ОБНОВЛЕНО 16 МАР

Метки

Метки – это быстрые таблицы данных, предназначенные для временной фиксации информации о сетевых пакетах и соединениях. Они используются для управления трафиком, выявления угроз и отладки правил фильтрации.

Типы меток

Система поддерживает следующие типы меток:

- **HMARK** — фиксирует адрес источника.
- **DHMARK** — фиксирует адрес назначения.
- **SDHMARK** — фиксирует адрес источника и назначения.
- **CONNMARK** — фиксирует полный 5-tuple соединения: IP-адрес источника и назначения, порты источника и назначения, транспортный протокол (L4).
- **HMARKC** — административная метка для создания чёрных и белых списков. Префиксы вводятся вручную и не зависят от правил фильтрации.

Поля записи метки

- **ID** — идентификатор записи.
- **Value** — числовой счётчик, управляемый правилами.
- **Age** — время, прошедшее с момента добавления записи.
- **Lifetime** — время до истечения записи. Обновляется при поступлении подходящих пакетов. Когда срок заканчивается, запись получает статус **expired**.

Принцип работы

> **Исключение**
> Механизм ниже не применяется к **HMARKC**.

Создание метки

Когда срабатывает правило, система создаёт запись с параметрами трафика, характерными для конкретного типа метки.

Применение метки в правилах

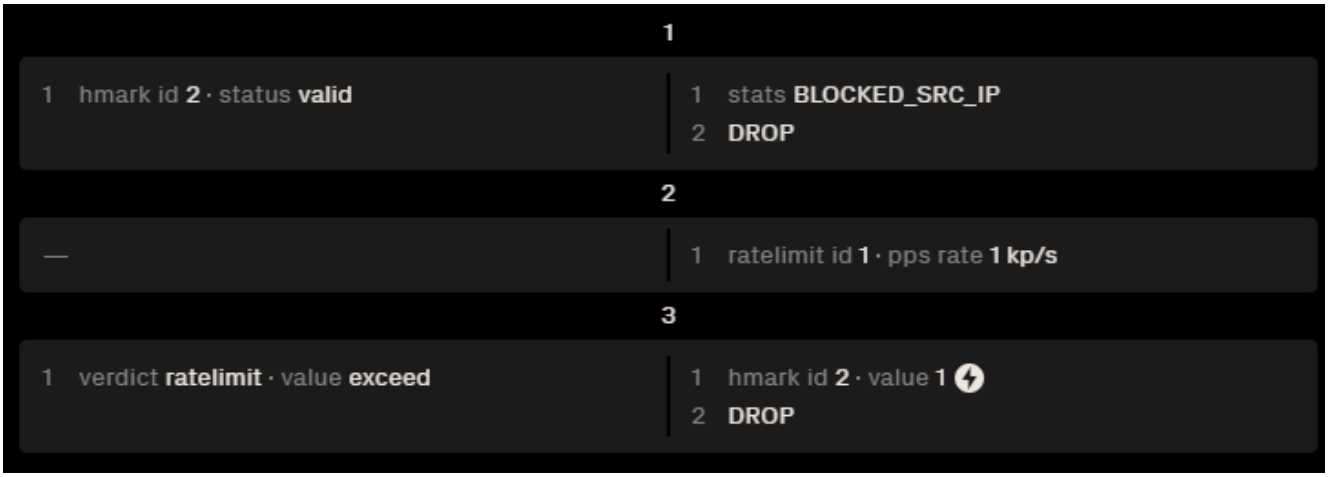
Для каждого нового пакета система проверяет, есть ли подходящая активная метка. Если метка найдена и она валидна, правило может применить действие: блокировку, перенаправление или другое требуемое поведение.

Обновление и удаление

При повторных нарушениях lifetime продлевается. Метка остаётся активной дольше. Когда срок истекает, метка автоматически удаляется. При необходимости её можно удалить вручную.

Пример использования HMARK

Сценарий: временная блокировка IP-адреса при превышении пороговой интенсивности пакетов.



Шаг 1. Блокировка по уже активной метке

Если у источника уже есть валидная метка в **HMARK id 2**, пакет сразу отбрасывается. Система фиксирует событие в статистике и завершает обработку.

Шаг 2. Измерение интенсивности

Если метки нет, система начинает измерять частоту пакетов. Порог — 1000 pps от одного источника.

Шаг 3. Реакция на превышение порога

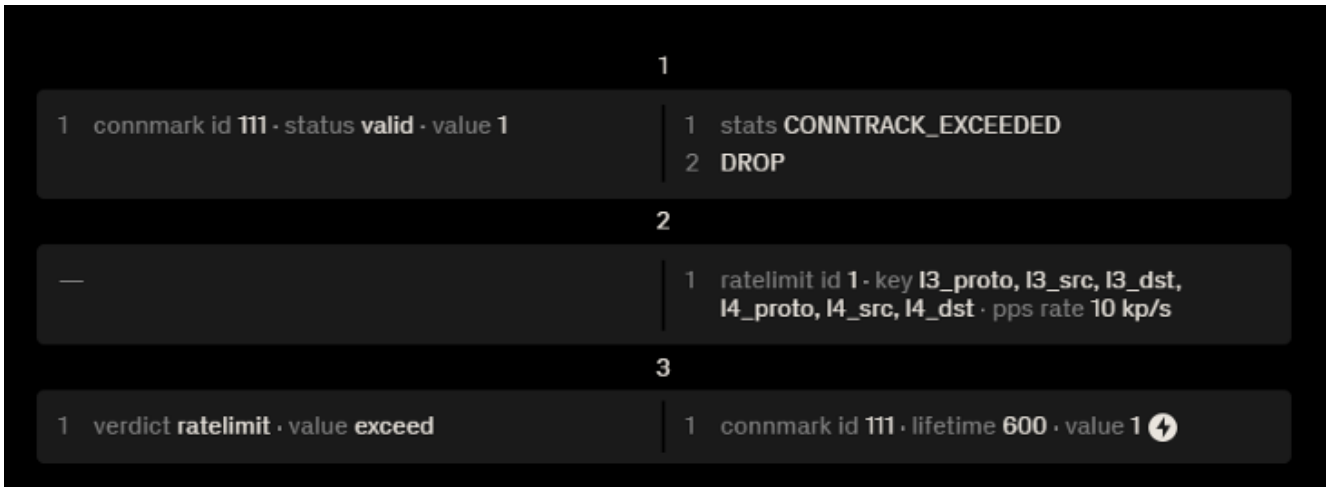
При превышении порога создаётся запись в **HMARK id 2**. Текущие пакеты отбрасываются.

Жизненный цикл

Пока запись **HMARK id 2** валидна, трафик блокируется на шаге 1. После истечения lifetime измерения возобновляются. При повторном превышении порога создаётся новая запись и блокировка обновляется

Пример использования CONNMARK

Сценарий: временная блокировка TCP/UDP-сессий при превышении порога трафика.



Шаг 1. Блокировка по уже активной метке

Если у источника уже есть валидная метка в **CONNMARK id 111**, пакет сразу отбрасывается. Система фиксирует событие в статистике и завершает обработку.

Шаг 2. Измерение интенсивности

Если метки нет, система начинает считать пакеты для каждого соединения отдельно. Соединение определяется:

- l3_proto — IPv4 или IPv6
- l3_src и l3_dst — IP-адрес источника и назначения
- l4_proto — TCP или UDP
- l4_src и l4_dst — порт источника и назначения

Порог — 10 000 pps на одно соединение.

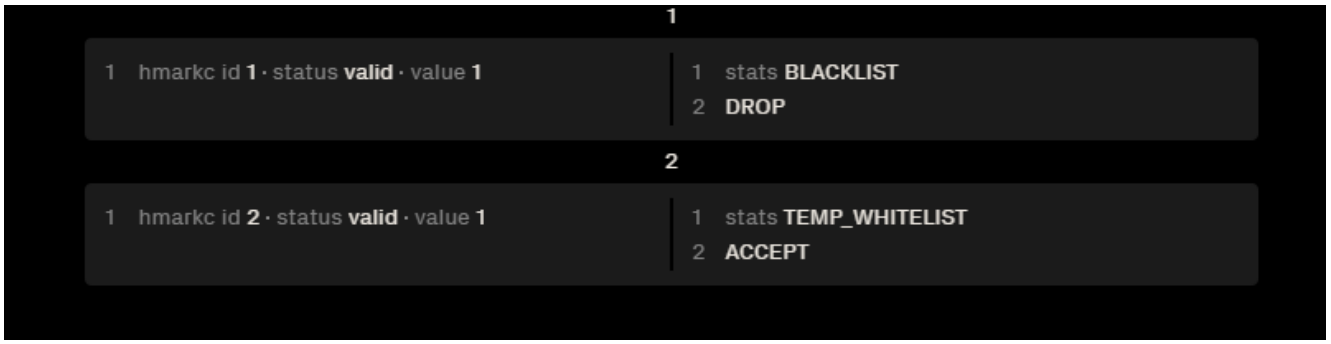
Шаг 3. Реакция на превышение порога

При превышении порога создаётся запись в **CONNMARK id 111** на 600 секунд. Текущий пакет и следующие отбрасываются шагом 1.

Жизненный цикл

Пока метка **CONNMARK id 111** активна, трафик блокируется на шаге 1 без повторных измерений. Когда lifetime истекает, пакеты снова проходят шаг 2. Если порог превышается, система обновляет метку и возвращает блокировку.

Пример использования HMARKC



Сценарий: адресное управление трафиком по заранее заданным префиксам.

Шаг 1. Добавление префикса

В разделе **Метки** создать новую метку **HMARKC** и добавить нужные префиксы.

Шаг 2. Применение в правилах

В условии совпадения выбрать **HMARKC** и задать действие:

- **DROP** — блокирует трафик указанных адресов. Правило работает как чёрный список.
- **ACCEPT** — пропускает трафик без дальнейшей фильтрации. Используется как белый список.

Жизненный цикл
Метка **HMARKC** управляется вручную. Автоматическое создание и продление **Lifetime** правилами не поддерживается.

Пример использования счётчика Value

Value помогает фиксировать повторные нарушения и усиливать реакцию системы при эскалации.

Первое срабатывание
При первом превышении порога создаётся метка **HMARK** со значением *value = 1*.

Повторные нарушения
Каждое новое превышение для того же источника увеличивает значение: *value = 2*, *value = 3* и далее.

Эскалация
Когда значение достигает порога источник можно обработать жёстче: добавить в префикс-сет или применить отдельное блокирующее правило.

Пример
10.0.0.1 отправил **600 TCP SYN-пакетов** → создаётся **HMARK** *value = 1*. Через **100 секунд** тот же адрес отправил **700 пакетов** → *value = 2*. Следующее превышение → *value = 3*, после чего источник блокируется через префикс-сет или соответствующее правило.