Problemas de Visibilidad de Identidad de Cliente Seguro con Túnel de Red MX75 en Acceso Seguro

Contenido

Problema

Cuando los terminales con Secure Client se implementan detrás de un túnel de red MX75 que se conecta a Secure Access, las identidades de usuario y de cliente de roaming no son visibles correctamente en el sistema. Se observan los siguientes comportamientos específicos:

- La configuración de backoff configurada para dar prioridad a Secure Client sobre las conexiones de túnel de red no funciona como se esperaba cuando los terminales están detrás del MX75
- Las reglas de direccionamiento de tráfico basadas en dominios no se aplican porque el tráfico se atribuye solamente a la identidad del túnel de red en lugar del cliente de roaming
- La búsqueda de actividad muestra información de ubicación de origen incompleta, mostrando solo la identidad del túnel de red mientras se omiten las identidades de usuario y cliente de itinerancia
- Las reglas de dirección de tráfico basadas en identidad (como las basadas en usuarios de Active Directory o en la identidad de clientes de roaming) no se aplican al tráfico que atraviesa el túnel MX75

Este comportamiento impide la segregación de identidad y la aplicación de políticas adecuadas para los terminales que se conectan a través de la infraestructura de túnel de red.

Entorno

- Implementación de Cisco Secure Access
- Dispositivo MX75 con configuración de túnel de red para acceso seguro
- Agentes de Secure Client instalados en todos los terminales
- Configuración de backoff deshabilitada en clientes de roaming para dar prioridad a Secure

Client sobre conexiones de túnel de red
- Reglas de direccionamiento de tráfico configuradas para el ruteo basado en dominio
- Políticas basadas en identidad configuradas para usuarios de Active Directory y clientes de roaming

Resolución

El problema se resolvió implementando una configuración de solución alternativa mediante un enfoque de red registrada en lugar de confiar en la visibilidad de identidad de roaming a través del túnel de red MX75.

Implementación de solución alternativa

Paso 1: Configuración de RSM (módulo de seguridad de roaming) con la red registrada

Reemplace la configuración de túnel de red existente por una implementación de RSM combinada con una configuración de red registrada. Esta configuración permite la atribución de identidad y la aplicación de políticas adecuadas.

Paso 2: Validar visibilidad de identidad

Después de implementar la configuración de red registrada, compruebe que:

- Las identidades de usuario se muestran correctamente en Búsqueda de actividad
- Las identidades de cliente de roaming son visibles y se les atribuyen correctamente
- Reglas de direccionamiento de tráfico basadas en la función de identidad del usuario y el cliente, según lo esperado

Paso 3: Probar la funcionalidad de dirección de tráfico

Confirme que las reglas de direccionamiento de tráfico basado en dominio y las políticas basadas en identidad se apliquen correctamente con la nueva configuración.

Enfoque alternativo

Para entornos en los que no se requiere segregación de identidad en redes privadas, considere la posibilidad de implementar la configuración de RSM - Internet. Este enfoque envía el tráfico RSM directamente a Internet en lugar de a través del túnel de la red privada, que puede proporcionar una visibilidad de identidad adecuada al tiempo que mantiene los controles de seguridad.

Análisis técnico

Durante la resolución de problemas, se recopiló la salida de diagnóstico mediante policy.test.sse.cisco.com para demostrar el comportamiento de atribución de identidad cuando los terminales se encontraban detrás del túnel MX75. El análisis confirmó que, si bien el routing de identidades de itinerancia a través de un túnel de red es técnicamente posible, no es un flujo operativo recomendado o admitido para este escenario de implementación específico.

Causa

La causa raíz está relacionada con la forma en que Secure Access gestiona la atribución de identidad cuando el tráfico atraviesa la infraestructura de túnel de red. Cuando los terminales se conectan a través del túnel de red MX75, el sistema atribuye todo el tráfico a la identidad del túnel en lugar de conservar las identidades de usuario y cliente de roaming individual. Este comportamiento se ha diseñado para las conexiones de túnel de red, pero entra en conflicto con el requisito de visibilidad de identidad individual y aplicación de políticas.

Aunque es técnicamente factible rutear identidades de roaming a través de túneles de red, esta configuración no se recomienda ni se admite como flujo operativo estándar debido a las limitaciones de atribución de identidad descritas anteriormente.

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).