

El acceso a Internet falla cuando el servicio Secure Client Umbrella SWG Agent está activo

Contenido

Problema

Cuando el servicio Cisco Secure Client - Umbrella SWG Agent se ejecuta en un portátil Dell con Windows, los usuarios no pueden acceder a ningún sitio web. Una vez detenido el servicio Umbrella SWG Agent, se restaura el acceso web normal. El problema ocurre con Cisco Secure Client versión 5.1.14.145, que incluye los módulos AnyConnect VPN y Umbrella. El archivo OrgInfo.json está presente en el directorio esperado y el certificado de CA raíz de Cisco Secure Access está instalado en el almacén de certificados raíz de confianza.

Entorno

- Producto: Cisco Secure Client (módulos AnyConnect VPN y Umbrella)
- Versión del software: 5.1.14.145
- Sistema operativo: Windows (portátil Dell)
- Servicio Umbrella SWG Agent habilitado/deshabilitado
- OrgInfo.json presente en %ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json
- CA raíz de Cisco Secure Access instalada en el almacén Entidades de certificación raíz de confianza
- Seguridad de DNS/Web activada en el panel de acceso seguro
- Perfil de seguridad asignado con el descifrado habilitado

Resolución

El problema se resolvió identificando y corrigiendo un error de sincronización del protocolo de tiempo de red (NTP) en el dispositivo cliente. La incapacidad de sincronizar el tiempo impidió la comunicación segura requerida por el agente SWG de Umbrella para el proxy del tráfico web, lo que dio como resultado paquetes de restablecimiento de TCP (RST) y la pérdida de acceso web. Una vez restaurada la sincronización de NTP, el acceso web funcionaba normalmente con el agente SWG activo.

Siga este completo flujo de trabajo de solución de problemas.

Paso 1: Verificar la configuración y los requisitos previos

- Asegúrese de que OrgInfo.json esté ubicado en
%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json.

- Confirme que la CA raíz de Cisco Secure Access está presente en el almacén de entidades emisoras de certificados raíz de confianza.
- Compruebe que la seguridad de DNS/Web está activada en el panel de acceso seguro.
- Verifique que el perfil de seguridad asignado tenga el descifrado habilitado.

Paso 2: Capture y analice el tráfico de red

Obtenga una captura de paquetes del tráfico del cliente dirigido al proxy SWG para identificar comportamientos anormales, como paquetes de reinicio TCP inesperados.

Descripción de la captura de paquetes que muestra el problema:

The packet capture revealed that TCP reset (RST) packets were being sent to the client, disrupting the

Paso 4: Validar las reglas del firewall del perímetro

- Inspeccione las reglas de firewall perimetral para asegurarse de que el tráfico entrante y saliente de los servidores SWG esté permitido en la interfaz de entrada.

Paso 5: Ejecutar el diagnóstico de sistemas y protocolos

Ejecute este comando en el cliente para verificar si hay errores de sincronización NTP:

```
curl ipinfo.io
```

Descripción del resultado del diagnóstico:

The output indicated NTP timing was out of sync on the client device.

Causa

La causa raíz fue un error en la sincronización NTP (protocolo de tiempo de red) en el dispositivo cliente. Este problema de sincronización impidió la comunicación segura entre el cliente y el servicio de proxy SWG de Umbrella, lo que dio lugar a paquetes de restablecimiento de TCP y a la pérdida de acceso web cuando el servicio SWG Agent estaba activo. La resolución del problema de sincronización de NTP restauró el funcionamiento correcto del agente SWG de Umbrella, permitiendo que el tráfico web se procesara de forma segura.

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).