Configuración de SSE Do Not Decrypt para el desvío del descifrado de IPS y SWG

Contenido

Problema

El tráfico HTTPS a los destinos de la categoría financiera sigue presentando un certificado SSE de Cisco en lugar del certificado del sitio web de origen, incluso después de agregar la categoría Finanzas o dominios específicos a una lista No descifrar (NoDescifrar) y aplicar la regla de acceso pertinente. Este comportamiento se observa cuando se accede a sitios a través de Zero Trust Access Client (TIA), lo que afecta específicamente al acceso a sitios web relacionados con la financiación, como https://onlinesbi.sbi.bank.in/, donde se requiere una visibilidad integral de los certificados.

El comportamiento esperado es que cuando se agrega un sitio o una categoría de contenido a la lista NoMIsta, el certificado del sitio web de origen se puede presentar en el navegador en lugar del certificado de Cisco SSE. Sin embargo, se sigue presentando el certificado SSE de Cisco, que indica que el descifrado del tráfico se sigue produciendo a pesar de la configuración de DND.

Entorno

- Cisco Secure Service Edge (SSE)
- Conectividad con Zero Trust Access Client (TIA)
- Descifrado IPS global activado
- IPS activo en políticas de acceso
- Categoría financiera configurada en la lista No descifrar dentro del perfil de seguridad
- Reglas de acceso aplicadas con los perfiles de seguridad correspondientes

Resolución

La resolución implica comprender que Cisco SSE realiza dos tipos distintos de descifrado y configurar los valores adecuados de No descifrar para ambos tipos de descifrado.

Introducción a los tipos de descifrado SSE

Cisco SSE realiza dos procesos de descifrado independientes:

- Descifrado SWG (gateway web segura): descifrado de proxy web
- Descifrado IPS: descifrado del sistema de prevención de intrusiones

Las entradas No descifrar configuradas dentro de un perfil de seguridad se aplican únicamente al descifrado SWG y no impiden el descifrado IPS. Cuando el descifrado IPS global está activado y IPS está activo en cualquier política de acceso, el descifrado IPS continúa produciéndose, lo que hace que el certificado de Cisco SSE se presente en el navegador.

Configuration Steps

Paso 1: Agregue sitios o categorías de contenido a la lista No descifrar proporcionada por el sistema.

La lista No descifrar proporcionada por el sistema se aplica a todos los perfiles IPS. Al agregar un sitio o una categoría de contenido a esta lista Suministrada por el sistema, se presenta el certificado del sitio web de origen, con lo que se evita de forma eficaz el descifrado IPS.

Paso 2: Verifique que no se requieran cambios adicionales en la política.

No es necesario hacer referencia a la lista No descifrar proporcionada por el sistema dentro de las políticas de acceso. La lista se aplica automáticamente a todos los perfiles IPS.

Pruebas de validación

Estos métodos de validación se pueden utilizar para confirmar la configuración correcta:

Método 1: Agregar dominio a la lista No descifrar proporcionada por el sistema

Si agrega el dominio específico a la lista No descifrar proporcionada por el sistema, se puede presentar el certificado del sitio web de origen en lugar del certificado de Cisco SSE.

Método 2: Desactivar temporalmente el descifrado IPS global (sólo para pruebas)

Si se desactiva temporalmente el descifrado IPS global, también se verá el certificado de origen para el sitio probado, lo que confirma que el descifrado IPS fue la causa de la presentación del certificado de Cisco SSE.

‘Resultados esperados’

Después de la configuración correcta:

- Los sitios o categorías de contenido agregados a la lista No descifrar proporcionada por el sistema presentan sus certificados de sitio web de origen.
- Tanto el descifrado SWG como el IPS se omiten para los sitios o categorías especificados.
- El navegador muestra el certificado del sitio web real en lugar del certificado de Cisco SSE.

Causa

El problema ocurre porque Cisco SSE realiza dos procesos de descifrado distintos: Descifrado SWG y descifrado IPS. No descifrar entradas configuradas dentro de perfiles de seguridad, solo omitir el descifrado SWG. Cuando el descifrado IPS global está activado y IPS está activo en las políticas de acceso, el descifrado IPS continúa produciéndose de forma independiente, lo que hace que el certificado de Cisco SSE se presente en el navegador incluso cuando los sitios se incluyen en las listas de perfiles de seguridad NoMlsta.

Para omitir completamente ambos tipos de descifrado, se deben agregar sitios o categorías de contenido a la lista No descifrar proporcionada por el sistema, que se aplica a todos los perfiles IPS y evita que se produzca el descifrado SWG e IPS.

Contenido relacionado

- Crear lista efectiva de no descifrado para acceso seguro
- Solución de problemas y recopilación de información básica para un acceso seguro
- 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).