1 Benutzerfirewall verwenden, um den Zugriff auf ein externes Netzwerk zu erlauben

Dokument-ID: 108401_de_00

Dokument-Bezeichnung: AH DE MGUARD USERFIREWALL 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 beschrieben, wie einem Firewall-Benutzer mithilfe von Benutzerfirewall-Regeln der Zugriff aus dem internen auf ein externes Netzwerk erlaubt wird.

1.1 Einleitung 1
1.2 Firewall-Benutzer anlegen 3
1.3 Benutzerfirewall-Template erstellen 4
1.4 Als Firewall-Benutzer anmelden 7

Eine Benutzerfirewall steht auf Geräten der RS2000-Serie und dem mGuard Blade-Controller nicht zur Verfügung.

1.1 Einleitung

Die Benutzerfirewall erlaubt es, benutzerspezifische Firewall-Regeln zu definieren, die nur für angelegte Firewall-Benutzer oder Benutzergruppen gelten.

Benutzerfirewall-Regeln haben Vorrang vor an anderer Stelle konfigurierten Firewall-Regeln (z. B. *Eingangsregeln/Ausgangsregeln*) und setzen diese ggf. außer Kraft.

Der Zugriff auf das Ziel wird dabei nicht auf der Grundlage von statisch konfigurierten Firewall-Regeln erlaubt, sondern dynamisch nach Anmeldung des Firewall-Benutzers mittels dem Firewall-Benutzer zugeordneten Benutzerfirewall-Regeln.

1.1.1 Beispiel

Die Netzwerkanbindung des Produktionsnetzwerks (Intern) an das Unternehmensnetzwerk (Extern) wird in diesem Beispiel mittels NAT (IP-Maskierung) ermöglicht (siehe auch Kapitel 1.4.1, „Option 1: Maskierung / IP-Masquerading“).

Gleichzeitig werden jedoch **alle Zugriffe** aus der Produktion auf das Unternehmensnetzwerk durch eine allgemeine Firewall-Regel (Ausgangsregel) verboten.

Mithilfe der Benutzerfirewall erhalten nun die Firewall-Benutzer *pwerner* und *hpotter* individuellen Zugriff auf Webserver und können somit auf die Webserver im Unternehmensnetzwerk zugreifen.

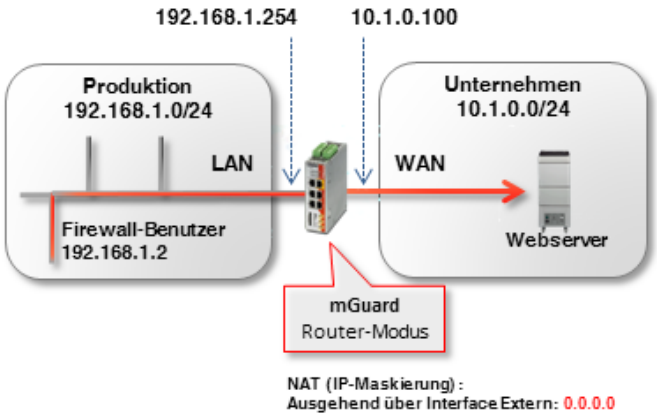

Bild 1-1 Firewall-Benutzer mit Zugriffsrechten auf HTTP(S)-Webserver

1.1.2 Vorgehen

Um den Zugriff auf einen Webserver über Port 80 (http) und 443 (https) für die Firewall-Benutzer *pwerner* und *hpotter* zu erlauben, sind folgende Arbeitsschritte notwendig:

1. Firewall-Benutzer anlegen
2. Benutzerfirewall-Template mit Firewall-Regeln erstellen
3. Benutzerfirewall aktivieren
4. Als Firewall-Benutzer anmelden

1.2 Firewall-Benutzer anlegen

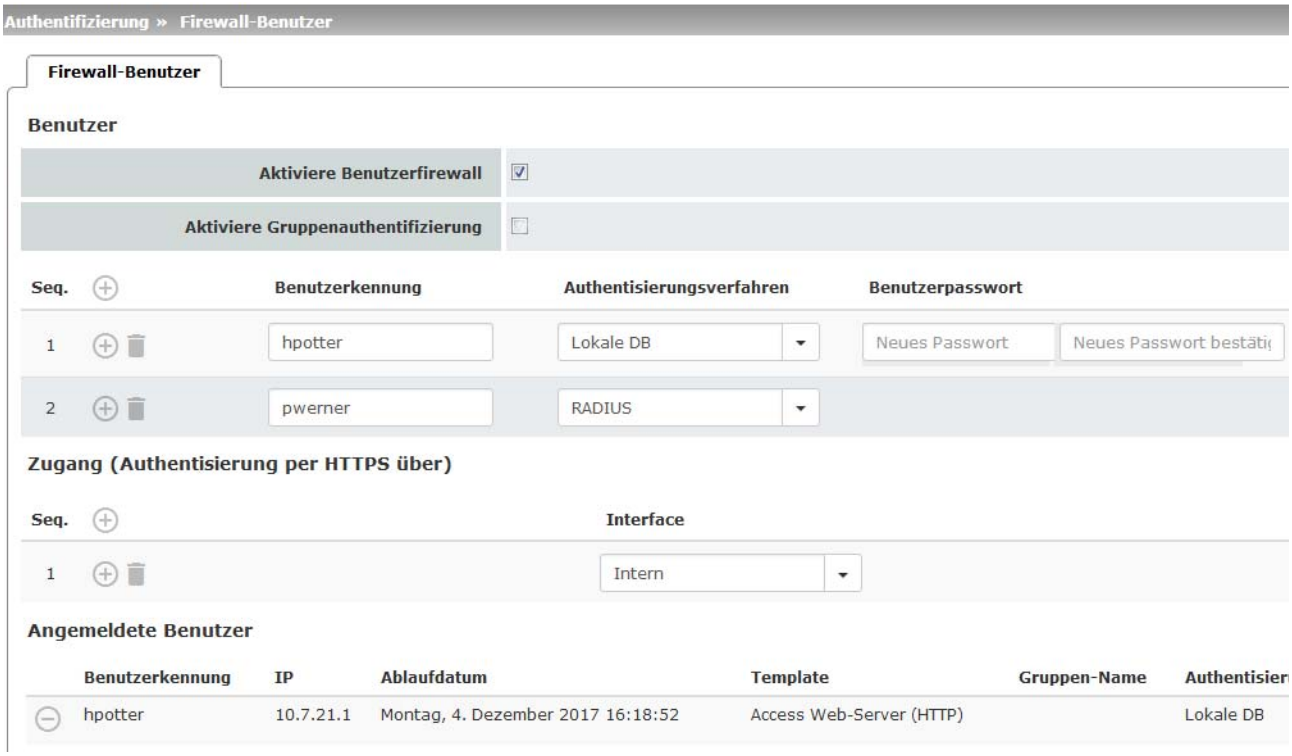

Bild 1-2 Firewall-Benutzer anlegen

Firewall-Benutzer werden unter **Authentifizierung >> Firewall-Benutzer** angelegt. Dort wird ebenfalls festgelegt, ob der Nutzer über einen RADIUS-Server oder ein lokal auf dem mGuard-Gerät konfiguriertes Benutzerpasswort authentifiziert wird.

Die allgemeine Konfiguration zur Verwendung eines RADIUS-Servers durch das mGuard-Gerät erfolgt im Menü **Authentifizierung >> RADIUS**.

Ein Firewall-Benutzer kann einem oder mehreren Benutzerfirewall-Templates zugeordnet werden (siehe „Registerkarte „Template-Benutzer““ auf Seite 5).

Um einen Firewall-Benutzer anzulegen, gehen Sie wie folgt vor (siehe auch mGuard-Firmwarehandbuch):

1. Melden Sie sich auf der Weboberfläche des mGuard-Geräts an.
2. Gehen Sie zu **Authentifizierung >> Firewall-Benutzer**.
3. Erstellen Sie die gewünschten Firewall-Benutzer.
4. Geben Sie jeweils das Authentisierungsverfahren für den Benutzer an (Password oder RADIUS-Server).
5. Geben Sie an, über welche Interfaces sich Firewall-Benutzer am mGuard-Gerät anmelden dürfen.

1.3 Benutzerfirewall-Template erstellen

In einem Benutzerfirewall-Template werden Firewall-Regeln erstellt und bereits existierenden Firewall-Benutzern zugewiesen.

Wenn ein Benutzerfirewall-Template oder eine Firewall-Regel eines Templates hinzugefügt, geändert, gelöscht oder deaktiviert wird, sind sofort alle eingeloggten Firewall-Benutzer betroffen.

Bestehende Verbindungen werden unterbrochen. Eine Ausnahme bildet die Änderung von Benutzerfirewall-Regeln, wenn unter **Netzwerksicherheit >> Paketfilter >> Erweitert** die Funktion „Bestehende Verbindungen nach Änderungen an der Firewall zurücksetzen“ deaktiviert ist. In diesem Fall wird eine Netzwerkverbindung, die aufgrund einer vorher erlaubten Regel besteht, nicht unterbrochen.

Wenn ein Firewall-Regelsatz (Template) **deaktiviert** und anschließend **aktiviert** wird, müssen sich betroffene eingeloggte Firewall-Benutzer zunächst ausloggen und dann wieder einloggen, um die Firewall-Regeln aus dem Template erneut für sich zu aktivieren.

Um ein Benutzerfirewall-Template zu erstellen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des mGuard-Geräts an.
2. Gehen Sie zu **Netzwerksicherheit >> Benutzerfirewall**.
3. Legen Sie ein neues Template an und klicken Sie auf das Icon *Zeile bearbeiten*.

1.3.1 Registerkarte „Allgemein“

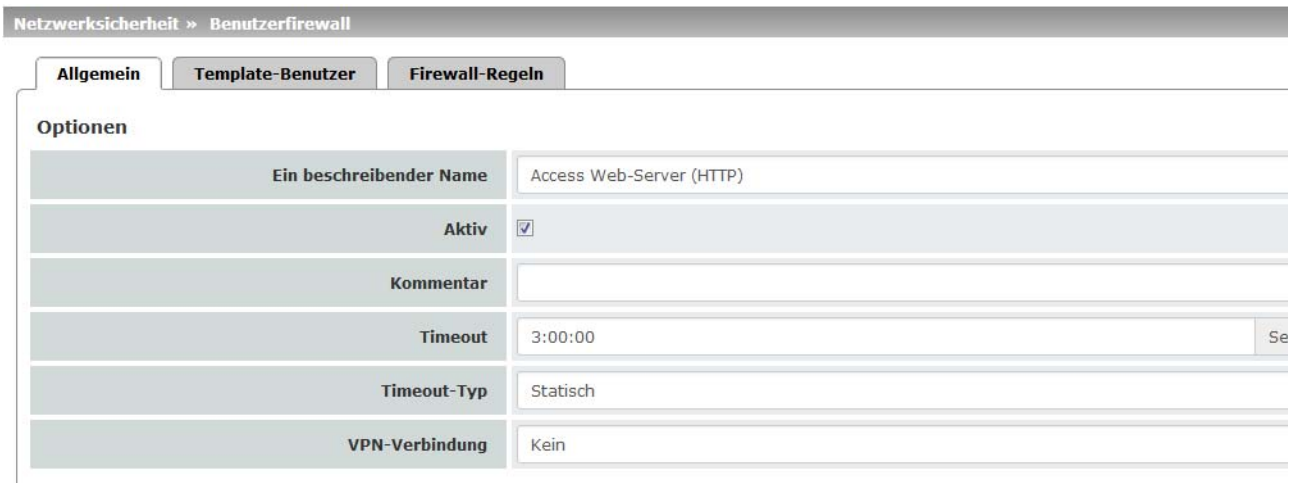

Bild 1-3 Benutzerfirewall-Template erstellen: Registerkarte *Allgemein*

Gehen Sie wie folgt vor (siehe auch mGuard-Firmwarehandbuch):

- Geben Sie dem Benutzerfirewall-Template einen beschreibenden Namen.
- Geben Sie an, wie lange eine Benutzerfirewall-Regel gültig sein soll, nachdem sich ein Firewall-Benutzer angemeldet hat (Timeout-Typ beachten).
- Wenn die Regeln des Benutzerfirewall-Templates ausschließlich in einer bestimmten VPN-Verbindung gültig sein sollen, geben Sie diese an.

1.3.2 Registerkarte „Template-Benutzer“

Bild 1-4 Benutzerfirewall-Template erstellen: Registerkarte *Template-Benutzer*

Gehen Sie wie folgt vor (siehe auch mGuard-Firmwarehandbuch):

- Geben Sie die Namen der Firewall-Benutzer an, für die die Regeln dieses Benutzerfirewall-Templates gelten sollen.

Die angegebenen Benutzer müssen unter **Authentifizierung >> Firewall-Benutzer >> Benutzer** definiert und angelegt werden (siehe „Firewall-Benutzer anlegen“ auf Seite 3).

ACHTUNG: Es wird nicht überprüft, ob die angegebenen Benutzernamen tatsächlich existieren. Achten Sie unbedingt auf die korrekte Schreibweise der Namen.

1.3.3 Registerkarte „Firewall-Regeln“

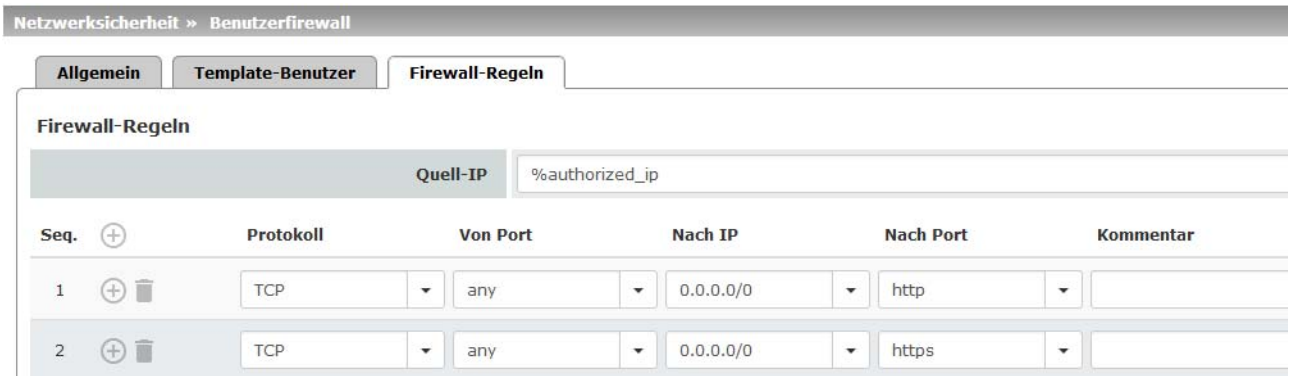

Bild 1-5 Benutzerfirewall-Template erstellen: Registerkarte *Firewall-Regeln*

Das Gerät erkennt automatisch, über welches Interface der Login erfolgt ist und wendet das Benutzerfirewall-Template entsprechend als Eingangs- (Anmeldung aus dem externen Netzwerk) oder Ausgangsregel (Anmeldung aus dem internen Netzwerk) an.

Wenn das Template mit dynamischem Timeout konfiguriert ist, setzen an dieser Stelle zugelassene UDP- und andere Netzwerkpakete (außer ICMP) den dynamischen Timeout auf den Ausgangswert zurück.

Um die Firewall-Regeln des Templates zu konfigurieren, gehen Sie wie folgt vor (siehe auch mGuard-Firmwarehandbuch):

- Geben Sie eine Quell-IP-Adresse an, von der aus Verbindungen zugelassen sind.

Wenn %authorized_ip angegeben ist, werden die Firewall-Regeln auf Datenpakete angewendet, die von der gleichen Quell-IP-Adresse gesendet wurden, von der aus sich der Benutzer angemeldet hat. Datenpakete von anderen IP-Adressen werden verworfen .

Wenn eine IP-Adresse angegeben wird, werden die Firewall-Regeln auf Datenpakete angewendet, die von dieser Quell-IP-Adresse gesendet wurden. Datenpakete von anderen IP-Adressen werden verworfen. Diese Option sollte z. B. verwendet werden, wenn sich ein Administrator am Gerät anmeldet, um die Benutzer-Firewall für einen Techniker zu aktivieren, der auf einem anderen Rechner arbeitet.

- Legen Sie Firewall-Regeln an, um den zugeordneten Firewall-Benutzern den Zugriff entsprechend der angelegten Regeln zu erlauben.

  In diesem Beispiel der Zugriff auf beliebige Webserver über die Netzwerkdienste *http* und *https*.

1.4 Als Firewall-Benutzer anmelden

Ein Firewall-Benutzer muss sich via Webbrowser per HTTPS auf der Weboberfläche des mGuard-Geräts anmelden, um die Firewall-Regeln zu aktivieren. Dies kann sowohl vom internen als auch vom externen Netzwerk aus (oder über VPN, DMZ und Einwahl) erfolgen. Um sich über das externe Netzwerk am Gerät anzumelden, muss der HTTPS-Fernzugriff auf dem mGuard-Gerät aktiviert sein (Menü **Verwaltung >> Web-Einstellungen >> Zugriff**).

Das Gerät erkennt automatisch, über welches Interface der Login erfolgt ist und wendet das Benutzerfirewall-Template entsprechend als *Eingangsregeln* (Anmeldung aus dem externen Netzwerk) oder *Ausgangsregel* (Anmeldung aus dem internen Netzwerk) an.

Um sich als Firewall-Benutzer anzumelden, gehen Sie wie folgt vor:

1. Öffnen Sie das Anmeldefenster auf der Weboberfläche des mGuard-Geräts.
2. Wählen Sie die Zugangsart „Benutzerfirewall“.
3. Geben Sie die Benutzerkennung und das Passwort des Firewall-Benutzers an.
4. Eine erfolgreiche Anmeldung wird im Anmeldefenster angezeigt.

Ergebnis

Alle Verbindungen zu einem HTTP(S)-Webserver über das ausgewählte Protokoll sind nach Anmeldung des Firewall-Benutzers bis zum Ablauf des Timeouts erlaubt.