# 1 Firewall-Regelsätze verwenden

Dokument-ID: 108402_de_00
Dokument-Bezeichnung: AH DE MGUARD FIREWALL RULESETS 1


Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

**Inhalt dieses Dokuments**

In diesem Dokument wird die Verwendung von Firewall-Regelsätzen beschrieben. Das Anlegen von Firewall-Regeln wird dadurch vereinfacht und beschleunigt.



## 1.1 Einleitung

Einzelne Firewall-Regeln können in Regelsätzen zusammengefasst werden. Diese Regelsätze können anschließend in Firewall-Regeln als Aktion ausgewählt und somit zur Anwendung gebracht werden.

### 1.1.1 Beispiel

Der externe Zugriff auf drei bestimmte Server im internen Netzwerk über die Netzwerkdienste *ftp*, *telnet* und *https* soll erlaubt werden. Der Zugriff auf alle übrigen Dienste und Netzwerkadressen aus dem externen Netz (WAN) soll verboten werden.

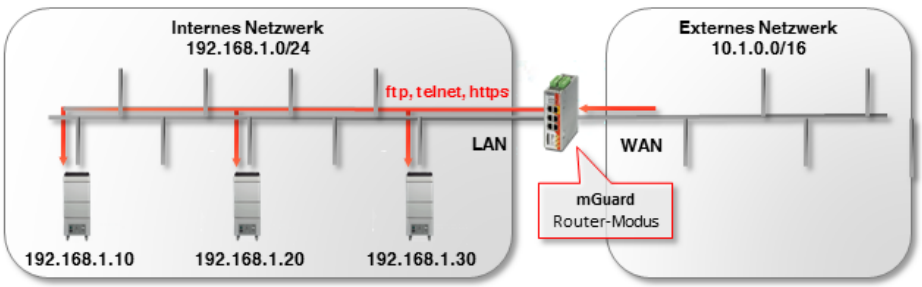


Bild 1-1 Zugriff auf spezielle Dienste auf bestimmten Servern erlauben

**Problem**

Ohne Regelsätze müssten neun Firewall-Regeln in einer Firewall-Tabelle angelegt werden: jeweils drei für jeden Dienst bzw. jede Server-IP-Adresse.

**Lösung**

Mithilfe von Regelsätzen können bestimmte Teilregeln, d. h. die Server-IP-Adressen oder die Netzwerkdienste, in Regelsätzen zusammengefasst werden. Diese können dann in Firewall-Tabellen als Aktion ausgewählt werden.

In diesem Beispiel reichen drei Eingangsregeln in der Firewall-Tabelle aus, um ausschließlich den Zugriff auf die drei Server und die drei Netzwerkdienste zu erlauben. Dazu muss **wahlweise** ein Regelsatz „*Server*“ oder ein Regelsatz *Service* angelegt werden (siehe „Beispiel 1 (Regelsatz: „Server“)“ und „Beispiel 2 (Regelsatz „Service“)“).

Bitte beachten Sie: Wenn eine Verbindung, die zu einem Firewall-Regelsatz passt, aufgebaut worden ist und diese Verbindung kontinuierlich Datenverkehr erzeugt, dann kann es sein, dass das Deaktivieren des Firewall-Regelsatzes diese Verbindung nicht wie erwartet unterbricht (siehe mGuard-Firmwarehandbuch).

### 1.1.2 Vorgehen

Um den Zugriff auf definierte Server und Netzwerkdienste zuzulassen, sind folgende Arbeitsschritte notwendig:

1. Firewall-Regelsatz anlegen.
2. Firewall-Regeln in Firewall-Tabelle anlegen und auf den Regelsatz verweisen.

## 1.2 Beispiel 1 (Regelsatz: „Server“)

Um den Regelsatz anzulegen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des mGuard-Geräts an.
2. Gehen Sie zu **Netzwerksicherheit >> Paketfilter >> Regelsätze**.
3. Legen Sie einen neuen Regelsatz mit dem Namen *Server* an und klicken Sie auf das Icon *Zeile bearbeiten*.
4. Konfigurieren Sie den Regelsatz gemäß Bild 1-2.

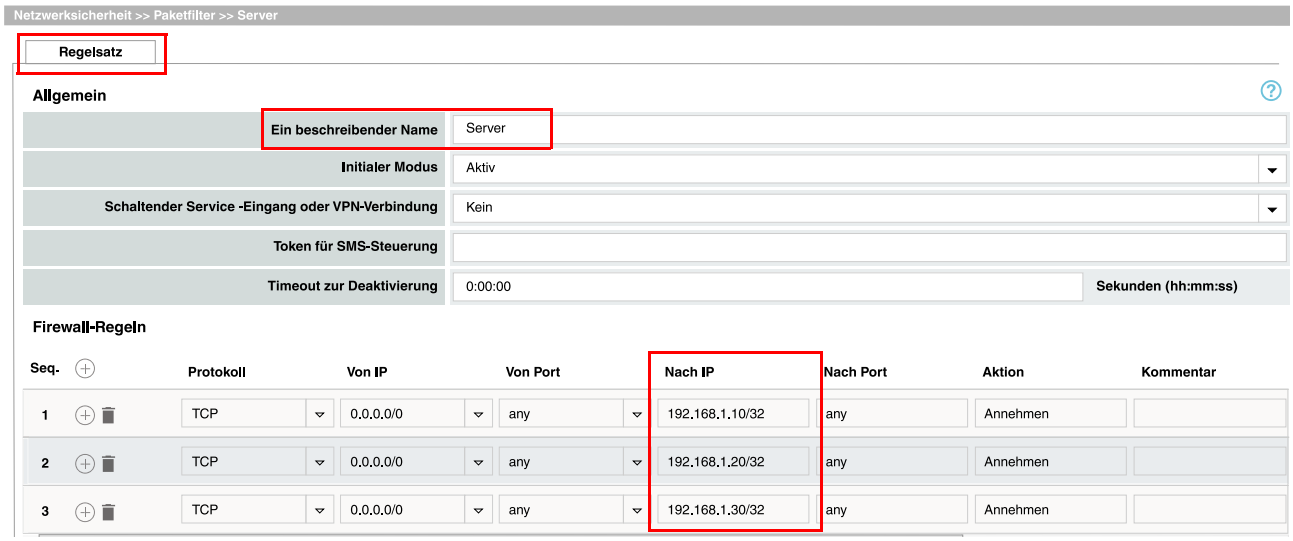


Bild 1-2 Im **Regelsatz** *Server* werden die zugelassenen Ziel-IP-Adressen (Ziel-Server) zusammengefasst.

Um den Regelsatz in einer Firewall-Regel anzuwenden, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des mGuard-Geräts an.
2. Gehen Sie zu **Netzwerksicherheit >> Paketfilter >> Eingangsregeln**.
3. Wählen Sie **Wende das unten angegebene Regelwerk an** aus.
4. Legen Sie drei Firewall-Regeln gemäß Bild 1-3 an.

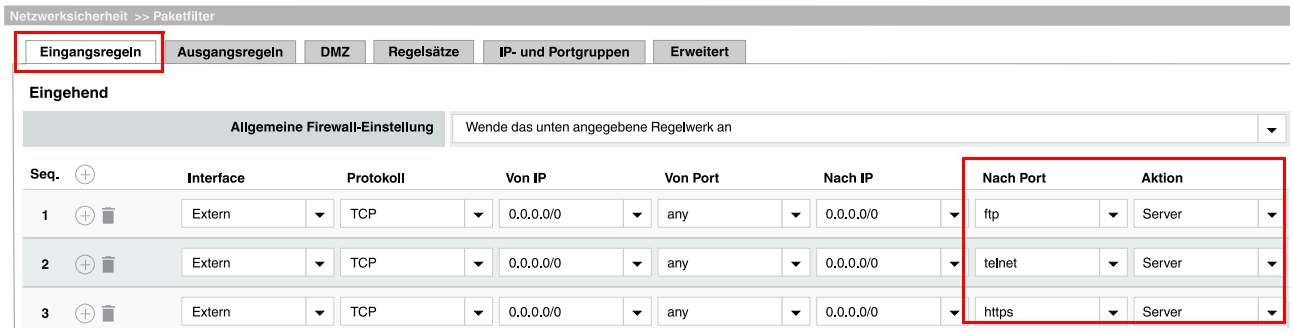


Bild 1-3 In der **Firewall-Tabelle** wird bei Zugriffen auf die angegebenen Netzwerkdienste als Aktion auf den Regelsatz *Server* verwiesen.

Die Firewall-Regeln definieren den Zugriff auf spezifische Netzwerkdienste (*Nach Port*) und verweisen auf den Regelsatz *Server*. In diesem wird der Zugriff auf die Ziele definiert.

## 1.3 Beispiel 2 (Regelsatz „Service“)

Anstatt die Server-IP-Adressen können Sie auch die Netzwerkdienste in einem Regelsatz zusammenfassen und diesen in den Firewall-Regeln anwenden. Die Einstellungen sind wie folgt (siehe Bild 1-4 und Bild 1-5).

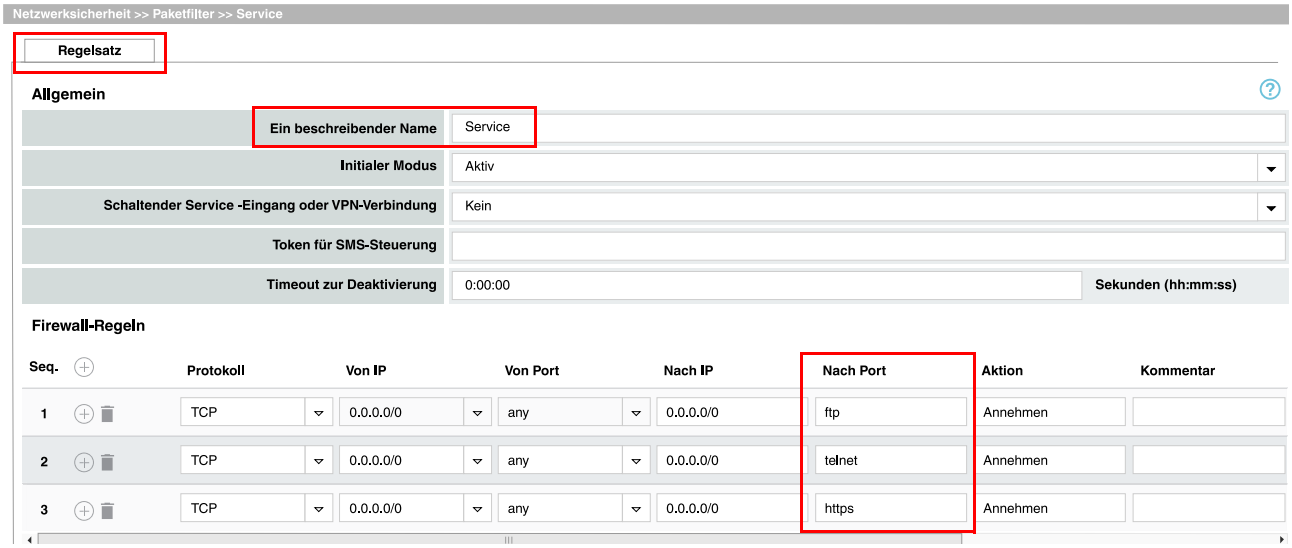


Bild 1-4 Im **Regelsatz** *Service* werden die erlaubten Netzwerkdienste zusammengefasst.

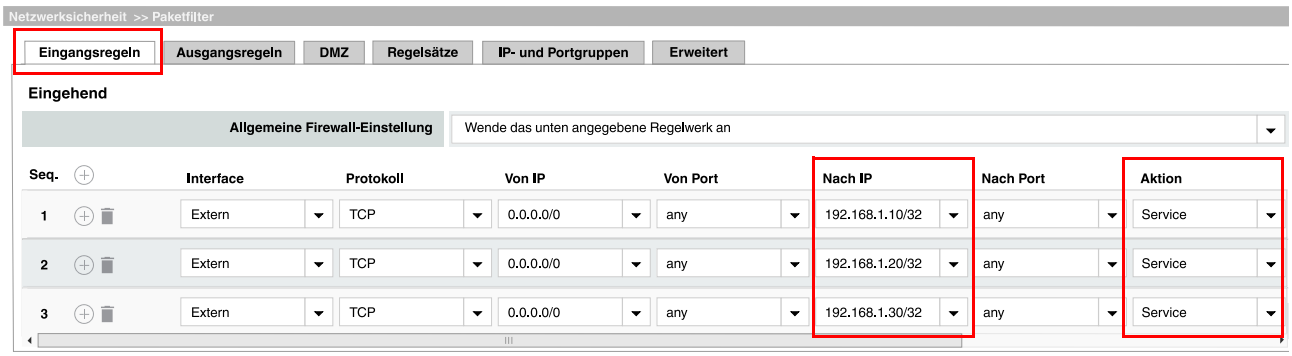


Bild 1-5 In der **Firewall-Tabelle** wird bei Zugriffen auf die angegebenen Ziel-IP-Adressen (Ziel-Server) als Aktion auf den **Regelsatz** *Service* verwiesen.

Die Firewall-Regeln definieren den Zugriff auf spezifische Ziel-IP-Adressen (*Nach IP*) und verweisen auf den Regelsatz *Service*. In diesem wird der Zugriff auf die erlaubten Netzwerkdienste definiert.