

Manejo del Error de Certificado de Descifrado SSL en Secure Access

Contenido

Problema

Los usuarios están experimentando páginas de error relacionadas con certificados cuando el descifrado SSL está habilitado en Cisco Secure Access. Se han recibido múltiples consultas con respecto a tres tipos específicos de errores de certificados:

- Errores de certificado de servidor de origen caducado
- Errores de discrepancia de CN/SAN del certificado en los que el nombre común o los nombres alternativos del asunto enumerados en el certificado no coinciden con el dominio al que se ha accedido
- Vínculo de lista de revocación de certificados (CRL) incrustado en el certificado del servidor de origen que causa problemas de conectividad

Estos errores de certificado son similares a las advertencias que normalmente se mostrarían en los exploradores web. Se plantea la cuestión de si Cisco Secure Access puede gestionar los errores relacionados con los certificados mostrando páginas de advertencia (similares a los navegadores o los filtros de contenido) y permitiendo el acceso después de mostrar la advertencia, o permitiendo el acceso en todos los casos. Además, es necesario comprender el comportamiento cuando se inhabilita el descifrado SSL y si el tráfico pasa a través independientemente de los problemas de certificado.

Entorno

- Cisco Secure Access: acceso a Internet (módulo de roaming, VA, DNS, SWG, PAC, IPS, certificados)
- Funcionalidad de descifrado SSL habilitada

- Varios dominios con problemas de validación de certificados
- Servidores de origen con varios problemas de certificados, incluidos vencimiento y discrepancia de dominio

Resolución

Limitaciones de manejo de errores de certificados

La gestión de errores relacionados con certificados no está disponible en Cisco Secure Access. El producto no admite:

- Presentación de páginas de advertencia de tipo explorador para problemas de certificados
- Configuración de control de errores de certificados específicos del dominio
- Gestión de errores personalizada basada en dominios de destino
- Páginas de advertencia de estilo de filtro de contenido con opciones de sustitución de usuario

Solución alternativa a la exclusión de descifrado SSL

El enfoque recomendado es excluir los dominios problemáticos del descifrado SSL mediante la configuración de descifrado del perfil de seguridad. Esto se puede configurar mediante:

Navegue hasta la sección Perfil de seguridad > Configuración de descifrado para excluir dominios específicos de la inspección SSL.

Cuando los dominios se excluyen del descifrado SSL, se produce este comportamiento:

- El tráfico de los dominios excluidos omite por completo la inspección SSL
- Secure Access no realiza la validación del certificado
- Los usuarios no encuentran páginas de error de certificado generadas por Secure Access

- Es posible que los errores del certificado original sigan estando visibles en el explorador del usuario si persisten los problemas del certificado

Comportamiento Descifrado SSL Desactivado

Cuando el descifrado SSL está deshabilitado para un dominio o globalmente, Cisco Secure Access transmite el tráfico (reenvío) independientemente de cualquier problema de certificado. El producto no inspecciona ni valida los certificados cuando el descifrado no está habilitado, lo que permite que todo el tráfico HTTPS pase de forma transparente.

Causa

Los errores de certificado se deben a problemas legítimos de validación de certificados en los servidores de origen, incluidos certificados caducados, discrepancias CN/SAN y problemas de conectividad de CRL. Cisco Secure Access realiza la validación de certificados como parte de su proceso de descifrado SSL y, cuando se producen estos fallos de validación, el producto genera páginas de error para evitar conexiones potencialmente inseguras. Este es el comportamiento de seguridad esperado de la función de inspección SSL.

Contenido relacionado

- [Documentación de configuración de Cisco Secure Access Decryption](#)
- [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).