SECURITY

Bintec User's Guide - VPN Access Series
Version 1.0

Purpose

This document is part of the user's guide to the installation and configuration of Bintec gateways running software release 7.1.4 or later. For up-to-the-minute information and instructions concerning the latest software release, you should always read our **Release Notes**, especially when carrying out a software update to a later release level. The latest **Release Notes** can be found at www.bintec.net.

Liability

While every effort has been made to ensure the accuracy of all information in this manual, Funkwerk Enterprise Communications GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information, changes and **Release Notes** for Bintec gateways can be found at www.bintec.net.

As multiprotocol gateways, Bintec gateways set up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. Funkwerk Enterprise Communications GmbH accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks

Bintec and the Bintec logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

Other product names and trademarks mentioned are usually the property of the respective companies and manufacturers.

Copyright

Guidelines and standards

Bintec gateways comply with the following guidelines and standards:

R&TTE Directive 1999/5/EG

CE marking for all EU countries and Switzerland

You will find detailed information in the Declarations of Conformity at www.bintec.net.

How to reach Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +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 France Telephone: +33 5 57 35 63 00 Fax: +33 5 56 89 14 05 Internet: www.bintec.fr

1 Security Menu

The *SECURITY* menu is described below.

```
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
```

The ***SECURITY*** menu is for configuring your gateway's security features.

The ***SECURITY*** menu provides access to the following submenus:

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

1 Security Menu

2 Cobion Orange Filter Submenu

The *COBION ORANGE FILTER* submenu is described below.

```
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
```

The ***SECURITY*** ➜ ***COBION ORANGE FILTER*** menu is used for configuring a ➤➤ **URL**-based content filtering service, which accesses the OrangeFilter (previously a product of Cobion AG) from Internet Security Systems (www.iss.net) during operation and checks how a requested Internet page has been classified by the OrangeFilter. The action resulting from the classification is configured on the gateway.

The ***SECURITY*** ➜ ***COBION ORANGE FILTER*** menu permits the configuration of basic parameters and access to other configuration menus:

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

The ***COBION ORANGE FILTER*** menu consists of the following fields:

Field	Description
Admin Status	Here you can activate the filter. Possible settings: ■ *disable* (default value): Content filtering is deactivated. ■ *enable*: Content filtering is activated. ■ *enable 30 day demo ticket*: Activates a 30-day demo license for the OrangeFilter.
Orange Filter Ticket	Here you enter the number of the OrangeFilter license purchased. The preset code assigned by ISS designates the device type. This entry is only necessary for ***ADMIN STATUS*** = *enable*.
Expiring Date	This field is only shown if a license has been entered and checked. It shows the expiry date of the license (relative to the time set on the gateway) and cannot be edited.
Ticket Status	Shows the result of the last validity check of the license. The validity of the license is checked every 23 hours.
Filtered Interfaces	Here you select for which of the existing Ethernet interfaces content filtering is to be activated. Only one interface can be specified. Internet pages called up via this interface are then monitored by content filtering. Possible values: *en0-1*, *en0-1-nov*, *en0-2*, *en0-2-nov*, *en0-3*, *en0-3-nov*, *none*. The default value is *none*.

Field	Description
History Entries	Here you define the number of entries to be saved in the content filtering history. Possible values are between *1* and *512* and the default value is *64*.

Table 2-1: ***COBION ORANGE FILTER*** menu fields

2.1 Configure White List Submenu

The *CONFIGURE WHITE LIST* submenu is described below.

```
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
```

The ***SECURITY*** ➜ ***COBION ORANGE FILTER*** ➜ ***CONFIGURE WHITE LIST*** menu contains a list of all URLs and IP addresses that can still be called up even if they are blocked as a result of the filter configuration and the classification in the OrangeFilter (the example contains arbitrary values; the default configuration contains no entries).

You can add other URLs or IP addresses to the list using the ***ADD*** button. The length of an entry is limited to 60 characters. Addresses listed in the White List are allowed automatically. It is not necessary to configure a suitable filter.

2.2 Configure Filters Submenu

The *CONFIGURE FILTERS* submenu is described below.

```
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
```

The ***SECURITY*** ➜ ***COBION ORANGE FILTER*** ➜ ***CONFIGURE FILTERS*** menu is for configuring which categories of Internet pages are to be handled and how. You configure the relevant filters for this purpose. A list of the filters already configured is shown (the example contains arbitrary values; the default configuration contains no filters). There are basically different approaches for configuring the filters:

- First a filter list can be created that only contains entries for those addresses that are to be blocked. In this case it is necessary to make an entry at the end of the filter list that allows all accesses that do not match a filter. (Setting for this: ***CATEGORY*** = *Default behaviour*, ***ACTION*** = *logging* or *allow*)
- If you only create entries for those addresses that are to be allowed or logged, it is not necessary to change the default behavior (= all other calls are blocked).

The filters are added or edited in the ***SECURITY*** ➜ ***COBION ORANGE FILTER*** ➜ ***CONFIGURE FILTERS*** ➜ ***ADD/EDIT*** menu.

```
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
```

The menu consists of the following fields:

Field	Description
Category	Here you select which category of addresses/URLs the filter is to be used on. The options are first the standard categories of the Cobion OrangeFilter (default value: *Anonymous Proxies*). Actions can also be defined for the following special cases: ■ *Default behaviour*: This category applies to all Internet addresses. ■ *No valid license ticket*: If the Cobion OrangeFilter license is invalid, this category applies to all Internet addresses.

Field	Description
Category (cont.)	■ *Orange Server not reachable*: If the Cobion OrangeFilter servers are not reachable, the action associated with this category is used. ■ *Other Category*: Some addresses are already known to the Cobion OrangeFilter, but not yet classified. The action associated with this category is used for such addresses. ■ *Unknown URL*: If an address is not known to the Cobion OrangeFilter, the action associated with this category is used.
Day	Here you select the days on which the filter is to be active. Possible settings: ■ *Everyday*: The filter is used every day of the week. ■ <*Workday*>: The filter is used on a certain day of the week. Only one day can be selected per filter; several filters must be configured if several individual days are to be covered. ■ *Monday-Friday*: The filter is used from Monday to Friday. The default setting is *Everyday*.
From	Here you enter the time at which the filter is to be activated. The time is entered in the form *hh:mm*. The default setting is *0:0*.

Field	Description
To	Here you enter the time at which the filter is to be deactivated. The time is entered in the form *hh:mm*. The default setting is *23:59*.
Action	Here you select the action to be executed if the filter matches a call. Possible settings: ■ *block*: The call of the requested page is prevented. ■ *logging*: The call is permitted, but logged. The logged events can be viewed in the ***SECURITY*** ➜ ***COBION ORANGE FILTER*** ➜ ***VIEW HISTORY*** menu. ■ *allow*: The call is permitted, but not logged. The default setting is *block*.
Priority	Here you assign the filter a priority. The filters are used in accordance with this priority. Possible values are between *0* and *999* and a value of *1* is the highest priority. The value *0* indicates an entry without priority, which is placed at the end of the filter list. The default value is *0*.

Table 2-2: ***CONFIGURE FILTERS*** ➜ ***ADD/EDIT*** menu fields

2.3 View History Submenu

The *VIEW HISTORY* submenu is described below.

```
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
```

You can view the recorded history of the content filter in the ***SECURITY*** ➜ ***COBION ORANGE FILTER*** ➜ ***VIEW HISTORY*** menu: The history logs all calls that are marked for logging by a relevant filter (***ACTION*** = *logging*), likewise all rejected calls.

3 Access Lists Submenu

The *ACCESS LISTS* submenu is described below.

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

        Filter
        Rules
        Interfaces

        EXIT
```

The ***SECURITY*** ➜ ***ACCESS LISTS*** menu is for defining ➤➤ **filters** for IP packets to allow or deny access to or from the various hosts in the connected networks. This enables you to prevent undesired connections being set up via the gateway.

Access lists define the type of IP traffic the gateway is to accept or deny. The access decision is based on information contained in the IP packets, e.g.:

- source and/or destination IP address
- packet protocol
- source and/or destination port (port ranges are supported)

Access lists are an effective means if, for example, sites with LANs interconnected over a Bintec gateway wish to deny all incoming FTP requests or only allow Telnet sessions between certain hosts.

IP filters (➤➤ **access list**s) in the gateway are based on the combination of filters and actions for filter rules (= rules) and the linking of these rules to form rule chains. They act on the incoming data packets to allow or deny access to the gateway for certain data.

Filter A filter describes a certain part of the IP data traffic based on the source and/or destination IP address, ➤➤ **netmask**, protocol, source and/or destination port.

Rule You use a rule to tell the gateway what to do with the filtered data packets, i.e. whether it should allow or deny them. You can also define several rules, which you arrange in the form of a chain to obtain a certain sequence.

Chain There are various approaches for the definition of rules and rule chains:

- Allow all packets that are not explicitly denied, i.e.:
  - Deny all packets that match Filter 1.
  - Deny all packets that match Filter 2.
  - ...
  - Allow the rest.
- Allow all packets that are explicitly allowed, i.e.:
  - Allow all packets that match Filter 1.
  - Allow all packets that match Filter 2.
  - ...
  - Deny the rest.
- Combination of the two possibilities described above.

A number of separate rule chains can be created. The same filter can also be used in different rule chains.

Interface You can also assign a rule chain individually to each interface.

Attention!

Make sure you don't lock yourself out when configuring filters.

If possible, access your gateway for filter configuration over the serial console interface or ISDN Login.

If you still access your gateway over your LAN (e.g. with telnet over ETH1), before you start filter configuration select the menu *SECURITY* ➧ *ACCESS LISTS* ➧ *INTERFACES* ➧ EDIT (e.g. for *en0-1*): First rule = *none*.

The ***ACCESS LISTS*** menu consists of the following submenus:

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

3.1 Filter Submenu

The *FILTER* submenu is described below.

```
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
```

The ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***FILTER*** menu is used for configuring filters. Each filter describes a certain part of the IP traffic and defines, for example, the IP addresses, the protocol, the source port or the destination port.

This menu lists all the IP access filters configured and shows the index number, description and conditions for every single filter. The abbreviations used in the Conditions column are explained in the field above the list.

The ***ADD/EDIT*** menu is used for configuration of the filters:

```
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
```

It consists of the following fields:

Field	Description
Description	Designation of the filter. Note that only the first 10 or 15 characters are visible in other menus.
Index	Cannot be changed here. The gateway assigns a number to newly defined filters automatically.
Protocol	Defines a protocol. Possible values: *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*. *any* matches any protocol, *tcp* matches only TCP data packets, etc. The default value is *any*.

Field	Description
Type	Only if ***PROTOCOL*** = *icmp*. Possible values: *any, echo reply, destination unreachable, source quench, redirect, echo, time exceeded, param problem, timestamp, timestamp reply, address mask, address mask reply*. The default value is *any*. See RFC 792.
Connection State	If ***PROTOCOL*** = *tcp*, you can define a filter based on the status of the TCP connection. Possible values: ■ *established*: All TCP packets that would not open any new TCP connection on routing over the **VPN Access** gateway match the filter. ■ *any (default value)*: All TCP packets match the filter.
Source Address	Defines the source IP address of the data packets.
Source Mask	Source Netmask. The combination of ***SOURCE ADDRESS*** and ***SOURCE MASK*** defines a range of source IP addresses.
Source Port	Source port number or range of source port numbers. For possible values see table “Selection options of Source Port and Destination Port,” on page 19. The default value is *any*.
Specify Port .. to Port	If ***SOURCE PORT*** or ***DESTINATION PORT*** = *specify* or *specify range*: Port numbers or range of port numbers.

Field	Description
Destination Address	Defines the destination IP address of the data packets.
Destination Mask	Netmask for ***DESTINATION ADDRESS***
Destination Port	Destination port number or range of destination port numbers that matches the filter. For possible values see table “Selection options of Source Port and Destination Port,” on page 19. The default value is *any*.
Type of Service <TOS>	Identifies the priority of the IP packet, cf. RFC 1349 and RFC 1812 (shown in binary format).
TOS Mask	Bitmask for Type of Service (shown in binary format).

Table 3-1: ***FILTER*** menu fields

The ***SOURCE PORT*** and ***DESTINATION PORT*** contain the following selection options:

Description	Meaning
any	All ➤➤ **port** numbers match the filter.
specify	Permits the entry of a port number under ***SPECIFY PORT***.
specify range	Permits the entry of a range of port numbers under ***SPECIFY PORT ... TO PORT ...***.
priv (0..1023)	Port numbers: *0* ... *1023*, so-called well-known ports
server (5000..32767)	Port numbers: *5000* ... *32767*.
clients 1 (1024..4999)	Port numbers: *1024* ... *4999*.
clients 2 (32768..65535)	Port numbers: *32768* ... *65535*.

Description	Meaning
unpriv (1024..65535)	Port numbers: *1024 ... 65535*.

Table 3-2: Selection options of ***SOURCE PORT*** and ***DESTINATION PORT***

3.2 Rules Submenu

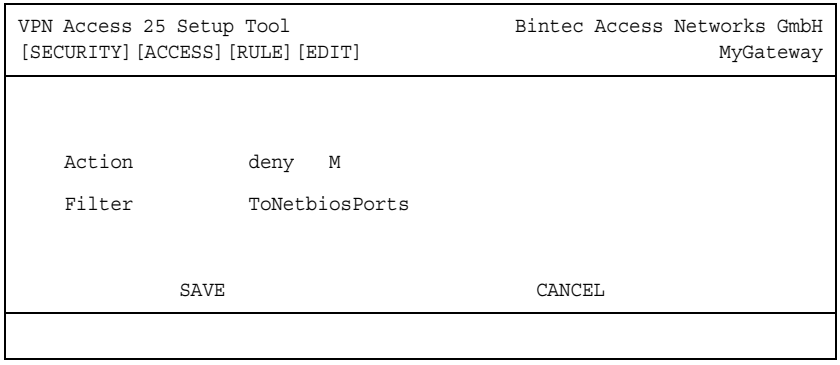
The *RULES* submenu is described below.

```
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
```

Rules for IP filters are configured in the ***IP*** ➜ ***ACCESS LISTS*** ➜ ***RULES*** menu. These can be created separately or incorporated in rule chains.

All the filter rules configured are listed in ***IP*** ➜ ***ACCESS LISTS*** ➜ ***RULES***. ***RF***, ***FI***, ***NRI***, ***ACTION***, ***FILTER*** (only the first ten characters are shown) and ***CONDITIONS*** are listed. The meaning of the abbreviations is shown in the top part of the Setup Tool window.

New rules are added or existing rules edited in the ***RULES*** ➜ ***ADD/EDIT*** menu.



The ***RULES*** ➜ ***ADD/EDIT*** menu consists of the following fields:

Field	Description
Index	Appears only for ***EDIT***. Cannot be changed. Shows the ***INDEX*** of existing rules. The gateway assigns a number to newly defined rules automatically.
Insert behind Rule	Appears only for ***ADD*** and if at least one rule exists. Defines the existing rule behind which the new rule is inserted. You can start a new independent chain with *none*.
Action	Defines the action to be taken for a filtered data packet. ■ *allow M* (default value): Allow packet if it matches the filter. ■ *allow !M*: Allow packet if it does not match the filter. ■ *deny M*: Deny packet if it matches the filter. ■ *deny !M*: Deny packet if it does not match the filter. ■ *ignore*: Use next rule.
Filter	Defines which filter is used.

Field	Description
Next Rule	Appears only if an existing rule is edited. Defines the next rule to be used.

Table 3-3: ***RULES*** menu fields

You can reorganize the indexing of the rules in the ***ACCESS LIST*** ➜ ***RULES*** ➜ ***REORG*** menu; the sequence of the configured rules is retained. The rule that is to receive rule ***INDEX 1*** is defined in the ***INDEX OF RULE THAT GETS INDEX 1*** field.

```
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
```

The rule chain that starts with rule ***INDEX 1*** is always applied as standard to the interface of the gateway (e.g. WAN partner).

3.3 Interfaces Submenu

The *INTERFACES* submenu is described below.

```
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
```

The ***IP*** ➜ ***ACCESS LISTS*** ➜ ***INTERFACES*** menu lists all the gateway's interfaces and shows the assignment of rule chains to the interfaces.

The assignment is configured in the ***IP*** ➜ ***ACCESS LISTS*** ➜ ***INTERFACES*** ➜ ***EDIT*** menu.

```
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
```

Here the configured rule chains are assigned to the individual interfaces and the gateway's behavior is defined for denying IP packets.

The ***EDIT*** submenu contains the following fields:

Field	Description
Interface	Name of interface that has been selected. This field cannot be edited.
First Rule	Defines the start of the rule chain to be applied to data packets received over ***INTERFACE***. If you enter *none* (default value), you specify that no filters are used for ***INTERFACE***.
Deny Silent	Defines whether the sender is to be informed if an IP packet is denied. Possible values: ■ *no*: The sender receives an ICMP message. ■ *yes* (default value): The sender is not informed.
Reporting Method	Defines whether a syslog message is to be generated if a packet is denied. Possible values: ■ *none*: No syslog message. ■ *info* (default value): A syslog message is generated with the protocol number, source IP address and source port number. ■ *dump*: A syslog message is generated with the contents of the first 64 bytes of the denied packet.

Table 3-4: ***INTERFACES*** submenu fields

3 Access Lists Submenu

4 Stateful Inspection Submenu

The *STATEFUL INSPECTION* submenu is described below.

The Stateful Inspection Firewall (SIF) provided for **VPN Access** gateways is a powerful security feature.

The SIF with dynamic packet filtering has a decisive advantage over static packet filtering (see "Access Lists Submenu" on page 13): The decision whether or not to send a packet cannot be made solely on the basis of source and destination addresses or ➤➤ **port**s, but also using dynamic packet filtering based on the state of the connection to a partner.

This means packets that belong to an already active connection can also be forwarded. The SIF also accepts packets that belong to an "affiliated connection". Example: The negotiation of an ➤➤ **FTP** connection takes place over port 21, but the actual data exchange can take place over a completely different port.

SIF and other security features

Bintec's Stateful Inspection Firewall fits into the existing security architecture of Bintec gateways very well due to its simple configuration. The configuration effort for the SIF is very easy compared with systems like Network Address Translation (➤➤ **NAT**) and ➤➤ IP **Access Lists** (IPAL).

As SIF, NAT and IPAL are active in the system simultaneously, attention must be given to possible interaction: If any packet is discarded by one of the security instances, this takes place immediately. This means it is irrelevant if this packet would be allowed by another instance. Your requirement for security features should therefore be accurately analyzed.

The essential difference between SIF and NAT/IPAL is that the rules for the SIF are generally applied globally, i.e. not restricted to one interface.

In principle, the same filter criteria are applied to the data traffic as are used in NAT and IPAL:

- Source and destination address of the packet (with an associated netmask)
- Service (preconfigured, e.g. Echo, FTP, HTTP)
- Protocol
- Port number(s)

To illustrate the differences in packet filtering, a list of the individual security instances and their method of operation is given below:

NAT One of the basic functions of NAT is the translation of the local IP addresses of your LAN into the global IP addresses you are assigned by your ➤➤ **ISP** and vice versa. All connections initiated externally are first blocked, i.e. every packet the gateway cannot assign to an existing connection is discarded. This means that a connection can only be set up from inside to outside. Without explicit permissions, NAT rejects every access from the ➤➤ **WAN** to the LAN.

IP Access Lists Here packets are allowed or discarded exclusively on the basis of the criteria listed above, i.e. the state of the connection is not considered (except for ***PROTOCOL*** = *tcp*).

SIF The SIF sorts out all packets that are not explicitly or implicitly allowed. The result can be a "deny", in which case no error message is sent to the sender of the discarded packet, or a "reject", where the sender is informed of the rejection of the packet.

Incoming packets are processed as follows:

- The SIF first checks if an incoming packet can be assigned to an existing connection. If so, it is forwarded. If the packet cannot be assigned to an existing connection, a check is made to see if a suitable connection is expected (e.g. as affiliated connection of an existing connection). If so, the packet is also accepted.
- If the packet cannot be assigned to any existing or expected connection, the SIF filter rules are applied: If a deny rule matches the packet, the packet is discarded without sending an error message to the sender of the packet; if a reject rule matches, the packet is discarded and an ➤➤ **ICMP** Host Unreachable message sent to the sender of the packet. The packet is only forwarded if an accept rule matches.
- All packets without matching rules are discarded without sending an error message to the sender once all the existing rules have been checked (=default behavior).

The menus in which you configure the SIF are described below.

The ***SECURITY*** ➜ ***STATEFUL INSPECTION*** menu shows global parameters and leads to submenus:

```
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
```

The ***STATEFUL INSPECTION*** menu consists of the following fields:

Field	Description
Adminstatus	Here you can basically activate and deactivate the feature. Possible settings: ■ *enable*: Default value ■ *disable*
Local Filter	Here you define whether locally initiated connections are also to be filtered by the SIF. Possible settings: ■ *enable*: Locally generated requests are also filtered. ■ *disable*: Locally generated requests are generally allowed (default value).

Field	Description
Full Filtering	Here you define whether packets are only to be filtered if they are sent to an interface other than the interface that created the connection. Possible settings: ■ *enable*: All packets are filtered (default value). ■ *disable*: Packets are only filtered if their destination interface differs from the output interface of the connection.
Logging level	Here you can select the SIF syslog level. The messages are output together with the messages of the other subsystems, see manual **Monitoring and Debugging,** Messages chapter). Possible settings: ■ *all*: All SIF activities are shown (default value). ■ *deny only*: Only reject and deny events are shown, cf. "Action" on page 31. ■ *accept only*: Only accept events are shown. ■ *none*: Syslog messages are not generated.

Table 4-1: ***STATEFUL INSPECTION*** menu fields

Access for configuration of the filters (***EDIT FILTERS***), services (***EDIT SERVICES***) and filter addresses (***EDIT ADDRESSES***) is via the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** menu. This menu also provides access to the ***ADVANCED SETTINGS*** menu.

4.1 Edit Filters Submenu

The *EDIT FILTERS* submenu is described below.

```
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
```

The configured SIF filter rules are listed in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** menu.

The default behavior with ***ACTION*** *allow* consists of two implicit filter rules: If an incoming packet can be assigned to an existing connection and if a suitable connection is expected (e.g. as affiliated connection of an existing connection), the packet is allowed.

The sequence of filter rules in the list is relevant: The filter rules are applied to each packet in succession until a rule matches. If overlapping occurs, i.e. more than one filter rule matches a packet, only the first rule is executed. This means that if the first rule denies a packet, whereas a later rule allows it, the packet is discarded. A deny rule also has no effect if a relevant packet has previously been allowed by another filter rule.

You can add a filter rule for the SIF or edit an existing rule in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD/EDIT*** menu.

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

  Source                      ANY
  Destination                 ANY
  Edit Addresses >

  Service                     KaZaA
  Edit Services >

  Action                      accept




          SAVE                                    CANCEL
```

The ***EDIT FILTERS*** ➜ ***ADD/EDIT*** menu consists of the following fields:

Field	Description
Source	Here you can select one of the preconfigured aliases for the source of the packet. The gateway reads the list of existing WAN and LAN interfaces and offers these as default setting. The default value is *ANY*. You can create a new alias in ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD/EDIT*** ➜ ***EDIT ADDRESSES*** ➜ ***ADD/EDIT*** see “Edit Addresses Submenu” on page 33
Destination	Here you can select one of the preconfigured aliases for the destination of the packet. The gateway reads the list of existing WAN and LAN interfaces and offers these as default setting. The default value is *ANY*. You can create a new alias in ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD/EDIT*** ➜ ***EDIT ADDRESSES*** ➜ ***ADD/EDIT*** see “Edit Addresses Submenu” on page 33

Field	Description
Service	Here you can select one of the preconfigured services, to which the packet to be filtered must be assigned. The extensive range of services configured ex works includes the following: ■ *ftp* ■ *telnet* ■ *smtp* ■ *dns* ■ *http* ■ *nntp* ■ *internet* ■ *netmeeting* You can configure other services in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD/EDIT*** ➜ ***EDIT SERVICES*** menu see “Edit Services Submenu” on page 32
Action	Here you select the action to be applied to a filtered packet. Possible values are: ■ *accept* (default value) ■ *deny* ■ *reject* The packet is denied for both *reject* and *deny*, but in the case of *deny* without sending an error message to the sender of the packet.

Table 4-2: ***EDIT FILTERS*** menu fields

4.2 Edit Services Submenu

The *EDIT SERVICES* submenu is described below.

The ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES*** menu shows a list of over 60 preconfigured service aliases.

Select ***ADD*** or an existing entry to access the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES*** ➜ ***ADD/EDIT*** menu, in which you can define another service alias or edit an existing alias. You can also access this menu via ***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
```

The ***EDIT SERVICES*** ➜ ***ADD/EDIT*** menu consists of the following fields:

Field	Description
Alias	Here you enter an alias for the service you want to configure.
Protocol	Here you select the protocol on which the service is based. The most important protocols are available for selection. (The default value for ***ADD*** is *ah*.)
ICMP Type	Only if you have set ***PROTOCOL*** to *icmp*. This field is set to *echo* per default. This setting covers the so-called pings. The value cannot be changed.

Field	Description
Port	Only if you have set ***PROTOCOL*** to *tcp*, *udp/tcp* or *udp*. Here you enter the port over which the service runs. Possible values are *1* to *65535*. The default value is *1*.
Range	Only if you have set ***PROTOCOL*** to *tcp*, *udp/tcp* or *udp*. Here you enter how many consecutive ports the service uses, incl. the value set in ***PORT***. Possible values are *1* to *65535*. If you do not enter a value, the gateway assumes the value *1* as default.

Table 4-3: ***EDIT SERVICES*** menu fields

4.3 Edit Addresses Submenu

The *EDIT ADDRESSES* submenu is described below.

All the configured aliases are listed in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESSES*** menu. The list contains the interfaces configured for the gateway. Select ***ADD*** or an existing entry to access the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESSES*** ➜ ***ADD/EDIT*** menu, in which you can create other address aliases or edit existing aliases. You can also access this menu via ***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
```

The ***EDIT ADDRESSES*** ➜ ***ADD/EDIT*** menu consists of the following fields:

Field	Description
Alias	Here you enter the alias name you want to configure.
Mode	Here you indicate whether you want to designate an IP address (*Address/Range* or *Address/Subnet*) or an interface (*interface*) with the alias. Possible values: ■ *interface* (default value) ■ *Address/Range* ■ *Address/Subnet*.
IP Address	Only if you have set ***MODE*** to *Address/Range* or *Address/Subnet*. Here you enter the IP address to which the alias is to apply.
IP Range	Only for ***MODE*** = *Address/Range* Here you enter the number of consecutive IP addresses incl. the address entered in ***IP ADDRESS***.

Field	Description
IP Mask	Only if you have set ***MODE*** to *Address/Subnet*. Here you enter the netmask belonging to the IP address of the host. The default value is *255.255.255.255*.
Interface	Only if you have set ***MODE*** to *interface*. Here you select the interface via which packets are to be received and sent. You can select from all configured WAN partners and LAN interfaces.

Table 4-4: ***EDIT ADDRESSES*** menu fields

4.4 Advanced Settings Submenu

The *ADVANCED SETTINGS* submenu is described below.

```
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
```

Settings for the session timeout are made in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***ADVANCED SETTINGS*** menu.

The ***ADVANCED SETTINGS*** menu consists of the following fields:

Field	Description
UDP inactivity Timeout	Here you can enter the inactivity time, after which a ➤➤ **UDP** session is regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *180*.
TCP inactivity Timeout	Here you can enter the inactivity time, after which a ➤➤ **TCP** session is regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *3600*.
PPTP inactivity Timeout	Here you can enter the inactivity time, after which a PPTP session is regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *86400*.
Other inactivity Timeout	Here you can enter the inactivity time, after which a session of another type is regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *30*.

Table 4-5: ***ADVANCED SETTINGS*** menu fields

5 SSH Daemon Submenu

The *SSH DAEMON* submenu is described below.

```
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
```

Your gateway offers encrypted access to the shell (see manual chapter **Access and Configuration**). You can activate (*running*, default value) or deactivate (*stopped*) this access in the ***SECURITY*** ➜ ***SSH DAEMON*** menu and have access to the menus for configuration of the SSH Login.

You need an SSH client application, e.g. PuTTY, to be able to reach the SSH Daemon.

If you wish to use SSH Login together with the PuTTY client, you must comply with some special configuration requirements, for which we have prepared FAQs. You will find these in the Service/Support section at www.bintec.net.

To be able to reach the shell of your gateway via an SSH client, make sure the settings for the SSH Daemon and SSH client are the same.

Note

After configuration you should check that the SSH Daemon has started: Enter `ps -e` in the shell and verify that `sshd` is executed.

If not, you must restart the gateway to start the SSH Daemon.

5.1 Static Settings Submenu

The *STATIC SETTINGS* submenu is described below.

```
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
```

The ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***STATIC SETTINGS*** menu is for selecting the basic parameters of the SSH Daemon.

The ***STATIC SETTINGS*** menu consists of the following fields:

Field	Description
Max. # of Clients	Here you enter how many simultaneous connections are allowed to the SSH Daemon. Any connections above this number are rejected until a connection is cleared. This field cannot be edited, as only a single SSH connection is possible.
Port # used for Connections	Here you enter the port at which a client can connect to the SSH Daemon. Possible values are *1* to *65535*. The default value is *22*.

Field	Description
Compression	Here you can activate (*enabled*) or deactivate (*disabled*) the use of data compression. The default value is *disabled*.
Verify Reverse Mapping	Here you select whether the SSH Daemon executes a reverse lookup of the client IP address. This verifies that the host name belonging to the IP address is correct, i.e. the IP address is not a fake. The connection is cleared if the IP address is a fake. Possible settings: ■ *disabled* (default value) ■ *enabled*.
Print Motd	Here you select whether the SSH Daemon sends a Message of the Day (MotD) as soon as a client has logged in. Possible settings: ■ *disabled* ■ *enabled* (default value).
Print LastLog	Here you select whether the SSH Daemon prints the date and time of the last login when a client logs in. Possible settings: ■ *disabled* (default value) ■ *enabled*.

Field	Description
Logging Level	Here you can select the syslog level for the syslog messages generated by the SSH Daemon. Possible settings: ■ *quiet*: No messages are recorded. ■ *fatal*: Only fatal errors of the SSH Daemon are recorded. ■ *error:* Fatal and simple errors of the SSH Daemon are recorded. ■ *info* (default value)*:* Fatal and simple errors of the SSH Daemon and information messages are recorded. ■ *debug*: All messages are recorded.

Table 5-1: ***STATIC SETTINGS*** menu fields

5.2 Timer Submenu

The *TIMER* submenu is described below.

```
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
```

You can configure the timing behavior of the SSH Daemon in the ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***TIMER*** menu.

The ***TIMER*** menu consists of the following fields:

Field	Description
Login Grace Time	Here you enter the time interval within which a client must authenticate before the SSH connection is cleared. Possible values are *0* to *3600* (seconds). A value of *0* means no limit and the default value is *600*.
TCP Keepalives	Here you select whether the gateway is to send keepalive packets. Possible settings: ■ *disabled* ■ *enabled*: Default value. The same value should be configured for both client and server.
ClientAliveCountMax	This field is only to be configured if ***TCP KEEPALIVES*** = *enabled*. Here you enter the number of keepalive packets sent by the gateway that may remain unanswered before the SSH Daemon clears the connection. Possible values are *0* to *10* and the default value is *3*.

Field	Description
ClientAliveInterval	This field is only to be configured if ***TCP KEEPALIVES*** = *enabled*. Here you enter the interval after which the SSH Daemon sends a Keepalive Request to the client if no more data is received from the client. Possible values are *1* to *3600* (seconds) and the default value is *10*.

Table 5-2: ***TIMER*** menu fields

5.3 Authentication Algorithms Submenu

The *AUTHENTICATION ALGORITHMS* submenu is described below.

```
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
```

The ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***AUTHENTICATION ALGORITHMS*** menu is for configuring the authentication mechanisms for SSH connection setup.

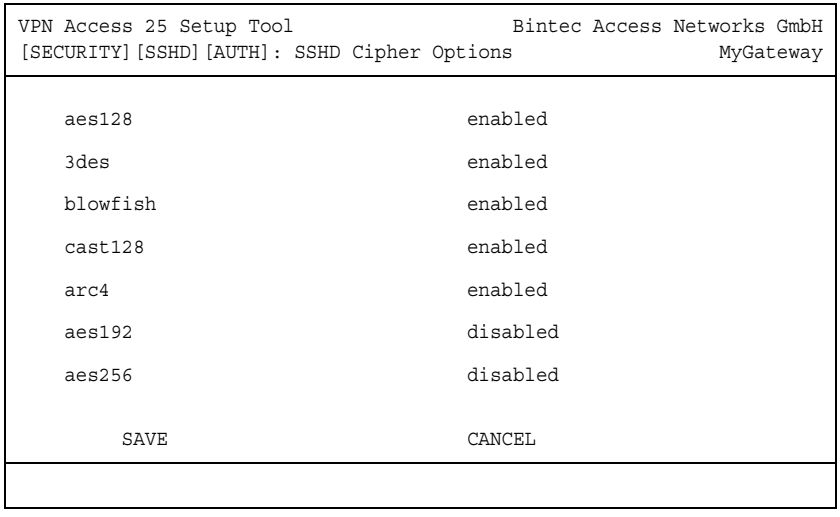
The ***AUTHENTICATION ALGORITHMS*** menu consists of the following fields:

Field	Description
Protocol Version	This shows which SSH version the SSH Daemon uses. This field cannot be edited, as only version 2 is currently supported.
Public Key	Here you select whether or not public key authentication of the client is allowed. Possible settings: ■ *disabled* ■ *enabled*: Default value. This feature is not available at present.
Password	Here you select whether or not password authentication of the client is allowed. (Logging in via the SSH client is only possible as *admin* user with the associated password.) Possible settings: ■ *disabled* ■ *enabled*: Default value.
Challenge Response	Here you select whether or not challenge response authentication of the client is allowed. Possible settings: ■ *disabled* ■ *enabled*: Default value. This feature is not available at present.

Table 5-3: ***AUTHENTICATION ALGORITHMS*** menu fields

5.4 Supported Ciphers Submenu

The *SUPPORTED CIPHERS* submenu is described below.



The ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***SUPPORTED CIPHERS*** menu is used for defining the algorithms that may be used for encryption of the SSH connection.

Possible algorithms:

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

For each of the algorithms listed in the menu you can select from *enabled* (default value for ***AES128, 3DES, BLOWFISH, CAST128, ARC4***) and *disabled* (default value for ***AES192, AES256***).

5.5 Message Authentication Codes Submenu

The *MESSAGE AUTHENTICATION CODES* submenu is described below.

```
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
```

In the ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***MESSAGE AUTHENTICATION CODES*** menu you can define the algorithms that are available for message authentication of the SSH connection.

Possible message hash algorithms:

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

For each of the algorithms listed in the menu you can select from *enabled* (default value for ***MD5, SHA1, RIPEMD160, SHA1-96***) and *disabled* (default value for ***MD5-96***).

5.6 Certification Management Submenu

The *CERTIFICATION MANAGEMENT* submenu is described below.

```
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 router's CPU speed


            Generate DSA Key

            Generate RSA Key




                  EXIT
```

In the ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***CERTIFICATION MANAGEMENT*** menu you can create the keys necessary for authentication (cf. "Public Key" on page 43). You can select a ➤➤ **DSA** key and an ➤➤ **RSA** key. We recommend you create both keys. The keys are saved internally in the system.

Creating the keys takes several minutes and cannot be aborted.

5.7 Monitoring Submenu

In the ***SECURITY*** ➜ ***SSH DAEMON*** ➜ ***MONITORING*** menu you can view the SSH client connections that are set up. If you select a connection by pressing **Return**, the following details are shown:

```
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
```

5 SSH Daemon Submenu

6 Local Services Access Control Submenu

The *LOCAL SERVICES ACCESS CONTROL* submenu is described below.

```
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
```

Access to the local ➤➤ **UDP** and ➤➤ **TCP** services on the **VPN Access** gateway (Telnet, ➤➤ **CAPI**, trace, etc.) can be controlled via the separate Setup Tool menu ***SECURITY*** ➜ ***LOCAL SERVICES ACCESS CONTROL***.

```
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
```

One or more restrictions can be defined for each service in ***SECURITY*** ➜ ***LOCAL SERVICES ACCESS CONTROL*** ➜ ***ADD/EDIT***. If no entry exists for a service, there are no access restrictions for this service, i.e. access to this service is possible

over all interfaces and from any source address, provided this is not prohibited by the use of NAT or global filters.

The ***LOCAL SERVICES ACCESS CONTROL*** ➜ ***ADD/EDIT*** menu consists of the following fields:

Field	Description
Service	Defines the local service on the **VPN Access** gateway, to which access is to be controlled with this entry. Possible values: ■ *snmp(udp)* (default value) ■ *rip(udp)* ■ *bootps(udp)* ■ *dns(udp)* ■ *telnet(tcp)* ■ *trace(tcp)* ■ *snmp(tcp)* ■ *capi(tcp)* ■ *tapi(tcp)* ■ *rfc1086(tcp)* ■ *http(tcp)* ■ *nbns(udp)* ■ *statmon(udp).*
Verify IP Address	Defines whether the source IP address is to be checked when an incoming request is received for the service selected under ***SERVICE***. Possible values: ■ *verify* ■ *don't verify* (default value).

Field	Description
IP Address	(Only if ***VERIFY IP ADDRESS*** = *verify*) Defines a host or network IP address from which incoming requests are allowed for the service selected under ***SERVICE***. If a request has a different source address, the next entry is checked.
Mask	(Only if ***VERIFY IP ADDRESS*** = *verify*) Defines a ➤➤ **netmask**. A network address is thus defined together with the ***IP ADDRESS***, from which incoming requests are allowed for the service selected under ***SERVICE***. If a request has a different source address, the next entry is checked. If the value of ***MASK*** is *0.0.0.0* or *255.255.255.255*, the entry is a host entry, i.e. the IP address must match exactly.
Verify Interface	Defines whether a check is to be made to determine which **VPN Access** gateway interface is used for an incoming request received for the service selected under ***SERVICE***. Possible values: ■ *verify* ■ *don't verify* (default value).
Interface	(Only if ***VERIFY INTERFACE*** = *verify*) Defines an interface of the **VPN Access** gateway. If the **VPN Access** gateway receives an incoming request over this interface for the service selected under ***SERVICE***, the connection is allowed. If the incoming request crosses another interface, the next entry is checked.

Table 6-1: ***LOCAL SERVICES ACCESS CONTROL*** menu fields

Index: Security