Использование утилиты «ebtables-legacy»

Назначение документа

Данный документ описывает особенности использования утилиты «ebtables-legacy-legacy» в Продукте «С-Терра Шлюз», а также кратко поясняет важные моменты подсистемы netfilter ядра Linux.

Краткое описание утилиты «ebtables-legacy»

Утилита «ebtables» - это инструмент для настройки фильтрации и трансляции сетевых адресов на сетевых интерфейсах и программных мостах Linux. Утилита «ebtables-legacy», в отличие от «iptables», работает, преимущественно, на втором (канальном) уровне сетевого стека, но также является пользовательским интерфейсом к подсистеме netfilter ядра Linux.

Краткое описание архитектуры подсистемы «netfilter» ядра Linux

Утилита «ebtables-legacy» содержит три таблицы (FILTER, NAT, BROUTE) и пять цепочек (PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING), принадлежащих подсистеме «netfilter» Таблицы определяют действия над пакетами, а цепочки – место совершения действия относительно пути прохождения пакетов и политику обработки. Каждая таблица состоит из набора цепочек, например, в таблице filter находятся три цепочки INPUT, FORWARD, OUTPUT.

Политика пакетов в цепочках

У каждой цепочки есть политика обработки пакетов. Политика может быть разрешающая (ACCEPT) – разрешено все, что не запрещено, или блокирующая (DROP) – запрещено все, что не разрешено. Посмотреть политику во всех цепочках таблицы filter утилиты «ebtables-legacy» можно при помощи команды:

```
root@sterragate:~# ebtables-legacy -L
Bridge table: filter

Bridge chain: INPUT, entries: 0, policy: ACCEPT

Bridge chain: FORWARD, entries: 0, policy: ACCEPT

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT
```

Назначение таблиц

1. FILTER – применяется для фильтрации фреймов или пакетов и содержит три цепочки: INPUT (для фреймов/пакетов, предназначенных криптошлюзу), FORWARD (для маршрутизируемых криптошлюзом фреймов/пакетов), OUTPUT (для локально сгенерированных фреймов/пакетов криптошлюзом).
2. NAT – применяется для выполнения трансляции mac-адресов и содержит три встроенные цепочки: PREROUTING (для изменения фрейма сразу после поступления на криптошлюз), OUTPUT (для изменения локально сгенерированных фреймов), POSTROUTING (для изменения фреймов перед их отправкой с криптошлюза).

© 2003-2025 S-Terra CSP

3. BROUTE– используется для маршрутизации внутри самого криптошлюза и содержит одну встроенную цепочку: BROUTING. Данная таблица используется для того, чтобы определить, что сделать с фреймом: действие DROP означает, что фрейм должен быть перенаправлен (выбор перенаправления решает пользователь: фрейм можно перенаправить на другой интерфейс или, например, на сетевой уровень, где работает утилита «iptables»), действие ACCEPT означает, что фрейм должен пойти по стандартному пути, а именно, отправиться на bridge-интерфейс.

Использование утилиты «ebtables-legacy»

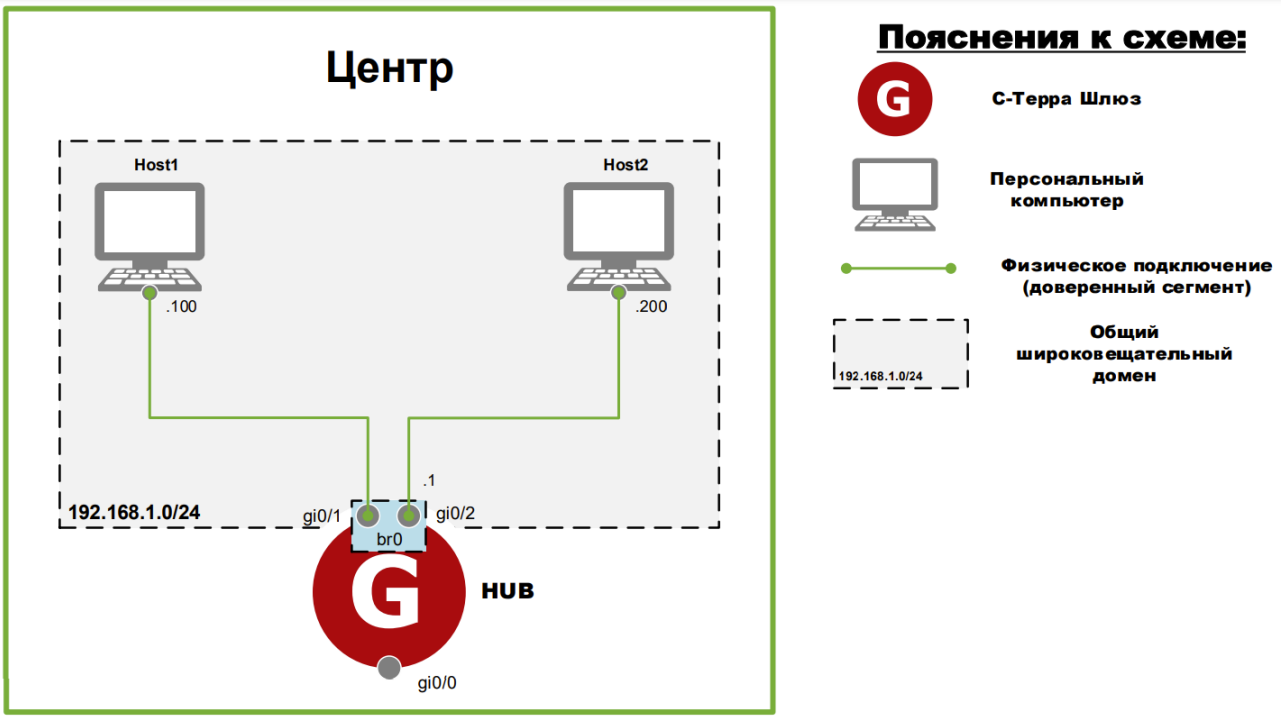


Рисунок 1. Схема взаимодействия

Предположим, пользователю необходимо объединить два оконечных устройства в одну подсеть при помощи криптошлюза и осуществлять фильтрацию трафика между данными устройствами. Для того, чтобы объединить устройства в одну подсеть, необходимо создать bridge-интерфейс на криптошлюзе и добавить в него сетевые интерфейсы, к которым подключены оконечные устройства.

Для реализации схемы взаимодействия и фильтрации трафика при помощи утилиты «ebtables-legacy» на криптошлюзе необходимо произвести следующие настройки:

1. Привести файл `/etc/network/interfaces` к следующему виду:

```
############################################################
# CAUTION: lines under special marker: ###netifcfg-*###
# contains autogenerated information. You can add/modify
# lines outside of those markers
############################################################

# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d

# loopback configuration
auto lo
iface lo inet loopback
```

```
auto eth0
iface eth0 inet manual

auto eth1
iface eth1 inet manual

auto br0
iface br0 inet static
address 192.168.1.1
netmask 255.255.255.0
bridge-ports eth0 eth1

allow-hotplug eth2
iface eth2 inet dhcp

###netifcfg-begin###
###netifcfg-end###
```

2. Далее, при помощи утилиты «ebtables-legacy» осуществить фильтрацию трафика. Например, запретить передачу ICMP-пакетов между устройствами:

```
root@sterragate:~# ebtables-legacy -A FORWARD --ip-src 192.168.1.100 --ip-dst
192.168.1.200 -p ipv4 --ip-proto icmp -j DROP
```

3. Запретить подключение по протоколу SSH устройству Host2 к устройству Host1 (при этом, у устройства Host1 останется возможность подключения по SSH к устройству Host2):

```
root@sterragate:~# ebtables-legacy -A FORWARD --ip-src 192.168.1.200 --ip-dst
192.168.1.100 -p ipv4 --ip-proto tcp --ip-destination-port 22 -j DROP
```

4. Аналогичным образом можно добавлять правила применительно к протоколу UDP:

```
root@sterragate:~# ebtables-legacy -A FORWARD --ip-src 192.168.1.200 --ip-dst
192.168.1.100 -p ipv4 --ip-proto udp --ip-destination-port 67 -j DROP
```

5. Для того, чтобы посмотреть правила в таблице «filter», необходимо воспользоваться командой:

```
root@sterragate:~# ebtables-legacy -L
```

```
Bridge table: filter

Bridge chain: INPUT, entries: 0, policy: ACCEPT

Bridge chain: FORWARD, entries: 3, policy: ACCEPT
-p IPv4 --ip-src 192.168.1.100 --ip-dst 192.168.1.200 --ip-proto icmp -j DROP
-p IPv4 --ip-src 192.168.1.200 --ip-dst 192.168.1.100 --ip-proto tcp --ip-dport
22 -j DROP
-p IPv4 --ip-src 192.168.1.200 --ip-dst 192.168.1.100 --ip-proto udp --ip-dport
67 -j DROP

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT
```

6. Просмотреть счётчики на каждом правиле можно при помощи команды:

```
root@sterragate:~# ebtables-legacy -L --Lc
```

```
Bridge table: filter

Bridge chain: INPUT, entries: 0, policy: ACCEPT

Bridge chain: FORWARD, entries: 3, policy: ACCEPT
-p IPv4 --ip-src 192.168.1.100 --ip-dst 192.168.1.200 --ip-proto icmp -j DROP ,
pcnt = 0 -- bcnt = 0
-p IPv4 --ip-src 192.168.1.200 --ip-dst 192.168.1.100 --ip-proto tcp --ip-dport
22 -j DROP , pcnt = 2 -- bcnt = 120
```

© 2003-2025 S-Terra CSP

```
-p IPv4 --ip-src 192.168.1.200 --ip-dst 192.168.1.100 --ip-proto udp --ip-dport
67 -j DROP , pcnt = 0 -- bcnt = 0

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT
```

7. Для того, чтобы удалить добавленное правило, необходимо воспользоваться командой:

```
root@sterragate:~# ebtables-legacy -D FORWARD --ip-src 192.168.1.100 --ip-dst
192.168.1.200 -p ipv4 --ip-proto icmp -j DROP
```

А затем проверить содержимое таблицы:

```
root@sterragate:~# ebtables-legacy -L --Lc
```

```
Bridge table: filter

Bridge chain: INPUT, entries: 0, policy: ACCEPT

Bridge chain: FORWARD, entries: 3, policy: ACCEPT
-p IPv4 --ip-src 192.168.1.200 --ip-dst 192.168.1.100 --ip-proto tcp --ip-dport
22 -j DROP , pcnt = 2 -- bcnt = 120
-p IPv4 --ip-src 192.168.1.200 --ip-dst 192.168.1.100 --ip-proto udp --ip-dport
67 -j DROP , pcnt = 0 -- bcnt = 0

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT
```

8. При необходимости можно добавить правила безопасности в таблицу «nat», например, воспользоваться DNAT (трансляцией внешнего MAC-адреса во внутренний):

```
root@sterragate:~# ebtables-legacy -t nat -A PREROUTING -p ipv4 -d
00:19:5B:3B:94:91 --ip-dst 192.168.2.96 -j dnat --to-dst 00:C0:9F:CF:42:4C --
dnat-target ACCEPT
```

А затем проверить содержимое таблицы:

```
root@sterragate:~# ebtables-legacy -t nat -L
```

```
Bridge table: nat

Bridge chain: PREROUTING, entries: 1, policy: ACCEPT
-p IPv4 -d 0:19:5b:3b:94:91 --ip-dst 192.168.2.96 -j dnat --to-dst
0:c0:9f:cf:42:4c --dnat-target ACCEPT

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT

Bridge chain: POSTROUTING, entries: 0, policy: ACCEPT
```

9. Для того, чтобы очистить все правила в таблице «filter», необходимо воспользоваться командой:

```
root@sterragate:~# ebtables-legacy -F
```

А затем проверить содержимое таблицы:

```
root@sterragate:~# ebtables-legacy -L
```

```
Bridge table: filter

Bridge chain: INPUT, entries: 0, policy: ACCEPT

Bridge chain: FORWARD, entries: 0, policy: ACCEPT

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT
```

10. Если же нужно очистить все правила в таблице «nat», то необходимо воспользоваться командой:

```
root@sterragate:~# ebtables-legacy -t nat -F
```

© 2003-2025 S-Terra CSP

А затем проверить содержимое таблицы:

```
root@sterragate:~# ebtables-legacy -t nat -L
```

```
Bridge table: nat

Bridge chain: PREROUTING, entries: 0, policy: ACCEPT

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT

Bridge chain: POSTROUTING, entries: 0, policy: ACCEPT
```

11. При необходимости можно выставить политику безопасности по умолчанию для любой из цепочек:

```
root@sterragate:~# ebtables-legacy -P FORWARD DROP
```

В данном случае политика по умолчанию DROP была выставлена для цепочки FORWARD:

```
root@sterragate:~# ebtables-legacy -L
```

```
Bridge table: filter

Bridge chain: INPUT, entries: 0, policy: ACCEPT

Bridge chain: FORWARD, entries: 0, policy: DROP

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT
```

Для того, чтобы вернуть политику безопасности по умолчанию к прежнему значению, необходимо воспользоваться командой:

```
root@sterragate:~# ebtables-legacy -P FORWARD ACCEPT
```

И проверить изменения:

```
root@sterragate:~# ebtables-legacy -L
```

```
Bridge table: filter

Bridge chain: INPUT, entries: 0, policy: ACCEPT

Bridge chain: FORWARD, entries: 0, policy: ACCEPT

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT
```

12. Для того, чтобы после перезагрузки ОС добавленные утилитой «ebtables-legacy» правила сохранились, необходимо выполнить команду:

```
root@sterragate:~# netfilter-persistent save
```

```
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/35-ebtables-legacy save
```

Будьте внимательны! При использовании утилиты `netfilter-persistent` также будут сохраняться правила утилиты «iptables».

13. Добавьте сервис `netfilter-persistent.service` в автозапуск для того, чтобы правила утилиты «ebtables-legacy» применялись во время старта криптошлюза:

```
root@sterragate:~# systemctl enable netfilter-persistent.service
```

```
Synchronizing state of netfilter-persistent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable netfilter-persistent
```

© 2003-2025 S-Terra CSP