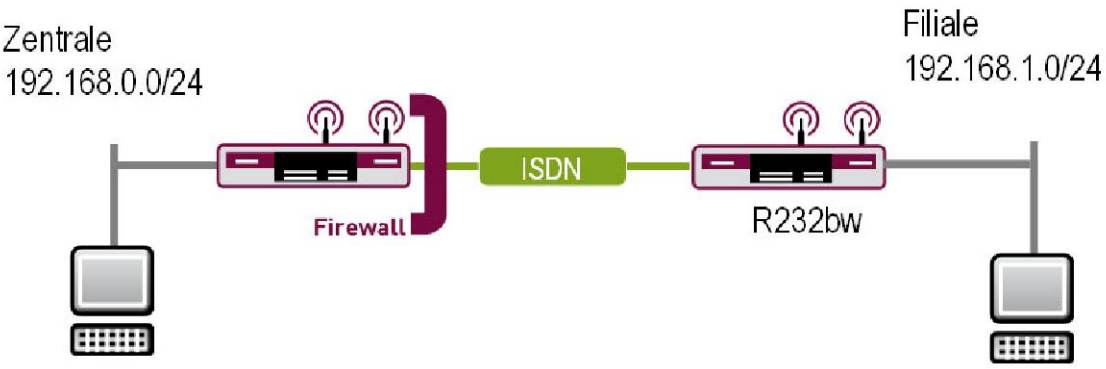
Konfigurationsanleitung
Access Control Lists (ACL)
Funkwerk

13. Oktober 2008 Version 1.0

1. Konfiguration der Access Listen



1.1 Einleitung

Im Folgenden wird die Konfiguration der Access Listen beschrieben. Sie möchten von jedem Rechner in Ihren Netzwerken den Ping benutzten um die Konnektivität zu testen. Zudem wollen Sie in Ihrem zentralen Netzwerk nur Ihren Rechner (192.168.0.2) für den Telnetzugriff auf den lokalen und den entfernten Router erlauben. Zudem Soll von der Filiale aus der Zugriff per Remote Desktop auf einen Zentralrechner (192.168.0.10) erlaubt werden. Nur in der Zentrale sind die Access Listen eingeschaltet.

Zur Konfiguration wird hierbei das Setup-Tool verwendet.

1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Grundkonfiguration des Routers.
- Ein Bootimage ab Version 7.5.1.
- Die Konfiguration erfordert eine LAN Kopplung z.B. über ISDN.

1.3 Konfiguration

Um Access Listen zu konfigurieren, müssen Sie im folgenden Menü Einstellungen vornehmen:

Setup Tool → Security → Access Lists

1.3.1 Filter anlegen

Mit den Filtern definieren Sie, welche Kriterien für das Paket überprüft werden, damit der Filter greift. Gehen Sie in folgendes Menü, um Filter anzulegen:

Setup Tool → Security → Access Lists → Filter → ADD

Zu erst legen Sie den Filter für den Ping an, der von jedem Rechner in alle Netzwerke erlaubt ist. Ping nutzt das Protokoll ICMP in den Datenpaketen:

```
R232bw Setup Tool                          Funkwerk Enterprise Communications GmbH
[SECURITY][ACCESS][FILTER][ADD]                                            r232bw
------------------------------------------------------------------------------

  Description                  PING
  Index

  Protocol  icmp               Type       any

  Source Address
  Source Mask



  Destination Address
  Destination Mask


  Type of Service (TOS)        00000000                  TOS Mask   00000000

                    SAVE                                  CANCEL
------------------------------------------------------------------------------
```

Folgende Punkte sind hier relevant:

Feld	Bedeutung
Description	Geben Sie dem Filter einen Namen
Protocol	Wählen Sie das Protokoll für den Filter aus.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Benennen Sie den Eintrag unter Description **z.B. PING**.
- Wählen Sie als Protocol: **icmp**.

INFO

Die Pakete die auf dem Interface eintreffen, werden nur eingehend von der Firewall überprüft.

Der nächste Filter soll den Zugriff vom internen Rechner per Telnet auf den lokalen und entfernten Router erlauben. Da Ihr Rechner keine Einschränkungen auf bestimmte Telnet Server hat, können Sie das Destination Feld frei lassen:

```
R232bw Setup Tool                     Funkwerk Enterprise Communications GmbH
[SECURITY][ACCESS][FILTER][EDIT]                                        r232bw
------------------------------------------------------------------------------

  Description                 Telnet_Local
  Index                       2

  Protocol  tcp               Connection State    any

  Source Address              192.168.0.2
  Source Mask                 255.255.255.255
  Source Port                 any


  Destination Address
  Destination Mask
  Destination Port            specify
  Specify Port                23
  Type of Service (TOS)       00000000                  TOS Mask  00000000

                    SAVE                                CANCEL

------------------------------------------------------------------------------
Enter string, max length = 48 chars
```

Folgende Punkte sind hier relevant:

Feld	Bedeutung
Description	Geben Sie dem Filter einen Namen.
Protocol	Wählen Sie das Protokoll für den Filter aus.
Source Address	Hier steht die Absender IP-Adresse aus dem Paket
Source Mask	Hier steht die Absender Maske. Muss bei einer einzelnen IP-Adresse immer 32 Bit lang sein.
Destination Port	Wählen Sie einen bestimmten Port oder Range aus.
Specify Port	Tragen Sie den Port oder die Range ein.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Benennen Sie den Eintrag unter Description: **z.B. Telnet_Local**.
- Wählen Sie als Protocol: **tcp**.
- Tragen Sie als Source Address: **z.B. 192.168.0.2** ein.
- Unter Source Mask setzen Sie: **z.B. 255.255.255.255** ein.
- Den Destination Port setzen Sie auf: **specify**.
- Bei Specify Port tragen Sie: **23** ein.

Nach der Konfiguration Ihrer Regeln wird der Zugriff auf den lokalen Router funktionieren. Da allerdings Ihre Filter und Regeln später automatisch auf allen Interfacen aktiv sind, werden die antwort Pakete vom Remote Router nicht mehr durch das eigene Wan-Partner Interface durchgelassen. Legen Sie einen weitern Filter für die Telnet Antwort Pakete in Ihrem Router an:

```
R232bw Setup Tool                          Funkwerk Enterprise Communications GmbH
[SECURITY][ACCESS][FILTER][ADD]                                            r232bw
-------------------------------------------------------------------------------

  Description                 Telnet_Antwort
  Index

  Protocol  tcp               Connection State    any

  Source Address              192.168.1.1
  Source Mask                 255.255.255.255
  Source Port                 specify
  Specify Port                23

  Destination Address         192.168.0.2
  Destination Mask            255.255.255.255
  Destination Port            any

  Type of Service (TOS)       00000000                  TOS Mask  00000000

                    SAVE                                CANCEL
-------------------------------------------------------------------------------
```

Folgende Punkte sind hier relevant:

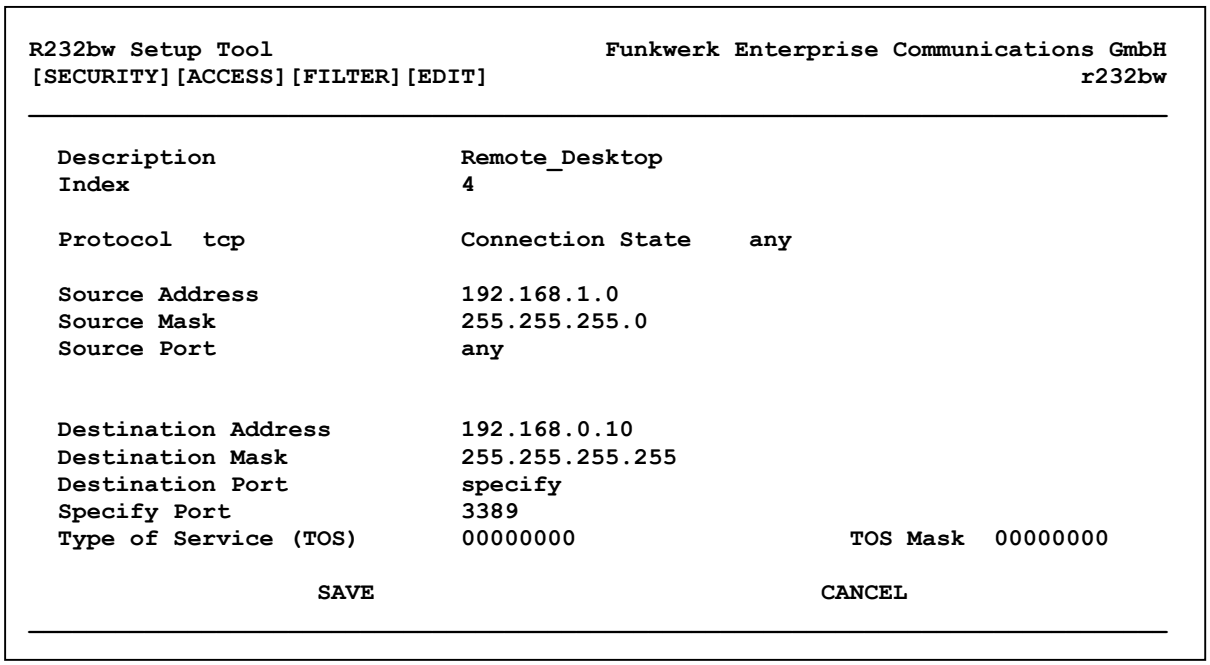
Feld	**Bedeutung**
Description	Geben Sie dem Filter einen Namen.
Protocol	Wählen Sie das Protokoll für den Filter aus.
Source Address	Hier steht die Absender IP-Adresse aus dem Paket.
Source Mask	Hier steht die Absender Maske.
Source Port	Wählen Sie einen bestimmten Port oder Range aus.
Specify Port	Tragen Sie den Port oder die Range ein.
Destination Address	Hier steht die Ziel IP-Adresse aus dem Paket.
Destination Mask	Hier steht die Ziel Maske.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Benennen Sie den Eintrag unter Description: **z.B. Telnet_Antwort**.
- Wählen Sie als Protocol: **tcp**.
- Tragen Sie als Source Address: **z.B. 192.168.1.1** ein.
- Unter Source Mask setzen Sie: **z.B. 255.255.255.255** ein.
- Den Source Port setzen Sie auf: **specify**.

- Bei Specify Port tragen Sie: **23** ein.
- Tragen Sie als Destination Address: **z.B. 192.168.0.2** ein.
- Unter Destination Mask setzen Sie: **z.B. 255.255.255.255** ein.

Der vierte Filter soll die Remote Desktop Verbindungen vom kompletten Filialnetz zum Rechner 192.168.0.10 in der Zentrale erlauben:



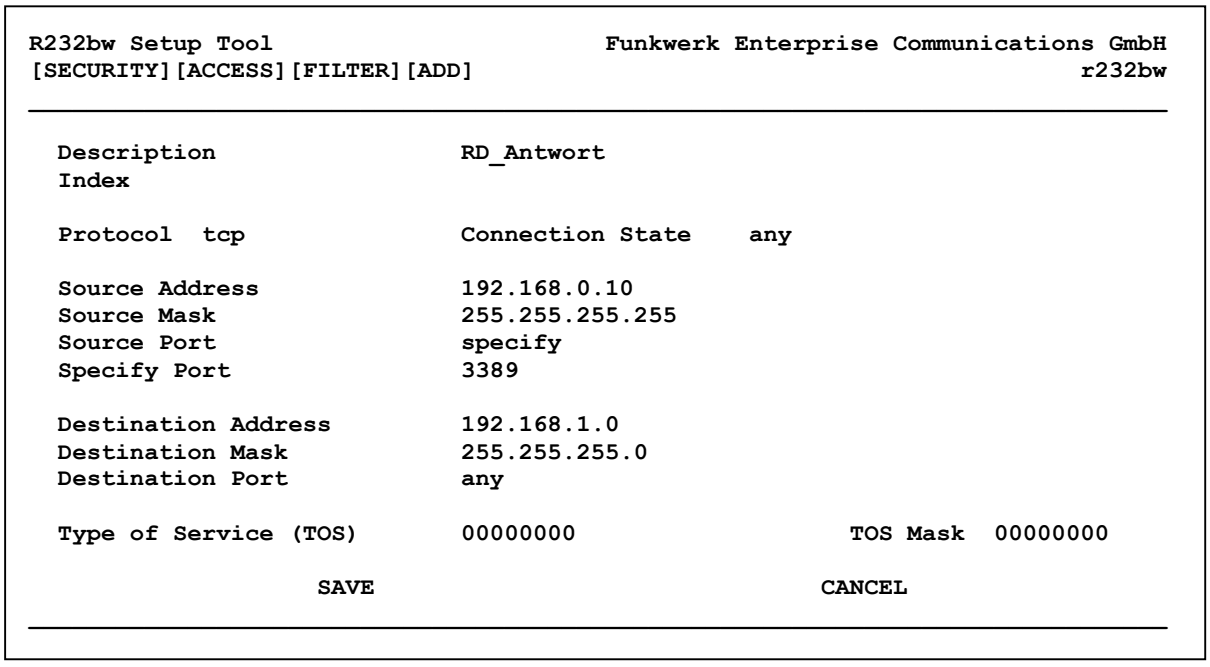
Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
Description	Geben Sie dem Filter einen Namen.
Protocol	Wählen Sie das Protokoll für den Filter aus.
Source Address	Hier steht die Absender IP-Adresse aus dem Paket.
Source Mask	Hier steht die Absender Maske.
Destination Address	Hier steht die Ziel IP-Adresse aus dem Paket.
Destination Mask	Hier steht die Ziel Maske.
Destination Port	Wählen Sie einen bestimmten Port oder Range aus.
Specify Port	Tragen Sie den Port oder die Range ein.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Benennen Sie den Eintrag unter Description: **z.B. Remote_Desktop**.
- Wählen Sie als Protocol: **tcp**.
- Tragen Sie als Source Address: **z.B. 192.168.1.0** ein.
- Unter Source Mask setzen Sie: **z.B. 255.255.255.0** ein.
- Tragen Sie als Destination Address: **z.B. 192.168.0.10** ein.
- Unter Destination Mask setzen Sie: **z.B. 255.255.255.255** ein.
- Den Destination Port setzen Sie auf: **specify**.
- Bei Specify Port tragen Sie: **3389** ein.

Auch bei Remote Desktop werden die Antwortpakete diesmal an der Ethernet Schnittstelle verworfen. Legen Sie einen fünften und letzten Filter an:



Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
Description	Geben Sie dem Filter einen Namen.
Protocol	Wählen Sie das Protokoll für den Filter aus.

Source Address	Hier steht die Absender IP-Adresse aus dem Paket.
Source Mask	Hier steht die Absender Maske.
Source Port	Wählen Sie einen bestimmten Port oder Range aus.
Specify Port	Tragen Sie den Port oder die Range ein.
Destination Address	Hier steht die Ziel IP-Adresse aus dem Paket.
Destination Mask	Hier steht die Ziel Maske.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Benennen Sie den Eintrag unter Description: **z.B. RD_Antwort**.
- Wählen Sie als Protocol: **tcp**.
- Tragen Sie als Source Address: **z.B. 192.168.0.10** ein.
- Unter Source Mask setzen Sie: **z.B. 255.255.255.255** ein.
- Den Source Port setzen Sie auf: **specify**.
- Bei Specify Port tragen Sie: **3389** ein.
- Tragen Sie als Destination Address: **z.B. 192.168.1.0** ein.
- Unter Destination Mask setzen Sie: **z.B. 255.255.255.0** ein.

INFO

Das Anlegen der Filter hat noch keine Auswirkung auf die Firewall. Erst die Konfiguration der ersten Regel bewirkt, dass die Firewall auf allen Interfacen Aktiv ist.

1.3.2 Regeln anlegen

Mit den Regeln definieren Sie, was mit den Paketen gemacht wird, wenn ein Filter greift. Gehen Sie in folgendes Menü, um Regeln anzulegen:

Setup Tool → Security → Access Lists → Rules → ADD

```
R232bw Setup Tool                          Funkwerk Enterprise Communications GmbH
[SECURITY][ACCESS][RULE][ADD]                                              r232bw
------------------------------------------------------------------------------


     Action                    Allow  M

     Filter                    Telnet_Local (2)



                     SAVE                                  CANCEL
------------------------------------------------------------------------------
```

Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
Action	Wählen Sie aus, ob die Pakete zum Filter erlaubt oder verweigert sind.
Filter	Wählen Sie den Filter für die Regel.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

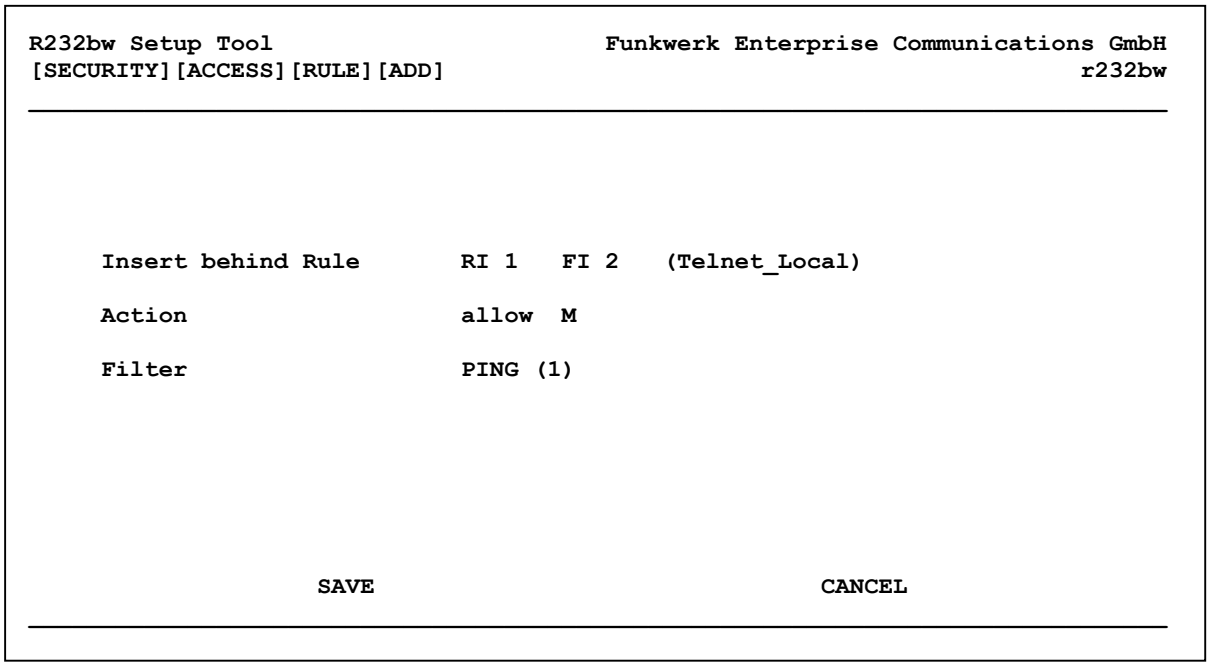
- Wählen Sie bei Action: **Allow M**.
- Bei Filter wählen Sie: **Telnet_Local (2)**.

INFO

Wenn Sie sich nicht als erstes durch den Telnet Filter erlauben fliegen Sie beim abspeichern aus der Telnet Sitzung raus. Alternativ deaktivieren Sie unter Access Lists → Interfaces die Regeln auf dem Ethernet Interface. Wenn Sie rausgeflogen sind, können Sie das Gerät neustarten oder über die serielle Schnittstelle weiter konfigurieren.

Alle weiteren 4 Regeln sind folgendermaßen zu konfigurieren:

Setup Tool → Security → Access Lists → Rules → ADD



Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
Insert behind Rule	Wählen Sie die Regel aus, die unmittelbar vor der Neuen stehen soll.
Action	Wählen Sie aus, ob die Pakete zum Filter erlaubt oder verweigert sind.
Filter	Wählen Sie den Filter für die Regel aus.

Gehen Sie folgendermaßen vor, um die Einträge zu konfigurieren:

- Bei Insert behind Rule markieren Sie: **RI 1 FI 2 (Telnet_Local)**.
- Wählen Sie bei Action: **Allow M**.
- Bei Filter wählen Sie: **PING (1)**.

- Bei Insert behind Rule markieren Sie: **RI 2 FI 1 (PING)**.
- Wählen Sie bei Action: **Allow M**.
- Bei Filter wählen Sie: **Telnet_Antwort (3)**.

- Bei Insert behind Rule markieren Sie: **RI 3 FI 3 (Telnet_Antwort)**.
- Wählen Sie bei Action: **Allow M**.
- Bei Filter wählen Sie: **Remote_Desktop (4)**.

- Bei Insert behind Rule markieren Sie: **RI 4 FI 4 (Remote_Desktop)**.
- Wählen Sie bei Action: **Allow M**.
- Bei Filter wählen Sie: **RD_Antwort (5)**.

INFO

Alle Pakete die nicht durch Filter und regeln erlaubt sind, werden implizit verweigert und somit verworfen.

INFO

Wenn Datenpakete von der Firewall verweigert werden, können Sie das im Debug Modus anhand spezieller Refuse Meldungen erkennen.