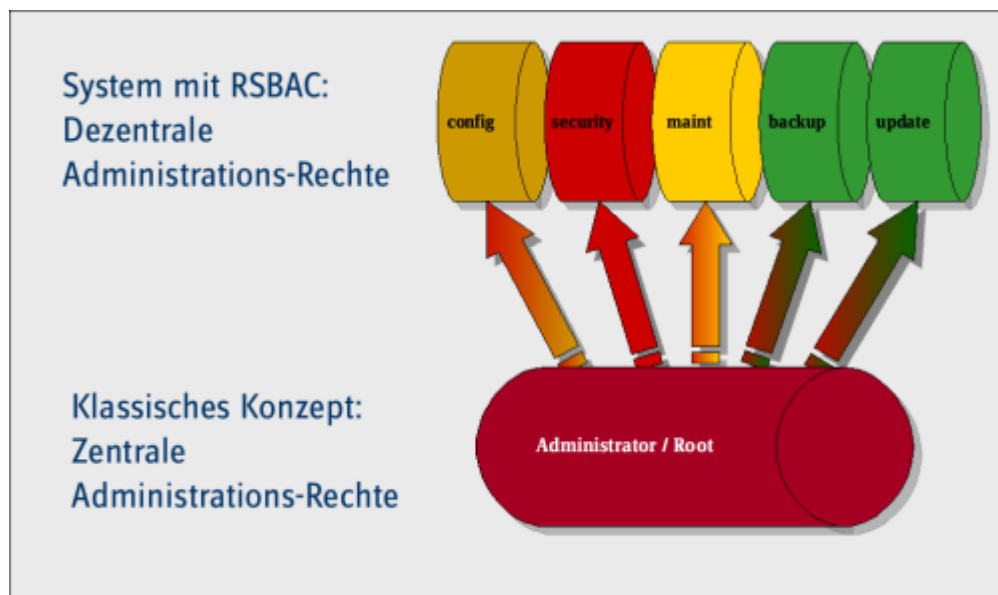


# Das Administrationskonzept der mp-Firewall

Die mp-Firewall hat speziell vordefinierte Benutzerrollen, die den herkömmlichen Administrator (root) ersetzen. Die großen Vorteile dieses dezentralen Administrationskonzeptes ist einerseits der Schutz des Administrationsaccount vor einer funktional unangemessen Allmacht<sup>1)</sup>. Andererseits wird durch die funktionale Aufteilung der einzelnen Administrationaufgaben eine Delegation der Aufgaben möglich. Zu den speziellen Rechten der einzelnen Administrationsrollen vergleichen Sie bitte die [Übersicht der Rollenrechte](#). Grundsätzlich lässt sich eine Unterteilung der Administrationsrollen in folgende Bereiche vornehmen:



## 1. Der Netzwerk-Bereich

Für die Systemadministration der mp-Firewall wurde die Rolle *config* geschaffen. Sie ist zuständig für die Netzwerkeinstellungen und allgemeine Systemvorgaben. Keinen Zugriff hingegen hat diese Administrationsrolle auf Benutzerverzeichnisse und Benutzereinstellungen. Damit ist ein Outsourcing der Wartungsaufgaben für das Netzwerk datenschutzrechtlich unbedenklich.

## 2. Der personenbezogene Bereich

Für diesen Administrationsbereich ist die Rolle *maint* vorgesehen. Diesem Administrationsaccount obliegt es, die Benutzerzugänge/E-Mailkonten der mp-Firewall zu pflegen. Es können Konten angelegt, Mailvorgaben gesetzt, Zugangsberechtigungen und -einschränkungen vorgenommen und Passwörter geändert werden. Dieser Administrator hat keine Möglichkeit einer inhaltlichen Kontrolle der Benutzerverzeichnisse und -daten.

## 3. Der Wartungs-Bereich

Für Wartungsaufgaben der mp-Firewall wurden die Rollen *backuser* und *update* vorgesehen. Sie haben nur einen sehr begrenzten Funktionsumfang und speziell definierte Rechte. Dabei ist der *backuser* ausschließlich für das Erstellen und Rücksichern von Backups und die dafür notwendigen Einstellungen verantwortlich. Gleiches gilt für die Rolle *update* bei der Pflege des Systems. Beide Rollen haben weder Zugriff auf die Netzwerkeinstellung noch dürfen sie Benutzerverzeichnisse einsehen.

## 4. Der Sicherheits-Bereich

Die zentrale Sicherheit der mp-Firewall wird über den Zugriffsrechterschutz RSBAC gewährleistet. Die RSBAC-Konfiguration ist bei Auslieferung komplett und sollte nicht von Benutzern verändert werden. Zur Bearbeitung der RSBAC-Sicherheitseinstellungen gibt es die Rollen *security* und *root*.

1)

Die herkömmliche Konzentration aller Administrationsaufgaben und Systemrechte in einem zentralen Account macht diesen besonders gefährlich; gelingt es Hackern an dieser Stelle einzudringen, haben sie Zugriff auf das gesamte System.

From:

<https://help.m-privacy.de/> -

Permanent link:

<https://help.m-privacy.de/doku.php/tightgate-firewall:administrationskonzept>

Last update: **2026/05/11 07:45**

