Configurar Políticas de Controle de Acesso de Plano de Controle para Secure Firewall Threat Defense e ASA

Contents

Introdução

Este documento descreve o processo para configurar as regras de acesso ao plano de controle para Secure Firewall Threat Defense e Adaptive Security Appliance (ASA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Defesa contra ameaças de firewall (FTD) segura
- Gerenciador de Dispositivos de Firewall Seguro (FDM)
- Centro de gerenciamento seguro de firewall (FMC)
- ASA com firewall seguro
- Lista de controle de acesso (ACL)
- FlexConfig

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Secure Firewall Threat Defense versão 7.2.5
- Secure Firewall Manager Center versão 7.2.5
- Secure Firewall Device Manager versão 7.2.5
- Secure Firewall ASA versão 9.18.3

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

O tráfego geralmente atravessa um firewall e é roteado entre interfaces de dados; em algumas circunstâncias, é benéfico negar o tráfego destinado 'para' o firewall seguro. O firewall seguro da Cisco pode usar uma lista de controle de acesso (ACL) do plano de controle para restringir o tráfego "para a caixa". Um exemplo de quando uma ACL de plano de controle pode ser útil seria controlar quais pares podem estabelecer um túnel VPN (Site-to-Site ou VPN de Acesso Remoto) para o firewall seguro.

Tráfego "pronto para usar" do Secure Firewall

O tráfego normalmente atravessa firewalls de uma interface (de entrada) para outra interface (de saída), o que é conhecido como tráfego "através da caixa" e é gerenciado por ambas, as Políticas de Controle de Acesso (ACP) e as regras de Pré-filtro.

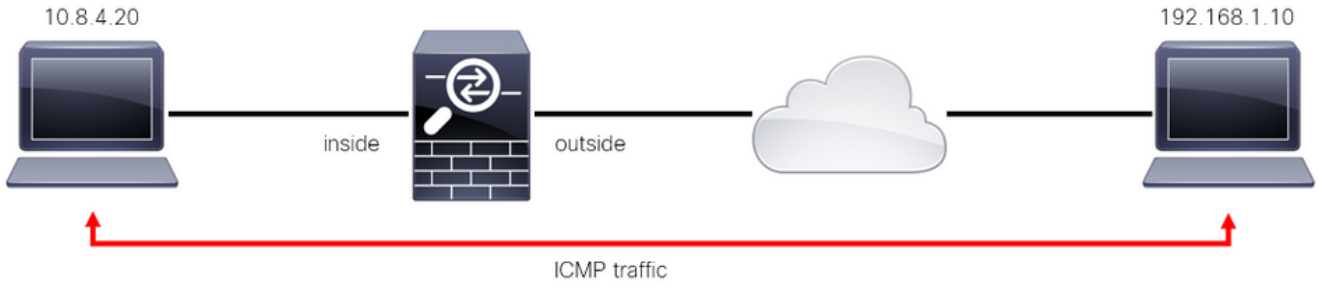

Imagem 1. Exemplo de tráfego por meio da caixa

Tráfego "pronto para usar" do firewall seguro

Há outros casos em que o tráfego é diretamente destinado a uma interface FTD (Site-to-Site ou Remote Access VPN), isso é conhecido como tráfego "to-the-box" e é gerenciado pelo plano de controle dessa interface específica.

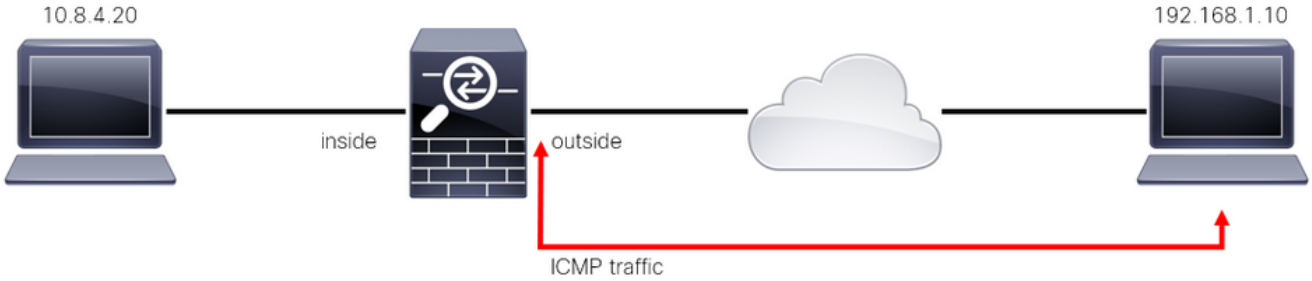

Imagem 2. Exemplo de tráfego pronto para usar

Considerações importantes sobre ACLs de plano de controle

- A partir do FMC/FTD versão 7.0, uma ACL de plano de controle deve ser configurada usando FlexConfig, usando a mesma sintaxe de comando usada no ASA.
- A palavra-chave control-plane é anexada à configuração do grupo de acesso, que aplicará o tráfego 'para' a interface de firewall segura. Sem a palavra de plano de controle anexada ao comando, a ACL restringiria o tráfego "através" do firewall seguro.
- Uma ACL de plano de controle não restringirá a entrada SSH, ICMP ou TELNET a uma interface de firewall segura. Eles são processados (permitidos/negados) de acordo com as políticas de configurações de plataforma e têm uma precedência mais alta.
- Uma ACL de plano de controle restringe o tráfego 'para' o próprio firewall seguro, enquanto a Política de controle de acesso para o FTD ou as ACLs normais para o ASA, controla o tráfego 'através' do firewall seguro.
- Diferentemente de uma ACL normal, não há um 'deny' implícito no final da ACL.
- No momento em que este documento está sendo criado, o recurso Geolocalização do FTD não pode ser usado para restringir o acesso 'ao' FTD.

Configurar

No próximo exemplo, um conjunto de endereços IP de um determinado país tenta forçar a VPN na rede tentando fazer login no FTD RAVPN. A melhor opção para proteger o FTD contra esses ataques de força bruta de VPN é configurar uma ACL de plano de controle para bloquear essas conexões à interface externa do FTD.

Configurações

Configurar uma ACL de plano de controle para o FTD gerenciado pelo FMC

Este é o procedimento que você precisa seguir em um FMC para configurar uma ACL de plano de controle para bloquear ataques de força bruta de VPN de entrada para a interface FTD externa:

Etapa 1. Abra a interface gráfica do usuário (GUI) do FMC via HTTPS e faça login com suas

credenciais.

Imagem 3. Página de início de sessão do FMC

Etapa 2. Você precisa criar uma ACL estendida. Para isso, navegue até Objetos > Gerenciamento de objetos.

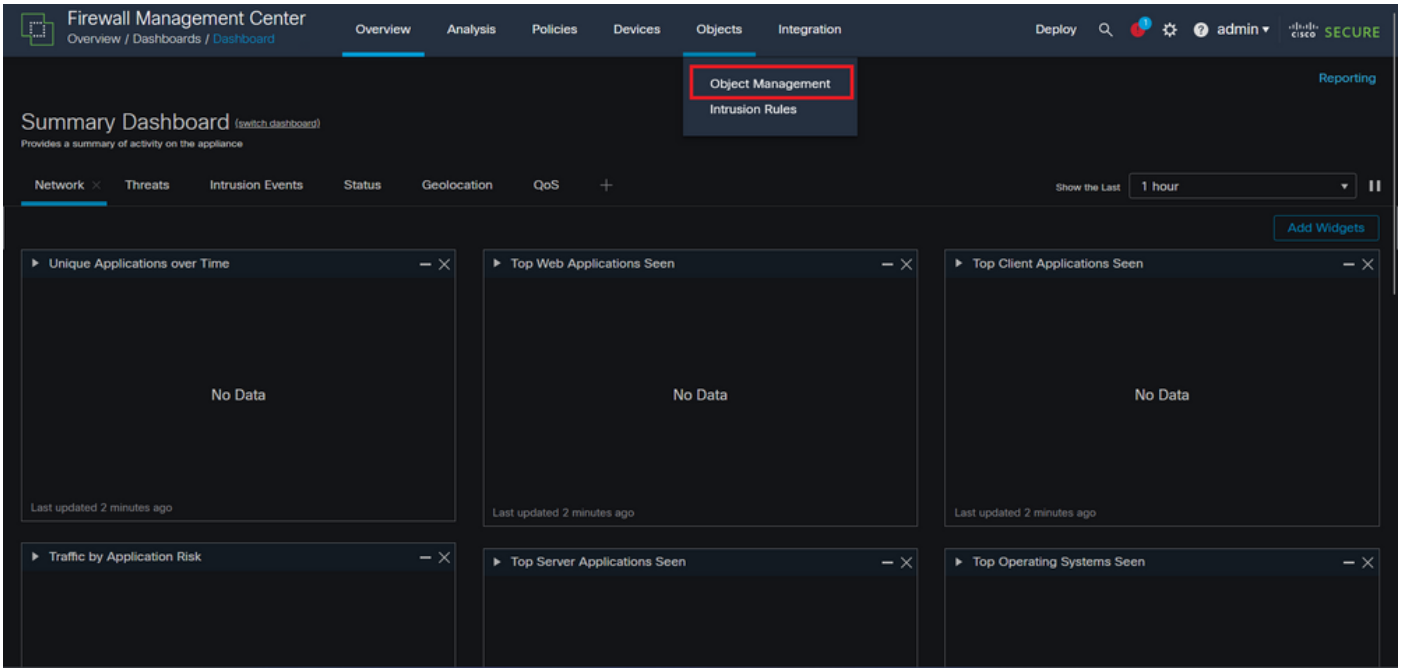

Imagem 4. Gerenciamento de objetos

Etapa 2.1. No painel esquerdo, navegue até Lista de acesso > Estendida para criar uma ACL estendida.

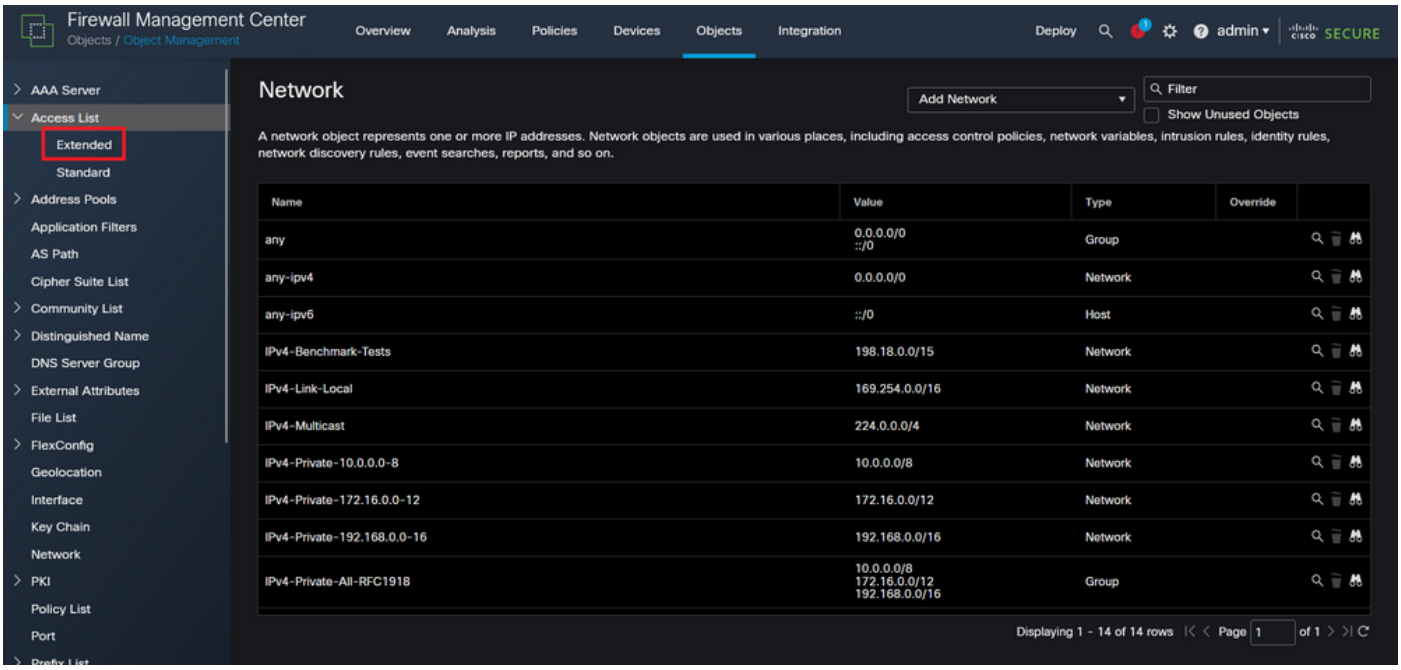

Imagem 5. Menu da ACL estendida

Etapa 2.2. Em seguida, selecione Adicionar lista de acesso estendida.

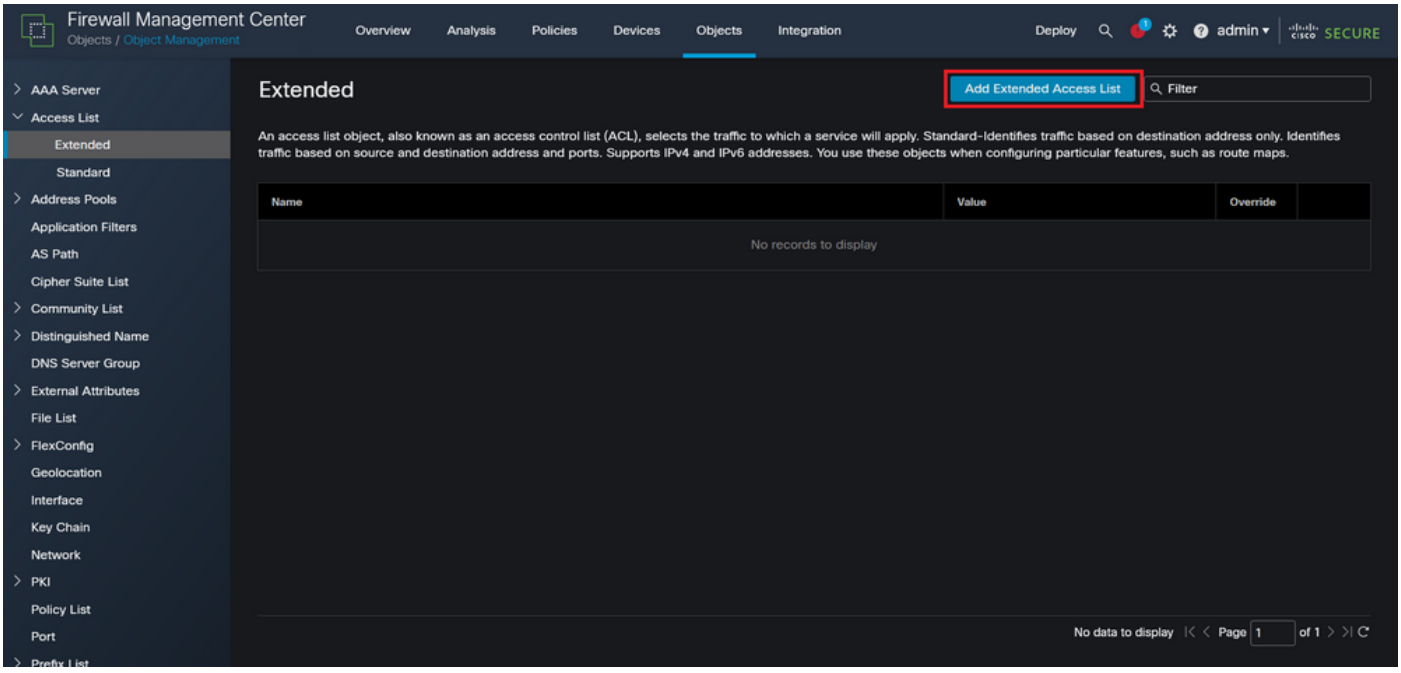

Imagem 6. Adicionar ACL estendida

Etapa 2.3. Digite um nome para a ACL estendida e clique no botão Adicionar para criar uma entrada de controle de acesso (ACE):

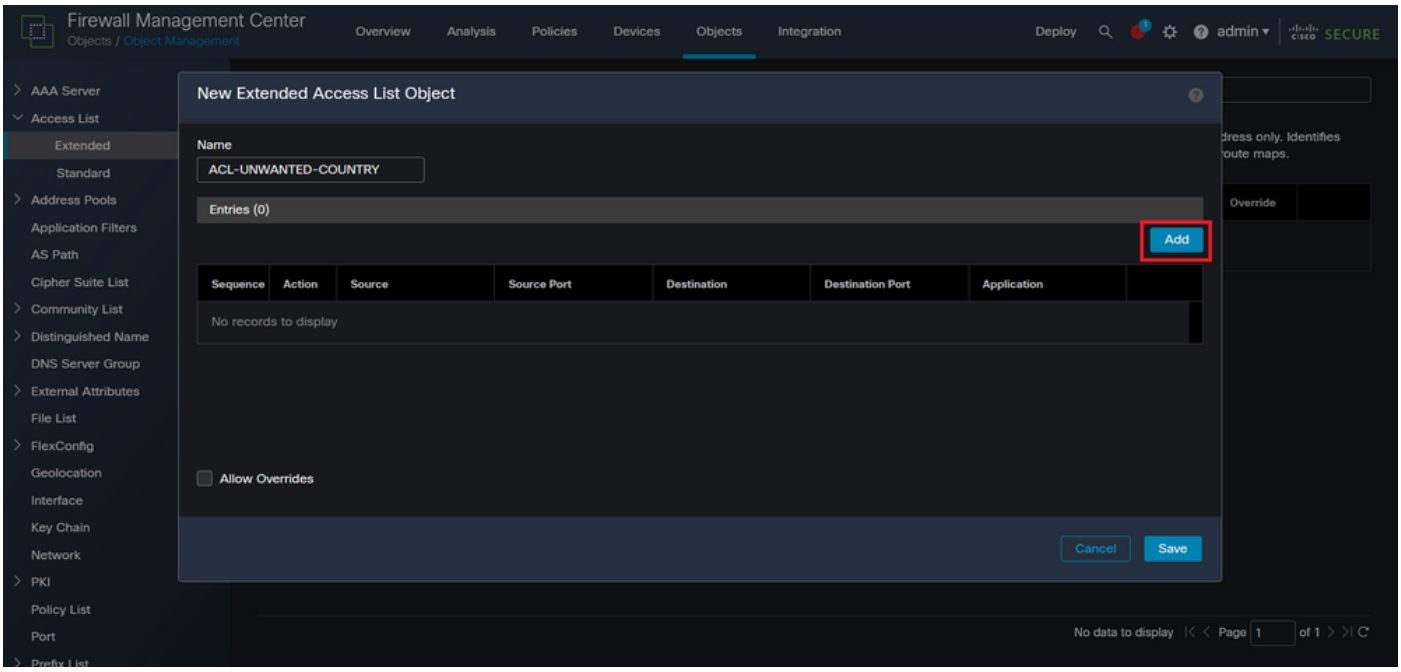

Imagem 7. Entradas de ACL estendida

Etapa 2.4. Altere a ação ACE para Block (Bloquear), adicione a rede de origem para corresponder ao tráfego que precisa ser negado para o FTD, mantenha a rede de destino como Any (Qualquer) e clique no botão Add (Adicionar) para concluir a entrada ACE:

- Neste exemplo, a entrada ACE configurada bloqueará ataques de força bruta de VPN provenientes da sub-rede 192.168.1.0/24.

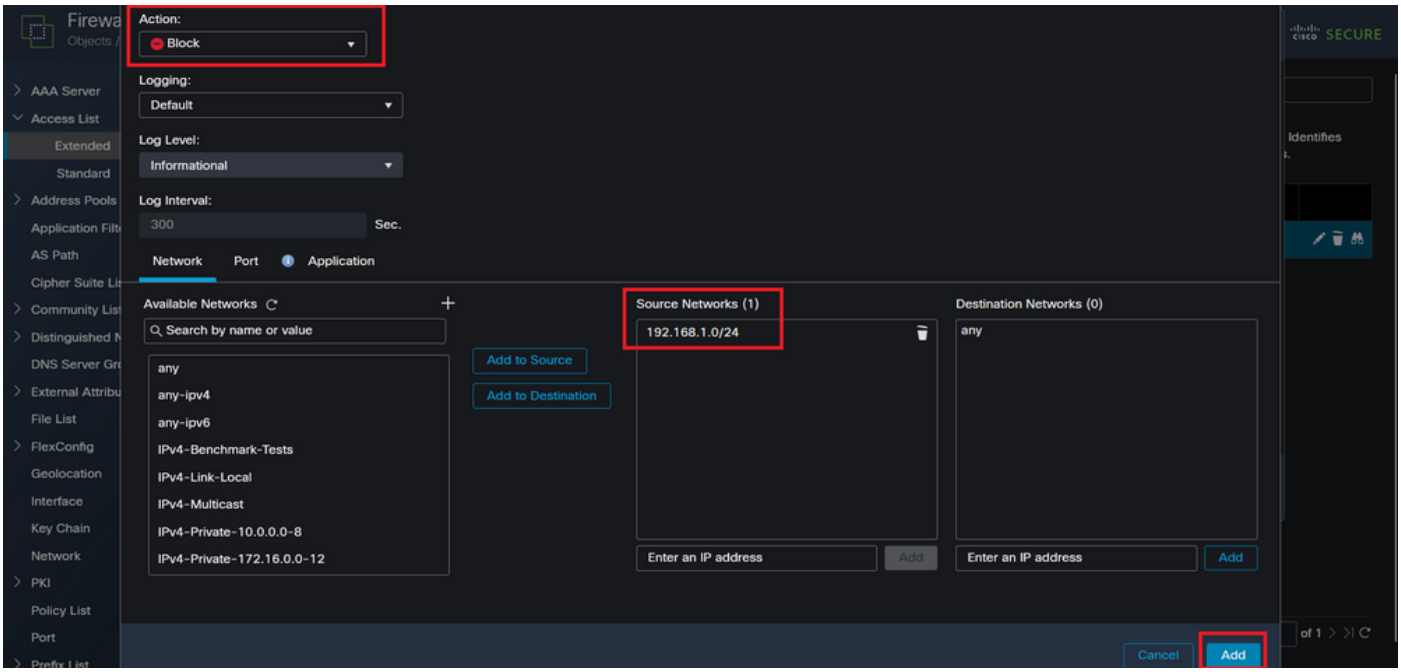

Imagem 8. Redes negadas

Etapa 2.5. Caso precise adicionar mais entradas ACE, clique no botão Add novamente e repita a etapa 2.4. Depois disso, clique no botão Save (Salvar) para concluir a configuração da ACL.

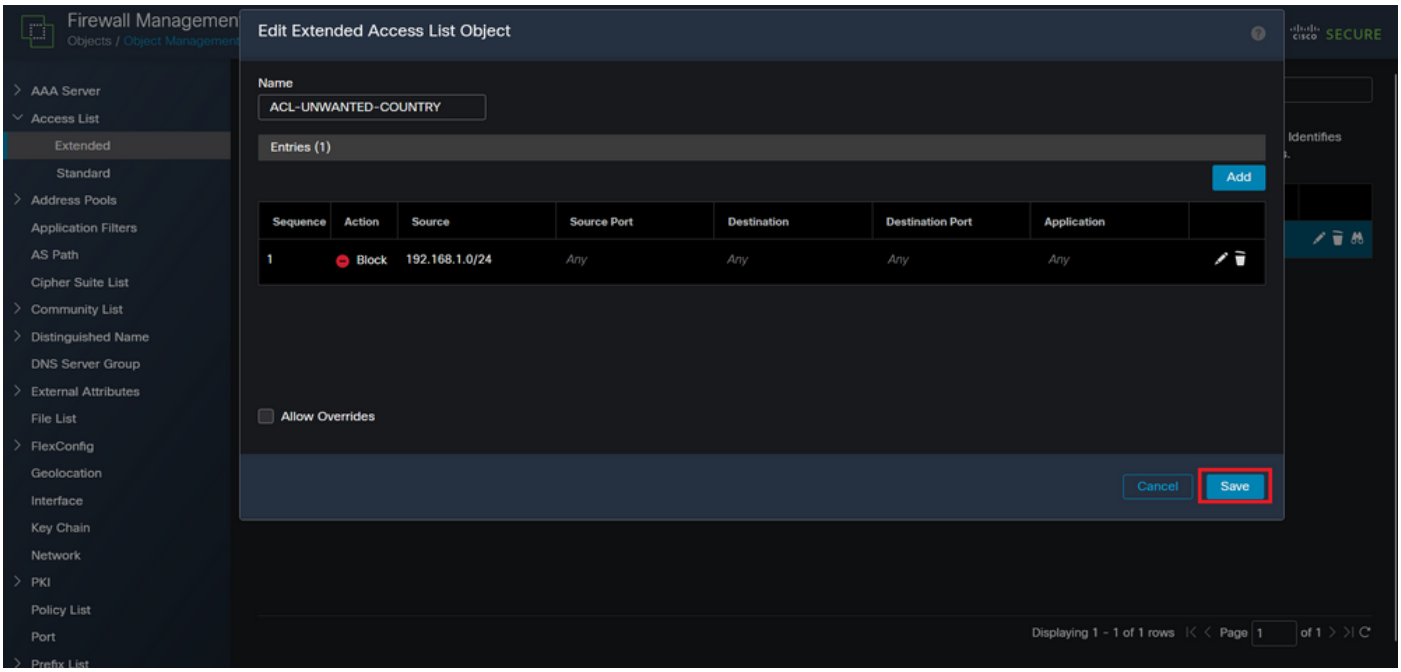

Imagem 9. Entradas de ACL estendida concluídas

Etapa 3. Em seguida, você precisa configurar um Objeto de configuração flexível para aplicar a ACL do plano de controle à interface FTD externa. Para isso, navegue até o painel esquerdo e selecione a opção FlexConfig > Objeto FlexConfig.

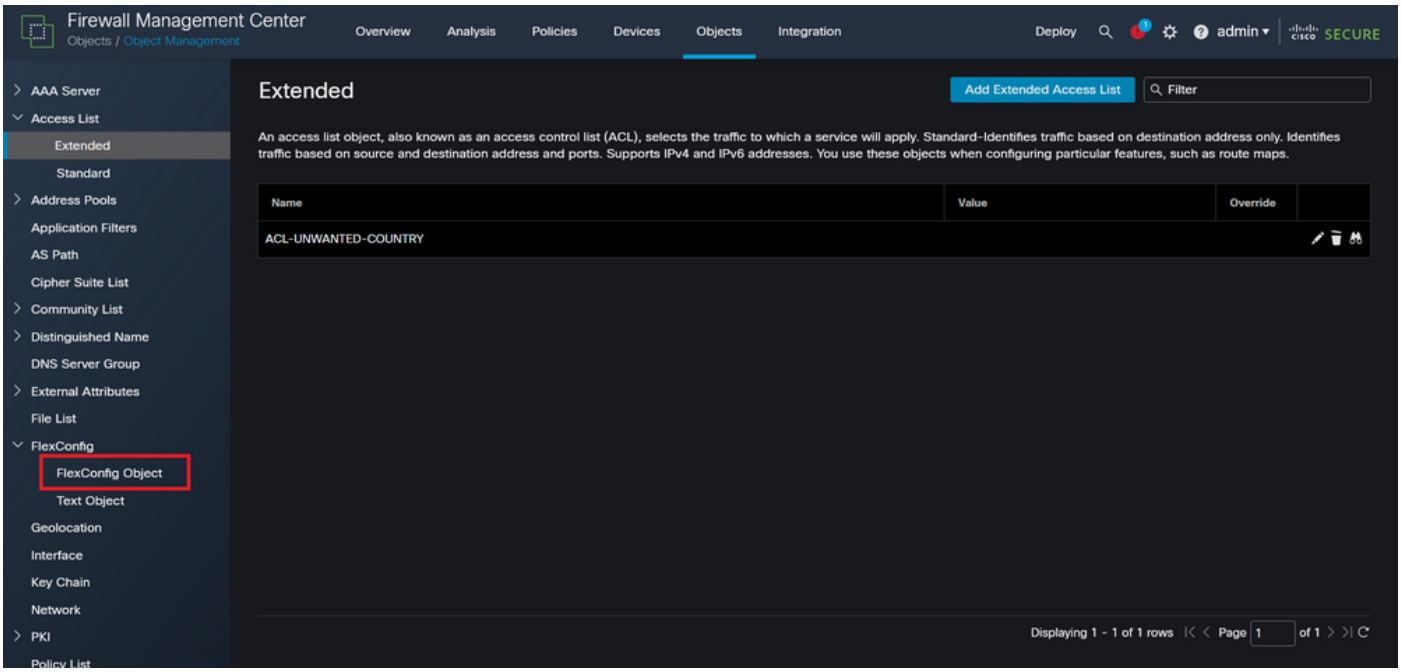

Imagem 10. Menu Objeto FlexConfig

Etapa 3.1. Clique em Adicionar objeto FlexConfig.

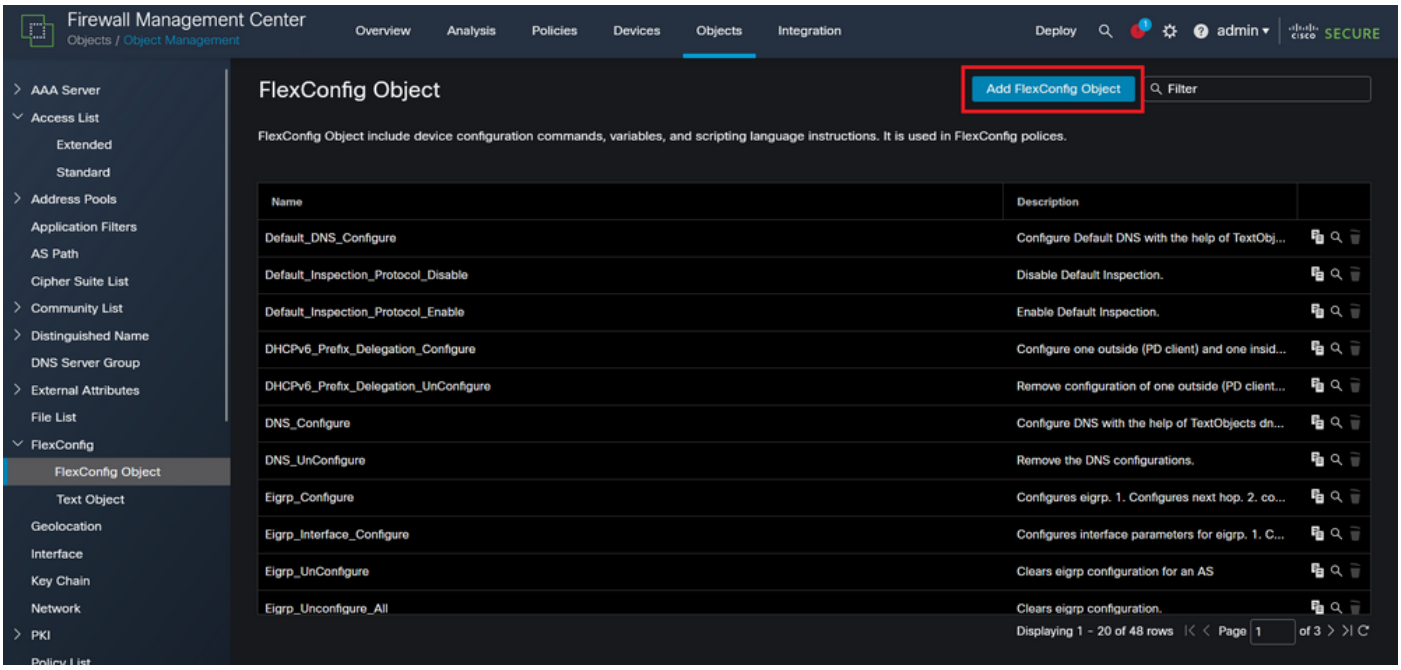

Imagem 11. Adicionar Objeto Flexconfig

Etapa 3.2. Adicione um nome para o objeto FlexConfig e insira um objeto de política de ACL. Para isso, selecione Inserir > Inserir objeto de política > Objeto de ACL estendida.

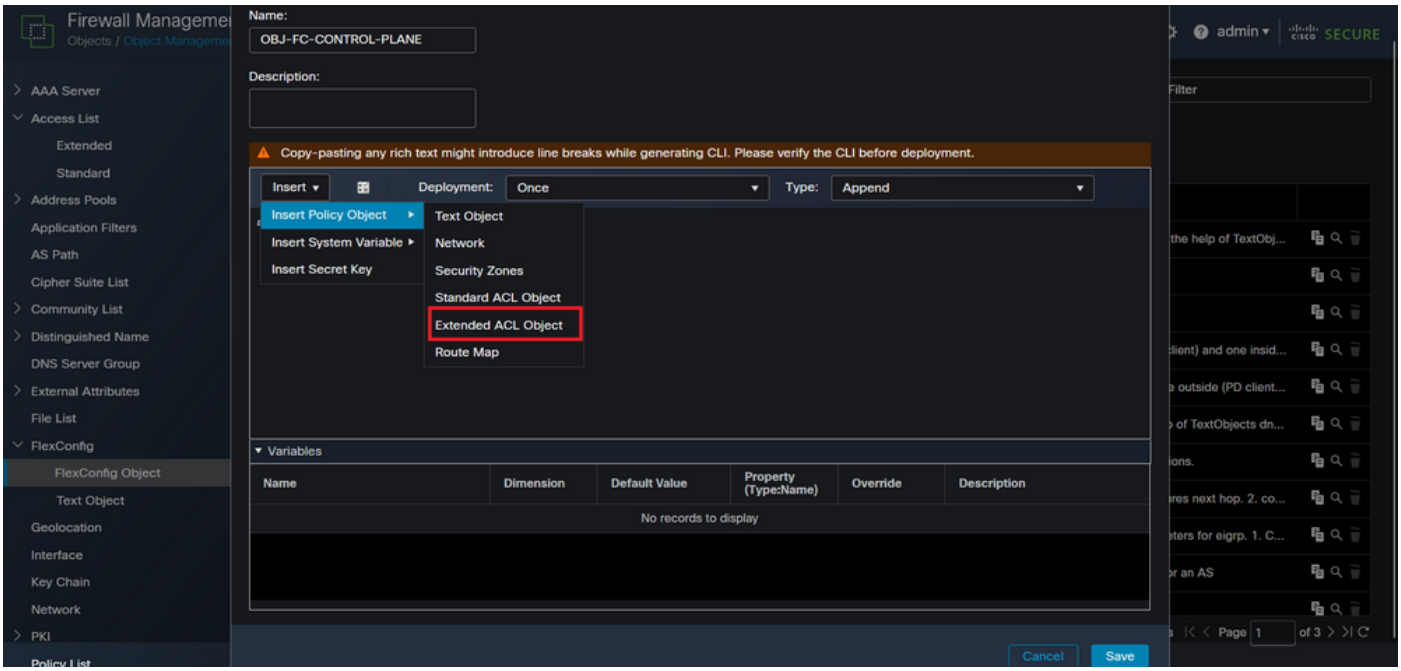

Imagem 12. Variável de objeto FlexConfig

Etapa 3.3. Adicione um nome para a variável de objeto ACL e, em seguida, selecione a ACL estendida que foi criada na Etapa 2.3, depois disso, clique no botão Salvar.

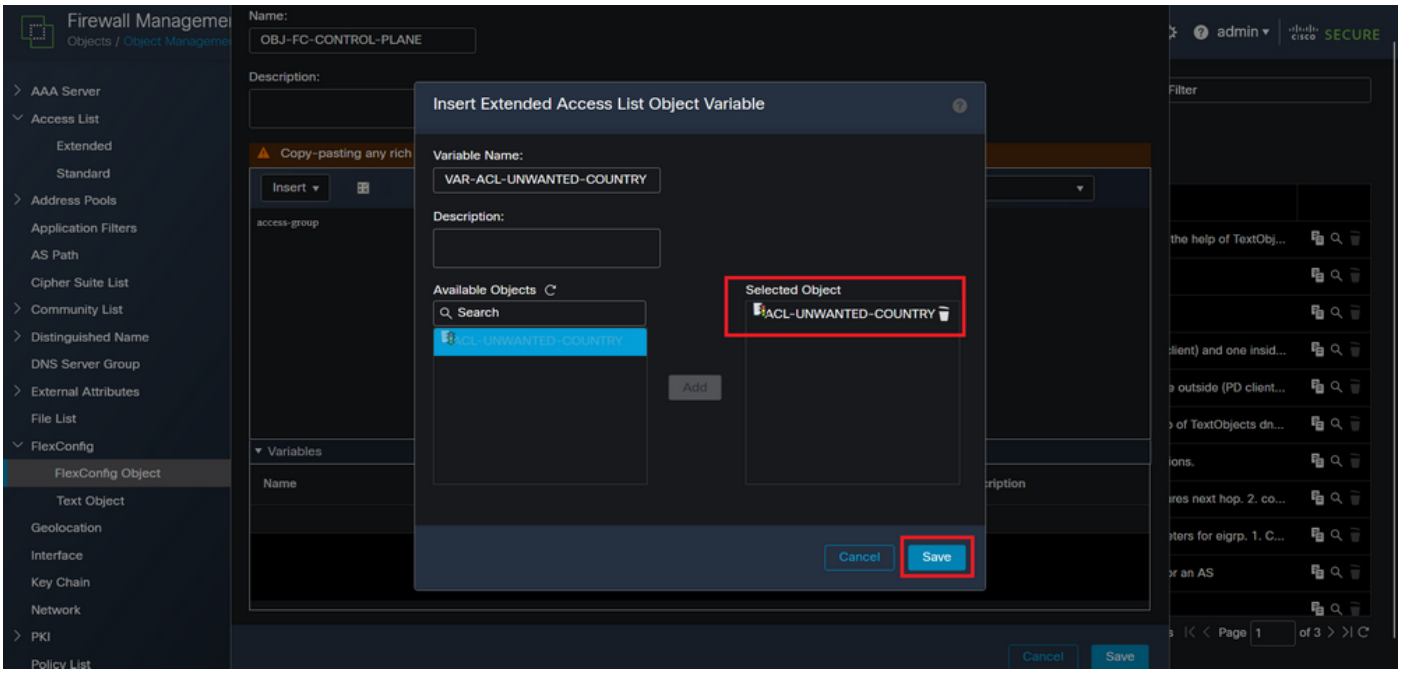

Imagem 13. Atribuição de ACL variável de objeto FlexConfig

Etapa 3.4. Em seguida, configure a ACL do plano de controle como entrada para a interface externa da seguinte maneira.

Sintaxe da linha de comando:

```
access-group "variable name starting with $ symbol" in interface "interface-name" control-plane
```

Isso se traduz no próximo exemplo de comando, que usa a variável ACL criada na Etapa 2.3 acima 'VAR-ACL-UNWANTED-COUNTRY' da seguinte maneira:

```
access-group $VAR-ACL-UNWANTED-COUNTRY in interface outside control-plane
```

É assim que ele deve ser configurado na janela do objeto FlexConfig. Depois disso, selecione o botão Salvar para concluir o objeto FlexConfig.

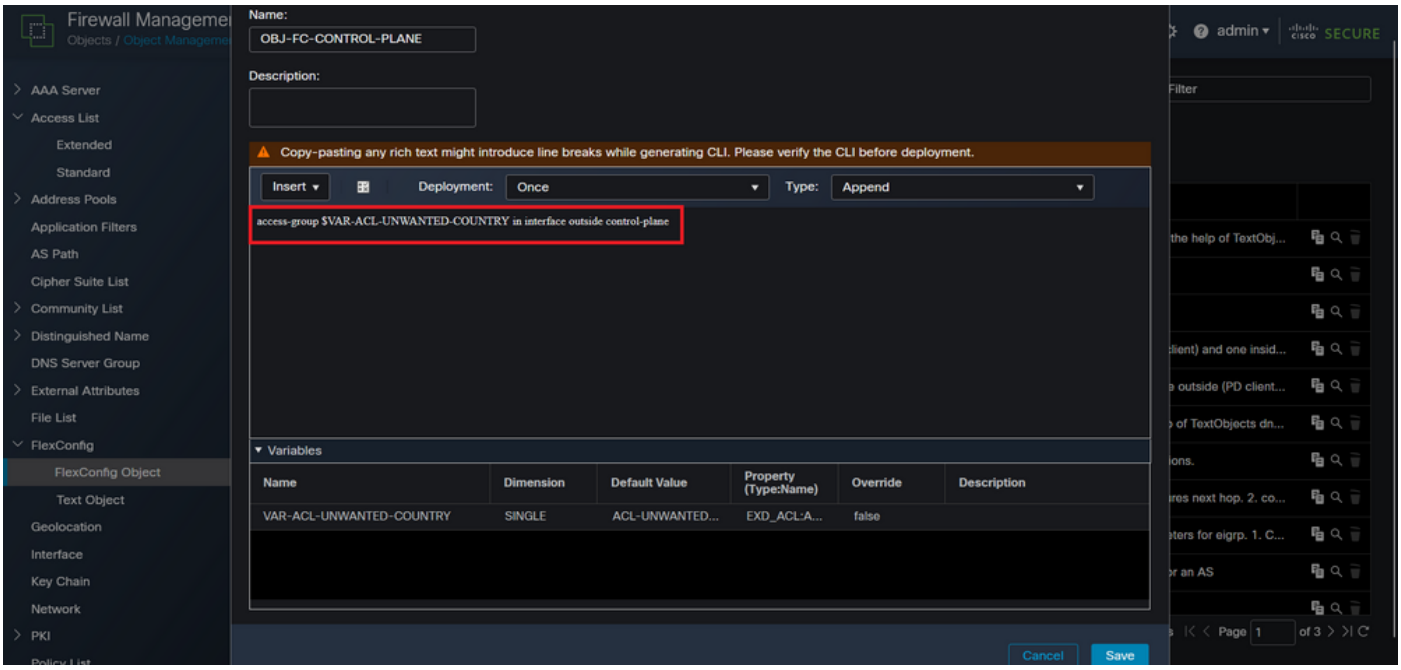

Imagem 14. Linha de comando completa do Objeto Flexconfig

Etapa 4. Você precisa aplicar a configuração do Objeto FlexConfig ao FTD; para isso, vá para Dispositivos > FlexConfig.

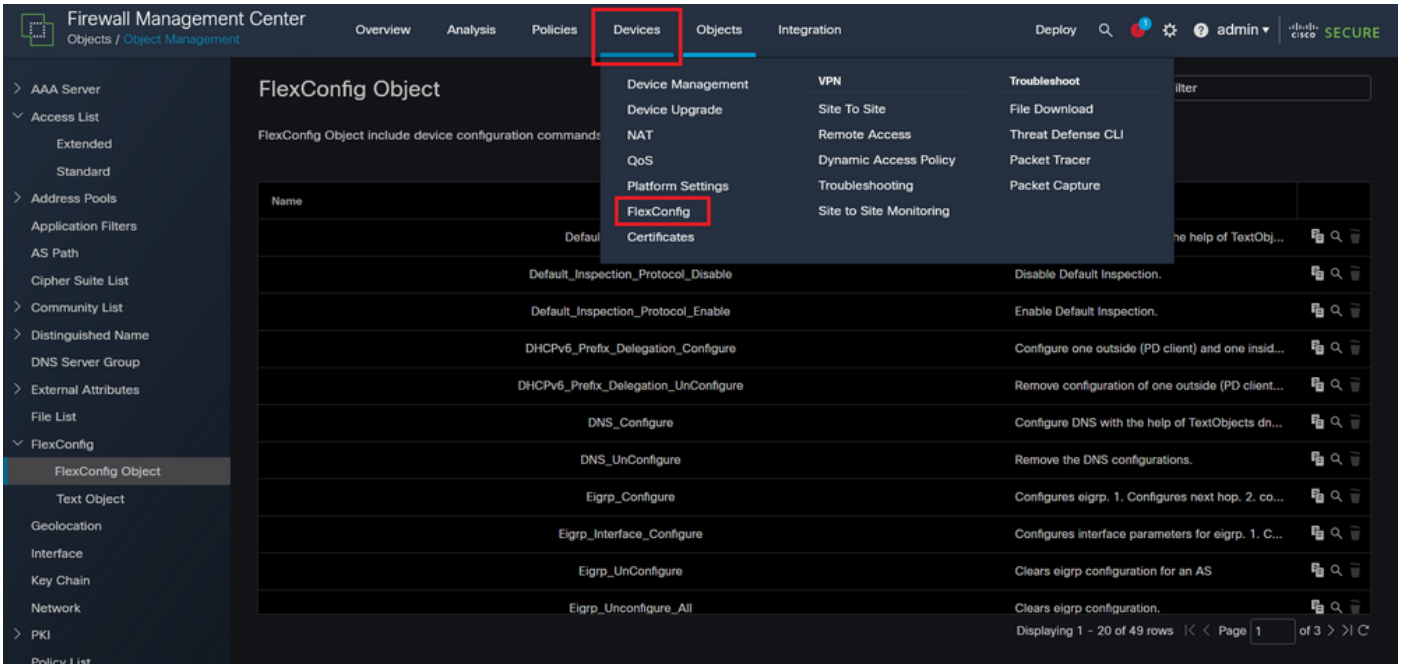

Imagem 15. Menu Política do FlexConfig

Etapa 4.1. Em seguida, clique em Nova política se ainda não houver um FlexConfig criado para o FTD ou edite a política FlexConfig existente.

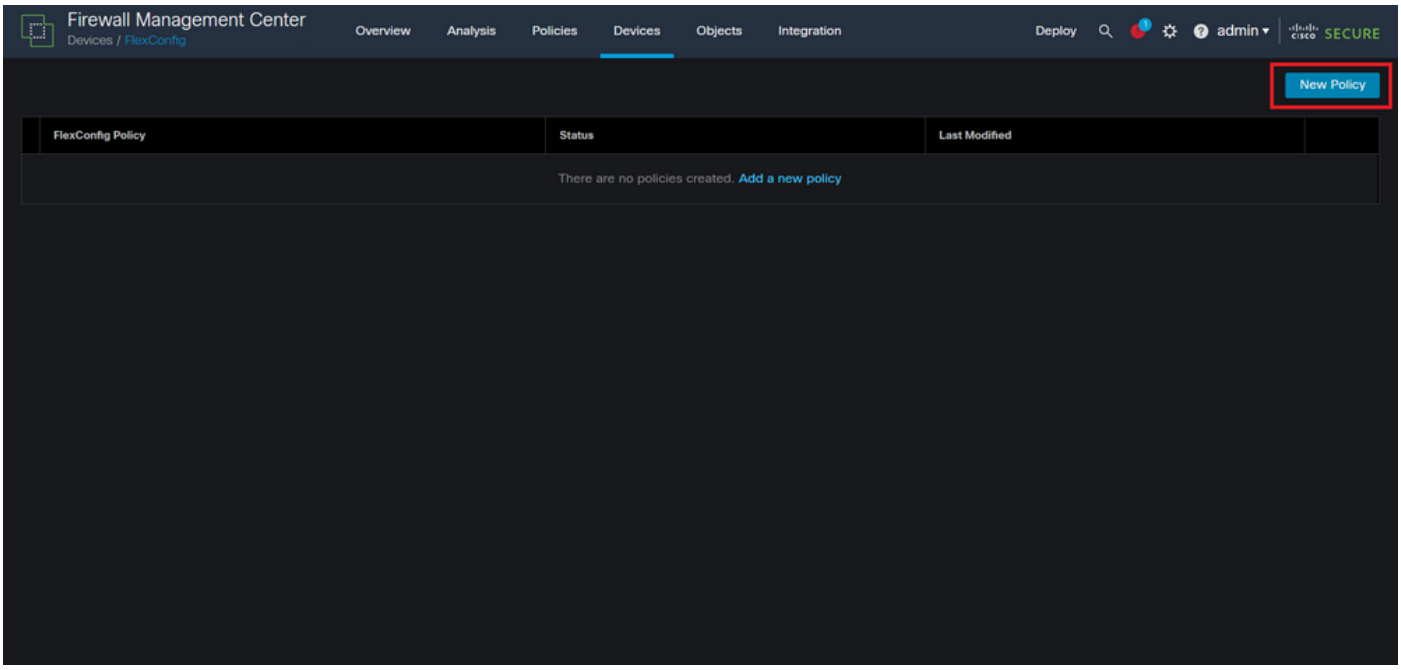

Imagem 16. Criação de política FlexConfig

Etapa 4.2. Adicione um nome para a nova política FlexConfig e selecione o FTD ao qual deseja aplicar a ACL de plano de controle criada.

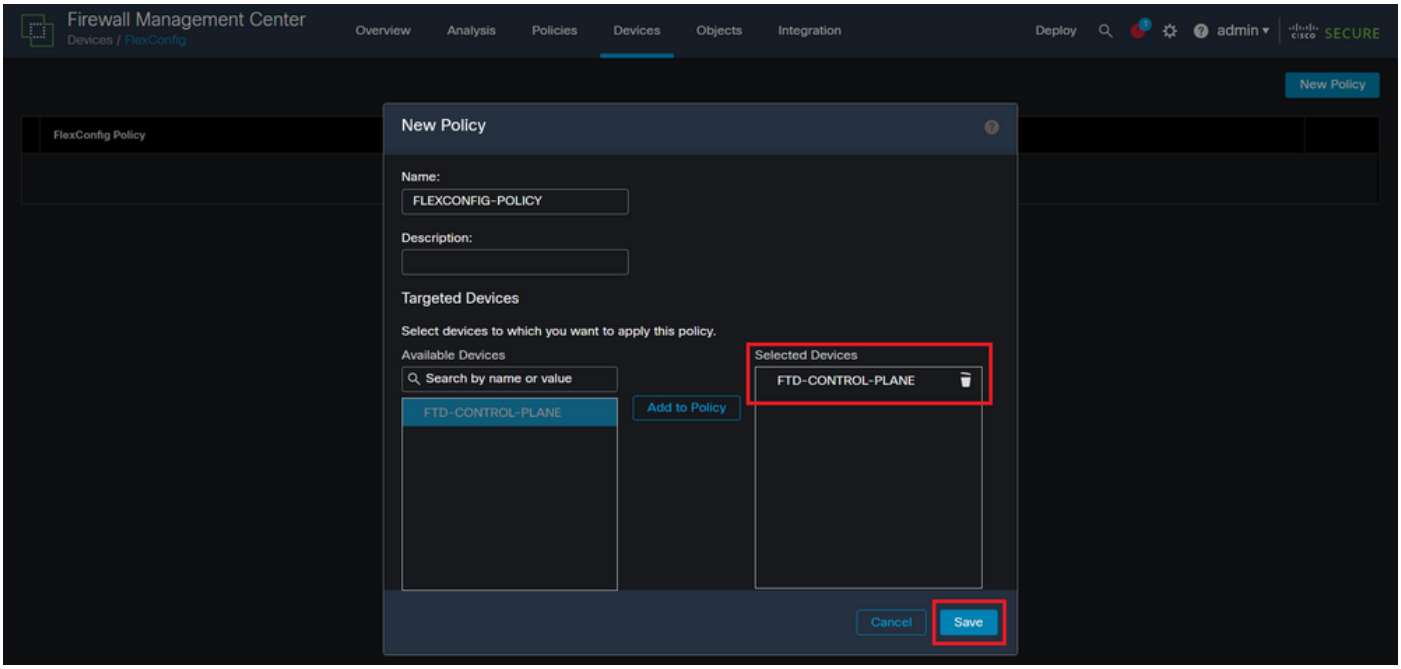

Imagem 17. Atribuição de dispositivo de Política FlexConfig

Etapa 4.3. No painel esquerdo, procure o objeto FlexConfig criado na etapa 3.2 acima e, em seguida, adicione-o à política FlexConfig clicando na seta para a direita localizada no meio da janela. Depois disso, clique no botão Salvar.

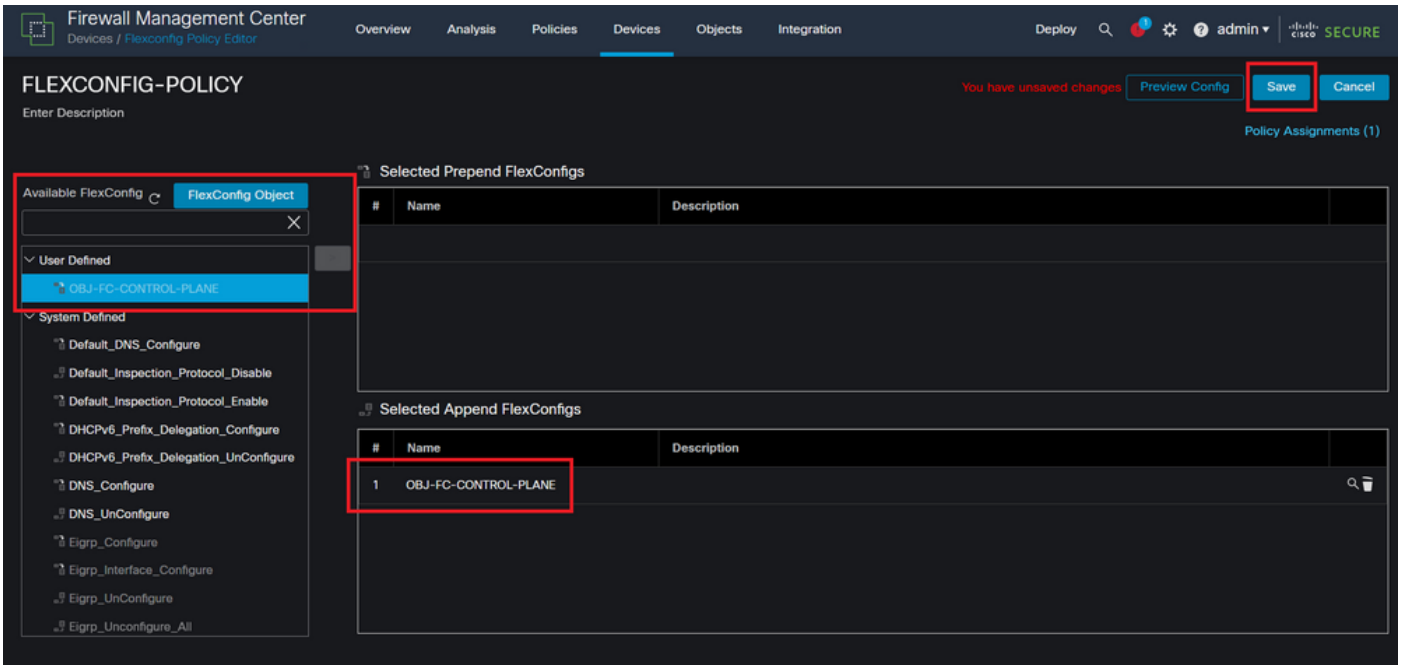

Imagem 18. Atribuição de objeto de Política FlexConfig

Etapa 5. Continue a implantar a alteração de configuração no FTD, para isso, navegue até Implantar > Implantação avançada.

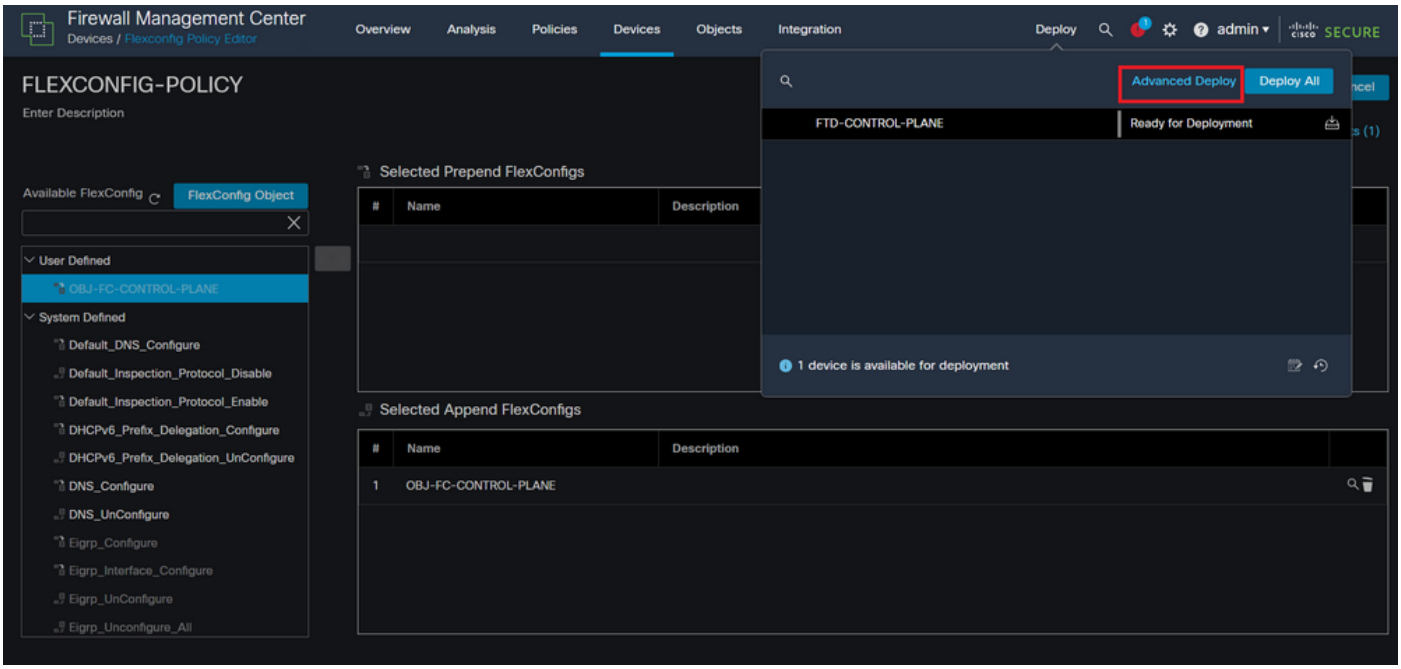

Imagem 19. Implantação Avançada de FTD

Etapa 5.1. Em seguida, selecione o FTD ao qual deseja aplicar a política FlexConfig. Se tudo estiver correto, clique em Implantar.

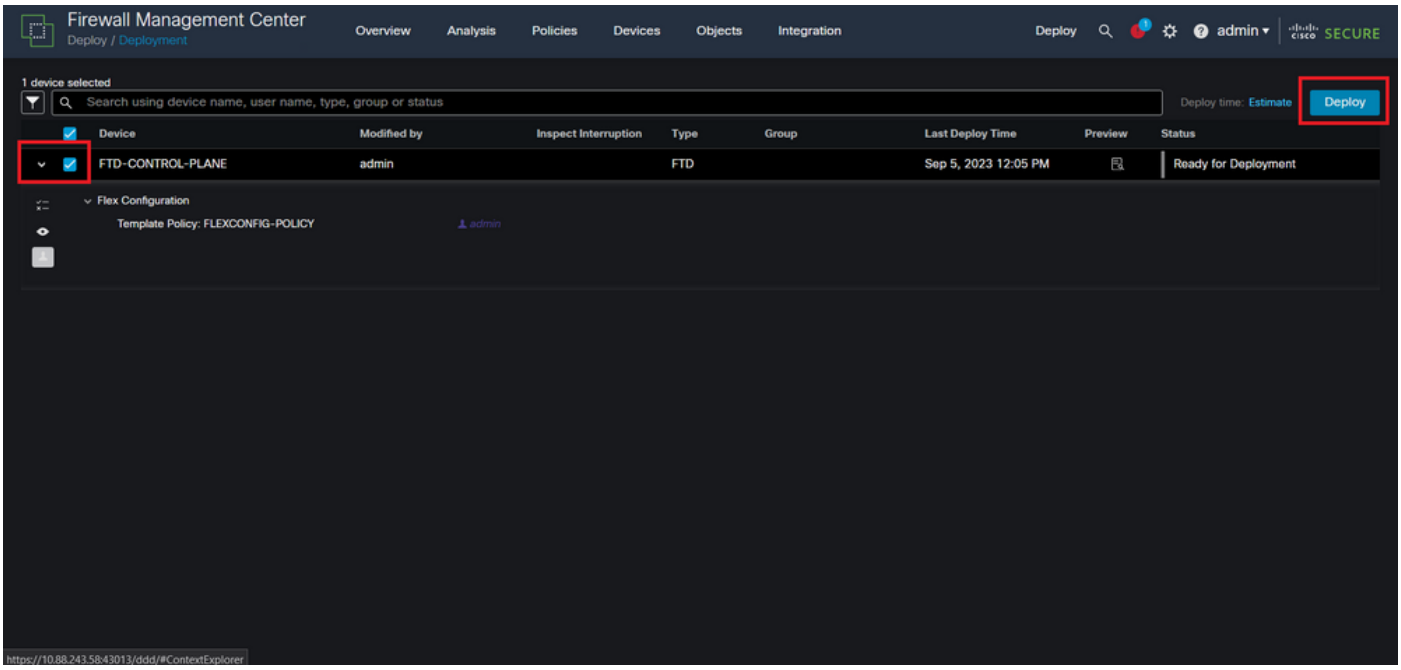

Imagem 20. Validação da implantação do FTD

Etapa 5.2. Depois disso, uma janela de confirmação da implantação será exibida, adicionará um comentário para rastrear a implantação e continuará a implantação.

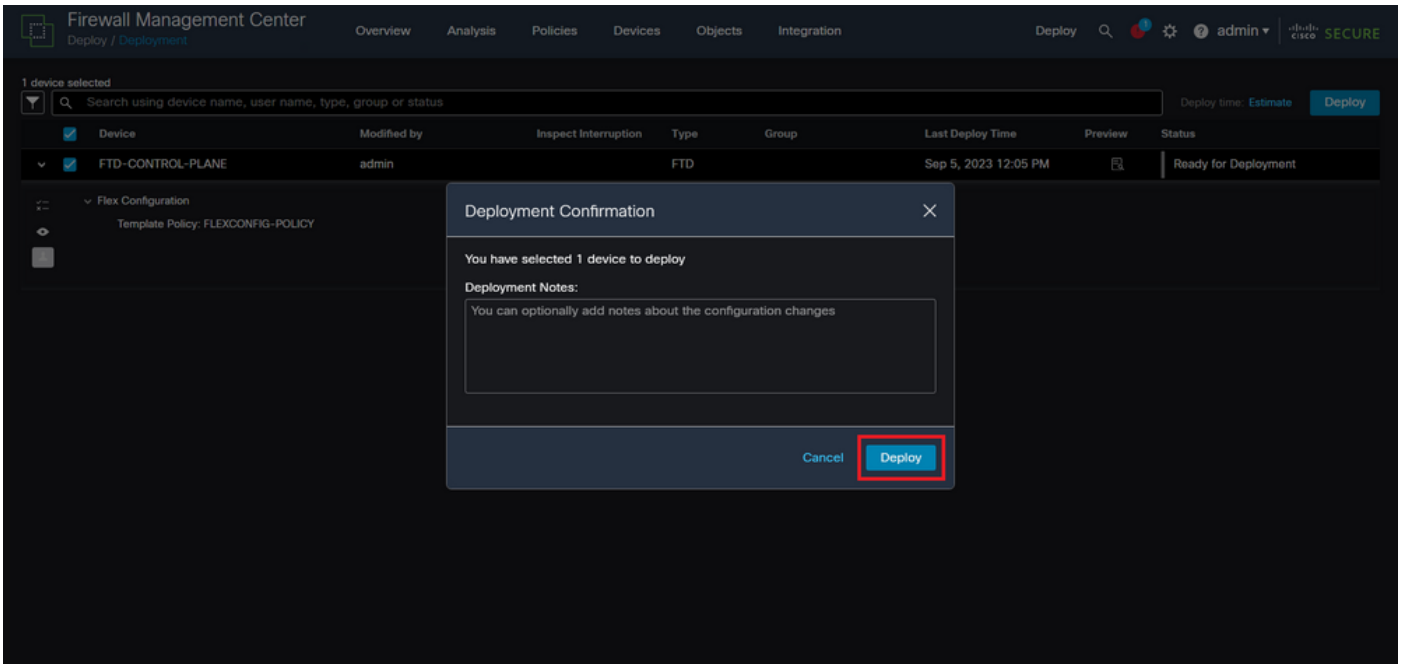

Imagem 21. Comentários de implantação do FTD

Etapa 5.3. Uma mensagem de aviso pode ser exibida durante a implantação de alterações de FlexConfig. Clique em Implantar somente se tiver certeza completa de que a configuração de política está correta.

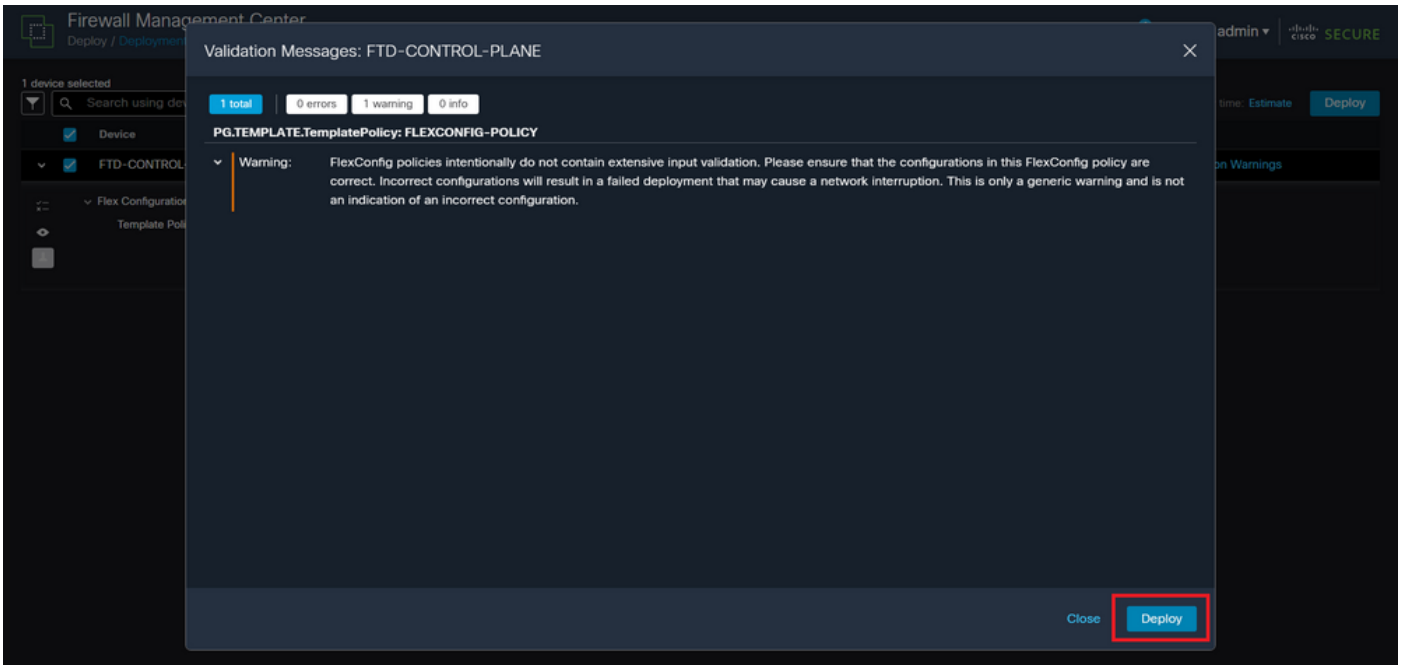

Imagem 22. Aviso do Flexconfig de Implantação do FTD

Etapa 5.4. Confirme se a implantação da política foi bem-sucedida para o FTD.

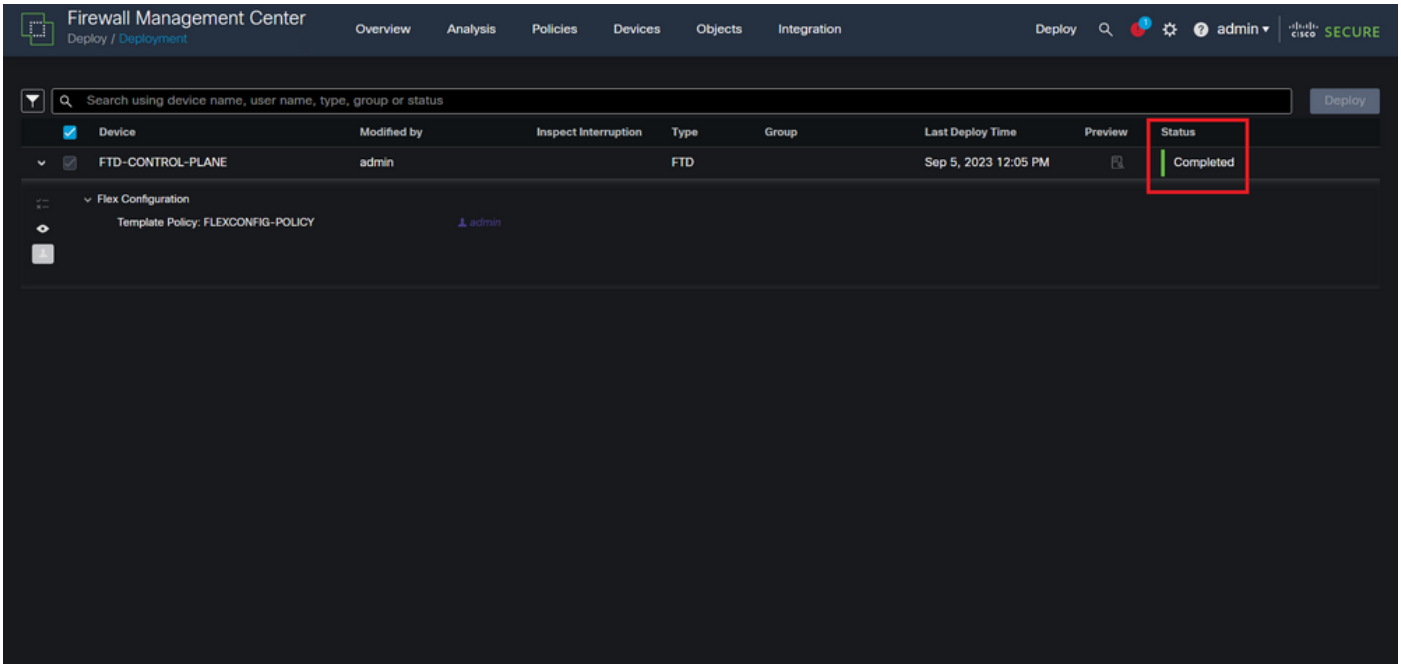

Imagem 23. Implantação do FTD bem-sucedida

Etapa 6. Se você criar uma nova ACL de plano de controle para o FTD ou se editou uma ACL existente que esteja ativamente em uso, é importante destacar que as alterações de configuração feitas não se aplicam a conexões já estabelecidas com o FTD, portanto, você precisa limpar manualmente as tentativas de conexão ativas ao FTD. Para isso, conecte-se ao CLI do FTD e limpe as conexões ativas da seguinte maneira.

Para limpar a conexão ativa para um endereço IP de host específico:

```
> clear conn address 192.168.1.10 all
```

Para limpar as conexões ativas de toda uma rede de sub-rede:

```
> clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

Para limpar as conexões ativas para um intervalo de endereços IP:

```
> clear conn address 192.168.1.1-192.168.1.10 all
```

Observação: é altamente recomendável usar a palavra-chave 'all' no final do comando clear conn address para forçar a limpeza das tentativas de conexão de força bruta de VPN ativas para o firewall seguro, principalmente quando a natureza do ataque de força bruta de VPN está iniciando uma explosão de tentativas de conexão constantes.

Configurar uma ACL de plano de controle para FTD gerenciado pelo FDM

Este é o procedimento que você precisa seguir em um FDM para configurar uma ACL de plano de controle para bloquear ataques de força bruta de VPN recebidos para a interface FTD externa:

Etapa 1. Abra a GUI do FDM via HTTPS e Efetue login com suas credenciais.

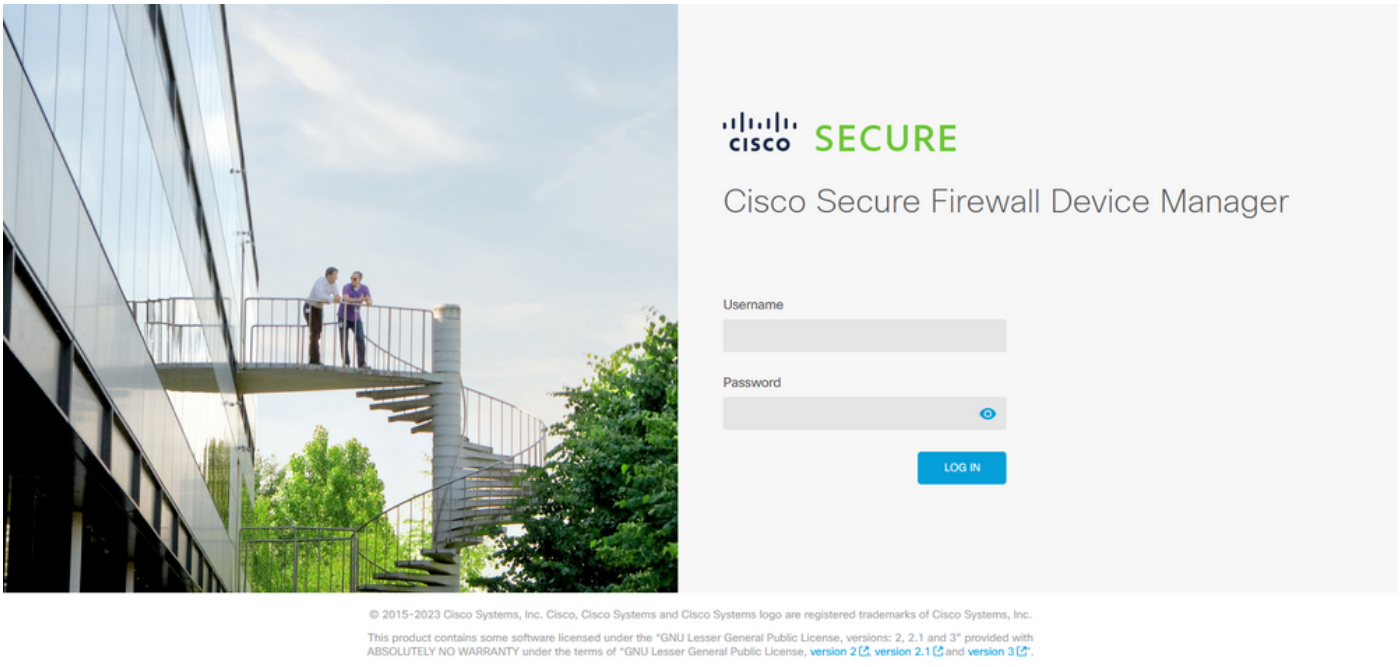

Imagem 24. Página Log-in do FDM

Etapa 2. Você precisa criar uma rede de objetos. Para isso, navegue até Objetos:

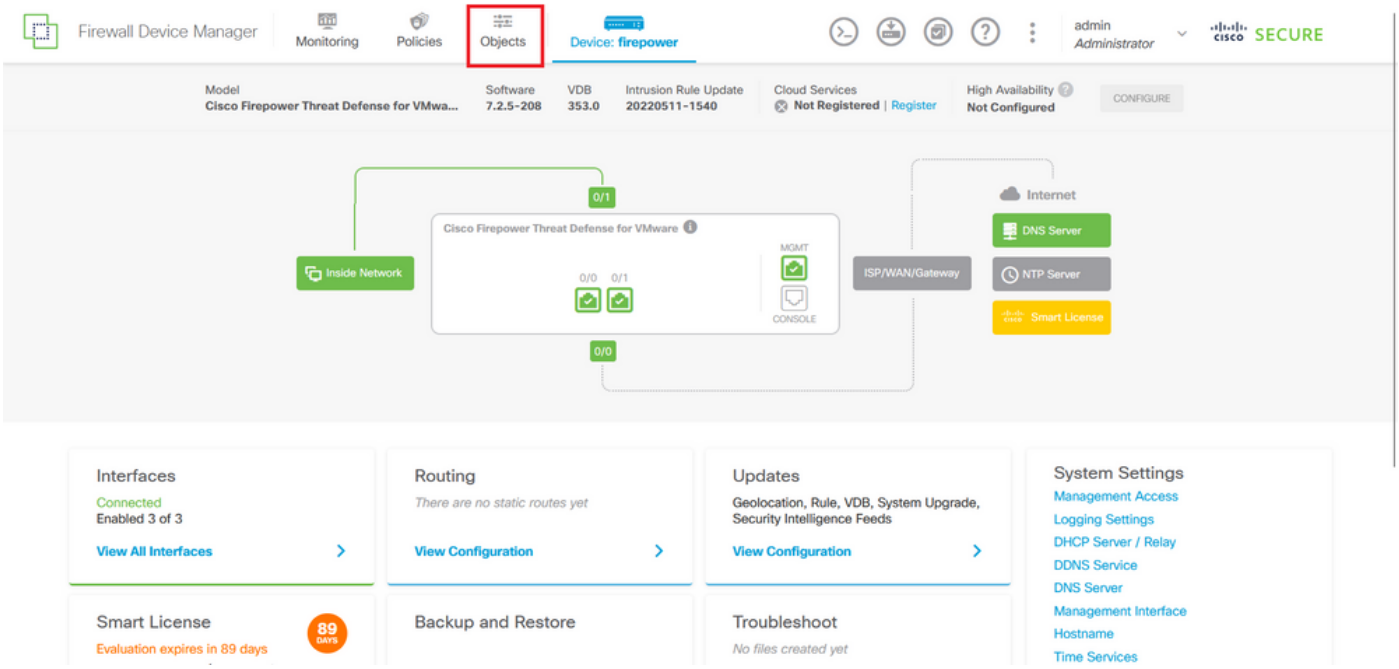

Imagem 25. Painel principal do FDM

Etapa 2.1. No painel esquerdo, selecione Redes e clique no botão '+' para criar um novo objeto de rede.

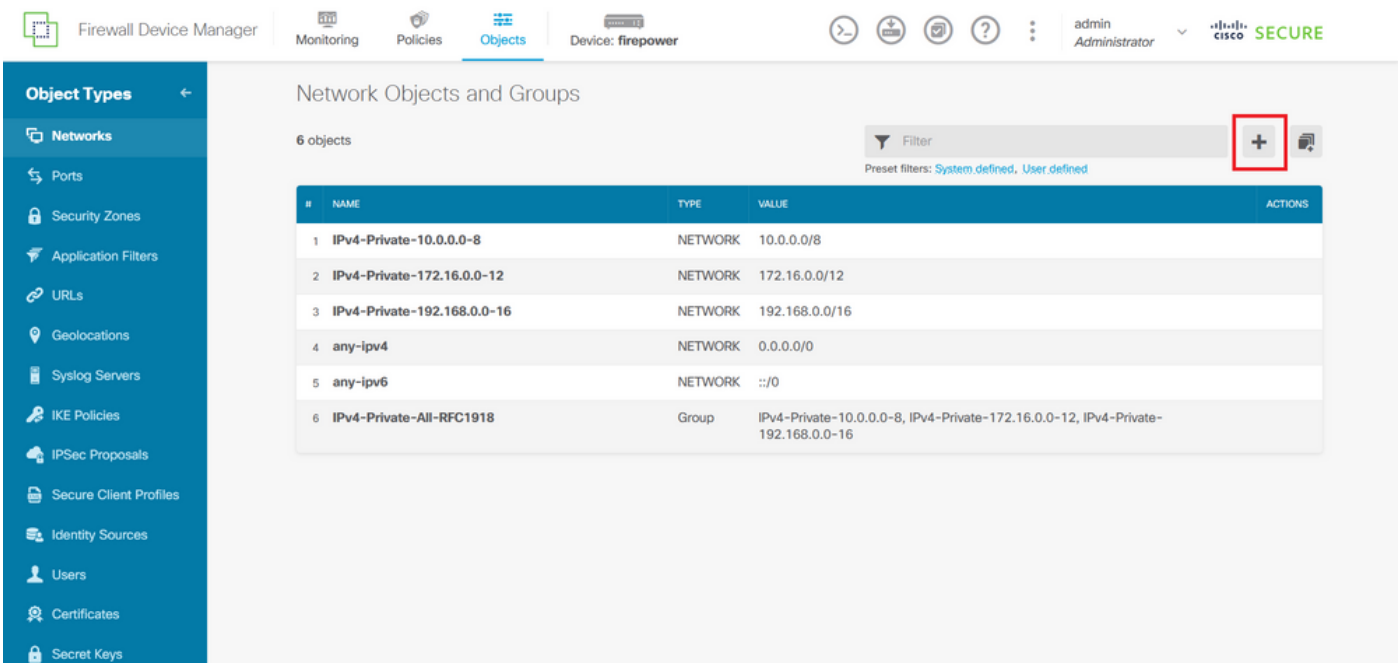

Imagem 26. Criação de objeto

Etapa 2.2. Adicione um nome para o objeto de rede, selecione o tipo de rede do objeto, adicione o endereço IP, o endereço de rede ou o intervalo de IPs para corresponder ao tráfego que precisa ser negado para o FTD. Em seguida, clique no botão Ok para concluir a rede de objetos.

- Neste exemplo, a rede de objetos configurada destina-se a bloquear ataques de força bruta de VPN provenientes da sub-rede 192.168.1.0/24.

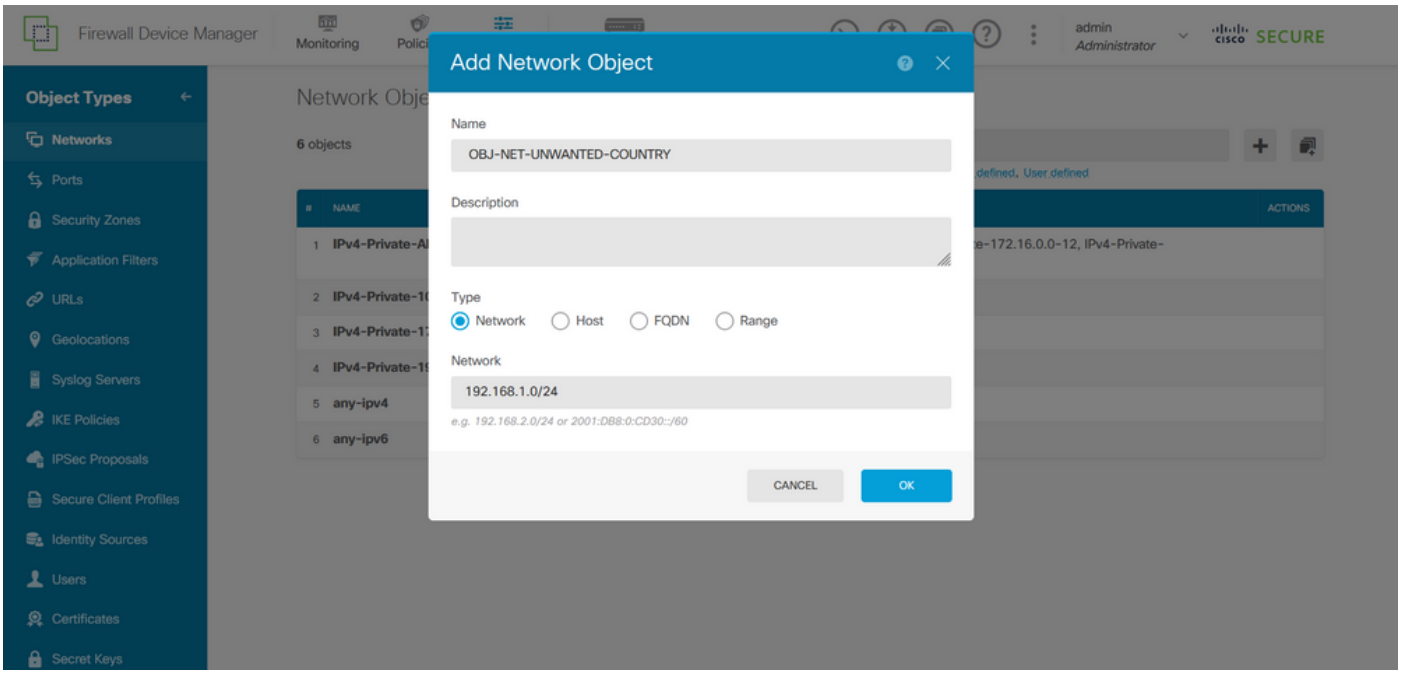

Imagem 27. Adicionar objeto de rede

Etapa 3. Em seguida, você precisa criar uma ACL estendida; para isso, navegue até a guia Device (Dispositivo) no menu superior.

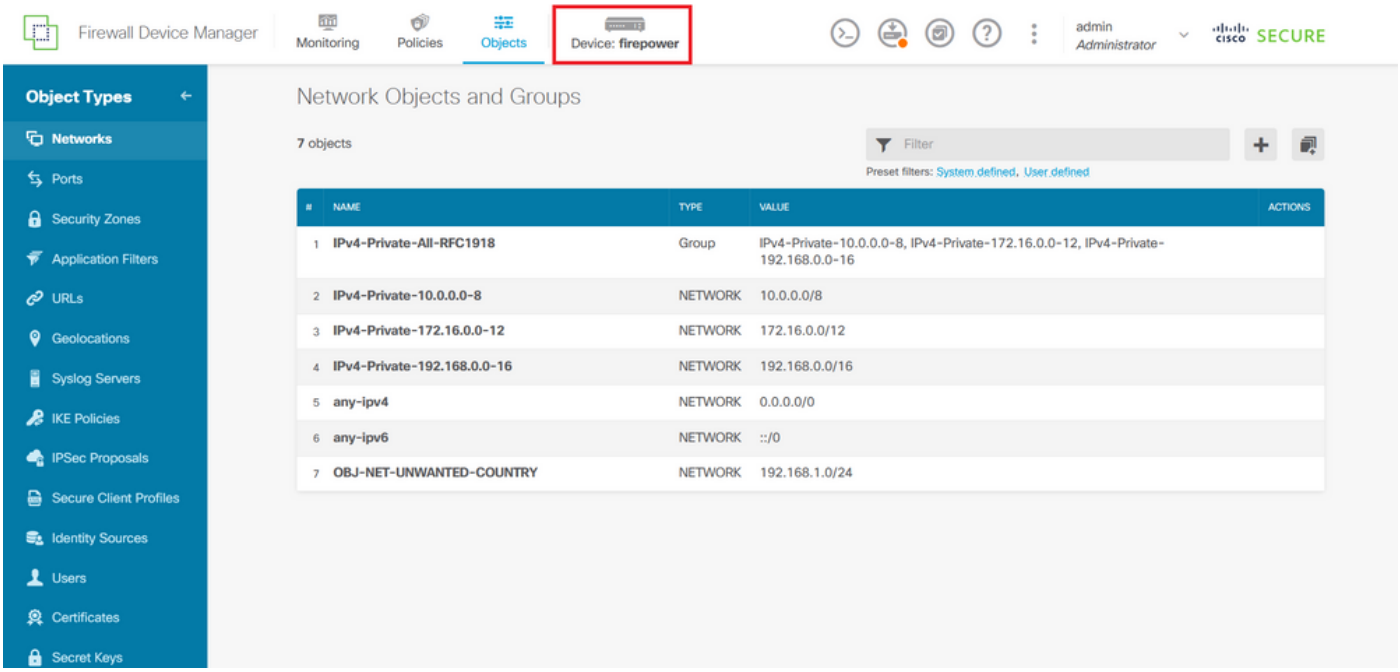

Imagem 28. Página de configurações do dispositivo

Etapa 3.1. Role para baixo e selecione Exibir configuração no quadrado Configuração avançada da seguinte maneira.

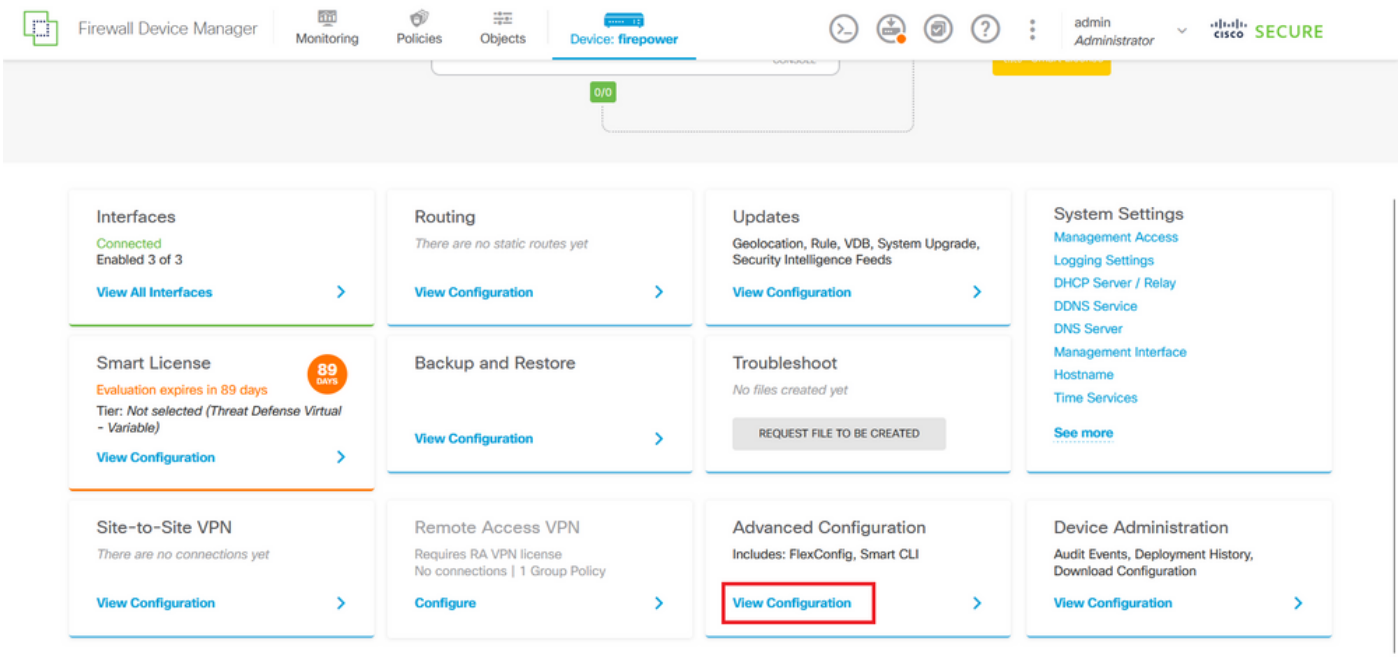

Imagem 29. Configuração Avançada do FDM

Etapa 3.2. Em seguida, no painel esquerdo, navegue até Smart CLI > Objects e clique em CREATE SMART CLI OBJECT.

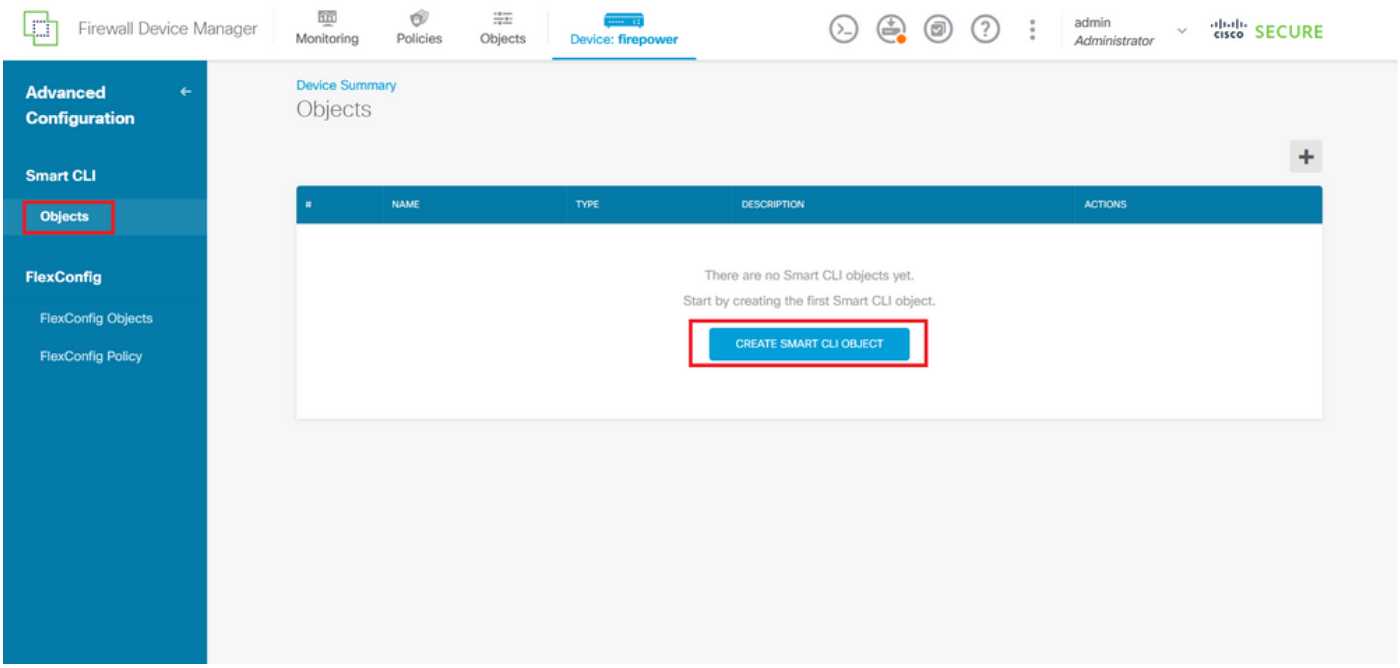

Imagem 30. Objetos Smart CLI

Etapa 3.3. Adicione um nome para a ACL estendida a ser criada, selecione Lista de acesso estendida no menu suspenso de modelos de CLI e configure as ACEs necessárias usando o objeto de rede criado na etapa 2.2 acima e clique no botão OK para concluir a ACL.

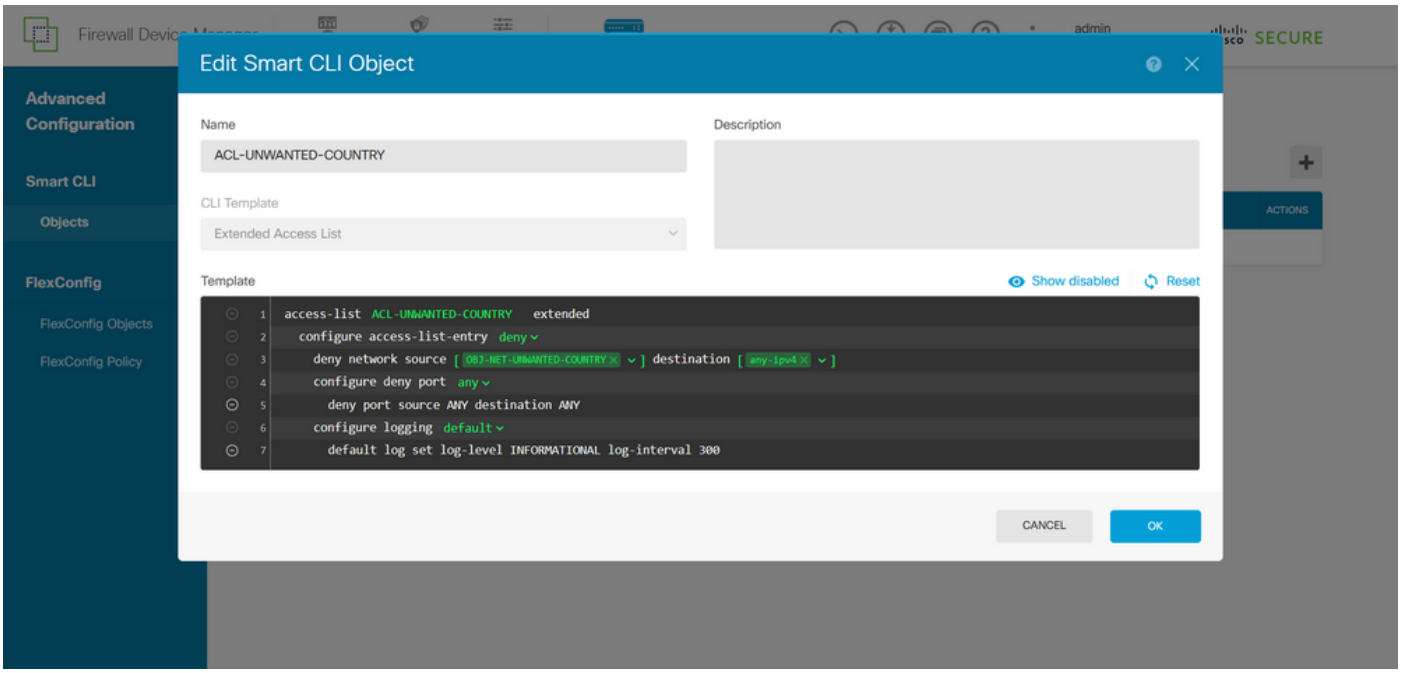

Imagem 31. Criação de ACL estendida

Observação: se precisar adicionar mais ACEs para a ACL, você poderá fazê-lo passando o mouse sobre a esquerda da ACE atual; em seguida, aparecerão três pontos clicáveis. Clique neles e selecione Duplicar para adicionar mais ACEs.

Etapa 4. Em seguida, você precisa criar um objeto FlexConfig, para isso, navegue até o painel esquerdo e selecione FlexConfig > Objetos FlexConfig e clique em CRIAR OBJETO FLEXCONFIG.

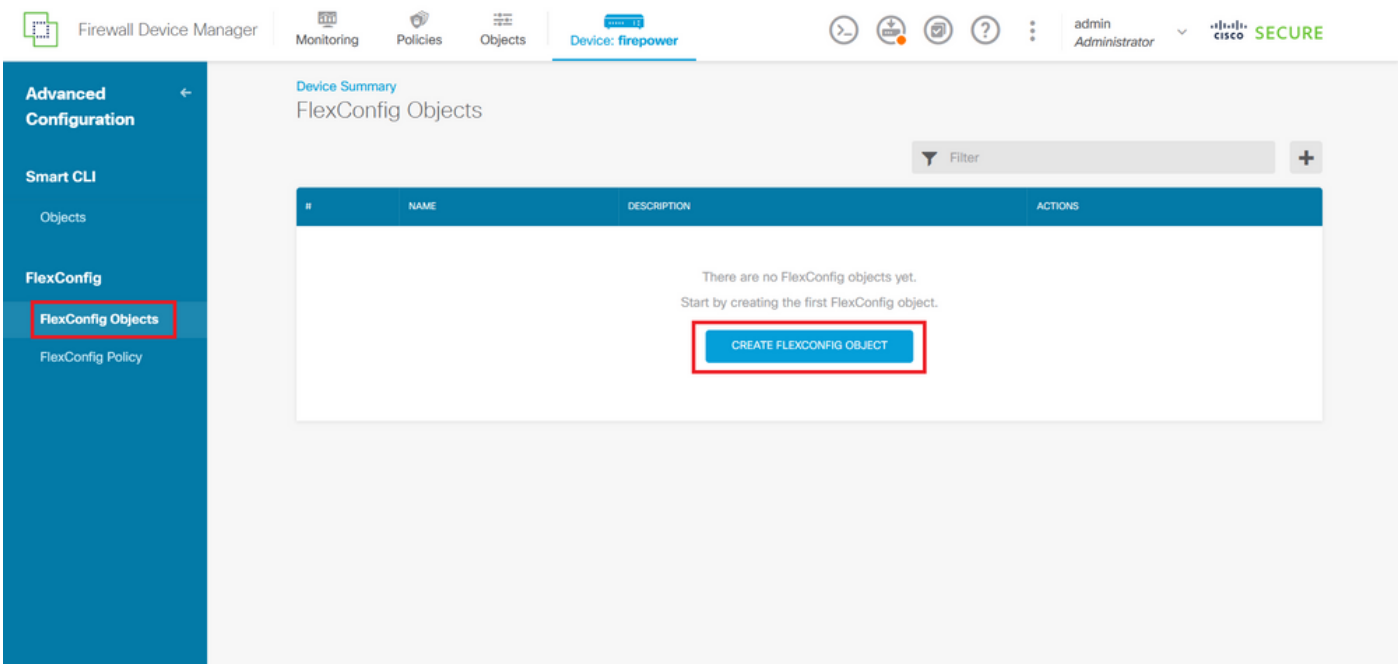

Imagem 32. Objetos FlexConfig

Etapa 4.1. Adicione um nome para o objeto FlexConfig para criar e configurar a ACL do plano de controle como entrada para a interface externa da seguinte maneira.

Sintaxe da linha de comando:

```
access-group "ACL-name" in interface "interface-name" control-plane
```

Isso se traduz no próximo exemplo de comando, que usa a ACL estendida criada na Etapa 3.3 "ACL-UNWANTED-COUNTRY" acima, da seguinte maneira:

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

É assim que ele deve ser configurado na janela do objeto FlexConfig. Depois disso, selecione o botão OK para concluir o objeto FlexConfig.

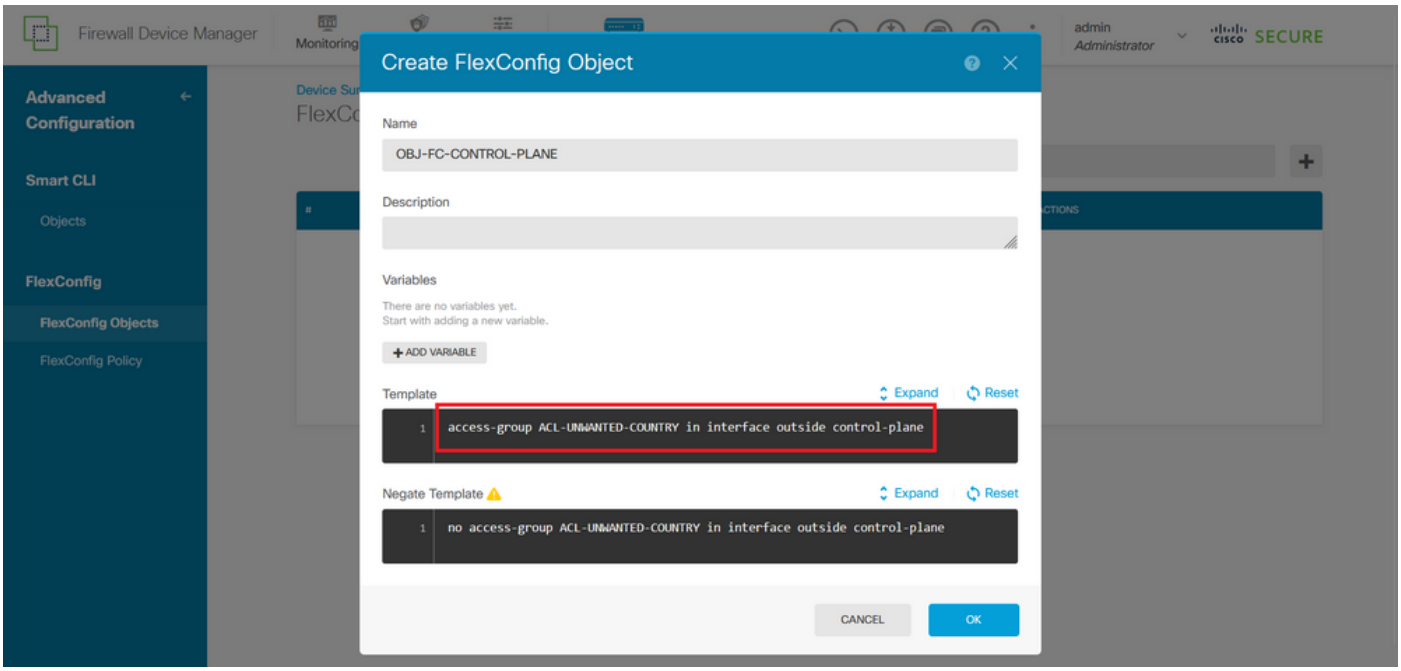

Imagem 3. Criação de Objeto FlexConfig

Etapa 5. Prossiga para criar uma Política FlexConfig, para isso, navegue até Flexconfig > Política FlexConfig, clique no botão '+' e selecione o objeto FlexConfig que foi criado na etapa 4.1 acima.

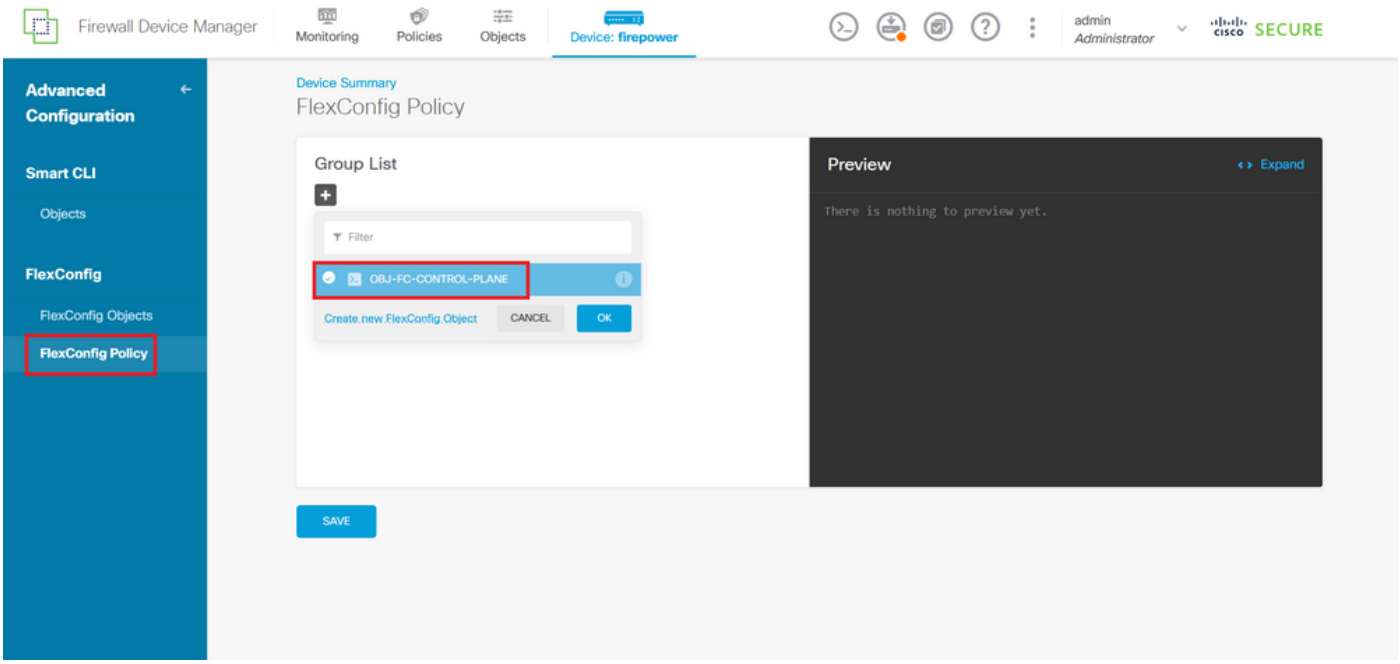

Imagem 34. Política FlexConfig

Etapa 5.1. Verifique se a visualização FlexConfig mostra a configuração correta da ACL do plano de controle criada e clique no botão Save (Salvar).

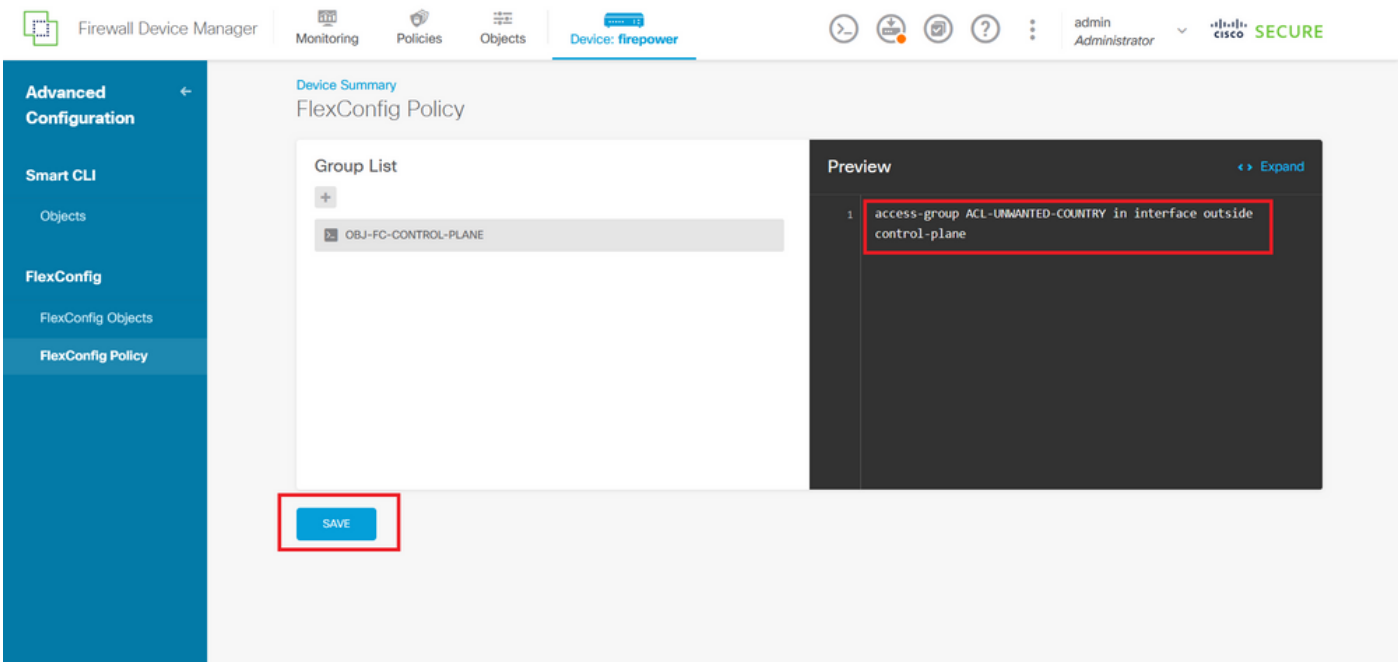

Imagem 35. Visualização da Política FlexConfig

Etapa 6. Implante as alterações de configuração no FTD que você deseja proteger contra os ataques de força bruta da VPN. Para isso, clique no botão Implantação no menu superior, confirme se as alterações de configuração a serem implantadas estão corretas e clique em IMPLANTAR AGORA.

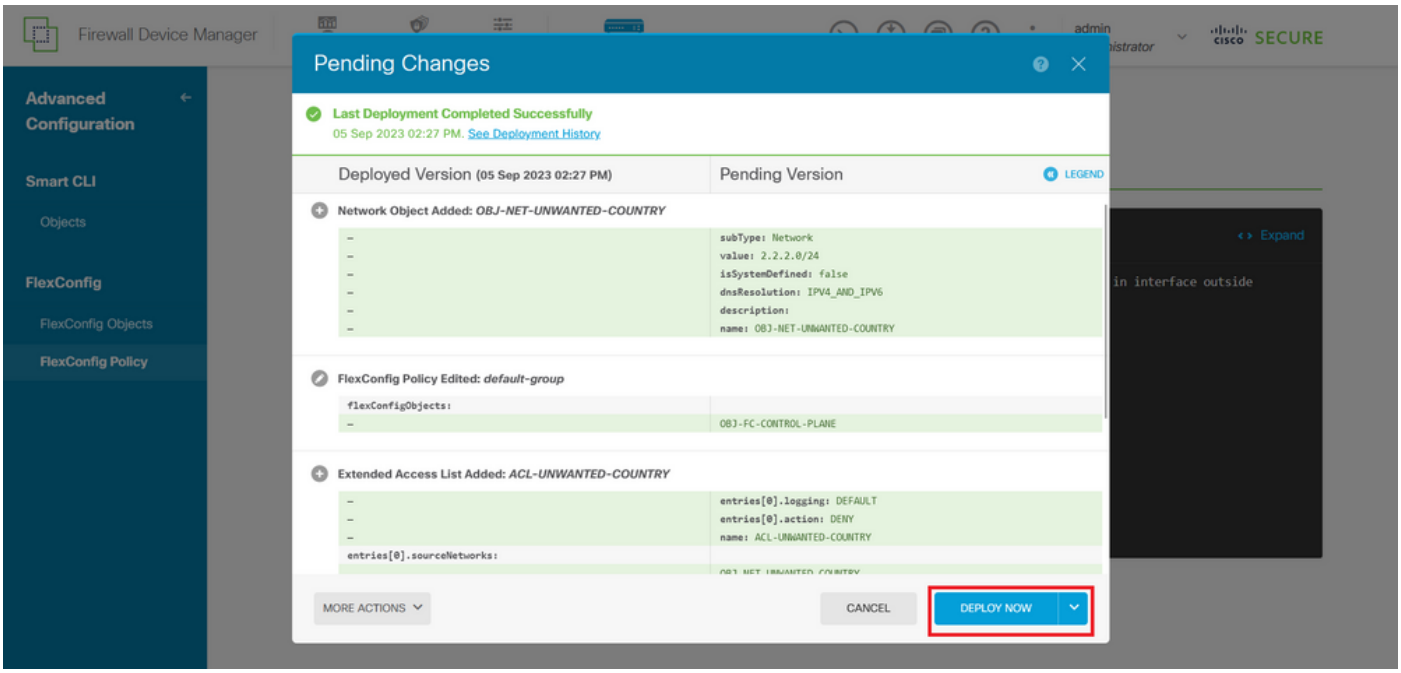

Imagem 36. Implantação Pendente

Etapa 6.1. Valide se a implantação da política foi bem-sucedida.

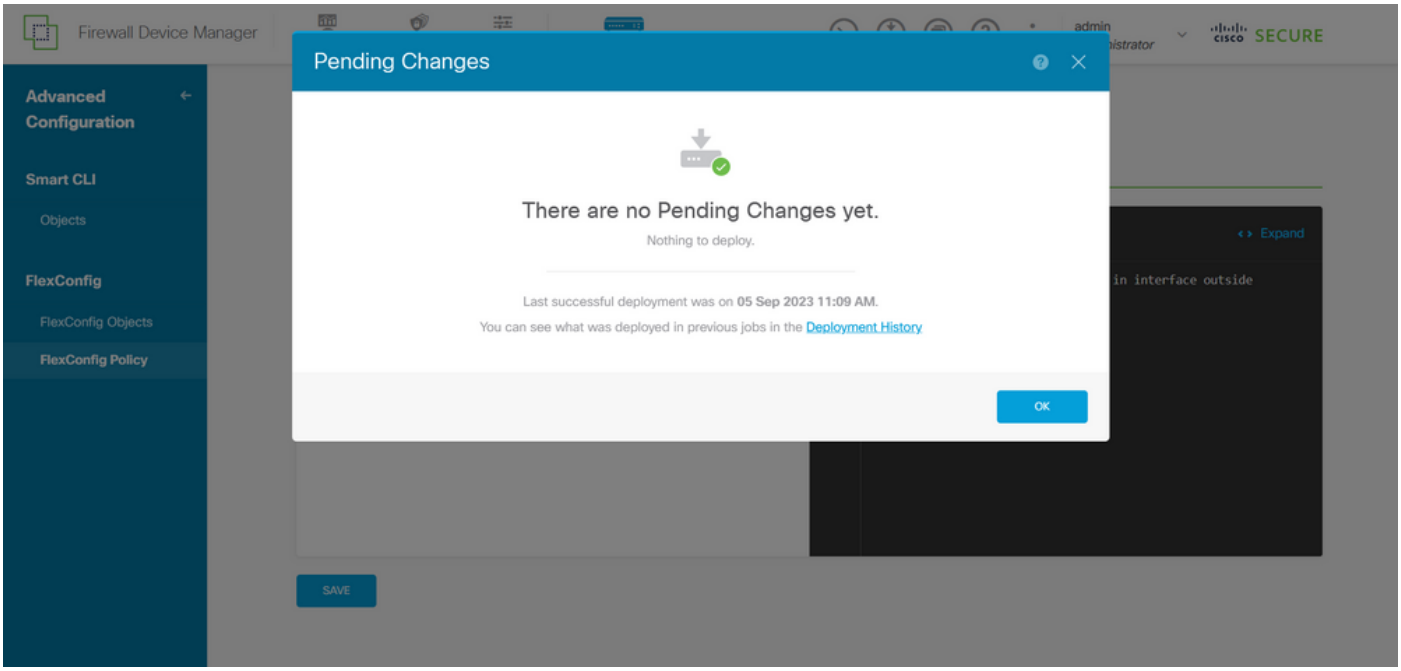

Imagem 37. Implantação bem-sucedida

Passo 7. Se você criar uma nova ACL de plano de controle para o FTD ou se editou uma ACL existente que esteja ativamente em uso, é importante destacar que as alterações de configuração feitas não se aplicam a conexões já estabelecidas com o FTD, portanto, você precisa limpar manualmente as tentativas de conexão ativas ao FTD. Para isso, conecte-se ao CLI do FTD e limpe as conexões ativas da seguinte maneira.

Para limpar a conexão ativa para um endereço IP de host específico:

```
> clear conn address 192.168.1.10 all
```

Para limpar as conexões ativas de toda uma rede de sub-rede:

```
> clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

Para limpar as conexões ativas para um intervalo de endereços IP:

```
> clear conn address 192.168.1.1-192.168.1.10 all
```

Observação: é altamente recomendável usar a palavra-chave 'all' no final do comando clear conn address para forçar a limpeza das tentativas de conexão de força bruta de VPN ativas para o firewall seguro, principalmente quando a natureza do ataque de força bruta de VPN está iniciando uma explosão de tentativas de conexão constantes.

Configurar uma ACL de plano de controle para ASA usando CLI

Este é o procedimento que você precisa seguir em uma CLI do ASA para configurar uma ACL de plano de controle para bloquear ataques de força bruta de VPN recebidos para a interface externa:

Etapa 1. Faça login no firewall seguro ASA via CLI e obtenha acesso ao "configure terminal" da seguinte maneira.

```
asa# configure terminal
```

Etapa 2. Use o próximo comando para configurar uma ACL estendida para bloquear um endereço IP de host ou um endereço de rede para o tráfego que precisa ser bloqueado para o ASA.

- Neste exemplo, você cria uma nova ACL chamada 'ACL-UNWANTED-COUNTRY' e a entrada ACE configurada bloqueará ataques de força bruta de VPN provenientes da sub-rede 192.168.1.0/24.

```
asa(config)# access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
```

Etapa 3. Use o próximo comando access-group para configurar a ACL 'ACL-UNWANTED-COUNTRY' como uma ACL de plano de controle para a interface ASA externa.

```
asa(config)# access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Etapa 4. Se você criar uma nova ACL de plano de controle ou se editou uma ACL existente que esteja ativamente em uso, é importante destacar que as alterações de configuração feitas não se aplicam a conexões já estabelecidas com o ASA, portanto, você precisa limpar manualmente as tentativas de conexão ativas com o ASA. Para isso, limpe as conexões ativas da seguinte maneira.

Para limpar a conexão ativa para um endereço IP de host específico:

```
asa# clear conn address 192.168.1.10 all
```

Para limpar as conexões ativas de toda uma rede de sub-rede:

```
asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

Para limpar as conexões ativas para um intervalo de endereços IP:

```
asa# clear conn address 192.168.1.1-192.168.1.10 all
```

Observação: é altamente recomendável usar a palavra-chave 'all' no final do comando clear conn address para forçar a limpeza das tentativas de conexão de força bruta de VPN ativas para o firewall seguro, principalmente quando a natureza do ataque de força bruta de VPN está iniciando uma explosão de tentativas de conexão constantes.

Configuração alternativa para bloquear ataques para um firewall seguro usando o comando 'shun'

No caso de uma opção imediata para bloquear ataques para o firewall seguro, você pode usar o comando 'shun'. O comando hunter permite bloquear conexões de um host de ataque.

- Depois de evitar um endereço IP, todas as conexões futuras do endereço IP de origem serão canceladas e registradas até que a função de bloqueio seja removida manualmente.

- A função de bloqueio do comando de bloqueio é aplicada independentemente de uma conexão com o endereço de host especificado estar ou não ativa no momento.

- Se você especificar o endereço de destino, as portas de origem e de destino e o protocolo, então você desconectará a conexão correspondente, bem como colocará um shun em todas as conexões futuras do IP de origem

  todas as conexões futuras são evitadas, não apenas aquelas que correspondem a esses parâmetros de conexão específicos.

- Você pode ter apenas um comando uneshuncommand por endereço IP de origem.

- Como o comando hunter é usado para bloquear ataques dinamicamente, ele não é exibido na configuração do dispositivo de defesa contra ameaças.

- Sempre que uma configuração de interface é removida, todos os shuns conectados a essa interface também são removidos.

- Sintaxe do comando Shun:

```
shun source_ip [ dest_ip source_port dest_port [ protocol]] [ vlan vlan_id]
```

- Para desativar um shun, use a forma no desse comando:

```
no shun source_ip [ vlan vlan_id]
```

Para evitar um endereço IP de host, siga as etapas abaixo para obter o firewall seguro. Neste exemplo, o comando 'shun' é usado para bloquear ataques de força bruta de VPN provenientes do endereço IP de origem 192.168.1.10.

Exemplo de configuração para FTD.

Etapa 1. Faça login no FTD via CLI e aplique o comando shun da seguinte maneira.

<#root>

>

shun 192.168.1.10

```
Shun 192.168.1.10 added in context: single_vf


Shun 192.168.1.10 successful
```

Etapa 2. Você pode usar os seguintes comandos show para confirmar os endereços IP shun no FTD e para monitorar as contagens de ocorrências shun por endereço IP:

```
<#root>

>

show shun

shun (outside) 192.168.1.10 0.0.0.0 0 0 0

>

show shun statistics

diagnostic=OFF, cnt=0
outside=ON, cnt=0

Shun 192.168.1.10 cnt=0, time=(0:00:28)
```

Exemplo de configuração para ASA

Etapa 1. Faça login no ASA via CLI e aplique o comando shun da seguinte maneira.

```
<#root>

asa#

 shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf


Shun 192.168.1.10 successful
```

Etapa 2. Você pode usar os seguintes comandos show para confirmar os endereços IP shun no ASA e para monitorar as contagens de ocorrências shun por endereço IP:

```
<#root>

asa#

show shun
```

```
shun (outside) 192.168.1.10 0.0.0.0 0 0 0

asa#
```

show shun statistics

```
outside=ON, cnt=0
inside=OFF, cnt=0
dmz=OFF, cnt=0
outside1=OFF, cnt=0
mgmt=OFF, cnt=0

Shun 192.168.1.10 cnt=0, time=(0:01:39)
```

Observação: para obter mais informações sobre o comando secure firewall shun, consulte a Referência de Comandos do Cisco Secure Firewall Threat Defense

---

Verificar

Para confirmar se a configuração da ACL do plano de controle está estabelecida para o firewall seguro, siga este procedimento:

Etapa 1. Faça login no firewall seguro via CLI e execute os próximos comandos para confirmar se a configuração da ACL do plano de controle foi aplicada.

Exemplo de saída para o DTF gerido pelo CVP:

<#root>

>

show running-config access-list ACL-UNWANTED-COUNTRY

```
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
```

>

show running-config access-group

```
***OUTPUT OMITTED FOR BREVITY***
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Exemplo de saída para o FTD gerenciado pelo FDM:

<#root>

> show running-config object id OBJ-NET-UNWANTED-COUNTRY

```
object network OBJ-NET-UNWANTED-COUNTRY
subnet 192.168.1.0 255.255.255.0
```

```
>
show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any4 log default

> show running-config access-group

***OUTPUT OMITTED FOR BREVITY***
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Exemplo de saída do ASA:

```
<#root>
asa#
show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

asa#
show running-config access-group

***OUTPUT OMITTED FOR BREVITY***
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Etapa 2. Para confirmar se a ACL do plano de controle está bloqueando o tráfego necessário, use o comando packet-tracer para simular uma conexão TCP 443 de entrada para a interface externa do firewall seguro e, em seguida, use o comando show access-list <acl-name> , a contagem de ocorrências da ACL deve ser incrementada toda vez que uma conexão de força bruta de VPN para o firewall seguro for bloqueada pela ACL do plano de controle:

- Neste exemplo, o comando packet-tracer simula uma conexão TCP 443 de entrada originada do host 192.168.1.10 e destinada ao endereço IP externo de nosso firewall seguro. A saída do "packet-tracer" confirma que o tráfego está sendo descartado e a saída do "show access-list" exibe os incrementos da contagem de ocorrências para nossa ACL de plano de controle:

Exemplo de saída para FTD

```
<#root>
>
```

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.251 443

Phase: 1
Type:

ACCESS-LIST

Subtype: log

Result: DROP

Elapsed time: 21700 ns
Config:
Additional Information:

Result:
input-interface: outside(vrfid:0)
input-status: up
input-line-status: up

Action: drop

Time Taken: 21700 ns

Drop-reason: (acl-drop) Flow is denied by configured rule

, Drop-location: frame 0x00005623c7f324e7 flow (NA)/NA

>

show access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f
access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any (

hitcnt=1

) 0x142f69bf

Exemplo de saída do ASA

<#root>

asa#

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.5 443

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 19688 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type:

```
ACCESS-LIST

Subtype: log

Result: DROP

Elapsed time: 17833 ns
Config:
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up

Action: drop

Time Taken: 37521 ns

Drop-reason: (acl-drop) Flow is denied by configured rule

, Drop-location: frame 0x0000556e6808cac8 flow (NA)/NA

asa#

show access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f
access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any

(hitcnt=1)

 0x9b4d26ac
```

Observação: se uma solução RAVPN como o Cisco Secure Client VPN for implementada no firewall seguro, uma tentativa real de conexão com o firewall seguro poderá ser realizada para confirmar se a ACL do plano de controle está funcionando conforme esperado para bloquear o tráfego necessário.

Bugs relacionados

- ENH | Conexões do AnyConnect Client baseadas em localização geográfica: ID de bug da Cisco CSCvs65322

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.