Configuración de políticas basadas en geolocalización para VPN de acceso remoto en Secure Firewall Threat Defence

Contenido

Introducción

Este documento describe el proceso para permitir o denegar conexiones RAVPN basadas en geolocalizaciones específicas en Secure Firewall Threat Defence (FTD).

Prerequisites

Requisitos y limitaciones

Cisco recomienda que tenga conocimiento sobre estos temas:

- Centro de gestión de firewall seguro (FMC)
- VPN de acceso remoto (RAVPN)
- Configuración de geolocalización básica

Los requisitos y limitaciones actuales de las políticas basadas en la geolocalización son:

- Solo es compatible con FTD versión 7.7.0+, gestionada por FMC versión 7.7.0+.
- No es compatible con FTD administrado por Secure Firewall Device Manager (FDM).

- No compatible en modo de clúster
- Las direcciones IP no clasificadas basadas en geolocalización no se clasifican por origen geográfico. Para estos, el FMC aplica la acción de política de acceso al servicio predeterminada.
- Las políticas de acceso al servicio basadas en geolocalización no se aplican a las páginas de WebLaunch, lo que le permite descargar Secure Client sin restricciones.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Secure Firewall versión 7.7.0
- Secure Firewall Management Center versión 7.7.0

Puede encontrar información detallada sobre esta función en la sección Administración del acceso VPN de usuarios remotos según geolocalización de la Guía de configuración de dispositivos de Cisco Secure Firewall Management Center 7.7.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

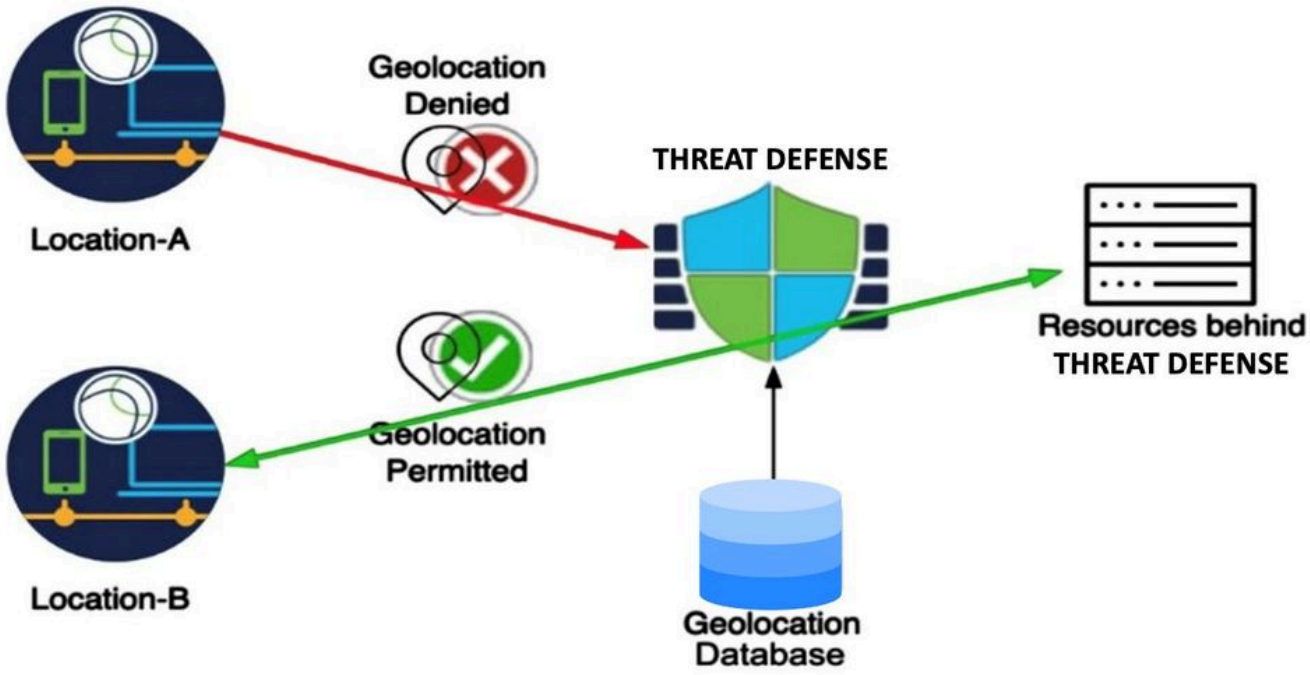
Las políticas de acceso basadas en la geolocalización ofrecen un valor significativo en la seguridad de la red actual, lo que permite bloquear el tráfico según su origen geográfico. Tradicionalmente, las organizaciones podían definir políticas de acceso al tráfico para el tráfico de red general que pasa a través del firewall. Ahora, con la introducción de esta función, es posible aplicar control de acceso basado en geolocalización para las solicitudes de sesión VPN de acceso remoto.

Esta función ofrece las siguientes ventajas:

- Reglas basadas en la geolocalización: Los clientes pueden crear reglas para permitir o denegar solicitudes RAVPN basadas en geolocalizaciones específicas, como países o continentes. Esto permite un control preciso sobre qué ubicaciones geográficas pueden iniciar sesiones VPN.
- Bloqueo previo a la autenticación: Las sesiones identificadas por estas reglas para una acción de denegación se bloquean antes de la autenticación y estos intentos se registran correctamente por motivos de seguridad. Esta acción preventiva ayuda a mitigar los intentos de acceso no autorizado.
- Cumplimiento y seguridad: Esta función ayuda a garantizar el cumplimiento de las políticas organizativas y de administración locales, a la vez que reduce la superficie de ataque del

servidor VPN.

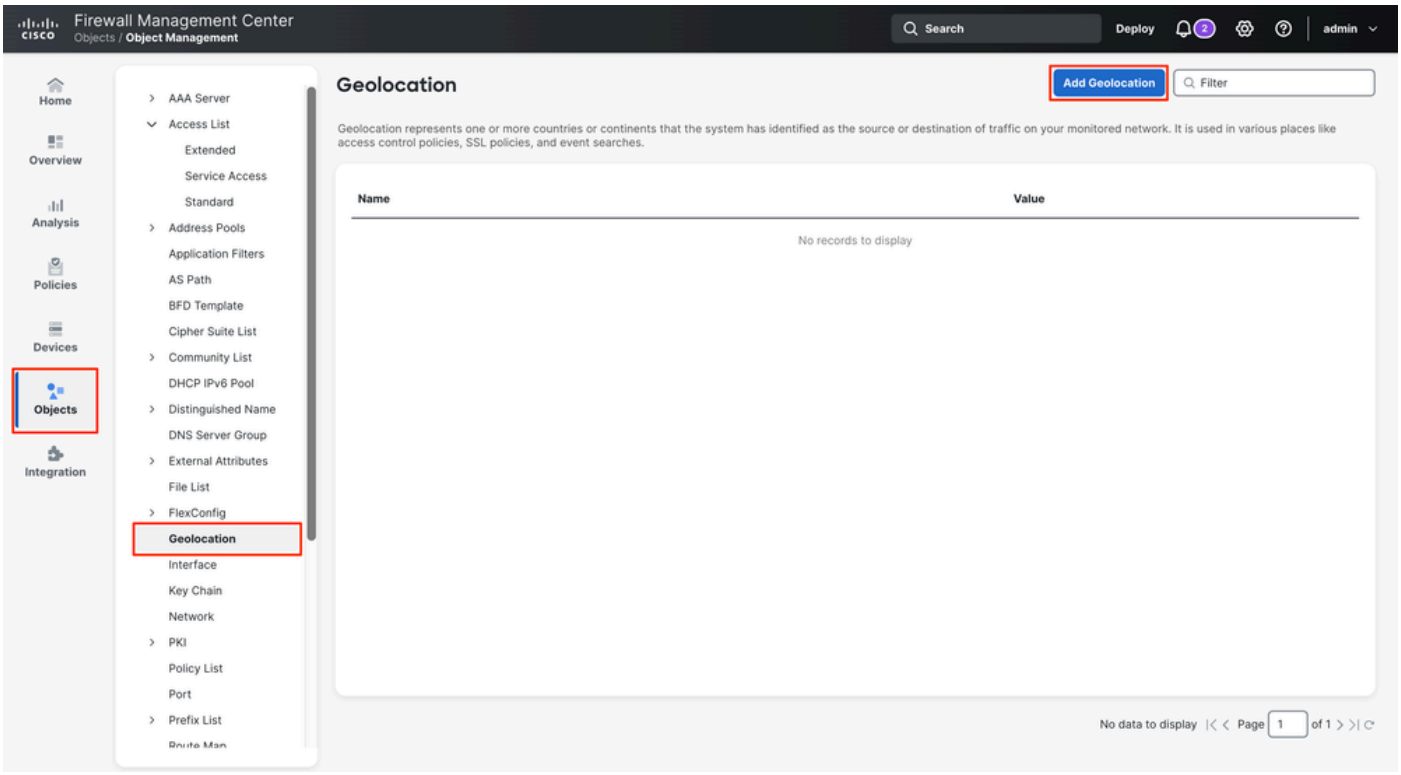
Dado que los servidores VPN tienen direcciones IP públicas accesibles a través de Internet, la introducción de reglas basadas en la geolocalización permite a las organizaciones restringir eficazmente las solicitudes de los usuarios desde geolocalizaciones específicas, reduciendo así la vulnerabilidad a los ataques de fuerza bruta.



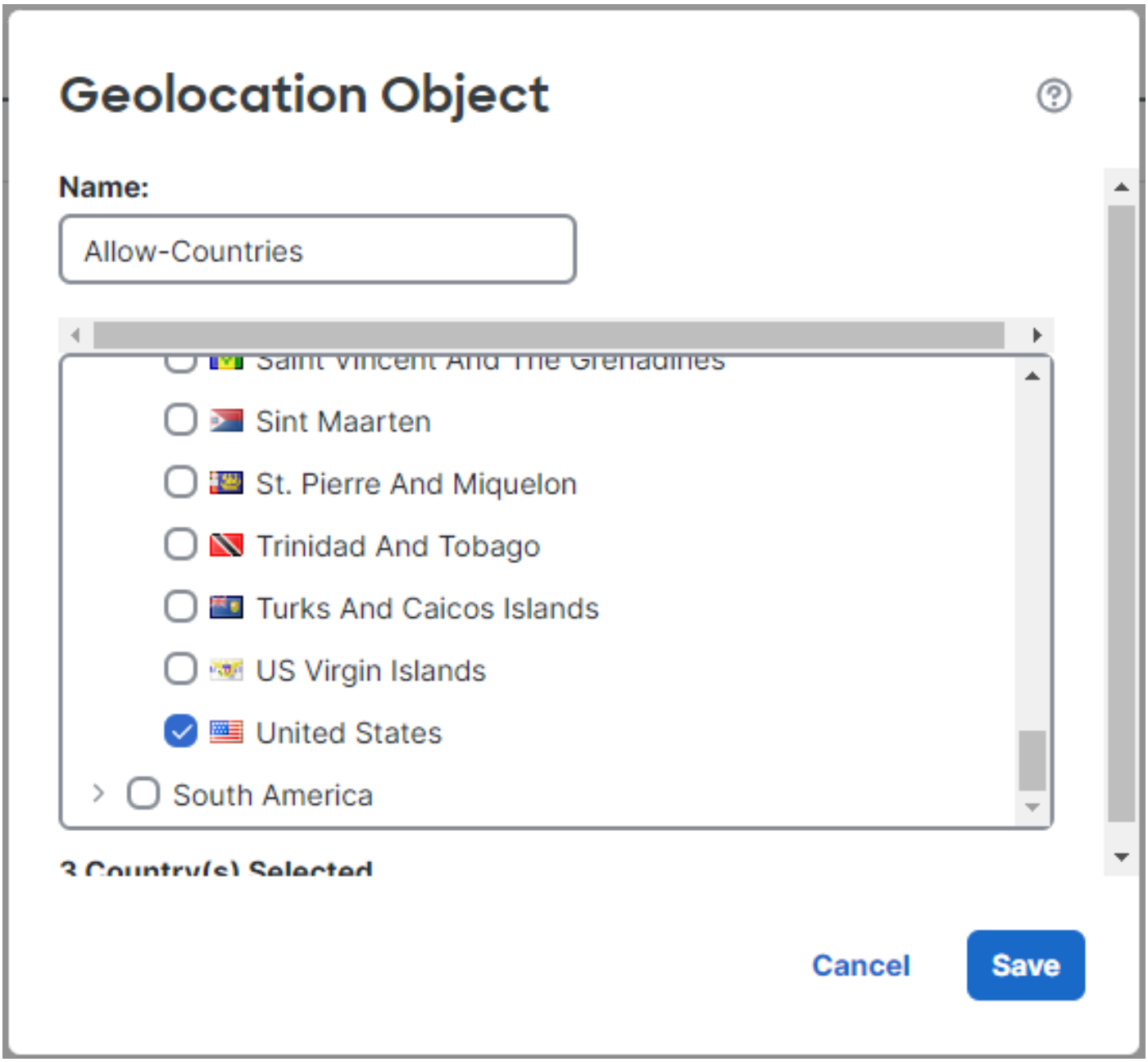
Configurar

Paso 1. Creación de un Objeto de Acceso al Servicio

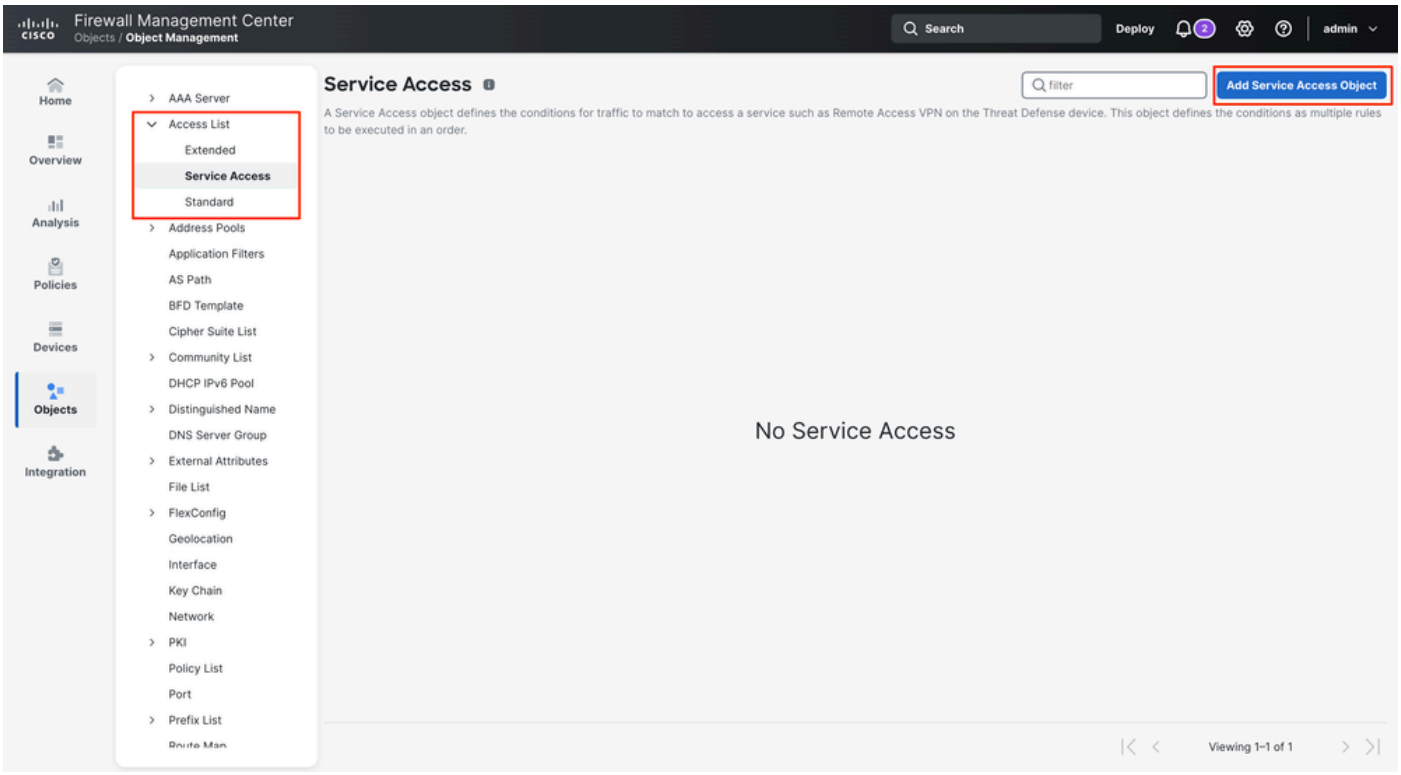
1. Inicie sesión en Secure Firewall Management Center.
2. Navegue hasta Objetos > Gestión de Objetos > Geolocalización y haga clic en Agregar Geolocalización para crear un objeto de Geolocalización.



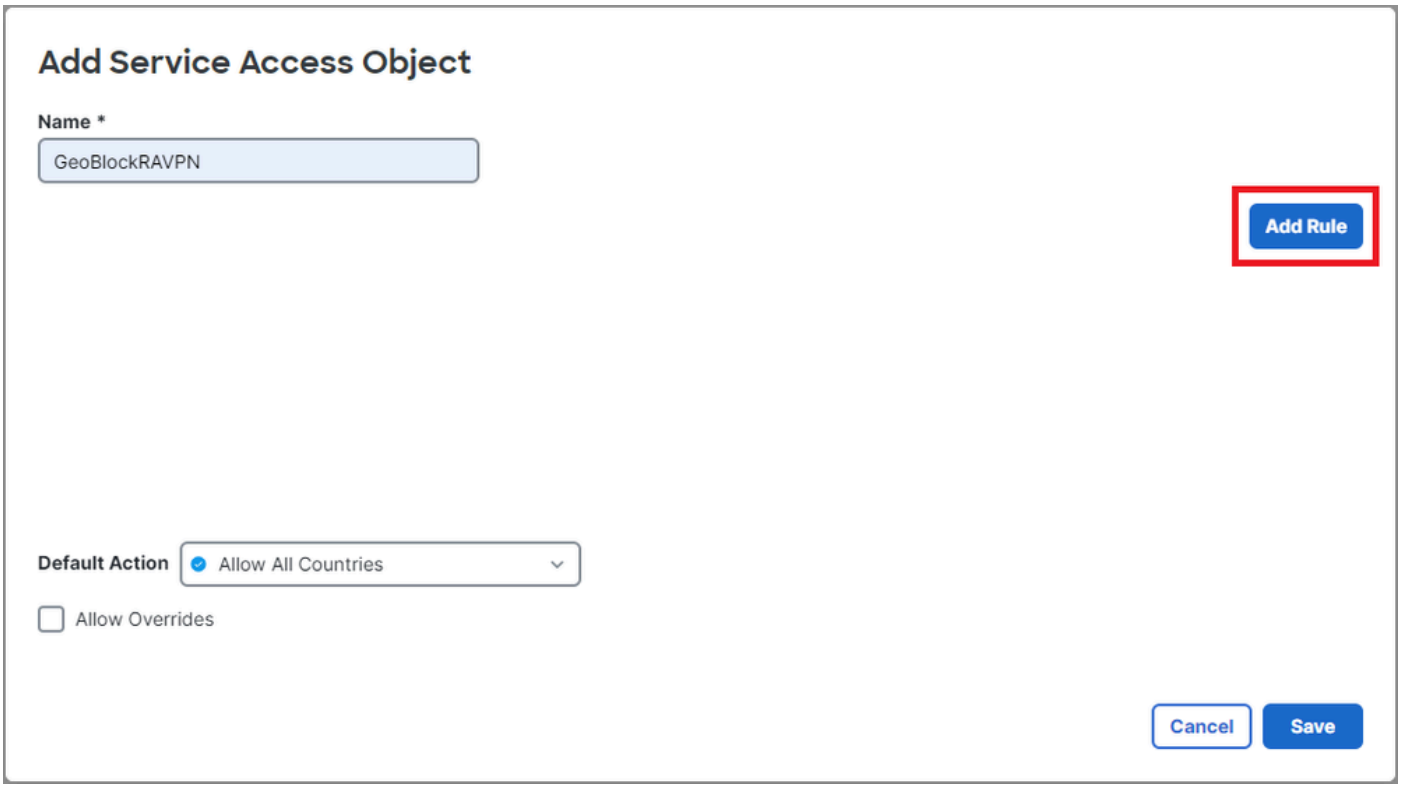
3. Cree el objeto seleccionando los indicadores de país adecuados para cada grupo, en función de si están permitidos o denegados.



4. Una vez creados los objetos de geolocalización, vaya a Objetos > Gestión de Objetos > Lista de Acceso > Acceso a Servicios y haga clic en Agregar Objeto de Acceso a Servicios.



5. Defina el nombre de la regla y, a continuación, haga clic en Agregar Regla.

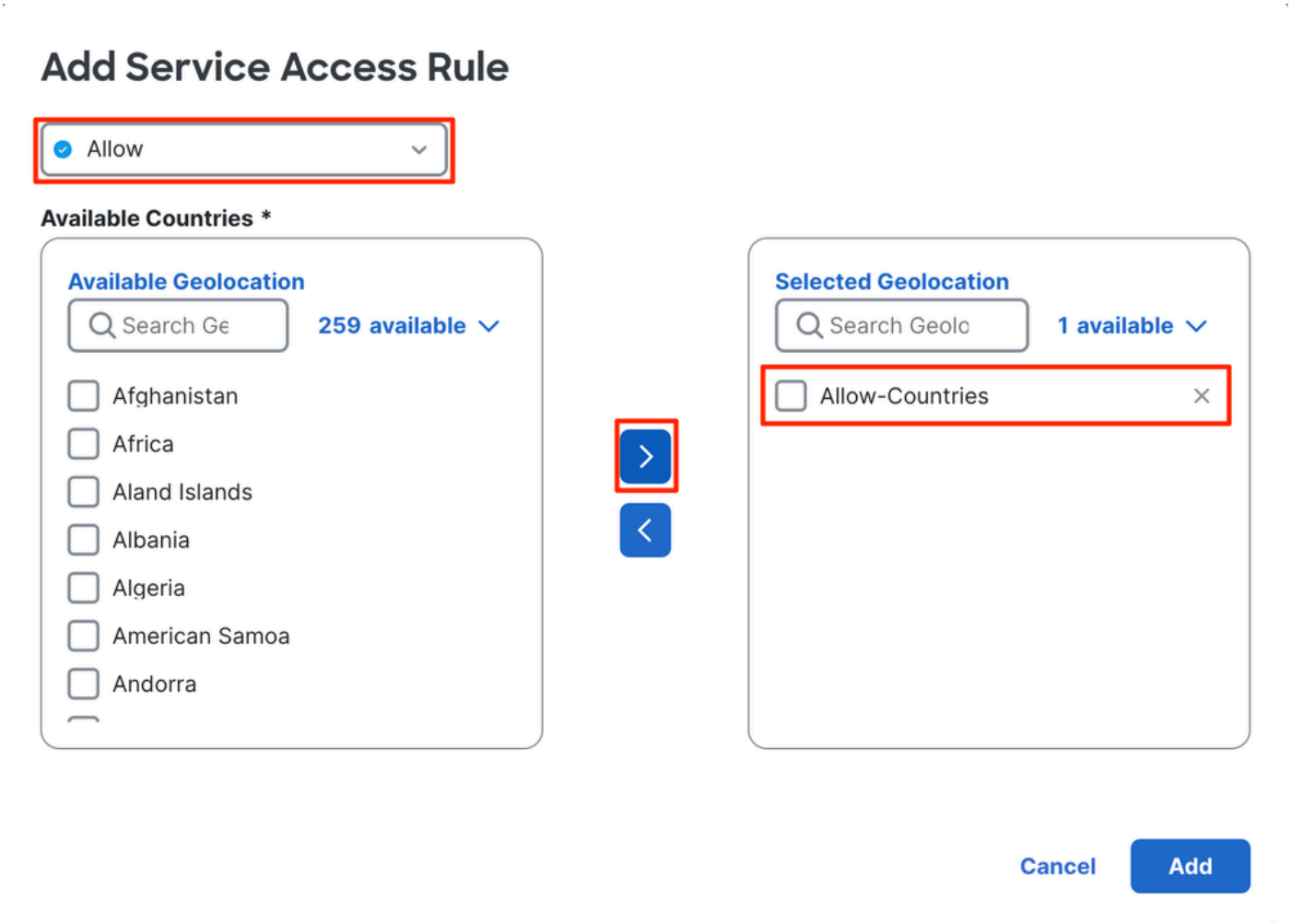


6. Seleccione la acción de la regla (permitir o denegar), localice el objeto Geolocation creado

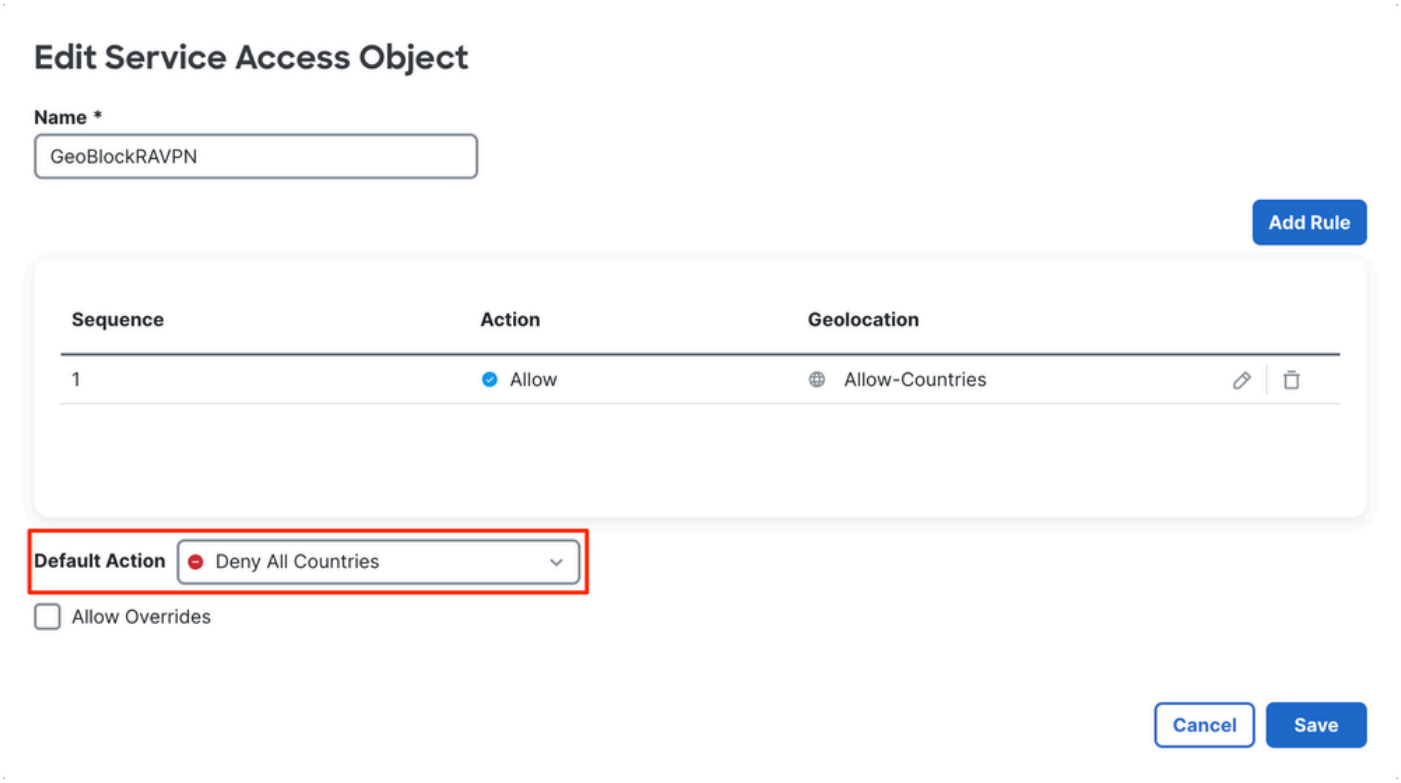
anteriormente y agréguelo a la regla haciendo clic en la flecha derecha. A continuación, haga clic en Agregar para crear la regla.

Nota: En un objeto de acceso a servicios, un objeto de geolocalización (país, continente o geolocalización personalizada) solo se puede utilizar en una regla.

Nota: asegúrese de configurar las reglas de acceso al servicio en el orden correcto, ya que estas reglas no se pueden reordenar.



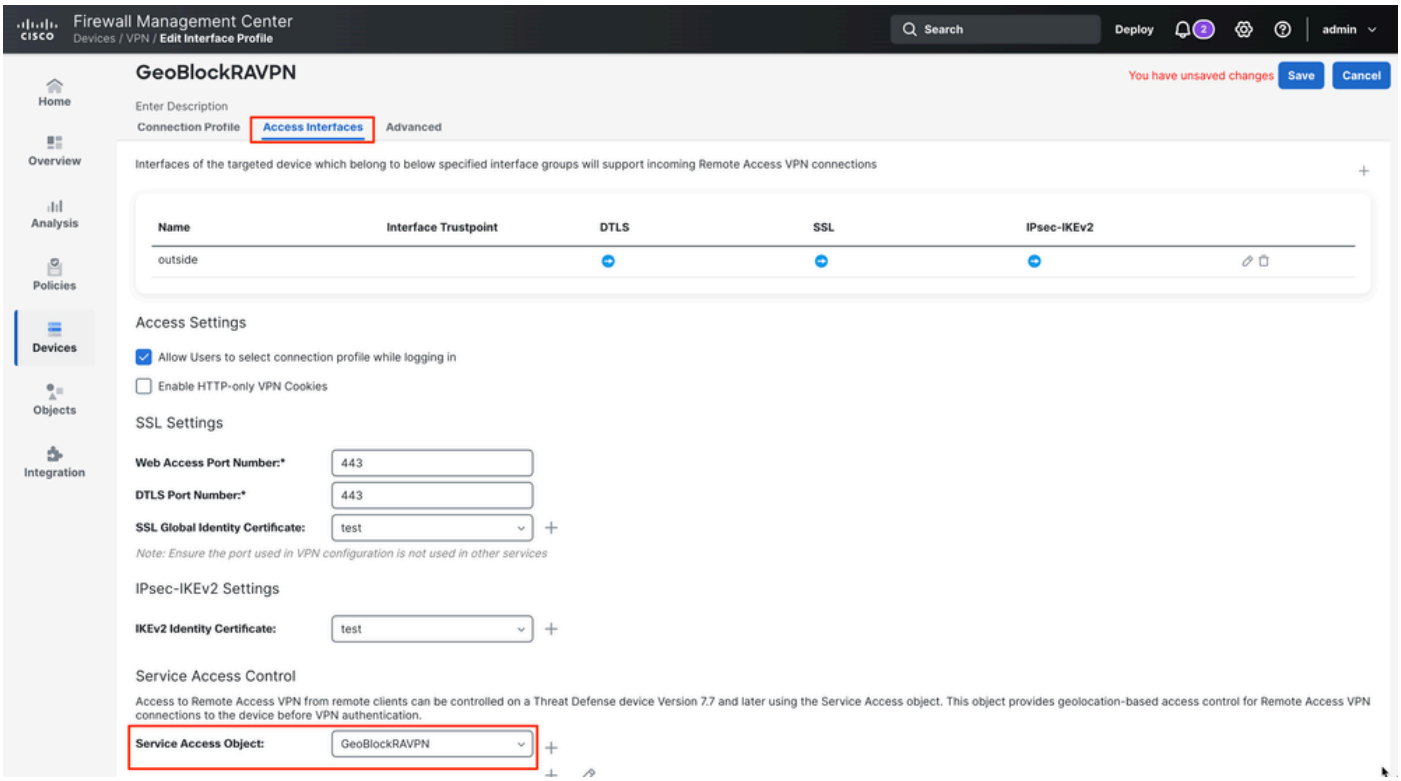
7. Cambie la acción por defecto a Denegar a Todos los Países para rechazar las solicitudes de sesión de otros países.



Paso 2. Aplique la configuración del objeto de servicio en RAVPN.

1. Navegue hasta la configuración RAVPN en Devices > Remote Access > RAVPN configuration object > Access interface.

2. En la sección Control de Acceso a Servicios, seleccione el Objeto de Acceso a Servicios que creó anteriormente.

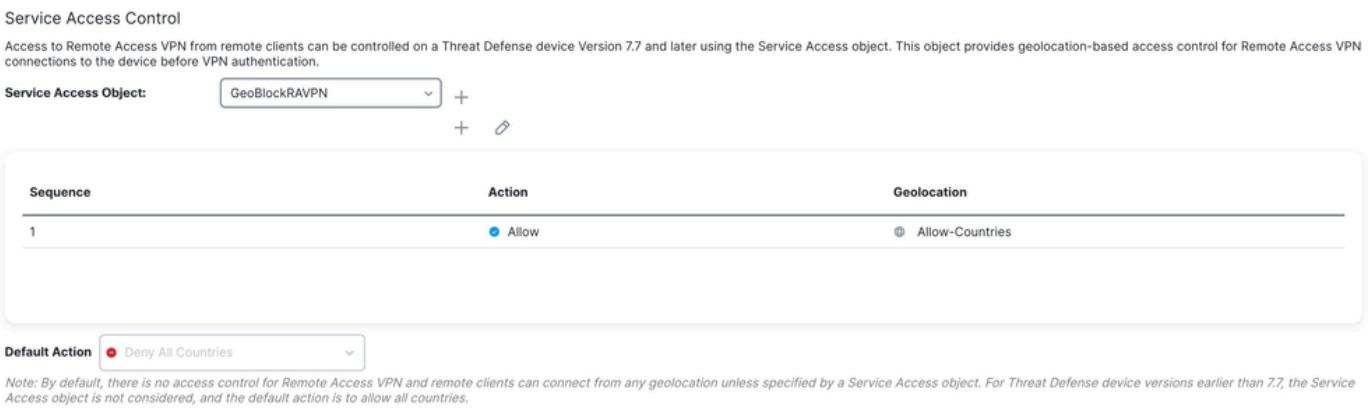


3. El objeto de acceso al servicio seleccionado ahora muestra el resumen de reglas y la acción por defecto.

4. Por último, guarde los cambios e implemente la configuración.

Verificación

Una vez guardada la configuración, las reglas aparecen en la sección Control de acceso al servicio, lo que permite validar qué grupos y países están bloqueados o permitidos.



Ejecute el show running-config service-access para garantizar que las reglas de acceso al servicio estén disponibles desde la CLI de FTD.

```
<#root>

firepower#

show running-config service-access


service-access permit ra-ssl-client ra-ikev2 geolocation FMC_GEOLOCATION_8589938211_418243765
service-access deny ra-ssl-client ra-ikev2 geolocation FMC_GEOLOCATION_8589938211_487190092
service-access permit ra-ssl-client ra-ikev2 geolocation any
```

Registros del sistema y supervisión

Secure Firewall introduce nuevos ID de syslog para capturar eventos relacionados con conexiones RAVPN bloqueadas por políticas basadas en geolocalización:

- 761031: Indica cuándo una política basada en geolocalización deniega una conexión IKEv2. Este syslog es parte de la clase de registro VPN existente.

%FTD-6-751031: Se ha denegado la sesión de acceso remoto IKEv2 para la capa faddr <client_ip> <device_ip> mediante una regla basada en ubicación geográfica (geo=<country_name>, id=<country_code>)

- 751031: Indica cuándo una política basada en geolocalización niega una conexión SSL. Este syslog es parte de la clase de registro WebVPN existente.

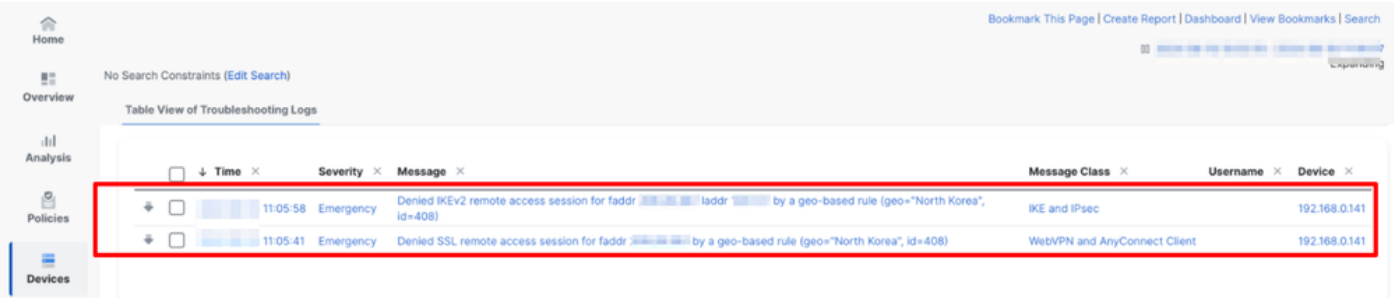
%FTD-6-716166: Sesión de acceso remoto SSL denegada para faddr <client_ip> por una regla basada en geografía (geo=<country_name>, id=<country_code>)

Nota: El nivel de gravedad predeterminado para estos nuevos registros del sistema es informativo cuando se habilita desde las clases de registro respectivas. Sin embargo, puede habilitar estos ID de syslog individualmente y personalizar su gravedad.

Supervisar conexiones bloqueadas

Para validar conexiones bloqueadas, navegue hasta Dispositivos > Solución de problemas > Resolución de problemas Logs. Aquí se muestran los registros relacionados con las conexiones bloqueadas, incluida información sobre las reglas que afectan a la conexión y el tipo de sesión.

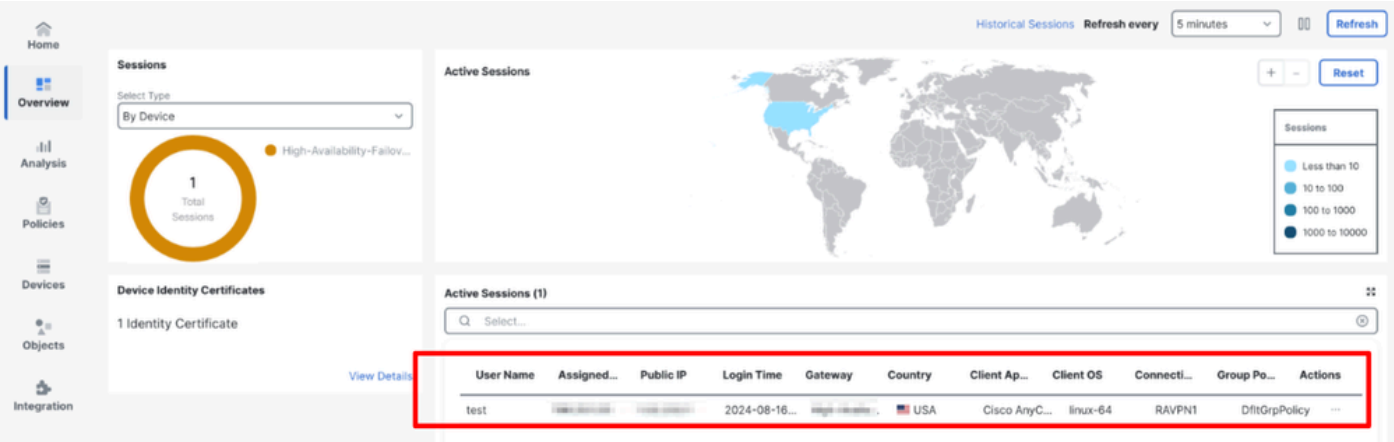
Nota: Syslog se debe configurar para recopilar esta información en los registros de solución de problemas.



Supervisar conexiones permitidas

Las sesiones permitidas se supervisan en Overview > Remote Access VPN dashboard, donde se muestra la información de la sesión, incluido el país de origen.

Nota: En este panel solo se muestran las conexiones de los países permitidos y los usuarios con permiso para conectarse. Las conexiones que se rechazan no se muestran en este panel.



Troubleshoot

Para solucionar problemas, siga estos pasos:

1. Verifique que las reglas estén configuradas correctamente en el objeto Service Access.
2. Compruebe si aparece un registro del sistema de denegación en la sección Registros de

solución de problemas cuando una geolocalización permitida solicita una sesión.
3. Asegúrese de que la configuración que se muestra en el FMC coincide con la de la CLI del FTD.
4. Utilice los siguientes comandos para recopilar más detalles útiles para solucionar problemas:

- debug geolocation <1-255>
- show service-access
- show service-access detail
- show service-access interface
- show service-access location
- show service-access service
- show geodb context
- show geodb counters
- show geodb ipv4
- show geodb ipv6

Información Relacionada

- Para obtener ayuda adicional, póngase en contacto con el TAC. Se necesita un contrato de asistencia válido:Contactos de asistencia globales de Cisco.
- También puede visitar la comunidad Cisco VPN aquí.

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).