firewalldの概要

概要

Linuxサーバとサービスを保護するための重要なツールである`firewalld`について習得します。firewalldは、多くの最新ディストリビューションにおけるデフォルトかつ主要なネットワーク防御メカニズムです。直感的なゾーンベースの管理と動的設定機能により、サービスを中断することなくネットワークトラフィックを正確に制御できます。

目的

`firewalld`は、複雑なファイアウォールのルールを直感的なゾーンとサービスに抽象化することで、Linuxシステム上のネットワークセキュリティを管理するための現代的、動的でユーザフレンドリな方法を提供するため、不可欠です。

所要時間

この記事の理解には30分ほどを要します。

目標

Linuxシステムのセキュリティを効果的に管理し強化すること。

要件

- `sudo`または`root`特権。`firewalld`コマンド、特にファイアウォールルールに永続的な変更を加えるコマンドには、昇格された特権が必要だからです。
- `firewalld`は、多くの最新のLinuxディストリビューションのデフォルトのファイアウォールです。システムにプリインストールされていない場合は、`firewalld`パッケージをインストールする必要があります。
- Linux端末の基本的な理解が不可欠です。

発行日: 11/12/2025

目次

1 firewalldについて

firewalldは、Linuxシステム上のネットワークトラフィックを柔軟かつ効率的に制御する動的ファイアウォール管理サービスです。既存の接続を中断することなく変更することができます。firewalldを使用する利点は次のとおりです。

- **動的設定:**既存の接続を切断することなく、変更を即座に適用できます。
- **ユーザフレンドリなインタフェース:**ゾーンとサービスは複雑なファイアウォールルールを簡素化します。
- **抽象化:**一般的なシナリオでは、nftablesルールを直接操作する必要はありません。
- **永続的な設定:**再起動後も維持されるルールを簡単に管理できます。
- **永続的な設定:**デフォルトでは、firewalldは、明示的に許可されていない限り、すべての着信トラフィックをブロックするdeny-all原則に基づいて動作します。

1.1 firewalldゾーン

ファイアウォールゾーンは、特定のネットワークインタフェースまたは送信元IPアドレスに対する送受信ネットワークトラフィックの処理方法を規定する定義済みのルールセットです。各ゾーンは、関連付けられているネットワークの異なる信頼レベルを表します。ネットワーク接続の発信元に基づいて、さまざまなセキュリティポリシーを適用できます。

ゾーンはセキュリティプロファイルのようなものです。たとえば、公共のWi-Fi接続と安全なホームネットワークに異なるファイアウォールルールを適用したい場合があります。firewalldゾーンを使用すると、こうした個別のルールセットを定義し、それに応じて適用できます。ネットワーク接続は、1つのfirewalldゾーンのルールのみに従います。firewalldゾーンには、多数のネットワークインタフェースまたは送信元IPアドレスを含めることができます。

/usr/lib/firewalld/zones/ディレクトリには、事前定義済みのゾーンが格納されます。次に例を示します。

```
> /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
```

事前定義済みゾーンのデフォルト設定の一部は次のとおりです。

`drop`

- **信頼レベル:**完全に信頼しません。
- **動作:**すべての受信ネットワークパケットは、応答なしでドロップされます。システムから開始された発信接続のみが許可されます。これにより、外部の攻撃者にはシステムが存在しないように見える「ステルス」モードが提供されます。
- **使用事例:**ステルス性とセキュリティを最大限に高めるために使用し、不要なトラフィックを完全に無視します。着信接続を絶対に受け入れてはいけないサーバの厳格なデフォルトとして適しています。

`block`

- **信頼レベル:**非常に低い。
- **動作:**すべての受信ネットワーク接続は、IPv4の場合は`icmp-host-prohibited`メッセージ、IPv6の場合は`icmp6-adm-prohibited`メッセージで拒否されます。これにより、接続が明示的に拒否されたことが送信者に通知されます。システムから開始された発信接続のみが可能です。
- **使用事例:**接続試行がブロックされていることを送信者に明示的に通知する場合に適用されます。

`public`

- **信頼レベル:**信頼できない、またはパブリック。
- **動作:**他のシステムを信頼しない、パブリックの信頼できないネットワークを表します。デフォルトでは、SSH、DHCPv6クライアントなど、選択された着信接続のみが受け入れられます。
- **使用事例:**ルータのWANインタフェースなど、インターネットに直接接続されたインタフェースの一般的なデフォルトゾーン。また、他のデバイスを制御できないネットワークへの接続も含まれます。

`external`

- **信頼レベル:**マスカレード付きの外部。
- **動作:**ファイアウォールがゲートウェイまたはルータとして機能する場合の外部ネットワーク向けです。通常、NATマスカレードはデフォルトで有効になっています。このネットワーク上の他のシステムを信頼していないという前提で、選択された着信接続のみが受け入れられます。
- **使用事例:**Linuxマシンがルータとして動作し、内部のプライベートネットワークをパブリックインターネットに接続する場合に使用されます。外部インタフェースはこのゾーンに配置され、内部ネットワークトポロジを隠しながら、内部クライアントがインターネットなどの外部リソースにアクセスできるようにします。

`dmz (Demilitarized Zone)`

- **信頼レベル:**制限されたパブリックアクセス。
- **動作:**パブリックアクセス可能だが、内部ネットワークへのアクセスは制限されているDMZゾーン内のシステム用。選択された着信接続のみが受け入れられます。デフォルトには通常、SSHや公開するその他のサービスが含まれます。
- **使用事例:**Webサーバ、メールサーバ、DNSサーバなどのパブリックサーバに適しています。これらのサーバは意図的にインターネットに公開されていますが、内部のより信頼できるネットワークからは隔離されています。中核となる内部インフラストラクチャへのリスクを最小限に抑えながら、インターネットにアクセスできる必要があるサービスをホストする場合に便利です。

`work`

- **信頼レベル:**ほぼ信頼(作業環境)。
- **動作:**作業環境では、通常、ネットワーク上の他のコンピュータを信頼します。SSHやDHCPv6クライアントなど、作業環境でよく使用される特定の着信接続を許可します。
- **使用事例:**オフィスネットワークや企業LAN上のシステムに適しています。

`home`

- **信頼レベル:**ほぼ信頼(ホーム環境)。
- **動作:**ホーム環境では、ネットワーク上の他のシステムをほぼ信頼します。パブリックゾーンや外部ゾーンよりも多くのサービスを許可します。多くの場合、ファイル共有、メディアサーバ、プリンタなどの一般的なホームネットワークサービスに加え、SSHやDHCPv6クライアントも含まれます。
- **使用事例:**ホームネットワークや小規模ホームオフィスのセットアップに最適です。

`trusted`

- **信頼レベル:**最も高い。
- **動作:**すべてのネットワーク接続は、フィルタリングなしで受け入れられます。このゾーンに割り当てられた接続にはファイアウォールは実装されていません。
- **使用事例:**信頼性の高い接続用に予約されています。

1.2 firewalldポリシーとルール

`firewalld`ポリシーは、従来のゾーンと比較して、より高度で柔軟なネットワークトラフィック管理方法を提供します。これにより、トラフィック、サービス、ポート、および許可、拒否、ドロップなどのアクションの送信元と宛先を指定する豊富なルールを定義できます。これらのポリシーは、複雑なルーティングやポート転送を設定したり、単一ホスト内で分離されたネットワークセグメントを作成したりする場合に便利です。

`firewalld`ポリシーは、ゾーンを利用してルールセットを定義します。ルールはステートフルかつ一方向に適用されるため、一方向にトラフィックフローを定義すると、`firewalld`はリターンパスを暗黙的に許可します。これらのポリシーは、入力ゾーン(トラフィックが入る場所)と出力ゾーン(トラフィックが出る場所)をリンクします。これにより、ポリシーのルールが適用される具体的なパスと方向が定義されます。たとえば、ポリシーは次のように表示できます。

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

ファイアウォールルールは、ネットワークトラフィックを正確に制御し、許可またはブロックしてシステムをセキュリティの脅威から保護できます。ファイアウォールルールは、送信元と送信先のIPアドレス、ポート、ネットワークインタフェースなどのさまざまな属性に基づい

て特定の基準を定義します。firewalldは、ファイアウォールルールをゾーンとポリシーに分けます。firewalldの各ゾーンには、関連するネットワークインタフェースへのトラフィック権限を規定する固有のルールセットがあります。

1.3 サービスとポート

事前定義済みのサービスが利用できる場合は、サービスを使用することが推奨されます。たとえば、HTTPがTCPポート80を使用していることを覚えておく代わりに、httpサービスを追加するだけで済みます。これにより、エラーが発生しにくくなり、管理も容易になります。サービスが事前定義されていない場合や、サービスにカスタムポートを使用している場合は、ポートを使用してください。デフォルトゾーンのアクティブなサービスとポートは、次のコマンドで確認できます。

```
> sudofirewall-cmd --list-services
```

```
> sudofirewall-cmd --list-ports
```

2 ファイアウォールルールとゾーンの管理

firewalldゾーンとそのルールは、グラフィカルなWebインタフェースCockpitまたはコマンドライン制御用の**firewall-cmd**ユーティリティを使用して設定できます。

2.1 firewalld-cmdユーティリティを使用したfirewallルールとゾーンの管理

CLIインタフェースを使用してfirewalldゾーンを管理できます。

2.1.1 firewalldゾーンの追加

新しいfirewalldゾーンを追加するには:

1. 新しいゾーンを作成します。例:

   ```
   > sudofirewall-cmd --permanent --new-zone=test
   ```

2. デフォルト動作を定義するゾーンの信頼レベルを設定します。

```
> sudofirewall-cmd --permanent --zone=example --set-target=trusted
```

3. firewalldサービスを再ロードして新しい設定を適用します。

```
> sudofirewall-cmd --reload
```

2.1.2 ゾーンへのサービスの追加

ゾーンにサービスを追加するには:

1. すべてのサービスを一覧表示して、サービスがすでに事前定義されているかどうかを確認します。

```
> sudofirewall-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. サービスは、ランタイムセッション用に一時的に追加することも、永続的に追加することもできます。例:

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

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

--permanentフラグにより、すべての再起動後も変更が維持されます。

3. firewalldサービスを再ロードして新しい設定を適用します。

```
> sudofirewall-cmd --reload
```

4. 結果を確認します。

```
> sudofirewall-cmd --zone=public --list-services
```

2.1.3 ゾーンへのポートの追加

アプリケーションに事前定義済みのサービスがない場合は、特定のポートまたはポートの範囲を開くことができます。

1. ポートは、ランタイムセッション用に一時的に追加することも、永続的に追加することもできます。例:

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

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

`--permanent`フラグにより、すべての再起動後も変更が維持されます。

2. `firewalld`サービスを再ロードして新しい設定を適用します。

```
> sudofirewall-cmd --reload
```

3. 結果を確認します。

```
> sudofirewall-cmd --zone=public --list-ports
```

2.1.4 `firewalld`ゾーンの削除

ゾーンを削除するには:

1. ゾーンがデフォルトでも使用中でもないことを確認します。

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

ゾーンが使用中またはデフォルトの場合、別のゾーンを設定します。例:

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

2. ネットワークインタフェースがゾーンにバインドされているかどうかを確認します。

```
> sudofirewall-cmd --zone=ZONE_TO_BE_DELETED --list-all
```

3. 出力の`interfaces`フィールドには、すべてのインタフェースが一覧表示されます。これらのインタフェースは別のゾーンに再割り当てする必要があります。次に例を示します。

```
> sudofirewall-cmd --zone=public --permanent --change-interface=ITERFACE_NAME
```

4. ゾーンを削除します。

```
> sudofirewall-cmd --permanent --delete-zone=ZONE_TO_BE_DELETED
```

5. firewalldサービスを再ロードして新しい設定を適用します。

```
> sudofirewall-cmd --reload
```

2.2 Cockpitによるファイアウォールルールとゾーンの管理

Cockpitでは、新しいゾーンの作成や既存のゾーンの更新を行うことができます。ファイアウォールの設定で、ゾーンにサービスを追加したり、ポートへのアクセスを許可したりできます。

注記: Cockpitサービスは必須

Cockpitサービスをデフォルトのファイアウォールゾーンから削除しないでください。Cockpitサービスがブロックされ、サーバから切断される可能性があります。

2.2.1 ファイアウォールゾーンの追加

public zone (パブリックゾーン)はデフォルトのファイアウォールゾーンです。新しいゾーンを追加するには、次の手順に従います。

手順 1: 新しいファイアウォールゾーンの追加

1. ネットワーキングページに移動します。
2. ルールとゾーンを編集するをクリックします。
3. ゾーンの追加をクリックします。
4. 信頼レベルを選択します。ネットワーク接続の各信頼レベルには、付属するサービスの事前定義済みのセットがあります(Cockpitサービスはすべての信頼レベルに付属します)。
5. ゾーン内で許可するアドレスを定義します。次のいずれかの値を選択します。
   - サブネット全体 - サブネット内のすべてのアドレスを許可します。
   - 範囲 - IPアドレスとルーティングプレフィクスのコンマ区切りリスト。たとえば、192.0.2.0/24, 2001:db8::/32です。

6. ゾーンの追加を選択して続行します。

2.2.2 ゾーンへの許可するサービスとポートの追加

次に説明するように、既存のファイアウォールゾーンにサービスを追加できます。

手順 2: ファイアウォールゾーンへのサービスの追加

1. ネットワーキングページに移動します。
2. ルールとゾーンを編集するをクリックします。
3. サービスの追加をクリックします。
4. サービスを追加するには、サービスをオンにして、リストからサービスを選択します。
5. カスタムポートを許可するには、カスタムポートをオンにして、UDPまたはTCP、あるいはその両方のポート値を指定します。このポートに識別子を割り当てることができます。
6. 変更を確認するには、サービスの追加またはポートの追加をそれぞれクリックします。

3 一般的なfirewalldコマンド

firewall-cmdコマンドラインツールは、firewalldデーモンの設定と管理に使用されます。これは強力で動的なユーティリティであり、サービスの全面的な再起動を必要とせずにファイアウォールルールを作成、変更、削除できるため、アクティブなネットワーク接続の中断を防ぐことができます。

一般的な**firewall-cmd**コマンド例には次のものがあります。

- firewalldが実行中かどうかチェックする。出力はrunning、not running、またはRUNNING_BUT_FAILEDです。次に例を示します。

```
> sudofirewall-cmd --state
running
```

- 利用可能なすべてのゾーンを一覧表示する。例:

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

- デフォルトゾーンを表示する。例:

```
> sudofirewall-cmd --get-default-zone
public
```

- アクティブなゾーンと割り当てられているゾーンを表示する。例:

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

- デフォルトゾーンのすべてのルールを表示する。例:

```
> sudofirewall-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
```

- 特定のゾーンのすべてのルールを表示する。例:

```
> sudofirewall-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
```

- 利用可能なすべての事前定義済みサービスを一覧表示する。例:

```
> sudofirewall-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
  [...]
```

- デフォルトゾーンで現在許可されているサービスを一覧表示する。例:

```
> sudofirewall-cmd --list-services
cockpit dhcpv6-client ssh
```

- デフォルトゾーンにサービスを永続的に追加する。例:

```
> sudofirewall-cmd --permanent --add-service=http
success
```

- サービスを完全に削除する。例:

```
> sudofirewall-cmd --permanent --remove-service=http
success
```

- デフォルトゾーンで現在開いているポートを一覧表示する。例:

```
> sudofirewall-cmd --list-ports
22/tcp
```

- 特定のTCPポートを一時的に開く。例:

```
> sudofirewall-cmd --add-port=8080/tcp
```

```
success
```

- 開いているポートを完全に削除する。例:

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

- 特定のゾーンにインタフェースを一時的に追加する。例:

```
> sudofirewall-cmd --zone=trusted --add-interface=eth1
success
```

4 firewalldのトラブルシューティング

firewalldのトラブルシューティングには、ステータスのチェック、ルールの確認、サービスの再起動または再ロードが含まれます。問題が発生した場合は、必要に応じてデバッグを有効にしたり、ログを調べたり、ファイアウォールルールを調整したりできます。

4.1 firewalldステータスのチェック

- **systemctl status**コマンドを使用します。例:

```
> sudosystemctl 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
```

- **firewall-cmd --state**コマンドは、running、not running、またはRUNNING_BUT_FAILED出力で簡単なステータスチェックを行います。次に例を示します。

```
> sudofirewall-cmd --state
running
```

- `firewalld`が実行されていない場合は、**`systemctl start firewalld`**コマンドを使用します。

```
> sudo  systemctl start firewalld
```

- `firewalld`サービスがマスクされている場合は、まずそのサービスのマスクを解除し、次に有効にしてから起動します。例:

```
> sudosystemctl unmask --now firewalld
```

```
> sudosystemctl enable firewalld
```

```
> sudosystemctl start firewalld
```

4.2 firewalldルールのチェック

- **`firewall-cmd --list-all-zones`**コマンドは、すべてのゾーンとそのルールを表示します。例:

```
> sudofirewall-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
          [...]
```

- **`firewall-cmd --list-ports`**コマンドは、開いているポートを表示します。例:

```
> sudofirewall-cmd --list-ports
22/tcp
```

- **`firewall-cmd --zone=`**`YOUR_ZONE`** `--list-all.`** コマンドは、特定のゾーンのポートを一覧表示します。例:

```
> sudofirewall-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 firewalldのデバッグ

- `--debug=[level]`を`FIREWALLD_ARGS`に追加して、`/etc/sysconfig/firewalld`のデバッグを有効にします。例:

```
> sudo  vi /etc/sysconfig/firewalld
```

```
# firewalld command line args
# possible values: --debug
FIREWALLD_ARGS=--debug=[level]
```

- `--debug`オプションを指定して`firewalld`を起動します。例:

```
> sudofirewalld --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'
[...]
```

すべてのログファイルは、`/var/log/firewalld`にあります。

5 詳細情報

`firewalld`の詳細は、次のリソースを参照してください。

- コンセプト、アーキテクチャ、ハウツー、すべてのマニュアルページへのリンクに関する公式ソース (https://firewalld.org/documentation/)
- `firewalld`のコマンドライン操作を理解するために不可欠なマニュアルページ (https://firewalld.org/documentation/man-pages/firewall-cmd.html)
- 優れた説明と実践例を含む包括的なリソースで、`nftables`についても網羅している (https://wiki.archlinux.org/title/Firewalld)

6 法的事項

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.