# Comportamiento de fallos de implementación de geolocalización con detección de amenazas habilitada en firewall seguro FTD

## Contenido

## Problema

Al intentar configurar el filtrado de tráfico basado en ubicación geográfica en un Cisco Secure Firewall FTD 3105, se encontraron varios problemas:

- La política de control de acceso basado en geografía (ACP) y las reglas de prefiltro no bloquearon los intentos de conexión de VPN de acceso remoto HTTPS (RA-VPN) para bloquear regiones en la interfaz externa de FTD.
- Después de actualizar a la versión 7.7.11, no se pudo implementar la configuración del acceso al servicio basado geográficamente RA-VPN cuando se incluyeron en la política los países de Países Bajos o Antillas Neerlandesas.
- La implementación de FMC falló en un 83% con este mensaje de error:

```
FMC >> object-group geolocation FMC_GEOLOCATION_184683596782_116848397
FMC >> location "Netherlands"
device >> [error] :
location "Netherlands"
^
ERROR: % Invalid input detected at '^' marker.
Config Error -- location "Netherlands"
```

## Entorno

- Cisco Secure Firewall Firepower Threat Defence (FTD) 3105 gestionado por FMC
- Versión de software actualizada: 7.7.11-1061

- Configuración de VPN de RA que requiere restricciones de acceso basadas en el país

# Resolución

La resolución implicaba varios pasos para validar correctamente un control de acceso basado en la ubicación geográfica en funcionamiento. Además, se descubrió una limitación con la detección de amenazas habilitada, lo que dio lugar a nuevas directrices sobre el comportamiento de coincidencia de tráfico.

1: Actualice tanto FMC como FTD a la versión 7.7.11-1061 para habilitar la funcionalidad de acceso al servicio basado geográficamente RA-VPN, ya que esta función solo es compatible con la versión 7.7.0 y posteriores.

2: Configure el acceso al servicio basado geográficamente RA-VPN de acuerdo con la documentación de Cisco y asócielo con la política RA-VPN.

3: Para resolver el error de implementación debido al Id. de error de Cisco CSCwq15499 al agregar países específicos como Países Bajos o Antillas Neerlandesas, aplique esta solución alternativa:

1. Cree un objeto de acceso al servicio RA-VPN en blanco sin configurar ningún país.
2. Aplique el objeto de acceso al servicio en blanco a la política RA-VPN e impleméntelo correctamente.
3. Edite el mismo objeto de acceso al servicio y agregue las reglas de país necesarias.
4. Implemente la configuración de nuevo: la implementación se realiza correctamente y el filtrado de ubicación geográfica está activo.

4: Verifique que la implementación se complete con éxito y que el acceso y los registros de RA-VPN reflejen las restricciones de país previstas. Supervise el sistema para asegurarse de que las restricciones de ubicación geográfica funcionan según lo previsto.

5: Determine si alguna función de detección de amenazas ya está habilitada en el FTD y coincidiría con el tráfico antes de que pueda alcanzar la política de acceso. Estas configuraciones hacen que se omitan las reglas de geolocalización, ya que la detección de amenazas toma el control antes de la aplicación de políticas.

<#root>

```
device# show run threat-detection
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

threat-detection service invalid-vpn-access
threat-detection service remote-access-authentication hold-down 1440 threshold 5
threat-detection service remote-access-client-initiations hold-down 1440 threshold 5
```

6: Correlacione los ID de syslog relacionados con las coincidencias y rechazos de la detección de amenazas para confirmar que el tráfico está llegando a la detección de amenazas en lugar de a la geolocalización.

- %FTD-4-401002: Shun agregó: IP_address IP_address port
- %FTD-4-401003: Rechazar borrado: IP_address
- %FTD-4-401004: Paquete rechazado: IP_address ==> IP_address on interface interface_name
- %FTD-4-733102: La detección de amenazas agrega el host a la lista de rechazo
- %FTD-4-733103: La detección de amenazas elimina el host de la lista de rechazo
- %FTD-4-733201: Detección de amenazas: Service[remote-access-client-initiations] Peer[peer-ip]: umbral de error de valor excedido: agregando shun a la interfaz de interfaz. SSL: Solicitudes de iniciación de cliente excesivas de RA.
- %FTD-4-733201: Detección de amenazas: Service[remote-access-client-initiations] Peer[peer-ip]: umbral de falla de umbral-valor excedido: agregando shun a la interfaz de interfaz. IKEv2:RA_excesiva_solicitudes_de_iniciación_de_cliente

```
<164>Feb 26 2026 23:05:45: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:07:36: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:12:25: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:00:00: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
<164>Feb 26 2026 23:00:01: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
<164>Feb 26 2026 23:00:01: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
---
device# show shun
```

# Causa

Los problemas encontrados tienen dos causas principales distintas:

- Limitación de coincidencia de reglas de geolocalización: El control de acceso basado geográficamente RA-VPN solo se soporta a partir de la versión de software 7.7.0 y superior. Además, la detección de amenazas RAVPN configurada puede actuar sobre el tráfico, lo que impide que coincida con las reglas basadas en la ubicación geográfica.
- ID de bug de Cisco CSCwq15499: En la versión 7.7.11, los errores de implementación ocurren cuando se agregan ciertos países a las políticas de acceso al servicio basadas geográficamente RA-VPN debido a un error de software conocido en el mecanismo de manejo de acceso al servicio geográfico RA-VPN.

## 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).