The use of BGP Flowspec in the protection against DDoS attacks

WISSEM CHOUK
Abstract

Flowspec is one of the latest DDoS attacks mitigation tools. It relies on BGPv4 to share its route specifications. It presents great advantages when it comes to effectively mitigate a (D)DoS attack. However, due to the lack of protection and security of BGP, Flowspec presents some vulnerabilities that can be used against the victim to initiate, enhance or continue an attack. An ISP is interested to include Flowspec in its mitigation tools. In this thesis, we will evaluate the potential use of Flowspec by the ISP after taking into consideration 3 uses cases where the protocol would not be able to act as intended.

Keywords: DDoS, Flowspec, BGP, Security, Networking
Abstract


Keywords: DDoS, Flowspec, BGP, Security, Networking
# Contents

## Introduction 8

1.1 Background ................................................................. 9
1.2 Problem ........................................................................ 10
1.3 Purpose ......................................................................... 10
1.4 Goal ............................................................................. 10
1.5 Benefits, Ethics and Sustainability ................................. 10
1.6 Research Methodology .................................................. 11
1.7 Outline ......................................................................... 13

## Background 14

2.1 DDoS types of attacks .................................................. 14
  2.1.1 Volume based attacks .............................................. 14
  2.1.2 State Exhaustion attacks .......................................... 16
  2.1.3 Application Layer attacks ....................................... 18
2.2 Mitigation Techniques .................................................. 20
  2.2.1 Network ACLs ...................................................... 20
  2.2.2 RTBH ................................................................. 22
2.3 BGP: Border Gateway Protocol .................................... 25
  2.3.1 BGP: Security issues .............................................. 28
2.4 Flowspec, the versatile solution against all (D)DoS attacks 29
2.5 Flowspec Pros ............................................................. 31
2.6 BGP Flowpsec in action ................................................ 32
List of Figures

2.1.1 UDP Flood attack
2.1.1 ICMP Flood attack
2.1.2 SYN Flood attack
2.1.2 Packet Fragmentation attack
2.1.2 Smurf attack
2.1.3 HTTP Get attack
2.1.3 Slow and Low attack
2.1 Distribution of DDoS attacks
2.2.2 Destination RTBH filtering
2.2.2 Source RTBH filtering
2.3 OSI Model with a highlight on DDoS attack sensible protocols
2.3 Example of a BGP route exchange between ASes [17]
2.3 BGP Operations [19]
2.4 BGP NLRI
2.4 Flowspec rules algorithm
2.5 Inter-domain DDoS mitigation using Flowspec
3.1.1 Case1 Topology
3.1.2 Case2 Topology
3.1.3 Case3 Topology [24]
4.1 The Use of Flowspec in a real-life situation
4.1 Distribution of the reasons of the non integration of Flowspec by the ISPs in their security
4.3.1 Mind Map of the problematic of DGC
4.3.6 Software architecture of the virtual environment
4.3.6 Topology of the initial virtual network
4.3.7 Components of the router
4.3.7 Topology of the final virtual network
4.3.8 Wireshark Capture of the UPDATE message in Test1
4.3.8 Result of the communication between PC-1 and PC-2 in Test1
4.3.8 Result of the communication between PC-4 and PC-2 in Test1
4.3.8 Wireshark Capture of the UPDATE message in Test2
4.3.8 Result of the communication between PC-1 and PC-2 in Test2 using TCP
4.3.8 Result of the communication between PC-1 and PC-2 using TCP on specific ports in Test2
4.3.8 Comparison between PC-1 and PC-4 UDP pings
List of Tables

2.2.1 Example of network ACL configuration
4.1 Comparison between the presentation of Flowspec and its use in practice
4.3 Comparison between the presentation of Flowspec, its use in practice and its tested features
Chapter 1

Introduction

During the last years, an increase in cyber attacks has been noticed. The scope of these attacks is getting wider and they are being more publicized on the mainstream media as they are disrupting everyday activities of end consumers and might evolve to severely harm our well-being. One of the latest widespread cyber attacks, the WannaCry ransomware attack has paralyzed more than 200,000 computers across 150 countries for 4 days in May 2017 [1]. It has been labeled as the worst attack that has ever been launched. This attack has contributed infringing awareness on the importance of security in IT. Even if the WannaCry ransomware attack has been very effective, it relies on the SMB (Server Message Block), a transport protocol over TCP. This breach is specific to the Windows XP OS.

However, the most common attacks do not need to rely on a breach in the protocol or the OS to harm the victim. The DDoS (Distributed Denial of Service) attack is part of this type of attacks. With the increase of connected devices (e.g. IoT) and the easy access to the DDoS-for-hire services [2], the DDoS attacks became more elaborate and common as their frequency has doubled between the first and the third quarter of 2017 [3]. Moreover, the attacks are continually evolving, becoming harder to mitigate. The latest DDoS attack in Sweden took place in October 2017 targeting Sweden’s Transport Administration (Trafikverket) causing delays in the trains schedule and a breakdown of the ticket booking app [4].

Organizations that have had DDoS protection projects on the back burnar are now reprioritizing these projects as their customers are demanding more protection against such attacks. In this context, the protection against DDoS attacks became a priority for the ISPs in fracture as well as their customers. They are actively working to keep up the pace with an always more elaborate attacks. The impact of a DoS attack on the network can have considerable repercussions on the victim. The main threat for a company that has been attacked is financial. Annually, DDoS attacks cost millions to the victim companies. It varies from 100,000$ to tens of millions of dollars per hour when services are down[10]. Denial of service attacks translate to an extended system timeout and, therefore, to a large amount of unexpected work. It delays the activity of the enterprise by days. Another impact of these kinds of attacks is the trustability of the attacked
company. Most of their customers (especially for ISPs) would doubt their security display. A bad buzz would result in an even worse financial impact.

Several types of attacks have been elaborated throughout the years. The mitigation technique can vary depending on the type of attack. In this context, DGC, a Swedish ISP has decided to pay more attention to its anti-DDoS protection. Even though many players have emerged in the past years providing a full anti-DDoS protection, the cost of these solutions remain high for a mid-sized company such as DGC [30]. The objective of DGC is to find a versatile and automatized alternative solution for all types of attacks.

In the latest years, a new method for DDoS protection has emerged. This solution relies on BGP Flowspec [12], a relatively new BGP (Border Gateway Protocol) extension that can be used to mitigate DDoS attacks. Since it relies on BGP, several vendors started to support it [29]. DGC wants to investigate the benefits in using BGP Flowspec both within its network and for the protection of its customers.

In this thesis, we will, first, go through the different types of attacks. Then, the different previous mitigation techniques will be described. In the third chapter, we will introduce BGP Flowspec, a new feature relying on BGP used to mitigate all types of DoS attacks. Finally, we will challenge this protocol and evaluate its reliability and efficiency.

1.1 Background

DGC is a network operator and ISP primarily operating on the Swedish market for business and public organizations (no consumer services). Over time there has been an escalation in DDoS attacks, both in volume and frequency [31]. As an operator, DGC has to deal with the increasing demand of protecting its customers and its own infrastructure. A few vendors have very dominated the commercial tools for detecting and mitigating attacks in the ISP/Operator level. This has led to costly solutions and services.

For DGC, DDoS-protection services have been offered as an added service to Internet access, but the production cost has been relatively high and therefore services are too expensive for most of their customers.

The mitigation of DDoS attacks can be done in several ways. The main methods used are black hole routing (RTBH), filtering and traffic limiting by using network ACLs (Access Control Lists) in routers. Black hole routing is used by DGC as a last resort to protect its customer or network from collateral damage. Once used it is effectively making the attack successful, removing the target/service from the Internet. After conducting tests on its infrastructure, DGC asserted that the most cost-effective way is to use a combination of the two measures; Using routers for rough filtering via network ACLs and scrubbing devices [32] for more advanced filtering.
DGC has been looking at alternatives to the commercial products to increase flexibility and to drastically reducing the cost of producing the services. A goal has been to provide an essential service as part of the Internet access services at no additional price. The service should be fully automated and handle some of the known and most frequent attack types.

With the mixed feedback on BGP Flowspec [25], DGC started paying attention to this new way to mitigate DDoS attacks and investigating the potential benefits that it could bring to the company and its customers.

1.2 Problem

DGC, as an ISP, is using an Arbor system for the protection against DDoS attacks [33]. This solution is too costly both for the ISP and for its customers as it is provided as an extra service [34]. Knowing that its infrastructure supports BGP Flowspec and in order to reduce the cost, DGC wants to investigate the potential use of BGP Flowspec as a DDoS mitigation tool used for both its network as well as its customers.

The research question we are facing is: How can BGP Flowspec be safely used by ISPs?

1.3 Purpose

The purpose of this thesis is to 1) analyze and understand the different types of attacks that could face DGC 2) analyze and document the mitigation techniques that DGC uses and 3) investigate the pros and cons of the use of BGP Flowspec as an alternative solution for the protection against DDoS attacks.

1.4 Goal

The goal of this thesis is to answer if it is the right decision for DGC to opt for BGP Flowspec as the solution against DDoS attacks. For this, we need to understand the type of attacks and compare BGP Flowspec with other mitigation techniques. To answer the question stated in Sec.1.2, we propose to theoretically study the vulnerabilities of BGP Flowspec based on 3 scenarios that can occur if specific security measures are not applied. The result of this research is answering the question How can DGC implement BGP Flowspec assuring the safety of its infrastructure?

1.5 Benefits, Ethics and Sustainability

Benefits. Two main actors would benefit from this research. The ISP would know of switching to an open source Flowspec based DDoS mitigation solution is the right
decision to take or is it safer to use a commercial solution. The customers of DGC would benefit from a cheaper DDoS protection solution if DGC chooses to use BGP Flowspec for its infrastructure and its clients' network.

**Ethics.** Concerns about data privacy and customer's trust appear in this context. DDoS attacks can harm the privacy of the victim if its data is not protected. The attacker can have access to sensitive information. Another aspect is the trust of the ISP who provides the DDoS protection. The ISP needs to make the right decision based on the situation. In this context, this research has to be as objective as possible since its outcome affects both the ISP and its customers.

**Sustainability.** The outcome of this research supports both individual and economic interests. The end user of the DDoS protection mechanism would benefit from a cheaper and better solution if DGC decides to switch to the new solution. The ISP would also economically benefit from it as this solution is cheaper than a commercial tool.

### 1.6 Research Methodology

The selection of which research methods and methodologies to use when conducting a research project is a critical aspect to be considered [40]. The goal of our study as mentioned above, is to implement a suitable environment to test BGP Flowspec in action for DGC. Based on this, our epistemological posture is constructivist. We propose to design with the information system actors of the site of our investigation a virtualized environment as a proof of concept (POC) to test the usability of BGP Flowspec. Constructivist methodologies are mainly qualitative. We deeply explore a real-life situation of a single case study (i.e DGC). To come up with prescriptions to overcome their dependency to protection solution vendors and reinforce their technical autonomy, we will follow the steps of the engineering design process [Link]. Prescriptive models have to propose good practices for the use of BGP Flowspec in an ISP environment. Prescriptive models require a fair amount of documentation and time investment to come up with good practices and possible actions to guide the project management team towards a solution.

In our case, the solution involves designing an emulated networking environment meeting criteria derived from the literature review. Since our project involves designing building and testing a virtual network involving the use of BGP Flowspec in a prescriptive vision, the steps of the diagram represented below will be followed.
Define the Problem
Do Background Research
Specify Requirements
Brainstorm and Choose Solution
Develop and Prototype Solution
Test Solution
Make Changes based on the tests and results
Solution meets Requirements
Solution doesn’t meet Requirements
Communicate Results

Engineering Methodology Diagram
1.7 Outline

The rest of the thesis is organized as follows: Chapter 2 introduces the theory and background needed to this research, Chapter 3 presents the different study cases where BGP Flowspec can be harmful for the infrastructure, research methodology and methods carried out in this research, Chapter 4 presents the results of the research. Finally, Chapter 5 discusses the conclusion of the thesis and gives insights about future work.
Chapter 2

Background

In this section we will introduce the different type of DDoS attacks then proceed to presenting the commonly used mitigation techniques.

2.1 DDoS types of attacks

DDoS attacks have had a severe impact on the victim's revenues, reputation, and resources. According to Incapsula's survey [34], around 66% of the DDoS attacks last more than 6 hours. Hours during which the attacked company's infrastructure is paralyzed. Incapsula estimates the average cost of an hour spent under a DDoS attack is around 40,000$. The impact on the company's revenues could, therefore, be disastrous. A successful DDoS attack can also negatively impact the reputation of the company translated in loss of customer trust [34] and, also, the hardware and software infrastructure of the victim.

If the impact of these attacks can cause a significant damage on the victim side, DDoS attacks are not very diverse and can be clustered in 3 main categories.

2.1.1 Volume based attacks

This type of attack aims to overwhelm the network by sending a considerable number of packets from different flows. It is mainly based on spoofed IP addresses. IP Spoofing consists in generating a random IP address before launching the IP packets meant to flood the victim's network [35]. The reason for this technique is to hide the identity of the attacker by providing a false IP address in the infected packets. The expected outcome is an inundation of the bandwidth causing congestion. The attacker aims to make the victim's network collapse.

2.1.1.1 UDP Floods

The attacker uses the available bandwidth by sending UDP packets with a spoofed range of IP address. This attack exhausts the network until it crashes.
The UDP Flooding attack is very complicated to detect and mitigate as the attacker can use different IPs. Moreover, the UDP packet can be filled with extra information increasing its volume. The packet size can be set to 65,536 bytes. UDP floods can be used with amplification. Amplifying the UDP flood attack consists in sending requests to UDP servers with the spoofed IP address of the victim. The servers then send the response to the victim, flooding its network’s bandwidth.

2.1.1.2 ICMP Floods

In this type of attack, shown in fig.5, a hacker sends ICMP echo requests, with the return addresses spoofed, to a large group of hosts on a network. The victim will respond doubling the charge on the network and congesting both the out/ingoing bandwidth. As a result, the system is overwhelmed and cannot provide services [5].
2.1.2 State Exhaustion attacks

This type of attack targets the connection state tables. These tables operate on multiple network devices such as firewalls and load balancers to store the state of the connection when an exchange of data is happening. If a significant amount of connections is requested, the connection state tables will be filled up [8].

2.1.2.1 SYN Floods

The attacker sends a significant number of TCP SYNs on a single IP-host until it fills up its table of half-opened connections. The attacker never sends the ACK packet after receiving the SYN, ACK from the victim. The host allocates resources but never gets a reply. With a high number of opened connections, the victim resource is exhausted. The host is then unreachable as it is unable to accept any additional connection.

![Fig. 3 SYN Flood attack](image1)

2.1.2.2 Packet fragmentation & Ping of Death

The fragmentation of packets is necessary for all networks in case the MTU (Maximum Transmission Unit) is larger than the maximum allowed size. A typical attack is to send fragmented packets that need to be assembled on the destination side but exceed the frame size of 1500 bytes and increases the CPU consumption. This results in a crash or reboot of the target.
2.1.2.3 Smurf attack

The attack is also based on overwhelming the target’s network bandwidth by sending a high number of ICMP echo requests to a broadcast IP address from a spoofed source address. When all the devices on the network respond to this request, the target’s computer will be flooded. Fraggle attacks have the same mechanism, they use UDP and send traffic to port 7 (echo) and 19 (chargen) instead of ICMP. The difference with the ICMP flood attack is that the Echo (ping packet) is sent to an IP broadcast address so that the request is forwarded to all the network devices. The response is, then, sent from all the devices to the victim [40].
2.1.3 Application Layer attacks

This type of attack targets layer 7 of the OSI (Open Systems Interconnection). The most sophisticated attacks as they are hard to detect [7] with the commonly used techniques like Netflow [6]. They target the Operating System of the machine.

2.1.3.1 HTTP Flood attack

An HTTP flood attack targets websites and online services. The attacker, using botnets or zombies, floods the target (website server or CDN server) with a significant amount of GET/POST requests. The victim replies to all of them until it crashes. The attack is most effective when it forces the server or application to allocate the maximum resources possible in response to every single request. Thus, the attacker will generally aim to inundate the server or application with multiple requests that are each as processing-intensive as possible.

Fig.6 HTTP Get attack
2.1.3.2 Slow and Low attacks

A Slow and Low flood attack targets websites and online services. The attacker floods the target (website server or CDN (Content Delivery Network) server) with an important amount of uncompleted GET/POST requests by opening parallel connections and keeping them open as long as possible. The victim needs to reply to all of them until it crashes.

![Diagram of Slow and Low attack]

Fig. 7 Slow and Low attack

The distribution of the number of attacks is not equal amongst the 3 types of attacks. Volumetric attacks are still the most common.

![Pie chart showing distribution of DDoS attacks]

Fig. 8 Distribution of DDoS attacks
This is not surprising as the number of usable devices to perform a reflection/amplification is growing daily especially with the spread of IoT devices [8]. This is the reason why several mitigation techniques have been developed to counter the attacks. The idea is to mitigate all types of attacks but these techniques are mostly focused on the volumetric attacks as they represent more than 3/4 of the total amount of attacks.

2.2 Mitigation Techniques

In order to protect the infrastructure from the growing number of DDoS attacks, several mitigation techniques have been developed. In this report, we will focus on 3 types that have been widely used throughout the years. We will present the network ACLS and RTBH under its two declinations.

2.2.1 Network ACLs

This technique has been one of the first to become widely used in the ISPs and enterprises. It is due to its ease of use and implementation.

Network ACLs are a set of rules that are applied to a host, server or router to control permissions. These rules are applied to stop a specific set of packets coming from a suspicious prefix. The list protects the whole network by applying the pre-configured rules as it controls the traffic coming to/going from that point.

The steps:

1. The network administrator configures a set of rules (mostly on the router) to deny/allow access to a number of IP addresses;
2. When an IP packet transits on the router, the rules are checked and, if there is a matching IP, the access is denied or allowed;
3. If the admin detects an attack, he updates the lists.

An extension of Network ACLs allows the configuration based on the TCP/UDP port and ICMP/IGMP type.

The general structure of an ACL is as follows [9]:

```
10 deny ip 10.28.235.10 0.0.0.0 0.0.0.0.0 255.255.255.255
20 deny ip 10.28.245.89 0.0.0.0 0.0.0.0 255.255.255.255
```
Network ACLs are very easy to configure and are straight to the point when it comes to mitigating an attack. However, this technique is rather reactive than preventive. The administrator needs to update the lists whenever an attack is detected. Moreover, the longer the lists the longer the time of treatment. As all packets have to be checked, a hardware upgrade is soon to be essential. Network ACLs are not distributed across the network and need to be implemented on all routers. For these reasons, this technique has been dropped for the big networks.

Table 1 Example of network ACL configuration

<table>
<thead>
<tr>
<th>Line #</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>A packet from SA 10.28.235.10 will be denied (dropped). This ACE filters out all packets received from 10.28.235.10. As a result, IPv4 traffic from that device will not be allowed and packets from that device will not be compared against any later entries in the list.</td>
</tr>
<tr>
<td>20</td>
<td>A packet from SA 10.28.245.89 will be denied (dropped). This ACE filters out all packets received from 10.28.245.89. As the result, IPv4 traffic from that device will not be allowed and packets from that device will not be compared against any later entries in the list.</td>
</tr>
<tr>
<td>30</td>
<td>A TCP packet from SA 10.28.18.100 with a DA of 10.28.237.1 will be permitted (forwarded). Since no earlier ACEs in the list have filtered TCP packets from 10.28.18.100 and destined for 10.28.237.1, the switch will use this ACE to evaluate such packets. Any packets that meet this criteria will be forwarded. (Any packets that do not meet this TCP source-destination criteria are not affected by this ACE.)</td>
</tr>
<tr>
<td>40</td>
<td>A TCP packet from source address 10.28.18.100 to any destination address will be denied (dropped). Since, in this example, the intent is to block TCP traffic from 10.28.18.100 to any destination except the destination stated in the ACE at line 30, this ACE must follow the ACE at line 30. (If their relative positions were exchanged, all TCP traffic from 10.28.18.100 would be dropped, including the traffic for the 10.28.18.1 destination.)</td>
</tr>
<tr>
<td>50</td>
<td>Any packet from any IPv4 SA to any IPv4 DA will be permitted (forwarded). The only traffic to reach this ACE will be IPv4 packets not specifically permitted or denied by the earlier ACEs.</td>
</tr>
</tbody>
</table>
2.2.2 RTBH

RTBH (Remotely Triggered Black Hole) filtering is described in IETF RFC3882 for the first time. In this IETF RFC, the idea was to use BGP to remotely announce a mitigation. The remote triggering started to be considered as a robust solution against DDoS attacks. The final version of RTBH was described in IETF RFC5635. It has been announced as a technique that "uses the routing protocol updates to manipulate route tables at the network edges anywhere else in the network to specifically drop undesirable traffic before it enters the service provider network". It is, therefore, not needed to manually update the rules. Instead of dropping the traffic, RTBH reroutes the undesired packets to a null route called NULL0.

2.2.2.1 Destination-Based Remotely Triggered Black Hole Filtering

In this first method, the attack is to be mitigated based on the destination address or the victim's address by blackholing the traffic directed to a specified IP address. The challenge here is to mitigate this infected traffic as close as possible to the source and not let it flood the ISPs network. The block-holing action is launched by a trigger which sends routing updates to the routers until it reaches the network's edge.
The steps:

1. The administrator has to configure the trigger and enable the iBGP announcement to the PE (Provider Edge) routers. The PEs need to have a configured static route to a null destination (an unused IP address) to blackhole the packets;

2. The administrator adds a static route to the trigger which forwards the route to its iBGP peers setting the next hop to the black hole route;

3. The PEs receive the update (green arrows) from the trigger and set their next hop to null0. The destination address of the attacking flow is now set to the black hole;

4. All traffic to the target is black-holed. Once the attack is over, the administrator manually removes the static route from the trigger. The trigger then updates its peers.

This method has been widely used and still is. It has the advantage to be semi automatized as the administrator only needs to configure the trigger router and not all routers, including iBGP routers when an attack occurs. It is, also, very effective when it comes to shutting down a DDoS attack. However, all the traffic directed towards a destination is dropped. The communication with the targeted IP address is impossible throughout the attack. This is considered a significant weakness of the destination based RTBH.

### 2.2.2.2 Source-Based Remotely Triggered Black Hole Filtering

This technique has been elaborated to overcome the weakness of the Destination based RTBH. The objective is to mitigate the attack at the source and, therefore, to give the ability to the victim to still be reachable during the attack. If the source address can be identified, it is smarter to drop the traffic in the edge based on this data.

In order to identify the legitimacy of the source address, an uRPF (unicast Reverse Path Forwarding) method is used. uRPF checks if the source address is in the FIB (Forward Information Base). If it exists then the packet is forwarded otherwise it is null0 routed.

The steps:

1. The administrator has to configure the trigger and enable the iBGP announcement to the PE routers. The PEs need to have a configured static route to a null destination (an unused IP address) to blackhole the packets. uRPF must be configured on the PEs;
2. The administrator adds a static route to the trigger which forwards the route to its iBGP peers setting the next hop to the black hole route.

3. The PEs receive the update (green arrows) from the trigger and set their next hop to null0. If the source address is not in the FIB, the traffic is dropped. The legitimate traffic (black arrows) is forwarded.

4. All traffic to the target is blackhole. Once the attack is over, the administrator manually removes the static route from the trigger. The trigger then updates its peers.

The source-based RTBH with uRPF has a new approach to DDoS attack mitigation with the option to rely on the source address instead of the destination address. The victim can communicate and have internet access during the ongoing attack. However, this method still lacks granularity as it only uses the IP address to block or allow the traffic. It also requires the continuous intervention of the administrator. Another weakness is the lack of action. The only way to mitigate the attack is to drop all traffic coming from a source.

Before presenting BGP Flowspec, we need to understand the mechanisms of BGP since Flowspec is a sublayer of BGP.
2.3 BGP: Border Gateway Protocol

BGP is policy based path vector protocol that is used to build paths between the ASes (Autonomous Systems) by exchanging the routing information. Each router stores all the routing info of its neighbors in the routing table. It, then, selects the best path based on the policy specification. The policy applied by BGP is commonly based on the shortest path in distance hops, the next hop IP address, the local preferences.

*Fig.11 OSI Model with a highlight on DDoS attack sensible protocols*
These policies can be configured by the network administrator. The BGP speakers, then, forward the routing information to their neighbors and so on. The goal of BGP is to forward the packets the fastest way possible.

1. The BGP speaker 192.0.2.1 of AS88 advertises the prefix 128.112.0.0/16 to its neighbor;

2. AS7018’s edge router verifies if the this is the best route it has and adds its routing table before forwarding it via iBGP to its neighbors within the AS;

3. Router 12.127.0.121 forwards the information to the next AS after adding its AS number to the AS PATH line and modifying the Next hop field to its own IP address;

4. AS12654 verifies the information and adds it to its routing table From now on, it AS12654 receives a packet with a destination address in AS88, it will by default forward it to 12.127.0.121;
BGP is an incremental protocol that is able to update its best path at any time if a router receives a better route. There are 4 types of BGP messages [18]:

1. **Open** the router is ready to establish a peering session;
2. **Notification** shuts down a peering session in case of error;
3. **Update** announces new routes and shuts down old routes if better and faster routes are discovered.
4. **Keep Alive** handshake at different time intervals to verify the connectivity between the peers is still alive.

As an incremental protocol, BGP can continuously update its routes. The incremental updates consist of two potential steps. The first one is the **announcement** where the router selects a new active route, adds the new node id to the path and finally announces the new route to its neighbors. The second part is the **withdrawal** where the router sends a withdrawal message to its neighbors once the old route is no longer active. The UPDATE messages contain the following information [20] [21]:

1. Unfeasible route length contains the length of the withdrawn route;
2. Withdrawn routes contains the IP address prefixes of the withdrawn routes;
3. Total Path attribute length contains the length of the new route information;

4. Path attributes contains
   1. AS_PATH the AS numbers of the route
   2. NEXT_HOP the gateway of the path
   3. ORIGIN the originating system preferences of the route;

5. NLRI contains the IP address prefixes of the feasible routes being advertised
   The fact that the UPDATE messages are very important in the incremental behavior of BGP hides an important security issue. There are no verification techniques implemented in BGP to ensure the veracity of the advertised route. The protocol is, therefore, much vulnerable to attacks. The injection of false information from an attacker is, therefore, very easily performed.

2.3.1 BGP: Security issues

BGP, as a routing protocol, inherits all the security problems. The fact that it is used across the ASes makes the problem more critical. If an error occurs in the routing information, it can be propagated all over the internet. As mentioned above, BGP has been designed to be highly scalable and controllable omitting all security concerns.

As Flowspec is relying on BGP UPDATE messages to propagate its flow information, we will focus on the vulnerabilities of UPDATE.

2.3.1.1 Incorrect routing updates

A BGP speaker can advertise a wrong UPDATE message. It can claim that it has a new faster route to its neighbor. Since the receiving router cannot validate or decline the route advertisement, it can only accept it and forward it further. The originating router can, for example, advertise a more specific prefix such incidents had happened in history like YouTube blockage [22].

The Youtube blockage incident happened in Pakistan, on February 2008. Pakistan Telecom AS17557 wanted to block the Youtube website, youtube.com in Pakistan which has 3 IPs in the DNS 208.65.153.238, 208.65.153.251 and 208.65.153.253. Pakistan Telecom ended up redirecting all the Youtube traffic to a more specific IP prefix.

2.3.1.2 BGP hijacking

Path hijacking is another attack based on BGP security issues. The attacker disguises itself as another network by announcing the prefix of the hijacked subnetwork as his. The attacker sends an UPDATE notification with a more specific prefix. This false information is then accepted by other ASes and propagated all over the Internet. As a result, the traffic is redirected to the attacker which leads to a DoS attack.
The outcome of such an attack can be disastrous. The attacker is in control of all BGP information transiting between the hijacked router and the neighboring ASes. All packets going through this AS can be modified or rerouted. All information can, therefore, be collected and stored. The routing tables become invalid. The attacker can also launch other attacks in the future after collecting all the needed information regarding the network architecture and the routing tables. BGP hijacking can lead to more dangerous outcomes than a simple denial of service. Incorrect routing UPDATEs, De-aggregation, Manipulation of path attributes, blackholing or eavesdropping, are all a potential result of the BGP hijacking [23].

2.4 Flowspec, the versatile solution against all (D)DoS attacks

Based on BGP, Flowspec is the most recent solution to mitigate all kinds of DDoS attacks. In this context, Flowspec has been announced as a combination of these mitigation techniques. BGP Flowspec has been proposed by the IETF RFC 5575 as a DDoS mitigation protocol to face all the threats caused by the all-time growing attacks. Flowspec has been developed to work on top of BGP. This choice has been made based on the wide usage of BGP4 as it is the main used protocol for routing packets between ISPs (Internet Service provider) and more generally between ASs (Autonomous Systems) [11]. The idea behind the introduction of Flowspec is simple: use an existing infrastructure (BGP4) to mitigate DDoS attacks. Flowspec adds an NLRI (Network Layer Reachability Information) into BGP (AFI=1, SAFI=133) encoding a new flow specification. The flow specification is then disseminated between all BGP routers and updated in the hardware. If there is matching flow, a policy is applied. As described in IETF RFC 5575, one of 4 rules can be applied to mitigate the undesired traffic [12].

A Flowspec NLRI is defined by two fields; the length of the NLRI and its value. The value has to

<table>
<thead>
<tr>
<th>Length</th>
<th>NLRI Value</th>
</tr>
</thead>
</table>

![Fig14.BGP NLRI](image)

contain a number of fields to identify the flow. If the value contains an important number of fields, the mitigated traffic will be more specific. The components of the NLRI are defined as types and are as follows:
**Type 1**: IP Destination Address- Refers to the IP address targeted by the DDoS attack

**Type 2**: IP Source Address- Refers to the IP address generating the DDoS attack

**Type 3**: IP Protocol- Type of IP protocol and values

**Type 4**: Port- source ports/ destination port of the DDoS attack (UDP, TCP, HTTP...)

**Type 5**: Destination Port- Targeted port

**Type 6**: Source Port- Origin port

Most of the Flowspec NLRIs are defined by these 6 types. However, the NLRI can provide more details about the flow by enabling the other fields (types)

**Type 7**: ICMP type- Matching the type field of an ICMP packet

**Type 8**: ICMP code- Matching the code fields of the ICMP packet

**Type 9**: TCP flags- Specifies the flags in TCP packets

**Type 10**: Packet length- the length of the packet

**Type 11**: DSCP- Diffserv code point used to classify the traffic and provide the QoS (Quality of Service)

**Type 12**: Fragment- Checks if it is a fragmented packet

An example of a Flowspec NLRI is to be provided in order to be able to understand the mechanism. All fields are encoded in hexadecimal. If we want to mitigate the following flow:

“All packets from 10.0.0.1/24 to 172.0.2.1/24 on port 25”

<table>
<thead>
<tr>
<th>Destination</th>
<th>Source</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01 18 0a 00 00 01</td>
<td>0x02 18 ac 00 02 01</td>
<td>0x04 81 19</td>
</tr>
</tbody>
</table>

The complete mechanism of Flowspec NLRIs can be found on the IETF RFC5575: Dissemination of Flow Specification Rules.

Once the attacked subnetwork (BGP router) provides the NLRI to all BGP routers, the upcoming packets can be compared to the flow. If there is a match between a packet and the non desired flow then a rule has to be applied.

---

**Fig 15. Flowspec rules algorithm**
The rules are defined using BGP extended communities [13] and are set up by the network administrator since the default behavior is to accept the traffic that matches the rule. The widely applied rules are as follows:

- **Traffic-rate**: This action limits the traffic to a certain threshold. When applied, all the traffic that matches the flow is rate limited to the beforehand set rate. If we take the example of the flow “All packets from 10.0.0.1/24 to 172.0.2.1/24 on port 25” and apply the limitation of this traffic to 1Mbps then the DDoS attack would be mitigated. The rate can be set to 0 and the traffic would be discarded.
- **Traffic-action**: This action allows the ISP to sample the traffic to be analyzed or to apply a rule on it.
- **Traffic-redirection**: This action redirects the matching traffic to a black hole or to a different VRF to be analyzed. This action is commonly used by ISPs to sample the traffic and to output some patterns for an easier detection.
- **Traffic-marking**: This action is used when the administrator doesn’t want to drop, rate-limit or redirect the traffic but edit the DSCP to lower the QoS of the flow. If the QoS is low the packets belonging to the flow are less likely to be treated.

The traffic filtering information can be configured by the network administrator to be accepted or denied.

If we summarize the mechanism of Flowspec, we can say it is decided in two parts. The first part consists of providing information matching the policy rule. The second one provides instructions to mitigate the infected traffic based on actions.

### 2.5 Flowspec Pros

After understanding how BGP Flowspec works, it is essential to tackle the advantages it has compared to the previously mentioned DDoS mitigation solutions and mechanisms. The first considerable advantage of Flowspec over the previously presented mitigation techniques is its **granularity** when defining the mitigation rules as it provides a big range of matching criteria. The 12 rule types give us the possibility to be as detailed as possible in the flow matching. It provides more options than an ACL and is equally as easier to configure. Added to this, it is distributed; all routers can signal an attack and distribute the matching flow. The order of matching types is from the **MSB (Most Significant bit)** to the **LSB (Least Significant Bit)**, from type1 to type12.

Another advantage that has been much welcomed by the system administrators and other network engineering is Flowspec’s **automation**. As it relies on BGP, it is way
easier to propagate the rules and filters to the edge routers of a given network. Thanks to the BGP Extended Communities[13], one router can share the new filters with its neighbors. The main idea here is to enable the client of an ISP to automatically mitigate its traffic in case of DDoS attack on it network [14] and the ISP to automate the rules distribution between its egress and ingress routers.

The implementation of Flowspec on an existing infrastructure has also been a leitmotiv to standardize IETF RFC5575. BGP is the main used protocol for intra and inter domain routing. This existing external relationship between the autonomous system based on BGP has accelerated the implementation of Flowspec on a large scale.

Now, if we compare Flowspec with some of the mitigation techniques that have been mentioned in 2.2 we can output a clear advantage for Flowspec.

Compared to the Firewalls and Network ACLs, Flowspec relies on an existing BGP infrastructure which allows the ISPs and their customers, to save the money that has to be invested on expensive and dedicated hardware. Even if the company invests in pricy hardware, it still has to be placed in the strategic areas of the network. Most of the time, more than one device is needed as the network of big companies can have more than one edge router. Sometimes, firewalls are also placed between independent VLANs to protect the network from internal threats[15]. Since all routers can mitigate DDoS threats with Flowspec, such an investment is not needed anymore.

Moreover, there is a sensible aspect that has to be taken into consideration, it is the performance and mitigation time. With Flowspec, the mitigation is done closer to the source. By sharing the rules, the mitigation is done closer and closer to the source of the attack. This characteristic has a considerable impact on the used resource since the capacity of the network is not wasted. If we can summarize the advantages of Flowspec, we can say that it is a better version of the BGP black hole routing because it includes more mitigation actions and relies on a separate NLRI.

2.6 BGP Flowpsec in action

Now that the importance and advantages of BGP Flowspec have been explained, it is important to understand how this protocol works in a real-life implementation as it has been proposed in IETF RFC5575.

The main focus when launching Flowspec was to make it as easy and automatized as possible to mitigate a DDoS attack on a given network. The main businesses that would benefit from it are ISPs (Internet Service Providers). The new protocol is to help them secure their network and more importantly to provide a more reliable security service to their customers. We will, therefore, take as an example an ISP/Enterprise relationship to understand how Flowspec works in a real-life model.
In Fig.12 we can see how Flowspec is supposed to be working in a real-life situation where a server (204.0.120.1) is under attack. In order to fully use the functionalities provided by Flowspec, the enterprise’s edge router initiates an announcement to the edge routers ISP that spreads the information around all the routers until reaching the network edge where the attack arises from. Each router within the ISP network applies the instruction previously configured by the network administrator/manager. Here, we took the example of a rate limiting to 0 for all the packets which have a size between 100 and 150 bytes. The BGP prefix is then installed on the CE (Customer Edge) router with an action “set to rate 0”.

The main perks of such a mechanism is to start the mitigation as close to the destination of the attack as possible. This would give the ISP customer the opportunity to configure its edge router to initiate the announcement and to choose which traffic to mitigate or not. Flowspec has been announced as the solution to make the mitigation of DDoS attacks as easy as possible and with the least required actions from the administrator as possible. We will here take an example of the configuration of a Cisco CE:

```
router BGP 64496
address family ipv4 flowspec
neighbor 204.0.120.54
remote-as 64511
address family ipv4 flowspec
```

**Fig.16 Inter-domain DDoS mitigation using Flowspec**
The **config file for the address family mapping** of the Cisco CE is very easy to understand and to modify. If we want to have a quick deeper look at the configuration here, we can translate it to:

CE router belonging to **AS64496** with an IP address version 4 enabling Flowspec communicates with the its neighbor (ISP PE) with an IP address version 4 **192.0.2.1** belonging to the **AS64511** and accepting flowspec announcements.

The PE router also has to enable its Flowspec **config file for the address family mapping**:

```
router BGP 64496
address family ipv4 flowspec
neighbor 192.0.2.1
remote-as 64511
address family ipv4 flowspec
```

The second required file on the CE router is the **Flowspec rule configuration file** [16]. It has to be as follows in order to mitigate the DDoS attack:

```
class-map type traffic match-all match-pkt-len
  match packet length 100-150
end-class-map
!
policy-map type pbr test2
  class type traffic match-pkt-len
    drop
!        
  class type traffic class-default
!        
end-policy-map
!
```

The rule configuration file is also straightforward. It can be translated as follows:

A class (rule) is configured to **match all packets** with a length between **100 and 150 bytes** and to **drop** them. In this case, all packets, regardless of the source or destination address are discarded.
If we summarize, the PE router has to be configured to enable Flowspec and to know its neighbors as well as its AS. The ingress routers also need to have had seen their config file configured and enabled to be able to forward the matching flow information and action. On the other hand, the CE, in addition to the configuration of its config file for the address family, its rule configuration file is to be set to launch the flowspec action.

From the Flowspec config files, we can clearly say that these settings are set to protect the customer network from a Slowloris attack. This type of attack, as seen in section 2.3, is based on a big amount of small-sized packets. It is, therefore, very easy to configure a Flowspec rule for it as no source or destination IP addresses are needed.

Chapter 3

Methodology
3.1 Flowspec’s security issues

Now that the configuration of Flowspec as described in IETF RFC5575 has been explained, we will see how vulnerable a Flowspec based infrastructure could be for both the enterprise and the ISP.

Since any of the routers are considered a Flowspec speaker, all of them have the rights to specify mitigation rules on any flow. Before getting in the details of Flowspec vulnerabilities, it is important to take a look at BGP’s security issues because it is the protocol on which Flowspec relies. We will consider here that the IP and TCP layers are secure.

3.1.1 Case study 1: Customer misconfigured router

In this case, we will see how a misconfigured router can cause a flow blocking on the ISP’s network, another customer of the ISP or its AS.

In this scenario, we will consider an ISP that has enabled Flowspec UPDATEs from its customer and configured its edge router to accept all the flow instructions from its customers as it has been described in IETF RFC5575.

The case taken into consideration here will be the blocking or rate limiting of the traffic on another customer’s AS. This case is the most likely to happen because ISPs have control over their internal network. This makes a BGP error over the ISP network very unlikely.

3.1.1.1 The topology

3.1.1.2 The situation

In this topology, we have a communication between two ASes via the same ISP. Both are this ISP’s customers and access the Internet through the same gateway. C1R1 is a router
within AS65000. It has misconfigured Flowspec configuration file. This could happen as the number of routers in an enterprise can be considerable and sometimes, there is no full time network administrator to take care of the network.

We will consider, as an example, that there is an increase of data transmission between enterprise1 and enterprise2 after the signing of a new contract whereas in C1R1 the config file has been set-up, a while ago, to **rate limit the traffic coming from enterprise2**.

### 3.1.1.3 The steps

1. C1R1 detects a high traffic coming from CE2. It initiates a Flowspec announcement to rate limit all traffic from CE2;
2. CE1 propagates the announcement to PE1, that, itself, shares it with its ISP peers including PE2;
3. PE2 rate limits the traffic coming from CE2 and, therefore, from AS65002.

Fig.17 Case1 Topology diagram
3.1.1.4 The result

As a result, AS65002’s upstream is limited until it is detected and the ISP disables this misconfiguration. This misconfiguration can be fatal for both enterprise 1 and enterprise 2 if they have important data to exchange. This situation is very specific but still can occur and there is no security provided by IETF RFC5575 to prevent this kind of misconfiguration. The situation generated by the misconfiguration of 1 ingress router is more dangerous as it would affect the ISP’s reputation when the misconfiguration wasn’t from an ISP’s router. It wouldn’t take more than a couple of seconds to re-enable the traffic between the 2 enterprises but the blocking needs to be detected and the Flowspec config file of C1R1 modified. Otherwise, as the ISP reenables the traffic for AS65002, it needs to decline all Flowspec UPDATEs from C1R1. However, there can be more misconfigured routers in enterprise 1’s network. The situation can, therefore, be tricky to solve.

3.1.2 Case study 2: Customer's rogue router

In this case, we will explore the danger of a rogue router in the customer side and its impact on the enterprise network. However, before diving into the case’s details, it is important to understand what a rogue router is.

A rogue router or rogue Access Point (AP) is a wireless AP that is connected to a secure network but doesn’t have any specific configuration or authorization (Soft Access Point). It can be the result of an oversight of the network administrator that has forgotten to update a non-secure module on the router. A malicious attacker can also have accessed the enterprise’s offices to install a rogue router. In most cases, the rogue AP is configured in a way that makes it easy to access, it is likely that it is configured as "OPEN", without any security protocol. This makes it easy for the person in charge to detect it. However, when a company has hundreds of APs inside their offices, it is common that a router can be misconfigured or not updated.

3.1.2.1 The topology

3.1.2.2 The situation

In this topology, the attacker is on the side of the enterprise. Once he has configured or found a rogue access point, he doesn’t have to be inside the organization’s office but can be nearby where he still receives the signal from the rogue AP. The attacker can be in his car in the parking lot or sitting on a bench next by. Once he penetrated the enterprise’s network, it is very easy for the attacker to change the configuration of all connected
routers. The security of the network is now threatened. Of course, the attacker can access sensitive content, data and logs but can also launch DDoS attacks via bots once the security disabled. He is now in control of the network. As we are focusing on the vulnerabilities of Flowspec and its potential uselessness against DDoS attacks, we will detail a scenario where the attacker launches a DDoS attack after penetrating the network.

### 3.1.2.3 The steps

1. The attacker accesses the AP and hacks into the network of the enterprise;
2. The attacker disables all Flowspec config files in the routers or modifies them;
3. The attacker uses botnets to launch a DDoS attack on AS65000 but the attack cannot be detected and mitigated;
4. The attacker keeps updating the Flowspec config file if they are brought back to normal by the network administrator.

**Fig.18 Case2 Topology diagram**

![Case2 Topology diagram](image-url)
3.1.2.4 The result

As a result, the enterprise’s network is paralyzed until they find the rogue AP and shuts it down or secure it. In the meanwhile, the attacker has full power on the network components and can keep launching DDoS attacks on the network without being blocked by Flowspec as the ISP routers have not been UPDATED. Moreover, if the attacker is granted access to one or several routers, he can launch Flowspec UPDATE messages with faulty rate limiting or black-holing actions. As a trusted AS, the ISP will forward the UPDATEs and apply the actions on its edges. The only way to prevent this from happening is to notify the ISP (phone, email…) of the wrongness of the UPDATE messages sent from AS65000. The ISP then takes action to deny all actions triggered by the enterprise. Once done, the enterprise needs to find the rogue AP and deny access to the network.

3.1.3 Case study 3: Hijacked BGP

In this case, we will explore the vulnerabilities of BGP Flowspec in a real-life situation when it comes to a hijacking (section 7.1.1).

3.1.3.1 The situation

Since BGP determines how data travels from its source to its destination, its manipulation can reroute data in an attacker’s favor, allowing him to intercept or modify traffic. The attacker can also freely launch wide DDoS attacks. So, BGP hijacking is performed by configuring an edge router to announce prefixes that have not been assigned to it. If the malicious announcement is more specific than the legitimate one, or claims to offer a shorter path, the traffic may be directed to the attacker. By broadcasting false prefix announcements, the compromised router may poison the Routing Information Base (RIB) of its peers: after poisoning one peer, the malicious routing information could propagate to other peers, to other Autonomous Systems, and onto the entire Internet [24].

3.1.3.2 The topology

3.1.3.3 The steps

1. Enterprise1 requests a path to 1.1.1.1 looking for Enterprise3 through its ISP1 which forwards the request to ISP2;
2. Attacker’s AS4 announces a more specific prefix /24 instead of the real one /16 belonging to Enterprise3;
3. ISP2 announces it to ISP1 which forwards the announcement to Enterprise1. The new Path is now in the RIBs of each router of the different ASes;
4. The attacker hiding behind AS4 can easily collect all the information transiting from Enterprise1 to Enterprise3 as well as launching DoS attacks.

3.1.3.4 The result

The fact that the attacker can redirect all the packets can very dangerous for both enterprises. However, what we are interested in are the vulnerabilities of Flowspec. Once the path to AS3 is hijacked by an attacker in AS4, it is easy to send a BGP Flowspec UPDATE rate limiting the upstream of Enterprise1. ISP1 and ISP2 would implement the new rule on their PEs. In this case, the attacker cannot retrieve the packets sent by Enterprise1 because it is now in quarantine. However, he can still launch
DDoS attacks on its infrastructure. Flowspec can here endanger the ISPs and the Enterprises.

Chapter 4

Results
4.1 Flowspec: The difference between IETF RFC5575 and practical use

Given its non-security, Flowspec has only rarely been used as described in IETF RFC5575. Even if it is a very promising and versatile protocol, the ISPs seem to be reluctant to propose Flowspec to their customers as part of the in-built security [25]. It is, however, appreciated as an ISP internal tool to protect the network within the ISP’s AS [25]. We will see how most of the ISPs that have integrated Flowspec in their security offer use it.

Instead of giving all Flowspec routers the full power to detect a suspicious flow of packets, make a decision to mitigate it and forward the action to the neighboring routers, the ISPs have chosen to secure their internal network by not accepting their customers’ actions without prior verification.

ISPs use a NOC (Network Operation Center), where the network is monitored, to configure new Flowspec routes. The BGP speakers are, therefore, not the ones allowed to set new routes and new actions to mitigate the attack. The customer needs to notify the ISP, that configures the new routes directly from the NOC then, using Flowspec, forwards the new actions to the BGP routers. In this case, the customer needs to notify the NOC by issuing a phone call, sending an email or logging into the ISP’s portal, if there is a provided one. The enterprise and the ISP, definitely, need some coordination in order to mitigate the attack.

Flowspec is, therefore, not used as described in IETF RFC5575 as the automation of the protocol is not used. The inter-AS route advertisement should only be enabled by the ISP if they can trust their customer. The enterprise have to detect the attack and cannot configure its own routers to take actions in order to stop the malicious flow. The enterprise can block the DDoS attack on its edge but still, have to notify the ISP so that the NOC can take action. The full automation announced in IETF RFC5575 has not been completely fulfilled, yet. The security issues of BGP are ubiquitous and cannot be bypassed to fully implement Flowspec.

In the next table, we will make a comparison between the use of Flowspec as described in IETF RFC5575 and how it should be used by ISPs [39].
Flowspec Advantages | Flowspec in IETF RFC5575 | Flowspec in practice
---|---|---
**Granularity** | Per flow | Per flow
**Automation** | Fully automatic | Not between ASes
**Actions** | Drop, Rate limit, Redirect | Drop, Rate limit, Redirect
**Speed** | 1-2 orders of magnitude faster (seconds/minutes instead of hours) | Depends how fast the enterprise detects the attack, notifies the ISP which takes action
**Efficiency** | Closer to the source | Enterprise’s edge, then ISP’s

Fig.20 The use of Flowspec in a real-life situation

[25]
It is clear that the ISPs value the security of their network and are not ready to give the keys of the attack management to their customers. The customers, on the other hands, start to be more aware of the importance of security but cannot allow themselves to change their security protocol to Flowspec, yet. For the bigger customers, some ISPs propose Flowspec as a premium tool managed by the NOC but is not fully integrated to their security solution just yet. In an investigation ran by Juniper in 2014 [25] on enterprises from various sectors of which 83% in the Telecommunication, Technology, Internet and Electronics sector, they had more than 60% responding negatively to whether or not they are using Flowspec as mitigation technique. For the 40% that have integrated Flowspec, 91% do not allow their customers to send Flowspec routes via BGP.

These stats provided by Juniper that the enterprises are not setting Flowspec as a priority. They are fine with the older technologies. However, with the add-ons made by the vendors like Cisco, Juniper or Alcatel, the customers can start reconsidering their position taken toward Flowspec. As stated in the Juniper Networks report [16], in order to see Flowspec take off, enterprises are waiting for ISPs to accept their Flowspec routes. As we have seen in Chapter 4, this might never happen or would be
via a NOC and a Flowpsec speaker. Another detail that has been revealed by this report is the fact that more vendors are supporting Flowspec. This is encouraging and might convince the ISPs to use it with eBGP.

4.2 The use of BGP Flowspec by DGC

BGP Flowspec is a potent to mitigate DDoS attacks. It presents a the advantages of both RTBH and network ACLs combined with an automatic triggering. This would be a considerable gain of time and resources for the ISP if an attack occurs. Furthermore, the fact the DGC’s hardware supports BGP Flowspec is another advantage as they do not need to invest in new devices. Thus, the cost of implementation should not be very high.

However and given the study cases we took into account, the potential use of BGP Flowspec by DGC would only be acceptable in iBGP. BGP Flowspec presents an important number of advantages that ISPs can benefit from but it can be risky for DGC to exchange route updates with external peers [38]. They need to trust the BGP action announcements of their customers. However, as they do not handle the network architecture and daily support of their customer’s infrastructure, they cannot ensure the legitimacy of the Flowspec announcement coming from external peers.

If we get back to the research question asked in the introduction, we can say that DGC can benefit from Flowspec by using it with iBGP to secure its own infrastructure from DDoS attacks. On the other hand, it is not safe to provide Flowspec based mitigation to their customers. If they decide to accept Flowspec announcements form their customers, they have to accept or deny the announcement by making it transit by the NOC.

4.3 Proposal of a safe testing environment for BGP Flowspec

According to our methodology choices respecting a prescriptive model, our intervention on the ISPs site took 6 months during which frequent interactions with the project team took place. This ongoing process of back and forth between the field and the literature allowed us to progressively build the proposed solution and to meet the needs of the project manager and his team.

In the following sections, we will give details of each step of the engineering design process we followed to present a solution.

4.3.1 Defining the problem/need
To define the problem/need we will use a mind mapping tool answering the following question:

- What is the problem or need expressed by DGC?
- Who has the problem or need within DGC?
- Why is it important to solve?

The following mind map will help us structure the information towards designing of the expected solution.

4.3.2 Do background research

This step allows us to learn from the experience of others to find out existing solutions to our research problem. For our engineering design project, we referred both to the theoretical solution described in RFC5575 and the experience feedback of the use of BGP Flowspec by network component vendors and Internet service providers. The output of this step is Table.2. Few research papers treating this topic were found. The main reference was for us the research done by Next Layer Communications and T-Mobile Austria [43] which treats the limits of BGP Flowspec from the perspective of the vendors by testing 4 routers from 4 different vendors (Juniper, Cisco, Alcatel, Huawei). This paper analyses some bugs related to either the propagation of Flowspec NLRIs between routers from different vendors. It also follows the propagation of the NLRI from the BGP daemon (ExaBGP).

4.3.3 Specify requirements
In this subsection, we specify the characteristics of the proposed solution to apply the findings stated in the section 4.1. As for the application of the use of BGP Flowspec, a potential solution would be to suggest a testing environment based on the good practices proposed in Table 2. Furthermore, DGC has requested the use of open source solutions in the building of the testing environment. Our choice fell on GoBGP, a BGP focused daemon, that allows network engineers to explore Software Defined Network (SDN) solutions applied to BGP.

Another BGP stack under the name of ExaBGP has been explored. Although ExaBGP is more widely used, as it has been around for a longer time, and has the same performance, GoBGP has appeared to be more flexible, user friendly and provides a more complete documentation to elaborate a testing environment.

4.3.4 Brainstorm Solution

Researchers and engineers recognize that there is always several possibilities to solve a problem. For our study, we are looking for an alternative solution for the protection of DGC against DDoS attacks for the reasons mentioned in section 4.3.1. Regarding the specific needs of the project team mentioned in section 4.3.3. We didn’t have to present a panel of solutions but were oriented towards the use of GoBGP in our solution as an alternative way to the use of commercial mitigation tools.

4.3.5 Develop the Solution

During our intervention at DGC and through the interaction with the project team, we had to refine and improve the solution proposal. A first prototype has been demonstrated but a the expected results were only partially met. This allowed us to rethink the proposed solution and review the state of the art in this field. In the following section we will give details about the steps we followed in the design of the solution.

4.3.6 Build a Prototype

Based on the requirements provided by DGC and the output of our theoretical research, a first prototype has been built to test the usage of BGP Flowspec. The following components have been chosen to emulate a testing environment:

- GNS3: An open source software to simulate and emulate a network [44]
- GoBGP: An open source BGP daemon for SDNs [45]
- Gabu: An open source User Interface (UI) to pilot the Flowspec rule injection to GoBGP

These tools will allow us to emulate a testing environment for DGC providing a simplified architecture of their infrastructure’s edge. The applicative architecture of the environment is as follows.
The Virtual Machine (VM) represents the NOC where ISPs control the attack mitigations and supervise uncommon behaviors of the network. It is within the same AS as the rest of the network components. We are here using iBGP to communicate between the NOC and the ISPs edge.

Fig 22. Software architecture of the virtual environment

Fig 23. Topology of the initial virtual network
Two Cisco IOSXRv router images accepting Flowspec routes have been used in the first prototype. IOSXRv-1 is linked to the "Flowspec-Server" via the interface who’s IP address is 192.168.100.22. The Flowspec rules received by IOSXRv-1 are disseminated to IOSXR-2.

The purpose of such an architecture is to mitigate the traffic coming from the "attacker" via its interface e0 with the IP address 10.10.11.2 preventing the supposed harmful traffic from reaching the "victim" found behind IOSXR-1.

4.3.7 Test and Redesign

At this step of the engineering research, multiple iterations are needed to reach the delivered solution. We had to test the first prototype, find if there are any problems and, then, make the necessary changes and retest our solution before settling the final design.

In this first design, we were able to propagate the Flowspec rules from the emulated security center, consisting in the user interface, the GoBGP stack and the virtual network interface, to IOSXRv-1. The destination router was able to recognize the rule and to store it in its RIB. However, the new rule is not applied by the router. The mitigated traffic is still flowing through the routers and reaching its destination.

After checking the environment configuration and performing a long investigation, it came out that the issue was not coming from the configuration but rather from the router image itself. A configuration on IOS-XRv wasn't accepted and uncommitted.

```
RP/0/0/CPU0:xrv1(config)#flowspec
RP/0/0/CPU0:xrv1(config-flowspec)#local-install interface-all
RP/0/0/CPU0:xrv1(config-flowspec)#commit

% Failed to commit one or more configuration items during a pseudo-atomic operation. All changes made have been reverted. Please issue 'show configuration failed [inheritance]' from this session to view the errors
```

When running the suggested command to have more details about the error, the following output is displayed

```
!! SEMANTIC ERRORS: This configuration was rejected by
!! the system due to semantic errors. The individual
!! errors with each failed configuration command can be
!! found below.
flowspec
```
The source of the problem has been identified. 'FS MGR', the management brick of Flowspec on Cisco IOS-XRv is not supported. The virtual router can, thus, only used as a client receiving Flowspec rules. The installation of the rule on the interface is, apparently, done via the Cisco hardware. Although, not many sources have tackled this topic, we managed to have a slight confirmation on a Github thread [41] and on a Japanese blog [42].

Once the source of the problem identified, another virtual router provided by a different vendor was required. The choice of Junos vMX 18.2.R1.9 provided by Juniper has been proposed by DGC as an alternative as it is used in their infrastructure. The architecture of the virtual image is different from the one provided by Cisco.

The vMX image has the advantage to contain 2 distinctive parts. A Control Plane (vMX-VCP-1) and a Forwarding Plane (vMX-VFP-1). We are, therefore, reassured in the fact that the disfunction encountered with the use of IOS-XRv will not be reproduced.
The second router's architecture being different from the first one, the virtual network topology has been modified. The Control Plane and Data Plane need to be connected via a switch. This component acts as an out-of-bound management device. The new network architecture is as follows:

Fig 25. Topology of the initial virtual network
The new virtual network topology has been slightly changed due to the hardware capacity. Junos vMX requires 6 Go of RAM to be fully functional. Adding up another router would no the sustainable for the bare metal server we are using to deploy the virtual network. However, it has been designed to allow extra components to be plugged in. The NOC VM is connected to the Control Plane via a virtual bridge. We added up 2 virtual PCs for testing purpose.

With this new topology, we have been able to bypass the issue encountered when using Cisco IOS-XRv. We are now able to send Flow specification rules from the NOC to the Junos router and challenge the applicability of these rules with a concrete set of tests.

4.3.8 Communicate Results
This step consists of communicating and demonstrating the results. The appendices in the end of this document will allow the project to use the solution as a starting point for further investigation in a perspective of cumulative research.

We aim to test our solution in the limits of the hardware specifications. We will, therefore, test the granularity of Flowspec. The mitigation of the attacks are not automatic as it transits by the NOC. The mitigation is triggered manually via the NOC user interface. We will follow the propagation of the flow from the its introduction in the NOC to its application by the router. The tests performed will be limited due to the limitation of the resources. We will mainly use pings to verify the mitigation of the attacks. The RIB of the router will be reinitialised between the tests and previous NLRI removed.

**4.3.8.1 Test1 : Testing Flowspec on 2 different IP addresses**

The first test is to drop all traffic from PC-1 (172.16.0.2) to PC-2 (172.17.0.2) regardless of any other flow specification. We, therefore, inject the following flow:

```plaintext
from src address 172.16.0.2 to 172.17.0.2 then drop
```

We, then, examine the BGP daemon, GoBGP to verify the propagation of the flow specification from the UI to the daemon. We run the following command:

```plaintext
gobgp global rib -a ipv4-flowspec
```

The expected output is as follows:

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>AS_PATH</th>
<th>Age</th>
<th>Attrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>* &gt; [destination: 172.17.0.2/32] [source: 172.16.0.2/32] fictitious</td>
<td></td>
<td></td>
<td>00:01:11</td>
<td>[{Origin: ?} {Extcomms:[discard]}]</td>
</tr>
</tbody>
</table>

We, then, inspect the propagation of the NLRI from the NOC to the router. Wireshark has been used as a supervision tool. It allowed us to have a precious details about the NLRI propagation. More details in appendix 3.
We can, now, verify the acceptance of the NLRI by the router by checking its RIB using the following command:

```
show route table inetflow.0 detail
```

The expected output is as follows:

```
inflow.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

172.17.0.2,172.16.0.2/term:1 (1 entry, 1 announced)
  *BGP  Preference: 170/-101
  Next hop type: Fictitious
  Address: 0x9a1d9dbc
  Next-hop reference count: 1
  Next-hop:
    State: <Active Int Ext>
    Local AS: 65000 Peer AS: 65000
    Age: 10:01
    Validation State: unverified
    Task: RT Flow
    Announcement bits (1): 0-Flow
    Communities: traffic-rate:0:0
    Accepted
    Local-pref:100
    Router ID: 192.168.100.133
```

Now that we have verified the good integration of the flow specification in the RIB. We are able to proceed to visualising the traffic mitigation by running ping commands from PC-1 to PC-2.

```
PC-1> ping 172.17.0.2
```

---

**Fig 26. Wireshark Capture of the UPDATE message in Test1**
With the first command, we are testing the communication between PC-1 and PC-2 using ICMP packets.

PC-1 and PC-2 are unable to communicate. However, we cannot be sure that the IP address has been taken into account. The granularity of flowspec on the IP address can only be verified when launching the same commands from another source. We will, therefore run the same set of commands from PC-4.

PC-4 and PC-2 are unable to communicate. However, we cannot be sure that the IP address has been taken into account. The granularity of flowspec on the IP address can only be verified when launching the same commands from another source. We will, therefore run the same set of commands from PC-4.
The first two pings are lost due to the fact that it is the first communication between PC-4 and PC-2 (as well as between PC-1 and PC-2). An ARP request is, therefore, sent to learn the MAC address of the destination. The rest of the packets are received by PC-2.

**4.3.8.2 Test2: Testing Flowspec on 2 different protocols**

The second test consists in dropping specific traffic from PC-1 (172.16.0.2) to PC-2 (172.17.0.2) by specifying the protocol and/or the ports. We will drop all UDP traffic from PC-4 to PC-3 and drop TCP traffic from PC-1, port number 2222 to PC-2, port number 2223.

```
from src address 172.16.0.2 to 172.17.0.2 protocol TCP src port 2222 dst port 2223 then drop
from src address 172.19.0.2 to 172.18.0.2 protocol then drop
```

We, then, examine the BGP daemon, GoBGP to verify the propagation of the flow specification from the UI to the daemon. We run the following command:

```
gobgp global rib -a ipv4-flowspec
```

The expected output is as follows:

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>AS_PATH</th>
<th>Age</th>
<th>Attrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; [destination: 172.17.0.2/32] [source: 172.16.0.2/32] [protocol:==tcp][destination-port:==2223] [source-port:==2222] fictitious</td>
<td>00:01:11 [{Origin: ?} {Extcomms:[discard]}]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*&gt; [destination: 172.18.0.2/32] [source: 172.19.0.2/32] [protocol:==udp] fictitious</td>
<td>00:01:11 [{Origin: ?} {Extcomms:[discard]}]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

We, then, inspect the propagation of the NLRI from the NOC to the router. Wireshark has been used as a supervision tool. It allowed us to have a precious details about the NLRI propagation. More details in Appendix 2.
We can, now, verify the acceptance of the NLRI by the router by checking its RIB using the following command

```
show route table inetflow.0 detail
```

The expected output is as follows:

```
inetflow.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

172.17.0.2,172.16.0.2,proto=6,dstport=2223,srcport=2222/term:1 (1 entry, 1 announced)
  *BGP  Preference: 170/-101
  Next hop type: Fictitious
  Address: 0x9a1d9dbc
  Next-hop reference count: 2
  Next-hop: State: <Active Int Ext>
  Local AS: 65000 Peer AS: 65000
  Age: 7:01
  Validation State: unverified
  Task: RT Flow
  Announcement bits (1): 0-Flow
  Communities: traffic-rate:0:0
  Accepted
  Local-pref:100
  Router ID: 192.168.100.133

172.18.0.2,172.19.0.2,proto=17/term:1 (1 entry, 1 announced)
  *BGP  Preference: 170/-101
  Next hop type: Fictitious
  Address: 0x9a1d9dbc
  Next-hop reference count: 2
  Next-hop: State: <Active Int Ext>
```
Now that the flow specifications are saved in the router RIB, we will launch a set of tests. The first command is the following

```
PC-1> ping 172.17.0.2 -3
```

We, here, aim to verify that we are able to ping PC-2 using TCP without specifying the source/destination ports. We are able to communicate with PC-2 under TCP.

![Fig 30. Result of the communication between PC-1 and PC-2 in Test2 using TCP](image)

We, now, specify the source and destination port and reiterate the test.

```
PC-1> ping 172.17.0.2 -3 -p 2223 -s 2222
```
The traffic is mitigated only when traffic is flowing between port 2222 and 2223 using TCP. It is, therefore, possible to mitigate traffic based on the protocol and the ports. We will, now, verify that UDP pings are enabled between PC-1 and PC-2 but not between PC-3 and PC-4. For that, we run the following commands.

```
PC-1> ping 172.17.0.2 -2
PC-4> ping 172.18.0.2 -2
```

The results are as follows:
The UDP traffic is mitigated between PC-4 and PC-3 only.

In this second set of tests, we were able to demonstrated the granularity of Flowspec. We are able to specify protocols and ports of the flow we want to mitigate.

After testing Flowspec in a virtual environment, we can take a look at If we have a look at Table.2 in section 4.1 and check how far we have been able to apply the characteristics of Flowspec in our environment.

### Flowspec Advantages

<table>
<thead>
<tr>
<th>Flowspec in IETF RFC5575</th>
<th>Flowspec in practice</th>
<th>Flowspec as tested in the virtual environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Granularity</td>
<td>Per flow</td>
<td>Per flow</td>
</tr>
<tr>
<td>Automation</td>
<td>Fully automatic</td>
<td>Not between ASes</td>
</tr>
<tr>
<td>Actions</td>
<td>Drop, Rate limit, Redirect</td>
<td>Drop, Rate limit, Redirect</td>
</tr>
<tr>
<td>Speed</td>
<td>1–2 orders of magnitude faster (seconds/minutes instead of hours)</td>
<td>Depends how fast the enterprise detects the attack, notifies the ISP which takes action</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Closer to the source</td>
<td>Enterprise’s edge, then ISP’s</td>
</tr>
<tr>
<td>Manageability</td>
<td>Fully automatic</td>
<td>NOC</td>
</tr>
</tbody>
</table>

Table.3 Comparison between the presentation of Flowspec, its use in practice and its tested features
We can say that we have been able to address 4 Flowspec advantages out of 6 listed. This is mainly due to the hardware limitations we encountered as several components are needed to test the different actions provided by Flowspec. We were able to drop the packets but not limit the rate as we only had access to VPCs allowing ping commands. As for the testing of Flowspec using eBGP, different ASes with Flowspec accepting routers had to be created. For this, we need to have access to a resource with 64 go of RAM or a lab with a functioning topology.
Chapter 5

Conclusion

5.1 Conclusion

This thesis analyzes the pros and cons of BGP Flowspec as a solution against DDoS attacks. BGP Flowspec, as described in RFC5575 cannot be implemented without considering its vulnerabilities. There are some important details to be taken care of before we can widely use Flowspec as a mitigation technique against DDoS attacks [38]. We have noticed that, through the study cases, Flowspec can contribute and facilitate a DDoS attack. It can be used against the victim due to the lack of security presented by BGP.

BGP Flowspec can still be used in an iBGP network where all hosts and routers are trusted. It is, indeed, used inside the ISPs network to protect the AS from potential attacks. However, ISPs do not support their costumers’ Flowspec routes just, yet. This is not due to the lack of trust in Flowspec but rather in the lack of trust in BGP. Before we can expect to widely use Flowspec, an important work has to be done to secure BGP. This has been started with the emergence of BGPSec [26] and S-BGP [27]. We also need to take into account that enterprises and ISPs are not setting Flowspec as a priority because they already have an older mitigation solution up and running.

Based on the good practices regarding the use of BGP Flowspec in a production environment, we provided a basic virtualized infrastructure to test the usability of Flowspec on the edge of an ISP network. We have been able to emulate the communication of the NOC with the ISP edge router accepting Flowspec. Tests on the virtual environment have been conducted and showed the possible usability of Flowspec in a testing environment.

DGC seems to be ready to implement Flowspec in the protection of their own infrastructure. The needed components for the use of Flowspec as a mitigation technique are in the possession of the ISP.

Further tests involving multiple physical routers accepting Flowspec and an enhanced hardware capacity need to be conducted. A lab with advanced network and supervision
components can be set up to have the full picture in regards with the implementation of Flowspec as the main mitigation technique for the ISP’s security.

5.2 Future work

After considering the conclusion and the things that have to be improved in this thesis, we enumerate a few lines about the future work

- The proposed virtual environment has fulfilled the needs for a prototype. BGP Flow specifications have been sent from the NOC to the router. Traffic has been mitigated according to the flows. However, more tests need to be run to be sure of the scalability of the solution. This project has been designed as a POC and cannot be used in a production environment, yet.

- A survey with the customers of DGC needs to be conducted to understand if the ISP can accept Flowspec announcements from them. If they are willing to share their security with their internet provider and if DGC is prone to handle the architecture and hardware security measures of its clients, then BGP Flowspec can be implemented with eBGP.

- The security of BGP itself needs to be assessed. The Border Gateway Protocol is widely used between all ASes but is yet to be secured. Several pieces of research have been conducted to investigate ways to secure BGP.
Appendix

Appendix 1: Configuration of Junos vMX

Working with interfaces
The environment is composed of 4 Virtual PCs and 1 VM. To display the interfaces of connection of these components:

```
show interfaces terse ge*
```

Ge interfaces are emulated Gigabit Ethernet interfaces. The interfaces names displayed in the router’s CLI are not the same as in the network emulator interface (GNS3).

<table>
<thead>
<tr>
<th>Link</th>
<th>Juniper Interface</th>
<th>GNS3 Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vMX-VFP &lt;-&gt; Flowspec-RR</td>
<td>Ge-0/0/2</td>
<td>Eth4</td>
</tr>
<tr>
<td>vMX-VFP &lt;-&gt; PC-1</td>
<td>Ge-0/0/0</td>
<td>Eth2</td>
</tr>
<tr>
<td>vMX-VFP &lt;-&gt; PC-2</td>
<td>Ge-0/0/1</td>
<td>Eth3</td>
</tr>
<tr>
<td>vMX-VFP &lt;-&gt; PC-3</td>
<td>Ge-0/0/3</td>
<td>Eth5</td>
</tr>
<tr>
<td>vMX-VFP &lt;-&gt; PC-4</td>
<td>Ge-0/0/4</td>
<td>Eth6</td>
</tr>
</tbody>
</table>

Adding an interface
In case you want to add a component to the network and once you linked it to vMX-VFP, you need to add an interface. We will here take as example the configuration on PC-1.

```
set interfaces ge-0/0/0 unit 0 family inet address 172.16.0.1/24
```

In this example, we have configured the interface ge-0/0/0 to be linked to the IP address 172.16.0.1/24. Unit is the term to identify the logical interface within a physical interface. Junos allows the stacking of several logical interfaces in one physical interface. Unit 0 is the first logical interface. In our case, we will only use one logical interface per physical interface.
**Working with BGP**

BGP needs to be enabled to be able to use Flowspec as a rule dissemination protocol between the VM and the router. To display the BGP configuration:

```
show protocols
```

This command will display all protocols used in the routers.

The protocols used here are BGP and OSPF. The BGP protocol is configured for the communication between The VM and the router through the interface IP address 192.168.100.22. The type of connection is internal as they are both within the same Autonomous System (AS). The neighbor address is 192.168.100.133 (192.168.100.33 has been configured as a backup option for the VM but is not used in the current configuration). The two components accept direct routes to each other. This means that all routes exchanged between the router and the VM are accepted. The following command shows the accepted routes.

```
show routing-policy
```

The OSPF protocol is enabled for the loopback address.

The next command is used to display the router IP address and AS.

```
show routing-options
```

**Configuring BGP**

This part will explain the set of commands used when adding another component using BGP and linked to vMX. We will take as an example the configuration of a BGP interface of vMX linked to a BGP-using router under the same AS and with the IP address 192.168.100.10.

The first part of the configuration is to set up the interface. We will work with interface ge-0/0/5.

```
edit interface ge-0/0/5 unit 0
set description « your preferred description »
set family inet address 192.168.100.11
```

When the interface configuration is done, we can proceed to configuring BGP.

```
edit protocols bgp group internal-peers
```
Now we need to configure the policy that accepts routes

```
edit policy-options policy-statement send-direct term 2
set from protocol direct
set then accept
```

Lastly, we have to set router ID and AS (here already done)

```
edit policy-options policy-statement send-direct term 2
Set router-id 192.168.100.22
set autonomous-system 65000
```

**Working with Flowspec**

To be able to receive and apply Flowspec routes, we need to configure BGP on vMX to accept Flow specification Routes. The configured router shows the following configuration:

```
show protocols
```

As shown in the previous section (Working with BGP), the output of this command shows the enabled protocols. Here, we need to focus on 2 specific lines:

```
family inet {
    unicast;
    flow;
}
```

This means that the router only accepts unicast routes and flow routes.

To prevent the Routing Information Base (RIB) from overflooding, we will set a limit of advertised flow specification s. By running:
There is a limit of 1000 prefixes stored on the RIB. A warning is shown when the RIB reaches 50% of occupancy.

**Appendix 2: Presentation of the NOC**

The virtual NOC we used to test our environment is composed of:

- **GoBGP** a BGP daemon developed in Go and used to emulate BGP as an SDN. More info here [44]
- **Gabu** an open source user interface to manage GoBGP [45]

The user interface is as follows
It is meant to help the network administrator managing the rules deployed on the routers without using the CLI. It is developed in Qt. It provides all Flowspec options.
Appendix 3: Wireshark Frames

Wireshark capture of test1

Frame 15: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface 0
Border Gateway Protocol - UPDATE Message
  Marker: fffffffffffffffffffffffffffffffff
  Length: 69
  Type: UPDATE Message (2)
  Withdrawn Routes Length: 0
  Total Path Attribute Length: 46
Path attributes
  Path Attribute - ORIGIN: INCOMPLETE
    Flags: 0x40, Transitive, Well-known, Complete
    Type Code: ORIGIN (1)
    Length: 1
    Origin: INCOMPLETE (2)
  Path Attribute - AS_PATH: empty
    Flags: 0x40, Transitive, Well-known, Complete
    Type Code: AS_PATH (2)
    Length: 0
  Path Attribute - LOCAL_PREF: 100
    Flags: 0x40, Transitive, Well-known, Complete
    Type Code: LOCAL_PREF (5)
    Length: 4
    Local preference: 100
  Path Attribute - MP_REACH_NLRI
    Flags: 0x80, Optional, Non-transitive, Complete
    Type Code: MP_REACH_NLRI (14)
    Length: 18
    Address family identifier (AFI): IPv4 (1)
    Subsequent address family identifier (SAFI): Flow Spec Filter (133)
      Next hop network address (0 bytes)
      Number of Subnetwork points of attachment (SNPA): 0
      Network layer reachability information (13 bytes)
        FLOW_SPEC_NLRI (13 bytes)
        NRLI length: 12
        Filter: Destination prefix filter (172.17.0.2/32)
        Filter type: Destination prefix filter (1)
        172.17.0.2/32
Destination IP filter prefix length: 32
Destination IP filter: 172.17.0.2
Filter: Source prefix filter (172.16.0.2/32)
Filter type: Source prefix filter (2)
172.16.0.2/32
Source IP filter prefix length: 32
Source IP filter: 172.16.0.2
Path Attribute - EXTENDED_COMMUNITIES
Flags: 0xc0, Optional, Transitive, Complete
Type Code: EXTENDED_COMMUNITIES (16)
Length: 8
Carried extended communities: (1 community)
  Flow spec traffic-rate: ASN 0, 0.000 Mbps [Transitive Experimental]
    Type: Transitive Experimental (0x80)
      1... .... = IANA Authority: Allocated on First Come First Serve Basis
      .0... .... = Transitive across AS: Transitive
      Subtype (Experimental): Flow spec traffic-rate (0x06)
    2-Octet AS: 0
    Rate shaper: 0

Wiseshark capture of test2 (1/2)

Frame 16: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
Border Gateway Protocol - UPDATE Message
  Marker: fffffffffffffffffffffffffffffffff
  Length: 80
  Type: UPDATE Message (2)
  Withdrawn Routes Length: 0
  Total Path Attribute Length: 57
  Path attributes
    Path Attribute - ORIGIN: INCOMPLETE
    Path Attribute - AS_PATH: empty
    Path Attribute - LOCAL_PREF: 100
    Path Attribute - MP_REACH_NLRI
      Flags: 0x80, Optional, Non-transitive, Complete
Type Code: MP_REACH_NLRI (14)
Length: 29
Address family identifier (AFI): IPv4 (1)
Subsequent address family identifier (SAFI): Flow Spec Filter (133)
Next hop network address (0 bytes)
Number of Subnetwork points of attachment (SNPA): 0
Network layer reachability information (24 bytes)
FLOW_SPEC_NLRI (24 bytes)
  NRLI length: 23
    Filter: Destination prefix filter (172.17.0.2/32)
      Filter type: Destination prefix filter (1)
      172.17.0.2/32
      Destination IP filter prefix length: 32
      Destination IP filter: 172.17.0.2
    Filter: Source prefix filter (172.16.0.2/32)
      Filter type: Source prefix filter (2)
      172.16.0.2/32
    Filter: Protocol / Next Header filter (=6)
      Filter type: Protocol / Next Header filter (3)
      Operator flags: 0x81, end-of-list, Value length: 1 byte: 1 <<, equal
      Decimal value: 6
    Filter: Destination port filter (=2223)
      Filter type: Destination port filter (5)
      Operator flags: 0x91, end-of-list, Value length: 2 bytes: 1 <<, equal
      Decimal value: 2223
    Filter: Source port filter (=2222)
      Filter type: Source port filter (6)
      Operator flags: 0x91, end-of-list, Value length: 2 bytes: 1 <<, equal
      Decimal value: 2222
Path Attribute - EXTENDED_COMMUNITIES
Wireshark capture of test2 (2/2)

Frame 21: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
Border Gateway Protocol - UPDATE Message
  Marker: fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
  Length: 72
  Type: UPDATE Message (2)
  Withdrawn Routes Length: 0
  Total Path Attribute Length: 49
  Path attributes
    Path Attribute - ORIGIN: INCOMPLETE
    Path Attribute - AS_PATH: empty
    Path Attribute - LOCAL_PREF: 100
    Path Attribute - MP_REACH_NLRI
      Flags: 0x80, Optional, Non-transitive, Complete
      Type Code: MP_REACH_NLRI (14)
      Length: 21
      Address family identifier (AFI): IPv4 (1)
      Subsequent address family identifier (SAFI): Flow Spec Filter (133)
      Next hop network address (0 bytes)
      Number of Subnetwork points of attachment (SNPA): 0
      Network layer reachability information (16 bytes)
        FLOW_SPEC_NLRI (16 bytes)
        NRLI length: 15
        Filter: Destination prefix filter (172.18.0.2/32)
        Filter type: Destination prefix filter (1)
        172.18.0.2/32
        Destination IP filter prefix length: 32
        Destination IP filter: 172.18.0.2
        Filter: Source prefix filter (172.19.0.2/32)
        Filter type: Source prefix filter (2)
        172.19.0.2/32
        Source IP filter prefix length: 32
        Source IP filter: 172.19.0.2
        Filter: Protocol / Next Header filter (=17)
        Filter type: Protocol / Next Header filter (3)
Operator flags: 0x81, end-of-list, Value
length: 1 byte: 1 <=, equal
Decimal value: 17
Path Attribute - EXTENDED_COMMUNITIES
References:


