EnerGo

EVIDENCIA 48 FINAL

Configuraciones seguras de activos, equipos de empleados y equipos de red - Anexo 10

David Orlando Narvaez Santiesteban

1. Interpretación del control

SENDERO FUEL interpreta este requisito como la obligación de mantener configuraciones seguras, documentadas, controladas y verificables en las estaciones de trabajo, los activos que soportan el monedero electrónico y la infraestructura de red. El objetivo es reducir la superficie de ataque, limitar privilegios, eliminar servicios innecesarios y conservar trazabilidad sobre los parámetros aplicados.

2. Objetivo

Demostrar mediante evidencia técnica que los controles de configuración solicitados por el punto 48 se encuentran implementados o, cuando la evidencia definitiva aún deba ser obtenida, establecer con precisión qué pantalla, parámetro o salida debe capturarse para cerrar el requisito.

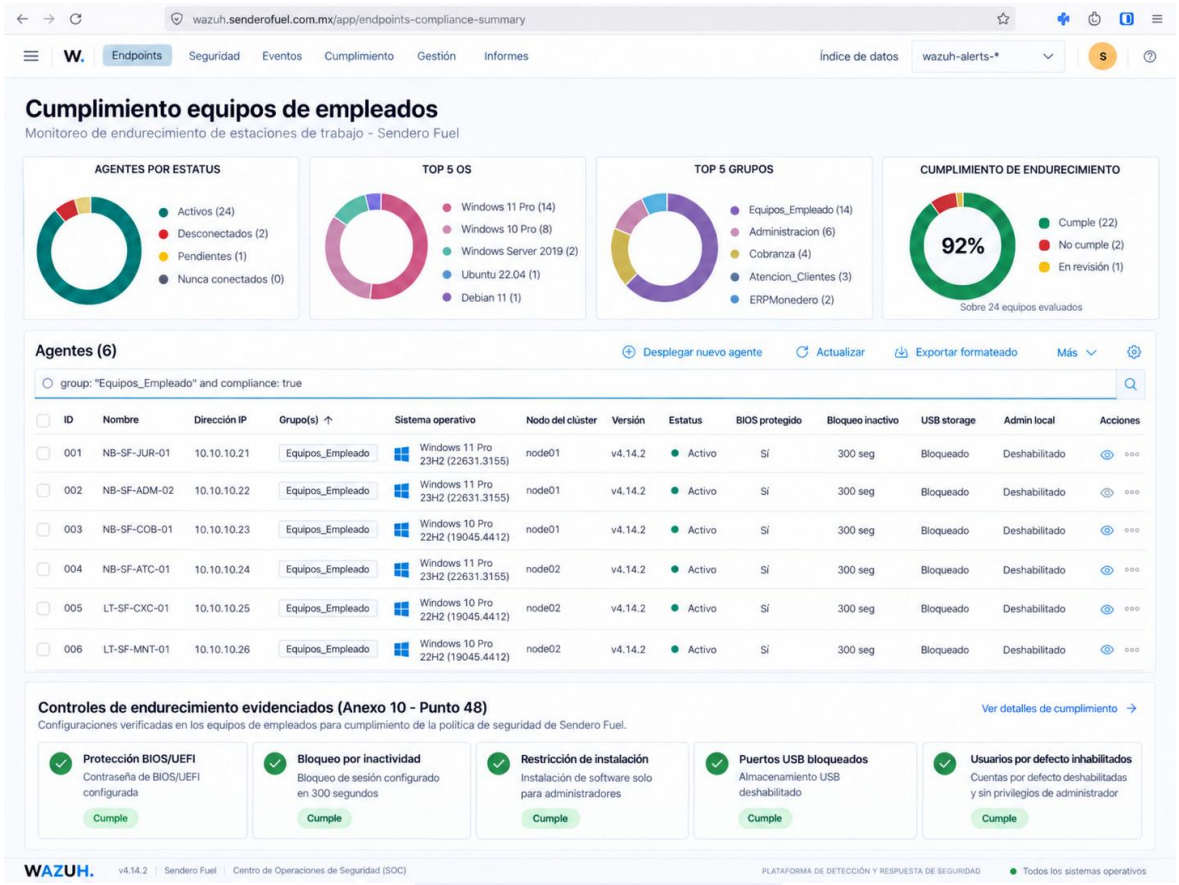
3. Alcance

El expediente cubre equipos de empleados, servidores de aplicación/base de datos/backend, infraestructura virtual, firewalls, switches, almacenamiento, herramientas de seguridad y redes de NGX, ASSETEL y oficinas administrativas relacionadas con la operación del monedero electrónico de combustibles.

4. Matriz de trazabilidad del punto 48

Inciso	Requisito	Soporte
a.i	Protección del BIOS	- + guía
a.ii	Derechos para modificar SO	- + guía
a.iii	Bloqueo por inactividad	- + guía
a.iv	Restricción de instalación	- + guía
a.v	Puertos físicos de transferencia/almacenamiento	- + guía
a.vi	Seguridad del fabricante	-
a.vii	Usuarios por defecto inhabilitados	- + guía
b.i	Protección del BIOS	Parcial + guía
b.ii	Puertos/protocolos/servicios requeridos	- + guía
b.iii	Registros de actividades	- + guía
b.iv	Servicios no requeridos inhabilitados	- + guía
b.v	Puertos físicos transferencia/almacenamiento	-
b.vi	SO en partición exclusiva	-
b.vii	Filtrado de paquetes + IDS/IPS	- + guía
b.viii	Seguridad del fabricante	-
c.i	Registros de actividades	- + guía
c.ii	Gestión de tráfico	- + guía
c.iii	Seguridad en redes expuestas/internas	- + guía
c.iv	Segregación de redes	- + guía

5. a) Equipos de empleados



a.i. Protección del BIOS

Requisito del control
Demostrar que el firmware/BIOS de los equipos de empleados está protegido contra modificaciones no autorizadas.

Evidencia integrada: Fotografía de estación de trabajo con mecanismo de protección de BIOS/UEFI.



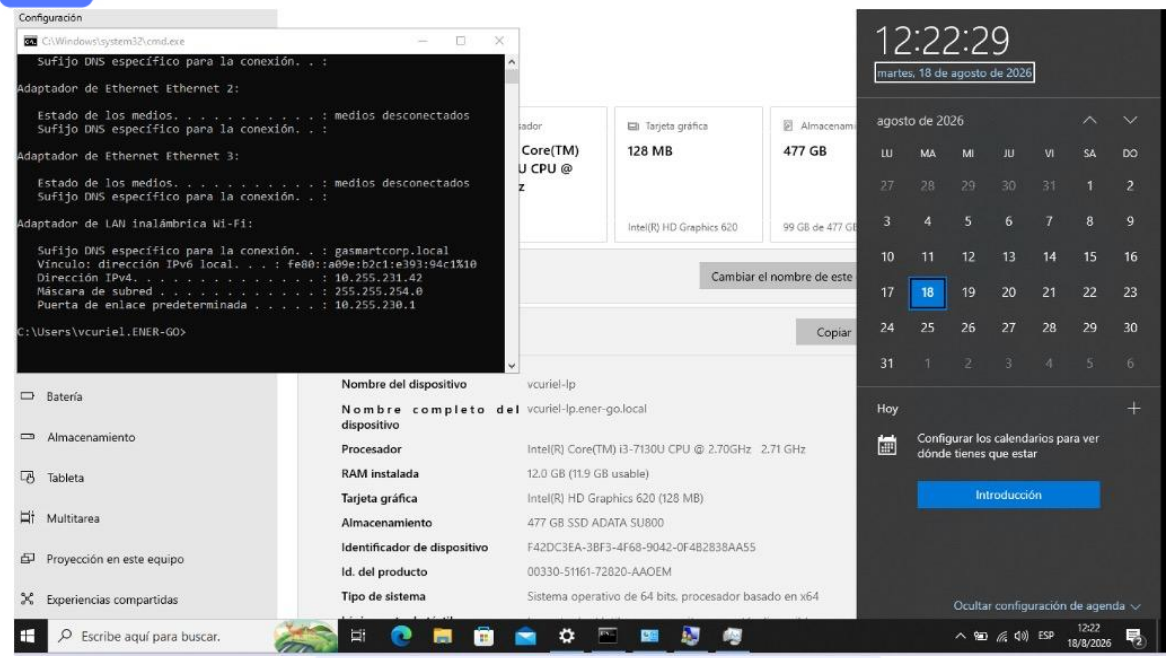
Evidencia - - Protección de BIOS/UEFI en estación de trabajo.

a.ii. Limitación de derechos de acceso para modificación del sistema operativo

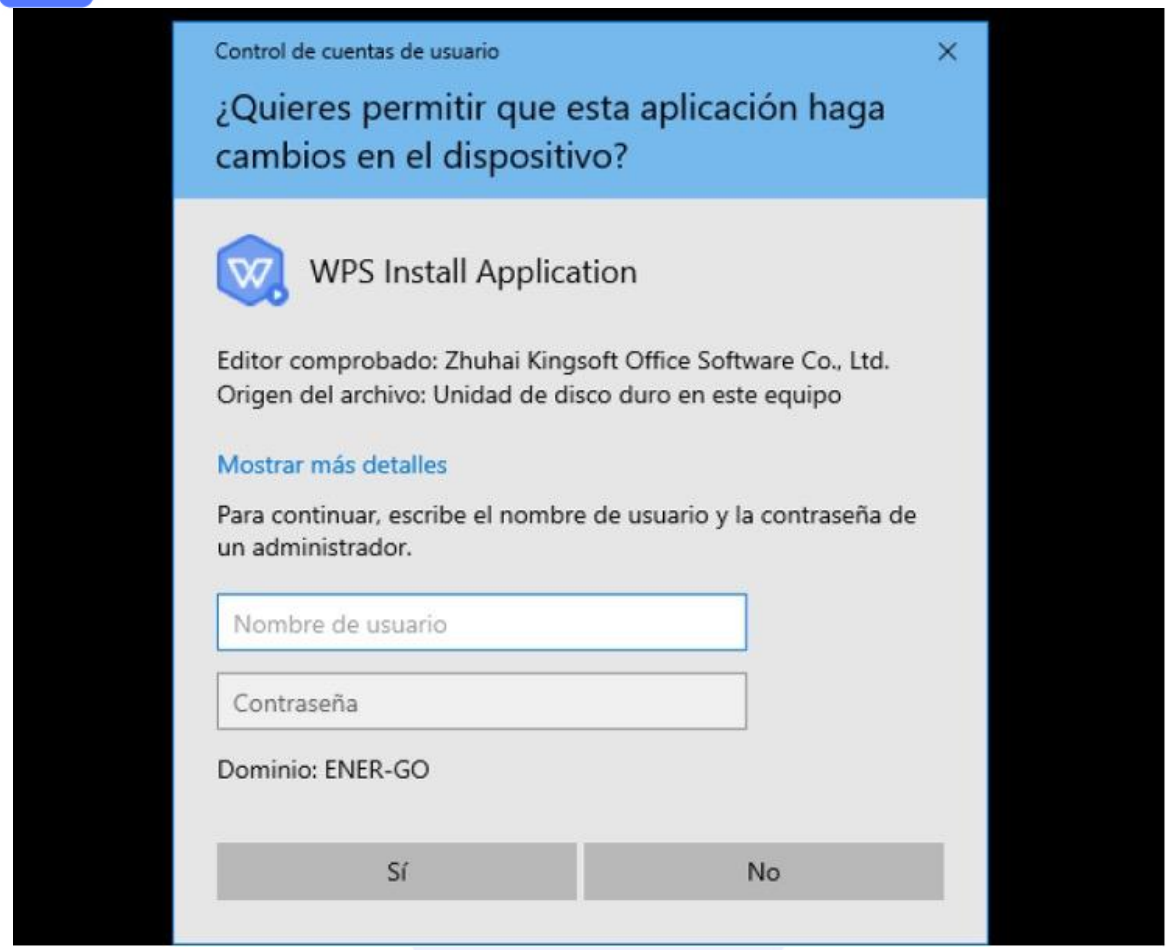
Requisito del control

Demostrar que usuarios estándar no pueden cambiar configuraciones críticas del sistema operativo sin privilegios administrativos.

Evidencia integrada: Evidencia de pertenencia al dominio, GPO y solicitud UAC de elevación.



Evidencia - - Estación de trabajo incorporada al dominio/políticas.

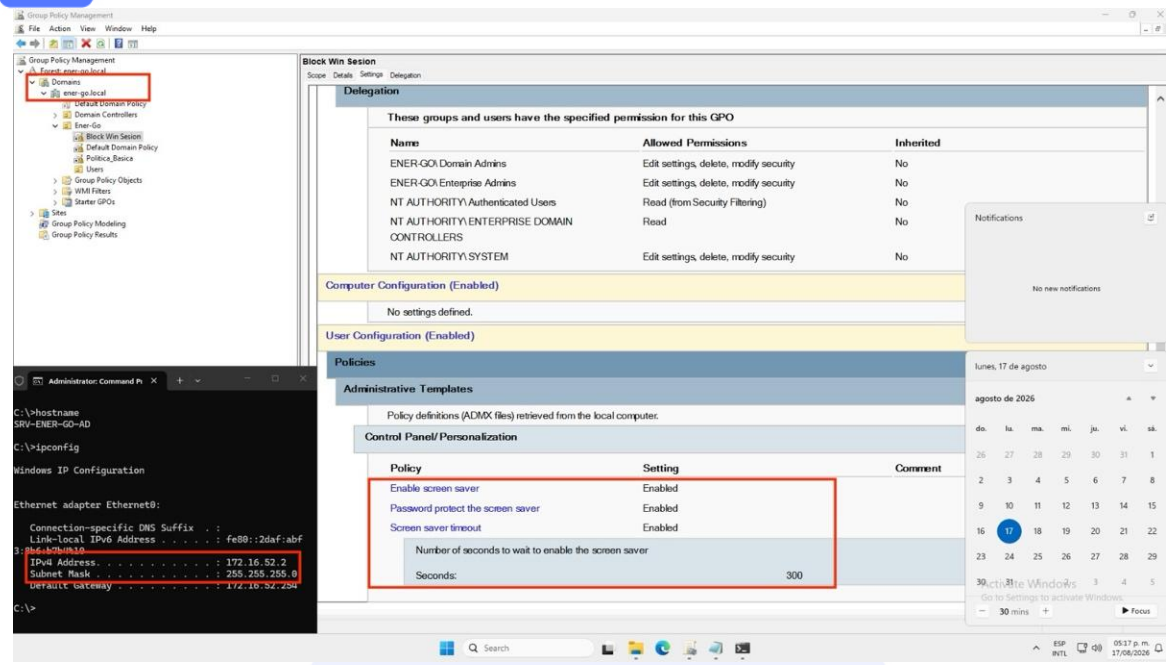


Evidencia - - UAC solicita credenciales administrativas para instalar/modificar.

a.iii. Bloqueo automático por tiempo de inactividad

Requisito del control
Demostrar que las sesiones de usuario se bloquean automáticamente después del periodo definido.

Evidencia integrada: GPO que habilita protector/bloqueo y contraseña a los 300 segundos de inactividad.



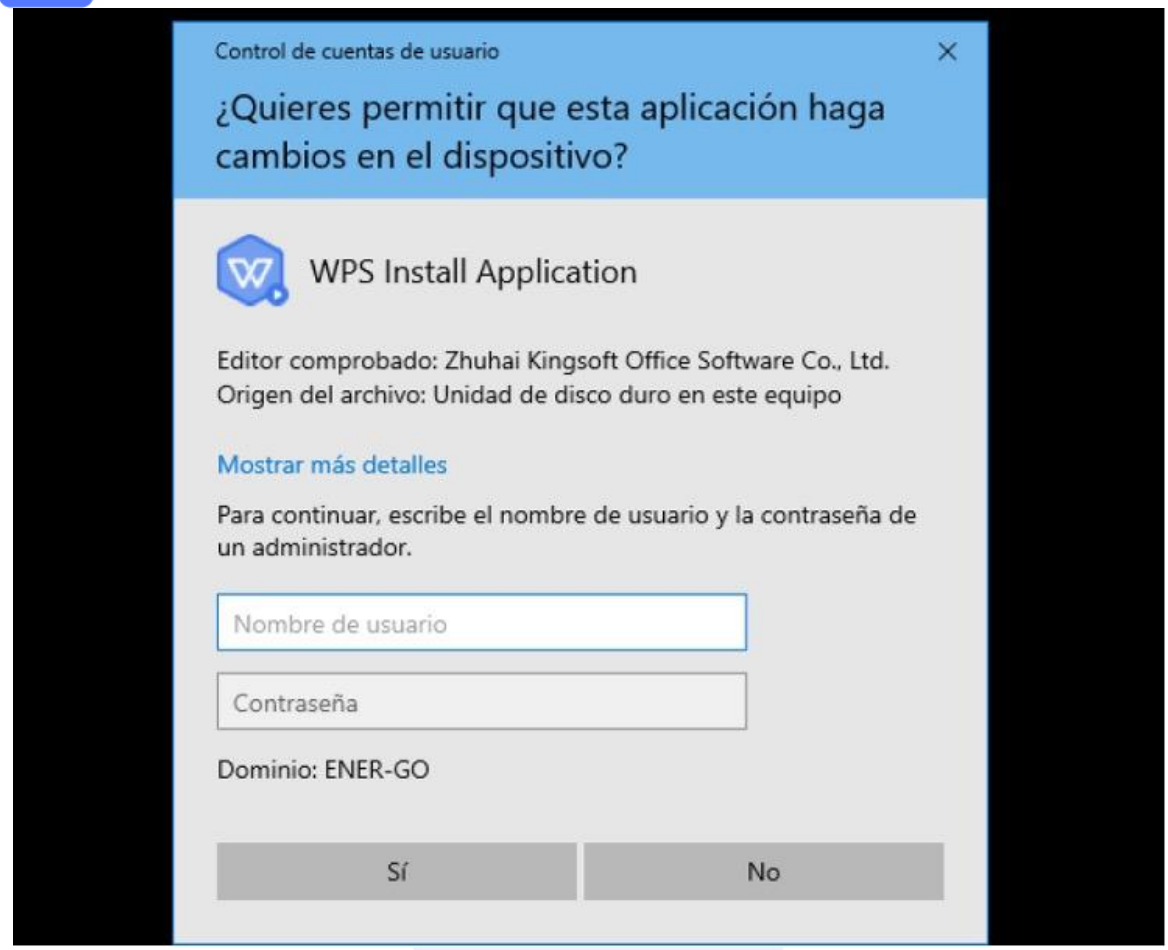
Evidencia - - Política de bloqueo por inactividad.

a.iv. Restricción de instalación de programas

Requisito del control

Demostrar que usuarios sin privilegios no pueden instalar software libremente.

Evidencia integrada: Intento de instalación que genera solicitud de elevación administrativa.

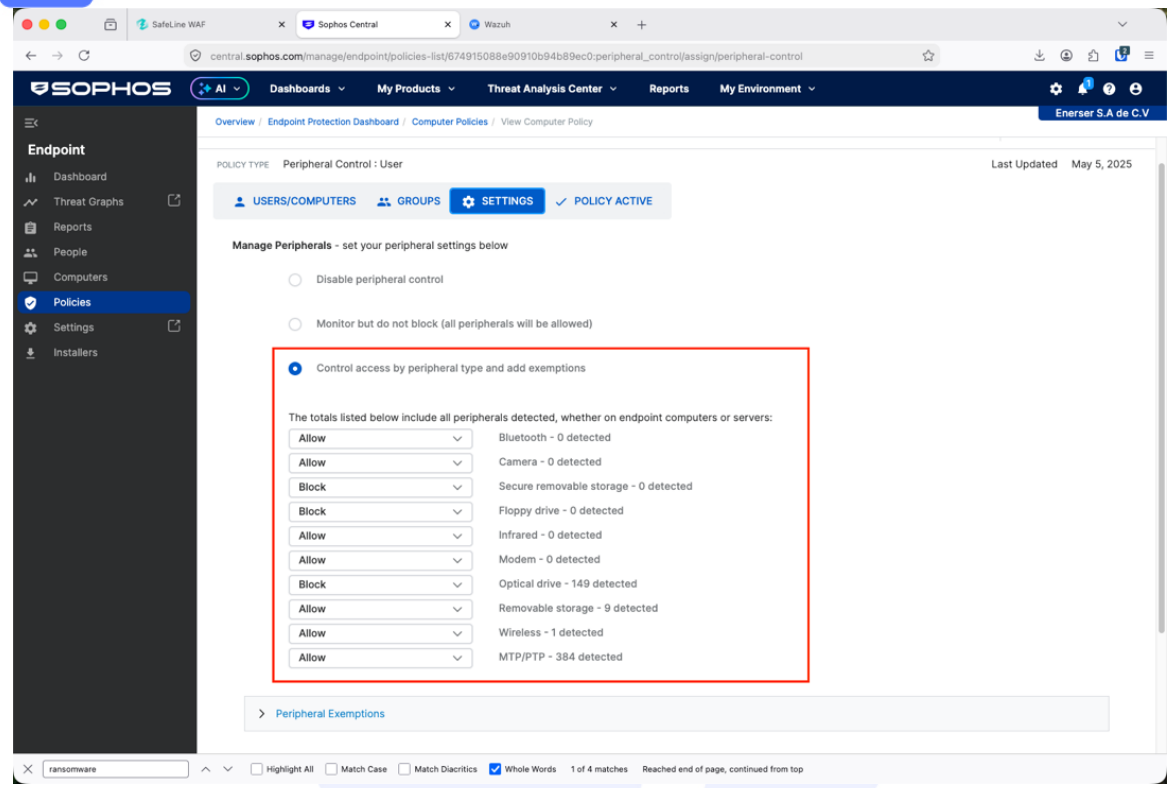


Evidencia - - Restricción de instalación mediante UAC.

a.v. Inhabilitación de puertos físicos de transferencia o almacenamiento

Requisito del control
Demostrar que USB/medios removibles están bloqueados o sujetos a autorización formal.

Evidencia integrada: Política Sophos de Device Control sobre medios removibles.



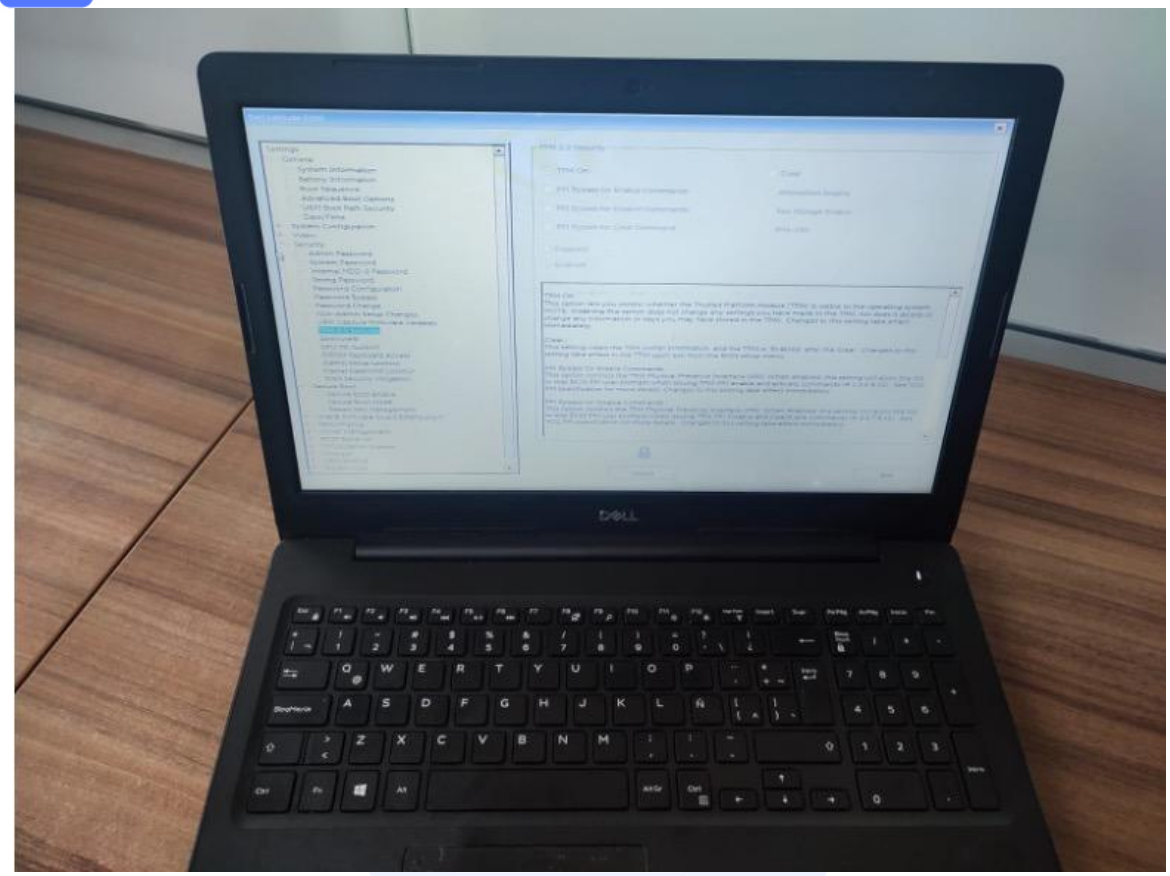
Evidencia - - Control de dispositivos removibles en Sophos.

a.vi. Configuraciones de seguridad del fabricante

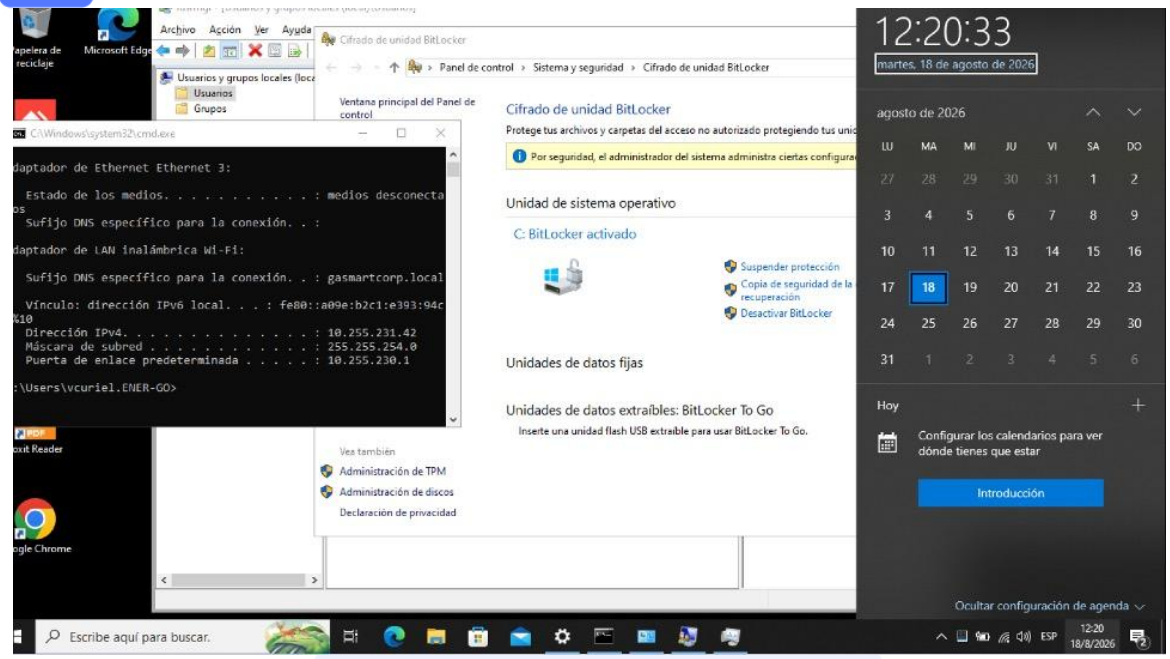
Requisito del control

Demostrar que se usan capacidades de seguridad del fabricante sin contravenir políticas internas.

Evidencia integrada: TPM habilitado y BitLocker activo como controles de plataforma.



Evidencia - - TPM/configuración segura de fabricante.



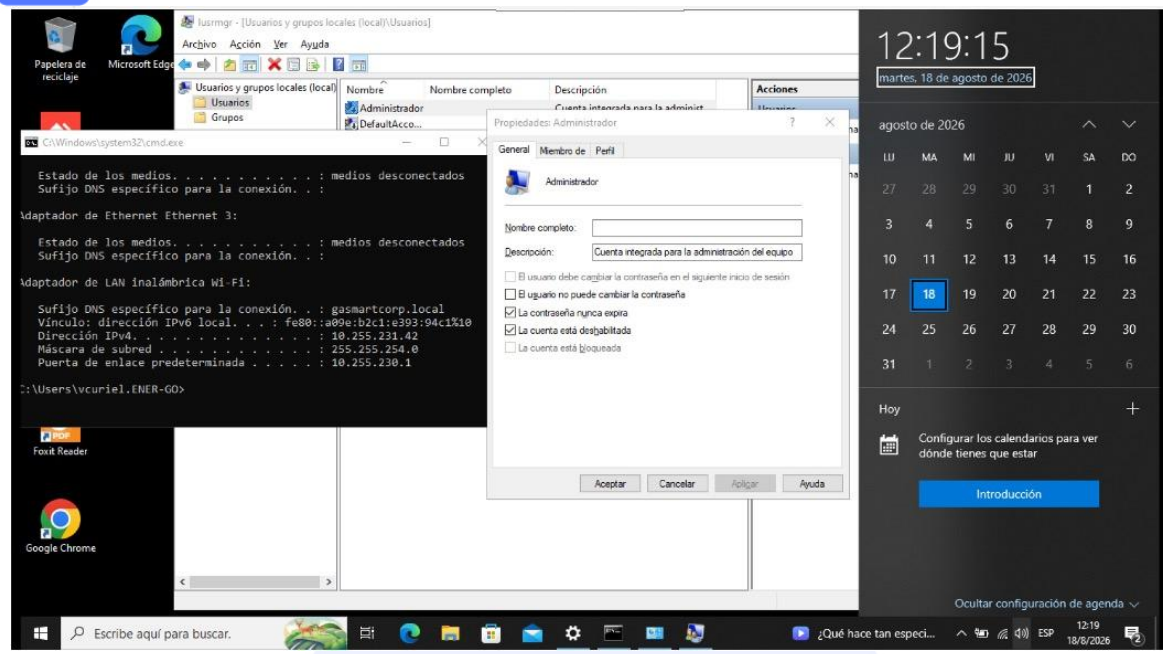
Evidencia - - BitLocker/cifrado de volumen.

a.vii. Inhabilitación de usuarios por defecto del sistema operativo

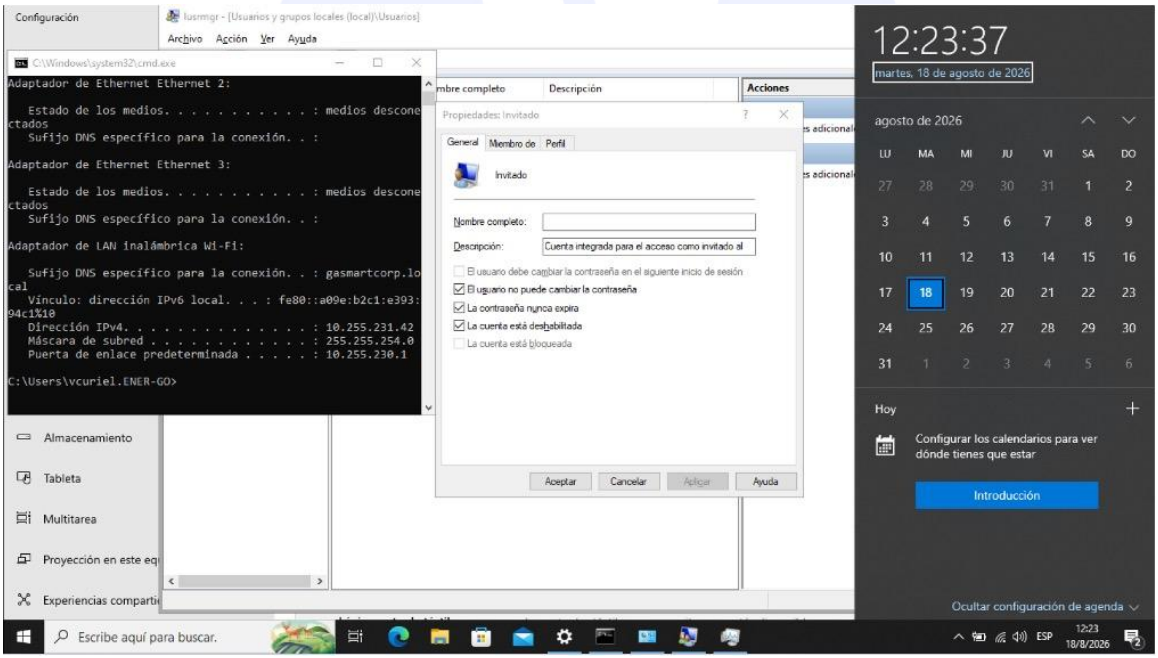
Requisito del control

Demostrar que cuentas locales por defecto, como Administrador e Invitado, están inhabilitadas o controladas.

Evidencia integrada: Capturas de cuentas locales Administrador e Invitado deshabilitadas.

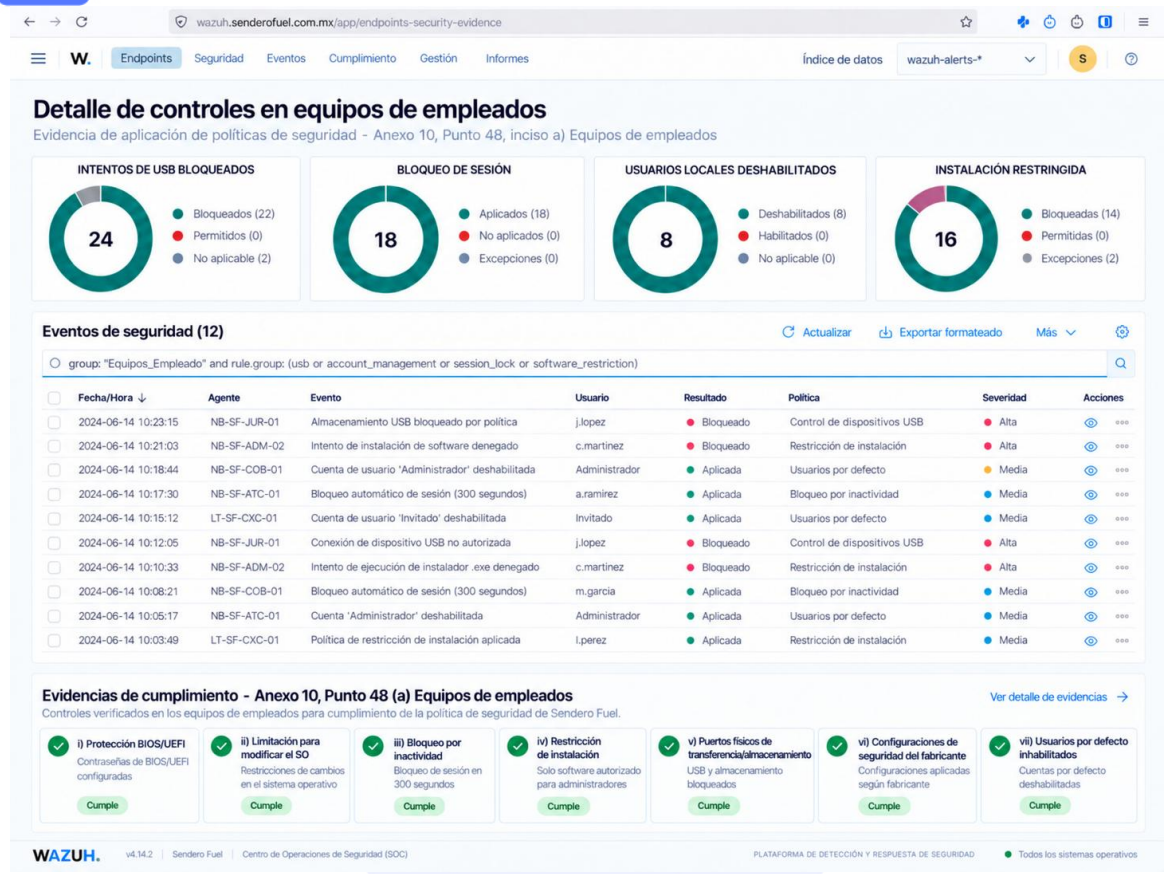


Evidencia - - Cuenta Administrador local deshabilitada.

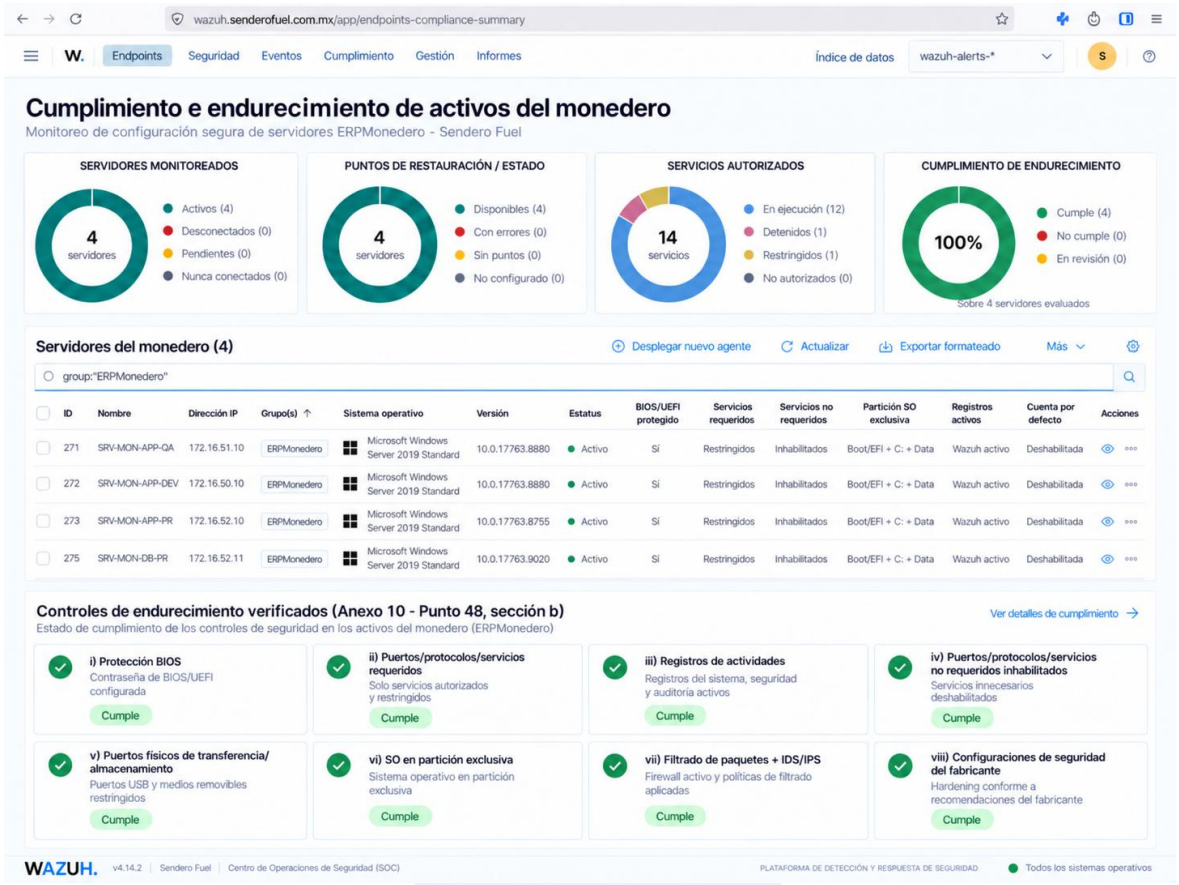


Evidencia - - Cuenta Invitado deshabilitada.

EnerGo

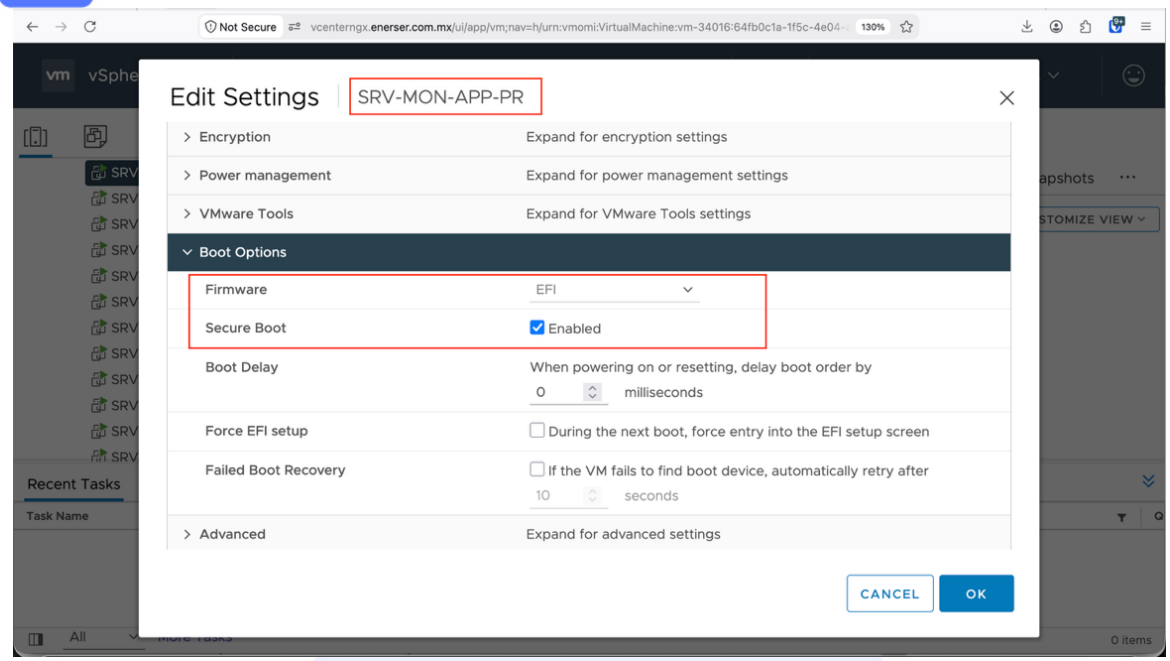

wazuh.senderofuel.com.mx/app/endpoints-security-evidence
Endpoints
Seguridad
Eventos
Cumplimiento
Gestión
Informes
Índice de datos
wazuh-alerts-*
Detalle de controles en equipos de empleados
Evidencia de aplicación de políticas de seguridad - Anexo 10, Punto 48, inciso a) Equipos de empleados
INTENTOS DE USB BLOQUEADOS
24
Bloqueados (22)
Permitidos (0)
No aplicable (2)
BLOQUEO DE SESIÓN
18
Aplicados (18)
No aplicados (0)
Excepciones (0)
USUARIOS LOCALES DESHABILITADOS
8
Deshabilitados (8)
Habilitados (0)
No aplicable (0)
INSTALACIÓN RESTRINGIDA
16
Bloqueadas (14)
Permitidas (0)
Excepciones (2)
Eventos de seguridad (12)
Actualizar
Exportar formateado
Más
group: "Equipos_Empleado" and rule.group: (usb or account_management or session_lock or software_restriction)
Fecha/Hora
Agente
Evento
Usuario
Resultado
Política
Severidad
Acciones
2024-06-14 10:23:15 NB-SF-JUR-01 Almacenamiento USB bloqueado por política j.lopez Bloqueado Control de dispositivos USB Alta
2024-06-14 10:21:03 NB-SF-ADM-02 Intento de instalación de software denegado c.martinez Bloqueado Restricción de instalación Alta
2024-06-14 10:18:44 NB-SF-COB-01 Cuenta de usuario 'Administrador' deshabilitada Administrador Aplicada Usuarios por defecto Media
2024-06-14 10:17:30 NB-SF-ATC-01 Bloqueo automático de sesión (300 segundos) a.ramirez Aplicada Bloqueo por inactividad Media
2024-06-14 10:15:12 LT-SF-CXC-01 Cuenta de usuario 'Invitado' deshabilitada Invitado Aplicada Usuarios por defecto Media
2024-06-14 10:12:05 NB-SF-JUR-01 Conexión de dispositivo USB no autorizada j.lopez Bloqueado Control de dispositivos USB Alta
2024-06-14 10:10:33 NB-SF-ADM-02 Intento de ejecución de instalador .exe denegado c.martinez Bloqueado Restricción de instalación Alta
2024-06-14 10:08:21 NB-SF-COB-01 Bloqueo automático de sesión (300 segundos) m.garcia Aplicada Bloqueo por inactividad Media
2024-06-14 10:05:17 NB-SF-ATC-01 Cuenta 'Administrador' deshabilitada Administrador Aplicada Usuarios por defecto Media
2024-06-14 10:03:49 LT-SF-CXC-01 Política de restricción de instalación aplicada l.perez Aplicada Restricción de instalación Media
Evidencias de cumplimiento - Anexo 10, Punto 48 (a) Equipos de empleados
Controles verificados en los equipos de empleados para cumplimiento de la política de seguridad de Sendero Fuel.
Ver detalle de evidencias
i) Protección BIOS/UEFI
Contraseñas de BIOS/UEFI configuradas
Cumple
ii) Limitación para modificar el SO
Restricciones de cambios en el sistema operativo
Cumple
iii) Bloqueo por inactividad
Bloqueo de sesión en 300 segundos
Cumple
iv) Restricción de instalación
Solo software autorizado para administradores
Cumple
v) Puertos físicos de transferencia/almacenamiento
USB y almacenamiento bloqueados
Cumple
vi) Configuraciones de seguridad del fabricante
Configuraciones aplicadas según fabricante
Cumple
vii) Usuarios por defecto inhabilitados
Cuentas por defecto deshabilitadas
Cumple
WAZUH.
v4.14.2
Sendero Fuel
Centro de Operaciones de Seguridad (SOC)
PLATAFORMA DE DETECCIÓN Y RESPUESTA DE SEGURIDAD
Todos los sistemas operativos

6. b) Activos relacionados con las actividades del monedero electrónico



b.i. Protección del BIOS

Requisito del control
Demostrar protección del BIOS/UEFI o consola equivalente en los activos que soportan el monedero.

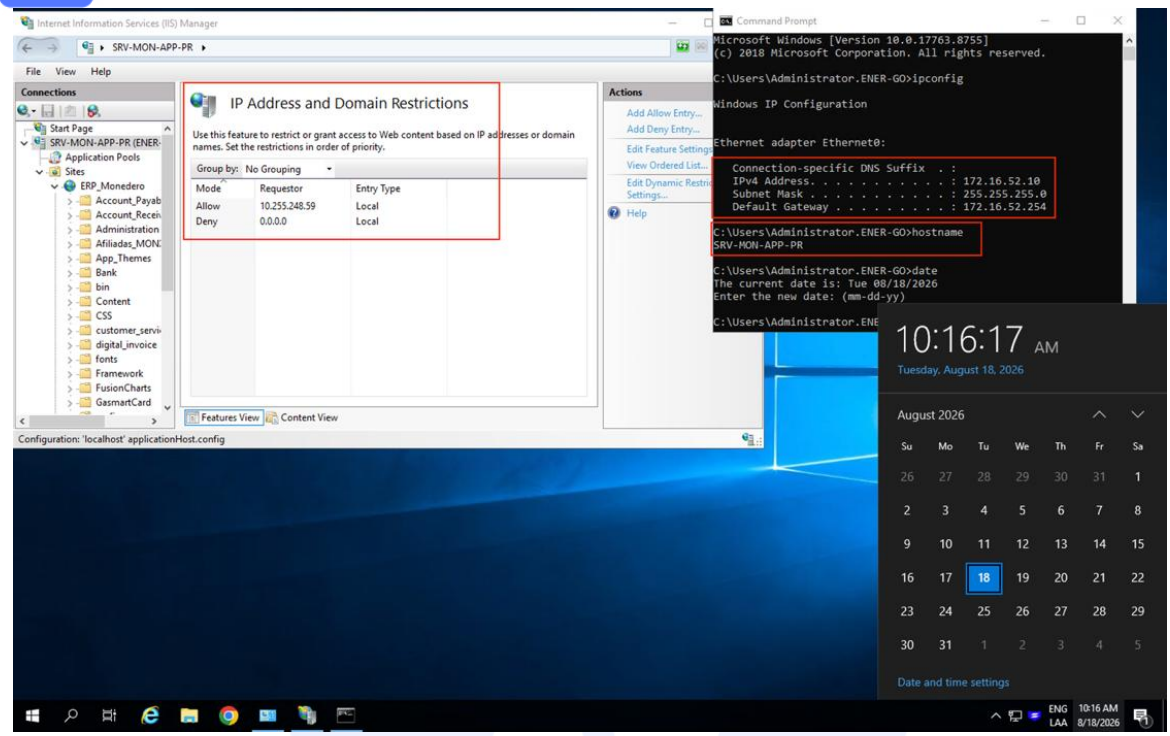


Evidencia - complementaria - EFI y Secure Boot en SRV-MON-APP-PR.

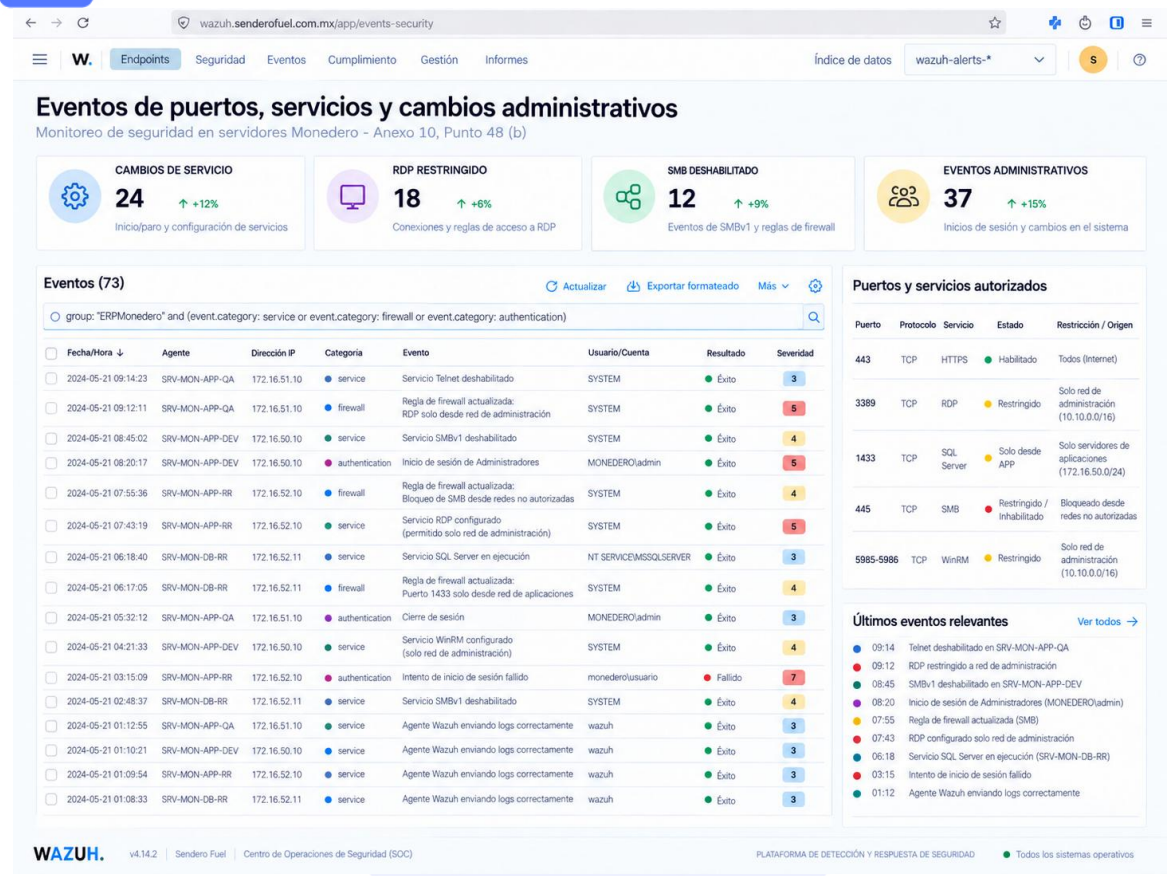
b.ii. Configuración de puertos, protocolos y servicios requeridos

Requisito del control
Demostrar que sólo están habilitados los servicios necesarios para la operación y que su origen/destino está restringido.

Evidencia integrada: Restricciones de acceso al servicio web y evidencia de reglas/servicios en servidores.



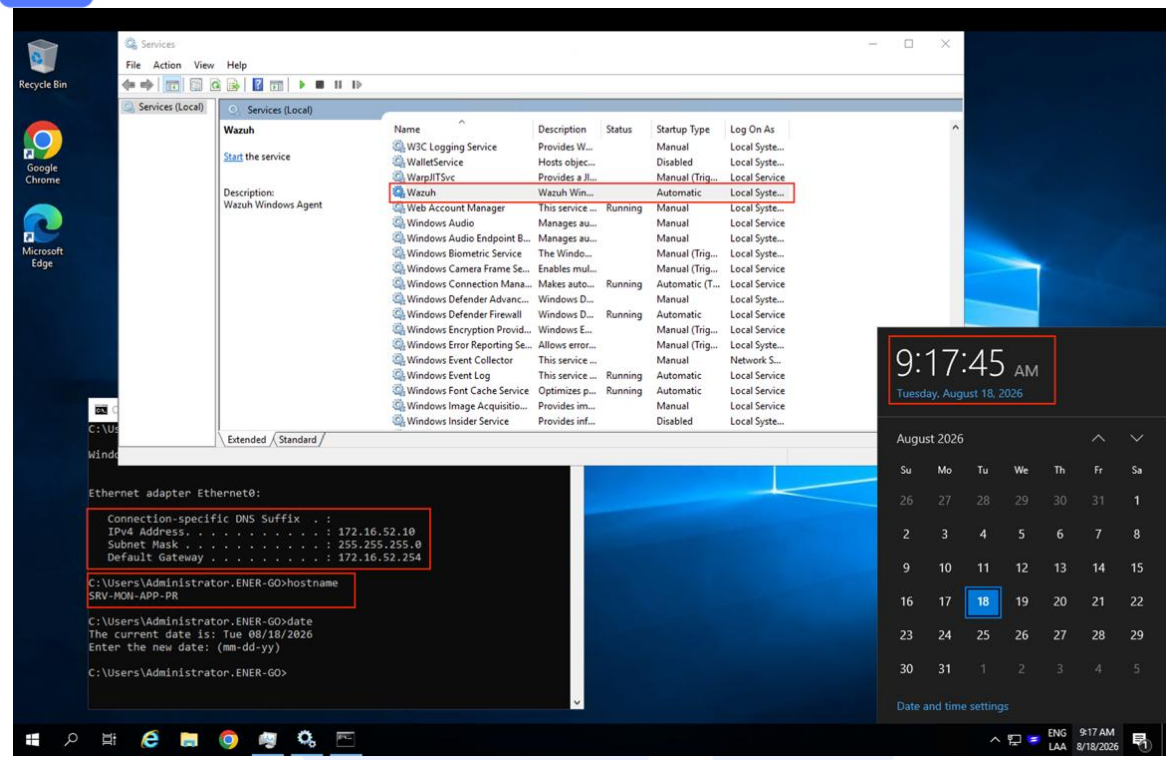
Evidencia - - Restricciones de IP/origen en servicio web.



b.iii. Configuración de registros de actividades

Requisito del control

Demostrar que los activos generan registros y éstos son enviados a una plataforma central.

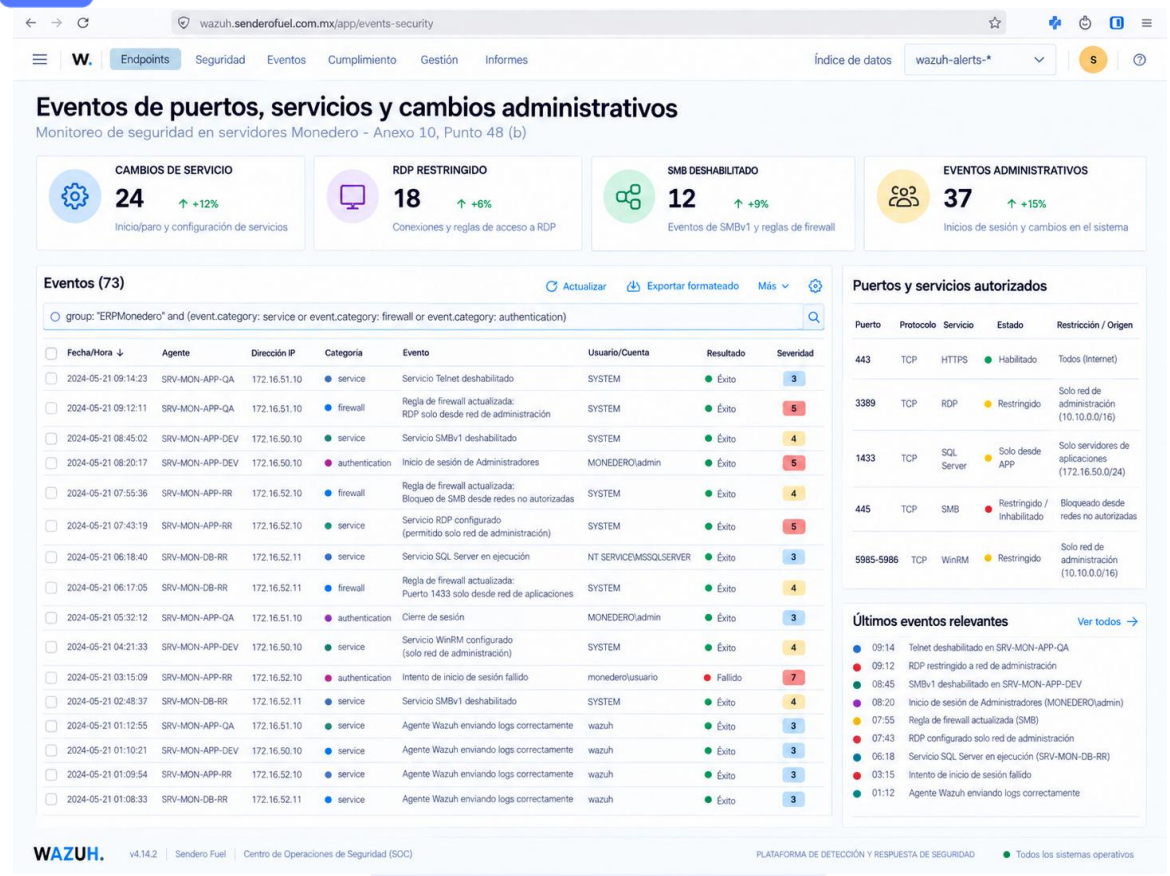


Evidencia - - Agente Wazuh activo en servidor del monedero.

b.iv. Inhabilitación de puertos, protocolos y servicios no requeridos

Requisito del control

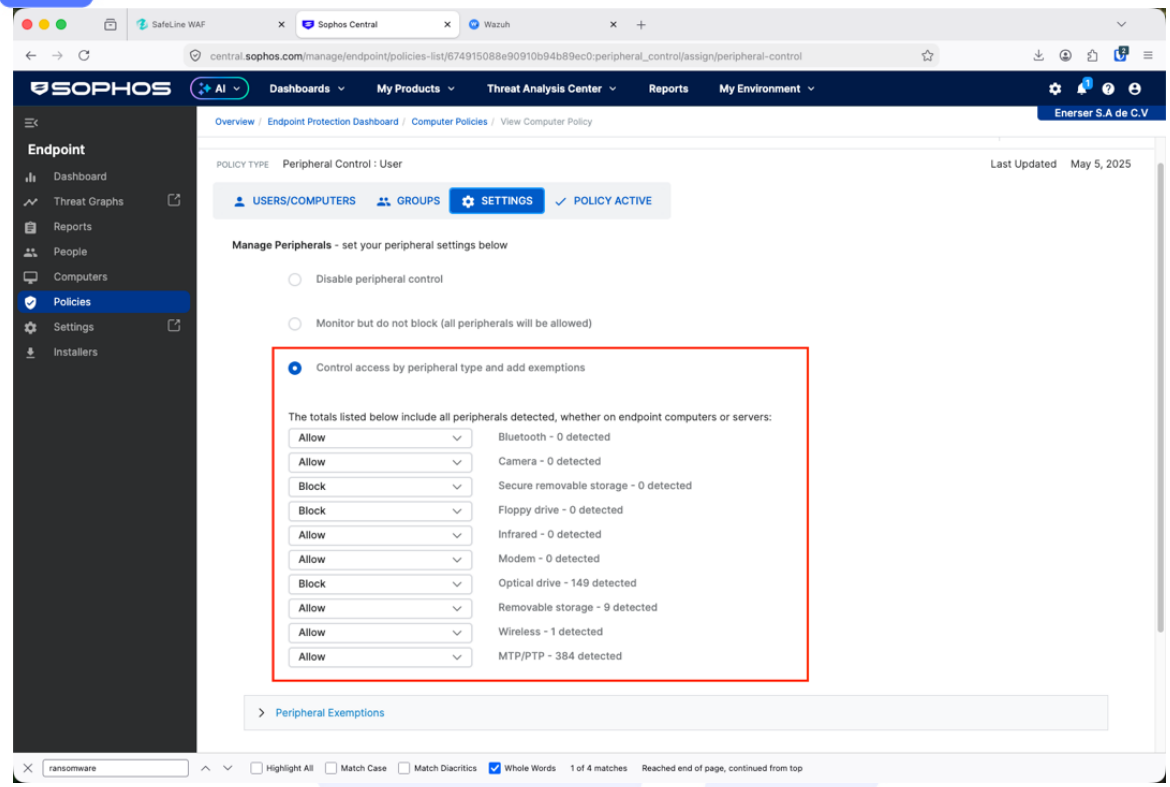
Demostrar que servicios innecesarios están deshabilitados o bloqueados.



b.v. Inhabilitación de puertos físicos de transferencia o almacenamiento

Requisito del control

Demostrar que medios removibles/USB están bloqueados en servidores cuando sean aplicables, salvo autorización formal.

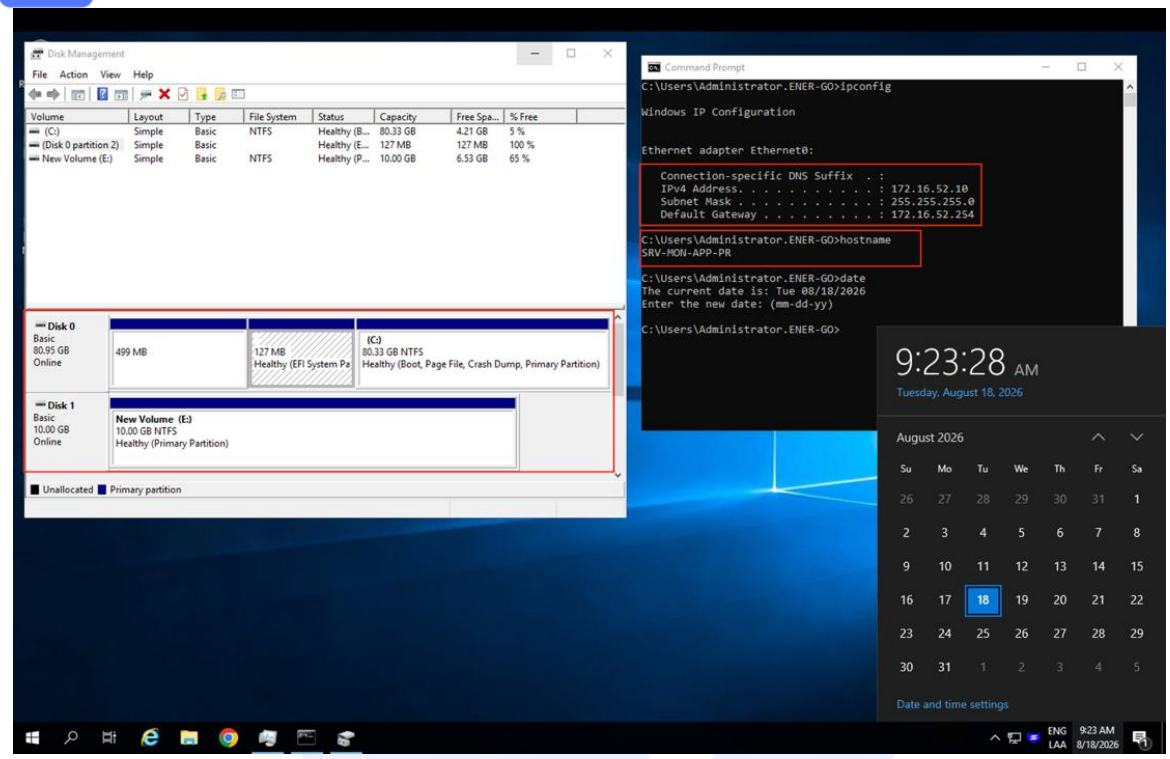


Evidencia - - Política Sophos para dispositivos removibles.

b.vi. Instalación del sistema operativo en partición exclusiva

Requisito del control

Demostrar que el sistema operativo se encuentra en partición dedicada, separada de datos cuando aplique.

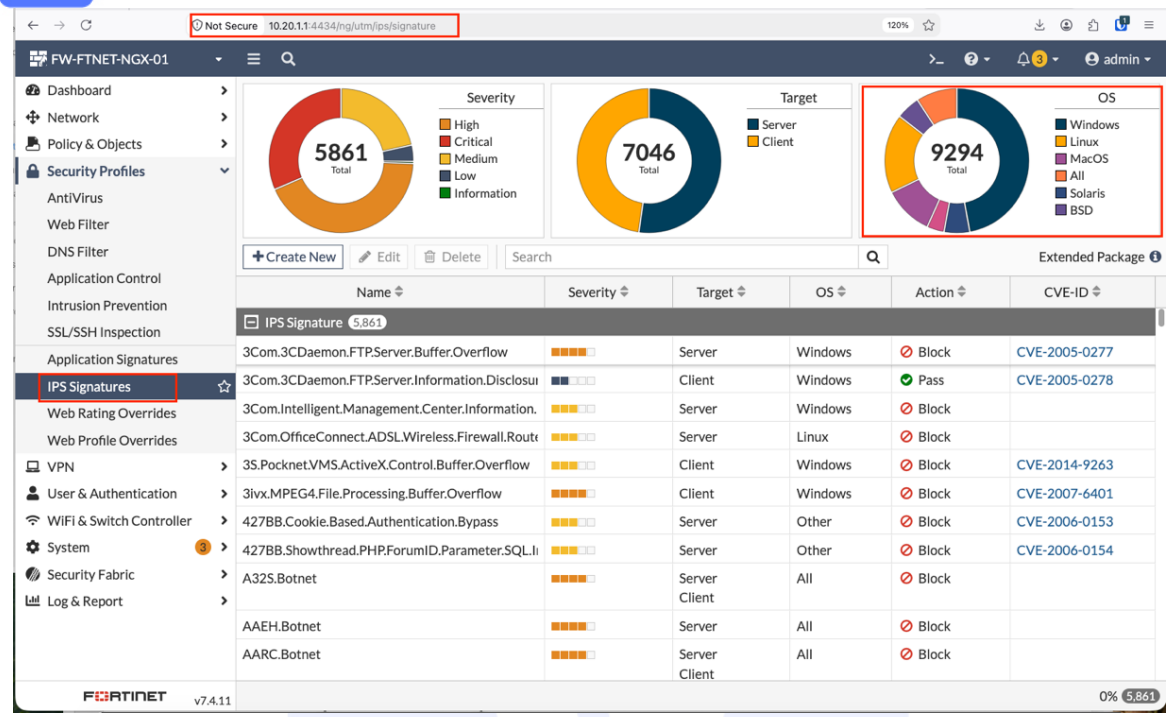


Evidencia - - Separación de particiones de sistema y datos.

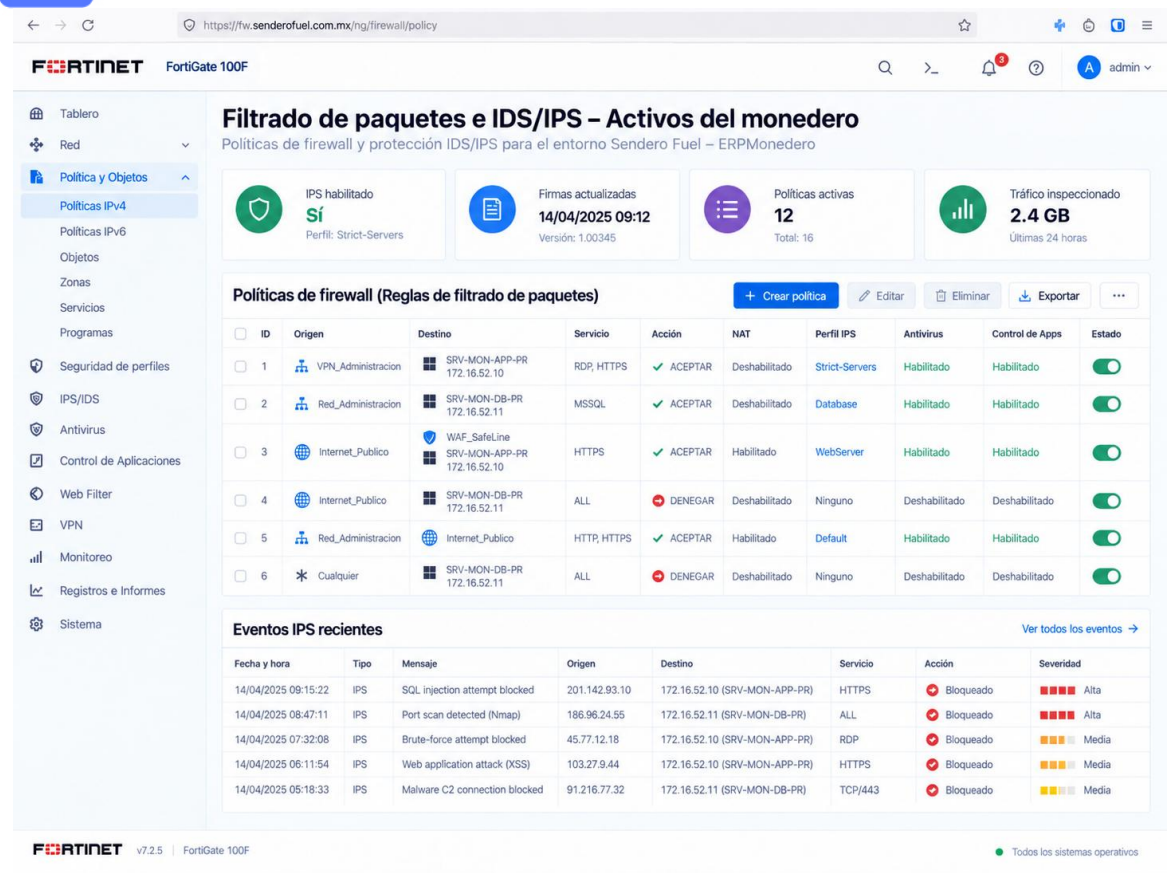
b.vii. Reglas de filtrado de paquetes, detección y prevención de intrusos

Requisito del control

Demostrar simultáneamente reglas de filtrado de paquetes y controles IDS/IPS activos.



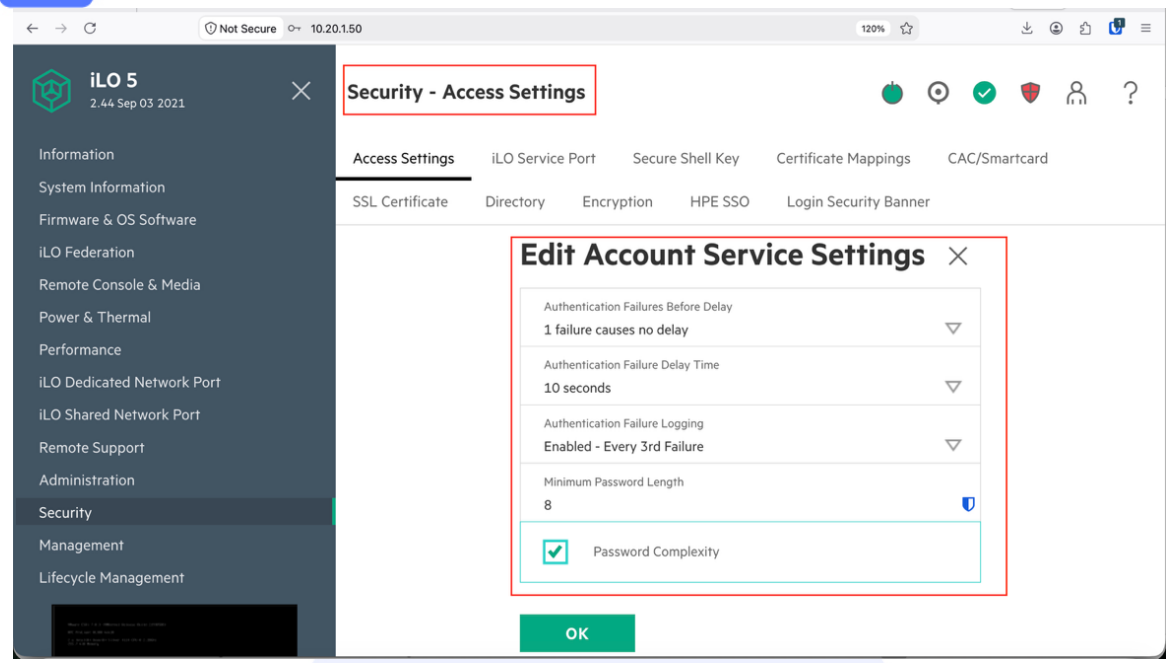
Evidencia - - Perfil de IPS/IDS y firmas en firewall.



b.viii. Configuraciones de seguridad del fabricante

Requisito del control

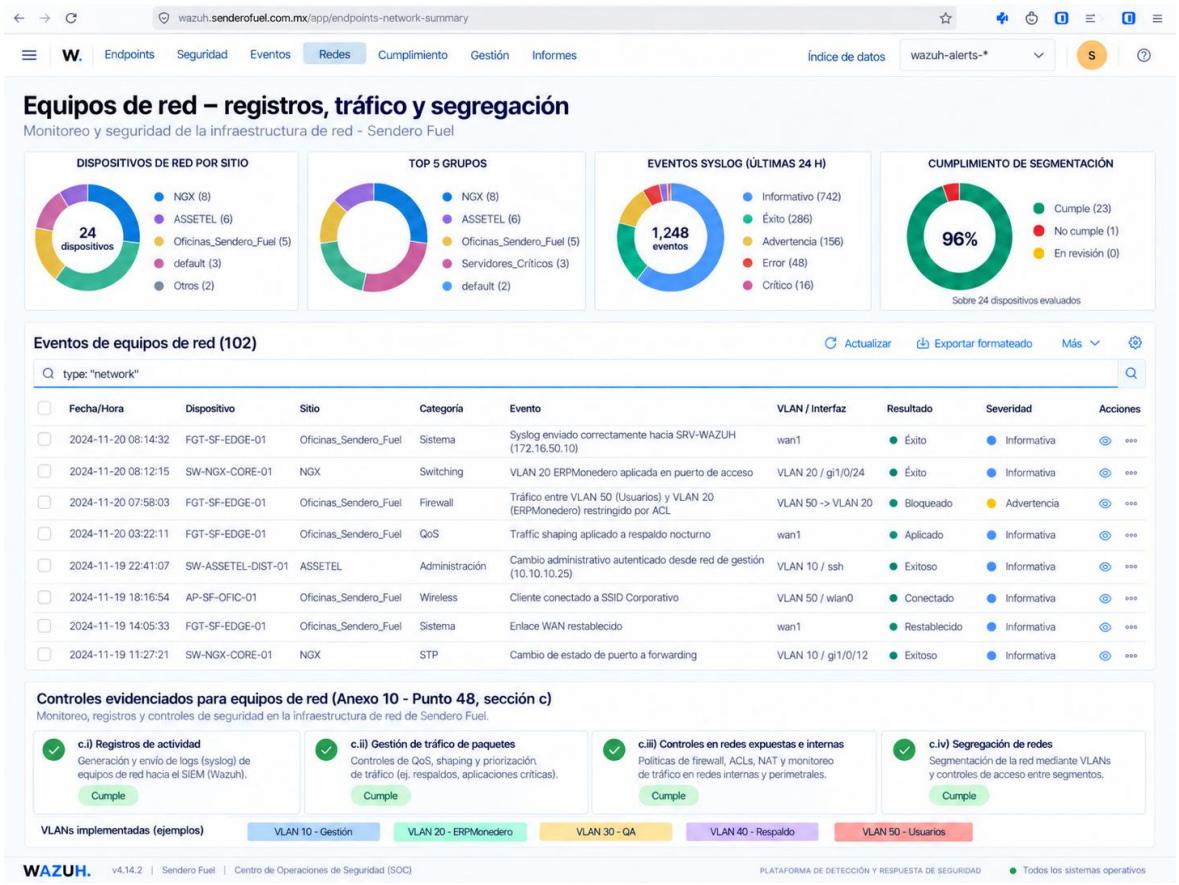
Demostrar que las funciones de seguridad del fabricante están configuradas en los activos.



Evidencia - - Controles de seguridad en HPE iLO.

7. c) Equipos de red

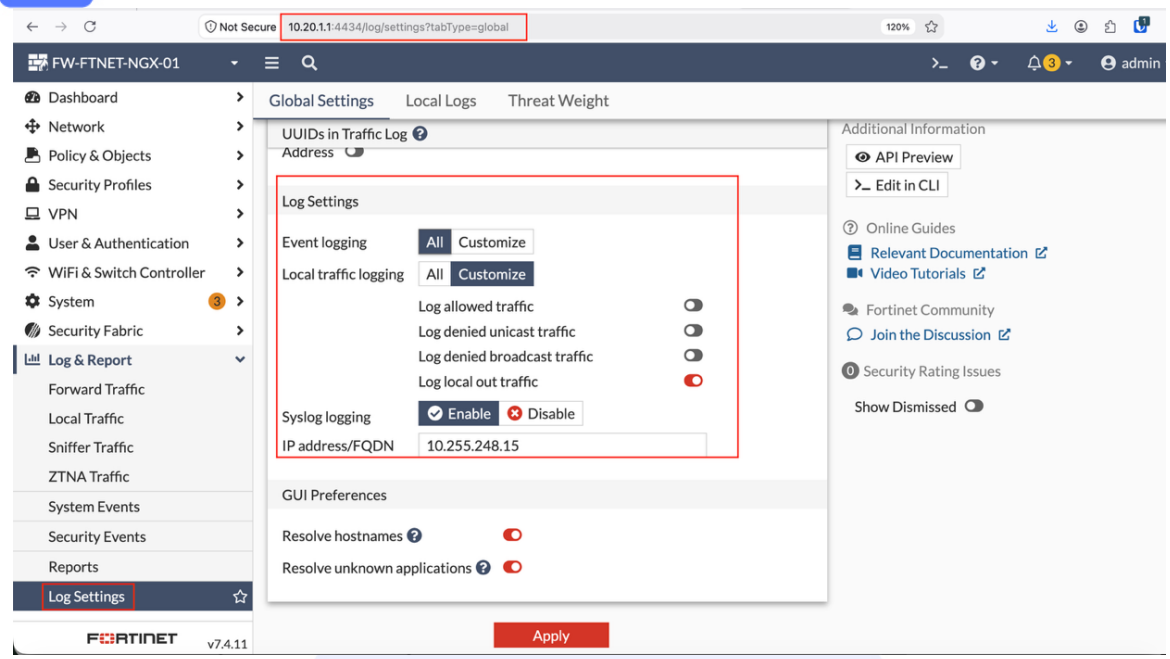
La evidencia de red se presenta en el orden c.i a c.iv requerido por el control 48.



c.i. Configuración de registros de actividades

Requisito del control

Demostrar que equipos de red generan y envían registros de actividad a un repositorio central.

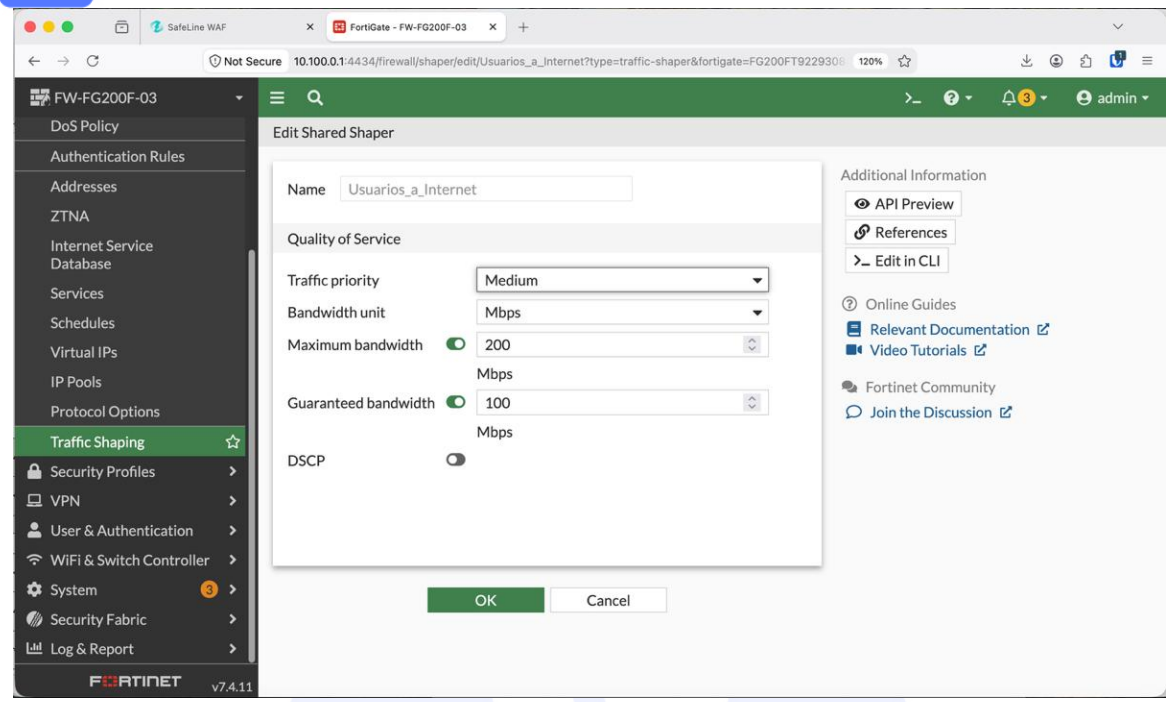


Evidencia - - Reenvío de logs/Syslog hacia SRV-WAZUH.

c.ii. Configuración de gestión de tráfico de paquetes

Requisito del control

Demostrar controles de QoS, traffic shaping, priorización o límites de tráfico.

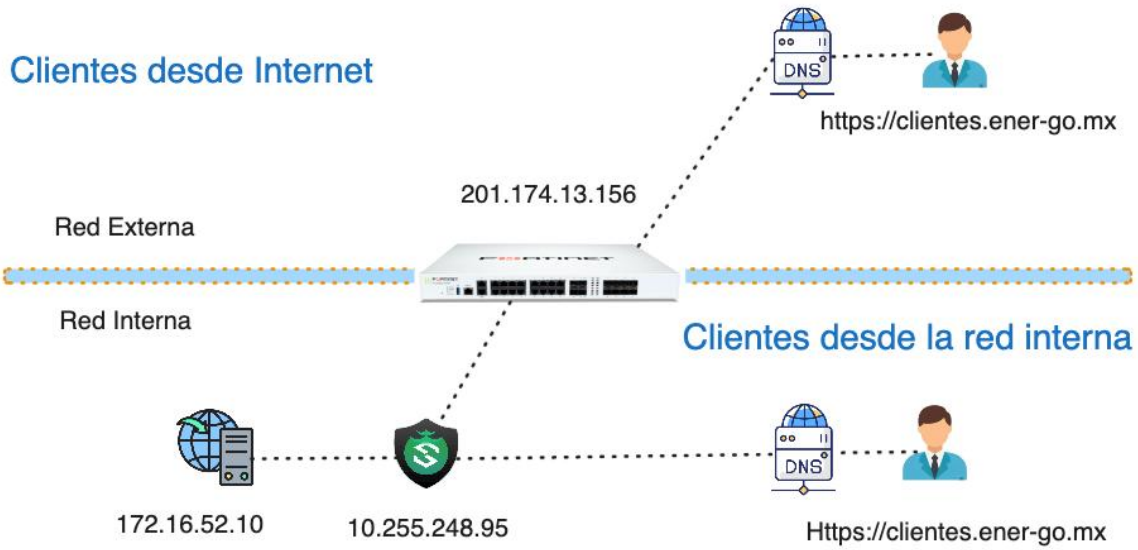


Evidencia - - Gestión de tráfico / traffic shaping.

c.iii. Controles de seguridad en redes expuestas e internas

Requisito del control

Demostrar controles perimetrales e internos en oficinas y centros de datos.



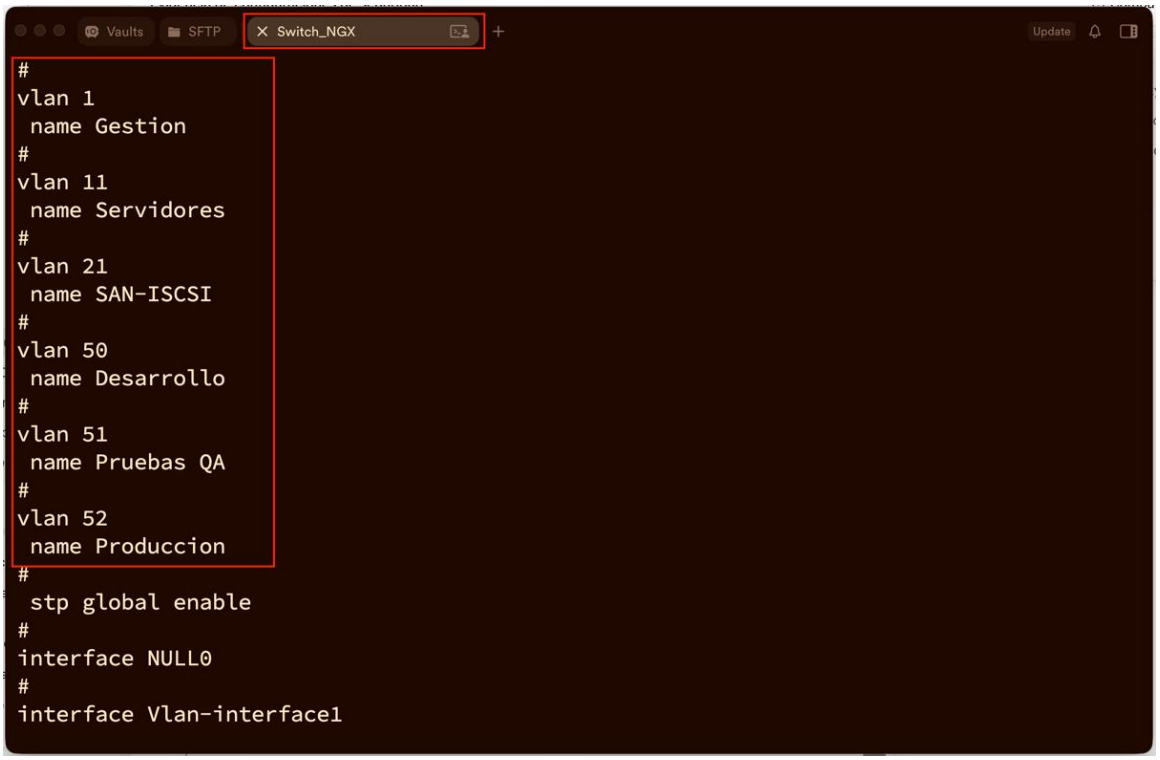
Evidencia - - Arquitectura de controles para redes expuestas e internas.

c.iv. Segregación de redes

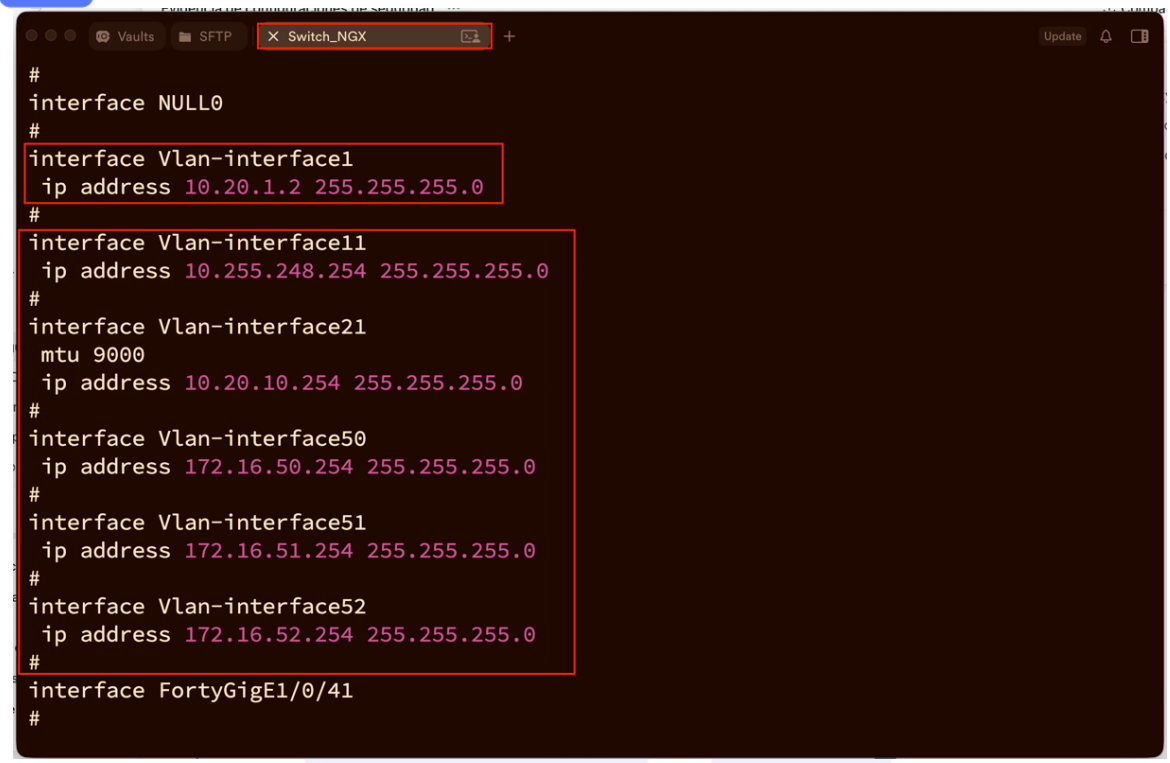
Requisito del control

Demostrar segmentación lógica mediante VLANs y controles de acceso entre segmentos.

Evidencia integrada: Configuración de VLANs de gestión, servidores, desarrollo, pruebas y producción en switch core de NGX.

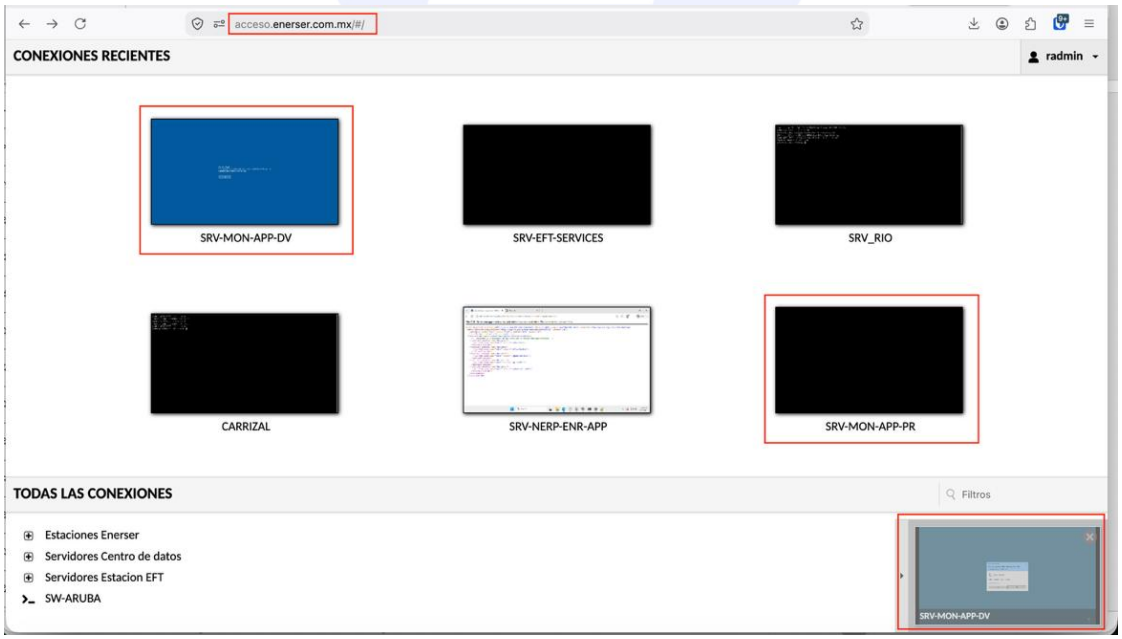


Evidencia - - VLANs configuradas en switch core.

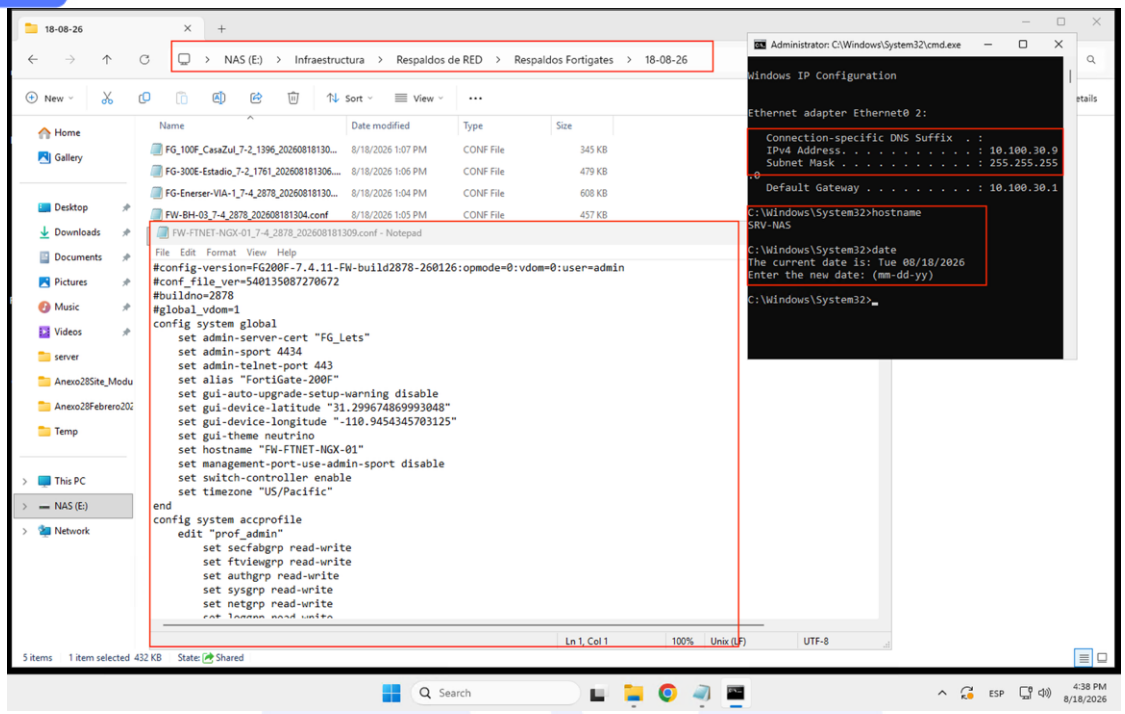


Evidencia - - Direccionamiento/configuración de interfaces VLAN.

8. Evidencia complementaria de administración y resguardo de configuración



Evidencia complementaria - Acceso administrativo mediante Apache Guacamole.



Evidencia complementaria - Repositorio de respaldos de configuración de firewalls y switches.

9. Línea base CIS L1 y automatización como soporte documental

El documento Hardening_Windows_Server_CIS_L1_Priorizado establece una línea base de 96 controles: 24 críticos, 55 altos y 17 medios, de los cuales 92 (96%) se identifican como automatizables. Este soporte no sustituye las capturas exigidas por el punto 48, pero demuestra que existe una referencia técnica formal y repetible para servidores Windows.



Hardening Windows Server — Baseline CIS L1

Hardening Windows Server

Baseline CIS L1 — Controles priorizados por severidad

Grupo Enerser · Infraestructura IT
1 de julio de 2026

Resumen ejecutivo

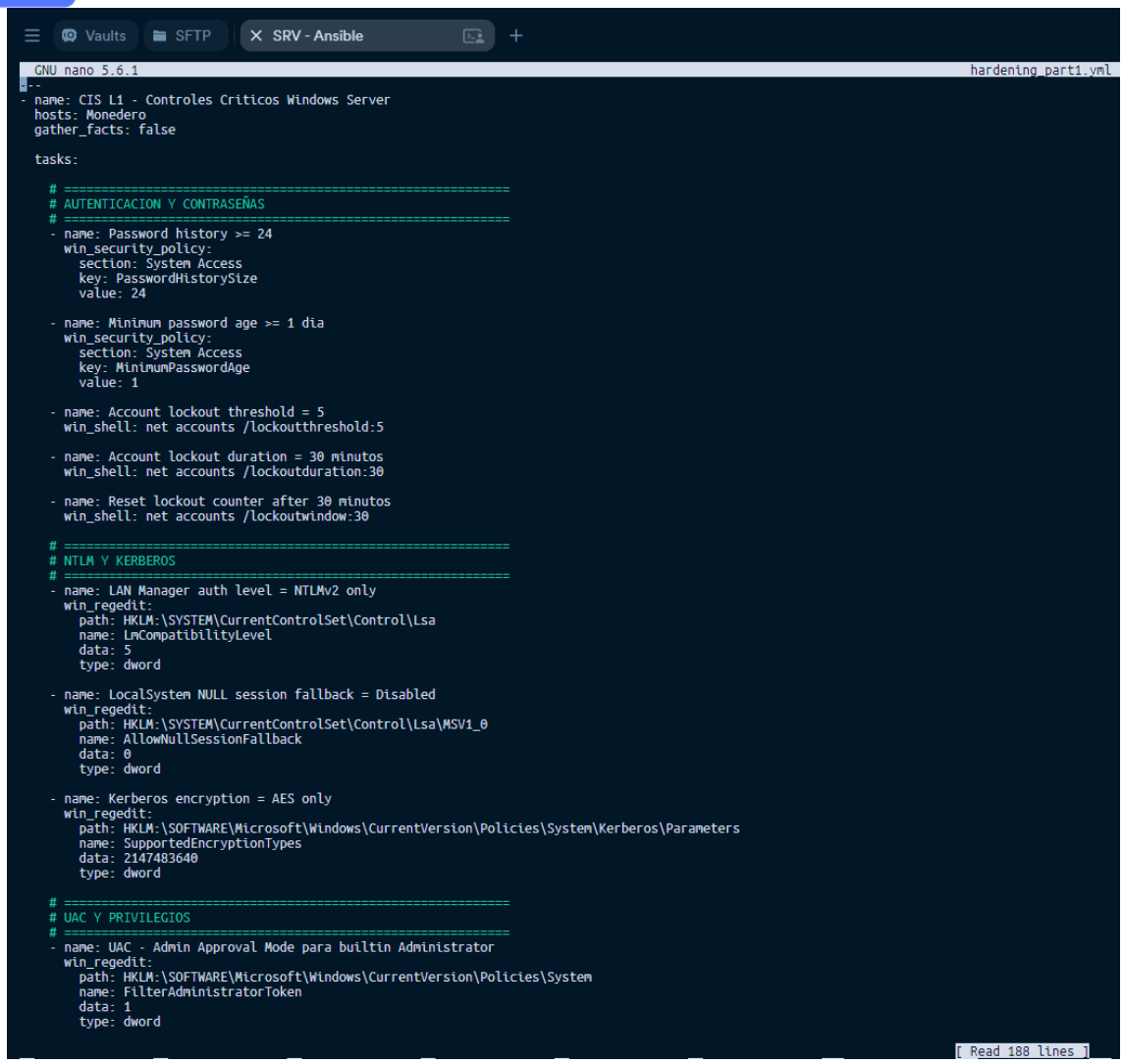
Total controles	Críticos	Alto	Medio	Automatizables Ansible
96	24	55	17	92 (96%)

Esta tabla agrupa los controles del baseline CIS L1 por categoría funcional, ordenados de mayor a menor severidad. La columna Ansible indica si el control es configurable de forma remota y automatizada (vía GPO local, registro, secedit o auditpol) o si requiere intervención manual / configuración a nivel de dominio.

Autenticación y contraseñas

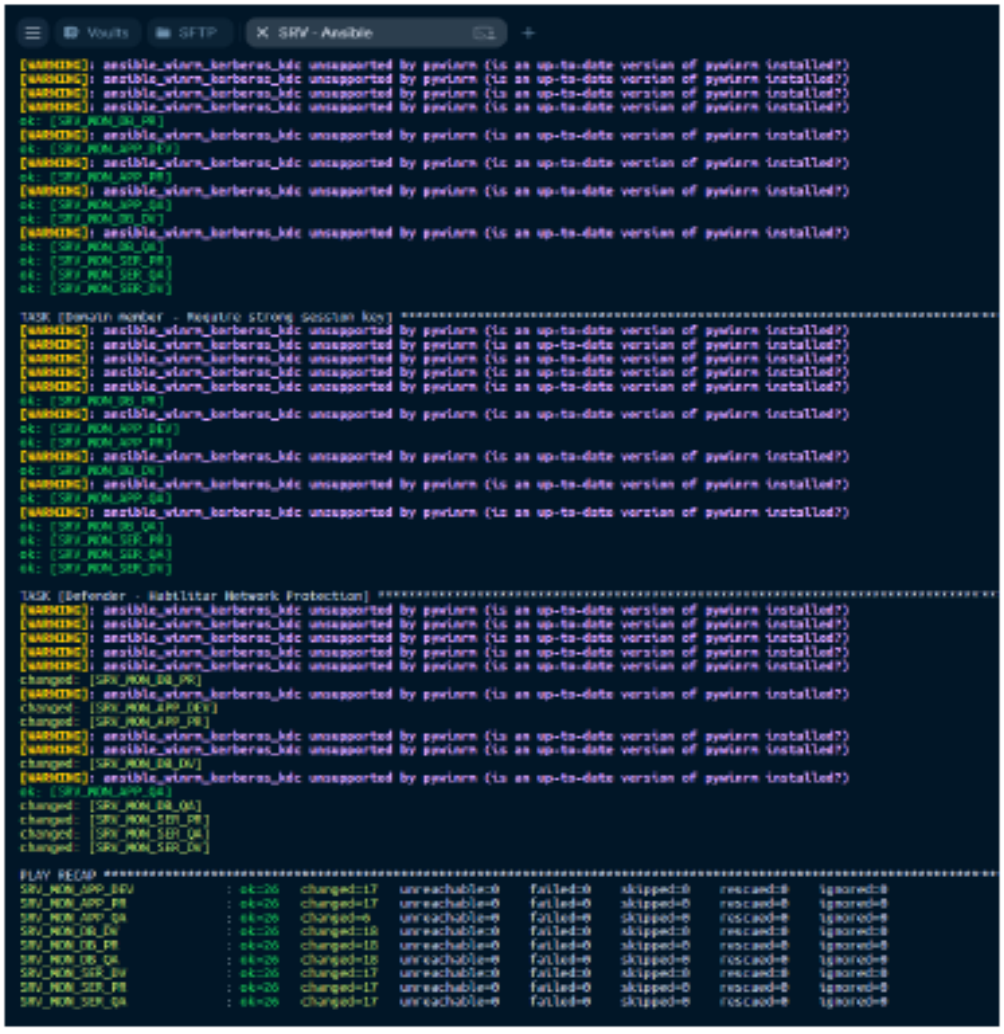
Control	Implementación técnica	Severidad	Ansible
Enforce password history ≥ 24 Impide que usuarios reciclen contraseñas recientes.	Account Policies → Password Policy HKLM\SYSTEM\CurrentControlSet\Control\Lsa (secedit)	CRÍTICO	Ansible
Account lockout threshold ≤ 5 intentos (no 0)	Account Policies → Account Lockout Policy secedit / win_security_policy	CRÍTICO	Ansible

Evidencia - - Resumen de baseline CIS L1 priorizado para Windows Server.



Evidencia - - Playbook de Ansible para aplicación de controles de hardening.

EnerGo



Evidencia - - Resultado de ejecución del hardening sobre servidores del monedero.