funkwerk
enterprise communications

bintec Workshop

Konfiguration von Network Address Translation

Version 0.9

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von bintec-Gateways ab Software-Release 7.1.4. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind zu finden unter www.funkwerk-ec.com.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie **Release Notes** für bintec-Gateways finden Sie unter www.funkwerk-ec.com.

Als Multiprotokollgateways bauen bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

bintec und das bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.funkwerk-ec.com.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Deutschland

Telefon: +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
Frankreich

Telefon: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Einleitung

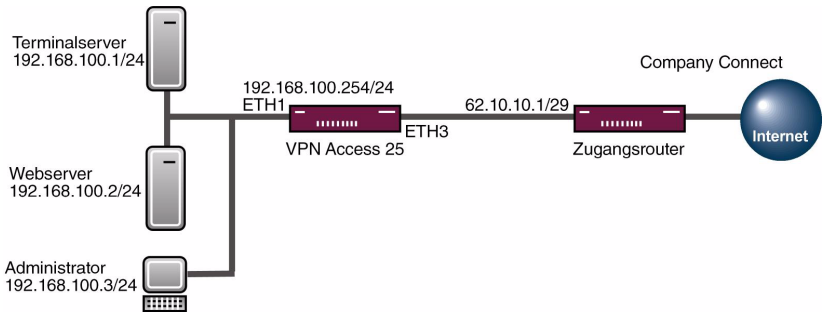
Im Folgenden wird die Konfiguration von Network Address Translation erklärt.

Sie haben eine permanente 2-Mbit Verbindung ins Internet mit 8 IP-Adressen. Ihr Ethernet Interface 3 (eth3) ist an dem Zugangsrouter angeschlossen. Dieser hat die IP-Adresse 62.10.10.1/29 während die restlichen IP's von 62.10.10.2 bis 62.10.10.6 auf dem Ethernet Interface 3 eingetragen sind. Sie konfigurieren NAT Freigaben, damit Sie per Telnet auf Ihren Router zugreifen können.

Ausserdem möchten Sie auf Ihren Terminalserver und auf den Firmen Webserver über das Internet zugreifen. Für die Administration auf Partner-Unternehmen von Ihrem internen Computer aus, benötigen Sie immer eine bestimmte externe IP-Adresse.

Zur Konfiguration wird hierbei das Setup-Tool verwendet.

1.1 Szenario



1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Grundkonfiguration des Routers. Empfohlen wird die Grundkonfiguration mit dem Wizard.
- Ein Bootimage ab Version 7.1.1.
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang. Hier als Beispiel *Company Connect* mit 8 IP-Adressen.

2 Konfiguration

2.1 Einstellungen im Menü Network Address Translation

Um Network Address Translation zu konfigurieren, müssen Sie im folgenden Menü Einstellungen vornehmen:

- Gehen Sie zu ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE***.

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


  Network Address Translation           on
  Silent Deny                           no
  PPTP Passthrough                      no

  Enter configuration for sessions :    requested from OUTSIDE
                                        requested from INSIDE




     SAVE                CANCEL
```

Folgende Felder sind relevant:

Feld	Bedeutung
Silent Deny	Wenn Sie Silent Deny einschalten, antwortet der Router nicht auf eingehende ICMP Pakete.
requested from OUTSIDE	Hier konfigurieren Sie, welche Verbindungen die von aussen initialisiert wurden, durch den Router dürfen.
requested from INSIDE	Hier konfigurieren Sie, ob bestimmte interne Rechner eine feste externe IP-Adresse bekommen.

Tabelle 2-1: Relevante Felder in ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE***

Hinweis

Wenn Sie die Sicherheit Ihres Internetzugangs erhöhen möchten, ist es empfehlenswert, ***SILENT DENY*** einzuschalten.

2.2 NAT - sessions from OUTSIDE

Gehen Sie in Folgendes Menü, um NAT Einträge zu konfigurieren:

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

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[IP] [NAT] [EDIT] [OUTSIDE] [ADD]: NAT -                          Zentrale
                                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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Protocol	Hier konfigurieren Sie das Protokoll, mit dem der Dienst arbeitet.

Feld	Bedeutung
Remote Address	Wenn Sie eine feste IP-Adresse haben, von der Sie auf das Gerät zugreifen dürfen, können Sie hier Einschränkungen vornehmen.
Remote Mask	Die Subnet Mask, die zu der Remote Address gehört. Muss bei einer einzigen IP immer 255.255.255.255 sein.
External Address	Ist die externe IP-Adresse des Routers, auf die Sie zugreifen, wenn Sie eine statische IP-Adresse haben.
External Mask	Die Subnet Mask, die zu der External Address gehört. Muss bei einer einzigen IP immer 255.255.255.255 sein.
External Port	Dies ist der Port, den Sie von extern am Router ansprechen.
Internal Address	Das ist die IP, auf die Sie umgeleitet werden möchten, wenn Sie den Router ansprechen.
Internal Mask	Die Subnet Mask, die zu der Internal Address gehört. Muss bei einer einzigen IP immer 255.255.255.255 sein.
Internal Port	Hier konfigurieren Sie den Port, den Sie auf dem internen System ansprechen möchten. Lassen Sie den Eintrag auf *ANY*, wenn sich der interne vom externen nicht unterscheidet.

Tabelle 2-2: Relevante Felder in ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE*** ➜ ***REQUESTED FROM OUTSIDE*** ➜ ***ADD***

2.2.1 NAT Einträge für Telnet

Ihr Router soll auf die feste IP-Adresse 62.10.10.2 über das Internet per Telnet administrierbar sein.

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

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT -                            Zentrale
                               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
```

Gehen Sie folgendermaßen vor, um die Freigabe zu konfigurieren:

- Das ***PROTOCOL*** stellen Sie auf *tcp*.
- Bei ***EXTERNAL ADDRESS*** tragen Sie Ihre IP-Adresse des Routers ein *62.10.10.2*.
- Unter ***EXTERNAL MASK*** steht die *255.255.255.255*.
- Den ***EXTERNAL PORT*** stellen Sie auf *specify/23*.
- Die ***INTERNAL ADDRESS*** konfigurieren Sie für den Router auf die Loopback-Adresse *127.0.0.1*.
- Die ***INTERNAL MASK*** bleibt auf *255.255.255.255*.

2.2.2 NAT Einträge für den Webserver

Der interne Webserver soll auf die IP-Adresse 62.10.10.3 anzusprechen sein.

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

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT -                              Zentrale
                               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
```

Gehen Sie folgendermaßen vor, um die Freigabe zu konfigurieren:

- Das ***PROTOCOL*** stellen Sie auf *tcp*.
- Bei ***EXTERNAL ADDRESS*** tragen Sie die externe IP-Adresse ein, die für den Webserver ist *62.10.10.3*.
- Unter ***EXTERNAL MASK*** steht die *255.255.255.255*.
- Den ***EXTERNAL PORT*** stellen Sie auf *specify 80*.
- Die ***INTERNAL ADDRESS*** konfigurieren Sie auf *192.168.100.2*.
- Die ***INTERNAL MASK*** bleibt auf *255.255.255.255*.

2.2.3 NAT Einträge für den Terminal Server

Der interne Terminal Server soll auf die IP-Adresse 62.10.10.4 anzusprechen sein. Damit nicht Angreifer bei dem offen Port 3389 leicht erkennen können, dass Sie einen Terminal Server einsetzen, sprechen Sie von extern mit Remote Desktop den Port 5000 an.

- Gehen Sie zu ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE*** ➜ ***REQUESTED FROM OUTSIDE*** ➜ ***ADD***.

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT -                              Zentrale
                               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
```

Gehen Sie folgendermaßen vor, um die Freigabe zu konfigurieren:

- Das ***PROTOCOL*** stellen Sie auf *tcp*.
- Bei ***EXTERNAL ADDRESS*** tragen Sie die externe IP-Adresse ein, die für den Terminal Server verwendet wird *62.10.10.4*.
- Unter ***EXTERNAL MASK*** steht die *255.255.255.255*.
- Den ***EXTERNAL PORT*** stellen Sie auf *specify 5000*.
- Die ***INTERNAL ADDRESS*** konfigurieren Sie auf *192.168.100.1*.
- Die ***INTERNAL MASK*** bleibt auf *255.255.255.255*.
- Den ***INTERNAL PORT*** stellen Sie auf *specify 3389*.

2.3 NAT - sessions from INSIDE

Gehen Sie in folgendes Menü, um NAT Einträge zu konfigurieren:

- ***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-              Zentrale
                               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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Protocol	Hier konfigurieren Sie das Protokoll, mit dem der Dienst arbeitet.
Remote Address	Wenn Sie eine feste IP-Adresse haben, auf die Sie zugreifen dürfen, können Sie hier Einschränkungen vornehmen.
Remote Mask	Die Subnet Mask, die zu der Remote Address gehört. Muss bei einer einzigen IP immer 255.255.255.255 sein.

Feld	Bedeutung
Remote Port	Dies ist der entfernte Port, auf den Sie zugreifen möchten, falls Sie Einschränkungen vornehmen möchten.
External Address	Ist die externe IP-Adresse des Routers, in die Sie übersetzen möchten, wenn Sie eine statische IP-Adresse haben.
External Mask	Die Subnet Mask, die zu der External Address gehört. Muss bei einer einzigen IP immer 255.255.255.255 sein.
External Port	Dies ist der Absenderport, in den Sie ggf. übersetzen möchten.
Internal Address	Das ist die IP-Adresse von dem internen Rechner.
Internal Mask	Die Subnet Mask, die zu der Internal Address gehört. Muss bei einer einzigen IP immer 255.255.255.255 sein.
Internal Port	Hier konfigurieren Sie den Port, den der Rechner als Absenderport nutzt.

Tabelle 2-3: Relevante Felder in ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***INTERFACE*** ➜ ***REQUESTED FROM INSIDE*** ➜ ***ADD***

2.3.1 NAT Einträge für die Administration

Der interne Rechner 192.168.100.3 wird für administrative Zwecke genutzt, um auf externe Partnerunternehmen über das Internet zuzugreifen. Dafür muss der PC immer dieselbe IP-Adresse wie der Absender verwenden. Hier als Beispiel die 62.10.10.5.

- Gehen Sie zu ***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-              Zentrale
                               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
```

Gehen Sie folgendermaßen vor, um die Einträge zu konfigurieren:

- Das ***PROTOCOL*** stellen Sie auf *any*.
- Bei ***EXTERNAL ADDRESS*** tragen Sie die externe IP-Adresse ein, die für den Terminal Server verwendet wird z.B. *62.10.10.5*.
- Unter ***EXTERNAL MASK*** steht die *255.255.255.255*.
- Die ***INTERNAL ADDRESS*** konfigurieren Sie auf z.B. *192.168.100.3*.
- Die ***INTERNAL MASK*** bleibt auf *255.255.255.255*.

3 Ergebnis

Sie haben NAT-Freigaben konfiguriert, damit Sie über das Internet per Telnet auf den Router zugreifen können. Zudem gestatten Sie den Zugriff auf Ihren internen Webserver und den Terminal Server über das Internet. Weiterhin haben Sie Ihrem Administrations-Rechner eine feste IP-Adresse für das Internet zugeteilt.

3.1 Test

Um die Einstellungen zu überprüfen, rufen Sie den Debugmodus an der Shell mit dem Befehl `debug all&` auf. Führen Sie von einem externen Rechner im Internet Telnet auf den Router (62.10.10.2) aus.

Folgende Meldung müsste erscheinen, wenn Sie von der IP-Adresse 80.65.48.135 kommen:

```
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
```

Führen Sie von dem Administrationsrechner Telnet auf eine externe IP-Adresse (z.B. 80.65.48.135) aus.

Folgende Meldung müsste erscheinen, wenn Sie auf die IP-Adresse 80.65.48.135 per Telnet zugreifen:

```
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 Konfigurationsschritte im Überblick

Telnet

Feld	Menü	Wert
Protocol	***REQUESTED FROM OUTSIDE → ADD***	*tcp*
External Address	***REQUESTED FROM OUTSIDE → ADD***	z.B. *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*

Webserver

Feld	Menü	Wert
Protocol	***REQUESTED FROM OUTSIDE → ADD***	*tcp*
External Address	***REQUESTED FROM OUTSIDE → ADD***	z.B. *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***	z.B. *192.168.100.2*
Internal Mask	***REQUESTED FROM OUTSIDE → ADD***	*255.255.255.255*

Terminal Server

Feld	Menü	Wert
Protocol	***REQUESTED FROM OUTSIDE → ADD***	*tcp*
External Address	***REQUESTED FROM OUTSIDE → ADD***	z.B. *62.10.10.4*
External Mask	***REQUESTED FROM OUTSIDE → ADD***	*255.255.255.255*

Feld	Menü	Wert
External Port	***REQUESTED FROM OUTSIDE ➜ ADD***	z.B. *specify 5000*
Internal Address	***REQUESTED FROM OUTSIDE ➜ ADD***	z.B. *192.168.100.1*
Internal Mask	***REQUESTED FROM OUTSIDE ➜ ADD***	*255.255.255.255*
External Port	***REQUESTED FROM OUTSIDE ➜ ADD***	*specify 3389*

Administrations Rechner

Feld	Menü	Wert
Protocol	***REQUESTED FROM INSIDE ➜ ADD***	*any*
External Address	***REQUESTED FROM INSIDE ➜ ADD***	z.B. *62.10.10.5*
External Mask	***REQUESTED FROM INSIDE ➜ ADD***	*255.255.255.255*
Internal Address	***REQUESTED FROM INSIDE ➜ ADD***	z.B. *192.168.100.3*
Internal Mask	***REQUESTED FROM INSIDE ➜ ADD***	*255.255.255.255*