Implementar medidas de proteção para Secure Client AnyConnect VPN

Contents

Introdução

Este documento descreve como melhorar a segurança da implementação da VPN de acesso remoto.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

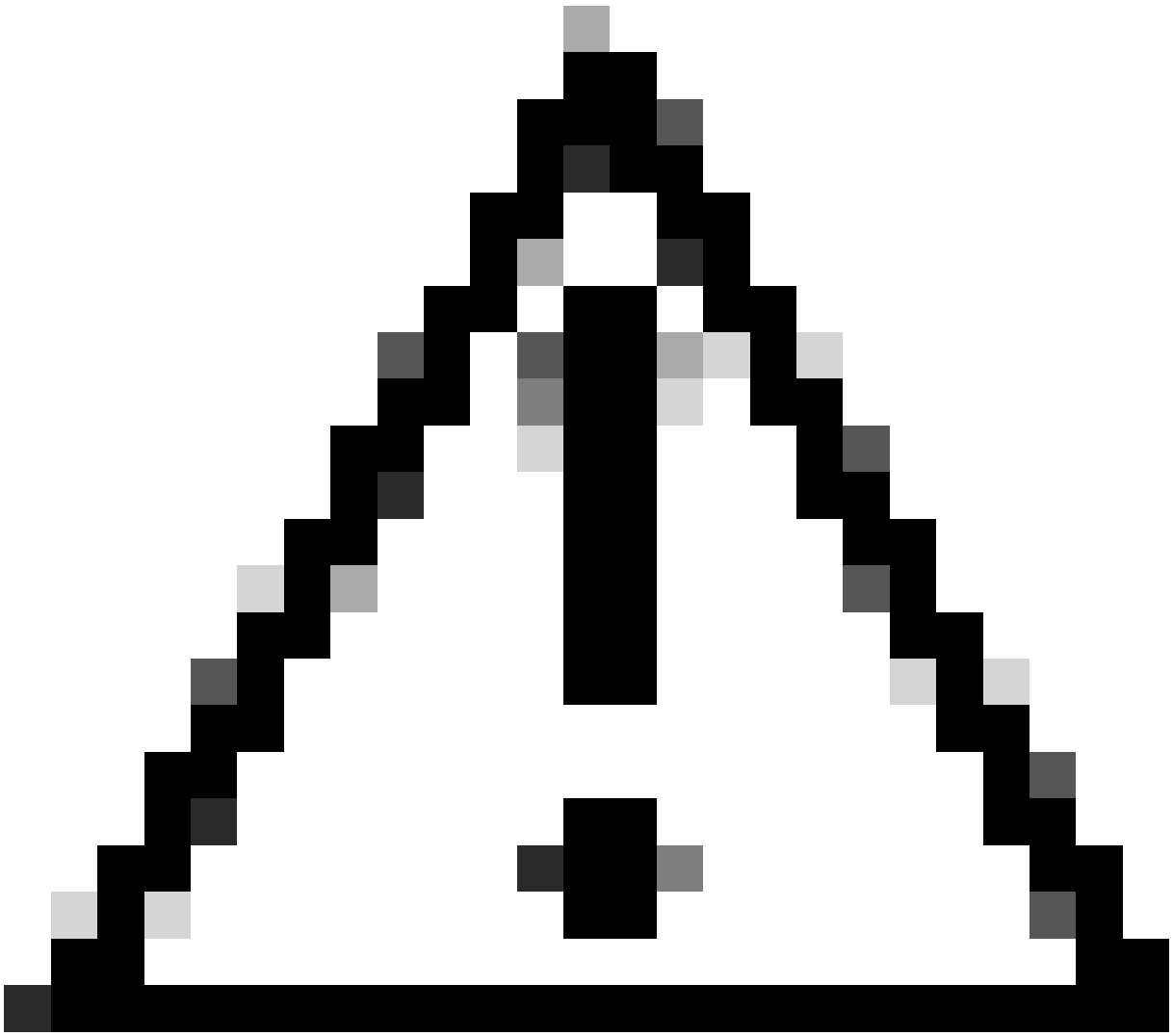
- Cisco Secure Client AnyConnect VPN
- Configuração de acesso remoto ASA/FTD.

Componentes Utilizados

O guia de práticas recomendadas baseia-se nas seguintes versões de hardware e software:

- Cisco ASA 9.x
- Firepower Threat Defense 7.x / FMC 7.x

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.



Cuidado: este documento não contém etapas do Firepower Device Manager (FDM). O FDM só oferece suporte à alteração do método de autenticação no DefaultWEBVPNGroup. Use ACLs de plano de controle ou uma porta personalizada na

---

seção 'Configurações Globais' da VPN de Acesso Remoto na interface do usuário do FDM. Entre em contato com o Cisco Technical Assistance Center (TAC) para obter assistência adicional, se necessário.

Informações de Apoio

A finalidade deste documento é garantir que a configuração do AnyConnect VPN do Cisco Secure Client esteja aderindo às melhores práticas de segurança em um mundo moderno onde os ataques de segurança cibernética são comuns.

Os ataques de força bruta geralmente envolvem tentativas repetidas de obter acesso a um recurso usando combinações de nome de usuário e senha. Os invasores tentam usar seu navegador da Internet, a interface de usuário de cliente seguro ou outras ferramentas para inserir vários nomes de usuário e senhas, esperando que correspondam a uma combinação legítima em um banco de dados AAA. Ao usar AAA para autenticação, esperamos que o usuário final insira seu nome de usuário e senha, já que isso é necessário para estabelecer a conexão. Ao mesmo tempo, não estamos verificando quem é o usuário até que ele insira suas credenciais. Por natureza, isso permite que os invasores aproveitem os seguintes cenários:

1. Nomes de domínio totalmente qualificados expostos para o Cisco Secure Firewall (especialmente ao usar aliases de grupo no perfil de conexão):
    - Se o invasor descobrir o FQDN do seu firewall VPN, ele terá a opção de selecionar o grupo de túneis usando o alias de grupo no qual deseja iniciar o ataque de força bruta.

2. Perfil de Conexão Padrão configurado com AAA ou Banco de Dados Local:
    - Se o invasor encontrar o FQDN do firewall VPN, ele poderá tentar atacar de forma forçada o servidor AAA ou o banco de dados local. Isso ocorre porque a conexão com o FQDN cai no Perfil de Conexão Padrão, mesmo que nenhum alias de grupo seja especificado.

3. Esgotamento de recursos no firewall ou em servidores AAA:
    - Os invasores podem sobrecarregar os servidores AAA ou os recursos de firewall enviando grandes quantidades de solicitações de autenticação e criando uma condição de negação de serviço (DoS).

Conceitos

Apelidos de grupo:

- Um nome alternativo pelo qual o firewall pode se referir a um perfil de conexão. Depois de iniciar uma conexão com o firewall, esses nomes aparecem em um menu suspenso na IU do Secure Client para que os usuários selecionem. A remoção de aliases de grupo remove a funcionalidade suspensa na IU do Secure Client.

URLs de grupo:

- Uma URL que pode ser vinculada a um perfil de conexão para que as conexões de entrada sejam mapeadas diretamente para um perfil de conexão desejado. Não há nenhuma funcionalidade suspensa, pois os usuários podem inserir a URL completa na IU do Secure Client ou a URL pode ser integrada a um 'Nome de exibição' no perfil XML para ocultar a URL do usuário.

A diferença aqui é quando os aliases de grupo são implementados, um usuário inicia uma conexão to vpn_gateway.example.com e é apresentado com aliases para selecionar a unidade para um perfil de conexão. Com URLs de grupo, um usuário inicia uma conexão com vpn_gateway.example.com/example_group e os direciona diretamente ao perfil de conexão sem a necessidade ou opção de um menu suspenso.

Práticas de fortalecimento do cliente seguro no Cisco Secure Firewall:

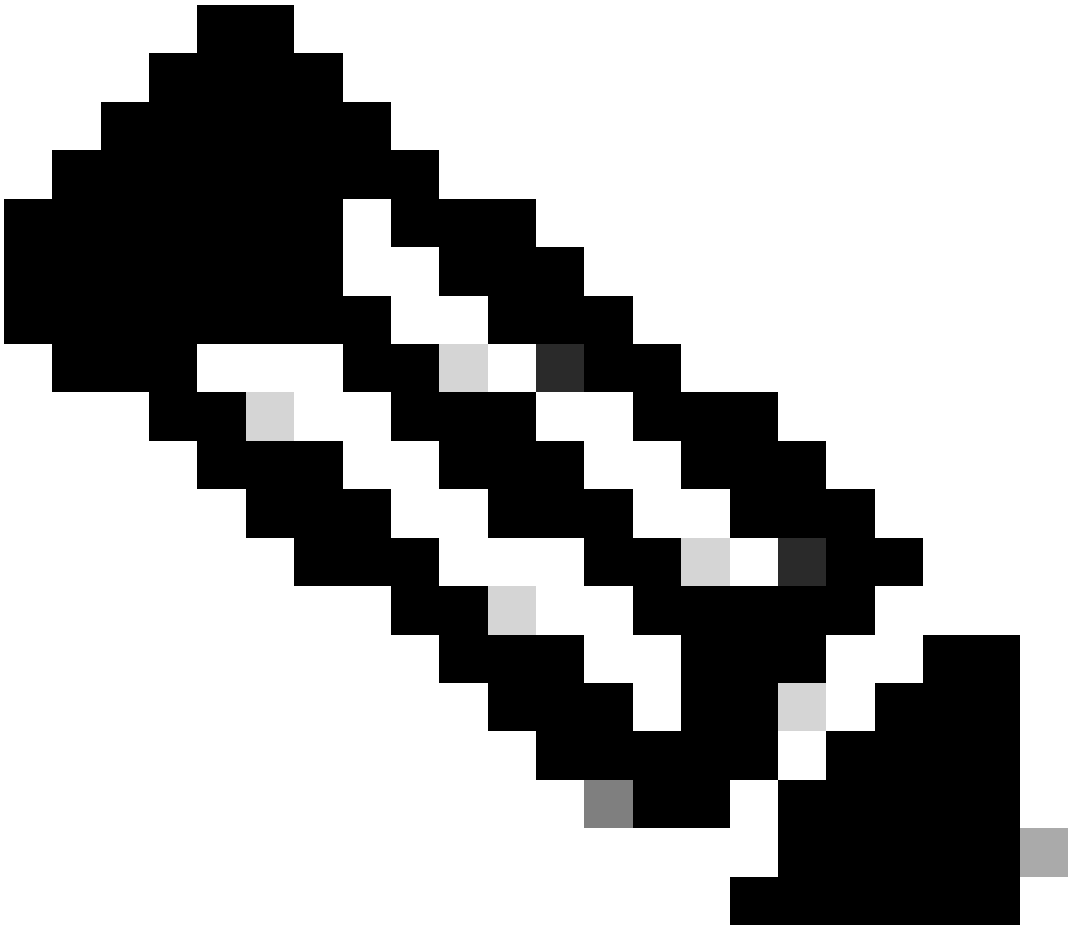
Esses métodos dependem do mapeamento de usuários legítimos para perfis de conexão/grupos de túneis apropriados, enquanto usuários potencialmente mal-intencionados são enviados para um grupo de túneis de interceptação que configuramos para não permitir combinações de nome de usuário e senha. Embora nem todas as combinações devam ser implementadas, a desabilitação de aliases de grupo e a alteração do método de autenticação de DefaultWEBVPNGroup e DefaultRAGroup são necessárias para que as recomendações funcionem de forma eficaz.

- Desabilite os aliases de grupo e use apenas group-url na configuração Perfil de Conexão; isso permite que você tenha um FQDN específico que não será fácil para um invasor descobrir e selecionar, já que apenas os clientes com o FQDN apropriado podem iniciar a conexão. Por exemplo, vpn_gateway.example.com/example_group é mais difícil para um invasor descobrir do que vpn_gateway.example.com.

- Desabilite a autenticação AAA no DefaultWEBVPNGroup e no DefaultRAGroup e configure a autenticação de certificado; isso evita uma possível força bruta contra o banco de dados local ou o servidor AAA. O invasor nesse cenário seria apresentado com erros imediatos ao tentar se conectar. Não há nenhum campo de nome de usuário ou senha, pois a autenticação é baseada em certificados, interrompendo, assim, tentativas de força bruta. Outra opção é criar um servidor AAA sem configuração de suporte para criar um sinkhole para solicitações mal-intencionadas.

- Utilize o mapeamento de certificado para o perfil de conexão. Isso permite que as conexões de entrada sejam mapeadas para perfis de conexão específicos com base nos atributos recebidos de certificados no dispositivo cliente. Os usuários que têm os certificados apropriados são mapeados corretamente, enquanto os invasores que falham nos critérios de mapeamento são enviados para o DefaultWEBVPNGroup.

- O uso de IKEv2-IPSec em vez de SSL faz com que os grupos de túneis dependam de um mapeamento de grupo de usuários específico no perfil XML. Sem esse XML na máquina do usuário final, os usuários são enviados automaticamente para o grupo de túneis padrão.



Observação: para obter mais informações sobre a funcionalidade de alias de grupo, consulte o ASA VPN Configuration Guide e observe a 'Tabela 1. Atributos do perfil de conexão para VPN SSL'.

Identificar ataques usando IDs de registro e syslog

Os ataques de força bruta representam o método predominante de comprometer as VPNs de acesso remoto, explorando senhas fracas para obter entrada não autorizada. É crucial saber como reconhecer os sinais de um ataque aproveitando o uso de registro e avaliando syslogs. Os IDs de syslogs comuns que podem indicar um ataque se encontrados com volume anormal são:

%ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database : user = admin : user

%ASA-6-113005

<#root>

%ASA-6-113005

: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =

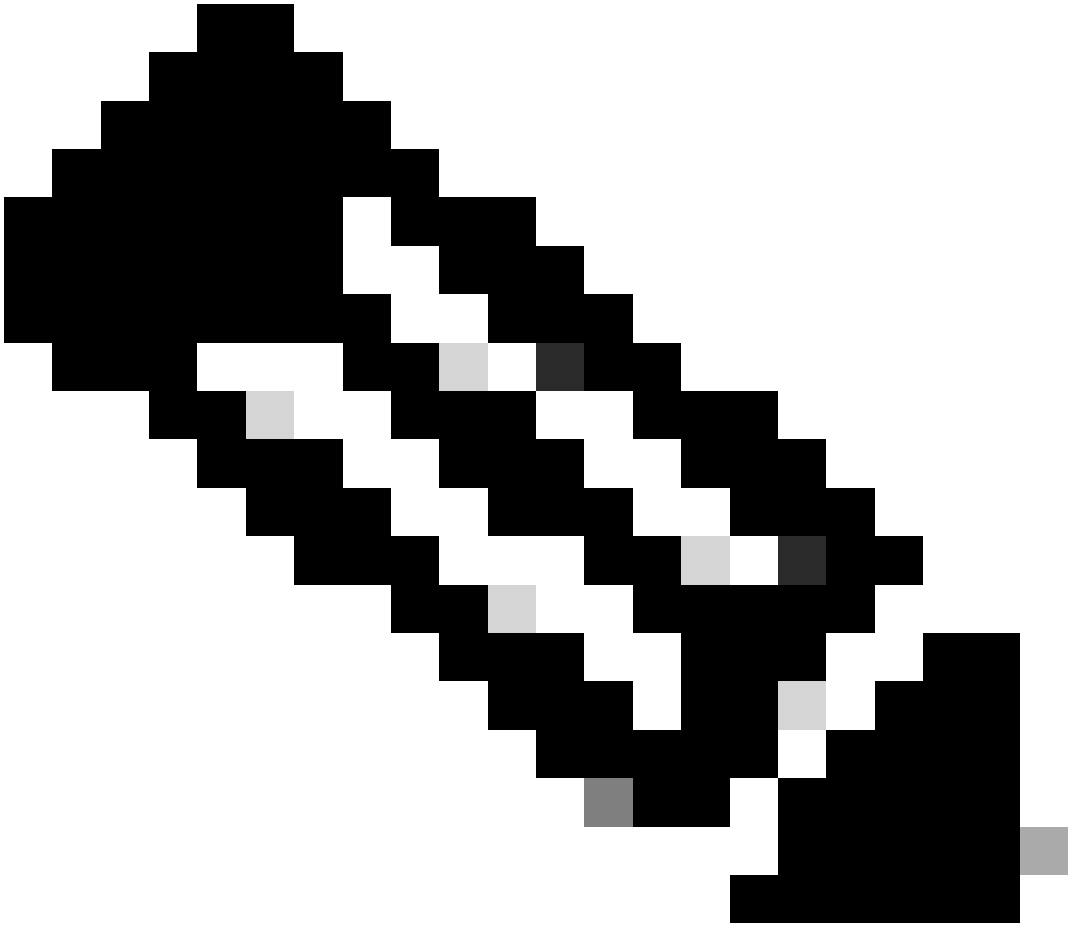
%ASA-6-716039

<#root>

%ASA-6-716039

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN

O nome de usuário está sempre oculto até que o comando no logging hide username seja configurado no ASA.



Observação: Observação: isso fornece informações sobre usuários válidos gerados ou conhecidos por IPs ofensivos. No entanto, tenha cuidado, pois os nomes de usuário são visíveis nos logs.

Registro do Cisco ASA:

Guia do usuário para proteger o firewall ASA
Capítulo Registro do Guia de configuração da CLI de operações gerais do Cisco Secure Firewall ASA Series

Registro do Cisco FTD:

Configurar o registro no FTD usando o FMC

Seção Configurar Syslog no capítulo Configurações de plataforma do Guia de Configuração de Dispositivos do Cisco Secure Firewall Management Center
Configurar e verificar o Syslog no Gerenciador de dispositivos do Firepower

Seção Definindo as configurações de registro do sistema no capítulo Configurações do sistema do Guia de configuração do Cisco Firepower Threat Defense para o Firepower Device Manager

Verificação de ataque

Para verificar, faça login no ASA ou na Interface de Linha de Comando (CLI) do FTD, execute o comando show aaa-server e investigue se há um número incomum de solicitações de autenticação tentadas e rejeitadas para qualquer um dos servidores AAA configurados:

<#root>

```
ciscoasa#
show aaa-server


Server Group: LOCAL - - - - - >>>> Sprays against the LOCAL database
Server Protocol: Local database
Server Address: None
Server port: None
Server status: ACTIVE, Last transaction at 16:46:01 UTC Fri Mar 22 2024
Number of pending requests 0
Average round trip time 0ms
Number of authentication requests 8473575 - - - - - >>>> Unusual increments
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 0
Number of rejects 8473574 - - - - - >>>> Unusual increments
```

<#root>

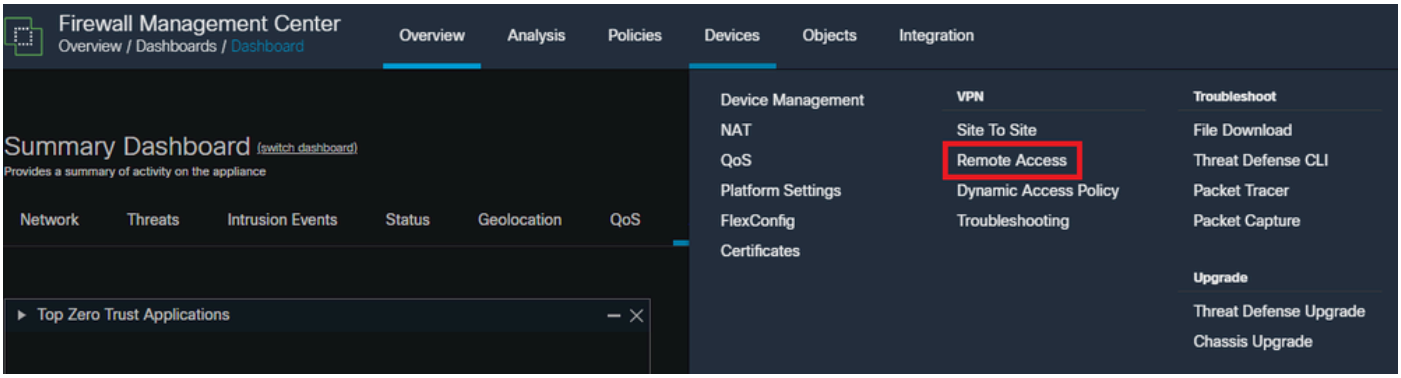
```
ciscoasa#
show aaa-server


Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
Number of authentication requests 2228536 - - - - - >>>> Unusual increments
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312
Number of rejects 2225363 - - - - - >>>> Unusual increments
Number of challenges 0
Number of malformed responses 0
```

```
Number of bad authenticators 0
Number of timeouts 1
Number of unrecognized responses 0
```

Exemplos de configuração do FMC

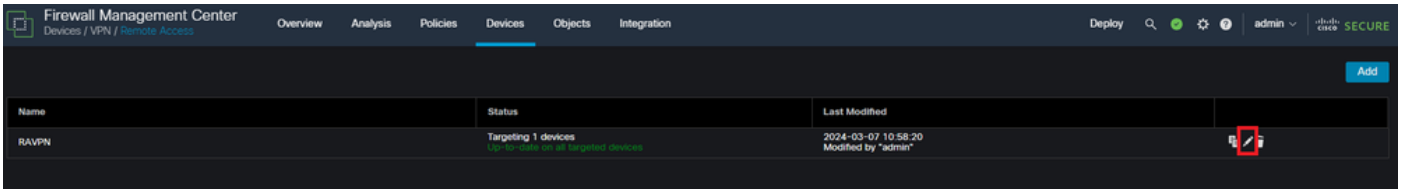
Desative a autenticação AAA nos perfis de conexão DefaultWEBVPNGroup e DefaultRAGroup

Navegue até Devices > Remote Access.



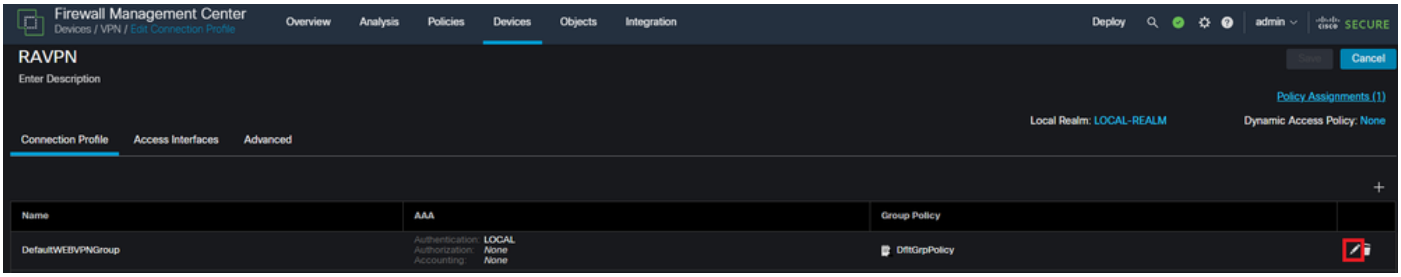
Exibe a navegação na GUI do FMC para acessar a configuração da política de VPN de acesso remoto.

Edite a Política de VPN de Acesso Remoto existente e crie um perfil de conexão chamado 'DefaultRAGroup'



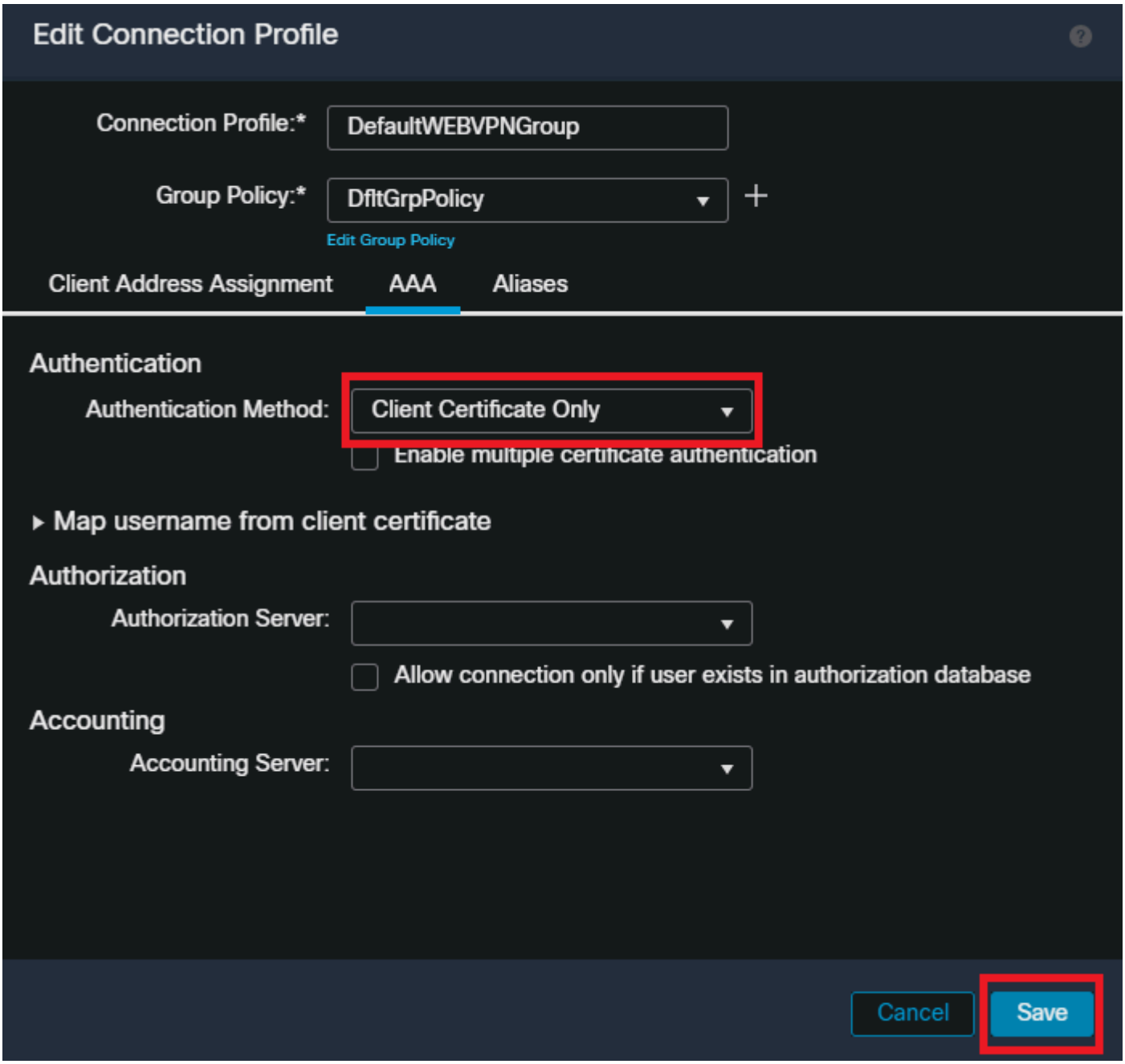
Exibe como editar a política de VPN de acesso remoto na interface do usuário do FMC.

Edite os perfis de conexão denominados 'DefaultWEBVPNGroup' e 'DefaultRAGroup'



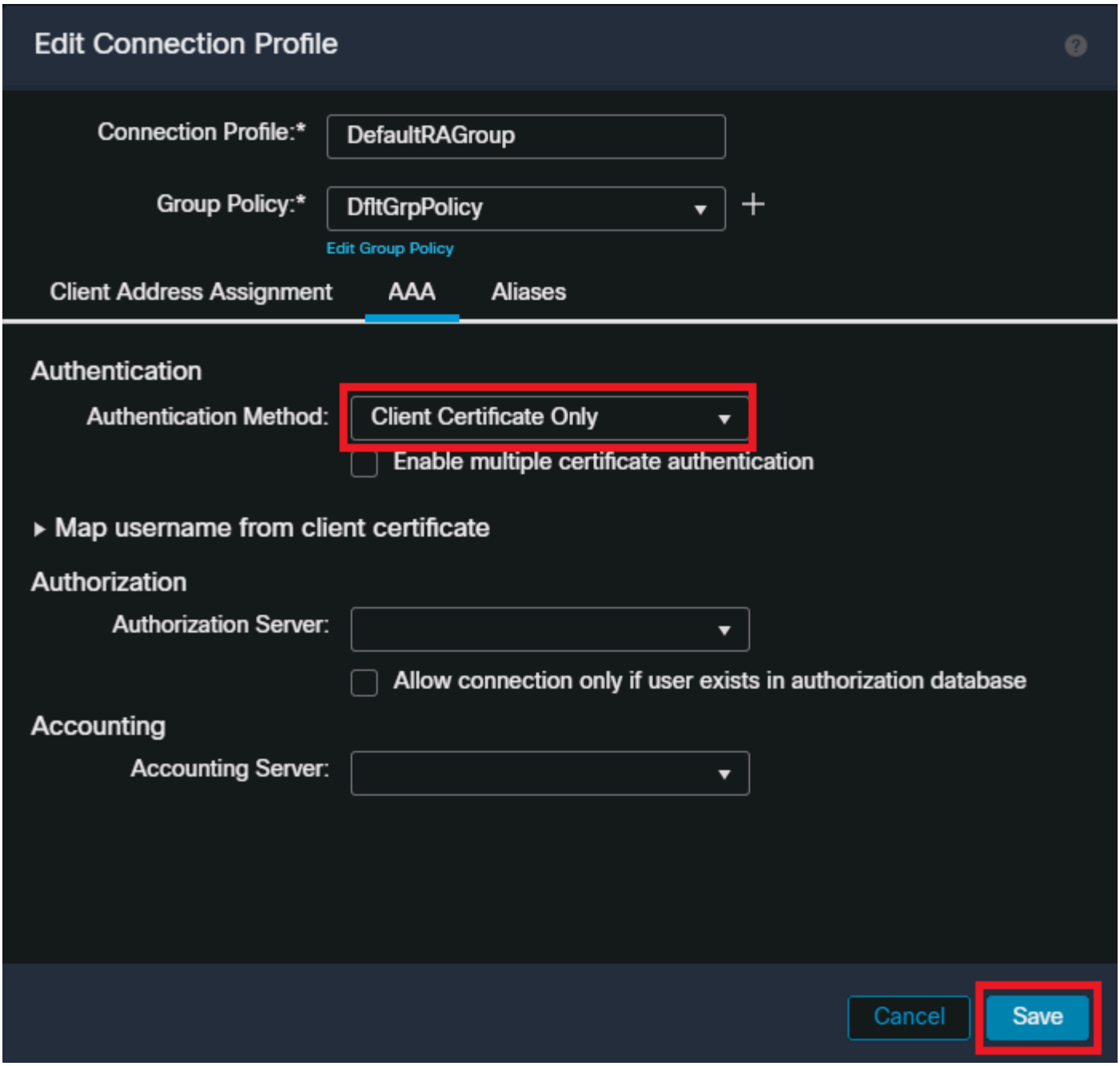
Exibe como editar o DefaultWEBVPNGroup na interface do FMC.

Navegue até a guia AAA e selecione o menu suspenso Authentication Method. Selecione 'Somente certificado do cliente' e selecione Salvar.

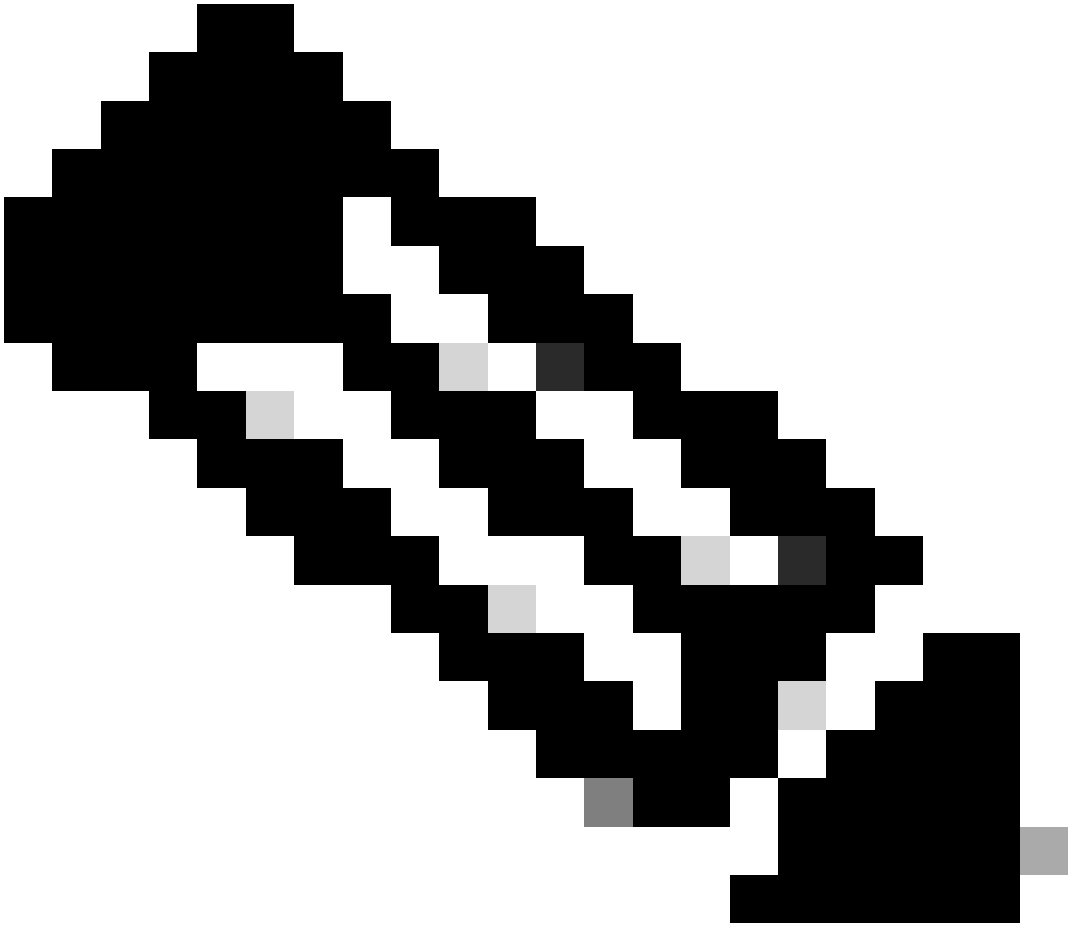


Alterando o método de autenticação para certificado de cliente somente para DefaultWEBVPNGroup na interface do usuário do FMC.

Edite o DefaultRAGroup e navegue até a guia AAA e selecione o menu suspenso Authentication Method. Selecione 'Somente certificado do cliente' e Salvar.



Alterar o método de autenticação para certificado de cliente somente para DefaultRAGroup na interface do usuário do FMC.

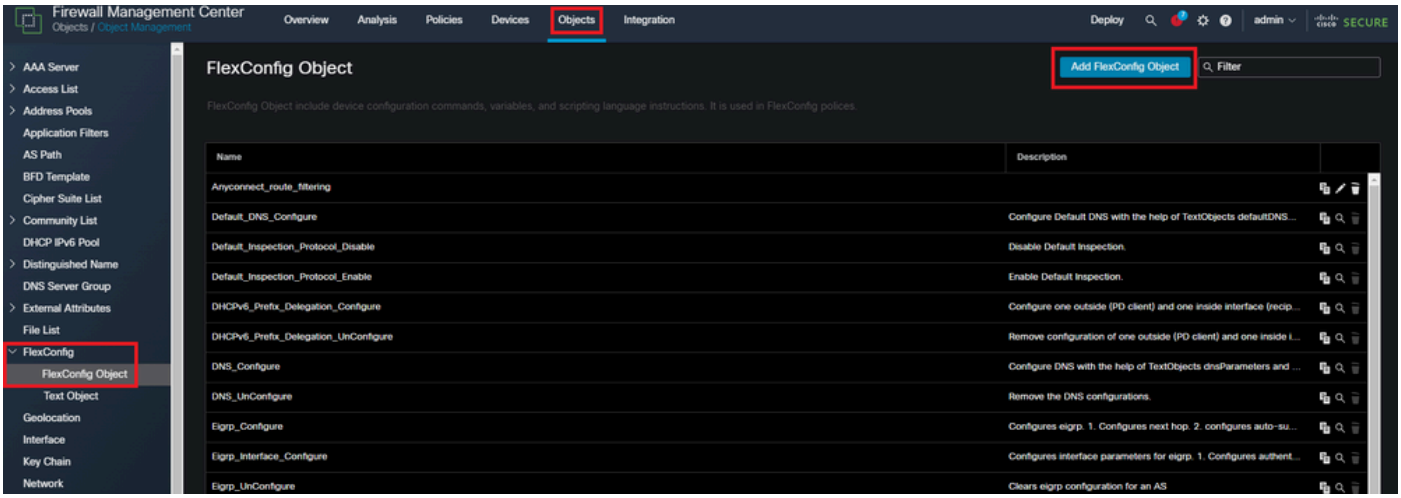


Observação: o método de autenticação também pode ser um servidor AAA sinkhole. Se esse método for usado, a configuração do servidor AAA será falsa e não processará nenhuma solicitação. Um pool de VPNs também deve ser definido na guia "Client Address Assignment" (Atribuição de endereço de cliente) para salvar as alterações.

Desative a verificação de host/postura de firewall seguro em DefaultWEBVPNGroup e DefaultRAGroup (opcional)

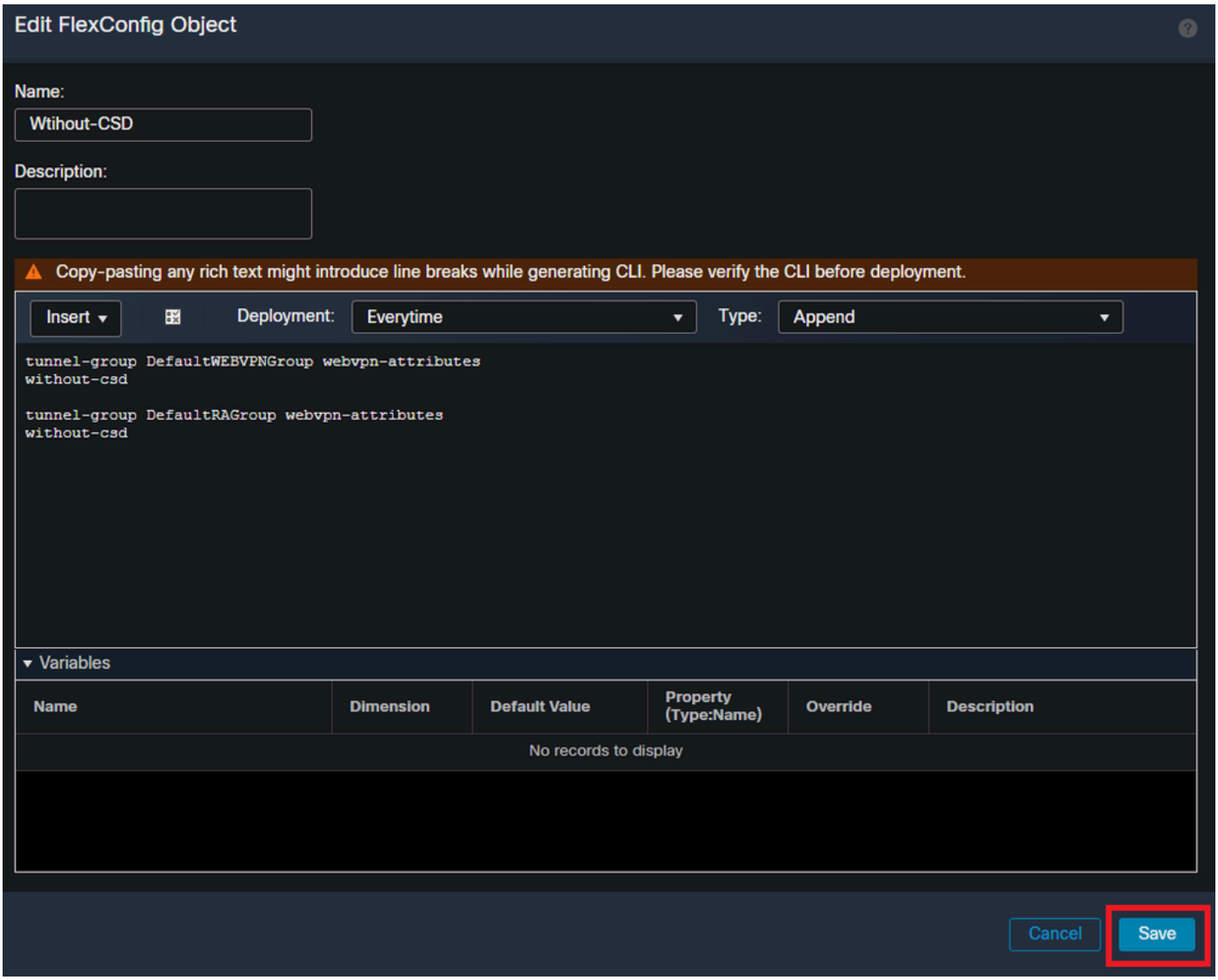
Isso só é necessário se você tiver o Hostscan / Secure Firewall Posture em seu ambiente. Essa etapa impede que os invasores aumentem a utilização de recursos no firewall causada pelo processo de verificação de endpoint. No FMC, isso é obtido com a criação de um objeto FlexConfig com o comando without-csd para desabilitar a funcionalidade de verificação de endpoint.

Navegue até Objetos > Gerenciamento de objetos > Objeto FlexConfig > Adicionar objeto FlexConfig.



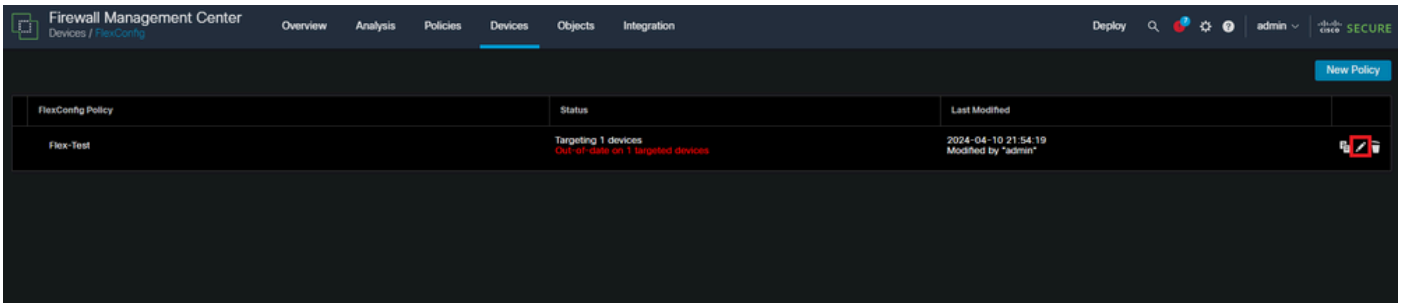
Navegação na interface do usuário do FMC para criar um objeto FlexConfig.

Nomeie o objeto FlexConfig, defina a implantação como Everytime com o tipo Append. Em seguida, insira a sintaxe exatamente como mostrada e salve o objeto.



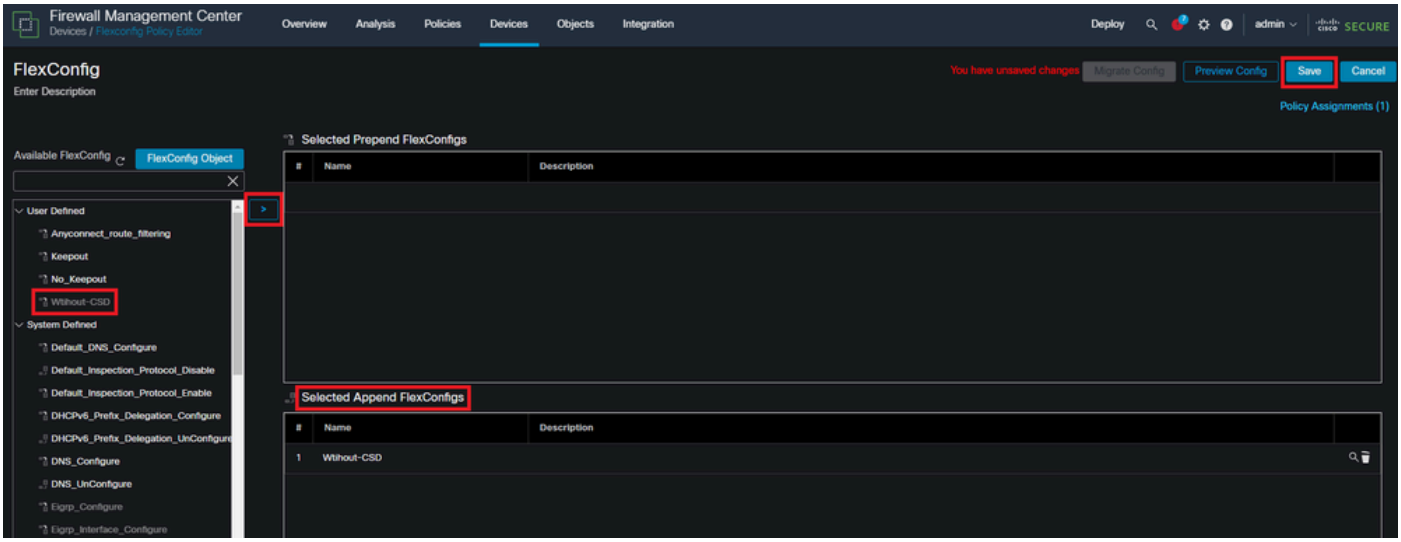
Criando um objeto FlexConfig com 'without-csd'

Navegue até Devices > FlexConfig e clique no Pencil para editar a Política FlexConfig.



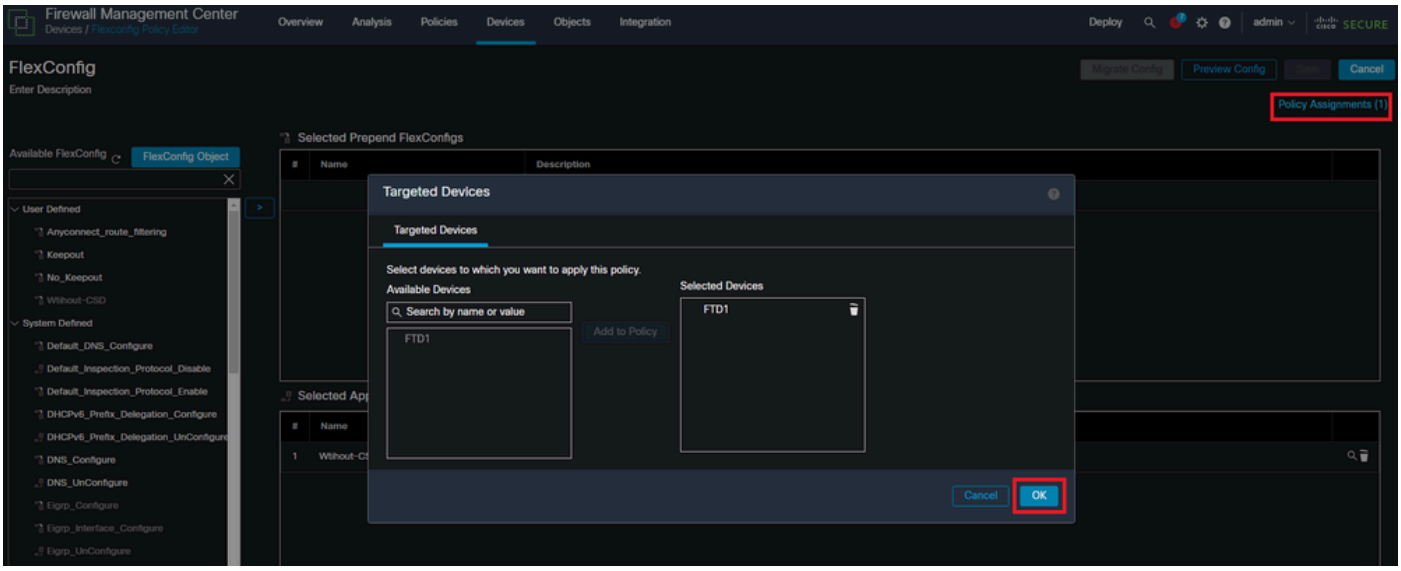
Edição da política FlexConfig no FMC.

Localize o objeto criado na seção Definido pelo usuário. Em seguida, selecione a seta para adicioná-la ao Seleted Append FlexConfigs. Por fim, selecione Salvar para salvar a política FlexConfig.



Anexe o objeto FlexConfig à política FlexConfig.

Selecione Policy Assignments e escolha o FTD ao qual você deseja aplicar esta política FlexConfig e, em seguida, selecione OK. Selecione Salvar novamente se esta for uma nova atribuição FlexConfig e implante as alterações. Após a implantação, verifique



Atribua a política FlexConfig a um dispositivo FirePOWER.

Insira o FTD CLI e emita o comando show run tunnel-group para o DefaultWEBVPNGroup e o DefaultRAGroup. Verifique se without-csd agora está presente na configuração.

<#root>

FTD72#

show run tunnel-group DefaultRAGroup

```
tunnel-group DefaultRAGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultRAGroup webvpn-attributes
authentication certificate
```

without-csd

FTD72#

show run tunnel-group DefaultWEBVPNGroup

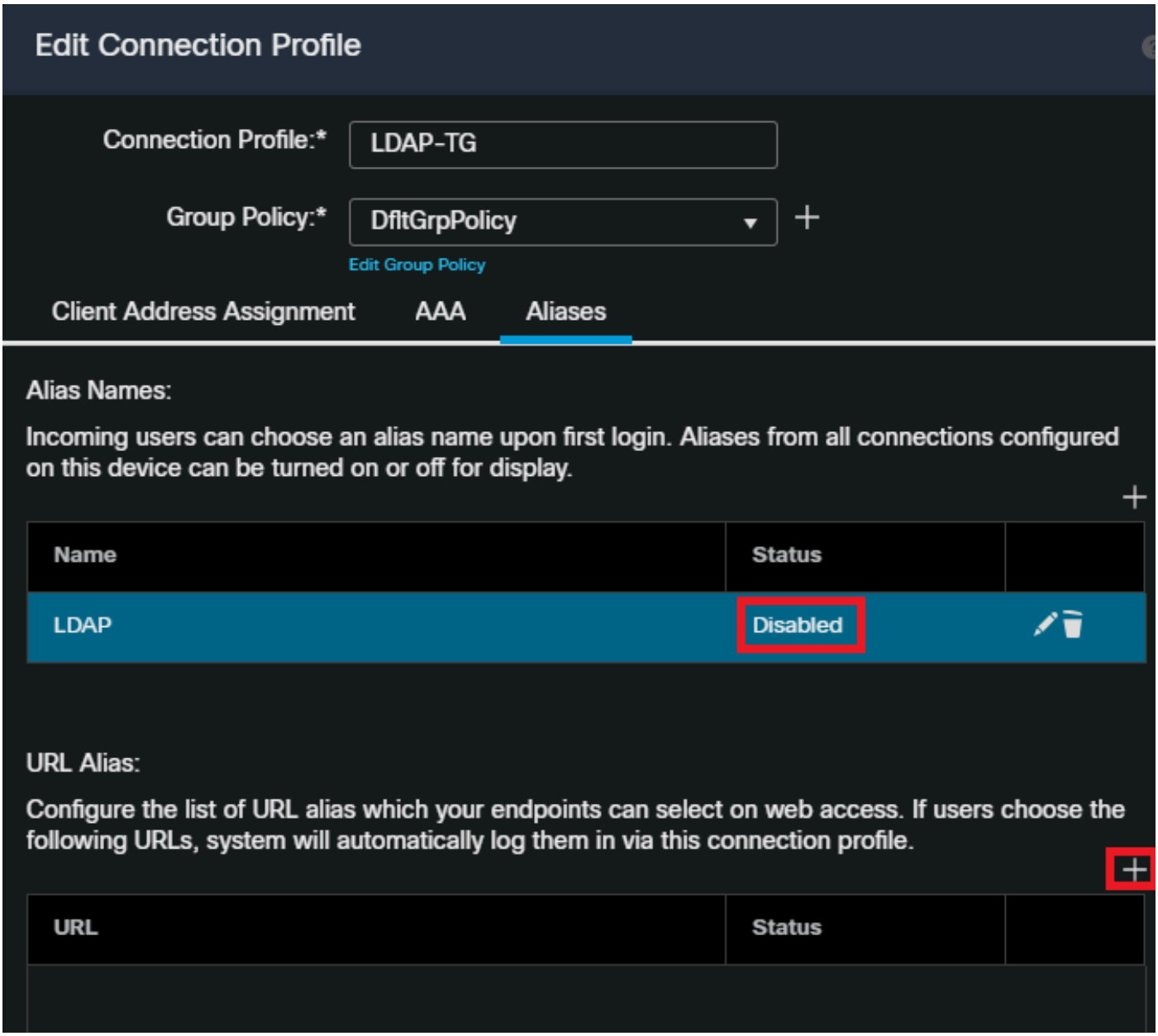
```
tunnel-group DefaultWEBVPNGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultWEBVPNGroup webvpn-attributes
authentication certificate
```

without-csd

Desabilitar aliases de grupo e Habilitar URLs de grupo

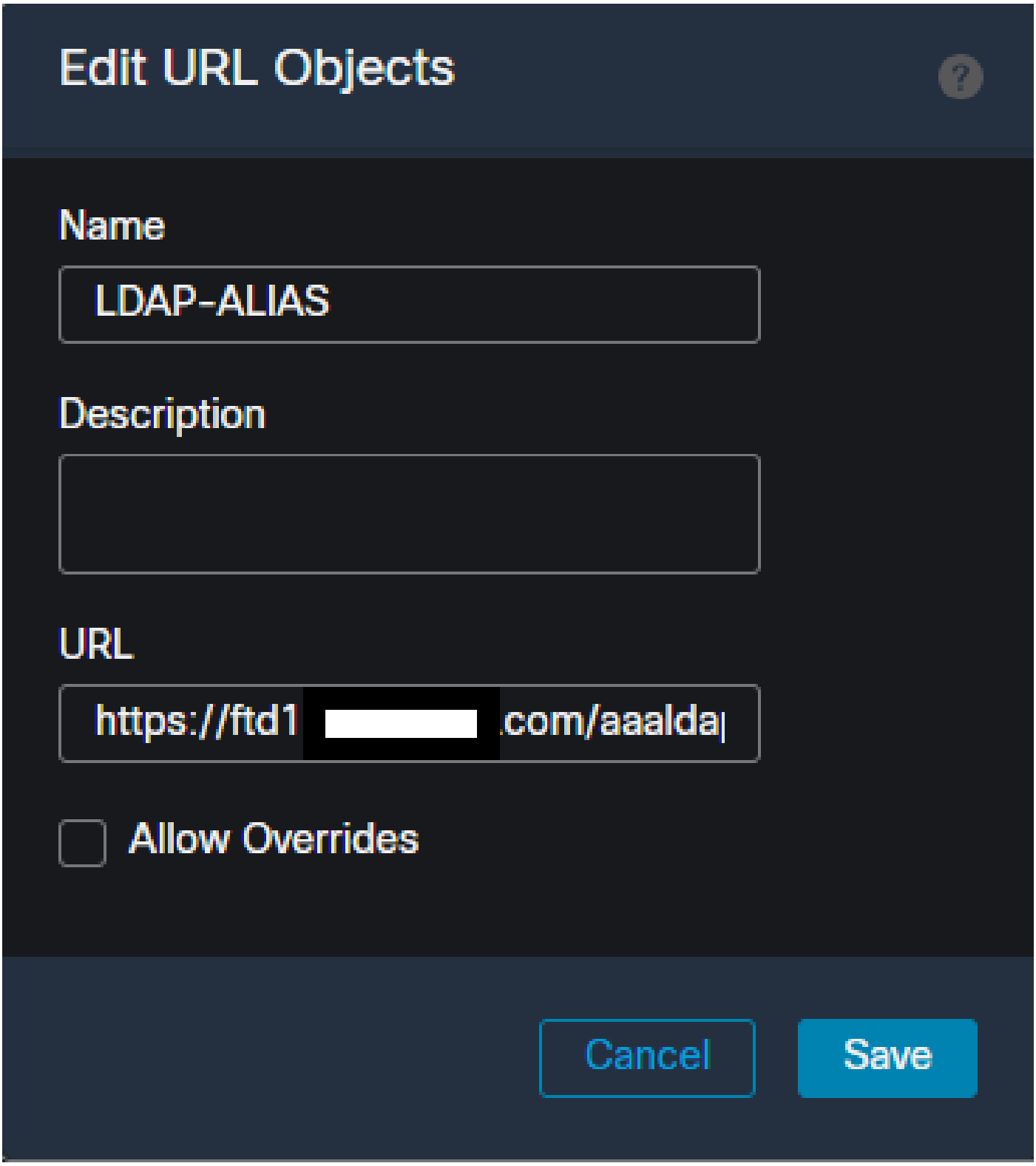
Navegue até um perfil de conexão e selecione a guia 'Aliases'. Desative ou exclua o alias de

grupo e clique no ícone de adição para adicionar um alias de URL.



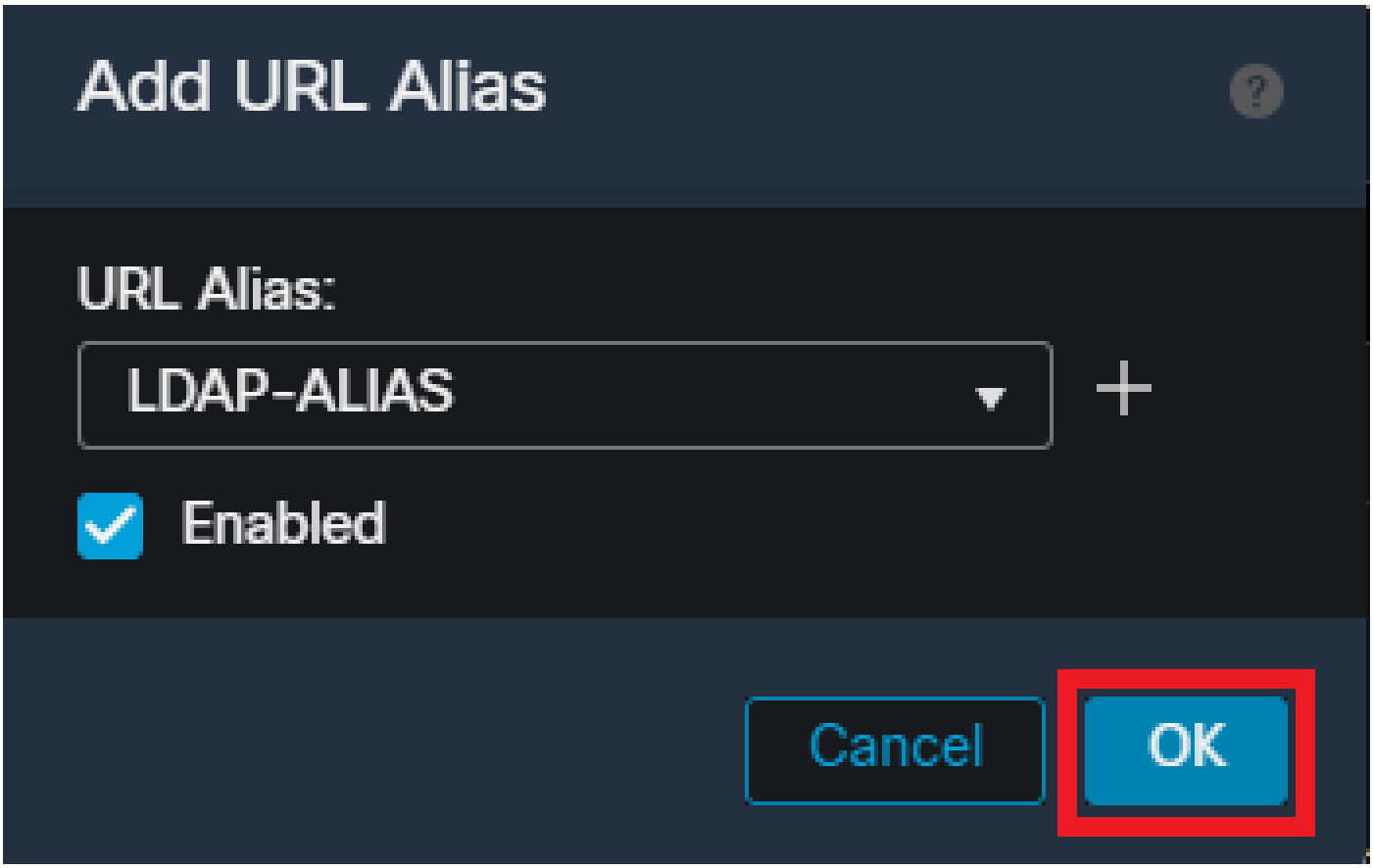
Desabilitando a opção group-alias para um grupo de túneis na interface do usuário do FMC.

Configure um nome de objeto para o alias de URL e preencha o FQDN e/ou o endereço IP do firewall para o URL, seguido do nome ao qual você deseja associar o perfil de conexão. Neste exemplo, escolhemos 'aaldap'. Quanto mais obscuro, mais seguro, pois é menos provável que os invasores adivinhem o URL completo, mesmo que tenham obtido seu FQDN. Quando terminar, selecione Salvar.



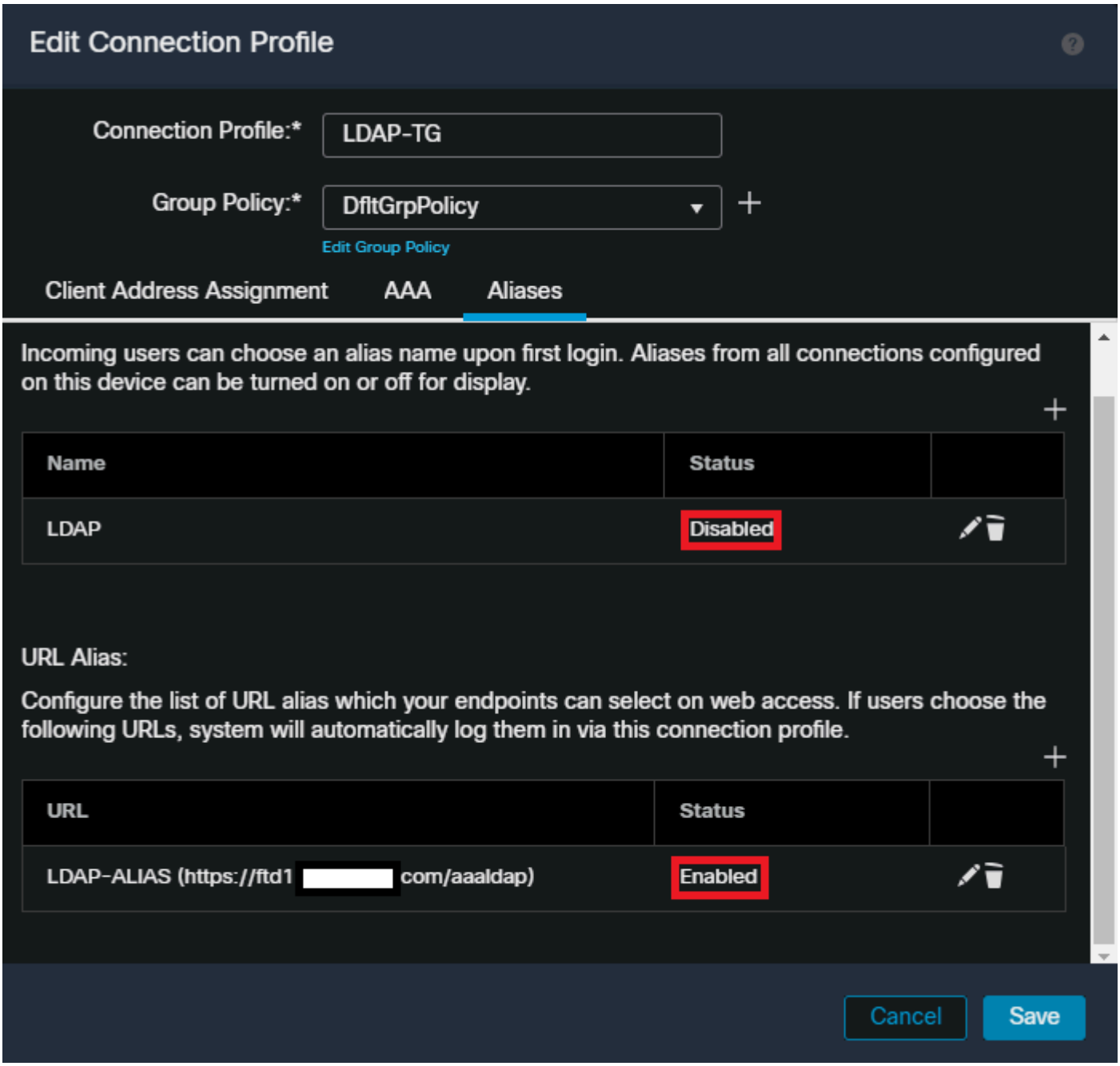
Criação de um objeto URL-Alias na interface do usuário do FMC.

Selecione o Alias de URL no menu suspenso, marque a caixa Enabled e selecione OK.



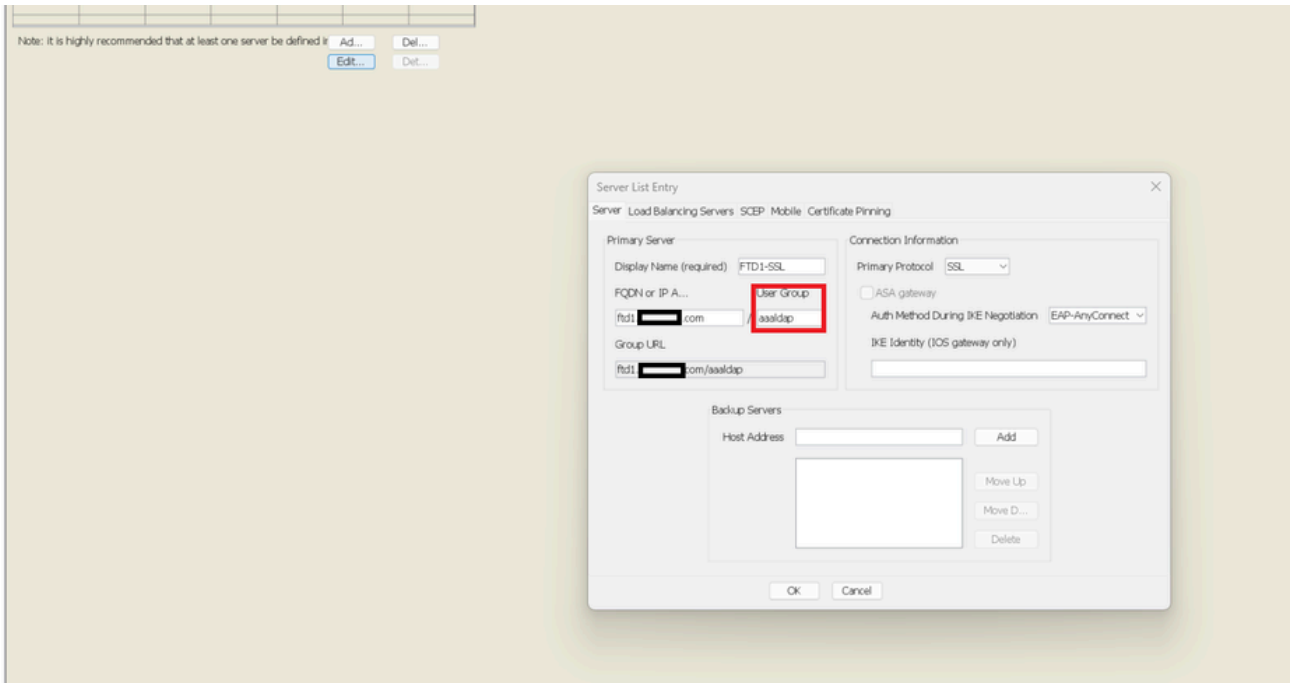
Verifique se o URL-Alias está habilitado na interface do usuário do FMC.

Verifique se o alias de grupo foi excluído ou desabilitado e se o Alias de URL está habilitado e selecione Salvar.



Ativação da opção URL-Alias para um grupo de túneis na interface do usuário do FMC.

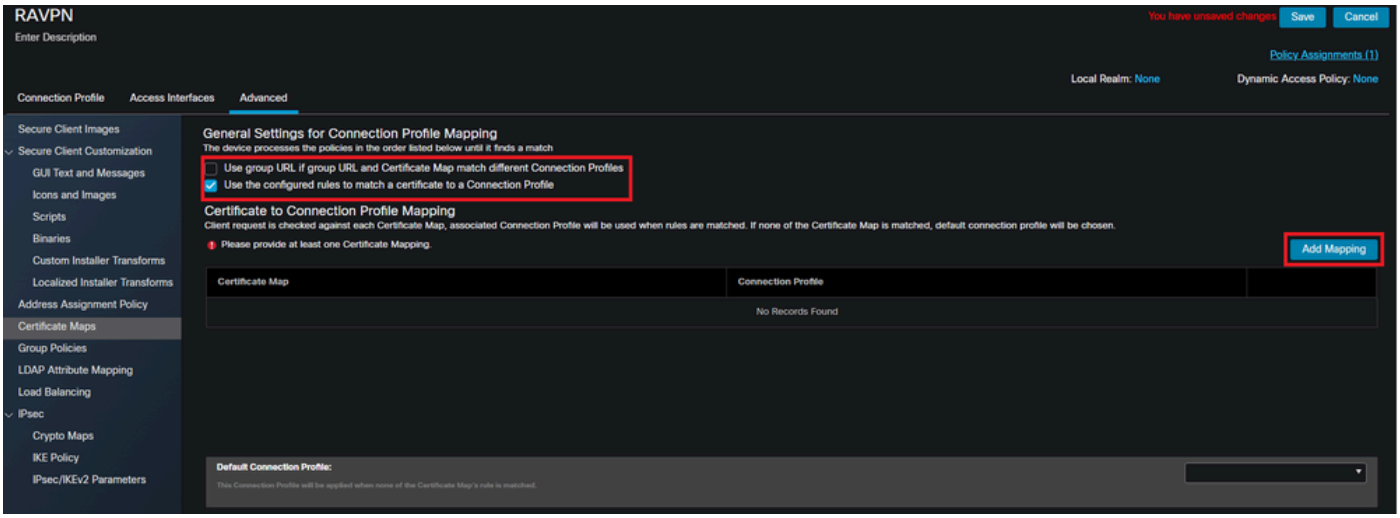
Se desejar, os aliases de URL também podem ser enviados como parte do XML. Isso é obtido editando o XML usando o VPN Profile Editor ou o ASA Profile Editor. Para fazer isso, navegue até a guia Lista de servidores e verifique se o campo Grupo de usuários corresponde ao Alias de URL do perfil de conexão ao usar SSL. Para IKEv2, certifique-se de que o campo User Group (Grupo de usuários) corresponda ao nome exato do perfil de conexão.



Editando o perfil XML para ter um URL-Alias para conexões SSL.

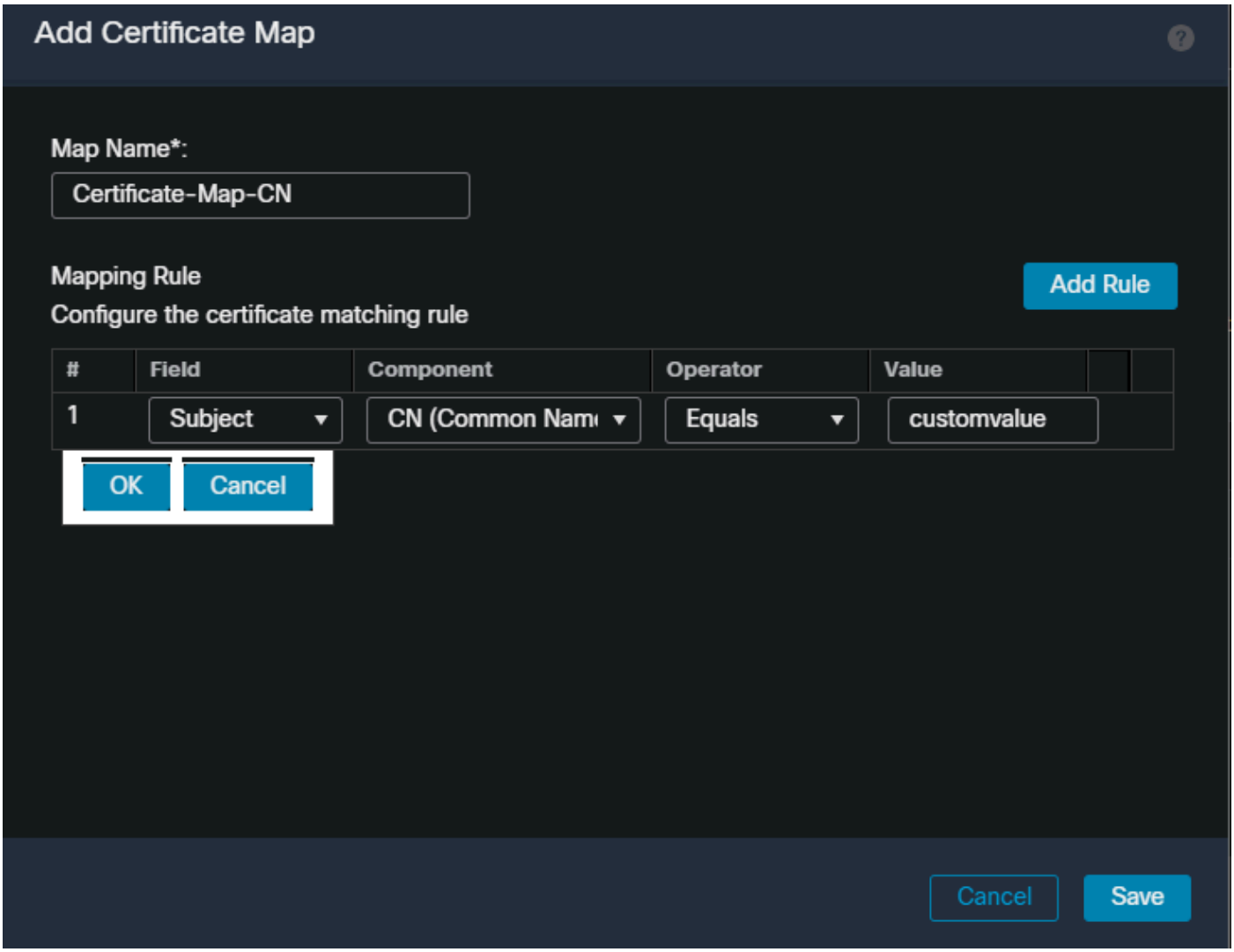
Mapeamento de certificado

Navegue até a guia Advanced dentro da Política de VPN de acesso remoto. Escolha uma opção de configuração geral com base na preferência. Depois de selecionado, selecione Adicionar Mapeamento.



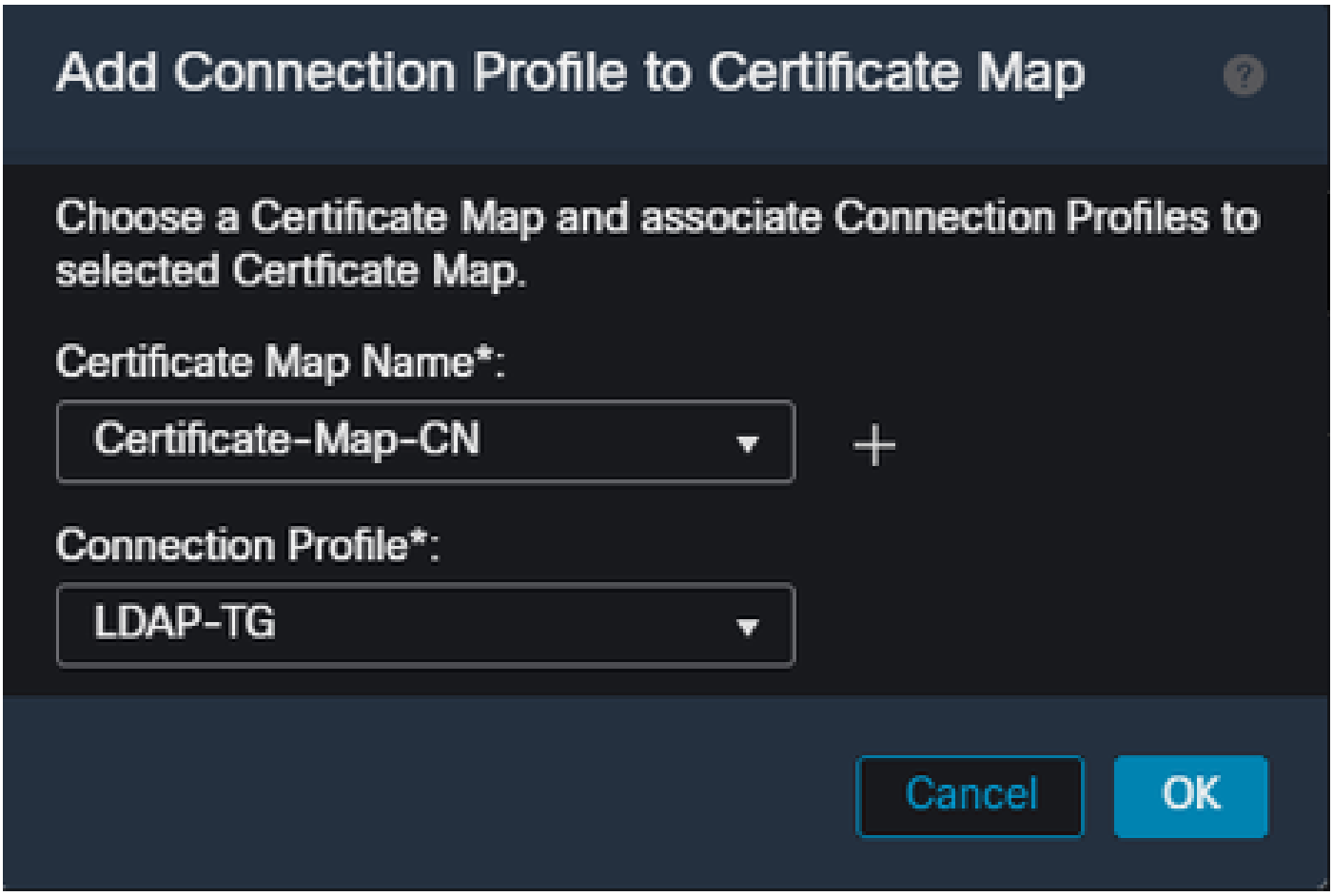
Navegar até a guia Avançado na interface do usuário do FMC para criar um objeto de mapa de certificado na interface do usuário do FMC.

Nomeie o objeto de mapa do certificado e selecione Adicionar Regra. Nesta regra, defina as propriedades do certificado que você deseja identificar para mapear o usuário para um determinado perfil de conexão. Quando terminar, selecione OK e, em seguida, Salvar.



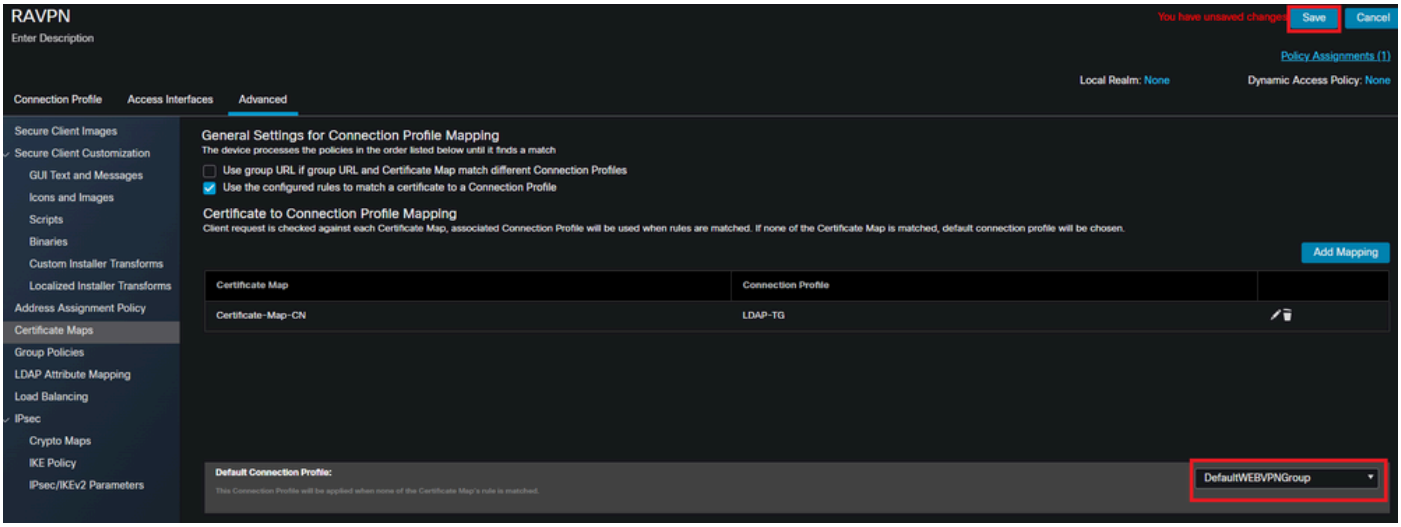
Crie um mapa de certificado e adicione critérios para o mapa na interface do usuário do FMC.

No menu suspenso, selecione o objeto de mapa de certificado e o perfil de conexão ao qual deseja que o mapa de certificado seja associado. Em seguida, selecione OK.



Vincule o objeto de mapa do certificado ao grupo de túneis desejado na interface do usuário do FMC.

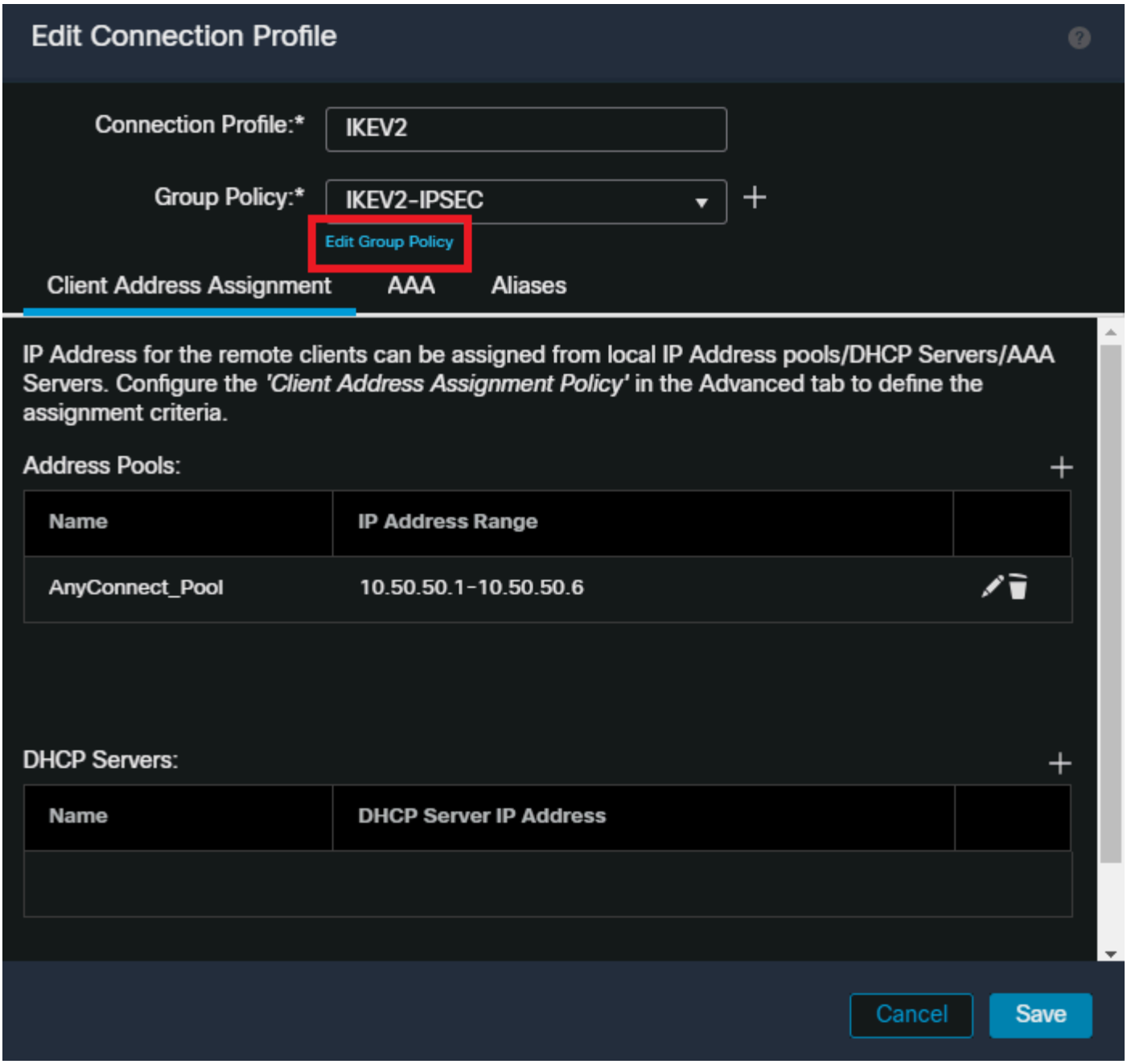
Verifique se o Perfil de Conexão Padrão está configurado como DefaultWEBVPNGroup para que, se um usuário falhar no mapeamento, ele seja enviado para o DefaultWEBVPNGroup. Quando terminar, selecione Save e implante as alterações.



Altere o perfil de conexão padrão do mapeamento de certificado para DefaultWEBVPNGroup na interface do usuário do FMC.

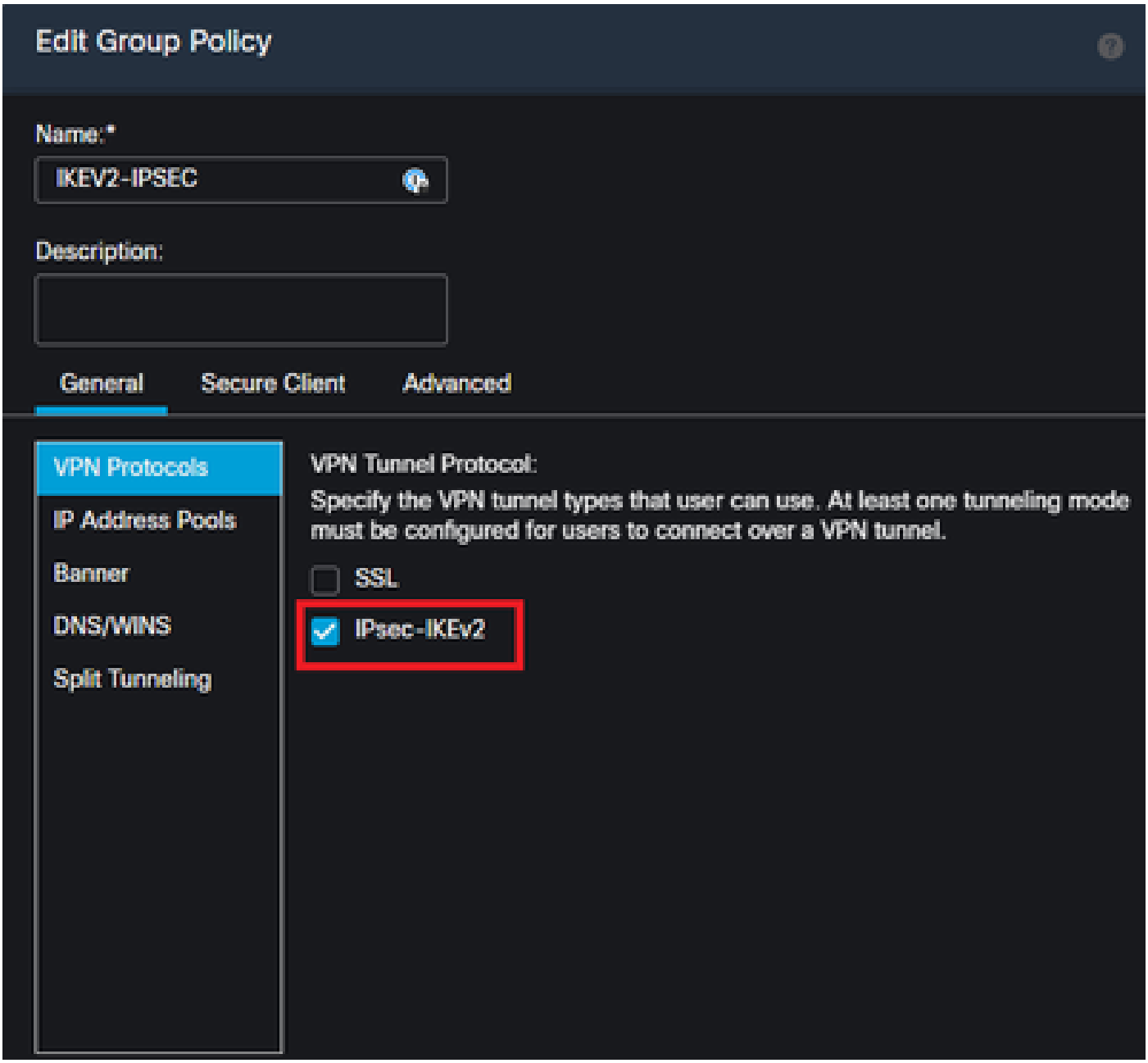
IPsec-IKEv2

Selecione o perfil de conexão IPsec-IKEv2 desejado e navegue para Editar política de grupo.



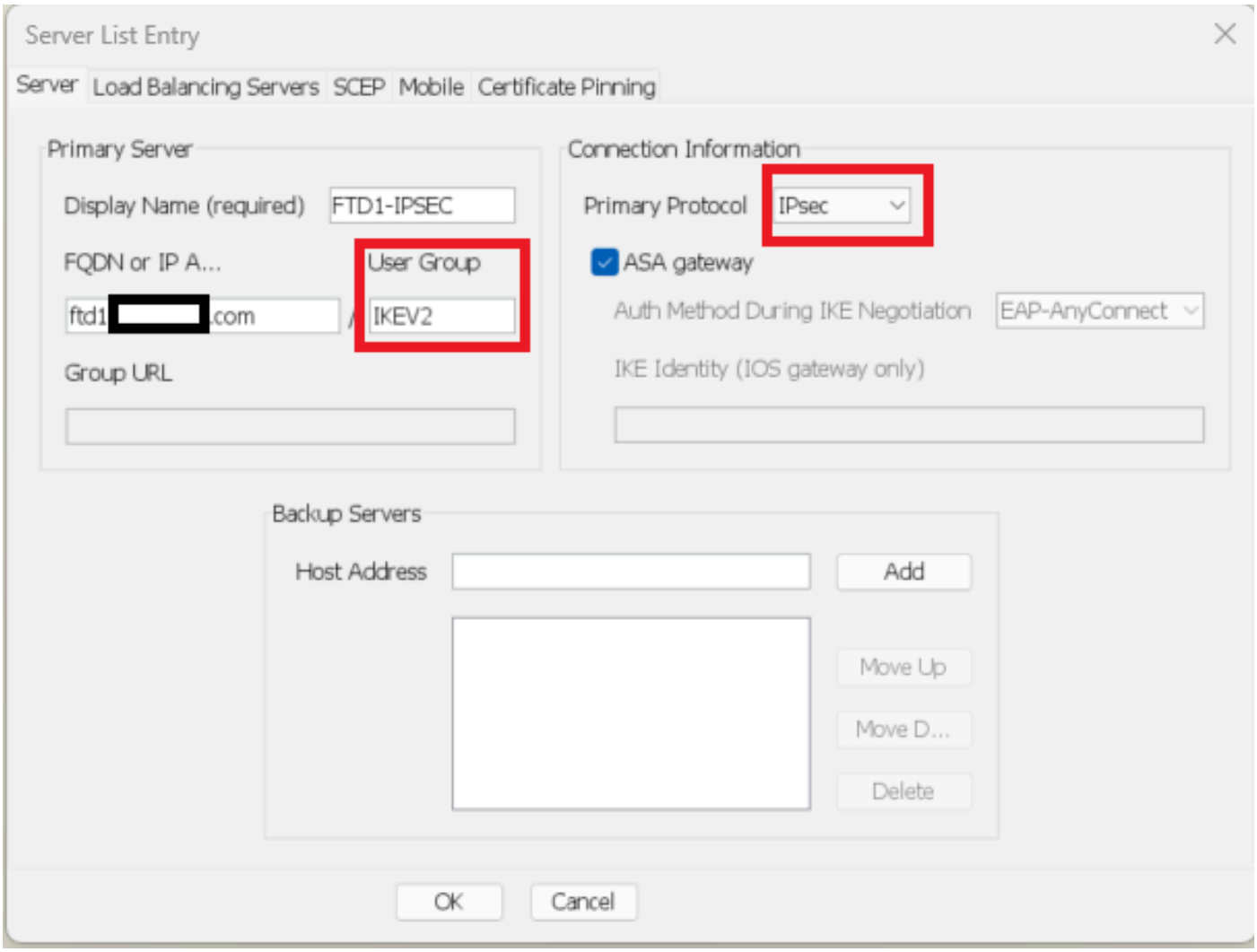
Edite uma política de grupo na interface do usuário do FMC.

Na guia General, navegue até a seção VPN Protocols e verifique se a caixa IPsec-IKEv2 está marcada.

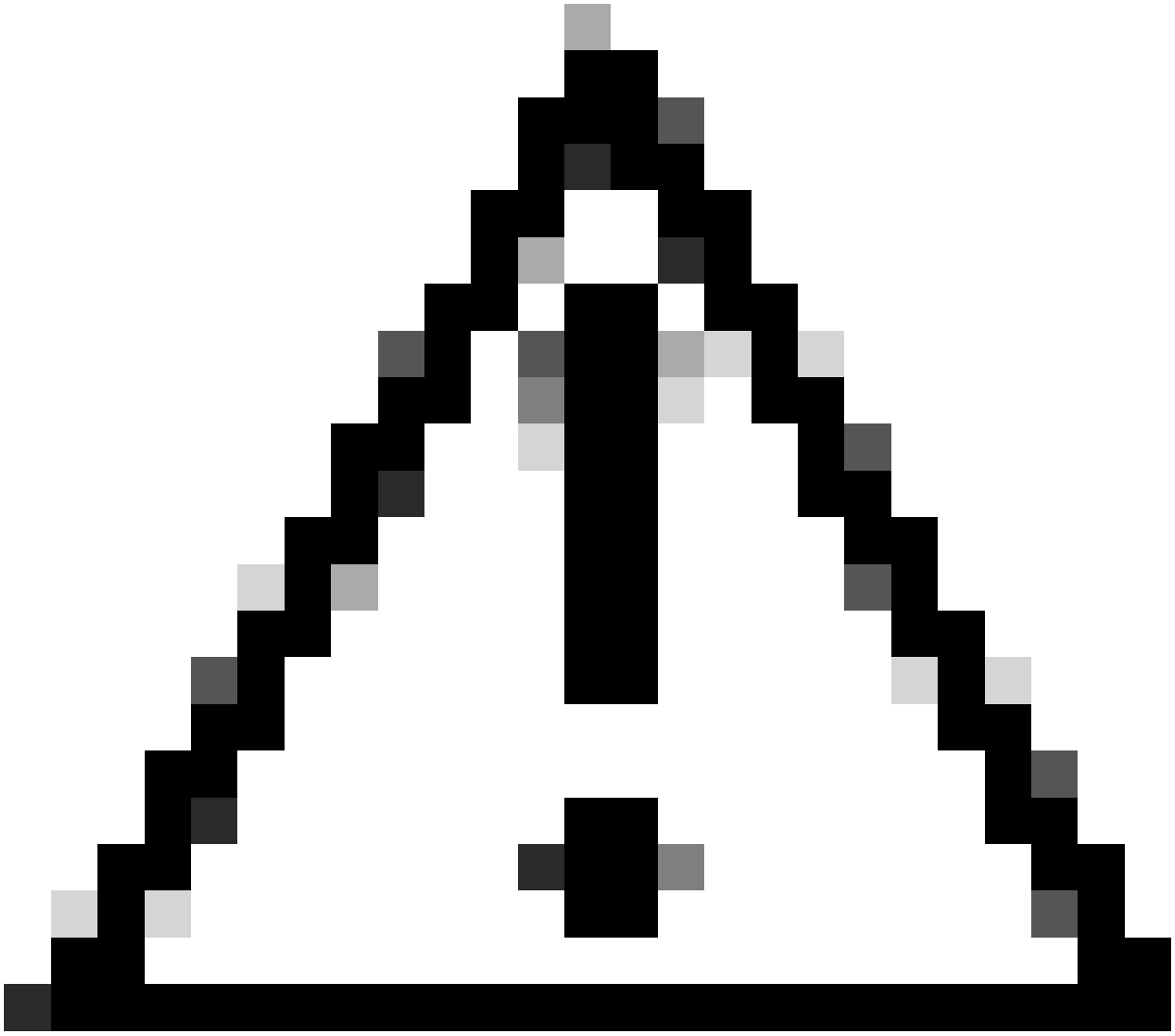


Habilite IPsec-IKEv2 em uma política de grupo na interface do usuário do FMC.

No Editor de perfis VPN ou no Editor de perfis ASA, navegue até a guia Lista de servidores. O nome do grupo de usuários DEVE corresponder exatamente ao nome do perfil de conexão no firewall. Neste exemplo, IKEV2 era o perfil de conexão / nome do grupo de usuários. O protocolo primário está configurado como IPsec. O 'Nome de exibição' no é exibido para o usuário na interface do usuário do Secure Client ao estabelecer uma conexão com este perfil de conexão.

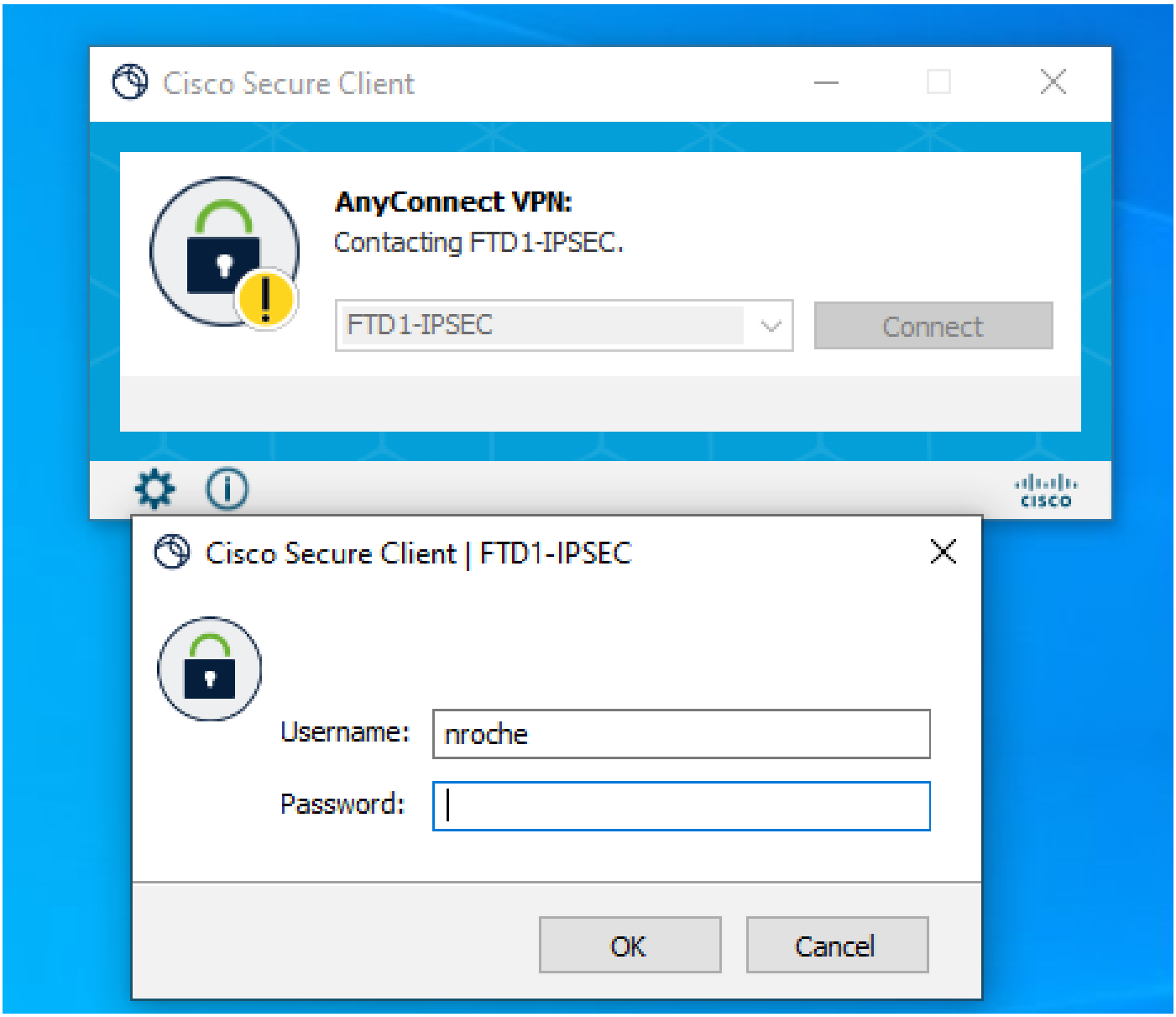


Edite o perfil XML para que o protocolo principal seja IPsec e o Grupo de usuários corresponda ao nome do perfil de conexão.



Cuidado: uma conexão SSL é necessária para enviar perfis XML do firewall para o cliente. Ao usar apenas IKEV2-IPsec, os perfis XML devem ser enviados aos clientes por meio de um método fora de banda.

Depois que o perfil XML é enviado ao cliente, o Secure Client usa o Grupo de Usuários do perfil XML para se conectar ao perfil de conexão IKEV2-IPsec.



Exibição da interface do usuário do cliente seguro da tentativa de conexão IPsec-IKEv2 RAVPN.

Exemplos de configuração do ASA

Desative a autenticação AAA nos perfis de conexão DefaultWEBVPNGroup e DefaultRAGroup

Insira a seção webvpn-attributes para grupo de túnel DefaultWEBVPNGroup e especifique a autenticação como baseada em certificado. Repita esse processo para o DefaultRAGroup. Os usuários que chegam a esses perfis de conexão padrão são forçados a apresentar um certificado para autenticação e não têm a oportunidade de inserir credenciais de nome de usuário e senha.

```
ASA# configure terminal
ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# authentication certificate

ASA# configure terminal
```

```
ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes
ASA(config-tunnel-webvpn)# authentication certificate
```

Desative a verificação de host/postura de firewall seguro em DefaultWEBVPNGroup e DefaultRAGroup (opcional)

Isso só é necessário se você tiver o Hostscan / Secure Firewall Posture em seu ambiente. Essa etapa impede que os invasores aumentem a utilização de recursos no firewall causada pelo processo de verificação de endpoint. Insira a seção webvpn-attributes para os perfis de conexão e DefaultWEBVPNGroup e DefaultRAGroup e implemente without-csd para desabilitar a funcionalidade de verificação de ponto de extremidade.

```
ASA# configure terminal
ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# without-csd

ASA# configure terminal
ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes
ASA(config-tunnel-webvpn)# without-csd
```

Desabilitar aliases de grupo e Habilitar URLs de grupo

Digite o grupo de túneis ao qual os usuários estão se conectando. Se houver um alias de grupo existente, desabilite-o ou remova-o. Neste exemplo, ele está desativado. Quando estiver concluído, crie um group-url usando o FQDN ou o endereço IP da interface de terminação RAVPN. O nome no final da url de grupo precisa ser obscuro. Evite valores comuns, como VPN, AAA, RADIUS e LDAP, pois eles facilitam para os invasores adivinharem a URL completa se obtiverem o FQDN. Em vez disso, use internamente nomes significativos que ajudem a identificar o grupo de túneis.

```
ASA# configure terminal
ASA(config)# tunnel-group NAME webvpn-attributes
ASA(config-tunnel-webvpn)# group-alias NAME disable
ASA(config-tunnel-webvpn)# group-url https://FQDN/name enable
```

Mapeamento de certificado

No modo de configuração global, crie um mapa de certificado e atribua a ele um nome e um número de sequência. Em seguida, defina uma regra que os usuários devem corresponder para utilizar o mapeamento. Neste exemplo, os usuários teriam que corresponder aos critérios de um valor de nome comum igual a "valor personalizado". Em seguida, insira a configuração de webvpn

e aplique o mapa de certificado ao grupo de túneis desejado. Depois de concluído, insira DefaultWEBVPNGroup e torne este grupo de túneis o padrão para usuários que falharem no mapeamento de certificado. Se os usuários falharem no mapeamento, eles serão direcionados para o DefaultWEBVPNGroup. Enquanto o DefaultWEBVPNGroup estiver configurado com autenticação de certificado, os usuários não terão a opção de passar credenciais de nome de usuário ou senha.

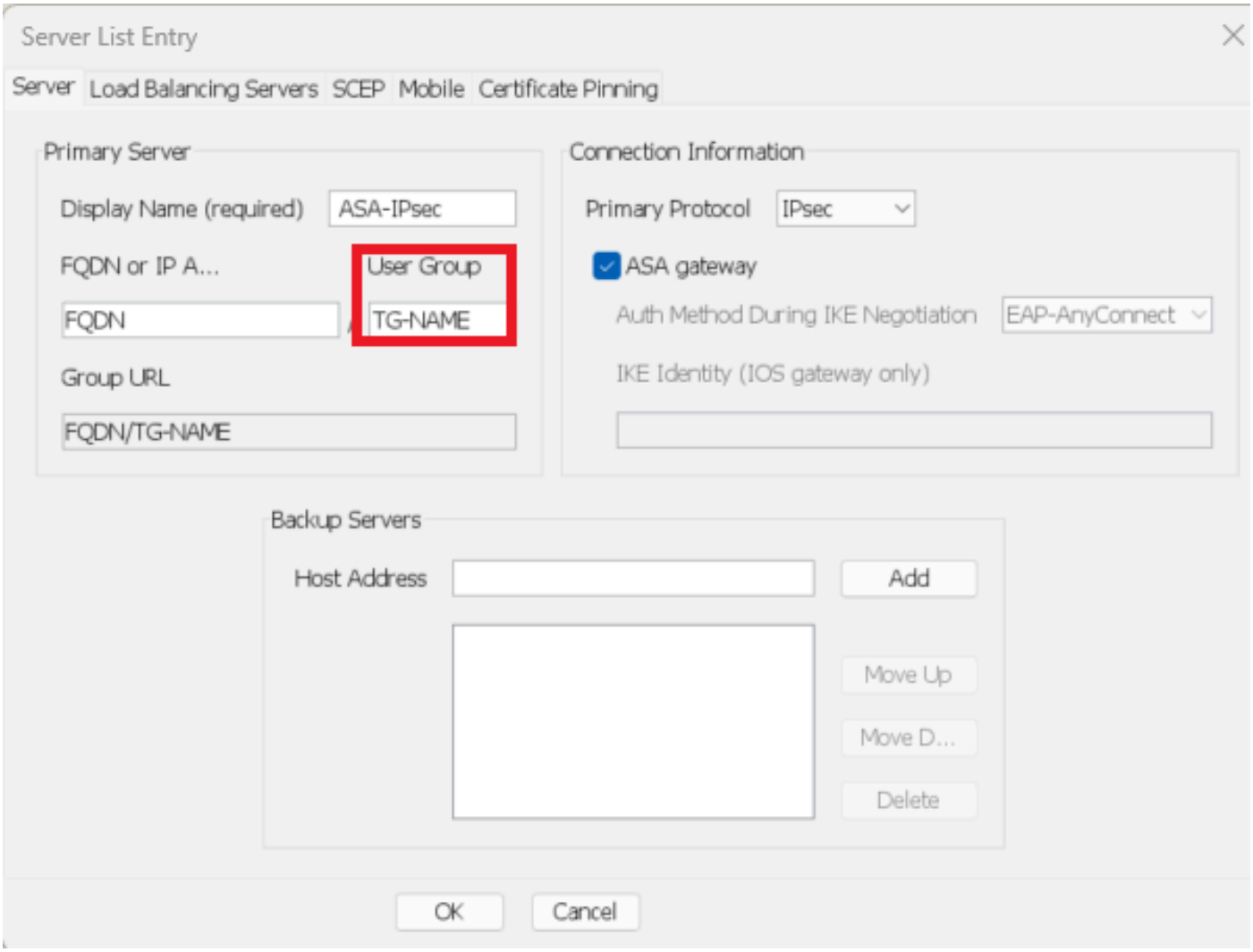
```
ASA(config)# crypto ca certificate map NAME 1
ASA(config-ca-cert-map)# subject-name attr cn eq customvalue

ASA(config)# webvpn
ASA(config-webvpn)# certificate-group-map NAME 1 TG-NAME

ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# tunnel-group-map default-group
```

IPsec-IKEv2

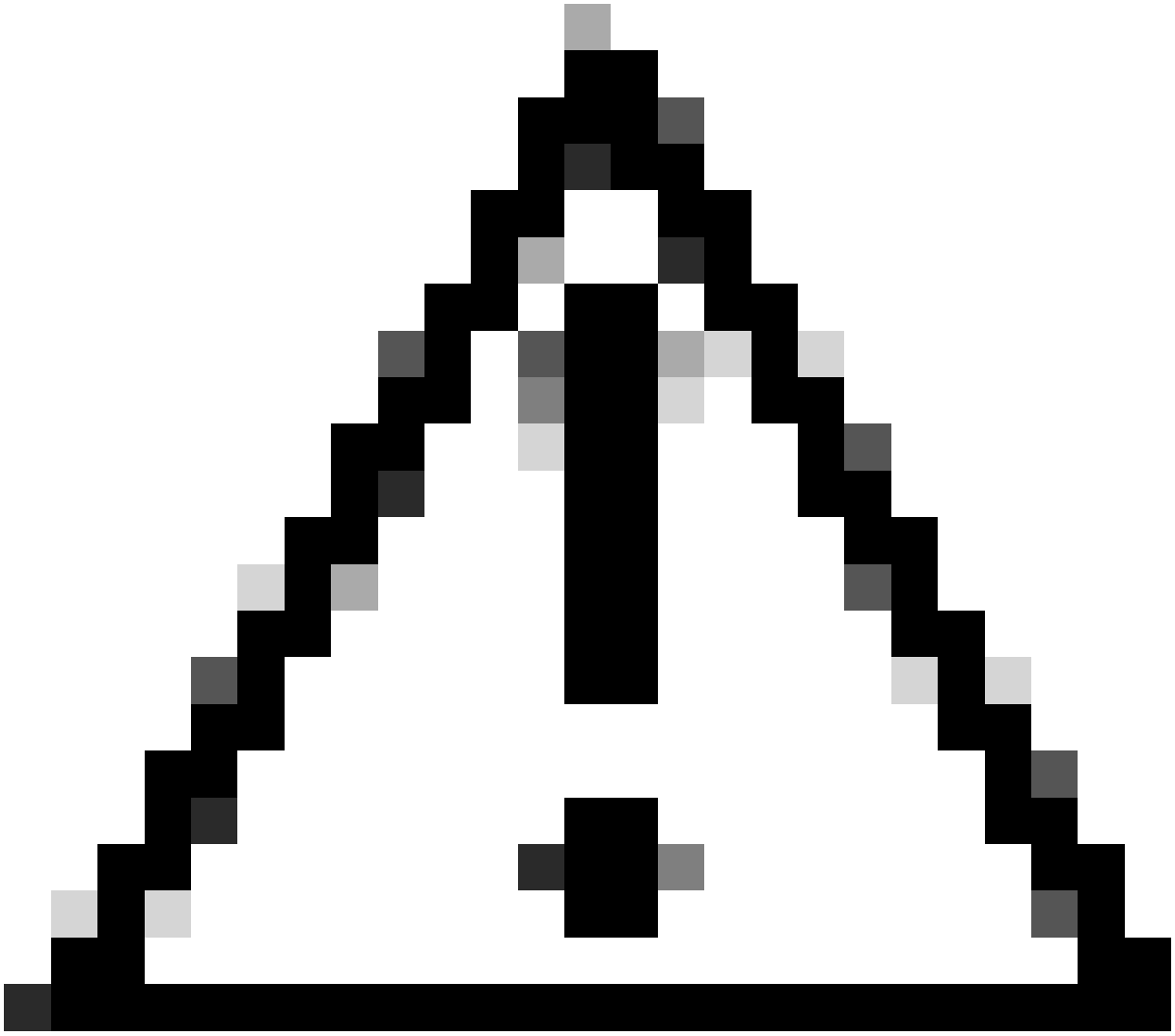
No modo de configuração global, você pode editar uma diretiva de grupo existente ou criar uma nova e inserir os atributos dessa diretiva de grupo. Quando estiver na seção de atributos, ative IKEv2 como o único protocolo de túnel VPN. Certifique-se de que essa política de grupo esteja vinculada a um grupo de túneis que será utilizado para conexões VPN de acesso remoto IPsec-IKEV2. Semelhante às etapas do FMC, você deve editar o perfil XML através do VPN Profile Editor ou do ASA Profile Editor e alterar o campo User Group para corresponder ao nome do grupo de túneis no ASA, e alterar o protocolo para IPsec.

```
ASA# configure terminal
ASA(config)# group-policy GP-NAME internal
ASA(config)# group-policy GP-NAME attributes
ASA(config-group-policy)# vpn-tunnel-protocol ikev2

ASA(config)# tunnel-group TG-NAME general-attributes
ASA(config-tunnel-general)# default-group-policy GP-NAME
```

No Editor de perfis VPN ou no Editor de perfis ASA, navegue até a guia Lista de servidores. O nome do grupo de usuários DEVE corresponder exatamente ao nome do perfil de conexão no firewall. O protocolo primário está configurado como IPsec. O nome de exibição é mostrado ao usuário na interface do usuário do Secure Client ao estabelecer uma conexão com este perfil de conexão.



Edite o perfil XML para que o nome do protocolo primário seja IPsec e o nome do Grupo de Usuários corresponda ao nome do grupo de túneis do ASA para conexões IPsec-IKEv2 RAVPN.



Cuidado: uma conexão SSL é necessária para enviar perfis XML do firewall para o cliente. Ao usar apenas IKEV2-IPsec, os perfis XML devem ser enviados aos clientes por meio de um método fora de banda.

Conclusão

Em resumo, a finalidade das práticas de proteção neste documento é mapear usuários legítimos para perfis de conexão personalizados, enquanto os invasores são forçados para o DefaultWEBVPNGroup e o DefaultRAGroup. Em uma configuração otimizada, os dois perfis de conexão padrão não têm nenhuma configuração de servidor AAA personalizada legítima. Além disso, a remoção de aliases de grupo impede que os invasores identifiquem facilmente perfis de conexão personalizados, removendo a visibilidade suspensa ao navegar para o FQDN ou o endereço IP público do firewall.

Informações Relacionadas

Suporte técnico e downloads da Cisco

Ataques de borrifo de senha

Vulnerabilidade de acesso não autorizado setembro de 2023

Guias de configuração do ASA

Guias de configuração do FMC/FDM

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.