NSCFLOW

Automatic DDoS attack blocking system.

What is DDoS?

DDoS (Distributed Denial of Service) is a cyberattack in which many infected devices or computers (called botnets) are used to overload an online service, a website, or a server by sending a large number of requests in a short period of time. The goal of a DDoS attack is to make the service or server unusable for legitimate users, causing service disruptions, delays in response, or total denial of service access. This can affect many areas, including businesses, government institutions, and critical infrastructure. DDoS attacks are often difficult to defend against, as they come from many distributed sources, making it difficult to block malicious traffic without affecting legitimate traffic.

Main features of NSCFLOW.

- **~1-2** Seconds reaction and interaction to traffic anomalies.
- Monitors both IPv4 and IPv6 protocols.
- Theoretically unlimited monitoring capacity.
- Web Dashboard interface for interaction and monitoring.
- Real-time graphical monitoring of traffic and anomalies.
- **Personalized** notifications in Email/SMS/SysLog etc.
- Accepts several telemetry protocols such as Netflow/sFlow/jFlow/IPFIX.
- Proactive monitoring of vulnerable ports such as 22,23,53,123,161,546,1900,5060,8728 etc.
- Software segmented according to functions to increase the security of functionality. Also, each software is compiled in Binary file and uses the CPU with Multithreading technology.
- High-performance **Scrubber**/Firewall, which makes decisions in less than 30microseconds. And +100Gbps capacity for each physical Server.
- Personalized limits for each IP or IPv4/6 Subnet.
- Enables BGP connections with the corresponding policy for each connection.
- Enables BGP FlowSpec and RTBH.
- Enables connections between different ISPs for the exchange of malicious IPs. So, if an IP attacks one of the ISPs, that SrcIP is automatically blocked in the others that use the NSCFLOW system.
- The software will be engineered **according to the ISP's** network design, policies, and service objectives.

DDoS Defense Techniques.

There are 3 main types of DDoS attacks, each with their own strategies and defense tools:

1. Volume-based attacks.

These attacks create a large number of requests at the network level, overwhelming network devices or servers. Some examples are UDP floods, ICMP floods, and forged packet attacks.

To protect against these attacks, anti-DDoS providers use powerful “scrubbing” techniques, where cloud or on-premises servers analyze traffic, block malicious requests, and allow legitimate ones. This method can withstand massive multi-gigabyte scale attacks. This is also known as DDoS deflation.

2. Protocol attacks.

These attacks take advantage of vulnerabilities in network protocols, such as SYN floods, fragmented packets, and Ping of Death.

Anti-DDoS defense tools block malicious traffic before it reaches your servers. More advanced solutions analyze traffic to distinguish legitimate users from automated clients and malicious bots.

3. Application-level attacks.

These attacks target application services and appear to come from real users. Examples include GET/POST floods, “low-and-slow” attacks, or attacks specific to Apache or Windows.

NSCFLOW Intelligent DDoS Detection & Mitigation Software.

This software is an advanced solution for monitoring and analyzing network traffic. This system combines NetFlow and sFlow data with network route information learned from BGP, enabling in-depth traffic analysis and providing near-real-time visibility into DDoS attacks.

Features:

- Automatic detection & classification of DDoS attacks.
- Traffic routing analysis to identify anomalous behavior.
- A unified process for detecting, classifying, tracking, and mitigating DDoS attacks.
- Integrated management with NSCFLOW Scrubber/Firewall, a powerful attack repelling system.

Attack Detection.

Many modern DDoS attacks use multi-vector attack strategies, combining several attack types simultaneously to evade traditional defenses. Such attacks usually target a specific IP, and changes in traffic patterns can be detected through NetFlow telemetry.

How does NSCFLOW detect attacks?

- Host Detection – Monitors all traffic passing through the network to detect suspicious changes.
- Fast Flood Detection – Can detect an attack in about 1-2 seconds, using automatic algorithms for threshold and time analysis.
- Unified System – The system has a dedicated service for each telemetry protocol such as Netflow-v5/v9, sFlow and IPFIX where this service reports the processed data to the central system.

How is telemetry reported to NSCFLOW

1. **sFlow**

The sFlow protocol (RFC 3176) is used, which is distinguished by the speed of traffic reporting. With this protocol, traffic anomalies can be detected within 1-2 seconds.

2. **NetFlow**

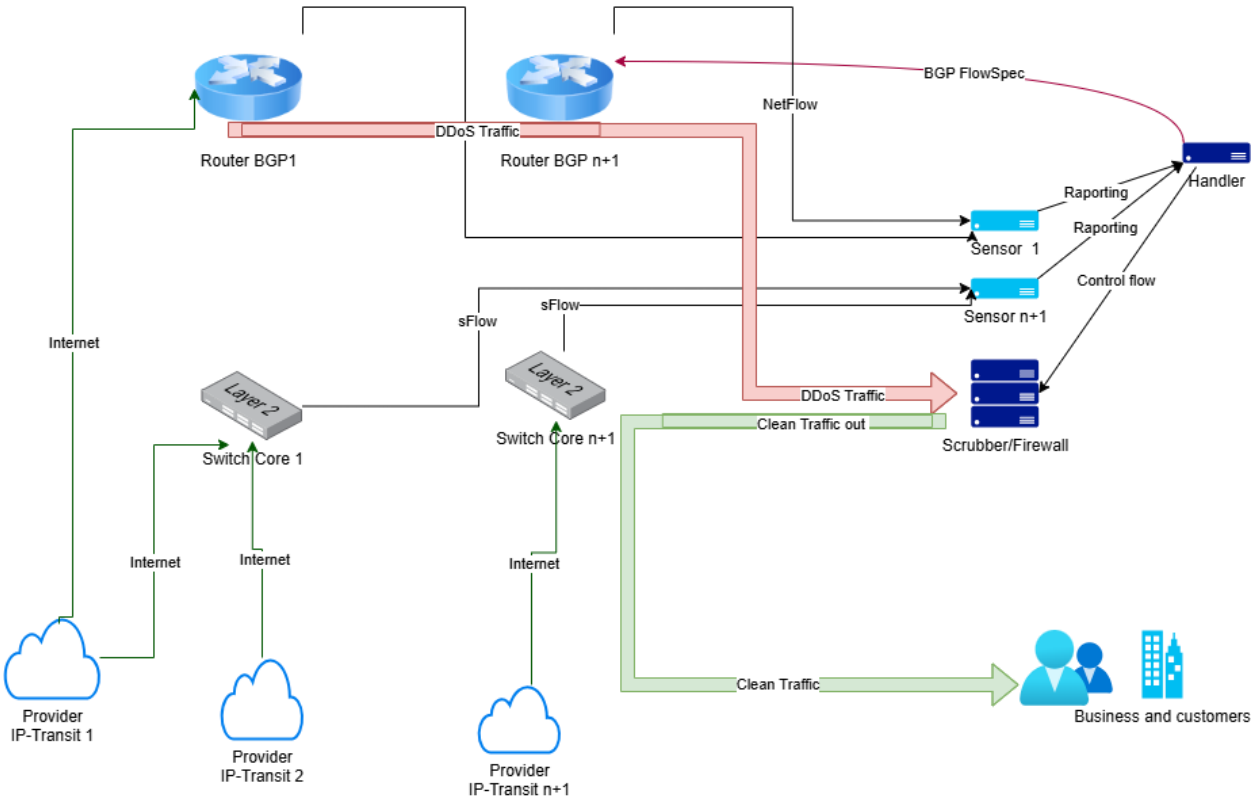
The NetFlow v9 protocol (RFC 3954) is used, which was developed by Cisco and is distinguished by the high details of the traffic reported through ISP routers. Or IPFIX in the case of Juniper routers or other brands that use IPFIX

There can be two or more devices (Router/Switch) that report with the corresponding protocol to a “Sensor” software service for analyzing traffic and reporting anomalies. Each “Sensor” reports to another central software “Handler,” which analyzes the reports and, based on the configurations adapted to the ISP network, executes the corresponding commands.

NSCFLOW Structure.

1. **Sensor**: This service receives telemetry data in the relevant NetFlow/sFlow protocols and performs their analysis. The values after analysis are sent to the “Handler”.
2. **Handler:** This service receives and unifies all reports from the “Sensors” and makes the relevant decisions according to the requirements and parameters set by the Administrator. It also enables BGP connections and WEB service as a monitoring and interacting interface.
3. **Collector:** Keeps history and analyzes telemetry data for their graphical presentation.
4. **Scrubber:** Software that enables filtering according to the needs of malicious DDoS traffic with high performance.

Sensors are dedicated to each telemetry protocol or reporting device. This allows for security in data analysis and high scalability in the case of a network with many devices / nodes.



“Handler” Tasks:

1. Notification of NOC (Network Operations Center) (SMS/Email etc.).
2. Syslog report in monitoring systems.
3. Notification of Clients if the IP being attacked belongs to one of the clients receiving service from the ISP.
4. Insertion of anomalies in the database.
5. BGP IPv4/IPv6 FlowSpec.
6. FlowSpec for DDoS redirection to Scrubber Server.
7. Remote Triggered Black Hole (RTBH).
8. Graphical reporting of the latest analyzed data.
9. Unification of all analysis coming from Sensors.
10. Monitoring Sensors for their performance.

What the Sensor analyzes in traffic:

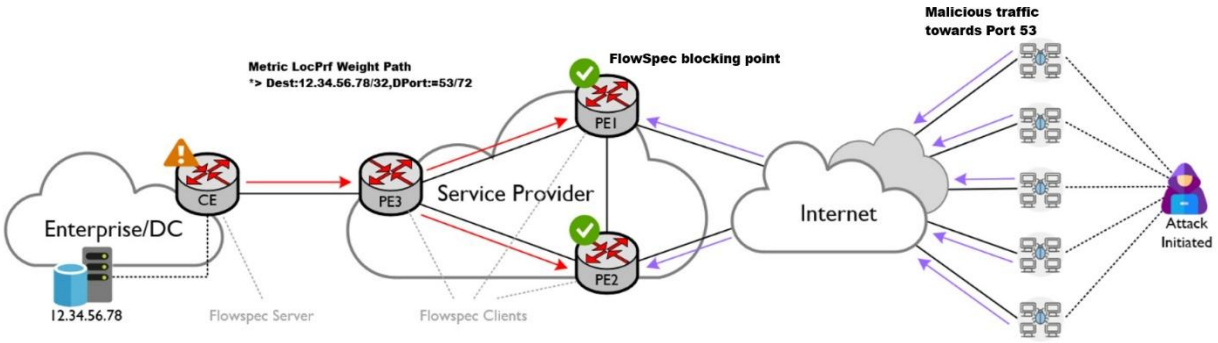
1. Traffic in Bytes/sec towards an IPv4/IPv6.
2. Number of communications/sec FLOWS towards an IPv4/IPv6.
3. Number of packets/sec towards an IPv4/IPv6.
4. Number of different ASNs that bring traffic towards an IPv4/IPv6.
5. Number of different Countries that bring traffic towards an IPv4/IPv6.
6. Active control of traffic towards different ports such as: DNS, NTP, SNMP, SSDP, SIP, SSH, Telnet etc. by controlling the number of different IPv4/IPv6 both in the source and in the destination.
7. Active control for TCP FLAGs such as SYN/SYN-ACK.
8. Active control for IPv4/IPv6 that bring traffic towards different ports, by counting the destination.
9. Active control for IPv4/IPv6 that receive traffic from different ports, counting the source.
10. Control of IP source from BlackList countries that send traffic to Vulnerable ports.

What happens in case of an anomaly:

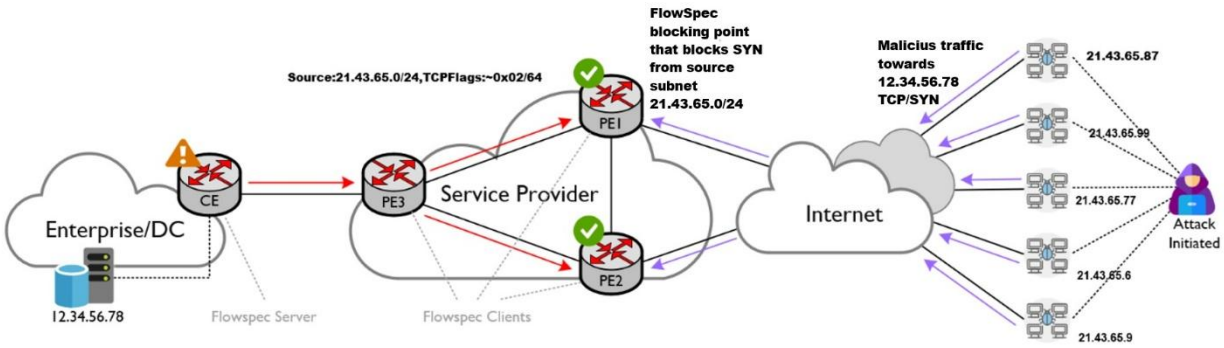
The “Handler” reacts by taking appropriate measures when it notices an anomaly in the reports coming from the “Sensor” based on personalized configurations set by the network administrator.

Examples:

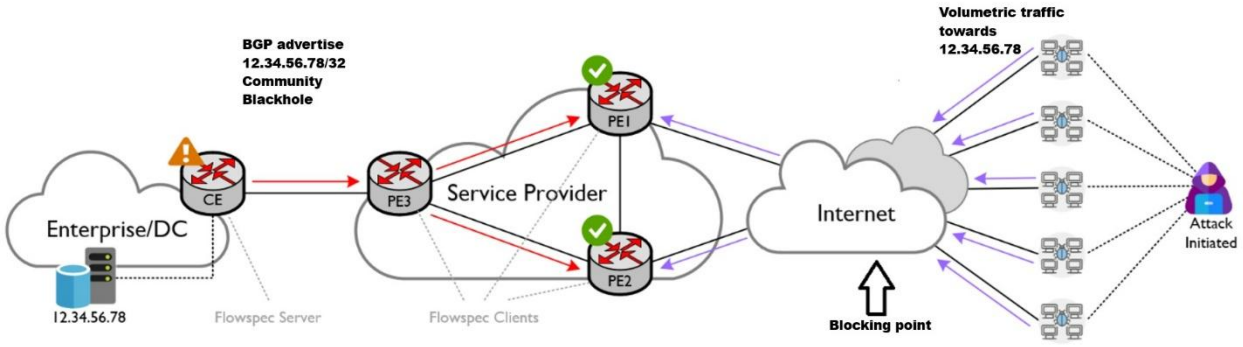
- If there is high traffic from many sources to a specific IPv4/IPv6 on DNS UDP port 53, BGP FlowSpec is executed and on ISP routers, traffic on port 53 to the specific IPv4/IPv6 is blocked.



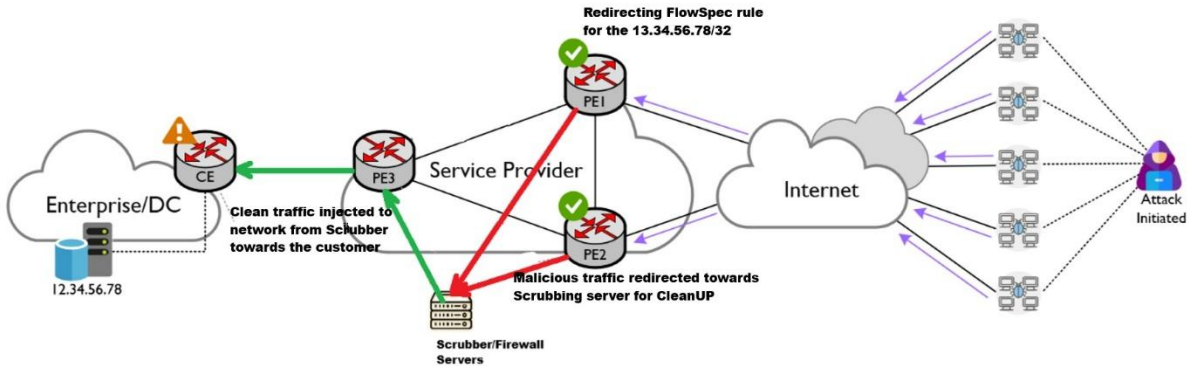
• If many different SYNs come from an IPv4/IPv6 to different IPs (mainly open port scans), BGP FlowSpec is executed and on the ISP routers, traffic from the corresponding /24 or /48 subnet is blocked for TCP FLAG SYN.



• In cases where the DDoS attack has a high traffic volume above X Gbps (condition set by Admin), the “Handler” executes Remote Triggered Black Hole (RTBH) for the IPv4/IPv6 that is attacked and traffic is blocked only to the provider. Within the ISP and its Peering connections, traffic to this IP in the RTBH is unaffected.



• In cases where the DDoS attack has a high volume but the Administrator has set the attacked IPs in “Protected” mode, then the “Handler” does not execute Remote Triggered Black Hole (RTBH) but BGP FlowSpec which enables the redirection of traffic towards the dedicated “Scrubber/Firewall” server which filters all malicious traffic and allows only legitimate traffic towards the respective destination. This happens without affecting the service provided by that IP.



Alerts that can be seen in the system:

• *3.84.3.0/24 SYN Flows Exceeded from SrcIPv4: 3.84.3.15, Flows: 22, UniqueDstIPs: 12*

It means that IP 3.84.3.15 has attempted SYN connections to 12 different IPs in the ISP network. This is in most cases a scan. The command executed in BGP FlowSpec is that any traffic from the 3.84.3.0/24 subnet with TCP Flag SYN will be DROP.

And from that source there will be no more SYNs to any IPs in the ISP network

• *77.42.19.86/32 Port: 53 Flows Exceeded to DstIPv4: 77.242.19.86, Flows: 16, UniqueSrcIPs: 7*

It means that towards IP 77.242.19.86 there is DNS traffic on port 53 from 7 different IPs from outside the network. This case is called DNS amplification attacks where usually there are devices with port 53 open and different actors send requests with spoofed IP and the responses are used for DDoS in other places. The command executed in this case is to close the traffic towards port 53 towards this IP.

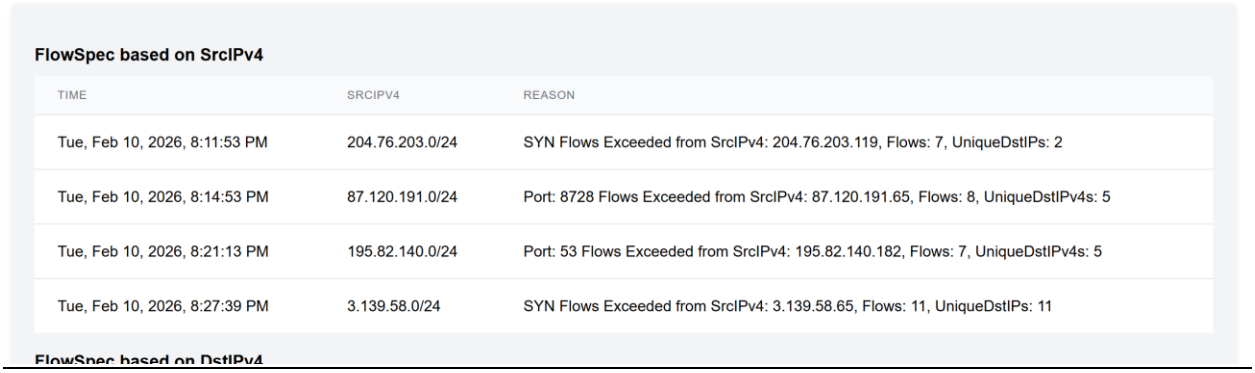
• *Blackhole for 80.70.80.70 Bytes Limit Exceeded 74774.80*

In this case towards this IP there has been a traffic beyond the limit set by Admin.
The command executed is RTBH and this IP is advertised to Providers for Blackhole which causes this IP to be taken out of service.
But the traffic within the ISP remains uninterrupted. So, you can continue the traffic with CDNs within the ISP or any other traffic.

• *Blackhole for 80.70.88.99 Packets Limit Exceeded 74.3*

In this case, there was traffic towards this IP with a number of packets higher than the limit set by the Admin. The command executed is RTBH and this IP is advertised to Providers for Blackhole which causes this IP to be taken out of service.
But the traffic within the ISP remains uninterrupted. So, you can continue the traffic with CDNs within the ISP or any other traffic.

FlowSpec example active rules



FlowSpec based on SrcIPv4

TIME	SRCIPV4	REASON
Tue, Feb 10, 2026, 8:11:53 PM	204.76.203.0/24	SYN Flows Exceeded from SrcIPv4: 204.76.203.119, Flows: 7, UniqueDstIPs: 2
Tue, Feb 10, 2026, 8:14:53 PM	87.120.191.0/24	Port: 8728 Flows Exceeded from SrcIPv4: 87.120.191.65, Flows: 8, UniqueDstIPv4s: 5
Tue, Feb 10, 2026, 8:21:13 PM	195.82.140.0/24	Port: 53 Flows Exceeded from SrcIPv4: 195.82.140.182, Flows: 7, UniqueDstIPv4s: 5
Tue, Feb 10, 2026, 8:27:39 PM	3.139.58.0/24	SYN Flows Exceeded from SrcIPv4: 3.139.58.65, Flows: 11, UniqueDstIPs: 11

FlowSpec based on DstIPv4

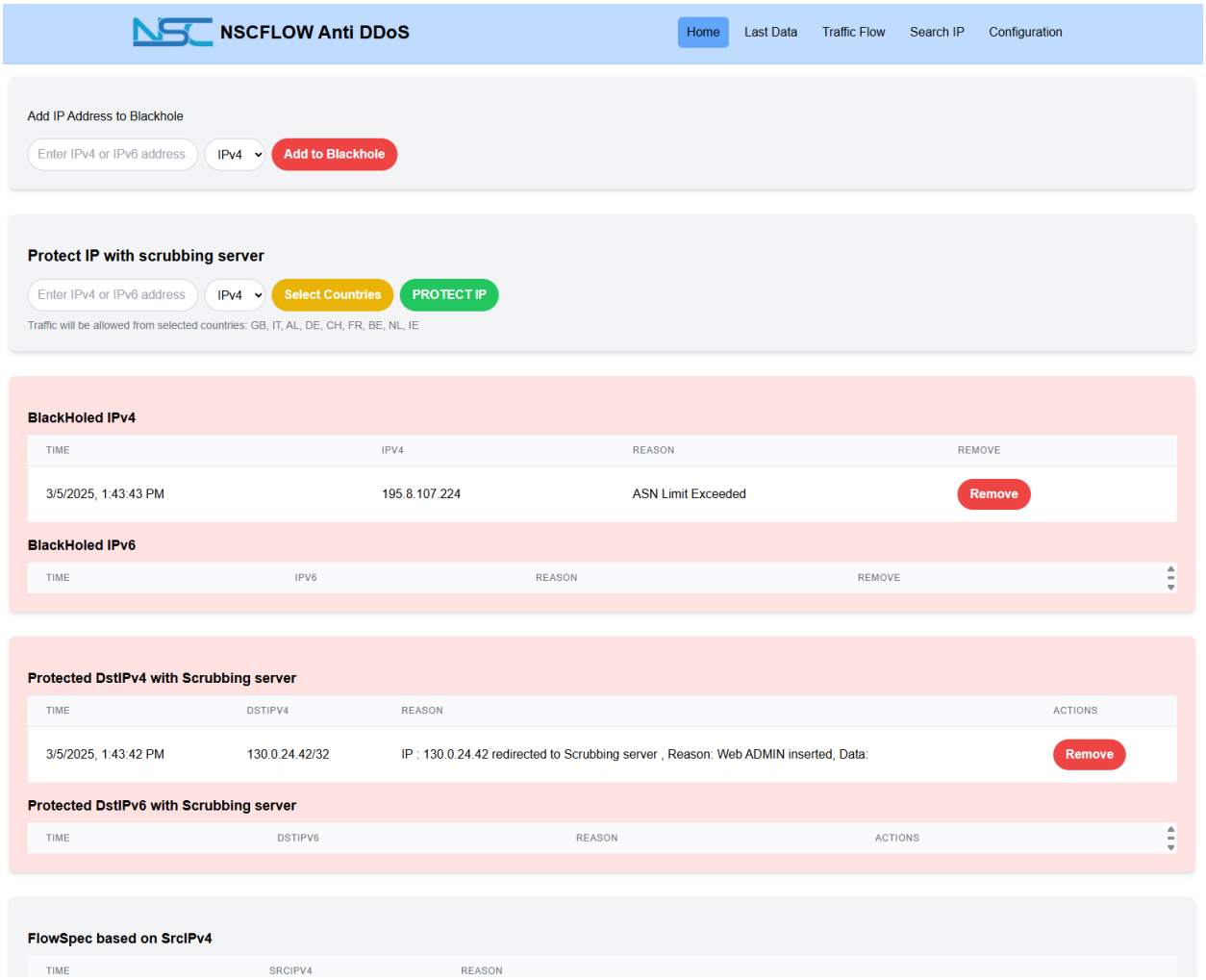
Parameters that are configured in the System:

1. Traffic limit in Bytes/s towards an IP.
2. Packets/s limit towards an IP.
3. Flows/s limit towards an IP.
4. States limit towards an IP.
5. ASN limit towards an IP.
6. BlackHole Community.
7. Scrubbing Community.
8. IP deployment time in Blackhole & FlowSpec.
9. IP Sources excluded from FlowSpec.
10. Custom limit of points 1-5 towards a list of single IPv4/IPv6 IP-s
11. Custom limit of points 1-5 towards a list of IPv4/IPv6 Subnets.
12. Custom port for Netflow/IPFIX/sFlow.
13. VLAN values as needed in sFlow.
14. List of IP subnets that in case of attack on them do not pass directly to BlackHole but the traffic is redirected towards the Firewall/Scrubbing Server.
15. Max Limit of DDoS traffic that will be allowed towards an IP under protection.
16. List of Whitelist Countries that will be allowed towards the IP of point 13
17. List of Subnets of clients associated with the respective emails so that in case of an attack towards them the system includes an email in the Notification.
18. Scrubbing policy for points 1-5.
19. Carpet Bombing limit. How many IP-s will scrubb before defaulting to RTBH.

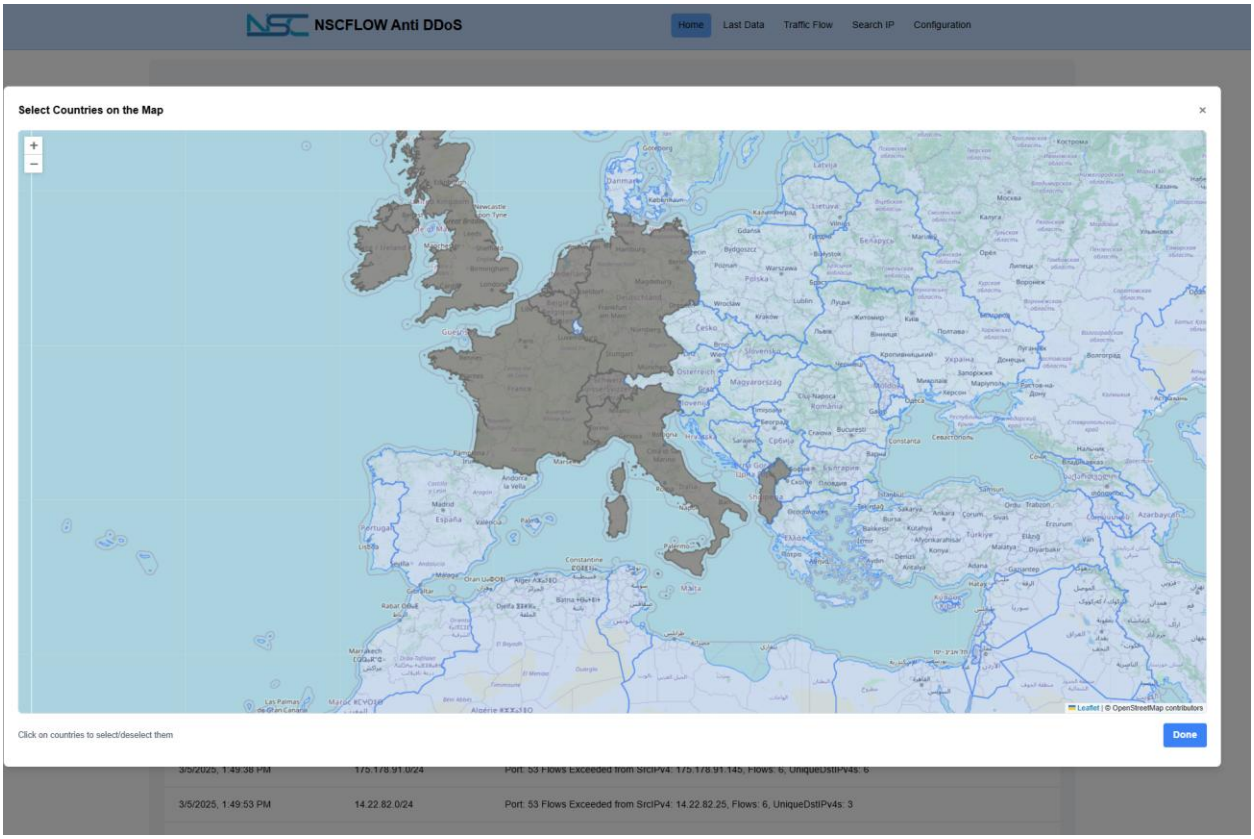
How to control the situation.

For the management and monitoring of IPs that are attacked, a Web is provided from the server where the software is installed. Where the Admin has the ability to:

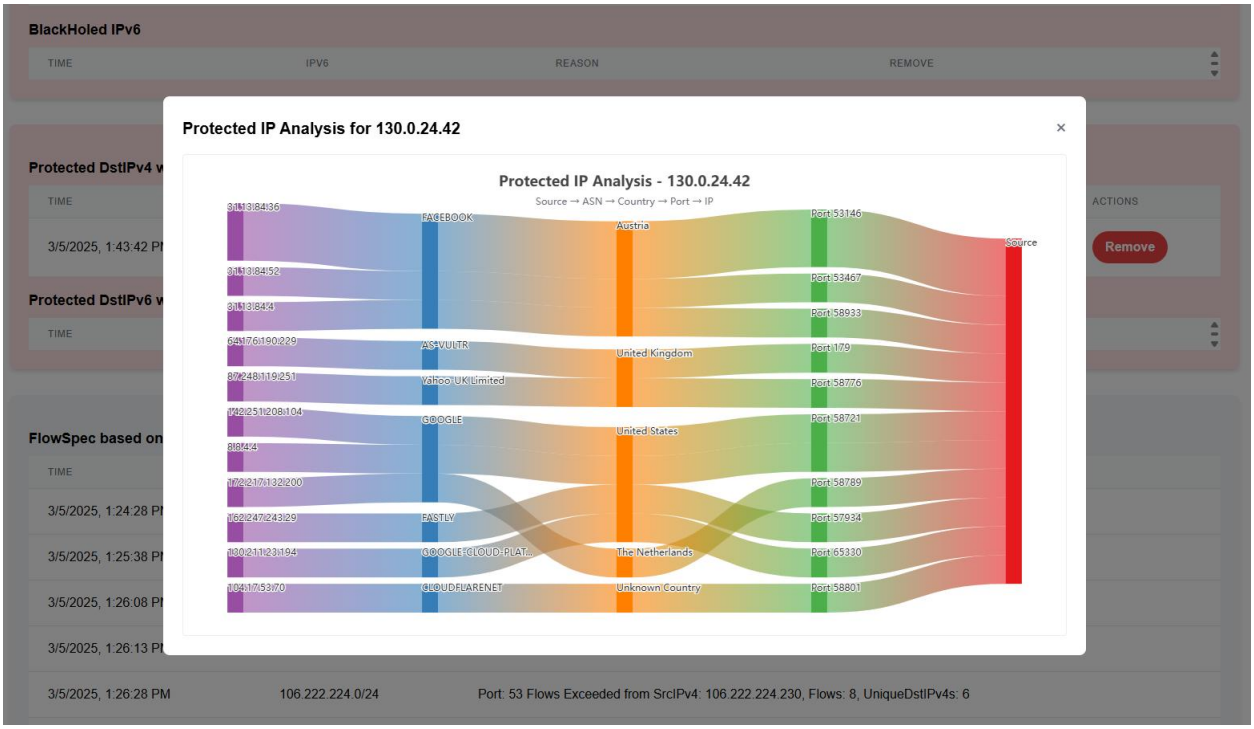
- Manually add IPv4/IPv6 to BlackHole.
- Manually remove IPv4/IPv6 from BlackHole that have been added by the system.
- Manually add/remove IPs in DDoS Protection/Filtering
- Check the reasons why the system has performed the relevant commands.
- Check the FlowSpec rules made by the system.
- Monitor the graphs that provide Top Datas for each of the methods.



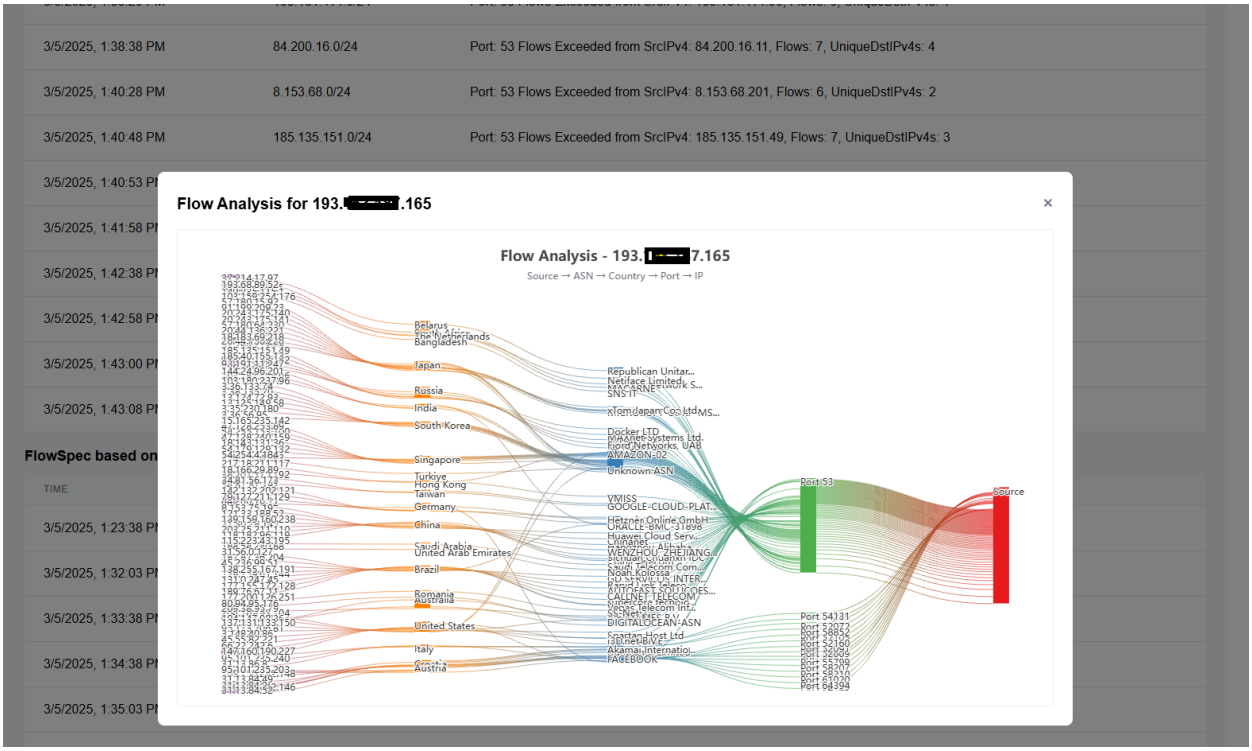
Possibility to select countries that allow traffic to the IP set to be redirected to Scrubber.



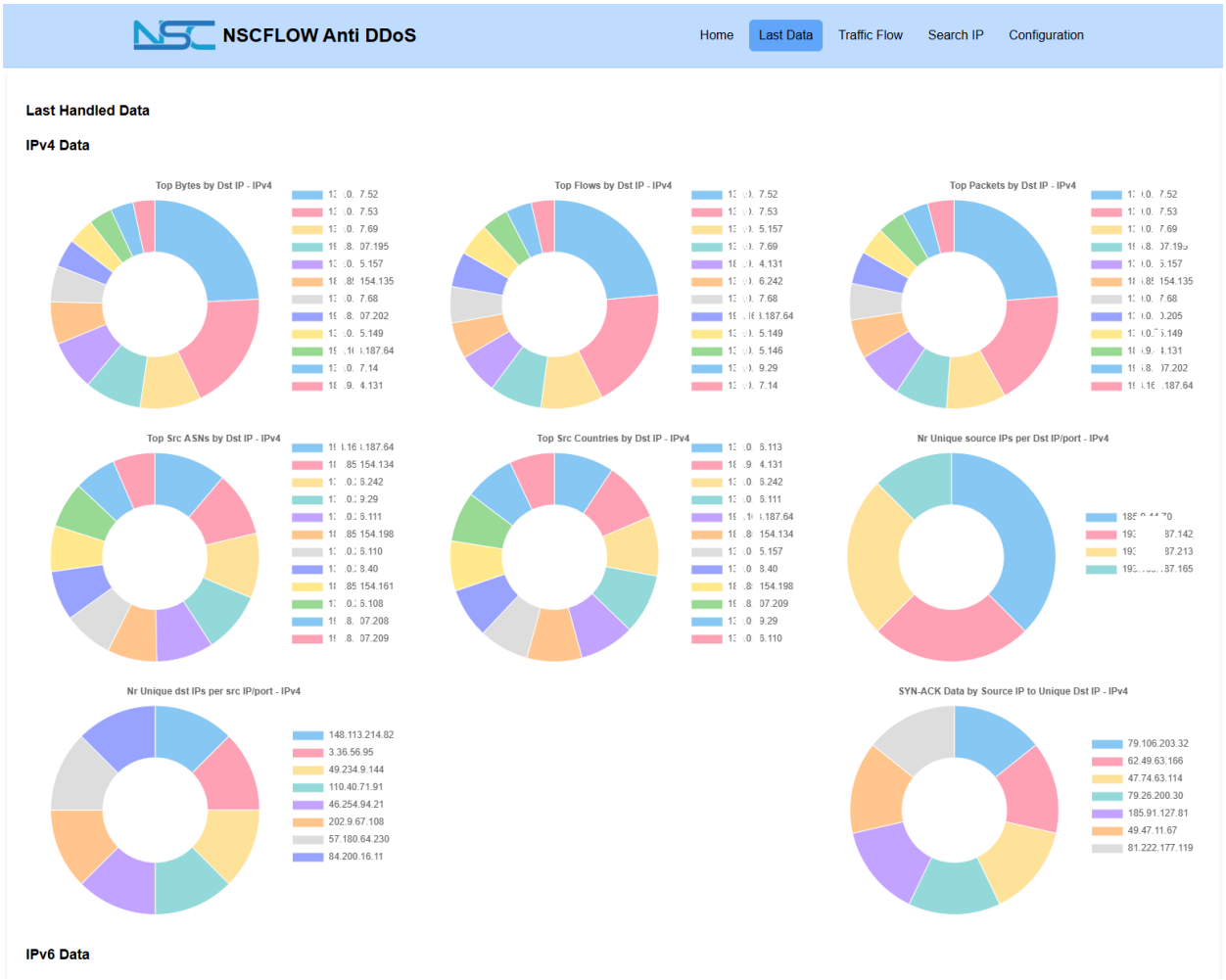
If you click on the IP, an interface with real-time traffic for that IP will appear in a POP up.

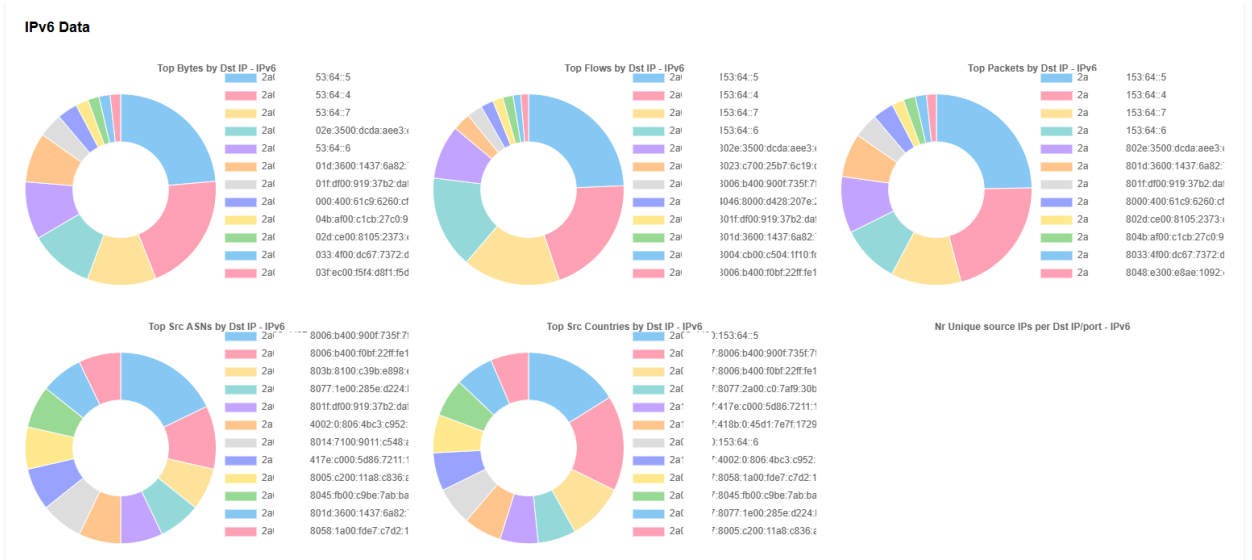


Also, traffic to IPs that are placed in FlowSpec

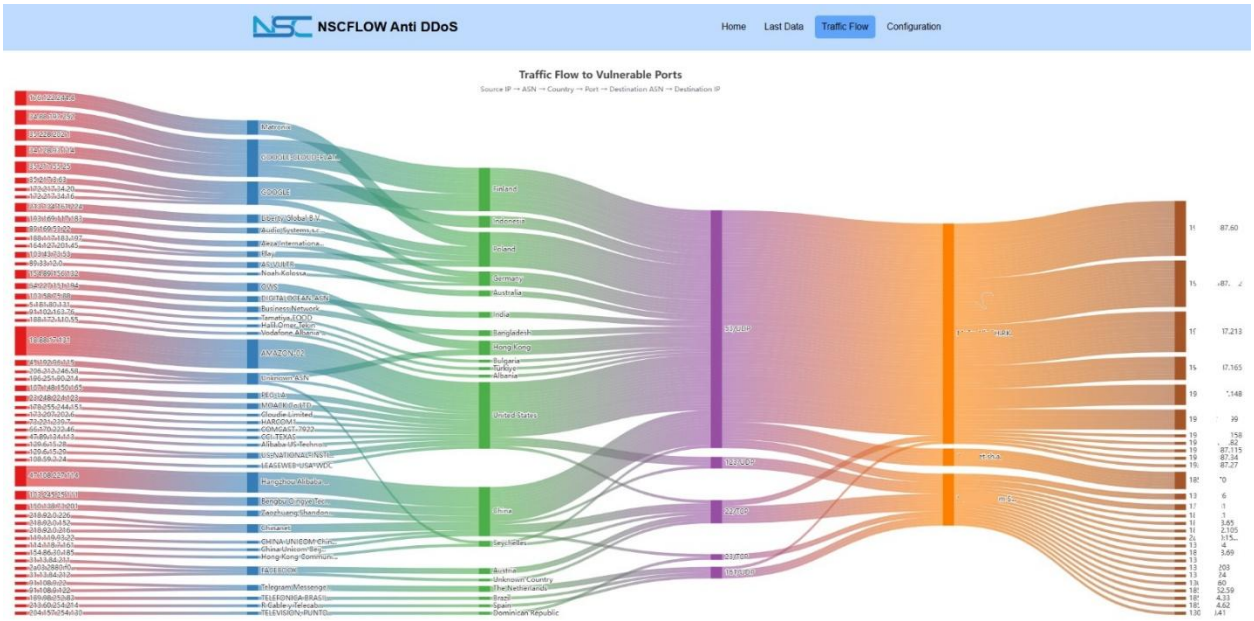


Latest IPv4 data (intentionally deleted IPs)

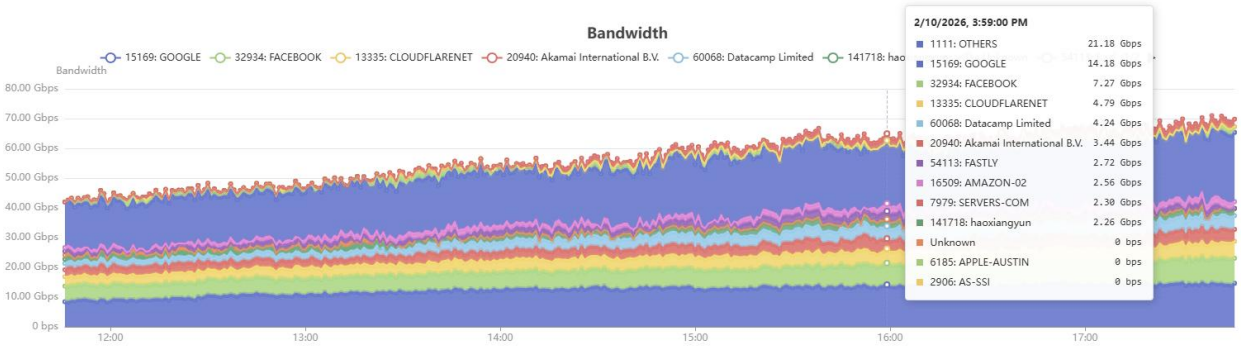


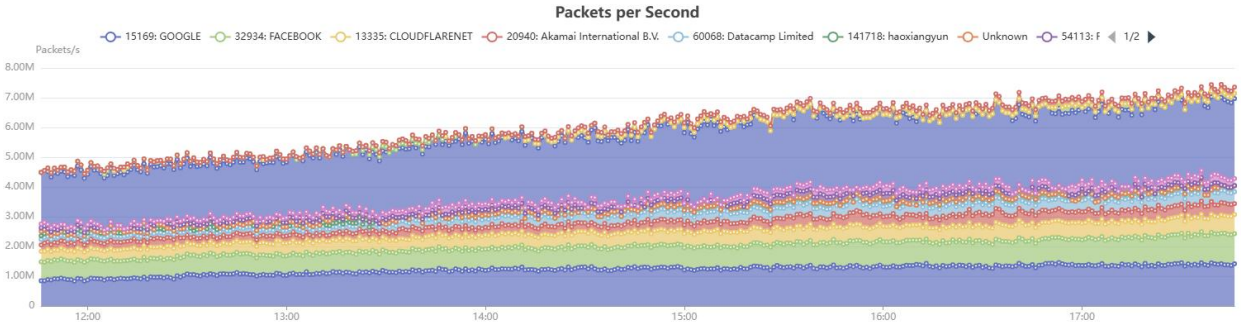


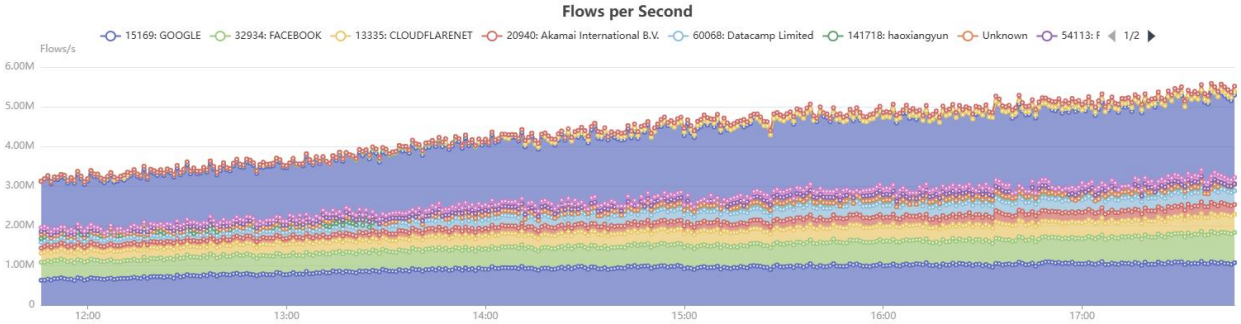
This graph enables real-time traffic control towards vulnerable ports such as 22,23,53,123, etc.



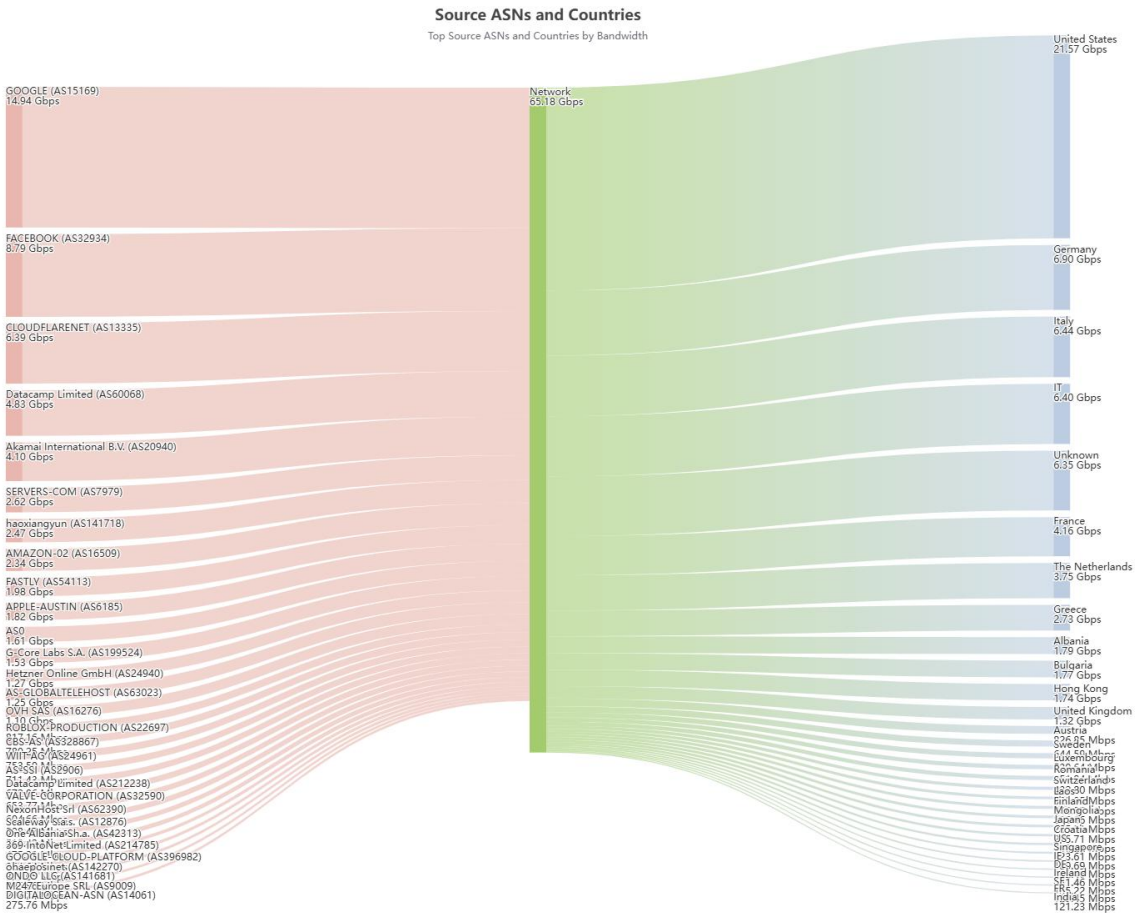
These graphs have a 6-hour history with minute-by-minute data on traffic/packets/flow per second.



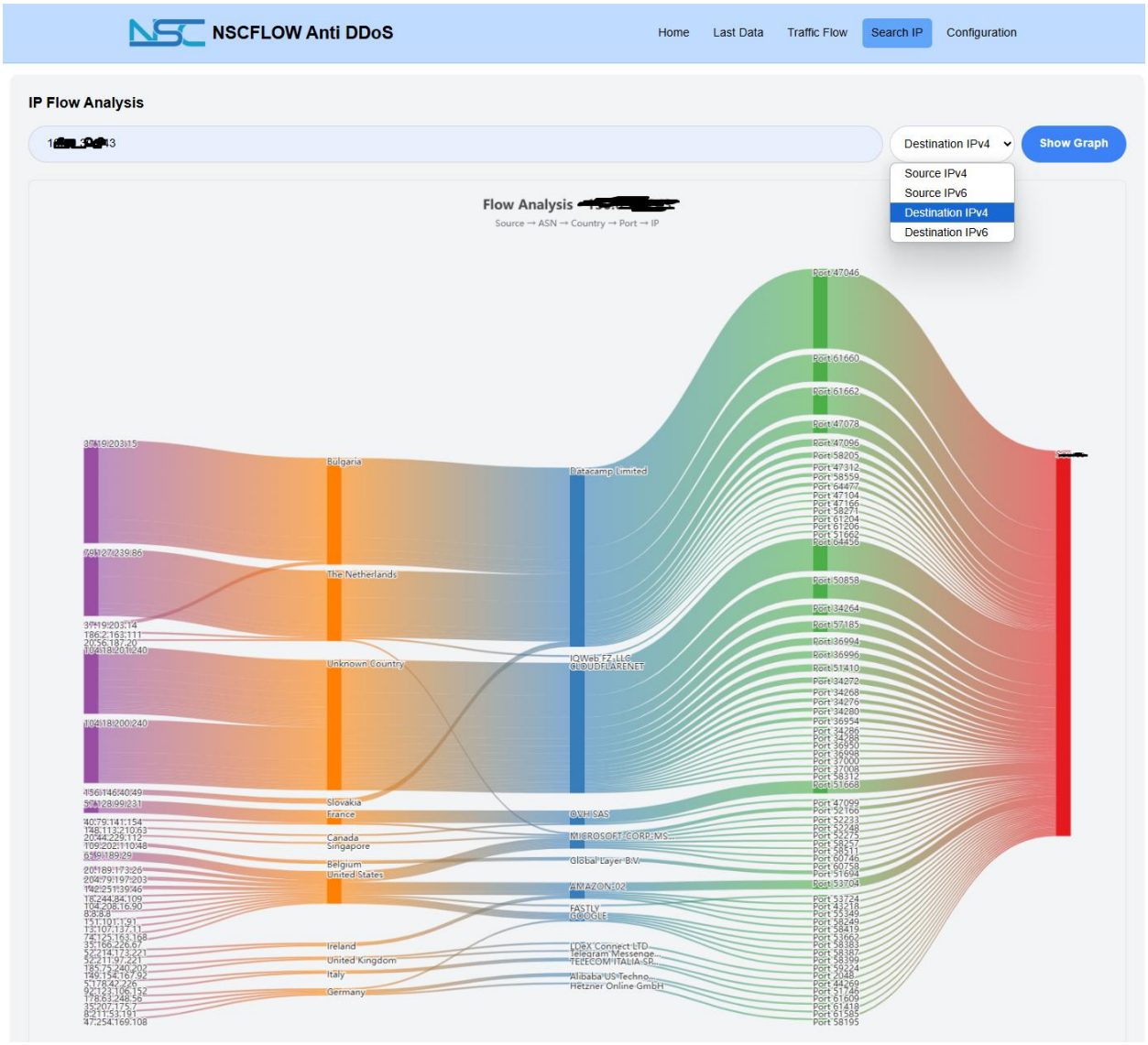




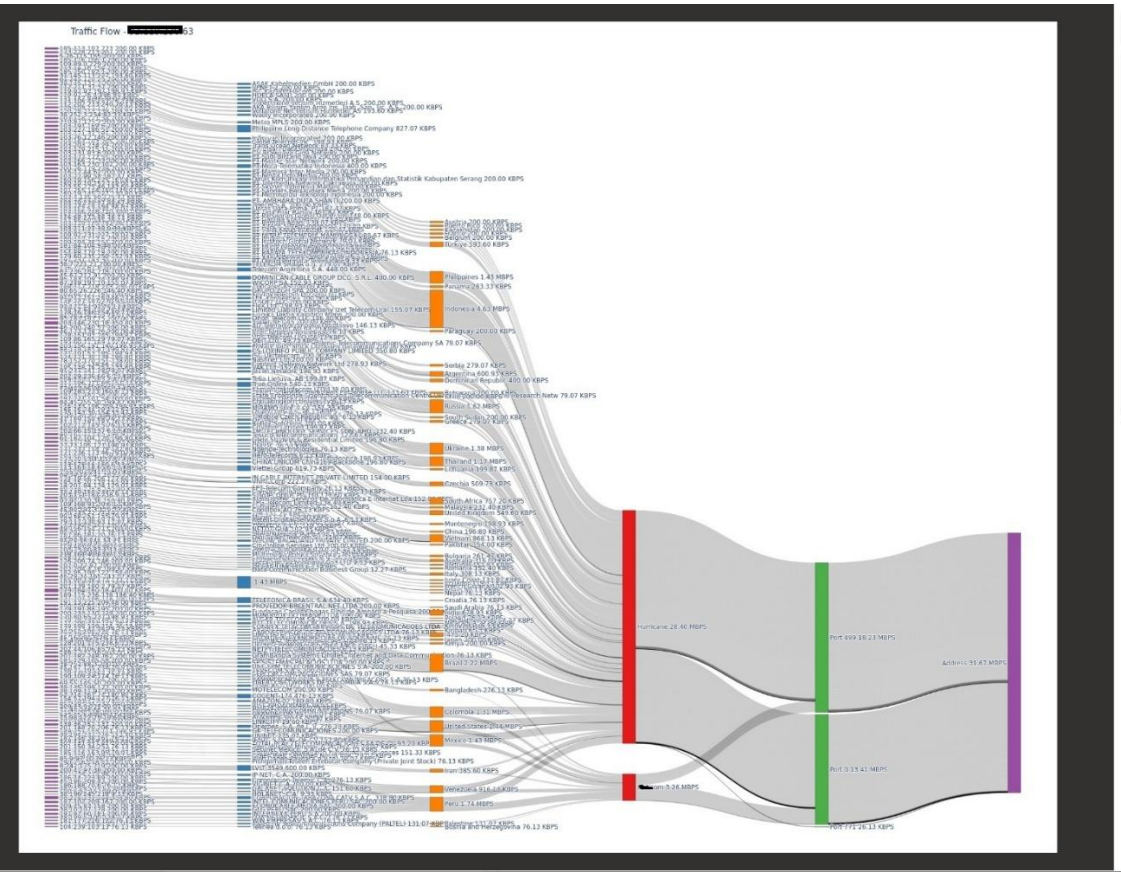
Another helpful graph for analyzing traffic sources.

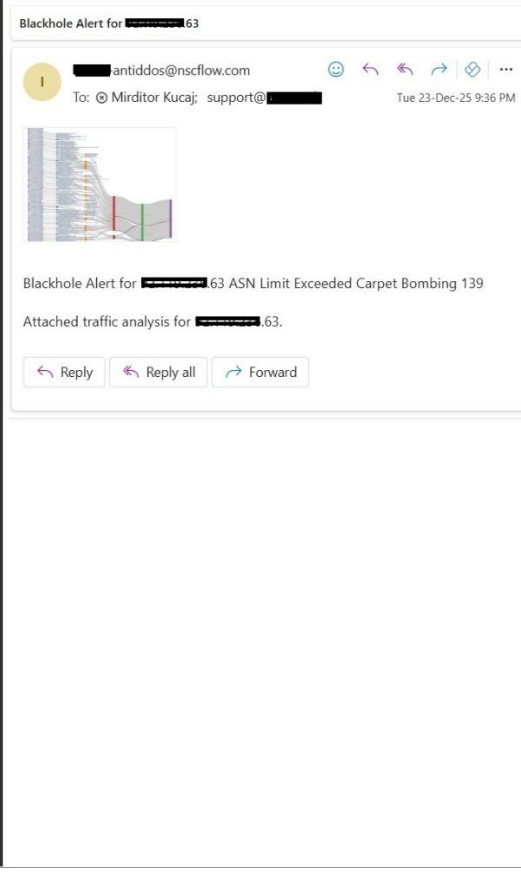


Ability to search and analyze traffic in real time for different IPs.



Here we have an example of an alert that comes from the email system, with an attachment that includes a detailed graph of what traffic is being generated for the IP being attacked.





What do we see in Router: #show bgp ipv4 flowspec

```
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 8642
BGP main routing table version 8642
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 8642/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
*> Source:45.125.45.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:46.164.115.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:47.113.189.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:62.113.114.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:84.54.47.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:88.218.61.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:89.110.90.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:93.183.94.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:94.103.84.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:94.103.93.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:103.8.69.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:104.168.243.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:124.222.127.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:180.188.43.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:183.90.188.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
*> Source:185.231.154.0/24,DPort:=53/64
                      0.0.0.0                                0 64606 ?
```

Configurations required on ISP routers/switches

This is usually tailored to the ISP network.

But usually you need:

- A dedicated vlan which will be called FLOW and all devices that will report sFlow or Netflow to send to the sensors with source IP set to the respective SVIs.
- On this vlan you need a subnet with Private IP which is only accessible by the network admin.
- Setting up the server connection in a part of the network that is not affected by any possible traffic congestion or disconnection for other reasons.
- BGP connection with the “Handler” of all routers that have the “Border Gateway” function on the Ipv4 & Ipv6 peer also with AFI in FlowSpec.
- Policy configuration in the FIB TABLE of the above routers.
- FlowSpec Policy configuration on the above routers.
- Netflow/IPFIX configuration on the above routers
- sFlow configuration with documented ports and VLANs on the Switches.

If a firewall/scrubber server will be installed

1. A dedicated VLAN is needed on which DDoS is routed to the Server
2. Another VLAN that will receive cleaned traffic from the Server
3. 2x 10/25/100G ports as appropriate for the Server.

Firewall/Scrubber Server

According to the DDoS traffic that will be decided to be accepted, it will be determined whether it will be necessary for a dedicated Server or not.

The most necessary part of this server is a 10/25/100G network card, etc. Nvidia/Intel model with the appropriate parameters for network processing.

At least 2 ports are needed. 1 for DDoS in and the other for Clean Traffic out

What does the server do:

- Controls the size of the packets.
- Controls the frequency of the packets.
- Checks TCP SYN/ACK connections.
- Checks Ports and their frequency of use.
- Checks Source IPs and determines which country they belong to.
- Checks Source IPs and determines which ASNs are allowed.
- Checks Whitelists of countries and ASN that should be allowed.
- So, it blocks all common DDoS attacks
    - UDP floods /SYN floods/ NTP amplification/ DNS amplification/ SSDP amplification / IP fragmentation/ SYN-ACK floods etc.