Error de conexión del cliente VPN de Azure con Seguridad web de acceso seguro habilitada

Contenido

Problema

Después de migrar de Umbrella a SSE y habilitar Web Security con una licencia SIA recién asignada, las conexiones de Azure VPN Client no se pueden establecer para los usuarios cuando Web Security está habilitado. El problema de conectividad del cliente VPN de Azure afecta a todos los clientes, lo que les impide conectarse a la VPN. Cuando se desinstala Cisco Secure Access Client de los equipos cliente, se restaura la conectividad VPN, lo que indica que el cliente Secure Access está bloqueando la conexión a los servicios VPN de Azure.

Al deshabilitar la seguridad web o desinstalar Cisco Secure Access Client se restaura la conectividad VPN, pero esto afecta al acceso de los usuarios a los recursos a través de la VPN de Azure cuando se necesita protección de seguridad web.

Entorno

- Cisco Secure Access (anteriormente SIA) con Web Security activado
- Azure VPN Client
- Migración de Umbrella a SSE completada
- Licencia SIA asignada recientemente

Resolución

La resolución implica agregar la dirección IP pública del gateway de VPN de Azure a la lista de excepciones de SSE/SWG para evitar la intercepción del tráfico que bloquea las conexiones VPN.

Paso 1: Identificar la dirección IP de la puerta de enlace VPN de Azure

Determine la dirección IP pública del gateway VPN de Azure.

Paso 2: Agregar una excepción basada en IP a SSE/SWG

1.- Agregue la dirección IP pública del gateway virtual de Azure a la lista de excepciones SSE/SWG en el entorno de Cisco Secure Access.

2.- Inicie sesión en el panel de Cisco Secure Access. Haga clic en Connect (Conexión), End user Connectivity (Conectividad del usuario final), Internet Security (Seguridad de Internet) y Add exception (Agregar excepción). Esto evita que el gateway web seguro intercepte e inspeccione el tráfico destinado al gateway VPN de Azure.

Paso 3: Probar conectividad VPN

Después de aplicar la excepción basada en IP, pruebe la conexión VPN de Azure para comprobar que los clientes pueden establecer correctamente conexiones VPN con la seguridad web habilitada.

Paso 4: Ampliar prueba

Amplíe la prueba de la excepción basada en IP a usuarios adicionales de todo el entorno para garantizar una funcionalidad uniforme antes de considerar que la resolución ha finalizado.

Causa

El problema se produce porque el mecanismo de excepciones de gateway web seguro (SWG) requiere una búsqueda de DNS para que un dominio cree una entrada de caché de dominio a IP. Cuando el cliente VPN de Azure se conecta directamente a la dirección IP sin realizar una

consulta DNS para la dirección URL de VPN, el módulo SWG no puede asignar el dominio a la dirección IP. Como resultado, el SWG continúa inspeccionando e interceptando el tráfico a la dirección IP, evitando que se establezca la conexión VPN.

El análisis de captura de paquetes no mostró consultas de DNS para la URL de VPN ni tráfico de intercepción SWG visible para la IP del gateway de Azure, lo que confirma que el SWG estaba bloqueando la conexión debido a la falta de asignación adecuada de dominio a IP en su caché.

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).