Содержание

Base SSG configuration for MIRROR scheme

1. Prepare the server according to the installation requirements.
2. Install and configure the VEOS OS
3. Set an IP address.
4. Apply for license installation and fastDPI to Service Desk.
5. After installing them, the following settings must be made in **`etc/dpi/fastdpi.conf`**:

Suppose the SCAT is connected as follows:

- `01-00.0, 01-00.1, 01-00.2` – receive the mirror traffic
- `01-00.3` – connected to a router that receives and forwards responses to subscribers and to the internet.

To set the DPI in mirroring mode, you have to specify the following in the configuration:

In the configuration for the inbound ports `in_dev` set the ports that accept mirror traffic:

```
in_dev=01-00.0:01-00.1:01-00.2
```

In the configuration for outgoing ports `tap_dev` set the port to which the forwarding response is sent:

```
tap_dev=01-00.3
```

Specify the mode – asymmetric

```
asym_mode=1
```

Specify the direction of `tap_dev` responses:

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

To send responses in mirroring mode it is correct to use an additional 1GbE card such as intel i350 (+ DNA license), configure a separate port in the system to send **tap_dev** forwarding, and use 10GbE ports for **in_dev** mirrored traffic flows.

Specify that VLAN should be reset:

```
strip_tap_tags=1
```

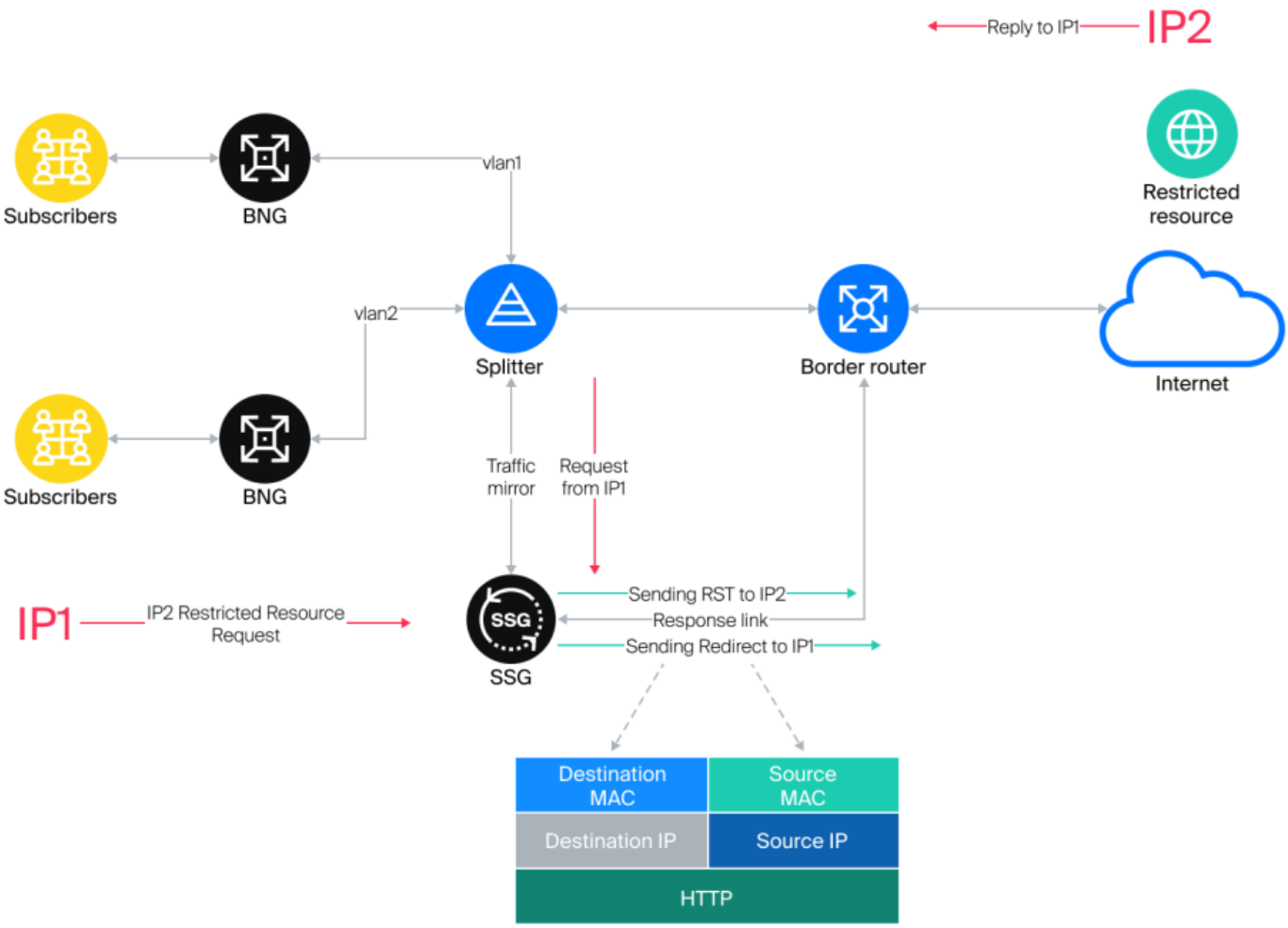
Set MAC change:

```
replace_source_mac=00:25:90:E9:43:59 #- MAC address of card out_dev - dna0
replace_destination_mac=78:19:F7:0E:B1:F4 #- MAC address of the router, or
the routing switch
```

Set the number of retries if there are network losses:

```
emit_duplication=3
#here, 3 is the number of repetitions (duplicates) of a packet with redirect
or blocking.
```

Implementation scheme and description of operation



When a request for a restricted resource is detected, the SSG sends an HTTP redirect to a placeholder page to the subscriber (IP1).
A TCP RST packet is sent to the restricted resource (IP2) to drop the connection. Blocking (HTTPS) and redirecting (HTTP) occurs because the SSG responds to the request from IP1 faster than IP2.

Header of the IP response packet

1. **Destination MAC** – MAC address of the router port where the response link is connected.
2. **Source MAC** – MAC address of the `out_dev` card.
3. **Source IP** – IP address of the restricted resource IP2.

4. **Destination IP** – IP address of user IP1.

Router configuration example

The port on the router where the reply link from the SSG is included should be configured as a normal L3 port. The task is to receive a packet from the SSG and forward it to the subscriber based on the common routing tables.

Configuration example: `eth1` is connected to the Juniper MX side

```
#Settings on tha MX side:
description from_SSG_redirect;
unit 0 {
  family inet {
  address a.b.c.d/30;
  }
}
```

Statistics collection

```
#FullNetflow/IPFIX
netflow=8
netflow_full_collector_type=2
netflow_dev=eth3
netflow_timeout=20
netflow_full_collector=172.18.254.124:1500
netflow_rate_limit=30
netflow_passive_timeout=40
netflow_active_timeout=120

#ClickStream/IPFIX
ipfix_dev=eth3
ipfix_tcp_collectors=172.18.254.124:1501

#SIP
ipfix_meta_tcp_collectors=172.18.254.124:1511
rlimit_fsize=32000000000
```

Further settings are made depending on which components are to be used. The settings are described in the SSG components section.