STATEFUL INSPECTION FIREWALL

bintec Workshop
Version 0.9

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

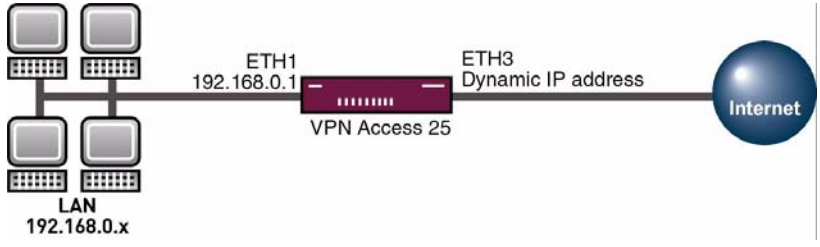
Funkwerk Enterprise Communications GmbH Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +49 180 300 9191 0 Fax: +49 180 300 9193 0 Internet: www.funkwerk-ec.com	Bintec France 6/8 Avenue de la Grande Lande F-33174 Gradignan France Telephone: +33 5 57 35 63 00 Fax: +33 5 56 89 14 05 Internet: www.bintec.fr

1 Introduction

The configuration of the SIF (Stateful Inspection Firewall) is described in the following chapters using a Bintec VPN Access 25 gateway (software version 7.1.6 patch 3).

1.1 Scenario

Only certain Internet services are to be available for the staff of a company (http, https, dns). Only the system administrator is to be able to set up a Telnet connection to the gateway and the director is to be able to use all the Internet services.



Note

Incorrect configuration of the Stateful Inspection Firewall can drastically effect the operation of the device or connections. The usual principle for firewalls also applies here: Everything that is not explicitly allowed is prohibited. This means accurate planning of the filter rules and filter rule chain is necessary.

1.2 Requirements

The following are required for the configuration:

- A bintec **VPN Access 25** gateway.
- A connection to the Internet (see, for example, FAQ **Configuring an xDSL connection**).

- Your LAN is connected over the first Ethernet interface (ETH 1) of your gateway.
- A configured PC (see User's Guide Part **Access and Configuration**).

2 Configuration of Stateful Inspection Firewall

2.1 Configuration of Alias Names for IP Addresses and Network Address

- Go to ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESSES***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][ADDRESSES]: Alias                 vpn25
                                             Addresses

   Alias Address List:

    Alias           IP Address    Mask/Range        Interface
    ANY             0.0.0.0       0.0.0.0           any
    LAN_EN0-1       ------        ------            en0-1
    LAN_EN0-1-SNAP  ------        ------            en0-1-snap
    LAN_EN0-2       ------        ------            en0-2
    LAN_EN0-2-SNAP  ------        ------            en0-2-snap
    LAN_EN0-3       ------        ------            en0-3
    LAN_EN0-3-SNAP  ------        ------            en0-3-snap
    LOCAL           ------        ------            LOCAL


     ADD                 DELETE              EXIT

Press <Ctrl-n>,<Ctrl-p> to scroll,<Space> tag/untag DELETE,<Return> to
edit
```

You can add your own alias names with ***ADD***.

- Go to ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESSES*** ➜ ***ADD***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][ADDRESSES][ADD]                    vpn25

          Alias                       internal network

          Mode                        Address/Subnet

          IP Address                  192.168.0.0
          IP Mask                     255.255.255.0


                    SAVE                                  CANCEL
```

The following fields are relevant:

Field	Meaning
Alias	Freely selectable alias name.
Mode	Mode used.
IP Address	IP address or network address.
IP Mask	Associated network mask.

Table 2-1: Relevant fields in ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESSES*** ➜ ***ADD***

Proceed as follows to define the necessary settings:

- Enter a name under ***ALIAS***, e.g. *internal network*.
- Set ***MODE*** to *Address/Subnet*.
- Enter your network address under ***IP ADDRESS***, e.g. *192.168.0.0*.
- Enter your netmask under ***IP MASK***, e.g. *255.255.255.0*.
- Press **SAVE** to confirm your settings.

You have now defined an alias name for network 192.168.0.0/24. Repeat this process for the configuration of the administrator, director and gateway. The complete alias list for our example looks like this:

- Go to ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESSES***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][ADDRESSES]: Alias                 vpn25
                                            Addresses

  Alias Address List:

 Alias             IP Address     Mask/Range       Interface
 ANY               0.0.0.0        0.0.0.0          any
 LAN_EN0-1         ------         ------           en0-1
 LAN_EN0-1-SNAP    ------         ------           en0-1-snap
 LAN_EN0-2         ------         ------           en0-2
 LAN_EN0-2-SNAP    ------         ------           en0-2-snap
 LAN_EN0-3         ------         ------           en0-3
 LAN_EN0-3-SNAP    ------         ------           en0-3-snap
 LOCAL             ------         ------           LOCAL
 administrator     192.168.0.20   255.255.255.255  any
 director          192.168.0.100  255.255.255.255  any
 internal network  192.168.0.0    255.255.255.0    any
 router address    192.168.0.1    255.255.255.255  any

     ADD                 DELETE              EXIT
```

2.2 Configuration of Alias Names for Services

- Go to ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES***.

Note

Here you find a large number of preconfigured services, which are sufficient for our example. You can also add your own services, e.g. *IKE*.

- Go to ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES*** ➜ ***ADD.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][SERVICES][ADD]                    vpn25

          Alias                  ike (udp:500)

          Protocol               udp

          Port                   500     Range 1



           SAVE                                  CANCEL
```

The following fields are relevant:

Field	Meaning
Alias	Freely selectable alias name.
Protocol	The protocol used by the service.
Port	Port or port range used by the service (this field need not be available if the protocol uses no ports, e.g. ESP).

Table 2-2: Relevant fields in ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES*** ➜ ***ADD***

Proceed as follows to define the necessary settings:

- Enter a name under ***ALIAS***, e.g. *ike (udp:500)*.
- Set ***PROTOCOL*** to *UDP*.
- Enter *500* as ***PORT***.
- Enter *1* as ***RANGE***.
- Press **SAVE** to confirm your entries.

You now have an alias name for packets that use UDP port 500.

2.3 Configuration of Filter Rules

Once you have completed the configuration of the alias names for IP addresses and services, you can define the filter rules.

Attention!

The correct configuration of the filter rules and the right arrangement in the filter rule chain are decisive factors for the operation of the Stateful Inspection Firewall. An incorrect configuration may possibly prevent further communication with the Internet!

- Go to ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS***.

Note

The filter list is empty the first time this menu is opened.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][FILTERS]: Configuration          vpn25

   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
```

You can add filters using the menu item **ADD**.

- Go to ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][ADD]                              vpn25

       Source                       internal network
       Destination                  ANY
       Edit Addresses >

       Service                      http
       Edit Services >

       Action                       accept


           SAVE                                    CANCEL
```

The following fields are relevant:

Field	Meaning
Source	Source IP address or alias name for this.
Destination	Destination IP address or alias name for this.
Service	Service that is to match the filter.
Action	Action to be taken if the service matches the filter

Table 2-3: Relevant fields in ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD***

Proceed as follows to define the necessary settings:

- Enter the alias for your internal network under ***SOURCE***, e.g. *internal network*.
- Set ***DESTINATION*** to *ANY*.
- Set ***SERVICE*** to *http*.
- Set ***ACTION*** to *accept*.
- Press **SAVE** to confirm your entries.

You have now configured a filter that allows HTTP from the internal network to any IP address.

Configure all the other filters required in a similar way to the example above. The complete filter rule chain looks like this:

- Go to ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][FILTERS]: Configuration           vpn25

   Stateful Inspection Filter List:

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

Pos. Source            Destination     Service     Action
  1  internal network  ANY             http        accept
  2  internal network  ANY             http (SSL)  accept
  3  internal network  ANY             dns         accept
  4  administrator     routeraddress   telnet      accept
  5  director          ANY             any         accept


     ADD                DELETE              SAVE                CANCEL
```

If you wish to change the sequence of the filters, you can tag a filter and move it up with "u" or down with "d".

You have now configured a filter rule chain that meets all the requirements of the scenario.

2 Configuration of Stateful Inspection Firewall

3 Activating SIF

- Go to ***SECURITY*** ➜ ***STATEFUL INSPECTION***.

```
VPN Access 25 Setup Tool                  Bintec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION]: Static settings                vpn25

   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 following field is relevant:

Field	Meaning
Adminstatus	Determines whether the Stateful Inspection Firewall is active or inactive.

Table 3-1: Relevant field in ***SECURITY*** ➜ ***STATEFUL INSPECTION***

Proceed as follows to define the necessary settings:

- Set ***ADMINSTATUS*** to *enable*.
- Leave all the other settings as they are.
- Press **SAVE** to confirm your settings.

Return to the main menu and finally save your new configuration in the flash memory with **EXIT** and **Save as boot configuration and exit**.

3 Activating SIF

4 Important Information

- When the Stateful Inspection Firewall is activated for the first time, all the active sessions are first interrupted. If you have configured the device over Telnet, your Telnet session is also ended. If the SIF configuration is correct, you can set up the connection again. Cause of this behavior: The status of sessions that are still active cannot be covered by the SIF.
- The end of the filter rule chain is followed by an invisible deny. This means all connections not previously allowed by a filter are discarded.
- A detailed description of the Stateful Inspection Firewall can also be found in the Release Notes for software version 6.2.5.

4 Important Information

5 Result

5.1 Test

The administrator is allowed access to the gateway over Telnet in the following test, but other users are denied as no appropriate rule exists.

Enter the following in the command line of the respective PC:

```
c:\>telnet 192.168.0.1
```

You can show debug outputs in the command line using the command `debug all&`. This enables you to detect sessions that have been accepted or rejected by the SIF. Enter the following in the command line of the gateway for this purpose:

```
vpn25:> debug all&
```

```
11:14:31 DEBUG/INET: SIF: Accept administrator[100:192.168.0.20:1277]
-> routeraddress[1:192.168.0.1:23] telnet:6
11:15:21 DEBUG/INET: SIF: No Rule ignore  192.168.0.30:1294 ->
192.168.0.1:23 Proto:6
```

5.2 Overview of Configuration Steps

Field	Menu	Description	Compulsory field
Alias	**SECURITY ➜ STATEFUL INSPECTION ➜ EDIT ADDRESSES ➜ ADD**	e.g. *internal network*	Yes
Mode	**SECURITY ➜ STATEFUL INSPECTION ➜ EDIT ADDRESSES ➜ ADD**	e.g. *Address/Subnet*	Yes
IP Address	**SECURITY ➜ STATEFUL INSPECTION ➜ EDIT ADDRESSES ➜ ADD**	e.g. *192.168.0.0*	Yes
IP Mask	**SECURITY ➜ STATEFUL INSPECTION ➜ EDIT ADDRESSES ➜ ADD**	e.g. *255.255.255.0*	Yes
Alias	**SECURITY ➜ STATEFUL INSPECTION ➜ EDIT SERVICES ➜ ADD**	e.g. *ike (udp:500)*	Yes
Protocol	**SECURITY ➜ STATEFUL INSPECTION ➜ EDIT SERVICES ➜ ADD**	e.g. *udp*	Yes
Port	**SECURITY ➜ STATEFUL INSPECTION ➜ EDIT SERVICES ➜ ADD**	*500*	Yes
Range	**SECURITY ➜ STATEFUL INSPECTION ➜ EDIT SERVICES ➜ ADD**	*1*	Yes
Source	**SECURITY ➜ STATEFUL INSPECTION ➜ EDIT FILTERS ➜ ADD**	*internal network*	Yes
Destination	**SECURITY ➜ STATEFUL INSPECTION ➜ EDIT FILTERS ➜ ADD**	e.g. *ANY*	Yes
Service	**SECURITY ➜ STATEFUL INSPECTION ➜ EDIT FILTERS ➜ ADD**	e.g. *http*	Yes
Action	**SECURITY ➜ STATEFUL INSPECTION ➜ EDIT FILTERS ➜ ADD**	*accept*	Yes
Adminstatus	**SECURITY ➜ STATEFUL INSPECTION**	*enable*	Yes