1 Häufige Fehler bei der Erstellung von Firewall-Regeln

Dokument-ID: 108403_de_00
Dokument-Bezeichnung: AH DE MGUARD FIREWALL MISCONFIG

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 werden häufige Fehler bei der Erstellung von Firewall-Regeln beschrieben (z. B. falsche Reihenfolge, falscher Quellport).

1.1 Einleitung

Die mGuard-Firewall funktioniert als dynamischer Paketfilter, der ein- und ausgehende Netzwerkpakete nach konfigurierten Regeln analysiert (siehe auch Kapitel 1, „Eigenschaften und Anwendungsmöglichkeiten der mGuard-Firewall“).

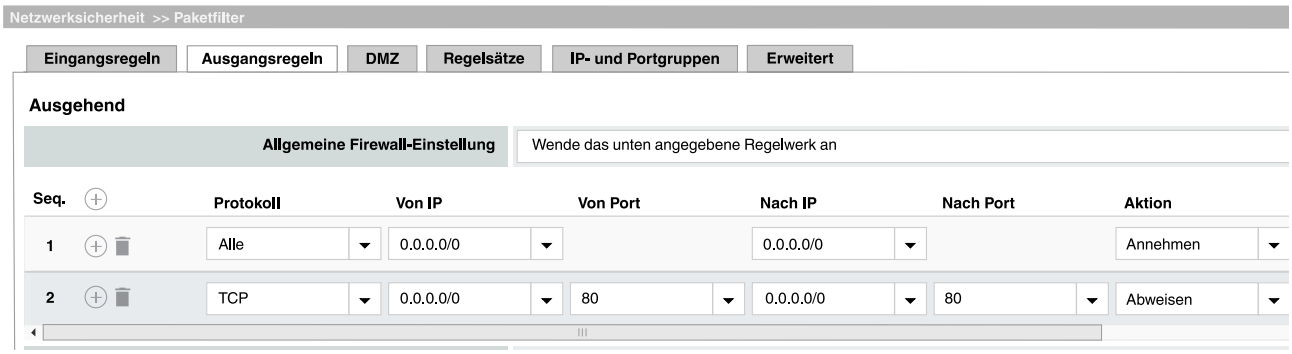
Häufiger Fehler: Entscheidend beim Anlegen von Firewall-Regeln in einer Tabelle ist deren Reihenfolge. Die in der Tabelle angelegten Firewall-Regeln werden nacheinander von oben nach unten geprüft. Wenn eine Regel zutrifft, wird die angegebene Aktion (*Annehmen, Verwerfen* oder *Abweisen)* ausgeführt und die nachfolgenden Regeln werden **nicht mehr** berücksichtigt.

1.1.1 Beispiel

Der Zugriff auf HTTP-Webserver aus dem internen Netzwerk soll mithilfe konfigurierter Firewall-Regeln unterbunden werden (mGuard-Menü: **Netzwerksicherheit >> Paketfilter >> Ausgangsregeln**).

Spezifizierte Ports (*Von Port* und *Nach Port*) werden nur berücksichtigt, wenn das Protokoll auf TCP oder UDP eingestellt ist.

1.2 Falsche Konfiguration



Fehler 1: Falsche Reihenfolge

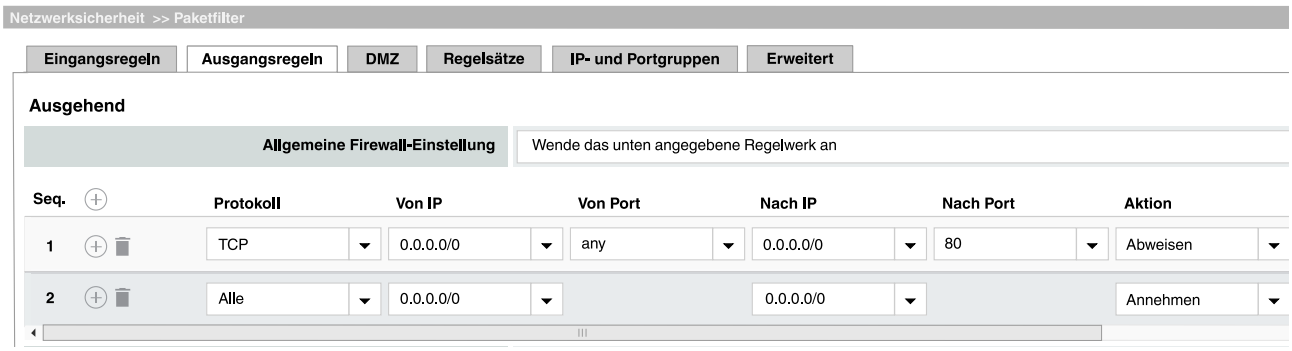
Da die erste Regel in Reihe 1 bereits für alle Paket zutrifft, werden die nachfolgenden Regeln nicht mehr überprüft. Eine ausgehende TCP-Verbindung auf Port 80 wird also nicht abgelehnt.

Fehler 2: Falscher Quellport

HTTP-Anfragen von Webbrowsern verwenden einen variierenden Quellport größer oder gleich 1024. Die Anfragen werden an Port 80 gesendet. Die angelegte Regel in Reihe 2 wird aufgrund des eingetragenen Quellports (*Von Port* = 80), also kleiner 1024, nicht zutreffen.

1.3 Richtige Konfiguration

In der richtigen Konfiguration muss die Reihenfolge der Firewall-Regeln so geändert werden, dass zuerst die Regel, die Zugriffe auf einen Webserver abweist, geprüft wird.



Als Quellport (*Von Port)* kann z. B. *any* angegeben werden, um die Anfragen eines Standard-Webbrowsers zu prüfen. Mit der Angabe des Zielports (*Nach Port* = 80) wird der Zugriff auf einen Webserver abgewiesen.

Wenn die erste Regel **zutrifft**, wird die zweite Regel nicht mehr beachtet. Wenn die erste Regel **nicht zutrifft**, erlaubt die zweite Regel den ausgehenden Datenverkehr.