Kommandozeile, Inbetriebnahme, Firewall, Ports, Installation, Aktualisierung

firewalld konfigurieren

Ab Version 6.0 verwendet der UCware Server *firewalld* als Frontend des im Grundsystem enthaltenen Paketfilters. Damit können Sie den Netzwerk-Schnittstellen der Telefonanlage geeignete Richtlinien für den jeweils erforderlichen Sicherheitsgrad zuweisen. Diese lassen sich bei Bedarf um individuelle Regeln ergänzen.

Sie können *firewalld* per SSH bzw. über die Kommandozeile aufrufen:

```
sudo firewall-cmd OPTION [OPTION...]
```

Hinweis:
Eine vollständige Übersicht möglicher Optionen finden Sie auf der Website von *firewalld*.

Manuelle Einstellungen gelten stets bis zum Neustart des Dienstes, sofern sie nicht mit der Option `–permanent` ausgeführt werden. Auf diese Weise können Sie eine Konfiguration zunächst testen und im Zweifelsfall wie folgt zurücksetzen:

```
sudo firewall-cmd --reload
```

Falls Sie den Dienst nicht benötigen, können Sie Ihn dauerhaft ausschalten:

```
sudo systemctl disable firewalld
```

Voreingestellte Richtlinien

Firewalld fasst die erforderlichen Richtlinien für unterschiedliche Nutzungsszenarien in sogenannten Zonen zusammen. Eine Netzwerk-Schnittstelle arbeitet in genau einer Zone und unterliegt dabei den zugehörigen Richtlinien. Systemweit lässt sich eine Standardzone für alle nicht explizit zugewiesenen Schnittstellen definieren.

Nach einer Neuinstallation sind die folgenden Zonen verfügbar:

Name	Beschreibung
drop	Verwirft alle eingehenden Verbindungen.
block	Weist alle eingehenden Verbindungen zurück.
external	Zur Anwendung auf Routern bzw. zur Network Address Translation.
dmz	Erlaubt eingehende Verbindungen über SSH.
public	Erlaubt eingehende Verbindungen über SSH, mDNS und DHCP. Dies ist die voreingestellte Standard-Zone.
work	Erlaubt eingehende Verbindungen über SSH, mDNS, IPP und DHCP.
home	Erlaubt eingehende Verbindungen über SSH, mDNS, IPP, DHCP und SMB.
internal	Entspricht **home**.
trusted	Erlaubt alle Verbindungen.

Hinweis:
Einzelheiten zur Konfiguration der voreingestellten Zonen finden Sie auf der Website von *firewalld*.

Wenn eine der voreingestellten Zonen für Ihr Nutzungsszenario ausreicht, müssen Sie lediglich die Anweisungen im letzten Abschnitt dieses Artikels ausführen.

Wenn keine der voreingestellten Zonen zu Ihrem Nutzungsszenario passt, haben Sie zwei Möglichkeiten:

- Sie können eine eigene Zone mit geeigneten Richtlinien erstellen. Dies ist nur für Anwendungsszenarien mit komplexen Richtlinien sinnvoll. Lesen Sie dazu die Dokumentation des Herstellers.
- Sie können die Richtlinie einer vorhandenen Zone um eigene Regeln für ausgewählte Services und/oder Ports ergänzen. Eine Kurzanleitung dazu finden Sie im Abschnitt Zone für UCware vorbereiten.

Standardzone anzeigen und ändern

UCware empfiehlt, eine Zone mit strengstmöglichen Richtlinien als systemweiten Standard zu verwenden und alle vorhandenen Netzwerk-Schnittstellen in vertrauenswürdigeren Zonen arbeiten zu lassen. Auf diese Weise stellen Sie sicher, dass neu hinzugefügte Schnittstellen automatisch der höchsten erforderlichen Sicherheitstufe unterliegen. Wenn die herstellerseitig als Standard definierte Zone `public` diese Ansprüche nicht erfüllt, müssen Sie den `default`-Status einer anderen Zone zuweisen.

Hinweis:
Wenn Sie eine neue default-Zone festlegen, werden die zugehörigen Regeln sofort angewandt:

- auf alle Schnittstellen, die **keiner** Zone zugewiesen sind
- auf alle Schnittstellen, die der ursprünglichen default-Zone zugewiesen waren

Um den systemweiten Standard festzulegen, gehen Sie wie folgt vor:

1. Zeigen Sie die vorhandenen Zonen und ihre aktuelle Konfiguration an:

```
sudo firewall-cmd --list-all-zones
```

2. Weisen Sie den Status `default` bei Bedarf einer anderen Zone zu:

```
sudo firewall-cmd --set-default-zone=block
```

Zone für UCware vorbereiten

Die folgende Anleitung geht von einem konkreten Beispiel aus. Dabei wird die Richtlinie der voreingestellten Zone `public` um weitere Regeln ergänzt. Passen Sie die Bezeichnung der Zone sowie die freigegebenen Services und Ports an Ihr eigenes Anwendungsszenario an.

1. Wählen Sie aus den vorhandenen Zonen eine geeignete aus und zeigen Sie ihre aktuellen Einstellungen an:

```
sudo firewall-cmd --zone=public --list-all
```

Hinweis:
Die Ausgabe listet nur solche Services und Ports auf, die von der voreingestellten Richtlinie der Zone abweichen.

2. Um darüber hinaus weitere Services freizugeben, fügen Sie diese einzeln oder als Liste hinzu:

```
sudo firewall-cmd --zone=public --add-service=https
```

```
sudo firewall-cmd --zone=public --add-service={ntp,https,sips}
```

Dadurch werden die Standard-Ports der jeweiligen Services freigegeben.

3. Um darüber hinaus weitere Ports und/oder Portbereiche freizugeben, fügen Sie diese einzeln oder als Liste hinzu:

```
sudo firewall-cmd --zone=public --add-port=8088/tcp
```

```
sudo firewall-cmd --zone=public --add-port={8088/tcp,10000-20000/udp}
```

4. Zeigen Sie die neuen Einstellungen der Zone mit `--list-all` an und prüfen Sie diese.

5. Um nicht benötigte Services oder Ports zu entfernen, verwenden Sie statt `--add` die Option `--remove`.

Alle bisherigen Schritte wirken sich nur temporär aus und lassen sich mit `sudo firewall-cmd --reload` zurücksetzen. Um die Einstellungen dauerhaft auf eine Netzwerk-Schnittstelle anzuwenden, führen Sie die Schritte im nächsten Abschnitt aus.

Netzwerk-Schnittstelle zuweisen

1. Verschieben Sie die gewünschte Netzwerk-Schnittstelle aus ihrer aktuellen in die neue Zone :

```
sudo firewall-cmd --zone=[ZONE] --change-interface=[SCHNITTSTELLE]
```

Dadurch werden alle voreingestellten und manuell hinzugefügten Regeln der neuen Zone **temporär** auf die verschobene Schnittstelle angewandt.

2. Übernehmen Sie Ihre temporären Änderungen dauerhaft:

```
sudo firewall-cmd --runtime-to-permanent
```

3. Testen Sie die Funktionen des UCware Servers mit dem UCC-Client und/oder angeschlossenen Tischtelefonen.