1. Konfiguration der Stateful Inspection Firewall

1.1 Einleitung

Im Folgenden wird die Konfiguration der Stateful Inspection Firewall beschrieben.
Es werden Richtlinien erstellt, die nur den Internet Verkehr vom privaten Netzwerk ins Internet erlauben. Dazu zählen die Protokolle HTTP, DNS, POP3 und SMTP die für Webseitenaufrufe und Email Kommunikation benötigt werden. Zusätzlich erlauben Sie von einem Rechner (192.168.1.2) den Zugriff per Telnet auf den Router für die Administration. Alle Rechner haben den Lokalen Router als Standard Gateway und als DNS konfiguriert.

Zur Konfiguration wird hierbei das Setup-Tool verwendet.

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 7.4.4
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang zum Provider
- Ihr LAN wird über die erste Ethernet-Schnittstelle (Ethernet Unit 1) Ihres Routers angeschlossen. Das Internet hat einen WAN-Partner mit dem Namen Provider.

1.3 Konfiguration

Um die Stateful Inspection Firewall zu konfigurieren, muss ausschließlich folgendes Menü konfiguriert werden:

Security -> Stateful Inspection

1.3.1 Einstellungen im Menü Stateful Inspection

```
R232bw Setup Tool                        Funkwerk Enterprise Communications GmbH
[SECURITY][STATEFUL INSPECTION]: Static settings                          r232bw
-------------------------------------------------------------------------------

   Stateful Inspection Firewall global settings:

          Adminstatus     :  enable
          Local Filter    :  disable
          Full Filtering  :  enable
          Logging level   :  all

          Edit Filters >
          Edit Services >
          Edit Addresses >

          Edit Service Groups>
          Edit Interface Groups>        Edit Address Groups>

          Advanced settings >

                     SAVE                                  CANCEL

-------------------------------------------------------------------------------
Use <Space> to select
```

Folgende Punkte sind hier relevant:

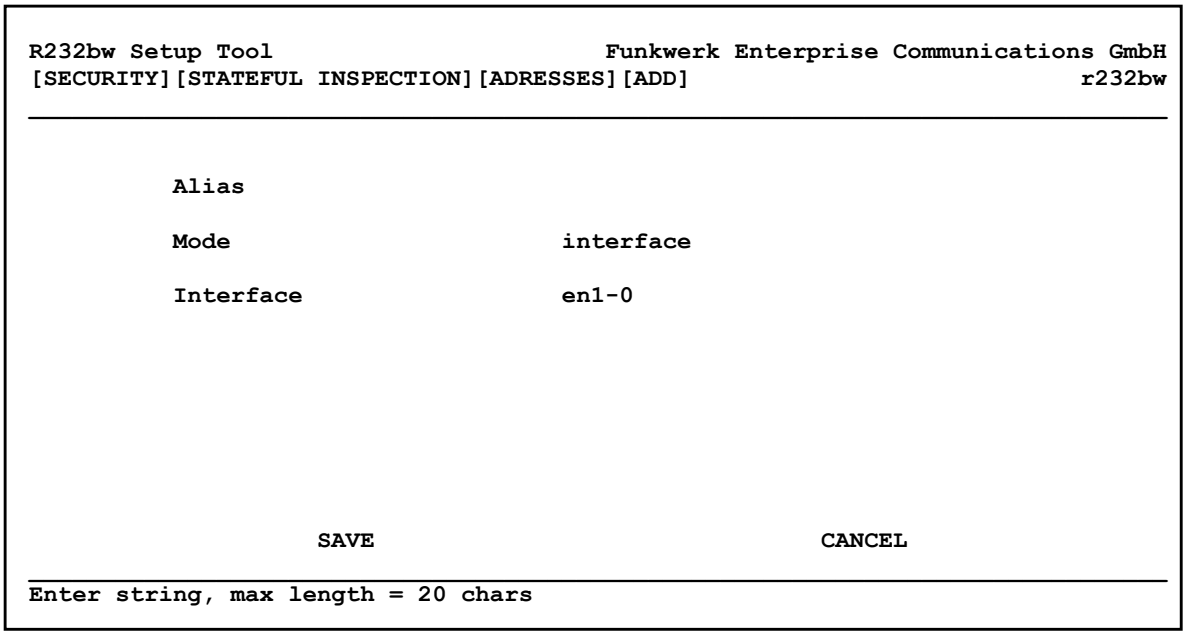
Feld	Bedeutung
Adminstatus	Hier können Sie nach der Konfiguration die Firewall ein und ausschalten.
Edit Filters	Der Zugriff auf bestimmte Dienste von IP-Adressen oder über Interface wird erlaubt oder verweigert.
Edit Services	Mit Angabe von Protokollen und Ports konfigurieren Sie Dienste.
Edit Addresses	Hinterlegen Sie hier Interface oder IP-Adressen für Einschränkungen.
Edit Service Groups	Hier können Sie Dienste gruppieren.
Edit Interface Groups	Hier können Sie Interface gruppieren.
Edit Address Groups	Hier können Sie Adressen gruppieren.

INFO
Die Menüs "Edit Services" und "Edit Addresses" finden Sie auch im Untermenü "Edit Filters" wieder.

1.3.1a Adressen und Interface anlegen

Um Ihre IP-Adressen im LAN und Interface auszuwählen, müssen Sie in folgendem Menü Einträge hinzufügen:

Security -> Stateful Inspection -> Edit Addresses -> ADD



Folgende Punkte sind wichtig:

Feld	Bedeutung
Alias	Hier geben Sie der IP-Adresse oder dem Interface einen Namen, der ausschließlich für die SIF gilt.
Mode	Geben Sie an, ob Sie eine IP-Adresse (oder Range) oder ein Interface hinzufügen möchten.
Interface/ IP-Address	Wählen Sie den WAN Partner aus oder tragen die IP-Adresse ein.

Gehen Sie folgendermaßen vor, um die Rechner IP-Adresse anzulegen:

- Benennen Sie den neuen Eintrag unter Alias: **Rechner**.
- Wählen Sie den Mode **Address/Subnet**.
- Unter IP-Address tragen Sie die IP-Adresse **192.168.1.2** vom Rechner ein.
- IP-Mask bleibt auf: **255.255.255.255**.
- Verlassen Sie das Menü mit: **Save**.
- Verlassen Sie das Menü Edit Addresses mit: **EXIT**.

1.3.1b Service Gruppen anlegen

Gehen Sie in folgendes Menü, um eine Service Gruppe für Ihre Internet Kommunikation anzulegen:

Security -> Stateful Inspection -> Edit Service Groups -> ADD

```
R232bw Setup Tool                     Funkwerk Enterprise Communications GmbH
[SECURITY][STATEFUL INSPECTION][SERVICE GROUPS][EDIT]                   r232bw
------------------------------------------------------------------------------

    Alias Internet

    Configure the Service Group Members

    Service Alias 1           http
    Service Alias 2           http (SSL)
    Service Alias 3           dns
    Service Alias 4           pop3
    Service Alias 5           smtp
    Service Alias 6           echo
    Service Alias 7
    Service Alias 8
    Service Alias 9
    Service Alias 10

                   SAVE                                  CANCEL

------------------------------------------------------------------------------
Enter string, max length = 60 chars
```

Folgende Punkte sind hier relevant:

Feld	Bedeutung
Alias	Hier geben Sie der Gruppe einen Namen.
Service Alias 1 - 10	Wählen Sie hier den Service der Gruppe aus.

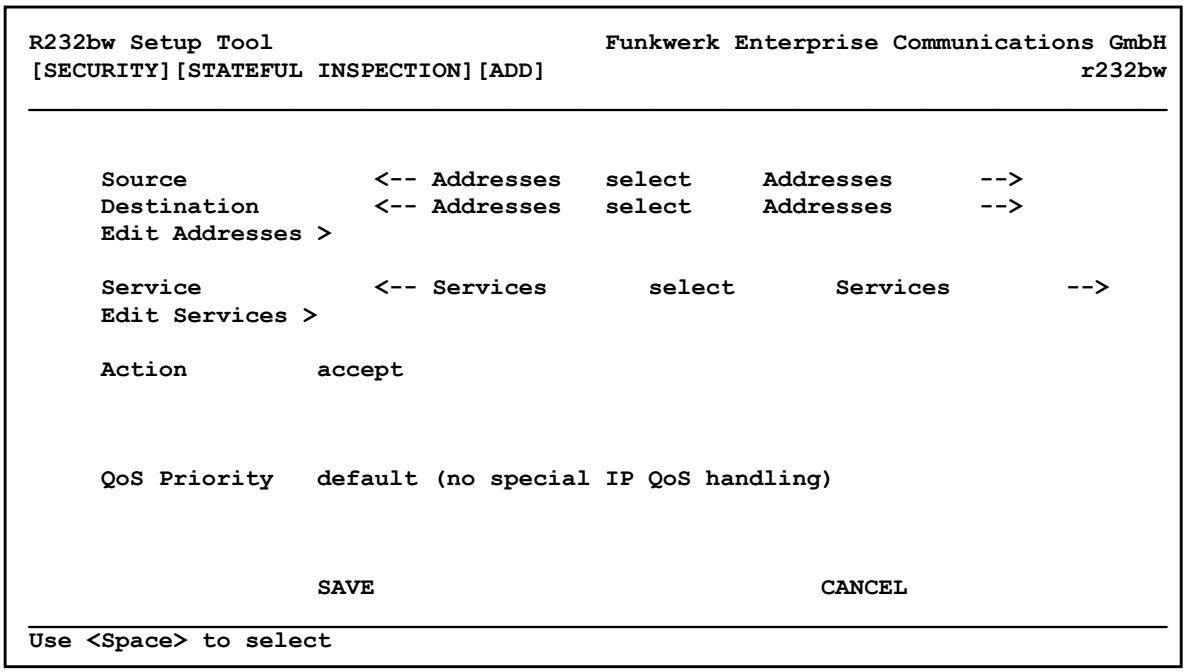
Gehen Sie folgendermaßen vor, um den Eintrag anzulegen:

- Unter Alias vergeben Sie den Namen an: **z.B. Internet**.
- Wählen Sie bei Service 1 – 6 jeweils die Dienste: **http, https, dns, pop3, smtp, echo** aus

1.3.1a Filter anlegen

Gehen Sie in folgendes Menü, um einen Filter anzulegen:

Security -> Stateful Inspection -> Edit Filters -> ADD



Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
Source	Bestimmt, von wo das Paket kommen darf (Absender IP-Adresse oder über ein Interface).
Destination	Bestimmt, wo das Paket hin darf (Ziel IP-Adresse oder über ein Interface).
Service	Hier wählen Sie den Dienst aus, der für den Filter erlaubt oder verweigert wird.
Action	Erlauben (accept) oder verweigern (deny) Sie den Service in dem Filter.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Unter Source wählen Sie das Absender Interface aus: **z.B. LAN_EN1-0**.
- Bei Destination wählen Sie **z.B. WAN_Provider** aus.
- Als Service wählen Sie: **- SERVICE GROUP -Internet**.
- Die Action setzen Sie auf: **accept**.
- Verlassen Sie das Menü mit **SAVE**.

INFO
Sollte der gewünschte Dienst nicht in der Liste auftauchen, können Sie im Menüpunkt "Edit Services" eigene Dienste anlegen. Die Zuordnung geschieht anhand von Protokollen und Ports.

Hinweis:
Alle Pakete die nicht explizit in den Filtern erlaubt sind, sind implizit verweigert.

Sie befinden sich jetzt wieder in der Übersicht von Edit Filters.
Ihr erster Eintrag muss folgendermaßen aussehen:

```
R232bw Setup Tool                    Funkwerk Enterprise Communications GmbH
[SECURITY][STATEFUL INSPECTION][ADD]                                  r232bw
-------------------------------------------------------------------------------
   Stateful Inspection Filter List:

         Press 'u' to move Filter up or press 'd' to move Filter down.

  Pos. Source              Destination         Service              Action
     1 LAN_EN1-0           WAN_PROVIDER        internet             accept









     ADD                 DELETE              SAVE                 CANCEL
-------------------------------------------------------------------------------
```

1.3.1b Weitere Filter anlegen

Alle Pakete die auf das LAN_EN0-1 Interface eintreffen und über das Internet Interface wollen, werden durchgelassen. Da Sie den Router als DNS Eingetragen haben und Ihn bei der Namensauflösung Fragen, müssen Sie einen neuen Filter erstellen der es uns erlaubt, den Router über das Ethernet Interface anzusprechen. Ein weiterer Filter den Sie anlegen ist der Telnet Zugriff vom Rechner mit der IP 192.168.1.2 auf den Router.

Gehen Sie in folgendes Menü um den Filter für DNS anzulegen:

Security -> Stateful Inspection -> Edit Filters -> ADD

- Wählen Sie als Source: **LAN_EN1-0** aus.
- Wählen Sie als Destination: **Local** aus.
- Bei Service stellen Sie: **DNS** ein.
- Action bleibt auf: **accept**.
- Verlassen Sie das Menü mit **SAVE**

Gehen Sie in folgendes Menü um den Filter für Telnet anzulegen:

Security -> Stateful Inspection -> Edit Filters -> ADD

- Wählen Sie als Source: **Rechner** aus.
- Wählen Sie als Destination: **Local** aus.
- Bei Service stellen Sie: **Telnet** ein.
- Action bleibt auf: **accept**.
- Verlassen Sie das Menü mit **SAVE**

Nachdem Sie Ihre Filter angelegt haben können Sie in folgendem Menü den Adminstatus auf **enabled** setzen um die Firewall zu aktivieren:

Security -> Stateful Inspection

1.4 Ergebnis

Sie haben die Stateful Inspection Firewall mit 3 Filtern konfiguriert und eingeschaltet. Filter 1 erlaubt den Zugriff vom internen Netz auf das Internet mit den gebräuchlichen Protokollen. Filter 2 erlaubt den internen Rechnern die DNS Anfrage an den Router zu schicken. Filter 3 gewährt dem Rechner den Zugriff zum Router per Telnet.

1.5 Kontrolle

Um die Firewall Einstellungen zu testen gehen Sie folgendermaßen vor:

- Telnet vom Rechner auf den Router muss funktionieren.
- Telnet von evtl. anderen vorhandenen Rechnern auf den Router darf nicht funktionieren.
- Geben Sie in Ihrem Browser www.funkwerk-ec.com ein um die Homepage von Funkwerk aufzurufen.
- Ein PING von einem Rechner zum Router darf nicht beantwortet werden.

INFO
Im DEBUG Modus an der Shell des Routers hinterlässt die Firewall Meldungen über erlaubte und verweigerte Verbindungen.

1.6 Konfigurationsschritte im Überblick

Feld	Menü	Wert
Alias	Security > Stateful Inspection > Edit Addresses > ADD	z.B. Rechner
Mode	Security > Stateful Inspection > Edit Addresses > ADD	Address/Subnet
IP-Address	Security > Stateful Inspection > Edit Addresses > ADD	Rechner IP-Adresse z.B. 192.168.1.2
Alias	Security > Stateful Inspection > Edit Service Groups > ADD	z.B. Internet
Service Alias 1 – 6	Security > Stateful Inspection > Edit Service Groups > ADD	http, https, dns, pop3, smtp, echo
Source	Security > Stateful Inspection > Edit Filters > ADD	LAN_EN1-0
Destination	Security > Stateful Inspection > Edit Filters > ADD	WAN_Provider
Service	Security > Stateful Inspection > Edit Filters > ADD	-- Service Group -- Internet
Action	Security > Stateful Inspection > Edit Filters > ADD	accept
Source	Security > Stateful Inspection > Edit Filters > ADD	LAN_EN1-0
Destination	Security > Stateful Inspection > Edit Filters > ADD	Local
Service	Security > Stateful Inspection > Edit Filters > ADD	DNS
Action	Security > Stateful Inspection > Edit Filters > ADD	accept
Source	Security > Stateful Inspection > Edit Filters > ADD	Rechner
Destination	Security > Stateful Inspection > Edit Filters > ADD	Local
Service	Security > Stateful Inspection > Edit Filters > ADD	Telnet
Action	Security > Stateful Inspection > Edit Filters > ADD	accept
Adminstatus	Security > Stateful Inspection	enable