ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Análisis Comparativo del Rendimiento y la Seguridad de Tecnologías VPN.

Autor:

Floril Condemaita Jonathan Steven

Director:

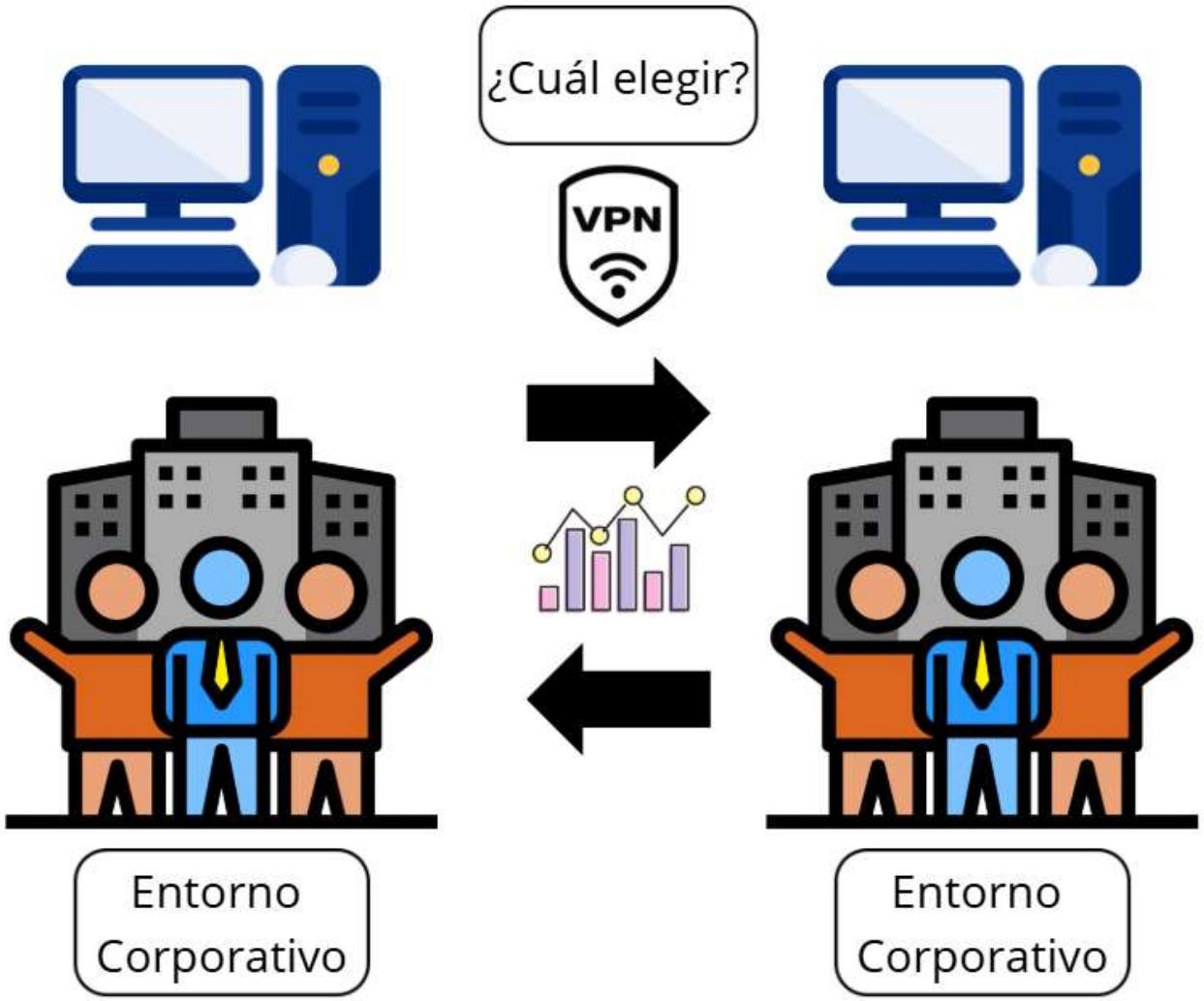
Ing. Núñez Agurto, Alberto Daniel, PhD.



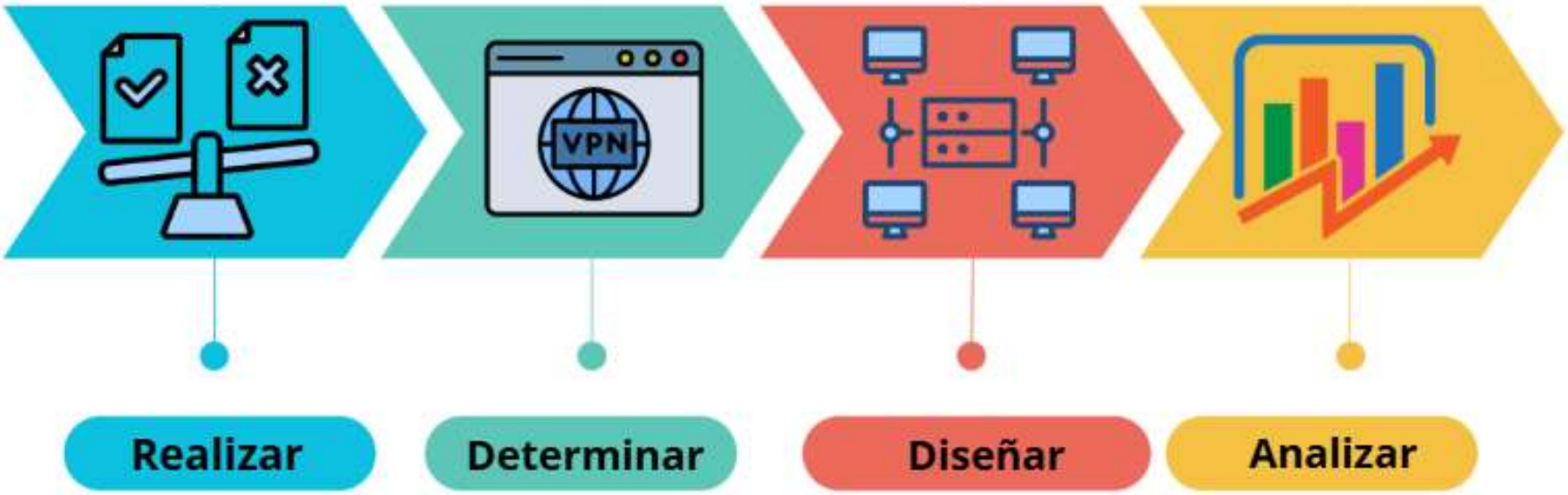
ÍNDICE DE CONTENIDO

1. Introducción
2. Objetivos
3. Marco Teórico
4. Metodología
5. Resultados
6. Conclusiones
7. Recomendaciones

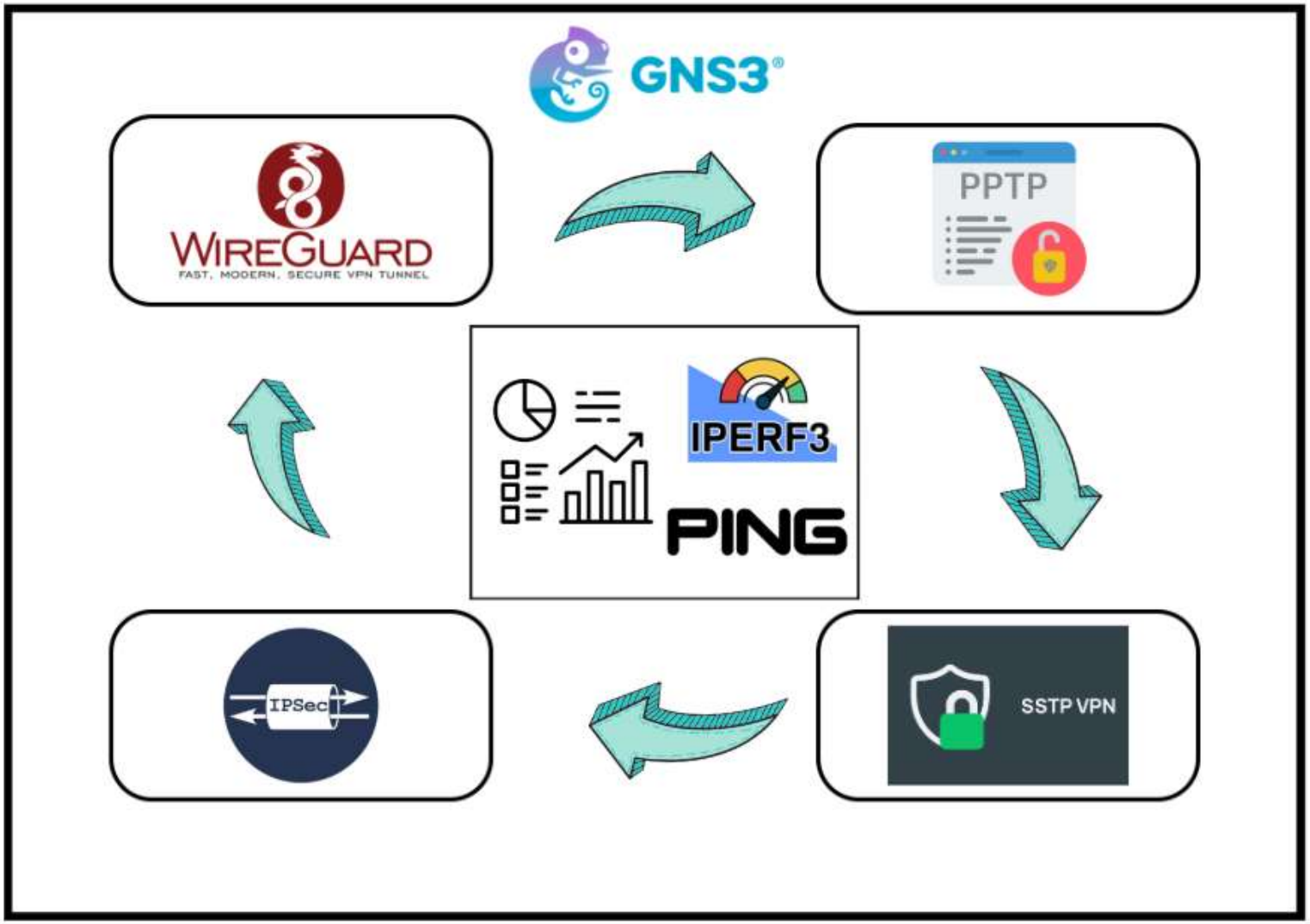
Introducción



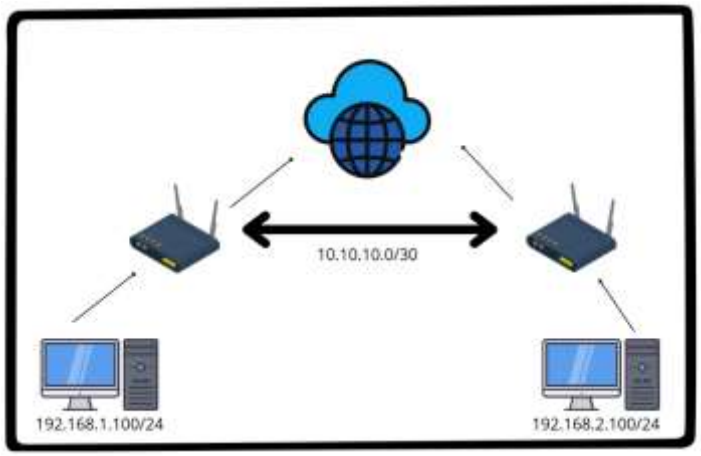
Objetivos



Alcance


GNS3
WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL
PPTP
IPERF3
PING
IPSec
SSTP VPN

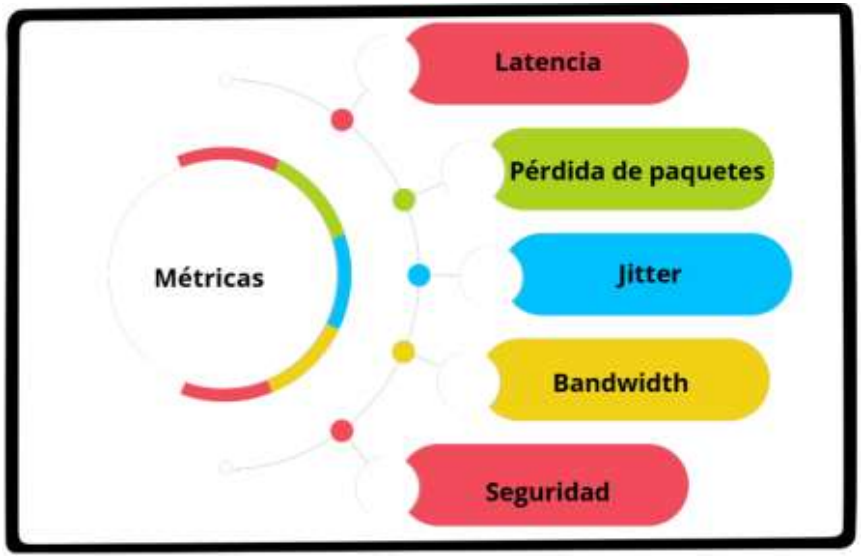
VPN



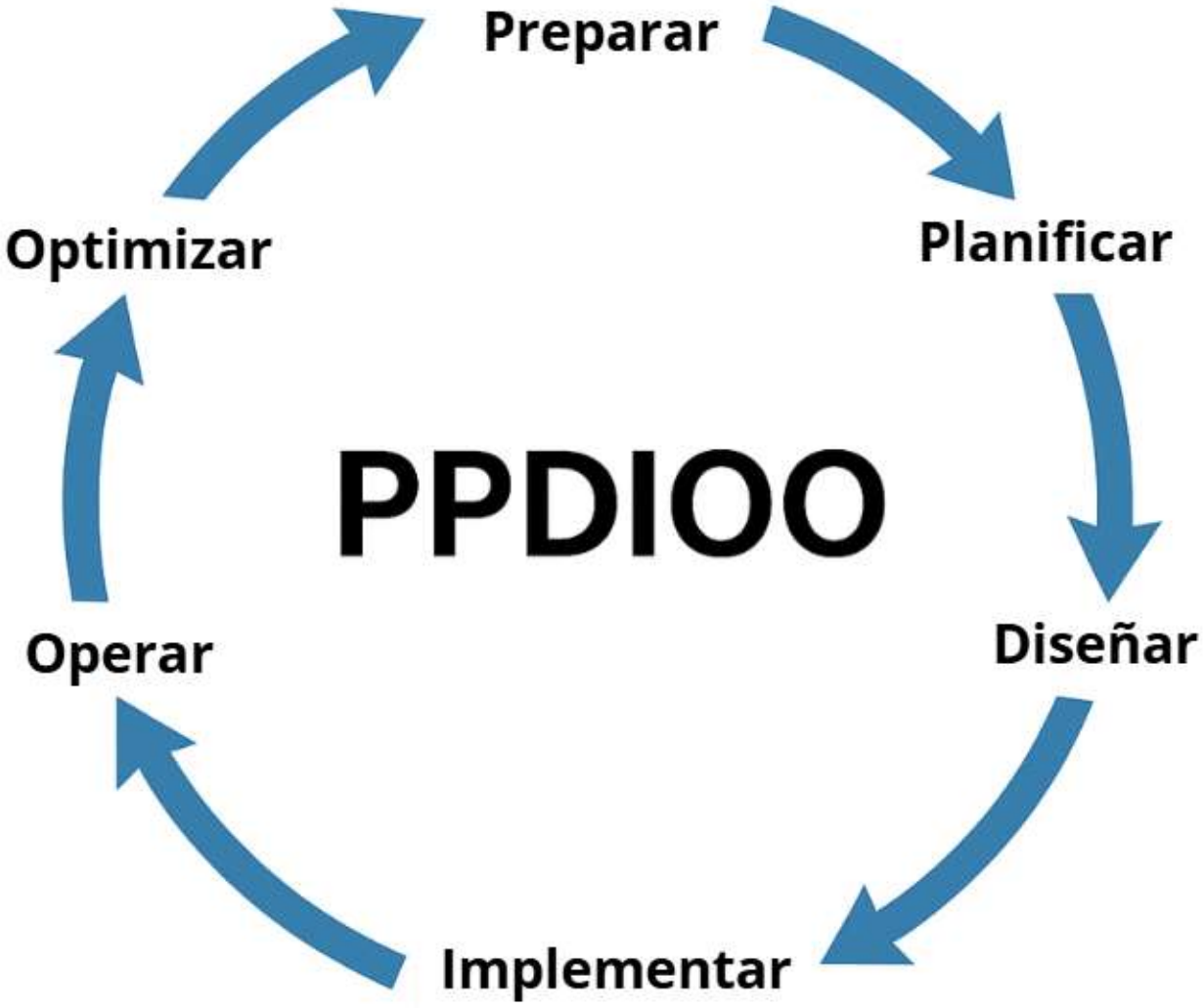
Entorno emulado



Métricas



Metodología

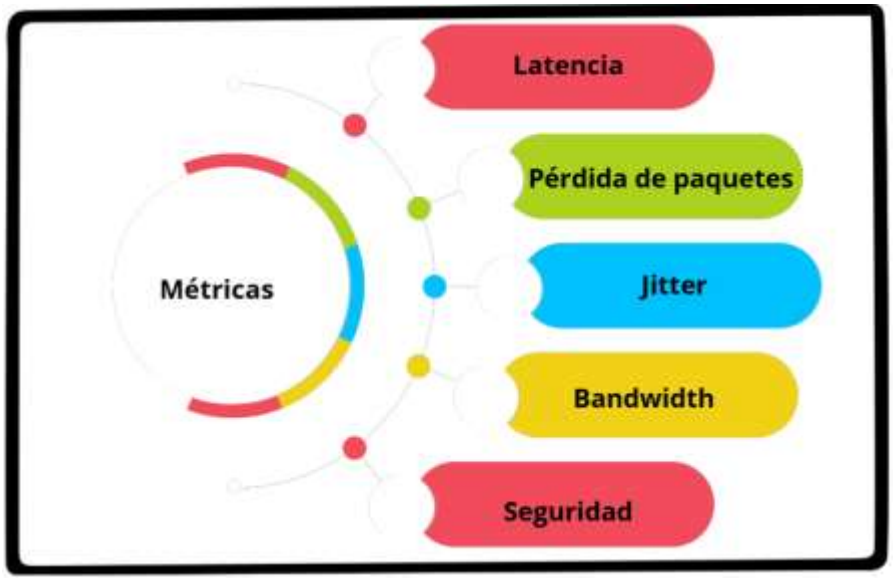


1.Preparar

Escenario



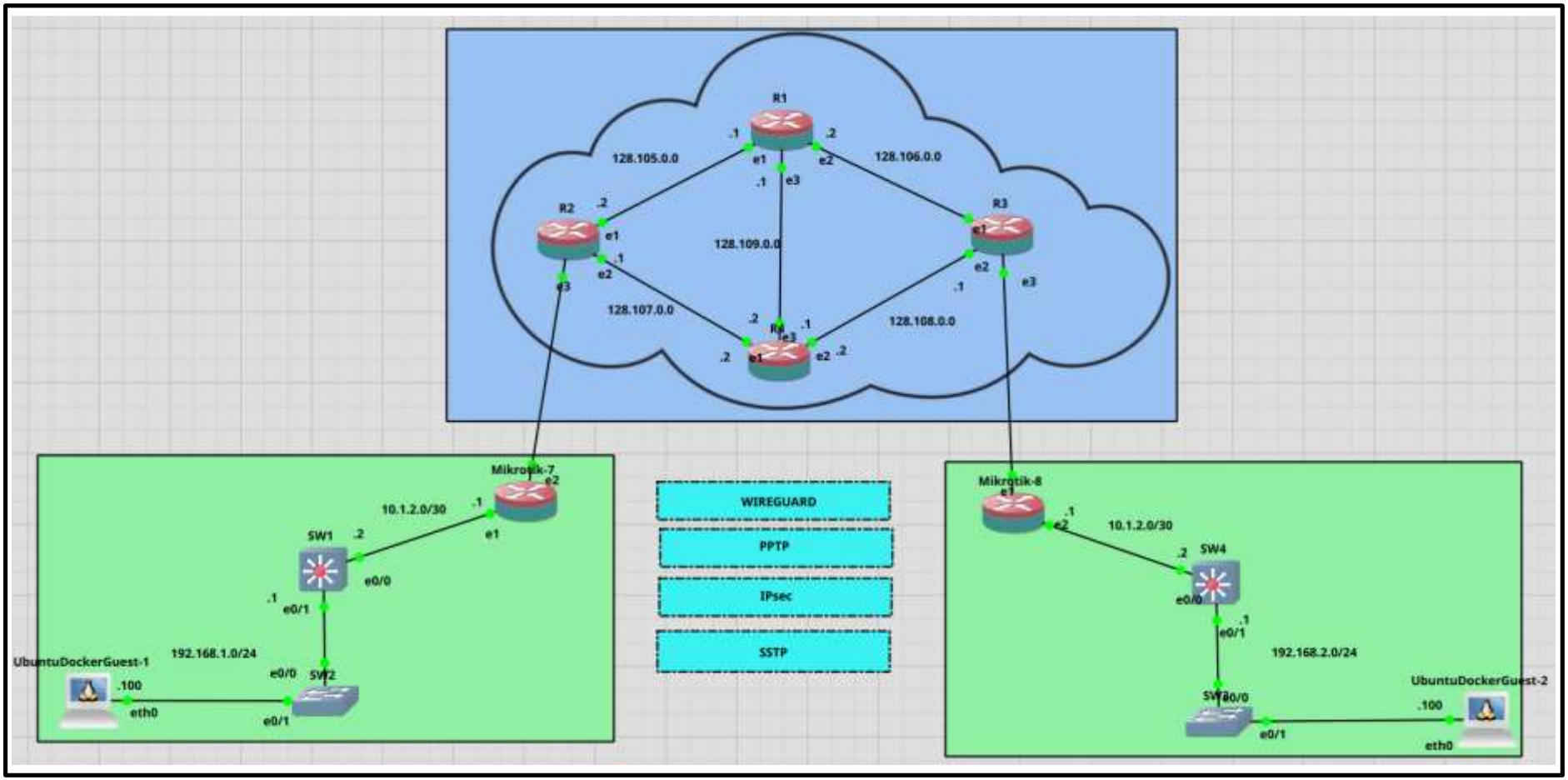
Métricas de evaluación



2. Planificar



3. Diseñar


R1
R2
R3
R4
128.105.0.0
128.106.0.0
128.109.0.0
128.107.0.0
128.108.0.0
Mikrotik-7
Mikrotik-8
10.1.2.0/30
SW1
SW2
SW4
192.168.1.0/24
192.168.2.0/24
UbuntuDockerGuest-1
UbuntuDockerGuest-2
WIREGUARD
PPTP
IPsec
SSTP

4. Implementar

Red WAN

Implementación de enrutamiento dinámico eBGP

BGP

Connection | Templates | Sessions | VPN

Name	Template	AFI	Router ID	Remote Address	Remot...	Remote AS	Local Role	Multihop	Tx TTL	Connect	Listen	Use BFD	Routing T...	VRF
Peer-R2	default		1.1.1.1	128.105.0.2/24		65532	ebgp						main	
Peer-R3	default		1.1.1.1	128.106.0.1/32		65533	ebgp						main	
Peer-R4	default		1.1.1.1	128.109.0.2/32		65534	ebgp						main	

BGP

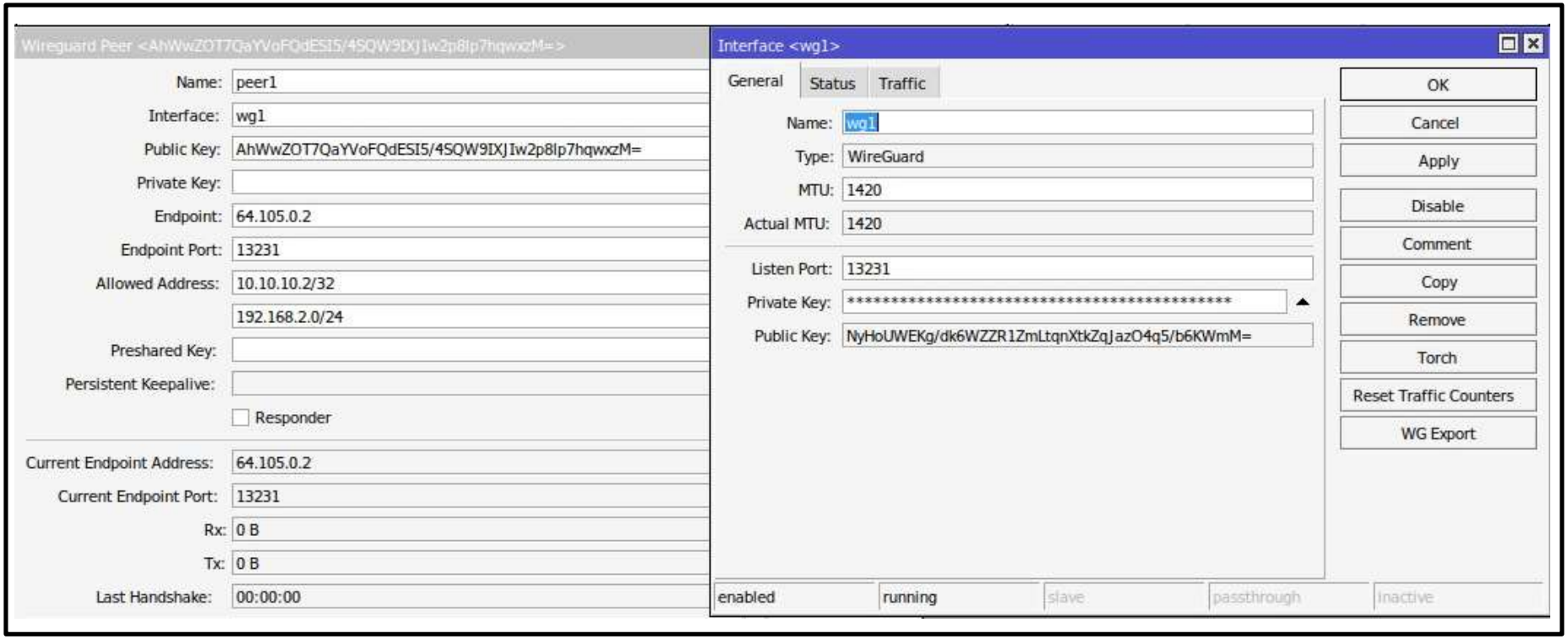
Connection | Templates | Sessions | VPN

Resend | Refresh | Stop | Clear | Dump Adv.

	Name	Prefix Count	Uptime	Remote Add...	Remote AS	Remot...	Remote ID	Remote Cap...	Local Address	Local AS	Local ...	Local ID	Local Capabi...
E	Peer-R2-1	7	00:07:27	128.105.0.2	65532	ip	2.2.2.2	mp rr as4 gr	128.105.0.1	65531	ip	1.1.1.1	mp rr as4 gr
E	Peer-R3-1	7	00:07:36	128.106.0.1	65533	ip	3.3.3.3	mp rr as4 gr	128.106.0.2	65531	ip	1.1.1.1	mp rr as4 gr
E	Peer-R4-1	10	00:07:35	128.109.0.2	65534	ip	4.4.4.4	mp rr as4 gr	128.109.0.1	65531	ip	1.1.1.1	mp rr as4 gr

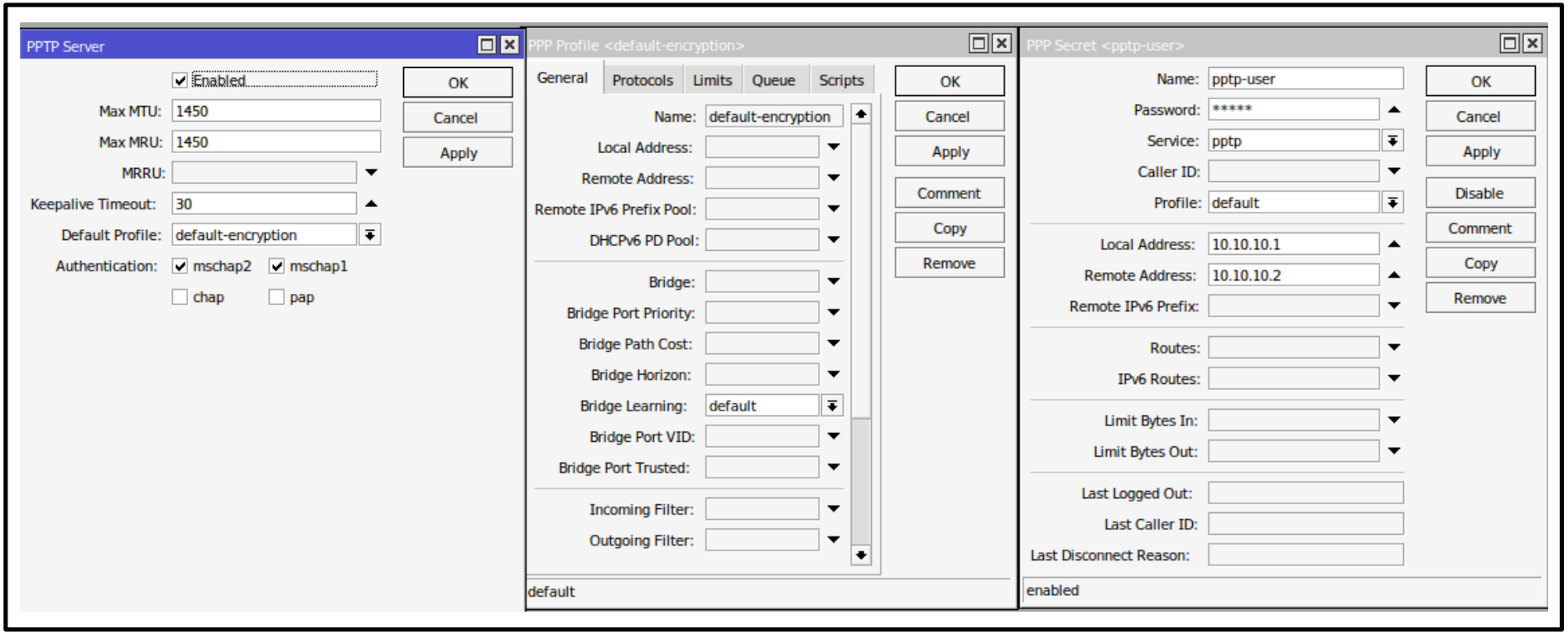
4. Implementar

Implementación WireGuard



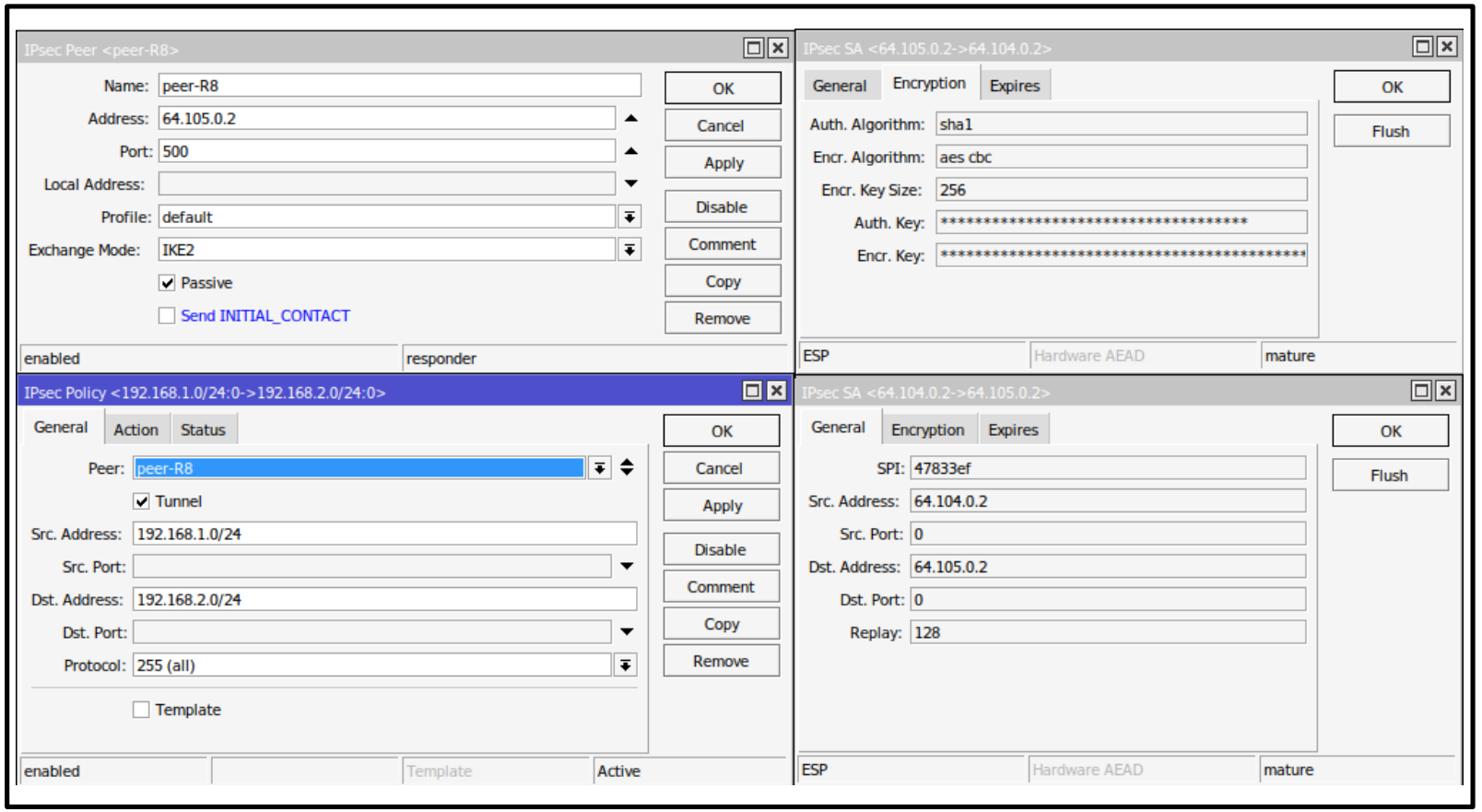
4. Implementar

Implementación PPTP



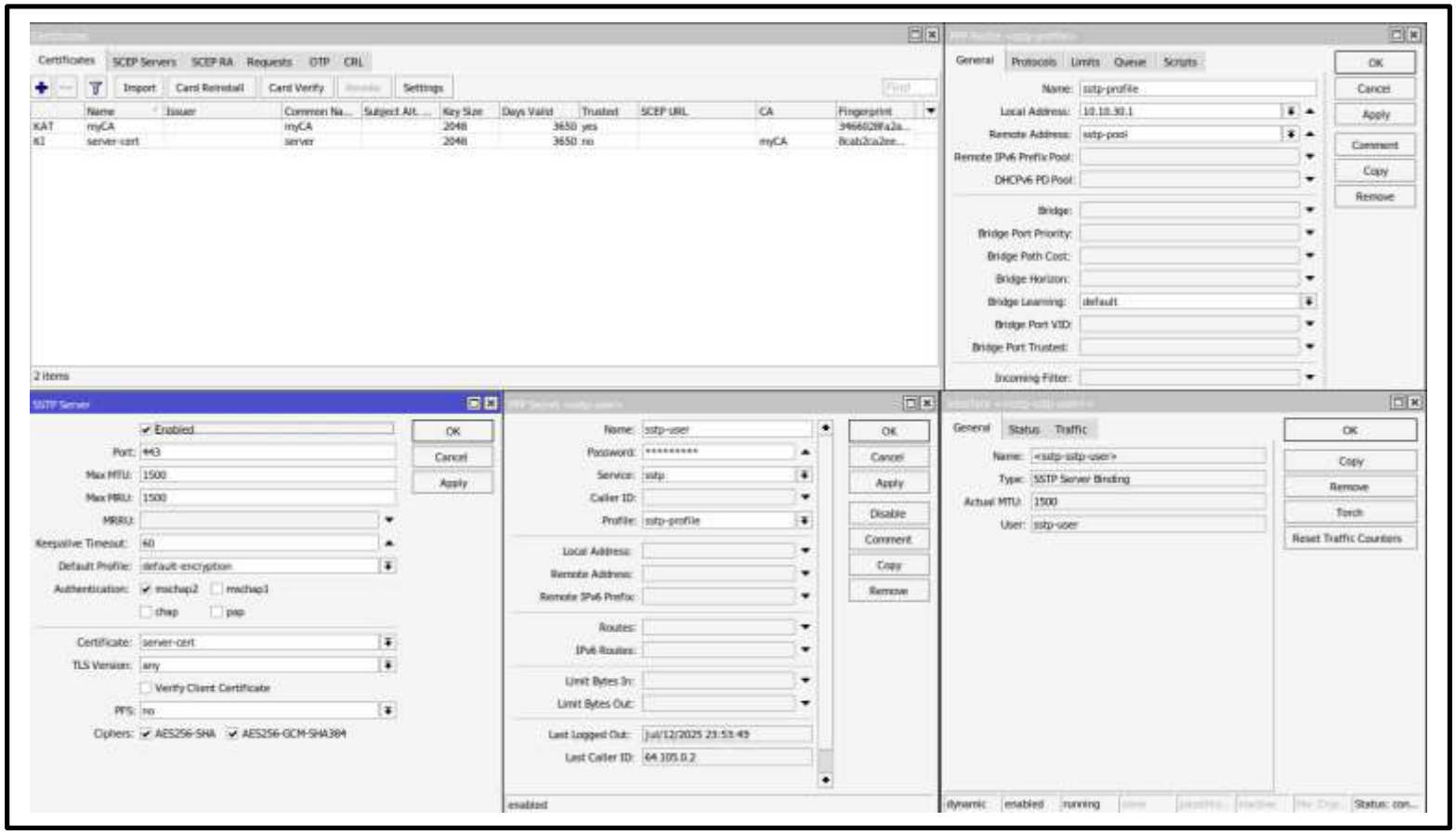
4. Implementar

Implementación IPsec



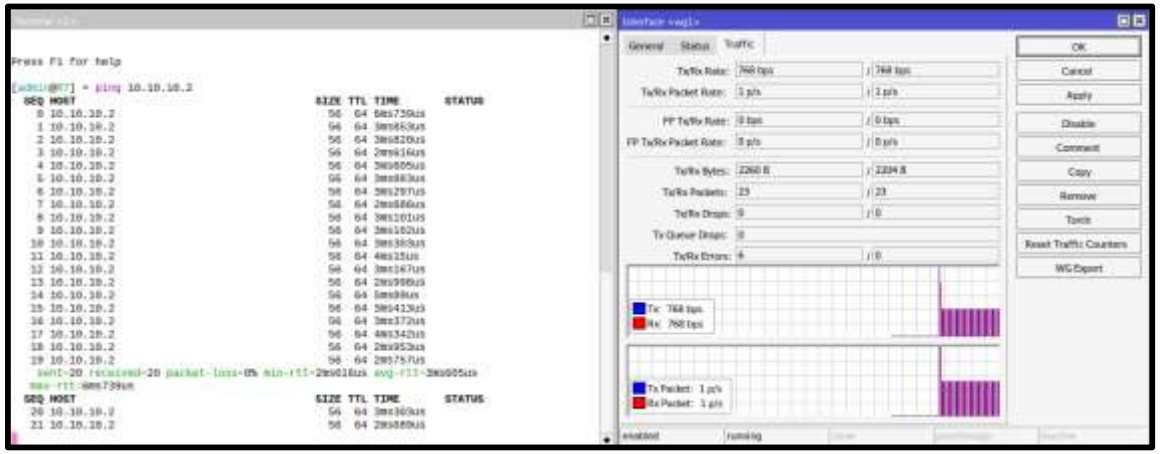
4. Implementar

Implementación SSTP

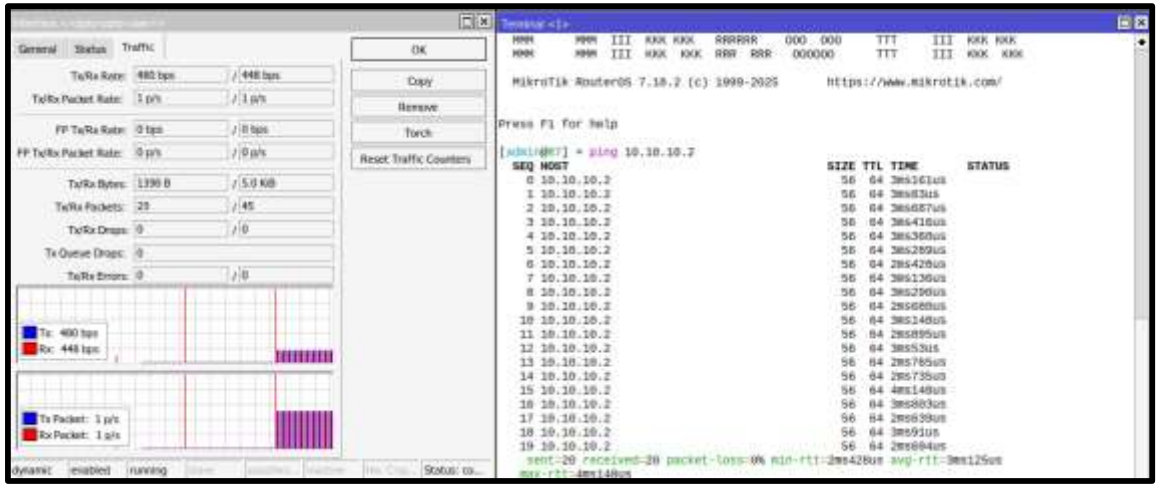


5. Operar

Operación WireGuard

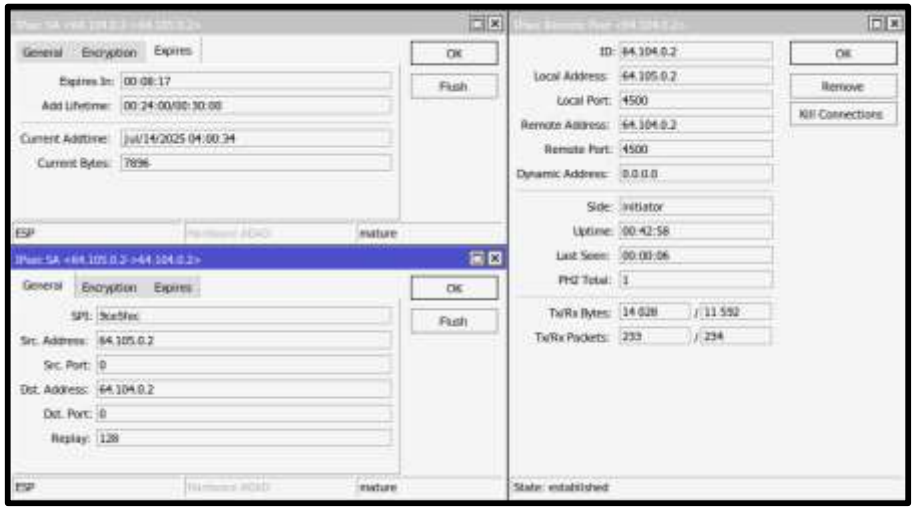


Operación PPTP

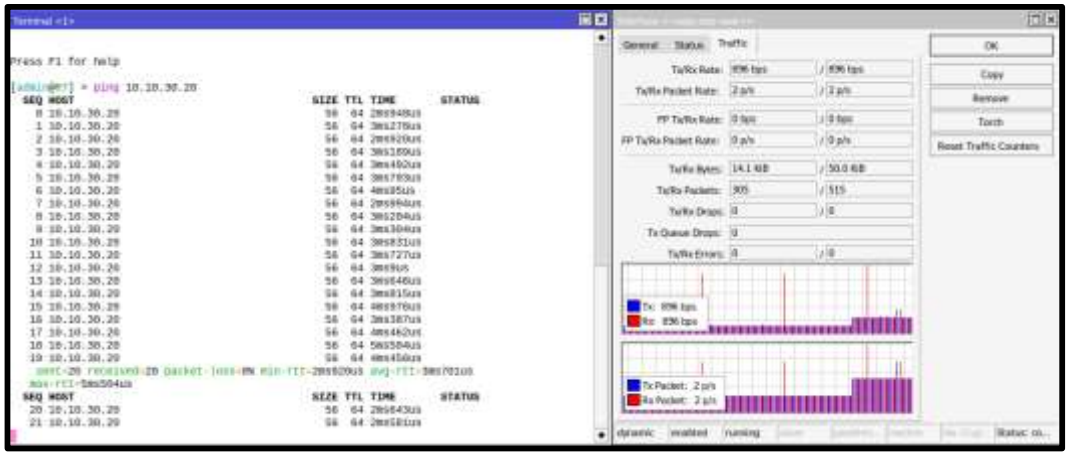


5. Operar

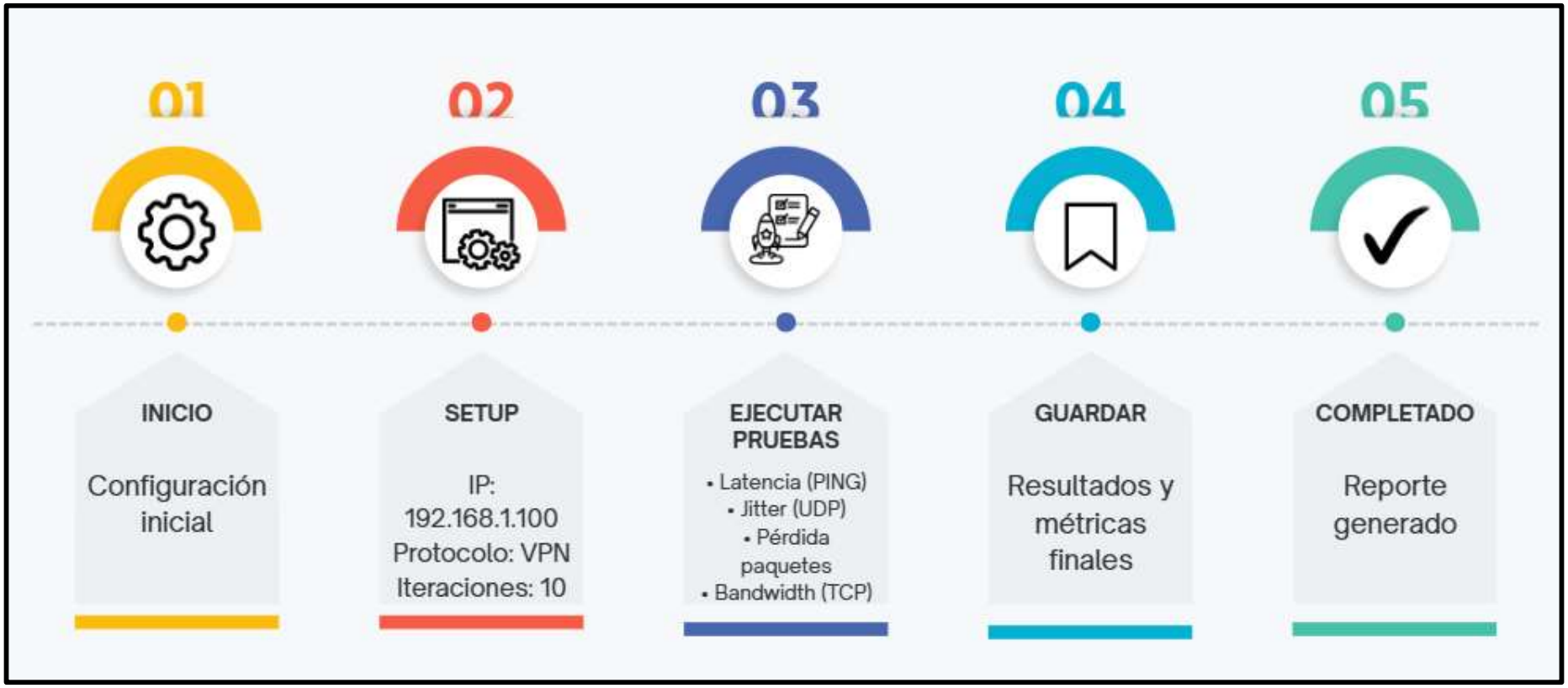
Operación IPsec



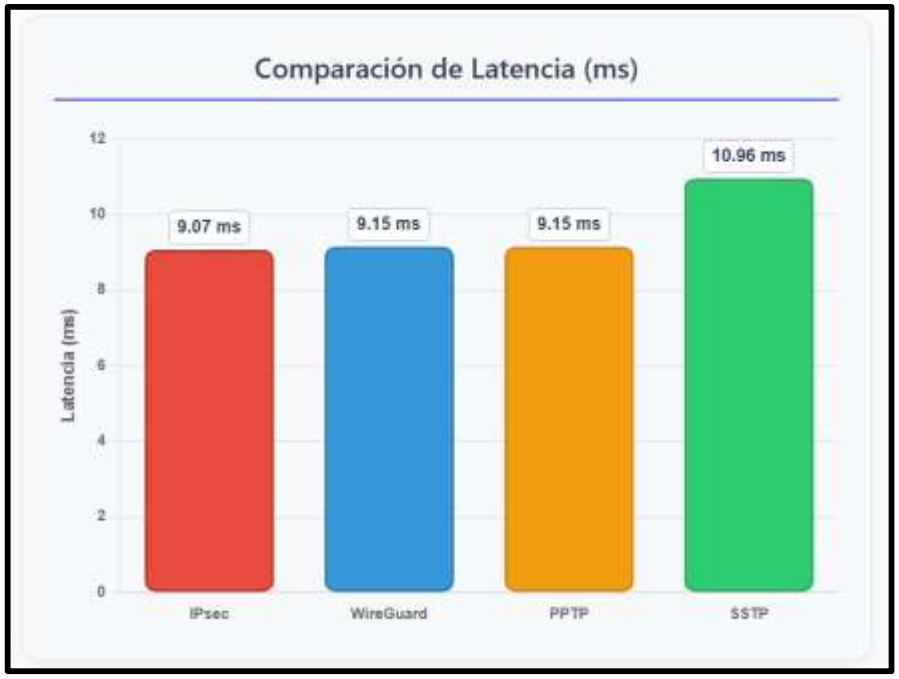
Operación SSTP



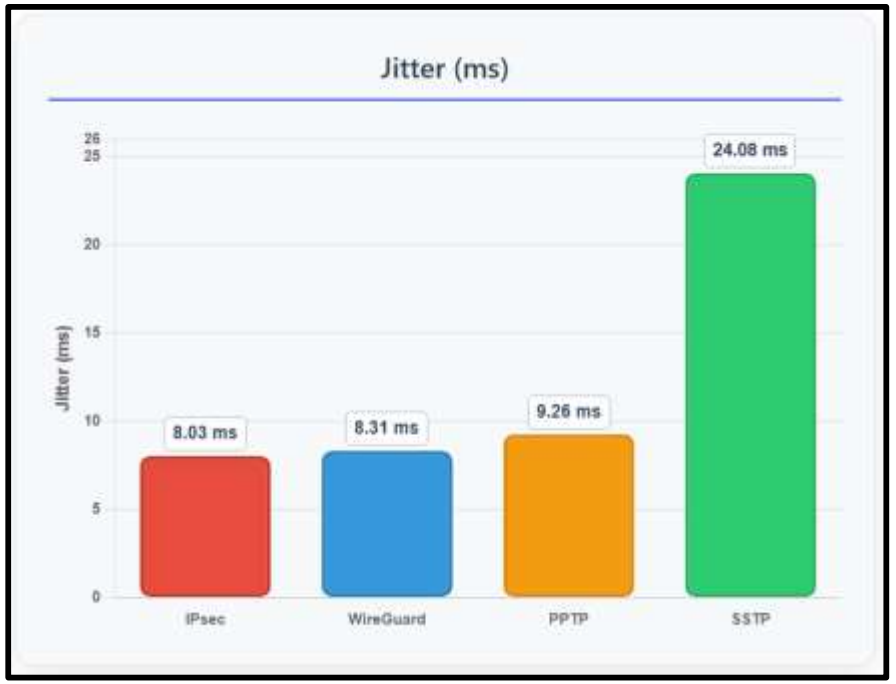
6. Optimizar


01
02
03
04
05
INICIO
Configuración inicial
SETUP
IP: 192.168.1.100
Protocolo: VPN
Iteraciones: 10
EJECUTAR PRUEBAS
• Latencia (PING)
• Jitter (UDP)
• Pérdida paquetes
• Bandwidth (TCP)
GUARDAR
Resultados y métricas finales
COMPLETADO
Reporte generado

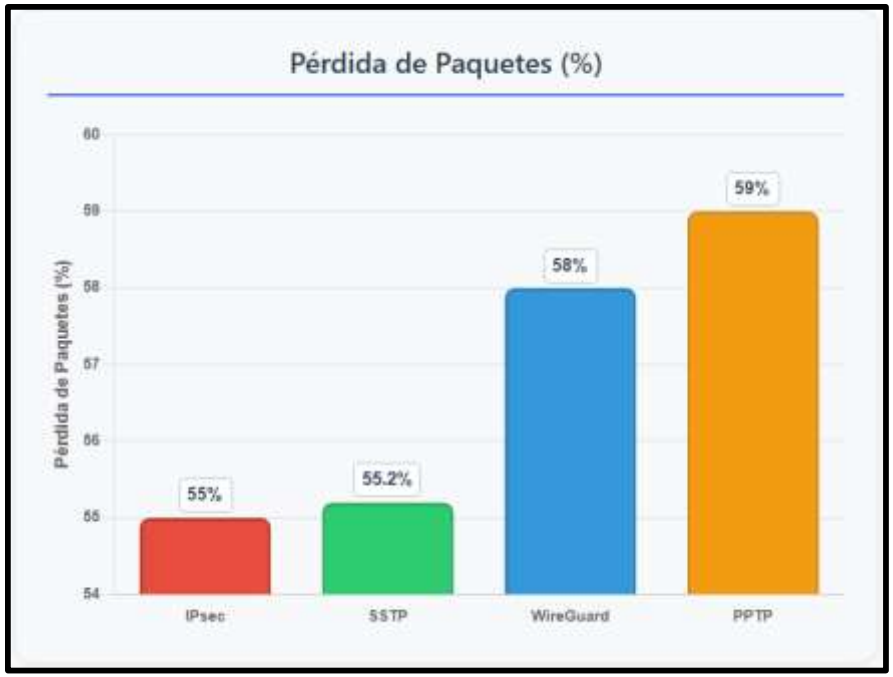
Latencia



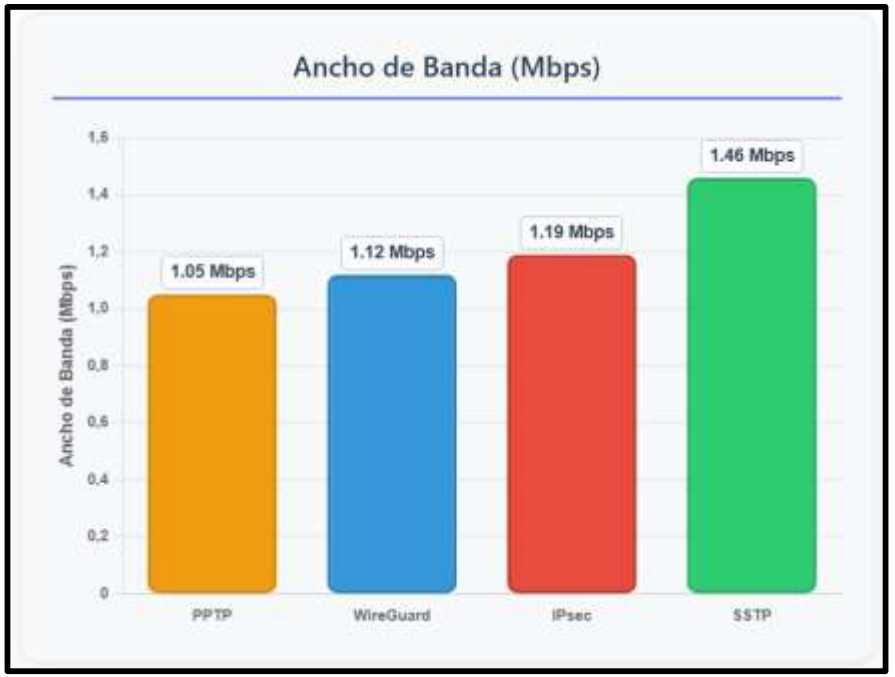
Jitter



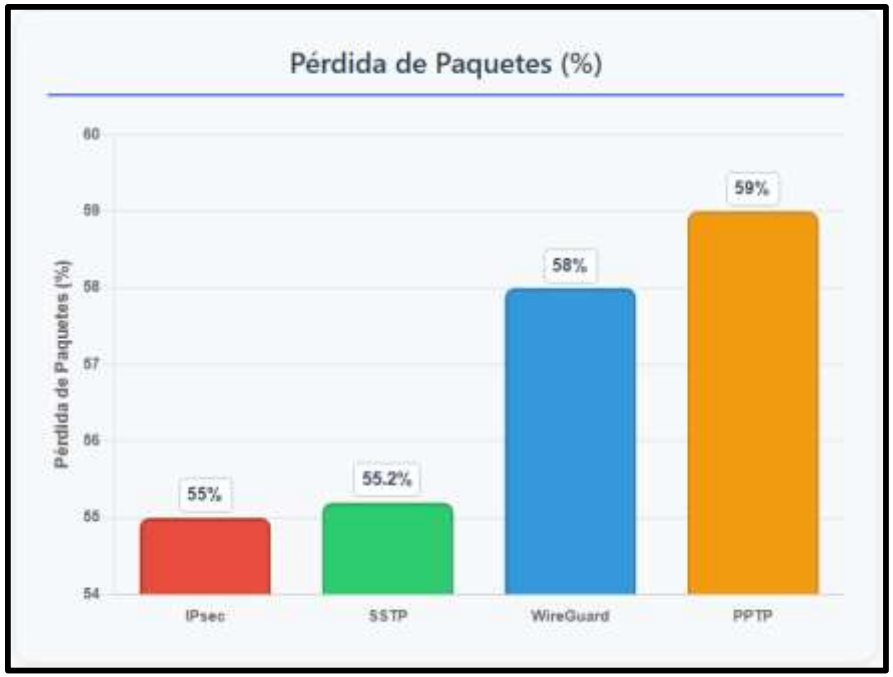
Pérdida de paquetes



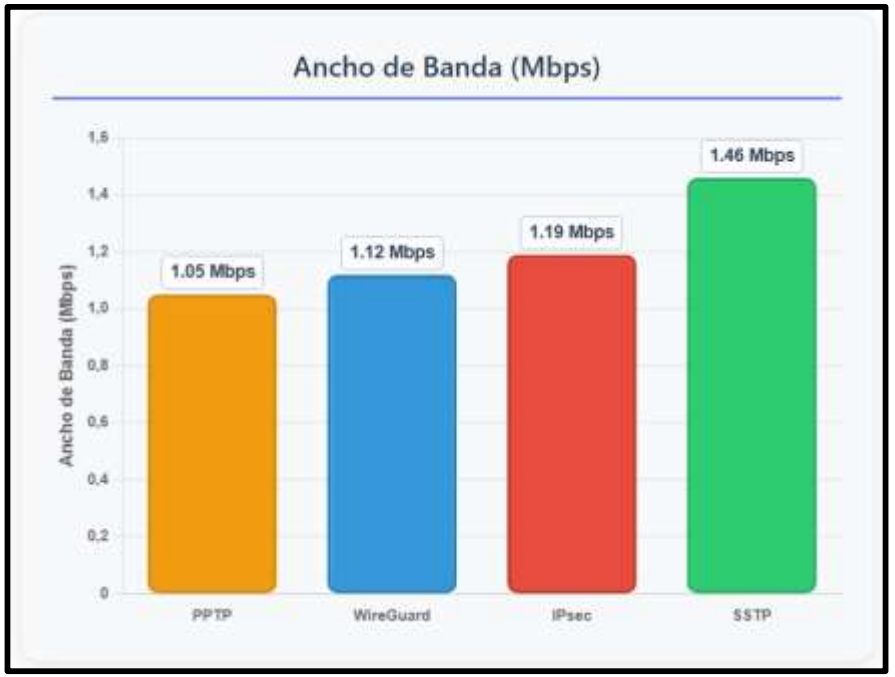
Bandwidth



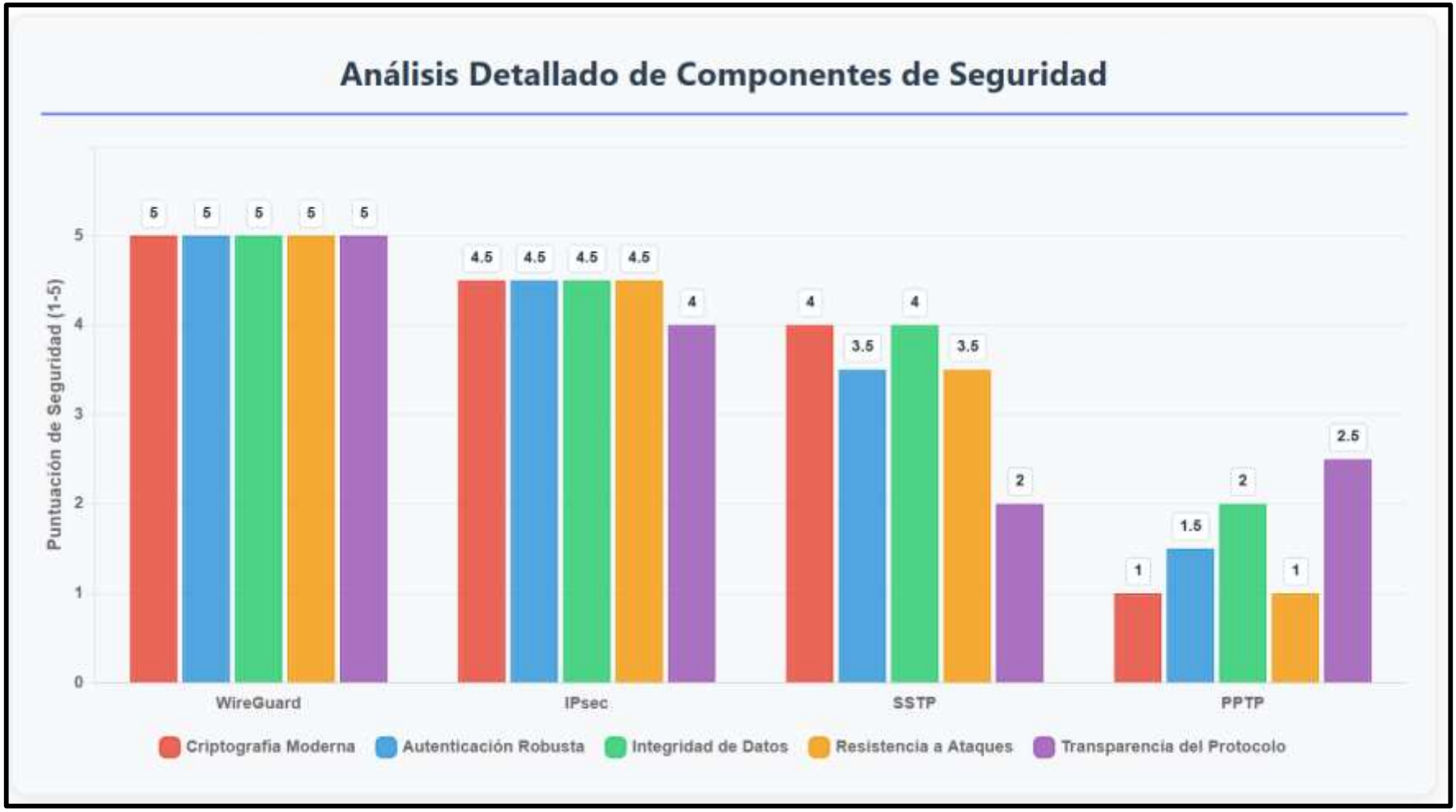
Pérdida de paquetes



Bandwidth



Seguridad


Análisis Detallado de Componentes de Seguridad
Puntuación de Seguridad (1-5)
0
1
2
3
4
5
5
5
5
5
5
4.5
4.5
4.5
4.5
4
4
3.5
4
3.5
2
1
1.5
2
1
2.5
WireGuard
IPsec
SSTP
PPTP
Criptografía Moderna
Autenticación Robusta
Integridad de Datos
Resistencia a Ataques
Transparencia del Protocolo

Conclusiones

Objetivo 1 Completado



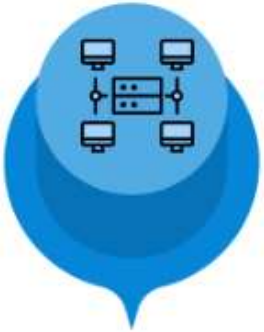
Se diseñó y configuró exitosamente el entorno de emulación de red, el cual permitió la implementación y evaluación de cada túnel VPN.

Objetivo 2 Completado



La presente investigación, determinó las tecnologías VPN para el análisis en el ámbito corporativo, identificando a IPsec, WireGuard, SSTP y PPTP como los protocolos relevantes.

Objetivo 3 Completado



Se desarrollaron y ejecutaron escenarios de red controlados para cada VPN, midiendo parámetros como latencia, jitter, pérdida de paquetes y ancho de banda.

Objetivo 4 Completado



El análisis reveló que IPsec y WireGuard ofrecieron el mejor rendimiento y seguridad, mientras que SSTP tuvo el ancho de banda mas destacado y PPTP fue la opción menos eficaz.

Recomendaciones

1

PROTOCOLO SEGÚN EL TRÁFICO

Para futuras implementaciones, se recomienda priorizar la configuración de protocolos VPN en función del tipo de tráfico y las características del entorno.

2

ELIMINA PPTP

Es imprescindible evitar el uso del protocolo PPTP, incluso en redes privadas o entornos de prueba, debido a sus vulnerabilidades estructurales en mecanismos de cifrado y autenticación.

3

AUTOMATIZA PRUEBAS Y MONITOREO

se sugiere implementar un sistema de automatización para las pruebas de rendimiento y supervisión de tráfico cifrado

4

GESTIÓN DEL CICLO DE VIDA VPN

Se sugiere implementar buenas prácticas de gestión del ciclo de vida de las VPN, que incluyan rotación periódica de claves, renovación de certificados, desactivación segura de túneles obsoletos y auditorías de configuración cada seis meses.

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

¡Gracias por su atención!

Autor:

Floril Condemaita Jonathan Steven

Director:

Ing. Núñez Agurto, Alberto Daniel, PhD.

