Connection tracking

????????

Отслеживание соединений (Connection tracking) позволяет ядру отслеживать все логические сетевые соединения или сессии и таким образом связывать все пакеты, которые могут составлять это соединение.

NAT полагается на эту информацию для однородного преобразования всех связанных пакетов.

Благодаря отслеживанию соединений можно использовать функциональность stateful firewall (состояния сеансов) даже с таким stateless протоколом, как UDP.

??????? ????????, ???????? ?? ???????????? ??????????:

- NAT
- firewall:
  - connection-bytes
  - connection-mark
  - connection-type
  - connection-state
  - connection-limit
  - connection-rate
  - layer7-protocol
  - new-connection-mark
  - tarpit

Список отслеживаемых соединений можно увидеть в `/ip firewall connection` для IPv4 и `/ipv6 firewall connection` для IPv6.

```
[admin@3C22-atombumba] /ip firewall connection> print
Flags: S - seen-reply, A - assured
# PR.. SRC-ADDRESS           DST-ADDRESS           TCP-STATE  TIMEOUT
0    udp 10.5.8.176:5678    255.255.255.255:5678  0s
1    udp 10.5.101.3:646     224.0.0.2:646         5s
2    ospf 10.5.101.161      224.0.0.5             9m58s
3    udp 10.5.8.140:5678    255.255.255.255:5678  8s
4    SA  tcp 10.5.101.147:48984 10.5.101.1:8291   established 4m59s

[admin@3C22-atombumba] /ipv6 firewall connection> print
Flags: S - seen reply, A - assured
# PRO.. SRC-ADDRESS                                DST-ADDRESS
```

```
0    udp fe80::d6ca:6dff:fe77:3698                ff02::1
1    udp fe80::d6ca:6dff:fe98:7c28                ff02::1
2    ospf fe80::d6ca:6dff:fe73:9822                ff02::5
```

????????? ??????????

На основе записей в таблице соединений входящий пакет может быть отнесён к одному из следующих состояний соединения: **new** (новое), **invalid** (недопустимое), **established** (установленное), **related** (связанное) или **untracked** (неотслеживаемое).

Существует два случая, когда пакет считается новым:

- в случае **бессостоя́тельных (stateless)** протоколов, например UDP — когда в таблице соединений нет записи для данного трафика;
- в случае **состоя́тельных (stateful)** протоколов, например TCP — новый пакет, открывающий соединение, всегда является TCP-пакетом с установленным флагом **SYN**.

Если пакет не новый, он может относиться к уже установленному (**established**) или связанному (**related**) соединению, либо не относиться ни к одному, что делает его **invalid**.

Пакет в состоянии **established** принадлежит существующему соединению, зарегистрированному в таблице connection tracking. Состояние **related** аналогично, но пакет связан с другим существующим соединением — например, это может быть ICMP-пакет с сообщением об ошибке или пакет для передачи данных FTP.

Состояние **untracked** — особый случай, когда с помощью правил таблицы **RAW** определён трафик, исключённый из отслеживания соединений (connection tracking). Такие правила позволяют пропускать определённые пакеты без обработки connection tracking, что повышает скорость обработки трафика устройством.

Любой другой пакет, не соответствующий указанным состояниям, считается **invalid** (недопустимым) и, как правило, должен быть отброшен.

Исходя из этого, можно создать базовый набор фильтрующих правил, который повысит производительность и снизит нагрузку на CPU: принимать пакеты состояний **established** и **related**, отбрасывать **invalid**, и применять детализированную фильтрацию только к **new**-пакетам.

```
ip firewall filter add chain=input connection-state=invalid action=drop comment="Drop Invalid co
add chain=input connection-state=established,related,untracked action=accept comment="Allow Esta
```

Такой набор правил не должен применяться на маршрутизаторах с асимметричной маршрутизацией, так как асимметрично маршрутизируемые пакеты могут быть признаны недействительными и отброшены.

FastTrack

IPv4 FastTrack — это специальный обработчик, который обходит стандартные возможности Linux, позволяя ускорить пересылку пакетов. Этот обработчик используется для соединений **TCP** и **UDP**, помеченных действием `fasttrack-connection`. Обработчик FastTrack поддерживает NAT (SNAT, DNAT или оба).

Следует отметить, что не все пакеты соединения могут быть обработаны FastTrack, поэтому вероятно, что некоторые пакеты будут идти по "медленному" пути даже при помеченном для FastTrack соединении. Это причина, по которой действие `fasttrack-connection` обычно сопровождается идентичным правилом с

```
action=accept
```

Пакеты, проходящие через **FastTrack**, обходят следующие механизмы системы:

- фаервол (firewall);
- отслеживание соединений (connection tracking);
- простые очереди (simple queues);
- дерево очередей (queue tree) с параметром `parent=global`;
- учёт трафика (IP accounting);
- шифрование IPSec;
- универсальный клиент Hotspot;
- назначение VRF.

Администратор должен самостоятельно убедиться, что использование **FastTrack** не конфликтует с другими элементами конфигурации.

??????????

Механизм **IPv4 FastTrack** активируется, если выполняются следующие условия:

- не используется конфигурация интерфейсов **mesh** или **metarouter**;
- не запущены инструменты **sniffer**, **torch** или **traffic generator**;
- инструмент **/tool mac-scan** не используется активно;
- инструмент **/tool ip-scan** не используется активно;
- в разделе **IP → Settings** включены опции **FastPath** и **Route Cache**.

??????

Например, для SOHO маршрутизаторов с заводской конфигурацией, вы можете применить FastTrack ко всему LAN-трафику одним правилом, размещенным в начале фильтра файрвола. Также требуется такое же правило с действием accept:

```
/ip firewall filter add chain=forward action=fasttrack-connection connection-state=established,r
/ip firewall filter add chain=forward action=accept connection-state=established,related
```

- Соединение обрабатывается FastTrack, пока оно не закрыто, не истекло по таймауту или не перезагружен маршрутизатор.

- Пустые правила исчезнут только после удаления/отключения правил FastTrack и перезагрузки маршрутизатора.
- Когда FastPath и FastTrack включены одновременно, активен может быть только один.
- Очереди (кроме Queue Trees, привязанных к интерфейсам), фильтр файрвола и правила mangle не применяются к FastTrack-трафику.

????????? ???????????? ??????????

Настройки отслеживания соединений управляются из меню `/ip firewall connection tracking`.

????????

Свойство	Описание
enabled (yes | no | auto; По умолчанию: auto)	Позволяет включать или отключать отслеживание соединений. Если отключено, перечисленные выше функции файрвола не работают. Если установлено в "auto", отслеживание соединений отключено до тех пор, пока не будет добавлено хотя бы одно правило файрвола.
liberal-tcp-tracking (yes | no; По умолчанию: no)	Включает или отключает либеральное отслеживание TCP соединений, переключая параметр ядра. Включение может позволить принять нарушенные пакеты, которые в противном случае считались бы ошибочными.
loose-tcp-tracking (yes; По умолчанию: yes)	
tcp-syn-sent-timeout (time; По умолчанию: 5s)	Таймаут SYN TCP.
tcp-syn-received-timeout (time; По умолчанию: 5s)	Таймаут SYN TCP.
tcp-established-timeout (time; По умолчанию: 1d)	Время, после которого считается таймаут установленного TCP соединения.
tcp-fin-wait-timeout (time; По умолчанию: 10s)	
tcp-close-wait-timeout (time; По умолчанию: 10s)	
tcp-last-ack-timeout (time; По умолчанию: 10s)	
tcp-time-wait-timeout (time; По умолчанию: 10s)	
tcp-close-timeout (time; По умолчанию: 10s)	
udp-timeout (time; По умолчанию: 30s)	Задержка для UDP соединений, которые видели пакеты только в одном направлении.
udp-stream-timeout (time; По умолчанию: 3m)	Задержка для UDP соединений, которые видели пакеты в обоих направлениях.
icmp-timeout (time; По умолчанию: 10s)	Таймаут для ICMP соединений.
generic-timeout (time; По умолчанию: 10m)	Таймаут для всех остальных соединений.

?????? ??? ??????

Свойство	Описание
max-entries (integer)	Максимальное количество записей, которые может содержать таблица отслеживания соединений. Это значение зависит от объема установленной оперативной памяти. Система не создает таблицу максимального размера при запуске, но может ее увеличить при необходимости, если есть свободная память, не превышая 1048576 записей.
total-entries (integer)	Текущее количество соединений в таблице отслеживания.

?????? ??????????

Список отслеживаемых соединений можно увидеть в `/ip firewall connection` для IPv4 и `/ipv6 firewall connection` для IPv6.

????????

Все свойства в списке соединений доступны только для чтения.

Свойство	Описание
assured (yes | no)	Указывает, что соединение гарантировано и не будет удалено при достижении максимального количества отслеживаемых соединений.
confirmed (yes | no)	Соединение подтверждено и пакет был отправлен с устройства.
connection-mark (string)	Отметка соединения, установленная правилом mangle.
connection-type (pptp | ftp)	Тип соединения; поле пустое, если невозможно определить тип соединения.
dst-address (ip)	Адрес назначения.
dst-port (integer)	Порт назначения.
dstnat (yes | no)	Соединение прошло через DST-NAT (например, перенаправление портов).
dying (yes | no)	Соединение в процессе окончания из-за таймаута.
expected (yes | no)	Соединение установлено с помощью помощников соединений (предопределенных правил сервиса).
fasttrack (yes | no)	Соединение обработано с помощью FastTrack.
gre-key (integer)	Данные поля GRE Key.
gre-protocol (string)	Протокол инкапсулированного полезного груза.
gre-version (string)	Версия протокола GRE, используемая в соединении.
hw-offload (yes | no)	Аппаратно ускоренное соединение.
icmp-code (string)	Поле ICMP Code.

Свойство	Описание
icmp-id (integer)	ID ICMP.
icmp-type (integer)	Номер типа ICMP.
orig-bytes (integer)	Количество байт, отправленных с исходного адреса по этому соединению.
orig-fasttrack-bytes (integer)	Количество байт FastTrack, отправленных с исходного адреса.
orig-fasttrack-packets (integer)	Количество пакетов FastTrack, отправленных с исходного адреса.
orig-packets (integer)	Количество пакетов, отправленных с исходного адреса по соединению.
orig-rate (integer)	Скорость передачи данных от исходного адреса.
protocol (string)	Тип IP протокола.
repl-bytes (integer)	Количество байт, полученных от адреса назначения.
repl-fasttrack-bytes (string)	Количество байт FastTrack, полученных от адреса назначения.
repl-fasttrack-packets (integer)	Количество пакетов FastTrack, полученных от адреса назначения.
repl-packets (integer)	Количество пакетов, полученных от адреса назначения.
repl-rate (string)	Скорость приема данных от адреса назначения.
reply-dst-address (ip)	Адрес назначения, ожидаемый для обратных пакетов.
reply-dst-port (integer)	Порт назначения, ожидаемый для обратных пакетов.
reply-src-address (ip)	Исходный адрес, ожидаемый для обратных пакетов.
reply-src-port (integer)	Исходный порт, ожидаемый для обратных пакетов.
seen-reply (yes | no)	Адрес назначения ответил на исходящий адрес.
src-address (ip)	Исходный адрес.
src-port (integer)	Исходный порт.
srcnat (yes | no)	Соединение проходит через SRC-NAT, включая пакеты, замаскированные через NAT.
tcp-state (string)	Текущее состояние TCP соединения.
timeout (time)	Время до удаления соединения из списка.
uses-helper (yes | no)	Применен помощник из "IP/Firewall/Service Port" к этому соединению.

Revision #1
Created 11 November 2025 15:21:23 by Admin
Updated 11 November 2025 15:35:11 by Admin