

Problema de conectividad de túnel IPSec de acceso seguro con el router de redes Versa debido a la negociación ESN

Contenido

Problema

Durante la implementación de Cisco Secure Access en una sucursal que utilizaba el router de red vertical como dispositivo periférico, se detectaron problemas de conectividad a pesar de que ambos túneles IPsec parecían operativos. T

Los síntomas específicos incluyeron:

- Sin conectividad desde la sucursal a Cisco Secure Access
- El acceso a Internet a través de rutas estáticas no funciona
- Tráfico cifrado unidireccional observado (sólo de salida a Secure Access)
- Estadísticas del router que muestran los paquetes salientes que se están enviando pero no los paquetes entrantes recibidos
- Detección de puntos inactivos que funciona bidireccionalmente entre el router SD-WAN y Secure Access
- Valores del Índice de parámetros de seguridad (SPI) para la coincidencia correcta del tráfico saliente
- La inestabilidad del túnel (restablecimiento) no resolvió el problema de conectividad
- Las capturas de pantalla y las capturas de paquetes confirmaron la falta de tráfico entrante
- El cambio de los cifrados de túnel de CBC a GCM no resolvió el problema

La investigación reveló que el tráfico no podía descifrarse en el lado de Cisco debido a errores de suma de comprobación, que se rastrearon hasta el router Versa que negociaba la funcionalidad ESN (número de secuencia extendido).

Entorno

- Implementación de Cisco Secure Access
- Router Versa-Networks como dispositivo periférico
- Configuración del túnel de identidad IP
- Configuración de túnel IPsec con intentos de cifrado CBC y GCM

Resolución

La resolución implicaba la inhabilitación de la negociación del número de secuencia extendido (ESN) en el router Versa para evitar errores de suma de comprobación que estaban causando errores de descifrado en el centro distribuidor de Cisco Secure Access.

Pasos a resolver

Paso 1: Identificar la causa raíz

La investigación determinó que el router Versa estaba negociando ESN (número de secuencia extendido), lo que estaba provocando que el centro distribuidor de Cisco Secure Access recibiera errores de suma de comprobación y no pudiera descifrar los paquetes generados por ESN.

Paso 2: Desactivar ESN en router Versa

Póngase en contacto con el servicio de soporte de Redes Versa o con el administrador del router para desactivar las comprobaciones y la negociación ESN en la configuración del router Versa. Esto se dirige al conocido error de funcionamiento de Versa que hace que ESN se negocie incorrectamente.

Paso 3: Verificar la conectividad

Después de inhabilitar la negociación ESN, confirme que se ha establecido el flujo de tráfico bidireccional y que se ha restaurado la conectividad completa desde la sucursal a Secure Access e Internet.

Paso 4: Supervisar el flujo de tráfico

Verifique que las estadísticas de paquetes entrantes y salientes en el router muestren un flujo de tráfico adecuado en ambas direcciones, lo que confirma la resolución exitosa del problema de tráfico unidireccional.

Causa

La causa raíz se identificó como un error conocido de Redes Versa (identificador de error de soporte de Versa: 122437 - ESN no debe ser negociado por VOS) donde el router Versa negocia incorrectamente la funcionalidad del número de secuencia extendido (ESN) durante el establecimiento del túnel IPsec. Esta negociación ESN hace que el centro distribuidor de Cisco Secure Access reciba paquetes con errores de suma de comprobación, lo que evita el descifrado correcto y da como resultado un flujo de tráfico unidireccional. El router Versa envía paquetes salientes con éxito, pero el tráfico de retorno no se puede procesar correctamente debido a los errores de descifrado relacionados con ESN.

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).