Ataques distribuidos de denegación de servicio

implementación de detección y mitigación en un ISP pequeño

LACNIC 25 – mayo 2016

La Habana - Cuba

Wardner Maia

md brasil
TI&TELECOM

Introduction

Wardner Maia

Ingeniero de electrónica y telecomunicaciones;
ISP desde 1995;
Entrenamientos desde 2002;
MD Brasil IT & Telecom CTO;
Miembro del Directorio de LACNIC.

Introduction

MD Brasil IT & Telecom

Proveedor de acceso a Internet en el estado de São Paulo - Brasil;

Integrador de equipos de telecomunicaciones;

Entrenamientos para ISPs;

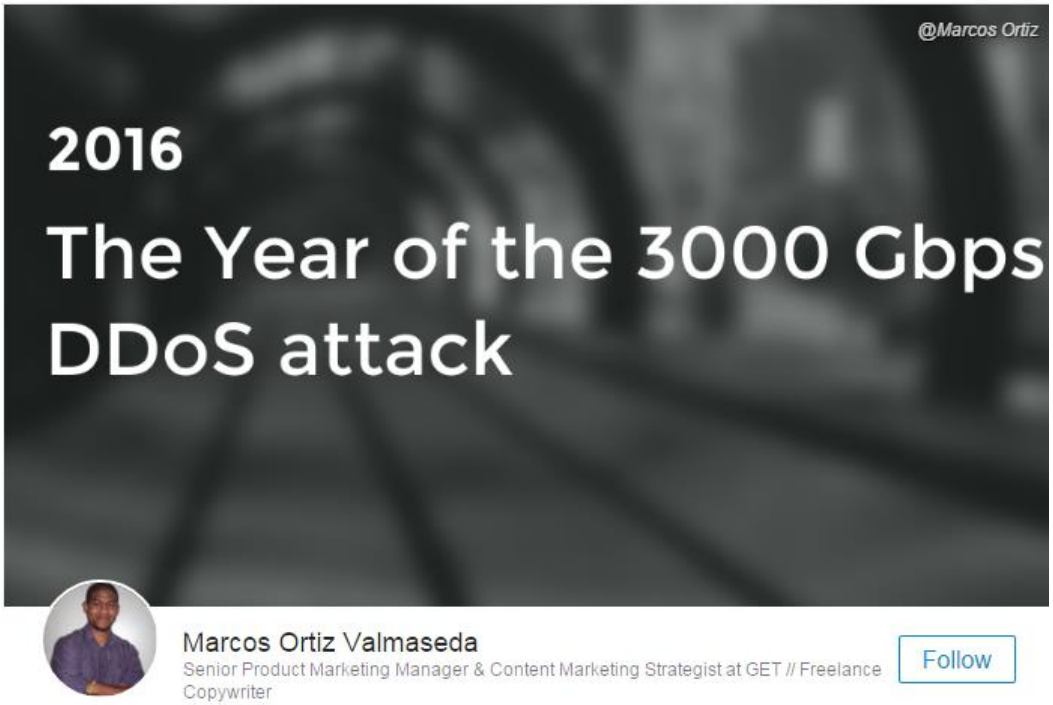
Servicios de consultoría.

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

DDoS – Detección y Mitigación

Por que este tema?

DDoS – ¿debo preocuparme?



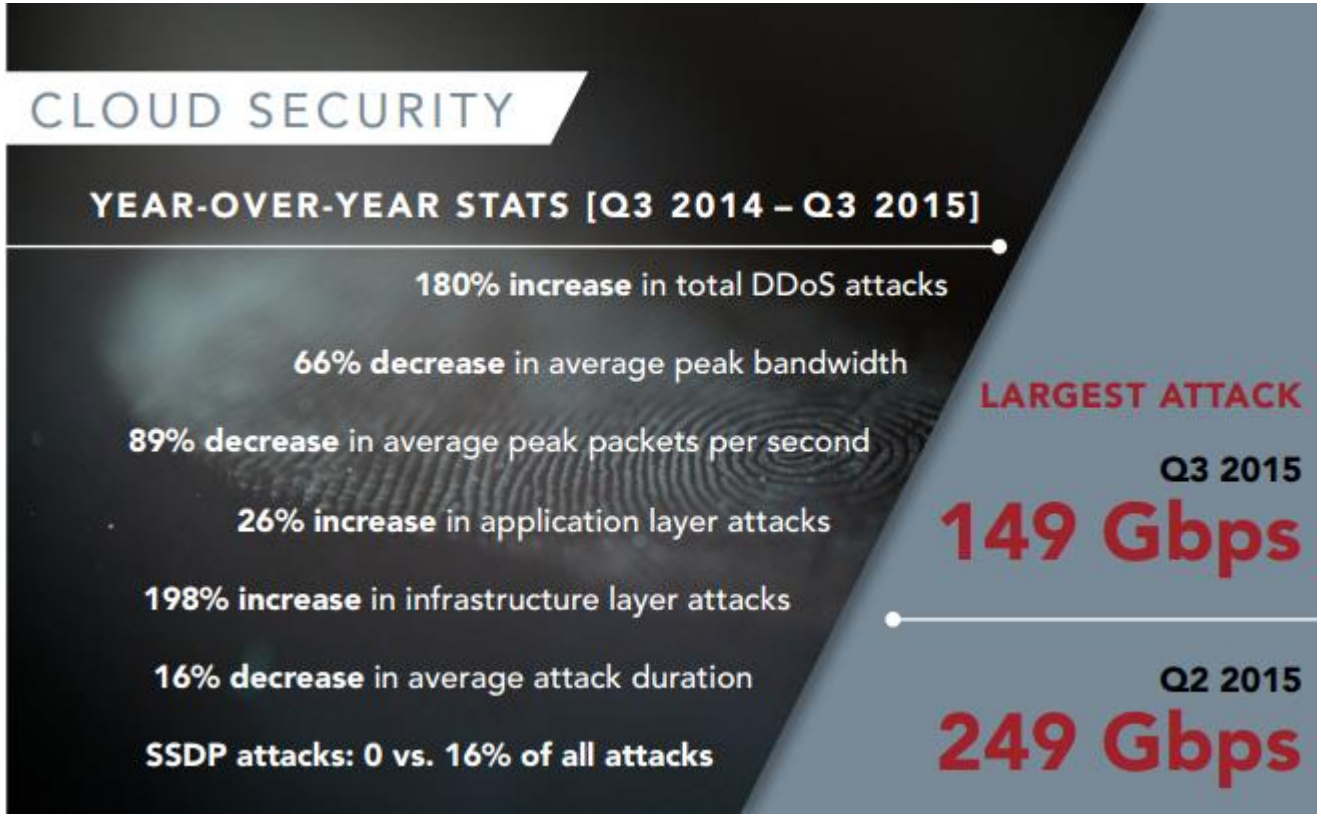
https://www.linkedin.com/pulse/2016-year-3000-gbps-ddos-attack-tech2016-marcos-ortiz-valmaseda?trk=pulse_spock-articles

Debemos estar listos para mayores y mayores ataques

¿Ataques DDoS son un "privilegio" de los grandes operadores e de los grandes centros de datos?

¿Puede mi pequeña/mediana) empresa ser un objetivo?

DDoS – ¿debo preocuparme?



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

DDoS – ¿debo preocuparme?

PCWorld
Work. Life. Productivity.

NEWS | REVIEWS | HOW-TO | VIDEO | BUSINESS | LAPTOPS | TABLETS

Privacy | Encryption | Antivirus

DDoS attacks increase in number, endanger small organizations

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

EDITION: US

ZDNet | SEARCH | CLOUD | CXO | HARDWARE | WINDOWS 10 | IOT | INNOVATION

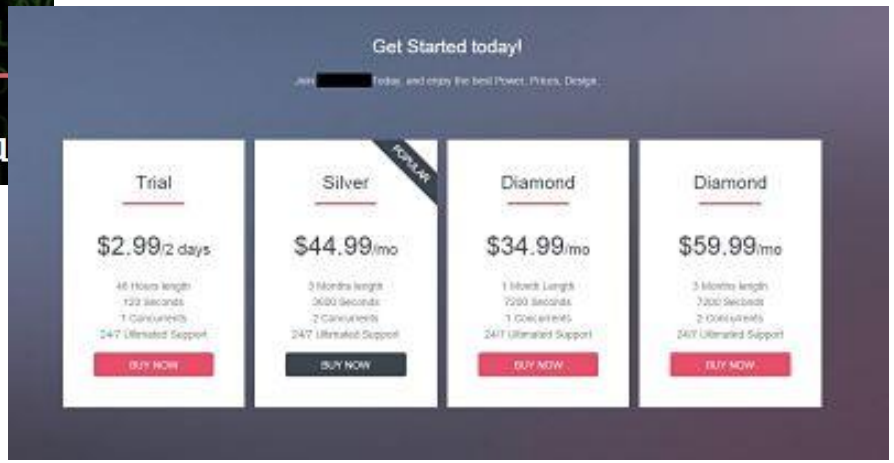
MUST READ SAMSUNG STARTS ANDROID MARSHMALLOW ROLLOUT FOR GALAXY S6, S6 EDGE

DDoS Attacks: Size doesn't matter

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

DDoS – ¿debo preocuparme?

¿Que tal contratar un ataque de DDoS por US$ 2.99?



DDoS – ¿debo preocuparme?

Ser objetivo de un ataque de DDoS no es una cuestión de "si", pero de cuando va a pasar.

¿Tenéis un plan formal de respuestas a incidentes?

DDoS – detección y mitigación

¿Para quienes es esta presentación?

Público objetivo y metas de la presentación

Esta presentación tiene como público objetivo, pequeños e medianos ISPs, que trabajan como proveedores de ultima milla;

Las principales metas de esta presentación son: mostrar la importancia de tener un plan en contra los ataques de DDoS y las sugerencias de como lo implementar.

Serán utilizadas básicamente herramientas open source.

- Sera presentado un caso real de implementación en un pequeño ISP en Brasil;

Agenda

Recordatorio de DDoS – componentes, y arquitectura;

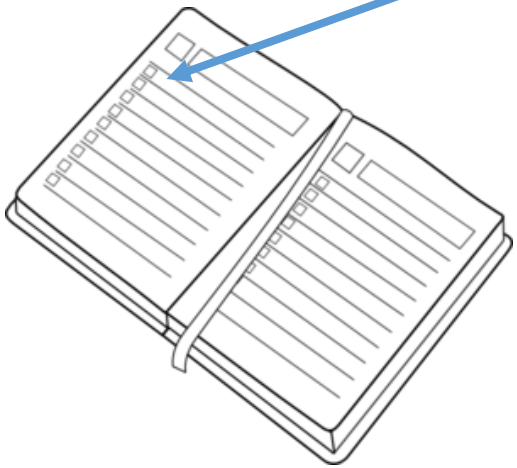
Enfrentamiento de los ataques – las buenas practicas en nuestra red para minimizarlos;

Enfrentamiento de los ataques – técnicas de mitigación posibles y sus implementaciones;

Automatizando la detección y mitigación en un ISP regional de Brasil

La cereza de la torta – Gráficos y informaciones sobre la red;

Agenda



Recordatorio de DDoS – componentes, y arquitectura;

Enfrentamiento de los ataques – las buenas practicas en nuestra red para minimizarlos;

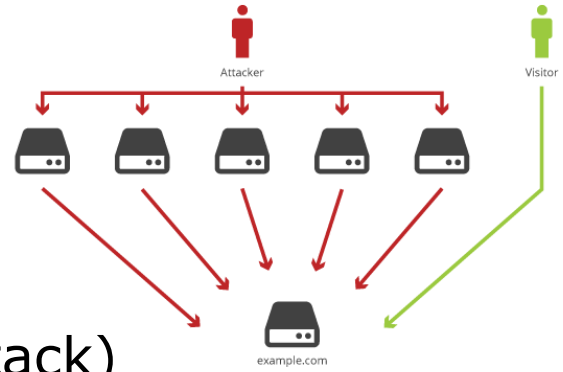
Enfrentamiento de los ataques – técnicas de mitigación posibles y sus implementaciones;

Automatizando la detección y mitigación en un ISP regional de Brasil

La cereza de la torta – Gráficos y informaciones sobre la red;

Recordatorio de DDoS
Conceptos básicos

Terminología



DoS (Denial of Service Attack)

Ataques de Negación de servicio

DDoS (Distributed Denial of Service Attack)

Ataques de Negación de servicio distribuidos

DRDoS (Distributed Reflected Denial of Service Attack)

Ataques de Negación de servicio distribuidos amplificados

Tipos de ataques Dos

1. Ataques a la camada de aplicación

Tienen como meta la saturación de recursos, explotando características de la camada 7;

- No necesitan muchas máquinas para y tampoco muchos recursos de ancho de banda para su realización.
- Ejemplos: HTTP POST, HTTP GET, SIP Invite flood, etc

Tipos de ataques Dos

2. Ataques de consumo de los recursos de hardware

Intentan consumir recursos como CPU e memoria, de equipos de rede como enrutadores y firewalls.

- Ejemplos: fragmentación y SYN flood

Tipos de ataques Dos

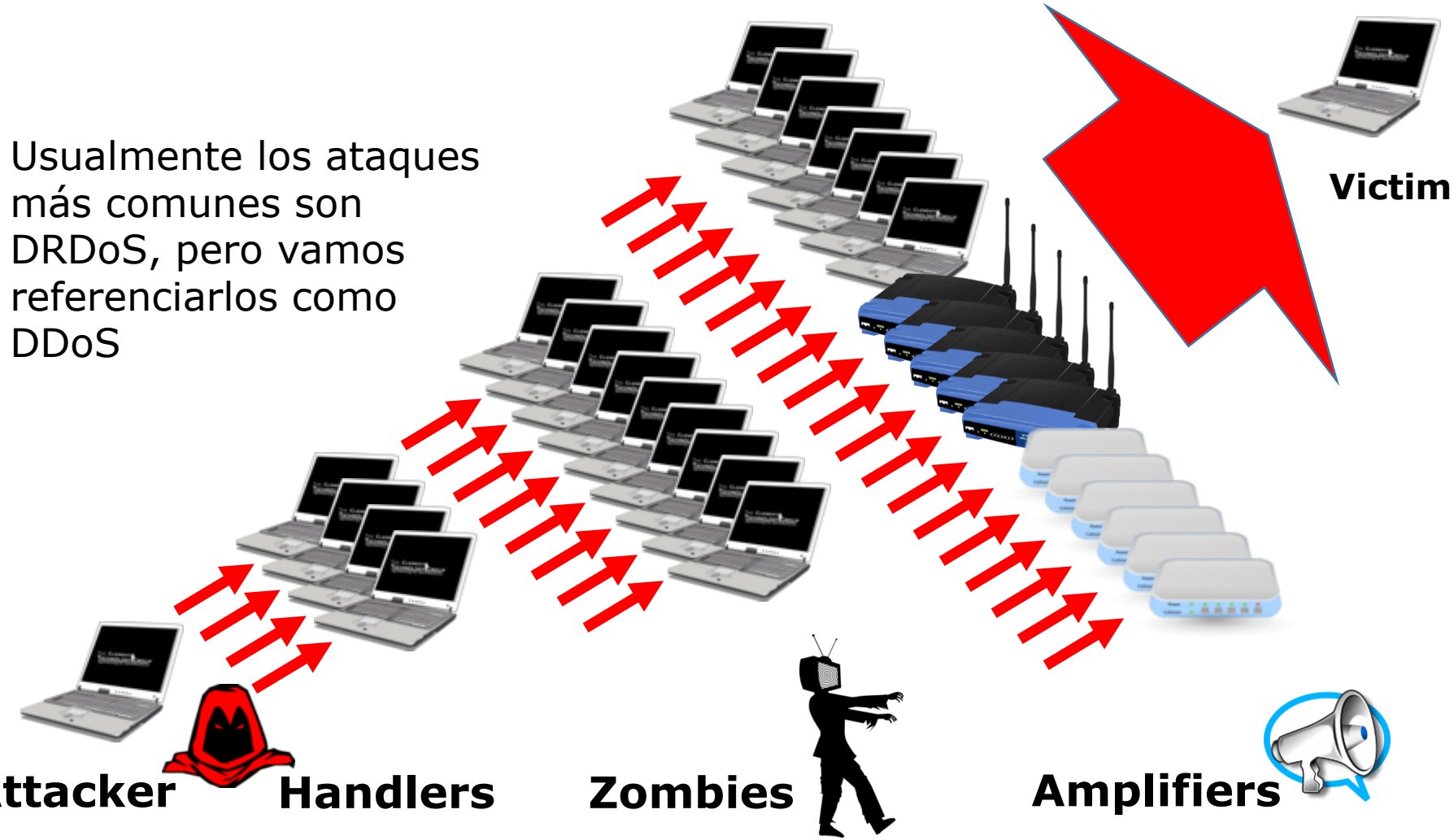
3. Ataques volumétricos

Tienen como meta consumir todos los recursos de ancho de banda de un link de datos.

- Utilizan los Botnets, máquinas comprometidas y equipos mal configurados que permiten la amplificación de requisiciones
- Hacen el Spoof de lo IP de la victima para forzar respuestas amplificadas a ella.

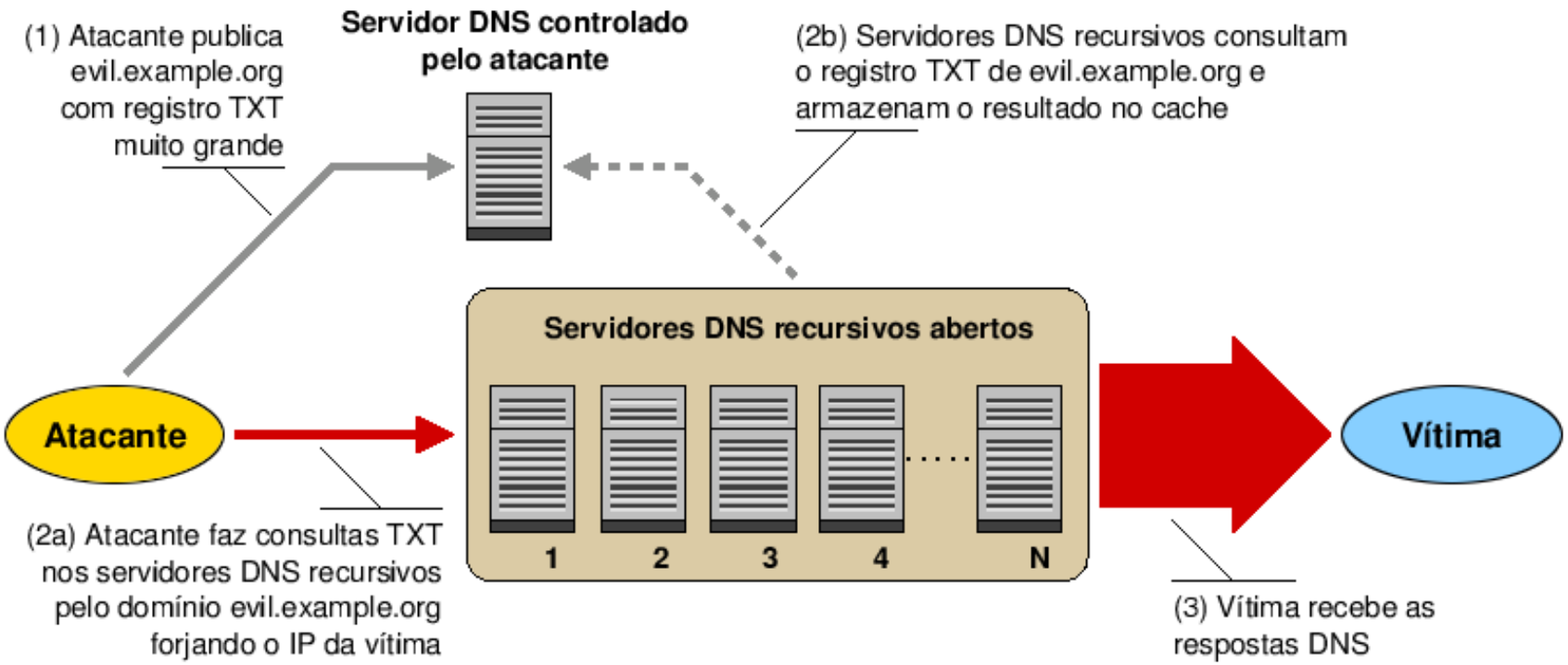
Anatomía de un ataque DRDoS

Usualmente los ataques más comunes son DRDoS, pero vamos referenciarlos como DDoS



DRDOS utilizando DNS

Esquema de ataque DRDoS utilizando DNSs recursivos abiertos



fuente: http://cert.br/docs/whitepapers/ddos

Amplificadores

Factores de amplificación

DNS (53/UDP): 28 hasta 54 veces;

NTP (123/UDP): 556.9 veces;

SNMPv2 (161/UDP): 6.3 veces;

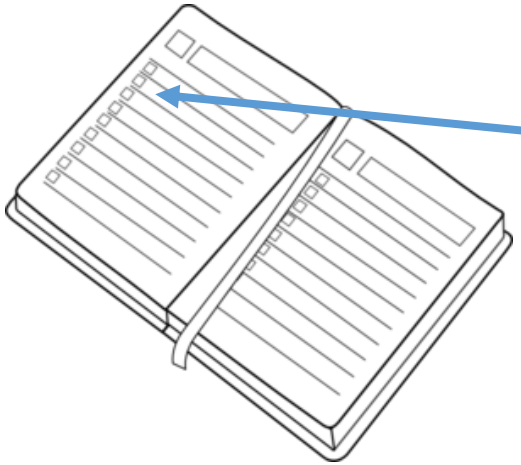
NetBIOS (137–139/UDP): 3.8 veces;

SSDP (1900/UDP): 30.8 veces;

CHARGEN (19/UDP): 358.8 veces.

fuente: http://cert.br/docs/whitepapers/ddos

Agenda



Recordatorio de DDoS – componentes, y arquitectura;

Enfrentamiento de los ataques – las buenas practicas en nuestra red para minimizarlos;

Enfrentamiento de los ataques – técnicas de mitigación posibles y sus implementaciones;

Automatizando la detección y mitigación en un ISP regional de Brasil

La cereza de la torta – Gráficos y informaciones sobre la red;

Deberes de casa

Facilitadores de DDoS

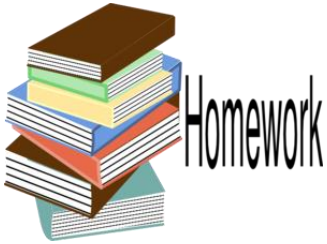
Máquinas comprometidas

Servidores o servicios mal configurados

ISPs que non implementan BCP-38 en sus upstreams

Ruteo para direcciones bogons

Deberes de casa



Implementación de BCP-38

Básicamente consiste en evitar el spoof de direcciones IP

→ Través de reglas de Firewall y o uRPF

Como regla general en nuestra red fue implementada

→ uRPF en el modo “strict” para los routers de acceso

→ uRPF en el modo “loose” para los routers de Borde

BCP-38 – Si todos la implementan no hay más spoof, luego no más DRDoS

Deberes de casa

Procurando amplificadores

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

Deberes de casa

Procurando amplificadores

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

```
% dig @201.[redacted]5 +edns=0 +ignore com ANY | grep rcvd
;; MSG SIZE  rcvd: 243
```

Como en este caso la respuesta es mayor que la requisición de 60 byte, és un amplificador.

Mitigación:

Forzar TCP modo TCP;

Asegurar resolver recursivos (Link);

Emplear Rate-limit en los servidores de autoritativos (Link).

Deberes de casa

NTP: ntpdc –nc monlist x.x.x.x

Cada línea es un paquete UDP con 468 bytes

Mitigación:

La mejor solución es deshabilitar monlist nos servidores NTP. En ntp.conf:

restrict default no query

Otra opción es el filtrado de paquetes UDP con puerto de origen 123 y tamaño de paquete 468

Deberes de casa

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

chequea por la vulnerabilidad mas común. public es e nombre default para la comunidad SNMP e 1.3 significa iso.org request OID.

Mitigación:

Importante no utilizar el valor default “public”

Recomendable restringir el rango de direcciones IP que pueden aceder SNMP

Deberes de casa

NetBios: nmblookup –A x.x.x.x

Mitigación:

Filtrar requisiciones NB y NBSTAT de redes externas.

Deberes de casa

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

Hay también el script abajo:

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

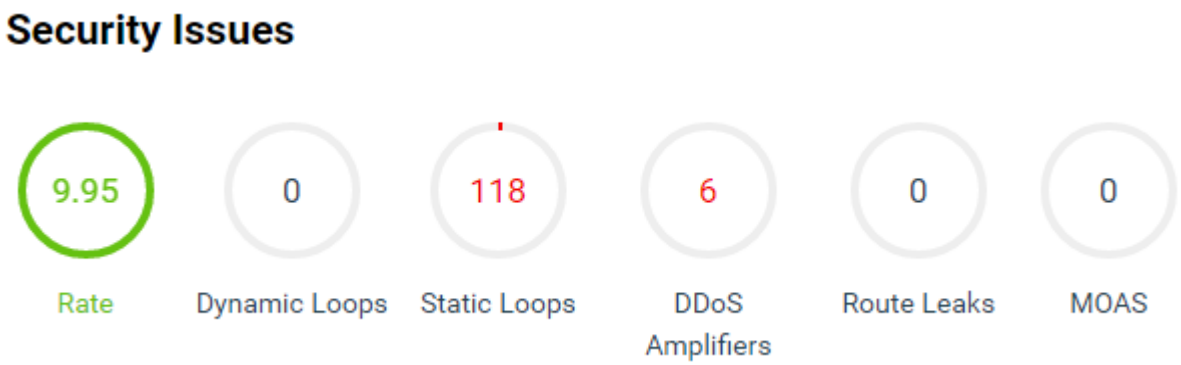
Mitigación: restringir rangos de IP

Deberes de casa

Procurando amplificadores

Un buén site que ayuda en esta busca és

http://radar.qrator.net



Deberes de casa

Blackholing para direcciones BOGONs

Subscribirse en lo servicio de Bogons de Team Cymru y poner en blackhole los prefijos Bogons.

TEAM CYMRU
COMMUNITY
SERVICES

HOW DO I OBTAIN A PEERING SESSION?

To peer with the bogon route servers, contact bogonrs@cymru.com. When requesting a peering session, please include the following information in your e-mail:

1. Which bogon types you wish to receive (traditional IPv4 bogons, IPv4 fullbogons, and/or IPv6 fullbogons)
2. Your AS number
3. The IP address(es) you want us to peer with
4. Does your equipment support MD5 passwords for BGP sessions?
5. Optional: your GPG/PGP public key

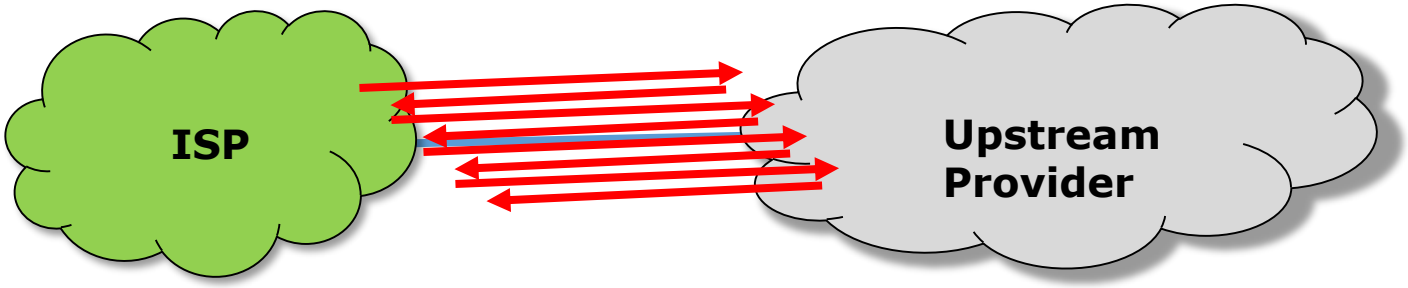
We will typically provide multiple peering sessions (at least 2) per remote peer for redundancy. If you would like more or less than 2 sessions please note that in your request. We try to respond to new peering requests within one to two business days, but, again, can provide no guarantees for this **free** service.

Remember that you must be able to accomodate up to **100 prefixes** for *traditional bogons*, and up to **50,000 prefixes** for *fullbogons*, and be capable of multihop peering with a private ASN. If you improperly configure your peering and route all packets destined for bogon addresses to the bogon route-servers, your peering session will be dropped.

Deberes de casa

Eliminar loopings estáticos

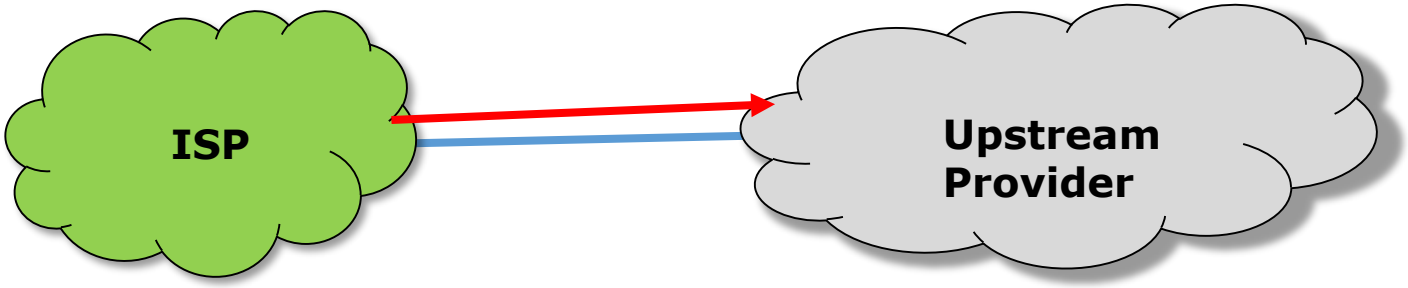
→ Asegurarse de que todo su espacio anunciado en BGP tiene rutas internas para sus redes, evitando así los **loopings estáticos;**



Si no hay rutas internas y lo spacio tiene que ser anunciado, asegúrate de poner en blackhole la parte no utilizada.

Reducir espacio de exposición

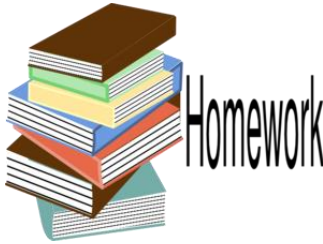
→ Reducir su espacio de exposición a los ataques DDoS anunciando sus bloques no utilizados como blackhole



NB: Depende de la existencia de una política en su(s) proveedores de conectividad

Deberes de casa

Ejemplo de reducción cuando se utiliza /30 para enlaces dedicados



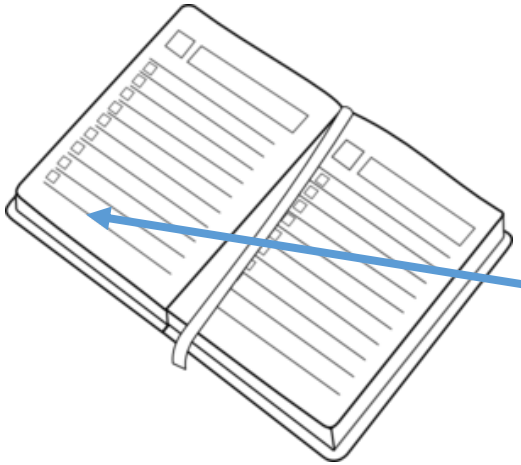
1.1.1.0/30 - 1.1.1.0 (dirección de red)

- 1.1.1.1 (dirección del router del ISP)
- **1.1.1.2 (dirección del cliente)**
- 1.1.1.3 (dirección de broadcast)

Solamente la dirección IP del cliente necesita conectividad a Internet. Los otros se puede poner en blackhole, ***bajando 75% del espacio de exposición!***

BGP and Security workshop by Tom Smyth (Wireless Connect, Ireland)

Agenda



Recordatorio de DDoS – componentes, y arquitectura;

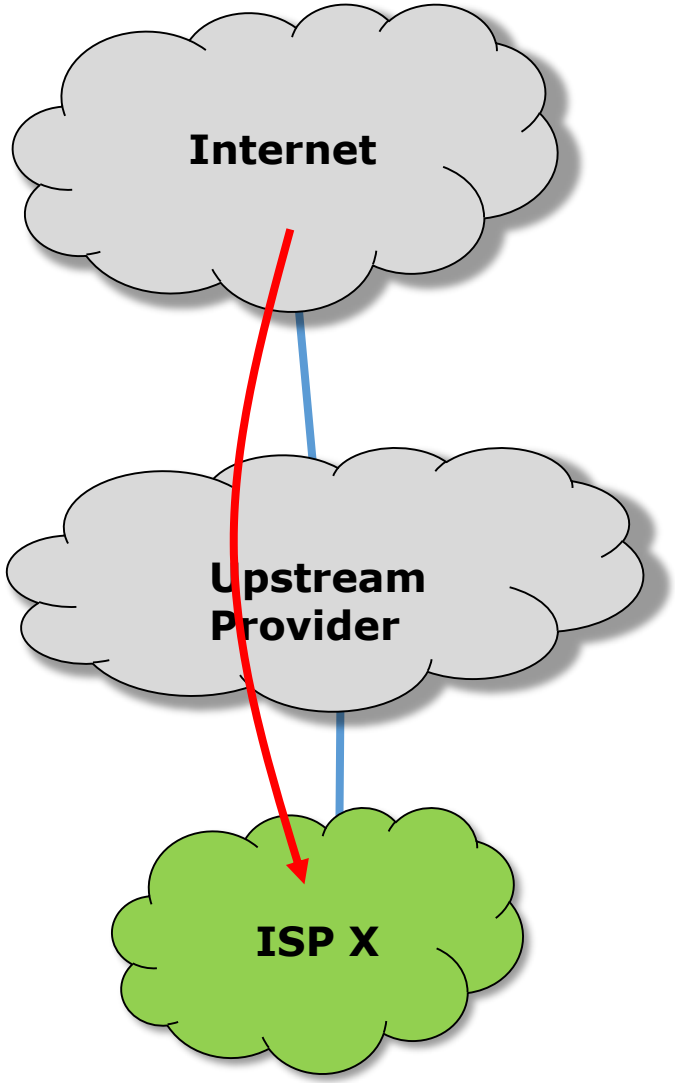
Enfrentamiento de los ataques – las buenas practicas en nuestra red para minimizarlos;

Enfrentamiento de los ataques – técnicas de mitigación posibles y sus implementaciones;

Automatizando la detección y mitigación en un ISP regional de Brasil

La cereza de la torta – Gráficos y informaciones sobre la red;

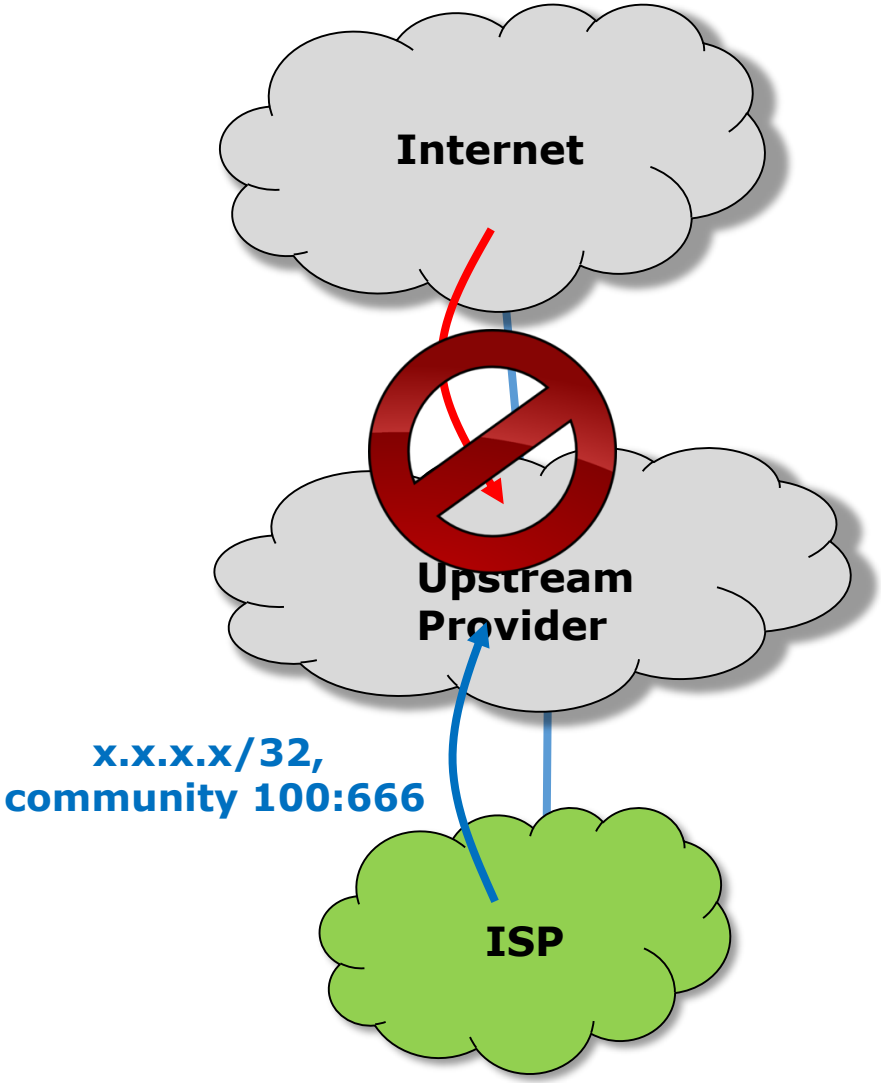
Blackhole remotamente accionado (RTBH)



ISP X esta sofriendo un ataque DDoS direccionado para el IP x.x.x.x/32, causando la inundación del link;

Su proveedor de upstream (ejemplo AS 100) tiene una política que pone en blackhole los anuncios /32 que tenga una community determinada (ejemplo 100:666);

Blackhole remotamente accionado (RTBH)



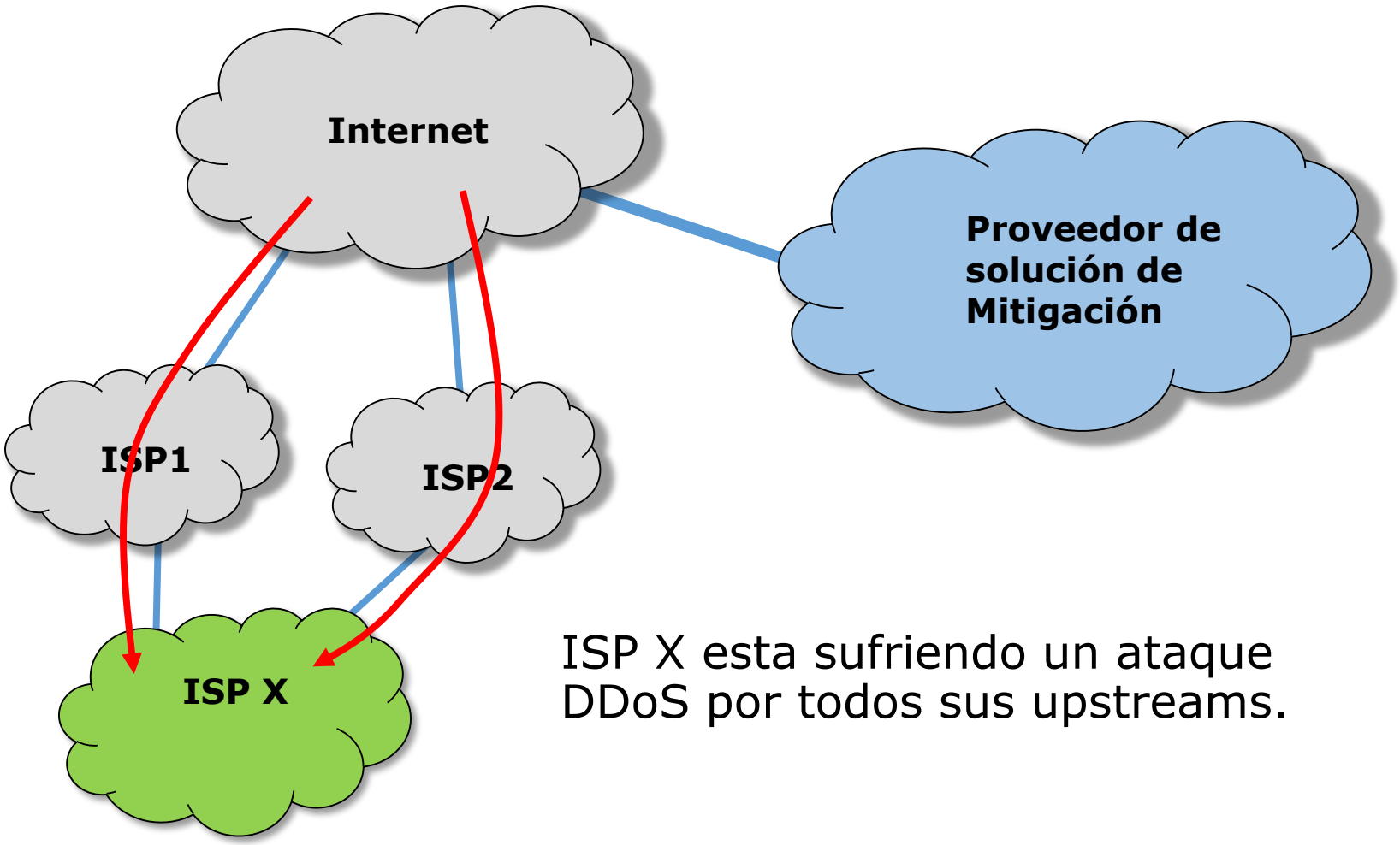
ISP anuncia para su upstream la dirección IP /32 con la community 100:666;

Upstream tiene filtros que reconocen la community y automáticamente ponen la dirección anunciada en blackhole;

La comunicación con este /32 es perdida, pero la inundación del link es parada;

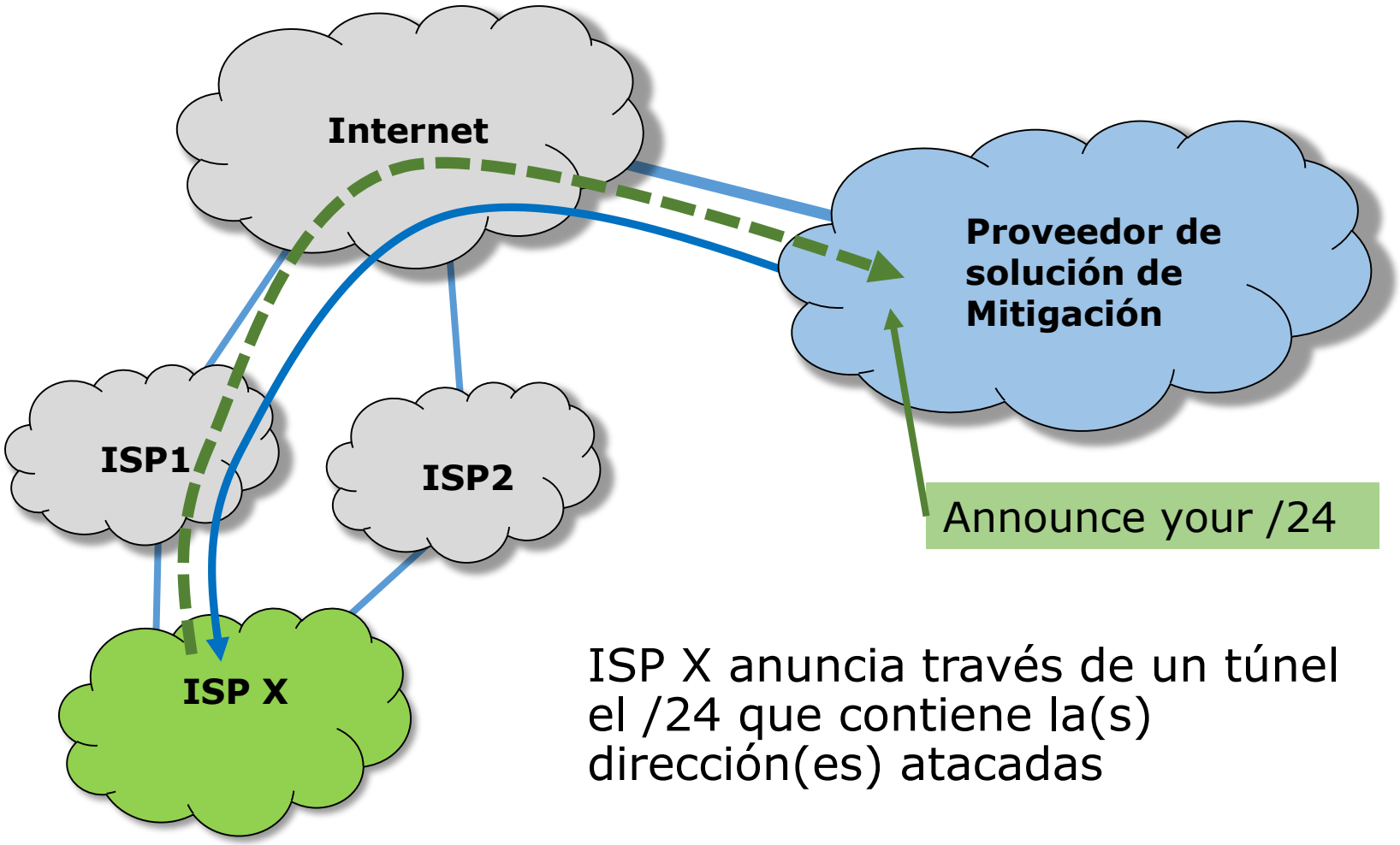
O SLA de los otros clientes es preservado, pero podemos decir que el ataque tuve suceso ☹

Mitigación en la nube (Sinkhole)



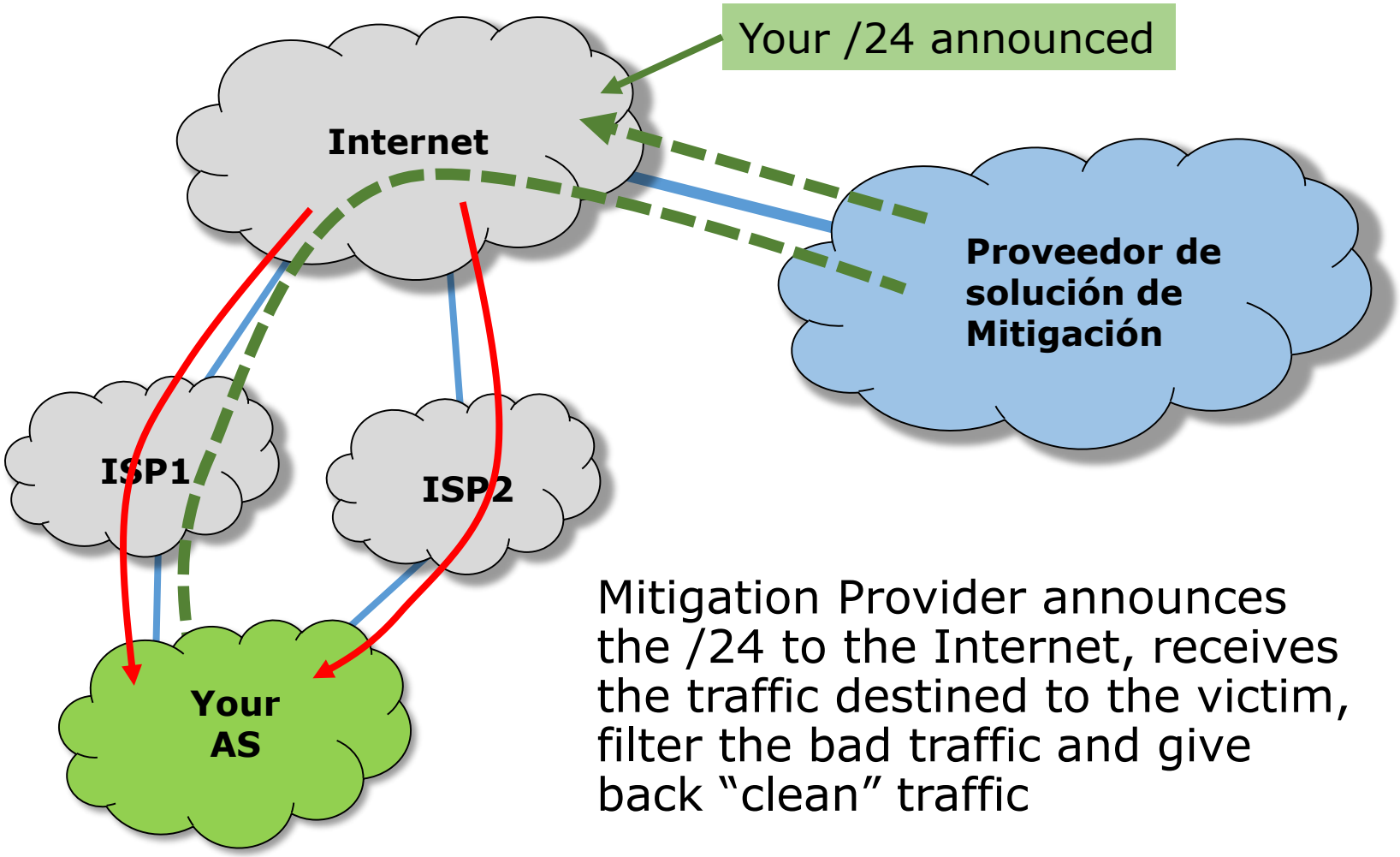
ISP X esta sufriendo un ataque DDoS por todos sus upstreams.

Mitigación en la nube



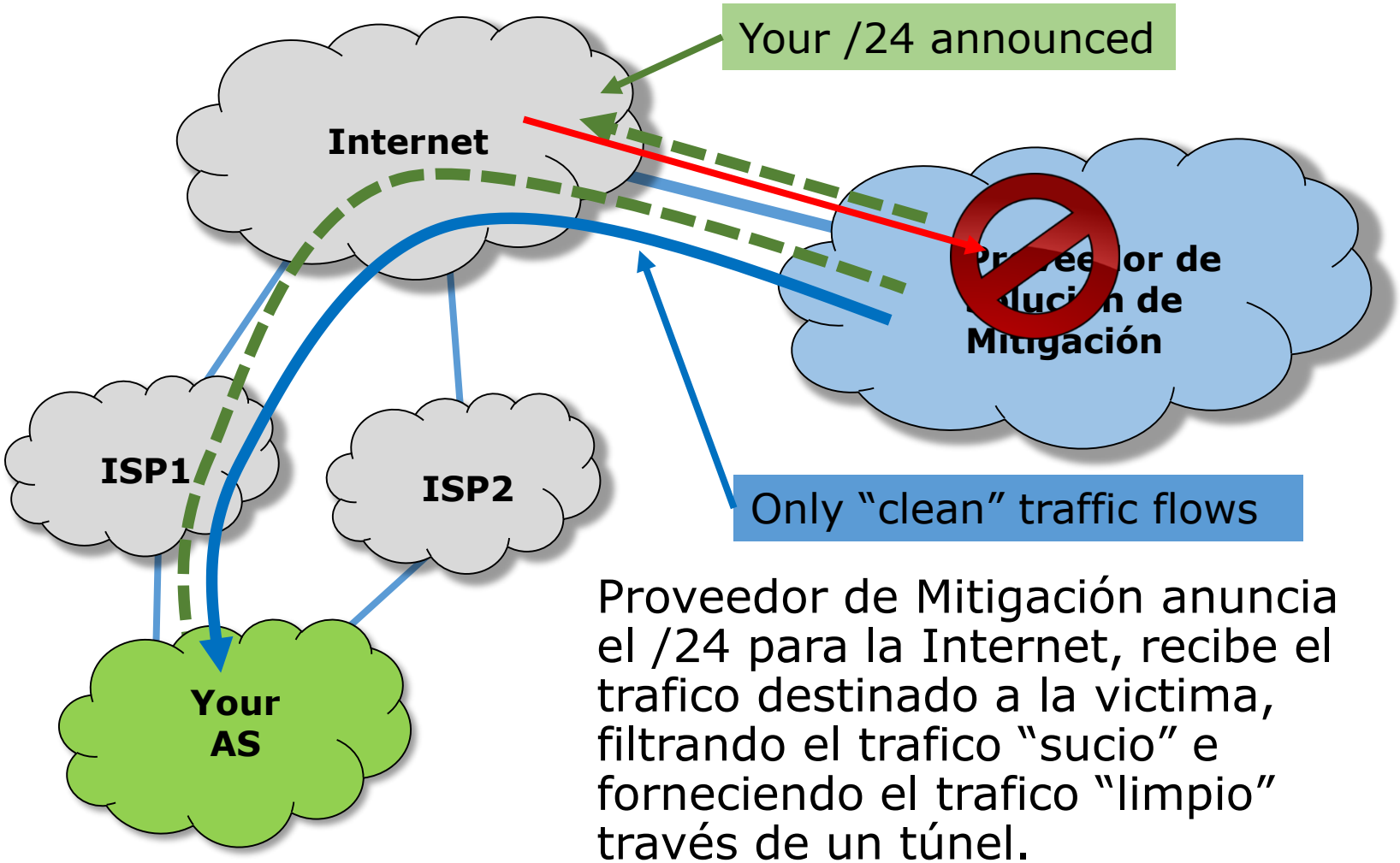
ISP X anuncia través de un túnel el /24 que contiene la(s) dirección(es) atacadas

Mitigación en la nube



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

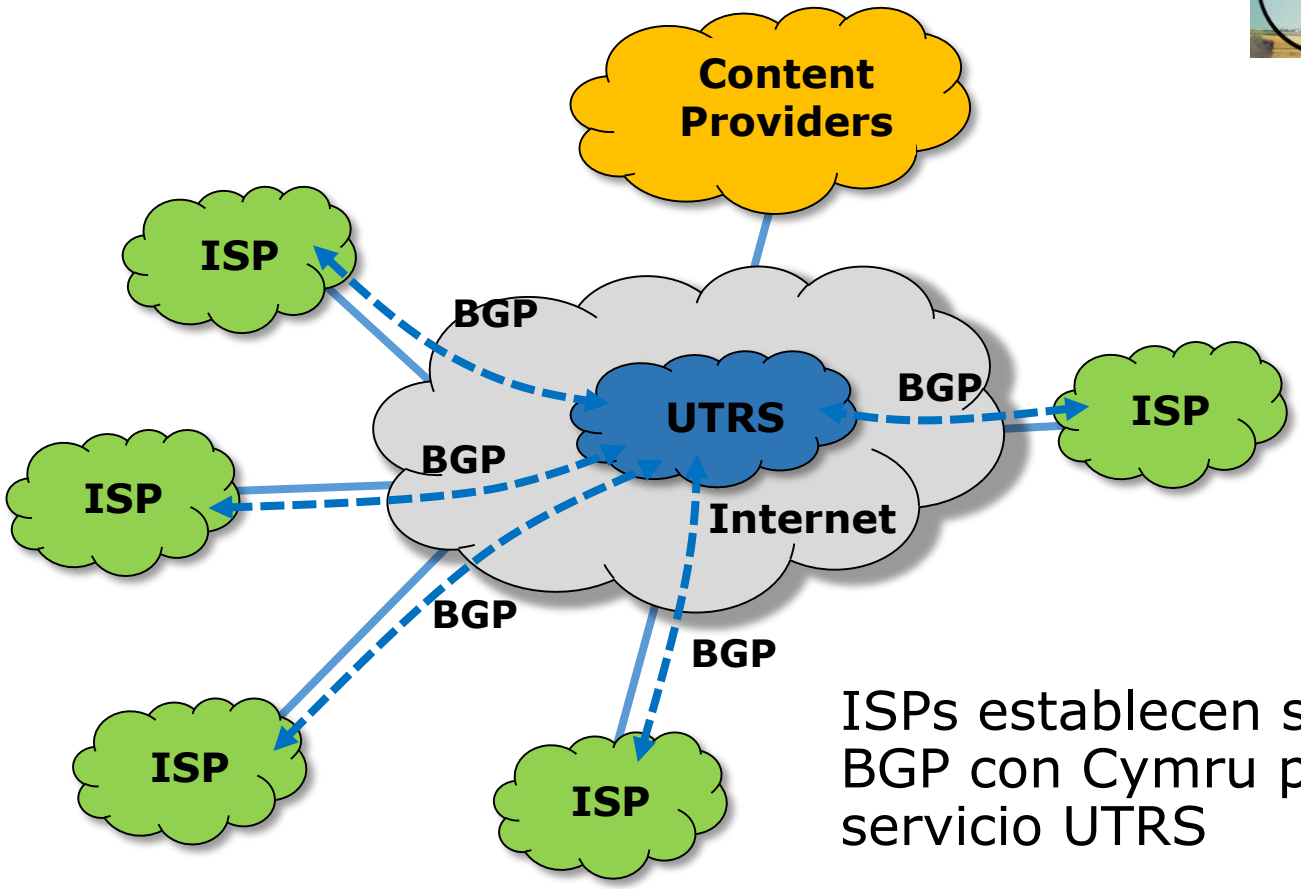
Mitigación en la nube



Proveedor de Mitigación anuncia el /24 para la Internet, recibe el trafico destinado a la victima, filtrando el trafico "sucio" e forneciendo el trafico "limpio" través de un túnel.

Cymru - UTRS

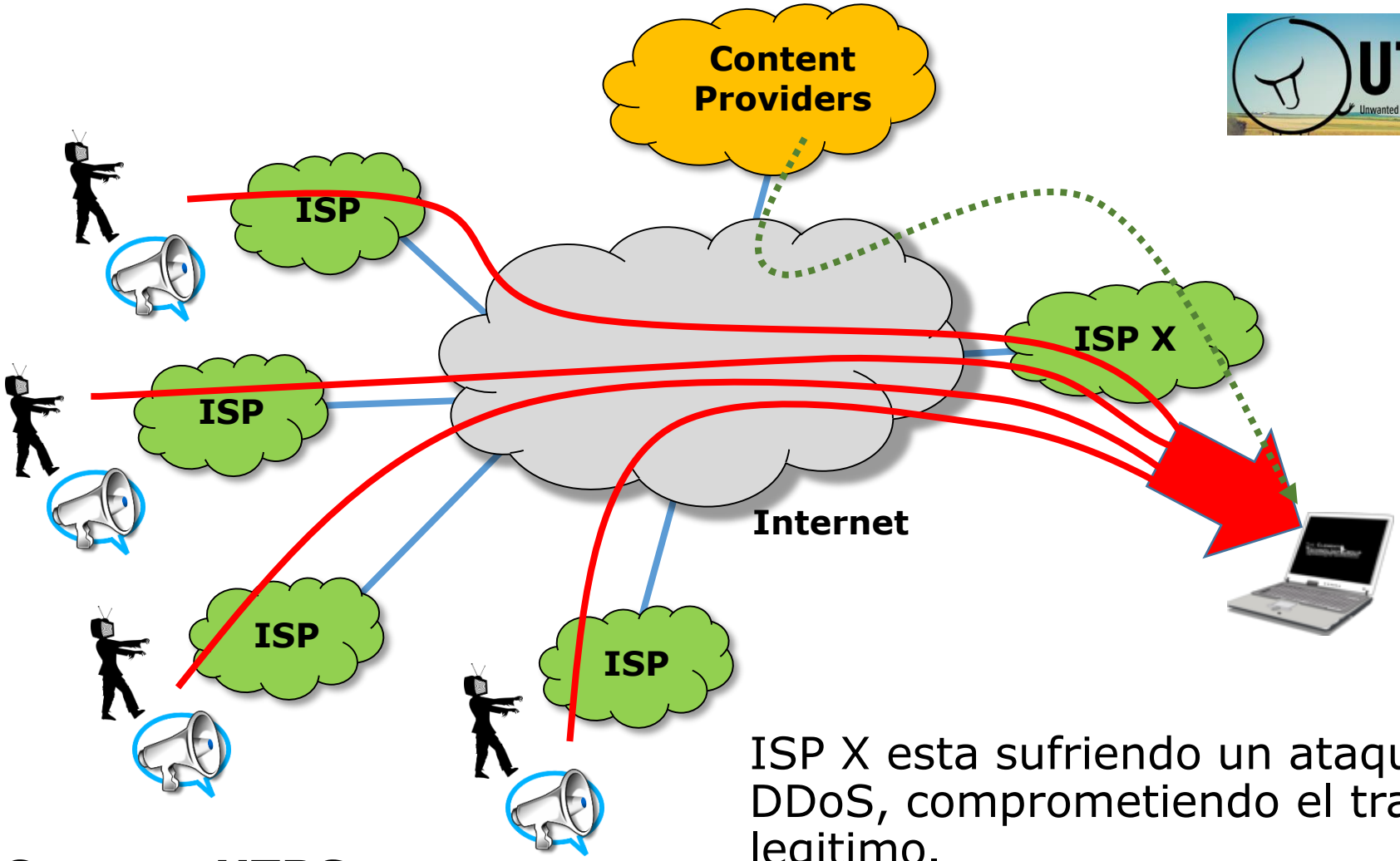
UTRS – Unwanted Traffic Removal



ISPs establecen sesiones BGP con Cymru para el servicio UTRS

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

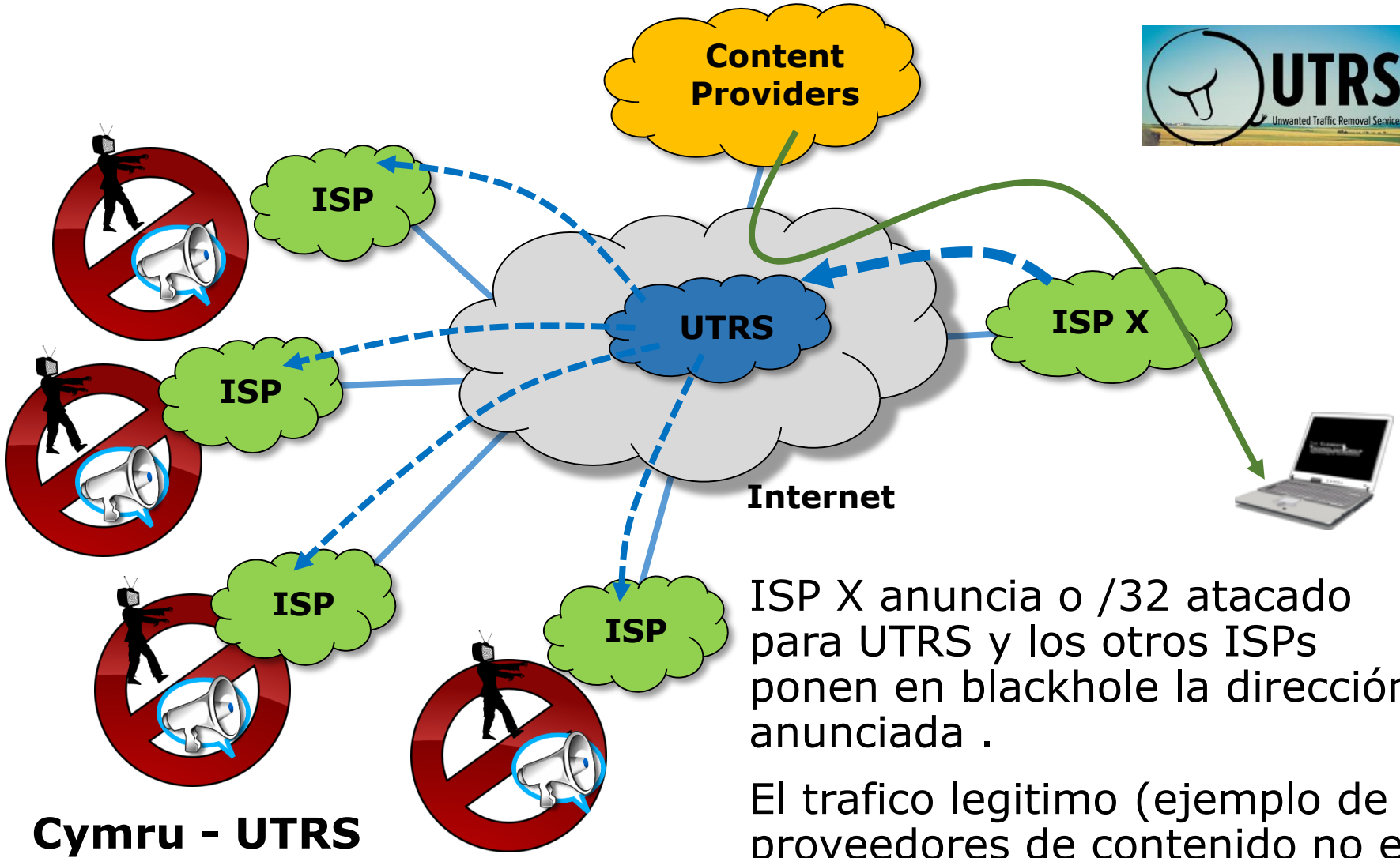
Cymru - UTRS



ISP X esta sufriendo un ataque DDoS, comprometiendo el trafico legitimo.

Cymru - UTRS

Cymru - UTRS



ISP X anuncia o /32 atacado para UTRS y los otros ISPs ponen en blackhole la dirección anunciada .

El trafico legitimo (ejemplo de proveedores de contenido no es afectado)

Ok, mitigación es posible, pero cuanto tiempo mi SLA será comprometido?

¿Cuanto tiempo del ataque hasta la mitigación?

Cualquier técnica de mitigación va a requerir una acción especifica, con cambio en los anuncios

Si el proceso es **manejado por humanos**, muchas chances hay de que el servicio sea comprometido por mucho, mucho tiempo…

Personas tienen que ser avisadas, y saber lo que hacer y hacerlo muy rápido.

Importante mencionar que en algunos ataques el acceso a el router puede ser comprometido de manera que hasta saber cual IP esta atacado puede ser complicado.

¿Cuanto tiempo del ataque hasta la mitigación?

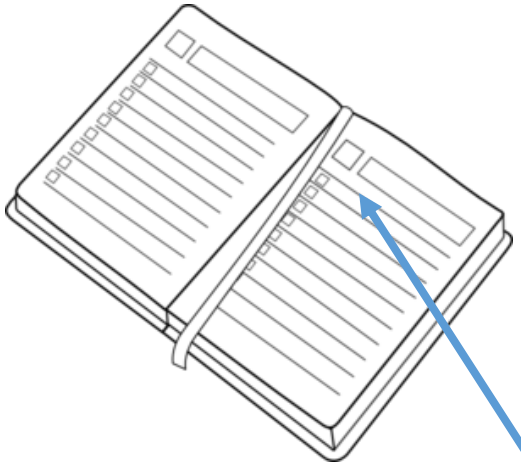
No hay chances para humanos acá..

Definitivamente necesitamos de una solución automática y rápida.

Sun Tzu – The art of war

In Peace, prepare for War…

Agenda



Recordatorio de DDoS – componentes, y arquitectura;

Enfrentamiento de los ataques – las buenas practicas en nuestra red para minimizarlos;

Enfrentamiento de los ataques – técnicas de mitigación posibles y sus implementaciones;

Automatizando la detección y mitigación en un ISP regional de Brasil

La cereza de la torta – Gráficos y informaciones sobre la red;

Automatizando la solución

Nuestra solución para mitigación de DDoS utiliza:

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

y una combinación de 2 herramientas open source:

→ **Fastnetmon**

→ **ExaBGP**

Detección de DDoS con Fastnetmon

El "corazón" de nuestra implementación es Fastnetmon

Fastnetmon es un analizador de ataques DoS/DDoS de alta performance que puede trabajar con muchos mecanismos de captura de pacotes, como:

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

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

ExaBGP

ExaBGP es un SDN BGP speaker construido en Python, conocido como el “Cuchillo Suizo” de BGP

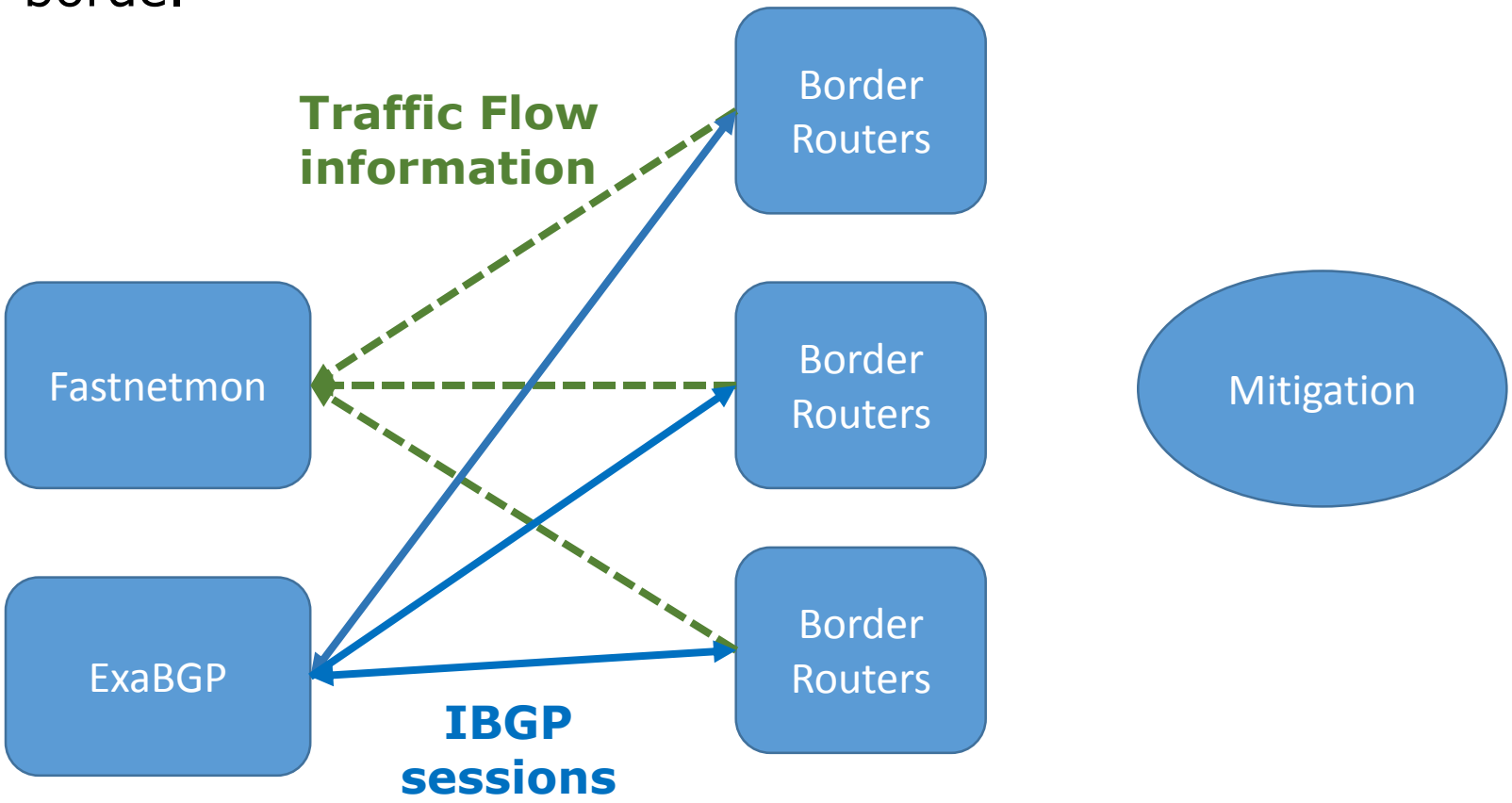
ExaBGP puede hacer muchas cosas relacionadas al protocolo que non son posibles hacer con un router real.

Es posible injertar rutas arbitrarias, obtener datos de ruteo, etc.

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

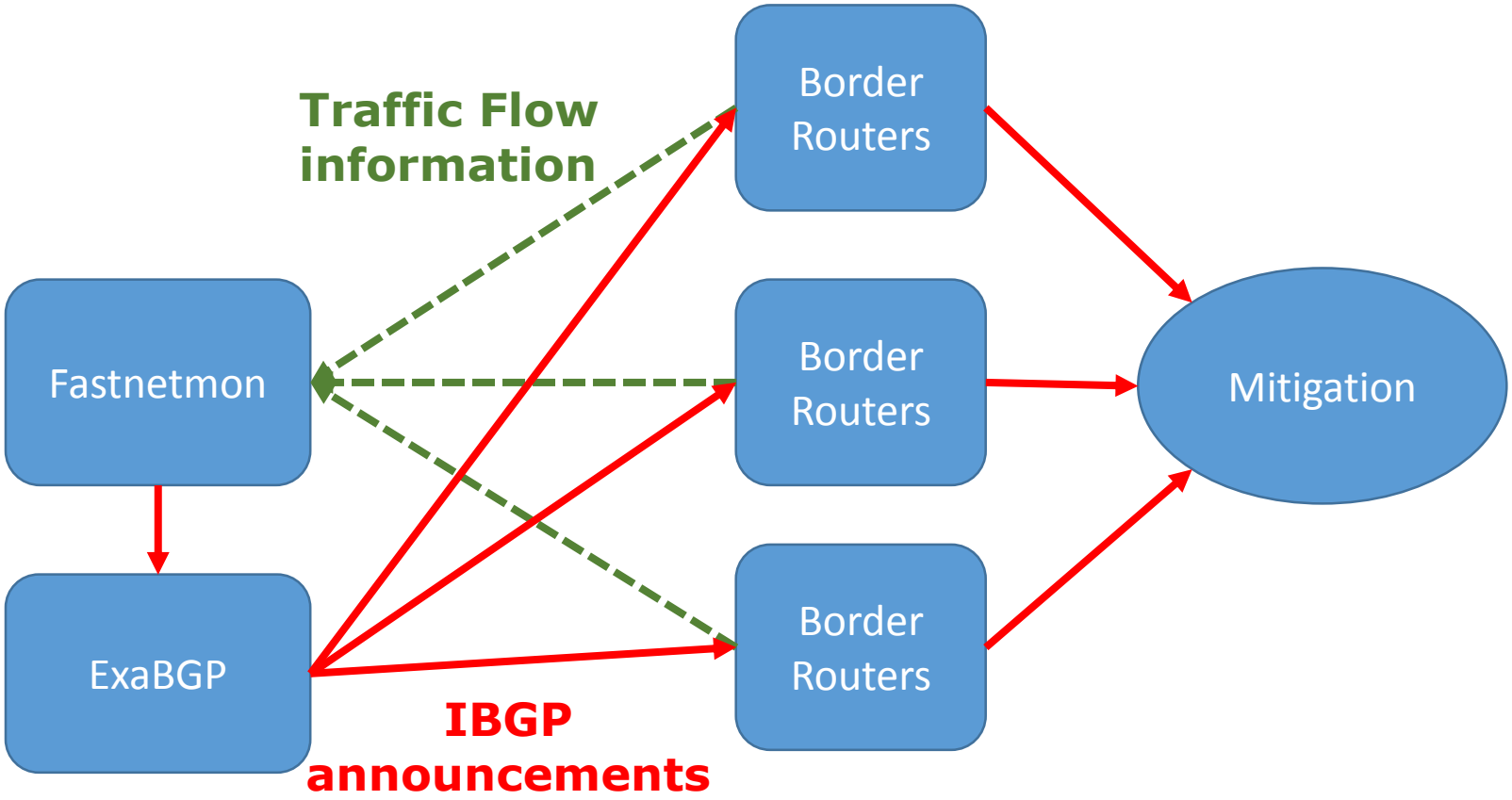
Esquema para detección y mitigación de DDoS

En condiciones normales los enrutadores de borde están enviando informaciones de Flows para Fastnetmon. ExaBGP tiene sesiones iBGP con los enrutadores de borde.



Esquema para detección y mitigación de DDoS

Cuando un DDoS es detectado, Fastnetmon dispara ExaBGP, que envía las rutas por iBGP con una community especifica para blackholing. Los enrutadores de borde anuncian dicha dirección para la solución de mitigación.



Instalación y configuración de Fastnetmon

Fastnetmon – Instalación y configuración

Instalador Automatico para Debian y CentOS

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

perl fastnetmon_install.pl

or

perl fastnetmon_install.pl --use git-master

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 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:~#
```

Fastnetmon – Instalación y configuración

Detalles de configuración

El fichero principal de configuración es un texto comprensible en:

/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 – Instalación y configuración

Configuración

Netflow configuration

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

netflow_port = 1234

netflow_host = 0.0.0.0

Ajuste la puerta de acuerdo con el router. IP puede ser mantenido 0.0.0.0, mas es mejor informar los IPs.

Fastnetmon – Instalación y configuración

Configuración – Thresholds

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

Integración con ExaBGP

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

Active exaBGP

Defina una community interna para blackholing

ExaBGP instalación y configuración

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

md brasil
TI&TELECOM

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:

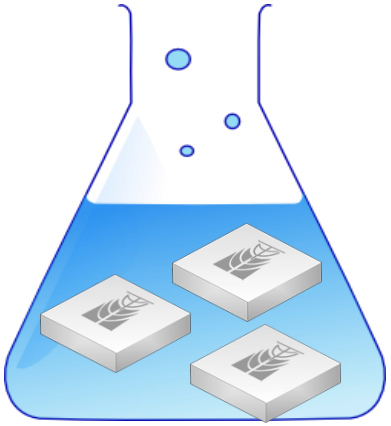
https://github.com/pavel-odintsov/fastnetmon/blob/master/docs/EXABGP_INTEGRATION.md

md brasil TI&TELECOM

Fastnetmon Client

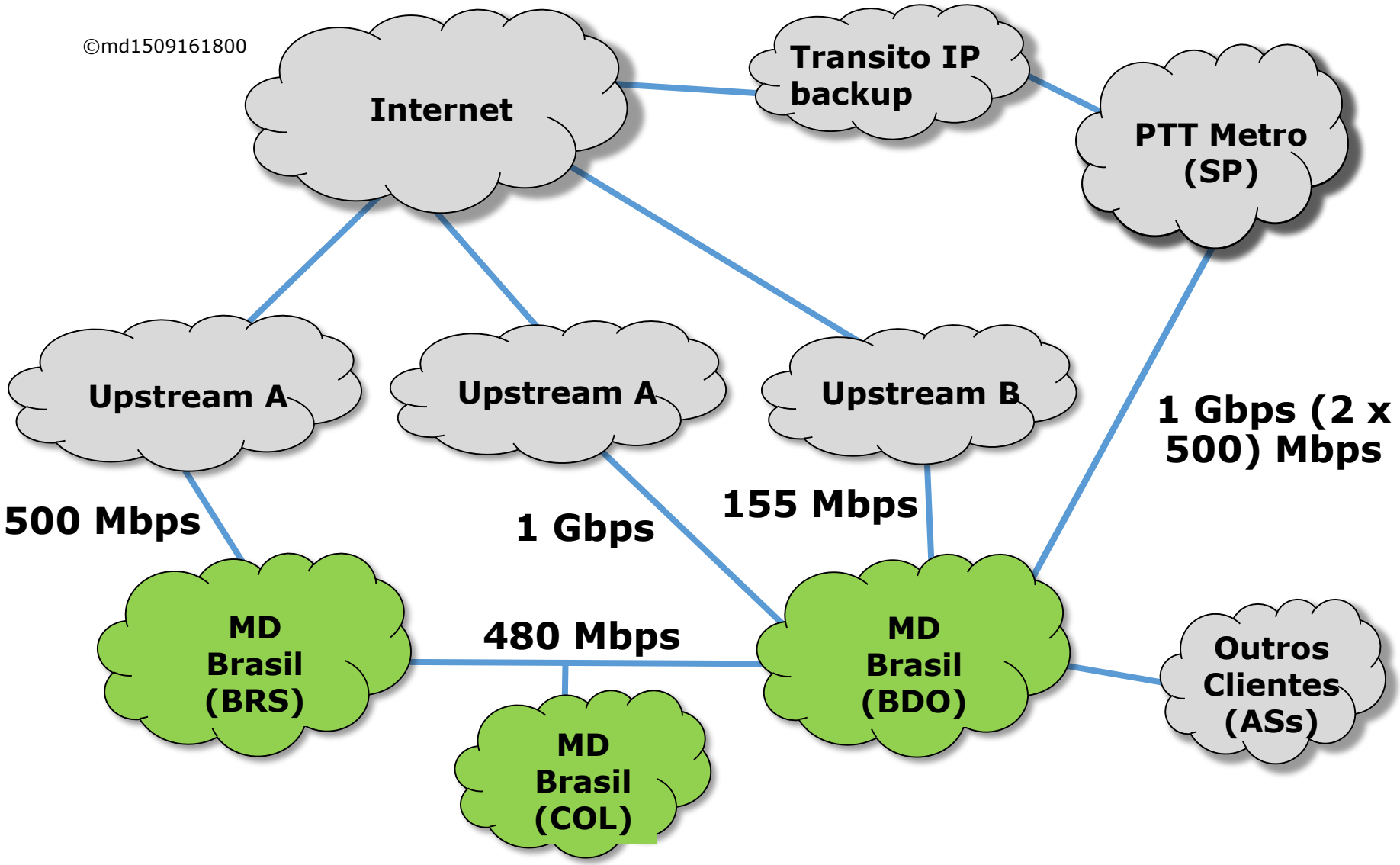
/opt/fastnetmon/fastnetmon_client

```
FastNetMon 1.1.3 master git-e298e77c9c72bb0f0cf063de41a0ad95e9d942de FastVPS Ees
ti 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]3.2               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]3.2               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
```

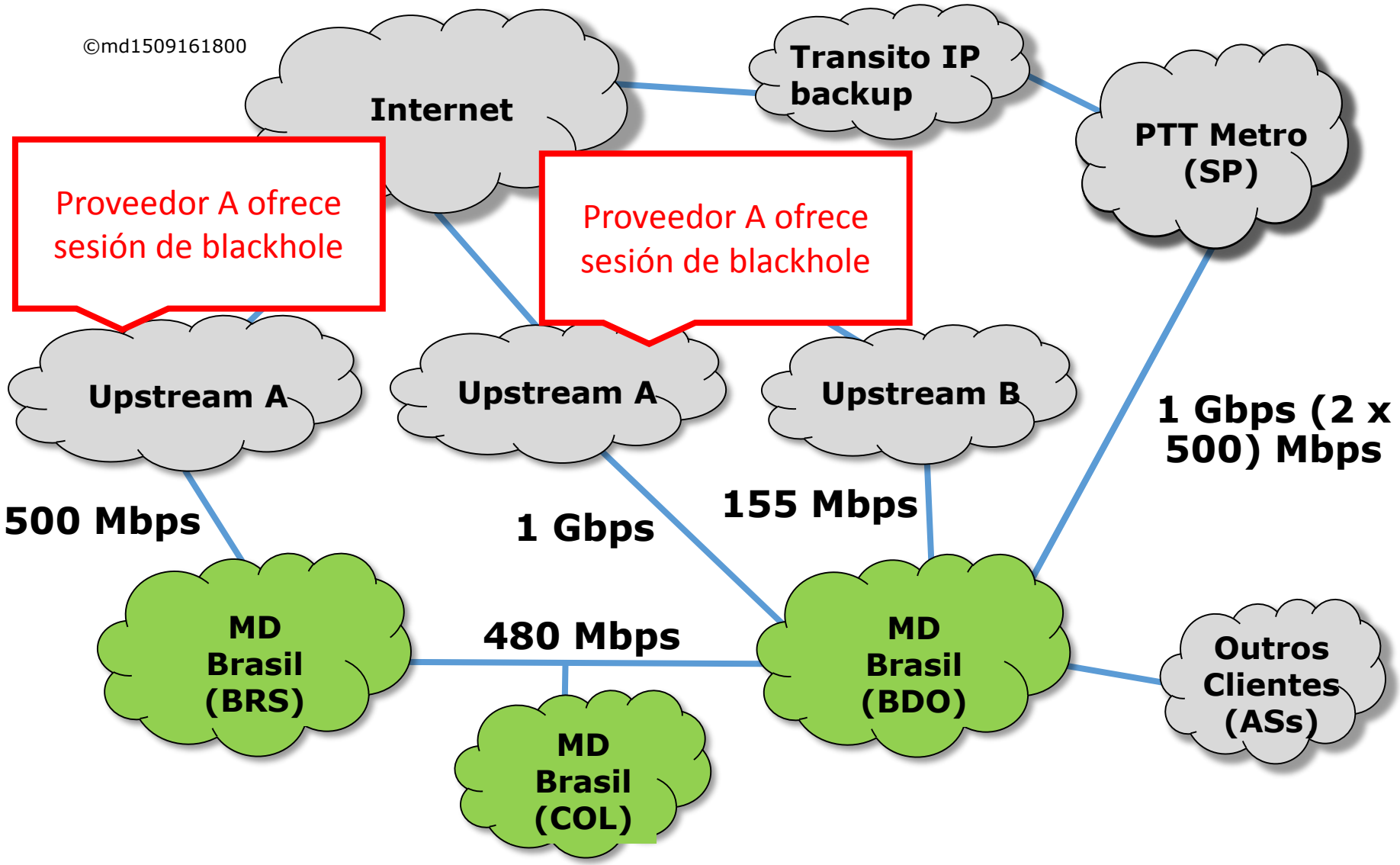


Implementación de caso concreto

Conectividad



Conectividad



Mitigación de DDoS

Proveedor de upstream A → ofrece sesión BGP exclusiva para anunciar blackhole.

→ Bajo ataque, anunciar red /24 más especifica por proveedor A en la sesión normal y el /32 atacado en la sesión de blackhole.

→ Estamos tentando viabilizar un grupo de ISP regionales para hacer un contrato con operador de mitigación.

Agenda

Recordatorio de DDoS – componentes, y arquitectura;

Enfrentamiento de los ataques – las buenas practicas en nuestra red para minimizarlos;

Enfrentamiento de los ataques – técnicas de mitigación posibles y sus implementaciones;

Automatizando la detección y mitigación en un ISP regional de Brasil

La cereza de la torta – Gráficos y informaciones sobre la red;

md brasil
TI&TELECOM

Otras implementaciones

NetHealer

NetHealer es una implementación que recibe los reportes de Fastnetmon y automatiza el proceso. (pero utiliza BIRD para el BGP).

Es una implementación exitosa empleada en un proveedor de servicios de Help Desk

https://github.com/zenvdeluca/net_healer

Vicente de Luca, de Zendesk – autor de NetHealer

La “cereza” de la torta

Con la instalación de Fastnetmon y otras herramientas, nosotros podemos mejorar nuestra implementación para tenernos más información y control de nuestra red.

Para eso, además de Fastnetmon, vamos necesitar otras herramientas:

InfluxDB + Grafana

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

InfluxDB

InfluxDB é un software open source para base de datos para series temporales sin dependencias externas. Es muy útil para registro y análisis de métricas y eventos.

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

Grafana

Grafana es otro open source empleado para presentar un dashboard e gráficos, utilizando diversas bases de datos como Graphite, Elasticsearch, OpenTSDB, Prometheus y InfluxDB

https://github.com/grafana/grafana

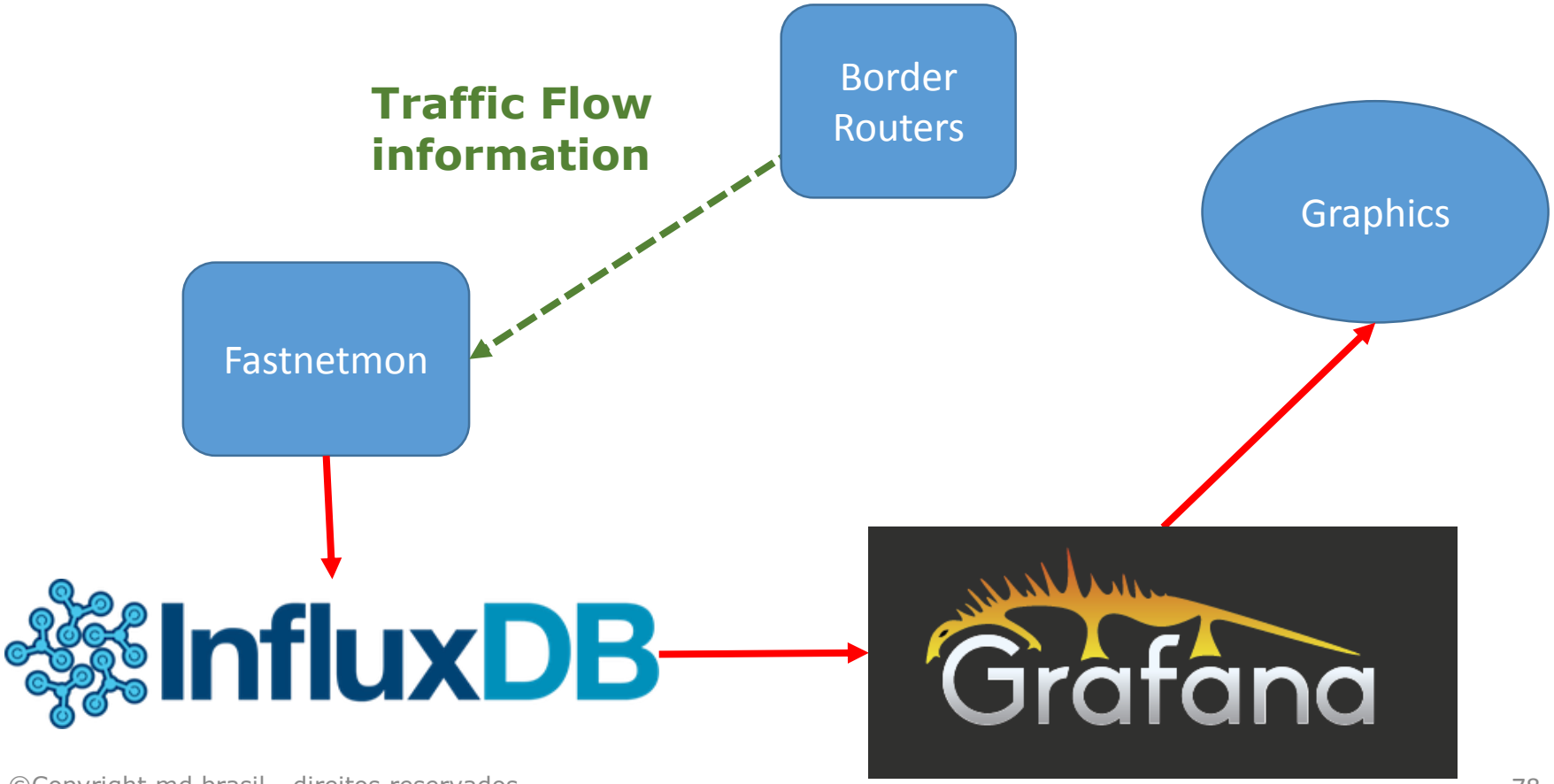
Instalación para Debian/Ubuntu

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

sudo dpkg -i grafana_2.6.0_amd64.deb

Esquema para detección y mitigación de DDoS

Integración de Fastnetmon + InfluxDB + Grafana



Fastnetmon + InfluxDB + Grafana

Este es un típico dashboard que se puede visualizar con la combinación de las herramientas

Agenda

Recordatorio de DDoS – componentes, y arquitectura;

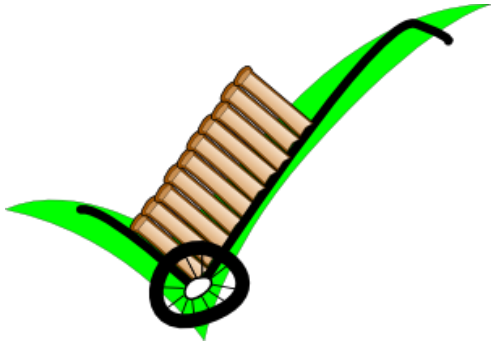
Enfrentamiento de los ataques – las buenas practicas en nuestra red para minimizarlos;

Enfrentamiento de los ataques – técnicas de mitigación posibles y sus implementaciones;

Automatizando la detección y mitigación en un ISP regional de Brasil

La cereza de la torta – Gráficos y informaciones sobre la red;

References



Defeating DDoS – Cisco White paper

Anatomy of a DDoS attack – Team Cymru

Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)

BGP and Security workshop by Tom Smyth (Wireless Connect, Ireland)

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

Preguntas?

Gracias!