SUSE

Einführung in `firewalld`

WAS?

Erfahren Sie mehr über `firewalld`, ein wichtiges Werkzeug zum Schützen von Linux-Servern und -Diensten. Es handelt sich dabei um den standardmäßigen und primären Netzwerkverteidigungsmechanismus bei vielen modernen Distributionen. Die Funktionen der intuitiven zonenbasierten Verwaltung und der dynamischen Konfiguration ermöglichen eine präzise Steuerung des Netzwerkverkehrs ohne Dienstunterbrechung.

WARUM?

`firewalld` ist unerlässlich, da es eine moderne, dynamische und benutzerfreundliche Möglichkeit zum Verwalten der Netzwerksicherheit auf Linux-Systemen bietet, indem komplexe Firewall-Regeln in intuitive Zonen und Dienste abstrahiert werden.

AUFWAND

Es dauert bis zu 30 Minuten, diesen Artikel zu lesen.

ZIEL

Die Sicherheit eines Linux-Systems effektiv verwalten und erhöhen.

ANFORDERUNGEN

- `sudo`- oder `root`-Rechte, da `firewalld`-Befehle – insbesondere die, die dauerhafte Änderungen an den Firewall-Regeln vornehmen – erhöhte Rechte erfordern.
- `firewalld` ist die Standard-Firewall bei vielen modernen Linux-Distributionen. Wenn sie auf Ihrem System nicht vorinstalliert ist, müssen Sie das `firewalld`-Paket installieren.
- Grundlegende Kenntnisse hinsichtlich des Linux-Terminals sind unerlässlich.

Veröffentlicht: 11.12.2025

Inhalt

1 Informationen zu `firewalld`

`firewalld` ist ein dynamischer Firewall-Verwaltungsdienst, der eine flexible und effiziente Möglichkeit zum Steuern des Netzwerkverkehrs auf Linux-Systemen bietet. Er ermöglicht Änderungen, ohne vorhandene Verbindungen zu unterbrechen. Die Verwendung von `firewalld` bietet folgende Vorteile:

- *Dynamische Konfiguration:* Wenden Sie Änderungen sofort an, ohne vorhandene Verbindungen zu unterbrechen.
- *Benutzerfreundliche Oberfläche:* Zonen und Dienste vereinfachen komplexe Firewall-Regeln.
- *Abstraktion:* Es besteht keine Notwendigkeit, `nftables`-Regeln für häufige Szenarien direkt zu ändern.
- *Dauerhafte Konfiguration:* Einfache Verwaltung von Regeln, die bei Neustarts beibehalten werden.
- *Dauerhafte Konfiguration:* Standardmäßig wird von `firewalld` ein `deny-all`-Prinzip verwendet, indem der gesamte eingehende Datenverkehr blockiert wird, sofern er nicht ausdrücklich zugelassen wurde.

1.1 `firewalld`-Zonen

Eine Firewall-Zone ist ein vordefinierter Satz aus Regeln, die vorgeben, wie eingehender und ausgehender Netzwerkverkehr für eine bestimmte Netzwerkschnittstelle oder Quell-IP-Adresse behandelt wird. Jede Zone stellt eine andere Vertrauensstufe für das Netzwerk dar, dem sie zugeordnet ist. Sie können je nach Ursprung der Netzwerkverbindung unterschiedliche Sicherheitsrichtlinien anwenden.

Zonen sind wie Sicherheitsprofile. Sie möchten beispielsweise für eine öffentliche WLAN-Verbindung und Ihr geschütztes Heimnetzwerk unterschiedliche Firewall-Regeln anwenden. Mithilfe von `firewalld`-Zonen können Sie diese unterschiedlichen Regelsätze definieren und entsprechend anwenden. Eine Netzwerkverbindung unterliegt den Regeln von nur einer `firewalld`-Zone. Eine `firewalld`-Zone kann viele Netzwerkschnittstellen oder Quell-IP-Adressen haben.

Im Verzeichnis `/usr/lib/firewalld/zones/` sind die vordefinierten Zonen gespeichert. Beispiel:

```
> /usr/lib/firewalld/zones ls
```

```
block.xml  dmz.xml  docker.xml  drop.xml  external.xml  home.xml  internal.xml  nm-
shared.xml  public.xml  trusted.xml  work.xml
```

Einige der Standardeinstellungen der vordefinierten Zonen lauten wie folgt:

`drop`

- *Vertrauensstufe:* Absolut nicht vertrauenswürdig.
- *Verhalten:* Alle eingehenden Netzwerkpakete werden ohne Antwort entfernt. Es sind nur ausgehende Verbindungen zulässig, die vom System initiiert wurden. Dies ermöglicht einen „heimlichen“ Modus, in dem das System für externe Angreifer nicht vorhanden zu sein scheint.
- *Anwendungsfall:* Wird für maximale Tarnung und Sicherheit verwendet und ignoriert unerwünschten Datenverkehr vollständig. Eignet sich als strenge Standardeinstellung für einen Server, der niemals eingehende Verbindungen annehmen soll.

`block`

- *Vertrauensstufe:* Sehr niedrig.
- *Verhalten:* Alle eingehenden Netzwerkverbindungen werden mit einer Meldung `icmp-host-prohibited` für IPv4 und einer Meldung `icmp6-adm-prohibited` für IPv6 abgelehnt. Dadurch wird dem Absender mitgeteilt, dass seine Verbindung ausdrücklich abgelehnt wurde. Es sind nur ausgehende Verbindungen möglich, die vom System initiiert wurden.
- *Anwendungsfall:* Wird angewendet, wenn Sie Absendern ausdrücklich signalisieren möchten, dass ihre Verbindungsversuche blockiert werden.

`public`

- *Vertrauensstufe:* Nicht vertrauenswürdig oder öffentlich.
- *Verhalten:* Stellt öffentliche, nicht vertrauenswürdige Netzwerke dar, in denen Sie anderen Systemen nicht vertrauen. Standardmäßig werden nur ausgewählte eingehende Verbindungen akzeptiert, z. B. SSH-, DHCPv6-Client usw.
- *Anwendungsfall:* Allgemeine Standardzone für Schnittstellen, die direkt mit dem Internet verbunden sind, beispielsweise die WAN-Schnittstelle Ihres Routers. Dazu gehören auch Verbindungen mit einem Netzwerk, bei dem Sie keine Kontrolle über andere Geräte haben.

`external`

- *Vertrauensstufe:* Extern mit Masquerading.
- *Verhalten:* Ist für externe Netzwerke vorgesehen, wenn die Firewall als Gateway oder Router fungiert. In der Regel ist das NAT-Masquerading standardmäßig aktiviert. Es werden nur ausgewählte eingehende Verbindungen akzeptiert. Dabei wird angenommen, dass Sie anderen Systemen in diesem Netzwerk nicht vertrauen.
- *Anwendungsfall:* Wird verwendet, wenn Ihr Linux-Computer als Router fungiert und ein internes privates Netzwerk mit dem öffentlichen Internet verbindet. Die externe Schnittstelle wird in dieser Zone platziert, um die interne Netzwerktopologie zu verbergen und internen Clients gleichzeitig den Zugriff auf externe Ressourcen wie das Internet zu ermöglichen.

`dmz (Demilitarized Zone)`

- *Vertrauensstufe:* Begrenzter öffentlicher Zugriff.
- *Verhalten:* Für Systeme in einer DMZ-Zone, die öffentlich aufrufbar sind, aber nur begrenzten Zugriff auf das interne Netzwerk haben. Es werden nur ausgewählte eingehende Verbindungen akzeptiert. Die Standardeinstellung umfasst in der Regel SSH und andere Dienste, die Sie bereitstellen.
- *Anwendungsfall:* Eignet sich für öffentlich aufrufbare Server wie Web-, E-Mail- und DNS-Server. Diese Server sind dem Internet absichtlich ausgesetzt, aber von Ihren internen, vertrauenswürdigeren Netzwerken isoliert. Nützlich, wenn Sie Dienste hosten möchten, die über das Internet aufrufbar sein müssen, und gleichzeitig das Risiko für Ihre interne Kerninfrastruktur minimieren möchten.

`work`

- *Vertrauensstufe:* Überwiegend vertrauenswürdig (Arbeitsumgebung).
- *Verhalten:* In einer Arbeitsumgebung vertrauen Sie anderen Computern im Netzwerk in der Regel. Lässt ausgewählte eingehende Verbindungen zu, die in einer Arbeitsumgebung üblich sind, z. B. SSH- und DHCPv6-Client.
- *Anwendungsfall:* Eignet sich für Büronetzwerke und Systeme in einem Firmen-LAN.

`home`

- *Vertrauensstufe:* Überwiegend vertrauenswürdig (Heimumgebung).
- *Verhalten:* In einer Heimumgebung vertrauen Sie den anderen Systemen im Netzwerk überwiegend. Ermöglicht mehr Dienste als öffentliche oder externe Zonen, häufig einschließlich gängiger Heimnetzwerkdienste wie Dateifreigabe, Medienserver und Drucker sowie SSH- und DHCPv6-Client.
- *Anwendungsfall:* Eignet sich am besten für Heimnetzwerke und kleine Home-Office-Einrichtungen.

`trusted`

- *Vertrauensstufe:* Am höchsten.
- *Verhalten:* Alle Netzwerkverbindungen werden ohne Filterung akzeptiert. Für Verbindungen, die dieser Zone zugewiesen sind, wurde keine Firewall implementiert.
- *Anwendungsfall:* Reserviert für Verbindungen mit höchster Vertrauensstufe.

1.2 `firewalld`-Richtlinien und -Regeln

`firewalld`-Richtlinien bieten im Vergleich zu traditionellen Zonen eine fortschrittlichere und flexiblere Möglichkeit zum Verwalten des Netzwerkverkehrs. Sie ermöglichen Ihnen die Definition umfassender Regeln, die Quelle und Ziel des Datenverkehrs, Dienste, Ports und Aktionen wie das Akzeptieren, Ablehnen und Löschen festlegen. Diese Richtlinien sind nützlich, um komplexes Routing und Portweiterleitungen einzurichten oder isolierte Netzwerksegmente innerhalb eines einzelnen Hosts zu erstellen.

`firewalld`-Richtlinien nutzen Zonen, um Regelsätze zu definieren. Sie wenden Regeln statusbezogen und in eine Richtung an, was bedeutet, dass Sie den Datenverkehrsfluss in eine Richtung definieren und `firewalld` den Rückpfad implizit zulässt. Diese Richtlinien verknüpfen eine Eingangszone (bei der der Datenverkehr eingeht) mit einer Ausgangszone (bei der der Datenverkehr ausgeht). Dadurch wird der spezifische Pfad und die Richtung definiert, für den oder die die Regeln einer Richtlinie gelten. Sie können die Richtlinien beispielsweise wie folgt anzeigen:

```
> /usr/lib/firewalld/policies ls
allow-host-ipv6.xml
```

Mithilfe von Firewall-Regeln können Sie den Netzwerkverkehr präzise steuern und ihn zulassen oder blockieren, um Ihr System vor Sicherheitsbedrohungen zu schützen. Firewall-Regeln definieren bestimmte Kriterien anhand verschiedener Attribute wie Quell- und Ziel-IP-Adressen, Ports und Netzwerkschnittstellen. `firewalld` unterteilt Firewall-Regeln in Zonen und Richtlinien. Jede Zone in `firewalld` verfügt über einen eindeutigen Regelsatz, der die Datenverkehrsberechtigungen für die zugehörigen Netzwerkschnittstellen vorgibt.

1.3 Dienste und Ports

Dienste werden empfohlen, wenn ein vordefinierter Dienst verfügbar ist. Anstatt sich beispielsweise zu merken, dass HTTP den TCP-Port 80 verwendet, können Sie einfach den `http`-Dienst hinzufügen. Dies ist weniger fehleranfällig und einfacher zu verwalten. Verwenden Sie Ports, wenn ein Dienst nicht vordefiniert ist oder wenn Sie einen benutzerdefinierten Port für einen Dienst verwenden. Sie können die aktiven Dienste und Ports für die Standardzonen wie folgt anzeigen:

```
> sudo firewall-cmd --list-services
```

```
> sudo firewall-cmd --list-ports
```

2 Verwalten von Firewall-Regeln und -Zonen

Sie können `firewalld`-Zonen und ihre Regeln mit der grafischen Weboberfläche Cockpit oder dem Dienstprogramm **`firewall-cmd`** für die Befehlszeilensteuerung konfigurieren.

2.1 Verwalten von Firewall-Regeln und -Zonen mithilfe des Dienstprogramms **`firewalld-cmd`**

Sie können die Befehlszeilenschnittstelle verwenden, um `firewalld`-Zonen zu verwalten.

2.1.1 Hinzufügen von `firewalld`-Zonen

So fügen Sie eine neue `firewalld`-Zone hinzu:

1. Erstellen Sie eine neue Zone. Beispiel:

```
> sudo firewall-cmd --permanent --new-zone=test
```

2. Legen Sie die Vertrauensstufe der Zone fest, die das Standardverhalten definiert:

```
> sudo firewall-cmd --permanent --zone=example --set-target=trusted
```

3. Laden Sie den `firewalld`-Dienst neu, um die neue Konfiguration anzuwenden:

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

2.1.2 Hinzufügen eines Diensts zu einer Zone

So fügen Sie einen Dienst einer Zone hinzu:

1. Listen Sie alle Dienste auf, um zu überprüfen, ob Ihr Dienst bereits vordefiniert ist:

```
> sudo firewall-cmd --get-services
      0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-
client amqp amqps anno-1602
      anno-1800 apcupsd audit ausweisapp2 bacula bacula-client bareos-director
 bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet
 bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-
agent civilization-iv civilization-v cockpit collectd condor-collector cratedb ctdb
 dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic
 dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client
 etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-
ldaps freeipa-replication freeipa-trust ftp galera
      ganglia-client ganglia-master git gpsd grafana gre http http3 https ident imap
 imaps ipfs ipp ipp-client ipsec irc ircs
      [...]
```

2. Sie können einen Dienst entweder vorübergehend für die Laufzeitsitzung oder dauerhaft hinzufügen. Beispiel:

```
> sudo  firewall-cmd --zone=public --add-service=http
```

```
> sudo  firewall-cmd --zone=public --permanent --add-service=http
```

Das `--permanent`-Flag stellt sicher, dass die Änderung bei allen Neustarts erhalten bleibt.

3. Laden Sie den `firewalld`-Dienst neu, um die neue Konfiguration anzuwenden:

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

4. Überprüfen Sie die Ergebnisse:

```
> sudo firewall-cmd --zone=public --list-services
```

2.1.3 Hinzufügen eines Ports zu einer Zone

Wenn Ihre Anwendung keinen vordefinierten Dienst hat, können Sie einen bestimmten Port oder einen Portbereich öffnen.

1. Sie können einen Port entweder vorübergehend für die Laufzeitsitzung oder dauerhaft hinzufügen. Beispiel:

```
> sudo  firewall-cmd --zone=public --add-port=8080/tcp
```

```
> sudo  firewall-cmd --zone=public --permanent --add-port=8080/tcp
```

Das `--permanent`-Flag stellt sicher, dass die Änderung bei allen Neustarts erhalten bleibt.

2. Laden Sie den `firewalld`-Dienst neu, um die neue Konfiguration anzuwenden:

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

3. Überprüfen Sie die Ergebnisse:

```
> sudo firewall-cmd --zone=public --list-ports
```

2.1.4 Löschen von `firewalld`-Zonen

So löschen Sie eine Zone:

1. Überprüfen Sie, dass es sich bei der Zone nicht um die Standardzone handelt und dass sie nicht verwendet wird:

```
> sudo  firewall-cmd --get-default-zone
```

Wenn die Zone verwendet wird oder es sich um die Standardzone handelt, legen Sie eine andere Zone fest. Beispiel:

```
> sudo  firewall-cmd --set-default-zone=NEW_DEFAULT_ZONE
```

2. Überprüfen Sie, ob Netzwerkschnittstellen an die Zone gebunden sind:

```
> sudo firewall-cmd --zone=ZONE_TO_BE_DELETED --list-all
```

3. Das Feld `interfaces` in der Ausgabe listet alle Schnittstellen auf. Diese Schnittstellen müssen einer anderen Zone neu zugewiesen werden. Beispiel:

```
> sudo firewall-cmd --zone=public --permanent --change-interface=ITERFACE_NAME
```

4. Löschen Sie die Zone:

```
> sudo firewall-cmd --permanent --delete-zone=ZONE_TO_BE_DELETED
```

5. Laden Sie den `firewalld`-Dienst neu, um die neue Konfiguration anzuwenden:

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

2.2 Verwalten von Firewall-Regeln und -Zonen mit Cockpit

Mit Cockpit können Sie neue Zonen erstellen oder bestehende Zonen aktualisieren. In den Firewall-Einstellungen können Sie Dienste zu einer Zone hinzufügen oder den Zugriff auf Ports erlauben.

Anmerkung: Der Cockpit-Dienst ist obligatorisch.

Entfernen Sie den Cockpit-Dienst nicht aus der Standard-Firewall-Zone, da der Cockpit-Dienst sonst blockiert und die Verbindung zum Server unterbrochen werden könnte.

2.2.1 Hinzufügen von Firewall-Zonen

Die *öffentliche Zone* ist die Standard-Firewall-Zone. Gehen Sie zum Hinzufügen einer neuen Zone wie folgt vor:

VORGEHEN 1: HINZUFÜGEN NEUER FIREWALL-ZONEN

1. Navigieren Sie zur Seite *Netzwerk*.
2. Klicken Sie auf *Regeln und Zonen bearbeiten*.
3. Klicken Sie auf *Zone hinzufügen*.
4. Wählen Sie die *Vertrauensstufe* aus. Jede Vertrauensstufe von Netzwerkverbindungen hat eine festgelegte Anzahl von Diensten (der Cockpit-Dienst ist in allen Vertrauensstufen enthalten).
5. Definieren Sie die zulässigen Adressen innerhalb der Zone. Wählen Sie einen der Werte aus:
   - *Ganzes Teilnetz*, um alle Adressen im Teilnetz zuzulassen.
   - *Bereich*: eine kommagetrennte Liste von IP-Adressen mit dem Routing-Präfix, zum Beispiel 192.0.2.0/24, 2001:db8::/32.
6. Fahren Sie mit *Zone hinzufügen* fort.

2.2.2 Hinzufügen von zulässigen Diensten und Ports zu einer Zone

Sie können einer bestehenden Firewall-Zone Dienste hinzufügen, wie unten beschrieben:

VORGEHEN 2: HINZUFÜGEN VON DIENSTEN ZU EINER FIREWALL-ZONE

1. Navigieren Sie zur Seite *Netzwerk*.
2. Klicken Sie auf *Regeln und Zonen bearbeiten*.
3. Klicken Sie auf *Dienste hinzufügen*.
4. Wenn Sie einen Dienst hinzufügen möchten, markieren Sie *Dienste* und wählen Sie die Dienste aus der Liste aus.
5. Wenn Sie eigene Ports zulassen möchten, markieren Sie *Benutzerdefinierte Ports* und geben Sie den Port-Wert für UDP und/oder TCP an. Sie können diesem Port eine Kennung zuweisen.

6. Klicken Sie zum Bestätigen der Änderungen auf *Dienste hinzufügen* bzw. *Ports hinzufügen*.

3 Gängige `firewalld`-Kommandos

Das Befehlszeilenwerkzeug **`firewall-cmd`** wird zum Konfigurieren und Verwalten des Daemons `firewalld` verwendet. Es handelt sich um ein leistungsstarkes, dynamisches Dienstprogramm, das das Erstellen, Ändern und Löschen von Firewall-Regeln ermöglicht, ohne dass ein vollständiger Neustart des Diensts erforderlich ist, wodurch eine Unterbrechung aktiver Netzwerkverbindungen verhindert wird.

Einige häufige **`firewall-cmd`**-Befehlsbeispiele beinhalten Folgendes:

- Überprüfen, ob `firewalld` ausgeführt wird Die Ausgaben lauten `running`, `not running` oder `RUNNING_BUT_FAILED`. Beispiel:

```
> sudo firewall-cmd --state
running
```

- Auflisten aller verfügbaren Zonen – Beispiel:

```
> sudo firewall-cmd --get-zones
 block dmz docker drop external home internal nm-shared public trusted work
```

- Anzeigen der Standardzone – Beispiel:

```
> sudo firewall-cmd --get-default-zone
public
```

- Anzeigen der aktiven Zonen und der zugewiesenen Zonen– Beispiel:

```
> sudo firewall-cmd --get-active-zones
docker
interfaces: docker0
public (default)
interfaces: lo enp1s0
```

- Anzeigen aller Regeln für die Standardzone – Beispiel:

```
> sudo firewall-cmd --list-all
public (default, active)
```

```
target: default
ingress-priority: 0
egress-priority: 0
icmp-block-inversion: no
interfaces: enp1s0 lo
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
rule family="ipv4" source address="192.168.1.100" service name="ssh" accept
```

- Anzeigen aller Regeln für eine bestimmte Zone – Beispiel:

```
> sudo firewall-cmd --zone=public --list-all
public (default, active)
target: default
ingress-priority: 0
egress-priority: 0
icmp-block-inversion: no
interfaces: enp1s0 lo
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
rule family="ipv4" source address="192.168.1.100" service name="ssh" accept
```

- Auflisten aller verfügbaren vordefinierten Dienste – Beispiel:

```
> sudo firewall-cmd --get-services
  0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client
 amqp amqps anno-1602 anno-1800
  apcupsd audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon
 bareos-storage bb bgp bitcoin bitcoin-rpc
  bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon
 cfengine checkmk-agent civilization-iv civilization-v
```

```
  cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp
 dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls
  docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server
 factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap
  freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-
master git gpsd grafana gre http http3 https ident imap imaps
  ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect
 kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver
  kube-control-plane kube-control-plane-secure kube-controller-manager kube-
controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-
secure
  [...]
```

- Auflisten der derzeit in der Standardzone zulässigen Dienste – Beispiel:

```
> sudo firewall-cmd --list-services
cockpit dhcpv6-client ssh
```

- Dauerhaftes Hinzufügen eines Diensts zur Standardzone – Beispiel:

```
> sudo firewall-cmd --permanent --add-service=http
success
```

- Dauerhaftes Entfernen eines Diensts – Beispiel:

```
> sudo firewall-cmd --permanent --remove-service=http
success
```

- Auflisten der derzeit in der Standardzone offenen Ports – Beispiel:

```
> sudo firewall-cmd --list-ports
22/tcp
```

- Vorübergehendes Öffnen eines bestimmten TCP-Ports – Beispiel:

```
> sudo firewall-cmd --add-port=8080/tcp
success
```

- Dauerhaftes Entfernen eines offenen Ports – Beispiel:

```
> sudo firewall-cmd --permanent --remove-port=8080/tcp
success
```

- Vorübergehendes Hinzufügen einer Schnittstelle zu einer bestimmten Zone – Beispiel:

```
> sudo firewall-cmd --zone=trusted --add-interface=eth1
```

```
success
```

4 Fehlerbehebung für `firewalld`

Die Fehlerbehebung von `firewalld` beinhaltet die Überprüfung des Status, die Überprüfung der Regeln und den Neustart oder das Neuladen des Diensts. Wenn Sie Probleme feststellen, können Sie das Debugging aktivieren, Protokolle prüfen und Firewall-Regeln bei Bedarf anpassen.

4.1 Überprüfen des `firewalld`-Status

- Verwenden Sie den Befehl **`systemctl status`**. Beispiel:

```
> sudo systemctl status  firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
Active: active (running) since Thu 2025-07-17 09:47:36 CEST; 5min ago
Invocation: a7ea482f16d2431fa92d6204c297ebd9
Docs: man:firewalld(1)
Main PID: 921 (firewalld)
Tasks: 2
CPU: 262ms
CGroup: /system.slice/firewalld.service
        └─921 /usr/bin/python3.13 /usr/sbin/firewalld --nofork --nopid
```

- Der Befehl **`firewall-cmd --state`** bietet eine schnelle Statusprüfung mit den Ausgaben `running`, `not running` oder `RUNNING_BUT_FAILED`. Beispiel:

```
> sudo firewall-cmd --state
running
```

- Wenn `firewalld` nicht ausgeführt wird, verwenden Sie den Befehl **`systemctl start firewalld`**.

```
> sudo  systemctl start firewalld
```

- Wenn der `firewalld`-Dienst maskiert ist, demaskieren Sie ihn zunächst, aktivieren und starten Sie ihn dann. Beispiel:

```
> sudo systemctl unmask --now firewalld
```

```
> sudo systemctl enable firewalld
```

```
> sudo systemctl start firewalld
```

4.2 Überprüfen von `firewalld`-Regeln

- Der Befehl **`firewall-cmd --list-all-zones`** zeigt alle Zonen und ihre Regeln an. Beispiel:

```
> sudo firewall-cmd --list-all-zones
       block
         target: %%REJECT%%
         ingress-priority: 0
         egress-priority: 0
         icmp-block-inversion: no
         interfaces:
         sources:
         services:
         ports:
         protocols:
         forward: yes
         masquerade: no
         forward-ports:
         source-ports:
         icmp-blocks:
         rich rules:

       dmz
         target: default
         ingress-priority: 0
         egress-priority: 0
         icmp-block-inversion: no
         interfaces:
         sources:
         services: ssh
         ports:
         protocols:
         forward: yes
         masquerade: no
         forward-ports:
         source-ports:
         icmp-blocks:
         rich rules:
```

```
        docker (active)
          target: ACCEPT
          ingress-priority: 0
          egress-priority: 0
          icmp-block-inversion: no
          [...]
```

- Der Befehl **`firewall-cmd --list-ports`** zeigt offene Ports an. Beispiel:

```
> sudo firewall-cmd --list-ports
22/tcp
```

- Der Befehl **`firewall-cmd --zone=`***`YOUR_ZONE`* **`--list-all.`** listet Ports für bestimmte Zonen auf. Beispiel:

```
> sudo firewall-cmd --zone=dmz --list-all
               dmz
                 target: default
                 ingress-priority: 0
                 egress-priority: 0
                 icmp-block-inversion: no
                 interfaces:
                 sources:
                 services: ssh
                 ports:
                 protocols:
                 forward: yes
                 masquerade: no
                 forward-ports:
                 source-ports:
                 icmp-blocks:
                 rich rules:
```

4.3 Debugging von `firewalld`

- Aktivieren Sie das Debugging in `/etc/sysconfig/firewalld` durch Hinzufügen von `--debug=[level]` zu `FIREWALLD_ARGS`. Beispiel:

```
> sudo  vi /etc/sysconfig/firewalld
# firewalld command line args
# possible values: --debug
```

```
FIREWALLD_ARGS=--debug=[level]
```

- Starten Sie `firewalld` mit der Option `--debug`. Beispiel:

```
> sudo firewalld --nofork --debug
2025-07-23 11:10:05 DEBUG1: start()
2025-07-23 11:10:05 DEBUG1: Loading firewalld config file '/etc/firewalld/
firewalld.conf'
2025-07-23 11:10:05 DEBUG1: CleanupOnExit is set to 'True'
2025-07-23 11:10:05 DEBUG1: CleanupModulesOnExit is set to 'False'
2025-07-23 11:10:05 DEBUG1: IPv6 rpfilter is enabled
2025-07-23 11:10:05 DEBUG1: LogDenied is set to 'off'
2025-07-23 11:10:05 DEBUG1: FirewallBackend is set to 'nftables'
2025-07-23 11:10:05 DEBUG1: FlushAllOnReload is set to 'False'
2025-07-23 11:10:05 DEBUG1: RFC3964_IPv4 is set to 'True'
2025-07-23 11:10:05 DEBUG1: NftablesFlowtable is set to 'off'
2025-07-23 11:10:05 DEBUG1: NftablesCounters is set to 'False'
2025-07-23 11:10:05 DEBUG1: Loading lockdown whitelist
2025-07-23 11:10:05 ipset not usable, disabling ipset usage in firewall. Other set
 backends (nftables) remain usable.
2025-07-23 11:10:05 iptables-restore and iptables are missing, IPv4 direct rules
 won't be usable.
2025-07-23 11:10:05 ip6tables-restore and ip6tables are missing, IPv6 direct rules
 won't be usable.
2025-07-23 11:10:05 ebtables-restore and ebtables are missing, eb direct rules won't
 be usable.
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/icmptypes/
address-unreachable.xml'
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/icmptypes/bad-
header.xml'
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/icmptypes/
beyond-scope.xml'
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/icmptypes/
communication-prohibited.xml'
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/icmptypes/
destination-unreachable.xml'
[...]
```

Alle Protokolldateien sind unter `/var/log/firewalld` verfügbar.

5 Weitere Informationen

Weitere Informationen zu `firewalld` finden Sie in den folgenden Ressourcen:

- Die offizielle Quelle für Konzepte, Architektur, Anleitungen und Links zu allen Handbuchseiten. (https://firewalld.org/documentation/)
- Handbuchseite, die zum Nachvollziehen der Befehlszeileninteraktion mit `firewalld` wichtig ist (https://firewalld.org/documentation/man-pages/firewall-cmd.html)
- Eine umfassende Ressource mit hervorragenden Erklärungen und praktischen Beispielen, die auch `nftables` abdeckt. (https://wiki.archlinux.org/title/Firewalld)

6 Rechtliche Hinweise

A GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent

copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through

arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See https://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with…Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.