Configuración de la detección de amenazas para los servicios VPN de acceso remoto en el administrador de dispositivos Cisco Firepower

Contenido

Introducción

Este documento describe el proceso de configuración de la detección de amenazas para los servicios VPN de acceso remoto en Cisco Firepower Device Manager (FDM).

Prerequisites

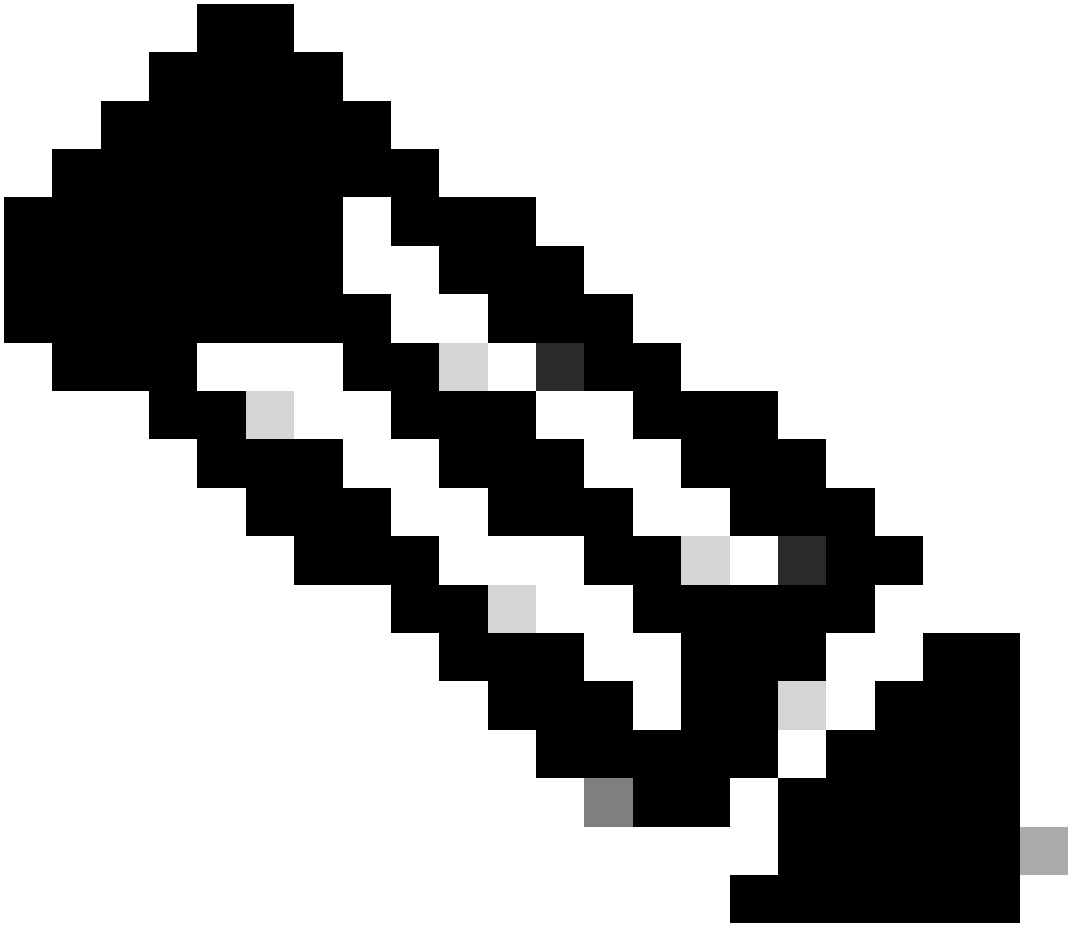
Cisco recomienda que conozca estos temas:

- Cisco Secure Firewall Threat Defence (FTD).
- Administrador de dispositivos Cisco Firepower (FDM).
- VPN de acceso remoto (RAVPN) en FTD.

Requirements

Estas funciones de detección de amenazas son compatibles con las versiones de Cisco Secure Firewall Threat Defence que se enumeran a continuación:

- 7.0 version train-> soportado desde7.0.6.3 y versiones más recientes dentro de este tren específico.
- 7.2 version train-> soportado desde7.2.9 y versiones más recientes dentro de este tren específico.
- 7.4 version train-> soportado desde7.4.2.1 y versiones más recientes dentro de este tren específico.
- 7.6 version train-> soportado desde7.6.0 y cualquier versión más reciente.



Nota: Actualmente, estas funciones no son compatibles con las versiones 7.1 o 7.3.

Componentes Utilizados

La información descrita en este documento se basa en estas versiones de hardware y software:

- Cisco Secure Firewall Threat Defence Virtual versión 7.4.2.1

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.

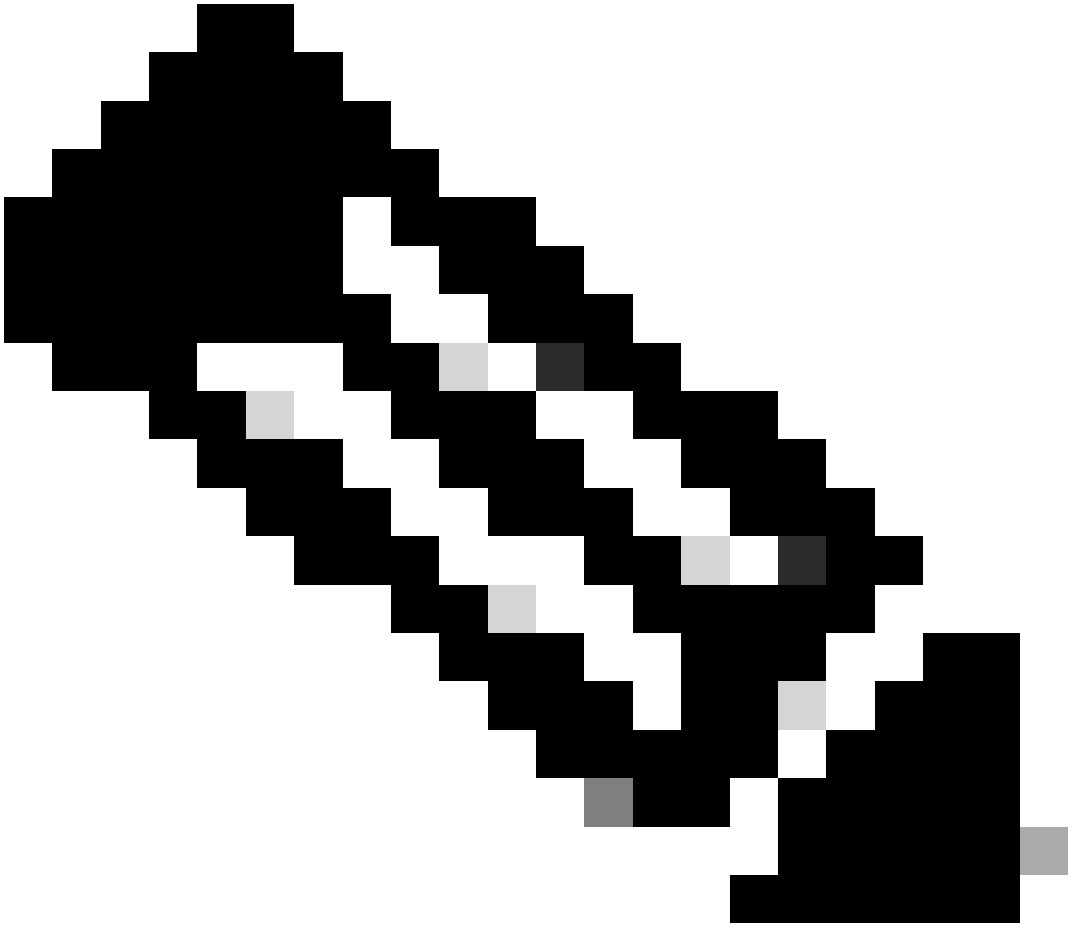
Antecedentes

Las funciones de detección de amenazas para los servicios VPN de acceso remoto ayudan a

evitar ataques DoS (del inglés Denial of Service, denegación de servicio) desde direcciones IPv4 bloqueando automáticamente el host (dirección IP) que excede los umbrales configurados para evitar más intentos hasta que elimine manualmente el rechazo de la dirección IP. Hay servicios independientes disponibles para los siguientes tipos de ataques:

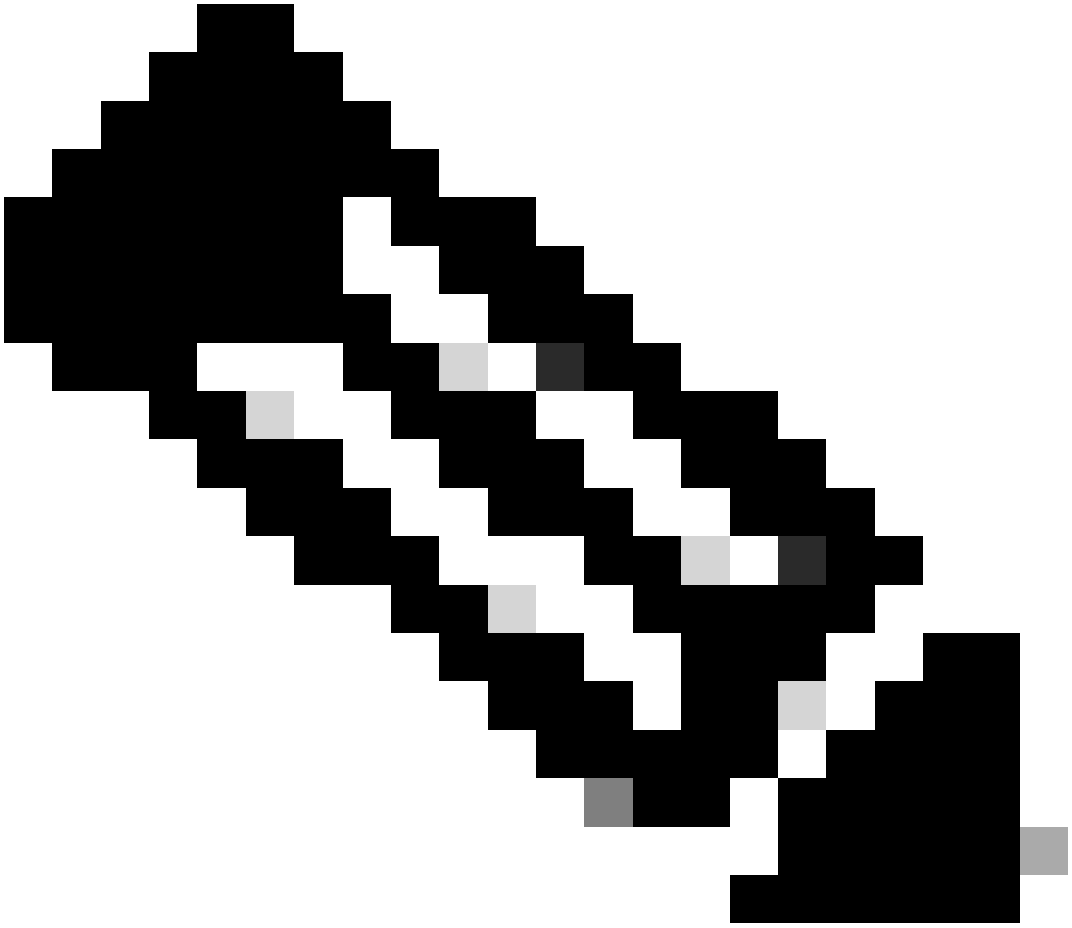
- Intentos de autenticación fallidos repetidos: Intentos de autenticación fallidos repetidos para los servicios VPN de acceso remoto (ataques de escaneo de nombre de usuario/contraseña por fuerza bruta).
- Ataques de iniciación de cliente: lugar en el que el atacante inicia pero no completa los intentos de conexión a una cabecera VPN de acceso remoto varias veces desde un único host.
- Intentos de conexión a servicios VPN de acceso remoto no válidos: cuando los atacantes intentan conectarse a grupos de túnel integrados específicos destinados únicamente al funcionamiento interno del dispositivo. Los terminales legítimos no intentan conectarse a estos grupos de túnel.

Estos ataques, incluso cuando no consiguen obtener acceso, pueden consumir recursos informáticos e impedir que usuarios válidos se conecten a los servicios VPN de acceso remoto. Cuando habilita estos servicios, el firewall rechaza automáticamente el host (dirección IP) que excede los umbrales configurados. Esto evita más intentos hasta que elimine manualmente la omisión de la dirección IP.



Nota: de forma predeterminada, todos los servicios de detección de amenazas para VPN de acceso remoto están desactivados.

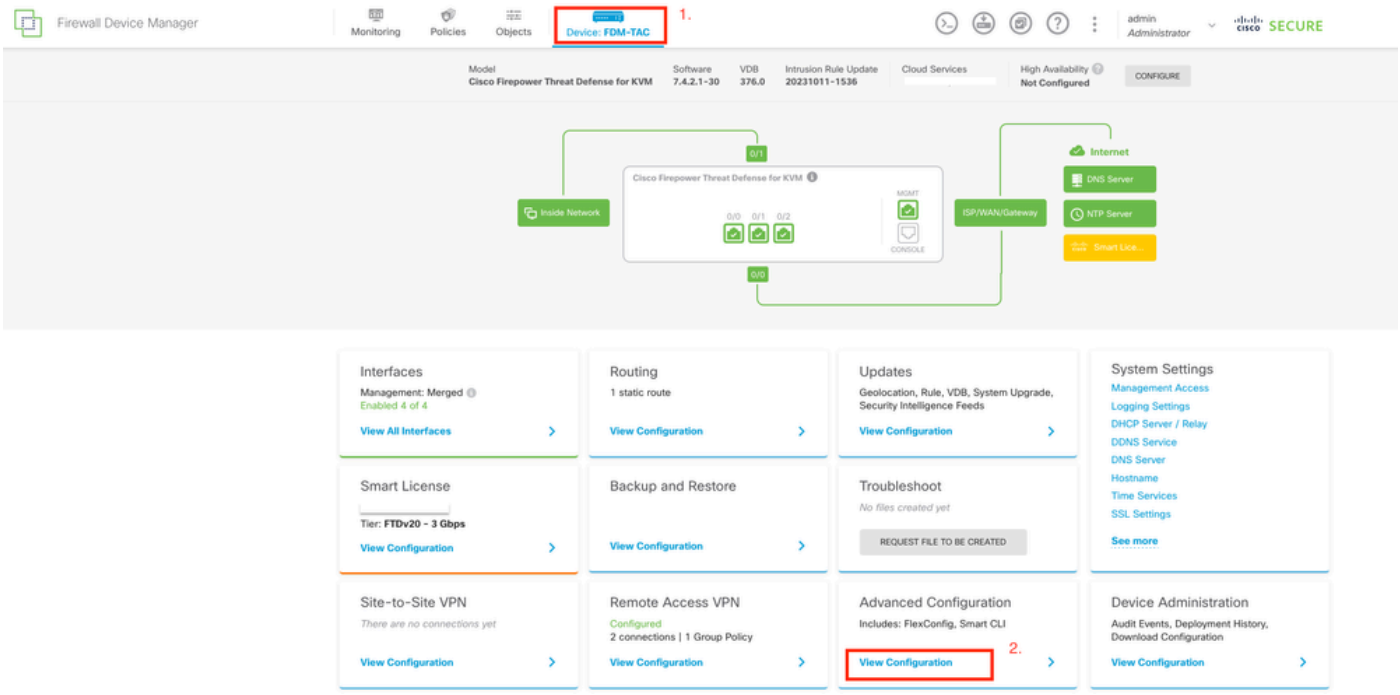
Configurar



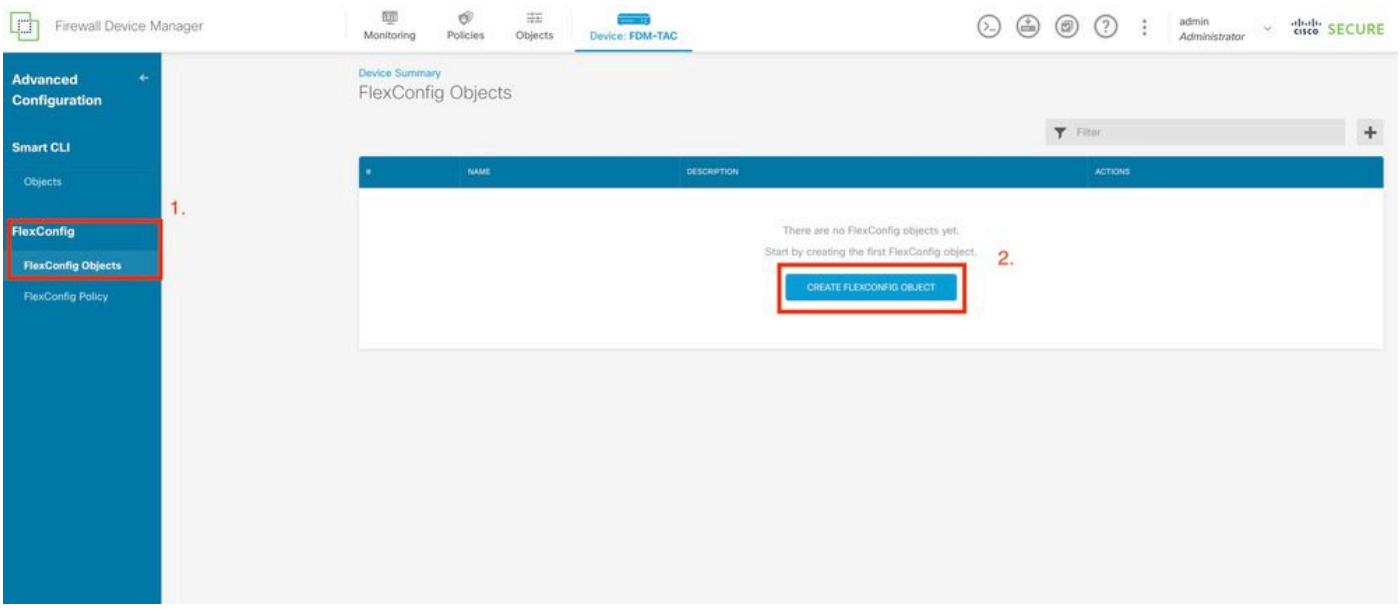
Nota: la configuración de estas funciones en Secure Firewall Threat Defence solo se admite actualmente mediante FlexConfig.

1. Inicie sesión en el administrador de dispositivos Firepower.

2. Para configurar el objeto FlexConfig, navegue hasta Device > Advanced Configuration > FlexConfig > FlexConfig Objects y, a continuación, haga clic en Create FlexConfig object.



Edite la configuración avanzada desde la página de inicio de FDM.



Cree un objeto FlexConfig.

3. Una vez abierta la ventana de objetos de FlexConfig, agregue la configuración necesaria para habilitar las funciones de detección de amenazas para la VPN de acceso remoto:

Característica 1: detección de amenazas para intentos de conexión a servicios VPN solo internos (no válidos)

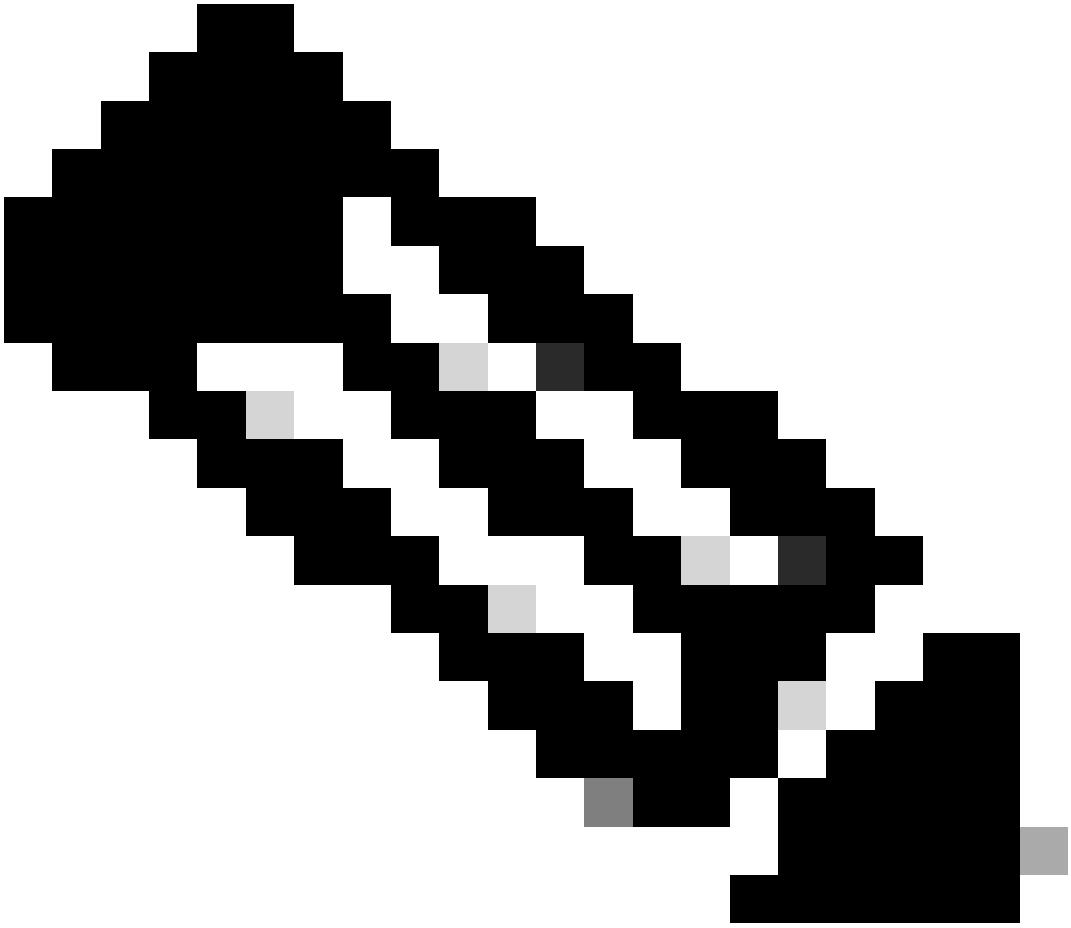
Para habilitar este servicio, agregue el comando threat-detection service invalid-vpn-access en el cuadro de texto del objeto FlexConfig.

Característica 2: Detección de amenazas para ataques de inicio de cliente VPN de acceso remoto

Para habilitar este servicio, agregue el comando threat-detection service remote-access-client-initiations hold-down <minutes> threshold <count> en el cuadro de texto del objeto FlexConfig, donde:

- hold-down <minutes> define el período después del último intento de inicio durante el cual se cuentan los intentos de conexión consecutivos. Si el número de intentos de conexión consecutivos cumple el umbral configurado en este período, se rechaza la dirección IPv4 del atacante. Puede establecer este período entre 1 y 1440 minutos.
- threshold <count> es el número de intentos de conexión necesarios dentro del período de espera para desencadenar un rechazo. Puede establecer el umbral entre 5 y 100.

Por ejemplo, si el período de espera es de 10 minutos y el umbral es de 20, la dirección IPv4 se rechaza automáticamente si hay 20 intentos de conexión consecutivos en un intervalo de 10 minutos.



Nota: Al establecer los valores de umbral y retención, tenga en cuenta el uso de NAT. Si utiliza PAT, que permite muchas solicitudes desde la misma dirección IP, considere valores más altos. Esto garantiza que los usuarios válidos tengan tiempo suficiente para conectarse. Por ejemplo, en un hotel, numerosos usuarios pueden intentar conectarse en un corto período de tiempo.

Característica 3: Detección de amenazas para errores de autenticación VPN de acceso remoto

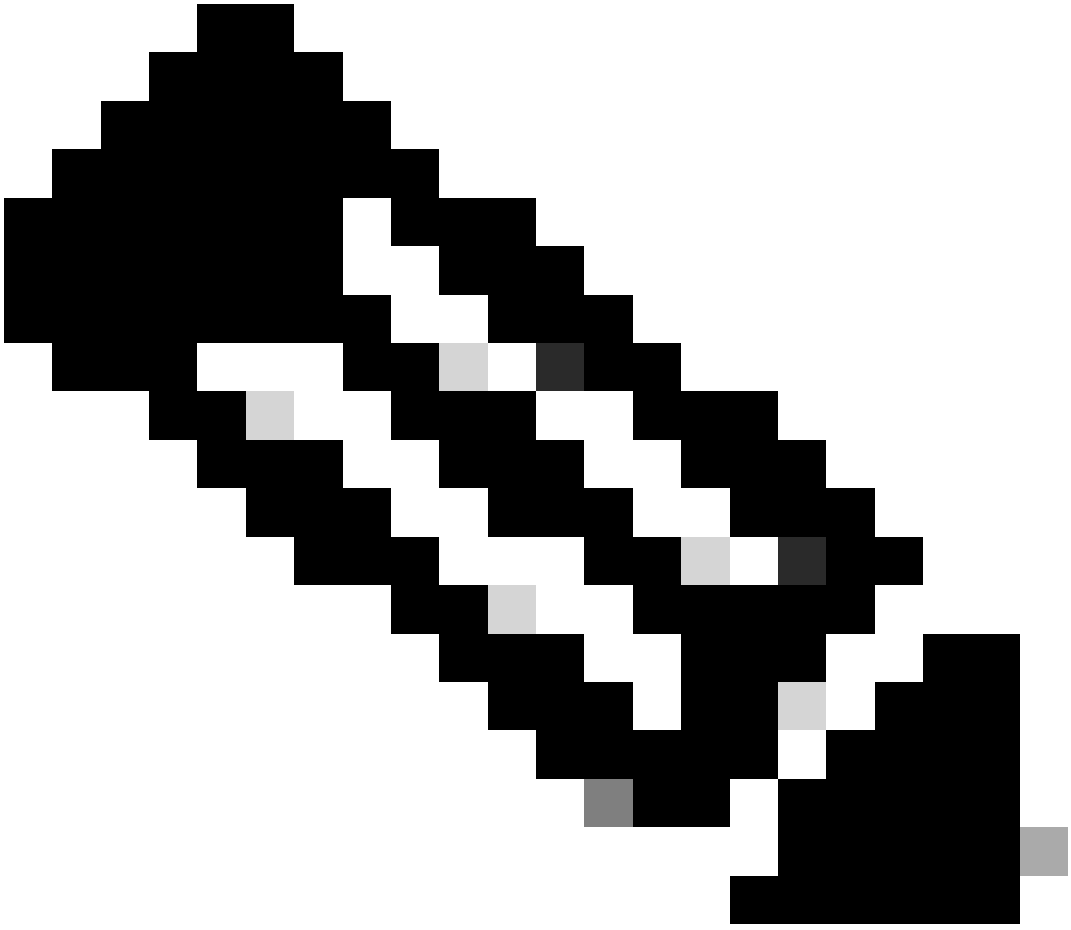
Para habilitar este servicio, agregue el comando threat-detection service remote-access-authentication hold-down<minutes> threshold <count> en el cuadro de texto del objeto FlexConfig, donde:

- hold-down <minutes> define el período después del último intento fallido durante el cual se cuentan los fallos consecutivos. Si el número de fallos de autenticación consecutivos cumple el umbral configurado en este período, se rechaza la dirección IPv4 del atacante. Puede establecer este período entre 1 y 1440 minutos.

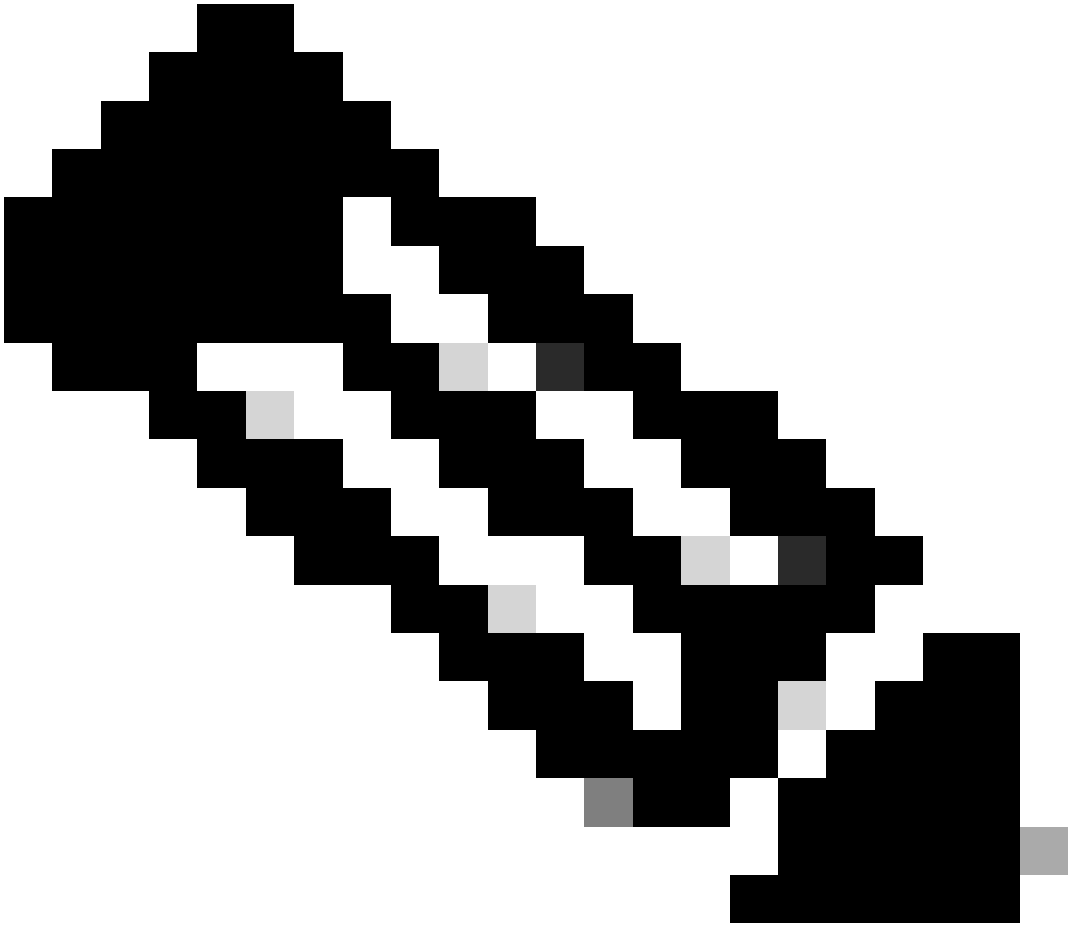
- threshold <count> es el número de intentos de autenticación fallidos necesarios dentro del período de espera para desencadenar un rechazo. Puede establecer el umbral entre 1 y 100.

Por ejemplo, si el período de espera es de 10 minutos y el umbral es de 20, la dirección IPv4 se rechaza automáticamente si se producen 20 errores de autenticación consecutivos en un intervalo de 10 minutos

---



Nota: Al establecer los valores de umbral y retención, tenga en cuenta el uso de NAT. Si utiliza PAT, que permite muchas solicitudes desde la misma dirección IP, considere valores más altos. Esto garantiza que los usuarios válidos tengan tiempo suficiente para conectarse. Por ejemplo, en un hotel, numerosos usuarios pueden intentar conectarse en un corto período de tiempo.

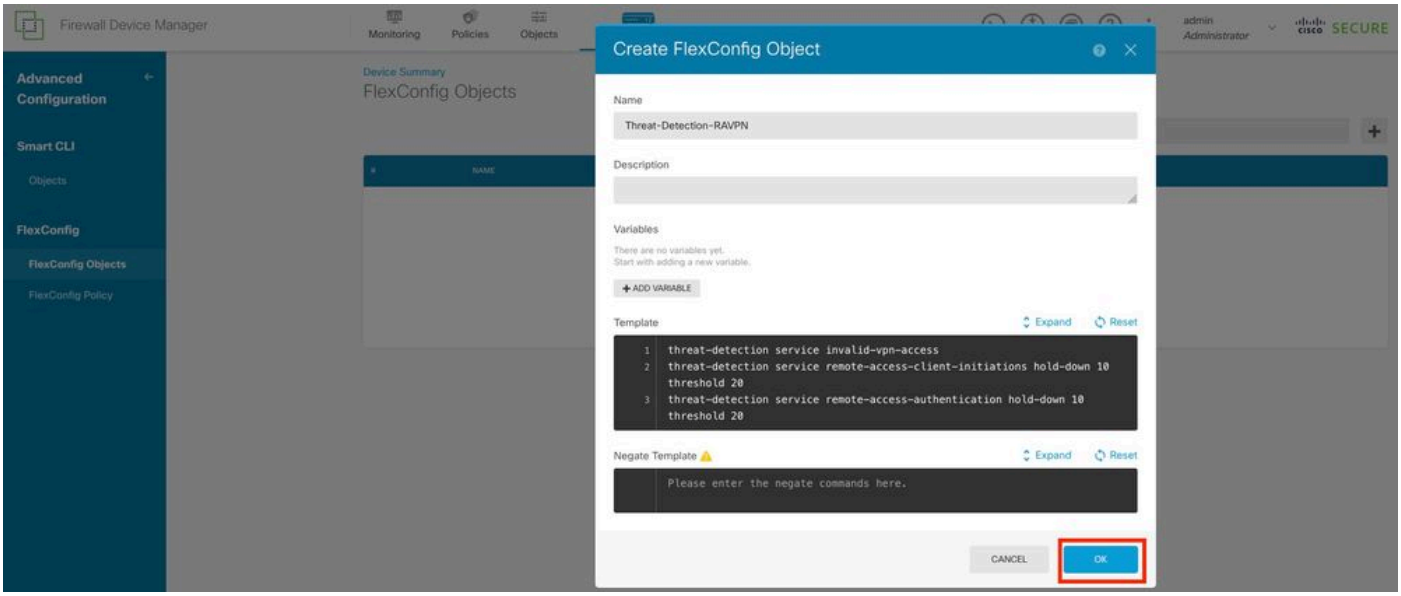


Nota: Los fallos de autenticación a través de SAML aún no se soportan.

Este ejemplo de configuración habilita los tres servicios de detección de amenazas disponibles para VPN de acceso remoto con un período de espera de 10 minutos y un umbral de 20 para la iniciación del cliente y los intentos de autenticación fallidos. Configure los valores hold-down y threshold según los requisitos de su entorno.

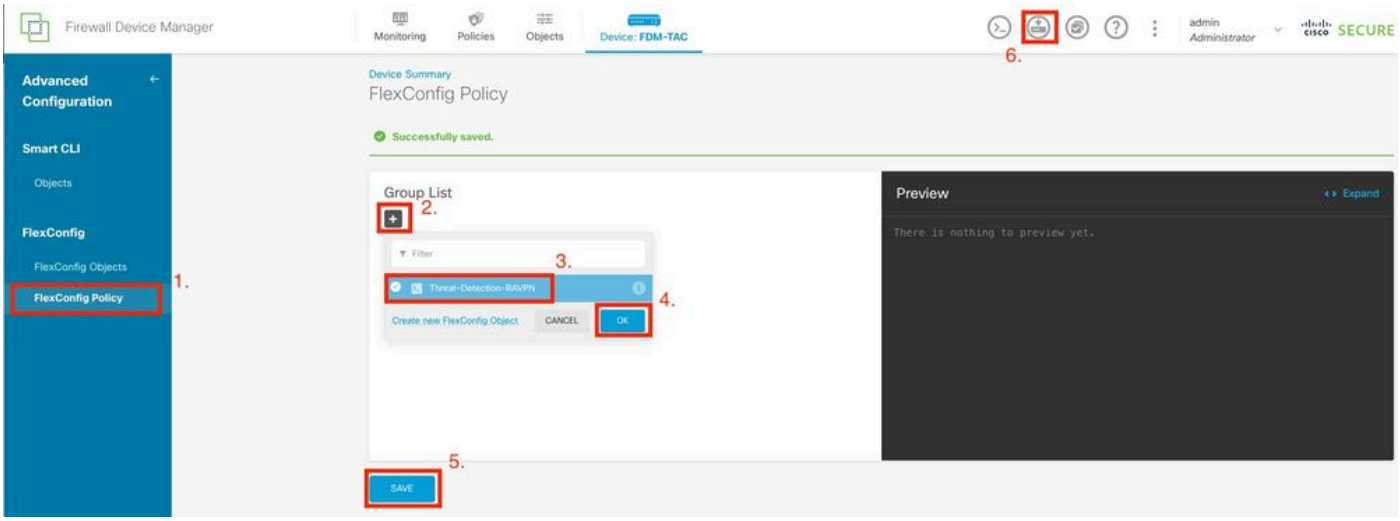
En este ejemplo se utiliza un único objeto FlexConfig para habilitar las 3 funciones disponibles.

```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```



Defina los criterios del objeto FlexConfig.

4. Una vez creado el objeto FlexConfig, navegue hasta FlexConfig > Política FlexConfig y busque el signo más debajo de Lista de grupos. Seleccione el objeto FlexConfig creado para la detección de amenazas de VPN de RA y haga clic en Aceptar para agregar el objeto a la lista de grupos. Esto rellena una vista previa CLI de los comandos, revise esta vista previa para garantizar la precisión. Seleccione SAVE e implemente los cambios en Firepower Threat Defence (FTD).



Edite la política FlexConfig y asigne el objeto FlexConfig.

Verificación

Para mostrar estadísticas de los servicios RAVPN de detección de amenazas, inicie sesión en la CLI del FTD y ejecute el comando show threat-detection service [service] [entries|details]. Donde el servicio puede ser: remote-access-authentication, remote-access-client-initiations, o invalid-vpn-access.

Puede limitar aún más la vista agregando estos parámetros:

- entries: muestra solo las entradas que están siendo rastreadas por el servicio de detección de amenazas. Por ejemplo, las direcciones IP que han tenido intentos de autenticación fallidos.
- details: muestra tanto los detalles del servicio como las entradas de servicio.

Ejecute el comando show threat-detection service para mostrar estadísticas de todos los servicios de detección de amenazas que están habilitados.

<#root>

```
FDM-TAC#

show threat-detection service


Service: invalid-vpn-access State : Enabled

    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0

Service: remote-access-authentication State : Enabled

    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 2

Name: remote-access-client-initiations State : Enabled

    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

Para ver más detalles de los atacantes potenciales que están siendo rastreados para el servicio de autenticación de acceso remoto, ejecute el comando show threat-detection service <service>entries.

<#root>

FDM-TAC#

show threat-detection service remote-access-authentication entries

Service:

remote-access-authentication

    Total entries: 2

```
Idx Source              Interface            Count          Age        Hold-down
--- ------------------- -------------------- -------------- ---------- ---------
  1 192.168.100.101/ 32              outside              1        721         0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

Para ver las estadísticas generales y los detalles de un servicio VPN de acceso remoto de detección de amenazas específico, ejecute el comando show threat-detection service <service>details.

<#root>

FDM-TAC#

show threat-detection service remote-access-authentication details

Service:

remote-access-authentication

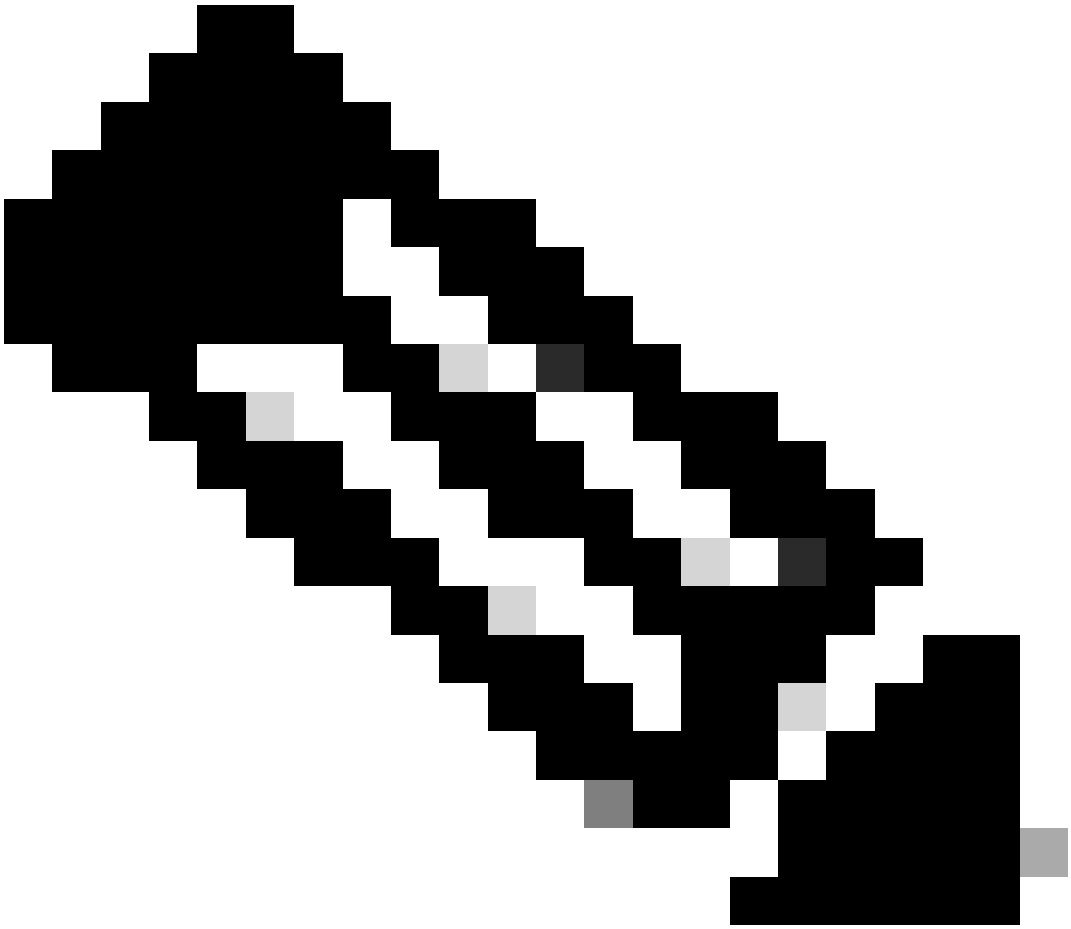
State :

Enabled

```
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age        Hold-down
--- ------------------- -------------------- -------------- ---------- ---------
  1 192.168.100.101/ 32              outside              1        721         0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2
```

```
NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```



> Nota: Las entradas solo muestran las direcciones IP sobre las que realiza un seguimiento el servicio de detección de amenazas. Si una dirección IP ha cumplido las condiciones para ser rechazada, el recuento de bloqueos aumenta y la dirección IP ya no se muestra como una entrada.

Además, puede monitorear los rechazos aplicados por los servicios VPN y eliminar los rechazos para una sola dirección IP o todas las direcciones IP con los siguientes comandos:

- show shun [ip_address]

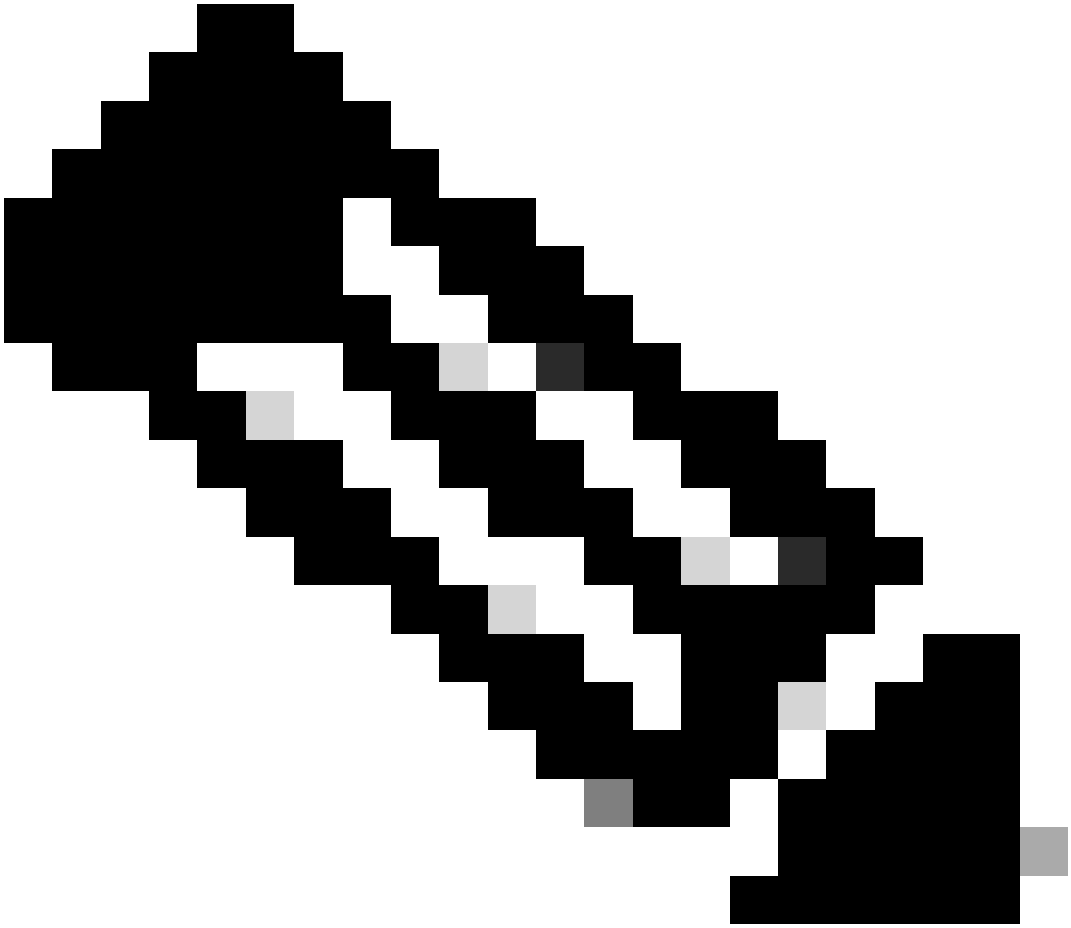
Muestra los hosts rechazados, incluidos los rechazados automáticamente por la detección de amenazas para los servicios VPN o manualmente mediante el comando shun. Opcionalmente, puede limitar la vista a una dirección IP especificada.

- no shun ip_address [interface if_name]

Quita el rechazo sólo de la dirección IP especificada. Opcionalmente, puede especificar el nombre de la interfaz para el rechazo, si la dirección se rechaza en más de una interfaz y desea dejar el rechazo en su lugar en algunas interfaces.

- clear shun

Elimina el rechazo de todas las direcciones IP y de todas las interfaces.



> Nota: las direcciones IP rechazadas por la detección de amenazas para los servicios VPN no aparecen en el comando show threat-detection shun, que se aplica únicamente a la detección de amenazas de análisis.

Para leer todos los detalles de cada resultado del comando y los mensajes syslog disponibles relacionados con los servicios de detección de amenazas para VPN de acceso remoto, consulte el documento Referencia de Comandos.

Información Relacionada

- Para obtener asistencia adicional, póngase en contacto con el centro de asistencia técnica (TAC). Se necesita un contrato de asistencia válido:Contactos de asistencia globales de Cisco.
- También puede visitar la Comunidad VPN de Cisco aquí.
- Soporte técnico y descargas de Cisco

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).