# DESCIFRADO E INSPECCIÓN DE TRÁFICO CIFRADO

## Protección de alto rendimiento contra el uso malicioso del cifrado

Según el Informe de amenazas cibernéticas 2018 de SonicWall, el tráfico cifrado representa actualmente casi el setenta por ciento del total de las comunicaciones basadas en Web de una organización. Si bien el cifrado de las sesiones de Internet ofrece numerosas ventajas, como la protección de la privacidad y la integridad de la información personal en el intercambio de datos, también observamos una tendencia emergente menos positiva, y es que los creadores de malware utilizan el cifrado para ocultar sus ataques de los firewalls. Los perpetradores de ataques no solo pueden eludir los firewalls y aprovechar los puntos ciegos para introducir malware que les permita acceder directamente a cualquier red, sino que además utilizan tecnología TLS/SSL para ocultar tráfico de comando y control con el fin de manipular los sistemas comprometidos prácticamente desde cualquier lugar. Las organizaciones que no inspeccionan el tráfico cifrado pierden gran parte del valor de sus sistemas de firewall. No pueden ver el contenido del tráfico, detectar descargas de malware, identificar archivos dañinos ni ver transmisiones no autorizadas de información privilegiada a sistemas externos.

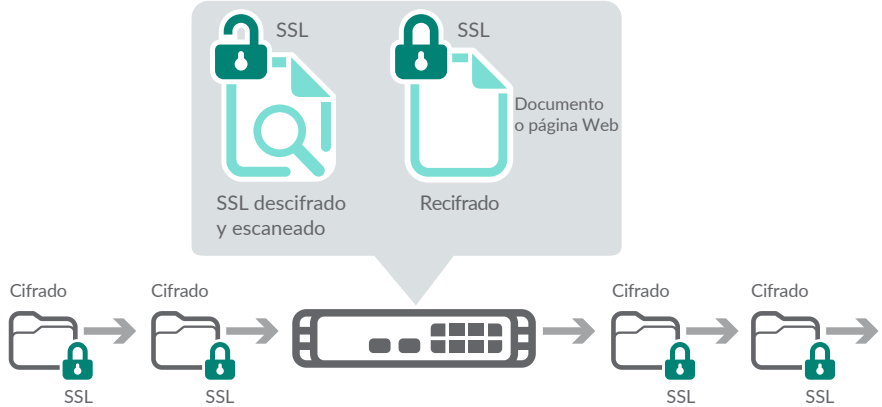
Las organizaciones pueden proteger sus redes contra estos riesgos de seguridad con la Inspección profunda de paquetes del tráfico TLS/SSL (DPI-SSL), y con un servicio adicional disponible en todos los dispositivos de seguridad de red NGFW (Firewall de próxima generación) y UTM (Gestión unificada de amenazas) de SonicWall. La tecnología DPI-SSL ofrece protección avanzada contra las amenazas cifradas utilizando el motor patentado de Inspección profunda de paquetes sin reensambaldo de SonicWall, que escanea una amplia variedad de protocolos de cifrado — como HTTPS, SMTPS, NNTPS, LDAPS, FTPS, TelnetS, IMAPS, IRCS y POPS, independientemente del puerto que se utilice.

Este servicio descifra el tráfico TLS/SSL, lo inspecciona en busca de amenazas y a continuación, si no se encuentran amenazas ni vulnerabilidades, lo cifra de nuevo y lo envía a su destino. Se trata de un servicio valiosísimo para proporcionar funciones críticas de seguridad y control de aplicaciones, así como para prevenir la filtración de datos.

Este servicio proporciona prestaciones críticas de seguridad, control de aplicaciones y prevención de filtración de datos para analizar el tráfico HTTPS y cifrado mediante TLS/SSL.

**Ventajas:**

- Aumento de la visibilidad del tráfico cifrado mediante SSL/TLS
- Bloqueo de las descargas de malware ocultas
- Frustración de la exfiltración de datos y de comunicaciones de comando y control
- Personalización de listas de inclusión y exclusión para el cumplimiento normativo



## Requisitos del sistema

| La inspección TLS/SSL está disponible con los siguientes firewalls de SonicWall: |
|---|
| SOHO / SOHO W |
| TZ300 / TZ300 W / TZ300P |
| TZ400 / TZ400 W |
| TZ500 / TZ500 W |
| TZ600 / TZ600P |
| NSa 2650 |
| NSa 3650 |
| NSa 4650 |
| NSa 5650 |
| NSa 6650 |
| NSa 9250 |
| NSa 9450 |
| NSa 9650 |
| SuperMassive 9800 |
| NSsp 12400 |
| NSsp 12800 |
| NSv 10 |
| NSv 25 |
| NSv 50 |
| NSv 100 |
| NSv 200 |
| NSv 300 |
| NSv 400 |
| NSv 800 |
| NSv 1600 |

**Partner Enabled Services**
¿Necesita ayuda para planificar, implementar u optimizar su solución SonicWall? Los Partners de servicios avanzados de SonicWall están cualificados para proporcionarle servicios profesionales de clase mundial. Si desea obtener más información, visite www.sonicwall.com/PES.

## Prestaciones

**Alto rendimiento y número de conexiones** — Los firewalls de próxima generación de SonicWall utilizan una arquitectura de procesadores avanzada y un número muy elevado de conexiones para mejorar el rendimiento DPI-SSL y la protección en todos los dispositivos conectados.

**Instalación segura y sencilla:** El servicio de descifrado e inspección DPI-SSL protege a los usuarios de la red con una configuración y una complejidad mínimas.

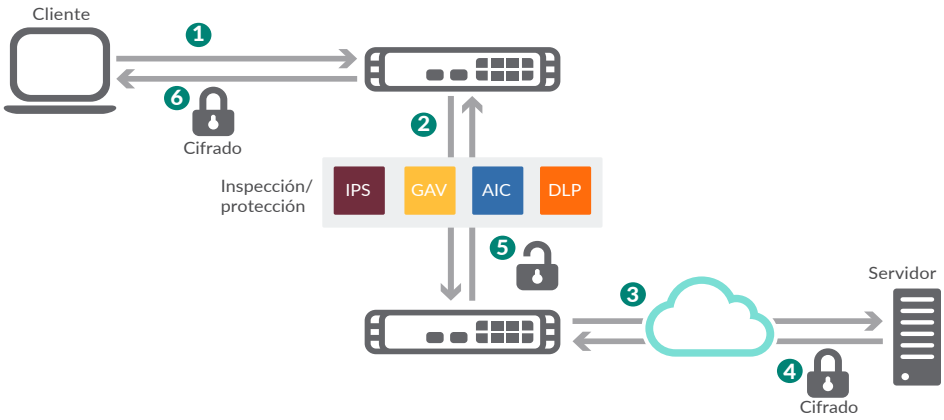
**Listas de inclusión/exclusión:** En implementaciones de tráfico elevado, los administradores pueden excluir las fuentes de confianza para maximizar el rendimiento de la red. Además, los administradores pueden determinar el tráfico que debe someterse a la inspección TLS/SSL mediante una lista personalizada en la que se especifican objetos de dirección, servicio, usuario o bien grupos con el fin de cumplir los requisitos legales y/o de privacidad.

**Modo de implementación de cliente:** Inspecciona el tráfico TLS/SSL cuando el cliente está en la LAN del firewall y accede al contenido situado en la WAN.

Una vez que el dispositivo ha descifrado e inspeccionado el tráfico cifrado, reescribe el certificado enviado por el servidor remoto y firma el certificado que acaba de crear con el certificado específico del usuario. Por defecto, esta es la entidad de certificación (CA) del dispositivo, aunque se puede seleccionar otro certificado.

**Modo de implementación de servidor:** Inspecciona el tráfico TLS/SSL cuando los clientes remotos se conectan a través de la WAN para acceder al contenido ubicado en la LAN del firewall, permitiendo al administrador configurar emparejamientos de un objeto de dirección y un certificado. Cuando el dispositivo detecta conexiones TLS/SSL al objeto de dirección, presenta el certificado emparejado y negocia el TLS/SSL con el cliente que se conecta. En este caso, el propietario del firewall de próxima generación de SonicWall es quien tiene los certificados y las claves privadas de los servidores del contenido de origen.

**Soporte completo:** Incluye prevención de intrusiones, prevención de malware, control de aplicaciones, filtrado de contenido/URL y prevención de comunicaciones de malware de comando y control.




### Inspección TLS/SSL — Modo de implementación de cliente

1. El cliente inicia el protocolo de enlace TLS/SSL con el servidor
2. El NGFW intercepta la solicitud y establece la sesión en el lugar del servidor utilizando sus propios certificados
3. El NGFW inicia el protocolo de enlace TLS/SSL con el servidor en nombre del cliente utilizando el certificado TLS/SSL definido por el administrador
4. El servidor completa el protocolo de enlace y crea un túnel seguro entre él y el NGFW
5. El NGFW vuelve a cifrar el tráfico y se lo envía al cliente
6. El NGFW descifra e inspecciona todo el tráfico procedente del cliente o dirigido al mismo en busca de amenazas e incumplimientos de las políticas

## Requisitos del sistema

La inspección TLS/SSL está disponible con los siguientes firewalls de próxima generación de SonicWall:

| FIREWALL | LICENCIA DE UN SOLO USO |
|---|---|
| SOHO / SOHO W | 01-SSC-0723 |
| TZ300 / TZ300 W / TZ300P | Incluido con la suscripción de servicios de seguridad |
| TZ400 / TZ400 W | Incluido con la suscripción de servicios de seguridad |
| TZ500 / TZ500 W | Incluido con la suscripción de servicios de seguridad |
| TZ600 / TZ600P | Incluido con la suscripción de servicios de seguridad |
| NS*a* 2650 | Incluido con la suscripción de servicios de seguridad |
| NS*a* 3650 | Incluido con la suscripción de servicios de seguridad |
| NS*a* 4650 | Incluido con la suscripción de servicios de seguridad |
| NS*a* 5650 | Incluido con la suscripción de servicios de seguridad |
| NS*a* 6650 | Incluido con la suscripción de servicios de seguridad |
| NS*a* 9250 | Incluido con la suscripción de servicios de seguridad |
| NS*a* 9450 | Incluido con la suscripción de servicios de seguridad |
| NS*a* 9650 | Incluido con la suscripción de servicios de seguridad |
| SuperMassive 9800 | Incluido con la suscripción de servicios de seguridad |
| NS*sp* 12400 | Incluido con la suscripción de servicios de seguridad |
| NS*sp* 12800 | Incluido con la suscripción de servicios de seguridad |
| NSv 10 | Incluido con la suscripción de servicios de seguridad |
| NSv 25 | Incluido con la suscripción de servicios de seguridad |
| NSv 50 | Incluido con la suscripción de servicios de seguridad |
| NSv 100 | Incluido con la suscripción de servicios de seguridad |
| NSv 200 | Incluido con la suscripción de servicios de seguridad |
| NSv 300 | Incluido con la suscripción de servicios de seguridad |
| NSv 400 | Incluido con la suscripción de servicios de seguridad |
| NSv 800 | Incluido con la suscripción de servicios de seguridad |
| NSv 1600 | Incluido con la suscripción de servicios de seguridad |

## Acerca de nosotros

SonicWall lleva más de 27 años combatiendo la industria del crimen cibernético y defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución automatizada de detección y prevención de brechas en tiempo real adaptada a las necesidades específicas de más de 500.000 organizaciones en más de 215 países y territorios, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.



SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Para más información, consulte nuestra página Web
www.sonicwall.com


DataSheet-DecryptionAndInspection-US-VG-MKTG4095