Red Hat Enterprise Linux Release 9.2 Manual Pages on 'iptables-restore-translate.8' command

$ man iptables-restore-translate.8

IPTABLES-TRANSLATE(8)   System Manager's Manual   IPTABLES-TRANSLATE(8)

NAME

    iptables-translate ? translation tool to migrate from iptables to nfta?

    bles

    ip6tables-translate ? translation tool to migrate from ip6tables to

    nftables

DESCRIPTION

    There is a set of tools to help the system administrator translate a

    given ruleset from iptables(8) and ip6tables(8) to nftables(8).

    The available commands are:

    ? iptables-translate

    ? iptables-restore-translate

    ? ip6tables-translate

    ? ip6tables-restore-translate

USAGE

    They take as input the original iptables(8)/ip6tables(8) syntax and

    output the native nftables(8) syntax.

    The iptables-restore-translate tool reads a ruleset in the syntax pro?

    duced by iptables-save(8). Likewise, the ip6tables-restore-translate

    tool reads one produced by ip6tables-save(8). No ruleset modifications

    occur, these tools are text converters only.

    The iptables-translate reads a command line as if it was entered to

    iptables(8), and ip6tables-translate reads a command like as if it was

entered to ip6tables(8).

EXAMPLES

Basic operation examples.

Single command translation:

root@machine:~# iptables-translate -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT

nft add rule ip filter INPUT tcp dport 22 ct state new counter accept

root@machine:~# ip6tables-translate -A FORWARD -i eth0 -o eth3 -p udp -m multiport --dports 111,222 -j ACCEPT

nft add rule ip6 filter FORWARD iifname eth0 oifname eth3 meta l4proto udp udp dport { 111,222} counter accept

Whole ruleset translation:

root@machine:~# iptables-save > save.txt

root@machine:~# cat save.txt

Generated by iptables-save v1.6.0 on Sat Dec 24 14:26:40 2016

*filter

:INPUT ACCEPT [5166:1752111]

:FORWARD ACCEPT [0:0]

:OUTPUT ACCEPT [5058:628693]

-A FORWARD -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT

COMMIT

Completed on Sat Dec 24 14:26:40 2016

root@machine:~# iptables-restore-translate -f save.txt

Translated by iptables-restore-translate v1.6.0 on Sat Dec 24 14:26:59 2016

add table ip filter

add chain ip filter INPUT { type filter hook input priority 0; }

add chain ip filter FORWARD { type filter hook forward priority 0; }

add chain ip filter OUTPUT { type filter hook output priority 0; }

add rule ip filter FORWARD tcp dport 22 ct state new counter accept

root@machine:~# iptables-restore-translate -f save.txt > ruleset.nft

root@machine:~# nft -f ruleset.nft

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;

        tcp dport ssh ct state new counter packets 0 bytes 0 accept

    }

    chain OUTPUT {

        type filter hook output priority 0; policy accept;

    }

}
```

LIMITATIONS

Some (few) extensions may be not supported (or fully-supported) for

whatever reason (for example, they were considered obsolete, or we

didn't have the time to work on them).

There are no translations available for ebtables(8) and arptables(8).

To get up-to-date information about this, please head to

https://wiki.nftables.org/.

SEE ALSO

nft(8), iptables(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@netfil?

ter.org>.

This documentation is free/libre under the terms of the GPLv2+.