GARR customer triggered blackholing

Silvia d'Ambrosio, Nino Ciurleo

Introduction

From discussions with the GARR working group on "contrast to DDoS", we understood the importance of a collaboration between GARR and its users to mitigate attacks.
With the other components of the group, some open source tools for detecting DDoS and related reporting have been studied and tested. From these analyzes came the idea of developing a possible mitigation system to be implemented jointly with users. The solution found is simple to implement and does not provide for high economic expense. This mitigation system could be extended up to Géant network.

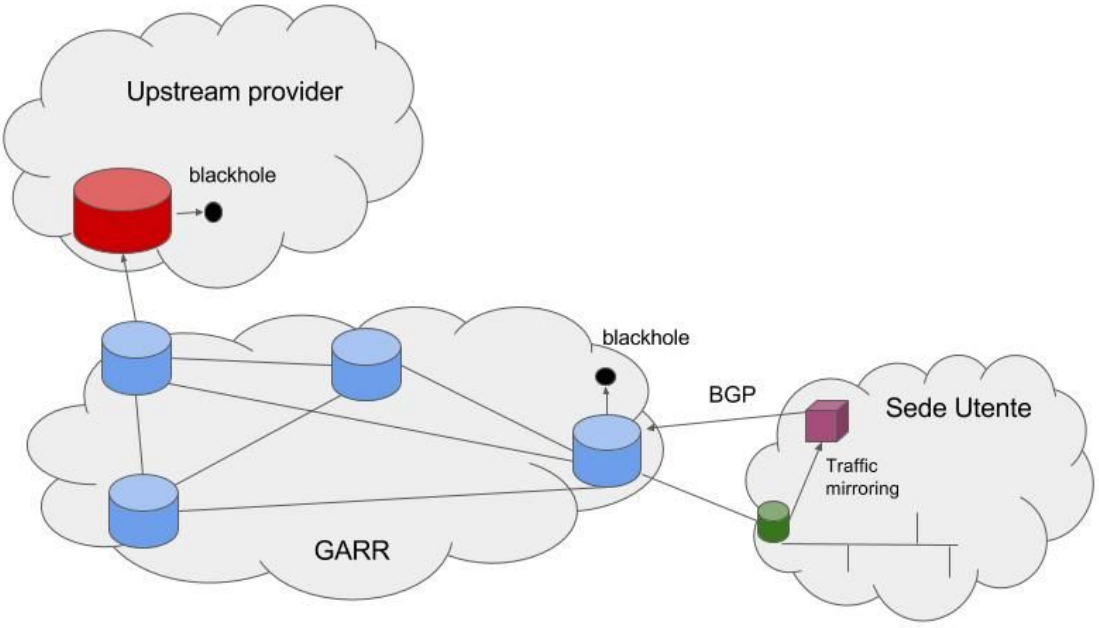
Goal

Allow GARR to offer a new type of "customer triggered blackholing" service to relieve attacks automatically and instantly, without explicit NOC intervention during the incident. By exploiting "blackhole" mechanisms, it avoids the saturation of network resources in case of DDoS attack and preserves overall connectivity. The filtering request, in fact, is handled directly by the user who assumes the responsibility of the addresses to be blocked.
Please note that this service has already been explicitly requested by some GARR users, including CINECA.

The main architecture is based on creating a new BGP session for the affected user, on which to receive "blackhole" announcements; such announcements would then be propagated to the upstream provider (Gèant too) and, if explicitly requested, on the rest of the backbone.
The APM of the user site may choose, at its discretion, whether manually configure the blackhole ad or use an automatic system. GARR side would be able to use only one service template regardless of the user-site approach.

The following is a detailed proposal of one of the possible realizable architectures, illustrating both the GARR side implementation and the possible automation of the user side system. This solution could be experienced with the GARR working group on "contrast to DDoS" and then proposed to the rest of the community as a case of use.

Architecture



GARR:
creating a BGP session between the GARR router and the device announcing the blackhole addresses (may be the same user's router) for sites that request to participate in the service. Policies configured for the new neighbor will only allow BGP announcements that meet the following features:

- prefixes included in the network range assigned to the user
- prefixes tagged with ad-hoc communities::
    - 137: 667 to activate the blackhole only on the upstream
    - 137: 666 to activate the black hole on the upstream and the GARR backbone

User site:
The user must generate announcements for the addresses he / she wants to activate the blackhole.
There are two ways to generate these announcements:

1) The apm configures manually, on its router or on the router that keeps the blackholing BGP session, announcing a BGP route for the prefixes to be black-holes.

2) Automatic generation of announcements from a dedicated machine.
3) The user router (green cylinder) performs mirroring of the IP traffic of the access link to a machine (purple box) capable of analyzing all the connection traffic to the GARR network, and automatically injecting the blackhole BGP routes over a threshold.

How it works

One of the possible solutions for traffic analysis and injection of black hole BGP routes is to use open source, free and free FastNetMon software for detecting attacks and exaBGP for injection of "blackhole" BGP routes. The hardware requirements are very limited, the machine on which it is to be installed can be a simple PC that, possibly equipped with a commercial network card, can analyze up to 10Gb / s traffic.

Studies have shown that Fastnetmon and exaBGP allow a high response rate to a DDoS attack. Being able to intervene automatically "in real time" also makes it possible to counteract even more recurring short-term volumetric attacks.

In fact, volumetric attacks aim at the saturation of a limited resource such as the bandwidth of a link or the number of packets / flows managed by network devices (routers, firewalls, nat, etc.). The APM is aware of not only the access bandwidth but also the details of the available resources of its site. Therefore, it is the APM itself that must configure the thresholds of the FastNetMon detection system appropriately.

In addition, the APM can properly identify the IP addresses to be included in the "whitelist" to inhibit reports for "licit" cases of volumetric traffic.

The working process of the system is as follows:

1. Traffic received on the user router is reflected to the FastNetMon machine
2. FastNetMon analyzes and classifies traffic based on the destination address
3. When a threshold value is exceeded to the same destination, a signal is generated
4. FastNetMon, via the exaBGP module, generates a blackhole BGP ad on peering with the GARR router
5. FastNetMon, tramite il modulo exaBGP, genera un annuncio BGP di “blackhole” sul peering con il router GARR
6. The GARR router propagates the "blackhole" announcement to the upstream provider and other network routers, based on the community set up.
7. FastenMon, upon expiration of a timer, removes the "blackhole" and verified the persistence of the attack.

It is also advisable to implement "blackhole" address monitoring system in such a way that this list is integrated into GINS (GARR Integrated Networking Suite), including time guidance on filtering. The information should be detected directly by the devices to be always aligned with the network configuration.

Real case

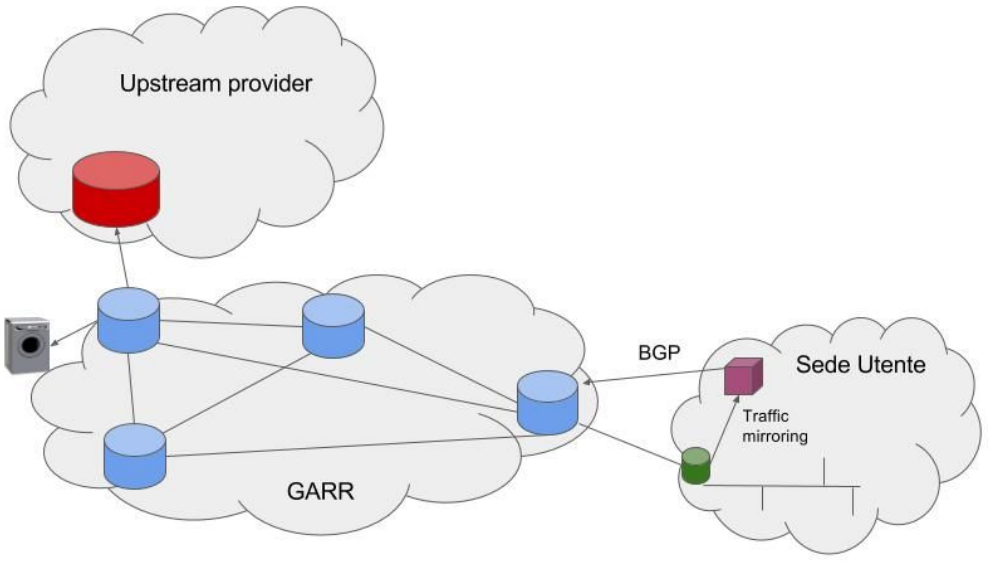
A laboratory with Marco Pirovano, APM of the "Bocconi" University of Milan, was implemented, where a server with a 10Gb / s network adapter was prepared and equipped with FastNetMon software. During the trial period a DDoS UDP flood attack was reported. In the appendix some details extracted from FastNetMon.

As noted by APM, in evaluating the threshold configuration, it is to be noted that the "bottleneck" has on the firewall installed downstream of the user router.

Future developments

- One possible extension of this service is the application of specific filterspec for blocking only attack traffic, avoiding the total isolation (with the "blackhole") of the attached machine.

- Another possible evolution might consider shifting traffic to a hypothetical scrubbing center installed in the GARR network or in Géant network.



- FastNetMon is also able to analyze traffic statistics exported with Netflow. It would be possible to develop a specific analysis system for small users directly managed by GARR, releasing the APM from the burden of managing a FastNetMon machine

Appendix

90.147.71.26_10_03_17_18:46:13
IP: 90.147.71.26
Attack type: udp_flood
Initial attack power: 134450 packets per second
Peak attack power: 134450 packets per second
Attack direction: incoming
Attack protocol: udp
Total incoming traffic: 477 mbps
Total outgoing traffic: 0 mbps
Total incoming pps: 134450 packets per second
Total outgoing pps: 0 packets per second
Total incoming flows: 0 flows per second
Total outgoing flows: 0 flows per second
Average incoming traffic: 477 mbps

Average outgoing traffic: 0 mbps
Average incoming pps: 134450 packets per second
Average outgoing pps: 0 packets per second
Average incoming flows: 0 flows per second
Average outgoing flows: 0 flows per second
Incoming ip fragmented traffic: 0 mbps
Outgoing ip fragmented traffic: 0 mbps
Incoming ip fragmented pps: 0 packets per second
Outgoing ip fragmented pps: 0 packets per second
Incoming tcp traffic: 0 mbps
Outgoing tcp traffic: 0 mbps
Incoming tcp pps: 0 packets per second
Outgoing tcp pps: 0 packets per second
Incoming syn tcp traffic: 0 mbps
Outgoing syn tcp traffic: 0 mbps
Incoming syn tcp pps: 0 packets per second
Outgoing syn tcp pps: 0 packets per second
Incoming udp traffic: 477 mbps
Outgoing udp traffic: 0 mbps
Incoming udp pps: 133176 packets per second
Outgoing udp pps: 0 packets per second
Incoming icmp traffic: 0 mbps
Outgoing icmp traffic: 0 mbps
Incoming icmp pps: 1273 packets per second
Outgoing icmp pps: 0 packets per second

Network: 90.147.71.0/24
Network incoming traffic: 2434 mbps
Network outgoing traffic: 0 mbps
Network incoming pps: 685079 packets per second
Network outgoing pps: 0 packets per second
Average network incoming traffic: 129 mbps
Average network outgoing traffic: 0 mbps
Average network incoming pps: 36466 packets per second
Average network outgoing pps: 0 packets per second
Average packet size for incoming traffic: 465.8 bytes
Average packet size for outgoing traffic: 0.0 bytes

2017-03-10 18:46:14.849727 24.242.80.18:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 52 sample ratio: 1
2017-03-10 18:46:14.849750 89.87.168.194:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 52 sample ratio: 1
2017-03-10 18:46:14.849766 216.184.74.9:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 57 sample ratio: 1
2017-03-10 18:46:14.849781 125.45.23.154:123 > 90.147.71.26:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 36 sample ratio: 1
2017-03-10 18:46:14.849796 114.34.196.78:0 > 90.147.71.26:0 protocol: icmp frag: 0 packets: 1 size: 70 bytes ttl: 243 sample ratio: 1
2017-03-10 18:46:14.849811 88.248.134.90:123 > 90.147.71.26:39177 protocol: udp frag: 0 packets: 1 size: 410 bytes ttl: 42 sample ratio: 1
2017-03-10 18:46:14.849826 194.85.80.51:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets:

1 size: 482 bytes ttl: 48 sample ratio: 1
2017-03-10 18:46:14.849841 80.95.184.130:123 > 90.147.71.26:39177 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 45 sample ratio: 1
2017-03-10 18:46:14.849855 183.234.216.18:123 > 90.147.71.26:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 43 sample ratio: 1
2017-03-10 18:46:14.849870 183.234.216.18:123 > 90.147.71.26:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 43 sample ratio: 1
2017-03-10 18:46:14.849885 85.131.152.210:123 > 90.147.71.26:39177 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 50 sample ratio: 1
2017-03-10 18:46:14.849900 65.116.97.190:123 > 90.147.71.26:39177 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 45 sample ratio: 1
2017-03-10 18:46:14.849915 125.45.23.154:123 > 90.147.71.26:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 36 sample ratio: 1
2017-03-10 18:46:14.849929 80.95.184.130:123 > 90.147.71.26:39177 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 45 sample ratio: 1
2017-03-10 18:46:14.849944 124.65.105.90:123 > 90.147.71.26:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 36 sample ratio: 1
2017-03-10 18:46:14.849959 128.241.3.69:123 > 90.147.71.26:39177 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 45 sample ratio: 1
2017-03-10 18:46:14.849973 124.65.105.90:123 > 90.147.71.26:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 36 sample ratio: 1
2017-03-10 18:46:14.849988 86.124.71.47:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 46 sample ratio: 1
2017-03-10 18:46:14.850002 194.85.80.51:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 48 sample ratio: 1
2017-03-10 18:46:14.850017 86.124.71.47:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 46 sample ratio: 1
2017-03-10 18:46:14.850031 193.165.53.102:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 48 sample ratio: 1
2017-03-10 18:46:14.850046 78.189.206.104:123 > 90.147.71.26:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 41 sample ratio: 1
2017-03-10 18:46:14.850062 119.53.0.106:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 36 sample ratio: 1
2017-03-10 18:46:14.850077 86.124.71.47:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 46 sample ratio: 1
2017-03-10 18:46:14.850091 86.124.71.47:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 46 sample ratio: 1
2017-03-10 18:46:14.850105 119.53.0.106:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 36 sample ratio: 1
2017-03-10 18:46:14.850120 119.53.0.106:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 36 sample ratio: 1
2017-03-10 18:46:14.850134 183.234.216.18:123 > 90.147.71.26:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 43 sample ratio: 1
2017-03-10 18:46:14.850149 132.248.47.212:123 > 90.147.71.26:22100 protocol: udp frag: 0 packets: 1 size: 194 bytes ttl: 44 sample ratio: 1
2017-03-10 18:46:14.850163 183.234.216.18:123 > 90.147.71.26:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 43 sample ratio: 1
2017-03-10 18:46:14.850178 49.255.252.205:123 > 90.147.71.26:39177 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 51 sample ratio: 1
2017-03-10 18:46:14.850192 80.95.184.130:123 > 90.147.71.26:39177 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 45 sample ratio: 1

2017-03-10 18:46:14.850207 216.184.74.9:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 57 sample ratio: 1
2017-03-10 18:46:14.850221 118.98.75.93:123 > 90.147.71.26:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 47 sample ratio: 1
2017-03-10 18:46:14.850236 24.242.80.18:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 338 bytes ttl: 52 sample ratio: 1
2017-03-10 18:46:14.850250 89.111.180.151:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 55 sample ratio: 1
2017-03-10 18:46:14.850265 193.165.53.102:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 48 sample ratio: 1
2017-03-10 18:46:14.850279 193.165.53.102:123 > 90.147.71.26:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 48 sample ratio: 1
2017-03-10 18:46:14.850294 95.6.71.113:123 > 90.147.71.26:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 42 sample ratio: 1
2017-03-10 18:46:14.850308 101.127.169.94:0 > 90.147.71.26:0 protocol: icmp frag: 0 packets: 1 size: 70 bytes ttl: 245 sample ratio: 1

[78:19:F7:5B:30:01 -> 00:04:96:8F:B0:45] [IPv4][24.242.80.18:123 -> 90.147.71.26:40992] [l3_proto=UDP][ip_fragmented: 0][hash=0][tos=0][tcp_seq_num=0] [caplen=482][len=482][parsed_header_len=0][eth_offset=0][l3_offset=14][l4_offset=34][payload_offset=42]
protocol: NTP master_protocol: Unknown