bintec Workshop

Konfiguration einer DMZ

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

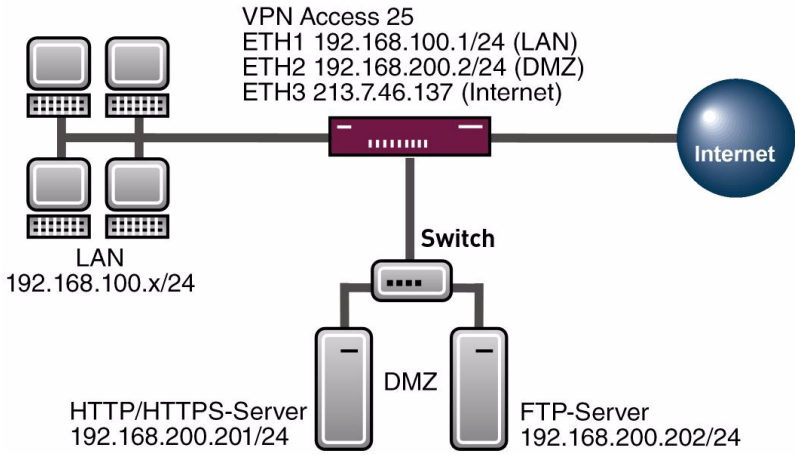
1 Einleitung 3
1.1 Szenario 3
1.2 Voraussetzungen 3
2 Konfiguration der DMZ 5
2.1 Konfiguration des Internetzugangs 5
2.2 Konfiguration der Requests from Outside 6
3 Überprüfung der Konfiguration 9
3.1 Test 9
3.2 Konfigurationsschritte im Überblick 10

1 Einleitung

Im Folgenden wird die Konfiguration einer DMZ (Demilitarized Zone) mittels eines Bintec VPN Access 25 Gateways (Software Version 7.1.6 Patch 3) beschrieben. Zur Konfiguration wird das Setup Tool verwendet.

1.1 Szenario

Alle HTTP/HTTPS- und FTP-Anfragen aus dem Internet sollen an den WEB- bzw. an den FTP-Server in der DMZ weitergeleitet werden.



1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein Bintec **VPN Access 25** Gateway.
- Internetzugang mit statischer öffentlicher IP-Adresse (siehe Bintec FAQ: **Grenzrouter an einer Internet Festverbindung mit fester IP-Adresse**).

- Einen WEB- und einen FTP-Server in der DMZ.
- PC einrichten (siehe Benutzerhandbuch Teil **Zugang und Konfiguration**).
- Ihr LAN wird an die Ethernet-Schnittstelle ETH1 Ihres Gateways angeschlossen.
- Ihre DMZ wird an die Ethernet-Schnittstelle ETH2 Ihres Gateways angeschlossen.

2 Konfiguration der DMZ

2.1 Konfiguration des Internetzugangs

Hinweis

Auf dem Interface, über welches die Internetverbindung realisiert wird, muss NAT aktiviert sein.

- Gehen Sie zu ***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
```

- Gehen Sie zu ***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
```

Folgendes Feld ist relevant:

Feld	Bedeutung
Network Address Translation	Bestimmt, ob NAT an oder aus ist.

Tabelle 2-1: Relevantes Feld in ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***NAME***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***NETWORK ADDRESS TRANSLATION*** *on*.
- Belassen Sie alle anderen Einstellungen beim Default.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

2.2 Konfiguration der Requests from Outside

Da auf dem Internet-Interface NAT aktiviert wurde, ist es nicht möglich, vom Internet auf interne Rechner zuzugreifen. Es soll Internetznutzern der HTTP/HTTPS Zugang zum WEB-Server und der FTP Zugang zum FTP-Server gestattet werden. Daher müssen Sie diese "Requests from Outside" erlauben.

- Gehen Sie zu ***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
```

Durch den Menüpunkt ***ADD*** können Sie Einträge hinzufügen.

- Gehen Sie zu ***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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Service	Art des Dienstes.
Protocol	Verwendetes Protokoll.
External Address	Angesprochene externe IP-Adresse.
External Mask	Netzmaske der externen IP-Adresse.
External Port	Angesprochener Port.
Internal Address	Interne IP-Adresse, an die Anfragen von außen geleitet werden sollen.
Internal Mask	Netzmaske der internen IP-Adresse.
Internal Port	Interner Port, an den Anfragen von außen geleitet werden sollen.

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

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***SERVICE*** *user defined*.
- Wählen Sie unter ***PROTOCOL*** *tcp*.
- Tragen Sie unter ***EXTERNAL ADDRESS*** Ihre öffentliche IP-Adresse ein, z.B. *213.7.46.137*.
- Tragen Sie unter ***EXTERNAL MASK*** Ihre zugehörige Netzmaske ein, z.B. *255.255.255.255*.
- Wählen Sie unter ***EXTERNAL PORT*** *specify*.
- Tragen Sie unter ***PORT*** *443* ein.
- Tragen Sie unter ***INTERNAL ADDRESS*** die IP-Adresse Ihres WEB-Servers ein, z.B. *192.168.200.201*.
- Tragen Sie unter ***INTERNAL MASK*** die Netzmaske Ihres WEB-Servers ein, z.B. *255.255.255.255*.
- Wählen Sie unter ***INTERNAL PORT*** *specify*.
- Tragen Sie unter ***PORT*** *443* ein.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

Sie haben nun konfiguriert, dass HTTPS-Anfragen auf Ihre externe IP-Adresse an Ihren WEB-Server in der DMZ weitergeleitet werden.

Konfigurieren Sie nun entsprechende Einträge für HTTP und für FTP.

Hinweis

Für manche Dienste, wie z.B. HTTP, gibt es bereits vorgefertigte Services. Dort brauchen Sie kein Protokoll und keine externen Ports mehr anzugeben, da diese bereits vorkonfiguriert sind.

3 Überprüfung der Konfiguration

Wenn Sie alle nötigen "Requests from Outside" konfiguriert haben, sollte die Liste wie folgt aussehen.

- Gehen Sie zu ***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
```

Durch diese Request-Liste werden nun HTTP- und HTTPS-Anfragen auf Ihre externe IP-Adresse an Ihren WEB-Server geleitet. FTP-Anfragen werden zu Ihrem FTP-Server geleitet. Andere Anfragen werden abgelehnt.

Gehen Sie zurück ins Hauptmenü und sichern Sie zum Abschluß Ihre neue Konfiguration im Flashmemory mit ***EXIT*** und ***SAVE AS BOOT CONFIGURATION AND EXIT***.

3.1 Test

Um mitverfolgen zu können, ob Anfragen umgeleitet werden, geben Sie in der Kommandozeile des Gateways Folgendes ein:

```
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:>
```

Wie der debug Auszug zeigt wurde die HTTP-Anfrage (Port 80) von der IP-Adresse *213.7.46.138* auf die IP-Adresse *192.168.200.201* umgeleitet. Ebenso wurde die FTP-Anfrage (Port 21) umgeleitet.

3.2 Konfigurationsschritte im Überblick

Feld	Menü	Wert	Pflichtfeld
Service	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	*user defined*	Ja
Protocol	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	*tcp*	Ja
External Address	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	z.B. *213.7.46.137*	Ja
External Mask	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ "***INTERNETINTERFACE***" ➜ ***REQUESTED FROM OUTSIDE***	z.B. *255.255.255.255*	Ja

Feld	Menü	Wert	Pflichtfeld
External Port	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***"INTERNETINTERFACE"*** ➜ ***REQUESTED FROM OUTSIDE***	*specify*	Ja
Port	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***"INTERNETINTERFACE"*** ➜ ***REQUESTED FROM OUTSIDE***	*443*	Ja
Internal Address	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***"INTERNETINTERFACE"*** ➜ ***REQUESTED FROM OUTSIDE***	z.B. *192.168.200.201*	Ja
Internal Mask	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***"INTERNETINTERFACE"*** ➜ ***REQUESTED FROM OUTSIDE***	z.B. *255.255.255.255*	Ja
Internal Port	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***"INTERNETINTERFACE"*** ➜ ***REQUESTED FROM OUTSIDE***	*specify*	Ja
Port	***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***"INTERNETINTERFACE"*** ➜ ***REQUESTED FROM OUTSIDE***	*443*	Ja