IPTables

Overview

List iptable chains

> sudo iptables -L |grep ^Chain

List Chain

> sudo iptables -L <chain>

List Chain verbose

> sudo iptables -L <chain> -v

List Drops

> sudo iptables -L |grep DROP or sudo iptables -L |grep REJECT

```
DROP       all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere             /* kubernetes firewall for dropping marked
packets */ mark match 0x8000/0x8000
DROP       ipencap--  anywhere               anywhere             /* cali:_wjq-Yrma8Ly1Svo */ /* Drop IPIP
packets from non-Calico hosts */
DROP       all  --  anywhere             anywhere             /* cali:IP8OSQl0VCkv3ZMk */ /* Unknown interface
*/
DROP       all  --  anywhere             anywhere             /* cali:Keps4Q7WlFrK90sC */ /* Unknown interface
*/
DROP       all  --  anywhere             anywhere             /* cali:USBWs6LRLyjceqok */ ctstate INVALID
DROP       all  --  anywhere             anywhere             /* cali:b5-lDh3P2YiCwdLE */ /* Drop if no
profiles matched */
DROP       all  --  anywhere             anywhere             /* cali:GLyML315f8bji4AQ */ /* Unknown endpoint */
DROP       all  --  anywhere             anywhere             /* cali:Lz2VNTVi4Ojv-dp9 */ /* Unknown interface
*/
DROP       all  --  anywhere             anywhere             /* cali:7b0UnS82qXoUi64w */ ctstate INVALID
DROP       all  --  anywhere             anywhere             /* cali:4Z4bC8wUf4-oIegz */ /* Drop if no
profiles matched */
```

Save iptables to file

> sudo **iptables-save** > iptables.txt

Restore iptables

> sudo iptables-restore iptables.txt

Add a rule

> sudo iptables -A INPUT -j ACCEPT -p tcp --destination-port 30500

Sample Set of Rules