ОБНОВЛЕНО 16 МАР

Логирование каждого пакета

Технически DosGate имеет возможность логирования каждого проходящего через него пакета. Для этого можно использовать быстрые таблицы данных (метки).

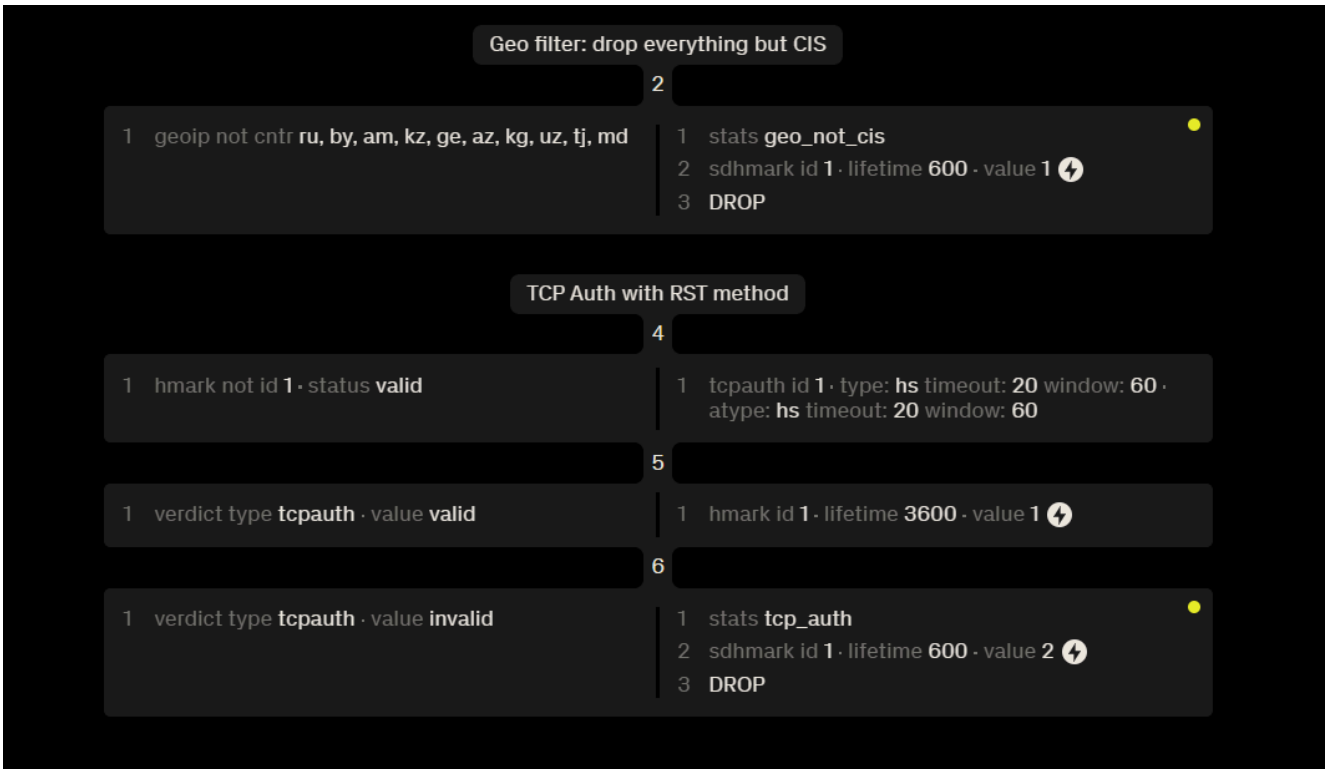
С помощью логирования каждого пакета, можно обладать максимальной детализацией по каждому проходящему через систему пакета (почему конкретный пакет был сброшен и когда). Данный функционал удобен если у вас есть серьезные требования по детализации статистики, а стандартных метрик аналитики (статистика на правило или общая статистика) вам недостаточно.

Данный режим понижает производительность платформы. Не рекомендуется к активации на платформах которые обрабатывают больше 20Mpps и процессором производительностью ниже Intel Xeon Gold 6230.

Подготовка платформы DosGate

- Определите тип хранения данных (один из, или несколько): hmark (IP-отправителя), dmark (IP-получателя), sdhmark (IP-отправителя и получателя), connmark (IP-отправителя и получателя, протокол, порт получателя и отправителя).
- Определите глубину хранения, например, 100 000 записей. Обновите максимальный размер таблицы в соответствии с документацией. По умолчанию каждая метка хранит до 1 000 000 записей.

Настройка профилей фильтрации



- Для каждого правила потребуется установить уникальный счетчик, например, sdhmark (он сохраняет пару l3_src и l3_dst).
- Счетчик должен быть установлен до терминального действия, например, до DROP или ACCEPT.
- Для каждого правила, укажите уникальный value. ID может быть одинаковым.

- Вы сможете определять сработавшее правило по value, а также пару l3_src и l3_dst к которым это правило было применено (при использовании sdhmark). По желанию, можно также указывать разный ID.

Интеграция с SIEM

С помощью API DosGate.

Получение списка профилей выбранной арены

```
curl --location 'http://<node_ip>/fapi' \
--header 'Content-Type: application/json' \
--data '{
    "url": "arena://<arena>",
    "cmd": "list"
}'
```

Получение списка правил каждого профиля

```
curl --location 'http://<node_ip>/fapi' \
--header 'Content-Type: application/json' \
--data '{
    "url": "profile://<arena>/<profile>",
    "cmd": "list"
}'
```

Получение всего списка записей

Все виды marktype: `shost` (hmark), `dhost` (dmark), `sdhost` (sdhmark), `conn` (connmark). Выберите в зависимости от используемых в профиле.

Обращаться к получению всего списка записей рекомендуется не чаще чем 1 раз в 3 секунды.

На получение 100 000 записей из метки уходит около 1100 мс., общий вес ответа около 4.8 Мбайт.

```
curl --location 'http://<node_ip>/fapi' \
--header 'User-Arena: first' \
--header 'Content-Type: application/json' \
--data '{
    "url": "mark://<arena>/<profile>",
    "type": "<marktype>",
    "cmd": "list"
}
```

Размещение данных в SIEM

Направьте полученные данные в SIEM вместе с временным отпечатком (когда вы получили эти данные) и названием ноды (произвольно, для удобства если ЦО состоит из нескольких DosGate). Можно исключить "lifetime", если не требуется или не используется.

Рекомендуется оставить название профиля и арены для удобства и дальнейшего разбора, так как профили могут быть разные, с разным набором правил и условий.

Также, направьте в SIEM набор правил. Правило можно сопоставить с записью из метки на основании value и/или ID.

Повторный запрос

Через выбранный интервал снова выполните тот же запрос к метке и отправьте обновлённые записи в SIEM.