Retos de la Configuración de la Tunelización Dividida de Secure Access

Contenido

Problema

Al configurar la función Cisco Secure Access (TIA) para el tráfico de túnel dividido, se encontraron varias complicaciones durante el proceso de configuración que impidieron una implementación adecuada:

- Retos de identificación del tráfico: Al configurar TIA para la tunelización dividida, todo el tráfico VPN debe excluirse de la inspección de seguridad de Internet. La identificación de los flujos de tráfico requeridos resultó difícil, y algunas URL de redirección fueron particularmente difíciles de rastrear y categorizar.
- Restricciones de tráfico de autenticación: Ciertos escenarios de túnel dividido requerían que el tráfico de autenticación se excluyera del proxy. Sin embargo, en función de las políticas existentes, el tráfico relacionado con la autenticación no se podía omitir del proxy, lo que provocaba conflictos de políticas.
- Riesgos de seguridad al desconectar la VPN: El tráfico de túnel dividido queda expuesto a la Internet abierta cuando la VPN se desconecta, lo que genera riesgos de seguridad adicionales que deben tenerse en cuenta durante la configuración.

Durante el proceso también se observaron otros problemas de configuración que requerían un análisis y una resolución más detallados.

Entorno

- Familia de productos: SECACCS (acceso seguro)
- Tecnología: Cisco Secure Access (TIA) con función de túnel dividido
- Configuración: Situaciones de tráfico de túnel dividido con políticas existentes

- Autenticación: Gestión del tráfico de autenticación basada en proxy
- Seguridad de la red: Requisitos de inspección de seguridad de Internet para tráfico VPN

Resolución

En función de los retos de configuración identificados con la tunelación dividida de Cisco Secure Access, se envió una solicitud de función completa para abordar las limitaciones identificadas y los conflictos de políticas.

Envío de solicitud de característica

Se ha abierto una solicitud de característica (CSE-I-5636) que se ha enviado al equipo de ingeniería correspondiente para que la revise a fin de hacer frente a estos retos de configuración:

- Capacidades mejoradas de identificación del tráfico para la exclusión del tráfico VPN de la inspección de seguridad de Internet
- Gestión mejorada de URL de redireccionamiento difíciles de rastrear y categorizar
- Resolución de las limitaciones del desvío del tráfico de autenticación con las políticas existentes
- Mitigación de riesgos de seguridad para la exposición del tráfico de túnel dividido durante la desconexión de VPN

Causa

Los retos de configuración se deben a las limitaciones actuales de la implementación de tunelación dividida de Cisco Secure Access (TIA), que no abordan adecuadamente los escenarios de implementación empresarial complejos. Específicamente, el sistema carece de suficiente control granular para la identificación y categorización del tráfico, tiene limitaciones para eludir el tráfico de autenticación cuando existen políticas, y no proporciona salvaguardias de seguridad adecuadas para el tráfico de túnel dividido cuando se interrumpen las conexiones VPN.

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).