Configurar políticas baseadas em localização geográfica para VPN de acesso remoto no Secure Firewall Threat Defense

Contents

Introdução

Este documento descreve o processo para permitir ou negar conexões RAVPN com base em geolocalizações específicas no Secure Firewall Threat Defense (FTD).

Pré-requisitos

Requisitos e limitações

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Centro de gerenciamento seguro de firewall (FMC)
- VPN de acesso remoto (RAVPN)
- Configuração básica de geolocalização

Os requisitos e limitações atuais para políticas baseadas em localização geográfica são:

- Suportado apenas no FTD versão 7.7.0+, gerenciado pelo FMC versão 7.7.0+.
- Não suportado no FTD gerenciado pelo Gerenciador de Dispositivos de Firewall Seguro (FDM).

- Não há suporte no modo de cluster
- Os endereços IP não classificados baseados em localização geográfica não são categorizados por origem geográfica. Para eles, o FMC aplica a ação de política de acesso ao serviço padrão.
- As políticas de acesso a serviços baseadas em localização geográfica não se aplicam às páginas WebLaunch, permitindo que você faça download do Secure Client sem restrições.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Secure Firewall versão 7.7.0
- Secure Firewall Management Center versão 7.7.0

Detalhes completos sobre esse recurso podem ser encontrados na seção Gerenciar o Acesso VPN de Usuários Remotos com Base na Geolocalização no Guia de Configuração de Dispositivos do Cisco Secure Firewall Management Center 7.7.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

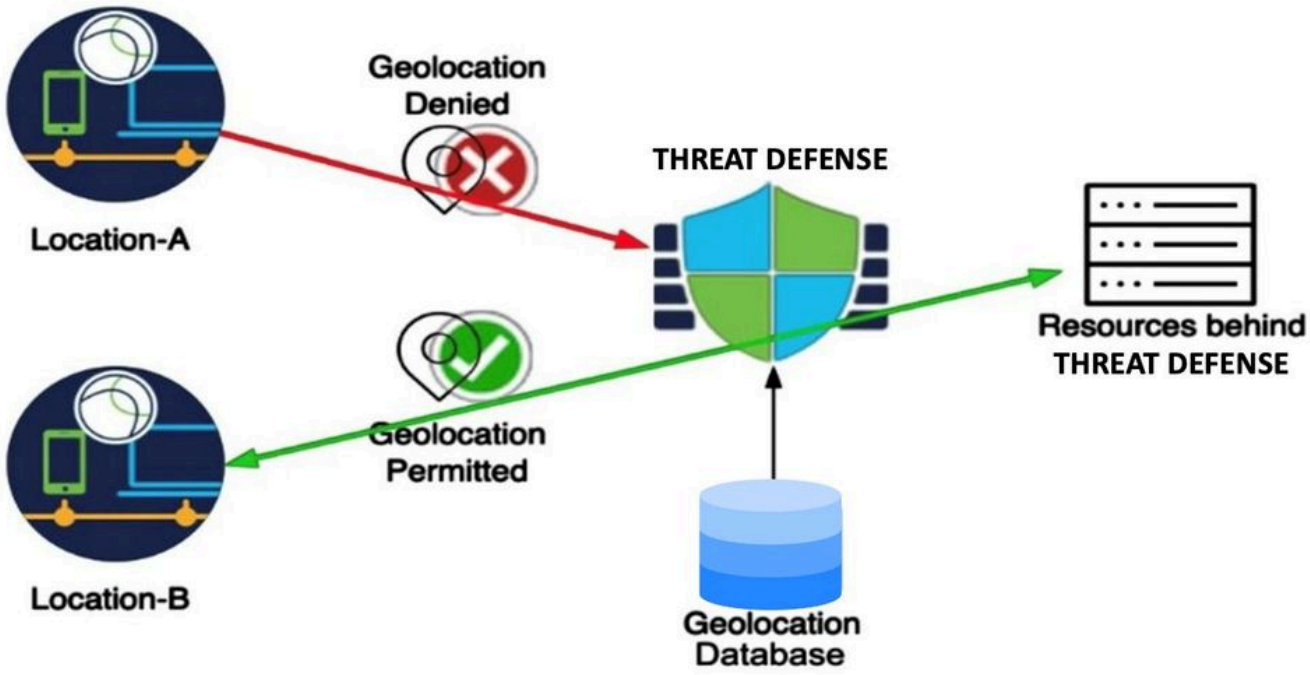
As políticas de acesso baseadas em geolocalização oferecem um valor significativo na segurança da rede atualmente, permitindo que o tráfego seja bloqueado com base em sua origem geográfica. Tradicionalmente, as organizações podem definir políticas de acesso de tráfego para o tráfego geral de rede que passa pelo firewall. Agora, com a introdução desse recurso, é possível aplicar o controle de acesso baseado em geolocalização para solicitações de sessão de VPN de Acesso Remoto.

Esse recurso oferece os seguintes benefícios:

- Regras baseadas em localização geográfica: Os clientes podem criar regras para permitir ou negar solicitações de RAVPN com base em geolocalizações específicas, como países ou continentes. Isso permite um controle preciso sobre quais localizações geográficas podem iniciar sessões de VPN.
- Bloqueio de pré-autenticação: As sessões identificadas por essas regras para uma ação de negação são bloqueadas antes da autenticação, e essas tentativas são registradas adequadamente para fins de segurança. Essa ação preventiva ajuda a reduzir as tentativas de acesso não autorizado.
- Conformidade e segurança: Esse recurso ajuda a garantir a adesão às políticas organizacionais e de governança locais, ao mesmo tempo em que reduz a superfície de

ataque do servidor VPN.

Como os servidores VPN têm endereços IP públicos acessíveis pela Internet, a introdução de regras baseadas em geolocalização permite que as organizações restrinjam efetivamente as solicitações dos usuários de geolocalizações específicas, reduzindo assim a vulnerabilidade a ataques de força bruta.

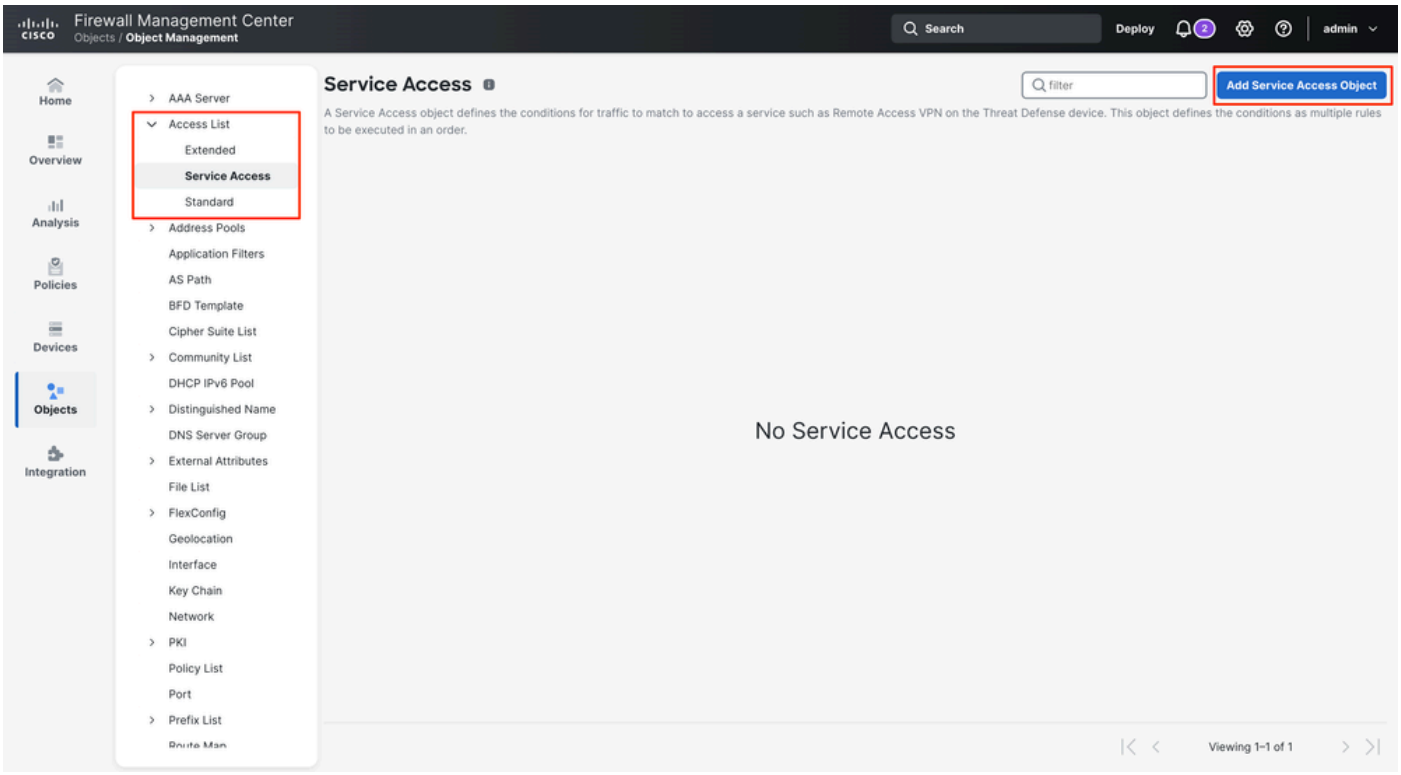


Configurar

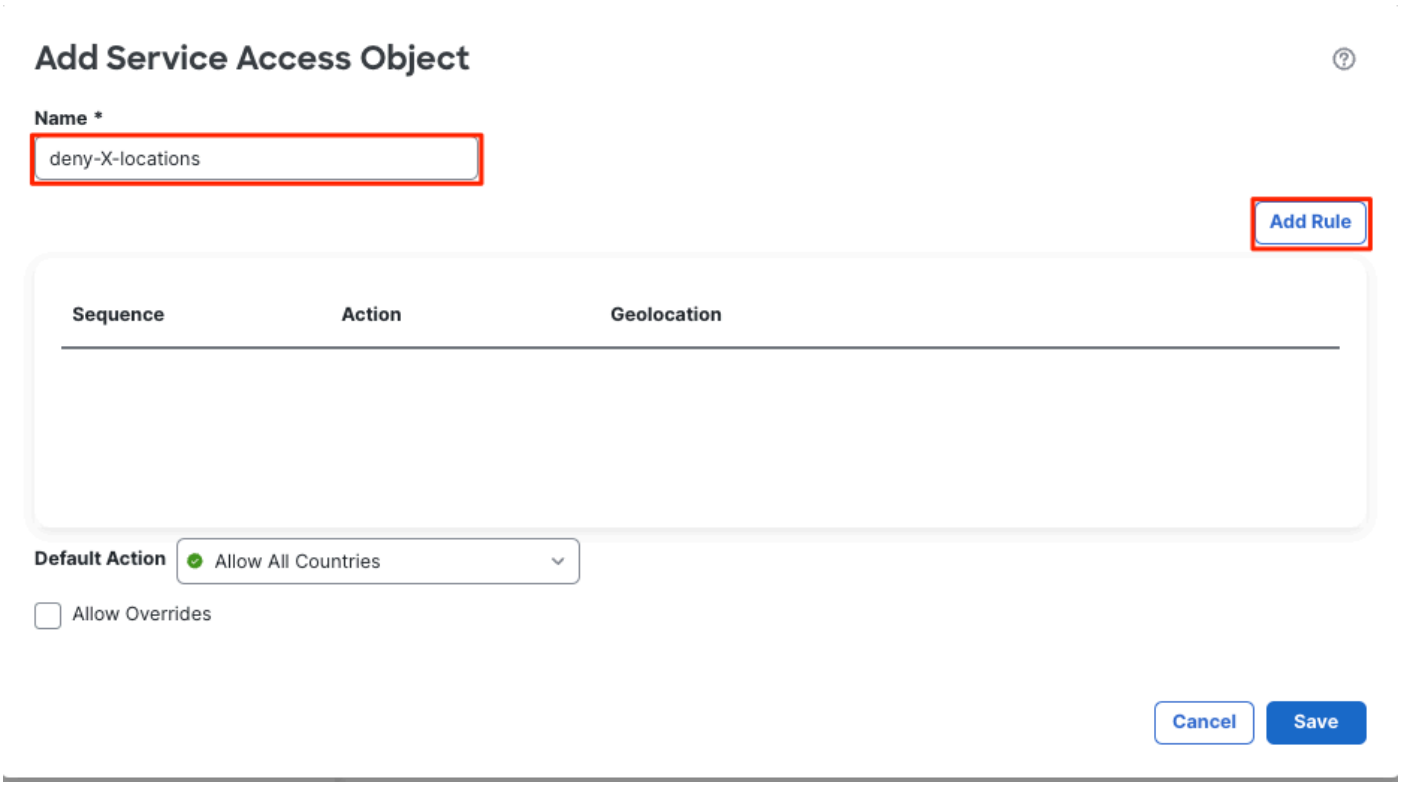
Etapa 1. Criar um Objeto de Acesso a Serviço

1. Faça login no Secure Firewall Management Center.

2. Navegue até Objetos > Gerenciamento de Objetos > Lista de Acesso > Acesso ao Serviço e clique em Adicionar Objeto de Acesso ao Serviço.



3. Defina o nome da regra e clique em Adicionar Regra.

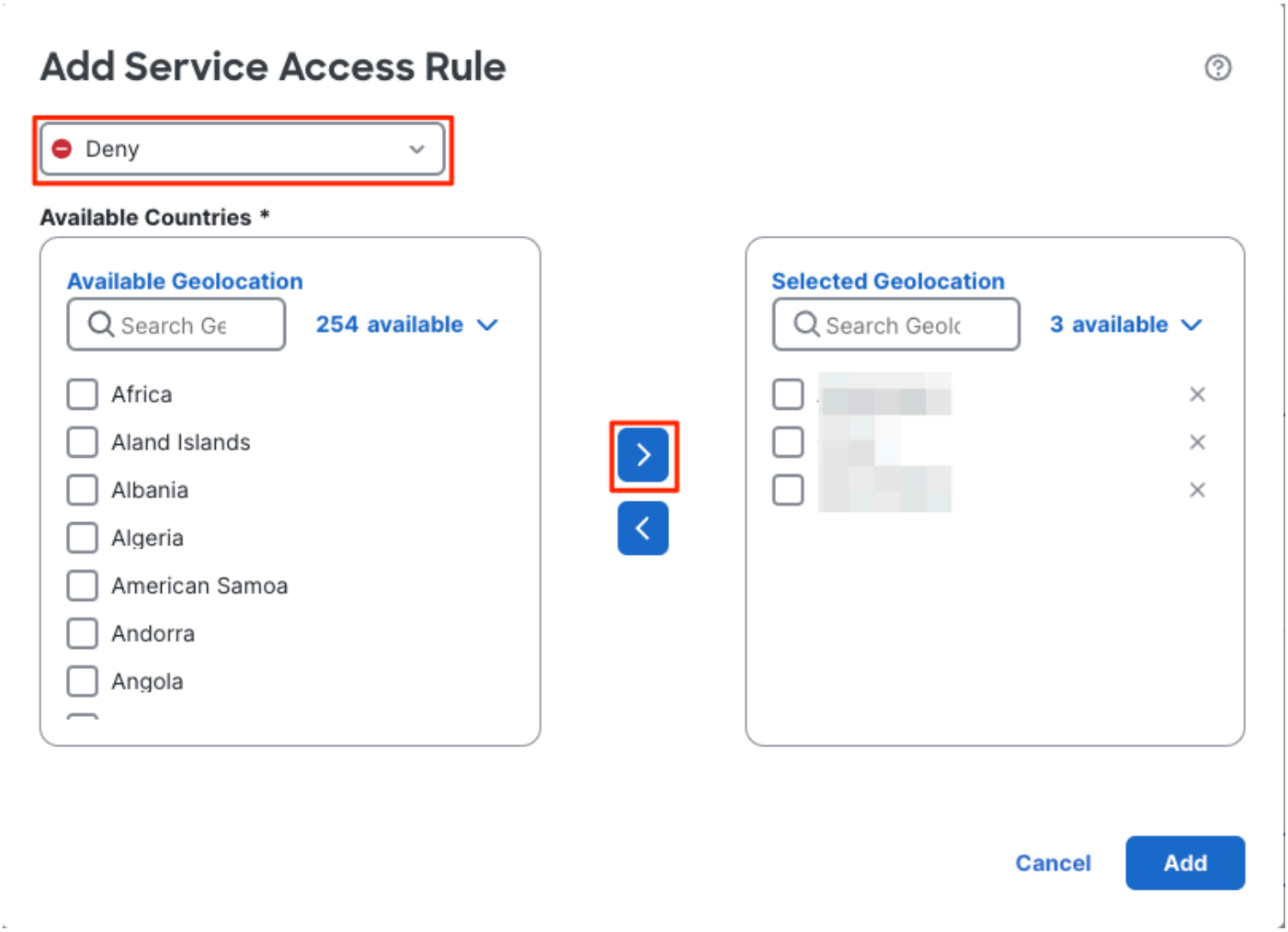


4. Configure a Regra de Acesso ao Serviço:

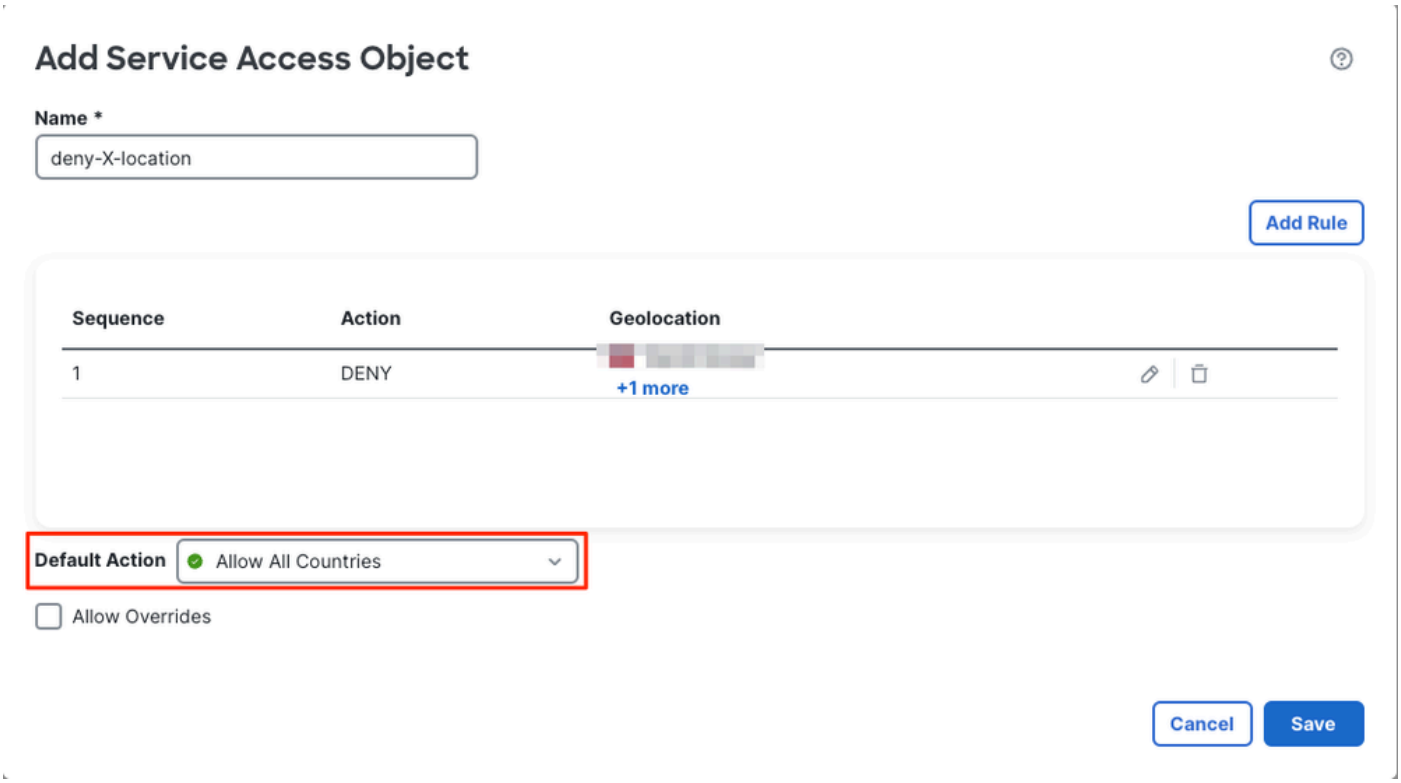
- Selecione a ação da regra: Permitir ou Negar.
- Em Países Disponíveis, selecione países, continentes ou objetos de geolocalização definidos pelo usuário e mova-os para a lista Geolocalização Selecionada.
- Clique em Adicionar para criar a regra.

Note: Em um objeto de acesso a serviços, um objeto de geolocalização (país, continente ou geolocalização personalizada) só pode ser usado em uma regra.

Observação: certifique-se de configurar as regras de acesso a serviços na ordem correta, pois essas regras não podem ser reordenadas.



5. Escolha a Ação Padrão: Permitir todos os países ou Negar todos os países. Esta ação se aplica a conexões que não correspondem a nenhuma das Regras de Acesso a Serviços configuradas.

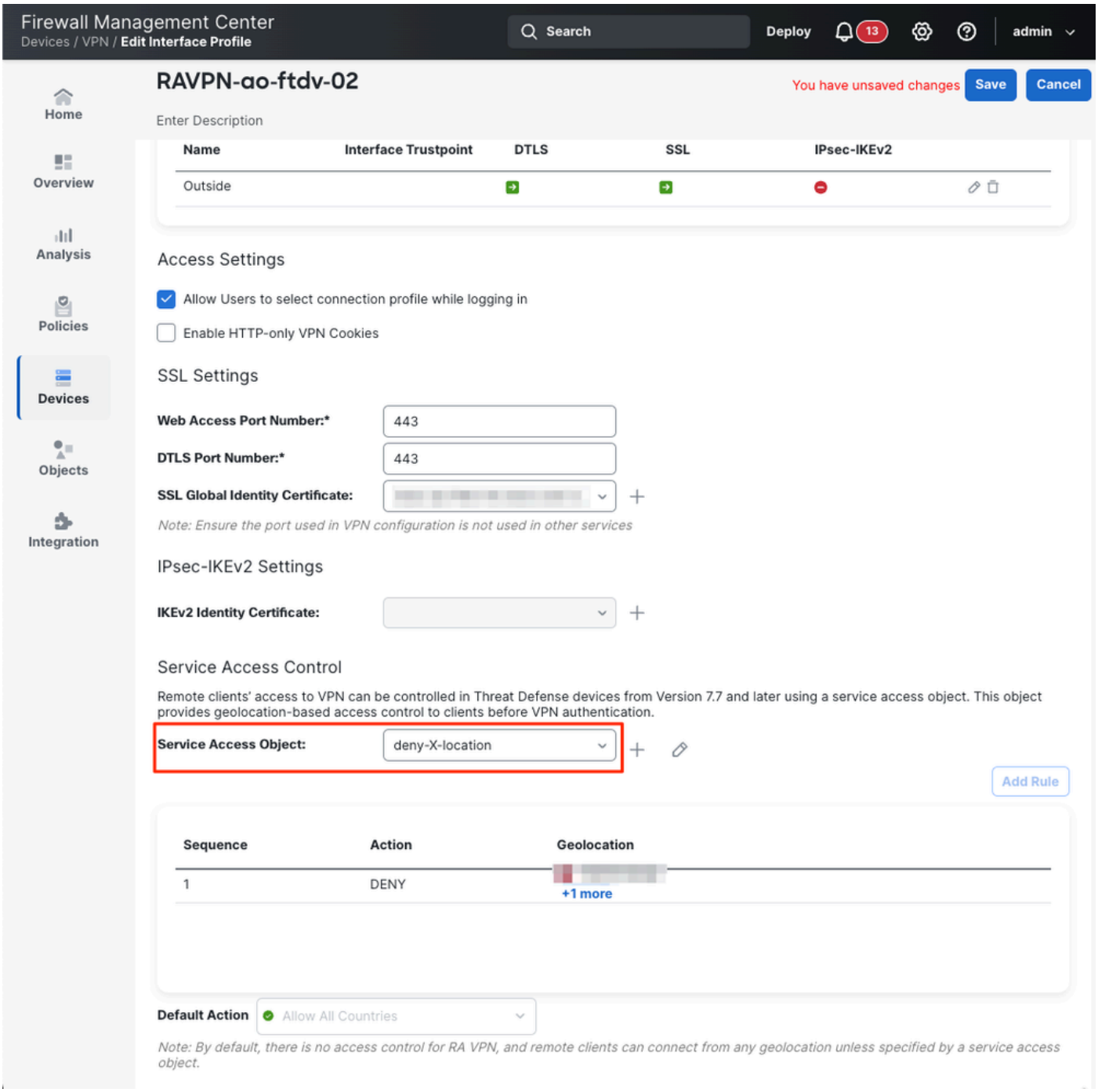


6. Clique em Salvar.

Etapa 2. Aplicar a configuração do Objeto de Serviço no RAVPN.

1. Navegue até a configuração RAVPN em Devices > Remote Access > RAVPN configuration object > Access interface.

2. Na seção Service Access Control, selecione o Service Access Object criado anteriormente.

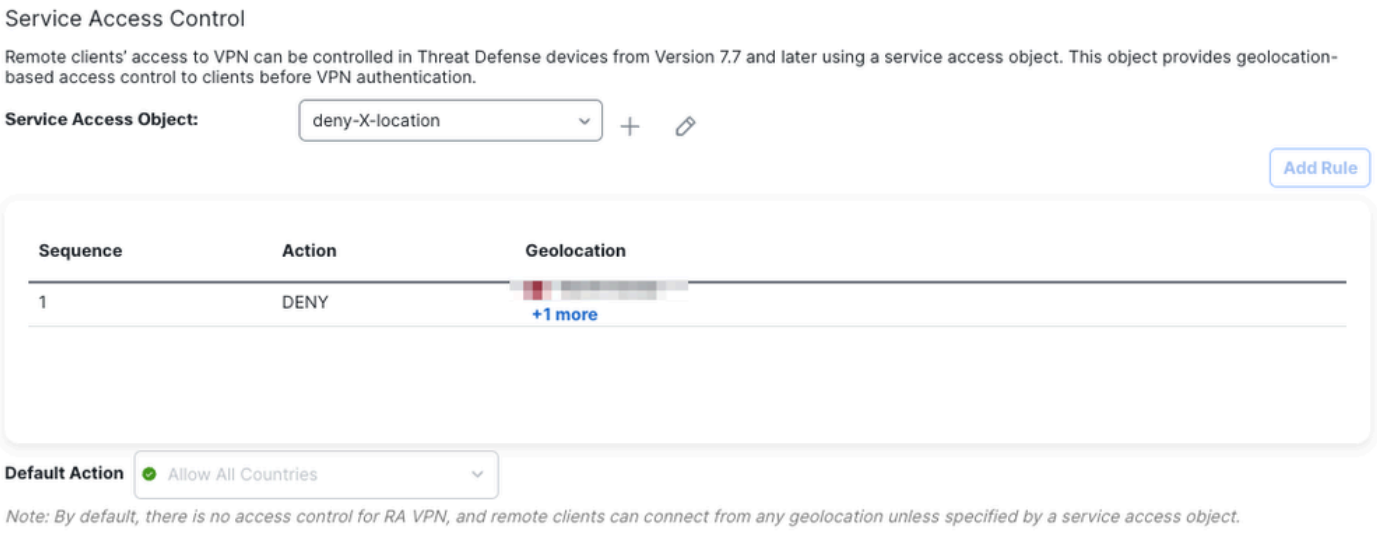


3. O objeto de Acesso ao Serviço que você selecionou agora exibe o resumo de regras e a ação padrão. Verifique se está correto.

4. Finalmente, Salve as alterações e Implante a configuração.

Verificar

Depois que a configuração é salva, as regras aparecem na seção Controle de acesso de serviço, permitindo que você valide quais grupos e países são bloqueados ou permitidos.



Execute o comando show running-config service-access para garantir que as regras de acesso ao serviço estejam disponíveis na CLI do FTD.

<#root>

```
firepower#
```

show running-config service-access

```
service-access deny ra-ssl-client geolocation FMC_GEOLOCATION_146028889448_536980902
service-access permit ra-ssl-client geolocation any

firepower# show running-config object-group idFMC_GEOLOCATION_146028889448_536980902
object-group geolocation FMC_GEOLOCATION_146028889448_536980902
location "Country X"
location "Country Y"
```

Syslogs e monitoramento

O Secure Firewall introduz novas IDs de syslog para capturar eventos relacionados a conexões RAVPN bloqueadas por políticas baseadas em geolocalização:

- 761031: Indica quando uma conexão IKEv2 é negada por uma política baseada em geolocalização. Este syslog faz parte da classe de log VPN existente.

%FTD-6-751031: Sessão de acesso remoto IKEv2 negada para faddr <client_ip> laddr <device_ip> por uma regra geográfica (geo=<country_name>, id=<country_code>)

- 751031: Indica quando uma conexão SSL é negada por uma política baseada em geolocalização. Este syslog faz parte da classe de log WebVPN existente.

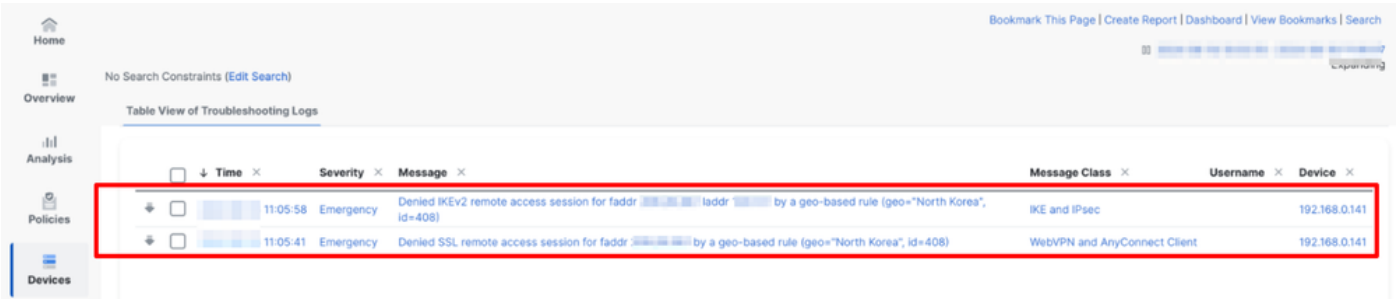
%FTD-6-716166: Sessão de acesso remoto SSL negada para faddr <client_ip> por uma regra baseada em região (geo=<country_name>, id=<country_code>)

Note: O nível de severidade padrão para esses novos syslogs é informativo quando habilitado nas respectivas classes de log. No entanto, você pode habilitar esses IDs de syslog individualmente e personalizar sua gravidade.

Monitorar Conexões Bloqueadas

Para validar as conexões bloqueadas, navegue até Devices > Troubleshoot > Troubleshooting Logs. Aqui, os logs relacionados às conexões bloqueadas são exibidos, incluindo informações sobre as regras que afetam a conexão e o tipo de sessão.

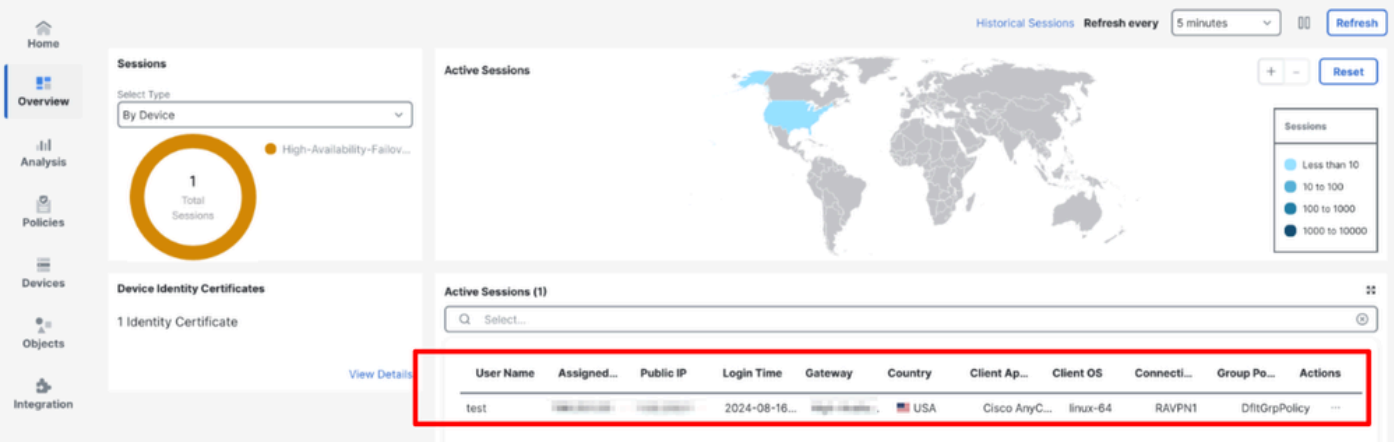
Note: O Syslog deve ser configurado para coletar essas informações nos Logs de Troubleshooting.



Monitorar Conexões Permitidas

As sessões permitidas são monitoradas em Overview > Remote Access VPN dashboard, onde as informações da sessão são exibidas, incluindo o país de origem.

Note: Apenas conexões de países e usuários com permissão para se conectar são exibidas nesse painel. As conexões rejeitadas não são exibidas nesse painel.



Troubleshooting

Para fins de solução de problemas, siga estas etapas:

1. Verifique se as regras estão configuradas corretamente no objeto Service Access.
2. Verifique se um syslog deny é exibido na seção Logs de Troubleshooting quando uma geolocalização permitida solicita uma sessão.
3. Certifique-se de que a configuração mostrada no FMC corresponda ao que está na CLI do FTD.
4. Use os próximos comandos para coletar mais detalhes que sejam úteis para fins de solução de 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 ipv4 location <País> detail
- show geodb counters
- show geodb ipv4 [lookup <endereço IP>]
- show geodb ipv6

Informações Relacionadas

- Para obter assistência adicional, entre em contato com o TAC. É necessário um contrato de suporte válido:Cisco Worldwide Support Contacts.
- Você também pode visitar a Comunidade Cisco VPN aqui.

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.