DDoS
Ataques distribuídos de negação de serviço

Importância, conceitos e técnicas para detecção e mitigação

MUM Brasil
Belo Horizonte – novembro 2016
Wardner Maia

Introdução

Wardner Maia

Engenheiro – Eletrônica e Telecomunicações;
ISP desde 1995;
Treinamentos para ISPs desde 2002;
Diretor técnico da MD Brasil IT & Telecom;
Diretor do LACNIC.

Introdução

MD Brasil IT & Telecom

Provedor de acesso à Internet no interior de SP;
Integração de equipamentos de telecomunicações;
Treinamentos e capacitação para ISPs;
Serviços de consultoria.

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

DDoS – Detecção e Mitigação

Por que este tema?

DDoS – Devo me preocupar?

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

Devemos estar prontos para cada vez maiores ataques!

DDoS – Devo me preocupar?

Ataque à estrutura da Dyn em outubro de 2016.

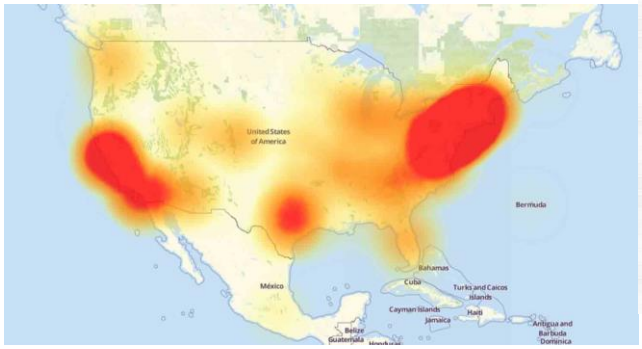
BusinessSolutions
Growth Strategies For The IT Channel

Home | Technology Centers | Channel Topics | Magazine | Blog | Channel Conferences

News Feature | November 2, 2016

DDoS Attack On Dyn Demonstrates Need For Serious Cybersecurity Investment

By Christine Kern, contributing writer



News | Regions | People | Data | Videos & Webinars

News feed Cisco partners with R_

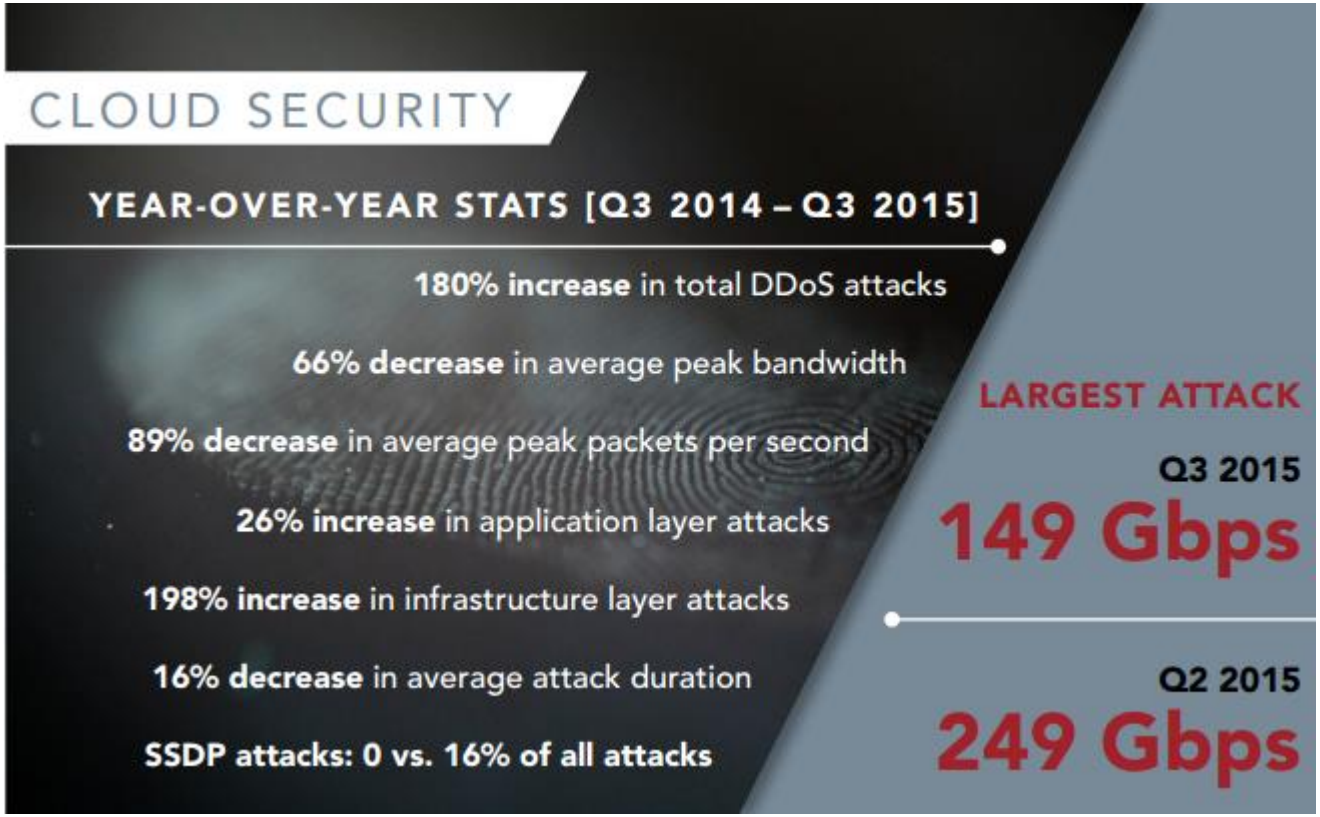
Home :: Markets :: Backhaul :: Oracle buys Dyn a month after DDoS attack

Oracle buys Dyn a month after DDoS attack

Ataques DDoS são “privilégio” dos grandes operadores e grandes datacenters?

Minha (pequena/média) empresa pode vir a ser um alvo?

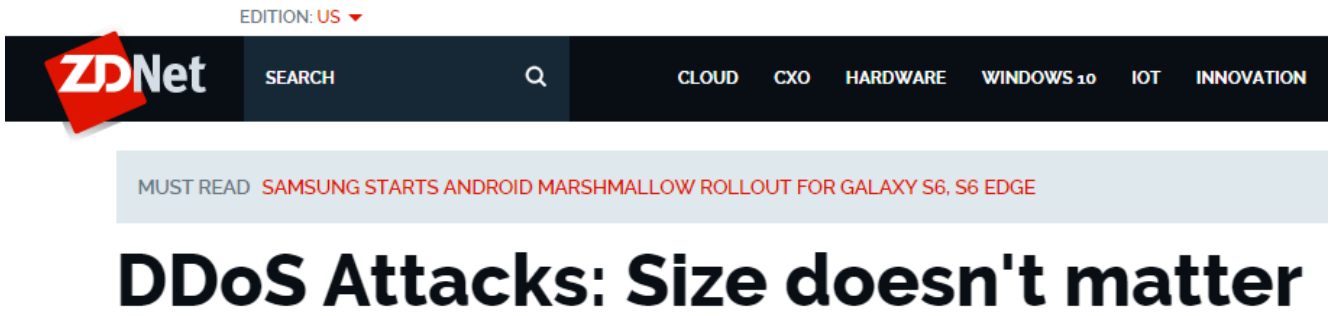
DDoS – devo me preocupar?



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

DDoS – devo me preocupar?

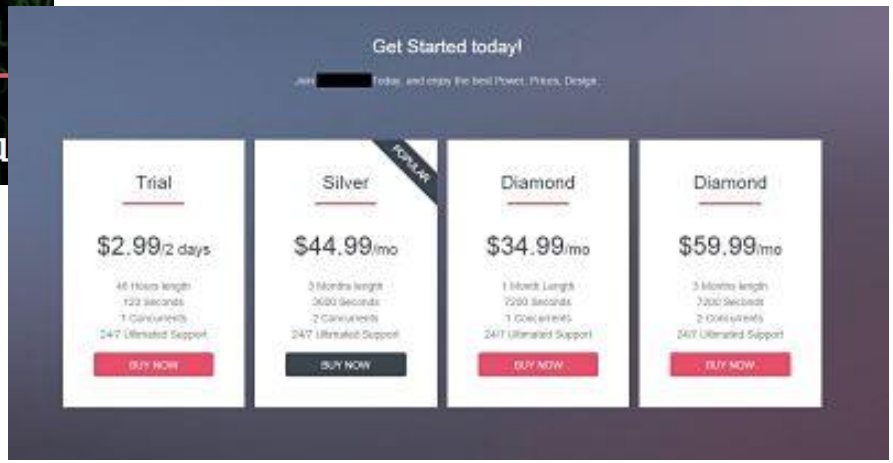
http://www.pcworld.com/article/3012963/security/ddos-attacks-increase-in-number-endanger-small-organizations.html



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

DDoS – devo me preocupar?

Que tal contratar um ataque de DDoS por US$ 2.99?



DDoS – devo me preocupar?

Ser alvo de un ataque de DDoS não é uma questão de "se", mas de quando isso vai acontecer!

Temos um plano formal de respostas a incidentes?

DDoS – detecção e mitigação

Para quem é essa apresentação?

Público alvo e objetivos

Esta apresentação tem como público alvo, pequenos e médios ISPs que trabalham como provedores de última milha;

Os principais objetivos dessa apresentação são: mostrar a importância dos ataques, os conceitos envolvidos e principalmente de ter um plano contra os ataques e as sugestões de como implementa-los.

Serão utilizadas basicamente ferramentas open source.

- Será apresentado un caso real de implementação em um provedor regional;

Agenda

Conceitos de DDoS – componentes, y arquitetura;

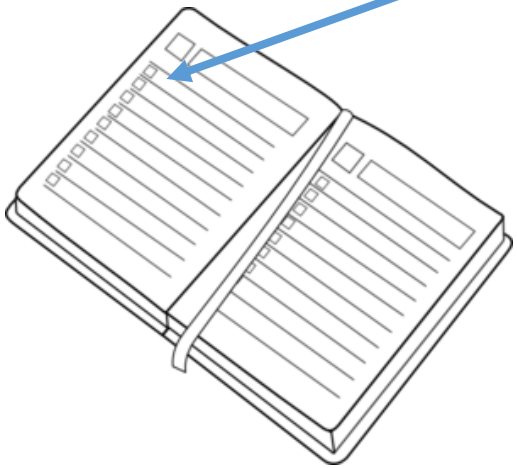
Enfrentamento dos ataques – as boas práticas em nossa rede para minimiza-los;

Enfrentamento dos ataques – técnicas de mitigação possíveis e suas implementações;

Automatizando a detecção e mitigação em um ISP regional no Brasil;

A “cereja do bolo” – Gráficos e informações detalhadas da rede;

Agenda



Conceitos de DDoS – componentes, y arquitetura;

Enfrentamento dos ataques – as boas práticas em nossa rede para minimiza-los;

Enfrentamento dos ataques – técnicas de mitigação possíveis e suas implementações;

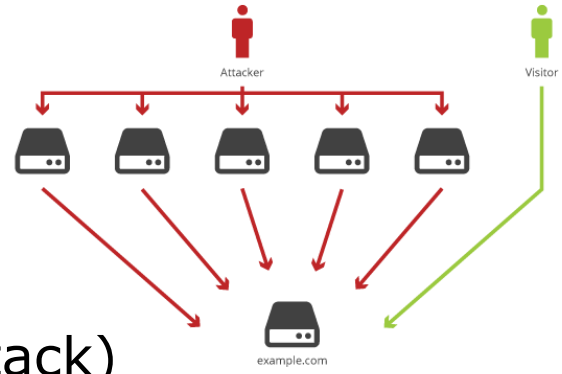
Automatizando a detecção e mitigação em um ISP regional no Brasil;

A “cereja do bolo” – Gráficos e informações detalhadas da rede;

Conceitos básicos de DDoS

Terminologia

DoS (Denial of Service Attack)
Ataques de Negação de Serviço



DDoS (Distributed Denial of Service Attack)
Ataques de Negação de serviço Distribuidos

DRDoS (Distributed Reflected Denial of Service Attack)
Ataques de Negação de Serviço Distribuidos Amplificados

Tipos de ataques Dos

1. Ataques à camada de aplicação

Tem como objetivo a saturação de recursos, explorando as características da camada 7;

- Não necessitam muitas máquinas e nem muitos recursos de largura de banda para sua realização.
- Exemplos: HTTP POST, HTTP GET, SIP Invite flood, etc

Tipos de ataques Dos

2. Ataques de consumo aos recursos de hardware

Tentam consumir recursos como CPU e memória, de equipamentos de rede, como roteadores e Firewalls.

- Exemplos: fragmentação e SYN flood

Tipos de ataques Dos

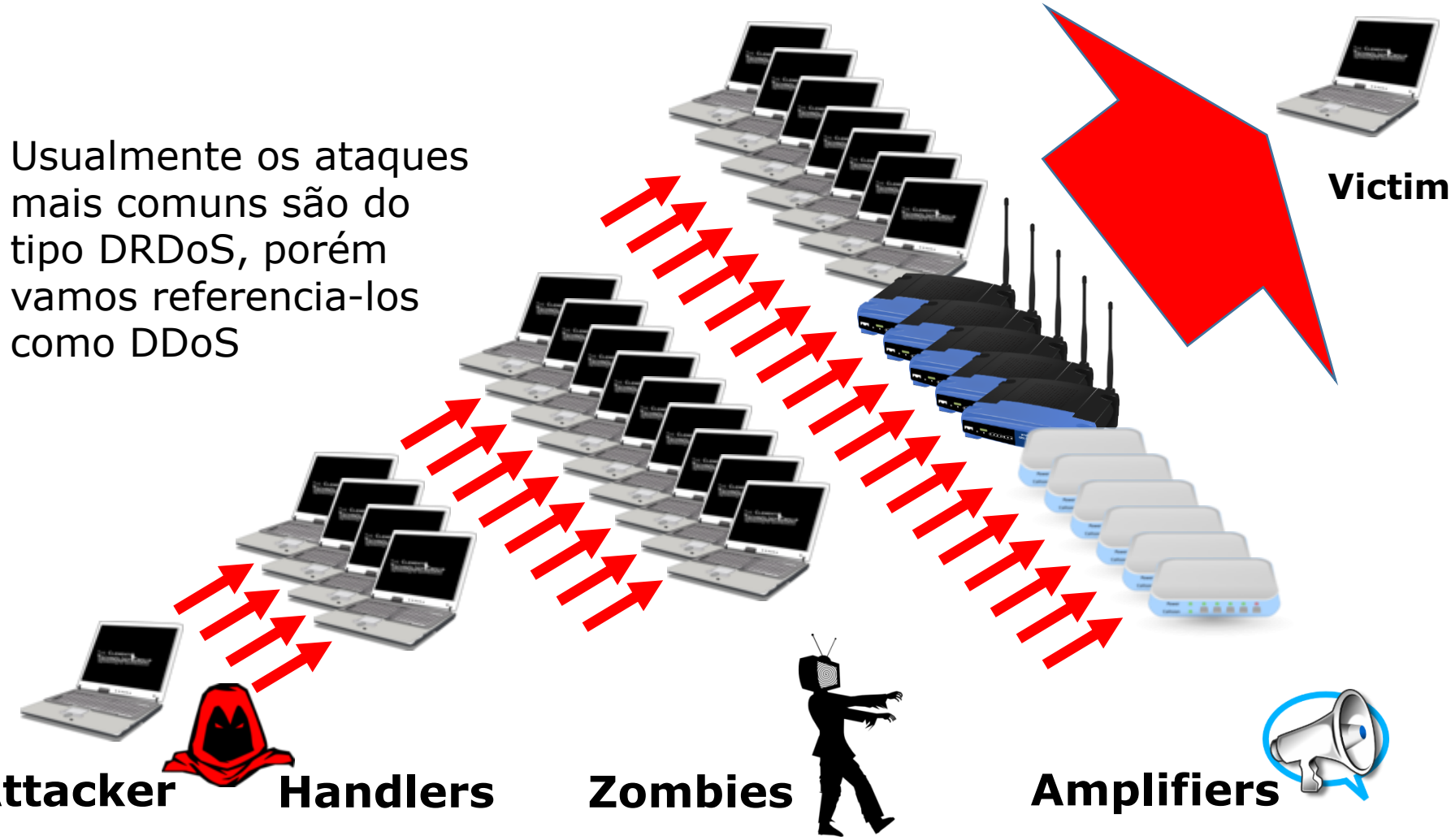
3. Ataques volumétricos

Tem como objetivo consumir os recursos de largura de banda de um link.

- Utilizam Botnets, máquinas comprometidas y equipamentos mal configurados que permitem a amplificação de requisições.
- Fazem o Spoof do IP da vitima para forçar respostas amplificadas a ela.

Anatomia de um ataque DRDoS

Usualmente os ataques mais comuns são do tipo DRDoS, porém vamos referencia-los como DDoS



Esquema de ataque DDoS utilizando amplificação de DNS

Vítima

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

Esquema de ataque DDoS utilizando amplificação de DNS

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

Esquema de ataque DDoS utilizando amplificação de DNS

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

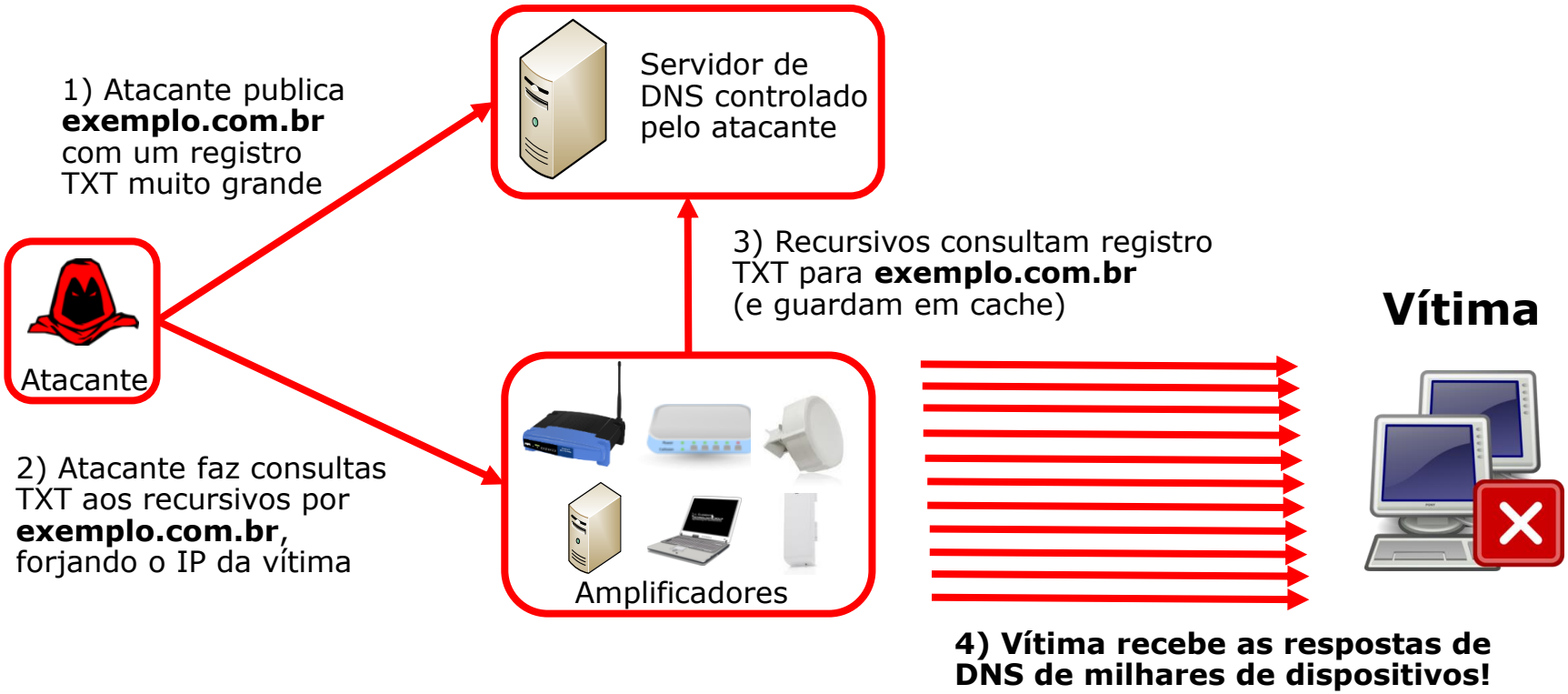
md brasil
TI&TELECOM

Esquema de ataque DDoS utilizando amplificação de DNS

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

md brasil
TI&TELECOM

Esquema de ataque DDoS utilizando amplificação de DNS

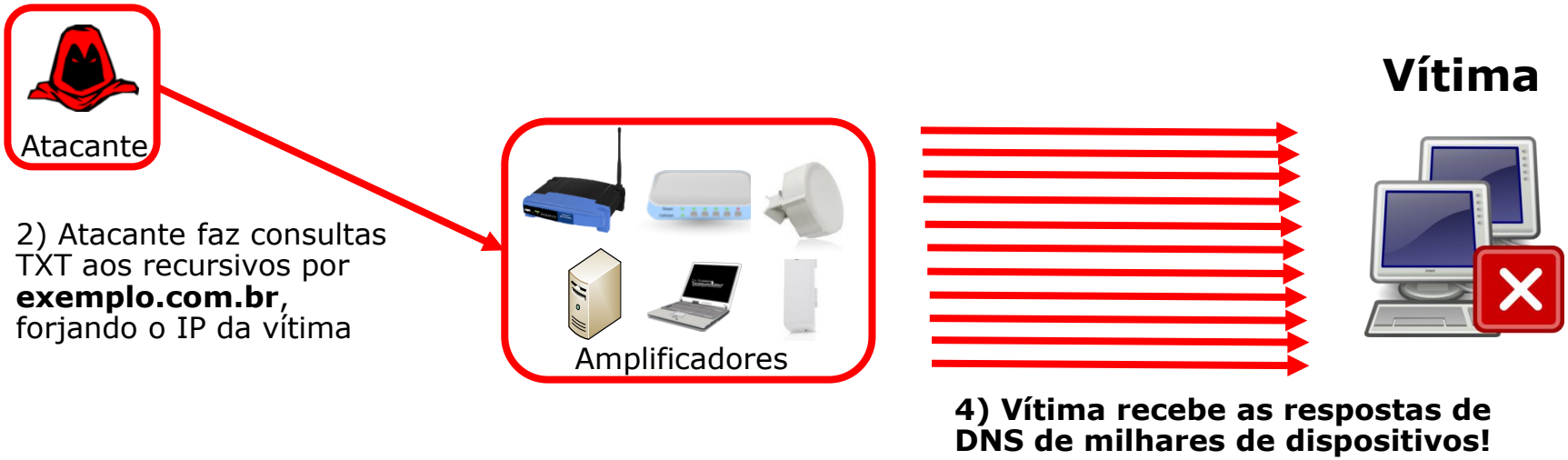


fonte: http://cert.br/docs/whitepapers/ddos

md brasil TI&TELECOM

Esquema de ataque DDoS utilizando amplificação de DNS

Uma vez que os resultados encontram-se nos caches dos amplificadores, a consulta com endereço forjado já provoca imediatamente o grande volume de respostas.



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

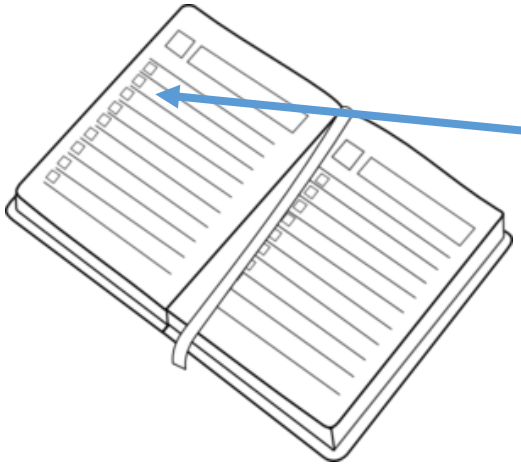
Amplificadores

Fatores de amplificação

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



Conceitos de DDoS – componentes, y arquitetura;

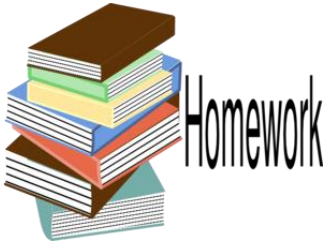
Enfrentamento dos ataques – as boas práticas em nossa rede para minimiza-los;

Enfrentamento dos ataques – técnicas de mitigação possíveis e suas implementações;

Automatizando a detecção e mitigação em um ISP regional no Brasil;

A "cereja do bolo" – Gráficos e informações detalhadas da rede;

Lições de casa



Facilitadores de DDoS

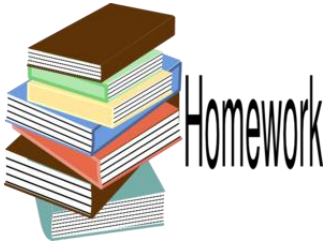
Máquinas comprometidas

Servidores o serviços mal configurados

ISPs que não implementam BCP-38 em seus upstreams

Roteio para endereços bogons

Lições de casa



Implementação de BCP-38

Basicamente consiste em evitar o spoof de endereços IP

→ Através de regras de Firewall e ou uRPF

Como regra geral em nossa rede foi implementado:

→ uRPF no modo “strict” para os roteadores de acesso

→ uRPF no modo “loose” para os roteadores de Borda

BCP-38 – Se todos implementassem, inexistiria spoof e portanto não mais DRDoS

Lições 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

Lições de casa

Procurando amplificadores

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

```
 % dig @201.[redacted]6 +edns=0 +ignore com ANY | grep rcvd
;; MSG SIZE  rcvd: 243
```

Como neste caso a resposta é maior que a requisição de 60 bytes, o dispositivo és um amplificador.

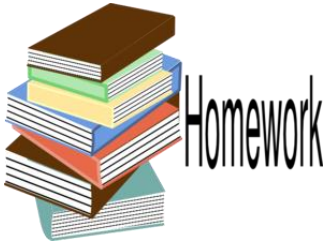
Mitigação:

Forçar TCP modo TCP;

Assegurar resolvedores recursivos (Link);

Empregar Rate-limit nos servidores autoritativos (Link).

Lições de casa



NTP: ntpdc –nc monlist x.x.x.x

Cada linha é um pacote UDP com 468 bytes

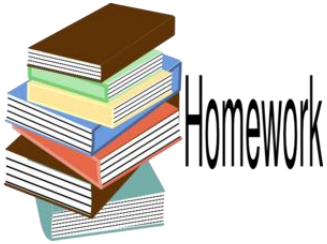
Mitigação:

A melhor solução é desabilitar monlist nos servidores NTP. Em ntp.conf:

restrict default no query

Outra opção é filtrar os pacotes UDP com porta de origen 123 e tamanho de pacote 468

Lições de casa



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

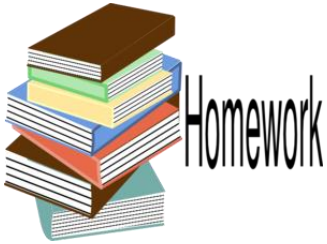
Checa pela vulnerabilidade mais comum. public é o nome default para la comunidade SNMP e 1.3 significa iso.org request OID.

Mitigação:

Importante no utilizar o valor default “public”

Recomendável restringir a faixa de endereços IP que podem acessar o SNMP

Lições de casa



NetBios: nmblookup –A x.x.x.x

Mitigação:

Filtrar requisições NB y NBSTAT de redes externas.

Lições de casa

SSDP: enviar um pacote UDP com destino a porta 1900 e o seguinte conteúdo:

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

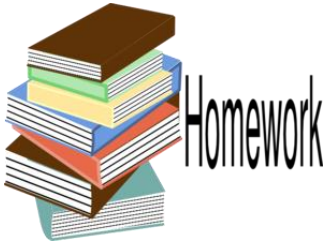
\r\n

Há tamben o script abaixo:

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

Mitigação: restringir faixas de endereços de IP e ou deshabilitar UPnP onde não necessário.

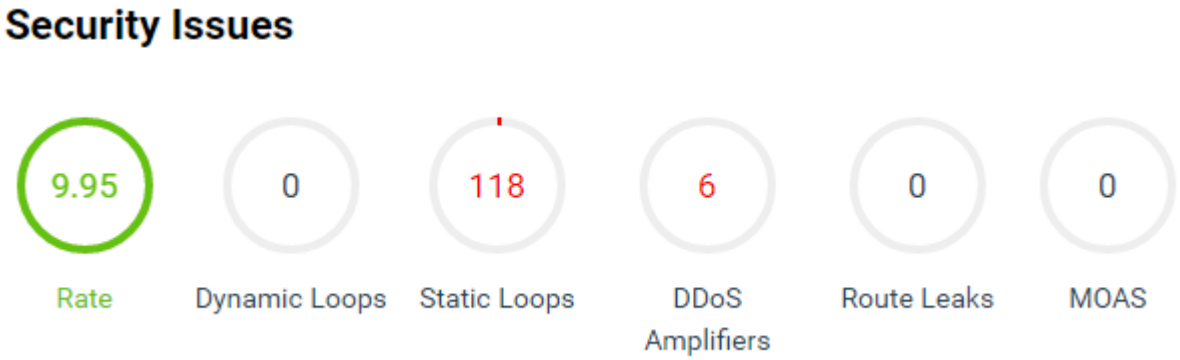
Lições de casa



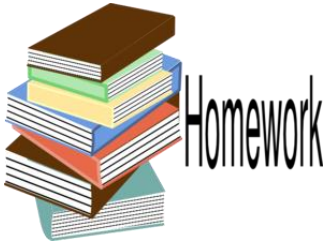
Procurando amplificadores

Um bom site que ajuda nesta busca é

http://radar.qrator.net



Lições de casa



Blackholing para endereços BOGONs

Assinar o serviço (gratuito) de Bogons de Team Cymru e colocar em blackhole os prefixos 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

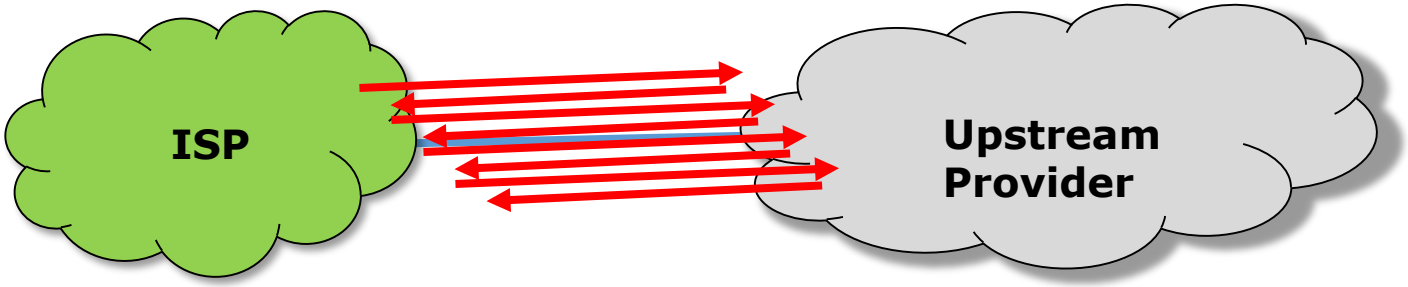
We will typically provide multiple peering sessions (at least 2) per remote peer for redundancy. If you would like more or less than 2 sessions please note that in your request. We try to respond to new peering requests within one to two business days, but, again, can provide no guarantees for this **free**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

Lições de casa

Eliminar loopings estáticos

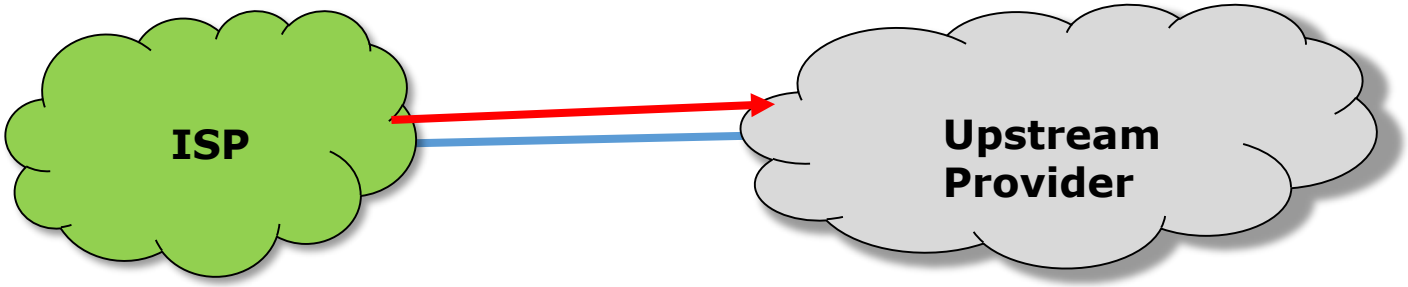
→ Assegurar que todo seu espaço anunciado no BGP tem rotas internas para suas redes, evitando assim os **loopings estáticos;**



Se não há rotas internas e o espaço tem que ser anunciado, assegurar-se de colocar em blackhole a parte não utilizada.

Reduzir o espaço de exposição

→ Reduzir o espaço de exposição aos ataques aos ataques DDoS anunciando os blocos não utilizados como blackhole



OBS: Depende da existência de uma política em seu(s) provedores de conectividade.

Lições de casa

Exemplo de redução quando se utiliza /30 para enlaces dedicados

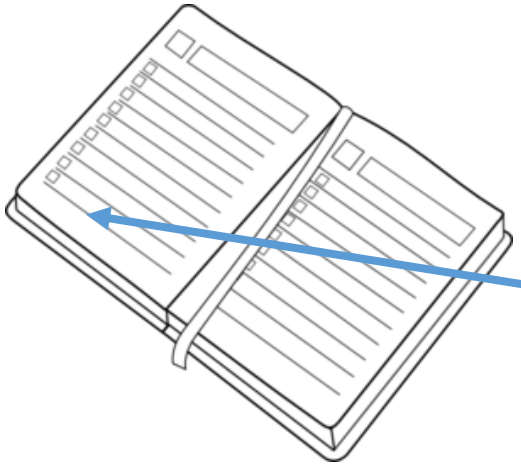
1.1.1.0/30 - 1.1.1.0 (endereço de rede)

- 1.1.1.1 (endereço do routeador do ISP)
- **1.1.1.2 (endereço do cliente)**
- 1.1.1.3 (endereço de broadcast)

Somente o endereço IP do cliente necessita conectividade (e em alguns casos nem este) a Internet. Os outros se podem colocar em blackhole, ***reduzindo 75% do espaço de exposição!***

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

Agenda



Conceitos de DDoS – componentes, y arquitetura;

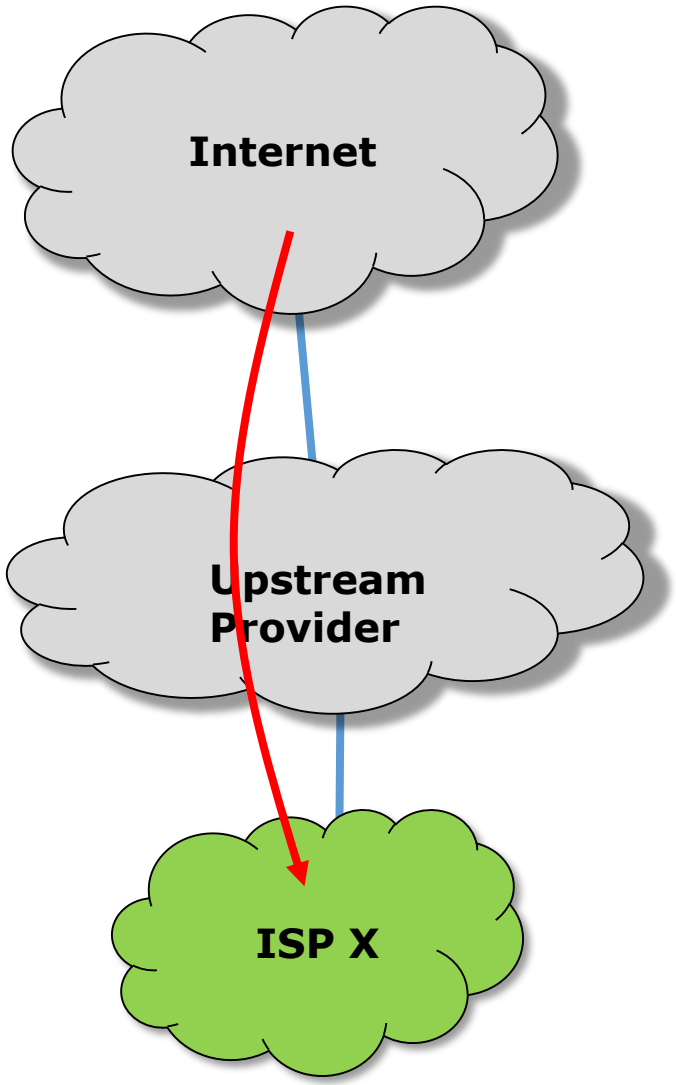
Enfrentamento dos ataques – as boas práticas em nossa rede para minimiza-los;

Enfrentamento dos ataques – técnicas de mitigação possíveis e suas implementações;

Automatizando a detecção e mitigação em um ISP regional no Brasil;

A "cereja do bolo" – Gráficos e informações detalhadas da rede;

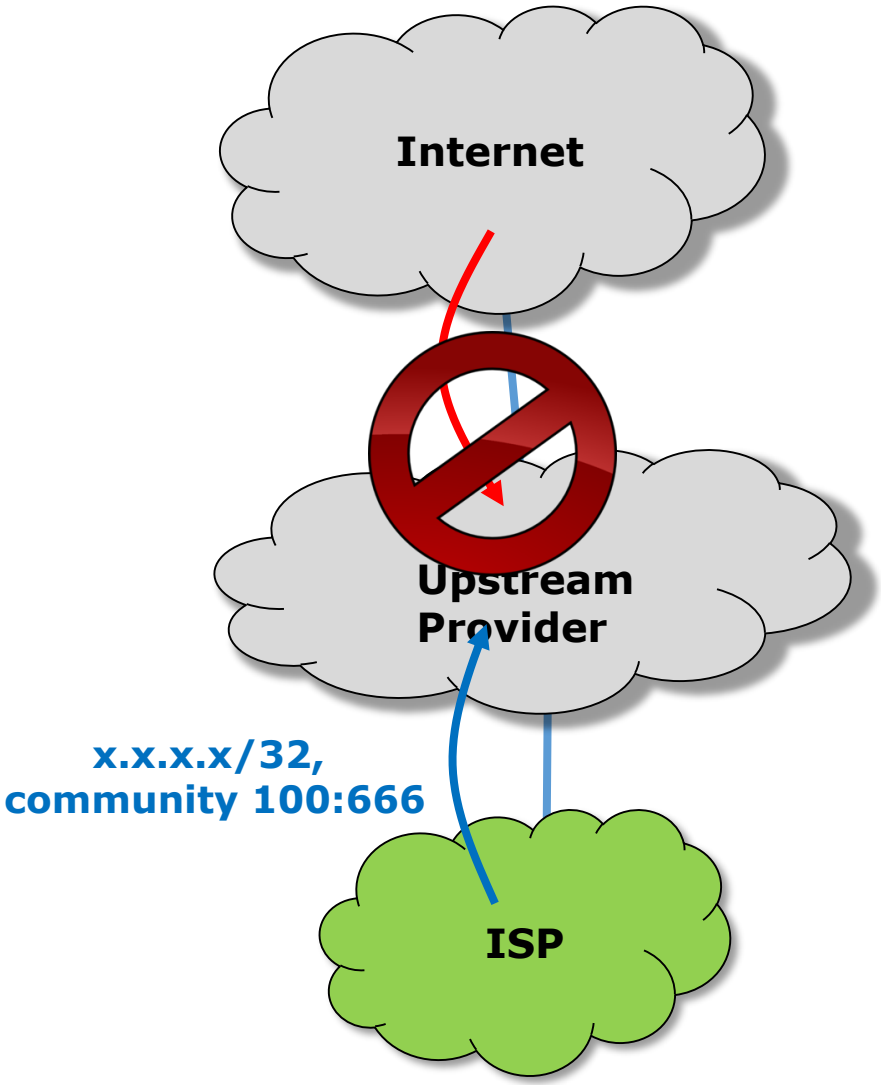
Blackhole acionado remotamente (RTBH)



O ISP X está sofrendo um ataque DDoS direcionado para o IP x.x.x.x/32, causando a inundação do link;

Seu provedor de upstream (exemplo AS 100) tem uma política que coloca em blackhole os anúncios /32 que tenha uma community determinada (exemplo 100:666);

Blackhole remotamente acionado (RTBH)



O ISP anuncia para seu upstream o endereço IP /32 atacado com a community 100:666;

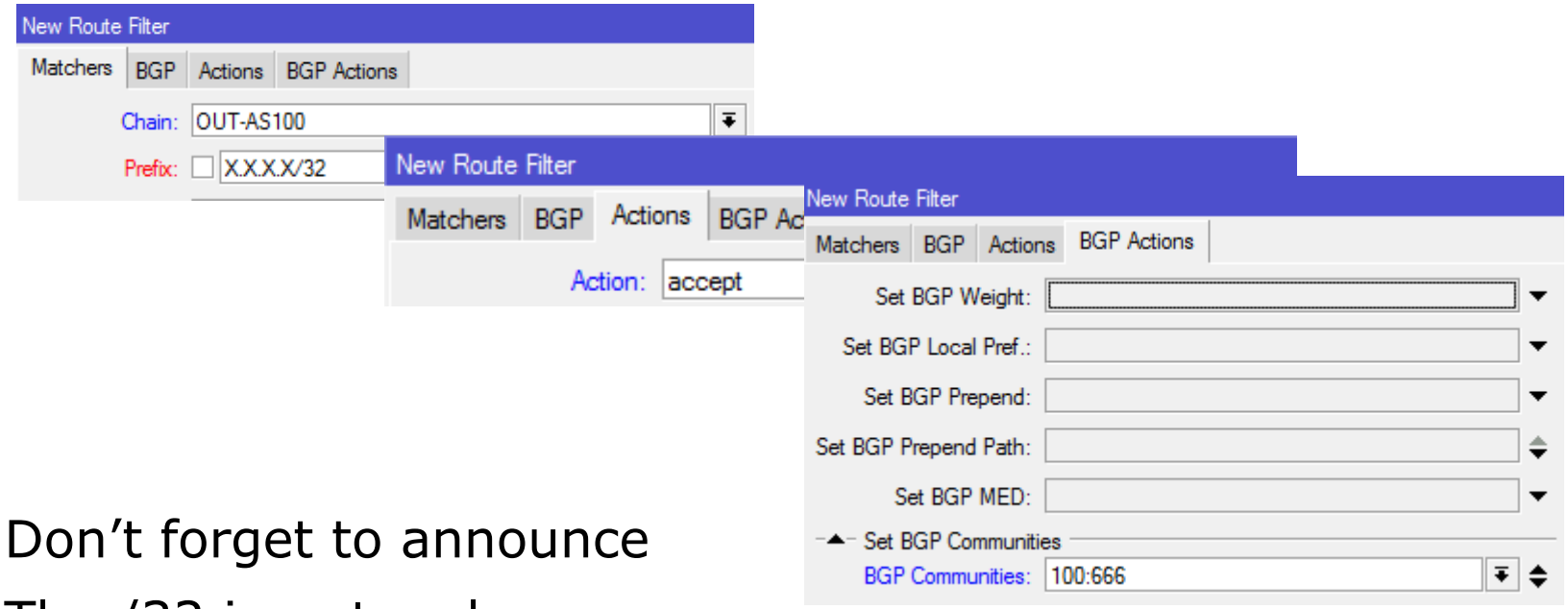
O Upstream tem filtros que reconhecem a community e automaticamente colocam o endereço anunciado em blackhole;

A comunicação com este /32 é perdida, porém cessa a inundação do link;

O SLA dos outros clientes é preservado, porém podemos dizer que o ataque teve sucesso ☹

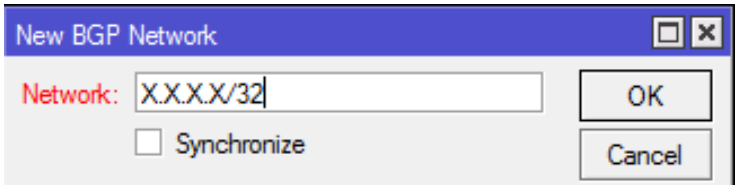
Implementation on RouterOS:

Make the filter:

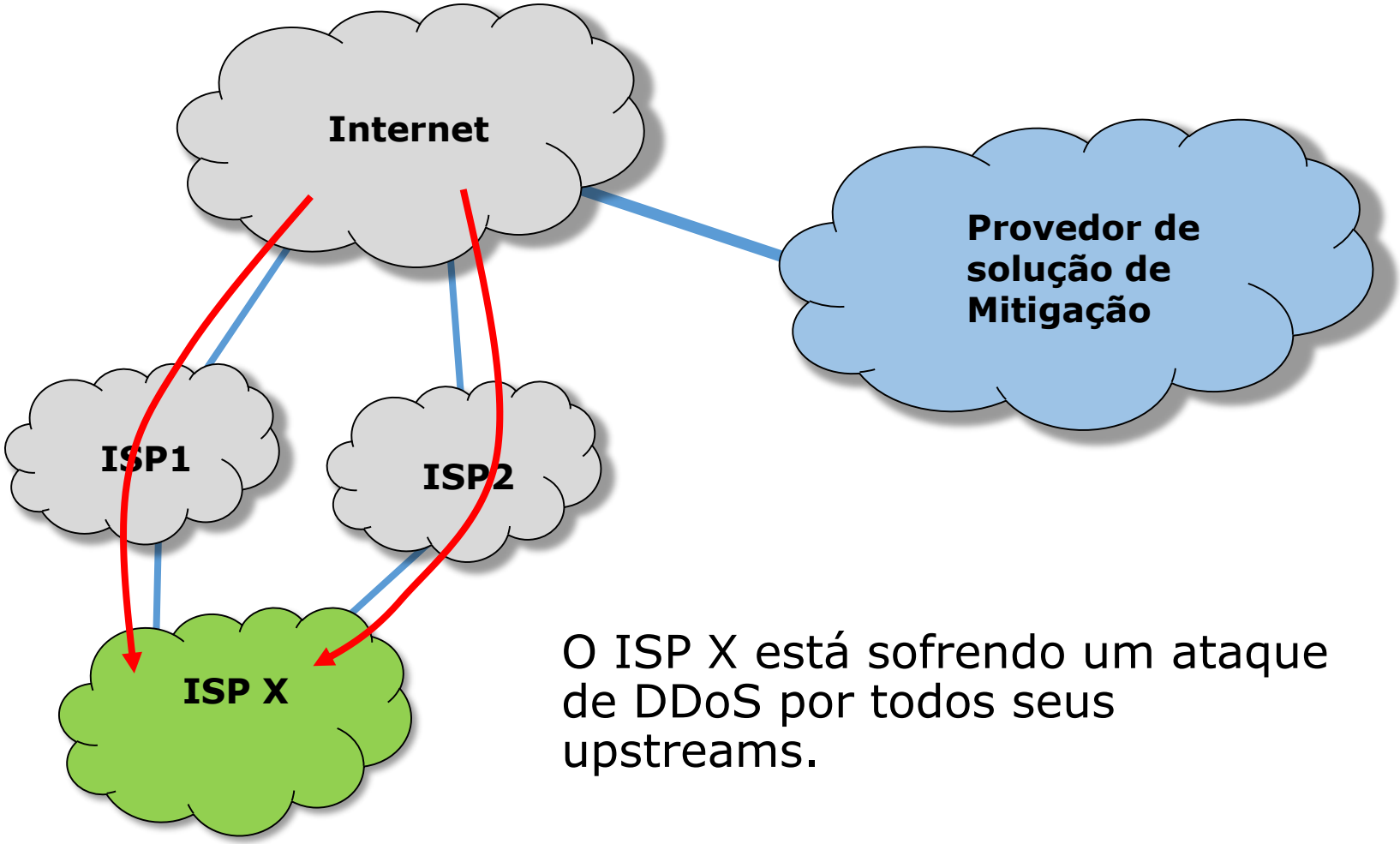


Don’t forget to announce

The /32 in networks

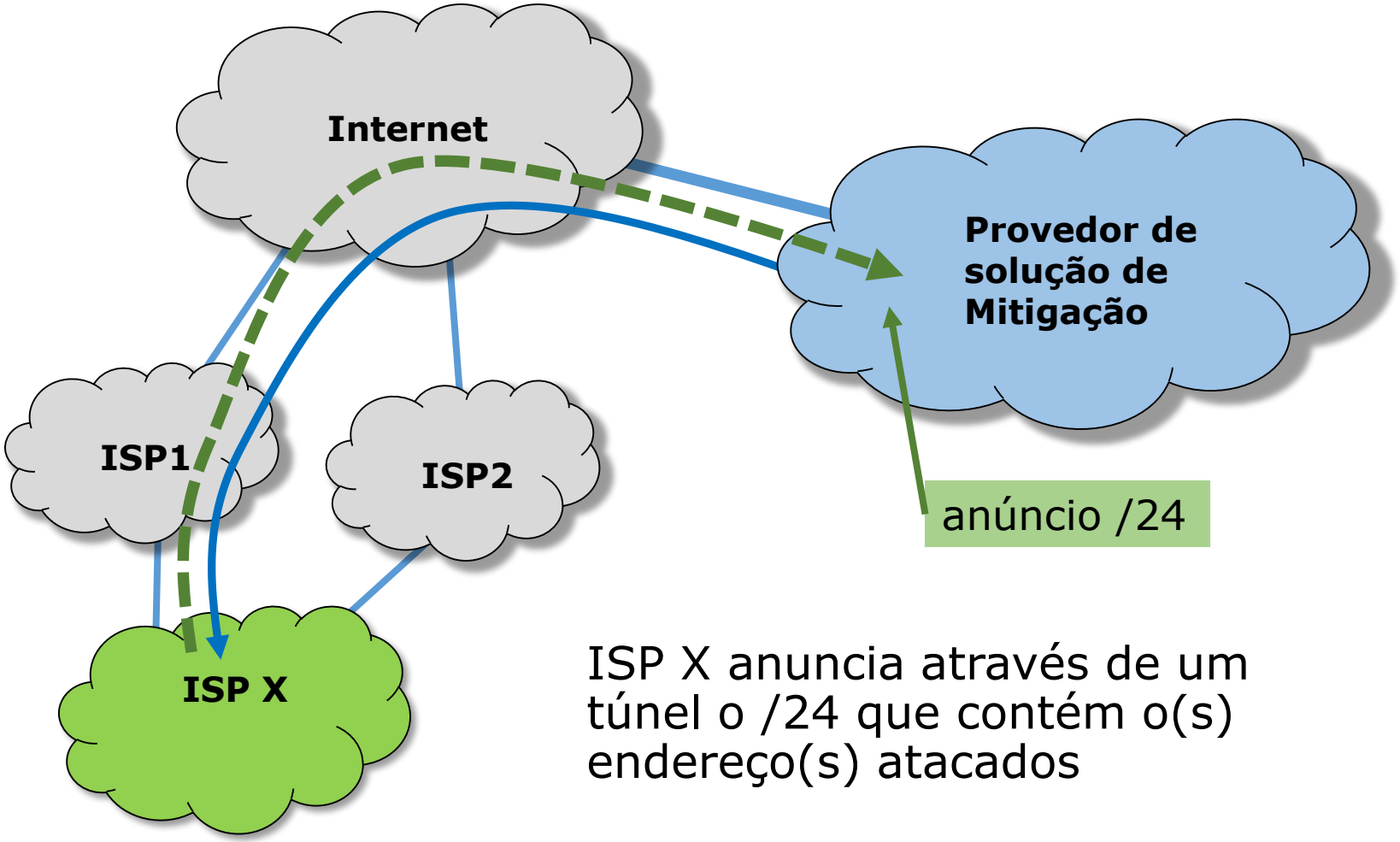


Mitigação na nuvem



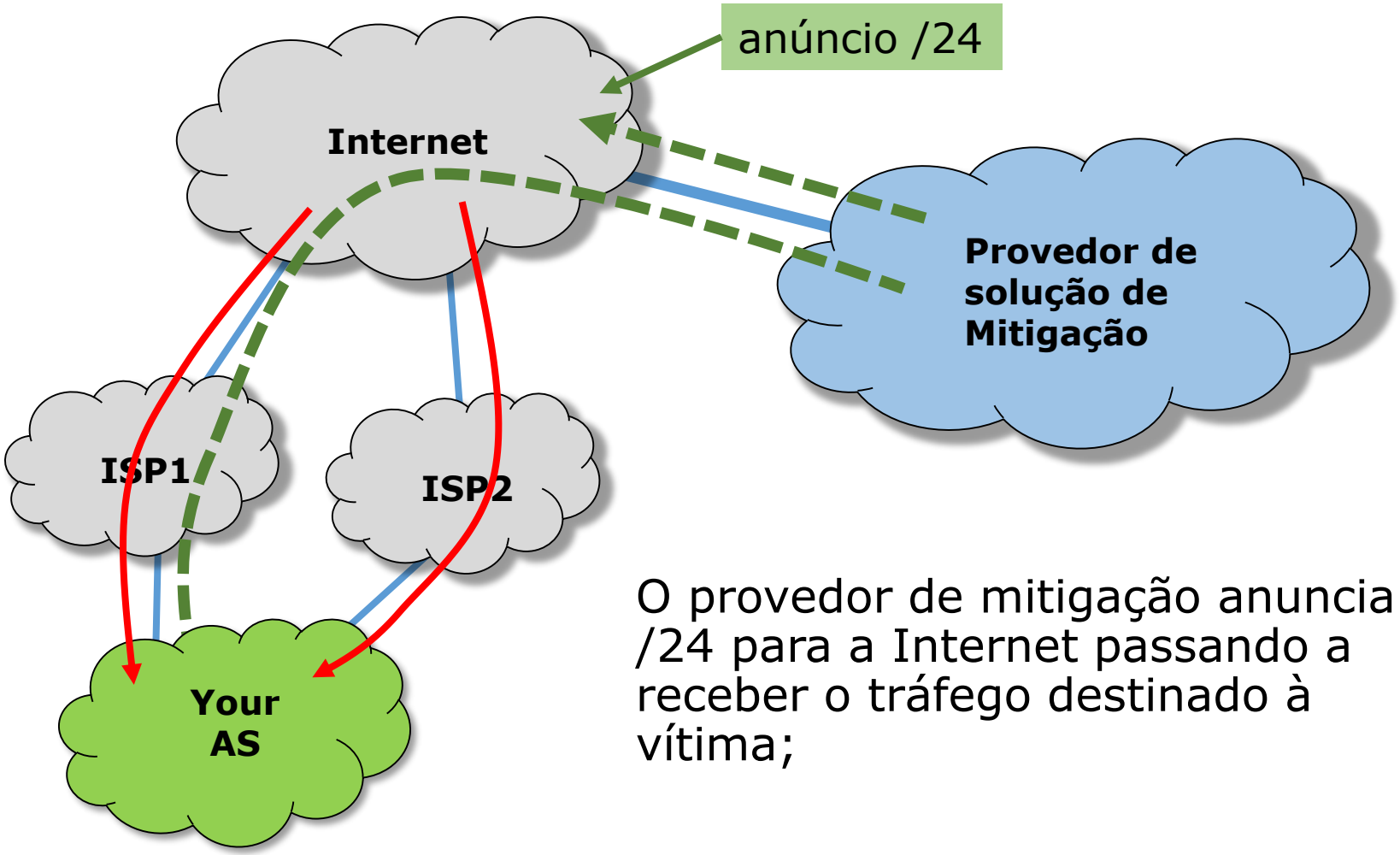
O ISP X está sofrendo um ataque de DDoS por todos seus upstreams.

Mitigação na nuvem



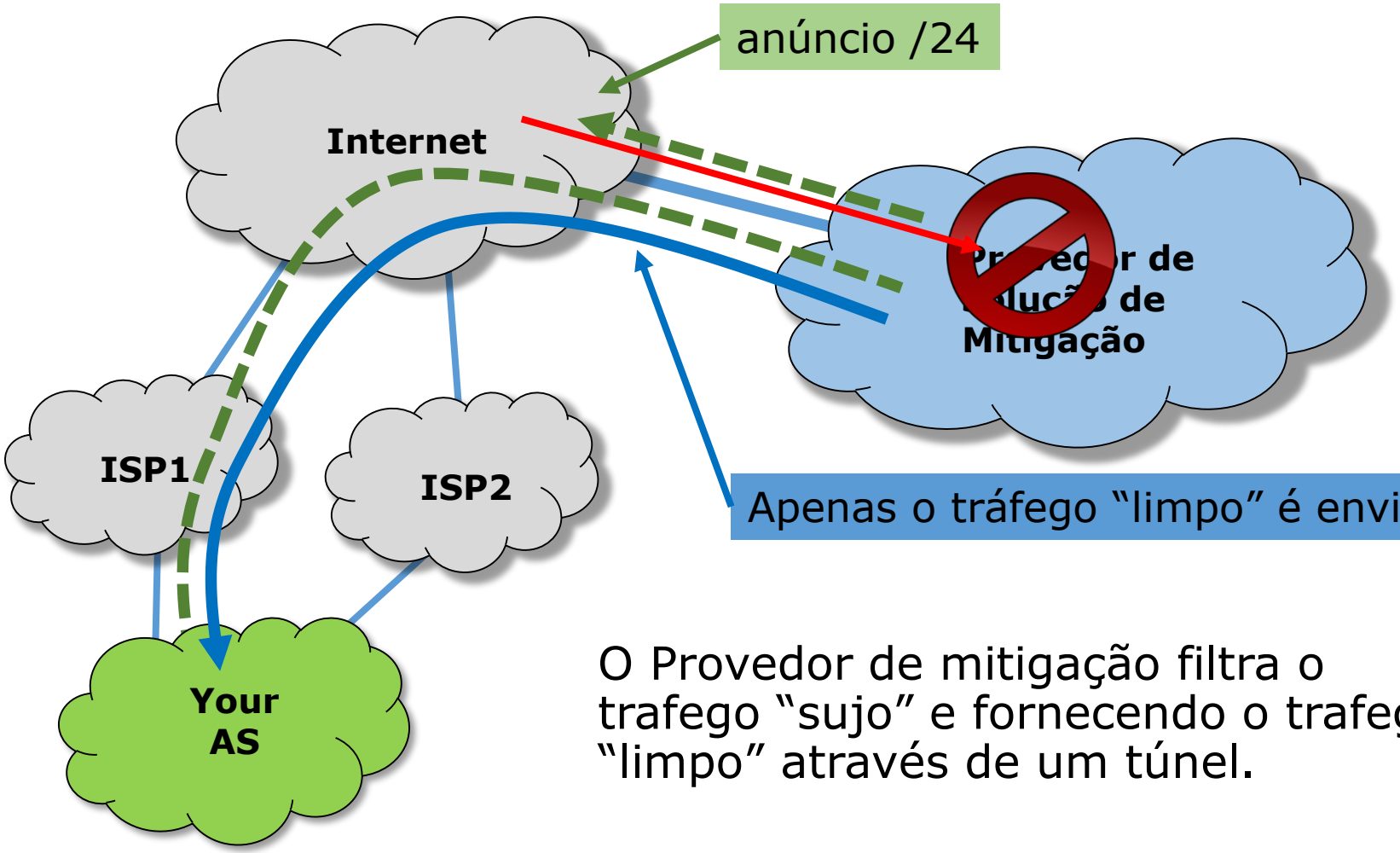
ISP X anuncia através de um túnel o /24 que contém o(s) endereço(s) atacados

Mitigação na nuvem



O provedor de mitigação anuncia o /24 para a Internet passando a receber o tráfego destinado à vítima;

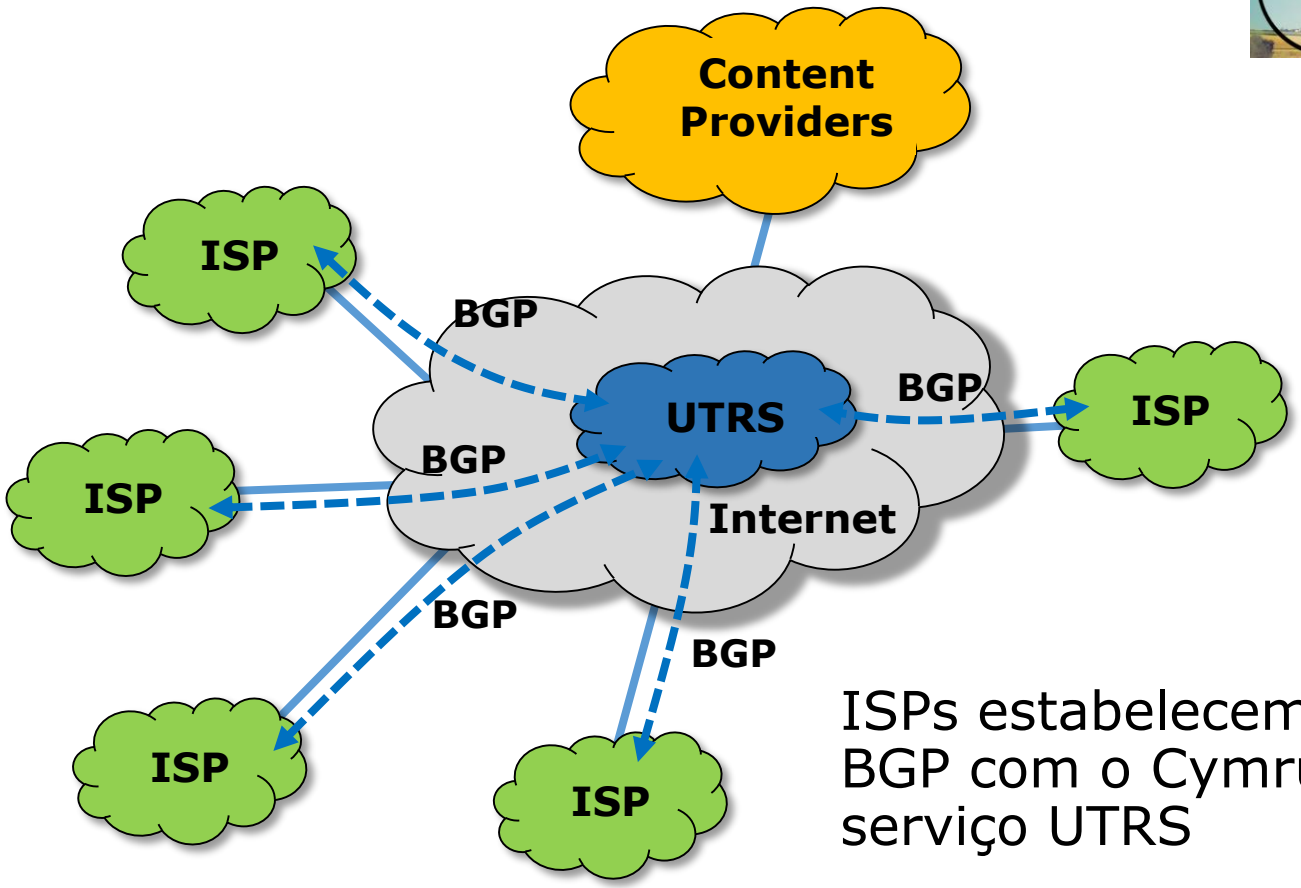
Mitigação na nuvem



O Provedor de mitigação filtra o trafego "sujo" e fornecendo o trafego "limpo" através de um túnel.

Cymru - UTRS

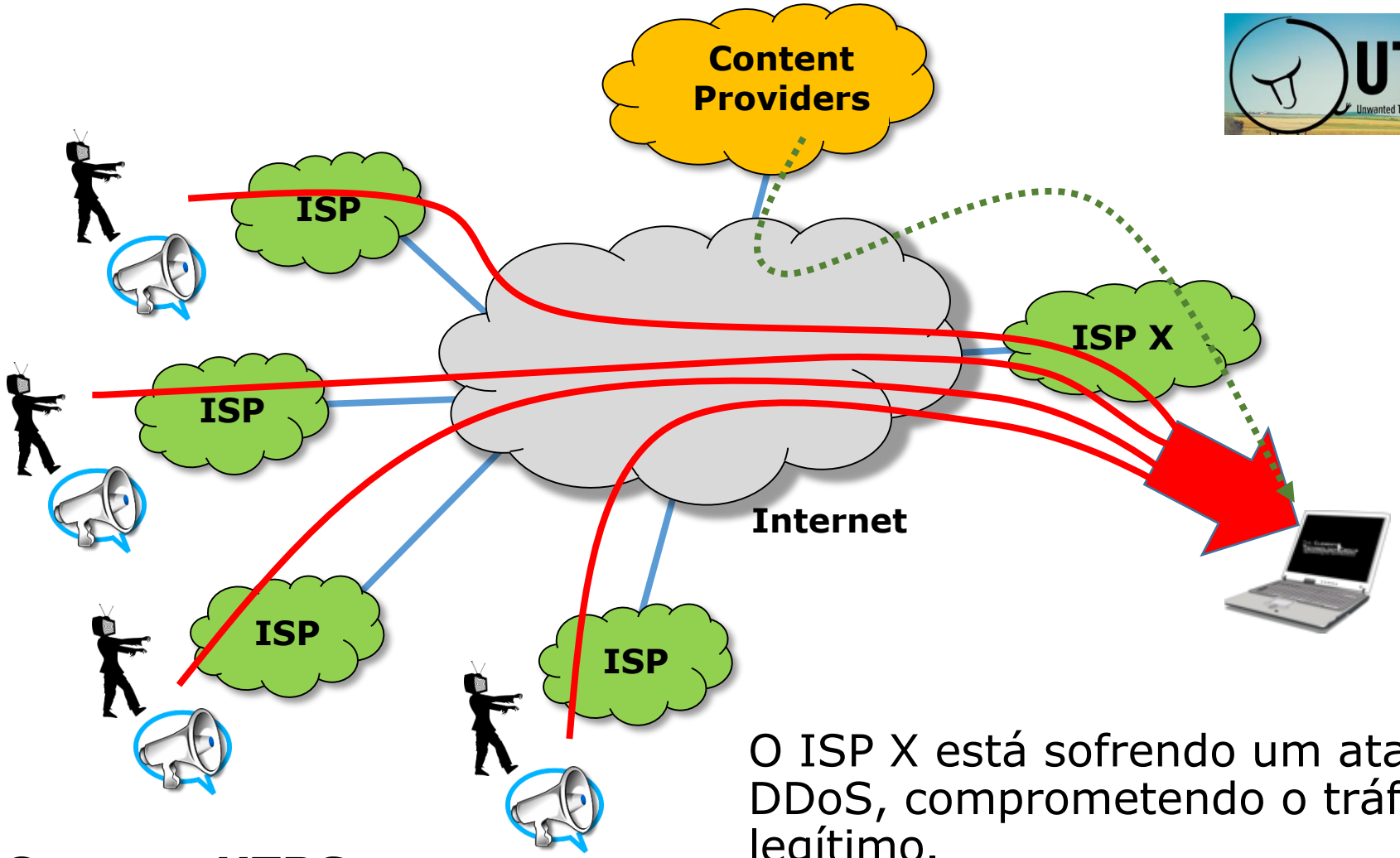
UTRS – Unwanted Traffic Removal



ISPs estabelecem sessões BGP com o Cymru para o serviço UTRS

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

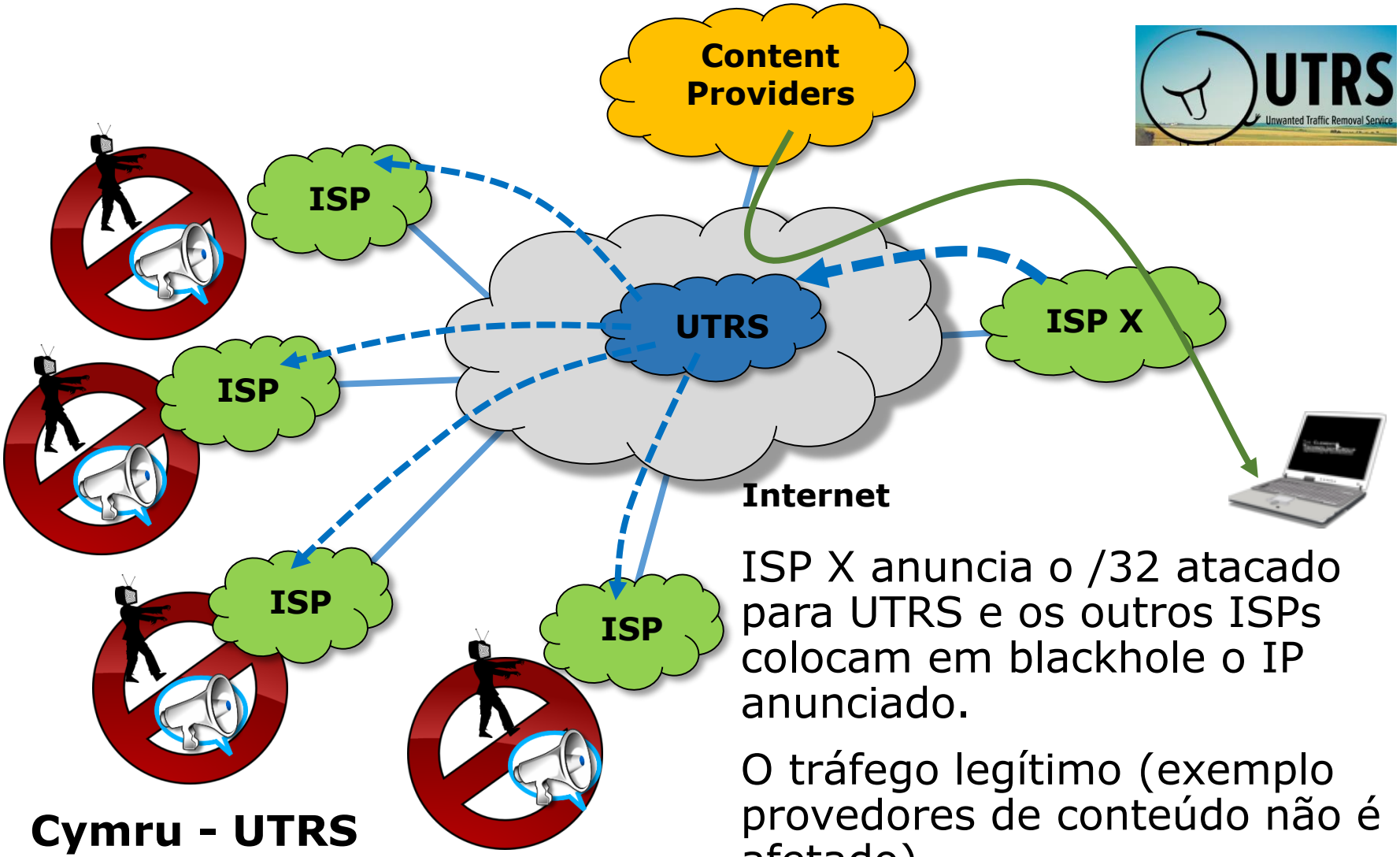
Cymru - UTRS



O ISP X está sofrendo um ataque DDoS, comprometendo o tráfego legítimo.

Cymru - UTRS

Cymru - UTRS



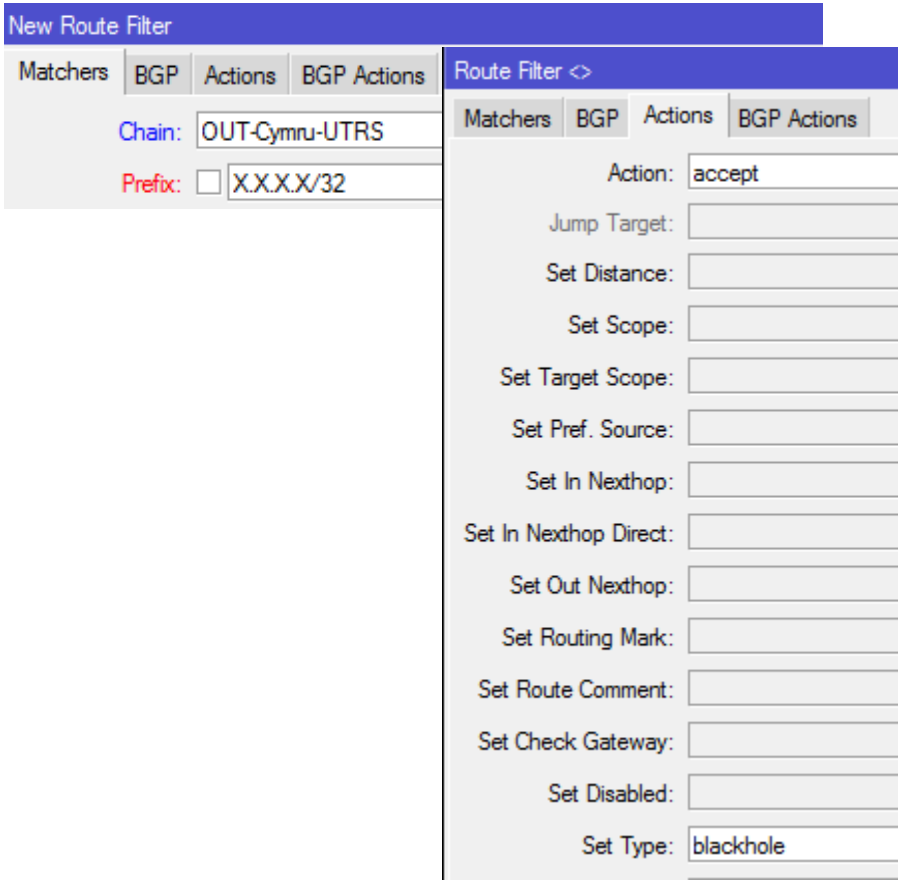
ISP X anuncia o /32 atacado para UTRS e os outros ISPs colocam em blackhole o IP anunciado.

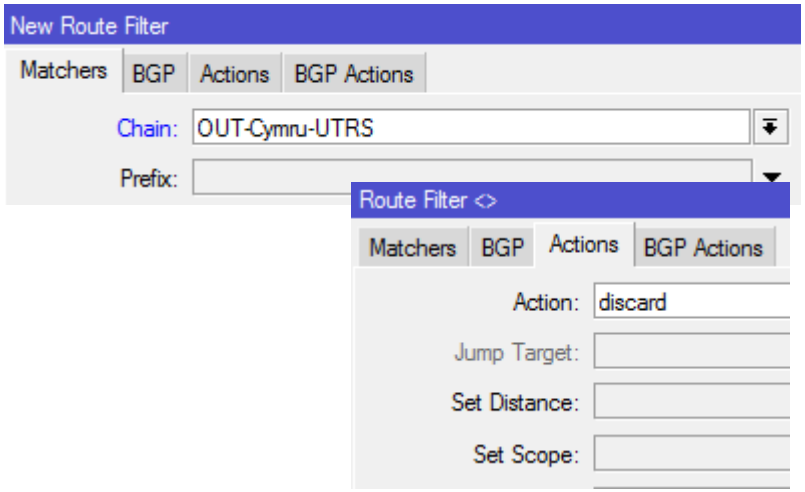
O tráfego legítimo (exemplo provedores de conteúdo não é afetado)

Cymru - UTRS

Implementação no RouterOS:

No caso de anunciar um /32

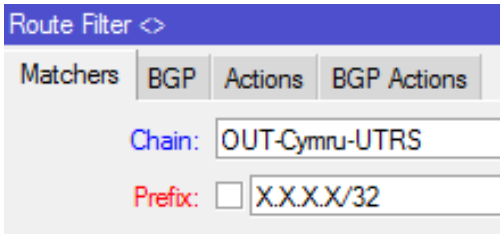


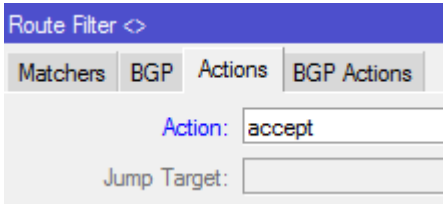


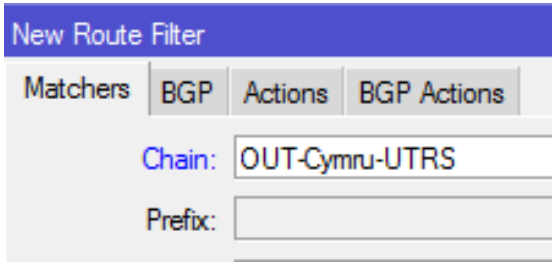
Cymru - UTRS

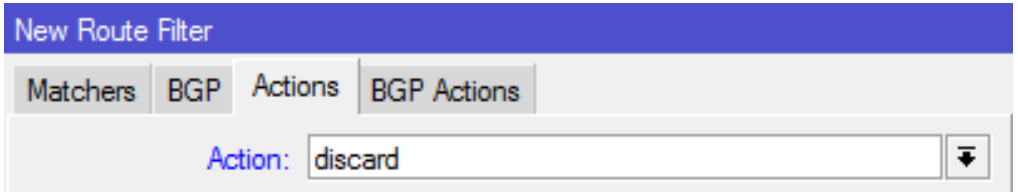
Implementação no RouterOS:

Para injetar no blackhole enviado ao UTRS









Ok, a mitigação é possível, porém quanto tempo meu SLA será comprometido?

Quanto tempo demora desde a detecção do ataque à ação?

Qualquer uma das técnicas necessitará uma ação de mudança de anúncios para ser efetivada.

Se o processo é **manejado por humanos**, muitas chances há de que o serviço seja comprometido por muito, muito tempo...

Pessoas tem que ser avisadas e saber o que fazer, e de forma rápida.

Importante mencionar que em alguns ataques o acesso ao roteador pode ser comprometido de tal forma que o próprio acesso ao roteador fica comprometido.

Quanto tempo demora desde a detecção do ataque à ação?

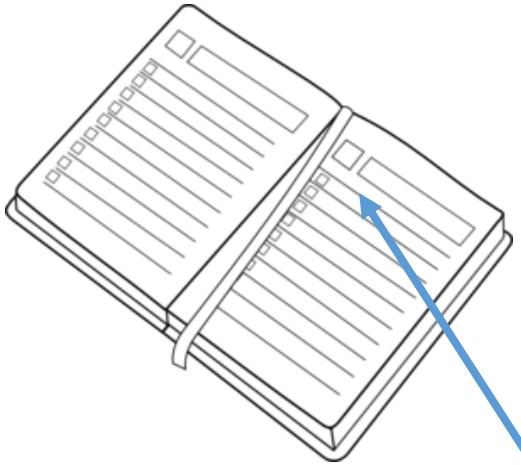
Definitivamente precisamos de uma solução automática.

E o momento de implementa-la é quando as coisas estão sob controle

Sun Tzu – The art of war

In Peace, prepare for War...

Agenda



Conceitos de DDoS – componentes, y arquitetura;

Enfrentamento dos ataques – as boas práticas em nossa rede para minimiza-los;

Enfrentamento dos ataques – técnicas de mitigação possíveis e suas implementações;

Automatizando a detecção e mitigação em um ISP regional no Brasil;

A “cereja do bolo” – Gráficos e informações detalhadas da rede;

Automatizando a solução

Nossa solução para mitigação de DDoS utiliza:

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

e uma combinação de 2 ferramentas open source:

→ **Fastnetmon**

→ **ExaBGP**

Detecção de DDoS com Fastnetmon

O "core" da nossa implementação é o Fastnetmon

Fastnetmon é um analisador de ataques DoS/DDoS de alta performance que pode trabalhar com muitos 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 é um SDN BGP speaker construído em Python, conhecido como o "Canivete Suíço" do BGP

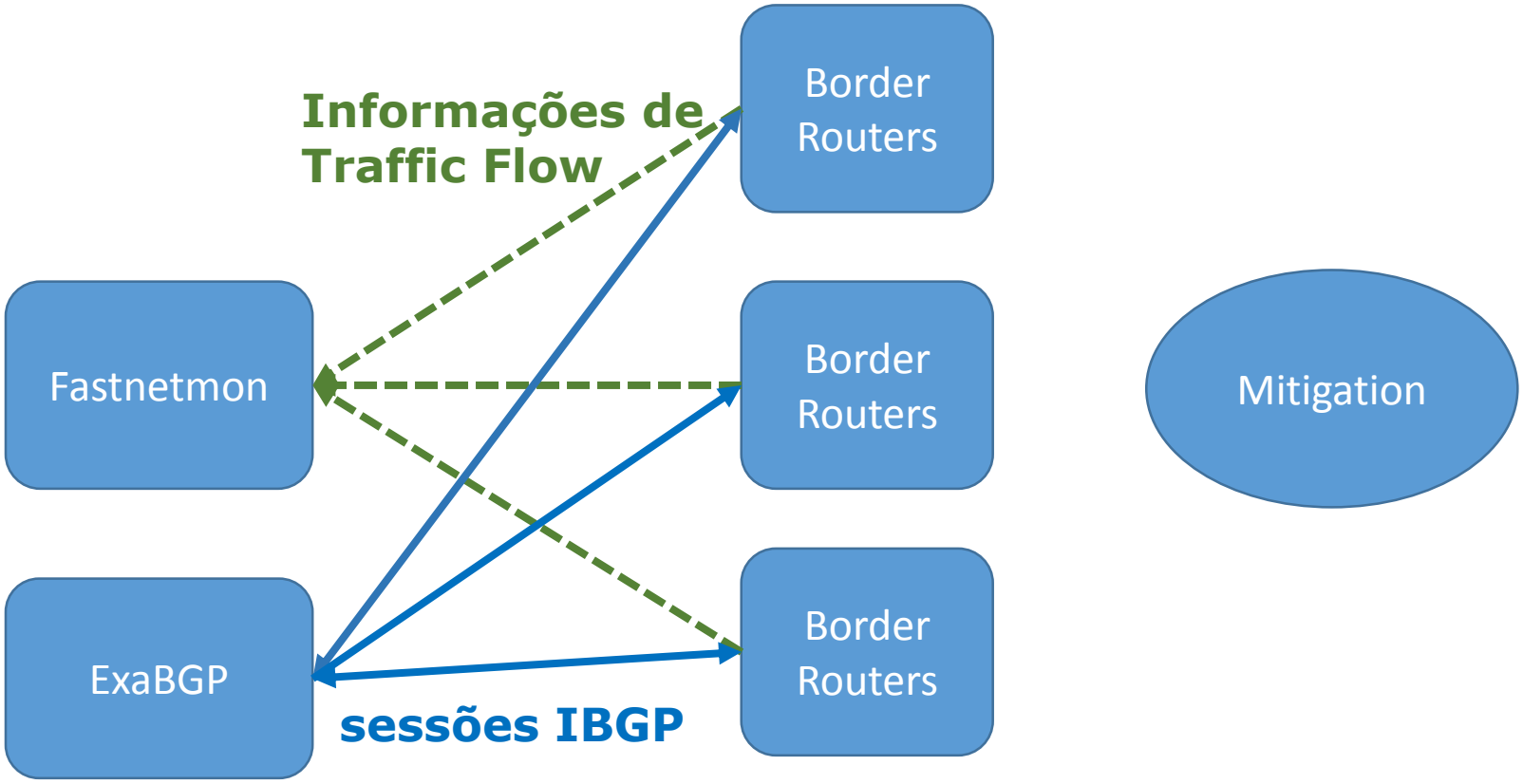
O ExaBGP pode fazer muitas coisas relacionadas ao protocolo que não seriam possíveis com um roteador real.

É possível injetar rotas arbitrárias, obter dados de roteamento, etc,

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

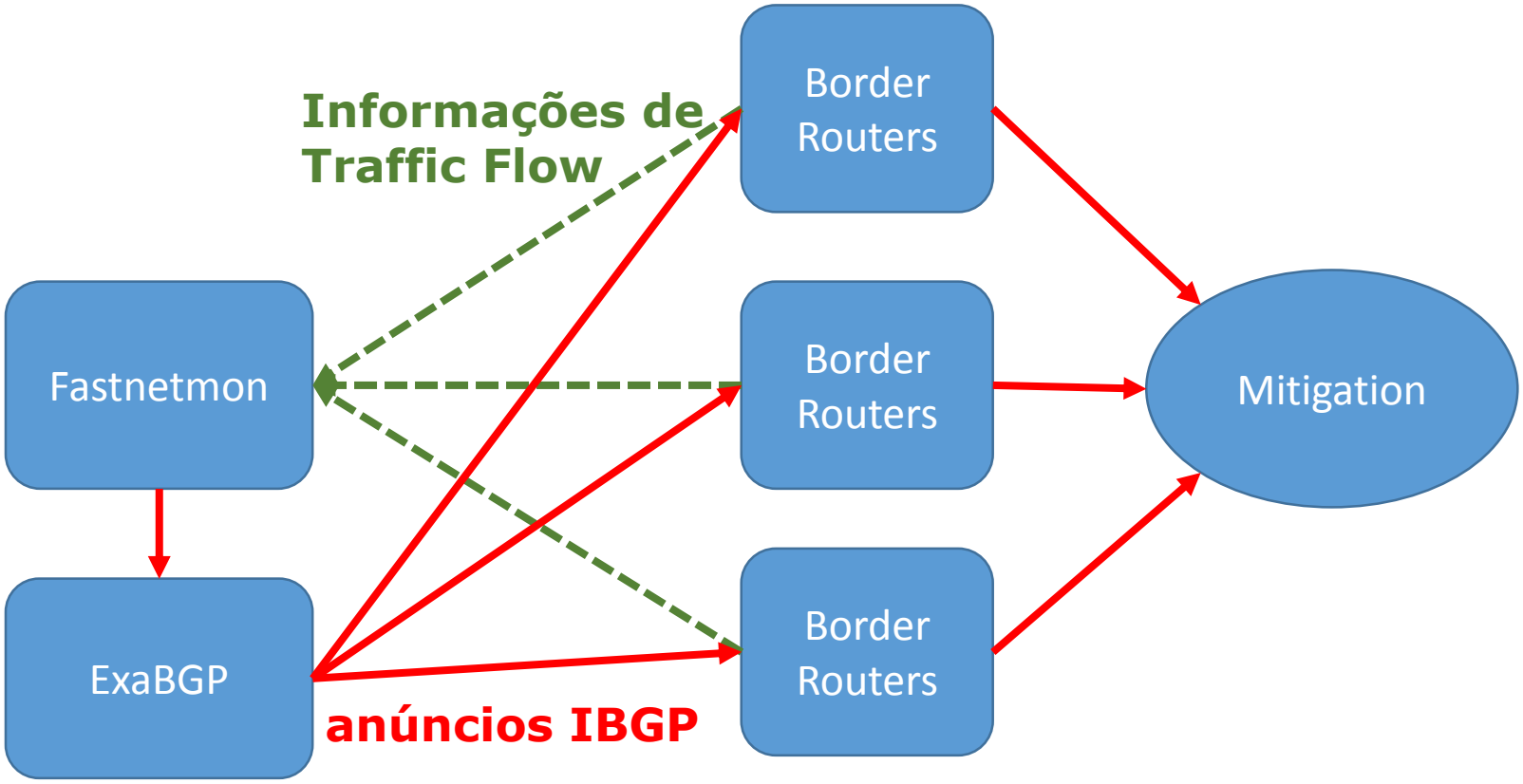
Esquema para detecção e mitigação de DDoS

Os roteadores de borda enviam informações de fluxos para o Fastnetmon. O ExaBGP tem sessões iBGP com os roteadores de borda.



Esquema para detecção e mitigação de DDoS

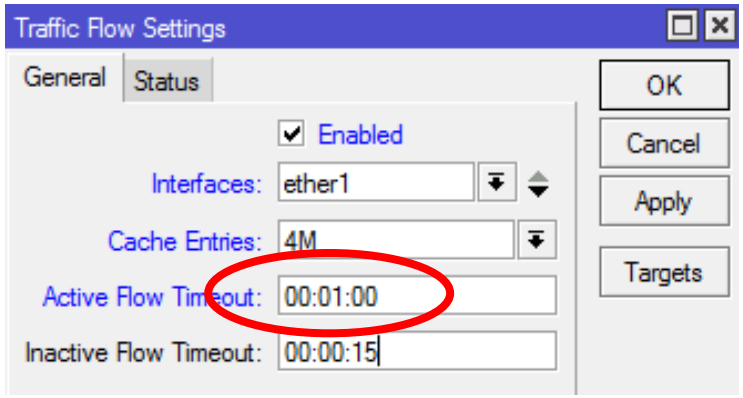
Quando um DDoS é detectado, o Fastnetmon automaticamente aciona o ExaBGP, que por sua vez envia as rotas por iBGP com uma community específica para blackholing. Os roteadores de borda anunciam este IP para a solução de mitigação adotada.

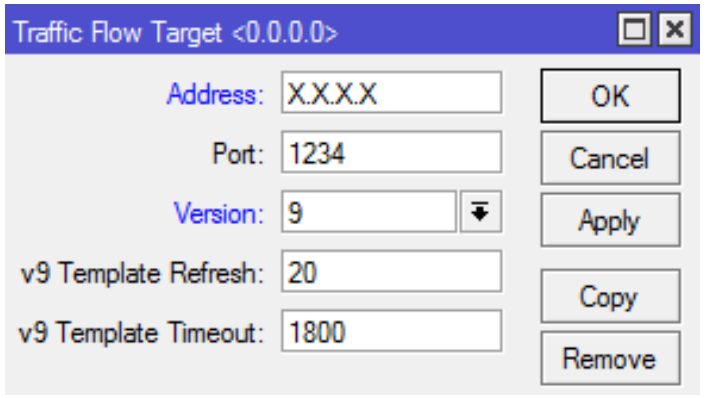


Configuração do Traffic Flow

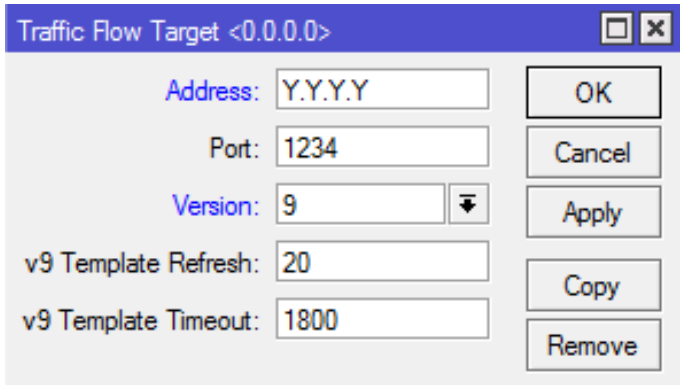
Traffic Flow

Configuração do Traffic Flow





Estamos usando duas instâncias do Fastnetmon, uma para notificação e outra para mitigação automática



Instalação e configuração do Fastnetmon

Fastnetmon – Instalación y configuración

Instalador automático 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

Instalando e rodando o Fastnetmon

Instalação 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
```

Instalando e rodando o Fastnetmon

Instalação 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
```

Instalando e rodando o Fastnetmon

Instalação 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 – detalhes de configuração

Detalhes de configuração

O arquivo principal de configuração é um texto amigável em:

/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 – detalhes de configuração

Configuração

Netflow configuration

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

netflow_port = 1234

netflow_host = 0.0.0.0

Ajuste a porta de acordo com o roteador. Melhor prática, informar o IP onde estão sendo coletados os fluxos.

Fastnetmon – detalhes de configuração

Configuração – limites

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

Fastnetmon – detalhes de configuração

Integração com 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 instalação e configuração

Instalação e configuração do ExaBGP

Instalação do ExaBGP (para Debian/Ubuntu)

apt-get install python-pip

pip install exabgp

Instalação do gerenciador bidirecional – socat

apt-get install socat

Instalação e configuração do ExaBGP

Crie um arquivo /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;
                }
}
```

Instalação e configuração do ExaBGP

Rode o 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

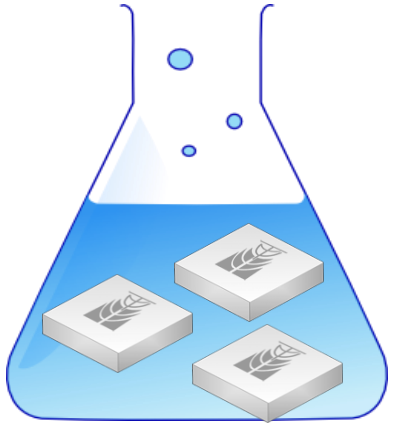
Referência:

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

Cliente Fastnetmon

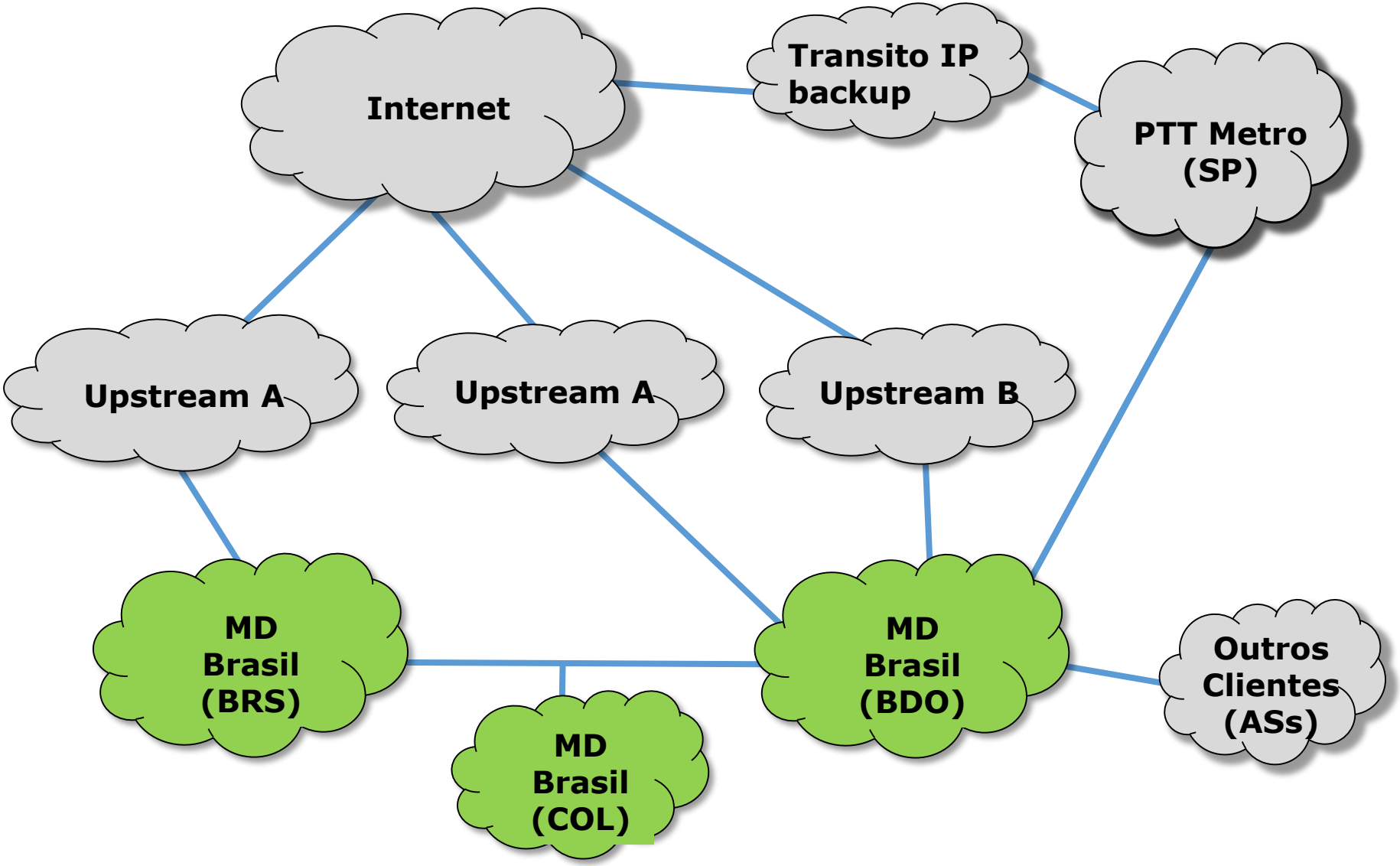
/opt/fastnetmon/fastnetmon_client

```
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
```

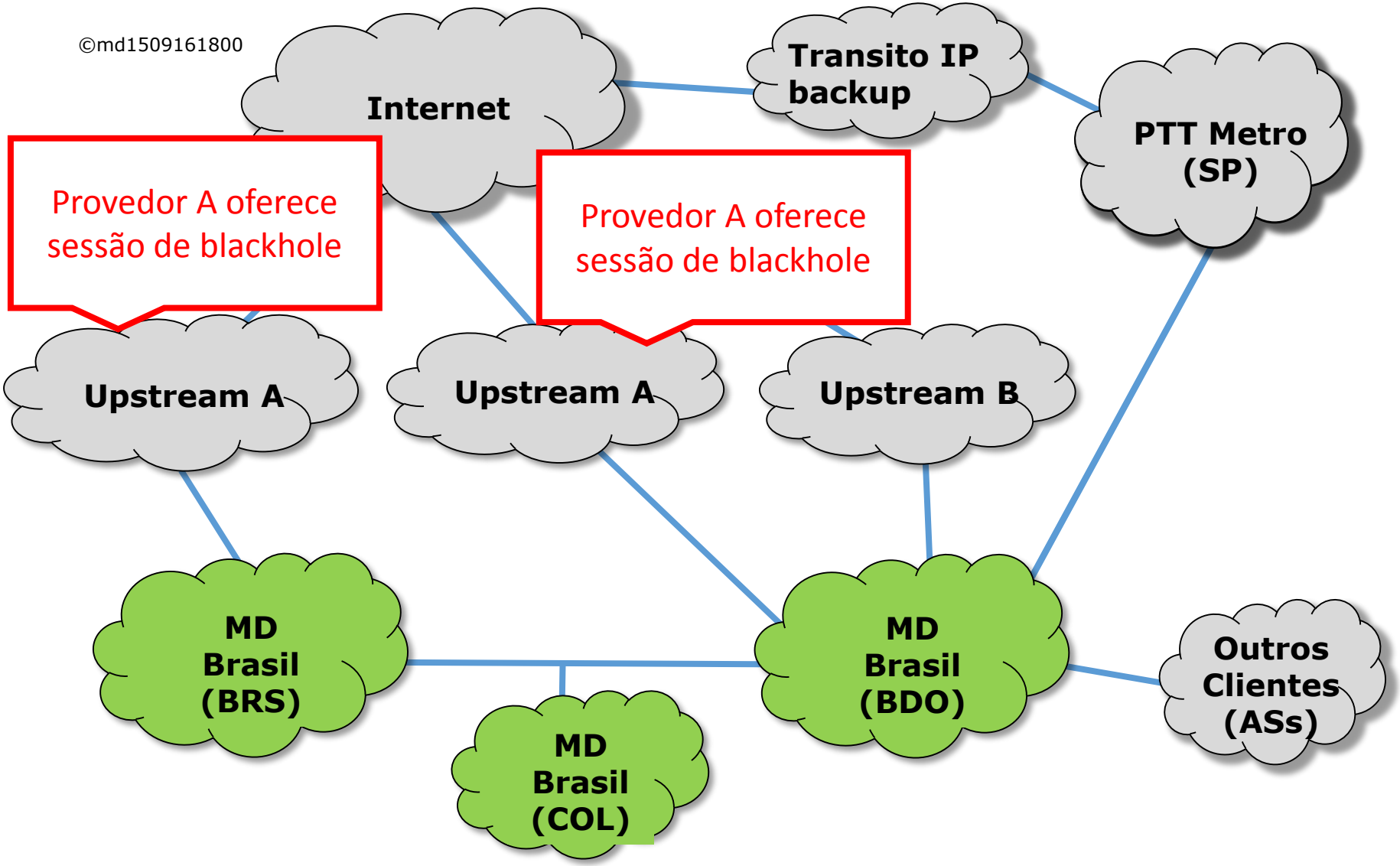


Implementação de caso concreto

Conectividade



Conectividade



Mitigação de DDoS

Provedor de upstream A → oferece sessão BGP exclusiva para anunciar blackhole.

→ Sob ataque, anunciar rede /24 mais específica pelo provedor A na sessão normal e o /32 atacado na sessão de blackhole.

→ Grupos de pequenos ISPs regionais que não tenham porte para contratar individualmente, podem viabilizar a contratação de um provedor de mitigação em conjunto.

Agenda

Conceitos de DDoS – componentes e arquitetura;

Enfrentamento dos ataques – as boas práticas em nossa rede para minimiza-los;

Enfrentamento dos ataques – técnicas de mitigação possíveis e suas implementações;

Automatizando a detecção e mitigação em um ISP regional no Brasil;

A “cereja do bolo” – Gráficos e informações detalhadas da rede;

Outras implementações

NetHealer

NetHealer é uma implementação que recebe os resultados do Fastnetmon e automatiza o processo de mitigação utilizando BIRD para o BGP.

É uma implementação empregada com bastante sucesso em um grande provedor de serviços na nuvem.

https://github.com/zenvdeluca/net_healer

Vicente de Luca, de Zendesk – autor do NetHealer

A cereja do bolo

Com a instalação do Fastnetmon e outras ferramentas, podemos melhorar nossa implementação para obter mais informações e controle de nossa rede.

Para tanto, além do Fastnetmon, necessitaremos de outras ferramentas:

InfluxDB + Grafana

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

InfluxDB

InfluxDB é um software open source para banco de dados de séries temporais sem dependências externas. Muito útil para registro e análise de métricas e eventos.

https://github.com/influxdata/influxdb

Instalação para 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 é outro open source empregado para apresentar um dashboard e gráficos, utilizando diversas bases de dados como Graphite, Elasticsearch, OpenTSDB, Prometheus e InfluxDB

https://github.com/grafana/grafana

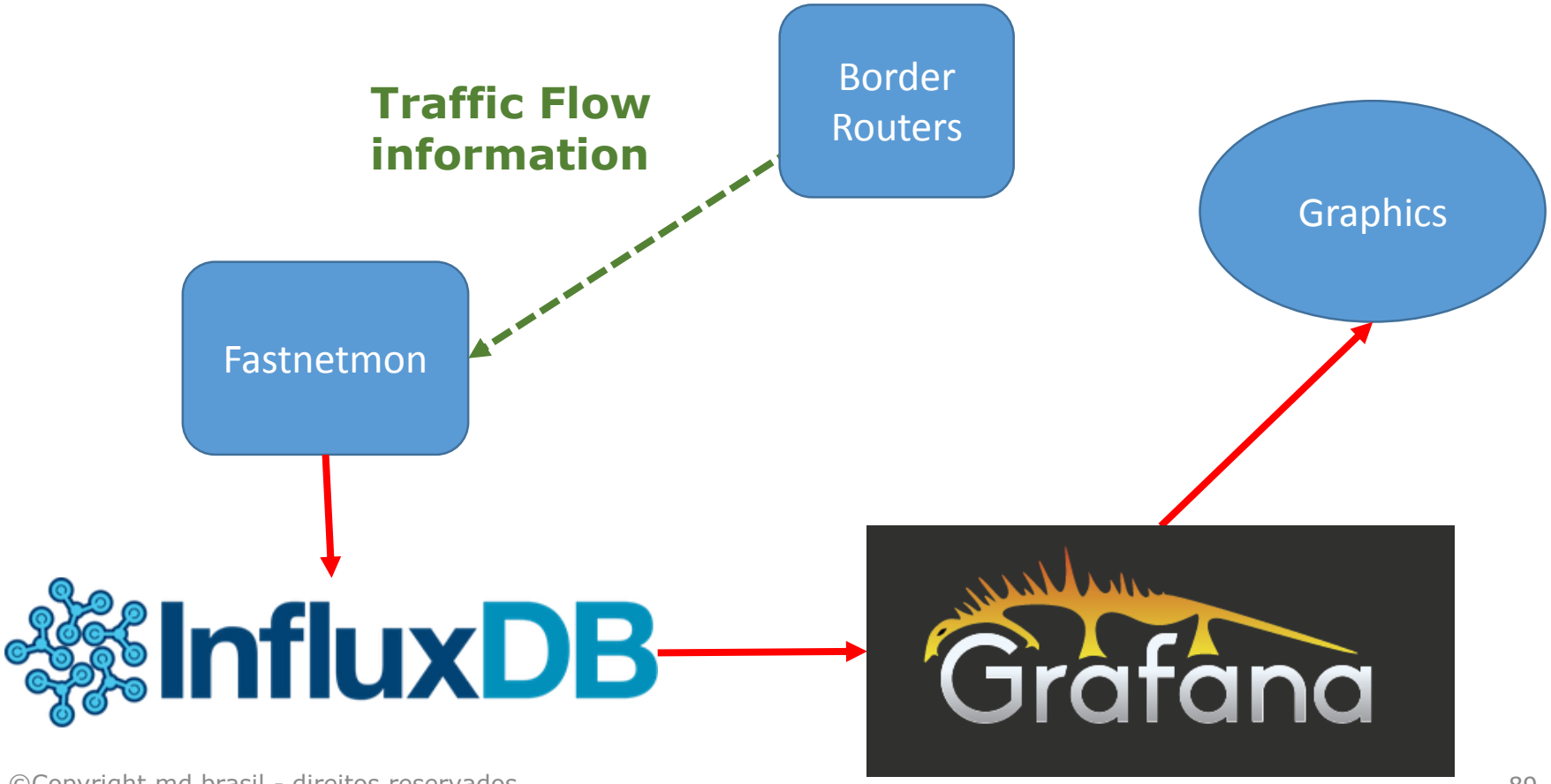
Instalação para Debian/Ubuntu

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

sudo dpkg -i grafana_2.6.0_amd64.deb

Integrando a solução

Integração de Fastnetmon + InfluxDB + Grafana



Fastnetmon + InfluxDB + Grafana

Este é um típico dashboard onde pode se visualizar o resultado obtido com a combinação das ferramentas

Trabalhos no IETF

DOTS – DDoS open threat signaling

DDoS Open Threat Signaling (DOTS) Working Group

draft-ietf-dots-use-cases-00

Roland Dobbins – Arbor Networks

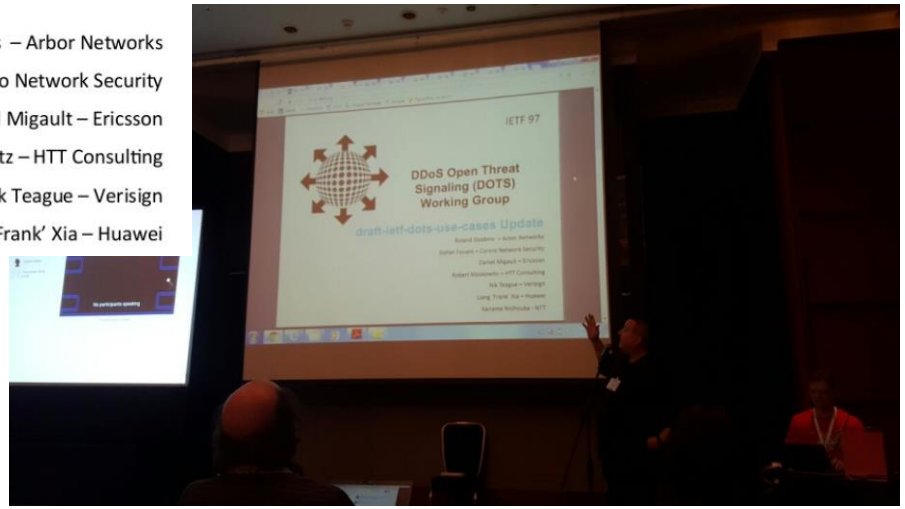
Stefan Fouant – Corero Network Security

Daniel Migault – Ericsson

Robert Moskowitz – HTT Consulting

Nik Teague – Verisign

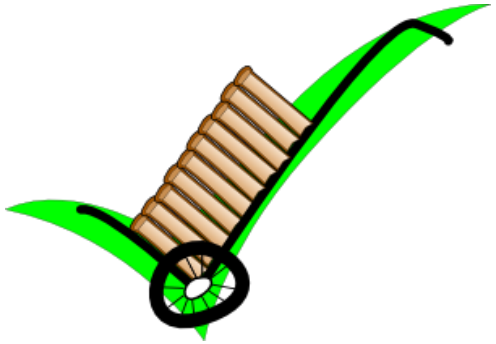
Liang 'Frank' Xia – Huawei



Agenda

- Conceitos de DDoS – componentes e arquitetura;
- Enfrentamento dos ataques – as boas práticas em nossa rede para minimiza-los;
- Enfrentamento dos ataques – técnicas de mitigação possíveis e suas implementações;
- Automatizando a detecção e mitigação em um ISP regional no Brasil;
- A “cereja do bolo” – Gráficos e informações detalhadas da rede;

Referências



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

Perguntas?

Obrigado!