EVIDENCIA 50 FINAL V1

Protección de las transferencias de información - Anexo 10

Expediente técnico de SENDERO FUEL para documentar los controles utilizados en la transferencia de información entre centros de datos, oficinas, usuarios, beneficiarios, estaciones de servicio, proveedores tecnológicos, servicios expuestos, APIs, integraciones, respaldos y canales administrativos.

1. Interpretación del control

SENDERO FUEL interpreta el punto 50 como la obligación de proteger la información durante su transferencia frente a intercepción, copia no autorizada, modificación, borrado, pérdida y transmisión de código malicioso. El control debe aplicarse a los canales internos y externos, incluyendo comunicaciones entre sedes, centros de datos, usuarios, terceros, aplicaciones, APIs, respaldos y canales administrativos.

2. Objetivo

Integrar evidencia técnica y documental que permita demostrar que las transferencias de información relacionadas con el monedero electrónico de combustibles se realizan mediante mecanismos seguros, trazables y controlados, y que existen medidas preventivas, detectivas y de recuperación acordes con el riesgo.

3. Alcance

- Centro de Datos NGX y Centro de Datos ASSETEL.
- Oficinas operativas y administrativas.
- Portales web y aplicaciones móviles para clientes/beneficiarios.
- APIs y servicios expuestos del monedero.
- Respaldos locales, réplicas, repositorios y almacenamiento en nube cuando aplique.
- Transferencias administrativas y conexiones con proveedores tecnológicos.
- Registros, archivos operativos y configuraciones que formen parte de los flujos del monedero.

4. Inventario y tipos de transferencia considerados

El archivo fuente identifica infraestructura física y virtual asociada a la operación del monedero, incluidos firewalls, switches, hosts VMware, almacenamiento, servidores de aplicación, bases de datos, backend, NTP, GLPI, Grafana y Wazuh. Para el control 50, la evidencia se organiza por flujo de transferencia y por riesgo protegido.

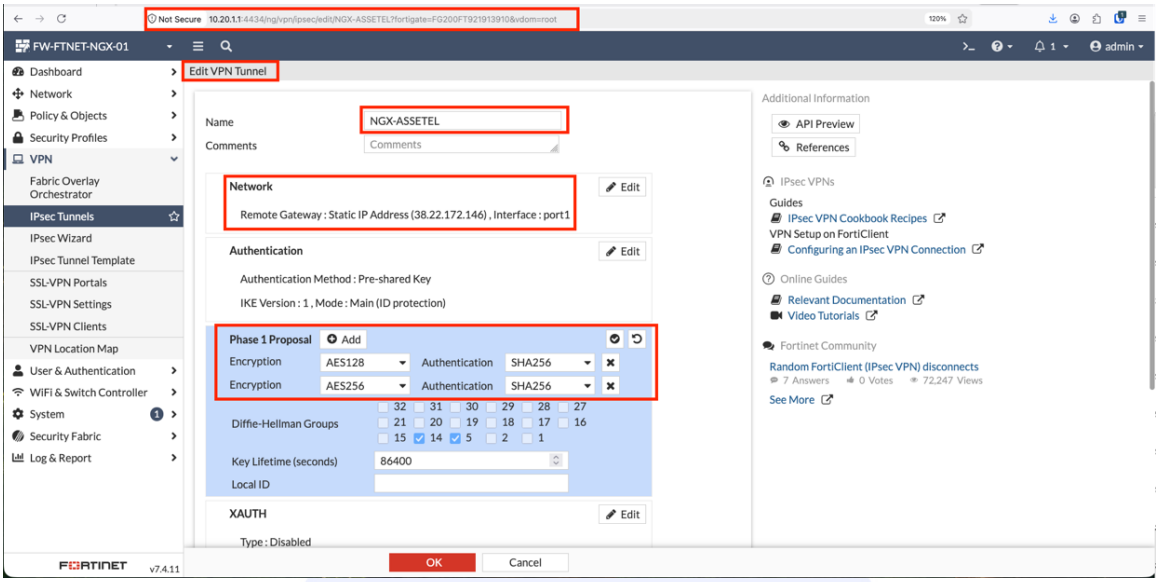
Tipo de transferencia	Origen / destino	Mecanismo evidenciado
Entre centros de datos	NGX ↔ ASSETEL	Túneles IPsec con AES y SHA-256
Oficinas ↔ centros de datos	Oficinas ↔ NGX / ASSETEL	Túneles IPsec
Clientes / beneficiarios	Navegador/app ↔ portal	HTTPS/TLS
APIs / servicios expuestos	Cliente/estación ↔ APIs	HTTPS + WAF SafeLine
Respaldos	VMware/Veeam ↔ StoreOnce/Wasabi	Proxy de backup + cifrado/HTTPS
Administración	Personal/proveedor ↔ infraestructura	Pendiente consolidar controles y trazabilidad específicos

5. Protección contra intercepción

5.1. Transferencia entre NGX y ASSETEL

Requisito	Demostrar que el canal entre centros de datos se encuentra cifrado y autenticado.
Estado	**INTEGRADA**

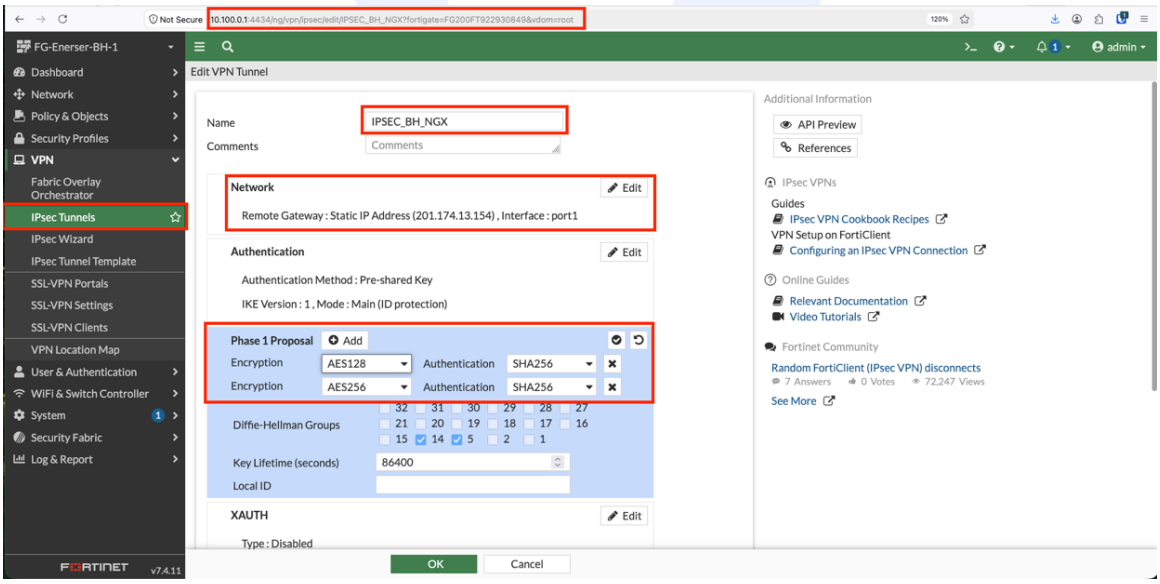
La evidencia muestra la configuración de un túnel IPsec desde el firewall de NGX hacia ASSETEL, utilizando algoritmos de cifrado AES128/AES256 y autenticación SHA-256.



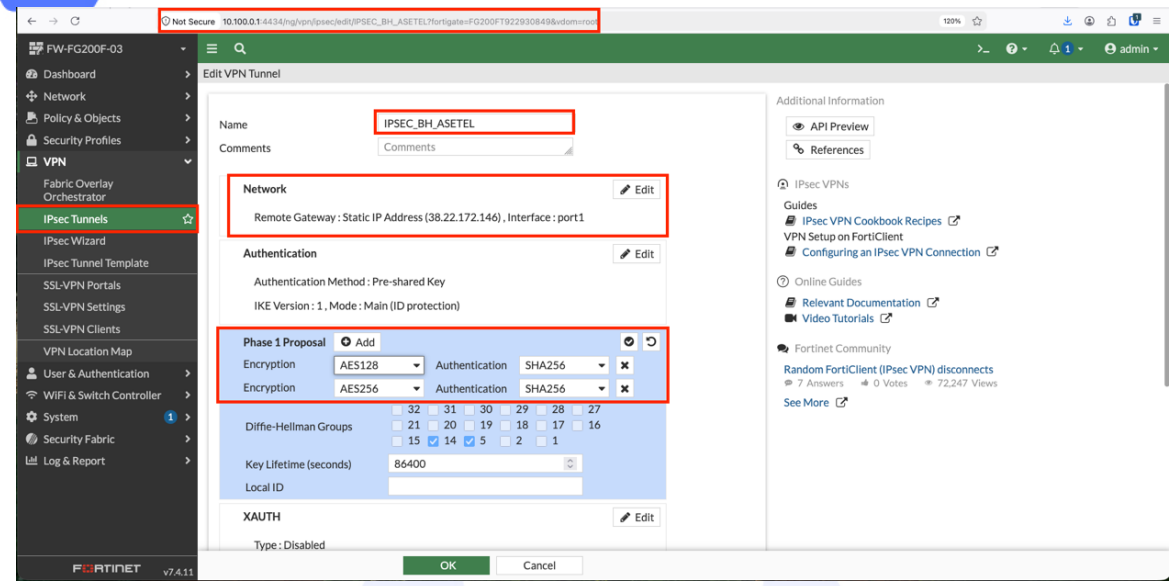
E50-INT-01. Configuración IPsec NGX ↔ ASSETEL.

5.2. Transferencias entre oficinas y centros de datos

Requisito	Demostrar que las comunicaciones de las oficinas hacia NGX/ASSETEL utilizan túneles cifrados.
Estado	**INTEGRADA**



E50-INT-02. Túnel IPsec oficinas ↔ NGX.

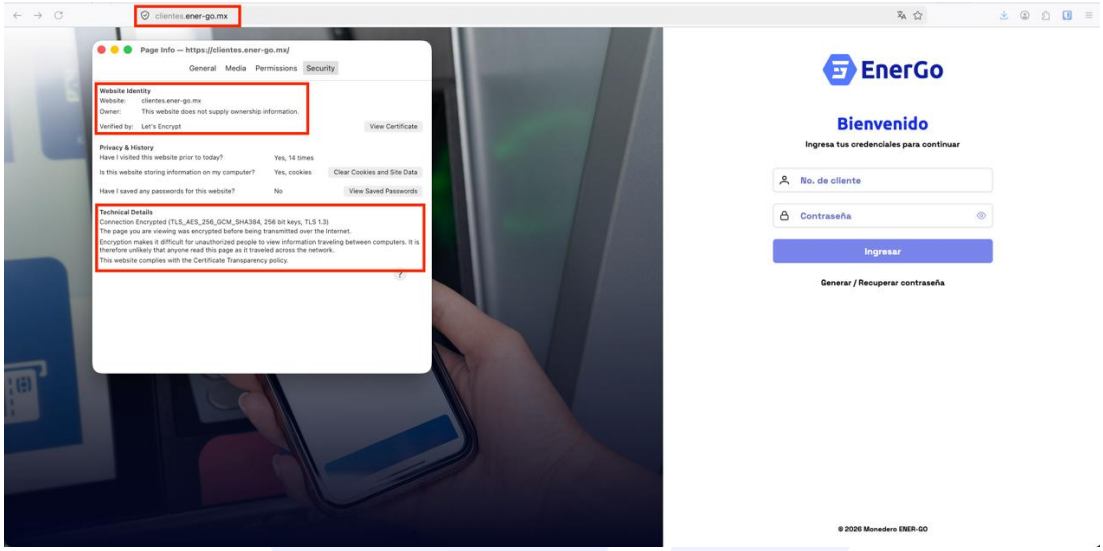


E50-INT-03. Túnel IPsec oficinas ↔ ASSETEL.

5.3. Transferencias con beneficiarios y usuarios

Requisito	Demostrar cifrado TLS en los canales web utilizados por beneficiarios/usuarios.
Estado	**INTEGRADA**

La evidencia muestra el portal de clientes utilizando HTTPS y un certificado emitido por Let's Encrypt. La versión final debe conservar la evidencia del certificado y la negociación TLS observada en el navegador.



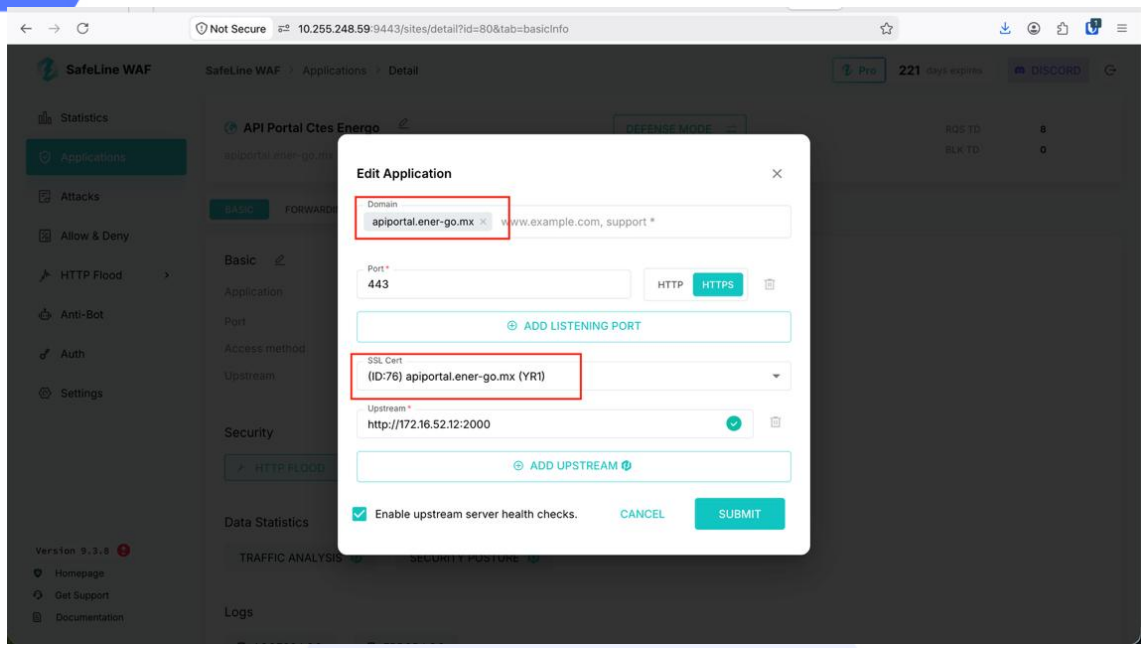
E50-INT-04. Certificado TLS del portal de clientes.

5.4. APIs y servicios expuestos

Requisito	Demostrar que las APIs se publican mediante HTTPS y que el WAF despacha el certificado correspondiente al dominio.
Estado	**INTEGRADA**



E50-INT-05. Certificado HTTPS observado en endpoint de API.



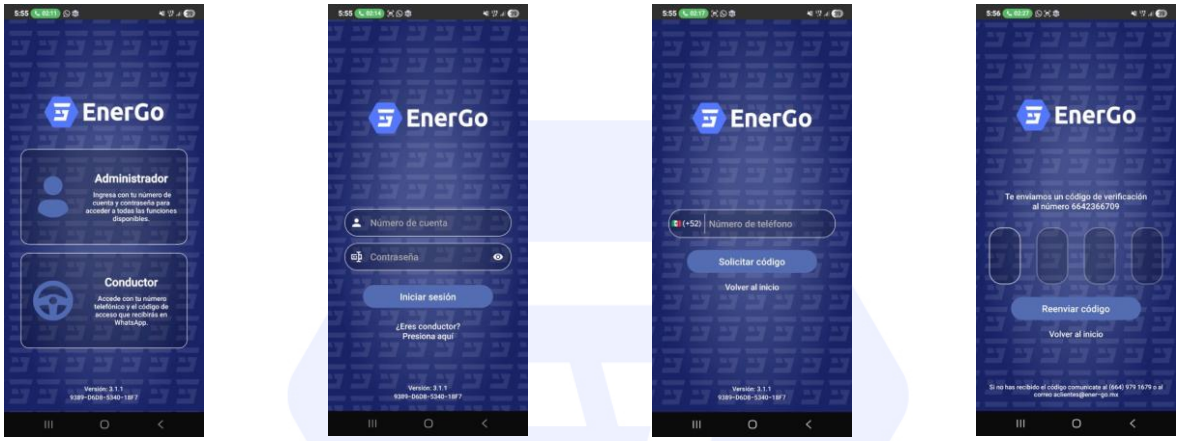
E50-INT-06. Configuración del certificado en SafeLine WAF.

6. Protección contra copia no autorizada

6.1. Control de acceso y autenticación fuerte

Requisito	Reducir la posibilidad de que personas no autorizadas accedan a información transferida.
Estado	**INTEGRADA**

La evidencia documenta un mecanismo de doble factor para el acceso de usuarios mediante credenciales y un código dinámico enviado al número previamente vinculado. Este control reduce el riesgo de acceso no autorizado.



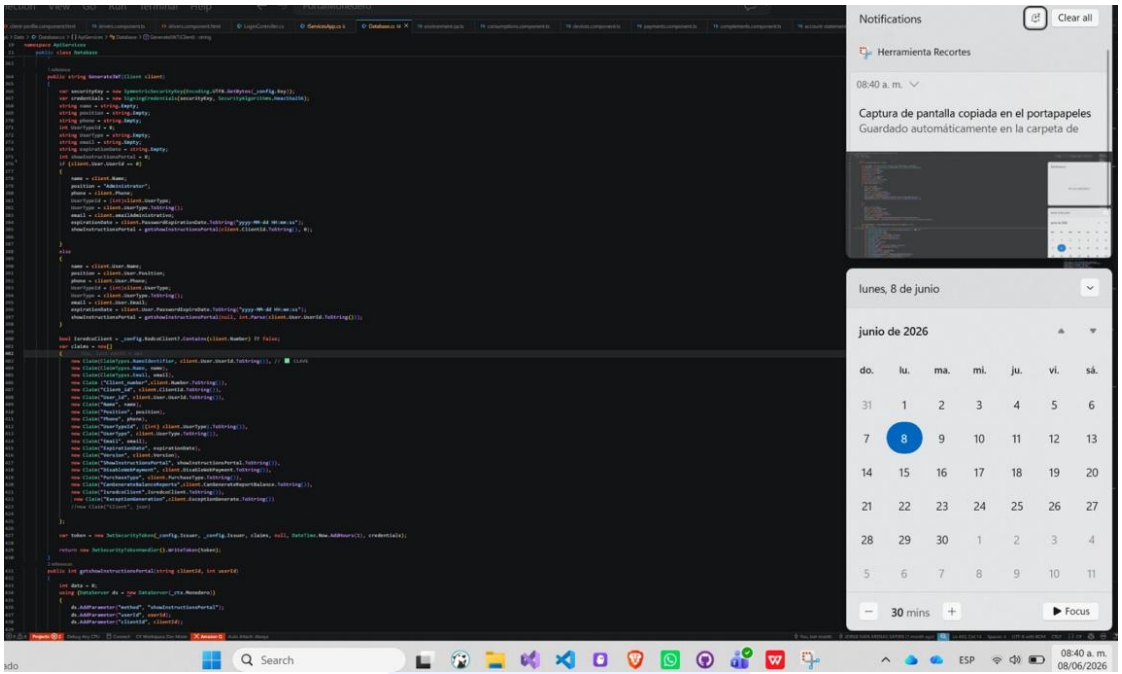
E50-COP-01. Secuencia de autenticación fuerte en aplicación móvil.

7. Protección contra modificación

7.1. Integridad de mensajes en aplicaciones y APIs

Requisito	Demostrar que el receptor puede detectar alteraciones de tokens/mensajes antes de procesarlos.
Estado	**INTEGRADA**

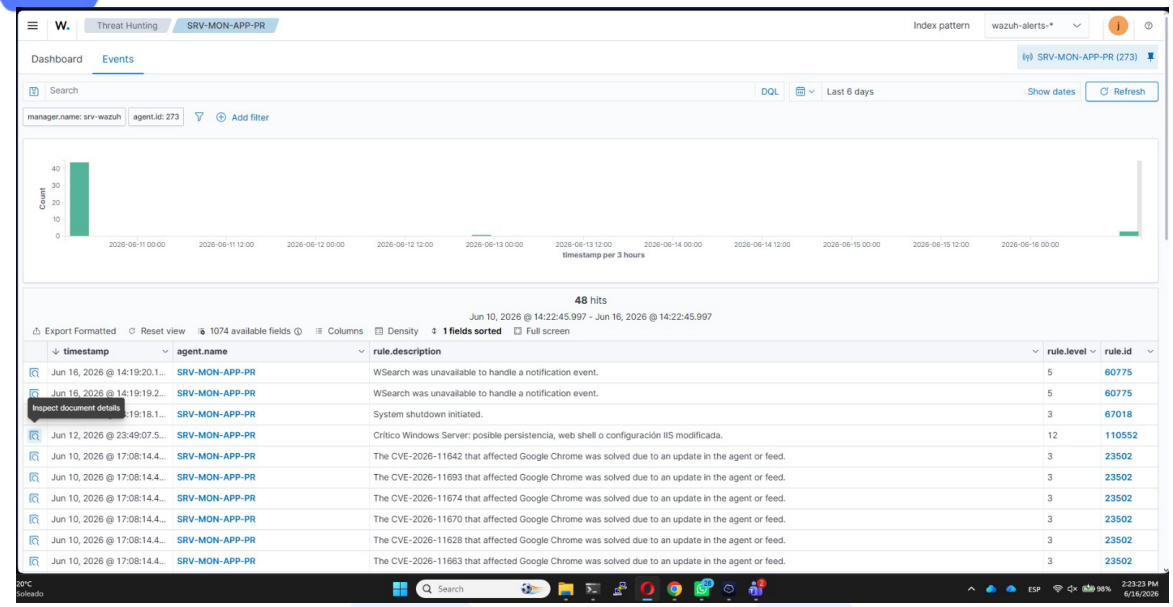
La evidencia muestra código relacionado con JWT firmado que permite verificar autenticidad e integridad.



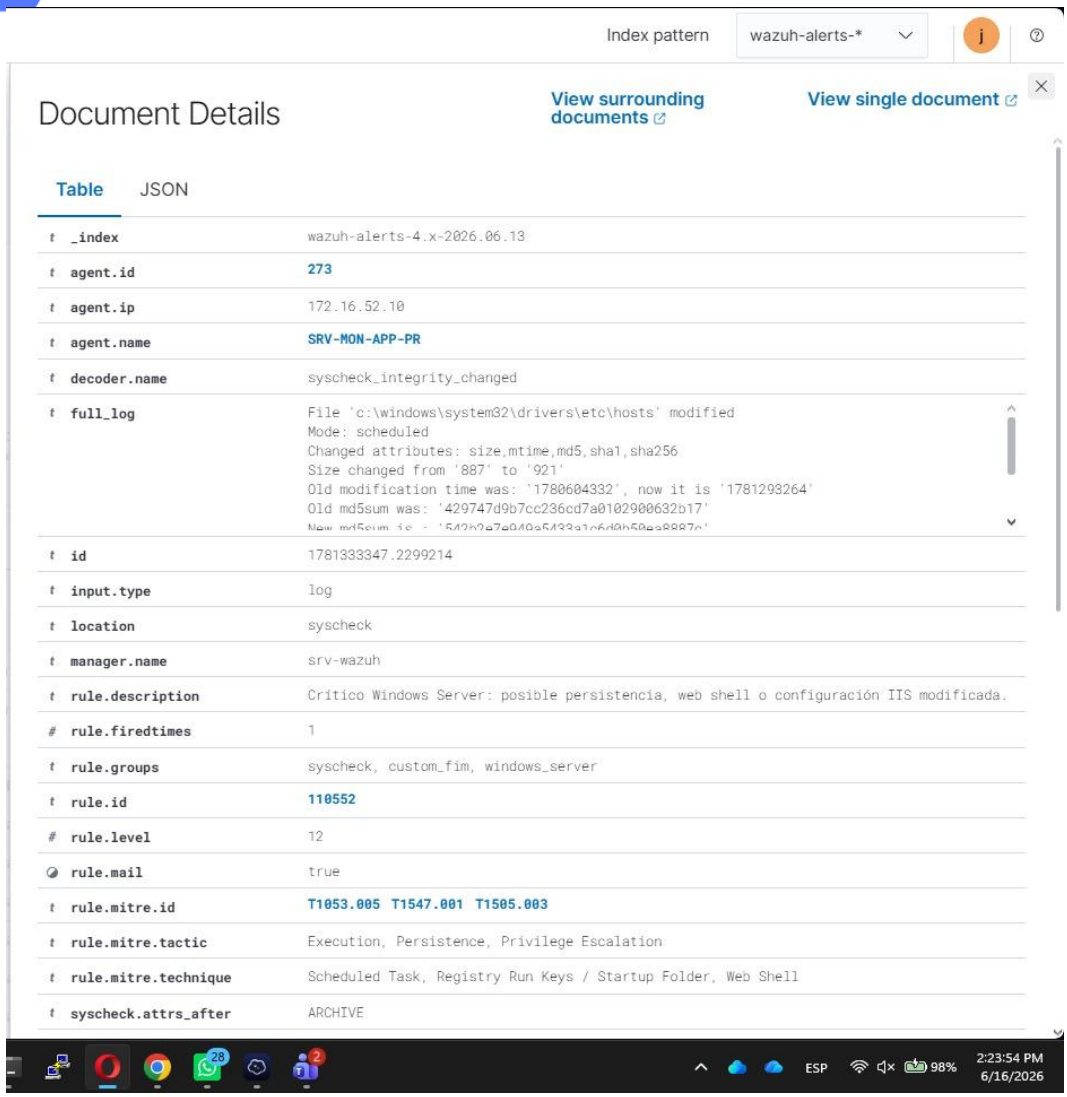
E50-MOD-01. Código de aplicación relacionado con generación/validación de JWT.

7.2. Integridad de archivos críticos mediante SIEM/FIM

Requisito	Detectar modificaciones no autorizadas sobre archivos críticos y conservar evidencia del evento.
Estado	**INTEGRADA**



E50-MOD-02. Vista de eventos de integridad en Wazuh.



E50-MOD-03. Detalle de evento de modificación de archivo crítico.

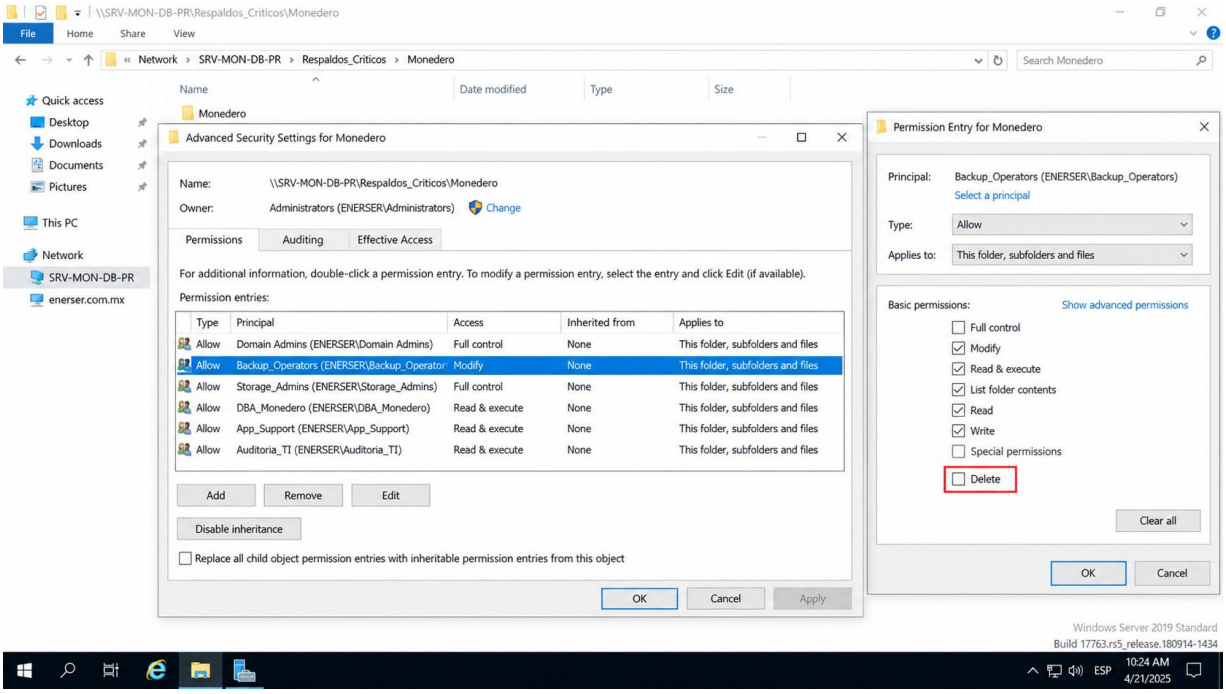
8. Protección contra borrado no autorizado

SENDERO FUEL debe demostrar controles preventivos, detectivos y de recuperación para evitar que información transferida, recibida o almacenada como resultado de una transferencia pueda ser eliminada accidentalmente o sin autorización.

8.1. Restricción de permisos de eliminación

Requisito	Demostrar que sólo roles autorizados pueden eliminar información en repositorios o sistemas críticos.
Estado	**INTEGRADA**

Descripción de la evidencia. La pantalla muestra la configuración avanzada de permisos sobre un repositorio crítico, permitiendo identificar los grupos autorizados y diferenciar privilegios de lectura, escritura, modificación y eliminación.

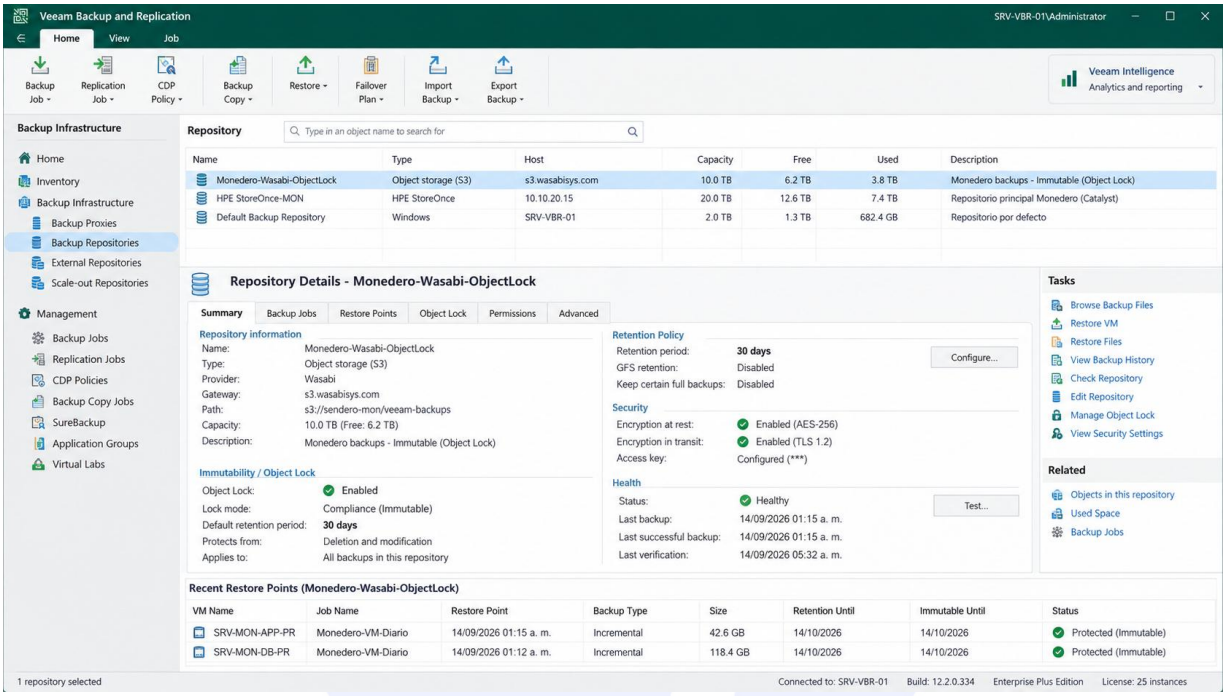


E50-BOR-01. Permisos de eliminación sobre repositorio crítico.

8.2. Retención e inmutabilidad

Requisito	Demostrar que los respaldos/puntos de recuperación no pueden eliminarse o alterarse durante el periodo de protección definido.
Estado	**INTEGRADA**

Descripción de la evidencia. La pantalla muestra un repositorio administrado desde Veeam con política de retención, protección contra modificación/eliminación e inmutabilidad mediante Object Lock.

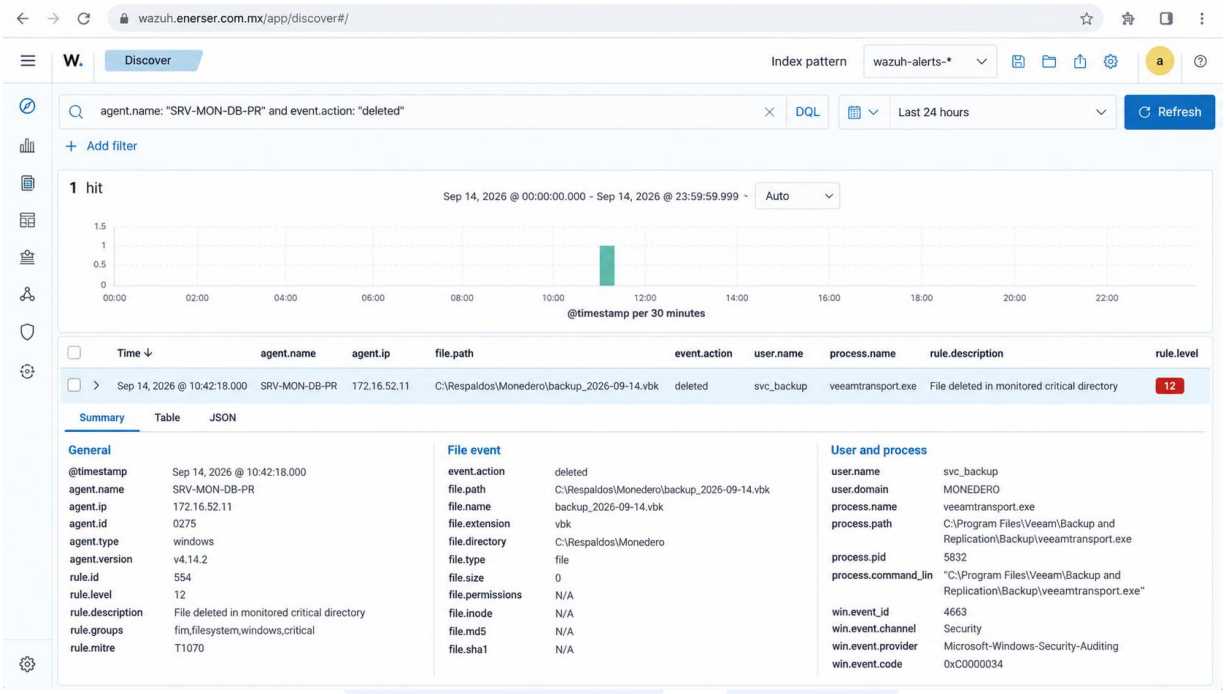


E50-BOR-02. Retención e inmutabilidad del repositorio de respaldos.

9.3. Detección de eliminación mediante Wazuh/FIM

Requisito	Demostrar que la eliminación de un archivo crítico genera un evento auditable.
Estado	**INTEGRADA**

Descripción de la evidencia. La pantalla muestra un evento de eliminación de archivo monitoreado por Wazuh/FIM. Deben conservarse visibles, como mínimo, el agente, dirección IP, ruta del archivo, acción deleted, usuario o proceso responsable, fecha/hora, descripción de la regla y severidad.

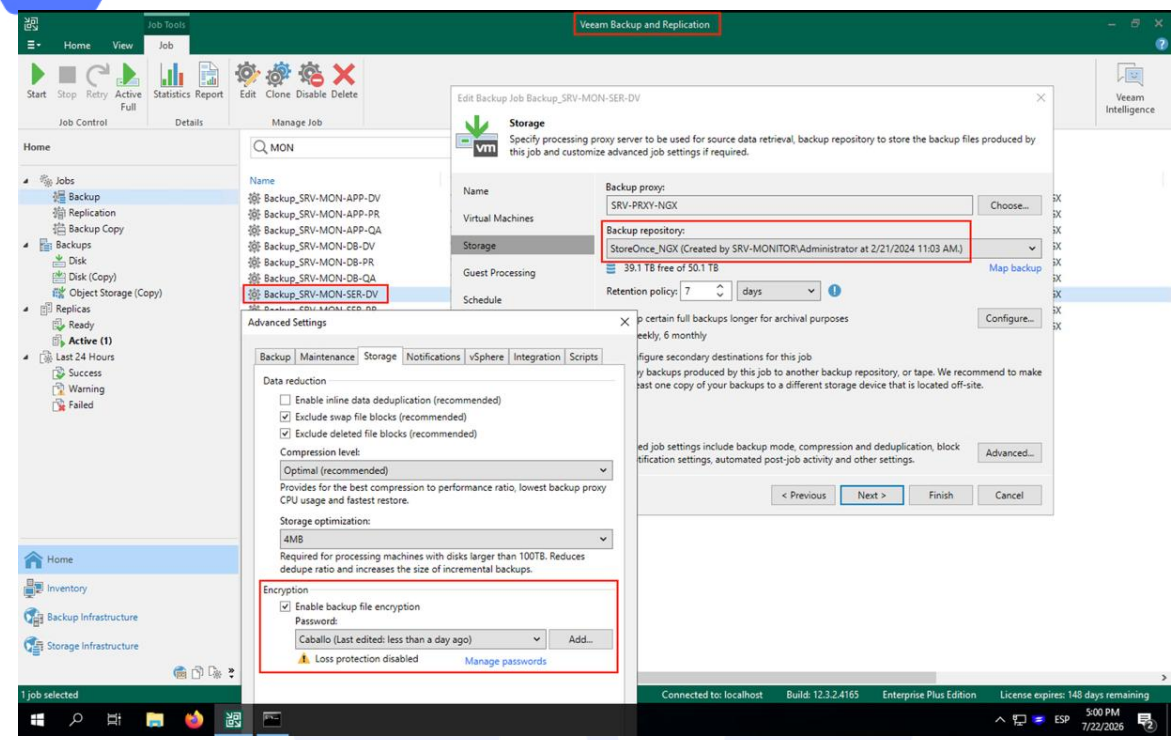


E50-BOR-03. Evento de eliminación detectado mediante Wazuh/FIM.

8.4. Recuperación posterior a borrado

Requisito	Demostrar que la información borrada puede recuperarse desde un punto válido.
Estado	**INTEGRADA**

La infraestructura documentada utiliza Veeam y repositorios de respaldo, lo que aporta capacidad de recuperación..



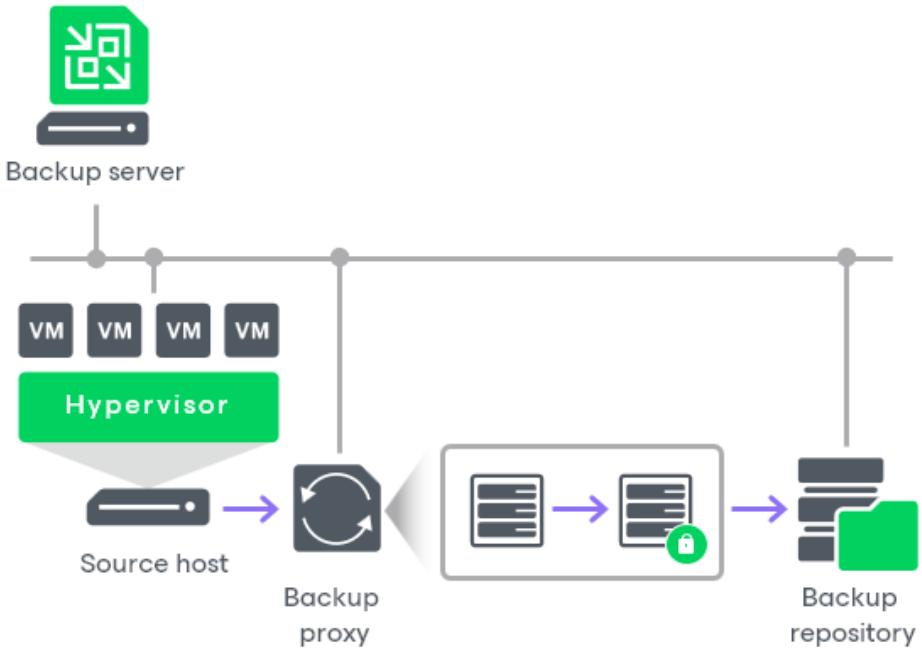
E50-BOR-04A. Configuración de tarea de respaldo cifrado en Veeam.

10. Protección contra pérdida

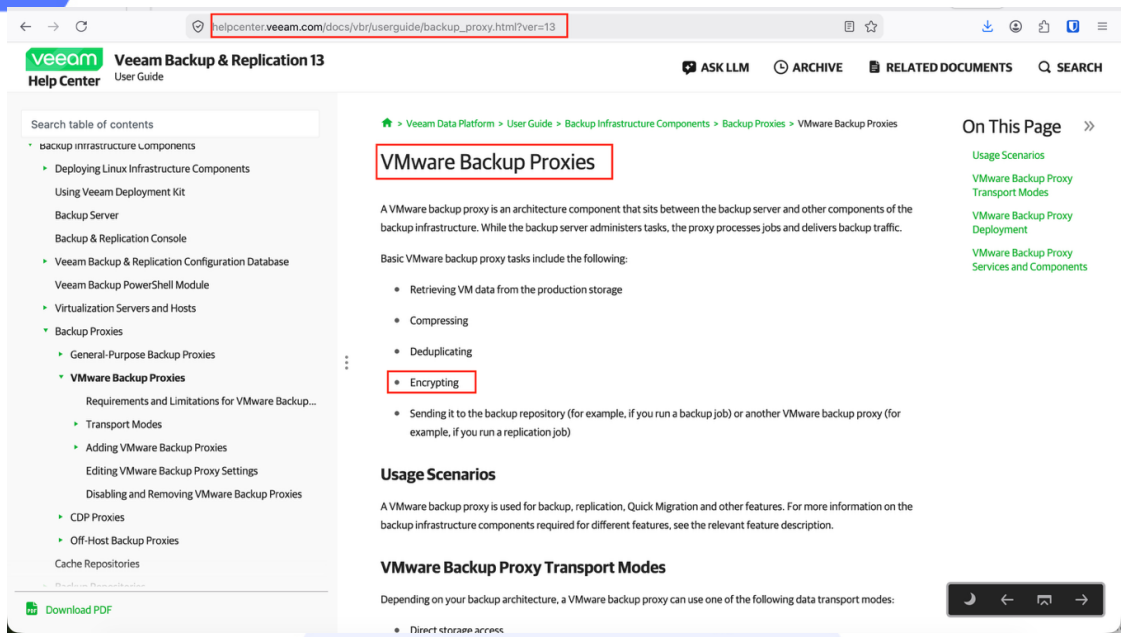
10.1. Arquitectura y canal de respaldos

Requisito	Demostrar que la transferencia de respaldos se realiza por mecanismos controlados y que existen copias recuperables.
Estado	**INTEGRADA**

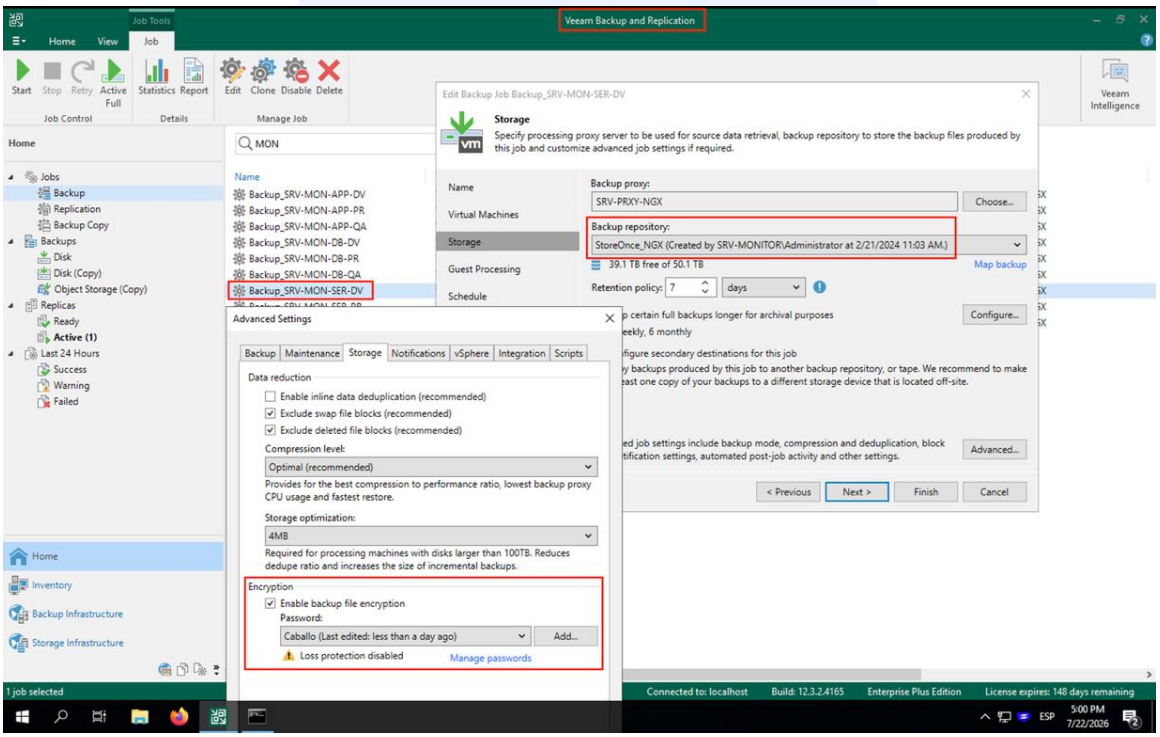
Se documenta como evidencia a Veeam Backup, uso de proxy de respaldo, almacenamiento en repositorio y una copia adicional en Wasabi como parte de una estrategia 3-2-1. La evidencia disponible soporta el objetivo de recuperación y disponibilidad.



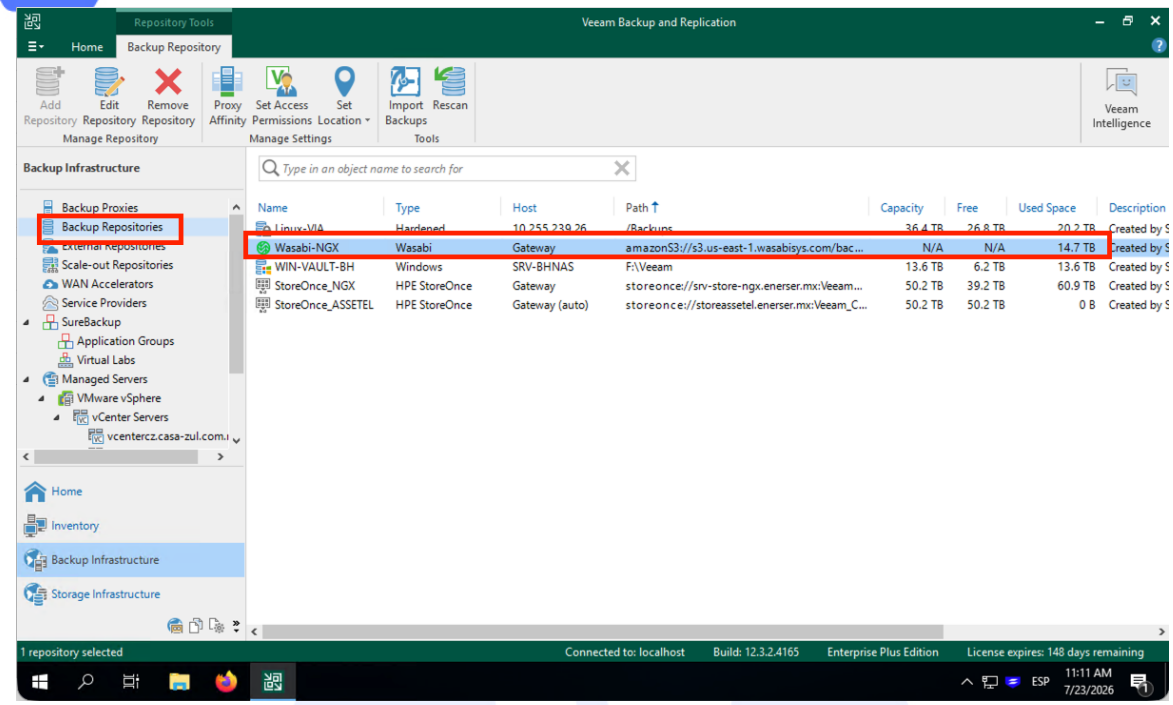
E50-PER-01. Arquitectura de transferencia mediante Veeam Backup Proxy.



E50-PER-02. Documentación del proxy y capacidades de cifrado.



E50-PER-03. Tarea de respaldo y almacenamiento cifrado en Veeam.



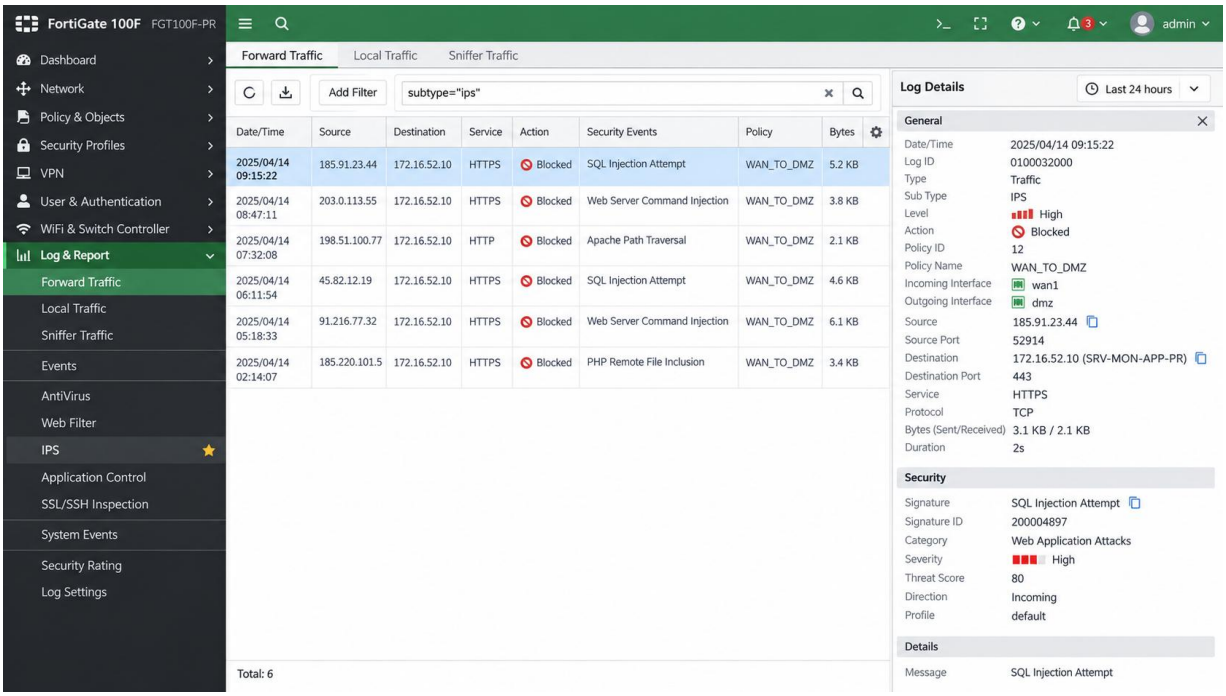
E50-PER-04. Repositorio de respaldo en nube/Wasabi configurado en Veeam.

10. Protección contra transmisión de código malicioso

10.1. IPS/IDS perimetral

Requisito	Detectar y bloquear patrones de ataque o tráfico malicioso antes de alcanzar los activos internos.
Estado	**INTEGRADA**

Descripción de la evidencia. La pantalla muestra un evento IPS/IDS bloqueado en FortiGate antes de alcanzar el activo interno. La evidencia real deberá identificar fecha/hora, IP de origen, activo e IP de destino, servicio, firma, política, severidad y acción de bloqueo.

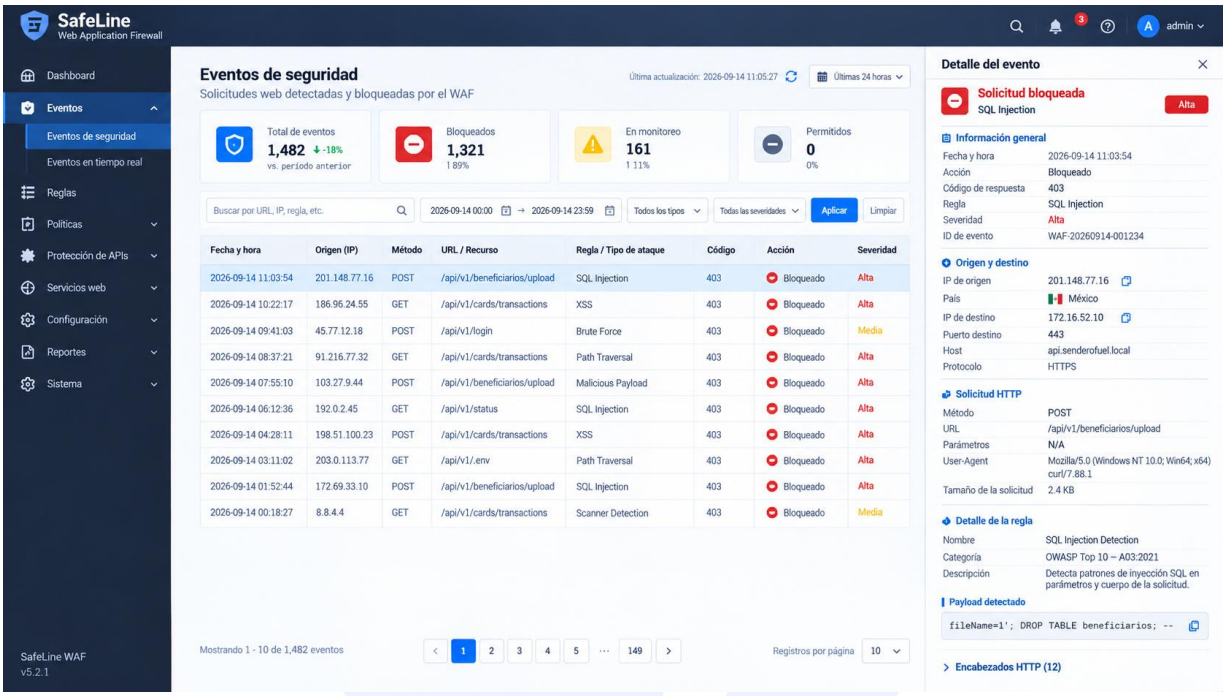


E50-MAL-01. Evento IPS/IDS bloqueado en FortiGate.

10.2. Protección WAF en APIs y servicios web

Requisito	Detectar y bloquear payloads maliciosos en HTTP/HTTPS.
Estado	**INTEGRADA**

Descripción de la evidencia. La pantalla muestra eventos de SafeLine WAF en los que solicitudes HTTP/HTTPS son rechazadas por reglas de seguridad. La evidencia real deberá identificar la URL o recurso, IP de origen, método, regla o tipo de ataque, fecha/hora, código de respuesta y acción ejecutada.

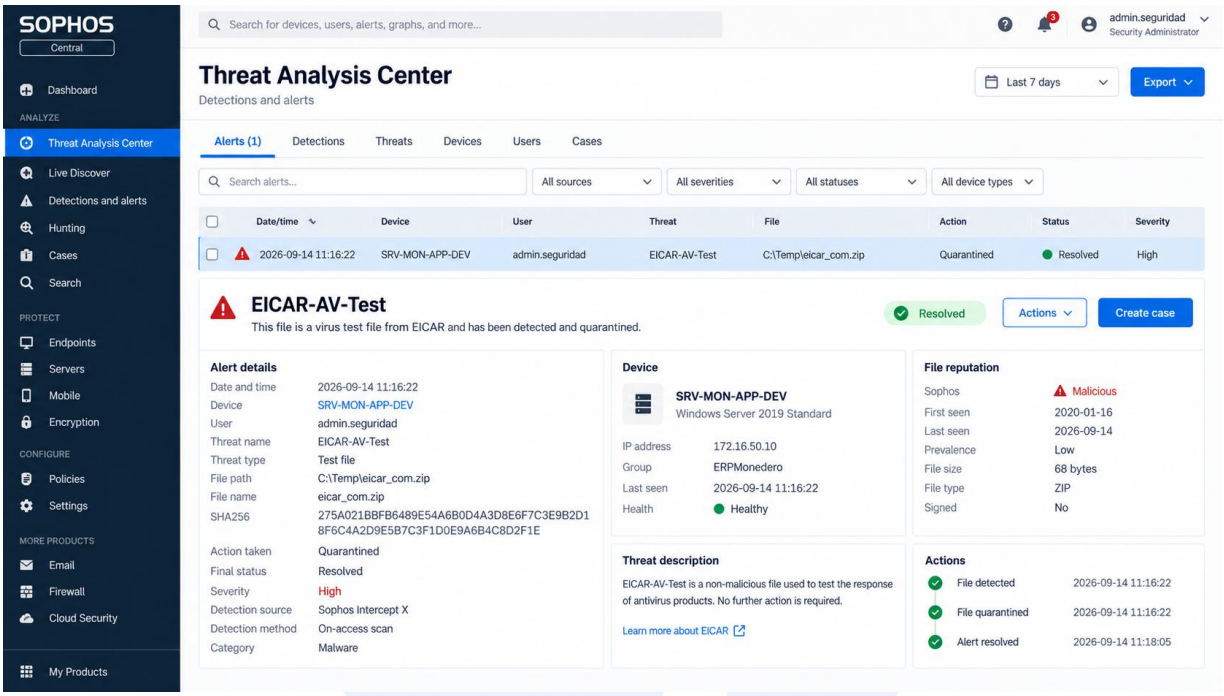


E50-MAL-02. Solicitud maliciosa bloqueada por SafeLine WAF.

10.3. Antimalware/XDR en endpoints y servidores

Requisito	Detectar, bloquear y poner en cuarentena código malicioso en el host.
Estado	**INTEGRADA**

Descripción de la evidencia. La pantalla muestra una detección antimalware en Sophos Central, incluyendo el activo, usuario, amenaza, archivo, hash, acción de cuarentena y estado final. La evidencia real deberá conservar estos campos y demostrar que el archivo fue bloqueado o contenido.

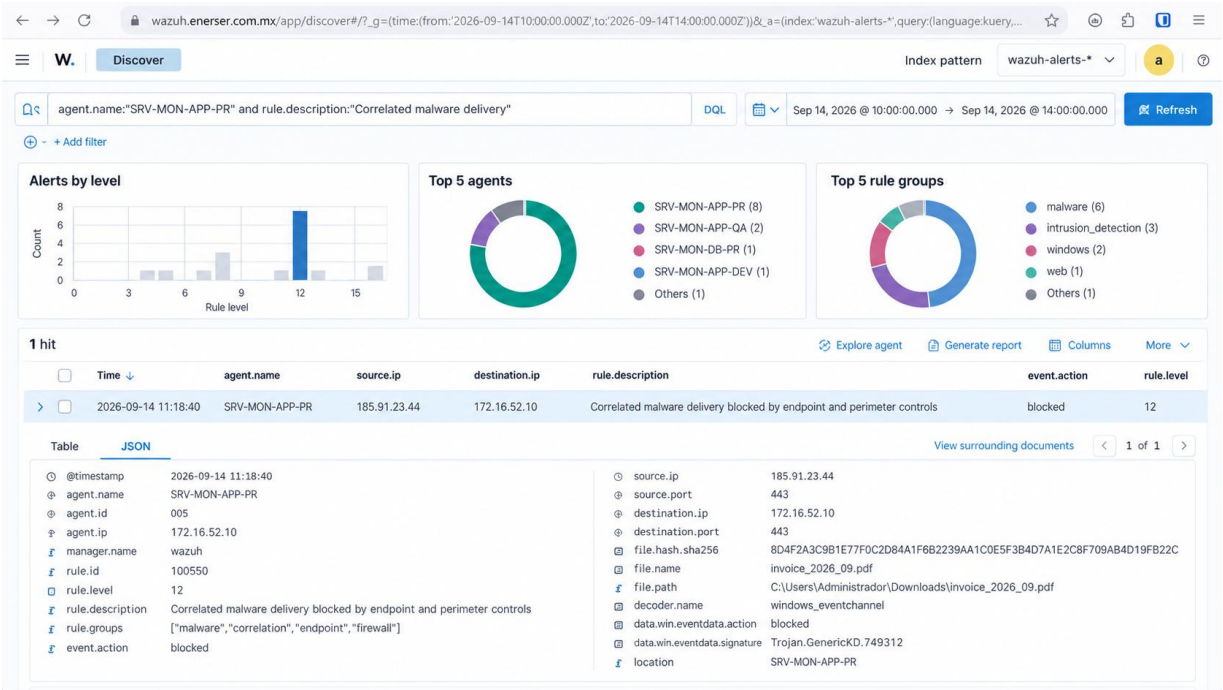


E50-MAL-03. Detección y cuarentena de archivo por Sophos XDR/Endpoint.

10.4. Correlación centralizada en Wazuh

Requisito	Conservar trazabilidad del evento y correlacionarlo con activo, usuario y acción de seguridad.
Estado	**INTEGRADA**

Descripción de la evidencia. La pantalla muestra la correlación del evento en Wazuh, permitiendo asociar el activo, origen, destino, descripción de la regla, acción, archivo/hash cuando aplique, nivel de severidad y marca de tiempo.



E50-MAL-04. Correlación centralizada de evento malicioso en Wazuh.

10.5. Validación de archivos/payloads antes del procesamiento

Requisito	Rechazar archivos o payloads no permitidos antes de incorporarlos al flujo operativo.
Estado	**INTEGRADA**

Descripción de la evidencia. La pantalla muestra la validación previa al procesamiento de un archivo cargado por API, incluyendo tipo MIME, extensión, tamaño, resultado antimalware, resultado de validación y motivo del rechazo..

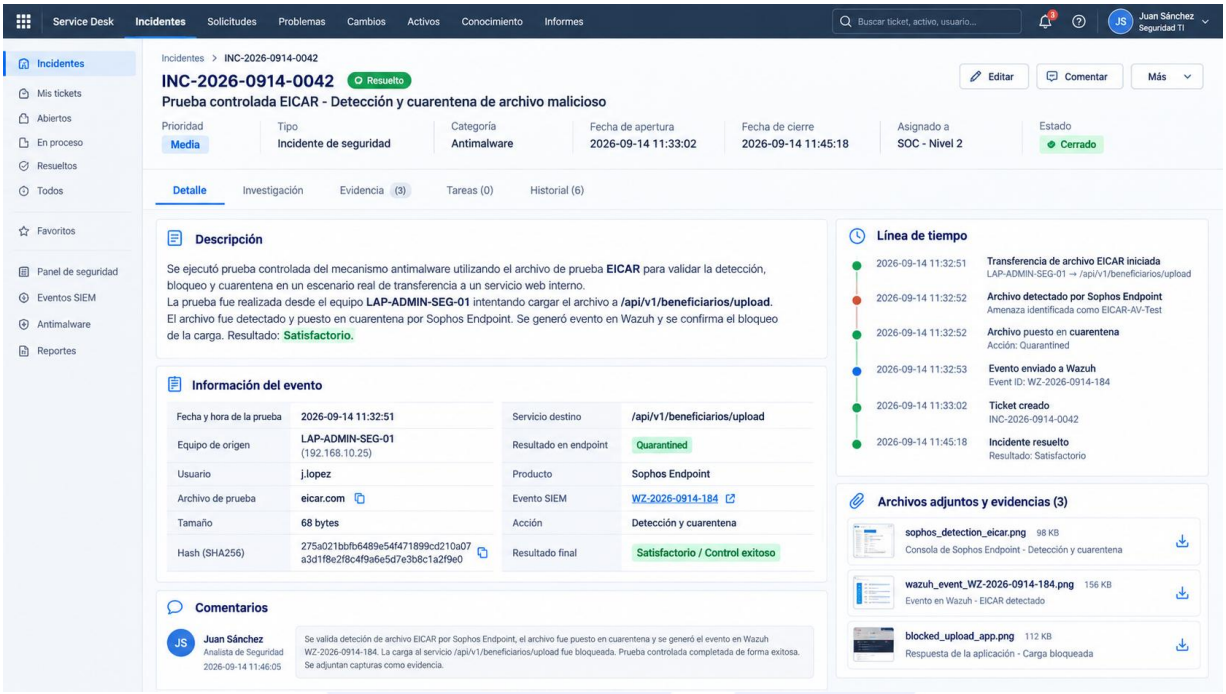


E50-MAL-05. Validación y rechazo de archivo antes del procesamiento.

10.6. Prueba controlada del control antimalware

Requisito	Demostrar que el mecanismo realmente detecta y bloquea una prueba segura.
Estado	**INTEGRADA**

Descripción de la evidencia. La pantalla documenta una prueba controlada con archivo EICAR, incluyendo intento de transferencia, detección, cuarentena, evento SIEM, ticket de incidente y resultado satisfactorio.



E50-MAL-06. Prueba controlada del mecanismo antimalware.