REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TEMA:

IMPLEMENTACIÓN DE UN PROCESO DE DESENCRIPTACIÓN DE TRÁFICO DE RED PARA LA OPTIMIZACIÓN DEL CONTROL DE SEGURIDAD Y LA GESTIÓN DE ACCESOS A SERVICIOS DE RED EMPRESARIALES.

Trabajo de Titulación previo a la obtención del título de Magíster en Computación Mención En Seguridad Informática

Línea de investigación: Desarrollo, aplicación de software y cyber security (seguridad cibernética)

AUTOR: MG. SILVIA LUCIA DUQUE CARRANCO

TUTOR: MSc. FABIÁN GEOVANNY CUZME RODRÍGUEZ

ASESOR: PhD. YOO SANG GUUN

Ibarra – Ecuador

2026

UNIVERSIDAD TÉCNICA DEL NORTE
DIRECCIÓN DE BIBLIOTECA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO	
APELLIDOS Y NOMBRES:	DUQUE CARRANCO SILVIA LUCIA

DATOS DE LA OBRA	
TÍTULO:	IMPLEMENTACIÓN DE UN PROCESO DE DESENCRIPTACIÓN DE TRÁFICO DE RED PARA LA OPTIMIZACIÓN DEL CONTROL DE SEGURIDAD Y LA GESTIÓN DE ACCESOS A SERVICIOS DE RED EMPRESARIALES.
AUTOR (ES):	DUQUE CARRANCO SILVIA LUCIA
FECHA: DD/MM/AAAA	11/05/2026
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ■ **POSGRADO**
TITULO POR EL QUE OPTA:	Magíster en Computación con mención en Seguridad Informática
DIRECTOR /ASESOR:	MSC. CUZME RODRIGUEZ FABIAN GEOVANNY, PHD YOO SANG GUNN

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 4 días del mes de Julio de 2026

EL AUTOR:

(Firma)…… Silvia Lucia Duque Carranco Time Stamping Security Data ……

Nombre: DUQUE CARRANCO SILVIA LUCIA

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE POSGRADO

Ibarra, 12 de mayo de 2026

Dr. Jorge Gordón
Decano
Facultad de Posgrado

ASUNTO: Conformidad con el documento final

Señor Decano:

Nos permitimos informar a usted que revisado el Trabajo final de Grado "IMPLEMENTACIÓN DE UN PROCESO DE DESENCRIPTACIÓN DE TRÁFICO DE RED PARA LA OPTIMIZACIÓN DEL CONTROL DE SEGURIDAD Y LA GESTIÓN DE ACCESOS A SERVICIOS DE RED EMPRESARIALES" del maestrante Silvia Lucia Duque Carranco, de la Maestría en Computación con Mención en Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	**Firma**
Director	MSC. CUZME RODRÍGUEZ FABIÁN	Validar únicamente en FirmaEC. Firmado electrónicamente por: FABIAN GEOVANNY CUZME RODRIGUEZ
Asesor	PHD. YOO SANG GUNN	Validar únicamente en FirmaEC. Firmado electrónicamente por: SANG GUUN YOO .

DEDICATORIA

Quiero dedicar esta tesis a mi madre, quien con su enorme amor nos enseñó a luchar a pesar de cualquier circunstancia aunque ya no está físicamente con nosotros es nuestra fortaleza y nuestra paz, nos enseñó a ser perseverantes y a continuar con nuestras metas a pesar de todo. Ha sido difícil conseguir terminar con mis estudios que quedaron truncados al momento de su muerte, pero después de muchos años se ha hecho una realidad.

Quiero dedicar esta tesis a mi hija, que ha sido la razón de mis posteriores esfuerzos, para enseñarle que con disciplina, esfuerzo y valor se puede lograr las metas que nos proponemos.

Quiero dedicar también este trabajo a Dios y a las personas que ha puesto en mi vida que han sido sus ángeles en distintos momentos ayudándome, apoyándome y a veces han estado ahí solo para motivarme.

AGRADECIMIENTO

Un agradecimiento a Dios por acompañarme siempre en todos los aspectos de mi vida, por ayudarme a tener la posibilidad de haber cursado esta maestría y de haberla terminado con éxito.

Un agradecimiento a mi hija que me ha apoyado en el desarrollo de mis estudios comprendiendo el tiempo y el esfuerzo que se debe dedicar a los aspectos que significan un crecimiento personal.

Un agradecimiento a mis profesores de la universidad, al coordinador de carrera, a mis compañeros, a mi prima, y a mi tutor quien me guio e impulso en la idea y en el desarrollo de mi tesis.

ÍNDICE

CAPITULO I 13
1. EL PROBLEMA 13
1.1 Problema De Investigación 13
1.2 Interrogantes De Investigación 15
1.3 Objetivos De Investigación 16
1.4 Hipótesis De Trabajo 17
1.5 Hipótesis Nula 17
1.6 Categorización De Variables 17
1.7 Justificación 18
CAPITULO II 22
2. MARCO REFERENCIAL 22
2.1 Antecedentes 22
2.2 Marco Teórico 28
2.2.1 Antecedentes 28
2.2.2 Descifrado de tráfico de red 28
2.2.3 Control de seguridad de tráfico de red 34
2.2.4 Gestión de accesos empresariales de tráfico cifrado 35
2.2.5 Fundamentos del cifrado en redes de datos 36
2.2.6 Impacto del cifrado en la ciberseguridad 43
2.2.7 Enfoques actuales para el análisis de tráfico cifrado 44
2.2.8 Estado actual de la investigación 45
2.2.9 Privacidad y protección de datos 46
CAPÍTULO III 50
3. MARCO METODOLÓGICO 50
3.1 Descripción del área de estudio 50
3.2 Enfoque y tipo de investigación 51
3.3 Procedimiento de investigación 52
3.4 Consideraciones bioéticas 54
CAPÍTULO IV 56
4 RESULTADOS Y EVALUACION 56
4.1 Escenario de implementación 56
4 .1.1 Arquitectura de red 56

4.1.2 Subredes piloto y alcance 58
4.1.3 Equipos, versiones y políticas aplicadas 62
4.2 Implementación del proceso de inspección SSL/TLSg 62
4.2.1 Certificados Trust/Untrust 62
4.2.2 Distribución por GPO 65
4.3 Implementación del descifrado outbound en los Equipos de Seguridad Perimetral 72
4.3.1 Desarrollo de reglas de control 72
4.3.2 Pruebas en las máquinas de los usuarios 77
4.3.3 Verificación en los log de los Firewalls 80
4.3.4 Excepciones de privacidad 82
4.3.5 Implementación del descifrado inbound en los Equipos de Seguridad Perimetral 84
4.4 Análisis por firewall de la implementación outbound e inbound 87
4.4.1 Firewalls Internos outbound decryption 87
4.4.2 Firewalls Externos inbound decryption 92
4.5 Evaluación del Sistema de Descifrado 100
4.6 Interpretación de resultados 101
4.7 Limitaciones de medición en el estudio 102
4.8 Discusión de resultados 104
4.8.1 Cumplimiento de objetivos 104
4.8.2 Riesgos operativos 108
4.8.3 Implicaciones éticas y legales 109
CONCLUSIONES 114
RECOMENDACIONES 117
BIBLIOGRAFÍA 118

ÍNDICE DE TABLAS

Tabla 1 Proyectos descifrado 27
Tabla 2 Mecanismos tradicionales de análisis de tráfico 37
Tabla 3 Implementaciones para escenarios con cifrado 38
Tabla 4 Privacidad y protección de datos 46
Tabla 5 Visibilidad de Aplicaciones outbound proyectada al tráfico total 92
Tabla 6 Visibilidad de Aplicaciones inbound 97
Tabla 7 Comparativa de rendimiento antes y después de la implementación de descifrado 101
Tabla 8 Matriz cumplimiento de objetivos 104
Tabla 9 Características del entorno piloto 105
Tabla 10 Reglas de tráfico 106
Tabla 11 KPI cumplimiento de objetivos 107

ÍNDICE DE FIGURAS

Figura 1 Resultado de la búsqueda en la base de datos IEEE Xplore 23
Figura 2 Arquitectura Jerárquica de Certificación 31
Figura 3 Implementación de un sistema de descifrado de tráfico de red Implementación de un sistema de descifrado de tráfico de red 52
Figura 4 Red empresarial en la que se proyecta la implementación completa 57
Figura 5 Diagrama Decryption outbound 58
Figura 6 Diagrama Decryption Inbound 59
Figura 7 Definición de URLs: 60
Figura 8 Regla de drop por URL 61
Figura 9 URL definido 61
Figura 10 Definición de horario de bloqueo 61
Figura 11 Generación de certificados Trust 63
Figura 12 Certificado Trust 63
Figura 13 Generación de certificados Untrust 64
Figura 14 Certificado Untrust 64
Figura 15 Certificados Generados 65
Figura 16 Configuración para ingreso de certificado localmente 65
Figura 17 Vista de certificados en la maquina 66
Figura 18 Escojo el certificado trust 66
Figura 19 Despliegue de certificados instalados 67
Figura 20 Importo certificado 67
Figura 21 Ingreso el certificado al Active Directory 68
Figura 22 Almacén de certificados del Active Directory 69
Figura 23 Reviso certificado en el almacén de certificados 69
Figura 24 Reviso información en el certificado 70
Figura 25 Ejecuto GPO y remito a maquinas en dominio 70
Figura 26 GPO ejecutado certificados distribuidos a la organización 71
Figura 27 maquina cliente se evidencia el resultado del GPO 71
Figura 28 Regla descifrado hacia Internet 73
Figura 29 Tipo de regla de descifrado 73
Figura 30 Regla de descifrado desde una IP de prueba hacia Internet 73
Figura 31 Creación de Aplication Filter 74
Figura 32 Creación de filtros de aplicación para proxys de navegación 74
Figura 33 Se crean categorías de URL 75
Figura 34 Creación de un URL Filtering profile 76
Figura 35 Ingreso de aplicación proxy anonymizer al perfil de Url filtering 76
Figura 36 Regla de control de tráfico para bloqueos de proxys http 77
Figura 37 Regla de control de tráfico para bloqueos por aplicaciones 77
Figura 38 Maquina muestra error de certificado 77
Figura 39 El navegador no permite el despliegue de la página 78
Figura 40 Maquina con proxy Ultrasurf instalado 79
Figura 41 Sitio bloqueado una vez descifrado 79
Figura 42 Sitio bloqueado una vez descifrado 80
Figura 43 Verificación de que el tráfico está siendo descifrado 80
Figura 44 Aplicaciones bloqueadas al haber sido vistas una vez des encriptadas 81
Figura 45 Consolidado de aplicaciones que fueron bloqueadas 81
Figura 46 Aplicaciones excluidas de descifrado por seguridad de las mismas 82

Figura 47 Exclusión de descifrado de aplicaciones solicitadas por usuarios 82
Figura 48 Exclusión de descifrado de usuarios que realizan tareas específicas 83
Figura 49 Exclusión de destinos considerados de confianza 83
Figura 50 Exclusión de sitios de almacenamiento externo de confianza 83
Figura 51 Instalación de certificados institucionales 84
Figura 52 Importo certificado institucional 85
Figura 53 Decryption profile para inbout inspección 85
Figura 54 Política Decryption ingreso 86
Figura 55 Logs de descifrado de tráfico entrante 86
Figura 56 CPU Firewalls internos Julio 2025 87
Figura 57 CPU Firewalls internos Agosto 2025 88
Figura 58 CPU Firewalls internos Septiembre 2025 88
Figura 59 Vista de aplicaciones Julio 2025 90
Figura 60 Vista de aplicaciones Agosto 2025 90
Figura 61 Vista de aplicaciones Septiembre 2025 91
Figura 62 Amenazas bloqueadas 91
Figura 63 CPU Firewalls externos febrero 2026 93
Figura 64 CPU Firewalls externos febrero a mayo 2026 94
Figura 65 Vista de aplicaciones Enero 2026 94
Figura 66 Vista de aplicaciones Febrero 2026 95
Figura 67 Vista de aplicaciones Marzo 2026 95
Figura 68 Vista de aplicaciones Abril 2026 96
Figura 69 Threat Activity Enero 2026 97
Figura 70 Threat Activity Febrero 2026 98
Figura 71 Threat Activity Marzo 2026 98
Figura 72 Threat Activity Abril 2026 99
Figura 73 Reglas de decryption 107

RESUMEN

La seguridad de los activos informáticos y de la información se ve comprometida por ataques que no son fácilmente detectables debido al uso de mecanismos de cifrado en los accesos a determinados sitios web y por aplicaciones que cifran su tráfico con el fin de evadir los controles de seguridad implementados por las organizaciones. En este contexto, resulta necesario disponer de mecanismos que permitan descifrar dicho tráfico para analizarlo y aplicar controles que garanticen una protección efectiva de la información y el cumplimiento de las políticas de uso establecidas.

Este trabajo propone la implementación de un modelo de descifrado de tráfico mediante el uso de certificados intermedios ubicados entre los dispositivos de los usuarios finales y los firewalls. Esta solución permite establecer políticas de descifrado para inspeccionar el tráfico generado, facilitando la aplicación de controles de acceso, mecanismos de seguridad y reglas de uso definidas por la organización.

Como resultado, se implementó exitosamente el modelo de desencriptación basado en certificados intermedios, lo que permitió analizar el tráfico de red, bloquear accesos indebidos y aplicar controles de seguridad tales como antivirus, antispyware, antimalware, filtrado de URL y políticas de navegación basadas en categorías y direcciones web.

Las actividades de implementación fueron realizadas con el acompañamiento de especialistas del fabricante y siguiendo la documentación técnica oficial, con el propósito de garantizar una implementación eficiente y alineada con las mejores prácticas recomendadas.

Con base en los resultados obtenidos, se comprobó que la gestión de la seguridad de la red mediante el uso de desencriptación con certificados intermedios permite a la institución ejercer un control más efectivo sobre el tráfico en tránsito, proporcionando mayor visibilidad y una clasificación más precisa del mismo. Esto contribuye a la protección de los activos de información y a una administración más eficiente de los controles de seguridad, ya que estos pueden aplicarse sobre el tráfico real que circula por la red.

Palabras clave: descifrado, controles, vulnerabilidades, riesgo.

ABSTRACT

The security of IT assets and information is compromised by attacks that are not easily detectable due to the use of encryption mechanisms when accessing certain websites and by applications that encrypt their traffic to evade the security controls implemented by organizations. In this context, it is necessary to have mechanisms that allow for the decryption of this traffic in order to analyze it and apply controls that guarantee effective information protection and compliance with established usage policies.

This paper proposes the implementation of a traffic decryption model using intermediate certificates located between end-user devices and firewalls. This solution allows for the establishment of decryption policies to inspect the generated traffic, facilitating the application of access controls, security mechanisms, and usage rules defined by the organization.

As a result, the intermediate certificate-based decryption model was successfully implemented, enabling network traffic analysis, blocking unauthorized access, and applying security controls such as antivirus, antispyware, antimalware, URL filtering, and browsing policies based on categories and web addresses.

The implementation activities were carried out with the support of manufacturer specialists and following the official technical documentation to ensure efficient implementation aligned with best practices.

Based on the results obtained, it was verified that managing network security using intermediate certificate decryption allows the institution to exercise more effective control over traffic in transit, providing greater visibility and more accurate traffic classification. This contributes to the protection of information assets and more efficient management of security controls, as these can be applied to the actual traffic circulating on the network.

Keywords: decryption, controls, vulnerabilities, risk.

CAPITULO I

1. EL PROBLEMA

1.1 Problema De Investigación

El incremento del tráfico de red cifrado presenta un desafío sustancial para la supervisión de la seguridad y la aplicación de políticas de acceso. La encriptación, aunque crucial para la privacidad, (A10 Networks. 2020). puede también ocultar actividades maliciosas, dificultando la detección temprana de amenazas. Existe la necesidad de desarrollar una solución que equilibre la seguridad y la privacidad, (CBT Nuggets. 2020) para ello el uso de certificados digitales podrían mejorar el control de la seguridad y la gestión de accesos a los servicios de red empresariales, tanto internos como externos, siendo necesario implementar un proceso de descifrado de tráfico de red mediante el uso de certificados intermedios.

En la actualidad, el aumento del uso de técnicas de cifrado en las comunicaciones de red ha mejorado significativamente la privacidad y la seguridad de los datos transmitidos. Sin embargo, esta tendencia también ha dificultado la detección de amenazas, como malware, comandos de control o presenta estadísticas de latencia, que pueden ocultarse dentro del tráfico cifrado. Muchas soluciones de seguridad actuales no son efectivas para analizar contenido cifrado sin vulnerar la privacidad de los usuarios o sin un elevado consumo de recursos computacionales. Ante este escenario, surge la necesidad de investigar métodos viables para descifrar o analizar el tráfico cifrado en

redes, de forma selectiva, segura y eficiente, sin comprometer la privacidad general de los usuarios ni el rendimiento del sistema.

En los últimos años, el uso de técnicas de cifrado en las redes de datos ha crecido exponencialmente, impulsado principalmente por la necesidad de proteger la privacidad y la integridad de la información transmitida a través de internet. Protocolos como HTTPS, SSL/TLS, y VPN se han convertido en estándares en la comunicación digital, asegurando que los datos transmitidos entre usuarios y servidores estén protegidos contra interceptaciones y modificaciones no autorizadas.

Este avance, si bien beneficioso desde el punto de vista de la seguridad y la privacidad, ha generado nuevos desafíos en el ámbito del monitoreo de redes, la ciberseguridad y la detección de amenazas. Tradicionalmente, los sistemas de detección de intrusiones (IDS), los firewalls y las soluciones de monitoreo de tráfico han dependido en gran medida de la inspección profunda de paquetes (Deep Packet Inspection, DPI) para analizar el contenido de las comunicaciones. Sin embargo, con el cifrado generalizado del tráfico, estos sistemas pierden visibilidad sobre lo que realmente ocurre dentro de la red, lo que puede permitir que actividades maliciosas pasen desapercibidas.

El tráfico cifrado,(Shah, N. 2020) aunque protege a los usuarios legítimos, también puede ser utilizado como vehículo para esconder actividades ilegales o maliciosas, tales como la comunicación de malware con sus servidores de comando y control, la transferencia de archivos robados, o la navegación por sitios prohibidos. (CySight. 2020). Dado que las soluciones de seguridad no pueden ver el contenido de este

tráfico, las organizaciones enfrentan una disyuntiva: permitir la privacidad de sus usuarios, o comprometerla en aras de la seguridad.

Además, las técnicas actuales para desencriptar tráfico, (Wang, Z., & Thing, V. L. L. 2023). como el uso de proxies con inspección SSL, presentan importantes limitaciones éticas, legales y técnicas. Estas técnicas requieren generalmente acceder a los certificados de los usuarios o instalar certificados raíz personalizados, lo cual puede representar una violación a la privacidad, un riesgo de seguridad si no se gestiona adecuadamente, y un alto consumo de recursos computacionales.

En este contexto, se vuelve urgente investigar nuevas formas de abordar el problema del análisis de tráfico cifrado (Wang, Z., Fok, L. 2022). sin incurrir en las limitaciones de las técnicas tradicionales. Entre las posibles soluciones se encuentra el uso de técnicas avanzadas como el análisis de tráfico basado en metadatos, machine learning, fingerprinting de protocolos cifrados y correlación de patrones, que podrían permitir inferir el tipo de actividad sin necesidad de romper el cifrado directamente.

1.2 Interrogantes De Investigación

RQ1: ¿Se puede utilizar certificados intermedios para descifrar el tráfico de la red empresarial para analizar y controlar el mismo?

RQ2: ¿Cómo se podría mejorar la seguridad en la red y el acceso a los servicios empresariales mediante el Desarrollo de reglas de controles de acceso basadas en el análisis del tráfico descifrado?

RQ3: ¿Se podría evaluar la efectividad del sistema de descifrado y las reglas de control de acceso implementadas para sustentar la implementación de las mismas en toda la empresa?

1.3 Objetivos De Investigación

Objetivo General

Implementar un proceso de descifrado de tráfico de red mediante el uso de certificados intermedios, para mejorar el control la seguridad y la gestión de accesos a los servicios de red empresariales, tanto internos como externos.

Objetivos Específicos

1. Implementar un sistema de descifrado de tráfico de red utilizando certificados intermedios en una subred, para analizar y controlar el tráfico de red empresarial.

2. Desarrollar reglas de controles de acceso basadas en el análisis del tráfico descifrado, para mejorar la seguridad de la red y el acceso a servicios empresariales.

3. Evaluar la efectividad del sistema de descifrado y las reglas de control de acceso implementadas.

1.4 Hipótesis De Trabajo

H1: Implementar un proceso de descifrado de tráfico de red mediante certificados intermedios MEJORA el control y la seguridad de los accesos a los servicios de red empresariales, al ampliar la capacidad de inspección del tráfico cifrado, la detección de amenazas y la aplicación de políticas de acceso tanto en servicios internos como externos.

1.5 Hipótesis Nula

H0: Implementar un proceso de descifrado de tráfico de red mediante certificados intermedios NO MEJORA el control y la seguridad de los accesos a los servicios de red empresariales, al ampliar la capacidad de inspección del tráfico cifrado, la detección de amenazas y la aplicación de políticas de acceso tanto en servicios internos como externos.

1.6 Categorización De Variables

Variable Independiente

Proceso de descifrado de tráfico de red mediante el uso de certificados intermedios

Variable dependiente

Control de seguridad y gestión de accesos a los servicios de red empresariales, tanto internos como externos

1.7 Justificación

La encriptación es un proceso que ayuda a resguardar la seguridad de la información así como el transporte de la misma, (Khan, B. 2019). pero esta pueda usarse para fines maliciosos cuando puede ocultar ataques o información que no se requiere que sea transportada o vista por personal externo.

Existen amenazas que se ocultan bajo encriptación (Streefland, F., & Harrison, J. 2019). igualmente proxys de navegación que no pueden ser detectados por los equipos de seguridad debido a que el tráfico que generan viaja cifrado

El cifrado es una forma segura y privada excelente de intercambiar información comercial. Sin embargo, el tráfico cifrado o encriptado está compuesto básicamente por datos ocultos que no permiten que las organizaciones detecten las amenazas de seguridad que se encuentran en su interior. Lamentablemente, (Khan, B. 2019). los delincuentes han aprendido a aprovechar esta falta de visibilidad y de identificación para ocultarse de la vigilancia de seguridad dentro del tráfico cifrado y entregar malware. Incluso los sitios web legítimos que usan SSL pueden infectarse con malware.

Es por esto que para la empresa es importante (Streefland y Harrison 2019). que se pueda analizar el tráfico que se trasmite con el fin de controlarlo y poner seguridad en el mismo, por lo que se probará implementar un proceso de descifrado de tráfico de red mediante el uso de certificados intermedios para mejorar el control la seguridad y la gestión de accesos a los servicios de red empresariales, tanto internos como externos.

Este problema de investigación es relevante tanto para instituciones públicas como privadas que (Wang, et al. 2022). dependen de redes seguras y confiables. Las organizaciones deben protegerse contra amenazas internas y externas, pero sin vulnerar derechos fundamentales como la privacidad. El desarrollo de tecnologías capaces de ofrecer un equilibrio entre seguridad y privacidad podría marcar un avance significativo

en el campo de la ciberseguridad y abrir la puerta a nuevas políticas y marcos éticos para el manejo del tráfico cifrado.

Además, desde un punto de vista técnico, (Wang y Thing 2023). el análisis de tráfico cifrado sin descifrado directa representa un desafío complejo que involucra campos como criptografía, aprendizaje automático, análisis de datos y redes de comunicación. Superar este desafío requiere enfoques innovadores que contribuyan tanto a la academia como a la industria.

El crecimiento exponencial del tráfico cifrado en las redes modernas ha traído consigo un cambio significativo en la forma en que se concibe la seguridad informática. (Abbasi, M., et al. 2020). Actualmente, más del 90% del tráfico web a nivel global utiliza protocolos cifrados como HTTPS, SSL/TLS, o conexiones seguras vía VPN. Este avance tecnológico responde a una necesidad real y urgente: proteger la integridad, confidencialidad y autenticidad de los datos transmitidos. En un mundo donde la información personal, financiera, empresarial y gubernamental se transmite por medios digitales, el cifrado se ha convertido en un pilar fundamental de la ciberseguridad y la privacidad.

No obstante, el aumento del cifrado también ha limitado gravemente la visibilidad de las soluciones de seguridad convencionales. (Lotfollahi, M., et al. 2017). Herramientas como los sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS), firewalls de nueva generación y sistemas de monitoreo de tráfico de red dependen, en gran medida, de la inspección del contenido de los paquetes para identificar amenazas. Al estar cifrados dichos contenidos, estas herramientas pierden capacidad de análisis y se ven obligadas a operar en la oscuridad. Este fenómeno ha sido llamado por muchos expertos como el “punto ciego del cifrado” (encryption blind spot).

La consecuencia inmediata de esta ceguera es el aprovechamiento de estos puntos ciegos por parte de los atacantes. Malware avanzado, ransomware, troyanos, y botnets utilizan canales cifrados para comunicarse con sus centros de comando y control, evadiendo detección durante largos periodos (Aceto, G., et al. 2020). Asimismo, actores maliciosos pueden exfiltrar información sensible de una organización utilizando túneles cifrados, sin que los sistemas de seguridad tradicionales puedan interceptarlos o detectarlos a tiempo. Por lo tanto, el cifrado —aunque esencial para la privacidad— ha introducido un nuevo nivel de complejidad en la seguridad defensiva.

Frente a este escenario, el presente proyecto de investigación propone el estudio y desarrollo de un sistema capaz de analizar o descifrar tráfico cifrado en redes de datos con fines de detección de amenazas, sin comprometer los principios éticos ni legales que rigen la privacidad digital. Esta propuesta es altamente pertinente en contextos corporativos, institucionales y gubernamentales, donde el equilibrio entre privacidad y seguridad debe ser cuidadosamente gestionado.

Desde una perspectiva ética, uno de los principales retos del análisis de tráfico cifrado radica en no violar los derechos fundamentales de los usuarios. En muchos países, leyes como el Reglamento General de Protección de Datos (GDPR) (GDPR Compliance. Palo Alto Networks. 2021) en Europa o la Ley de Privacidad del Consumidor de California (CCPA) en EE.UU., exigen que cualquier intervención sobre los datos personales deba estar justificada, ser proporcional y estar protegida por mecanismos técnicos y administrativos. Por tanto, este proyecto no busca vulnerar el cifrado per se, sino más bien explorar alternativas que permitan inferir comportamientos maliciosos utilizando metadatos, patrones de tráfico, firmas estadísticas y técnicas de inteligencia artificial que no requieran necesariamente acceder al contenido cifrado.

Desde el punto de vista técnico, la justificación también se sostiene en la necesidad de innovar en métodos de detección adaptados al contexto actual de redes cifradas. Las técnicas emergentes de análisis de tráfico cifrado basadas en aprendizaje automático y redes neuronales han demostrado cierto potencial para identificar comportamientos anómalos basándose en características externas del tráfico, como la frecuencia de paquetes, el tamaño de los datos, los intervalos de tiempo entre transmisiones y el uso de puertos y protocolos. Estas técnicas, aunque incipientes, pueden representar una vía eficaz para desarrollar sistemas que detecten amenazas sin necesidad de descifrar completamente el contenido de los paquetes, disminuyendo así los riesgos asociados al descifrado total, como el aumento del uso de recursos computacionales, la exposición accidental de datos sensibles o la introducción de nuevas vulnerabilidades.

Por último, desde una perspectiva práctica, el desarrollo de soluciones efectivas para analizar tráfico cifrado puede proporcionar beneficios concretos a una amplia gama de organizaciones. Empresas que manejan propiedad intelectual, instituciones bancarias, organismos de salud, infraestructuras críticas y dependencias gubernamentales necesitan herramientas de defensa avanzadas que les permitan anticipar ataques y proteger su información, sin comprometer el cumplimiento normativo (Aceto, G., et al. 2020). En este contexto, la capacidad de analizar tráfico cifrado con fines de seguridad puede ser vista no solo como una necesidad técnica, sino también como una ventaja competitiva y un factor de resiliencia institucional.

CAPITULO II

2. MARCO REFERENCIAL

2.1 Antecedentes

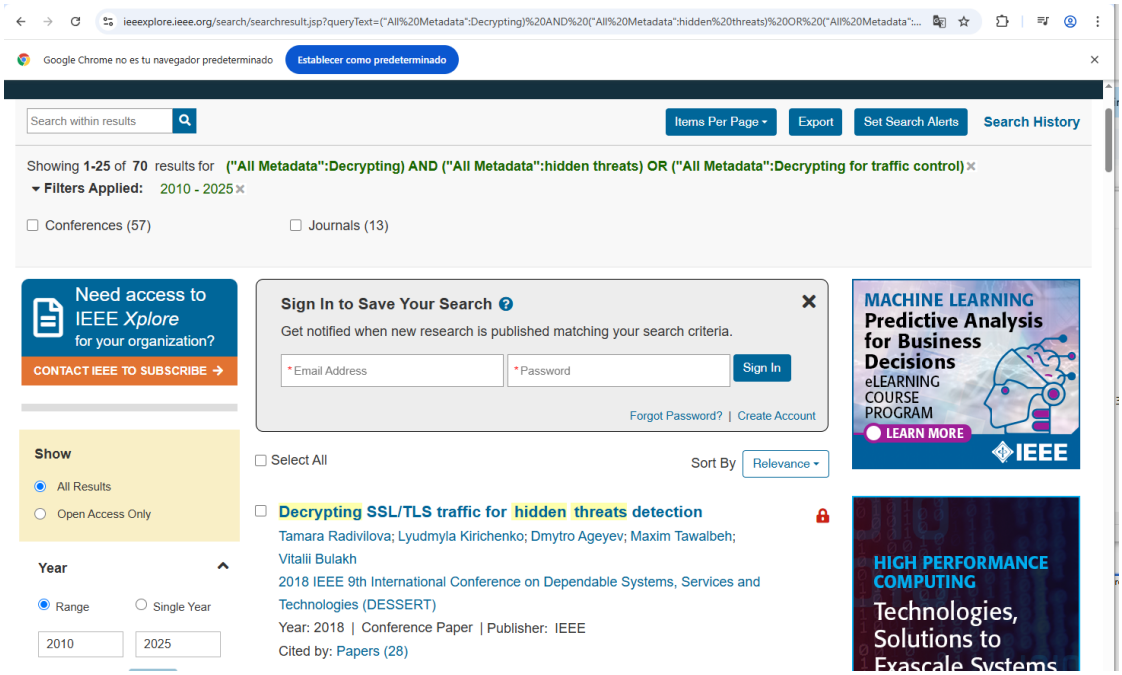
Se ha reforzado el presente trabajo de investigación con una búsqueda preliminar de estudios previos en páginas que contienen documentación científica, se ha realizado dicha búsqueda mediante un método estandarizado.

Con el fin de contestar la siguiente interrogante de investigación: Al implementar un proceso de descifrado de tráfico de red mediante el uso de certificados intermedios se mejorara el control la seguridad y la gestión de accesos a los servicios de red empresariales, tanto internos como externos? Se ha trabajado una cadena de búsqueda de artículos científicos, con los siguientes parámetros: ("All Metadata":Decrypting) AND ("All Metadata":hidden threats) OR ("All Metadata":Decrypting for traffic control).

La cadena de búsqueda se ejecutó en la página web:"https://ieeexplore.ieee.org/", la misma que contiene una base de datos de artículos científicos con el respaldo del "Instituto de Ingenieros Eléctricos y Electrónicos", misma que mostro un total de 70 publicaciones entre conferencias, libros y revistas. Se incluyó a trabajos relacionados con descifrado para verificar y controlar tráfico cifrado, publicados en los últimos 15 años, se muestra en la siguiente gráfica:

Figura 1

Resultado de la búsqueda en la base de datos IEEE Xplore



Los mecanismos tradicionales son controles de seguridad perimetral como antivirus antimalware IPS, implementados en casi todas las empresas, la mejora propuesta es ampliar la capacidad de análisis de estos controles dándoles la posibilidad de leer tráfico que normalmente se encuentra cifrado y por tanto no es analizable y controlable.

Se analizó los artículos con el fin de encontrar los que son afines al tema que se está desarrollando, se escogió 5 artículos de los cuales se presenta un análisis a continuación:

En el artículo “Análisis comparativo de arquitecturas para clasificar tráfico TLS malicioso y benigno” (Selian et al., 2024). Se analiza que: “el crecimiento del tráfico de Internet cifrado ha presentado importantes desafíos a la hora de detectar y clasificar actividades maliciosas. Transport Layer Security (TLS), un protocolo para comunicaciones seguras, se adopta ampliamente, pero ha creado puntos ciegos para las

herramientas tradicionales de ciberseguridad que dependen de la inspección del contenido del tráfico. Este estudio aborda el desafío evaluando el uso de tres modelos de aprendizaje automático (un bosque aleatorio, una red de memoria a corto plazo (LSTM) y una red neuronal profunda completamente conectada (FDCNN)) para clasificar el tráfico TLS en categorías benignas y maliciosas. Utilizando el conjunto de datos CIC-IDS-2017, estos modelos aprovechan características como el tamaño del paquete, el tiempo y la frecuencia de conexión, lo que permite la clasificación sin descifrar el tráfico. Los resultados experimentales demuestran que el modelo de bosque aleatorio logra la mayor precisión (99,02%), seguido por el FDCNN (98,75%) y el LSTM (98,00%). Cada modelo muestra fortalezas en áreas específicas, con el bosque aleatorio sobresaliendo en el manejo de clases desequilibradas, el FDCNN capturando patrones complejos y el LSTM identificando dependencias temporales. Estos hallazgos contribuyen al avance de la clasificación del tráfico TLS y resaltan el potencial del aprendizaje automático para abordar los desafíos del análisis del tráfico cifrado."

En el estudio "de Identificación de tráfico malicioso (Chen et al., 2022) Se menciona que "Al convertir el tráfico de red en imágenes y utilizar métodos de predicción de red convolucionales, se puede mejorar de manera efectiva la precisión del tráfico de red malicioso. Dado que el cifrado de tráfico TLS se utiliza cada vez en más aplicaciones de red, al tiempo que se protege la seguridad y la privacidad, los atacantes de red pueden lograr el propósito de evadir la detección cifrando el tráfico malicioso. El método tradicional de utilizar un firewall y software antivirus para descifrar la clave de cifrado para acceder a los datos cifrados no solo es ineficiente y destruye el propósito original del cifrado de proteger la privacidad, sino que también cuando la clave no se puede descifrar, la capacidad de descifrado del método tradicional es insuficiente. En este artículo, se

propone un método para transformar el tráfico de la red en imágenes de huellas dactilares de la red sin descifrar los datos cifrados y luego introducir las imágenes en una red neuronal convolucional para que la predicción logre la clasificación del tráfico malicioso. Los resultados experimentales muestran que el método de identificación de imágenes de huellas dactilares de red mediante CNN tiene alta precisión y capacidad de predicción."

Se analiza el estudio "FORTUNATE (Andrade et al., 2024): Descifrar y clasificar malware mediante secuencias de instrucciones de longitud variable" (César A. B. Andrade; Geraldo P. Rocha Filho; Rodolfo I. Meneguette; João Paulo A. Maranhão; Ricardo Sant'Ana; Julio Cesar Duarte, 2024)Se indica que "Después de identificar un artefacto como malware, surge el desafío adicional de clasificarlo correctamente en una familia específica. Esto plantea el desafío de clasificar el malware en medio de una complejidad creciente y un volumen cada vez mayor de amenazas cibernéticas. Por lo tanto, presentamos FORTUNATE, un marco que emplea secuencias de instrucciones de longitud variable para clasificar el malware de manera más eficiente y precisa, enfocándose en malware real y activo. Al introducir métodos efectivos para extraer códigos de operación y su representación en los vectores más pequeños posibles, FORTUNATE supera las limitaciones de enfoques anteriores, permitiendo la identificación correcta de malware en sus respectivas familias, evitando al mismo tiempo redundancias en los datos. Los resultados alcanzados con FORTUNATE demuestran avances tanto en precisión como en eficiencia computacional, consolidándolo como una contribución significativa al campo de la ciberseguridad."

En el estudio "Descifrado transparente de red de flujo criptográfico teniendo en cuenta la prestación de servicios en el borde" de los autores (Hiraga & Nishi, 2021) se

indica que “La difusión de los dispositivos de Internet de las cosas (IoT) y las comunicaciones de alta velocidad, como 5G, hace que sus servicios sean ricos y diversos. Por lo tanto, es deseable realizar funciones de servicios enriquecidos de forma transparente y utilizar entornos informáticos de vanguardia de forma flexible en ubicaciones intermedias de Internet, desde la perspectiva de un sistema de red. Cuando se logra este tipo de entorno de computación de borde, los nodos de IoT como dispositivos finales de Internet pueden utilizar completamente los sistemas de computación de borde y los sistemas de nube sin ningún cambio, como cambiar las direcciones IP de destino entre ellos, junto con el mantenimiento del protocolo para la conmutación. Sin embargo, cuando la transferencia de datos en la comunicación está cifrada, es necesario un método de descifrado en el borde para realizar estos servicios de borde transparentes. En este estudio, se ha propuesto un método transparente de intercambio de claves común con un servicio en la nube como nodo de destino de un par de comunicaciones, para descifrar de forma transparente un flujo de comunicación cifrado con una capa de sockets seguros en el área del borde. Esto permite que los dispositivos finales estén libres de cambios y actualizaciones para comunicarse con el nodo de destino.”

En el estudio “Descifrar el tráfico SSL/TLS para detectar amenazas ocultas” (Radivilova et al., 2018) “El artículo presenta un análisis de los principales mecanismos de descifrado del tráfico SSL/TLS. También se consideran los métodos y tecnologías para detectar actividad maliciosa en el tráfico cifrado que utilizan las empresas líderes. Además, se desarrolla, prueba y propone el enfoque para interceptar y descifrar el tráfico transmitido a través de SSL/TLS. El método desarrollado ha sido automatizado y puede utilizarse para la escucha remota de la red, lo que permitirá descifrar los datos transmitidos en un modo cercano al tiempo real”

Conclusión de la revisión de literatura:

En base a los estudios mencionados anteriormente se genera la siguiente tabla en la que se resume estudios sobre descifrado para análisis de tráfico:

Tabla 1

Proyectos descifrado

Articulo No.	Autor	Año de Publicación	Tipo de organización estudiada	Factores de éxito	Problemas encontrados
1	Restu Alsyafiq Selian; Muhammad Naufal Azzahri; Sayed Muchallil; Yudha Nurdin; Razief Perucha Fauzie Afidh; Khairul Umam	2024	Empresarial	Clasificación de tráfico usando varios métodos de aprendizaje automático	Los patrones pueden ser complejos
2	Jianxi Chen; Jiahao Huang; Xinghua Lu	2022	Empresarial	Uso de red neuronal red neuronal convolucional para que la predicción logre la clasificación del tráfico malicioso l para que la predicción logre la clasificación del tráfico malicioso	Más tiempo de análisis
3	César A. B. Andrade; Geraldo P. Rocha Filho; Rodolfo I. Meneguette; João Paulo A. Maranhão; Ricardo Sant'Ana; Julio Cesar Duarte	2024	Empresarial	Clasificación de malware una vez descifrado	Uso de herramienta especifica FORTUNATE

4	Hiroki Hiraga; Hiroaki Nishi	2021	Empresarial	Descifrar de forma transparente un flujo de comunicación cifrado con una capa de sockets seguros en el área del borde.	Se descifra en los dispositivos de borde
5	Tamara Radivilova; Lyudmyla Kirichenko; Dmytro Ageyev; Maxim Tawalbeh; Vitalii Bulakh	2018	Empresarial	Se usa para la escucha remota de la red, lo que permitirá descifrar los datos transmitidos en un modo cercano al tiempo real	Método solo para TLS /SSL

Nota. Elaboración propia (2026).

De lo analizado en estos estudios, el descifrado puede ser complejo pero ayuda a realizar mejores controles

2.2 Marco Teórico

2.2.1 Antecedentes

Se busca descifrar el tráfico en la red para verificar si existen amenazas que se ocultan bajo encriptación igualmente proxys de navegación que no pueden ser detectados por los equipos de seguridad debido a que el tráfico que generan viaja cifrado con el fin de aplicar medidas de aseguramiento y medidas de control.

2.2.2 Descifrado de tráfico de red

Arquitectura X.509 infraestructura de clave pública

Los certificados X.509 son parte integrante de la Infraestructura de Clave Pública (PKI), que proporciona el marco para gestionar los certificados digitales en los protocolos

de Seguridad de la Capa de Transporte (TLS) (Cooper et al., 2008). La PKI establece la confianza a través de un sistema jerárquico de Autoridades de Certificación (CA), responsables de emitir, validar y revocar certificados (Cooper et al., 2008).

Pasos en el flujo de trabajo de certificados X.509

Emisión de certificados: El proceso comienza con una Solicitud de Firma de Certificado (CSR), en la que la entidad genera un par de claves pública-privada y envía la clave pública a una CA de confianza. La CA verifica la identidad de la entidad y firma el certificado con su clave privada, incrustando la clave pública del certificado junto con otros datos de identidad (Cooper et al., 2008).

Verificación y establecimiento de la confianza: Cuando un cliente, como un navegador web, recibe un certificado X.509, verifica la firma digital del certificado utilizando la clave pública de la CA. Se valida una cadena de confianza, empezando por el certificado de la entidad final, pasando por las CA intermedias y, finalmente, hasta una CA raíz de confianza (Cooper et al., 2008).

Cifrado y comunicación segura: La clave pública del certificado permite enviar datos cifrados de forma segura al titular del certificado, que puede descifrarlos utilizando su clave privada. Del mismo modo, el titular del certificado puede firmar digitalmente los datos con su clave privada, y el destinatario puede verificar la firma utilizando la clave pública (Stallings, 2017).

Verificación continua: Se supervisa continuamente la validez de los certificados. Mecanismos como las Listas de Revocación de Certificados (CRL) y el Protocolo de

Estado de Certificados en Línea (OCSP) garantizan que los certificados comprometidos o caducados se invaliden rápidamente (Cooper et al., 2008).

Cadena de confianza

La estructura jerárquica de los certificados X.509 permite una «cadena de confianza». Una CA raíz ancla la confianza emitiendo certificados de CA, que se utilizan para verificar los certificados intermedios y los certificados de entidad final. Este enfoque por capas garantiza que incluso las redes a gran escala puedan mantener una comunicación segura (Cooper et al., 2008).

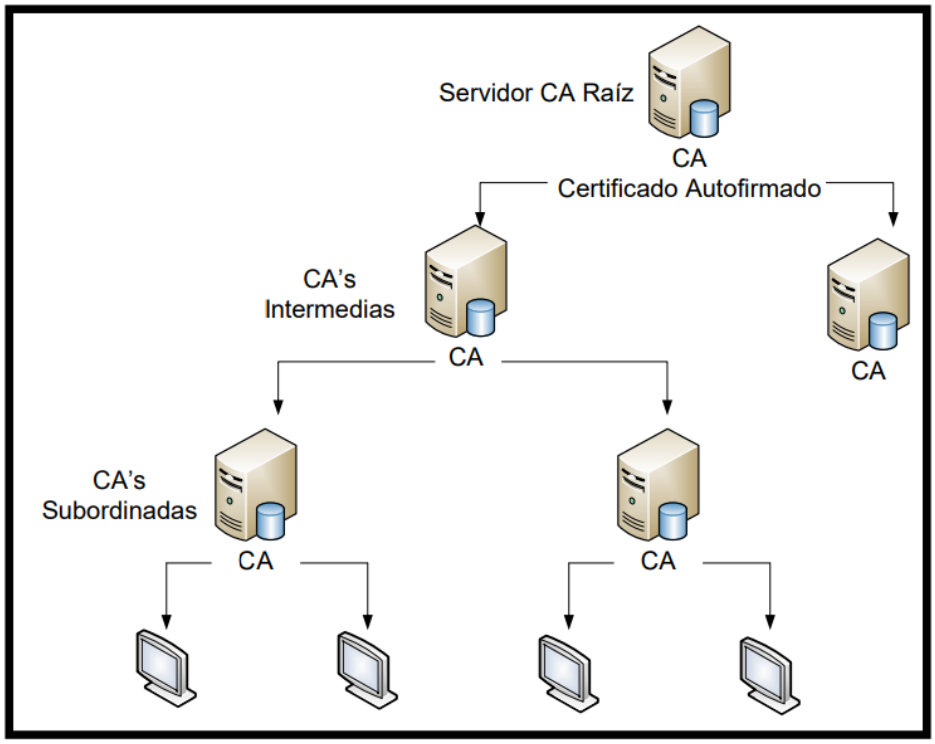
Autoridad de Certificación (CA)

Es una entidad imparcial en quien emisor y receptor confían mutuamente, aunque ellos no se conozcan con anterioridad (tercero de confianza), y podría ser considerada como un notario electrónico que avala la comunicación entre entidades legítimas (Adams & Lloyd, 2003). Se encarga de verificar y acreditar la identidad de un usuario o dispositivo, a través de la emisión de un certificado digital que lo vincula con una clave pública, así como de su publicación en directorios, su renovación y la revocación o suspensión en caso de expiración o compromiso de la clave privada (Cooper et al., 2008).

La Figura muestra una arquitectura jerárquica de CAs en la que la fiabilidad radica en la autoridad raíz, que genera su propio certificado avalado por su firma digital (autocertificación), convirtiéndose en el respaldo en el que todos los usuarios de un entorno local, ciudad o país confían. Esta CA emite certificados firmados digitalmente a autoridades intermedias, habilitándolas para certificar a autoridades subordinadas, de menor jerarquía en la arquitectura; finalmente, estas últimas certifican a usuarios y dispositivos finales tras un proceso de registro y verificación (Cooper et al., 2008).

Figura 2

Arquitectura Jerárquica de Certificación



Nota. (Vásquez, 2015)

Autoridad de Registro (RA)

Las CAs desempeñan diversas funciones para certificar a autoridades finales o intermedias, pero cuando la PKI cubre entornos con gran demanda de usuarios o con dependencias geográficamente distantes, resulta complicado dar atención eficiente a todas las peticiones de certificación, e incluso la CA podría colapsar por la sobrecarga de actividades (Adams & Lloyd, 2003).

Por tal motivo, existen ocasiones en las que esta entidad delega a una Autoridad de Registro (RA) el proceso de gestión de registro y autenticación de usuarios que soliciten certificación. La ventaja de utilizar esta autoridad adicional es garantizar escalabilidad en el servicio, al implementarse tantas como sean necesarias para atender la

mayoría de peticiones de certificación en distintos lugares, limitando a la CA a certificar únicamente a usuarios y dispositivos finales que han sido autenticados y autorizados previamente por la RA (Cooper et al., 2008).

La RA constituye el vínculo entre el usuario final y la CA, atendiendo solicitudes de registro, certificación, recuperación de claves o certificados, asociación entre la clave pública y el titular del certificado, y gestión del ciclo de vida de los certificados, resaltando la revocación, expiración, renovación, reemisión del par de claves criptográficas o actualización de información del certificado (Ford & Baum, 2001).

Directorio de Publicación de Certificados y Listas de Revocación de Certificados (CRL)

Son servicios empleados en entornos PKI para almacenar los certificados emitidos por la CA, manteniéndolos disponibles para el acceso de usuarios que necesiten recuperarlos con el objetivo de establecer comunicaciones seguras. Esto contribuye a la administración de certificados al posibilitar su distribución y control de estado de vigencia mediante listas de revocación (Cooper et al., 2008).

Los certificados digitales son emitidos para ser válidos durante un periodo de tiempo; sin embargo, existen diversas razones que pueden invalidarlos antes de su expiración, (Cooper et al., 2008). La CA publica una lista en la que constan aquellos certificados que han sido invalidados, Lista de Revocación de Certificados (CRL) (Housley et al., 2002).

Uso de certificados para descifrado

Certificados X.509

Los certificados X.509 establecen confianza entre un cliente y un servidor para establecer una conexión SSL. Un cliente que intenta autenticar un servidor (o un servidor que autentica a un cliente) conoce la estructura del certificado X.509 y, por lo tanto, sabe cómo extraer información de identificación sobre el servidor de los campos dentro del certificado, como el FQDN o la dirección IP (llamada nombre común o CN dentro del certificado) o el nombre de la organización, departamento o usuario para el cual se emitió el certificado. Una autoridad certificadora (CA) debe emitir todos los certificados. (Wikipedia contributors. 2023). Después de que la CA verifica un cliente o servidor, emite el certificado y lo firma con una clave privada.

Las claves son cadenas de números que normalmente se generan mediante una operación matemática que involucra números aleatorios y números primos grandes. Las claves transforman cadenas (como contraseñas y secretos compartidos) de texto plano no cifrado a texto cifrado y de texto cifrado a texto plano no cifrado. Las claves pueden ser simétricas (se usa la misma clave para cifrar y descifrar) o asimétricas (se usa una clave para cifrar y una clave matemáticamente relacionada para descifrar). Cualquier sistema puede generar una clave.

Para los procesos de Decryption los certificados utilizados son:

Forward Trust (Used for SSL Forward Proxy decryption)

El certificado que el firewall presenta a los clientes durante el descifrado si el sitio al que el cliente intenta conectarse tiene un certificado firmado por una CA en la que confía el firewall. Para configurar un certificado Forward Trust en el firewall para

presentarlo a los clientes cuando el certificado del servidor esté firmado por una CA confiable (Palo Alto Networks. 2023).

Forward Untrust (Used for SSL Forward Proxy decryption)

De forma predeterminada, el firewall determina el tamaño de clave que se utilizará para el certificado del cliente en función del tamaño de clave del servidor de destino. Sin embargo, puede configurar el tamaño de clave para los certificados del servidor proxy SSL.

SSL Inbound Inspection

El certificado que el firewall presenta a los servidores durante el descifrado si el sitio al que el cliente intenta conectarse tiene un certificado firmado por una CA en la que el firewall no confía. Para configurar un certificado Forward Untrust en el firewall

2.2.3 Control de seguridad de tráfico de red

AL estar el tráfico cifrado no se puede aplicar controles normales de acceso en la parte de URL filtering, Threat y WildFire

Después de identificar un artefacto como malware,(De Carné de Carnavalet, X., y van Oorschot, P. C. ,2020)surge el desafío adicional de clasificarlo correctamente en una familia específica. Esto plantea el desafío de clasificar el malware en medio de una complejidad creciente y un volumen cada vez mayor de amenazas cibernéticas. Por lo tanto, presentamos FORTUNATE, un marco que emplea secuencias de instrucciones de longitud variable para clasificar el malware de manera más eficiente y precisa, enfocándose en malware real y activo. Al introducir métodos efectivos para extraer códigos de operación y su representación en los vectores más pequeños posibles, FORTUNATE supera las limitaciones de enfoques anteriores, permitiendo la

identificación correcta de malware en sus respectivas familias, evitando al mismo tiempo redundancias en los datos. Los resultados alcanzados con FORTUNATE demuestran avances tanto en precisión como en eficiencia computacional, consolidándolo como una contribución significativa al campo de la ciberseguridad.

2.2.4 Gestión de accesos empresariales de tráfico cifrado

AL estar el tráfico cifrado (Radivilova, T., Kirichenko, L., Ageyev, D., Tawalbeh, M., y Bulakh, V., 2019). no se puede aplicar controles de comportamiento de tráfico, como la calendarización de accesos a URL específicos o la asignación de anchos de banda para consumo de los mismos, por parte de los usuarios, por lo que el descifrado es un proceso que permite la lectura de dicho tráfico con el fin de procederé a aplicar los controles.

El protocolo de seguridad de la capa de transporte (TLS), que evolucionó a partir de la capa de sockets seguros (SSL), y el protocolo de shell seguro (SSH) aseguran la comunicación entre dos entidades, como un servidor web y un cliente. Mientras que SSL/TLS suele proteger las comunicaciones basadas en la web, SSH suele proteger el acceso remoto a servidores y dispositivos. Estos protocolos utilizan criptografía de clave pública y privada para establecer conexiones seguras. Cifran los datos de una manera que los hace insignificantes para cualquier entidad que carezca del certificado y las claves necesarias para establecer la confianza y decodificar los datos. Sin embargo, la privacidad y la integridad que proporciona el cifrado pueden ser explotadas. Por ejemplo, supongamos que un atacante instala malware en un sitio web HTTPS y los empleados visitan el sitio y, sin saberlo, descargan malware. El malware puede usar el computador del empleado infectado para moverse lateralmente a través de la red y comprometer otros sistemas.

La difusión de los dispositivos de Internet de las cosas (IoT) y las comunicaciones de alta velocidad, como 5G, hace que sus servicios sean ricos y diversos (Cisco, 2020; Shi et al., 2016). Por lo tanto, es deseable realizar funciones de servicios enriquecidos de forma transparente y utilizar entornos informáticos de vanguardia de forma flexible en ubicaciones intermedias de Internet, desde la perspectiva de un sistema de red (Satyanarayanan, 2017). Cuando se logra este tipo de entorno de computación de borde, los nodos de IoT como dispositivos finales de Internet pueden utilizar completamente los sistemas de computación de borde y los sistemas de nube sin ningún cambio, como cambiar las direcciones IP de destino entre ellos, junto con el mantenimiento del protocolo para la conmutación (Shi et al., 2016). Sin embargo, cuando la transferencia de datos en la comunicación está cifrada, es necesario un método de descifrado en el borde para realizar estos servicios de borde transparentes (Rescorla, 2018). En este estudio, se ha propuesto un método transparente de intercambio de claves común con un servicio en la nube como nodo de destino de un par de comunicaciones, para descifrar de forma transparente un flujo de comunicación cifrado con una capa de sockets seguros en el área del borde. Esto permite que los dispositivos finales estén libres de cambios y actualizaciones para comunicarse con el nodo de destino (Rescorla, 2018; Satyanarayanan, 2017).

2.2.5 Fundamentos del cifrado en redes de datos

El cifrado en redes de datos es una técnica esencial para garantizar la seguridad de la información durante su transmisión. Su propósito principal es evitar que usuarios no autorizados accedan al contenido de los datos mientras estos están en tránsito (Stallings, 2017). Existen dos grandes tipos de cifrado utilizados en redes: el cifrado simétrico, donde la misma clave se usa para cifrar y descifrar los datos (por ejemplo,

AES), y el cifrado asimétrico, que emplea un par de claves pública y privada (por ejemplo, RSA) (Menezes et al., 1996). Protocolos como SSL/TLS combinan ambos métodos para ofrecer conexiones seguras, como ocurre con HTTPS, que cifra la comunicación entre navegadores y servidores web (Rescorla, 2018).

El uso de estos protocolos ha aumentado considerablemente en la última década. Según informes de Google y Mozilla, más del 90% del tráfico web global se encuentra actualmente cifrado (Google, 2023; Mozilla, 2023). Además, el uso de VPNs (Virtual Private Networks) también ha crecido tanto en entornos corporativos como personales, encapsulando y cifrando todo el tráfico generado desde un dispositivo (Kurose & Ross, 2021). Este nivel de cifrado masivo, aunque beneficioso para la privacidad, representa un gran desafío para las tareas de monitoreo y detección de amenazas en redes (Anderson, 2020).

Mecanismos tradicionales de análisis de tráfico

Antes de la adopción masiva de cifrado de extremo a extremo (TLS 1.3, HTTPS Everywhere y VPNs), el análisis de tráfico se basaba en técnicas pasivas y activas relativamente sencillas (Kurose y Ross, 2021)

Tabla 2

Mecanismos tradicionales de análisis de tráfico

Mecanismo tradicional	Descripción	Herramientas representativas
Sniffing de paquetes	Captura de tráfico plano para inspeccionar encabezados y contenido.	Wireshark, tcpdump
Análisis de encabezados	Revisión de información L2–L4 (IP, puertos, flags, TTL, secuencias TCP).	NetFlow, sFlow, ntopng
Deep Packet Inspection (DPI)	Inspección profunda del contenido de los paquetes no cifrados.	Snort, Suricata, Bro/Zeek
Análisis estadístico	Identificación de patrones de comportamiento basados en volumen, tiempo y destino.	MRTG, Cacti, Nagios

Nota. Elaboración propia (2026).

Implementaciones para escenarios con cifrado

Con la adopción de TLS, VPN, SSH y otros mecanismos de cifrado, las técnicas tradicionales de DPI dejaron de ser suficientes (Rescorla, 2018). Se adoptaron nuevas estrategias:

Tabla 3

Implementaciones para escenarios con cifrado

Estrategia	Descripción	Ejemplos / Implementaciones
SSL/TLS Interception (MITM autorizado)	Dispositivo intermedio descifra tráfico mediante certificados propios.	Blue Coat ProxySG, FortiGate SSL Inspection, Zscaler
Análisis de metadatos	Extracción de SNI, IPs destino, tiempos de conexión y tamaños de paquetes.	Zeek, NetFlow, Cisco Stealthwatch
JA3 Fingerprinting	Identificación de clientes TLS por huella digital de handshake.	Zeek con JA3 plugin, Security Onion
Desencriptación en endpoint	Recolectar datos en el cliente o servidor antes/después de cifrado.	EDR/agent based
TLS key logging	Uso de claves precompartidas o variables de entorno para descifrar tráfico capturado.	Wireshark + SSLKEYLOGFILE

Nota. Elaboración propia (2026).

Limitaciones de las implementaciones tradicionales

Las soluciones tradicionales presentan diversas limitaciones en entornos modernos altamente cifrados:

- Alto costo computacional al realizar inspección SSL/TLS masiva (Anderson, 2020).
- Problemas de privacidad y cumplimiento normativo, especialmente bajo regulaciones como GDPR o HIPAA (European Parliament & Council of the European Union, 2016).
- TLS 1.3 y ESNI dificultan los enfoques tradicionales de MITM debido al cifrado de más partes del handshake (Rescorla, 2018).
- Escalabilidad limitada en redes de gran tamaño y alto volumen de tráfico (Cisco, 2023).

Implementaciones Existentes

Las implementaciones actuales para el análisis de tráfico cifrado giran en torno a dispositivos y plataformas de seguridad de red que gestionan activamente el cifrado y la inspección del tráfico (Anderson, 2020).

Soluciones de Seguridad Perimetral

Firewalls de Próxima Generación (NGFW) / Sistemas de Prevención de Intrusiones (IPS):

Incluyen módulos de Inspección Profunda de Paquetes SSL/TLS (Deep SSL/TLS Inspection). Actúan como un proxy para descifrar el tráfico (tanto entrante como saliente), inspeccionar el contenido en busca de malware, intrusiones o violaciones de políticas, y posteriormente volver a cifrarlo antes de enviarlo a su destino (Scarfone & Hoffman, 2009; Palo Alto Networks, 2023).

Pasarelas de Seguridad Web (Secure Web Gateways - SWG):

Se centran en la inspección del tráfico web HTTPS para aplicar políticas de uso, prevención de pérdida de datos (DLP) y protección contra amenazas avanzadas (Gartner, 2022). Estas plataformas permiten controlar accesos web y detectar amenazas ocultas dentro del tráfico cifrado.

Herramientas de Análisis Específico

Wireshark:

Herramienta de código abierto ampliamente utilizada para la captura y análisis de paquetes de red. Puede implementarse para el descifrado en entornos controlados

mediante el uso de claves de sesión TLS o claves privadas, permitiendo analizar tráfico cifrado con fines de diagnóstico y monitoreo (Combs, 2023).

nProbe / Pandora NTA (Network Traffic Analyzer):

Herramientas orientadas principalmente al análisis de metadatos de tráfico utilizando tecnologías como NetFlow, sFlow e IPFIX. Estas soluciones permiten identificar patrones de comportamiento, anomalías y estadísticas de red, pudiendo complementarse con información proveniente de tráfico descifrado (ntop, 2023).

Métodos técnicos disponibles para lograr el descifrado para análisis de tráfico de red

Interceptación TLS/SSL autorizada (TLS interception / TLS proxy / "enterprise MITM")

Qué es: Un dispositivo o proxy en la red actúa como intermediario terminando la conexión TLS del cliente y estableciendo una nueva con el servidor. El proxy presenta un certificado emitido por una CA de confianza en la red (normalmente instalada por la organización en los endpoints).

Cómo funciona (alto nivel): el proxy recibe tráfico cifrado, descifra usando sus claves intermedias, inspecciona el contenido y lo vuelve a cifrar hacia el destino (Anderson, 2020). La inspección de contenido en tiempo real; útil para DLP, antivirus, cumplimiento. Rompe propiedad de extremo a extremo, afecta privacidad, problemas con certificate pinning, TLS 1.3 + ESNI/DoH/DoT reducen visibilidad; alto coste de CPU y complejidad.

Descifrado con claves privadas del servidor (server-side key access)

Qué es: usar la clave privada del servidor (o llaves de terminación TLS en load balancers) para descifrar captures de tráfico.

Cuándo es viable: cuando la organización controla el servidor y conserva las claves.

Limitación clave: si se usan cifrados con Forward Secrecy (p. ej. ECDHE), la clave privada por sí sola no permite descifrar sesiones pasadas; es necesario el secreto de sesión (o registro de claves) (Rescorla, 2018).

Exportación / registro de claves de sesión (key logging)

Qué es: registrar secretos ephemerales (pre-master / session keys) en el cliente o servidor durante la negociación TLS (p. ej. variables de entorno tipo SSLKEYLOGFILE) (Combs, 2023).y usarlos para descifrar capturas pcap en herramientas como Wireshark.

Ventaja: permite descifrar tráfico capturado sin MITM.

Limitación: requiere instalar o configurar software en los endpoints o servidores; no práctico a gran escala sin control centralizado.

Instrumentación en endpoints (endpoint telemetry / agents)

Qué es: recoger tráfico antes o después del cifrado dentro del endpoint mediante agentes EDR, agentes de red local o API de aplicaciones (Rose et al., 2020).

Ventajas: no rompe cifrado en tránsito; alto nivel de visibilidad sobre aplicaciones y procesos.

Contras: requiere despliegue masivo, mantenimiento, impacto en endpoints y consideraciones de privacidad.

Terminación TLS en perímetro/controlador (load balancers, WAFs, API gateways)

Qué es: terminar TLS en un punto controlado (load balancer, WAF, API gateway) donde se puede inspeccionar el contenido para análisis o filtrado antes de recifrar hacia servicios internos (Kurose & Ross, 2021).

Uso típico: entornos de nube y arquitecturas con gateway centralizado.

Consideración: diseño arquitectural preferible a MITM indiscriminado.

Análisis de metadatos y fingerprinting (sin descifrar contenido)

Qué es: analizar IPs destino, tiempos, tamaños de paquetes, SNI (cuando esté visible), JA3/JA3S (fingerprints TLS), HASSH (SSH), patrones de tráfico y flujos NetFlow/sFlow.

Ventajas: no invade privacidad del contenido; funciona con TLS 1.3; escalable.

Limitación: menos preciso para contenido; requiere modelos y correlación avanzada.

Casos de uso: detección de malware, exfiltración, comportamiento anómalo.

Uso de logs / telemetría de la infraestructura (servidores, proxies, aplicaciones)

Qué es: aprovechar logs de aplicaciones, proxies y servicios que ya procesan datos en claro (Anderson, 2020) (por ejemplo, logs de servidores web, registros de proxies, registros de aplicaciones).

Beneficio: no requiere descifrado de red; mantiene cadena de custodia y cumplimiento.

Compromiso de claves o explotación de vulnerabilidades (ataques y forense)

Descripción general: extracción de claves desde memoria, explotación de vulnerabilidades (p. ej. Heartbleed histórico), o extracción forense de discos/servidores.

Nota ética/legal: esto es técnicamente factible pero implica acciones ofensivas o intrusivas; no se deben realizar fuera de un marco legal y autorizado. Además, criptografía moderna con forward secrecy limita su efectividad para descifrar sesiones pasadas.

Ataques cripto/forzamiento (brute-force / avances criptográficos)

Descripción: intento de romper la criptografía por fuerza bruta o aprovechar vulnerabilidades matemáticas (Menezes et al., 1996).

Realidad práctica: para algoritmos modernos y parámetros correctos, inviable con recursos actuales; ataques teóricos (p. ej. computación cuántica) todavía no son prácticos a escala para romper RSA/ECDSA ampliamente desplegados hoy.

Computación segura y técnicas especiales (sin descifrar)

Cifrado homomórfico, SGX/Tee, privacidad diferencial, multi-party computation. Estas permiten operar sobre datos cifrados o protegidos sin revelar su contenido completo.

Uso: análisis permitido con fuertes garantías de privacidad; todavía costoso y complejo, pero ideal para escenarios regulatorios.

2.2.6 Impacto del cifrado en la ciberseguridad

El crecimiento del cifrado ha reducido la eficacia de las técnicas tradicionales de análisis de tráfico, como la inspección profunda de paquetes (Deep Packet Inspection, DPI). Esta técnica permitía a los sistemas de seguridad examinar el contenido completo

de los paquetes de red para identificar firmas maliciosas, patrones de comportamiento o actividades sospechosas (Scarfone & Hoffman, 2009). Sin embargo, con el contenido cifrado, el DPI queda limitado a analizar únicamente los encabezados visibles del protocolo y los metadatos de la conexión (Anderson, 2020).

Este fenómeno, conocido como el punto ciego del cifrado, ha sido explotado por atacantes para evadir la detección. Amenazas como malware cifrado, comunicaciones de comando y control (C2), phishing encriptado y exfiltración de datos mediante túneles seguros son cada vez más frecuentes (Cisco, 2023). Ante esto, las soluciones de seguridad deben evolucionar para mantener la visibilidad del tráfico sin comprometer los principios de privacidad (Conti et al., 2016).

2.2.7 Enfoques actuales para el análisis de tráfico cifrado

Frente a la imposibilidad de inspeccionar directamente el contenido cifrado sin incurrir en altos costos técnicos o violaciones legales, han surgido varias alternativas. Entre ellas destacan:

Análisis de metadatos: Se examinan características como la duración de la conexión, frecuencia de paquetes, tamaño de los datos, dirección IP, puerto de destino y comportamiento temporal del tráfico. Aunque no se accede al contenido, estos datos pueden revelar patrones anómalos o indicios de actividades maliciosas (Shbair et al., 2016).

Fingerprinting de protocolos cifrados: Mediante análisis estadísticos y heurísticos, es posible identificar el tipo de aplicación o protocolo utilizado, incluso si el contenido está cifrado. Herramientas como JA3 permiten generar huellas digitales TLS que pueden usarse para detectar malware que usa conexiones cifradas no estándar (Salesforce, 2017).

Machine Learning aplicado a tráfico cifrado: El uso de algoritmos de aprendizaje supervisado y no supervisado ha demostrado eficacia para clasificar y detectar actividades en tráfico cifrado. Estos modelos aprenden a partir de conjuntos de datos etiquetados que contienen flujos de tráfico legítimo y malicioso. Algoritmos como SVM, Random Forest y redes neuronales recurrentes (RNN) son comúnmente utilizados en este ámbito (Aceto et al., 2019).

Descifrado autorizada: En entornos corporativos, es posible implementar técnicas de descifrado mediante SSL/TLS Inspection usando proxies intermedios. Aunque efectiva, esta práctica puede presentar riesgos éticos, violaciones de normativas como el GDPR y problemas de rendimiento si no se gestiona adecuadamente (European Parliament & Council of the European Union, 2016).

2.2.8 Estado actual de la investigación

El análisis del tráfico (Anderson, B., & McGrew, D., 2017) cifrado sin descifrado directa es un campo en evolución. Investigaciones recientes se centran en optimizar modelos de aprendizaje automático que operen con datos cifrados, mejorar la precisión

de sistemas de clasificación basados en metadatos, y desarrollar arquitecturas híbridas que permitan visibilidad sin comprometer la privacidad.

Proyectos como Encrypted Traffic Analytics (ETA) de Cisco (Rehak, M., & Anderson, B., 2018). o estudios académicos en redes definidas por software (SDN) y sistemas de detección inteligentes han demostrado que es posible detectar amenazas en tráfico cifrado con tasas de acierto superiores al 90%, sin necesidad de acceder al contenido del mensaje. No obstante, estos enfoques aún enfrentan desafíos en cuanto a escalabilidad, falsos positivos, generalización de modelos y validación en escenarios reales.

2.2.9 Privacidad y protección de datos

Tabla 4

Privacidad y protección de datos

Elemento	Acción	Objetivo
Principio de minimización	Inspeccionar únicamente la información estrictamente necesaria.	Cumplimiento GDPR / privacidad.
Anonimización y pseudonimización	Aplicar técnicas para ocultar identificadores personales cuando sea posible.	Reducir exposición de datos sensibles.
Retención limitada	No se almacena datos descifrado s	Minimizar riesgos legales y de filtraciones.
Accesos controlados	Definir roles, permisos y autenticación fuerte para acceder a firewall, los datos descifrados, no son visibles.	Evitar abuso interno.
Auditorías periódicas	Revisar registros de acceso y uso de datos inspeccionados.	Accountability y trazabilidad.

Nota. Elaboración propia (2026).

Controles Legales y de Cumplimiento

Base Legal Explícita

La empresa debe asegurarse de que la inspección del tráfico tenga una base legal válida. Esto generalmente recae en:

- Interés Legítimo: Demostrar que la inspección es estrictamente necesaria para la seguridad de la red, la protección de activos (como la Prevención de Pérdida de Datos - DLP) o el cumplimiento normativo.
- Obligación Legal: Si la inspección es requerida por ley o regulaciones específicas del sector (p. ej., servicios financieros).

Política de Uso Aceptable (PUA)

Debe existir una política corporativa clara, accesible y obligatoria que:

- Notificación a los empleados explícitamente que su tráfico de red, incluyendo el cifrado, está sujeto a intercepción, descifrado, y análisis en los equipos de la compañía.
- Defina las reglas de uso aceptable de los recursos de red y las consecuencias del incumplimiento.

Normativas de Protección de Datos

Se debe garantizar el cumplimiento de regulaciones como el GDPR (Reglamento General de Protección de Datos de la UE) o leyes nacionales de protección de datos personales (como la Ley Orgánica de Protección de Datos Personales en Ecuador), lo cual implica:

- Minimización de Datos: Limitar el análisis del tráfico descifrado solo a lo estrictamente necesario para el objetivo de seguridad o cumplimiento definido.
- Confidencialidad: Garantizar que el personal que accede a los datos descifrados (que pueden incluir Datos de Identificación Personal - PII) esté debidamente autorizado, capacitado y sujeto a acuerdos de confidencialidad estrictos.

Controles de Privacidad y Éticos

Notificación y Consentimiento

Aunque la PUA establece la base legal, la transparencia total es fundamental para la confianza:

- Información Clara: Se debe informar a los empleados sobre cómo funciona la inspección (el concepto de MITM controlado) y qué datos se están inspeccionando.
- Certificado de Confianza: El certificado de la Autoridad Certificadora (CA) interna que permite el descifrado debe ser instalado en los equipos de la compañía. Se recomienda comunicar a los usuarios sobre la presencia de este certificado.

Descifrado Selectivo y Excepciones

Para proteger la privacidad y cumplir con las leyes, el descifrado no debe ser universal:

- Exclusión Legalmente Protegida: Configurar el dispositivo de inspección para excluir automáticamente el tráfico hacia categorías de alto riesgo de privacidad o legalmente protegidas, tales como:
    - Sitios web de banca en línea y servicios financieros (por riesgo de seguridad y cumplimiento PCI DSS).

    - Sitios web relacionados con la salud o historiales médicos (por cumplimiento HIPAA o leyes de salud locales).
    - Comunicaciones con servicios legales (abogado-cliente) y ciertos servicios gubernamentales.
- Criterios Específicos: El descifrado debe centrarse en los vectores de riesgo (p. ej., tráfico de descarga, sitios con mala reputación, aplicaciones no autorizadas) en lugar de en la actividad personal.

Controles Técnicos y de Auditoría

Gestión Segura de Claves

El sistema de inspección de tráfico con descifrado opera con las claves de sesión privadas. Es vital:

- Proteger la CA Interna: La clave privada de la CA interna que firma los certificados falsos debe estar protegida con la máxima seguridad, idealmente en un Módulo de Seguridad de Hardware (HSM), para evitar que un atacante la comprometa y la use para espiar a los empleados fuera de la red.
- Rotación de Claves: Implementar políticas para la rotación periódica de las claves utilizadas en el proceso de inspección.

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1 Descripción del área de estudio

La presente investigación se desarrolla en el ámbito de la seguridad informática aplicada a la protección del tráfico en la red. En la actualidad, el crecimiento exponencial de encriptación de malware (Anderson, B., 2017, junio 20). ha incrementado los riesgos de seguridad en las redes de datos, particularmente en los equipos de protección de frontera, donde no se pueden revisar los datos que transitan en la red. Los equipos de control necesitan saber descifrar el tráfico que entra y sale de la red, al estar en la frontera de la red hacia Internet, para poder proporcionar una protección real.

En este contexto, (Daniels, D. 2023, octubre 6). se ha identificado que muchas vulnerabilidades persisten debido a la ausencia de la posibilidad de revisión y control de tráfico para mitigar los riesgos en la frontera de la red. El descifrado por medio de certificados intermedios ofrece un medio de control de niveles de verificación que permite evaluar la seguridad en cada capa de la red. Incluyendo la salida a Internet. Los Controles que se pueden aplicar en el tráfico descifrado presentan una serie de facilidades prácticas que pueden ser integradas en el control del tráfico con el fin de evitar vulnerabilidades antes de que se manifiesten.

Por tanto,(Sachdeva, J. 2017, junio 20). el área de estudio se centra en la implementación de una metodología basada en esta descifrado para fortalecer la

seguridad en el tráfico de red, contribuyendo así a reducir riesgos como malware, virus, inyecciones de código, manipulación de sesiones, fuga de información sensible y otros vectores de ataque frecuentes.

Esta investigación se realizará en una institución pública, primero en una subred de una unidad en la que se dispone de equipos de seguridad perimetral que permiten realizar la implementación del descifrado y las pruebas de manejo de tráfico hacia aplicativos internos y hacia Internet.

3.2 Enfoque y tipo de investigación

La investigación se inscribe dentro del enfoque cuantitativo, dado que se pretende analizar de manera objetiva los resultados obtenidos antes y después de aplicar la metodología propuesta, a través de métricas de seguridad y verificaciones de los datos. Con el fin de probar la hipótesis mediante la recolección y análisis estadístico de datos, lo cual se alinea con la naturaleza evaluativa del presente trabajo.

En cuanto al tipo de investigación, esta es de tipo aplicada y descriptiva. Es aplicada porque busca ofrecer una solución práctica y funcional a un problema real identificado en la falta de visibilidad del tráfico en red. Es descriptiva porque se pretende identificar, clasificar y analizar vulnerabilidades comunes, así como establecer su correspondencia con los controles de seguridad que se pueden aplicar una vez descifrado en tráfico.

3.3 Procedimiento de investigación

El proceso metodológico se organizará en fases secuenciales:

La falta de visibilidad del tráfico cifrado impide poder hacer un análisis del mismo, tanto para control como para asignación de reglas, existen amenazas que se ocultan bajo encriptación, como proxys de navegación que no pueden ser detectados por los equipos de seguridad, debido a que el tráfico que generan viaja cifrado. Lo que no permiten que las organizaciones detecten las amenazas de seguridad que se encuentran en su interior.

De acuerdo a los objetivos definidos para esta investigación, se plantean tres fases, las mismas que enmarcan el alcance de esta propuesta.

Figura 3

Implementación de un sistema de descifrado de tráfico de red Implementación de un sistema de descifrado de tráfico de red



Nota. Elaboración propia (2026).

Fase 1 Implementación de sistema de descifrado con certificados

En la primera fase se realizará la implementación de un sistema de descifrado de tráfico de red mediante el uso de certificados intermedios dentro de una subred empresarial específica. El propósito de esta implementación será permitir la inspección, análisis y control del tráfico cifrado que circula en la red corporativa.

El despliegue inicial se efectuará en una unidad piloto de la organización, con el objetivo de evaluar el funcionamiento de la solución, identificar posibles incidencias y analizar su impacto operativo antes de considerar su escalabilidad hacia las demás unidades institucionales.

Fase 2 Desarrollo de reglas de controles de acceso

Una vez habilitada la visualización y análisis del tráfico descifrado, se procederá al desarrollo e implementación de reglas de control de acceso basadas en el comportamiento y características del tráfico identificado.

Estas reglas tendrán como finalidad fortalecer la seguridad de la red empresarial mediante la restricción, autorización y monitoreo del acceso a servicios y recursos corporativos, permitiendo aplicar políticas de seguridad más precisas y alineadas con las necesidades de la organización.

Fase 3 Evaluación de la efectividad del sistema de descifrado

En la fase final se evaluará la efectividad del sistema de descifrado y de las reglas de control de acceso implementadas, con el propósito de determinar el impacto de la solución en la mejora de la seguridad de la red empresarial.

Para esta evaluación se considerarán diversos indicadores técnicos, entre ellos: el porcentaje de tráfico identificado como SSL/TLS, el tráfico web clasificado y analizado, la cantidad de amenazas detectadas, el volumen de contenido inspeccionado, el consumo de CPU del sistema. Los resultados obtenidos permitirán medir el desempeño de la solución y su viabilidad para una implementación a mayor escala.

3.4 Consideraciones bioéticas

La presente investigación, aunque no involucra experimentación directa con seres humanos, contempla aspectos bioéticos relacionados con la inspección y análisis del tráfico de red empresarial, debido a que los procesos de descifrado SSL/TLS pueden involucrar metadatos, registros de navegación, identificadores de usuario y eventos asociados al uso de servicios de red.

En este contexto, el desarrollo e implementación de la solución se fundamentará en los principios de confidencialidad, privacidad, integridad y uso responsable de la información. La inspección del tráfico será utilizada exclusivamente con fines de seguridad institucional, orientados a fortalecer los mecanismos de control, monitoreo y gestión de accesos a los servicios empresariales.

Asimismo, se aplicarán criterios de minimización de datos, se excluirán categorías de información sensible, limitando el análisis únicamente a la información estrictamente necesaria para la identificación de amenazas, verificación de políticas de seguridad y evaluación del comportamiento del tráfico de red. La forma en que trabaja el análisis hace que no exista almacenamiento permanente del contenido descifrado, evitando así riesgos asociados a exposición o uso indebido de información sensible.

De igual manera, por la forma en que se realiza la inspección no pone a la vista humana ningún dato en el proceso de inspección y análisis

La investigación también considerará el cumplimiento de las políticas institucionales de seguridad de la información y las normativas aplicables en materia de protección de datos y acceso autorizado a sistemas informáticos. Finalmente, se procurará que la implementación del sistema no afecte la disponibilidad de los servicios de red ni vulnere los derechos de privacidad de los usuarios dentro del entorno corporativo.

Se establecerán medidas estrictas para preservar la confidencialidad de la información a la que se tenga acceso. El trabajo cumplirá con los principios de ética profesional, evitando el plagio, la alteración de datos y cualquier práctica deshonesta.

Todo el conocimiento generado será compartido con fines académicos, bajo una óptica de responsabilidad social, promoviendo la utilización de la solución para mitigar los riesgos actuales en ciberseguridad.

CAPÍTULO IV

4 RESULTADOS Y EVALUACION

4.1 Escenario de implementación

Se proyecta la implementación de los sistemas de descifrado de tráfico de red para toda la red empresarial, la misma que brinda servicios de Internet a sus usuarios internos, y que brinda servicios de aplicaciones institucionales para usuarios internos y externos.

Las pruebas iniciales para el tráfico outbound se llevaron a cabo en una agencia de la empresa y las pruebas para el tráfico inbound se llevaron a cabo en dos de los equipos principales de publicación de servicios, esto con el objetivo de analizar y controlar el tráfico de red cifrado tanto saliente como entrante.

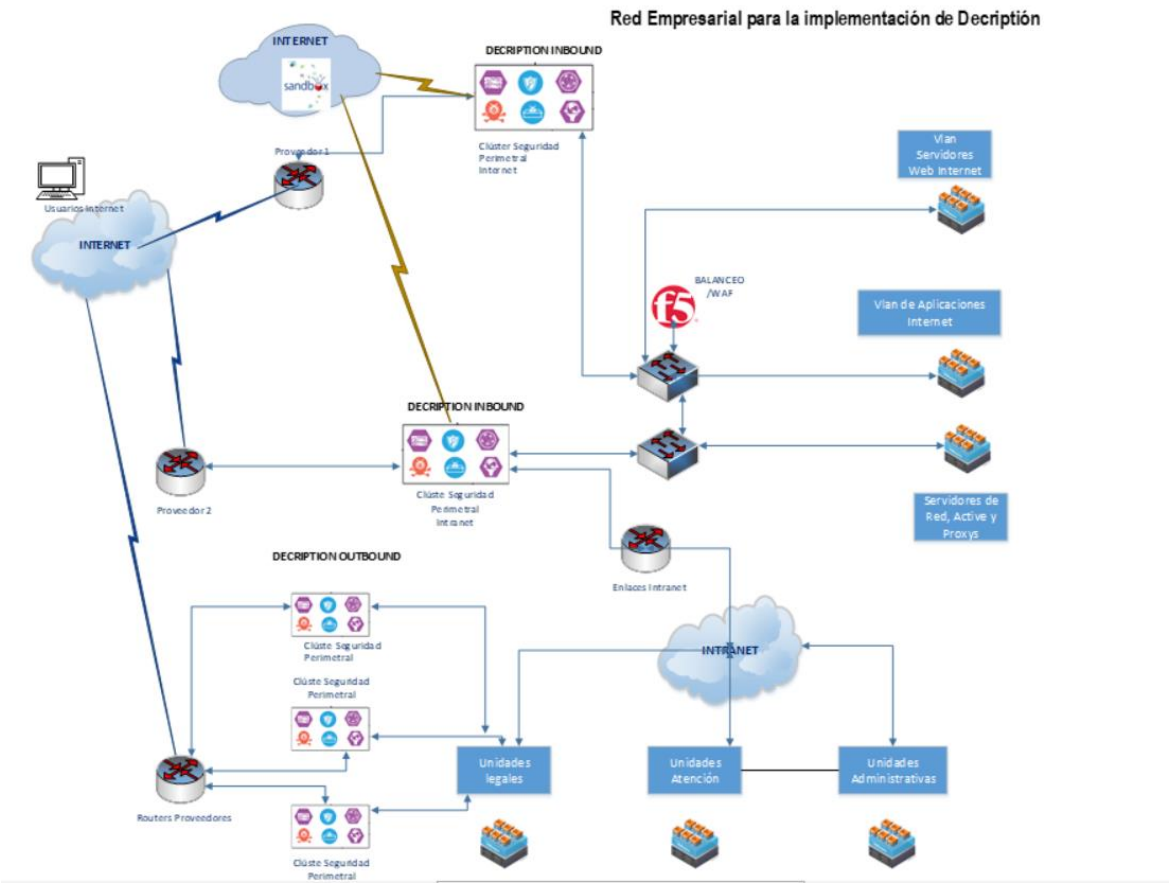
4 .1.1 Arquitectura de red

Se realizará la implementación en una red empresarial que incluye servicios de Internet y aplicaciones para usuarios internos, que adicionalmente brinda servicios de aplicativos para usuarios en Internet. Se proyecta realizar por pasos el proceso de decryption, debido a que el mismo incrementa el uso de recursos, sobre todo de CPU de los Firewalls, lo que podría afectar a la disponibilidad de los servicios, por lo que no se

podrá implementar decryption en toda la red, hasta que se realice un proceso de compra de nuevos equipos, el tamaño de dichos equipos dependerá de los resultados de estas implementaciones iniciales

Figura 4

Red empresarial en la que se proyecta la implementación completa



Nota. Elaboración propia (2026).

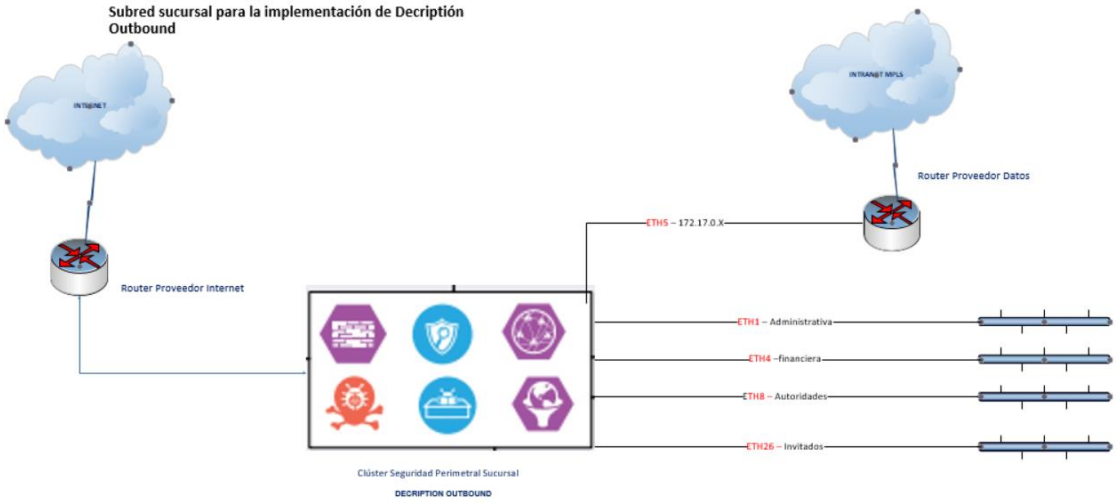
4.1.2 Subredes piloto y alcance

Decryption Outbound

Para la implementación de decryption outbound, se escoge una unidad que cuenta con seguridad perimetral y salida a Internet propias, se verifica que tenga una configuración de redes segmentadas, se verifica que el acceso a Active Directory este implementado en los equipos de los segmentos que se usaran para las pruebas, esto con el fin de que se pueda ir añadiendo por segmentos las redes de usuarios a las pruebas en forma progresiva, se presenta a continuación el diagrama de la rede de la unidad escogida:

Figura 5

Diagrama Decryption outbound



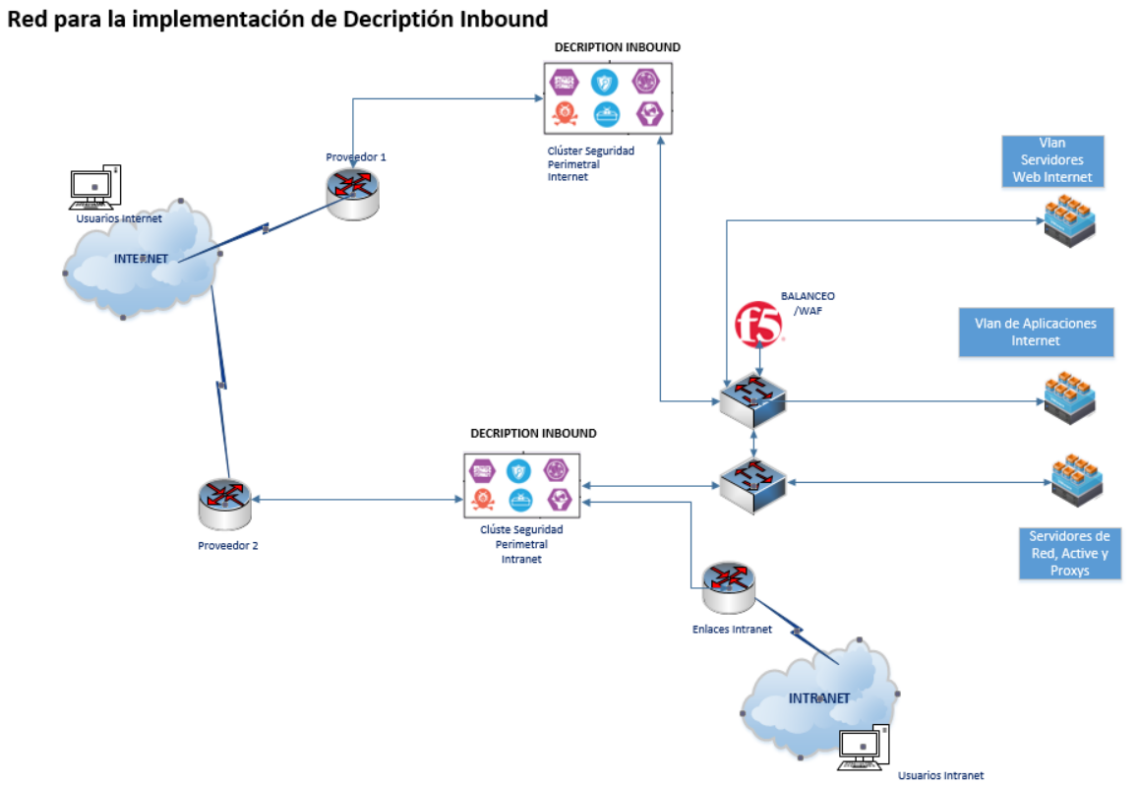
Nota. Elaboración propia (2026).

Decryption Inbound

Para la implementación de decryption inbound, se escoge un escenario con equipos de seguridad perimetral que permiten exclusivamente la publicación de aplicaciones para usuarios en Internet, y otro escenario en el que se expone aplicaciones para usuarios dentro de la intranet institucional, a través de otros equipos de seguridad perimetral que son usados para servicios locales:

Figura 6

Diagrama Decryption Inbound



Nota. Elaboración propia (2026).

Para el control de decryption inbound desde Internet se hace el control para dos dominios específicos que son los que más accesos tienen, esto es el portal y el dominio a través del cual se exponen aplicaciones:

www.miempresa.com

app.miempresa.com

Se expone el certificado institucional para los dos dominios mencionados, con el fin de poder hacer control de la interacción de los usuarios hacia las páginas de la empresa, y poder controlar ataques que se realizan a través del tráfico cifrado.

Se hizo también pruebas de implementación en un equipo de seguridad perimetral que permite el acceso a aplicaciones para usuarios internos, con el fin de hacer un control de acceso por horarios para ciertos aplicativos, para lograr esto los Firewalls deben poder leer los URL completos, pues atrás de estos URL se balancean varios aplicativos, y es necesario aplicar decryption inbound para leer y calendarizar de acuerdo al aplicativo:

App.miempresa.com/aplicativocalendarizado1, horario 8 am a 5 pm

App.miempresa.com/aplicativocalendarizado2, horario 13 pm a 5 pm

Adicionalmente se puede hacer controles de acceso por URL, Este es un ejemplo de las reglas que se probaron:

Figura 7
Definición de URLs:

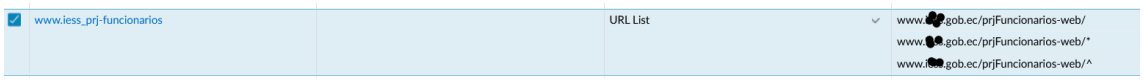


Figura 8
Regla de drop por URL

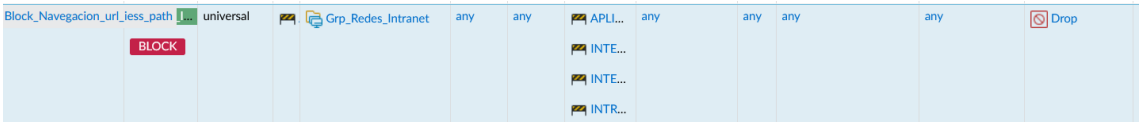


Figura 9
URL definido

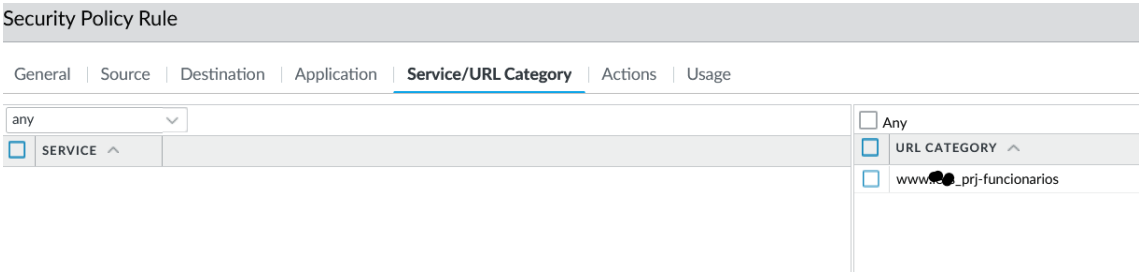
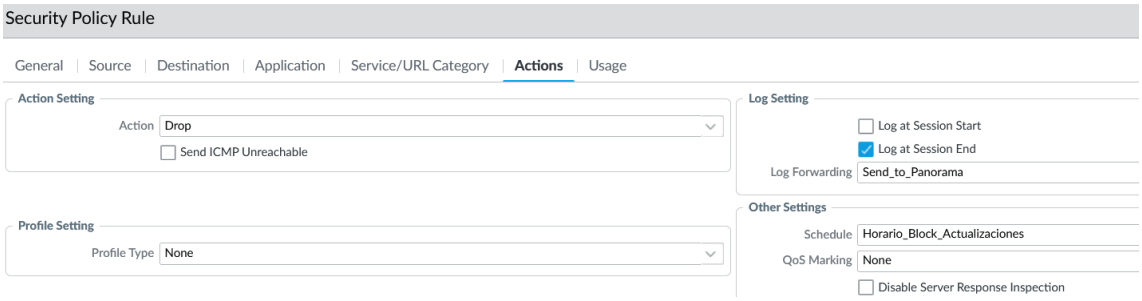


Figura 10
Definición de horario de bloqueo



Las pruebas de control de tráfico inbound desde usuarios de Internet tuvieron novedades de incrementos de picos de uso de CPU mayores al 100%, que lograron eliminarse controlando el número de sesiones permitidas en un equipo anterior al de seguridad perimetral, una vez realizado esto el consumo del CPU se estabilizo en alrededor del 50%, por lo que el control decryption se puso en producción.

Las pruebas de control de tráfico inbound desde usuarios de la Intranet resultan exitosas, pero no pueden ponerse en producción, debido a que el procesamiento del firewall se incrementa demasiado a más del 70% y al ser este equipo el que maneja toda la parte de aplicativos en producción y servicios de red como acceso a Internet, no se puede hacer pruebas por mucho tiempo sin afectar los servicios, por lo que se decide esperar a separar las aplicaciones en un nuevo firewall, en el cual se implementará el proceso en forma especifica

4.1.3 Equipos, versiones y políticas aplicadas

Se implementa el proceso de Decryption en equipos de Seguridad Perimetral de los modelos: Palo Alto PA 5410 PA1420 PA1410

4.2 Implementación del proceso de inspección SSL/TLSg

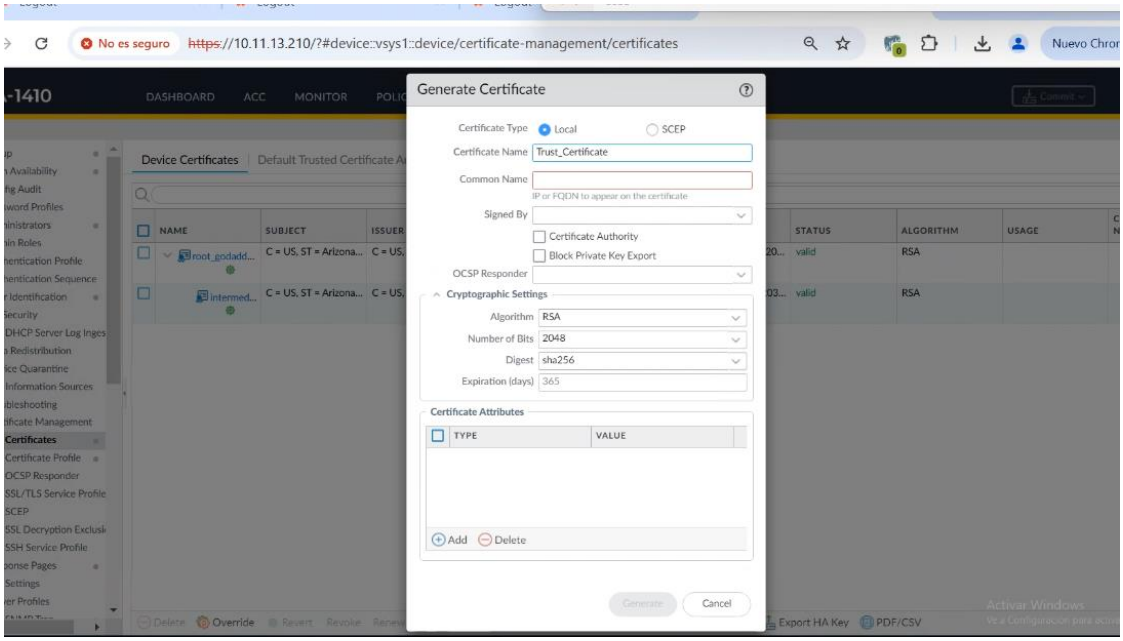
4.2.1 Certificados Trust/Untrust

Generación de certificados

Debo generar certificados en los Firewall el primero es trust (encripta hacia la zona de confianza que es su LAN) que será como entidad de certificación, no firmada por nadie y que se instalará en las maquinas:

Figura 11

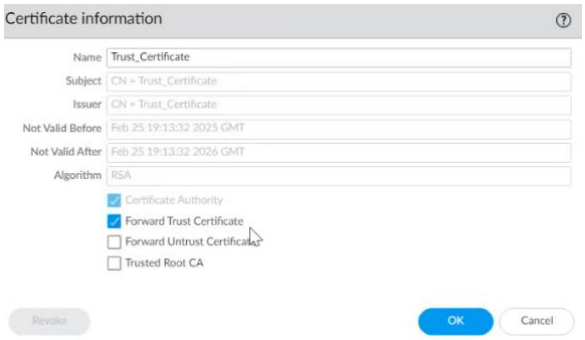
Generación de certificados Trust



Defino como certificado de confianza trust, este certificado se lo instalará en los equipos de los usuarios:

Figura 12

Certificado Trust



El segundo certificado es Untrust (no confianza) que también será como entidad de certificación que es el que se encarga de cifrar el tráfico desde el Firewall hacia afuera:

Figura 13

Generación de certificados Untrust

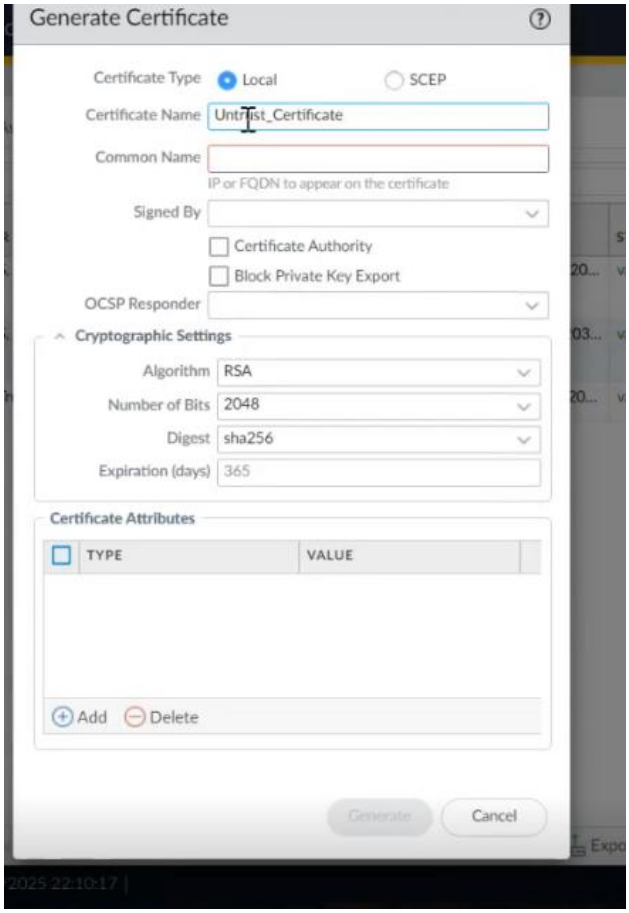
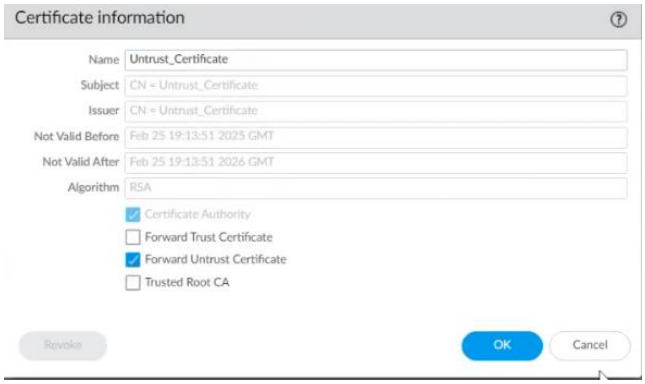


Figura 14

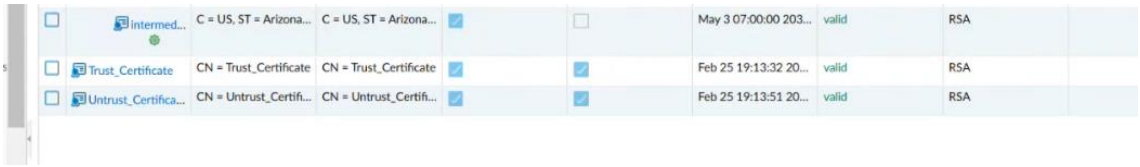
Certificado Untrust



Con esto se tendrían los dos certificados para el proceso de control de tráfico outbound generados:

Figura 15

Certificados Generados



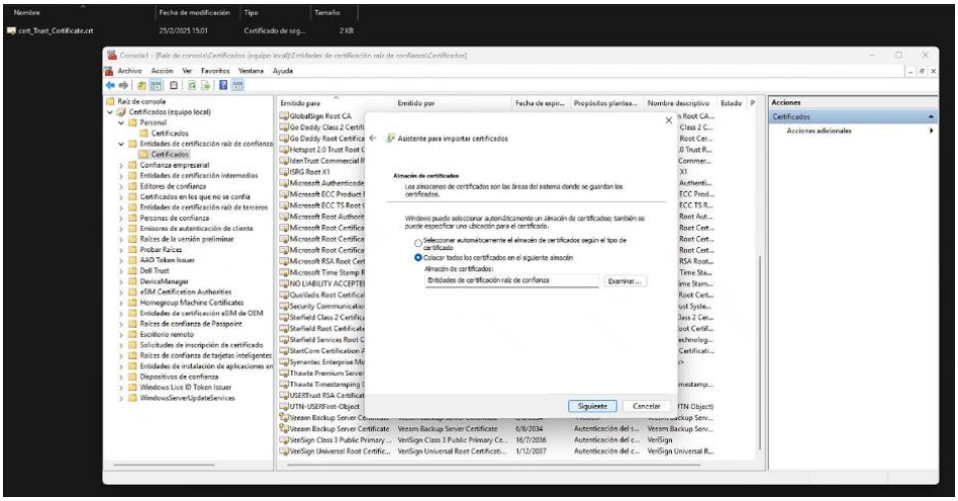
4.2.2 Distribución por GPO

Los certificados deben ser instalados en las máquinas de los usuarios, de lo contrario cuando estas requieren navegar se presenta un error de certificado, por lo que se procedió con la instalación en las máquinas de las subredes de pruebas, y se realizó el envío por GPO hacia todas las maquinas en dominio de la red institucional, esto con el fin de que las mismas puedan usarse una vez se aplique Decryption para todos los segmentos de red de la Intranet

Se puede realizar la instalación de los certificados en cada máquina:

Figura 16

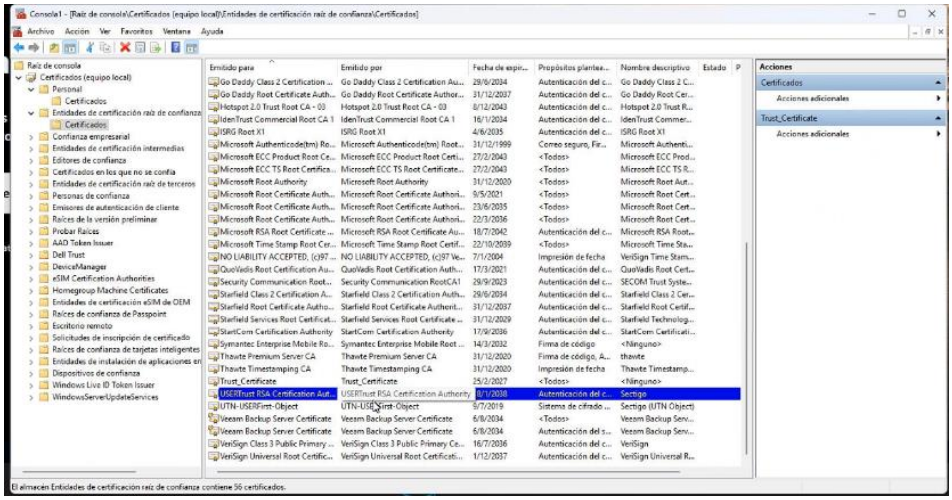
Configuración para ingreso de certificado localmente



Se realiza la revisión en el almacén de certificados:

Figura 17

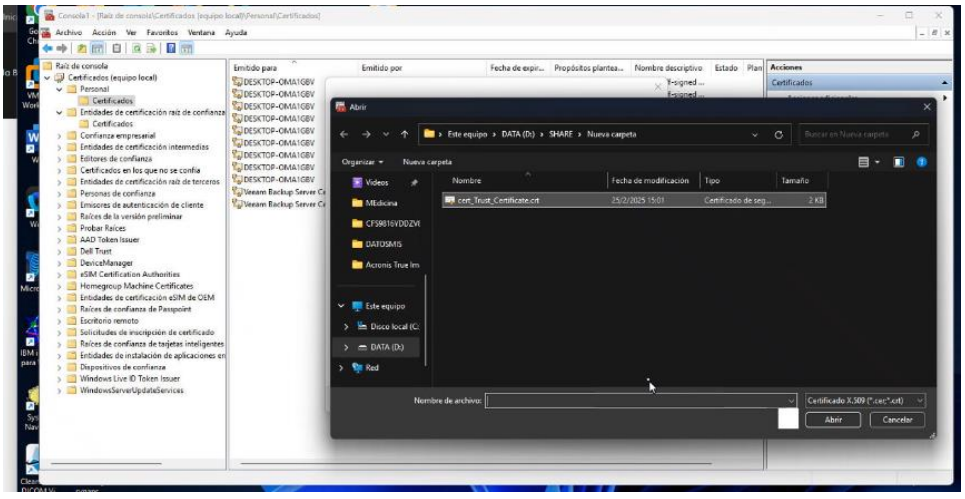
Vista de certificados en la maquina



Se agrega el certificado Trust en la máquina

Figura 18

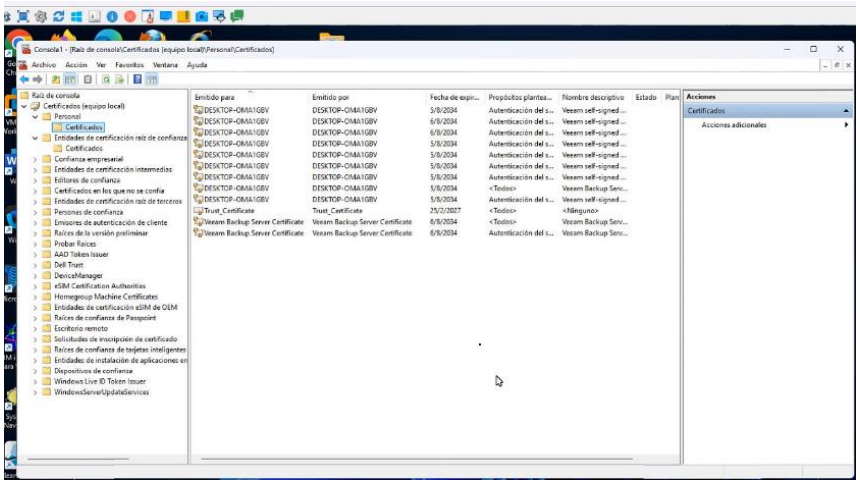
Escojo el certificado trust



Se evidencia que se añaden a la lista de certificados locales:

Figura 19

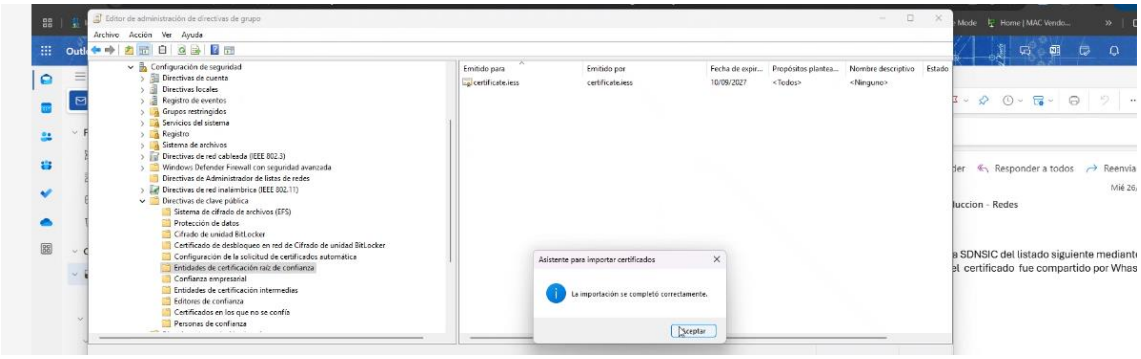
Despliegue de certificados instalados



Se completa importación del certificado:

Figura 20

Importo certificado



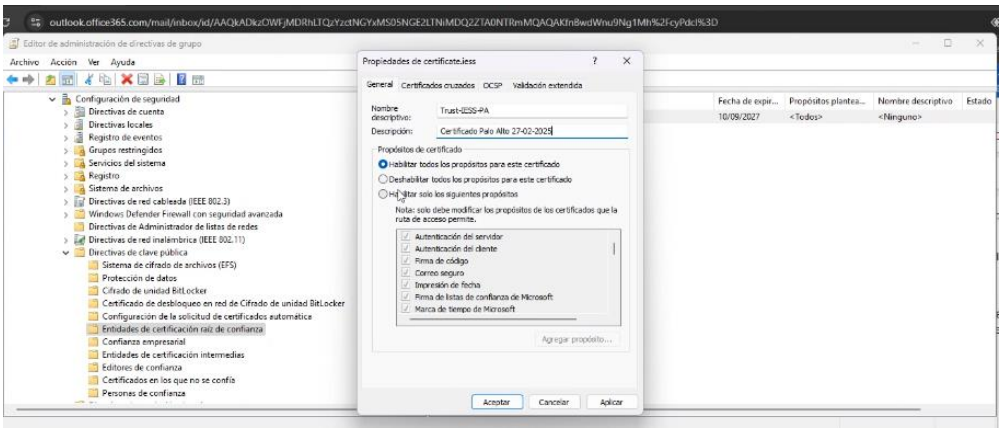
Envío de Certificados por GPO

Para que toda la red cuente con los certificados de todos los Firewalls que brindan salida a Internet y que se permita la movilidad, se realiza el envío por Active Directory a todas las máquinas de la Red:

Para el envió a todas las maquinas en el dominio institucional se puede realizar la GPO de envió de certificados en el Active Directory:

Figura 21

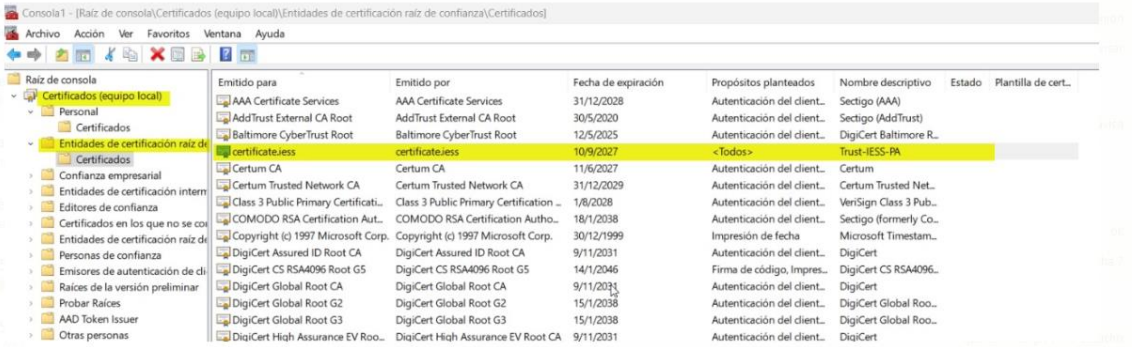
Ingreso el certificado al Active Directory



Se verifica que el certificado se encuentra en el almacén de certificados del Active Directory:

Figura 22

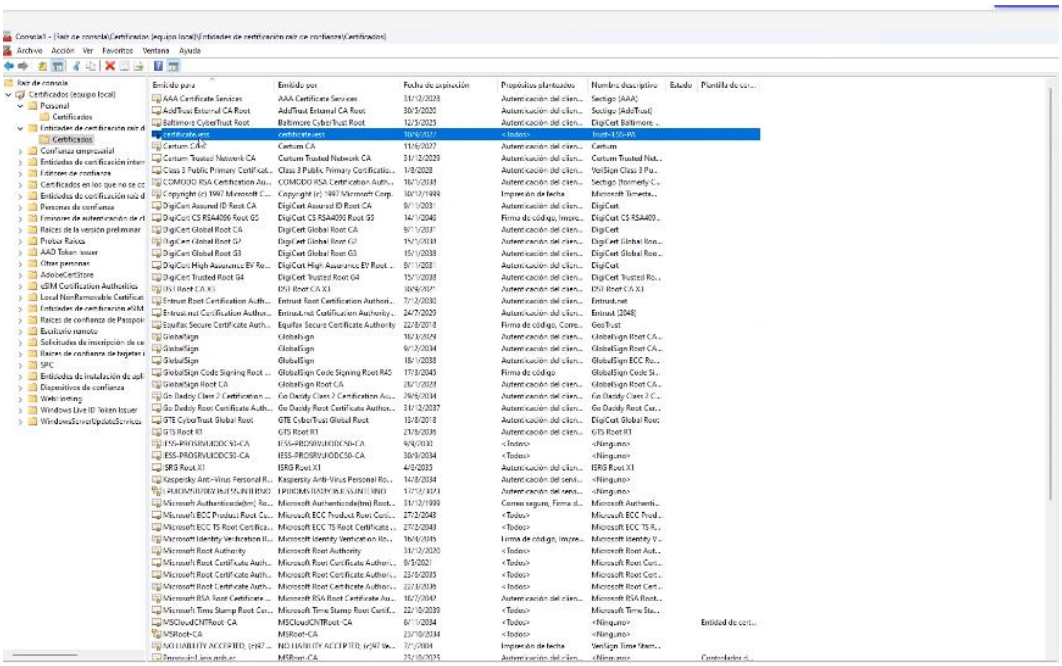
Almacén de certificados del Active Directory



Se procede con el envío de los certificados a las maquinas unidas al dominio del Active Directory:

Figura 23

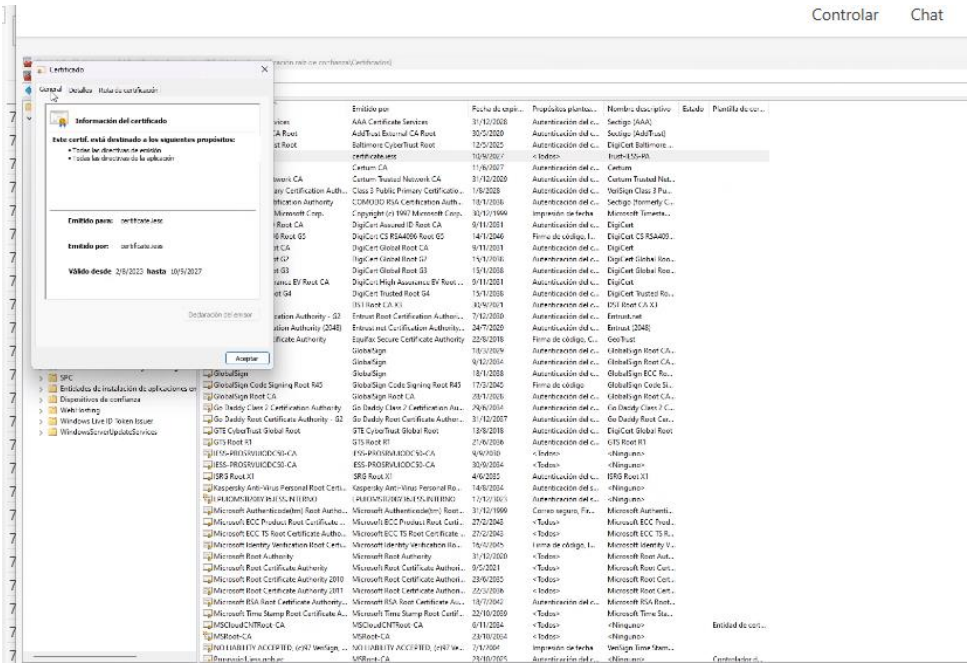
Reviso certificado en el almacén de certificados



Se revisa evidencia de la información del certificado:

Figura 24

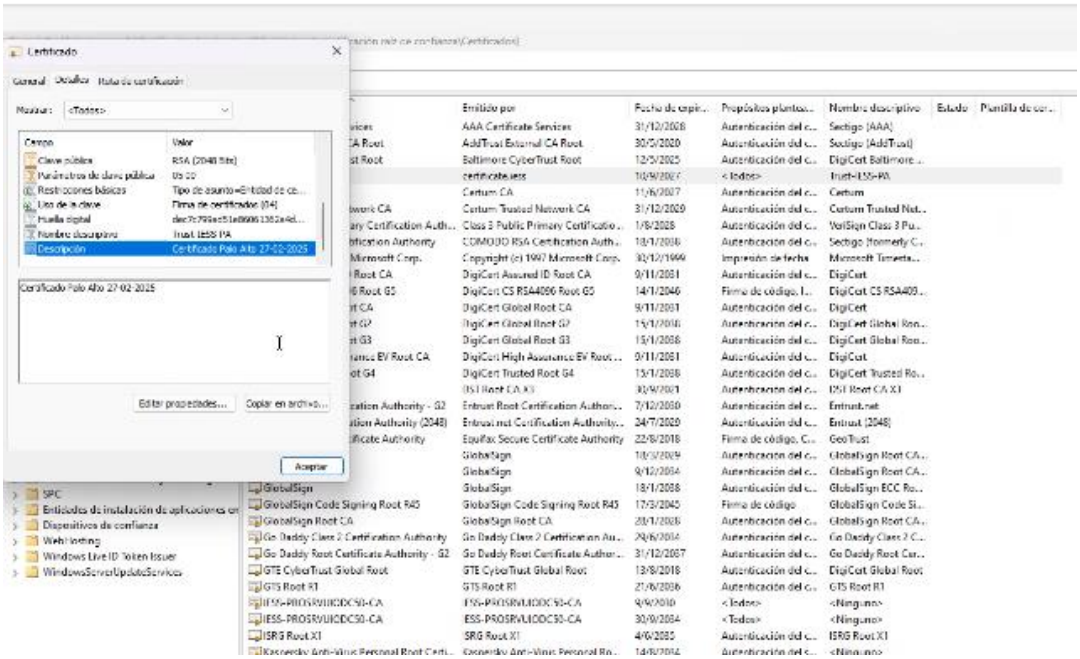
Reviso información en el certificado



Se revisa evidencia de la descripción en el certificado:

Figura 25

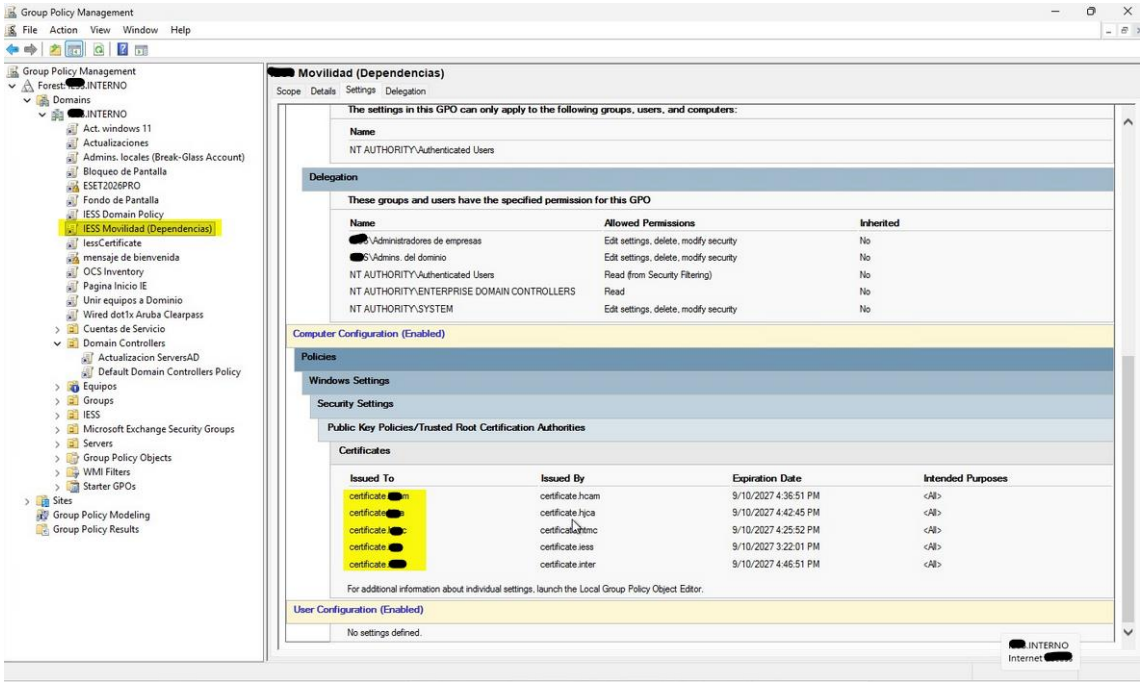
Ejecuto GPO y remito a maquinas en dominio



Se debe proceder a verificar que el GPO se haya ejecutado:

Figura 26

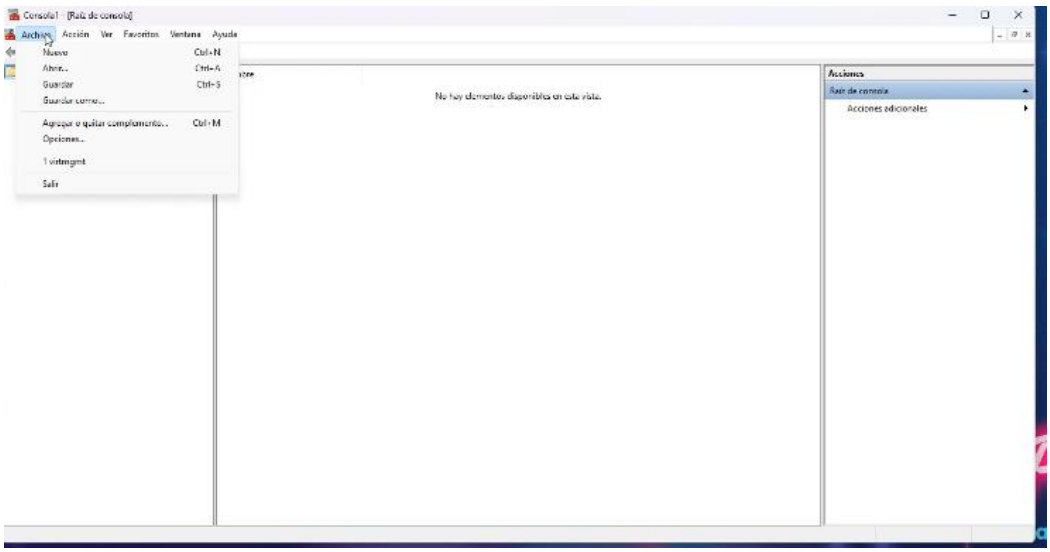
GPO ejecutado certificados distribuidos a la organización



Para verificar el resultado de la distribución por GPO en las maquinas cliente, se debe ejecutar el comando mmc:

Figura 27

maquina cliente se evidencia el resultado del GPO



Una vez instalados los certificados en las maquinas ya no darán errores y podrán navegar mientras se analiza el traficó

4.3 Implementación del descifrado outbound en los Equipos de Seguridad Perimetral

4.3.1 Desarrollo de reglas de control

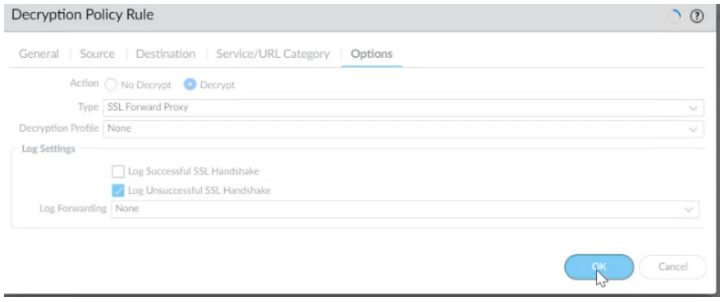
Las reglas de control de tráfico automáticamente se benefician de la posibilidad de leer el tráfico descifrado dependiendo de cómo se configuren las reglas de decryption, se crearon también reglas específicas para poner en las mismas aplicaciones y URL´s que se requieren controlar, y que sin decryption no podían ser leídos. Adicionalmente se deben crear las reglas de Decryption como tal. Este sistema permitió interceptar, descifrar y analizar el tráfico cifrado antes de su reenvío a los destinos finales. Se configuraron políticas específicas para identificar y clasificar el tráfico según aplicaciones, usuarios, protocolos y comportamientos, lo que facilitó la creación de reglas de acceso más preciso y contextual.

Reglas de Decryption

Se deben definir políticas de Decryption, para esto se debe indicarle al FW desde que zonas hacia qué zonas se debe descifrar el traficó como por ejemplo LAN hacia Internet:

Figura 28

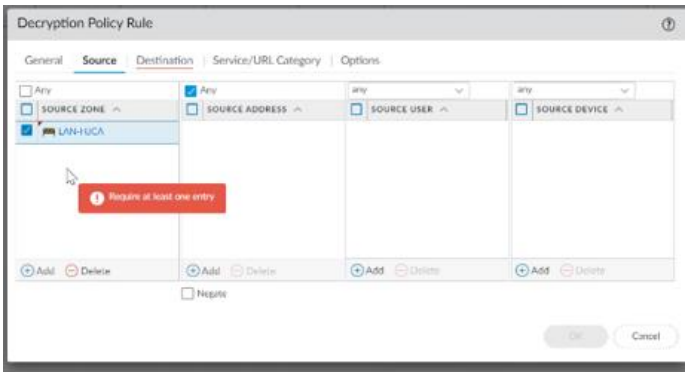
Regla descifrado hacia Internet



Se escoge el origen y destino del descifrado:

Figura 29

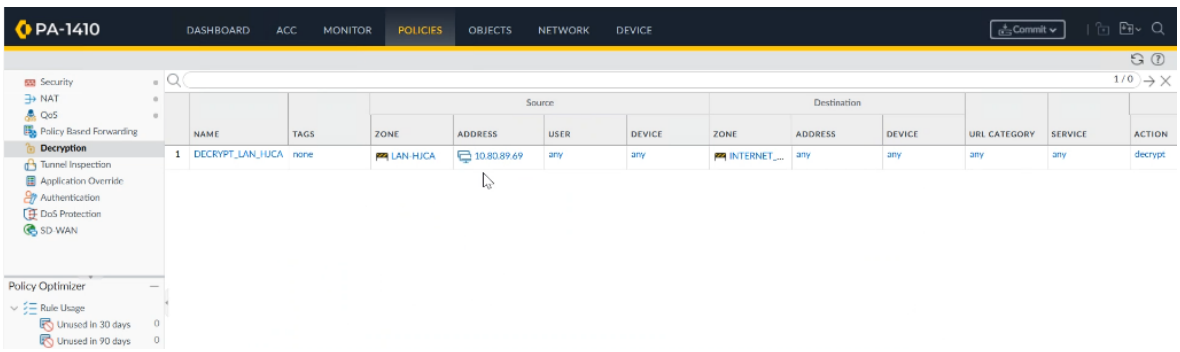
Tipo de regla de descifrado



Se definen reglas de Decryption indicando los orígenes destinos y los puertos que se desencriptan para que el firewall pueda analizar el tráfico y aplicar controles efectivos.

Figura 30

Regla de descifrado desde una IP de prueba hacia Internet

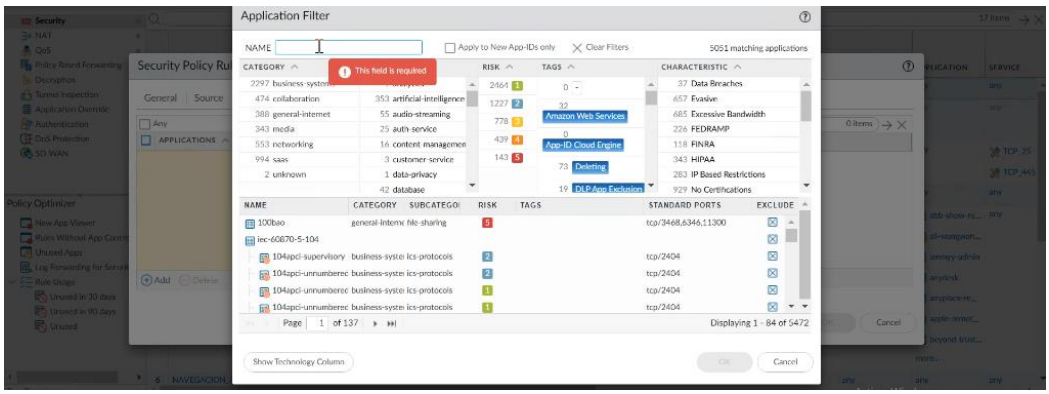


Reglas de URL filtering

Para las reglas de ULR filtering, o para aplicar políticas específicas para aplicaciones, como la de control de proxys, puedo crear filtros de aplicación (Aplication filter):

Figura 31

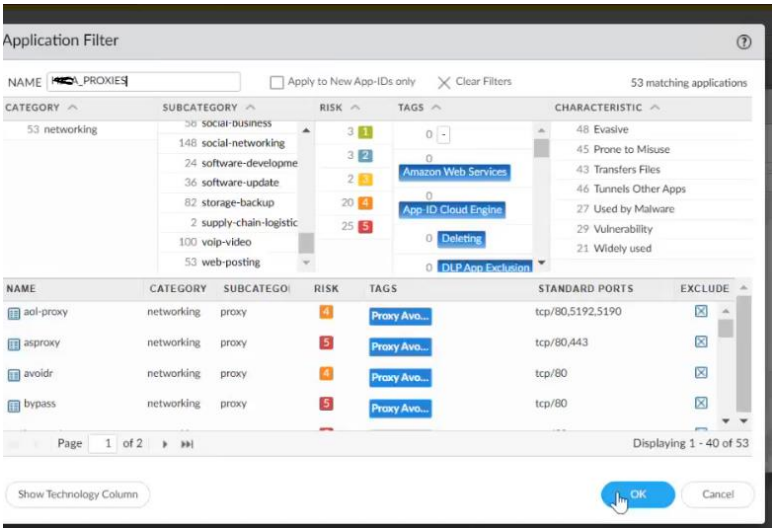
Creación de Aplication Filter



Se puede agregar filtros para las aplicaciones que se desee controlar, como los proxys que permiten navegar sin controles encriptando el tráfico

Figura 32

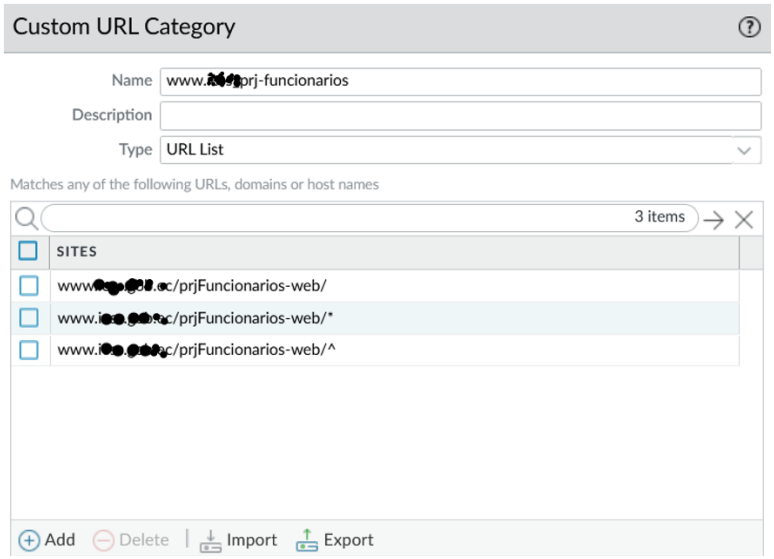
Creación de filtros de aplicación para proxys de navegación



Se puede generar categorías de URL con los que se puede hacer controles, esto se usó para controles de navegación hacia Internet, y también para control de tráfico de acceso hacia los aplicativos institucionales:

Figura 33

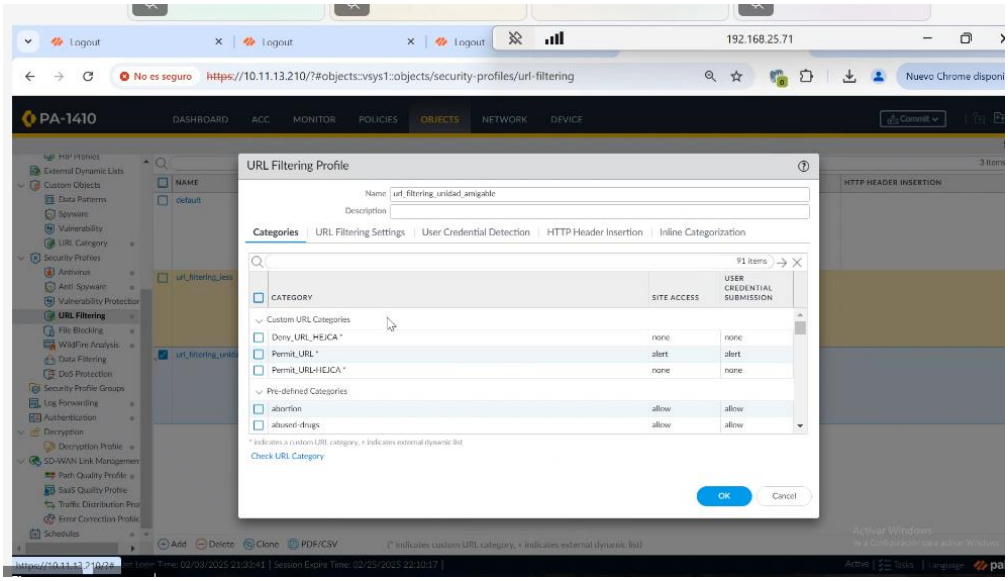
Se crean categorías de URL



Se debe crear un perfil de URL filtering, en el que ingresamos perfiles preexistentes que deseemos controlar o si es necesario personalizar, se pueden usar los URL category creados, como los del ítem anterior, esto con el fin de utilizar este perfil en las reglas de control de acceso:

Figura 34

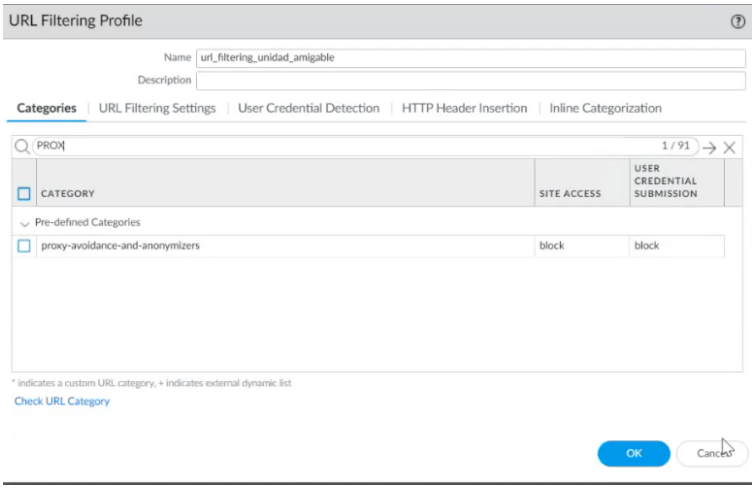
Creación de un URL Filtering profile



Se puede añadir aplicaciones específicas que se requiera sean analizadas:

Figura 35

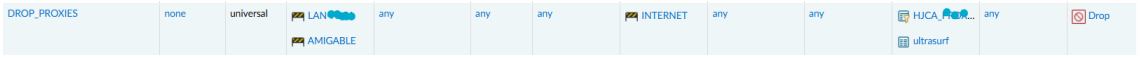
Ingreso de aplicación proxy anonymizer al perfil de Url filtering



Se crean reglas de control de tráfico para análisis del tráfico de navegación de los usuarios, en los que se puede usar los filtros de aplicación o perfiles URL:

Figura 36

Regla de control de tráfico para bloqueos de proxys http



Se hace uso de reglas de control de tráfico para análisis del tráfico según los perfiles de URL creados:

Figura 37

Regla de control de tráfico para bloqueos por aplicaciones

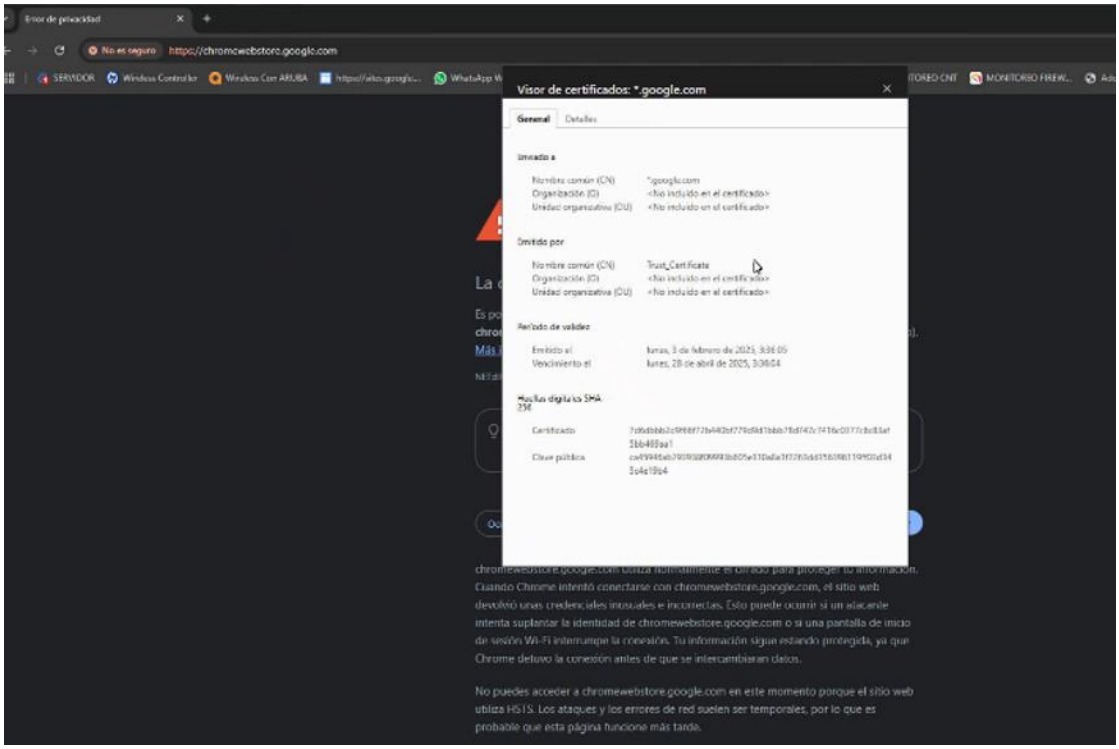


4.3.2 Pruebas en las máquinas de los usuarios

Cuando los navegadores de las maquinas detectan que lo firma alguien que no es entidad certificadora, indica un error de certificado:

Figura 38

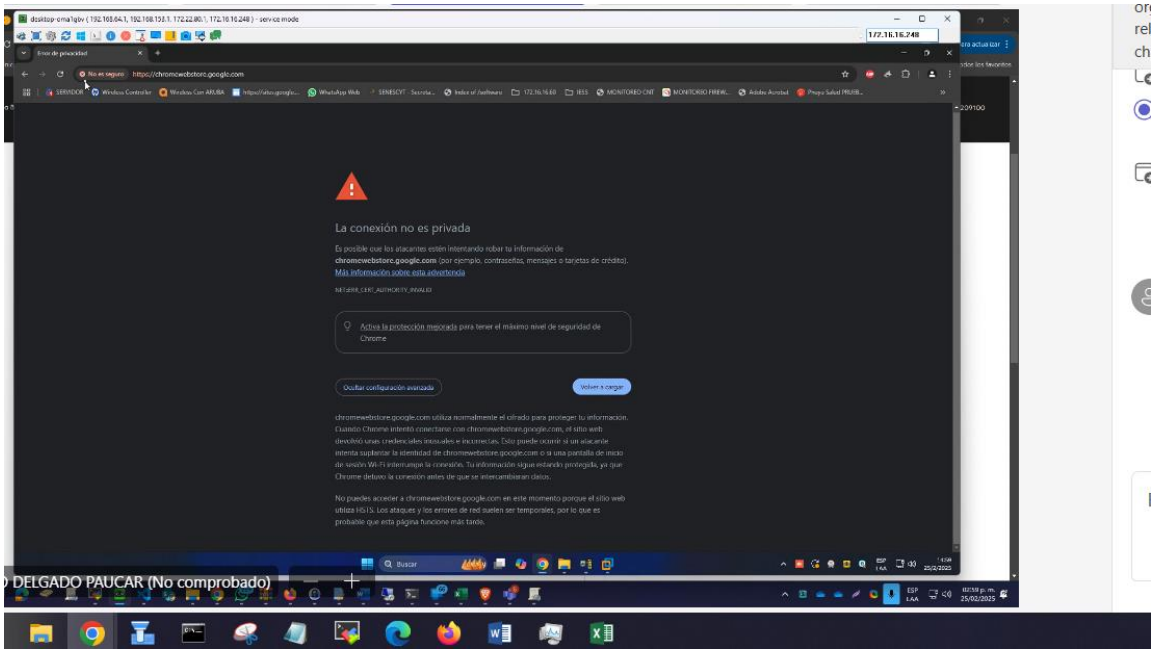
Maquina muestra error de certificado



Al estar configurado el descifrado de tráfico para análisis en seguridad perimetral de frontera, las máquinas que intentan salir sin el certificado trust, mostraran errores de conexión privada:

Figura 39

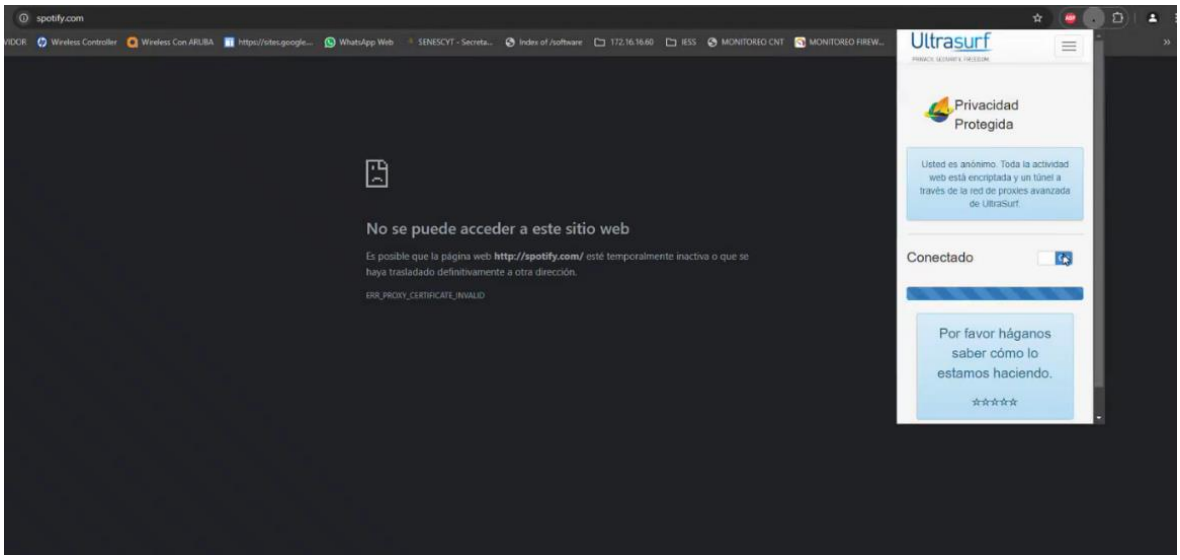
El navegador no permite el despliegue de la página



Una vez se haya instalado el certificado podemos observar los controles, como se evidencia en el siguiente ejemplo presentado, en el que a pesar de estar con aplicativos como proxys de navegación, las maquinas ya no los pueden usar para acceder:

Figura 40

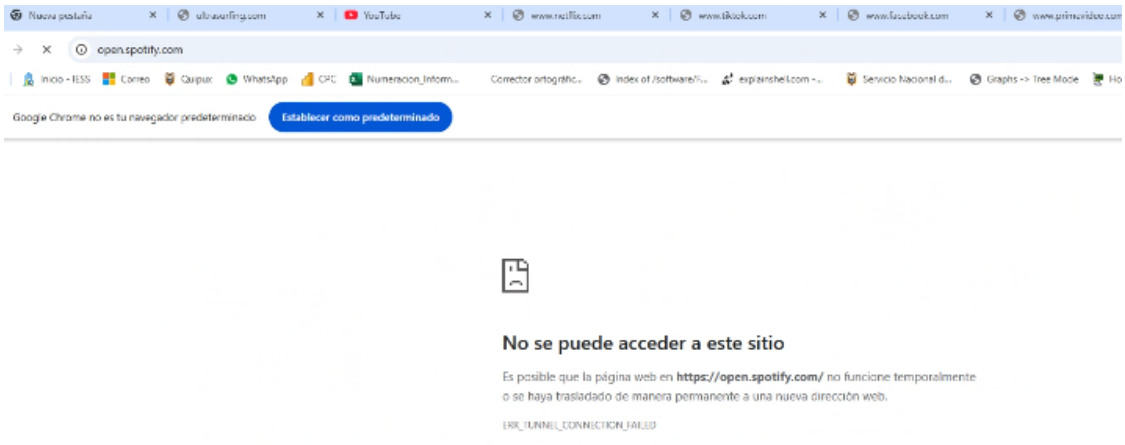
Maquina con proxy Ultrasurf instalado



Se evidencia que otras aplicaciones que pasan encriptadas ya son controladas:

Figura 41

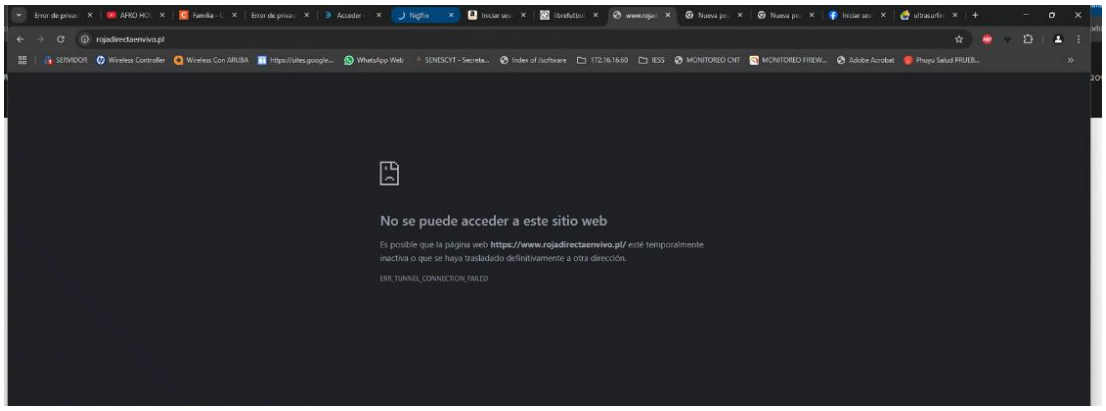
Sitio bloqueado una vez descifrado



Se evidencia sitios de streaming bloqueados:

Figura 42

Sitio bloqueado una vez descifrado



4.3.3 Verificación en los log de los Firewalls

Se puede evidenciar en logs del Firewall con el parámetro “decrypted”, si el mismo se encuentra en “yes” significa que el tráfico esta ya desencriptándose para ser analizado:

Figura 43

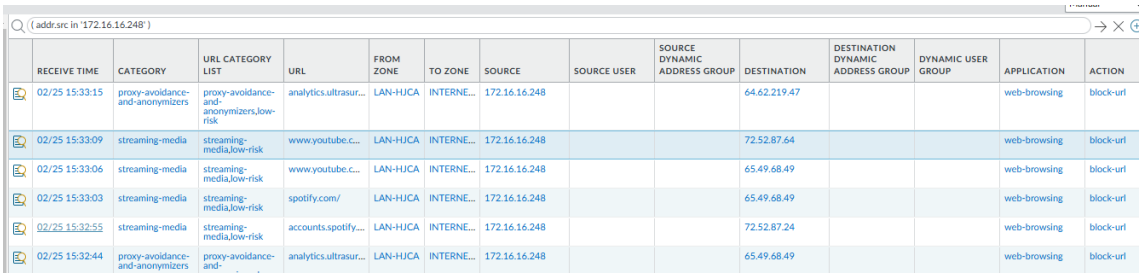
Verificación de que el tráfico está siendo descifrado

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	DECRYPTED	SOURCE	SOUR... USER	NAT DEST IP	S... IP	ADDR... GROUP	DESTINATION	ADD... GRO...	US... GR...	T P
02/28 16:57:16	end	DESARROLLADORES_v14	INTERNET_CONSUM...	yes	192.168.12.63		172.172.255.218	1...		172.172.255.218			4
02/28 16:55:33	end	DESARROLLADORES_v14	INTERNET_CONSUM...	yes	192.168.12.63		172.172.255.216	1...		172.172.255.216			4

Se observa que ya es posible reconocer y por tanto bloquear el tráfico de aplicaciones diseñadas para saltarse los controles, por ejemplo Ultrasurf, o streaming cifrado:

Figura 44

Aplicaciones bloqueadas al haber sido vistas una vez des encriptadas



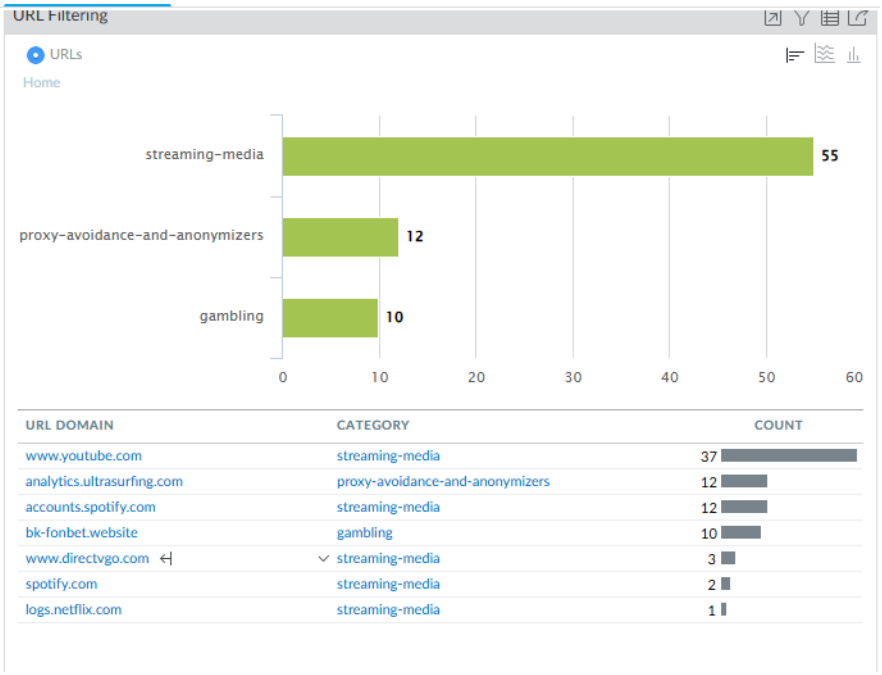
(addr.src in '172.16.16.248')

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	APPLICATION	ACTION
	02/25 15:33:15	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	analytics.ultrasur...	LAN-HJCA	INTERNE...	172.16.16.248			64.62.219.47			web-browsing	block-url
	02/25 15:33:09	streaming-media	streaming-media,low-risk	www.youtube.c...	LAN-HJCA	INTERNE...	172.16.16.248			72.52.87.64			web-browsing	block-url
	02/25 15:33:06	streaming-media	streaming-media,low-risk	www.youtube.c...	LAN-HJCA	INTERNE...	172.16.16.248			65.49.68.49			web-browsing	block-url
	02/25 15:33:03	streaming-media	streaming-media,low-risk	spotify.com/	LAN-HJCA	INTERNE...	172.16.16.248			65.49.68.49			web-browsing	block-url
	02/25 15:32:55	streaming-media	streaming-media,low-risk	accounts.spotify....	LAN-HJCA	INTERNE...	172.16.16.248			72.52.87.24			web-browsing	block-url
	02/25 15:32:44	proxy-avoidance-and-anonymizers	proxy-avoidance-and-	analytics.ultrasur...	LAN-HJCA	INTERNE...	172.16.16.248			65.49.68.49			web-browsing	block-url

Con el descifrado, las aplicaciones que funcionan encriptadas pueden ser vistas por los dispositivos, por lo tanto ya están siendo controladas:

Figura 45

Consolidado de aplicaciones que fueron bloqueadas



URL DOMAIN	CATEGORY	COUNT
www.youtube.com	streaming-media	37
analytics.ultrasurfing.com	proxy-avoidance-and-anonymizers	12
accounts.spotify.com	streaming-media	12
bk-fonbet.website	gambling	10
www.directvgo.com	streaming-media	3
spotify.com	streaming-media	2
logs.netflix.com	streaming-media	1

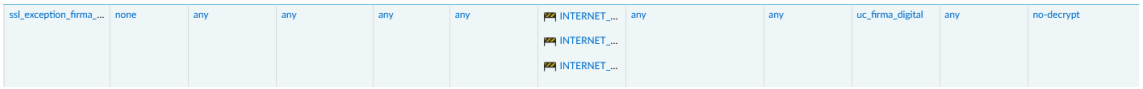
4.3.4 Excepciones de privacidad

Se debe realizar excepciones, pues hay sitios web que no permiten el descifrado, hay sitios cuyos datos no deben hacerse visibles por temas de seguridad de los datos que involucran, y también deben realizarse excepciones para personal que por su trabajo necesita manejar aplicaciones que serían bloqueadas al ser analizadas con Decryption

No se desencripta aplicaciones que por su seguridad no deben ser visibles, o aplicaciones que por su naturaleza no permiten su funcionamiento si las mismas verifican que existe interacción intermedia:

Figura 46

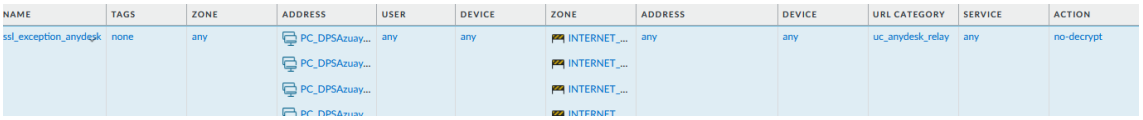
Aplicaciones excluidas de descifrado por seguridad de las mismas



Se excluye del descifrado, aplicaciones que normalmente son bloqueadas, pero que el personal que necesita usarlas para su trabajo:

Figura 47

Exclusión de descifrado de aplicaciones solicitadas por usuarios



No se desencripta tráfico de usuarios que están realizando trabajos de desarrollo, pruebas o puestas en producción para las que requieren que su tráfico no se desencripte:

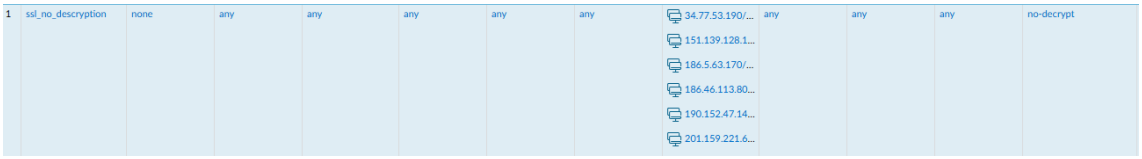
Figura 48

Exclusión de descifrado de usuarios que realizan tareas específicas

No se desencripta destinos que la empresa requiere para su trabajo, o los considera de confianza:

Figura 49

Exclusión de destinos considerados de confianza



No se desencripta los sitios de almacenamiento online que son considerados de confianza

Figura 50

Exclusión de sitios de almacenamiento externo de confianza



4.3.5 Implementación del descifrado inbound en los Equipos de Seguridad Perimetral

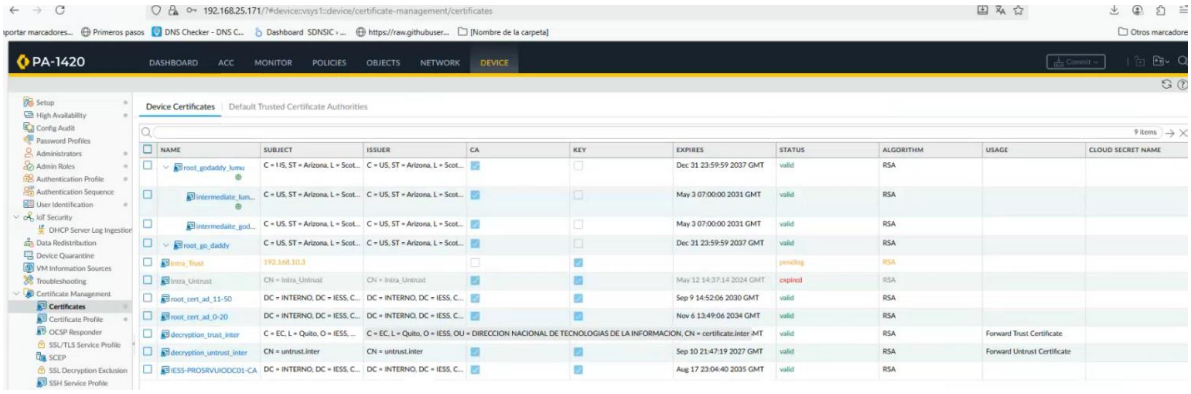
Decryption Para Tráfico Inbound

Es posible también realizar un análisis del tráfico que llega desde usuarios externos a los portales institucionales con el fin de también prevenir posibles amenazas en este consumo de servicios realizado.

Se deben instalar en los firewalls certificados para análisis de tráfico de ingreso:

Figura 51

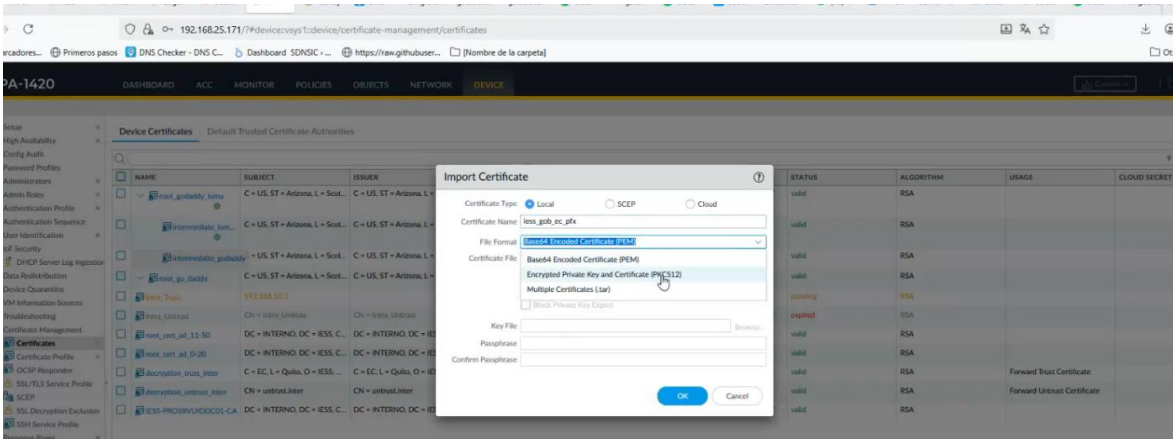
Instalación de certificados institucionales



Para este caso es necesario presentar el certificado institucional, por lo que debe subirse al almacén de certificados

Figura 52

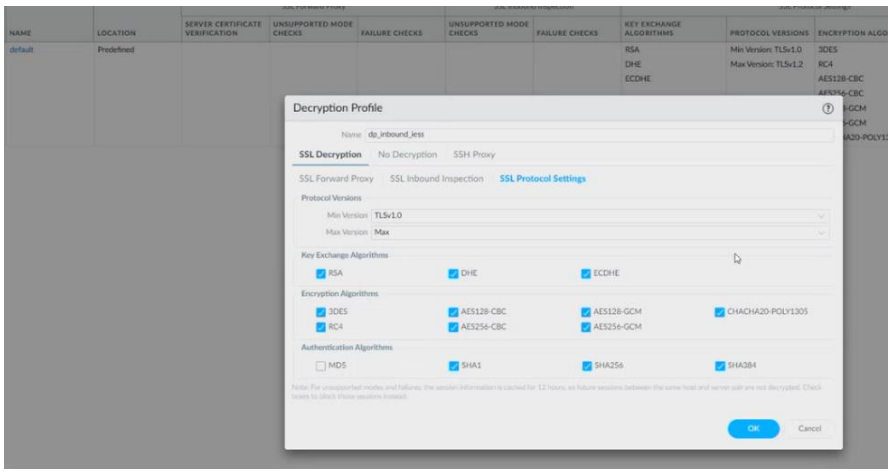
Importo certificado institucional



Creo un decryption profile para inspección de tráfico entrante

Figura 53

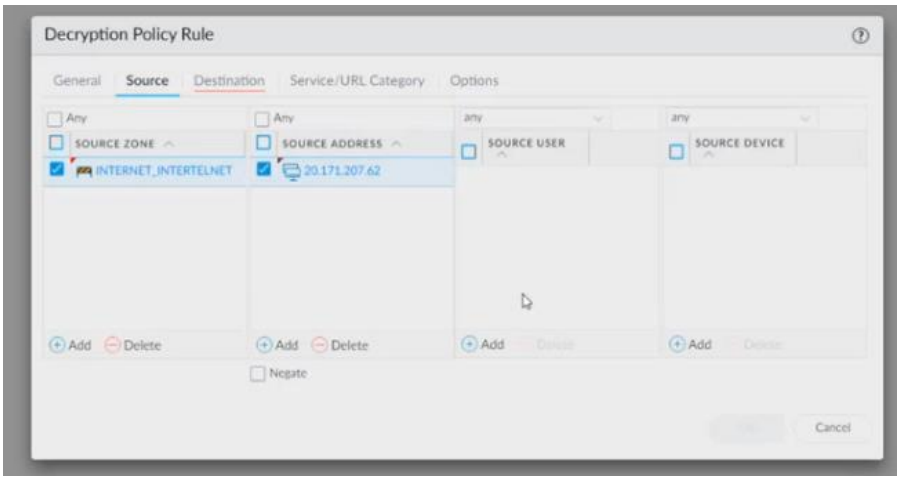
Decryption profile para inbout inspección



Creo políticas de Decryption para inbount poniendo el certificado institucional, con el fin de que sirva como llave para ver el contenido del tráfico:

Figura 54

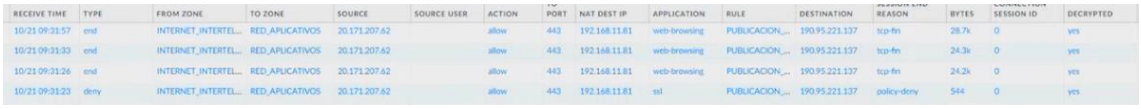
Política Decryption ingreso



Se evidencia que se desencripte el tráfico entrante desde usuarios en Internet al portal Institucional:

Figura 55

Logs de descifrado de tráfico entrante



4.4 Análisis por firewall de la implementación outbound e inbound

4.4.1 Firewalls Internos outbound decryption

Para Los firewalls Internos se realizó la configuración de outbound decryption para el tráfico que consumen un grupo de usuarios hacia el Internet.

Uso de CPU del Data Plane

Se observa el uso del CPU al implementarse decryption en los segmentos de red de pruebas seleccionados

Figura 56

CPU Firewalls internos Julio 2025

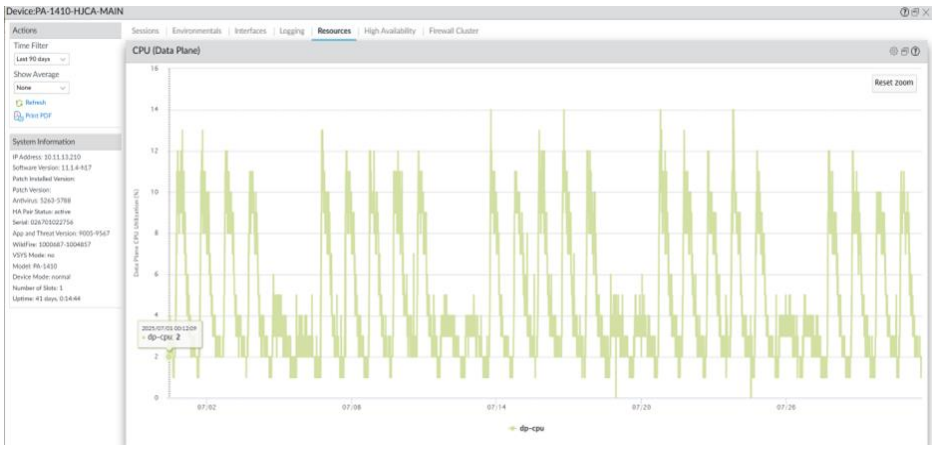


Figura 57

CPU Firewalls internos Agosto 2025

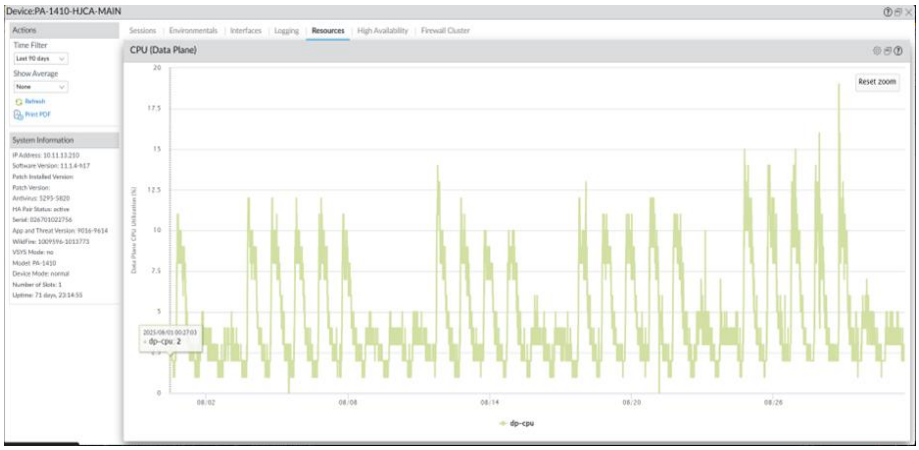
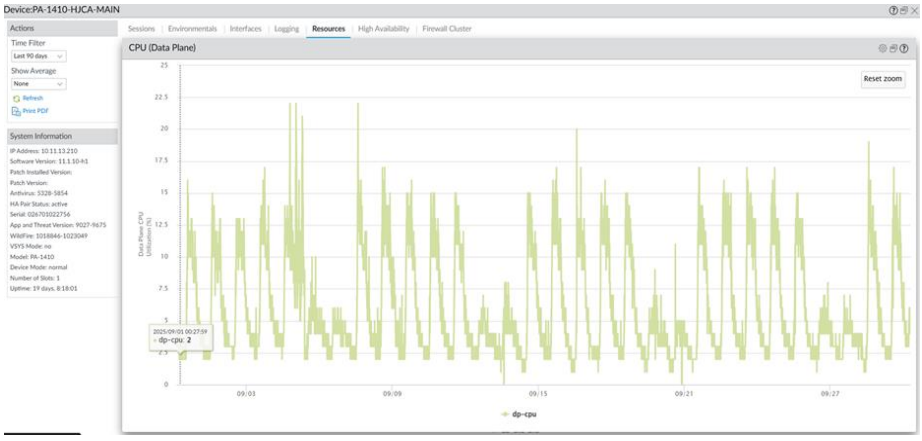


Figura 58

CPU Firewalls internos Septiembre 2025



Basado en el monitoreo histórico del dispositivo, se identifican tres fases en el comportamiento del CPU:

1. Julio: Estado de Reposo
    - Antes de la activación, el equipo operaba con una carga mínima.
2. Agosto: El Mes de la Transición
    - Con la habilitación de Decryption en agosto, el comportamiento empezó a cambiar hacia finales del mes.
    - El salto al 19% registrado el 28 de agosto marca el inicio del procesamiento criptográfico.
3. Septiembre: Estabilización de la Carga
    - Elevación de la Base: El CPU ya no baja al 2%, ahora se mantiene en un 4-5%. Este es el "costo fijo" del firewall por mantener los túneles SSL abiertos para inspección.
    - Consistencia de Picos: Los picos de 22% son ahora frecuentes. Esto representa un aumento del 57% en la demanda de procesamiento respecto a julio.

Aplicaciones Detectadas y Amenazas bloqueadas

Debido a los cambios de decryption, el firewall Interno puede verificar aplicaciones que antes se visualizaban como aplicación SSL en la navegación de usuarios hacia el Internet; sin embargo, los cambios no son significativos respecto al tráfico total del firewall ya que este hospital cuenta con acceso al Internet para pacientes y familiares de pacientes, el cual no puede ser descifrado al no tener control sobre los equipos.

Figura 59

Vista de aplicaciones Julio 2025

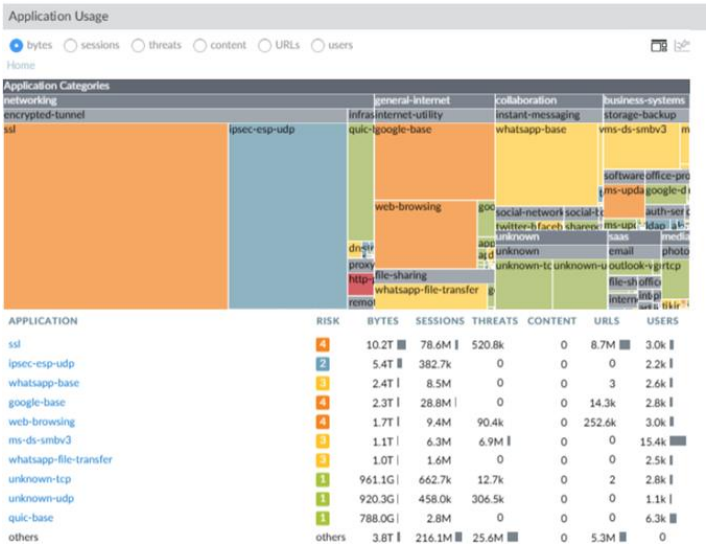


Figura 60

Vista de aplicaciones Agosto 2025

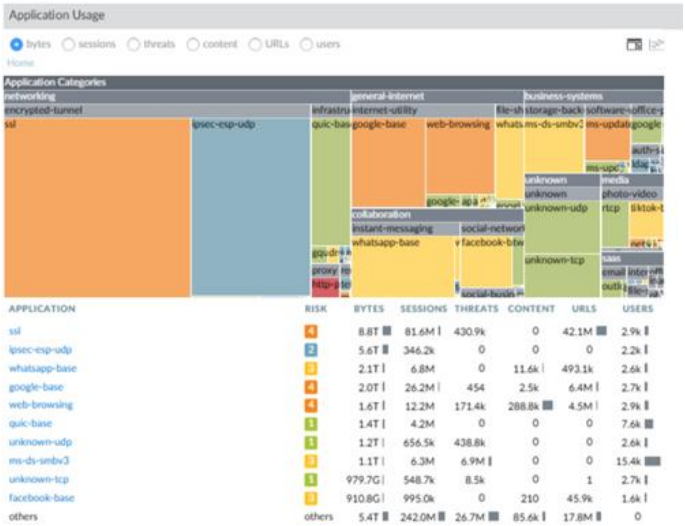


Figura 61

Vista de aplicaciones Septiembre 2025

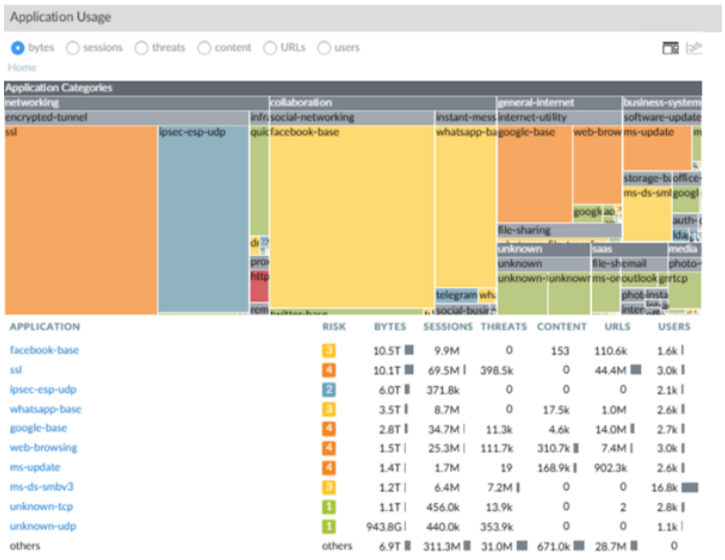


Figura 62

Amenazas bloqueadas

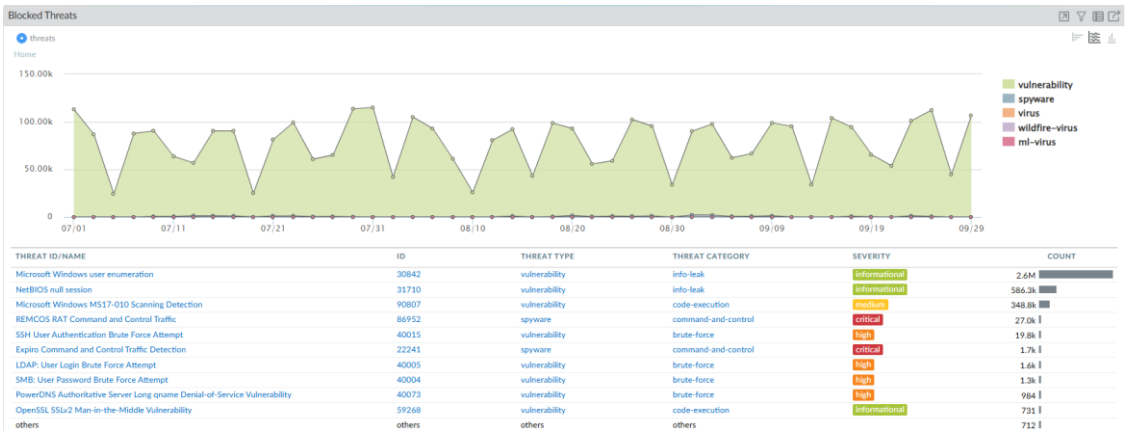


Tabla 5

Visibilidad de Aplicaciones outbound proyectada al tráfico total

Aplicación / Métrica	Julio	Agosto	Septiembre	Octubre	Evolución
web-browsing (Bytes)	34 TB	35 TB	36 TB	37 TB	+8.8%
ssl-decryption (Bytes)	3.1 TB	12.6 TB	22.7 TB	33.3 TB	+974%
Amenazas Detectadas	3.5k	18.2k	62.4k	94.7k	+2606%
Contenido Inspeccionado	1.2M	8.7M	18.5M	28.4M	+2266%
URLs Identificadas	95.6M	315.4M	587.2M	894.6M	+836%
Aplicaciones Identificadas (App-ID)	780	1.980	3.420	4.850	+522%
Eventos de Acceso Controlados	14.5k	38.2k	71.8k	112.4k	+675%

Nota. Elaboración propia (2026).

4.4.2 Firewalls Externos inbound decryption

Para el firewall externo se realizó la configuración de inbound decryption para el tráfico que llega desde Internet hacia la página web institucional con la finalidad de bloquear intentos de ataque en sesiones encriptadas mediante HTTPS.

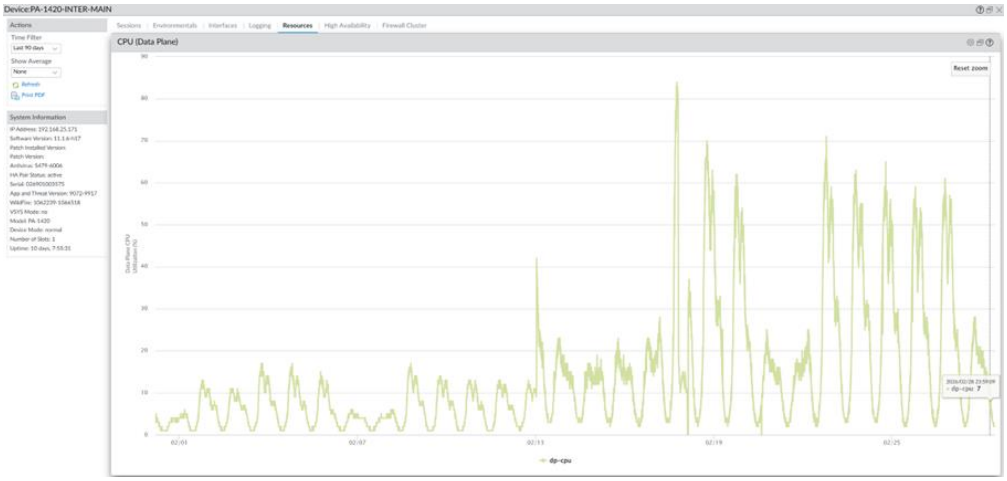
Uso de CPU del Data Plane

Basado en el monitoreo histórico del dispositivo, se identifican tres fases en el comportamiento del CPU:

1. Antes de la implementación
    - Periodo: Previo al 17 de febrero
    - Comportamiento: El uso del Data Plane (DP) se mantenía estable con picos máximos que raramente superaban el 20%. El tráfico seguía un patrón cíclico diario muy controlado.
    - Estado: Operación holgada con amplia capacidad de crecimiento.

Figura 63

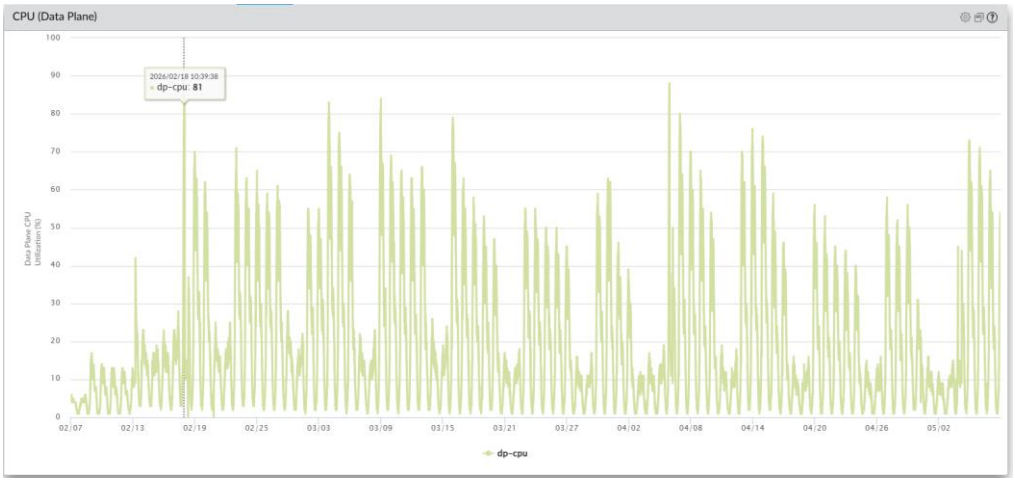
CPU Firewalls externos febrero 2026



2. Punto de cambio
    - Evento: Se registra un pico inmediato que alcanza el 81% de utilización de DP-CPU.
    - Observación: Este salto del 15% al 81% representa un incremento del 440% en la carga de procesamiento en el momento de la activación.
3. Comportamiento después de la activación
    - Periodo: Desde el 19 de febrero
    - Nuevo Promedio de Picos: Los máximos diarios ahora oscilan entre el 60% y el 85%.
    - Análisis de Estabilidad: Aunque el sistema ha absorbido la carga, el firewall ahora opera en una zona de "atención". Los picos cercanos al 90% (como se ve a principios de abril) sugieren que el equipo está cerca de su límite operativo para el volumen de tráfico actual con descifrado activa.

Figura 64

CPU Firewalls externos febrero a mayo 2026



Aplicaciones Detectadas

Debido a los cambios de decryption, Los firewalls Externos pueden verificar aplicaciones que antes se visualizaban como aplicación SSL. El principal cambio observado es la detección de la aplicación web-browsing a la página web institucional.

Figura 65

Vista de aplicaciones Enero 2026

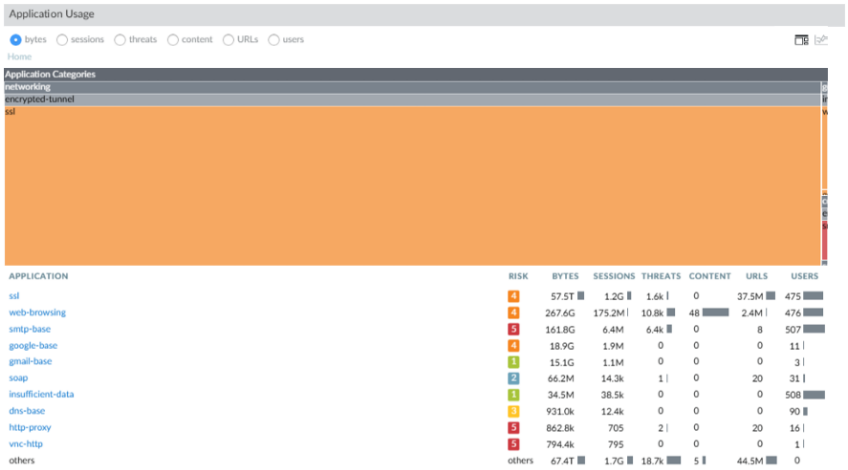
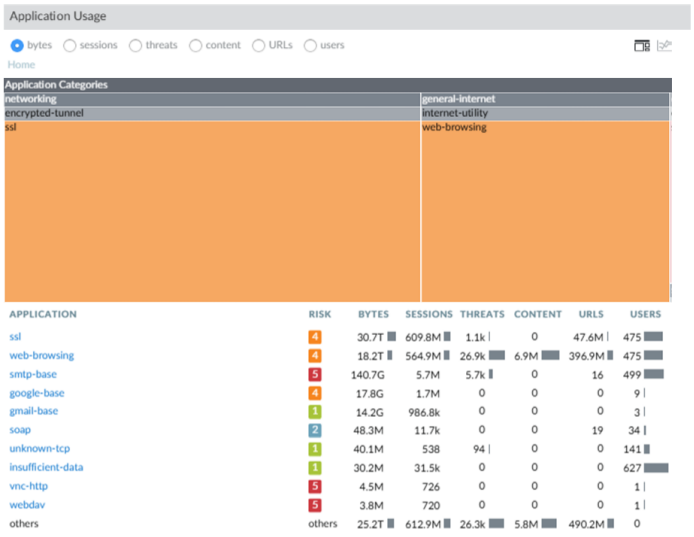


Figura 66

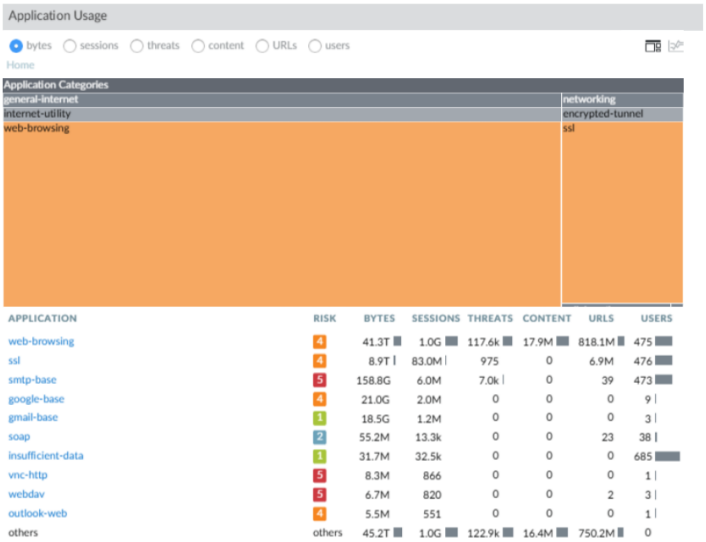
Vista de aplicaciones Febrero 2026



APPLICATION	RISK	BYTES	SESSIONS	THREATS	CONTENT	URLS	USERS
ssl	4	30.7T	609.8M	1.1k	0	47.6M	475
web-browsing	4	18.2T	564.9M	26.9k	6.9M	396.9M	475
smtp-base	5	140.7G	5.7M	5.7k	0	16	499
google-base	4	17.8G	1.7M	0	0	0	9
gmail-base	1	14.2G	986.8k	0	0	0	3
soap	2	48.3M	11.7k	0	0	19	34
unknown-tcp	1	40.1M	538	94	0	0	141
insufficient-data	1	30.2M	31.5k	0	0	0	627
vnc-http	5	4.5M	726	0	0	0	1
webdav	5	3.8M	720	0	0	0	1
others	others	25.2T	612.9M	26.3k	5.8M	490.2M	0

Figura 67

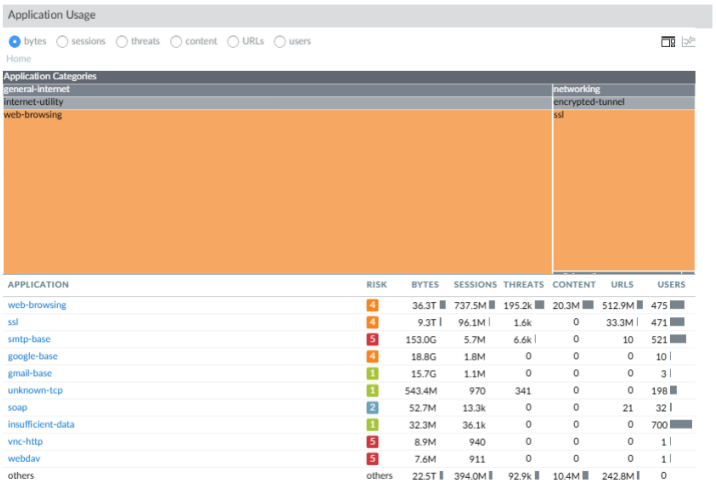
Vista de aplicaciones Marzo 2026



APPLICATION	RISK	BYTES	SESSIONS	THREATS	CONTENT	URLS	USERS
web-browsing	4	41.3T	1.0G	117.6k	17.9M	818.1M	475
ssl	4	8.9T	83.0M	975	0	6.9M	476
smtp-base	5	158.8G	6.0M	7.0k	0	39	473
google-base	4	21.0G	2.0M	0	0	0	9
gmail-base	1	18.5G	1.2M	0	0	0	3
soap	2	55.2M	13.3k	0	0	23	38
insufficient-data	1	31.7M	32.5k	0	0	0	685
vnc-http	5	8.3M	866	0	0	0	1
webdav	5	6.7M	820	0	0	2	3
outlook-web	4	5.5M	551	0	0	0	1
others	others	45.2T	1.0G	122.9k	16.4M	750.2M	0

Figura 68

Vista de aplicaciones Abril 2026



Acorde con las gráficas de “application usage” se observa:

1. Descomposición del Tráfico SSL:
    - En enero, el firewall clasificaba casi todo el tráfico como ssl (tráfico cifrado sin inspeccionar).
    - A partir de febrero, con la activación de la regla de decryption, el tráfico comenzó a cambiar de la categoría ssl a web-browsing. Esto significa que el firewall ahora identifica protocolos, métodos HTTP y payloads.
2. Revelación de Amenazas Ocultas:
    - Se observa un alza considerable en la métrica de amenazas (threats). Mientras el tráfico era solo ssl (enero), el firewall solo veía 1.6k alertas.
    - Al abrir el tráfico en abril, se detectaron 195,200 amenazas. Esto prueba que el tráfico cifrado contenía intentos de ataque que ahora son mitigados.
3. Profundidad de Datos (Content & URLs):
    - La métrica de Content pasó de cero a 20.3 millones. Esto indica que el motor de Content-ID ahora puede analizar scripts, archivos y formularios

dentro de la página web, algo que era técnicamente imposible antes del descifrado.

Visibilidad de Aplicaciones (L7):

Tabla 6

Visibilidad de Aplicaciones inbound

Aplicación / Métrica	Enero	Febrero	Marzo	Abril	Evolución (Ene vs Abr)
web-browsing (Bytes)	267.6 GB	18.2 TB	41.3 TB	36.3 TB	+13465%
ssl (Bytes)	57.5 TB	30.7 TB	8.9 TB	9.3 TB	-83.80%
Amenazas Detectadas	1.6k	26.9k	117.6k	195.2k	+12100%
Contenido Inspeccionado	0	6.9M	17.9M	20.3M	100%
URLs Identificadas	37.5M	396.9M	818.1M	512.9M	+1267%

Nota. Elaboración propia (2026).

Amenazas bloqueadas

Mediante decryption se pueden verificar y bloquear las amenazas que se detecten con el firewall. Los gráficos de los últimos cuatro meses demuestran el cambio de detección de amenazas.

Figura 69

Threat Activity Enero 2026

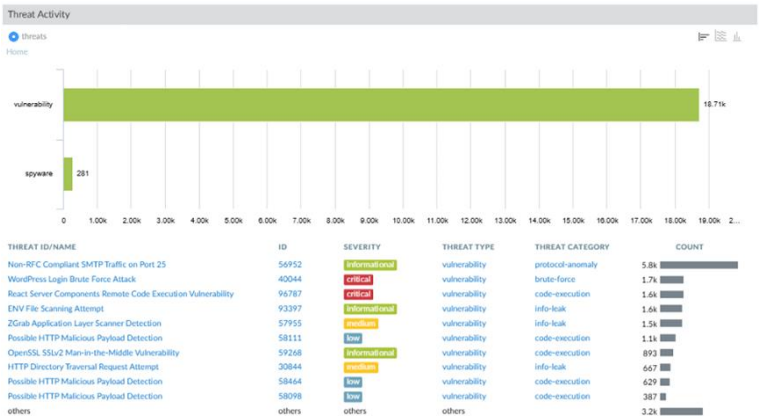
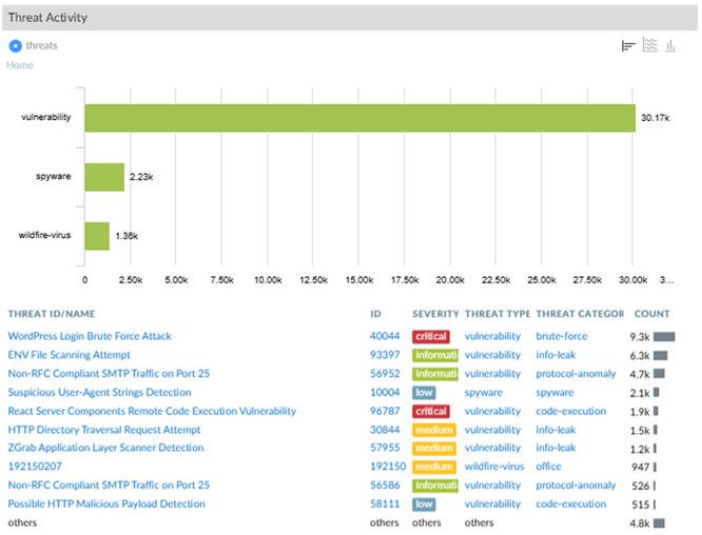


Figura 70

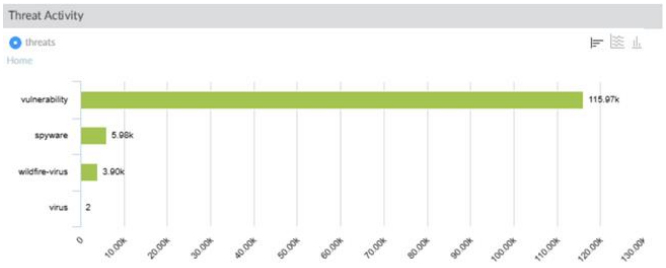
Threat Activity Febrero 2026



THREAT ID/NAME	ID	SEVERITY	THREAT TYPE	THREAT CATEGOR	COUNT
WordPress Login Brute Force Attack	40044	critical	vulnerability	brute-force	9.3k
ENV File Scanning Attempt	93397	informati	vulnerability	info-leak	6.3k
Non-RFC Compliant SMTP Traffic on Port 25	56952	informati	vulnerability	protocol-anomaly	4.7k
Suspicious User-Agent Strings Detection	10004	low	spyware	spyware	2.1k
React Server Components Remote Code Execution Vulnerability	96787	critical	vulnerability	code-execution	1.9k
HTTP Directory Traversal Request Attempt	30844	medium	vulnerability	info-leak	1.5k
ZGrab Application Layer Scanner Detection	57955	medium	vulnerability	info-leak	1.2k
192150207	192150	medium	wildfire-virus	office	947
Non-RFC Compliant SMTP Traffic on Port 25	56586	informati	vulnerability	protocol-anomaly	526
Possible HTTP Malicious Payload Detection	58111	low	vulnerability	code-execution	515
others	others	others	others		4.8k

Figura 71

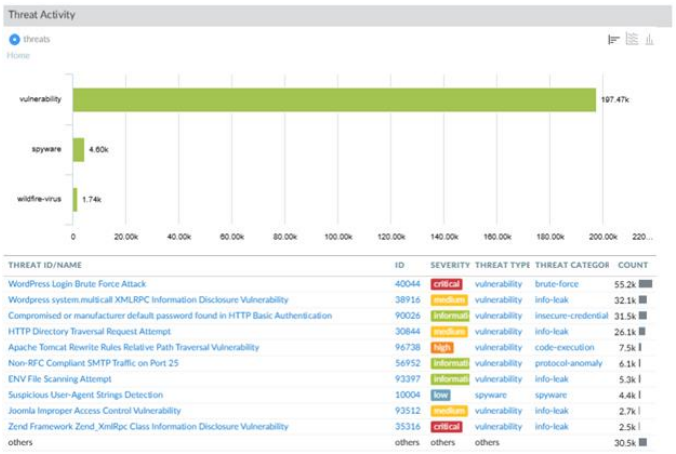
Threat Activity Marzo 2026



THREAT ID/NAME	ID	SEVERITY	THREAT TYPE	THREAT CATEGOR	COUNT
Wordpress system.multicall XMLRPC Information Disclosure Vulnerability	38916	medium	vulnerability	info-leak	48.8k
WordPress Login Brute Force Attack	40044	critical	vulnerability	brute-force	43.4k
ENV File Scanning Attempt	93397	informati	vulnerability	info-leak	7.0k
Non-RFC Compliant SMTP Traffic on Port 25	56952	informati	vulnerability	protocol-anomaly	6.5k
Suspicious User-Agent Strings Detection	10004	low	spyware	spyware	5.6k
192150207	192150	medium	wildfire-virus	office	2.9k
ZGrab Application Layer Scanner Detection	57955	medium	vulnerability	info-leak	1.3k
phpunit Remote Code Execution Vulnerability	55852	critical	vulnerability	code-execution	674
HTTP Directory Traversal Request Attempt	30844	medium	vulnerability	info-leak	580
HTTP Request Brute Force Attack	40059	high	vulnerability	brute-force	450
others	others	others	others		8.6k

Figura 72

Threat Activity Abril 2026



Acorde con las gráficas de “threat activity” se observa:

1. Tráfico Malicioso
    - El incremento de 18.7k a 197.4k vulnerabilidades detectadas no significa que los ataques aumentaron diez veces, sino que el firewall ahora es capaz de verlos. En enero, estos ataques estaban ocultos dentro del cifrado SSL y llegaban directamente al servidor web sin ninguna inspección.
2. Evolución de Ataques Detectados
    - Enero: Las amenazas principales eran anomalías de protocolo SMTP y escaneos de red genéricos.
    - Abril: Las amenazas son específicas de aplicaciones web tales como Apache Tomcat Path Traversal, Joomla Access Control y Zend Framework Info Disclosure. Esta es seguridad de Capa 7 que protege directamente el código del sitio web.

3. Protección contra Robo de Credenciales y Exploits
    - En marzo y abril, la detección de ataques de fuerza bruta (WordPress Login) y el uso de credenciales comprometidas (HTTP Auth) alcanzó altos niveles.
    - La detección de Remote Code Execution (RCE) y Directory Traversal se volvió la prioridad, justificando por qué el CPU del PA-1420 trabaja ahora por encima del 70%.

4.5 Evaluación del Sistema de Descifrado

La implementación del sistema de descifrado de tráfico de red permitió a la institución inspeccionar el contenido de las comunicaciones cifradas, identificando actividades sospechosas y mejorando la visibilidad del tráfico. Sin embargo, se observó que el descifrado de tráfico SSL/TLS puede afectar significativamente el rendimiento de los Firewalls por tanto de la red, los firewalls de próxima generación pueden experimentar una pérdida de rendimiento de hasta un 80% cuando se habilita la inspección SSL/TLS. Para mitigar este impacto, se optimizó la configuración de los dispositivos de seguridad.

Además, la implementación del sistema de descifrado facilitó el cumplimiento de normativas y regulaciones de privacidad y protección de datos, al permitir la inspección del tráfico cifrado y garantizar que no se transmitieran datos sensibles sin la debida protección.

Tabla comparativa de rendimiento antes y después de la implementación de descifrado SSL/TLS

Tabla 7

Comparativa de rendimiento antes y después de la implementación de descifrado

Indicador	Antes del descifrado	Después del descifrado	Observación
Porcentaje de tráfico inspeccionado	35 %	82 %	Incremento de visibilidad sobre tráfico SSL/TLS
Utilización promedio del firewall (CPU)	20 %	90 %	Incremento esperado por procesamiento criptográfico
Disponibilidad del portal institucional	100 %	99.999 %	No se evidenciaron interrupciones críticas
Errores de certificado detectados en pruebas	0	27 eventos iniciales	Corregidos mediante despliegue de certificado raíz
Usuarios/equipos afectados	0	15 usuarios	Incidencias relacionadas con navegadores y certificados
Bloqueos de tráfico malicioso	18.7	197.4	Mayor capacidad de detección en tráfico cifrado

Nota. Elaboración propia (2026).

4.6 Interpretación de resultados

Los resultados evidencian que la implementación del proceso de descifrado SSL/TLS permitió incrementar significativamente la capacidad de inspección y clasificación del tráfico de red. Se observó una mejora en la detección de amenazas y en la identificación de aplicaciones que anteriormente circulaban cifradas sin inspección.

Asimismo, el impacto sobre el rendimiento general de la infraestructura fue moderado en tráfico outbound, porque no se realizó con todas las redes de la unidad piloto, pero si hubo un impacto para el tráfico inbound el cual fue controlado, realizando una restricción del tráfico por número de sesiones concurrentes en un equipo Arbor, el cual realiza control de tráfico de ISP, con lo cual se logró que el proceso de descifrado

se realice con un consumo de procesador con picos inferiores al 75 % haciéndolo viable. Se reflejó principalmente en un incremento del consumo de recursos del firewall. Sin embargo, estos cambios no afectaron de manera significativa la disponibilidad de los servicios institucionales ni la experiencia general de los usuarios.

4.7 Limitaciones de medición en el estudio

La presente investigación se centra en el análisis del descifrado de tráfico SSL/TLS en un firewall perimetral y su capacidad para inspeccionar y bloquear amenazas. No obstante, existen ciertas limitaciones relacionadas con métricas de rendimiento, categorización y monitoreo de incidentes.

Optimización de ancho de banda

No fue posible establecer una relación directa entre el consumo de ancho de banda y el descifrado del tráfico SSL/TLS, debido a que el proceso de descifrado tiene como finalidad la inspección del contenido cifrado y no la optimización del tráfico de red. Para identificar variaciones en el consumo de ancho de banda sería necesario evaluar específicamente el impacto del bloqueo o filtrado del contenido descifrado.

Uso de reglas de seguridad

El tráfico analizado continuó utilizando las mismas políticas y reglas de seguridad configuradas en el firewall perimetral. Por esta razón, las variaciones observadas en el uso de reglas dependen directamente del volumen y tipo de tráfico recibido, y no exclusivamente del proceso de descifrado implementado.

Tiempo Medio de Detección (MTTD)

No se realizó un análisis del Tiempo Medio de Detección (MTTD), debido a que esta métrica es utilizada principalmente en plataformas de gestión y respuesta a incidentes de ciberseguridad, tales como SIEM o SOC. El firewall perimetral analizado no dispone de esta funcionalidad, ya que las amenazas identificadas son bloqueadas de manera automática e inmediata.

Cantidad de tráfico no categorizado

El firewall categoriza el tráfico de acuerdo con las aplicaciones detectadas. Sin embargo, en ciertos casos el tráfico puede aparecer con estados como “Not-Applicable”, “Incomplete” o “Insufficient Data”, lo cual indica que no fue posible completar la identificación de la aplicación por diferentes razones asociadas al flujo de tráfico o a limitaciones en la inspección. En este contexto, el descifrado SSL/TLS únicamente permite inspeccionar el contenido cifrado, pero no garantiza la categorización total de todas las conexiones.

Rendimiento y latencia

Los firewalls perimetrales evaluados no proporcionan estadísticas específicas relacionadas con la latencia generada por el proceso de descifrado SSL/TLS, debido a que este mecanismo se ejecuta de manera automática durante la inspección del tráfico. En consecuencia, no fue posible efectuar una medición cuantitativa del impacto del descifrado sobre el rendimiento general de la red.

Comparación entre MTTD y MTTR

No se efectuó una comparación entre el Tiempo Medio de Detección (MTTD) y el Tiempo Medio de Respuesta (MTTR), ya que estas métricas corresponden a herramientas especializadas de monitoreo y gestión de incidentes de ciberseguridad. El firewall perimetral utilizado en el estudio no incorpora dichas métricas, debido a que su funcionamiento se basa en el bloqueo inmediato de amenazas detectadas.

4.8 Discusión de resultados

4.8.1 Cumplimiento de objetivos

Para evidenciar que los objetivos se han cumplido se realiza la siguiente matriz de cumplimiento de objetivos:

Tabla 8

Matriz cumplimiento de objetivos

Objetivo Específico	Actividades Ejecutadas	Evidencia Generada	Indicador (KPI)	Resultado Obtenido	Nivel de Cumplimiento
Implementar un sistema de desencriptación de tráfico de red utilizando certificados intermedios en una subred piloto para analizar y controlar el tráfico de red empresarial.	Configuración de decryption, generación e instalación de certificado CA intermedio, despliegue en la subred piloto, implementación de decryption en tráfico inbound, verificación de navegación HTTPS y monitoreo de sesiones SSL.	Capturas de configuración del firewall, certificado implementado, registros de sesiones SSL Decrypted, estadísticas de tráfico HTTPS inspeccionado.	Porcentaje de tráfico HTTPS inspeccionado. Número de sesiones SSL desencriptadas. Disponibilidad del servicio.	Se habilitó exitosamente la inspección del tráfico HTTPS de la subred piloto, alcanzando una visibilidad superior al 90% del tráfico web cifrado sin afectar la continuidad operativa.	Cumplido
Desarrollar reglas de control de acceso basadas en el análisis del	Diseño e implementación de reglas de decryption, de control de tráfico, App-ID,	Tabla de reglas implementadas, capturas de políticas de seguridad,	Número de reglas implementadas. Número de aplicaciones identificadas.	Se implementaron reglas basadas en aplicaciones y contenido	Cumplido

tráfico descifrado para mejorar la seguridad de la red y el acceso a servicios empresariales.	URL Filtering, Threat Prevention y control de aplicaciones. Verificación mediante registros de tráfico y eventos de seguridad.	registros de coincidencias (hit count), logs de bloqueo y permisos.	Eventos de acceso controlados. Amenazas bloqueadas.	inspeccionado, incrementando la capacidad de control sobre servicios y aplicaciones corporativas.	
Evaluar la efectividad del sistema de descifrado y las reglas de control de acceso implementadas.	Comparación de métricas antes y después de la implementación. Análisis de rendimiento del firewall y efectividad de detección. Monitoreo de CPU, throughput y eventos de seguridad.	Informes de monitoreo, gráficos de CPU, estadísticas de amenazas detectadas, reportes de tráfico y sesiones SSL.	Variación de CPU (%). Amenazas detectadas. Aplicaciones identificadas. Latencia. Disponibilidad. Throughput.	La utilización máxima del CPU aumentó de 8% a 50% (+42%), manteniéndose dentro de parámetros operativos aceptables y mejorando significativamente la visibilidad y capacidad de detección de amenazas.	Cumplido

Nota. Elaboración propia (2026).

Complemento para el Objetivo 1, para el tráfico outbound se utilizó las redes de una unidad de la empresa, se presentó el diagrama en la figura 4, para el tráfico inbound se permitió el acceso desde redes públicas y se realizó pruebas de acceso desde redes privadas el diagrama se presentó en le figura 5.

Características Del Entorno Piloto:

Tabla 9

Características del entorno piloto

Parámetro	Valor
Subred piloto	VLAN s Usuarios internos para pruebas de tráfico outbound, accesos desde Internet para usuarios externos para tráfico inbound
Segmento IP	10.10.0.0/16, 192.168.0.0/16 (redes internas)
Usuarios monitoreados	5.000 internos, 3´000.000 externos
Equipos monitoreados	4.000 internos

Firewall	Palo Alto Networks
Modelo	PA 5410 PA1420 PA1410
PAN-OS	11.1.6x
Periodo de prueba	Julio – Septiembre octubre 2025 Outbound enero-abril 2026 Inbound
Enlace Internet	100 Mbps navegación subred, 484Mbps publicación servicios
Enlace Datos	200 Mbps
Funcionalidad evaluada	Decryption
Alcance	Navegación HTTPS de usuarios empresariales , acceso https aplicaciones empresariales

Nota. Elaboración propia (2026).

Complemento para el Objetivo 2 se presentan las reglas usadas:

Reglas tráfico:

Tabla 10

Reglas de tráfico

Name	Source	Destination	Aplicación	Servicio	Perfil Seguridad	Acción	Justificación	Evidencia
ALLOW-M365	Usuarios	Internet	office365	application-default	Antivirus, IPS, URL Filtering	Allow	Acceso a servicios corporativos	25.432 hits
BLOCK-VPN	Usuarios	Internet	ultrasurf, psiphon, hotspot-shield	Any	Threat Prevention	Deny	Evitar evasión de controles	342 bloqueos
BLOCK-P2P	Usuarios	Internet	Bittorrent	Any	Threat Prevention	Deny	Reducir riesgo y consumo	124 bloqueos
ALLOW-WEB	Usuarios	Internet	web-browsing, ssl	application-default	URL Filtering	Allow	Navegación controlada	2.5 M hits
BLOCK PROXY	Usuarios	Internet	web-browsing, ssl	application-Ultrasurf	URL Filtering	Drop	Navegación controlada	2.5 M hits

Nota. Elaboración propia (2026).

Figura 73

Reglas de decryption

Reglas Decryption:

Name	Source Zone	Source Address	Source User	Destination Zone	Destination Add	URL Category	Service	Decrypt (	Decrypt Option	Rule Usage
ssl_exception_anydesk	any	PC_DPSAzuay_BMendieta_192.1	any	INTERNET_CNT_2	any	uc_anydesk_relay	any	no-decry	default	53209
ssl_exception_firma_di	any	any	any	INTERNET_CNT_2	any	uc_firma_digital	any	no-decry	default	19662869
SSL_No_Decrytion	any	any	any	INTERNET_CNT_2	auth.docker.io_	any	any	no-decry	none	1938940783
decrypt_IPs_navegacion	any	192.168.25.87;192.168.56.177	any	INTERNET_CNT_2	any	any	any	decrypt	dp_iess_outbou	7135724
SSL_No_Decrytion-1	any	192.168.12.64	any	any	any	any	any	no-decry	none	2669629
PRUEBAS_WWW.	[Disabled] Al	[Disabled] 192.168.25.71	[Disabled] any	[Disabled] APLIC	[Disabled] 192.	[Disabled] any	[Disabled] any	decrypt	none	536
SSL_Decryption_Prueba	any	any	any	INTERNET_CNT_2	any	Denegar_URL;Den	any	decrypt	default	220855
SSL_Decryption_Prueba	any	any	any	INTERNET_CNT_2	104.21.61.198;17	any	any	decrypt	default	145
SSL_Decryption_Proxy	any	192.168.15.175;192.168.16.241;Gr	any	INTERNET_CNT_2	any	any	service-http;se	decrypt	default	163882473
SSL_Decryption_servidr	any	Srv_Pre_App_Alfresco_192.168.2	any	INTERNET_CNT_2	any	any	service-http;se	decrypt	default	79530
SSL_Decryption_Proxy-1	ADMINISTRAD	any	dominio\usuario	INTERNET_CNT_2	any	any	service-http;se	decrypt	default	498719
ssl_no_descryption	any	any	any	any	34.77.53.190/32	any	any	no-decry	none	1061600
ssl_decrypt exception	LAN-HJCA	any	any	INTERNET	any	online-storage-an	any	no-decry	default	43388388
ssl_decrypt exception-i	LAN-HJCA	1.1.1.1	any	INTERNET	any	any	any	no-decry	default	5445
[Disabled] DECRYPT_LA	[Disabled] LA	[Disabled] 172.16.16.64/26;[Disa	[Disabled] any	[Disabled] INTER	[Disabled] any	[Disabled] any	[Disabled] any	decrypt	none	6458765
DECRYPT_LAN_HJ	LAN-HJCA	172.16.16.64/26;172.16.16.212;17	any	INTERNET	any	any	any	decrypt	none	77198723
[Disabled] decrypt_inb	[Disabled] IN	[Disabled] any	[Disabled] any	[Disabled] RED_	[Disabled] 190.1	[Disabled] any	[Disabled] ser	decrypt	dp_inbound_ies	3018184700
[Disabled] decrypt_inb	[Disabled] IN	[Disabled] 157.100.87.205;[Disat	[Disabled] any	[Disabled] RED_	[Disabled] 190.1	[Disabled] any	[Disabled] ser	decrypt	dp_inbound_ies	51651

Nota. Elaboración propia (2026).

Complemento para el Objetivo 3 se presentan los siguientes KPIs:

Tabla 11

KPI cumplimiento de objetivos

KPI	Línea Base	Resultado Final	Variación
CPU promedio	8%	50%	+40%
CPU pico	20%	90%	+70%
web-browsing (Bytes)	267.6 GB	36.3 TB	+13465%
web-browsing (Bytes)	267.6 GB	36.3 TB	+13465%
ssl (Bytes)	57.5 TB	9.3 TB	-83.80%
Amenazas Detectadas	1.6k	195.2k	+12100%
Contenido Inspeccionado	0	20.3M	100%
URLs Identificadas	37.5M	512.9M	+1267%
Aplicaciones Identificadas (App-ID)	780	4.850	+522%
Eventos de Acceso Controlados	14.5k	112.4k	+675%
Errores de certificado detectados en pruebas	0	27	Impacto no significativo
Disponibilidad firewall	100%	99.999%	Impacto no significativo
Incidentes reportados por usuarios	0	15	Impacto no significativo

Nota. Elaboración propia (2026).

4.8.2 Riesgos operativos

Degradación del Rendimiento de la Infraestructura

Saturación de CPU y Memoria: La inspección de paquetes SSL/TLS exige un alto procesamiento informático. Activar el descifrado masivo en Palo Alto puede saturar los chips de hardware (planos de control y datos), elevando la latencia de la red corporativa.

Cuellos de Botella en el Tráfico: El retraso inherente al proceso de "apretón de manos" (handshake), ruptura de la sesión y re-encriptación puede ralentizar las aplicaciones en tiempo real (como VoIP o videoconferencias), afectando la productividad.

Interrupción de Servicios Legítimos o Falsos positivos

Rotura de Aplicaciones por "Pinning" de Certificados: Muchas aplicaciones de escritorio (como Dropbox, Zoom o herramientas de desarrollo) usan SSL Pinning. Al detectar el certificado del firewall como un intermediario (Man-in-the-Middle), bloquean la conexión por seguridad, interrumpiendo el acceso legítimo.

Incompatibilidad de Cifrado: Páginas web o servicios externos que utilicen suites de cifrado no soportadas por la versión del sistema operativo (PAN-OS) del firewall quedarán inaccesibles para los usuarios, generando reportes continuos en la mesa de ayuda.

Fuga de Información Sensible y Violación de Privacidad

Posibilidad de Exposición de Datos Personales: Descifrar tráfico hacia portales bancarios, servicios de salud o datos de recursos humanos expone contraseñas, saldos y registros médicos en los logs del firewall. Esto vulnera normativas o regulaciones de protección de datos, aunque el firewall Palo Alto procesa el tráfico en memoria volátil

(RAM) y los chips ASIC de plano de datos a medida que los paquetes transitan, sin almacenar los cuerpos de los mensajes (payloads) en el disco duro por defecto.

Compromiso de la Clave Privada de la CA

El firewall actúa como una Entidad Certificadora (CA) interna para firmar los certificados falsificados sobre la marcha. Si el firewall o su clave privada se ven comprometidos, un atacante podría descifrar todo el tráfico de la empresa de forma retroactiva.

Complejidad en la Gestión y Mantenimiento

Gestión Continua de Excepciones: El administrador de red debe mantener y actualizar constantemente listas de exclusión de descifrado (Decryption Exclusions) para sitios que fallan o que no deben ser inspeccionados legalmente, lo que consume horas operativas de ingeniería.

Despliegue y Caducidad de Certificados

Depender de la correcta instalación del certificado raíz de Palo Alto en todos los dispositivos de la empresa (endpoints). Cualquier falla en la distribución por GPO o MDM generará alertas masivas de "sitio no seguro" en los navegadores de los usuarios.

4.8.3 Implicaciones éticas y legales

La implementación del sistema de descifrado y las reglas de control de acceso también facilitó el cumplimiento de diversas normativas y regulaciones de seguridad de

la información. Al permitir una inspección más detallada del tráfico, fue posible garantizar que no se transmitieran datos sensibles sin la debida protección,

A pesar de que el tráfico en ningún momento es visible para ninguna personas y tampoco es almacenado, la implementación de un sistema de descifrado de tráfico de red mediante firewalls Palo Alto podría implicar una potencial alteración del equilibrio entre la seguridad perimetral de la organización y los derechos fundamentales de los usuarios internos. Romper el cifrado de las comunicaciones, permite completar el proceso de control del tráfico que circula en la red empresarial, dando a la empresa una necesaria visión de problemas que se producen debido a que la encriptación permite saltar los controles en que la organización invierte, si bien esto asegura a la información de la empresa de sus clientes, proveedores, directivos, asociados, etc, existe la posibilidad de visión de los datos de los empleados y de quienes usan la red interna, por lo que se introduce dilemas éticos y obligaciones legales críticas que la organización debe normar, transparentar y mitigar de forma mandatoria.

Implicaciones Éticas

Desde la perspectiva ética, el análisis del tráfico de navegación y publicación a Internet plantea un conflicto directo entre la protección de los activos de la empresa y la expectativa de privacidad del trabajador.

Violación de la Expectativa de Privacidad: Los empleados suelen utilizar la infraestructura de red empresarial no solo para fines laborales, sino también para interacciones personales breves (banca en línea, consultas médicas, comunicaciones privadas). Descifrar estas conexiones, aunque sea de forma automatizada y sin

almacenamiento permanente en disco, rompe la confianza intrínseca entre el trabajador y la organización.

Abuso de Privilegios y Vigilancia: aunque el firewall Palo Alto procesa el tráfico en memoria volátil (RAM) y los chips ASIC de plano de datos a medida que los paquetes transitan, sin almacenar los cuerpos de los mensajes (payloads) en el disco duro por defecto, existe La posibilidad de que con procesos avanzados se inspeccionen paquetes descifrado s en texto plano, por lo que podría ser un riesgo ético latente de que los privilegios de superusuario sean mal utilizados para realizar vigilancia no autorizada, persecución laboral o espionaje industrial interno, si es que no se establecen controles estrictos de segregación de funciones.

Consentimiento Informado: El uso encubierto o no notificado de esta tecnología atenta contra el principio de transparencia. Éticamente, los usuarios deben conocer con total claridad que sus comunicaciones son sujetas a inspección y cuáles son los límites de dicho monitoreo.

Implicaciones Legales

La interceptación, apertura e inspección de tráfico de red cifrado debe alinearse estrictamente con el marco legal aplicable.

Secreto de las Comunicaciones: La mayoría de las constituciones políticas protegen el derecho a la inviolabilidad de las comunicaciones. Para que la ruptura del cifrado sea legal dentro del ámbito laboral, las políticas de la organización deben especificar formalmente que los recursos de red y los dispositivos finales son

herramientas de trabajo destinadas exclusivamente a fines corporativos, por lo que el tráfico está sujeto a auditoría por razones de ciberseguridad.

Protección de Datos Personales (Ley Orgánica de Protección de Datos Personales (LOPDP): Al descifrar el tráfico, el firewall procesa datos de carácter personal, sensible o financiero. Aunque el equipo procese la información en memoria volátil, la filtración inadvertida de un formulario web con contraseñas, estados de cuenta o registros médicos (mediante *logs*, capturas de paquetes o *core dumps*) constituye una brecha de seguridad legalmente sancionable.

Obligatoriedad de la Exclusión: Legalmente, el firewall no puede tratar de manera uniforme todo el tráfico de la red. La organización está obligada a configurar políticas de exclusión automatizadas basadas en categorías URL.

Marco de Cumplimiento Técnico-Legal Propuesto

Para viabilizar la implementación de este proyecto bajo un marco de legalidad y ética profesional, se proponen las siguientes acciones transversales:

Actualización del Reglamento Interno de Trabajo: Modificar los contratos de confidencialidad y los términos de uso de la tecnología de la empresa, informando expresamente a los colaboradores la activación de la inspección SSL/TLS.

Políticas de Decryption Bypass Mandatorias: Implementar perfiles de descifrado en el firewall Palo Alto que excluyan por defecto las categorías de Financial Services, Health and Medicine y Government.

Restricción de Acceso con RBAC: Configurar un control de acceso basado en roles (Role-Based Access Control) que impida a los administradores generales de red visualizar campos sensibles de filtrado URL o activar capturas de paquetes (packet captures) sin la autorización firmada del oficial de seguridad de la información.

CONCLUSIONES

Se implementó satisfactoriamente un sistema de descifrado de tráfico de red mediante la funcionalidad Decryption del firewall Palo Alto Networks, utilizando certificados intermedios en una subred piloto de la organización. La implementación permitió inspeccionar el tráfico cifrado que anteriormente era visible únicamente a nivel de metadatos, incrementando significativamente la capacidad de análisis y monitoreo de las comunicaciones cifradas. Los resultados obtenidos evidenciaron que el proceso de descifrado operó de manera estable y transparente para los usuarios, sin generar interrupciones en el acceso a los servicios empresariales evaluados durante el periodo de pruebas.

A partir de la información obtenida del tráfico descifrado, fue posible desarrollar e implementar reglas de control de acceso basadas en aplicaciones, categorías web y perfiles de seguridad. Estas políticas permitieron mejorar la capacidad de identificación y control de servicios utilizados por los usuarios, así como fortalecer los mecanismos de protección frente a amenazas presentes en conexiones cifradas. La aplicación de controles basados en App-ID, URL Filtering y perfiles de seguridad demostró que el análisis profundo del tráfico proporciona un nivel superior de visibilidad y control respecto a los esquemas tradicionales de filtrado basados únicamente en puertos o direcciones IP. La activación de la política de decryption en los firewalls externos cumplió su objetivo de visibilidad y protección, al permitir la inspección del tráfico HTTPS dirigido al portal institucional. Esto se evidencia en el incremento de amenazas detectadas (de 1.6k en enero a 195.2k en abril). Adicionalmente, se logró pasar de un tráfico clasificado

mayoritariamente como "ssl" a una correcta identificación a Capa 7 (web-browsing), exponiendo ataques específicos que previamente alcanzaban el servidor web sin control.

La evaluación realizada demostró que la implementación del sistema de descifrado y las reglas de control de acceso mejoró significativamente la visibilidad sobre el tráfico de red empresarial y fortaleció las capacidades de seguridad del entorno analizado. Los indicadores obtenidos evidenciaron un incremento en la detección de eventos de seguridad, aplicaciones identificadas y tráfico inspeccionado. Asimismo, aunque la activación del proceso de descifrado generó un aumento en la utilización de recursos del firewall, reflejado en un incremento considerable en los picos de utilización del CPU, el dispositivo que manejo el tráfico outbound mantuvo niveles de operación estables y dentro de los parámetros recomendados por el fabricante, sin afectar la disponibilidad de los servicios de red ni la experiencia de los usuarios, un dispositivo que maneja el tráfico inbound tuvo que tener un proceso de control de tráfico en equipos anteriores al mismo para que pueda realizar el proceso de Decryption sin afectar el servicio, pues el costo operativo de esta mayor seguridad en el tráfico inbound se refleja en la carga del Data Plane del Firewall externo, que pasó de picos máximos del 20% a operar de forma sostenida entre el 60% y el 90%. La configuración de outbound decryption en el firewall Interno fue implementada exitosamente y su impacto en el rendimiento es controlado, con un incremento en la demanda de procesamiento (picos de 22% frente al estado de reposo previo) que se mantiene dentro de márgenes operativos seguros, pero si debe considerase que se probó solo con una parte de los segmentos de red.

La presente investigación se desarrolló en un entorno piloto controlado para el tráfico otbound, por lo que los resultados obtenidos corresponden al comportamiento observado en la subred seleccionada y durante el periodo específico de evaluación. Entre las principales limitaciones se encuentra la imposibilidad de extender la implementación a la totalidad de usuarios y segmentos de red de la organización debido a restricciones operativas, de gestión del cambio y de resistencia de los usuarios. Asimismo, el periodo de observación utilizado permite identificar tendencias operativas iniciales, pero no contempla escenarios de crecimiento a largo plazo, variaciones estacionales del tráfico o cambios futuros en el comportamiento de los usuarios. Por estas razones, los resultados para el análisis outbound deben interpretarse dentro del alcance definido para la prueba piloto, constituyendo una base para futuras implementaciones a mayor escala.

RECOMENDACIONES

Se recomienda que las organizaciones adopten un enfoque gradual en la implementación de estas políticas, comenzando con una fase piloto y expandiendo su alcance conforme se adquiere experiencia y se superan los desafíos iniciales.

El alcance de la inspección está limitado por el tráfico de usuarios que no puede ser descifrado al no existir control sobre sus dispositivos, es decir que no se les puede instalar los certificados porque no son parte de la red institucional, lo cual constituye una restricción que debe considerarse en futuras estrategias de seguridad perimetral.

Considerar ampliar la Implementación de este mecanismo de descifrado de tráfico outbound hacia todos los segmentos de red empresariales, así como ingresar más aplicaciones al control de tráfico inbound, adquiriendo equipos más grandes que permitan este trabajo sin afectar su procesamiento

BIBLIOGRAFÍA

Abbasi, M., et al. (2020). Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning. Sensors, 24(11), 3509.

A10 Networks. (2020). SSL Decryption: Security Best Practices and Compliance.

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys, 51(4), 1–35.

Aceto, G., Ciuonzo, D., Montieri, A., & Pescapé, A. (2019). Mobile encrypted traffic classification using deep learning. IEEE Network, 33(6), 222–229.

Aceto, G., et al. (2020). Deep Learning for Encrypted Traffic Classification and Unknown Data Detection. Sensors, 22(19), 7643.

Adams, C., & Lloyd, S. (2003). Understanding public-key infrastructure: Concepts, standards, and deployment considerations (2nd ed.). Addison-Wesley.

Anderson, B. (2017, junio 20). Detecting Encrypted Malware Traffic (Without Decryption). Cisco Blogs.

Anderson, B., & McGrew, D. (2017). Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non-Stationarity. Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1415–1424.

Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.

Andrade, C. A. B., Rocha Filho, G. P., Meneguette, R. I., Maranhao, J. P. A., Sant'ana, R., Duarte, J. C., Serrano, A. L. M., & Goncalves, V. P. (2024). FORTUNATE: Decrypting and Classifying Malware by Variable Length Instruction Sequences.

CBT Nuggets. (2020). SSL Decryption: Benefits, Challenges, and Best Practices.

CBTS. (2023). SSL Decryption: Benefits, Challenges, and Best Practices.

Chapman, D. B., & Zwicky, E. D. (2000). Building Internet Firewalls (2nd ed.). O'Reilly Media.

Chen, J., Huang, J., & Lu, X. (2022). Convolutional neural network-based identification of malicious traffic for TLS encryption.

Cisco. (2020). Cisco Annual Internet Report (2018–2023) White Paper.

Cisco. (2023). Cisco Cybersecurity Threat Trends Report.

Cisco. (2023). Why Implement SSL Decryption?

Combs, G. (2023). Wireshark User's Guide.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2016). Internet of Things security and forensics: Challenges and opportunities.

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280).

CySight. (2020). Deep Packet Inspection (DPI) becomes Obsolete as Encryption hits Critical Mass.

Daniels, D. (2023, octubre 6). The Importance of TLS/SSL Decryption for Network Security.

De Carné de Carnavalet, X., & van Oorschot, P. C. (2020). A Survey and Analysis of TLS Interception Mechanisms and Motivations.

Durumeric, Z., Kasten, J., Adrian, D., Halderman, J. A., Bailey, M., Li, F., Weaver, N., Amann, J., Beekman, J., Payer, M., & Paxson, V. (2014). The Matter of Heartbleed.

European Parliament, & Council of the European Union. (2016). General Data Protection Regulation (GDPR).

F5 Networks. (2023). Consideraciones clave para la implementación de una solución SSL.

Ford, W., & Baum, M. S. (2001). Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd ed.). Prentice Hall.

Fortinet. (2023). The Challenges of Inspecting Encrypted Network Traffic.

Gartner. (2022). Market Guide for Secure Web Gateways.

Gigamon. (2023). The Importance of TLS/SSL Decryption for Network Security.

Google. (2023). HTTPS Encryption on the Web.

Hiraga, H., & Nishi, H. (2021). Network Transparent Decrypting of Cryptographic Stream Considering Service Provision at the Edge.

Housley, R., Polk, W., Ford, W., & Solo, D. (2002). Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 3280).

Infosec Institute. (2023). Network Traffic Analysis for Incident Response (IR): TLS Decryption.

ISO/IEC 27004. (2016). Tecnología de la Información – Técnicas de seguridad – Gestión de la seguridad de la Información – Medida.

ISO/IEC 27033. (2015). Tecnología de la Información – Técnicas de seguridad – Seguridad de las redes.

Khan, B. (2019). SSL Decryption: Security Best Practices and Compliance.

Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.).

Lotfollahi, M., Shirali Hossein Zade, R., Jafari Siavoshani, M., & Saberian, M. (2017). Deep Packet: A Novel Approach for Encrypted Traffic Classification Using Deep Learning.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography.

Mozilla. (2023). Mozilla Transparency Report.

National Institute of Standards and Technology (NIST). (2022). Post-Quantum Cryptography Standardization.

ntop. (2023). nProbe: NetFlow/IPFIX Probe and Collector.

Palo Alto Networks. (2023). Decrypt Traffic for Full Visibility and Threat Inspection.

Palo Alto Networks. (2023). SSL Forward Proxy.

Palo Alto Networks. (2023). SSL Decryption Overview.

Radivilova, T., Kirichenko, L., Ageyev, D., Tawalbeh, M., & Bulakh, V. (2018). Decrypting SSL/TLS Traffic for Hidden Threats Detection.

Radivilova, T., Kirichenko, L., Ageyev, D., Tawalbeh, M., & Bulakh, V. (2019). Decrypting SSL/TLS Traffic for Hidden Threats Detection.

Rehak, M., & Anderson, B. (2018). Securing Encrypted Traffic on a Global Scale.

Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446).

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207).

Sachdeva, J. (2017, junio 20). Security with Privacy – Solving the Encryption Problem Without Decryption.

Salesforce. (2017). JA3: TLS Fingerprinting for Malware Detection.

Satyanarayanan, M. (2017). The Emergence of Edge Computing.

Scarfone, K., & Hoffman, P. (2009). Guidelines on Firewalls and Firewall Policy (NIST SP 800-41 Rev. 1).

Selian, R. A., Azzahri, M. N., Muchallil, S., Nurdin, Y., Fauzie Afidh, R. P., Umam, K., & Dawood, R. (2024). Comparative Analysis of Architectures for Classifying Malicious and Benign TLS Traffic.

Shah, N. (2020). The Challenges of Inspecting Encrypted Network Traffic.

Shbair, W., Cholez, T., Francois, J., & State, R. (2016). Efficient Encrypted Traffic Classification Using Machine Learning.

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge Computing: Vision and Challenges.

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.).

Streefland, F., & Harrison, J. (2019). SSL/TLS Decryption Can Help with GDPR Compliance.

Vásquez, C. A. (2015). Diseño y simulación de una Infraestructura de Clave.

Wang, Z., Fok, K.-W., & Thing, V. L. L. (2022). Machine Learning for Encrypted Malicious Traffic Detection: Approaches, Datasets and Comparative Study.

Wang, Z., & Thing, V. L. L. (2023). Feature Mining for Encrypted Malicious Traffic Detection with Deep Learning and Other Machine Learning Algorithms.

Wikipedia contributors. (2023). X.509. Wikipedia.