目次

awall (Alpine Wall) を使う

v4.4.0β6 から FirewallD の代わりに Alpine Wall[1)]を利用可能にしました。
起動時間を10秒以上高速化することが可能です。

QuickStart

基本的な設定は標準で入れてありますので FirewallD での設定とほぼ同じままで良ければ FirewallD を無効化して awall を有効化します。

FirewallD の無効化

```
root@plum:~# systemctl disable firewalld
Synchronizing state of firewalld.service with SysV service script with
/lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable firewalld
insserv: warning: current start runlevel(s) (empty) of script `firewalld'
overrides LSB defaults (2 3 4 5).
insserv: warning: current stop runlevel(s) (0 1 2 3 4 5 6) of script
`firewalld' overrides LSB defaults (0 1 6).
Removed /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
```

awall の有効化

```
root@plum:~# systemctl enable awall
Created symlink /etc/systemd/system/multi-user.target.wants/awall.service →
/etc/systemd/system/awall.service.
```

再起動

再起動すると awall により iptables が設定されて起動します。

```
root@plum:~# reboot
```

初期設定

設定ファイルは、/etc/awall/[optional, private] にあります。

```
root@plum:/etc/awall# ls -lR
.:
total 0
lrwxrwxrwx 1 root root 29 Nov 15 12:11 main.json ->
/etc/awall/optional/main.json
drwxr-xr-x 2 root root 32 Nov 15 14:01 optional
drwxr-xr-x 2 root root 51 Nov 15 14:01 private

./optional:
total 1
-rw-r--r-- 1 root root 72 Nov 15 14:01 main.json

./private:
total 2
-rw-r--r-- 1 root root 549 Nov 15 13:18 base.json
-rw-r--r-- 1 root root 202 Nov 15 14:01 filter.json
```

base.json でインターフェース毎のゾーン設定、ゾーン毎の基本的なポリシ(ACCEPT, DROP など)を設定しています。

base.json

```
{
    "description": "Base zones and policies",
    "zone": {
        "WAN": {
            "iface": [
                "ppp0",
                "ppp1"
            ]
        },
        "LAN": {
            "iface": [
                "eth0",
                "eth1",
                "br0",
                "wg+"
            ]
        },
        "Closed": {
            "iface": [
                "ppp500",
```

```
                "ppp501",
                "ppp502",
                "ppp503"
            ]
        }
    },
    "policy": [
        {
            "in": "_fw",
            "out": "WAN",
            "action": "accept"
        },
        {
            "in": "LAN",
            "action": "accept"
        },
        {
            "out": "LAN",
            "action": "accept"
        },
        {
            "in": "WAN",
            "action": "drop"
        },
        {
            "in": "Closed",
            "action": "accept"
        }
    ],
    "snat": [
        {
            "out": [
                "WAN",
                "Closed"
            ]
        }
    ],
    "clamp-mss": [
        {
            "out": [
                "WAN",
                "Closed"
            ]
        }
    ]
}
```

filter.json で、ポリシーから外れる条件を記述しています。

filter.json

```
{
    "description": "Filter",
    "filter": [
        {
            "in": "WAN",
            "out": "_fw",
            "service": "ssh",
            "action": "accept",
            "conn-limit": {
                "count": 3,
                "interval": 20
            }
        }
    ]
}
```

生成された iptables rule

以上の設定から生成された iptables rule は次のようになります。

```
# Generated by iptables-save v1.6.1 on Fri Nov 15 14:51:36 2019
*nat
:PREROUTING ACCEPT [81:13188]
:INPUT ACCEPT [81:13188]
:OUTPUT ACCEPT [25:1862]
:POSTROUTING ACCEPT [25:1862]
:awall-masquerade - [0:0]
-A POSTROUTING -o ppp0 -j MASQUERADE
-A POSTROUTING -o ppp1 -j MASQUERADE
-A POSTROUTING -o ppp500 -j MASQUERADE
-A POSTROUTING -o ppp501 -j MASQUERADE
-A POSTROUTING -o ppp502 -j MASQUERADE
-A POSTROUTING -o ppp503 -j MASQUERADE
-A POSTROUTING -m set --match-set awall-masquerade src -j awall-masquerade
-A awall-masquerade -m set ! --match-set awall-masquerade dst -j MASQUERADE
COMMIT
# Completed on Fri Nov 15 14:51:36 2019
# Generated by iptables-save v1.6.1 on Fri Nov 15 14:51:36 2019
*mangle
:PREROUTING ACCEPT [799:61223]
:INPUT ACCEPT [799:61223]
:FORWARD ACCEPT [0:0]
```

```
:OUTPUT ACCEPT [578:61713]
:POSTROUTING ACCEPT [578:61713]
-A POSTROUTING -o ppp0 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --
clamp-mss-to-pmtu
-A POSTROUTING -o ppp1 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --
clamp-mss-to-pmtu
-A POSTROUTING -o ppp500 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --
clamp-mss-to-pmtu
-A POSTROUTING -o ppp501 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --
clamp-mss-to-pmtu
-A POSTROUTING -o ppp502 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --
clamp-mss-to-pmtu
-A POSTROUTING -o ppp503 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --
clamp-mss-to-pmtu
COMMIT
# Completed on Fri Nov 15 14:51:36 2019
# Generated by iptables-save v1.6.1 on Fri Nov 15 14:51:36 2019
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:icmp-routing - [0:0]
:limit-ssh-0 - [0:0]
:logdrop-0 - [0:0]
:logdrop-ssh-0 - [0:0]
-A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -i ppp0 -p tcp -m tcp --dport 22 -j limit-ssh-0
-A INPUT -i ppp1 -p tcp -m tcp --dport 22 -j limit-ssh-0
-A INPUT -p icmp -j icmp-routing
-A INPUT -i eth0 -j ACCEPT
-A INPUT -i eth1 -j ACCEPT
-A INPUT -i br0 -j ACCEPT
-A INPUT -i wg+ -j ACCEPT
-A INPUT -i ppp0 -j logdrop-0
-A INPUT -i ppp1 -j logdrop-0
-A INPUT -i ppp500 -j ACCEPT
-A INPUT -i ppp501 -j ACCEPT
-A INPUT -i ppp502 -j ACCEPT
-A INPUT -i ppp503 -j ACCEPT
-A FORWARD -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -j icmp-routing
-A FORWARD -i eth0 -j ACCEPT
-A FORWARD -i eth1 -j ACCEPT
-A FORWARD -i br0 -j ACCEPT
-A FORWARD -i wg+ -j ACCEPT
-A FORWARD -o eth0 -j ACCEPT
-A FORWARD -o eth1 -j ACCEPT
-A FORWARD -o br0 -j ACCEPT
-A FORWARD -o wg+ -j ACCEPT
-A FORWARD -i ppp0 -j logdrop-0
```

```
-A FORWARD -i ppp1 -j logdrop-0
-A FORWARD -i ppp500 -j ACCEPT
-A FORWARD -i ppp501 -j ACCEPT
-A FORWARD -i ppp502 -j ACCEPT
-A FORWARD -i ppp503 -j ACCEPT
-A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p icmp -j icmp-routing
-A OUTPUT -o ppp0 -j ACCEPT
-A OUTPUT -o ppp1 -j ACCEPT
-A OUTPUT -o eth0 -j ACCEPT
-A OUTPUT -o eth1 -j ACCEPT
-A OUTPUT -o br0 -j ACCEPT
-A OUTPUT -o wg+ -j ACCEPT
-A icmp-routing -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A icmp-routing -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A icmp-routing -p icmp -m icmp --icmp-type 12 -j ACCEPT
-A limit-ssh-0 -m recent --update --seconds 20 --hitcount 3 --name limit-
ssh-0 --mask 255.255.255.255 --rsource -j logdrop-ssh-0
-A limit-ssh-0 -m recent --set --name limit-ssh-0 --mask 255.255.255.255 --
rsource -j ACCEPT
-A logdrop-0 -m limit --limit 1/sec -j LOG
-A logdrop-0 -j DROP
-A logdrop-ssh-0 -m limit --limit 1/sec -j LOG
-A logdrop-ssh-0 -j DROP
COMMIT
# Completed on Fri Nov 15 14:51:36 2019
```

設定例

DNAT(Port Forwarding)

WAN 側から TCP/10080 に来たパケットを、LAN 内の 192.168.253.1:80 へ転送するルールを設定してみます。

private/dnat.json

```
{
  "dnat": [
    {
      "in": "WAN",
      "service": {
        "proto": "tcp",
        "port": "10080"
      },
```

```
      "to-addr": "192.168.253.1",
      "to-port": 80
    }
  ]
}
```

これを読み込むために、optional/main.json を変更します。

optional/main.json

```
{
  "description": "Main firewall",

  "import": [
    "base",
    "filter",
    "dnat"    # <--- 追加
  ]
}
```

awall を再設定します。

```
root@plum:~# awall activate -f
Warning: firewall not enabled for inet6
ipset creation failed: awall-masquerade
```

iptables のルールを確認すると、下記 **PREROUTING** エントリが追加されていることが確認できます。

```
*nat
:PREROUTING ACCEPT [6:972]
:INPUT ACCEPT [6:972]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:awall-masquerade - [0:0]
-A PREROUTING -i ppp0 -p tcp -m tcp --dport 10080 -j DNAT --to-destination
192.168.253.1:80
-A PREROUTING -i ppp1 -p tcp -m tcp --dport 10080 -j DNAT --to-destination
192.168.253.1:80
... 以下略
```

1)
Alpine Linux で使用されている firewall です