Table of Contents

Network Interaction

1. Is STP processed transparently?

Yes.

2. Can SSG support a configuration with a single 10G network interface in the server, where traffic passes through SSG using two VLANs (in and out)?

No. This is not planned for future support.

3. Can SSG set up a BGP link with a border router for exporting prefixes that need to be routed through SSG?

Yes, this is possible. More about router settings.

4. If during a test connection to the internal LAN the 'ping' time hasn't changed, should there be a delay?

The delay on the device, if the hardware meets our recommendations, does not exceed 30 µs (microseconds) or 0.03 ms (milliseconds). 'Ping' measurements start at 1 ms. Measuring such delays requires special software and equipment; in our lab, we use counters in nanoseconds supported by modern network cards.

5. If implementing mirroring, can SSG remove tags on the output (out_dev=dnaX) when traffic with different tags comes on in_dev=dna1:dna2?

SSG will send a response with the original packet tag if VLAN translation settings have not been applied.

6. What is SSG? Is it a router, NAT, transparent proxy, or is it transparent to network devices?

SSG is a DPI device, similar to Cisco SCE. It operates as a bridge, without IP addressing, and is invisible on the network.
The delay when using it is no more than 30 microseconds (based on tests, 16 µs), which is virtually indistinguishable from a direct connection.
See detailed connection diagrams for SSG.

7. In what form is aggregated traffic provided? Are ports grouped through LACP?

Yes, you can use LACP and LAG for traffic aggregation.
See detailed connection diagrams for SSG.

8. At which point should the system connect, before or after termination on BRAS (in other words, at L2 or L3)?

It depends on the task: if the platform connects as a DPI, then after the termination point; if BRAS, NAT functionality is required, then the SSG platform performs traffic termination directly.
Connection diagrams.

9. How to optimize the WEB server network stack?

Apply the following settings:

```
net.core.netdev_max_backlog=10000
net.core.somaxconn=262144
net.ipv4.tcp_syncookies=1
net.ipv4.tcp_max_syn_backlog = 262144
net.ipv4.tcp_max_tw_buckets = 720000
net.ipv4.tcp_tw_recycle = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_fin_timeout = 30
net.ipv4.tcp_keepalive_time = 1800
net.ipv4.tcp_keepalive_probes = 7
net.ipv4.tcp_keepalive_intvl = 30
net.core.wmem_max = 33554432
net.core.rmem_max = 33554432
net.core.rmem_default = 8388608
net.core.wmem_default = 4194394
net.ipv4.tcp_rmem = 4096 8388608 16777216
net.ipv4.tcp_wmem = 4096 4194394 16777216
```

10. Why does one BGP session come up while another does not?

Example:

- Check `tcpdump`. On the client's interface, mtu = 9000.
- On one session, mss = 1480 during sync, while on the other, mss = 8500.
  This indicates that one peer has a standard mtu of 1500, while the other has an increased mtu.
- On sessions where mss is higher than 1480 and there is an IP header, set the settings in MX:

```
neighbor 95.167.18.57 {
traceoptions {
file as12389.log size 1m files 3;
}
 description "-= RT AS12389 Upload =-";
 import [ bogus-reject MM-IN ];
 export REJECT-ALL;
  peer-as 12389;
  tcp-mss 1460;
}
 tcp-mss 1460;
```

Administration questions