1 Eigenschaften und Anwendungsmöglichkeiten der mGuard-Firewall

Dokument-ID: 108405_de_00
Dokument-Bezeichnung: AH DE MGUARD FIREWALL

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 die grundlegende Funktionsweise der mGuard-Firewall sowie verschiedene Anwendungsmöglichkeiten beschrieben.

1.1 Stateful-Packet-Inspection-Firewall

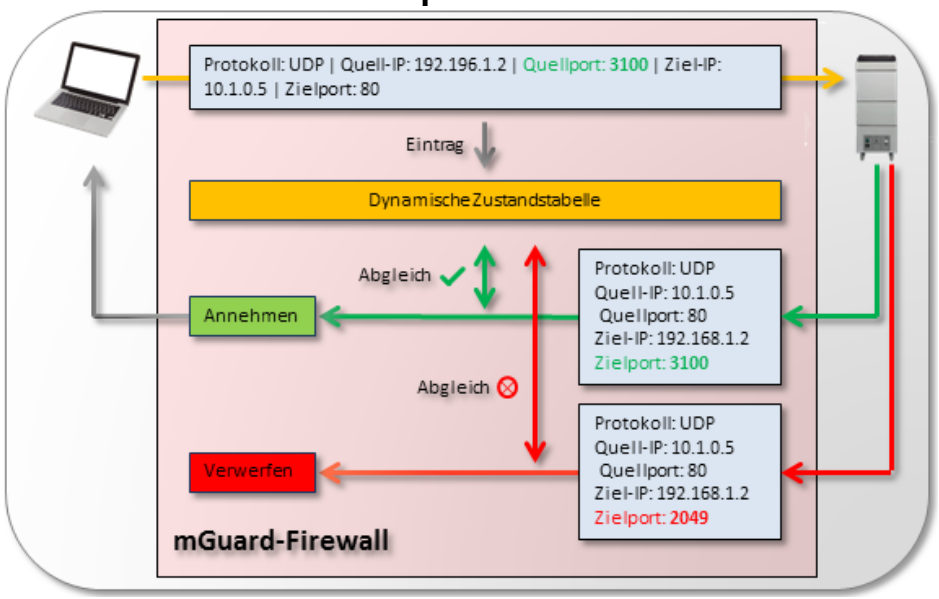

Bild 1-1 Passieren ein- oder ausgehende Pakete die mGuard-Firewall (oranger Pfeil), werden ihre Eigenschaften (z. B. Protokoll, Absender-IP/Port, Ziel-IP/Port) in einer dynamischen Zustandstabelle gespeichert. Die Eigenschaften des zu erwartenden Antwortpakets werden ebenfalls gespeichert, damit auch dieses durch die Firewall gelangt. Antwortpakete werden dann mit den Werten der Zustandstabelle verglichen. Entsprechen die Pakete den dynamisch eingetragenen Werten der Zustandstabelle, werden sie angenommen (grüner Pfeil). Stimmen sie nicht überein, werden die Pakete verworfen (roter Pfeil).

Die mGuard-Firewall funktioniert als dynamischer Paketfilter (*Stateful-Packet-Inspection-Firewall*), der ein- und ausgehende Netzwerkpakete nach konfigurierten Regeln analysiert.

Durch die dynamische Paketfilterung können Antwortpakete die eingehende Firewall automatisch passieren, wenn die Antwortpakete zweifelsfrei der Anfrage zugeordnet werden können, die zuvor die ausgehende Firewall passiert hat.

Die Konfiguration von Eingangsregeln, um Antworten auf ausgehende Anfragen zu akzeptieren, ist deshalb grundsätzlich nicht erforderlich. Tatsächlich könnte eine Eingangsregel so konfiguriert sein, dass sie alle eingehenden Pakete verwirft. Eingehende Antworten auf Anfragen würden trotzdem angenommen.

1.2 Statische Firewall

Mithilfe von statischen Firewall-Regeln werden Zugriffe auf der Grundlage von Netzwerken (IP-Adressen, Protokolle und Ports) geregelt.

Diese Regeln sind statisch und für die ausgewählten Interfaces immer aktiv, nachdem sie angelegt wurden. D. h. bestimmte Geräte/Netzwerke können miteinander kommunizieren.

(**Beispiel**: siehe Kapitel 1.3, „Firewall-Regeln konfigurieren“)

1.3 Dynamisch aktivierte Firewall (über Firewall-Regelsätze)

Firewall-Regeln, die in Firewall-Regelsätzen zusammengefasst sind, können dynamisch aktiviert oder deaktiviert werden. Die Aktivierung/Inaktivierung erfolgt wahlweise über

– die Weboberfläche,
– eine SMS,
– einen Schalter/Taster,
– den Aufbau einer VPN-Verbindung.

Wie bei statischen Firewall-Regeln werden die Zugriffe auf der Grundlage von Netzwerken (IP-Adressen, Protokolle und Ports) geregelt. Die Regeln sind aber nur bei Bedarf aktiv.

(**Beispiel „Firewall-Regelsatz“**: siehe Kapitel 1, „Firewall-Regelsätze verwenden“)

1.4 Benutzerfirewall

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.

Eine Benutzerfirewall-Regel tritt dann in Kraft, wenn sich ein der Regel zugeordneter Firewall-Benutzer über die Weboberfläche des mGuard-Geräts anmelden. Die Authentifizierung erfolgt über die interne Datenbank oder einen RADIUS-Server.

(**Beispiel**: siehe Kapitel 1, „Benutzerfirewall verwenden, um den Zugriff auf ein externes Netzwerk zu erlauben“)