Geolocation Deploy Failure Behavior with Threat Detection Enabled on Secure Firewall FTD

Contents

Issue

When attempting to configure geo-location based traffic filtering on a Cisco Secure Firewall FTD 3105, several issues were encountered:

- Geo-based Access Control Policy (ACP) and prefilter rules did not block HTTPS Remote Access VPN (RA-VPN) connection attempts block regions to the FTD outside interface.
- After upgrading to version 7.7.11, configuring RA-VPN geo-based service access failed to deploy when **Netherlands** or **Netherlands Antilles** countries were included in the policy.
- FMC deployment failed at 83% with this error message:

```
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"
```

Environment

- Cisco Secure Firewall Firepower Threat Defense (FTD) 3105 managed by FMC
- Upgraded software version: 7.7.11-1061
- RA-VPN configuration requiring country-based access restrictions

Resolution

The resolution involved multiple steps to properly validate a working geo-location based access control. Additionally, a limitation with Threat Detection enabled was discovered, leading to new guidance provided regarding traffic matching behavior.

1: Upgrade both FMC and FTD to version 7.7.11-1061 to enable RA-VPN geo-based service access functionality, as this feature is only supported from version 7.7.0 and later.

2: Configure RA-VPN geo-based service access according to Cisco documentation and associate it with the RA-VPN policy.

3: To resolve the deployment failure due to Cisco bug ID CSCwq15499 when adding specific countries like **Netherlands** or **Netherlands Antilles**, apply this workaround:

1. Create a blank RA-VPN service access object with no countries configured.
2. Apply the blank service access object to the RA-VPN policy and deploy successfully.
3. Edit the same service access object and add the required country rules.
4. Deploy the configuration again - the deployment now succeeds and geo-location filtering is active.

4: Verify that the deployment completes successfully and that RA-VPN access and logs reflect the intended country restrictions. Monitor the system to ensure geo-location restrictions are functioning as expected.

5: Determine if any Threat Detection feature is already enabled on the FTD which would match traffic before it can reach the access policy. Such configurations causes geolocation rules to be skipped as Threat Detection takes over prior to policy application.

<#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: Correlate any syslog IDs relating to Threat Detection matches and shuns to confirm traffic is hitting Threat Detection instead of Geolocation.

- %FTD-4-401002: Shun added: IP_address IP_address port port
- %FTD-4-401003: Shun deleted: IP_address
- %FTD-4-401004: Shunned packet: IP_address ==> IP_address on interface interface_name

- %FTD-4-733102: Threat-detection adds host host to shun list
- %FTD-4-733103: Threat-detection removes host host from shun list
- %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] Peer[peer-ip]: failure threshold of value exceeded: adding shun to interface interface. SSL: RA excessive client initiation requests.
- %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] Peer[peer-ip]: failure threshold of threshold-value exceeded: adding shun to interface interface. IKEv2:RA_excessive_client_initiation_requests

```
<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
```

Cause

The issues encountered have two distinct root causes:

- **Geolocation Rule-Matching Limitation:** RA-VPN geo-based access control is only supported starting from software version 7.7.0 and above. Additionally, configured RAVPN Threat Detection can act on traffic, which prevents it from matching on geo-based rules.
- **Cisco bug ID CSCwq15499:** On version 7.7.11, deployment failures occur when adding certain countries to RA-VPN geo-based service access policies due to a known software bug in the RA-VPN geo service access handling mechanism.

Related Content

- Cisco Technical Support & Downloads