Содержание

7 FAQ

<html>

</html>

<html>

</html>

1. Can one use the own list rather than the one loaded from clouds?
   Can one make DPI to use our list of restricted resources only?
   Answer: Yes. The cloud service is implemented for your convenience, in order not to process Department of Justice list manually. The cloud list functionality is configured by federal_black_list.
2. Do you pass STP transparently?
   Answer: Yes.
3. Does the filtering by Federal Supervision Agency for Information Technologies and Communications and Department of Justice lists work in case VAS Experts DPI processes the outbound traffic only?
   Can your system operate passing not the whole traffic but only that one bound to IP addresses from restricted resources list?
   Answer: Asymmetric connection is supported but it is not advised. The reasons are:
   - most of options become unavailable (for example, analytics requires both inbound and outbound streams for protocol analysis and so on);
   - sending the traffic according to PKH scheme (i.e. only IPs from a list) creates an additional trouble. Our SW does not support the router's control option (and it is not scheduled for future implementation). It means you have to develop this part by yourself.
4. What is the license price for dna&libzero?
   Answer: Approximately:
   - 1GbE port costs $40-55
   - 10GbE port costs $250-325

5. Can one use two ports of four-ports card 02:00.0 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01) for asymmetric filtering?
   Answer: Yes. The VAS Experts DPI runs with this network card at several of our customers.

6. The source code for libzero and DNA drivers for Intel network interfaces are available for download on ntop.org. Can you briefly describe what functionality is restricted in these drivers compared to commercial ones (http://www.nmon.net/shop/cart.php)?
   Answer: Ntop license for dna & libzero is the commercial one. There are no free or GPL licenses for these products. Some part of sources is absent. It is responsible for licensing and connection layer: a part of libzero and driver's code.

7. Does your solution allow the following connection scheme: a server has one 10G network interface. The VAS Experts DPI traffic passes through this interface by means of two VLAN representing input and output?
   Answer: No. The future support is not scheduled.

8. Can your system arrange BGP link to a border in order to export prefixes that require their traffic to be sent to the VAS Experts DPI?
   Answer: No. The future support is not scheduled.

9. Are the url2dic and ip2bin utilities source codes available? Can we get them for FreeBSD 9 x64?
   Answer: Source codes for utilities are not available and we do not plan to provide them in a future. FreeBSD allows to run native Linux applications: http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/linuxemu-lbc-install.html . The archive with binary utilities is available for FreeBSD 9.2.

10. Is the request https://IP:443 to a resource from custom_ip_black_list to be redirected in a same way as request by http (port 80)? In our case the request is plainly blocked with no redirect to "choke" page.
    Answer: https request can not be redirected. It requires decoding of the traffic using a private key or a root certificate. That is why we just block the traffic.

11. What is the aggregation logic when working by your list and external one?
    Answer: own lists are used as separate ones. They are added to cloud ones (if the service is on).

12. Can DPI pass the tagged traffic and implement filtering policy on certain VLANs?
    Answer: Yes. The VAS Experts DPI processes tagged traffic - VLAN, QinQ, MPLS.
    Currently there is no option to indicate the VLAN to block the traffic on. This functionality can be implemented in future versions.

13. All the tagged traffic passing through DPI is filtered and there is no need to create any VLANs on DPI server itself. Is it right?
    Answer: Yes.

14. The process fastdpi_1gb по top shows the load about 140% (4 core CPU) even on non connected server. Is it OK? 'top' shows CPU Load 160-220% on the flow of 50 Mb. Is it correct or we need to fix something?
    Answer: The high idle load is caused by constant queries to network cards, rather than by interrupts. This allows to achieve low latency. The higher is data flow the larger part of this load becomes a useful one. We advise to check CPU load by mpstat -P ALL utility.

15. We connected the internal local area network for tests. Ping's time remains the same. Should it be some delay?
    Answer: The equipment delay is no higher than 30 us if the equipments meets our recommendations. Ping measurements start from 1 ms. In order to detect such small delays one needs specific software and hardware. We use nanosecond timers (supported by modern network cards) in our test bench.

16. Is it possible to increase maximum number of fdpi_ctrl connections ? We have got such errors during sync billing services: ctrl : too many connections=4,max_connections=4
    Answer: Yes, its possible. Set in config file /etc/dpi/fastdpi.conf the parameter -

ctrl_max_connection=4

17. For local_passthrough=1 how DPI will process the traffic of local ASN? Where is the traffic counted? How will SSG handle traffic priority by protocols, will it take into account the traffic going to these ASNs in the general flow or not ?
    Traffic will pass through SCAT, but it will not be processed at all, netflow data will be discounted?
    local_passthrough=1 – traffic transit.
    Answer: traffic will not be processed completely, the only place where it will be accounted for is in netflow on autonomous systems.

18. In mirror schema in_dev=dna1:dna2 receives tagged traffic is DPI can clear the tag for output packets tap_dev=dnaX?
    Answer: Yes, use parameter strip_tap_tags=1 in the config file.

19. How can I get IP list for BGP /32 route ?
    Answer: to anonnce IP for BGP routes you have make script like:
    bin2ip /var/lib/dpi/blcacheip.bin > tmp.txt
    dic2host /var/lib/dpi/blcache.bin|dig +short -f -|grep -E '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' » tmp.txt
    sort -u tmp.txt > ip.lst
    For processing script use crone. Also you can use exabgp for BGP annoncing.

20. When is licence expired?

    ```
    grep 'expiration_date=' /etc/dpi/fastdpi.lic
    expiration_date=20991231
    формат: YYYYMMDD
    ```

21. How to save licences information?

    ```
    /etc/dpi/fastdpi.lic
    /etc/dpi/fastdpi.sig
    /etc/pf_ring/*
    ```