EVIDENCIA 52 FINAL

Expediente técnico de SENDERO FUEL para documentar los controles de seguridad aplicados a los servicios expuestos del monedero electrónico de combustibles, estructurado conforme al numeral 52 del Anexo 10 de la RMF 2026.

1. Interpretación del control

SENDERO FUEL interpreta el numeral 52 como la obligación de identificar de forma verificable los servicios expuestos y demostrar que éstos cuentan con controles que reduzcan el riesgo de fraude, filtración y pérdida de integridad o confidencialidad durante el procesamiento de transacciones.

2. Objetivo

Consolidar la evidencia técnica existente y complementarla con evidencia de operación que permita demostrar la eficacia de los controles aplicados a servicios expuestos, manteniendo trazabilidad entre activo, servicio, amenaza, control y resultado observado.

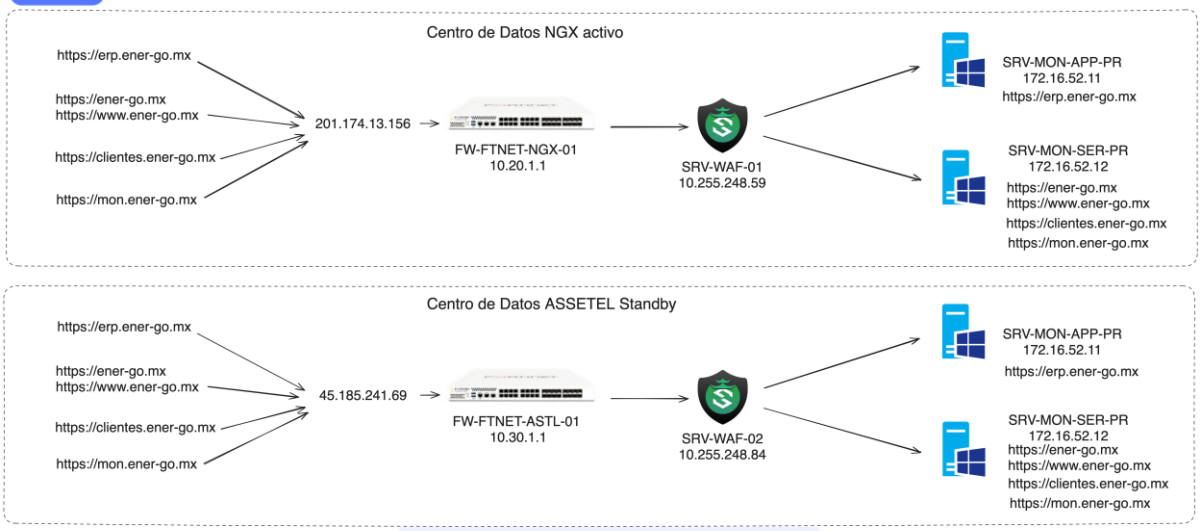
3. Alcance

- Servicios web y portales publicados para clientes y beneficiarios.
- APIs y servicios backend asociados al monedero.
- Firewalls perimetrales y WAF de NGX y ASSETEL.
- Accesos administrativos a infraestructura y consolas.
- Servicios de monitoreo, autenticación y administración asociados a los activos expuestos.
- Controles de aplicación destinados a evitar transacciones incompletas, mal enrutamiento, alteración de mensajes, revelación y copia no autorizada.

4. Identificación de servicios expuestos

El documento fuente identifica los siguientes servicios de producción expuestos a Internet. Antes de la emisión definitiva deberá validarse la uniformidad de dominios y nomenclaturas contra el inventario DNS y el inventario maestro de activos.

URL	Descripción	Acceso	Función	Ubic.	IP	Pto.	Tipo	Prop.
https://erp.ener-go.mx	ERP de monedero (Producción)	Confidencial	FrontEnd	NGX	201.174.13.156	443	Virtual	EnerGo
https://ener-go.mx	Página Web EnerGo (Producción)	Confidencial	FrontEnd	NGX	201.174.13.156	443	Virtual	EnerGo
https://clientes.ener-go.mx	Portal para gestión de la cuenta (Producción)	Confidencial	FrontEnd	NGX	201.174.13.156	443	Virtual	EnerGo
https://mon.ener-go.mx	Servicios web para portal y aplicaciones móviles	Confidencial	BackEnd	NGX	201.174.13.156	443	Virtual	EnerGo
N/A	Firewall FortiGate 200F	Confidencial	Seguridad	NGX	201.174.13.156	443	Físico	Enerser
N/A	Firewall FortiGate 300E	Confidencial	Seguridad	ASSETEL	45.185.241.69	443	Físico	Enerser
N/A	SafeLine WAF	Confidencial	Seguridad	NGX	201.174.13.156	443	Virtual	Enerser
N/A	SafeLine WAF	Confidencial	Seguridad	ASSETEL	45.185.241.69	443	Virtual	Enerser



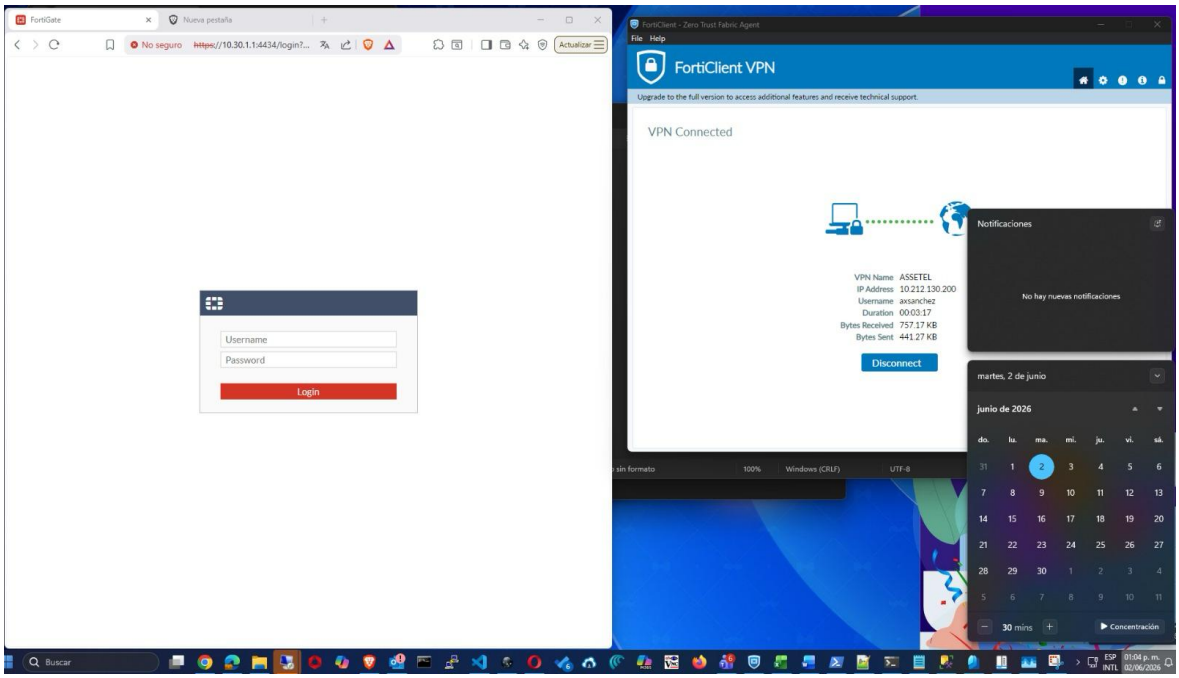
E52-EXP-01. Arquitectura de servicios expuestos en NGX y ASSETEL.

5. Inciso a) Controles de seguridad contra fraudes y filtración de información

5.1. Servicios administrativos no expuestos y acceso por VPN

Requisito	Demostrar que las consolas administrativas no se encuentran directamente expuestas a Internet y que el acceso se realiza por un canal controlado.
Estado	**INTEGRADA**

Las consolas de administración de vCenter, GLPI, switches y firewalls se mantienen en redes privadas. El acceso administrativo se realiza mediante VPN SSL de Fortinet, evitando la publicación directa de consolas de gestión.



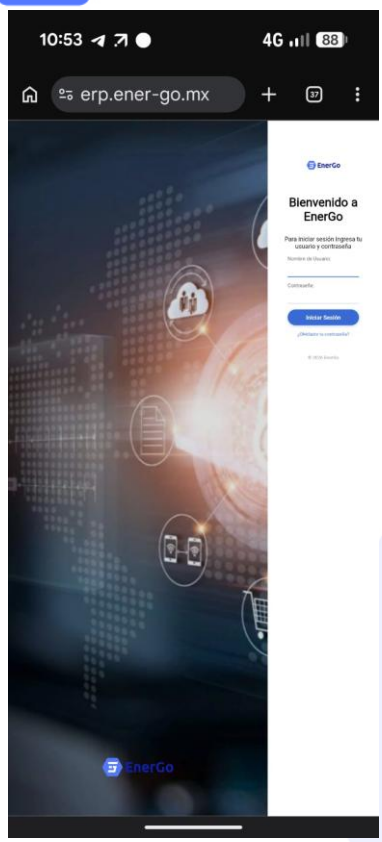
E52-A-01. Acceso administrativo a infraestructura mediante VPN SSL.

5.2. Ambientes no expuestos

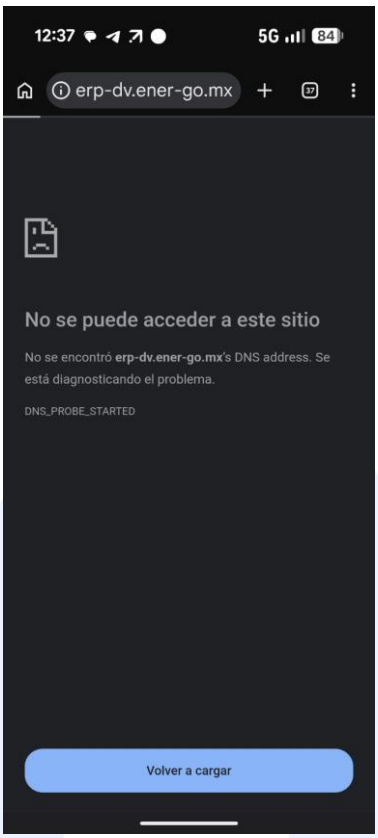
Requisito	Demostrar que los ambientes de desarrollo y QA no se encuentran publicados a Internet.
Estado	**INTEGRADA**

La evidencia fuente muestra que el ambiente productivo responde desde Internet mientras que los ambientes de desarrollo y QA no son accesibles públicamente.

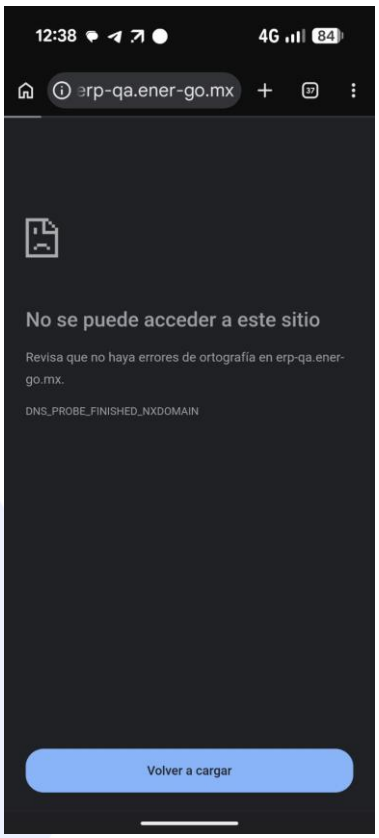
EnerGo



Producción accesible



Desarrollo no expuesto

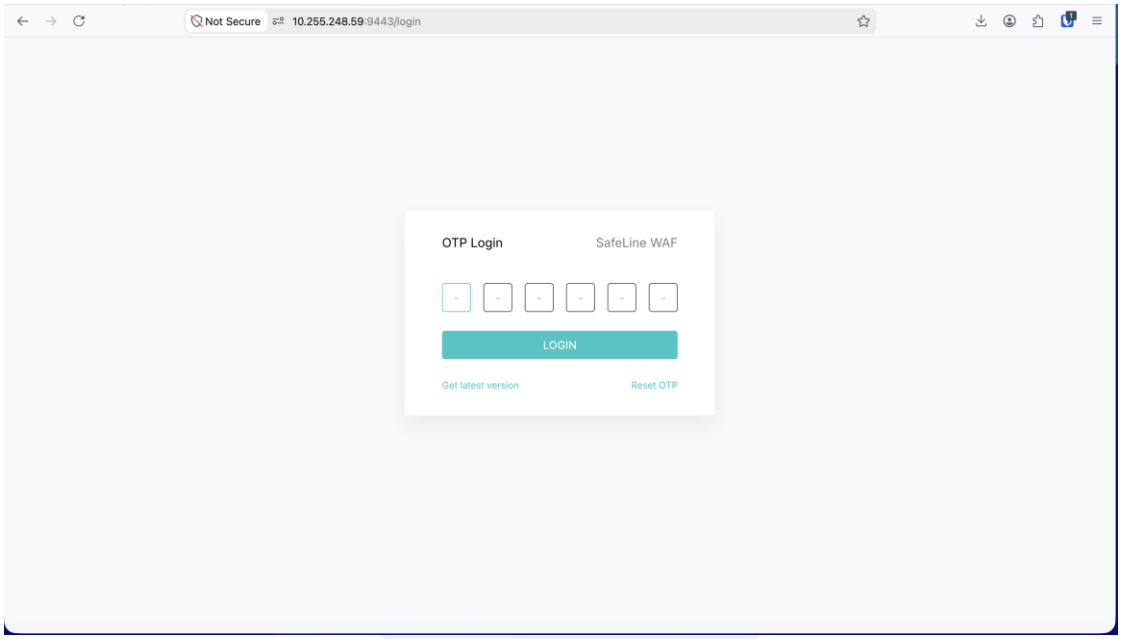


QA no expuesto

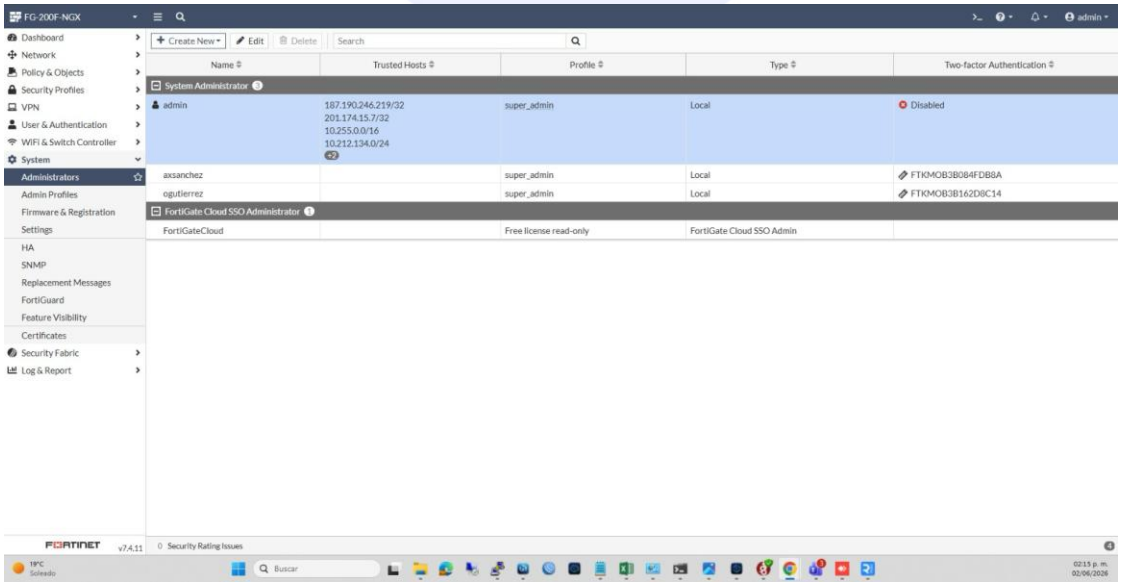
5.3. Autenticación robusta y accesos privilegiados

Requisito	Reducir el riesgo de fraude por suplantación de usuarios y administradores mediante autenticación reforzada y accesos controlados.
Estado	**INTEGRADA**

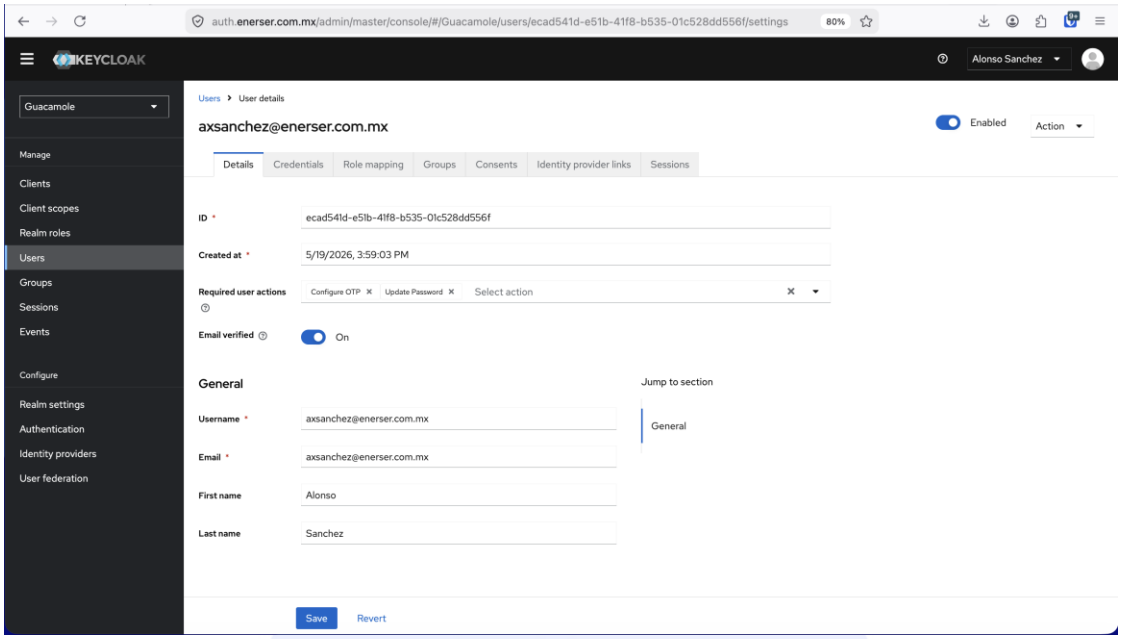
Se documentan controles MFA/OTP para SafeLine, FortiGate, Keycloak/Guacamole y los canales de usuario del monedero. Apache Guacamole concentra el acceso RDP sin exponer puertos administrativos directamente a Internet.



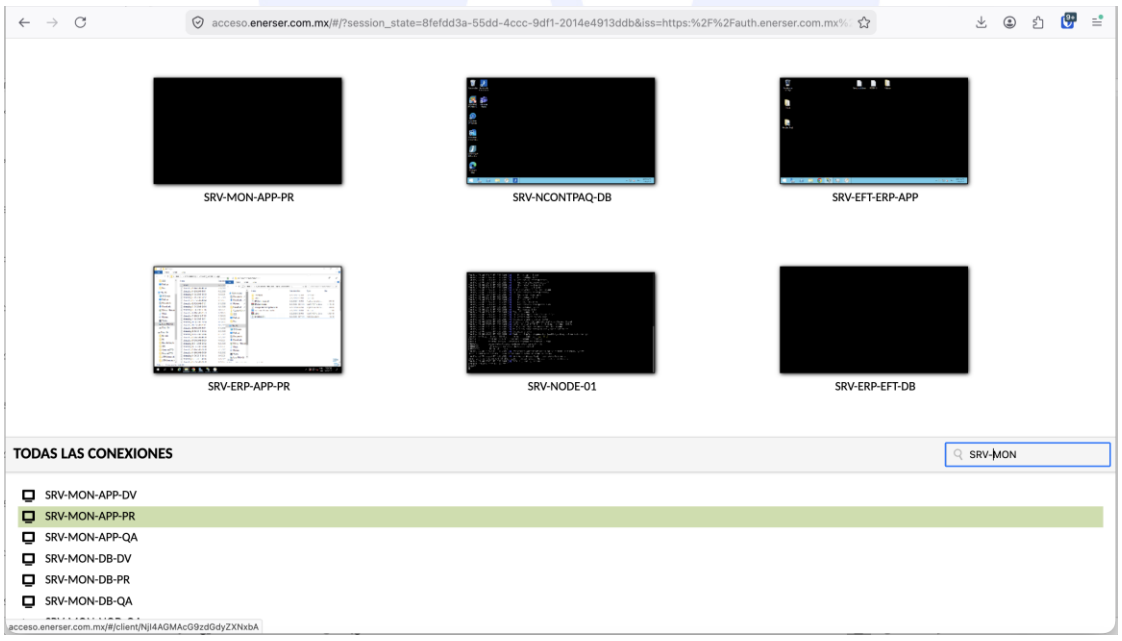
E52-A-03. SafeLine WAF solicita OTP después de las credenciales.



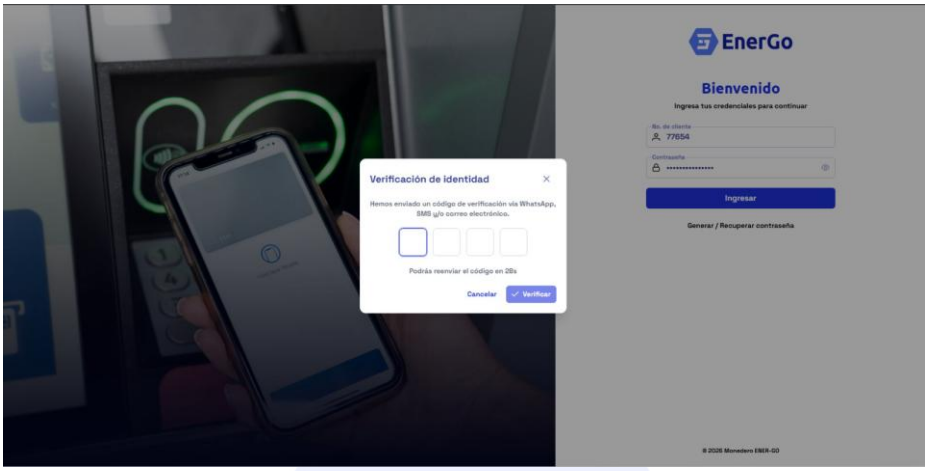
E52-A-03. FortiGate aplica autenticación reforzada y restricción de origen.



E52-A-03. Keycloak gestiona identidad para el acceso administrativo.



E52-A-03. Apache Guacamole concentra conexiones a servidores del monedero.



E52-A-03. Portal de clientes - autenticación inicial.



E52-A-03. Portal de clientes - segundo factor.

5.4. MFA en aplicación móvil



Ingreso de usuario



Solicitud de código

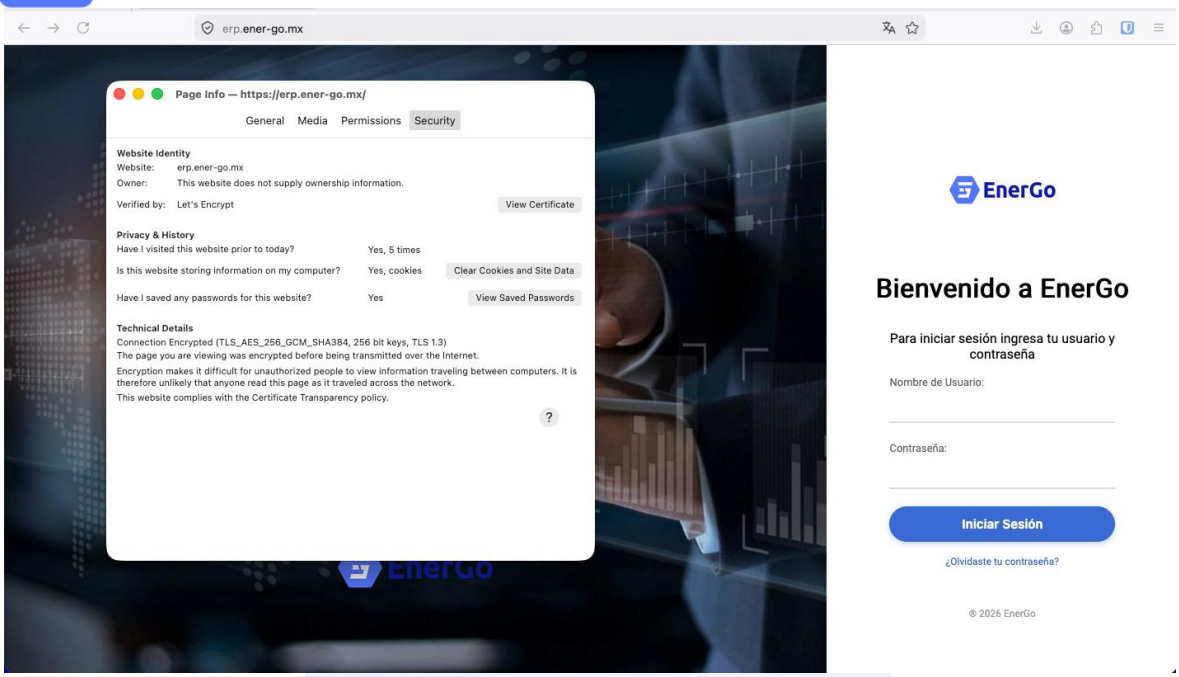


Validación de segundo factor

5.5. Cifrado en tránsito y TLS vigente

Requisito	Demostrar que los servicios expuestos utilizan cifrado en tránsito y certificados válidos.
Estado	**INTEGRADA**

Los canales web documentados utilizan HTTPS/TLS. La evidencia fuente muestra un certificado válido emitido por Let’s Encrypt para el servicio publicado.

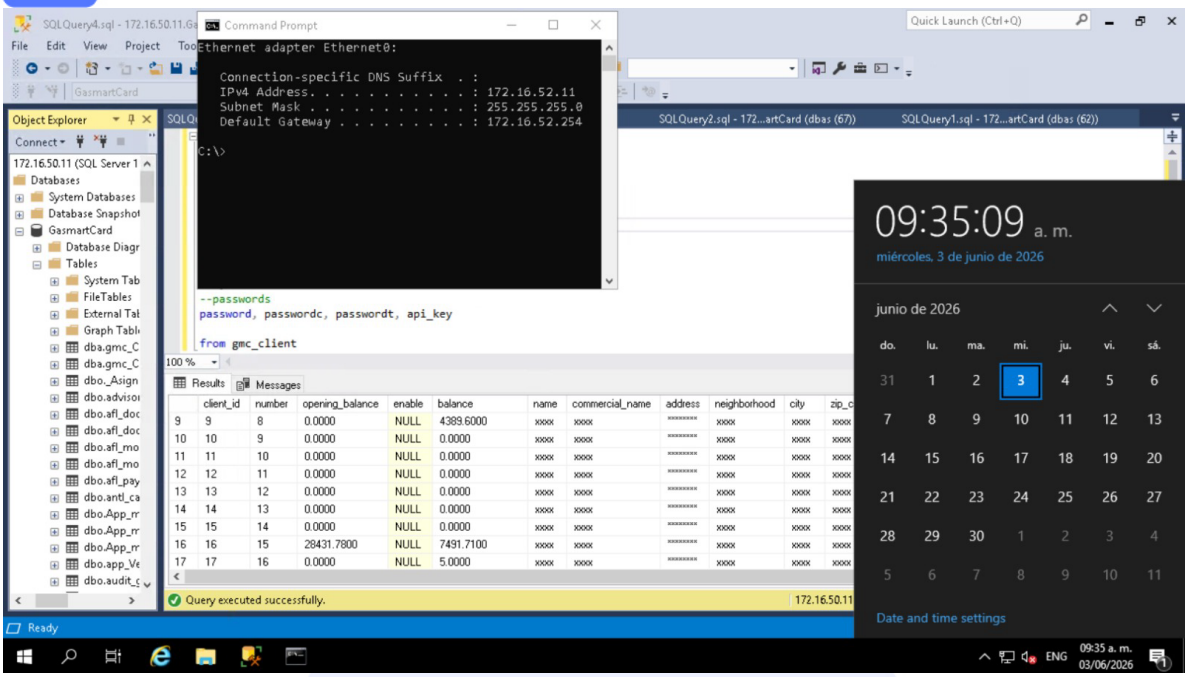


E52-A-05. Evidencia de certificado TLS en servicio web expuesto.

5.6. Protección de datos sensibles

Requisito	Reducir el impacto de una exposición no autorizada mediante controles sobre datos sensibles.
Estado	**INTEGRADA**

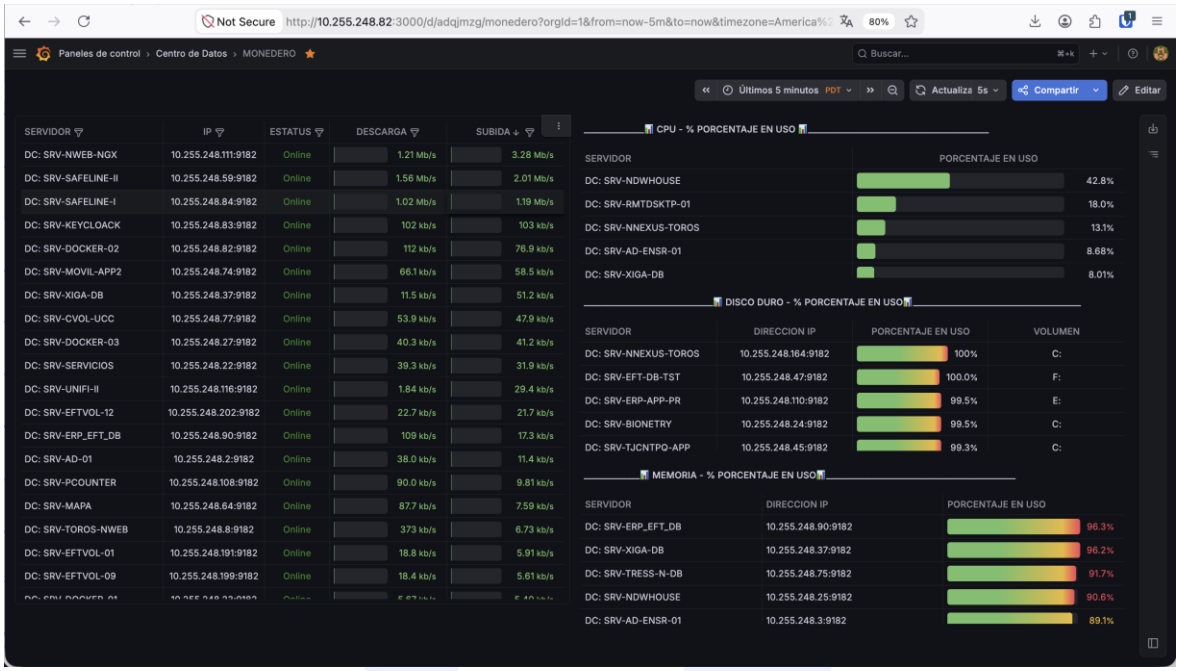
La base de datos del monedero documenta enmascaramiento de datos sensibles en consultas operativas, disminuyendo la exposición de valores completos a usuarios sin necesidad de conocerlos.



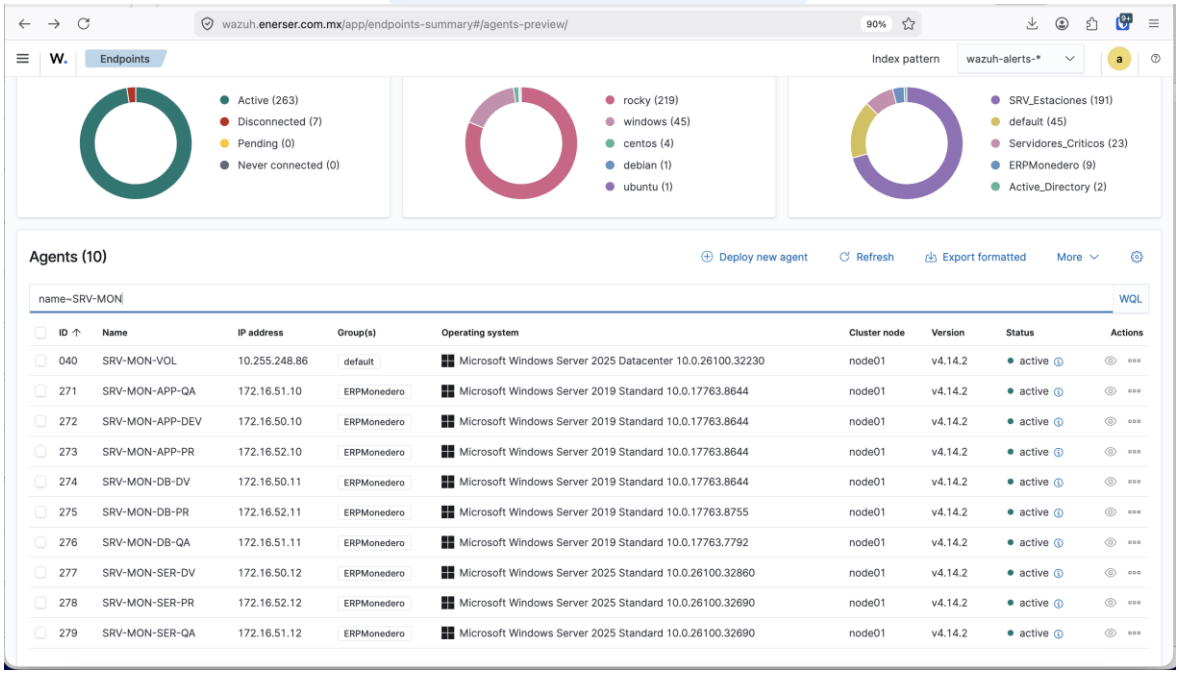
E52-A-06. Consulta a base de datos con datos sensibles enmascarados.

5.7. Registro y monitoreo de eventos

Requisito	Mantener visibilidad y trazabilidad sobre servidores y eventos de seguridad relacionados con servicios expuestos.
Estado	**INTEGRADA**



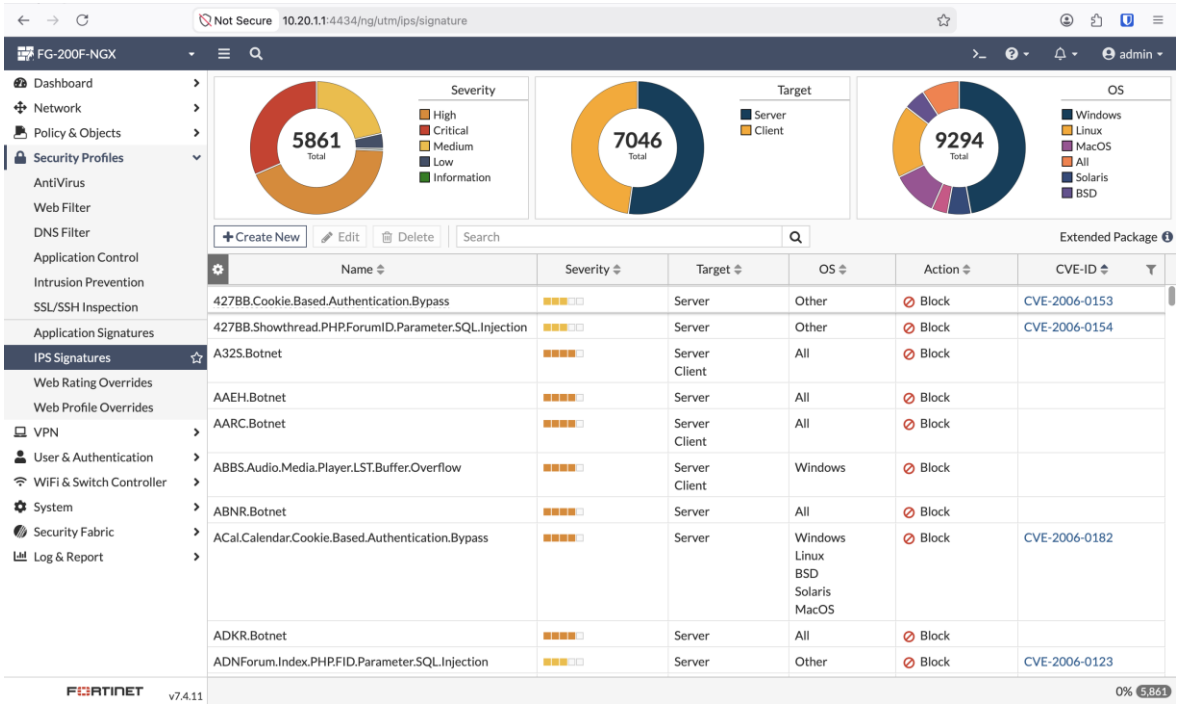
E52-A-07. Monitoreo de recursos en Grafana.



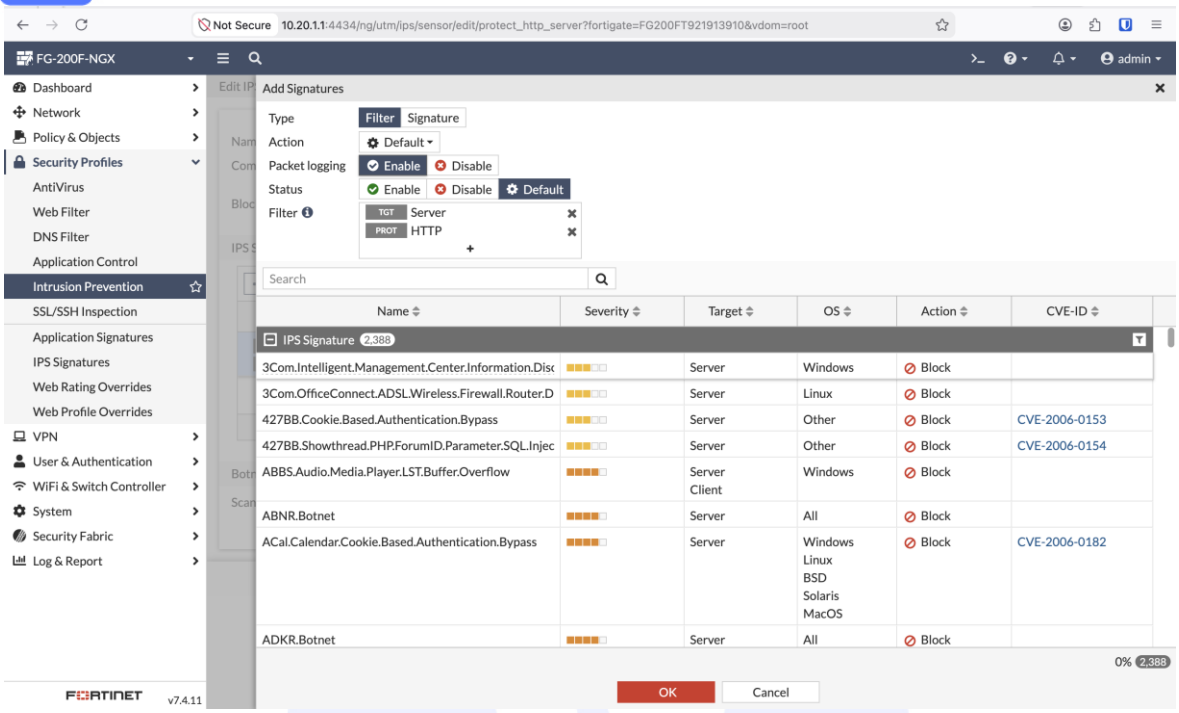
5.8. Firewall, IPS/IDS y WAF

Requisito	Demostrar protección perimetral y de aplicación frente a ataques, escaneos, malware y abuso de APIs.
Estado	**INTEGRADA**

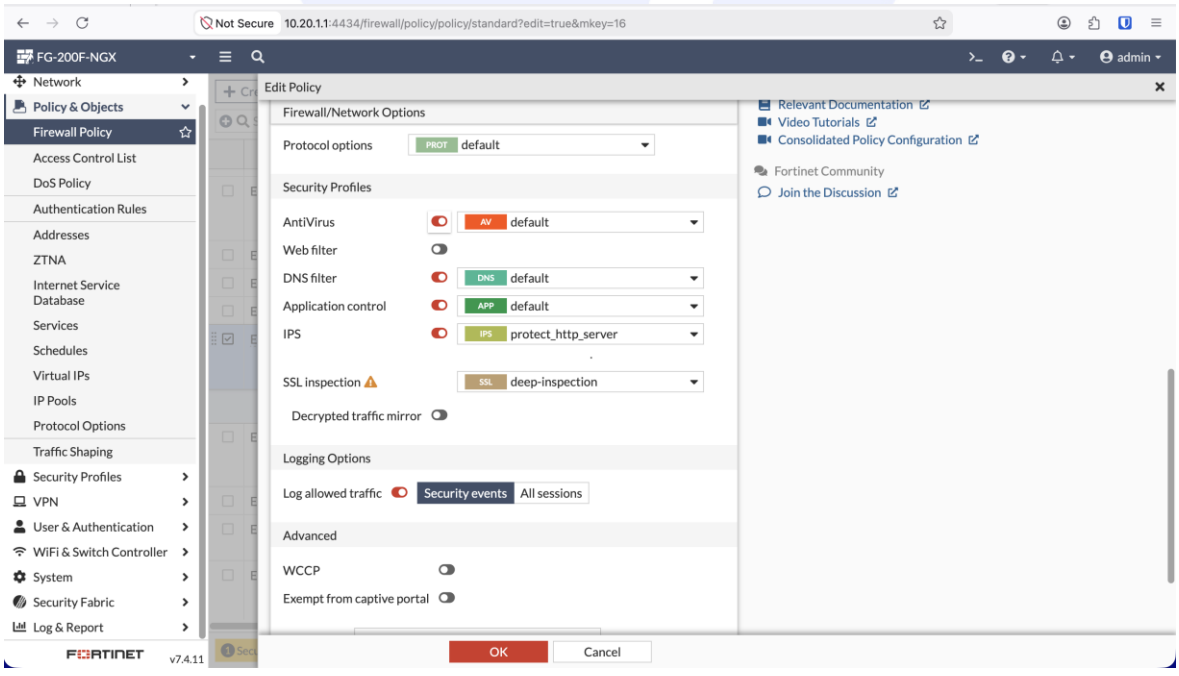
La arquitectura implementa defensa en profundidad: firewall de red FortiGate con IPS/IDS y una segunda capa WAF SafeLine que opera como proxy reverso y analiza tráfico HTTP/HTTPS antes de reenviarlo a los servidores.



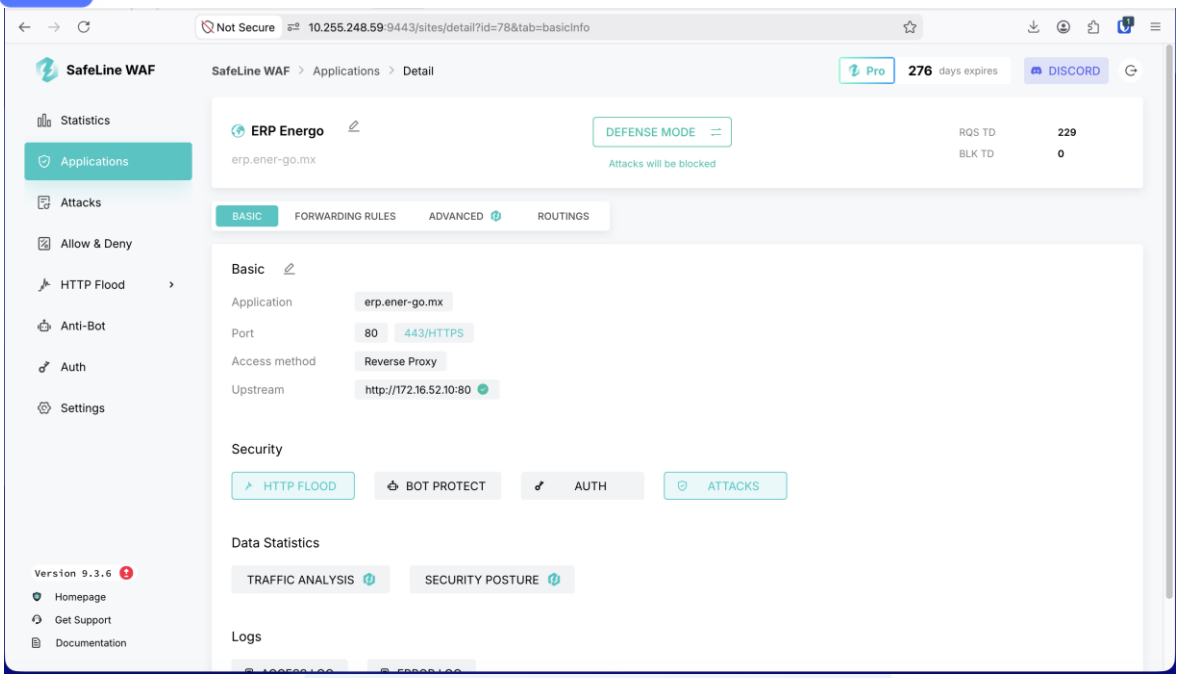
E52-A-09. Base de firmas IPS en FortiGate.



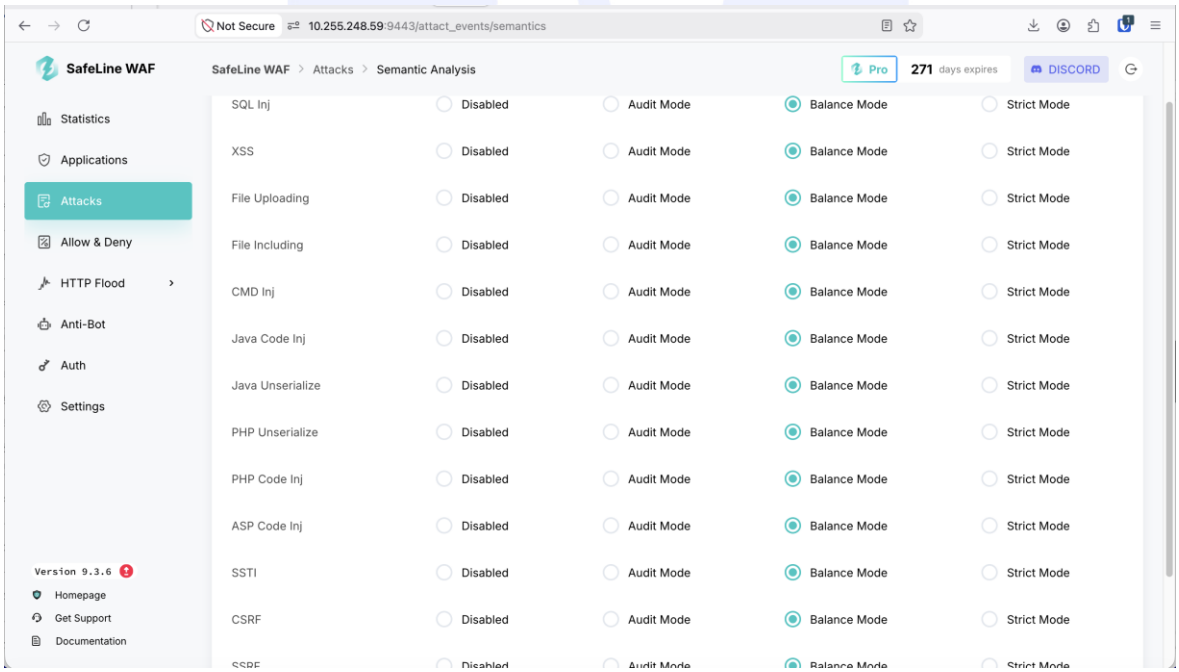
E52-A-09. Perfil IPS para servidores HTTP/HTTPS.



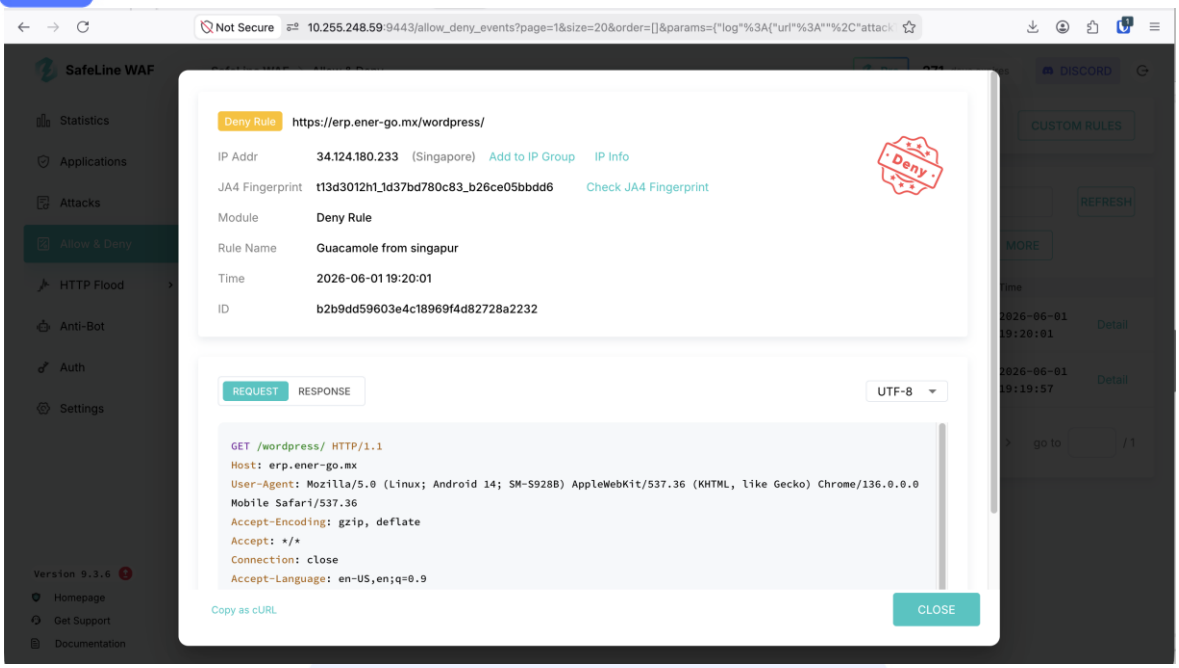
E52-A-09. Uso del perfil IPS en regla de entrada.



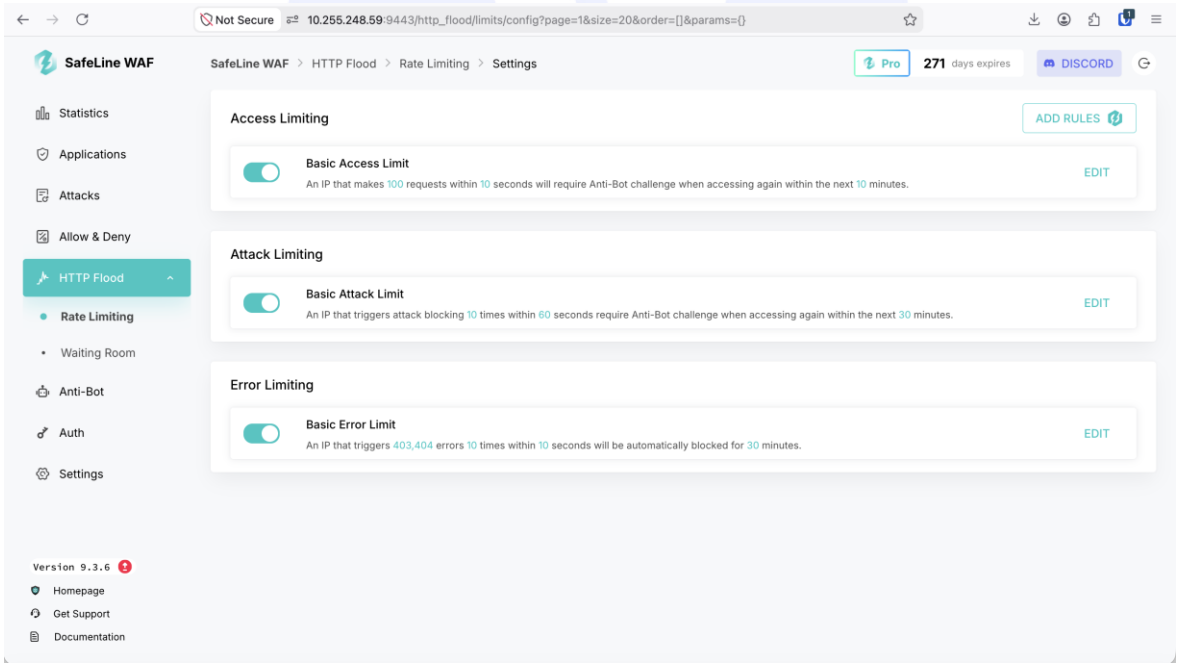
E52-A-09. Publicación de aplicación detrás de SafeLine WAF.



E52-A-09. Configuración de controles del WAF.



E52-A-09. Evento bloqueado por patrón anómalo.



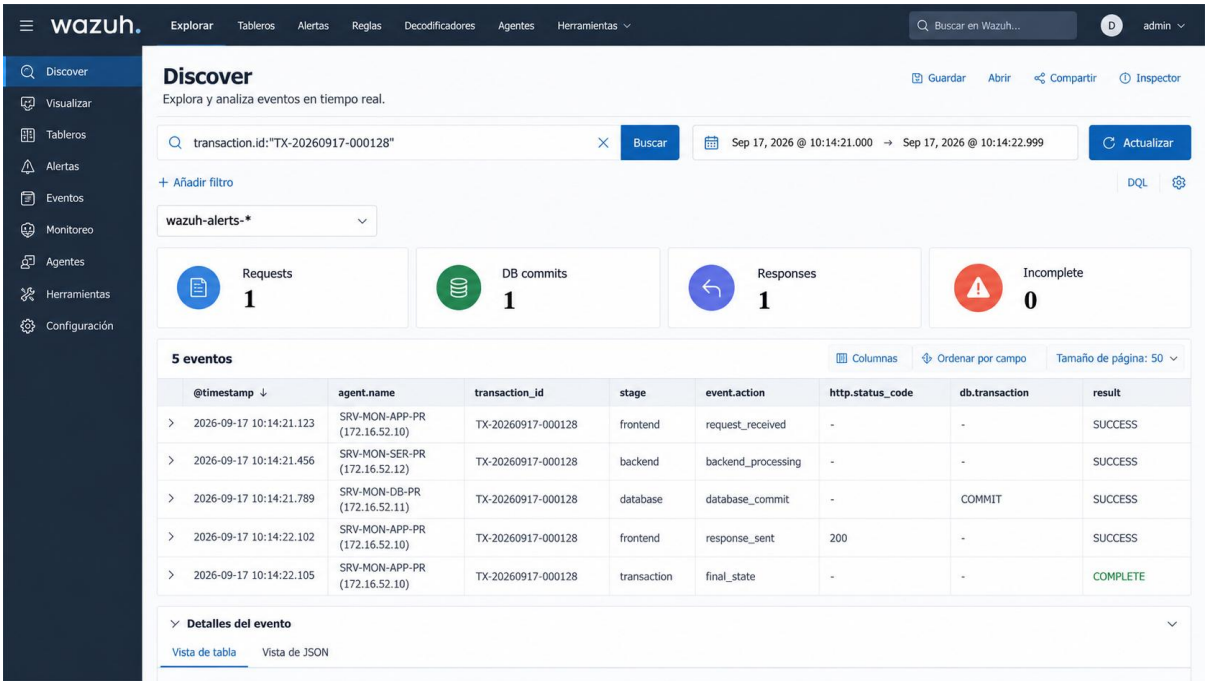
E52-A-09. Configuración de límites/rate limiting.

6. Inciso b) Controles para evitar transmisión incompleta, mal enrutamiento, alteración de mensajes, revelación de información y copia no autorizada

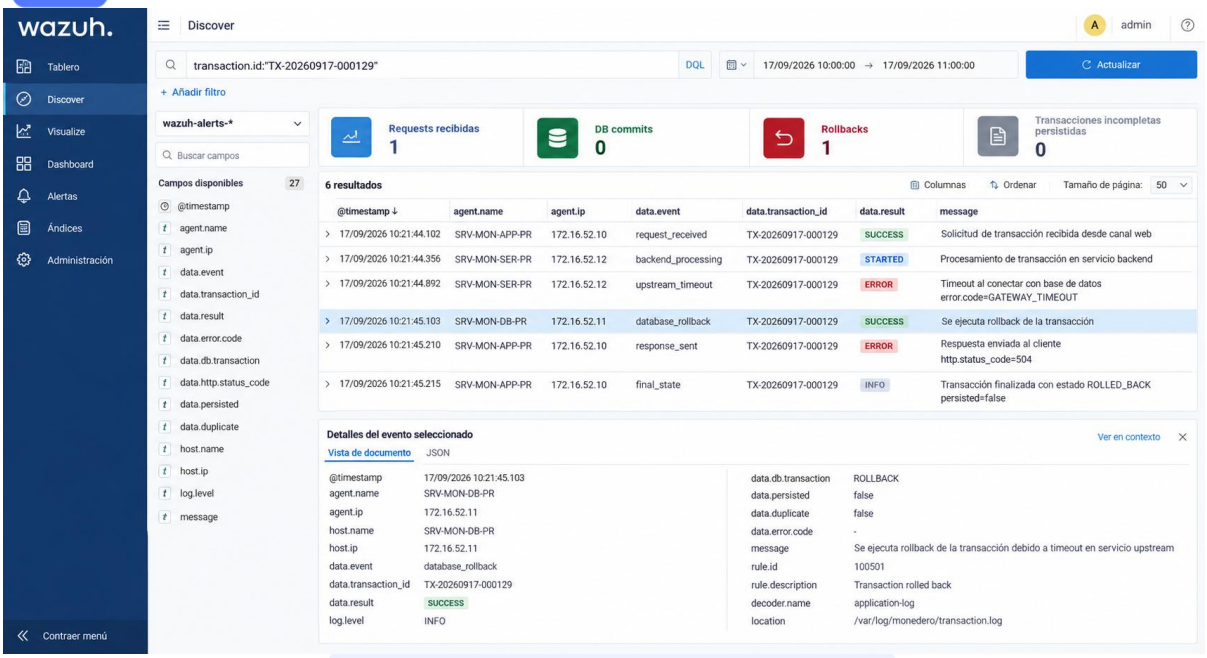
6.1. Transmisión incompleta de transacciones

Requisito	Demostrar que una transacción queda trazada de extremo a extremo y que una falla antes del commit no deja una operación parcial persistida.
Estado	**INTEGRADA**

El control debe permitir correlacionar la misma transacción en frontend, backend y base de datos mediante un identificador único. La evidencia muestra dos escenarios: una operación completada y una operación interrumpida que ejecuta rollback y no persiste datos parciales.



E52-B-01. Transacción completa: request recibido, procesamiento backend, COMMIT en base de datos y respuesta HTTP 200 con estado final COMPLETE.



E52-B-02. Transacción interrumpida: timeout de backend, ROLLBACK en SRV-MON-DB-PR, respuesta de error y persisted=false.

6.2. Mal enrutamiento

Requisito	Demostrar que cada host/URL se enruta únicamente hacia el backend autorizado y que los hosts no registrados son rechazados sin seleccionar upstream.
Estado	**INTEGRADA**

SafeLine opera como reverse proxy. La evidencia de configuración debe relacionar explícitamente dominio, backend autorizado, IP, puerto y protocolo. Una prueba negativa debe demostrar que un Host no registrado recibe rechazo y no se reenvía hacia un servidor interno.

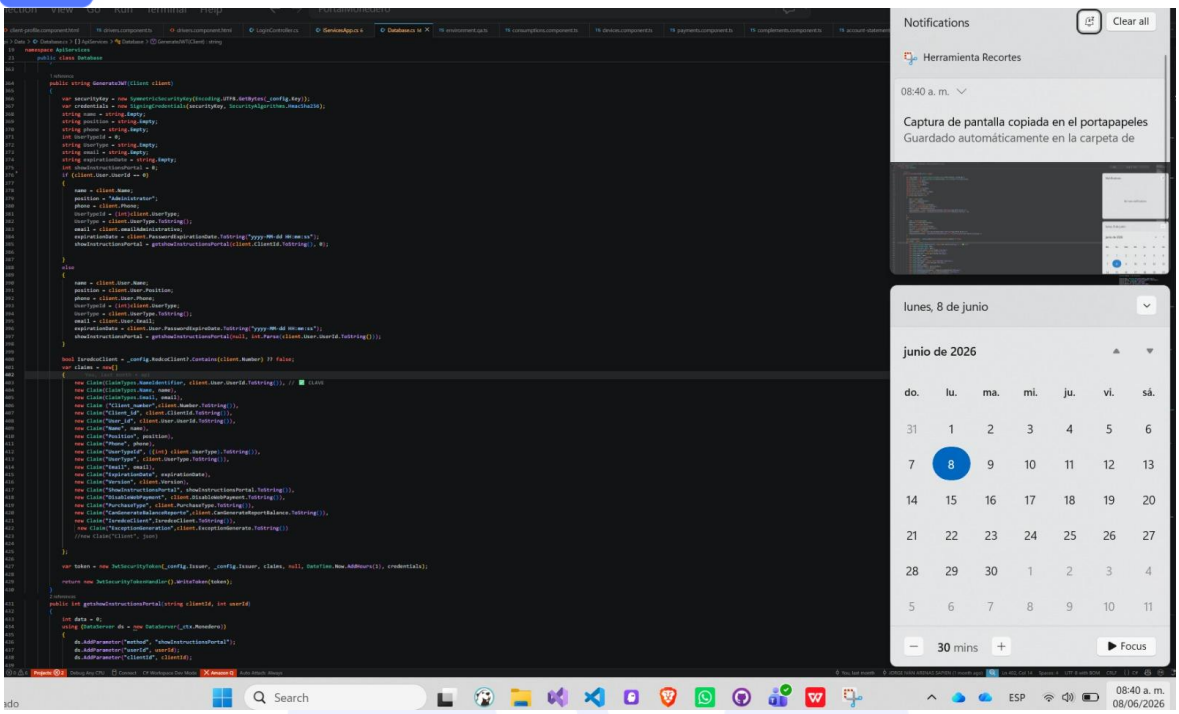


E52-B-03. Mapeo de dominios a backends autorizados y prueba de host no autorizado.

6.3. Alteración de mensajes

Requisito	Demostrar que una modificación del mensaje/token es detectada y rechazada antes de que la operación sea procesada.
Estado	**INTEGRADA**

El documento fuente incluye código relacionado con generación de JWT. Para acreditar el control de integridad se incorpora una prueba comparativa: un JWT válido es aceptado y un token cuyo payload fue alterado falla la validación de firma y recibe HTTP 401.



E52-B-04. Código de aplicación relacionado con generación/validación de JWT.

API Security Console 17/09/2026

Validación de integridad de JWT

Endpoint: POST /api/v1/cards/transactions

Prueba 1 - Token válido

alg	RS256
kid	monedero-prod-2026-01
iss	https://mon.ener-go.mx
aud	portal-clientes
exp	2026-09-17T13:20:00-06:00

Firma criptográfica **VALIDA**

HTTP 200 OK

transaction_id: TX-20260917-000128

Resultado **Solicitud aceptada y procesada**

Prueba 2 - Token alterado

alg	RS256
kid	monedero-prod-2026-01
iss	https://mon.ener-go.mx
aud	portal-clientes
claim alterado	amount: 1000 -> 9000

Firma criptográfica **INVALIDA**

HTTP 401 Unauthorized

error: JWT_SIGNATURE_INVALID

Resultado **Solicitud rechazada antes del procesamiento**

La modificación del encabezado o payload invalida la firma y el servidor rechaza el mensaje.

E52-B-05. Validación de firma JWT: token válido frente a token alterado.

6.4. Revelación de información

Requisito	Demostrar que la información no se revela en claro a terceros o usuarios sin necesidad de conocerla.
Estado	**INTEGRADA**

Este riesgo se cubre mediante controles combinados ya documentados: TLS/HTTPS en tránsito, redes administrativas privadas, MFA y enmascaramiento de datos sensibles en base de datos. Las evidencias E52-A-05 y E52-A-06 forman parte integral de este inciso.

6.5. Copia no autorizada

Requisito	Demostrar que los canales administrativos y endpoints restringen mecanismos de copia, extracción o transferencia de información no autorizada.
Estado	**INTEGRADA**

Para accesos privilegiados, la configuración debe restringir portapapeles, redirección de unidades, transferencia de archivos, SFTP e impresión virtual cuando no sean necesarios. En endpoints, la política de control de dispositivos debe bloquear medios removibles y registrar los intentos.



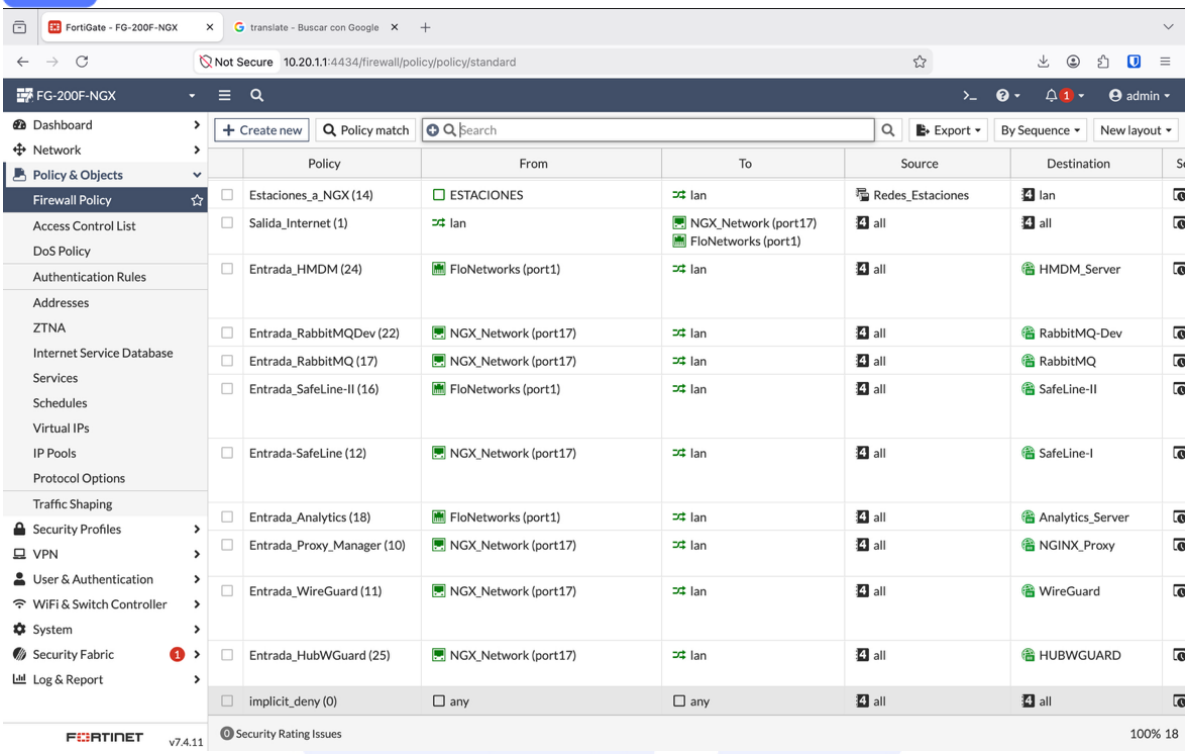
E52-B-06. Restricciones Guacamole



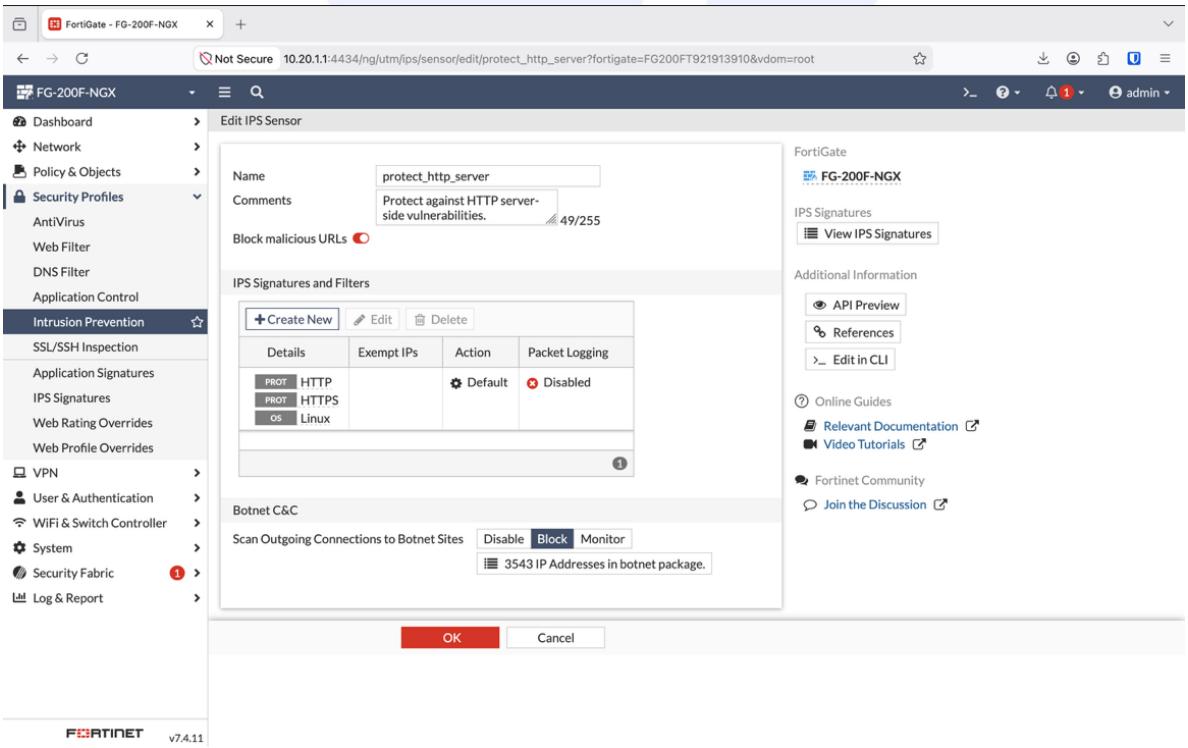
E52-B-07. Sophos Device Control

7. Evidencia técnica complementaria por activo

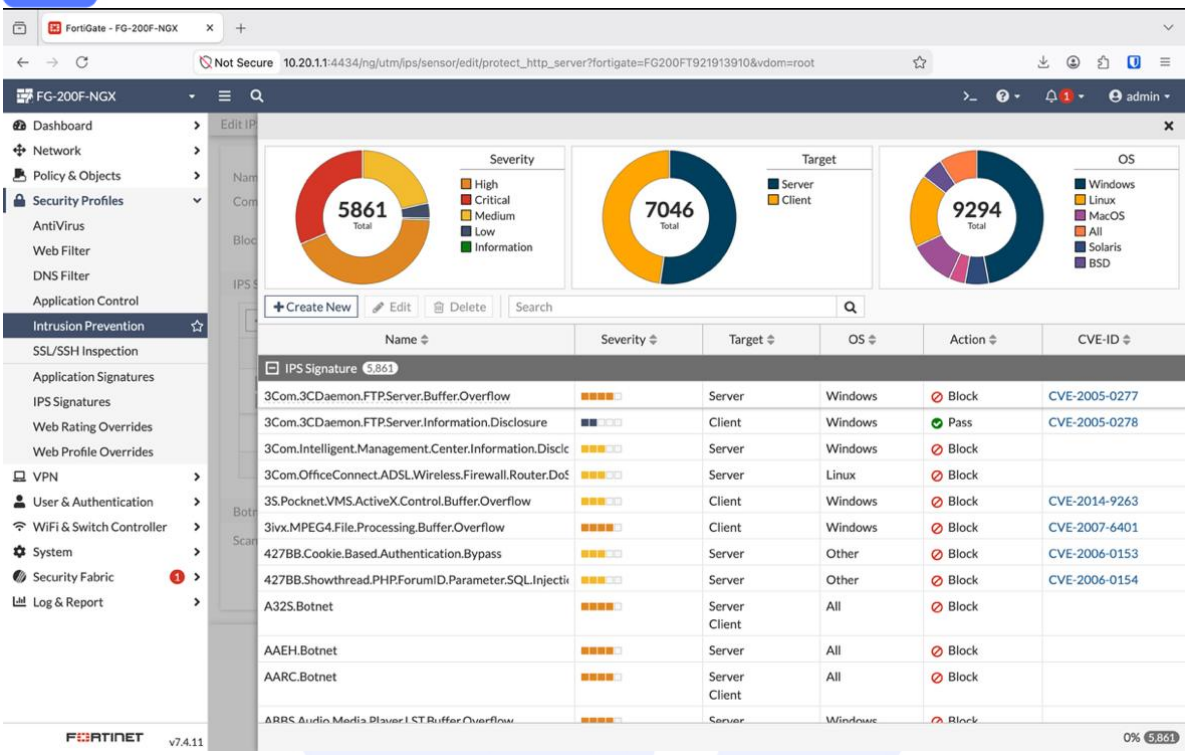
Las siguientes capturas del documento fuente complementan la trazabilidad técnica por activo y muestran la configuración de firewalls, IPS, filtrado web, MFA y servicios backend asociados al perímetro de exposición.



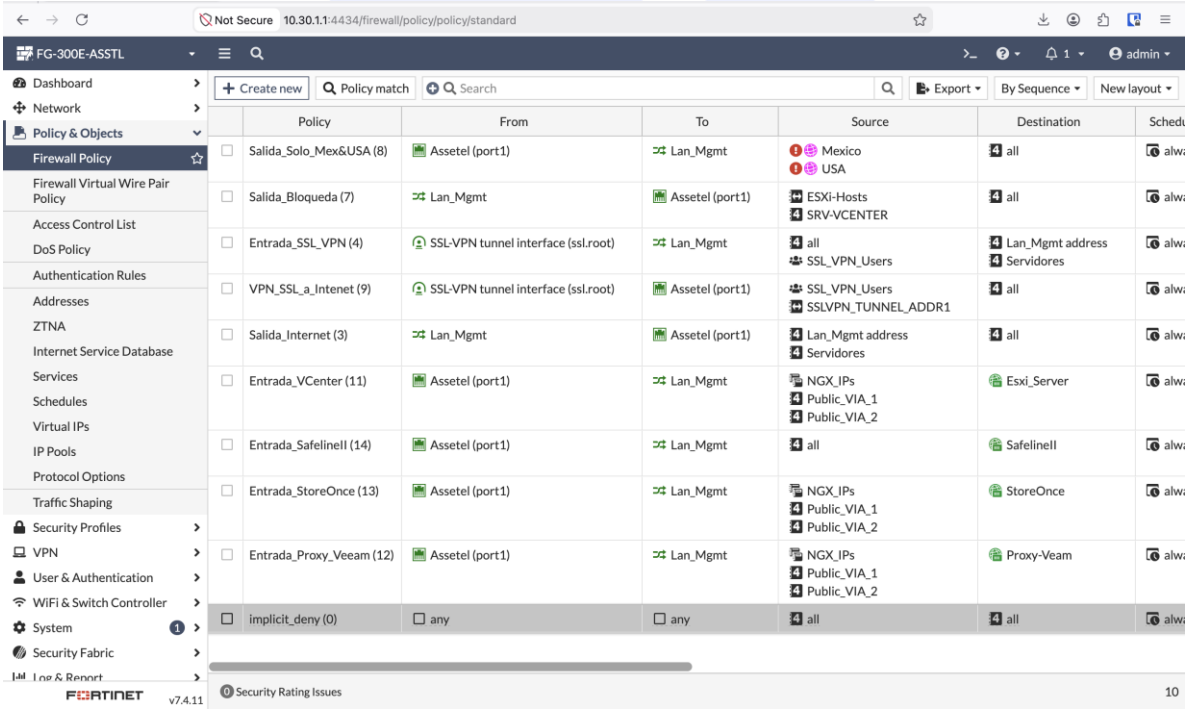
E52-TEC-28. Políticas de firewall - NGX.



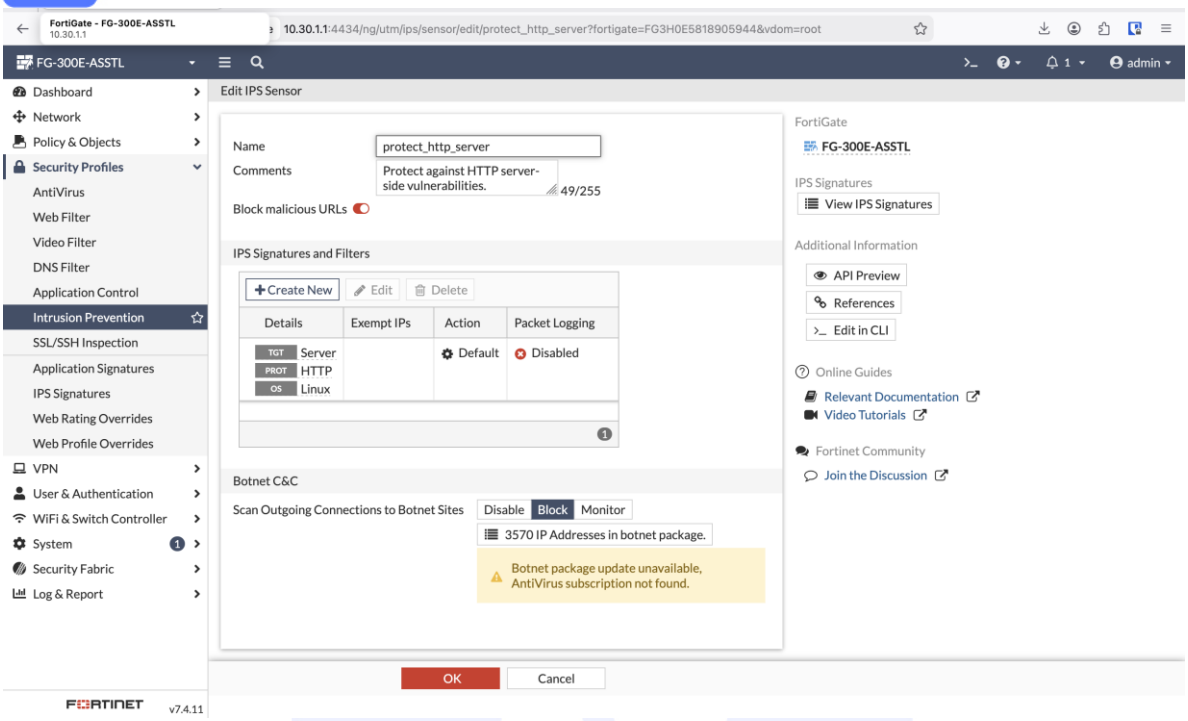
E52-TEC-29. Definición de perfil IPS - NGX.



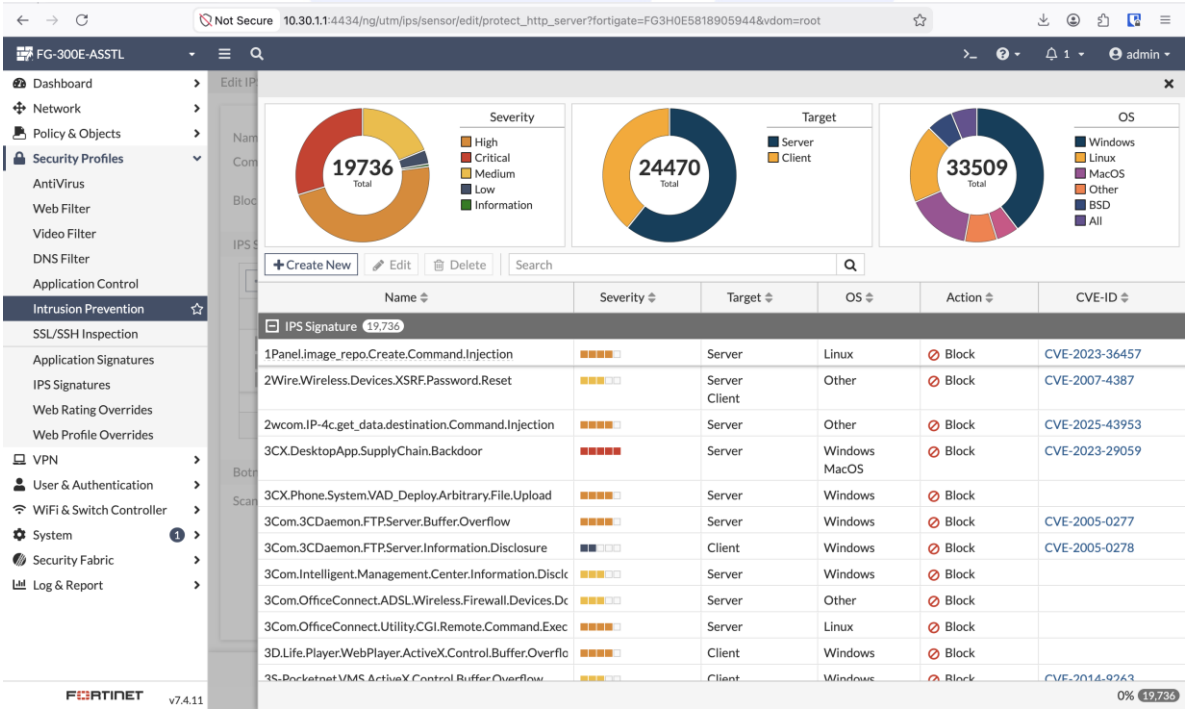
E52-TEC-30. Firmas incluidas en perfil IPS - NGX.



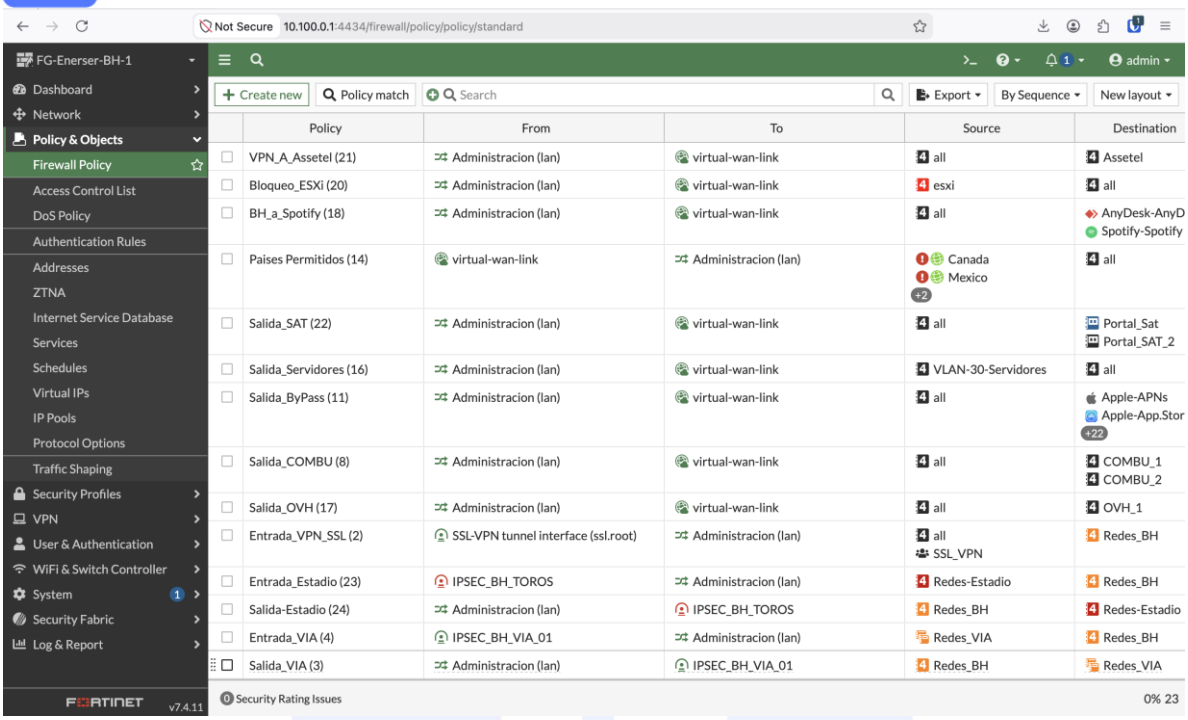
E52-TEC-31. Políticas de firewall - ASSETEL.



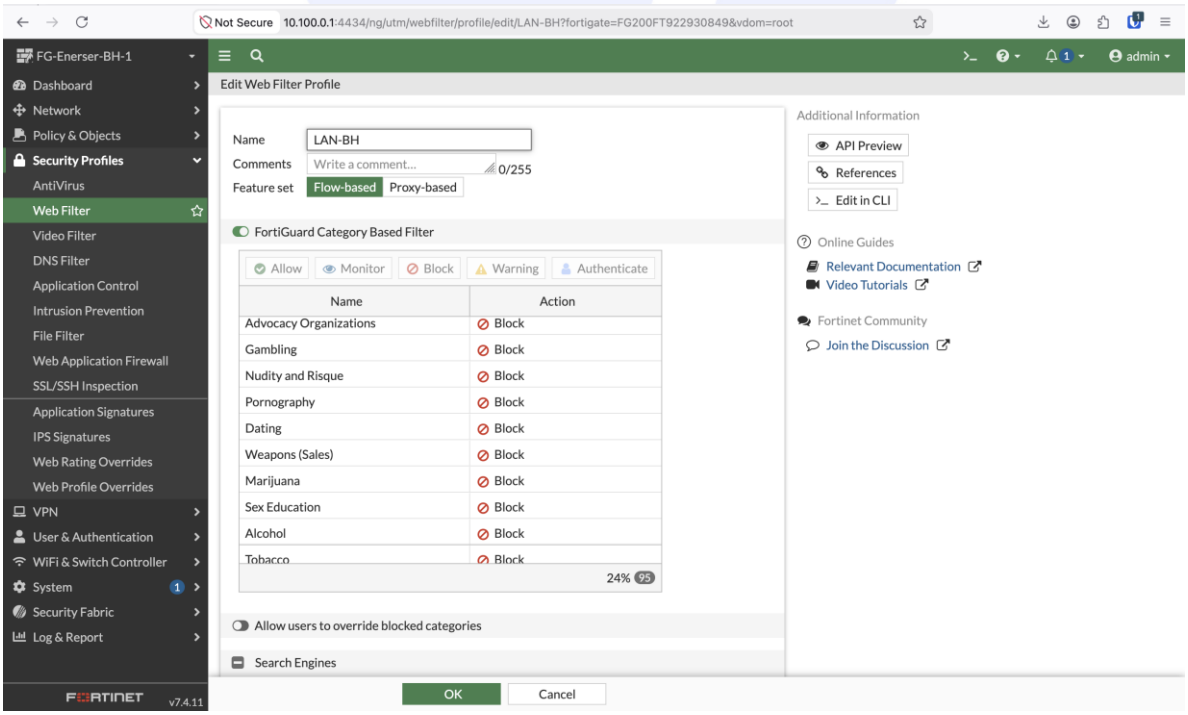
E52-TEC-32. Definición de perfil IPS - ASSETEL.



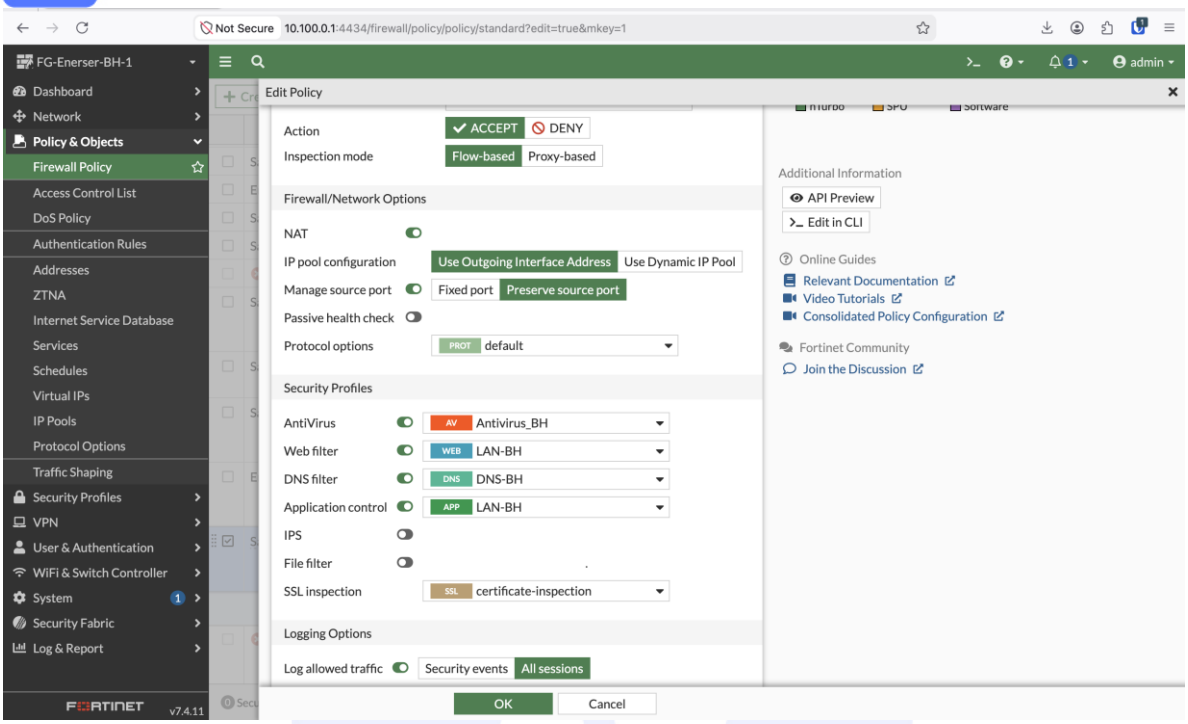
E52-TEC-33. Firmas incluidas en perfil IPS - ASSETEL.



E52-TEC-34. Políticas de firewall - oficinas.



E52-TEC-35. Perfil de filtrado de contenido web - oficinas.



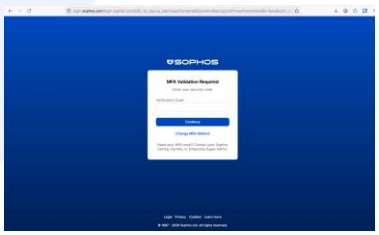
E52-TEC-36. Aplicación del perfil de filtrado en política.



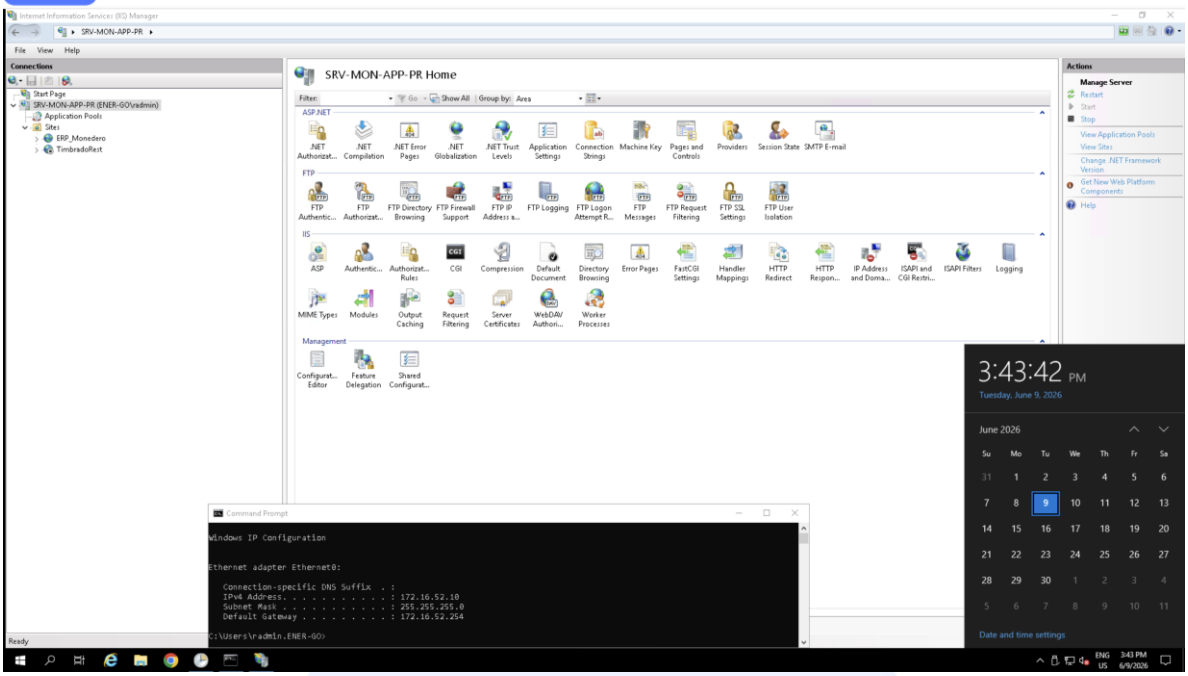
Sophos - inicio de sesión



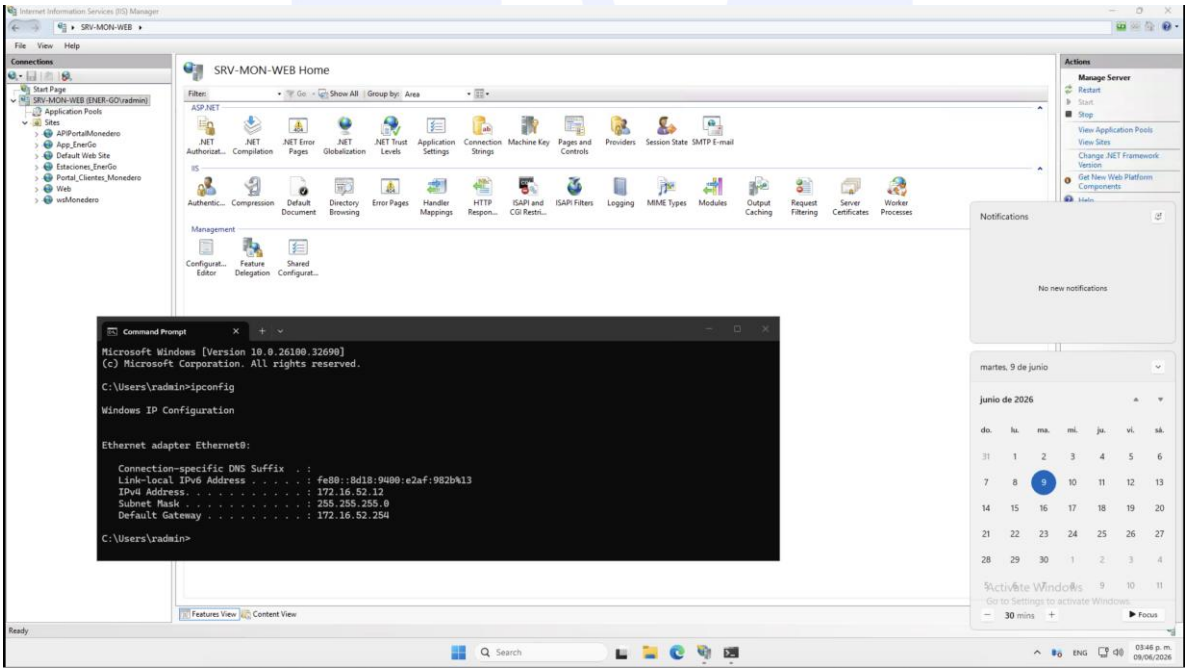
Sophos - credenciales



Sophos - MFA



E52-TEC-40. Servicios web/backend en SRV-MON-APP-PR.



E52-TEC-41. Servicios backend asociados al monedero.