

Manual de Uso del Sistema de Monitoreo de Flujo de Red

Manual de uso y configuración

Universidad Politecnica de Victoria



[Marzo 2024]

Índice

1. Introducción	5
1.1. Antecedentes	5
1.2. Definición del problema y justificación del proyecto	5
1.3. Objetivo General	5
1.4. Objetivos Particulares	6
1.5. Alcances y Limitaciones del Proyecto	6
2. Requisitos del Sistema	7
2.1. Requisitos de Hardware	7
2.1.1. Para la Raspberry Pi	7
2.1.2. Para la ESP32	7
2.2. Requisitos de Software	7
2.2.1. Para la Raspberry Pi	7
2.2.2. Para la ESP32	8
2.3. Conectividad.	8
2.4. Funcionalidades clave.	8
2.5. Requisitos adicionales.	8
3. Instalación	10
3.1. Instalación y configuración de los software de monitoreo de trafico.	10
3.1.1. Instalación y configuración de Pfsense.	10
3.1.2. Instalación y configuración de Ntopng.	13
3.2. Consulta de los reportes de tráfico.	16
3.3. Configuración de la Raspberry.	18
3.4. Instalación de Grafana y Influx.	18
3.5. Conectar Influx con NTopng.	19
3.5.1. Configuración Influx con Grafana.	21
3.6. Pruebas.	23
3.6.1. Comunicación entre InfluxDB y el ESP32.	23
4. Configuración Inicial	24
4.1. Configuración de Hardware	24
4.1.1. Raspberry Pi	24
4.1.2. ESP32	24
4.2. Configuración de Software	24
4.2.1. Raspberry Pi	24
4.2.2. ESP32	24
5. Funcionalidades Principales	26
5.1. Funcionalidades de la Raspberry Pi	26
5.2. Funcionalidades de la ESP32	26
5.3. Funcionalidades de Ntopng	26
5.4. Funcionalidades de InfluxDB	26

6. Configuración Avanzada	28
6.1. Optimización de Ntopng	28
6.2. Configuración de InfluxDB	28
7. Resolución de Problemas	29
7.1. Problema 1: Falta de Conexión de Ntopng a InfluxDB	29
7.2. Problema 2: Rendimiento Lento de Grafana	29
7.3. Problema 3: Configuración Incorrecta de Alertas en Ntopng	30
7.4. Problema 4: Error de Configuración de Grafana	30
7.5. Problema 5: Configuración Incorrecta de la Biblioteca InfluxDB en ESP32	30
7.6. Problema 6: Falla en la Generación de Alarmas	31
7.7. Problema 7: Conflictos de Puertos	31
7.8. Problema 8: Error de Autenticación en InfluxDB	32
7.9. Problema 9: Falta de Datos en las Consultas de ESP32	32
8. Actualizaciones y Mantenimiento	33
8.1. Actualizaciones de Software	33
8.2. Mantenimiento Preventivo	33
9. Recursos Adicionales	35
9.1. Documentación Oficial	35
9.2. Tutoriales en Línea	35
9.3. Comunidades y Foros	35

Índice de figuras

1.	Pfsense: Inicio de Proyecto.	10
2.	Pfsense: Package Manager Error solucionado.	11
3.	Pfsense: Configuración de la instalación de Ntopng en el sistema.	12
4.	Pfsense: Especificaciones del Pfsense.	12
5.	Pfsense: Gráfica de tráfico vista desde Pfsense.	12
6.	NTopng: Inicio de Proyecto.	13
7.	Ntopng: Vistazo al Networkchart dentro de Ntopng.	14
8.	Ntopng: Vistazo a la infomacion de host chart dentro de Ntopng.	14
9.	Ntopng: Vistazo de los Top Host dentro del Dashboard de Ntopng.	15
10.	Red del pfSense dada por el access point conectado al pfSense.	15
11.	NTopng: Informacion del reporte de flujo en el formato .json	16
12.	Ntopng: Informacion de un host designado dentro de la red.	17
13.	Ntopng: Información de un host designado dentro de la red.	17
14.	Configuración de la Raspberry Pi como sistema final.	18
15.	InfluxDb: Consulta de los datos almacenados dentro de la base de datos ntop vinculada a ntopng.	19
16.	Ntopng: Configuración de InfluxDB dentro de Ntopng en el apartado de pre- ferencias.	20
17.	InfluxDB: Consulta de los datos almacenados dentro de la base de datos ntop vinculada a ntopng.	21
18.	Caso de uso: Monitoreo de un usuario en la red.	22
19.	Diagrama de Componentes.	22
20.	Arduino IDE: Consulta a la tabla host:traffic.	23

Índice de cuadros

1.	Requisitos de Hardware Raspberry Pi	7
2.	Requisitos de Hardware ESP32	7
3.	Requisitos de Software Raspberry Pi	7
4.	Requisitos de Software ESP32	8
5.	Descripción de los datos consultados a través de la ESP.	23

1. Introducción

En un entorno cada vez más dependiente de la conectividad y la tecnología, la estabilidad y eficacia de los sistemas de red se vuelven fundamentales para el funcionamiento fluido de cualquier institución. La capacidad de mantener estos sistemas estables y seguros refleja directamente la eficacia del trabajo de automatización de alarmas y la gestión del sistema de red en su conjunto. Este manual aborda la implementación y uso del sistema de monitoreo de flujo de red, diseñado para optimizar la gestión de la red y mejorar su eficiencia operativa en la Universidad Politécnica de Victoria.

1.1. Antecedentes

En el panorama tecnológico actual, la estabilidad y el rendimiento de los sistemas de conexión a redes son aspectos críticos para el funcionamiento eficiente de cualquier institución. Este proyecto surge como respuesta a la necesidad de mejorar la infraestructura de red existente en la Universidad Politécnica de Victoria. Inicialmente, se implementó un sistema basado en Telegraf y pfSense. Sin embargo, se identificó que Telegraf proporcionaba datos de manera desorganizada, dificultando la detección y resolución eficiente de problemas. Esta limitación planteó la necesidad de explorar nuevas soluciones.

Con el propósito de superar estos desafíos, se tomó la decisión de implementar ntopng y desarrollar este proyecto. El objetivo principal de esta iniciativa es optimizar la gestión de la red, proporcionando una mayor capacidad de resolución de problemas y mejorando la eficiencia operativa en la institución.

1.2. Definición del problema y justificación del proyecto

La estructura de la red de la Universidad Politécnica de Victoria ha experimentado una expansión a lo largo de los años, acompañada por un aumento en el consumo de los servicios de red debido a la población estudiantil. Esto ha generado una considerable congestión en el tráfico, saturando el ancho de banda y afectando la calidad del servicio. Previamente se identificó que la fuente principal de este problema son usuarios que emplean una gran cantidad de recursos de la red, ya sea consciente o inconscientemente. Para abordar este problema, se propone implementar un sistema de alarma que notifique la presencia de usuarios que estén saturando la red, utilizando la plataforma ntopng.

1.3. Objetivo General

El objetivo general de este manual es proporcionar una guía para la implementación y uso del sistema de monitoreo de flujo de red en la Universidad Politécnica de Victoria. Se busca desarrollar un sistema de monitoreo efectivo que permita detectar y responder a problemas de saturación de red y usuarios problemáticos, mejorando así la calidad del servicio de red en la institución.

1.4. Objetivos Particulares

- Implementar ntopng para monitorear el tráfico de red en tiempo real.
- Configurar un sistema de alarma que notifique la presencia de usuarios que estén saturando la red.
- Desarrollar un prototipo funcional de la alarma utilizando hardware ESP32.
- Evaluar la efectividad del sistema de monitoreo y la alarma en la detección y respuesta a problemas de saturación de red.

1.5. Alcances y Limitaciones del Proyecto

Este manual aborda la implementación de un prototipo de monitoreo de la carga de la red local de la Universidad Politécnica de Victoria. El alcance del proyecto incluye el diseño, desarrollo e implementación de un sistema de monitoreo efectivo utilizando ntopng y hardware ESP32. Sin embargo, este manual no cubre la implementación a gran escala del sistema en toda la universidad ni considera todos los posibles escenarios de uso. Además, las limitaciones del proyecto incluyen la fase inicial de desarrollo del prototipo y no abordan completamente la integración con otros sistemas de la institución.

2. Requisitos del Sistema

En esta sección se detallan los requisitos mínimos necesarios para el funcionamiento adecuado del sistema. Estos requisitos abarcan tanto aspectos de hardware como de software.

2.1. Requisitos de Hardware

Los requisitos de hardware especifican las características técnicas mínimas que deben cumplir los dispositivos en los cuales se instalará el sistema. Estos requisitos incluyen aspectos como la capacidad de procesamiento, memoria RAM, almacenamiento, así como otros componentes relevantes para el rendimiento del sistema.

2.1.1. Para la Raspberry Pi

Cuadro 1: Requisitos de Hardware Raspberry Pi

Componente	Modelo/Especificación
Micro SD	Adata v30 A2
Cargador	PWR+ de 5V y 3.3A
Raspberry Pi	3 Model B

2.1.2. Para la ESP32

Cuadro 2: Requisitos de Hardware ESP32

Componente	Requisito
Hardware	Compatible con la librería de InfluxDB para ESP32

2.2. Requisitos de Software

Los requisitos de software describen las aplicaciones, librerías y sistemas operativos necesarios para ejecutar el sistema de manera efectiva en las plataformas designadas. Se detallan las versiones y configuraciones específicas requeridas para garantizar la compatibilidad y funcionalidad adecuada.

2.2.1. Para la Raspberry Pi

Cuadro 3: Requisitos de Software Raspberry Pi

Software	Versión
Ubuntu Server	23.10
InfluxDB	1.8.10
Grafana	Última versión estable
Ntop Community Edition	Última versión estable
Pfsense	2.7.2

2.2.2. Para la ESP32

Cuadro 4: Requisitos de Software ESP32

Software	Requisito
Librería compatible con InfluxDB	Para ESP32
Arduino IDE	Para la programación

2.3. Conectividad.

Esta sección aborda los aspectos relacionados con la conectividad del sistema, incluyendo la configuración de redes y la comunicación entre dispositivos. Se destacan los pasos necesarios para establecer una conexión robusta y confiable entre los componentes del sistema.

- Configuración de InfluxDB para aceptar conexiones entrantes.
- Configuración de Ntopng para enviar datos a InfluxDB.
- Configuración de Grafana para conectarse a InfluxDB y visualizar los datos almacenados.

2.4. Funcionalidades clave.

En esta sección se enumeran las funcionalidades principales que el sistema debe ofrecer para cumplir con sus objetivos. Se describen las capacidades esenciales del sistema, como el monitoreo en tiempo real del tráfico de red y la gestión del ancho de banda.

1. Monitoreo en tiempo real del tráfico de red.
2. Almacenamiento de datos históricos para análisis.
3. Identificación de aplicaciones y servicios que generan tráfico.
4. Gestión del ancho de banda y control de calidad de servicio (QoS).
5. Integración con otros sistemas mediante consultas a la base de datos.

2.5. Requisitos adicionales.

Aquí se presentan los requisitos complementarios que deben ser considerados para el correcto funcionamiento y mantenimiento del sistema. Se incluyen aspectos como la disponibilidad de conexión a Internet, la capacidad de almacenamiento y la estabilidad del suministro eléctrico.

1. Conexión estable a Internet para la Raspberry Pi y la ESP32.
2. Espacio de almacenamiento adecuado en la Raspberry Pi para los datos recopilados.

3. Configuración correcta de direcciones IP y puertos para la comunicación entre los dispositivos.
4. Asegurar un suministro de energía estable para evitar interrupciones en el funcionamiento del sistema.

3. Instalación

Esta sección detalla los pasos necesarios para instalar y configurar el software de monitoreo de tráfico en los dispositivos designados. Se proporcionan instrucciones claras y concisas para llevar a cabo la instalación de manera efectiva.

3.1. Instalación y configuración de los software de monitoreo de trafico.

En esta sección, se describe el proceso de instalación y configuración de los software de monitoreo de tráfico utilizados en el proyecto. Estos programas son fundamentales para comprender y gestionar eficientemente el flujo de datos en una red y como monitorear el trafico de dicha red para el uso del dispositivo como se ve en la imagen 18.

3.1.1. Instalación y configuración de Pfsense.

En este apartado se describen las primeras tareas llevadas a cabo durante la estadía de proyecto. Durante el primer periodo de investigación del proyecto, se realizaron actividades en el departamento de sistemas. Se instaló el sistema Pfsense en el CPU asignado por el departamento, el cual contenía la versión 2.7.2 de Pfsense. Posteriormente, se procedió a instalar el equipo en el espacio designado por el departamento y a conectarlo a la red.

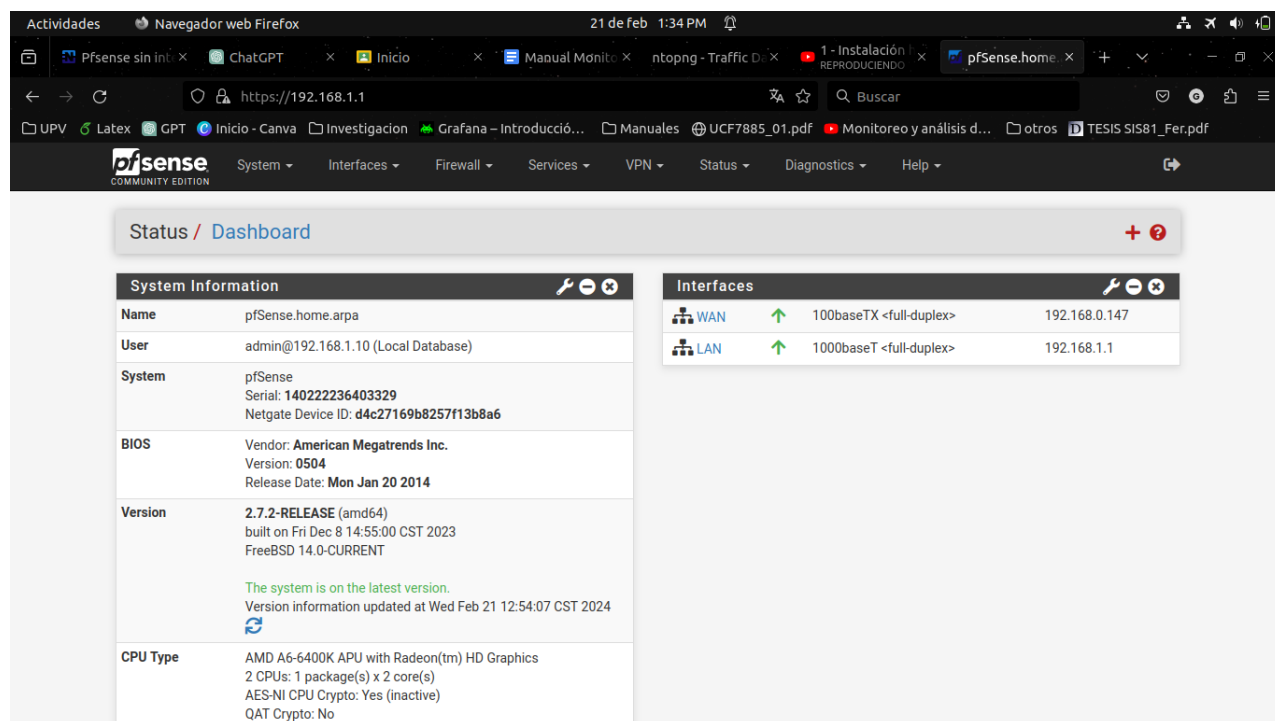


Figura 1: Pfsense: Inicio de Proyecto.

Se encontraron dificultades con la conectividad a la red desde el Pfsense, así como problemas

para instalar los paquetes de Ntopng y Telegraf en el apartado de Gestor de Paquetes o Package Manager. Estos inconvenientes se resolvieron después de solucionar los problemas de conexión a la red del servidor Pfsense y conectar el equipo de trabajo externo mediante un cable de red a la LAN del servidor.

Para complementar este proceso inicial, se llevó a cabo un exhaustivo análisis de las configuraciones de red existentes y se identificaron posibles puntos de mejora en la infraestructura. Esto incluyó la revisión de la topología de red, la asignación de direcciones IP, así como la evaluación de posibles y vulnerabilidades en la seguridad.

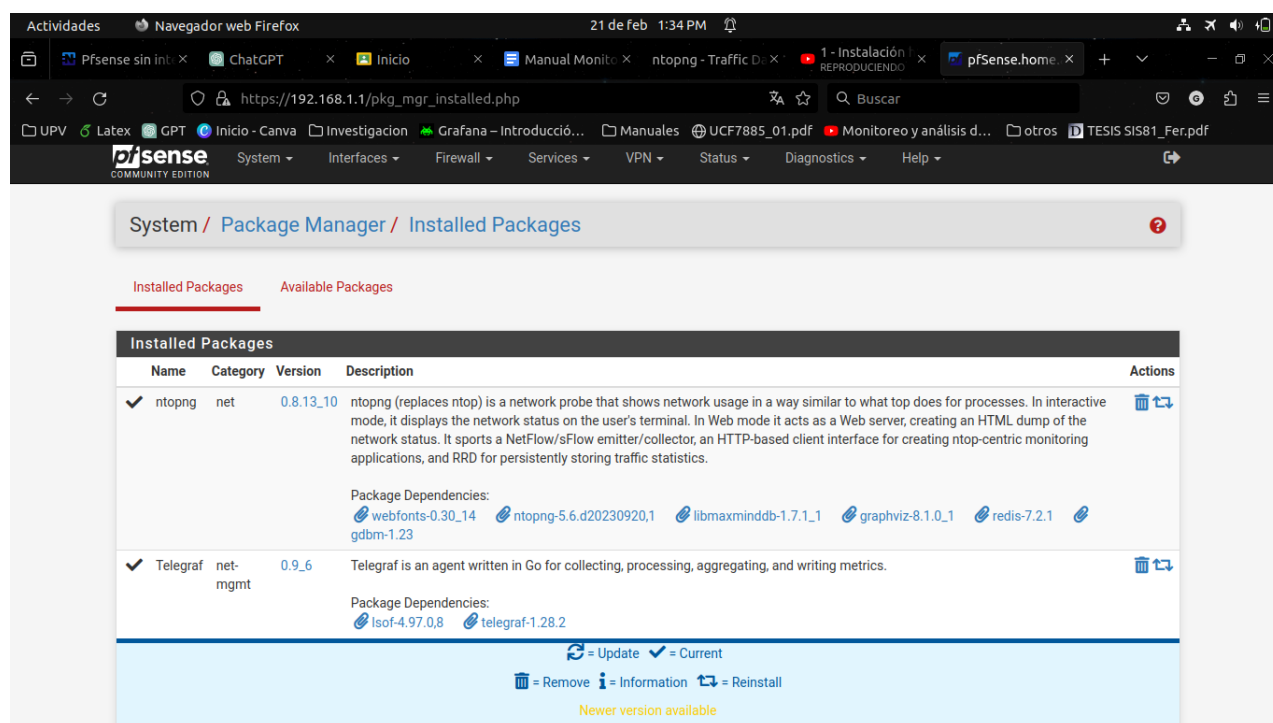


Figura 2: Pfsense: Package Manager Error solucionado.

Una configuración general de Pfsense implica definir la arquitectura de red, asignando interfaces como WAN, LAN y, si es necesario, OPT para segmentos adicionales. Luego, se establecen direcciones IP estáticas o se configura un servidor DHCP para asignar direcciones automáticamente. La configuración del firewall es esencial, definiendo reglas para controlar el tráfico entre las interfaces y hacia/desde Internet, junto con la configuración de NAT si se requiere. Se activan servicios de red como DNS, DHCP y NTP para el funcionamiento básico de la red, mientras que la configuración de VPN proporciona conectividad segura para dispositivos remotos.

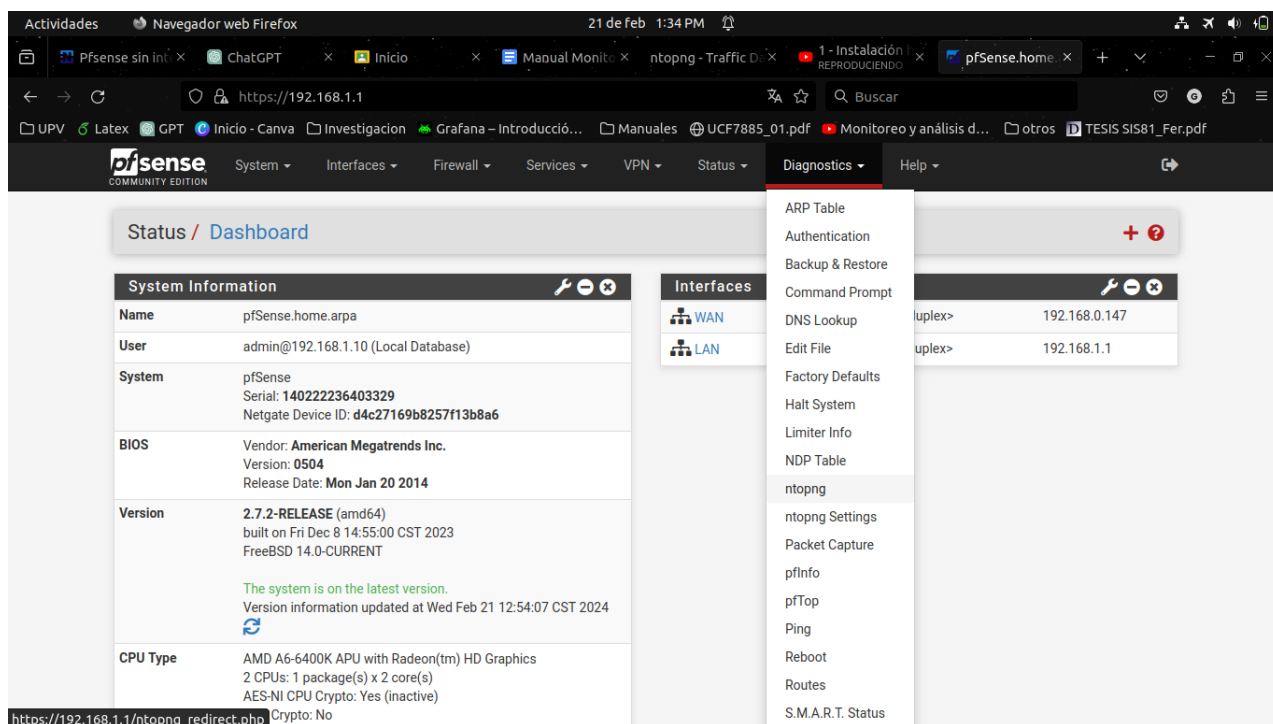


Figura 3: Pfsense: Configuración de la instalación de Ntopng en el sistema.

La supervisión de la actividad de red a través de registros y la programación de actualizaciones automáticas para mantener el sistema seguro y estable son pasos críticos en la configuración. Dependiendo de las necesidades específicas, se pueden implementar servicios adicionales y medidas de seguridad para fortalecer la red contra posibles amenazas estas configuraciones se hicieren con el apoyo de el ingeniero Jaime del Departamento de sistemas y de la informacion sobre instalacion del sistema y configuracion[hernandez2023instalacion].

System Information	
Name	pfSense.home.arpa
User	admin@192.168.1.13 (Local Database)
System	pfSense Serial: 14022236403329 Netgate Device ID: d4c27169b8257f13b8a6
BIOS	Vendor: American Megatrends Inc. Version: 0504 Release Date: Mon Jan 20 2014
Version	2.7.2-RELEASE (amd64) built on Fri Dec 8 20:55:00 UTC 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Thu Feb 29 19:18:48 UTC 2024
CPU Type	AMD A6-6400K APU with Radeon(tm) HD Graphics 2 CPUs: 1 package(s) x 2 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

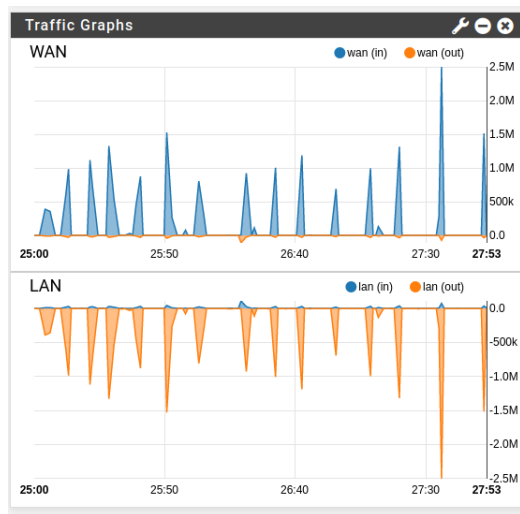


Figura 4: Pfsense: Especificaciones del Pfsense.Figura 5: Pfsense: Gráfica de tráfico vista desde Pfsense.

3.1.2. Instalación y configuración de Ntopng.

Para configurar Ntopng en Pfsense, primero se instala el paquete desde el Gestor de Paquetes de Pfsense. Una vez instalado, se accede a la interfaz web de Ntopng para realizar la configuración inicial, que incluye la definición de las interfaces de red a monitorear y la configuración de las opciones de visualización y generación de informes. Es importante configurar correctamente las opciones de almacenamiento para evitar la saturación del disco duro. Además, se pueden configurar alertas para notificar sobre eventos importantes en la red. Después de la configuración inicial, se monitorea continuamente el tráfico de red utilizando Ntopng para obtener información detallada sobre el uso de la red, el tráfico de aplicaciones y las tendencias de uso. Ntopng por defecto esta en el puerto 3000, lo cual se debe tomar en cuenta para las instalaciones y sistemas utilizados en el futuro.

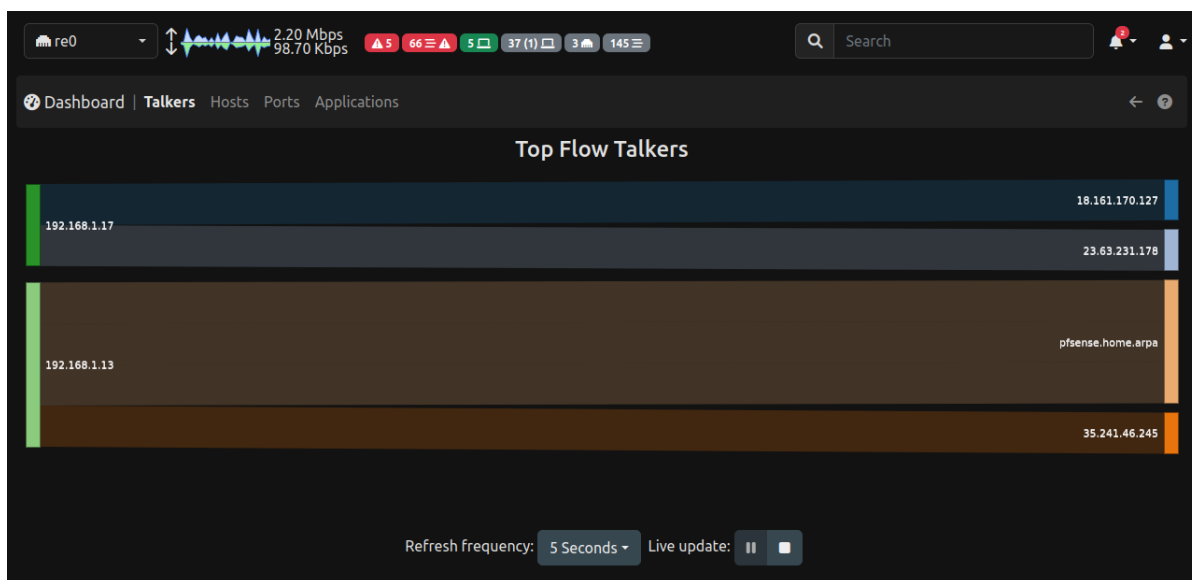


Figura 6: NTopng: Inicio de Proyecto.

Dentro de Ntopng, una herramienta avanzada de monitoreo de red, se pueden encontrar diversas funcionalidades y datos relacionados con el tráfico de red. Algunas de las características y datos que se pueden obtener incluyen:

1. **Información de tráfico en tiempo real:** Ntopng proporciona una vista en tiempo real del tráfico de red, incluyendo el flujo de datos, protocolos utilizados, direcciones IP de origen y destino, puertos, y mucho más. Esto permite a los administradores de red tener una comprensión instantánea de cómo se está utilizando la red en ese momento.
2. **Estadísticas de tráfico histórico:** Además del monitoreo en tiempo real, Ntopng también ofrece la capacidad de visualizar estadísticas históricas de tráfico. Esto incluye datos sobre el tráfico pasado, tendencias de uso de la red, patrones de tráfico, y análisis de la actividad de red a lo largo del tiempo.

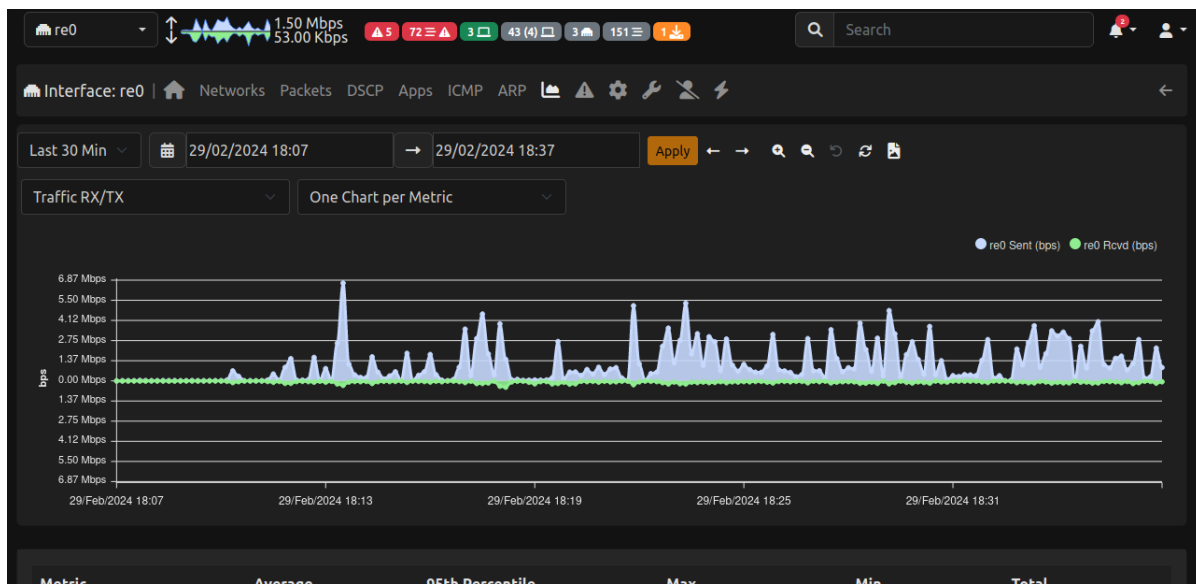


Figura 7: Ntopng: Vistazo al Networkchart dentro de Ntopng.

3. **Análisis detallado de protocolos:** Ntopng es capaz de analizar y categorizar el tráfico de red según los diferentes protocolos utilizados. Esto incluye protocolos como TCP, UDP, ICMP, así como aplicaciones específicas como HTTP, FTP, DNS, entre otros. Proporciona información detallada sobre la cantidad de tráfico generado por cada protocolo, las conexiones establecidas y otros detalles relevantes.
4. **Identificación de aplicaciones y servicios:** Ntopng puede identificar las aplicaciones y servicios específicos que generan tráfico en la red. Esto permite a los administradores detectar y supervisar el uso de aplicaciones específicas, identificar posibles problemas de rendimiento o seguridad, y tomar medidas apropiadas según sea necesario.

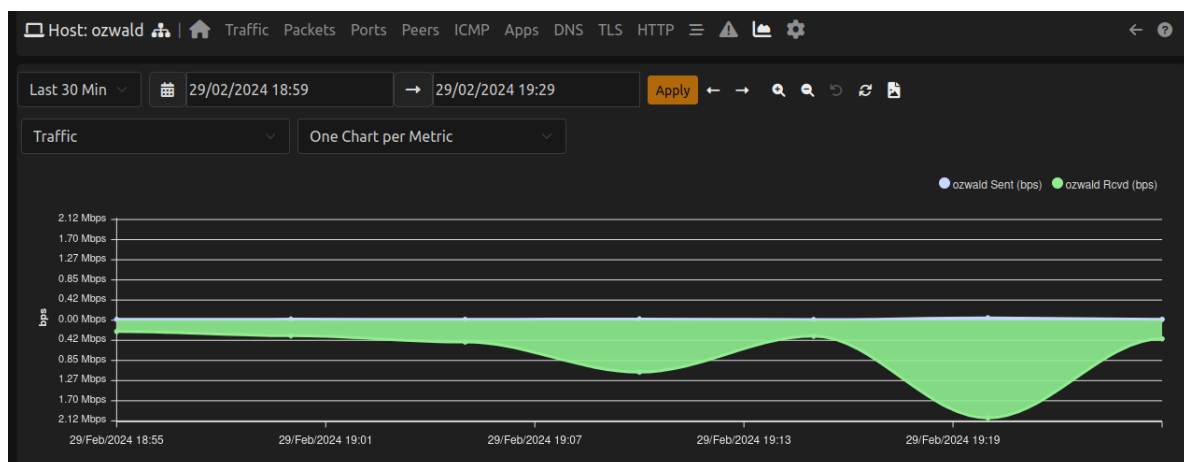


Figura 8: Ntopng: Vistazo a la infomacion de host chart dentro de Ntopng.

5. **Gestión de ancho de banda:** Ntopng ofrece herramientas para gestionar y contro-

lar el ancho de banda de la red. Esto incluye la capacidad de establecer políticas de QoS (Calidad de Servicio), priorizar ciertos tipos de tráfico sobre otros, limitar el ancho de banda para aplicaciones específicas, y realizar otras acciones para optimizar el rendimiento de la red.

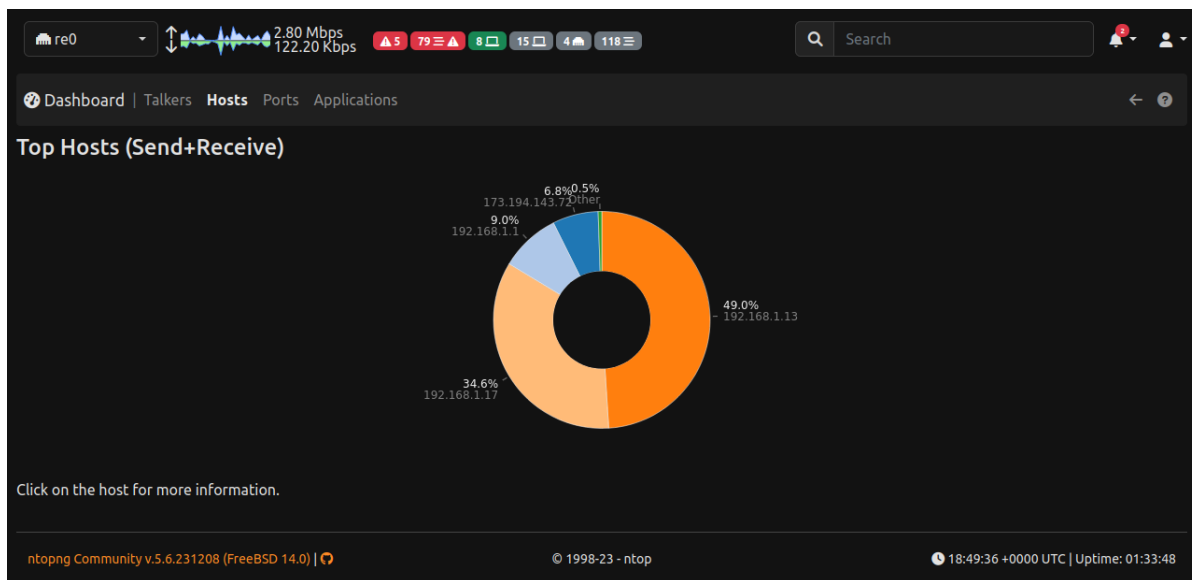


Figura 9: Ntopng: Vistazo de los Top Host dentro del Dashboard de Ntopng.

Para facilitar el acceso remoto al Pfsense y Ntopng en el contexto del proyecto, se implementó una solución mediante la conexión de un punto de acceso (Access Point) a la LAN del servidor Pfsense. Esta configuración permite a los usuarios acceder de forma remota al Pfsense ingresando a través de la dirección IP 192.168.1.1. El punto de acceso está dedicado exclusivamente para este propósito, garantizando un acceso seguro y controlado al sistema desde ubicaciones externas a la red local.

La incorporación del punto de acceso proporciona una capa adicional de seguridad al permitir que el acceso remoto se realice de manera controlada y protegida. Los usuarios autorizados pueden conectarse de forma segura al Pfsense y Ntopng desde cualquier ubicación externa, lo que mejora la flexibilidad y la accesibilidad del sistema sin comprometer la integridad de la red interna. Esta solución garantiza que el acceso remoto sea seguro y eficiente, cumpliendo con los requisitos del proyecto para habilitar la supervisión y gestión remota de la red a través de Pfsense y Ntopng.

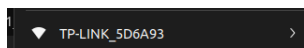


Figura 10: Red del pfSense dada por el access point conectado al pfSense.

3.2. Consulta de los reportes de tráfico.

El reporte de tráfico proporciona información detallada sobre los dispositivos conectados, incluyendo su dirección IP, dirección MAC, sistema operativo, ID de red local y tráfico de red, como UDP y TCP. Durante el proceso de implementación, se consideraron dos posibles soluciones: migrar el archivo .JSON de forma pública como se muestra en la figura 11, aunque no se contaba con información detallada sobre cómo realizar este proceso, o implementar una Raspberry Pi con Influx y Grafana. Después de probar ambas opciones, se decidió finalmente optar por la segunda alternativa. Para llevar a cabo esta decisión, se utilizó Raspberry Imager para instalar una versión específica de Linux Server (v23.10) en la Raspberry. Sin embargo, surgieron desafíos físicos, especialmente relacionados con el cargador de la Raspberry, que causaron interrupciones en dos ocasiones. Actualmente, se ha resuelto este problema mediante el uso de un cargador de 5V y 3.3A para garantizar un suministro de energía adecuado y evitar futuros problemas de configuración debidos a la falta de voltaje.

La versión empresarial de ntopng ofrece un reporte más exhaustivo; sin embargo, es posible que acceder a este informe desde la ESP32 requiera autorización de acceso al sistema sin mostrar directamente los resultados. Una alternativa que se planteó fue acceder a la información a través de Influx. Sin embargo, se identificó que ntopng no es compatible con la versión v2 de InfluxDb, por lo que se optó por utilizar una de las versiones v1, específicamente la 1.8.10, para garantizar la compatibilidad y el funcionamiento adecuado del sistema. Este enfoque permitirá una integración efectiva de los datos de tráfico en la plataforma de monitoreo, facilitando el análisis y la visualización de la información recopilada.

JSON	Datos sin procesar	Cabeceras
Guardar	Copiar	Contraer todo Expandir todo Filtar JSON
rc:		0
▼ rsp:		
udp.bytes.rcvd:		191293133
pkts_ratio:		-0.46737080812454
udp.packets.rcvd:		159384
bytes.sent.anomaly_index:		23
bytes.rcvd.anomaly_index:		13
tcp.packets.seq_problems:		true
other_ip.bytes.sent.anomaly_index:		25
▼ ndpi:		
▼ Skype_Teams:		
packets.sent:		17
breed:		"Acceptable"
num_flows:		0
bytes.sent:		2392
bytes.rcvd:		17359
packets.rcvd:		19
duration:		5
▼ MDNS:		
packets.sent:		50
breed:		"Acceptable"
num_flows:		9
bytes.sent:		6143
bytes.rcvd:		704
packets.rcvd:		8
duration:		115
▼ HTTP:		
packets.sent:		8
breed:		"Acceptable"

Figura 11: NTopng: Información del reporte de flujo en el formato .json

Host: ozwald		
Router/AccessPoint MAC Address	Cisco-Li_C4:6D:9E	
Host MAC Address	0E:39:36:6C:70:F2	Computer
IP Address	192.168.1.17 [192.168.1.0/24]	Host Pool: Default
OS	Android [WChat/1.2]	
Name	ozwald	
Active Monitoring	Add ICMP Monitor +	
Behavioural Counter Anomalies	4	
First / Last Seen	29/02/2024 11:54:33 [01:33:57 ago]	29/02/2024 13:28:10 [00:20 ago]

Figura 12: Ntopng: Información de un host designado dentro de la red.

Reset Host Stats	Reset Host Stats	Reset Blacklisted Hosts Stats
Additional Host Names	Source	Name
	DHCP	ozwald
	MDNS	android-5
Download	JSON	1 min Filter (BPF) pcap Download

Figura 13: Ntopng: Información de un host designado dentro de la red.

La implementación de soluciones de monitoreo de tráfico se ha enfrentado a diversos desafíos técnicos y físicos, pero se ha logrado avanzar hacia una configuración exitosa utilizando una Raspberry Pi 3 Model B con InfluxDb v1.8.10 [HowToCre53:online] y Grafana. A pesar de las limitaciones de compatibilidad entre ntopng e InfluxDb, se ha encontrado una solución viable mediante la utilización de la versión 1.8.10 de InfluxDb, lo que asegura la integración efectiva de los datos de tráfico para su posterior análisis y visualización.

3.3. Configuración de la Raspberry.

Durante la instalación del sistema operativo en la Raspberry Pi mediante Raspberry Imager, se exploraron las opciones avanzadas de configuración. Inicialmente, se consideraron los sistemas CORE 22 y CORE 20, sin embargo, debido a dificultades de configuración, se optó por el sistema Linux Server 23.10, el cual ha sido utilizado desde entonces. A pesar de esta elección, surgieron varios problemas relacionados con la conectividad a la red y el acceso mediante SSH, que se atribuyeron a problemas de configuración de puertos y otros inconvenientes técnicos. Para la instalación del sistema operativo, se empleó una tarjeta Micro SD Adata v30 A2 14.

Además de los problemas de conectividad mencionados, se identificó un inconveniente con el cargador utilizado inicialmente. Se empleaba un cargador de 5V y 2.5A, el cual no proporcionaba la potencia suficiente y ocasionaba que la Raspberry Pi se apagara de manera intermitente. Esta situación se resolvió posteriormente con la adquisición y uso de un cargador de mayor capacidad (5V y 3.3A), garantizando un suministro de energía adecuado y evitando futuras interrupciones en el funcionamiento del dispositivo.

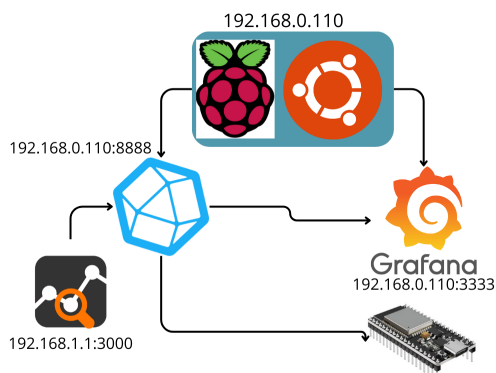


Figura 14: Configuración de la Raspberry Pi como sistema final.

3.4. Instalación de Grafana y Influx.

En el desarrollo de este proyecto, se utilizaron Grafana y InfluxDB en su versión v1 para facilitar la consulta externa de los datos recopilados por Ntopng a través de la Raspberry Pi. Con el fin de evitar conflictos de puertos, se modificaron las configuraciones predeterminadas: Grafana se configuró para operar en el puerto 3333, mientras que InfluxDB se configuró para funcionar en el puerto 8888. Esto se decidió porque Ntopng utiliza el puerto 3000 de forma predeterminada [githubInfluxDBSupport].

La conectividad entre InfluxDB y Grafana se estableció con éxito después de realizar ajustes en la configuración de los puertos y llevar a cabo una investigación exhaustiva sobre cómo realizar la conexión y vinculación entre ambos programas. Estos ajustes fueron fundamentales para garantizar una comunicación sin problemas entre Grafana, InfluxDB y Ntopng, permitiendo así el análisis y la visualización eficientes de los datos de tráfico de red recopilados por Ntopng a través de la Raspberry Pi.

3.5. Conectar Influx con NTopng.

La conexión entre InfluxDB y Ntopng en el contexto de este proyecto implica establecer una integración que permita almacenar los datos recopilados por Ntopng en la base de datos de series temporales proporcionada por InfluxDB. Para lograr esto, se siguen varios pasos:

1. **Configuración de InfluxDB:** En primer lugar, se configura InfluxDB para que esté listo para recibir y almacenar los datos de Ntopng. Esto incluye la instalación de InfluxDB en la raspberry, la configuración de la base de datos designada como ntop.

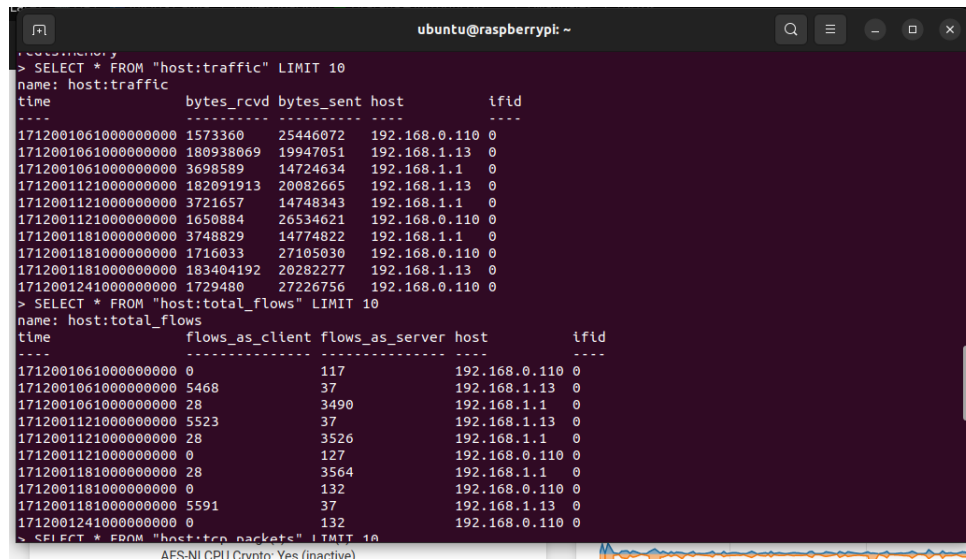


Figura 15: InfluxDb: Consulta de los datos almacenados dentro de la base de datos ntop vinculada a ntopng.

2. **Configuración de Ntopng:** Una vez configurado InfluxDB, se configura Ntopng para que envíe los datos recopilados a InfluxDB. Esto generalmente implica configurar Ntopng para que utilice InfluxDB como un destino de almacenamiento para sus datos de monitoreo de red. Esto se realiza mediante la configuración de Ntopng para que envíe datos a través del protocolo de línea de comandos de InfluxDB o mediante la configuración de una interfaz específica en Ntopng para enviar datos a InfluxDB.

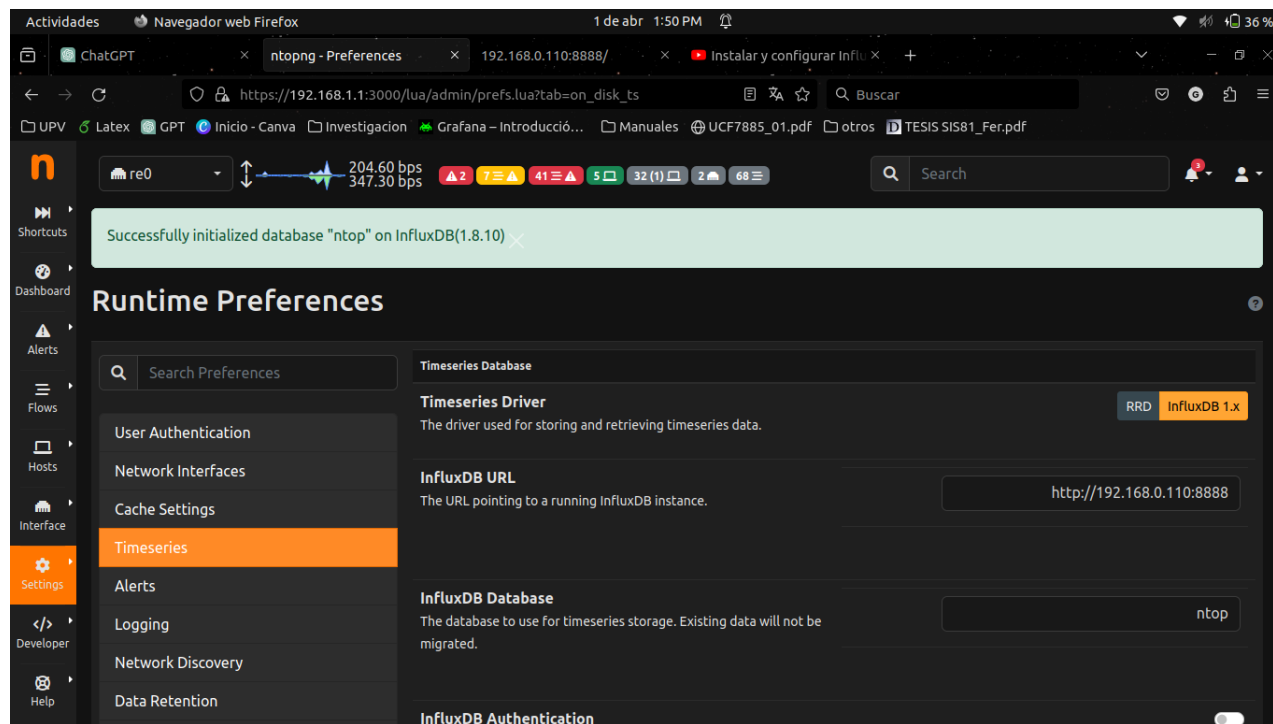


Figura 16: Ntopng: Configuración de InfluxDB dentro de Ntopng en el apartado de preferencias.

3. **Pruebas y ajustes:** Después de configurar ambas aplicaciones, es importante realizar pruebas para asegurarse de que la conexión entre Ntopng e InfluxDB esté funcionando correctamente. Esto implica monitorear el flujo de datos desde Ntopng hasta InfluxDB y realizar ajustes según sea necesario para garantizar una conexión estable y confiable.

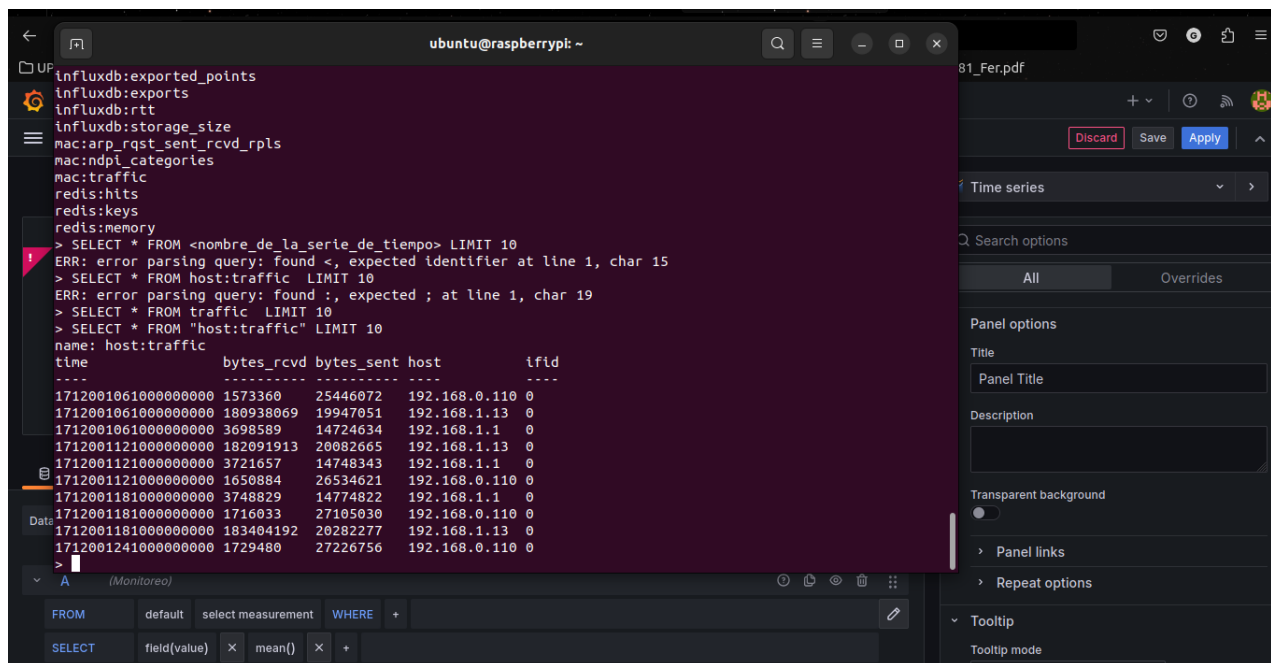


Figura 17: InfluxDB: Consulta de los datos almacenados dentro de la base de datos ntop vinculada a ntopng.

3.5.1. Configuración Influx con Grafana.

La configuración de InfluxDB con Grafana implica integrar la base de datos de series temporales de InfluxDB [grafanaInfluxDBData] con la plataforma de visualización de datos de Grafana para poder analizar y visualizar los datos almacenados en InfluxDB.

1. **Configuración de Grafana:** Después de configurar InfluxDB, se procede a configurar Grafana para que pueda conectarse a la base de datos de InfluxDB y visualizar los datos almacenados. Esto implica agregar un origen de datos en Grafana y especificar los detalles de conexión, como la dirección del servidor InfluxDB, el puerto y el nombre de la base de datos previamente hecha en influxDB[anthony2018metrics].
2. **Creación de paneles y gráficos:** Una vez que Grafana está conectado a InfluxDB, se pueden crear paneles y gráficos personalizados para visualizar los datos de la serie temporal almacenados en InfluxDB. Grafana ofrece una amplia gama de opciones de visualización [leppanen2021data] y configuración que permiten crear paneles de control personalizados, como los que se muestran en la imagen 17.

En la imagen 18 observamos el caso de uso de un usuario en la red, y cómo la alarma funciona a través de consultas a InfluxDB, que a su vez recibe sus datos de ntopng y de pfSense.

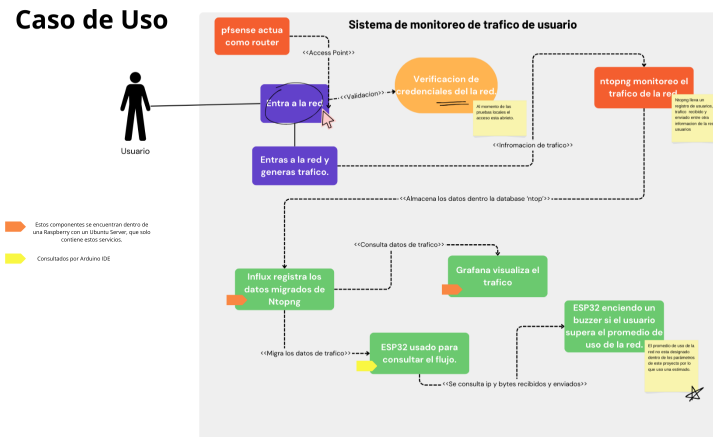


Figura 18: Caso de uso: Monitoreo de un usuario en la red.

Y de nuestro sistema, basándonos en sus componentes como se muestran en la imagen 19.

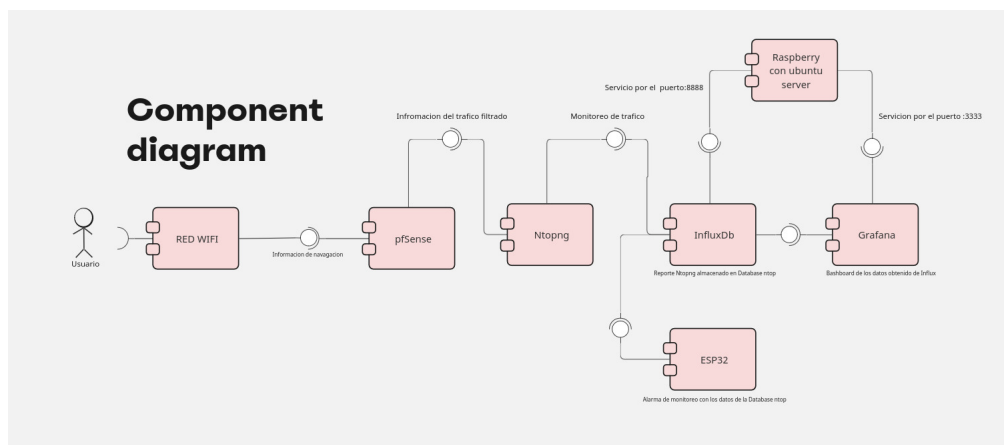


Figura 19: Diagrama de Componentes.

3.6. Pruebas.

Nuestra prueba de consulta a través de un ESP32 fue para verificar el host que ocupa más bytes, que está registrado en InfluxDB.

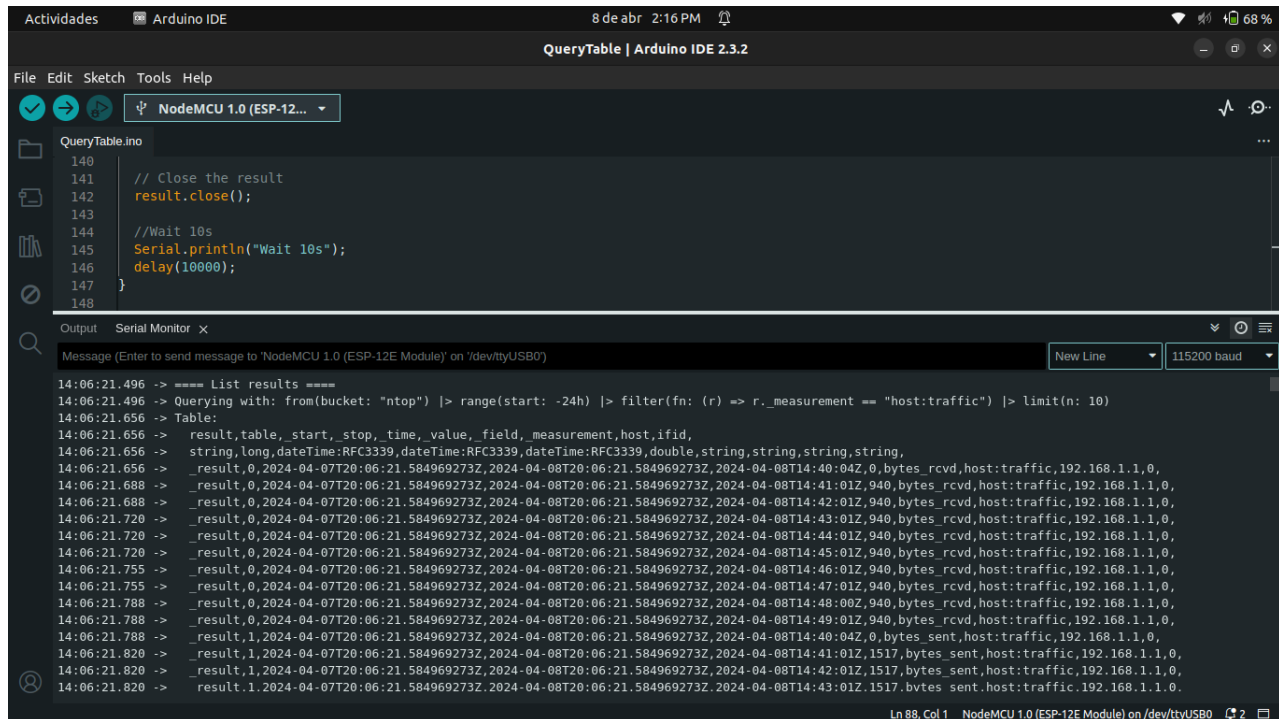
3.6.1. Comunicación entre InfluxDB y el ESP32.

La comunicación con InfluxDB se llevó a cabo utilizando la librería de InfluxDB para las versiones v1 y v2. Dentro de la documentación de la librería, se encuentra información y comentarios sobre cómo adaptarla según la versión que se esté utilizando y la placa. Utilizando uno de los ejemplos de consultas que se incluyen en la librería, se realizaron pruebas de conexión a la base de datos con éxito. Las siguientes tablas (5) representan las columnas de la consulta a la tabla 'host:traffic':

Cuadro 5: Descripción de los datos consultados a través de la ESP.

result	table	_start	_stop	_time	_value	_field	_measurement	host	ifid
14:23:32.559	string	long	dateTime:RFC3339	dateTime:RFC3339	dateTime:RFC3339	double	string	string	string

Así como se muestra en la siguiente imagen (ver Figura 20), la información dentro de la tabla se desglosa.



The screenshot shows the Arduino IDE interface with a sketch named 'QueryTable.ino'. The sketch contains a loop that sends an InfluxDB query to the serial monitor. The query is: `from(bucket: "ntop") |> range(start: -24h) |> filter(fn: (r) => r._measurement == "host:traffic") |> limit(n: 10)`. The serial monitor output shows the results of the query, which are formatted as a table with columns: result, table, _start, _stop, _time, _value, _field, _measurement, host, and ifid. The output shows 10 rows of data, including timestamps, hostnames, and values.

Figura 20: Arduino IDE: Consulta a la tabla host:traffic.

4. Configuración Inicial

4.1. Configuración de Hardware

Antes de comenzar con la configuración del software, es importante asegurarse de contar con el hardware adecuado para cada dispositivo. A continuación, se detallan los requisitos de hardware para la Raspberry Pi y la ESP32:

4.1.1. Raspberry Pi

- Micro SD Adata v30 A2.
- Cargador PWR+ de 5V y 3.3A.
- Raspberry Pi 3 Model B.

4.1.2. ESP32

- Hardware compatible con la librería de InfluxDB para ESP32.

4.2. Configuración de Software

Una vez confirmado que se cuenta con el hardware necesario, procederemos con la configuración del software requerido para cada dispositivo:

4.2.1. Raspberry Pi

Para la Raspberry Pi, se requiere el siguiente software:

- Ubuntu Server 23.10.
- InfluxDB 1.8.10.
- Grafana.
- Ntop Community Edition.
- Pfsense 2.7.2.

4.2.2. ESP32

Para la ESP32, será necesario instalar el siguiente software:

- Librería compatible con InfluxDB para ESP32.
- Arduino IDE para la programación.

Asegúrese de contar con acceso a Internet y seguir las instrucciones específicas de instalación de cada software en su respectivo dispositivo.

5. Funcionalidades Principales

En esta sección se describen las principales funcionalidades que ofrece el sistema implementado en la Raspberry Pi y la ESP32.

5.1. Funcionalidades de la Raspberry Pi

La Raspberry Pi cuenta con las siguientes funcionalidades principales:

- Monitoreo de tráfico de red mediante Ntop Community Edition.
- Análisis y visualización de datos mediante InfluxDB y Grafana.
- Gestión del firewall mediante Pfsense 2.7.2.

5.2. Funcionalidades de la ESP32

La ESP32 ofrece las siguientes funcionalidades principales:

- Captura y envío de datos de telemetría a través de la librería compatible con InfluxDB.
- Programación y control de dispositivos mediante Arduino IDE.

Estas funcionalidades son fundamentales para el correcto funcionamiento del sistema y cumplen con los objetivos establecidos para el proyecto.

5.3. Funcionalidades de Ntopng

Ntopng proporciona las siguientes funcionalidades clave:

- Monitoreo en tiempo real del tráfico de red.
- Análisis detallado del tráfico, incluyendo protocolos utilizados, ancho de banda consumido, y patrones de tráfico.
- Generación de informes y estadísticas sobre el tráfico de red.
- Detección de anomalías y comportamientos inusuales en el tráfico de red.
- Integración con otros sistemas de monitoreo y herramientas de análisis.

Estas funcionalidades permiten un monitoreo efectivo y una gestión proactiva del tráfico de red en el entorno del sistema.

5.4. Funcionalidades de InfluxDB

InfluxDB ofrece las siguientes funcionalidades principales:

- Almacenamiento de series temporales de datos de manera eficiente y escalable.
- Consultas y análisis avanzados de datos temporales.
- Soporte para la integración con diversas fuentes de datos y herramientas de visualización.
- Capacidad para el procesamiento en tiempo real de datos entrantes.
- Escalabilidad horizontal para manejar grandes volúmenes de datos.

Estas funcionalidades son esenciales para el almacenamiento y análisis efectivo de los datos de telemetría generados por el sistema, permitiendo la visualización y la toma de decisiones basadas en datos.

6. Configuración Avanzada

La configuración avanzada del sistema aborda aspectos más detallados y específicos para optimizar el rendimiento y la funcionalidad. Incluye lo siguiente:

6.1. Optimización de Ntopng

Para optimizar el rendimiento de Ntopng, se pueden considerar las siguientes configuraciones:

- Ajuste de los parámetros de captura de paquetes para adaptarse al entorno de red específico.
- Configuración de alertas personalizadas para notificar sobre eventos importantes o anomalías.
- Implementación de filtros de tráfico para reducir el ruido y centrarse en la información relevante.
- Programación de tareas de limpieza y mantenimiento para gestionar eficientemente el almacenamiento de datos.

Estas optimizaciones ayudarán a Ntopng a funcionar de manera más efectiva y a proporcionar información precisa sobre el tráfico de red.

6.2. Configuración de InfluxDB

Para configurar InfluxDB de manera óptima, se pueden seguir estas recomendaciones:

- Ajuste de la retención de datos y políticas de almacenamiento para gestionar el espacio en disco de manera eficiente.
- Configuración de la autenticación y autorización para garantizar la seguridad de los datos almacenados.
- Establecimiento de puntos de control y respaldo para proteger los datos contra pérdidas.
- Monitoreo del rendimiento del servidor InfluxDB para identificar cuellos de botella y optimizar el rendimiento.

Estas configuraciones avanzadas asegurarán que InfluxDB funcione de manera confiable y eficiente, gestionando eficazmente los datos de telemetría del sistema.

7. Resolución de Problemas

En esta sección se describen algunos problemas comunes que pueden surgir durante la configuración y operación del sistema, así como las soluciones recomendadas para abordarlos.

7.1. Problema 1: Falta de Conexión de Ntopng a InfluxDB

Descripción del Problema: Ntopng no puede conectarse correctamente a la base de datos InfluxDB, lo que impide la recopilación y almacenamiento de datos de telemetría.

Solución:

- Verificar la configuración de conexión en Ntopng para asegurarse de que los parámetros de conexión a InfluxDB sean correctos.
- Tener en cuenta que Ntopng puede no ser compatible con las versiones v2.X de InfluxDB para la conexión. En caso de utilizar una versión v2.X, considerar la posibilidad de actualizar a una versión compatible o buscar alternativas de integración.
- Comprobar que InfluxDB esté en funcionamiento y accesible desde la red.
- Revisar los registros de Ntopng y los registros de InfluxDB para identificar posibles errores de conexión o problemas de autenticación.
- Asegurarse de que el usuario utilizado por Ntopng tenga los permisos adecuados para escribir en la base de datos de InfluxDB.

7.2. Problema 2: Rendimiento Lento de Grafana

Descripción del Problema: Grafana experimenta un rendimiento lento al cargar paneles o al realizar consultas a la base de datos InfluxDB.

Solución:

- Optimizar las consultas de Grafana para reducir la carga en la base de datos InfluxDB.
- Aumentar los recursos del servidor donde se ejecuta Grafana, como la CPU y la memoria RAM, para mejorar el rendimiento.
- Revisar la configuración de almacenamiento en caché de Grafana para asegurarse de que esté configurada de manera adecuada.
- Considerar la posibilidad de distribuir la carga de trabajo de Grafana en varios servidores para mejorar la escalabilidad y el rendimiento.

7.3. Problema 3: Configuración Incorrecta de Alertas en Ntopng

Descripción del Problema: Las alertas configuradas en Ntopng no se activan correctamente, lo que impide la detección oportuna de eventos importantes en la red.

Solución:

- Verificar la configuración de alertas en Ntopng para asegurarse de que los umbrales y las condiciones estén configurados correctamente.
- Revisar los registros de Ntopng para identificar posibles errores o advertencias relacionadas con la configuración de alertas.
- Probar las alertas configuradas utilizando escenarios simulados para verificar su funcionamiento.
- Actualizar Ntopng a la última versión disponible, ya que los problemas de alertas pueden haber sido corregidos en versiones posteriores.

7.4. Problema 4: Error de Configuración de Grafana

Descripción del Problema: Grafana no muestra los datos correctamente o no se conecta correctamente a la base de datos InfluxDB.

Solución:

- Verificar la configuración de la fuente de datos en Grafana para asegurarse de que los parámetros de conexión a InfluxDB sean correctos.
- Comprobar que Grafana tenga acceso a la base de datos InfluxDB y que los puertos necesarios estén abiertos.
- Revisar los registros de Grafana en busca de errores relacionados con la conexión a InfluxDB.
- Asegurarse de que la consulta de Grafana esté formulada correctamente para recuperar los datos deseados de InfluxDB.

7.5. Problema 5: Configuración Incorrecta de la Biblioteca InfluxDB en ESP32

Descripción del Problema: La conexión desde un dispositivo ESP32 a la base de datos InfluxDB no se establece correctamente, lo que impide la recuperación de datos de telemetría.

Solución:

- Verificar la configuración de conexión en el código del ESP32 para asegurarse de que los parámetros de conexión a InfluxDB sean correctos.
- Comprobar que el dispositivo ESP32 tenga acceso a la red y pueda comunicarse con el servidor InfluxDB.
- Revisar los registros del dispositivo ESP32 para identificar posibles errores de conexión o problemas de autenticación.
- Asegurarse de que la biblioteca InfluxDB utilizada sea compatible con la versión de InfluxDB en uso y esté correctamente instalada en el entorno de desarrollo.

7.6. Problema 6: Falla en la Generación de Alarmas

Descripción del Problema: Las alarmas no se generan correctamente cuando se superan ciertos umbrales de tráfico de red, lo que dificulta la detección de problemas de congestión o actividad anómala.

Solución:

- Verificar la lógica de generación de alarmas en el código y asegurarse de que los umbrales estén configurados correctamente.
- Comprobar que los dispositivos encargados de monitorear el tráfico de red estén funcionando correctamente y proporcionen datos precisos.
- Revisar cualquier registro o mensaje de error generado durante el proceso de generación de alarmas para identificar posibles problemas.
- Realizar pruebas adicionales con diferentes escenarios de tráfico de red para validar la efectividad de las alarmas en diferentes condiciones.

7.7. Problema 7: Conflictos de Puertos

Descripción del Problema: Se producen conflictos de puertos al intentar ejecutar varios componentes del sistema en el mismo servidor, lo que impide su correcto funcionamiento.

Solución:

- Revisar la configuración de los puertos utilizados por cada componente del sistema y asegurarse de que no haya duplicados o superposiciones.
- Cambiar los puertos en conflicto para evitar colisiones y garantizar que cada componente pueda operar de manera independiente.
- Verificar la configuración del cortafuegos o firewall en el servidor para asegurarse de que los puertos necesarios estén abiertos y permitan el tráfico entrante y saliente.

- Reiniciar los servicios afectados después de realizar cambios en la configuración de los puertos para aplicar los ajustes correctamente.

7.8. Problema 8: Error de Autenticación en InfluxDB

Descripción del Problema: Se produce un error de autenticación al intentar acceder a la base de datos InfluxDB, lo que impide que otros componentes del sistema puedan recuperar o escribir datos.

Solución:

- Verificar las credenciales de autenticación (nombre de usuario y contraseña) utilizadas para acceder a InfluxDB y asegurarse de que sean correctas.
- Comprobar los permisos de acceso del usuario en la configuración de InfluxDB para garantizar que tenga los privilegios adecuados para realizar las operaciones requeridas.
- Revisar los registros de InfluxDB en busca de mensajes de error relacionados con la autenticación para identificar posibles problemas.
- Si se utiliza autenticación basada en tokens, asegurarse de que el token de acceso utilizado sea válido y esté configurado correctamente en el código o la configuración del cliente.

7.9. Problema 9: Falta de Datos en las Consultas de ESP32

Descripción del Problema: El dispositivo ESP32 no puede recuperar datos de la base de datos InfluxDB o las consultas no devuelven los resultados esperados.

Solución:

- Verificar la configuración de la consulta en el código del ESP32 para asegurarse de que esté formulada correctamente y especifique los datos deseados.
- Comprobar la conectividad de red del dispositivo ESP32 y asegurarse de que pueda comunicarse correctamente con el servidor InfluxDB.
- Revisar los registros del servidor InfluxDB para identificar posibles problemas de conexión o consultas mal formadas desde el dispositivo ESP32.
- Asegurarse de que los datos necesarios estén disponibles en la base de datos InfluxDB y no hayan sido eliminados o corrompidos.

Estas soluciones proporcionan orientación para abordar algunos problemas comunes que pueden surgir durante la configuración y operación del sistema. En caso de problemas adicionales, se recomienda consultar la documentación oficial de cada componente y buscar ayuda en comunidades en línea o foros especializados.

8. Actualizaciones y Mantenimiento

El sistema desarrollado requiere de actualizaciones y mantenimiento periódico para garantizar su correcto funcionamiento y seguridad. A continuación, se proporcionan algunas instrucciones generales para llevar a cabo estas tareas:

8.1. Actualizaciones de Software

Las actualizaciones de software son importantes para mantener el sistema seguro y funcionando de manera óptima. Se recomienda seguir estos pasos para realizar actualizaciones:

1. **Verificar Disponibilidad de Actualizaciones:** Regularmente, comprueba si hay actualizaciones disponibles para los componentes del sistema, como InfluxDB, Grafana, Ntopng, y el firmware del dispositivo ESP32.
2. **Realizar Copias de Seguridad:** Antes de aplicar cualquier actualización, realiza copias de seguridad completas de los datos y la configuración del sistema para evitar pérdidas de información en caso de fallos durante el proceso de actualización.
3. **Seguir las Instrucciones del Fabricante:** Para cada componente del sistema, sigue las instrucciones proporcionadas por el fabricante para aplicar las actualizaciones de manera adecuada. Esto puede incluir el uso de herramientas específicas, comandos de terminal, o interfaces web.
4. **Probar las Actualizaciones:** Después de aplicar las actualizaciones, realiza pruebas exhaustivas para asegurarte de que todas las funciones del sistema sigan operando correctamente y de que no se hayan introducido nuevos problemas.

8.2. Mantenimiento Preventivo

El mantenimiento preventivo es fundamental para prevenir problemas y garantizar un funcionamiento continuo del sistema. Aquí hay algunas actividades que se deben llevar a cabo regularmente:

- **Monitorización de la Salud del Sistema:** Utiliza herramientas de monitorización para supervisar el rendimiento del sistema, la utilización de recursos y la detección temprana de posibles problemas.
- **Limpieza y Mantenimiento Físico:** Limpia regularmente los dispositivos físicos, como la Raspberry Pi y el ESP32, para eliminar el polvo y la suciedad que puedan afectar a su rendimiento. Además, verifica que los cables y conexiones estén en buen estado.
- **Revisión de Configuraciones:** Periodicamente, revisa la configuración del sistema para asegurarte de que esté optimizada y actualizada según las mejores prácticas recomendadas por los fabricantes y la comunidad.

- **Gestión de Usuarios y Permisos:** Verifica y actualiza los permisos de usuario y las credenciales de acceso al sistema para garantizar la seguridad y prevenir accesos no autorizados.

Siguiendo estas recomendaciones de actualización y mantenimiento, podrás mantener tu sistema en un estado óptimo de funcionamiento y seguridad a lo largo del tiempo.

9. Recursos Adicionales

Para obtener más información sobre el sistema desarrollado y sus componentes, así como para acceder a tutoriales y documentación técnica útil, se proporcionan los siguientes recursos adicionales:

9.1. Documentación Oficial

- **InfluxDB Documentación Oficial:**
<https://docs.influxdata.com/influxdb/>
- **Grafana Documentación Oficial:**
<https://grafana.com/docs/>
- **Ntopng Documentación Oficial:**
<https://www.ntop.org/guides/ntopng/>
- **pfSense Documentación Oficial:**
https://docs-netgate-com.translate.goog/pfsense/en/latest/recipes/external-wireless.html?_x_tr_sl=auto&_x_tr_tl=es&_x_tr_hl=es

9.2. Tutoriales en Línea

- **Tutorial de InfluxDB y Grafana:**
<https://www.youtube.com/watch?v=SKtrwlzkTEY>
- **Tutorial de Ntopng:**
<https://www.youtube.com/watch?v=P8oxTUoF2Nw>

9.3. Comunidades y Foros

- **Comunidad de InfluxDB en Reddit:**
<https://www.reddit.com/r/influxdb/>
- **Foro de Grafana:**
<https://community.grafana.com/>
- **Foro de ESP32 en Espressif:**
<https://esp32.com/>

Estos recursos adicionales pueden ser de gran ayuda para resolver problemas, obtener información técnica detallada y seguir aprendiendo sobre las tecnologías utilizadas en el sistema desarrollado.