Содержание

Out-of-line network schema for SCAT

(SPAN ports or optical splitter)

if block url is detected SCAT sends HTTP redirect for browser to stub WEB page with information about blocking.

Packet headers:

- Destination MAC - routers' MAC of port where outgoing link is pluged in
- Source MAC - out_dev NICs' MAC
- Source IP - IP of blocked host (IP2)
- Destination IP - users' IP (IP1)

VLAN can be keeped or cleared by configurable parameter.

To IP2 (blocked host) sending a packet with TCP RST for connection reset. Blocking (HTTPS) and redirecting (HTTP) ocures because of difference in response time between SCAT and blocked host. SCAT is close to users' IP1 then blocked IP2.

Router settings

Router port where SCATs' outgoing link is pluged in has to be L3 mode as usual. Main task is receive packet from SCAT and route it by subscrider by general routing tables.

Config sample for Juniper: To Juniper MX pluged in eth1

- Juniper MX settings:
- description from_SKAT_redirect;
- unit 0 {
- family inet {
- address a.b.c.d/30;
- }
- }

SCAT Config sample

Let SKAT be connected as follows:

```
dna1,dna2,dna3 - receive the mirrored traffic
dna0 - is connected to the router that receives and redirects subscribers'
queries and to Internet
```

One has to configure DPI for mirrored traffic processing as follows:

First, assign the input ports that receive the mirrored traffic to in_dev:

```
in_dev=dna1:dna2:dna3
```

Second, assign the ports that get the redirection request to tap_dev:

```
tap_dev=dna0
```

Enable asymmetric mode:

```
asym_mode=1
```

Set direction of replies tap_dev:

```
emit_direction=2
tap_mode=2
```

Set to clear VLAN in outgoing packets:

```
strip_tap_tags=1
```

And configure MAC replacement:

```
replace_source_mac=00:25:90:E9:43:59 - MAC address of out_dev card: dna0
replace_destination_mac=78:19:F7:0E:B1:F4 - the router port MAC address that
has a general routing table
```

It is advised to use an additional 1GbE network card to send the replies in mirrored traffic mode. For example, intel i350 (with DNA license) can be used. This allows to configure an individual port for sending redirection replies and to reserve 10GbE ports to receive the mirrored traffic.