Firewalld について

http://itpro.nikkeibp.co.jp/atcl/column/14/072400026/072400001/
CentOS7 から採用されたファイヤーウォール。
これまで利用されてきた iptables のバックエンドのパケットフィルターに対して
設定を行う。
iptables との違いは、動的にポリシーが変更できることと、
public や home などのゾーンという概念導入されたこと。

iptables サービスを使っても firewalld サービスを使っても結果的には
iptables コマンドでパケットフィルターに対して設定を行なっている。

firewalld の使い方

http://www.unix-power.net/centos7/firewalld.html
http://www.mk-mode.com/octopress/2014/08/09/centos-7-0-setting-of-firewall/

稼働状況の確認

```
systemctl status firewalld
firewall-cmd --state
```

コマンド

■ゾーンやサービスの確認

コマンド	意味	備考
firewall-cmd --list-all	現在有効なゾーンの設定確認	--
firewall-cmd --list-all-zones	全てのゾーンの設定確認	--
firewall-cmd --get-services	定義済みサービス名確認	--
firewall-cmd --get-default-zone	デフォルトゾーンの確認	--
firewall-cmd --set-default-zone=trusted	デフォルトゾーンの変更	--
firewall-cmd --zone=trusted --change-interface=eno1	ゾーンのインターフェイスを付け替え	--
firewall-cmd --reload	設定の再読み込み	--

■サービス

コマンド	意味	備考
firewall-cmd --zone=public --list-services	public ゾーンで許可されているサービスの一覧を確認	--
firewall-cmd --zone=public --add-service=ftp	public ゾーンに ftp サービスの許可を追加	恒久的に設定する場合は --permanent を付ける

firewall-cmd --zone=public --query-service=ftp	public ゾーンで ftp サービスが許可されているか確認	--
firewall-cmd --zone=public --remove-service=ftp	public ゾーンから ftp サービスの許可を削除	恒久的に設定する場合は --permanent を付ける

■ポート

コマンド	意味	備考
firewall-cmd --zone=public --list-ports	public ゾーンで許可されているサービスの一覧を確認	--
firewall-cmd --zone=public --add-port=4000/tcp	public ゾーンにポート TCP:4000 の許可を追加	恒久的に設定する場合は --permanent を付ける
firewall-cmd --zone=public --add-port=4000-4005/tcp	public ゾーンにポート TCP:4000 ～ 4005 の許可を追加	恒久的に設定する場合は --permanent を付ける
firewall-cmd --zone=public --remove-port=4000/tcp	public ゾーンからポート TCP:4000 の許可を削除	恒久的に設定する場合は --permanent を付ける

■ ICMP

コマンド	意味	備考
firewall-cmd --zone=public --list-icmp-blocks	public ゾーンで禁止されている ICMP の一覧を確認	--
firewall-cmd --zone=public --add-icmp-block=echo-request	public ゾーンに echo-request の禁止を追加	恒久的に設定する場合は --permanent を付ける
firewall-cmd --zone=public --query-icmp-block=echo-request	public ゾーンで echo-request が禁止されているか確認	--
firewall-cmd --zone=public --remove-icmp-block=echo-request	public ゾーンから echo-request の禁止を削除	恒久的に設定する場合は --permanent を付ける

■マスカレード

コマンド	意味	備考
firewall-cmd --zone=public --list-icmp-blocks	public ゾーンでの IP マスカレードの設定を確認	--
firewall-cmd --zone=public --add-masquerade	public ゾーンで IP マスカレードを有効にする	恒久的に設定する場合は --permanent を付ける
firewall-cmd --zone=public --remove-masquerade	public ゾーンで IP マスカレードを無効にする	恒久的に設定する場合は --permanent を付ける

■ポートフォワード

コマンド	意味	備考
firewall-cmd --zone=public --list-forward-ports	public ゾーンでのポートフォワードの設定を確認	--

firewall-cmd --zone=public --add-forward-port=port=22 :proto=tcp:toport=8888	public ゾーンで TCP:99 宛のパケットを TCP:8888 宛に変更する設定を追加	恒久的に設定する場合は --permanent を付ける
firewall-cmd --zone=public --query-forward-port=port=22 :proto=tcp:toport=8888	public ゾーンに TCP:99 宛のパケットを TCP:8888 宛に変更する設定が適用されているか確認	--
firewall-cmd --zone=public --remove-forward-port=port=22 :proto=tcp:toport=8888	public ゾーンで TCP:99 宛のパケットを TCP:8888 宛に変更する設定を削除	恒久的に設定する場合は --permanent を付ける

iptables で確認

最終的にどんなポートがどのように設定されているかは iptables コマンドで確認できる。

```
iptables --list -n
```

サービスの設定ファイル

※サービス一覧

```
# ls /usr/lib/firewalld/services/
```

※ ICMP タイプ一覧

```
# ls /usr/lib/firewalld/icmptypes/
```

GUI での設定

```
firewall-config
```