UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Vínculos

https://revistas.udistrital.edu.co/index.php/vinculos/

Revista VÍNCULOS
Ciencia, Tecnología y Sociedad
Un Enlace hacia el Futuro

Recibido: 4 de febrero 2026 / Aceptado: 15 de mayo 2026

DISEÑO E IMPLEMENTACIÓN DE UNA VPN IPSEC SITE-TO-SITE ENTRE FIREWALLS PALO ALTO Y FORTINET PARA LA INTERCONEXIÓN SEGURA ENTRE UNA ALCALDÍA Y UN BANCO CERCANO EN EL PROCESO DE RECAUDO

DESIGN AND IMPLEMENTATION OF AN IPSEC SITE-TO-SITE VPN BETWEEN PALO ALTO AND FORTINET FIREWALLS FOR SECURE INTERCONNECTION BETWEEN A MUNICIPAL GOVERNMENT OFFICE AND A NEARBY BANK IN THE REVENUE COLLECTION PROCESS

Sergio Daniel Cárdenas Sánchez A[1], Fabián Chaparro Becerra B[2]

Resumen:

Este documento establece la planificación y ejecución de una VPN IPsec Site-to-Site entre dos firewalls Palo Alto y Fortinet, y del cierre del proceso de recolección de datos entre una Alcaldía Distrital y una entidad bancaria. Se logró

determinar la problemática del cierre de la recolección de datos sin una red privada y con el riesgo de intercepción, modificación y acceso no autorizado. Se utilizó una metodología de tipo aplicada y descriptiva que abarca el análisis de requerimientos, la configuración del túnel IPsec, la validación de IKE y el análisis de desempeño. De la interoperabilidad, se logró determinar que el túnel presenta estabilidad y que el impacto de la latencia fue mínimo. Por lo tanto, la solución se considera segura en comparación con los enlaces dedicados, además de mejorar los niveles de confidencialidad, integridad y disponibilidad.

Palabras claves: VPN IPsec, seguridad de la información, firewalls, redes institucionales, recaudo financiero.

Abstract

This document outlines the planning and implementation of a site-to-site IPsec VPN between two firewalls, Palo Alto and Fortinet, and the closure of the data collection process between a District Mayor's Office and a bank. The problem of closing the data collection process without a private network, and the associated risks of interception, modification, and unauthorized access, was identified. An applied and descriptive methodology was used, encompassing requirements analysis, IPsec tunnel configuration,

IKE validation, and performance analysis. Interoperability was assessed, revealing that the tunnel is stable and that latency impacts were minimal. Therefore, the solution is considered secure compared to dedicated links, and it also improves confidentiality, integrity, and availability.

Keywords: IPsec VPN, information security, firewalls, institutional networks, financial Collection.

1. Introducción

La solución más completa es la creación de una interconexión segura mediante el diseño e implementación de una VPN IPsec site-to-site entre firewalls Palo Alto y Fortinet que permite la interconexión entre una alcaldía y un banco en el proceso de recaudo. Esta estructura provee una vía segura, de forma que el flujo de información

1 Estudiante de Especialización en Gestión de las Nuevas Tecnologías de las Comunicaciones, Universidad Santo Tomás Tunja, Boyacá, Colombia. electrónico personal e institucional e-mail: sergio.cardenass@usantoto.edu.co ORCID: https://orcid.org/0009-0001-4379-7326

2 Decano, Especialización en Gestión de las Nuevas Tecnologías de las Comunicaciones, Universidad Santo Tomás Tunja, Boyacá, Colombia. Correo electrónico personal e institucional e-mail: william.chaparro@usantoto.edu.co ORCID: https://orcid.org/0000-0002-3554-1531

entre el banco y la alcaldía, en la transferencia de datos financieros y administrativos, pueda asegurarse,

en términos de confidencialidad, integridad y autenticidad, a pesar de que la vía elegida sea una red pública. El flujo de datos es un elemento crítico y fundamental para la administración de datos sensibles de los usuarios y para el manejo y control de las transacciones monetarias.

Uno de los más importantes en este tipo de interconexiones es el método de autenticación entre pares, que en la gran mayoría de los casos es mediante pre shared keys o certificados digitales. En una interconexión entre una municipalidad y una entidad bancaria, el uso de certificados es más confiable y escalable. Esta autenticación mutua hace que los dos comunicantes, por los cuales se autorizan las comunicaciones, reduzcan prácticamente, los riesgos de spoofing y man in the middle [1].

Desde la fase de diseño, se debe abordar el diseño de la interconexión de ambas organizaciones y la determinación de los rangos y direcciones de la IP, la segmentación interna, los servicios críticos y las políticas de seguridad existentes. La capacidad de integrar sistemas de diferentes proveedores como Palo Alto y Fortinet depende de la correcta configuración de los parámetros de IPsec en cuanto a cifrado, autenticación y tiempos de vida de la asociación de seguridad (SA). Un diseño que sea detallado y meticuloso reduce el riesgo de incompatibilidad y proporciona una mayor sostenibilidad a largo plazo al túnel VPN.

El establecimiento de vínculos seguros y operativos entre espacios de trabajo de instituciones públicas y entidades financieras es uno de los retos más importantes al manejar información y datos de carácter personal y financiero. Diferentes autores han mencionado que uno de los métodos más comunes que se utilizan para proteger la información en la comunicación de datos que viajan por redes públicas es el uso de VPN en núcleos IPsec, ya que estas redes ofrecen un nivel de confidencialidad, integridad y autenticación a través de mecanismos de criptografía y de intercambio de claves seguros [2].

La implementación también debe considerar políticas de enrutamiento, sean estáticas o dinámicas, que sean compatibles con la VPN. Esto permite asegurarse de que el tráfico dirigido a los sistemas de recolección viaje solo por el túnel seguro y encriptado, y que no lo hagan por rutas inseguras. Una mejor definición de inter acciones de red evita la fuga de tráfico y controla en mayor medida el intercambio de información entre las dos partes.

Por otro lado, los estudios más recientes en el área de seguridad de redes han evidenciado que hay posibilidades de interoperabilidad entre dispositivos de diferentes fabricantes, siempre que los dispositivos de interconexión hayan sido configurados de manera previa para el uso de los protocolos IKEv2 e IPsec. Por lo tanto, en este escenario, la construcción de una VPN de tipo Site-to-Site entre un banco y una alcaldía, se convierte en una necesidad de tipo funcional, a la vez, en una exigencia normativa y una necesidad de control de riesgos en la manipulación de datos financieros [3].

2. OBJETIVOS

2.1 Objetivo General

Implementar una VPN IPsec Site-to-Site entre dispositivos Palo Alto y Fortinet que permita una conexión segura para la transmisión de datos financieros.

2.2 Objetivos Específicos

- Analizar los requerimientos técnicos y de seguridad de ambas sedes.
- Configurar los dispositivos de seguridad para establecer el túnel VPN.
- Validar la conectividad mediante pruebas técnicas y de rendimiento.

3. METODOLOGÍA

3.1. Justificación técnica de la arquitectura seleccionada

Al evaluar las alternativas de interconexión segura entre sedes, es imperativo contrastar la tecnología de VPN IPsec sobre redes públicas (Internet) frente a soluciones de redes privadas tradicionales como MPLS (Multiprotocol Label Switching). Si bien MPLS ofrece garantías de rendimiento, la implementación de túneles IPsec Site-to-Site ha ganado preeminencia debido a su flexibilidad, cifrado nativo y optimización de recursos financieros. En la Tabla 1 se exponen las diferencias técnicas y operativas clave que fundamentan la elección de una arquitectura VPN IPsec para este diseño.

Tabla 1. Comparativa técnica y operativa entre arquitecturas VPN IPsec y MPLS

Criterio	VPN IPsec	MPLS Dedicado
Seguridad	Alta (Cifrado nativo AES/SHA)	Media (Tráfico sin cifrar)
Costo	Bajo/Medio	Alto (Pago recurrente)
Despliegue	Rápido (Horas)	Lento (Semanas/Meses)
Escalabilidad	Ágil (Configuraciónlógica)	Lenta (Depende del ISP)

ISSN 1794-211 X • e-lSSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2023). pp. 91-98. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

QoS / SLA	Best-Effort (Variable)	Garantizado (Priorización)
Proveedor	Agnóstico al ISP	Vendor Lock-in

3.2 Procedimiento de implementación de la VPN IPsec

Los procedimientos que se desarrollan con respecto al establecimiento de una IPsec VPN son construidos de tal modo que, de la forma más sencilla, y al mismo tiempo de la forma más eficiente, se logre la interconexión segura y estable entre las redes de la Alcaldía y del Banco. Este procedimiento inicia con la preparación del entorno.

En este, los dispositivos Palo Alto y Fortinet deben tener conectividad a Internet, deben tener IPs asignadas y deben tener acceso administrativo para que se puedan hacer las configuraciones necesarias. Un mejor diseño en esta etapa se traduce en menores concentraciones de errores y hace más fluida la interoperabilidad entre los dispositivos.

En la fase dos se procede a la interconexión de los firewalls mediante la creación del túnel VPN IPsec y la configuración de los parámetros de autenticación, encriptación y de integridad que sean compatibles entre los dos dispositivos. Esto incluye configurar IKE y las negociaciones de las fases, los traffic selectors y las políticas de seguridad que permiten el flujo del tráfico a través del túnel. También se ejecuta la configuración de las rutas para que el tráfico a la red remota sea dirigido a la VPN.

Finalmente, el proceso incluye la validación y ajuste de la implementación a través de pruebas técnicas de conectividad del túnel y monitoreo. Se realizan pruebas de comunicación que cruzan las redes locales para verificar la encriptación del tráfico y la estabilidad de la conexión. Se realizan ajustes finos basados en los resultados, y todo el proceso se documenta para garantizar la trazabilidad y la capacidad de replicar la solución en futuros entornos institucionales.

4. RESULTADOS

4.1. Características de la topología implementada entre la alcaldía y el banco:

El análisis de las imágenes muestra que, en el caso de la Alcaldía y el Banco, la topología es la de un esquema de interconexión site-to-site sobre Internet con una VPN de tipo IPsec. Cada institución tiene un firewall que actúa como punto de terminación de dicho túnel y control de concesión de tráfico. La red interna de la Alcaldía y la red del Banco quedan aisladas y sólo pueden comunicarse a través del túnel que establecen ambos dispositivos de seguridad.

La figura 1 muestra la segmentación de las redes en la cual cada sede tiene una LAN interna, controlada por su firewall, y una WAN que les da acceso a Internet. El túnel de la VPN es construido

entre las interfaces externas de los firewalls, lo que permite que el tráfico va hacia la red remota sea encapsulado y protegido, ocultando las IPs internas. Además, la seguridad aumenta porque se limita la apertura de las puertas de acceso y se hace un control de los flujos de tráfico de manera centralizada a los dispositivos de la frontera.

En un flujo similar, la topología representa un flujo de comunicación bidireccional claramente definido entre las dos redes, permitiendo que los sistemas de recolección del alcalde se comuniquen de manera segura con los servicios del banco. La falta de dispositivos intermedios complejos reduce la latencia y los posibles puntos de fallo, mejorando así la supervisión y gestión del enlace VPN. Este diseño es adecuado para entornos donde la disponibilidad y la seguridad son de máxima importancia.

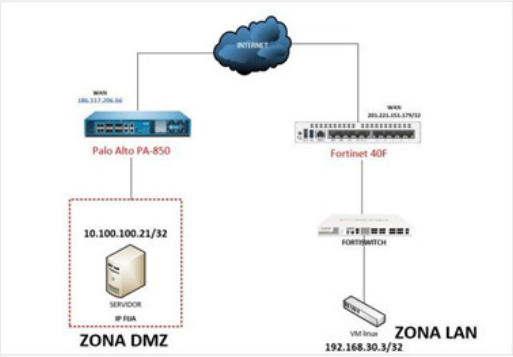

Figura 1 Topología implementada
Fuente: elaboración propia

La metodología empleada en el análisis, desde el punto de vista de la topología, se ajusta a la normativa de buenas prácticas en el diseño de la seguridad de redes institucionales, mostrando el uso de arquitectura, a la vez, simple y robusta. Las conexiones site-to-site permiten a las dos sedes funcionar como si estuviesen en la misma red privada, evitando la necesidad de exponer servicios directamente a Internet. Este hecho cobra especial relevancia en la transferencia de datos, como el manejo de información financiera y procesamiento de transacciones de recaudo.

La más importante de las características del diseño en general y la topología, es la escalabilidad. Al estar construida sobre una VPN IPsec entre firewalls, el diseño puede incorporar más sedes y extender los rangos de red. Adicionalmente, la topología permite la inclusión de diferentes niveles de control, a través de las políticas de seguridad, en la segmentación y control de los servicios que se comunican a través del túnel, lo que mejora el control de acceso [15].

ISSN 1794-211 X • e-ISSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2023). pp. 91-98. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

En resumen, la topología propuesta mejora significativamente la gestión y el mantenimiento de la solución a largo plazo. Al integrar los componentes de seguridad y enrutamiento en los firewalls, los administradores obtienen la capacidad de monitorear el estado del túnel, analizar el tráfico y responder a varios incidentes de manera oportuna. En general, el diseño busca equilibrar la seguridad, la eficiencia operativa y la simplicidad, cumpliendo con los requisitos de interconexión segura entre un municipio y el banco.

4.2. Requerimientos de seguridad para la transmisión de datos:

Dentro de la figura 2 se analiza que la comunicación entre la alcaldía y el banco utiliza redes públicas y túneles VPN IPsec como el servicio más seguro. El diagrama muestra cómo la información sensible se asegura en una caja y se cifra en el firewall de origen, para ser descifrada en el firewall de destino. Durante su viaje a través de Internet, la información no puede ser interceptada ni analizada, debido a su tránsito por Internet. Implementar controles de seguridad perimetral también es preciso, lo que asegura que solo el tráfico permitido, el que está autorizado, entre en la VPN.

Figura 2. Red de comunicación segura entre la alcaldía y el banco.

Fuente: elaboración propia

En términos generales, los estándares de seguridad de la información institucional se centran en los principios de confidencialidad, integridad y disponibilidad. Para lograr la confidencialidad, se pueden aplicar mecanismos de cifrado que protegen la información del acceso no autorizado, mientras que la integridad asegura que la información que se transmite no sea alterada. Además, es esencial que los sistemas de recolección estén operando a su máxima disponibilidad. Ininterrumpida, confiable y sin interrupciones.

Otro requisito importante es la autenticación de los puntos finales de comunicación y el control de acceso de los recursos compartidos. Es importante que tanto la Alcaldía como el Banco autentiquen la identidad del dispositivo remoto antes de establecer la comunicación, para reducir los riesgos de suplantación. Igualmente, para proteger los datos y minimizar la superficie de ataque en la interconexión entre ambas entidades, se deben definir las políticas de seguridad y el tráfico permitido a través del túnel VPN debe limitarse a los servicios necesarios.

4.3. Compatibilidad e interoperabilidad entre Palo Alto PA-850 y Fortinet 40F:

La figura 3 sugiere que la interoperabilidad del firewall Palo Alto PA-850 y los firewalls Fortinet 40F se puede lograr configurando correctamente los parámetros del protocolo IPsec en ambos dispositivos. El diagrama muestra cómo, a pesar de ser de diferentes fabricantes, es posible establecer un túnel VPN estable, siempre que se configuren parámetros de cifrado, autenticación y selección de tráfico compatibles. Esta representación muestra que la estandarización de IPsec permite proporcionar comunicaciones seguras entre sistemas diferentes.

En términos generales, la interoperabilidad entre dispositivos de Palo Alto y Fortinet es una consecuencia del uso de los protocolos abiertos y estandarizados IPsec e IKE. Ambos firewalls también ofrecen soporte para una amplia gama de

algoritmos criptográficos y de autenticación, lo que facilita la definición de los parámetros comunes requeridos para establecer un túnel VPN. Sin embargo, la interoperabilidad requiere una revisión minuciosa de las configuraciones, ya que

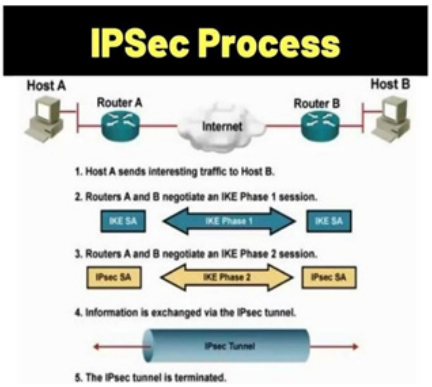

Figura 3. Esquema de interoperabilidad entre Palo Alto y Fortinet

Fuente: Ipcisco (2024).

las diferencias terminológicas o las formas particulares de implementar un parámetro dado pueden resultar en la falla de la conexión.

Los beneficios de la interoperabilidad de un Palo Alto PA-850 y un Fortinet 40F son considerables. Permite aprovechar la infraestructura ya disponible y evita la dependencia de un único proveedor, lo que también reduce los costos de adquisición y aumenta la flexibilidad en el diseño de la red. Cuando se implementa correctamente, esta interoperabilidad ofrece la certeza de que la comunicación siempre será segura, confiable y estable, demostrando que la incorporación de diferentes soluciones de seguridad de distintos fabricantes en un mismo ecosistema es, sin duda, una opción correcta.

4.4 Resultados de la configuración del túnel VPN IPseec Site-to-Site VI-BI.

ISSN 1794-211 X • e-lSSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2023). pp. 91-98. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

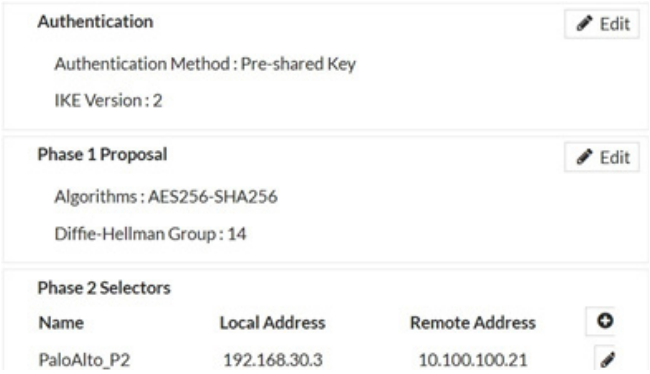

Figura 4. Configuración del método de autenticación mediante IKEv2.

Fuente: elaboración propia

De forma general, IKEv2 es el protocolo que realiza la autentificación de los dos extremos de la comunicación y la negociación de las claves que se utilizarán para el cifrado del túnel VPN. Entre sus versiones, IKEv2 muestra la ventaja de ofrecer mayor estabilidad y un mejor manejo de reconexiones y de la negociación, lo que es especialmente relevante en el ámbito institucional, donde IKEv2 sigue siendo una de las herramientas robustas que responde a los cambios en la conectividad.

Configurar correctamente el método de autentificación es fundamental para asegurar el enlace. Este mecanismo garantiza que solo los dispositivos autorizados puedan establecer la VPN. Junto con el uso de IKEv2 y una autentificación adecuada, esto genera confianza entre las partes, reduce los riesgos de ataques de suplantación y asegura que la transmisión de datos entre la alcaldía y el banco se realice dentro de un marco seguro sólido y fiable.

4.5. Resultados de la Fase 1 de IKE: cifrado, hash y grupo Diffie-Hellman:

La figura 5 muestra que la Fase 1 de IKE está adecuadamente establecida entre Palo Alto PA- 850 y Fortinet 40F, confirmando la compatibilidad de los parámetros criptográficos configurados. Ambos dispositivos complementan el uso de un algoritmo de cifrado fuerte, un método hash para asegurar la integridad y un grupo común de Diffie-Hellman para el intercambio seguro de claves. El estado exitoso de la negociación muestra que se ha establecido un canal seguro para proteger los procesos iniciales de autenticación y negociación.

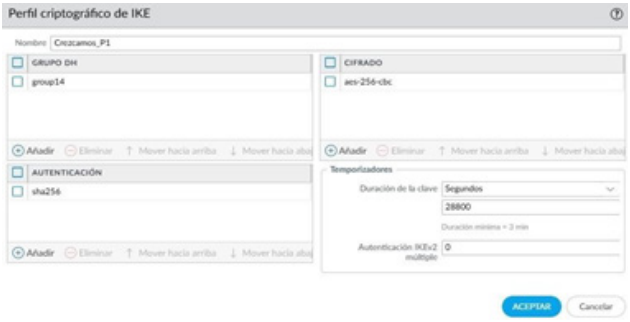

Figura 5. Parámetros criptográficos de la Fase 1 de IKE.

Fuente: elaboración propia

Por norma general, el primer objetivo de la Fase 1 de IKE es la construcción de una relación de seguridad confiable entre ambos extremos de la VPN. En esta fase, se establecen los parámetros de la VPN, entre los que se encuentran los algoritmos de cifrado que protegen las comunicaciones, los algoritmos hash que resguardan la integridad de los mensajes y el grupo de Diffie-Hellman que, de forma segura, genera las claves que se compartirán. La escogencia de estos parámetros

impacta con fuerza el evitar exposiciones, logrando así una seguridad criptoanalítica de excelencia. Un resultado positivo en la fase 1 es indicativo de que el IKE construido es funcional y la exposición ofrecida por la seguridad es suficiente para que la organización opere, enfrente, y se interrelacione con otros ecosistemas en el ámbito institucional.

La sólida estructura criptoalgorítmica, junto con el grupo de Diffie-Hellman en el que se fundamenta la negociación inicial del túnel VPN, asegura que la negociación será completamente segura de cualquier ataque de intercepción y de manipulación. Esto permite que la Fase 2 de IPsec se configure en condiciones altamente favorables, ya que la seguridad es llevada a un nivel más alto respecto a la comunicación de los datos entre la Alcaldía y el Banco.

4.6 Parámetros criptográficos homologados entre Palo Alto y Fortinet.

Tabla 2. Parámetros criptográficos homologados entre Palo Alto y Fortinet.

Parámetro Técnico	Fase 1 (IKE Gateway / Proposal)	Fase 2 (IPsec Crypto / Proposal)
Versión de IKE	IKEv2	N/A
Protocolo IPsec	N/A	ESP
Algoritmo de Cifrado	AES-256	AES-256
Algoritmo de Hash	SHA-256	SHA-256

ISSN 1794-211 X • e-lSSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2023). pp. 91-98. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

Intercambio de Claves	Diffie-Hellman Group 14	PFS Habilitado (DH Group 14)
Autenticación	Pre-Shared Key (PSK)	N/A
Tiempo de Vida (Lifetime)	86400 segundos (24 horas)	3600 segundos (1 hora)

Para garantizar la confidencialidad, integridad y autenticidad del tráfico entre las arquitecturas de Palo Alto Networks y Fortinet, se estableció una VPN IPsec basada en el protocolo IKEv2 (Internet Key Exchange version 2). La elección de IKEv2 obedece a su mayor robustez frente a ataques de denegación de servicio (DoS) y su eficiencia en el proceso de negociación en comparación con IKEv1.

4.7. Resultados de la Fase 2: selectores de tráfico y políticas IPsec:

La figura 6 muestra que la negociación de la Fase 2 de IPsec se realizó correctamente entre el firewall Palo Alto y el Fortinet. Muestra que el trazo de los selectores de tráfico locales y remotos está correcto. Estos selectores definen los rangos de direcciones IP y las subredes que serán parte del túnel VPN y que, por lo tanto, serán. encapsuladas y cifradas".

La coincidencia de parámetros en los dos dispositivos indica que la negociación de la Fase 2 no tuvo conflictos y que el tráfico fue y es exitosamente enrulado a través del túnel.

Figura 6. Resultados de la Fase 2 de Ipsec.

Fuente: elaboración propia

En términos generales, el objetivo de la Fase 2 de IPsec es crear las asociaciones de seguridad que protegen el manejo del tráfico entre las redes. Para esto se eligen los algoritmos que se van a aplicar a los paquetes en términos de cifrado y de integridad, así como los tiempos de vida de las asociaciones de seguridad. Una adecuada configuración de la Fase 2 es la que va a ayudar a que la información que se maneja en las redes entre la alcaldía y el banco se mantenga segura de intervenciones no autorizadas y de modificaciones durante la transmisión.

Finalmente, las políticas asociadas con la Fase 2 de IPsec son instrumentales en la gobernanza del tráfico que atraviesa el túnel VPN. Tales políticas permiten un control más estricto de la comunicación hacia los servicios y las redes que son estrictamente necesarias para el proceso de recolección, reduciendo así la superficie de ataque y previniendo que el enlace seguro sea abusado. Los hallazgos muestran que definir adecuadamente el selector de tráfico y las políticas de IPsec mejora directamente la estabilidad, seguridad y eficiencia de la interconexión entre la alcaldía y el banco.

4.8. Establecimiento exitoso del túnel y asociaciones de seguridad activas:

El análisis de la figura 7 revela la exitosa creación del túnel VPN IPsec entre los firewalls Palo Alto y Fortinet, mostrando el estado activo de las asociaciones de seguridad. El estado visual confirma que las negociaciones de IKE y las asociaciones IPsec están levantadas, lo que indica que los parámetros de autentificación, encriptación y los selectores de tráfico son compatibles en ambos extremos. Este estado operativo confirma que el túnel está listo para comenzar el transporte seguro del tráfico.

Figura 7. Estado activo del túnel VPN Ipsec.

Fuente: elaboración propia

Desde un nivel de abstracción más alto, el éxito en el establecimiento del túnel representa un gran avance en la construcción de una VPN site-to-site, dado que se asegura de que existe un canal de comunicación que está cifrado y autenticado entre las dos redes. Las asociaciones de seguridad activas son un indicativo de que los elementos de la criptografía están funcionando y no han existido problemas en el mecanismo de intercambio de claves. Esto protege de manera confiable y robusta la comunicación entre la Alcaldía y el Banco.

Las asociaciones de seguridad activas han permanecido reflejando la estabilidad del vínculo de la VPN durante su operación continua. Un túnel estable permite la transmisión continua de datos financieros y administrativos, lo cual es medular en la actividad de recaudo. Estos resultados evidencian que la infraestructura implementada cumple con los requerimientos de disponibilidad y seguridad, aportando confianza operativa y disminuyendo el riesgo de fallas en la comunicación entre ambas entidades.

4.9. Análisis de rendimiento y estabilidad de la VPN.

La figura 8 muestra los resultados de la prueba de conectividad que el gobierno municipal y el banco realizaron sobre la VPN encriptada por IPsec utilizando

ISSN 1794-211 X • e-lSSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2023). pp. 91-98. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

solicitudes de ping ICMP (Protocolo de Mensaje de Control de Internet). Los tiempos de respuesta muestran que la latencia es baja y consistente, y no hubo paquetes perdidos. Esto prueba que los procesos de encapsulación y encriptación del túnel VPN no añaden ningún retraso a la latencia de comunicación. Esto confirma que el rendimiento del túnel es adecuado para sostener el intercambio constante de datos administrativos y fiscales que se necesitan para los procesos de recaudación de impuestos.

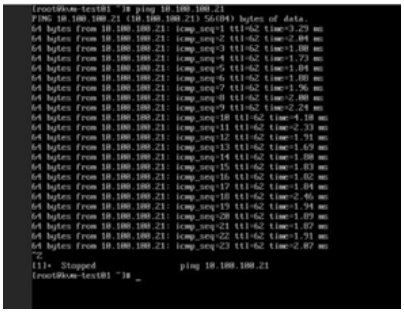

Figura 8. Prueba de conectividad ICMP a través del túnel VPN.

Fuente: elaboración propia

En el caso particular de Ikev-ATN y la implementación de una VPN IPsec, el rendimiento y la estabilidad de la VPN dependen de la tunelización de las políticas de encriptación, así como del alcance de los dispositivos de seguridad en la línea y la calidad de la conexión de Internet. En el caso analizado, el uso de algoritmos de encriptación y el ajuste de las políticas y reglas de enrutamiento en la VPN IPsec lograron un flujo de información constante, ininterrumpido y seguro. La estabilidad del túnel VPN crea las condiciones para proporcionar un servicio ininterrumpido, sin demoras que puedan afectar la validación de pagos y la sincronización de datos en tiempo real entre las instituciones.

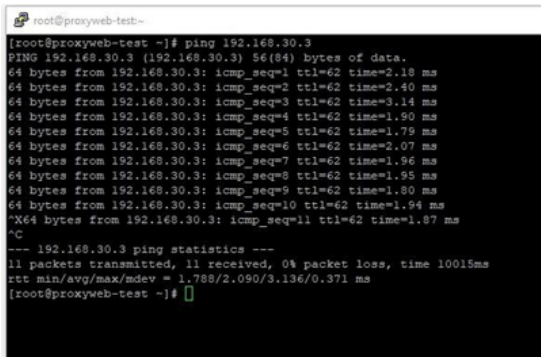

Figura 9 Monitoreo del estado y estabilidad del túnel VPN

En la figura 9 se muestra el monitoreo de los túneles y el tráfico con las herramientas de firewall de Palo Alto. Los registros y gráficas muestran pares de seguridad activos, y en periodos prolongados, con escasas reinicializaciones y ausencia de fallos en la negociación. Estos datos corroboran que la VPN mantuvo un comportamiento estable a lo largo del tiempo, lo que es fundamental en el entorno institucional, donde la disponibilidad y la confiabilidad de la comunicación son determinantes para el eficaz desempeño de la actividad de cobranza.

Establecer un VPN IPsec site to site entre los firewalls de Palo Alto y Fortinet, fue una solución adecuada para asegurar la interconexión entre la oficina de la alcaldía y un banco, durante el proceso de cobro. Durante el trabajo, se evidenció que un diseño y parametrización adecuada de los niveles de seguridad, permitiría asegurar la confidencialidad, integridad y autenticidad de los flujos administrativos y financieros, en espacios de red pública. Se lograron disminuir de manera significativa los niveles de riesgo en la exposición de información, y se aumentó la confianza institucional en los procesos.

Los resultados de las pruebas técnicas, así como el monitoreo del túnel VPN, evidenciaron la estabilidad, el desempeño óptimo y la interoperabilidad de dispositivos de distintos proveedores, sin dificultades. El éxito en la negociación de las fases IKE e IPsec, junto con tráfico y configuración de políticas de seguridad, determinadas, aseguraron una conexión continua y completa. La solución implementada, además, demostró ser, en comparación con las opciones más tradicionales, como las líneas arrendadas, una alternativa más operativa y económicamente eficiente, sin comprometer la seguridad. Finalmente, me gustaría señalar que los VPN IPsec site-to-site muestran una alternativa viable y escalable para la interconexión de redes institucionales en entornos heterogéneos. La singularidad de la documentación del proceso de implementación y validación proporciona un valor añadido, ya que podría servir como guía para futuras implementaciones en otras entidades del sector público y privado. En resumen, la solución propuesta no solo abordó el problema, sino que también promovió positivamente el desarrollo de buenas prácticas en seguridad de la información y gestión de redes.

4.10. Tabla de Resultados Reales

Tabla 3 Métricas de rendimiento del túnel.

Métrica de Red	Valor Obtenido	Estado
Latencia Mín.	1.78 ms	Óptimo
Latencia Avg.	2.09 ms	Óptimo
Latencia Máx.	3.13 ms	Estable
Packet Loss	0%	Exitoso

ISSN 1794-211 X • e-lSSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2023). pp. 91-98. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

5. APORTE

El principal aporte de este trabajo radica en la demostración empírica de interoperabilidad estricta entre arquitecturas de seguridad heterogéneas (PAN-OS de Palo Alto Networks y FortiOS de Fortinet) aplicadas a un entorno de alta criticidad: el sector financiero y gubernamental. A diferencia de los escenarios ideales descritos en la literatura de los fabricantes, este artículo documenta la resolución de incompatibilidades nativas en la negociación de parámetros IKEv2 y Traffic Selectors.

Al establecer un túnel IPsec Site-to-Site con estándares criptográficos robustos (AES-256 y tributario sobre infraestructuras de red públicas, logrando una reducción significativa en los costos operativos frente a la contratación de enlaces dedicados privados (como MPLS), sin sacrificar el cumplimiento de las normativas de seguridad de la información.

6. TRABAJO FUTURO

A partir de la estabilidad y los resultados de latencia obtenidos en esta interconexión, las futuras líneas de desarrollo e investigación se centrarán en la escalabilidad y la automatización de la arquitectura:

• **6.1 Evolución hacia SD-WAN y Alta Disponibilidad:** Migrar la topología estática actual hacia una arquitectura de red definida por software (SD-WAN) que permita el enrutamiento dinámico del tráfico de recaudo a través de múltiples enlaces WAN concurrentes, integrando clústeres de Alta Disponibilidad (HA) en ambos extremos para mitigar puntos únicos de fallo.

• **6.2 Transición a arquitecturas Zero Trust (ZTNA):** Complementar el túnel IPsec perimetral con políticas de Acceso a la Red de Confianza Cero (ZTNA), garantizando que la autenticación y el cifrado no solo se realicen de sitio a sitio, sino a nivel de usuario y aplicación específica del banco y la alcaldía.

• **6.3 Monitorización Analítica y Automatización:** Desarrollar scripts de automatización que consuman las APIs REST de los firewalls Palo Alto y Fortinet para extraer los logs de tráfico y estado de las asociaciones de seguridad (SA) en tiempo real. Esto permitirá entrenar modelos de detección de anomalías que identifiquen intentos de disrupción del túnel o degradación del servicio antes de que impacten el proceso de recaudo.

7. REFERENCIAS

[1] C. Rubio, "Implementación de canales dedicados con la integración de VPNs IPSEC," Nov. 1, 2024. [Online]. Available: https://hdl.handle.net/20.500.12495/1376

[2] C. A. Buendía-Ardón and C. O. Pocasangre- Jiménez, "Alternativas de seguridad de datos en la red local para medianas y pequeñas empresas," Dec. 8, 2025. [Online]. Available:

[3] Y. Pabón, "Fortalecer los procesos contables internos de la Oficina de Recaudo de la Secretaría de Hacienda de la alcaldía de Pailitas, Cesar durante el segundo semestre de 2023," May 20, 2024. [Online]. Available: https://repository.unad.edu.co/handle/10596/ 62128

[4] M. K. P. Ureña and Y. T. Yañez, "Propuesta para la elaboración de un manual de procesos y procedimientos para optimizar el recaudo en la subsecretaría de rentas e impuestos de la alcaldía de San José de Cúcuta," Revista Investigación & Gestión, vol. 7, no. 2, Jul. 2024, doi: 10.22463/26651408.5038.

[5] J. O. Heredia-Arias, L. V. Mata-Criollo, C.F. Barreno-Flores and G. E. Vallejo-Mata, "Implementación de una solución SD-WAN para el uso eficiente de los recursos de red en su aplicación en la Empresa Asertia en el año 2021," MQRInvestigar, vol. 8, no. 2, pp. 195–208, Apr. 2024, doi: 10.56048/mqr20225.8.2.2024.195208.

[6] Andrade, "Diseño de solución de escritorios virtuales en nube orientados a proveedores tecnológicos de entidades financieras como opción de acceso seguro a la red de datos corporativa," Nov.21, 2023. [Online]. Available: http://hdl.handle.net/10757/672559

[7] A. Andaluz and J. Guanoluisa, "Implementación de una red VPN 'Virtual Private Network' para la mejora de la seguridad dentro de la red local inalámbrica de la Empresa de distribución de material de Construcción y Ferretero 'Distribuidora Gómez', mediante el uso de protocolos IPsec y TCP/IP," Tesis de pregrado, Universidad Técnica de Cotopaxi, 2022. [Online]. Available: http://repositorio.utc.edu.ec/handle/27000/9740

[8] Y. Prieto and J. Alvarez, "Fortalecimiento de la seguridad y privacidad de la información en una entidad pública del estado colombiano a través de la implementación de los Modelos de Seguridad y Privacidad de la Información (MSPI), Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) y la Norma ISO 27001," Apr. 12, 2024. [Online]. Available:

https://repository.unad.edu.co/handle/10596/ 60771

[9] R. Gonzales, "Diseño de una red de acceso remoto utilizando WireGuard como protocolo VPN para la encriptación de los procesos de gestión remota de una empresa agroindustrial del Perú," May 30, 2025. [Online]. Available: http://hdl.handle.net/10757/685771

[10] D. A. Q. Taraguay, D. I. A. Loachamin and H. M. R. Araujo, "El futuro de las redes privadas virtuales (VPN) en la era post- pandemia: Innovación y seguridad," Revista Retos Para la Investigación, vol. 4, no. 1, pp. 46–64, Mar. 2025, doi: 10.62465/rri.v4n1.2025.123.

[11] V. V. Aparicio-Izurieta, "Seguridad con IP seguro en Internet (IPSEC)," Sapienza International Journal of Interdisciplinary Studies, vol. 3, no. 1, pp. 978–987, Feb. 2022, doi: 10.51798/sijis.v3i1.278.

[12] Y. A. P. Loor and J. Herrera, "Evaluación del rendimiento de una red IPv6 utilizando IPSec en modo túnel," 2023. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?co digo=10526511

[13] E. Pastor, "Implementación de una solución remota con doble factor de autenticación y control de acceso de dispositivo para incrementar la seguridad informática en una empresa privada," Tesis de pregrado, Universidad Tecnológica del Perú, 2022. [Online]. Available: https://hdl.handle.net/20.500.12867/6551

[14] C. Contreras, "Análisis de la interconexión para el soporte de equipos de impresión en la zona Atlántico norte de Colombia de la empresa Ricoh utilizando redes de nueva generación ARMS," Aug. 5, 2024. [Online]. Available: https://repository.unad.edu.co/handle/10596/ 63635

[15] A. A. Á. Coello, "Redes privadas virtuales y ciberseguridad: revisión bibliométrica y sistemática de las tendencias de investigación, los protocolos y las aplicaciones (2004–2024)," Revista Científica Multidisciplinar G-nerando, vol. 6, no. 2, Nov. 2025, doi: 10.60100/rcmg.v6i2.631.