NAME

xtables-compat – compat tools to migrate from iptables to nftables

DESCRIPTION

xtables-compat is set of tools to help the system administrator migrate the ruleset from **iptables(8)**, **ip6tables(8)**, **arptables(8)**, and **ebtables(8)** to **nftables(8)**.

The **xtables-compat** set is composed of several commands:

- iptables-compat
- iptables-compat-save
- iptables-compat-restore
- ip6tables-compat
- ip6tables-compat-save
- ip6tables-compat-restore
- arptables-compat
- ebtables-compat

These tools use the libxtables framework extensions and hook to the nf_tables kernel subsystem using the **nft_compat** module.

USAGE

The compat tools set allows you to manage the nf_tables backend using the native syntax of **iptables(8)**, **ip6tables(8)**, **arptables(8)**, and **ebtables(8)**.

You should use the compat tools exactly the same way as you would use the corresponding original tool.

Adding a rule will result in that rule being added to the nf_tables kernel subsystem instead. Listing the ruleset will use the nf_tables backend as well.

When these tools were designed, the main idea was to replace each legacy binary with a symlink to the corresponding compat tool, for example:

```
/sbin/iptables  --> /usr/sbin/iptables-compat
/sbin/ip6tables --> /usr/sbin/ip6tables-compat
/sbin/arptables --> /usr/sbin/arptables-compat
/sbin/ebtables  --> /usr/sbin/ebtables-compat
```

EXAMPLES

One basic example is creating the skeleton ruleset in nf_tables from the compat tools, in a fresh machine:

```
root@machine:~# iptables-compat -L
[...]
root@machine:~# ip6tables-compat -L
[...]
root@machine:~# arptables-compat -L
[...]
root@machine:~# ebtables-compat -L
[...]
root@machine:~# nft list ruleset
table ip filter {
```

```
        chain INPUT {
                type filter hook input priority 0; policy accept;
        }

        chain FORWARD {
                type filter hook forward priority 0; policy accept;
        }

        chain OUTPUT {
                type filter hook output priority 0; policy accept;
        }
}
table ip6 filter {
        chain INPUT {
                type filter hook input priority 0; policy accept;
        }

        chain FORWARD {
                type filter hook forward priority 0; policy accept;
        }

        chain OUTPUT {
                type filter hook output priority 0; policy accept;
        }
}
table bridge filter {
        chain INPUT {
                type filter hook input priority -200; policy accept;
        }

        chain FORWARD {
                type filter hook forward priority -200; policy accept;
        }

        chain OUTPUT {
                type filter hook output priority -200; policy accept;
        }
}
table arp filter {
        chain INPUT {
                type filter hook input priority 0; policy accept;
        }

        chain FORWARD {
                type filter hook forward priority 0; policy accept;
        }

        chain OUTPUT {
                type filter hook output priority 0; policy accept;
        }
}
```

(please note that in fresh machines, listing the ruleset for the first time results in all tables an chain being created).

To migrate your complete filter ruleset, in the case of **iptables(8)**, you would use:

```
root@machine:~# iptables-save > myruleset              # reads from x_tables
root@machine:~# iptables-compat-restore myruleset  # writes to nf_tables
```

LIMITATIONS

You should use **Linux kernel >= 4.2**.

Some (few) extensions may be not supported (or fully-supported) for whatever reason (for example, they were considered obsolete).

To get up-to-date information about this, please head to **http://wiki.nftables.org/**.

SEE ALSO

nft(8), **xtables-translate(8)**

AUTHORS

The nftables framework is written by the Netfilter project (https://www.netfilter.org).

This manual page was written by Arturo Borrero Gonzalez <arturo@debian.org> for the Debian project, but may be used by others.