# FIREWALL TOOLBOX

## Informe completo

### Detalles del dispositivo

| | |
|---|---|
| Número de serie: | 0040103CD830 |
| Nombre del firewall: | UDS-NSV270 |
| Modelo del dispositivo: | SonicWall NSv 270 |
| Tiempo de actividad: | 0 Days, 0 Hours, 22 Minutes, 15 Seconds |
| Versión de firmware: | 7.3.0-7012-R8150 |

### Detalles del informe

| | |
|---|---|
| Creado el: | 15.09.2026 16:37:00 |
| Archivo EXP: | C:\Us...ox\Repository\0040103CD830\exp_api_downloaded.exp |
| Marca de tiempo EXP: | 15.09.2026 16:33:48 |
| Archivo TSR: | C:\Us...ox\Repository\0040103CD830\tsr_api_downloaded.wri |
| Marca de tiempo TSR: | 15.09.2026 16:33:49 |

### Información adicional

*- IPv6 está deshabilitado. Los informes relacionados con IPv6 no están incluidos*

*- Las reglas añadidas automáticamente se excluyen de este informe*

## Índice

## Explicación

**Alineación de la configuración con las mejores prácticas**


Este informe evalúa la configuración actual del firewall SonicWall en función de las recomendaciones de mejores prácticas establecidas. Su propósito es identificar la configuración que ya se ajusta a los estándares operativos y de seguridad, al tiempo que destaca las áreas en las que podrían ser recomendables mejoras. La evaluación tiene como objetivo respaldar una revisión estructurada de la configuración del dispositivo en materia de seguridad, mantenibilidad, resiliencia y fiabilidad general del servicio.

Una configuración de firewall bien alineada ayuda a reducir el riesgo operativo, simplifica la administración y mejora la transparencia durante las actividades de soporte y auditoría. Además de los controles de seguridad técnicos, la alineación con las mejores prácticas también incluye la coherencia de la configuración, una identificación clara del dispositivo y la eliminación de configuraciones innecesarias u obsoletas. Por lo tanto, cada sección revisada en este informe está diseñada para proporcionar tanto una indicación del estado como una breve explicación de por qué el elemento evaluado es relevante desde una perspectiva operativa o de seguridad.

Se presta especial atención al estado del software y del firmware del firewall. El informe comprueba si el firmware actualmente instalado está actualizado y si se han detectado indicios de un downgrade de firmware no compatible. Esto es importante porque un firmware obsoleto puede exponer al dispositivo a problemas conocidos, mientras que los escenarios de downgrade no compatibles pueden afectar la estabilidad, la compatibilidad y el soporte del proveedor. Por lo tanto, un estado de firmware conforme es un requisito clave para un funcionamiento seguro y fiable.

El informe también revisa si IPv6 está habilitado y si su uso parece apropiado para el entorno. Si no se requiere IPv6, generalmente debería deshabilitarse para reducir la superficie de ataque innecesaria y la complejidad administrativa. De la misma manera, el informe evalúa si la alta disponibilidad está habilitada. Cuando la alta disponibilidad no está en uso, se recomienda encarecidamente su implementación, ya que mejora la resiliencia y reduce el tiempo de inactividad en caso de fallo de hardware o mantenimiento planificado.

Otra área importante es la redundancia de conectividad. Se revisa la configuración para determinar si hay disponibles varias conexiones WAN. Si solo se utiliza un único enlace ascendente WAN, se recomienda encarecidamente una conexión WAN adicional para mejorar la redundancia y mantener la conectividad a Internet durante interrupciones del proveedor. También se consideran configuraciones de optimización relacionadas con la WAN, como la MTU. Si la MTU de la WAN parece configurada de forma inusualmente baja, esto debería revisarse, ya que valores de MTU innecesariamente bajos pueden reducir la eficiencia de transmisión y afectar negativamente al rendimiento.

Desde una perspectiva de seguridad, el informe incluye comprobaciones relacionadas con la protección de cuentas de usuario, el fortalecimiento de VPN y las capacidades de defensa contra amenazas. Evalúa si las cuentas administrativas están protegidas mediante autenticación de dos factores, algo muy recomendado para reducir el riesgo de acceso no autorizado mediante credenciales débiles, reutilizadas o comprometidas. También se revisa la configuración VPN en busca de algoritmos de cifrado obsoletos, cifrados débiles o configuraciones heredadas que puedan reducir la seguridad de las comunicaciones cifradas. Además, el informe comprueba si las funciones de detección y prevención están habilitadas, ya que estas funciones son esenciales para identificar actividad sospechosa y bloquear posibles amenazas en una etapa temprana.

La visibilidad administrativa y la disciplina operativa se abordan además mediante comprobaciones como el registro de auditoría interna y el estado de packet capture. Una función de auditoría interna habilitada es importante porque proporciona trazabilidad para los cambios de configuración y las acciones administrativas, lo que respalda la resolución de problemas, las investigaciones de seguridad y los requisitos de cumplimiento. El informe también identifica si Packet Capture sigue en ejecución. Una captura de paquetes continuamente activa puede indicar una resolución de problemas inconclusa y puede generar una sobrecarga innecesaria si se deja habilitada sin un motivo operativo válido.

Finalmente, el informe considera el estado de utilización general del firewall. Revisar la utilización general es importante para determinar si el dispositivo opera dentro de un rango de carga aceptable o se acerca a los límites de capacidad. Una utilización constantemente alta puede indicar riesgos de rendimiento y debería evaluarse más a fondo. En conjunto, los hallazgos de este informe proporcionan una visión práctica de la calidad de la configuración actual y ayudan a identificar medidas que pueden mejorar la postura de seguridad, la estabilidad operativa y la mantenibilidad a largo plazo.

## El nombre del firewall ha sido modificado

*Cambiar el nombre de un firewall SonicWall de su número de serie a un nombre de dispositivo significativo mejora la administración, la resolución de problemas y la generación de informes. Un nombre descriptivo facilita identificar de un vistazo la ubicación, el rol o la asignación de cliente del firewall, especialmente en entornos con múltiples dispositivos. Esto reduce la confusión, agiliza las actividades de soporte y disminuye el riesgo de errores de configuración u operativos.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| El nombre del firewall ha sido modificado | Estado | - |

## Firmware y configuración

*Esta sección muestra si la versión de firmware actual está en uso y si se ha detectado un downgrade de firmware no compatible. Esto permite evaluar rápidamente el estado del software e identificar posibles riesgos para el funcionamiento, la compatibilidad y el soporte.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| La versión de firmware está actualizada | actualización disponible | Actualizar firmware |

## Downgrade de firmware no compatible

*Esta es una comprobación para verificar si se ha producido un downgrade de firmware no compatible*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Downgrade de firmware no compatible | no detectado | - |

## Estado de IPv6

*Si IPv6 no es necesario en el entorno, debe deshabilitarse para reducir la superficie de ataque innecesaria y la complejidad administrativa.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Estado de IPv6 | deshabilitado | - |

## Estado de alta disponibilidad

*Si la alta disponibilidad no está habilitada, se recomienda encarecidamente su uso para mejorar la resiliencia y reducir el tiempo de inactividad en caso de fallo de hardware o mantenimiento. Ayuda a garantizar la continuidad del servicio y aumenta la disponibilidad general de la infraestructura de seguridad.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Estado de alta disponibilidad | presente | - |

## Líneas WAN redundantes

*Si solo se utiliza una única conexión WAN, se recomienda encarecidamente una línea WAN adicional para mejorar la redundancia y mantener la conectividad a Internet en caso de interrupción del proveedor. Varias conexiones WAN también aumentan la disponibilidad general y pueden admitir failover o balanceo de carga.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Líneas WAN redundantes | configurado | - |

## Configuración VPN

*Esta sección destaca posibles problemas en la configuración VPN, como algoritmos de cifrado obsoletos, cifrados débiles o configuraciones heredadas. Estos hallazgos pueden reducir la seguridad general de la conexión VPN y provocar problemas de compatibilidad, cumplimiento o soporte. Se recomienda revisar y actualizar la configuración VPN para alinearla con los estándares de seguridad y las mejores prácticas actuales.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Algoritmos VPN inseguros utilizados | sí | Reconfigurar túneles VPN |

## Auditoría interna del firewall

*Esta sección muestra si la función de auditoría interna está habilitada en el firewall SonicWall. Una función de auditoría habilitada es importante porque registra los cambios de configuración y las acciones administrativas, mejorando la trazabilidad y la responsabilidad. Esto respalda la resolución de problemas, las investigaciones de seguridad y los requisitos de cumplimiento.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Auditoría interna del firewall | habilitado | - |

## Cuenta de administrador integrada utilizada para la administración

*Si la auditoría interna está activa, esta función comprueba si se detectó el usuario Admin genérico en el registro de auditoría. Se recomienda utilizar cuentas personalizadas para la administración*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Cuenta de administrador integrada utilizada para la administración | sí | utilizar cuentas per |

## Funciones de detección y prevención

*Esta sección muestra si las funciones de detección y prevención están habilitadas en el firewall SonicWall.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Funciones de detección y prevención | habilitado | - |

## Packet Capture en ejecución

*Esta sección muestra si Packet Capture sigue en ejecución actualmente en el firewall SonicWall.*
*Una captura de paquetes continuamente activa debe revisarse, ya que puede indicar una resolución de problemas inconclusa y puede consumir recursos del sistema o generar datos de captura innecesarios.*
*Si ya no es necesaria, debe detenerse para evitar una sobrecarga innecesaria y un impacto operativo.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Packet Capture en ejecución | no | - |

## Protección de cuentas

*Esta sección muestra si las cuentas de usuario en el firewall SonicWall están protegidas con autenticación de dos factores (2FA).*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Cuenta Admin protegida con TOTP | no | Habilitar servicio o función |
| Cuentas de usuario protegidas con TOTP | no | Habilitar servicio o función |

## Utilización del firewall

*La supervisión de la utilización general es importante para identificar condiciones de carga elevada que puedan afectar al rendimiento, la estabilidad o la eficacia de los servicios de seguridad.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Utilización del último minuto | 0 % | OK |
| Utilización de la última hora | 0 % | OK |
| Utilización del último día | 0 % | OK |
| Utilización del último día | 0 % | OK |

## Servicios de seguridad con licencia pero no utilizados

*Este informe muestra el número de servicios de seguridad que tienen licencia pero no están en uso*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Número de servicios | 1 | Habilitar servicio o función |

## Servicio de seguridad no activado

*Habilitar un servicio de seguridad en una zona mientras el propio servicio está deshabilitado globalmente no proporciona ninguna protección efectiva. Aunque la configuración de la zona indica que el servicio está activo, el motor subyacente no se está ejecutando, por lo que no se realiza ninguna inspección ni filtrado. Esto puede crear una falsa sensación de seguridad y provocar políticas de firewall mal configuradas.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Servicio de seguridad no activado | sí | Habilitar servicio o función |

## Configuración WAN MTU

*Una MTU WAN configurada correctamente es importante para garantizar una transmisión eficiente de paquetes y una comunicación de red estable. Si el valor de MTU está configurado demasiado bajo, puede reducir el rendimiento, aumentar la sobrecarga y afectar negativamente al rendimiento de las aplicaciones o conexiones VPN.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| Se detectó un tamaño de MTU WAN bajo | no detectado | - |

## Tiempo de espera de conexión TCP

*Cambiar el tiempo de espera TCP global afecta a todas las sesiones TCP procesadas por el firewall. Generalmente se recomienda dejar el valor predeterminado sin cambios y ajustar los tiempos de espera solo para reglas de acceso individuales cuando sea necesario.*

| Función - Configuración | Estado | Recomendación |
|---|---|---|
| l tiempo de espera TCP predeterminado ha | sido modificadono detectado | - |

## Reglas de firewall no utilizadas durante mucho tiempo

*Las reglas que actualmente no están en uso no aportan valor operativo. Para mantener el marco claro y eficiente, estas reglas no utilizadas deben reevaluarse y, cuando proceda, eliminarse*

| Tipo de regla | Número de ocurrencias |
|---|---|
| Reglas de firewall nunca utilizadas (IP v4) | 0 |
| Reglas de firewall no utilizadas durante mucho tiempo (IP v4) | 21 |

## Reglas de firewall deshabilitadas

*Las reglas que actualmente no están en uso no aportan valor operativo. Para mantener el marco claro y eficiente, estas reglas no utilizadas deben reevaluarse y, cuando proceda, eliminarse*

| Tipo de regla | Número de ocurrencias |
|---|---|
| Reglas de firewall deshabilitadas (IP v4) | 0 |

## Reglas de firewall que permiten el acceso desde la WAN a redes internas

*Las reglas de firewall que permiten el acceso desde la WAN a la red interna aumentan la exposición y deben restringirse solo a los servicios esenciales, validando regularmente la necesidad empresarial*

| Tipo de regla | Número de ocurrencias |
|---|---|
| Reglas de firewall que permiten el acceso desde la WAN a redes internas (IP v4) | 0 |

## Reglas ANY <> ANY

*Las reglas que permiten cualquier origen hacia cualquier destino en cualquier puerto crean una exposición excesiva y deben evitarse a menos que exista una necesidad empresarial claramente justificada y documentada.*

| Tipo de regla | Número de ocurrencias |
|---|---|
| Reglas ANY <> ANY (IP v4) | 0 |

## Reglas que permiten el acceso de administración

*Las reglas que permiten el acceso de administración deben limitarse estrictamente a fuentes autorizadas y servicios protegidos, ya que presentan un alto riesgo si se exponen demasiado ampliamente.*

| Tipo de regla | Número de ocurrencias |
|---|---|
| Reglas que permiten el acceso de administración (IP v4) | 4 |

## Políticas NAT no utilizadas

*Las políticas NAT no utilizadas no cumplen ninguna función activa y deben revisarse periódicamente para determinar si siguen siendo necesarias o pueden eliminarse.*

| Tipo de regla | Número de ocurrencias |
|---|---|
| Políticas NAT no utilizadas (IP v4) | 0 |

## Políticas NAT deshabilitadas

*Las políticas NAT no utilizadas no cumplen ninguna función activa y deben revisarse periódicamente para determinar si siguen siendo necesarias o pueden eliminarse.*

| Tipo de regla | Número de ocurrencias |
|---|---|
| Políticas NAT deshabilitadas (IP v4) | 0 |

## Información adicional

*- Las reglas añadidas automáticamente se excluyen de este informe*


# Informe de seguridad

## Explicación

La auditoría de seguridad se centra en identificar posibles riesgos de seguridad y debilidades en las políticas. Analiza las reglas de firewall en busca de configuraciones excesivamente permisivas, detecta objetos no utilizados o riesgosos, y revisa los privilegios de usuario y los derechos de acceso. El objetivo es destacar configuraciones incorrectas que podrían ser explotadas o que infringen las mejores prácticas, proporcionando información práctica para mejorar la postura de seguridad general.

# Informe de configuración de auditoría

## Explicación

**Auditoría interna del firewall**
*La auditoría interna en los firewalls es un componente esencial para mantener la integridad operativa, la responsabilidad y la seguridad dentro de un entorno de red. El firewall representa uno de los puntos de control más críticos en una organización, y la auditoría proporciona visibilidad sobre los cambios de configuración, los eventos de acceso y las acciones administrativas que influyen directamente en la postura de seguridad de la red.*

**Responsabilidad y trazabilidad**
*Los registros de auditoría documentan quién realizó los cambios, cuándo se realizaron y qué se modificó. Esta trazabilidad garantiza que las responsabilidades se asignen claramente y que cualquier configuración incorrecta, desviación de los estándares o cambio no autorizado pueda identificarse y corregirse rápidamente.*

**Detección de modificaciones no autorizadas o riesgosas**
*Los firewalls afectan directamente al control de acceso, la protección de datos y el flujo de tráfico. La auditoría interna permite a los administradores detectar cambios de configuración intencionados o accidentales, ayudando a identificar incidentes de seguridad, violaciones de políticas o posibles usos indebidos de privilegios administrativos.*

**Apoyo al cumplimiento normativo y la gobernanza**
*Muchos marcos regulatorios exigen la auditoría de sistemas críticos como los firewalls. Los registros de auditoría interna respaldan el cumplimiento de estándares relevantes para sectores como finanzas, salud y gobierno. Proporcionan prueba de que se siguen las políticas y de que los mecanismos de protección se aplican correctamente.*

**Perspectiva operativa y mejora continua**
*Los registros de auditoría ayudan a los equipos de seguridad a comprender el historial de configuración y las tendencias operativas. La revisión periódica de estos registros permite a las organizaciones perfeccionar las políticas de acceso, identificar problemas recurrentes y fortalecer las prácticas de gestión de cambios.*

**Investigación de incidentes y análisis forense**
*Cuando ocurre un evento de seguridad, los datos de auditoría interna suelen ser una de las fuentes de evidencia más valiosas. Permiten a los investigadores reconstruir las acciones realizadas en el firewall, analizar las causas raíz y determinar si la actividad maliciosa o el error humano contribuyeron al incidente.*

**Conclusión**
*La auditoría interna es necesaria para garantizar la transparencia, la coherencia y la responsabilidad en las operaciones del firewall. Mejora la seguridad, respalda los requisitos normativos, permite una resolución de problemas más rápida y proporciona una base clave para una gestión de red resiliente.*

# Informe de configuración de auditoría

## Audit Details

Auditoría interna: on

Registros de auditoría encontrados en el informe TS:2000

Entrada de auditoría más reciente encontrada en el informe TS:15.09.2026 16:33:49

Entrada de auditoría más antigua encontrada en el informe TS27.07.2026 08:29:20

## Usuarios identificados en el registro de auditoría

- UDSAdmin
- admin
- apiuser
- HA Sync

## Información adicional

**Uso de una cuenta de administrador genérica**

Se ha detectado la cuenta de usuario *"admin"* en los registros de auditoría. Se recomienda evitar el uso de cuentas de administrador genéricas o compartidas para la administración del firewall. En su lugar, cada administrador debería iniciar sesión utilizando una cuenta personalizada.

El uso de identidades de usuario individuales garantiza que los cambios de configuración puedan rastrearse

**Comentario**
La cuenta *HA Sync* es un usuario interno del sistema utilizado exclusivamente para sincronizar datos de configuración y operativos entre dispositivos en una configuración de alta disponibilidad (HA). Esta cuenta no está destinada al inicio de sesión manual ni al uso administrativo.

# Informe de reglas con DPI SSL deshabilitado

## Explicación

Reglas con Deep Packet Inspection desactivada
La Deep Packet Inspection (DPI) permite al firewall analizar el tráfico más allá de la información básica de conexión, como el origen, el destino y el puerto. Es un requisito importante para aplicar servicios de seguridad y detectar amenazas en el tráfico de red.
Este informe identifica las reglas de acceso para las que Deep Packet Inspection está desactivada. El tráfico que coincide con estas reglas puede eludir la inspección basada en DPI y, por lo tanto, podría no beneficiarse de todos los servicios de seguridad configurados.
La desactivación de DPI puede ser apropiada para determinados tipos de tráfico, por ejemplo, debido a requisitos de compatibilidad, consideraciones de rendimiento o porque el tráfico correspondiente no requiere una inspección adicional. Sin embargo, DPI normalmente solo debería desactivarse de forma intencionada y por un motivo documentado.
Revise las reglas enumeradas en este informe y compruebe que la desactivación de DPI sea necesaria. Si no existe un motivo específico, considere activar DPI para garantizar que el tráfico reciba el nivel de inspección de seguridad previsto.

## Reglas en las que la inspección Client DPI SSL está desactivada



| Ena | A | Name | SrcZone | DstZone | SrcNet | DstNet | SrcSvc | DstSvc | DPI Disabled |
|---|---|---|---|---|---|---|---|---|---|
| YES | A | Allow WAN1 | LAN | WAN | KlausMeier | any | any | any | True |
| YES | A | Heating Maintenance | WAN | LAN | any | LAN Subnets | any | SSH | True |

*- Las reglas añadidas automáticamente se excluyen de este informe*

*Número de registros: 2*

## Descifrado DPI-SSL de cliente

### Explicación

La inspección Client DPI-SSL es una función de seguridad clave que permite al firewall inspeccionar el tráfico HTTPS saliente cifrado. Sin descifrado, los servicios de seguridad como Gateway Anti-Virus, Intrusion Prevention, Capture ATP, Content Filtering y Application Control tienen una visibilidad limitada de las conexiones cifradas, lo que puede permitir que las amenazas eludan la inspección.
Este informe verifica si la inspección Client DPI-SSL está licenciada y habilitada en el firewall. También identifica las zonas en las que la inspección de cliente está activa y destaca cualquier regla de acceso en la que DPI-SSL se haya deshabilitado explícitamente. Las excepciones a nivel de regla deben revisarse cuidadosamente, ya que pueden crear puntos ciegos en los que el tráfico cifrado no se inspecciona y los servicios de seguridad no pueden aplicarse por completo.
Las organizaciones deben garantizar que la inspección Client DPI-SSL esté habilitada donde corresponda y que las excepciones se limiten a aplicaciones o servicios con requisitos de compatibilidad documentados. La revisión periódica de la configuración de DPI-SSL ayuda a mantener la visibilidad del tráfico cifrado y reduce el riesgo de amenazas no detectadas.

## Descifrado DPI-SSL de cliente

```
DPI SSL Licensed:          yes
```

```
El descifrado SSL para el tráfico saliente está deshabilitado (!)
```

## Descifrado DPI-SSL de cliente



| Zone | DPI SSL Client |
|---|---|
| LAN | On |
| WAN | Off |
| DMZ | Off |
| VPN | Off |
| SSLVPN | Off |
| MULTICAST | Off |
| DMZ-unsec | Off |
| DMZ-sec | Off |
| Test | On |
| 150971-Test | Off |
| 060466 | Off |

## Reglas en las que la inspección Client DPI SSL está desactivada



| Ena | A | Name | SrcZone | DstZone | SrcNet | DstNet | SrcSvc | DstSvc | DPI-SSL Client Disabled |
|---|---|---|---|---|---|---|---|---|---|
| YES | A | Heating Maintenance | WAN | LAN | any | LAN Subnets | any | SSH | True |
| YES | A | Complicated Rule | DMZ-unsec | Test | any | any | Citrix UDP | any | True |
| YES | A | Rule6 | DMZ-sec | Test | any | Test13 | Citrix TCP | any | True |

*- Las reglas añadidas automáticamente se excluyen de este informe*

*Número de registros: 3*

## Funciones de detección y prevención

### Explicación

Las opciones Randomize IP ID y Enable Stealth Mode proporcionan protección adicional contra el reconocimiento de red y ciertas clases de ataques. Aleatorizar el campo IP Identification dificulta que los atacantes realicen fingerprinting del sistema operativo o deduzcan patrones de tráfico, mientras que el modo sigiloso (Stealth Mode) evita que el firewall responda a intentos de conexión no solicitados, reduciendo su visibilidad en redes no confiables.

## Funciones de detección y prevención

### Modo sigiloso (Stealth Mode)

| | |
|---|---|
| Modo sigiloso activado | on |

### Randomize IP ID

| | |
|---|---|
| Randomize IP ID activado | on |

## Reglas que permiten cualquier destino y cualquier puerto (IPv4)

### Explicación

**Por qué las reglas de firewall que permiten "Any" son riesgosas**
*En el ámbito de la seguridad de red, las reglas de firewall desempeñan un papel fundamental en el control del tráfico entrante y saliente de una red. Una práctica común, aunque muy desaconsejada, es la implementación de reglas "de cualquiera a cualquiera". Estas reglas permiten un flujo de tráfico sin restricciones desde cualquier origen a cualquier destino, permitiendo básicamente que todo tipo de paquetes de datos pasen a través del firewall sin ningún filtrado.*

**Implicaciones de seguridad** *La principal preocupación con las reglas "de cualquiera a cualquiera" es el importante riesgo de seguridad que representan. Los firewalls están diseñados para actuar como guardianes, examinando el tráfico entrante y saliente para proteger la red de accesos no autorizados, ciberataques y otras actividades maliciosas. Al establecer reglas que permiten indiscriminadamente todo el tráfico, se elude la función esencial del firewall, exponiendo la red a posibles amenazas. Esta puerta abierta puede ser explotada por atacantes para acceder a información sensible, inyectar malware o lanzar otros exploits perjudiciales.*

**Falta de control del tráfico** *Además de las vulnerabilidades de seguridad, las reglas "de cualquiera a cualquiera" dificultan la capacidad de supervisar y controlar eficazmente el tráfico de red. Una gestión de red eficaz depende de comprender y gestionar el flujo de datos. Las reglas sin restricciones dificultan el seguimiento, el análisis o la priorización del tráfico, lo que puede provocar problemas de rendimiento de red, incluida la congestión del ancho de banda y una menor eficiencia.*

**Cumplimiento normativo y mejores prácticas** *En muchos sectores, los requisitos normativos exigen un control y una supervisión estrictos del tráfico de datos. Las reglas "de cualquiera a cualquiera" pueden infringir los estándares de cumplimiento, provocando repercusiones legales y de reputación. Además, las mejores prácticas de ciberseguridad abogan por un principio de mínimo privilegio, en el que solo se permite el tráfico necesario, lo que subraya aún más lo desaconsejable de este tipo de reglas permisivas.*

**Recomendación** *En lugar de adoptar reglas "de cualquiera a cualquiera", se recomienda implementar reglas de firewall específicas y bien definidas basadas en el principio de mínimo privilegio. Estas reglas deben adaptarse para permitir únicamente el tráfico necesario y legítimo requerido para las operaciones comerciales, garantizando tanto la seguridad de la red como un rendimiento óptimo.*

## Reglas que permiten cualquier destino y cualquier puerto (IPv4)



| Ena | A | Name | SrcZone | DstZone | SrcNet | DstNet | SrcSvc | DstSvc | |
|---|---|---|---|---|---|---|---|---|---|
| YES | A | Allow WAN1 | DMZ-sec | WAN | any | any | Enhanced TV | any | |
| YES | A | Complicated Rule | DMZ-unsec | Test | any | any | Citrix UDP | any | |
| YES | A | Allow WAN1 | DMZ-unsec | WAN | any | any | Citrix UDP | any | |
| YES | A | Allow Citrix | any | | any | any | Citrix UDP | any | Example any<> any |
| YES | A | Allow FTP | any | | any | any | FTP | any | |

*- Las reglas añadidas automáticamente se excluyen de este informe*

*Número de registros: 5*

# Reglas de firewall que permiten servicios de administración desde redes no confiables (IPv4)

## Explicación

**Reglas de firewall que permiten servicios de administración desde redes no confiables**
Los servicios de administración como SSH (Secure Shell), HTTPS (Hypertext Transfer Protocol Secure) e interfaces de administración similares están destinados al acceso privilegiado. Permitirlos directamente desde redes no confiables introduce múltiples problemas de seguridad.

**Por qué estas reglas son riesgosas:**
**Exposición a ataques**
Permitir el acceso a los servicios de administración a través de Internet los expone a ataques como intentos de inicio de sesión por fuerza bruta, explotación de vulnerabilidades de software o ataques de denegación de servicio dirigidos al servicio.

**Elevación de privilegios**
Si un atacante logra conectarse a un servicio de administración, podría obtener acceso a nivel de administrador. Esto podría permitirle modificar las configuraciones del firewall, crear mecanismos de acceso persistentes o interrumpir la comunicación de red.

**Interceptación y espionaje (sniffing)**
Los protocolos de administración no cifrados pueden permitir que los atacantes intercepten información sensible. Incluso los servicios cifrados pueden estar en riesgo si las claves están expuestas, se utiliza cifrado obsoleto o existen fallos de implementación.

**Falta de monitoreo**
Las interfaces de administración a menudo no se supervisan tan a fondo como los sistemas orientados al usuario, lo que aumenta la probabilidad de que el acceso no autorizado pase desapercibido.

**Complejidad y error humano**
Cuantos más servicios se exponen externamente, mayor es el riesgo de errores de configuración o errores operativos, que pueden provocar la exposición accidental de sistemas críticos.

**Mejores prácticas recomendadas**
El acceso de administración debe limitarse estrictamente a redes internas confiables. Si se requiere administración remota, debe realizarse a través de canales de acceso seguros, como conexiones VPN con cifrado fuerte. Debe implementarse la autenticación multifactor siempre que sea posible, los servicios de administración deben supervisarse activamente para detectar intentos de acceso no autorizado, y los dispositivos deben mantenerse actualizados con los parches actuales para mitigar vulnerabilidades conocidas.

## Reglas de firewall que permiten servicios de administración desde redes no confiables (IPv4)



| Ena | A | Name | SrcZone | DstZone | SrcNet | DstNet | SrcSvc | DstSvc | |
|---|---|---|---|---|---|---|---|---|---|
| YES | A | Test 24 | WAN | 060466 | any | any | any | OSPF | |
| YES | A | Test 25 | WAN | 060466 | any | any | any | POP3 (Retrieve E-Mail) | |
| YES | A | Test 23 | WAN | 060466 | any | any | any | MSN | |
| YES | A | Heating Maintenance | WAN | LAN | any | LAN Subnets | any | SSH | Temp, Rule to allow M... |

*- Las reglas añadidas automáticamente se excluyen de este informe*

*Número de registros: 4*

## Opciones de acceso de administración

### Explicación

**Opciones de acceso de administración y consideraciones de seguridad**

*Existen varios métodos disponibles para acceder a la administración del firewall, cada uno con distintas ventajas de usabilidad e implicaciones de seguridad. Dado que las interfaces de administración del firewall proporcionan control administrativo sobre infraestructura de red crítica, una exposición inadecuada de estos métodos de acceso puede introducir un riesgo significativo.*

*El acceso no autorizado a la administración del firewall puede resultar en la manipulación de la configuración, la divulgación de parámetros de seguridad sensibles o incluso el compromiso total del entorno de red. Por esta razón, es esencial revisar periódicamente qué mecanismos de acceso de administración están habilitados y garantizar que solo permanezcan accesibles métodos seguros, justificados y adecuadamente protegidos.*

*Restringir el acceso de administración a redes confiables, aplicar una autenticación fuerte y supervisar la actividad administrativa son prácticas clave para mantener un panorama de configuración seguro y controlado.*

## Opciones de acceso de administración

### Central Management

| | |
|---|---|
| Central Management (NSM / GMS): | off |
| NSM ZeroTouch: | enabled |

### SSL-VPN

| | |
|---|---|
| SSL VPN Web Management: | on |
| SSL VPN SSH Management: | off |

### API

| | |
|---|---|
| API access: | enabled |

## Opciones de acceso de administración: Gestión de interfaces



| Interface | Zone | HTTP | HTTPS | PING | SSH | SNMP | API |
|---|---|---|---|---|---|---|---|
| X0 | LAN | off | on | on | on | on | on |
| X1 | WAN | off | on | on | on | off | on |
| X2 | DMZ-unsec | off | on | on | off | off | on |
| X3 | DMZ-sec | off | on | on | off | off | on |
| X4 | HA Data & Control | off | off | off | off | off | off |
| X5 | WAN | off | off | on | off | off | off |
| X6 | LAN | off | on | on | off | off | on |
| X7 | DMZ-sec | off | off | off | off | off | off |
| X6:V100 | LAN | off | off | off | off | off | off |

## Opciones de acceso de administración: IPSec (VPN)



| Tunnel-Name | Enabled | HTTP | HTTPS | SSH | SNMP |
|---|---|---|---|---|---|
| WAN GroupVPN | False | off | off | off | off |
| SNWL Policy Mode | False | off | on | on | on |
| Test | False | off | off | off | off |
| Bad Tunnel | False | off | off | off | off |
| To TZ570 | True | off | off | off | off |
| Remote Site1 | True | off | off | off | off |
| New York | True | off | off | off | off |

# Servicios de seguridad - Resumen activados y desactivados

## Explicación

**Servicios de seguridad activos**
*Este informe muestra qué servicios de seguridad están actualmente habilitados en el dispositivo. Sin embargo, la activación a nivel de sistema solo indica que la funcionalidad del servicio está disponible; no garantiza que el tráfico se esté inspeccionando realmente.*

*Para analizar eficazmente el tráfico, los servicios de seguridad también deben asignarse explícitamente a zonas o aplicarse a reglas de firewall específicas. Sin este paso de configuración, las tecnologías habilitadas pueden permanecer inactivas para los flujos de red relevantes, lo que reduce la cobertura de protección.*

## Estado del servicio de seguridad

| | |
|---|---|
| Deep Packet Inspection for SSL (DPI-SSL) | Off |
| Gateway AV | On |
| Anti-Spyware | On |
| Intrusion Prevention | On |
| App Control | On |
| Content Filtering Service | On |
| GeoIP Filtering | On |

## Información adicional

**No hay ningún túnel VPN de tipo "route-all" configurado**

Actualmente no hay ningún túnel VPN de enrutamiento total (route-all) configurado y activo. Este es un escenario común en entornos donde todo el tráfico se reenvía a un dispositivo de seguridad ascendente, responsable de la inspección del tráfico, la aplicación de políticas y el procesamiento de seguridad adicional.

En estas configuraciones, el firewall funciona principalmente como un dispositivo de enrutamiento o segmentación, mientras que la inspección más profunda la gestiona una solución de seguridad centralizada, como una puerta de enlace web segura, un servicio de seguridad en la nube o una plataforma de inspección dedicada.

# Servicios de seguridad - Asignación por zona

## Explicación

**Servicios de seguridad**
Este informe muestra qué servicios de seguridad están habilitados en cada zona. Si bien habilitar un servicio globalmente pone su funcionalidad a disposición, la protección real solo se aplica si el servicio está asignado activamente a nivel de zona.

Los servicios de seguridad vinculados a zonas determinan qué segmentos de red reciben inspección frente a amenazas como malware, intentos de intrusión o contenido no deseado. Las zonas sin las asignaciones de servicio correspondientes pueden permanecer insuficientemente protegidas, incluso si la función está habilitada en el sistema.

Esta visión general ayuda a identificar brechas de cobertura, verificar que las zonas críticas (como el LAN o las áreas de acceso VPN) estén adecuadamente protegidas, y garantizar que las políticas de inspección se alineen con los requisitos de seguridad de la organización.

## Información adicional

Los servicios de seguridad marcados con (!) están habilitados en la zona pero deshabilitados globalmente.

## Servicios de seguridad - Asignación por zona



| Zone | ClientAV | GatewayAV | IPS | AntiSpyware | DPI SSL Client | DPI SSL Server | SSLControl |
|---|---|---|---|---|---|---|---|
| LAN | Off | On | On | On | On (!) | Off | Off |
| WAN | Off | On | On | On | Off | On (!) | Off |
| DMZ | Off | Off | Off | Off | Off | Off | Off |
| VPN | Off | Off | Off | Off | Off | Off | Off |
| SSLVPN | Off | Off | Off | Off | Off | Off | Off |
| MULTICAST | Off | Off | Off | Off | Off | Off | Off |
| DMZ-unsec | Off | Off | Off | Off | Off | Off | Off |
| DMZ-sec | Off | Off | Off | Off | Off | Off | Off |
| Test | Off | On | On | On | On (!) | Off | Off |
| 150971-Test | Off | Off | Off | Off | Off | Off | Off |
| 060466 | Off | On | On | On | Off | Off | Off |

# Protección de cuentas de usuario

## Explicación

**Resumen de protección de cuentas de usuario**
Este informe enumera todas las cuentas de usuario e indica cómo están protegidas, incluyendo si la autenticación de dos factores (2FA) está habilitada. Esto ayuda a verificar la solidez de los mecanismos de autenticación e identificar cuentas que puedan requerir protección adicional.

## Protección de cuentas de usuario



| Nombre de usuario | TOTP habilitado |
|---|---|
| **admin** | **NO** |
| All LDAP Users | NO |
| apiuser | NO |
| Isabel | NO |
| LocalAdmin | YES |
| mschmitz | NO |
| Robert | NO |
| Sylvia | NO |
| Udo | NO |
| Uwe | NO |
| Webadmin | NO |

## Métodos de autenticación externa de usuarios

### Explicación

**Resumen de la configuración de autenticación externa**
*Este informe enumera qué sistemas de autenticación externa están configurados, si están habilitados, y destaca cualquier posible problema de seguridad relacionado con su configuración. La autenticación externa puede fortalecer significativamente la gestión de identidades de usuario cuando se implementa correctamente, pero una configuración incorrecta puede introducir riesgos de seguridad y operativos.*

**LDAP (Lightweight Directory Access Protocol)**
*Cuando se utiliza LDAP, las solicitudes de autenticación se reenvían a un directorio externo como Microsoft Active Directory. El uso de LDAP centraliza la identidad de usuario y la gestión de contraseñas, reduciendo la dependencia de cuentas locales. Sin embargo, la autenticación LDAP siempre debe protegerse mediante TLS (LDAPS). La comunicación LDAP no cifrada expone nombres de usuario, contraseñas e información de pertenencia a grupos a la interceptación, aumentando el riesgo de robo de credenciales.*

**Autenticación RADIUS**
*RADIUS se utiliza comúnmente para el acceso VPN y los servicios de autenticación centralizados. Admite métodos de desafío-respuesta, registro centralizado y aplicación estandarizada de políticas de autenticación. Los riesgos de seguridad surgen cuando los secretos compartidos son débiles o se reutilizan en varios sistemas. Además, si los servidores RADIUS dejan de estar disponibles, el acceso podría interrumpirse a menos que se configuren mecanismos de respaldo adecuados.*

**Autenticación TACACS+**
*TACACS+ se utiliza normalmente para la autenticación administrativa, especialmente en entornos empresariales. Separa las funciones de autenticación, autorización y contabilidad (AAA), lo que garantiza una actividad administrativa trazable y un control granular de privilegios. Aunque es seguro por diseño, TACACS+ requiere una configuración adecuada de canales cifrados y claves únicas. Las interrupciones centrales de TACACS+ pueden bloquear el acceso administrativo a menos que exista redundancia.*

*Configurar y proteger adecuadamente los sistemas de autenticación externa ayuda a mejorar la responsabilidad, reducir la complejidad de gestión y reforzar la seguridad general de acceso. La revisión periódica de la disponibilidad, la configuración de cifrado, la asignación de políticas de autenticación y el comportamiento de respaldo garantiza procesos de autenticación fiables y seguros en todo el entorno.*

### LDAP

| Server | Enabled | TLS | UserName |
|---|---|---|---|
| udsserver.uds.local | on | on | UDSReadDir |

### Radius

| Server | Enabled | VPN |
|---|---|---|
| 10.10.33.11 | off | off(!) |

### Tacacs

| Server | Enabled | VPN |
|---|---|---|
| 1.2.3.4 | off | off(!) |

## Resumen de usuarios administrativos

### Explicación

**Usuario administrativo**
*Este informe enumera a todos los usuarios que tienen privilegios administrativos. Las cuentas con derechos administrativos tienen acceso elevado a la configuración, cambios de políticas, información sensible y funciones de administración del sistema.*
*Revisar estos usuarios garantiza que solo el personal autorizado conserve el acceso privilegiado y respalda el cumplimiento normativo, la responsabilidad y las prácticas de control de acceso seguro.*

### Users with Full Admin Rights

UDSAdmin

mschmitz

Webadmin

LocalAdmin

Uwe

apiuser

UDS-SNWL-Admins@uds.local

### Users with Limited Admin Rights

- no entries -

### Users with Read-Only Admin Rights

Udo

### Users with Guest Admin Rights

Robert

Sylvia

### Información adicional

**Aviso importante sobre las asignaciones de grupos LDAP**
Si se asignan derechos administrativos a grupos LDAP, todos los miembros de esos grupos heredan automáticamente los privilegios de administrador. Esto significa que cualquier cambio en la pertenencia a LDAP -como añadir nuevos usuarios o sincronizar estructuras de directorio externas- puede conceder involuntariamente acceso elevado.

La revisión periódica de las asignaciones de grupos y su pertenencia es esencial para garantizar que solo el personal autorizado reciba privilegios administrativos y que el control de acceso permanezca alineado con las políticas de seguridad de la organización.

## Buenas prácticas para la seguridad VPN

### Explicación

**Seguridad VPN**
*Las redes privadas virtuales (VPN) son esenciales para proteger los datos a través de redes no confiables. Para seguir siendo eficaces, su configuración criptográfica debe revisarse y actualizarse periódicamente. Los métodos obsoletos debilitan la seguridad, reducen el cumplimiento normativo y exponen a las organizaciones a riesgos innecesarios.*

**Por qué son importantes las revisiones periódicas:**

**- Seguridad:**
*Las ciberamenazas evolucionan rápidamente. Los métodos antiguos de cifrado o autenticación pueden verse comprometidos con la potencia informática moderna.*
**- Cumplimiento normativo:**
*Muchos sectores requieren un cifrado fuerte para cumplir con los requisitos regulatorios.*
**- Control de acceso:**
*Una autenticación sólida impide el uso no autorizado de la VPN.*
**- Protección de datos:**
*El cifrado actualizado garantiza la confidencialidad e integridad de la información sensible.*
**- Rendimiento y preparación futura:**
*Los estándares más recientes aumentan no solo la seguridad, sino también la eficiencia y la escalabilidad.*

**Elementos inseguros que deben evitarse:**
**- Cifrados simétricos:**
*DES y 3DES son obsoletos y vulnerables.*
**- Grupos Diffie-Hellman (DH):**
*Los grupos 1 (768 bits), 2 (1024 bits) y 5 (1536 bits) son demasiado débiles.*
**- Versiones IKE:**
*IKEv1 está obsoleto; se recomienda IKEv2.*
**- Funciones hash:**
*MD5 y SHA-1 se consideran comprometidos y ya no son seguros.*
**- Gestión de claves:**
*Las claves precompartidas (PSK) débiles o estáticas son fáciles de adivinar o de vulnerar por fuerza bruta.*

**Opciones seguras recomendadas**

**- Cifrado:**
*- AES-128 o AES-256.*
**- Intercambio de claves:**
*- Grupos DH ≥ 2048 bits o Elliptic Curve Diffie-Hellman (P-256/P-384).*
**- Protocolo:**
*- IKEv2 para configuraciones VPN modernas.*
**- Integridad:**
*- SHA-256 o superior.*
**- Autenticación:**
*Preferir certificados; si se usan PSK, utilizar claves fuertes y aleatorias.*

**Conclusión**
*Las VPN son tan seguras como sus bases criptográficas. Evitando algoritmos débiles y adoptando estándares modernos, se protegen los datos sensibles, se cumplen los requisitos normativos y se prepara la red para futuros desafíos. Revise y actualice regularmente la configuración de su VPN para mantenerse seguro.*

### Explicación

(!) = inseguro © = precaución

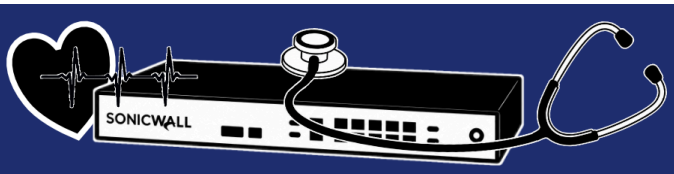
## Buenas prácticas para la seguridad VPN

| Ena | Name | Phase1 Exchange Mode | Phase1 DH-Group | Phase 1 Encr | Phase1 Auth | Phase2 Protcl | Phase2 Encr | Phase2 Auth | Phase 2 PFS | Phase 2 DH-Group |
|---|---|---|---|---|---|---|---|---|---|---|
| yes | New York | Main (!) | 224-Bit R ECP Group | AES-128 (C) | MD5 (!) | ESP | DES (!) | AES-XCBC (C) | off (!) | Group 2 (!) |
| yes | Remote Site1 | IKEv2 | Group 2 (!) | AESCGM16-256 (C) | SHA-1 (!) | ESP | AESGMAC-128 | n/a | off (!) | Group 2 (!) |
| yes | To TZ570 | IKEv2 | Group 1 (!) | AES-256 | SHA-1 (!) | ESP | AES-256 | n/a | on | n/a |

## Configuración criptográfica de la política VPN: algoritmos inseguros utilizados

| Unsafe | | |
|---|---|---|
| **Category** | **Type** | **Comment** |
| DH Group | 192-Bit R ECP Group | Too small ECC group |
| Encryption | DES | Broken unsafe |
| IKE | Aggressive | Leads to info leaks insecure |
| Integrity | MD5 | Broken collisions possible |
| Integrity | SHA-1 | Deprecated collision attacks |
| Misc | None | No encryption integrity |

| Not recommended | | |
|---|---|---|
| **Category** | **Type** | **Comment** |
| DH Group | 224-Bit R ECP Group | Borderline ECC group aging out |
| Encryption | 3DES | Legacy slow 112-bit effective strength |
| Encryption | AES-XCBC | Niche less common not widely supported |
| IKE | Main | Standard for IKEv1 secure but older |
| Protocol | AH | Rarely used integrity only no encryption |




# Informe de estado (Health Report)

## Explicación

El informe de mantenimiento ayuda a identificar los elementos de configuración que deben revisarse periódicamente para mantener el firewall limpio, eficiente y fácil de gestionar. Con el tiempo, las configuraciones de firewall crecen de forma natural a medida que se añaden nuevas reglas, objetos, VPN y servicios. Sin un mantenimiento periódico, las entradas obsoletas o no utilizadas pueden acumularse, aumentando la carga administrativa y dificultando la resolución de problemas.
Este informe destaca los elementos de configuración que pueden requerir atención, como reglas de firewall deshabilitadas o no utilizadas, políticas NAT inactivas, objetos de dirección y servicio no utilizados, servicios de seguridad caducados y otros elementos de configuración que ya no se utilizan activamente. También identifica configuraciones que podrían beneficiarse de una optimización o limpieza.
El propósito de este informe no es recomendar la eliminación automática de cada elemento enumerado. En su lugar, proporciona a los administradores una visión estructurada de los componentes de configuración que deben verificarse antes de realizar cualquier cambio. Algunos objetos o reglas pueden seguir siendo necesarios para proyectos futuros, entornos temporales, procedimientos de recuperación ante desastres o servicios de uso poco frecuente.
El mantenimiento periódico ofrece varios beneficios importantes:
- Reduce la complejidad de la configuración y mejora la legibilidad.
- Facilita considerablemente la resolución de problemas y las auditorías.
- Ayuda a identificar elementos de configuración obsoletos u olvidados.
- Reduce el riesgo de errores de configuración accidentales.
- Mejora la gestionabilidad a largo plazo del firewall.
- Respalda un entorno de seguridad bien documentado y mantenido de forma profesional.
Un firewall bien mantenido es más fácil de administrar, más fácil de auditar y proporciona una base más sólida para futuros cambios de configuración y mejoras de seguridad.

# Análisis de utilización del firewall

## Explicación

**Análisis de utilización del firewall**
Estos gráficos ilustran el nivel de utilización del firewall durante el período anterior a la exportación de datos. Una utilización elevada puede provocar una degradación del rendimiento, incluido el procesamiento retrasado del tráfico o la pérdida de paquetes. Para obtener información significativa, el Technical Support Report utilizado como fuente de datos debería generarse idealmente durante un período de alta carga del sistema.

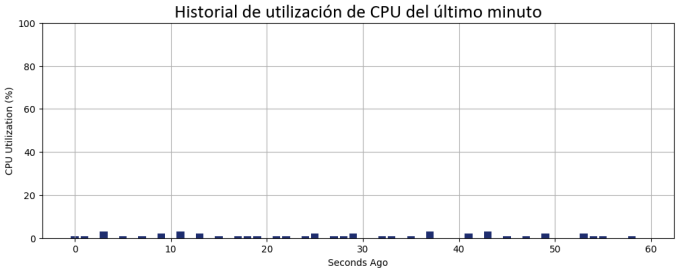
**Fuentes de datos recomendadas**
Las estadísticas de utilización más precisas suelen obtenerse de sistemas de monitoreo externos basados en NetFlow o SNMP. Para la generación de informes basada en NetFlow, SonicWall ofrece una solución dedicada llamada *Analytics*, que se integra perfectamente con los firewalls SonicWall.

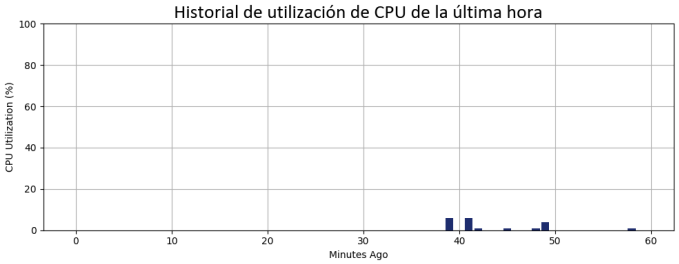
**Consideraciones importantes para entornos HA**
Si faltan valores de utilización para el intervalo de tiempo seleccionado, verifique si el firewall opera en un clúster de alta disponibilidad (HA). Cuando la unidad en espera se activa durante el período del informe, es posible que los datos de utilización no se capturen en el dispositivo esperado, lo que da lugar a información de gráficos incompleta o faltante.

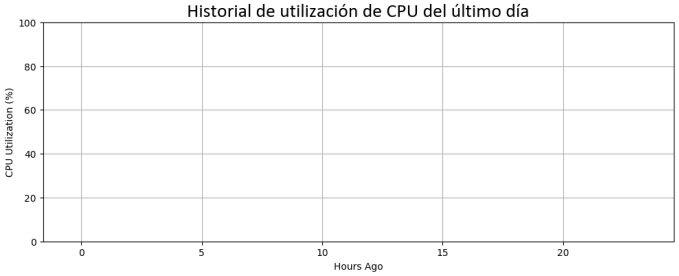
## Análisis de utilización del firewall

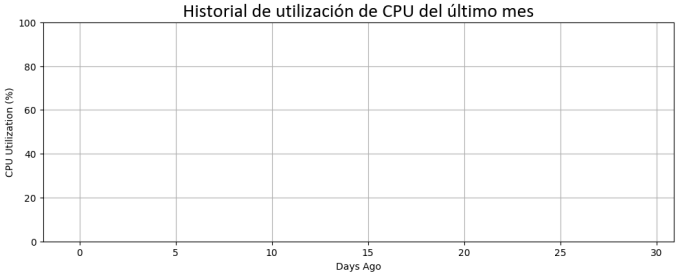
| Intervalo de tiempo | Promedio | Estado |
|---|---|---|
| Minuto: | 0 % | OK |
| Hora: | 0 % | OK |
| Día: | 0 % | OK |
| Mes: | 0 % | OK |

### Gráficos de utilización del rendimiento



## Firmware Version Check

### Explicación

**Comparación de versiones de firmware**
Esta sección compara la versión de firmware actualmente instalada con la última versión disponible en MySonicWall. Esto ayuda a identificar si el dispositivo está actualizado, requiere una actualización recomendada o ejecuta una compilación de software obsoleta que puede carecer de mejoras, correcciones de errores o mejoras de seguridad.

### Firmware Version Check:

```
Firmware Installed on Firewall:  7.3.0-7012-R8150
Latest Firmware on MySonicWall:  7.3.3-7015
Firmware Release Date:           26.06.2026
Release Note URL:
https://software.sonicwall.com/Firmware/Documentation/232-006386-00_RevJ_SonicOS_7.3_ReleaseNotes.pdf
```

### Información adicional

El firmware 7.3.3-7015 está disponible en MySonicWall.com; considere actualizar a esa versión

# Resumen del historial de configuración y firmware

## Explicación

**Resumen del historial de configuración y firmware**
La siguiente tabla proporciona una visión general de los estados de configuración pasados y las versiones de firmware implementadas en el dispositivo. Destaca la frecuencia con la que se migraron las configuraciones y si se produjeron downgrades de firmware no compatibles.

**Downgrades no compatibles**
Un downgrade de firmware se considera no compatible si no se importó posteriormente ninguna configuración de la versión de firmware degradada. En tales casos, no se puede garantizar la compatibilidad del sistema y pueden surgir problemas operativos.

**Impacto de configuraciones obsoletas o migradas con frecuencia**
Los conjuntos de configuración que se han migrado repetidamente o se han utilizado en varios dispositivos pueden acumular gradualmente incoherencias o parámetros obsoletos. Esto puede provocar comportamientos inesperados, un rendimiento degradado o errores de procesamiento de la configuración durante futuras migraciones o actualizaciones.

| Firmware | TimeStamp | Action | Comment |
|---|---|---|---|
| 7.0.1-5145-2363 | 24.01.2024 01:33:01 | Settings import | |
| 7.1.1-7040-5387 | 24.01.2024 08:25:53 | Firmware applied | |
| 7.1.1-7047-5557 | 01.03.2024 07:37:45 | Firmware applied | |
| 7.1.1-7047-5557 | 27.11.2024 18:21:03 | Settings import | |
| 7.1.1-7058-6162 | 03.12.2024 20:01:06 | Firmware applied | |
| 7.1.1-7058-6162 | 05.02.2025 21:58:08 | Settings import | |
| 7.1.1-7058-6162 | 21.03.2025 16:23:00 | Settings import | |
| 7.1.3-7015-6965 | 31.03.2025 21:24:27 | Firmware applied | |
| 7.3.0-7012-8150 | 08.09.2025 18:29:24 | Firmware applied | |
| 7.3.0-7012-8150 | 10.03.2026 14:38:34 | Settings import | |
| 7.3.0-7012-8150 | 10.03.2026 16:27:54 | Settings import | |
| 7.3.0-7012-8150 | 11.03.2026 02:01:27 | Settings import | |
| 7.3.0-7012-8150 | 11.03.2026 09:10:26 | Settings import | |
| 7.3.0-7012-8150 | 11.03.2026 11:03:15 | Settings import | |
| 7.3.0-7012-8150 | 21.05.2026 21:28:13 | Settings import | |

## Información adicional

No se detectó ningún downgrade de firmware no compatible

## Resumen del historial de configuración y firmware

### Explicación

**Resumen de conversión de configuración**
Este informe indica si la configuración se convirtió utilizando la herramienta de conversión de SonicWall. Esto ayuda a identificar configuraciones migradas y ofrece información sobre si la configuración proviene de plataformas anteriores o implementaciones previas.

### Details

```
La configuración se convirtió en el pasado: No
```

# Fiabilidad - Alta disponibilidad

## Explicación

**Importancia de la alta disponibilidad en los sistemas de firewall**

**1. Aplicación continua de la seguridad**
La alta disponibilidad (HA) garantiza el funcionamiento ininterrumpido de los sistemas de firewall, manteniendo controles de seguridad continuos incluso durante problemas de hardware, actualizaciones o mantenimiento planificado. Esto evita brechas en la detección de amenazas, la validación de accesos y la aplicación de políticas.

**2. Reducción del tiempo de inactividad**
En una configuración HA, un firewall secundario asume automáticamente el control si la unidad primaria deja de estar disponible. Este failover fluido minimiza el tiempo de inactividad, garantizando un acceso ininterrumpido a aplicaciones y servicios críticos.

**3. Mayor fiabilidad del sistema**
Tener varios firewalls funcionando en un par redundante aumenta la resiliencia frente a fallos de hardware, corrupción de la configuración o interrupciones inesperadas. La fiabilidad de la infraestructura de seguridad de red mejora significativamente.

**4. Soporte a la continuidad del negocio**
Las organizaciones que dependen de la conectividad en tiempo real, el acceso a la nube y los servicios en línea no pueden tolerar interrupciones de red prolongadas. La HA protege las operaciones comerciales manteniendo activa la aplicación de la seguridad durante eventos operativos y escenarios de fallo.

**5. Beneficios de rendimiento con la distribución de carga**
Algunos entornos HA admiten la distribución de carga, mejorando el rendimiento al equilibrar sesiones o rutas de tráfico entre varios dispositivos. Esto evita cuellos de botella en el procesamiento y aumenta el rendimiento general de la red.

**6. Capacidad de recuperación ante desastres**
La HA desempeña un papel crucial en la planificación de la recuperación ante desastres. Cuando falla un dispositivo primario, la unidad secundaria mantiene activas las políticas, el enrutamiento, los túneles VPN y los servicios de seguridad, reduciendo el impacto operativo durante las actividades de recuperación.

**7. Alineación regulatoria y de cumplimiento**
Muchos sectores requieren disponibilidad garantizada de los controles de seguridad y mecanismos de failover trazables. Implementar HA respalda las iniciativas de cumplimiento, la preparación para auditorías y los compromisos de nivel de servicio.

**8. Mejor experiencia de usuario y cliente**
Con un acceso de red ininterrumpido, los usuarios experimentan menos interrupciones del servicio y una restauración más rápida tras los fallos. Esto contribuye directamente a niveles de satisfacción más altos y a una prestación de servicio más estable.

**Resumen**
La alta disponibilidad en los sistemas de firewall es una base fundamental para la resiliencia empresarial. Garantiza protección continua, minimiza el tiempo de inactividad operativo, respalda la recuperación ante desastres, mejora el rendimiento y facilita el cumplimiento normativo. Al reducir las interrupciones del servicio y mantener una conectividad segura, la HA mejora significativamente tanto la eficacia operativa como la de seguridad.

## Fiabilidad - Alta disponibilidad

### High Availability Settings

| | |
|---|---|
| High Availability: | Enabled |
| HA Primary Serial-Number: | 0040103CD830 |
| HA Secondary Serial-Number: | 0040103F5B1C |
| HA Stateful Sync: | Enabled |
| HA Preempt Mode: | Disabled |
| HA Control Interface: | X4 |
| HA Data Interface: | X4 |
| HA Role: | Primary |
| HA Firmware mismatch with peer: | No |
| HA Active Time: | 0 Days 00:21:47 |

### High Availability Status

| | |
|---|---|
| HA Firewall Status: | Active |
| HA Peer State: | Peer not found / not active |
| HA Peer in sync: | No |

## Información sobre el ciclo de vida del producto

### Explicación

**Información sobre el ciclo de vida del producto**
Esta sección ofrece información sobre el estado actual del ciclo de vida del producto. Ayuda a determinar si un dispositivo cuenta con soporte completo, se acerca al fin del soporte o ya ha superado su período de mantenimiento oficial.

Para descripciones detalladas del ciclo de vida, hitos importantes y calendarios de soporte actuales, consulte la documentación oficial sobre el ciclo de vida de los productos SonicWall disponible a través de los recursos de soporte de SonicWall.

| Description | Value |
|---|---|
| Model: | SonicWall NSA NSV 270 |
| Last Order Date: | 15.04.2022 |
| ARM Begin: | 16.04.2022 |
| LRM Begin: | 16.04.2024 |
| 1 Year LOD: | 15.04.2025 |
| End of Support: | 16.04.2026 |

### Información adicional

¡Vuelva a verificar esta información en el sitio web oficial de SonicWall!

# Servicios de seguridad - Resumen del estado de licencia

## Explicación

**Licencias de servicios de seguridad**
Este informe muestra qué servicios tienen actualmente una licencia activa. Los servicios con licencia son totalmente funcionales y capaces de proporcionar la protección o el conjunto de funciones previstos. Los servicios sin una licencia válida pueden tener funcionalidad limitada o estar completamente inactivos.

Esta vista ayuda a verificar si las funciones de seguridad y basadas en suscripción requeridas siguen operativas, y ayuda a planificar renovaciones para evitar interrupciones del servicio.

## Servicios de seguridad - Resumen del estado de licencia

| Nombre del servicio | Estado de la licencia | Recuento | Vencimiento |
|---|---|---|---|
| Node Upgrade | None | | Unlimited |
| Active/Active Clustering Service | None | | Unlimited |
| NSM Essential (Retired) | Not Licensed | | Unlimited |
| NSM Advanced (Retired) | Disabled | | 05.02.2026 |
| Capture Client Basic | Not Licensed | | Unlimited |
| Content Filtering Client | None | | Unlimited |
| Capture Client Advanced | Not Licensed | | Unlimited |
| Capture Client Premier | Not Licensed | | Unlimited |
| Deep Packet Inspection for SSL (DPI-SSL) | Licensed | | Unlimited |
| Deep Packet Inspection for SSH (DPI-SSH) | None | | Unlimited |
| Virtual Assist | None | | Unlimited |
| SSL VPN | Licensed | 2 Max: 100 | Unlimited |
| Global VPN Client | Licensed | 50 Max: 1000 | Unlimited |
| Global VPN Client Enterprise | None | | Unlimited |
| WAN Acceleration Client | None | | Unlimited |
| WAN Acceleration Software | None | | Unlimited |
| Botnet Block | None | | Unlimited |
| Stateful High Availability | Licensed | | Unlimited |
| Comprehensive Anti-Spam Service | None | | Unlimited |
| External IDS Support | None | | Unlimited |
| CSC Analytics (includes Reporting) | None | | Unlimited |
| CSC Management | None | | Unlimited |
| CSC Management Lite | None | | Unlimited |
| CSC Management and Reporting | None | | Unlimited |
| CSC Management and 7-day Reporting | None | | Unlimited |
| Syslog Analytics | Expired | | 03.02.2024 |
| Comprehensive/Advanced Gateway Security Suite | None | | Unlimited |
| Gateway AV | None | | Unlimited |
| Anti-Spyware | None | | Unlimited |
| Intrusion Prevention | None | | Unlimited |
| App Control | None | | Unlimited |
| App Visualization | None | | Unlimited |
| Content Filtering: Premium Edition | None | | Unlimited |
| Analyzer | None | | Unlimited |
| Capture Advanced Threat Protection | Licensed | | 14.02.2027 |
| Standard Support | Not Licensed | | Unlimited |
| 24x7 Support | Licensed | | 14.02.2027 |
| SonicOS Expanded | None | | Unlimited |
| Software and Firmware Updates | None | | Unlimited |
| Hardware Warranty | None | | Unlimited |
| Remote Implementation Service | None | | Unlimited |
| Gateway Anti-malware/Intrusion Prevention/App Control | Licensed | | 14.02.2027 |
| Content Filtering Service | Licensed | | 14.02.2027 |
| Secure Connect Lite | None | | Unlimited |
| Secure Connect | None | | Unlimited |
| Advanced Reporting & Analytics (7 days) | Licensed | | 14.02.2027 |
| DNS Filtering | Licensed | | 14.02.2027 |

## Servicios de seguridad - Resumen del estado de licencia

| Nombre del servicio | Estado de la licenciaRecuento | Vencimiento |
|---|---|---|
| Advanced Protection Security Suite | Licensed | 14.02.2027 |
| Managed Protection Security Suite | Not Licensed | Unlimited |
| Web and Chat Only Support | None | Unlimited |
| Basic Reporting (7 days) | Not Licensed | Unlimited |
| Essential Protection Service Suite | Disabled | 05.02.2026 |
| Advanced Reporting & Analytics | None | Unlimited |
| Threat Protection Service Suite | None | Unlimited |
| Model Upgrade | Not Licensed | Unlimited |
| GeoIP Filtering | None | Unlimited |

# Fiabilidad - Failover de WAN

## Explicación

**Importancia del failover de WAN en los sistemas de firewall**

**1. Conectividad a Internet ininterrumpida**
El failover de WAN garantiza un acceso continuo a Internet cambiando automáticamente a una conexión de respaldo si falla el enlace WAN principal. Esto es crucial para mantener las operaciones comerciales que dependen de la conectividad a Internet.

**2. Mayor fiabilidad y disponibilidad**
Al proporcionar una conexión secundaria, el failover de WAN mejora la fiabilidad y la disponibilidad de los servicios de red. Esto reduce el tiempo de inactividad y aumenta la productividad general.

**3. Continuidad del negocio**
Las interrupciones de red pueden provocar pérdidas financieras, reducción de la satisfacción del cliente y retrasos operativos. El failover de WAN apoya la continuidad del negocio al minimizar las interrupciones y mantener el acceso a aplicaciones y servicios críticos.

**4. Balanceo de carga y mejor rendimiento**
Algunas plataformas de firewall admiten tanto el failover como el balanceo de carga. Esto permite distribuir el tráfico entre varios enlaces WAN, optimizando el ancho de banda y mejorando el rendimiento para los usuarios finales.

**5. Soporte para recuperación ante desastres**
Durante interrupciones inesperadas o fallos de infraestructura, el failover garantiza que los procesos de recuperación permanezcan accesibles e ininterrumpidos, preservando la disponibilidad del servicio y la integridad de los datos.

**6. Mantenimiento de la postura de seguridad**
Los firewalls con capacidad de failover garantizan que todo el tráfico -durante el funcionamiento normal y durante los eventos de failover- continúe pasando por las inspecciones de seguridad. Esto evita eludir las medidas de protección durante las interrupciones.

**7. Eficiencia de costos**
Aunque la implementación de líneas WAN secundarias tiene costos asociados, prevenir las interrupciones del servicio ayuda a evitar pérdidas financieras, disminuciones de productividad e insatisfacción del cliente, lo que se traduce en ahorros a largo plazo.

**Resumen**
El failover de WAN es una capacidad crucial en los sistemas de firewall. Mantiene el acceso continuo a Internet, apoya la recuperación ante desastres, mejora la fiabilidad, refuerza la consistencia de la seguridad y protege la continuidad del negocio. Al reducir el tiempo de inactividad y mejorar el rendimiento, el failover de WAN ayuda a las organizaciones a mantener la calidad del servicio y la eficiencia operativa.

## Fiabilidad - Failover de WAN

### WAN Interface Summary

Number of WAN Interfaces configured & enabled: 2

| Interface | Type | Comment | PacketsIn | PacketsOut |
|---|---|---|---|---|
| X1 | WAN | Default WAN | 9268 | 9071 |
| X5 | WAN | | 1215 | 328 |

WAN Load Balancing is: enabled

| Interface | Probing | Type | Prim Dest | Protocol | Alt Dest | Protocol |
|---|---|---|---|---|---|---|
| X1 | Logical | At least one target should reply | 204.212.170.23 | TCP | 8.8.8.8 | ICMP |
| X5 | Physical | None | None | None | None | None |

# Informe de configuración

## Explicación

La auditoría de configuración revisa la configuración técnica y la preparación operativa del entorno del firewall. Evalúa características del sistema como la alta disponibilidad (HA), el failover WAN y el estado de los servicios de seguridad. Además, comprueba si los componentes clave están configurados correctamente y alineados con los estándares de implementación recomendados.

# Tiempo de espera de conexión TCP

## Explicación

El tiempo de espera de conexión TCP determina cuánto tiempo mantiene el firewall una sesión TCP inactiva en su tabla de conexiones antes de eliminarla. El valor predeterminado global de 15 minutos es una configuración razonable para la mayoría de los entornos y proporciona un buen equilibrio entre admitir tráfico de red legítimo y conservar los recursos del firewall.
Cambiar el tiempo de espera TCP global afecta a todas las conexiones TCP que pasan por el firewall. Aumentar este valor innecesariamente puede provocar que las sesiones obsoletas permanezcan en memoria durante períodos prolongados, consumiendo entradas de la tabla de conexiones y reduciendo potencialmente la capacidad general del dispositivo. En entornos grandes o con mucho tráfico, esto puede tener un impacto notable en el rendimiento del firewall y en el uso de recursos.
Sin embargo, algunas aplicaciones requieren períodos de inactividad más largos para mantener conexiones persistentes. Algunos ejemplos son ciertas aplicaciones de bases de datos, software cliente/servidor heredado o sistemas de control industrial especializados. En estos casos, se considera una buena práctica dejar el tiempo de espera global en su valor predeterminado y, en su lugar, configurar un tiempo de espera TCP personalizado solo en las reglas de acceso específicas que lo requieran.
Aplicar tiempos de espera extendidos a nivel de regla ofrece varias ventajas:
Minimiza el impacto en el firewall en general.
Limita el aumento del consumo de recursos a las aplicaciones afectadas.
Reduce el número de sesiones obsoletas en la tabla de conexiones.
Hace visibles y más fáciles de documentar los requisitos especiales de las aplicaciones.
Simplifica futuras auditorías y la resolución de problemas.
Este informe muestra la configuración actual del tiempo de espera TCP global y enumera todas las reglas de acceso que utilizan un valor de tiempo de espera TCP personalizado. Las reglas con configuraciones no predeterminadas deben revisarse periódicamente para garantizar que la excepción siga siendo necesaria y esté adecuadamente documentada.
Como recomendación general, el tiempo de espera TCP global debe permanecer en su valor predeterminado siempre que sea posible, mientras que los requisitos específicos de las aplicaciones deben abordarse mediante anulaciones del tiempo de espera por regla.

## General TCP Setting

Tiempo de espera de conexión TCP global: 69

## Información adicional

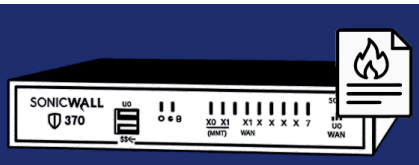
El tiempo de espera de conexión TCP predeterminado ha sido modificado. Se recomienda mantener la configuración general en 15 minutos. Si un determinado servicio requiere valores diferentes, cambie el tiempo de espera TCP en una regla específica

## Reglas en las que se ha modificado el tiempo de espera TCP predeterminado



| Ena | A | Name | SrcZone | DstZone | SrcNet | DstNet | SrcSvc | DstSvc | TCP Timeout |
|---|---|---|---|---|---|---|---|---|---|
| YES | A | Rule6 | DMZ-sec | Test | any | Test13 | Citrix TCP | any | 66 |
| YES | A | Complicated Rule | DMZ-unsec | Test | any | any | Citrix UDP | any | 10 |
| YES | A | Heating Maintenance | WAN | LAN | any | LAN Subnets | any | SSH | 30 |

*Número de registros: 3*




# Informe de documentación

## Explicación

El informe de documentación proporciona una visión estructurada del entorno del firewall y sus elementos de configuración clave. Recopila y presenta información relevante del sistema, incluyendo configuración de red, asignaciones de interfaces, configuraciones de zona y políticas aplicadas.
El informe está diseñado para servir como referencia integral para los administradores, apoyando tanto las tareas operativas como la transferencia de conocimiento. Garantiza que los detalles de configuración importantes estén claramente documentados y sean fácilmente accesibles, reduciendo la dependencia de la inspección manual del sistema.
Además, la documentación ayuda a mantener la transparencia y la coherencia en todo el entorno, facilitando la resolución de problemas, las auditorías y los cambios futuros.

# Todos los registros de auditoría

## Explicación

**Auditoría interna del firewall**
*La auditoría interna en los firewalls es un componente esencial para mantener la integridad operativa, la responsabilidad y la seguridad dentro de un entorno de red. El firewall representa uno de los puntos de control más críticos en una organización, y la auditoría proporciona visibilidad sobre los cambios de configuración, los eventos de acceso y las acciones administrativas que influyen directamente en la postura de seguridad de la red.*

**Responsabilidad y trazabilidad**
*Los registros de auditoría documentan quién realizó los cambios, cuándo se realizaron y qué se modificó. Esta trazabilidad garantiza que las responsabilidades se asignen claramente y que cualquier configuración incorrecta, desviación de los estándares o cambio no autorizado pueda identificarse y corregirse rápidamente.*

**Detección de modificaciones no autorizadas o riesgosas**
*Los firewalls afectan directamente al control de acceso, la protección de datos y el flujo de tráfico. La auditoría interna permite a los administradores detectar cambios de configuración intencionados o accidentales, ayudando a identificar incidentes de seguridad, violaciones de políticas o posibles usos indebidos de privilegios administrativos.*

**Apoyo al cumplimiento normativo y la gobernanza**
*Muchos marcos regulatorios exigen la auditoría de sistemas críticos como los firewalls. Los registros de auditoría interna respaldan el cumplimiento de estándares relevantes para sectores como finanzas, salud y gobierno. Proporcionan prueba de que se siguen las políticas y de que los mecanismos de protección se aplican correctamente.*

**Perspectiva operativa y mejora continua**
*Los registros de auditoría ayudan a los equipos de seguridad a comprender el historial de configuración y las tendencias operativas. La revisión periódica de estos registros permite a las organizaciones perfeccionar las políticas de acceso, identificar problemas recurrentes y fortalecer las prácticas de gestión de cambios.*

**Investigación de incidentes y análisis forense**
*Cuando ocurre un evento de seguridad, los datos de auditoría interna suelen ser una de las fuentes de evidencia más valiosas. Permiten a los investigadores reconstruir las acciones realizadas en el firewall, analizar las causas raíz y determinar si la actividad maliciosa o el error humano contribuyeron al incidente.*

**Conclusión**
*La auditoría interna es necesaria para garantizar la transparencia, la coherencia y la responsabilidad en las operaciones del firewall. Mejora la seguridad, respalda los requisitos normativos, permite una resolución de problemas más rápida y proporciona una base clave para una gestión de red resiliente.*

## Información adicional

**Resumen de eventos de auditoría**
Esta sección enumera todos los eventos de auditoría extraídos del Technical Support Report (TSR). Proporciona visibilidad sobre los cambios de configuración realizados en el firewall e identifica a los usuarios responsables de dichas acciones.

**Nota importante**
Los registros de auditoría no se sincronizan entre dispositivos cuando la alta disponibilidad (HA) está habilitada. Como resultado, los cambios realizados en la unidad secundaria (activa) durante los períodos de failover pueden no aparecer en el registro de auditoría del dispositivo principal. ¡Futuras versiones de FirewallToolbox podrían abordar este problema!

Este informe ayuda a validar la actividad administrativa, respalda la responsabilidad y ayuda a identificar cambios de configuración no deseados o no autorizados.

## Información adicional

Este informe muestra solo las 10 entradas más recientes. Ejecute el informe individual para ver todos los resultados.

# Firewall Internal Admin Audit Records

ID: 3749 Timestamp: 15.09.2026 16:33:49
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19526)

ID: 3749 Timestamp: 15.09.2026 16:33:49
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19526)

ID: 3748 Timestamp: 15.09.2026 16:33:49
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19525)

ID: 3748 Timestamp: 15.09.2026 16:33:49
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19525)

ID: 3747 Timestamp: 15.09.2026 16:31:36
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46610)

ID: 3747 Timestamp: 15.09.2026 16:31:36
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46610)

ID: 3746 Timestamp: 15.09.2026 16:31:36
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46608)

ID: 3746 Timestamp: 15.09.2026 16:31:36
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46608)

# Firewall Internal Admin Audit Records

```
ID:          3745      Timestamp:   15.09.2026 16:18:33
Description: End Configuration Mode
Old:
New:
Status:
User:        UDSAdmin
Session:     GMS
Source:      127.0.0.1 (50325)
```


```
ID:          3745      Timestamp:   15.09.2026 16:18:33
Description: End Configuration Mode
Old:
New:
Status:
User:        UDSAdmin
Session:     GMS
Source:      127.0.0.1 (50325)
```

# Todas las reglas (IPv4)

## Explicación

Este informe proporciona un inventario completo de todas las reglas de acceso IPv4 configuradas en el firewall, excluyendo las reglas de acceso predeterminadas integradas. Para cada regla, el informe enumera el estado de habilitación, la acción (Permitir/Denegar), el nombre de la regla, las zonas de origen y destino, los objetos de red de origen y destino, los objetos de servicio, los comentarios del administrador y el UUID único de la regla.
Mantener un inventario actualizado de las reglas de firewall es una parte esencial de la administración del firewall y la auditoría de seguridad. Permite a los administradores revisar la política de seguridad implementada, verificar que las reglas sigan el principio de mínimo privilegio, identificar reglas obsoletas o redundantes y garantizar que la documentación de las reglas sea completa y significativa. La revisión periódica de la base de reglas ayuda a reducir la complejidad de la configuración, mejora la resolución de problemas y minimiza el riesgo de acceso no intencionado causado por reglas de firewall obsoletas o excesivamente permisivas.

## Todas las reglas (IPv4)



| Ena | A | Name | SrcZone | DstZone | SrcNet | DstNet | SrcSvc | DstSvc | |
|---|---|---|---|---|---|---|---|---|---|
| YES | A | My Rule | DMZ-sec | DMZ-unsec | any | any | any | FTP Data | |
| YES | A | Test 17 | DMZ-sec | DMZ-unsec | any | any | any | HTTPS | |
| YES | A | Test 20 | DMZ-sec | DMZ-unsec | any | any | any | Kazaa / FastTrack | |
| YES | A | Test 21 | DMZ-sec | DMZ-unsec | any | any | any | Lotus Notes | |
| YES | A | Test 19 | DMZ-sec | DMZ-unsec | any | any | any | IKE | |
| YES | A | Test 18 | DMZ-sec | DMZ-unsec | any | any | any | ICMP | |
| YES | A | Rule6 | DMZ-sec | Test | any | Test13 | Citrix TCP | any | |
| YES | A | Rule10 | DMZ-sec | Test | WAN-GoogleDNS-8.8.8.8 | any | Direct Connect | any | |
| YES | A | Allow WAN1 | DMZ-sec | WAN | any | any | Enhanced TV | any | |
| YES | A | Test 22 | DMZ-unsec | DMZ-sec | any | any | any | MSN | |
| YES | A | Allow syslog | DMZ-unsec | DMZ-unsec | any | any | SSH Management | any | |
| YES | A | Complicated Rule | DMZ-unsec | Test | any | any | Citrix UDP | any | |
| YES | A | Allow WAN1 | DMZ-unsec | WAN | any | any | Citrix UDP | any | |
| YES | A | Allow WAN1 | LAN | WAN | KlausMeier | any | any | any | |
| YES | A | Allow management via ... | SSLVPN | LAN | SSLVPN-NetExtender Range | any | any | HTTPS Management | |
| YES | A | Test 24 | WAN | 060466 | any | any | any | OSPF | |
| YES | A | Test 25 | WAN | 060466 | any | any | any | POP3 (Retrieve E-Mail) | |
| YES | A | Test 23 | WAN | 060466 | any | any | any | MSN | |
| YES | A | Heating Maintenance | WAN | LAN | any | LAN Subnets | any | SSH | Temp, Rule to allow M... |
| YES | A | Allow Citrix | any | | any | any | Citrix UDP | any | Example any<> any |
| YES | A | Allow FTP | any | | any | any | FTP | any | |

*- Las reglas añadidas automáticamente se excluyen de este informe*

*Número de registros: 21*

# Reglas de administración (IPv4)

## Explicación

**Reglas de firewall que permiten el acceso de administración en firewalls SonicWall (SSH / HTTPS)**

Los firewalls SonicWall proporcionan servicios de administración como SSH y HTTPS para permitir a los administradores configurar, supervisar y mantener el dispositivo. Estos servicios otorgan acceso privilegiado al firewall y a sus controles de seguridad. Por lo tanto, las reglas de firewall que permiten el acceso de administración deben gestionarse con extremo cuidado, ya que una exposición incorrecta puede introducir graves riesgos de seguridad y operativos.

**Riesgos de seguridad**
Permitir el acceso de administración a través de reglas de firewall aumenta la superficie de ataque del dispositivo SonicWall. Las interfaces de administración son un objetivo común para los atacantes, ya que un acceso exitoso proporciona control administrativo directo. Los servicios SSH o HTTPS expuestos pueden estar sujetos a intentos de inicio de sesión por fuerza bruta, ataques de relleno de credenciales o explotación de vulnerabilidades en el plano de administración de SonicWall o en el firmware subyacente.

Si un atacante obtiene acceso administrativo, puede modificar las reglas del firewall, deshabilitar servicios de seguridad, alterar configuraciones VPN o crear puertas traseras persistentes. Tales acciones pueden resultar en la interceptación de tráfico, pérdida de la integridad de la red o el compromiso total del entorno protegido.

**Exposición a ataques basados en la red**
Cuando los servicios de administración de SonicWall son accesibles desde redes no confiables (como la WAN o zonas definidas de forma amplia), se vuelven visibles a escaneos automatizados, actividades de reconocimiento y ataques de denegación de servicio. Incluso cuando se utilizan protocolos cifrados como HTTPS o SSH, persisten riesgos si el firmware está desactualizado, se habilitan configuraciones criptográficas débiles o el acceso no está suficientemente restringido.

Además, las reglas de acceso de administración mal configuradas pueden exponer involuntariamente puertos administrativos en varias interfaces o zonas, aumentando la probabilidad de acceso accidental o no autorizado.

**Impacto operativo y de cumplimiento**
Las reglas de acceso de administración demasiado permisivas complican la supervisión y la detección de incidentes en los firewalls SonicWall. Los intentos de acceso no autorizado pueden ser difíciles de distinguir de la actividad administrativa legítima, especialmente si el registro y las alertas no están configurados de forma estricta. Desde una perspectiva de cumplimiento, el acceso de administración sin restricciones o no documentado a menudo infringe las políticas de seguridad internas y los requisitos normativos que exigen un control estricto sobre el acceso privilegiado y las interfaces administrativas.

**Mejores prácticas recomendadas para firewalls SonicWall**
El acceso de administración en los dispositivos SonicWall debe restringirse a redes internas confiables o zonas de administración dedicadas. Debe evitarse el acceso de administración directo desde interfaces WAN siempre que sea posible. Si se requiere administración remota, debe realizarse a través de conexiones VPN seguras con autenticación y cifrado fuertes.

Otros controles recomendados incluyen limitar el acceso por dirección IP de origen, habilitar la autenticación multifactor para usuarios administrativos, mantener actualizado el firmware de SonicWall y revisar periódicamente las reglas de acceso de administración y los registros de auditoría. Estas medidas ayudan a garantizar que el acceso administrativo permanezca controlado, auditable y alineado con las mejores prácticas de seguridad de SonicWall.

## Reglas de administración (IPv4)

### Explicación

**Objetos y grupos de servicios de administración**
Los elementos enumerados a continuación representan los objetos y grupos de servicio clasificados como servicios de administración. Estos suelen incluir protocolos y puertos utilizados para el acceso administrativo, la configuración de dispositivos y las funciones de supervisión.

Identificar estos servicios ayuda a determinar dónde se permite el acceso de administración y garantiza que las interfaces administrativas se apliquen solo a áreas confiables y controladas de la red.

| Service Objects |
| --- |
| Citrix TCP |
| Citrix TCP (Session Reliability) |
| Citrix UDP |
| GMS HTTPS |
| HTTP |
| HTTP Management |
| HTTPS |
| HTTPS Management |
| IKE (Key Exchange) |
| IKE (Traversal) |
| Kerberos TCP |
| Ping |
| SSH |
| SSH Management |
| Syslog |

| Service-Groups |
| --- |
| Citrix |
| Idle HF |
| Management Services |
| IKE |
| Kerberos |
| Interface Management Services |

## Reglas de administración (IPv4)



| Ena | A | Name | SrcZone | DstZone | SrcNet | DstNet | SrcSvc | DstSvc | |
|---|---|---|---|---|---|---|---|---|---|
| YES | A | Test 17 | DMZ-sec | DMZ-unsec | any | any | any | HTTPS | |
| YES | A | Test 19 | DMZ-sec | DMZ-unsec | any | any | any | IKE | |
| YES | A | Allow management via ... | SSLVPN | LAN | SSLVPN-NetExtender Range | any | any | HTTPS Management | |
| YES | A | Heating Maintenance | WAN | LAN | any | LAN Subnets | any | SSH | Temp, Rule to allow M... |

*Número de registros: 4*

# Interfaces (IPv4)

## Explicación

**Resumen de configuración de interfaces**
Este informe muestra todas las interfaces configuradas junto con su configuración asignada. Proporciona visibilidad sobre los roles de las interfaces, la información de direccionamiento y los parámetros operativos, ayudando a evaluar la conectividad, la segmentación y la estructura general de la red.

## Interfaces (IPv4)

| Name | Zone | Comment | Assignment | IP | Subnet Mask | Gateway |
|---|---|---|---|---|---|---|
| X0 | LAN | Default LAN | Static LAN | 10.100.10.254 | 255.255.255.0 | 0.0.0.0 |
| X1 | WAN | Default WAN | Static | 10.10.15.1 | 255.255.255.0 | 10.10.15.254 |
| X2 | DMZ-unsec | | Static LAN | 10.100.30.254 | 255.255.255.0 | 0.0.0.0 |
| X3 | DMZ-sec | | Static LAN | 10.100.40.254 | 255.255.255.0 | 0.0.0.0 |
| X4 | HA Data & Control | | n/a | n/a | n/a | n/a |
| X5 | WAN | | Static | 10.10.16.1 | 255.255.255.0 | 172.16.1.254 |
| X6 | LAN | | Static LAN | 192.168.1.254 | 255.255.255.0 | 0.0.0.0 |
| X6:V100 | LAN | | Static LAN | 192.168.2.254 | 255.255.255.0 | 0.0.0.0 |
| X7 | DMZ-sec | | Static LAN | 192.169.1.1 | 255.255.255.0 | 0.0.0.0 |

*Número de registros: 9*

# Resumen de pertenencia a usuarios y grupos

## Explicación

**Usuarios y pertenencia a grupos**
*Este informe proporciona una lista detallada de todos los usuarios junto con sus pertenencias a grupos asociadas. En función de estas afiliaciones, destaca los derechos de acceso VPN efectivos que los usuarios heredan a través de los grupos asignados.*
*Esto ayuda a identificar quién tiene acceso a los recursos VPN, verificar el derecho de acceso correcto y detectar posibles cuentas con privilegios excesivos derivados de permisos basados en grupos.*

## Resumen de pertenencia a usuarios y grupos

All LDAP Users
-es miembro del grupo:  Trusted Users
-es miembro del grupo:  SSLVPN Services
-es miembro del grupo:  LAN Access66
- Otorga derechos de acceso a:WAN Primary IP
- Otorga derechos de acceso a:LAN Primary Subnet
- Otorga derechos de acceso a:WAN-GoogleDNS-8.8.8.8
Isabel
-es miembro del grupo:  Trusted Users
-es miembro del grupo:  Content Filtering Bypass
-es miembro del grupo:  Limited Administrators
LocalAdmin
-es miembro del grupo:  Trusted Users
-es miembro del grupo:  SonicWALL Administrators
Robert
-es miembro del grupo:  Trusted Users
-es miembro del grupo:  Guest Administrators
Sylvia
-es miembro del grupo:  Trusted Users
-es miembro del grupo:  Guest Administrators
UDS-SNWL-Admins@uds.local
-es miembro del grupo:  SonicWALL Administrators
Udo
-es miembro del grupo:  Trusted Users
-es miembro del grupo:  SonicWALL Read-Only Admins
Uwe
-es miembro del grupo:  Trusted Users
-es miembro del grupo:  SonicWALL Administrators
-es miembro del grupo:  SSLVPN Services
-es miembro del grupo:  LAN Access66
- Otorga derechos de acceso a:WAN Primary IP
- Otorga derechos de acceso a:LAN Primary Subnet
- Otorga derechos de acceso a:WAN-GoogleDNS-8.8.8.8
Webadmin
-es miembro del grupo:  Trusted Users
-es miembro del grupo:  SonicWALL Administrators
-es miembro del grupo:  SSLVPN Services
apiuser
-es miembro del grupo:  Trusted Users
-es miembro del grupo:  SonicWALL Administrators
mschmitz
-es miembro del grupo:  Trusted Users
-es miembro del grupo:  SonicWALL Administrators
-es miembro del grupo:  SSLVPN Services
-es miembro del grupo:  LAN Access66
- Otorga derechos de acceso a:WAN Primary IP
- Otorga derechos de acceso a:LAN Primary Subnet

mschmitz (continuación)

- Otorga derechos de acceso a:WAN-GoogleDNS-8.8.8.8

# Directorios de usuarios externos

## Información adicional

*Cuando el número de cuentas de usuario locales en un firewall supera un umbral reducido (típicamente alrededor de 10 usuarios), gestionar las identidades directamente en el firewall se vuelve ineficiente, propenso a errores y difícil de escalar. En tales entornos, se recomienda encarecidamente integrar un directorio de usuarios externo como LDAP, RADIUS o TACACS+.*

**1. Gestión centralizada de usuarios**
*Los directorios de usuarios externos proporcionan una única fuente fiable para las identidades de usuario.*
*- Las cuentas de usuario se crean, modifican y eliminan en un único sistema central.*
*- Cambios como actualizaciones de contraseñas o desactivación de cuentas se aplican inmediatamente a todos los sistemas conectados.*
*- El esfuerzo administrativo se reduce significativamente en comparación con mantener usuarios individualmente en cada firewall.*

*Esto se vuelve cada vez más importante a medida que crece el número de usuarios y los cambios de personal ocurren con mayor frecuencia.*

**2. Mayor seguridad y menor riesgo**
*Gestionar un número creciente de usuarios locales de firewall aumenta con el tiempo el riesgo de brechas de seguridad.*
*- Las cuentas huérfanas pueden permanecer activas después de que los empleados abandonen la organización.*
*- Las políticas de contraseñas pueden ser inconsistentes o no aplicarse de manera uniforme.*
*- La administración manual de usuarios aumenta la probabilidad de errores de configuración.*

*Los sistemas de autenticación externos aplican políticas de seguridad coherentes, incluyendo complejidad de contraseñas, rotación de contraseñas, reglas de bloqueo de cuentas y, cuando es compatible, autenticación multifactor.*

**3. Mejor escalabilidad y mantenibilidad a largo plazo**
*Los firewalls están diseñados principalmente para la inspección de tráfico y la aplicación de políticas, no para la gestión del ciclo de vida de identidades.*
*- Gestionar un pequeño número de usuarios locales puede ser aceptable.*
*- Más allá de aproximadamente 10 usuarios, la carga administrativa crece de forma desproporcionada.*
*- Los directorios externos escalan a decenas, cientos o miles de usuarios sin aumentar la complejidad en el firewall.*

*El firewall se convierte en un consumidor de servicios de identidad en lugar del propietario de los datos de usuario.*

**4. Control de acceso basado en roles (RBAC)**
*Los directorios de usuarios externos permiten asignar derechos de acceso mediante grupos en lugar de cuentas de usuario individuales.*
*- Los usuarios se asignan a grupos de directorio, como usuarios VPN o administradores de firewall.*
*- Las reglas de firewall hacen referencia a estos grupos en lugar de a usuarios específicos.*
*- Los cambios de acceso pueden implementarse sin modificar la configuración del firewall.*

*Esta separación entre la gestión de identidades y la autorización mejora la claridad, la coherencia y la eficiencia operativa.*

**5. Auditoría y cumplimiento más sencillos**
*Los estándares de seguridad y las políticas internas suelen requerir una trazabilidad clara del acceso de los usuarios.*
*Los sistemas de autenticación externos proporcionan registros de autenticación centralizados, eventos de inicio de sesión trazables y una responsabilidad clara por usuario.*

*Esto simplifica considerablemente las auditorías y respalda el cumplimiento con marcos como ISO 27001, NIST o requisitos de gobernanza interna.*

**6. Integración perfecta con la infraestructura existente**
*La mayoría de las organizaciones ya operan sistemas de identidad centralizados.*
*- LDAP o Active Directory para identidades de usuario*
*- RADIUS para acceso VPN y de red*
*- TACACS+ para el control de acceso administrativo*

*Integrar el firewall en estos sistemas evita bases de datos de usuarios duplicadas y alinea el acceso al firewall con los procesos de TI establecidos.*

**7. Reducción de errores operativos**
*La gestión manual de usuarios en firewalls suele provocar problemas operativos.*
*- Eliminaciones de cuentas olvidadas*
*- Permisos inconsistentes*
*- Desviación de configuración con el tiempo*

*Delegar la autenticación a un sistema externo da como resultado configuraciones de firewall más limpias y reduce el riesgo de error humano.*

**Conclusión**
*Si bien los usuarios locales del firewall pueden ser suficientes para entornos muy pequeños, no escalan de manera efectiva.*
*Una vez que el número de usuarios supera aproximadamente los 10, el uso de un directorio de usuarios externo ofrece claros beneficios en términos de seguridad, escalabilidad, eficiencia administrativa y capacidad de auditoría.*

*Para entornos medianos y grandes, integrar LDAP, RADIUS o TACACS+ se considera una mejor práctica y un requisito fundamental para operaciones de firewall sostenibles y seguras.*

# Informe de zonas

## Explicación

Este informe muestra detalles sobre las zonas

# Informe de zonas



| Zone | Type | Member Interfaces | Trust | Active Security Services | SSLVPN | SSO |
|---|---|---|---|---|---|---|
| 060466 | 1 | None | Blocked | GAV, IPS, ASPY | No | No |
| 150971-Test | 1 | None | Blocked | None | No | No |
| DMZ | 2 | None | Allowed | None | No | Yes |
| DMZ-sec | 2 | X3, X7 | Blocked | None | No | Yes |
| DMZ-unsec | 2 | X2 | Blocked | None | No | No |
| LAN | 1 | X0, X6, X6:V100 | Allowed | GAV, IPS, ASPY, DPI-SSL-C | No | Yes |
| MULTICAST | 6 | None | Blocked | None | No | No |
| SSLVPN | 8 | None | Blocked | None | Yes | No |
| Test | 1 | None | Blocked | GAV, IPS, ASPY, DPI-SSL-C | No | Yes |
| VPN | 5 | None | Blocked | None | No | No |
| WAN | 0 | X1, X5 | Blocked | GAV, IPS, ASPY, DPI-SSL-S, GVPN | Yes | No |

*Número de registros: 11*

# Informe de mantenimiento

## Explicación

El informe de mantenimiento ayuda a identificar los elementos de configuración que deben revisarse periódicamente para mantener el firewall limpio, eficiente y fácil de gestionar. Con el tiempo, las configuraciones de firewall crecen de forma natural a medida que se añaden nuevas reglas, objetos, VPN y servicios. Sin un mantenimiento periódico, las entradas obsoletas o no utilizadas pueden acumularse, aumentando la carga administrativa y dificultando la resolución de problemas.
Este informe destaca los elementos de configuración que pueden requerir atención, como reglas de firewall deshabilitadas o no utilizadas, políticas NAT inactivas, objetos de dirección y servicio no utilizados, servicios de seguridad caducados y otros elementos de configuración que ya no se utilizan activamente. También identifica configuraciones que podrían beneficiarse de una optimización o limpieza.
El propósito de este informe no es recomendar la eliminación automática de cada elemento enumerado. En su lugar, proporciona a los administradores una visión estructurada de los componentes de configuración que deben verificarse antes de realizar cualquier cambio. Algunos objetos o reglas pueden seguir siendo necesarios para proyectos futuros, entornos temporales, procedimientos de recuperación ante desastres o servicios de uso poco frecuente.
El mantenimiento periódico ofrece varios beneficios importantes:
- Reduce la complejidad de la configuración y mejora la legibilidad.
- Facilita considerablemente la resolución de problemas y las auditorías.
- Ayuda a identificar elementos de configuración obsoletos u olvidados.
- Reduce el riesgo de errores de configuración accidentales.
- Mejora la gestionabilidad a largo plazo del firewall.
- Respalda un entorno de seguridad bien documentado y mantenido de forma profesional.
Un firewall bien mantenido es más fácil de administrar, más fácil de auditar y proporciona una base más sólida para futuros cambios de configuración y mejoras de seguridad.

# Convenciones de nomenclatura de objetos de dirección

## Explicación

**Importancia de las convenciones de nomenclatura comunes para los objetos de dirección**
La gestión eficaz de los objetos de dirección del firewall es esencial para mantener un entorno de red seguro y bien organizado. Un factor clave que contribuye a esta eficacia es el uso de convenciones de nomenclatura coherentes y significativas.

**Claridad y administración más rápida**
Cuando los objetos de dirección siguen estándares de nomenclatura uniformes, los administradores pueden reconocer de inmediato su propósito, ubicación o servicio relacionado sin necesidad de revisar datos de configuración detallados. Esto reduce el tiempo dedicado a la resolución de problemas, la actualización de reglas o los cambios de políticas, y minimiza la posibilidad de modificar el objeto incorrecto.

**Coherencia y precisión en la configuración**
Los formatos de nomenclatura estandarizados establecen uniformidad en todas las configuraciones. Esto evita duplicaciones, previene confusiones y reduce los errores de configuración que podrían dar lugar a permisos de acceso no deseados o flujos de comunicación bloqueados. Los nombres predecibles permiten a los administradores interpretar las políticas del firewall de forma más eficiente y precisa.

**Mejor colaboración y transferencia de conocimiento**
Las convenciones de nomenclatura coherentes permiten a los equipos trabajar con un entendimiento compartido. Los administradores que no están familiarizados con una configuración pueden, aun así, interpretar de inmediato el uso de los objetos y sus dependencias. Esto mejora la colaboración, simplifica la incorporación de nuevo personal y garantiza la continuidad a lo largo del tiempo, incluso cuando cambian las responsabilidades.

**Conclusión**
Las convenciones de nomenclatura comunes fortalecen la mantenibilidad, la precisión y la transparencia de las configuraciones del firewall. Al mejorar la claridad, reducir la complejidad de la configuración y fomentar la colaboración, contribuyen significativamente a una administración de red segura y sostenible.

## Convenciones de nomenclatura de objetos de dirección

| Address Object Name old | Address Object Name new |
|---|---|
| SSLVPN-NetExtender Range | AO-SSLVPN-NetExtender Range-192.168.168.100 |
| WAN-GoogleDNS-8.8.8.8 | AO-WAN-GoogleDNS-8.8.8.8 |
| WAN-TZ570-10.10.10.254 | AO-WAN-TZ570-10.10.10.254 |
| LAN-UDS-Analytics-10.100.10.50 | AO-LAN-UDSAnalytics-10.100.10.50 |
| WAN-GoogleDNS-8.8.8.8-2 | AO-WAN-GoogleDNS2-8.8.8.8 |
| TZ570 LAN | AO-VPN-TZ570 LAN-10.10.10.0 |
| Server | AO-LAN-Server-10.99.10.223 |
| MartinSchmitz | AO-LAN-MartinSchmitz-1.1.1.1 |
| KlausMeier | AO-LAN-KlausMeier-1.1.2.2 |
| FTP Server Private | AO-LAN-FTP Server Private-172.20.20.101 |
| FTP Server Public1 | AO-WAN-FTP Server Public1-10.10.20.2 |
| Test | AO-LAN-Test-10.100.10.99 |
| Test1 | AO-LAN-Test1-10.100.10.99 |
| Test4 | AO-LAN-Test4-10.100.10.99 |
| x0 und x6 subnet | AO--x0 und x6 subnet-0.0.0.0 |
| Test12 | AO-LAN-Test12-10.100.10.99 |
| Test_111 | AO-LAN-Test_111-10.100.10.111 |
| Test_112 | AO-LAN-Test_112-10.100.10.112 |
| Test_113 | AO-LAN-Test_113-10.100.10.113 |
| Test_114 | AO-LAN-Test_114-10.100.10.114 |
| Test_115 | AO-LAN-Test_115-10.100.10.115 |
| Test_116 | AO-LAN-Test_116-10.100.10.116 |
| Test_117 | AO-LAN-Test_117-10.100.10.117 |
| Test_118 | AO-LAN-Test_118-10.100.10.118 |
| Test13 | AO-LAN-Test13-10.100.10.13 |
| Syslog Synology | AO-WAN-Syslog Synology-10.10.40.50 |
| Test Group | AO--Test Group-0.0.0.0 |

# Objetos de dirección duplicados

## Explicación

**Análisis de objetos de dirección duplicados**
Los objetos de dirección duplicados -donde nombres diferentes hacen referencia a la misma dirección IP o red- pueden generar múltiples desafíos operativos y de seguridad en los firewalls.
**1. Mayor complejidad y riesgo de configuración incorrecta**
Cuando varios objetos hacen referencia al mismo destino, los administradores pueden no saber cuál utilizar. Esto complica la creación de políticas, aumenta la probabilidad de usar el objeto incorrecto y ralentiza las auditorías, la resolución de problemas y los procesos de cambio.
**2. Políticas conflictivas o superpuestas**
Diferentes objetos que representan la misma IP pueden usarse de forma inconsistente entre reglas. Una regla puede permitir el tráfico mientras otra lo bloquea, lo que provoca un comportamiento impredecible y dificulta el análisis de políticas.
**3. Aplicación inconsistente de la seguridad**
Cuando diferentes equipos o administradores crean objetos separados para el mismo recurso, la aplicación de políticas se fragmenta. Esto puede provocar accesos no intencionados o una cobertura parcial de las políticas, debilitando la postura de seguridad general.
**4. Mayor esfuerzo de mantenimiento**
Cualquier cambio que afecte a un objeto duplicado debe actualizarse en todas las referencias de las políticas. Pasar por alto una ubicación puede provocar reglas obsoletas, brechas en las restricciones de acceso o desviación de la configuración.
**Mejores prácticas recomendadas**
– *Consolidar los objetos de dirección:* identificar entradas duplicadas y sustituirlas por un único objeto que represente cada IP, subred o recurso.
– *Utilizar convenciones de nomenclatura claras:* los nombres deben reflejar el propósito o la identidad del recurso, mejorando la consistencia y la legibilidad.
– *Realizar auditorías periódicas:* la limpieza periódica reduce la redundancia y mejora la calidad de las políticas.
– *Documentar el uso y la propiedad:* una documentación adecuada ayuda durante el mantenimiento y evita la recreación de objetos innecesarios.

La limpieza de objetos de dirección duplicados mejora la claridad de las reglas, simplifica la administración de políticas, reduce los errores operativos y contribuye a una configuración de seguridad más sólida y predecible.

## Duplicate Address Objects

| IP | Name |
|---|---|
| - no se encontraron registros - | |

# Registro externo

## Explicación

El registro/telemetría externa en un firewall (por ejemplo, Syslog, IPFIX/NetFlow, traps SNMP) es importante porque el firewall es uno de los pocos dispositivos que puede observar de manera fiable quién habló con quién, cuándo, cómo y qué se bloqueó o permitió. Sin exportar esas señales, esencialmente se está operando a ciegas: es posible que se siga estando protegido por la política, pero se pierde la capacidad de detectar, investigar y demostrar lo que ocurrió.
Desde una perspectiva de seguridad, los registros externos son la base para la detección y respuesta a incidentes. Los ataques rara vez se anuncian con una única alarma evidente. Aparecen como patrones: fallos de inicio de sesión repetidos, anomalías VPN, coincidencias de políticas, conexiones salientes inesperadas, movimiento lateral o tráfico hacia destinos sospechosos. Un SIEM o una plataforma de registros puede correlacionar estos patrones entre fuentes (firewall + endpoints + identidad + servidores). Los eventos del firewall a menudo proporcionan el primer indicador de alta calidad de que algo va mal, y la telemetría de flujo (NetFlow/IPFIX) proporciona la "narrativa de red" necesaria para comprender el alcance y el impacto.
La recopilación externa también es crítica para la forense y la responsabilidad. Los firewalls tienen una retención de registros locales limitada y pueden perder datos durante reinicios, actualizaciones o rotación de almacenamiento. El registro centralizado preserva la evidencia durante períodos más largos, respalda los requisitos legales/normativos y permite informes fiables. En la práctica, muchas investigaciones comienzan días o semanas después del compromiso inicial. Si los registros solo se conservaran localmente, el período de tiempo clave podría haber desaparecido ya.
Operativamente, la telemetría mejora la estabilidad y la resolución de problemas. La supervisión SNMP y las traps proporcionan alertas tempranas sobre presión de CPU/memoria, errores de interfaz, inestabilidad de túneles o saturación de recursos, problemas que pueden parecer "interrupciones aleatorias" a menos que se disponga de datos de series temporales. Los registros de flujo ayudan a validar el uso del ancho de banda, identificar a los principales generadores de tráfico, detectar errores de configuración (por ejemplo, enrutamiento asimétrico) y confirmar si un cambio de política tuvo realmente el efecto previsto.
Finalmente, el registro/telemetría externa respalda la mejora continua. Permite medir la eficacia de las políticas, ajustar las reglas demasiado permisivas o ruidosas, e identificar TI en la sombra o servicios de riesgo. En resumen: exportar registros y telemetría del firewall convierte el firewall de una caja que "bloquea el tráfico" en un control que se puede verificar, auditar y operacionalizar, lo cual marca la diferencia entre tener controles de seguridad y tener garantía de seguridad.

## Registro externo

| Central Management | |
|---|---|
| Central Management (NSM / GMS): | off |
| NSM ZeroTouch: | enabled |

| Syslog | |
|---|---|
| Syslog Server Name: | n/a |
| Syslog Standby Server Name: | n/a |
| Syslog Server Port: | n/a |

| Netflow | |
|---|---|
| Netflow Internal: | n/a |
| Netflow External: | n/a |
| Netflow External Address: | n/a |

| Log to FTP Server | |
|---|---|
| Log to FTP Server: | |
| FTP Server IP Address: | n/a |

## Reglas de firewall deshabilitadas

### Explicación

**Importancia de las reglas de firewall deshabilitadas**
*Las reglas de firewall deshabilitadas, aunque no aplican activamente controles de seguridad, siguen siendo relevantes dentro de la configuración del firewall y de la estrategia de seguridad general.*
**Copia de seguridad operativa y reactivación rápida**
*Las reglas deshabilitadas suelen servir como alternativas de configuración predefinidas. Los administradores pueden deshabilitar temporalmente una regla durante el mantenimiento, la resolución de problemas o cambios planificados y volver a habilitarla más tarde sin necesidad de rediseñar o recrear la política. Esto garantiza una restauración rápida de los controles de seguridad previstos.*
**Documentación de configuración y auditoría**
*Las reglas inactivas ofrecen información sobre conjuntos de reglas históricos y decisiones de seguridad anteriores. Mantenerlas visibles respalda las auditorías, la verificación del cumplimiento y el análisis forense al preservar la intención de la configuración y el historial de cambios.*
**Flexibilidad para requisitos futuros**
*A medida que cambian los entornos de red, las reglas previamente deshabilitadas pueden volver a ser relevantes. Conservarlas permite una reactivación o modificación rápida sin tener que recrear desde cero políticas de acceso complejas u objetos de dirección.*
**Conclusión**
*Aunque las reglas de firewall deshabilitadas no filtran activamente el tráfico, siguen siendo puntos de referencia útiles para la recuperación operativa, la documentación de configuraciones anteriores y la adaptación rápida a futuros requisitos de seguridad. Deben revisarse periódicamente para garantizar que sigan siendo válidas, intencionadas y alineadas con los objetivos de seguridad actuales.*

## Reglas de firewall deshabilitadas



| Ena | A | Name | SrcZone | DstZone | SrcNet | DstNet | SrcSvc | DstSvc |
|---|---|---|---|---|---|---|---|---|

- no se encontraron registros -

*Número de registros: 0*

# Reglas de firewall no utilizadas durante mucho tiempo (IPv4)

## Explicación

**Reglas de firewall no utilizadas durante un período prolongado**
Las reglas de firewall que no se han utilizado durante un largo período de tiempo suelen indicar rutas de acceso obsoletas, servicios retirados o configuraciones heredadas que ya no son relevantes. Mantener reglas no utilizadas aumenta la carga administrativa y puede crear una exposición de seguridad innecesaria.

Las reglas inactivas pueden reactivarse o modificarse por error, concediendo potencialmente accesos no deseados o debilitando la aplicación de políticas. Eliminar o deshabilitar estas reglas ayuda a mantener una base de reglas limpia, mejora la manejabilidad y reduce la superficie de ataque general del entorno.

La revisión periódica de las reglas no utilizadas garantiza que solo permanezcan las rutas de acceso necesarias y activamente utilizadas, respaldando tanto la eficiencia operativa como las mejores prácticas de seguridad.

El siguiente informe muestra las reglas no utilizadas durante más de 365 días.

## Reglas de firewall no utilizadas durante mucho tiempo (IPv4)



| Ena | A | Name | SrcZone | DstZone | SrcNet | DstNet | SrcSvc | DstSvc | Last time hit |
|---|---|---|---|---|---|---|---|---|---|
| YES | A | Allow WAN1 | LAN | WAN | KlausMeier | any | any | any | Reglas de firewall no... |
| YES | A | Heating Maintenance | WAN | LAN | any | LAN Subnets | any | SSH | Reglas de firewall no... |
| YES | A | Test 24 | WAN | 060466 | any | any | any | OSPF | Reglas de firewall no... |
| YES | A | Test 25 | WAN | 060466 | any | any | any | POP3 (Retrieve E-Mail) | Reglas de firewall no... |
| YES | A | Test 23 | WAN | 060466 | any | any | any | MSN | Reglas de firewall no... |
| YES | A | Allow WAN1 | DMZ-unsec | WAN | any | any | Citrix UDP | any | Reglas de firewall no... |
| YES | A | Allow syslog | DMZ-unsec | DMZ-unsec | any | any | SSH Management | any | Reglas de firewall no... |
| YES | A | Test 22 | DMZ-unsec | DMZ-sec | any | any | any | MSN | Reglas de firewall no... |
| YES | A | Complicated Rule | DMZ-unsec | Test | any | any | Citrix UDP | any | Reglas de firewall no... |
| YES | A | Allow WAN1 | DMZ-sec | WAN | any | any | Enhanced TV | any | Reglas de firewall no... |
| YES | A | My Rule | DMZ-sec | DMZ-unsec | any | any | any | FTP Data | Reglas de firewall no... |
| YES | A | Test 17 | DMZ-sec | DMZ-unsec | any | any | any | HTTPS | Reglas de firewall no... |
| YES | A | Test 20 | DMZ-sec | DMZ-unsec | any | any | any | Kazaa / FastTrack | Reglas de firewall no... |
| YES | A | Test 21 | DMZ-sec | DMZ-unsec | any | any | any | Lotus Notes | Reglas de firewall no... |
| YES | A | Test 19 | DMZ-sec | DMZ-unsec | any | any | any | IKE | Reglas de firewall no... |
| YES | A | Test 18 | DMZ-sec | DMZ-unsec | any | any | any | ICMP | Reglas de firewall no... |
| YES | A | Rule6 | DMZ-sec | Test | any | Test13 | Citrix TCP | any | Reglas de firewall no... |
| YES | A | Rule10 | DMZ-sec | Test | WAN-GoogleDNS-8.8.8.8 | any | Direct Connect | any | Reglas de firewall no... |
| YES | A | Allow Citrix | any | | any | any | Citrix UDP | any | Reglas de firewall no... |
| YES | A | Allow FTP | any | | any | any | FTP | any | Reglas de firewall no... |
| YES | A | Allow management via ... | SSLVPN | LAN | SSLVPN-NetExtender Range | any | any | HTTPS Management | 2025-03-31 11:40:59 |

*- Las reglas añadidas automáticamente se excluyen de este informe*

*Número de registros: 21*

## Políticas NAT (traducción de direcciones de red) deshabilitadas (IPv4)

### Explicación

**Políticas NAT deshabilitadas y su impacto**
Las políticas NAT (traducción de direcciones de red) deshabilitadas en los firewalls pueden generar problemas operativos y de seguridad significativos dentro de una red. A continuación se presenta un resumen de los principales riesgos e implicaciones técnicas asociadas con las reglas NAT inactivas o eliminadas.

**1. Pérdida de segmentación de red**
Las políticas NAT respaldan la separación lógica entre redes internas y externas al traducir las direcciones IP internas antes de que el tráfico salga de la red.
**Riesgos potenciales:**
– *Exposición de IP internas:* sin NAT, los esquemas de direccionamiento internos pueden ser visibles externamente, haciendo accesibles dispositivos previamente aislados.
– *Aislamiento reducido entre zonas:* el NAT respalda el aislamiento entre segmentos LAN, DMZ y WAN. El NAT deshabilitado puede difuminar involuntariamente los límites de seguridad.

**2. Mayores riesgos de seguridad**
El NAT proporciona indirectamente una capa de seguridad al impedir conexiones entrantes no solicitadas hacia hosts internos.
**Posibles consecuencias:**
– Los atacantes pueden dirigirse directamente a los dispositivos internos
– Las restricciones basadas en el firewall pueden eludirse
– Los recursos internos se vuelven más fáciles de enumerar o escanear

**3. Fallos de comunicación**
Muchos flujos de comunicación de red asumen que el NAT está activo para la traducción y el enrutamiento.
**Cuando el NAT está deshabilitado:**
– Los dispositivos pueden perder el acceso a servicios externos
– Los usuarios pueden experimentar conectividad inconsistente
– La resolución de problemas se vuelve más compleja debido a fallos de enrutamiento o servicios inaccesibles

**4. Problemas con la conectividad multi-red y VPN**
Las VPN, el enrutamiento y las tecnologías de acceso remoto a menudo dependen del NAT para alinear los espacios de direcciones internas y externas.
**Riesgos clave:**
– Las sesiones de acceso remoto pueden fallar
– Puede producirse solapamiento de red cuando los espacios IP entran en conflicto
– Los sistemas externos no pueden enrutar correctamente el tráfico de retorno

**5. Desafíos en la aplicación de políticas y el monitoreo**
La lógica de control de acceso a menudo aprovecha el NAT para rastrear y clasificar los flujos.
**Consecuencias del NAT deshabilitado:**
– Capacidad reducida para supervisar o correlacionar el tráfico
– Dificultad para atribuir la actividad a dispositivos/usuarios específicos
– Brechas en la precisión del registro

**6. Mayor consumo de espacio IP público**
El NAT permite que muchos dispositivos internos compartan una o un pequeño grupo de direcciones IP públicas.
**Sin NAT:**
– Cada sistema puede requerir su propia IP enrutable
– El agotamiento de IPv4 se convierte en una preocupación operativa real

**Conclusión**
Las políticas NAT deshabilitadas pueden provocar fallos de enrutamiento inesperados, límites de protección debilitados y una mayor exposición de seguridad. En la mayoría de los entornos, el NAT no solo sirve para la traducción de direcciones, sino también como método para aplicar el aislamiento, la visibilidad de registro y un comportamiento de enrutamiento predecible. Para operaciones estables y seguras, las políticas NAT deben revisarse cuidadosamente, mantenerse adecuadamente y deshabilitarse solo en escenarios de diseño intencionados y bien controlados.

*- Las reglas añadidas automáticamente se excluyen de este informe*

## Políticas NAT (traducción de direcciones de red) deshabilitadas (IPv4)



| Ena | Name | Original Source | Translated Source | Original Destination | Translated Destination | Original Service | Translated Service |
|---|---|---|---|---|---|---|---|
| NO | Test disabled NAT | DMZ-sec Subnets | Original | Any | Server | Citrix UDP | Original |
| NO | My Rule | DMZ-unsec Subnets | Original | All WAN IP | DEAG_Test | Any | Original |
| NO | Deact 3 | FTP Server Private | FTP Server Public1 | Any | Original | Any | Original |

## Políticas NAT habilitadas y sin coincidencias (IPv4)

### Explicación

**Políticas NAT sin coincidencias de tráfico**
Este informe destaca las políticas NAT (traducción de direcciones de red) que están actualmente habilitadas pero no se han utilizado dentro del período monitoreado. Una política NAT sin coincidencias registradas generalmente indica que la regla ya no corresponde a flujos de tráfico activos o está asociada con servicios, redes o dispositivos que ya no están en uso.

**Posibles causas de políticas NAT no utilizadas**
– El servicio correspondiente ya no está activo
– Ha cambiado una referencia de dispositivo o red
– El enrutamiento fue rediseñado, dejando obsoleta esta traducción NAT
– Una regla temporal o relacionada con una migración nunca se eliminó

**Por qué importan las políticas NAT no utilizadas**
**1. Mayor complejidad de las políticas**
Las entradas NAT no utilizadas dificultan la comprensión y el mantenimiento de la configuración. Los administradores pueden dedicar tiempo adicional a evaluar reglas que ya no son relevantes, ralentizando la resolución de problemas y la gestión de cambios.

**2. Riesgo de activación accidental**
Una política NAT inactiva puede activarse si cambian las condiciones de la red o el enrutamiento. Esto podría exponer inadvertidamente dispositivos internos, alterar las asignaciones de direcciones o eludir las políticas de acceso previstas.

**3. Posible exposición de seguridad**
Aunque no se utilice, una regla NAT sigue definiendo una posible ruta de traducción. Si se activa involuntariamente, puede:
– revelar el direccionamiento interno
– habilitar conexiones entrantes o salientes no deseadas
– eludir los puntos de filtrado o inspección esperados

**4. Menor eficiencia operativa**
Los grandes conjuntos de reglas NAT aumentan la carga de trabajo administrativa y reducen la claridad de la configuración. Eliminar las entradas obsoletas da como resultado un conjunto de políticas más limpio y predecible, y reduce el riesgo operativo.

**Prácticas de mantenimiento recomendadas**
– Verificar periódicamente si las reglas NAT siguen siendo necesarias
– Documentar la propiedad y el propósito previsto de las reglas
– Eliminar las asignaciones no utilizadas o deshabilitarlas temporalmente para su validación
– Revisar las políticas NAT después de rediseños de red, migraciones o actividades de desmantelamiento

**Conclusión**
Las políticas NAT habilitadas sin actividad de tráfico suelen indicar objetos de configuración obsoletos o innecesarios. Limpiar las reglas no utilizadas reduce la complejidad, evita rutas de exposición no intencionadas y mejora la mantenibilidad y la postura de seguridad. La revisión periódica garantiza que la política del firewall refleje con precisión el comportamiento de red requerido y activo.

*- Las reglas añadidas automáticamente se excluyen de este informe*

## Políticas NAT habilitadas y sin coincidencias (IPv4)



| Ena | Name | Original Source | Translated Source | Original Destination | Translated Destination | Original Service | Translated Service |
|---|---|---|---|---|---|---|---|
| NO | Test disabled NAT | DMZ-sec Subnets | Original | Any | Server | Citrix UDP | Original |
| YES | Test 1 | DMZ-sec Subnets | Original | Any | CSE_Access_Tier_AIP_1 | Citrix TCP | Original |
| NO | My Rule | DMZ-unsec Subnets | Original | All WAN IP | DEAG_Test | Any | Original |
| NO | Deact 3 | FTP Server Private | FTP Server Public1 | Any | Original | Any | Original |
| YES | Default NAT Policy | Any | Any | Any | Any | Any | Original |

## Configuración WAN MTU

### Explicación

Esta sección comprueba si la configuración WAN MTU del firewall SonicWall está configurada de forma inusualmente baja.
Un valor de MTU demasiado bajo puede reducir la eficiencia de transmisión y afectar negativamente al rendimiento de la red.
Si se detecta dicha configuración, debe revisarse para confirmar que es técnicamente necesaria y no el resultado de una limitación de configuración innecesaria.

| | | | | |
|---|---|---|---|---|
| X1 | WAN | 1500 | ok | - |
| X5 | WAN | 1500 | ok | - |