Restricción de acceso geográfico para conexiones VPN y acceso de confianza cero

Contenido

Problema

Las organizaciones que requieren restricciones de acceso geográfico para conexiones de acceso de confianza cero (ZTA) y VPN pueden detectar que las políticas de ZTA y VPN existentes deben desactivarse al intentar implementar controles de acceso basados en países. Los usuarios experimentan una completa pérdida de acceso a los recursos necesarios cuando las políticas están desactivadas debido a la incapacidad de localizar opciones de restricción geográfica nativas en la interfaz del producto Secure SSE. El requisito específico de restringir el acceso a las conexiones que se originan solo dentro de un país determinado no se puede configurar usando capacidades de productos integradas, lo que resulta en un impacto generalizado en el usuario cuando las políticas existentes se desactivan en un intento de implementar tales restricciones.

Entorno

- Producto Cisco Secure Access Service Edge (SASE)/Secure SSE
- Implementación de acceso de confianza cero (ZTNA)
- Servicios VPN que requieren control de acceso geográfico
- Políticas de acceso a recursos privados
- Organización que requiere restricciones de acceso específicas del país

Resolución

Actualmente, el producto Cisco Secure SSE no proporciona funcionalidad nativa para restringir el acceso a recursos privados en función de la ubicación geográfica o el país del usuario. Los

enfoques descritos en las siguientes secciones se pueden considerar para abordar esta limitación.

Envío de solicitud de característica

Se debe enviar una solicitud de función a Cisco para agregar capacidades de restricción geográfica para el acceso ZTA y VPN. El equipo del producto evalúa esta solicitud de mejora para su posible inclusión en futuras versiones. Las organizaciones pueden colaborar con su Cisco Account Manager para ayudar a priorizar estas solicitudes de funciones en función de los requisitos empresariales.

Consideración manual de la solución alternativa

Una posible solución alternativa manual implica agregar rangos de direcciones IP públicas específicas del país como grupos de objetos de red en las políticas de acceso.

Paso 1: Obtenga los intervalos de direcciones IP públicas del país del registro regional de Internet (RIR) adecuado.

Paso 2: Cree grupos de objetos de red que contengan los intervalos de IP identificados. Configure los grupos de objetos de red dentro de la configuración de la política de acceso para incluir los rangos de direcciones IP específicos asignados al país de destino.

Paso 3: Aplique los grupos de objetos de red a las políticas de acceso. Modifique las políticas de acceso existentes para hacer referencia a los grupos de objetos de red creados, limitando de forma efectiva el acceso a las conexiones que se originan en los rangos de IP especificados.

Limitaciones importantes

Este enfoque manual tiene importantes limitaciones, ya que se basa en definiciones de intervalo IP estático y no puede dar cuenta de asignaciones de IP dinámicas, usuarios móviles o servicios VPN que podrían eludir las restricciones geográficas. Además, este método requiere un mantenimiento continuo para garantizar la precisión del rango de IP.

Gestión de políticas temporales

Hasta que haya una solución permanente disponible, las organizaciones deben evitar deshabilitar todas las políticas ZTA y VPN simultáneamente. En su lugar, considere la posibilidad de implementar un enfoque por fases en el que las políticas de acceso críticas permanezcan activas mientras se abordan los requisitos de restricción geográfica a través de medios alternativos o a la espera de mejoras de los productos.

Causa

La arquitectura del producto Cisco Secure SSE no incluye funciones nativas de control de acceso geográfico para el acceso a recursos privados. El marco de políticas de acceso al producto está diseñado en torno a la identidad del usuario, el estado del dispositivo y los controles basados en la red, pero no incorpora la ubicación geográfica como parámetro de aplicación de políticas. Esto representa una brecha en la capacidad del producto en lugar de un problema de configuración o un defecto de software.

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).