

Implementación de una herramienta de monitorización de redes en una nube híbrida

UOC

Alberto Fernández Sánchez

Grado de Ingeniería
Informática
TFG – Redes de
computadores

Nombre Tutor/a de TF

Amadeu Albós Raya

**Profesor/a responsable de
la asignatura**

Joan Manuel Marquès Puig

Universitat Oberta
de Catalunya

Fecha Entrega

Junio 2024



Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada [3.0 España de Creative Commons](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)

FICHA DEL TRABAJO FINAL

Título del trabajo:	<i>Implementación de una herramienta de monitorización de redes en una nube híbrida</i>
Nombre del autor:	<i>Alberto Fernández Sánchez</i>
Nombre del consultor/a:	<i>Amadeu Albós Raya</i>
Nombre del PRA:	<i>Joan Manuel Marquès Puig</i>
Fecha de entrega (mm/aaaa):	<i>06/2024</i>
Titulación o programa:	<i>Grado de Ingeniería informática</i>
Área del Trabajo Final:	<i>Redes de computadores</i>
Idioma del trabajo:	<i>Castellano</i>
Palabras clave	<i>Nube híbrida, IPSec, monitorización</i>

Resumen del Trabajo

La implementación de infraestructuras basadas en un diseño de nubes híbridas está dando una solución a la necesidad de muchas organizaciones que ven la necesidad de implementar servicios en centros de datos bien on premise bien en el *cloud* pero que necesitan cierta conectividad entre ambos ámbitos.

El trabajo que se presenta es el resultado del estudio y adaptación de las redes corporativas cada vez más interconectadas con servicios en las nubes públicas, presentándose de este modo nuevas necesidades tanto de acceso sino también de seguridad.

Entendiendo que los pilares de la seguridad son la confidencialidad, integridad y disponibilidad, se ha desarrollado en este estudio una solución para aquellas redes que ven como requisito el interconectar su infraestructura tradicional a los servicios de las nubes públicas y tratar de identificar cualquier problema asociado mediante un sistema de monitorización basado en protocolo SNMP. Para conseguir los objetivos se ha implementado una infraestructura virtual que ofrecerá los dispositivos de sistemas y comunicaciones dentro de lo que podría ser un centro de datos tradicional de un lado, y del otro, se ha desplegado tanto sistemas como comunicaciones para ofrecer conectividad del lado de la nube pública y siendo comunicados mediante el uso de IPSec y enrutamiento dinámico.

Abstract

The implementation of infrastructures based on a hybrid cloud design is providing a solution to the need of organizations that see the need to implement services in data centers either on premise or in the cloud but need some connectivity between both areas.

The work presented is the result of the study and adaptation of corporate networks increasingly interconnected with services in public clouds, thus presenting new needs for both access and security.

Understanding that the pillars of security are confidentiality, integrity and availability, this study has developed a solution for those networks that see as a requirement to interconnect their traditional infrastructure to public cloud services and try to identify any associated problems through a monitoring system based on SNMP protocol.

To achieve the objectives, a virtual infrastructure has been implemented that will offer the systems and communications devices within what could be a traditional data center on one side, and on the other side, both systems and communications have been deployed to offer connectivity on the public cloud side and being communicated using IPSec and dynamic routing.

Índice

1. Introducción	2
1.1. Contexto y justificación del Trabajo	2
1.2. Objetivos del Trabajo	2
1.3. Impacto en sostenibilidad, ético-social y de diversidad	3
1.4. Enfoque y método seguido	5
1.4.1. Implementación de la estrategia	5
1.4.2. Detalles de las fases del proyecto	6
1.5. Planificación del Trabajo	6
1.5.1. Tareas contempladas en el plan de trabajo	7
1.5.2. Hitos para considerar y fechas asociadas a las entregas del proyecto	11
1.6. Breve resumen de los productos obtenidos	11
1.7. Breve descripción de los otros capítulos de la memoria	11
2. Análisis de la solución y requisitos técnicos	13
2.1. Escenario de base y problemáticas identificadas	13
2.2. Objetivos y requisitos técnicos a los que se debe dar respuesta	14
2.2.1. Objetivos técnicos	15
2.2.2. Requisitos	17
2.3. Análisis de vías habituales para resolver problemáticas similares	18
3. Diseño de la solución	20
3.1. Análisis de requisitos para el despliegue de la solución	20
3.2. Explicación de la arquitectura a alto nivel	21
3.3. Matriz de funcionalidades y protocolos asociados	22
3.4. Elementos clave dentro de la solución por funcionalidad	23
3.5. Comparación de las opciones disponibles	23
3.6. Selección y justificación de la solución	26
3.7. Diseño de la solución y diagramas de servicio	26
3.7.1. Diseño de la solución y arquitectura cloud (HLD)	26
3.7.2. Diseño de la solución propuesta a bajo nivel (LLD) en capa 3	27
3.7.3. Diseño del proyecto en entorno GNS3	27
3.7.4. Flujo de comunicaciones (matriz)	28
3.8. Inventario de la solución	28
4. Implementación de la solución técnica	30
4.1. Implementación del entorno de CPD local	30
4.1.1. Implementación del entorno de virtualización para realizar funciones de CPD local	31
4.1.2. Implementación del servidor de monitorización en CPD local	33
4.2. Implementación del entorno en el CPD cloud	33
4.2.1. Creación del VPC en AWS	34
4.2.2. Creación del Customer Gateway en AWS	34
4.2.3. Creación de Virtual Private Gateway (VGW)	35

5. Resultados	37
5.1. <i>Resultados obtenidos a nivel de despliegue del entorno CPD On-premises</i>	<i>37</i>
5.1.1. Resultados y pruebas GNS3.....	37
5.1.2. Resultados y pruebas Appliance Cisco virtual	38
5.2. <i>Resultados obtenidos a nivel de despliegue de entorno Cloud público</i>	<i>38</i>
5.3. <i>Resultados obtenidos a nivel de comunicaciones IP.....</i>	<i>39</i>
5.4. <i>Resultados obtenidos a nivel de monitorización SNMP</i>	<i>40</i>
5.5. <i>Resultados obtenidos a nivel de plataforma de monitorización</i>	<i>41</i>
6. Conclusiones y nuevas líneas de trabajo	43
6.1. <i>Conclusiones del trabajo.....</i>	<i>43</i>
6.2. <i>Consecución de los objetivos</i>	<i>44</i>
6.3. <i>Líneas de trabajo futuras</i>	<i>44</i>
6.3.1. Añadir integración con otras herramientas de monitorización	44
6.3.2. Posibilidad de incorporar SNMPv3	45
7. Glosario	46
8. Bibliografía	47
9. Anexos	50
<i>Anexo 1: Estudio sobre entornos de virtualización.....</i>	<i>50</i>
<i>Anexo 2: Estudio sobre proveedores de servicios de nube pública IaaS.....</i>	<i>53</i>
<i>Anexo 3: Estudio de herramientas de monitorización de redes en la actualidad.....</i>	<i>57</i>
<i>Anexo 4: Estudio de tipos de VPN a considerar para la solución</i>	<i>58</i>
<i>Anexo 5: Estudio relativo a la implementación IPsec</i>	<i>60</i>
<i>Anexo 6: Estudio relativo a los mecanismos de routing</i>	<i>62</i>
<i>Anexo 7: Implementación de GNS3.....</i>	<i>64</i>
<i>Anexo 8: Implementación del servidor NMS.....</i>	<i>65</i>
<i>Anexo 9: Configuración de los equipos de comunicaciones en CPD local</i>	<i>67</i>

Lista de figuras

Ilustración 1 Planificación temporal del proyecto Gantt.....	9
Ilustración 2 Escala de tiempo asociada al Gantt del proyecto	10
Ilustración 3 Situación inicial con problemáticas de seguridad asociadas al sistema de monitorización	13
Ilustración 4 Conceptualización de una red híbrida según NIST 500-292.....	16
Ilustración 5 Diseño conceptual de la solución para monitorizar la red híbrida	20
Ilustración 6 Diseño de la solución y arquitectura <i>cloud</i>	26
Ilustración 7 Diseño de la solución propuesta a bajo nivel. Capa 3 (red).	27
Ilustración 8 Diseño del proyecto en entorno GNS3.....	28
Ilustración 9 Infraestructura virtualizada del CPD On-premises objeto del proyecto	30
Ilustración 10 configuración de routing en switch de CPD local	31
Ilustración 11 configuración del routing en la máquina NMS que realiza los pools SNMP al resto de equipos gestionados	31
Ilustración 12 Esquema del router CPD local (on-premises).....	32
Ilustración 13 Obtención de la IP por DHCP el CPE On-Premises	32
Ilustración 14 Implementación de las diferentes VLANs de servicio que forman parte del CPD Local	32
Ilustración 15 Configuración de SNMP en equipamiento Cisco para gestionar desde NMS.....	33
Ilustración 16 VPC resultante en AWS.....	34
Ilustración 17 Resultado del Customer Gateway en AWS	35
Ilustración 18 Virtual Private Gateway desplegado para soportar la conexión VPN	36
Ilustración 19 Verificación de la topología correcta y funcionando en GNS3 ...	37
Ilustración 20 Resultado de integración del router CPE Cisco Systems	38
Ilustración 21 Resultado satisfactorio de integración de la versión IOS y appliance en GNS3.....	38
Ilustración 22 verificación de los túneles IP desde el CPE_ROUTER_CPD	39
Ilustración 23 Estado de los túneles IPsec desde el lado del router CPE_ROUTER_CPD	39
Ilustración 24 Validación del estado de los túneles desde AWS	39
Ilustración 25 Estado de las sesiones eBGP contra el Cloud AWS.....	40
Ilustración 26 Ejemplo de salida de validación por snmpwalk contra el router principal del CPD Local	41
Ilustración 27 Creación de dashboard en LibreNMS satisfactoria	42
Ilustración 28 Posibilidad de integrar GNS3 con software de emulación adicional	50
Ilustración 29 interfaz gráfico de EVE-NG. Fuente: Acta Electrotechnica et Informatica, Vol. 23, No. 3, 2023.....	51
Ilustración 30 Modelo de responsabilidad compartida. Fuente: Cloud Security Gandbook. Eyal Estrin.....	53
Ilustración 31 Cuadrante mágico de Gartner 2023.....	55
Ilustración 32 Posicionamiento competitivo del proveedor de la nube (Fuente: Synergy Research Group).....	56

Ilustración 33 Ejemplo conceptualizado de VPN Site-to-Site en AWS. Fuente: AWS para arquitectos de soluciones. Shrivastava.....	59
Ilustración 34 Integración de GNS3 con VMWare Workstation	64
Ilustración 35 verificación de permisos.....	65
Ilustración 36 Configuración del servidor web NGINX.....	66
Ilustración 37 Configuración SNMP en el NMS LibreNMS	66

“Es justo dejar una nota de agradecimiento a Fran, Sergi, Jairo, Víctor y todas aquellas personas que Dios pone en tu camino para tomar el rumbo correcto. A todos, gracias.”

1. Introducción

1.1. Contexto y justificación del Trabajo

Este proyecto que se presenta está centrado en la **implementación de una herramienta de monitorización de redes en una nube híbrida** [1]

Se ha decidido tratar esta temática debido al alto crecimiento que se tiene hoy en día de infraestructuras corporativas ya no sólo en entornos *on-premises* sino teniendo en cuenta los despliegues de sistemas y arquitectura de comunicaciones que dependen del *Cloud*. A raíz de esto, como consecuencia, se constata la necesidad de ser vigiladas para garantizar la disponibilidad de estas.

Siguiendo una evolución de las comunicaciones clásicas que se obtenían entre dispositivos interconectados demandando servicios de un CPD tradicional, la sociedad poco a poco ha tenido que adaptarse a nuevos paradigmas tras el despliegue de entornos en nubes públicas estableciendo una demanda de comunicaciones entre entornos clásicos (conocidos también como nubes privadas) con entornos Cloud situados en infraestructuras públicas. Estos entornos mixtos se conocerán como nubes híbridas [2].

Atendiendo a esta necesidad, la mayor problemática por parte de las empresas es garantizar una monitorización de sus sistemas independientemente de donde estén alojados (en tornos *on-premise*, *cloud* o híbridos).

Otra de las problemáticas asociadas, es evitar que las comunicaciones que permiten una monitorización de una infraestructura híbrida no viajen a través de un medio compartido como es Internet, sin antes garantizar confidencialidad en los datos.

El hecho de adoptar un proyecto de monitorización dentro de una infraestructura de nube híbrida se fundamenta porque da respuesta a las necesidades de empresas que requieren escalabilidad, un mayor control de recursos, inversión moderada y un mayor control sobre los datos [3]

En lo personal, la temática escogida responde a un objetivo claro de dar respuesta y adaptar los mundos tradicionales de comunicaciones y sistemas a los nuevos paradigmas y necesidades que nos plantean las nubes públicas y sus servicios consiguiendo además desplegar un sistema de vigilancia del estado de los componentes críticos de una organización.

1.2. Objetivos del Trabajo

El presente proyecto, es la consecuencia de querer plasmar aspectos que he ido adquiriendo tanto en mi vida académica como en mi vida profesional y tratando siempre de aportar solución a problemáticas actuales planteadas por empresas convencionales con redes tradicionales.

Además de lo comentado, veo una necesidad personal de conocer más las tecnologías y servicios que plantean los proveedores de nubes públicas, así como las soluciones que permiten conectar ambos mundos, el mundo tradicional local y las soluciones basadas en el *cloud*.

Es por ello por lo que, a nivel personal, el presente trabajo presenta los siguientes objetivos:

- Profundizar acerca de los servicios de conectividad en las nubes públicas.
- Adentrarse en el catálogo de soluciones para desplegar entornos híbridos.
- Conocer las posibilidades de seguridad en comunicaciones.
- Ser capaz de desplegar comunicaciones desde entornos locales contra la nube.
- Desplegar soluciones de monitorización de dispositivos mediante el uso de plataformas SNMP.

En resumen, la finalidad esencial del presente trabajo es demostrar la posibilidad de monitorizar una red corporativa a través de una nube híbrida, demostrando que es posible desplegar dispositivos en la nube y que sean gestionables desde un punto central.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

Del lado de las tres dimensiones relacionadas con la competencia de compromiso ético y global (CGEC), hay que indicar que se ha tratado de forma escrupulosa con el compromiso ético y global asociado que sostiene:

"Actuar de forma honesta, ética, sostenible, socialmente responsable y respetuosa con los derechos humanos y la diversidad, tanto en la práctica académica como en la profesional" [4]

Por otro lado, el presente proyecto cumple está alineado con las tres grandes dimensiones de sostenibilidad, ético-social, diversidad con los ODS correspondiente agrupado por impacto:

ODS con impacto positivo



- ODS 8 - Decent work and economic growth
- ODS 9 - Industry, innovation and infrastructure
- ODS 11- Sustainable cities and communities
- ODS 12- Responsible consumption and production

ODS con impacto neutro



- ODS 1 - No poverty
- ODS 2 - Zero hunger
- ODS 5 - Gender equality
- ODS 6 - Clean water and sanitation
- ODS 7 - Affordable and clean energy
- ODS 10 - Reduced inequalities
- ODS 13 - Climate action
- ODS 14 - Life below water

ODS con impacto negativo



- N/A (no se han identificado ODS con impacto negativo)

Centrándonos en los **impactos positivos** del presente trabajo cabría señalar los siguientes según se extrae del cuadro resumen anterior:

I. **Sostenibilidad:**

● **ODS 9 - *Industry, innovation and infrastructure***: Este proyecto implica la implementación de infraestructura de red innovadora y la integración de tecnologías avanzadas para crear una red híbrida. Contribuye al desarrollo de infraestructuras tecnológicas más eficientes y avanzadas, lo que es fundamental para el crecimiento sostenible y la innovación en el sector de las telecomunicaciones y la informática.

● **ODS 12 - *Responsible consumption and production***: Al utilizar una infraestructura de red híbrida, el proyecto puede promover el uso responsable de recursos al optimizar la infraestructura y reducir la necesidad de hardware físico. Esto puede conducir a un uso más eficiente de la energía y los recursos, lo que es fundamental para la producción y el consumo responsables en el ámbito de las tecnologías de la información y la comunicación.

● **ODS 13 - *Climate action***: La implementación de una red híbrida con AWS puede contribuir a la reducción de emisiones de carbono al promover el uso de servicios en la nube, lo que puede requerir menos hardware físico y, por lo tanto, menos consumo de energía. Además, al utilizar tecnologías innovadoras y eficientes, el proyecto puede

ayudar a mitigar el impacto ambiental asociado con la infraestructura de red tradicional.

II. Comportamiento ético y responsabilidad social (RS)

- **ODS 8 - Decent work and economic growth:** Está relacionado con el proyecto. La implementación de una monitorización de red en una nube híbrida con AWS puede promover el crecimiento económico al fomentar la adopción de tecnologías avanzadas y la innovación en el sector de las telecomunicaciones y la informática. Además, al crear nuevas oportunidades de empleo relacionadas con la gestión y mantenimiento de la infraestructura de red, el proyecto podría contribuir al objetivo de garantizar un trabajo decente y el crecimiento económico.

1.4. Enfoque y método seguido

La problemática presentada cuyo objeto versa el presente proyecto, va a seguir una línea clara siguiendo la metodología en cascada del PMBOK [5] debido a su estructura secuencial y clara, ideal para proyectos con requisitos bien definidos desde el principio. Esta metodología se divide en fases como planificación, diseño, implementación y prueba, con entregables específicos y criterios de aceptación claros. Esto facilita la gestión de recursos, el seguimiento del progreso y la evaluación exhaustiva de riesgos, minimizando impactos negativos. Se consideraron metodologías alternativas como Agile, pero se determinó que el enfoque en cascada era más adecuado para este proyecto específico debido a su naturaleza predecible y planificada.

1.4.1. Implementación de la estrategia

La metodología PMBOK en cascada va a permitir implementar la estrategia definida para el proyecto de la mejor manera posible considerando el escenario. La implementación se va a dividir en una serie de fases claramente definidas, como la planificación, el diseño, la implementación y las pruebas correspondientes, cada una con entregables específicos y criterios de aceptación claros. Esto facilitará la gestión de los recursos, la asignación de tareas y el seguimiento del progreso a través de un control establecido en la planificación.

Además, el enfoque en cascada va a permitir una evaluación exhaustiva de los riesgos y la gestión de cambios de manera formal y controlada, lo que minimiza los impactos negativos en el proyecto.

Para ello, se opta por tratar de adaptar diferentes soluciones y productos y con ello llegar a un objetivo mucho más ambicioso donde se cubra varias tecnologías tanto a nivel de sistemas como a nivel de comunicaciones.

Con respecto a la forma de encarar los puntos más importantes que van a formar parte de este proyecto, se va a tratar de seguir una metodología que sigue un enfoque secuencial y lineal (también conocido como cascada) [6] podría ser beneficiosa para un proyecto de integración de redes *cloud* híbridas debido a su estructura clara y secuencial, **que ayuda a organizar las etapas del proyecto de manera ordenada.**

Además, al adoptar una aproximación clásica de gestión de proyectos, se va a promover una documentación exhaustiva, lo que es crucial para registrar requisitos y cambios de este a lo largo del plazo definido.

Se va a controlar, en consecuencia, todos los cambios de forma formal y fomenta las pruebas detalladas, lo que garantiza la calidad del proyecto. Además, proporciona visibilidad del progreso, facilitando el seguimiento y la orientación durante el desarrollo del proyecto. A través de este enfoque, se puede garantizar una ejecución exitosa del proyecto, cumpliendo con los objetivos establecidos y satisfaciendo las necesidades de los entregables en plazos identificados.

1.4.2. Detalles de las fases del proyecto

El proyecto de este modo se compondrá de los siguientes grandes bloques englobados en diferentes fases:

- **Fase 0 – Plan de trabajo:**
 - En donde se tratará de desarrollar las grandes líneas y puntos de acción del proyecto, desde un punto de vista estratégico.
 - Justificación del proyecto.
- **Fase 1 – Estudio y análisis de la solución**
 - Análisis de entorno y requisitos técnicos y funcionales.
 - Inventario de dispositivos y características necesarias.
- **Fase 2 – Diseño de la solución**
 - Realizar un diseño HLLD, LLD de la solución
 - Aspectos reseñables del diseño
 - Hay que destacar los elementos más importantes que forman parte del diseño.
- **Fase 3 – Implementación de la solución**
 - Instalación, despliegue y configuración de la solución.
- **Fase 4 – Batería de pruebas y resultados obtenidos**
 - Pruebas de conectividad entre entornos
 - Validación de *check-list*
- **Fase 5 – Conclusiones**
 - Conclusiones extraídas del trabajo realizado
 - Trabajos futuros y nuevas vías.
- **Fase 6 – Entrega del producto final**
 - Entrega de la memoria final actualizada
 - Defensa de trabajo final de grado

1.5. Planificación del Trabajo

Siguiendo los puntos de argumentación anteriores, se han identificado las tareas fundamentales sobre el proyecto de monitorización de la red. Para ello, se elabora un diagrama de Gantt y una línea de tiempo para visualizar las tareas, duración y secuencia temporal del proyecto. Esta combinación facilita la comunicación, coordinación y seguimiento del progreso, permitiendo ajustes

para cumplir con los plazos y objetivos establecidos para avanzar en el cumplimiento de los hitos e identificar el camino crítico del proyecto.

Al combinar el diagrama de Gantt y la línea de tiempo, se logra una representación integral y visual de la planificación del proyecto, lo que facilita la comunicación y la coordinación entre los miembros del equipo y otras partes interesadas. Además, esta herramienta permite realizar un seguimiento del progreso del proyecto a lo largo del tiempo y realizar ajustes según sea necesario para garantizar el cumplimiento de los plazos y objetivos establecidos.

1.5.1. Tareas contempladas en el plan de trabajo

Nombre de tarea	Duración	Comienzo	Fin
Fase 0 Plan de trabajo	7 días	lun 04/03/24	mar 12/03/24
Elaboración Plan de trabajo	7 días	lun 04/03/24	mar 12/03/24
Entrega Plan de trabajo	0 días	mar 12/03/24	mar 12/03/24
FASE I Estudio y análisis de la solución	8 días	mié 13/03/24	vie 22/03/24
Definición requisitos de la solución	4 días	mié 13/03/24	lun 18/03/24
Inventario de la solución	2 días	mar 19/03/24	mié 20/03/24
Actualizar documentación Fase I	2 días	jue 21/03/24	vie 22/03/24
Fin del estudio y análisis de la solución	0 días	mié 20/03/24	mié 20/03/24
FASE II Diseño de la solución	14 días	jue 21/03/24	mar 09/04/24
Análisis herramientas del entorno	12 días	jue 21/03/24	vie 05/04/24
Diseñar HLD y LLD	1 día	lun 08/04/24	lun 08/04/24
Documentar aspectos reseñables del diseño	1 día	mar 09/04/24	mar 09/04/24
Fin diseño de la solución	0 días	mar 09/04/24	mar 09/04/24
Entrega primer seguimiento	0 días	mar 09/04/24	mar 09/04/24
FASE III Implementación de la solución	11 días	mar 23/04/24	mar 07/05/24
Instalación del entorno de virtualización local	6 días	mar 23/04/24	mar 30/04/24
Despliegue de appliances en entorno virtual	5 días	mié 01/05/24	mar 07/05/24
Despliegue de servidor de monitorización	1 día	mié 01/05/24	mié 01/05/24
Despliegue de entorno <i>cloud</i>	2 días	jue 02/05/24	vie 03/05/24
Configurar los elementos gestionables	1 día	lun 06/05/24	lun 06/05/24
Actualizar documentación FASE III	1 día	mar 07/05/24	mar 07/05/24

Fin implementación de la solución	0 días	mar 07/05/24	mar 07/05/24
Entrega segundo seguimiento	0 días	mar 07/05/24	mar 07/05/24
FASE IV Batería de pruebas y resultados obtenidos	9 días	vie 10/05/24	mié 22/05/24
Pruebas de conectividad entre entornos	5 días	vie 10/05/24	jue 16/05/24
Validación con <i>check-list</i>	2 días	vie 17/05/24	lun 20/05/24
Actualizar documentación FASE IV	2 días	mar 21/05/24	mié 22/05/24
Finalización fase de pruebas	0 días	mié 22/05/24	mié 22/05/24
FASE V Conclusiones	5 días	jue 23/05/24	mié 29/05/24
Conclusiones extraídas del trabajo realizado	3 días	jue 23/05/24	lun 27/05/24
Trabajos futuros y nuevas vías	2 días	mar 28/05/24	mié 29/05/24
Finalización conclusiones	0 días	mié 29/05/24	mié 29/05/24
FASE VI Entrega de producto	22 días	jue 30/05/24	vie 28/06/24
Entrega de la memoria final actualizada	3 días	jue 30/05/24	lun 03/06/24
Revisión de documentación	6 días	mar 04/06/24	mar 11/06/24
Entrega final de memoria	0 días	mar 11/06/24	mar 11/06/24
Preparación defensa de trabajo final	13 días	mié 12/06/24	vie 28/06/24
Defensa Trabajo Final - Finalización TFG	0 días	vie 28/06/24	vie 28/06/24

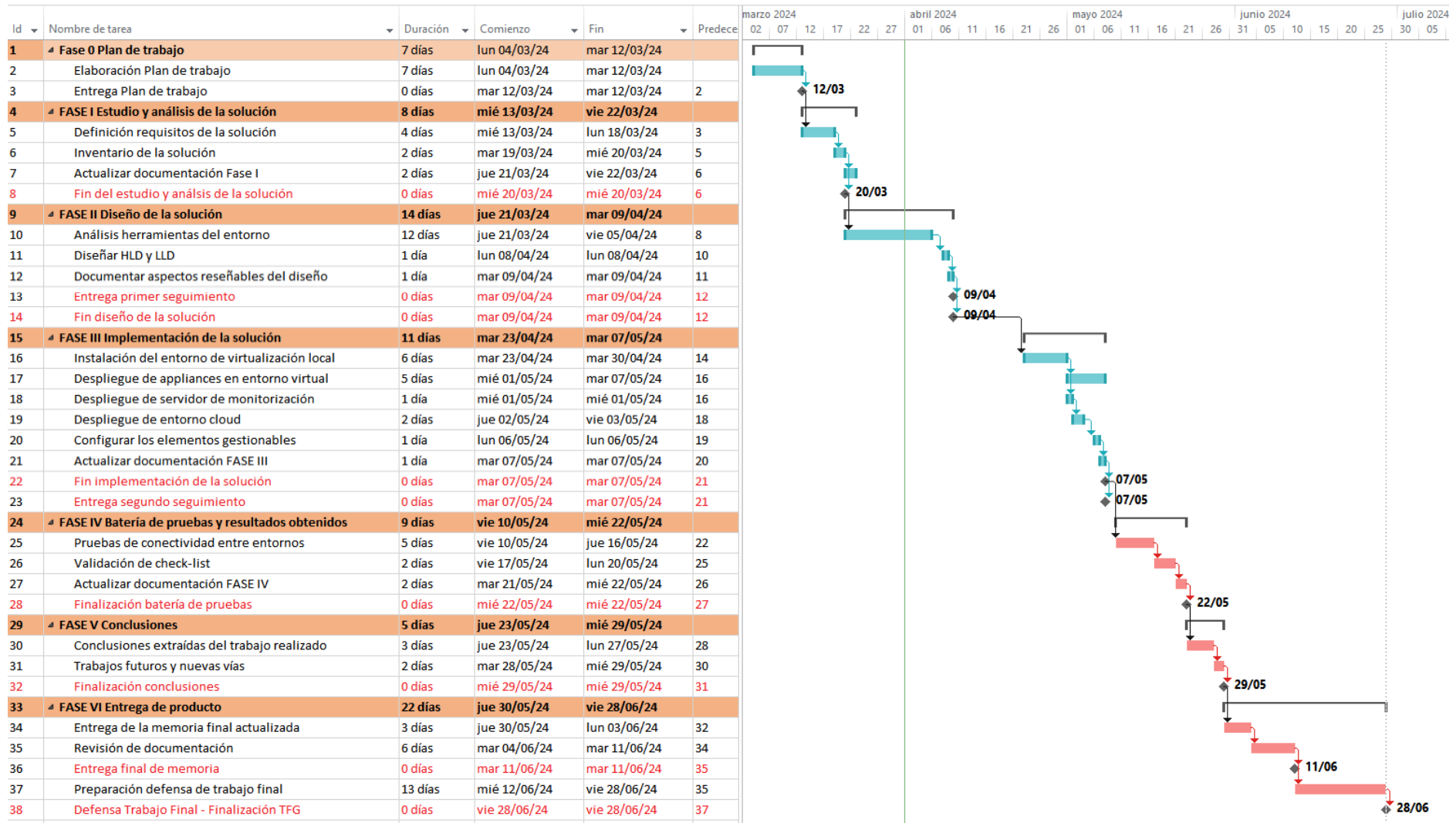


Ilustración 1 Planificación temporal del proyecto Gantt

A continuación, se desglosa cada una de las fases asociadas a la línea temporal del proyecto:

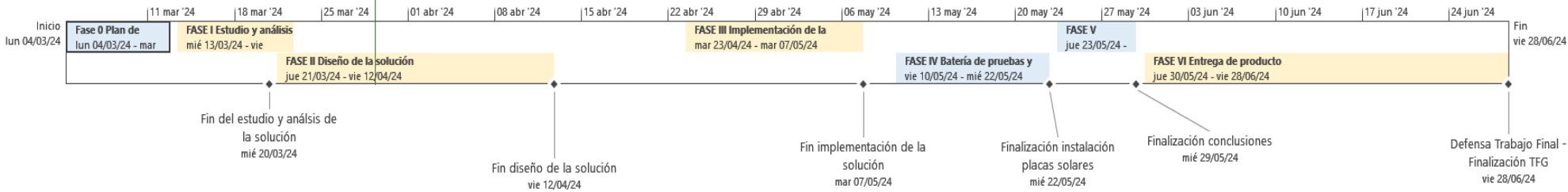


Ilustración 2 Escala de tiempo asociada al Gantt del proyecto

1.5.2. Hitos para considerar y fechas asociadas a las entregas del proyecto

De forma resumida la lista de hitos más importantes del proyecto quedaría resumidos en la siguiente tabla:

Hitos de entregas a considerar	Fecha de la entrega
Entrega del plan de trabajo	12 marzo 2024
Entrega primer seguimiento	9 de abril 2024
Entrega segundo seguimiento	7 de mayo 2024
Entrega final de memoria	11 junio 2024
Defensa Trabajo Final	28 de junio 2024

Estos hitos han sido añadidos al diagrama de Gantt del proyecto.

1.6. Breve resumen de los productos obtenidos

En el contexto del Trabajo de Fin de Grado (TFG), centrado en la implementación de una herramienta de monitorización basada en SNMP para supervisar redes en una nube híbrida, los principales productos que se pueden identificar son los siguientes, adaptados a las necesidades específicas de este proyecto:

- Diseño e implementación de la infraestructura de comunicaciones sobre la que se va a desplegar el resto de los elementos que serán monitorizados.
- Despliegue de los protocolos de seguridad que permitan definir la red híbrida
- Diseño e implementación que permita la monitorización de los equipos gestionados en la red híbrida.

1.7. Breve descripción de los otros capítulos de la memoria

Se estructurará el trabajo de la memoria en los siguientes capítulos principales:

1. **Introducción:** En este capítulo se pondrá en relieve un análisis alto nivel de la solución propuesta y el porqué de la solución escogida. Además, se profundizará en el plan de trabajo a realizar acotado en el tiempo.
2. **Análisis de la solución y requisitos técnicos:** Se partirá en este capítulo realizando un análisis de posibles soluciones tecnológicas que den respuesta a las necesidades expuestas en el capítulo anterior. Además, se hará un estudio pormenorizado de las compatibilidades de los diferentes elementos y requisitos técnicos para su despliegue.
3. **Diseño de la solución:** Se indicará a través de diferentes diseños de la solución explicando los elementos principales, junto a diferentes diagramas a alto y bajo nivel.
4. **Implementación de la solución técnica:** En el capítulo de implementación de la solución técnica se explicarán los aspectos de la configuración de las comunicaciones tanto a nivel interno como a nivel externo (*on-premise* y *cloud*).

5. **Resultados de pruebas y check-list:** En este capítulo se tratará de realizar unas pruebas de validación añadiendo el resultado obtenido en base a los objetivos del proyecto.
6. **Conclusiones y nuevas líneas de trabajo:** Se tratarán los objetivos logrados, análisis de las problemáticas identificadas y nuevas líneas de trabajo a futuro.
7. **Glosario:** Glosario con términos y acrónimos más representativos.
8. **Bibliografía:** Lista numerada de las referencias usadas en la presente memoria de trabajo en formato IEEE.
9. **Anexos:** Anexos que refuercen la memoria del trabajo realizado.

2. Análisis de la solución y requisitos técnicos

2.1. Escenario de base y problemáticas identificadas

El presente proyecto, parte de un escenario básico de una pequeña o mediana empresa, que tiene desplegada una infraestructura tradicional en un CPD local y dispositivos a monitorizar situados en una nube pública.

Como se puede apreciar la **situación de partida**, sería unas comunicaciones básicas, donde se está haciendo uso de un medio compartido sin ningún tipo de seguridad en las comunicaciones:

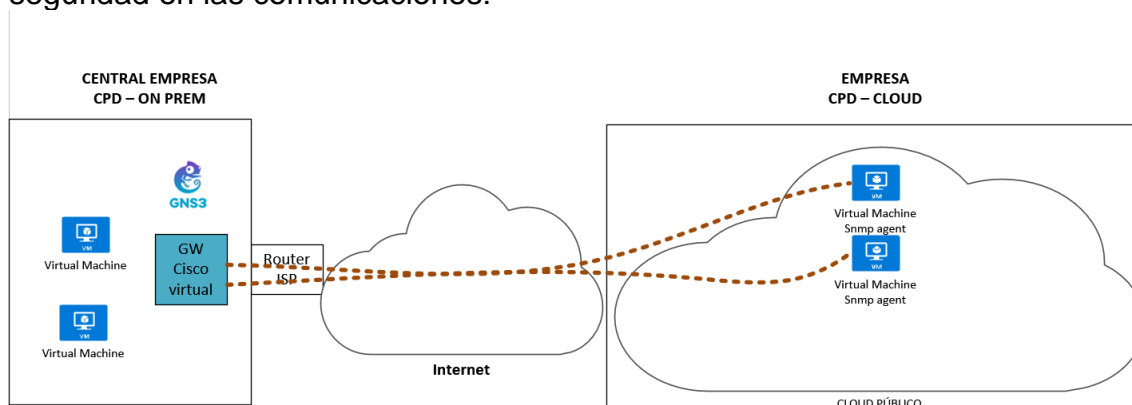


Ilustración 3 Situación inicial con problemáticas de seguridad asociadas al sistema de monitorización

Como se aprecia en la ilustración, el escenario de partida plantea una serie de cuestiones que deben ser enumeradas:

En términos de seguridad, algunas dificultades que podrían plantearse en un escenario de redes corporativas interconectadas con servicios en la nube pública incluyen:

- Vulnerabilidades en la transmisión de datos sensibles a través de internet.
- Riesgos de acceso no autorizado a la red corporativa desde entornos externos.
- Responder a los desafíos relativos a la confidencialidad e integridad de la información.
- Posibles brechas de seguridad en la autenticación y autorización de usuarios.

En cuanto a la conectividad, se podrían identificar las siguientes problemáticas:

- Limitaciones en el ancho de banda y la calidad de la conexión entre los entornos on-premise y la nube pública.
- Posibles interrupciones en la conectividad que afecten la disponibilidad de los servicios.

- Dificultades en la gestión de la red para asegurar una comunicación fluida y estable entre los diferentes entornos.

En relación con la monitorización de la red, las dificultades podrían ser:

- Falta de visibilidad completa sobre el rendimiento y la salud de la red en entornos híbridos.
- Desafíos para recopilar y analizar datos de monitorización de forma centralizada y eficiente.
- Complejidad en la identificación y resolución de problemas de red en un entorno distribuido y heterogéneo.

Estas dificultades en seguridad, conectividad y monitorización de la red son aspectos críticos para considerar al diseñar una solución de monitorización para redes en una nube híbrida, ya que impactan en la operatividad, la eficiencia y la seguridad de la infraestructura de red.

2.2. Objetivos y requisitos técnicos a los que se debe dar respuesta

El ámbito del proyecto se establece en una red corporativa de empresa que tiene como necesidad ir desplegando dispositivos en la nube pública pero que quiere monitorizarlos con el **fin de garantizar su supervisión continuada 24x7x365** a través de su centro de supervisión de sistemas.

Hay que indicar que los objetivos identificados serán considerados como finalidades a lograr con la propia finalización del proyecto.

Del lado del apartado de requisitos, se recogerán las funcionalidades que se espera del sistema, con el fin de en una revisión del estado del arte obtener las bases para afrontar el proyecto y que servirán para la fase del diseño de la solución.

De forma general por la parte de los objetivos y finalidades del proyecto de implementación de una herramienta de monitorización en una nube híbrida, se pueden establecer las siguientes finalidades a alcanzar:

- Garantizar la seguridad de las comunicaciones entre entornos on-premises y la nube, asegurando la confidencialidad de la información transmitida.
- Facilitar la operación y mantenimiento de la solución de monitorización, asegurando que sea fácil de mantener y operar por el personal técnico.
- Lograr la escalabilidad de la solución, permitiendo adaptarse a las características de rendimiento del sistema y a las necesidades cambiantes de la red.
- Proporcionar visibilidad completa y en tiempo real de la infraestructura híbrida de la empresa, permitiendo una monitorización centralizada y eficiente.
- Cumplir con los controles de seguridad y normativas establecidas por la empresa en cuanto a la protección de datos y la gestión de riesgos.

- Implementar sistemas de monitorización centralizados y agentes en los elementos gestionados para supervisar el estado y el rendimiento de la red.
- Definir y configurar paneles de control (*dashboards*) que formen parte del sistema de monitorización del centro de soporte de la empresa, facilitando la visualización de datos relevantes para la toma de decisiones.

Estos objetivos y finalidades del proyecto se centran en los resultados esperados y en los beneficios que se buscan obtener con la implementación de la herramienta de monitorización en la nube híbrida, sin detallar tareas específicas, para orientar la dirección y el propósito de la solución de manera clara y concisa.

Del lado de los requisitos funcionales del sistema de monitorización de redes en la nube híbrida se centrarán en las funcionalidades y capacidades esperadas para satisfacer las necesidades operativas y de gestión de la red. A continuación, se enumeran los requisitos funcionales del sistema:

1. Detectar el estado de salud de los dispositivos gestionados en la red híbrida para garantizar su correcto funcionamiento.
2. Proporcionar conectividad entre el entorno de la nube pública y la infraestructura del *datacenter* local para asegurar la comunicación efectiva.
3. Implementar protocolos estándar de monitorización para recopilar datos de rendimiento y estado de los dispositivos de red.
4. Monitorizar de forma continua y en tiempo real el tráfico de la red para identificar posibles saturaciones y cuellos de botella.
5. Recopilar y centralizar los logs de los dispositivos gestionados en un cuadro de mando para un análisis eficiente.
6. Visualizar el estado de la red en tiempo real a través de un *dashboard* único que muestre información relevante para la toma de decisiones.
7. Mantener un inventario actualizado de los equipos gestionados en la red híbrida, incluyendo información detallada de cada dispositivo.

Estos requisitos funcionales del sistema de monitorización se enfocan en las capacidades necesarias para supervisar y gestionar de manera efectiva la red en un entorno híbrido, sin mencionar tecnologías o soluciones específicas en esta etapa del proyecto.

2.2.1. Objetivos técnicos

En este apartado se explicará la finalidad que trata de conseguir el presente proyecto a alto nivel.

La **infraestructura tipo a desplegar**, contará con los elementos más representativos para poder demostrar la correcta implementación de la solución y la demostración de la solución a los problemas a solventar como lo son los de la vigilancia y gestión de equipamiento en redes híbridas que involucran tanto equipamiento en un CPD tradicional con instalaciones físicas, como

equipamiento virtual desplegado en una nube pública consiguiendo monitorizar los elementos críticos de la red.

Esta **infraestructura estaría adecuada a dar soporte a grupos de trabajadores cuyo número oscilaría entre 50 y 100 personas**, por lo que habría que adecuar la solución a este dimensionamiento de usuarios.

Partiendo de base que el presente trabajo tiene como punto de partida de una empresa que tiene una infraestructura heterogénea, conceptualmente, la solución que se adapta mejor es el de desplegar el servicio de monitorización sobre una nube híbrida, tal como reza la publicación del NIST 500-292 [7]

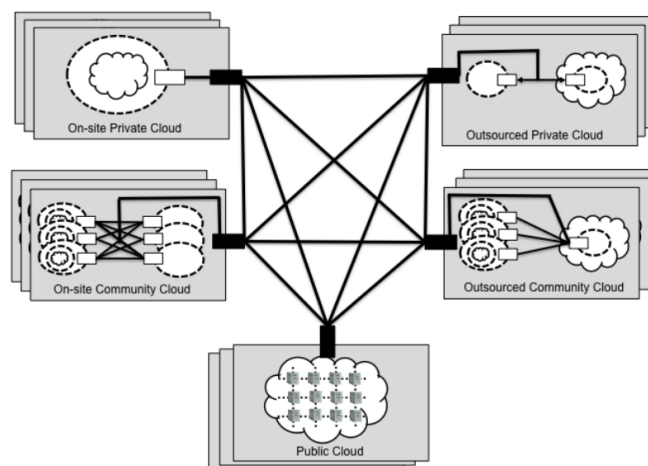


Ilustración 4 Conceptualización de una red híbrida según NIST 500-292

El **servidor central de monitorización** se encontrará emplazado en la zona de la nube privada On-Site (un CPD tradicional pero que ya cuenta con sistemas de virtualización desplegados en su sede central).

Del lado de los dispositivos gestionados por el sistema de monitorización, se encontrarán tanto en las dependencias de la sede central donde se encuentra la infraestructura de nube privada (el datacenter) como en la zona que está desplegada en el proveedor *cloud* público por lo que se necesitaría que el servidor de **monitorización cuente con conectividad IP y más concretamente a través del protocolo SNMP**.

A la hora de dotar comunicaciones y crear la red híbrida, **habrá que garantizar las dimensiones de seguridad de la compañía (confidencialidad, integridad y disponibilidad)**, por lo que habrá que adaptar un diseño que comulgue con una red híbrida de comunicaciones garantizando los pilares fundamentales de la seguridad, es por ello por lo que habrá que **adoptar una arquitectura basada en una red VPN que a través del uso de la suite de IPSec** se logrará que las comunicaciones sean seguras extremo a extremo.

De forma resumida se identifica en la siguiente matriz el conjunto de objetivos técnicos que debería cumplir el proyecto:

Objetivos técnicos identificados	Consideraciones	Descripción de la finalidad
Implementar un diseño de red robusto	Evaluar mejor diseño en escenarios híbridos	Se tratará de implementar el mejor diseño orientado a dar

		<i>conectividad y definición de redes híbridas.</i>
<i>Conectividad segura entre dispositivos gestionados</i>	<i>Despliegue de una red híbrida privada de comunicaciones</i>	<i>Se implementará conectividad IP que permita conectar el CPD local y el CPD en el cloud</i>
<i>Implementar un protocolo de monitorización estandarizado y sencillo</i>	<i>SNMP</i>	<i>Se implementará SNMP por una mayor estandarización a nivel de monitorización de red.</i>
<i>Desplegar un sistema de monitorización libre basado en Linux</i>	<i>Sistema NMS</i>	<i>Se desplegará un sistema NMS que permita aglutinar las alarmas de la red híbrida.</i>
<i>Definición de una red dinámica IP tolerante a fallos</i>	<i>Routing dinámico</i>	<i>Se implementará un protocolo de routing dinámico que tenga tolerancia a cambios en la red</i>

2.2.2. Requisitos

En el presente apartado se enumerarán los diferentes requisitos ya sean funcionales y no funcionales que permitirá la presente solución alcanzar los objetivos.

Los requisitos funcionales que se han identificado son los que necesariamente deben darse por satisfechos para dar por finalizado el proyecto con garantías de éxito.

Del lado de los **requisitos funcionales** se identifica lo siguiente:

Requisito funcional identificado	Descripción
<i>Detectar estado de salud</i>	<i>Se identificará el estado de salud de los dispositivos gestionados que forman parte de la red híbrida.</i>
<i>Proporcionar la conectividad a la solución</i>	<i>Se deberá levantar conectividad entre el Cloud Público y la infraestructura de Datacenter local</i>
<i>Implementación de protocolos estándar</i>	<i>Como requisito funcional en el contexto de la solución de monitorización de redes híbridas.</i>
<i>Detectar riesgo de saturación</i>	<i>Se monitorizará de forma permanente y en tiempo real el caudal de los circuitos para identificar saturaciones de circuitos.</i>
<i>Recepción de logs centralizadas</i>	<i>Se definirá un cuadro de mando que reciba los logs de los dispositivos en tiempo real.</i>
<i>Visualización del estado de la red en tiempo real en un mismo dashboard</i>	<i>Se deberá tener disponible de un cuadro de mando que muestre información del estado de la red en tiempo real.</i>
<i>Inventario de la red híbrida y sus equipos</i>	<i>Se definirá un inventario de los equipos gestionados y sus identificativos.</i>

Por la parte de los requisitos no funcionales, hay que indicar que serán recogidos aquellos ítems que hagan referencia a las características intrínsecas que debe cumplir el sistema resultante de la solución propuesta.

Es por ello por lo que se identifican los siguientes **requisitos no funcionales**:

Requisito no funcional identificado	Descripción
<i>Solución de monitorización basada en software libre</i>	<i>La solución por implementar relativa a la parte de monitorización deberá ser una solución GPL para permitir el ahorro en costes de producto.</i>
<i>Solución de monitorización que permita la gestión de diferentes fabricantes</i>	<i>La solución de monitorización a implementar debería ser capaz de obtener datos de los fabricantes de comunicaciones y sistemas más usados en la actualidad.</i>
<i>Facilidad de implementación de la solución</i>	<i>Se identifica como un requisito no funcional como la facilidad de implementación de la solución que permitirá cumplir con los hitos del proyecto, al ahorrar coste en horas de implementación.</i>
<i>Solución segura</i>	<i>Además de asegurar las comunicaciones entre entornos on-premises y cloud se deberá garantizar la confidencialidad de la información.</i>
<i>Solución fácil de mantener</i>	<i>La solución para desplegar deberá asegurar que la solución sea fácil de mantener y operar.</i>
<i>Escalabilidad de la solución</i>	<i>La solución para desplegar podrá ser escalable en cuanto a características de rendimiento de sistema.</i>

2.3. Análisis de vías habituales para resolver problemáticas similares

Siguiendo el hilo de investigación del proyecto, se toma como referencia las diferentes soluciones que pretenden de dotar visibilidad al departamento técnico de una empresa para toda la infraestructura híbrida en su totalidad. Aunque el fin último sea el de crear un sistema de monitorización en una red corporativa, se deben tener identificadas los puntos de acción más eficientes para la problemática del presente proyecto:

- Una **red de comunicaciones robusta** que sirva de apoyo para la solución definitiva.
- Posteriormente **se debe implementar los controles de seguridad** correspondientes a nivel de cumplimiento normativo de la empresa.
- **Se desplegarán los sistemas de monitorización centrales.**
- **Implementación de agentes** de los elementos gestionados.
- **Definición de los “dashboard”** que formarán parte del sistema de monitorización del centro de soporte de la empresa.

Del lado de la seguridad y de las redes de comunicaciones robustas, se obtiene a través de diferentes publicaciones[8]las recomendaciones para las mejores prácticas para asegurar redes híbridas, como controles de seguridad, segmentación de red, en entornos de nube híbrida [9]

Las soluciones técnicas más utilizadas son de crear sistemas de monitorización, bien centralizados o distribuidos que permitan tener una visibilidad en tiempo real de la red. Dependiendo del software de monitorización a desplegar este tendrá un diseño u otro.

Basado en esto, las **soluciones GNU/GPL de monitorización de redes, se implementan con una arquitectura centralizada** en lugar de distribuida por motivos de sencillez y costes.

Por ello, lo habitual es desplegar un **servidor central de monitorización que recoja la información SNMP de todos los dispositivos** y plasme en un mismo panel de control alarmas y gráficas asociadas. En consecuencia, se suele dotar un canal de comunicaciones seguras que garanticen la confidencialidad de la información al viajar a través de un medio compartido (internet).

Por lo tanto, el análisis de vías habituales para resolver problemáticas similares, como la implementación de protocolos de enrutamiento dinámico y la garantía de seguridad en las comunicaciones, se alinea con las mejores prácticas y recomendaciones en entornos de redes híbridas, como se menciona en las referencias citadas.

3. Diseño de la solución

3.1. Análisis de requisitos para el despliegue de la solución

Una vez determinadas las diferentes soluciones que compondrán el proyecto de monitorización del *cloud* híbrido, se procede a hacer un análisis a alto nivel de los componentes y se identifican diferentes elementos a implementar:

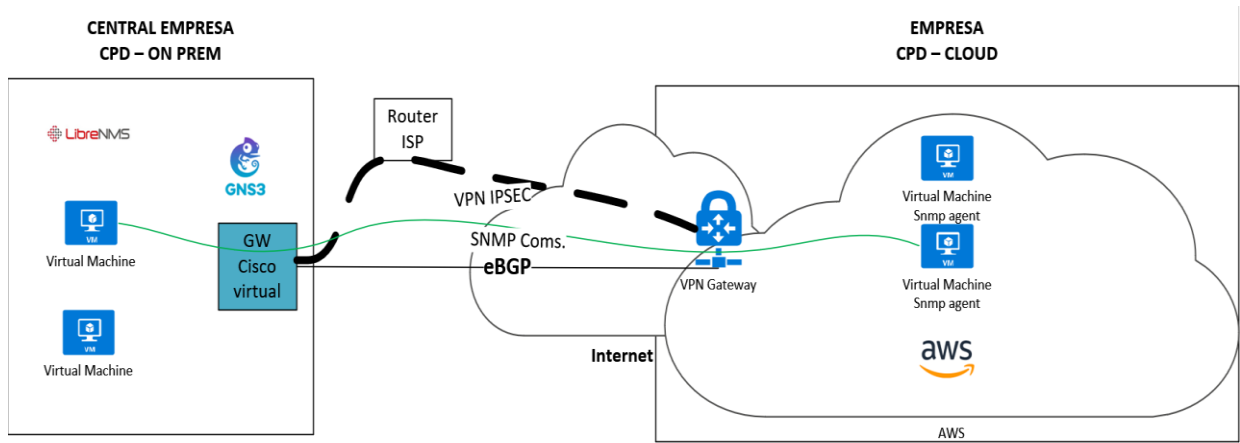


Ilustración 5 Diseño conceptual de la solución para monitorizar la red híbrida

A continuación, se establece una relación entre el diseño propuesto y los requisitos identificados:

Requisitos	Diseño propuesto
Detectar el estado de salud de los dispositivos gestionados en la red híbrida	Implementación de un sistema de monitorización que recopile datos de rendimiento y estado de los dispositivos en tiempo real, permitiendo identificar posibles problemas de salud de la red
Proporcionar conectividad entre la nube pública y el <i>datacenter</i> local	Establecimiento de una VPC en el entorno de la nube pública que sirva como conexión con los elementos de la red, garantizando una comunicación efectiva entre los entornos
Implementar protocolos estándar de monitorización	Utilización de protocolos estándar para la monitorización de la red híbrida, asegurando la compatibilidad y eficiencia en la recopilación de datos de rendimiento.
Monitorizar el tráfico de la red en tiempo real	Despliegue de un sistema de monitorización que permita la monitorización continua y en tiempo real del tráfico de la red, facilitando la detección de posibles saturaciones
Recopilar y centralizar logs de los dispositivos	Configuración de un cuadro de mando que reciba y centralice los logs de los dispositivos gestionados, permitiendo un análisis eficiente de la información.

Visualizar el estado de la red en tiempo real	Creación de un dashboard único que muestre información actualizada del estado de la red en tiempo real, facilitando la toma de decisiones por parte del personal de supervisión.
Mantener un inventario de equipos gestionados	Definición de un inventario detallado de los equipos gestionados en la red híbrida, asegurando un seguimiento preciso de los dispositivos y sus características.

Esta relación entre el diseño propuesto y los requisitos identificados muestra cómo la solución planteada aborda de manera efectiva las necesidades operativas y de gestión de la red en la nube híbrida, garantizando la resolución de los problemas planteados en el proyecto de monitorización.

En consecuencia, se extraen los siguientes puntos que serán importantes para una correcta implementación de la solución a nivel de diseño e implementación:

- **A nivel de *cloud* público (dentro del entorno AWS)**, se debe contar con una VPC que ofrecerá la infraestructura virtual y servirá de conexión con los diferentes elementos.
- **Dentro de la solución que hará de CPD *On-Premises* (Cloud Privado)** Desplegar de un entorno de emulación GNS3 en laboratorio que servirá para abstraerse y conceptualizar la implementación del CPD On-premises de la empresa.
- Además, el entorno de GNS3, se deberán contar con diferentes **IOS compatibles y que soporte además IPsec y BGP**.
- **Se debe contar con un enrutador de operadora tradicional que soporte NAT-T** o lo que es lo mismo (NAT *traversal*), que permitirá que las IP NAT logren atravesar el punto final y que además la negociación IKE e IPsec se establezca satisfactoriamente.
- Será necesario, además, el despliegue de un **sistema de virtualización como VMware Workstation** que conecte con el proyecto de GNS3 y despliegue las máquinas virtuales necesarias como la del servidor NMS.

3.2. Explicación de la arquitectura a alto nivel

La arquitectura general del sistema de monitorización en la nube híbrida y su diseño asociado es la consecuencia de garantizar la supervisión continua y eficiente de los dispositivos desplegados tanto en el entorno local como en la nube pública como se ha explicado en los puntos anteriores.

Esta arquitectura se compone de varios **componentes clave** que interactúan entre sí para recopilar datos de rendimiento, estado y seguridad de la red.

A continuación, se detalla la arquitectura general y se justifica su diseño:

Componentes de la arquitectura:

1. **VPC en la Nube Pública (AWS):** Este componente proporciona la infraestructura virtual necesaria en la nube pública para alojar los dispositivos y servidores monitorizados. Actúa como punto de conexión con los elementos de la red y facilita la comunicación entre los entornos local y remoto.

2. **CPD On-Premises (Cloud Privado):** Representa el entorno local de la empresa donde se encuentran los dispositivos físicos y servidores que también deben ser monitorizados. Se establece una conexión segura entre el CPD local y la VPC en la nube para garantizar la integridad de los datos.
3. **Sistema de Monitorización Centralizado:** Este componente se encarga de recopilar, procesar y visualizar los datos de rendimiento y estado de los dispositivos gestionados en la red híbrida. Proporciona un dashboard central que permite a los administradores supervisar la red en tiempo real y tomar decisiones informadas.
4. **Agentes de Monitorización:** Se despliegan en los dispositivos gestionados para recopilar información específica sobre su funcionamiento y estado. Estos agentes envían datos al sistema de monitorización centralizado para su análisis y presentación.

Interacción de alto nivel:

- La VPC en la nube pública y el CPD On-Premises establecen una conexión segura a través de protocolos como IPSec y BGP, permitiendo la comunicación bidireccional entre los entornos.
- Los agentes de monitorización instalados en los dispositivos gestionados recopilan datos de rendimiento y estado, que son enviados al sistema centralizado para su procesamiento.
- El sistema de monitorización centralizado recibe, almacena y visualiza la información recopilada, proporcionando a los administradores una visión completa y actualizada del estado de la red híbrida.

Justificación del diseño dentro del proyecto:

- Esta arquitectura garantiza la conectividad segura entre los entornos local y en la nube, permitiendo una supervisión efectiva de todos los dispositivos.
- La centralización de la monitorización facilita la gestión y el mantenimiento de la red, asegurando una respuesta rápida ante posibles incidencias.
- La interacción entre los componentes permite una monitorización proactiva y en tiempo real, contribuyendo a la seguridad y eficiencia de la infraestructura de red híbrida.

Estos elementos en su conjunto dotarán la capacidad necesaria para proporcionar una supervisión de la red integral y en tiempo real, cumpliendo de este modo los objetivos marcados en los apartados anteriores.

3.3. Matriz de funcionalidades y protocolos asociados

A continuación, se adjunta una matriz explicativa relativa a funcionalidad de la solución por protocolo adoptado:

ÁMBITO	FUNCIONALIDAD	PROTOCOLO / ESTÁNDAR	DESCRIPCIÓN
GLOBAL	Monitorización	SNMP v2	Implementación de SNMP v2

CPDs	Conectividad	IP - Routing estático	Configuración routing estático dispositivos finales
EDGE	Conectividad	BGP - Routing estático	Conectividad BGP para intercambio de prefijos
EDGE	Conectividad	IPSec	Suite de protocolos para dotar comunicaciones seguras extremo a extremo
CPD On-Premise	Conectividad	802.1Q - VLAN	Conectividad capa 2 para segmentar redes por funcionalidad
CPDs	Monitorización	Syslog	Implementación envío de mensajes por <i>Syslog</i>

3.4. Elementos clave dentro de la solución por funcionalidad

Del lado de los elementos clave que forman parte del proyecto, se identifican los siguientes:

ITEM	FUNCIONALIDAD	DESCRIPCIÓN
GNS3	Emulación	Entorno emulación
VMWare Workstation	Virtualización	Entorno virtualización
Enrutador CPE	Encaminamiento	Concentrador BGP - IPSEC
Switch	Conmutación y segmentación	Conmutador de CPD
Máquina virtual	Estación final	Equipo final virtualizado
VPC	Zona virtual	Zona virtual AWS
Versión IOS	Firmware Cisco Systems	Versión firmware Cisco
Customer Gateway	Interfaz AWS – VPN	Conector entre AWS y VPN
Virtual Private Gateway	Conector Gateway con VPC	Conexión con la zona VPC
Túnel IPSec	Conexión VPN IPSec	Seguridad VPN IPSEC S2S
Sistema Autónomo BGP	Enrutamiento <i>eBGP</i>	Se define la conexión BGP contra el ASN
LibreNMS	Software NMS	Solución de monitorización para conformar NMS

3.5. Comparación de las opciones disponibles

Del lado del tipo de **arquitectura de comunicaciones** se hace el siguiente análisis con las diferentes opciones ([ver anexo para más detalle](#)):

Posibilidades para tratar para dotar comunicaciones en redes híbridas	Ventajas	Inconvenientes
Monitorización sobre infraestructura VPN/MPLS	Se garantiza los cumplimientos de SLA por parte de proveedor. Mayores garantías de seguridad.	Requiere una gran inversión con operadora

Monitorización sobre infraestructura VPN IPSec	Supone un ahorro de costes frente a una solución basada en VPN	Cierta complejidad en la configuración adicional.
Monitorización de infraestructuras en redes compartidas	Simplificación del despliegue de la solución	Seguridad comprometida para las organizaciones.

Por el lado de las opciones disponibles dentro de las **soluciones de NMS** se identifica lo siguiente ([ver anexo para mayor detalle](#)):

Opciones analizadas en NMS	Ventajas	Inconvenientes
LibreNMS	Integración con otros proyectos SW Amplia integración para entornos de redes	No tiene infraestructura en HA
Nagios	Muy usado en infraestructuras de sistemas. Generación de alertas en tiempo real	No tiene infraestructura en HA Complejidad en la configuración y mantenimiento
Zabbix	Plantillas disponibles creadas por la comunidad.	No tiene infraestructura en HA

Del lado de opciones disponibles dentro del **ámbito de servicios IaaS** se identifica lo siguiente ([ver anexo para mayor detalle](#)):

Opciones analizadas en proveedores IaaS	Ventajas	Inconvenientes
Microsoft Azure	Mayor adopción en empresas con soluciones O365	Sigue estando por detrás de AWS en profundidad de mercado y soluciones
Google Cloud Platform	Muy usado en soluciones avanzadas como IA, ML	No tiene gran profundidad de mercado en soluciones de conectividad
Amazon Web Services (AWS)	Líder en soluciones IaaS Mayor documentación generada por la comunidad	Estancamiento en soluciones a largo plazo

Relativo a las opciones analizadas del lado de **implementación de IPSec** ([ver anexo para mayor detalle](#)):

Modo Túnel de IPsec	Modo Transporte de IPsec
En este modo, todo el paquete IP original, incluida la cabecera IP, se cifra y se encapsula dentro de otro paquete IP.	En este modo, solo la carga útil del paquete IP se cifra y se autentica, dejando intactas las cabeceras IP originales.

Es útil para crear conexiones seguras entre dos redes, como una VPN sitio a sitio, donde los datos deben atravesar redes públicas no seguras.	Es adecuado para proteger la comunicación punto a punto dentro de una misma red o entre dos hosts.
El paquete IP original se convierte en la carga útil del nuevo paquete IP, y este último se dirige hacia el destino a través de la red segura.	La encapsulación se realiza solo en los datos del paquete, lo que minimiza el impacto en el tamaño total del paquete y en la sobrecarga de procesamiento.
El modo túnel proporciona un alto nivel de seguridad y privacidad para toda la comunicación entre las dos redes, pero puede tener un mayor costo computacional debido a la encapsulación de los paquetes completos.	Aunque ofrece seguridad para los datos transportados, no protege la información de la cabecera IP, lo que significa que cierta información sobre la comunicación puede ser visible para terceros.

Por la parte del estudio de la conectividad y *routing* de la solución, se identifican las siguientes opciones para ser incorporadas ([ver anexo para más detalle](#)):

Opciones analizadas en conectividad y routing dinámico	Ventajas	Inconvenientes
EIGRP	Fácil implementación	No tan robusto en políticas de routing No apto para redes malladas No estandarizado Menos seguro que BGP
BGP	Solución estandarizada Soportada por todos los fabricantes Gran flexibilidad para políticas de routing Solución muy usada en diseños de redes VPN	Implementación compleja

Analizando los entornos de simulación y virtualización a desplegar, se extrae el siguiente cuadro ([ver anexo para más detalle](#)):

Opciones analizadas sobre entornos de virtualización	Ventajas	Inconvenientes
EVE-NG	Interfaz ligero	Problemas de compatibilidad reportados Producto no tan maduro como otras alternativas Solución gratis pero limitada
GNS3	Solución consolidada Alta colaboración en la comunidad	Requiere cliente pesado

3.6. Selección y justificación de la solución

Una vez analizada cada una de las tecnologías identificadas en los puntos anteriores y analizando las ventajas e inconvenientes de cada una de ellas se procede a extraer una matriz resultante.

La matriz resultante de las tecnologías y soluciones que formarán parte de la solución será:

Tecnología / Solución necesaria a implementar	Tecnología / Solución / Producto a incorporar
Arquitectura VPN	VPN IPSec Site-to-Site (S2S)
NMS	LibreNMS
Proveedor IaaS	Amazon AWS
Modo de Operación IPSec	IPSec modo túnel
Protocolo de routing dinámico	BGP
Entorno de virtualización / emulación	GNS3

3.7. Diseño de la solución y diagramas de servicio

A continuación, se exponen diferentes diseños atendiendo a diferentes clasificaciones:

3.7.1. Diseño de la solución y arquitectura *cloud* (HLD)

Se adjunta diagrama de diseño de la solución de monitorización conceptualizado a nivel *cloud*:

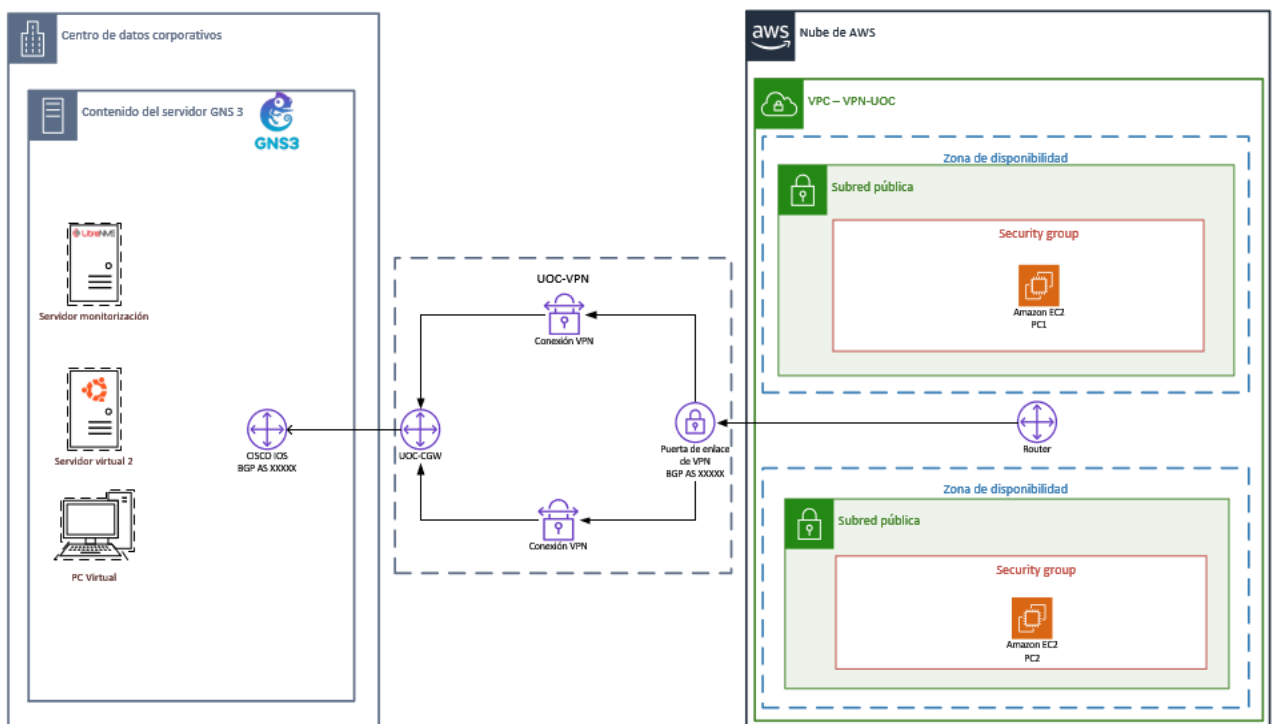


Ilustración 6 Diseño de la solución y arquitectura *cloud*

El diseño dará respuesta a los requisitos indicados en los apartados anteriores garantizando la conectividad entre el centro de datos corporativos (infraestructura on-premises) y el centro de datos situado en la nube pública (AWS).

3.7.2. Diseño de la solución propuesta a bajo nivel (LLD) en capa 3

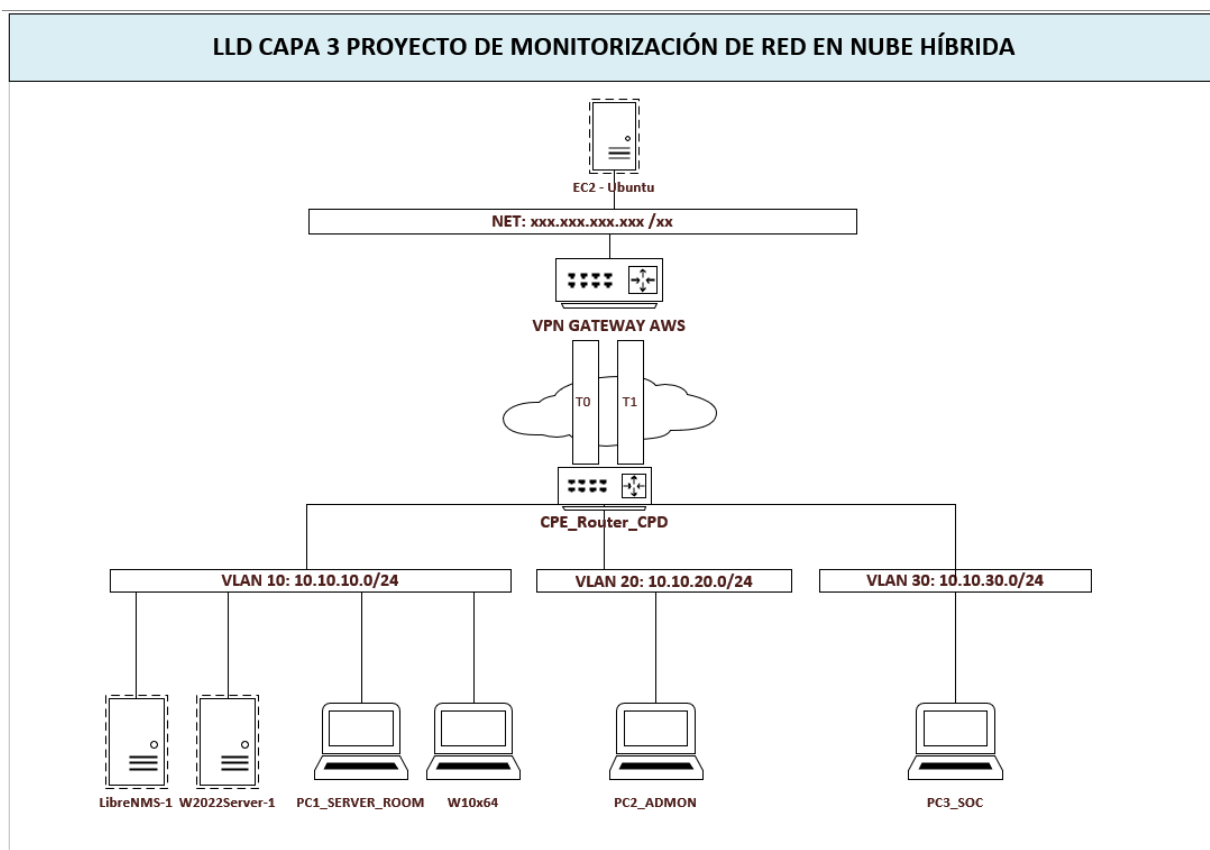


Ilustración 7 Diseño de la solución propuesta a bajo nivel. Capa 3 (red).

3.7.3. Diseño del proyecto en entorno GNS3

A continuación, se muestra como quedaría el diseño del proyecto dentro del propio entorno de emulación GNS3:

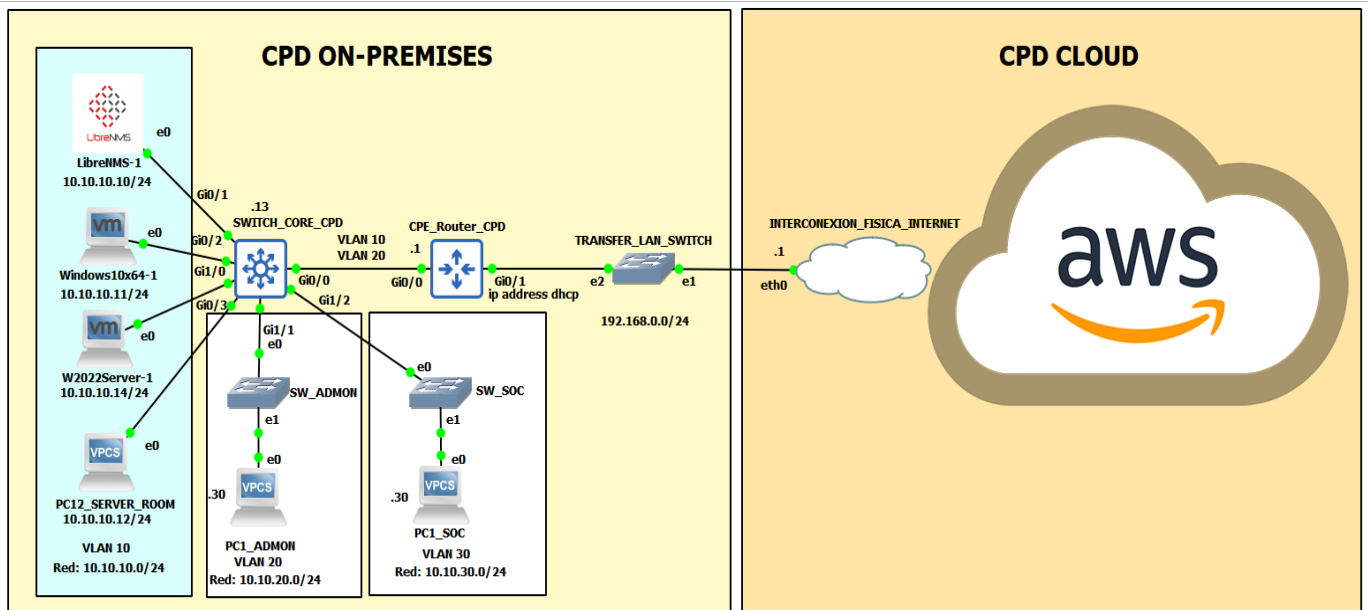


Ilustración 8 Diseño del proyecto en entorno GNS3

Se puede apreciar que, para obtener conectividad con la infraestructura pública en la nube, se requiere hacer una conexión tipo puente al adaptador de red del entorno lo que permitiría el entorno virtualizado formar parte de la red local con acceso a Internet.

3.7.4. Flujo de comunicaciones (matriz)

Con el fin de identificar el flujo de comunicaciones crítico para el correcto funcionamiento de la solución y aplicar las medidas de seguridad oportunas, se decide implementar una matriz de tráfico asociando sentido de la comunicación, dirección IP, puerto necesario y si es TCP o UDP:

ORIGEN	DESTINO	PUERTO	CAPA 4	DESCRIPCIÓN
10.10.10.10/24	172.31.0.0/16	161	UDP	Permitir conexión SNMP <i>Pool</i> a agentes
172.31.0.0/16	10.10.10.10/24	162	UDP	Permitir envíos SNMP <i>Trap</i> a NMS
10.10.10.11/24	172.31.0.0/16	22	TCP	Permitir conexiones entrantes SSH
172.31.0.0/16	10.10.10.10/24	514	UDP	Permitir conexiones entrantes Syslog a NMS
10.10.0.0/16	172.31.0.0/16	80	TCP	Permitir conexiones web HTTP a AWS
10.10.0.0/16	172.31.0.0/16	443	TCP	Permitir conexiones web CPD On-Prem, HTTPS AWS

3.8. Inventario de la solución

A continuación, se identifican los diferentes tipos de inventario clasificados por el tipo, versión y nemónico:

NEMÓNICO	IP	TIPO	VERSIÓN	SITE
LibreNMS-1	10.10.10.10/24	NMS	24.3.0.5	CPD On-Premises

Windows10x64-1	10.10.10.11/24	Endpoint (VM)	W10	CPD On-Premises
PC1_Server_Room	10.10.10.12/24	Endpoint (VPC)	0.8.3	CPD On-Premises
Int_Vlan_10_SW_Admon	10.10.10.13/24	SVI	N/A	CPD On-Premises
W2022Server-1	10.10.10.14/24	W Server	W2022 Server	CPD On-Premises
PC2_Admon	10.10.20.30/24	Endpoint (VPC)	0.8.3	CPD On-Premises
Int_Vlan_11_SW_Admon	10.10.20.13/24	SVI	N/A	CPD On-Premises
PC3_SOC	10.10.30.30/24	Endpoint (VPC)	0.8.3	CPD On-Premises
CPE_Router_CPD	10.10.10.1/24 10.10.20.1/24 10.10.30.1/24	Router CPE	15.9(3)M3	CPD On-Premise
<i>i-0cee8f4f03d6cbd23</i>	172.31.18.15/16	Server Ubuntu	Acting	CPD AWS

4. Implementación de la solución técnica

En este capítulo se detallarán todos los aspectos de la implementación del diseño presentado en el apartado anterior ([capítulo 3. “Diseño de la solución”](#)).

Como a lo largo del documento se tratará de diferenciar los diferentes elementos críticos que forman parte del proyecto de monitorización de la red híbrida corporativa.

4.1. Implementación del entorno de CPD local

Para la implementación del entorno que hará las funciones del CPD local se ha optado por usar GNS3 [10] y VMware Workstation [11] que ofrecerá todo el entorno de comunicaciones y sistemas del CPD *on-premises*.

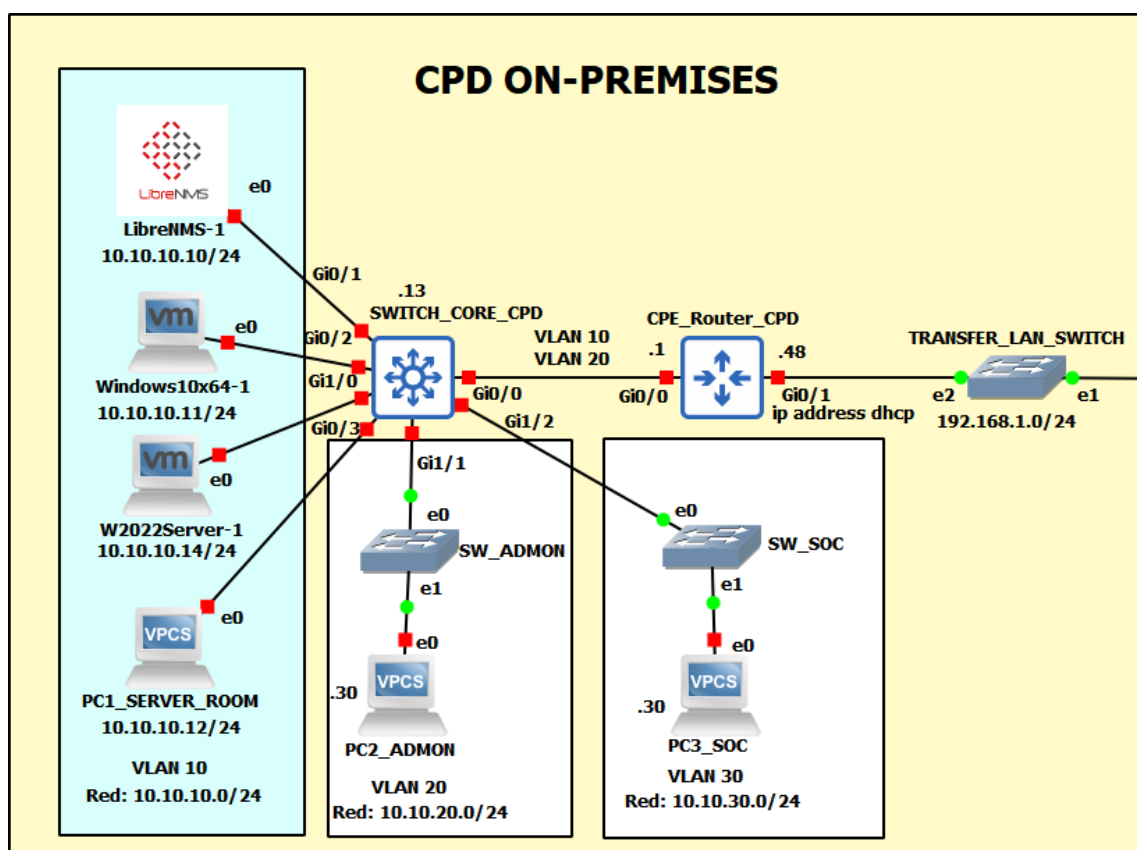


Ilustración 9 Infraestructura virtualizada del CPD On-premises objeto del proyecto

Como se puede apreciar en la ilustración, se aprecia un esquema de red implementado en GNS3 donde se ha tratado de reproducir a nivel de comunicaciones, todo el entorno que formaría parte del CPD *On-premises*, contando con los elementos imprescindibles para desplegar la solución NMS y el *router* del CPD que tendrá una labor fundamental a la hora de establecer las comunicaciones con el Cloud público.

Adicionalmente se pueden apreciar algunos elementos auxiliares para dar un ámbito más complejo tratando de representar diferentes departamentos de la empresa en sus respectivas *vlan*s y su rango de direccionamiento asociado. En los siguientes puntos se tratarán los aspectos de implementación del entorno en el CPD local (on-premises):

4.1.1. Implementación del entorno de virtualización para realizar funciones de CPD local

Para la implementación del entorno de virtualización se ha tenido muy presente una correcta segmentación tanto a nivel de capa 2 (capa de enlace), como de capa 3 (capa de red).

Además, como se indica en sucesivos puntos, se ha seguido un orden que permita ir cerrando todos los requisitos técnicos que se identificó en [capítulo 2 “Análisis de la solución y requisitos técnicos”](#).

Despliegue de comunicaciones en CPD local

Se definen las configuraciones en base al plan de direccionamiento y se segmenta la red a nivel de capa 2 mediante el uso de VLANS también definidas.

Para ello se han configurado tanto el switch como el router de CPD On-premises.

Dicha configuración se ha hecho de forma secuencial, primero resolviendo los problemas de conectividad a nivel de VLAN y luego a nivel de IP mediante el uso de rutas estáticas y ruta por defecto para identificar el dispositivo que concentrará las peticiones para dar salida bien a Internet o bien al CPD remoto que será el *cloud*.

```
SWITCH_CORE_CPD#show run | i ip route
ip route 0.0.0.0 0.0.0.0 10.10.10.1
ip route 0.0.0.0 0.0.0.0 10.10.20.1
ip route 0.0.0.0 0.0.0.0 10.10.30.1
```

Ilustración 10 configuración de routing en switch de CPD local

```
alberto@LibreNMS:~$ route
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
default          _gateway       0.0.0.0        UG    20100 0      0 ens33
10.10.10.0       0.0.0.0        255.255.255.0  U    100   0      0 ens33
link-local       0.0.0.0        255.255.0.0    U    1000  0      0 ens33
alberto@LibreNMS:~$
```

Ilustración 11 configuración del routing en la máquina NMS que realiza los pools SNMP al resto de equipos gestionados

Implementación del router CPE del CPD local (appliance Cisco)

Se despliega a través de GNS3 un *appliance* virtual de Cisco Systems cuya versión es **Cisco IOSv 15.9(3)M3**. La configuración de este está detallada en el anexo correspondiente.

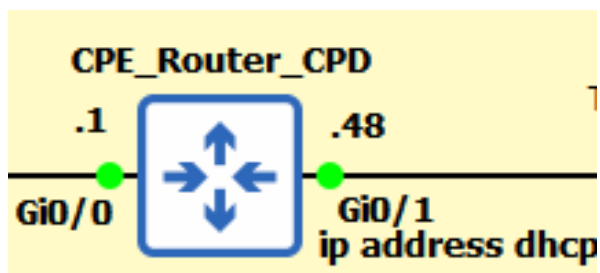


Ilustración 12 Esquema del router CPD local (on-premises)

La IP que va a negociar en **Gi0/1** va a ser por **DHCP** contra el router residencial físico y salida a Internet.

```
CPE_ROUTER_CPD#show ip int brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0      unassigned      YES NVRAM   up          up
GigabitEthernet0/0.10   10.10.10.1      YES NVRAM   up          up
GigabitEthernet0/0.20   10.10.20.1      YES NVRAM   up          up
GigabitEthernet0/0.30   10.10.30.1      YES NVRAM   up          up
GigabitEthernet0/1      192.168.1.48    YES DHCP    up          up
GigabitEthernet0/2      unassigned      YES NVRAM   administratively down down
GigabitEthernet0/3      unassigned      YES NVRAM   administratively down down
CPE_ROUTER_CPD#
```

Ilustración 13 Obtención de la IP por DHCP el CPE On-Premises

Por la parte **LAN** se configura como encapsulación **802.1Q** para soportar el diseño de **“router on a stick”**.

Implementación del switch de CPD local (appliance Cisco)

El **switch virtual de Cisco** también se despliega a través de **GNS3** y esto se debe a que este elemento va a ser una pieza clave para realizar la segmentación de redes por funcionalidad:

```
SWITCH_CORE_CPD#show vlan
VLAN Name                Status      Ports
-----
1    default                 active      Gi1/3, Gi2/0, Gi2/1, Gi2/2
                                           Gi2/3, Gi3/0, Gi3/1, Gi3/2
                                           Gi3/3
10   VLAN_10_SERVERS_CPD     active      Gi0/1, Gi0/2, Gi0/3, Gi1/0
20   VLAN_20_OFICINAS_CPD    active      Gi1/1
30   VLAN_30_SOC              active      Gi1/2
1002 fddi-default            act/unsup
1003 token-ring-default     act/unsup
1004 fddinet-default         act/unsup
1005 trnet-default          act/unsup
```

Ilustración 14 Implementación de las diferentes VLANs de servicio que forman parte del CPD Local

Como se puede apreciar, las etiquetas por VLAN serán las siguientes:

- 10 VLAN_10_SERVERS_CPD
- 20 VLAN_20_OFICINAS_CPD
- 30 VLAN_30_SOC

Todas definidas con un propósito que es el de separación de tráfico por funcionalidad teniendo más seguridad en capa 2.

4.1.2. Implementación del servidor de monitorización en CPD local

Instalación y configuración del servidor LibreNMS

Se parte de un despliegue mediante una máquina virtual basada en Linux (distribución Ubuntu).

Posteriormente se hace la instalación a nivel de producto **siguiendo las recomendaciones de la página oficial del software** [12].

Se configura para tener a nivel de comunicaciones conectividad con el resto de entorno GNS3.

Configuración de agentes SNMP en equipamiento CPD on-premises

Dependiendo del tipo de dispositivo, la configuración de SNMP se ha realizado de una forma diferente.

Del lado del router CPE que realizará las conexiones IPsec y BGP contra la infraestructura *cloud*, se han definido de la siguiente manera:

```
CPE_ROUTER_CPD#show run | i snmp
mmi snmp-timeout 180
snmp-server community UOC R0
snmp-server location 36205, Vigo, Spain
snmp-server contact afernandezsanchez0@uoc.edu
snmp-server chassis-id
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
```

Ilustración 15 Configuración de SNMP en equipamiento Cisco para gestionar desde NMS

De este modo se logrará que el enrutador CPE pueda escuchar las peticiones SNMP que le van a llegar del servidor de gestión e integrarlo como equipo a monitorizar.

4.2. Implementación del entorno en el CPD cloud

Siguiendo al análisis de la solución, se pasaría a tratar la parte de la implementación en el CPD en la nube.

Como se ha ido apreciando en la parte de análisis, una parte fundamental de este punto va a consistir en dotar conectividad con el CPD local y para ello se deben pensar en soluciones como se han mencionado de IPsec con BGP lo que haría una solución robusta y poder enviar las notificaciones SNMP de totalmente seguras al servidor de gestión.

Es por ello, por lo que se deberá ir desplegando diferentes elementos que serán importantes del lado *cloud* que ayudarán a la resolución de la problemática de la conectividad en la red híbrida entre elementos desplegados en la nube y elementos desplegados on-premises.

4.2.1. Creación del VPC en AWS

El primer paso para considerar como elemento fundamental en la solución cloud es el **VPC (Virtual Private Cloud)** dado que ayudará a dotar eficiencia, seguridad y estabilidad a la solución de la infraestructura que desplegaremos.

Al establecer una VPC, se podrán desplegar diferentes instancias a medida de una forma dinámica y flexible dotando de la solución que sea tremendamente adaptable a nuestros propósitos.

vpc-e203e49f

Detalles | Mapa de recursos | CIDR | Registros de flujo | Etiquetas | Integraciones

Detalles	
ID de la VPC vpc-e203e49f	Estado Available
Tenencia Default	Conjunto de opciones de DHCP dopt-4656d63c
VPC predeterminada Sí	CIDR IPv4 172.31.0.0/16
Métricas de uso de direcciones de red Desactivado	Grupos de reglas del firewall de DNS de Route 53 Resolver -

Ilustración 16 VPC resultante en AWS

Además, ayudará a desplegar nuevas máquinas virtuales que a su vez estarán enviando información SNMP al servidor central, por lo que tendríamos una red altamente monitorizada.

Las redes asociadas a su vez irán conectadas a otros elementos que permitirán su propagación hasta el CPD On-premises como pueden ser el IGW (Internet Gateway).

4.2.2. Creación del Customer Gateway en AWS

En el contexto de AWS, el CGW (Customer Gateway) sería el componente clave que nos va a permitir la configuración y despliegue de la conexión VPN (Virtual Private Network) entre la infraestructura de la nube pública de AWS y la red local del CPD.

VPC > Gateways de cliente > cgw-0eb0b6bc1e42ea782

cgw-0eb0b6bc1e42ea782 / UOC-CGW [Información](#)

Detalles

ID de la gateway de cliente cgw-0eb0b6bc1e42ea782	Estado ✔ Disponible	Tipo ipsec.1
BGP ASN 65000	ARN del certificado -	Dispositivo -

Etiquetas

Etiquetas 1

Q Buscar etiquetas

Clave	Valor
Name	UOC-CGW

Ilustración 17 Resultado del Customer Gateway en AWS

También va a ejercer un papel fundamental en la solución final de la red de monitorización híbrida debido a que va a permitir una conexión segura entre los entornos locales del CPD on-premises y los recursos desplegados en la nube (EC2).

En relación con los objetivos y problemáticas del proyecto, el Customer Gateway va a ayudar en los siguientes puntos:

- Conectividad segura entre entornos.
- Integración de las infraestructuras.
- Escalabilidad y flexibilidad

4.2.3. Creación de Virtual Private Gateway (VGW)

Otro de los elementos fundamentales en el proceso de la creación de la conectividad para la red híbrida resultante que nos servirá de base para el sistema de monitorización es el conocido Virtual Private Gateway.

Al implementar un VGW en AWS, se crea un enlace seguro que conecta de manera protegida la infraestructura en la nube con las redes locales, permitiendo la integración de sistemas y la transferencia segura de datos. Esta conexión VPN a través del VGW garantiza la privacidad y la integridad de la información transmitida, lo que resulta fundamental para salvaguardar los datos sensibles y críticos de la empresa.

Además, la configuración del Virtual Private Gateway en AWS brinda escalabilidad a la infraestructura de red, permitiendo gestionar múltiples conexiones VPN para adaptarse a las cambiantes necesidades de conectividad de los clientes. Esta capacidad es especialmente relevante en entornos híbridos donde se requiere una comunicación fluida entre los recursos locales y los recursos en la nube.

Gateways privadas virtuales (1/1) [información](#) 🔄 Acciones ▾

🔍 *Buscar recurso por atributo o etiqueta*

Name	ID de la puerta de enlace priv...	Estado	Tipo	VPC	Amazon ASN
UOC-VPG	vgw-00a70f405eeac3feb	🟢 Adjunto	ipsec.1	vpc-e203e49f	64512

Puerta de enlace privada virtual [vgw-00a70f405eeac3feb](#) / UOC-VPG

[Detalles](#) | [Etiquetas](#)

Detalles

ID de la puerta de enlace privada virtual 📄 vgw-00a70f405eeac3feb	Estado 🟢 Adjunto	Tipo ipsec.1	VPC vpc-e203e49f
Amazon ASN 📄 64512			

Ilustración 18 Virtual Private Gateway desplegado para soportar la conexión VPN

Al desplegar el elemento como IPSec, nos aseguramos de que la conexión sea segura y además ya tenemos identificado el sistema autónomo remoto que permitirá el enrutamiento BGP permitiendo de este modo el intercambio de prefijos que serán fundamentales para que tengan conectividad entre ellos y podamos tener la monitorización a nivel global de una forma segura.

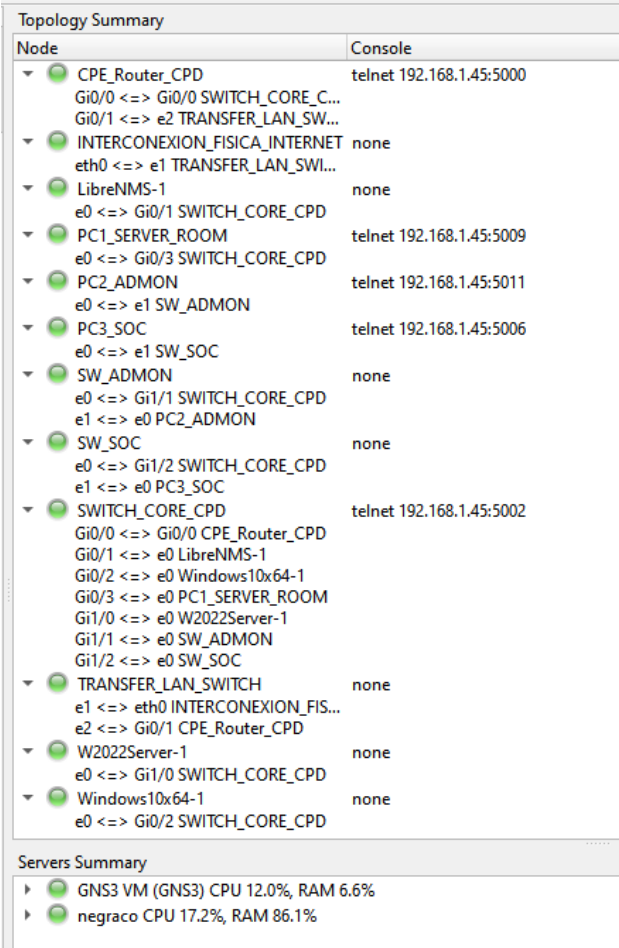
5. Resultados

5.1. Resultados obtenidos a nivel de despliegue del entorno CPD *On-premises*

Se ha conseguido desplegar el equipamiento virtualizado e integrarlo con el software de GNS3, además se consigue verificar que las instancias y *appliances* trabajan correctamente dentro del entorno.

5.1.1. Resultados y pruebas GNS3

Se realizan diversas pruebas a nivel de hipervisor que certifican el correcto funcionamiento de los elementos.



Node	Console
▼ CPE_Router_CPD Gi0/0 <=> Gi0/0 SWITCH_CORE_C... Gi0/1 <=> e2 TRANSFER_LAN_SW...	telnet 192.168.1.45:5000
▼ INTERCONEXION_FISICA_INTERNET eth0 <=> e1 TRANSFER_LAN_SWI...	none
▼ LibreNMS-1 e0 <=> Gi0/1 SWITCH_CORE_CPD	none
▼ PC1_SERVER_ROOM e0 <=> Gi0/3 SWITCH_CORE_CPD	telnet 192.168.1.45:5009
▼ PC2_ADMON e0 <=> e1 SW_ADMON	telnet 192.168.1.45:5011
▼ PC3_SOC e0 <=> e1 SW_SOC	telnet 192.168.1.45:5006
▼ SW_ADMON e0 <=> Gi1/1 SWITCH_CORE_CPD e1 <=> e0 PC2_ADMON	none
▼ SW_SOC e0 <=> Gi1/2 SWITCH_CORE_CPD e1 <=> e0 PC3_SOC	none
▼ SWITCH_CORE_CPD Gi0/0 <=> Gi0/0 CPE_Router_CPD Gi0/1 <=> e0 LibreNMS-1 Gi0/2 <=> e0 Windows10x64-1 Gi0/3 <=> e0 PC1_SERVER_ROOM Gi1/0 <=> e0 W2022Server-1 Gi1/1 <=> e0 SW_ADMON Gi1/2 <=> e0 SW_SOC	telnet 192.168.1.45:5002
▼ TRANSFER_LAN_SWITCH e1 <=> eth0 INTERCONEXION_FIS... e2 <=> Gi0/1 CPE_Router_CPD	none
▼ W2022Server-1 e0 <=> Gi1/0 SWITCH_CORE_CPD	none
▼ Windows10x64-1 e0 <=> Gi0/2 SWITCH_CORE_CPD	none

Servers Summary
▶ GNS3 VM (GNS3) CPU 12.0%, RAM 6.6%
▶ negraco CPU 17.2%, RAM 86.1%

Ilustración 19 Verificación de la topología correcta y funcionando en GNS3

Por lo tanto, las pruebas realizadas para verificar el despliegue del entorno de CPD *On-premises*, se consideran **satisfactorias**.

5.1.2. Resultados y pruebas Appliance Cisco virtual

Se realizan diversas pruebas de verificación de la correcta integración del *appliance* virtual de Cisco:

```
=> show device
QEMU VM CPE_Router_CPD is started
Running on server GNS3 VM (GNS3) with port 80
Local ID is 1 and server ID is 25913611-4173-49fd-a0b2-ec2dc85f238a
Number of processors is 1 and amount of memory is 512MB
Console is on port 5000 and type is telnet
Gi0/0 connected to SWITCH_CORE_CPD on port Gi0/0
  MAC address is 0c:91:36:11:00:00
Gi0/1 connected to TRANSFER_LAN_SWITCH on port Ethernet2
  MAC address is 0c:91:36:11:00:01
Gi0/2 is empty
  MAC address is 0c:91:36:11:00:02
Gi0/3 is empty
  MAC address is 0c:91:36:11:00:03
```

Ilustración 20 Resultado de integración del router CPE Cisco Systems

La versión IOS “*vios-adventerprisek9-m.spa.159-3.m3.qcow2*” carga perfectamente :

```
CPE_ROUTER_CPD#show version
Cisco IOS Software, IOSv Software (VIOS-ADVENTERPRISEK9-M), Version 15.9(3)M3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Wed 27-Jan-21 09:58 by prod_rel_team

ROM: Bootstrap program is IOSv

CPE_ROUTER_CPD uptime is 4 hours, 15 minutes
System returned to ROM by reload
System restarted at 16:20:48 CEST Wed Apr 3 2024
System image file is "flash0:/vios-adventerprisek9-m"
Last reload reason: Unknown reason
```

Ilustración 21 Resultado satisfactorio de integración de la versión IOS y appliance en GNS3

5.2. Resultados obtenidos a nivel de despliegue de entorno Cloud público

A continuación, se recogen los resultados obtenidos relativos al despliegue del entorno Cloud público:

Item	Descripción	Resultado
Despliegue de máquina <i>cloud</i>	Se desplegará una máquina que haga funciones de servidor en <i>cloud</i> gestionable	Satisfactorio
Creación VPN IPSec <i>Cloud</i>	Se desplegará la configuración de una VPN que cuente con seguridad	Satisfactorio

Definición de configuración BGP	Creación de conectividad BGP en <i>cloud</i>	Satisfactorio
---------------------------------	--	---------------

En este punto damos por validada la parte de configuración y despliegue de los elementos críticos de la red híbrida.

5.3. Resultados obtenidos a nivel de comunicaciones IP

La sección relativa a las comunicaciones IP es fundamental para el correcto funcionamiento de los sistemas desplegados.

Como elemento principal tenemos la prueba de levantamiento de túneles asociados a las comunicaciones IPSec:

```
CPE_ROUTER_CPD#show ip int brief | i Tun
Tunnel1      169.254.197.166 YES NVRAM  up
Tunnel2      169.254.204.102 YES NVRAM  up
CPE_ROUTER_CPD#
```

Ilustración 22 verificación de los túneles IP desde el CPE_ROUTER_CPD

Del lado puro IPSec, se verifica el estado de los túneles en ambos extremos:

```
CPE_ROUTER_CPD#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state         conn-id status
100.27.53.11 192.168.1.48 QM_IDLE      1002 ACTIVE
34.192.94.128 192.168.1.48 QM_IDLE      1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

Ilustración 23 Estado de los túneles IPSec desde el lado del router CPE_ROUTER_CPD

Luego del lado del Cloud AWS, se verifica satisfactoriamente el estado de los túneles:

Conexión de VPN vpn-0dde3fedcb97043bb / UOC-VPN

Detalles Detalles del túnel Etiquetas

Estado del túnel						
Número de túnel	Dirección IP externa	CIDR IPv4 interno	CIDR IPv6 interno	Estado	Último cambio de estado	
Tunnel 1	34.192.94.128	169.254.197.164/30	-	Arriba	May 29, 2024, 10:30:28 (UTC+02:00)	
Tunnel 2	100.27.53.11	169.254.204.100/30	-	Arriba	May 29, 2024, 10:28:19 (UTC+02:00)	

Verificación correcta de los túneles del lado de AWS

Ilustración 24 Validación del estado de los túneles desde AWS

Finalmente del lado de las sesiones BGP, se comprueba que se reciben los prefijos correspondientes al cloud y que ambas sesiones quedan correctamente establecidas:

```

CPE_ROUTER_CPD#show ip bgp summary
BGP router identifier 169.254.204.102, local AS number 65000
BGP table version is 12, main routing table version 12
8 network entries using 1152 bytes of memory
10 path entries using 840 bytes of memory
5/3 BGP path/bestpath attribute entries using 800 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2816 total bytes of memory
BGP activity 8/0 prefixes, 10/0 paths, scan interval 60 secs

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
169.254.197.165 4      64512   184    194     12   0    0 00:29:39    1
169.254.204.101 4      64512   183    195     12   0    0 00:29:33    1
CPE_ROUTER_CPD#

```

Ilustración 25 Estado de las sesiones eBGP contra el Cloud AWS

Se define la siguiente matriz de conectividad IP para verificar que los criterios mínimos de conexión se cumplen:

Item	Descripción	Resultado
Comunicación interna CPD On-Premises	Se verifica conectividad IP a nivel interno entre todos los equipos del CPD local	Satisfactorio
Comunicación interna CPD Cloud	Se verifica conectividad del equipamiento desplegado en la nube	Satisfactorio
Establecimiento de sesión BGP red híbrida	Se verifica el establecimiento de sesión BGP entre el equipamiento local y el remoto, además del intercambio de prefijos IP	Satisfactorio
Conectividad IP entre servidor NMS y dispositivos gestionados	Se verifica conectividad IP entre el servidor NMS y los dispositivos gestionados	Satisfactorio

Con esto se verifica satisfactoriamente que la infraestructura a nivel de comunicaciones está configurada correctamente y que los elementos críticos de la infraestructura híbrida cuentan con la conectividad IP necesaria para pasar al siguiente punto de la conectividad a nivel de SNMP.

5.4. Resultados obtenidos a nivel de monitorización SNMP

En este apartado se tratará las diferentes pruebas a nivel SNMP en diferentes ámbitos.

Se han realizado diversas pruebas tanto a nivel de pool SNMP como a nivel de producto para validar la solución mediante comandos “snmpwalk”:

```

snmpwalk -v2c -c UOC localhost
snmpwalk -v2c -c UOC 10.10.10.13
snmpwalk -v2c -c UOC 10.10.10.1
snmpwalk -v2c -c UOC 172.31.18.15

```



```

alberto@LibreNMS:~$ sudo snmpwalk 10.10.10.1 -v2c -c UOC
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software, IOSv Software (VIOS-ADVENTERPRISEK9-M)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Wed 27-Jan-21 09:58 by prod_rel_team"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.1041
iso.3.6.1.2.1.1.3.0 = Timeticks: (139493) 0:23:14.93
iso.3.6.1.2.1.1.4.0 = STRING: "afernandezsanchez@uoc.edu "
iso.3.6.1.2.1.1.5.0 = STRING: "CPE_ROUTER_CPD.uoc-lab.com"
iso.3.6.1.2.1.1.6.0 = STRING: "36205, Vigo, Spain"
iso.3.6.1.2.1.1.7.0 = INTEGER: 70

```

Ilustración 26 Ejemplo de salida de validación por snmpwalk contra el router principal del CPD Local

Una vez cubierto y evaluado los resultados de conectividad a nivel IP, se puede comprobar la lista de resultados obtenidos que ayudarán a evaluar el éxito del desarrollo del proyecto:

Item	Descripción	Resultado
Conectividad SNMP dentro del propio NMS	Se realizará comandos "snmpwalk" para verificar la correcta implementación del servicio SNMP en el NMS	Satisfactorio
Verificación de conectividad SNMP desde NMS a elementos gestionados del CPD local	Se realizarán diferentes pruebas de conectividad vía "snmpget" desde el servidor de gestión a los elementos gestionados dentro del propio CPD local	Satisfactorio
Verificación de conectividad SNMP desde NMS a elementos gestionados en el CPD del cloud	Se realizan pruebas de snmpget y pool snmp desde NMS a elementos remotos del cloud público	Satisfactorio

5.5. Resultados obtenidos a nivel de plataforma de monitorización

Cuando ya quedan verificados los elementos más básicos que tendrá la solución tanto a nivel de arquitectura, conectividad IP y conectividad SNMP, se puede realizar la fase de verificación de pruebas y toma de resultados más focalizado a nivel de producto NMS, que como se indica en los apartados anteriores, será el servidor que consiga almacenar toda la información procedente de la red híbrida y representarla en modo gráfico a través de una interfaz web.

Es por eso por lo que centrándonos a nivel de producto LibreNMS se establece una serie de pruebas con sus respectivos resultados asociados:

Item	Descripción	Resultado
Creación y personalización de un <i>dashboard</i>	Se creará y personalizará un tablero que sirva para aglutinar los eventos más representativos de la red y el estado de esta	Satisfactorio
Alta, modificación y baja de dispositivos gestionados	Se verificará que se puede dar de alta elementos gestionados en el NMS mediante comunidad SNMP fijada. Del mismo modo se	Satisfactorio

	podrá modificar y borrar dicho elemento	
Inventario de dispositivos	Prueba de creación de inventario de dispositivos gestionados	Satisfactorio
Gráficas de estado de red	Gráficas generadas por los datos obtenidos a través de SNMP por equipo	Satisfactorio
Alta, baja y modificación de usuarios	Se definirán diferentes usuarios que puedan acceder al sistema de monitorización	Satisfactorio
Recepción de logs centralizados en la NMS	Se visualizarán los logs aglutinados en la misma NMS enviados por los diferentes elementos de red.	Satisfactorio

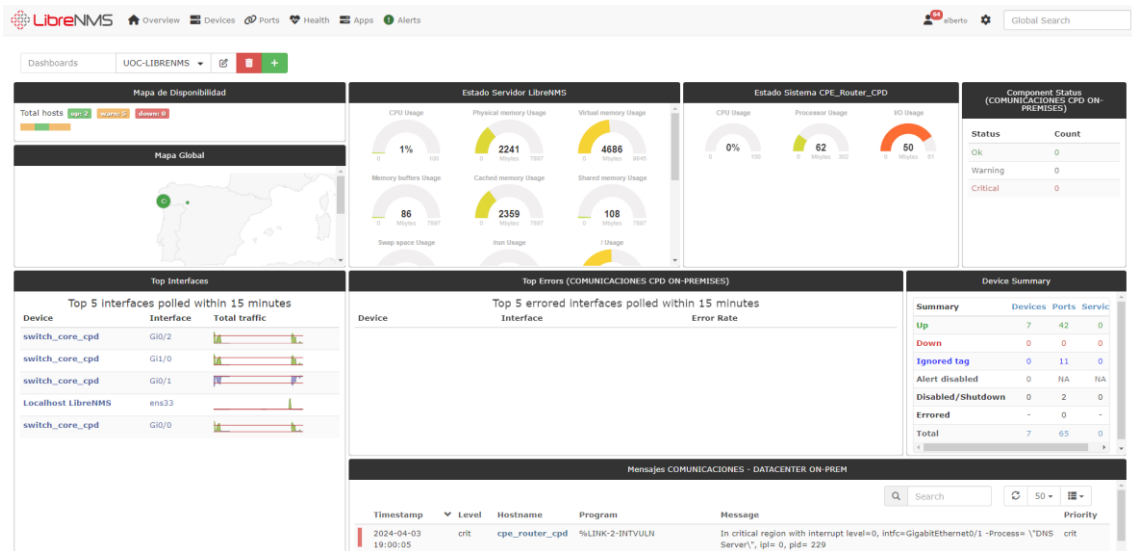


Ilustración 27 Creación de dashboard en LibreNMS satisfactoria

6. Conclusiones y nuevas líneas de trabajo

6.1. Conclusiones del trabajo

La evolución de las comunicaciones ha supuesto un nuevo paradigma que ha obligado a adaptarse a unas nuevas necesidades al entrelazarse el mundo tradicional de comunicaciones, con las infraestructuras basadas en la nube.

En consecuencia, las empresas cada vez han requerido una mayor supervisión obligando de este modo tener los dispositivos vigilados y monitorizados para garantizar la disponibilidad y continuidad del negocio.

El proyecto que se ha presentado "*Implementación de una herramienta de monitorización de redes en una nube híbrida*", ha pretendido dar respuesta a las necesidades habituales que se puede plantear cualquier organización hoy en día, con el ánimo de desplegar sistemas (en este caso de monitorización) desplegados en diferentes ámbitos, tanto *on-premises* como en la nube pública.

El caso de presentar el proyecto basado en el sistema de monitorización ha servido para identificar las típicas necesidades de las empresas y la problemática asociada a las mismas en términos de seguridad.

En el proyecto, se ha propuesto un diseño de un servidor de monitorización situado en infraestructura local, pero con conectividad con la nube pública, definiendo así lo que se conoce una red híbrida, teniendo conectividad SNMP con cada uno de los elementos gestionados.

La realización del presente proyecto ha ayudado en lo personal a aprender cómo establecer comunicaciones en entornos de redes híbridas y desplegar sistemas de monitorización que ayuden a conocer el estado de una red compleja.

Ha sido un desafío técnico el hecho de conseguir conectividad desde un entorno emulado como es el GNS3 hasta un entorno basado en la nube como es AWS pero gracias a la documentación oficial se ha conseguido implementar la solución en tiempo y forma.

Del lado de la parte de resultados, como se ha podido verificar en el apartado correspondiente, se ha conseguido cumplir de forma satisfactoria a los puntos enumerados y que debía contar como mínimo la solución propuesta. Una parte que, si ha sorprendido acerca de la parte de implementación, ha sido lo verdaderamente flexible que es la herramienta LibreNMS a la hora de hacer integraciones con todo tipo de dispositivos gestionados y, sobre todo, la posibilidad de integrar con otros proyectos y soluciones.

Atendiendo a la parte de la planificación, aunque si es cierto que se han conseguido alcanzar los hitos propuestos, ha supuesto un hándicap en diferentes fases del proyecto sobre todo en la parte de documentación y formato.

Quizás el riesgo mayor de haber seguido un proyecto clásico en cascada ha sido identificado en la fase final de la implementación cuando se identificaron algunos problemas de alta en la plataforma AWS asociada a la facturación, solventados con un cambio de método de pago pero que retrasó en dos días la planificación.

6.2. Consecución de los objetivos

En este punto se hará un repaso de la consecución de los objetivos técnicos marcados en el inicio del proyecto y el estado de cumplimiento final una vez realizadas las tareas de pruebas:

Objetivos por cubrir de la solución	Conseguido	Comentarios
<i>Implementar un diseño de red robusto</i>	<i>Satisfactoriamente</i>	<i>Se ha implementado una red híbrida robusta que ha permitido ser apta para un escenario de servicio</i>
<i>Conectividad segura entre dispositivos gestionados</i>	<i>Satisfactoriamente</i>	<i>Se ha verificado la conectividad entre los diferentes elementos de red que han conformado la red híbrida</i>
<i>Implementar un protocolo de monitorización estandarizado y sencillo</i>	<i>Satisfactoriamente</i>	<i>Se ha conseguido alcanzar la implementación de SNMP v2c</i>
<i>Desplegar un sistema de monitorización libre basado en Linux</i>	<i>Satisfactoriamente</i>	<i>Se ha configurado y adaptado un sistema de monitorización gracias a LibreNMS</i>
<i>Definición de una red dinámica IP tolerante a fallos</i>	<i>Satisfactoriamente</i>	<i>Se ha implementado una red de comunicaciones con doble túnel y con routing dinámico</i>

6.3. Líneas de trabajo futuras

Aunque a líneas generales se ha conseguido cumplir con creces, también es cierto que el presente proyecto puede servir de base para otros con más funcionalidades que las probadas con la solución LibreNMS en entornos híbridos.

Una vez resuelta la raíz de la problemática identificada, que no es otra que el de garantizar conectividad y seguridad entre todos los elementos gestionados. El modelo se podría replicar en otros entornos

6.3.1. Añadir integración con otras herramientas de monitorización

Queda abierto por lo tanto y atendiendo a la flexibilidad de la solución a integrar con otros tipos de proyectos que pueden garantizar que la solución sea mucho más potente a la hora de monitorizar servicios, gestionar inventariado y lo que es todavía más interesante, la gestión de configuraciones.

Por lo tanto, se propone como futuras líneas de investigación añadir integraciones con los siguientes paquetes y proyectos:

- **Smokeping.** [13]
- **Oxidized.** [14]

6.3.2. Posibilidad de incorporar SNMPv3

Una de las vías a estudiar a futuro, es la implementación de SNMPv3 en escenarios donde el dispositivo lo permita.

Evaluar la posibilidad de incorporar SNMPv3 en la solución de monitorización y el impacto que tendría a nivel de configuración de la solución, dado que la versión 3 del protocolo da mayores garantías y prestaciones a la hora de implementar la solución más segura, al incluir autenticación, privacidad y control de acceso.

Las otras versiones de protocolo carecen de mecanismo nativo de cifrado, como lo podría soportar en el modelo SNMPv3 en el nivel de implementación *authPriv*, soportando mecanismos de autenticación a través del uso de HMAC-MD5 o HMAC-SHA y algoritmos de cifrado como pueden ser DES o AES [15].

7. Glosario

- On-prem: On premises (en local).
- IaaS: Tipo de despliegue en el que el cliente aprovisiona su propia infraestructura en la nube.
- IP: Internet Protocol.
- AWS: Amazon Web Services.
- Azure: Microsoft Azure.
- CIPS: Cloud infrastructure and platform services.
- Framework: entorno o marco de trabajo
- VPN: Virtual Private Network.
- Community: Clave de acceso, dentro del entorno SNMP para intercambiar información de equipos gestionados.
- SNMP: Simple Network Management Protocol
- PC: Personal Computer
- NMS: Network Management Station
- IP: Internet Protocol
- RFC: Request For Comments
- OID: Object Identifier
- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol
- BGP: Border Gateway Protocol
- MIB: Management Information Base
- Traps: Mensajes de notificación enviados por dispositivos de red gestionados por SNMP.
- Switches: Dispositivos de comunicaciones que sirven para conectar segmentos de red.
- Nube Pública: Ref. modelo de Cloud Computing, donde el prestatario da acceso a cualquier cliente que necesite recursos deslocalizados.
- Nube Privada: Ref. modelo de Cloud Computing, donde se prestan servicios en dependencias del cliente.
- Nube Híbrida: Combinación de características de Nube Pública y Nube Privada.
- CPD: Centro de procesamiento de datos.
- SSH: Secure Shell

8. Bibliografía

- [1] A. Shrivastwa, *Hybrid cloud for architects: build robust hybrid cloud solutions using AWS and OpenStack*, 1st edition. Birmingham, [England]; Packt Publishing, 2018.
- [2] Amazon Web Services, “¿Qué es la nube híbrida? - Explicación de la computación en la nube híbrida - AWS.” Accessed: Mar. 10, 2024. [Online]. Available: <https://aws.amazon.com/es/what-is/hybrid-cloud/>
- [3] European Knowledge Center for Information Technology, “Nube híbrida es la última tendencia empresarial,” Nube híbrida o hybrid cloud: la última tendencia empresarial. Accessed: Mar. 10, 2024. [Online]. Available: <https://www.ticportal.es/noticias/cloud-computing/nube-hibrida-tendencia-empresarial>
- [4] “¿Cómo incorporar la competencia ‘Comportamiento ético y global’ al Trabajo Final (TF)?”
- [5] J. A. Sarmiento Rojas, C. H. Correa Candamil, and D. E. Jiménez Roa, *Gestión de proyectos aplicada al PMBOK 6ED*. in Colección investigación UPTC. Tunja: Editorial UPTC, 2020.
- [6] “Metodologías de Gestión de Proyectos - OPM Integral.” Accessed: Mar. 12, 2024. [Online]. Available: <https://opmintegral.com/gestion-de-proyectos/metodologias-de-gestion-de-proyectos/>
- [7] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, and D. Leaf, “NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and Technology,” 2020. doi: 10.6028/NIST.SP.500-292.
- [8] “(44) Hybrid Cloud Architecture Part 3: Security - YouTube,” Hybrid Cloud Architecture Part 3: Security. Accessed: May 04, 2024. [Online]. Available: https://www.youtube.com/watch?v=_bjDY9omL9I
- [9] R. Samani, *CSA guide to cloud computing : implementing cloud privacy and security*, 1st edition. Waltham, Maryland: Elsevier, 2015.
- [10] Various, “GNS3 Windows Install | GNS3 Documentation,” GNS3. Accessed: Apr. 03, 2024. [Online]. Available: <https://docs.gns3.com/docs/getting-started/installation/windows>
- [11] “Windows VM | Workstation Pro | VMware.” Accessed: Apr. 17, 2024. [Online]. Available: <https://www.vmware.com/products/workstation-pro.html>
- [12] “Installing LibreNMS - LibreNMS Docs.” Accessed: Apr. 05, 2024. [Online]. Available: <https://docs.librenms.org/Installation/Install-LibreNMS/>
- [13] “Smokeping - LibreNMS Docs.” Accessed: May 27, 2024. [Online]. Available: <https://docs.librenms.org/Extensions/Smokeping/>
- [14] “Oxidized - LibreNMS Docs.” Accessed: May 27, 2024. [Online]. Available: <https://docs.librenms.org/Extensions/Oxidized/>
- [15] “Configuración de SNMPv3 para dispositivos que utilizan IOS - Cisco Community.” Accessed: May 27, 2024. [Online]. Available: <https://community.cisco.com/t5/documentos-data-center/configuraci%C3%B3n-de-snmpv3-para-dispositivos-que-utilizan-ios/ta-p/3154635>
- [16] Various, “Getting Started with GNS3 | GNS3 Documentation.” Accessed: Mar. 31, 2024. [Online]. Available: <https://docs.gns3.com/docs/>

- [17] J. C. Neumann, *The book of GNS3 : build virtual network labs using Cisco, Juniper, and more*, 1st edition. San Francisco, California: No Starch Press, 2015.
- [18] M. Harahus, M. Čavojský, G. Bugár, and M. Pleva, "Interactive Network Learning: An Assessment of EVE-NG Platform in Educational Settings," *Acta electrotechnica et informatica*, vol. 23, no. 3, pp. 3–9, 2023, doi: 10.2478/aei-2023-0011.
- [19] E. Estrin, *Cloud security handbook : find out how to effectively secure cloud environments using AWS, Azure, and GCP*. Birmingham: Packt Publishing, Limited, 2022.
- [20] D. Santana, *Cloud computing demystified for aspiring professionals : hone your skills in AWS, Azure, and Google Cloud Computing and boost your career as a cloud engineer*, 1st ed. Birmingham, England: Packt Publishing, Limited, 2023.
- [21] R. Modi, *Azure for architects : implementing cloud design, DevOps, containers, IoT, and severless solutions on your public cloud*, Second edition. Birmingham: Packt, 2019.
- [22] Various, "¿Qué es la IaaS? Explicación de la infraestructura como servicio - AWS." Accessed: Mar. 30, 2024. [Online]. Available: <https://aws.amazon.com/es/what-is/iaas/>
- [23] B. Butler, "Gartner's IaaS Magic Quadrant: a who's who of cloud market: Gartner's Magic Quadrant for IaaS has familiar names and surprising omissions," *Network World (Online)*, 2012.
- [24] B. Analyst *et al.*, "Magic Quadrant for Strategic Cloud Platform Services," Dec. 2023.
- [25] N. R. Fachrurrozi, A. A. Wirabudi, and S. A. Rozano, "Design of network monitoring system based on LibreNMS using Line Notify, Telegram, and Email notification," *Sinergi (Fakultas Teknologi Industri Univeritas Mercu Buana.*, vol. 27, no. 1, pp. 111–122, 2023, doi: 10.22441/sinergi.2023.1.013.
- [26] Wolfgang. Barth, *Nagios System and Network Monitoring*, 2nd ed. San Francisco: No Starch Press, 2008.
- [27] N. Liefting, *Zabbix 5 IT infrastructure monitoring cookbook : explore the new features of Zabbix 5 for designing, building, and maintaining your Zabbix setup*. Birmingham, England: Packt Publishing, Limited, 2021.
- [28] McGuire, Schoenbrun, and Sharkey, "Topologías y diseño de Azure VPN Gateway | Microsoft Learn." Accessed: Mar. 30, 2024. [Online]. Available: <https://learn.microsoft.com/es-es/azure/vpn-gateway/design#highly-available>
- [29] S. Shrivastava, *AWS for solutions architects : the definitive guide to AWS solutions architecture for migrating to, building, scaling, and succeeding in the cloud*, Second edition. in Expert insight. Birmingham, England: Packt Publishing Ltd., 2023.
- [30] V. Bollapragada, *IPSec VPN Design*. Cisco Press, 2005.
- [31] "Installing LibreNMS - LibreNMS Docs." Accessed: May 29, 2024. [Online]. Available: <https://docs.librenms.org/Installation/Install-LibreNMS/#prepare-linux-server>

9. Anexos

Anexo 1: Estudio sobre entornos de virtualización

En la actualidad, la mayoría de las empresas dispone de su propio sistema de almacenamiento y virtualización para hacer frente a las necesidades de sistemas que demanda la organización.

Estas soluciones de infraestructura en la nube son fundamentalmente soluciones propietarias a través de diferentes fabricantes de referencia pero que tienen asociados costes adicionales como puede ser el de licenciamiento o pago por uso (p.e. VMware vSphere, VMware NSX etc.).

Las alternativas disponibles en cuestión de relación precio analizadas para una correcta implementación de la solución debido a que conformará la PoC (*proof of concept*) han sido las siguientes:

GNS3:

GNS3, es un software gratuito y de código abierto creado por Jeremy Grossman bastante utilizado dentro de la comunidad usado por la gran mayoría de ingenieros de redes a nivel mundial para emular, probar y validar escenarios virtuales y reales [16]. Decir que no es un simple software de simulación, sino que tiene funcionalidades de emulación esto le permite desplegar *appliance* virtuales e integrarlas en escenarios reales como puede ser el caso del presente proyecto de monitorización en redes híbridas.

La robustez del proyecto radica en que han contribuido al mismo personas de relevancia como Christophe Fillot, creador del programa de emulación de procesador MIPS (Dynamips) que permite ejecutar el sistema operativo de diferentes modelos de Cisco Systems.

Otro de los potenciales de GNS3 es la capacidad de integrar con otro software de emulación y virtualización (QEMU, Virtualbox, VMware, Docker etc.) que permite crear estructuras híbridas de comunicaciones [17]:

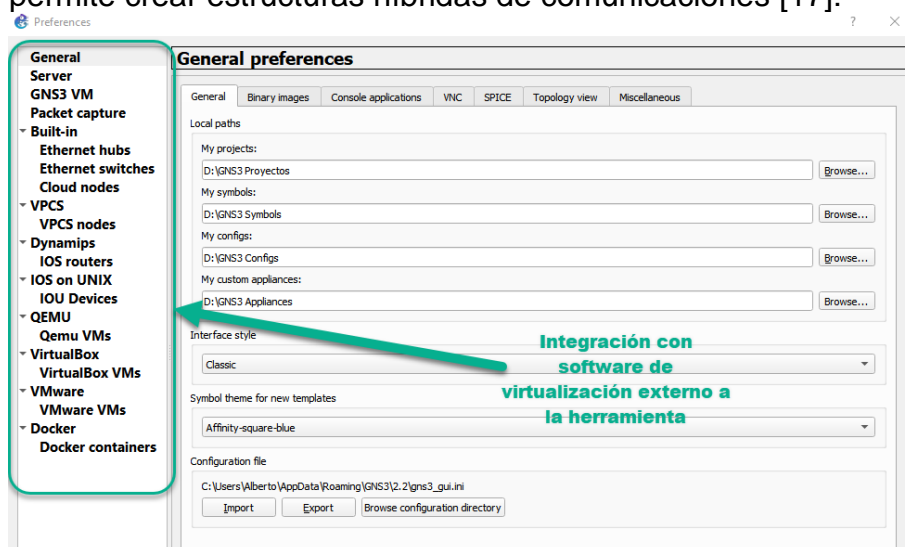


Ilustración 28 Posibilidad de integrar GNS3 con software de emulación adicional

La popularidad del software GNS3 radica en que existen otras opciones muy robustas pero que se quedan cortas por ser simplemente simuladores de

comandos como es el caso de software de RouterSim o Boson NetSim o bien requieren pago por uso como puede ser el caso de Virtual Internet Routing Lab (VIRL).

Teniendo en cuenta que realiza funciones de hardware emulado al usar una aplicación de hipervisor *backend* para emular el *appliance hardware* seleccionado, permitiendo de este modo cargar imágenes de los firmwares de dispositivos deseados, como podría ser una imagen IOS de Cisco Systems.

EVE-NG:

EVE-NG es otra de las opciones muy usadas por la comunidad de ingenieros y estudiantes de redes de comunicaciones y sistemas, siendo una de las opciones de software de emulación de red muy demandadas.

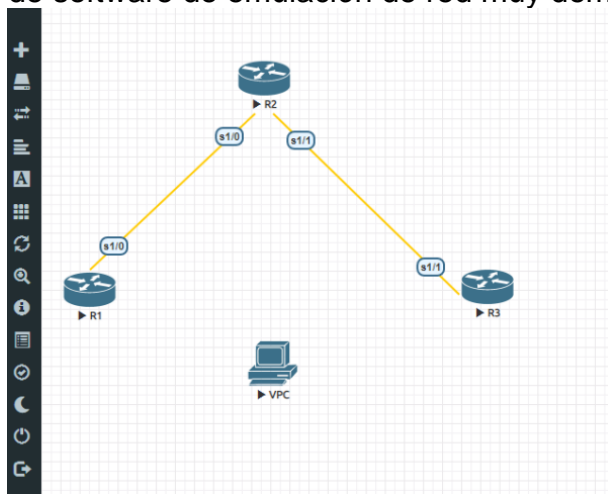


Ilustración 29 interfaz gráfico de EVE-NG. Fuente: Acta Electrotechnica et Informatica, Vol. 23, No. 3, 2023

De hecho, EVE-NG poco a poco ha ido ocupando su espacio dentro de la comunidad debido a su interfaz gráfica bastante más ligero que el de GNS3.

El hecho de trabajar plantillas web, permite al usuario una mejor experiencia de uso.

No obstante, se aprecia que aún le queda un recorrido mayor de madurez al detectarse durante análisis diferentes problemas asociados a compatibilidad e integración con software de terceros.

Durante la prueba de integración se experimentaron diversos problemas en el consumo de recursos, por lo que fue necesario desestimar esta opción.

Otro factor negativo, es que la comunidad de usuarios no es tan extensa como en GNS3 al ser el software más extendido y popular hoy en día, hecho que permite una mejor colaboración dentro de la comunidad de desarrollo.

Sumado a que la versión completa es de pago y requiere licenciamiento, hace que la comunidad de estudiantes e ingenieros de redes aún desconfíen de su uso.

Conclusiones a raíz de los entornos analizados:

Aunque es cierto que EVE-NG se está posicionando como un referente en software de emulación de sistemas y red y la experiencia de usuario es elevada,

es cierto que diferentes estudios han mostrado a EVE-NG con ciertas carencias en aspectos de compatibilidad y fiabilidad [18] .

Por todo lo comentado en los puntos anteriores, se opta por trabajar con GNS3 como software de referencia a la hora de implementar el entorno de virtualización y emulación del proyecto.

Las razones en conclusión por decantarse por GNS3 han sido:

- Una mayor comunidad de usuarios con gran cantidad de foros y documentación asociada.
- Software abierto y totalmente gratuito, sin tener que pagar suscripciones por tipo de uso como sucede en EVE-NG.
- Mayor facilidad a la hora de integrar con herramientas de terceros (GNS + VMware).

Anexo 2: Estudio sobre proveedores de servicios de nube pública IaaS

Entendiendo la necesidad de desplegar comunicaciones contra servidores concretos, se identifica la necesidad de encontrar un proveedor en la nube que cumpla con los requisitos del modelo de responsabilidad compartida, más concretamente el de soluciones IaaS [19], debido a una posible necesidad de implementar servidores con una versión determinada en el centro de datos *cloud*:

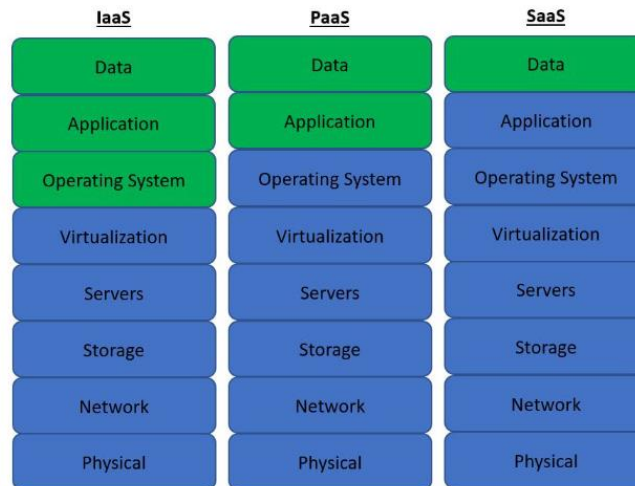


Ilustración 30 Modelo de responsabilidad compartida. Fuente: Cloud Security Gandbook. Eyal Estrin

En la actualidad los grandes proveedores *cloud* cuentan con las grandes ventajas de tener infraestructura en la nube como puede ser una mejor escalabilidad y tolerante a fallas [20]

Partiendo de este requisito inicial, se puede establecer una serie de baremos que permitirán determinar la mejor opción para desplegar la solución de la red híbrida y proceder en su paso final a interconectarla y dotarla de monitorización y gestión a través de SNMP.

La selección de la mejor opción a adoptar para el proyecto se basará fundamentalmente por la profundidad de mercado del fabricante y por la documentación asociada a casos de uso similares que pudieran ayudar al buen desarrollo del proyecto.

Microsoft Azure:

Sin duda **Microsoft Azure** se ha convertido en uno de los líderes en soluciones de IaaS dentro del amalgama de nubes públicas en la actualidad. La oferta de hecho está continuamente creciendo [21].

Azure junto a Google Cloud y AWS, son hoy en día las grandes referencias para considerar contando con una gran profundidad de mercado.

Las ventajas de Azure es que la hace apta por su versatilidad en soluciones O365 y otros productos Microsoft para empresas.

Google Cloud Platform:

Google a través de **Google Cloud Platform** también ofrece su suite de infraestructuras de referencia dentro de IaaS con el añadido de tener la innovación en aspectos concretos para Machine Learning, Big Data o Inteligencia Artificial.

Amazon Web Services:

Los servicios más comúnmente utilizados en **AWS** como proveedor de IaaS suelen ser:

- **Amazon EC2**
- **Amazon S3**
- **Amazon VPC**

Según se extrae de la propia web oficial de AWS, es la "*plataforma más completa y ampliamente adoptada del mundo*" [22] .

Además, las soluciones IaaS cuentan históricamente con una **gran flexibilidad y facilidad de uso** junto a un programa de formación y certificación bastante establecido dentro de la comunidad.

Conclusiones acerca de los proveedores cloud:

La solución que se ha determinado adoptar dentro de proveedores IaaS es la de AWS en base a los informes Gartner analizados los últimos años [23] , hacen de AWS un líder de mercado dentro de las soluciones actuales como IaaS en nubes públicas:

2023 Magic Quadrant ☰



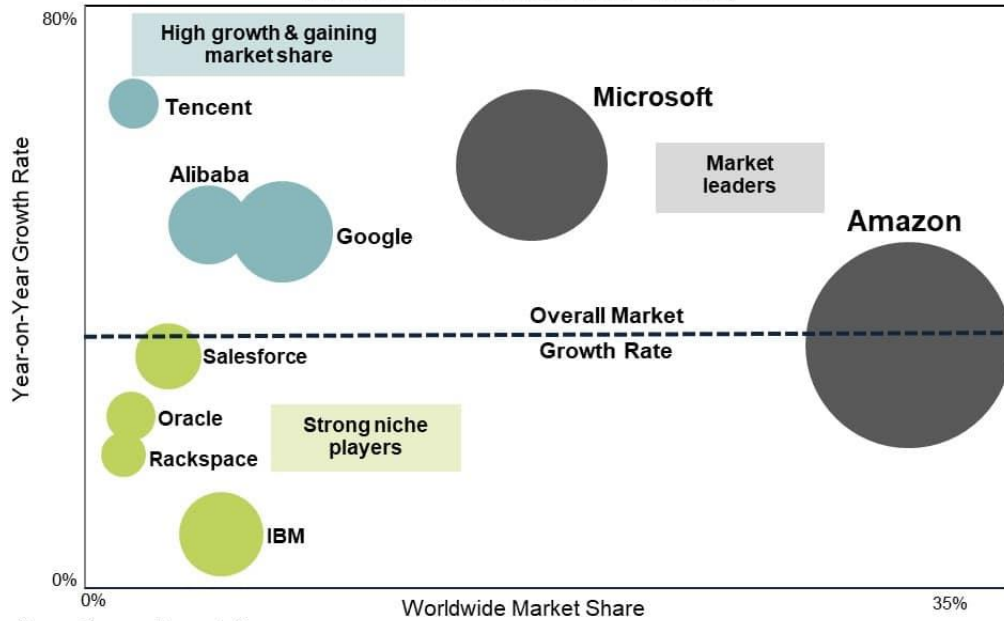
Ilustración 31 Cuadrante mágico de Gartner 2023

En la anterior imagen se puede apreciar como Amazon Web Services sigue siendo un líder de referencia para este tipo de soluciones [24]

Por otro lado, a nivel de pruebas de concepto realizadas por ingeniero sobre diferentes soluciones IaaS, se puede apreciar que la gran mayoría están realizadas sobre infraestructura AWS en primer lugar y seguido de Microsoft Azure.

Cloud Provider Competitive Positioning

(IaaS, PaaS, Hosted Private Cloud - Q4 2019)



Source: Synergy Research Group

Ilustración 32 Posicionamiento competitivo del proveedor de la nube (Fuente: Synergy Research Group)

Anexo 3: Estudio de herramientas de monitorización de redes en la actualidad

Se realiza un análisis descriptivo de las herramientas de monitorización SNMP más utilizadas en la actualidad, con un enfoque en aquellas de código abierto y software libre. Se describen las alternativas consideradas para la selección de la herramienta:

LibreNMS

Es una plataforma de monitorización de red y sistema de gestión de red (NMS) de código abierto y gratuita. Ofrece una amplia gama de funciones, incluyendo la detección automática de dispositivos, gráficos de rendimiento, alertas, informes y más.

Uno de los atractivos de LibreNMS es que puede integrarse con otros proyectos libres para tener una solución centralizada de monitorización, envío de alertas etc. [25]

Nagios

Aunque Nagios no es exclusivamente una herramienta SNMP, tiene la capacidad de integrar módulos para la monitorización SNMP. Es una plataforma de monitorización de red de código abierto ampliamente utilizada que proporciona alertas en tiempo real, visualización de estado y generación de informes.[26]

Tras el análisis de la herramienta se determina que tiene limitaciones tanto a nivel de monitorización. Además, la configuración y mantenimiento es complejas, siendo necesario intervenir de forma manual en la mayoría de los ajustes.

Zabbix

Zabbix es otra de las opciones disponibles siendo una plataforma de monitorización de red de código abierto que proporciona alertas, visualización de tendencias y creación de mapas [27].

Conclusiones acerca de la herramienta de monitorización a incorporar

En base a la literatura consultada y algunas pruebas realizadas de concepto. La elección tomada a cerca de la herramienta a incorporar es LibreNMS por varios motivos:

- Posicionamiento fuerte en entornos de redes y comunicaciones.
- Personalización e integración con otras herramientas y soluciones GNU/GPL.
- Gran versatilidad y facilidad de despliegue de la solución, lo que permitirá optimizar tiempo de proyecto para desplegar las comunicaciones híbridas.

Anexo 4: Estudio de tipos de VPN a considerar para la solución

Partiendo de que el presente proyecto supone un paradigma de computación que va a requerir conectividad entre un CPD tradicional e infraestructura CPD que lo estará en la nube, o lo que es lo mismo, se debe crear conectividad en una infraestructura híbrida, es necesario plantearse el despliegue de lo que se conoce como una VPN o lo que es lo mismo una Virtual Private Network.

La explicación es que los escenarios de nube híbrida entran en escena cuando se necesita mantener carga de trabajo de TI tanto en instalaciones locales como en la nube. En estas casuísticas se requerirá una conectividad altamente confiable entre ambos extremos.

Esta conexión VPN nos permitirá la conexión entre una nube privada (que será nuestro datacenter tradicional con el sistema de virtualización on-premises) y una nube pública, como se ha tratado en los puntos anteriores.

En la actualidad se encuentran estandarizadas diferentes soluciones que permitirán desplegar comunicaciones VPN en redes híbridas mediante el uso de VPN Gateways [28]

Como se detallará en los siguientes puntos, por norma general los proveedores cloud ofrecen dos variantes de soluciones VPN:

- VPN de sitio a sitio: Que establecerá un túnel seguro entre la infraestructura on-premises y el VPG (Virtual Private Gateway)
- VPN de cliente: Que será el dispositivo final quien levante la VPN contra la infraestructura remota en el cloud público.

VPN de sitio a sitio (VPN S2S)

Esta solución es la más extendida cuando se implementan soluciones y arquitecturas híbridas, dotando comunicaciones seguras entre el cloud privado y el cloud público, por ejemplo. Es decir, dos infraestructuras con la suficiente relevancia para comunicarse entre ellas a través de protocolos seguros [29]

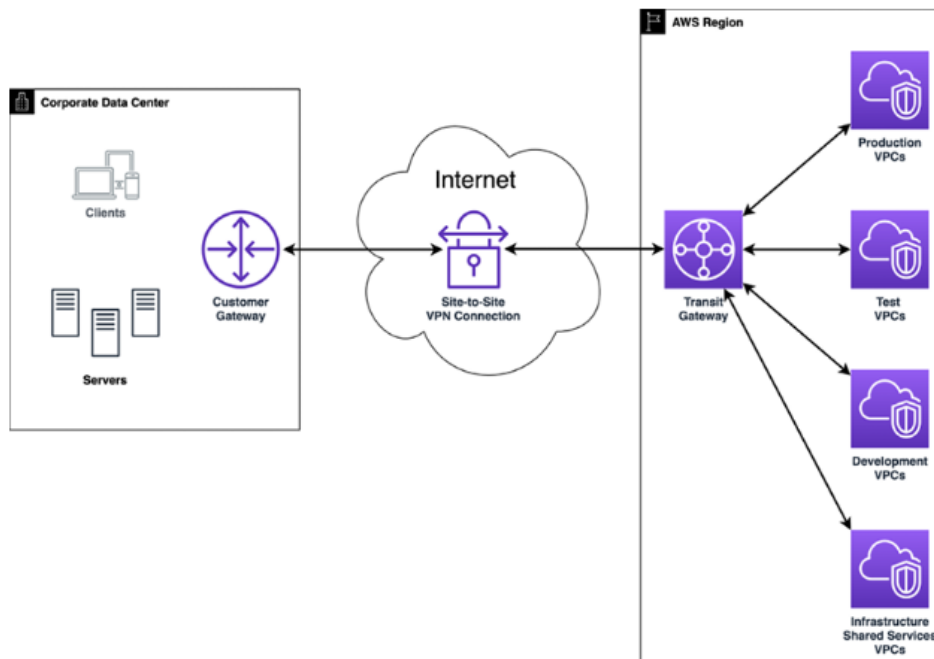


Ilustración 33 Ejemplo conceptualizado de VPN Site-to-Site en AWS. Fuente: AWS para arquitectos de soluciones. Shrivastava.

VPN de Punto a sitio (VPN P2S) o VPN de Cliente

Por otro lado, las implementaciones de VPN del tipo cliente (la nomenclatura exacta difiere dependiendo del proveedor cloud) están más orientadas a ofrecer conectividad remota, pero a dispositivos finales, dejando de ser interesantes para conectividades de cierta relevancia que alojen varios servicios o diferentes subredes IP.

Este tipo de conectividades están más recomendadas para usuarios remotos (end-user) que quieren acceder a la infraestructura corporativa desplegada en la nube (por ejemplo, haciendo uso de software cliente VPN).

Conclusiones acerca del diseño VPN a incorporar

Atendiendo al análisis de los tipos de VPN ofertados por las soluciones IaaS de clouds públicos, se obtiene que la mejor implementación que se adapta a las necesidades del proyecto de monitorización de redes híbridas es la de VPN Site-to-Site por lo que se incorpora al lote de trabajo.

Anexo 5: Estudio relativo a la implementación IPsec

Se detallan los aspectos técnicos relacionados con la implementación de la VPN IPSEC site-to-site, incluyendo la configuración de parámetros de seguridad y tipos de protocolos utilizados. Se describen las alternativas consideradas para la implementación de la VPN y se explican los criterios utilizados para tomar la decisión final.

Descripción de IPsec

IPsec (Internet Protocol Security) es un conjunto de protocolos ampliamente utilizado en el ámbito de la seguridad de la información para asegurar las comunicaciones en redes IP. Este conjunto de protocolos ofrece una serie de servicios de seguridad, incluyendo autenticación, integridad, confidencialidad y protección contra la retransmisión de datos.

Operando en la capa de red (Capa 3) del modelo OSI, IPsec es esencial para proteger el tráfico de datos tanto en redes públicas como en redes privadas virtuales (VPNs). Sus componentes principales son el Encabezado de Autenticación (AH) y la Carga de Seguridad Encapsulada (ESP). Mientras que AH se encarga de garantizar la autenticación e integridad de los datos, ESP proporciona servicios de confidencialidad y autenticación.

Cada parte comunicante puede ser un host individual o una pasarela de seguridad (SG) que actúa como límite entre una parte protegida y una no protegida de una red. Por lo tanto, IPsec se puede utilizar en aplicaciones como acceso remoto a una LAN corporativa (formando una VPN), para interconectar diferentes partes de una empresa de manera segura a través de Internet, o para asegurar las comunicaciones de hosts o routers que actúan como hosts al intercambiar información de enrutamiento [30]

IPsec ofrece flexibilidad en su implementación, permitiendo diferentes modos como el modo túnel y el modo transporte. El conocido modo túnel realiza el cifrado del paquete IP en su totalidad, mientras que el modo transporte solo cifra la carga útil del paquete IP. Es por ello por lo que **IPsec va a resultar una pieza clave en el proyecto de comunicaciones híbridas**, debido a que va a dar la respuesta a dos de los tres grandes pilares de la seguridad como lo es la confidencialidad y la integridad.

La disponibilidad como tal, sería buscada a través de una solución de arquitectura robusta que permita redundancia.

Modos de funcionamiento IPsec a considerar

Se identifican diferentes modos de funcionamiento IPsec en base a qué nivel se produce el cifrado:

IPsec modo transporte

El modo de transporte de IPsec protege los datos de usuario entre dos puntos finales en una red. En este modo, únicamente la carga útil del paquete IP se cifra y se autentica, dejando intactas las direcciones IP originales de origen y destino. Es útil cuando se necesita proteger la comunicación punto a punto dentro de una red privada o VPN, pero no la cabecera IP.

IPsec modo túnel

El modo túnel de IPSec cifra y autentica todo el paquete IP, incluida la cabecera IP original, y lo encapsula en un nuevo paquete IP con una nueva cabecera IP de túnel. Este modo es ideal para proteger las comunicaciones entre redes o subredes, como las conexiones de VPN sitio a sitio, ya que permite crear túneles seguros a través de redes no seguras, como Internet.

Conclusiones acerca del modo de funcionamiento IPSec a incorporar

Analizando ambas opciones podemos extraer las siguientes conclusiones:

Modo Túnel de IPsec	Modo Transporte de IPsec
En este modo, todo el paquete IP original, incluida la cabecera IP, se cifra y se encapsula dentro de otro paquete IP.	En este modo, solo la carga útil del paquete IP se cifra y se autentica, dejando intactas las cabeceras IP originales.
Es útil para crear conexiones seguras entre dos redes, como una VPN sitio a sitio, donde los datos deben atravesar redes públicas no seguras.	Es adecuado para proteger la comunicación punto a punto dentro de una misma red o entre dos hosts.
El paquete IP original se convierte en la carga útil del nuevo paquete IP, y este último se dirige hacia el destino a través de la red segura.	La encapsulación se realiza solo en los datos del paquete, lo que minimiza el impacto en el tamaño total del paquete y en la sobrecarga de procesamiento.
El modo túnel proporciona un alto nivel de seguridad y privacidad para toda la comunicación entre las dos redes, pero puede tener un mayor costo computacional debido a la encapsulación de los paquetes completos.	Aunque ofrece seguridad para los datos transportados, no protege la información de la cabecera IP, lo que significa que cierta información sobre la comunicación puede ser visible para terceros.

Hay que indicar que ambos modos de funcionamiento de IPSec ofrecen niveles de seguridad significativos, cada uno con sus propias ventajas y consideraciones.

- **IPSec modo transporte** es más adecuado para comunicaciones punto a punto dentro de una red. Del otro.
- **IPSec modo túnel** es preferible para proteger las comunicaciones entre redes o subredes.

Dado que el caso actual que presenta la problemática de este proyecto requiere comunicación entre dos Datacenter (uno *on-premises* y otro en cloud) creando de este modo una nube híbrida, **el modo que más se ajusta a las necesidades es el de IPSec modo túnel.**

Anexo 6: Estudio relativo a los mecanismos de routing

Se analiza el uso de protocolos de enrutamiento en redes híbridas con VPN IPSEC, con un enfoque en el protocolo eBGP. Se describen las alternativas consideradas para el enrutamiento y se explican los motivos de la elección de eBGP, incluyendo su capacidad para facilitar la propagación eficiente de rutas entre entornos locales y en la nube.

Análisis de diferentes protocolos de routing a incorporar en el proyecto

A través de los siguientes puntos se va a hacer un análisis alto nivel de las funcionalidades y objeto del uso de cada uno de los protocolos candidatos para formar parte de la solución de las comunicaciones entre el CPD *On-premises* y el CPD *cloud*, conformando de esta manera una nube híbrida:

Enrutamiento estático

El enrutamiento estático implica la configuración manual de rutas hacia destinos específicos en la red. Es una opción simple y adecuada para redes pequeñas y estáticas donde los cambios en la topología son mínimos. Sin embargo, su mantenimiento puede volverse complejo en entornos dinámicos, como una red en la nube híbrida, donde las rutas pueden cambiar con frecuencia.

BGP

BGP (*Border Gateway Protocol*) es un protocolo de enrutamiento dinámico ampliamente utilizado en entornos de Internet y grandes redes empresariales definido en su versión BGP-4 a través del RFC 4271. Ofrece escalabilidad y flexibilidad, adaptándose bien a entornos como una red en la nube híbrida, donde la conectividad entre diferentes dominios de enrutamiento es crucial. BGP permite la selección de rutas óptimas y proporciona resiliencia en la conectividad.

EIGRP

EIGRP (*Enhanced Interior Gateway Routing Protocol*) se trata de un protocolo propietario desarrollado por Cisco Systems. Si bien ofrece beneficios como rápida convergencia y eficiencia de ancho de banda, su uso está limitado a entornos que ejecutan equipos de red Cisco exclusivamente. En una red dentro de la nube híbrida que puede involucrar múltiples proveedores y dispositivos de red, esta dependencia puede ser una limitación.

Conclusiones asociadas a la incorporación de protocolos de routing en proyecto

Tras el análisis de los diferentes protocolos de enrutamiento, se concluye que la incorporación de BGP en el proyecto de una red cloud híbrida sería lo óptimo para la problemática que nos presenta el caso del proyecto de monitorización de un sistema alojado en una nube híbrida.

El protocolo BGP como se ha mencionado, va a ofrecer a la solución de la red híbrida escalabilidad, flexibilidad y resiliencia, lo que lo hace adecuado para gestionar las complejidades de la conectividad entre el data center *on-premises* y el *cloud* público.

Aunque el enrutamiento estático puede ser útil en ciertos casos, y EIGRP puede ofrecer beneficios específicos para entornos Cisco, **BGP destaca como la mejor opción general para este escenario particular y será la solución para incorporar en el proyecto.**

Anexo 7: Implementación de GNS3

Se procede a instalar el entorno GNS3 siguiendo las recomendaciones de la página oficial del software [10]. El software está relacionado también con el despliegue de una máquina virtual que correrá sobre VMware Workstation.

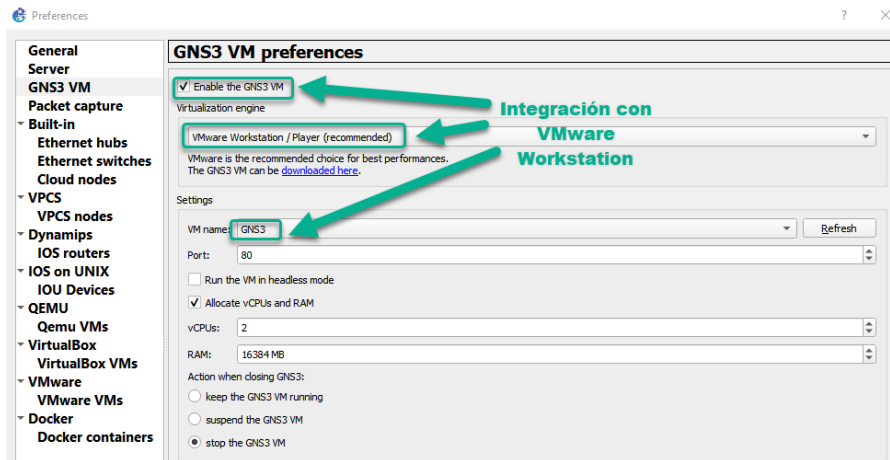


Ilustración 34 Integración de GNS3 con VMWare Workstation

Anexo 8: Implementación del servidor NMS

Para la implementación del servidor de monitorización (NMS), se ha seguido las recomendaciones hechas por parte de la página oficial del producto LibreNMS teniendo en cuenta la tipología de la plataforma y el entorno [31]

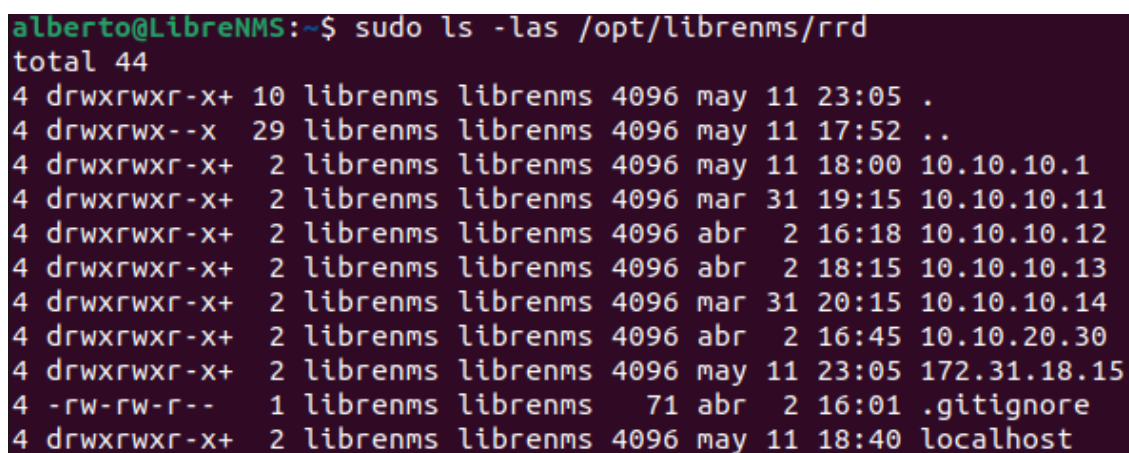
A través de la guía oficial del producto se ha podido implementar LibreNMS para Ubuntu 22.04 que es la distribución implementada.

El producto se ha obtenido tal como indica la formación, del proyecto git correspondiente:

```
cd /opt
git clone https://github.com/librenms/librenms.git
```

Además de lo anterior se ha generado el usuario “librenms” junto a los permisos de diferentes rutas como:

```
/opt/librenms/rrd
/opt/librenms/logs
/opt/librenms/bootstrap/cache/
/opt/librenms/storage/
```



```
alberto@LibreNMS:~$ sudo ls -las /opt/librenms/rrd
total 44
4 drwxrwxr-x+ 10 librenms librenms 4096 may 11 23:05 .
4 drwxrwx--x 29 librenms librenms 4096 may 11 17:52 ..
4 drwxrwxr-x+ 2 librenms librenms 4096 may 11 18:00 10.10.10.1
4 drwxrwxr-x+ 2 librenms librenms 4096 mar 31 19:15 10.10.10.11
4 drwxrwxr-x+ 2 librenms librenms 4096 abr 2 16:18 10.10.10.12
4 drwxrwxr-x+ 2 librenms librenms 4096 abr 2 18:15 10.10.10.13
4 drwxrwxr-x+ 2 librenms librenms 4096 mar 31 20:15 10.10.10.14
4 drwxrwxr-x+ 2 librenms librenms 4096 abr 2 16:45 10.10.20.30
4 drwxrwxr-x+ 2 librenms librenms 4096 may 11 23:05 172.31.18.15
4 -rw-rw-r-- 1 librenms librenms 71 abr 2 16:01 .gitignore
4 drwxrwxr-x+ 2 librenms librenms 4096 may 11 18:40 localhost
```

Ilustración 35 verificación de permisos

En la fase posterior, se ha ajustado la configuración de la zona horaria a la que corresponde.

Otro aspecto para considerar es la configuración del servidor web:

```

alberto@LibreNMS:~$ more /etc/nginx/conf.d/librenms.conf
server {
    listen      80;
    server_name librenms;
    root        /opt/librenms/html;
    index       index.php;

    charset utf-8;
    gzip on;
    gzip_types text/css application/javascript text/javascript application/x-javascript image/svg+xml text/plain text/xsd text/xsl text/xml image/x-icon;
    location / {
        try_files $uri $uri/ /index.php?$query_string;
    }
    location ~ [^/]\.php(/|$) {
        fastcgi_pass unix:/run/php-fpm-librenms.sock;
        fastcgi_split_path_info ^(.+\.php)(/.+)$;
        include fastcgi.conf;
    }
    location ~ /\.(!well-known).* {
        deny all;
    }
}

```

Ilustración 36 Configuración del servidor web NGINX

Y finalmente la parte de SNMP quedaría configurada de este modo:

```

alberto@LibreNMS:~$ sudo more /etc/snmp/snmpd.conf
# Change RANDOMSTRINGGOESHERE to your preferred SNMP community string
com2sec readonly default UOC

group MyROGroup v2c          readonly
view all included .1          80
access MyROGroup ""         any          noauth   exact all none none

syslocation State Galicia Building , City Vigo, Country ES [42.22949518070047, -8.71950413702797]
syscontact Alberto Fernandez <afernandezsanchez0@uoc.edu>

#OS Distribution Detection
extend distro /usr/bin/distro

#Hardware Detection
# (uncomment for x86 platforms)
#extend manufacturer '/bin/cat /sys/devices/virtual/dmi/id/sys_vendor'
#extend hardware '/bin/cat /sys/devices/virtual/dmi/id/product_name'
#extend serial '/bin/cat /sys/devices/virtual/dmi/id/product_serial'

# (uncomment for ARM platforms)
#extend hardware '/bin/cat /sys/firmware/devicetree/base/model'
#extend serial '/bin/cat /sys/firmware/devicetree/base/serial-number'
alberto@LibreNMS:~$

```

Ilustración 37 Configuración SNMP en el NMS LibreNMS

Anexo 9: Configuración de los equipos de comunicaciones en CPD local

Aunque la configuración varía de un elemento a otro dependiendo la funcionalidad y rol dentro del diseño de la red, se pueden extraer algunos detalles de configuración más característicos:

Crypto Keyring para ambos túneles:

```
crypto keyring keyring-vpn-0dde3fedcb97043bb-1
  local-address GigabitEthernet0/1
  pre-shared-key address 100.27.53.11 key U7PSBB_nbSrP5.iDdBzKF23svQ5R1BfT
crypto keyring keyring-vpn-0dde3fedcb97043bb-0
  local-address GigabitEthernet0/1
  pre-shared-key address 34.192.94.128 key tBZGA4WlN.Sx0Ec37PQWwb7bMFhTxkhq
```

Transform-set para ambos túneles:

```
crypto ipsec transform-set ipsec-prop-vpn-0dde3fedcb97043bb-0 esp-aes esp-sha-
hmac
  mode tunnel
crypto ipsec transform-set ipsec-prop-vpn-0dde3fedcb97043bb-1 esp-aes esp-sha-
hmac
  mode tunnel
```

Crypto IPSec Profile:

```
crypto ipsec profile ipsec-vpn-0dde3fedcb97043bb-0
  set transform-set ipsec-prop-vpn-0dde3fedcb97043bb-0
  set pfs group2
!
crypto ipsec profile ipsec-vpn-0dde3fedcb97043bb-1
  set transform-set ipsec-prop-vpn-0dde3fedcb97043bb-1
  set pfs group2
```

Interface Tunnel:

```
interface Tunnel1
  ip address 169.254.197.166 255.255.255.252
  ip virtual-reassembly in
```

```
ip tcp adjust-mss 1379
tunnel source GigabitEthernet0/1
tunnel mode ipsec ipv4
tunnel destination 34.192.94.128
tunnel protection ipsec profile ipsec-vpn-0dde3fedcb97043bb-0
!
interface Tunnel2
ip address 169.254.204.102 255.255.255.252
ip virtual-reassembly in
ip tcp adjust-mss 1379
tunnel source GigabitEthernet0/1
tunnel mode ipsec ipv4
tunnel destination 100.27.53.11
tunnel protection ipsec profile ipsec-vpn-0dde3fedcb97043bb-1
```

Configuración BGP:

```
router bgp 65000
bgp log-neighbor-changes
neighbor 169.254.197.165 remote-as 64512
neighbor 169.254.197.165 timers 10 30 30
neighbor 169.254.204.101 remote-as 64512
neighbor 169.254.204.101 timers 10 30 30
!
address-family ipv4
network 0.0.0.0
redistribute connected
neighbor 169.254.197.165 activate
neighbor 169.254.197.165 default-originate
neighbor 169.254.197.165 soft-reconfiguration inbound
neighbor 169.254.204.101 activate
neighbor 169.254.204.101 default-originate
neighbor 169.254.204.101 soft-reconfiguration inbound
exit-address-family
```