Valoración del proyecto conjunto: Doraemon

ASOR - AdARed.

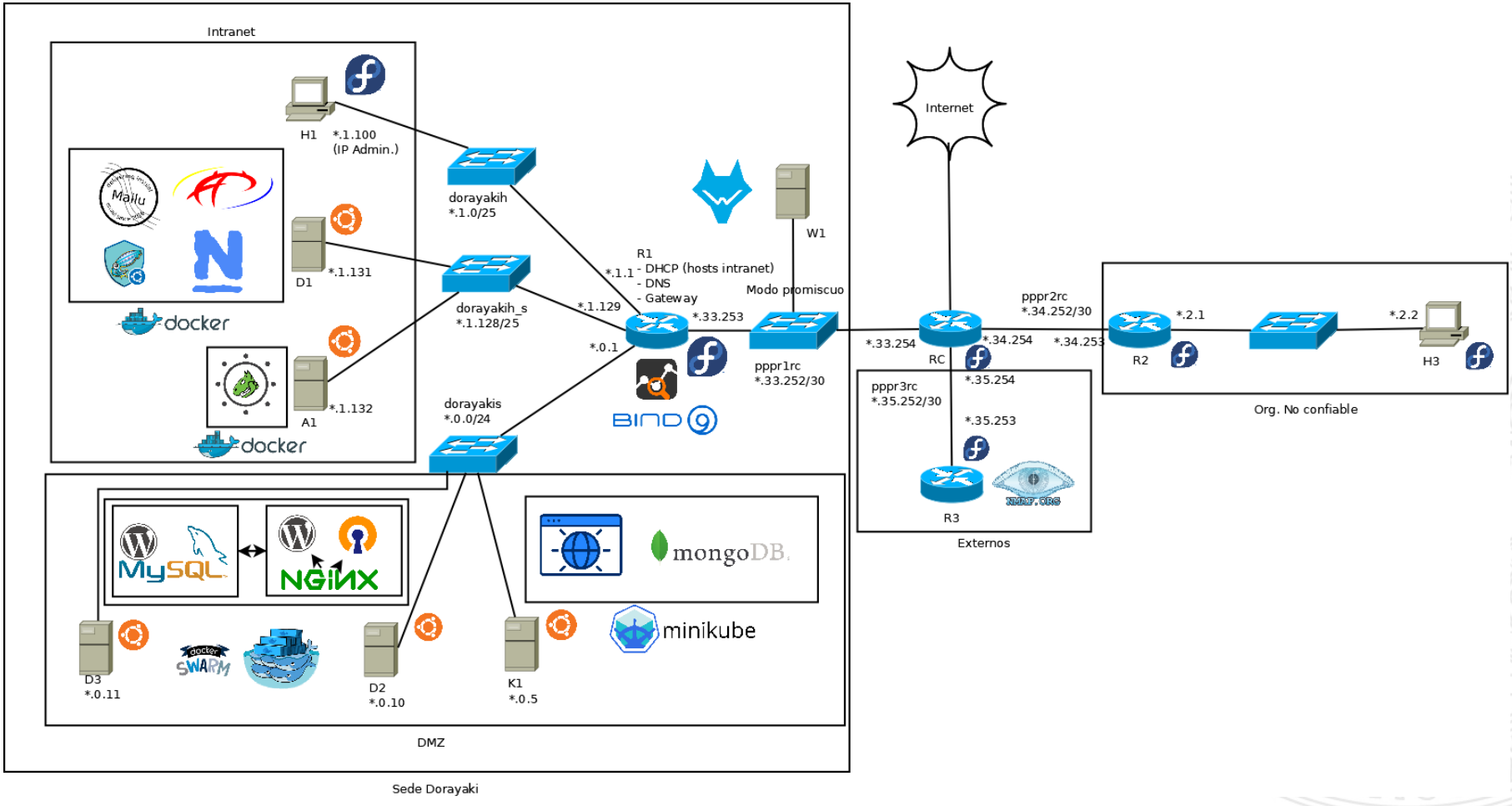
Álvaro González Moya
alvaro.gonzalezm@um.es

16/12/2024

UNIVERSIDAD DE
MURCIA

Topología de red

UNIVERSIDAD DE MURCIA



Máquinas y sus servicios

Resúmen general

UNIVERSIDAD DE MURCIA

R1:

- **DNAT** para los servicios de la DMZ (www, vpn)
- **DHCP** para los hosts de la Intranet (192.168.1.0/25)
- **Firewall** de la organización/entre zonas
- **DNS**: Interno/Externo (bind9, named)
- **Control y análisis de tráfico** entrante/saliente con *ntopng*

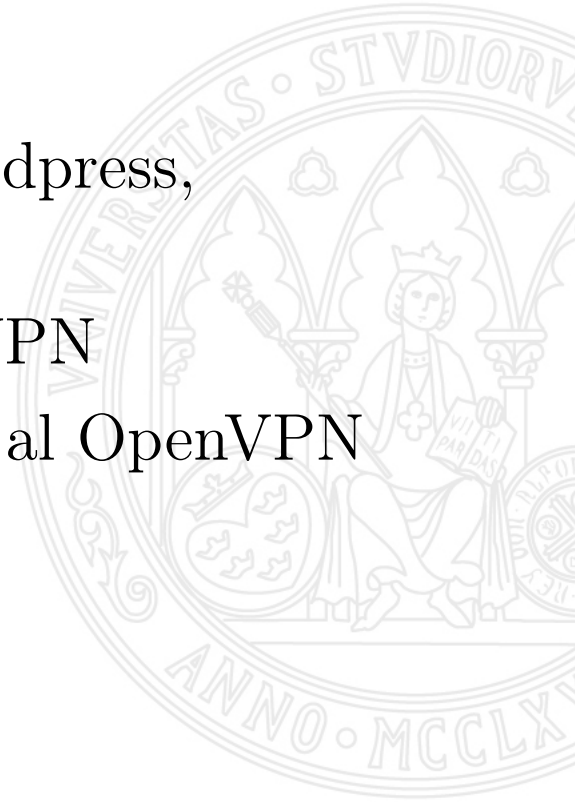
D1: Servicios internos de la organización
A1: Detección de vulnerabilidades
D2-D3: Máquinas en Swarm, servicios públicos
K1: Webapp Kubernetes

Traducción de direcciones

UNIVERSIDAD DE MURCIA

Cada router de la topología hace SNAT con su IP "pública" (.33.253)
R1 expone los servicios de D2-D3:

- 443 TCP: 443 Nginx reverse proxy (Wordpress, Dashboard usuario OpenVPN)
- 943 TCP: 943 Dashboard Admin OpenVPN
- 1194 UDP: 1194 UDP Conexiones VPN al OpenVPN AS



Filtrado de paquetes

UNIVERSIDAD DE MURCIA

- Política por defecto: **denegar**
- Fuerte filtrado DMZ->Intranet, Intranet->DMZ, con **reglas para permitir monitoreo** (Nagios)
- Servicios permitidos intranet: HTTP(s), DNS, servicios DMZ con **IP privada**
- Sólo permitir **tráfico** entrante **Internet -> DMZ** a los **servidores que hospedan cada servicio**
- Las políticas mencionadas se implementan tanto en los **hosts** como en el **router de la organización**
- Bloqueando los paquetes ICMP *time exceeded*, los **routers** de la topología **no se exponen en un *traceroute***

Servicios desplegados

Servicios internos

UNIVERSIDAD DE MURCIA

Servicios dockerizados:

- **Nagios** para la monitorización de las maquinas
- **Mailu** como solución de correo basada en contenedores
- **Squid** como proxy web (no transparente)
- **ProFTPd** como agente FTP
- **OpenVAS** como herramienta de búsqueda de vulnerabilidades

Servicios tradicionales:

- **Ntop** para la monitorización y rendimiento de la red
- **Bind9/Named** como DNS interno/externo

Servicios desplegados

Servicios externos

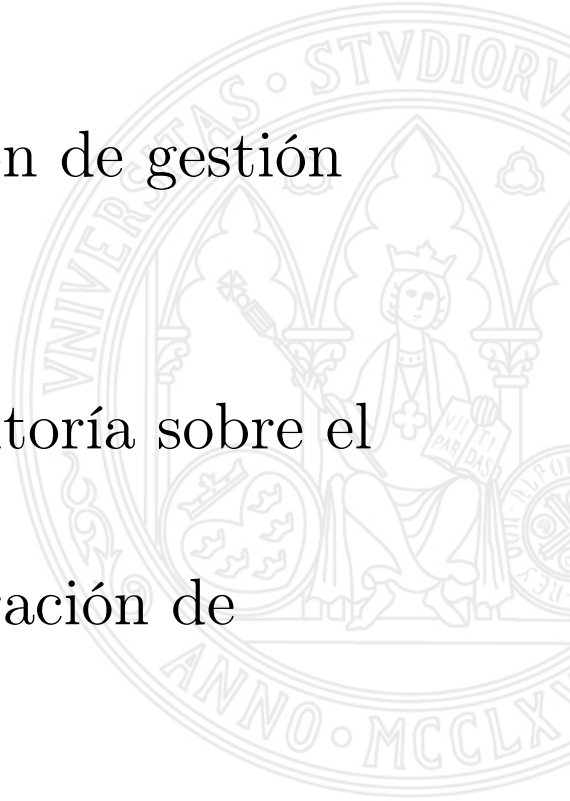
UNIVERSIDAD DE MURCIA

Servicios dockerizados:

- **Wordpress** como página web/blog de la empresa
- **Nginx** como reverse proxy
- **OpenVPN Acess Server** como solución de gestión de conexiones VPN

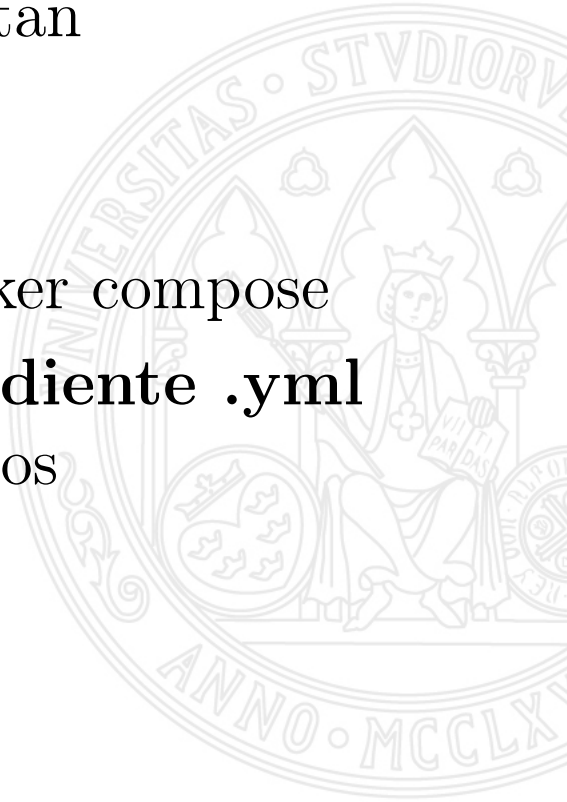
Servicios tradicionales:

- **Nmap** como herramienta básica de auditoría sobre el *gateway* de la empresa
- **Wazuh** (modo promiscuo) para la generación de alertas de posibles ataques

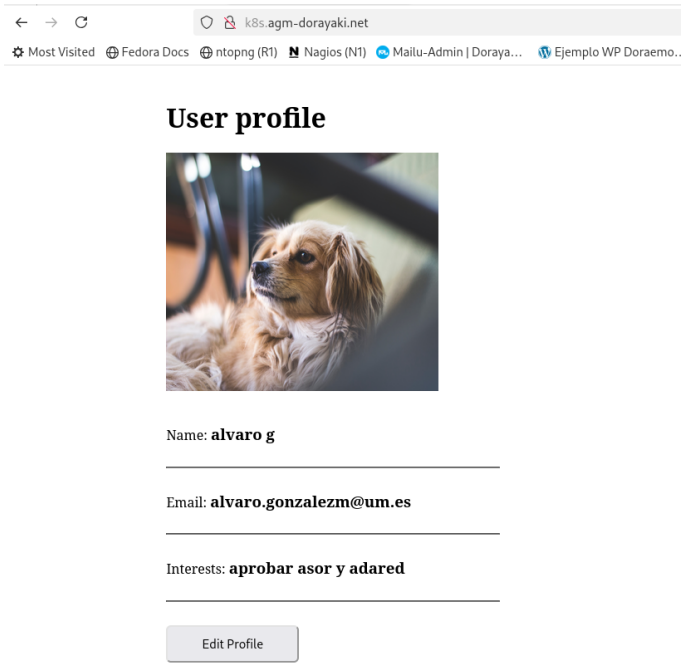


La mayoría de servicios de la organización estan desplegados sobre **contenedores Docker**:

- D1: docker compose (un solo nodo)
- D2-D3: docker swarm (multi-nodo), docker compose
- Todos los servicios tienen **su correspondiente .yml** y **ficheros de configuración** modificados



Minikube + Regla Port forward (k8s.agm-dorayaki.net)

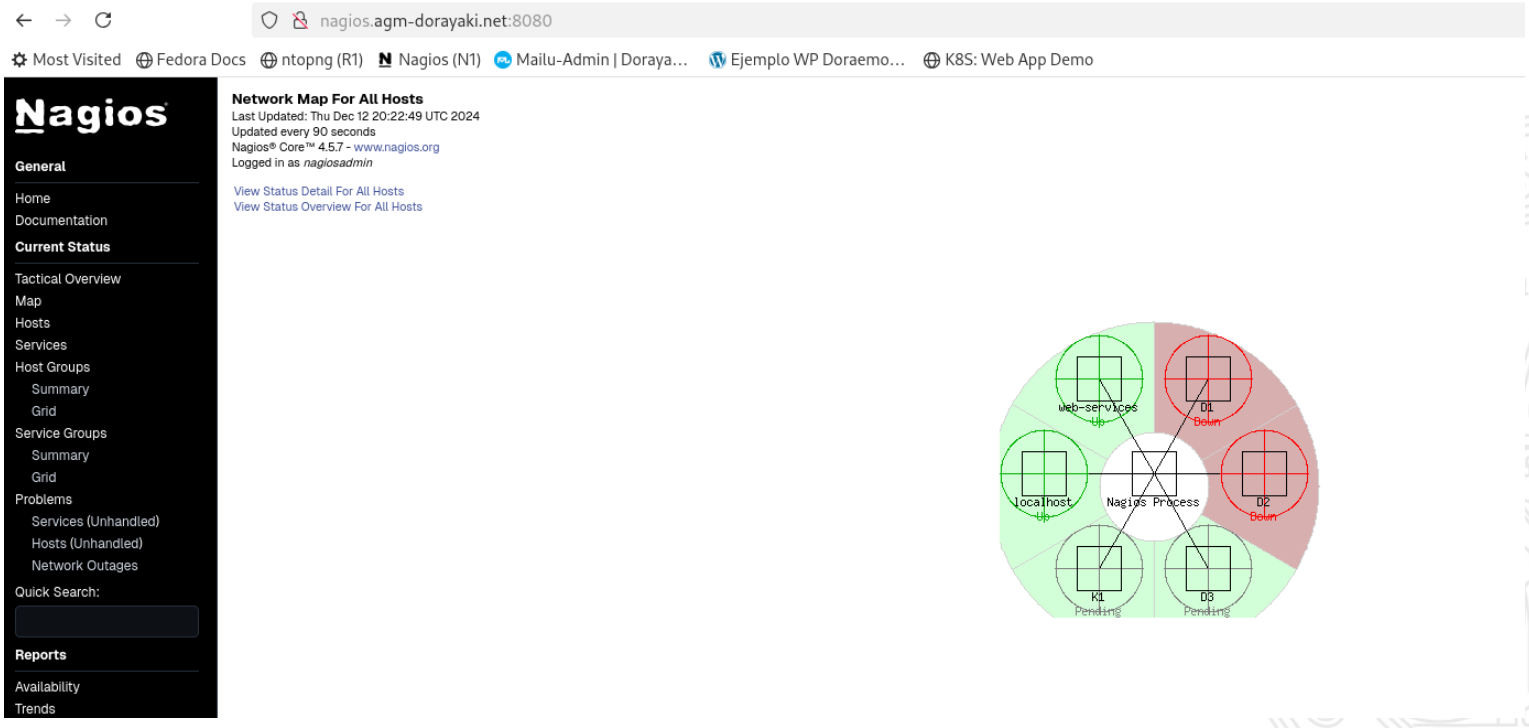


- Problemas con kubeadm: falta de recursos (RAM)
- Solución: **k3s**

Monitorización/control disponibilidad

Nagios

Docker, D1 (Intranet), nagios.agm-dorayaki.net(8080)



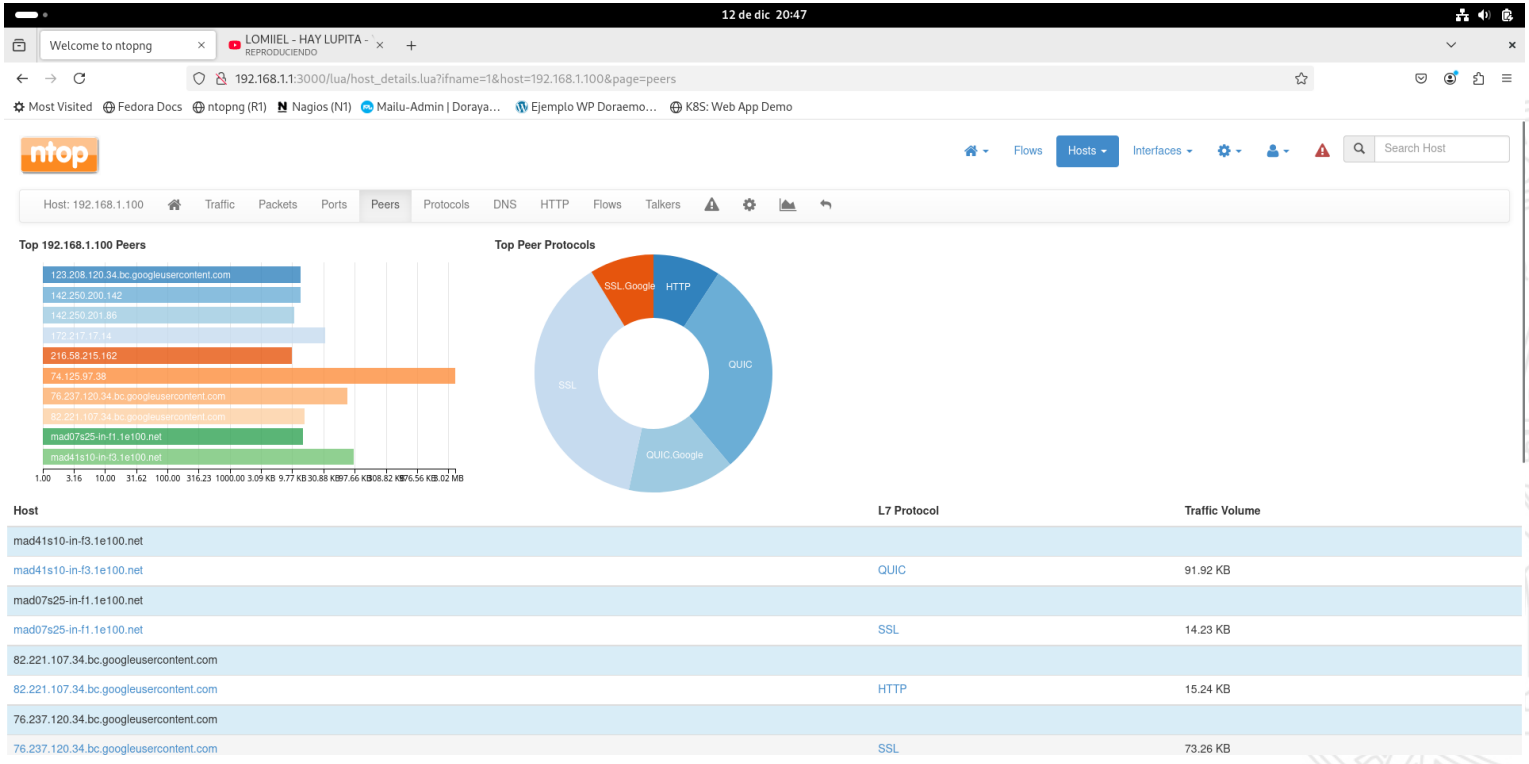
Fichero de configuración (hosts/servicios):
docker/intranet/nagios.cfg (repositorio)

Control de uso de la red

Ntop-ng

UNIVERSIDAD DE MURCIA

ntopng-blake, R1 (acceso Intranet), IP Gateway



Generación de alertas, análisis de hosts...

Servicios públicos básicos

DNS

UNIVERSIDAD DE MURCIA

- dns.agm-dorayaki.net
- Named: parte de bind9
- Dos zonas: external, internal. Resuelven IP's y registros A diferentes
- **external**: ns1, www, vpn
- **internal**: ns1, www, vpn, smtp, pop, mail (+MX), proxy, ftp, openvas, nagios, k8s

```
view "internal" {
        match-clients { 192.168.1.0/24; };

        zone "agm-dorayaki.net" {
                type master;
                file "/var/named/agm-dorayaki.net.zone.internal";
        };
        include "/etc/named.rfc1912.zones";
        include "/etc/named.root.key";
};

view  "exteral" {
        match-clients { any; };

        zone "agm-dorayaki.net" {
                type master;
                file "/var/named/agm-dorayaki.net.zone.external";
        };
        include "/etc/named.rfc1912.zones";
        include "/etc/named.root.key";
};
```

Servicios públicos básicos

Web

UNIVERSIDAD DE MURCIA

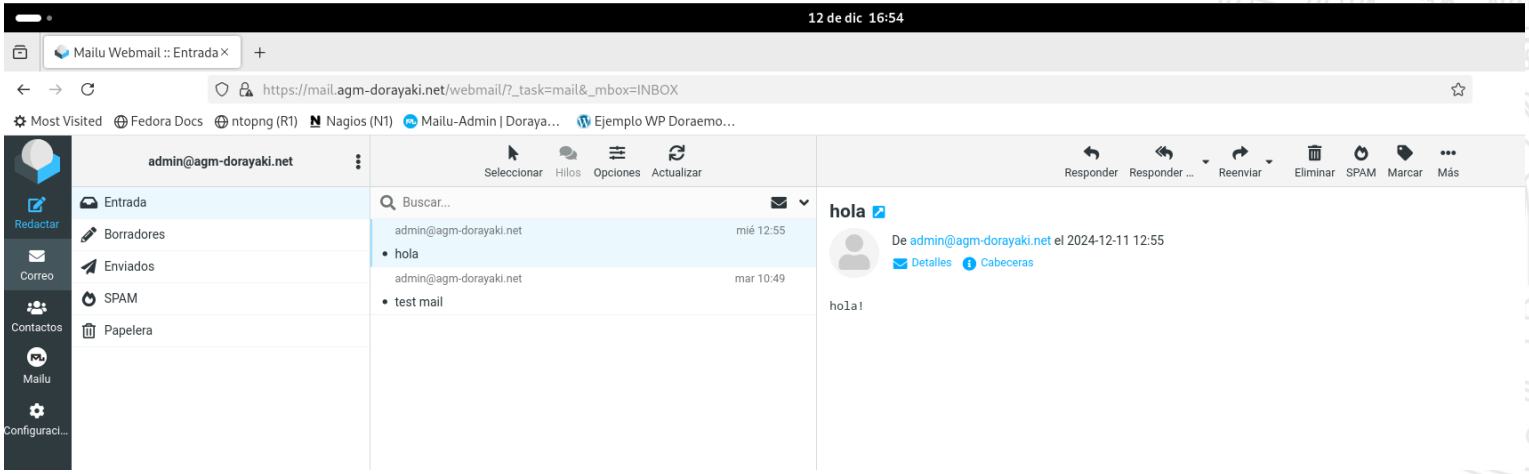
- www.agm-dorayaki.net (accesible publicamente)
- **Wordpress** (Apache) + **SQL**
- **Swarm**: alta disponibilidad, escalado automático

Servicios públicos básicos

Correo electrónico

UNIVERSIDAD DE MURCIA

- **Mailu**: solución desplegada sobre contenedores
- mail/pop3/smtp.agm-dorayaki.net
- Fácil configuración: servicio generación ficheros .yml y .env
- Correo tradicional (POP3, SMTP) + **Webmail**

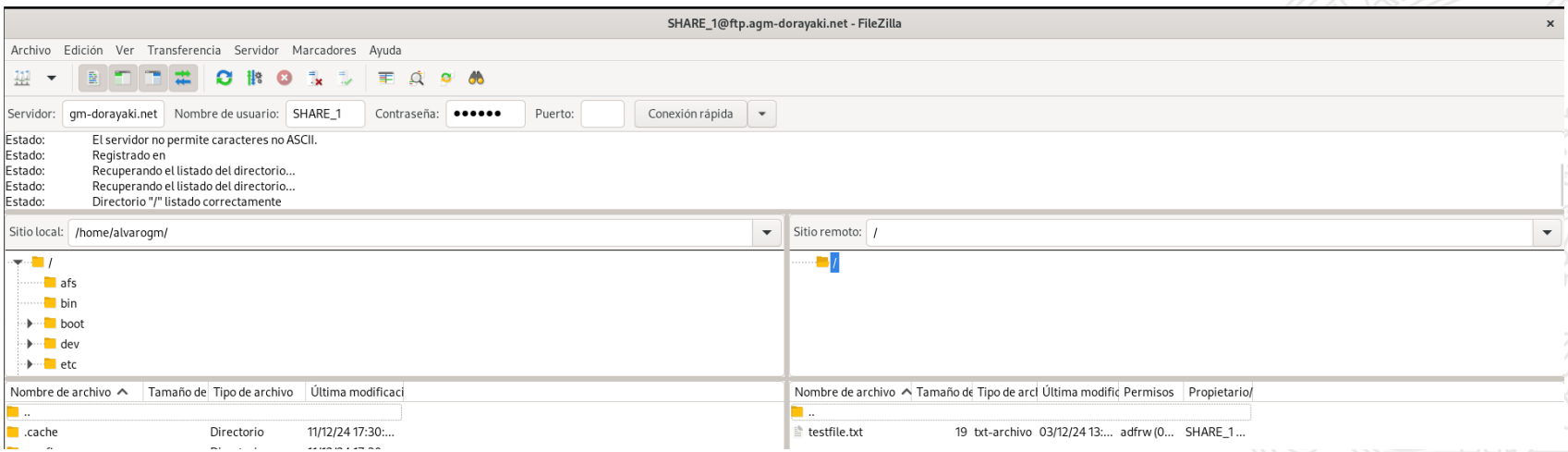


Servicios públicos básicos

FTP

UNIVERSIDAD DE MURCIA

- **Proftpd**: contenedor Docker
- 5 usuarios (shares) desplegados (test)

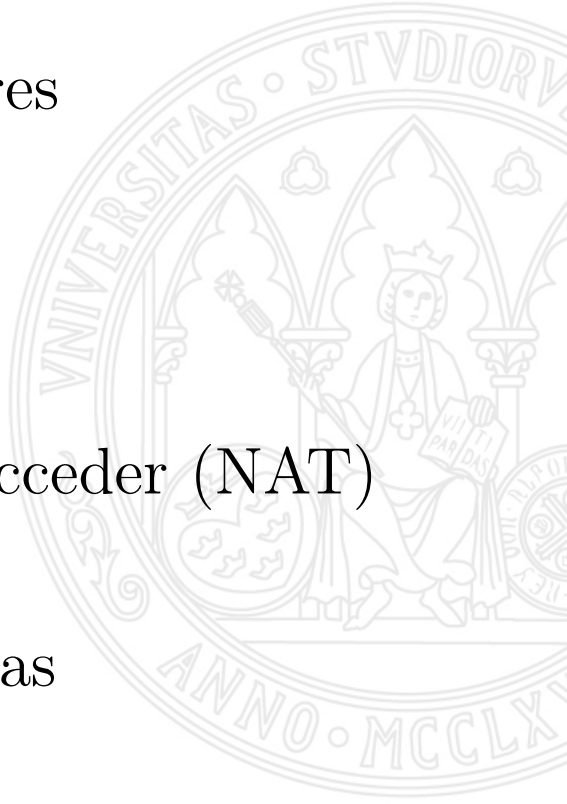


Acceso seguro a la sede de la empresa

OpenVPN AS

UNIVERSIDAD DE MURCIA

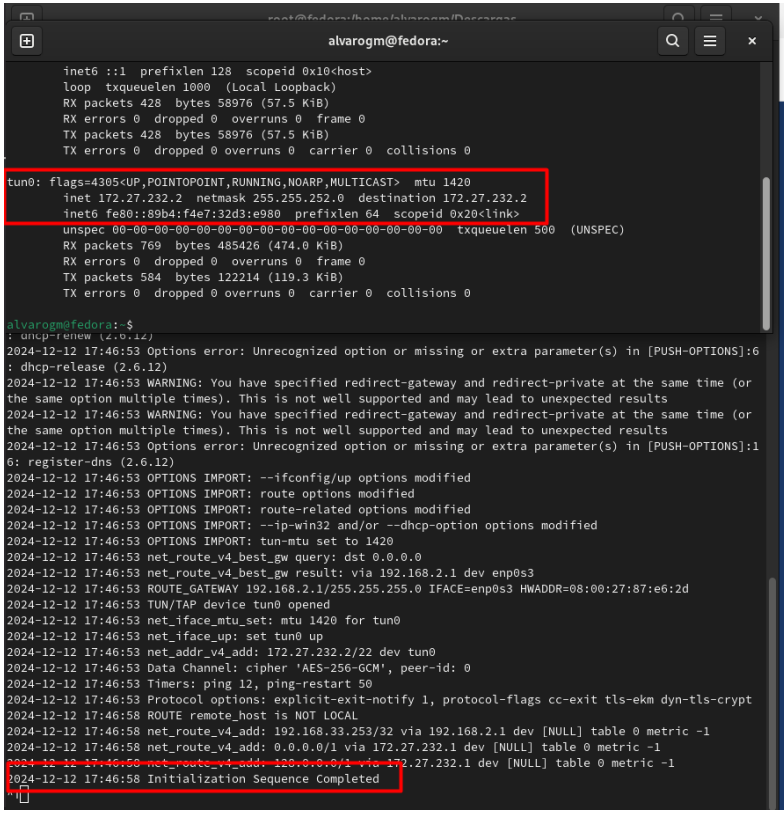
- vpn.agm-dorayaki.net
- Solución **administrada de OpenVPN**
- Desplegable y escalable sobre contenedores
- Autenticación de usuarios sencilla
- Permisos integrados
- Descarga de perfil de conexión
- Definición de subredes a las que puede acceder (NAT)
- Layer 3 (Capa de red)
- Versión gratuita: 2 conexiones simultáneas

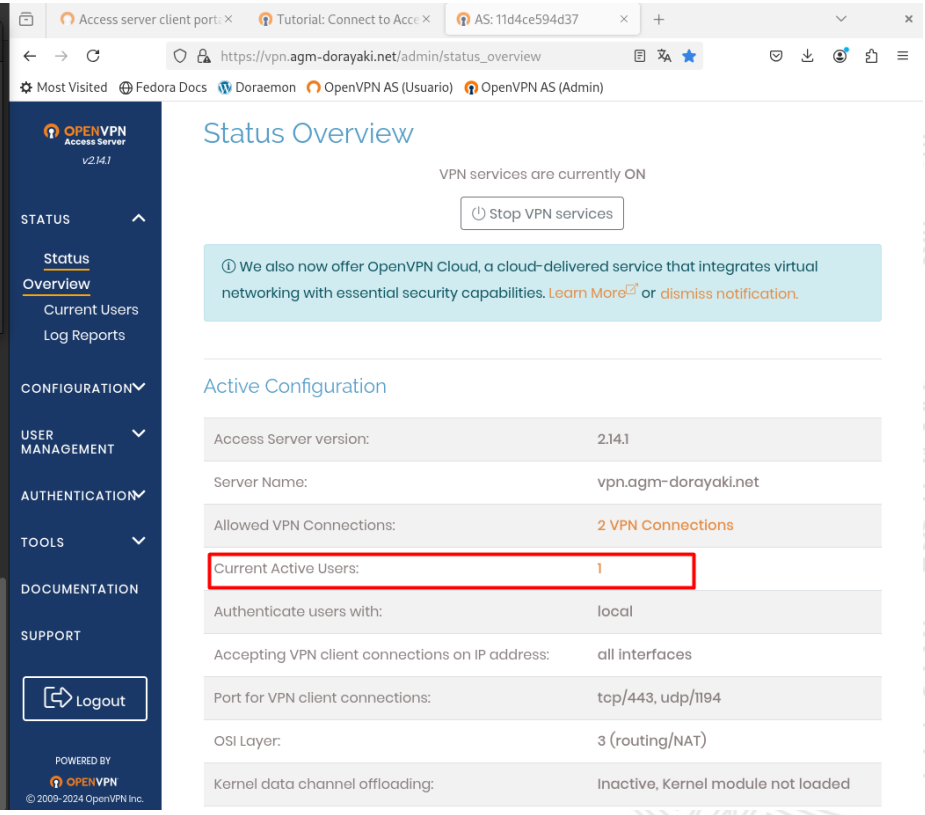


Acceso seguro a la sede de la empresa

Ejemplo de conexión desde Org. No conf.

UNIVERSIDAD DE MURCIA



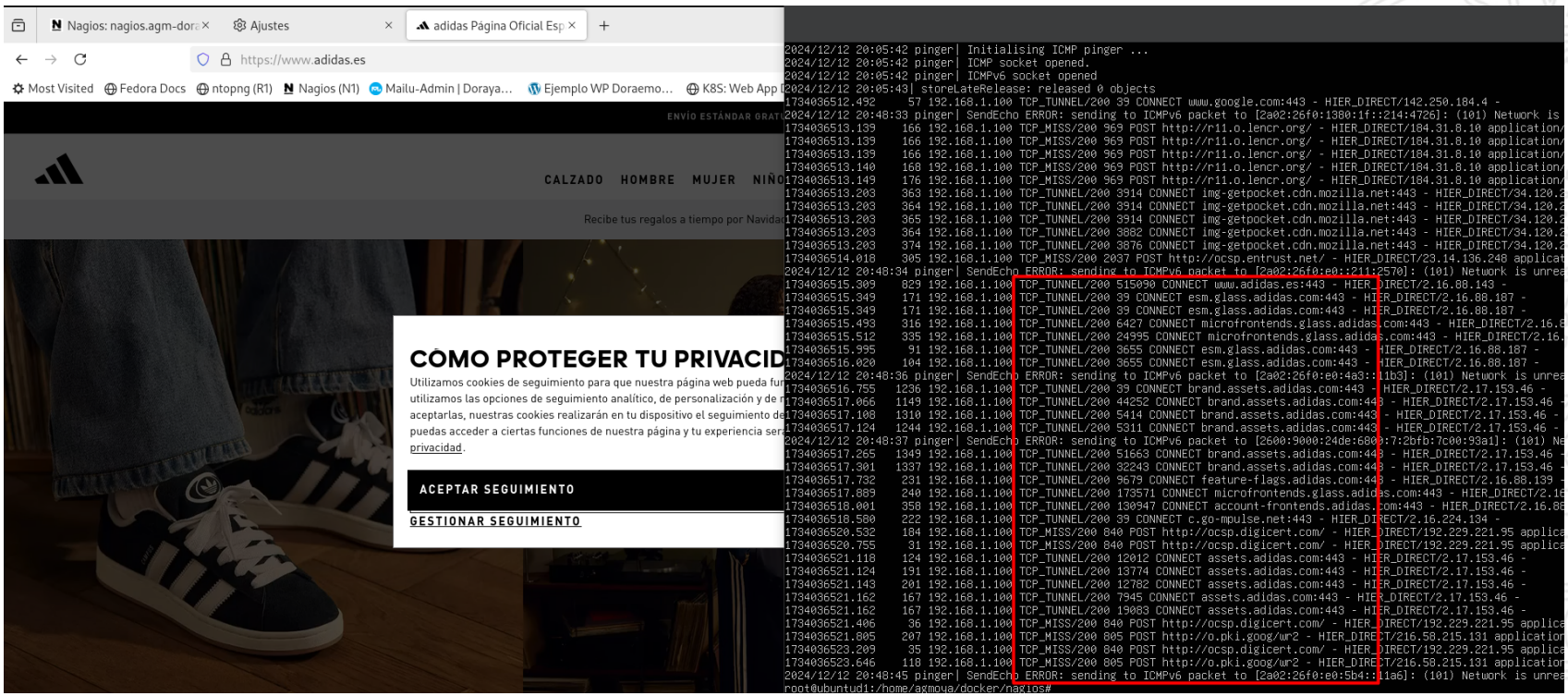


Control uso web empleados

Proxy web: Squid

UNIVERSIDAD DE MURCIA

- proxy.agm-dorayaki.net
- **Sarg** (Squid Analysis Report Generator): generación de informes



Basado en **3 herramientas**:

- **Nmap**: escaneo de puertos/versión servicios. Nos da **inventario**
- **OpenVAS**: identificación de vulnerabilidades sobre servicios identificados anteriormente
- **Wazuh**: solución más moderna que Snort (utiliza Suricata), generación de alertas/intrusos.

Auditoría de seguridad

Nmap

UNIVERSIDAD DE MURCIA

- Ejecutar contra toda máquina del proyecto
- Asegurarse de que el mínimo número de servicios están expuestos
- Ejecución de prueba: sobre gateway a Internet de la org. (**R1**)

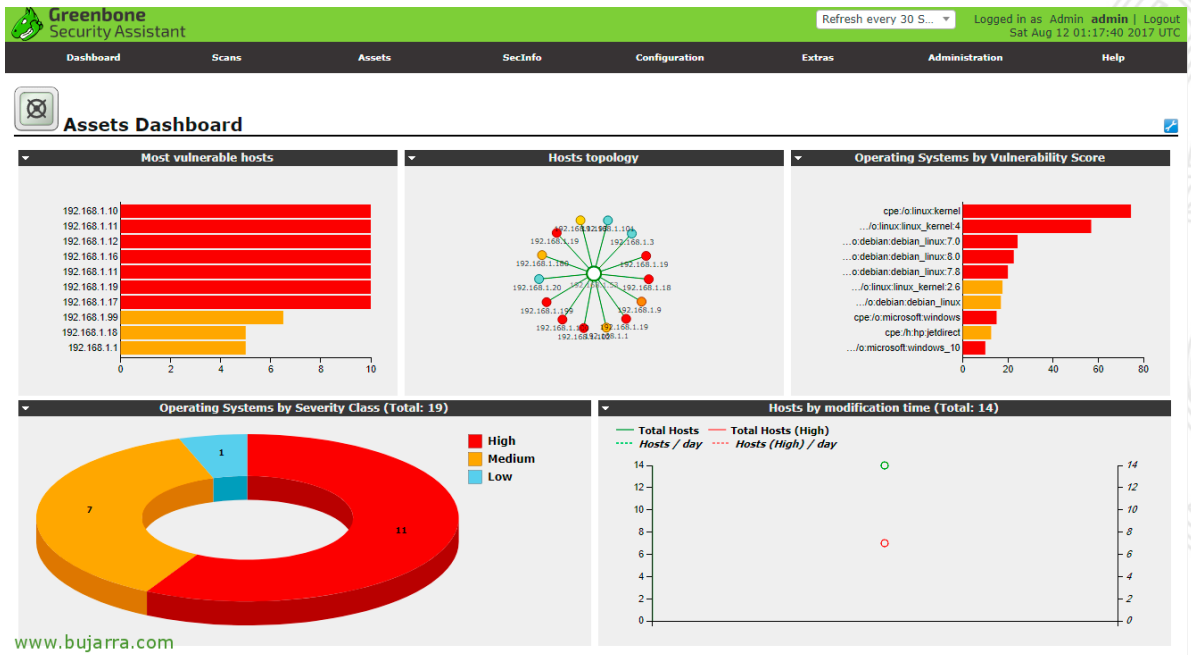
```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-12-12 18:18 CET
Nmap scan report for 192.168.33.253
Host is up (0.00033s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 9.6 (protocol 2.0)
53/tcp   open  domain          NLnet Labs NSD
443/tcp  open  ssl/http        nginx 1.27.3
3000/tcp open  http            Mongoose httpd
9090/tcp open  ssl/zeus-admin?
```

Auditoría de seguridad

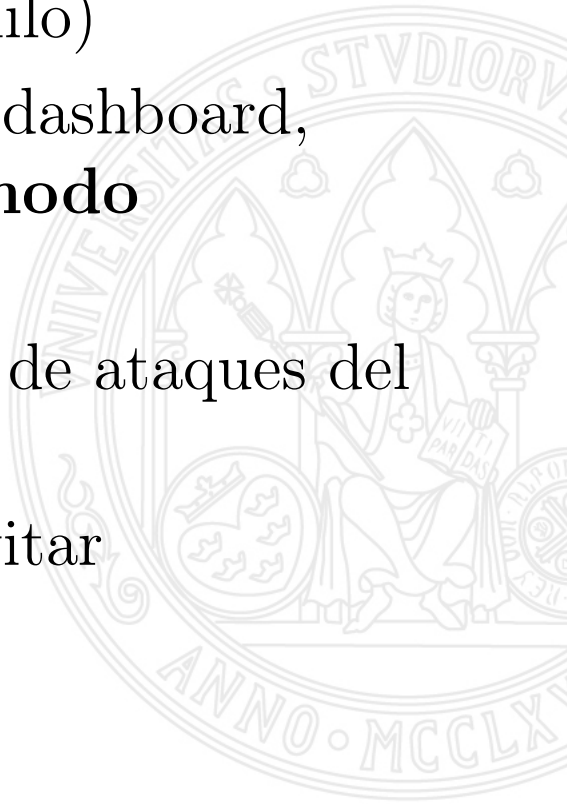
OpenVAS (GreenBone)

UNIVERSIDAD DE MURCIA

- openvas.agm-dorayaki.net
- Máquina separada, desplegado sobre contenedores
- Encontrar vulnerabilidades sobre servicios encontrados con Nmap



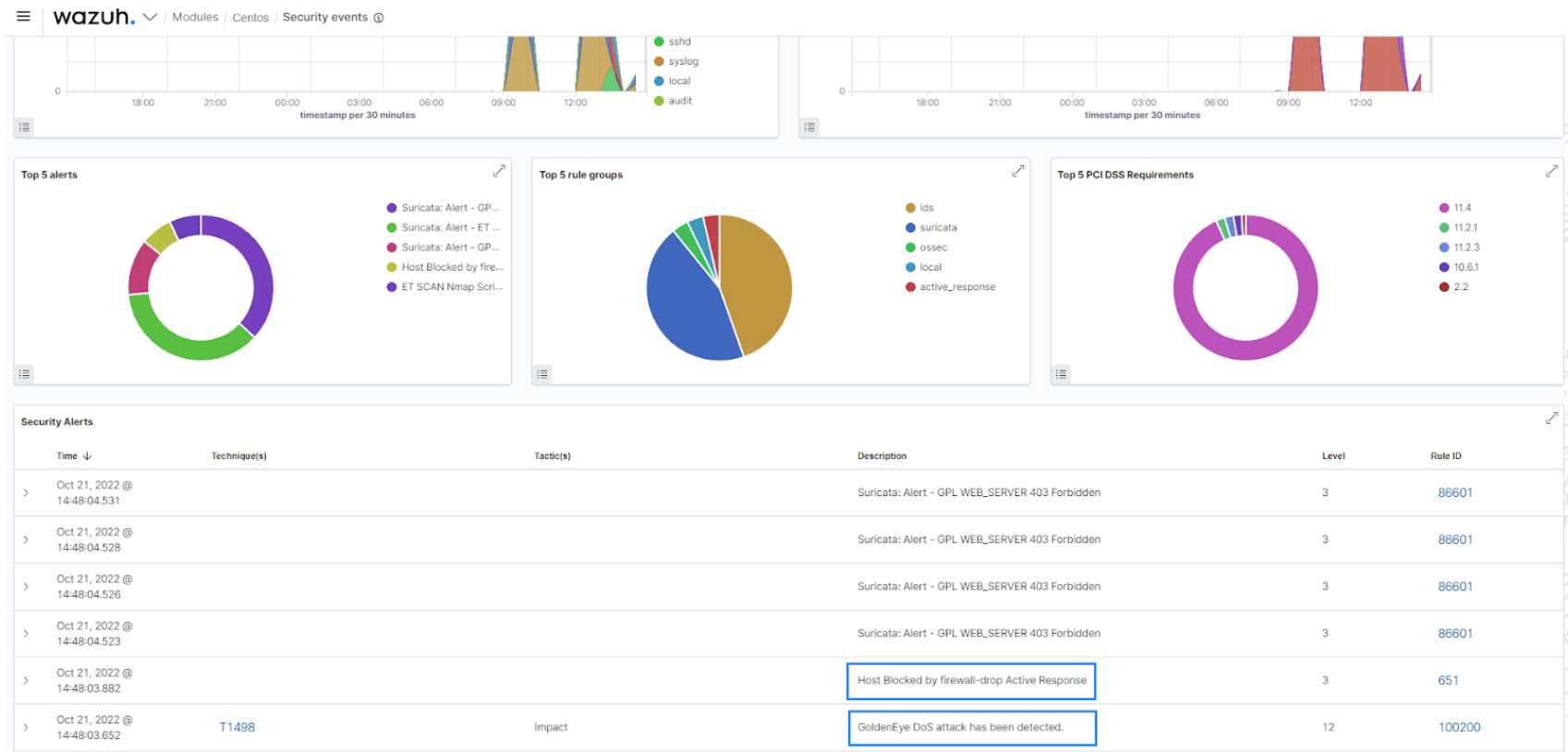
- También tiene vulnerability detection, pero lo utilizaremos por **Suricata** (Snort multihilo)
- Imagen linux personalizada: programas, dashboard, reglas firewall... conectada a switch en **modo promisuco**
- Sobre gateway: **generación de alertas** de ataques del exterior
- Sobre DMZ: **detección de intrusos**, evitar movimientos laterales



Auditoría de seguridad

Wazuh

UNIVERSIDAD DE MURCIA



Código fuente

UNIVERSIDAD DE MURCIA

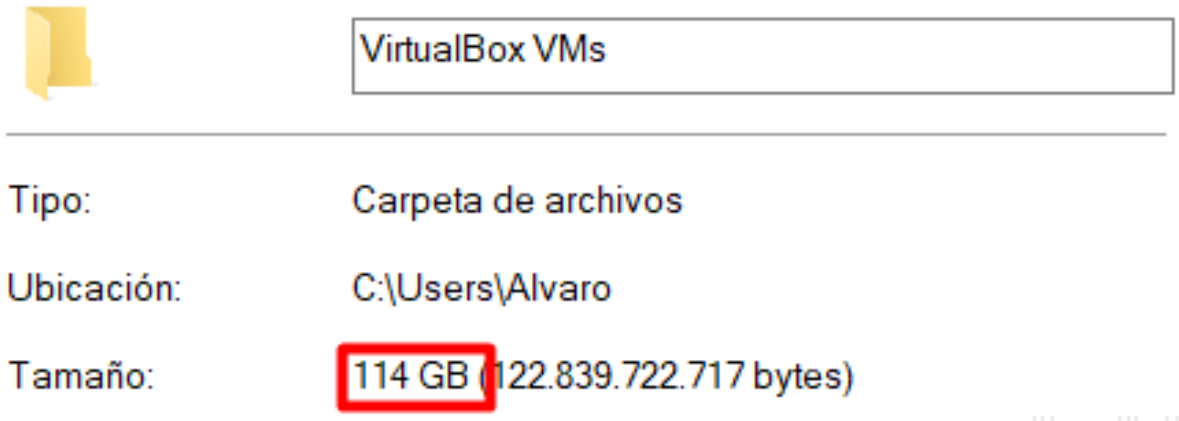
Enlace al repositorio

- Scripts de configuración de las máquinas (<nombre_maquina.sh)
- **Comprobar nombre script con máquina desplegada**: existen ficheros de servidores antiguos
- Docker compose, k8s
- Ficheros de configuración de servicios

Agradecimientos

UNIVERSIDAD DE MURCIA

- A mi SSD



- **Joaquín Molina** (kinomakino) por sus consejos sobre el plan de auditoría