Iptables

Инфо:

Iptables - это инструмент для управления файрволом в операционной системе Linux. Он позволяет настраивать правила безопасности и контролировать трафик сети.

В Ubuntu iptables является утилитой уровня ядра и доступен по умолчанию. В Ubuntu 22 (и других версиях Ubuntu) установка iptables не требуется, так как она уже включена в ядро Linux и доступна изначально.

Iptables предоставляет мощные возможности фильтрации и маршрутизации пакетов в Linux. Он работает на уровне ядра и используется для настройки правил файрвола и сетевых политик.

Применение:

1. Просмотр текущих правил:

```
ptables -L
```

имер вывода:

```
hain INPUT (policy ACCEPT)
arget     prot opt source               destination
CCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ROP       tcp  --  anywhere             anywhere             tcp dpt:http

hain FORWARD (policy ACCEPT)
arget     prot opt source               destination

hain OUTPUT (policy ACCEPT)
arget     prot opt source               destination
```

```
епочки (Chain):
hain INPUT: Цепочка, которая обрабатывает входящий трафик (пакеты, направленные к системе).
```

```
Chain FORWARD: Цепочка, которая обрабатывает пересылаемый трафик (пакеты, которые должны быть переданы через систему).
Chain OUTPUT: Цепочка, которая обрабатывает исходящий трафик (пакеты, отправляемые системой).

Столбцы для каждой цепочки:
target: Цель, то есть действие, которое будет выполнено с пакетом, если он соответствует правилу.
prot: Протокол, к которому относится правило (например, TCP, UDP).
opt: Опции, связанные с протоколом или действием.
source: Исходный адрес или сеть, откуда ожидается входящий трафик.
destination: Целевой адрес или порт, куда направляется трафик.

Из примера. В цепочке INPUT есть два правила:
Первое правило разрешает входящий TCP-трафик на порт SSH (22) с любого источника.
Второе правило блокирует входящий TCP-трафик на порт HTTP (80) с любого источника.
Цепочка FORWARD не содержит правил.
Цепочка OUTPUT не содержит правил.
```

В iptables есть несколько возможных состояний для параметра `target` в правилах. Некоторые из наиболее распространенных состояний `target` включают:

1. `ACCEPT`: Пакет будет принят и разрешен.
2. `DROP`: Пакет будет отброшен и удален, без отправки какого-либо уведомления отправителю.
3. `REJECT`: Пакет будет отброшен и отправлено уведомление отправителю о том, что пакет был отклонен.
4. `LOG`: Пакет будет принят, но информация о пакете будет записана в системный журнал или файл журнала для целей мониторинга и отладки.
5. `DNAT`: Изменение адреса назначения (Destination NAT) позволяет перенаправить пакеты на другой адрес и/или порт.
6. `SNAT`: Изменение адреса источника (Source NAT) позволяет заменить исходный адрес пакета на другой адрес и/или порт.
7. `MASQUERADE`: Вид NAT, который заменяет исходный адрес источника на адрес интерфейса, через который пакет покидает систему.
8. `REDIRECT`: Перенаправление пакетов на локальный порт или сокет.
9. `MARK`: Пометка пакетов для дальнейшей обработки другими инструментами или правилами.

Каждое состояние `target` в iptables выполняет определенное действие с пакетом, определенным правилом. Выбор подходящего состояния `target` зависит от ваших потребностей и требований конкретной ситуации.

2. Очистка существующих правил:

```
iptables -F
```

3. Закрыть \ открыть доступа к порту:

```
ptables -A INPUT -p tcp --dport <порт> -j DROP
ptables -A INPUT -p tcp --dport <порт> -j ACCEPT
```

4. Разрешение доступа только для определенных IP-адресов (вайтлист):

```
ptables -A INPUT -p tcp --dport <порт> -s <IP-адрес> -j ACCEPT
```

имер:

```
ptables -A INPUT -p tcp --dport 51821 -s 192.168.1.100 -j ACCEPT
```

манда добавляет правило в цепочку INPUT, которая разрешает входящий TCP-трафик на рт 51821 только от указанного IP-адреса.

5. Сохранение и загрузка правил iptables:

```
ptables-save > /etc/iptables/rules.v4 #записать изменения в файл
ptables-restore < /etc/iptables/rules.v4 #загрузить правила в iptables
```

Дополнительно:

обы правила iptables из файла `/etc/iptables/rules.v4` автоматически применялись при грузке системы, можно использовать инструменты настройки системы для запуска манды `iptables-restore` при старте.

пример можно настроить службу `netfilter-persistent` или через `systemd`.

стройка `netfilter-persistent`:

```
pt install netfilter-persistent
etfilter-persistent reload #применить правила iptables без перезагрузки системы
```

тозагрузка netfilter-persistent при старте системы:

```
ystemctl enable netfilter-persistent
```

Настройка через `systemd`:

```
im /etc/systemd/system/iptables.service
```

бавить в файл службы текст:

```
Unit]
escription=Load iptables rules
fter=network.target

Service]
ype=oneshot
xecStart=/sbin/iptables-restore /etc/iptables/rules.v4

Install]
antedBy=multi-user.target
```

лее можно загрузить и активировать службу, она будет запускаться при старте системы:

```
udo systemctl daemon-reload
udo systemctl enable iptables.service
```

я применения правил без перезапуска системы можно выполнить:

```
ystemctl start iptables.service
```

лучить список правил с номерами:

```
ptables -L INPUT --line-numbers
```

алить правило по номеру:

```
ptables -D INPUT <номер>
```

Revision #13
Created 7 May 2023 21:39:48 by Maru
Updated 11 May 2023 14:15:44 by Maru