Comportamento de Falha de Implantação de Geolocalização com Detecção de Ameaça Habilitada no FTD de Firewall Seguro

Contents

Problema

Ao tentar configurar a filtragem de tráfego baseada em localização geográfica em um Cisco Secure Firewall FTD 3105, vários problemas foram encontrados:

- As regras de pré-filtro e a Política de Controle de Acesso (ACP) com base na região não bloquearam as tentativas de conexão de VPN de Acesso Remoto (RA-VPN) HTTPS, bloqueando regiões para a interface externa do FTD.
- Após a atualização para a versão 7.7.11, a configuração do acesso de serviço baseado em região RA-VPN falhou ao ser implantada quando os países da Holanda ou Antilhas Holandesas foram incluídos na política.
- Falha na implantação do FMC em 83% com esta mensagem de erro:

```
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"
```

Ambiente

- Cisco Secure Firewall Firepower Threat Defense (FTD) 3105 gerenciada pelo FMC
- Versão de software atualizada: 7.7.11-1061

- Configuração de RA-VPN que exige restrições de acesso com base no país

Resolução

A resolução envolveu várias etapas para validar corretamente um controle de acesso baseado em localização geográfica. Além disso, foi descoberta uma limitação com a detecção de ameaças ativada, levando a novas orientações sobre o comportamento de correspondência de tráfego.

1: Atualizar o FMC e o FTD para a versão 7.7.11-1061 a fim de permitir a funcionalidade de acesso ao serviço com base geográfica do RA-VPN, uma vez que esta funcionalidade só é suportada a partir da versão 7.7.0 e posterior.

2: Configure o acesso ao serviço baseado em região RA-VPN de acordo com a documentação da Cisco e associe-o à política de RA-VPN.

3: Para resolver a falha de implantação devido ao bug da Cisco ID CSCwq15499 ao adicionar países específicos como Holanda ou Antilhas Holandesas, aplique esta solução alternativa:

1. Crie um objeto de acesso ao serviço RA-VPN em branco sem países configurados.
2. Aplique o objeto de acesso ao serviço em branco à política RA-VPN e implante-o com êxito.
3. Edite o mesmo objeto de acesso a serviço e adicione as regras de país necessárias.
4. Implantar a configuração novamente - a implantação agora é bem-sucedida e a filtragem de localização geográfica está ativa.

4: Verifique se a implantação foi concluída com êxito e se o acesso e os registros de RA-VPN refletem as restrições do país pretendidas. Monitore o sistema para garantir que as restrições de localização geográfica estejam funcionando conforme esperado.

5: Determine se algum recurso de Detecção de Ameaças já está habilitado no FTD, o que corresponderia ao tráfego antes que ele possa alcançar a política de acesso. Essas configurações fazem com que as regras de geolocalização sejam ignoradas à medida que a detecção de ameaças assume o controle antes da aplicação da política.

<#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 todos os IDs de syslog relacionados a correspondências de detecção de ameaças e shuns para confirmar se o tráfego está atingindo a detecção de ameaças em vez da geolocalização.

- %FTD-4-401002: Shun adicionado: IP_address Porta da porta do endereço IP
- %FTD-4-401003: Excluir: endereço_IP
- %FTD-4-401004: Pacote rejeitado: IP_address ==> IP_address na interface interface_name
- %FTD-4-733102: A detecção de ameaças adiciona o host à lista de exceções
- %FTD-4-733103: A detecção de ameaças remove o host da lista de exceções
- %FTD-4-733201: Detecção de ameaças: Serviço[remote-access-client-initiations] Par[peer-ip]: limiar de falha de valor excedido: adicionando shun à interface interface. SSL: RA excedeu solicitações de iniciação do cliente.
- %FTD-4-733201: Detecção de ameaças: Serviço[remote-access-client-initiations] Par[peer-ip]: limiar de falha de valor de limiar excedido: adicionando shun à interface interface. IKEv2:RA_too_client_initi_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
```

Causa

Os problemas encontrados têm duas causas raiz distintas:

- Limitação de correspondência de regra de localização geográfica: O controle de acesso

baseado em região RA-VPN é suportado somente a partir da versão de software 7.7.0 e superior. Além disso, a Detecção de Ameaças de RAVPN configurada pode atuar no tráfego, o que a impede de corresponder regras baseadas em localização geográfica.

- ID de bug Cisco CSCwq15499: Na versão 7.7.11, ocorrem falhas de implantação ao adicionar determinados países às políticas de acesso a serviços baseados em região geográfica do RA-VPN devido a um bug de software conhecido no mecanismo de tratamento de acesso a serviços geográficos do RA-VPN.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.