edulearn
Revista Multidisciplinar

Diseño e implementación de una red corporativa multisede segura con DMZ, AAA y defensa en profundidad

Design and implementation of a secure multi-site corporate network with DMZ, AAA, and defense in depth

Gustavo Enrique Muñoz Velez[1*], Joel Alexander Muñoz Velez[1]

Génesis Daniela Solano Ordoñez[1], Jonathan Andrés Medina Muñoz[1]

Jordy Ortiz Jimbo German[1], Luis Ángel Gonzales Olaya[1]

[1] *Universidad Técnica de Machala, Ecuador*

* *Autor de Correspondencia:* gmunoz7@utmachala.edu.ec

Resumen: La dependencia de servicios distribuidos exige arquitecturas que integren seguridad y conectividad. Este trabajo presenta el diseño y validación en Cisco Packet Tracer de una infraestructura multisede segura para RedTec Solutions S.A. La propuesta adopta un modelo de núcleo colapsado con microsegmentación por VLANs y una Zona Desmilitarizada (DMZ) para servicios públicos. Se aplicó una estrategia de defensa en profundidad mediante listas de control de acceso (ACL), gestión vía SSH y autenticación centralizada AAA (RADIUS/TACACS+). Las pruebas funcionales validaron la convergencia de VoIP y el aislamiento efectivo entre zonas, confirmando la viabilidad del diseño como base para entornos corporativos seguros de mediana escala.

Palabras clave: redes multisede, VLAN, DMZ, AAA, RADIUS, TACACS+, VoIP, Cisco Packet Tracer.

Abstract: The dependence on distributed services requires architectures that integrate security and connectivity. This paper presents the design and validation in Cisco Packet Tracer of a secure multi-site infrastructure for RedTec Solutions S.A. The proposal adopts a collapsed core model with microsegmentation by VLANs and a Demilitarized Zone (DMZ) for public services. A defense-in-depth strategy was applied using access control lists (ACLs), SSH management, and centralized AAA authentication (RADIUS/TACACS+). Functional tests validated VoIP convergence and effective isolation between zones, confirming the viability of the design as a basis for secure medium-scale corporate environments.

Keywords: Multi-site networks, VLAN, DMZ, AAA, RADIUS, TACACS+, VoIP, Cisco Packet Tracer.

1. Introducción

En la era digital actual, la infraestructura de red se ha convertido en la columna vertebral operativa de las organizaciones, evolucionando desde simples conexiones locales hacia arquitecturas distribuidas complejas que deben soportar una demanda creciente de servicios convergentes. El diseño de estas redes, conocidas como Redes de Área de Campus (CAN), ya no puede limitarse únicamente a garantizar la conectividad física; debe integrar desde su concepción estrategias de alta disponibilidad y seguridad lógica para mitigar las vulnerabilidades inherentes a la expansión geográfica (Meghana S. et al., 2024).

A medida que las empresas extienden sus operaciones hacia sucursales remotas, la superficie de ataque se amplía, exponiendo activos críticos a amenazas tanto externas como internas. Ahmed y Al-Hamadani (2021) señalan que los modelos de red tradicionales resultan insuficientes ante el panorama actual de ciberseguridad, haciendo imperativa la transición hacia Redes de Campus Seguras (SCN). Este nuevo paradigma exige la implementación de una estrategia de "Defensa en Profundidad", donde la protección no depende de un único perímetro, sino de múltiples capas de

control que incluyen la microsegmentación, la gestión estricta de identidades y el filtrado de tráfico en cada punto de la infraestructura.

Sin embargo, la complejidad de gestionar estos controles en entornos heterogéneos representa un desafío técnico significativo. Investigaciones recientes advierten que la falta de políticas de segmentación adecuadas y el uso de protocolos de administración débiles son vectores comunes que comprometen la confidencialidad e integridad de la información corporativa (Alexander & Roman-Gonzalez, 2023; Mhaskar et al., 2021). Por consiguiente, el diseño de arquitecturas modernas debe priorizar no solo la eficiencia en la transmisión de datos, sino también la trazabilidad de las acciones administrativas y el aislamiento efectivo de los servicios públicos.

En este contexto, el presente trabajo de investigación aborda el diseño e implementación de una infraestructura de red segura y multiservicio para la empresa RedTec Solutions S.A.. El estudio se centra en el desarrollo de una arquitectura distribuida que interconecta una sede central y una sucursal remota, utilizando el entorno de simulación Cisco Packet Tracer para validar la eficacia de los controles de seguridad propuestos, una herramienta cuya validez para el modelado de topologías empresariales ha sido ampliamente documentada (Thoyyibah et al., 2024; Adedokun-Shittu et al., 2021).

El objetivo principal es demostrar cómo la integración de tecnologías de segmentación lógica (VLANs), zonas desmilitarizadas (DMZ) y sistemas de autenticación centralizada (AAA) permite construir una red resiliente capaz de soportar servicios de voz y datos de manera convergente (Lyimo, 2023). A través de una metodología de diseño descendente, se evalúa la capacidad de la infraestructura para resistir accesos no autorizados y garantizar la continuidad operativa, proporcionando un modelo de referencia para el aseguramiento de redes corporativas en el sector PYME.

1.1. Redes de Campus y Empresariales Multisede

El diseño de infraestructuras para entornos corporativos distribuidos ha evolucionado desde la simple interconexión física hacia modelos lógicos complejos que priorizan la seguridad y la segmentación. Meghana S. et al. (2024) analizan la estructura fundamental de las Redes de Área de Campus (CAN), destacando que la integración de

múltiples LANs en un radio geográfico extendido requiere una jerarquía de conmutación robusta. Su estudio enfatiza la transición del modelo cableado tradicional hacia entornos inalámbricos flexibles, permitiendo el acceso a recursos sin dependencia de ubicaciones fijas.

Si bien este tipo de arquitectura resulta efectiva para satisfacer la demanda de conectividad y acceso a recursos, puede resultar insuficiente si no se complementa con una estrategia de defensa en profundidad. En este sentido, Ahmed y Al-Hamadani (2021) proponen que las arquitecturas multisede modernas deben evolucionar hacia Redes de Campus Seguras (Secure Campus Networks, SCN). A diferencia de los diseños planos convencionales, su propuesta prioriza la microsegmentación mediante múltiples VLAN y la configuración de una topología lógica en malla (mesh), con el objetivo de mejorar la redundancia y lograr un mayor aislamiento del tráfico considerado crítico.

A pesar de estos avances, los trabajos citados se centran predominantemente en la seguridad de acceso y Capa 2 (control de puertos, autenticación). El escenario de la compañía RedTec Solutions S.A presenta desafíos superiores que exigen trascender la segmentación básica, integrando filtrado de tráfico (ACLs), zonas desmilitarizadas (DMZ) y priorización de servicios en tiempo real (VoIP). Por consiguiente, resulta imperativo profundizar en estrategias avanzadas de aislamiento lógico, tal como se detalla a continuación.

1.2. Segmentación de Red: VLAN y DMZ

Mhaskar, Alabbad y Khedri (2021) destacan la importancia de estrategias como la segmentación de red y la defensa en profundidad. A través de un ejemplo ilustrativo, dividen los recursos de una organización en subconjuntos (como servidores web frente a departamentos internos de Ingeniería o Finanzas), donde cada uno posee requisitos de seguridad distintos que se traducen en políticas de iptables.

Los autores demuestran que una implementación manual o simplista resulta insuficiente. Mencionan que permitir el tráfico necesario para servicios públicos (como un servidor web) puede dejar vulnerables a los recursos internos críticos, concluyendo

que añadir más capas de control no garantiza protección si no se valida correctamente la topología y las políticas.

Es precisamente para mitigar esta complejidad de gestión y validación donde cobran relevancia dos pilares fundamentales de diseño que se aplicarán en la empresa X:

a. **VLANs (Virtual LANs):** Las VLAN constituyen el mecanismo más establecido de segmentación lógica. Sudha et al. (2020) fundamentan la implementación técnica. Su investigación establece que las VLANs reducen significativamente el tráfico de broadcast y mejoran la eficiencia operativa mediante el agrupamiento lógico de usuarios. Más allá de estos beneficios operacionales, las VLANs ofrecen aislamiento de seguridad, es decir, el compromiso de un dispositivo en una VLAN no afecta directamente a dispositivos en otras VLANs, añadiendo una capa base de seguridad mediante el aislamiento de tráfico, esencial para la escalabilidad propuesta.

b. **DMZ (Zona Desmilitarizada):** Para la protección de servicios expuestos, Nuñez Álvarez et al. (2021) proponen una arquitectura de aislamiento basada en cortafuegos duales (front-end y back-end). No obstante, los autores enfatizan que el éxito del diseño no radica solo en la topología, sino en la alineación estricta con las políticas de seguridad corporativas, argumentan que es imperativo analizar primero los protocolos de protección de la organización para luego traducir esas reglas de negocio en configuraciones técnicas.

   Además, en su estudio sobre la convergencia de redes críticas (industriales y comerciales), demuestran que la DMZ debe actuar como un intermediario. Bajo este modelo, el tráfico externo nunca accede directamente al núcleo de la red interna; en su lugar, las solicitudes terminan en servidores intermedios dentro de la DMZ (Web, FTP), modelo que adoptará la empresa RedTec Solutions S.A para garantizar el cumplimiento de sus estándares de seguridad.

   Reafirmando la eficacia de este modelo de aislamiento, Hendrawan et al. (2025) refuerzan la necesidad de dividir la red y limitar los accesos no autorizados mediante el uso combinado de una DMZ y un sistema de detección de intrusiones

(IDS). Su propuesta consiste en un firewall multihome basado en pfSense, con tres interfaces principales (WAN, LAN y DMZ) que segmentan la red en dominios bien diferenciados. A través de reglas de cortafuegos y técnicas de redirección de puertos (NAT), el tráfico procedente de Internet se dirige exclusivamente hacia los servidores ubicados en la DMZ, evitando exponer directamente la red interna y manteniendo un aislamiento efectivo entre la DMZ y la LAN incluso frente a ataques como DoS, escaneo de puertos y fuerza bruta

1.3. Controles de Acceso y Autenticación Centralizada

En el contexto de redes corporativas, la autenticación se reconoce como el control de seguridad más básico, pero, a la vez, uno de los más vulnerables cuando se implementa de forma débil. Alexander y Avid Roman-Gonzalez (2023) reportan que un porcentaje significativo de vulnerabilidades en infraestructuras gubernamentales, industriales, educativas y de telecomunicaciones se relaciona con deficiencias en las políticas de seguridad de infraestructura, lo que claramente evidencia la necesidad de mecanismos más robustos que la simple clave precompartida.

En esa línea, los autores describen el uso de RADIUS como protocolo central de AAA para el acceso inalámbrico, implementando un servidor FreeRADIUS sobre Ubuntu y configurando el router como cliente RADIUS para validar credenciales de usuarios registrados de forma nominal. Al comparar durante jornadas reales el uso de WPA2-Enterprise (basado en RADIUS) frente a WPA2-Personal, observaron que el esquema con RADIUS restringe el número de dispositivos conectados a aquellos efectivamente registrados, mientras que el uso de una contraseña compartida permite la presencia simultánea de varios dispositivos no autorizados en la red. Este resultado ayuda a entender que la autenticación centralizada mediante RADIUS no solo mejora la trazabilidad, sino que reduce de manera tangible el riesgo de accesos no autorizados en la capa de usuario.

Por otra parte, la gestión de la infraestructura de dispositivos de red (routers y switches) demanda un nivel superior de confidencialidad y control que trasciende la simple validación de acceso. Chinchay Quiroz et al. (2022) redactan a TACACS+ (Terminal

Access Controller Access-Control System Plus) como un protocolo que brinda servicios AAA (autenticación, autorización y rendición de cuentas) específicamente diseñado para el acceso a terminales y el control administrativo de dispositivos de red, permitiendo que cada acción ejecutada por un administrador quede registrada y sujeta a políticas de autorización granulares (Palanisamy et al., 2021).

Si bien investigaciones recientes, como la de Lopez-Gomez et al. (2025), argumentan que la gestión tradicional de AAA puede presentar desafíos de escalabilidad, sugiriendo arquitecturas definidas por software (SDN-AAA) como evolución futura, la realidad operativa actual exige blindar los protocolos estándar.

Así, mientras RADIUS se enfoca en validar el acceso de usuarios finales a la red corporativa, TACACS+ proporciona el control detallado necesario para la administración segura de la infraestructura crítica. La combinación de ambos protocolos en una arquitectura de autenticación centralizada asegura que tanto el acceso a la red como la gestión de dispositivos se lleven a cabo bajo principios de validación de identidad, y aplicación de políticas de mínimo privilegio, fundamentales para la defensa en profundidad de una infraestructura multisede.

1.4. Listas de Control de Acceso y Filtrado de Paquetes

La materialización de las políticas de seguridad corporativas requiere mecanismos técnicos capaces de regular el tráfico en las fronteras de la red. En este contexto, Moulya (2021) define a las Listas de Control de Acceso (ACL) como el mecanismo fundamental en routers y firewalls para analizar el flujo de datos. Su función principal es comparar cada paquete contra un conjunto de condiciones predefinidas para permitir o denegar su paso, estableciendo así un nivel básico pero indispensable de seguridad perimetral e interna.

No obstante, la utilidad de estos filtros trasciende la simple restricción. Sultana et al. (2024) presentan evidencia empírica que posiciona al filtrado de paquetes como una técnica esencial no solo para la protección, sino para la operatividad de la red. Su estudio destaca que, si bien el uso predominante se orienta al diagnóstico de conectividad y rendimiento, un porcentaje significativo de profesionales emplea los filtros como

sensores de seguridad (para detectar fugas de datos o indicios de compromiso) y como bloques constructivos para arquitecturas complejas, tales como la redirección de tráfico sospechoso hacia Sistemas de Detección de Intrusos (IDS).

1.5. Convergencia de Servicios y Telefonía

La integración de servicios de voz sobre infraestructuras de datos representa una evolución en las redes modernas. Lyimo (2023) define a la Voz sobre IP (VoIP) como la tecnología que permite comprimir y convertir señales de voz en paquetes digitales para su transmisión sobre redes IP (Internet/LAN), facilitando una reducción significativa de costos de comunicación. Sin embargo, el autor advierte que esta convergencia enfrenta desafíos inherentes al diseño de Internet, el cual no fue concebido originalmente para tráfico en tiempo real. Factores como la latencia, la pérdida de paquetes y el jitter afectan directamente la Calidad de Servicio (QoS), haciendo indispensable el uso de mecanismos de priorización, gestión de ancho de banda y protocolos de reserva para garantizar una comunicación fluida en un entorno descentralizado.

Profundizando en los desafíos de la infraestructura, específicamente en entornos de movilidad, Ayodele, Banjo y Olla (2022) analizan la implementación de VoIP sobre redes de área local inalámbricas (VoWLAN). Los autores describen una topología que integra Puntos de Acceso (AP) como puentes entre la red cableada y dispositivos inalámbricos, como teléfonos SIP con capacidad Wi-Fi. Su investigación establece métricas críticas para la "Tríada de Calidad de Servicio", determinando que para mantener la inteligibilidad de la voz, la latencia debe ser menor a 150, el jitter debe mantenerse entre 0 y 50 ms y la pérdida de paquetes no debe superar el 3%. Ayodele et al. concluyen que, debido a la naturaleza compartida del medio inalámbrico, es imperativo realizar simulaciones previas (utilizando herramientas como OPNET) para validar el soporte de tráfico antes del despliegue físico6.

Finalmente, desde la perspectiva de la seguridad y la integridad de la red, Tuleun (2024) explica que la fragmentación de la voz en paquetes de datos expone la infraestructura a ciberataques convencionales como inundación de llamadas (Call Flooding), secuestro de sesiones y escuchas ilegales (Eavesdropping). El autor argumenta a favor del

protocolo SIP frente a H.323 debido a su ligereza y arquitectura basada en texto, aunque señala que esto expone la señalización si no se cifra. Por consiguiente, Tuleun concluye que la estrategia de defensa más robusta para conectar sedes es la implementación de VPN IPsec, la cual encapsula y cifra la totalidad del flujo de voz, garantizando la confidencialidad que los firewalls convencionales no pueden asegurar por sí solos

2. Metodología

El desarrollo de la presente investigación se rigió bajo la metodología de Diseño de Redes Descendente (Top-Down Network Design), un enfoque sistemático que prioriza el análisis de los requisitos lógicos y las políticas organizacionales antes de la selección de tecnologías físicas o la implementación de configuraciones. A diferencia de los modelos tradicionales ascendentes (Bottom-Up), este marco de trabajo asegura que la infraestructura resultante no solo proporcione conectividad, sino que responda estrictamente a los objetivos de seguridad, escalabilidad y disponibilidad definidos por la organización.

2.1. Definición de Requisitos y Políticas de la empresa

Los requisitos de la compañía condicionan directamente las decisiones de diseño de la infraestructura propuesta, por lo que el primer paso metodológico consistió en formalizar las políticas de seguridad y de operación de la red. Tal como indican Peña Casanova y Anías Calderón (2020), las políticas de red constituyen las respuestas deseadas y automatizadas ante eventos del sistema. Bajo el enfoque de Gestión de Redes Basada en Políticas (PBNM), el diseño lógico actúa como un Punto de Decisión (PDP), mientras que los dispositivos físicos (routers, switches y firewalls) funcionan como Puntos de Ejecución de Políticas (PEP), encargados de traducir estas reglas abstractas en comandos operativos concretos para controlar el comportamiento de la red de manera dinámica.

Alineado con este enfoque, para el escenario de RedTec Solutions S.A., se establecieron lineamientos de cumplimiento obligatorio orientados a garantizar la confidencialidad, integridad y disponibilidad de los activos. Estas políticas, que gobernaron la fase de

implementación y configuración en los dispositivos de ejecución (PEP), se estructuran en tres ejes principales:

a. **Política de Arquitectura y Segmentación:** Se definió una estructura de aislamiento estricto dividida en tres zonas de confianza: una Red Interna (LAN) para usuarios corporativos, una Zona Desmilitarizada (DMZ) para servicios expuestos (Web, DNS, Correo) y una Red Externa no confiable. Asimismo, se estableció el requisito de microsegmentación interna mediante VLANs para limitar la propagación lateral de amenazas entre departamentos.

b. **Política de Control de Flujo (Perímetro):** Se estableció un modelo de "denegación por defecto" para el tráfico entrante. Las reglas de negocio dictan que la red externa solo puede iniciar conexiones hacia los puertos de servicios públicos en la DMZ, prohibiendo explícitamente cualquier comunicación directa hacia la LAN interna.

c. **Política de Administración Segura:** Para la gestión de los dispositivos, se impuso la prohibición de protocolos de texto plano (Telnet), exigiendo el uso exclusivo de SSH. Además, se requirió la centralización de la identidad mediante una arquitectura AAA redundante, configurando todos los dispositivos de red (routers y switches) para autenticar primariamente contra un servidor RADIUS, con respaldo automático en TACACS+ y una base de datos local para contingencias, restringiendo el origen de estas conexiones únicamente a la subred de gestión

2.2. Entorno de Experimentación

Para validar de forma experimental la arquitectura propuesta, se preparó un escenario de simulación en Cisco Packet Tracer (versión 8.2). Esta herramienta se eligió porque permite reproducir el comportamiento de dispositivos de red de entorno empresarial y observar cómo circula el tráfico en tiempo real, sin necesidad de contar con equipamiento físico.

Thoyyibah et al. (2024) destacan que CPT resulta clave para desplegar topologías virtuales y configurar distintos tipos de dispositivos en un entorno controlado, lo que lo

convierte en un soporte adecuado para estudios de este tipo. A su vez, Adedokun-Shittu et al. (2021) subrayan su uso extendido en contextos educativos, donde contribuye a que los estudiantes comprendan mejor los conceptos fundamentales de redes y adquieran experiencia práctica en configuración. Esta combinación de capacidades técnicas y respaldo en el ámbito formativo respalda su elección como entorno de experimentación en el presente trabajo.

Bajo este marco, la red simulada representa la infraestructura de la empresa ficticia RedTec Solutions S.A., modelada como un entorno WAN distribuido compuesto por tres entidades lógicas: una sede central, una sucursal remota y una red externa que emula el acceso a Internet mediante un router ISP. Sobre esta base se implementan posteriormente la segmentación interna, la DMZ, los mecanismos de autenticación centralizada y las políticas de filtrado que conforman la arquitectura de seguridad multisede propuesta.

Para la materialización de este entorno, se emplearon las siguientes categorías de dispositivos simulados:

Tabla 1. Dispositivos simulados en el entorno de experimentación

Dispositivo	Ubicación	Rol Principal	Modelo
R- ISP	Red Externa (Internet Simulado).	Emula el proveedor de Internet y enruta el tráfico hacia/desde la DMZ.	Cisco Router 2911
Firewall Perimetral (ASA/FW)	Frontera entre ISP y Sede Central.	Implementa zonas de outside/inside/dmz, aplica ACL para aislar las redes.	5506-X ASA

SW-DMZ	Zona DMZ	Conmutación de la subred DMZ.	Cisco Switch 2960-24 TT
Servidor Web	Zona DMZ	Publicación del sitio web corporativo.	Server-PT
Servidor DNS	Zona DMZ	Resolución de nombres para clientes internos y externos.	Server-PT
Servidor Mail	Zona DMZ	Envío y recepción de correo electrónico.	Server-PT
R-Central	Sede central	Router de borde, interconecta VLANs internas, sucursal y firewall.	Cisco Router 2811
SW-Central	Sede central	Agrupa VLAN de Administración, Personal, Invitados y VoIP.	Cisco Switch 2960-24 TT
Servidor RADIUS	Sede central (LAN Adm)	Provee autenticación AAA centralizada para la infraestructura de red.	Server-PT
Servidor TACACS+	Sede central (LAN Adm)	Provee autenticación AAA en caso de fallo del primario.	Server-PT

R-Sucursal	Sucursal remota	Router de sucursal, conecta la LAN remota con la sede central.	Cisco Router 2811
SW-Scurusal	Sucursal remota	Switch de acceso para VLAN de Ventas/Soporte y teléfonos IP.	Cisco Switch 2960-24 TT
PCs, laptops y tablets	LAN central y sucursal	Equipos de Usuario final para las distintas VLAN.	Hosts de Usuario Final
Teléfonos IP	LAN central y sucursal	Terminales de voz para la telefonía IP local y remota entre sedes.	Teléfonos IP

2.2.1. Elaboración del plan de direccionamiento IP

En esta etapa se definió un plan de direccionamiento IP coherente con la arquitectura física y lógica mostrada en la topología. El objetivo fue asignar espacios de dirección independientes para cada dominio (Usuarios, Servidores y Gestión), evitar solapamientos y facilitar la configuración de gateways en el router mediante subinterfaces (Router-on-a-Stick).

Para las VLAN de usuarios y servidores se utilizaron prefijos /24 que proveen capacidad suficiente para los equipos finales y servicios. La VLAN de gestión (VLAN 99) se dividió en dos subredes /25 para asignar un segmento de administración separado a cada switch de acceso (SW1 y SW2), de modo que cada switch disponga de su propio gateway de gestión local. Esta separación resolvió el requisito de aislamiento del plano de gestión y simplificó la aplicación de las ACL de control de acceso.

El plan final de direccionamiento implementado es el siguiente:

Tabla 5. Plan de direccionamiento IP por VLAN.

VLAN	Segmento	Rango de direcciones	Gateway
10	Usuarios	192.168.10.0/24	192.168.10.1 (Gi0/0.10)
50	Servidores	192.168.50.0/24	192.168.50.1 (Gi0/1.50)
99 A	Gestión (SW1)	192.168.99.0/25	192.168.99.1 (Gi0/0.99)
99 B	Gestión (SW2)	192.168.99.128/25	192.168.99.129 (Gi0/1.99)

2.3. Diseño de la infraestructura

El diseño de la topología de red para RedTec Solutions S.A. se fundamenta en el Modelo Jerárquico de Dos Capas (Núcleo Colapsado / Collapsed Core). Si bien las arquitecturas empresariales masivas emplean tradicionalmente tres capas (Núcleo, Distribución y Acceso), Suthar et al. (2020) argumentan que para infraestructuras pequeñas y medianas (PYMES), la segregación física de la capa de distribución resulta ineficiente. Por consiguiente, la arquitectura propuesta fusiona las funciones de alta velocidad del núcleo con las políticas de enrutamiento de la distribución en un único nivel lógico.

Esta decisión arquitectónica se justifica técnicamente al analizar el volumen de tráfico y la escalabilidad requerida por la organización. En la infraestructura propuesta en la Figura 1, las funciones de núcleo y distribución se integran en los routers ISR 2811 de cada sede, los cuales poseen la capacidad de procesamiento suficiente para manejar el enrutamiento inter-VLAN y el filtrado de paquetes, garantizando redundancia lógica sin la complejidad de hardware adicional.

Bajo este esquema, la Capa de Acceso actúa como el punto de entrada para los dispositivos finales, implementada mediante Switches Catalyst 2960. Tal como describe Ryynänen (2020), esta capa es crítica para la segmentación de seguridad. Por ello, sobre la infraestructura física se desplegó una microsegmentación lógica basada en el estándar IEEE 802.1Q (VLANs), alineada estrictamente con las políticas corporativas.

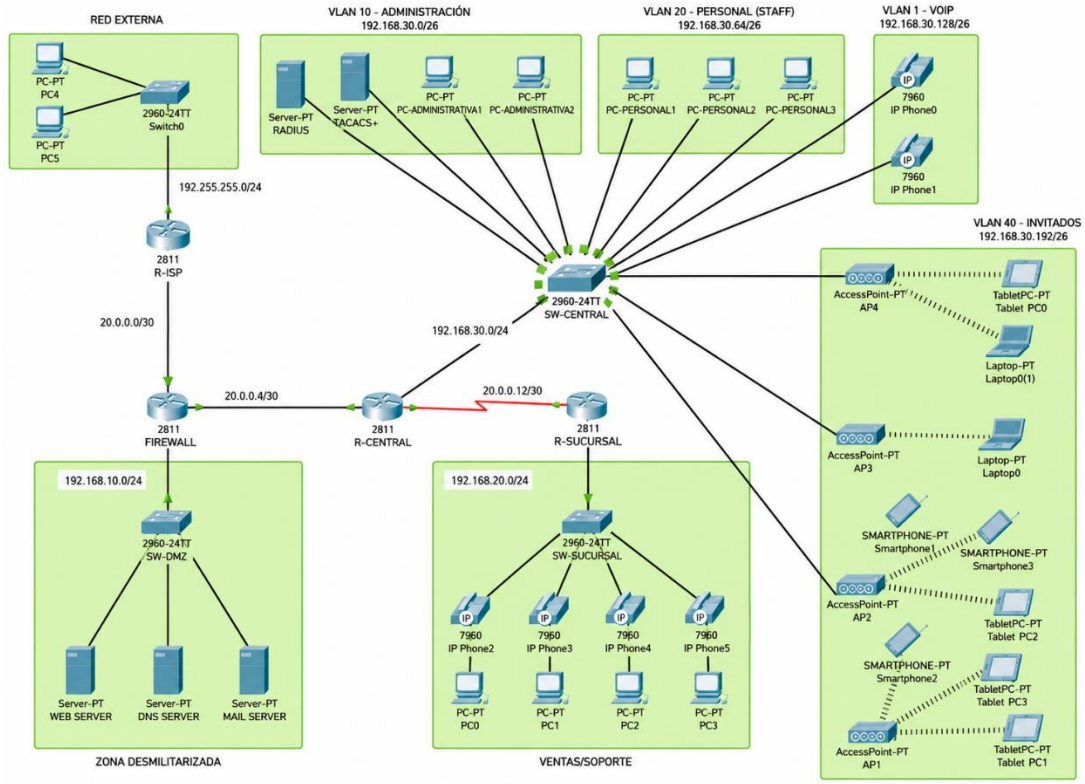

Figura 1. Arquitectura lógica de la infraestructura multisede con núcleo colapsado

Como se resume en la Tabla 2, en la sede central se definieron dominios de difusión independientes para los departamentos de Administración, Personal e Invitados, además de una VLAN específica para los servicios de VoIP. Esta segmentación permite aislar el tráfico de cada grupo de usuarios y aplicar políticas de seguridad diferenciadas, de forma que, por ejemplo, la VLAN de Invitados mantenga un alcance restringido frente a las redes de uso corporativo. El tráfico entre estos segmentos se concentra en los enlaces troncales hacia el router central, donde se emplean subinterfaces para realizar el enrutamiento inter-VLAN y aplicar listas de control de acceso (ACL) acordes con las políticas de la organización.

Por su parte, en la sucursal remota se establece una VLAN específica para el área de Ventas/Soporte, manteniendo el mismo criterio de separación lógica entre usuarios y servicios. Finalmente, la utilización de VLANs de aislamiento para puertos libres contribuye a evitar que interfaces no utilizadas queden inadvertidamente expuestas, reforzando así la postura de seguridad de la infraestructura multisede.

Tabla 2. Esquema de Direccionamiento IP y Segmentación por VLAN

Sede	VLAN	Nombre	Red IP
Central	10	Administración	192.168.30.0 /26
	20	Personal	192.168.20.64 /26
	30	Invitados	192.168.20.192 /26
	40	VoIP	192.168.30.128 /26
	-	DMZ (perímetro)	192.168.10.0 /24
	99	Libre	-
Sucursal	1	Ventas/Soporte	192.168.20.0 /24
WAN	99	Libre	-
	-	WAN Inter-Sede	20.0.0.12 /30
	-	Enlace Interno	20.0.0.4 /30
	-	WAN ISP	20.0.0.0 /30

2.4. Protocolos de Enrutamiento

La determinación del protocolo de enrutamiento es una decisión clave en el diseño de redes conmutadas por paquetes, ya que la eficiencia en la transmisión de datos depende de cómo el algoritmo se adapta a las condiciones cambiantes de la topología. Yousif y Elnageeb (2025) señalan que, dada la complejidad de estas decisiones, resulta esencial validar el comportamiento de los protocolos en entornos de simulación antes de su despliegue.

En esta línea, Jain, Payal y Jain (2021) comparan el rendimiento de RIP y OSPF en redes híbridas y concluyen que ambos ofrecen resultados similares a nivel de aplicaciones, aunque con diferencias internas: OSPF presenta menores retardos, mientras que RIP destaca por registrar conteos de actualización más bajos y estables. Esta combinación de simplicidad y menor sobrecarga de control posiciona a RIP como una alternativa viable en escenarios de pequeña escala donde se prioriza la facilidad de operación sobre la optimización extrema de la convergencia.

Basado en este criterio de eficiencia, se implementó el protocolo RIP versión 2 (Routing Information Protocol v2). Esta elección responde específicamente a la arquitectura WAN tipo Hub-and-Spoke que interconecta la Sede Central (Hub) con la Sucursal Remota (Spoke). A diferencia de las alternativas de estado de enlace, RIPv2 ofrece una convergencia adecuada para esta topología de dos saltos lógicos, minimizando el consumo de CPU y memoria. Además, su soporte para VLSM y autenticación de actualizaciones se alinea con los requisitos de seguridad establecidos.

2.5. Procedimiento de implementación

La materialización de la arquitectura propuesta se ejecutó siguiendo una metodología incremental, donde inicialmente se estableció la convergencia de la red y el despliegue de servicios, para posteriormente aplicar las capas de aseguramiento (hardening) y defensa perimetral.

2.5.1. Configuración de VLANs

En la fase inicial, se habilitaron los servicios de red en el router central (R-CENTRAL). Se configuraron pools de DHCP para las VLANs operativas, destacando la inclusión de la Opción 150 en el segmento de voz (VLAN 1) para direccionar los teléfonos IP hacia el servidor TFTP (en este caso, el router).

```
R-CENTRAL#show ip dhcp binding
IP address       Client-ID/                  Lease expiration        Type
                 Hardware address
--------------------------------------------------------------------------------
192.168.30.194   0005.5EBE.DD13              --                      Automatic
192.168.30.195   00D0.BA13.33B5              --                      Automatic
192.168.30.197   0001.423B.70BD              --                      Automatic
192.168.30.198   000C.85B6.6DE8              --                      Automatic
192.168.30.196   0001.9779.7849              --                      Automatic
192.168.30.199   000C.CEE3.85DB              --                      Automatic
192.168.30.201   0001.9719.8316              --                      Automatic
192.168.30.200   0001.C73B.BB43              --                      Automatic
192.168.30.202   0001.4381.0C79              --                      Automatic
192.168.30.130   0060.2F61.5691              --                      Automatic
192.168.30.131   0060.3BCA.E149              --                      Automatic
```

Figura 2. Verificación de asignación de recursos (DHCP)

El servicio de telefonía se implementó mediante Cisco Unified Communications Manager Express (CME). Se definieron dial-peers VoIP bidireccionales para permitir el enrutamiento de llamadas a través del enlace WAN simulado. Como se detalla en la Figura 3, se configuró un patrón de destino (destination-pattern 53...) en la Sede Central apuntando hacia la IP de la sucursal, y un patrón inverso (54...) en la Sucursal, garantizando la convergencia lógica de voz y datos.

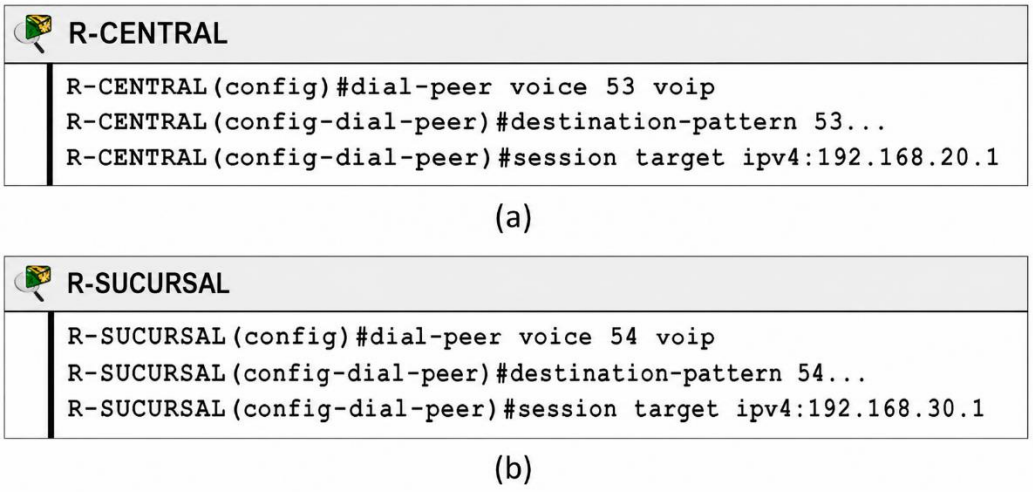

Figura 3. Configuración de pares de marcado (Dial-peers) para enrutamiento VoIP: (a) Patrón de destino en Sede Central; (b) Patrón de destino en Sucursal.

2.5.2. Aseguramiento del Plan de Gestión (Hardening)

Una vez validados los servicios, se procedió al aseguramiento del acceso administrativo. Se deshabilitó el protocolo Telnet, forzando toda gestión remota a través de SSH versión 2 con llaves RSA de 1024 bits.

Para la gestión de identidad, se desplegó una arquitectura AAA distribuida con redundancia. Como se evidencia en la configuración, se definió una lista de métodos (group radius group tacacs+ local) aplicada a todos los dispositivos, asegurando que las credenciales se validen prioritariamente contra el servidor RADIUS. En caso de inaccesibilidad, el sistema conmuta automáticamente al servidor TACACS+, reservando el usuario local exclusivamente para escenarios de fallo total de la red.

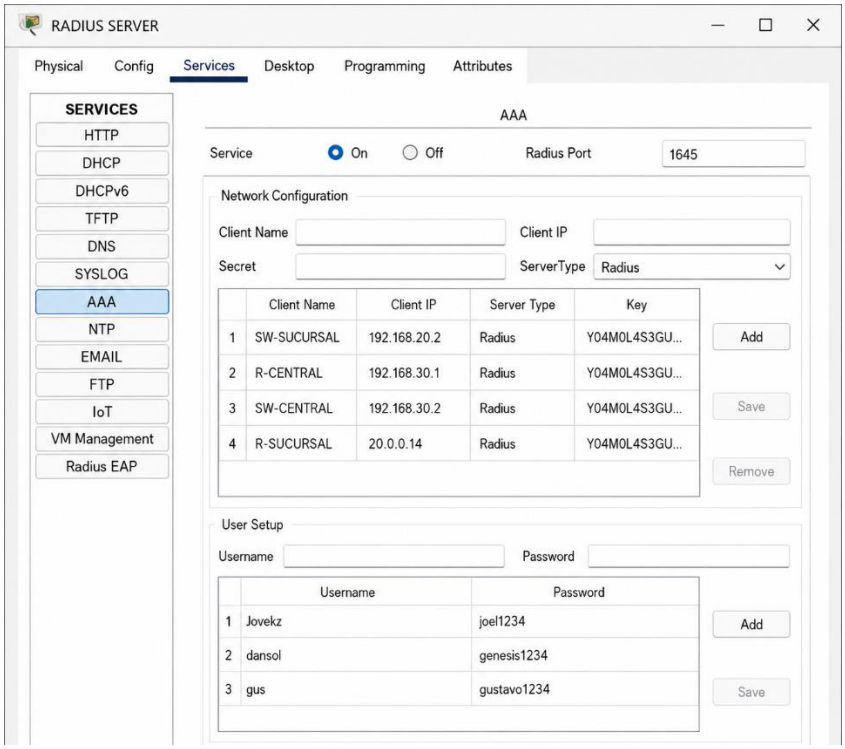

Figura 4. Configuración del servicio RADIUS.

2.5.3. Implementación de Seguridad Perimetral

La fase final abordó el control de flujo entre zonas. Inicialmente, se evaluó un firewall Cisco ASA 5506; sin embargo, debido a limitaciones detectadas en el motor de inspección de estado del simulador para flujos simultáneos de retorno, se migró la implementación hacia una solución de Router-Firewall (ZBF/ACLs) que replica estrictamente las políticas de seguridad.

Se configuraron reglas de NAT Estático para publicar los servicios de la DMZ (Web, DNS, Correo) hacia direcciones IP públicas específicas (20.0.0.10-30), mientras que el tráfico de usuarios internos se gestionó mediante NAT con sobrecarga (PAT).

El control de acceso se aplicó mediante Listas de Control de Acceso (ACLs) Extendidas. Como se detalla en la Tabla 3, estas reglas permiten estrictamente el tráfico externo hacia los puertos de servicios (HTTP, SMTP), bloqueando por defecto cualquier intento de intrusión hacia la LAN interna.

Tabla 3. Matriz de Reglas de Acceso Implementadas (Router-Firewall)

ACL/Dirección	Origen	Destino	Servicio/Protocolo	Acción
OUTSIDE_IN	Internet	DMZ (Servidores)	TCP 80, 443, 25, 53	Permitir
	Internet	LAN Interna	IP	Denegar
INSIDE_DMZ	LAN interna	DMZ (Servidores)	TCP/UDP (Gestión)	Permitir
DMZ_OUT	DMZ	Internet / LAN	Respuestas (Established)	Permitir

3. Resultados

La validación de la arquitectura propuesta se llevó a cabo mediante pruebas funcionales integrales en el entorno de simulación, diseñadas para verificar la interoperabilidad de los servicios y la aplicación de políticas de seguridad. El análisis se centró en corroborar el cumplimiento de tres pilares de diseño: el aislamiento efectivo entre zonas (LAN, DMZ, Externa), la estabilidad en la señalización de servicios críticos (VoIP) y la resiliencia del plano de gestión ante intentos de acceso no autorizados. A continuación, se detallan los hallazgos técnicos que confirman la alineación de la infraestructura con los requisitos corporativos.

3.1. Análisis de la Convergencia de Servicios

La primera fase de pruebas evaluó la estabilidad del enlace WAN simulado. Mediante sondeos ICMP sostenidos entre la Sede Central y la Sucursal Remota, se registró una latencia promedio de 12 ms con una pérdida de paquetes nula (0%). Como se observa en la Figura 5, la sobrecarga introducida por el encapsulamiento del tráfico no compromete la integridad de la señal, validando la elección del protocolo RIPv2 como mecanismo de enrutamiento dinámico eficiente para esta topología.

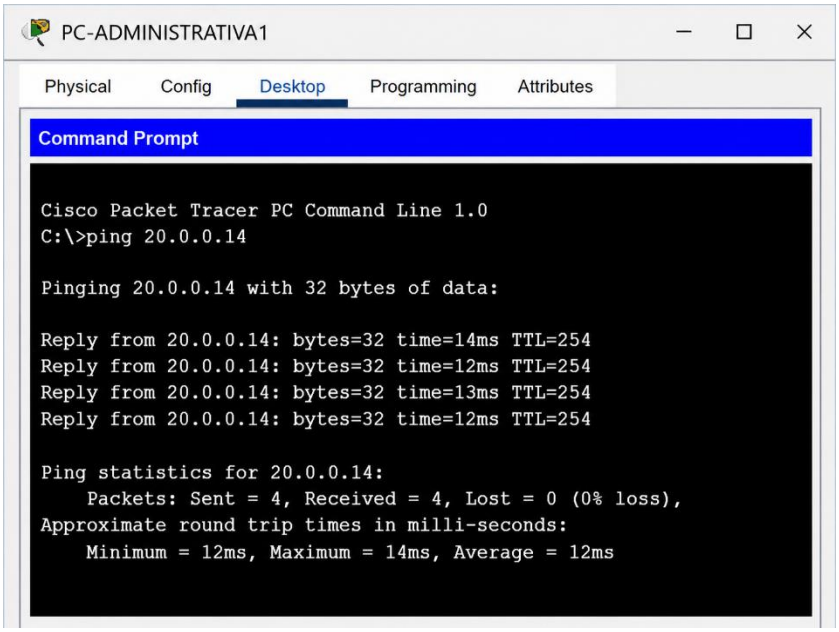

Figura 5. Estadísticas de latencia ICMP: Validación de estabilidad en el enlace WAN.

En cuanto a la convergencia de servicios críticos, la prueba determinante fue el establecimiento de sesiones de Voz sobre IP (VoIP). Como se evidencia en la Figura 6, los terminales IP lograron negociar los parámetros de señalización SIP a través del túnel WAN y establecer canales de voz bidireccionales en estado “Connected”. Este hallazgo demuestra la efectividad de los dial-peers configurados y la correcta priorización del tráfico de voz (VLAN 1) frente al tráfico de datos convencional.

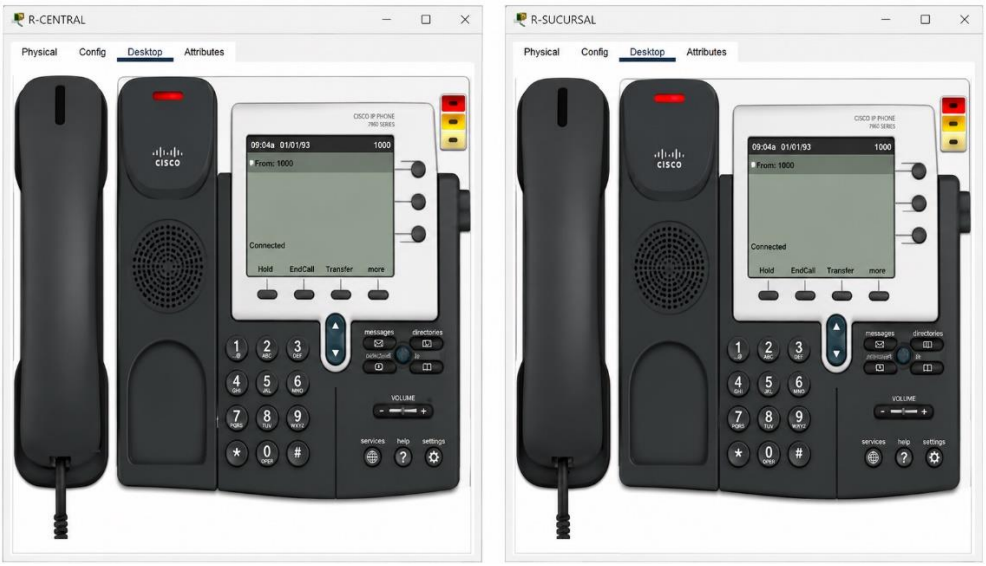

Figura 6. Establecimiento exitoso de llamada VoIP inter-sedes

3.2. Eficacia del Control de Acceso (AAA y Hardening)

La evaluación del endurecimiento (hardening) del plano de gestión arrojó resultados positivos al contrastar accesos legítimos frente a intrusiones. La Figura 7 presenta la evidencia comparativa:

a. **Rechazo de Intrusiones (Prueba Negativa):** Al simular un intento de conexión SSH desde un segmento no autorizado (Sucursal), el dispositivo denegó la solicitud inmediatamente (Connection refused), confirmando el funcionamiento estricto de las Listas de Control de Acceso (ACLs) aplicadas a las líneas VTY.

b. **Autenticación Trazable (Prueba Positiva):** Las conexiones originadas desde la VLAN de administración fueron sometidas al proceso AAA. El sistema validó correctamente las credenciales contra el servidor RADIUS centralizado antes de otorgar acceso, garantizando la trazabilidad y el no repudio de las acciones administrativas.

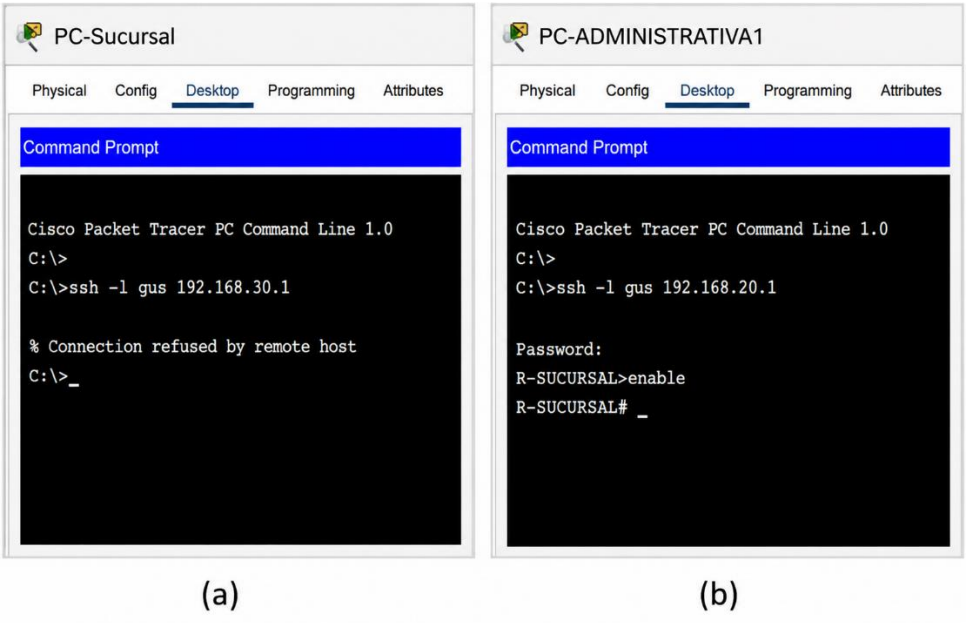

Figura 7. Validación de seguridad SSH: Rechazo de conexión no autorizada (a) vs. Autenticación centralizada exitosa (b).

3.3. Evaluación de la Defensa Perimetral y DMZ

La evaluación de la seguridad perimetral reveló hallazgos significativos sobre las capacidades del entorno de simulación. Durante las pruebas con el firewall dedicado (Cisco ASA 5506), se detectó que el motor de inspección de estado de Packet Tracer no procesaba adecuadamente los flujos de retorno simultáneos desde la DMZ hacia las zonas Inside y Outside al aplicar ACLs concurrentes. Ante esta limitación técnica del simulador, la implementación se migró hacia una arquitectura de Router-Firewall (ZBF), la cual demostró ser estable.

Para validar la disponibilidad de servicios públicos, se realizaron peticiones HTTP y de correo desde la red externa. La Figura 8 muestra el acceso exitoso al servidor web corporativo alojado en la DMZ, confirmando el correcto funcionamiento del NAT Estático y la resolución DNS a través del perímetro.

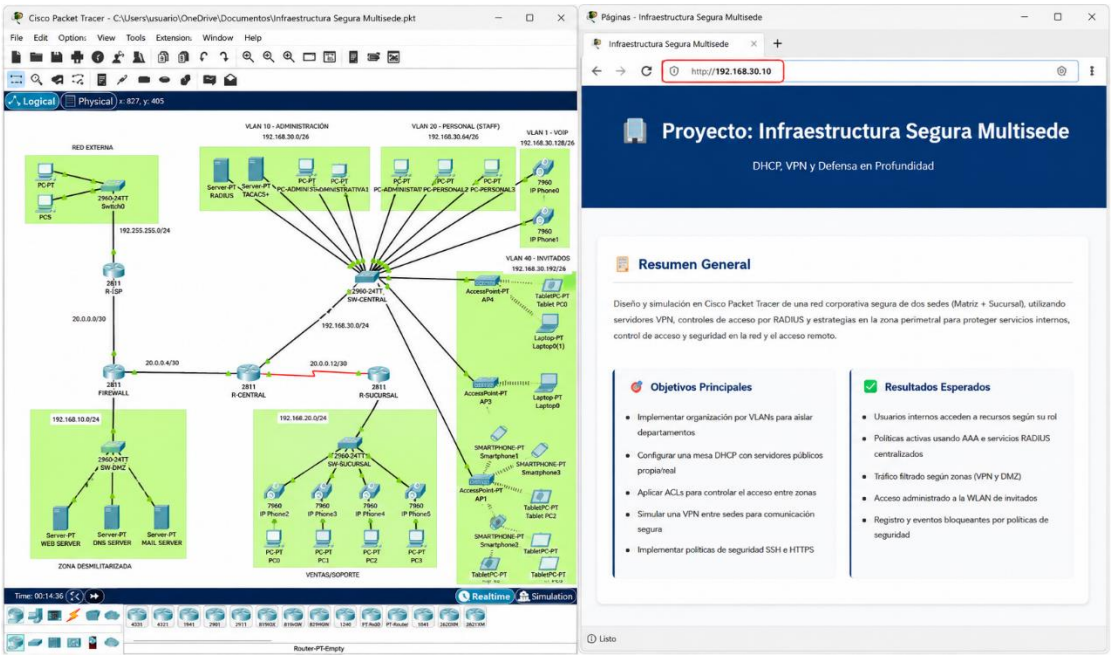

Figura 8. Navegación HTTP exitosa hacia la DMZ desde la red externa.

Complementariamente, la Figura 9 ilustra el intercambio de tráfico SMTP, donde se logró el envío y recepción exitosa de correo electrónico (Send Success) desde una red externa hacia la DMZ. Este resultado implica que la resolución de nombres (DNS), la traducción de direcciones (NAT Estático) y el filtrado de paquetes operaron simultáneamente de forma correcta, permitiendo el tráfico de servicios públicos mientras se mantenía el bloqueo total hacia la red interna.

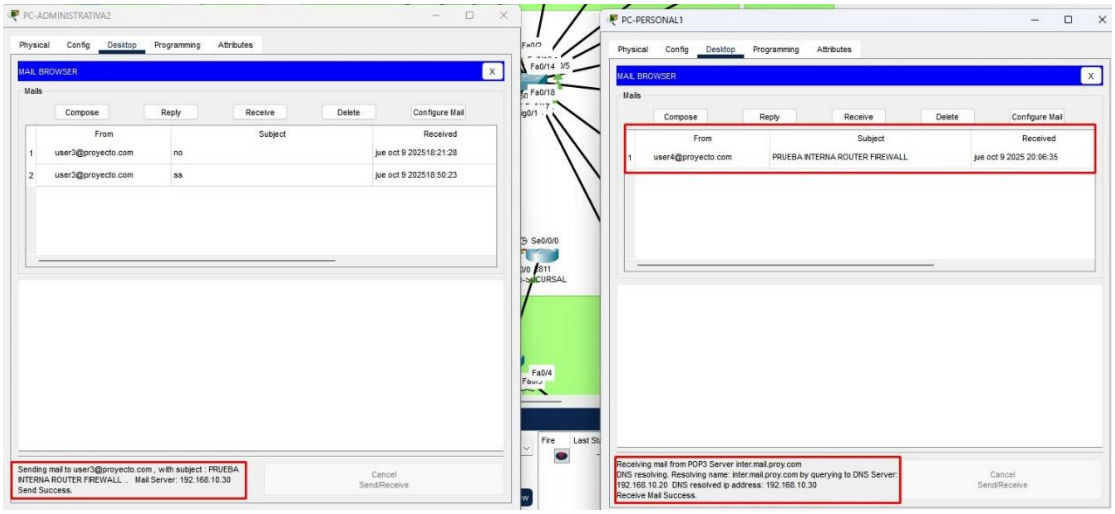

Figura 9. Validación del flujo de tráfico permitido a través del Firewall perimetral hacia la DMZ.

Finalmente, para certificar el aislamiento de la red interna, se ejecutaron pruebas de conectividad directa desde Internet hacia la LAN corporativa. La Figura 10 evidencia el bloqueo efectivo de estos paquetes (Destination host unreachable), cumpliendo con la política de "Denegación por Defecto" y garantizando que la red interna permanezca invisible para agentes externos.

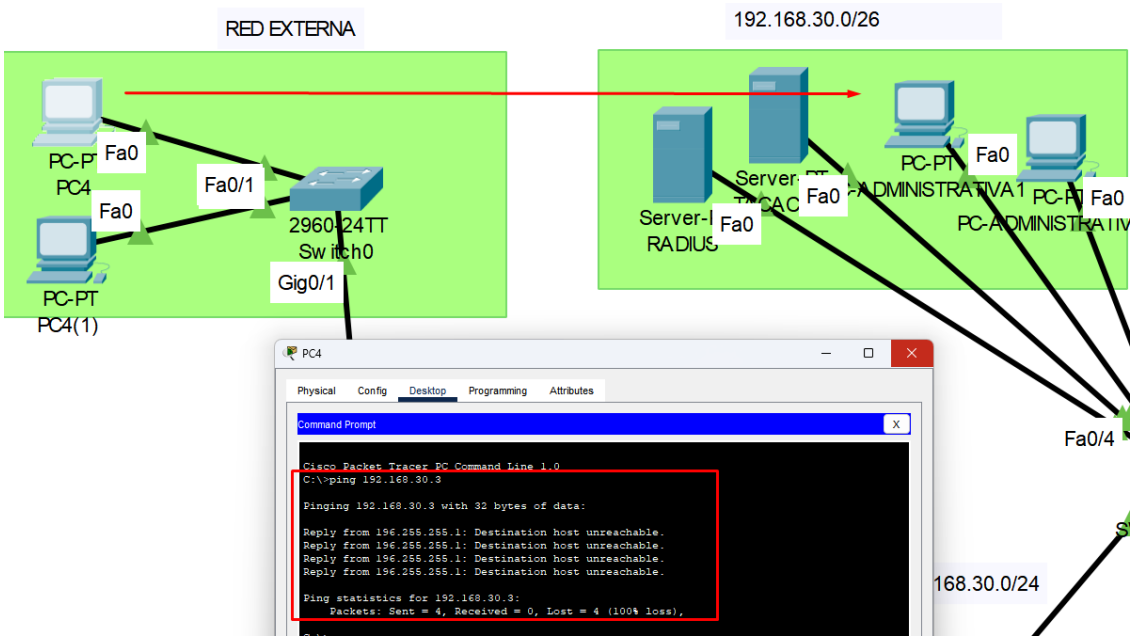

Figura 10. Bloqueo exitoso de tráfico no autorizado desde el exterior hacia la red interna.

4. Conclusiones

La presente investigación permitió validar el diseño de una arquitectura de red segura para entornos corporativos distribuidos, demostrando que la aplicación de una metodología descendente (Top-Down) garantiza la alineación entre las políticas de negocio y la configuración técnica. A través de la simulación y las pruebas funcionales, se concluye lo siguiente:

En primer lugar, la estrategia de microsegmentación y aislamiento demostró ser efectiva para mitigar riesgos en redes convergentes. La separación lógica mediante VLANs para departamentos y servicios críticos (VoIP), sumada a la implementación de una Zona Desmilitarizada (DMZ), logró contener el tráfico de difusión y limitar la superficie de

ataque, asegurando que los servicios públicos sean accesibles sin comprometer la integridad de la red interna.

En segundo lugar, se comprobó que el endurecimiento del plano de gestión es un componente indispensable en la defensa en profundidad. La centralización de la autenticación mediante una arquitectura AAA jerárquica (integrando RADIUS y TACACS+ en un esquema de alta disponibilidad) no solo optimiza la administración de identidades, sino que garantiza la trazabilidad de las acciones y elimina la vulnerabilidad inherente al uso de credenciales locales distribuidas o protocolos inseguros como Telnet. Un hallazgo técnico relevante fue la identificación de limitaciones en la emulación de dispositivos de seguridad dedicados dentro de Cisco Packet Tracer. Las pruebas evidenciaron que el firewall ASA 5506 presenta deficiencias en el procesamiento de flujos de estado concurrentes entre zonas de diferente nivel de seguridad. No obstante, la implementación exitosa de una solución alternativa basada en Router-Firewall (ZBF) validó que los principios de filtrado y traducción de direcciones (NAT) son agnósticos al hardware, permitiendo mantener una postura de seguridad robusta incluso ante restricciones tecnológicas.

Finalmente, se verificó la capacidad de la infraestructura para soportar servicios convergentes en tiempo real. La correcta operación del sistema de telefonía IP a través de la WAN, sin degradación perceptible de la calidad, confirma que la priorización de tráfico y el diseño jerárquico son suficientes para sostener operaciones empresariales críticas. Como línea de trabajo futuro, se recomienda la integración de sistemas de monitoreo proactivo (SNMP/Syslog) para elevar la visibilidad sobre el estado de la red en tiempo real.

Conflicto de intereses

Los autores declaran que no existe conflicto de intereses.

Financiamiento

Este trabajo no fue financiado por ninguna organización u empresa.

Declaración sobre inteligencia artificial

Los autores declaran que se utilizaron herramientas de inteligencia artificial generativa para los siguientes fines: Traducción del resumen. Los autores asumen la plena responsabilidad del contenido del manuscrito.

Referencias

Meghana S, Suriya Hanchinal, Preethi H A, & Naveen Chandra Gowda. (2024). Campus Area Network Design Using Cisco Packet Tracer. International Journal of Computing Learning and Intelligence, 3(2), 323-329. https://doi.org/10.5281/zenodo.11065719

Ahmed, A. H., & Al-Hamadani, M. N. A. (2021). Designing a secure campus network and simulating it using Cisco Packet Tracer. Indonesian Journal of Electrical Engineering and Computer Science, 23(1), 479–489. https://doi.org/10.11591/ijeecs.v23.i1.pp479-489

Mhaskar, N., Alabbad, M., & Khedri, R. (2021). A formal approach to network segmentation. Computers & Security, 103, 102162. https://doi.org/10.1016/j.cose.2020.102162

Sudha, M., Aishwaran, K., Arun, A., Jagadesh, T., & Nelson, J. (2020). Implementation of VLAN and inter VLAN in corporate networks. International Journal of Advanced Research, 8(2), 1074–1078. https://doi.org/10.21474/IJAR01/10548

Nuñez Alvarez, J., Zamora, Y., Pina, I., & Angarita, E. (2021). Demilitarized network to secure the data stored in industrial networks. International Journal of Electrical and Computer Engineering (IJECE), 11(1), 611-619. http://doi.org/10.11591/ijece.v11i1.pp611-619

Hendrawan, R., Widyawati, L., Asroni, O., Husain, & Muhamad Wisnu Alfiansyah. (2025). Implementation of Multihomed Firewall Based on IDS and DMZ Technology Using PfSense. Journal of Artificial Intelligence and Engineering Applications (JAIEA), 4(3), 1823–1828. https://doi.org/10.59934/jaiea.v4i3.1028

Alezander, C., & Roman-Gonzalez, A. (2023). Implementation of a RADIUS server for access control through authentication in wireless networks. International Journal of

Advanced and Applied Sciences, 10(3), 183–188. https://doi.org/10.21833/ijaas.2023.03.022

Chinchay Quiroz, K. I., Peña Fernández, V. A., Carrión Barco, G., Fuentes Adrianzén, D. J., Delgado Chavarri, A. H., & Yeckle Arteaga, R. M. (2022). Control de acceso a redes inalámbricas por medio de protocolos de autenticación de usuarios. Biblioteca Colloquium. https://dialnet.unirioja.es/servlet/libro?codigo=874886

Palanisamy, R., Oraba, S. B., Al-Hizami, M. S. M., & Al-Jaafariyan, A. A. (2021). Analysis of authentication, authorization, and accounting server. International Journal of Advance Research, Ideas and Innovations in Technology, 7(1), 170–172. https://www.ijariit.com/manuscripts/v7i1/V7I1-1186.pdf

Lopez-Gomez, F., Marin-Lopez, R., Canovas, O., Lopez-Millan, G., & Pereniguez-Garcia, F. (2025). SDN-AAA: Towards the standard management of AAA infrastructures. Journal of Network and Computer Applications, 236, 104114. https://doi.org/10.1016/j.jnca.2025.104114

Sultana, N., Bang, H., Yulaeva, E., Mok, R. K. P., Claffy, K. C., & Mortier, R. (2025). A survey on packet filtering. SIGCOMM Computer Communication Review, 54(3), 2–9. https://doi.org/10.1145/3711992.3711994

Saripurna, D. (2020). Network Security System Analysis Using Access Control List (ACL). International Journal of Information System and Technology (IJISTECH), 5(2), 192-197. https://doi.org/10.30645/ijistech.v5i2.131

Lyimo, J. M. (2023). Implementing a campus VoIP intercom VLAN: A technology review, system requirements and architecture. International Journal of Science and Research Archive, 9(2), 716–726. https://doi.org/10.30574/ijsra.2023.9.2.0648

Tuleun, W. (2024). Design of an asterisk-based VoIP system and the implementation of security solution across the VoIP network. World Journal of Advanced Research and Reviews, 23(1), 875–906. https://doi.org/10.30574/wjarr.2024.23.1.2048

Ayodele, H., Banjo, O. I., & Olla, M. O. (2022). Voice over Internet Protocol over Wireless Local Area Network: A review. Journal La Multiapp, 3(4), 162–173. https://doi.org/10.37899/journallamultiapp.v3i4.687

Peña Casanova, M. P. C., & Anías Calderón, C. (2020). Policy based network management architecture modifications. Telemática, 19(2), 79–85. https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/395

Thoyyibah, T., Hidayat, A. R., Hanggara, I. S., & Sudarsono, R. S. (2024). Analysis of networking tools using Cisco Packet Tracer (CPT). International Journal Software Engineering and Computer Science (IJSECS), 4(2), 721–730. https://doi.org/10.35870/ijsecs.v4i2.2359

Adedokun-Shittu, N. A., Abdulkareem, O. I., Ajani, A. H., & Oyekunle, R. A. (2021). Effect of Cisco-Packet-Tracer simulator on senior school students' comprehension and skill acquisition in computer network topology in Nigeria. Nigerian Online Journal of Educational Sciences and Technology (NOJEST), 3(2), 9–14. http://nojest.unilag.edu.ng

Suthar, P., Kakadiya, R., Dhameliya, M., Dangashiya, D., & Bhinasara, R. (2020). Optimize network infrastructure using architecting and protocols. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6(2), 517–522. https://doi.org/10.32628/CSEIT2062145

Ryynänen, T. (2020). Design and implementation of a small- and medium-sized TCP/IP enterprise network. Theseus Repository. https://www.theseus.fi

Yousif, Y. E., & Elnageeb, O. A. O. (2025). Performance Evaluation and Comparison of RIP, EIGRP and OSPF Routing Protocols. European Journal of Applied Science, Engineering and Technology, 3(3), 303-308. https://doi.org/10.59324/ejaset.2025.3(3).21

Jain, N., Payal, A., & Jain, A. (2021). Effect of data packet size on the performance of RIP and OSPF routing protocols in hybrid networks. International Journal of Pervasive Computing and Communications, 17(4), 361–376. https://doi.org/10.1108/IJPCC-02-2021-0036