SECURITY

Bintec Benutzerhandbuch - VPN Access Reihe
Version 1.1

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von Bintec-Gateways ab Software-Release 7.1.4. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind zu finden unter www.bintec.de.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer 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 **Release Notes** für Bintec-Gateways finden Sie unter www.bintec.de.

Als Multiprotokollgateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.bintec.de.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Deutschland

Telefon: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

Bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
Frankreich

Telefon: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Menü Security

Im Folgenden wird das Menü *SECURITY* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY]: Security Configuration                              MyGateway

     Cobion Orange Filter >
     Access Lists >
     Stateful Inspection >

     SSH Daemon >


     Local Services Access Control >


     EXIT
```

In dem Menü ***SECURITY*** konfigurieren Sie die Sicherheitsfunktionen Ihres Gateways.

Über das Menü ***SECURITY*** gelangen Sie in folgende Untermenüs:

- ***COBION ORANGE FILTER***
- ***ACCESS LISTS***
- ***STATEFUL INSPECTION***
- ***SSH DEAMON***
- ***LOCAL SERVICES ACCESS CONTROL***

1 Menü Security

2 Untermenü Cobion Orange Filter

Im Folgenden wird das Untermenü *COBION ORANGE FILTER* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ORANGE FILTER]: Static Settings                    MyGateway


  Admin Status         : disable
  Orange Filter Ticket: B1BT

  Ticket Status        :

  Filtered Interface   : none
  History Entries      : 64

  Configure White List >
  Configure Filters >
  View History >


            SAVE                          CANCEL
```

Im Menü ***SECURITY*** ➜ ***COBION ORANGE FILTER*** lässt sich ein ➤➤ **URL**-basierter Content Filtering Dienst konfigurieren, der zur Laufzeit auf das OrangeFilter (vorher Produkt der Cobion AG) der Firma Internet Security Systems (www.iss.net) zugreift und überprüft, wie eine angeforderte Internet-Seite durch das OrangeFilter kategorisiert worden ist. Die Aktion, die sich aus der Kategorisierung ergibt, wird auf dem Gateway konfiguriert.

Das Menü ***SECURITY*** ➜ ***COBION ORANGE FILTER*** erlaubt die Konfiguration grundlegender Parameter sowie den Zugang zu weiteren Konfigurationsmenüs:

- ***CONFIGURE WHITE LIST***
- ***CONFIGURE FILTERS***
- ***VIEW HISTORY***.

Das Menü ***COBION ORANGE FILTER*** besteht aus folgenden Feldern:

Feld	Wert
Admin Status	Hier können Sie das Filter aktivieren. Die verfügbaren Einstellungen sind: ■ *disable* (Defaultwert): Content Filtering ist deaktiviert. ■ *enable*: Content Filtering ist aktiviert. ■ *enable 30 day demo ticket*: Eine 30-Tage-Demo-Lizenz des OrangeFilter wird aktiviert.
Orange Filter Ticket	Hier tragen Sie die Nummer der erworbenen OrangeFilter-Lizenz ein. Die voreingestellte, von ISS vergebene Kennung bezeichnet den Gerätetyp. Die Eingabe ist nur nötig für ***ADMIN STATUS*** = *enable*.
Expiring Date	Dieses Feld wird nur angezeigt, wenn eine Lizenz eingetragen und überprüft worden ist. Es zeigt das Ablaufdatum der Lizenz (relativ zur eingestellten Zeit auf dem Gateway) an und kann nicht editiert werden.
Ticket Status	Hier wird das Ergebnis der letzten Gültigkeitsprüfung des Lizenz angezeigt. Die Gültigkeit der Lizenz wird alle 23 Stunden überprüft.
Filtered Interfaces	Hier wählen Sie aus, für welches der vorhandenen Ethernet-Interfaces Content Filtering aktiviert werden soll. Es kann lediglich ein Interface spezifiziert werden. Die Aufrufe von Internetseiten, die über dieses Interface gehen, werden dann vom Content Filtering überwacht. Mögliche Werte: *en0-1*, *en0-1-nov*, *en0-2*, *en0-2-nov*, *en0-3*, *en0-3-nov*, *none*. Defaultwert ist *none*.

Feld	Wert
History Entries	Hier definieren Sie die Anzahl an Einträgen, die in der Content Filtering History gespeichert werden sollen. Der Wertebereich liegt zwischen *1* und *512*, der Defaultwert ist *64*.

Tabelle 2-1: Felder im Menü ***COBION ORANGE FILTER***

2.1 Untermenü Configure White List

Im Folgenden wird das Untermenü *CONFIGURE WHITE LIST* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ORANGE FILTER][WHITE LIST]: Url List              MyGateway

 White List:

   Url / Address
   www.bintec.de
   www.heise.de



   ADD                 DELETE              EXIT
```

Das Menü ***SECURITY*** ➜ ***COBION ORANGE FILTER*** ➜ ***CONFIGURE WHITE LIST*** enthält eine Liste derjenigen URLs bzw. IP-Adressen, die auch dann aufgerufen werden können, wenn sie aufgrund der Filterkonfiguration und der Klassifizierung im OrangeFilter blockiert würden (das Beispiel enthält beliebige Werte; in der Defaultkonfiguration sind keine Einträge enthalten).

Über die Schaltfläche ***ADD*** kann man weitere URLs oder IP-Adressen der Liste hinzufügen. Die Länge eines Eintrags ist auf 60 Zeichen begrenzt. Adressen, die in der White List geführt sind, werden automatisch zugelassen. Die Konfiguration eines entsprechenden Filters ist nicht notwendig.

2.2 Untermenü Configure Filters

Im Folgenden wird das Untermenü *CONFIGURE FILTERS* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ORANGE FILTER][FILTER]: Filter List                MyGateway

 Content Filter List:

Category                Day              Start  Stop   Action   Prio
Anonymous Proxies       Everyday         00:00  23:59  block     1
Criminal Activities     Everyday         00:00  23:59  block     11
Pornography / Nudity    Everyday         00:00  23:59  block     12
Unknown URL             Monday - Friday  00:00  23:59  logging   20
Ordering                Monday - Friday  00:00  23:59  logging   21
Default behaviour       Everyday         00:00  23:59  allow     30

   ADD                  DELETE              EXIT
```

Im Menü ***SECURITY*** ➜ ***COBION ORANGE FILTER*** ➜ ***CONFIGURE FILTERS*** konfigurieren Sie, welche Kategorien von Internetseiten auf welche Weise behandelt werden sollen. Hierfür konfigurieren Sie entsprechende Filter. Eine Liste der bereits konfigurierten Filter wird angezeigt (das Beispiel enthält beliebige Werte; in der Defaultkonfiguration sind keine Filter enthalten). Bei der Konfiguration der Filter gibt es grundsätzlich unterschiedliche Ansätze:

- Zum einen kann man eine Filterliste anlegen, die nur Einträge für solche Adressen enthält, die blockiert werden sollen. In diesem Fall ist es notwendig, am Ende der Filterliste einen Eintrag vorzunehmen, der alle Zugriffe, auf die kein Filter zutrifft, gestattet. (Einstellung dafür: ***CATEGORY*** = *Default behaviour*, ***ACTION*** = *logging* oder *allow*)
- Wenn Sie nur Einträge für solche Adressen anlegen, die zugelassen bzw. protokolliert (logging) werden sollen, ist eine Änderung des Default-Verhaltens (=alle übrigen Aufrufe werden geblockt) nicht notwendig.

Die Filter werden im Menü ***SECURITY*** ➜ ***COBION ORANGE FILTER*** ➜ ***CONFIGURE FILTERS*** ➜ ***ADD/EDIT*** hinzugefügt bzw. bearbeitet.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ORANGE FILTER][FILTER][ADD]                        MyGateway


      Category :  Anonymous Proxies

      Day      :  Everyday
      From     :  [0 :0 ]   To : [23:59]
      Action   :  block
      Priority :  0



              SAVE                                    CANCEL
```

Das Menü besteht aus folgenden Feldern:

Feld	Wert
Category	Hier wählen Sie aus, auf welche Kategorie von Adressen/URLs das Filter angewendet werden soll. Zur Auswahl stehen zum einen die Standardkategorien des Cobion OrangeFilters (Defaultwert: *Anonymous Proxies*). Darüber hinaus können Aktionen für folgende Sonderfälle definiert werden: ■ *Default behaviour*: Diese Kategorie trifft auf alle Internet-Adressen zu. ■ *No valid license ticket*: Wenn die Cobion OrangeFilter-Lizenz ungültig ist, trifft diese Kategorie auf alle Internet-Adressen zu.

Feld	Wert
Category (Forts.)	■ *Orange Server not reachable*: Sollten die Cobion-OrangeFilter-Server nicht erreichbar sein, wird die mit dieser Kategorie verbundene Aktion angewendet. ■ *Other Category*: Manche Adressen sind dem Cobion OrangeFilter bereits bekannt, aber noch nicht kategorisiert. Für derartige Adressen wird die mit dieser Kategorie verbundene Aktion angewendet. ■ *Unknown URL*: Wenn eine Adresse dem Cobion OrangeFilter nicht bekannt ist, wird die mit dieser Kategorie verbundene Aktion angewendet.
Day	Hier wählen Sie aus, an welchen Tagen das Filter aktiv sein soll. Zur Verfügung stehen: ■ *Everyday*: Das Filter gilt für jeden Tag der Woche. ■ *<Wochentag>*: Das Filter gilt für einen bestimmten Tag der Woche. Es kann pro Filter nur ein Tag ausgewählt werden, für mehrere einzelne Tage müssen mehrere Filter angelegt werden. ■ *Monday-Friday*: Das Filter gilt Montags bis Freitags. Default ist *Everyday*.
From	Hier geben Sie ein, nach welcher Uhrzeit das Filter aktiviert werden soll. Die Eingabe erfolgt nach dem Schema *hh:mm*. Default ist *0:0*.

Feld	Wert
To	Hier geben Sie ein, zu welcher Uhrzeit das Filter deaktiviert werden soll. Die Eingabe erfolgt nach dem Schema *hh:mm*. Default ist *23:59*.
Action	Hier wählen Sie die Aktion, die ausgeführt werden soll, wenn das Filter auf einen Aufruf zutrifft. Zur Verfügung stehen: ■ *block*: Der Aufruf der angeforderten Seite wird unterbunden. ■ *logging*: Der Aufruf wird zugelassen, aber protokolliert. Einsicht in die protokollierten Ereignisse ist im Menü ***SECURITY ➜ COBION ORANGE FILTER ➜ VIEW HISTORY*** möglich. ■ *allow*: Der Aufruf wird zugelassen, ohne protokolliert zu werden. Default ist *block*.
Priority	Hier weisen Sie dem Filter eine Priorität zu. Die Filter werden gemäß dieser Priorität angewendet. Der Wertebereich liegt zwischen *0* und *999*, ein Wert von *1* entspricht der höchsten Priorität. Der Wert *0* gibt an, dass es sich um einen Eintrag ohne Priorität handelt, er wird an die letzte Stelle der Filterliste gestellt. Defaultwert ist *0*.

Tabelle 2-2: Felder im Menü ***CONFIGURE FILTERS ➜ ADD/EDIT***

2.3 Untermenü View History

Im Folgenden wird das Untermenü *VIEW HISTORY* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ORANGE FILTER][HISTORY]: History List              MyGateway

History List:

Date  Time     Client      Url            Category            Action

11/12  16:09.52 192.168.0.1 www.xxx.de/    Pornography/Nudity  block
11/12  16:09.52 192.168.0.2 www.droge.de/  Drugs               block

                           EXIT
```

Im Menü ***SECURITY*** ➜ ***COBION ORANGE FILTER*** ➜ ***VIEW HISTORY*** können Sie die aufgezeichnete History des Content Filters einsehen. In der History werden alle Aufrufe protokolliert, die durch einen entsprechenden Filter dafür markiert werden (***ACTION*** = *logging*), ebenso alle abgewiesenen Aufrufe.

3 Untermenü Access Lists

Im Folgenden wird das Untermenü *ACCESS LISTS* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ACCESS]: IP Access Lists                            MyGateway


        Filter
        Rules
        Interfaces

        EXIT
```

In ***SECURITY*** ➜ ***ACCESS LISTS*** definieren Sie ➤➤ **Filter** für IP-Pakete, um den Zugang von bzw. zu den verschiedenen Hosts in angeschlossenen Netzwerken zu erlauben oder zu sperren. So können Sie verhindern, dass über das Gateway unzulässige Verbindungen aufbaut werden.

Access Listen definieren die Art des IP-Traffics, den das Gateway annehmen oder ablehnen soll. Die Zugangsentscheidung basiert auf Informationen, die in den IP-Paketen enthalten sind, z. B.:

- Quell- und/oder Ziel IP-Adresse
- Protokoll des Pakets
- Quell- und/oder Ziel-Port (Portbereiche werden unterstützt)

Möchten z.B. Standorte, deren LANs über ein Bintec Gateway miteinander verbunden sind, alle eingehenden FTP-Anfragen ablehnen, oder Telnet-Sitzungen nur zwischen bestimmten Hosts zulassen, sind Access Listen ein effektives Mittel.

IP-Filter (➤➤ **Access List**s) auf dem Gateway basieren auf der Kombination von Filtern und Aktionen zu Filterregeln (=rules) und der Verknüpfung dieser Regeln zu sogenannten Regelketten. Sie wirken auf die eingehenden Datenpa-

kete und können so bestimmten Daten den Zutritt zum Gateway erlauben oder verbieten.

Filter Ein Filter beschreibt einen bestimmten Teil des IP-Datenverkehrs, basierend auf Quell- und/oder Ziel-IP-Adresse, ➤➤ **Netzmaske**, Protokoll, Quell- und/oder Ziel-Port.

Regel Mit einer Regel teilen Sie dem Gateway mit, wie es mit gefilterten Datenpaketen umgehen soll – ob es sie annehmen oder abweisen soll. Sie können auch mehrere Regeln definieren, die Sie in Form einer Kette organisieren und ihnen damit eine bestimmte Reihenfolge geben.

Kette Für die Definition von Regeln bzw. Regelketten gibt es verschiedene Ansätze:

- Nehme alle Pakete an, die nicht explizit verboten sind, d. h.:
  - Weise alle Pakete ab, auf die Filter 1 zutrifft.
  - Weise alle Pakete ab, auf die Filter 2 zutrifft.
  - ...
  - Lass den Rest durch.
- Nehme nur Pakete an, die explizit erlaubt sind, d. h.:
  - Nehme alle Pakete an, auf die Filter 1 zutrifft.
  - Nehme alle Pakete an, auf die Filter 2 zutrifft.
  - ...
  - Weise den Rest ab.
- Kombination aus den beiden oben beschriebenen Möglichkeiten.

Es können mehrere getrennte Regelketten angelegt werden. Eine gemeinsame Nutzung von Filtern in verschiedenen Regelketten ist dabei möglich.

Schnittstelle Sie können jeder Schnittstelle individuell eine Regelkette zuweisen.

Achtung!

Achten Sie darauf, dass Sie sich beim Konfigurieren der Filter nicht selbst aussperren:

Greifen Sie zur Filter-Konfiguration möglichst über die serielle Konsolen-Schnittstelle oder mit ISDN-Login auf Ihr Gateway zu.

Wenn Sie trotzdem über Ihr LAN (z. B. mit telnet über ETH1) auf Ihr Gateway zugreifen, wählen Sie vor Beginn der Filter-Konfiguration im Menü *SECURITY* ➧ *ACCESS LISTS* ➧ *INTERFACES* ➧ EDIT (z.B. für *en0-1*) aus: First Rule = *none*.

Das Menü ***ACCESS LISTS*** besteht aus folgenden Untermenüs:

- ***FILTER***
- ***RULES***
- ***INTERFACES***

3.1 Untermenü Filter

Im Folgenden wird das Untermenü *FILTER* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ACCESS][FILTER]: Configure IP Access Filter       MyGateway

 Abbreviations: sa (source IP address)          sp (source port)
                da (destination IP address)     dp (destination port)
                it (icmp type)                  estab (TCP established)

  Index Descr           Conditions
  1     ToNetbiosPorts  dp 137-139


     ADD                 DELETE              EXIT
```

Das Menü ***SECURITY → ACCESS LISTS → FILTER*** dient zur Konfiguration von Filtern. Jedes Filter beschreibt einen bestimmten Teil von IP-Traffic und definiert z. B. die IP-Adressen, das Protokoll, den Quell- oder Ziel-Port.

In diesem Menü werden alle angelegten IP Access Filter aufgelistet. Angezeigt werden Indexnummer, Beschreibung und Bedingungen für jedes einzelne Filter. In der Spalte Bedingungen werden Abkürzungen verwendet. Diese werden im Feld oberhalb der Liste erläutert.

Das Menü ***ADD/EDIT*** dient der Konfiguration der Filter:

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY] [ACCESS] [FILTER] [EDIT]                              MyGateway

 Description                ToNetbiosPorts
 Index                      1

 Protocol  any

 Source Address
 Source Mask
 Source Port                any


 Destination Address
 Destination Mask
 Destination Port           specify range
 Specify Port               137       to Port   139
 Type of Service (TOS)      00000000  TOS Mask  00000000

                  SAVE                                CANCEL
```

Es besteht aus folgenden Feldern:

Feld	Wert
Description	Bezeichnung des Filters. Beachten Sie, dass in anderen Menüs nur die ersten 10 bzw. 15 Zeichen sichtbar sind.
Index	Kann hier nicht verändert werden. Das Gateway vergibt hier neu definierten Filtern automatisch eine Nummer.

Feld	Wert
Protocol	Legt ein Protokoll fest. Mögliche Werte: *any, icmp, ggp, ip, tcp, egp, igp, pup, chaos, udp, hmp, xns_idp, rdp, rsvp, gre, esp, ah, tlsp, skip, kryptolan, iso-ip, igrp, ospf, ipip, ipx-in-ip, vrrp, l2tp*. Die Option *any* passt auf jedes Protokoll. Defaultwert ist *any*.
Type	Nur bei ***PROTOCOL*** = *icmp*. Mögliche Werte: *any, echo reply, destination unreachable, source quench, redirect, echo, time exceeded, param problem, timestamp, timestamp reply, address mask, address mask reply*. Defaultwert ist *any*. Siehe RFC 792.
Connection State	Bei ***PROTOCOL*** = *tcp* können Sie ein Filter definieren, das den Status von TCP-Verbindung berücksichtigt. Mögliche Werte: ■ *established*: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das **VPN Access** Gateway keine neue TCP-Verbindung öffnen würden. ■ *any (Defaultwert)*: Das Filter passt auf alle TCP-Pakete.
Source Address	Quell-IP-Adresse der Datenpakete
Source Mask	Netzmaske zu ***SOURCE ADDRESS***
Source Port	Quell-Port-Nummer bzw. Bereich von Quell-Port-Nummern. Mögliche Werte siehe Tabelle “Auswahlmöglichkeiten von Source Port bzw. Destination Port” auf Seite 19. Defaultwert ist *any*.

Feld	Wert
Specify Port .. to Port	Bei ***SOURCE PORT*** bzw. ***DESTINATION PORT*** = *specify* bzw. *specify range*: Port-Nummern bzw. Bereich von Port-Nummern.
Destination Address	Definiert die Ziel-IP-Adresse der Datenpakete.
Destination Mask	Netzmaske zu ***DESTINATION ADDRESS***
Destination Port	Ziel-Port-Nummer bzw. Bereich von Ziel-Port-Nummern, auf den das Filter passt. Mögliche Werte siehe Tabelle “Auswahlmöglichkeiten von Source Port bzw. Destination Port” auf Seite 19. Defaultwert ist *any*.
Type of Service <TOS>	Kennzeichnet die Priorität des IP-Pakets, vgl. RFC 1349 und RFC 1812. (Angabe im binären Format)
TOS Mask	Bitmaske für Type of Service. (Angabe im binären Format)

Tabelle 3-1: Felder im Menü ***FILTER***

SOURCE PORT bzw. ***DESTINATION PORT*** enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
any	Das Filter passt auf alle ➤➤ **Port**-Nummern.
specify	Ermöglicht Eingabe einer Port-Nummer unter ***SPECIFY PORT***.
specify range	Ermöglicht Eingabe eines Bereiches von Port-Nummern unter ***SPECIFY PORT ... TO PORT ...***.
priv (0..1023)	Port-Nummern: *0 ... 1023*, sog. Well Known Ports
server (5000..32767)	Port-Nummern: *5000 ... 32767*
clients 1 (1024..4999)	Port-Nummern: *1024 ... 4999*

Wert	Bedeutung
clients 2 (32768..65535)	Port-Nummern: *32768 ... 65535*
unpriv (1024..65535)	Port-Nummern: *1024 ... 65535*

Tabelle 3-2: Auswahlmöglichkeiten von ***SOURCE PORT*** bzw. ***DESTINATION PORT***

3.2 Untermenü Rules

Im Folgenden wird das Untermenü *RULES* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ACCESS][RULE]: Configure IP Access Rules           MyGateway

 Abbreviations:   RI  (Rule Index)      M  (Action if filter matches)
                  FI  (Filter Index)   !M  (Action if filter does not
                                            match)
                  NRI (Next Rule Index)

  RI   FI   NRI  Action    Filter      Conditions
  1    1    0    deny M    ToNetbiosP  sp 137-139



    ADD             DELETE          REORG         EXIT
```

Im Menü ***IP*** ➜ ***ACCESS LISTS*** ➜ ***RULES*** werden Regeln für IP-Filter konfiguriert. Diese können separat angelegt oder in Regelketten eingebunden werden.

In ***IP*** ➜ ***ACCESS LISTS*** ➜ ***RULES*** werden alle angelegten Filterregeln aufgelistet. Aufgeführt werden ***RF***, ***FI***, ***NRI***, ***ACTION***, ***FILTER*** (nur die ersten 10 Zeichen werden angezeigt) und ***CONDITIONS***. Die Bedeutung der Abkürzungen steht im oberen Teil des Setup Tool Fensters.

Hinzufügen neuer oder Editieren bestehender Regeln erfolgt im Menü ***RULES*** ➜ ***ADD/EDIT.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY] [ACCESS] [RULE] [EDIT]                                MyGateway


    Action          deny   M

    Filter          ToNetbiosPorts


              SAVE                              CANCEL
```

Das Menü ***RULES*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Index	Erscheint nur bei ***EDIT***. Kann nicht verändert werden. Hier wird der ***INDEX*** von bestehenden Regeln angezeigt. Das Gateway vergibt neu definierten Regeln automatisch eine Nummer.
Insert behind Rule	Erscheint nur, bei ***ADD*** und wenn mindestens eine Regel vorhanden ist. Legt fest, hinter welche bestehende Regel die neue Regel eingefügt wird. Mit *none* beginnen Sie eine neue eigenständige Kette.

Feld	Wert
Action	Legt fest, wie mit einem gefilterten Datenpaket verfahren wird. ■ *allow M* (Defaultwert): Paket annehmen, wenn das Filter passt. ■ *allow !M*: Paket annehmen, wenn das Filter nicht passt. ■ *deny M*: Paket abweisen, wenn das Filter passt. ■ *deny !M*: Paket abweisen, wenn das Filter nicht passt. ■ *ignore*: Nächste Regel anwenden.
Filter	Legt fest, welches Filter verwendet wird.
Next Rule	Erscheint nur, wenn eine bestehende Regel editiert wird. Legt fest, welche Regel als nächste angewendet wird.

Tabelle 3-3: Felder im Menü ***RULES***

Im Menü ***ACCESS LIST*** ➜ ***RULES*** ➜ ***REORG*** können Sie die Indizierung der Regeln neu ordnen lassen, wobei die Reihenfolge der angelegten Regeln beibehalten wird. Im Feld ***INDEX OF RULE THAT GETS INDEX 1*** wird diejenige Regel festgelegt, die den Rule ***INDEX 1*** erhalten soll.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ACCESS][RULE][REORG]: Reorganize Rules              MyGateway

       Index of Rule that gets Index 1      none


            REORG                                   CANCEL
```

Standardmäßig wird immer die Regelkette, die mit Rule ***INDEX** 1* anfängt, auf die Schnittstelle des Gateways (z. B. WAN-Partner) angewendet.

3.3 Untermenü Interfaces

Im Folgenden wird das Untermenü *INTERFACES* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ACCESS][INTERFACES]: Configure First Rules          MyGateway


 Configure first rules for interfaces

 Interface       First Rule             First Filter
 en0-1           1    (no access rules)
 en0-1-snap      1    (no access rules)
 en0-2           1    (no access rules)
 en0-2-snap      1    (no access rules)
 en0-3           1    (no access rules)
 en0-3-snap      1    (no access rules)


 EXIT
```

In ***IP*** ➜ ***ACCESS LISTS*** ➜ ***INTERFACES*** werden alle Interfaces des Gateways aufgelistet und die Zuordnung von Regelketten zu den Interfaces angezeigt.

Die Konfiguration der Zuordnung erfolgt im Menü ***IP*** ➜ ***ACCESS LISTS*** ➜ ***INTERFACES*** ➜ ***EDIT***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ACCESS][INTERFACES][EDIT]                           MyGateway


   Interface            en0-1
   First Rule           RI 1   FI 1   (to-netbios-ports)

   Deny Silent          yes
   Reporting Method     info


                 SAVE                                  CANCEL
```

Hier werden die konfigurierten Regelketten den einzelnen Interfaces zugeordnet und das Verhalten des Gateways beim Abweisen von IP-Paketen festgelegt.

Das Untermenü ***EDIT*** enthält folgende Felder:

Feld	Wert
Interface	Name des Interfaces, das ausgewählt wurde. Dieses Feld kann nicht bearbeitet werden.
First Rule	Definiert den Beginn der Regelkette, die auf Datenpakete, die über ***INTERFACE*** eingehen, angewendet werden soll. Mit *none* (Defaultwert) legen Sie fest, dass auf ***INTERFACE*** keine Filter angewendet werden.
Deny Silent	Legt fest, ob beim Abweisen eines IP-Paketes der Absender informiert werden soll. Mögliche Werte: ■ *no*: Der Absender erhält eine ICMP-Nachricht. ■ *yes* (Defaultwert): Der Absender wird nicht informiert.
Reporting Method	Legt fest, ob bei Abweisung eines IP-Paketes eine Syslog-Meldung erzeugt werden soll. Mögliche Werte: ■ *none*: Keine Syslog-Meldung. ■ *info* (Defaultwert): Eine Syslog-Meldung mit Angabe von Protokollnummer, Quell-IP-Adresse und Quell-Port-Nummer wird generiert. ■ *dump*: Eine Syslog-Meldung mit dem Inhalt der ersten 64 Bytes des abgewiesenen Pakets wird generiert.

Tabelle 3-4: Felder im Untermenü ***INTERFACES***

3 Untermenü Access Lists

4 Untermenü Stateful Inspection

Im Folgenden wird das Untermenü *STATEFUL INSPECTION* beschrieben.

Mit einer Stateful Inspection Firewall (SIF) verfügen **VPN Access** Gateways über eine leistungsfähige Sicherheitsfunktion.

Zusätzlich zur sogenannten statischen Paketfilterung (siehe "Untermenü Access Lists" auf Seite 13) hat eine SIF durch dynamische Paketfilterung einen entscheidenden Vorteil: Die Entscheidung, ob ein Paket weitergeleitet wird, kann nicht nur aufgrund von Quell- und Zieladressen oder ➤➤ **Port**s, sondern auch mittels dynamischer Paketfilterung aufgrund des Zustands (state) der Verbindung zu einem Partner gefällt werden.

Es können also auch solche Pakete weitergeleitet werden, die zu einer bereits aktiven Verbindung gehören. Dabei akzeptiert die SIF auch Pakete, die zu einer "Tochterverbindung" gehören. Bsp.: Die Aushandlung einer ➤➤ **FTP**-Verbindung findet über den Port 21 statt, der eigentliche Datenaustausch kann aber über einen völlig anderen Port erfolgen.

SIF und andere Sicherheitsfunktionen

Bintecs Stateful Inspection Firewall fügt sich wegen ihrer einfachen Konfiguration gut in die bestehende Sicherheitsarchitektur der Bintec-Gateways ein. Systemen wie Network Address Translation (➤➤ **NAT**) und ➤➤ IP **Access Lists** (IPAL) gegenüber ist der Konfigurationsaufwand der SIF vergleichbar einfach.

Da SIF, NAT und IPAL gleichzeitig im System aktiv sind, muss man auf mögliche Wechselwirkungen achten: Wenn ein beliebiges Paket von einer der Sicherheitsinstanzen verworfen wird, so geschieht dies unmittelbar, d. h. es ist irrelevant, ob es von einer anderen Instanz zugelassen werden würde. Daher sollte man den eigenen Bedarf an Sicherheitsfunktionen genau analysieren.

Der wesentliche Unterschied zwischen SIF und NAT/IPAL besteht darin, dass die Regeln der SIF generell global angewendet werden, d. h. nicht auf ein Interface beschränkt sind.

Grundsätzlich werden aber die selben Filterkriterien auf den Datenverkehr angewendet wie bei NAT und IPAL:

- Quell- und Zieladresse des Pakets (mit einer zugehörigen Netzmaske)
- Dienst (vorkonfiguriert, z. B. Echo, FTP, HTTP)

- Protokoll
- Portnummer(n)

Um die Unterschiede in der Paketfilterung zu verdeutlichen, folgt eine Aufstellung der einzelnen Sicherheitsinstanzen und ihrer Funktionsweise:

NAT Eine der Grundfunktionen von NAT ist die Umsetzung lokaler IP-Adressen Ihres LANs in die globalen IP-Adressen, die Ihnen von Ihrem ➤➤ **ISP** zugewiesen werden, und umgekehrt. Dabei werden zunächst alle von außen initiierten Verbindungen abgeblockt, d. h. jedes Paket, dass das Gateway nicht einer bereits bestehenden Verbindung zuordnen kann, wird abgewiesen. Auf diese Art kann eine Verbindung lediglich von innen nach außen aufgebaut werden. Ohne explizite Genehmigungen wehrt NAT jeden Zugriff aus dem ➤➤ **WAN** auf das LAN ab.

IP Access Lists Hier werden Pakete ausschließlich aufgrund der oben aufgeführten Kriterien zugelassen oder abgewiesen, d. h. der Zustand der Verbindung wird nicht berücksichtigt (ausser bei ***PROTOCOL*** = *tcp*).

SIF Die SIF sondert alle Pakete aus, die nicht explizit oder implizit zugelassen werden. Dabei gibt es sowohl einen "deny", bei dem keine Fehlermeldung an den Sender des zurückgewiesenen Pakets ausgegeben wird, als auch einen "reject", bei dem der Sender über die Ablehnung des Pakets informiert wird.

Die Bearbeitung eingehender Pakete erfolgt folgendermaßen:

- Zunächst überprüft die SIF, ob ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann. Ist dies der Fall, wird es weitergeleitet. Kann das Paket keiner bestehenden Verbindung zugeordnet werden, wird überprüft, ob eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden). Ist dies der Fall, wird das Paket ebenfalls akzeptiert.
- Wenn das Paket keiner bestehenden und auch keiner zu erwartenden Verbindung zugeordnet werden kann, werden die SIF-Filterregeln angewendet: Trifft auf das Paket eine Deny-Regel zu, wird es abgewiesen, ohne dass eine Fehlermeldung an den Sender des Pakets geschickt wird; trifft eine Reject-Regel zu, wird das Paket abgewiesen und eine ➤➤ **ICMP**-Host-Unreachable-Meldung an den Sender des Paktes ausgegeben. Nur wenn auf das Paket eine Accept-Regel zutrifft, wird es weitergeleitet.

- Alle Pakete, auf die keine Regel zutrifft, werden nach Kontrolle aller vorhandenen Regeln ohne Fehlermeldung an den Sender abgewiesen (=Defaultverhalten).

Im Folgenden werden die Menüs, in denen Sie die SIF konfigurieren, beschrieben.

Das Menü ***SECURITY*** ➜ ***STATEFUL INSPECTION*** zeigt globale Parameter an und führt in weitere Untermenüs:

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION]: Static settings              MyGateway

  Stateful Inspection Firewall global settings:

         Adminstatus    :  enable
         Local Filter   :  disable
         Full Filtering :  enable
         Logging level  :  all


         Edit Filters >
         Edit Services >
         Edit Addresses >

         Advanced settings >


                  SAVE                          CANCEL
```

Das Menü ***STATEFUL INSPECTION*** besteht aus folgenden Feldern:

Feld	Wert
Adminstatus	Hier können Sie die Funktion grundsätzlich aktivieren und deaktivieren. Zur Verfügung stehen: ■ *enable*: Defaultwert ■ *disable*

Feld	Wert
Local Filter	Hier legen Sie fest, ob lokal initiierte Verbindungen ebenfalls von der SIF gefiltert werden sollen. Zur Verfügung stehen: ■ *enable*: Lokal erzeugte Requests werden ebenfalls gefiltert. ■ *disable*: Lokal erzeugte Requests werden generell zugelassen (Defaultwert).
Full Filtering	Hier legen Sie fest, ob nur Pakete gefiltert werden sollen, die an ein anderes Interface gesendet werden als das, das die Verbindung erzeugt hat. Zur Verfügung stehen: ■ *enable*: Alle Pakete werden gefiltert (Defaultwert). ■ *disable*: Nur Pakete, bei denen sich das Ziel-Interface vom Ausgangs-Interface der Verbindung unterscheidet, werden gefiltert.

Feld	Wert
Logging level	Hier können Sie den SIF-Syslog-Level auswählen. Die Ausgabe der Meldungen erfolgt zusammen mit den Meldungen der anderen Subsysteme, siehe Handbuch Teil **Monitoring and Debugging,** Kapitel Messages). Zur Verfügung stehen: ■ *all*: Alle SIF-Aktivitäten werden angezeigt (Defaultwert). ■ *deny only*: Nur Reject- und Deny-Ereignisse werden angezeigt, vgl. "Action" auf Seite 33. ■ *accept only*: Nur Accept-Ereignisse werden angezeigt. ■ *none*: Syslog Messages werden nicht erzeugt.

Tabelle 4-1: Felder im Menü ***STATEFUL INSPECTION***

Vom Menü ***SECURITY*** ➜ ***STATEFUL INSPECTION*** gelangt man zur Konfiguration der Filter (***EDIT FILTERS***) sowie der Services (***EDIT SERVICES***) und der Adressen für die Filter (***EDIT ADDRESSES***). Darüber hinaus gelangt man in das Menü ***ADVANCED SETTINGS***.

4.1 Untermenü Edit Filters

Im Folgenden wird das Untermenü *EDIT FILTERS* beschrieben.

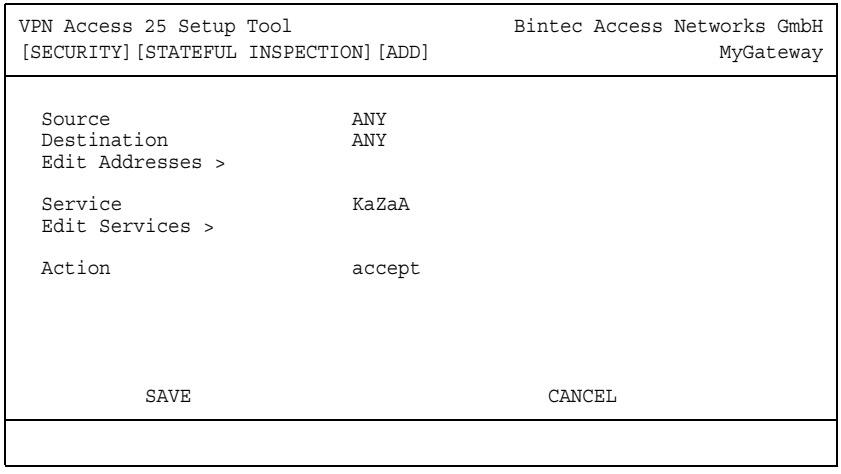
```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][FILTERS]: Configuration      MyGateway

 Stateful Inspection Filter List:

       Press 'u' to move Filter up or press 'd' to move Filter down.

Pos. Source           Destination          Service              Action




   ADD                 DELETE               SAVE                 CANCEL
```

Die konfigurierten SIF Filterregeln werden im Menü ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** aufgelistet.

Das Default-Verhalten mit der ***ACTION*** *allow* besteht aus zwei impliziten Filterregeln: wenn ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann und wenn eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden), wird das Paket zugelassen.

Die Abfolge der Filterregeln in der Liste ist relevant: Die Filterregeln werden der Reihe nach auf jedes Paket angewendet, bis eine Filterregel zutrifft. Kommt es zu Überschneidungen, d. h. trifft für ein Paket mehr als eine Filterregel zu, wird lediglich die erste Filterregel ausgeführt. Wenn also die erste Filterregel ein Paket zurückweist, während eine später es zulässt, so wird es abgewiesen. Ebenso bleibt eine Deny-Regel ohne Auswirkung, wenn ein entsprechendes Paket zuvor von einer anderen Filterregel zugelassen wird.

Im Menü ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD/EDIT*** fügen Sie eine Filterregel für die SIF hinzu oder editieren eine bestehende.



Das Menü ***EDIT FILTERS*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Source	Hier können Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets auswählen. Das Gateway liest die Liste bestehender WAN- und LAN-Interfaces aus und bietet diese als Voreinstellung an. Defaultwert ist *ANY*. Einen neuen Alias erstellen Sie in ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD/EDIT*** ➜ ***EDIT ADDRESSES*** ➜ ***ADD/EDIT***. Siehe “Untermenü Edit Addresses” auf Seite 35.

Feld	Wert
Destination	Hier können Sie einen der vorkonfigurierten Alias für das Ziel des Pakets auswählen. Das Gateway liest die Liste bestehender WAN- und LAN-Interfaces aus und bietet diese als Voreinstellung an. Defaultwert ist *ANY*. Einen neuen Alias erstellen Sie ebenfalls in ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD/EDIT*** ➜ ***EDIT ADDRESSES*** ➜ ***ADD/EDIT***. Siehe “Untermenü Edit Addresses” auf Seite 35.
Service	Hier können Sie einen der vorkonfigurierten Dienste auswählen, dem das zu filternde Paket zugeordnet sein muss. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: ■ *ftp* ■ *telnet* ■ *smtp* ■ *dns* ■ *http* ■ *nntp* ■ *internet* ■ *netmeeting* Im Menü ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD/EDIT*** ➜ ***EDIT SERVICES*** können Sie weitere Dienste konfigurieren. Siehe “Untermenü Edit Services” auf Seite 33.

Feld	Wert
Action	Hier wählen Sie die Aktion, die auf ein gefiltertes Paket angewendet werden soll. Die möglichen Werte sind: ■ *accept* (Defaultwert) ■ *deny* ■ *reject* Sowohl bei *reject* als auch bei *deny* wird das Paket abgewiesen, bei *deny* jedoch, ohne dass eine Fehlermeldung an den Sender des Pakets ausgegeben wird.

Tabelle 4-2: Felder im Menü ***EDIT FILTERS***

4.2 Untermenü Edit Services

Im Folgenden wird das Untermenü *EDIT SERVICES* beschrieben.

Im Menü ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES*** wird eine Liste von über 60 vorkonfigurierten Dienstaliasen angezeigt.

Durch ***ADD*** oder die Auswahl eines bestehenden Eintrags gelangen Sie in das Menü ***SECURITY*** ➜ ***STATEFIUL INSPECTION*** ➜ ***EDIT SERVICES*** ➜ ***ADD/EDIT,*** in dem Sie einen weiteren Dienstalias definieren oder einen bestehenden editieren können. In dieses Menü gelangen Sie auch über ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD*** ➜ ***EDIT SERVICES*** ➜ ***ADD/EDIT***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][SERVICES][ADD]                MyGateway

            Alias

            Protocol                    ah




          SAVE                                  CANCEL
```

Das Menü ***EDIT SERVICES*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Alias	Hier geben Sie einen Alias für den Dienst ein, den Sie konfigurieren wollen.
Protocol	Hier wählen Sie das Protokoll aus, auf dem der Dienst basiert. Es stehen die wichtigsten Protokolle zur Auswahl. (Bei ***ADD*** is *ah* Defaultwert.)
ICMP Type	Nur wenn Sie für ***PROTOCOL*** den Wert *icmp* gewählt haben. Der Wert dieses Felds ist werkseitig auf *echo* gesetzt. Diese Einstellung deckt die sogenannten Pings ab. Der Wert kann nicht verändert werden.
Port	Nur wenn Sie für ***PROTOCOL*** den Wert *tcp*, *udp/tcp* oder *udp* gewählt haben. Hier geben Sie den Port an, über den der Dienst läuft. Mögliche Werte sind *1* bis *65535*. Defaultwert ist *1.*

Feld	Wert
Range	Nur, wenn Sie für ***PROTOCOL*** den Wert *tcp*, *udp/tcp* oder *udp* gewählt haben. Hier geben Sie an, wieviele aufeinanderfolgende Ports inkl. des in ***PORT*** eingestellten Wertes der Dienst verwendet. Mögliche Werte sind *1* bis *65535*. Wenn Sie keinen Wert eingeben, nimmt das Gateway den Wert *1* als Default an.

Tabelle 4-3: Felder im Menü ***EDIT SERVICES***

4.3 Untermenü Edit Addresses

Im Folgenden wird das Untermenü *EDIT ADDRESSES* beschrieben.

Im Menü ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESSES*** werden alle konfigurierten Aliase aufgelistet. Die Liste besteht aus den auf dem Gateway konfigurierten Interfaces. Durch ***ADD*** oder die Auswahl eines bestehenden Eintrags gelangen Sie in das Menü ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESSES*** ➜ ***ADD/EDIT***, in dem sie weitere Adressaliase anlegen oder bestehende ändern können. In dieses Menü gelangt man auch über ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD*** ➜ ***EDIT ADDRESSES*** ➜ ***ADD/EDIT***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][ADDRESSES][ADD]                MyGateway

          Alias
          Mode                          interface
          Interface                     en0-1


           SAVE                                    CANCEL
```

Das Menü ***EDIT ADDRESSES*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Alias	Hier geben Sie einen Aliasnamen ein, den Sie einrichten wollen.
Mode	Hier geben Sie an, ob Sie eine IP-Adresse (*Address/Range* oder *Adress/Subnet*) oder ein Interface (*interface*) mit dem Alias bezeichnen wollen. Mögliche Werte: ■ *interface* (Defaultwert) ■ *Address/Range* ■ *Address/Subnet*.
IP-Address	Nur, wenn Sie für ***MODE*** den Wert *Address/Range* oder *Address/Subnet* gewählt haben. Hier geben Sie die IP-Adresse ein, für die der Alias gelten soll.
IP-Range	nur für ***MODE*** = *Address/Range* Hier geben Sie die Anzahl der aufeinanderfolgenden IP-Adressen inkl. der in ***IP-ADDRESS*** eingegebenen Adresse an.
IP-Mask	Nur, wenn Sie für ***MODE*** den Wert *Address/Subnet* gewählt haben. Hier geben Sie die zur IP-Adresse des Hosts gehörende Netzmaske ein. Defaultwert ist *255.255.255.255*.
Interface	Nur, wenn Sie für ***MODE*** den Wert *interface* gewählt haben. Hier wählen Sie das Interface aus, über das Pakete empfangen und gesendet werden. Sie können unter allen konfigurierten WAN-Partnern und LAN-Interfaces wählen.

Tabelle 4-4: Felder im Menü ***EDIT ADDRESSES***

4.4 Untermenü Advanced settings

Im Folgenden wird das Untermenü *ADVANCED SETTINGS* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][ADVANCED]: Settings          MyGateway

 Stateful Inspection session expiration:

        UDP   inactivity Timeout : 180
        TCP   inactivity Timeout : 3600
        PPTP  inactivity Timeout : 86400
        Other inactivity Timeout : 30




           SAVE                                    CANCEL
```

Im Menü ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***ADVANCED SETTINGS*** werden Einstellungen zum Session Timeout vorgenommen.

Das Menü ***ADVANCED SETTINGS*** besteht aus folgenden Feldern:

Feld	Wert
UDP inactivity Timeout	Hier können Sie eingeben, nach welcher Zeit der Inaktivität eine ➤➤ **UDP**-Session als abgelaufen betrachtet wird (in Sekunden). Zur Verfügung stehen Werte von *30* bis *86400*. Der Defaultwert ist *180*.
TCP inactivity Timeout	Hier können Sie eingeben, nach welcher Zeit der Inaktivität eine ➤➤**TCP**-Session als abgelaufen betrachtet wird (in Sekunden). Zur Verfügung stehen Werte von *30* bis *86400*. Der Defaultwert ist *3600*.

Feld	Wert
PPTP inactivity Timeout	Hier können Sie eingeben, nach welcher Zeit der Inaktivität eine PPTP-Session als abgelaufen betrachtet wird (in Sekunden). Zur Verfügung stehen Werte von *30* bis *86400*. Der Defaultwert ist *86400*.
Other inactivity Timeout	Hier können Sie eingeben, nach welcher Zeit der Inaktivität eine Session eines anderen Typs als abgelaufen betrachtet wird (in Sekunden). Zur Verfügung stehen Werte von *30* bis *86400*. Der Defaultwert ist *30*.

Tabelle 4-5: Felder im Menü ***ADVANCED SETTINGS***

5 Untermenü SSH Daemon

Im Folgenden wird das Untermenü *SSH DAEMON* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][SSHD]: SSH Daemon Configuration                    MyGateway


    SSH Daemon                                  running

    Static Settings >
    Timer >

    Authentication Algorithms >
    Supported Ciphers >
    Message Authentication Codes >


    Certification Management >

    Monitoring >

         SAVE                                   EXIT
```

Ihr Gateway bietet einen verschlüsselten Zugang zur Shell (siehe Handbuch Teil **Zugang und Konfiguration**). Diesen Zugang können Sie im Menü ***SECURITY*** ➜ ***SSH DAEMON*** aktivieren (*running*, Defaultwert) oder deaktivieren (*stopped*) und haben Zugriff auf die Menüs zur Konfiguration des SSH Login.

Um den SSH Daemon ansprechen zu können, wird eine SSH Client-Anwendung, z.B. PuTTY, benötigt.

Wenn Sie SSH Login zusammen mit dem PuTTY-Client verwenden wollen, müssen Sie einige Besonderheiten bei der Konfiguration beachten. Wir haben diesbezüglich eine FAQ erstellt. Sie finden diese im Bereich Service/Support auf www.bintec.de.

Um die Shell Ihres Gateways über einen SSH Client erreichen zu können, stellen Sie sicher, dass die Einstellungen beim SSH Daemon und dem SSH Client übereinstimmen.

Hinweis

Nach der Konfiguration sollten Sie kontrollieren, dass der SSH Daemon gestartet ist: Geben Sie in der Shell `ps -e` ein und verifizieren Sie, dass der `sshd` aufgeführt ist.

Sollte dies nicht der Fall sein, müssen Sie das Gateway neu starten, um den SSH-Daemon zu starten.

5.1 Untermenü Static Settings

Im Folgenden wird das Untermenü *STATIC SETTINGS* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][SSHD][STATIC]: SSHD Static Options                  MyGateway


  Max. # of Clients                 1
  Port # used for Connections       22
  Compression                       disabled

  Verify Reverse Mapping            disabled




  Print Motd                        enabled
  Print LastLog                     disabled


  Logging Level                     info

              SAVE                          CANCEL
```

Im Menü ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***STATIC SETTINGS*** bestimmen Sie grundlegende Parameter des SSH Daemons.

Das Menü ***STATIC SETTINGS*** besteht aus folgenden Feldern:

Feld	Wert
Max. # of Clients	Hier wird angegeben, wie viele gleichzeitige Verbindungen zum SSH-Daemon gestattet sind. Weitere Verbindungen werden abgewiesen, bis eine Verbindung beendet ist. Das Feld ist nicht editierbar, da nur eine einzelne SSH-Verbindung möglich ist.
Port # used for Connections	Hier geben Sie an, auf welchem Port sich ein Client mit dem SSH-Daemon verbinden kann. Mögliche Werte sind *1* bis *65535*. Der Defaultwert ist *22*.
Compression	Hier können Sie die Verwendung von Datenkompression aktivieren (*enabled*) bzw. deaktivieren (*disabled*). Der Defaultwert ist *disabled*.
Verify Reverse Mapping	Hier wählen Sie aus, ob der SSH-Daemon einen "Reverse Lookup" der Client-IP-Adresse durchführt. Dabei wird verifiziert, dass der zur IP-Adresse gehörende Host-Name korrekt ist, die IP-Adresse also nicht gefälscht wurde. Falls die IP-Adresse gefälscht wurde, wird die Verbindung abgebrochen. Zur Verfügung stehen: ■ *disabled* (Defaultwert) ■ *enabled*.
Print Motd	Hier wählen Sie aus, ob der SSH-Daemon eine "Message of the Day (MotD)" ausgibt, sobald sich ein Client angemeldet hat. Zur Verfügung stehen: ■ *disabled* ■ *enabled* (Defaultwert).

Feld	Wert
Print LastLog	Hier wählen Sie aus, ob der SSH-Daemon beim Login eines Clients Datum und Uhrzeit des letzten Logins ausgeben soll. Zur Verfügung stehen: ■ *disabled* (Defaultwert) ■ *enabled*.
Logging Level	Hier können Sie den Syslog-Level für die vom SSH-Daemon generierten Syslog Messages auswählen. Zur Verfügung stehen: ■ *quiet*: Es werden keine Meldungen aufgezeichnet. ■ *fatal*: Es werden nur schwerwiegende Fehler des SSH Daemon aufgezeichnet. ■ *error:* Es werden schwerwiegende Fehler und einfache Fehler des SSH Daemon aufgezeichnet. ■ *info* (Defaultwert)*:* Es werden schwerwiegende Fehler, einfache Fehler des SSH Daemon und Infomeldungen aufgezeichnet. ■ *debug* Es werden alle Meldungen aufgezeichnet.

Tabelle 5-1: Felder im Menü ***STATIC SETTINGS***

5.2 Untermenü Timer

Im Folgenden wird das Untermenü *TIMER* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][SSHD][TIMER]: SSHD Timer Options                    MyGateway

 Login Grace Time                    600

 TCP Keepalives                      enabled

 ClientAliveCountMax                 3

 ClientAliveInterval                 10



                SAVE                              CANCEL
```

Im Menü ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***TIMER*** können Sie zeitabhängiges Verhalten des SSH-Daemon konfigurieren.

Das Menü ***TIMER*** besteht aus folgenden Feldern:

Feld	Wert
Login Grace Time	Hier geben Sie den Zeitraum ein, innerhalb dessen sich ein Client authentisieren muss, bevor die SSH-Verbindung abgebrochen wird. Zur Verfügung stehen Werte von *0* bis *3600* (Sekunden). Ein Wert von *0* bedeutet keine Begrenzung, der Defaultwert ist *600*.
TCP Keepalives	Hier wählen Sie aus, ob das Gateway Keepalive-Pakete senden soll. Zur Verfügung stehen: ■ *disabled* ■ *enabled*: Defaultwert. Der Wert sollte für Client und Server gleich konfiguriert werden.

Feld	Wert
ClientAliveCountMax	Diese Feld ist nur für ***TCP KEEPALIVES*** = *enabled* zu konfigurieren. Hier geben Sie die Anzahl der vom Gateway gesendeten Keepalive-Pakete an, die unbeantwortet bleiben dürfen, bevor der SSH-Daemon die Verbindung unterbricht. Zur Verfügung stehen Werte von *0* bis *10*, der Defaultwert ist *3*.
ClientAliveInterval	Diese Feld ist nur für ***TCP KEEPALIVES*** = *enabled* zu konfigurieren. Hier geben Sie das Intervall an, nach dessen Ablauf der SSH-Daemon einen Keepalive Request an den Client sendet, wenn keine Daten mehr vom Client empfangen werden. Zur Verfügung stehen Werte von *1* bis *3600* (Sekunden), der Defaultwert ist *10*.

Tabelle 5-2: Felder des Menüs ***TIMER***

5.3 Untermenü Authentication Algorithms

Im Folgenden wird das Untermenü *AUTHENTICATION ALGORITHMS* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][SSHD][AUTH]: SSHD Authentication Options          MyGateway

  Protocol Version                  2


  Public Key                        enabled
  Password                          enabled
  Challenge Response                enabled


           SAVE                           CANCEL
```

Im Menü ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***AUTHENTICATION ALGORITHMS*** können Sie die Mechanismen der Authentisierung für einen SSH-Verbindungsaufbau konfigurieren.

Das Menü ***AUTHENTICATION ALGORITHMS*** besteht aus folgenden Feldern:

Feld	Wert
Protocol Version	Hier wird angezeigt, welche SSH-Version der SSH-Daemon verwendet. Das Feld ist nicht editierbar, da derzeit lediglich Version 2 unterstützt wird.
Public Key	Hier wählen Sie aus, ob eine Public-Key-Authentisierung des Clients zulässig ist oder nicht. Zur Verfügung stehen: ■ *disabled* ■ *enabled*: Defaultwert. Diese Funktion steht derzeit noch nicht zur Verfügung.

Feld	Wert
Password	Hier wählen Sie aus, ob eine Passwort-Authentisierung des Clients zulässig ist oder nicht. (Das Anmelden über den SSH Client ist nur als Benutzer *admin*, mit dem dazugehörigen Passwort möglich.) Zur Verfügung stehen: ■ *disabled* ■ *enabled*: Defaultwert.
Challenge Response	Hier wählen Sie aus, ob eine Challenge-Response-Authentisierung des Clients zulässig ist oder nicht. Zur Verfügung stehen: ■ *disabled* ■ *enabled*: Defaultwert. Diese Funktion steht derzeit noch nicht zur Verfügung.

Tabelle 5-3: Felder des Menüs ***AUTHENTICATION ALGORITHMS***

5.4 Untermenü Supported Ciphers

Im Folgenden wird das Untermenü *SUPPORTED CIPHERS* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][SSHD][AUTH]: SSHD Cipher Options                  MyGateway

    aes128                                  enabled
    3des                                    enabled
    blowfish                                enabled
    cast128                                 enabled
    arc4                                    enabled
    aes192                                  disabled
    aes256                                  disabled

         SAVE                               CANCEL
```

Im Menü ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***SUPPORTED CIPHERS*** können Sie die Algorithmen festlegen, die für die Verschlüsselung der SSH-Verbindung verwendet werden dürfen.

Mögliche Algorithmen:

- ***AES128***
- ***3DES***
- ***BLOWFISH***
- ***CAST128***
- ***ARC4***
- ***AES192***
- ***AES256***

Für jeden der im Menü aufgelisteten Algorithmen können Sie zwischen *enabled* (Defaultwert für ***AES128, 3DES, BLOWFISH, CAST128, ARC4***) und *disabled* (Defaultwert für ***AES192, AES256***) wählen.

5.5 Untermenü Message Authentication Codes

Im Folgenden wird das Untermenü *MESSAGE AUTHENTICATION CODES* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][SSHD][MACS]: SSHD Message Authentication Codes    MyGateway

 md5                                  enabled
 sha1                                 enabled
 ripemd160                            enabled
 sha1-96                              enabled
 md5-96                               disabled


      SAVE                            CANCEL
```

Im Menü ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***MESSAGE AUTHENTICATION CODES*** können Sie die Algorithmen festlegen, die zur Message-Authentisierung der SSH-Verbindung zur Verfügung stehen.

Mögliche Message Hash-Algorithmen:

- ***MD5***
- ***SHA1***
- ***RIPEMD160***
- ***SHA1-96***
- ***MD5-96***

Für jeden der im Menü aufgelisteten Algorithmen können Sie zwischen *enabled* (Defaultwert für ***MD5, SHA1, RIPEMD160, SHA1-96***) und *disabled* (Defaultwert für ***MD5-96***) wählen.

5.6 Untermenü Certification Management

Im Folgenden wird das Untermenü *CERTIFICATION MANAGEMENT* beschrieben.

```
VPN Access 25 Setup Tool                  Bintec Access Networks GmbH
[SECURITY][SSHD][KEYS]: SSHD Certification Management        MyGateway

   CAUTION: Key generation may take some minutes
            depending on your routers CPU speed


            Generate DSA Key

            Generate RSA Key




                  EXIT
```

Im Menü ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***CERTIFICATION MANAGEMENT*** können Sie die zur Authentisierung notwendigen Schlüssel erstellen (vgl. “Public Key” auf Seite 45). Sie können einen ➤➤ **DSA**- und einen ➤➤ **RSA**-Schlüssel wählen, wir empfehlen, beide Schlüssel zu erstellen. Die Schlüssel werden systemintern abgespeichert.

Das Erstellen der Schlüssel nimmt mehrere Minuten in Anspruch und kann nicht abgebrochen werden.

5.7 Untermenü Monitoring

Im Menü ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***MONITORING*** können Sie die aufgebauten SSH-Client Verbindungen einsehen. Wenn Sie eine Verbindung durch Drücken der Bestätigungstaste auswählen, werden folgende Details sichtbar:

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][SSHD][SESSIONS][][DETAILS]: SSH Daemon              MyGateway
                                        Session Details

          Account                       admin
          Connection State              active
          Remote IP-Address             192.168.1.1:3446

          Negotiated Cipher             aes128-cbc
          Negotiated MAC                hmac-sha1
          Negotiated Compression        none

          Established Time              00:06:02
          Total Bytes IN                26616
          Total Bytes OUT               31180


                         EXIT
```

6 Untermenü Local Services Access Control

Im Folgenden wird das Untermenü *LOCAL SERVICES ACCESS CONTROL* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][LOCALSRV]: Local Services Access Control          MyGateway

  Services for which no entry exists are NOT access restricted

  Service       Source-Addr     Source-Mask     Interface

  telnet(tcp)   192.168.1.1     255.255.255.0   don't verify
  http(tcp)     192.168.1.2     255.255.255.0   don't verify



   ADD                 DELETE              EXIT
```

Der Zugang zu den lokalen ➤➤ **UDP**- bzw. ➤➤ **TCP**-Diensten auf dem **VPN Access** Gateway (Telnet, ➤➤ **CAPI**, trace, usw.) kann über ein eigenes Setup-Tool-Menü, ***SECURITY*** ➜ ***LOCAL SERVICES ACCESS CONTROL***, geregelt werden.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][LOCALSRV][ADD]                                    MyGateway

  Service                                   snmp(udp)

  Verify IP Address                         don't verify


  Verify Interface                          don't verify


           SAVE                                   CANCEL
```

Für jeden Dienst können in ***SECURITY*** ➜ ***LOCAL SERVICES ACCESS CONTROL*** ➜ ***ADD/EDIT*** eine oder mehrere Einschränkungen definiert werden. Ist für einen

Dienst kein Eintrag vorhanden, so gelten keine Zugriffsbeschränkungen für diesen Dienst, d. h. es kann über alle Schnittstellen und von jeder Quelladresse auf diesen Dienst zugegriffen werden, sofern dies nicht durch Einsatz von NAT oder globalen Filtern verboten wurde.

Das Menü ***LOCAL SERVICES ACCESS CONTROL*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Service	Definiert den lokalen Dienst auf dem **VPN Access** Gateway, zu dem der Zugang u. a. mit diesem Eintrag geregelt werden soll. Mögliche Werte: ■ *snmp(udp)* (Defaultwert) ■ *rip (udp)* ■ *bootps(udp)* ■ *dns(udp)* ■ *telnet(tcp)* ■ *trace(tcp)* ■ *snmp(tcp)* ■ *capi(tcp)* ■ *tapi(tcp)* ■ *rfc1086(tcp)* ■ *http(tcp)* ■ *nbns(udp)* ■ *statmon(udp).*

Feld	Wert
Verify IP Address	Definiert, ob bei einer eingehenden Anfrage auf den unter ***SERVICE*** festgelegten Dienst die Quell-IP-Adresse überprüft werden soll. Mögliche Werte: ■ *verify* ■ *don't verify* (Defaultwert).
IP Address	(nur bei ***VERIFY IP ADDRESS*** = *verify*) Definiert eine Host- bzw. Netzwerk-IP-Adresse, von der eingehende Anfragen auf den unter ***SERVICE*** festgelegten Dienst erlaubt werden. Hat eine Anfrage eine andere Quelladresse, wird zum nächsten Eintrag übergegangen.
Mask	(nur bei ***VERIFY IP ADDRESS*** = *verify*) Definiert eine ➤➤ **Netzmaske**. Zusammen mit ***IP ADDRESS*** wird damit eine Netzwerkadresse definiert, von der eingehende Anfragen auf den unter ***SERVICE*** festgelegten Dienst erlaubt werden. Hat eine Anfrage eine andere Quelladresse, wird zum nächsten Eintrag übergegangen. Ist der Wert von ***MASK*** *0.0.0.0* oder *255.255.255.255*, handelt es sich um einen Host-Eintrag, d. h. die IP-Adresse muss exakt passen.
Verify Interface	Definiert, ob bei einer eingehenden Anfrage auf den unter ***SERVICE*** festgelegten Dienst überprüft werden soll, über welche **VPN Access** Gateway-Schnittstelle die Anfrage eingeht. Mögliche Werte: ■ *verify* ■ *don't verify* (Defaultwert).

Feld	Wert
Interface	(nur bei ***VERIFY INTERFACE*** = *verify*) Definiert eine Schnittstelle des **VPN Access** Gateways. Erreicht das **VPN Access** Gateway eine eingehende Anfrage auf den unter ***SERVICE*** festgelegten Dienst über diese Schnittstelle, wird die Verbindung erlaubt. Überquert die eingehende Anfrage eine andere Schnittstelle, wird zum nächsten Eintrag übergegangen.

Tabelle 6-1: Felder im Menü ***LOCAL SERVICES ACCESS CONTROL***

Index: Security