bintec Workshop

Configuration of DMZ

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

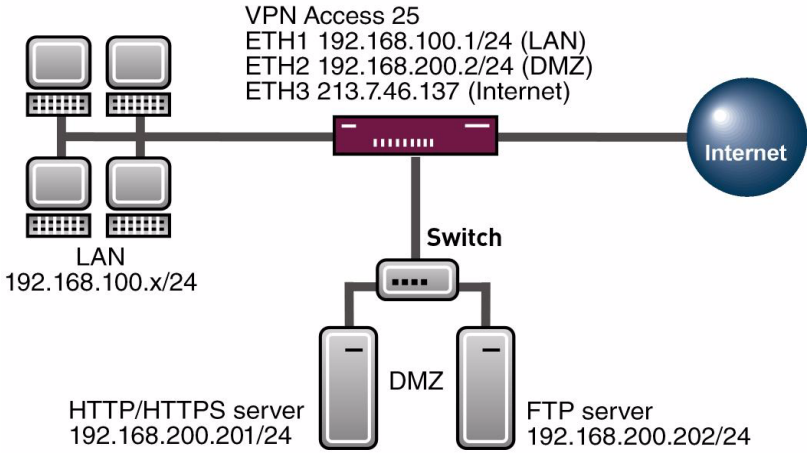
Funkwerk Enterprise Communications GmbH Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +49 180 300 9191 0 Fax: +49 180 300 9193 0 Internet: www.funkwerk-ec.com	Bintec France 6/8 Avenue de la Grande Lande F-33174 Gradignan France Telephone: +33 5 57 35 63 00 Fax: +33 5 56 89 14 05 Internet: www.bintec.fr

1 Introduction

The configuration of a DMZ (Demilitarized Zone) using a Bintec VPN Access 25 gateway (software version 7.1.6 patch 3) is described in the following chapters. The Setup Tool is used for the configuration.

1.1 Scenario

All HTTP/HTTPS and FTP requests from the Internet are to be forwarded to the WEB server and FTP server in the DMZ.



1.2 Requirements

The following are required for the configuration:

- A Bintec **VPN Access 25** gateway.
- Internet access with static public IP address (see Bintec FAQ: **Border router on an Internet leased line with fixed IP address**).

- A WEB server and FTP server in the DMZ.
- A configured PC (see User's Guide Part **Access and Configuration**).
- Your LAN is connected to the ETH1 Ethernet interface of your gateway.
- Your DMZ is connected to the ETH2 Ethernet interface of your gateway.

2 Configuration of DMZ

2.1 Configuration of Internet Access

Note

NAT must be activated on the interface used to provide the Internet connection.

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

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][NAT]: NAT Configuration                                      vpn25

  Select IP Interface to be configured for NAT

  Name                  Nat      Static mappings     Static mappings
                                  from Outside         from Inside
  en0-1                 off          0                    0
  en0-1-snap            off          0                    0
  en0-2                 off          0                    0
  en0-2-snap            off          0                    0
  en0-3                 off          0                    0
  en0-3-snap            off          0                    0
  Internet              on           0                    0

  EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to select/edit
```

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

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][NAT][EDIT]: NAT Configuration Internet                       vpn25

  Network Address Translation           on
  Silent Deny                           no
  PPTP Passthrough                      no

  Enter configuration for sessions:    requested from OUTSIDE
                                        requested from INSIDE


     SAVE               CANCEL
```

The following field is relevant:

Field	Meaning
Network Address Translation	Determines whether NAT is on or off.

Table 2-1: Relevant field in ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***NAME***

Proceed as follows to define the necessary settings:

- Set ***NETWORK ADDRESS TRANSLATION*** to *on*.
- Leave all the other settings as they are.
- Press **SAVE** to confirm your settings.

2.2 Configuration of Requests from Outside

As NAT is activated on the Internet interface, it is not possible to access internal PCs from the Internet. Internet users are to be allowed HTTP/HTTPS access to the WEB server and FTP access to the FTP server. You must therefore allow these "Requests from Outside".

- Go to ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE]: NAT sessions from OUTSIDE (Internet)   vpn25

Abbreviations: r(remote) i(internal) e(external) a(address) p(port)

  Service      Conditions
  ------------------------------------------------------------

     ADD                 DELETE                          EXIT
```

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

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

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][EDIT]: NAT sessions                        vpn25
                                from OUTSIDE (Internet)

  Service                       user defined
  Protocol                      tcp

  Remote Address
  Remote Mask


  External Address              213.7.46.137
  External Mask                 255.255.255.255
  External Port                 specify          Port  443

  Internal Address              192.168.200.201
  Internal Mask                 255.255.255.255
  Internal Port                 specify          Port  443

            SAVE                                 CANCEL
```

The following fields are relevant:

Field	Meaning
Service	Type of service.
Protocol	Protocol used.
External Address	External IP address reached.
External Mask	Netmask of external IP address.
External Port	Port reached.
Internal Address	Internal IP address to which the requests from outside are to be directed.
Internal Mask	Netmask of internal IP address.
Internal Port	Internal port to which the requests from outside are to be directed.

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

Proceed as follows to define the necessary settings:

- Set ***SERVICE*** to *user defined*.
- Set ***PROTOCOL*** to *tcp*.
- Enter your public IP address under ***EXTERNAL ADDRESS***, e.g. *213.7.46.137*.
- Enter your associated netmask under ***EXTERNAL MASK***, e.g. *255.255.255.255*.
- Set ***EXTERNAL PORT*** to *specify*.
- Enter *443* under ***PORT***.
- Enter the IP address of your WEB server under ***INTERNAL ADDRESS***, e.g. *192.168.200.201*.
- Enter the netmask of your WEB server under ***INTERNAL MASK***, e.g. *255.255.255.255*.
- Set ***INTERNAL PORT*** to *specify*.
- Enter *443* under ***PORT***.
- Press **SAVE** to confirm your settings.

You have now configured your system so that HTTPS requests are forwarded to your external IP address at your WEB server in the DMZ.

Now configure the corresponding entries for HTTP and FTP.

Note

Preconfigured services are already available for some services, such as HTTP. This means you no longer need to state the protocol or external ports, as these are already configured.

3 Checking the Configuration

The list should look like this when you have configured all the necessary "Requests from Outside".

- Go to ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE]: NAT sessions from OUTSIDE (Internet)   vpn25

  Abbreviations: r(remote) i(internal) e(external) a(address) p(port)


 Service      Conditions
 ------------------------------------------------------------
 20/tcp       ea 213.7.46.137/32, ia 192.168.200.202/32, ep 20, ip 20
 443/tcp      ea 213.7.46.137/32, ia 192.168.200.201/32, ep 443, i...
 ftp          ea 213.7.46.137/32, ia 192.168.200.202/32, ep 21, ip 21
 http         ea 213.7.46.137/32, ia 192.168.200.201/32, ep 80, ip 80



     ADD                 DELETE                          EXIT
```

This Request List now causes HTTP and HTTPS requests to be forwarded to your external IP address at your WEB server. FTP requests are forwarded to your FTP server. Other requests are denied.

Return to the main menu and finally save your new configuration in the flash memory with ***EXIT*** and ***SAVE AS BOOT CONFIGURATION AND EXIT***.

3.1 Test

To trace whether requests are forwarded, enter the following in the command line of the gateway:

```
vpn25:>debug all
```

```
01:00:47 DEBUG/INET: NAT: new incoming session on ifc 300 prot 6 192.168.200.201
:80/213.7.46.137:80 <- 213.7.46.138:1054
01:00:48 DEBUG/INET: NAT: new incoming session on ifc 300 prot 6 192.168.200.201
:80/213.7.46.137:80 <- 213.7.46.138:1055
01:01:04 DEBUG/INET: NAT: delete session on ifc 300 prot 6 192.168.200.201:80/21
3.7.46.137:80 <-> 213.7.46.138:1054
01:01:05 DEBUG/INET: NAT: delete session on ifc 300 prot 6 192.168.200.201:80/21
3.7.46.137:80 <-> 213.7.46.138:1055
01:01:22 DEBUG/INET: NAT: new incoming session on ifc 300 prot 6 192.168.0.202:2
1/213.7.46.137:21 <- 213.7.46.138:1056
01:01:43 DEBUG/INET: NAT: new incoming session on ifc 300 prot 6 192.168.0.202:2
1/213.7.46.137:21 <- 213.7.46.138:1057
01:01:47 DEBUG/INET: NAT: delete session on ifc 300 prot 6 192.168.0.202:21/213.7.46.137:21 <->
213.7.46.138:1056
vpn25:>
```

As the debug extract shows, the HTTP request (port 80) has been forwarded from IP address *213.7.46.138* to IP address *192.168.200.201*. The FTP request (port 21) has also been forwarded.

3.2 Overview of Configuration Steps

Field	Menu	Description	Compulsory field
Service	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	*user defined*	Yes
Protocol	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	*tcp*	Yes
External Address	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	e.g. *213.7.46.137*	Yes
External Mask	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	e.g. *255.255.255.255*	Yes

Field	Menu	Description	Compulsory field
External Port	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	*specify*	Yes
Port	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	*443*	Yes
Internal Address	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	e.g. *192.168.200.201*	Yes
Internal Mask	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	e.g. *255.255.255.255*	Yes
Internal Port	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	*specify*	Yes
Port	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	*443*	Yes