目次

Firewall の設定 (Alpine Wall)

MA-S1xx シリーズ、MA-X3xx シリーズ及び MA-E3xxシリーズのVer5.0.0以降では、Firewall(iptables) の設定にAlpine Wall[1]を利用しています。
WebUI Firewall 設定 のページでも設定できます。

初期設定

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

```
root@gemini:/etc/awall# ls -lR
.:
total 0
lrwxrwxrwx 1 root root  29 Nov 15  2019 main.json ->
/etc/awall/optional/main.json
drwxr-xr-x 2 root root  32 Nov 18  2019 optional
drwxr-xr-x 2 root root 102 Jul 20  2020 private

./optional:
total 1
-rw-r--r-- 1 root root 143 Nov 18  2019 main.json

./private:
total 3
-rw-r--r-- 1 root root 471 Nov 18  2019 base.json
-rw-r--r-- 1 root root  20 Nov 15  2019 dnat.json
-rw-r--r-- 1 root root 197 Nov 15  2019 filter.json
-rw-r--r-- 1 root root  20 Nov 15  2019 snat.json
-rw-r--r-- 1 root root 161 Jul 20  2020 zone.json
```

zone.json で、インターフェース毎のゾーン設定を記述しています。

zone.json

```
{
    "description": "Base zones",
    "zone": {
        "WAN": { "iface": [ "ppp0", "ppp1", "usb0", "wlan0" ] },
        "LAN": { "iface": [ "eth0", "br0", "ppp100", "wg+" ] }
    }
}
```

base.json で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 policies",

    "zone": {
        "Closed" : { "iface": [ "ppp500", "ppp501" ] }
    },

    "policy": [
        { "in": "_fw", "out": "WAN", "action": "accept" },
        { "in": "LAN", "action": "accept" },
        { "out": "LAN", "action": "accept" },
        { "in": "WAN", "action": "drop" },
        { "in": "Closed", "action": "accept" },
        { "out": "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。

```
# Completed on Thu Dec 23 18:03:47 2021
# Generated by iptables-save v1.8.4 on Thu Dec 23 18:03:47 2021
*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 -i wlan0 -p tcp -m tcp --dport 22 -j limit-ssh-0
-A INPUT -i usb0 -p tcp -m tcp --dport 22 -j limit-ssh-0
-A INPUT -i ppp0 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i ppp1 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i wlan0 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i usb0 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i ppp0 -p udp -m udp --dport 23081 -j ACCEPT
-A INPUT -i ppp1 -p udp -m udp --dport 23081 -j ACCEPT
-A INPUT -i wlan0 -p udp -m udp --dport 23081 -j ACCEPT
-A INPUT -i usb0 -p udp -m udp --dport 23081 -j ACCEPT
-A INPUT -p icmp -j icmp-routing
-A INPUT -i eth0 -j ACCEPT
-A INPUT -i br0 -j ACCEPT
-A INPUT -i ppp100 -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 wlan0 -j logdrop-0
-A INPUT -i usb0 -j logdrop-0
-A INPUT -i ppp500 -j ACCEPT
-A INPUT -i ppp501 -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 br0 -j ACCEPT
-A FORWARD -i ppp100 -j ACCEPT
-A FORWARD -i wg+ -j ACCEPT
-A FORWARD -o eth0 -j ACCEPT
-A FORWARD -o br0 -j ACCEPT
-A FORWARD -o ppp100 -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 wlan0 -j logdrop-0
-A FORWARD -i usb0 -j logdrop-0
-A FORWARD -i ppp500 -j ACCEPT
-A FORWARD -i ppp501 -j ACCEPT
-A FORWARD -o ppp500 -j ACCEPT
-A FORWARD -o ppp501 -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 wlan0 -j ACCEPT
-A OUTPUT -o usb0 -j ACCEPT
-A OUTPUT -o eth0 -j ACCEPT
-A OUTPUT -o br0 -j ACCEPT
-A OUTPUT -o ppp100 -j ACCEPT
-A OUTPUT -o wg+ -j ACCEPT
-A OUTPUT -o ppp500 -j ACCEPT
-A OUTPUT -o ppp501 -j ACCEPT
```

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-port": 80
    }
  ]
}
```

awall を再設定します。

```
root@gemini:/# awall activate -f
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 [0:0]
:INPUT ACCEPT [0:0]
: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
-A PREROUTING -i usb0 -p tcp -m tcp --dport 10080 -j DNAT --to-destination
192.168.253.1:80
-A PREROUTING -i wlan0 -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