funkwerk
enterprise communications

bintec Workshop

Configuration of Access Lists and Filters

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.funkwerk-ec.com.

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.funkwerk-ec.com.

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.funkwerk-ec.com.

How to reach Funkwerk Enterprise Communications GmbH

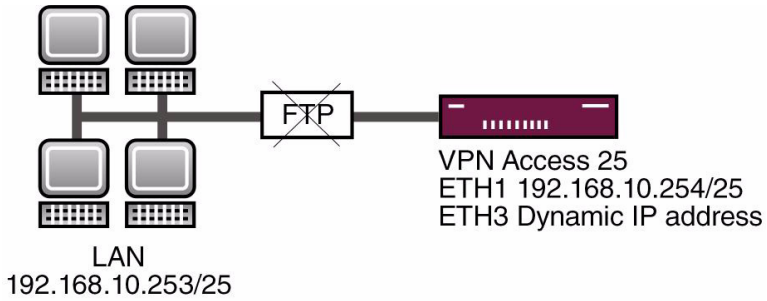
Funkwerk Enterprise Communications GmbH Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +49 180 300 9191 0 Fax: +49 180 300 9193 0 Internet: www.funkwerk-ec.com	Bintec France 6/8 Avenue de la Grande Lande F-33174 Gradignan France Telephone: +33 5 57 35 63 00 Fax: +33 5 56 89 14 05 Internet: www.bintec.fr

1 Introduction

The configuration of access lists and filters is described in the following chapters using a Bintec VPN Access 25 gateway. The Setup Tool is used for the configuration.

1.1 Scenario

You wish to prevent a certain address range using the FTP protocol. The address range is 192.168.10.192/25.



1.2 Requirements

The following are required for the configuration:

- A Bintec **VPN Access 25** gateway.
- A connection to the Internet (see Bintec 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 Access List

2.1 Deactivating all Filters

- Go to ***SECURITY ➜ ACCESS LISTS ➜ INTERFACES ➜ EN0-1.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ACCESS][INTERFACES][EDIT]                              vpn25

      Interface                 en0-1
      First Rule                none

      Deny Silent               yes
      Reporting Method          info


         SAVE                                   CANCEL
```

The following field is relevant:

Field	Meaning
First Rule	The rule to be applied.

Table 2-1: Relevant field in ***SECURITY ➜ ACCESS LISTS ➜ INTERFACES ➜ EN0-1***

Proceed as follows to define the necessary settings:

- Set ***FIRST RULE*** to *none.*
- Leave all the other settings as they are.
- Press **SAVE** to confirm your settings.

Note

Repeat this step for all interfaces. Setting ***FIRST RULE*** to *none* deactivates the rule. As all the interfaces are now set to *no access rule*, you can start creating new filters without the risk of locking yourself out by denying access.

3 Configuration of Filters

3.1 Configuring the First Filter

- Go to ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***FILTER*** ➜ ***ADD.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ACCESS][FILTER][EDIT]                                  vpn25

  Description               Deny FTP
  Index                     1

  Protocol  tcp             Connection State    any

  Source Address            192.168.10.192
  Source Mask               255.255.255.128
  Source Port               any


  Destination Address
  Destination Mask
  Destination Port          specify range
  Specify Port              20        to Port   21
  Type of Service (TOS)     00000000                TOS Mask  00000000

         SAVE                                CANCEL
```

The following fields are relevant:

Field	Meaning
Description	Description of the filter.
Protocol	Type of filtered protocol.
Connection State	State of interface to which the filter is to be applied.
Source Address	Source address, e.g. a network.
Source Mask	Associated netmask.
Source Port	The source port to be filtered.
Destination Address	Destination address, e.g. a network.

Field	Meaning
Destination Mask	Associated netmask.
Destination Port	The destination port to be filtered.
Specify Port	Port number.

Table 3-1: Relevant fields in ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***FILTER*** ➜ ***ADD***

Proceed as follows to define the necessary settings:

- Enter a name under ***DESCRIPTION***, e.g. *Deny FTP.*
- Set ***PROTOCOL*** to *tcp*.
- Set ***CONNECTION*** to *State any*.
- Enter your IP address as ***SOURCE ADDRESS***, e.g. *192.168.10.192*.
- Enter your network address as ***SOURCE MASK***, e.g. *255.255.255.128*.
- Set ***SOURCE PORT*** to *any*.
- Set ***DESTINATION PORT*** to *specify range*.
- Set ***SPECIFY PORT*** to *20*.
- Enter *21* under ***TO PORT***.
- Press **SAVE** to confirm your settings.

3.2 Configuring a Second Filter

Go to ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***FILTER*** ➜ ***ADD.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ACCESS][FILTER][EDIT]                                  vpn25

  Description               allow all
  Index                     2

  Protocol            any

  Source Address
  Source Mask
  Source Port               any


  Destination Address
  Destination Mask
  Destination Port          any

  Type of Service (TOS)     00000000              TOS Mask  00000000

                    SAVE                                CANCEL
```

The following fields are relevant:

Field	Meaning
Description	Description of the filter.
Protocol	Type of filtered protocol.
Connection State	State of interface to which the filter is to be applied.
Source Address	Source address, e.g. a network.
Source Mask	Associated netmask.
Source Port	The source port to be filtered.
Destination Address	Destination address, e.g. a network.
Destination Mask	Associated netmask.
Destination Port	The destination port to be filtered.

Table 3-2: Relevant fields in ***SECURITY → ACCESS LISTS → FILTER → ADD***

Proceed as follows to define the necessary settings:

- Enter a name under ***DESCRIPTION***, e.g. *allow all*
- Leave all the other settings as they are.
- Press **SAVE** to confirm your settings.

4 Defining Rules

4.1 Defining the First Rule

- Go to ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***RULES*** ➜ ***ADD.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ACCESS][RULE][ADD]                                    vpn25

     Action                    deny  M

     Filter                    Deny FTP (1)


                     SAVE                                  CANCEL

Use <Space> to select
```

The following fields are relevant:

Field	Meaning
Action	Action to be executed.
Filter	Filter to be used.

Table 4-1: Relevant fields in ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***RULES*** ➜ ***ADD***

Proceed as follows to define the necessary settings:

- Set ***ACTION*** to *deny M*.
- Set ***FILTER*** to *Deny FTP*.
- Press **SAVE** to confirm your settings.

4.2 Defining the Second Rule

- Go to ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***RULES*** ➜ ***ADD.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ACCESS][RULE][ADD]                                    vpn25

     Insert behind Rule       RI 1   FI 1   (ftp)

     Action                   allow  M

     Filter                   allow all (2)


                         SAVE                          CANCEL

Use <Space> to select
```

The following fields are relevant:

Field	Meaning
Insert behind Rule	The rule after which this rule to be applied.
Action	Action to be executed.
Filter	Filter to be used.

Table 4-2: Relevant fields in ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***RULES*** ➜ ***ADD***

Proceed as follows to define the necessary settings:

- Set ***INSERT BEHIND RULE*** to *RI 1 FI 1 (ftp).*
- Set ***ACTION*** to *allow M*.
- Set ***FILTER*** to *allow all.*
- Press **SAVE** to confirm your settings.

5 Applying Rules to an Interface

- Go to ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***INTERFACES*** ➜ ***EN0-1***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SECURITY][ACCESS][INTERFACES][EDIT]                              vpn25

     Interface                en0-1
     First Rule               RI 1   FI 1   (Deny FTP)

     Deny Silent              yes
     Reporting Method         info


                    SAVE                                  CANCEL
```

The following fields are relevant:

Field	Meaning
Interface	The interface to which the rule is applied.
First Rule	Defines which rule is to be applied first to this interface.

Table 5-1: Relevant fields in ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***INTERFACES*** ➜ ***EN0-1***

Proceed as follows to define the necessary settings:

- Set ***FIRST RULE*** to *RI 1 FI 1 (Deny FTP)*.
- 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**.

6 Result

This configuration ensures that incoming IP packets with the source address *192.168.10.192/25* and destination port *20 - 21* are discarded by the *en0-1* interface. It also ensures that all other packets are forwarded. If the second rule was not set to *allow all*, the default setting *deny all* would take effect and the interface would deny all incoming IP packets!

6.1 Test

You can see whether the FTP requests are denied under ***MONITORING AND DEBUGGING*** ➜ ***MESSAGES***.

- Go to ***MONITORING AND DEBUGGING*** ➜ ***MESSAGES.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[MONITOR][MESSAGE]: Syslog Messages                                vpn25

Subj  Lev Message

INET INF NAT: refused incoming session on ifc 10001 prot 6 213.7.46.9^
INET INF dialup if 10001 prot 17 192.168.10.254:1026->62.104.191.241:
PPP INF freenet: local IP address is 213.7.46.99, remote is 62.104.21
INET INF NAT: refused incoming session on ifc 10001 prot 6 213.7.46.9
INET INF refuse from if 100 prot 6 192.168.10.253:1158->213.217.69.67
INET INF refuse from if 100 prot 6 192.168.10.253:1157->62.146.2.97:2
INET INF NAT: refused incoming session on ifc 10001 prot 6 213.7.46.9
INET INF NAT: refused incoming session on ifc 10001 prot 6 213.7.46.9
INET INF NAT: refused incoming session on ifc 10001 prot 6 213.7.46.9
INET INF NAT: refused incoming session on ifc 10001 prot 6 213.7.46.9
INET INF NAT: refused incoming session on ifc 10001 prot 6 213.7.46.9
INET INF NAT: refused incoming session on ifc 10001 prot 6 213.7.46.9v



EXIT      RESET
```

As you can see, the request from the IP address *192.168.10.253* has been denied on the FTP server with the IP address *62.146.2.97*.

6.2 Overview of Configuration Steps

Field	Menu	Description	Compulsory field
Description	***Security → Access Lists → Filter → ADD***	e.g. *Deny FTP*	
Protocol	***Security → Access Lists → Filter → ADD***	e.g. *tcp*	Yes
Connection State	***Security → Access Lists → Filter → ADD***	*any*	Yes
Source Address	***Security → Access Lists → Filter → ADD***	e.g. *192.168.10.192*	Yes
Source Mask	***Security → Access Lists → Filter → ADD***	e.g. *255.255.255.128*	Yes
Source Port	***Security → Access Lists → Filter → ADD***	e.g. *any*	Yes
Destination Port	***Security → Access Lists → Filter → ADD***	*specify range*	Yes
Specify Port	***Security → Access Lists → Filter → ADD***	e.g. *20 - 21*	Yes
Action	***Security → Access Lists → Rules → ADD***	*deny M*	Yes
Filter	***Security → Access Lists → Rules → ADD***	*Deny FTP (1)*	Yes
Insert behind Rule	***Security → Access Lists → Rules → ADD***	*RI 1 FI 1 (ftp)*	Yes
Action	***Security → Access Lists → Rules → ADD***	*allow M*	Yes
Filter	***Security → Access Lists → Rules → ADD***	*allow all (2)*	Yes
Interface	***Security → Access Lists → Interfaces → en0-1***	*ETH1*	Yes
First Rule	***Security → Access Lists→ Interfaces → en0-1***	*RI 1 FI 1 (Deny FTP)*	Yes