KONFIGURATION VON ACCESS LISTEN UND FILTERN

Bintec Workshop
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

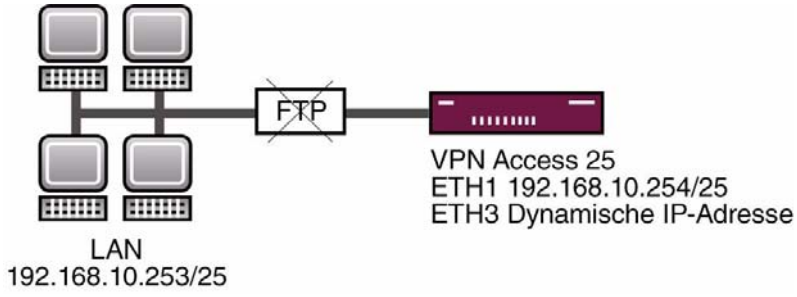
Telefon: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Einleitung

Im Folgenden wird die Konfiguration von Access Listen und Filtern anhand von einem Bintec VPN Access 25 Gateway beschrieben. Zur Konfiguration wird hierbei das Setup Tool verwendet.

1.1 Szenario

Sie wollen einem bestimmten Adressbereich verbieten das FTP-Protokoll zu nutzen. Der Adressbereich ist 192.168.10.192/25.



1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein Bintec **VPN Access 25** Gateway.
- Bestehende Internetverbindung (siehe Bintec FAQ: Konfiguration einer xDSL Verbindung).
- Ihr LAN wird über die erste Ethernet-Schnittstelle (ETH 1) Ihres Gateways angeschlossen.
- PC einrichten (siehe Benutzerhandbuch Teil Zugang und Konfiguration).

1 Einleitung

2 Konfiguration der Access Liste

2.1 Deaktivieren aller Filter

- Gehen Sie zu ***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
```

Folgendes Feld ist relevant:

Feld	Bedeutung
First Rule	Die anzuwendende Regel.

Tabelle 2-1: Relevantes Feld in ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***INTERFACES*** ➜ ***EN0-1***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***FIRST RULE*** *none.*
- Belassen Sie alle anderen Einstellungen.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

Hinweis

Wiederholen Sie diesen Schritt für alle Interfaces. In dem Sie die Einstellung ***FIRST RULE*** auf *none* setzen, wird die Regel deaktiviert. Da nun alle Interfaces auf *no access rule* stehen, können Sie beginnen neue Filter zu erstellen ohne Gefahr zu laufen, sich selbst auszusperren.

2 Konfiguration der Access Liste

3 Konfiguration von Filtern

3.1 Den ersten Filter anlegen

- Gehen Sie zu ***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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Description	Beschreibung des Filters.
Protocol	Art des gefilterten Protokolls.
Connection State	Status des Interfaces, auf die der Filter angewendet werden soll.
Source Address	Quelladresse, z.B. ein Netzwerk.
Source Mask	Zugehörige Netzmaske.
Source Port	Der zu filternde Quell-Port.
Destination Address	Zieladresse, z.B. ein Netzwerk.

Feld	Bedeutung
Destination Mask	Zugehörige Netzmaske.
Destination Port	Der zu filternde Ziel-Port.
Specify Port	Portnummer.

Tabelle 3-1: Relevante Felder in ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***FILTER*** ➜ ***ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Tragen Sie unter ***DESCRIPTION*** einen Namen ein, z.B. *Deny-FTP.*
- Wählen Sie unter ***PROTOCOL*** *tcp*.
- Wählen Sie unter ***CONNECTION*** *State any*.
- Tragen Sie als ***SOURCE ADDRESS*** Ihre IP-Adresse ein, z.B. *192.168.10.192*.
- Tragen Sie als ***SOURCE MASK*** Ihre Netzadresse ein, z.B. *255.255.255.128*.
- Wählen Sie unter ***SOURCE PORT*** *any*.
- Wählen Sie unter ***DESTINATION PORT*** *specify range*.
- Wählen Sie unter ***SPECIFY PORT*** *20* ein.
- Tragen Sie unter ***TO PORT*** *21* ein.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

3.2 Einen zweiten Filter anlegen

Gehen Sie zu ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***FILTER*** ➜ ***ADD.***

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

  Description               alles erlauben
  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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Description	Beschreibung des Filters.
Protocol	Art des gefilterten Protokolls.
Connection State	Status des Interfaces, auf die der Filter angewendet werden soll.
Source Address	Quelladresse, z.B. ein Netzwerk.
Source Mask	Zugehörige Netzmaske.
Source Port	Der zu filternde Quell-Port.
Destination Address	Zieladresse, z.B. ein Netzwerk.
Destination Mask	Zugehörige Netzmaske.
Destination Port	Der zu filternde Ziel-Port.

Tabelle 3-2: Relevante Felder in ***SECURITY → ACCESS LISTS → FILTER → ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Tragen Sie unter ***DESCRIPTION*** einen Namen ein, z.B. *alles erlauben*.
- Belassen Sie alle anderen Einstellungen.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

4 Regeln festlegen

4.1 Erste Regel erstellen

- Gehen Sie zu ***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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Action	Auszuführende Aktion.
Filter	Der zu verwendende Filter.

Tabelle 4-1: Relevante Felder in ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***RULES*** ➜ ***ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***ACTION*** *deny M*.
- Wählen Sie unter ***FILTER*** *Deny-FTP*.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

4.2 Zweite Regel erstellen

- Gehen Sie zu ***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                   alles erlauben (2)


                         SAVE                          CANCEL

Use <Space> to select
```

Folgende Felder sind relevant:

Feld	Bedeutung
Insert behind Rule	Nach welcher Regel soll diese Regel angewendet werden.
Action	Auszuführende Aktion.
Filter	Der zu verwendende Filter.

Tabelle 4-2: Relevante Felder in ***SECURITY*** ➜ ***ACCESS LISTS*** ➜ ***RULES*** ➜ ***ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***INSERT BEHIND RULE*** *RI 1 FI 1 (ftp).*
- Wählen Sie unter ***ACTION*** *allow M*.
- Wählen Sie unter ***FILTER*** *alles erlauben.*
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

5 Regeln auf ein Interface anwenden

- Gehen Sie zu ***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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Interface	Auf welches Interface wird die Regel angewandt.
First Rule	Legt fest, welche Regel als erste, auf dieses Interface, angewendet wird.

Tabelle 5-1: Relevante Felder in ***SECURITY ➜ ACCESS LISTS ➜ INTERFACES ➜ EN0-1***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie als ***FIRST RULE*** *RI 1 FI 1 (Deny-FTP)*.
- Belassen Sie alle anderen Einstellungen bei default.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

Gehen Sie zurück ins Hauptmenü und sichern Sie zum Abschluß Ihre neue Konfiguration im Flashmemory mit **EXIT** und **Save as boot configuration and exit**.

5 Regeln auf ein Interface anwenden

6 Ergebnis

Diese Konfiguration stellt sicher, dass am *en0-1* Interface eingehende IP-Pakete mit Source Address *192.168.10.192/25* und Destination Port *20 - 21* verworfen werden. Außerdem ist sichergestellt, dass alle anderen Pakete weitergeleitet werden. Wäre die zweite Rule nicht mit *allow all* gesetzt, würde defaultmäßig ein *deny all* wirksam und damit wäre das Interface für alle eingehenden IP-Pakete gesperrt!

6.1 Test

Unter ***MONITORING AND DEBUGGING*** ➜ ***MESSAGES*** können Sie mitverfolgen, ob die FTP Anfragen geblockt werden.

- Gehen Sie zu ***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
```

Wie zu sehen ist, wurde die Anfrage von der IP-Adresse *192.168.10.253* auf den FTP-Server mit der IP-Adresse *62.146.2.97* geblockt.

6.2 Konfigurationsschritte im Überblick

Feld	Menü	Wert	Pflichtfeld
Description	***SECURITY → ACCESS LIST → FILTER → ADD***	z.B. *Deny-FTP*	
Protocol	***SECURITY → ACCESS LIST → FILTER → ADD***	z.B. *tcp*	Ja
Connection State	***SECURITY → ACCESS LIS T→ FILTER → ADD***	*any*	Ja
Source Address	***SECURITY → ACCESSLIST → FILTER → ADD***	z.B. *192.168.10.192*	Ja
Source Mask	***SECURITY → ACCESS LIST → FILTER → ADD***	z.B. *255.255.255.128*	Ja
Source Port	***SECURITY → ACCESS LIST → FILTER → ADD***	z.B. *any*	Ja
Destination Port	***SECURITY → ACCESS LIST → FILTER → ADD***	*specify range*	Ja
Specify Port	***SECURITY → ACCESS LIST → FILTER → ADD***	z.B. *20 - 21*	Ja
Action	***SECURITY → ACCESS LIST → RULES → ADD***	*deny M*	Ja
Filter	***SECURITY → ACCESS LIST → RULES → ADD***	*Deny-FTP (1)*	Ja
Insert behind Rule	***SECURITY → ACCESS LIST → RULES → ADD***	*RI 1 FI 1 (ftp)*	Ja
Action	***SECURITY → ACCESS LIST → RULES → ADD***	*allow M*	Ja
Filter	***SECURITY → ACCESS LIST → RULES → ADD***	*alles erlauben (2)*	Ja
Interface	***SECURITY → ACCESS LIST → INTERFACES → EN0-1***	*ETH1*	Ja
First Rule	***SECURITY → ACCESS LIST → INTERFACES → EN0-1***	*RI 1 FI 1 (Deny-FTP)*	Ja