



# CAPPI

CAMARA ARGENTINA DE PEQUEÑOS PROVEEDORES DE INTERNET

# Monitoreo para ISP

Usos de Herramientas de  
monitoreo para ISP  
Optativas / Necesarias

# Darío Fernández

## Research SRL

(2007) Integradores de tecnología

Enlaces punto a punto y multipunto

(2009) Despliegue de troncales de fibra óptica

(2013) IXP Posadas, ISP

(2018) Gpon - Garupá - Misiones

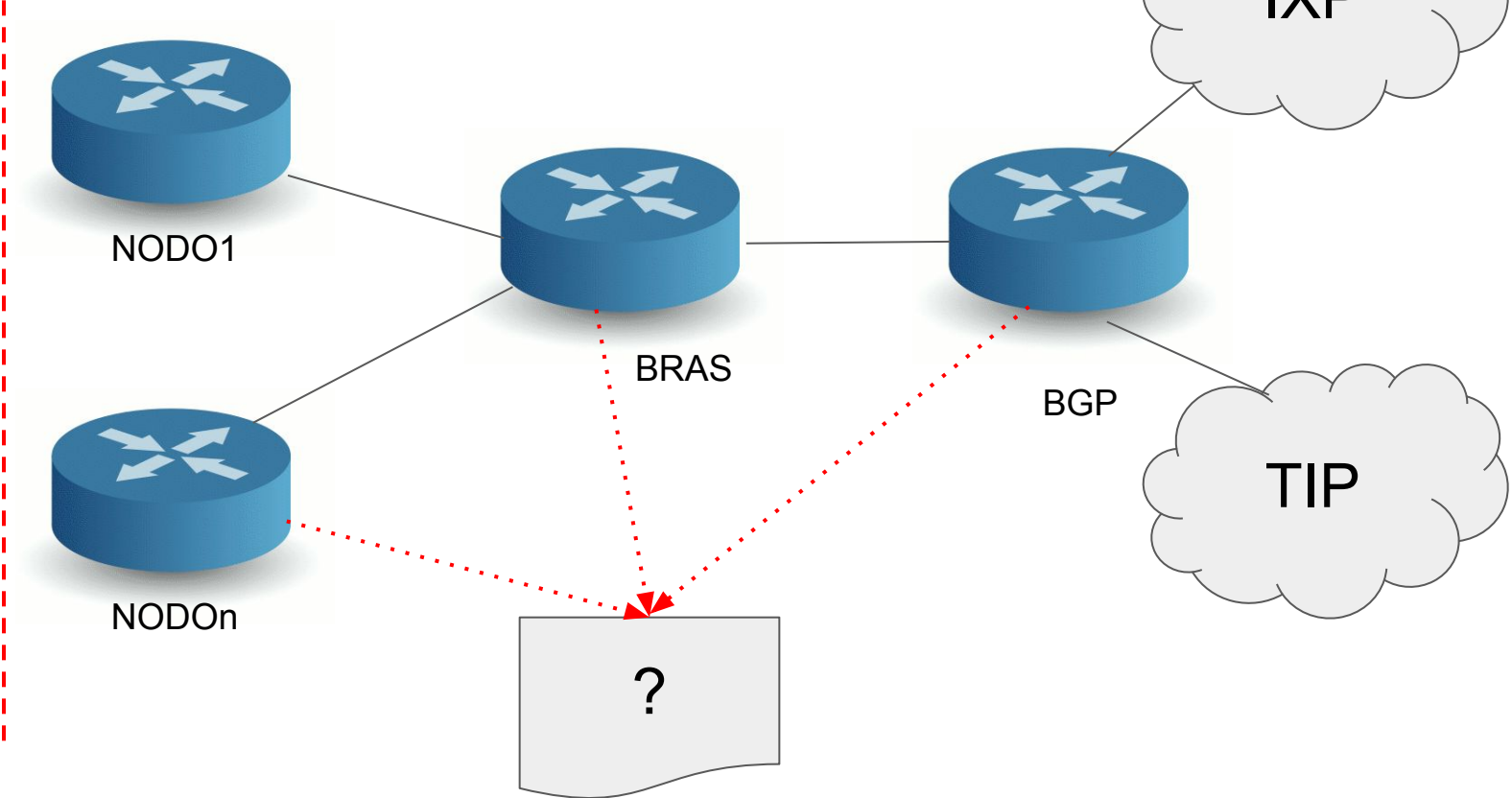
# ISP

Cientes

Cientes

Cientes

Cientes




# Virtualización

La virtualización de servidores permite ejecutar múltiples sistemas operativos en un solo servidor físico por medio de máquinas virtuales que ofrecen un elevado rendimiento. Entre las ventajas principales, se incluyen las siguientes:  
Mayor eficiencia del entorno de TI

**CITRIX®**  
**XenServer**

**X PROXMOX**

 **vmware®**  
**ESXi**

 **Microsoft**  
**Hyper-V**



Download ISO image : Descargue el Proxmox VE ISO, luego cópielo a una unidad flash USB o CD / DVD para usarlo. [Link de descargas](#)

Boot from USB or CD/DVD: Presione 'Entrar' para iniciar el asistente de instalación automática en su hardware dedicado.

Configure via GUI: Puede hacer todo a través de su navegador web. No necesita instalar una herramienta de administración separada.

Detalles y documentation: [Link de Wiki](#)

Vista por Servidor

Centro de datos (TomasGuido)

- > 360gen10
- > nn-blanco
- > r720a
- > **r720xd1**

Nodo 'r720xd1'

[Reboot](#)
[Cierre ordenado](#)
[>\\_ Shell](#)
[Acciones masivas](#)
[Ayuda](#)

[Resumen](#)
[Notas](#)
[>\\_ Shell](#)
[Sistema](#)
[Red](#)
[Certificados](#)
[DNS](#)
[Hosts](#)
[Horario](#)
[Syslog](#)
[Actualizaciones](#)
[Cortafuego](#)
[Discos](#)
 LVM

 LVM-Thin

 Directorio

 ZFS

Versiones de Paquetes de Programas

Hora (promedio)

**r720xd1 (Tiempo de uso: 15 días 01:46:40)**
**Uso de CPU** 27.12% de 40 CPU(s)


**Carga promedio** 12.47, 11.00, 10.88


**Memoria RAM** 48.78% (122.85 GiB de 251.84 GiB)


**Espacio de Disco(root)** 5.77% (5.43 GiB de 93.99 GiB)


**Retardo I/O** 3.66%

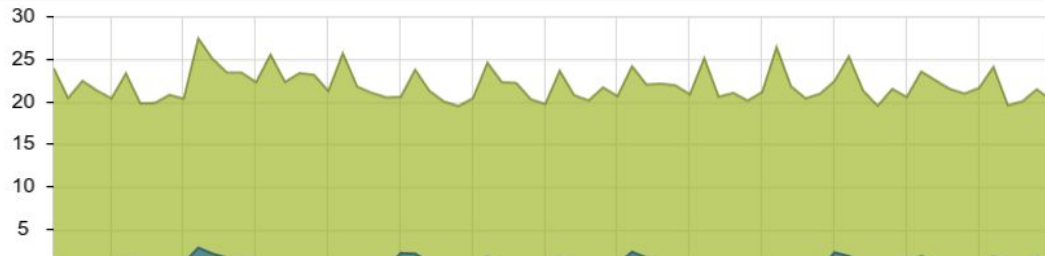
**Compartiendo KSM** 0 B


**Memoria SWAP** 0.00% (0 B de 8.00 GiB)

**CPU(s)** 40 x Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz (2 Sockets)

**Versión del kernel** Linux 5.3.13-3-pve #1 SMP PVE 5.3.13-3 (Fri, 31 Jan 2020 08:17:11 +0100)

**Versión de PVE Manager** pve-manager/6.1-7/13e58d5e

**Uso de CPU**


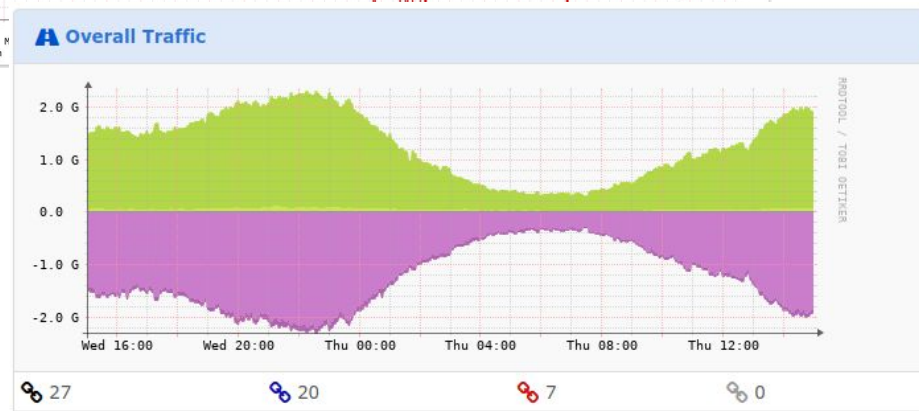
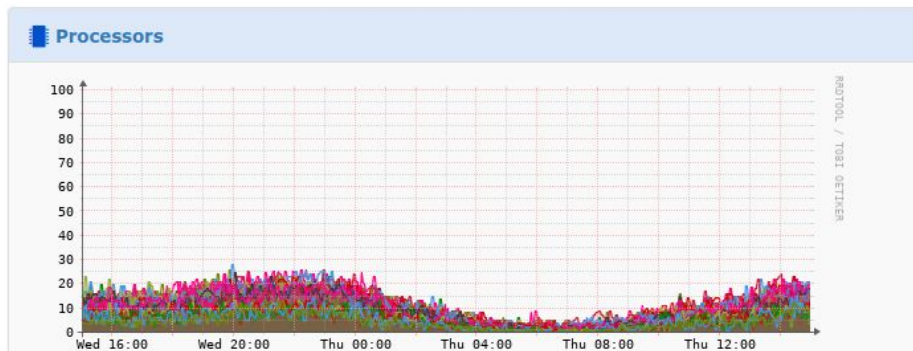
# Que quiero saber?

Uso de CPU?

Tráfico de una Interface?

Potencia de un link?

Pérdida de paquetes hacia un destino?





# SNMP: Simple Network Management Protocol

Protocolo simple de administración de red

- Posee comandos de Lectura/Escritura
- utiliza el Puerto 161 UDP
- SNMPv1 y v2
- SNMPv3 con seguridad
- Se utiliza un NMS (Network Manager System)  
Sistema administrador de red

# Observium / LibreNMS

The image displays two overlapping network monitoring dashboards: Observium (top) and LibreNMS (bottom).

**Observium Dashboard:**

- Navigation:** Overview, Graphs, Health, Ports, Inventory, Logs, Alerts.
- Device Details (Huawei Integrated Access Software):**
  - Description: OLT-GRP-01
  - Vendor: Huawei
  - Operating system: Huawei IAS
  - System name: ma5680t-ixfo-sines
  - Contact: Noc Operator at 543764619600
  - Location: Planta transmisora Multimedios SAPEM - Arsat
  - Uptime: 1 year, 4 days, 10h 59m 20s
  - Last reboot: 2019-07-13 04:33:35
- Temperature:** A list of temperature sensors including H801X2CS\_0\_18, H802SCUN\_0\_7, H802SCUN\_0\_8, H805GPFD\_0\_10, H805GPFD\_0\_11, and H805GPFD\_0\_9.
- Ports:** A line graph showing port status over time. Summary: 54 ports, 48 green, 6 red, 0 grey.

**LibreNMS Dashboard:**

- Navigation:** Overview, Devices, Services, Ports, Health, Alerts.
- Device Details (Huawei Integrated Access Software):**
  - System Name: ma5683t-neara4
  - Hardware: SmartAX
  - Operating System: Huawei SmartAX MA5683V800R17C10B056
  - Serial: 020LGTJ02011423
  - Object ID: .1.3.6.1.4.1.2011.2.133
  - Contact: soporte@researchrli.com.ar
  - Device Added: 1 day 23 hours 41 minutes 14 seconds ago
  - Last Discovered: 3 hours 3 minutes 5 seconds ago
  - Uptime: 268 days 1 hour 29 seconds
  - Location: Calle 186 & Calle 53b, Posadas, Misiones
  - Lat / Lng: -27.436898, -55.906865
- Processors:** A line graph showing processor usage. Summary: H805GPFD processor x5, 9% usage.
- Temperature:** A table of temperature sensors with current readings:

Sensor	Temperature
H801X2CS	29 °C
H802SCUN	27 °C
H802SCUN	28 °C
H805GPFD	44 °C
H805GPFD	41 °C
H805GPFD	36 °C
- Power:** A table of power consumption:

Component	Power
Chassis Total	339 W
H801GICF	4 W
H801X2CS	18 W
H802SCUN	50 W
H802SCUN	50 W
H805GPFD	50 W
H805GPFD	50 W
H805GPFD	50 W
- Overall Traffic:** A line graph showing network traffic over time. Summary: 52 connections, 41 active, 11 blocked, 0 disabled.

# Instalación de LibreNMS

## LibreNMS Documentation

- [LibreNMS Docs](#)
- [LibreNMS Installation Guides](#)
- [GitHub LibreNMS](#)

## Centos / Ubuntu

- Support for both Apache and Nginx Web Servers
- [Installation Guide](#)

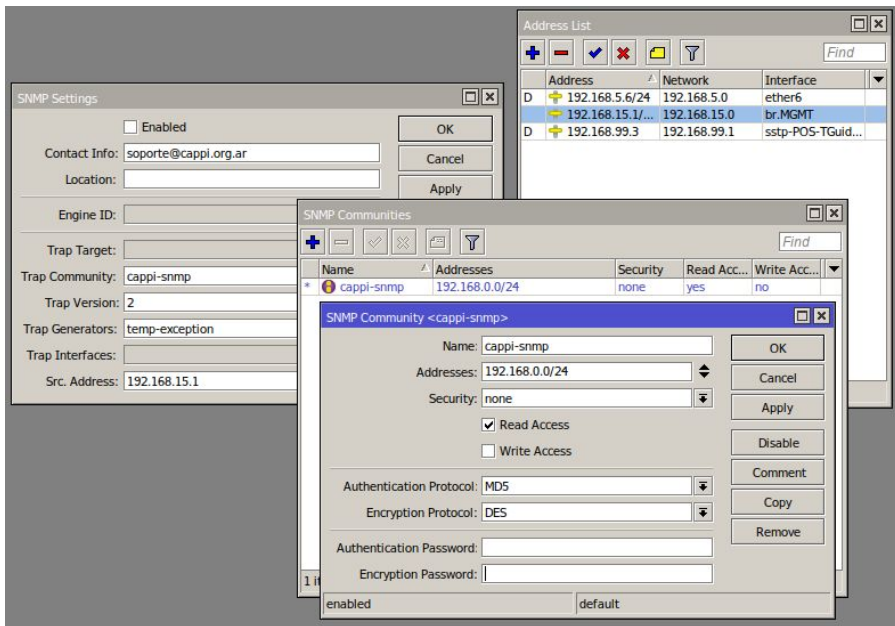
## Virtual Machines

- LibreNMS Virtual Machines: [Documentation](#)
- LibreNMS: [OVA Images](#)

## Docker Images

- Docker image documentation located on: [GitHub LibreNMS/Docker](#)
- LibreNMS on: [dockerhub](#)
- LibreNMS on: [QUAY](#)

# Agregar un nuevo dispositivo



## Add Device

Devices will be checked for Ping/SNMP reachability before being probed.

Hostname or IP: 192.168.15.1

SNMP:  ON

SNMP Version: v2c | port | udp

Port Association Mode: ifIndex

### SNMPv1/2c Configuration

Community: capi-snmp

Force add (No ICMP or SNMP checks performed):  OFF

Add Device

# Custom OIDs

Si se que preguntar puedo agregarlo a mano?

[Overview](#) [Graphs](#) [Health](#) [Ports](#) [STP](#) [Inventory](#) [Logs](#) [Alerts](#) [Alert Stats](#) [Latency](#) [Notes](#)



[Device Settings](#) | [SNMP](#) | [Port Settings](#) | [Applications](#) | [Alert Rules](#) | [Modules](#) | [Services](#) | [IPMI](#) | [Health](#) | [Storage](#) | [Processors](#) | [Memory](#) | [Misc](#) | [Components](#) | **Custom OID**

## Custom OIDs

Name	OID	Value	Unit	Alert Threshold		Warning Threshold		Alerts	Passed	Action
				High	Low	High	Low			
<a href="#">+ Add New OID</a>										10
RX-ONT[0/0/0]	iso.3.6.1.4.1.2011.6.128.1.1.2.51.1.4.4194304000.0	-17.57	dBm					<input type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
RX-ONU2[0/0/1]	iso.3.6.1.4.1.2011.6.128.1.1.2.51.1.4.4194304000.1	-14.03	dBm					<input type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>

### Seriales de ONU

iso.3.6.1.4.1.2011.6.128.1.1.2.46.1.30.4194304000.0 = Hex-STRING: 48 57 54 43 61 FD A2 9C  
iso.3.6.1.4.1.2011.6.128.1.1.2.46.1.30.4194304000.1 = Hex-STRING: 48 57 54 43 F2 94 2D 9F  
iso.3.6.1.4.1.2011.6.128.1.1.2.43.1.3.4194304000.0 = Hex-STRING: 48 57 54 43 61 FD A2 9C  
iso.3.6.1.4.1.2011.6.128.1.1.2.43.1.3.4194304000.1 = Hex-STRING: 48 57 54 43 F2 94 2D 9F

### Modelo

iso.3.6.1.4.1.2011.6.128.1.1.2.45.1.4.4194304000.0 = STRING: "HG8546M"  
iso.3.6.1.4.1.2011.6.128.1.1.2.45.1.4.4194304000.1 = STRING: "EG8141A5"

### Versión de Soft

iso.3.6.1.4.1.2011.6.128.1.1.2.45.1.5.4194304000.0 = STRING: "V3R017C10S125"  
iso.3.6.1.4.1.2011.6.128.1.1.2.45.1.5.4194304000.1 = STRING: "V5R019C20S110"

### RX-Power

iso.3.6.1.4.1.2011.6.128.1.1.2.51.1.4.4194304000.0 = INTEGER: -1762  
iso.3.6.1.4.1.2011.6.128.1.1.2.51.1.4.4194304000.1 = INTEGER: -1403

### Voltaje

iso.3.6.1.4.1.2011.6.128.1.1.2.51.1.5.4194304000.0 = INTEGER: 3320  
iso.3.6.1.4.1.2011.6.128.1.1.2.51.1.5.4194304000.1 = INTEGER: 3360

### Distancia calculada en base a la potencia

iso.3.6.1.4.1.2011.6.128.1.1.2.46.1.20.4194304000.0 = INTEGER: 23  
iso.3.6.1.4.1.2011.6.128.1.1.2.46.1.20.4194304000.1 = INTEGER: 3  
el valor 419430400 sale de Frame/Slot/Port y el .XX corresponde a la ONU-ID registrada en ese puerto

# Templates de Alerta

Existen Templates creados por la comunidad y también se pueden crear templates para generar alertas, su documentación [aquí](#)

Alert Template :: Docs

Template name:

Template:  

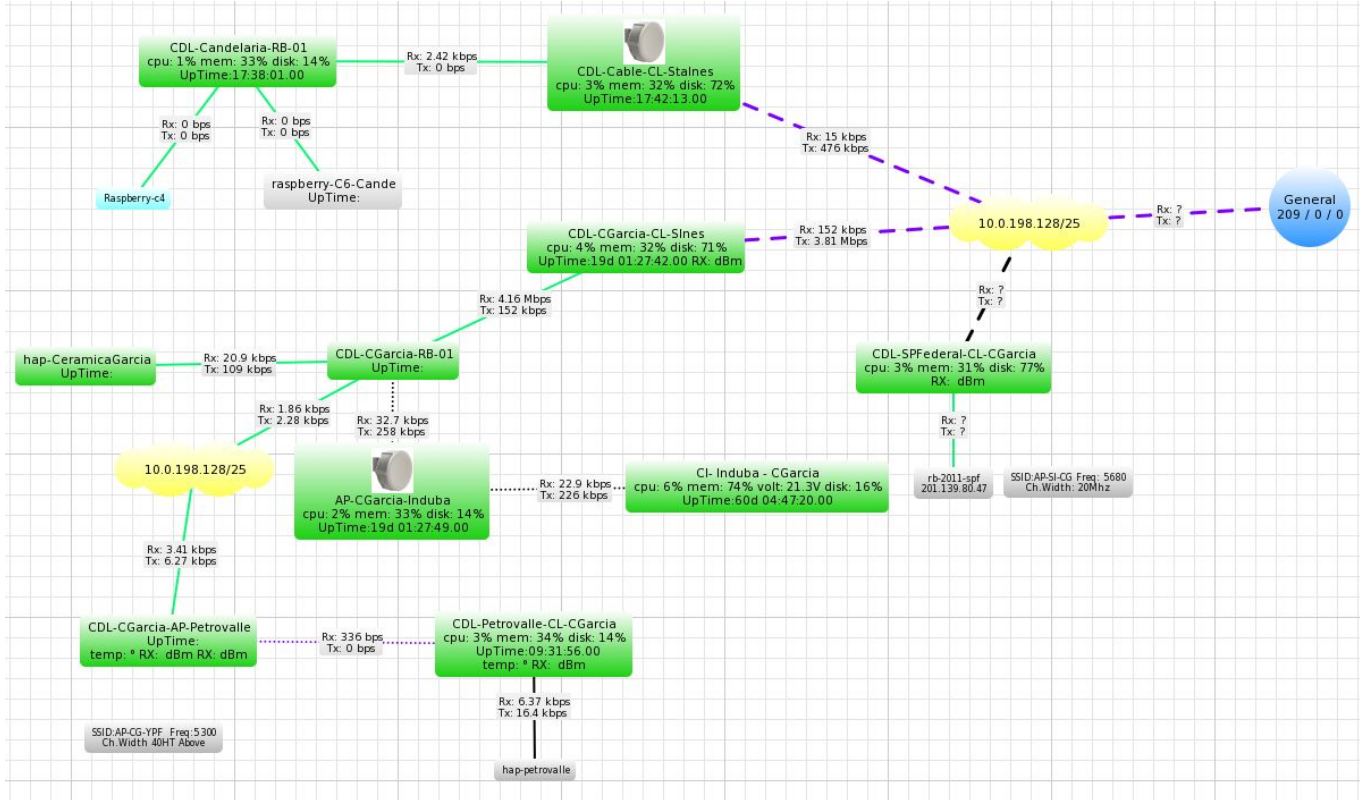
```
{{ $alert->title }}
Severity: {{ $alert->severity }}
@if ($alert->state == 0) Time elapsed: {{ $alert->elapsed }} @endif
Timestamp: {{ $alert->timestamp }}
Unique-ID: {{ $alert->uid }}
Rule: @if ($alert->name) {{ $alert->name }} @else {{ $alert->rule }} @endif
@if ($alert->faults) Faults:
@foreach ($alert->faults as $key => $value)
  #{{ $key }}: {{ $value['string'] }}
  Temperature: {{ $value['sensor_current'] }}
  Previous Measurement: {{ $value['sensor_prev'] }}
@endforeach
@endif
```

Attach template to rules:

Alert title:

Recovery title:

# Un duda y the dude?



# Zabbix



Zabbix es un software empresarial de monitoreo de redes, equipos y aplicaciones, que permite conocer y registrar el estado en tiempo real e histórico de los mismos.

Zabbix ofrece funcionalidades avanzadas de monitoreo, alertas y características de visualización de hoy que están ausentes en otros sistemas de vigilancia, incluso algunos de los mejores sistemas comerciales.

Zabbix es una solución Open Source; con lo cual puede ahorrar miles de dólares en licencias; teniendo como solución un producto tan bueno como cualquier sistema licenciado.



# Zabbix

The ZABBIX logo consists of the word "ZABBIX" in a bold, white, sans-serif font, centered within a solid red rectangular background.

Documentación: [Zabbix 5.0 LTS Manual](#)

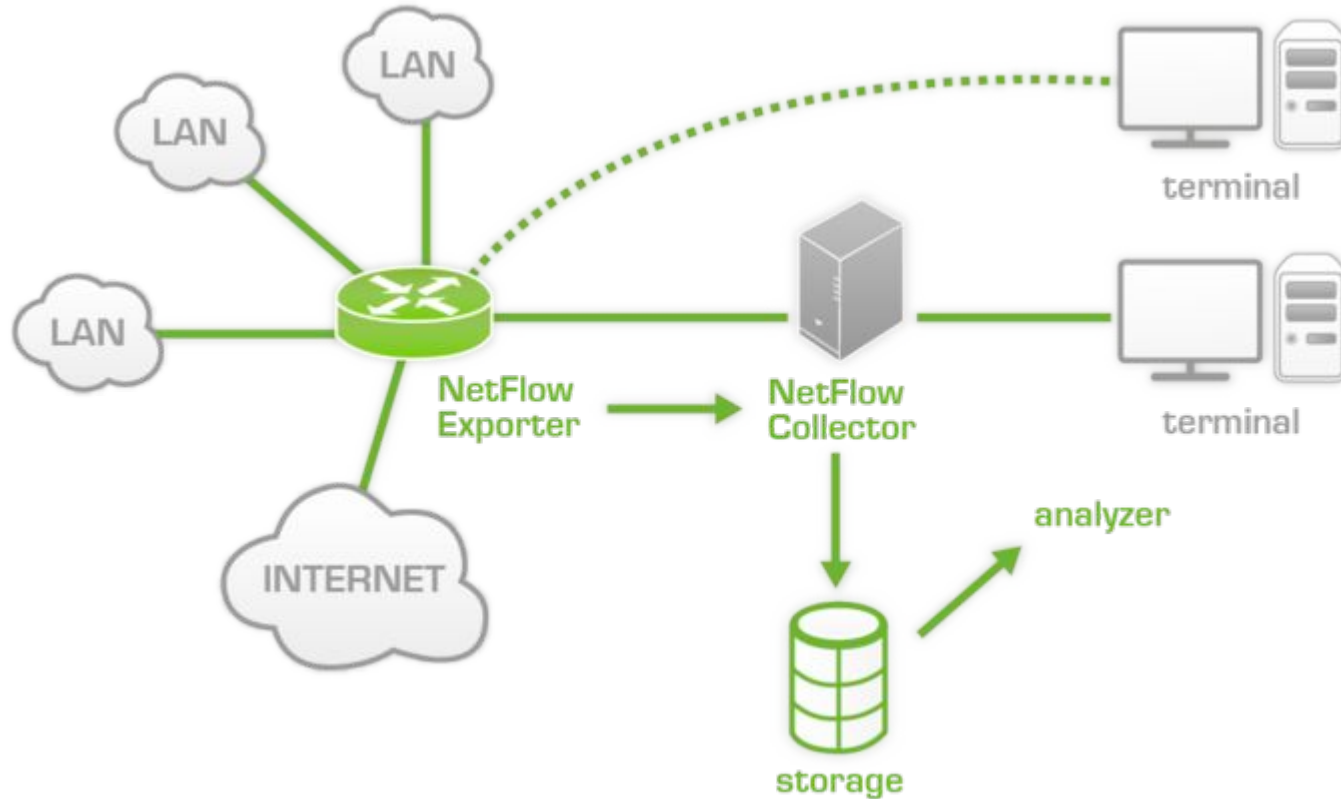
Máquinas virtuales e Imágenes: [links](#)

Comunidad zabbix en Portugués y Español: [link](#)

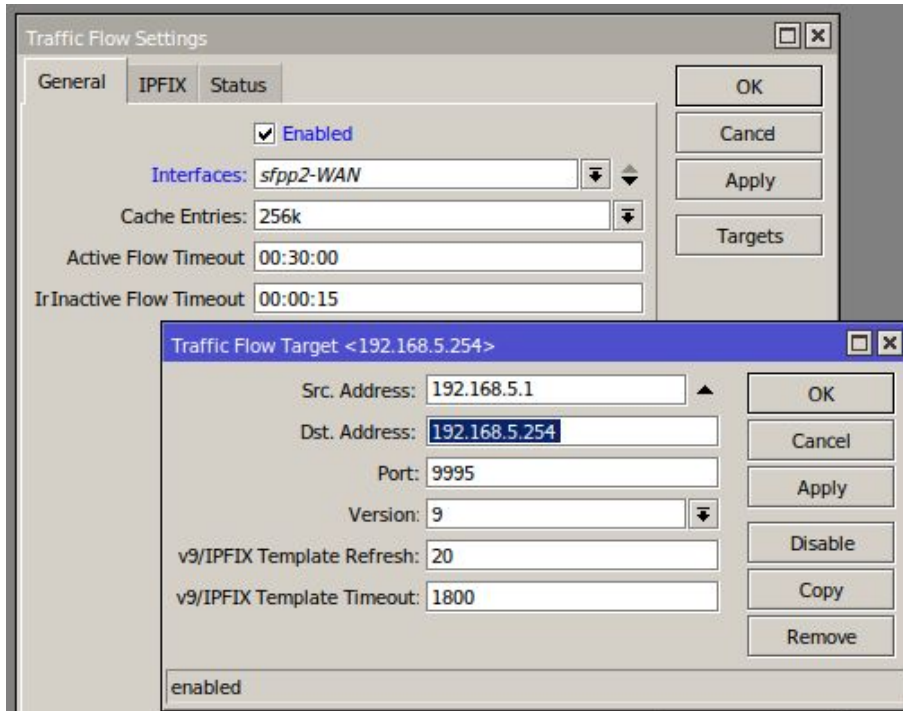
Configurar zabbix con telegram: [link](#)

Zabbix en github: [mas de 9k de repositorios](#)

# Exportador / Colector / Analizador de tráfico



# Exportar



Flujos de información a medida que entran o salen por una interface

NETFLOW v5 y v9 (Cisco)

IPFIX (IETF)

sFLOW (HP / Huawei)

Mikrotik: ip->Traffic Flow  
Netflow v5/9 / IPFIX

# Colector + Analizador de flow

Es responsable de la recepción, el almacenamiento y el procesamiento previo de los datos de flujo recibidos de un exportador de flujo.

SolarWinds: versión de prueba gratuita, [link](#)

PRTG (SNMP+Netflow): versión gratuita 100 sensores, [link](#)

ManageEngine: versión de prueba 30 días, [link](#)

nProbe + ntopng: versión de prueba muy limitada ([nProbe](#)), ([ntopng](#))

nfdump + nfsen: “the oldies but goldies” Referencias [Santiago Aggio](#)

# nfdump + nfsen

nfdump colector: [link-github](#) o desde el repositorio del SO directamente

nfcapd: colector de Netflow

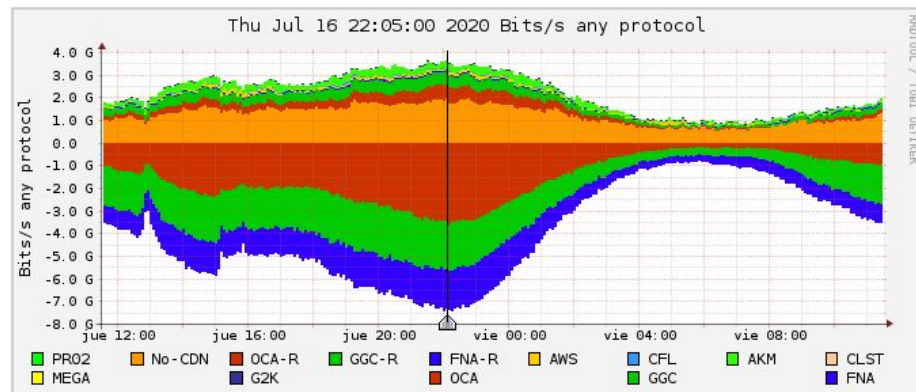
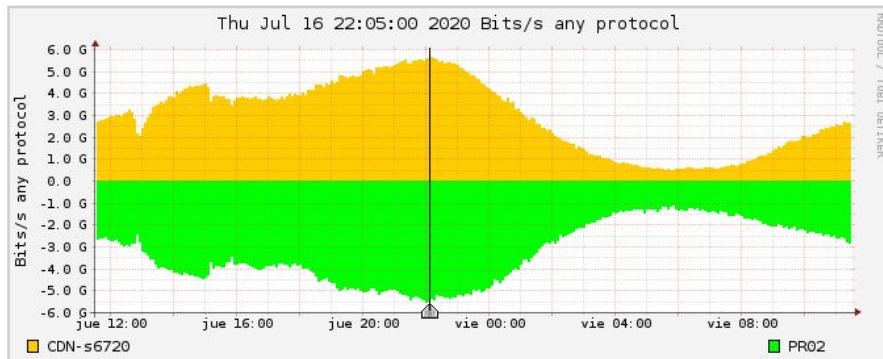
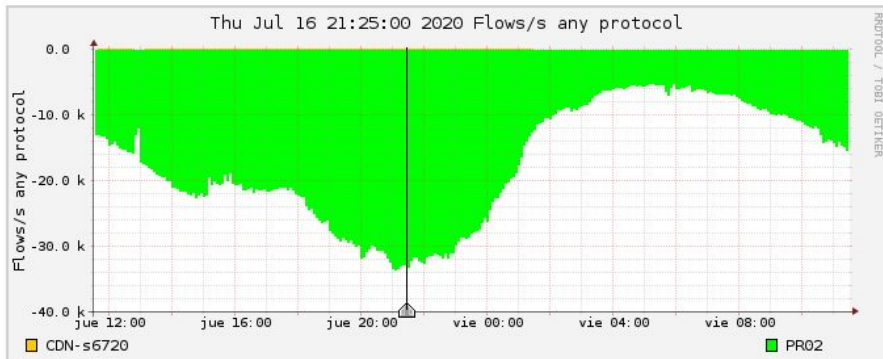
sfcapd: colector de sFlow

nfsen: analizador [instalación](#)

Nota: apache + php + nfdump + nfsen

Nota2: nfsen-ng -> [link](#)

# nfdump + nfsen



## Statistics timeslot Jul 16 2020 - 22:05

Channel:	Flows:		Packets:		Traffic:			
	all:	all:	all:	tcp:	udp:	icmp:	other:	
<input checked="" type="checkbox"/> G2K	0.2 /s	0.2 /s	111.7 b/s	13.4 b/s	4.1 b/s	94.2 b/s	0 b/s	
<input checked="" type="checkbox"/> MEGA	3.2 /s	12.0 /s	72.6 kb/s	69.0 kb/s	2.6 kb/s	1.0 kb/s	0 b/s	
<input checked="" type="checkbox"/> CLST	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s	
<input checked="" type="checkbox"/> AKM	472.7 /s	24.3 k/s	267.9 Mb/s	267.8 Mb/s	62.9 kb/s	7.5 kb/s	2.3 b/s	
<input checked="" type="checkbox"/> CFL	92.0 /s	4.6 k/s	49.0 Mb/s	49.0 Mb/s	15.9 kb/s	107.8 b/s	0 b/s	
<input checked="" type="checkbox"/> AWS	390.5 /s	9.1 k/s	80.0 Mb/s	77.1 Mb/s	2.9 Mb/s	13.5 kb/s	0 b/s	
<input checked="" type="checkbox"/> FNA-R	1.2 k/s	12.0 k/s	57.0 Mb/s	28.6 Mb/s	28.5 Mb/s	319.4 b/s	0 b/s	
<input checked="" type="checkbox"/> GGC-R	2.4 k/s	58.1 k/s	540.2 Mb/s	205.7 Mb/s	334.5 Mb/s	11.5 kb/s	0 b/s	
<input checked="" type="checkbox"/> OCA-R	308.3 /s	57.4 k/s	662.5 Mb/s	662.5 Mb/s	0 b/s	140.7 b/s	0 b/s	
<input checked="" type="checkbox"/> No-CDN	25.2 k/s	412.9 k/s	2.0 Gb/s	1.6 Gb/s	412.1 Mb/s	1.3 Mb/s	3.5 Mb/s	
<input checked="" type="checkbox"/> PR02	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s	
<input checked="" type="checkbox"/> OCA	145.9 /s	300.5 k/s	3.4 Gb/s	3.4 Gb/s	0 b/s	0 b/s	0 b/s	
<input checked="" type="checkbox"/> GGC	67.2 /s	193.1 k/s	2.1 Gb/s	1.1 Gb/s	996.3 Mb/s	0 b/s	0 b/s	
<input checked="" type="checkbox"/> FNA	1.4 k/s	161.3 k/s	1.7 Gb/s	979.3 Mb/s	725.7 Mb/s	155.7 b/s	0 b/s	
<b>TOTAL</b>	<b>all:</b>	<b>all:</b>	<b>all:</b>	<b>tcp:</b>	<b>udp:</b>	<b>icmp:</b>	<b>other:</b>	
	31.7 k/s	1.2 M/s	11.0 Gb/s	8.4 Gb/s	2.5 Gb/s	1.4 Mb/s	3.5 Mb/s	

All None Display:  Sum  Rate

# Usando herramientas

nfsen + plugins -> flowdoh

## Flows:

Rank	Host Address	IP Address	Flows	% Flows		
1	ipv4-cl [redacted]	201.1 [redacted]	434,063	13.5%	🔗	🗨
2	ipv4-cl [redacted]	201.1 [redacted]	409,365	12.8%	🔗	🗨
3	2803: [redacted]	2803: [redacted]	177,975	5.5%	🔗	🗨
4	2803: [redacted]	2803: [redacted]	172,428	5.4%	🔗	🗨
5	ipv4-cl [redacted]	201.1 [redacted]	64,737	2.0%	🔗	🗨
6	2803: [redacted] 5ba:a211	2803: [redacted] 5ba:a211	61,009	1.9%	🔗	🗨
7	whats [redacted] 1.facebook.com	2a03: [redacted] 260	60,930	1.9%	🔗	🗨
8	dns.google	8.8.8.8	59,422	1.9%	🔗	🗨
9	2803: [redacted] e66:b9f0	2803: [redacted] e66:b9f0	58,254	1.8%	🔗	🗨
10	ipv4-cl [redacted]	138.18 [redacted]	56,845	1.8%	🔗	🗨

Top Talkers Alerts

Timeslot: 2019-11-20 22:00 Jump: 1 hour

Showing results for the timeslot at 2019-11-20 22:00

## Top Talkers:

## Bytes:

Rank	Host Address	IP Address	Bytes	% Bytes		
1	168.19 [redacted]	168.19 [redacted]	42,134 MB	19.9%	🔗	🗨
2	168.19 [redacted]	168.19 [redacted]	16,874 MB	8.0%	🔗	🗨
3	168.19 [redacted]	168.19 [redacted]	14,490 MB	6.9%	🔗	🗨
4	2803: [redacted]	2803: [redacted]	14,224 MB	6.7%	🔗	🗨
5	2803: [redacted]	2803: [redacted]	13,625 MB	6.4%	🔗	🗨
6	168.19 [redacted]	168.19 [redacted]	12,827 MB	6.1%	🔗	🗨
7	2001: [redacted] 0:358e	2001: [redacted] 0:face:b00c:0:358e	10,016 MB	4.7%	🔗	🗨
8	2001: [redacted] :3333:a3f	2001: [redacted] 0:face:b00c:3333:a3f	9,858 MB	4.7%	🔗	🗨
9	2803: [redacted]	2803: [redacted]	5,553 MB	2.6%	🔗	🗨
10	ipv4-cl [redacted] n.ar	138.18 [redacted]	5,164 MB	2.4%	🔗	🗨

37%

# DNS (Software)

- 1) BIND : Autoritativo, Recursivo, DNSSEC, IPv4/v6, Response Rate Limit, large
- 2) UNBOUND : “Autoritativo...”, Recursivo, Cache, DNSSEC, DNS-over-TLS, DNSSEC, IPv4/v6
- 3) DNSMASQ : “Autoritativo...”, Cache, DNSSEC, IPv4/v6, small/local
- 4) POWERDNS : Autoritativo o Recursivo, IPv4/v6, statistics, high-end features (Filtering, parental control), small/large

[https://en.wikipedia.org/wiki/Comparison\\_of\\_DNS\\_server\\_software](https://en.wikipedia.org/wiki/Comparison_of_DNS_server_software)



# Cache y filtrado

## Pi-hole: dns black hole, DNSMASQ



System | **Blocklists** | DNS | DHCP | API / Web interface | Privacy | Teleporter

Blocklists used to generate Pi-hole's Gravity: 9

Enabled	List	Delete
<input checked="" type="checkbox"/>	<a href="https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts">https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts</a>	
<input checked="" type="checkbox"/>	<a href="https://mirror1.malwaredomains.com/files/justdomains">https://mirror1.malwaredomains.com/files/justdomains</a>	
<input checked="" type="checkbox"/>	<a href="http://sysctl.org/cameleon/hosts">http://sysctl.org/cameleon/hosts</a>	
<input checked="" type="checkbox"/>	<a href="https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist">https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist</a>	
<input type="checkbox"/>	<a href="https://s3.amazonaws.com/lists.disconnect.me/simple_tracking.txt">https://s3.amazonaws.com/lists.disconnect.me/simple_tracking.txt</a>	
<input type="checkbox"/>	<a href="https://s3.amazonaws.com/lists.disconnect.me/simple_ad.txt">https://s3.amazonaws.com/lists.disconnect.me/simple_ad.txt</a>	
<input type="checkbox"/>	<a href="https://hosts-file.net/ad_servers.txt">https://hosts-file.net/ad_servers.txt</a>	
<input type="checkbox"/>	<a href="https://raw.githubusercontent.com/HenningVanRaumle/pihole-ytadblock/master/ytadblock.txt">https://raw.githubusercontent.com/HenningVanRaumle/pihole-ytadblock/master/ytadblock.txt</a>	
<input type="checkbox"/>	<a href="https://github.com/anudeepND/youtubeadsblacklist/blob/master/domainlist.txt">https://github.com/anudeepND/youtubeadsblacklist/blob/master/domainlist.txt</a>	

Upstream DNS Servers

IPv4	IPv6	Name
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Google (ECS)
<input type="checkbox"/>	<input type="checkbox"/>	OpenDNS (ECS)
<input type="checkbox"/>	<input type="checkbox"/>	Level3
<input type="checkbox"/>	<input type="checkbox"/>	Comodo
<input type="checkbox"/>	<input type="checkbox"/>	DNS.WATCH
<input type="checkbox"/>	<input type="checkbox"/>	Quad9 (filtered, DNSSEC)
<input type="checkbox"/>	<input type="checkbox"/>	Quad9 (unfiltered, no DNSSEC)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Quad9 (filtered + ECS)
<input type="checkbox"/>	<input type="checkbox"/>	Cloudflare

### Whitelist

Add a domain (example.com or sub.example.com)

- app.getresponse.com
- debian.org
- github.com

<https://pi-hole.net/>

# Cache y filtrado

## pfBlockerNG: addon para pfSense, via UNBOUND

The screenshot shows the pfSense Package Manager interface. The 'Available Packages' tab is selected. A search for 'pfblocker' has been performed, resulting in two entries:

Name	Version	Description	Action
pfBlockerNG	2.1.2_3	pfBlockerNG is the Next Generation of pfBlocker. Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. GeoIP database by MaxMind Inc. (GeoLite2 Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced Integration for Proofpoint ET IQRisk IP Reputation Threat Sources. Domain Name (DNSBL) blocking via Unbound DNS Resolver.	<a href="#">+ Install</a>
pfBlockerNG-devel	2.1.2_2	pfBlockerNG is the Next Generation of pfBlocker. Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. GeoIP database by MaxMind Inc. (GeoLite2 Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced Integration for Proofpoint ET IQRisk IP Reputation Threat Sources. Domain Name (DNSBL) blocking via Unbound DNS Resolver.	<a href="#">+ Install</a>

The screenshot shows the pfSense DNSBL configuration page. The 'DNSBL Feeds' tab is active. The 'Info' section shows the current configuration for the 'ADs' feed. The 'DNSBL Source Definitions' section lists several feeds with their respective URLs and actions. The 'Settings' section shows the 'Action' set to 'Unbound' and the 'Update Frequency' set to 'Once a day'.

Name / Description	Format	State	Source	Header/Label	Action
ADs - Collection of Advertisement Domain Feeds.					
https://adaway.org/hosts.txt	Auto	ON		Adaway	<a href="#">Delete</a>
https://s3.amazonaws.com/lists.disconnect.me/simple_ad.txt	Auto	ON		D_Me_Ads	<a href="#">Delete</a>
https://s3.amazonaws.com/lists.disconnect.me/simple_tracking.txt	Auto	ON		D_Me_Tracking	<a href="#">Delete</a>
https://hosts-file.net/ad_servers.txt	Auto	ON		hhHosts_ATS	<a href="#">Delete</a>
http://sysctl.org/cameleon/hosts	Auto	ON		Cameleon	<a href="#">Delete</a>
https://www.squidblacklist.org/downloads/dp-ads.acl	Auto	ON		SBL_Ads	<a href="#">Delete</a>
https://pgl.yoyo.org/adserver/serverlist.php?hostformat=nohtml	Auto	ON		Yoyo	<a href="#">Delete</a>

The screenshot shows the 'DNSBL Feeds Summary' table in pfSense. The table lists the feeds and their configuration:

Name	Description	Action	Frequency	Logging	Actions
ADs	ADs - Collectio...	Unbound	Once a day	Enabled	<a href="#">Edit</a> <a href="#">Delete</a>
Malicious	Malicious - Col...	Unbound	Once a day	Enabled	<a href="#">Edit</a> <a href="#">Delete</a>

<https://www.linuxincluded.com/block-ads-malvertising-on-pfsense-using-pfblockerng-dnsbl/>

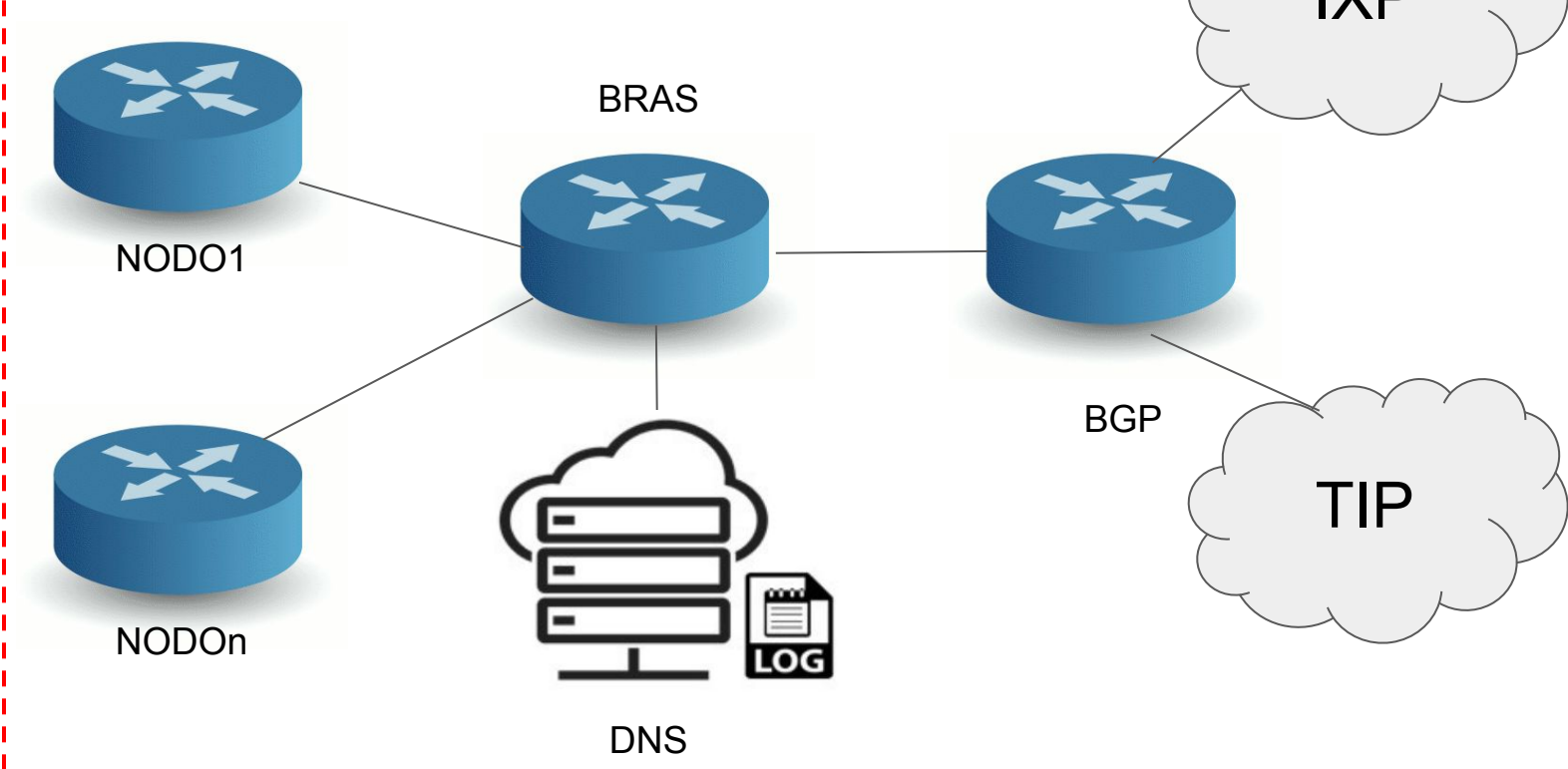
# ISP

Clientes

Clientes

Clientes

Clientes



# Objetivo principal

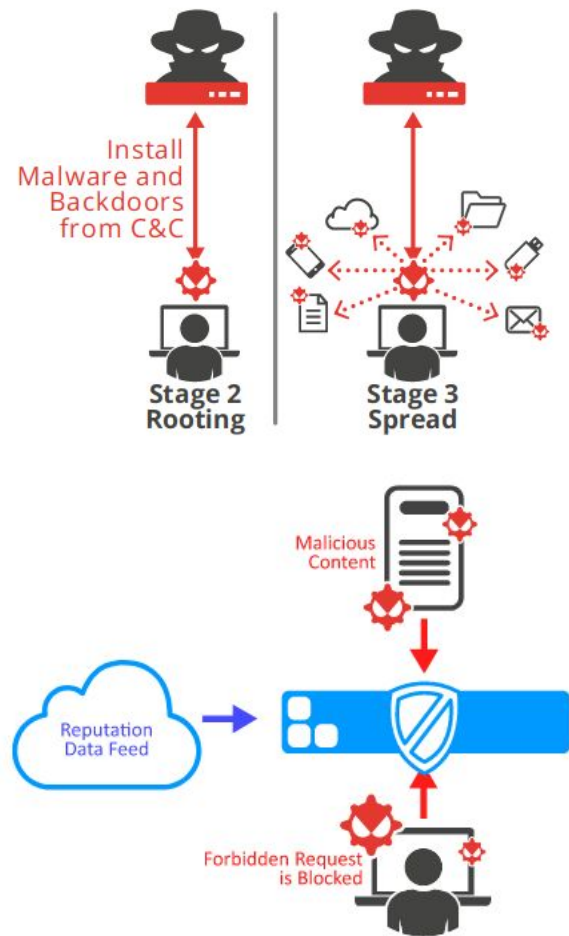
En el entorno actual, la evolución de los dispositivos móviles e IoT, Smart se está convirtiendo en la norma.

No a todos los dispositivos se puede proteger con un firewall o antivirus, hay que bloquear la fuente.

Prevención contra phishing / malware, bloqueando el acceso a dominios comprometidos.

Agilizar respuesta de flujos DNS en nuestra red

Bloquear publicidad? (opcional?)



# Recurros DNS

**i** Status running

**♥** HA State none

**📄** Node pve01

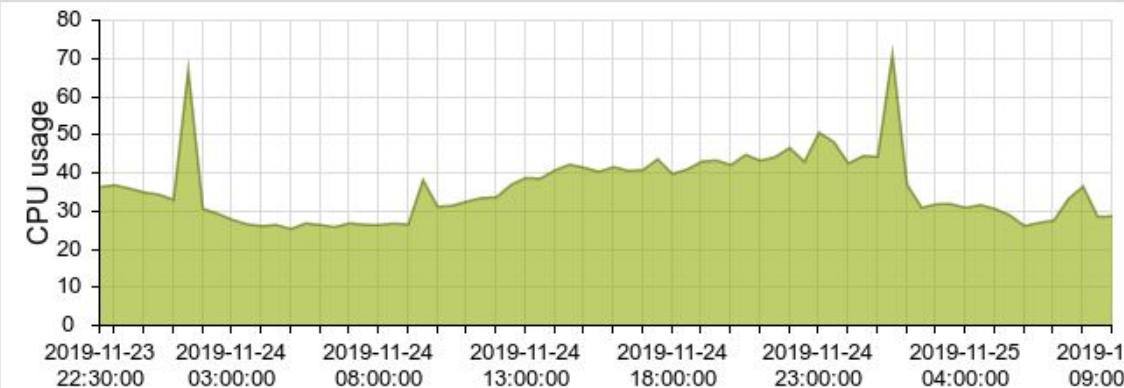
**🖨️** CPU usage 36.06% of 4 CPU(s)

**📄** Memory usage 79.73% (3.19 GiB of 4.00 GiB)

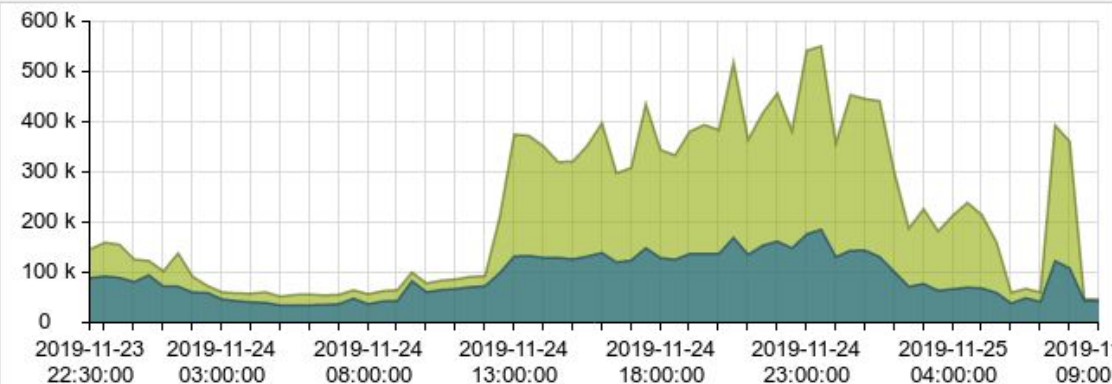
**📄** Bootdisk size 10.00 GiB

2 x VM:	pfSense
CPU	4 cores
RAM	4 GB
HD	10 GB

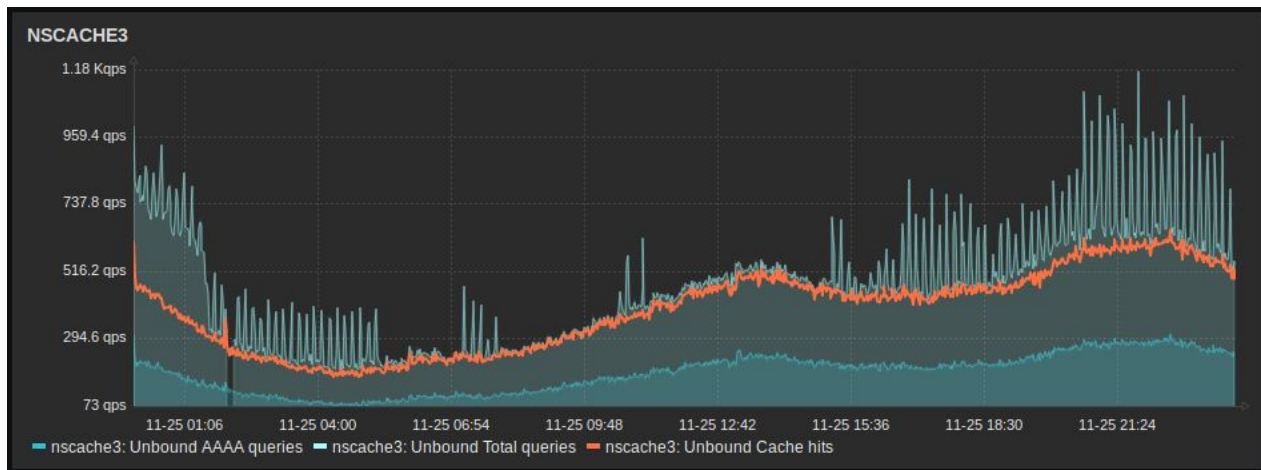
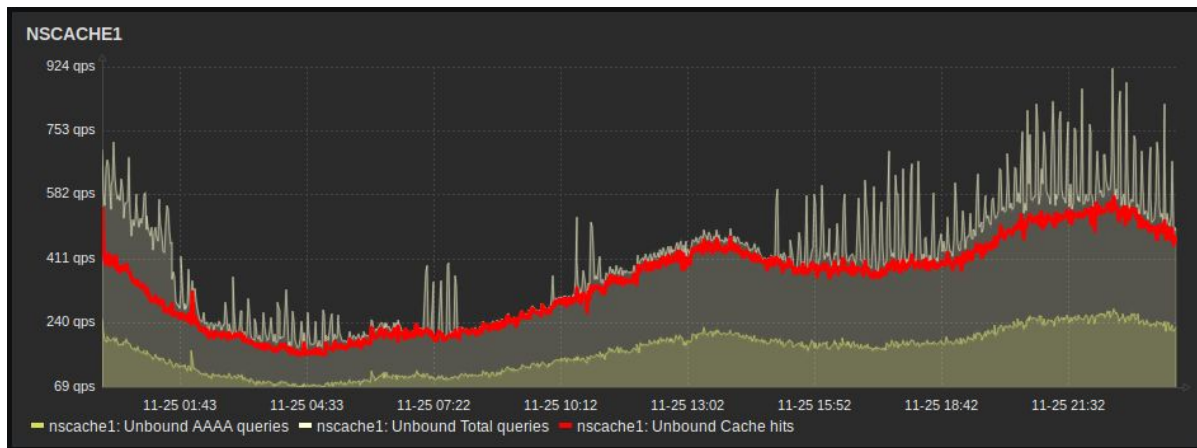
## CPU usage



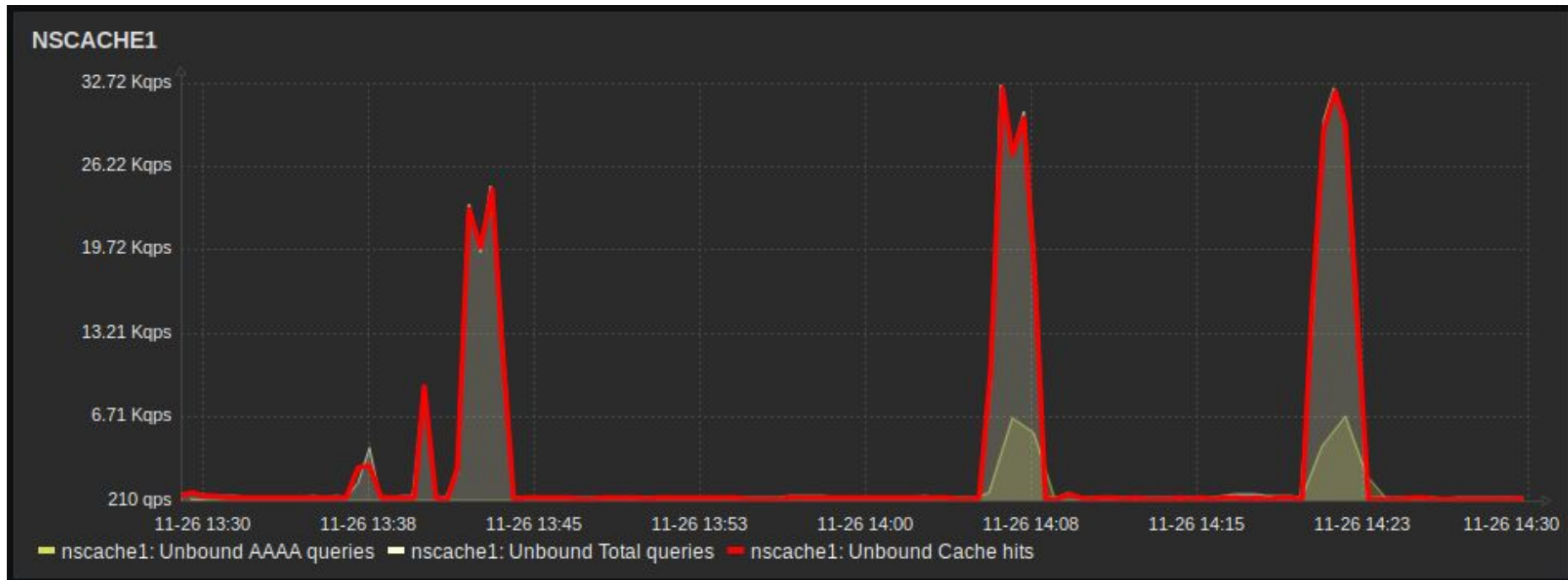
## Network traffic



# Recursos DNS



# Benchmark DNS



# Referencias

**pi-hole:** Network-wide Ad Blocking

<https://pi-hole.net> - <https://github.com/pi-hole/pi-hole/#one-step-automated-install>

**pfSense:** Firewall Open Source

<https://pfsense.org> - <https://docs.netgate.com/pfsense/en/latest/install/installing-pfsense.html> - <https://www.linuxincluded.com/block-ads-malvertising-on-pfsense-using-pfblockerng-dnsbl/>

**OPNsense:** Fork derivado de pfSense (2015)

<https://opnsense.org> - <https://devinstechblog.com/block-ads-with-dns-in-opnsense/>

**Unbound:** Validating, recursive, caching DNS resolver

<https://nlnetlabs.nl/projects/unbound/about/> - <https://nlnetlabs.nl/documentation/unbound/howto-setup/> - <https://medium.com/@steffinstanly/unbound-dns-blocking-3567986a5735>

**dns-zone-blacklist:** Genera archivos de zona para Bind, Unbound y Dnsmasq

<https://github.com/oznu/dns-zone-blacklist> -

**StevenBlack/hosts:** Listas de hosts para ser utilizadas, se actualizan con frecuencia.

<https://github.com/StevenBlack/hosts> -



# Referencias

**dnsperf:** DNS query load simulator

<https://www.dns-oarc.net/> - <https://www.dns-oarc.net/tools/dnsperf> -  
<https://github.com/DNS-OARC/dnsperf>

**DNS Benchmark:** Domain Name Speed Benchmark

<https://www.grc.com/dns/benchmark.htm>

**<https://n9.cl/mxz4>**



Darío Fernández - [dfernandez@researchsrl.com.ar](mailto:dfernandez@researchsrl.com.ar)  
Research SRL - [www.researchsrl.com.ar](http://www.researchsrl.com.ar)  
IXFO - Internet x fibra óptica - [www.ixfo.com.ar](http://www.ixfo.com.ar)