

Implemente medidas de refuerzo para AnyConnect VPN de cliente seguro

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Conceptos](#)

[Prácticas de protección de clientes en Cisco Secure Firewall:](#)

[Identificación de ataques mediante ID de registro y registro del sistema](#)

[Verificación de ataques](#)

[Ejemplos de Configuración de FMC](#)

[Deshabilitar la autenticación AAA en los perfiles de conexión DefaultWEBVPNGroup y DefaultRAGroup](#)

[Desactivar la posición de HostScan / Firewall seguro en DefaultWEBVPNGroup y DefaultRAGroup \(opcional\)](#)

[Desactivar alias de grupo y activar URL de grupo](#)

[Asignación de certificados](#)

[IPsec-IKEv2](#)

[Ejemplos de Configuración de ASA](#)

[Deshabilitar la autenticación AAA en los perfiles de conexión DefaultWEBVPNGroup y DefaultRAGroup](#)

[Desactivar la posición de HostScan / Firewall seguro en DefaultWEBVPNGroup y DefaultRAGroup \(opcional\)](#)

[Desactivar alias de grupo y activar URL de grupo](#)

[Asignación de certificados](#)

[IPsec-IKEv2](#)

[Conclusión](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo mejorar la seguridad de su implementación de VPN de acceso remoto.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

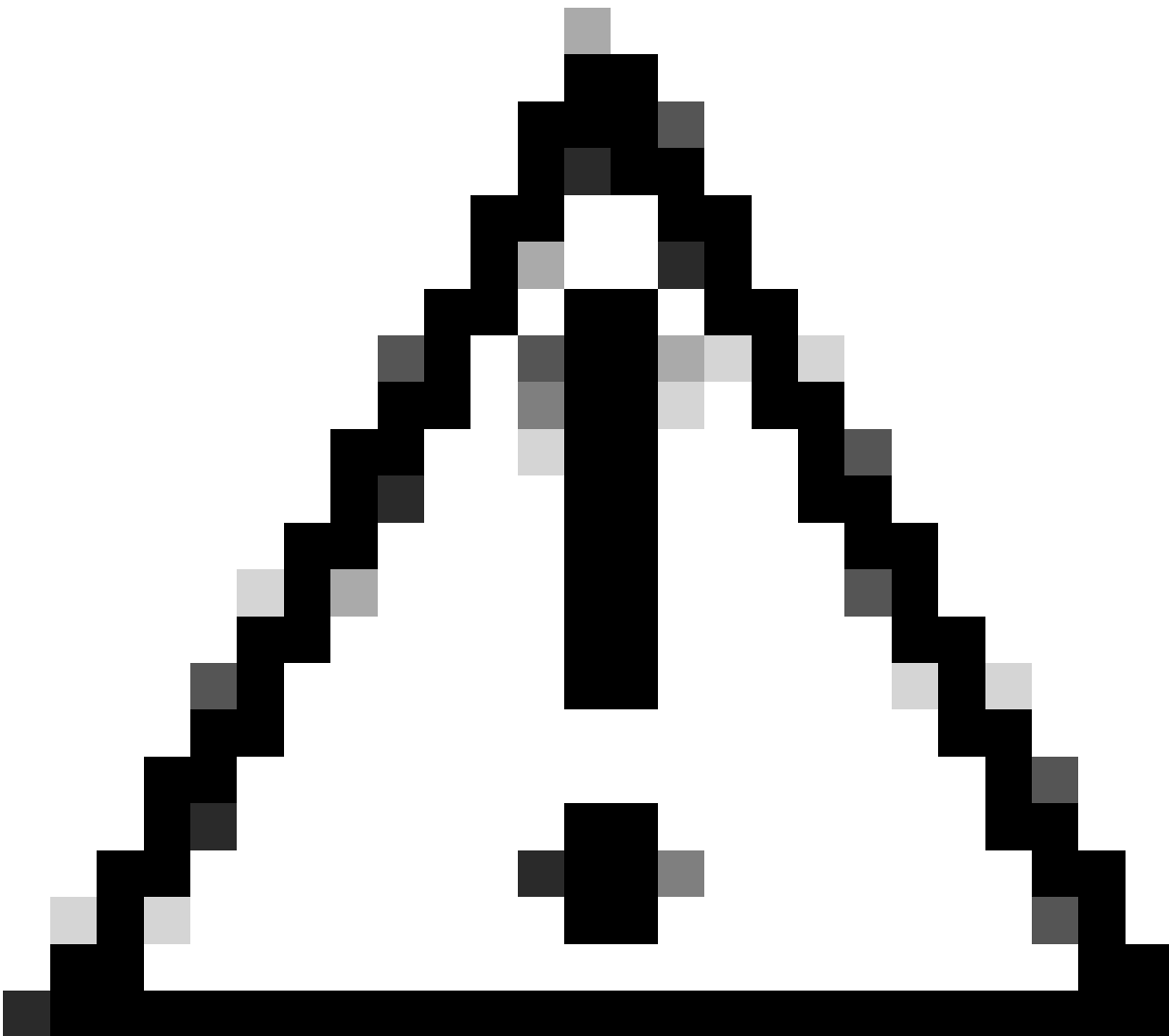
- VPN AnyConnect de Cisco Secure Client.
- Configuración de acceso remoto ASA/FTD.

Componentes Utilizados

La guía de prácticas recomendadas se basa en las siguientes versiones de hardware y software:

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

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.



Precaución: este documento no contiene pasos para Firepower Device Manager (FDM). FDM sólo admite el cambio del método de autenticación en DefaultWEBVPNGroup. Utilice ACL de plano de control o un puerto personalizado en la sección "Configuración"

global" de VPN de acceso remoto de la interfaz de usuario de FDM. Póngase en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) para obtener más ayuda si la necesita.

Antecedentes

El objetivo de este documento es garantizar que la configuración de AnyConnect VPN de Cisco Secure Client se ajuste a las prácticas recomendadas de seguridad en un mundo moderno en el que los ataques de ciberseguridad son habituales.

Los ataques de fuerza bruta suelen implicar intentos repetidos de obtener acceso a un recurso mediante combinaciones de nombre de usuario y contraseña. Los atacantes intentan utilizar su navegador de Internet, la interfaz de usuario de cliente seguro u otras herramientas para introducir varios nombres de usuario y contraseñas con la esperanza de que coincidan con una combinación legítima en una base de datos AAA. Al utilizar AAA para la autenticación, esperamos que el usuario final introduzca su nombre de usuario y contraseña, ya que esto es necesario para establecer la conexión. Al mismo tiempo, no estamos verificando quién es el usuario hasta que introduzca sus credenciales. Por naturaleza, esto permite a los atacantes aprovechar estos escenarios:

1. Expuso nombres de dominio completamente calificados para Cisco Secure Firewall (especialmente cuando se utilizan alias de grupo en el perfil de conexión):
 - Si el atacante descubre el FQDN de su firewall VPN, tendrá la opción de seleccionar el grupo de túnel mediante el alias del grupo en el que desea iniciar el ataque de fuerza bruta.
2. Perfil de conexión predeterminado configurado con AAA o base de datos local:
 - Si el atacante encuentra el FQDN del firewall VPN, puede intentar atacar por fuerza bruta el servidor AAA o la base de datos local. Esto ocurre porque la conexión al FQDN cae en el perfil de conexión predeterminado, incluso si no se especifican alias de grupo.
3. Agotamiento de recursos en el firewall o en servidores AAA:
 - Los atacantes pueden saturar los servidores AAA o los recursos de firewall enviando grandes cantidades de solicitudes de autenticación y creando una condición de denegación de servicio (DoS).

Conceptos

Alias de grupo:

- Nombre alternativo con el que el firewall puede hacer referencia a un perfil de conexión. Después de iniciar una conexión con el firewall, estos nombres aparecen en un menú desplegable en la interfaz de usuario de Secure Client para que los usuarios los

seleccionen. La eliminación de alias de grupo quita la funcionalidad desplegable en la interfaz de usuario de Secure Client.

URLs de grupo:

- Dirección URL que se puede vincular a un perfil de conexión para que las conexiones entrantes se asignen directamente a un perfil de conexión deseado. No hay funcionalidad de lista desplegable, ya que los usuarios pueden introducir la URL completa en la interfaz de usuario de Secure Client, o la URL se puede integrar con un 'Display Name' en el perfil XML para ocultar la URL al usuario.

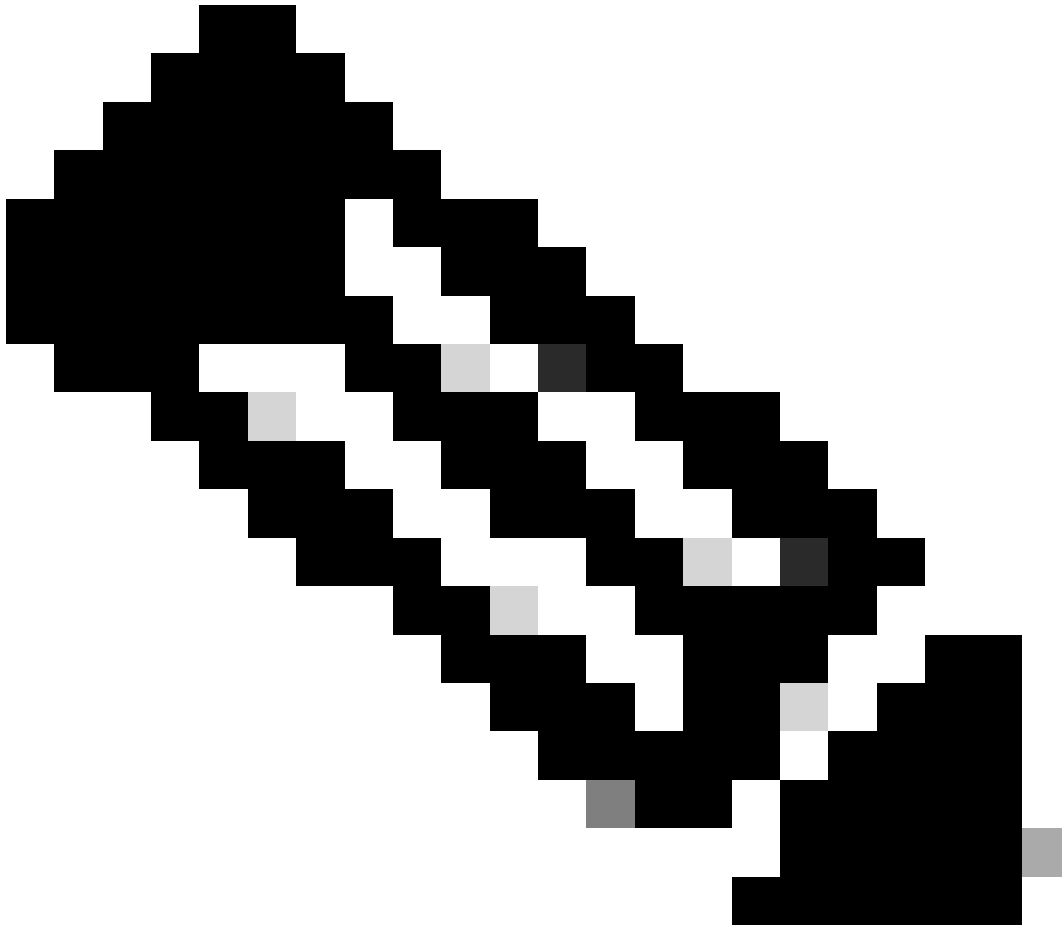
La diferencia aquí es que cuando se implementan alias de grupo, un usuario inicia una conexión to `vpn_gateway.example.com` y se le presentan alias para seleccionar que los llevan a un perfil de conexión. Con las URLs de grupo, un usuario inicia una conexión a `vpn_gateway.example.com/example_group` y eso los conduce directamente al perfil de conexión sin la necesidad u opción de un menú desplegable.

Prácticas de protección de clientes en Cisco Secure Firewall:

Estos métodos se basan en la asignación de usuarios legítimos a grupos de túnel/perfiles de conexión adecuados, mientras que los usuarios potencialmente maliciosos se envían a un grupo de túnel de trampa que configuramos para no permitir combinaciones de nombre de usuario y contraseña. Aunque no se deben implementar todas las combinaciones, para que las recomendaciones funcionen de forma eficaz, es necesario deshabilitar los alias de grupo y cambiar el método de autenticación de DefaultWEBVPNGroup y DefaultRAGroup.

- Deshabilite los alias de grupo y utilice solamente el url de grupo en la configuración del perfil de conexión, esto le permite tener un FQDN específico que no será fácil para un atacante descubrir y seleccionar ya que solamente los clientes con el FQDN adecuado pueden iniciar la conexión. Por ejemplo, `vpn_gateway.example.com/example_group` es más difícil de descubrir para un atacante que `vpn_gateway.example.com`.
- Inhabilite la autenticación AAA en DefaultWEBVPNGroup y DefaultRAGroup y configure la autenticación de certificados, esto evita una posible fuerza bruta contra la base de datos local o el servidor AAA. En este escenario, al atacante se le presentarían errores inmediatos al intentar conectarse. No existe ningún campo de nombre de usuario o contraseña, ya que la autenticación se basa en certificados, con lo que se detienen los intentos de fuerza bruta. Otra opción es crear un servidor AAA sin configuración auxiliar para crear un agujero negro para las solicitudes maliciosas.
- Utilice la asignación de certificados para el perfil de conexión. Esto permite que las conexiones entrantes se asignen a perfiles de conexión específicos en función de los atributos recibidos de los certificados en el dispositivo cliente. Los usuarios que tienen los certificados adecuados se asignan correctamente, mientras que los atacantes que no cumplen los criterios de asignación se envían al grupo DefaultWEBVPN.

- El uso de IKEv2-IPSec en lugar de SSL hace que los grupos de túnel dependan de una asignación de grupo de usuarios específica en el perfil XML. Sin este XML en el equipo del usuario final, los usuarios se envían automáticamente al grupo de túnel predeterminado.
-



Nota: Para obtener más información sobre la funcionalidad de alias de grupo, consulte la [Guía de Configuración de VPN ASA](#) y observe la 'Tabla 1. Atributos de perfil de conexión para SSL VPN'.

Identificación de ataques mediante ID de registro y registro del sistema

Los ataques de fuerza bruta representan el método predominante para poner en peligro las VPN de acceso remoto y aprovechar las contraseñas débiles para obtener entradas no autorizadas. Es fundamental saber reconocer los signos de un ataque aprovechando el uso del registro y la evaluación de los registros del sistema. Los ID de syslogs comunes que pueden indicar un ataque si se encuentra con un volumen anormal son:

%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

El nombre de usuario siempre está oculto hasta que se configura el comando no logging hide username en ASA.



Nota: Esto proporciona información sobre si las IP infractoras generan usuarios válidos o los conocen; sin embargo, tenga cuidado ya que los nombres de usuario son visibles en los registros.

Registro de Cisco ASA:

[Guía del usuario para proteger el firewall ASA](#)

[Capítulo sobre el registro](#) de la Guía de configuración de la CLI de operaciones generales de Cisco Secure Firewall ASA Series

Registro de FTD de Cisco:

[Configuración del inicio de sesión en FTD mediante el FMC](#)

[Sección Configurar Syslog](#) del capítulo Configuración de la plataforma de la Guía de configuración de dispositivos de Cisco Secure Firewall Management Center

[Configuración y verificación de Syslog en el administrador de dispositivos Firepower](#)

[Sección Configuración de los parámetros de registro del sistema](#) del capítulo Configuración del sistema de la Guía de configuración de Cisco Firepower Threat Defense para Firepower Device Manager

Verificación de ataques

Para verificarlo, inicie sesión en la interfaz de línea de comandos (CLI) de ASA o FTD, ejecute el comando `show aaa-server` e investigue si existe un número inusual de solicitudes de autenticación intentadas y rechazadas en cualquiera de los 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
```

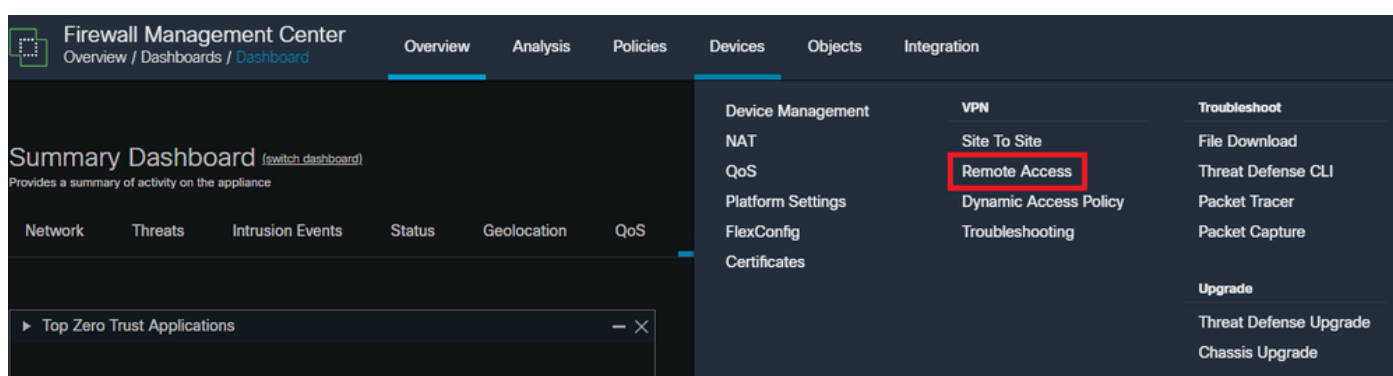
```
Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
Number of 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

Ejemplos de Configuración de FMC

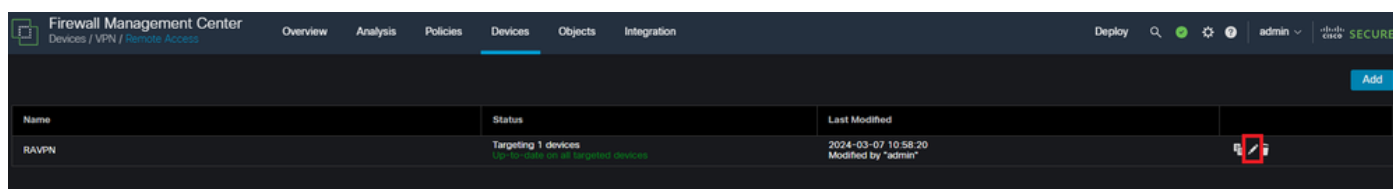
Deshabilitar la autenticación AAA en los perfiles de conexión
DefaultWEBVPNGroup y DefaultRAGroup

Vaya a Devices > Remote Access.



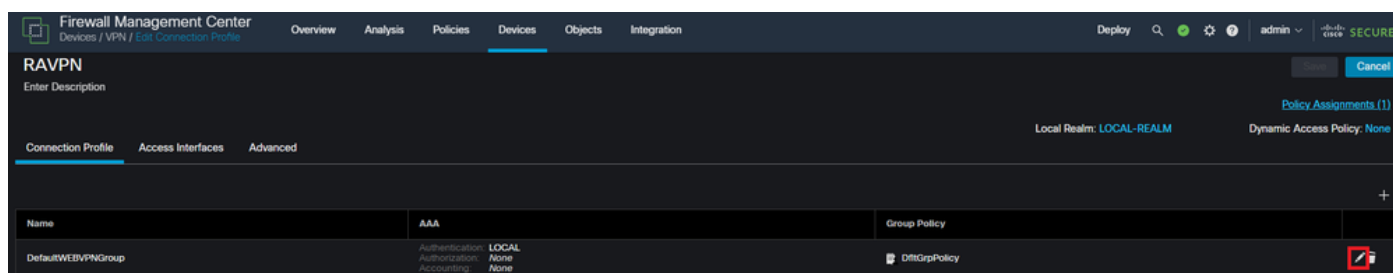
Muestra cómo navegar por la GUI de FMC para llegar a la configuración de la directiva VPN de acceso remoto.

Edite la directiva VPN de acceso remoto existente y cree un perfil de conexión denominado 'DefaultRAGroup'



Muestra cómo editar la directiva VPN de acceso remoto en la interfaz de usuario de FMC.

Edite los perfiles de conexión denominados 'DefaultWEBVPNGroup' y 'DefaultRAGroup'



Muestra cómo editar el DefaultWEBVPNGroup en la interfaz de usuario de FMC.

Vaya a la pestaña AAA y seleccione el menú desplegable Authentication Method. Seleccione

'Solo certificado de cliente' y seleccione Guardar.

The screenshot shows the 'Edit Connection Profile' interface with the following elements:

- Header:** 'Edit Connection Profile' with a help icon.
- Fields:**
 - Connection Profile:* DefaultWEBVPNGroup
 - Group Policy:* DfltGrpPolicy (with a '+' icon and a link to 'Edit Group Policy')
- Tabs:** Client Address Assignment, AAA (selected), Aliases.
- Authentication Section:**
 - Authentication Method: Client Certificate Only (highlighted with a red box)
 - Enable multiple certificate authentication
 - ▶ Map username from client certificate
- Authorization Section:**
 - Authorization Server: [Dropdown]
 - Allow connection only if user exists in authorization database
- Accounting Section:**
 - Accounting Server: [Dropdown]
- Buttons:** Cancel and Save (highlighted with a red box).

Cambio del método de autenticación al certificado de cliente sólo para DefaultWEBVPNGroup en la interfaz de usuario de FMC.

Edite DefaultRAGroup y Navegue hasta la pestaña AAA y seleccione el menú desplegable Authentication Method. Seleccione 'Solo certificado de cliente' y seleccione Guardar.

Edit Connection Profile

Connection Profile:*

Group Policy:* +

[Edit Group Policy](#)

Client Address Assignment

AAA

Aliases

Authentication

Authentication Method:

Enable multiple certificate authentication

▶ Map username from client certificate

Authorization

Authorization Server:

Allow connection only if user exists in authorization database

Accounting

Accounting Server:

Cancel

Save

Cambiar el método de autenticación a certificado de cliente sólo para DefaultRAGroup en la interfaz de usuario de FMC.

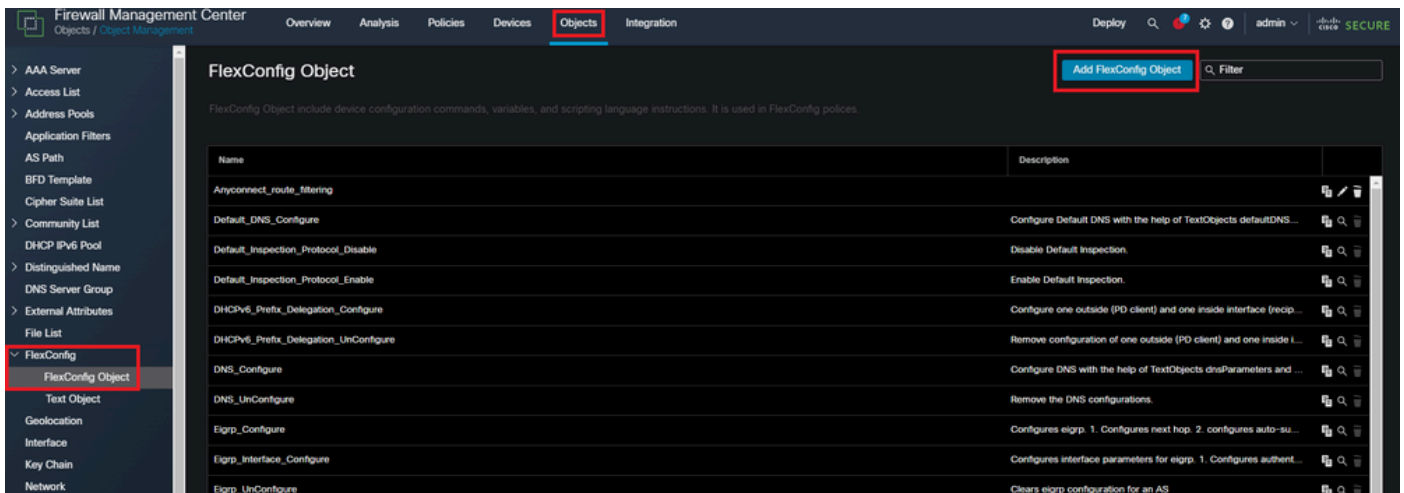


Nota: El método de autenticación también puede ser un servidor AAA sinkhole. Si se utiliza este método, la configuración del servidor AAA es falsa y en realidad no procesa ninguna solicitud. Para guardar los cambios, también debe definirse un grupo VPN en la ficha 'Asignación de direcciones de cliente'.

Desactivar la posición de HostScan / Firewall seguro en DefaultWEBVPNGroup y DefaultRAGroup (opcional)

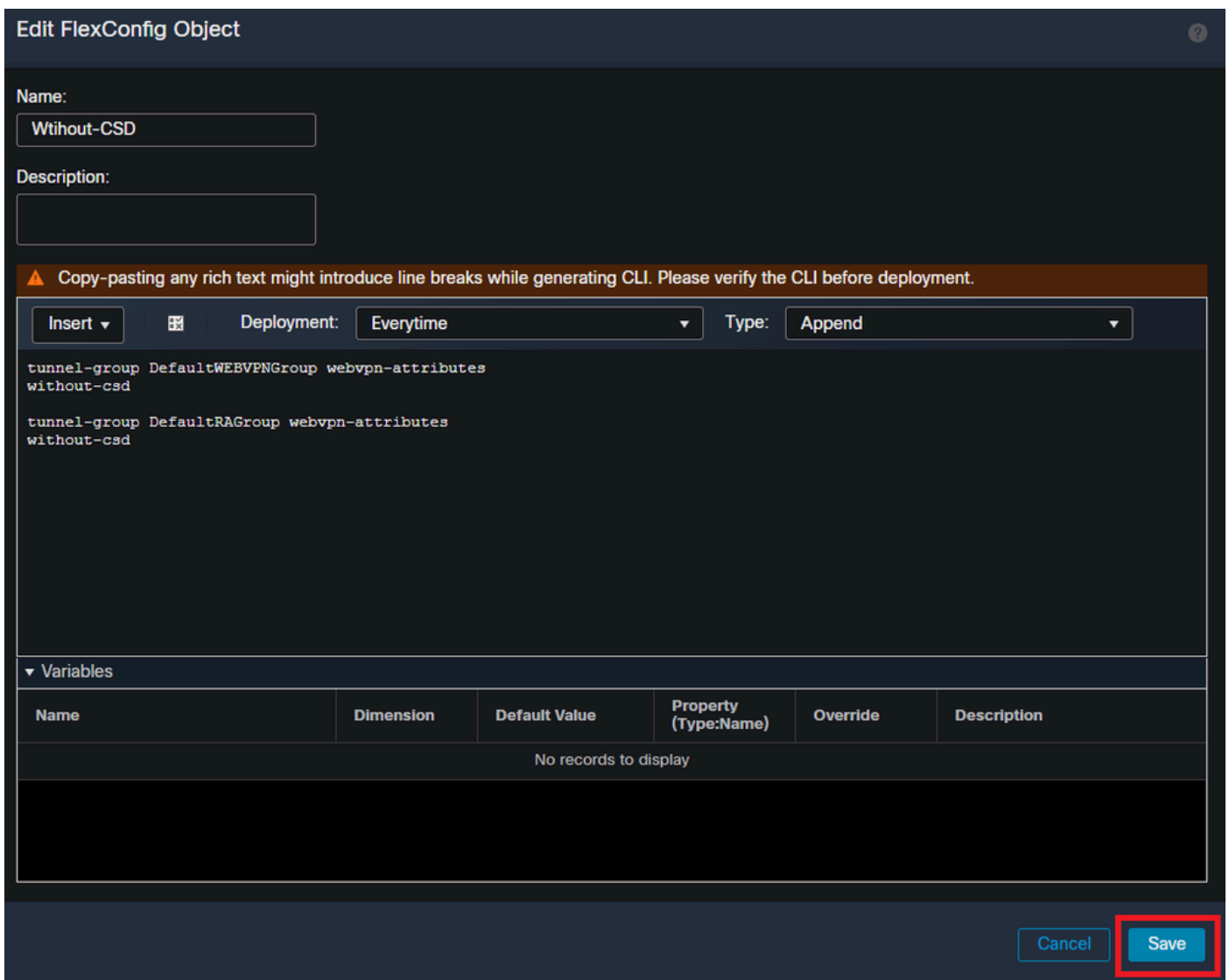
Esto sólo es necesario si su entorno dispone de una posición de Hostscan/Secure Firewall. Este paso evita que los atacantes aumenten la utilización de recursos en el firewall provocada por el proceso de análisis de terminales. En el FMC, esto se logra mediante la creación de un objeto FlexConfig con el comando `without-csd` para deshabilitar la funcionalidad de escaneo del terminal.

Vaya a **Objetos > Gestión de objetos > Objeto FlexConfig > Agregar objeto FlexConfig**.



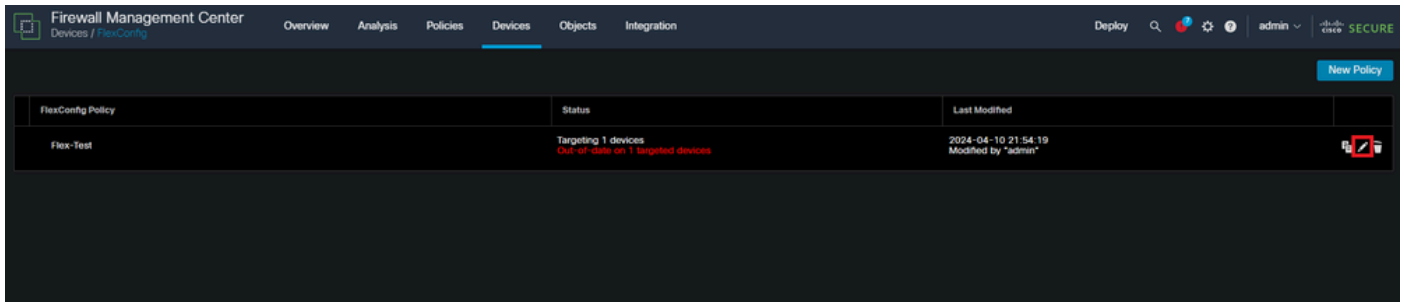
Navegación por la interfaz de usuario de FMC para crear un objeto FlexConfig.

Dé un nombre al objeto FlexConfig y establezca la implementación en Everytime con el tipo Append. A continuación, introduzca la sintaxis tal y como se muestra y guarde el objeto.



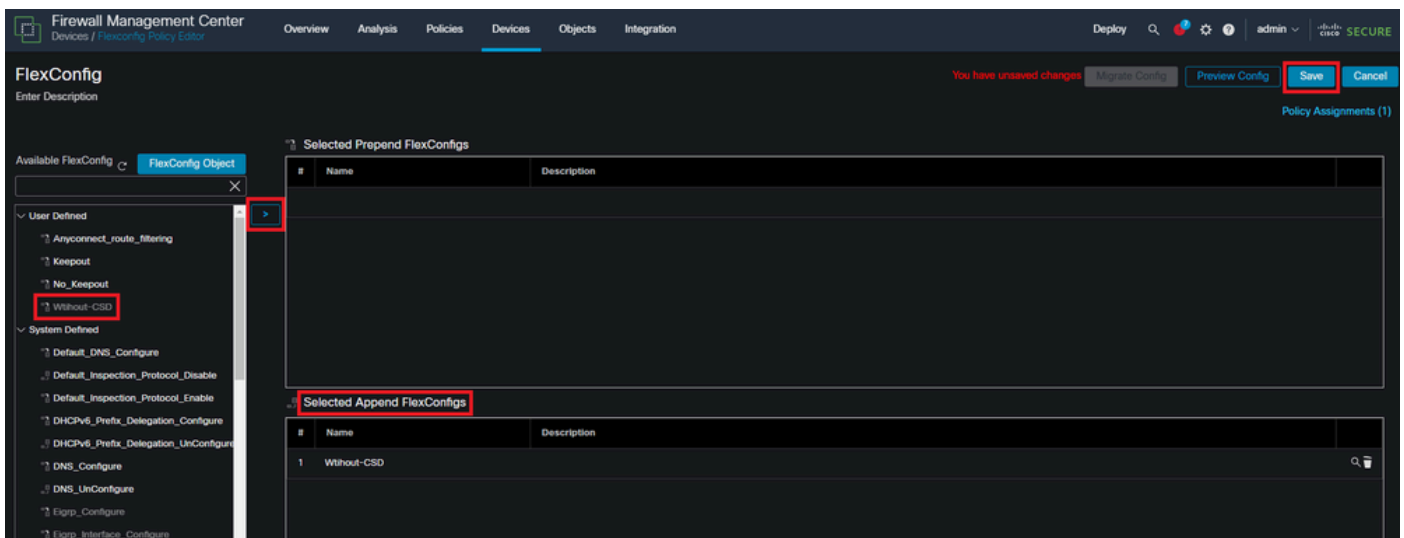
Creación de un objeto FlexConfig con 'without-csd'

Navegue hasta Devices > FlexConfig y luego haga clic en Pencil para editar la política FlexConfig.



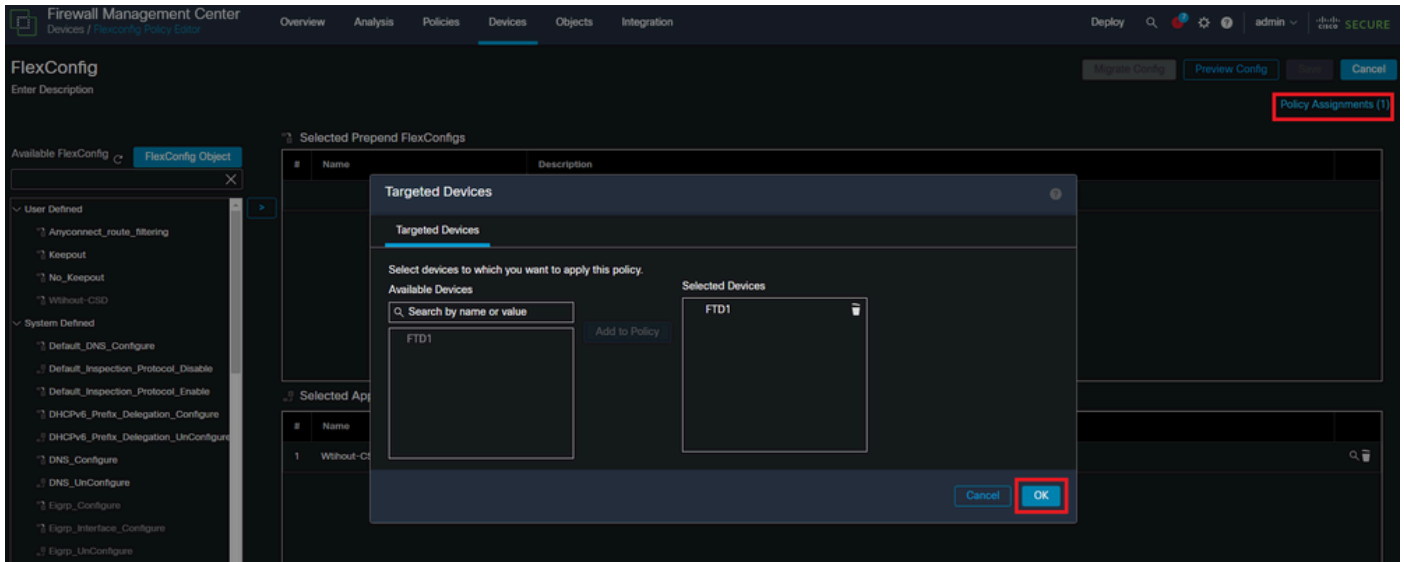
Edición de la política FlexConfig en el FMC.

Localice el objeto creado en la sección Definido por el usuario. A continuación, seleccione la flecha para agregarla a Selected Append FlexConfigs. Por último, seleccione Save para guardar la política FlexConfig.



Ajunte el objeto FlexConfig a la directiva FlexConfig.

Seleccione Policy Assignments y elija el FTD al que desea aplicar esta política FlexConfig y, a continuación, seleccione OK. Seleccione Guardar de nuevo si se trata de una nueva asignación de FlexConfig e implemente los cambios. Una vez implementado, verifique



Asigne la política FlexConfig a un dispositivo FirePOWER.

Ingrese la CLI de FTD y ejecute el comando `show run tunnel-group` para `DefaultWEBVPNGroup` y `DefaultRAGroup`. Verifique que `without-csd` esté presente en la configuración.

```
<#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
```

Desactivar alias de grupo y activar URL de grupo

Desplácese hasta un perfil de conexión y seleccione la ficha 'Alias'. Desactive o elimine el alias de

grupo y haga clic en el icono más para agregar un alias de URL.

Edit Connection Profile

Connection Profile:* LDAP-TG

Group Policy:* DfltGrpPolicy +
[Edit Group Policy](#)

Client Address Assignment AAA **Aliases**

Alias Names:
Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display. +

Name	Status	
LDAP	Disabled	

URL Alias:
Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile. +

URL	Status	
-----	--------	--

Inhabilitación de la opción de alias de grupo para un grupo de túnel dentro de la IU de FMC.

Configure un nombre de objeto para el alias de URL y rellene el FQDN o la dirección IP del firewall para la URL, seguido del nombre con el que desea asociar el perfil de conexión. En este ejemplo, hemos elegido 'aaldap'. Cuanto más oscuro, más seguro, ya que es menos probable que los atacantes adivinen la URL completa, incluso si han obtenido su FQDN. Una vez finalizado, seleccione Save.

Edit URL Objects



Name

LDAP-ALIAS

Description

URL

https://ftd1 [redacted] .com/aaalda|

Allow Overrides

Cancel

Save

Creación de un objeto URL-Alias en la interfaz de usuario de FMC.

Seleccione el URL Alias en el menú desplegable, marque la casilla Enabled y seleccione OK.

Add URL Alias



URL Alias:

LDAP-ALIAS



Enabled

Cancel

OK

Asegúrese de que URL-Alias esté habilitado en la interfaz de usuario de FMC.

Asegúrese de que el alias de grupo se haya eliminado o deshabilitado y compruebe que el alias de URL está ahora habilitado y, a continuación, seleccione Guardar.


Edit Connection Profile

Connection Profile:* LDAP-TG

Group Policy:* DfltGrpPolicy [Edit Group Policy](#)


Client Address Assignment AAA **Aliases**

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Name	Status	
LDAP	Disabled	

URL Alias:

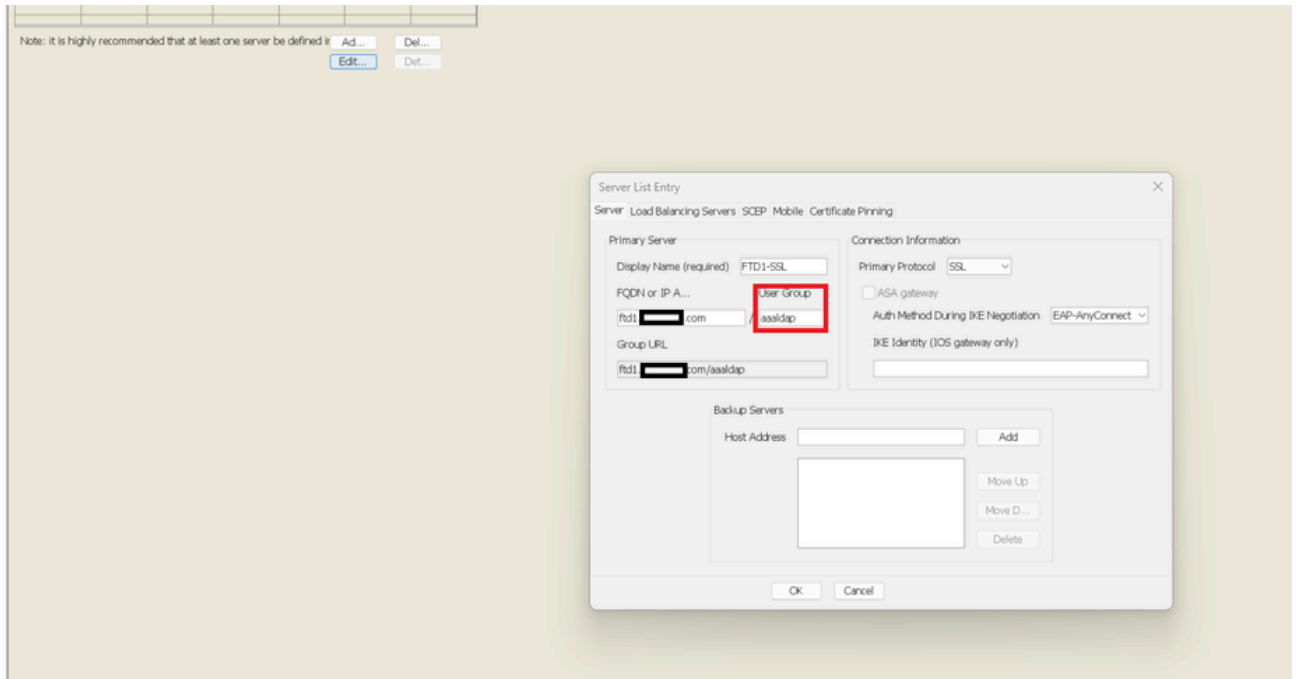
Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.

URL	Status	
LDAP-ALIAS (https://ftd1 [redacted] com/aaaldap)	Enabled	

[Cancel](#) [Save](#)

Habilitación de la opción URL-Alias para un grupo de túnel dentro de la IU de FMC.

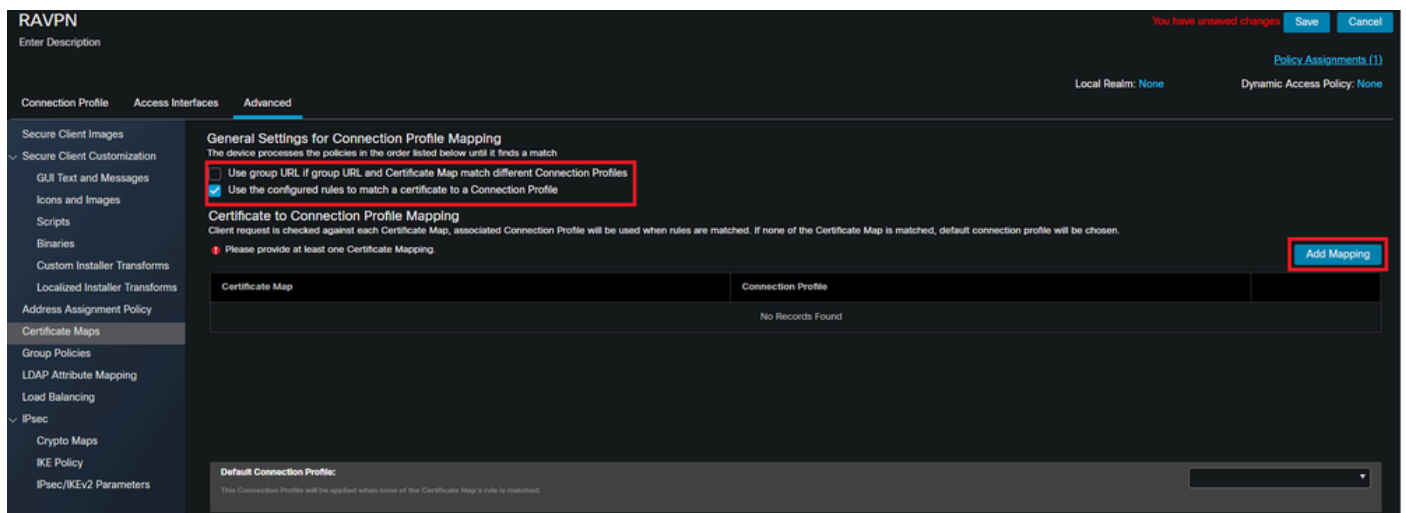
Si lo desea, también se pueden insertar alias de URL como parte del XML. Esto se logra editando el XML mediante el Editor de perfiles VPN o el Editor de perfiles ASA. Para ello, vaya a la ficha Server List (Lista de servidores) y asegúrese de que el campo User Group (Grupo de usuarios) coincida con el alias de URL del perfil de conexión cuando utilice SSL. Para IKEv2, asegúrese de que el campo Grupo de usuarios coincide con el nombre exacto del perfil de conexión.



Edición del perfil XML para que tenga un URL-Alias para las conexiones SSL.

Asignación de certificados

Vaya a la pestaña Advanced dentro de la Política VPN de acceso remoto. Elija una opción de configuración general basada en las preferencias. Una vez seleccionado, seleccione Add Mapping.



Vaya a la ficha Advanced (Opciones avanzadas) de la interfaz de usuario de FMC para crear un objeto de asignación de certificados en la interfaz de usuario de FMC.

Asigne un nombre al objeto de asignación de certificados y seleccione Agregar regla. En esta regla, defina las propiedades del certificado que desea identificar para asignar el usuario a un perfil de conexión determinado. Una vez finalizado, seleccione Aceptar y, a continuación, Guardar.

Add Certificate Map



Map Name*:

Certificate-Map-CN

Mapping Rule

Add Rule

Configure the certificate matching rule

#	Field	Component	Operator	Value
1	Subject	CN (Common Name)	Equals	customvalue

OK

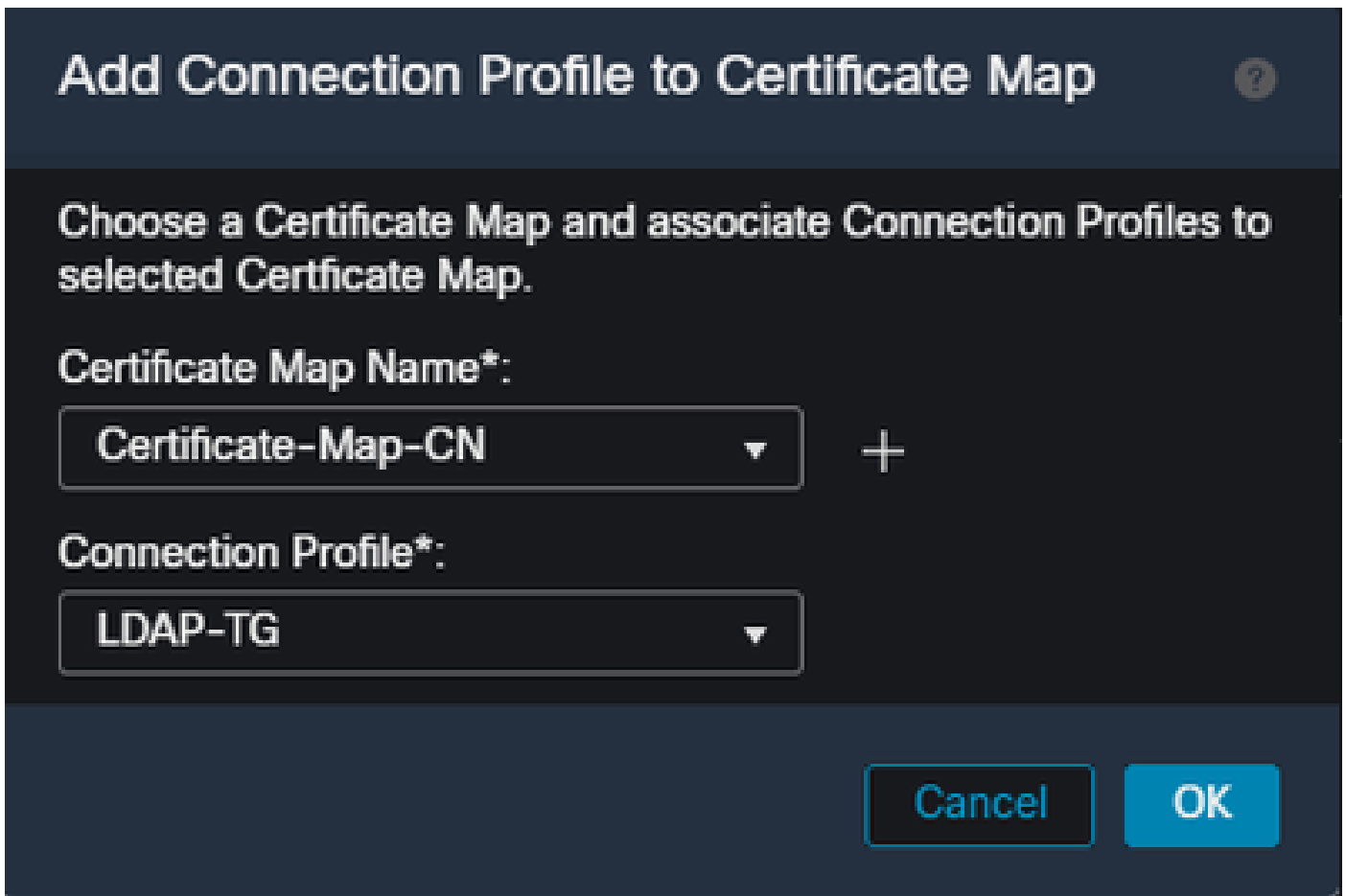
Cancel

Cancel

Save

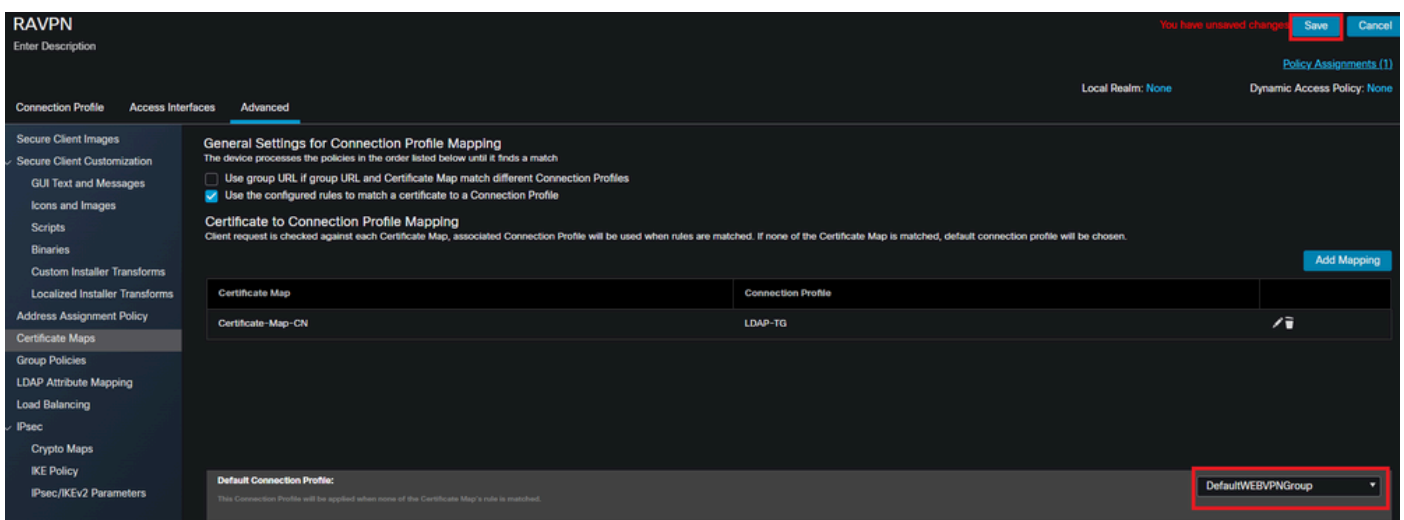
Cree un mapa de certificado y agregue criterios para el mapa dentro de la interfaz de usuario de FMC.

En el menú desplegable, seleccione el objeto de mapa de certificado y el perfil de conexión con el que desea asociar el mapa de certificado. A continuación, seleccione Aceptar.



Vincule el objeto de mapa de certificado al grupo de túnel deseado dentro de la interfaz de usuario de FMC.

Asegúrese de que el perfil de conexión predeterminado esté configurado como DefaultWEBVPNGroup para que, si un usuario falla en la asignación, se envíe al DefaultWEBVPNGroup. Una vez finalizado, seleccione Save e implemente los cambios.



Cambie el perfil de conexión predeterminado para la asignación de certificados al DefaultWEBVPNGroup en la interfaz de usuario de FMC.

IPsec-IKEv2

Seleccione el perfil de conexión IPsec-IKEv2 deseado y desplácese hasta Editar directiva de

grupo.

Edit Connection Profile

Connection Profile:* IKEV2


Group Policy:* IKEV2-IPSEC +

[Edit Group Policy](#)

Client Address Assignment AAA Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools: +

Name	IP Address Range	
AnyConnect_Pool	10.50.50.1-10.50.50.6	

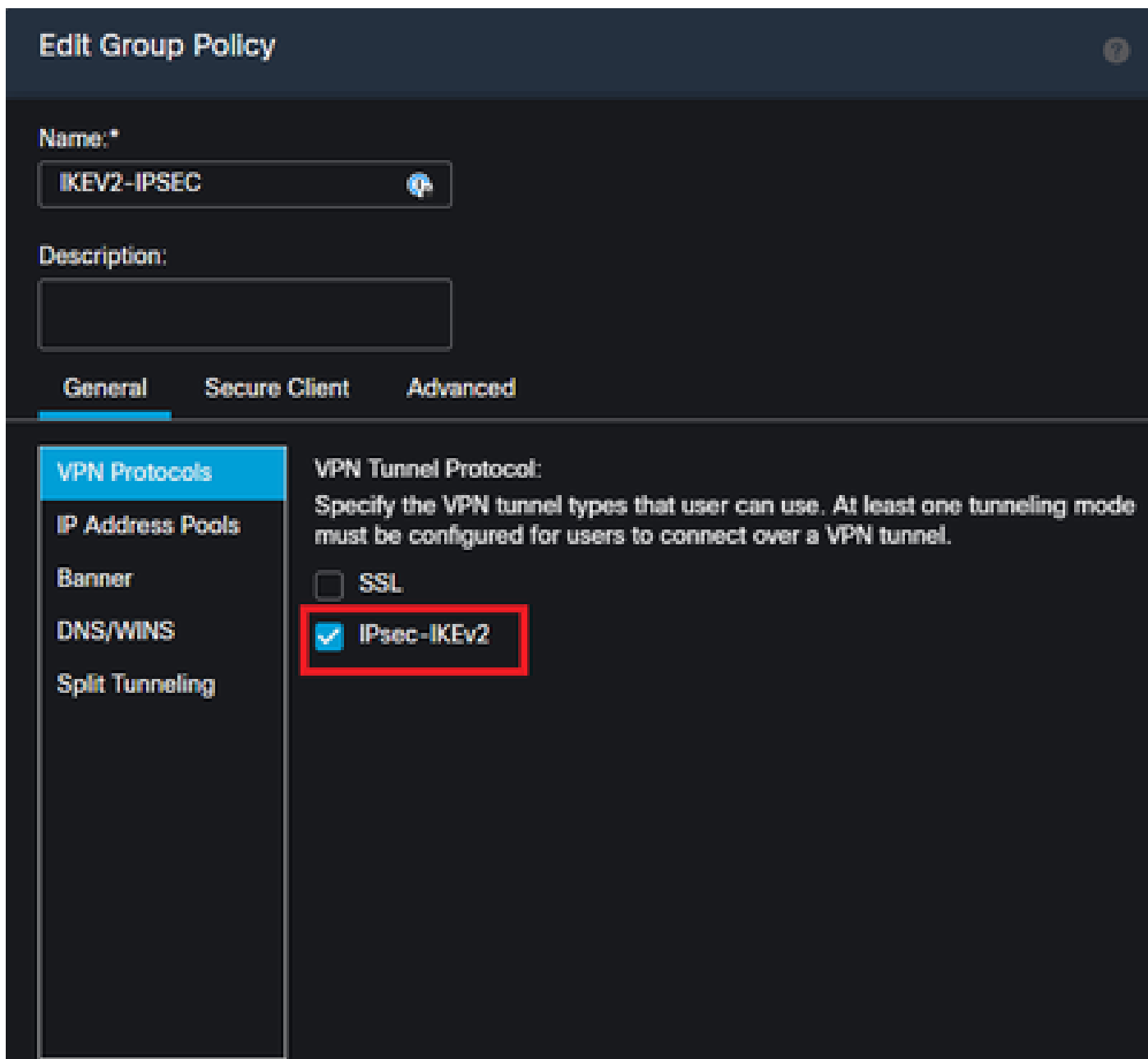
DHCP Servers: +

Name	DHCP Server IP Address	
------	------------------------	--

Cancel Save

Edite una política de grupo en la interfaz de usuario de FMC.

En la pestaña General, navegue hasta la sección VPN Protocols y asegúrese de que la casilla IPsec-IKEv2 esté marcada.



Habilite IPsec-IKEv2 dentro de una política de grupo en la IU de FMC.

En el Editor de perfiles VPN, o el Editor de perfiles ASA, vaya a la pestaña Lista de servidores. El nombre del grupo de usuarios DEBE coincidir exactamente con el nombre del perfil de conexión del firewall. En este ejemplo, IKEV2 era el perfil de conexión/nombre de grupo de usuarios. El protocolo principal se configura como IPsec. El 'Nombre para mostrar' de se muestra al usuario en la interfaz de usuario de Secure Client cuando se establece una conexión con este perfil de conexión.

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) FTD1-IPSEC

FQDN or IP A... User Group

ftd1[redacted].com / IKEV2

Group URL

Connection Information

Primary Protocol IPsec

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address

Add

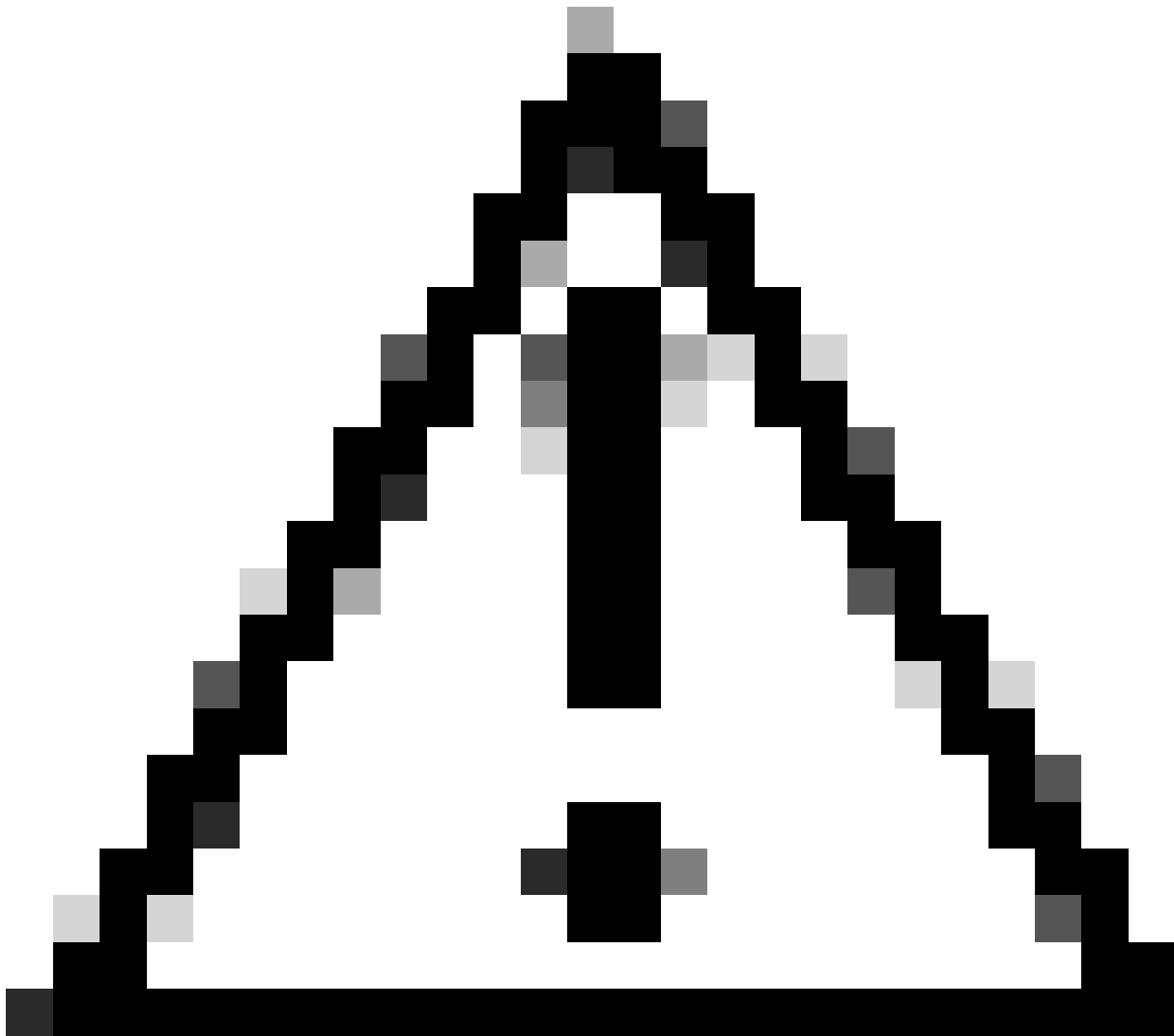
Move Up

Move D...

Delete

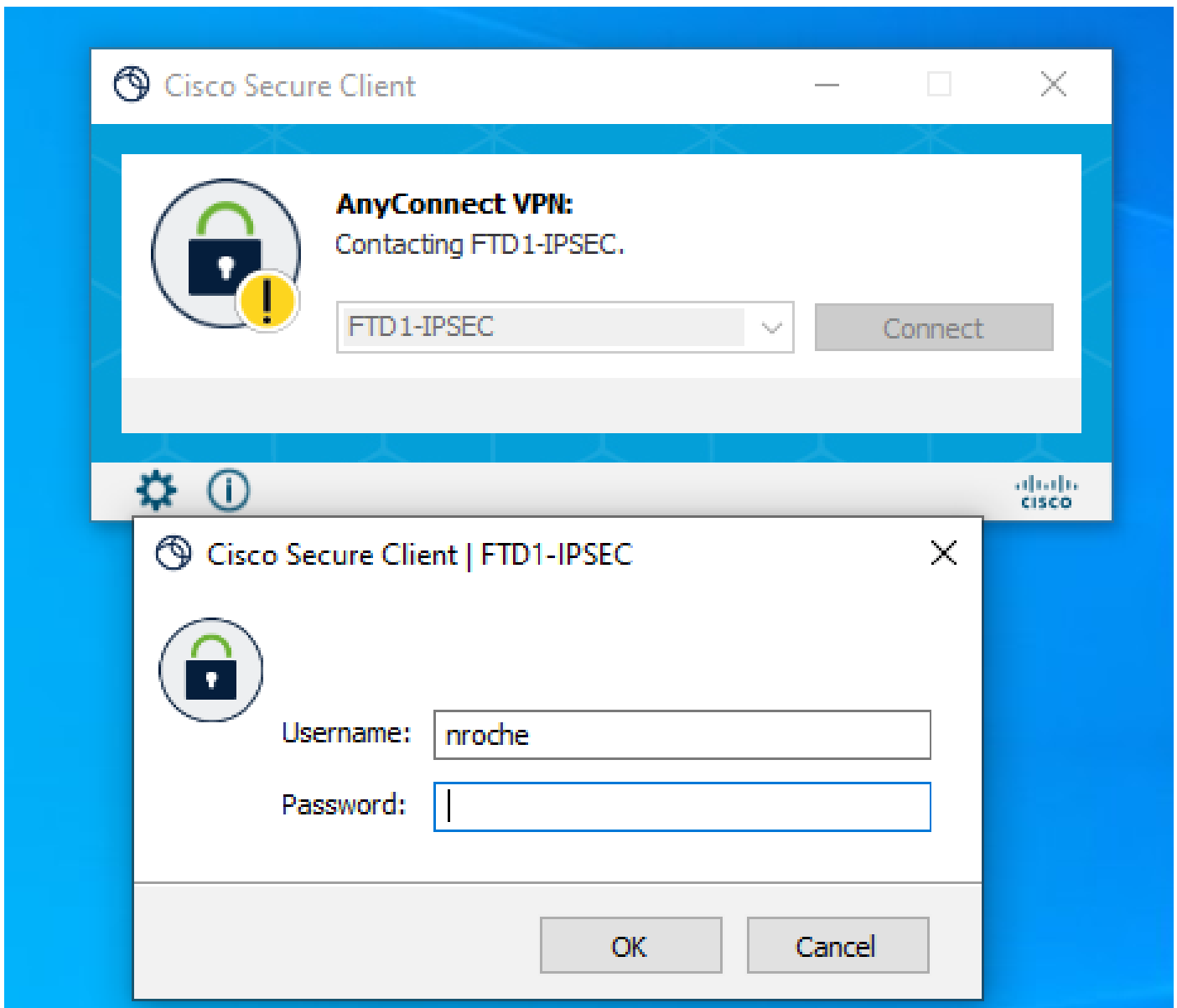
OK Cancel

Edite el perfil XML de modo que el protocolo principal sea IPsec y el grupo de usuarios coincida con el nombre del perfil de conexión.



Precaución: se requiere una conexión SSL para enviar perfiles XML al cliente desde el firewall. Cuando sólo se utiliza IKEV2-IPsec, los perfiles XML deben enviarse a los clientes mediante un método fuera de banda.

Una vez que el perfil XML se envía al cliente, Secure Client utiliza el grupo de usuarios del perfil XML para conectarse al perfil de conexión IKEV2-IPsec.



Vista de IU de cliente seguro del intento de conexión RAVPN IPsec-IKEv2.

Ejemplos de Configuración de ASA

Deshabilitar la autenticación AAA en los perfiles de conexión DefaultWEBVPNGroup y DefaultRAGroup

Ingrese la sección webvpn-attributes para el grupo de túnel DefaultWEBVPNGroup y especifique la autenticación como basada en certificados. Repita este proceso para DefaultRAGroup. Los usuarios que acceden a estos perfiles de conexión predeterminados se ven obligados a presentar un certificado para su autenticación y no se les da la oportunidad de introducir credenciales de nombre de usuario y contraseña.

```
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
```

Desactivar la posición de HostScan / Firewall seguro en DefaultWEBVPNGroup y DefaultRAGroup (opcional)

Esto sólo es necesario si su entorno dispone de una posición de Hostscan/Secure Firewall. Este paso evita que los atacantes aumenten la utilización de recursos en el firewall provocada por el proceso de análisis de terminales. Ingrese la sección webvpn-attributes para los perfiles de conexión y DefaultWEBVPNGroup y DefaultRAGroup e implemente without-csd para inhabilitar la funcionalidad de escaneo del extremo.

```
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
```

Desactivar alias de grupo y activar URL de grupo

Introduzca los grupos de túnel a los que se conectan los usuarios. Si existe un alias de grupo, inhabílitelo o quítelo. En este ejemplo está inhabilitado. Una vez que se haya completado, cree una url de grupo usando el FQDN o la dirección IP de la interfaz de terminación de RAVPN. El nombre en el extremo del group-url debe ser oscuro. Evite los valores comunes como VPN, AAA, RADIUS y LDAP, ya que facilitan a los atacantes adivinar la URL completa si obtienen el FQDN. En su lugar, utilice nombres significativos internamente que le ayuden a identificar el grupo de túnel.

```
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
```

Asignación de certificados

En el modo de configuración global, cree un mapa de certificado y asígnele un nombre y un número de secuencia. A continuación, defina una regla con la que los usuarios deben coincidir para utilizar la asignación. En este ejemplo, los usuarios tendrían que coincidir con los criterios de

un valor de nombre común que sea igual a "customvalue". A continuación, introduzca la configuración de webvpn y aplique el mapa de certificado al grupo de túnel deseado. Una vez completado, ingrese el DefaultWEBVPNGroup y haga de este grupo de túnel el predeterminado para los usuarios que no pasen la asignación de certificados. Si los usuarios no superan la asignación, se les dirige al DefaultWEBVPNGroup. Mientras que DefaultWEBVPNGroup está configurado con autenticación de certificados, los usuarios no tienen la opción de pasar credenciales de nombre de usuario o contraseña.

```
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

En el modo de configuración global, puede editar una política de grupo existente o crear una nueva e introducir los atributos para dicha política de grupo. Una vez que esté en la sección de atributos, habilite IKEv2 como el único protocolo de túnel VPN. Asegúrese de que esta política de grupo esté vinculada a un grupo de túnel que se va a utilizar para las conexiones VPN de acceso remoto IPsec-IKEV2. De forma similar a los pasos de FMC, debe editar el perfil XML a través del Editor de perfiles VPN o el Editor de perfiles ASA y cambiar el campo User Group (Grupo de usuarios) para que coincida con el nombre del grupo de túnel en ASA, y cambiar el protocolo a 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
```

En el Editor de perfiles VPN, o el Editor de perfiles ASA, vaya a la pestaña Lista de servidores. El nombre del grupo de usuarios DEBE coincidir exactamente con el nombre del perfil de conexión del firewall. El protocolo principal se configura como IPsec. El nombre para mostrar se muestra al usuario en la interfaz de usuario de Secure Client al establecer una conexión con este perfil de conexión.

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) ASA-IPsec

FQDN or IP A... User Group

FQDN TG-NAME

Group URL

FQDN/TG-NAME

Connection Information

Primary Protocol IPsec

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address

Add

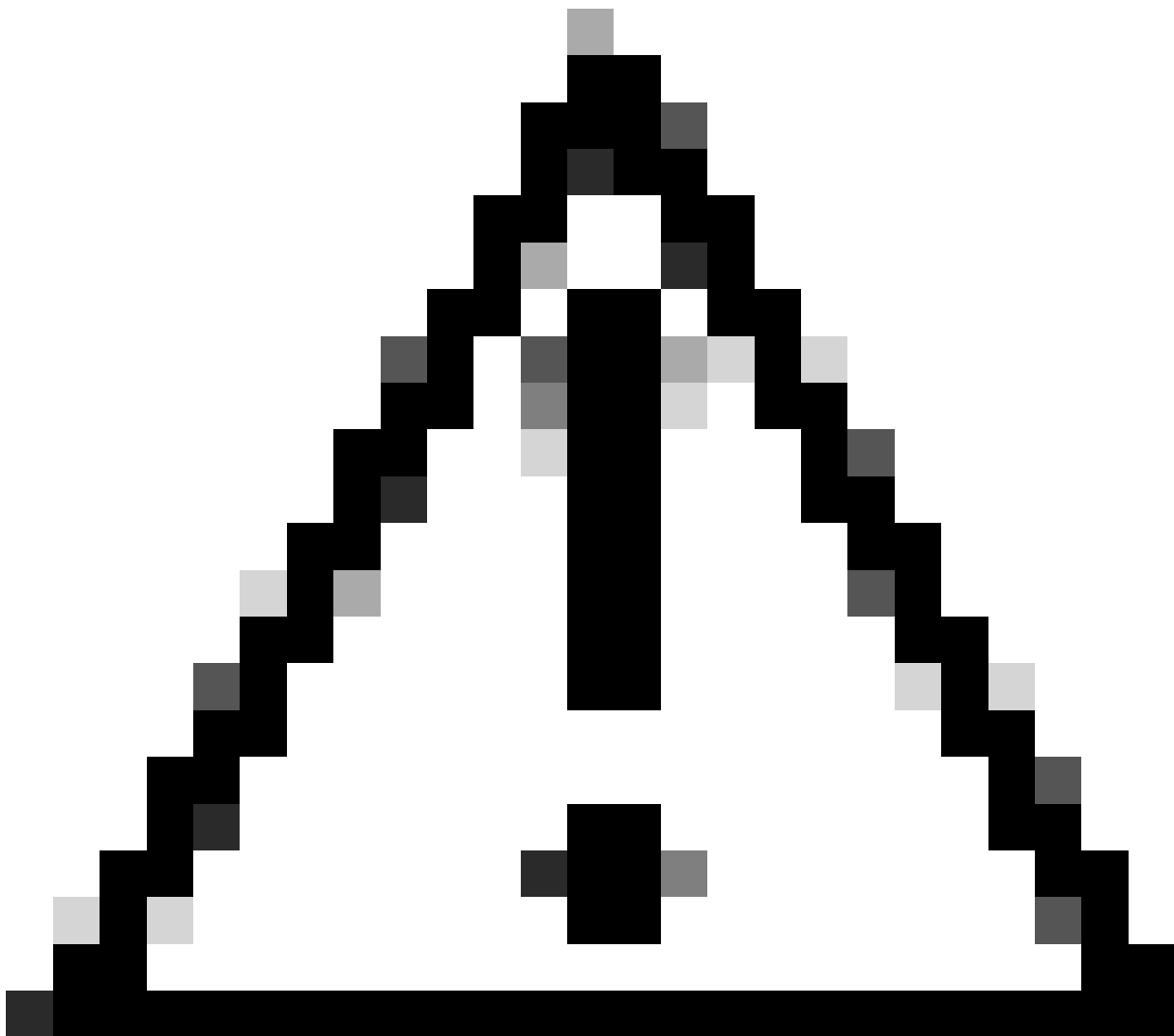
Move Up

Move D...

Delete

OK Cancel

Edite el perfil XML de modo que el nombre del protocolo principal sea IPsec y el nombre del grupo de usuarios coincida con el nombre del grupo de túnel del ASA para las conexiones RAVPN IPsec-IKEv2.



Precaución: se requiere una conexión SSL para enviar perfiles XML al cliente desde el firewall. Cuando sólo se utiliza IKEV2-IPsec, los perfiles XML deben enviarse a los clientes mediante un método fuera de banda.

Conclusión

En resumen, el propósito de las prácticas de endurecimiento de este documento es asignar usuarios legítimos a perfiles de conexión personalizados mientras los atacantes se ven obligados a usar DefaultWEBVPGGroup y DefaultRAGroup. En una configuración optimizada, los dos perfiles de conexión predeterminados no tienen ninguna configuración de servidor AAA personalizada legítima. Además, la eliminación de alias de grupo evita que los atacantes identifiquen fácilmente perfiles de conexión personalizados al eliminar la visibilidad desplegable al navegar al FQDN o la dirección IP pública del firewall.

Información Relacionada

[Soporte técnico y descargas de Cisco](#)

[Ataques por pulverización de contraseña](#)

[Unauthorized Access Vulnerability, septiembre de 2023](#)

[Guías de configuración de ASA](#)

[Guías de configuración de FMC/FDM](#)

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).