funkwerk
enterprise communications

# bintec Workshop

# Network Address Translation Configuration


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

# 1 Introduction

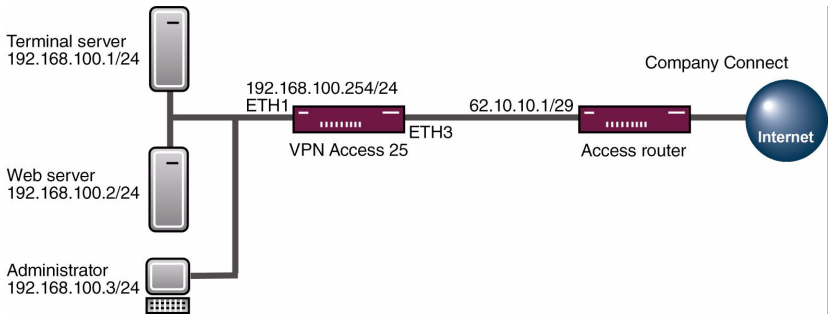
**The configuration of Network Address Translation is described in the chapters below.**

You have a permanent 2-Mbps connection to the Internet with 8 IP addresses. Your Ethernet interface 3 (eth3) is connected to the access router. This has the IP address 62.10.10.1/29, whereas the remaining IPs from 62.10.10.2 to 62.10.10.6 are entered on Ethernet interface 3. You configure NAT enables for accessing your router with Telnet.

You would also like to access your terminal server and the corporate Web server over the Internet. For administration at partner companies from your internal computer, you always need a certain external IP address.

The Setup Tool is used for the configuration.

## 1.1 Scenario




## 1.2 Requirements

The following requirements must be fulfilled for the configuration:

- Basic configuration of router. The basic configuration using the Wizard is recommended.
- A boot image of version 7.1.1 or later.
- A working Internet access. For example, *Company Connect* with 8 IP addresses.

# 2 Configuration

## 2.1 Settings in Network Address Translation Menu

You must make settings in the following menu for configuring Network Address Translation:

- Go to ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][NAT][EDIT]: NAT Configuration (en0-3)                  Head_Office


  Network Address Translation           on
  Silent Deny                           no
  PPTP Passthrough                      no

  Enter configuration for sessions:    requested from OUTSIDE
                                       requested from INSIDE




     SAVE                CANCEL
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Silent Deny | If you enable Silent Deny, the router does not answer incoming ICMP packets. |
| requested from OUTSIDE | For configuring which connections initialized from outside are allowed to pass through the router. |
| requested from INSIDE | For configuring whether certain internal PCs receive a permanent external IP address. |

Table 2-1: Relevant fields in ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE***

**Note**

If you would like to increase the security of your Internet access, it is advisable to enable ***SILENT DENY***.

## 2.2 NAT Sessions from OUTSIDE

Go to the following menu to configure NAT entries:

- ***IP ➜ NETWORK ADDRESS TRANSLATION ➜ INTERFACE ➜ REQUESTED FROM OUTSIDE ➜ ADD***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT -                          Head_Office
                               sessions from OUTSIDE (en0-3)


  Service                      user defined
  Protocol                     icmp

  Remote Address
  Remote Mask


  External Address
  External Mask
  External Port                any

  Internal Address
  Internal Mask                255.255.255.255
  Internal Port                any

            SAVE                                  CANCEL

Use <Space> to select
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Protocol | For configuring the protocol used by the service. |

| Field | Meaning |
|---|---|
| Remote Address | If you have a permanent IP address from which you can access the device, you can define restrictions here. |
| Remote Mask | The subnet mask that belongs to the remote address. This must always be 255.255.255.255 for a single IP. |
| External Address | The external IP address of the router you access if you have a static IP address. |
| External Mask | The subnet mask that belongs to the external address. This must always be 255.255.255.255 for a single IP. |
| External Port | This is the router port you reach from outside. |
| Internal Address | The IP address to which you wish to be forwarded when you reach the router. |
| Internal Mask | The subnet mask that belongs to the internal address. This must always be 255.255.255.255 for a single IP. |
| Internal Port | For configuring the port you wish to reach on the internal system. Leave the entry set to *ANY* if the internal and external port are the same. |

Table 2-2: Relevant fields in ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE*** ➜ ***REQUESTED FROM OUTSIDE*** ➜ ***ADD***

### 2.2.1 NAT Entries for Telnet

It should be possible to administrate your router using Telnet over the Internet router with the permanent IP address 62.10.10.2.

- Go to ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE*** ➜ ***REQUESTED FROM OUTSIDE*** ➜ ***ADD***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT -                         Head_Office
                               sessions from OUTSIDE (en0-3)


  Service                     user defined
  Protocol                    tcp

  Remote Address
  Remote Mask


  External Address            62.10.10.2
  External Mask               255.255.255.255
  External Port               specify          Port  23

  Internal Address            127.0.0.1
  Internal Mask               255.255.255.255
  Internal Port               any

           SAVE                                CANCEL
```

Proceed as follows to configure the enable:

- Set ***PROTOCOL*** to *tcp*.
- Enter your router's IP address *62.10.10.2* under ***EXTERNAL ADDRESS***.
- ***EXTERNAL MASK*** is set to *255.255.255.255*.
- Set ***EXTERNAL PORT*** to *specify/23*.
- Configure the ***INTERNAL ADDRESS*** for the router to the loopback address *127.0.0.1*.
- The ***INTERNAL MASK*** remains set to *255.255.255.255*.

### 2.2.2 NAT Entries for Web Server

The internal Web server is to be reachable under the IP address 62.10.10.3.

- Go to ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE*** ➜ ***REQUESTED FROM OUTSIDE*** ➜ ***ADD***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT -                          Head_Office
                               sessions from OUTSIDE (en0-3)


  Service                      user defined
  Protocol                     tcp

  Remote Address
  Remote Mask


  External Address             62.10.10.3
  External Mask                255.255.255.255
  External Port                specify          Port  80

  Internal Address             192.168.100.2
  Internal Mask                255.255.255.255
  Internal Port                any

            SAVE                                CANCEL
```

Proceed as follows to configure the enable:

- Set ***PROTOCOL*** to *tcp*.
- Enter the external IP address for the Web server under ***EXTERNAL ADDRESS***, i.e. *62.10.10.3*.
- ***EXTERNAL MASK*** is set to *255.255.255.255*.
- Set ***EXTERNAL PORT*** to *specify 80*.
- Configure ***INTERNAL ADDRESS*** to *192.168.100.2*.
- The ***INTERNAL MASK*** remains set to *255.255.255.255*.

### 2.2.3 NAT Entries for Terminal Server

The internal terminal server is to be reachable under the IP address 62.10.10.4. To prevent attackers easily recognizing from the open port 3389 that you are using a terminal server, you reach port 5000 from outside with the remote desktop.

- Go to ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE*** ➜ ***REQUESTED FROM OUTSIDE*** ➜ ***ADD***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT -                         Head_Office
                               sessions from OUTSIDE (en0-3)


  Service                     user defined
  Protocol                    tcp

  Remote Address
  Remote Mask



  External Address            62.10.10.4
  External Mask               255.255.255.255
  External Port               specify          Port  5000

  Internal Address            192.168.100.1
  Internal Mask               255.255.255.255
  Internal Port               specify          Port  3389

            SAVE                                CANCEL
```

Proceed as follows to configure the enable:

- Set ***PROTOCOL*** to *tcp*.
- Enter the external IP address used for the terminal server under ***EXTERNAL ADDRESS***, i.e. *62.10.10.4*.
- ***EXTERNAL MASK*** is set to *255.255.255.255*.
- Set ***EXTERNAL PORT*** to *specify 5000*.
- Configure ***INTERNAL ADDRESS*** to *192.168.100.1*.
- The ***INTERNAL MASK*** remains set to *255.255.255.255*.
- Set ***INTERNAL PORT*** to *specify 3389*.

## 2.3 NAT Sessions from INSIDE

Go to the following menu to configure NAT entries:

- ***IP ➜ NETWORK ADDRESS TRANSLATION ➜ INTERFACE ➜ REQUESTED FROM INSIDE ➜ ADD***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT Configuration -          Head_Office
                               sessions from INSIDE (en0-3)

  Service                      user defined
  Protocol                     icmp

  Remote Address
  Remote Mask
  Remote Port                  any

  External Address
  External Mask                255.255.255.255
  External Port                any

  Internal Address
  Internal Mask
  Internal Port                any

            SAVE                                  CANCEL

Use <Space> to select
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Protocol | For configuring the protocol used by the service. |
| Remote Address | If you have a permanent IP address you are allowed to access, you can define restrictions here. |
| Remote Mask | The subnet mask that belongs to the remote address. This must always be 255.255.255.255 for a single IP. |
| Remote Port | The remote port you access if you wish to make restrictions. |

| Field | Meaning |
|---|---|
| External Address | The external IP address of the router to which you translate if you have a static IP address. |
| External Mask | The subnet mask that belongs to the external address. This must always be 255.255.255.255 for a single IP. |
| External Port | The sender port to which you translate, if applicable. |
| Internal Address | The IP address of the internal PC. |
| Internal Mask | The subnet mask that belongs to the internal address. This must always be 255.255.255.255 for a single IP. |
| Internal Port | For configuring the port used by the PC as sender port. |

Table 2-3: Relevant fields in ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE*** ➜ ***REQUESTED FROM INSIDE*** ➜ ***ADD***

### 2.3.1 NAT Entries for Administration

The internal PC 192.168.100.3 is used for administrative purposes to access external partner companies over the Internet. The PC here must always use the same IP address as the sender. In this case, for example, 62.10.10.5.

- Go to ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE*** ➜ ***REQUESTED FROM OUTSIDE*** ➜ ***ADD***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT Configuration -          Head_Office
                               sessions from INSIDE (en0-3)

  Service                      user defined
  Protocol                     any

  Remote Address
  Remote Mask
  Remote Port                  any

  External Address             62.10.10.5
  External Mask                255.255.255.255
  External Port                any

  Internal Address             192.168.100.3
  Internal Mask                255.255.255.255
  Internal Port                any

           SAVE                                  CANCEL
```

Proceed as follows to configure the entries:

- Set ***PROTOCOL*** to *any*.
- Enter the external IP address used for the terminal server under ***EXTERNAL ADDRESS***, e.g. *62.10.10.5*.
- ***EXTERNAL MASK*** is set to *255.255.255.255*.
- Configure ***INTERNAL ADDRESS***, e.g. to *192.168.100.3*.
- The ***INTERNAL MASK*** remains set to *255.255.255.255*.

# 3 Result

You have configured NAT enables so that you can access the router with Telnet over the Internet. You also allow access to your internal Web server and the terminal server over the Internet. In addition, you have assigned your administration PC a permanent IP address for the Internet.

## 3.1 Test

To check the settings, activate debug mode in the shell with the command `debug all&`. Run Telnet on the router (62.10.10.2) from an external PC on the Internet.

The following message must appear if you are from the IP address 80.65.48.135:

```
12:14:20 DEBUG/INET: NAT: new incoming session on ifc 300 prot 6
127.0.0.1:23/62.10.10.2:23 <- 80.65.48.135:1024
```

Run Telnet from the administration PC to an external IP address (e.g. 80.65.48.135).

The following message must appear if you access the IP address 80.65.48.135 with Telnet:

```
12:14:20 DEBUG/INET: NAT: new outgoing session on ifc 300 prot 6
192.168.100.3:1039/62.10.10.5:32788 -> 80.65.48.135:23
```

## 3.2 Overview of Configuration Steps

**Telnet**

| Field | Menu | Description |
|---|---|---|
| Protocol | ***REQUESTED FROM OUTSIDE → ADD*** | *tcp* |
| External Address | ***REQUESTED FROM OUTSIDE → ADD*** | e.g. *62.10.10.2* |
| External Mask | ***REQUESTED FROM OUTSIDE → ADD*** | *255.255.255.255* |
| External Port | ***REQUESTED FROM OUTSIDE → ADD*** | *specify 23* |
| Internal Address | ***REQUESTED FROM OUTSIDE → ADD*** | *127.0.0.1* |
| Internal Mask | ***REQUESTED FROM OUTSIDE → ADD*** | *255.255.255.255* |

**Web Server**

| Field | Menu | Description |
|---|---|---|
| Protocol | ***REQUESTED FROM OUTSIDE → ADD*** | *tcp* |
| External Address | ***REQUESTED FROM OUTSIDE → ADD*** | e.g. *62.10.10.3* |
| External Mask | ***REQUESTED FROM OUTSIDE → ADD*** | *255.255.255.255* |
| External Port | ***REQUESTED FROM OUTSIDE → ADD*** | *specify 80* |
| Internal Address | ***REQUESTED FROM OUTSIDE → ADD*** | e.g. *192.168.100.2* |
| Internal Mask | ***REQUESTED FROM OUTSIDE → ADD*** | *255.255.255.255* |

**Terminal Server**

| Field | Menu | Description |
|---|---|---|
| Protocol | ***REQUESTED FROM OUTSIDE → ADD*** | *tcp* |
| External Address | ***REQUESTED FROM OUTSIDE → ADD*** | e.g. *62.10.10.4* |
| External Mask | ***REQUESTED FROM OUTSIDE → ADD*** | *255.255.255.255* |

| Field | Menu | Description |
|---|---|---|
| External Port | ***REQUESTED FROM OUTSIDE ➜ ADD*** | e.g. *specify 5000* |
| Internal Address | ***REQUESTED FROM OUTSIDE ➜ ADD*** | e.g. *192.168.100.1* |
| Internal Mask | ***REQUESTED FROM OUTSIDE ➜ ADD*** | *255.255.255.255* |
| External Port | ***REQUESTED FROM OUTSIDE ➜ ADD*** | *specify 3389* |

**Administration PC**

| Field | Menu | Description |
|---|---|---|
| Protocol | ***REQUESTED FROM INSIDE ➜ ADD*** | *any* |
| External Address | ***REQUESTED FROM INSIDE ➜ ADD*** | e.g. *62.10.10.5* |
| External Mask | ***REQUESTED FROM INSIDE ➜ ADD*** | *255.255.255.255* |
| Internal Address | ***REQUESTED FROM INSIDE ➜ ADD*** | e.g. *192.168.100.3* |
| Internal Mask | ***REQUESTED FROM INSIDE ➜ ADD*** | *255.255.255.255* |