El cliente VPN no puede verificar correctamente el error de modificación de la tabla de reenvío IP en Secure Client RAVPN Split-Tunnel/Default DNS

Contenido

Problema

Los usuarios de Mac experimentan errores intermitentes al intentar la autenticación CLI para aplicaciones internas mientras están conectados a Cisco Secure Client VPN. Los errores se presentan como errores de "host no encontrado" durante la autenticación CLI y al utilizar comandos como `curl`. Sin embargo, los comandos de resolución DNS como `nslookup` y `dig` se ejecutan correctamente. El problema se produce aleatoriamente y se puede resolver temporalmente volviendo a conectar la VPN, después de lo cual la conectividad funciona durante un breve período antes de que el problema vuelva a ocurrir. La VPN de túnel dividido está en uso y Cisco Umbrella está activo. El problema no se produce cuando se usa Palo Alto GlobalProtect VPN.

- Mensaje de error: "host no encontrado" en los comandos de autenticación CLI y `curl`.
- Mensaje de error: el cliente VPN no pudo comprobar correctamente las modificaciones de la tabla de reenvío IP. Problema de resolución del servidor de nombres de dominio (DNS) al conectar recursos privados
- comandos `nslookup` y `dig` correctos
- Conectividad intermitente después de volver a conectar VPN
- VPN de acceso remoto de túnel dividido y módulo Umbrella habilitado
- Problema reproducible solo con Cisco Secure Client VPN en dispositivos MacOS

Entorno

- Producto: Cisco Secure Client (CSC) con varios módulos
- Plataforma: dispositivos Mac corporativos
- Configuración del perfil VPN: perfil VPN de acceso remoto - omitir acceso seguro - Modo de túnel dividido y modo DNS seleccionados como "DNS predeterminado"
- Filtrado de DNS: habilitado para Cisco Umbrella
- Versiones de módulo:
    - Gestión de la nube v1.0.0.23
    - VPN AnyConnect v5.1.13.177
    - Umbrella v5.1.13.177

    - DART v5.1.13.17
    - Condición de firewall seguro v5.1.13.177
    - Network Visibility Module v5.1.13.177
- Datos de diagnóstico: paquetes DART recopilados para su análisis
- Observado solo en Cisco Secure Client VPN (no en Palo Alto GlobalProtect)

Resolución

- Durante la depuración de la configuración de túnel dividido del perfil VPN (`naic.org`) y la tabla de ruteo VPN AnyConnect en el lado del cliente, se observó este comportamiento:
    - Escenario de trabajo: al realizar una `nslookup` para los dominios locales no probados de Vault, las solicitudes DNS gestionadas por los servidores DNS configurados dentro del perfil VPN se resolvieron correctamente en direcciones 10.x. De forma correspondiente, la tabla de routing se actualizó con la IP resuelta (por ejemplo, 10.59.130.193) en rutas no seguras.
    - Escenario no operativo - Sin embargo, cuando las mismas solicitudes DNS fueron manejadas por el DNS local del sistema macOS (192.168.x.x) configurado en el adaptador untun4 y en0 en lugar de los servidores DNS definidos en el perfil VPN, este comportamiento se ha observado claramente desde la captura de paquetes mientras se detectó el problema.
    - los dominios privados se resolvieron a un rango de IP de 34.x.x.x , lo que provocó el problema de conectividad. La captura de Wireshark ayudó a identificar esta causa raíz subyacente del problema.
- Desde el punto de vista del diseño y la configuración, con una configuración de perfil VPN de túnel dividido, se recomienda utilizar DNS dividido en lugar de confiar en DNS del sistema local/DNS predeterminado.
- Además, se ha agregado la entrada `us-east-eks-amazonaws.com` para garantizar que el tráfico de este clúster EKS se dirija correctamente a través de la interfaz de túnel remoto.
- También se discutió que la interfaz RAVPN debe tener prioridad sobre el módulo Umbrella y no debe entrar en conflicto con el archivo `OrgInfo.json` que contiene el ID de organización de Umbrella.
- Durante nuestro proceso de solución de problemas, hemos hecho una instalación nueva del cliente CSC sin el módulo Umbrella, con ese escenario no pudimos ver el problema. Pude revisar desde la perspectiva de Umbrella también, el dominio raíz naic.org configurado en la lista de dominios internos para omitir Umbrella, lo que significa que las resoluciones de dominio local se reenvían al sistema DNS configurado macOS no interceptado por el módulo Umbrella DNS en la interfaz de loopback a nivel del núcleo.

Esto se alinea con la resolución del problema cuando no hay un módulo Umbrella en su lugar. Con la configuración de perfil VPN adecuada que incluye los dominios correctos en la regla de dirección de tráfico y la configuración de DNS dividido, no deberíamos ver el problema incluso con el modelo Umbrella está ENCENDIDO.

El usuario confirmó que el problema se resolvió después de modificar el modo DNS en el túnel de división y editó la configuración del perfil VPN.

Causa

Perfil VPN - Omitir acceso seguro - Se supone que el modo DNS debe establecer en Túnel dividido (las opciones más vistas de un caso práctico) e incluir todos los dominios de aplicación privados/internos en la configuración de DNS dividido para resolver el problema.

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).