Extended CACL(control plane ACL)

By modifying the configuration file "iptables.json", the user can customize the filter rules of the control plane, which are loaded into iptables.

The configuration file should include all extended rules written in iptables commands. When the switch boots up or service reloads, the rules in this file will be applied into iptables, located just before existing rules of SONiC CACL rules, which are also inserted into iptables.

The precedence of rules matching will be:

SONiC default control plane rules (system reserved)
Extended CACL rules
SONiC CACL rules (Refer to Control Plane ACL)

Topology:

0223_article.png

Procedure:
Step 1. Add IP address to front port and management interface eth0 (Refer to Management and front port IPv4/IPv6 Address). This step is for verifying the results.

```
admin@7726:~$ sudo config interface ip add eth0 192.168.97.16/16
admin@7726:~$ sudo config interface ip add Ethernet0 10.0.0.1/24
```

Step 2. Create a file named "iptables.json" and add desired iptables rules into this file. Example as follows:

```
admin@7726:~$ sudo vi iptables.json
{
    "ipv4":[
        "-A INPUT -i eth0 -p tcp --dport 443 -j ACCEPT",
        "-A INPUT -p tcp --dport 443 -j DROP",
        "-A INPUT -i eth0 -p tcp --dport 8080 -j ACCEPT",
        "-A INPUT -p tcp --dport 8080 -j DROP"
    ],
    "ipv6":[
    ]
}
```

This example applies the rules that accept IPv4 TCP packets from eth0 to port 443 and 8080, and will drop the packets from other ports(front ports) to port 443 and 8080.
Step 3. Copy this file to /etc/sonic/iptables.json

```
admin@7726:~$ sudo cp iptables.json /etc/sonic/iptables.json
```

Step 4. Reboot device or restart service "caclmgrd" to load config, and then check iptables

```
admin@7726:~$ sudo service caclmgrd restart
admin@7726:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -s 127.0.0.1/32 -i lo -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A INPUT -p udp -m udp --dport 67:68 -j ACCEPT
-A INPUT -p udp -m udp --dport 546:547 -j ACCEPT
-A INPUT -p udp -m udp --dport 4789 -j ACCEPT
```

```
-A INPUT -p udp -m udp --sport 49152:65535 --dport 3784 -j ACCEPT
-A INPUT -p udp -m udp --dport 3785 -j ACCEPT
-A INPUT -p udp -m udp --sport 49152:65535 --dport 4784 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 179 -j ACCEPT
-A INPUT -p tcp -m tcp --sport 179 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 443 -j ACCEPT <---------------- rule
loaded from file
-A INPUT -p tcp -m tcp --dport 443 -j DROP <------------------------- rule
loaded from file
-A INPUT -i eth0 -p tcp -m tcp --dport 8080 -j ACCEPT <-------------- rule
loaded from file
-A INPUT -p tcp -m tcp --dport 8080 -j DROP <------------------------- rule
loaded from file
-A INPUT -d 10.0.0.0/32 -j DROP
-A INPUT -m ttl --ttl-lt 2 -j ACCEPT
The customized rules are added
Step 5. If user wants to modify the external rules, they can edit the
"iptables.json" file. After the modification is done, reboot device or restart
service "caclmgrd" (as in Step 4) to apply the updated rules.

Step 6. To remove all rules applied via external file, user can remove the
/etc/sonic/iptables.json file, then reboot device or restart service "caclmgrd"
(as in Step 4). Leaving the iptables.json file empty and re-applying the
configuration can achieve the same goal.

Result:
To check if the rules work, scan listen ports with external devices using nmap:

admin@host-01:~$ sudo nmap -v 192.168.97.16
...omitted...
Host is up (0.00030s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
443/tcp open https
8080/tcp open http-proxy
8888/tcp open sun-answerbook
...omitted...

admin@host-02:~$ sudo nmap -v 10.0.0.1
...omitted...
Host is up (0.0026s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
443/tcp filtered https
8080/tcp filtered http-proxy
8888/tcp open sun-answerbook
...omitted...
port 443 and 8080 are "filtered" on front port interface, "open" on mgmt port
interface
```