ОБНОВЛЕНО 16 МАР

# Чейны

**Чейны**— это отдельная ветка правил, используемая для обработки и фильтрации сетевого трафика. Она представляет собой набор правил, определяющих порядок обработки пакетов.

Чейны используются для выборочного применения механизмов защиты в режиме постоянного трафика через DosGate. Это позволяет избежать непрерывной активации защитных мер, таких как TCP-аутентификация и другие контрмеры, которые могут негативно повлиять на легитимный трафик.

По своей структуре чейны аналогичны стандартным правилам фильтрации: в них можно задавать условия обработки пакетов, а также использовать готовые пресеты для унификации и удобства настройки.

## Принцип работы

- Основной профиль содержит базовый набор правил обработки пакетов.
- В зависимости от условий, заданных в профиле, пакеты могут быть перенаправлены в определённый чейн.
- В чейне хранятся дополнительные правила, которые выполняются только для перенаправленных пакетов.
- Это позволяет изолировать специфические механизмы защиты и включать их только при превышении заданных порогов, минимизируя влияние на легитимный трафик.

## Пример использования чейна на примере фильтрации трафика по географическому признаку

Рассмотрим работу чейна на примере разделения трафика по стране-источнику.

1. Анализ входящего трафика
   При поступлении пакета система анализирует его source-адрес и определяет страну-

источник с использованием базы GeoIP.

2. Сопоставление с правилами профиля и перенаправление в чейн
   В профиле настроено правило, проверяющее, принадлежит ли трафик России. Если условие не выполняется, срабатывает действие **GOTO**, перенаправляющее пакет в отдельный чейн "Not-RU". Это логически изолированный блок правил, применяемых только к данному типу трафика.
3. Применение строгих политик фильтрации Внутри чейна "Not-RU" могут быть настроены дополнительные механизмы защиты, например:
   - Ограничение количества соединений с одного IP (rate limit).
   - Фильтрация по протоколам (например, блокировка UDP-амплификаций).
   - Блокировка трафика с известных вредоносных IP.
4. Принятие вердикта

Если пакет соответствует критериям блокировки, он отбрасывается. Если пакет проходит фильтры, он возвращается в основной профиль и продолжает обработку.