TERABIT SECURITY

DDoS Protection System

Installation Guide

Software version: 2.0

Table of contents

Introduction

DDoS Protection System (hereinafter DPS) enables companies to defend networks and critical applications against DDoS-attacks. The protection system performs external monitoring of your network, assesses critical network parameters and responds promptly, preventing a DDoS-attack. DPS provides support to a wide range of hardware manufacturers and a possibility of flexible and nonstandard installation. The system will help you ensure maximum network availability and remedy failures caused by a DDoS attack.

DPS may be supplied in the form of hardware, virtual machine image, or software, represented by an installation package. *This guide only describes the installation option using an installation package.*

Section 1 - Installation Guide

Part 1. System requirements

Requirements to hard - and software recommended for DPS installation are presented in the Table below:

Operating system	
Linux	Ubuntu 14.04.4 LTS server edition, x86_64 (http://releases.ubuntu.com/14.04.4/ubuntu-14.04.4-server-amd64.iso) without graphical environment. Kernel 4.2 required (package: linux-generic-lts-wily). Filesystem: ext4 without LVM (if possible)
Hardware	
Processor (CPU)	4-8 cores of Intel Xeon E5/E3 2.4Ghz or more (for sFLOW and NetFlow capture mode) 4 additional cores per 10GE port for mirror capture mode
Memory (RAM)	16GB ECC RAM
Disk drives (Storage)	256GB-1Tb SSD drives redundancy enabled (RAID-1 or RAID-10 recommended)
Network interfaces	Management network interface - 100-1000 mbps with assigned white/globally routable IP address (need for licensing purposes) with least 5 mbps to external networks. Capture interface NIC (for mirror capture: only Intel NIC's with e1000e, igb, ixgbe and i40e drivers; for sflow/netflow capture any NIC with 1G/10G).

Part 2. Prerequisite for Installation

Before DPS installation, you will need the hardware (the recommended requirements are presented in Part 1. System requirements) and a public ip-address that will be used for generation of the license key.

Note: in case of a change of the ip-address, the product license needs to be updated.

For the license key generation, register and make an inquiry at the licensing server https://billing.terabitsecurity.com.

To download the installation file, follow the link:
http://install.terabitsecurity.com/installer

Part 3. Installation procedure

Step	Command	Description
1	wget http://install.terabitsecurity.com/installer	Download the installation file Note: The file can be downloaded by any convenient method, use of wget is not obligatory.
2	chmod +x installer ./installer	Start of the installation process

The process of installation is performed automatically. After a correct completion of installation, the following message is displayed:

```
Install successfully completed
```

Important: in course of installation, information necessary for further work is provided:

1. The address assigned to the client's server, and for which, the license has been issued.
2. The password of admin user, used for further authorization.

As an example, a part of the installation log is presented below:

```
2016/02/24 20:26:58 Create schema
2016/02/24 20:26:59 Create config
2016/02/24 20:26:59 Create admin user
2016/02/24 20:27:00 Please login into web frontend with address http://dps_address
with login admin and password FiSbeYiL4409
2016/02/24 20:27:00 We set your email address to info@terabitsecurity.com
2016/02/24 20:27:00 Install DPS optimized drivers for traffic capture
2016/02/24 20:30:14 Update package manager cache
```

To verify the correctness of installation, make sure that the DPS-process (daemon) was automatically started. This check can be made, e.g., using the command:

```
ps -aux | grep dps
```

If the command returns information about the process, proceed to the next item of the check; if the process is not found, process should be started, using «start» command.

```
service dps start
```

or

```
service dps restart
```

Check the web site accessibility, using link http://dps_address (a link from the installer log). If the web site authorization page opens (Fig. 1.1), installation is considered to have been successful, and one may proceed to the basic system configuration.

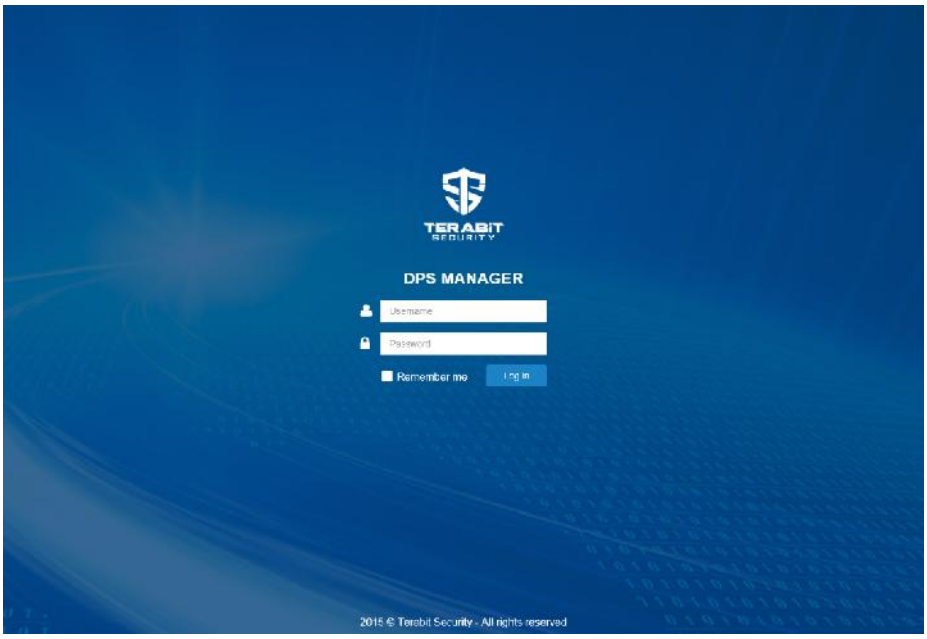

Fig. 1.1. Authorization page

In the process of installation, two packets - «DPS» and «DPS-FRONTEND» - are installed. In case of the need of their reinstallation, the following should be done, e.g., for the «DPS» packet:

```
apt-get remove dps
apt-get update
apt-get install -y dps
```

After the completion of the installation procedure, the system should be set. All settings are made, using a web interface.

Section 2 - Basic configuration

All configuration activities are performed in the Configuration section, accessible to the Sysadmin.

Step 1. Network & DDoS Mitigations – Network configuration

One should add the list of the subnets (List of your company networks) whose traffic needs to be analyzed (Fig. 2.1)

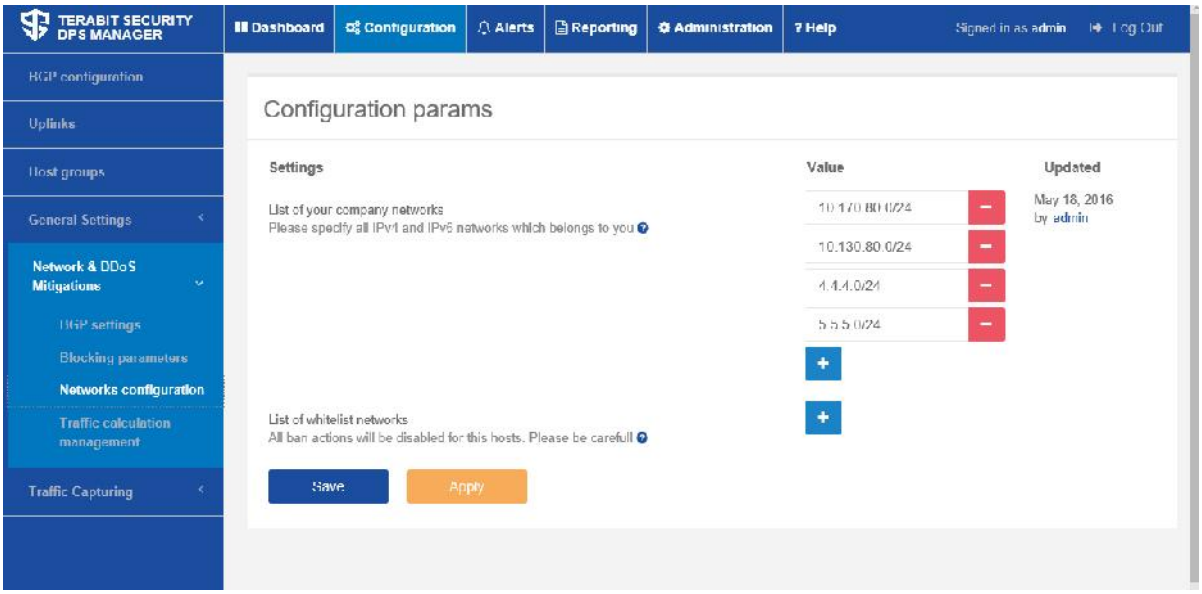

Fig. 2.1. Network configuration form

Note: in case of big network prefixes, the System load grows proportionately. The aggregate size of the networks is not to exceed /8. If bigger networks need to be supported, several independent DPS installations should be used.

If some network prefixes need to be ignored, the List of whitelist networks may be filled in for that.
After the changes are made, use Save or Apply button to save or apply those settings.

Step 2. Host Groups
Set threshold values and Mitigation Rules for the global host group - «global» (Fig. 2.2).

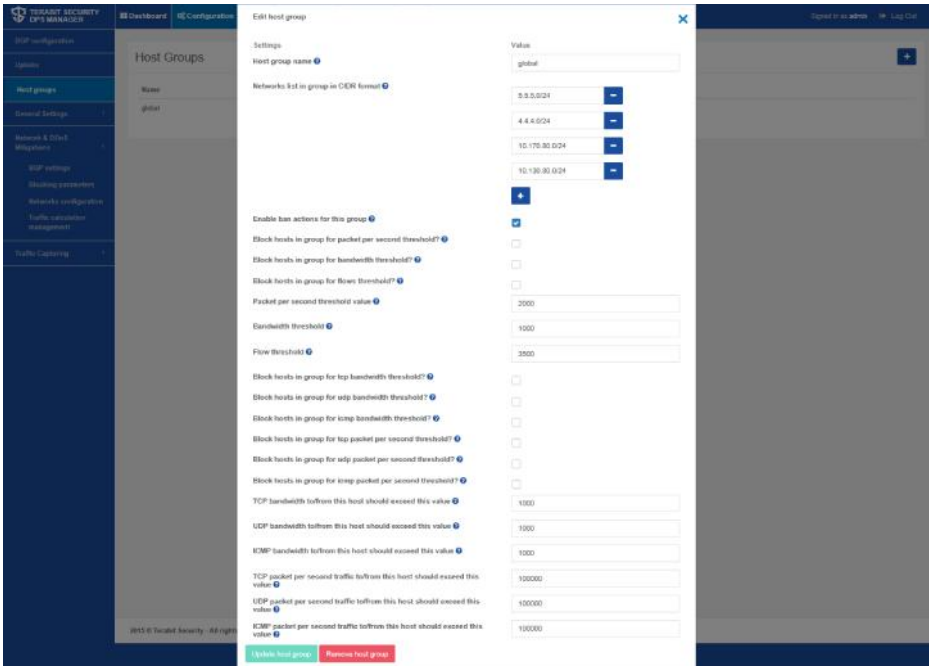

Fig. 2.2. Threshold value and mitigation rule setting form

If necessary, the network can be divided into subgroups, keeping in mind that such networks should be entered in the List of your company networks, as described in Step 1.

Step 3. Traffic Capturing

The method of traffic capture for analysis should be specified. The current DPS version supports three methods of traffic capture:

NetFlow – a network protocol designed for network traffic metering, developed by Cisco Systems company.

Mirror/SPAN – a technology of duplication of packets from one port or (VLAN) network switch to another. Cisco designates this technology as SPAN (Switched Port Analyzer).

sFlow (similar to NetFlow) - a standardized network protocol, designed for traffic analysis.

NetFlow configuration form is presented below

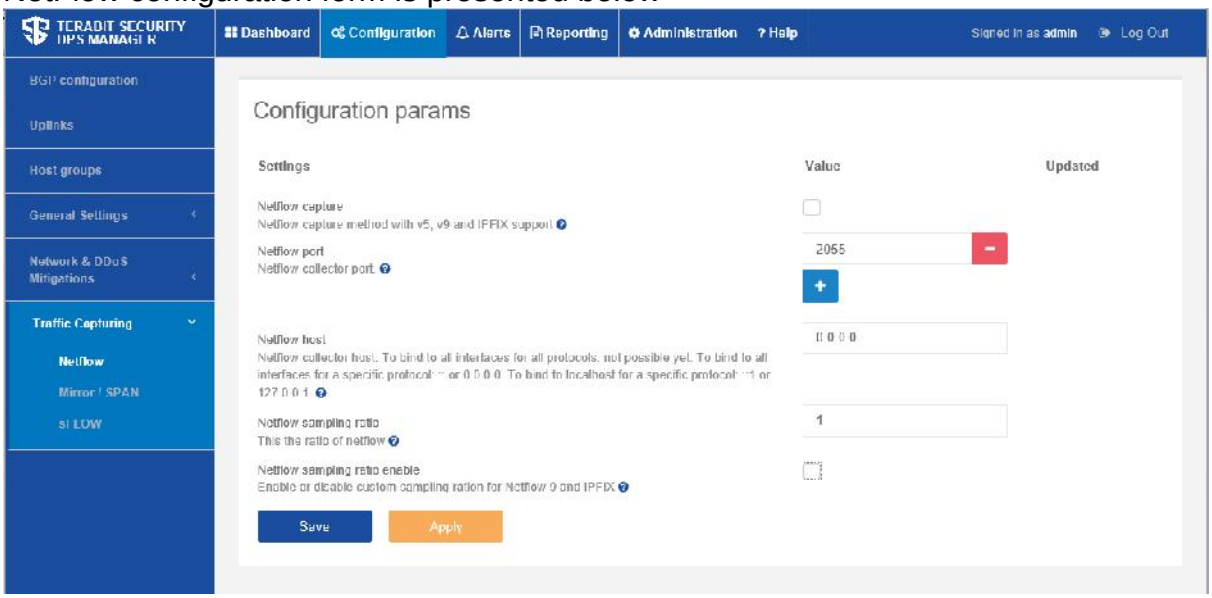

Fig. 2.3. NetFlow configuration form

Note: for NetFlow versions 9 and 10 (IPFIX), Netflow sampling ratio parameters should be set.

Mirror/SPAN configuration form is presented below (Fig. 2.4)

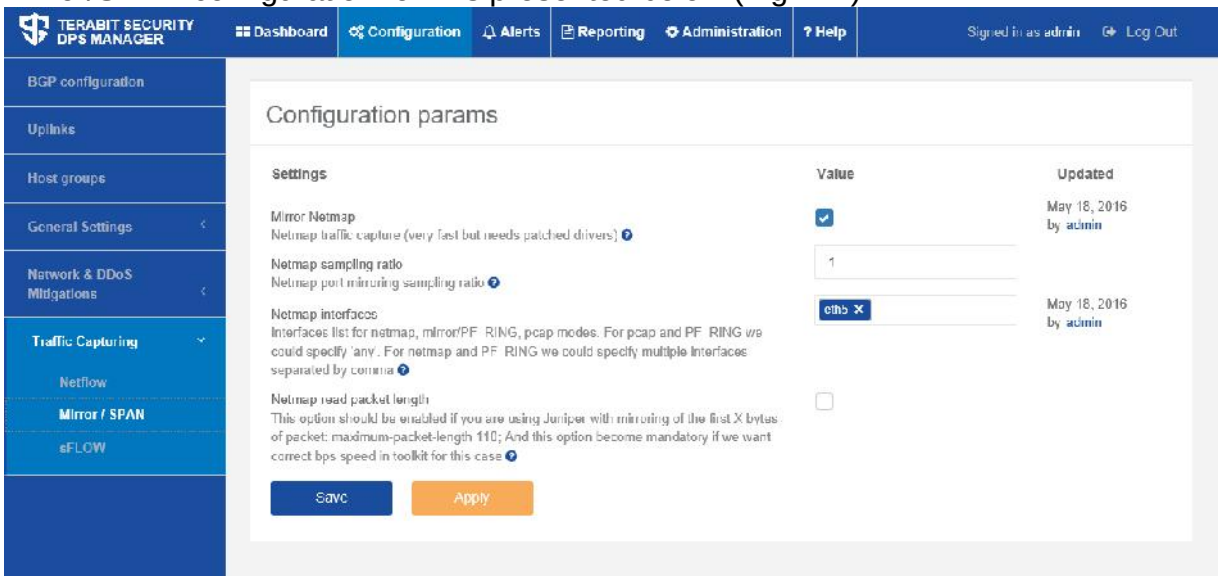

Fig. 2.4. Mirror/SPAN configuration form

sFlow monitoring may be set at all the required switch interfaces. Packet sampling is performed by hardware means, so that all the interfaces can be monitored, using very little hardware resources.

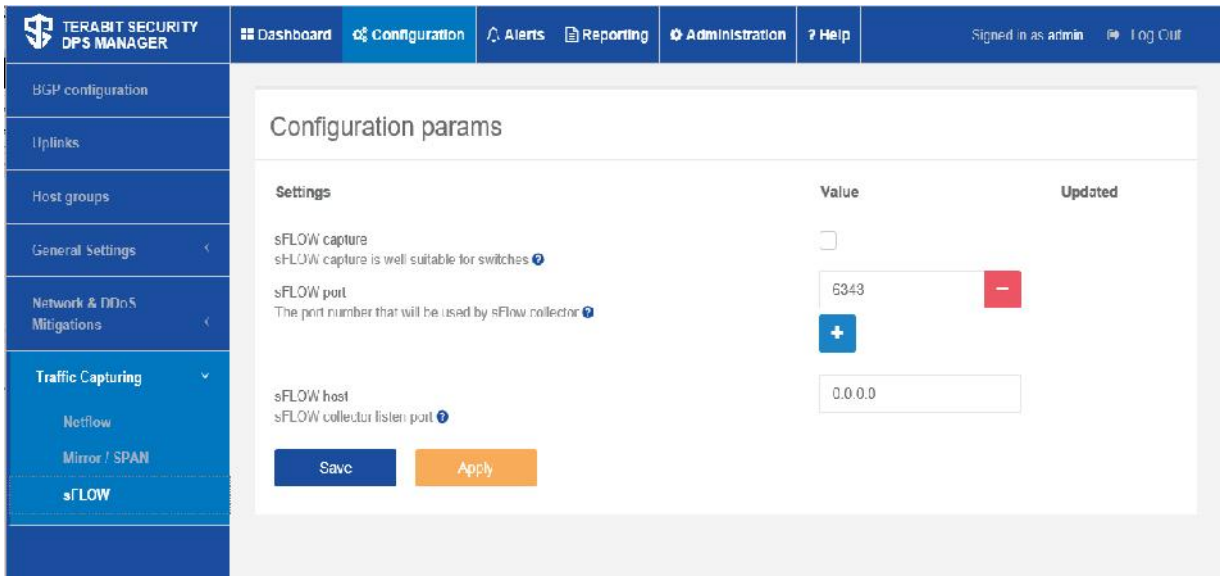

Fig. 2.5. sFlow configuration form

When choosing sFlow as a source of information for traffic analysis, it is important to choose optimal values of the sampling frequency. The sampling frequency is chosen, when sFlow is set on the switch.

The values recommended to be used for traffic monitoring in most networks are presented in the Table below. However, if the traffic level is unusually high, the sampling frequency may be reduced (for instance, a sample of 1 out of 5000 packets may be set instead of 1 out of 2000 packets for a 10 Gb/s channel).

Link speed	Sampling Rate
10 Mb/s	1 in 200
100 Mb/s	1 in 500
1 Gb/s	1 in 1000
10 Gb/s	1 in 2000

The polling counter interval is also set on the switch. The polling interval should be set so as to export values of counters at least twice more frequently than the data are sent. For instance, in order to monitor channel utilization to the accuracy of a minute, choose the polling interval from 20 to 30 seconds. SFlow polling counter presents a very efficient mechanism making it possible to perform more frequent polling at a lower cost than it would be possible using the SNMP protocol.

Step 4. Network & DDoS Mitigations – Traffic calculation management

For sFlow or Mirror protocols, Traffic calculation management settings may be left unchanged (by default).

For NetFlow v5, v9, v10 (ipfix) minimum possible values of the parameters of active / inactive flow timeout should be set on the equipment, noting that those values should coincide with each other. After that, the value of the average calculation time for subnets is set, exceeding the value of active / inactive flow timeout by 5-10 seconds.

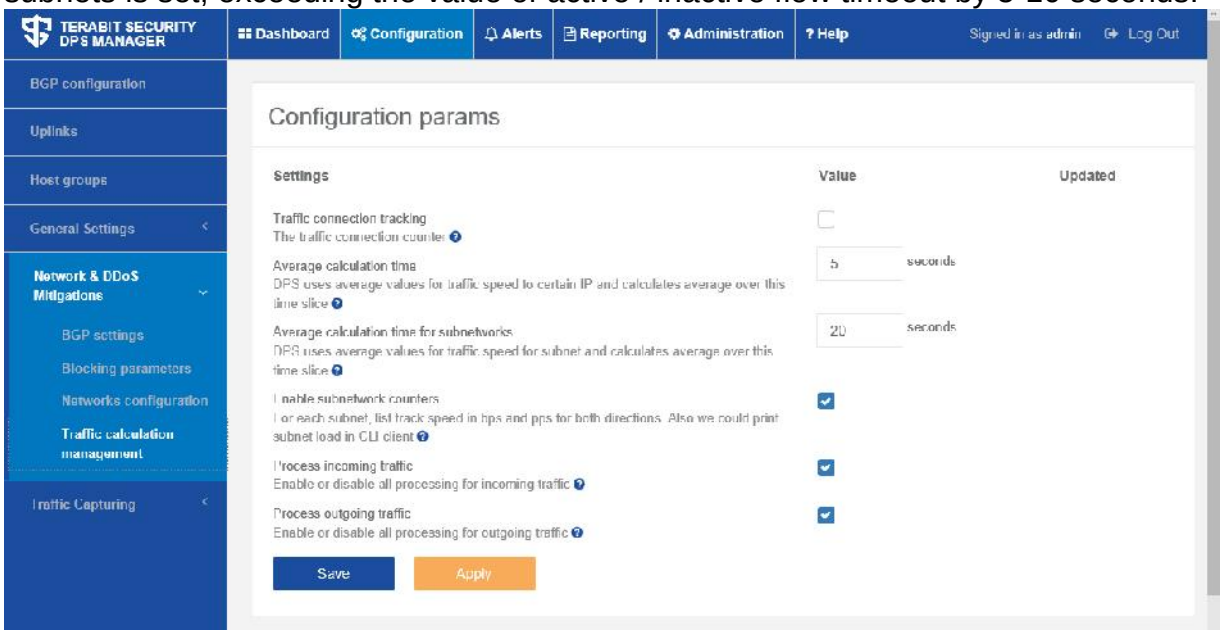

Fig. 2.6. Traffic calculation parameters configuration form

For instance, the router supports the minimum parameter value for active flow timeout - 30 seconds, for inactive flow timeout - 45 seconds. In such case, the bigger supported value is set on the equipment, namely: active flow timeout - 45 seconds and inactive flow timeout - 45 seconds. Respectively, the average calculation time in DPS is set equal to 50 seconds (45+5).

Note: active flow timeout shows how frequently the NetFlow cache is updated with active session traffic data; inactive flow timeout shows the time during

which, in absence of data transmission in the current flow, it closes, and the information thereof is written in the cache.

Step 5. BGP configuration

Next, the parameters of BGP setting should be set for a DPS session with network appliances. For that, add configuration for the «peer» by pushing «+» button (Fig. 2.7).

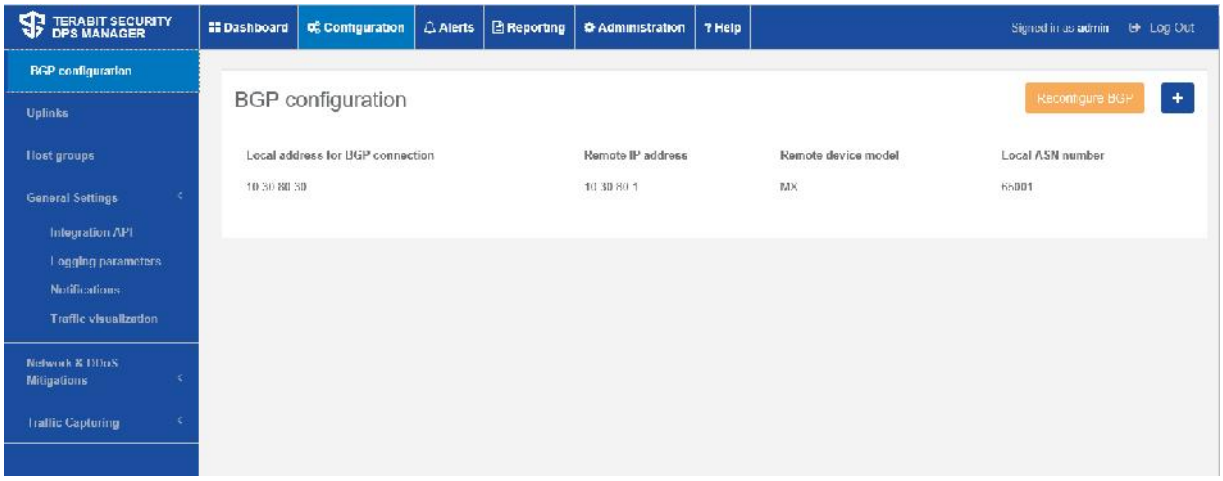

Fig. 2.7. List of BGP connections

The BGP connection parameters setting form is presented below (Fig. 2.8)

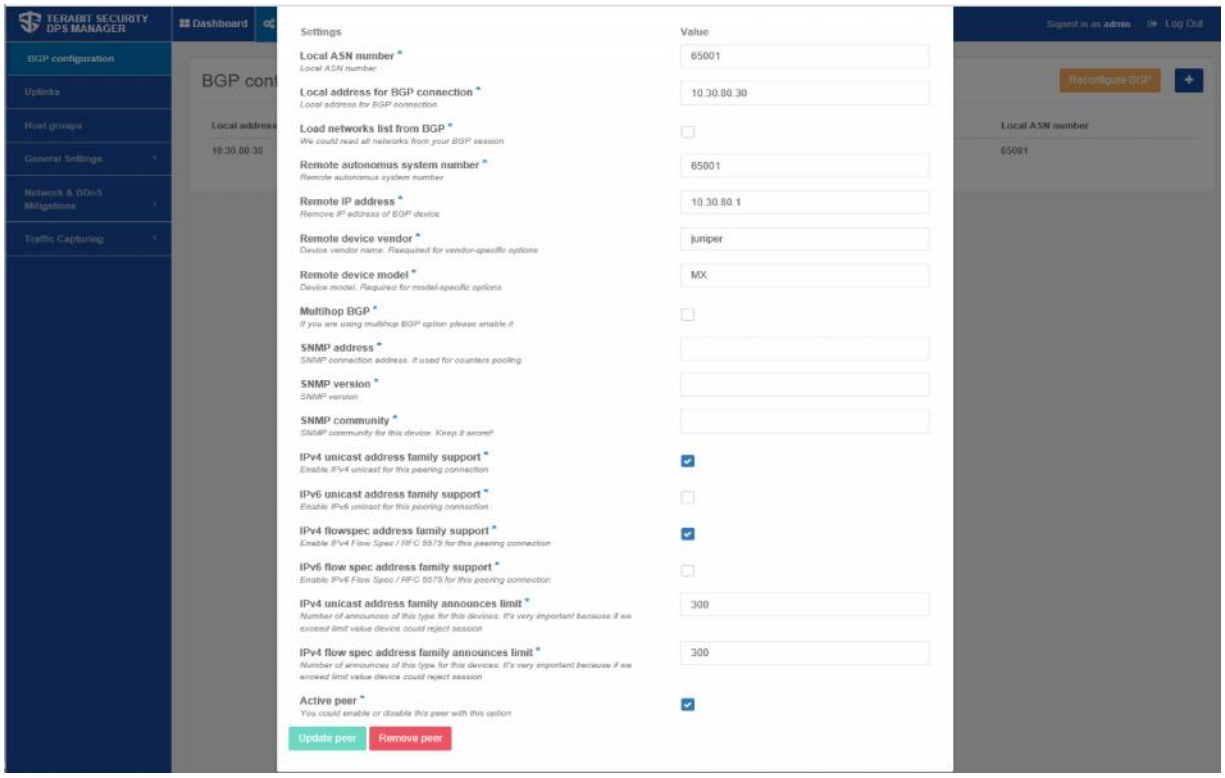

Fig. 2.8. BGP connection setting form

Note: description of parameters specified during BGP setting can be found in the relevant RFC, « Additional information» section.

The following parameters are obligatory:

- Local/Remote autonomous system number (ASN) (local and remote autonomous system number).
- Local/Remote address for BGP connection (local ip-address and remote ip-address for BGP session setting).
- Remote device vendor and model (remote device manufacturer and model).
- Set of parameters IPv4/IPv6 unicast and flowspec address family support.
- Announces limit – limitation of the number of the announced routes.

Parameters «Multihop BGP option» and SNMP options are not obligatory and are set on an as-needed basis.

A session with a «peer» is activated/deactivated by pushing the button «Active peer».

After changes are made, use Save & Apply button to save and apply those settings.

BGP client settings can be performed, using the page Network & DDoS Mitigations – BGP settings (Fig. 2.9)

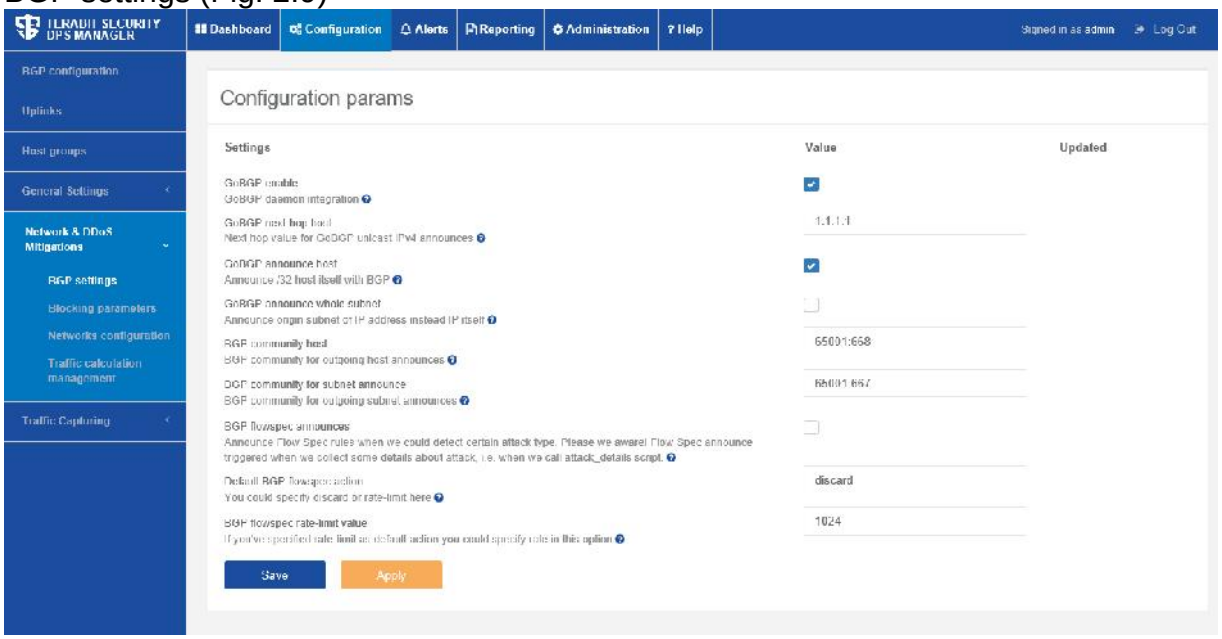

Fig. 2.9. BGP configuration form

Step 6. Network & DDoS Mitigations – Blocking parameters

Below (Fig. 2.10) is the form of traffic block settings in case of a threat of a DDoS attack. At the stage of initial setting and testing DPS it is recommended to leave all parameters of traffic blocking unchanged, since this mode impacts commercial traffic, and incorrect settings can bring adverse effects.

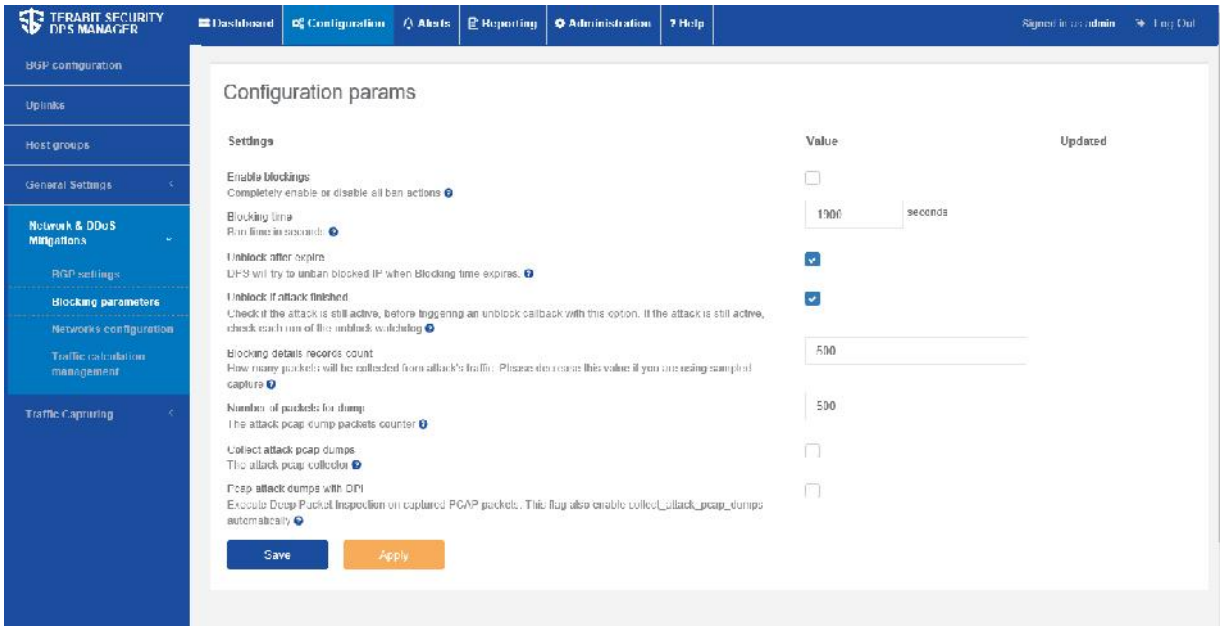

Fig. 2.10. Traffic block settings form

Step 7. General Settings – Logging, Notifications, Traffic visualization parameters

This step involves setting of logging, delivery of messages about attack events, and setting of traffic visualization parameters. The setting forms are presented on Fig. 2.11, 2.12, 2.13.

After the System installation, it is recommended to leave those settings unchanged.

Logging of system events lets you use both the syslog for the system, on which DPS is installed, and the syslog of a remote device.

Logs are stored in the «/var/log/dps/dps.log» file.

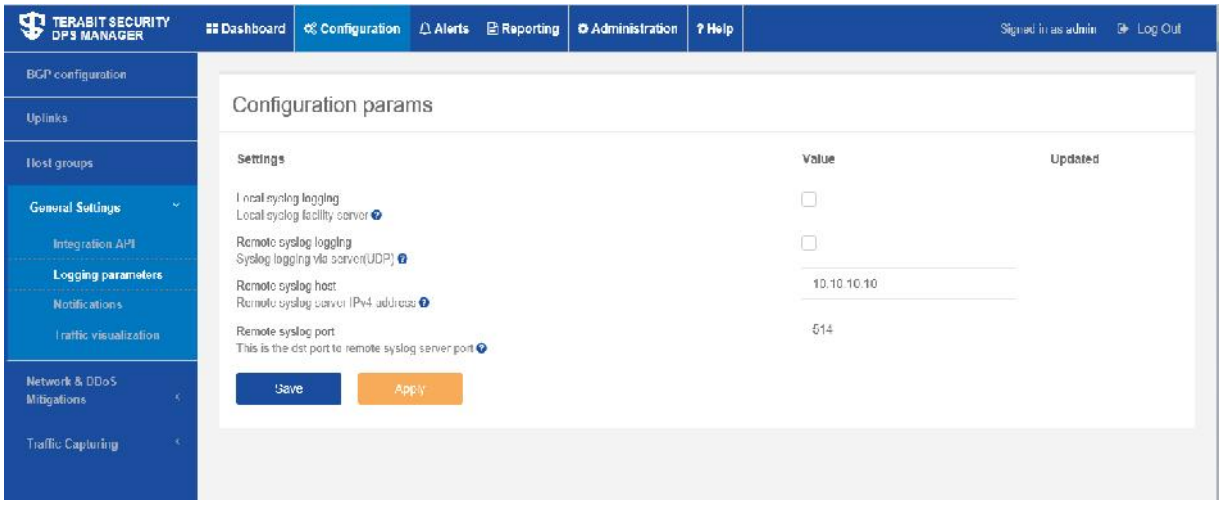

Fig. 2.11. Logging setting form

Traffic visualization form is used to set data display format and DPS Dashboard graphs (Fig. 2.12).

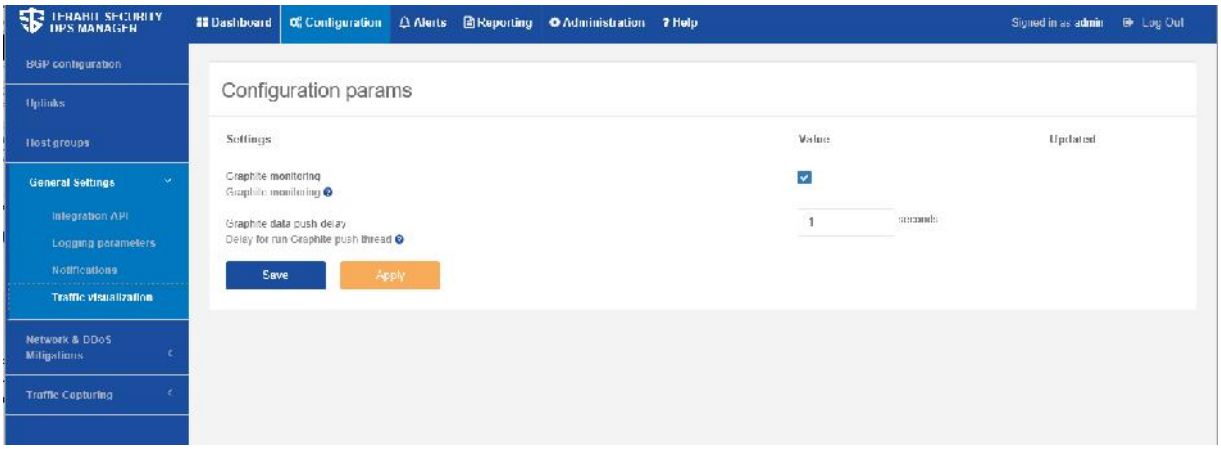

Fig. 2.12. Traffic visualization setting form

Step 8. Users

At that step, accounts of DPS administrators can be managed. During the first access to the form, there should be one account in the list of users, which is created automatically during DPS installation («Installation procedure» section).

Fig. 2.14 shows a form with the list of users, where an account can be added, blocked or deleted.

The form of account parameters' editing (Fig. 2.14) lets you change the password, email, role, activate the function of acceptance of events (is active), specify the period of time allowed to accept events, and appoint the relevant host group, chosen from the list of host groups set during Step 2.

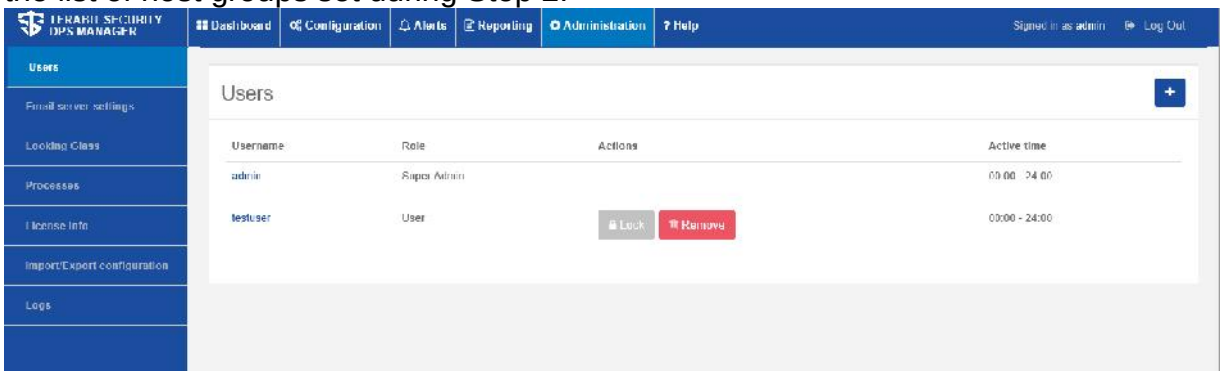

Fig. 2.13. List of users

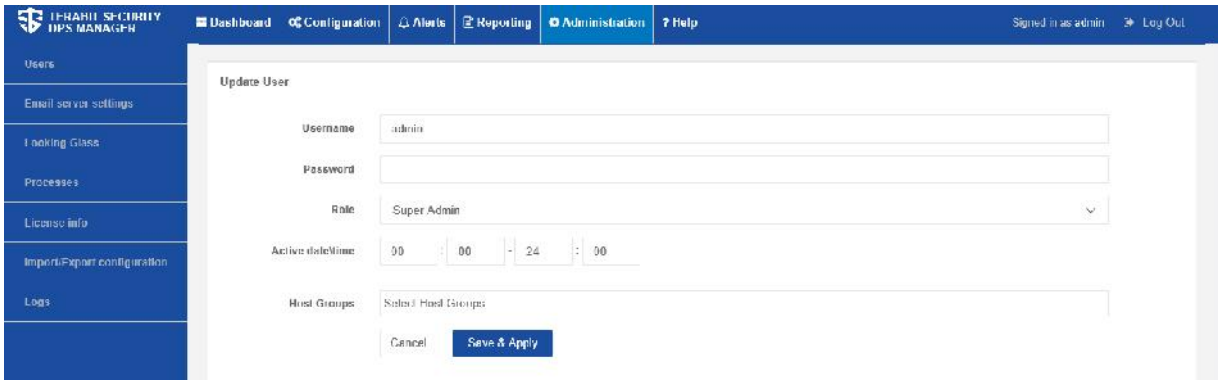

Fig. 2.14. DPS administrator account editing form

Step 9. Dashboard

After the configuration is changed, correctness of the settings made must be checked. This can be done using DPS Dashboard that graphically presents traffic information (Fig. 2.15).

Note: at initial setting, graph plotting will take some time, dependent on the capacity of your system.

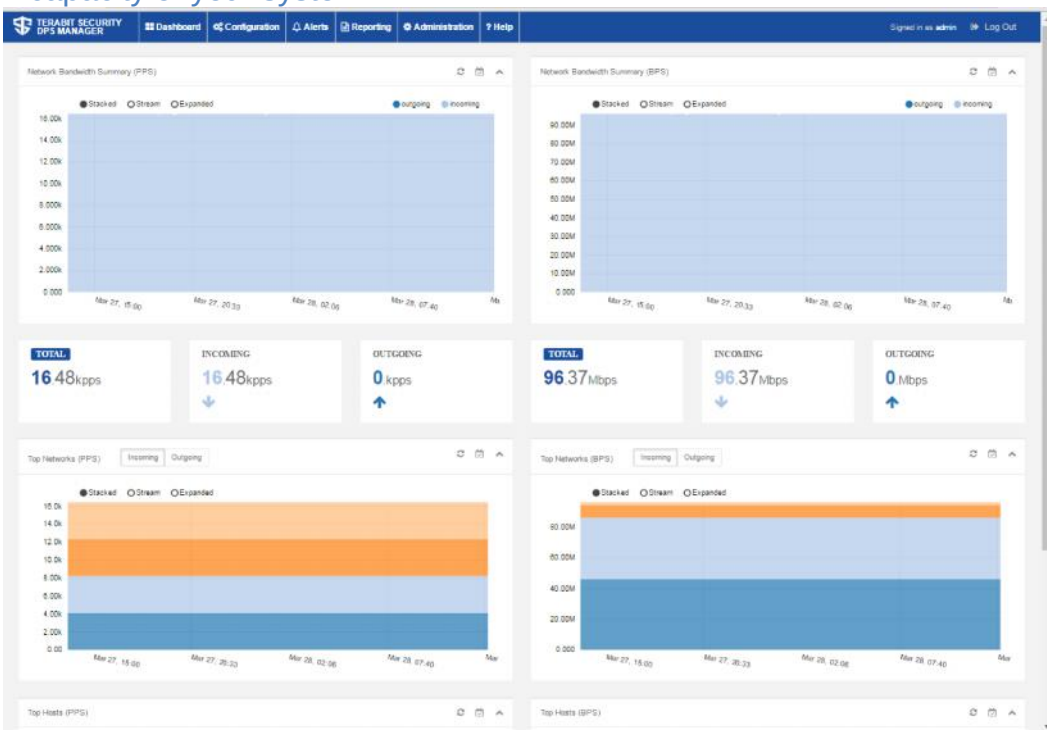

Fig. 2.15. Dashboard

Section 3 - Possible errors and recommendations of their remedy

1. Access to a resource with an installation file is forbidden

```
root@DPS-u14:~# wget http://install.terabitsecurity.com/installer -Oinstaller
--2016-02-24 17:49:32--  http://install.terabitsecurity.com/installer
Resolving install.terabitsecurity.com (install.terabitsecurity.com)...
136.243.59.72
Connecting
to install.terabitsecurity.com (install.terabitsecurity.com)|136.243.59.72|:80...
connected.
HTTP request sent, awaiting response... 403 Forbidden
2016-02-24 17:49:32 ERROR 403: Forbidden.
```

In case of emergence of such situation please verify the presence of a license and check if your ip-address corresponds to the address, for which the license was issued. You should also check if access from your ip-address is allowed, and if the port at the licensing server is open.

Check accessibility of the ip-address accordingly, using the command:

```
$ ping license.terabitsecurity.com
```

In case of successful execution, this command is to return, e.g., the following result:

```
Reply from 136.243.59.72: bytes=32 time=36ms TTL=47
```

Check, if the port at the licensing server is open, using the command:

```
$ telnet 72.59.243.136 10777
```

In case of successful execution, this command is to return, e.g., the following result:

```
Trying 72.59.243.136...
Connected to 72.59.243.136.
Escape character is '^]'.
Connection closed by foreign host
Connection closed by foreign host means the remote PORT is OPEN, if REFUSED it means the remote port is closed
```

2. Use of a non-standard version of Ubuntu kernel.

```
You are using not standard Ubuntu 14.04's kernel. We could try to work with it but could not guarantee stability
Please install recommended standard long term support kernel version: 3.13:
```

In case of emergence of such situation please verify the version of the kernel of your operating system. If your kernel version is obsolete (older than 3.13), the kernel of your operating system needs to be reinstalled; if your kernel version is higher than 3.13, this will cause no problems in DPS operation.

In case of emergence of problems, which you cannot solve on your own, you may apply to the support service by email **support@terabitsecurity.com**

Section 4 - Additional information

Useful links

Description	Link
Web site	https://terabitsecurity.com
Blog	https://terabitsecurity.com/blog
Installation download link	http://install.terabitsecurity.com/installer
Support	http://support.terabitsecurity.com support@terabitsecurity.com

RFC list

RFC	Description
RFC 4271	Protocol BGP-4 (https://tools.ietf.org/html/rfc4271)
RFC 4760	Multiprotocol Extensions for BGP-4 (https://tools.ietf.org/html/rfc4760)
RFC 5575	Dissemination of Flow Specification Rules (https://tools.ietf.org/html/rfc5575)
RFC 4893	BGP Support for Four-octet AS Number Space (https://tools.ietf.org/html/rfc4893)
RFC 7011	Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information (https://tools.ietf.org/html/rfc7011)
RFC 7015	Flow Aggregation for the IP Flow Information Export (IPFIX) Protocol (https://tools.ietf.org/html/rfc7015)
RFC 5103	Bidirectional Flow Export Using IP Flow Information Export (IPFIX) (https://tools.ietf.org/html/rfc5103)
RFC 7606	BGP Communities Attribute (https://tools.ietf.org/html/rfc1997)
RFC 4360	BGP Extended Communities Attribute (https://tools.ietf.org/html/rfc4360)

IOS XR configuration example

Part 1. Exporter Map

To configure the Exporter map, you need to define the destination (flow collector server), the source interface, the port used for exporting, the version of NetFlow, and the timeout rates.

```
ios-xr(config)# flow exporter-map ANALYZER-EM
ios-xr(config-fem)# destination 172.30.2.2
ios-xr(config-fem)# source gi0/0/0/0
ios-xr(config-fem)# transport udp 2055
ios-xr(config-fem)# version v9
ios-xr(config-fem)# template data timeout 60
ios-xr(config-fem)# options interface-table timeout 60
ios-xr(config-fem)# exit
```

Part 2. Sampler Map

The Sampler map defines the sample rate, recommended sample value is 10000 for optimal performance.

```
ios-xr(config)# sampler-map ANALYZER-SM
ios-xr(config-sm)# random 1 out-of 10000
ios-xr(config)# exit
```

Part 3. Flow Monitor Map

The Flow Monitor map defines the cache timeout values and associates the exporter map with this map.

```
ios-xr(config)# flow monitor-map ANALYZER-FMM
ios-xr(config-fmm)# record ipv4
ios-xr(config-fmm)# exporter ANALYZER-EM
ios-xr(config-fmm)# cache timeout active 60
ios-xr(config-fmm)# cache timeout inactive 15
ios-xr(config-fmm)# exit
```

Part 4. Next you need to apply the maps to the appropriate interfaces

Now that you have your maps defined, you need to apply the Flow Monitor and Sampler maps to each of your active interfaces:

```
ios-xr(config)# interface Gi0/0/0/0
ios-xr(config-if)# flow ipv4 monitor ANALYZER-FMM sampler ANALYZER-SM ingress
ios-xr(config-if)# exit
```

After you have the NetFlow configuration completed, you can analyze the data with DPS.

For more information, see NetFlow Commands on Cisco ASR 9000 Series Router and NetFlow Commands on Cisco IOS XR Software.

Description	Links
Cisco	http://www.cisco.com
Cisco ASR 9000 Series Aggregation Services Router Netflow Configuration Guide	http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-2/netflow/configuration/guide/b_netflow_cg42asr/b_netflow_cg42asr_chapter_00.html
Configuration Guides	http://www.cisco.com/c/en/us/support/routers/asr-9000-series-aggregation-services-routers/products-installation-and-configuration-guides-list.html

Junos BGP Configuration example

Here is the example of the **BGP session settings** for **unicast** and **flow_spec** for Juniper MX series routers (Junos 14.2R3.8) group DPS_BGP:

```
protocols {
    bgp {
        group DPS_BGP {
            type internal;
            local-address 10.30.80.1;
            family inet {
                unicast;
                flow {
                    no-validate NO-VALIDATION;
                }
            }
            peer-as 65001;
            local-as 65001;
            neighbor 10.30.80.30;
        }
    }
```

Part 1. NLRI FlowSpec Validation

FlowSpec BGP update received should pass Validation Steps before their installation from the Adj-RIB-IN to LOC-RIB. Next-Hop validation must not be taken into account, because NH FlowSpec (RFC 5575) is always set to 0. But other Validations have to be done before installation (extracted from RFC):

a) The originator of the flow specification matches the originator of the best-match unicast route for the destination prefix embedded in the flow specification.

b) There are no more specific unicast routes, when compared with the flow destination prefix, that have been received from a different neighboring AS than the best-match unicast route, which has been determined in step a).

These validations can cause some problems when you use for example external Server to inject FlowSpec updates. Implementations may de-activate these validation steps

To add policy-options NO-VAIDATION:

```
policy-options {
    policy-statement NO-VALIDATION {
        term 1 {
            then accept;
        }
    }
```

Part 2. Junos traffic capturing Configuration

a) Below is the configuration for and Configuration of the traffic mirroring:

(i) Here are settings for the mirroring instance for traffic capturing (family inet in our case), also we set the output interface (xe-0/1/0.0) for captured traffic:

```
set forwarding-options port-mirroring input rate 1
set forwarding-options port-mirroring input run-length 1
set forwarding-options port-mirroring input maximum-packet-length 9200

set forwarding-options port-mirroring family inet output interface xe-
0/1/0.0 next-hop 172.30.2.2
set forwarding-options port-mirroring family inet output no-filter-check
```

(ii) Firewall filter settings for traffic capturing (also family inet):

```
set firewall family inet filter agl-mirror-inet term 1 then count agl-
mirror-inet_1
set firewall family inet filter agl-mirror-inet term 1 then log
deactivate firewall family inet filter agl-mirror-inet term 1 then log
set firewall family inet filter agl-mirror-inet term 1 then port-mirror
set firewall family inet filter agl-mirror-inet term 1 then accept
```

Firewall filter we will apply later on the interfaces we want to mirror traffic on (input and/or output direction depending on our needs):

```
set interfaces xe-0/1/1 unit 331 family inet filter input agl-mirror-inet
set interfaces xe-0/1/1 unit 331 family inet filter output agl-mirror-inet
```

Complete configuration example of the source interface for traffic mirroring:

```
set interfaces xe-0/1/1 description External_link
set interfaces xe-0/1/1 hierarchical-scheduler
set interfaces xe-0/1/1 flexible-vlan-tagging
set interfaces xe-0/1/1 mtu 9100
set interfaces xe-0/1/1 encapsulation flexible-ethernet-services

set interfaces xe-0/1/1 unit 331 vlan-id 331
set interfaces xe-0/1/1 unit 331 family inet filter input agl-mirror-inet
set interfaces xe-0/1/1 unit 331 family inet address 10.30.60.1/24
```

Output layer 3 interface, we send captured traffic (link to DPS analyzer):

```
set interfaces xe-0/1/0 description "Inet_mirroring_output_to_DPS_SRV"
set interfaces xe-0/1/0 hierarchical-scheduler
set interfaces xe-0/1/0 flexible-vlan-tagging
set interfaces xe-0/1/0 mtu 1500
set interfaces xe-0/1/0 encapsulation flexible-ethernet-services
set interfaces xe-0/1/0 gigether-options no-auto-negotiation
set interfaces xe-0/1/0 unit 0 vlan-id 70
set interfaces xe-0/1/0 unit 0 family inet
address 172.30.2.1/24 arp 172.30.2.2 mac 38:ea:a7:33:88:f0
```

It is the same interface we pointed earlier in the port-mirroring forwarding instance settings as the output interface:

```
set forwarding-options port-mirroring family inet output interface xe-
0/1/0.0 next-hop 172.30.2.2
```

(iii) Configuration is completed, check the results:

```
Junos> show forwarding-options port-mirroring
Instance Name: &global_instance
  Instance Id: 1
  Input parameters:
    Rate                  : 1
    Run-length            : 1
    Maximum-packet-length : 9200
  Output parameters:
    Family              State     Destination          Next-hop
    inet                up        xe-0/1/0.0           172.30.2.2
```

b) Sampling instance configuration (example for version-ipfix).

Note: before configuring the traffic sampling please check the hardware - you need to have the MPC cards installed in your device.

(iv) First of all you need to create the templates with the timeouts for traffic sampling:

```
set services flow-monitoring version-ipfix template ipv4-template flow-
active-timeout 60
set services flow-monitoring version-ipfix template ipv4-template flow-
inactive-timeout 30
set services flow-monitoring version-ipfix template ipv4-template
template-refresh-rate seconds 10
set services flow-monitoring version-ipfix template ipv4-template option-
refresh-rate seconds 10
set services flow-monitoring version-ipfix template ipv4-template ipv4-
template
```

(v) Activate the sampling instance on the appropriate MPC card (chassis config) and also in the global configuration settings:

```
 set chassis fpc 4 sampling-instance ipfix

set forwarding-options sampling instance ipfix input rate 100
set forwarding-options sampling instance ipfix family inet output flow-
server 172.30.2.2 port 2055
set forwarding-options sampling instance ipfix family inet output flow-
server 172.30.2.2 version-ipfix template ipv4-template
set forwarding-options sampling instance ipfix family inet output inline-
jflow source-address 172.30.2.1
```

(vi) Configure the interfaces you want to sample traffic on (input and/or output direction depending on your needs):

```
set interfaces xe-0/1/1 unit 331 family inet sampling input
```

Note: before the applying sampling filter on interface, you need to deactivate all the filters you used for traffic mirroring if they were applied before on this interface.

(vii) Check the sampling:

```
> show services accounting flow inline-jflow fpc-slot 4
  Flow information
    FPC Slot: 4
```

```
    Flow Packets: 686237393, Flow Bytes: 807732897754
    Active Flows: 2, Total Flows: 4860
    Flows Exported: 4857, Flow Packets Exported: 4857
    Flows Inactive Timed Out: 1, Flows Active Timed Out: 4857
```

Related links from Juniper TechDocs:

Description	Links
Juniper Networks	http://www.juniper.net
Juniper TechLibrary	http://www.juniper.net/techpubs/
Junos OS Services Interfaces Library for Routing Devices	http://www.juniper.net/techpubs/en_US/junos15.1/information-products/pathway-pages/services-interfaces/index.html
Active Flow Monitoring Overview	http://www.juniper.net/techpubs/en_US/junos15.1/information-products/pathway-pages/services-interfaces/flow-monitoring.html
Configuring Traffic Sampling	http://www.juniper.net/documentation/en_US/junos15.1/topics/usage-guidelines/services-configuring-traffic-sampling.html
Monitoring, Sampling, and Collection Services Interfaces Feature Guide for Routing Devices	http://www.juniper.net/techpubs/en_US/junos15.1/information-products/pathway-pages/services-interfaces/flow-monitoring.pdf

IOS XR Blackhole Configuration Example

a) (Optional) Configuration on the Trigger Router:

Configure a static route redistribution policy that sets a community on static routes marked with a special tag 777, and apply it in BGP:

```
route-policy Blackhole-trigger
  if tag is 777 then
    set community (65001:668, no-export) additive
    pass
  else
    pass
  endif
  end-policy

router bgp 65001
 address-family ipv4 unicast
  redistribute static route-policy Blackhole-trigger
 !
 neighbor 10.30.80.30
  remote-as 65001
  address-family ipv4 unicast
   route-policy bgp_all in
   route-policy bgp_all out
```

Configure a static route with the special tag for the source prefix that needs to be black-holed:

```
router static
 address-family ipv4 unicast
 10.7.7.7/32 Null0 tag 777
```

You can also add there the static routes you need to blackhole to mitigate DDoS attack manually. But the better choice is to use the route policy to discard the unicast BGP announces from DPS BGP daemon. Details pointed in next chapter.

b) Configuration on the Border Router:

Configure a route policy that matches the community set on the trigger router and configure set next-hop discard:

```
route-policy Blackhole
  if community matches-any (65001:668, 65001:667) then
    set next-hop discard
  else
    pass
  endif
end-policy
```

Use this configuration to discard the traffic for unicast routes announced from the DPS BGP daemon (please use options BGP community host 65001:668

and BGP community for subnet announces 65001:667 in DPS BGP configuration).

Apply the route policy on the iBGP peers:

```
router bgp 65001
 address-family ipv4 unicast
 !
 neighbor 10.30.80.30
  remote-as 65001
  address-family ipv4 unicast
   route-policy Blackhole in
   route-policy bgp_all out
```

For more information, see Commands on Cisco ASR 9000 Series Router and on Cisco IOS XR Software.

Description	Links
ASR9000 Source-based Remotely Triggered Blackhole Filtering with RPL Next-hop Discard Configuration Example	http://www.cisco.com/c/en/us/support/docs/routers/asr-9000-series-aggregation-services-routers/116386-configure-asr9000-00.html
Tutorial: Options for Blackhole and Discard Routing	https://www.nanog.org/meetings/nanog32/presentations/soricelli.pdf

Junos Blackhole Configuration Example

On all BGP routers in your network you need set a route that will be discarded:

```
lab_user@MX-1> show configuration routing-options
static {
    route 10.7.7.7/32 discard;
}
```

On all routers for routes learned with a certain community set their next-hop pointing to the discard route:

```
lab_user@MX-1> show configuration policy-options
policy-statement BLACK-HOLE-FILTER {
    term 1 {
        from community BLACK_HOLE;
        then {
            next-hop 10.7.7.7;
        }
    }
}
community BLACK_HOLE members [ 65001:668 65001:667 ];
}
```

Apply this as an inbound filter on iBGP sessions (and for BGP session with your DPS BGP daemon):

```
lab_user@MX-1> show configuration protocols bgp group DPS_SRV
import BLACK-HOLE-FILTER;
```

Configure the route policy that matches the community set on the trigger router or your DPS BGP daemon and configure next-hop to discard. Use this configuration to block blackhole routes on your network. This will discard the traffic for unicast routes announced from the DPS BGP daemon (please use options BGP community host 65001:668 and BGP community for subnet announces 65001:667 in DPS BGP configuration).