SERVICIO SECURITY HEALTH CHECK DE SONICWALL

Asegúrese de que su inversión en tecnología SonicWall está completamente optimizada para proteger su red

Visión general

El Servicio Security Health Check de SonicWall está diseñado para proporcionar a los clientes una revisión completa de su sistema de seguridad de red de SonicWall e identificar cualquier brecha de seguridad que requiera tomar medidas. Los partners de servicios avanzados proporcionan a sus clientes un informe de chequeo que incluirá tanto los resultados como posibles acciones recomendadas. Estas pueden incluir optimizaciones específicas de la configuración de SonicWall que pueden convertirse en proyectos complementarios de resolución o también sugerencias más generales centradas en la red que pueden convertirse en proyectos ulteriores de migración de red, destinados a establecer una topología más eficiente. Esta guía está pensada para ofrecer a los clientes de SonicWall una visión clara de las prestaciones del servicio Security Health Check.

Actividades incluidas

Security Health Check es un servicio de un día de duración que revisa la configuración existente para garantizar que se siguen las mejores prácticas en las siguientes áreas

Comprobación del estado global del dispositivo

- Versión del firmware y revisión de nuevas versiones
- Revisión de licencias

Comprobación de mejores prácticas de la seguridad de red

- Políticas NAT y redirección de puertos
- Normas de acceso del firewall
- Políticas de acceso entre zonas
- Configuración inalámbrica
- Configuración y políticas generales
- Gestión de usuarios y configuración de accesos
- Visualización y control de aplicaciones
- Túnel VPN y configuración SSL-VPN
- Gestión HTTP y WAN
- Configuración de protocolización

Comprobación de los servicios de seguridad

- Content Filtering Service (CFS)
- Gateway Anti-Virus (GAV)
- Intrusion Prevention Service (IPS)
- Anti-spyware
- Filtrado Geo-IP
- Filtrado botnet
- Inspección profunda de paquetes de tráfico SSL - DPI-SSL
- Inspección profunda de paquetes de tráfico SSH - DPI-SSH

El partner encargado de prestar el servicio Security Health Check también podrá formular recomendaciones en las siguientes áreas:

- Nuevas implementaciones de servicio (SSO, LDAP, autenticación de doble factor)
- Nuevas implementaciones de producto e integraciones de red
- Segmentación de red, cifrado en tránsito y planificación de acceso remoto (anexo)
- Planificación de talleres de mejores prácticas
- Migraciones de producto y traducciones de configuración

Actividades no incluidas

Security Health Check está diseñado como servicio de evaluación y validación de mejores prácticas de seguridad de un día de duración.
El ámbito del servicio está marcado por el tamaño y la complejidad del entorno del cliente.

Como tal, este servicio no incluye la optimización de la configuración en el emplazamiento del cliente, con la excepción de una posible sincronización de licencias o activación de Capture ATP, en caso de requerirse. Los servicios de resolución son proyectos complementarios basados en el informe de chequeo y sus resultados.

Las actividades incluidas en el servicio Security Health Check arriba mencionadas, se llevarán a cabo según los más altos estándares y se centrarán en las áreas más importantes del entorno del cliente y en los elementos considerados de mayor prioridad.

Tampoco está incluida la configuración de los siguientes servicios, aunque puede ofrecerse como actividad complementaria a petición del cliente:

- Configuración general e implementación
- Cliente Global VPN/SSL-VPN
- Configuración de Sonic Point
- Inicio de sesión único (SSO)
- Comprehensive Anti-Spam Service
- GMS
- Analyzer
- Seguimiento y solución de casos de soporte
- Autenticación LDAP/Radius
- Aceleración WAN
- Virtual Assist
- Enforced Client Anti-Virus
- Formación
- Sándwich de firewalls
- Alta disponibilidad/agrupación (clústeres)
- Realización de pruebas de funciones del producto

Informe Security Health Check

Al final del servicio de un día de duración, el cliente recibirá un informe de su partner de servicios avanzados SonicWall. Este informe documentará el estado de cada una de las configuraciones y servicios de seguridad revisados e incluirá recomendaciones para la mejora del sistema de seguridad. A continuación se incluye una tabla como ejemplo de un informe de chequeo.

Ejemplo de un informe: Security Health Check – NSA2600

MEJORES PRÁCTICAS	ESTADO PREVIO AL CHEQUEO	RECOMENDACIONES/CORRECCIONES IMPLEMENTADAS
Estado general del sistema		La conexión LDAP debería cambiarse a TLS. Actualmente ejecutándose en 389 sin protección.
Políticas de acceso entre zonas		Eliminar zonas no utilizadas (como WLAN, que tenía múltiples normas de acceso activadas).
Reconexión y equilibrio de carga WAN	No disponible	
Políticas de enrutamiento	No disponible	
Políticas NAT/Redirección de puertos		La asignación externa de puertos (NAT c/origen = cualquiera) debería estar limitada a IP de orígenes conocidos. Las conexiones RDP externas para el administrador de TI no deberían estar permitidas (en su lugar, IPSec/SSL-VPN debería estar configurado para permitir el acceso desde fuera de la RDP).
Configuración DHCP/DNS		Como primera opción se debería configurar un IP de servidor DNS interno.
Configuración inalámbrica	No disponible	
Normas de acceso del firewall		Se debería llevar a cabo una revisión de las normas existentes. Para las demás normas, habilite los servicios de protección Geo-IP y Botnet.
Visualización y control de aplicaciones		Habilitado; pendiente de reinicio. Esto facilitará una visión más detallada de los flujos, como flujos de inspección por país de origen.
Configuración del firewall		Habilitar la protección contra ataques TCP/UDP/ICMP.
Configuración del túnel VPN	No disponible	
Configuración SSL-VPN	No disponible	
Gestión remota	No disponible	
Gestión HTTP(S)		Mantener la gestión HTTP deshabilitada. Permitir solo HTTPS. Cambiar el puerto HTTPS a 8443 en caso de que se quiera utilizar SSL-VPN en el futuro (este utilizará TCP: 443).
Configuración Log/Syslog		Reforzar la longitud mínima de la contraseña. Esta debería cambiar de su valor por defecto de 1 a quizás 8.
Configuración de usuarios y accesos		Se debe personalizar Local Syslog. La protocolización de cada paquete permitido limitará su funcionalidad. Hemos puesto en orden la configuración Syslog actual. No obstante, para disponer de un historial más largo y unas mejores vistas, debería utilizarse una mejor solución de informe (p. ej. GMS/Analyzer). Puede implementarse Analyzer, ya que el conjunto de licencias actual incluye una licencia de Analyzer.
Alta disponibilidad	No disponible	El acceso del usuario se lleva a cabo a través de SSO/LDAP. El caso SR3974813 debería examinarse detenidamente con el soporte técnico si el problema sigue repitiéndose tras la actualización del firmware.
Acceso remoto VPN	No disponible	Para facilitar la redundancia y evitar los puntos únicos de fallo, las oficinas centrales (NSA2600) deberían configurarse en modo de alta disponibilidad.

SERVICIOS DE SEGURIDAD	ESTADO PREVIO AL CHEQUEO	RECOMENDACIONES/CORRECCIONES IMPLEMENTADAS
Antivirus en pasarela	Habilitado parcialmente	Configurar: CIFS/NetBios habilitada.
Intrusion Prevention Service	Habilitado	Habilitar Detectar todo para Alto, Medio, Bajo. Habilitar Impedir todo para Alto, Medio, Bajo. Configurar la redundancia de registros para Alto/Medio en 30 s.
Anti-spyware	Habilitado	Habilitar Detectar todo para Alto, Medio, Bajo. Habilitar Impedir todo para Alto, Medio, Bajo. Configurar la redundancia de registros para Bajo en 30 s.
Filtrado Geo-IP	Habilitado	Bloquear los países de origen de tráfico sospechoso localizados en los registros en los que no se lleva a cabo ninguna actividad comercial legítima.
Filtrado Botnet	Deshabilitado	Bloquear conexiones desde/hacia los servicios Botnet Command and Control con la habilitación de la protocolización.
Content Filtering Service	Habilitado	Además de las categorías bloqueadas por defecto, bloquear también las siguientes: Malware, Radicalización, Pay2Surf, Hackeo y Puenteo de proxys.
DPI-SSL	Deshabilitado	En caso de una distribución del certificado SonicWall a través de AD, es muy recomendable DPI-SSL. El 65 % del tráfico se pasa por alto al escanear sin DPI-SSL.
DPI-SSH	Deshabilitado; no existe licencia	SSH es el pilar fundamental para muchas configuraciones, transferencias de archivos y servicios VPN «in the wild». Es muy recomendable una inspección del tráfico DPI-SSL.
Capture ATP	Habilitado parcialmente	CIFS y tipos de archivo adicionales: PDF, Office, archivos. Bloquear el archivo hasta que se reciba un veredicto.

Observaciones

- Durante nuestra estancia en el emplazamiento, hemos implementado algunos de los cambios recomendados anteriormente. Sin embargo, la mayoría de ellos deberían llevarse a cabo durante un período de inactividad con la diligencia debida (haciendo un backup de la configuración/firmware antes de realizar cambios).
- El acceso remoto VPN es el método preferido para acceder a recursos internos/centralizados (como prestaciones internas de compartición de archivos o servidores internos de escritorios remotos). Con una solución de estas características, podrá aplicar al punto terminal cliente el más reciente parche o actualización para el sistema operativo, poner al día el software antivirus/anti-spyware de punto terminal con las últimas actualizaciones y restringir el acceso a recursos en caso de que el punto terminal cliente no cumpla con todos los criterios de la política de seguridad.
- La segmentación adecuada de la red con escaneo de tráfico entre zonas debería limitar aún más la posible difusión horizontal de amenazas.

Resumen

- Las redes segmentadas frenarán los ataques de filtraciones de datos.
- Impedir el movimiento lateral es ideal, ya que existe una mayor probabilidad de detectar una amenaza si esta permanece en el sistema más tiempo a la vez que se merma su capacidad de dañar al sistema.
- La segmentación de red impide que un sistema sin parches y vulnerable acceda a las demás máquinas de la red y las infecte (comportamiento típico del ransomware).

Puntos clave

SonicWall ayuda a segmentar la red, a cifrar el tráfico y a detectar y prevenir intrusiones. Asimismo, ofrece protección contra amenazas de día cero y ataques globales de exfiltración de datos y extorsión.

Estos servicios pueden reducir significativamente la superficie de ataque en sistemas protegidos y también la cantidad de recursos sujetos al estándar PCI (o cualquier otro estándar equivalente).

Requisitos para el cumplimiento de normas de seguridad

El servicio Security Health Check puede ayudar a los clientes a cumplir los requisitos PCI-DSS o RGPD.

Cumplimiento de normas de seguridad PCI-DSS

Requisitos

- No almacene datos de autenticación confidenciales una vez se haya completado el proceso de autorización de la tarjeta. Proteja el número de su tarjeta con cifrado.
- El almacenamiento reforzado de los datos de la tarjeta debe protegerse dentro de un perímetro de seguridad definido mediante un conjunto específico de controles que mantengan la seguridad de la red.
- La red debe estar también segmentada y protegida, lo cual incluye una separación de las redes inalámbricas con firewalls. Se recomienda utilizar elementos de seguridad adicionales, como la detección y prevención de intrusiones, además de otros mecanismos de alerta.
- Para el acceso remoto debe utilizar una autenticación de doble factor. Estos sofisticados controles de acceso también deben reforzarse con contramedidas de seguridad físicas, como el uso de cámaras y métodos de supervisión para el acceso a áreas restringidas.
- Se exige realizar pruebas de penetración, tanto anualmente como tras cambios importantes en el sistema. Además, se deben llevar a cabo escaneos de vulnerabilidad trimestrales tanto internos (red y aplicación) como externos.
- La validación solamente confirma que su sistema cumple las respectivas normas en el momento que se realizó el chequeo. Para gestionar su riesgo de filtraciones a largo plazo debe garantizar el cumplimiento continuo de las normas.

Cumplimiento de normas de seguridad del RGPD

- Auditar el enfoque actual de gestión de datos.
- Establecer la posición actual y los procesos existentes en torno a la protección de datos.
- Auditar el conjunto de datos de todos los clientes de la empresa, incluidas las áreas en las que la información personal identificable (PII) podría no estar protegida adecuadamente.

Con SonicWall, podrá:

- Segmentar la red e implementar puertas de acceso de seguridad entre módulos de negocio.
- Proteger datos en dispositivos móviles y oficinas remotas de forma similar a los datos gestionados de forma centralizada.
- Asegurar el acceso remoto y cifrar los datos en tránsito.
- Acceder al refuerzo de políticas para la compartición de archivos y otros servicios y recursos compartidos en la red.

Para obtener más detalles sobre nuestra oferta de servicios de partners, visite www.sonicwall.com o póngase en contacto con su partner de servicios avanzados SonicWall.

Acerca de nosotros

SonicWall lleva más de 25 años combatiendo la industria del crimen cibernético, defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 negocios globales en más de 150 países, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

Si tiene alguna duda sobre el posible uso de este material, póngase en contacto con nosotros:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Para más información, consulte nuestra página web.
www.sonicwall.com

Brochure-SecurityHealthCheck-IMAG-US-MKTG868

SONICWALL®