

## Общие сведения

ERSPAN позволяет зеркаливать трафик локального порта (с низкой пропускной способностью) на удаленный IP, например, на уже развернутый блок Security Onion. Затем трафик порта инкапсулируется в ERSPAN, затем в GRE и отправляется одному/нескольким адресатам.

ERSPAN — это технология Cisco, которая доступна только на некоторых платформах, включая: Catalyst 6500, 7600, Nexus и ASR 1000.

Одним из способов получения доступа к инкапсулированному трафику на хосте назначения является использование демона RCDCAP. Она представляет собой демон, создающий виртуальный интерфейс, если таковой отсутствует, на котором происходит декапсуляция заголовков GRE и ERSPAN перед подачей трафика на предыдущий интерфейс.

Затем Security Onion может подключаться к этому интерфейсу, как и к любому другому, и в случае отказа демона RCDCAP продолжать прослушивать этот интерфейс, даже если декапсулированный трафик уже будет недоступен.

Исходные данные для описанного далее примера:

- IP-адрес коммутатора — 172.16.0.1;
- Отслеживаемый порт коммутатора — GigabitEthernet0/10;
- IP-адрес назначения мониторинга Security Onion — 10.10.10.10 на eth2 (является выделенным интерфейсом).

## Настройка на стороне Security Onion

Для того чтобы настроить ERSPAN на стороне Security Onion, выполните следующие шаги:

**Шаг 1.** Включите репозиторий Inverse для Security Onion:

```
sudo bash -c 'cat << EOL >/etc/apt/sources.list.d/securityonion-inverse.list deb http://inverse.ca/downloads/AxelNAC/securityonion trusty trusty EOL' gpg --keyserver keyserver.ubuntu.com --recv 19CDA6A9810273C4 gpg --export --armor 19CDA6A9810273C4 | sudo apt-key add —'
```

**Шаг 2.** Установите RCDCAP:

```
sudo apt-get update  
sudo apt-get install rcdcap
```

**Шаг 3.** Измените сетевой файл (/etc/network/interfaces) таким образом, чтобы у eth2 был IP-адрес и соответствующий MTU. Декапсулированный трафик будет подаваться на mon1:

```
auto eth2  
iface eth2 inet static  
    адрес 10.10.10.10  
    netmask 255.255.255.240  
    up ip link set $IFACE arp on up  
    up ip link set dev $IFACE mtu 1900  
    post-up ethtool -G $IFACE rx 4096; for i in rx tx sg tso ufo gso gro lro;  
        do ethtool -K $IFACE $i off; done  
    post-up echo 1 > /proc/sys/net/ipv6/conf/$IFACE/disable_ipv6  
    9  
auto mon1  
iface mon1 inet manual  
    pre-up rcdcap -i eth1 --erspan --tap-persist --tap-device $IFACE  
        --expression "host 172.16.0.1" -d  
    up ip link set $IFACE promisc on arp off up  
    down ip link set $IFACE promisc off down  
    post-up ethtool -G $IFACE rx ; for i in rx tx sg tso ufo gso gro lro; do  
        ethtool -K $IFACE $i off; done  
    post-up echo 1 > /proc/sys/net/ipv6/conf/$IFACE/disable_ipv6
```

**Шаг 4.** Повторно запустите мастер настройки Security Onion и убедитесь, что пропущен шаг настройки сети.

**Шаг 5.** Убедитесь, что для мониторинга выбран mon1:

```
sudo sosetup
```

## Настройка на стороне коммутатора

Для того чтобы настроить ERSPAN на стороне коммутатора, выполните следующие команды:

```
monitor session 10 type erspan-source  
description ERSPAN to 10.10.10.10  
source interface GigabitEthernet0/10  
destination  
erspan-id 10  
ip address 10.10.10.10  
origin ip address 172.16.0.1  
no shutdown ! Default is shutdown
```

Ревизия: 3

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.2.0 -> AxelNAC. Руководство администратора -> Интеграция с системами обнаружения вторжений (IDS) -> ERSPAN

<https://docs.axel.pro/entry/335/>