

Содержание

Настройка авторизации по DHCP и ARP 3

Настройка авторизации по DHCP и ARP

1. Активация BRAS в FastDPI
2. Что такое сессия абонента
3. Обработка DHCP
4. Обработка ARP
 1. ARP inspection
 2. Авторизация по ARP-запросам
5. IP source guard
6. Замыкание локального трафика
7. Терминация трафика
 1. Терминация на уровне автономной системы
 2. Задание параметров терминации для каждого выходного интерфейса
8. Ручное изменение свойств абонента
9. Трассировка СКАТ BRAS



Обзор L2 DHCP Mode

BRAS L2 для VLAN/Q-in-Q-сетей обеспечивает следующие функции:

- *DHCP*: мониторинг DHCP-запросов от клиентов, немедленная авторизация клиента по Radius-протоколу в случае успешного ответа DHCP-сервера
- *ARP proxy* – мониторинг ARP-запросов из локальной сети, блокирование ARP-запросов из WAN
- *IP source guard* – проверка, что LAN-пакет принадлежит той же самой VLAN, из которой была DHCP-регистрация. Если это условие нарушается, пакет отбрасывается.
- *Замыкание* локального трафика
- *Терминация трафика* из LAN в WAN, *оригинация (приземление)* ответного трафика из WAN в LAN

Для выполнения этих функций fastDPI BRAS должен знать, когда начинается и когда заканчивается сессия клиента, а также оперировать не только IP-адресами пользователей, но и их MAC-адресами и тегами VLAN/QinQ-сетей. С помощью этих знаний возможно отфильтровать неправомерные запросы, тем самым повысив безопасность локальной сети в целом.

FastDPI BRAS L2 подходит как для VLAN-сетей, так и для QinQ (double VLAN, VLAN-per-user)-сетей. QinQ-сеть более предпочтительна, так как позволяет однозначно идентифицировать пользователя независимым от железа пользователя способом, но и для обычной VLAN-сети (с одним VLAN-заголовком пакета), где номер VLAN фактически идентифицирует не пользователя, а группу пользователей, например, подъезд дома или многоквартирный дом целиком, fastDPI BRAS позволяет реализовать некоторую защиту.



Функции BRAS L2 имеют смысл только при эксплуатации fastDPI в режиме моста, в разрыв.

BRAS работает в основном на уровне L2, что означает, что если пакет из LAN дропается или

принимается решение отправить его обратно в LAN, никакого распознавания содержимого пакета (payload) не производится.



При внедрении L2 BRAS, особенно на тестовом стенде с малым количеством тестовых абонентов, следует учитывать, что в силу архитектурных особенностей и оптимизации под большой объем проходящего трафика BRAS может некорректно работать с абонентской базой, состоящей из 1-2 абонентов, что выражается в задержках ответов на DHCP/PPPoE пакеты. Для полноценной работы L2 BRAS необходимо загрузить СКАТ каким-либо трафиком, чтобы не простаивали рабочие потоки.