Firewall - Rule persistence

- Firewall rule
- Categories
- How it is handled in RDKB
- Steps to persist the new rules
    - If to replace all the rules with your set of rules
    - To have new rules on top of existing rules
    - Manual adding of firewall rules on board
- Limitations

Firewall rule

- Firewall rules defines what kind of Internet traffic is allowed or blocked
- Firewall Rules examine the control information in individual packets.
- These rules either block or allow the packets based on rules that are defined on the device or in code

Categories

- 4 categories of rules

    a. raw - To route raw packets
    b. mangle - QoS configuration
    c. nat - routing for IPv4 LAN , ipv6
    d. filter - filtering internal packets before forward

How it is handled in RDKB

- 10_firewall exe is responsible for firewall events and it registers for sysevent callback with service name as firewall.
- Handler script is firewall_log_handle.sh.
- If any firewall event occurs sysevent is triggered with firewall-restart event name.
- On firewall-restart event service_start() method gets called.
- Ip4table and Ip6table rules are prepared by reading data from shared memory, written into /tmp/.ipt and /tmp/.ipt_v6 files respectively.
- Iptable rules are restored using these files.

Steps to persist the new rules

If to replace all the rules with your set of rules

1. Create a script and place it under ./meta-rdk-broadband/recipes-ccsp/util/utopia
2. Add and install in utopia.bb file

```
SRC_URI += "file://iptables.sh"

install -m 755 ${WORKDIR}/iptables.sh ${D}${sysconfdir}
```

3. In firewall.c file , create your function to invoke the script instead of service_start(); in main()

```
static int new_firewall()

{

system("sh /etc/iptables.sh");

return 0;

}
```

To have new rules on top of existing rules

1. Install your script under /etc
2. Invoke your script from firewall_log_handle.sh file

```
/fss/gw/usr/bin/GenFWLog -c
/fss/gw/usr/bin/firewall $*
/etc/fw_iptables.sh
/fss/gw/usr/bin/GenFWLog -gc
```

3. In script , the rules has to be cleared/flushed before adding . During firewall restarts , if the rules are not cleared before adding , the same rules will be listed multiple times in "iptables -L / -S" .

- Manual adding of firewall rules on board

1. Place all your new rules in a script under /nvram
2. In firewall_log_handle.sh file , add a condition as below

```
if [ -f /nvram/<file>.sh ] then
  . /nvram/<file>.sh
fi
```

3. Suppose , if any script already running with few set of ip rules (from source code) which is invoked in firewall_log_handle.sh file , follow the below steps
4. copy the existing script from /<original-path> to /nvram
5. The changes (adding new rules manually) should be done in the script under /nvram
6. In firewall_log_handle.sh file , add the condition as

```
if [ -f /nvram/<file>.sh ] then
  . /nvram/<file>.sh
else
  . /<original-path>/<file>.sh
fi
```

7. Once the complete verification is done , the script file from /nvram has to be deleted .

Limitations

1. We should not add/remove the rules directly in firewall.c file since it is common to all other boards
2. We can do by enabling DISTRO_FEATURE . But again we should be knowing the exact rules to remove/add . This should not affect the basic functionalities like board bring up , components bring up , routing packets, etc.,