Verificación del descifrado IPS en Cisco Secure Access

Contenido

Problema

Al utilizar Cisco Secure Access con RAVPN (VPN de acceso remoto) a través de Secure Client, las organizaciones deben verificar si el descifrado y la inspección de IPS (Sistema de prevención de intrusiones) se realizan correctamente para el tráfico a sitios web específicos. El principal desafío es confirmar que los procesos de descifrado e inspección de TLS funcionan correctamente a través de métodos distintos de los registros de la interfaz de usuario de administración estándar, como la búsqueda de actividad. Entre los requisitos de verificación específicos se incluyen la identificación de comprobaciones de certificados en el lado del cliente o mecanismos de depuración/generación de informes que puedan admitir la validación de pruebas y proporcionar una confirmación adicional del funcionamiento de IPS más allá de la interfaz de gestión.

Entorno

- Cisco Secure Access (CSA) con funcionalidad RAVPN
- Cisco Secure Client para conexiones VPN de acceso remoto
- Funciones de descifrado e inspección de IPS habilitadas
- Tráfico TLS/SSL que requiere descifrado para inspección de seguridad
- Tráfico web desde clientes RAVPN a sitios web externos

Resolución

Existen dos métodos para verificar que el descifrado IPS y la inspección funcionan correctamente para el tráfico VPN de acceso remoto en Cisco Secure Access:

Método 1: Búsqueda de actividad de IU de gestión (método principal)

La función de búsqueda de actividad de la interfaz de gestión de Cisco Secure Access proporciona el método más fiable para confirmar las operaciones de descifrado e inspección de IPS. Esta interfaz muestra registros detallados y análisis que muestran cuándo los servicios de seguridad han descifrado e inspeccionado el tráfico.

Para acceder a la búsqueda de actividad:

Navegue hasta el panel de gestión de Cisco Secure Access y localice la funcionalidad de búsqueda de actividad para revisar los registros de inspección de tráfico y el estado de descifrado de sesiones de usuario específicas y sitios web de destino.

Para habilitar los registros de descifrado, esta configuración se puede habilitar en la configuración global:

Panel -> Seguro -> Directiva de acceso -> Valores predeterminados de regla y configuración global -> Configuración global -> Registro de descifrado.

Método 2: Verificación de certificados del lado del cliente

Como método de verificación adicional, puede realizar comprobaciones de certificados en el cliente para confirmar que se está descifrando el tráfico.

Cuando Cisco Secure Access descifra e inspecciona correctamente el tráfico TLS, presenta su propio certificado al cliente en lugar del certificado del sitio web original.

Para comprobar el descifrado mediante la inspección de certificados:

1. Compruebe el certificado del sitio web
Abra los detalles del certificado en el navegador y revise el emisor y el período de validez.

Si la CA raíz de Cisco Secure Access emite el certificado con un período de validez de ~10 días, indica el descifrado del sistema de prevención de intrusiones en el nivel de firewall.

Si la validez del certificado es de aproximadamente 5 días, indica descifrado basado en gateway web seguro.

2. Validar el emisor del certificado (denominación de DC)

Este método de verificación de certificados del cliente sirve como técnica de confirmación complementaria junto con el método de búsqueda de actividad principal, lo que proporciona una garantía adicional de que los procesos de descifrado IPS funcionan según lo previsto.

El sistema de prevención de intrusiones no descifra:

El descifrado del sistema de prevención de intrusiones se llevará a cabo si:

· Se habilita en la configuración global Y

· El sistema de prevención de intrusiones está habilitado para al menos una de las reglas de política de acceso (creo que aunque la regla está deshabilitada, esta condición sigue siendo aplicable)

Desea omitir un dominio del descifrado del sistema de prevención de intrusiones

Utilice el sistema proporcionado no descifrar lista y agregar dominio en el sistema proporcionado no descifrar lista.

or

Utilice el descifrado basado en el origen en Configuración global en Cisco Secure access:

NOTA: Esto funcionará si NO hay NINGUNA NAT de salida configurada en la configuración del túnel de red en Secure Access.

Causa

La necesidad de varios métodos de verificación surge del requisito de validar la aplicación de políticas de seguridad en entornos empresariales. Mientras que los registros de la interfaz de usuario de administración proporcionan una visibilidad completa, los métodos de verificación en el lado del cliente ofrecen puntos de confirmación adicionales que pueden ser útiles para las pruebas de conformidad, la resolución de problemas y los escenarios de validación en los que el

acceso directo a las interfaces de administración puede estar limitado o cuando se requieren varios puntos de verificación para los procedimientos de prueba exhaustivos.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).