CAPPI

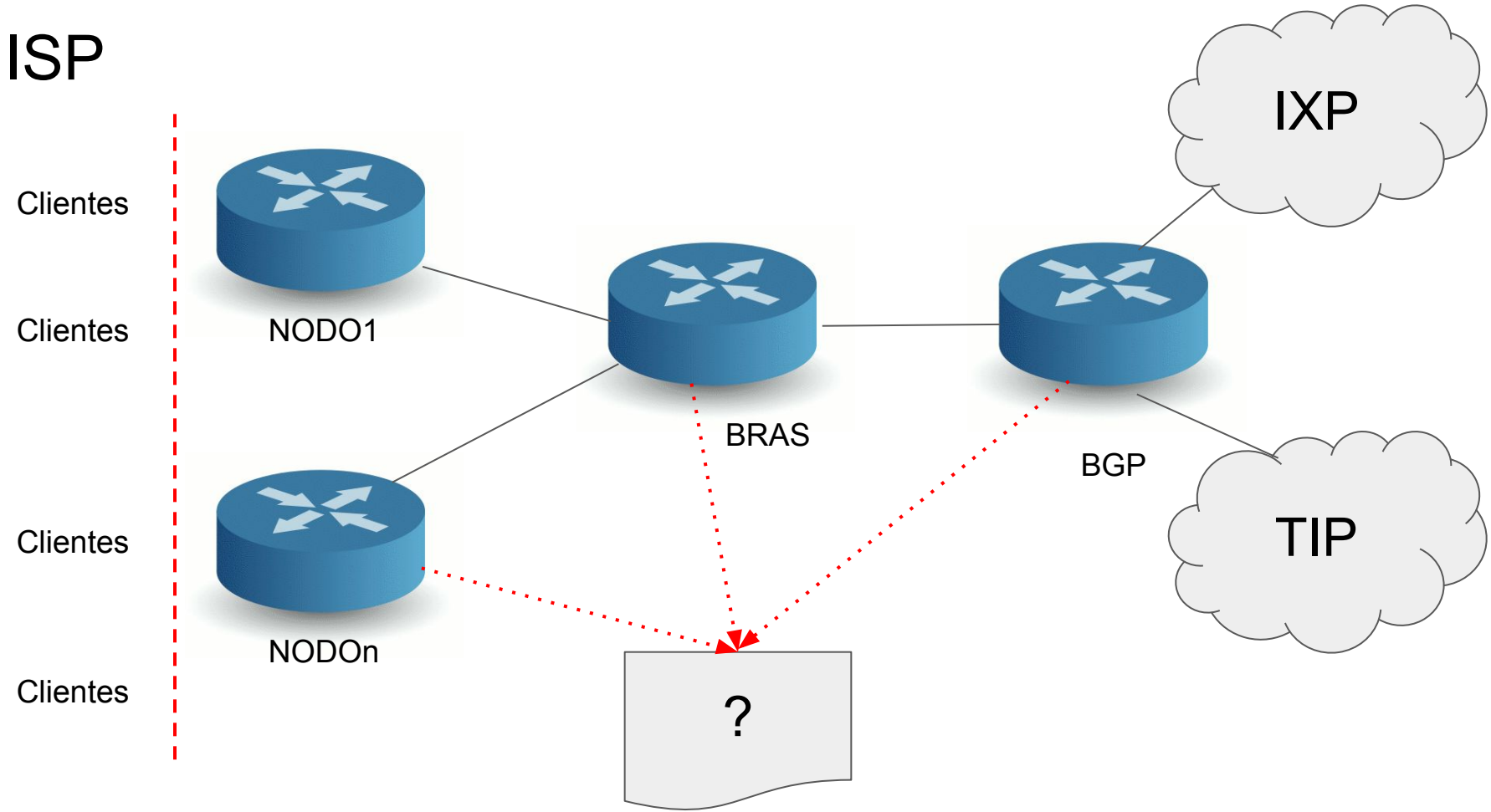
CAMARA ARGENTINA DE PEQUEÑOS PROVEEDORES DE INTERNET

Monitoreo para ISP

Usos de Herramientas de monitoreo para ISP
Optativas / Necesarias

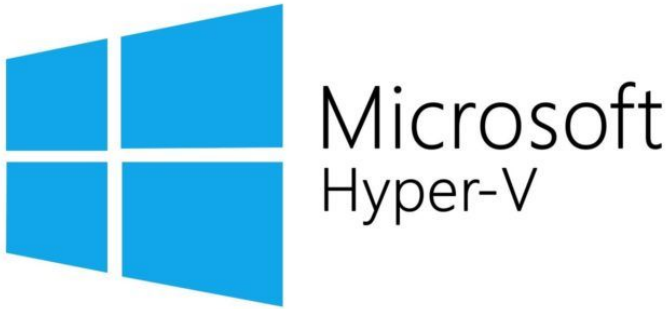
Darío Fernández Research SRL

(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
Clientes
Clientes
Clientes
Clientes
NODO1
NODOn
BRAS
BGP
IXP
TIP
?

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

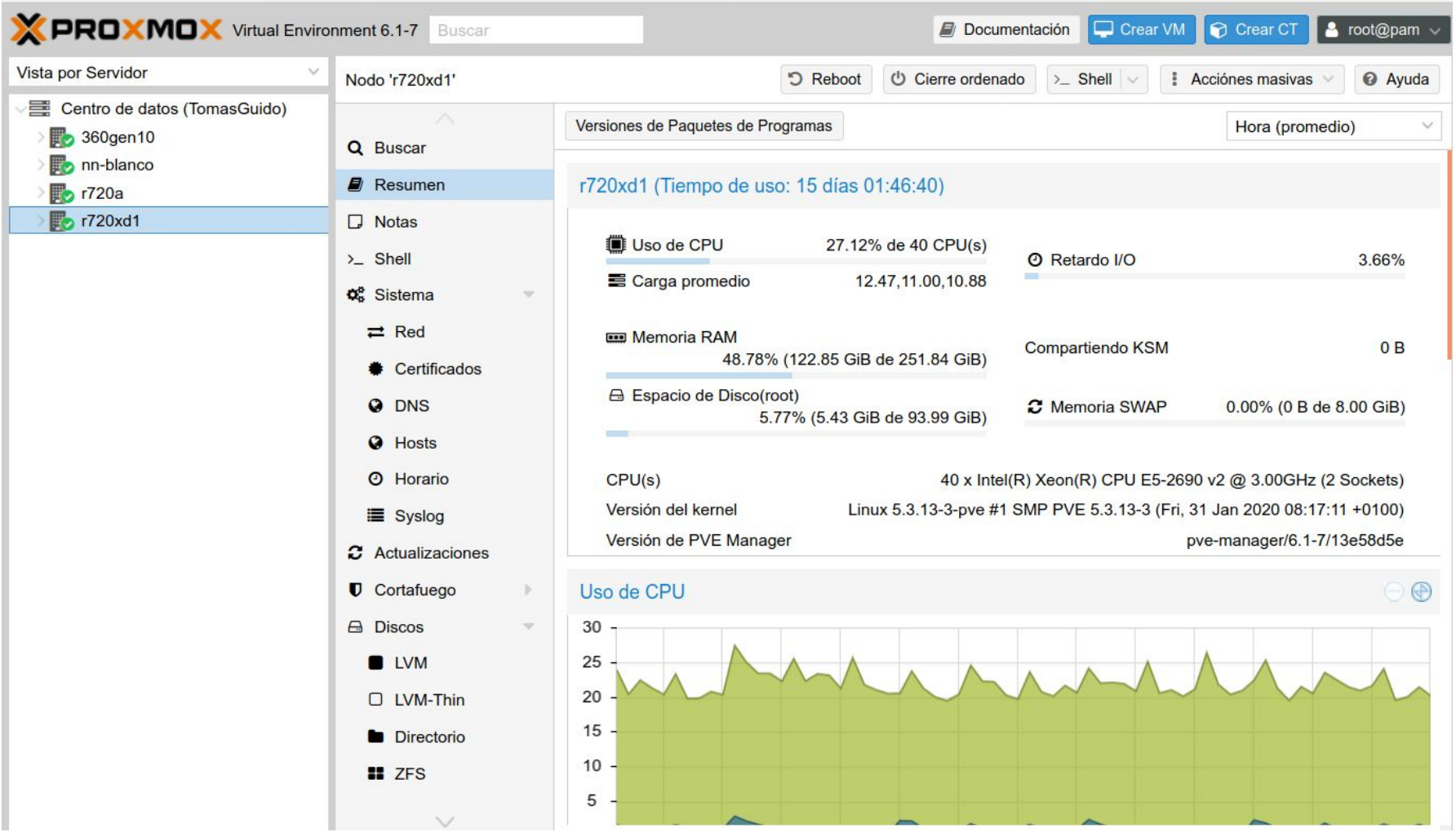


Download ISO image : Descargue el Proxmox VE ISO, luego cópielo a una unidad flash USB o CD / DVD para usarlo. Link de descargas

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


PROXMOX Virtual Environment 6.1-7
Buscar
Documentación
Crear VM
Crear CT
root@pam
Vista por Servidor
Centro de datos (TomasGuido)
360gen10
nn-blanco
r720a
r720xd1
Nodo 'r720xd1'
Reboot
Cierre ordenado
Shell
Acciónes masivas
Ayuda
Buscar
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
Retardo I/O 3.66%
Memoria RAM 48.78% (122.85 GiB de 251.84 GiB)
Compartiendo KSM 0 B
Espacio de Disco(root) 5.77% (5.43 GiB de 93.99 GiB)
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
30
25
20
15
10
5

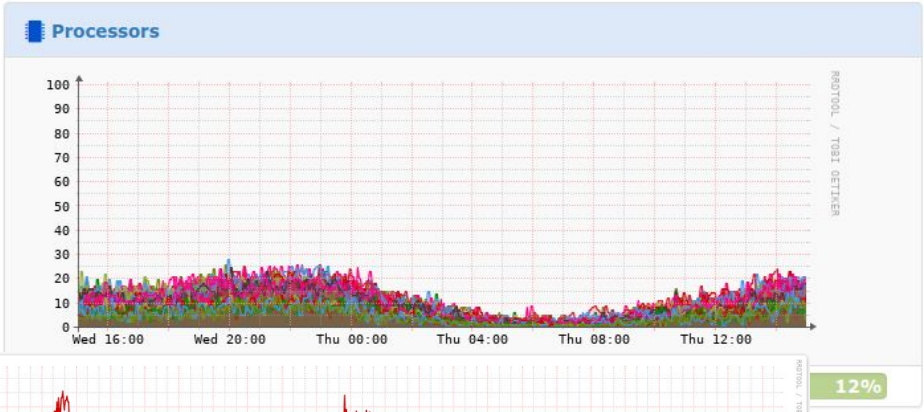
Que quiero saber?

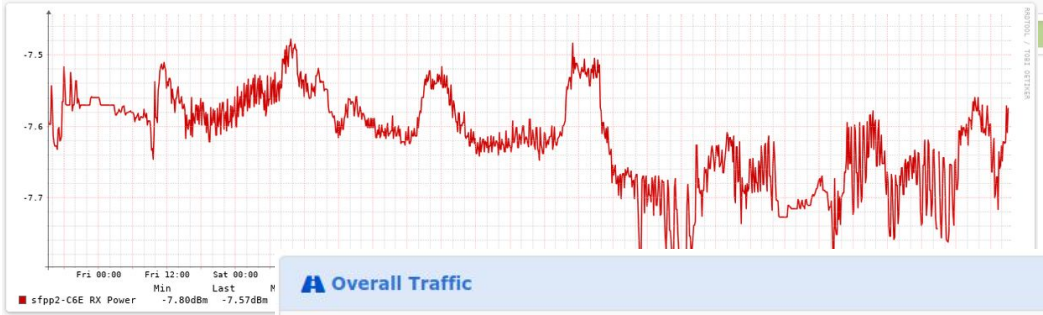
Uso de CPU?

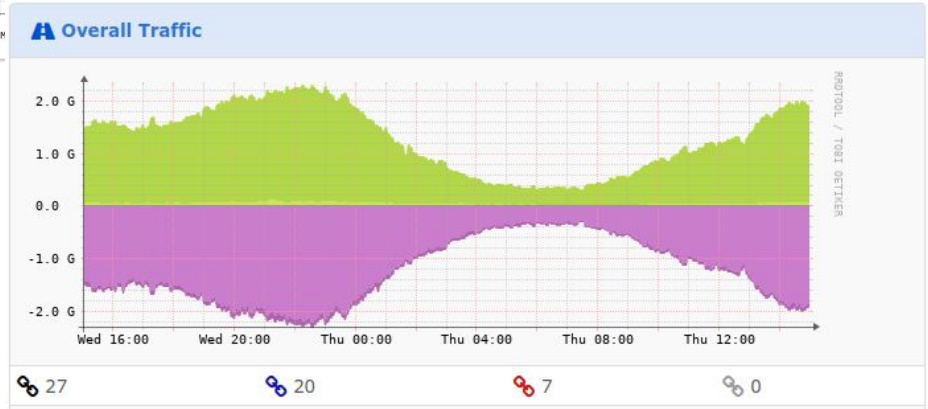
Tráfico de una Interface?

Potencia de un link?

Pérdida de paquetes hacia un destino?





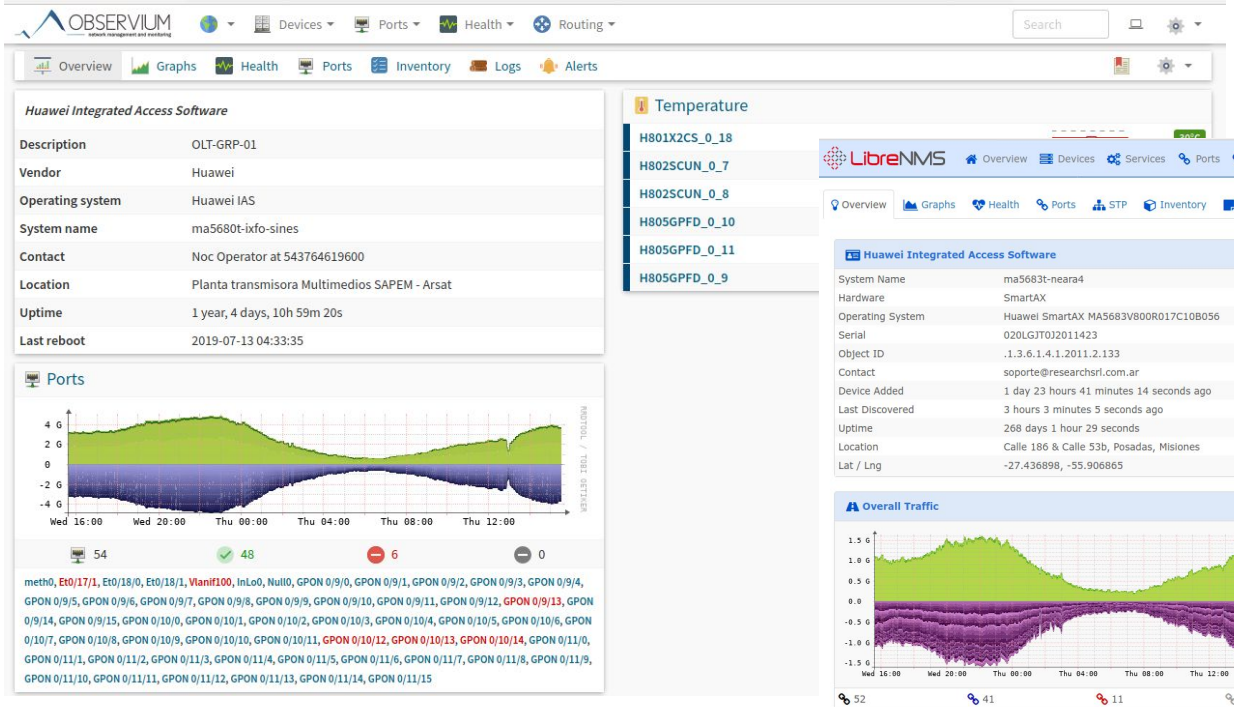


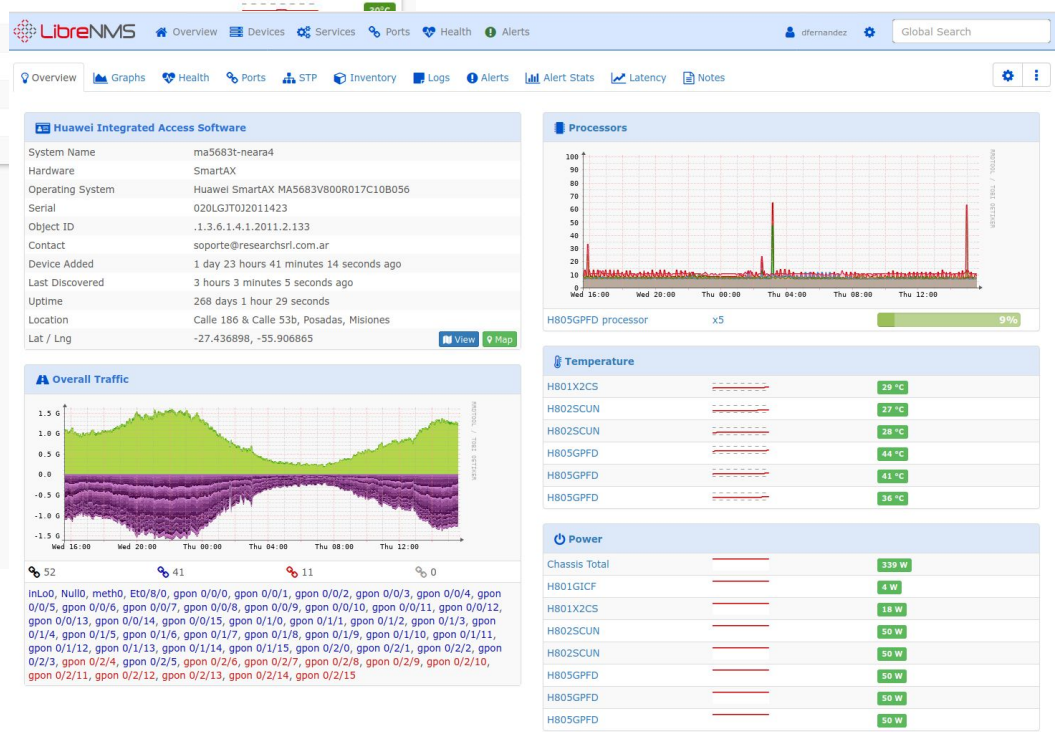
SNMP: Simple Network Management Protocol

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





Instalación de LibreNMS

LibreNMS Documentation

- LibreNMS Docs
- LibreNMS Installation Guides
- GitHub LibreNMS

Centos / Ubuntu

- Support for both Apache and Nginx Web Servers
- Installation Guide

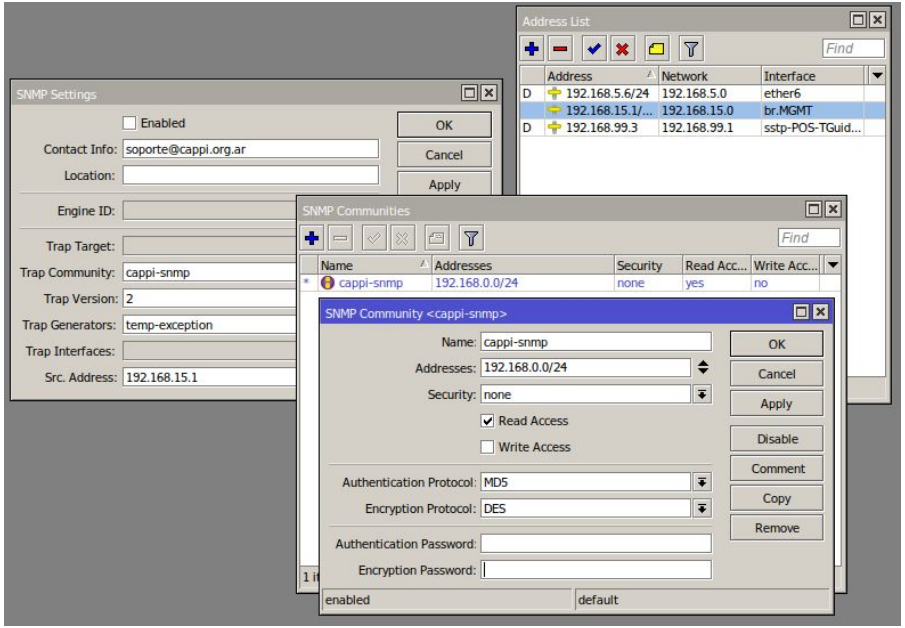
Virtual Machines

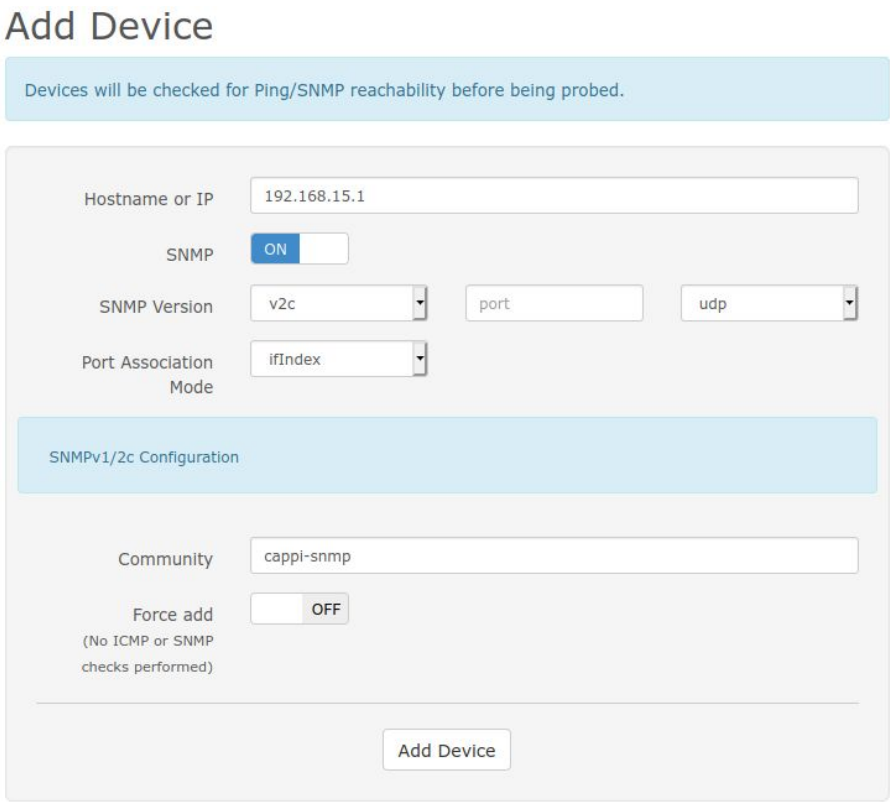
- LibreNMS Virtual Machines: Documentation
- LibreNMS: OVA Images

Docker Images

- Docker image documenation located on: GitHub LibreNMS/Docker
- LibreNMS on: dockerhub
- LibreNMS on: QUAY

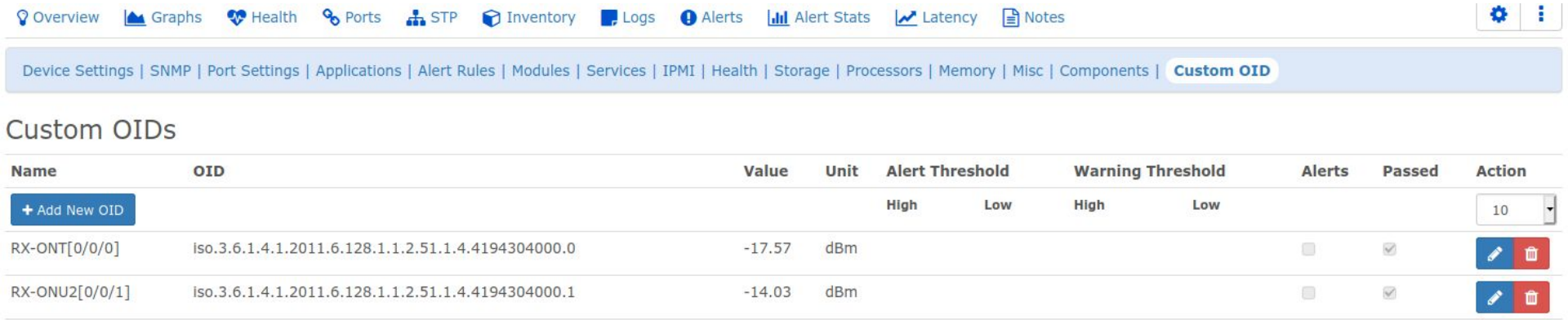
Agregar un nuevo dispositivo





Custom OIDs

Si se que preguntar puedo agregarlo a mano?



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"

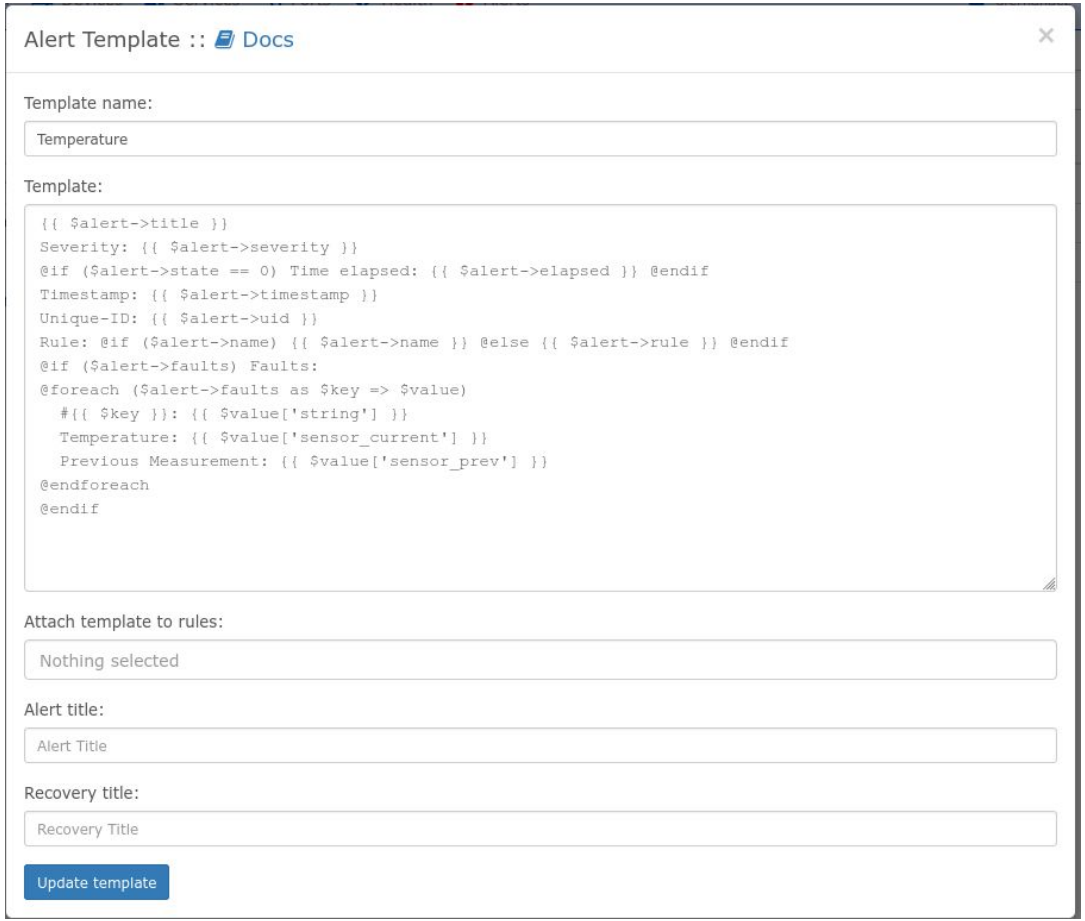
RX-Power
iso.3.6.1.4.1.2011.6.128.1.1.2.51.1.4.4194304000.0 = INTEGER: -1762
iso.3.6.1.4.1.2011.6.128.1.1.2.51.1.4.4194304000.1 = INTEGER: -1403

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

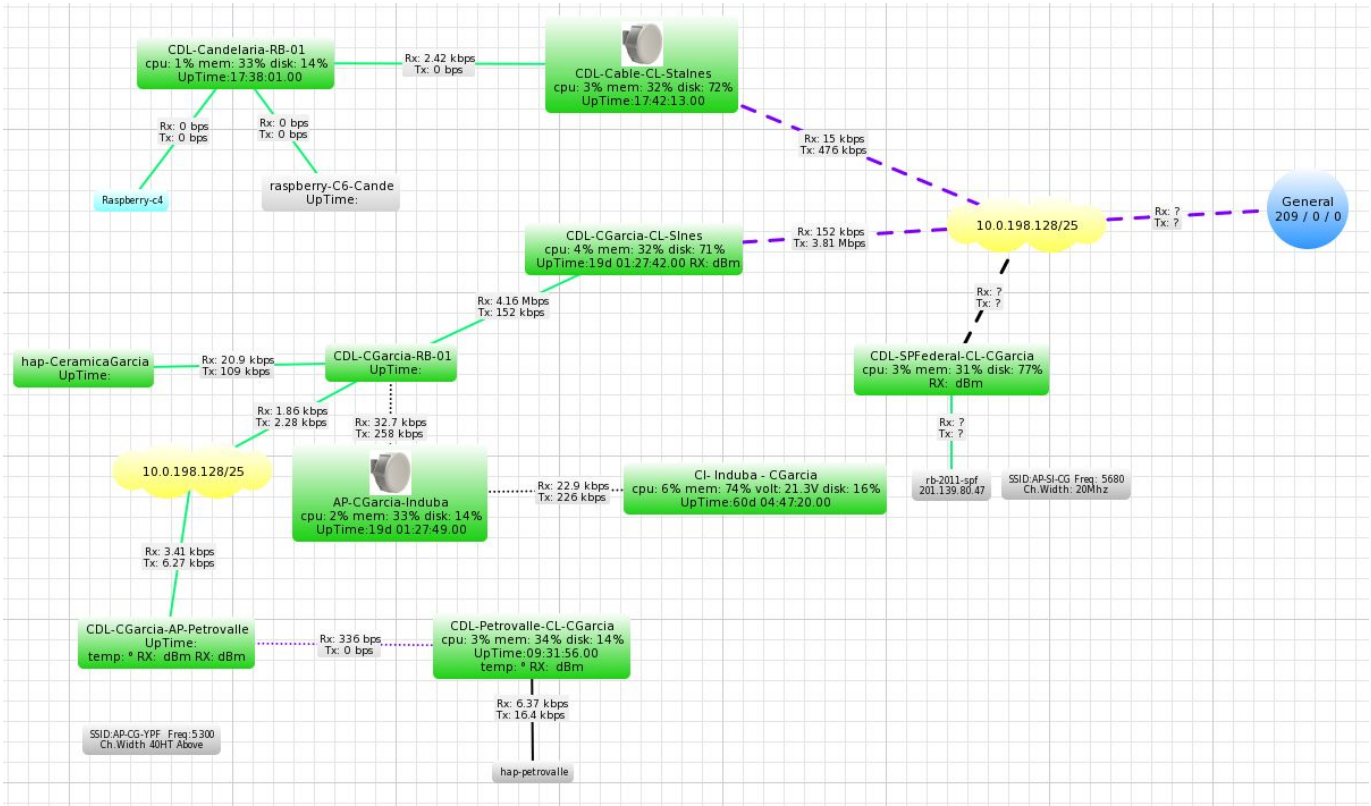
Distancia calculada en base a la potencia
iso.3.6.1.4.1.2011.6.128.1.1.2.46.1.20.4194304000.0 = INTEGER: 23
iso.3.6.1.4.1.2011.6.128.1.1.2.46.1.20.4194304000.1 = INTEGER: 3
el valor 419430400 sale de Frame/Slot/Port y el .XX corresponde a la ONU-ID registrada en ese puerto

Templates de Alerta

Existen Templates creados por la comunidad y también se pueden crear templates para generar alertas, su documentación aquí



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

Documentación: Zabbix 5.0 LTS Manual

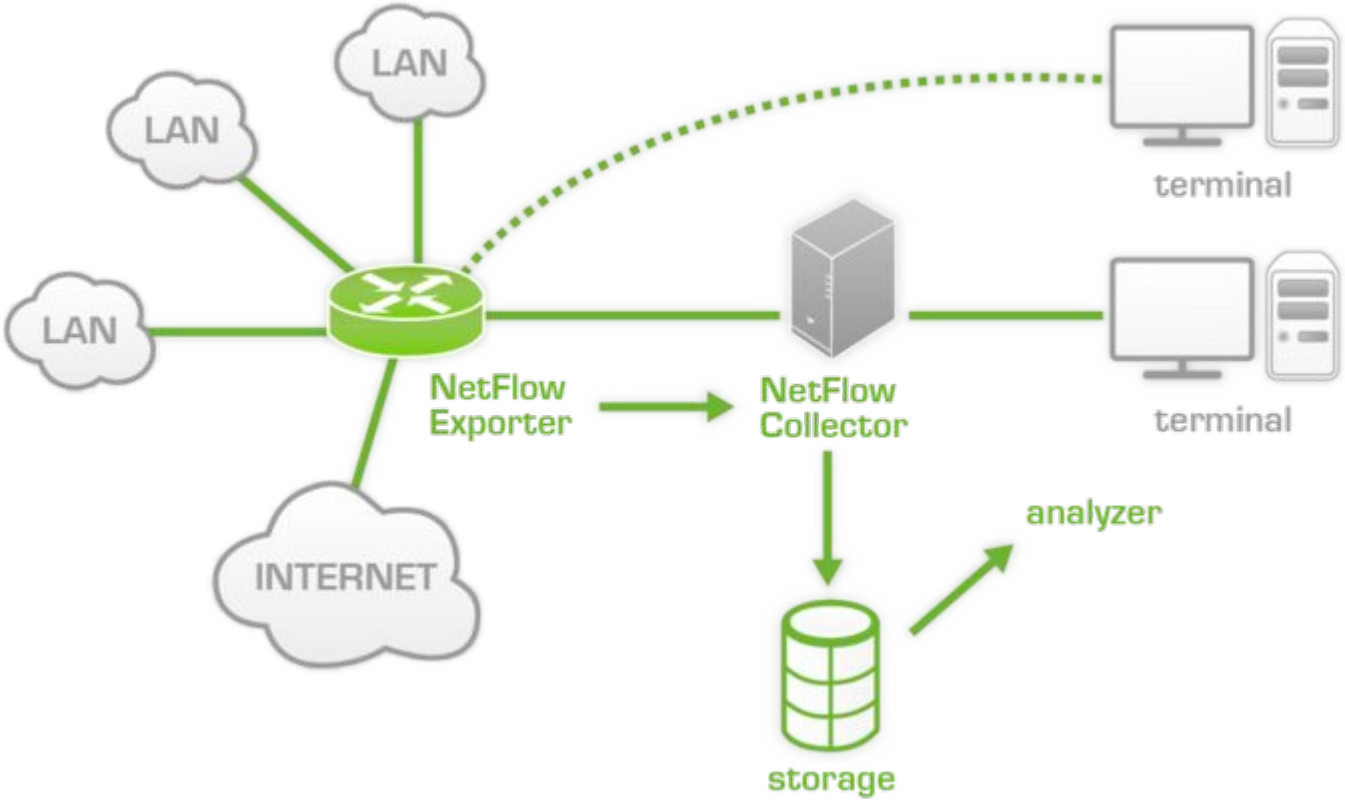
Máquinas virtuales e Imágenes: links

Comunidad zabbix en Portugués y Español: link

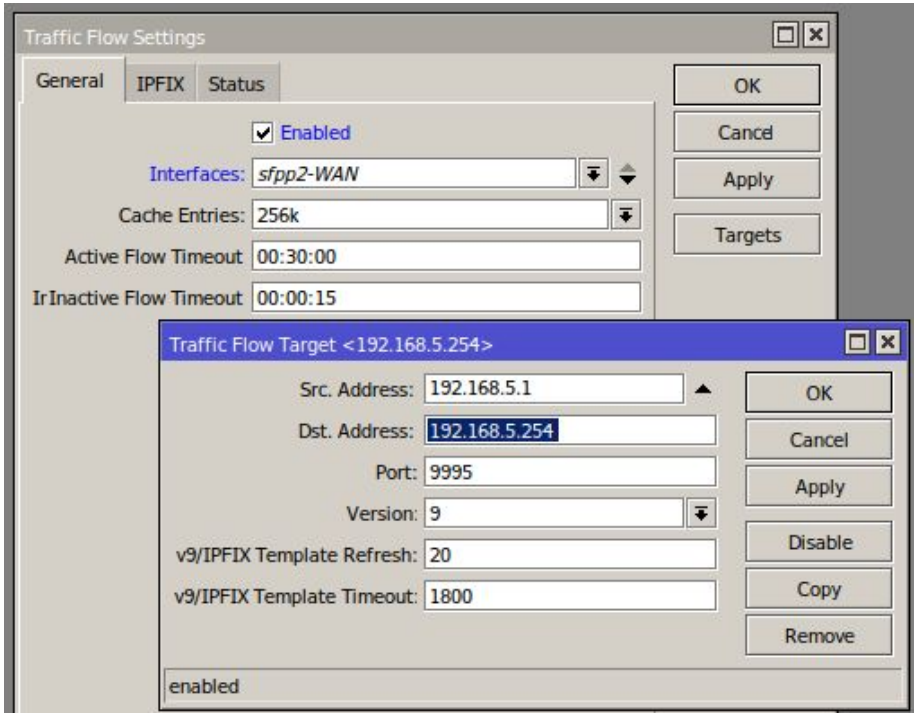
Configurar zabbix con telegram: link

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 dias, link

nProbe + ntopng: version 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

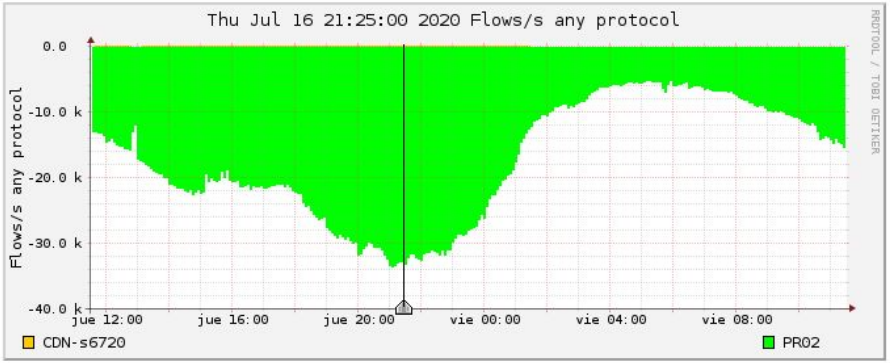
sfcapd: colector de sFlow

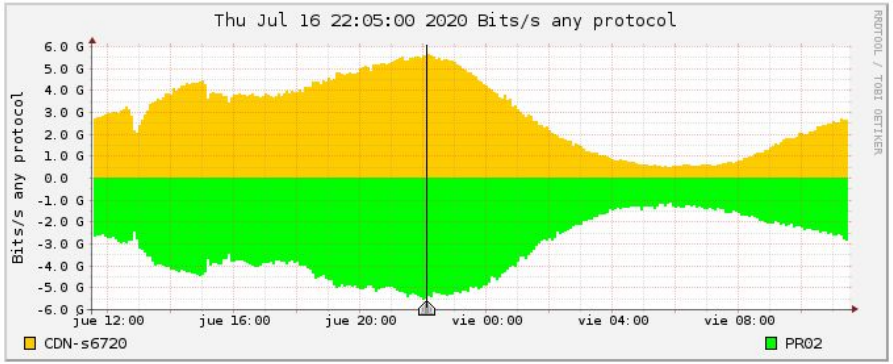
nfsen: analizador instalación

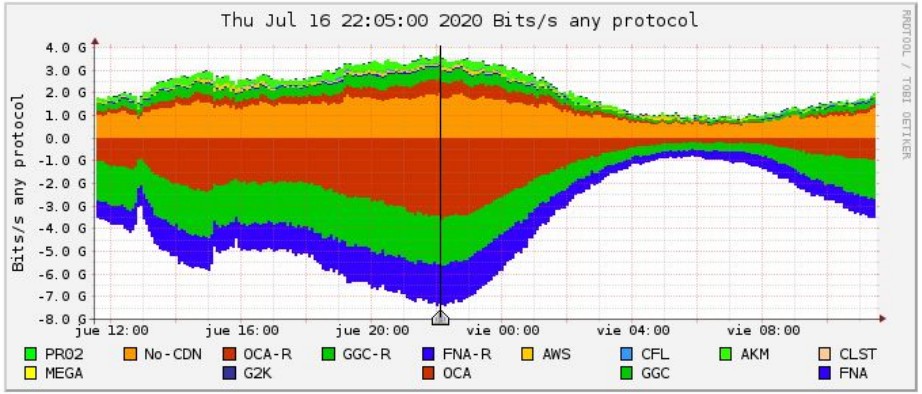
Nota: apache + php + nfdump + nfsen

Nota2: nfsen-ng -> link

nfdump + nfsen







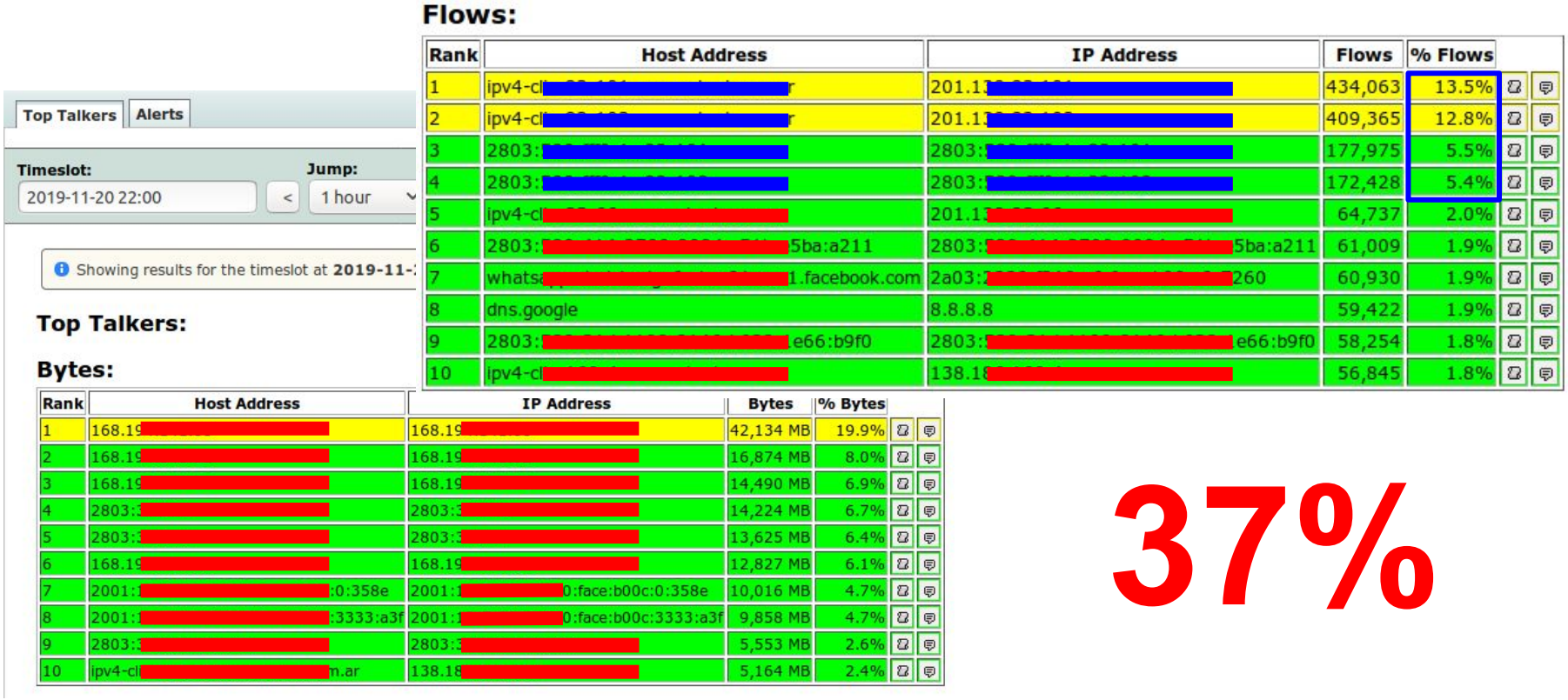
Statistics timeslot Jul 16 2020 - 22:05

Channel:	Flows:	Packets:	Traffic:				
	all:	all:	all:	tcp:	udp:	icmp:	other:
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
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
CLST	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
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
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
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
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
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
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
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
PR02	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
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
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
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
	all:	all:	all:	tcp:	udp:	icmp:	other:
TOTAL	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



37%

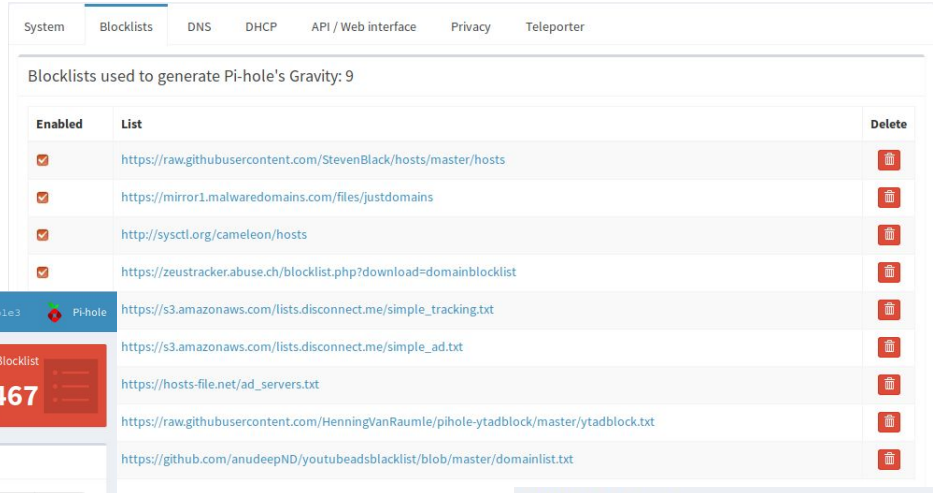
DNS (Software)

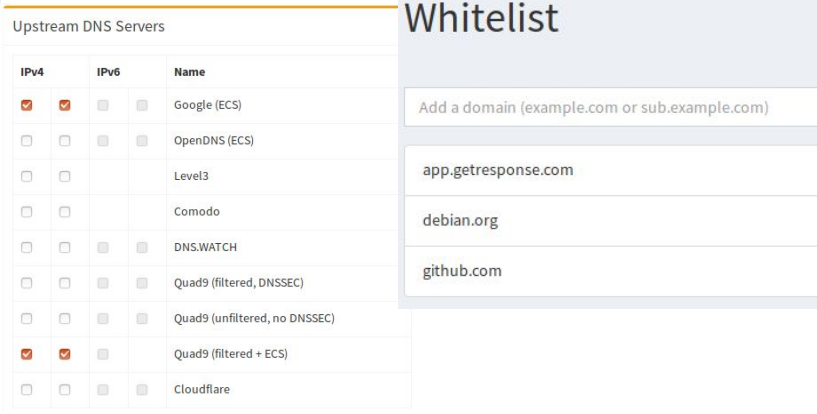
1) BIND : Autoritativo, Recursivo, DNSSEC, IPv4/v6, Response Rate Limit, large
2) UNBOUND : “Autoritativo...”, Recursivo, Cache, DNSSEC, DNS-over-TLS, DNSSEC, IPv4/v6
3) DNSMASQ : “Autoritativo...”, Cache, DNSSEC, IPv4/v6, small/local
4) POWERDNS : Autoritativo o Recursivo, IPv4/v6, statistics, high-end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

https://en.wikipedia.org/wiki/Comparison_of_DNS_server_software

Cache y filtrado

Pi-hole: dns black hole, DNSMASQ

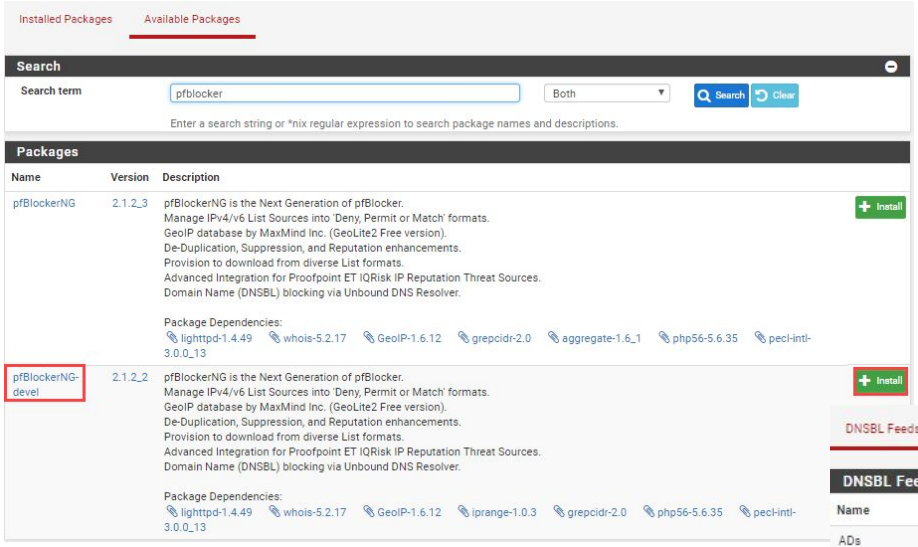


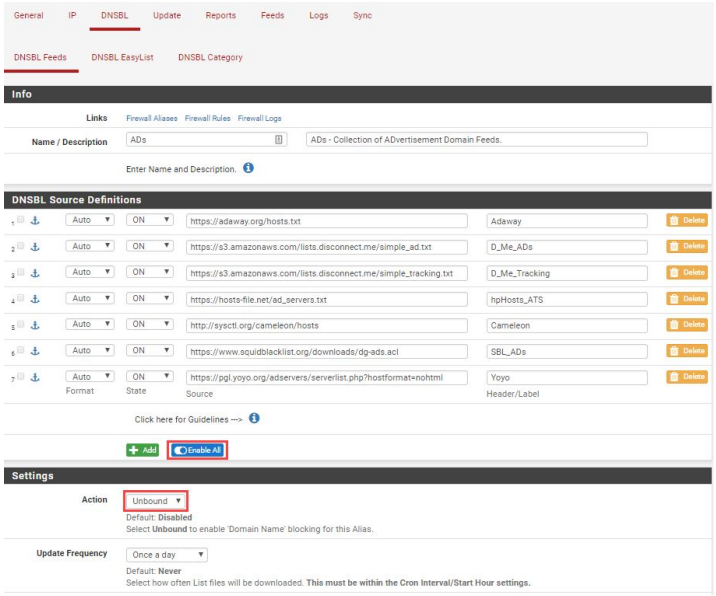


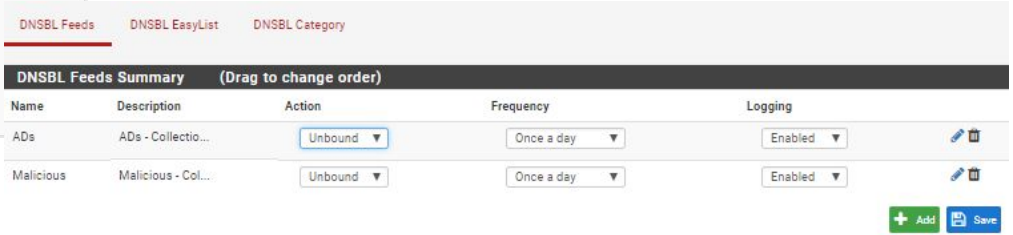
https://pi-hole.net/

Cache y filtrado

pfBlockerNG: addon para pfSense, via UNBOUND

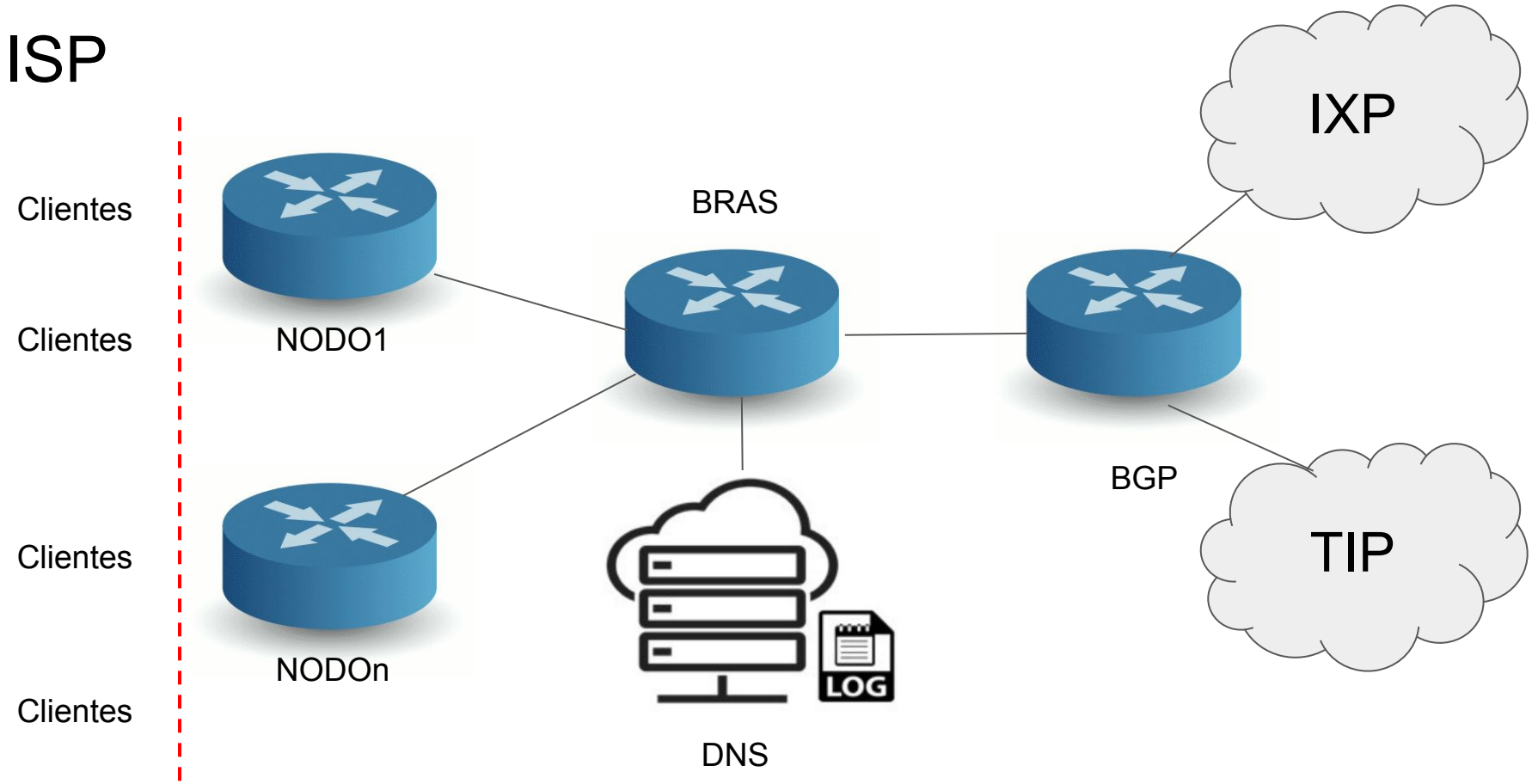






https://www.linuxincluded.com/block-ads-malvertising-on-pfsense-using-pfblockerng-dnsbl/

ISP


Clientes
Clientes
Clientes
Clientes
NODO1
NODOn
BRAS
DNS
LOG
BGP
IXP
TIP

Objetivo principal

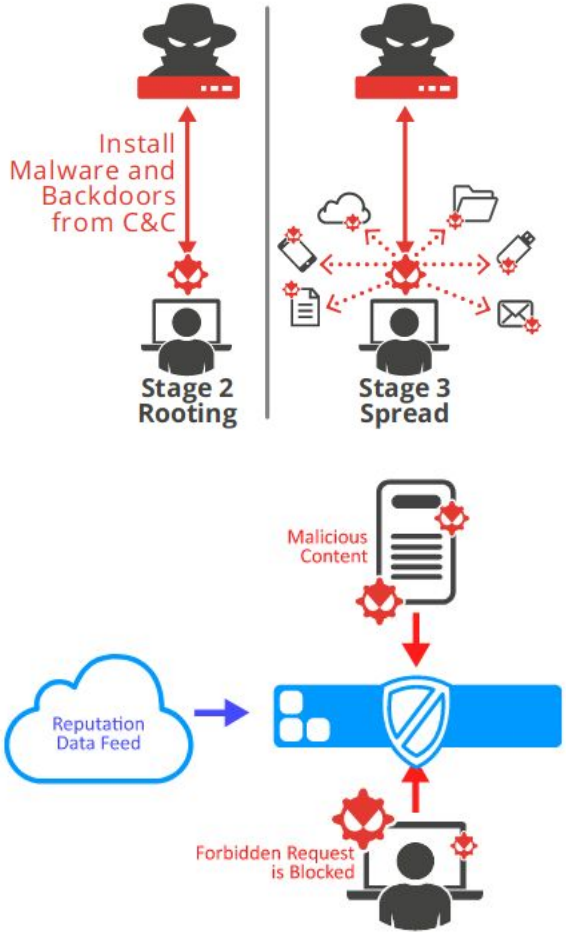
En el entorno actual, la evolución de los dispositivos móviles e IoT, Smart se está convirtiendo en la norma.

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

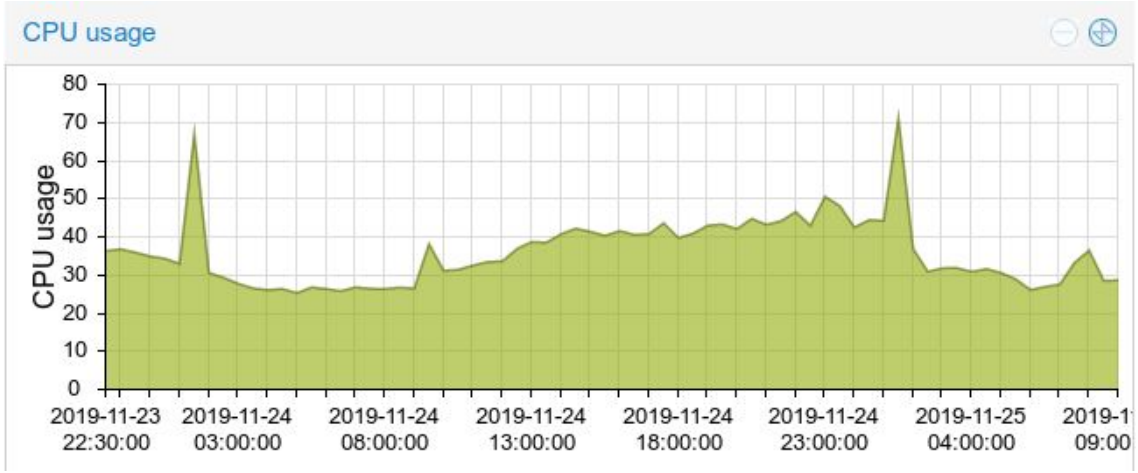
Bloquear publicidad? (opcional?)

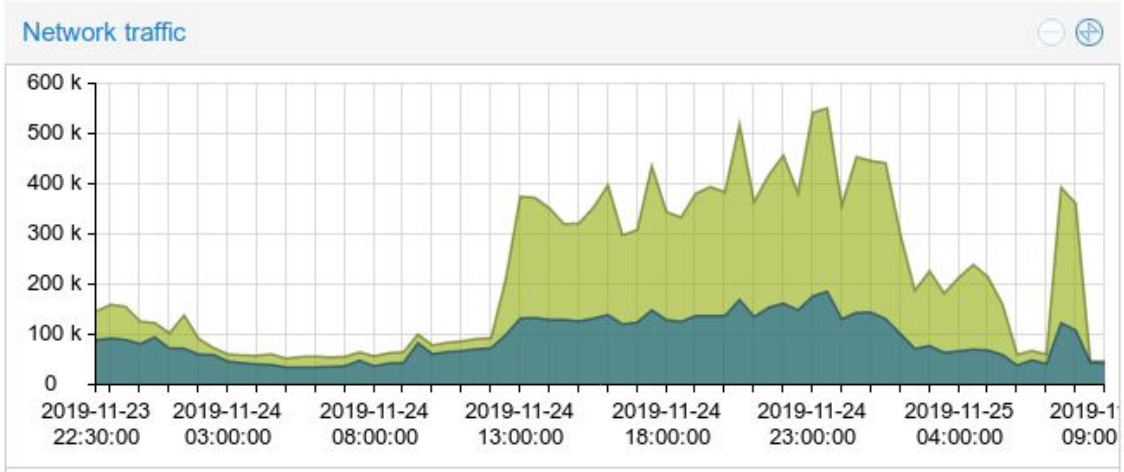


Recursos DNS

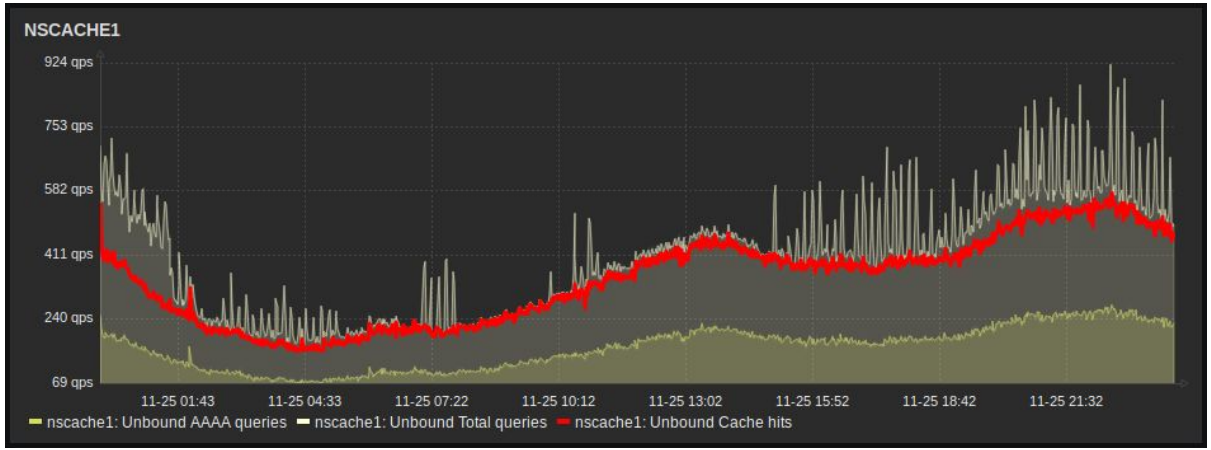
Status	running
HA State	none
Node	pve01
CPU usage	36.06% of 4 CPU(s)
Memory usage	79.73% (3.19 GiB of 4.00 GiB)
Bootdisk size	10.00 GiB

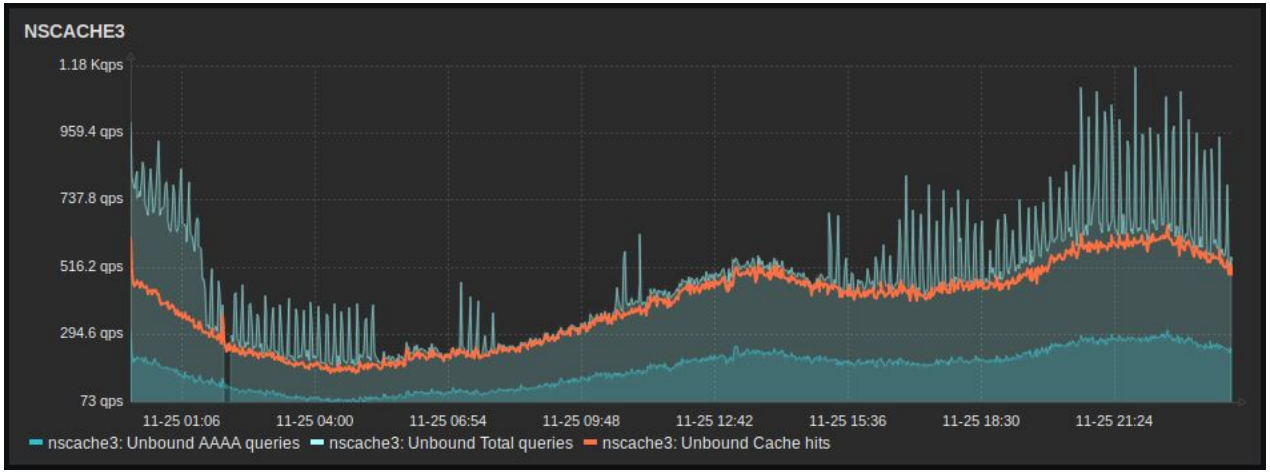
2 x VM:	pfSense
CPU	4 cores
RAM	4 GB
HD	10 GB





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
Research SRL - www.researchsrl.com.ar
IXFO - Internet x fibra óptica - www.ixfo.com.ar