Consideraciones sobre el comportamiento y el bloqueo de URL de la conexión VPN manual de TND de Secure Client

Contenido

Problema

Cuando se utiliza un perfil VPN con la función Trusted Network Detection (TND) configurada con la configuración Trusted Network establecida en Disconnect, los terminales ubicados dentro de la red de confianza todavía pueden establecer correctamente una conexión VPN cuando los usuarios inician conexiones manualmente mediante Cisco Secure Client.

Este comportamiento se produce a pesar de que la configuración de TND se haya configurado para desconectar las sesiones VPN cuando se detecta el terminal en una red de confianza.

Entre las preocupaciones específicas identificadas se incluyen:

- Las conexiones VPN manuales de los terminales de redes de confianza no se pueden controlar ni bloquear mediante la configuración TND estándar
- Incertidumbre sobre si la configuración de Cisco Secure Access (CSA) puede bloquear las conexiones VPN manuales desde terminales de redes de confianza
- Preguntas sobre la estabilidad de la URL de conexión del perfil VPN (xxxx.vpn.sse.cisco.com) y si cambia periódicamente, lo que podría afectar a las estrategias de bloqueo basadas en firewall

Entorno

- Implementación de Cisco Secure Access (CSA)
- Configuración del perfil de Cisco Secure Client con VPN

- Función Trusted Network Detection (TND) activada
- Configuración de red de confianza de TND configurada como Desconectar
- Terminales ubicados dentro de una red de confianza configurada
- Infraestructura de firewall para el control de acceso a la red

Resolución

Comprensión del comportamiento de TND con conexiones VPN manuales

El comportamiento observado es coherente con la funcionalidad documentada de Cisco Secure Client. Según la documentación de Cisco, TND no desconecta ni impide una sesión VPN que un usuario inicie manualmente mientras se encuentra en una red de confianza. Este es el comportamiento esperado, independientemente de los parámetros de configuración de TND.

Los principales aspectos técnicos son:

- La funcionalidad de desconexión automática de TND se aplica solo a las conexiones VPN establecidas automáticamente.
- Las conexiones VPN manuales iniciadas por los usuarios omiten el comportamiento de desconexión TND.
- No existe ninguna configuración de CSA para bloquear las conexiones VPN manuales de los terminales de red de confianza.

Estrategia de mitigación operativa

El método principal para controlar las conexiones VPN manuales desde los terminales de la red de confianza es a través de controles de nivel de red:

Paso 1: Implemente el bloqueo de URL del firewall: Configure el firewall de red de confianza para bloquear el acceso a la URL de conexión del perfil de VPN (xxxx.vpn.sse.cisco.com). Esto evita que los terminales de la red de confianza lleguen al extremo del servicio VPN.

Paso 2: Verificar estabilidad de URL: El identificador URL del perfil VPN (la parte xxxx) es específico de los arrendatarios y no se espera que cambie periódicamente. Esto proporciona un destino estable para las reglas de bloqueo del firewall.

Validación y pruebas

Las pruebas han confirmado que el bloqueo de la URL de conexión del perfil de VPN en el firewall de red de confianza impide correctamente que los terminales establezcan conexiones VPN, incluso cuando los usuarios intentan realizar conexiones manuales a través de Cisco Secure Client.

Causa

Este comportamiento se describe por diseño en la implementación de Cisco Secure Client TND. La función TND está diseñada específicamente para administrar conexiones VPN automáticas basadas en el estado de confianza de la red, pero intencionalmente no interfiere con las conexiones VPN manuales iniciadas por el usuario. Este diseño permite a los usuarios anular el comportamiento automático cuando sea necesario y, al mismo tiempo, proporciona detección de red y gestión de conexiones automatizadas para los casos prácticos habituales.

Contenido relacionado

- Guía de Cisco Secure Client Administrator - Configuración de TND
- 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).