

Seguridad perimetral con OPNSense

Ramón Onrubia Pérez
Catedrático de Informática y Comunicaciones
Coordinador CETI CIPFP Mislata
r.onrubiaperez@edu.gva.es

¿Quiénes somos?

- **CIPFP Mislata:** Centro Integrado Público de FP en Mislata
- Impartimos el **curso de especialización** (“máster”) **en ciberseguridad IT** para FP desde 2020
- Premio **Trofeo Red Seguridad** al centro SegurTIC en el año 2021
- **Centro Nacional de Excelencia en Ciberseguridad** por el Ministerio de Educación y Formación Profesional
- Academia **Cisco** y **Fortinet**
- **Ramón Onrubia Pérez:**
 - ✓ Ingeniero Superior de Telecomunicación por la UPV y miembro de la junta del COITCV
 - ✓ Catedrático de secundaria en Informática y Comunicaciones
 - ✓ Coordinador y profesor de Hacking Ético del máster de ciberseguridad en el CIPFP Mislata
 - ✓ En el ámbito de la ciberseguridad y el networking desde hace más de 26 años
 - ✓ Desde 2006 Instructor Cisco y formador de instructores con más de 20 certificaciones (CCIE SCOR y ENCOR, CCNP, CCNP Wireless, CCDP, CCNA, Devnet, etc.)
 - ✓ Premio Cisco Instructor Above and Beyond a nivel europeo
 - ✓ <https://www.linkedin.com/in/ramón-onrubia-pérez-675ba51/>

OPNsense, es un cortafuegos libre basado en **FreeBSD** con características bastante potentes, comparable a muchos cortafuegos del mercado. Algunas de sus características según la página oficial son:

- Stateful inspection firewall
- Intrusion Detection and Prevention
- Virtual Private Network
- Traffic Shaper
- Two-factor Authentication
- Captive portal
- Forward Caching Proxy (transparent) with Blacklist support
- High Availability & Hardware Failover
- Build-in reporting and monitoring tools including RRD Graphs
- Netflow Exporter
- DNS Server & DNS Forwarder & Dynamic DNS
- DHCP Server and Relay
- Encrypted configuration backup to Google Drive
- And more...

¿Qué necesitamos?

- Anfitrión con al menos 8 GB RAM recomendadas
- Software de virtualización: VirtualBox, VMWare, KVM...
- ISO de OPNSense:
 - <https://opnsense.org/download/>
 - Arquitectura amd64, imagen DVD
- Documentación muy amplia: <https://docs.opnsense.org/>

Consola y GUI

```
OPNsense CyberOps RECE [Corriendo] - Oracle VM VirtualBox
Forums:  https://forum.opnsense.org/
Code:    https://github.com/opnsense
Reddit:  https://reddit.com/r/opnsense

*** firewall-cyberops.lan: OPNsense 25.1.7_4 (amd64) ***

LAN (em1)    -> v4: 192.168.56.100/24
WAN (em0)    -> v4/DHCP4: 10.0.2.15/24

HTTPS: sha256 6E 9F 2A F4 92 61 FB 7F 65 A5 47 50 C7 8C 53 E2
          FC 68 8F 9C 53 5B 8B 26 83 E6 BE 86 B9 AE 8F BB
SSH:  SHA256 ywqlw63RtsmfPWXY5LLcnIo0Z5iInmt11SkUYFSU54 (ECDSA)
SSH:  SHA256 D/9TTqP80igCRhBCd07i8w1PUsxk6Yi/2HD+WBUXU1k (ED25519)
SSH:  SHA256 iE+Xg7yduiqnW5LP7aqawLHTa01ecyUsxyv+ppUQ+/E (RSA)

0) Logout
1) Assign interfaces
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system
6) Reboot system
7) Ping host
8) Shell
9) pfTop
10) Firewall log
11) Reload all services
12) Update from console
13) Restore a backup

Enter an option: 
```



Nombre de usuario:

Contraseña:

Iniciar sesión

OPNsense (c) 2014-2025 Deciso B.V.



root@firewall-cyberops.lan



- Lobby
- Panel de control
- Licencia
- Contraseña
- Cerrar Sesión
- Informes
- Sistema
- Interfaces
- Cortafuegos
- VPN
- Servicios
- Encendido
- Ayuda

Lobby: Panel de control

System Information

Nombre
firewall-cyberops.lan

Versiónes
OPNsense 25.1.7_4-amd64
FreeBSD 14.2-RELEASE-p3
OpenSSL 3.0.16

Actualizaciones
[Clic para comprobar actualizaciones.](#)

Tiempo de Actividad
06:27:38

Promedio de carga
1.04, 0.89, 0.83

Fecha/Hora Actual
Sun Jun 1 18:13:41 CEST 2025

Last configuration change
Sat May 31 19:20:08 CEST 2025

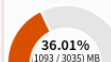
CPU

Intel(R) Core(TM) i7-7500U CPU @
2.70GHz (2 cores, 2 threads)

Total

53

Memoria



Disco



Puertas de enlace

- WAN_DHCP6 (activo)
undefined
- WAN_DHCP (activo)
10.0.2.2

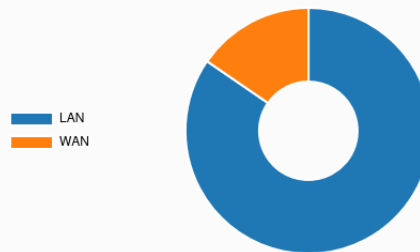
Announcements

Re: OPNsense 25.1.7 released
Fri, 23 May 2025 10:50:08 GMT
A hotfix release was issued as
25.1.7_4:

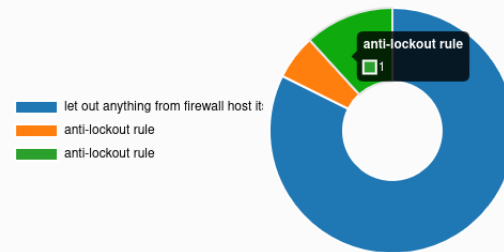
o dnsmasq: fix physical interface
in dhcp-boot
o ipsec: fix ipsec column identifier

**OPNsense 25.4.1 business
edition released**
Thu, 22 May 2025 11:47:17 GMT
This business release is based on

Estadísticas de Interfaz



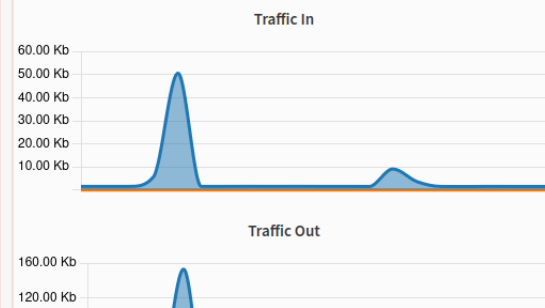
Cortafuegos



Servicios

- | | | | |
|-----------------------------|--|--|--|
| C-ICAP server | | | |
| ClamAV Daemon | | | |
| System Configuration Daemon | | | |
| Cron | | | |
| DHCPv4 Server | | | |
| freshclam daemon | | | |
| FTP Proxy Server | | | |
| Uppox and GnuPG | | | |

Gráfico del tráfico





- Lobby
- Informes
- Sistema
 - Acceso
 - Configuración
 - Firmware
 - Estado
 - Ajustes
 - Registro de cambios
 - Actualizaciones
 - Complementos
 - Paquetes
 - Reportero
 - Archivo de registro
 - Puertas de enlace
 - Alta disponibilidad
 - Rutas

Sistema: Firmware

Estado Ajustes Registro de cambios Actualizaciones Complementos Paquetes

modo avanzado

Mirror (default)

Escribir Community

Suscripción Business

Usage Community

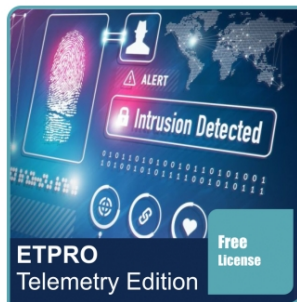
Development

Guardar Cancelar

Software & Licenses

OPNsense® Business Edition, ET PRO Ruleset, Sensei

Default sorting Showing all 7 results



ETPRO Telemetry edition

€0,00

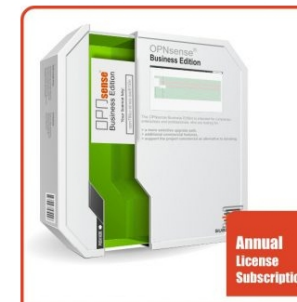
Select options



OPNsense Business Edition (3Yr)

SALE!

€447,00 €399,00



OPNsense® Business Edition 1yr subscription

€149,00 / year

Sign up now

 **OPNsense®** < Securing networks made easy

Lobby

Informes

Sistema

- Acceso
- Configuración
- Firmware
 - Estado
 - Ajustes
 - Registro de cambios
 - Actualizaciones
 - Complementos
 - Paquetes
- Reportero
 - Archivo de registro
- Puertas de enlace
- Alta disponibilidad
- Rutas

Sistema: Firmware

EstadoAjustesRegistro de cambiosActualizacionesComplementosPaquetes

Escribir	opnsense
Versión	25.1.7_4
Architecture	amd64
Commit	86e8d5f88
Mirror	https://pkg.opnsense.org/FreeBSD:14:amd64/25.1
Repositories	OPNsense (Priority: 11)
Updated on	Sat May 31 19:20:08 CEST 2025
Checked on	Sun Jun 1 18:16:28 CEST 2025

Comprobar actualizaciones

Run an audit

Plugins

La funcionalidad de OPNSense puede ser ampliada con plugins gratuitos y comerciales como:

- ClamAV: antivirus libre basado en firmas
- I-CAP: protocolo para análisis de contenido web
- Rspamd: filtro anti-spam para correo-e
- OpenDNS (Cisco Umbrella): seguridad en la capa dns
- ZeroTier: SDN
- Tinc: VPN multipunto
- ZenArmor (Sensei): características avanzadas de NGFW bajo suscripción
- ...

 **OPNsense**®
Securing networks made easy

root@

Lobby

Informes

Sistema

Acceso

Configuración

Firmware

Estado

Ajustes

Registro de cambios

Actualizaciones

Complementos

Paquetes

Reportero

Archivo de registro

Puertas de enlace

Alta disponibilidad

Rutas

Ajustes

Snapshots

Confianza

Asistente

Archivos de Registro

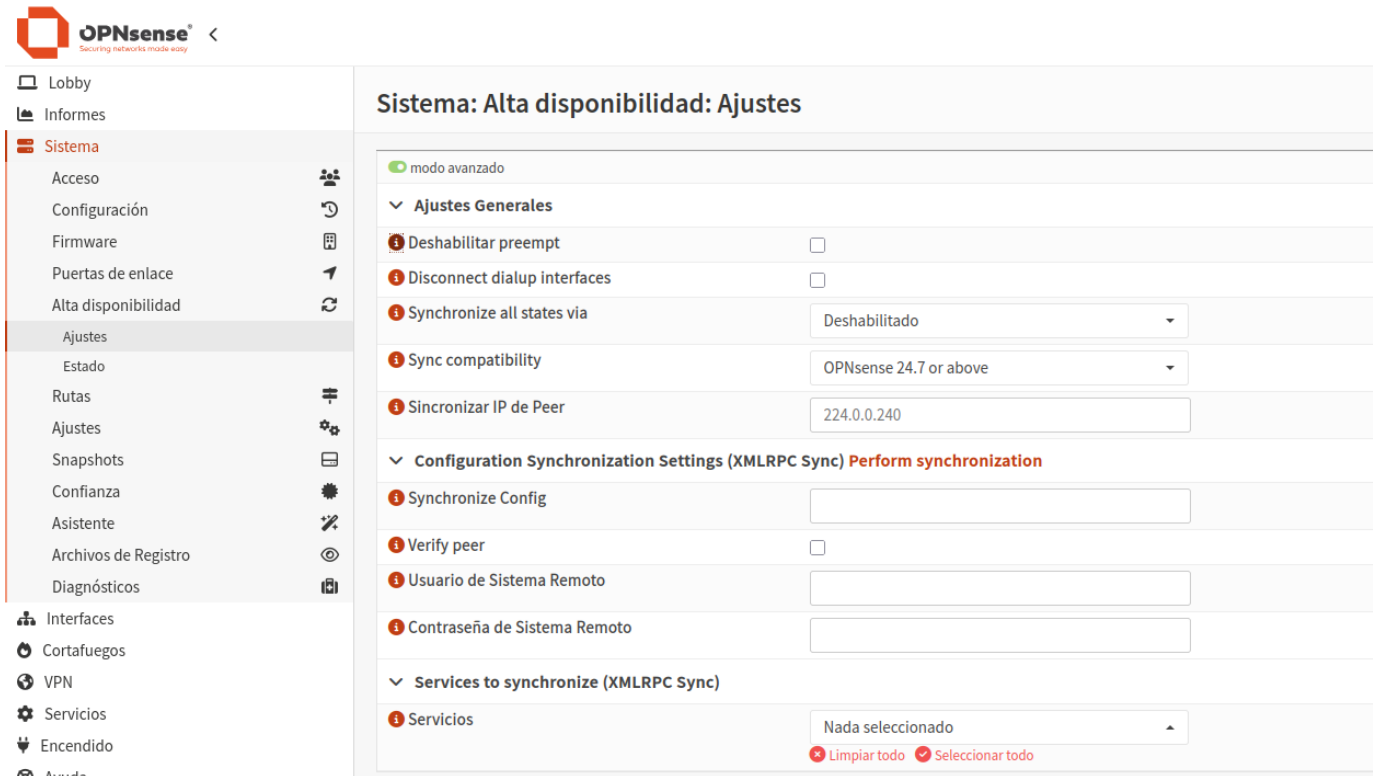
Diagnósticos

Sistema: Firmware

EstadoAjustesRegistro de cambiosActualizacionesComplementosPaquetes

Nombre	Versión	Tamaño	Nivel	Repository	Comentar
os-c-icap (instalado)	1.8	50.1KiB	3	OPNsense	c-icap connects the web proxy with a virus scanner
os-clamav (instalado)	1.8_3	47.7KiB	3	OPNsense	Antivirus engine for detecting malicious threats
os-ftp-proxy (instalado)	1.0_4	41.5KiB	3	OPNsense	Control ftp-proxy processes
os-squid (instalado)	1.2_1	294KiB	2	OPNsense	Squid is a caching proxy for the web
os-acme-client	4.9	789KiB	3	OPNsense	ACME Client
os-apcupsd	1.2_3	61.7KiB	3	OPNsense	APCUPSD - APC UPS daemon
os-beats	1.0	31.6KiB	3	OPNsense	Send logs, network, metrics and heartbeat to Elasticsearch
os-bind	1.33_1	155KiB	3	OPNsense	BIND domain name service
os-cache	1.0_1	563B	3	OPNsense	Webserver cache
os-caddy	2.0.0	236KiB	3	OPNsense	Modern Reverse Proxy with Automatic HTTPS, Dynamic DN
os-chrony	1.5_2	20.5KiB	3	OPNsense	Chrony time synchronisation
os-collectd	1.4_1	36.5KiB	3	OPNsense	Collect system and application performance metrics periodic
os-cpu-microcode-amd	1.1	504B	2	OPNsense	AMD CPU microcode updates
os-cpu-microcode-intel	1.1	508B	2	OPNsense	Intel CPU microcode updates

OPNsense utiliza el Protocolo de Redundancia de Direcciones Comunes (CARP) para la conmutación por error de hardware. Se pueden configurar dos o más firewalls como un grupo de conmutación por error. Si una interfaz del firewall principal falla o este se desconecta por completo, el firewall secundario se activa.



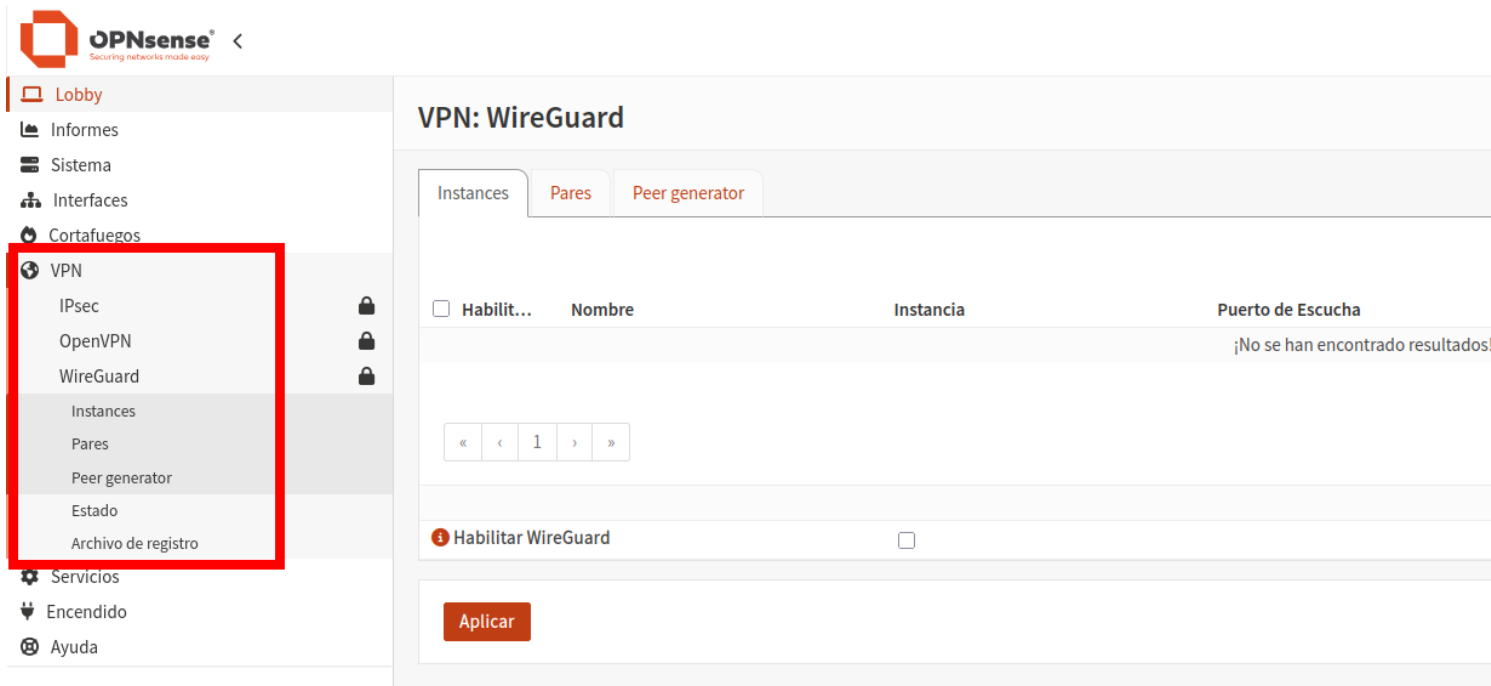
The screenshot displays the OPNsense web interface. On the left is a sidebar menu with the following items: Lobby, Informes, Sistema (highlighted), Acceso, Configuración, Firmware, Puertas de enlace, Alta disponibilidad, Ajustes (highlighted), Estado, Rutas, Ajustes, Snapshots, Confianza, Asistente, Archivos de Registro, Diagnósticos, Interfaces, Cortafuegos, VPN, Servicios, Encendido, and Avanza. The main content area is titled 'Sistema: Alta disponibilidad: Ajustes'. It features a 'modo avanzado' toggle and a 'Ajustes Generales' section with the following settings: 'Deshabilitar preempt' (checkbox), 'Disconnect dialup interfaces' (checkbox), 'Synchronize all states via' (dropdown set to 'Deshabilitado'), 'Sync compatibility' (dropdown set to 'OPNsense 24.7 or above'), and 'Sincronizar IP de Peer' (text input '224.0.0.240'). Below this is the 'Configuration Synchronization Settings (XMLRPC Sync)' section with a 'Perform synchronization' button and settings for 'Synchronize Config' (text input), 'Verify peer' (checkbox), 'Usuario de Sistema Remoto' (text input), and 'Contraseña de Sistema Remoto' (text input). The final section is 'Services to synchronize (XMLRPC Sync)' with a 'Servicios' dropdown set to 'Nada seleccionado' and buttons for 'Limpiar todo' and 'Seleccionar todo'.

OPNsense tiene un sistema de creación de reglas muy intuitivo que se aplican a la interfaz seleccionada o también pueden ser flotantes. Es muy fácil habilitar o deshabilitar reglas, crear alias de hosts, puertos o protocolos e incluso definir policy routing (puertas de enlace diferentes según ip de origen, protocolo, puerto, etc)

Cortafuegos: Reglas: LAN
Seleccionar categoría

☐		Protocolo	Origen	Puerto	Destino	Puerto	Puerta de Enlace	Programar	Descripción ?
<i>Reglas generadas automáticamente</i>									
☐	x → ⚡ i	IPv4 TCP	LAN red	*	193.110.128.199/24	80 (HTTP)	*	*	
☐	▶ → ⚡ i	IPv4 *	LAN red	*	*	*	*	*	Default allow LAN to any rule
☐	▶ → ⚡ i	IPv6 *	LAN red	*	*	*	*	*	Default allow LAN IPv6 to any rule
☐	▶ → ⚡ i	IPv4 TCP	LAN red	*	127.0.0.1	3128	*	*	redirigir tráfico a proxy
☐	▶ → ⚡ i	IPv4 TCP	LAN red	*	127.0.0.1	3129	*	*	redirigir tráfico a proxy
▶	permitir	✗ bloquear	✗ rechazar	i registro	→ entrada	⚡			
▶	permitir (deshabilitado)	✗ bloquear (deshabilitado)	✗ rechazado (deshabilitado)	i registro (deshabilitado)	← salida	⚡			
📅 Programación Activa/Inactiva (clic para ver/editar)									
🏷 Alias (clic para ver/editar)									
Las reglas LAN se evalúan de forma predeterminada sobre la base de la primera coincidencia (es decir, se ejecutará la acción de la primera regla para que coincida con un paquete). Esto significa que si usas reglas d atención al orden de las reglas. Todo lo que no se pasa explícitamente se bloquea de forma predeterminada.									

OPNsense tiene soporte para varias de tecnologías de VPN como **IPSec**, **OpenVPN**, **Wireguard**, **Tinc**, **ZeroTier...**



OPNsense Securing networks made easy

Lobby

- Informes
- Sistema
- Interfaces
- Cortafuegos
- VPN**
 - IPsec
 - OpenVPN
 - WireGuard
 - Instances
 - Pares
 - Peer generator
 - Estado
 - Archivo de registro
- Servicios
- Encendido
- Ayuda

VPN: WireGuard

Instances Pares Peer generator

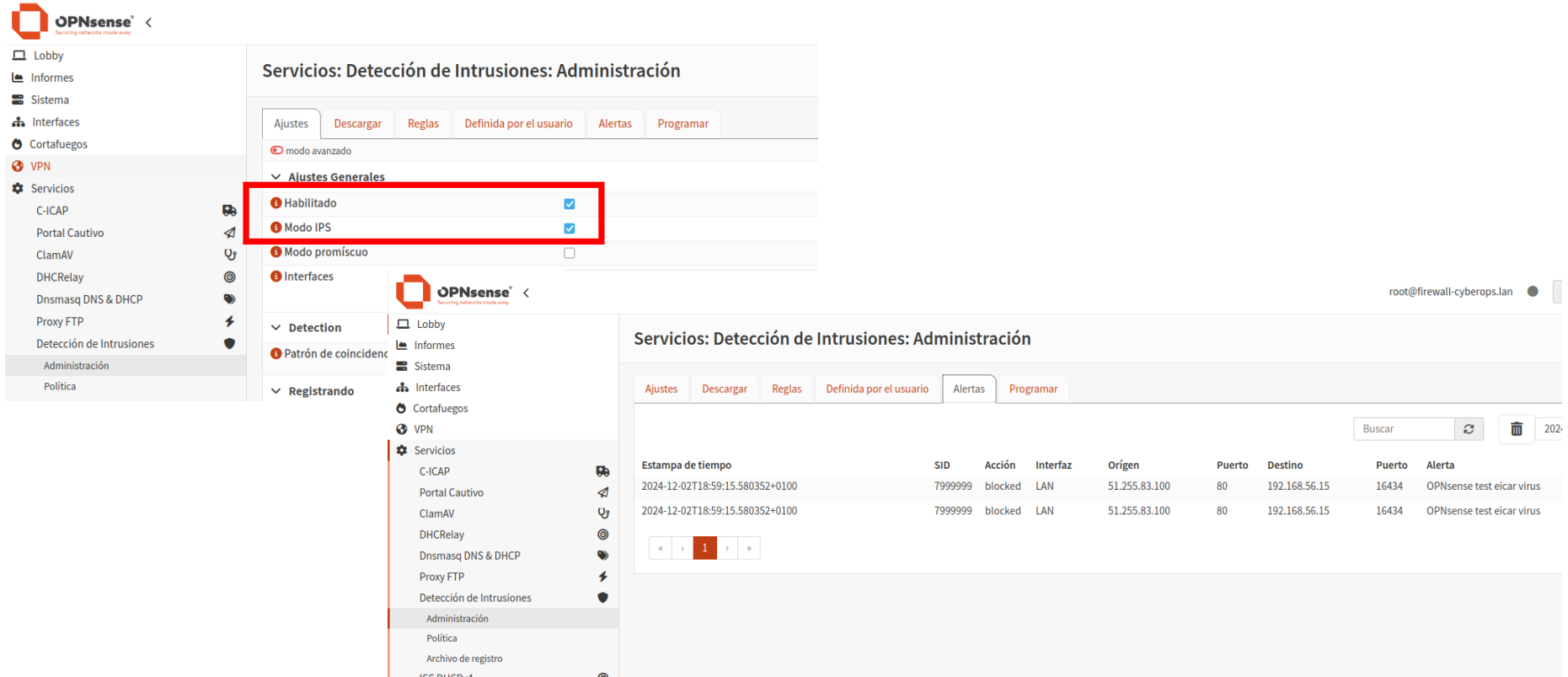
☐ Habilit...	Nombre	Instancia	Puerto de Escucha
¡No se han encontrado resultados!			

« < 1 > »

Habilitar WireGuard ☐

Aplicar

OPNsense a través de Suricata puede funcionar tanto como NIDS y NIPS (debe habilitarse)



The image shows two screenshots of the OPNsense web interface. The left screenshot displays the 'Servicios: Detección de Intrusiones: Administración' page with the 'Alustes Generales' section highlighted by a red box. The right screenshot shows the 'Alertas' tab with a table of detection events.

Servicios: Detección de Intrusiones: Administración

Alustes Descargar Reglas Definida por el usuario Alertas Programar

modo avanzado

Alustes Generales

- Habilitado ☒
- Modo IPS ☒
- Modo promiscuo ☐

Detection

Patrón de coincidenc

Registrando

Servicios: Detección de Intrusiones: Administración

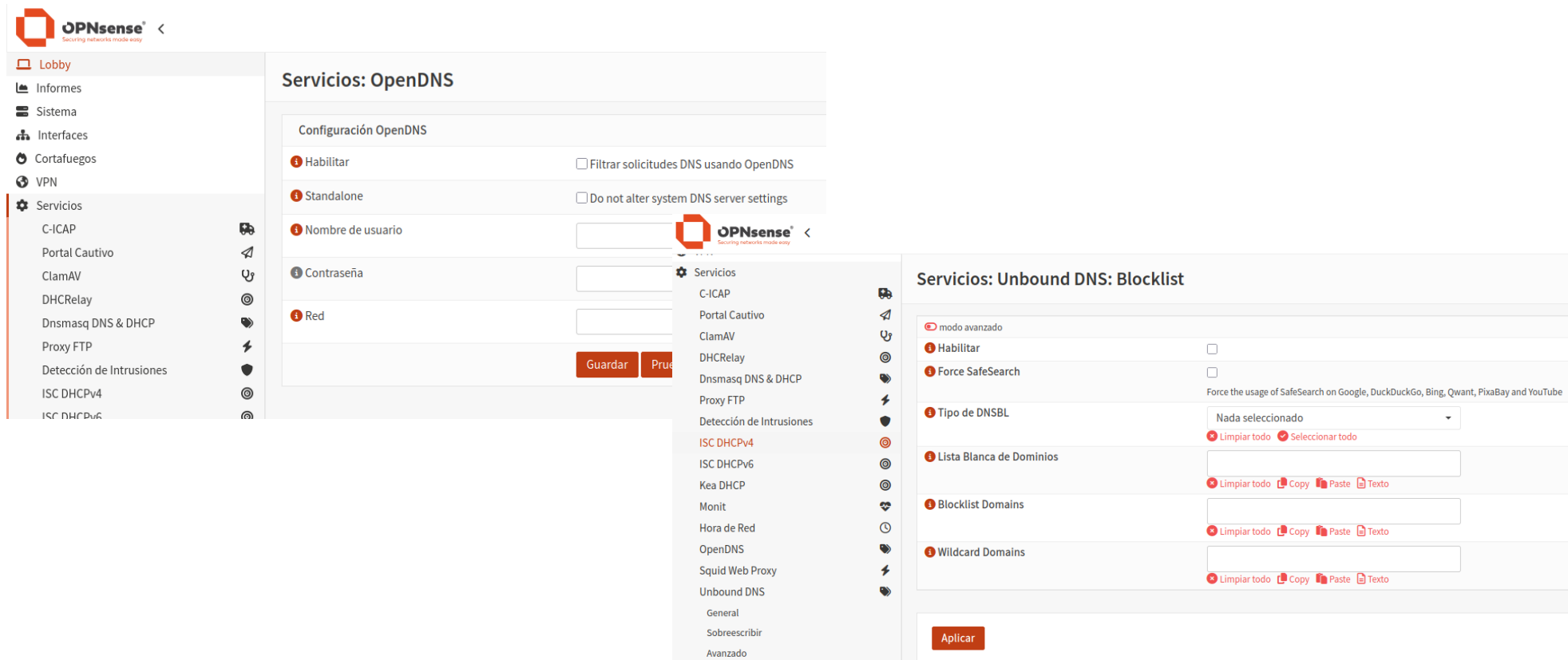
Alustes Descargar Reglas Definida por el usuario Alertas Programar

Buscar [icon] [icon] 202

Estampa de tiempo	SID	Acción	Interfaz	Origen	Puerto	Destino	Puerto	Alerta
2024-12-02T18:59:15.580352+0100	7999999	blocked	LAN	51.255.83.100	80	192.168.56.15	16434	OPNsense test eicar virus
2024-12-02T18:59:15.580352+0100	7999999	blocked	LAN	51.255.83.100	80	192.168.56.15	16434	OPNsense test eicar virus

« < 1 > »

Puede utilizar los servicios de Cisco Umbrella (OpenDNS) o su propio servicio con listas negras públicas (Outbound DNS) y SafeSearch de Google, DuckDuckGo, Bing, Qwant, PixaBay y YouTube



The screenshot displays the OPNsense web interface, specifically the 'Servicios: OpenDNS' configuration page. The left sidebar shows the navigation menu with 'Servicios' selected. The main content area is titled 'Servicios: OpenDNS' and contains a 'Configuración OpenDNS' section. This section includes several settings: 'Habilitar' (checked), 'Filtrar solicitudes DNS usando OpenDNS' (unchecked), 'Standalone' (checked), 'Do not alter system DNS server settings' (unchecked), 'Nombre de usuario' (empty field), 'Contraseña' (empty field), and 'Red' (empty field). Below these fields are 'Guardar' and 'Probar' buttons. A second window is overlaid on the first, showing the 'Servicios: Unbound DNS: Blocklist' configuration page. This page has a 'modo avanzado' toggle and settings for 'Habilitar' (checked), 'Force SafeSearch' (checked), 'Tipo de DNSBL' (set to 'Nada seleccionado'), 'Lista Blanca de Dominios' (empty field), 'Blocklist Domains' (empty field), and 'Wildcard Domains' (empty field). Each of these fields has a 'Limpiar todo' button and a 'Seleccionar todo' button. At the bottom of this window is an 'Aplicar' button.

OPNsense puede interceptar las conexiones HTTPS de los clientes para analizar el tráfico y detectar amenazas. Se puede combinar con los servicios **ICAP** (Protocolo de Adaptación de Contenido de Internet) y **ClamAV**



Informes

Sistema

Interfaces

Cortafuegos

VPN

Servicios

C-ICAP

Portal Cautivo

ClamAV

DHCRely

Dnsmasq DNS & DHCP

Proxy FTP

Detección de Intrusiones

ISC DHCPv4

ISC DHCPv6

Kea DHCP

Monit

Hora de Red

OpenDNS

Squid Web Proxy

Servicios: Squid Web Proxy: Administración

Ajustes Generales Proxy

Redirigir Proxy

Proxy Auto-Config

Listas de Control de Acceso Remotas

Apoyo

modo avanzado

Interfaces Proxy

LAN

Limpiar todo Seleccionar todo

Puerto Proxy

3128

Habilitar proxy transparente HTTP



Habilitar Inspección SSL



Registrar sólo información SNI



Puerto de Proxy SSL

3129

CA a usar

CIPFP Mislata https interception AC

SSL sitios de no colisión

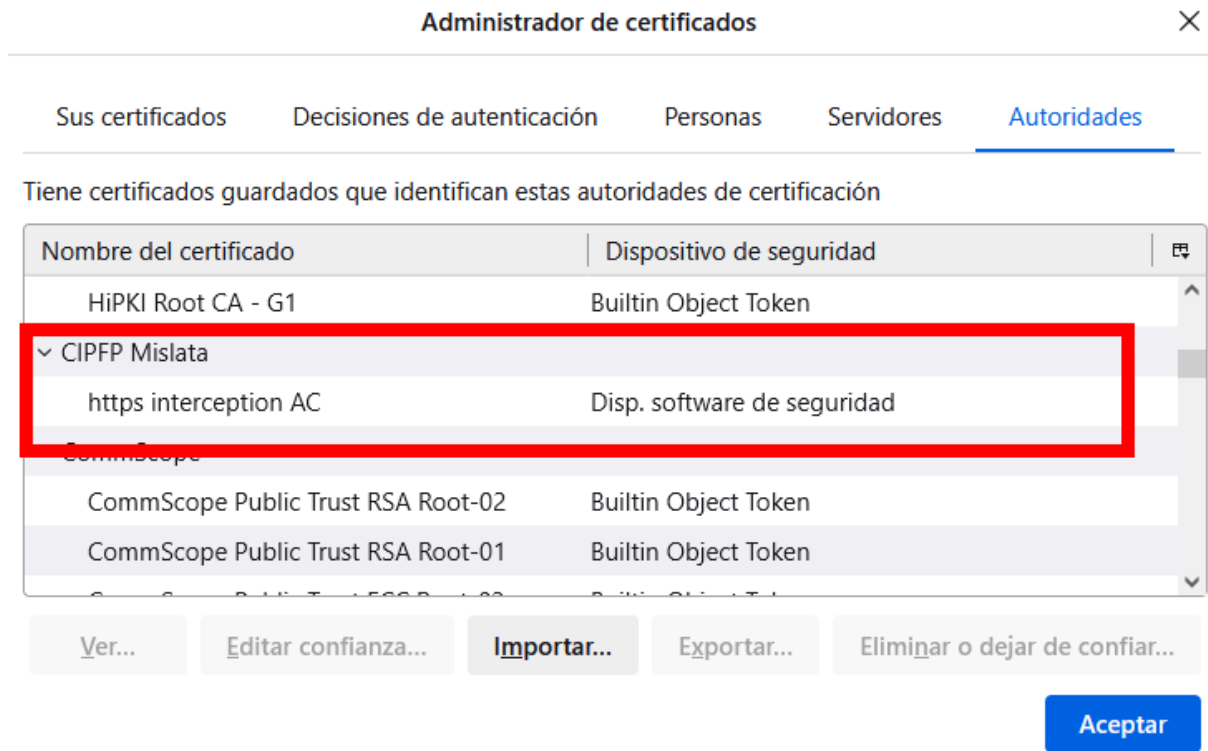
.bbva.es .caixabank.es

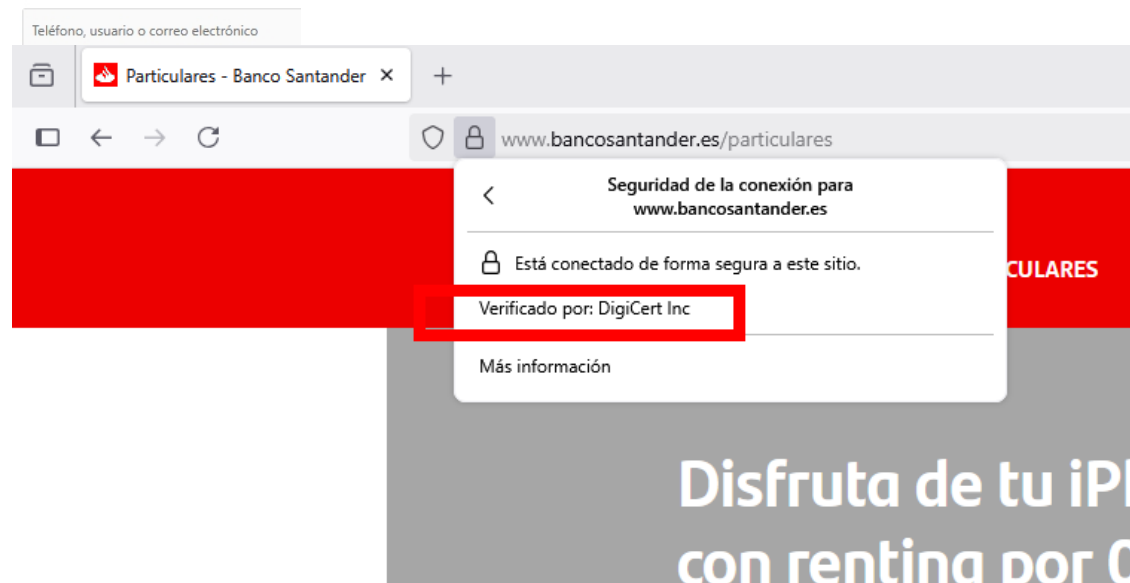
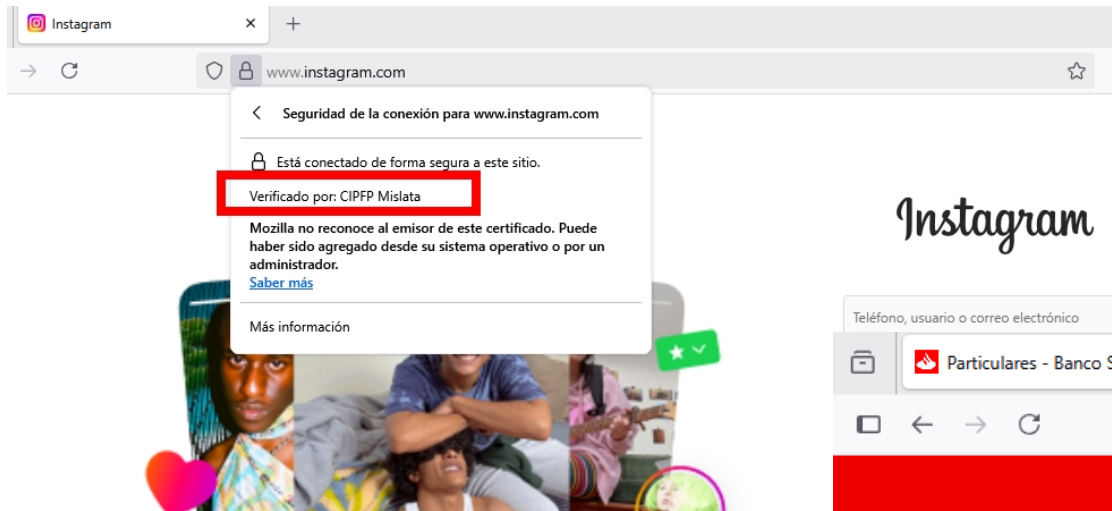
.bancosantander.es

Limpiar todo Copy Paste Texto

Aplicar

Es necesario importar el certificado de la CA generado por OPNSense, en todos los endpoints de la organización. Puede hacerse con directivas de grupo en AD o con herramientas como Intune:







Informes

Sistema

Interfaces

Cortafuegos

VPN

Servicios

C-ICAP

Portal Cautivo

ClamAV

DHCRelay

Dnsmasq DNS & DHCP

Proxy FTP

Detección de Intrusiones

ISC DHCPv4

ISC DHCPv6

Servicios: Squid Web Proxy: Administración

Ajustes Generales Proxy

Redirigir Proxy

Proxy Auto-Config

Listas de Control de Acceso

Habilitar ICAP



Modificar URL de Solicitud

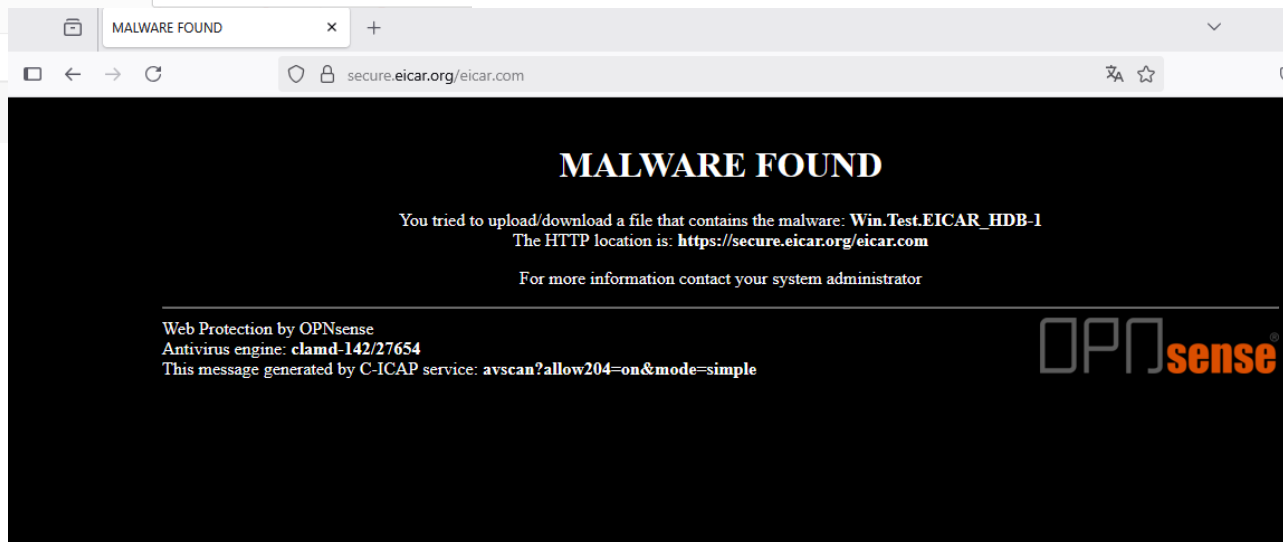
icap://[::1]:1344/avscan

Modificar URL de Respuesta

icap://[::1]:1344/avscan

Lista de Exclusión

Aplicar



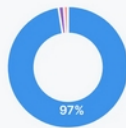
Plugin Zenarmor

- Application Control
- Cloud Application Control (Web 2.0 Controls)
- Advanced Network Analytics
- Web Filtering & Security
- Cloud Threat Intelligence
- User-based Filtering and Reporting
- Active Directory Integration
- RESTful API
- Cloud-based centralized management & Reporting
- Application / Web-category-based Traffic Shaping and Prioritization
- Policy-based filtering and QoS
- Encrypted Threats Prevention
- All-ports full TLS Inspection (for every TCP port, not just HTTPS) Coming soon

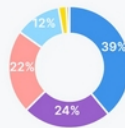
- Lobby
- Reporting
- System
- Interfaces
- Firewall
- VPN
- Services
- Zenarmor (Business)
 - Dashboard
 - Devices
 - Reports
 - Live Sessions
 - Activity Explorer
 - Policies
 - Settings
 - Notifications
- Power
- Help

Today, **zenarmor** detected **356** and blocked **347** potentially harmful activities according to your rules.

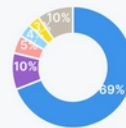
Top Threats



Top Hosts



Top Apps



Engine

Status: **Running**

Version: 1.16 - Dec 18, 2023 20:20

Application DB: 1.16.23121814 - Dec 18, 2023 20:20

Start on boot: ☒

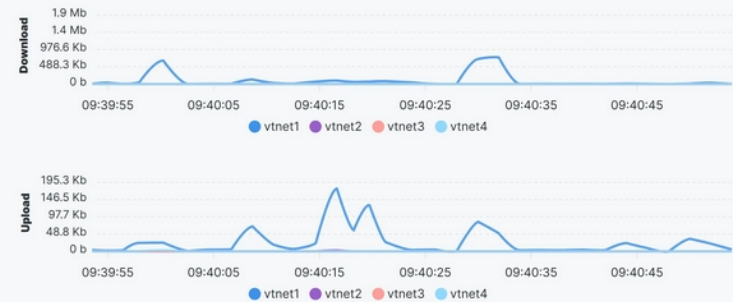
Reporting Database

Status: **Running**

Type: elasticsearch

Start on boot: ☒

Traffic Graph (Throughput)



CPU Utilization

Usage: 0%
Load: 0.7 0.73 0.54

Disk Space Utilization

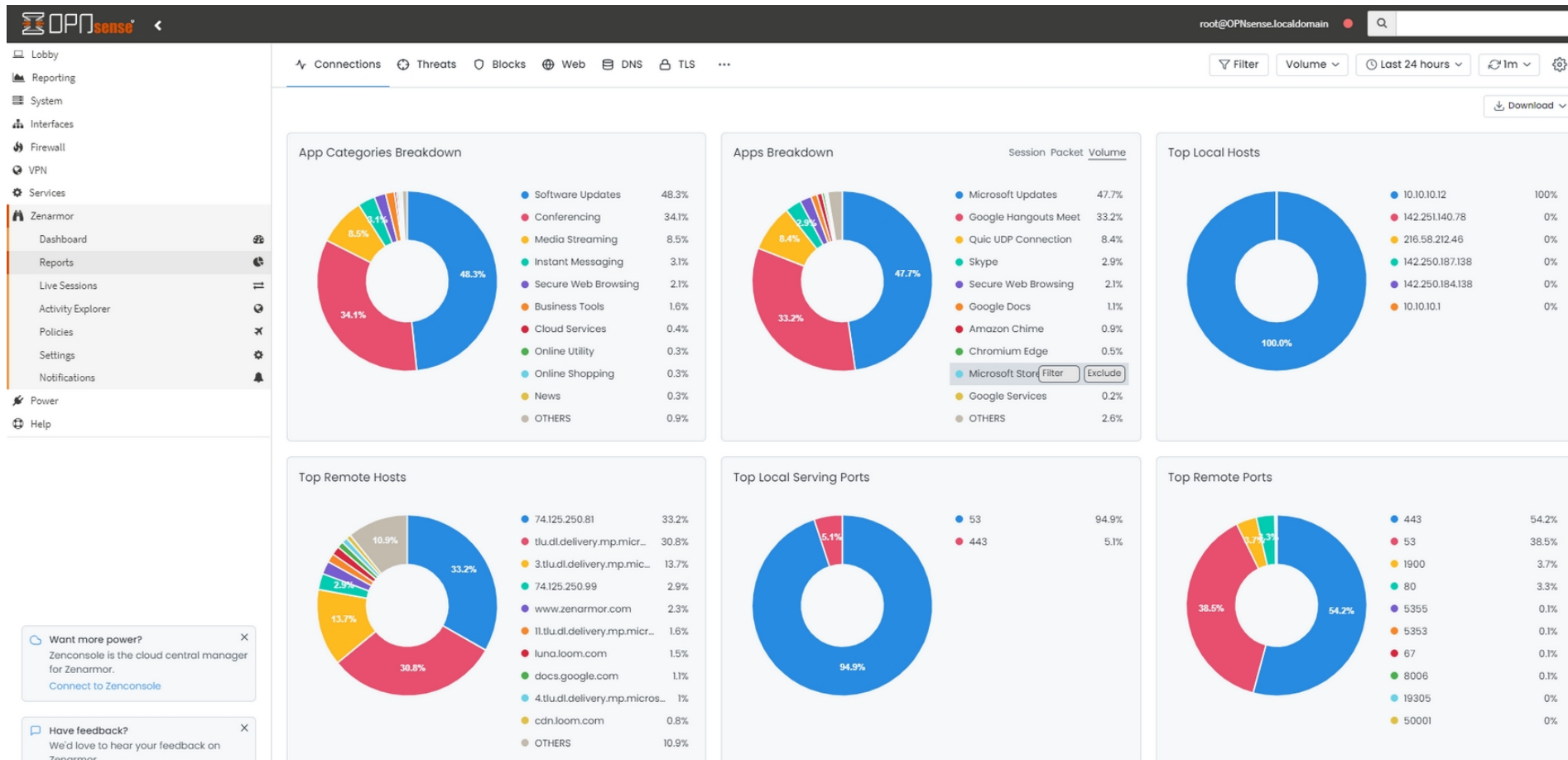
Usage: 56.9 MB / 20.6 GB
Mount: /var/log

Memory Utilization

Used: 3.9 GB
Total: 7.9 GB

Cloud Nodes Status

Europe **UP** 100%
Europe2 **UP** 100%



Default Discard Apply Changes X

Configuration Security App Controls Web Controls Exclusions

Essential Security ...

Category name	Status
DNS over HTTPS	Blocked ☒
Malware/Virus	Blocked ☒
Phishing	Blocked ☒
Hacking	Blocked ☒
Spam sites	Blocked ☒
Potentially Dangerous	Blocked ☒
Parked Domains	Blocked ☒
Firstly Seen Sites	Blocked ☒

Advanced Security ...

Category name	Status
Recent Malware/Phishing/Virus Outbreaks	Blocked ☒
Botnet C&C 	Blocked ☒
Botnet DGA Domains 	Blocked ☒
DNS Tunneling 	Blocked ☒
Compromised Website	Blocked ☒
Spyware and Adware	Blocked ☒
Keyloggers and Monitoring	Blocked ☒
Proxy	Blocked ☒
Dead Sites	Blocked ☒
Dynamic DNS Sites	Blocked ☒
Newly Registered Sites	Blocked ☒
Newly Recovered Sites	Blocked ☒
Malformed DNS 	Blocked ☒

Engineering Department ✕

Configurations Security App Controls Web Controls Exclusions

☐ Display custom applications only + Create Custom App

All Categories

Category Name	Number of blocked sub-categories	Status
A.I. Tools	0 / 25	Allowed ☐
Ad Tracker	213 / 213	Blocked ☒
Ads	351 / 351	Blocked ☒
Blogs	0 / 54	Allowed ☐
Business Tools	0 / 132	Allowed ☐
Cloud Services	0 / 107	Allowed ☐
Conferencing	0 / 18	Allowed ☐
Database	0 / 19	Allowed ☐
Email	0 / 43	Allowed ☐

Create Custom Application

Application Name

Description

Category

Protocol

IP Addresses

+ Add IP Address

Hostnames

+ Add Hostname

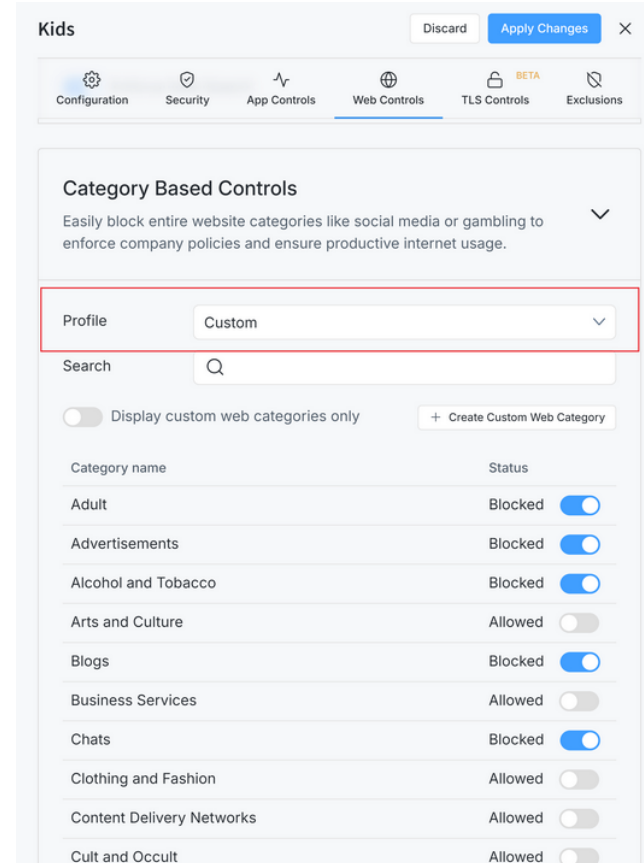
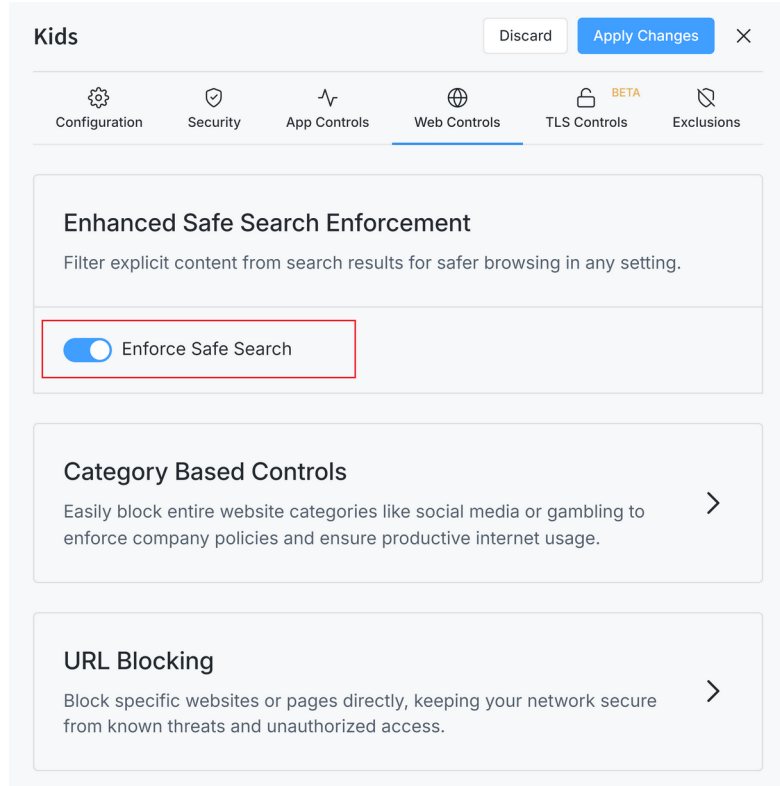
Ports

+ Add Port

☐ I accept sharing of this application signature with zenarmor team to improve App Database quality.
[Privacy Policy](#)

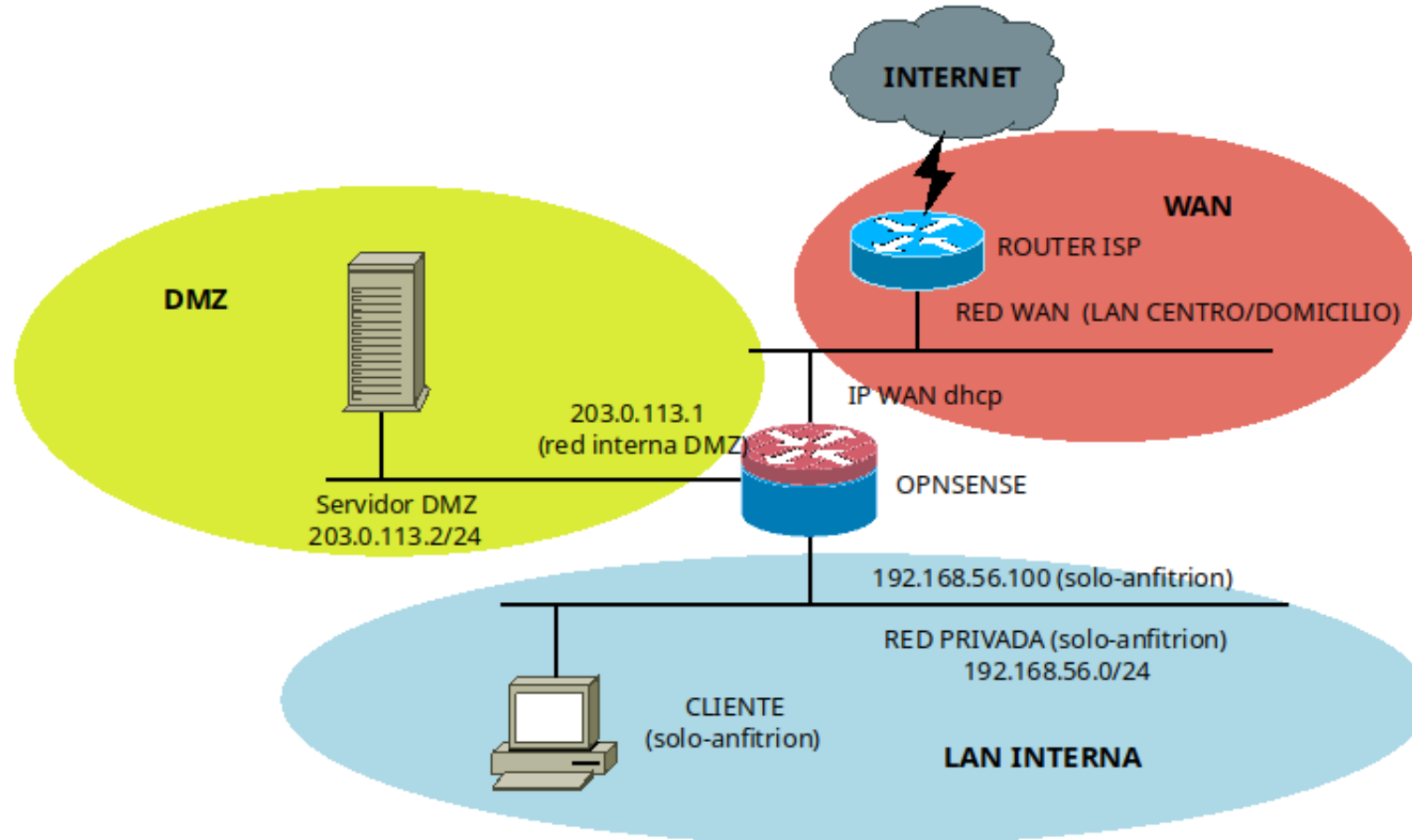
Cancel

Create

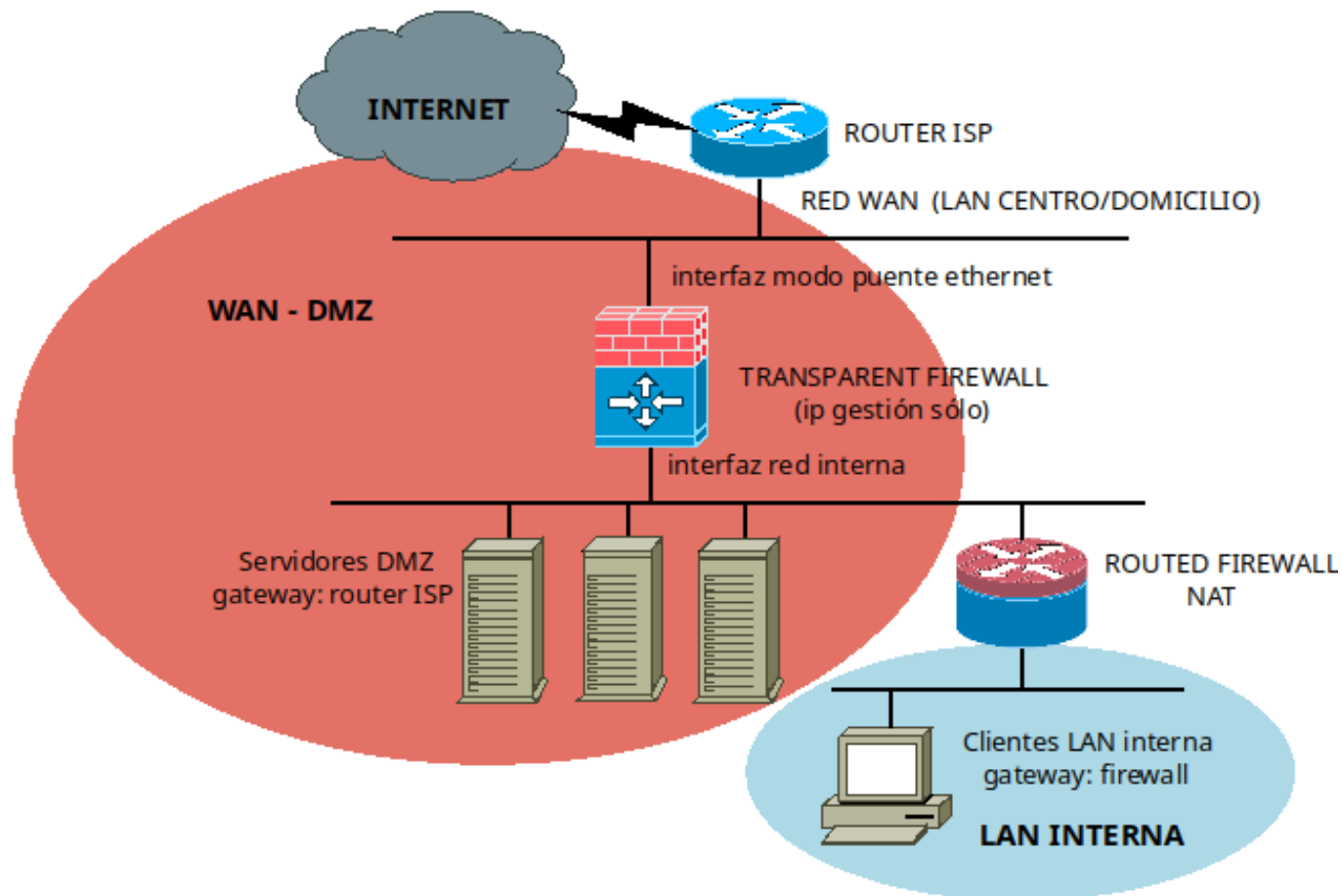


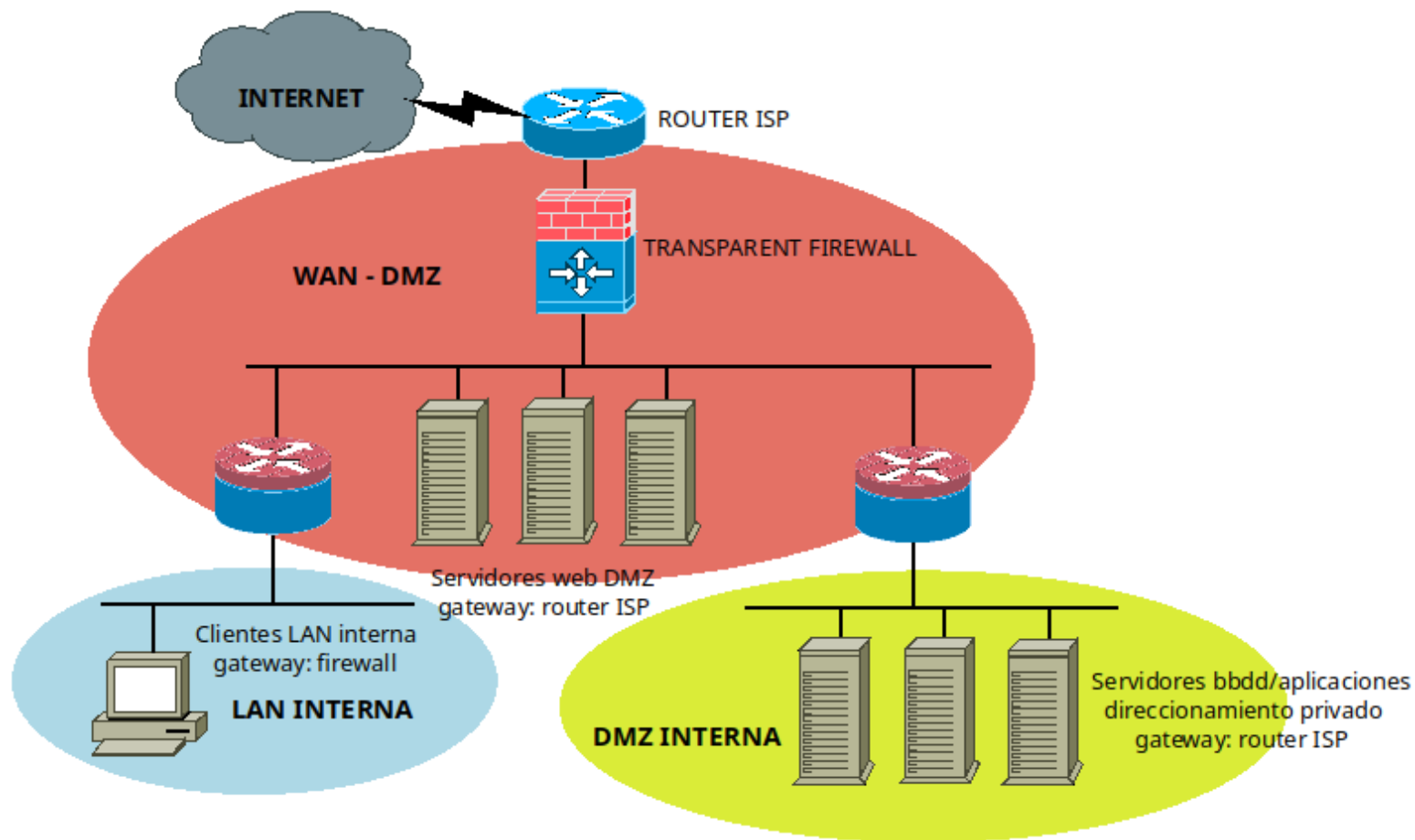
Algunos Labs con OPNSense usados en prácticas y proyectos

Firewall único

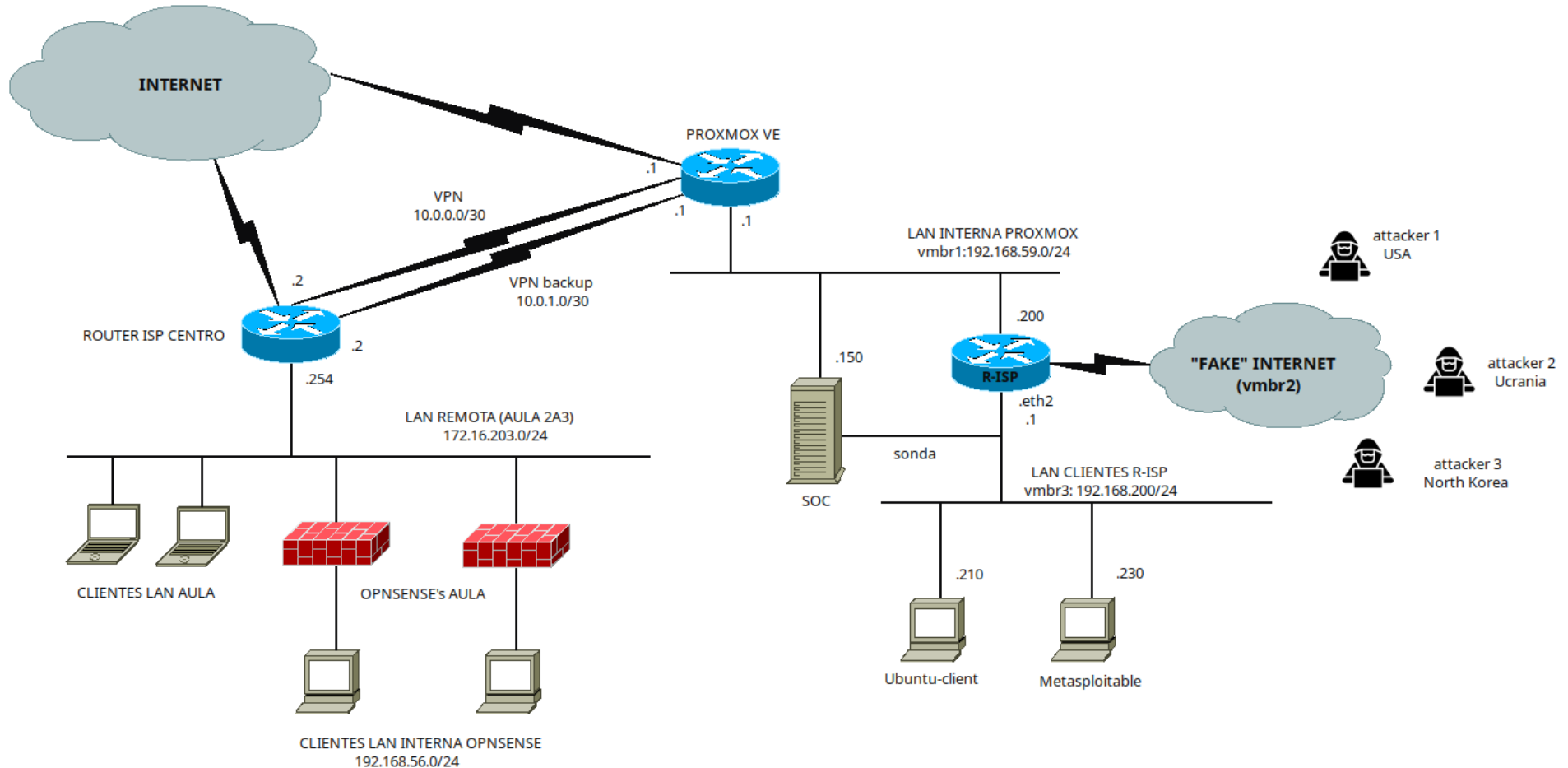


Doble capa de firewall

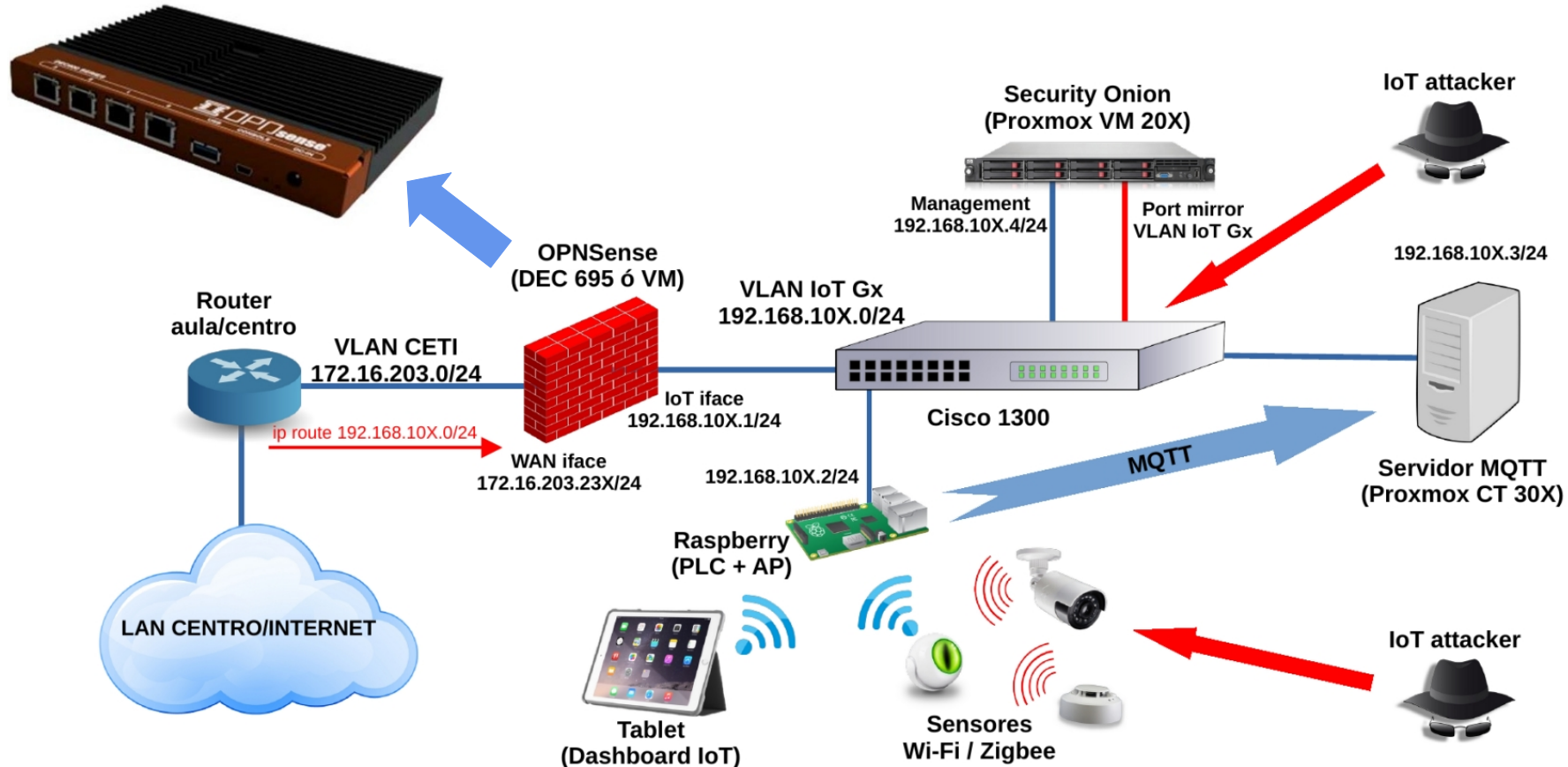




Curso operaciones ciberseguridad RECE



Lab proyecto IoT



¡Muchas gracias!