den betroffenen ViPNet Coordinator HW/VA-Knoten in ViPNet Network Manager deaktiviert ist (s. Dokument „ViPNet Coordinator HW/VA. Administratorhandbuch“).
2. Versenden Sie die Schlüssel für den betroffenen ViPNet Coordinator HW/VA-Knoten in ViPNet Network Manager.
3. Konfigurieren Sie eine Site-to-Site (s. Verbindungen über einen geschützten IPsec-Kanal auf S. 44) oder Client-to-Site (s. Einrichtung des Zugangs mobiler Geräte zu Unternehmensressourcen über einen geschützten IPsec-Kanal auf S. 49) IPsec-Verbindung in der Befehlszeilenschnittstelle von ViPNet Coordinator HW/VA.
4. Aktivieren Sie nicht die IPsec-Gateway-Funktion in ViPNet Network Manager. Anderenfalls gehen die durchgeführten IPsec-Einstellungen verloren.

Verbindungen über einen geschützten IPsec-Kanal

Nehmen wir an, in einer Firma wurde aus Datenschutzgründen das ViPNet VPN-Netzwerk eingerichtet. Die Organisation kooperiert mit einer anderen Firma, in welcher keine ViPNet Technologie zum Einsatz kommt. Es soll nun ein geschützter Verbindungskanal zwischen den Geschäftsstellen dieser beiden Betriebe eingerichtet werden.

Für die Lösung dieser Aufgabe kann die Verschlüsselung des Traffics zwischen den beiden Geschäftsstellen mit Hilfe des IPsec-Protokolls konfiguriert werden. Die IPsec-Technologie ermöglicht es, zwei entfernte Netzwerke durch einen geschützten Kanal miteinander zu verbinden. Die Tunnelung und die Verschlüsselung des Traffics werden dabei auf speziell dafür konfigurierten Gateways, die sich in beiden Netzwerken befinden, durchgeführt. Auf Seiten des ViPNet Netzwerks sollte ViPNet Coordinator HW/VA als IPsec-Gateway verwendet werden. Auf Seiten des entfernten Netzwerks kann diese Funktion von anderen Geräten übernommen werden, zum Beispiel von Cisco-Geräten oder von einem Linux-, FreeBSD- oder Windows Server.

Achtung! Zwischen zwei ViPNet Coordinator HW/VA-Knoten, die innerhalb eines Netzwerks befinden, ist die Einrichtung eines geschützten IPSec-Kanals nicht möglich.

Das Schema der geschützten Interaktion zweier Netzwerke unter Verwendung der IPsec-Technologie wird in der folgenden Abbildung vorgestellt.

Abbildung 2: Aufbau von Verbindungen über das IPsec-Protokoll

Der Knoten des Remotenetzwerks 10.0.0.2 baut eine Verbindung zum Knoten 172.16.0.2 im ViPNet Netzwerk auf. Dabei werden die IP-Pakete des Knotens 10.0.0.2 offen zum Gerät „Remote Gate“ übertragen. Auf diesem Gerät wird die Verschlüsselung der IP-Pakete und die Übersetzung der Absender-IP-Adresse in die externe Geräteadresse 87.142.218.3 durchgeführt. Anschließend führt ViPNet Coordinator HW/VA die umgekehrte Aktion durch und leitet die Pakete in ihrem Originalzustand an den Knoten 172.16.0.2 weiter.

Damit IPsec-Verbindungen konfiguriert werden können, sollten auf Remote Gate-Geräten und in ViPNet Coordinator HW/VA die IP-Adressen der interagierenden Netzwerke, die eigenen Geräteadressen, das Verschlüsselungsprotokoll und der Modus der Anmeldung untereinander abgestimmt werden.

Führen Sie in ViPNet Coordinator HW/VA die folgenden Schritte aus, um Verbindungen über das IPsec-Protokoll zu konfigurieren:

1. Definieren Sie mit Hilfe des folgenden Befehls die IP-Adresse des Netzwerkadapters, der für Verbindungen zum entfernten Netzwerk genutzt werden soll:

   ```
   service ipsec listen <IP-Adresse>
   ```

2. Geben Sie mit Hilfe des folgenden Befehls die IP-Adresse des Geräts, der im entfernten Netzwerk die Rolle des IPsec-Gateways übernehmen soll, an:

   ```
   service ipsec site2site peer add <remote IP-Adresse>
   ```

   Hinweis. Beim Hinzufügen der Adresse eines entfernten IPsec-Gateways werden automatisch lokale Regeln des offenen Netzwerks erstellt (s. Konfiguration der Filterregeln für offene IP-Pakete auf S. 61), die Verbindungen zwischen ViPNet Coordinator HW/VA und dem Gateway des Remotenetzwerks über das ESP-Protokoll (IP-Protokollnummer 50) sowie UDP-Verbindungen über Ports 500 und 4500 erlauben.

3. Definieren Sie die Authentifizierungsparameter für das Remotenetzwerk-Gateway.

   Wenn Sie Authentifizierung mittels Pre-Shared Key (PSK) verwenden möchten:

   - Legen Sie den PSK-Authentifizierungstyp fest:

```
service ipsec site2site peer set <remote IP-Adresse> auth type psk
```

- Legen Sie ein Passwort für die Authentifizierung auf dem Remotenetzwerk-Gateway mit Hilfe des folgenden Befehls fest. Das Passwort darf 8 bis 63 Zeichen lang sein.

  ```
  service ipsec site2site peer set <remote IP-Adresse> psk password add
  <Passwort>
  ```

Achtung! Der Passwort darf die folgenden Zeichen nicht enthalten: Fragezeichen (?), umgekehrter Schrägstrich (\), einfaches Anführungszeichen (‘).

Wenn Sie Zertifikatsauthentifizierung (RSA) verwenden möchten:

- Legen Sie den RSA-Authentifizierungstyp fest:

  ```
  service ipsec site2site peer set <remote IP-Adresse> auth type rsa
  ```

- Stellen Sie sicher, dass Sie über das Zertifikat und den privaten Schlüssel des ViPNet Coordinator HW/VA-Knotens, das Zertifikat des Remotegateways, das Stammzertifikat der Zertifizierungsstelle und die Zertifikatsperrliste (CRL) verfügen. Importieren Sie die Zertifikate auf dem ViPNet Coordinator HW/VA-Knoten (s. Importieren von Zertifikaten und CRLs auf S. 53).

- Legen Sie die erforderlichen Zertifikate und CRLs fest:

  ```
  service ipsec site2site peer set <remote IP-Adresse> rsa hostcert
  <Zertifikat Ihres Knotens>
  ```

  ```
  service ipsec site2site peer set <remote IP-Adresse> rsa hostkey
  <Zertifikat Ihres Knotens>
  ```

  ```
  service ipsec site2site peer set <remote IP-Adresse>rsa peercert
  <Zertifikat remotes Gateways>
  ```

  ```
  service ipsec site2site peer set <remote IP-Adresse> rsa cacert
  <Zertifikat der Zertifizierungsstelle>
  ```

  ```
  service ipsec site2site peer set <remote IP-Adresse> rsa crl
  <Zertifikatsperrliste>
  ```

  Wenn Sie beim Ausführen der oben aufgelisteten Befehle eine Liste der verfügbaren Zertifikate anzeigen möchten, lassen Sie den Zertifikatsnamen leer oder verwenden Sie das Zeichen „?“. Führen Sie zum Beispiel den folgenden Befehl aus:

  ```
  service ipsec site2site peer set 87.142.218.3 rsa hostcert
  ```

4 Definieren Sie die Verschlüsselungsparameter, die für den Schutz der Verbindung benutzt werden:

- Geben Sie den Verschlüsselungsalgorithmus mit Hilfe des folgenden Befehls an:

  ```
  service ipsec site2site peer set <remote IP-Adresse> crypo {3des | aes}
  ```

- Geben Sie den Algorithmus für die Berechnung des Hash-Werts mit Hilfe des folgenden Befehls an:

  ```
  service ipsec site2site peer set <remote IP-Adresse> hash <Algorithmus>
  ```

  Zulässige Werte für diesen Parameter: `md5`, `sha1`, `sha256`, `sha384`, `sha512`.

- Legen Sie die Nummer der Diffie-Hellman-Gruppe mit Hilfe des folgenden Befehls fest:

  ```
  service ipsec site2site peer set <remote IP-Adresse> group <Nummer der Gruppe>
  ```

  Zulässige Werte für diesen Parameter: 1, 2, 5, 14, 15, 16, 17, 18.

- Legen Sie die Gültigkeitsdauer der Sitzungsschlüssel in Sekunden:

  ```
  service ipsec site2site peer set <remote IP-Adresse> lifetime <Schlüsselgültigkeitsdauer>
  ```

5 Definieren Sie die Adressen der Netzwerke, zwischen denen ein geschützter Kanal eingerichtet werden soll, mit Hilfe des folgenden Befehls:

```
service ipsec site2site peer set <remote IP-Adresse> spd add localnet <IP-Adresse des lokalen Netzwerks> remotenet <IP-Adresse des entfernten Netzwerks>
```

Lokales Netzwerk und entferntes Netzwerk sind die Netzwerke, die sicher verbunden werden sollen. Die Adressen der Netzwerke werden in Form von Präfixen festgelegt, zum Beispiel 172.16.0.0/24.

Adresse des lokalen Servers ist eine externe IP-Adresse des ViPNet Coordinator HW/VAs. Adresse des entfernten Servers ist eine externe IP-Adresses des IPSec-Servers im entfernten Netzwerk.

6 Führen Sie den folgenden Befehl aus, um den automatischen Start von Diensten, die Verbindungen über das IPSec-Protokoll durchführen, beim Start von ViPNet Coordinator HW/VA zu aktivieren:

```
service ipsec site2site mode on
```

7 Führen Sie den folgenden Befehl aus, um den IPsec-Dienst zu starten:

```
service ipsec site2site start
```

8 Konfigurieren Sie auf dem ViPNet Coordinator HW/VA-Knoten eine Transitregel, die den Traffic zwischen dem Remotenetzwerk und dem lokalen Netzwerk, das Sie in ViPNet Network Manager definiert haben, erlaubt.

Hinweis. Wenn Sie möchten, dass die Computer des Remotenetzwerks auf geschützte ViPNet Knoten im lokalen Netzwerk zugreifen können, dann sollten Sie Firewall-Regeln auf den lokalen Knoten definieren, die den eingehenden Traffic der Remoteknoten erlauben.

---

9 Falls sich der ViPNet Coordinator HW/VA-Knoten hinter einer externen Firewall befindet, konfigurieren Sie auf der Firewall passende Filterregeln. Diese Regeln sollten eingehende UDP-Pakete auf Ports 500 und 4500 erlauben, wenn die lokale IP-Adresse von ViPNet Coordinator HW/VA das Ziel der Pakete ist.

10 Benachrichtigen Sie den Administrator des Remotenetzwerks über die Notwendigkeit, das Routing des Traffics von ViPNet Knoten auf allen Remotenetzwerkknoten inklusive dem Gateway zu konfigurieren. Dabei sollten sichtbare IP-Adressen verwendet werden:

    Sichtbare Adressen der ViPNet Netzwerkknoten werden in der Konfigurationsdatei des privaten Netzwerks definiert (Parameter `accessip` im Bereich `[id]` bei jedem Netzwerkknoten). Verwenden Sie zum Anzeigen der Konfigurationsdatei den Befehl `iplir show config`.

    Sichtbare Adressen der offenen Knoten entsprechen den reellen IP-Adressen dieser Knoten.

11 Stellen Sie sicher, dass die IPsec-Verbindungsparameter auf dem ViPNet Coordinator HW/VA und auf dem Remotenetzwerk-Gateway miteinander kompatibel sind.

12 Führen Sie den folgenden Befehl aus, um die Site-to-Site Verbindungseinstellungen anzuzeigen:

```
service ipsec site2site show
```

Beispiel für Konfiguration der Verbindung (in Übereinstimmung mit dem Schema oben):

```
service ipsec site2site listen 215.67.161.15
service ipsec site2site peer add 87.142.218.3
service ipsec site2site peer set 87.142.218.3 auth type psk
service ipsec site2site peer set 87.142.218.3 psk password add qwertyuiop
service ipsec site2site peer set 87.142.218.3 crypo aes
service ipsec site2site peer set 87.142.218.3 hash md5
service ipsec site2site peer set 87.142.218.3 group 5
service ipsec site2site peer set 87.142.218.3 lifetime 3600
service ipsec site2site peer set 87.142.218.3 spd add localnet
172.16.0.0/24 remotenet 10.0.0.0/24
service ipsec site2site start
service ipsec site2site mode on
```

Einrichtung des Zugangs mobiler Geräte zu Unternehmensressourcen über einen geschützten IPsec-Kanal

Moderne Geschäftsprozesse sehen einen aktiven Einsatz mobiler Endgeräte vor. Mit Hilfe von mobilen Geräten können Mitarbeiter, die sich nicht an ihren Arbeitsplätzen befinden, das betriebliche E-Mail-System, die Möglichkeiten der IP-Telefonie oder andere Ressourcen des Firmennetzwerks nutzen.

Für den gesicherten Zugriff auf firmeninterne Ressourcen, die sich im ViPNet Netzwerk befinden, können die mobilen Endgeräte Apple iPad und iPhone eingesetzt werden. Der Schutz des Traffics wird dabei mit Hilfe einer Kombination der IPSec- und der ViPNet Technologie sichergestellt.

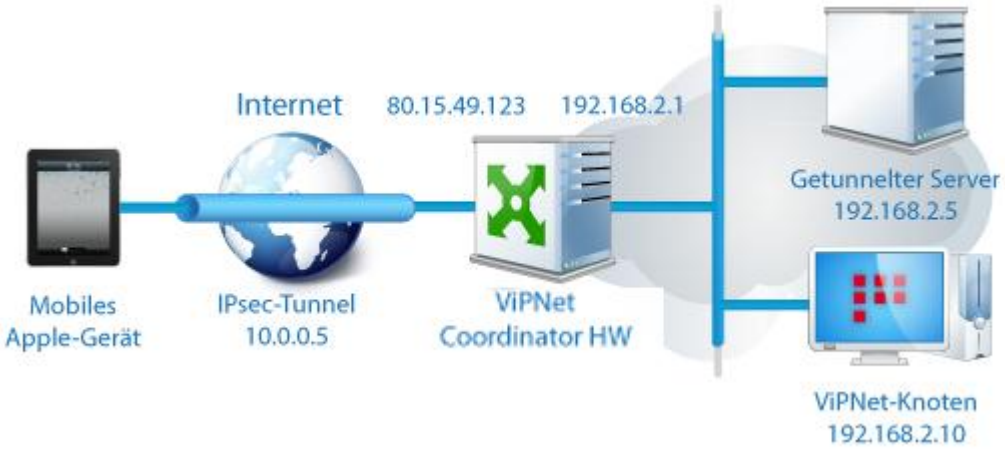

Abbildung 3: Mobiles Apple-Gerät beim Aufbau der Verbindung zum ViPNet Security Gateway

Ein ViPNet Coordinator HW/VA-Knoten wird als Gateway zwischen IPsec und ViPNet eingesetzt und ermöglicht den Zugang mobiler Geräte zu getunnelten und geschützten ViPNet Knoten. Das mobile Gerät baut dabei eine Verbindung zum ViPNet Coordinator HW/VA über das IPsec-Protokoll auf.Es wird ein gesicherter Client-to-Site IPsec-Kanal erstellt und dem mobilen Gerät automatisch eine IP-Adresse aus dem Netzwerkbereich 192.168.30.0/24 zugewiesen. Der Traffic des mobilen Geräts wird vom ViPNet Coordinator HW/VA-Knoten entschlüsselt. Dann wird der unverschlüsselte Traffic entweder zu einem offenen Knoten hinter dem ViPNet Coordinator HW/VA weitergeleitet oder mit ViPNet Schlüsseln verschlüsselt und an einen geschützten ViPNet Knoten übermittelt. Knoten, die sich im geschützten Netzwerk hinter dem ViPNet Coordinator HW/VA befinden, können über ihre IP-Adressen von den mobilen Geräten angesprochen werden.

Die Benutzer der mobilen Geräte, die mit ViPNet Coordinator HW/VA über das IPsec-Protokoll verbunden sind, werden normalerweise in der Lage sein, auf Ressourcen des unternehmensinternen Netzwerks zuzugreifen. Wenn zusätzlich der Zugang mobiler IPsec-

Clients zum Internet eingerichtet werden soll, können Sie dazu den integrierten Proxyserver verwenden oder NAT-Regeln auf dem ViPNet Coordinator HW/VA-Knoten konfigurieren.

ViPNet Coordinator HW/VA unterstützt bis zu 20 gleichzeitige Client-to-Site IPsec-Verbindungen. Darüber hinaus kann die Anzahl der mobilen Clients im ViPNet Netzwerk durch die ViPNet VPN-Lizenz begrenzt sein.

Wenn nötig, können Laptops und Desktopcomputer mit dem Betriebssystem Windows oder Mac OS ebenfalls als IPsec-Clients eingesetzt werden.

Gehen Sie wie folgt vor, um eine standortübergreifende IPsec-Verbindung (Client-to-Site) in ViPNet Coordinator HW/VA zu konfigurieren:

1. Legen Sie die IP-Adresse des Netzwerkadapters, der von IPsec-Clients für den Verbindungsaufbau zum ViPNet Coordinator HW/VA-Knoten verwendet werden soll, mit Hilfe des folgenden Befehls fest:

   ```
   service ipsec listen <IP-Adresse>
   ```

2. Definieren Sie die Authentifizierungsparameter für L2TP-Verbindungen.

   Wenn Sie Authentifizierung mittels Pre-Shared Key (PSK) verwenden möchten:

   - Legen Sie den PSK-Authentifizierungstyp fest:

     ```
     service ipsec client2site peer auth type psk
     ```

   - Definieren Sie ein Passwort für die Authentifizierung auf dem Remotenetzwerk-Gateway mit Hilfe des folgenden Befehls. Das Passwort darf 8 bis 63 Zeichen lang sein.

     ```
     service ipsec client2site peer psk password add <Passwort>
     ```

   

   Achtung! Der Passwort darf die folgenden Zeichen nicht enthalten: Fragezeichen (?), umgekehrter Schrägstrich (\), einfaches Anführungszeichen (‘).

   Wenn Sie Zertifikatsauthentifizierung (RSA) verwenden möchten:

   - Legen Sie den RSA-Authentifizierungstyp fest:

     ```
     service ipsec client2site peer auth type rsa
     ```

   - Stellen Sie sicher, dass Sie über das Zertifikat und den privaten Schlüssel des ViPNet Coordinator HW/VA-Knotens, das Stammzertifikat der Zertifizierungsstelle und die Zertifikatsperrliste (CRL) verfügen. Importieren Sie die Zertifikate auf dem ViPNet Coordinator HW/VA-Knoten (s. Importieren von Zertifikaten und CRLs auf S. 53).

   - Legen Sie die erforderlichen Zertifikate und Zertifikatsperrlisten (CRLs) fest:

```
service ipsec client2site peer rsa hostcert <Zertifikat des Netzwerkknotens>
```

```
service ipsec client2site peer rsa hostkey <Privater Schlüssel des Netzwerkknotens>
```

```
service ipsec client2site peer rsa cacert <Zertifikat der Zertifizierungsstelle>
```

```
service ipsec client2site peer rsa crl <Zertifikatsperrliste>
```

Wenn Sie beim Ausführen der oben aufgelisteten Befehle eine Liste der verfügbaren Zertifikate anzeigen möchten, lassen Sie den Zertifikatsnamen leer oder verwenden Sie das Zeichen „?“. Führen Sie zum Beispiel den folgenden Befehl aus:

```
service ipsec client2site peer rsa hostcert
```

3 Definieren Sie die Verschlüsselungsparameter für den Schutz der Verbindung:

- Legen Sie den kryptografischen Algorithmus mit Hilfe des folgenden Befehls fest:

  ```
  service ipsec client2site peer crypo {3des | aes}
  ```

- Legen Sie den Hashalgorithmus mit Hilfe des folgenden Befehls fest:

  ```
  service ipsec client2site peer hash <Algorithmus>
  ```

  Es können folgende Werte angegeben werden: `md5`, `sha1`, `sha256`, `sha384`, `sha512`.

- Legen Sie die Nummer einer Diffie-Hellman-Gruppe mit Hilfe des folgenden Befehls fest:

  ```
  service ipsec client2site peer group <Gruppennummer>
  ```

  Es können folgende Werte angegeben werden: 1, 2, 5, 14, 15, 16, 17, 18.

- Legen Sie die Gültigkeitsdauer der Sitzungsschlüssel in Sekunden fest:

  ```
  service ipsec client2site peer lifetime <Gültigkeitsdauer der Schlüssel>
  ```

  Es kann ein Wert zwischen 60 und 86400 angegeben werden.

4 Definieren Sie den IP-Adressbereich für Clients, die sich über das IPsec-Protokoll zum ViPNet Coordinator HW/VA verbinden:

```
service ipsec client2site peer range <Start-IP-Adresse>-<End-IP-Adresse>
```

5 Wenn IPsec-Clients auf geschützte ViPNet Netzwerkknoten zugreifen sollen, fügen Sie in ViPNet Network Manager für den ViPNet Coordinator HW/VA-Knoten den zuvor definierten IP-Adressbereich zur Liste der getunnelten IP-Adressen hinzu. Versenden Sie dann Schlüsselupdates an die ViPNet Netzwerkknoten.

6 Wenn nötig, legen Sie die IP-Adresse des DNS-Servers, der von IPsec-Clients verwendet werden soll, mit Hilfe des folgenden Befehls fest:

```
service ipsec client2site dns set <IP-Adresse des DNS-Servers>
```

Standardmäßig wird die IP-Adresse 8.8.8.8 (Google Public DNS) verwendet.

7 Definieren Sie eine Liste von IPsec-Clients, die auf geschützte Ressourcen zugreifen sollen:

- Legen Sie zum Hinzufügen eines IPsec-Clients den Namen und das Passwort für den neuen Benutzer mit Hilfe des folgenden Befehls fest:

  ```
  service ipsec client2site peer user add <Benutzername> password <Benutzerpasswort>
  ```

  

  Achtung! Der Benutzerpasswort darf die folgenden Zeichen nicht enthalten: Fragezeichen (?), umgekehrter Schrägstrich (\), einfaches Anführungszeichen (‘).

- Führen Sie zum Löschen eines IPsec-Clients den folgenden Befehl aus:

  ```
  service ipsec client2site peer user delete <Benutzername>
  ```

- Führen Sie zum Anzeigen der Liste von IPsec-Clients den folgenden Befehl aus:

  ```
  service ipsec client2site peer user list
  ```

8 Wenn Sie für Dienste, die sich über das IPsec-Protokoll verbinden, die Autostart-Funktion aktivieren möchten, führen Sie zum Startzeitpunkt von ViPNet Coordinator HW/VA den folgenden Befehl aus:

```
service ipsec client2site mode on
```

9 Führen Sie den folgenden Befehl aus, um den IPsec-Dienst zu starten

```
service ipsec client2site start
```

10 Leiten Sie die IP-Adresse des ViPNet Coordinator HW/VAs, die Authentifizierungsparameter (Pre-Shared Key oder Zertifikat), die Benutzernamen und Passwörter an diejenigen Benutzer weiter, die den Zugang zu unternehmensinternen Ressourcen benötigen. Die Benutzer sollten dann IPsec-Einstellungen auf ihren mobilen Geräten oder Computern in Übereinstimmung mit den bereitgestellten Daten konfigurieren.

11 Führen Sie den folgenden Befehl aus, um die Site-to-Site-Verbindungseinstellungen anzuzeigen:

```
service ipsec site2site show
```

Hier ein Beispiel für die Konfiguration einer Site-to-Site-Verbindung (gemäß dem oben aufgeführten Schema):

```
service ipsec client2site listen 80.15.49.123
service ipsec client2site peer set 87.142.218.3 auth type psk
service ipsec client2site peer psk password add qwertyuiop
```

```
service ipsec client2site peer crypo aes
service ipsec client2site peer hash md5
service ipsec client2site peer group 5
service ipsec client2site peer lifetime 3600
service ipsec client2site peer range 10.0.0.2-10.0.0.254
service ipsec client2site dns set 192.168.2.2
service ipsec client2site peer user add JohnB password 2jhbff42
service ipsec client2site peer user add MrSmith password 32fra24f
service ipsec client2site mode on
service ipsec client2site start
```

Importieren von Zertifikaten und CRLs

Wenn Sie für IPsec-Verbindungen Zertifikatsauthentifizierung (RSA) konfigurieren möchten, dann sollten Sie zunächst die erforderlichen Zertifikate und Zertifikatsperrlisten (CRLs) in ViPNet Coordinator HW/VA importieren. Wenn Sie für Ihren Knoten kein Zertifikat besitzen, dann können Sie eine Zertifikatsanfrage erstellen und das ausgestellte Zertifikat anschließend importieren.

Zum Anfordern eines Zertifikats für den Knoten:

1. Erstellen Sie einen privaten Schlüssel und eine Zertifikatsanfrage. Führen Sie dazu in der ViPNet Coordinator HW/VA-Befehlsshell den folgenden Befehl aus (geben Sie dabei den erforderlichen Zertifikatsnamen, die Länge des privaten Schlüssels und den Hash-Algorithmus an):

   ```
   service cert request create name <Zertifikatsname> bits <Schlüssellänge>
   digest {md5 | sha1}
   ```

   Für Schlüssellänge können folgende Werte angegeben werden: 1024, 1536, 2048, 3072, 4096.

   Beim Ausführen dieses Befehls werden ein privater Schlüssel und eine Anfragedatei mit dem Namen <Zertifikatsname>_req.pem erstellt.

2. Schließen Sie einen abnehmbaren USB-Datenträger an den Computer an und kopieren Sie die erstellte Anfrage mit Hilfe des folgenden Befehls auf den USB-Datenträger:

   ```
   service cert export <Name der Anfragedatei> via usb
   ```

3. Leiten Sie die Zertifikatsanfrage an Ihre Zertifizierungsstelle weiter. Sie erhalten dann das ausgestellte Zertifikat zusammen mit dem Stammzertifikat der Zertifizierungsstelle und der Zertifikatsperrliste (CRL).

Zum Importieren eines Zertifikats, eines privaten Schlüssels oder einer CRL:

1. Schließen Sie einen USB-Datenträger mit den Dateien, die Sie importieren möchten, an den Computer an.

   Die zulässigen Dateierweiterungen sind .pem (für private Schlüssel), .cer (für DER-verschlüsselte Zertifikate) und .crl (für Zertifikatsperrlisten).

2. Führen Sie in der ViPNet Coordinator HW/VA-Befehlsshell den folgenden Befehl aus:

   ```
   service cert import via usb
   ```

   Es wird eine Liste von Dateien angezeigt, die auf dem USB-Datenträger gefunden wurden.

3. Wählen Sie die Datei aus, die Sie importieren möchten.

Führen Sie den folgenden Befehl aus, um eine Liste der installierten privaten Schlüssel, Zertifikate und Zertifikatsperrlisten (CRL) anzuzeigen:

```
service cert list
```

Führen Sie den folgenden Befehl aus, um ein Zertifikat anzuzeigen:

```
service cert show cert <Zertifikatsname>
```

Konfiguration der integrierten Firewall

Allgemeine Informationen

Die Software ViPNet Coordinator HW/VA verfügt über Möglichkeiten zur Filterung und Übersetzung von Adressen für den offenen (nicht verschlüsselten) IP-Traffic (auf S. 85). Die Verarbeitungsregeln für offene IP-Pakete (s. Konfiguration der integrierten Firewall auf S. 55) und die Dienstparameter der Firewall (s. Konfiguration der Dienstparameter auf S. 57) werden in der Konfigurationsdatei der Firewall gespeichert.

Die Konfigurationsdatei besteht aus mehreren Bereichen, die eine oder mehrere Regeln zur Verarbeitung offener IP-Pakete enthalten. Die Verarbeitungsregeln umfassen folgende Arten von Regeln:

- Antispoofing-Regeln (s. Konfiguration des Antispoofings auf S. 59);
- Filterregeln für IP-Pakete (s. Konfiguration der Filterregeln für offene IP-Pakete auf S. 61);
- Regeln der Adressenübersetzung (s. Konfiguration der Umsetzung der IP-Adressen (NAT) auf S. 70).

Führen Sie im Befehlszeileinterpreter (auf S. 84) den Befehl `iplir config firewall` aus, um die Konfigurationsdatei der Firewall zu editieren.

Daten über Ereignisse, die in Zusammenhang mit der Verarbeitung des IP-Traffics durch die ViPNet Coordinator HW/VA-Firewall stehen, werden in der Logdatei der registrierten IP-Pakete erfasst (s. Logdatei der registrierten IP-Pakete auf S. 74).

Konfiguration der Dienstparameter

Die Dienstparameter der Firewall werden in der Firewall-Konfigurationsdatei im Bereich `[settings]` definiert. Nach dem Anlegen der Konfigurationsdatei enthält der Bereich `[settings]` zunächst keine Parameter, es werden stattdessen Standardwerte verwendet, die weiter unten aufgeführt sind.

Der Bereich `[settings]` enthält folgende Parameter:

- `max-connections` – maximale Anzahl an gleichzeitigen Verbindungen. Es muss berücksichtigt werden, dass die Anzahl der verarbeiteten reellen physikalischen Verbindungen bei nur etwa einem Drittel dieses Werts liegen wird. Der Standardwert beträgt `300000`, das ist der maximal zulässige Wert für diesen Parameter. Wenn die Anzahl an gleichzeitigen Verbindungen eingeschränkt werden soll, muss dieser Wert entsprechend herabgesetzt werden.

- `dynamic-ports` – Portbereich, der für dynamisches NAT verwendet wird. Standardmäßig hat der Parameter den Wert `60000-65000`.

- `connection-ttl-tcp` – Zeitintervall (in Sekunden). Nachdem das letzte Paket, das zu der TCP-Verbindung gehört, registriert wurde, beginnt die Wartezeit. Wenn sie den im Parameter angegebenen Wert überschreitet, wird die Verbindung unterbrochen (time-out). Standardmäßig hat der Parameter den Wert `3600` (60 Min.).

- `connection-ttl-udp` – Zeit (in Sekunden). Nach dem Zeitablauf wird die Verbindung nach der letzten Registrierung eines Pakets, das zu dieser UDP-Verbindung gehört, wegen Zeitüberschreitung (time out) abgebrochen. Standardmäßig ist der Wert des Parameters `300` (`5` Min.).

- `dynamic-timeouts` – aktiviert/deaktiviert den Modus für dynamische Timeouts der Verbindungen (`yes`/`no`). Standardmäßig ist der Wert des Parameters auf `no` gesetzt.

  Der Modus der dynamischen Timeouts wird für die Verhinderung der flood-Angriffe eingesetzt. Er funktioniert wie folgt: wenn die Anzahl der Verbindungen einen bestimmten Anteil vom Maximum erreicht, dann werden die Timeouts aller Verbindungen um einen bestimmten Wert reduziert. Je näher die Anzahl der Verbindungen zum Maximum ist, umso größer ist dieser Wert. Timeouts können aber nur ein bestimmtes Minimum erreichen. Wenn die Anzahl der Verbindungen auf einen bestimmten Anteil von der maximalen Anzahl sinkt, werden die Timeouts auf den normalen Wert zurückgesetzt.

- `cleanup-interval` – Häufigkeit der Entfernung der veralteten Verbindungen (mit abgelaufenen Timeouts). Standardmäßig ist der Wert des Parameters auf `5` gesetzt (Sekunden).

  Große Werte führen dazu, dass die veralteten Verbindungen nicht genau genug (zeitlich) entfernt werden. Kleinere Werte führen zur größeren Prozessorauslastung.

Konfiguration des Antispoofings

Antispoofing-Regeln ermöglichen es, für jeden Netzwerkadapter eine Liste der IP-Adressen zu erstellen, von denen Pakete empfangen werden dürfen. Alle Pakete, die von den Adressen gesendet werden, die nicht in der Liste enthalten sind, werden blockiert. Außerdem werden alle Pakete blockiert, die von Adressen gesendet werden, die als erlaubte Adressen für andere Netzwerkadapter gelten. Wie der Name schon sagt, besteht die Hauptaufgabe des Anti-Spoofings im Schutz gegen das sogenannte Spoofing. Spoofing ist eine Art von Angriffen im Netz, die auf der Fälschung der IP-Adressen basiert. Der Angreifer sendet an einen Netzwerkknoten Pakete, die als Absenderadresse nicht die eigene Adresse enthalten, sondern eine andere Adresse, die dem Netzwerkknoten bekannt ist. Man kann beispielsweise aus dem Internet ein IP-Paket an ein Gateway senden und als Absenderadresse die Adresse eines privaten internen Netzwerks angeben, das auch mit dem Gateway verbunden ist. Dabei kann der Angreifer Zugriff auf bestimmte Dienste bekommen, auf die man nur aus dem internen Netzwerk zugreifen kann. Die Antispoofing-Regeln schließen diese Möglichkeit aus.

Die Antispoofing-Regeln werden im Bereich `[antispoof]` der Firewall-Konfigurationsdatei definiert.

Der Bereich `[antispoof]` enthält folgende Parameter:

- `antispoof` – aktiviert und deaktiviert Antispoofing. Der Parameter kann den Wert `yes` oder `no` haben. Standardmäßig ist der Wert auf `no` gesetzt.
- Parameter mit Namen, die den Namen der Netzwerkadapter entsprechen. Der Wert jedes Parameters ist eine Liste von Adressen, die für diesen Netzwerkadapter erlaubt sind. Die Liste kann aus einzelnen durch Komma getrennten Adressen, Adressbereichen, Adressmasken und Schlüsselwörter bestehen. Alle Adressen in der Liste müssen zu Subnetzen gehören, die mit diesem Netzwerkadapter verbunden sind. In der Liste der Adressen können folgende Schlüsselwörter angegeben werden:
  - `anypublic` – alle Adressen, die im Internet erlaubt sind, d.h. alle Adressen, außer Adressen, die für spezielle Zwecke verwendet werden: für den lokalen Netzwerkadapter (127.0.0.0/8) und für private Netzwerke (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16);
  - `subnet` – gesamtes Subnetz, dem dieser Netzwerkadapter angehört, was durch seine IP-Adresse und die Subnetzmaske bestimmt wird.

    Wenn Antispoofing aktiviert ist, erfolgt bei jedem Start des Steuerungs-Daemons oder bei einer Änderung der Netzwerkeigenschaften eine automatische Erstellung der Liste mit dem Schlüsselwort `subnet`.

Der Bereich `[antispoof]` muss unbedingt alle Netzwerkadapter außer dem lokalen Netzwerkadapter (loopback) enthalten. Der Traffic auf dem lokalen Netzwerkadapter kann nicht gefiltert werden und lässt grundsätzlich alle Pakete durch. Eingehende IP-Pakete aus dem Bereich 127.0.0.0/8 werden auf allen Netzwerkadaptern ViPNet unabhängig von den Einstellungen des Antispoofings blockiert.

Beim Start des Steuerungs-Daemons wird geprüft, ob das Antispoofing aktiviert ist. Wenn es aktiviert ist, wird geprüft, ob alle Netzwerkadapter im Bereich `[antispoof]` eingetragen sind, die dem Steuerungsdämon bekannt sind. Fehlende Netzwerkadapter werden automatisch zum Bereich `[antispoof]` mit dem Wert `subnet` hinzugefügt.

Beispiel des Bereichs `[antispoof]`:

```
[antispoof]
antispoof= yes
eth0= anypublic
eth1= 192.168.1.0/24
```

Antispoofing ist in diesem Beispiel aktiviert und funktioniert folgendermaßen:

- Der Netzwerkadapter `eth0` erhält IP-Pakete von allen IP-Adressen ausgenommen private IP-Adressen (der Netzwerkadapter ist mit dem Internet verbunden);
- Der Netzwerkadapter `eth1` erhält Pakete von Adressen 192.168.1.1 bis 192.168.1.255 (der Netzwerkadapter ist mit dem lokalen Netzwerk verbunden).

Wenn in diesem Beispiel auf den Netzwerkadapter eth0 ein Paket aus dem Internet mit der Absenderadresse aus dem Netzwerk 192.168.1.0/24 oder 192.168.201.0/24 empfangen wird, wird dieses Paket blockiert. Damit wird ein sicherer Schutz vor Spoofing gewährleistet.

Konfiguration der Filterregeln für offene IP-Pakete

Pakete, die nach Antispoofing-Regeln nicht aussortiert wurden, werden mithilfe der Filterregeln weiter bearbeitet. Regeln für die Filterung der offenen IP-Pakete werden in den Bereichen `[local]`, `[broadcast]`, `[tunnel]` und `[forward]` der Firewall-Konfigurationsdatei definiert.

Im Bereich `[local]` werden Regeln für die Filterung der lokalen Pakete definiert. Lokale Pakete haben als Absender oder Empfänger den lokalen Netzwerkknoten.

Im Bereich `[broadcast]` werden Regeln für die Filterung der Broadcast-Pakete definiert:

Die Bereiche `[local]` und `[broadcast]` sind obligatorisch. Beim Start des Steuerungs-Daemons wird geprüft, ob die Bereiche in der Konfigurationsdatei vorhanden sind. Wenn einer der Bereiche fehlt, wird er automatisch mit Standardeinstellungen zur Firewall-Konfigurationsdatei hinzugefügt.

Im Bereich `[forward]` wird die Filterung der Transitpakete konfiguriert. Das sind Pakete, die diesen Netzwerkknoten auf dem Weg vom Absender zum Empfänger passieren. Standardmäßig enthält die Firewall-Konfigurationsdatei einen leeren Bereich `[forward]`. Damit die Transitpakete den Netzwerkknoten passieren können, müssen sie entweder im Bereich `[forward]` erlaubt sein, oder die Netzwerkadapter müssen die Pakete weiterleiten können. In der Sicherheitsstufe 4 für eingehende Pakete und in den Sicherheitsstufen 3 und 4 für ausgehende Pakete sind die Transitpakete grundsätzlich erlaubt. In allen anderen Sicherheitsstufen müssen die Transitpakete im Bereich `[forward]` erlaubt sein. Dies gilt auch, wenn die Umsetzung der Netzwerkadressen (NAT) verwendet wird. Eine solche Konfiguration wird unten detailliert beschrieben.

Im Bereich `[tunnel]` werden die Filterregeln für getunnelte Pakete definiert. Das sind Pakete, die zwischen Ressourcen, die von diesem Netzwerkknoten (Coordinator) getunnelt werden, und den geschützten Netzwerkknoten des ViPNet Netzwerks übertragen werden. In der Konfigurationsdatei muss der Bereich `[tunnel]` unbedingt vorhanden sein. Beim Start des Steuerungs-Daemons wird geprüft, ob der Bereich vorhanden ist. Wenn der Bereich fehlt, wird er automatisch zur Firewall-Konfigurationsdatei hinzugefügt. Der hinzugefügte Bereich enthält eine Regel, die standardmäßig den Traffic zwischen allen tunnelnden Ressourcen und allen geschützten Netzwerkknoten, die mit dem gegebenen Netzwerkknoten verbunden sind, erlaubt.

Bei der Filterung der IP-Pakete der TCP-, UDP- und ICMP-Protokolle werden verschiedene Parameter der Pakete analysiert. Mithilfe der Filterregeln können das Protokoll, die Adresse und

die Portnummer des Absenders, die Adresse und die Portnummer des Empfängers und die Richtung des Verbindungsaufbaus kontrolliert werden. Die Filterung anhand der Richtung des Verbindungsaufbaus ermöglicht es, nur Pakete bestimmter Verbindungen passieren zu lassen. Nur die Anfragen für den Verbindungsaufbau in eine bestimmte Richtung sowie die Antworten auf diese Anfragen können erlaubt werden. Die Anfragen für den Verbindungsaufbau in die Gegenrichtung können blockiert werden.

Für die Filterung der IP-Pakete aller anderen Protokolle (nicht TCP/UDP/ICMP) werden virtuelle Verbindungen anhand der IP-Adresse und der Protokollnummer, aufgebaut. Somit ist es ausreichend, durch eine Filterregel die Anfrage für den Verbindungsaufbau zu erlauben. Alle Antworten werden automatisch erlaubt sein (wenn sie von der gleichen IP-Adresse und über das gleiche Protokoll kommen).

Jeder der Bereiche kann mehrere Filterregeln enthalten. Die Syntax der Filterregeln ist für alle Bereiche gleich.

Jede Regel wird im Parameter `rule` beschrieben. Sein Wert besteht aus folgenden Komponenten:

```
rule= <Filter> <Bedingung> <Zeit> <Aktion>
```

oder

```
rule= <Filter> <Aktion> <Bedingung> <Zeit>
```

Der Filter muss an der ersten Stelle angegeben werden. Die Reihenfolge der anderen Komponenten ist unwichtig.

Jede Komponente einer Regel besteht aus mehreren Teilen. Diese Teile nennt man Token. Das **Token** stellt ein Dienstwort dar, nach dem ein Parameter angegeben werden kann.

Komponenten der Regeln, Token innerhalb der Komponenten, Dienstwörter und Parameter innerhalb der Token werden durch Leerzeichen getrennt.

Filter

Der Filter beschreibt Regeleigenschaften, die keine unmittelbare Auswirkung auf die Bearbeitung der Pakete haben, und wird immer am Anfang der Regel angegeben. Sie kann aus folgenden Token bestehen, die in der angeführten Reihenfolge angegeben werden sollten:

- `num <Nummer>` – Nummer der Regel innerhalb des Bereichs (von 0 bis 65535). Durch die Nummer wird die Reihenfolge der Filteranwendung festgelegt. Zuerst werden die Filter mit kleineren Nummern angewendet. Sobald die erste Filterregel in der Reihenfolge auf das Paket zutrifft, wird sie angewendet, das Paket wird erlaubt oder verboten, und eine weitere Filterung findet nicht statt.

Das Token `num` muss nicht angegeben werden. In diesem Fall versucht ViPNet selbstständig, eine Nummer zu vergeben. Bei der Nummernvergabe durch ViPNet werden die Nummern der Regeln, die vor der Regel und nach der Regel definiert wurden, berücksichtigt. Dabei kann das Ergebnis von dem gewünschten Ergebnis abweichen, daher empfehlen wir, die Nummer immer explizit anzugeben.

- `name <Name>` – deutet auf den Namen (die Beschreibung) der Regel hin, der in Anführungszeichen aufgeführt ist. Das Token name kann auch ausgelassen werden.

- `disable` – kennzeichnet, ob die gegebene Regel temporär deaktiviert und inaktiv ist. Das Token `disable` ist optional, sein Fehlen weist darauf hin, dass die Regel aktiv ist.

Bedingung

Die Bedingung beschreibt, welche Parameter ein Paket haben muss, damit es von der Regel bearbeitet werden kann. Eine Bedingung kann aus folgenden Token bestehen:

- `proto <Protokoll>` – Protokoll des IP-Pakets. Es werden die Protokolle `tcp`, `udp` und `icmp` unterstützt. Es können auch beliebige Protokollnummern angegeben werden. Wenn eine Regel Pakete von unterschiedlichen Protokollen bearbeiten muss, dann müssen diese durch Komma getrennt angegeben werden.

  Anstatt eines Protokolls kann das Schlüsselwort `any` angegeben werden, was bedeutet, dass die Bedingung für alle Protokolle gilt.

  Im Bereich `[broadcast]` können nur die Werte `udp` und `icmp` angegeben werden.

- `type <Typ>` – Typ der ICMP-Nachricht. Das Token darf nur in der Bedingung für das Protokoll ICMP (`proto icmp`) angegeben werden. Man darf es für andere Protokolle und bei der Wahl aller Protokolle (`proto any`) nicht verwenden. Im Token `type` kann nur ein Typ angegeben werden, der durch einen Code von 0 bis 255 repräsentiert wird.

  Wenn in der Bedingung für das Protokoll ICMP das Token `type` nicht angegeben wurde, dann wird diese Bedingung für beliebige Typen der ICMP-Nachrichten angewendet.

Hinweis. Das Token `type` muss unbedingt angegeben werden, wenn in der Bedingung für das Protokoll ICMP das Token code angegeben wurde (s. unten).

- `code <Code>` – Code der ICMP-Nachricht. Das Token darf nur in der Bedingung für das Protokoll ICMP (`proto icmp`) angegeben werden. Man darf es für andere Protokolle und bei der Wahl aller Protokolle (`proto any`) nicht verwenden. Im Token kann nur ein Code angegeben werden, der durch eine Zahl von 0 bis 255 repräsentiert wird.

Wenn in der Bedingung für das Protokoll ICMP das Token code nicht angegeben wurde, dann wird diese Bedingung für alle Codes der ICMP-Nachrichten angewendet.

- `from <Liste der Adressen>` – beschreibt Bedingungen für die Adresse und die Portnummer des Absenders. Die IP-Adresse und der Port werden durch einen Doppelpunkt getrennt, z.B.: `92.168.201.1:22`. Wenn keine Portnummer angegeben wird, folgt der Adresse kein Doppelpunkt. Die Bedingung wird dann für alle Portnummern angewendet.

Hinweis. Für das Protokoll `icmp` (`proto icmp`) darf keine Portnummer angegeben werden, auch wenn die Werte aller Ports definiert werden (`proto any`).

Auch IP-Adressen Bereiche oder Subnetzmasken können definiert werden, z.B.: `192.168.1.1-192.168.1.10:22` oder `192.168.201.0/24:22`. Die Angabe der Portbereiche ist ebenfalls zugelassen, z.B. `192.168.201.0/24:1024-65535`. Mehrere IP-Adressen und Ports können kombiniert und durch Komma getrennt angegeben werden, z.B.: `192.168.1.1-192.168.1.10:22,172.16.1.0.24:25`.

Aus den Adressen, Ports, Bereichen und Subnetzmasken können Gruppen gebildet werden, welche in runde Klammern eingeschlossen und durch Komma getrennt werden. So können mehrere IP-Adressen Bereiche oder Subnetzmasken mit einem Portbereich definiert werden, ohne ihn mehrmals anzugeben. Zum Beispiel bedeutet die Zeile

```
(192.168.201.0/24,172.16.1.0/24):1024-65535
```

, dass „Pakete von allen IP-Adressen in den Netzwerken 192.168.201.0/24 und 172.16.1.0/24, bei denen die Portnummer des Absenders im Bereich von 1024 bis 65535 liegt“. Komplexere Formen mit gleichzeitiger Gruppierung der Adressen und Portnummern und Aufzählung der Gruppen sind ebenfalls möglich. Zum Beispiel hat die Zeile

```
(192.168.201.0/24,172.16.1.0/24):(22,25,6660-6667),10.0.0.0/8:1024-
65535
```

folgende Bedeutung: „Pakete von allen IP-Adressen in den Netzwerken 192.168.201.0/24 und 172.16.1.0/24, bei denen die Portnummer des Absenders 22 oder 25 entspricht, oder im Bereich von 6660 bis 6667 liegt, sowie Pakete von IP-Adressen im Netzwerk 10.0.0.0/8, bei denen die Portnummer des Absenders im Bereich von 1024 bis 65535 liegt“.

Statt Adressen und ihren Bereichen können folgende Schlüsselwörter angegeben werden:

- `anyip` – alle Adressen (im Bereich 0.0.0.0-255.255.255.255);
- `broadcast` – die Adresse 255.255.255.255.

- `to <Liste der Adressen>` – beschreibt Bedingungen für die Adresse und Portnummer des Empfängers. Die Syntax des Tokens ist die gleiche wie die Syntax des Tokens `from`.

Im Bereich `[broadcast]` des Tokens to können nur folgende Adressen angegeben werden:

- `broadcast` – die Adresse 255.255.255.255;
- `directed-broadcast` – Broadcast-Adressen aller Subnetze, die mit den Netzwerkadaptern des Netzwerkknotens verbunden sind. Wenn die Regel in den Treiber geladen wird, wird der Wert durch die Liste der entsprechenden Broadcast-Adressen ersetzt;
- Broadcast-Adressen aller Subnetze, die mit den Netzwerkadaptern des Netzwerkknotens verbunden sind. Die Angabe einer konkreten Broadcast-Adresse wirkt sich auf die ausgerichteten Broadcast-Pakete aus, die in die Subnetze gesendet werden.

- `in` oder `out` – Verbindungsrichtung. Diese Angabe bezieht sich nicht auf die Paketrichtung, sondern auf die Richtung des Verbindungsaufbaus. ViPNet überwacht, zu welchen Verbindungen einzelne Pakete gehören, und blockiert diese oder lässt sie entsprechend den Regeln durch. Wenn zum Beispiel im Bereich `[local]` die Bedingung

  ```
  proto tcp from 192.168.1.1 to anyip out
  ```

  definiert wurde, dann wird sie für alle lokalen Pakete angewendet, die zu Verbindungen gehören, die von der IP-Adresse 192.168.1.1 initiiert wurden, d.h. die von dieser Adresse an entfernte Knoten gesendeten Pakete sowie entsprechende Antwortpakete. Wenn jedoch ein Netzwerkknoten versucht, eine Verbindung zur Adresse 192.168.1.1 herzustellen, dann fallen alle Pakete, die zu dieser Verbindung gehören, nicht unter diese Bedingung.

  Für das Protokoll TCP werden die Verbindungen immer überwacht. Für das verbindungslose Protokoll UDP wird ebenfalls versucht, die in den meisten Fällen hergestellte virtuelle Verbindung zwischen Anwendungen, die UDP verwenden, zu überwachen. Es wird zum Beispiel die folgende Bedingung definiert:

  ```
  proto udp from 192.168.1.1 to anyip:53 out
  ```

  Sobald ein Netzwerkknoten mit der Adresse 192.168.1.1 ein UDP-Paket an den Port 53 eines anderen Netzwerkknotens sendet, wird automatisch eine virtuelle Verbindung hergestellt. Wenn nach einer kurzen Zeit eine Antwort auf den Port kommt, von dem das erste Paket gesendet wurde, dann gehört diese Antwort der Bedingung nach zur hergestellten virtuellen Verbindung. Virtuelle Verbindungen werden getrennt, wenn keine Datenübertragung innerhalb eines für das gegebene Protokoll definierten Zeitintervalls stattfindet.

  Wenn Anwendungen für den Datenaustausch per UDP-Protokoll unterschiedliche Portnummern für das Senden und Empfangen verwenden, kann die virtuelle Verbindung nicht überwacht werden. In diesem Fall müssen die Token `in` oder `out` als die der Verbindungsrichtung entsprechenden Werte betrachtet werden.

Die Token `proto`, `from` und `to` müssen unbedingt in der Bedingung angegeben werden. Wenn die Parameter unwichtig sind, sollte man `any` (im Token `proto`) oder `anyip` (in Tokens `from`

und `to`) angeben. Die Verbindungsrichtung ist optional, dabei wird angenommen, dass Verbindungen, die in beide Richtungen hergestellt werden, der Bedingung entsprechen. Die Token `type` und `code` in der Bedingung für das Protokoll ICMP sind optional.

Beispiele für vollständige Bedingungen:

```
proto any from anyip to 192.168.201.1:22 in
proto tcp,udp from anyip:53 to 192.168.0.0/16,172.16.1.0/24
proto tcp from 10.0.0.1 to (192.168.0.0/16,172.16.1.0/24):(22,25) out
proto icmp type 8 code 0 from anyip to anyip
```

Besonderheiten der Bedingungen in den Filterregeln für getunnelte Pakete

Für Filterregeln getunnelter Pakete aus dem Bereich `[tunnel]` werden Bedingungen unter der Berücksichtigung folgender Besonderheiten angegeben:

- In einem der Token `from` und `to` muss eine Liste der Adressen von getunnelten Ressourcen und im anderen eine Liste der IDs von geschützten Netzwerkknoten, die mit getunnelten Ressourcen interagieren, angegeben werden.
- Eine Liste der IDs wird nach gleichen Regeln wie eine Liste der Adressen erstellt. Zum Beispiel: `0x10e10000/16:(22,25)`. Für die Angabe aller IDs wird das Schlüsselwort `anyid` verwendet.
- Statt der Schlüsselwörter `anyid` und `anyip` kann das Schlüsselwort any (auch mit Portnummern) verwendet werden. Wenn in einem der Token `from` oder `to` das Schlüsselwort `any` angegeben wird, dann muss any auch im anderen Token verwendet werden, sonst ist die Bedingung falsch definiert. Diese Schreibweise ersetzt zwei Regeln: die erste Regel, in der im Token `from` das Schlüsselwort `anyip` und im Token `to` das Schlüsselwort `anyid` stehen, und die zweite Regel, in der im Token `from` das Schlüsselwort `anyid` und im Token `to` das Schlüsselwort `anyip` stehen.

Aktion

Eine Aktion beschreibt, was mit einem Paket, das die Bedingung erfüllt, passieren soll. Für die Angabe einer Aktion kann einer von zwei Token verwendet werden:

- `pass` – das Paket muss erlaubt werden.
- `drop` – das Paket muss blockiert werden.

Zeit

Es kann festgelegt werden, ob eine Regel immer oder nur zu einer bestimmten Zeit gilt. Wenn keine Zeitangaben gemacht werden, gilt die Regel stets. Mit dem Parameter `time` können beliebige Zeitfenster für die Gültigkeit einer Regel definiert werden. Nach `time` können mehrere Zeitfenster definiert werden, welche durch Komma getrennt werden.

```
time <Status>,<Regelmäßigkeit>,<Zeitintervall>
```

Status kann eine der folgenden Werte haben:

- `on` – die Regel ist für definierte Zeitabschnitte aktiviert, für die restliche Zeit ist sie deaktiviert;
- `off` – die Regel ist für definierte Zeitabschnitte deaktiviert, für die restliche Zeit ist sie aktiviert (im Gegensatz zum Wert `on`);
- `disable` – die Zeitabschnitte sind auf inaktiv gesetzt und die Regel gilt immer.

Regelmäßigkeit kann einen der folgenden Werte haben:

- `daily` – die Regel gilt täglich. In diesem Fall wird nur ein Zeitfenster definiert, während dessen die Regel gilt (wenn der Status auf `on` gesetzt ist) oder nicht gilt (wenn der Status auf `off` gesetzt ist)
- `weekly` – die Regel gilt wöchentlich. Für jeden Wochentag kann ein Zeitfenster definiert werden, während dessen die Regel gilt (wenn der Status auf `on` gesetzt ist) oder nicht gilt (wenn der Status auf `off` gesetzt ist). Dies ermöglicht z.B. die Berücksichtigung eines Wochenendes.

Zeitfenster wird in Abhängigkeit von der Regelmäßigkeit folgendermaßen definiert:

- Nach `daily` wird ein Zeitfenster in Form `hh:mm-HH:MM` definiert, in dem `hh:mm` die Startzeit und `HH:MM` die Endzeit ist. Die Startzeit gehört zum Zeitfenster, die Endzeit nicht. Es können von 0 bis 59 Minuten und von 0 bis 24 Stunden angegeben werden. Wenn die Stundenanzahl 24 beträgt, können die Minuten nur auf 00 gesetzt werden, diese Zeit bedeutet dann 0 Uhr des nächsten Tages.
- Nach `weekly` können mehrere Zeitfenster definiert werden. Jeder Wochentag wird auf Englisch mit den ersten drei Buchstaben gekennzeichnet (mon, tue, wed, thu, fri, sat, sun), danach folgt ein Gleichheitszeichen „=“ und das Zeitfenster für den ausgewählten Wochentag im gleichen Format wie für daily, z. B.: `mon=9:00-18:00`. Wenn mehrere Tage nacheinander angegeben sind, müssen sie durch Komma getrennt werden, z.B.: `mon=9:00-18:00,tue=10:00-18:00`. Für verschiedene Wochentage kann die gleiche Zeit festgelegt

werden. Dabei werden die Wochentage durch Doppelpunkt getrennt, z. B.: `sat:sun=00:00-24:00`.

Es ist nicht notwendig, Zeitfenster für alle Wochentage zu definieren. Wenn für einen Wochentag kein Zeitfenster definiert ist, wird die Regel an diesem Tag deaktiviert, wenn der Status auf `on` gesetzt ist und aktiviert, wenn der Status auf `off` gesetzt ist.

Beispiele:

```
time off,daily,9:00-18:00
time on,weekly,mon:tue:wed:thu:fri=9:00-18:00,sat:sun=00:00-24:00
```

Standard Filterregeln für unverschlüsselte IP-Pakete

Die Konfigurationsdatei der Firewall wird im Zuge der Installation von ViPNet Coordinator HW/VA automatisch erstellt. Die Datei enthält einen Pflichtbereich mit standardmäßigen Parametern. Einige dieser Regeln sind deaktiviert, anstatt `disable` werden für sie Kommentare zu den entsprechenden Zeilen verwendet. Um die Regel zu aktivieren, ist es ausreichend, den Kommentar zu löschen.

Während der Konfiguration können die Regeln vom Systemadministrator geändert werden, aber die Standardkonfiguration kann in jedem Pflichtbereich jederzeit wiederhergestellt werden. Dafür soll der Bereich aus der Firewall-Konfigurationsdatei gelöscht werden. Beim nächsten Start des Steuerungsdaemons wird der fehlende Bereich mit seinen Standardeinstellungen automatisch zu der Firewall-Konfigurationsdatei hinzugefügt.

Im Bereich `[local]` sind standardmäßig folgende Regeln vorhanden:

```
rule= proto udp from anyip:67 to anyip:68 pass
rule= proto udp from anyip:68 to anyip:67 pass
# rule= proto udp from anyip:138 to anyip:138 pass
rule= proto udp from anyip to anyip:53 pass
rule= proto udp from anyip to anyip:123 pass
```

Die ersten zwei regeln lassen die IP-Pakete des DHCP-Dienstes (Ports 67 und 68) durch, welcher für die dynamische Vergabe der IP-Adressen an die Netzwerkknoten zuständig ist. Diese Regeln sind aktiviert.

Die dritte Regel erlaubt Pakete des NetBIOS-Dienstes (netbios-dgm, Port 138) durchzulassen. Der NetBIOS-Dienst ist für den Datenaustausch zwischen Netzwerkknoten zuständig, wenn im lokalen Netzwerk NetBIOS-Namen verwendet werden. Diese Regel ist deaktiviert (kommentiert).

Die vierte Regel erlaubt ausgehende IP-Pakete auf den Port 53 der DNS-Server (auf S. 84) durchzulassen. Die fünfte Regel erlaubt die eingehenden Pakete auf Port 123 des NTP-Servers durchzulassen. Diese Regeln sind aktiviert.

Im Bereich `[broadcast]` sind standardmäßig folgende Regeln vorhanden:

```
rule= proto udp from anyip:67 to anyip:68 pass
rule= proto udp from anyip:68 to anyip:67 pass
# rule= proto udp from anyip:138 to anyip:138 pass
# rule= proto udp from anyip:137 to anyip:137 pass
```

Die ersten drei Regeln sind die gleichen wie im Bereich `[local]`. Die vierte Regel lässt die Pakete des NetBIOS Dienstes (netbios-ns, Port 137) durch. Der NetBIOS Dienst ist für die Registrierung und die Überprüfung der NetBIOS Namen der Netzwerkknoten im lokalen Netzwerk zuständig. Diese Regel ist deaktiviert (kommentiert).

Im Bereich `[tunnel]` ist standardmäßig folgende Regel vorhanden:

```
rule= proto any from any to any pass
```

Diese Regel ist aktiviert und erlaubt den Traffic zwischen allen getunnelten Geräten und geschützten Netzwerkknoten, die mit dem ViPNet Coordinator HW/VA verbunden sind. Diese Regel entspricht den zwei folgenden Regeln für getunnelte Geräte:

```
rule= proto any from anyid to anyip pass
rule= proto any from anyip to anyid pass
```

Konfiguration der Umsetzung der IP-Adressen (NAT)

ViPNet Coordinator HW/VA verfügt über eine NAT-Funktion. Die NAT-Technologie ermöglicht, die IP-Adressen eines Netzwerks in die IP-Adressen eines andern Netzwerks umzuwandeln. Es werden zwei Arten der Umsetzung unterstützt:

- **Dynamisches NAT** oder Masquerading (Umsetzung der Absenderadresse). Diese Art von NAT wird im Regelfall dann verwendet, wenn mehrere Netzwerkknoten einzelner Benutzer mit dem Internet verbunden werden sollen. Dabei werden auf dem ViPNet Coordinator HW/VA die unterschiedlichen IP-Adressen, die einem Netzwerkknoten vergeben werden können durch die externe IP-Adresse des ViPNet Coordinator HW/VA ersetzt. Auf dem Rückweg werden die Pakete mit der aktuellen IP-Adresse des Netzwerkknotens versehen und an diesen weitergeleitet.

Hinweis. Die Absenderadressen können ausschließlich in eigene IP-Adressen, die auf dem Adapter angegeben sind, umgesetzt werden.

- **Statisches NAT** oder Forwarding (Umsetzung der Empfängeradresse). Diese Art von NAT wird eingesetzt, wenn aus dem Internet der Zugriff auf ein Netzwerkknoten im geschützten Netzwerk erfolgen soll. Bei den IP-Paketen, welche auf die externe IP-Adresse des ViPNet Coordinator HW/VA eingehen, wird die Empfängeradresse geändert und die Pakete werden auf den entsprechenden Netzwerkknoten weitergeleitet. Die Antworten werden mit der geänderten IP-Adresse des Versenders zurück gesendet.

NAT-Regeln werden in der Firewall-Konfigurationsdatei im Bereich `[nat]` konfiguriert.

Syntax für Regeln der Adressenübersetzung

NAT-Regeln sind in ihrer Schreibweise den Filterregeln (s. Konfiguration der Filterregeln für offene IP-Pakete auf S. 61) ähnlich. Sie werden mit dem Parameter `rule` deklariert. Der Parameter besteht aus mehreren Teilen:

```
rule= <NAT-Regel> <Aktion> <Bedingung>
```

Die NAT-Regel wird immer an der ersten Stelle angegeben, alle weiteren Teile können beliebige Reihenfolge haben.

Hinweis. Im Gegensatz zu den Filterregeln kann für die NAT-Regeln keine Zeit definiert werden.

NAT-Regel wird identisch mit dem `Filter` aus den Filterregeln definiert (s. Konfiguration der Filterregeln für offene IP-Pakete auf S. 61).

Aktion wird durch `change` deklariert mit den Angaben, was und wodurch ersetzt wird. Je nachdem, ob es sich um eine dynamische oder statische Umsetzung handelt, haben die Regeln folgende Schreibweise:

- Bei der dynamischen Umsetzung: `change src=<Adresse>:dynamic`

  `<Adresse>` – ist die IP-Adresse des externen Netzwerkadapters des ViPNet Coordinator HW/VA. Zum Beispiel: `change src=194.87.0.8:dynamic`.

- Bei der statischen Umsetzung: `change dst=<Adresse>:<Port>`

  `<Adresse>` und `<Port>` sind die IP-Adresse und der Port des Netzwerkknotens im lokalen Netzwerk. Zum Beispiel: `change dst=192.168.201.1:8080`.

Bedingung die NAT-Regel hat die gleiche Schreibweise wie die Bedingung der Filterregel, allerdings mit einigen Abweichungen:

- Beim dynamischen NAT für `proto` und `to` muss `anyip` angegeben werden.
- Beim dynamischen NAT definiert `from` die IP-Adressen des geschützten Netzwerks, welche umgesetzt werden sollen. Dabei können in `from` nur einzelne oder mehrere gelistete IP-Adressen, IP-Adressen Bereiche und Masken angegeben werden. Es können keine Ports oder Portbereiche definiert werden.
- Beim statischen NAT soll `from` auf `anyip` gesetzt werden und bei `to` sollen die externe IP-Adresse und der Port des ViPNet Coordinator HW/VA angegeben werden, auf die die IP-Pakete eingehen, welche der Umsetzung unterliegen. In diesem Fall für `to` können nur einzelne oder mehrere gelistete IP-Adressen und Ports angegeben werden. Keine Adressen-Masken- und Portbereiche sind zugelassen.

Beispiele für NAT-Regeln:

- Dynamische Umsetzung:

```
rule= num 10 change src=194.87.0.8:dynamic proto any from 192.168.201.0/24
to anyip
```

- Statische Umsetzung:

```
rule= num 100 change dst=10.0.0.7:8080 proto tcp from anyip to
194.87.0.8:80
```

Zusammenwirken der Filterung und NAT

Nachdem die Umsetzung der IP-Adressen erfolgte, werden die IP-Pakete gefiltert. Die Regeln für die Filterung sind in Bereichen `[local]` und `[forward]` festgelegt. In jedem Paket werden die IP-Adresse des Versenders vor der Filterung und die Adresse des Empfängers nach der Filterung überprüft.

Beispiel für dynamische Umsetzung:

Ein ViPNet Coordinator HW/VA mit einem lokalen Netzwerk 10.0.1.0/24 hat die externe IP-Adresse 194.87.0.8. Die Regel im Bereich `[nat]` dafür ist:

```
rule= num 10 change src=194.87.0.8:dynamic proto tcp from 10.0.1.0/24 to
anyip
```

Im Bereich `[forward]`, soll folgende Regel definiert werden:

```
rule= num 100 pass proto tcp from 10.0.1.0/24 to anyip
```

Wenn die internen Netzwerkknoten keine TCP Verbindungen mit der externen IP-Adresse 194.226.82.50 aufbauen sollen, muss im Bereich `[forward]` folgende Regel hinzugefügt werden:

```
rule= num 90 drop proto tcp from 10.0.1.0/24 to 194.226.82.50
```

In `from` wird die IP-Adresse des lokalen Netzwerkknotens vor der Umsetzung angegeben und in `to` die IP-Adresse des Empfänger-Netzwerkknotens aus dem Internet.

Beispiel für statische Umsetzung:

Alle IP-Pakete, die auf Port 80 ankommen, sollen auf den lokalen Netzwerkknoten 10.0.1.1 mit dem Port 8080 weitergeleitet werden. Die Regel im Bereich `[nat]` dafür ist:

```
rule= num 10 change dst=10.0.1.1:8080 proto tcp from anyip to
194.87.0.8:80
```

Die Filterregel im Bereich `[forward]` dafür ist:

```
rule= num 100 pass proto tcp from anyip to 10.0.1.1:8080
```

Wenn nun die eingehenden Verbindungen zu diesem lokalen Netzwerkknoten von der externen IP-Adresse 194.226.82.50 blockiert werden sollen, muss `[forward]` um die folgende Regel ergänzt werden:

```
rule= num 90 drop proto tcp from 194.226.82.50 to 10.0.1.1:8080
```

5

Logdatei der registrierten IP-Pakete

Konfiguration der Logdatei der IP-Pakete

Daten über Ereignisse, die in Zusammenhang mit der Verarbeitung von IP-Paketen durch ViPNet Coordinator HW/VA-Netzwerkadapter stehen, werden in der Registrierungslogdatei erfasst. Für jeden Netzwerkadapter können das Ausmaß der Detalisierung der registrierten Daten und die maximale Größe der Logdatei festgelegt werden.

Führen Sie die folgenden Schritte aus, um die Parameter der Registrierung von IP-Paketen, die einen bestimmten Netzwerkadapter passieren, zu konfigurieren:

1. Wechseln Sie in der Befehlszeilenschnittstelle in den Administratormodus.
2. Führen Sie den folgenden Befehl aus, um die Konfigurationsdatei des Netzwerkadapters zu editieren:

   ```
   iplir config <Adaptername>
   ```

   

   Hinweis. Benutzen Sie den Befehl `inet show interface`, um eine Liste aller Netzwerkadapter anzuzeigen.

3. Geben Sie im Bereich `[db]` die benötigten Werte für die folgenden Parameter an:
   - `maxsize`: maximale Größe der Logdatei in MB.

     Wenn die Größe der Logdatei den angegebenen maximal Wert erreicht, beginnt das System, die ältesten Einträge durch neue zu ersetzen.

     Wenn der Wert dieses Parameters gleich Null ist, dann wird für den betroffenen Netzwerkadapter keine Logdatei geführt.
   - `timediff`: Zeitintervall (in Sekunden), innerhalb von welchem Ereignisse mit gleichen Merkmalen in einem Eintrag der Logdatei zusammengefasst werden. Vorgegebener Standardwert ist 60 Sekunden.

     Beispiel: Einträge über durchgelassene verschlüsselte IP-Pakete, bei denen die Adressen und Ports des Absenders und de s Empfängers übereinstimmen, werden zusammengefasst.

     Wenn der Wert dieses Parameters gleich Null ist, dann wird jedes IP-Paket mit einem eigenen Eintrag der Logdatei registriert.

- `registerall`: Parameter, der die Registrierung aller IP-Pakete aktiviert oder deaktiviert. Dieser Parameter kann die folgenden Werte annehmen:
  - `on`: alle IP-Pakete registrieren;
  - `off` (Standardwert): nur blockierte IP-Pakete sowie Ereignisse, die in Zusammenhang mit Änderungen von IP-Adressen der ViPNet Netzwerkknoten stehen, registrieren;
- `registerbroadcast`: Parameter, der die Registrierung von Broadcast-IP-Paketen aktiviert oder deaktiviert. Dieser Parameter kann die folgenden Werte annehmen:
  - `on`: Broadcast-Pakete registrieren,
  - `off` (Standardwert): Broadcast-Pakete nicht registrieren.
- `registertcpserverport`: Parameter, der die Registrierung des Absenderports des IP-Pakets bei Verbindungen über das TCP-Protokoll aktiviert oder deaktiviert. Dieser Parameter kann die folgenden Werte annehmen:
  - `on`: Absenderport nicht registrieren. In diesem Fall werden die Einträge der Logdatei nach dem Empfängerport gruppiert.
  - `off` (Standardwert): Absenderport registrieren.

4 Drücken Sie die Tastenkombination **Strg+O**, um die Konfigurationsdatei zu speichern, und drücken Sie anschließend die Taste **Eingabe**.

5 Drücken Sie die Tastenkombination **Strg+X**, um die Datei zu schließen.

Logdatei der registrierten IP-Pakete anzeigen

Die Logdatei der registrierten IP-Pakete enthält Informationen über die unverschlüsselten und verschlüsselten IP-Pakete, die von ViPNet Coordinator HW/VA-Netzwerkschutztreiber auf allen Netzwerkadaptern des Rechners bearbeitet wurden.

Die Logdatei für IP-Pakete enthält nur Angaben zu IP-Paketen und nicht zu Verbindungen. Alle erlaubten Transitpakete werden in der Logdatei zwei Mal angezeigt – als eingehende IP-Pakete eines Netzwerkadapters und als ausgehende IP-Pakete des anderen Netzwerkadapters. Alle erlaubten lokalen IP-Pakete werden nur einmal angezeigt – als ein- oder ausgehende Pakete eines Netzwerkadapters. Alle blockierten IP-Pakete werden nur einmal angezeigt – als blockierte Pakete des Netzwerkadapters, auf dem sie blockiert wurden. Dies betrifft sowohl die verschlüsselten als auch die unverschlüsselten IP-Pakete.

Die Logdatei für IP-Pakete kann mit dem Befehl `iplir view` angesehen werden. Die Einträge können wahlweise nach folgenden Kriterien angezeigt werden:

- Zeitabschnitt;
- Netzwerkadapter;
- IP-Protokoll;
- Paketrichtung – eingehende oder ausgehende Pakete;
- Ereignistyp;
- IP-Adresse oder IP-Adressen Bereich des Absenders oder des Empfängers des Pakets;
- Lokaler Port oder Portbereich für TCP, UDP;
- Entfernter Port oder Portbereich für TCP, UDP;
- Benutzername des Absenders oder des Empfängers aus dem geschützten Netzwerk.

Nach Eingabe des Befehls `iplir view` wird folgendes Fenster angezeigt:

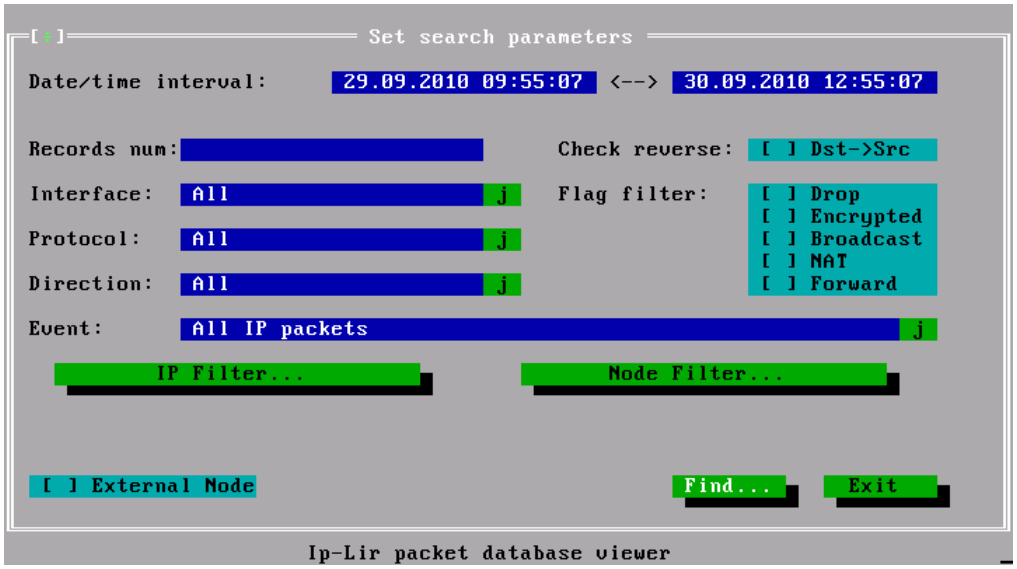

Abbildung 4: Einstellung der Suchparameter in der Logdatei der registrierten IP-Pakete

Standardmäßig wird angenommen, dass in der lokalen Logdatei gesucht wird. Wenn in der Logdatei eines entfernten Netzwerkknotens gesucht werden soll, muss die Option **External Node** aktiviert werden, wobei nach der Aktivierung der Benutzer aufgefordert wird, das Passwort des ViPNet Netzwerk Administrators einzugeben. Wenn das Passwort korrekt ist, erscheint die Schaltfläche **Select** rechts von der Option **External Node**. Diese Schaltfläche öffnet ein Fenster mit der Liste der geschützten Netzwerkknoten, in dem der benötigte Netzwerkknoten ausgewählt werden kann Um eine Verbindung erfolgreich herzustellen, muss der entfernte Netzwerkknoten auf der TCP/IP-Ebene verfügbar sein und über ein Steuerungsprogramm verfügen. Wenn keine Verbindung hergestellt werden kann, wird eine entsprechende Meldung angezeigt, und das Programm wird beendet.

Für die Suche können folgende Parameter angegeben werden:

- **Date/time interval** – Datum- und Zeitintervall im Format DD.MM.YYYY HH:MM:SS, um nach während dieses Zeitraums registrierten Einträgen zu suchen.
- **Records num** – Anzahl der angezeigten Ergebnisse.
- **Interface** – Netzwerkadapter (wird aus der Liste der verfügbaren Netzwerkadapter ausgewählt).

  Als verfügbar gelten Netzwerkadapter, die eine Logdatei für IP-Pakete haben. Die Suche wird in der Logdatei des ausgewählten Netzwerkadapters durchgeführt. Als Parameter kann der Name des Netzwerkadapters oder der Wert **All** für alle Netzwerkadapter ausgewählt werden.
- **Protocol** – Parameter für die Suche von Paketen mit ausgewähltem Protokoll.

Als Parameter kann ein bestimmtes Protokoll oder der Wert All für alle Protokolle angegeben werden.

- **Direction** – Richtung des Pakets. Der Parameter kann folgende Werte haben:
  - **All** – eingehende und ausgehende Pakete;
  - **Incoming** – eingehende Pakete;
  - **Outgoing** – ausgehende Pakete.
- **Check reverse** – Kennzeichnet die Registrierung von Antwortpaketen (vom Empfänger an den Absender) in der Logdatei.

  Sollte nur dann verwendet werden, wenn eine bestimmte IP-Adresse (**IP Filter**) oder ein Netzwerkknoten (**Node Filter**) als Absender oder Empfänger von Paketen angegeben werden kann.
- **Flag filter** – Kennzeichnet die Suche nach Paketen, die einem oder mehreren der nachfolgenden Parameter entsprechen:
  - **Drop** – blockierte Pakete;
  - **Encrypted** – verschlüsselte Pakete;
  - **Broadcast** – Broadcast-Pakete;
  - **NAT** – umgesetzte Pakete;
  - **Forward** – Transitpakete.
- **Event** – Kennzeichnet die Suche nach allen Paketen mit einem bestimmten Ereignis.

  Der Wert wird aus der Liste ausgewählt. Standardmäßig sind alle Ereignisse ausgewählt.
- **IP Filter** – Öffnet ein Fenster für die Angabe folgender Suchparameter:
  - **Source IP address** – **All**, gültiger Adressenbereich oder eine gültige IP-Adresse des Absenders;
  - **Destination IP address – All**, gültiger Adressenbereich oder eine gültige IP-Adresse des Empfängers;
  - **Source port** – Portnummer oder Portbereich (0-65535) des Absenders für Protokolle TCP und UDP;
  - **Destination port** – Portnummer oder Portbereich (0-65535) des Empfängers für Protokolle TCP und UDP;
- **Node Filter** – öffnet ein Fenster für die Angabe von Parametern für den Netzwerkknoten des Empfängers und/oder des Absenders: **Source** und/oder **Destination**.

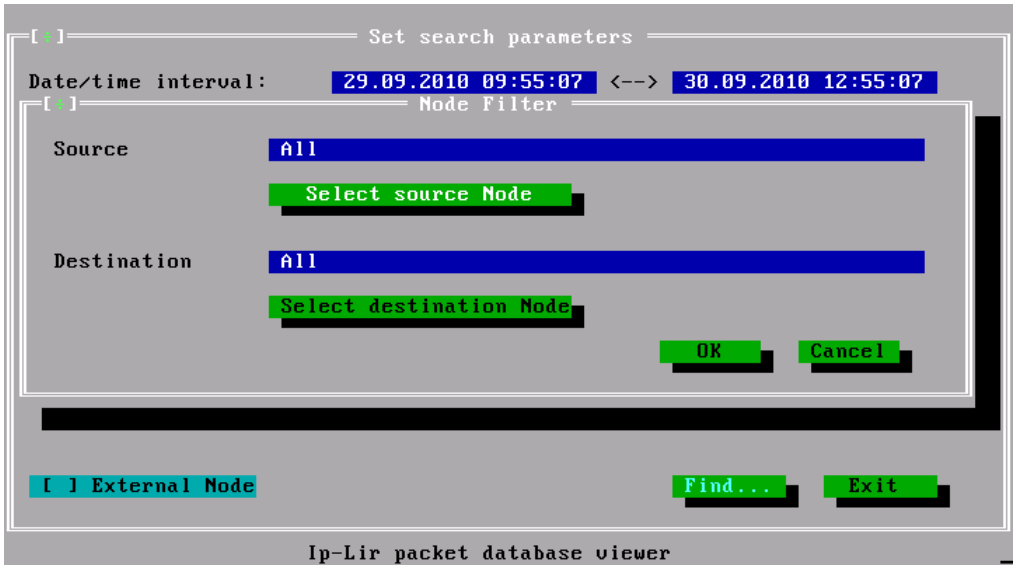

Abbildung 5: Angabe von Parametern für eine Anfrage, die den Netzwerkknoten des Empfängers und/oder des Absenders berücksichtigt

Für die Wahl des Absender- oder Empfänger-Netzwerkknotens verwenden Sie die entsprechenden Schaltflächen: **Select source Node** oder **Select destination Node**. Es öffnet sich ein Fenster mit einer Liste von geschützten Netzwerkknoten und Suchfunktion.

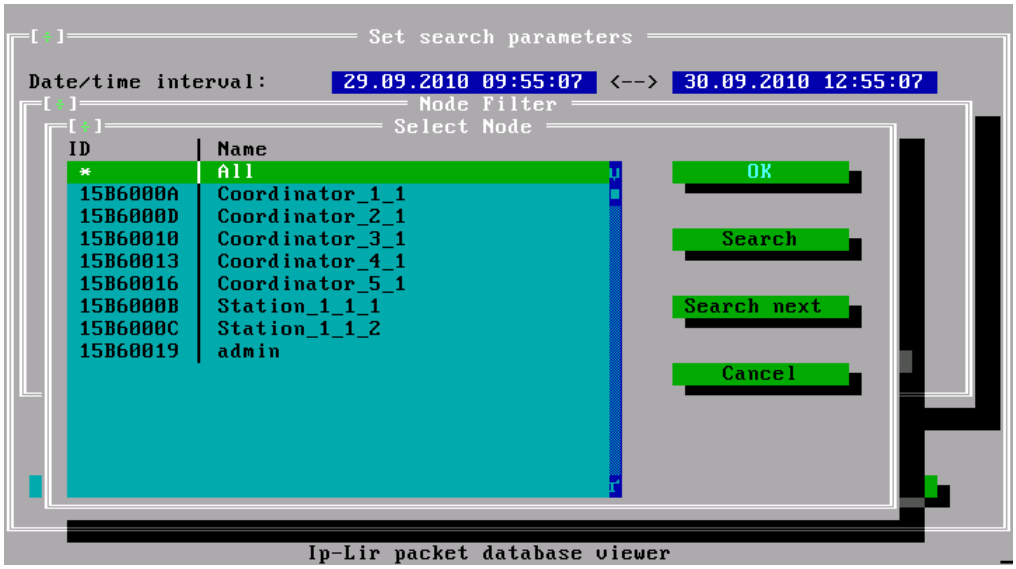

Abbildung 6: Liste der geschützten Netzwerkknoten für die Auswahl des Absenders oder Empfängers

Das Fenster enthält eine Liste aller geschützten ViPNet Netzwerkknoten, die mit dem aktuellen Netzwerkknoten verbunden sind. Die Netzwerkknoten in der Liste sind in alphabetischer Reihenfolge sortiert. Die linke Spalte zeigt die hexadezimale Kennung des

Netzwerkknotens. Zusätzliches Dienstelement **All** entspricht der Auswahl aller Netzwerkknoten.

Für die Suche klicken Sie auf die Schaltfläche **Search**. In einem separaten Fenster können Suchkriterien manuell oder durch die Auswahl der früher eingegebenen Kriterien aus der Dropdownliste festgelegt werden. Als Suchkriterium kann sowohl der Name des Netzwerkknotens als auch seine eindeutige Kennung verwendet werden. Bei der Suche nach der eingegebenen Zeichenfolge wird sowohl der **Name** als auch die **ID** des Netzwerkknotens berücksichtigt.

Die Schaltfläche **Search next** wird für die schnelle Suche nach dem nächsten Element der Liste verwendet, das die Suchkriterien erfüllt.

Um die Suche mit angegebenen Parametern zu starten klicken Sie auf die Schaltfläche Find im unteren Teil des Hauptfensters (s. Abbildung auf S. 78). Um das Programm zu beenden klicken Sie auf die Schaltfläche **Exit**.

Eine Liste von gefundenen Einträgen wird im Fenster **View results** (s. Abbildung auf S. 82) angezeigt. Die Einträge sind nach der Registrierungszeit von Paketen geordnet. Die Liste besteht aus folgenden Spalten:

- Datum und Zeit der Paket-Registrierung.
- Netzwerkadapter, auf dem das Ereignis registriert wurde.
- Richtung des registrierten Pakets: „<“ ausgehende, „>“ eingehende und das Flag des Ereignisses:
  - **C** – verschlüsseltes Paket;
  - **B** – Broadcast-Paket;
  - **D** – blockiertes Paket;
  - **T** – Transitpaket (routingfähiges Paket);
  - **R** – das Paket wird nach NAT-Regeln des offenen Netzwerks umgesetzt;
  - **N** – das Paket wurde nach NAT-Regeln des offenen Netzwerks umgesetzt.
- Protokoll.
- IP-Quelladresse.
- Lokaler Port für Protokolle TCP и UDP.
- IP-Zieladresse.
- Port des entfernten Computers für Protokolle TCP und UDP.

Im unteren Fensterteil werden Informationen über das in der Liste ausgewählte Ereignis angezeigt:

- Der dem Paket zugewiesene Name des Ereignisses, присвоенного IP-пакету.
- Protokoll.
- Paketgröße.
- Es wird die Gesamtgröße aller zu einem Ereignis gehörenden Pakete angezeigt, wenn der Zähler größer als Eins ist. Für die verschlüsselten Pakete wird ihre Gesamtgröße mit allen Headern angezeigt, die für den Betrieb des geschützten Netzwerks notwendig sind.
- Anzahl von Paketen, die zu einem Ereignis gehören .
- Netzwerkknoten des Absenders.
- Netzwerkknoten des Empfängers.

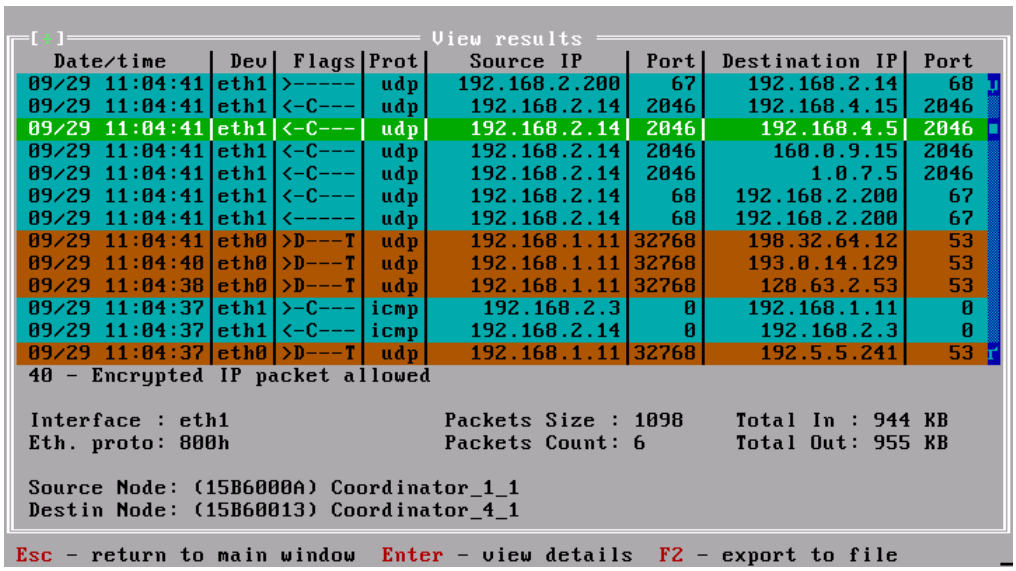

Abbildung 7: Liste der gefundenen Einträge

Achtung! Mit der Taste F2 (export to file) können auf dem MiniGate keine Logs in Dateien exportiert werden.

Jedes Ereignis aus der Auflistung kann mit der Taste **Enter** detailliert angezeigt werden.

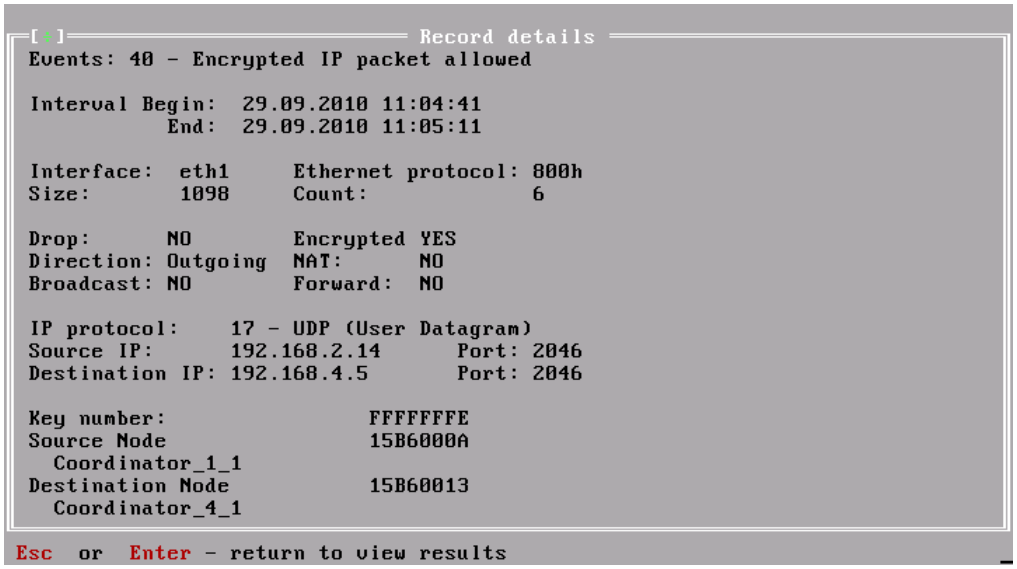

Abbildung 8: Detaillierte Information über ein Ereignis

Im unteren Teil des Fensters mit Suchergebnissen (s. Abbildung auf S. 82) befinden sich die Felder **Total In** und **Total Out**, welche die Gesamtgröße der ein- und ausgehenden Pakete enthalten. Die Gesamtgröße wird für alle zum Suchergebnis gehörenden Pakete berechnet. Wenn ein Paket keine Information über seine Größe enthält, wird seine Größe bei der Berechnung der Gesamtgröße nicht berücksichtigt. In diesem Fall wird nach dem Wert der Größe im entsprechenden Feld (**Total In** und/oder **Total Out**) ein Sternchen angezeigt. Es bedeutet, dass der Traffic nicht vollständig berücksichtigt wurde. Wenn keiner der Einträge Informationen über die Paketgröße enthält, wird im entsprechenden Feld (**Total In** und/oder **Total Out**) der Wert **N/A** angezeigt. Ein Sternchen wird in diesem Fall nicht angezeigt.

Die Maßeinheiten für die Anzeige der Gesamtgröße werden wie folgt gewählt:

- wenn die Gesamtgröße kleiner als 100 Kilobyte ist, dann wird die Größe in Byte angezeigt und das Suffix „B“ an den Wert angehängt;
- Wenn die Gesamtgröße größer als 100 Kilobyte und kleiner als 100 Megabyte ist, dann wird die Größe in Kilobyte angezeigt und das Suffix „KB“ an den Wert angehängt;
- wenn die Gesamtgröße größer als 100 Megabyte ist, dann wird die Größe in Megabyte angezeigt und das Suffix „MB“ an den Wert angehängt.

Glossar

B

Befehlszeileinterpreter

Befehlsshell, die zum Administrieren der Software ViPNet Coordinator HW/VA mit Hilfe einer Reihe spezieller Befehle eingesetzt wird.

D

DHCP (Dynamic Host Configuration Protocol)

Ein Netzwerkprotokoll der Anwendungsschicht, das es den Rechnern ermöglicht, IP-Adressen und andere für die Arbeit im TCP/IP-Netzwerk erforderlichen Parameter automatisch zu beziehen. Dazu zählen Parameter wie Subnetzmaske, Gateway-IP-Adresse, IP-Adressen der DNS Server, IP-Adressen der WINS Server.

DHCP-Server

Server, der die IP-Adressen der Clients automatisch verwaltet und entsprechende Einstellungen im Netzwerk durchführt.

DNS-Server

Server, der einen Teil der DNS-Datenbank verwaltet, die für den Zugriff auf Computernamen in der Internet-Domäne verwendet wird (Beispiel: ns.domain.net). In der Regel werden Domänendaten auf zwei DNS-Servern gespeichert, die als „Primary DNS“ und „Secondary

DNS“ bezeichnet werden (die Duplizierung wird durchgeführt, um die Hochverfügbarkeit des Systems zu verbessern).

Der DNS-Server wird auch Domänennamenserver und Nameserver (DNS) genannt.

F

Firewall

Gerät oder Programm, das auf einem Netzwerkknoten an der Grenze des Netzwerks installiert ist, den gesamten ein- und ausgehenden IP-Traffic überprüft und Entscheidungen über die mögliche Weiterleitung des Traffics zu seinem Zielpunkt trifft. Das heißt, die Firewall dient der Verhinderung von unerlaubtem Zugriff von einem Netzwerk auf ein anderes. Die Firewall ist normalerweise für die Übersetzung der internen IP-Adressen in Adressen, auf die von einem externen Netzwerk aus zugegriffen werden kann, zuständig (Durchführung von NAT). In ViPNet werden drei Typen von Firewalls mit NAT unterschieden:

- ViPNet Coordinator – Modus, bei welchem als Firewall ein Computer mit installierter ViPNet Coordinator -Software auftritt, der NAT für verschlüsselten Traffic sicherstellt.
- Mit statischer Adressenübersetzung – Modus, bei dem zwischen dem geschützten Knoten und dem externen Netzwerk eine Firewall aufgestellt ist, die statische Umsetzung von IP-Adressen durchführt, d. h. die Interaktion externer Knoten mit einer bestimmten internen Netzwerkadresse über das UDP-Protokoll mit vorgegebenem Port sicherstellt.
- Mit dynamischer Adressenübersetzung – Modus, bei dem zwischen dem geschützten Knoten und dem externen Netzwerk eine Firewall aufgestellt ist, die dynamische Umsetzung von IP-Adressen durchführt. Dabei sollte im offenen Netzwerk ein Coordinator präsent sein, der die Verbindungen aufrechterhalten kann. Firewalls dieses Typs werden eingesetzt, wenn Verbindungen zum externen Netzwerk zum Beispiel über ein xDSL-Modem aufgebaut werden, das als Router auftritt, oder wenn dazu drahtlose Geräte, GPRS-Netze oder andere Anbieter, die private IP-Adressen zur Verfügung stellen, verwendet werden.

Siehe: Externes Netzwerk, Internes Netzwerk, Grenze des lokalen Netzwerkes, Dynamisches NAT, Geschützter Netzwerkknoten, Router, Statisches NAT, Netzwerkadressenübersetzung (NAT) (auf S. 86), Private IP-Adresse.

I

IP-Traffic

Datenfluss, der entsprechend den Regeln des IP-Protokolls über die Netzwerke übertragen wird.

Siehe: IP-Paket.

N

Netzwerkadapter

Ist eine elektronische Schaltung zur Verbindung eines Computers mit einem lokalen Netzwerk zum Austausch von Daten.

Siehe: Netzwerk, IP-Adresse.

Netzwerkadressenübersetzung (NAT)

Network Address Translation ist der Sammelbegriff für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden.

Siehe: Externes Netzwerk, Internes Netzwerk, Dynamisches NAT, Statisches NAT.

Netzwerkfilter

Eine Zusammensetzung von Parametern, auf deren Basis die Firewall der ViPNet Software bestimmte IP-Pakete blockiert oder erlaubt.

Netzwerkprotokoll

Ein Netzwerkprotokoll ist eine Vereinbarung, nach der Daten zwischen Computern bzw. Prozessen ausgetauscht werden, die durch ein Netz miteinander verbunden sind.

NTP-Server

Server der genauen Uhrzeit, der dafür zuständig ist, die Systemzeit der Computer, Arbeitsstationen, Server und anderer Netzwerkgeräte zu synchronisieren. Dieser Server tritt als Vermittler zwischen dem Referenzzeitgeber und dem lokalen Netzwerk auf. Er erhält die genaue Zeit vom Referenzzeitgeber über einen speziellen Verbindungskanal (Schnittstelle) und leitet die Daten an jeden Netzwerkknoten weiter. Dadurch wird die Synchronisation der Geräte untereinander sichergestellt.

O

Offener Netzwerkknoten

Ein Netzwerkobjekt ohne ViPNet Software.

V

ViPNet Netzwerk

Mit Hilfe von ViPNet Software aufgebautes logisches Netzwerk.

Siehe: ViPNet Netzwerkknoten.

Index