Comportamiento del protocolo RAVPN de Cisco Secure Access con TLS/DTLS e IPsec (IKEv2) con configuración dual

Contenido

Problema

Cuando los protocolos TLS/DTLS e IPsec (IKEv2) están habilitados en Cisco Secure Access RAVPN con el protocolo principal establecido en IPsec (IKEv2), se producen errores de conexión al intentar establecer la conectividad VPN desde redes en las que se bloquea el tráfico IPsec (puertos UDP 500/4500). Secure Client adopta de forma predeterminada la opción IPsec en el menú desplegable de IU de cliente y no conmuta automáticamente por error a TLS/DTLS cuando falla la conectividad IPsec, lo que da como resultado errores de conexión e incapacidad para establecer la conectividad RAVPN desde entornos de red restringidos.

Entorno

- Cisco Secure Access RAVPN con configuración de protocolo dual
- Protocolos TLS/DTLS e IPsec (IKEv2) habilitados
- Configuración del protocolo principal configurada como IPsec (IKEv2)
- Secure Client con menú desplegable de selección de protocolos que contiene opciones IPsec y TLS independientes
- Entorno de red que bloquea el tráfico IPsec en los puertos UDP 500 y 4500

Resolución

El comportamiento observado es esperado y por diseño. Cisco Secure Access RAVPN no realiza la conmutación por fallo automática del protocolo de IPsec (IKEv2) a TLS/DTLS cuando ambos protocolos están habilitados y el protocolo principal encuentra problemas de conectividad.

Se requiere selección manual de protocolo

Al conectarse desde redes que bloquean el tráfico IPsec, los usuarios deben seleccionar manualmente el protocolo adecuado en Secure Client:

Paso 1: Abra la aplicación Secure Client

Paso 2: Localice el menú desplegable de selección de protocolo en la interfaz del cliente

Paso 3: Cambiar manualmente la selección de la opción IPSec a la opción TLS

Paso 4: Inicie la conexión VPN mediante el protocolo TLS/DTLS

Aclaración del comportamiento del protocolo

La configuración del protocolo principal en Cisco Secure Access RAVPN determina el protocolo predeterminado presentado en Secure Client, pero no habilita la funcionalidad de failover automático. Cuando TLS/DTLS e IPsec (IKEv2) están habilitados:

- Secure Client muestra opciones de protocolo independientes en el menú desplegable
- El cliente adopta de forma predeterminada la configuración del protocolo principal (IPsec en este caso)
- No se produce conmutación automática entre protocolos en función de las condiciones de conectividad de la red
- Los usuarios deben seleccionar manualmente el protocolo adecuado según su entorno de red

Causa

Cisco Secure Access RAVPN está diseñado sin funcionalidad de failover de protocolo automático. Cuando los protocolos TLS/DTLS e IPsec (IKEv2) están habilitados, el sistema requiere la selección manual de protocolos a través de la interfaz de Secure Client. La configuración del protocolo principal sólo determina la selección predeterminada en el menú desplegable del cliente y no implementa la lógica de conmutación automática cuando se encuentran problemas de conectividad con el protocolo principal.

Contenido relacionado

- Documentación de Cisco Secure Access
- 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).