UNIVERSITAS Miguel Hernández

Cisco Networking Academy

CIPFP Mislata
Centre Integrat Públic
Formació Professional Superior

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

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...

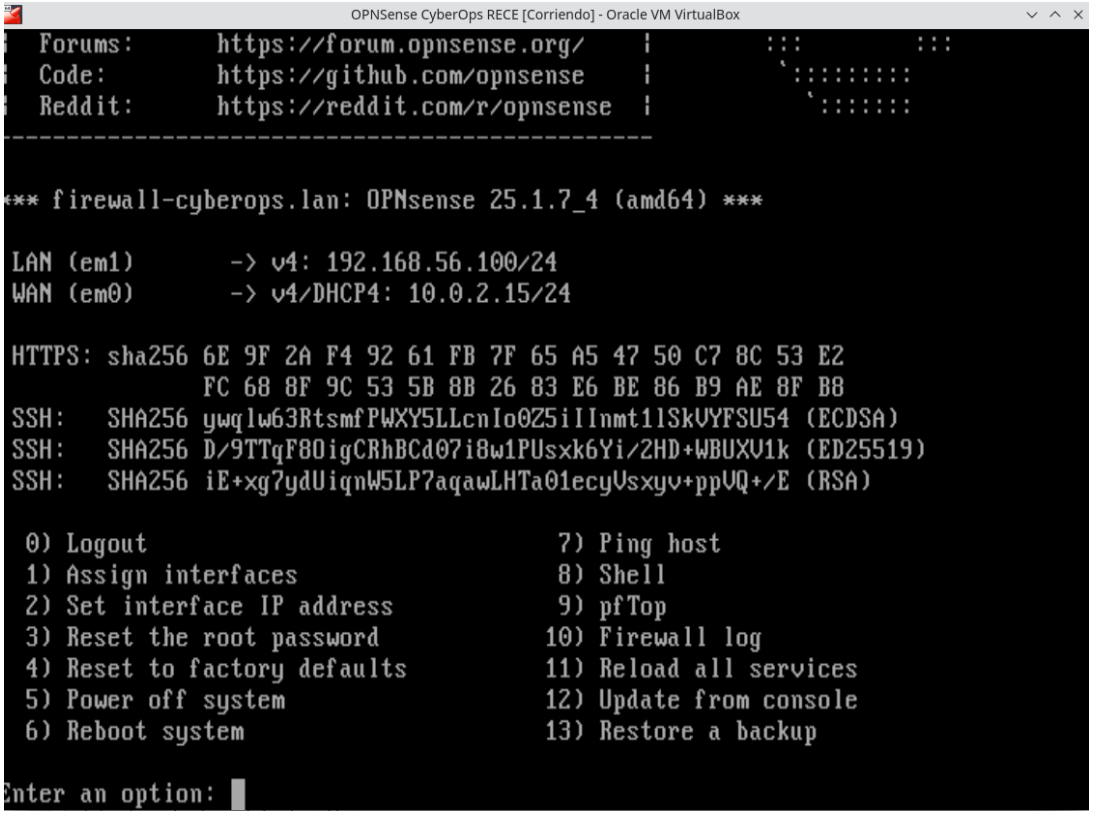
UNIVERSITAS Miguel Hernández

¿Qué necesitamos?

CIPFP Mislata
Centre Integrat Públic Formació Professional Superior

- 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/

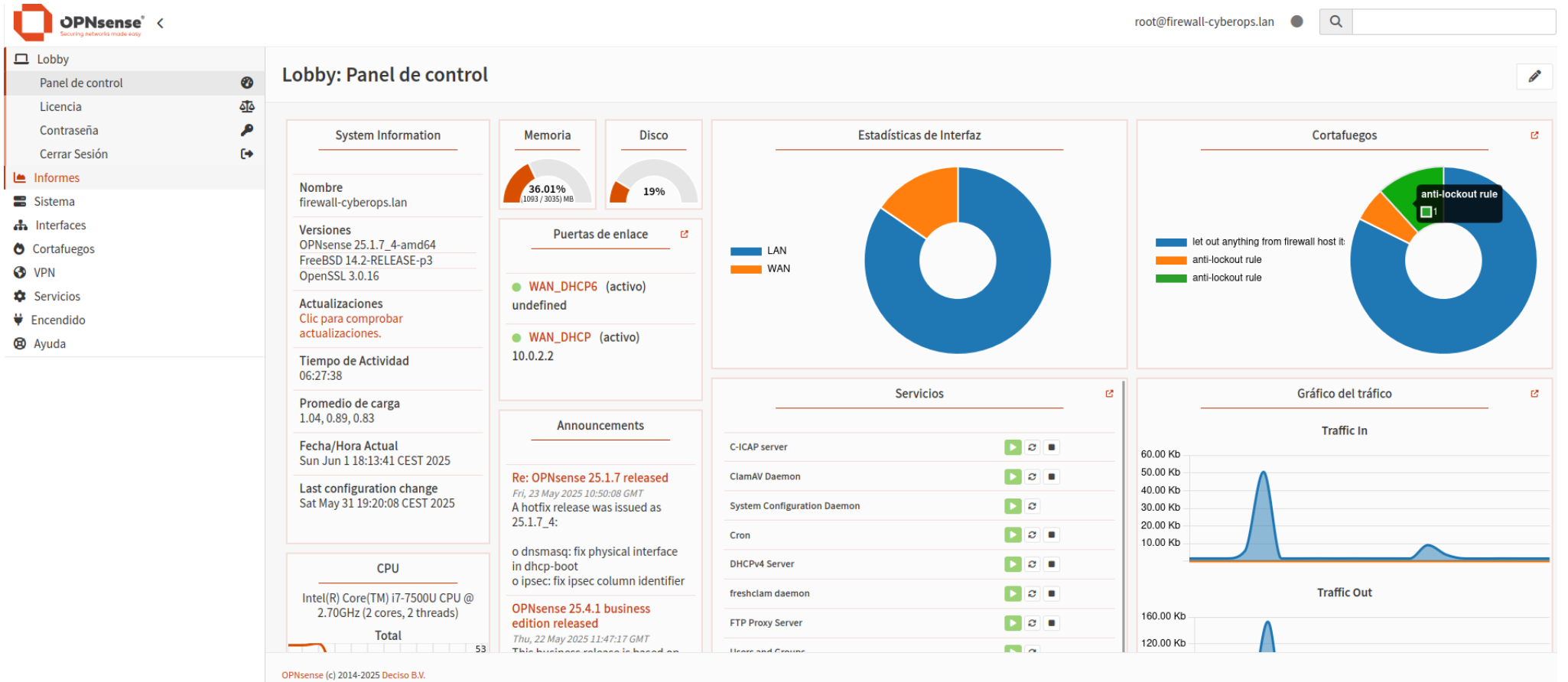
Consola y GUI



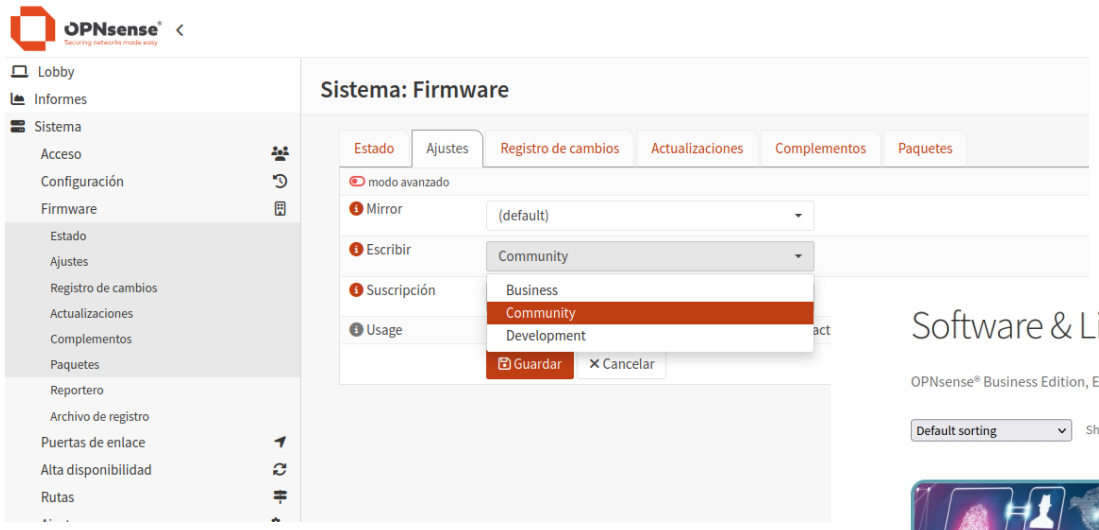
UNIVERSITAS Miguel Hernández

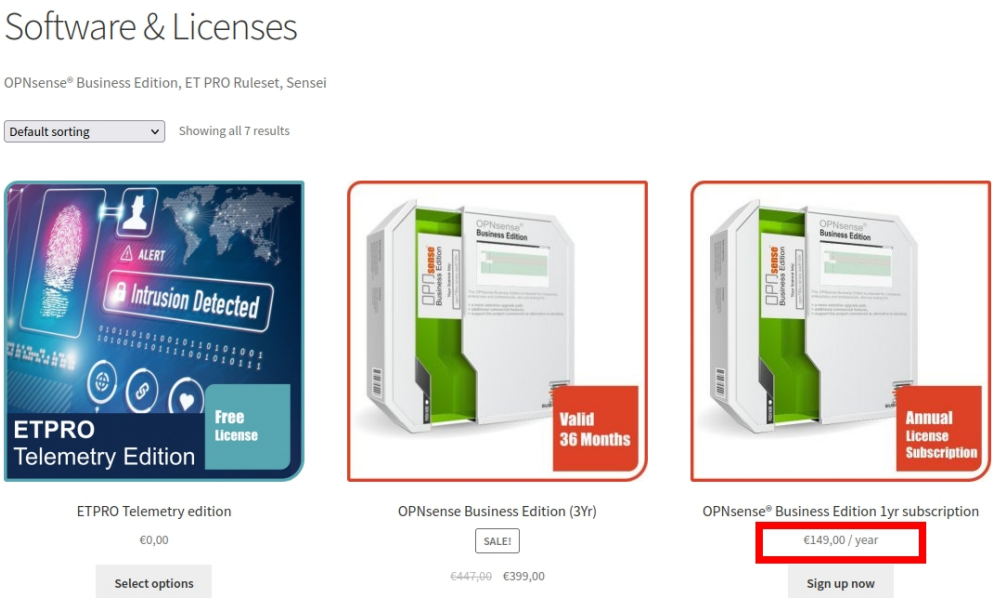
Panel de Control

CIPFP Mislata
Centre Integrat Públic
Formació Professional Superior

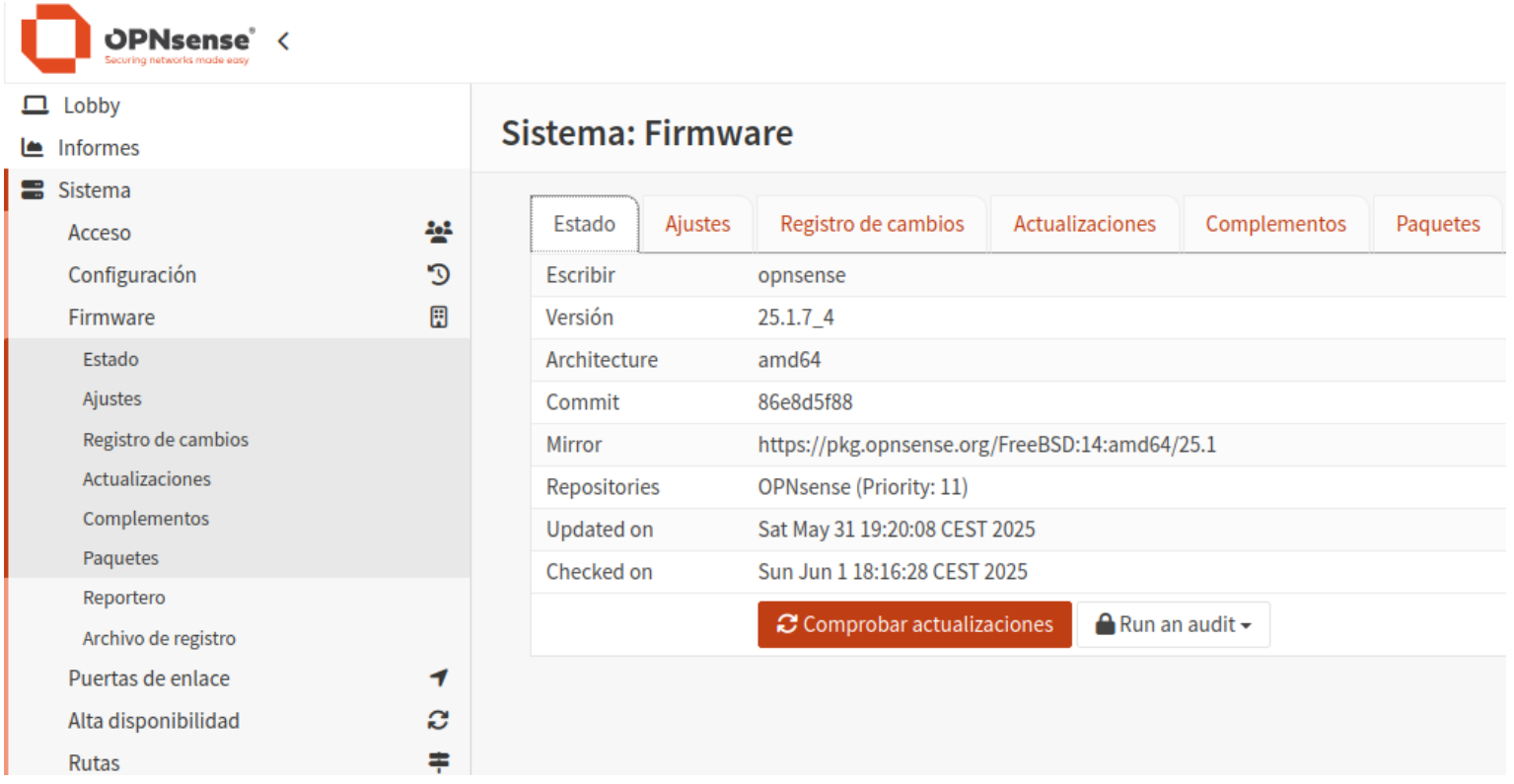


Licencia


OPNsense
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
Community
Development
Usage
Guardar
Cancelar


Software & Licenses
OPNsense® Business Edition, ET PRO Ruleset, Sensei
Default sorting
Showing all 7 results
ALERT
Intrusion Detected
ETPRO
Telemetry Edition
Free
License
Valid
36 Months
Annual
License
Subscription
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

Firmare y actualizaciones

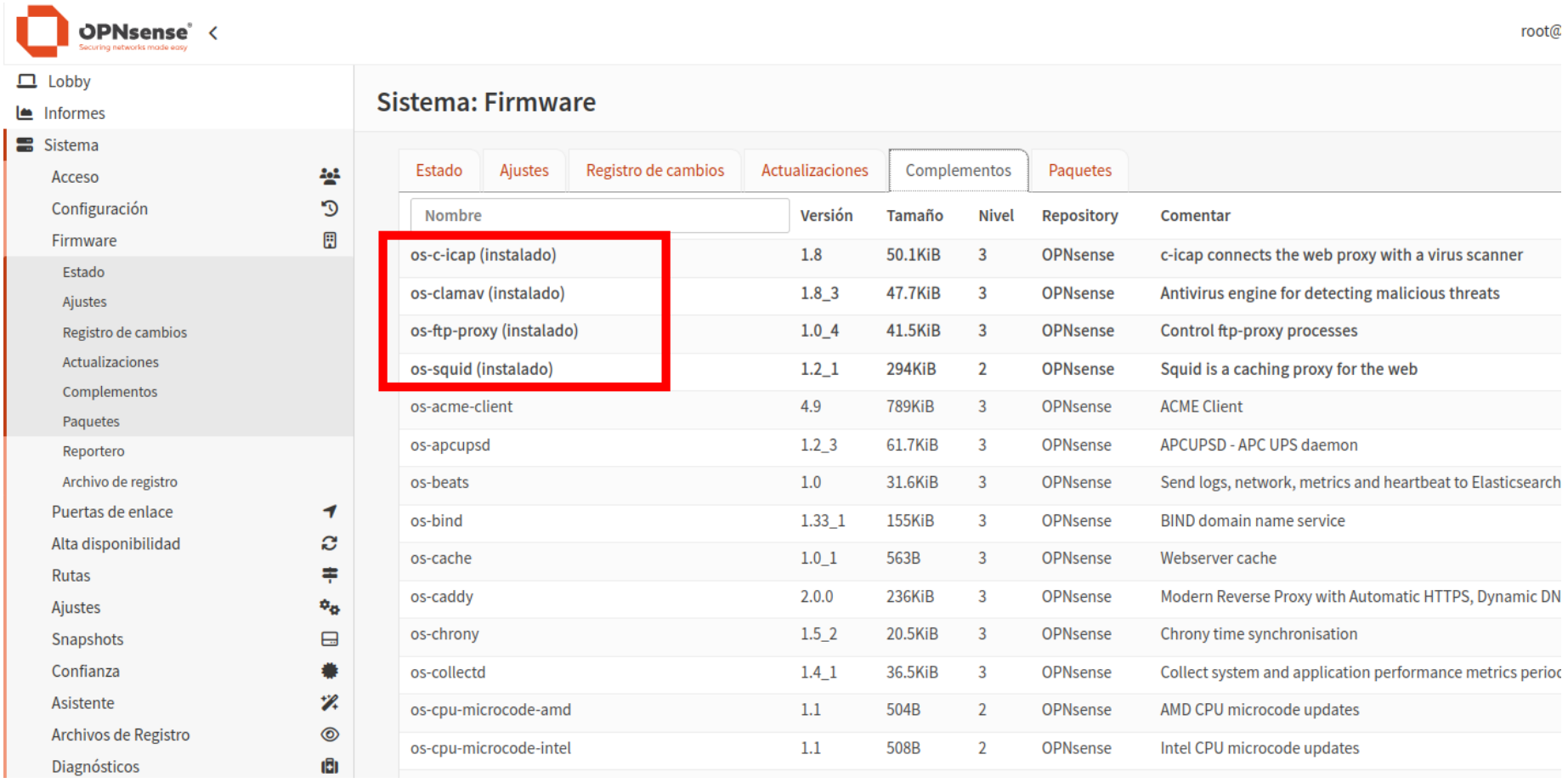


Plugins

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

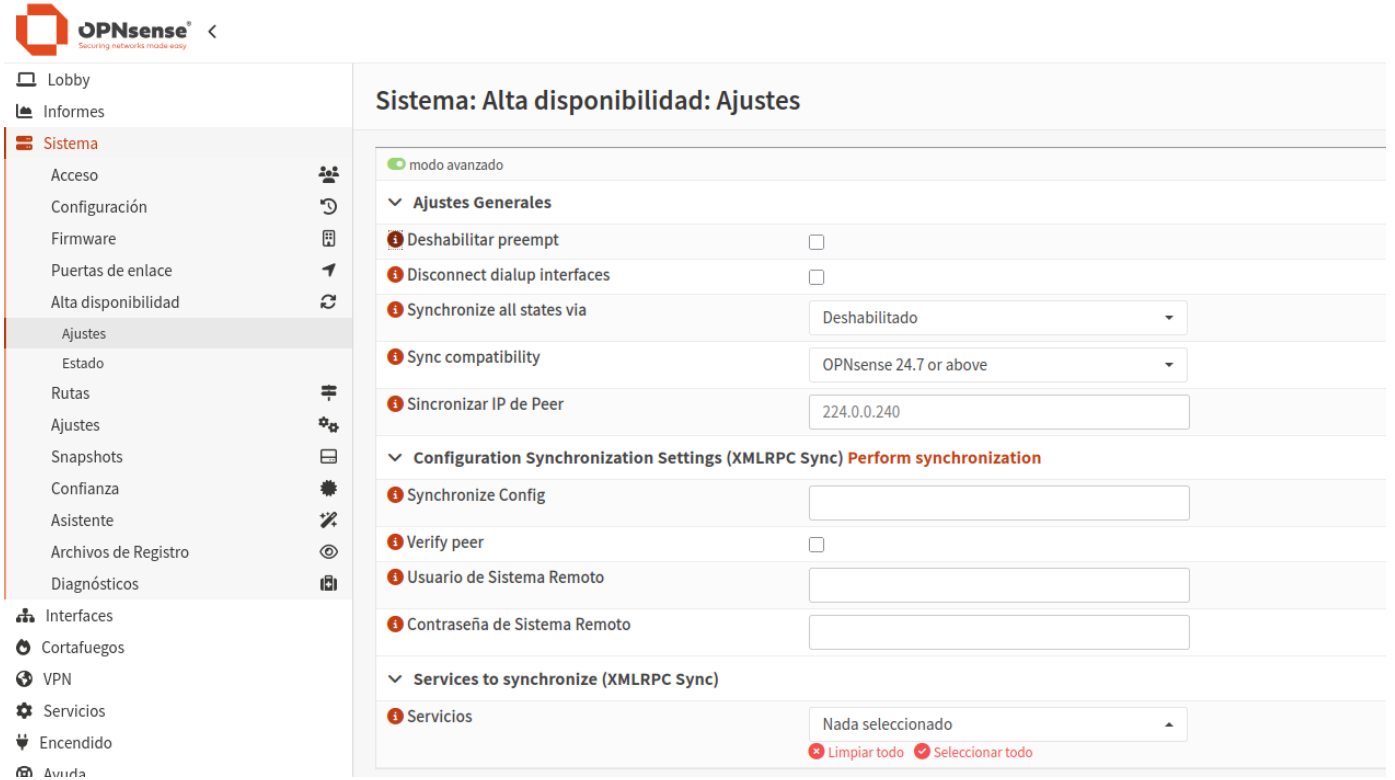
- ClamAV: antivirus libre basado en firmas
- I-CAP: protocolo para análisis de contenido web
- Rspamd: filtro anti-spam para correo-e
- OpenDNS (Cisco Umbrella): seguridad en la capa dns
- ZeroTier: SDN
- Tinc: VPN multipunto
- ZenArmor (Sensei): características avanzadas de NGFW bajo suscripción
- ...

Plugins


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
Estado
Ajustes
Registro de cambios
Actualizaciones
Complementos
Paquetes
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 perioc
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

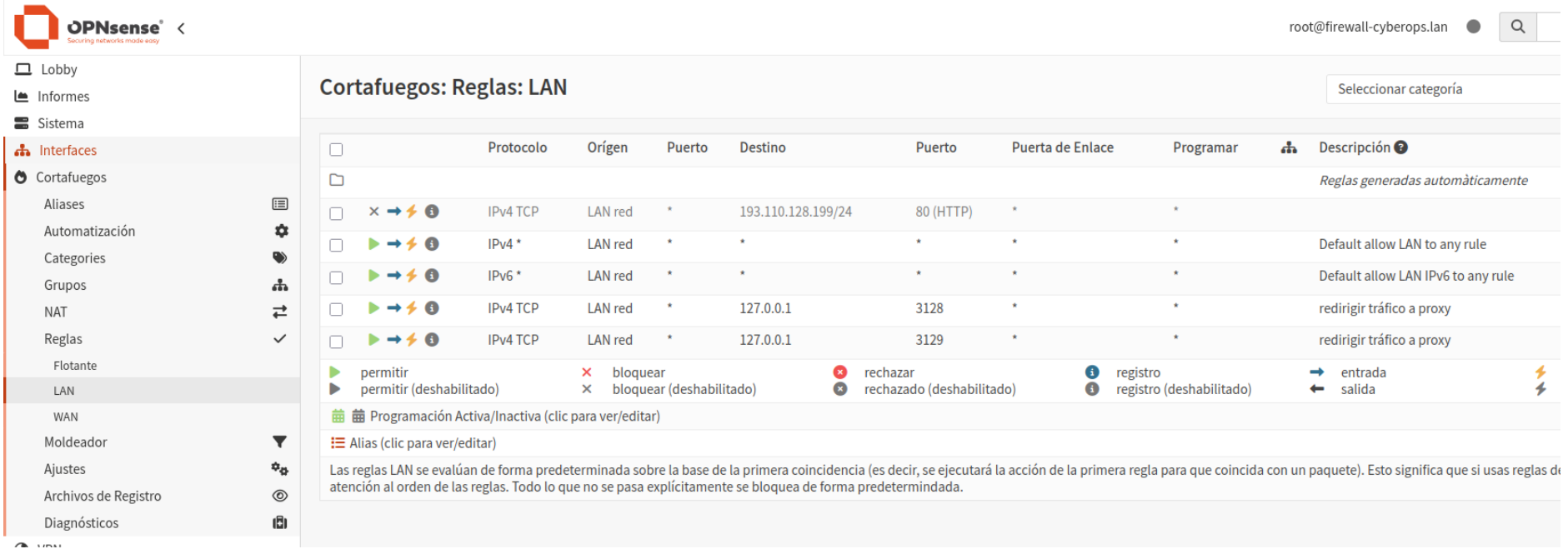
Alta disponibilidad

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.



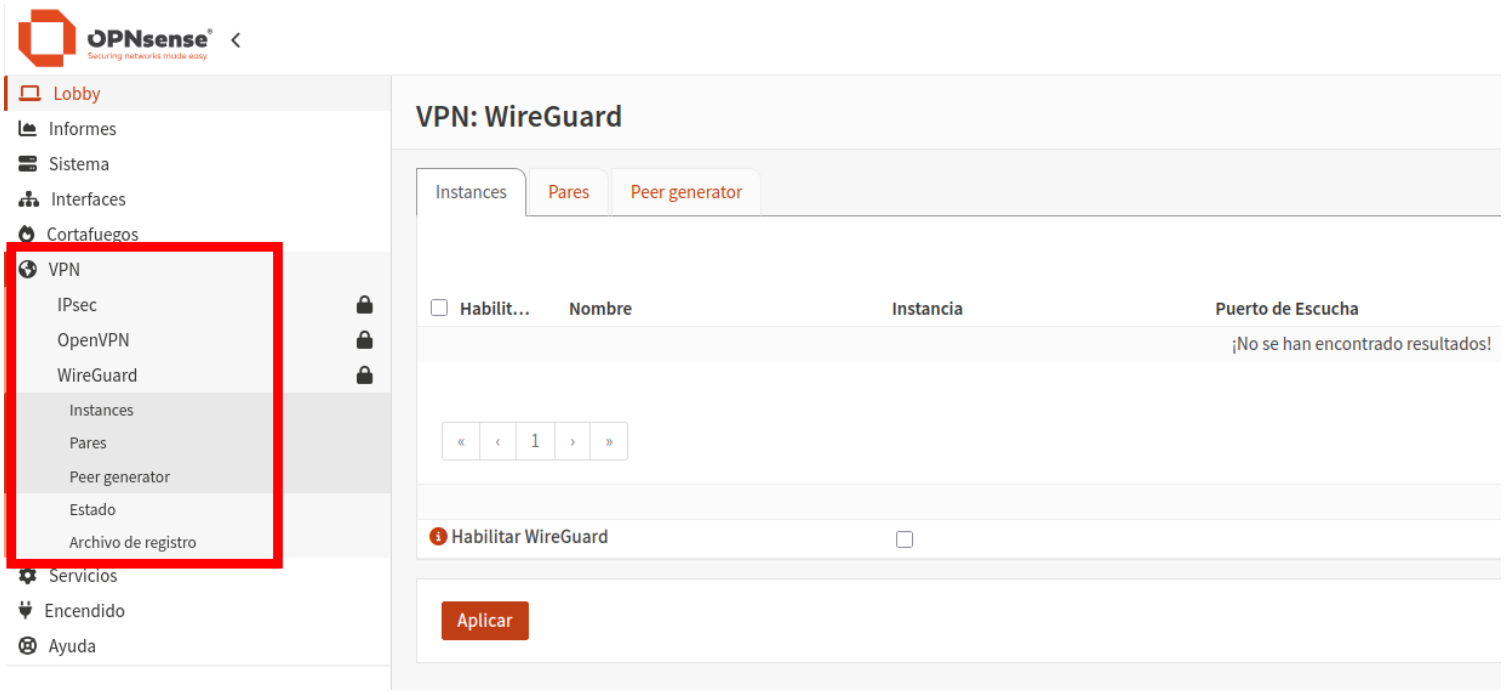
Reglas cortafuegos

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)



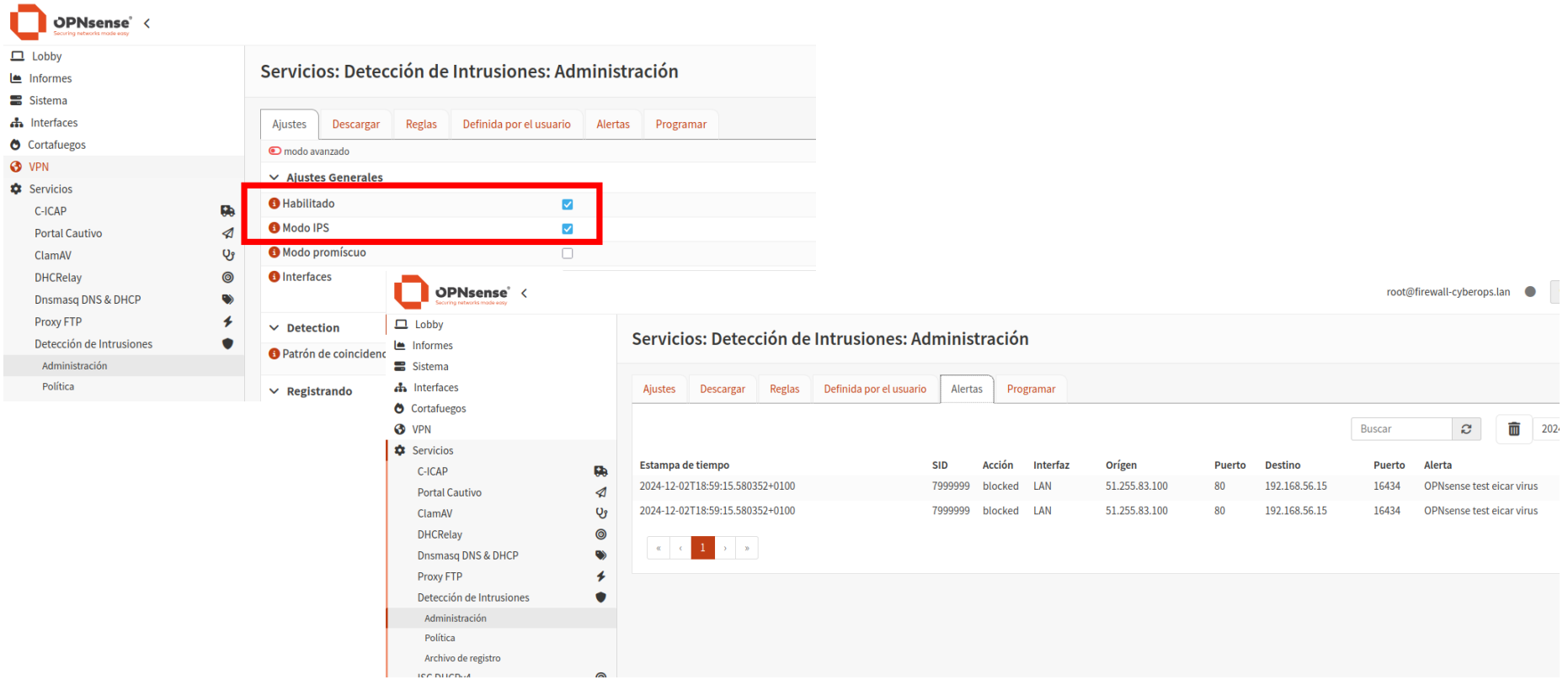
VPN

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



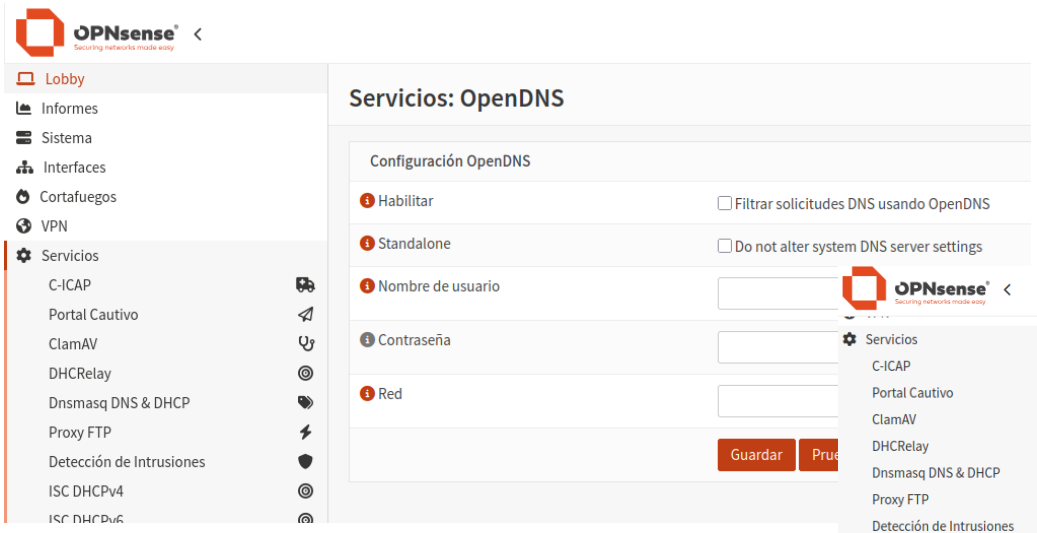
NIDS/NIPS

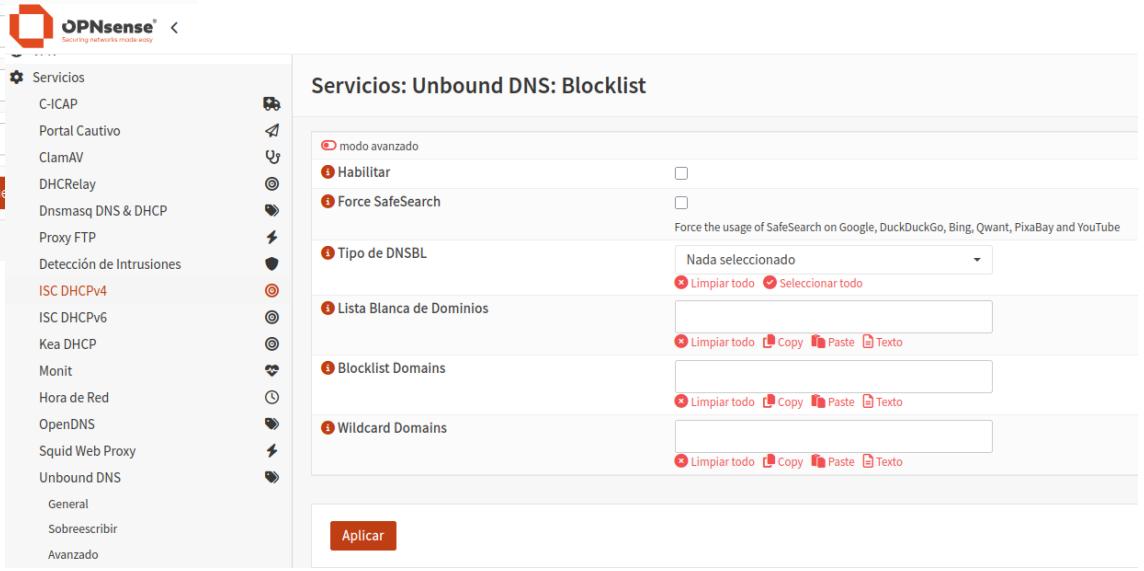
OPNsense a través de Suricata puede funcionar tanto como NIDS y NIPS (debe habilitarse)



Protección DNS

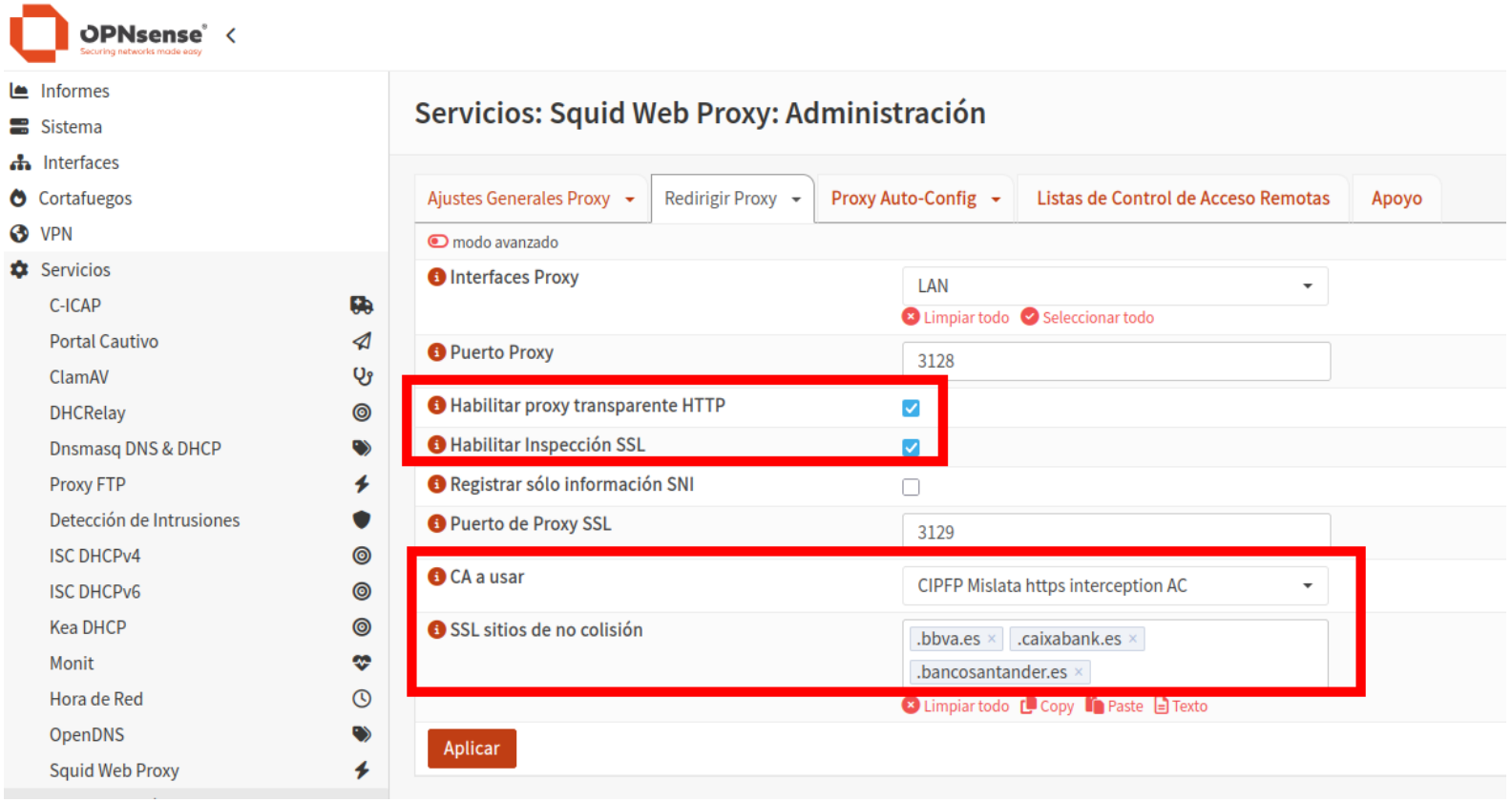
Puede utilizar los servicios de Cisco Umbrella (OpenDNS) o su propio servicio con listas negras públicas (Outbound DNS) y SafeSearch de Google, DuckDuckGo, Bing, Qwant, PixaBay y YouTube





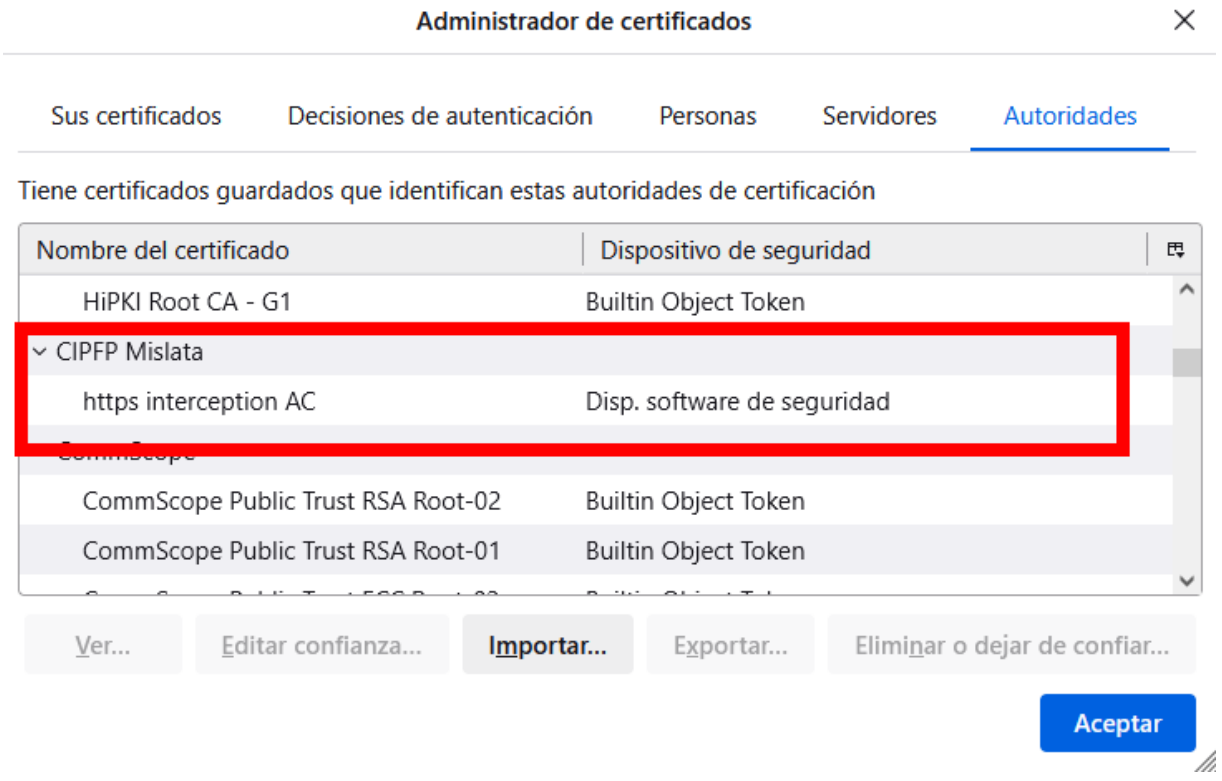
Intercepción HTTPS

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**

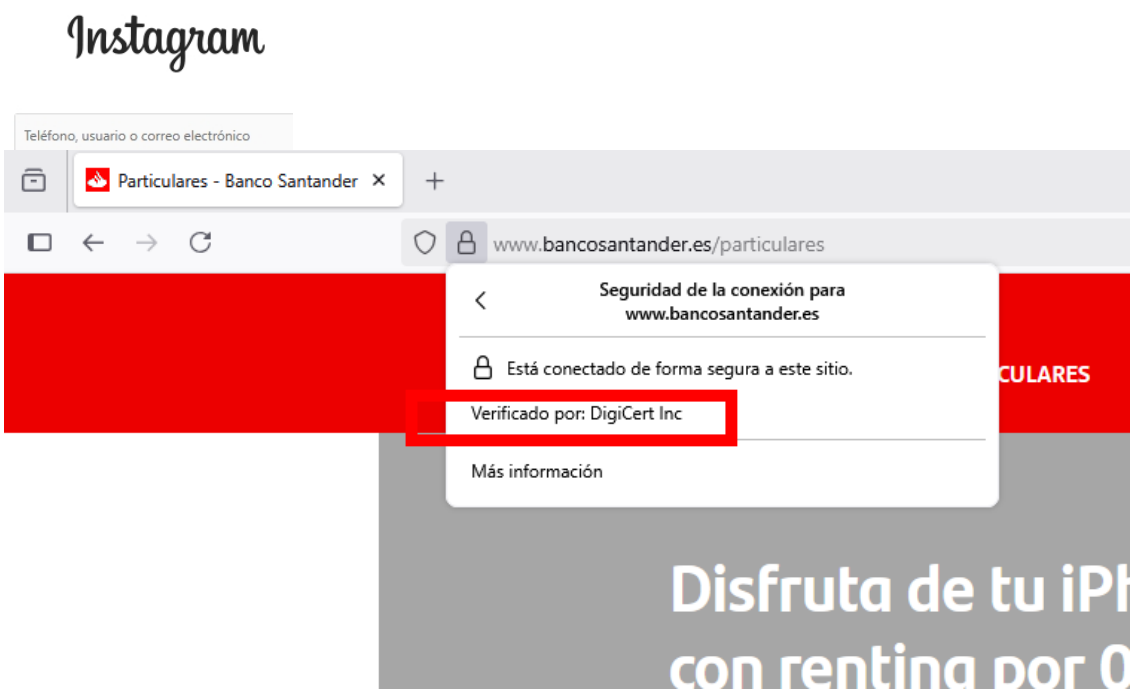


Intercepción HTTPS

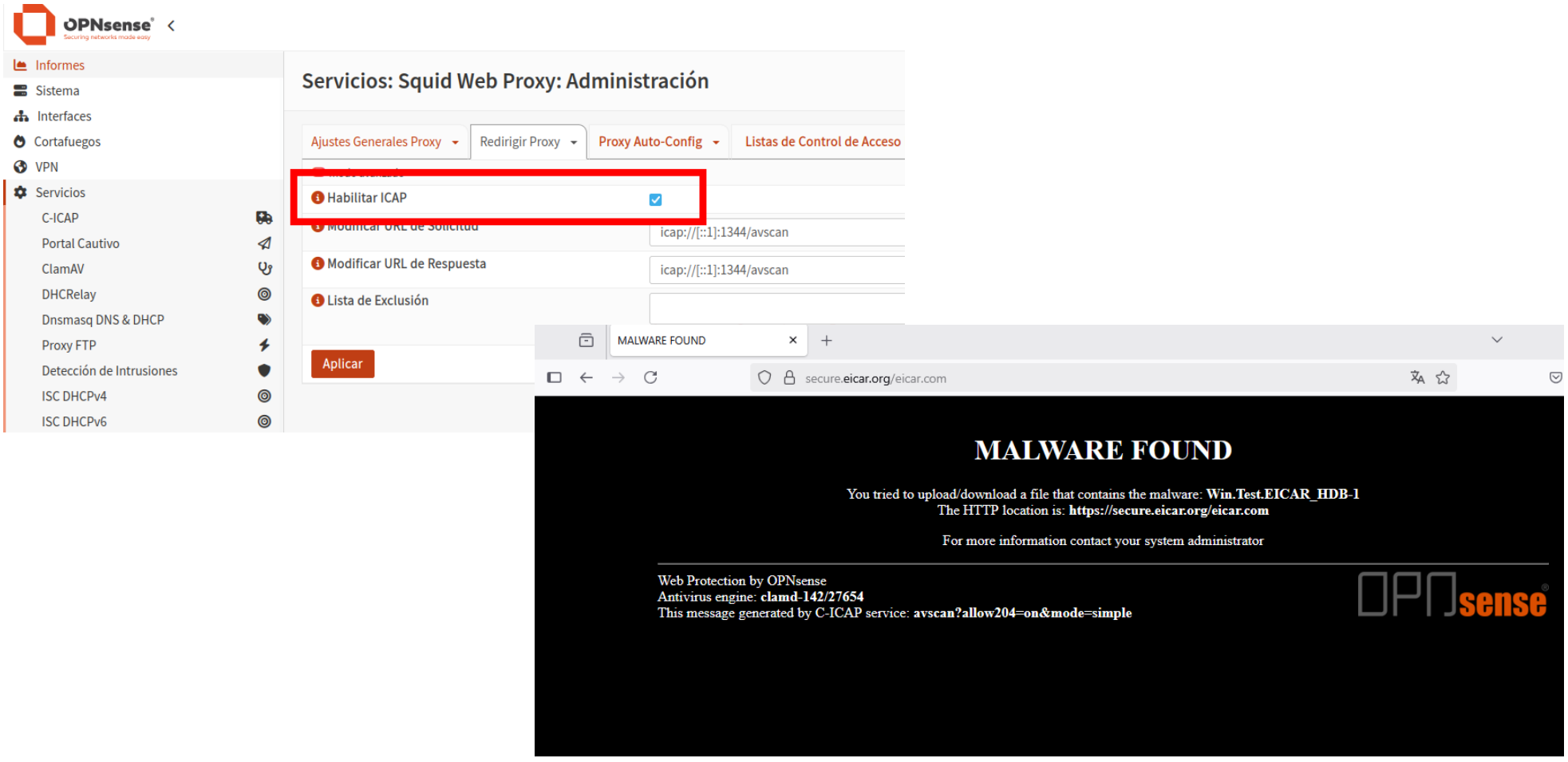
Es necesario importar el certificado de la CA generado por OPNSense, en todos los endpoints de la organización. Puede hacerse con directivas de grupo en AD o con herramientas como Intune:



Intercepción HTTPS



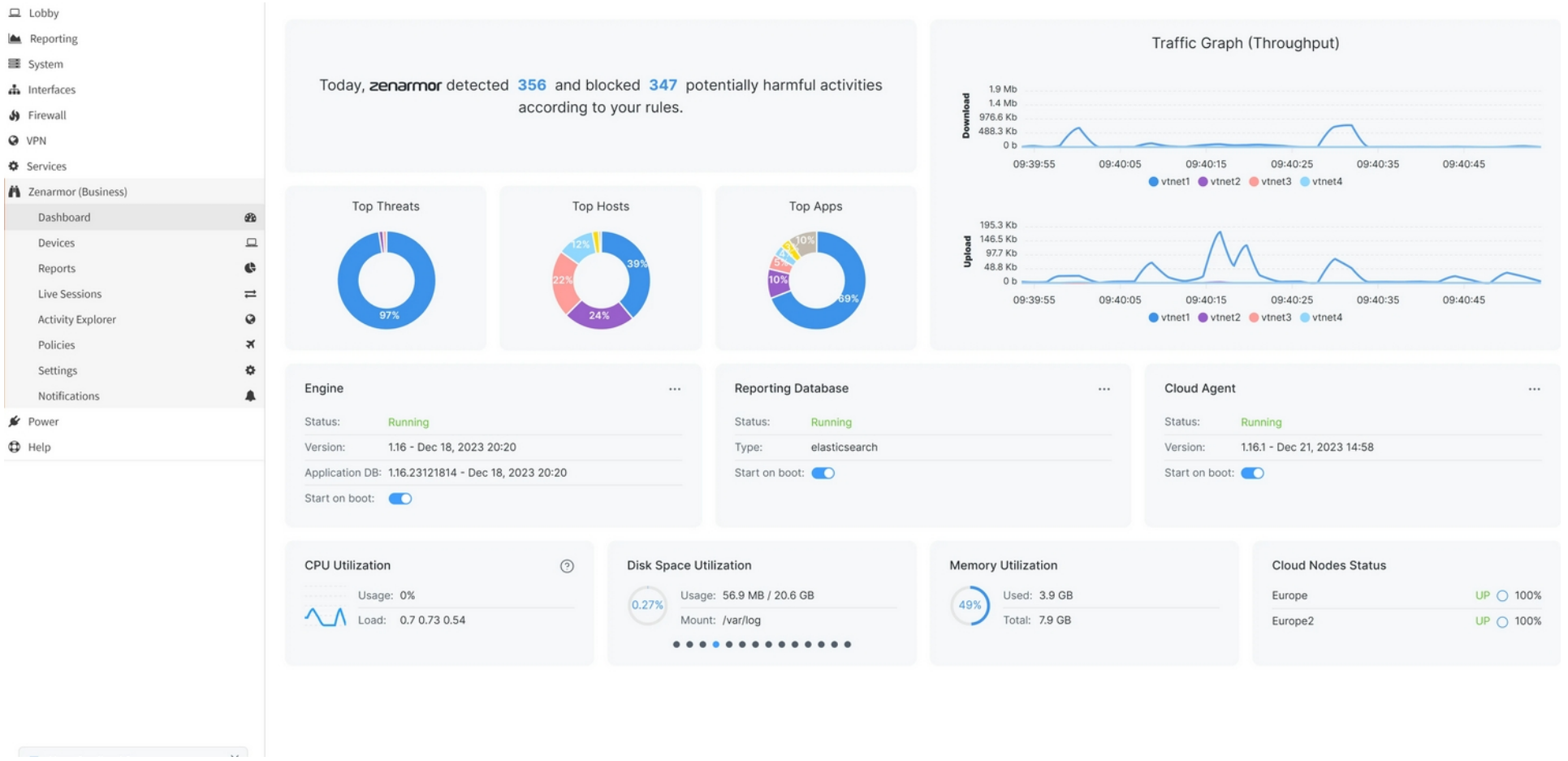
Detección de malware por HTTPS



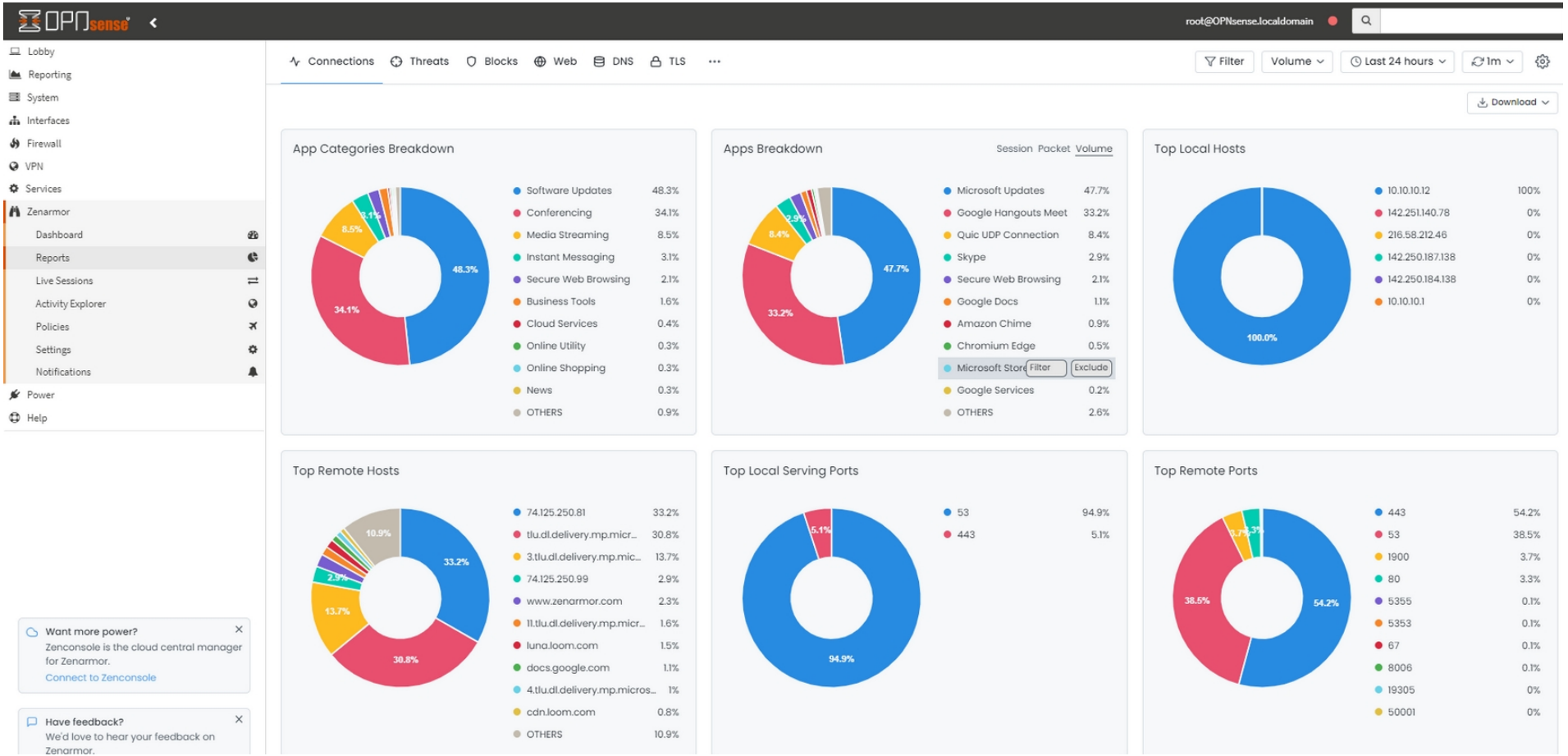
Plugin Zenarmor

- 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

Zenarmor - Dashboard



Zenarmor - Reports



Zenarmor - Security

Default Discard Apply Changes

Configuration | Security | App Controls | Web Controls | Exclusions

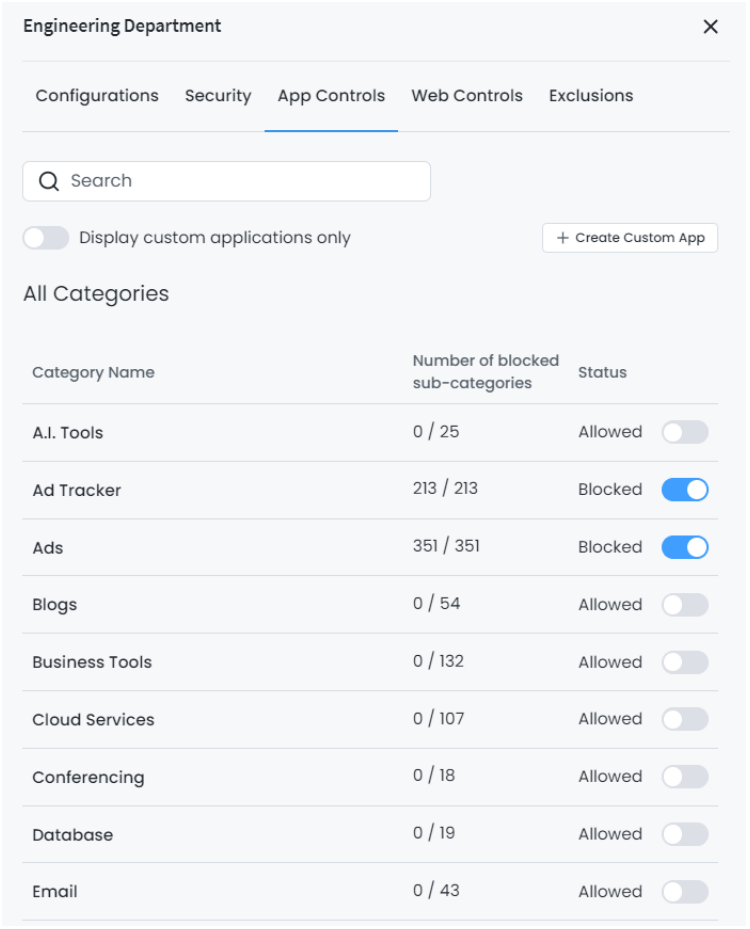
Essential Security

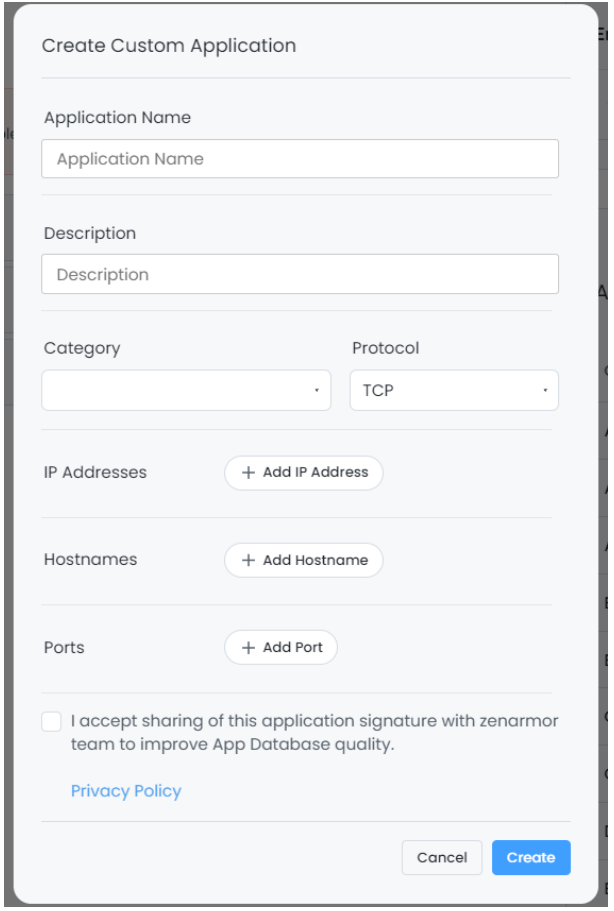
Category name	Status
DNS over HTTPS	Blocked
Malware/Virus	Blocked
Phishing	Blocked
Hacking	Blocked
Spam sites	Blocked
Potentially Dangerous	Blocked
Parked Domains	Blocked
Firstly Seen Sites	Blocked

Advanced Security

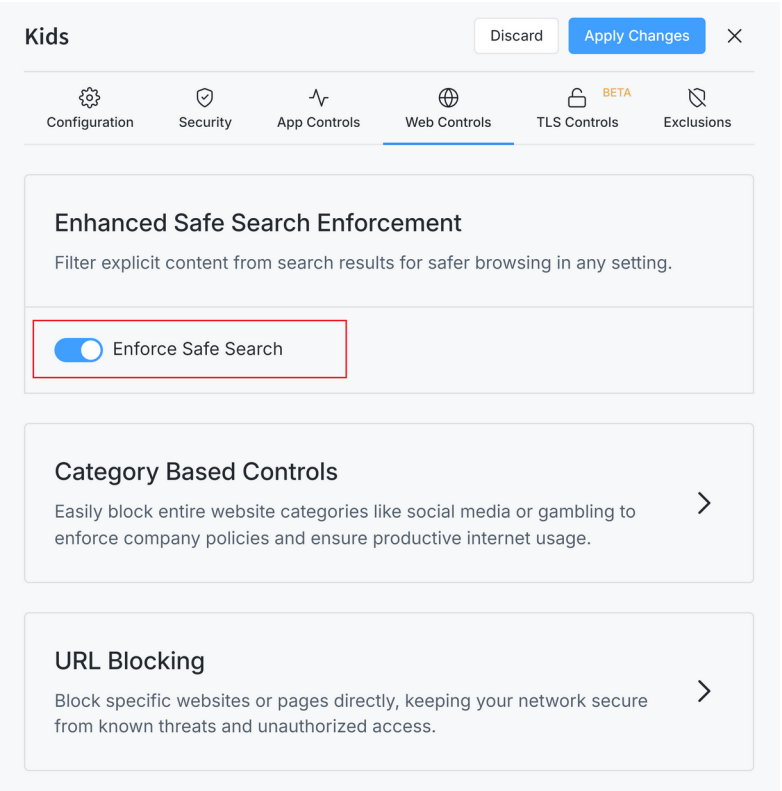
Category name	Status
Recent Malware/Phishing/Virus Outbreaks	Blocked
Botnet C&C NEW	Blocked
Botnet DGA Domains NEW	Blocked
DNS Tunneling NEW	Blocked
Compromised Website	Blocked
Spyware and Adware	Blocked
Keyloggers and Monitoring	Blocked
Proxy	Blocked
Dead Sites	Blocked
Dynamic DNS Sites	Blocked
Newly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

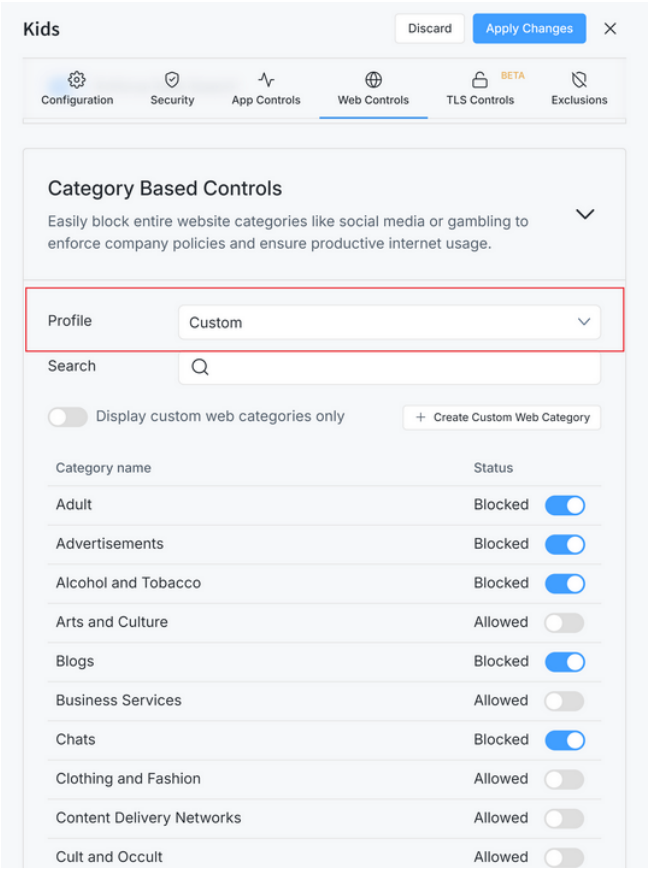
Zenarmor – App Control





Zenarmor – Web Control



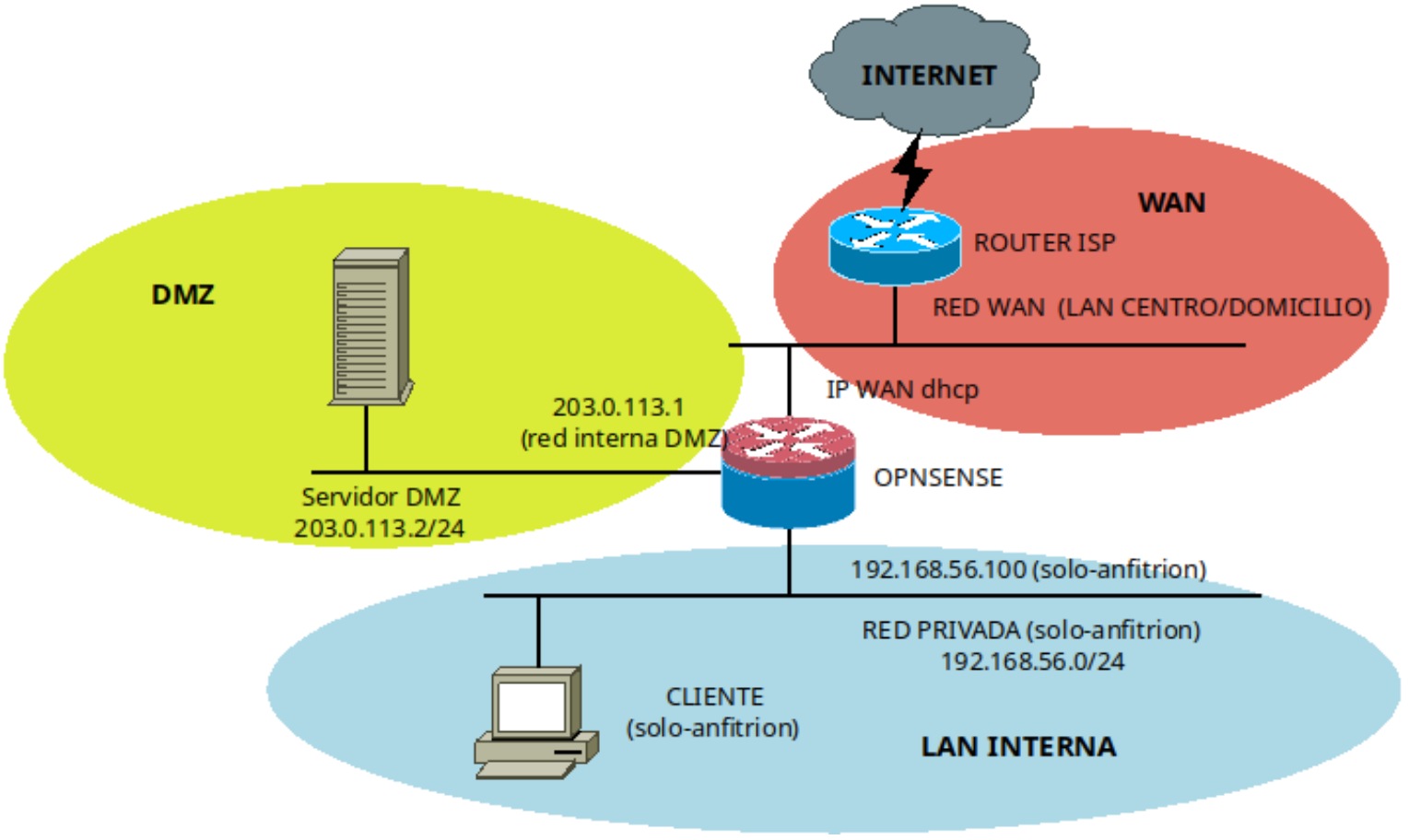


UNIVERSITAS Miguel Hernández

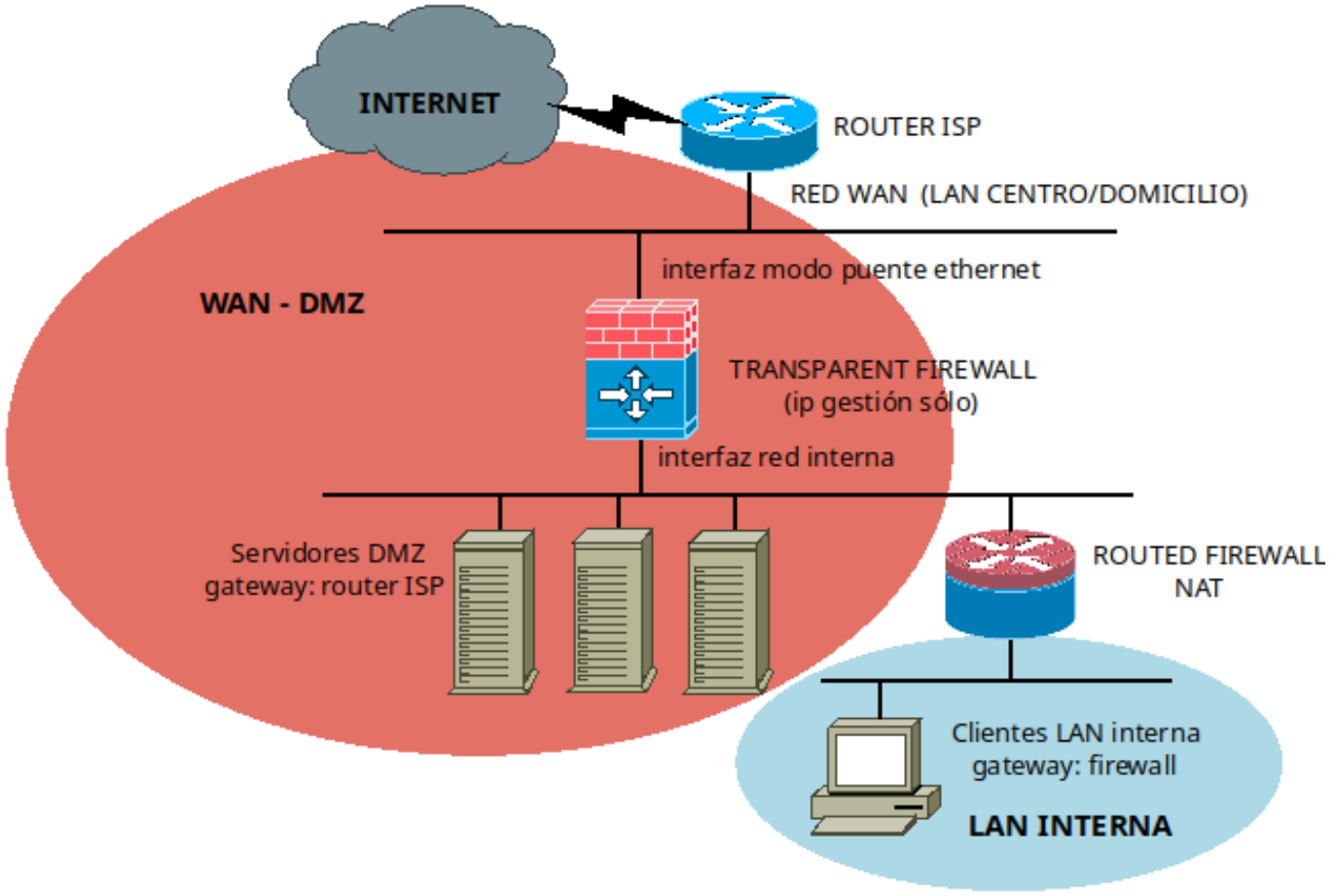
CIPFP Mislata
Centre Integrat Públic
Formació Professional Superior

Algunos Labs con OPNSense usados en prácticas y proyectos

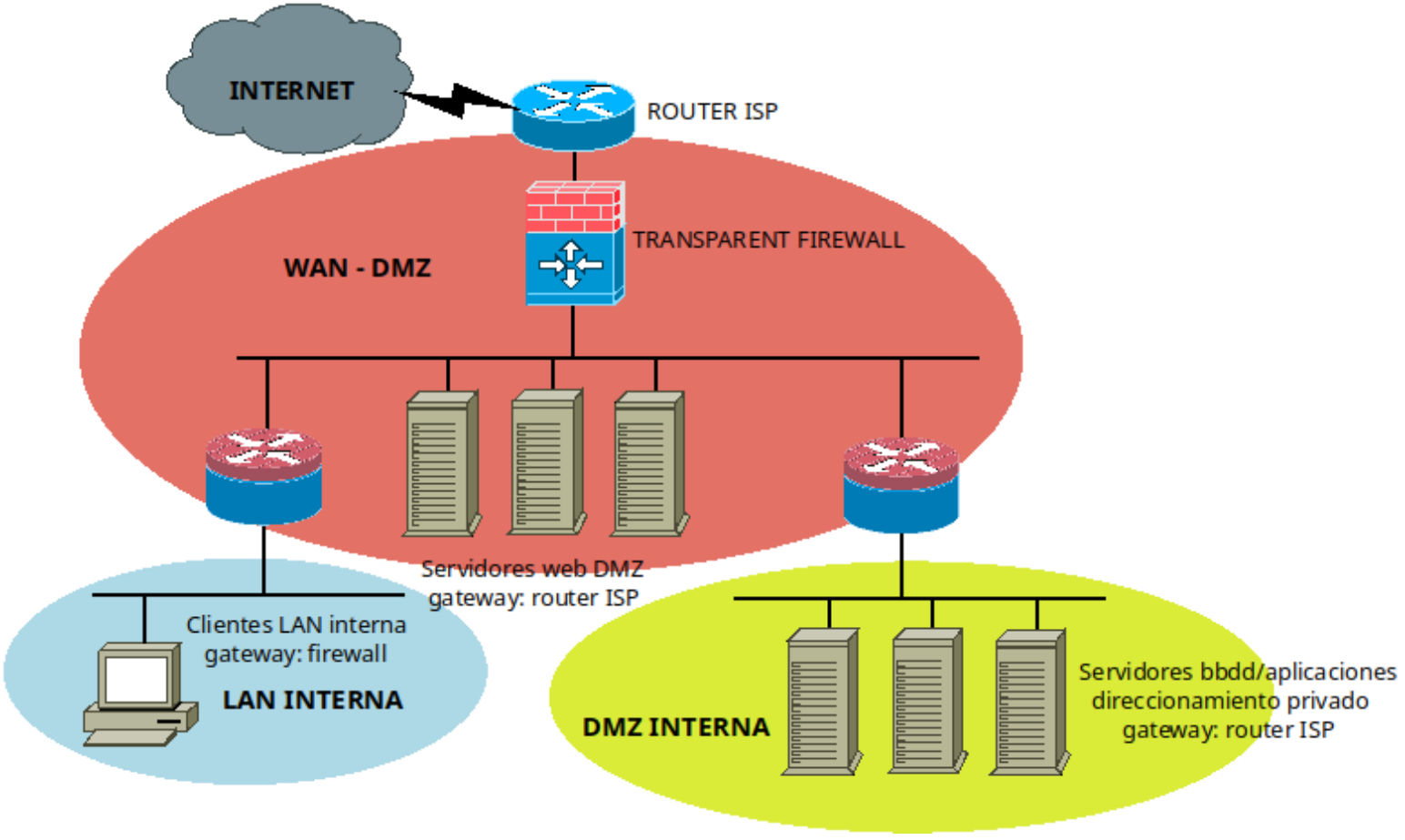
Firewall único



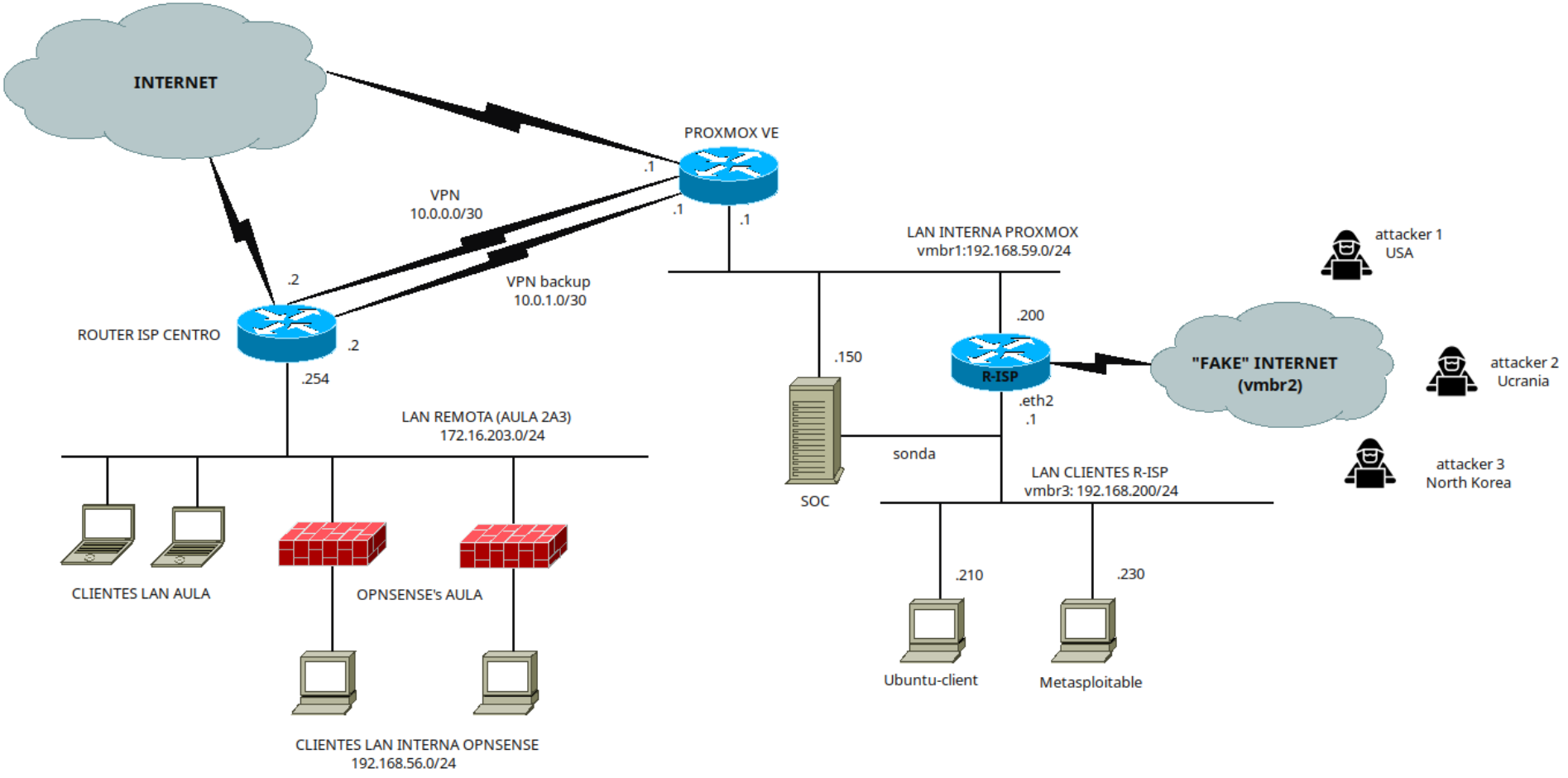
Doble capa de firewall



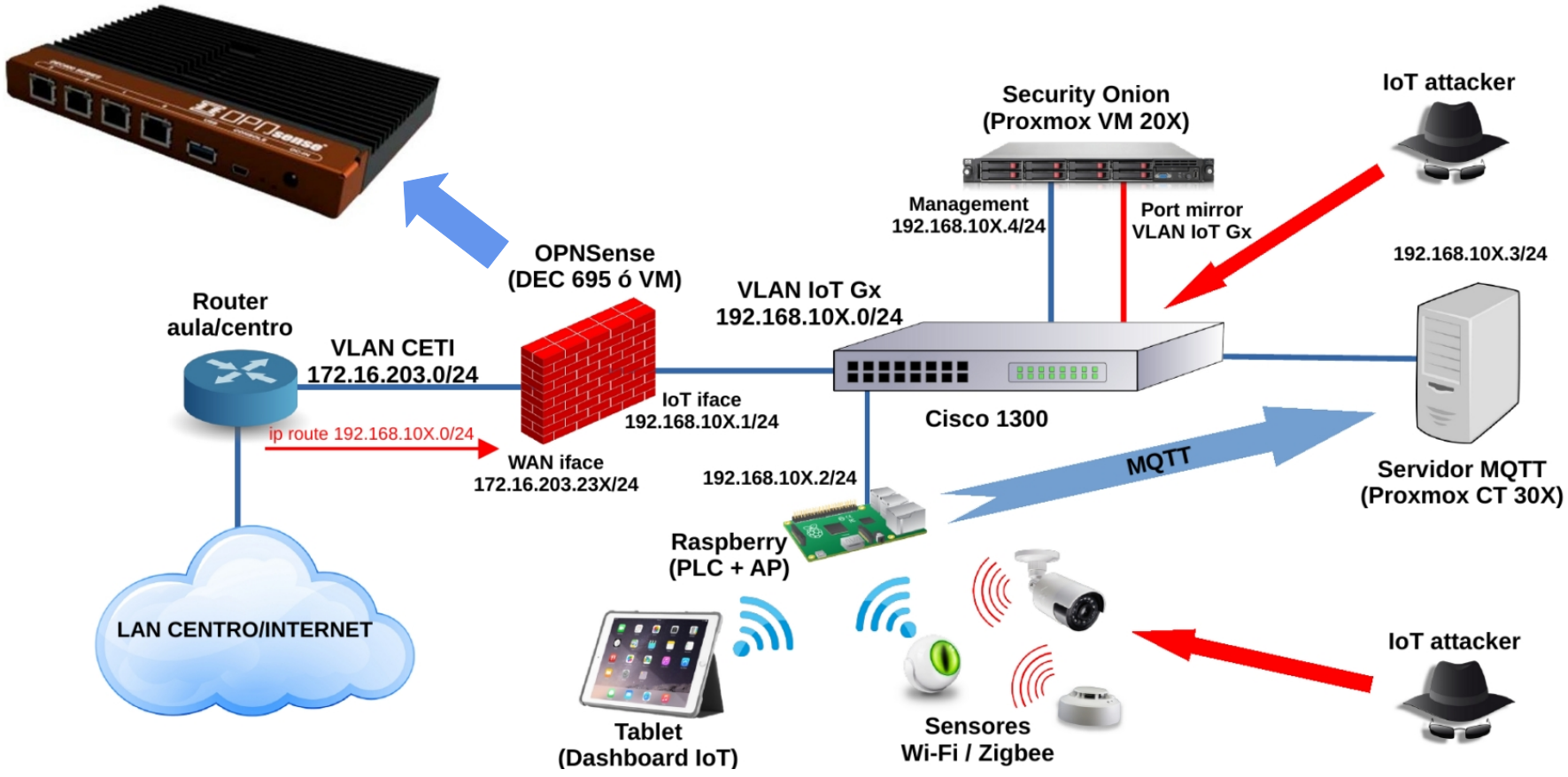
E-commerce + LAN interna



Curso operaciones ciberseguridad RECE



Lab proyecto IoT



UNIVERSITAS Miguel Hernández

CIPFP Mislata
Centre Integrat Públic
Formació Professional Superior

¡Muchas gracias!