Soluciones Open Source para VPNs a través de CGNAT: Alternativas P2P

Valentín Torassa Colombero[1], Santiago Roatta[2], María Eugenia Casco[1]

[1] Facultad de Tecnología Informática, Universidad Abierta Interamericana (UAI),Rosario, Argentina
[2] Facultad de Cs. Exactas, Ingeniería y Agrimensura, Universidad Nacional de Rosario, Rosario, Argentina

valentintorassa@alumnos.uai.edu.ar
MariaEugenia.Casco@uai.edu.ar
sroatta@fceia.unr.edu.ar

Resumen. El uso creciente de Carrier-Grade NAT (CGNAT) por parte de los proveedores de Internet ha limitado la capacidad de los usuarios para acceder de forma remota y segura a sus dispositivos y redes privadas. Las VPNs convencionales como OpenVPN y WireGuard han sido utilizadas para este propósito, pero requieren configuraciones técnicas y, en muchos casos, una IP pública estática. Este estudio explora soluciones open source que permiten la conectividad segura sin la necesidad de una IP pública, centrándose en ZeroTier y Tailscale, dos tecnologías basadas en redes P2P que facilitan la conexión a través de CGNAT utilizando NAT tranversal. Se implementa y evalúa ZeroTier combinado con NGINX como proxy reverso para exponer servicios internos, así como Tailscale en su configuración P2P sin servidor central. Se comparan ambas soluciones, ofreciendo una visión clara sobre su viabilidad como alternativas accesibles a las VPNs tradicionales. Finalmente, se propone el desarrollo de una solución *self-hosted* basada en Nebula, ofreciendo una opción flexible y completamente descentralizada. El estudio busca proporcionar al usuario final soluciones sencillas y efectivas para conectarse de forma segura a su red privada sin depender de direcciones IP públicas ni configuraciones técnicas.

Palabras Clave: VPN, CGNAT, Redes P2P, Open Source.

Open Source Solutions for VPNs over CGNAT: P2P Alternatives

Abstract. The increasing use of Carrier-Grade NAT (CGNAT) by Internet providers has limited the ability of users to remotely and securely access their devices and private networks. Conventional VPNs such as OpenVPN and WireGuard have been used for this purpose, but require technical configurations and, in many cases, a static public IP. This study explores open source solutions that enable secure connectivity without the need for a public IP, focusing on ZeroTier and Tailscale, two technologies based on P2P networks that facilitate connection through CGNAT using NAT traversal. ZeroTier combined with NGINX as a reverse proxy to expose internal services is implemented and evaluated, as well as Tailscale in its P2P configuration without a central server. Both solutions are compared, providing a clear view on their viability as affordable alternatives to traditional VPNs. Finally, the development of a self-hosted solution based on Nebula is proposed, offering a flexible and fully decentralized option. The study aims to provide the end user with simple and effective solutions to securely connect to their private network without relying on public IP addresses or technical configurations.

KeyWords: VPN, CGNAT, Redes P2P, Open Source.

1 Introducción

Las redes privadas virtuales (VPNs) han sido durante mucho tiempo la solución estándar para el acceso remoto seguro a redes privadas [1]. Sin embargo, la evolución de la infraestructura de Internet ha introducido nuevos desafíos, especialmente con la adopción masiva de Carrier-Grade NAT (CGNAT), una técnica que permite a los proveedores de servicios de Internet (ISP) asignar una única dirección IP pública a múltiples usuarios; Como consecuencia, la disponibilidad de direcciones IP públicas individuales se ha reducido significativamente, lo que ha llevado a un aumento en su costo y a restricciones en su asignación para usuarios residenciales y pequeñas empresas [2].

Esto dificulta el acceso remoto a dispositivos y servidores privados, ya que elimina la posibilidad de conexiones entrantes directas a través de Port Forwading [2]. En este contexto, han surgido soluciones alternativas basadas en redes P2P y herramientas de proxy reverso que buscan sortear estas limitaciones sin necesidad de configurar túneles VPN tradicionales [3].

1.1 Conectividad y seguridad en redes con CGNAT

El uso de CGNAT por parte de los ISP introduce restricciones que impactan significativamente en la conectividad de usuarios y empresas. Al eliminar la asignación de IPs públicas únicas, los dispositivos detrás de CGNAT no pueden recibir conexiones entrantes directas, dificultando la implementación de servicios como acceso remoto, servidores web, juegos en línea y videoconferencias P2P [2]. Este problema es especialmente crítico para empresas y usuarios que requieren una conexión segura y estable a sus redes privadas sin depender de soluciones propietarias costosas o configuraciones complejas [1].

Ante estas limitaciones, surge la necesidad de encontrar alternativas eficientes que permitan el acceso remoto sin comprometer la seguridad [4]. Las VPNs tradicionales, aunque efectivas, presentan desafíos en términos de configuración, rendimiento y compatibilidad sobre todo si debe realizar un bypass de CGNAT, lo que motiva la exploración de nuevas tecnologías basadas en arquitecturas distribuidas [1][2].

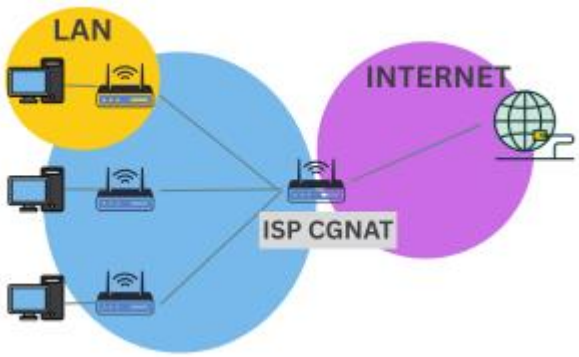

Fig. 1. Esquema del funcionamiento de CGNAT

1.2 Objetivo del estudio

El objetivo principal de esta investigación es desarrollar una solución sencilla y accesible que permita a cualquier usuario configurar y utilizar una VPN sin necesidad de conocimientos avanzados en redes ni de contratar una IP pública y fija [1]. Este estudio busca eliminar esa barrera, proporcionando alternativas open source que permitan a los usuarios finales disfrutar de una conectividad segura sin depender de direcciones IP públicas [2].

Para lograr esto, se analizarán y compararán dos enfoques principales en el ámbito de la conectividad segura:

1. **VPNs tradicionales** (OpenVPN, WireGuard) y sus dificultades para atravesar CGNAT [1][2].

2. **Redes P2P modernas** (ZeroTier y Tailscale), que evitan la necesidad de IP pública, simplifican la configuración y mejoran la experiencia del usuario al automatizar la conectividad [4][5].

Se explorará, por otro lado, el uso de NGINX como proxy reverso en combinación con ZeroTier para evaluar si esta solución puede mejorar la accesibilidad y posibilidad de ofrecer servicios internos [3].

En última instancia, este estudio pretende ofrecer una opción práctica y eficiente para que cualquier usuario, sin importar su nivel de experiencia técnica, pueda implementar una solución VPN funcional y segura, superando las limitaciones impuestas por CGNAT [1][2].

1.3 Alcance y metodología

Este estudio abordará la implementación y evaluación de soluciones open source para conectividad segura sin IP pública, enfocándose en alternativas que faciliten su uso al usuario final [1]. Se analizarán ZeroTier y Tailscale, dos tecnologías que eliminan la necesidad de una IP pública mediante redes P2P [4][5], y se evaluará la integración de NGINX como proxy reverso para exponer servicios internos [3].

2 Estado del Arte: VPNs y Soluciones P2P

El acceso seguro a redes privadas a través de Internet ha sido históricamente dominado por VPNs tradicionales, que permiten la creación de túneles cifrados entre clientes y servidores [1]. Sin embargo, con la adopción masiva de Carrier-Grade NAT (CGNAT) por parte de los proveedores de Internet, estas soluciones han encontrado diversas dificultades [2]; Este contexto ha impulsado la aparición de redes P2P, que buscan simplificar las conexiones remota sin configuraciones técnicas [4].

2.1 Conectividad y seguridad en redes con CGNAT

Las VPNs tradicionales han sido la base de la conectividad segura en redes privadas durante años, utilizando protocolos como IPsec, OpenVPN y WireGuard. IPsec es ampliamente utilizado en entornos empresariales, ofreciendo cifrado robusto a nivel de red, pero su configuración demanda recursos técnicos y suele requerir soporte explícito en firewalls y routers [1]. OpenVPN, por su parte, es una solución basada en SSL/TLS que proporciona flexibilidad y seguridad, aunque su rendimiento se ve afectado en redes con CGNAT, ya que depende de configuraciones específicas y ciertamente experimentales para atravesar NAT, incluso necesitando de combinarse con otras herramientas. WireGuard es una alternativa más moderna y eficiente, con mejor rendimiento y menor sobrecarga, pero también enfrenta dificultades cuando no se dispone de una IP pública accesible [2].

El principal problema de estas soluciones es que dependen de servidores intermediarios o requieren configuraciones de port forwading o asignación dinamica para permitir conexiones. En la mayoría de los casos en que necesitan a travesar un CGNAT, es necesario habilitar port forwarding, utilizar servidores VPS o configurar relays, lo que añade costos y complejidad para el usuario final [2]. Estas limitaciones han llevado a la búsqueda de alternativas más flexibles, como las redes P2P, que eliminan la necesidad de infraestructura adicional y simplifican la conectividad.

2.2 Redes P2P aplicadas a la Conectividad Segura

Las redes P2P han surgido como una solución innovadora para la conectividad segura, permitiendo a los dispositivos conectarse directamente sin la intervención de un servidor central [4]. A diferencia de las VPNs tradicionales, que requieren un punto intermedio para establecer la comunicación, las redes P2P utilizan técnicas de NAT traversal para permitir conexiones directas entre dispositivos, incluso cuando se encuentran detrás de CGNAT [5].

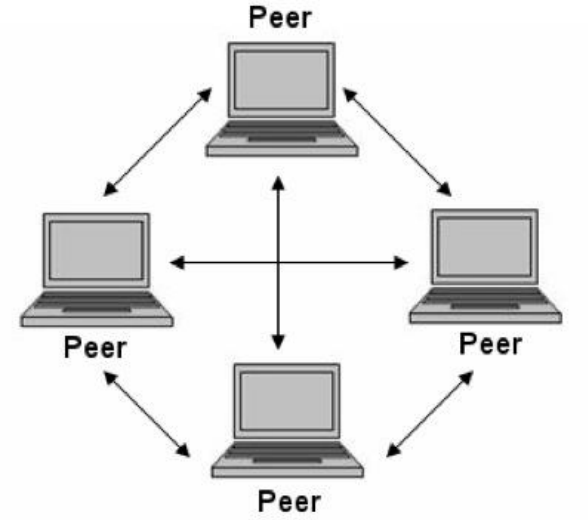

Fig. 2. Esquema del funcionamiento de una red P2P. Tomada Gabriel Duarte, 2015. Articulo Tecnológico. *https://significado.com/p2p-peer-to-peer/*

Una VPN P2P es un tipo de red virtual en la que los dispositivos participantes pueden comunicarse entre sí sin necesidad de un servidor dedicado [4].

ZeroTier y Tailscale han desarrollado soluciones que automatizan la detección y establecimiento de rutas de comunicación mediante técnicas avanzadas de NAT traversal, permitiendo la creación de túneles cifrados sin intervención manual del usuario [5][6].

ZeroTier implementa un modelo híbrido que combina principios de redes definidas por software (SDN) con técnicas de peer-to-peer (P2P), eliminando la dependencia de servidores VPN centralizados [5]. Utiliza un directorio de control distribuido, donde los nodos pueden registrarse y obtener información sobre sus pares sin que el tráfico pase a través de un servidor central. Para la conectividad, emplea técnicas de traversal NAT como UDP Hole Punching, estableciendo conexiones directas entre dispositivos cuando es posible, o recurriendo a nodos intermedios si la comunicación directa no es viable [5]. Esta arquitectura permite crear redes privadas virtuales (VPNs) dinámicas, en las que los dispositivos pueden comunicarse sin necesidad de asignaciones de direcciones IP públicas o modificaciones en los firewalls locales [4].

Por otro lado, Tailscale está construido sobre WireGuard, un protocolo VPN altamente eficiente y seguro basado en criptografía moderna. A diferencia de ZeroTier, Tailscale no implementa una red SDN descentralizada, sino que utiliza un sistema de gestión centralizado en la nube, donde los dispositivos se autentican y establecen conexiones según las reglas definidas por el usuario. Su infraestructura en la nube actúa como un coordinador de rutas, permitiendo que los clientes se descubran y configuren automáticamente mediante STUN, TURN y relays cuando es necesario. Este enfoque simplifica la configuración para el usuario, ya que no es necesario abrir puertos, configurar reglas de firewall ni definir manualmente los peers, dado que Tailscale gestiona dinámicamente las rutas de comunicación y la autenticación de dispositivos dentro de la red [6].

El principal beneficio de estas soluciones es que eliminan la necesidad de una IP pública fija, ya que pueden atravesar CGNAT utilizando técnicas de NAT traversal. Otro aspecto clave es la simplicidad de implementación, ya que los usuarios pueden configurar y utilizar estas soluciones sin necesidad de conocimientos avanzados en redes [4][5]. ZeroTier y Tailscale automatizan el proceso de conexión y autenticación, eliminando la necesidad de configuraciones manuales o ajustes en el router.

3 Tecnologías Evaluadas

3.1 ZeroTier

ZeroTier es una solución de red definida por software (SDN) que combina VPNs tradicionales y redes P2P, permitiendo la creación de redes privadas virtuales con conectividad directa entre dispositivos. Su arquitectura se basa en un modelo híbrido en el que un conjunto de nodos raíz facilita el descubrimiento de pares y la gestión de identidades, pero sin actuar como intermediarios permanentes en la comunicación [5]. Una vez establecida la conexión, los dispositivos pueden comunicarse directamente utilizando técnicas de NAT traversal, como UDP hole punching [4].

Desde el punto de vista práctico, la implementación de ZeroTier en una red privada es sencilla y accesible para cualquier usuario. Solo es necesario instalar el cliente en los dispositivos que se desean conectar, unirse a una red previamente creada y gestionar las reglas de acceso desde la plataforma de administración. Una de sus principales ventajas es el soporte en diferentes sistemas operativos desde Windows, Linux, macOS y dispositivos móviles, sin requerir configuraciones adicionales en el firewall o router del usuario [5]. En este estudio, se ha explorado su integración con NGINX para exponer servicios internos dentro de la red virtual [3].

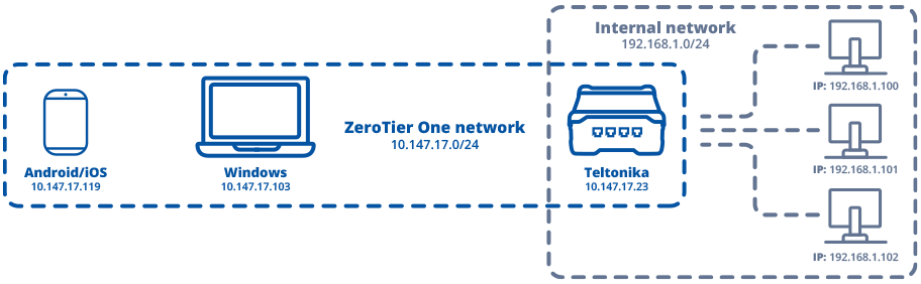

Fig. 3. Diagrama Arquitectura y Topología ZeroTier. Tomada de Teltonika Networks. *https://wiki.teltonika-networks.com/view/ZeroTier_Configuration*

3.2 Tailscale

Tailscale es otra solución basada en redes P2P, pero con un enfoque diferente. A diferencia de ZeroTier, Tailscale está construido sobre WireGuard, lo que le permite aprovechar la seguridad y eficiencia de este protocolo, al tiempo que incorpora un sistema de gestión basado en la nube. Su arquitectura se apoya en un servicio centralizado que facilita la autenticación y el establecimiento de túneles cifrados entre dispositivos, eliminando la necesidad de configurar manualmente claves o reglas de firewall [6].

Uno de los principales beneficios de Tailscale es su simplicidad de configuración. Los usuarios pueden registrar sus dispositivos utilizando autenticación basada en cuentas de Google, Microsoft o GitHub, y la plataforma automáticamente establece la conectividad entre ellos [6]. Al igual que ZeroTier, Tailscale permite el NAT traversal mediante técnicas como STUN y relay cuando es necesario [4].

Desde el punto de vista de la implementación práctica, Tailscale es una alternativa viable para usuarios que buscan una solución rápida para acceder de forma remota a sus dispositivos [6]. Su compatibilidad con Subnet Routing y Exit Nodes permite extender la red a múltiples dispositivos sin necesidad de una infraestructura centralizada [6]. Sin embargo, su arquitectura basada en la nube puede generar ciertas dependencias externas que no están presentes en soluciones como ZeroTier y otras totalmente self-hosted como Headscale o Nebula [7].

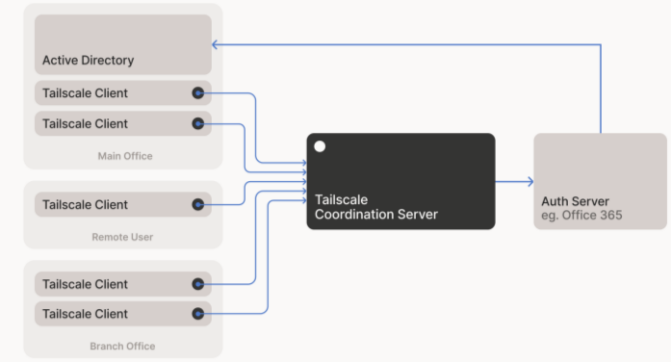

Fig. 4. Diagrama Arquitectura Tailscale. Tomada de Tailscale.
https://tailscale.com/blog/how-tailscale-works

3.3 NGINX como Reverse Proxy

NGINX es una herramienta ampliamente utilizada para la gestión del tráfico HTTP, pero en este estudio se ha considerado su aplicación como proxy reverso en redes sin IP pública. Su principal ventaja radica en la posibilidad de exponer servicios internos sin necesidad de abrir puertos manualmente o modificar configuraciones en el router. Esto es especialmente útil cuando se combina con tecnologías como ZeroTier, ya que permite que un servidor dentro de la red privada pueda actuar como un punto de acceso a otros servicios internos [3].

En la implementación evaluada, se ha analizado la viabilidad de utilizar NGINX junto con ZeroTier para exponer servicios de manera segura dentro de una red virtual [3]. Dado que ZeroTier permite la interconexión de dispositivos a nivel de capa 2 o capa 3, NGINX puede actuar como un intermediario dentro de la misma red virtual sin necesidad de una IP pública. Esto resulta útil para servir aplicaciones web, API internas o sistemas de acceso remoto [3].

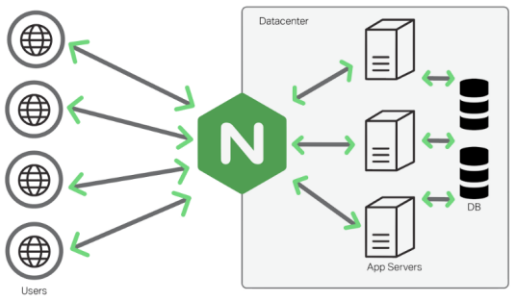

Fig. 5. Esquema Funcionamiento NGINX. Tomada de FreeCodeCamp.
https://www.freecodecamp.org/news/an-introduction-to-nginx-for-developers-62179b6a458f/

4 Implementación Practica

Para evaluar la viabilidad de las soluciones propuestas en entornos con CGNAT, se han implementado y analizado dos configuraciones distintas: ZeroTier combinado con NGINX y Tailscale en su configuración P2P pura.

4.1 Configuración de una VPN con ZeroTier y NGINX

Creación y Configuración de la Red Virtual
ZeroTier proporciona un Network Controller a través de su plataforma ZeroTier Central, donde se crean redes privadas con topologías personalizadas. Para iniciar la configuración, se accede al portal y se genera un Network ID, que posteriormente es utilizado para que los dispositivos se unan a la red [5].

Instalación y Conexión de los Dispositivos
En cada nodo de la red, se instala el cliente ZeroTier, permitiendo la autenticación en la red privada y el establecimiento de rutas entre los dispositivos [5]. A diferencia de las VPN tradicionales, esta conexión no requiere configuración manual de túneles ni apertura de puertos en el firewall, ya que ZeroTier gestiona automáticamente la conectividad mediante NAT traversal [4].

Autorización de Dispositivos y Asignación de Direcciones
Una vez que los dispositivos han solicitado unirse a la red, el administrador los autoriza manualmente desde la plataforma web. ZeroTier permite definir direcciones privadas en diferentes rangos (ejemplo: 192.168.192.0/24), creando una red privada que se comporta de manera similar a una LAN física [5].

Integración de ZeroTier con NGINX como Reverse Proxy
NGINX es una herramienta que funciona en la capa de transporte y aplicación, permitiendo recibir solicitudes desde Internet y redirigirlas a servicios internos sin exponer directamente la infraestructura subyacente. Dentro de una red ZeroTier, su rol es actuar como punto de acceso para los servicios internos, resolviendo la limitación de CGNAT sin necesidad de direcciones IP públicas [3].

NGINX se instala en un servidor dentro de la red ZeroTier y se configura para recibir tráfico en puertos específicos, los cuales son reenviados a otros dispositivos internos. Este modelo de proxy inverso permite el acceso a servicios como servidores web**,** bases de datos o APIs sin modificar la infraestructura de red existente [3].

4.2 Implementación de Tailscale sin VPS (P2P puro)

Implementación en una Red P2P
Instalación y Registro en la Plataforma
La instalación de Tailscale es sencilla y se realiza mediante un único comando en Linux o utilizando instaladores gráficos en Windows/macOS. Una vez instalado, el

usuario se autentica utilizando una cuenta de Google, GitHub o Microsoft, lo que permite la gestión centralizada de los dispositivos [6].

Autenticación y Establecimiento de Conexiones
Al iniciar sesión, Tailscale automáticamente descubre otros dispositivos de la red y establece las rutas necesarias para la comunicación. En la mayoría de los casos, se evita el uso de relay servers y los dispositivos pueden comunicarse directamente [6].

Uso de Subnet Routing y Exit Nodes
Uno de los aspectos más avanzados de Tailscale es la capacidad de gestionar el tráfico de red a través de Subnet Routing y Exit Nodes, lo que permite extender la conectividad a redes completas o utilizar un nodo como puerta de acceso [7].

Subnet Routing: Extensión de Red
En entornos donde se desea acceder a una LAN completa a través de Tailscale, un dispositivo puede actuar como gateway, anunciando rutas hacia subredes locales. Esto permite que otros dispositivos en la red Tailscale accedan a toda la infraestructura interna de la red local sin configuraciones adicionales en el firewall o router [6][7].

Exit Nodes: Redirección del Tráfico de Internet
Un Exit Node permite que el tráfico de un dispositivo sea enrutado a través de otro dispositivo en la red Tailscale, lo que resulta útil para eludir restricciones de red o proteger la identidad del usuario. Luego, en la interfaz de administración de Tailscale, se habilita la opción de usar este dispositivo como punto de salida, permitiendo que otros nodos envíen su tráfico a través de él [6][7].

5 Desarrollo de una Solución Open Source para Usuarios

Si bien soluciones como ZeroTier y Tailscale han demostrado ser efectivas para la conectividad segura en entornos con CGNAT [5][6], ambas son proyectos mantenidos por empresas, lo que introduce cierto grado de dependencia en infraestructura externa, aunque sean de código abierto [7]. Para garantizar una solución completamente self-hosted y alineada con los principios del software libre, este estudio propone el desarrollo de una herramienta basada en Nebula, una VPN P2P altamente escalable, diseñada para conectar dispositivos sin necesidad de servidores centralizados ni autenticación en la nube [8].

Nebula se diferencia de otras soluciones porque no requiere un servidor de control externo, sino que opera de manera completamente descentralizada, permitiendo que los dispositivos se conecten directamente a través de un sistema de autenticación mutua basada en certificados y un nodo lighthouse. Esta arquitectura ofrece una alternativa más segura y flexible para aquellos usuarios que buscan máximo control sobre su infraestructura de red sin depender de servicios comerciales o empresas externas [8].

Esta solución plantea el desarrollo de una herramienta que automatice la configuración de Nebula, permitiendo a cualquier usuario desplegar su propia VPN sin la complejidad de configurar manualmente cada nodo. La solución estará enfocada en ofrecer una implementación sencilla y accesible, asegurando que incluso usuarios sin experiencia en administración de redes puedan aprovechar los beneficios de una red privada completamente selfhosted y descentralizada [8].

5.1 Desarrollo de una Herramienta para el Usuario Común

El principal desafío de las soluciones selfhosted como Nebula es su complejidad de configuración [8]. A diferencia de soluciones más centralizadas como Tailscale o ZeroTier, donde la gestión de la red es automatizada a través de servicios en la nube [6][5], Nebula requiere que los usuarios administren sus propios certificados, configuraciones y reglas de firewall [8].

Para resolver este problema, se propone el desarrollo de una herramienta de implementación automatizada, que permita a los usuarios desplegar una VPN basada en Nebula sin necesidad de configurar manualmente cada dispositivo. Esta herramienta deberá ser capaz de:

- **Automatizar la instalación y configuración de Nebula** en distintos sistemas operativos, eliminando la necesidad de configuraciones manuales avanzadas.
- **Generar y distribuir certificados automáticamente**, permitiendo que los dispositivos se autentiquen de manera segura sin intervención del usuario.
- **Configurar nodos "Lighthouse" de manera automática**, asegurando que los dispositivos puedan encontrarse incluso si requiere ajustarlo a una IP dinámica con un nombre de dominio.
- **Ofrecer una interfaz gráfica intuitiva para administrar la red**, permitiendo visualizar los dispositivos conectados y realizar cambios sin necesidad de acceder a la línea de comandos.

5.2 Incorporación de la Herramienta al Ecosistema GNU

Para garantizar que esta solución sea completamente libre y accesible, se distribuirá bajo una licencia open source y se publicará en plataformas como GitHub y GitLab, permitiendo que la comunidad colabore en su desarrollo y mejora.

Se explorará la posibilidad de incluir la herramienta en repositorios oficiales de distribuciones GNU/Linux, permitiendo su instalación a través de gestores de paquetes como apt, dnf y pacman.

Asimismo, se generará una documentación completa y accesible, incluyendo tutoriales, ejemplos de configuración y guías de solución de problemas, con el objetivo de facilitar la adopción de la herramienta en distintos entornos. Se incentivará la partici-

pación activa de la comunidad, permitiendo que los usuarios propongan mejoras, reporten errores y colaboren en el desarrollo de nuevas funcionalidades.

6 Conclusiones y Futuro

Las pruebas realizadas han permitido identificar las fortalezas y debilidades de cada tecnología en el contexto de la conectividad segura sin IP pública.

ZeroTier ha demostrado ser una solución altamente funcional y adaptable, permitiendo crear redes privadas sin necesidad de configuraciones manuales complejas. Su compatibilidad con múltiples plataformas y su enfoque en redes peer-to-peer descentralizadas lo convierten en una opción robusta para usuarios que buscan flexibilidad, simplicidad y un código abierto [5].

Tailscale, por otro lado, ha sobresalido por su facilidad de uso y configuración automática, eliminando gran parte de la complejidad técnica de las VPN tradicionales. Su enfoque en la seguridad y administración centralizada simplifica la gestión de redes privadas, pero su dependencia de un servicio en la nube representa una limitación para quienes buscan una solución completamente libre y controlada por el usuario [6].

NGINX ha sido evaluado como una herramienta complementaria clave dentro de la arquitectura propuesta. Su uso como reverse proxy ha demostrado ser una estrategia eficaz para exponer servicios internos sin necesidad de modificar la infraestructura de red del usuario. Su integración con ZeroTier permite que cualquier dispositivo dentro de la red pueda acceder a servicios internos de manera segura y sin exponer direcciones IP públicas [3].

Nebula, también, ha demostrado ser una de las soluciones más flexibles y completamente self-hosted, al permitir la creación de redes privadas descentralizadas sin necesidad de depender de una infraestructura centralizada. Su enfoque en seguridad, autenticación mutua y segmentación de red la convierte en una alternativa atractiva para quienes buscan máximo control y privacidad [7].

En términos generales, la elección entre Nebula, ZeroTier o Tailscale dependerá de la prioridad que tenga el usuario en términos de control y facilidad de implementación. Para aquellos que buscan una solución totalmente selfhosted y sin dependencias externas, Nebula es la mejor opción. Para quienes buscan facilidad de configuración y menor curva de aprendizaje, ZeroTier con NGINX o Tailscale pueden ser alternativas más prácticas.

6.1 Propuestas Futuras

Para Nebula, una de las propuestas más relevantes es la implementación de un sistema de despliegue automatizado, que permita a los usuarios configurar y administrar su red privada sin necesidad de realizar configuraciones manuales extensas. Esto incluiría la creación de herramientas gráficas que faciliten la administración de nodos y reglas de firewall.

Finalmente, una dirección futura clave es la optimización de Nebula para escenarios de alta disponibilidad y rendimiento, explorando su funcionamiento con múltiples Lighthouses, redundancia de nodos y segmentación avanzada de redes. Este enfoque permitiría que Nebula sea utilizado en infraestructuras más exigentes, proporcionando conectividad segura y estable incluso en entornos corporativos o de servidores distribuidos.

Bibliografía

1. Song, L. (2022). Set Up Your Own IPsec VPN, OpenVPN and WireGuard Server (Build Your Own VPN).
2. C. Donley, L. Howard, V. Kuarsingh, J. Berg, and J. Doshi. (2013). RFC 7021: Assessing the Impact of Carrier-Grade NAT on Network Applications. RFC Editor, USA.
3. Soni, R. (2016). Nginx. Berkeley: Apress.
4. Phuoc, H. C., Hunt, R., & McKenzie, A. (2008). NAT traversal techniques in peer-to-peer networks. In Proceedings of the New Zealand Computer Science Research Student Conference (NZCSRSC).
5. Sánchez Rubio, M. (2022). VPN ZeroTier: instalación, configuración y fundamentos teóricos (Doctoral dissertation, Universitat Politècnica de València).
6. Master, A., & Garman, C. (2021). A WireGuard Exploration.
7. Kjorveziroski, V., Bernad, C., Gilly, K., & Filiposka, S. (2024). Full-mesh VPN performance evaluation for a secure edge-cloud continuum. Software: Practice and Experience.
8. Huber, R. (2019). Nebula: Open Source Overlay Networking. Nebula Technical Documentation, https://nebula.defined.net/docs/.