Error de confianza SSL/TLS de Secure Client Umbrella Module durante el registro del dispositivo

Contenido

Problema

Durante la implementación de Cisco Secure Client con el módulo Umbrella, los dispositivos dejaron de sincronizarse con el panel y se informó de que estaban "inactivos". Los clientes afectados experimentaron errores de confianza SSL/TLS al intentar registrarse en devices.api.sse.cisco.com, lo que impidió el registro correcto del dispositivo y la cobertura de protección.

La interfaz de usuario mostró Umbrella como inactivo con estos mensajes de estado:

- Umbrella está inactivo.
- Actualmente no está protegido por el gateway web seguro.
- El gateway web seguro no tiene licencia / está deshabilitado.

Las conclusiones del diagnóstico revelaron una falla de confianza de SSL/TLS uniforme durante el registro con este mensaje de error en los registros de Secure Client:

```
[ERROR] < 10> Device Registration: Registration failed against https://devices.api.sse.cisco.com/deploy
```

Entorno

- Implementación del módulo Cisco Secure Client con Umbrella en más de 2000 terminales
- Infraestructura SD-WAN con políticas de ruta

- Túneles Umbrella heredados en su lugar
- Configuración de la red que permite todos los destinos requeridos según la documentación de Cisco
- No hay ningún descifrado SSL activo para los destinos de Cisco en el perímetro

Resolución

La resolución implicaba identificar y corregir un problema de configuración de ruteo que estaba causando que el tráfico de registro del dispositivo fuera mal dirigido a través de los túneles Umbrella heredados.

Identificación de causa raíz

El análisis de los datos de captura de paquetes reveló que el certificado TLS presentado para la conexión API era un certificado de Cisco Umbrella en lugar del certificado esperado de Cisco Secure Access/Let's Encrypt. Identifique la dirección IP para devices.api.sse.cisco.com.

Investigaciones adicionales identificaron una política de ruta SD-WAN que coincidía con la subred 146.112.0.0/16, lo que hacía que el tráfico a devices.api.sse.cisco.com se enrutara a túneles Umbrella heredados en lugar del destino previsto.

Cambios de configuración

Para resolver el problema, se tomaron las siguientes medidas:

- Paso 1: Elimine las rutas estáticas problemáticas. Las rutas estáticas que apuntan 146.112.0.0/16 a los túneles Umbrella heredados se eliminaron de la configuración SD-WAN.
- Paso 2: Valide la conectividad. Después de eliminar las rutas estáticas, se probaron los clientes afectados para asegurarse de que pudieran conectarse y registrarse correctamente en devices.api.sse.cisco.com.

Verificación

La cadena de certificados esperada para devices.api.sse.cisco.com debe aparecer como se muestra a continuación:

```
openssl s_client -connect devices.api.sse.cisco.com:443
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R13
verify return:1
depth=0 CN = api.sse.cisco.com
verify return:1
---
Certificate chain
 0 s:CN = api.sse.cisco.com
   i:C = US, O = Let's Encrypt, CN = R13
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar  5 14:13:56 2026 GMT; NotAfter: Jun  3 14:13:55 2026 GMT
 1 s:C = US, O = Let's Encrypt, CN = R13
   i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT
```

Después de implementar los cambios de configuración, los clientes afectados se conectaron y registraron correctamente, y la implementación se completó correctamente.

Causa

La causa raíz fue una política de ruta SD-WAN que coincidió con la subred 146.112.0.0/16, lo que provocó que el tráfico de registro de dispositivos destinado a devices.api.sse.cisco.com (146.112.59.104) se enrutara incorrectamente a través de los túneles Umbrella heredados. Esto dio lugar a la presentación de un certificado TLS incorrecto (certificado de Cisco Umbrella en lugar del certificado esperado de Cisco Secure Access/Let's Encrypt), lo que provocó errores de confianza SSL/TLS durante el proceso de registro del dispositivo.

Contenido relacionado

- Documentación de los requisitos de red de Cisco Secure Client

- 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).