Configuración del bloqueo de tráfico basado en geolocalización en FTD para el filtrado de tráfico entrante y saliente

Contenido

Problema

- Describa cuál es la mejor manera de bloquear el tráfico según la geolocalización en Cisco Secure Firewall Threat Defence (FTD), tanto para el tráfico que se origina en una región como para el tráfico destinado a una región.
- Surgen preguntas sobre si se requieren reglas de control de acceso independientes para el filtrado de tráfico entrante y saliente, y si se deben crear objetos de geolocalización adicionales cuando las entradas de geolocalización ya están disponibles en la pestaña Geolocations bajo la pestaña Networks de la regla de control de acceso.

Entorno

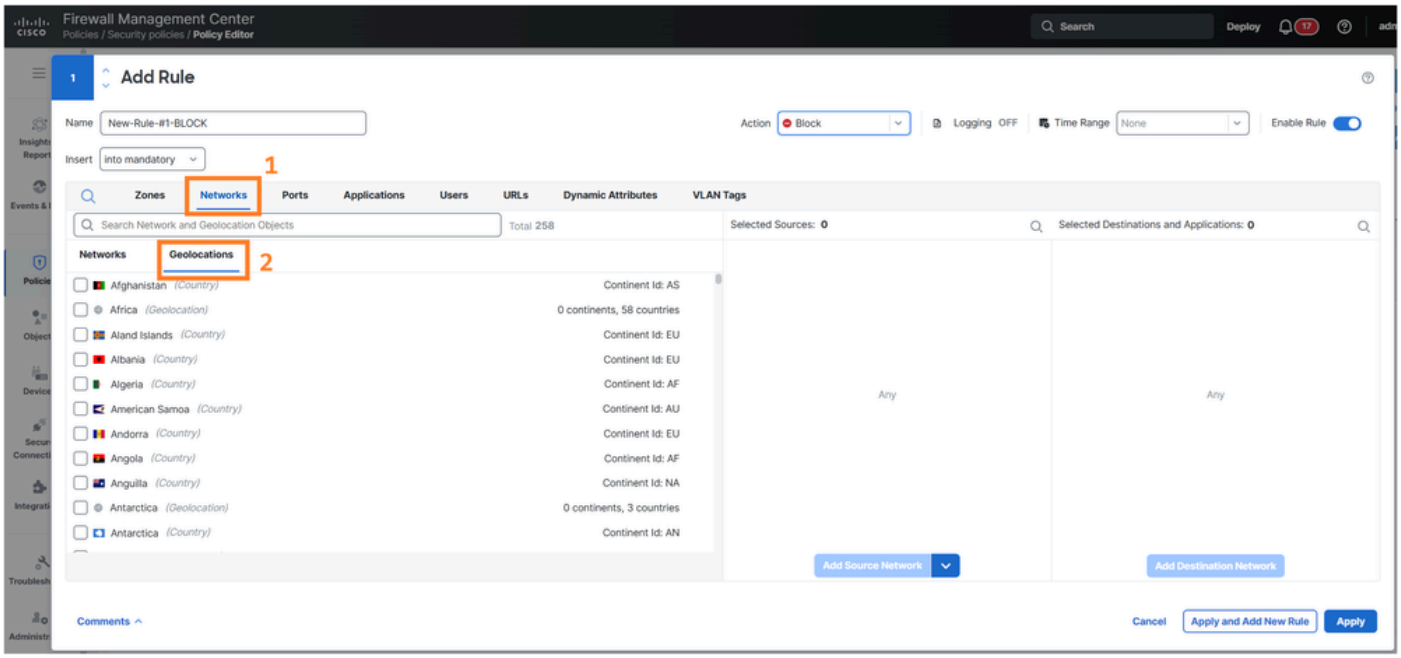
- Software FTD versión 7.1. Otras versiones de software también se ven afectadas.
- Software Cisco Secure Firewall Management Center (FMC) versión 7.1. Otras versiones de software también se ven afectadas.

Resolución

El filtrado del tráfico basado en la geolocalización en Cisco FTD se puede gestionar de forma eficaz utilizando la funcionalidad de geolocalizaciones existente disponible en la ficha Redes, sección Regla de la política de control de acceso de la interfaz de usuario (IU) de FMC. El enfoque de configuración depende de la dirección de tráfico específica y de los requisitos de la política.

Acceso a la configuración de geolocalización

Vaya a Directivas > Directivas de seguridad > Editor de directivas, edite una regla y seleccione Redes > Geolocalizaciones tab en la interfaz de usuario de FMC. Las entradas de geolocalización existentes disponibles en esta sección se pueden utilizar directamente para crear políticas de control de acceso sin necesidad de objetos de geolocalización independientes.



Estrategia de creación de reglas

El enfoque de creación de reglas varía en función de la direccionalidad del tráfico y los objetivos de las políticas.

Para bloquear el tráfico entrante desde geolocalizaciones específicas

Cree reglas de control de acceso que identifiquen el tráfico de origen originado en regiones geográficas específicas y apliquen acciones de bloqueo. Estas reglas deben colocarse correctamente en el orden de las reglas para garantizar la aplicación correcta de las políticas.

Para controlar el tráfico saliente a geolocalizaciones específicas

Configure reglas de control de acceso que identifiquen el tráfico de destino dirigido hacia regiones geográficas específicas. Dependiendo de la política de seguridad, se pueden configurar para permitir o bloquear el tráfico a esos destinos.

Requisitos de reglas independientes

Al implementar el filtrado de geolocalización bidireccional, se necesitan reglas de control de acceso independientes porque:

- El filtrado entrante requiere reglas que evalúen los atributos de geolocalización de origen.
- El filtrado de salida requiere reglas que evalúen los atributos de geolocalización de destino.
- La direccionalidad del tráfico determina qué campo de geolocalización (origen o destino) evalúa el motor de control de acceso.

La configuración de reglas específicas depende de la topología de red, los requisitos de seguridad y los objetivos de control de flujo de tráfico deseados para cada región geográfica.

Causa

La necesidad de clarificación surge de la complejidad de la implementación del control de acceso basado en geolocalización, donde se requieren diferentes tipos de reglas y configuraciones en función de la dirección del tráfico. La disponibilidad de entradas de geolocalización preexistentes en la ficha Redes de las reglas de control de acceso de la directiva de seguridad puede crear confusión sobre si es necesaria la creación de objetos adicionales para la implementación de la directiva.

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).