Comportamiento de registro de DNS y registro de dispositivos con Cisco Secure Client en iOS para VPN de acceso remoto

Contenido

Problema

Cuando se utiliza Cisco Secure Client en iOS (iPad) para establecer una VPN de acceso remoto con Cisco Secure Access mediante la autenticación SAML a través de Microsoft Entra ID, los registros DNS no se muestran en Secure Access después de una conexión VPN correcta, aunque los registros web y de firewall se generen correctamente. Además, el iPad no aparece en Roaming Devices > Mobile Devices en el panel Secure Access después de establecer la conexión VPN.

Los síntomas específicos observados incluyen:

- Los registros de acceso remoto muestran eventos de "conexión" correctos en Secure Access
- Se generan registros web y de firewall que muestran la identidad de usuario autenticado SAML
- Los registros de DNS están completamente ausentes del registro de acceso seguro
- La información del dispositivo iPad no se incluye en la sección Dispositivos de roaming de acceso seguro
- Todo el tráfico fluye a través del túnel VPN (no se ha configurado ningún túnel dividido)

Entorno

- iPad con iOS 26.2
- Cliente seguro de Cisco

- Proveedor de identidad: ID de Microsoft Entra
- Conector de seguridad: No instalado
- Cisco Secure Access con autenticación SSO configurada
- implementación de autenticación SAML
- Perfil VPN configurado con el modo DNS establecido como predeterminado
- No se ha configurado ninguna tunelización dividida (todo el tráfico enrutado a través de VPN)
- Gestión de dispositivos móviles (MDM) utilizada para la distribución de perfiles

Resolución

Se espera el comportamiento observado para la configuración documentada. Cisco Secure Client en iOS funciona como un cliente VPN (equivalente de AnyConnect) y no incluye la funcionalidad equivalente de RSM de forma predeterminada. Security Connector es el componente equivalente a RSM en iOS que se requiere para el llenado de identidad de terminales y el control de DNS de estilo Umbrella.

Comprensión de la arquitectura

La ausencia de registros DNS y registro de dispositivos se debe a lo siguiente:

- Cisco Secure Client por sí solo proporciona conectividad VPN, pero carece de la funcionalidad de agente de terminal necesaria para la visibilidad de DNS
- Se necesita un conector de seguridad (equivalente a RSM en Windows) para el control DNS y el registro de dispositivos en Secure Access
- Sin el conector de seguridad, las consultas de DNS se gestionan mediante servidores DNS obtenidos mediante VPN sin visibilidad de Umbrella/Secure Access

Solución de registro de DNS mediante la dirección de tráfico

Para habilitar el registro de DNS sin instalar el conector de seguridad, configure el direccionamiento del tráfico para dirigir las consultas de DNS a los servidores DNS de Umbrella:

Paso 1: Configuración de Traffic Steering en Secure Access

Navegue hasta Traffic Steering > Add > Add a source y especifique la IP del servidor DNS como origen.

Paso 2: Tráfico DNS directo a servidores Umbrella

Configure el perfil VPN para que utilice servidores DNS de Umbrella (208.67.222.222 y 208.67.220.220) para garantizar que las consultas DNS sean visibles para Secure Access.

Paso 3: Validar registro DNS

Después de implementar la configuración del direccionamiento del tráfico, los registros de DNS deben ser visibles en el panel de acceso seguro para las sesiones VPN.

Configuración del modo DNS del perfil VPN

La configuración "Modo DNS" en el perfil VPN no está relacionada con la ausencia de registros DNS en esta configuración. Las sesiones RAVPN (VPN de acceso remoto) utilizan los servidores DNS obtenidos mediante VPN independientemente de esta configuración, y la visibilidad del registro depende de si el tráfico DNS se dirige a la infraestructura DNS supervisada.

Opción de instalación del conector de seguridad

La instalación de Security Connector en iOS permitirá:

- Visibilidad de registro de DNS en Secure Access
- Identidad de terminal y funciones de registro de dispositivos mejoradas
- Protección y control de DNS de tipo paraguas

El conector de seguridad se puede utilizar junto con Secure Client, pero se requieren

consideraciones de diseño y exclusión de tráfico adecuadas para evitar conflictos entre los dos componentes.

Causa

La causa principal es la arquitectura: Cisco Secure Client en iOS proporciona conectividad VPN, pero no incluye la funcionalidad de agente de terminal necesaria para la visibilidad de DNS y el registro de dispositivos en Secure Access. Esta funcionalidad requiere la instalación del conector de seguridad o la configuración del direccionamiento del tráfico para dirigir las consultas de DNS a través de la infraestructura supervisada. Sin estos componentes, las consultas DNS omiten la supervisión de acceso seguro y la información de identidad del dispositivo no se rellena en la sección de dispositivos móviles.

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).