Configuración de las políticas de control de acceso del plano de control para Secure Firewall Threat Defence y ASA

Contenido

Introducción

Este documento describe el proceso para configurar las reglas de acceso del plano de control para Secure Firewall Threat Defense y Adaptive Security Appliance (ASA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protección frente a amenazas de firewall (FTD)
- Administrador de dispositivos de firewall seguro (FDM)
- Centro de gestión de firewall seguro (FMC)
- ASA de firewall seguro
- Lista de control de acceso (ACL)
- FlexConfig

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Secure Firewall Threat Defence versión 7.2.5
- Secure Firewall Manager Center versión 7.2.5
- Secure Firewall Device Manager versión 7.2.5
- Secure Firewall ASA versión 9.18.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El tráfico normalmente atraviesa un firewall y se enruta entre interfaces de datos; en algunas circunstancias, es beneficioso denegar el tráfico destinado al firewall seguro. El firewall seguro de Cisco puede utilizar una lista de control de acceso (ACL) del plano de control para restringir el tráfico "listo para usar". Un ejemplo de cuándo una ACL del plano de control puede ser útil sería controlar qué peers pueden establecer un túnel VPN (VPN de sitio a sitio o de acceso remoto) al firewall seguro.

Tráfico "mediante el dispositivo" de firewall seguro

El tráfico normalmente atraviesa los firewalls de una interfaz (entrante) a otra interfaz (saliente), lo que se conoce como tráfico 'mediante el dispositivo' y lo gestionan tanto las políticas de control de acceso (ACP) como las reglas de prefiltrado.

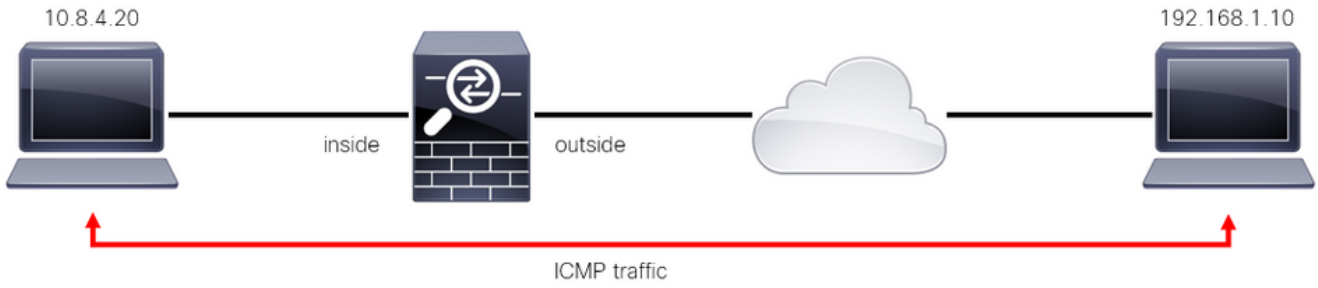

Imagen 1. Ejemplo de tráfico listo para usar

Tráfico "listo para usar" de firewall seguro

Hay otros casos en los que el tráfico está destinado directamente a una interfaz FTD (VPN de sitio a sitio o de acceso remoto), esto se conoce como tráfico "a la caja" y es administrado por el plano de control de esa interfaz específica.

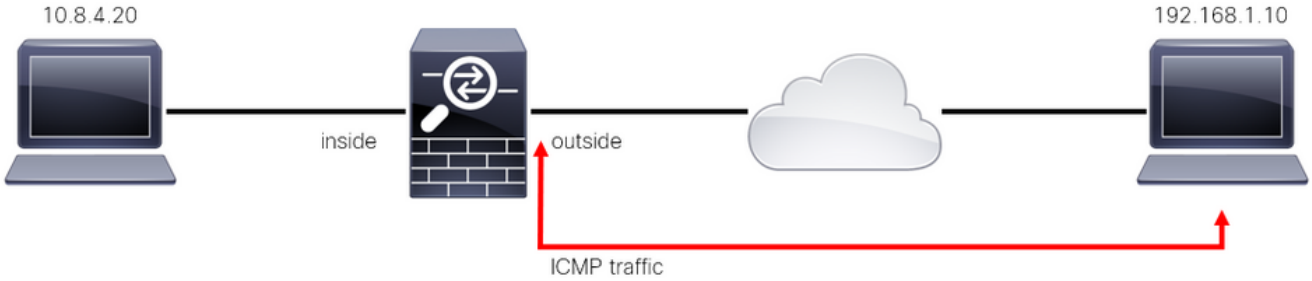

Imagen 2. Ejemplo de tráfico To-the-box

Consideraciones Importantes sobre las ACL del Plano de Control

- A partir de la versión 7.0 de FMC/FTD, se debe configurar una ACL del plano de control mediante FlexConfig, utilizando la misma sintaxis de comandos utilizada en el ASA.
- La palabra clave control-plane se anexa a la configuración del grupo de acceso, que aplica el tráfico 'a' la interfaz de firewall segura. Sin la palabra del plano de control anexada al comando, la ACL restringiría el tráfico a 'través' del firewall seguro.
- Una ACL de plano de control no restringe SSH, ICMP o TELNET entrante a una interfaz de firewall segura. Se procesan (se permiten o deniegan) según las directivas de configuración de la plataforma y tienen mayor prioridad.
- Una ACL del plano de control restringe el tráfico "al" propio firewall seguro, mientras que la política de control de acceso para el FTD o las ACL normales para el ASA, controla el tráfico "a través" del firewall seguro.
- A diferencia de una ACL normal, no hay una 'deny' implícita al final de la ACL.
- La función de búsqueda de grupos de objetos (OGS) no funciona en las ACL del plano de control, CSCwi58818.
- En el momento de la creación de este documento, la función de geolocalización de FTD no se puede utilizar para restringir el acceso al FTD.

Configurar

En el siguiente ejemplo, un conjunto de direcciones IP de un país determinado intenta aplicar fuerza bruta VPN a la red al intentar iniciar sesión en el RAVPN FTD. La mejor opción para proteger el FTD contra estos ataques de fuerza bruta VPN es configurar una ACL de plano de control para bloquear estas conexiones a la interfaz FTD externa.

Configuraciones

Configuración de una ACL de plano de control para FTD gestionada por FMC

Este es el procedimiento que debe seguir en un FMC para configurar una ACL del plano de control para bloquear los ataques de fuerza bruta de VPN entrantes a la interfaz FTD externa:

Paso 1. Abra la interfaz gráfica de usuario (GUI) de FMC mediante HTTPS e inicie sesión con sus credenciales.

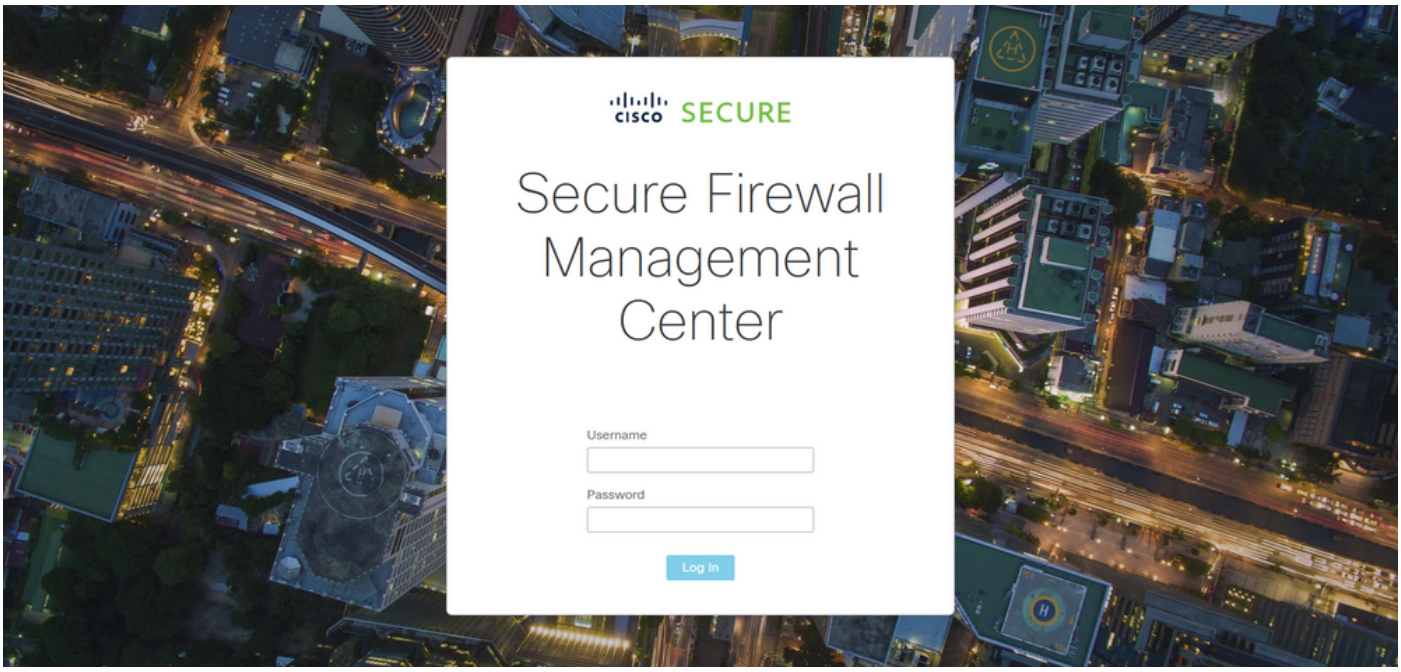

Imagen 3. Página de inicio de sesión de FMC

Paso 2. Necesita crear una ACL extendida. Para esto, navegue hasta Objetos > Administración de objetos.

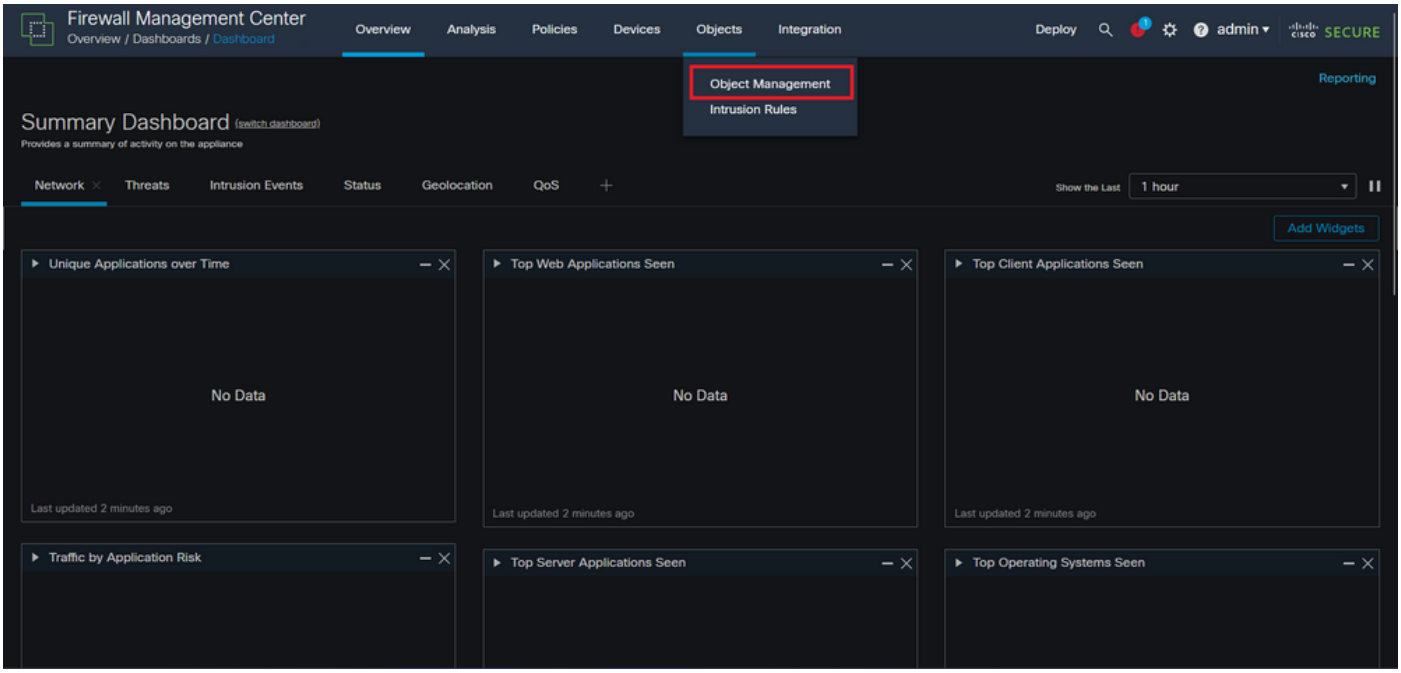

Imagen 4. Gestión de objetos

Paso 2.1. En el panel izquierdo, navegue hasta Lista de acceso > Extendida para crear una ACL extendida.

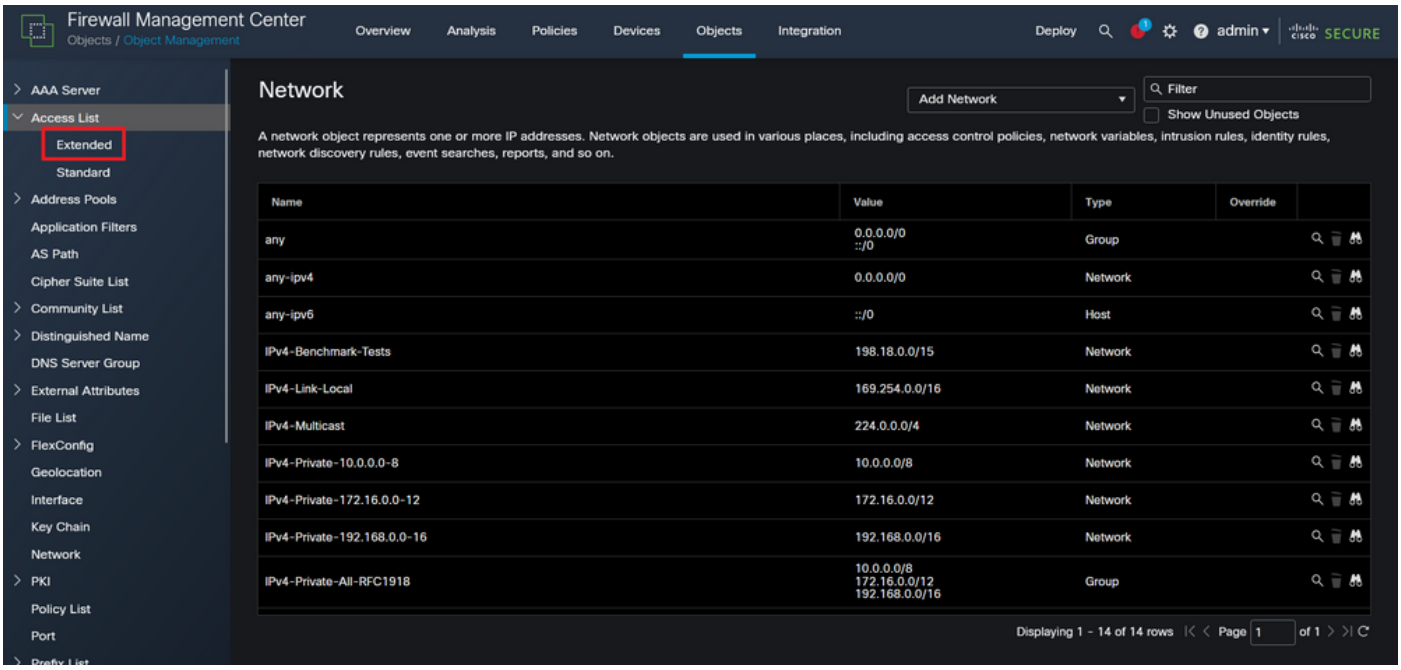

Imagen 5. Menú ACL extendido

Paso 2.2. A continuación, seleccione Add Extended Access List.

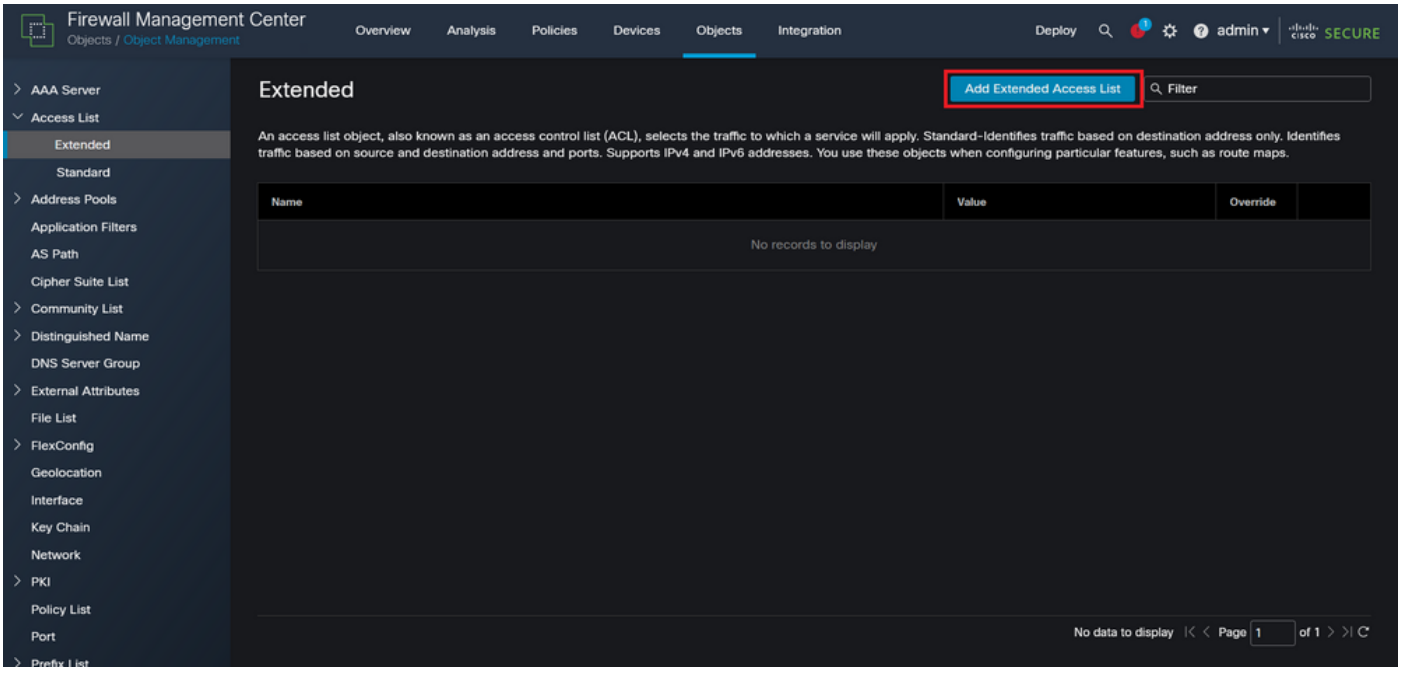

Imagen 6. Agregar ACL extendida

Paso 2.3. Escriba un nombre para la ACL extendida y, a continuación, haga clic en el botón Add para crear una entrada de control de acceso (ACE):

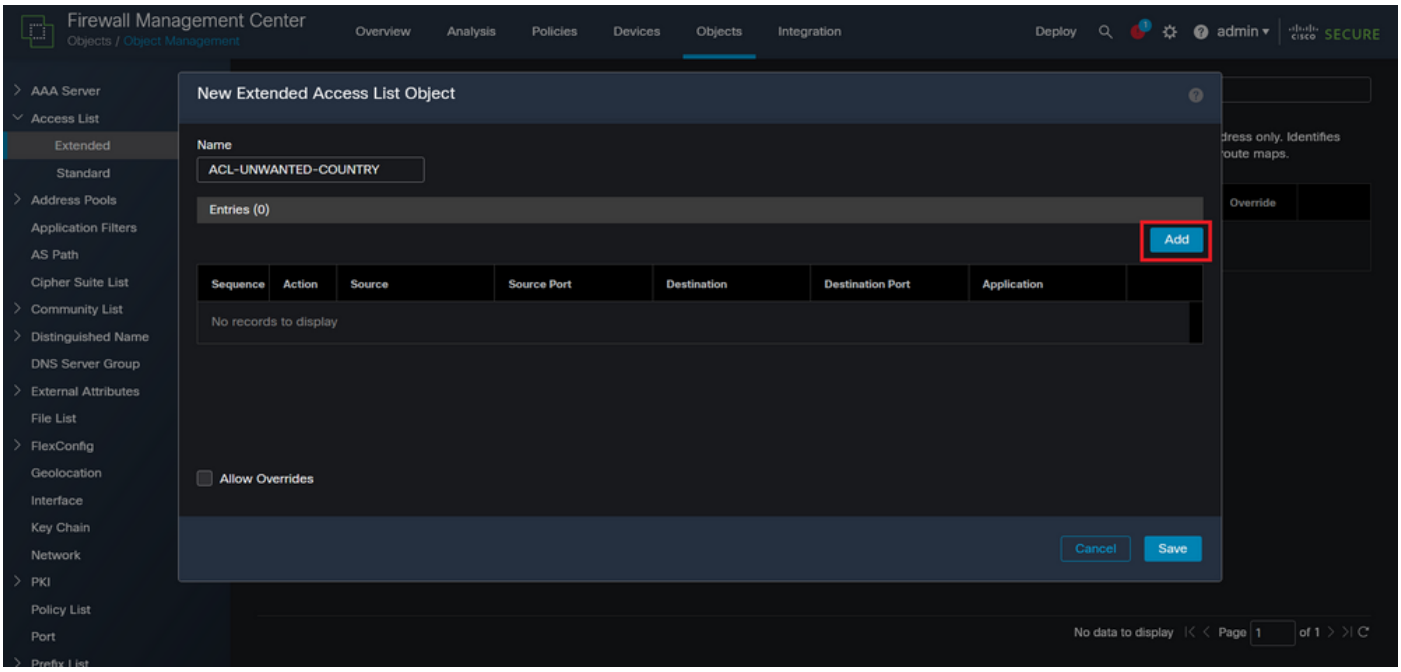

Imagen 7. Entradas de ACL extendidas

Paso 2.4. Cambie la acción ACE a Block, luego agregue la red de origen para que coincida con el tráfico que debe ser denegado al FTD, mantenga la red de destino como Any y haga clic en el botón Add para completar la entrada ACE:

- En este ejemplo, la entrada ACE configurada bloquea los ataques de fuerza bruta VPN que provienen de la subred 192.168.1.0/24.

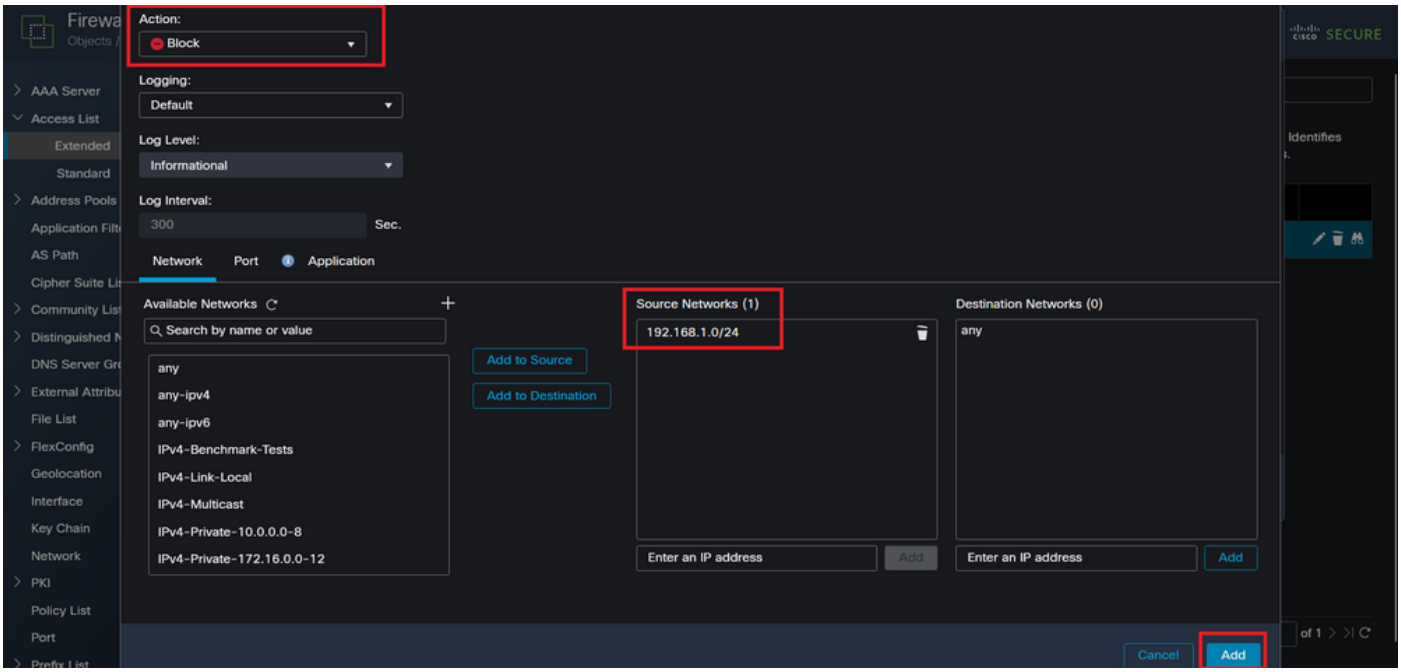

Imagen 8. Redes denegadas

Paso 2.5. En caso de que necesite agregar más entradas ACE, vuelva a hacer clic en el botón Add y repita el paso 2.4. Después de esto, haga clic en el botón Save (Guardar) para completar la configuración de ACL.

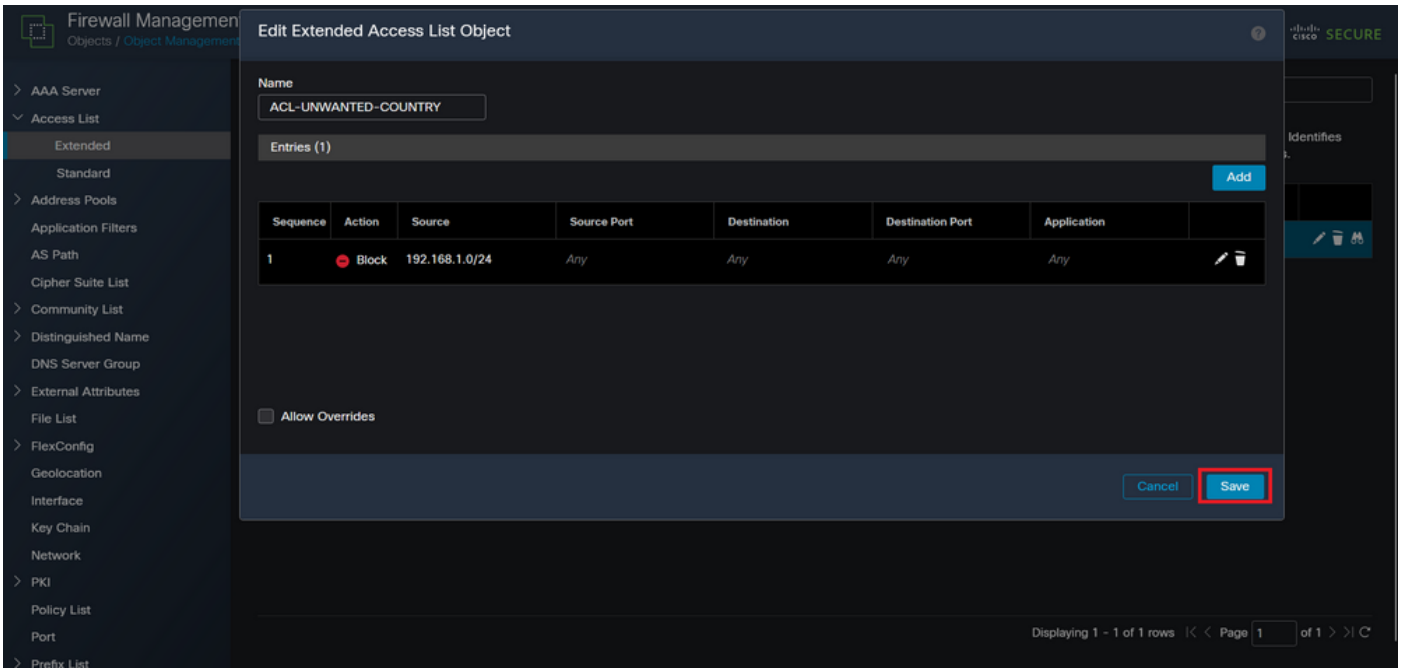

Imagen 9. Entradas de ACL extendidas completadas

Paso 3. A continuación, debe configurar un objeto Flex-Config para aplicar la ACL del plano de control a la interfaz FTD externa. Para ello, vaya al panel izquierdo y seleccione la opción FlexConfig > Objeto FlexConfig.

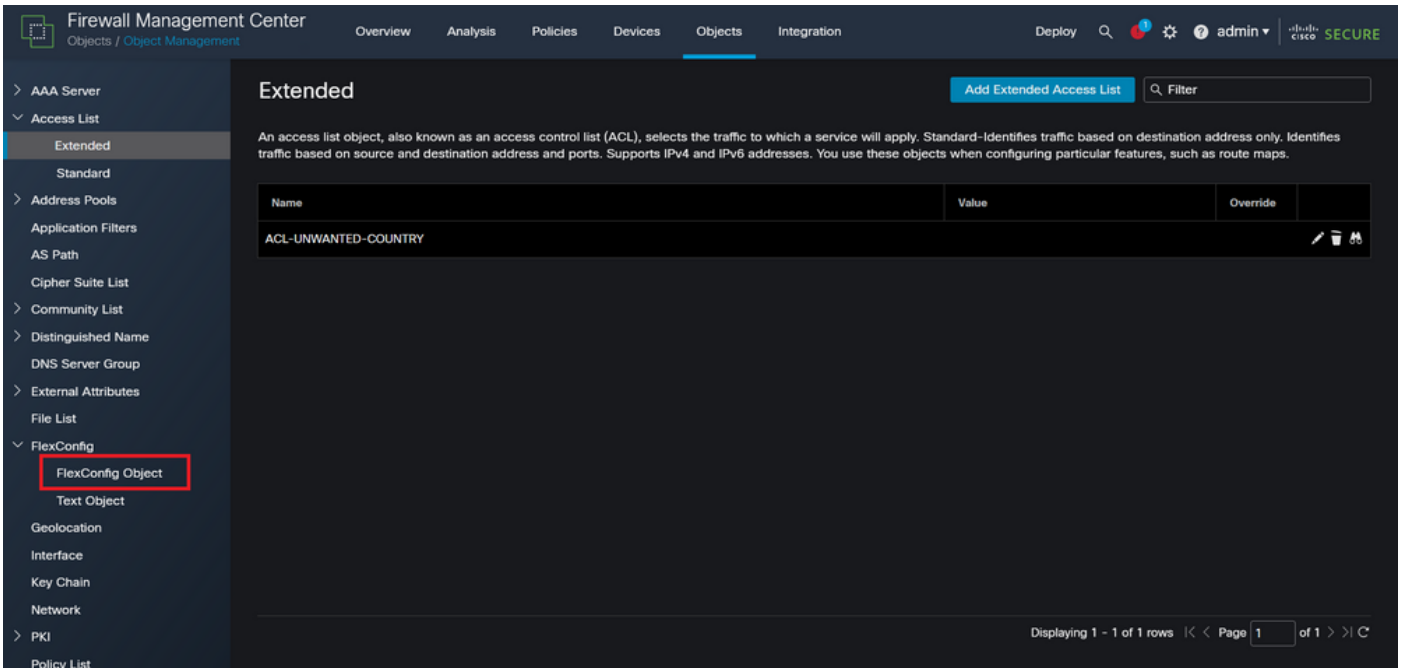

Imagen 10. Menú Objeto FlexConfig

Paso 3.1. Haga clic en Add FlexConfig Object.

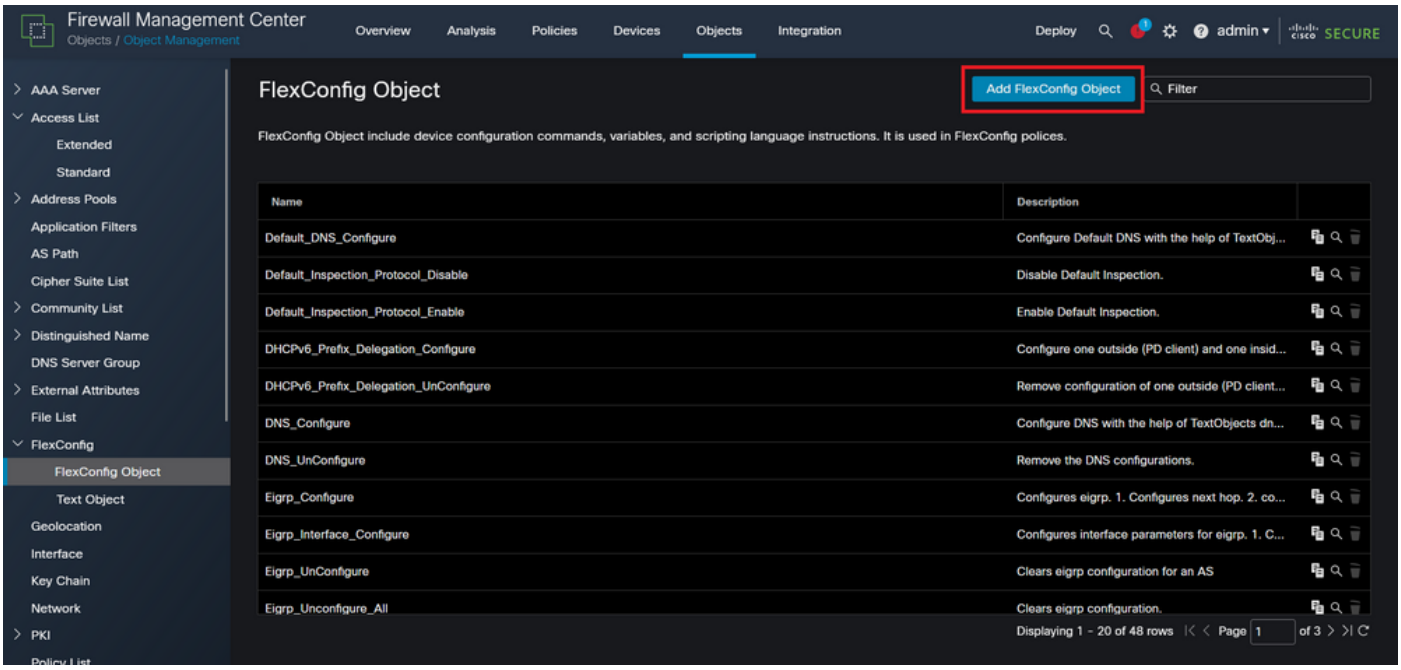

Imagen 1. Agregar Objeto Flexconfig

Paso 3.2. Agregue un nombre para el objeto FlexConfig y, a continuación, inserte un objeto de directiva ACL. Para ello, seleccione Insertar > Insertar objeto de directiva > Objeto ACL extendido.

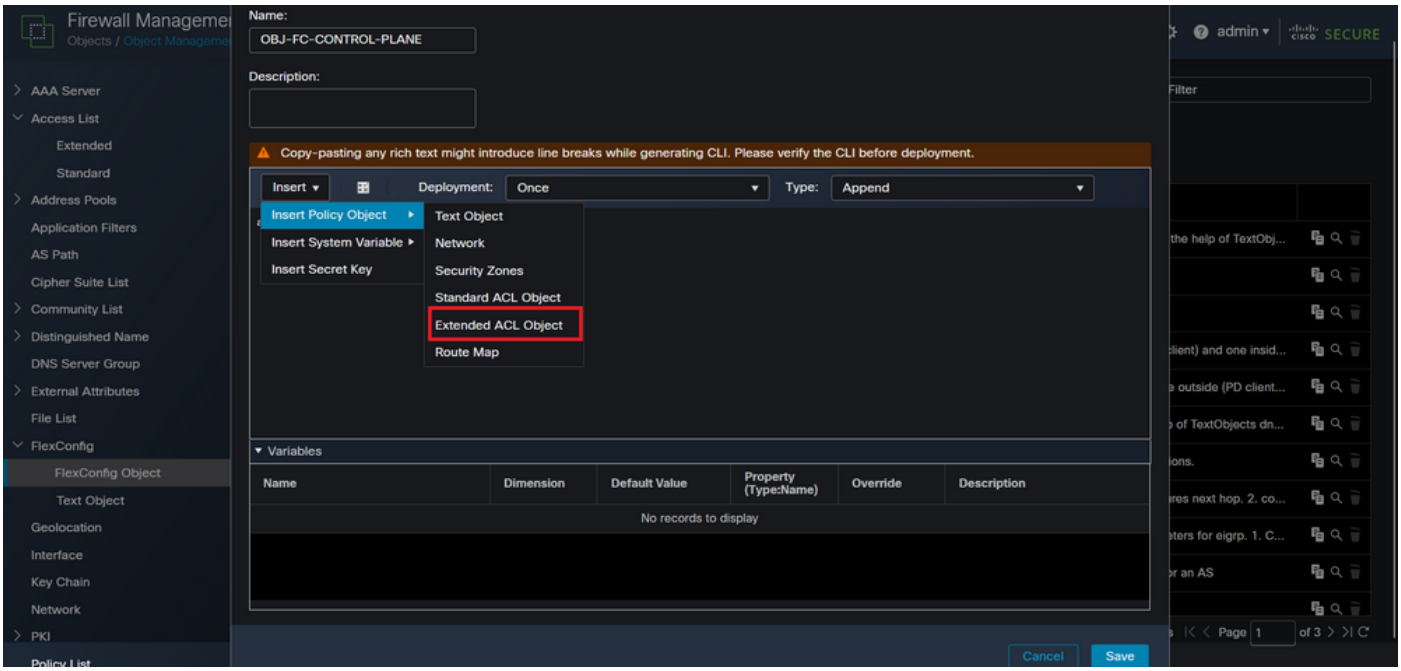

Imagen 12. Variable de objeto FlexConfig

Paso 3.3. Agregue un nombre para la variable de objeto ACL y luego, seleccione la ACL extendida que se creó en el Paso 2.3, después de esto, haga clic en el botón Save.

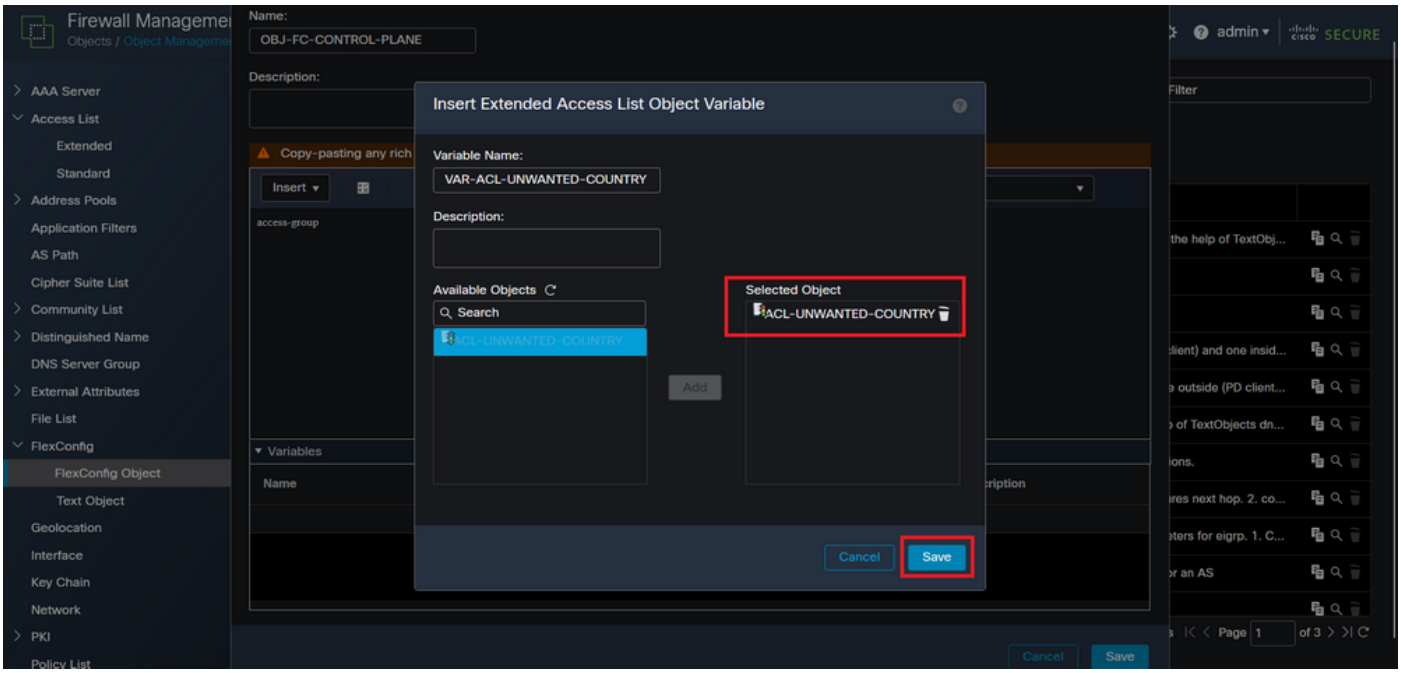

Imagen 13. Asignación de ACL de variable de objeto FlexConfig

Paso 3.4. Luego, configure la ACL del plano de control como entrante para la interfaz exterior.

Sintaxis de la línea de comandos:

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

Esto se traduce en el siguiente ejemplo de comando, que utiliza la variable ACL creada en el Paso 2.3 'VAR-ACL-UNWANTED-COUNTRY':

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

Así es como debe configurarse en la ventana de objetos de FlexConfig. Después de esto, seleccione el botón Save para completar el objeto FlexConfig.

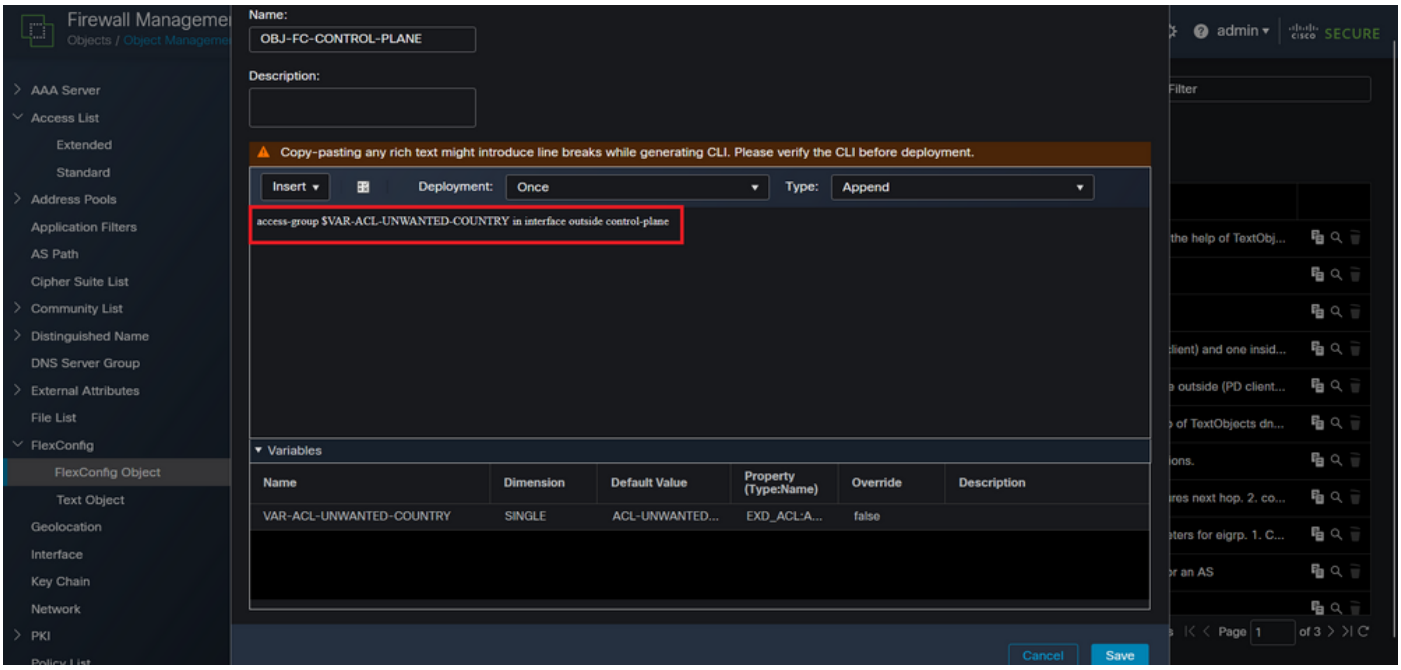

Imagen 14. Línea de comandos completa del objeto Flexconfig

Nota: Se recomienda encarecidamente configurar la ACL del plano de control sólo para las interfaces que reciben sesiones VPN de acceso remoto entrantes en el firewall seguro, como la interfaz externa.

Paso 4. Debe aplicar la configuración del objeto FlexConfig al FTD. Para ello, vaya a Dispositivos > FlexConfig.

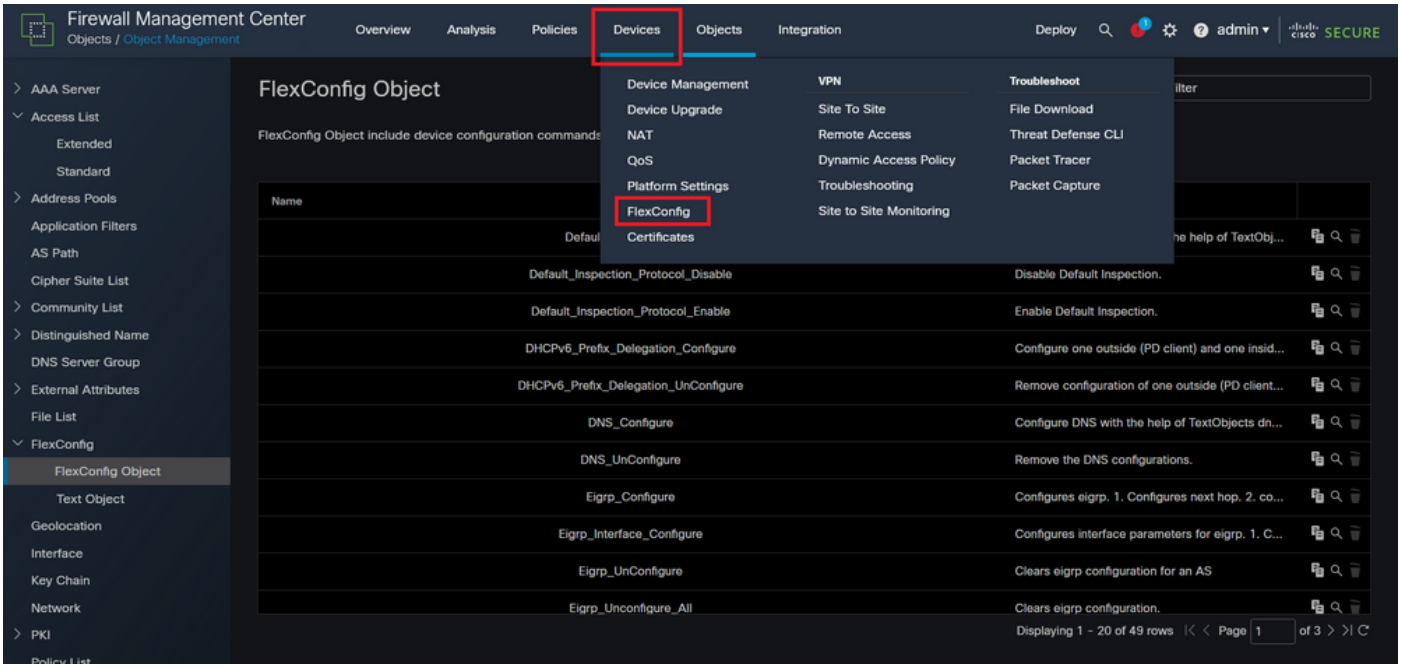

Imagen 15. Menú Política de FlexConfig

Paso 4.1. A continuación, haga clic en New Policy (Nueva política) si aún no hay una FlexConfig creada para el FTD o edite la política FlexConfig existente.

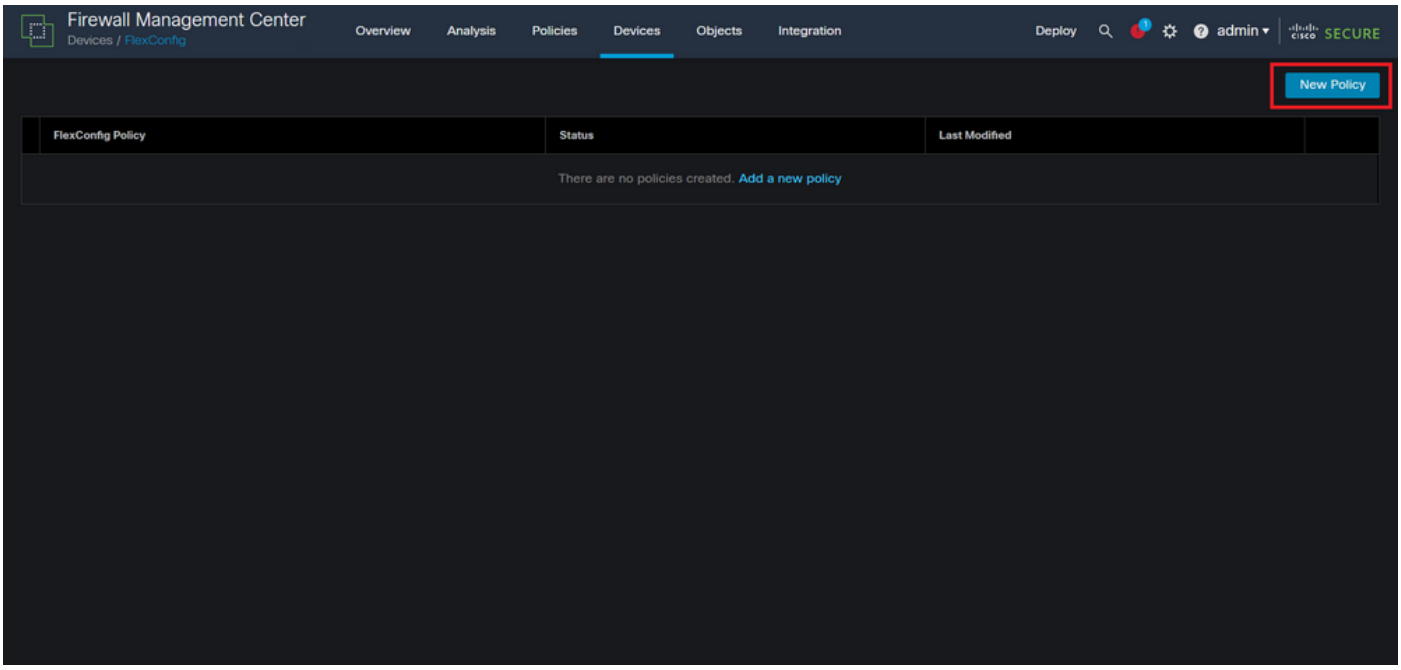

Imagen 16. Creación de la política FlexConfig

Paso 4.2. Agregue un nombre para la nueva política FlexConfig y seleccione el FTD al que desea aplicar la ACL del plano de control creada.

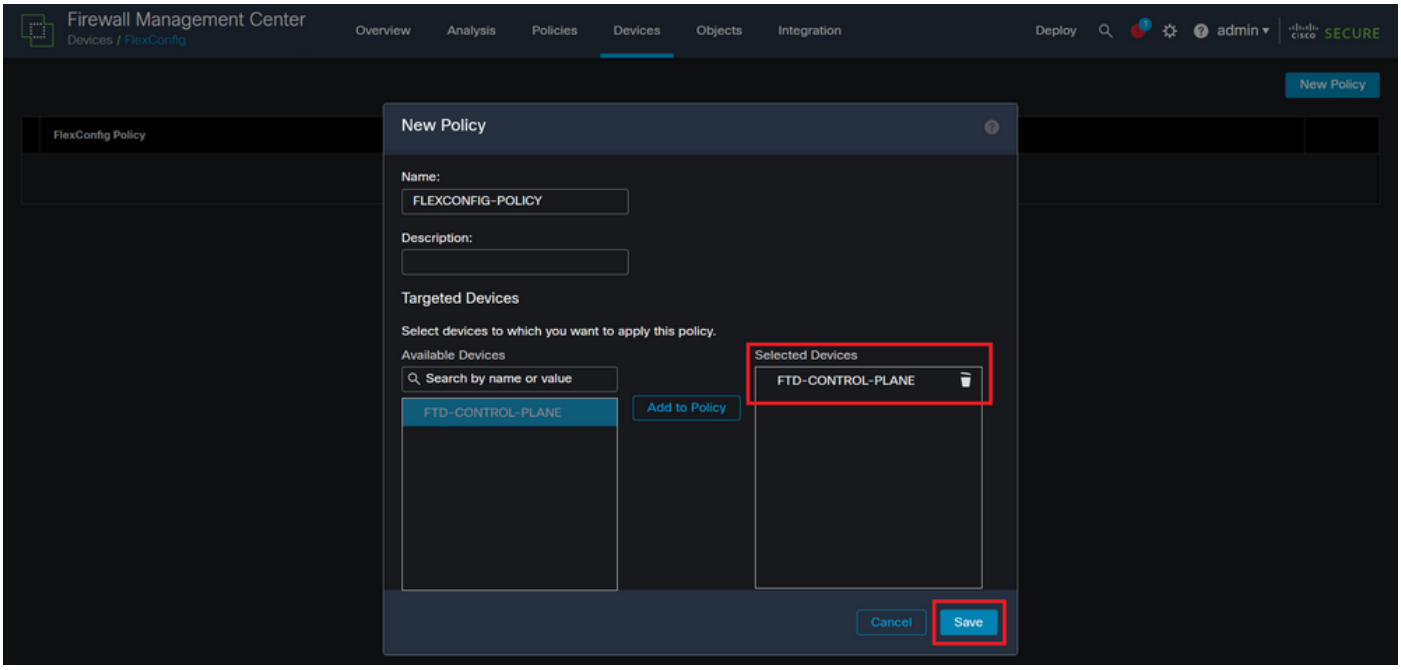

Imagen 17. Asignación de dispositivo de política FlexConfig

Paso 4.3. En el panel izquierdo, busque el objeto FlexConfig creado en el paso 3.2 y, a continuación, agréguelo a la directiva FlexConfig haciendo clic en la flecha derecha situada en el centro de la ventana. A continuación, haga clic en el botón Save.

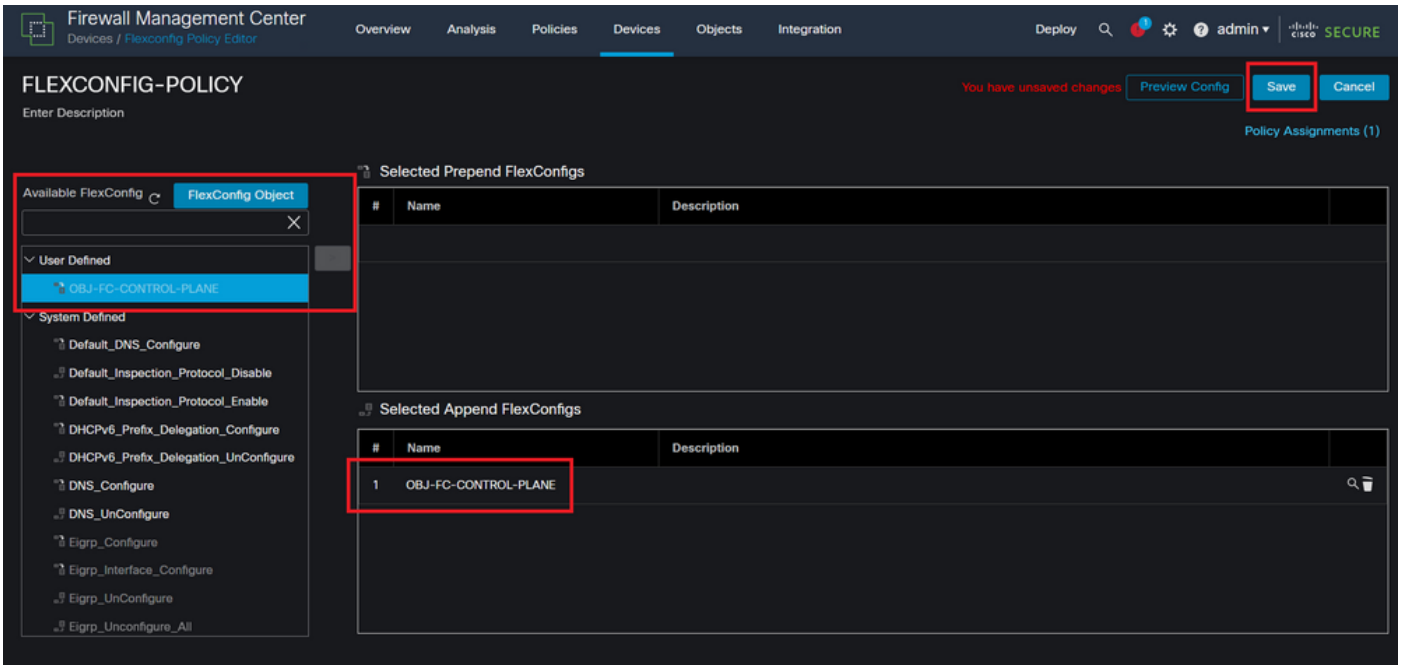

Imagen 18. Asignación de objeto de política FlexConfig

Paso 5. Continúe implementando el cambio de configuración en el FTD. Para ello, navegue hasta Deploy > Advanced Deploy.

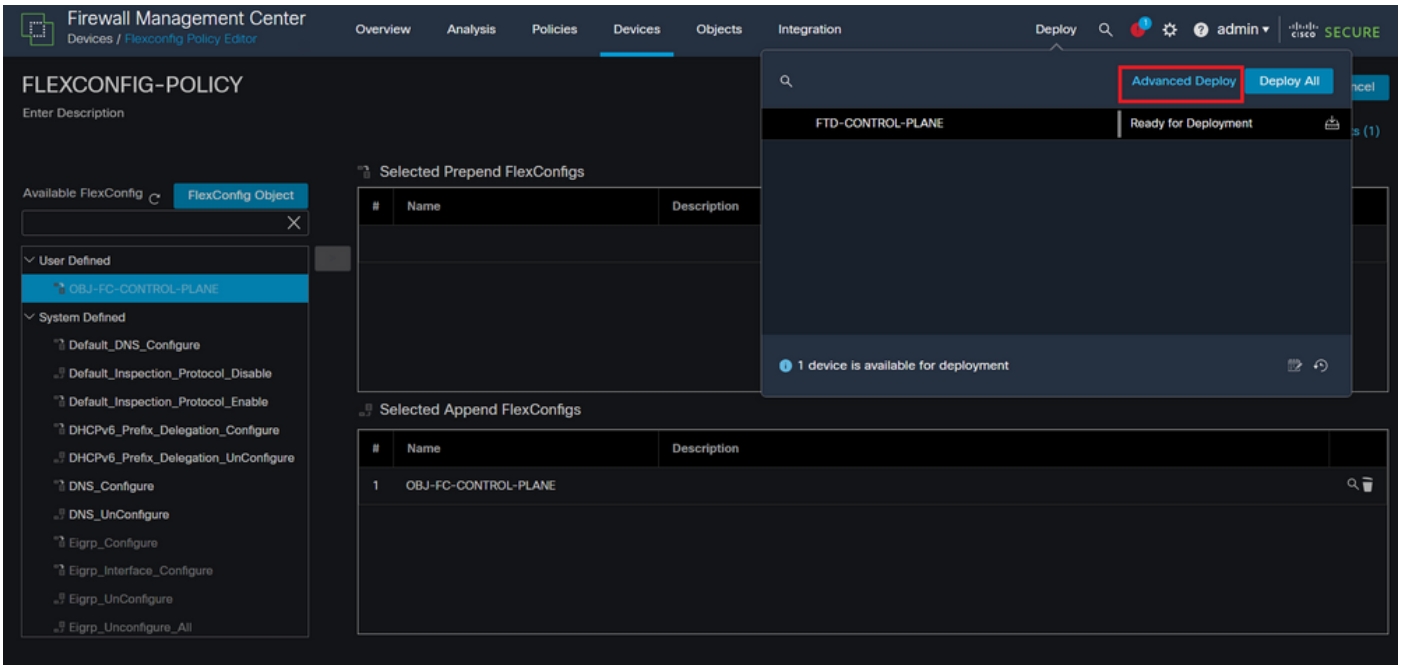

Imagen 19. Implementación avanzada de FTD

Paso 5.1. A continuación, seleccione el FTD al que desea aplicar la política FlexConfig. Si todo es correcto, haga clic en Deploy.

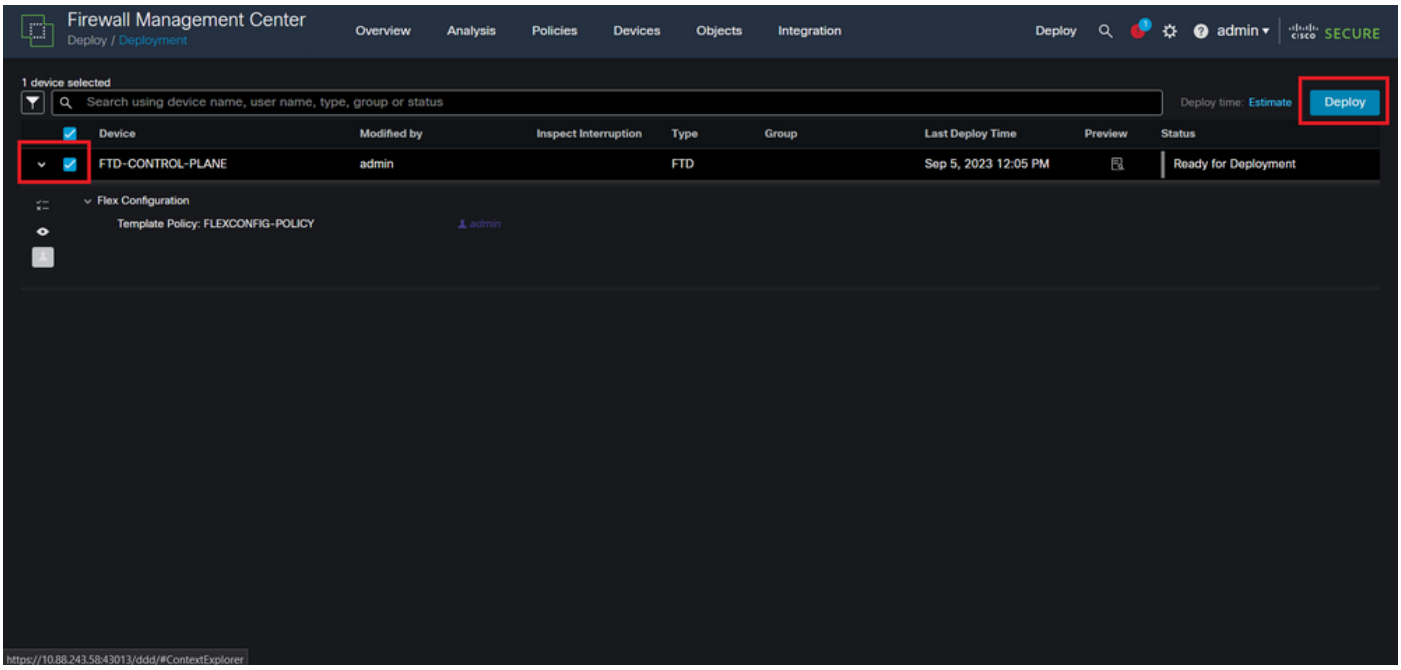

Imagen 20. Validación de implementación de FTD

Paso 5.2. Después de esto, se muestra una ventana de confirmación de implementación, agregue un comentario para realizar un seguimiento de la implementación y continúe con el proceso de implementación.

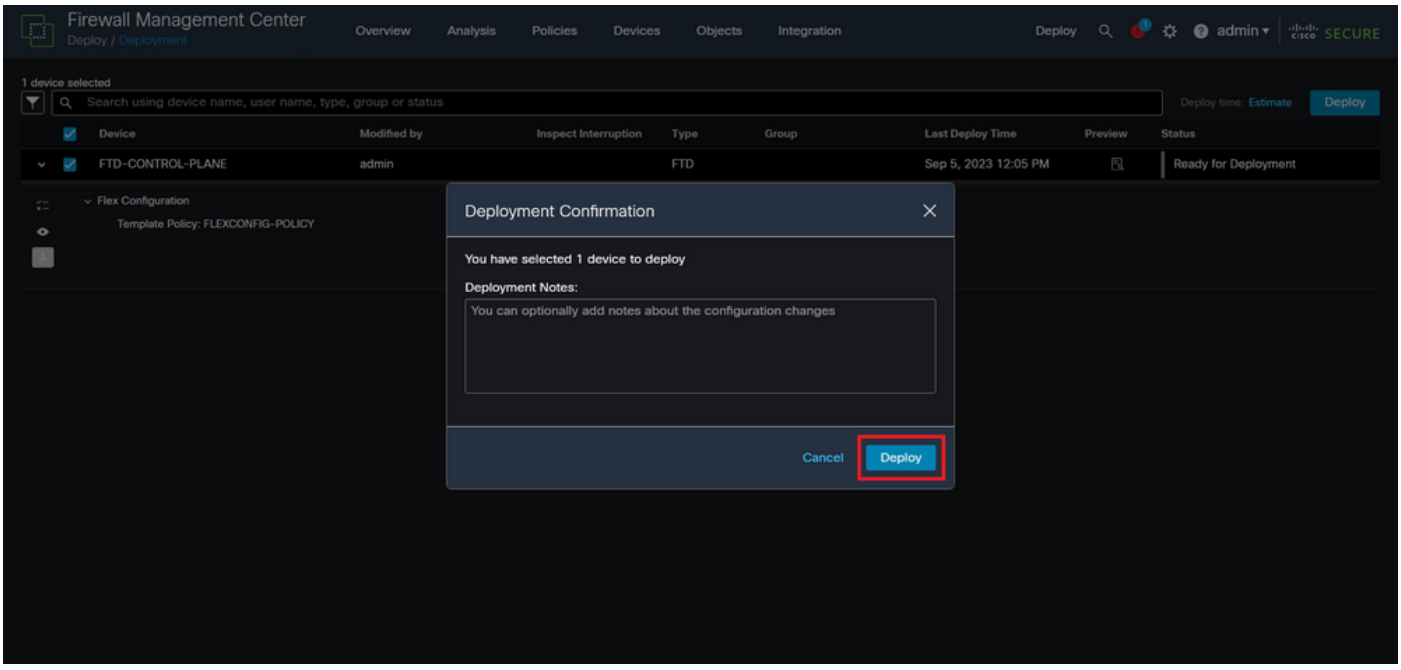

Imagen 21. Comentarios de implementación de FTD

Paso 5.3. Puede aparecer un mensaje de advertencia al implementar los cambios de FlexConfig. Haga clic en Deploy sólo si está completamente seguro de que la configuración de la directiva es correcta.

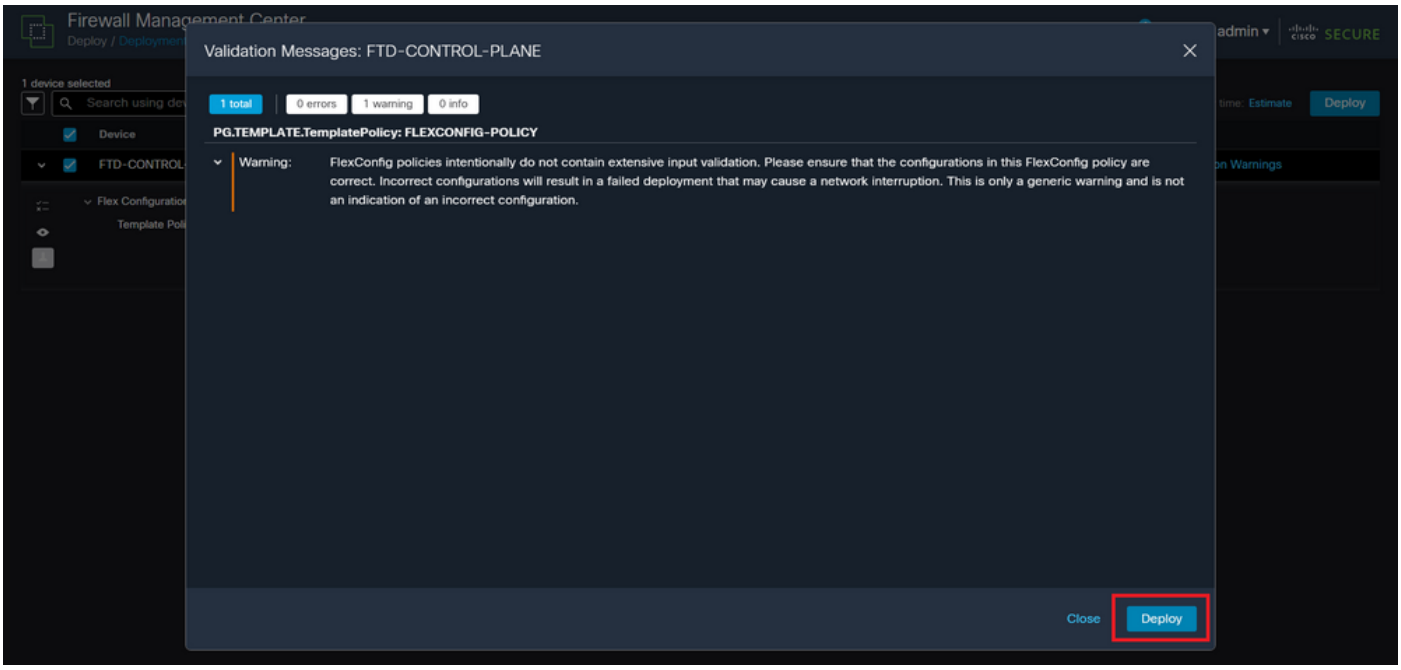

Imagen 2. Advertencia de Flexconfig de implementación de FTD

Paso 5.4. Confirme que la implementación de la política es correcta para el FTD.

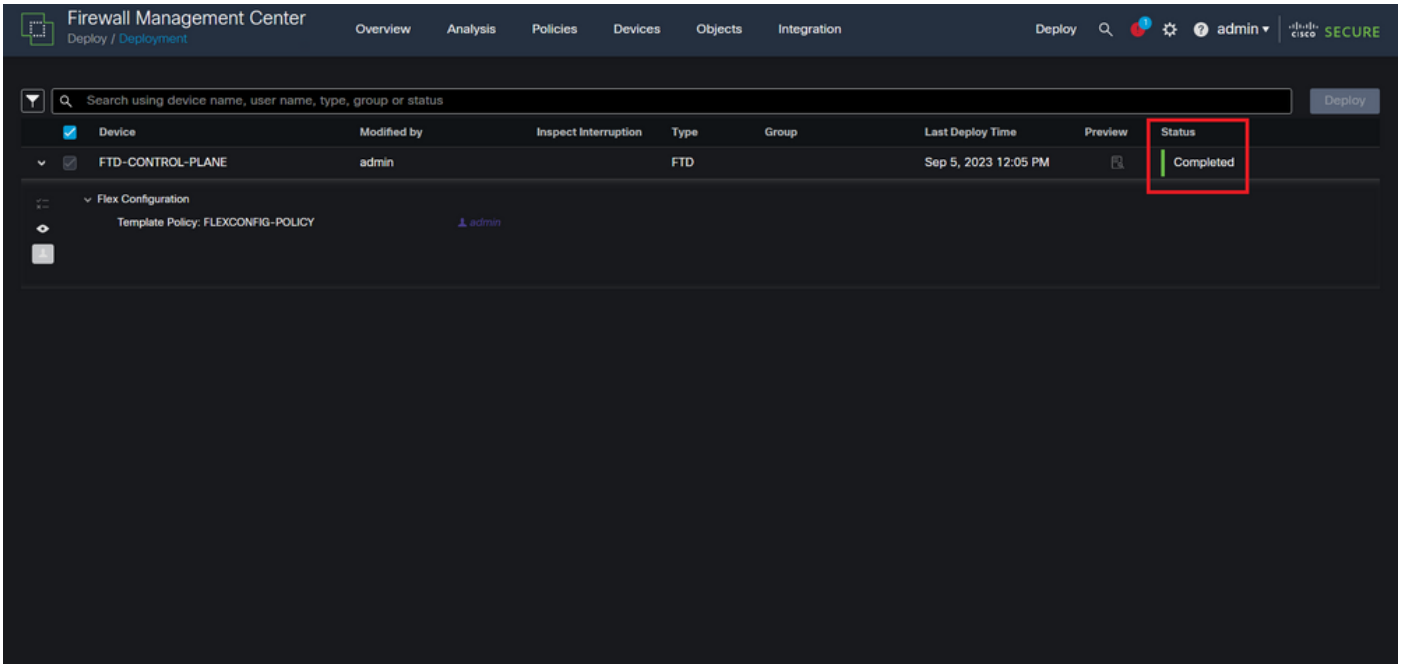

Imagen 23. Implementación de FTD correcta

Paso 6. Si crea una nueva ACL de plano de control para el FTD o si editó una existente que está en uso activamente, es importante resaltar que los cambios de configuración realizados no se aplican a las conexiones ya establecidas al FTD; por lo tanto, debe borrar manualmente los intentos de conexión activos al FTD. Para ello, conéctese a la CLI del FTD y borre las conexiones activas.

Para borrar la conexión activa para una dirección IP de host específica:

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

Para borrar las conexiones activas para una red de subred completa:

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

Para borrar las conexiones activas para un rango de direcciones IP:

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

Nota: Se recomienda utilizar la palabra clave 'all' al final del comando clear conn address para forzar la eliminación de los intentos de conexión de fuerza bruta VPN activos al firewall seguro, principalmente cuando la naturaleza del ataque de fuerza bruta VPN está lanzando una ráfaga de intentos de conexión constantes.

[VÍDEO] Configuración de una ACL de plano de control para FTD gestionada por FMC

Configuración de una ACL de plano de control para FTD gestionada por FDM

Este es el procedimiento que debe seguir en un FDM para configurar una ACL del plano de control para bloquear los ataques de fuerza bruta de VPN entrantes a la interfaz FTD externa:

Paso 1. Abra la GUI de FDM mediante HTTPS e inicie sesión con sus credenciales.

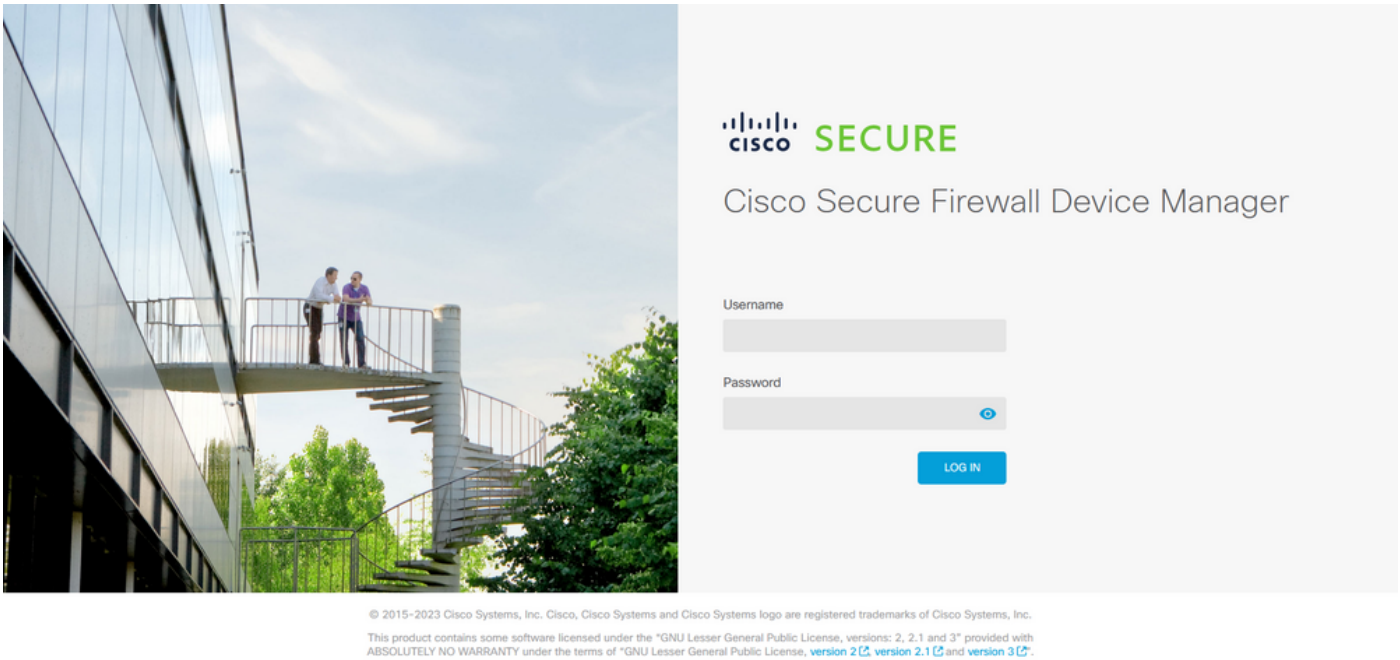

Imagen 24. Página de inicio de sesión de FDM

Paso 2. Debe crear una red de objetos. Para esto, navegue hasta Objetos:

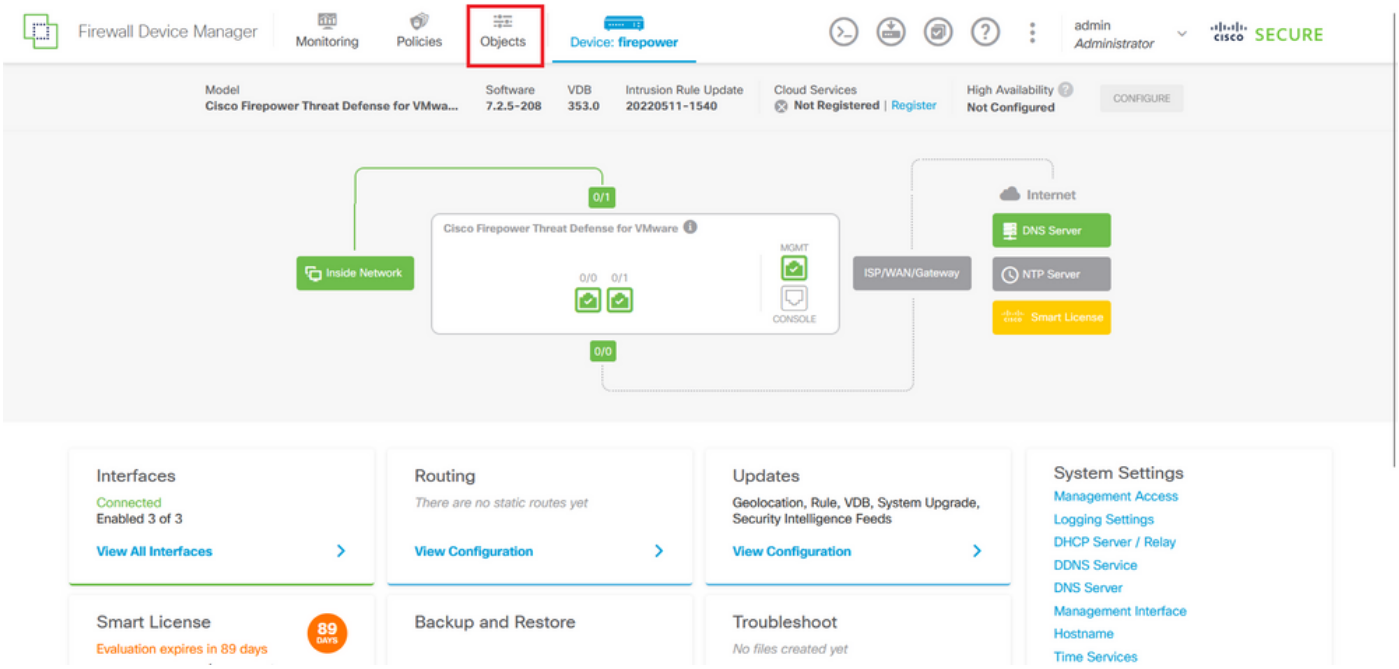

Imagen 25. Panel principal de FDM

Paso 2.1. En el panel izquierdo, seleccione Redes y, a continuación, haga clic en el botón '+' para crear un nuevo objeto de red.

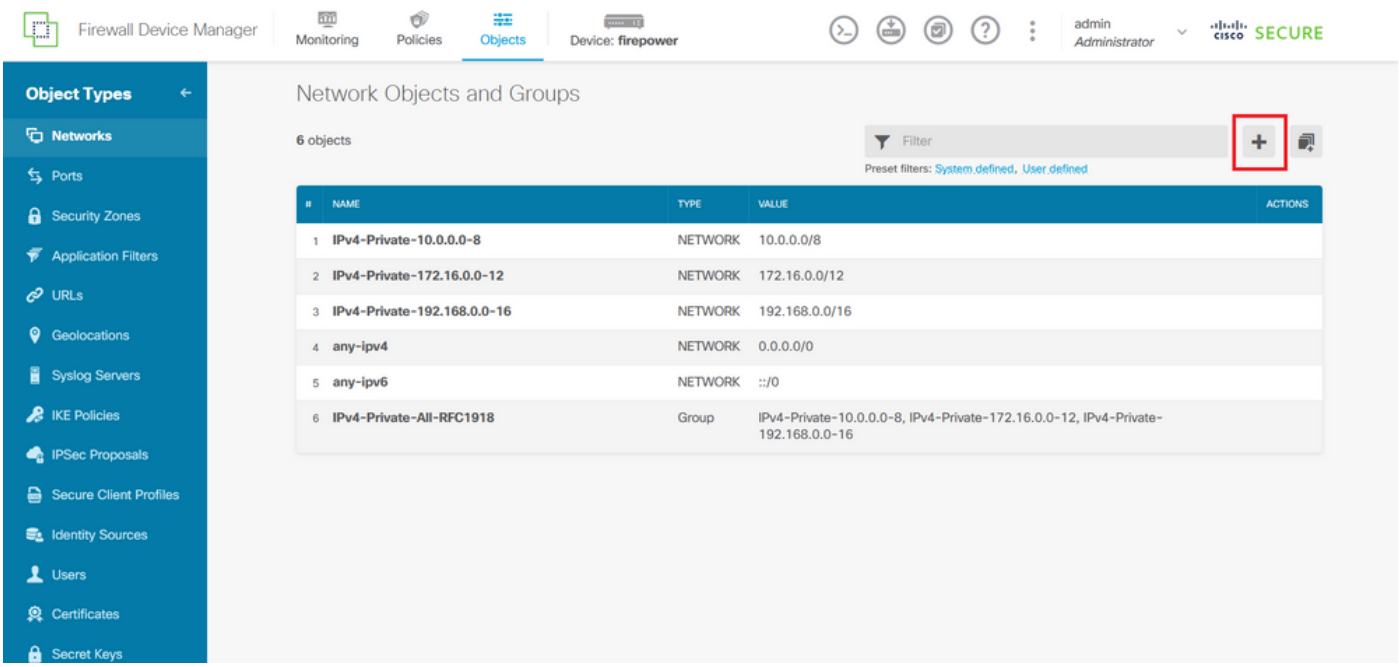

Imagen 26. Creación de objetos

Paso 2.2. Agregue un nombre para el objeto de red, seleccione el tipo de red para el objeto, agregue la dirección IP, la dirección de red o el rango de IP para que coincidan con el tráfico que debe denegarse al FTD. A continuación, haga clic en el botón Ok para completar la red de objetos.

- En este ejemplo, la red de objetos configurada está pensada para bloquear los ataques de fuerza bruta de VPN que provienen de la subred 192.168.1.0/24.

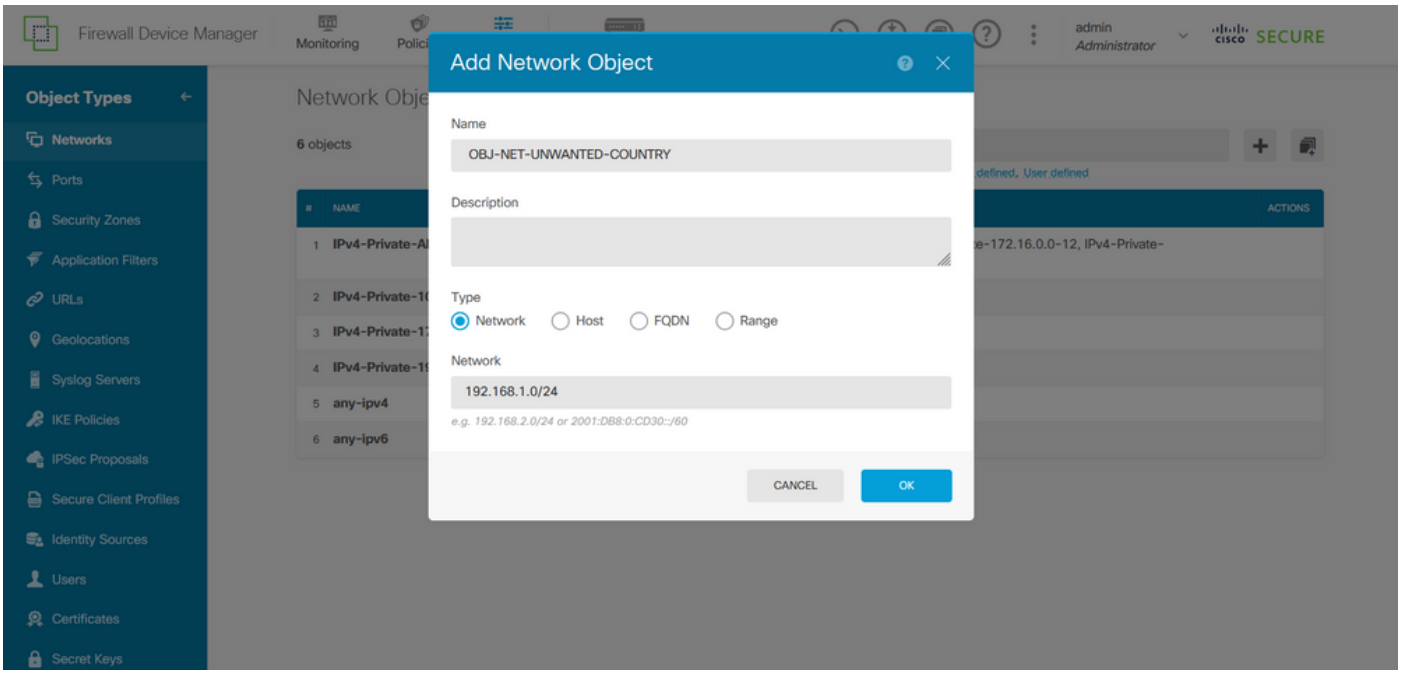

Imagen 27. Agregar objeto de red

Paso 3. A continuación, debe crear una ACL extendida; para ello, vaya a la pestaña Device en el menú superior.

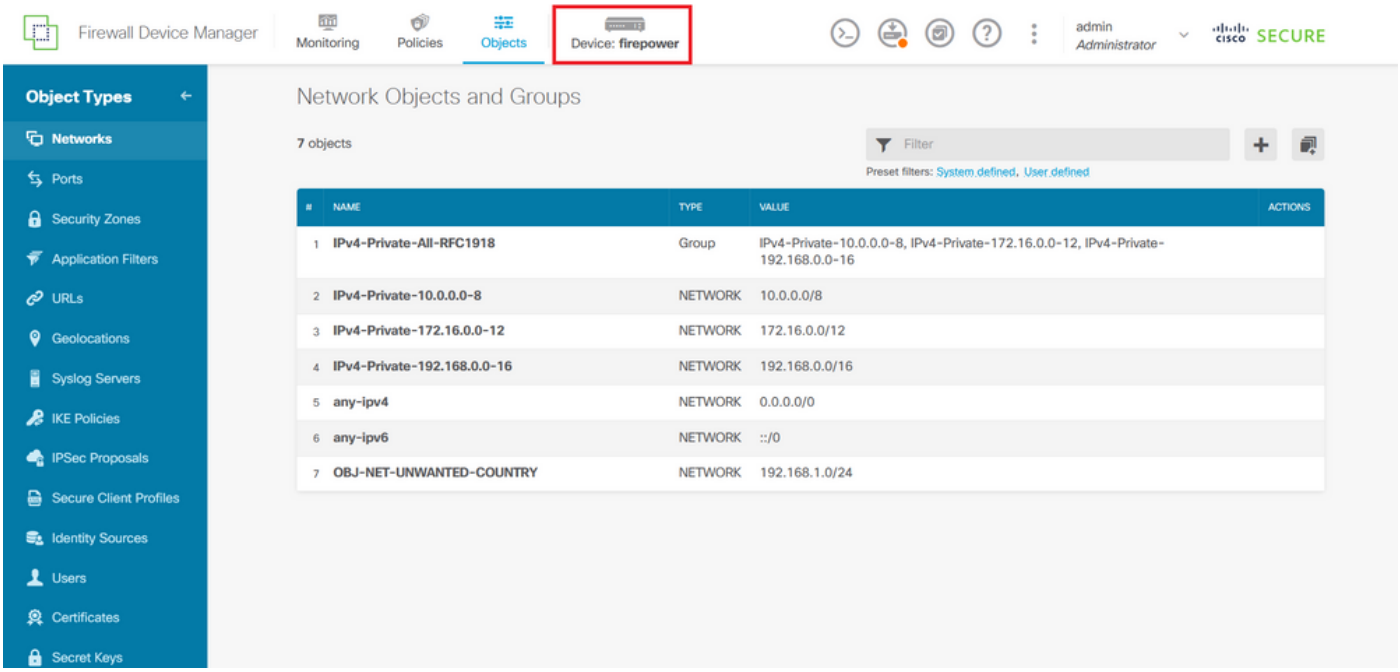

Imagen 28. Página Configuración del dispositivo

Paso 3.1. Desplácese hacia abajo y seleccione View Configuration en el cuadro Advanced Configuration (Configuración avanzada), como se muestra en la imagen.

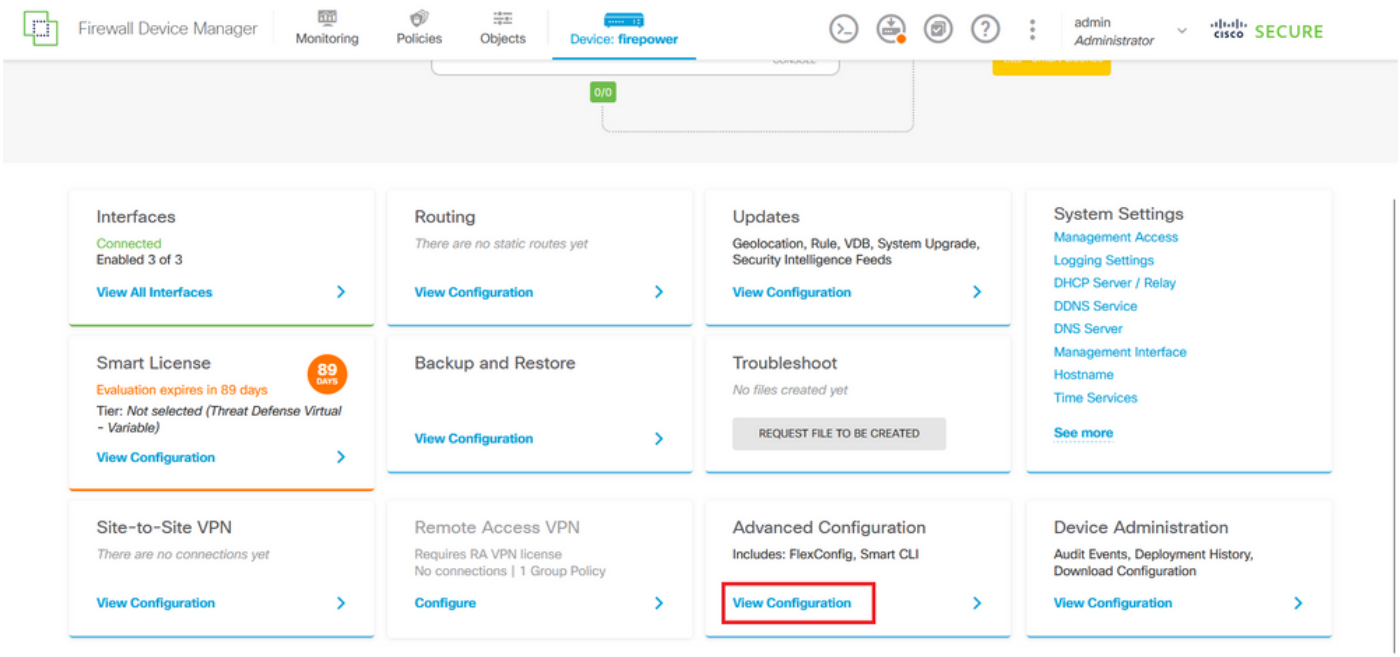

Imagen 29. Configuración avanzada de FDM

Paso 3.2. Luego, en el panel izquierdo, navegue hasta Smart CLI > Objects y haga clic en CREATE SMART CLI OBJECT.

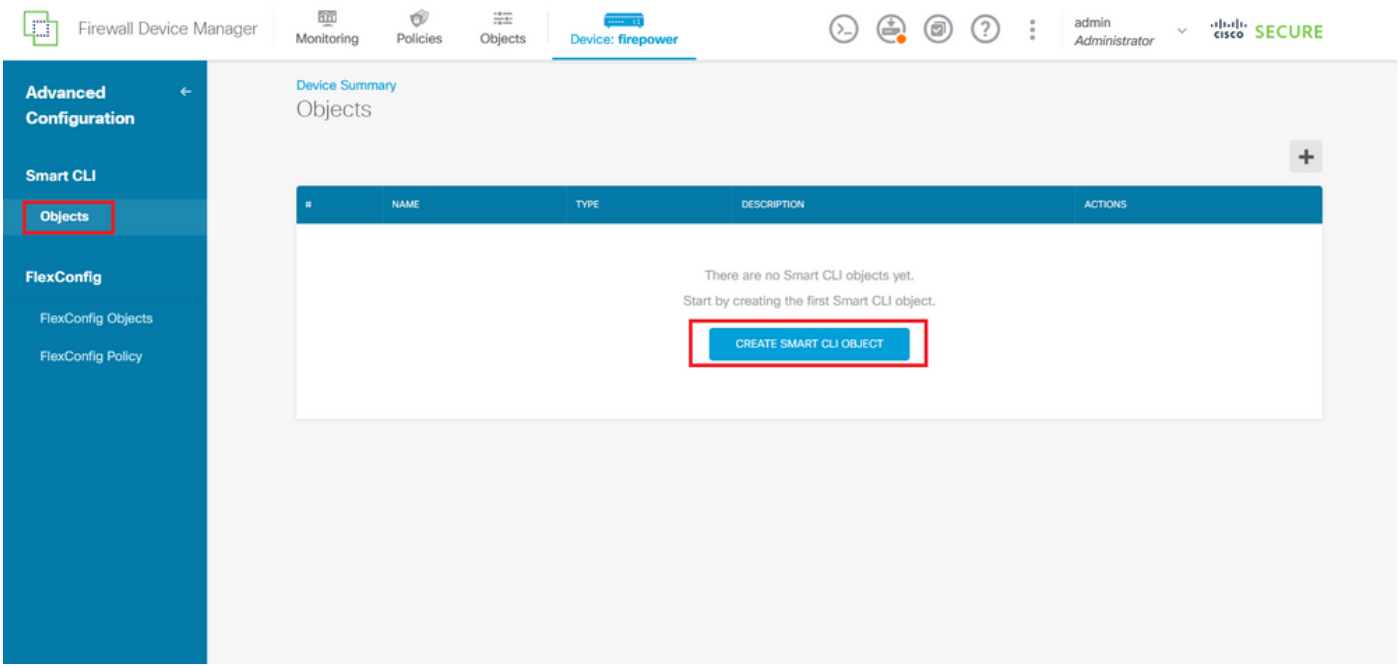

Imagen 30. Objetos CLI inteligentes

Paso 3.3. Agregue un nombre para la ACL extendida que desea crear, seleccione Extended Access List en el menú desplegable de la plantilla CLI, y configure las ACE requeridas mediante el objeto de red creado en el paso 2.2, luego haga clic en el botón OK para completar la ACL.

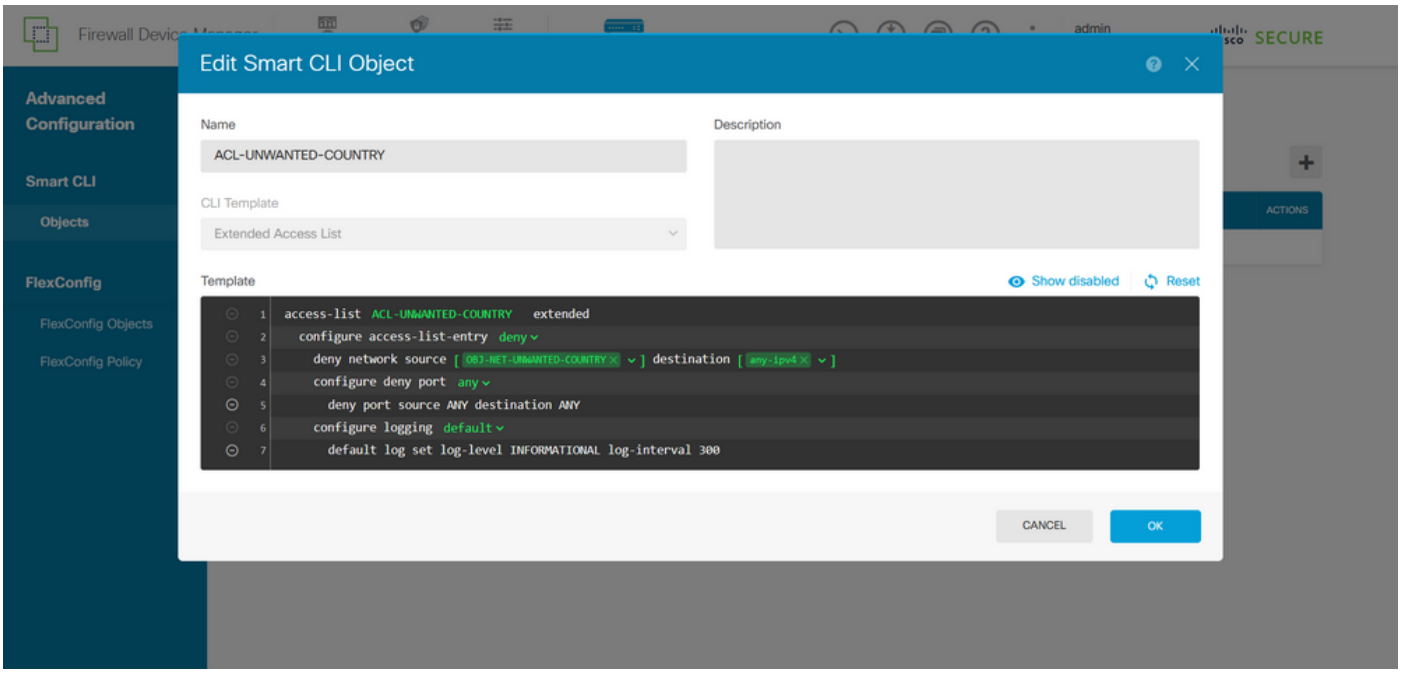

Imagen 31. Creación de ACL ampliada

Nota: Si necesita agregar más ACE para la ACL, puede hacerlo pasando el ratón sobre la izquierda de la ACE actual; entonces no aparecen tres puntos en los que se puede hacer clic. Haga clic en ellos y seleccione Duplicar para agregar más ACE.

Paso 4. A continuación, debe crear un objeto FlexConfig; para ello, vaya al panel izquierdo, seleccione FlexConfig > Objetos FlexConfig y haga clic en CREATE FLEXCONFIG OBJECT.

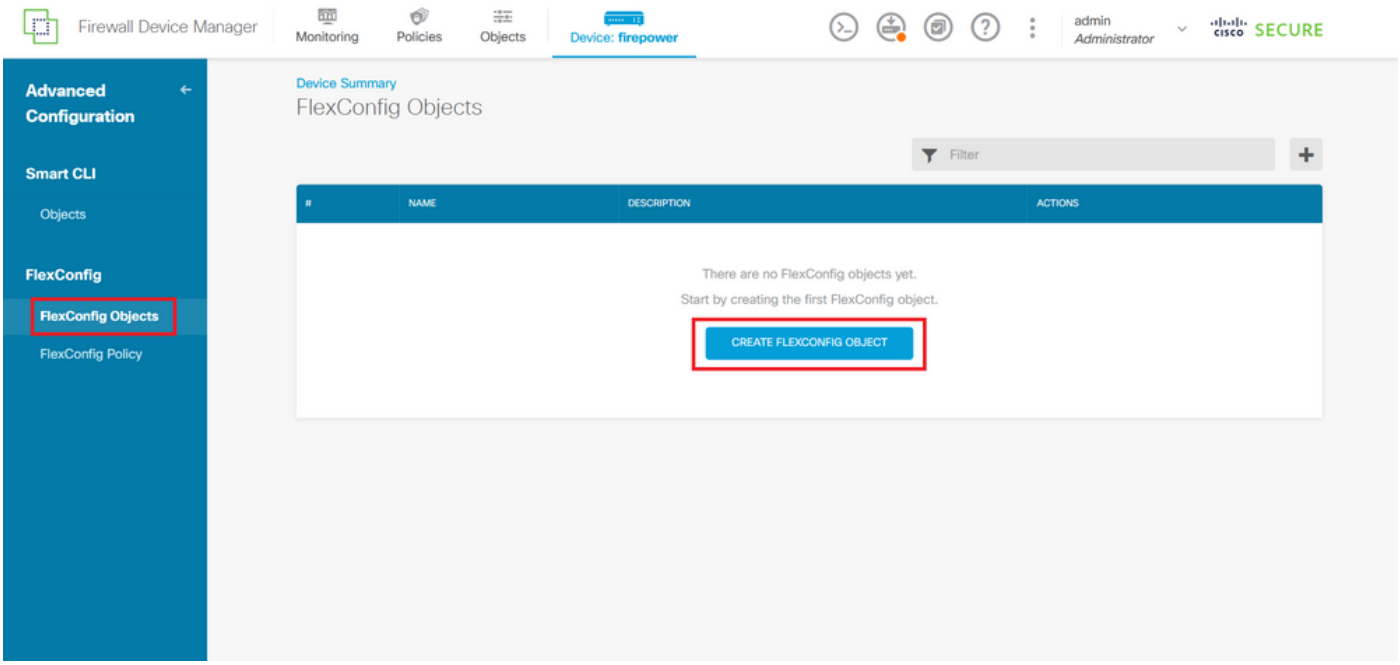

Imagen 32. Objetos FlexConfig

Paso 4.1. Agregue un nombre para el objeto FlexConfig para crear y configurar la ACL del plano de control como entrante para la interfaz externa, como se muestra en la imagen.

Sintaxis de la línea de comandos:

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

Esto se traduce en el siguiente ejemplo de comando, que utiliza la ACL extendida creada en el Paso 3.3 'ACL-UNWANTED-COUNTRY':

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

Así es como se puede configurar en la ventana de objetos de FlexConfig. Después de esto, seleccione el botón Aceptar para completar el objeto de FlexConfig.

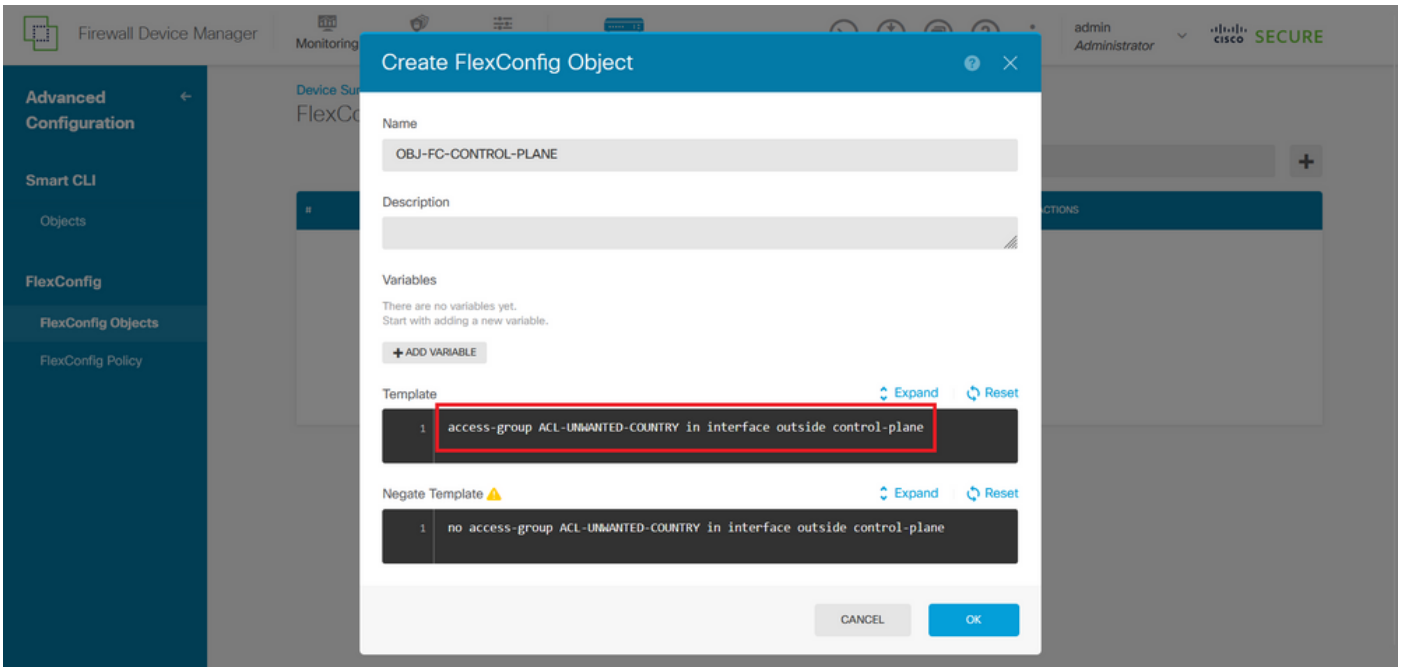

Imagen 3. Creación de objetos FlexConfig

Nota: Se recomienda encarecidamente configurar la ACL del plano de control sólo para las interfaces que reciben sesiones VPN de acceso remoto entrantes en el firewall seguro, como la interfaz externa.

Paso 5. Proceda a crear una política FlexConfig; para ello, navegue hasta Flexconfig > Política FlexConfig, haga clic en el botón '+' y seleccione el objeto FlexConfig que se creó en el paso 4.1.

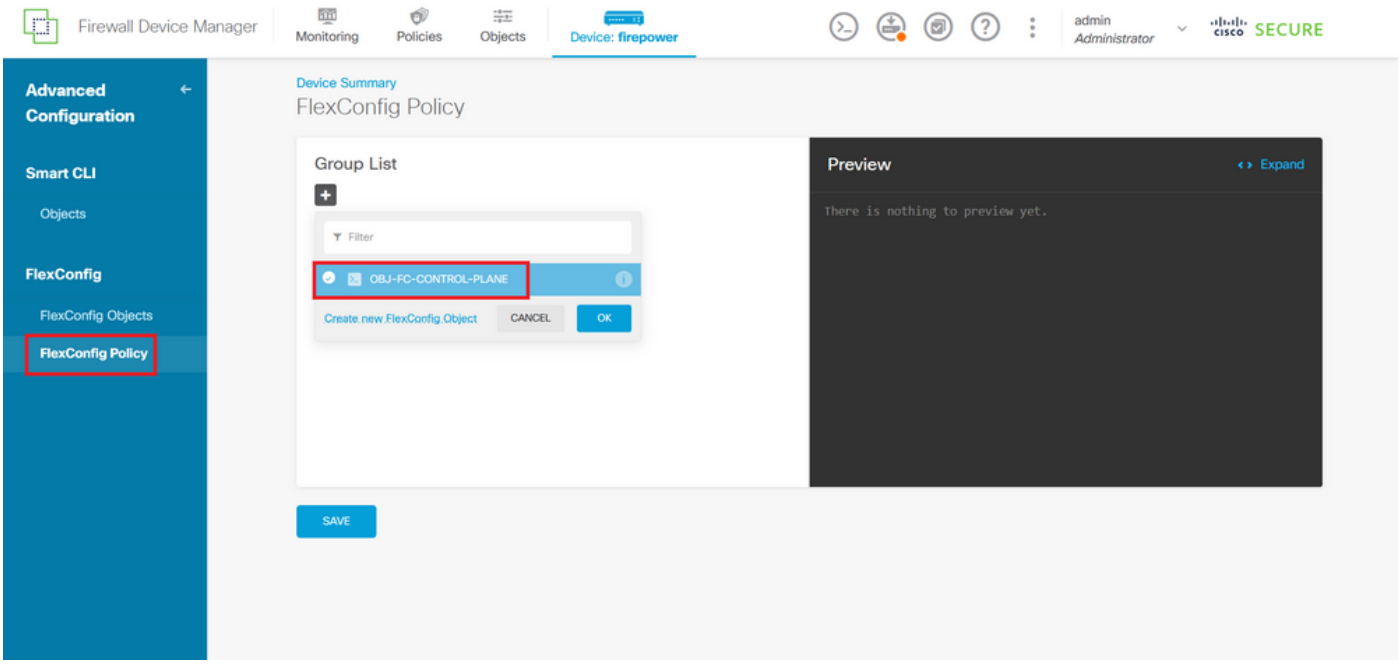

Imagen 34. Política FlexConfig

Paso 5.1. Valide que la vista previa de FlexConfig muestre la configuración correcta para la ACL del plano de control creada y haga clic en el botón Save.

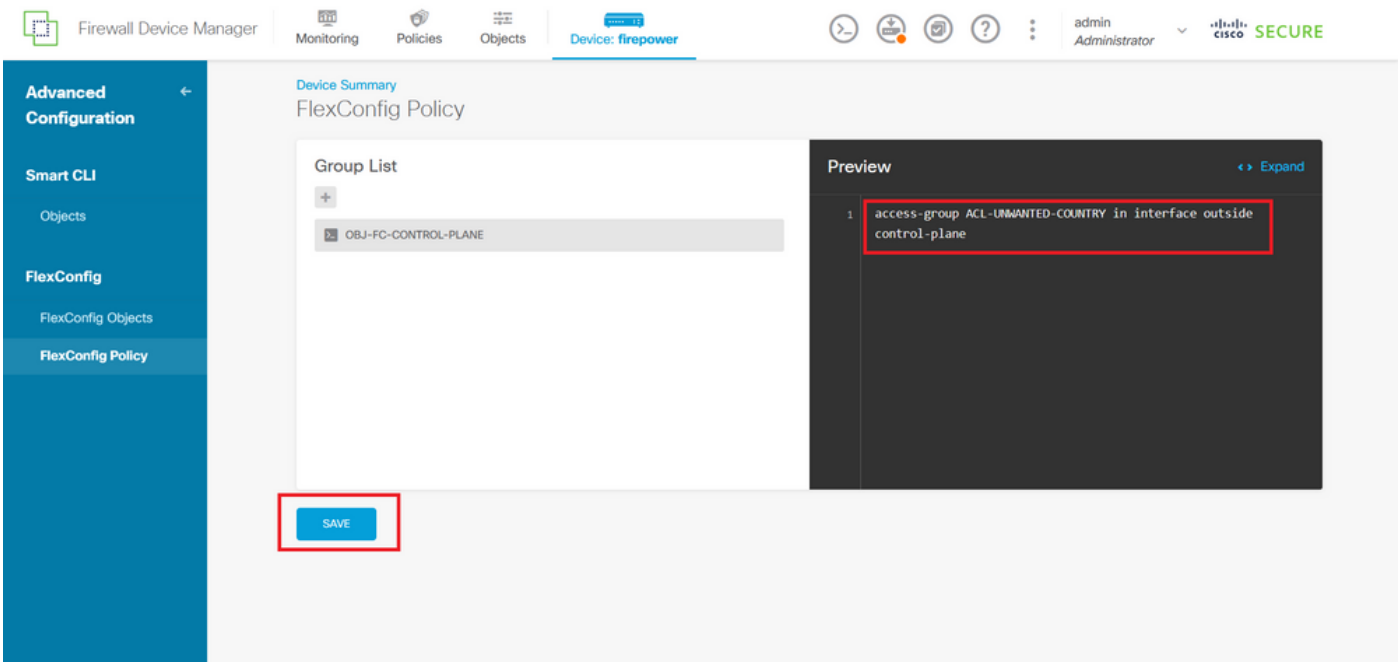

Imagen 35. Vista previa de política FlexConfig

Paso 6. Implemente los cambios de configuración en el FTD que desea proteger contra los ataques de fuerza bruta VPN; para ello, haga clic en el botón Deployment en el menú superior, valide que los cambios de configuración para implementar son correctos y, a continuación, haga clic en DEPLOY NOW.

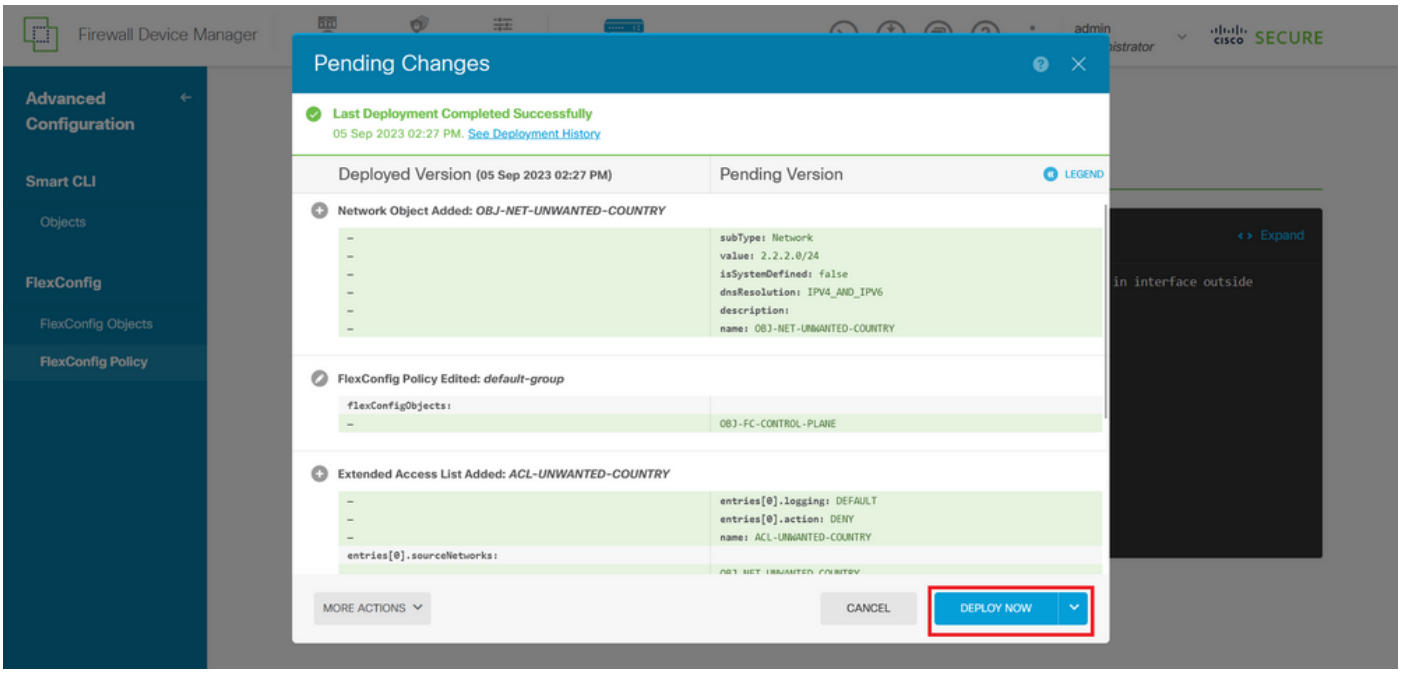

Imagen 36. Implementación pendiente

Paso 6.1. Valide que la implementación de la política se realice correctamente.

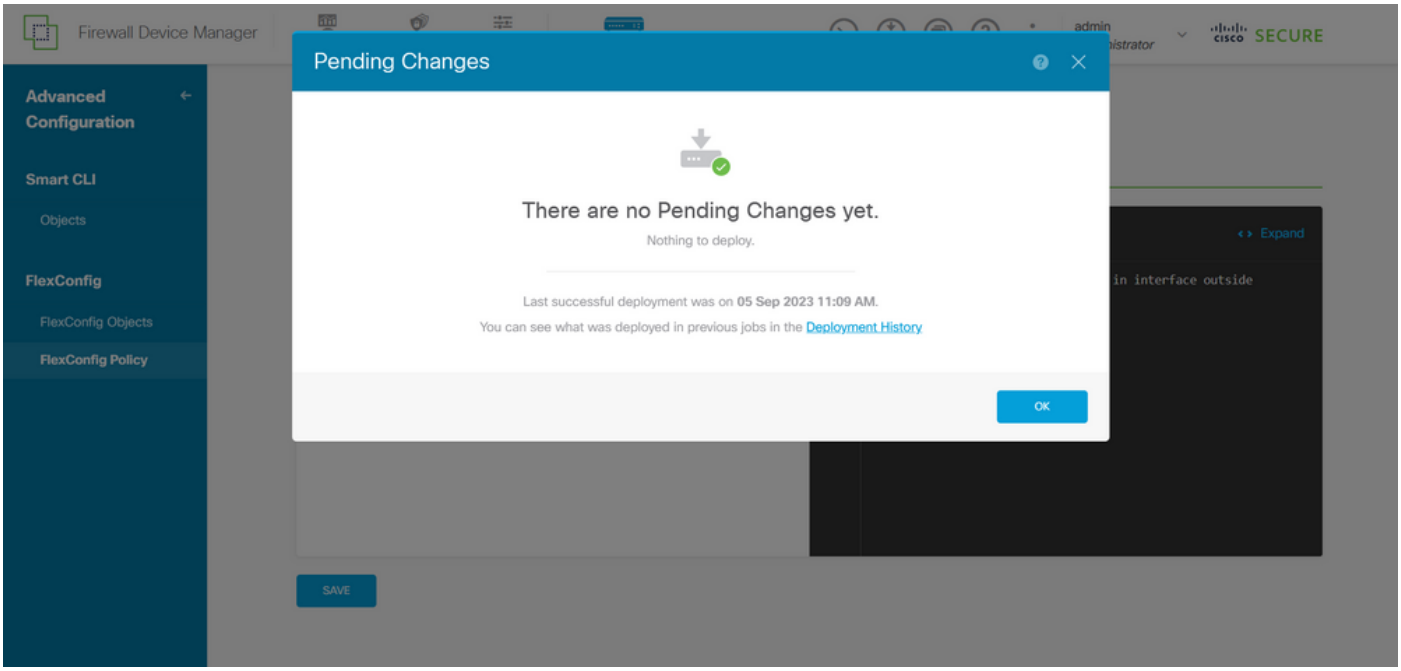

Imagen 37. Implementación correcta

Paso 7. Si crea una nueva ACL de plano de control para el FTD o si editó una existente que está en uso activamente, es importante resaltar que los cambios de configuración realizados no se aplican a las conexiones ya establecidas al FTD; por lo tanto, debe borrar manualmente los intentos de conexión activos al FTD. Para ello, conéctese a la CLI del FTD y borre las conexiones activas.

Para borrar la conexión activa para una dirección IP de host específica:

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

Para borrar las conexiones activas para una red de subred completa:

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

Para borrar las conexiones activas para un rango de direcciones IP:

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

Nota: Se recomienda utilizar la palabra clave 'all' al final del comando clear conn address para forzar la eliminación de los intentos de conexión de fuerza bruta VPN activos al firewall seguro, principalmente cuando la naturaleza del ataque de fuerza bruta VPN está lanzando una ráfaga de intentos de conexión constantes.

Configuración de una ACL de plano de control para ASA mediante CLI

Este es el procedimiento que debe seguir en una CLI ASA para configurar una ACL del plano de control para bloquear los ataques de fuerza bruta de VPN entrante a la interfaz externa:

Paso 1. Inicie sesión en el firewall ASA seguro a través de CLI y obtenga acceso al 'configure terminal'.

```
asa# configure terminal
```

Paso 2. Utilice el siguiente comando para configurar una ACL extendida para bloquear una dirección IP de host o una dirección de red para el tráfico que debe bloquearse en el ASA.

- En este ejemplo, crea una nueva ACL llamada 'ACL-UNWANTED-COUNTRY' y la entrada ACE configurada bloquea los ataques de fuerza bruta VPN que provienen de la subred 192.168.1.0/24.

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

Paso 3. Utilice el siguiente comando access-group para configurar la ACL 'ACL-UNWANTED-

COUNTRY' como ACL de plano de control para la interfaz externa de ASA.

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

Nota: Se recomienda encarecidamente configurar la ACL del plano de control sólo para las interfaces que reciben sesiones VPN de acceso remoto entrantes en el firewall seguro, como la interfaz externa.

Paso 4. Si crea una nueva ACL del plano de control o si editó una existente que está en uso activamente, es importante resaltar que los cambios de configuración realizados no se aplican a las conexiones ya establecidas con el ASA, por lo tanto, necesita borrar manualmente los intentos de conexión activos con el ASA. Para ello, borre las conexiones activas.

Para borrar la conexión activa para una dirección IP de host específica:

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

Para borrar las conexiones activas para una red de subred completa:

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

Para borrar las conexiones activas para un rango de direcciones IP:

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

Nota: Se recomienda utilizar la palabra clave 'all' al final del comando clear conn address para forzar la eliminación de los intentos de conexión de fuerza bruta VPN activos al firewall seguro, principalmente cuando la naturaleza del ataque de fuerza bruta VPN está lanzando una ráfaga de intentos de conexión constantes.

Configuración alternativa para bloquear los ataques de firewall seguro mediante el comando 'shun'

En caso de que exista una opción inmediata para bloquear los ataques al firewall seguro, puede utilizar el comando 'shun'. El comando hunle permite bloquear las conexiones de un host atacante. Aquí tiene más detalles sobre este comando shun:

- Una vez que rechaza una dirección IP, todas las conexiones futuras de la dirección IP de origen se descartan y se registran hasta que la función de bloqueo se elimina manualmente.
- La función de bloqueo del comando hunse aplica independientemente de si una conexión con la dirección de host especificada está actualmente activa.
- Si especifica la dirección de destino, los puertos de origen y de destino y el protocolo, descarta la conexión coincidente y envía una señal de rechazo a todas las conexiones futuras desde la dirección IP de origen; todas las conexiones futuras se rechazan, no sólo las que coincidan con estos parámetros de conexión específicos.
- Sólo puede tener uncomando hunpor dirección IP de origen.
- Dado que el comando hunse utiliza para bloquear ataques dinámicamente, no se muestra en la configuración del dispositivo de defensa contra amenazas.
- Siempre que se elimina una configuración de interfaz, también se eliminan todos los shuns conectados a esa interfaz.
- Sintaxis del comando Shun:

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

- Para inhabilitar un shun, utilice la forma no de este comando:

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

Para rechazar una dirección IP de host, proceda como se indica a continuación para el firewall seguro. En este ejemplo, el comando 'shun' se utiliza para bloquear los ataques de fuerza bruta de VPN que provienen de la dirección IP de origen 192.168.1.10.

Ejemplo de configuración de FTD.

Paso 1. Inicie sesión en el FTD mediante CLI y aplique el comando shun.

```
<#root>

>

 shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf


Shun 192.168.1.10 successful
```

Paso 2. Puede utilizar los comandos show para confirmar las direcciones IP rechazadas en el FTD y para monitorear los recuentos de aciertos rechazados por dirección 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)
```

Ejemplo de configuración para ASA

Paso 1. Inicie sesión en ASA a través de CLI y aplique el comando shun.

<#root>

```
asa#

 shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf


Shun 192.168.1.10 successful
```

Paso 2. Puede utilizar los comandos show para confirmar las direcciones IP rechazadas en el ASA y para monitorear los recuentos de aciertos rechazados por dirección 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)
```

Nota: Para obtener más información sobre el comando secure firewall shun, consulte la Referencia de Comandos de Cisco Secure Firewall Threat Defence

Verificación

Para confirmar que la configuración de ACL del plano de control está en su lugar para el firewall seguro, continúe:

Paso 1. Inicie sesión en el firewall seguro a través de CLI y ejecute los siguientes comandos para confirmar que se ha aplicado la configuración de ACL del plano de control.

Ejemplo de salida del FTD gestionado por el CSP:

```
<#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
```

Ejemplo de salida del FTD gestionado por 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
```

Ejemplo de salida para 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
```

Paso 2. Para confirmar que la ACL del plano de control está bloqueando el tráfico requerido, utilice el comando packet-tracer para simular una conexión TCP 443 entrante con la interfaz externa del firewall seguro, luego utilice el comando show access-list <acl-name> el conteo de aciertos de la ACL puede incrementarse cada vez que la ACL del plano de control bloquea una conexión VPN de fuerza bruta con el firewall seguro:

- En este ejemplo, el comando packet-tracer simula una conexión TCP 443 entrante originada en el host 192.168.1.10 y destinada a la dirección IP externa de nuestro firewall seguro. El resultado del 'packet-tracer' confirma que el tráfico se está descartando y el resultado del 'show access-list' muestra los incrementos de conteo de aciertos para nuestra ACL del plano de control en su lugar:

Ejemplo de salida 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

Ejemplo de salida para 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
```

Nota: Si se implementa una solución RAVPN como Cisco Secure Client VPN en el firewall seguro, se podría realizar un intento real de conexión al firewall seguro para confirmar que la ACL del plano de control funciona como se esperaba para bloquear el tráfico requerido.

Errores relacionados

- ENH | Conexiones de AnyConnect Client basadas en geolocalización: ID de bug de Cisco CSCvs65322
- DOC: La búsqueda de grupos de objetos de ASA/FTD no admite ACL del plano de control: ID de bug de Cisco CSCwi58818

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).