Índice:

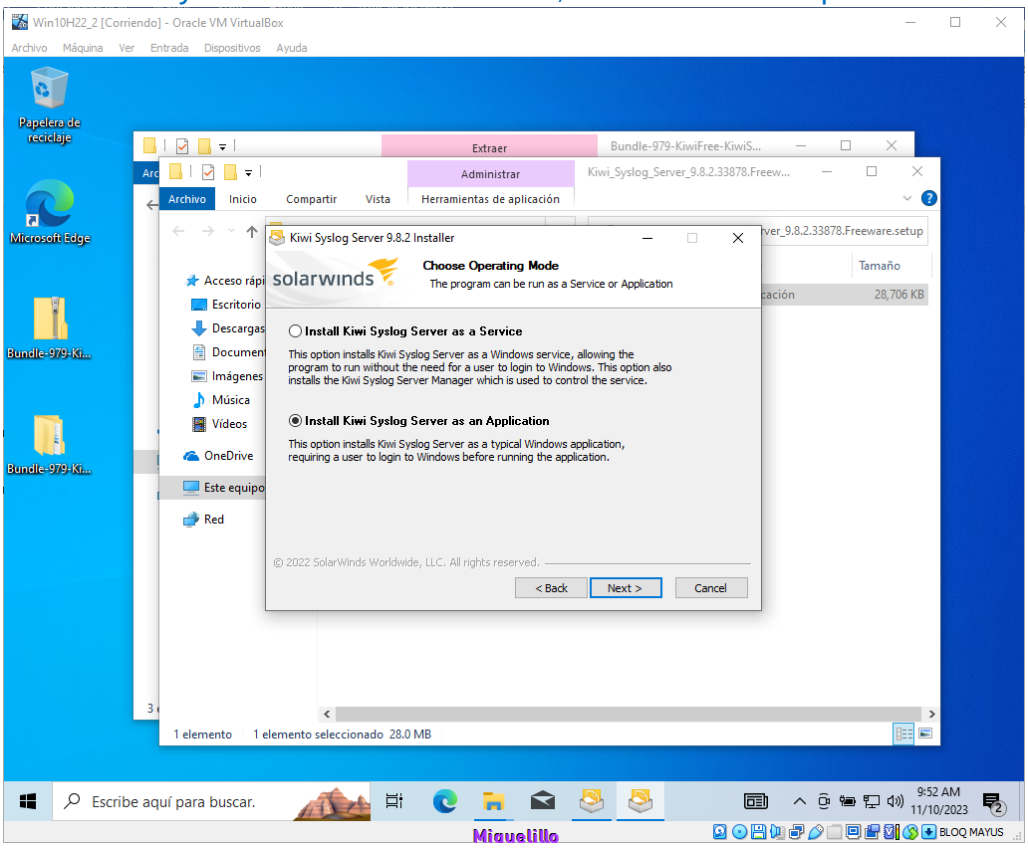
Ejercicio 1

a) Descarga e instala software que monitorice y supervise el tráfico de la red y realiza filtrado de servicios de red : Syslog, SNMP y NetFlow.

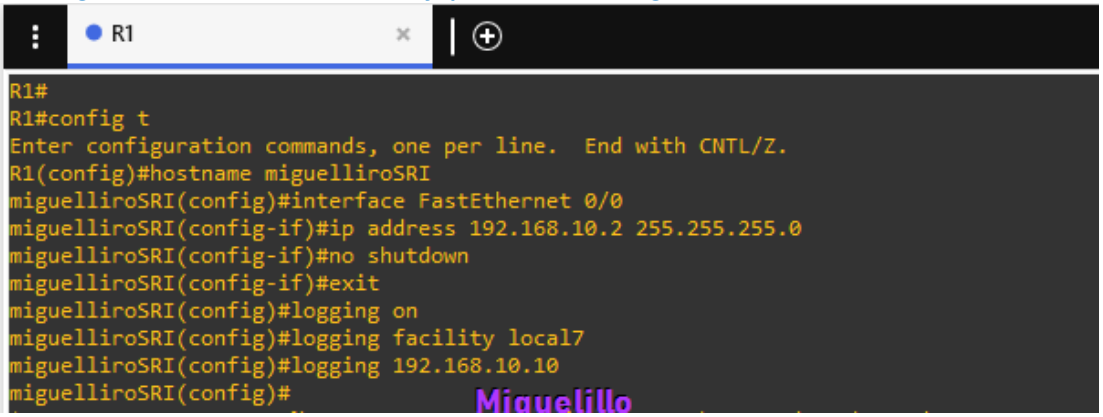
Solución:

Escenario

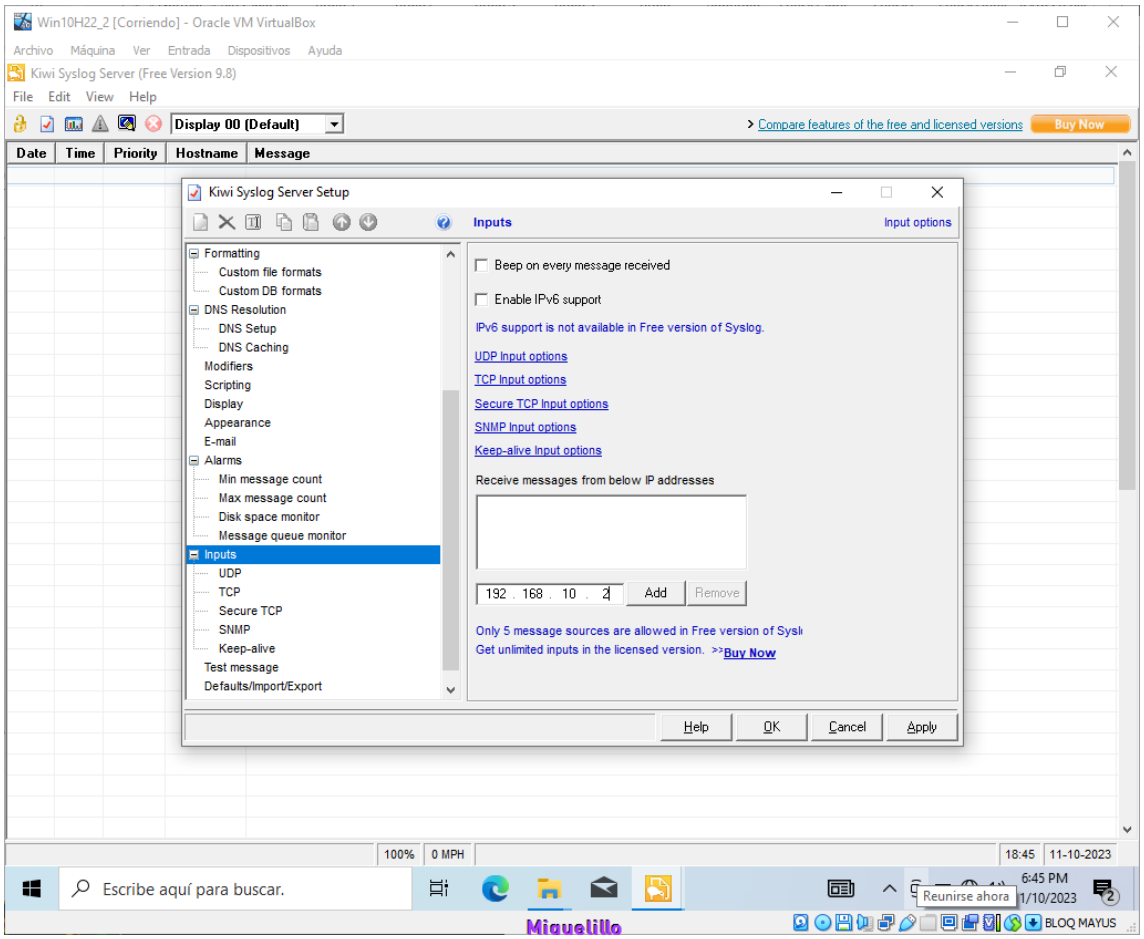
SYSLOG voy a utilizar el software **kiwi**, lo instaré como Aplicación



Configuramos la **IP** del router y para enviar registros al servidor SYSLOG

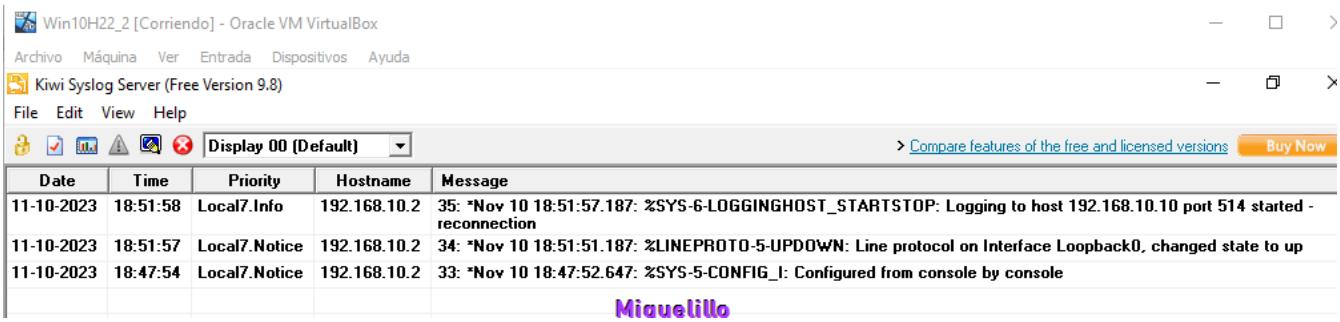


Vamos al kiwi a **File→Setup→Inputs** e introducimos la **IP** del router

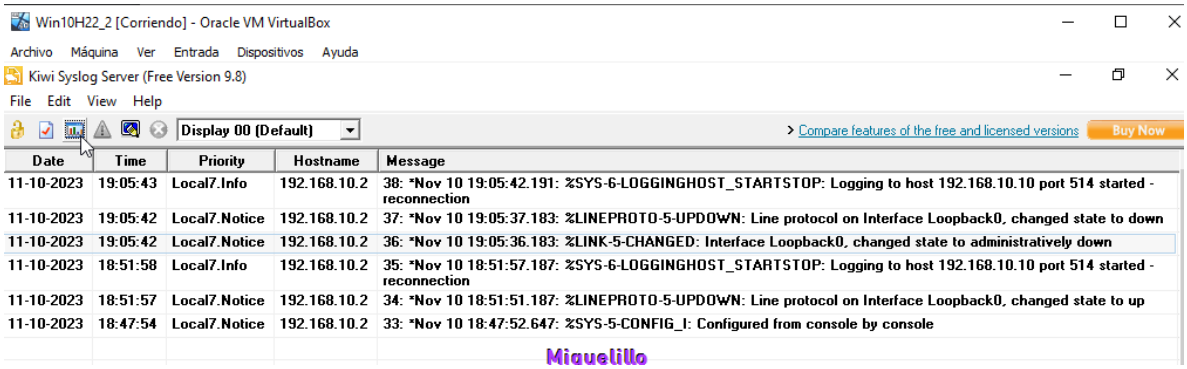


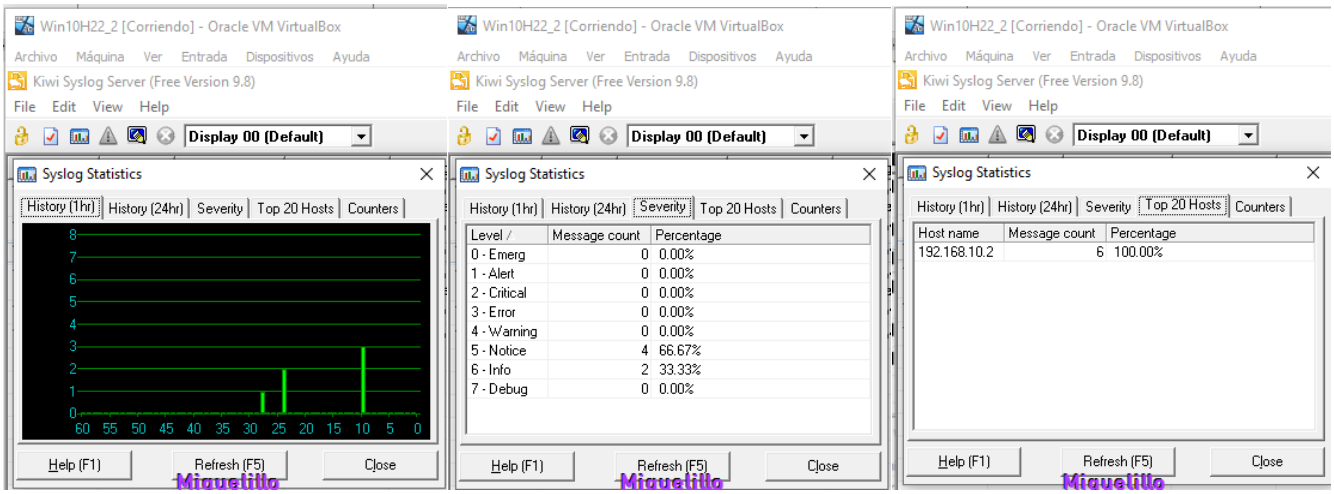
Generamos tráfico para ver registros

Podemos ver cómo ha registrado el tráfico y los cambios en el router.

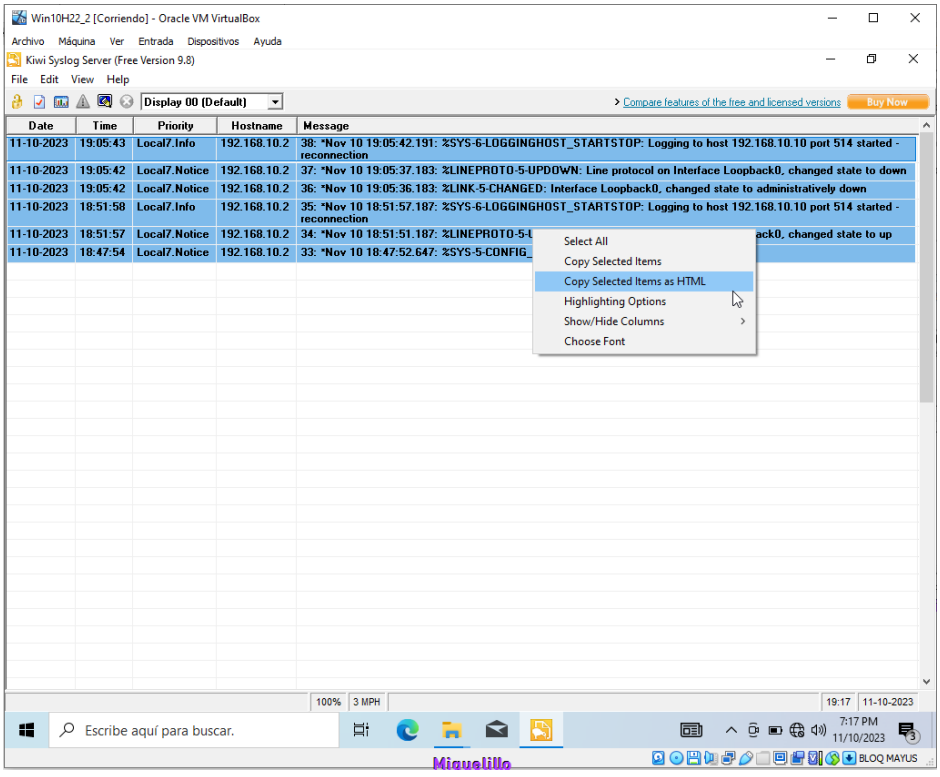


Si cicamos en **View Static** podemos verlo en formato de gráfica los registros también las estadísticas

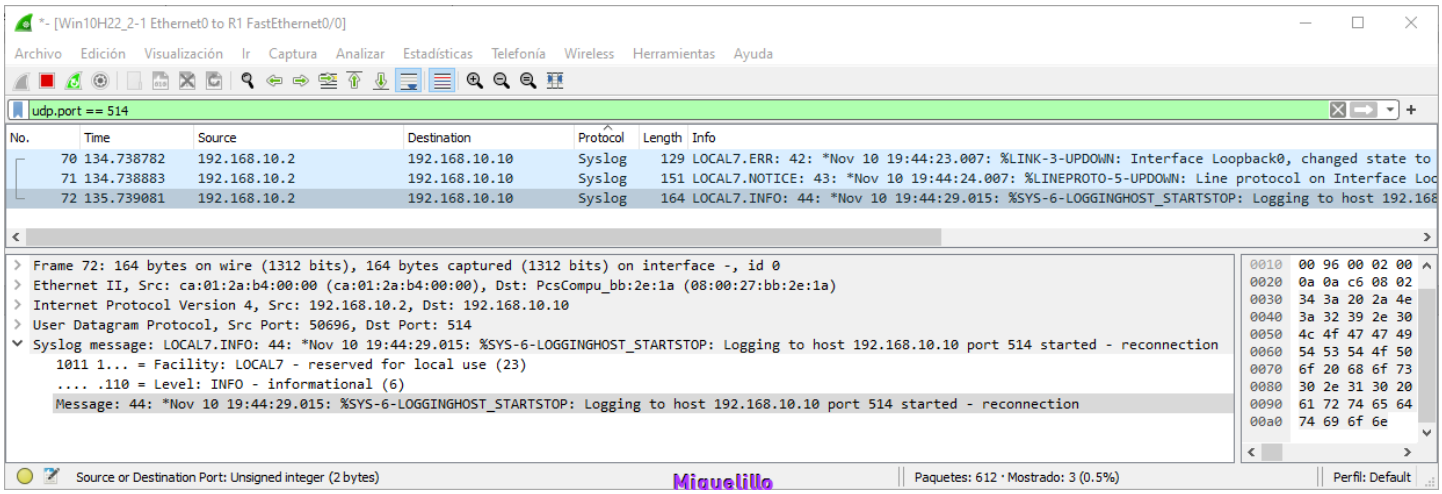




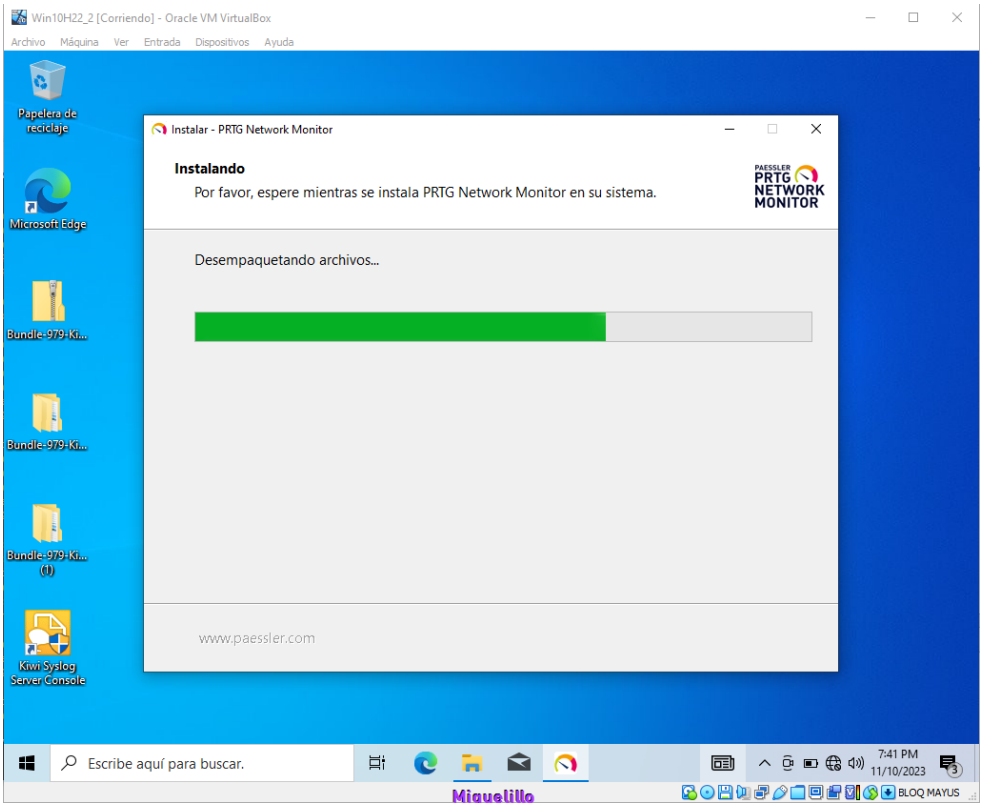
En caso de querer verlo en formato HTML seleccionamos la celdas **Clic derecho→ Copy Selected Items as HTML**



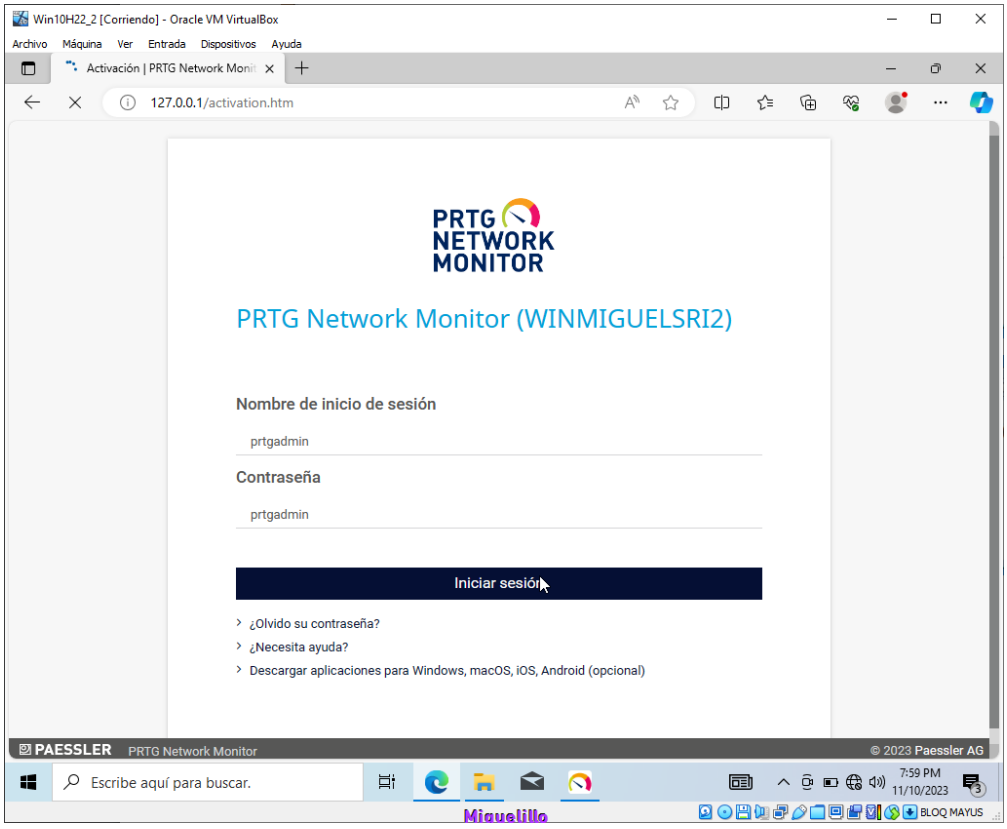
Con wireshark podemos capturar el tráfico Syslog que informa por el puerto UDP 514



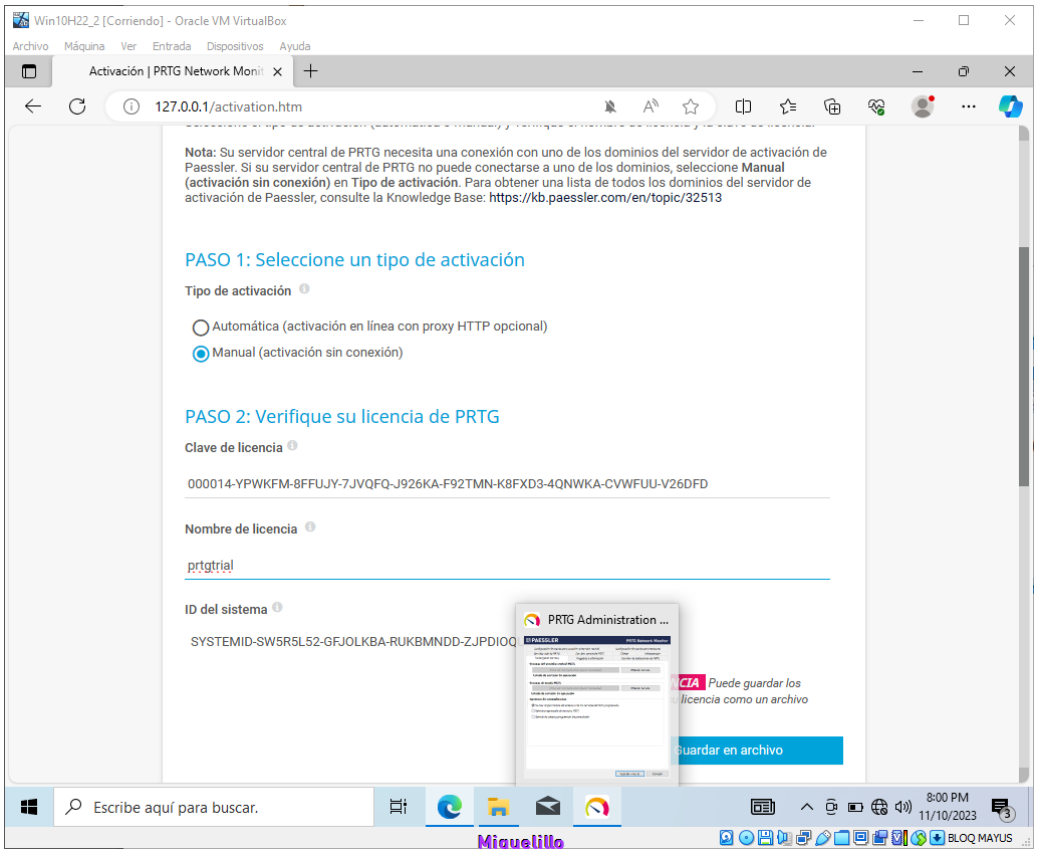
SNMP voy a usar PRTG



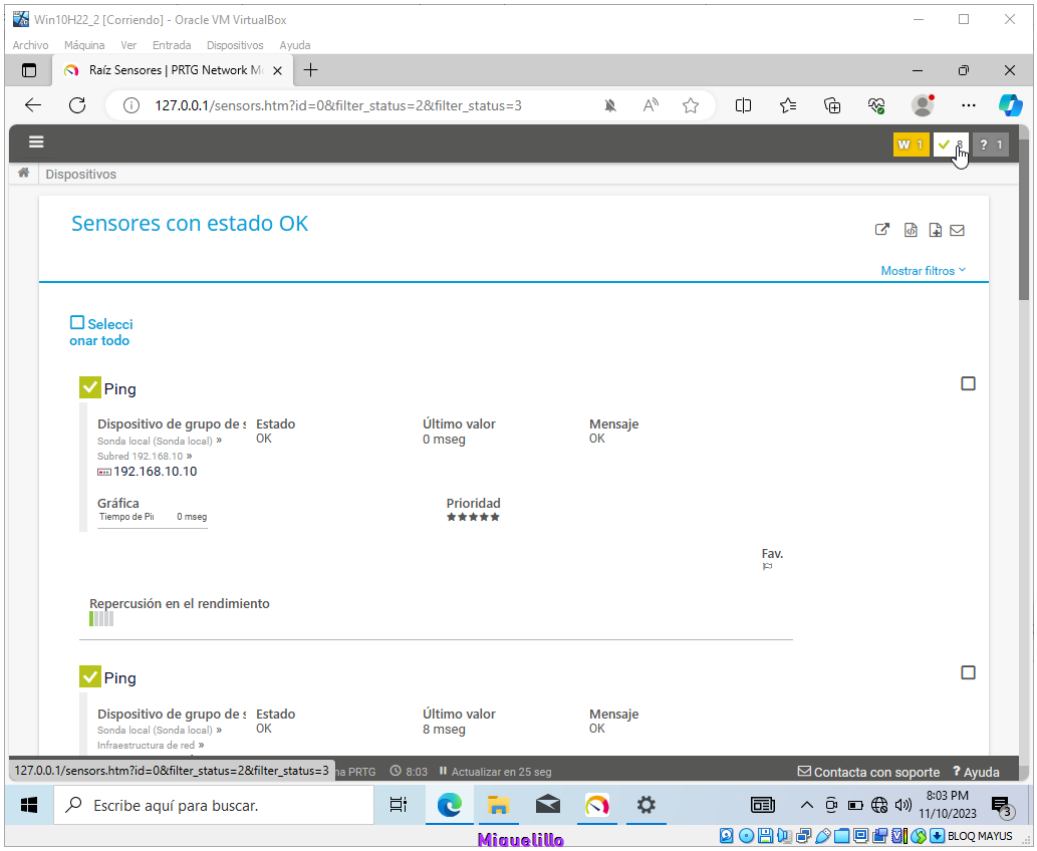
Iniciamos sesión en el launcher del navegador



Activo la licencia

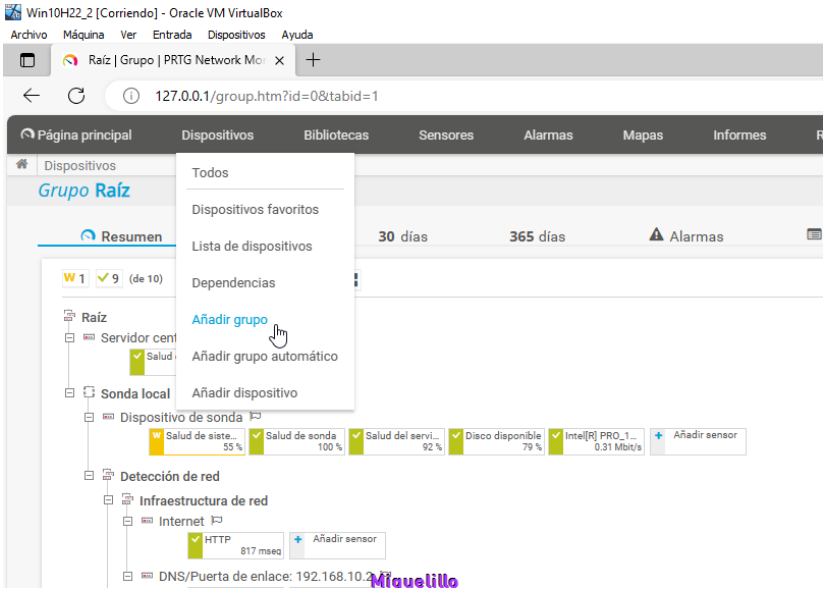


Una vez activada la licencia

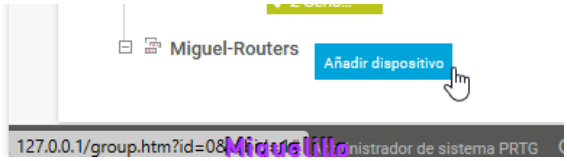


Configuramos el router para que se cominique con el servidor snmp

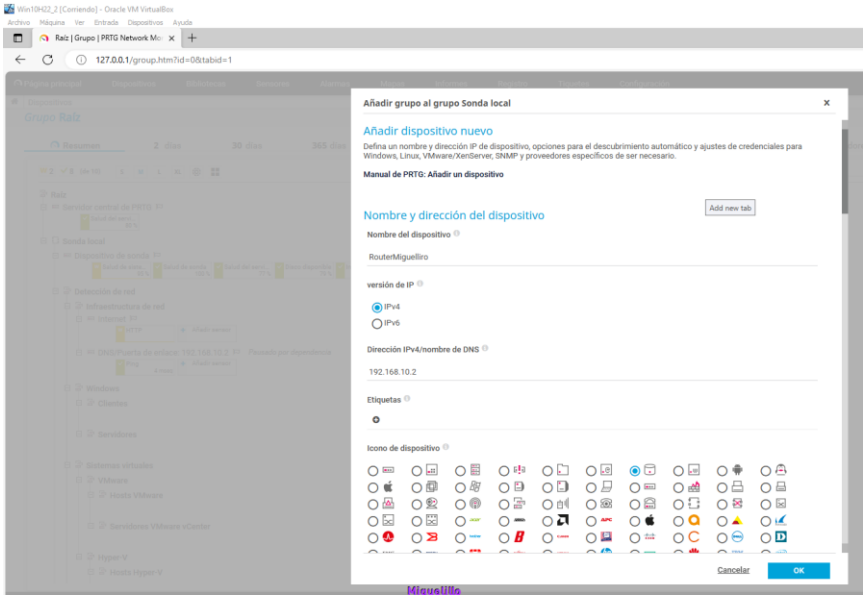
Vamos a **Dispositivos→ Añadir Grupo** y creamos un grupo



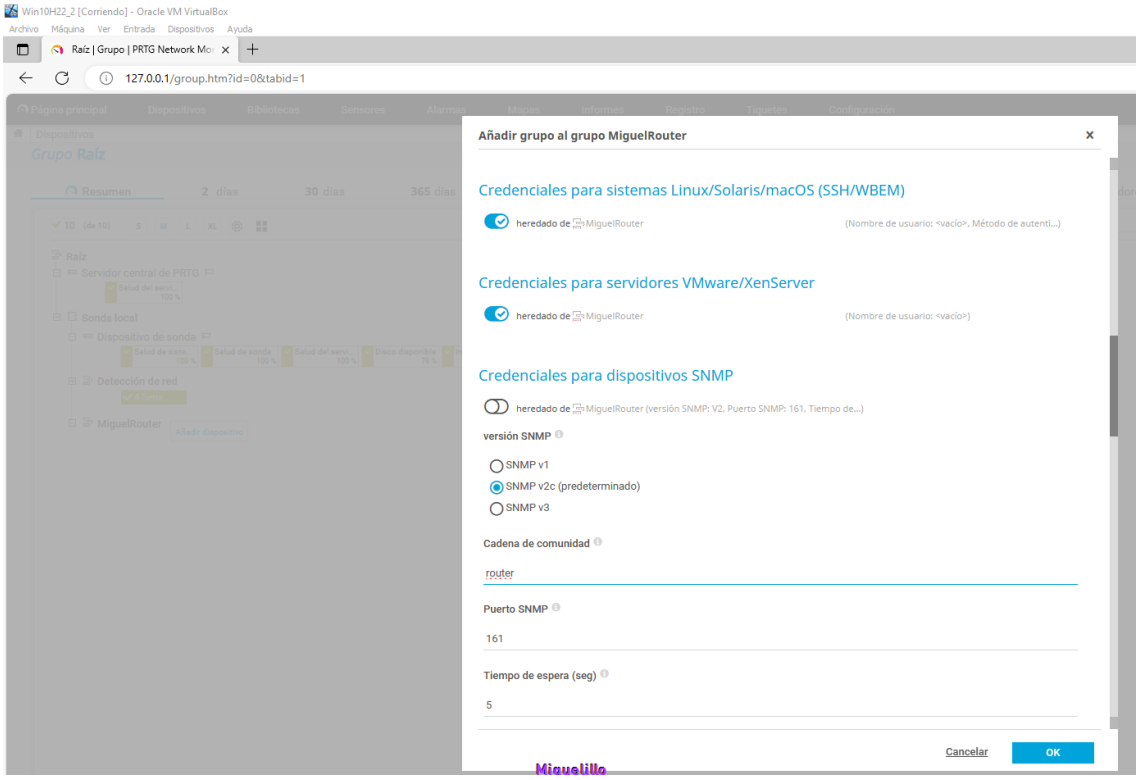
Vamos a dispositivos a los grupos que hemos hecho y clicamos en **Añadir dispositivo**



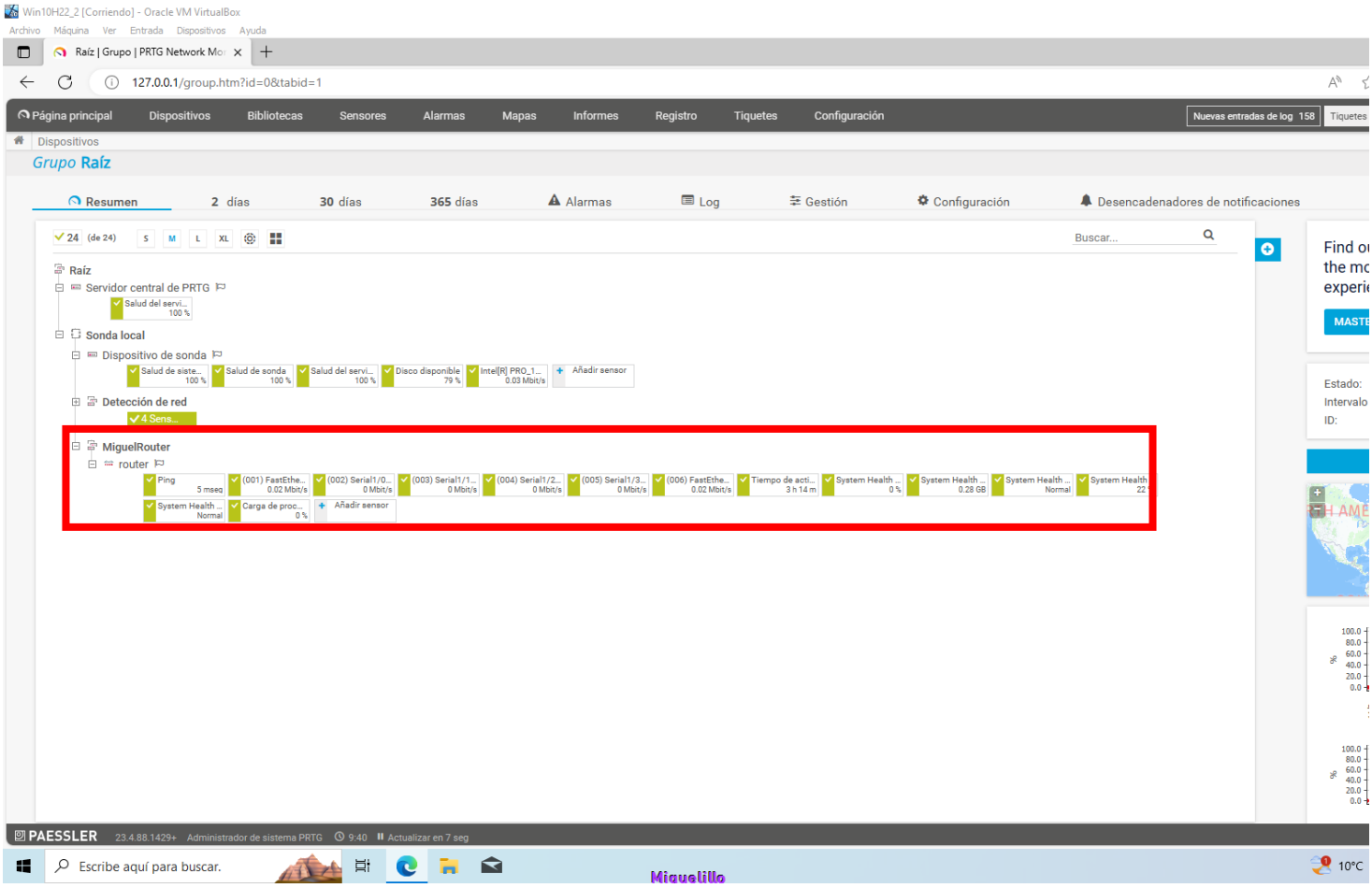
Introducimos IP, nombre y un icono si queremos para reconocerlo



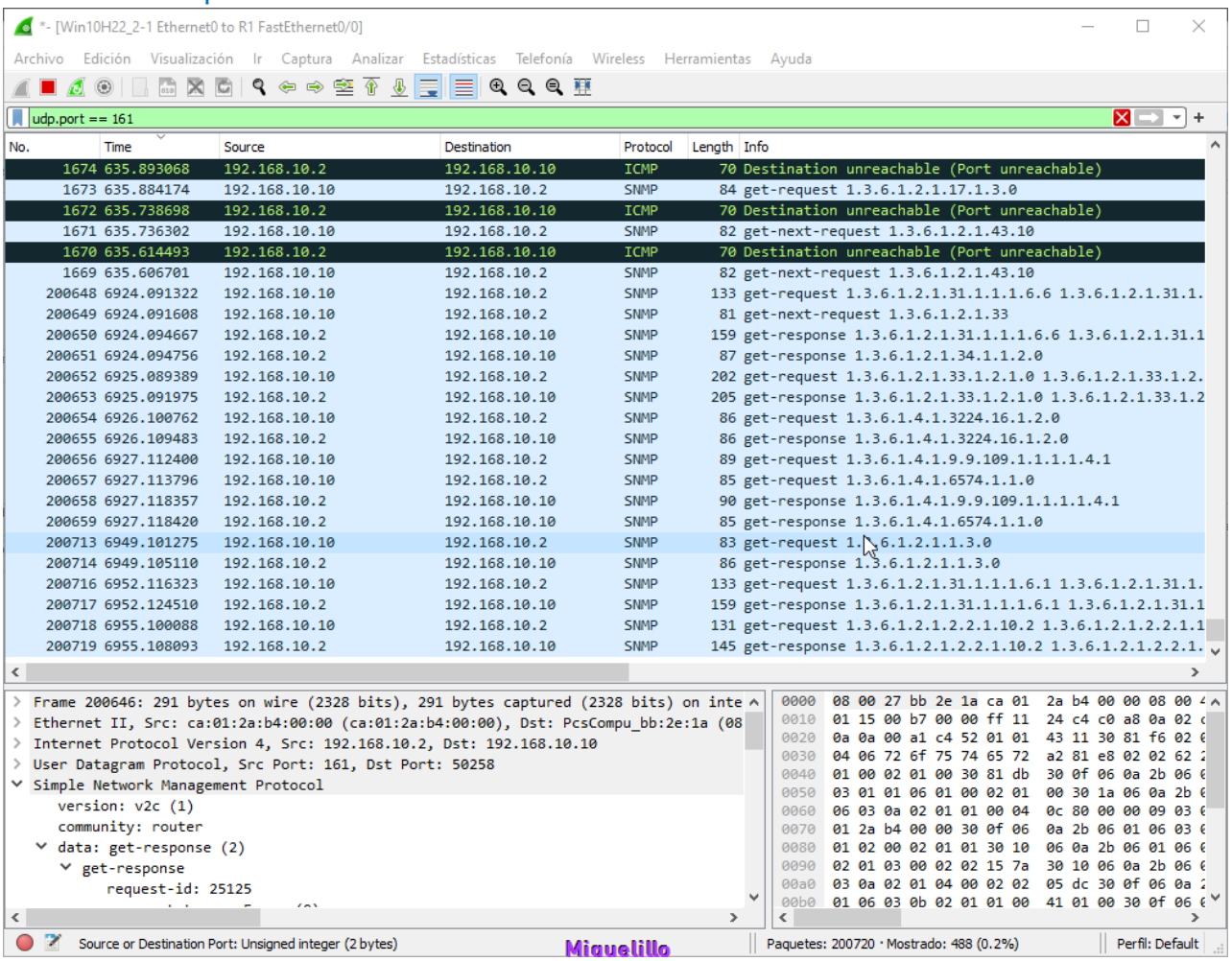
Asignamos las cerdenciaqles del SNMP



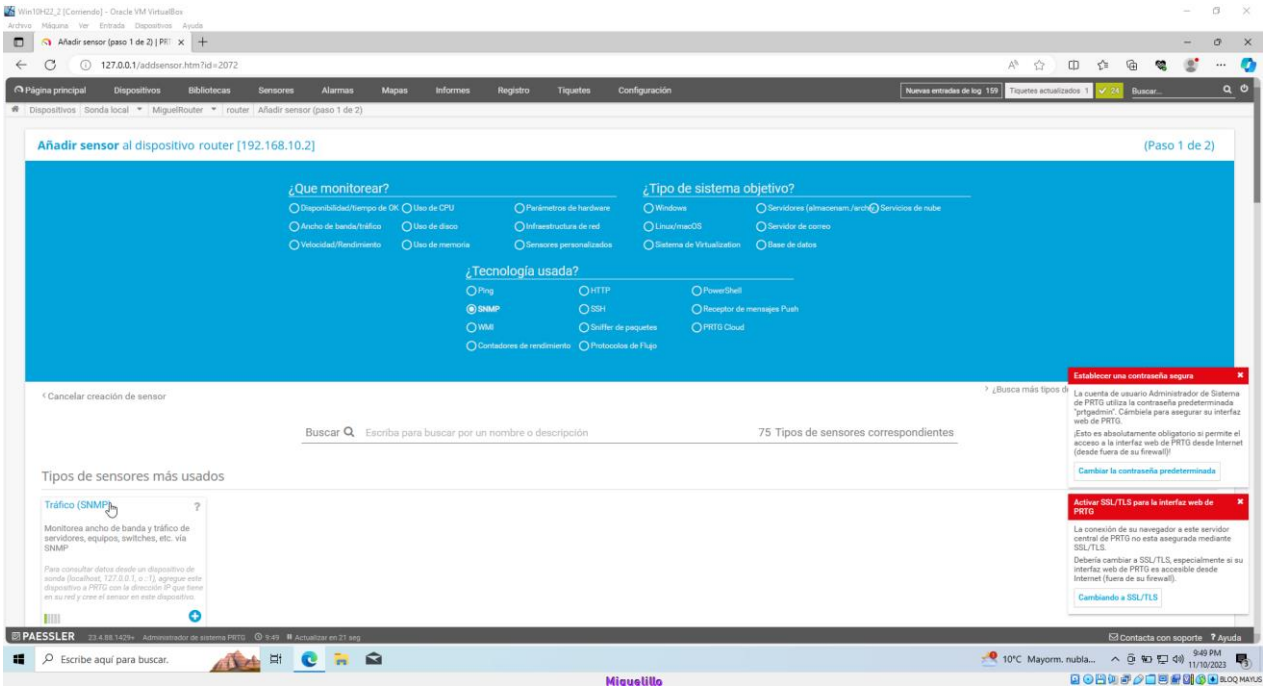
Vemos que ha hecho conectividad



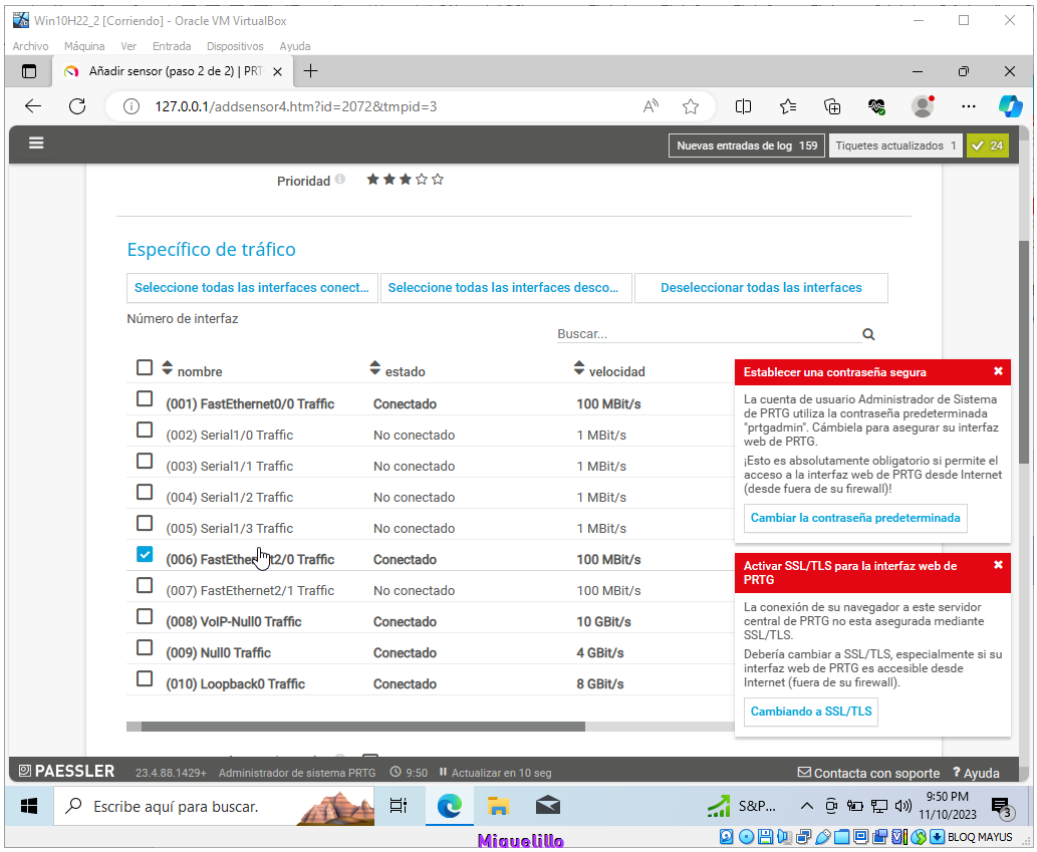
Si capturamos el tráfico por el puerto UDP 161 podemos ver los mensajes para descubrir el dispositivo.

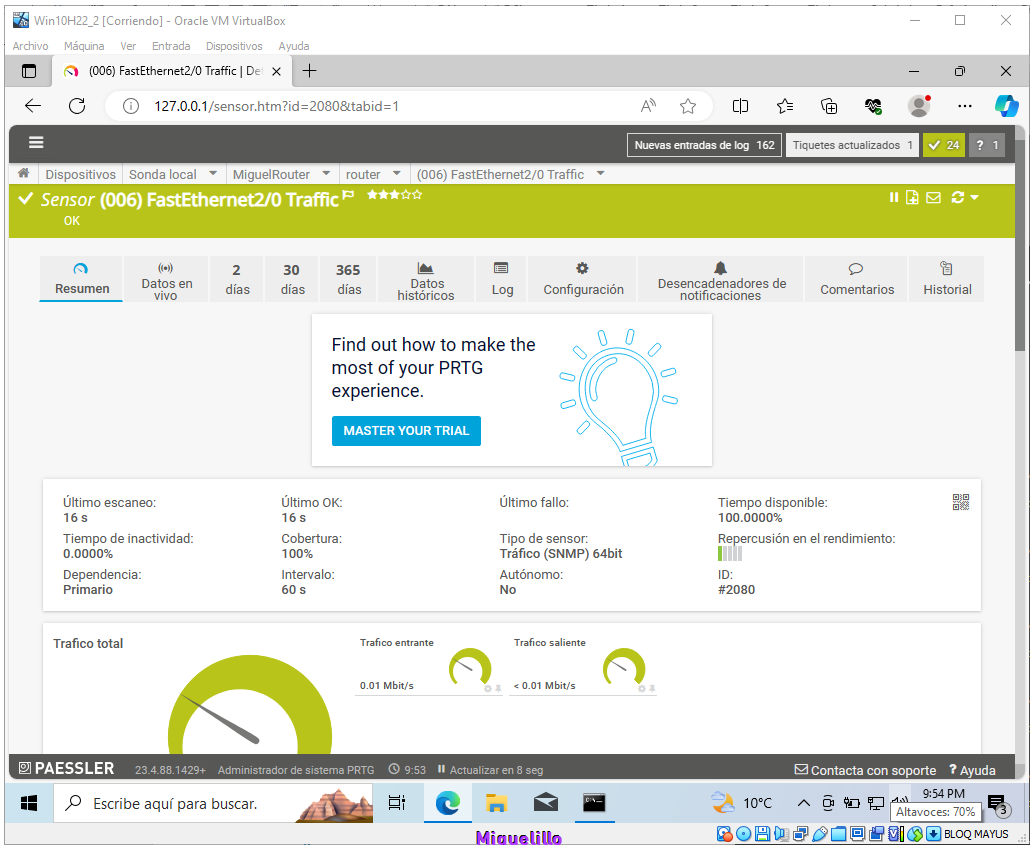


Clicamos en **Añadir un sensor** y seleccionamos **SNMP**

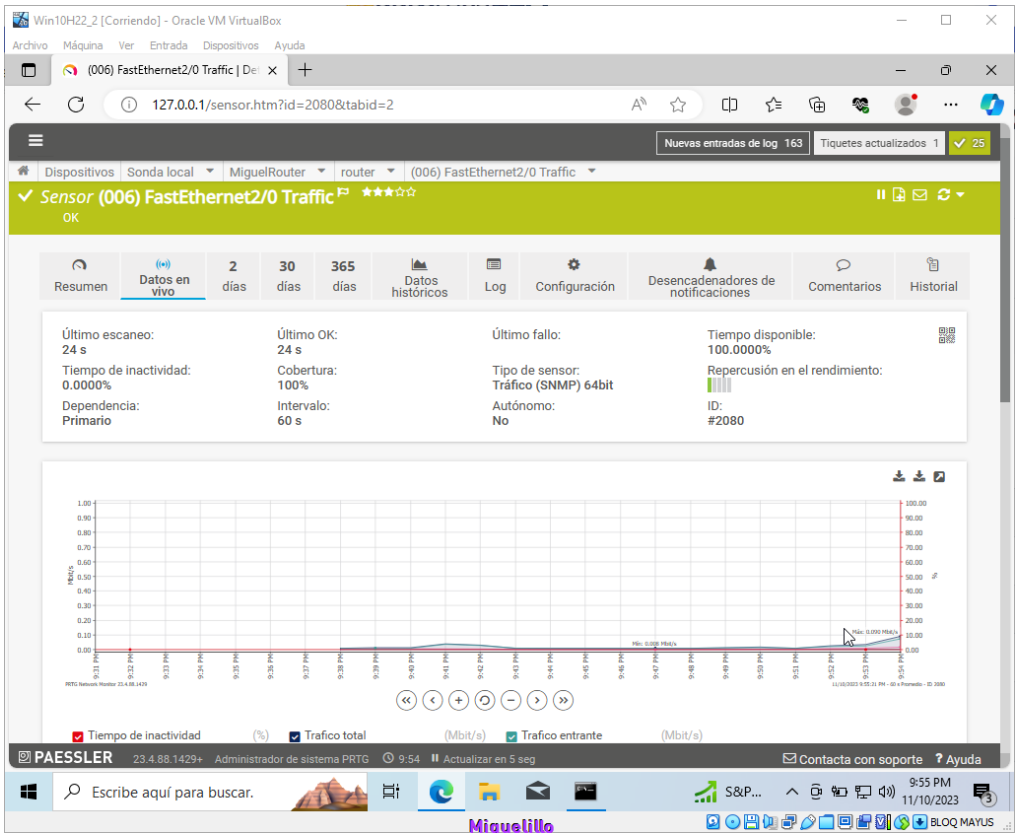


Seleccionamos el interfaz del que queramos ver el tráfico

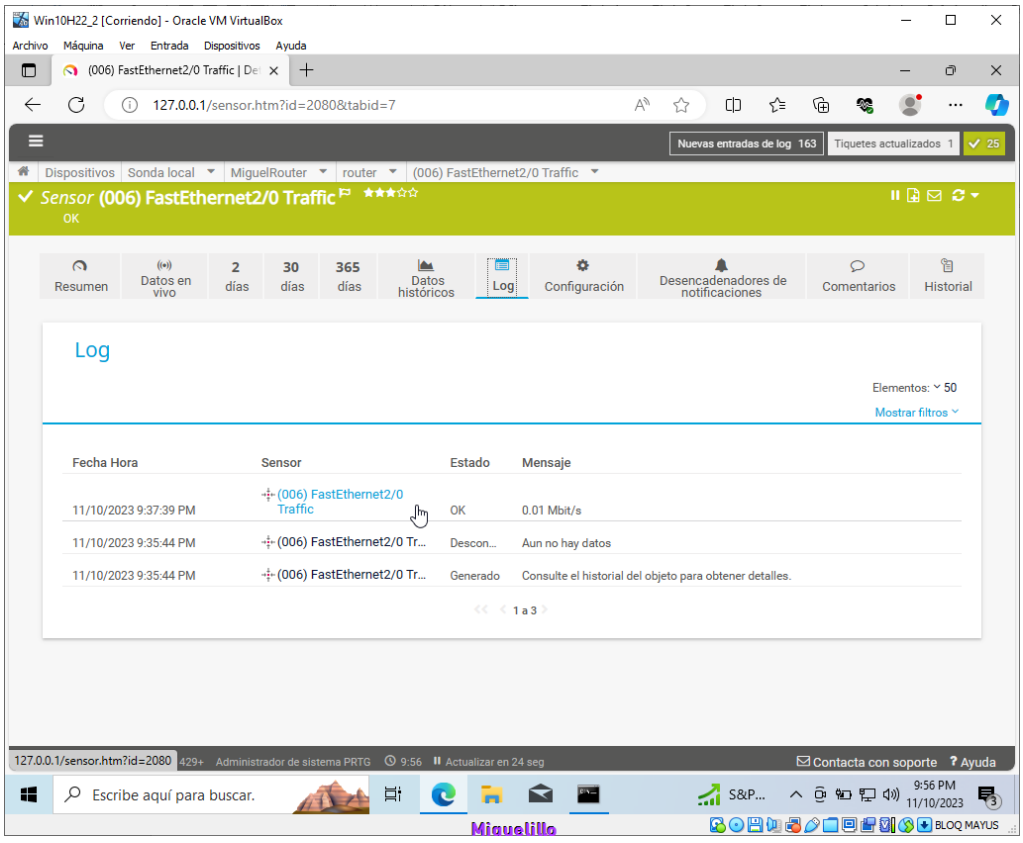




Podemos verlo en vivo clicando **Datos en vivo**

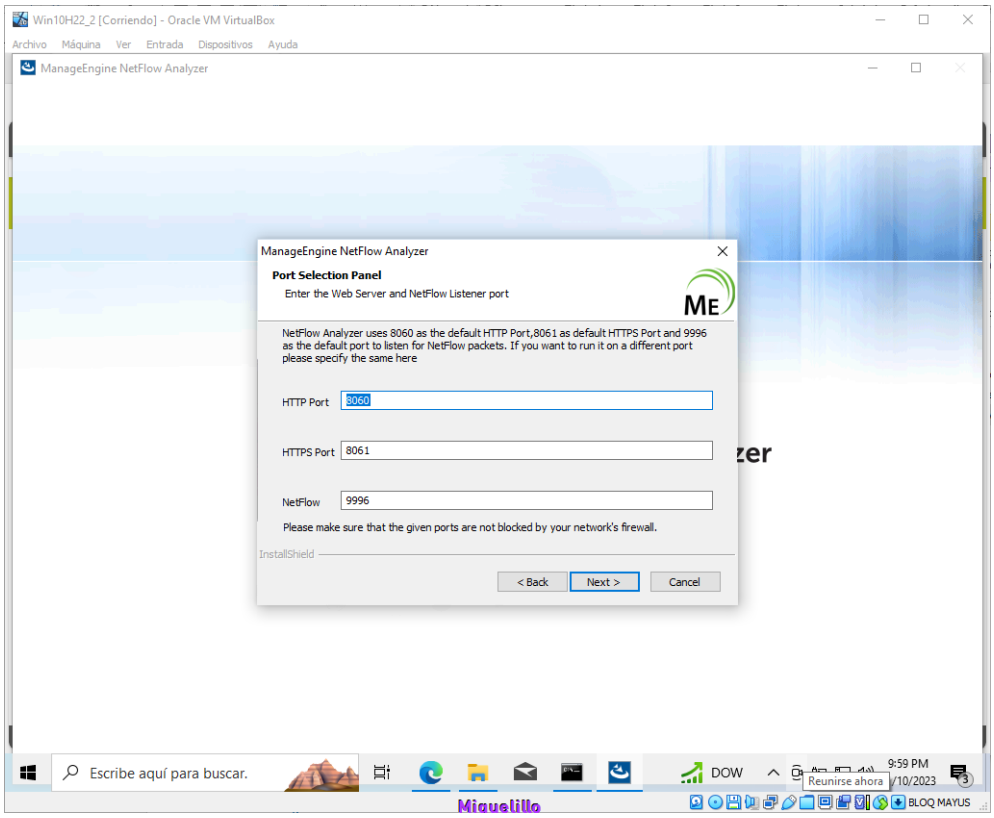


También podemos consultar los logs

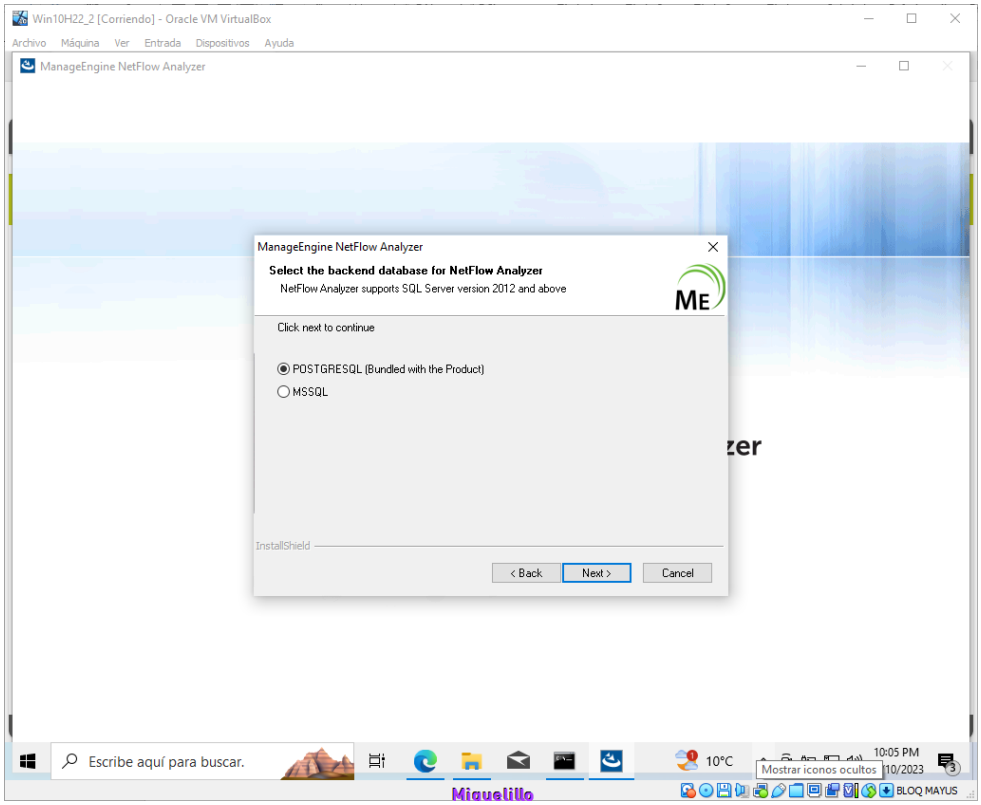


NETFLOW usaré netflow analyzer

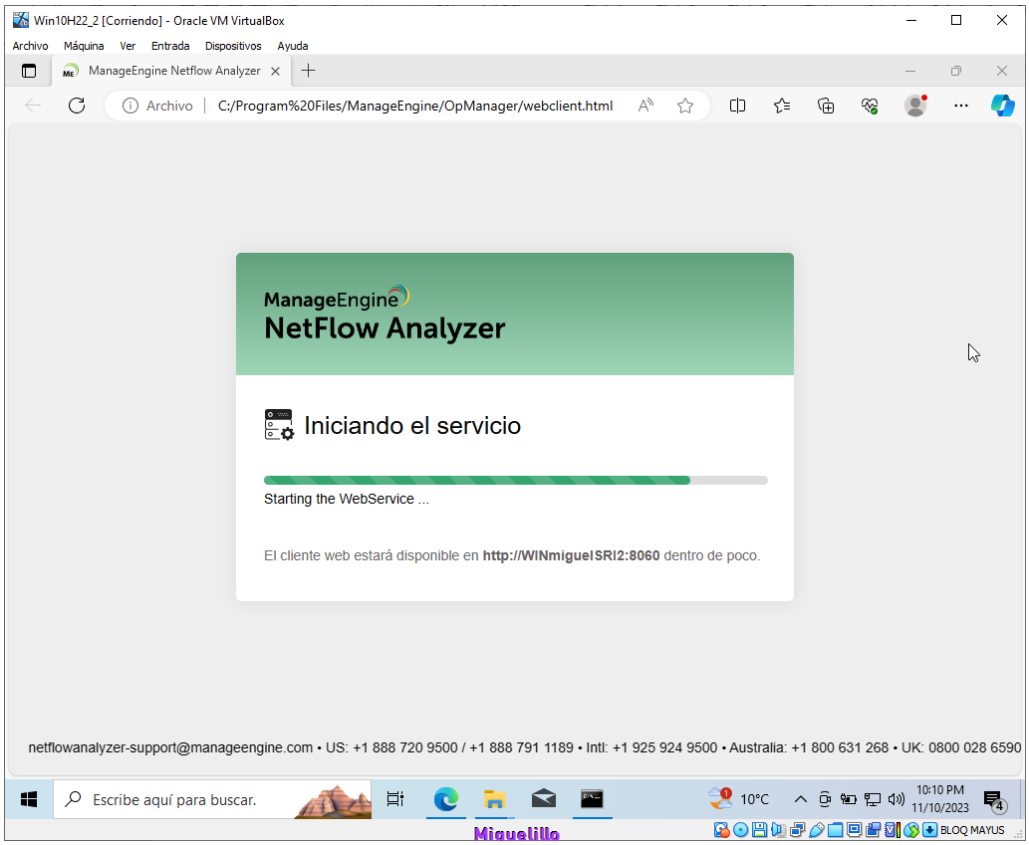
Configuramos los puertos



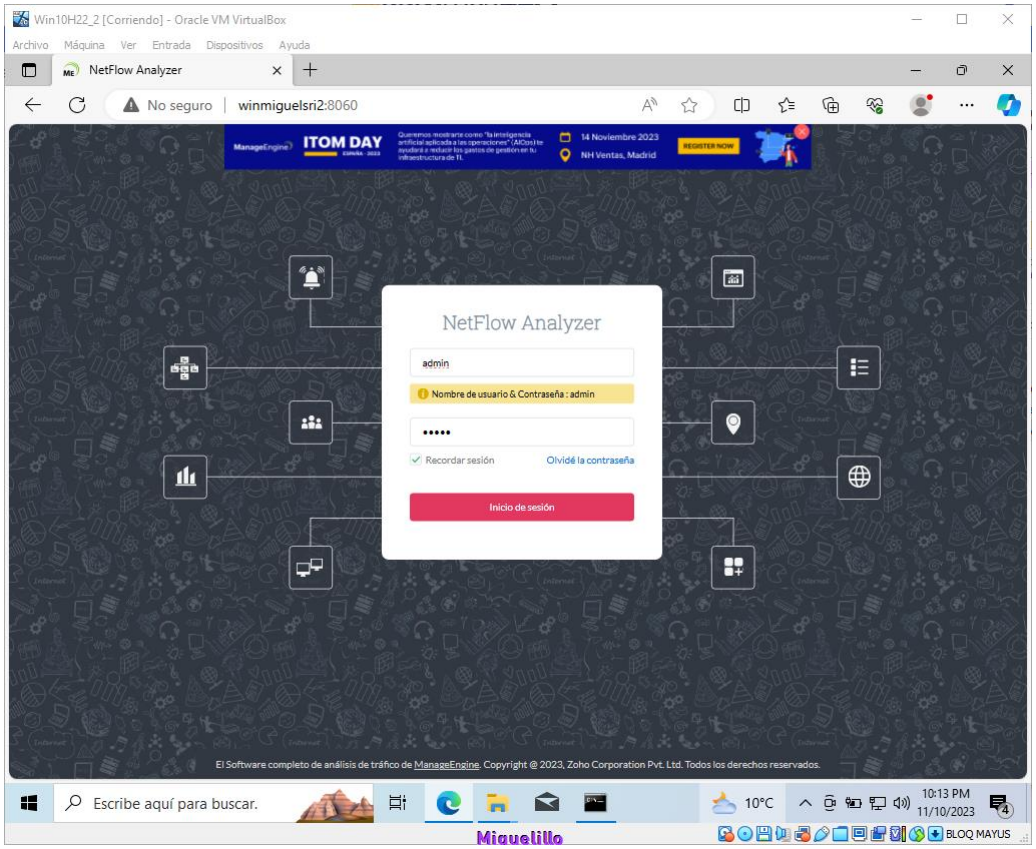
Usaremos POSTGRESQL



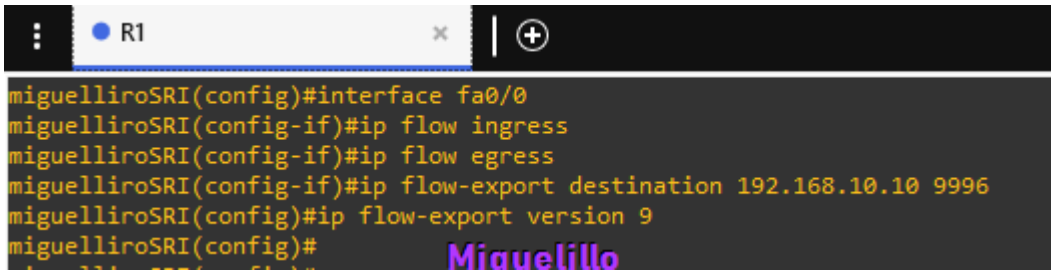
Esperamos a que inicie



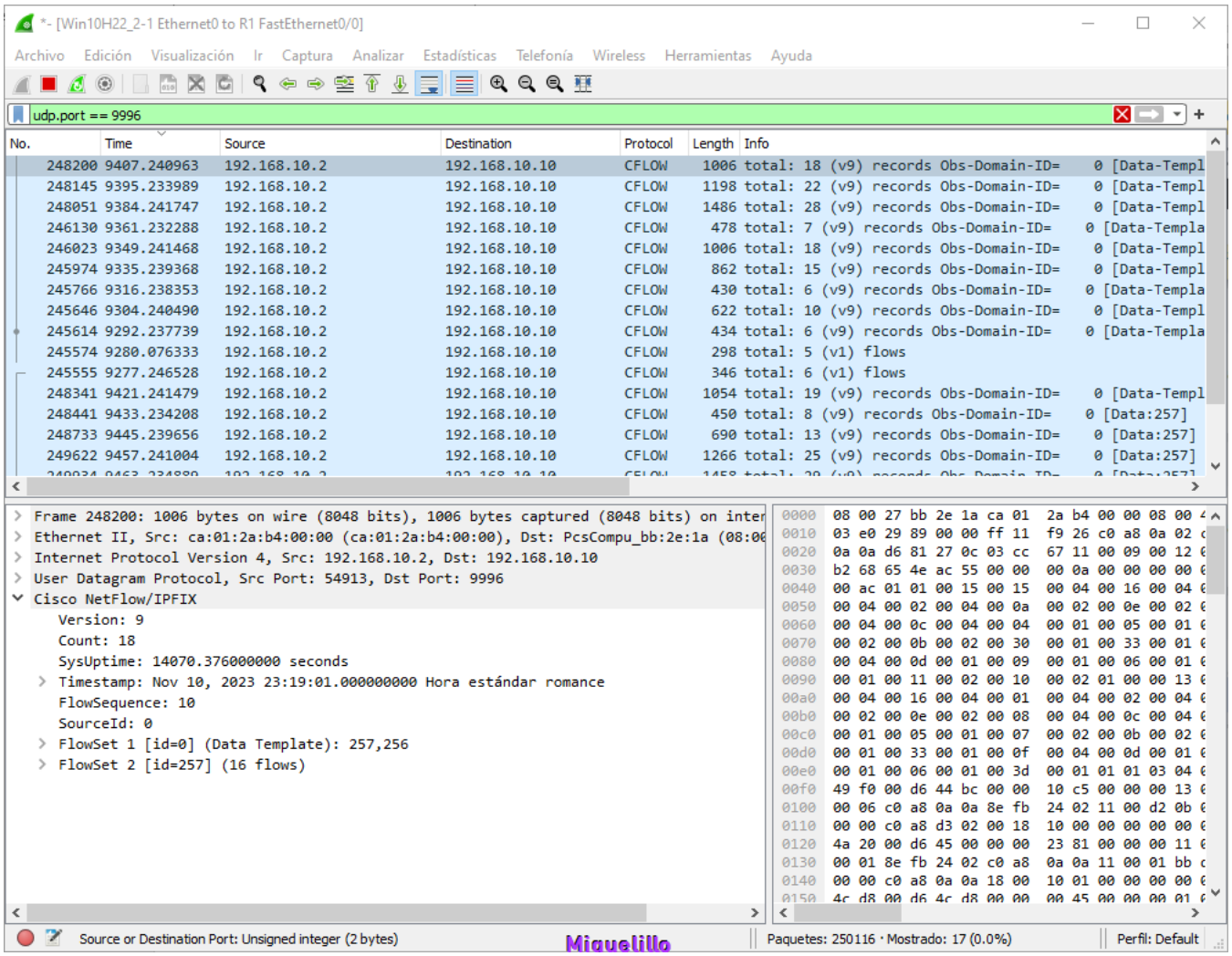
Iniciamos sesión con las credenciales por defecto



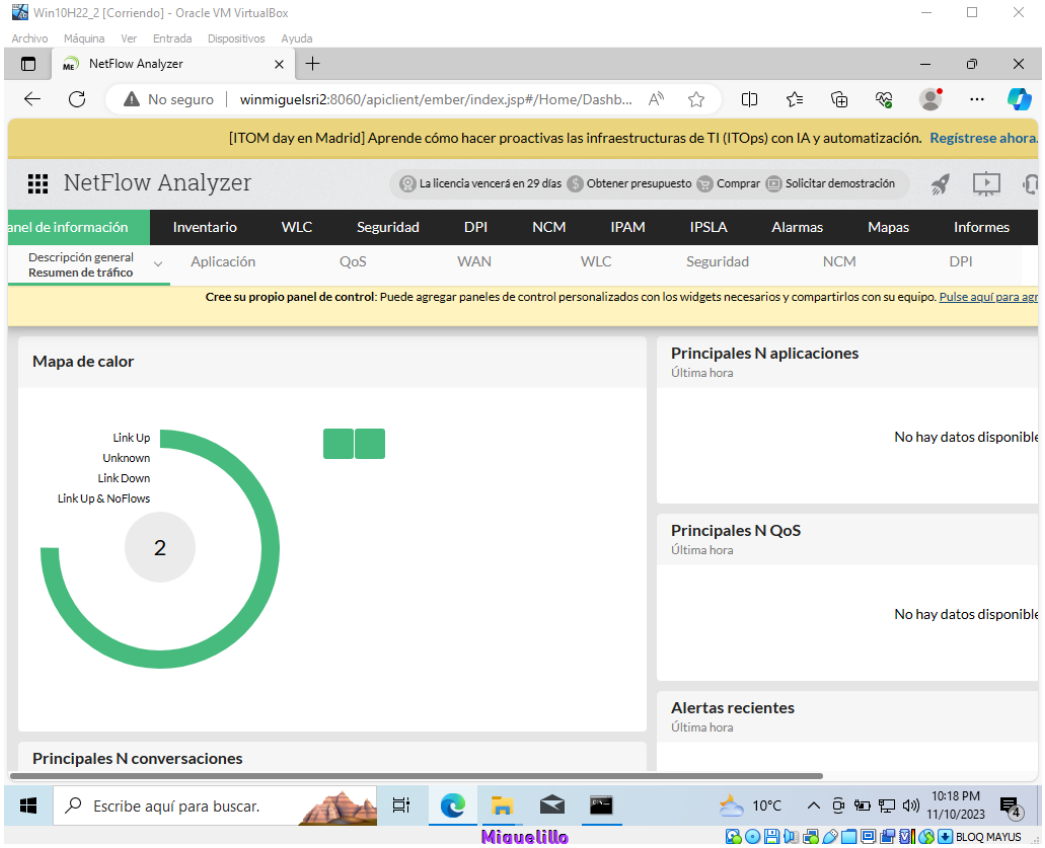
Configuramos al router para vincularlo con el servidor netflow



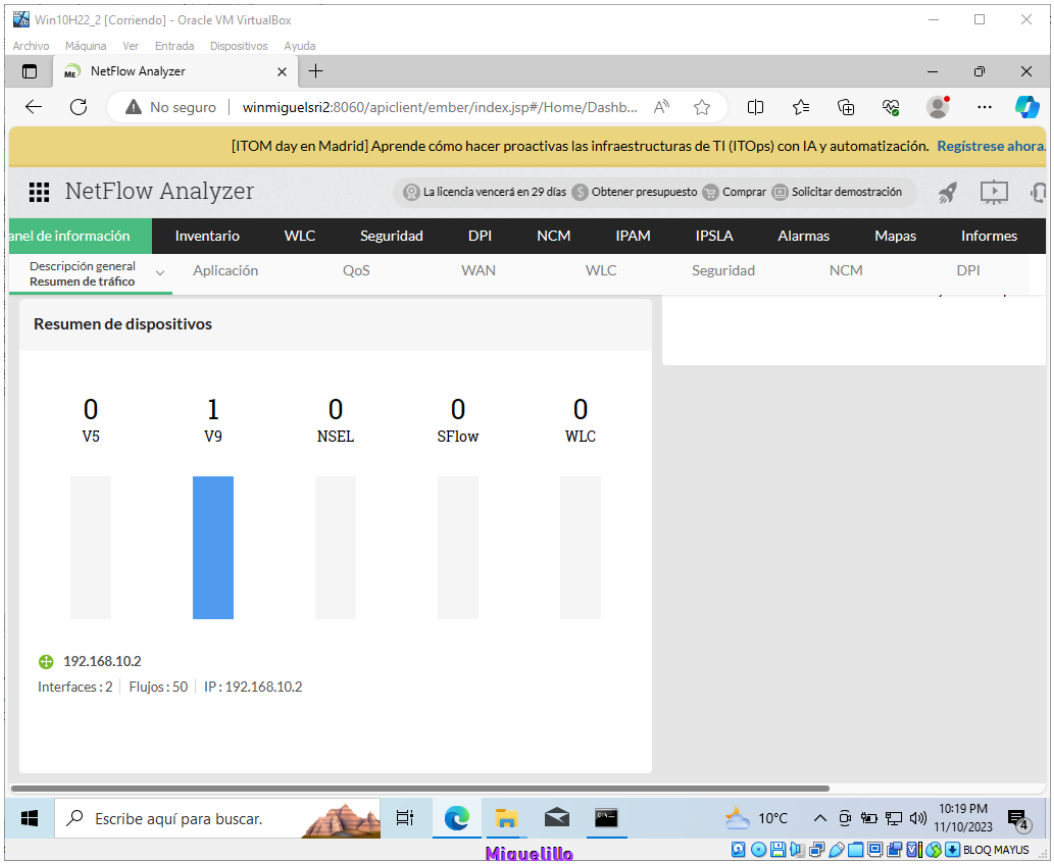
Podemos ver la comunicación en el wireshark por el puerto 9996



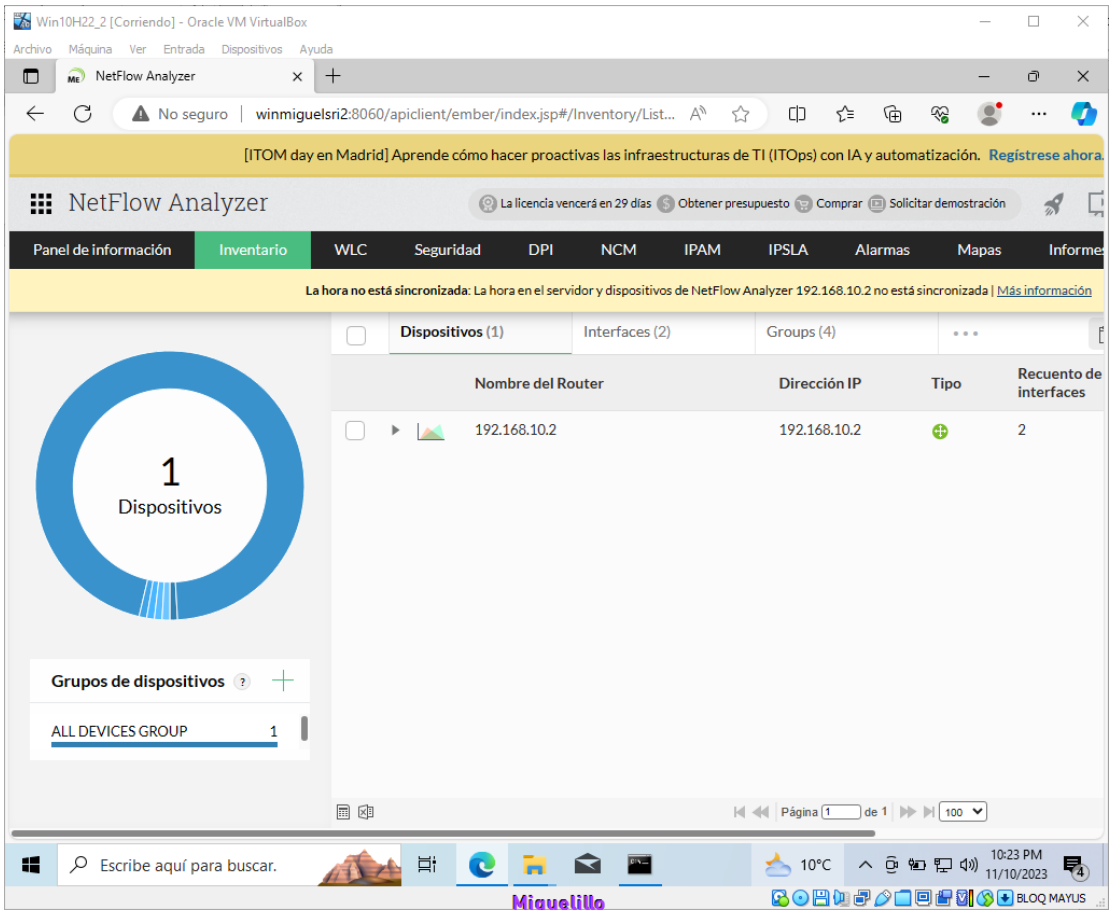
Podemos ver en el panel de información información sobre el router



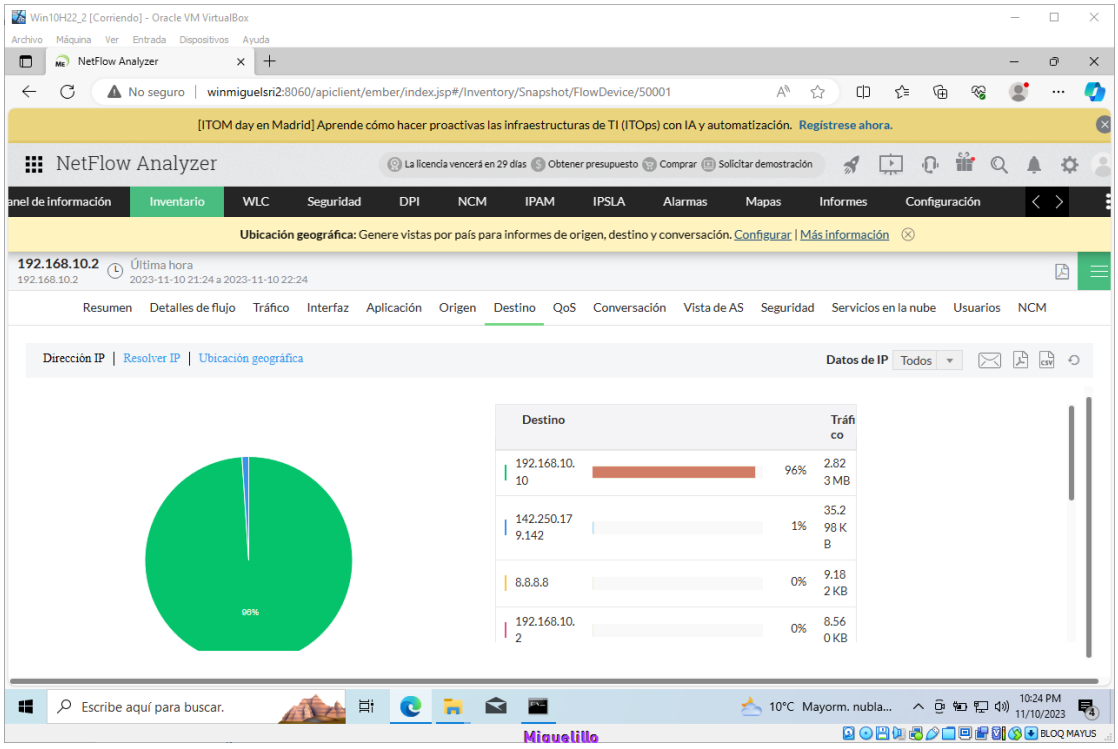
Vemos la IP del router interfaces avivas la versión del netflow



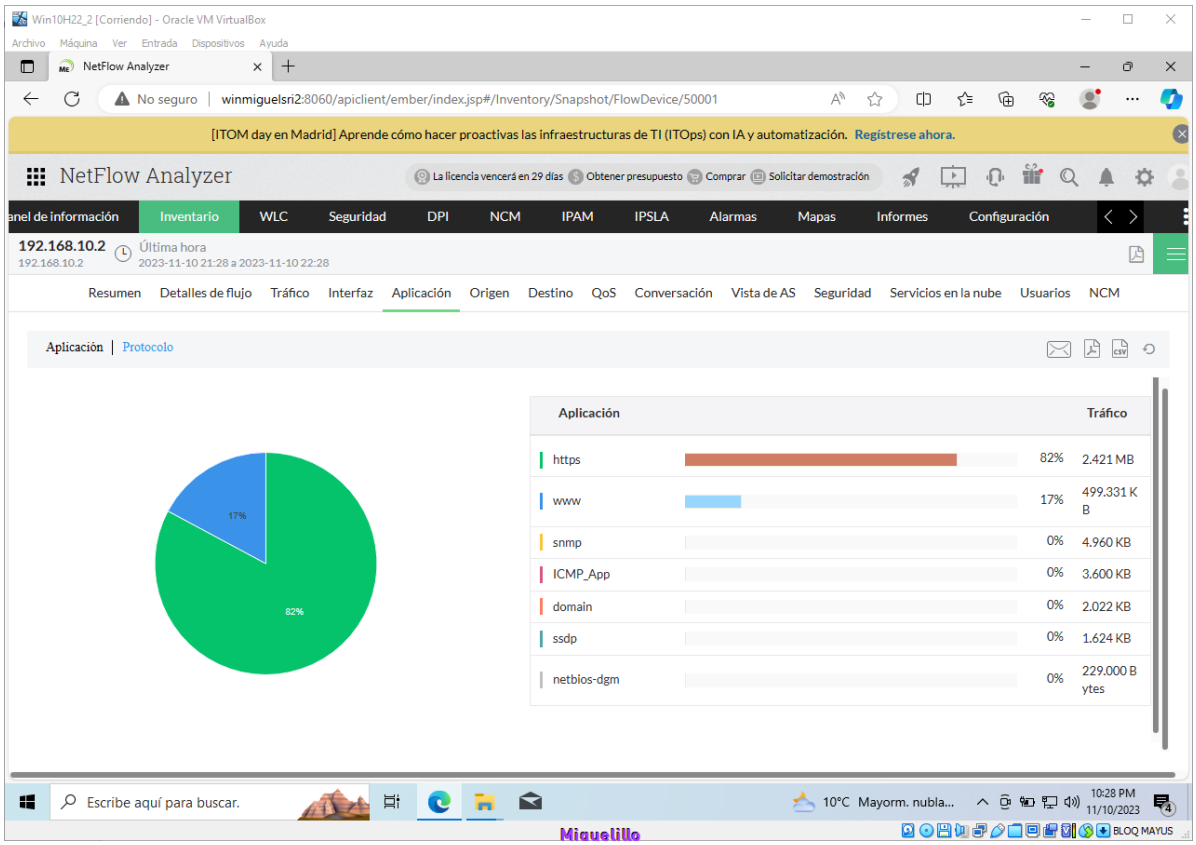
En **Inventario podemos ver los dispositivos**



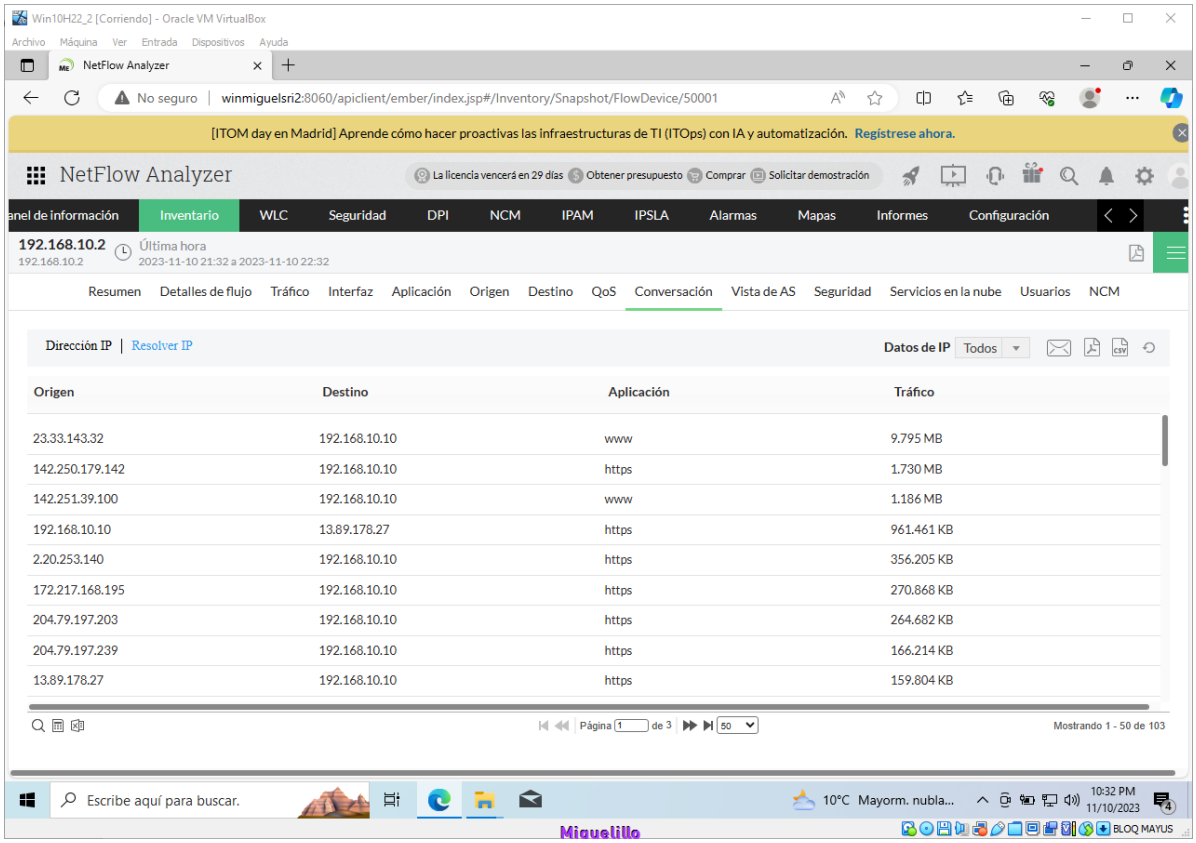
Desntro del router podemos ver los destinos principales a los que se dirige el trafico



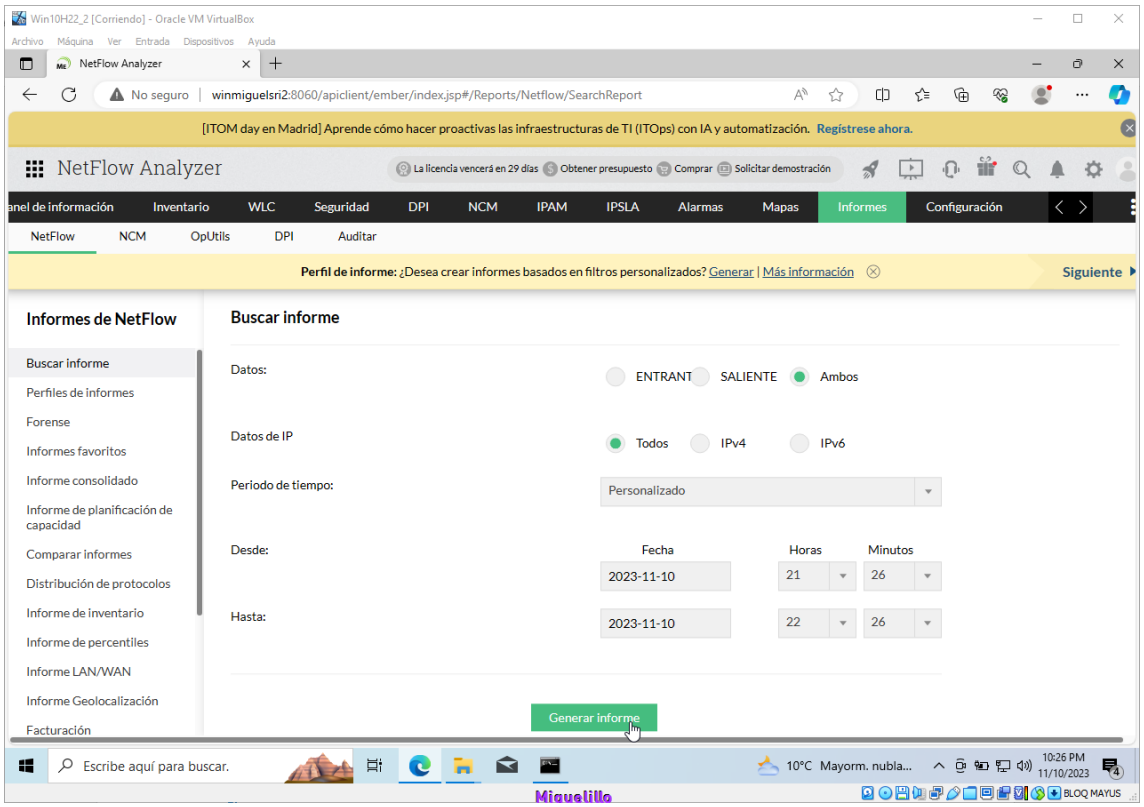
Podemos ver los protocolos más usados para comunicarse



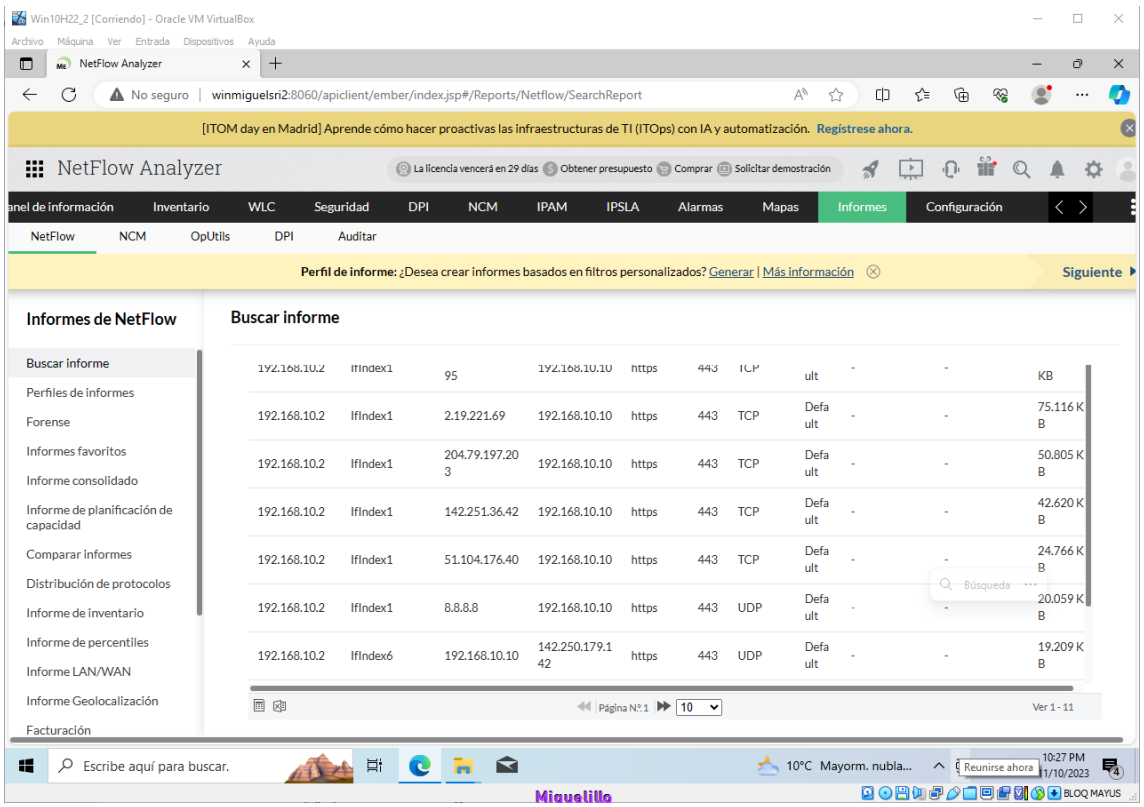
El trafico de IPs



Si vamos a **Inoformes → Buscar informe** podremos generar uno



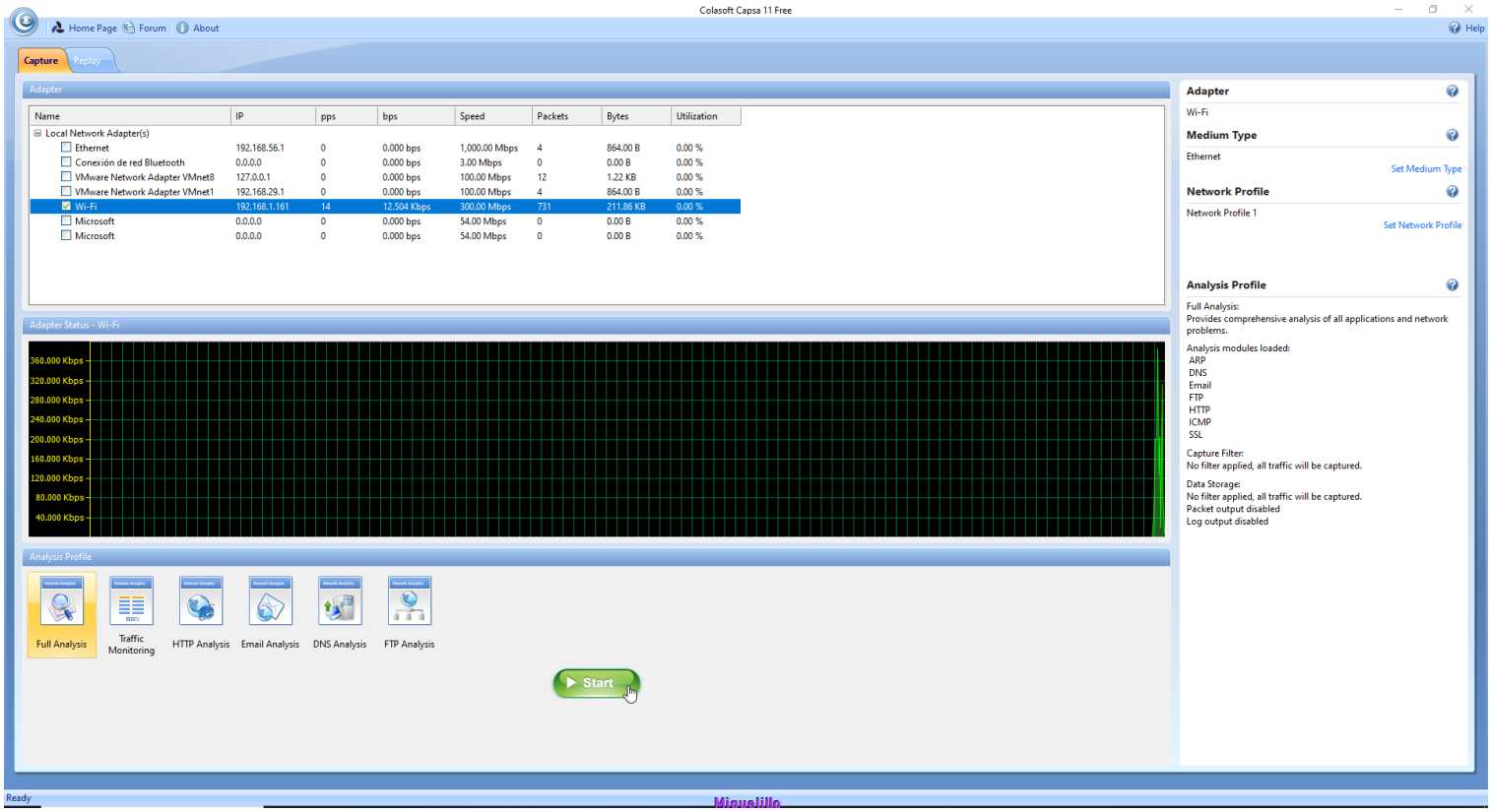
El informe generado:



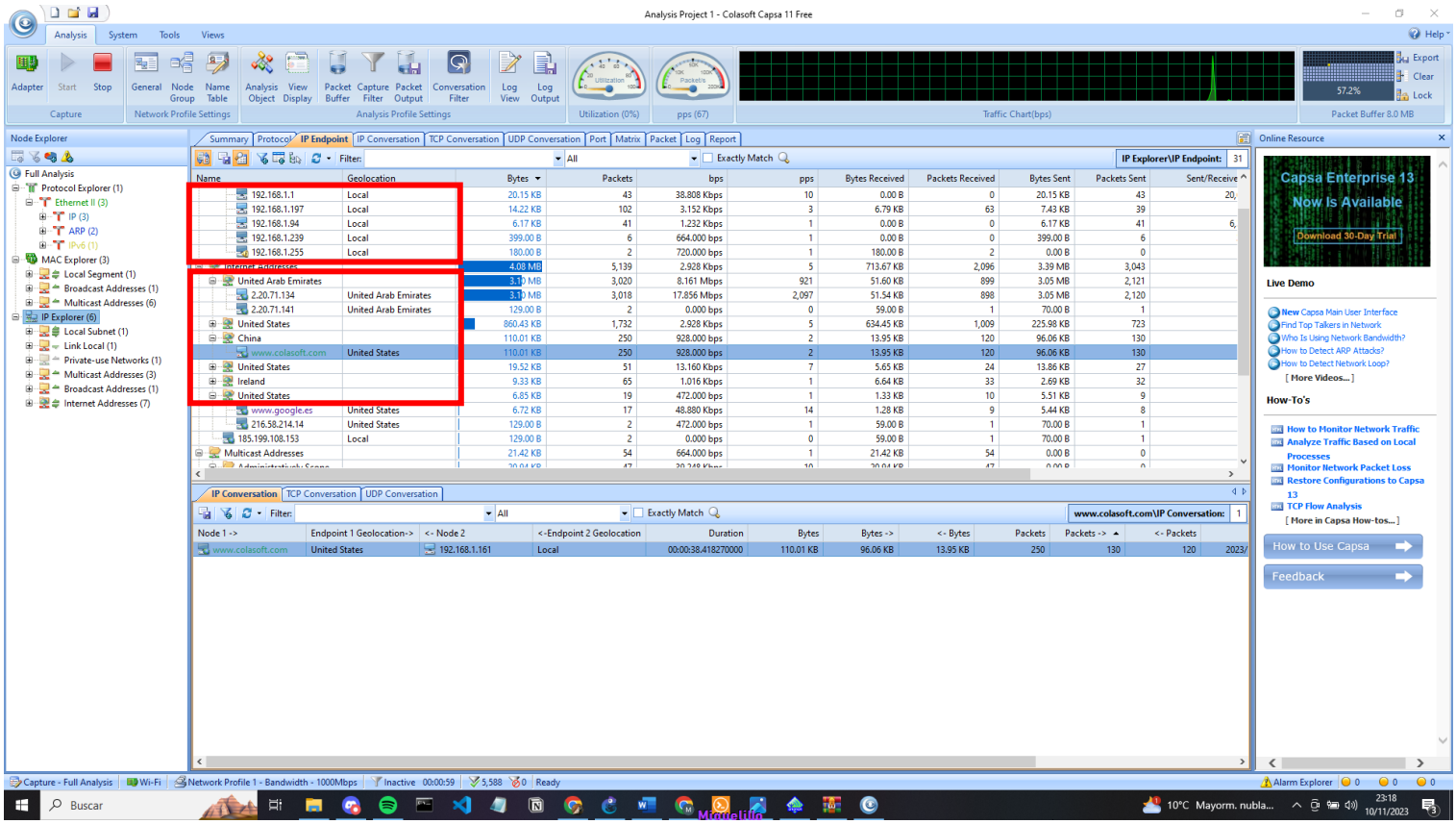
b) Descarga e instala software que monitorice redes inalámbricas y realiza filtrados de red para monitorizar sólo el tráfico deseado.

Solución:

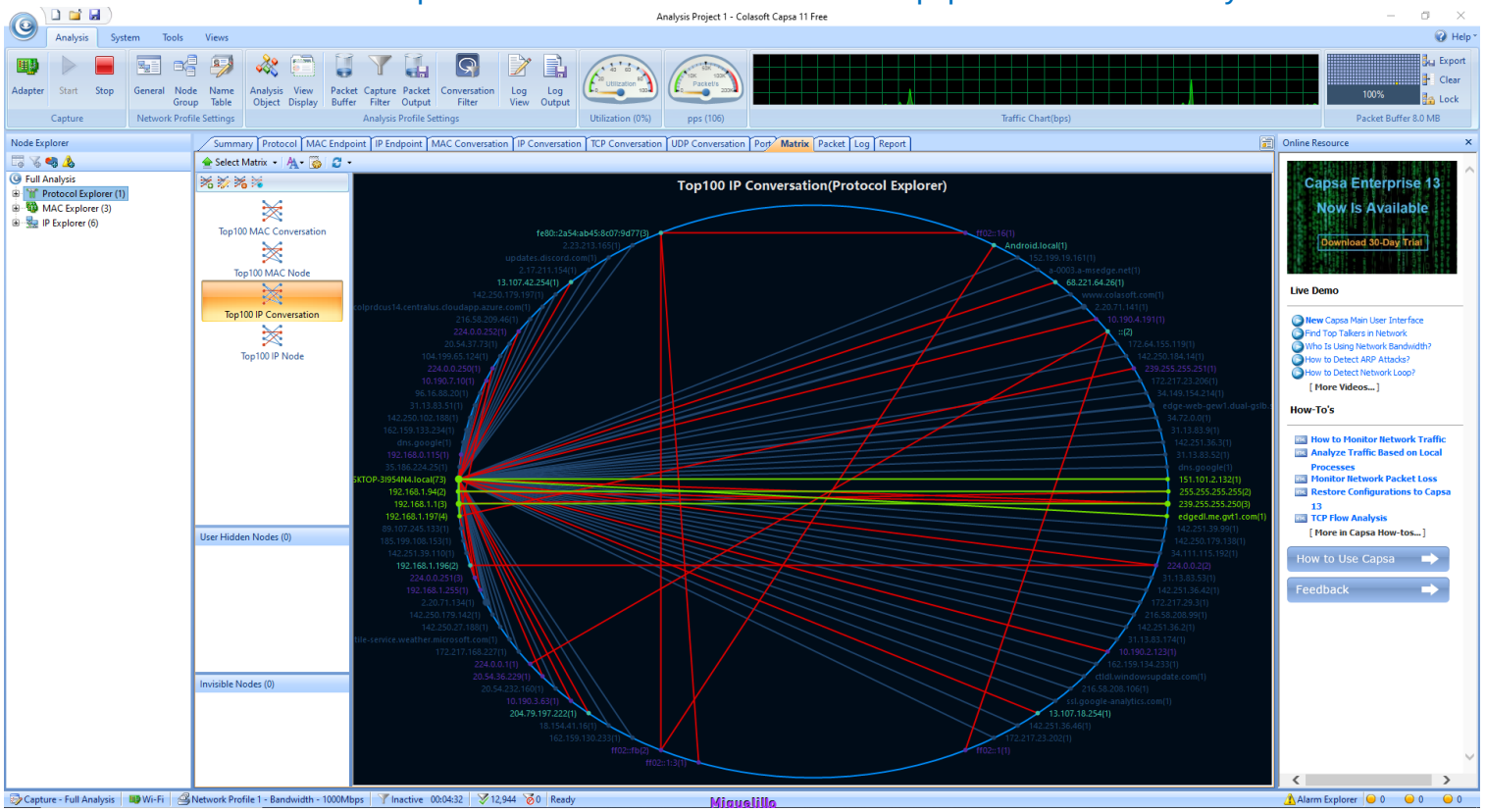
Voy a utilizar **Colasoft Capsa 11 Free** le tendremos que indicar el adaptador que vamos a usar



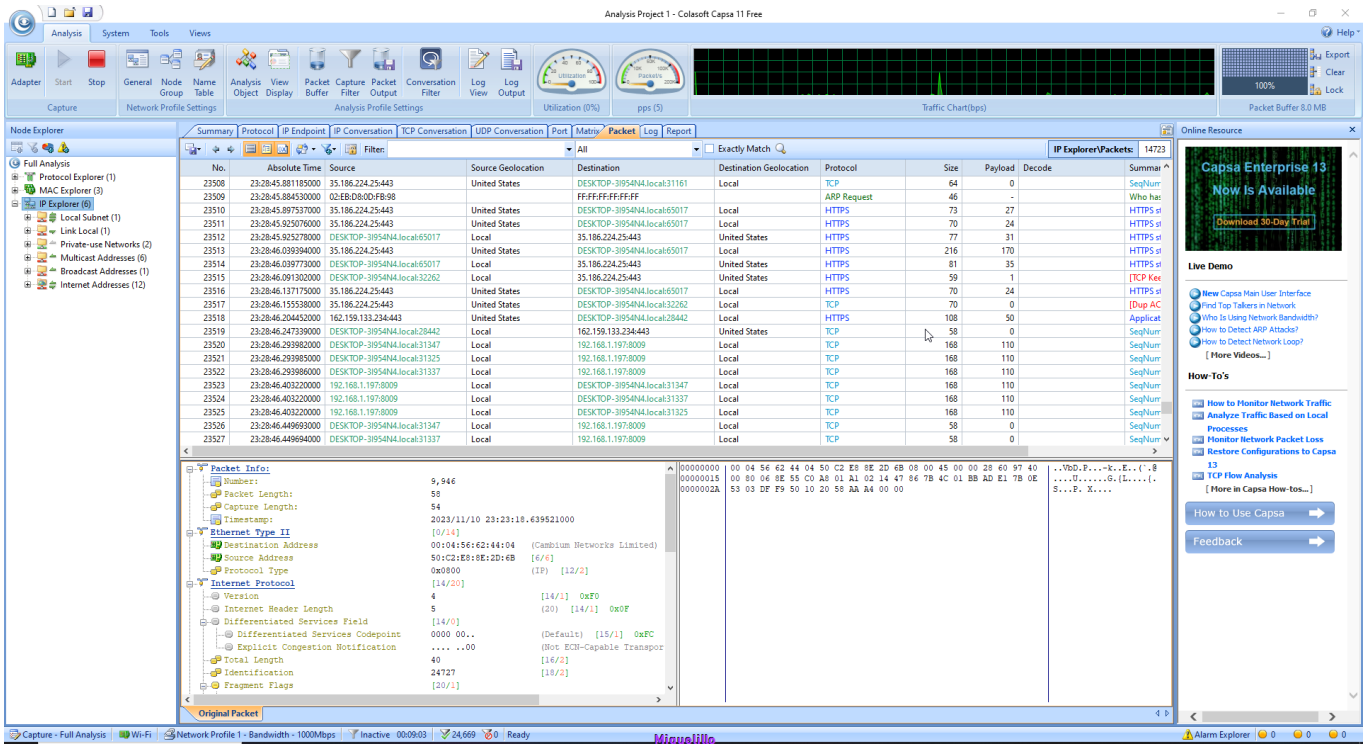
Podemos ver distintos equipos de la red y con los que se comunica su geolocaización



Podemos ver un esquema de comunicación entre equipos de esta red y de otras redes



Podemos ver los paquetes que se envían



Protocolos más utilizados