Distributed Denial of Service Attacks

Detection and Mitigation

European MUM – 2016

Ljubljana / Slovenia

Wardner Maia

Introduction

Wardner Maia

Electronic and Telecommunications Engineer;
Internet Service Provider since 1995;
Training Business since 2002;
Certified Mikrotik Trainer since 2007;
MD Brasil IT & Telecom CTO;
Member of the board of directors of LACNIC.

Introduction

MD Brasil IT & Telecom

Internet Access Provider in São Paulo state - Brazil;
Telecom equipment manufacturer and integrator;
Mikrotik Training Center since 2007;
Consulting services worldwide.

http://mdbrasil.com.br http://mikrotikbrasil.com.br

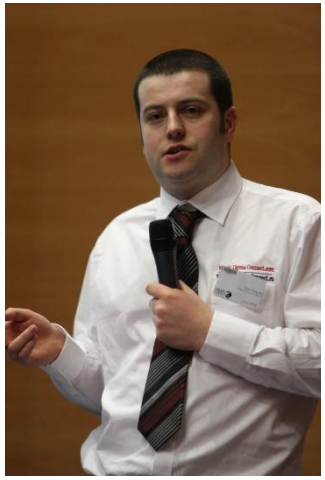
Previous Participations on European MUMs

Wireless Security (2008 – Krakow/PL)
Wireless Security for OLPC project (2009 – Prague/CZ)
Layer 2 Security (2010 – Wroclaw/PL)
Routing Security (2011 – Budapest/HU)
IPv6 Security (2012 - Warsaw/PL)
BGP Filtering (2013 – Zagreb/CR)
MPLS VPNs Security (2014 – Venice/IT)
Network Simulation (2015 – Prague/CZ)

Today: DDoS attacks – detection and mitigation

http://mikrotikbrasil.com.br/artigos

DDoS attacks



Last year our good friend Tom Smyth (Wireless Connect – Ireland) did a great presentation about DDoS.

http://mum.mikrotik.com/2015/CZ/info

There is a lot of useful information on that work:

Concepts about DDoS, BCP 38, UrPF, how to reduce the surface of attacks blackholing unused space, etc, etc,

Definitely get that presentation and do your Homework!

DDoS – Detection and Mitigation

Why (again) this subject?

DDoS – Should I care?

https://www.linkedin.com/pulse/2016-year-3000-gbps-ddos-attack-tech2016-marcos-ortiz-valmaseda?trk=pulse_spock-articles

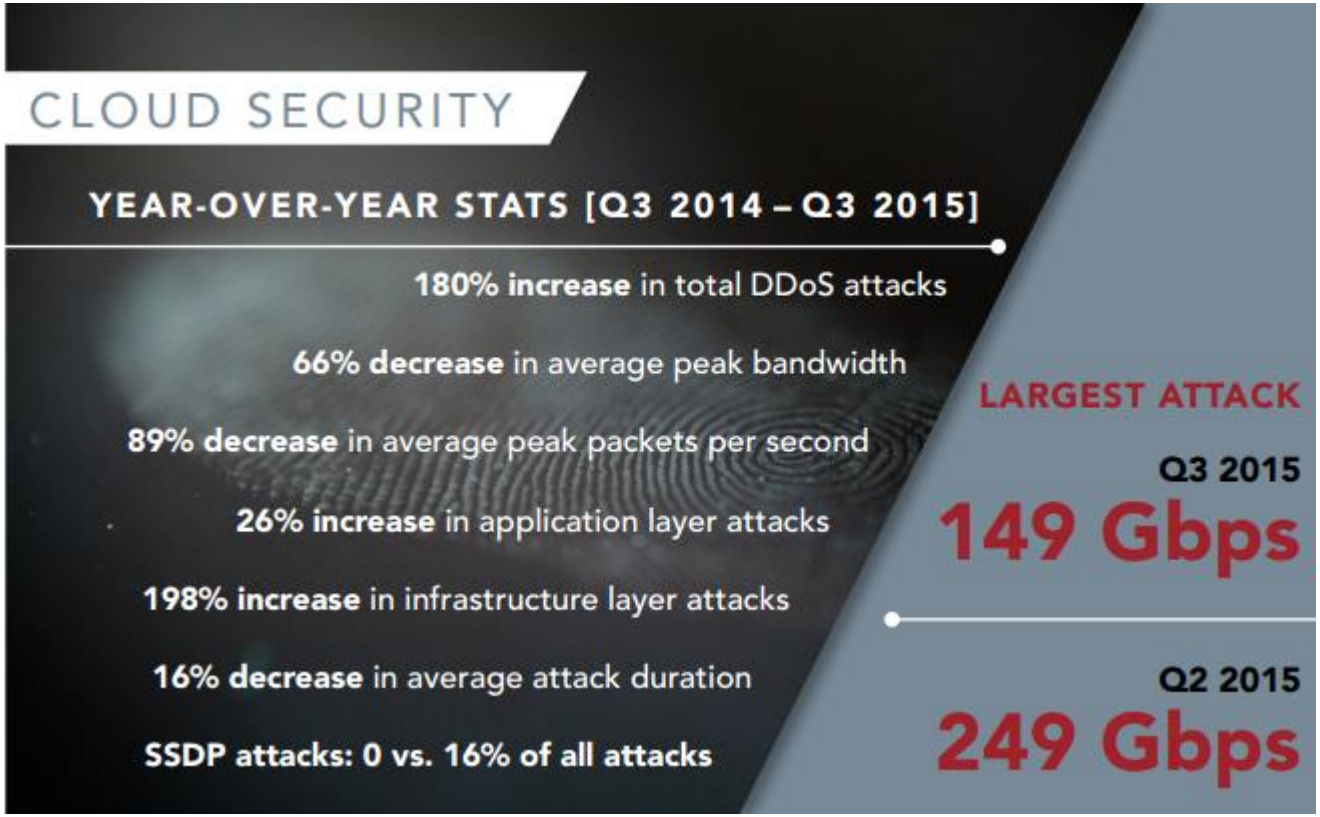
We have to be prepared for bigger and bigger attacks

md brasil
TI&TELECOM

Is DDoS a “privilege” of Big Operators and Data Centers?

Could my (small/medium) company be a target?

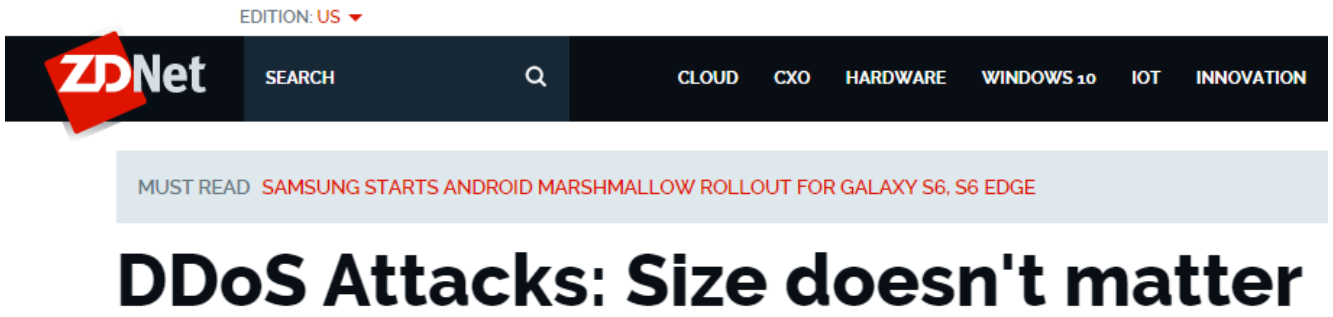
DDoS – Should I Care?



https://www.stateoftheinternet.com/downloads/pdfs/Q3-2015-SOTI-Connectivity-Executive-Summary.pdf

DDoS – Should I Care?

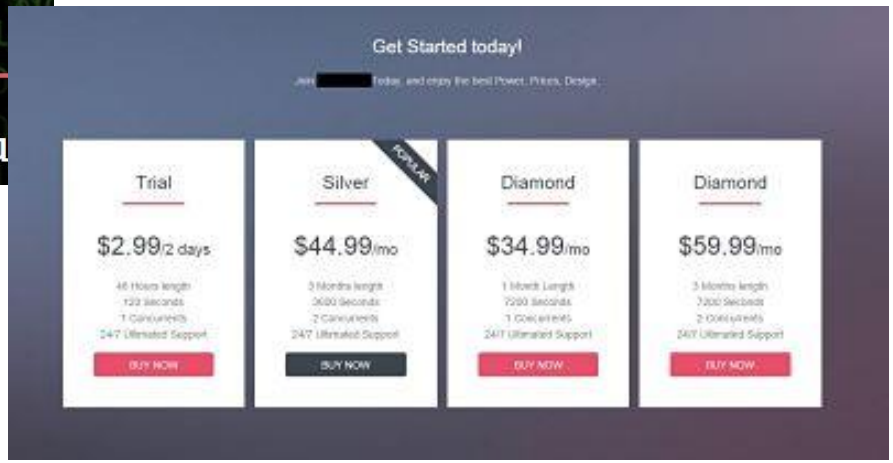
http://www.pcworld.com/article/3012963/security/ddos-attacks-increase-in-number-endanger-small-organizations.html



http://www.zdnet.com/article/ddos-attacks-size-doesnt-matter/

DDoS – Should I Care?

How about to hire a DDoS attack, for US$ 2.99?



DDoS – Should I Care?

Being a target of a DDoS attack is not a matter of "if" but "when" it will happen.

Do you have a formal Incident Response Plan?

DDoS – Detection and Mitigation

Whom this presentation is intended for?

Target Audience and Presentation Goals

This presentation is targeted to small an medium ISPs, mainly in the business of Last mile Internet Access;

The main goals of this presentation are: to show that it's important to have a plan to deal with DDoS and a suggestion on how to implement it.

- A real case scenario implementation will be showed;

- We'll try to fit the presentation in the 45 minutes we have.

Agenda

Background on DDoS – components and architecture and mitigation techniques;

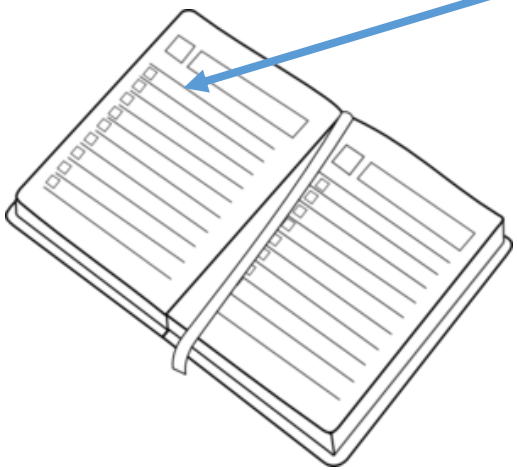
Tools used for Detection and Mitigation in an ISP environment;

Hands On! Seeing things working;

The Cherry of the Cake – Cool Graphics and information about your network;

6’

Agenda



Background on DDoS – components and architecture and mitigation techniques;

Tools used for Detection and Mitigation in an ISP environment;

Hands On! Seeing things working;

The Cherry of the Cake – Cool Graphics and information about your network;

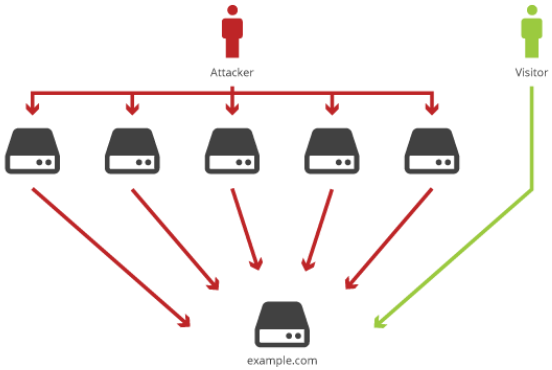
6’

Background on DDoS
Basic concepts

Dos Types

DoS

Denial of Service Attack



DDoS

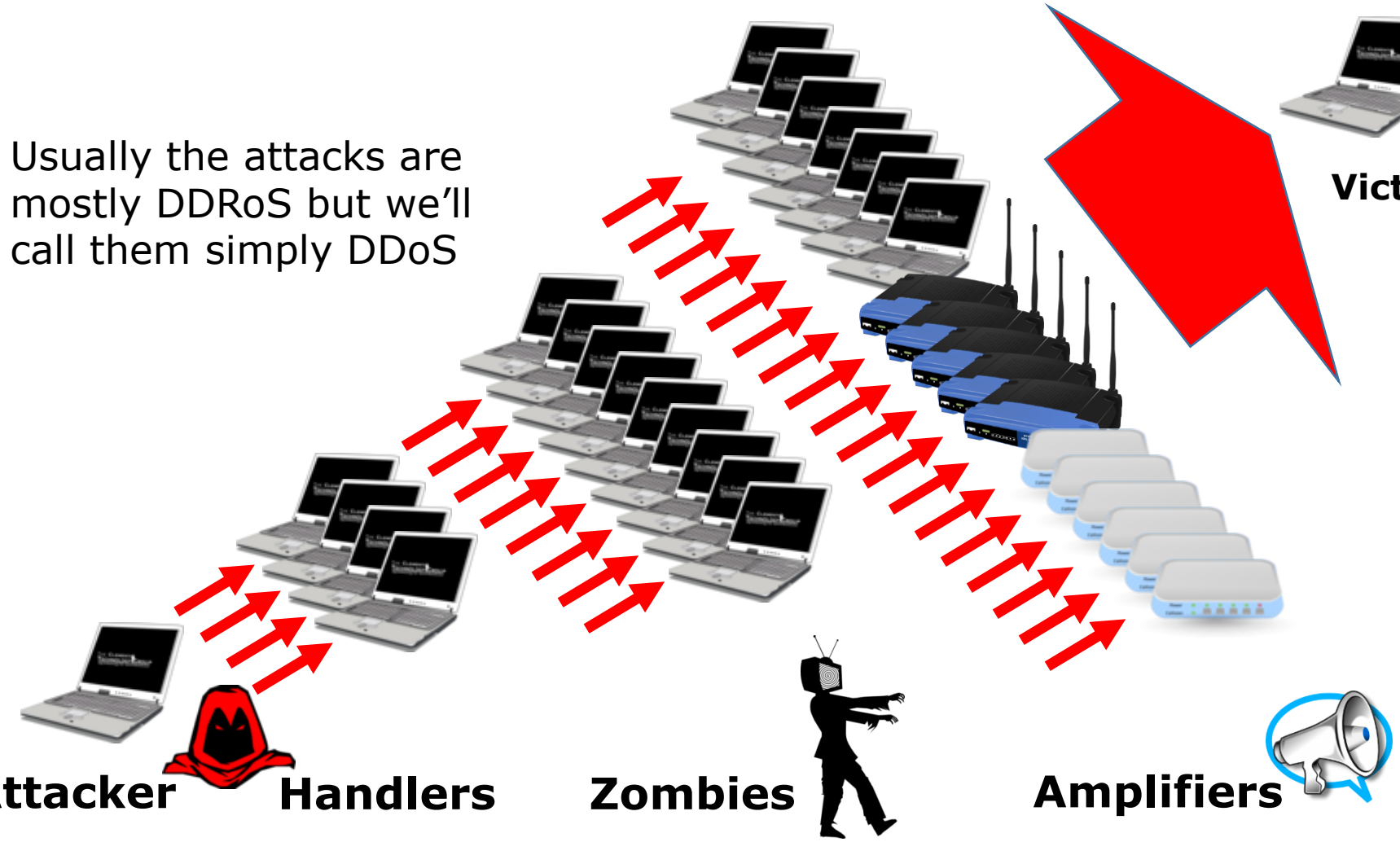
Distributed Denial of Service Attack

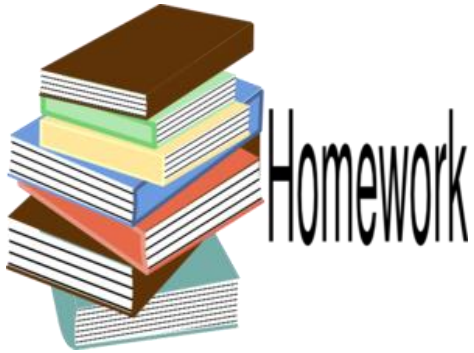
DRDoS

Distributed Reflected Denial of Service Attack

Anatomy of a DRDoS attack

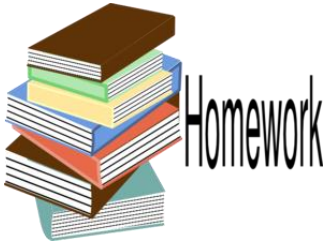
Usually the attacks are mostly DDRoS but we'll call them simply DDoS





How to fight against DDoS?

Prevention



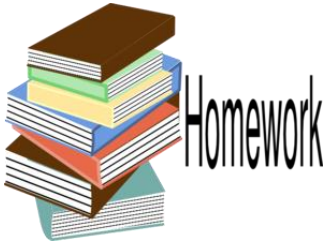
Doing our homework

→ Implement BCP-38 (RFC 2827), by firewall rules and uRPF (mostly you'll do a good job for the rest of the world);

→ Find and fix the amplifiers (DNS, SSDP, NTP, SNMP, NETBIOS) on your network (Extra Slides at the end of this presentation have the commands to do it);

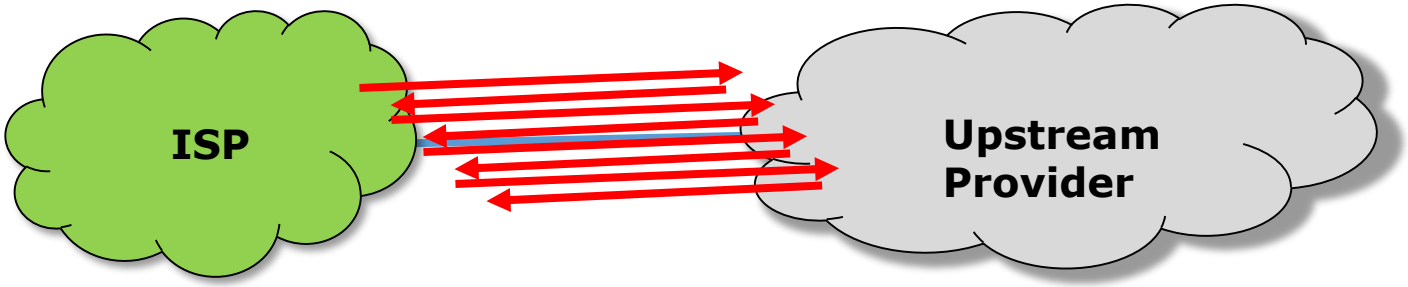
→ Subscribe to Team Cymru Bogons Service and automatically black-hole Bogons Prefixes

Prevention



Doing our homework

→ Ensure that all your space announced to eBGP have internal routes to your network, avoiding **static loops;**

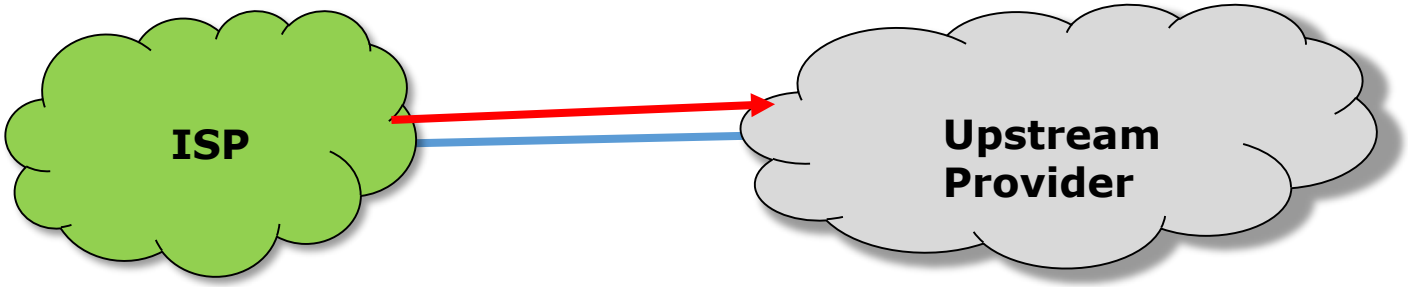


One single 64 bytes ping with TTL = 250, will generate 2 mbps of traffic ☹

Prevention

Doing our homework

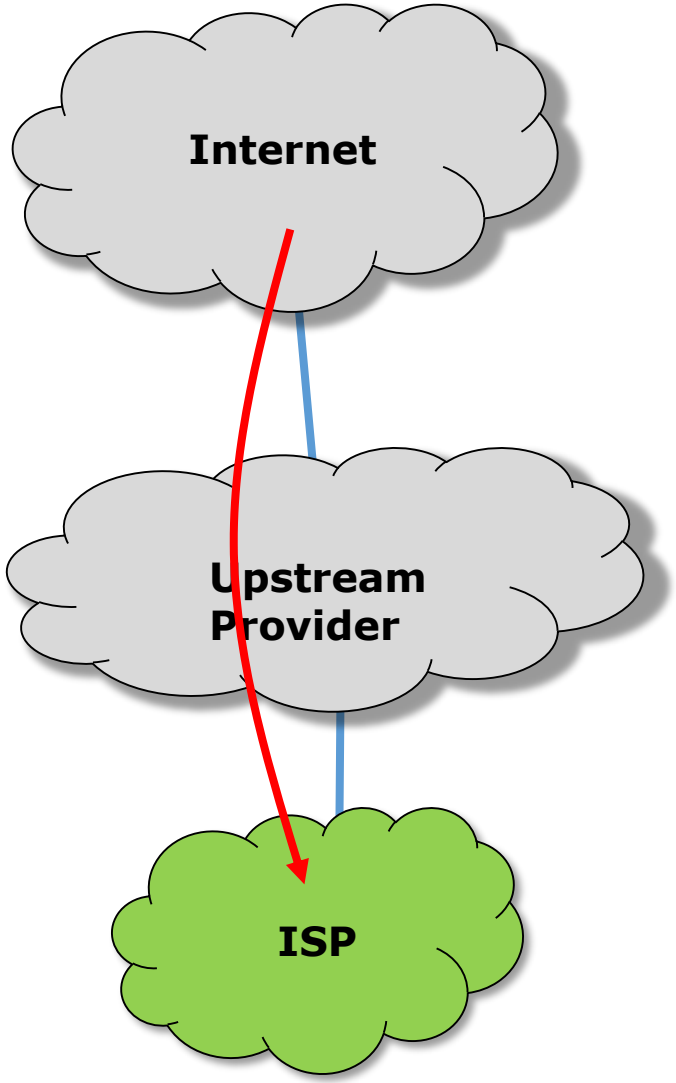
→ Reduce your exposition to DDoS announcing your unused space as black-hole (See Tom's hints for that)



NB: Depends on your Upstream Provider's policy

Mitigation Techniques

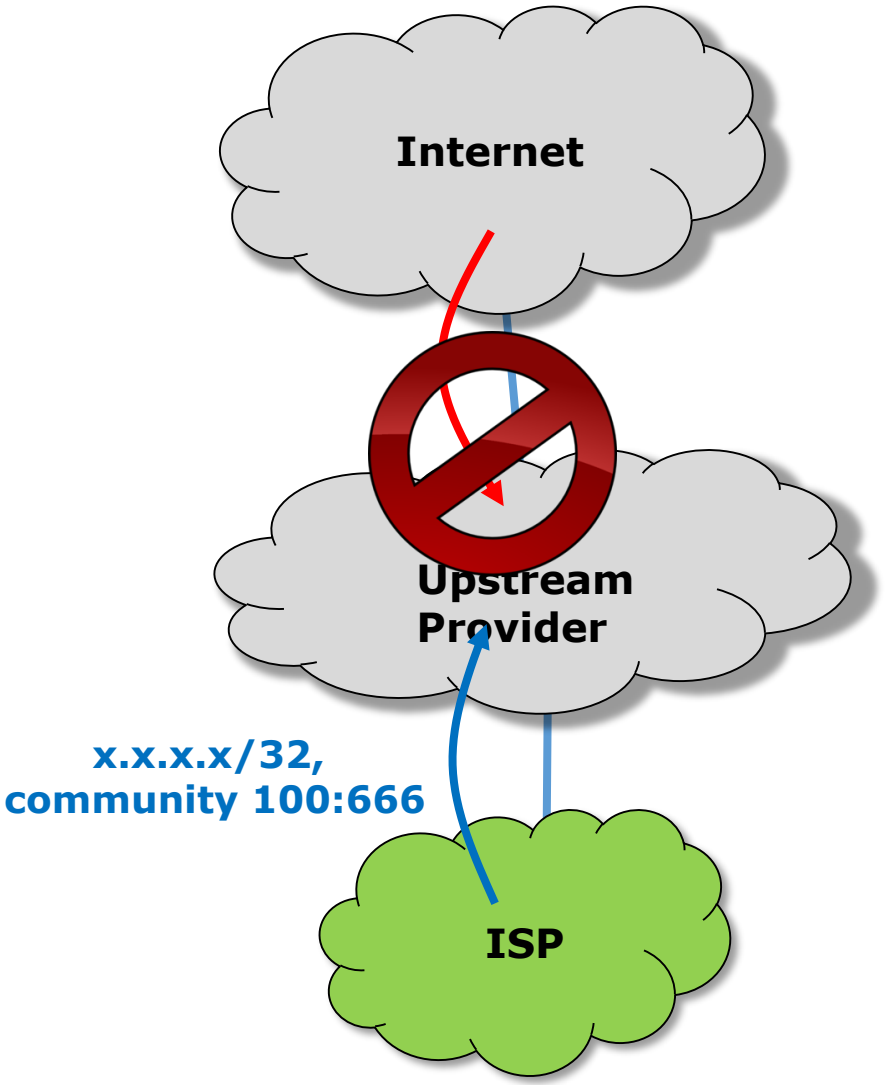
Remote Triggered Blackhole



ISP is suffering a DDoS attack targeting IP x.x.x.x/32;

Upstream provider (e.g. AS 100) provides a policy that black-hole any /32 announcement with a specific community (e.g. 100:666);

Remote Triggered Blackhole



ISP announces to the Upstream provider the /32 with the community;

Upstream provider put the /32 in blackhole;

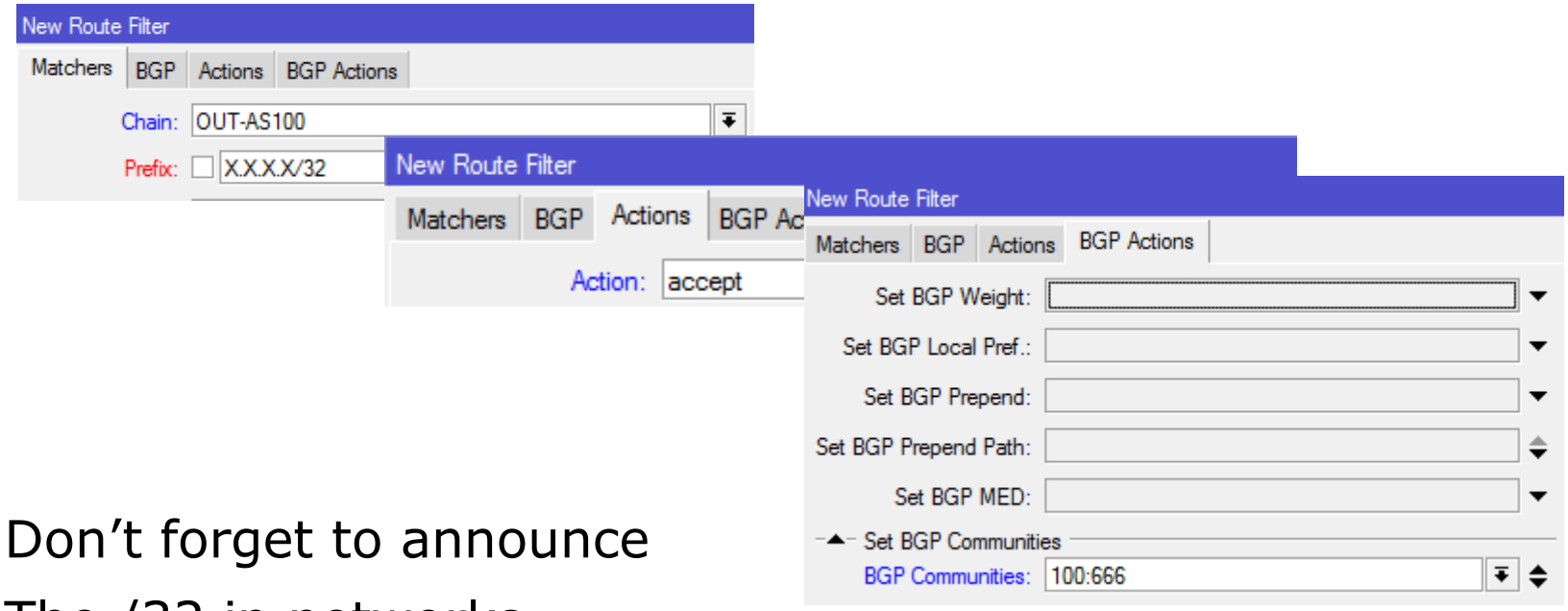
Communication with /32 is lost and channel overflow stops;

Other customer's SLA is saved, but unfortunately we can say that DDoS succeeded ☹

DDoS
Mitigation Techniques

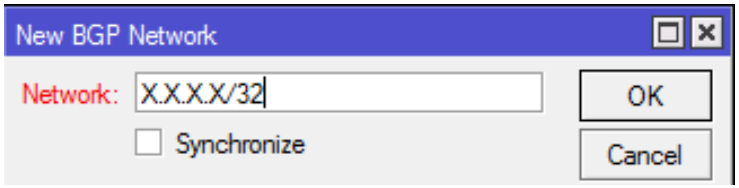
Implementation on RouterOS:

Make the filter:

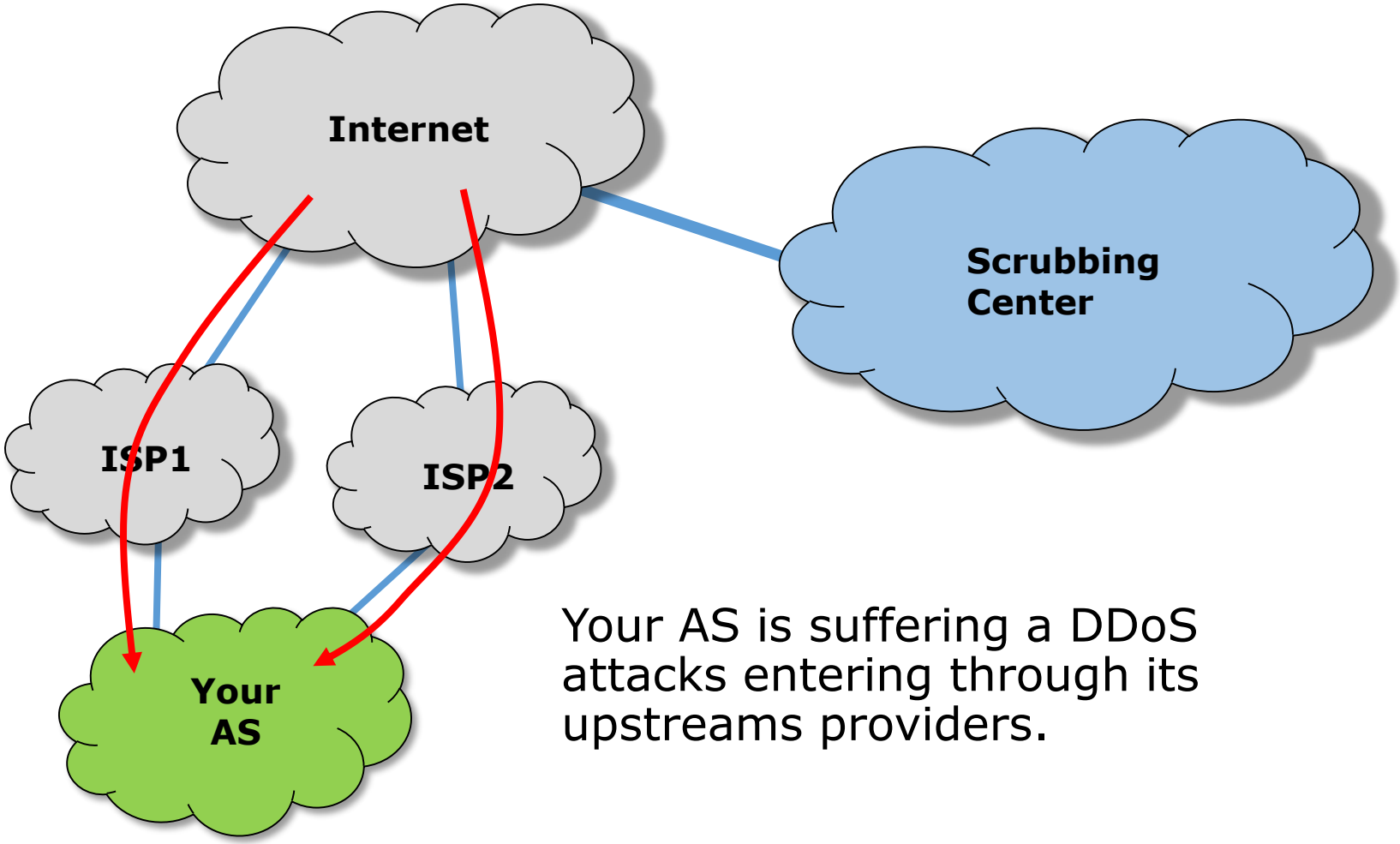


Don’t forget to announce

The /32 in networks

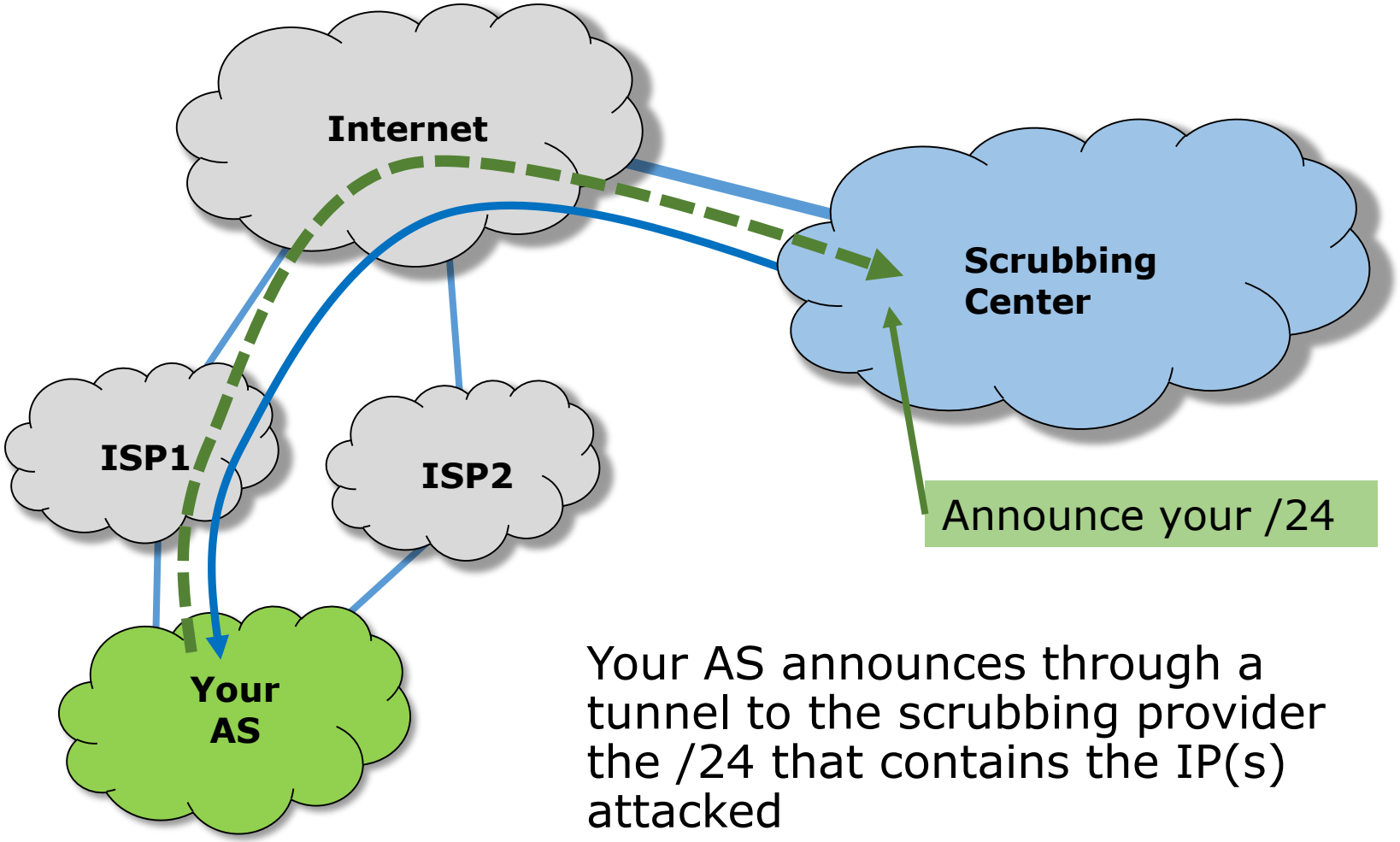


Mitigation On the Cloud



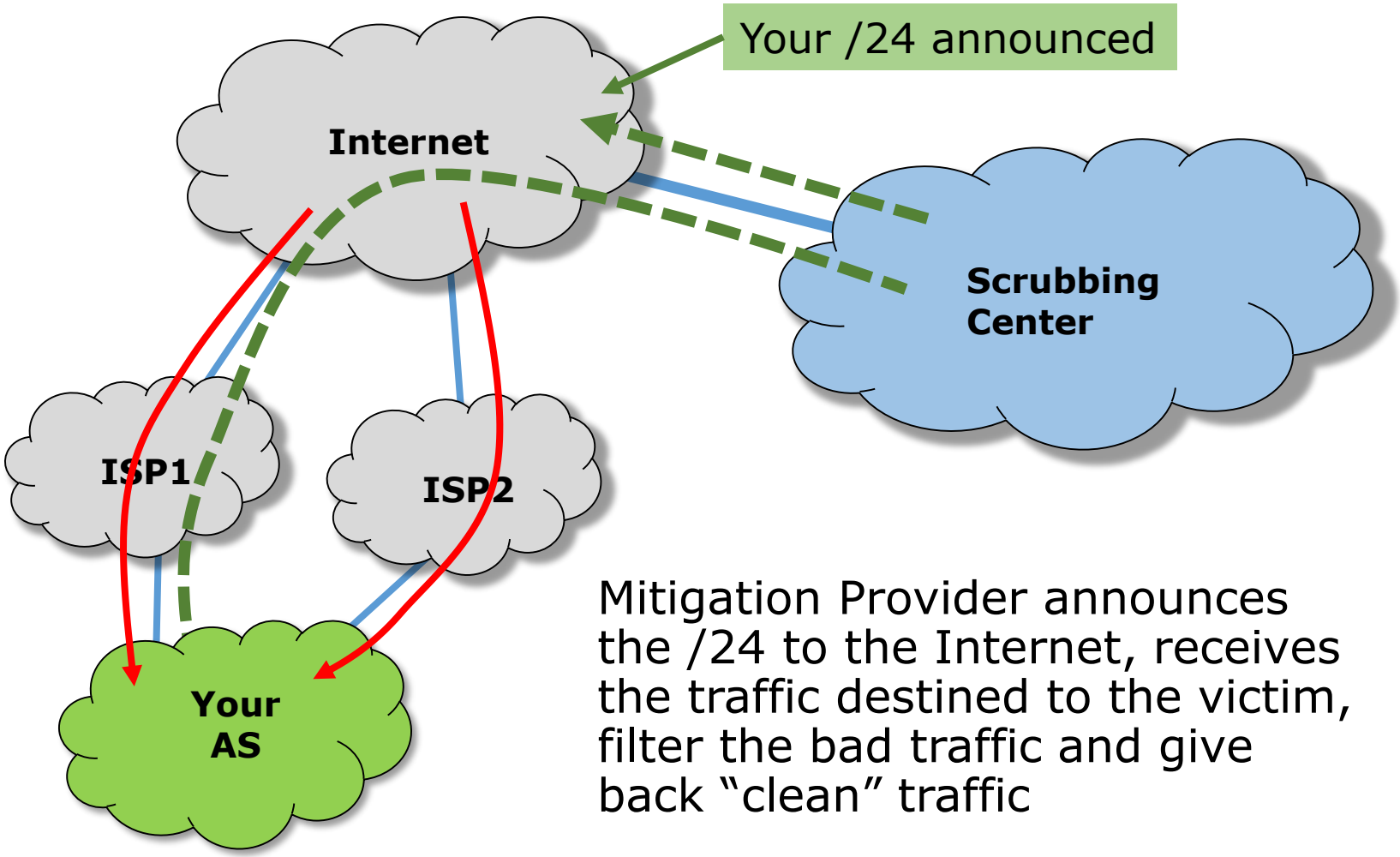
Your AS is suffering a DDoS attacks entering through its upstreams providers.

Mitigation On the Cloud



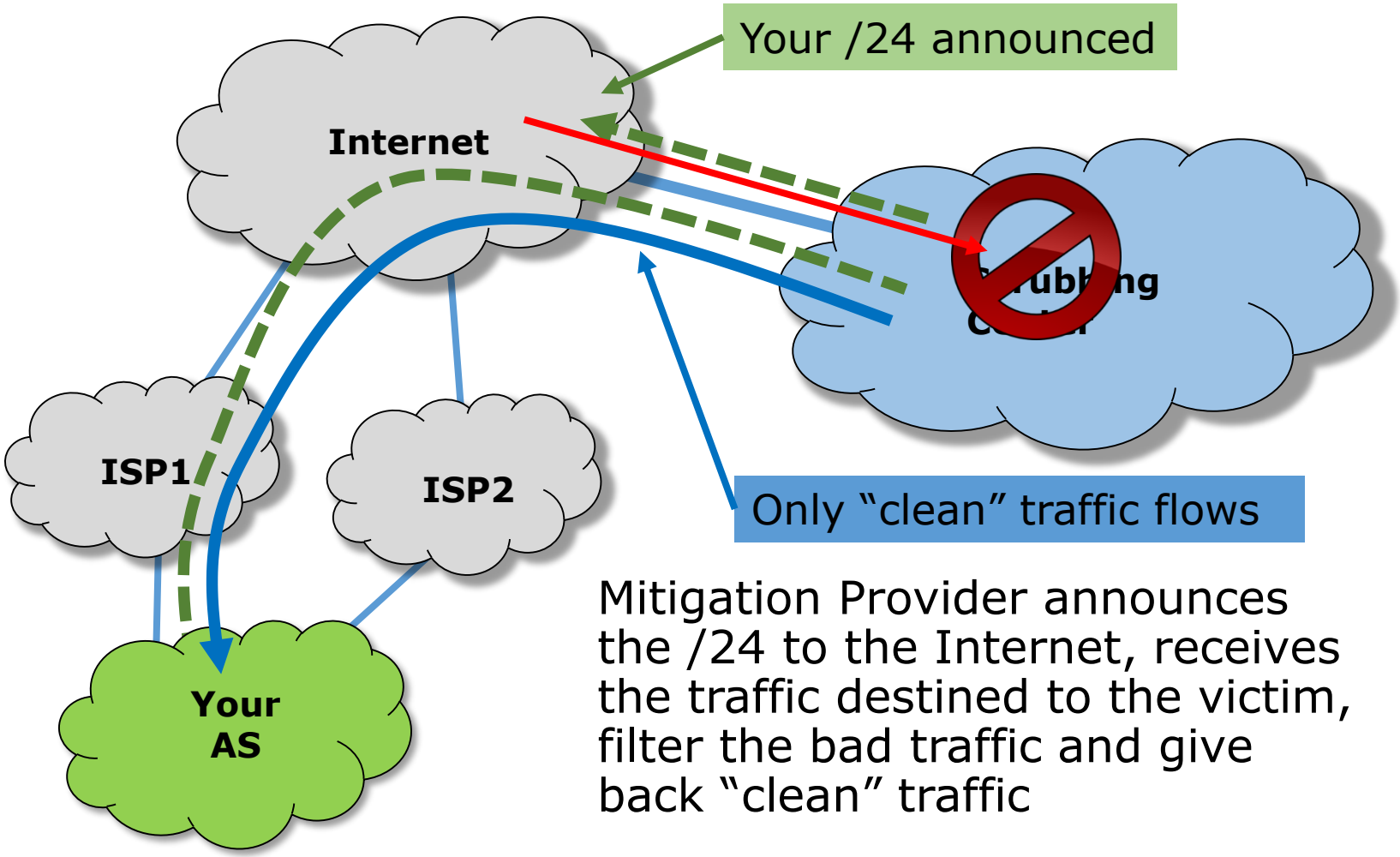
Your AS announces through a tunnel to the scrubbing provider the /24 that contains the IP(s) attacked

Mitigation On the Cloud



Mitigation Provider announces the /24 to the Internet, receives the traffic destined to the victim, filter the bad traffic and give back “clean” traffic

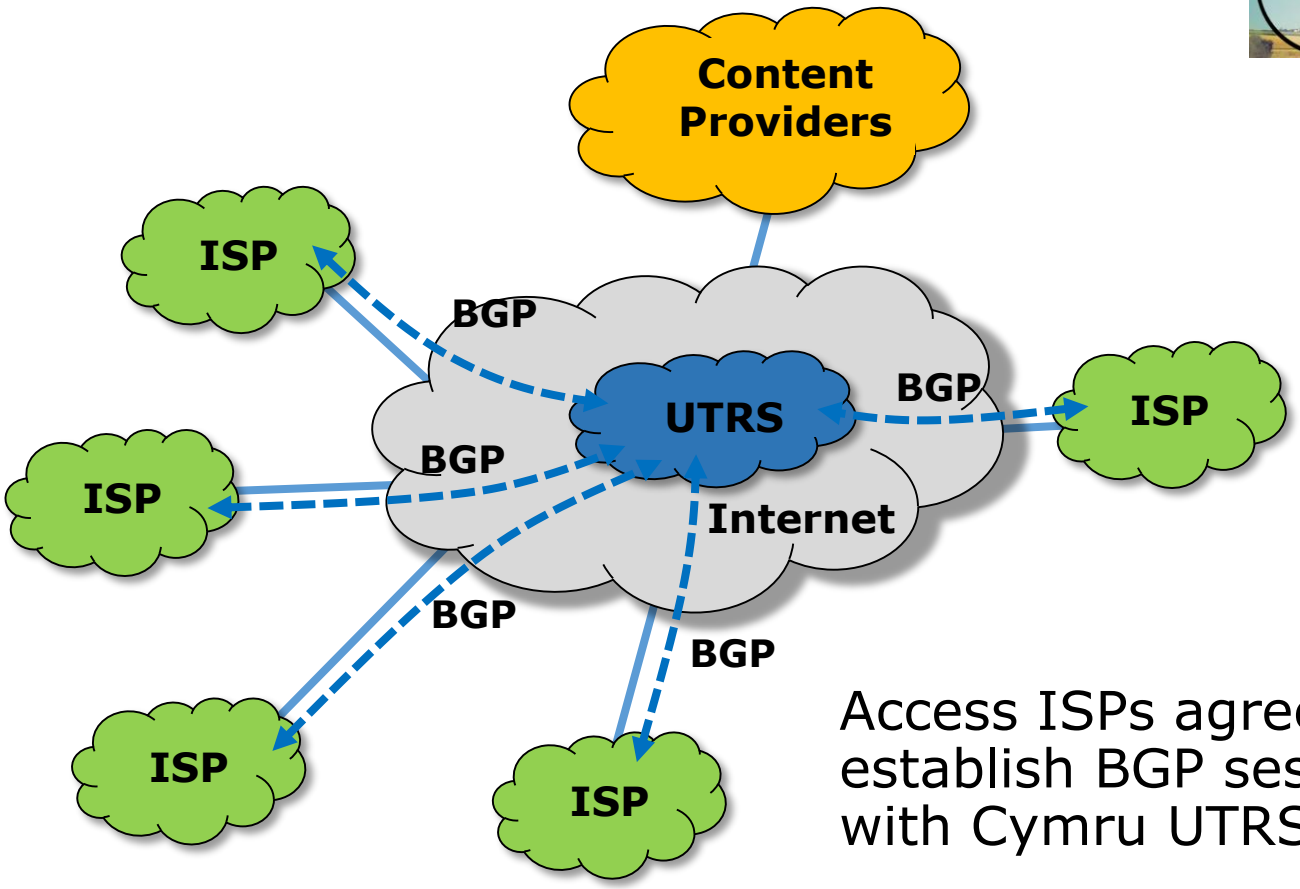
Mitigation On the Cloud



Mitigation Provider announces the /24 to the Internet, receives the traffic destined to the victim, filter the bad traffic and give back “clean” traffic

Cymru - UTRS

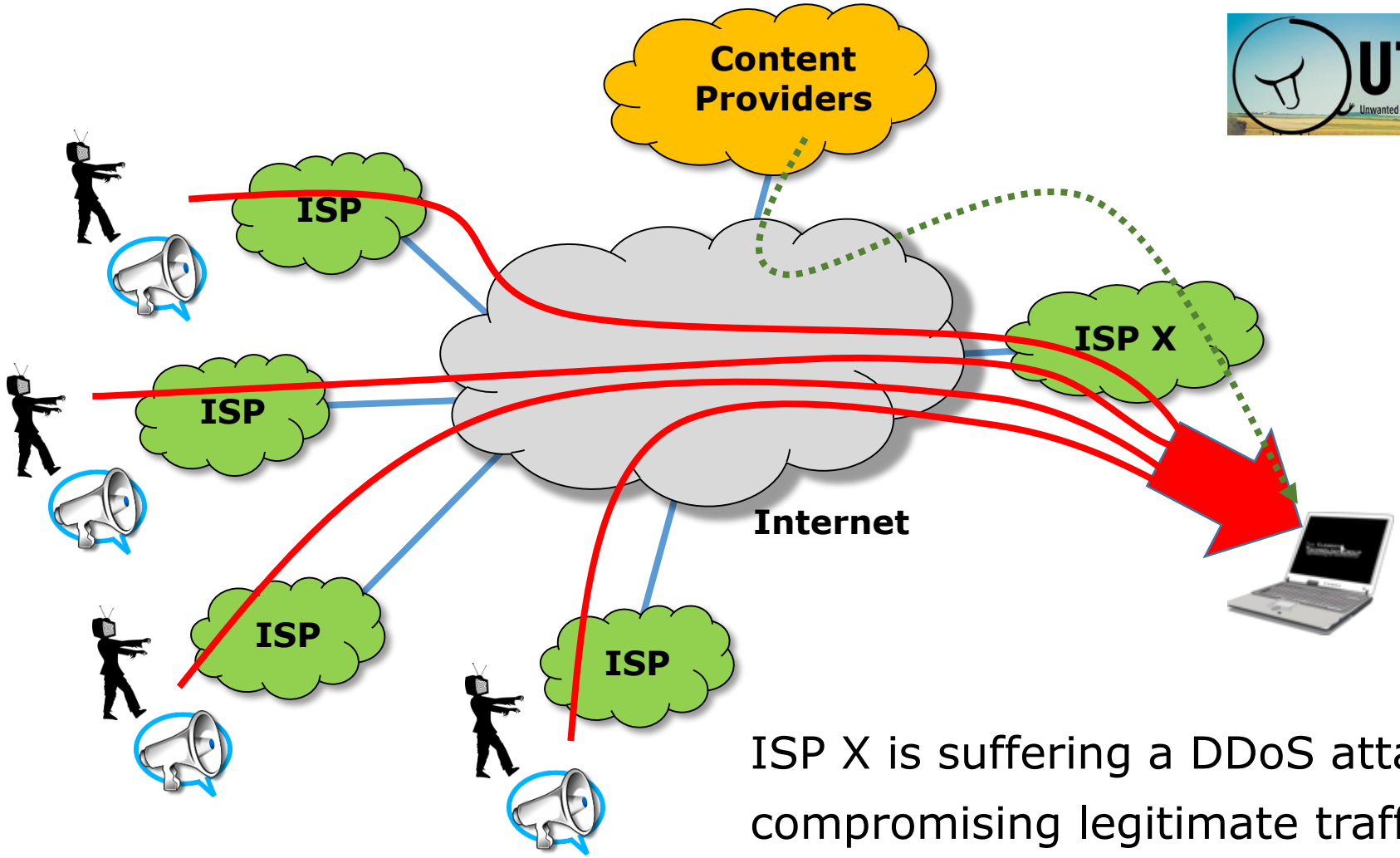
UTRS – Unwanted Traffic Removal



Access ISPs agree to establish BGP sessions with Cymru UTRS service

http://www.team-cymru.org/UTRS/

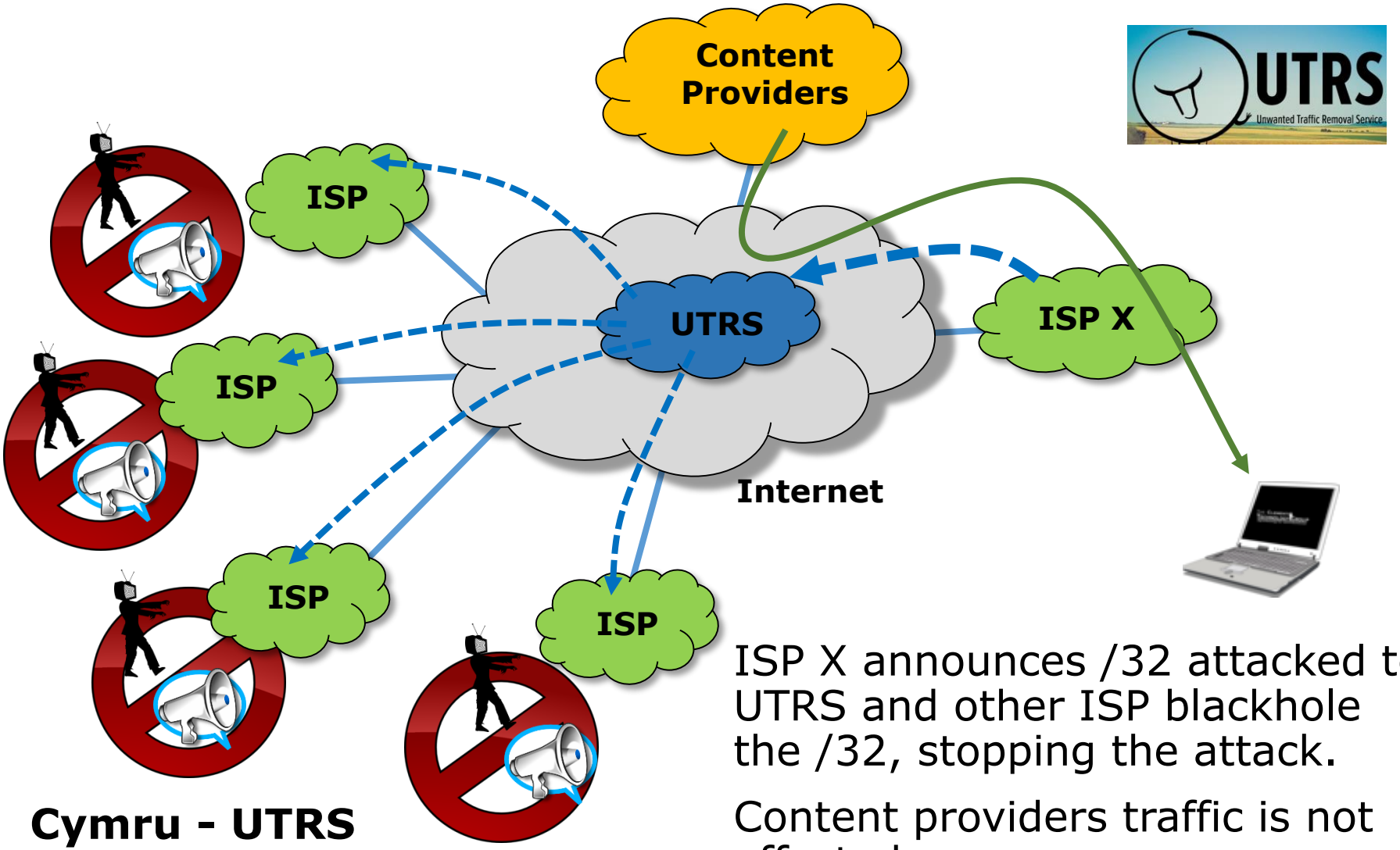
Cymru - UTRS



ISP X is suffering a DDoS attack compromising legitimate traffic

Cymru - UTRS

Cymru - UTRS



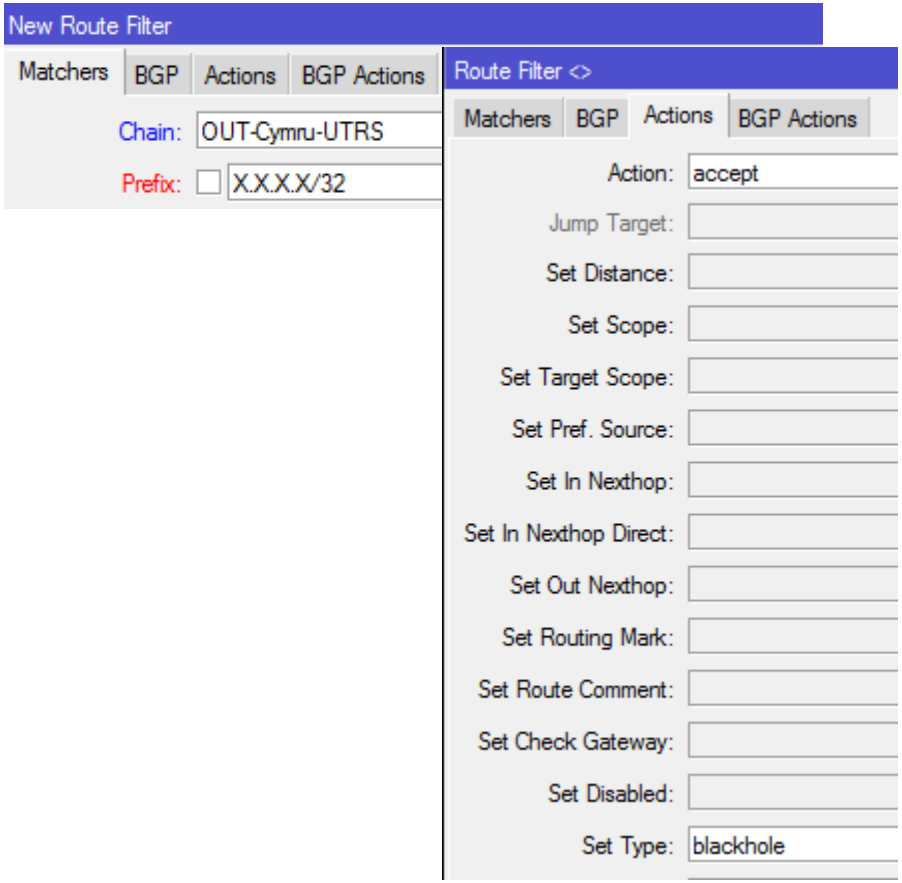
ISP X announces /32 attacked to UTRS and other ISP blackhole the /32, stopping the attack.

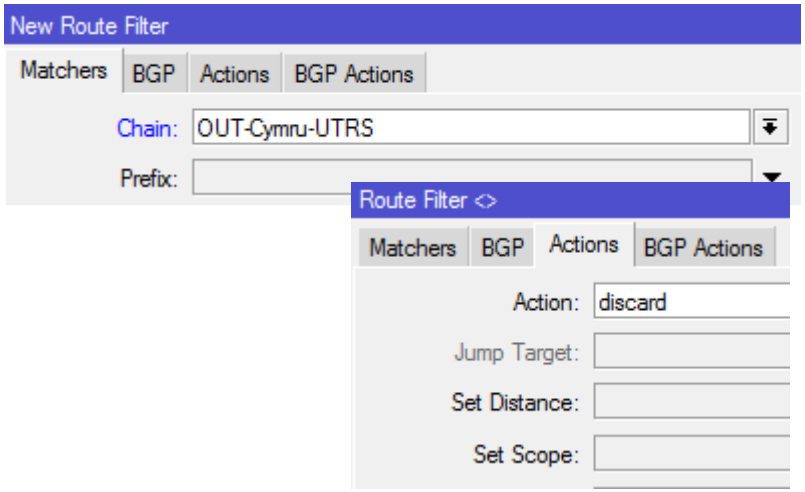
Content providers traffic is not affected.

Cymru - UTRS

Implementation on RouterOS:

In Case you want to announce /32

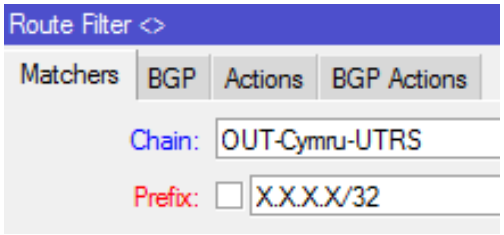


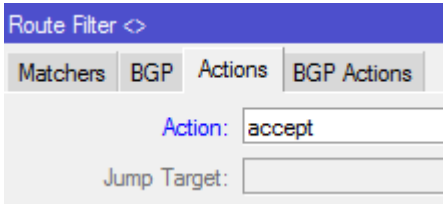


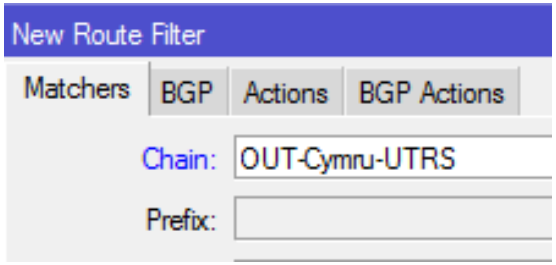
Cymru - UTRS

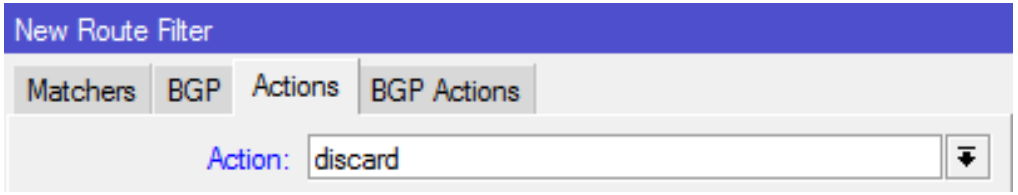
Implementation on RouterOS:

To black-hole announcements sent to UTRS









Ok, mitigation is possible, but how much time my SLA will be compromised?

From the attack to the action

All mitigation techniques will require a specific action, like blackholing to upstreams providers or changes in route announcements.

If the process is **handled by humans**, big chances are that service will be compromised for a very, very long time. People have to know what to do and have to do it fast.

Don’t forget that in some attacks the access to the router can be compromised and you don’t know even which IP is being attacked!

From the attack to the action

No chances for humans here.

Definitely, we do need an **automated** solution !

Sun Tzu – The art of war

In Peace, prepare for War…

Agenda

Background on DDoS – components and architecture and mitigation techniques;

Tools used for Detection and Mitigation in an ISP environment;

Hands On! Seeing things working;

The Cherry of the Cake – Cool Graphics and information about your network;

18’

From the attack to the action

Our automatic solution for DDoS mitigation uses:

→ **Mikrotik Traffic Flow (Net Flow)**

and a combination of 2 open source tools:

→ **Fastnetmon**

→ **ExaBGP**

DDoS Detection with Fastnetmon

The core of our solution is Fastnetmon

A high performance DoS/DDoS load analyzer built on top of multiple packet capture engines. Supports:

- NetFlow (Traffic Flow) v5, v9;
- IPFIX;
- sFLOW v5
- Port mirror/SPAN capture with PF_RING, NETMAP and PCAP

https://github.com/pavel-odintsov/fastnetmon

md brasil
TI&TELECOM

ExaBGP

BGP based SDN application

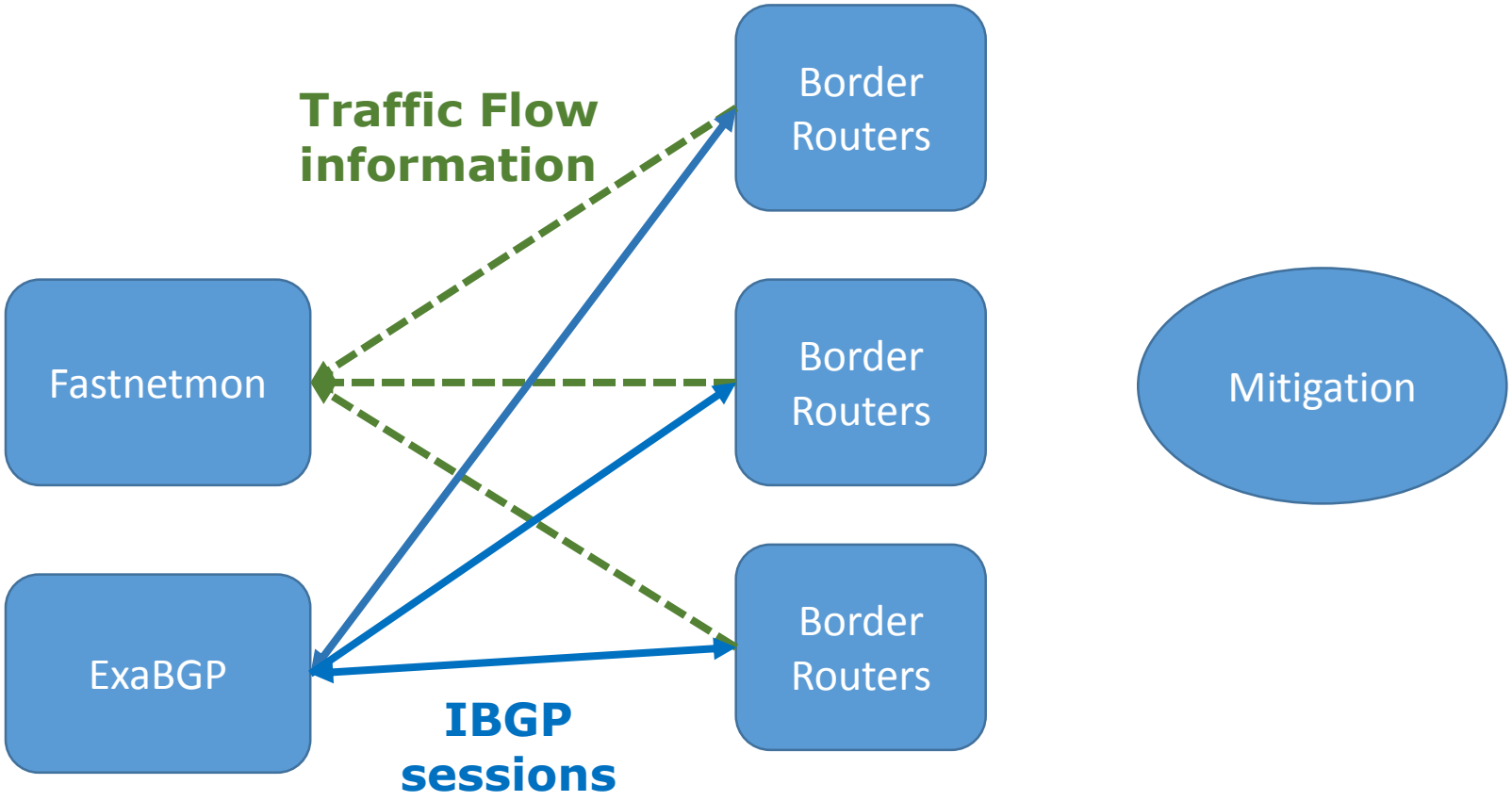
Known as the BGP “Swiss Knife”, ExaBGP can do a lot of related to the protocol usually not possible with a real BGP router.

With ExaBGP is possible to interact with routers, injecting arbitrary routes, collecting routing data, etc.

https://github.com/Exa-Networks/exabgp

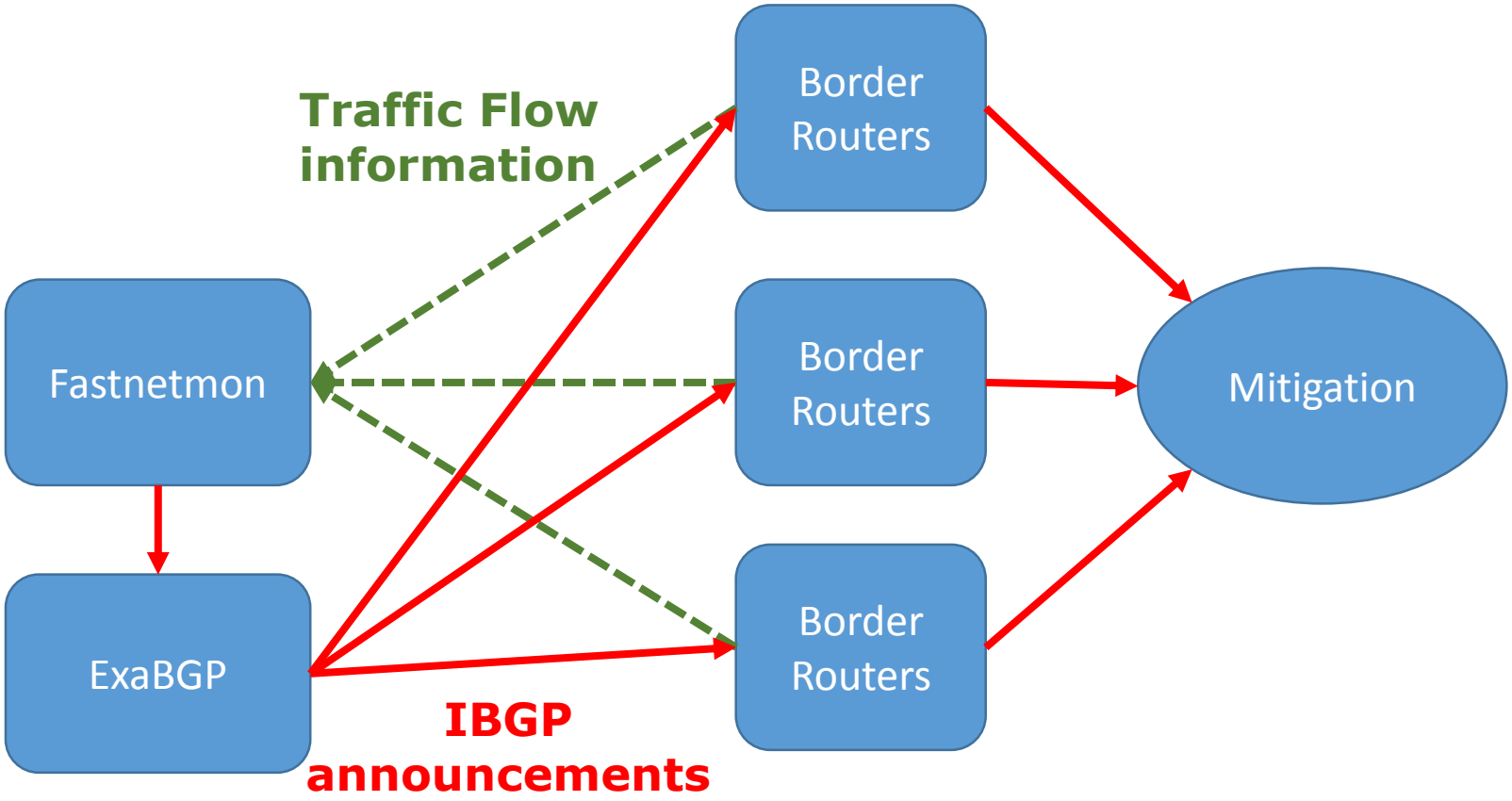
DDoS Detection and Mitigation Schema

In normal conditions Mikrotik Border Routers are sending Traffic Flow information to Fastnetmon and ExaBGP has iBGP sessions with the Border Routers.



DDoS Detection and Mitigation Schema

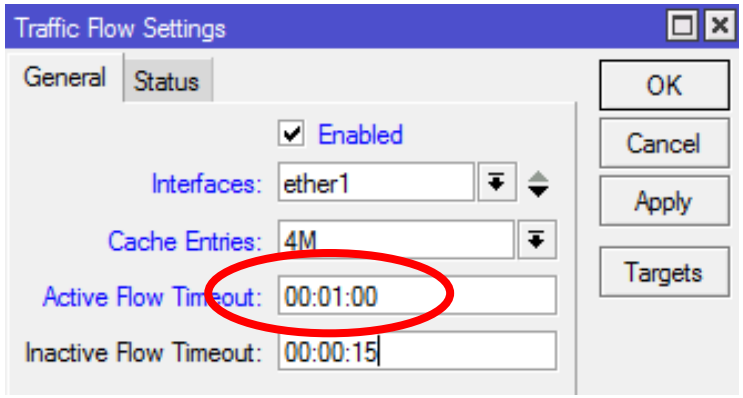
When a DDoS is detected, Fastnetmon triggers ExaBGP, that send iBGP routes with a specific community for blackholing. Border routers announce to mitigation solution

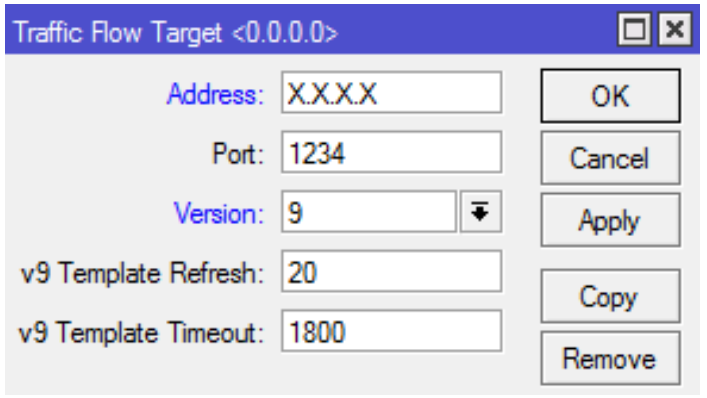


Traffic Flow Configuration

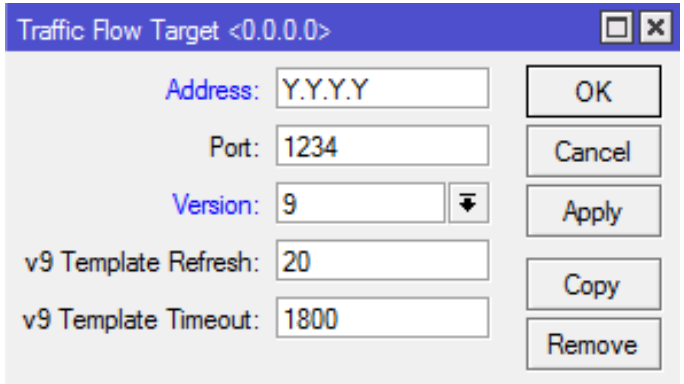
Traffic Flow

Traffic Flow configuration





We are using 2 instances for DDoS detection, one only for notifications and one for mitigation triggering.



Fastnetmon Installation and Configuration

Fastnetmon – Installation and Configuration

Automatic Installer for Debian and CentOS

Wget https://raw.githubusercontent.com/FastVPSEestiOu/fastnetmon/master/fastnetmon_install.pl

perl fastnetmon_install.pl

or

perl fastnetmon_install.pl --use git-master

Fastnetmon – Installation and Configuration

Configuration Details

The main configuration is a comprehensive text file in /etc/fastnetmon.conf

list of all your networks in CIDR format

networks_list_path = /etc/networks_list

list networks in CIDR format which will be not monitored for attacks

white_list_path = /etc/networks_whitelist

Fastnetmon – Installation and Configuration

Configuration

Netflow configuration

it's possible to specify multiple ports here, using commas as delimiter

netflow_port = 1234

netflow_host = 0.0.0.0

Adjust Port according to Mikrotik configuration. IP can be leaved as 0.0.0.0 but is better to inform the real IPs.

Fastnetmon – Installation and Configuration

Configuration – Thresholds

```
# Limits for Dos/DDoS attacks
threshold_pps = 20000
threshold_mbps = 1000
threshold_flows = 3500
```

Fastnetmon – Installation and Configuration

Integration with ExaBGP

```
# announce blocked IPs with BGP protocol with ExaBGP
exabgp = on
exabgp_command_pipe = /var/run/exabgp.cmd
exabgp_community = 65001:666
```

Turn exabgp on

Define an internal community for blackholing

ExaBGP Installation and Configuration

ExaBGP Installation and Configuration

ExaBGP Installation (for Debian/Ubuntu)

apt-get install python-pip

pip install exabgp

Installing the bidirectional pipe handler – socat

apt-get install socat

ExaBGP Installation and Configuration

Create a file /etc/exabgp_blackholing.conf

```
group anything {
        local-as 100;
        peer-as 100;
        router-id 1.1.1.1;
        neighbor 2.2.2.2 {
                local-address 1.1.1.1;
                }
        # process management
        process service-dynamic {
                run /usr/bin/socat stdout pipe:/var/run/exabgp.cmd;
                }
}
```

ExaBGP Installation and Configuration

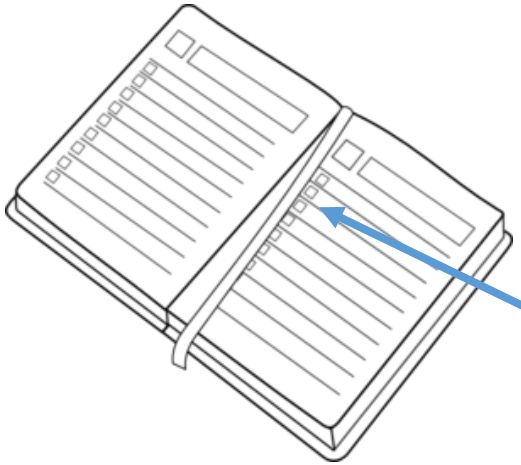
Run Exabgp

env exabgp.daemon.user=root exabgp.daemon.daemonize=true exabgp.daemon.pid=/var/run/exabgp.pid exabgp.log.destination=/var/log/exabgp.log exabgp /etc/exabgp_blackholing.conf

Source:

https://github.com/pavel-odintsov/fastnetmon/blob/master/docs/EXABGP_INTEGRATION.md

Agenda



Background on DDoS – components and architecture and mitigation techniques;

Tools used for Detection and Mitigation in an ISP environment;

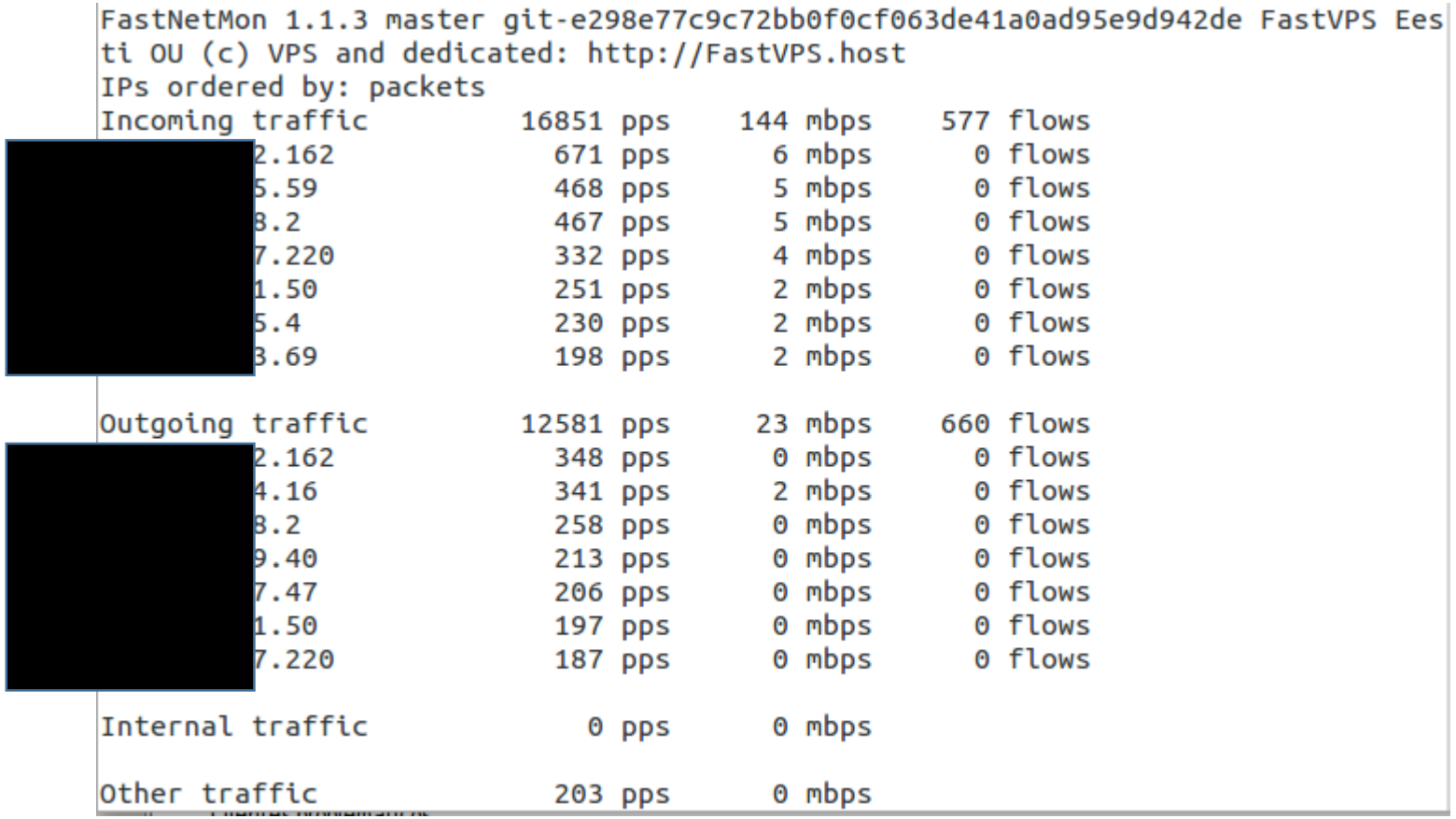
Hands On! Seeing things working;

The Cherry of the Cake – Cool Graphics and information about your network;

25’

Fastnetmon Client

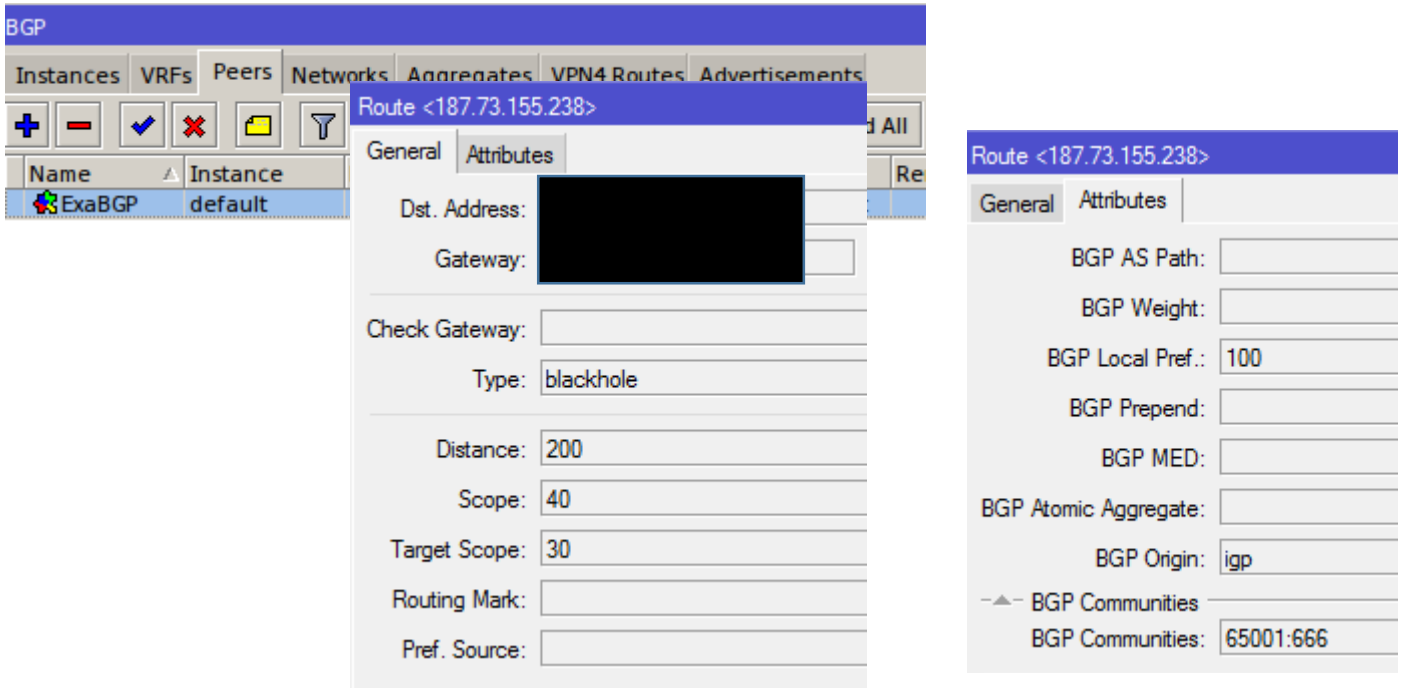
/opt/fastnetmon/fastnetmon_client

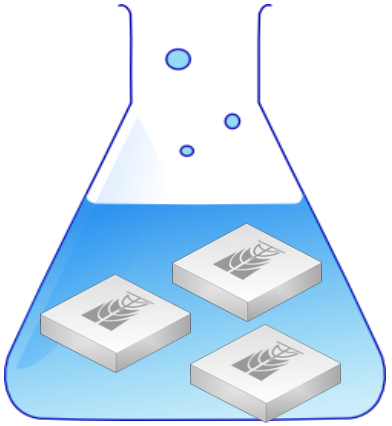


```
FastNetMon 1.1.3 master git-e298e77c9c72bb0f0cf063de41a0ad95e9d942de FastVPS Eesti OU (c) VPS and dedicated: http://FastVPS.host
IPs ordered by: packets
Incoming traffic          16851 pps     144 mbps     577 flows
[redacted]2.162             671 pps       6 mbps       0 flows
[redacted]5.59              468 pps       5 mbps       0 flows
[redacted]8.2               467 pps       5 mbps       0 flows
[redacted]7.220             332 pps       4 mbps       0 flows
[redacted]1.50              251 pps       2 mbps       0 flows
[redacted]5.4               230 pps       2 mbps       0 flows
[redacted]3.69              198 pps       2 mbps       0 flows

Outgoing traffic          12581 pps      23 mbps     660 flows
[redacted]2.162             348 pps       0 mbps       0 flows
[redacted]4.16              341 pps       2 mbps       0 flows
[redacted]8.2               258 pps       0 mbps       0 flows
[redacted]9.40              213 pps       0 mbps       0 flows
[redacted]7.47              206 pps       0 mbps       0 flows
[redacted]1.50              197 pps       0 mbps       0 flows
[redacted]7.220             187 pps       0 mbps       0 flows

Internal traffic              0 pps       0 mbps

Other traffic               203 pps       0 mbps
```

Fastnetmon Client

/opt/fastnetmon/fastnetmon_client

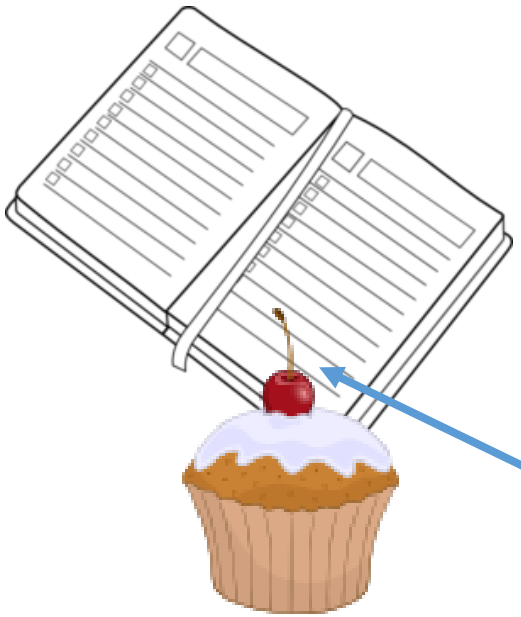




Pause for Hands ON

Let’s see things working

Agenda



Background on DDoS – components and architecture and mitigation techniques;

Tools used for Detection and Mitigation in an ISP environment;

Hands On! Seeing things working;

The Cherry of the Cake – Cool Graphics and information about your network;

32’

DDoS Detection with Fastnetmon

With the installation of Fastnetmon and other tools we can improve our implementation in order to have more information and control of our network.

For that purpose, besides **Fastnetmon** we will need some other tools:

InfluxDB + Grafana

https://github.com/FastVPSEestiOu/fastnetmon/blob/master/docs/INFLUXDB_INTEGRATION.md

Many thanks to my friend **Vicente de Luca**, from Zendesk who helped us a lot with the implementation.

DDoS Detection with Fastnetmon

InfluxDB is an open source distributed time series database with no external dependencies. It's useful for recording metrics, events, and performing analytics.

https://github.com/influxdata/influxdb

Installation for Debian/Ubuntu

wget https://s3.amazonaws.com/influxdb/influxdb_0.10.1-1_amd64.deb

sudo dpkg -i influxdb_0.10.1-1_amd64.deb

DDoS Detection with Fastnetmon

Grafana is an open source, feature rich metrics dashboard and graph editor for Graphite, Elasticsearch, OpenTSDB, Prometheus and InfluxDB

https://github.com/grafana/grafana

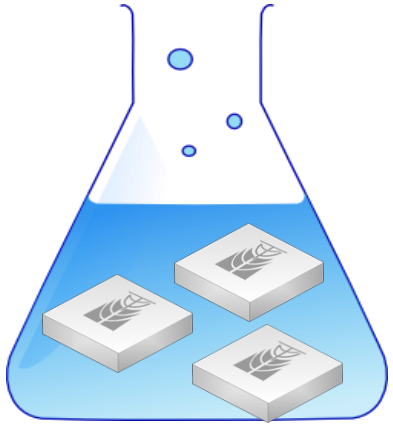
Installation for Debian/Ubuntu

wget https://grafanarel.s3.amazonaws.com/builds/grafana_2.6.0_amd64.deb

sudo dpkg -i grafana_2.6.0_amd64.deb

DDoS Detection with Fastnetmon

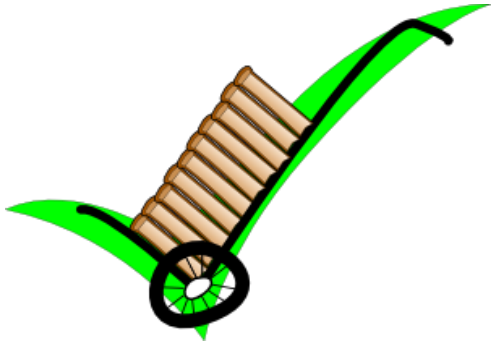
This is a typical dashboard you can do with grafana



Pause for Hands ON

Let’s see things working

References



Defeating DDoS – Cisco White paper

Anatomy of a DDoS attack – Team Cymru

Radware's DDoS Handbook: The Ultimate Guide to Everything You Need to Know about DDoS Attacks

An Introduction to DDoS Attacks and Defense Mechanisms: An Analyst's Handbook by B. B. Gupta

FastNetMon – Open Source DDoS Mitigation Toolkit – Presentation on RIPE71 meeting

Detecting and Mitigating DDoS: A FastNetMon Use Case by Vicente de Luca – Presentation at RIPE71 meeting

References

https://www.stateoftheinternet.com/downloads/pdfs/Q3-2015-SOTI-Connectivity-Executive-Summary.pdf

http://www.pcworld.com/article/3012963/security/ddos-attacks-increase-in-number-endanger-small-organizations.html

http://www.zdnet.com/article/ddos-attacks-size-doesnt-matter/

https://github.com/pavel-odintsov/fastnetmon/blob/master/docs/EXABGP_INTEGRATION.md

https://github.com/Exa-Networks/exabgp

https://github.com/FastVPSEestiOu/fastnetmon/blob/master/docs/INFLUXDB_INTEGRATION.md

https://github.com/grafana/grafana

Many Thanks to

Tom Smyth for the background in DDoS and all cooperation and technical information exchange;

Pavel Odinstov who developed the wonderful tool Fastnetmon and for the efforts in support;

Vicente de Luca for introduce me to Fastnetmon and the support on activating and configuring InfluxDB and Grafana

Thomas Mangin for the work with ExaBGP (I don't know him personally, but watched a lot of presentations)

All people from **open source community**, involved in cool projects ☺

Mikrotik guys, who gave us the opportunity to be in this cool event.

Download Page

Presentation and related material can be obtained in the URL:

http://mdbrasil.com.br/downloads

or in Mikrotik Web Site

Extra Slides

Background on DDoS
How to find amplifiers

DNS:

dig @x.x.x.x +edns +ignore com ANY

NTP:

ntpdc –nc monlist x.x.x.x

SNMP:

snmpbulkget -v2c -c public x.x.x.x 1.3

NetBios

nmblookup –A x.x.x.x

x.x.x.x = IP address

Background on DDoS
How to find amplifiers

SSDP

send UDP packet with destination port 1900 and the following payload:

SSDP

M-SEARCH * HTTP/1.1 \r\n

Host: x.x.x.x:1900 \r\n

Man: "ssdp:discover" \r\n

MX: 3 \r\n

ST: ssdp:all \r\n

\r\n

You can also use this script below:

https://gist.github.com/provegard/1435555

Installing and running Fastnetmon

Installing 1/3

```
root@fastnetmon:~# perl fastnetmon_install.pl --use-git-master
Hello, my dear Customer!

We need about ten minutes of your time for installing FastNetMon toolkit
You could make coffee/tee or you will help project and fill this short survey:
 http://bit.ly/fastnetmon_survey
I would be very glad if you spent this time and shared your DDoS experience :)

We detected your OS as debian Linux 8.3

Please provide your email address at company domain for free tool activation.
We will not share your email with any third party companies.
Email: maia@mdbrasil.com.br
```

Installing and running Fastnetmon

Installing 2/3

```
You have really nice server with 4 CPU's and we will use they all for build process :)
Update package manager cache
Install PF_RING dependencies with package manager
Download PF_RING 6.0.3 sources
Unpack PF_RING
Build PF_RING kernel module
Unload PF_RING if it was installed earlier
Load PF_RING module into kernel
PF_RING loaded correctly
Build PF_RING lib
Create library symlink
Add pf_ring to ld.so.conf
Install json library
Download archive
Uncompress it
Build it
Install it
Download nDPI
Configure nDPI
Build and install nDPI
Add ndpi to ld.so.conf
Download Luajit
Unpack Luajit
Build and install Luajit
```

Installing and running Fastnetmon

Installing 3/3

```
Install fastnetmon to dir /opt/fastnetmon
Create stub configuration file
Select eth0 as active interfaces
Tune config
If you have any issues, please check /var/log/fastnetmon.log file contents
Please add your subnets in /etc/networks_list in CIDR format one subnet per line
We found systemd enabled distro and created service: fastnetmon.service
You could run it with command: systemctl start fastnetmon.service
We have built project in 6.75 minutes
root@fastnetmon:~#
```

Background on DDoS Categories

Volumetric - Flood-based attacks that can be at layer 3, 4, or 7.

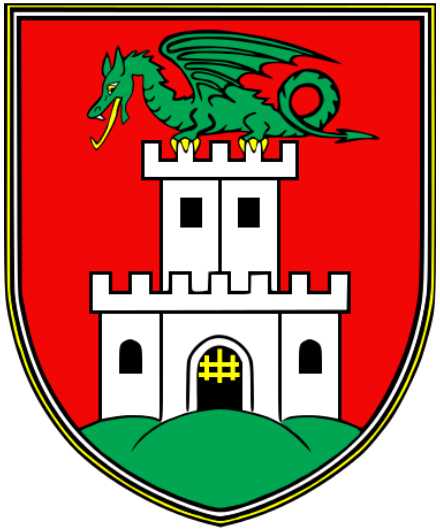
Asymmetric - Attacks designed to invoke timeouts or session-state changes.

Computational - Attacks designed to consume CPU and memory.

Vulnerability-based - Attacks that exploit software vulnerabilities.

https://f5.com/solutions/enterprise/reference-architectures/ddos-protection

Hvala!



Copyright Notice
(Aviso sobre direitos autorais)

English:

This material is an effort intended to improve the level of knowledge of professionals that work with Mikrotik RouterOS and should be used solely for self-study purposes.

Digital copies and/or any printed material contained in this presentation or derived from it are property of MD Brasil TI & Telecom and cannot be used for any kind of training, presentation or workshop, even non-commercial ones.

Reproduction of any part or picture requires previous written authorization of MD Brasil. For information about how to obtain such authorization, please contact mdbrasil@mdbrasil.com.br.

Portuguese:

Este material é um esforço que visa aprimorar o grau de conhecimento de profissionais que trabalham com Mikrotik RouterOS e deve ser usado apenas com objetivos de auto estudo.

Cópias digitais e/ou materiais impressos com conteúdo desta apresentação ou dela derivados são de propriedade a MD Brasil TI & Telecom a não podem ser usados para qualquer tipo de treinamento, apresentação ou seminário, mesmo os de finalidades não comerciais.

A reprodução de qualquer parte ou figura requer prévia autorização por escrito da MD Brasil. Para informações sobre como obter esta autorização, por favor contate mdbrasil@mdbrasil.com.br.