

## Índice:

Ejercicio 1 .....	2
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.....	2
b) Descarga e instala software que monitorice redes inalámbricas y realiza filtrados de red para monitorizar sólo el tráfico deseado. ....	21

# Ejercicio 1

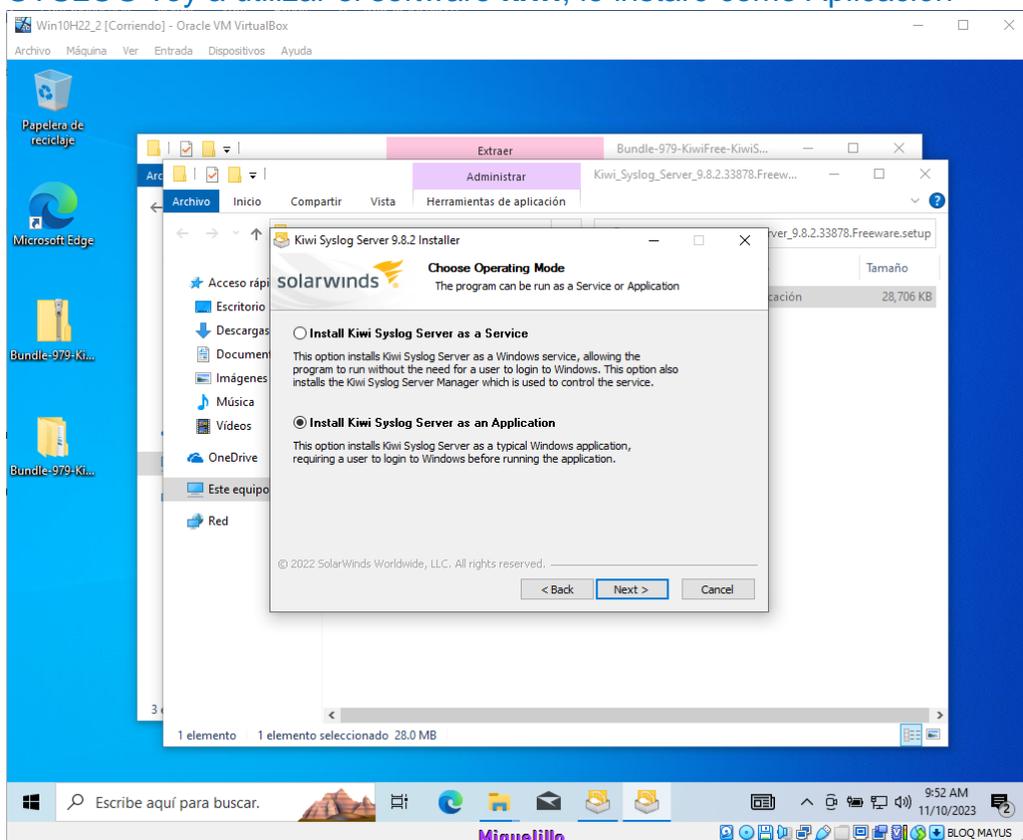
a) Descarga e instala software que monitore y supervise el tráfico de la red y realiza filtrado de servicios de red : Syslog, SNMP y NetFlow.

Solución:

Escenario  
Win10H22\_2-1



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

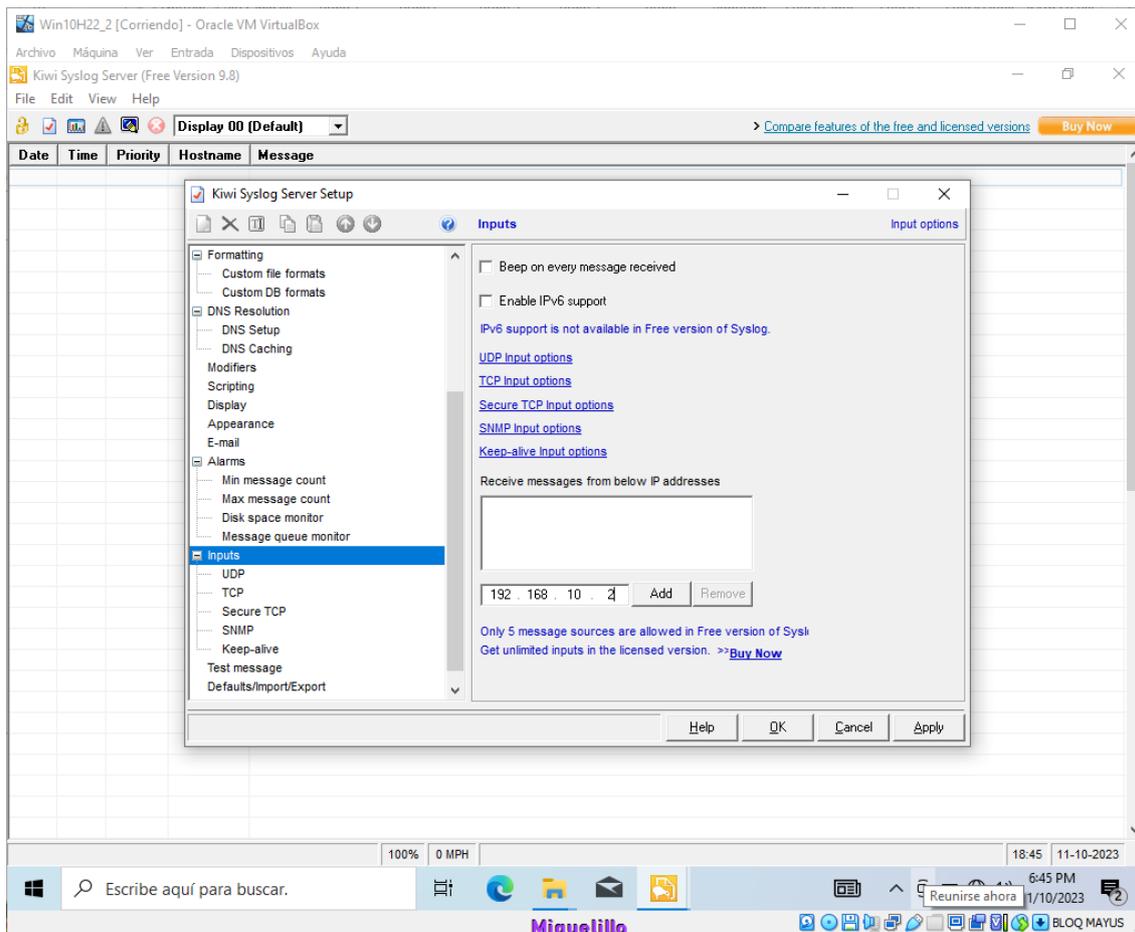


Configuramos la IP del router y para enviar registros al servidor SYSLOG

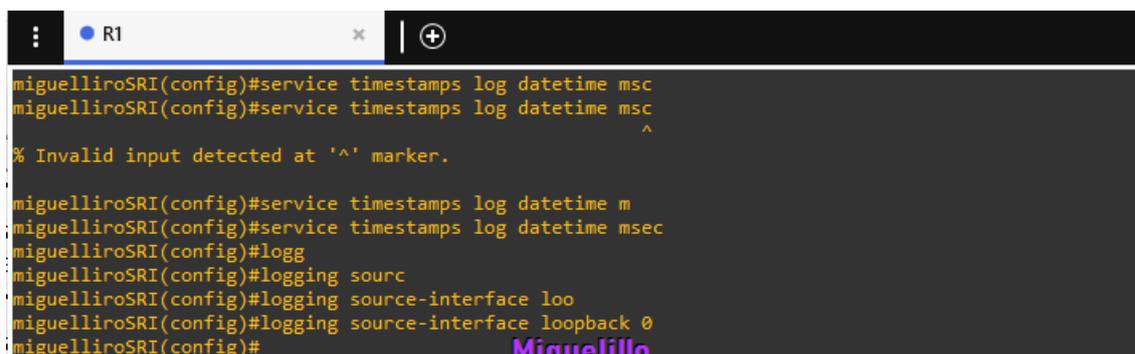
```

R1#
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname miguelliroSRI
miguelliroSRI(config)#interface FastEthernet 0/0
miguelliroSRI(config-if)#ip address 192.168.10.2 255.255.255.0
miguelliroSRI(config-if)#no shutdown
miguelliroSRI(config-if)#exit
miguelliroSRI(config)#logging on
miguelliroSRI(config)#logging facility local7
miguelliroSRI(config)#logging 192.168.10.10
miguelliroSRI(config)#
    
```

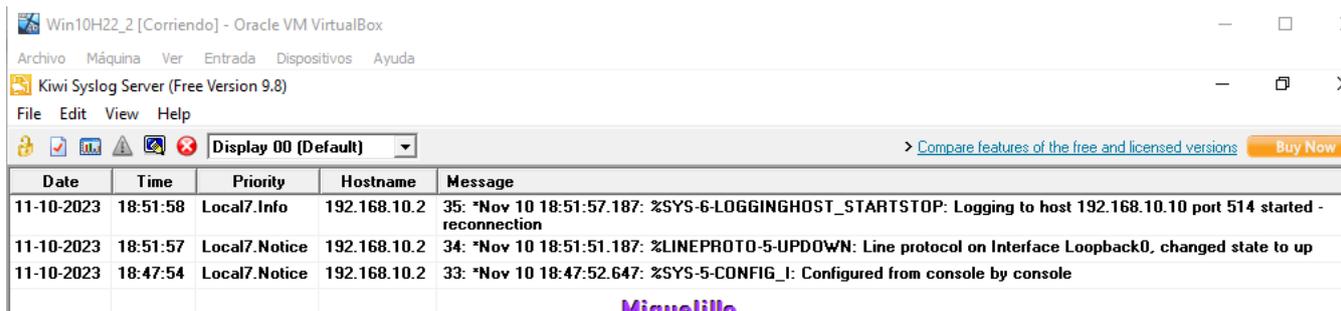
Vamos al kiwi a **File**→**Setup**→**Inputs** e introducimos la IP del router



Generamos tráfico para ver registros



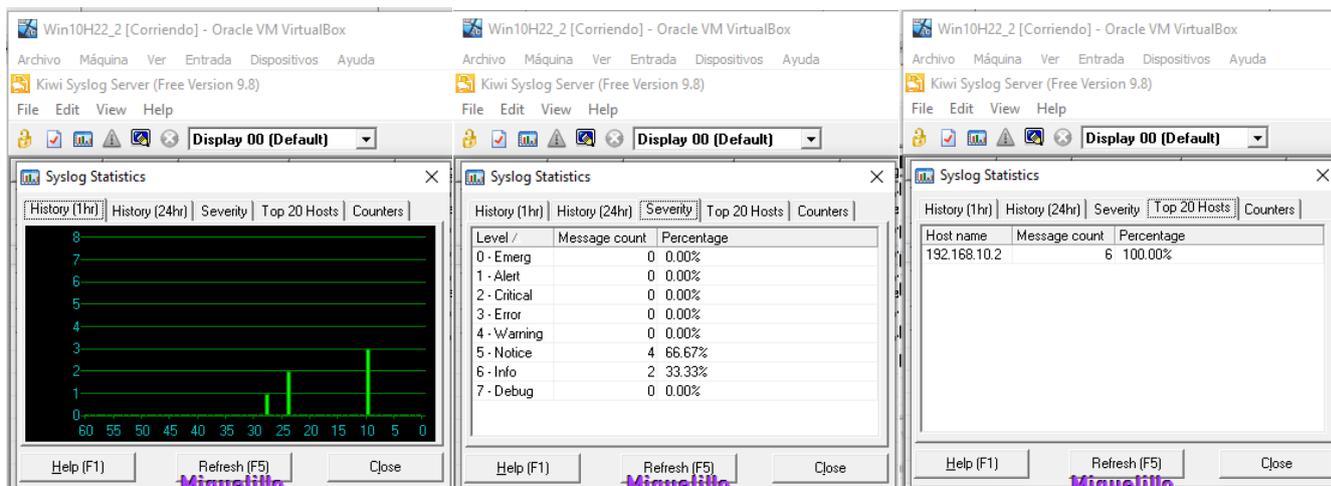
Podemos ver cómo ha registrado el tráfico y los cambios en el router.



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

Date	Time	Priority	Hostname	Message
11-10-2023	19:05:43	Local7.Info	192.168.10.2	38: *Nov 10 19:05:42.191: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.10 port 514 started - reconnection
11-10-2023	19:05:42	Local7.Notice	192.168.10.2	37: *Nov 10 19:05:37.183: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down
11-10-2023	19:05:42	Local7.Notice	192.168.10.2	36: *Nov 10 19:05:36.183: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down
11-10-2023	18:51:58	Local7.Info	192.168.10.2	35: *Nov 10 18:51:57.187: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.10 port 514 started - reconnection
11-10-2023	18:51:57	Local7.Notice	192.168.10.2	34: *Nov 10 18:51:51.187: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
11-10-2023	18:47:54	Local7.Notice	192.168.10.2	33: *Nov 10 18:47:52.647: %SYS-5-CONFIG-I: Configured from console by console

Miguelillo



Miguelillo

Miguelillo

Miguelillo

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

Context menu options:

- Select All
- Copy Selected Items
- Copy Selected Items as HTML
- Highlighting Options
- Show/Hide Columns
- Choose Font

Miguelillo

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

The screenshot shows the Wireshark interface with a capture filter of 'udp.port == 514'. The packet list pane displays three Syslog packets:

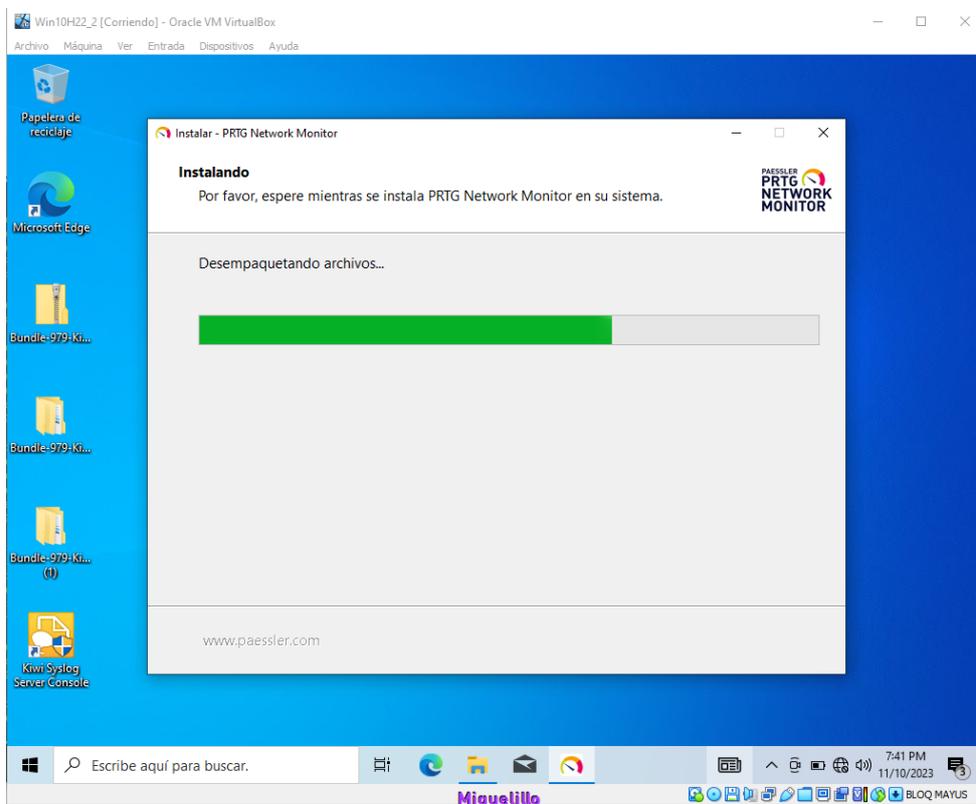
No.	Time	Source	Destination	Protocol	Length	Info
70	134.738782	192.168.10.2	192.168.10.10	Syslog	129	LOCAL7.ERR: 42: *Nov 10 19:44:23.007: %LINK-3-UPDOWN: Interface Loopback0, changed state to
71	134.738883	192.168.10.2	192.168.10.10	Syslog	151	LOCAL7.NOTICE: 43: *Nov 10 19:44:24.007: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loc
72	135.739081	192.168.10.2	192.168.10.10	Syslog	164	LOCAL7.INFO: 44: *Nov 10 19:44:29.015: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168

Packet 72 is expanded to show the following details:

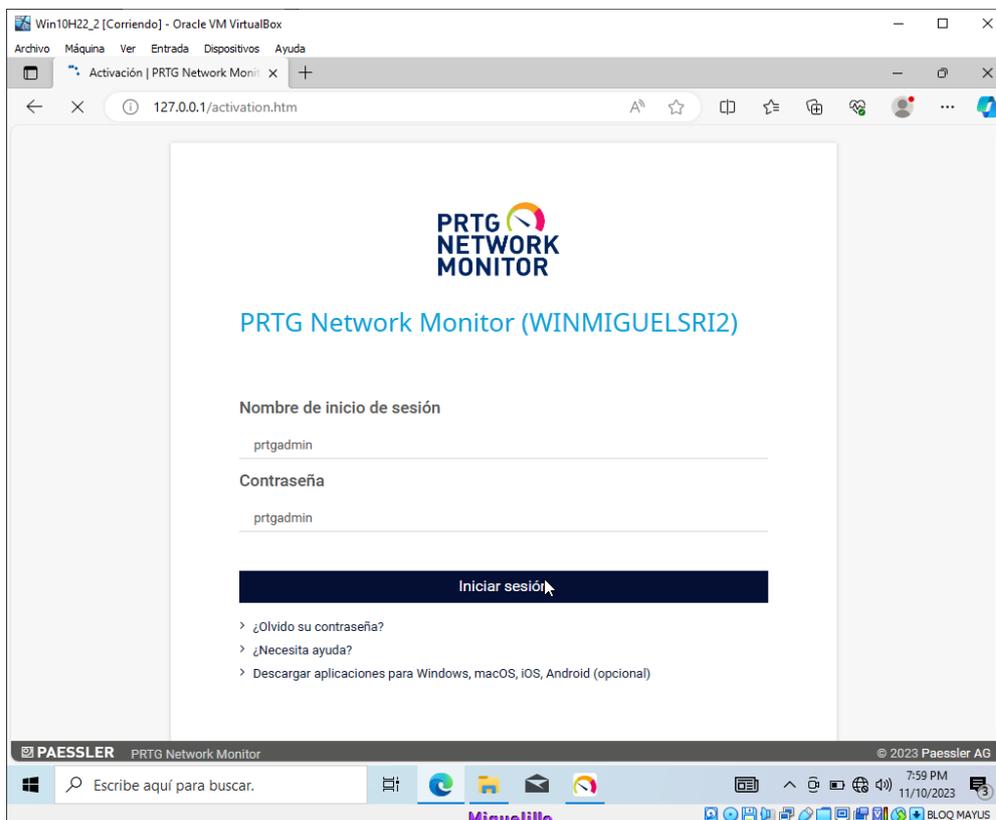
- Frame 72: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0
- Ethernet II, Src: ca:01:2a:b4:00:00 (ca:01:2a:b4:00:00), Dst: PcsCompu\_bb:2e:1a (08:00:27:bb:2e:1a)
- Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.10.10
- User Datagram Protocol, Src Port: 50696, Dst Port: 514
- Syslog message: LOCAL7.INFO: 44: \*Nov 10 19:44:29.015: %SYS-6-LOGGINGHOST\_STARTSTOP: Logging to host 192.168.10.10 port 514 started - reconnection
  - 1011 1... = Facility: LOCAL7 - reserved for local use (23)
  - .... .110 = Level: INFO - informational (6)
  - Message: 44: \*Nov 10 19:44:29.015: %SYS-6-LOGGINGHOST\_STARTSTOP: Logging to host 192.168.10.10 port 514 started - reconnection

The bottom status bar shows: Paquetes: 612 · Mostrado: 3 (0.5%) and Perfil: Default.

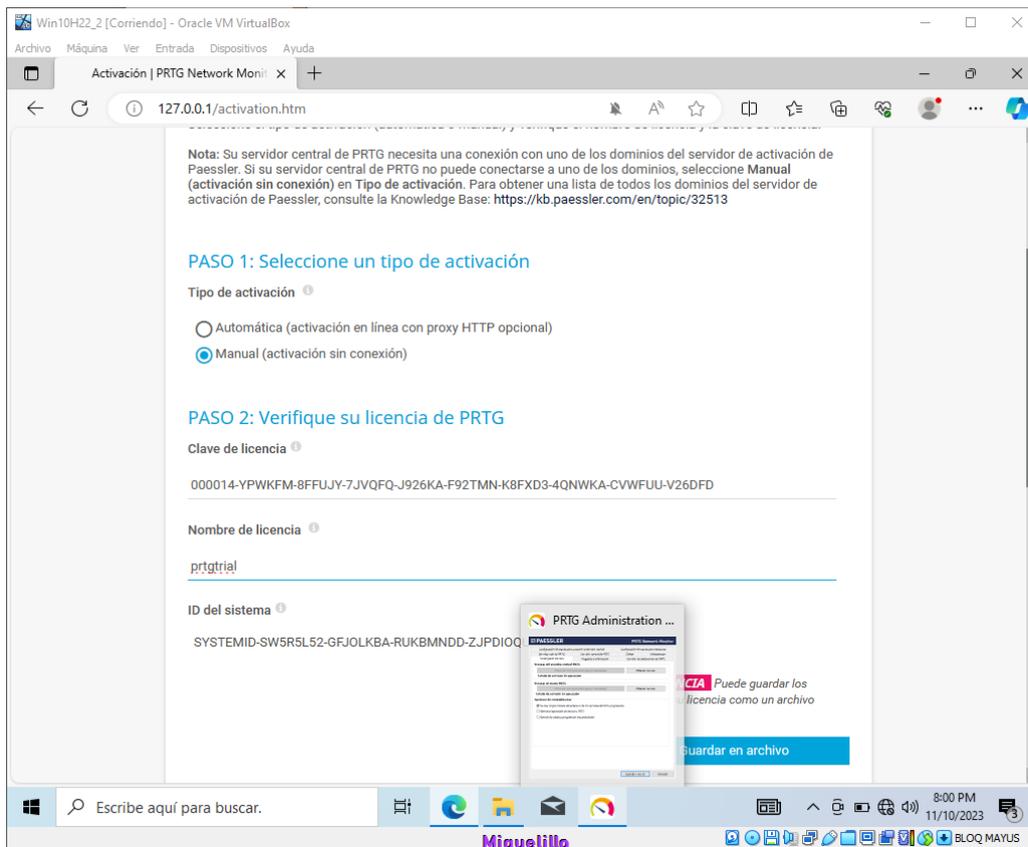
## SNMP voy a usar PRTG



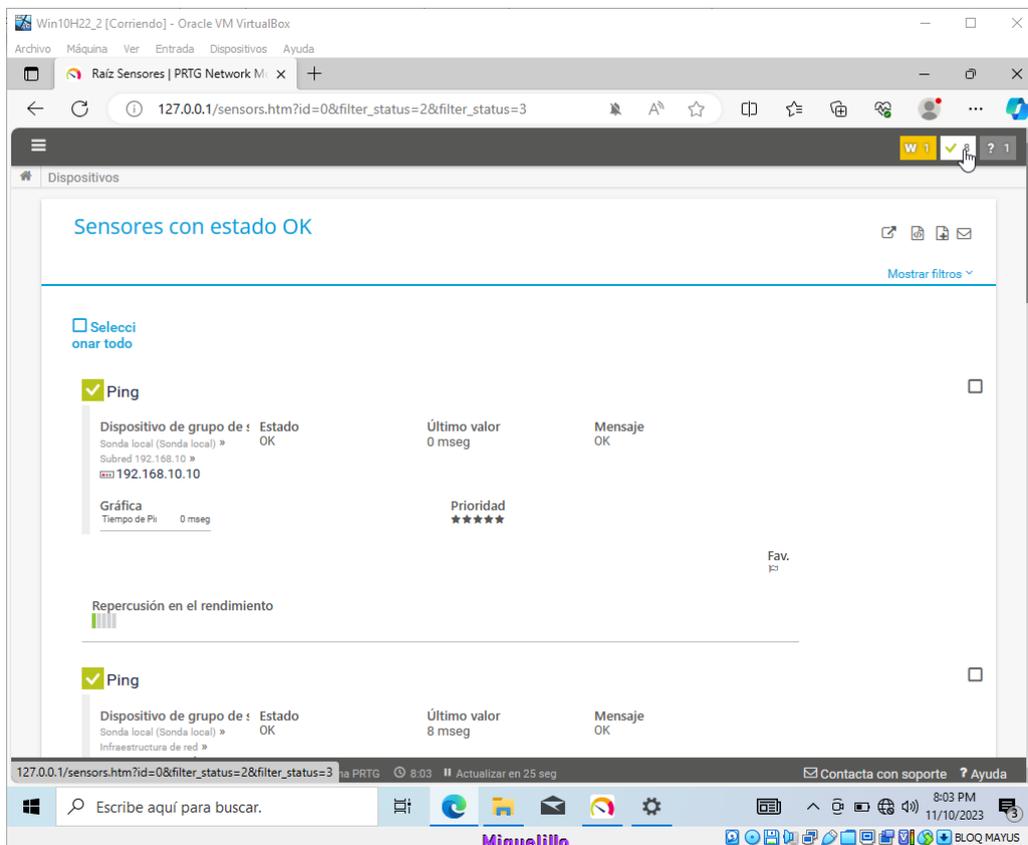
## Iniciamos sesión en el launcher del navegador



### Activo la licencia



### Una vez activada la licencia



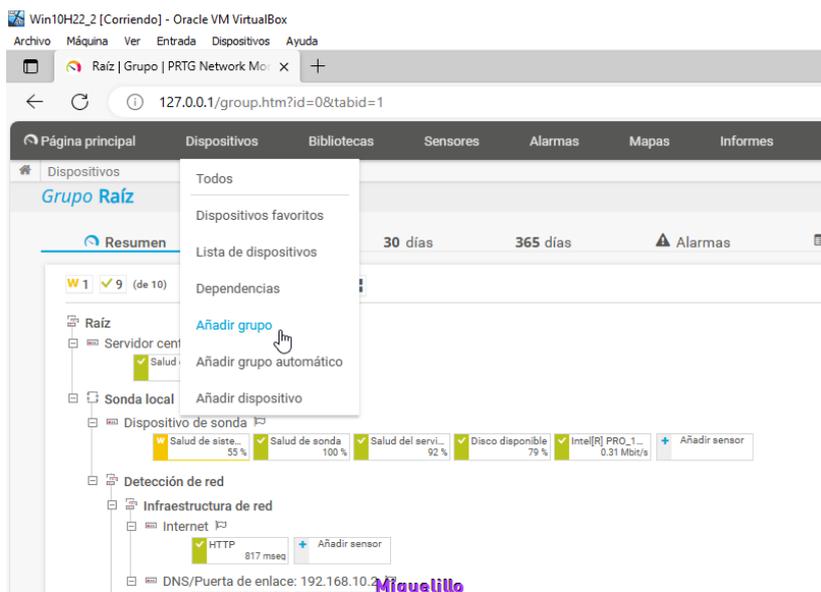
Configuramos el router para que se cominique con el servidor snmp

```

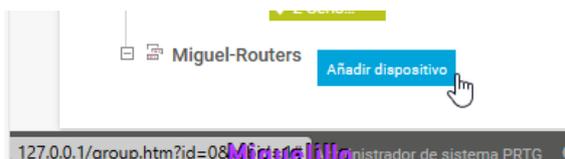
miguelliroSRI(config)#snmp-server community router rw
miguelliroSRI(config)#snmp-server community router ro
miguelliroSRI(config)#snmp-server host 192.168.10.10 router
miguelliroSRI(config)#
    
```

Miguelillo

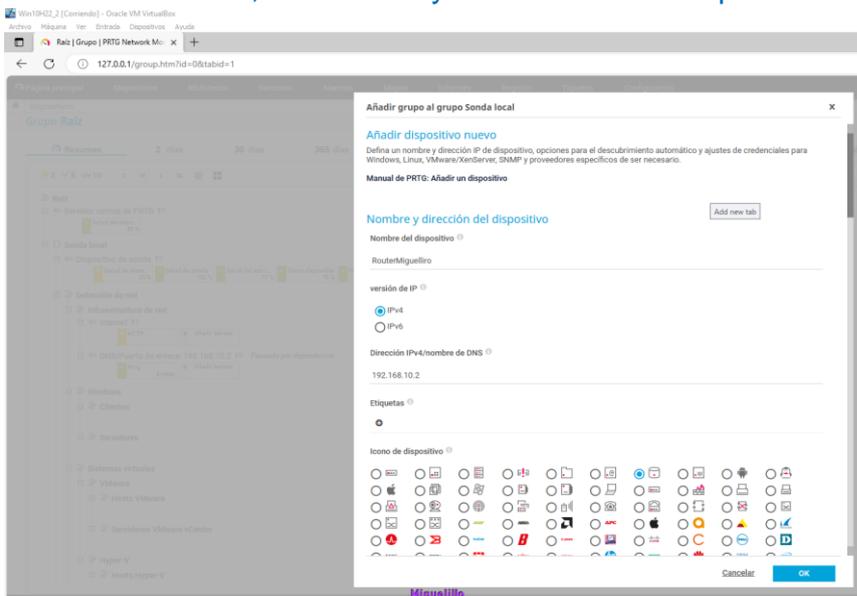
Vamos a **Dispositivos** → **Añadir Grupo** y creamos un grupo



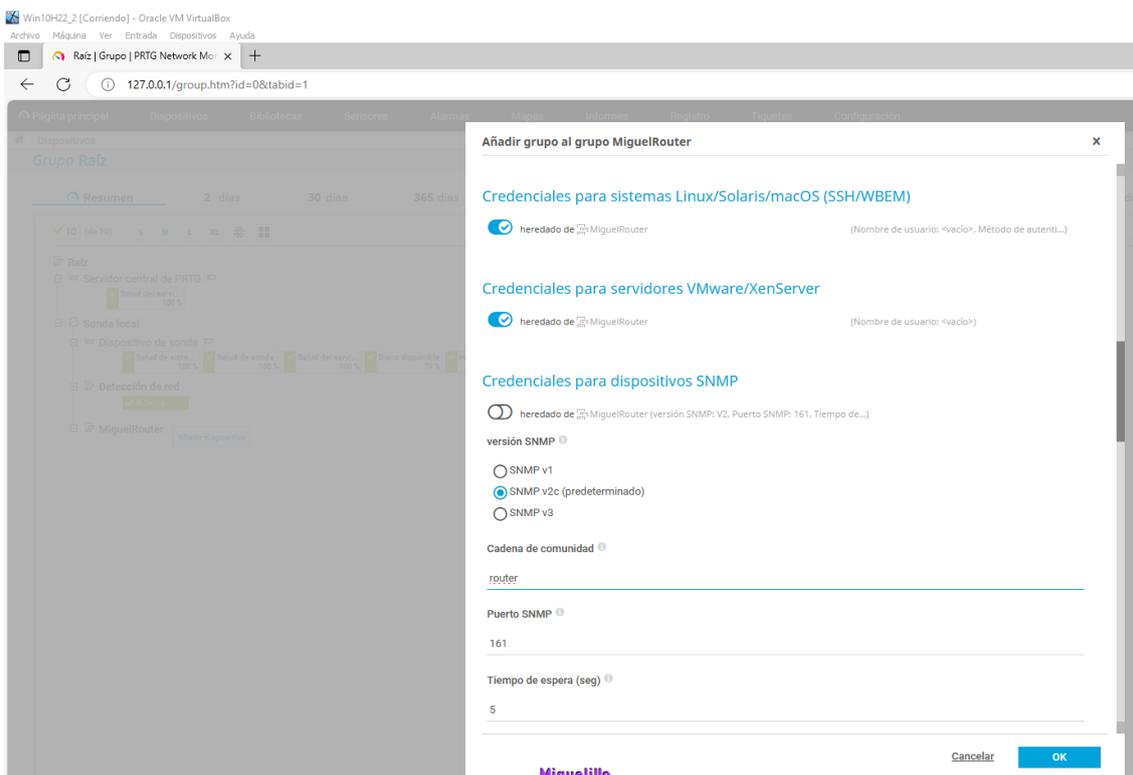
Vamos a dispositivos a los grupos que hemos hecho y clicamos en **Añadir dispositivo**



Introducimos IP, nombre y un icono si queremos para reconocerlo



Asignamos las credenciales del SNMP



Vemos que ha hecho conectividad

The screenshot shows the PRTG Network Monitor interface for a device named 'MiguelRouter'. The interface is in Spanish and displays various system and network sensors. A red box highlights the 'router' section, which contains several sensors with green checkmarks, indicating they are operational and connected. The sensors include:

- Ping: 5 msec
- (001) FastEtHe...: 0.02 Mbit/s
- (002) Serial1/0...: 0 Mbit/s
- (003) Serial1/1...: 0 Mbit/s
- (004) Serial1/2...: 0 Mbit/s
- (005) Serial1/3...: 0 Mbit/s
- (006) FastEtHe...: 0.02 Mbit/s
- Tiempo de acti...: 3 h 14 m
- System Health ...: 0 %
- System Health ...: 0.28 GB
- System Health ...: Normal
- System Health ...: 22
- System Health ...: Normal
- Carga de proc...: 0 %
- Añadir sensor

The interface also shows a navigation menu at the top with options like 'Página principal', 'Dispositivos', 'Bibliotecas', 'Sensores', 'Alarmas', 'Mapas', 'Informes', 'Registro', 'Tiquetes', and 'Configuración'. The status bar at the bottom indicates the user is 'PAESSLER' and the system is 'Administrador de sistema PRTG'.

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

No.	Time	Source	Destination	Protocol	Length	Info
1674	635.893068	192.168.10.2	192.168.10.10	ICMP	70	Destination unreachable (Port unreachable)
1673	635.884174	192.168.10.10	192.168.10.2	SNMP	84	get-request 1.3.6.1.2.1.17.1.3.0
1672	635.738698	192.168.10.2	192.168.10.10	ICMP	70	Destination unreachable (Port unreachable)
1671	635.736302	192.168.10.10	192.168.10.2	SNMP	82	get-next-request 1.3.6.1.2.1.43.1.0
1670	635.614493	192.168.10.2	192.168.10.10	ICMP	70	Destination unreachable (Port unreachable)
1669	635.606701	192.168.10.10	192.168.10.2	SNMP	82	get-next-request 1.3.6.1.2.1.43.1.0
200648	6924.091322	192.168.10.10	192.168.10.2	SNMP	133	get-request 1.3.6.1.2.1.31.1.1.1.6.6 1.3.6.1.2.1.31.1.1
200649	6924.091608	192.168.10.10	192.168.10.2	SNMP	81	get-next-request 1.3.6.1.2.1.33
200650	6924.094667	192.168.10.2	192.168.10.10	SNMP	159	get-response 1.3.6.1.2.1.31.1.1.1.6.6 1.3.6.1.2.1.31.1.1
200651	6924.094756	192.168.10.2	192.168.10.10	SNMP	87	get-response 1.3.6.1.2.1.34.1.1.2.0
200652	6925.089389	192.168.10.10	192.168.10.2	SNMP	202	get-request 1.3.6.1.2.1.33.1.2.1.0 1.3.6.1.2.1.33.1.2.1
200653	6925.091975	192.168.10.2	192.168.10.10	SNMP	205	get-response 1.3.6.1.2.1.33.1.2.1.0 1.3.6.1.2.1.33.1.2.1
200654	6926.100762	192.168.10.10	192.168.10.2	SNMP	86	get-request 1.3.6.1.4.1.3224.16.1.2.0
200655	6926.109483	192.168.10.2	192.168.10.10	SNMP	86	get-response 1.3.6.1.4.1.3224.16.1.2.0
200656	6927.112400	192.168.10.10	192.168.10.2	SNMP	89	get-request 1.3.6.1.4.1.9.9.109.1.1.1.4.1
200657	6927.113796	192.168.10.10	192.168.10.2	SNMP	85	get-request 1.3.6.1.4.1.6574.1.1.0
200658	6927.118357	192.168.10.2	192.168.10.10	SNMP	90	get-response 1.3.6.1.4.1.9.9.109.1.1.1.4.1
200659	6927.118420	192.168.10.2	192.168.10.10	SNMP	85	get-response 1.3.6.1.4.1.6574.1.1.0
200713	6949.101275	192.168.10.10	192.168.10.2	SNMP	83	get-request 1.3.6.1.2.1.1.3.0
200714	6949.105110	192.168.10.2	192.168.10.10	SNMP	86	get-response 1.3.6.1.2.1.1.3.0
200716	6952.116323	192.168.10.10	192.168.10.2	SNMP	133	get-request 1.3.6.1.2.1.31.1.1.1.6.1 1.3.6.1.2.1.31.1.1
200717	6952.124510	192.168.10.2	192.168.10.10	SNMP	159	get-response 1.3.6.1.2.1.31.1.1.1.6.1 1.3.6.1.2.1.31.1.1
200718	6955.100088	192.168.10.2	192.168.10.2	SNMP	131	get-request 1.3.6.1.2.1.2.2.1.10.2 1.3.6.1.2.1.2.2.1.1
200719	6955.108093	192.168.10.2	192.168.10.10	SNMP	145	get-response 1.3.6.1.2.1.2.2.1.10.2 1.3.6.1.2.1.2.2.1.1

Frame 200646: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface...  
 Ethernet II, Src: ca:01:2a:b4:00:00 (ca:01:2a:b4:00:00), Dst: PcsCompu\_bb:2e:1a:08...  
 Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.10.10  
 User Datagram Protocol, Src Port: 161, Dst Port: 50258  
 Simple Network Management Protocol  
 version: v2c (1)  
 community: router  
 data: get-response (2)  
 get-response  
 request-id: 25125

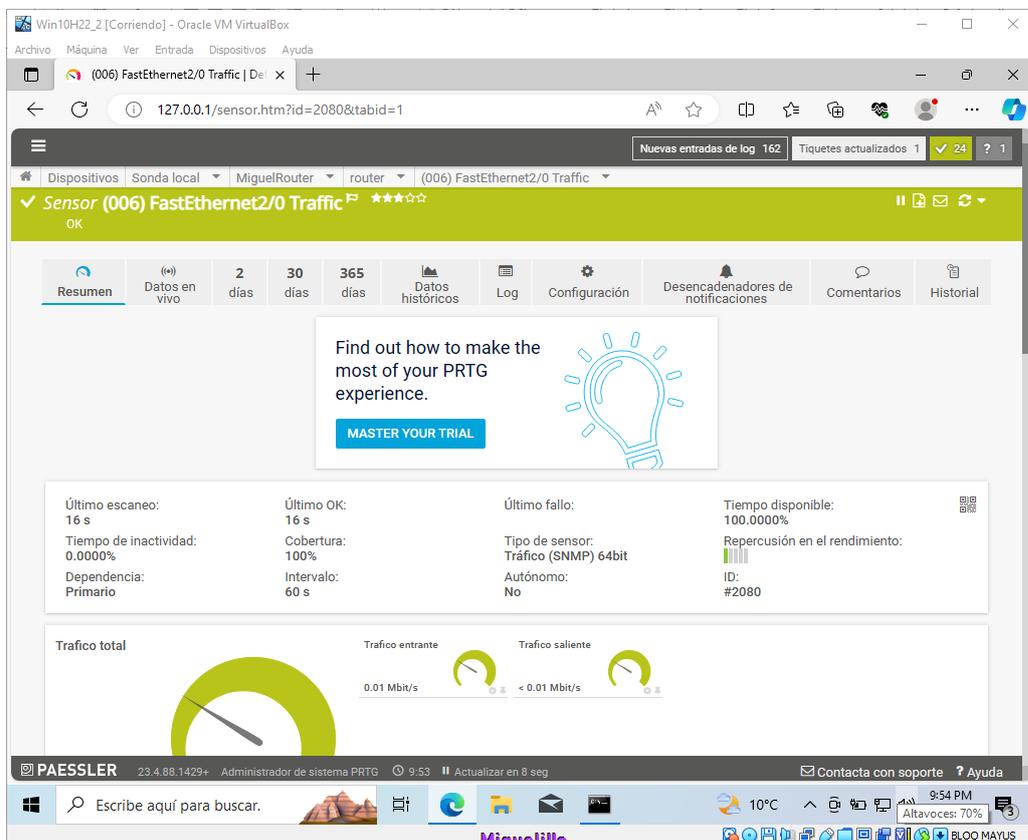
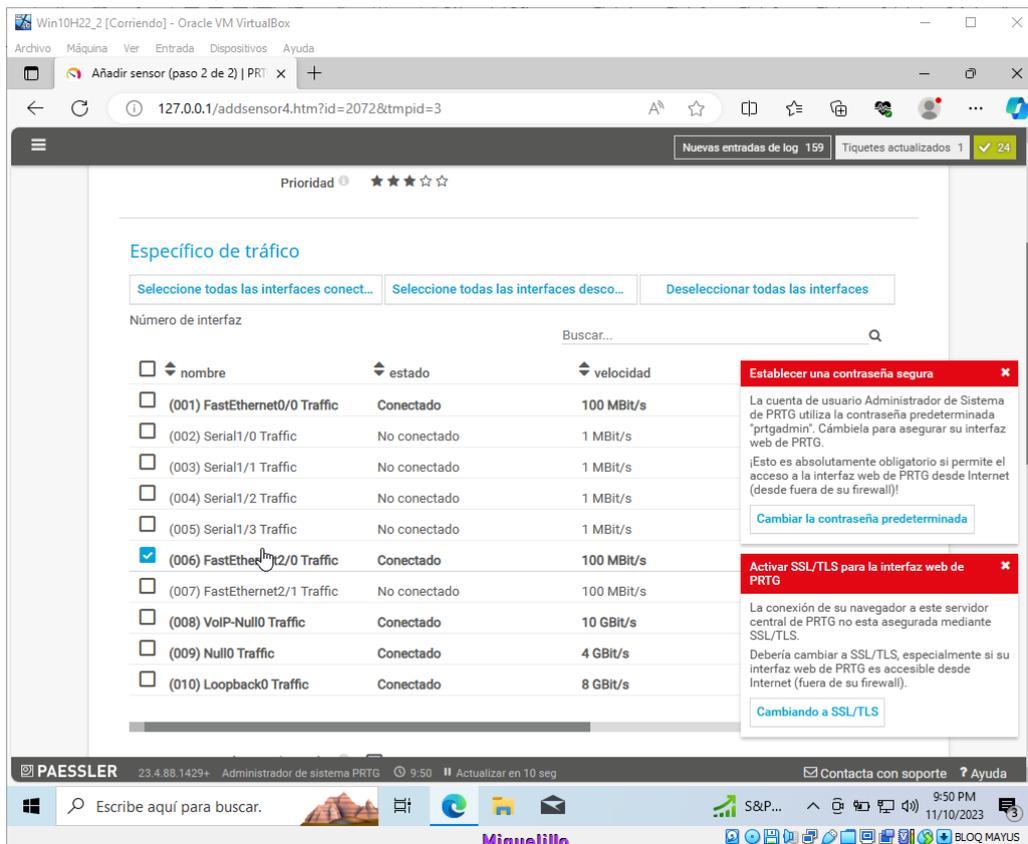
Clicamos en Añadir un sensor y seleccionamos SNMP

¿Que monitorear?  
 Disponibilidad/tiempo de OK  Uso de CPU  Parámetros de hardware  ¿Tipo de sistema objetivo?  
 Ancho de banda/tráfico  Uso de disco  Infraestructura de red  Windows  Servidores (almacenamiento/servicio) Servicios de nube  
 Velocidad/Rendimiento  Uso de memoria  Sensores personalizados  Linux/macOS  Servidor de correo  
 Sistema de Virtualización  Base de datos

¿Tecnología usada?  
 Ping  HTTP  PowerShell  SNMP  SSH  Receptor de mensajes Push  WMI  Sniffer de paquetes  PRTG Cloud  Contadores de rendimiento  Protocolos de flujo

Tipos de sensores más usados  
 Tráfico (SNMP)  
 Monitorea ancho de banda y tráfico de servidores, equipos, switches, etc. via SNMP

Seleccionamos el interfaz del que queremos ver el tráfico



Podemos verlo en vivo clicando Datos en vivo

Win10H22\_2 [Corriendo] - Oracle VM VirtualBox

127.0.0.1/sensor.htm?id=2080&tabid=2

Nuevas entradas de log 163 Tiquetes actualizados 1

Dispositivos Sonda local MiguelRouter router (006) FastEthernet2/0 Traffic

✓ Sensor (006) FastEthernet2/0 Traffic OK

Resumen Datos en vivo 2 días 30 días 365 días Datos históricos Log Configuración Desencadenadores de notificaciones Comentarios Historial

Último escaneo: 24 s	Último OK: 24 s	Último fallo:	Tiempo disponible: 100.0000%
Tiempo de inactividad: 0.0000%	Cobertura: 100%	Tipo de sensor: Tráfico (SNMP) 64bit	Repercusión en el rendimiento:
Dependencia: Primario	Intervalo: 60 s	Autónomo: No	ID: #2080

Gráfico de tráfico (Mbit/s) vs tiempo.

PAESSLER 23.4.88.1429+ Administrador de sistema PRTG 9:54 Actualizar en 5 seg

9:55 PM 11/10/2023

También podemos consultar los logs

Win10H22\_2 [Corriendo] - Oracle VM VirtualBox

127.0.0.1/sensor.htm?id=2080&tabid=7

Nuevas entradas de log 163 Tiquetes actualizados 1

Dispositivos Sonda local MiguelRouter router (006) FastEthernet2/0 Traffic

✓ Sensor (006) FastEthernet2/0 Traffic OK

Resumen Datos en vivo 2 días 30 días 365 días Datos históricos Log Configuración Desencadenadores de notificaciones Comentarios Historial

Log

Elementos: 50

Mostrar filtros

Fecha Hora	Sensor	Estado	Mensaje
11/10/2023 9:37:39 PM	(006) FastEthernet2/0 Traffic	OK	0.01 Mbit/s
11/10/2023 9:35:44 PM	(006) FastEthernet2/0 Tr...	Descon...	Aun no hay datos
11/10/2023 9:35:44 PM	(006) FastEthernet2/0 Tr...	Generado	Consulte el historial del objeto para obtener detalles.

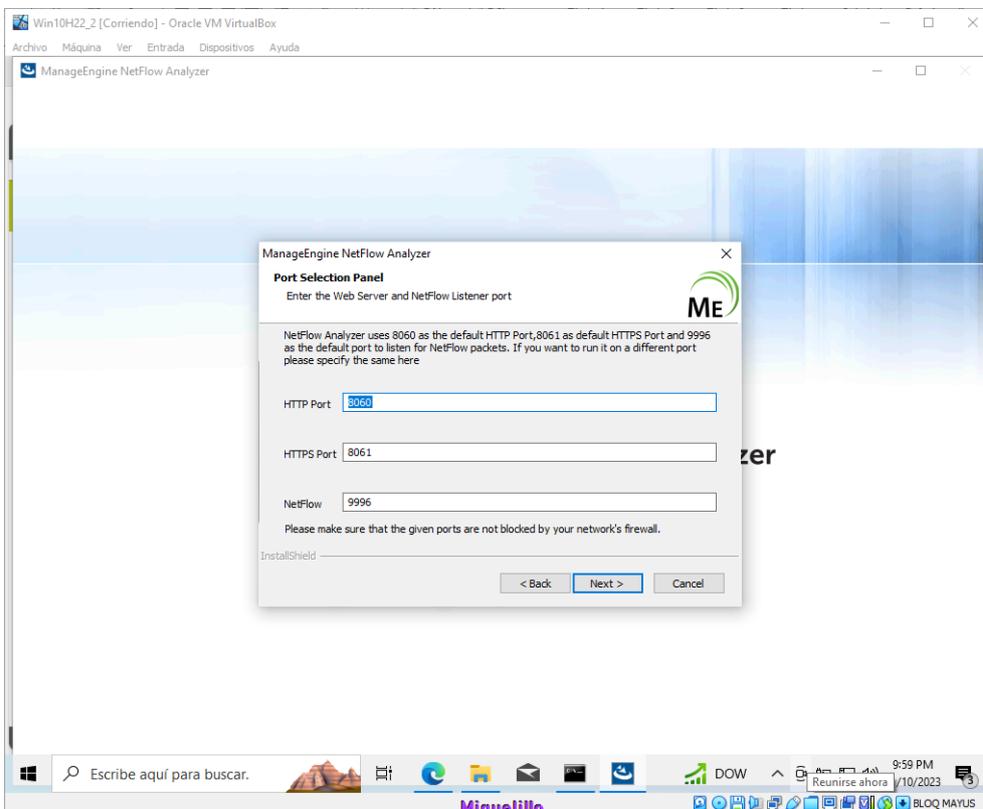
1 a 3 >

127.0.0.1/sensor.htm?id=2080 429+ Administrador de sistema PRTG 9:56 Actualizar en 24 seg

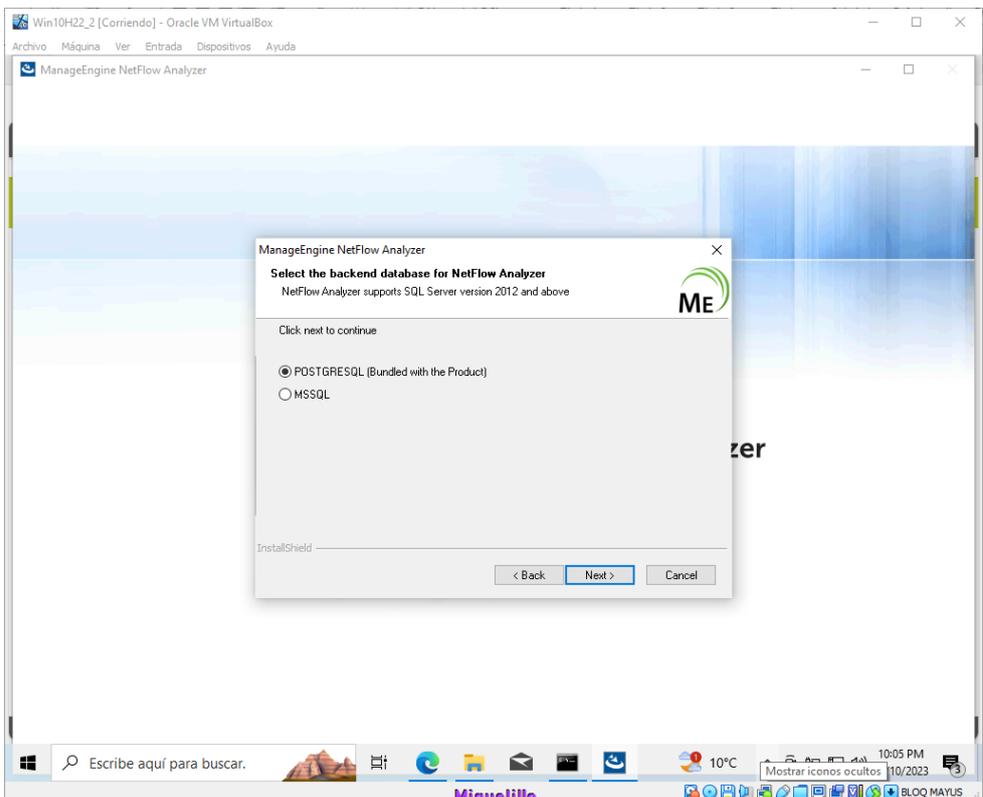
9:56 PM 11/10/2023

# NETFLOW usaré netflow analyzer

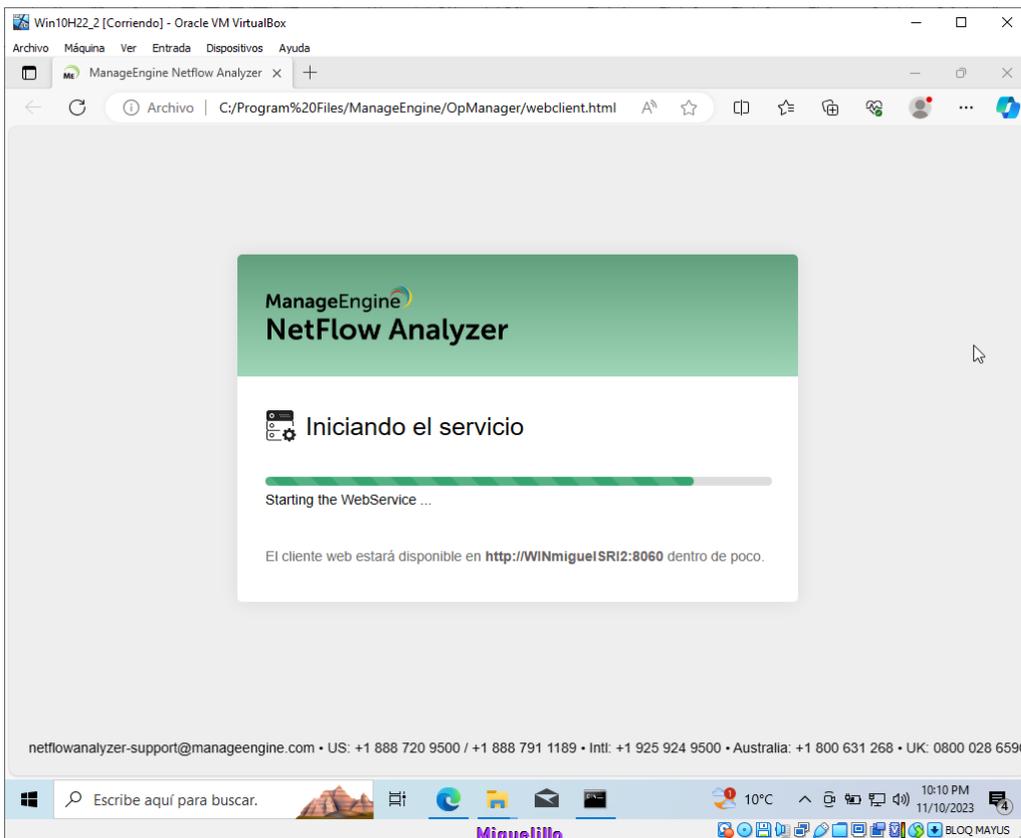
Configuramos los puertos



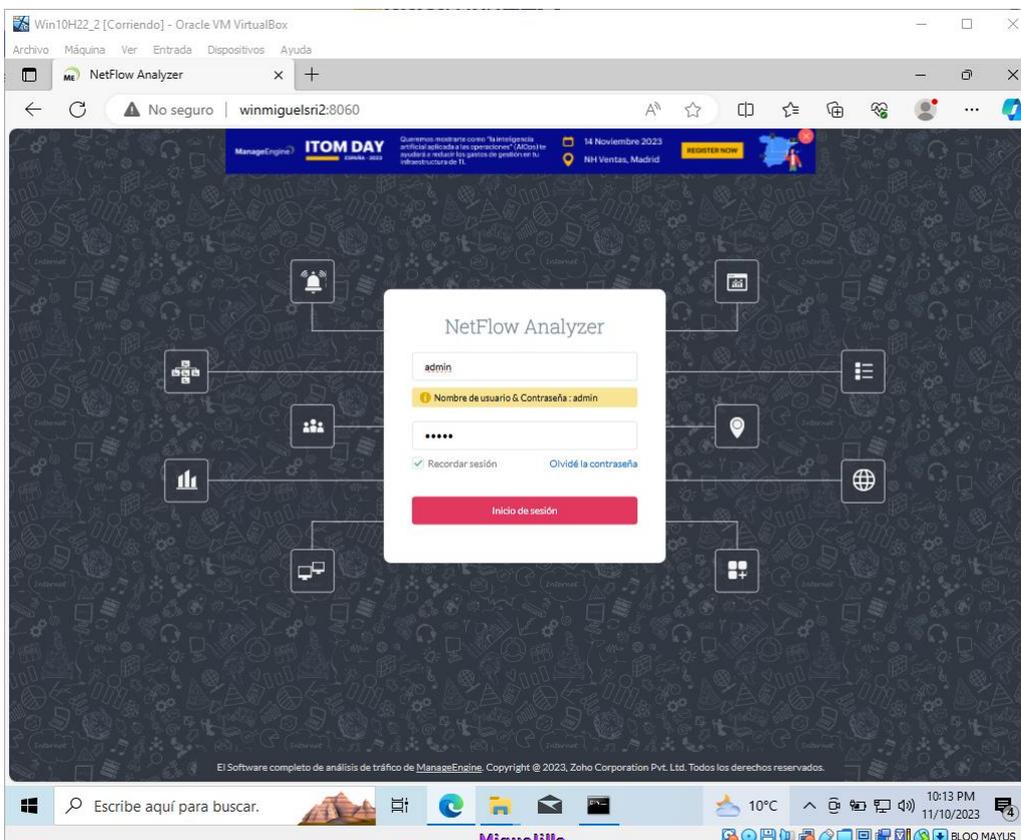
Usaremos POSTGRESQL



Esperamos a que inicie



Iniciamos sesión con las credenciales por defecto



Configuramos al router para vincularlo con el servidor netflow

```
miguelliroSRI(config)#interface fa0/0
miguelliroSRI(config-if)#ip flow ingress
miguelliroSRI(config-if)#ip flow egress
miguelliroSRI(config-if)#ip flow-export destination 192.168.10.10 9996
miguelliroSRI(config)#ip flow-export version 9
miguelliroSRI(config)#
```

Podemos ver la comunicación en el wireshark por el puerto 9996

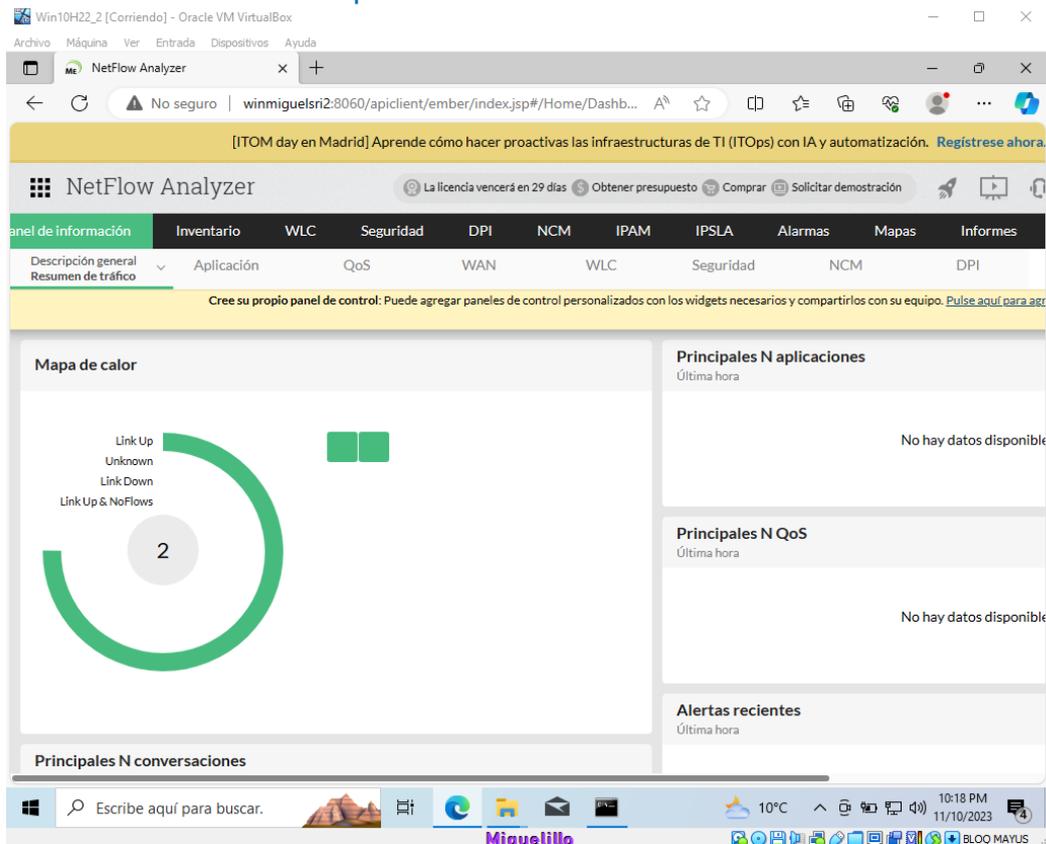
udp.port == 9996

No.	Time	Source	Destination	Protocol	Length	Info
248200	9407.240963	192.168.10.2	192.168.10.10	CFLOW	1006	total: 18 (v9) records Obs-Domain-ID= 0 [Data-Templ
248145	9395.233989	192.168.10.2	192.168.10.10	CFLOW	1198	total: 22 (v9) records Obs-Domain-ID= 0 [Data-Templ
248051	9384.241747	192.168.10.2	192.168.10.10	CFLOW	1486	total: 28 (v9) records Obs-Domain-ID= 0 [Data-Templ
246130	9361.232288	192.168.10.2	192.168.10.10	CFLOW	478	total: 7 (v9) records Obs-Domain-ID= 0 [Data-Templa
246023	9349.241468	192.168.10.2	192.168.10.10	CFLOW	1006	total: 18 (v9) records Obs-Domain-ID= 0 [Data-Templ
245974	9335.239368	192.168.10.2	192.168.10.10	CFLOW	862	total: 15 (v9) records Obs-Domain-ID= 0 [Data-Templ
245766	9316.238353	192.168.10.2	192.168.10.10	CFLOW	430	total: 6 (v9) records Obs-Domain-ID= 0 [Data-Templa
245646	9304.240490	192.168.10.2	192.168.10.10	CFLOW	622	total: 10 (v9) records Obs-Domain-ID= 0 [Data-Templ
245614	9292.237739	192.168.10.2	192.168.10.10	CFLOW	434	total: 6 (v9) records Obs-Domain-ID= 0 [Data-Templa
245574	9280.076333	192.168.10.2	192.168.10.10	CFLOW	298	total: 5 (v1) flows
245555	9277.246528	192.168.10.2	192.168.10.10	CFLOW	346	total: 6 (v1) flows
248341	9421.241479	192.168.10.2	192.168.10.10	CFLOW	1054	total: 19 (v9) records Obs-Domain-ID= 0 [Data-Templ
248441	9433.234208	192.168.10.2	192.168.10.10	CFLOW	450	total: 8 (v9) records Obs-Domain-ID= 0 [Data:257]
248733	9445.239656	192.168.10.2	192.168.10.10	CFLOW	690	total: 13 (v9) records Obs-Domain-ID= 0 [Data:257]
249622	9457.241004	192.168.10.2	192.168.10.10	CFLOW	1266	total: 25 (v9) records Obs-Domain-ID= 0 [Data:257]

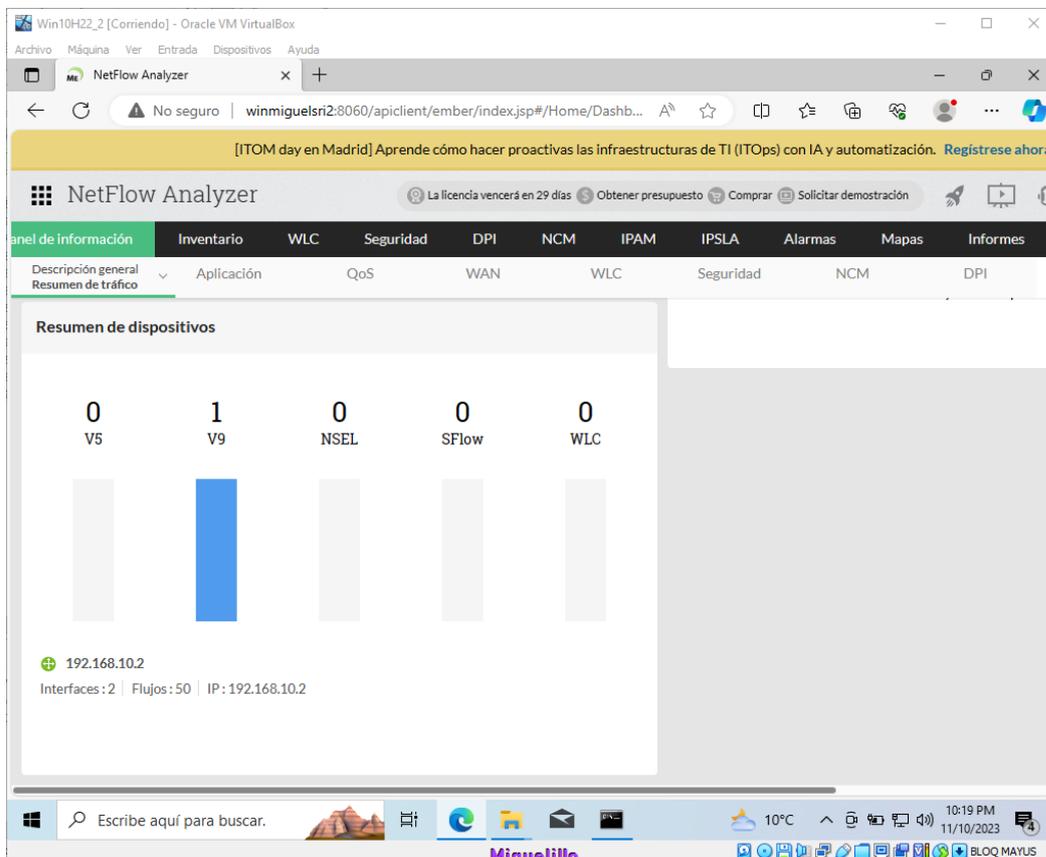
> Frame 248200: 1006 bytes on wire (8048 bits), 1006 bytes captured (8048 bits) on inter  
 > Ethernet II, Src: ca:01:2a:b4:00:00 (ca:01:2a:b4:00:00), Dst: PcsCompu\_bb:2e:1a (08:06:27:bb:2e:1a)  
 > Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.10.10  
 > User Datagram Protocol, Src Port: 54913, Dst Port: 9996  
 > Cisco NetFlow/IPFIX  
 Version: 9  
 Count: 18  
 SysUptime: 14070.376000000 seconds  
 > Timestamp: Nov 10, 2023 23:19:01.000000000 Hora estándar romance  
 FlowSequence: 10  
 SourceId: 0  
 > FlowSet 1 [id=0] (Data Template): 257,256  
 > FlowSet 2 [id=257] (16 flows)

Paquetes: 250116 · Mostrado: 17 (0.0%) Perfil: Default

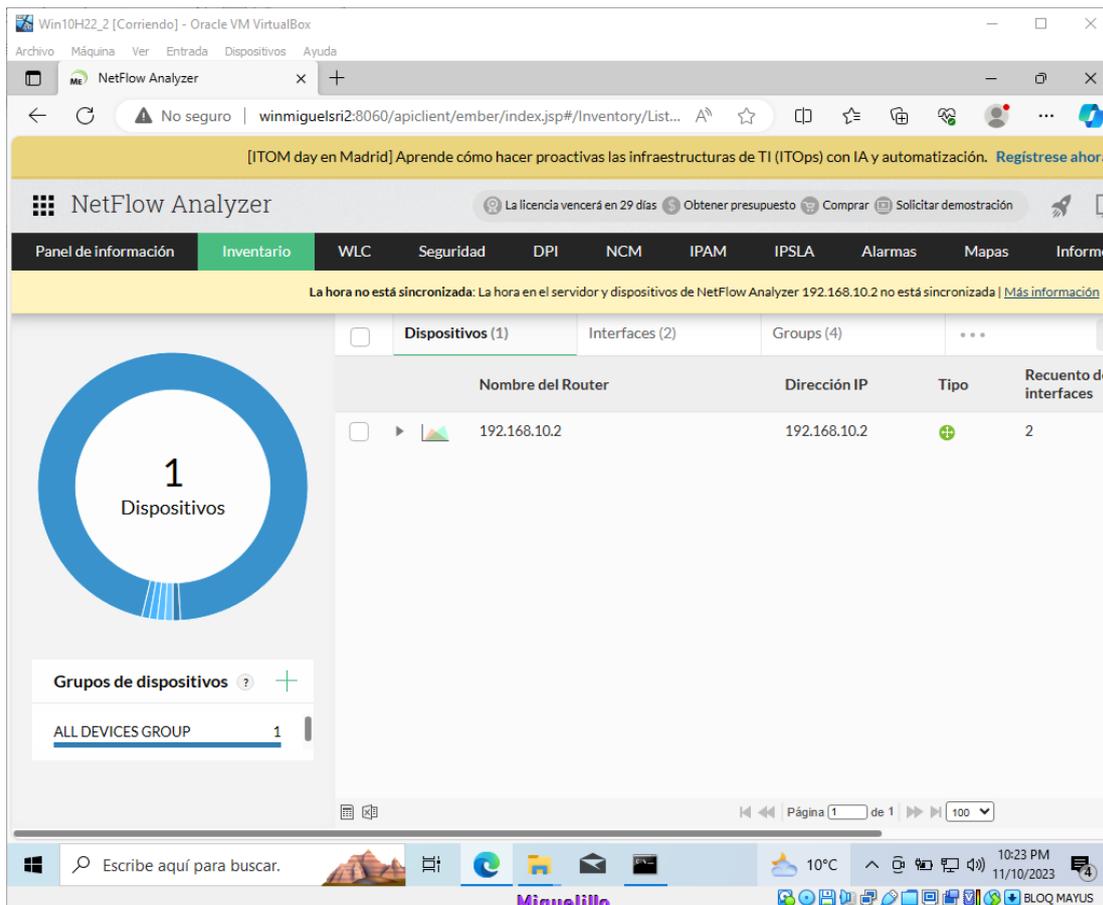
Podemos ver en el panel de información información sobre el router



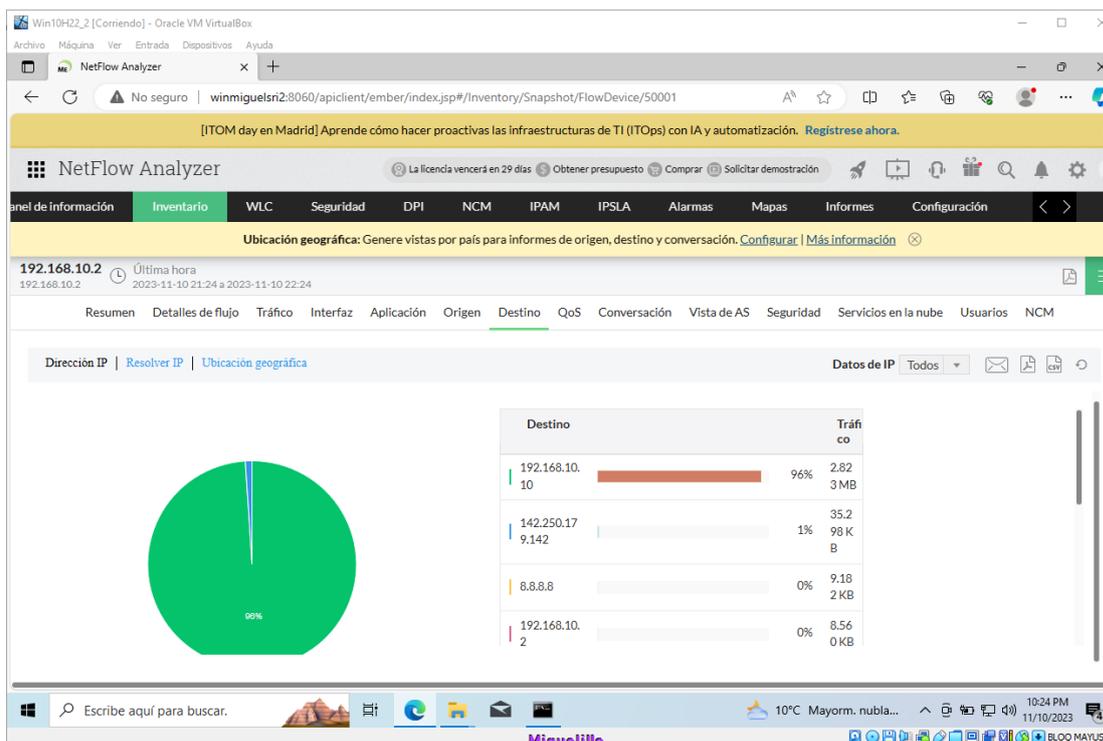
Vemos la IP del router interfaces avivas la versión del netflow



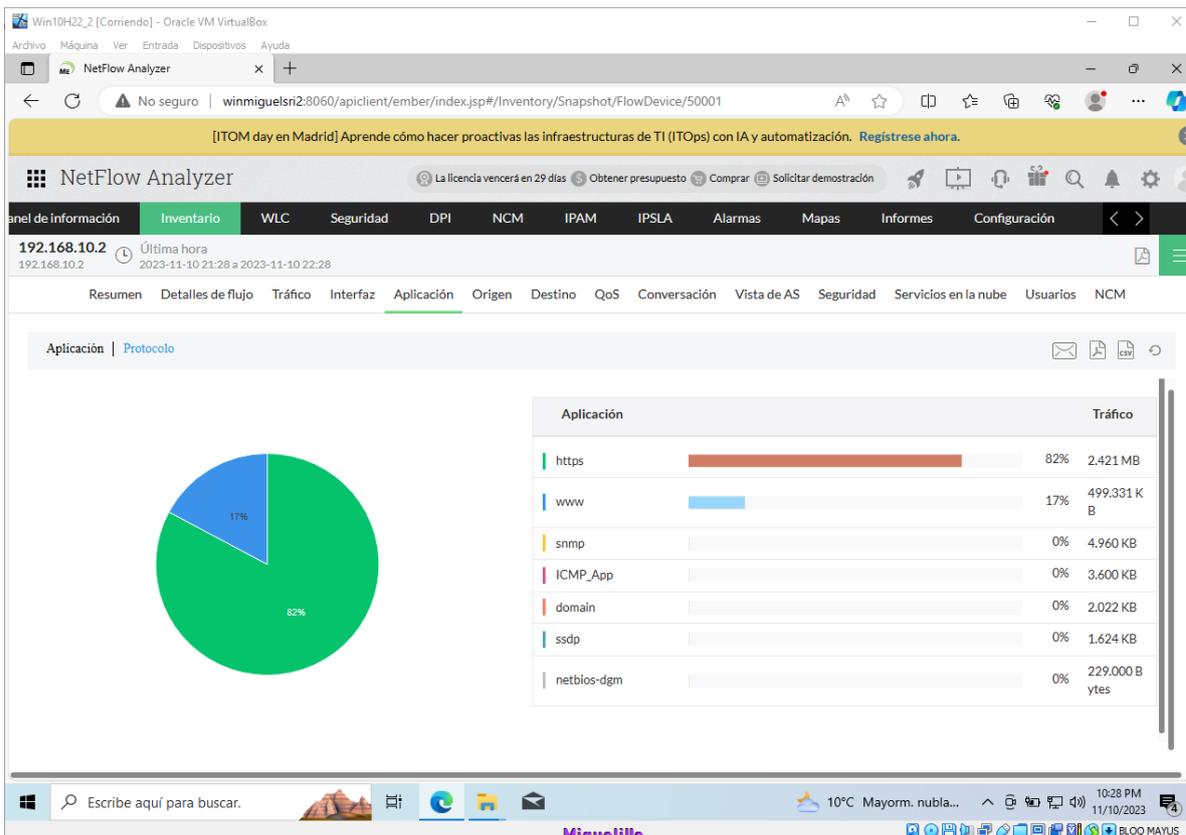
### En Inventario podemos ver los dispositivos



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



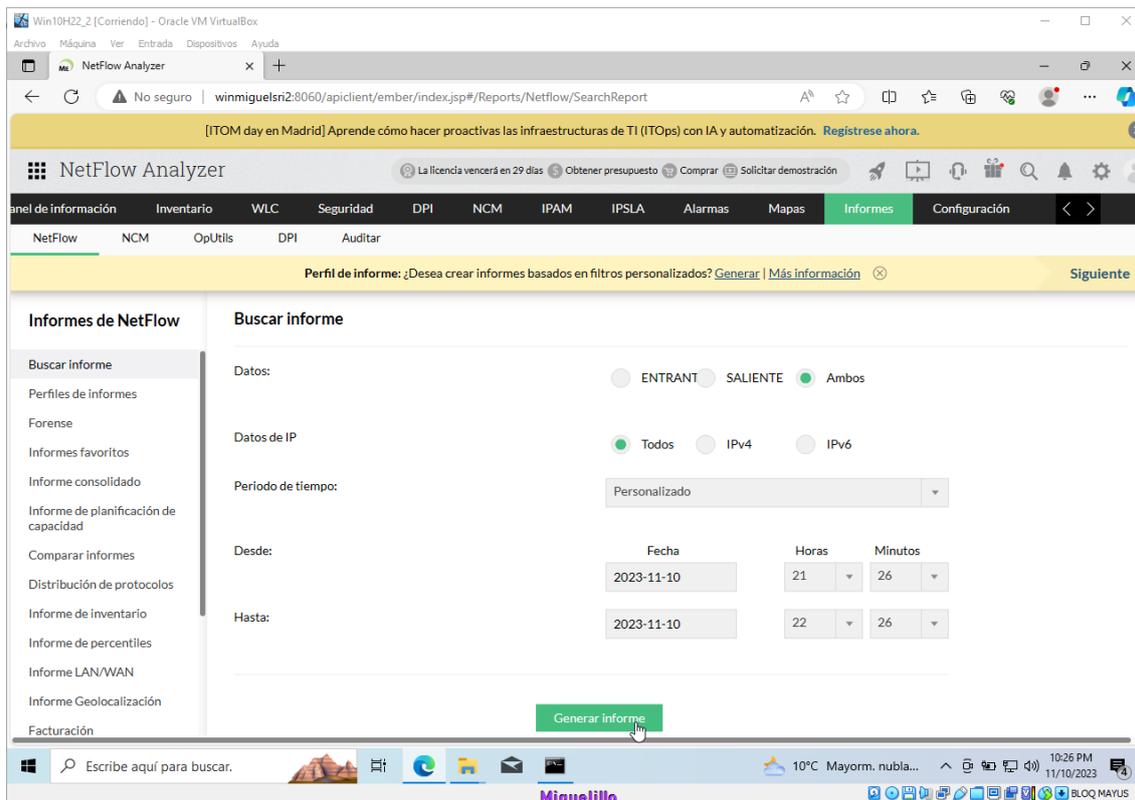
Podemos ver los protocolos más usados para comunicarse



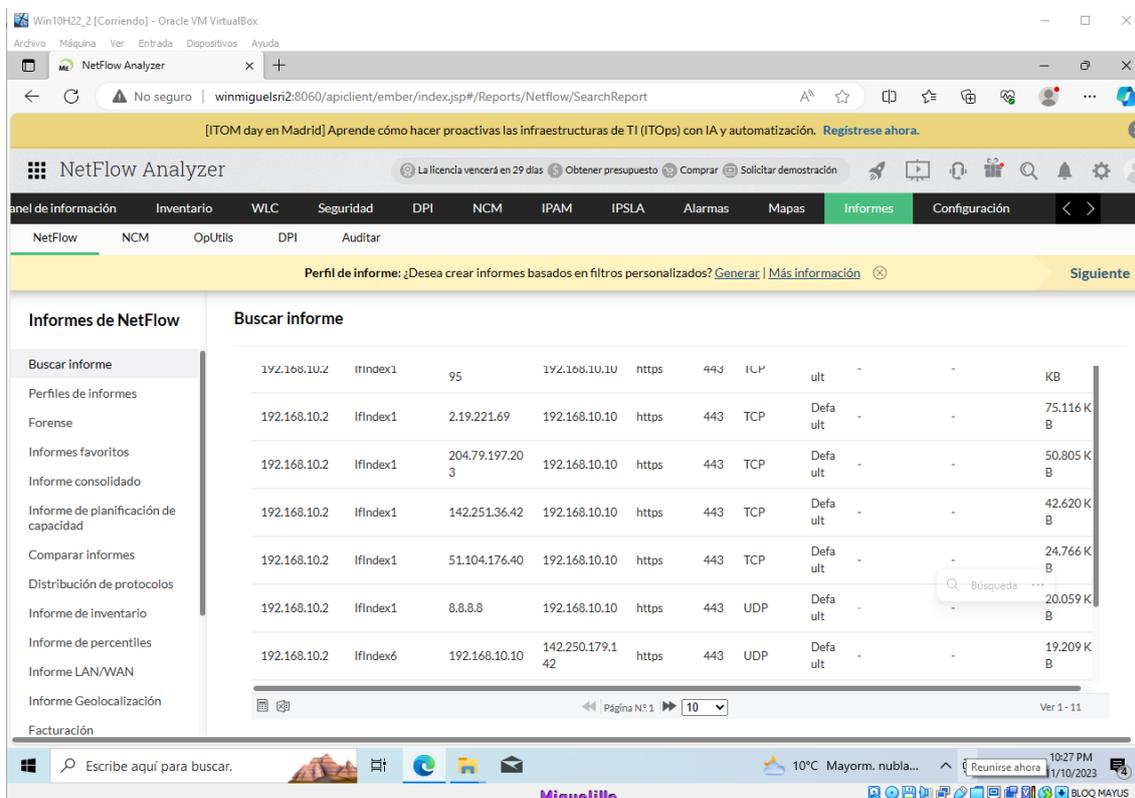
El trafico de IPs

Origen	Destino	Aplicación	Tráfico
23.33.143.32	192.168.10.10	www	9.795 MB
142.250.179.142	192.168.10.10	https	1.730 MB
142.251.39.100	192.168.10.10	www	1.186 MB
192.168.10.10	13.89.178.27	https	961.461 KB
2.20.253.140	192.168.10.10	https	356.205 KB
172.217.168.195	192.168.10.10	https	270.868 KB
204.79.197.203	192.168.10.10	https	264.682 KB
204.79.197.239	192.168.10.10	https	166.214 KB
13.89.178.27	192.168.10.10	https	159.804 KB

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



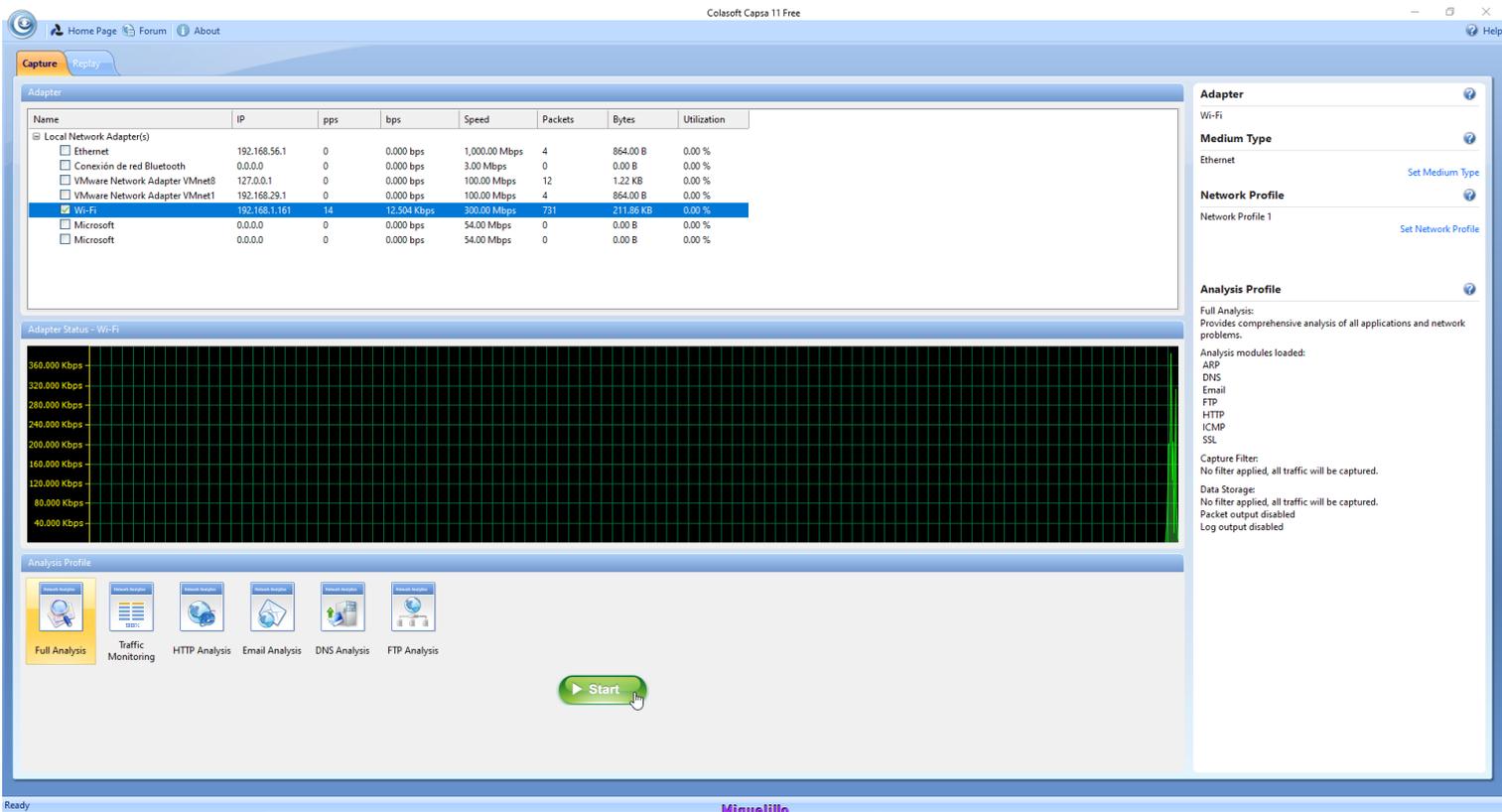
El informe generado:



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 geolocalización

The screenshot shows the 'IP Endpoint' table in Wireshark. The table lists various IP addresses, their geolocations, and associated network statistics. A red box highlights a specific set of local IP addresses.

Name	Geolocation	Bytes	Packets	bps	pps	Bytes Received	Packets Received	Bytes Sent	Packets Sent	Sent/Receive
192.168.1.1	Local	20.15 KB	43	38.808 Kbps	10	0.00 B	0	20.15 KB	43	20
192.168.1.197	Local	14.22 KB	102	3.152 Kbps	3	6.79 KB	63	7.43 KB	39	6
192.168.1.94	Local	6.17 KB	41	1.232 Kbps	1	0.00 B	0	6.17 KB	41	1
192.168.1.239	Local	399.00 B	6	664.000 bps	1	0.00 B	0	399.00 B	6	6
192.168.1.255	Local	180.00 B	2	720.000 bps	1	180.00 B	2	0.00 B	0	0
<b>Internet Addresses</b>										
United Arab Emirates	United Arab Emirates	4.08 MB	5,139	2.928 Kbps	5	713.67 KB	2,096	3.39 MB	3,043	
2.20.71.134	United Arab Emirates	3.11 MB	3,020	8.161 Mbps	921	51.60 KB	899	3.05 MB	2,121	
2.20.71.141	United Arab Emirates	3.11 MB	3,018	17.856 Mbps	2,097	51.54 KB	898	3.05 MB	2,120	
United States	United States	129.00 B	2	0.000 bps	0	59.00 B	1	70.00 B	1	
United States	United States	860.43 KB	1,732	2.928 Kbps	5	634.45 KB	1,009	225.98 KB	723	
China	China	110.01 KB	250	922.000 bps	2	13.95 KB	120	96.06 KB	130	
www.colossof.com	United States	110.01 KB	250	928.000 bps	2	13.95 KB	120	96.06 KB	130	
United States	United States	19.52 KB	51	13.160 Kbps	7	5.65 KB	24	13.86 KB	27	
Ireland	Ireland	9.33 KB	65	1.016 Kbps	1	6.64 KB	33	2.69 KB	32	
United States	United States	6.65 KB	19	472.000 bps	1	1.33 KB	10	5.51 KB	9	
www.google.es	United States	6.72 KB	17	48.880 Kbps	14	1.28 KB	9	5.44 KB	8	
216.58.214.14	United States	129.00 B	2	472.000 bps	1	59.00 B	1	70.00 B	1	
185.199.108.153	Local	129.00 B	2	0.000 bps	0	59.00 B	1	70.00 B	1	
Multicast Addresses		21.42 KB	54	664.000 bps	1	21.42 KB	54	0.00 B	0	

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

The screenshot shows the 'Matrix' view in Wireshark, titled 'Top100 IP Conversation (Protocol Explorer)'. It displays a complex network graph where nodes represent IP addresses and lines represent communication flows between them. The nodes are arranged in a circular pattern, with a central node and many peripheral nodes connected to it.

Podemos ver los paquetes que se envían

No.	Absolute Time	Source	Source Geolocation	Destination	Destination Geolocation	Protocol	Size	Payload	Decode	Summary
23508	23:28:45.881185000	35.186.224.254:43	United States	DESKTOP-3954N4.local:31161	Local	TCP	64	-	-	SeqNurr
23509	23:28:45.884530000	02:EB:D8:0D:FB:58	United States	FF:FF:FF:FF:FF:FF	Local	ARP Request	46	-	-	Who has
23510	23:28:45.897537000	35.186.224.254:43	United States	DESKTOP-3954N4.local:65017	Local	HTTPS	73	27	-	HTTIPS st
23511	23:28:45.925076000	35.186.224.254:43	United States	DESKTOP-3954N4.local:65017	Local	HTTPS	70	24	-	HTTIPS st
23512	23:28:45.925278000	DESKTOP-3954N4.local:65017	Local	35.186.224.254:43	United States	HTTPS	77	31	-	HTTIPS st
23513	23:28:46.039394000	35.186.224.254:43	United States	DESKTOP-3954N4.local:65017	Local	HTTPS	216	170	-	HTTIPS st
23514	23:28:46.039773000	DESKTOP-3954N4.local:65017	Local	35.186.224.254:43	United States	HTTPS	81	35	-	HTTIPS st
23515	23:28:46.091302000	DESKTOP-3954N4.local:32262	Local	35.186.224.254:43	United States	HTTPS	59	1	-	TCP ket
23516	23:28:46.137175000	35.186.224.254:43	United States	DESKTOP-3954N4.local:65017	Local	HTTPS	70	24	-	HTTIPS st
23517	23:28:46.155538000	35.186.224.254:43	United States	DESKTOP-3954N4.local:28442	Local	TCP	70	0	-	[Dup AC
23518	23:28:46.204452000	162.159.133.234:443	United States	DESKTOP-3954N4.local:28442	Local	HTTPS	108	50	-	Applicat
23519	23:28:46.247339000	DESKTOP-3954N4.local:28442	Local	162.159.133.234:443	United States	TCP	58	0	-	SeqNurr
23520	23:28:46.293982000	DESKTOP-3954N4.local:31347	Local	192.168.1.197:8009	Local	TCP	168	110	-	SeqNurr
23521	23:28:46.293985000	DESKTOP-3954N4.local:31325	Local	192.168.1.197:8009	Local	TCP	168	110	-	SeqNurr
23522	23:28:46.293986000	DESKTOP-3954N4.local:31337	Local	192.168.1.197:8009	Local	TCP	168	110	-	SeqNurr
23523	23:28:46.403220000	192.168.1.197:8009	Local	DESKTOP-3954N4.local:31347	Local	TCP	168	110	-	SeqNurr
23524	23:28:46.403220000	192.168.1.197:8009	Local	DESKTOP-3954N4.local:31337	Local	TCP	168	110	-	SeqNurr
23525	23:28:46.403220000	192.168.1.197:8009	Local	DESKTOP-3954N4.local:31325	Local	TCP	168	110	-	SeqNurr
23526	23:28:46.449693000	DESKTOP-3954N4.local:31347	Local	192.168.1.197:8009	Local	TCP	58	0	-	SeqNurr
23527	23:28:46.449694000	DESKTOP-3954N4.local:31337	Local	192.168.1.197:8009	Local	TCP	58	0	-	SeqNurr

Protocolos más utilizados

Name	Bytes	Packets	bps	pps	Bytes%	Packets%
Ethernet II	13.44 MB	27,021	13,184 Kbps	200	100.000%	100.000%
IP	13.38 MB	26,084	12,672 Kbps	19	99.566%	96.532%
TCP	10.52 MB	17,170	5,592 Kbps	8	79.072%	63.542%
SSL	9.73 MB	8,045	3,640 Kbps	4	72.423%	29.773%
HTTP	284.21 KB	478	19,344 Kbps	5	2.066%	1.769%
DNS	22.95 KB	194	4,760 Kbps	4	0.167%	0.718%
DNS Query	15.85 KB	146	3,624 Kbps	3	0.115%	0.540%
DNS Response	7.10 KB	48	1,136 Kbps	1	0.052%	0.178%
Private	1.33 KB	23	472.000 bps	1	0.010%	0.085%
UDP	2.75 MB	8,852	7,080 Kbps	11	20.447%	32.760%
SSL	2.38 MB	7,551	2,352 Kbps	4	17.730%	27.945%
SSDP	227.68 KB	523	1,768 Kbps	1	1.655%	1.936%
MDNS	20.84 KB	71	3,592 Kbps	1	0.151%	0.263%
DNS	7.70 KB	68	6,024 Kbps	6	0.056%	0.252%
DNS Response	5.63 KB	34	3,816 Kbps	3	0.037%	0.126%
DNS Query	2.07 KB	34	2,208 Kbps	3	0.019%	0.126%
MNPD	1.39 KB	9	1,264 Kbps	1	0.010%	0.033%
BOOTP	692.00 B	2	0.000 bps	0	0.005%	0.007%
DHCP	692.00 B	2	0.000 bps	0	0.005%	0.007%
NBGM	247.00 B	1	0.000 bps	0	0.002%	0.004%
SMB	247.00 B	1	0.000 bps	0	0.002%	0.004%
SMB MAILS...	247.00 B	1	0.000 bps	0	0.002%	0.004%
LLMNR	79.00 B	1	0.000 bps	0	0.001%	0.004%
ICMP	3.48 KB	6	4,752 Kbps	1	0.025%	0.022%