Iptables commands

Iptable is an interface of the command line used for setting-up and maintaining tables for Netfilter Firewall in IPv4, added within the Linux kernel. The firewall will match packets with some rules described in the tables and take the defined action on any feasible match.

Let's discuss some features.

- Tables are the chain's set name.
- Chain is a set of many rules.
- Rule can be defined as any condition used for matching packet.
- Target can be defined as any action taken if any feasible rule matches. QUEUE, DROP, ACCEPT are some of the examples of the target.
- Policy is a default operation taken in no match case with an inbuilt chain and could be DROP or ACCEPT.

Syntax:

1. iptables --table TABLE -A/-C/-D? CHAIN rule --jump Target

Types of Tables of iptables

Tables can be categorized into five different types:

- **Filter:** Filter tables are the default applied table for the filtering of packets. It contains chains such as FORWARD, INPUT, and OUTPUT.
- **Nat:** Net tables are connected to **Network Address Translation**. It contains POSTROUTING and PREROUTING chains.
- **Mangle:** These types of tables are used for particular packet alteration. Its inbuilt chains contain OUTPUT and PREROUTING.
- **Raw:** It configures exceptions through connection tracking. Its built-in chains contain OUTPUT and PREROUTING.
- **Security:** These tables are used for MAC (Mandatory Access Control).

Types of Chains of iptables

Some built-in chains of iptable can be categorized into the following types:

- **INPUT:** INPUT chains define rules set for packets intended to sockets of localhost.
- **FORWARD:** FORWARD chains used for various packets routed from the device.
- **OUTPUT:** OUTPUT chains used for locally produced packets, specified to be set outside.
- **PREROUTING:** PREROUTING chains are used for changing packets as these packets arrive.
- **POSTROUTING:** POSTROUTING chains are used for changing packets as these packets are leaving.

Types of Options of iptables

1. -A, -append: It can append to any chain given in the parameters.

Syntax:

```
1. iptables [-t table] --append [chain] [parameters]
```

Example: The append command can drop each traffic coming over a port.

```
1. iptables -t filter --append INPUT -j DROP
```

2. -D -delete: It can delete rules through a particular chain.

Syntax:

```
1. iptables [-t table] --delete [chain] [rule_number]
```

Example: The delete command can delete rule 2 through the INPUT chain.

```
1. iptables -t filter --delete INPUT 2
```

3. -C, -check: It can check when any rule is available within a chain or not. This command will return 0 when the rule endures and provide 1 when it doesn't.

Syntax:

1. iptables [-t table] --check [chain] [parameters]

Example: This command can check whether a particular rule is available within the INPUT chain.

1. iptables -t filter --check INPUT -s 192.168.1.123 -j DROP

Types of parameters of iptables

Iptables command facilitates parameters that are used for matching a packet and implement the particular actions. Some important parameters are discussed as follows:

1. -p, -proto: It is a protocol that any packet pursues. Feasible values can be ssh, icmp, udp, tcp, etc.

Syntax:

1. iptables [-t table] -A [chain] -p {protocol_name} [target]

Example: The protocol parameter can append any rule within the INPUT chain for dropping every udp packet.

1. iptables -t filter -A INPUT -p udp -j DROP

2. -s, -source: It is applied for matching with the packet's source address.

Syntax:

1. iptables [-t table] -A [chain] -s {source_address} [target]

Example:

The source parameter can append the rules within the INPUT chain for accepting each packet originating through 192.168.1.230.

1. iptables -t filter -A INPUT -s 192.168.1.230 -j ACCEPT

3. -d, -destination: It is used for matching with the packet's destination address.

Syntax:

1. iptables [-t table] -A [chain] -d {destination_address} [target]

Example: The destination parameter can append the rules within the OUTPUT chain for dropping each packet intended for 192.168.1.123.

1. iptables -t filter -A OUTPUT -d 192.168.1.123 -j DROP

4. -i, -in-interface: It can match the packets with the particular in-interface and hold the action.

Syntax:

1. iptables [-t table] -A [chain] -i {interface} [target]

Example: The interface parameter can append the rules within the INPUT chain for dropping each packet intended to the wireless interface.

1. iptables -t filter -A INPUT -i wlan0 -j DROP

5. -o, -out-interface: It can match the packets along with the particular out-interface.

6. -j, -jump: The jump parameter defines an operation to be taken over a match.

Syntax:

1. iptables [-t table] -A [chain] [parameter] -j [target]

Example: The jump parameter can add the rules within the FORWARD chain for dropping each packet.

1. iptables -t filter -A FORWARD -j DROP