

實施安全客戶端AnyConnect VPN的強化措施

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[概念](#)

[思科安全防火牆上的安全客戶端強化實踐：](#)

[使用日誌記錄和系統日誌ID辨識攻擊](#)

[攻擊驗證](#)

[FMC配置示例](#)

[停用DefaultWEBVPNGroup和DefaultRAGroup連線配置檔案中的AAA身份驗證](#)

[在DefaultWEBVPNGroup和DefaultRAGroup上停用Hostscan/安全防火牆狀態（可選）](#)

[停用組別名並啟用組URL](#)

[憑證對應](#)

[IPsec-IKEv2](#)

[ASA配置示例](#)

[停用DefaultWEBVPNGroup和DefaultRAGroup連線配置檔案中的AAA身份驗證](#)

[在DefaultWEBVPNGroup和DefaultRAGroup上停用Hostscan/安全防火牆狀態（可選）](#)

[停用組別名並啟用組URL](#)

[憑證對應](#)

[IPsec-IKEv2](#)

[結論](#)

[相關資訊](#)

簡介

本文檔介紹如何提高遠端訪問VPN實施的安全性。

必要條件

需求

思科建議您瞭解以下主題：

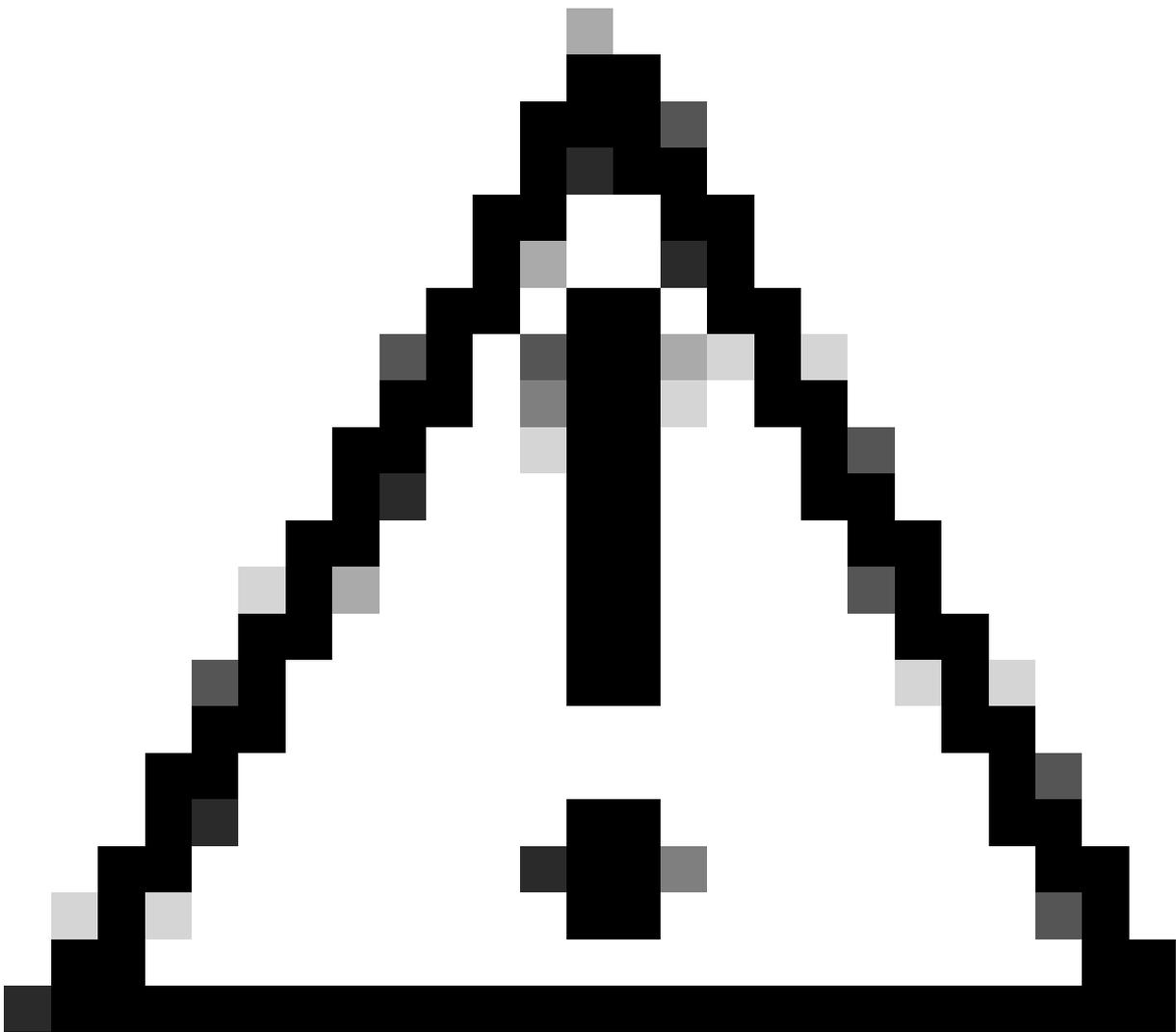
- 思科安全客戶端AnyConnect VPN。
- ASA/FTD遠端訪問配置。

採用元件

最佳實踐指南基於以下硬體和軟體版本：

- Cisco ASA 9.x
- Firepower威脅防禦7.x/FMC 7.x

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。



注意：本文檔不包含Firepower裝置管理器(FDM)的步驟。FDM僅支援變更DefaultWEBVPNGroup上的驗證方法。請使用控制平面ACL，或在FDM UI中的遠端訪問VPN「全局設定」部分中使用自定義埠。如果需要，請聯絡Cisco技術支援中心(TAC)以獲取進一步幫助。

背景資訊

本文檔的目的是確保Cisco安全客戶端AnyConnect VPN配置在網路安全攻擊司空見慣的現代世界中遵循安全最佳實踐。

暴力攻擊通常涉及使用使用者名稱和密碼組合反覆嘗試訪問資源。攻擊者嘗試使用他們的網際網路瀏覽器、安全客戶端使用者介面或其他工具輸入多個使用者名稱和密碼，希望它們與AAA資料庫中的合法組合相匹配。使用AAA進行身份驗證時，我們期望終端使用者輸入其使用者名稱和密碼，因為這對於建立連線是必要的。同時，在使用者輸入其認證之前，我們不會驗證其身份。從本質上講，這使得攻擊者能夠利用以下場景：

1. 已公開Cisco Secure Firewall的完全限定域名（特別是在連線配置檔案中使用組別名時）：
 - 如果攻擊者發現VPN防火牆的FQDN，則他們可以選擇使用要啟動暴力攻擊的組別名選擇隧道組。
2. 使用AAA或本地資料庫配置的預設連線配置檔案：
 - 如果攻擊者找到VPN防火牆的FQDN，他們可能會嘗試對AAA伺服器或本地資料庫進行暴力攻擊。出現這種情況是因為與FQDN的連線位於預設連線配置檔案上，即使未指定組別名也是如此。
3. 防火牆或AAA伺服器上的資源耗盡：
 - 攻擊者可透過傳送大量身份驗證請求和建立拒絕服務(DoS)條件來壓垮AAA伺服器或防火牆資源。

概念

Group-Aliases：

- 防火牆用來參照連線設定檔的替代名稱。啟動與防火牆的連線後，這些名稱將顯示在Secure Client UI的下拉選單中，供使用者選擇。刪除group-aliases會刪除Secure Client UI中的下拉功能。

組URL：

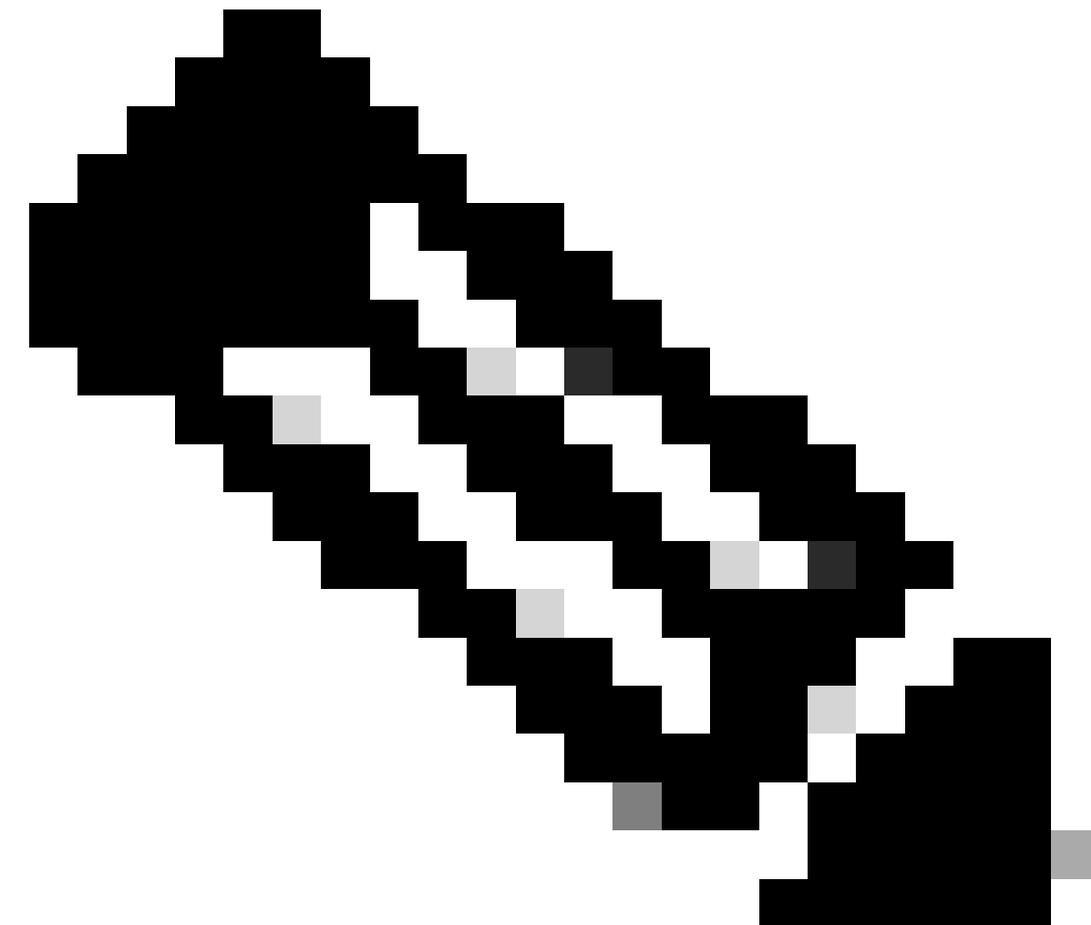
- 可連結至連線設定檔的URL，以便將傳入連線直接對應至所需的連線設定檔。沒有下拉功能，因為使用者可以在安全客戶端UI中輸入完整的URL，或者可以將URL與XML配置檔案中的「顯示名稱」整合，以向使用者隱藏URL。

此處不同之處在於，當實現組別名時，使用者啟動連線到 `vpn_gateway.example.com`，並顯示別名以選擇將它們驅動到連線配置檔案。使用group-URL，使用者啟動到 `vpn_gateway.example.com/example_group` 的連線，然後將其直接驅動到連線配置檔案，而無需下拉選單或下拉選單的選項。

思科安全防火牆上的安全客戶端強化實踐：

這些方法依賴於將合法使用者對映到正確的隧道組/連線配置檔案，同時將潛在惡意使用者傳送到陷阱隧道組，我們將此陷阱隧道組配置為不允許使用者名稱和密碼組合。雖然並非必須實作所有組合，但若要让建議有效運作，就必須停用群組別名並變更DefaultWEBVPNGroup和DefaultRAGroup的驗證方法。

- 停用組別名，並且僅在連線配置檔案配置中使用group-url，這使您具有特定FQDN，攻擊者無法輕易發現和選擇該FQDN，因為只有具有正確FQDN的客戶端才能啟動連線。例如vpn_gateway.example.com/example_group比vpn_gateway.example.com更難被攻擊者發現。
- 在DefaultWEBVPNGroup和DefaultRAGroup中停用AAA身份驗證並配置證書身份驗證，這樣可避免對本地資料庫或AAA伺服器執行暴力操作。此場景中的攻擊者嘗試連線時會立即看到錯誤。由於身份驗證基於證書，因此沒有使用者名稱或密碼欄位，從而停止暴力嘗試。另一種方案是建立不支援配置的AAA伺服器，為惡意請求建立漏洞。
- 利用連線設定檔的憑證對應。這允許傳入連線根據從客戶端裝置上的證書接收的屬性對映到特定連線配置檔案。具有正確證書的使用者被正確對映，而對映條件失敗的攻擊者被傳送到DefaultWEBVPNGroup。
- 使用IKEv2-IPSec而不是SSL會導致隧道組依賴XML配置檔案中的特定使用者組對映。如果終端使用者電腦上沒有此XML，則使用者將自動傳送到預設隧道組。



注意：有關組別名功能的詳細資訊，請參閱[ASA VPN配置指南](#)並觀察「表1」。SSL

VPN的連線配置檔案屬性」。

使用日誌記錄和系統日誌ID辨識攻擊

暴力攻擊是破壞遠端訪問VPN的主要方法，它利用弱密碼來獲取未經授權的訪問。瞭解如何使用日誌記錄和評估syslog來辨識攻擊跡象至關重要。常見的syslog ID可指示在遇到異常卷時發生的攻擊，這些系統日誌包括：

```
%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
```

在ASA上配置了no logging hide username命令之前，使用者名稱始終處於隱藏狀態。

注意：注意：如果有效的IP生成或獲知了有效的使用者，這可提供見解。但是，請謹慎使用，因為使用者名稱在日誌中可見。

Cisco ASA日誌記錄：

[安全ASA防火牆使用手冊](#)

《Cisco Secure Firewall ASA系列常規操作CLI配置指南》中的[日誌記錄](#)一章

Cisco FTD記錄：

[透過 FMC 設定 FTD 中的記錄](#)

Cisco Secure Firewall Management Center裝置配置指南的Platform Settings章節中的[Configure Syslog](#)部分

[在Firepower裝置管理器中配置和驗證系統日誌](#)

[Configuring System Logging Settings](#)部分（位於適用於Firepower裝置管理器的Cisco Firepower威脅防禦配置指南的系統設定章節中）

攻擊驗證

要進行驗證，請登入到ASA或FTD命令列介面(CLI)，運行show aaa-server命令，並調查嘗試和拒絕的任何已配置AAA伺服器的身份驗證請求的不尋常數量：

```
<#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#
```

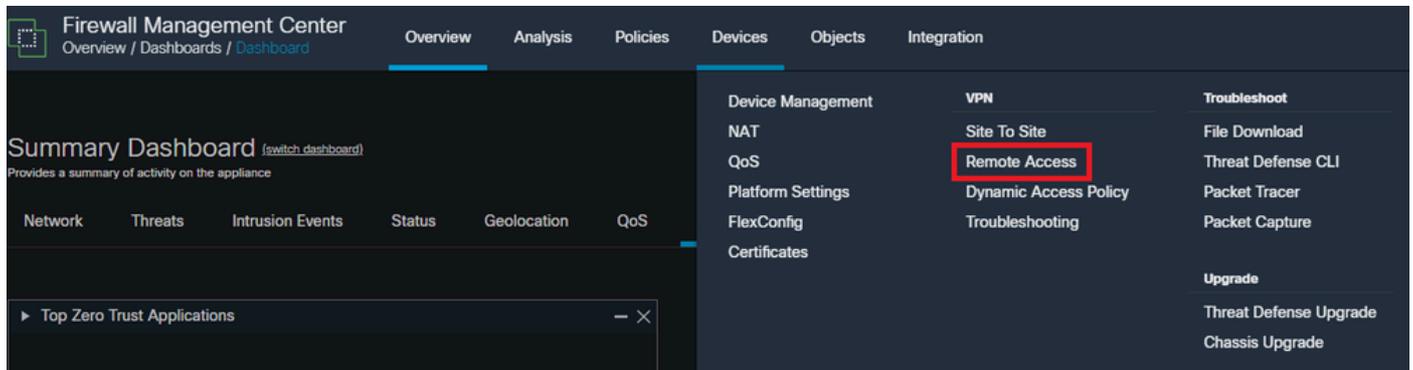
```
show aaa-server
```

```
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
```

FMC配置示例

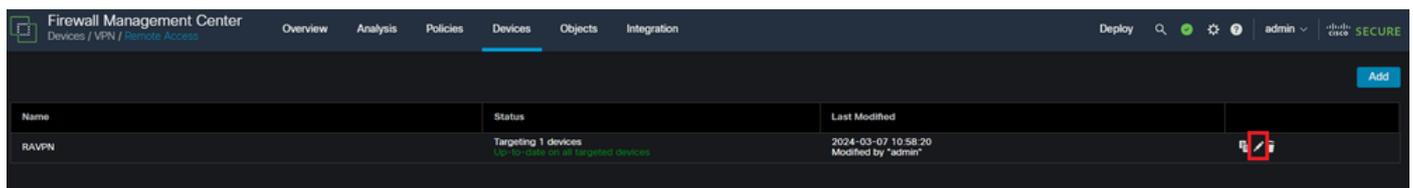
停用DefaultWEBVPNGroup和DefaultRAGroup連線配置檔案中的AAA身份驗證

導航到裝置>遠端訪問。



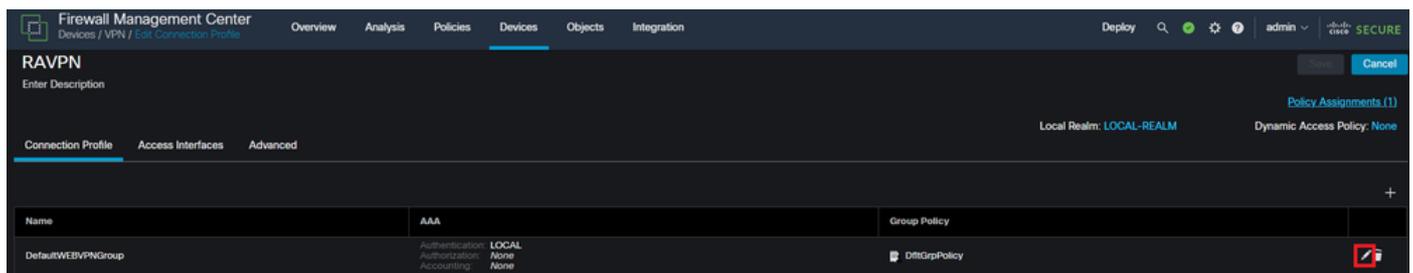
顯示導航FMC GUI以訪問遠端訪問VPN策略配置。

編輯現有的遠端訪問VPN策略並建立名為「DefaultRAGroup」的連線配置檔案



顯示如何在FMC UI中編輯遠端訪問VPN策略。

編輯名為「DefaultWEBVPNGroup」和「DefaultRAGroup」的連線配置檔案



顯示如何在FMC UI中編輯DefaultWEBVPNGroup。

導航到AAA頁籤並選擇Authentication Method下拉選單。選擇Client Certificate Only並選擇Save。

Edit Connection Profile

Connection Profile:* DefaultWEBVPNGroup

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

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: Client Certificate Only ▼

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

將FMC UI內DefaultWEBVPNGroup的驗證方法變更為使用者端憑證。

編輯DefaultRAGroup並導航到AAA頁籤並選擇Authentication Method下拉選單。選擇「Client Certificate Only」並選擇Save。

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

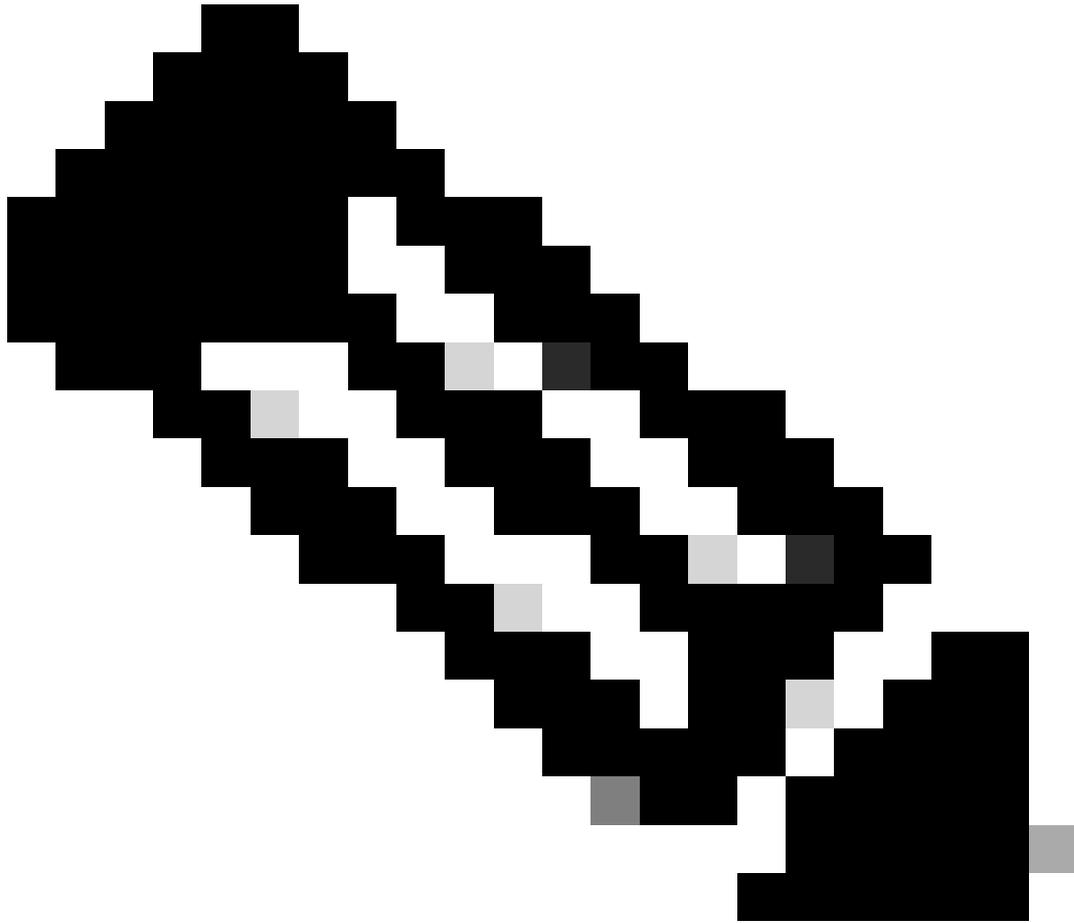
Accounting

Accounting Server:

Cancel

Save

將身份驗證方法更改為FMC UI中DefaultRAGroup的客戶端證書。

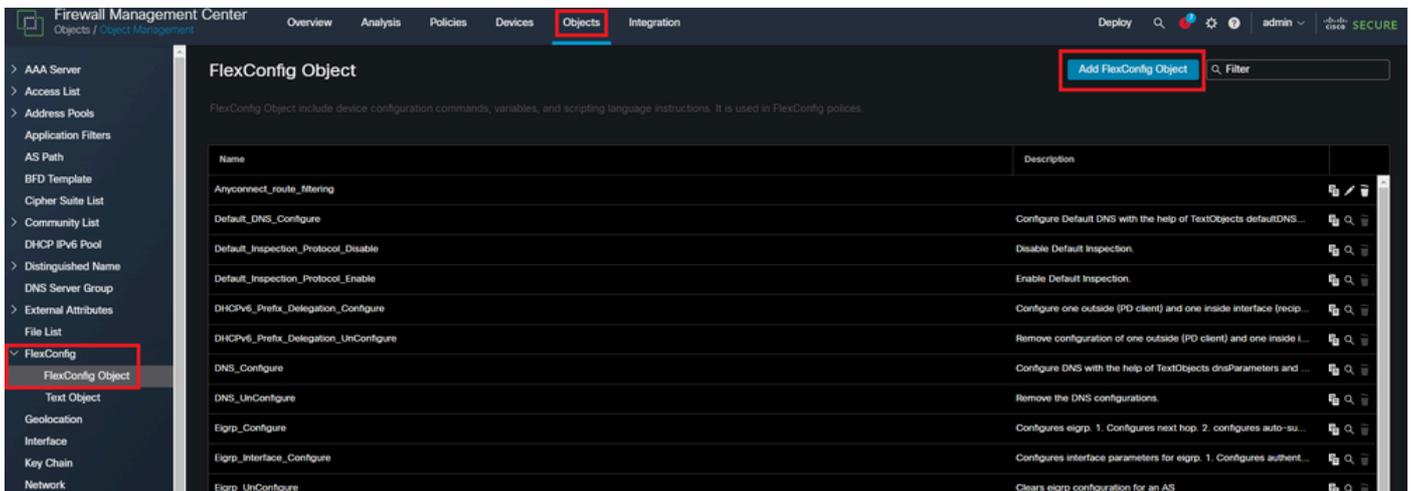


注意：身份驗證方法也可以是Sinkhole AAA伺服器。如果使用此方法，則AAA伺服器配置是虛假的，實際上不會處理任何請求。還必須在「Client Address Assignment」頁籤中定義VPN池以儲存更改。

在DefaultWEBVPNGroup和DefaultRAGroup上停用Hostscan/安全防火牆狀態（可選）

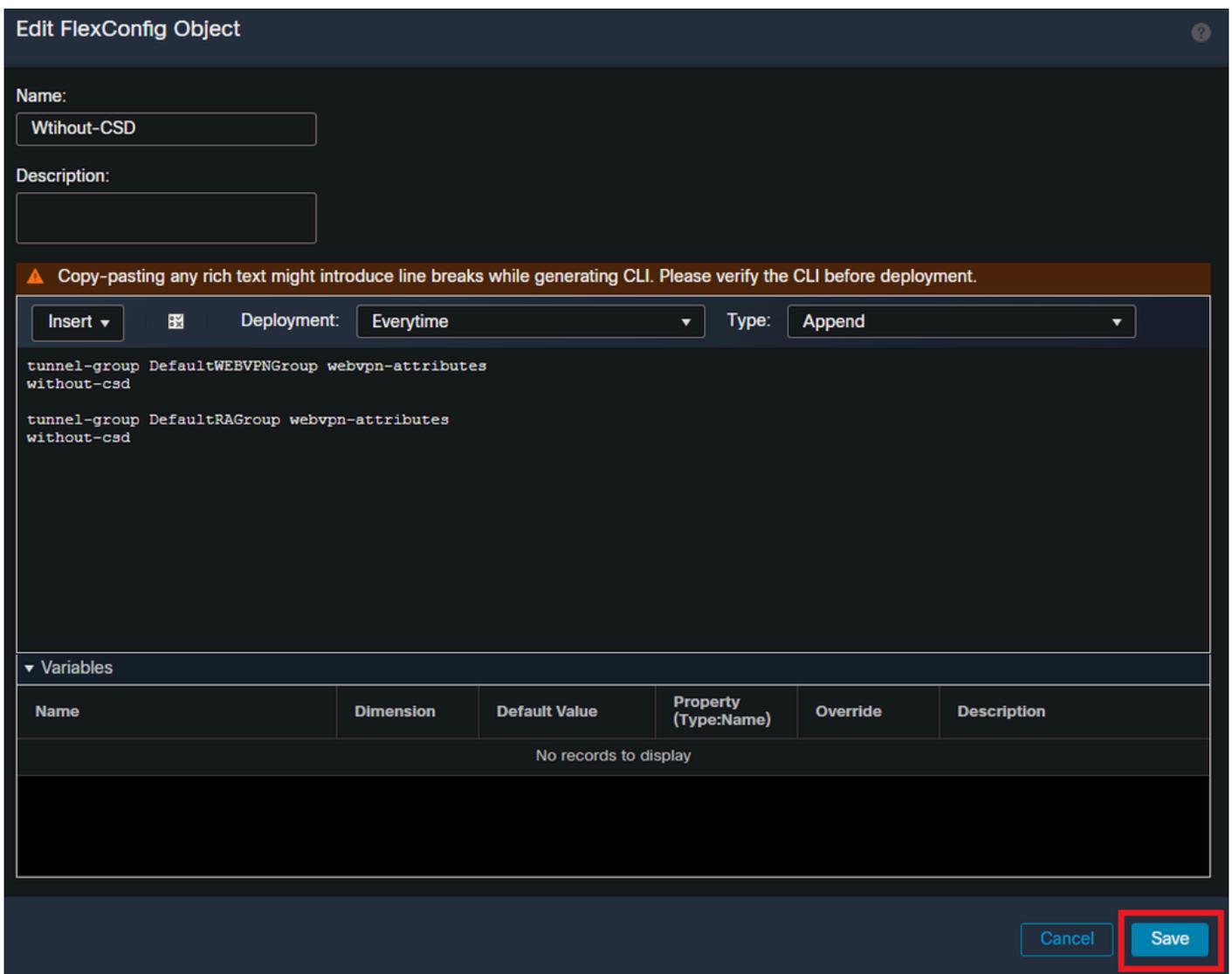
僅當您的環境中具有Hostscan/安全防火牆狀態時才需要執行此操作。此步驟可防止攻擊者增加由終端掃描進程引起的防火牆上的資源利用率。在FMC中，這是透過使用without-csd命令建立FlexConfig對象以停用終端掃描功能來實現的。

導覽至物件>物件管理> FlexConfig物件>新增FlexConfig物件。



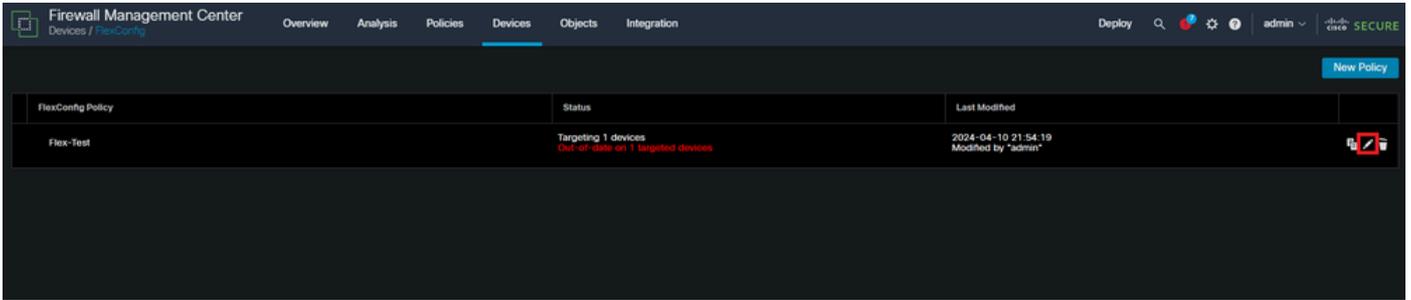
瀏覽FMC UI以建立FlexConfig物件。

為FlexConfig對象命名，將部署設定為Everytime，型別為Append。然後，完全按照所示輸入語法並儲存對象。



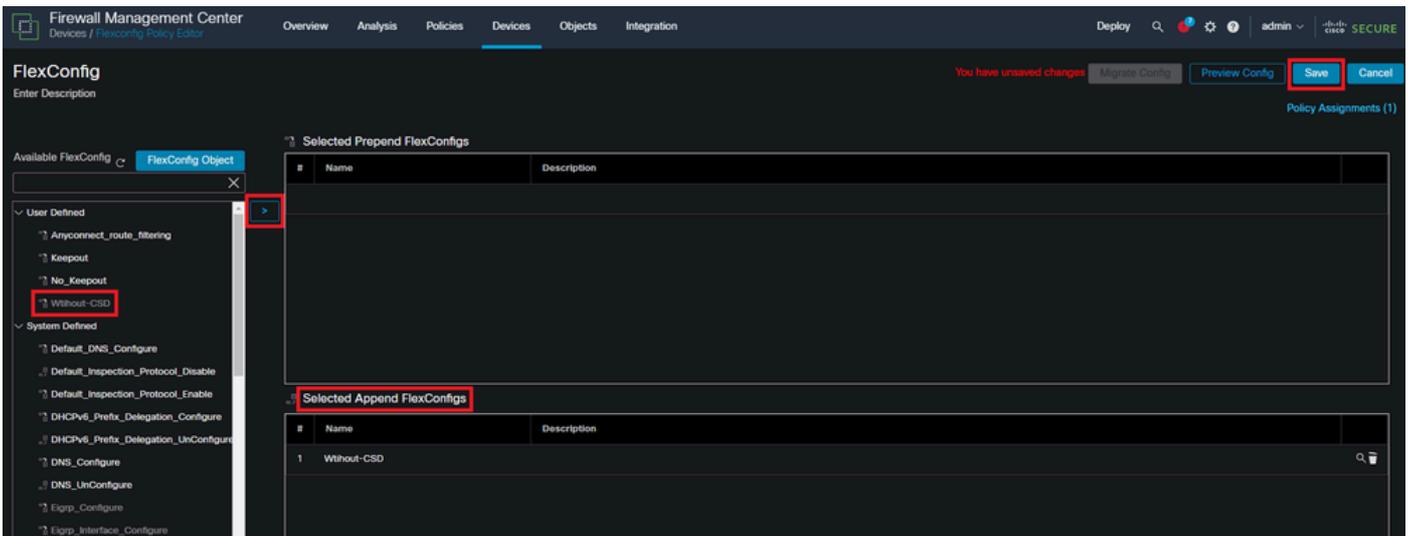
使用'without-csd'建立FlexConfig物件

導航到裝置 > FlexConfig，然後按一下鉛筆編輯FlexConfig策略。



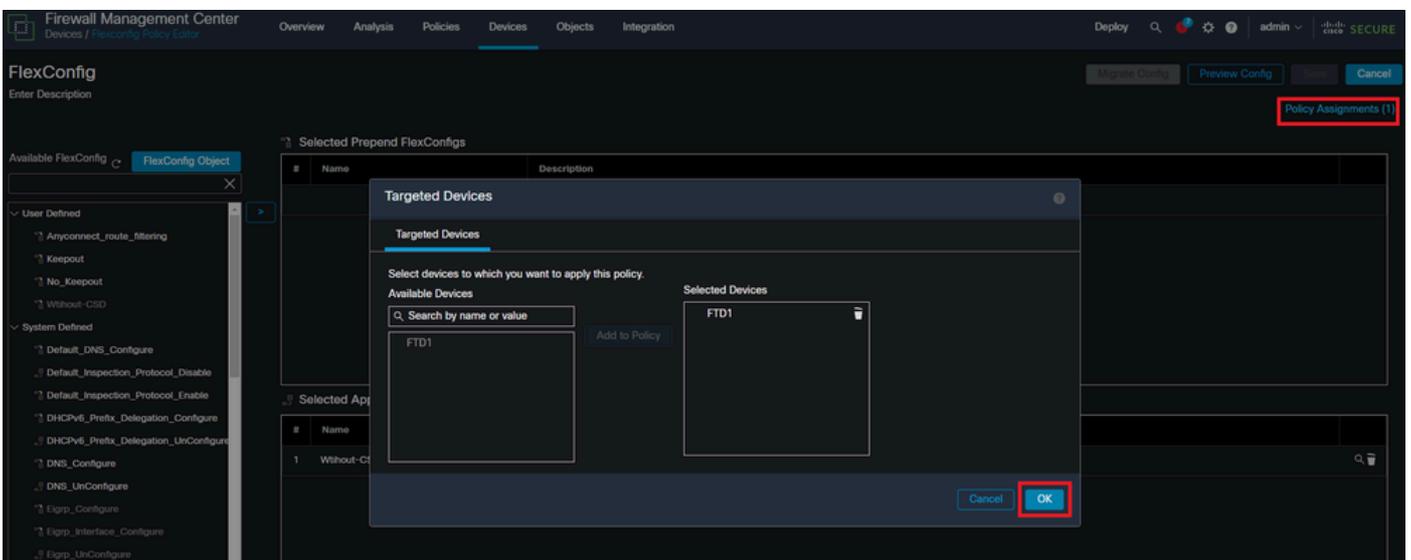
在FMC中編輯FlexConfig策略。

找到您從「使用者定義」區段建立的物件。然後，選擇箭頭將其增加到所選附加FlexConfigs。最後，選擇Save以儲存FlexConfig策略。



將FlexConfig對象附加到FlexConfig策略。

選擇策略分配，並選擇您要應用此FlexConfig策略的FTD，然後選擇確定。如果這是新的FlexConfig分配，請再次選擇Save，然後部署更改。部署後，驗證



將FlexConfig策略分配給FirePOWER裝置。

輸入FTD CLI並為DefaultWEBVPNGroup和DefaultRAGroup發出命令show run tunnel-group。驗證配置中現在是否存在without-csd。

```
<#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
```

停用組別名並啟用組URL

導航到連線配置檔案並選擇「別名」頁籤。停用或刪除組別名，然後按一下plus圖示增加URL別名

。

Edit Connection Profile

Connection Profile:* LDAP-TG

Group Policy:* DfitGrpPolicy +

[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	

在FMC UI中停用隧道組的組別名選項。

為URL別名配置對象名稱，並為URL填寫防火牆的FQDN和/或IP地址，後跟您希望與連線配置檔案關聯的名稱。在本例中，我們選擇「aaaldap」。越不清楚，安全性越高，因為即使攻擊者已經獲取您的FQDN，他們猜測完整URL的可能性也更低。完成後，選擇Save。

Edit URL Objects



Name

LDAP-ALIAS

Description

URL

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

Allow Overrides

Cancel

Save

在FMC UI中建立URL別名物件。

從下拉選單中選擇URL別名，選中Enabled框並選擇OK。

Add URL Alias



URL Alias:

LDAP-ALIAS



Enabled

Cancel

OK

確保在FMC UI中啟用URL別名。

確保刪除或停用了組別名，並檢查您的URL別名當前是否已啟用，然後選擇儲存。

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:

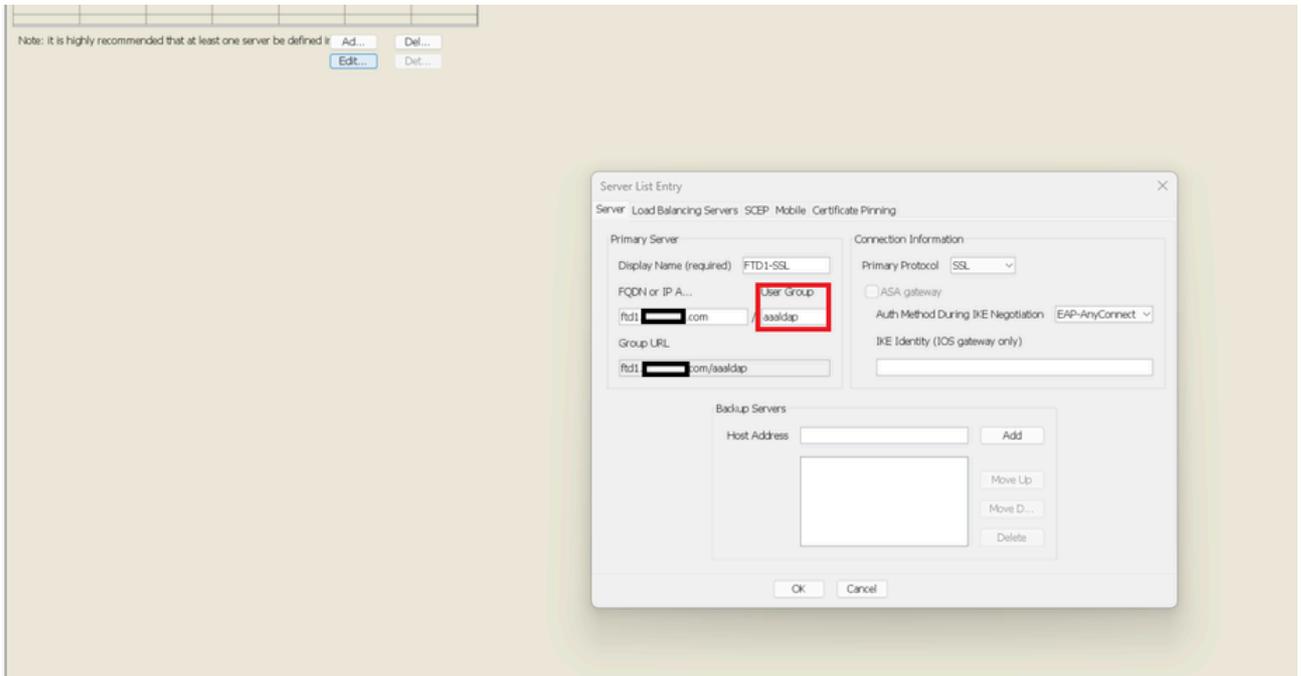
Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.

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

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

在FMC UI中啟用隧道組的URL-Alias選項。

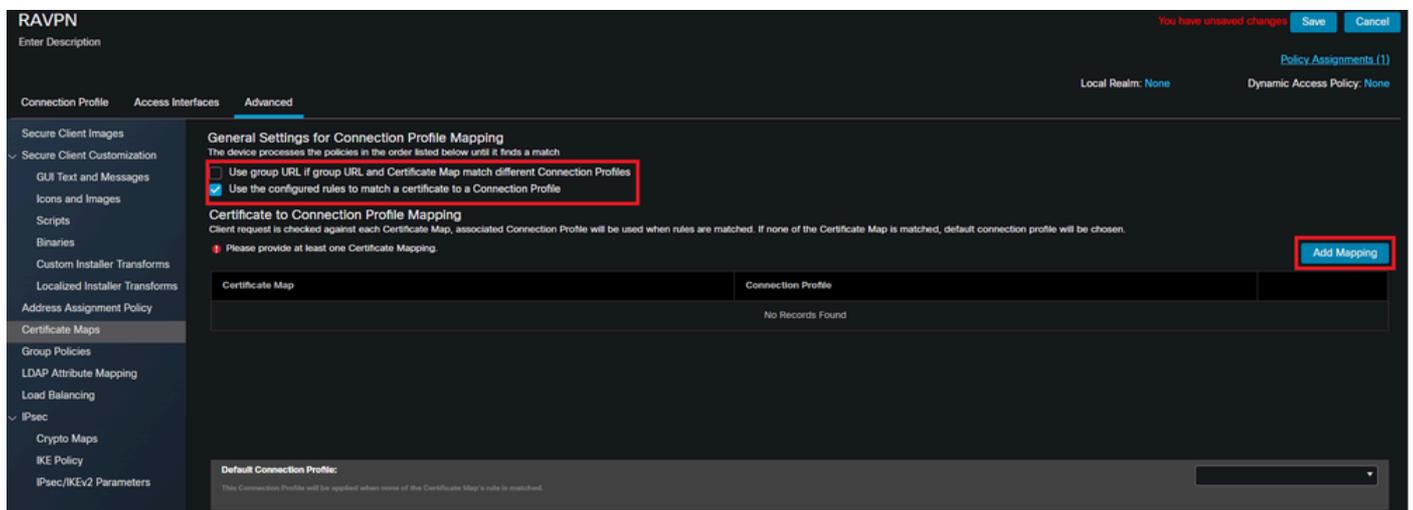
如果需要，也可以將URL別名推送為XML的一部分。這是透過使用VPN配置檔案編輯器或ASA配置檔案編輯器編輯XML來實現的。要完成此操作，請導航到Server List頁籤，並確保在使用SSL時User Group欄位與連線配置檔案的URL別名匹配。對於IKEv2，確保User Group欄位與連線配置檔案的確切名稱匹配。



編輯XML設定檔，使其具有SSL連線的URL別名。

憑證對應

導航到Remote Access VPN Policy中的Advanced頁籤。根據偏好設定選擇一般設定選項。選擇後，請選擇Add Mapping。



導航到FMC UI中的「高級」頁籤，在FMC UI中建立證書對映對象。

為證書對映對象命名並選擇Add Rule。在此規則中，定義您要標識的證書屬性以將使用者對映到特定連線配置檔案。完成後，選擇OK，然後選擇Save。

Add Certificate Map

Map Name*:
Certificate-Map-CN

Mapping Rule Add Rule
Configure the certificate matching rule

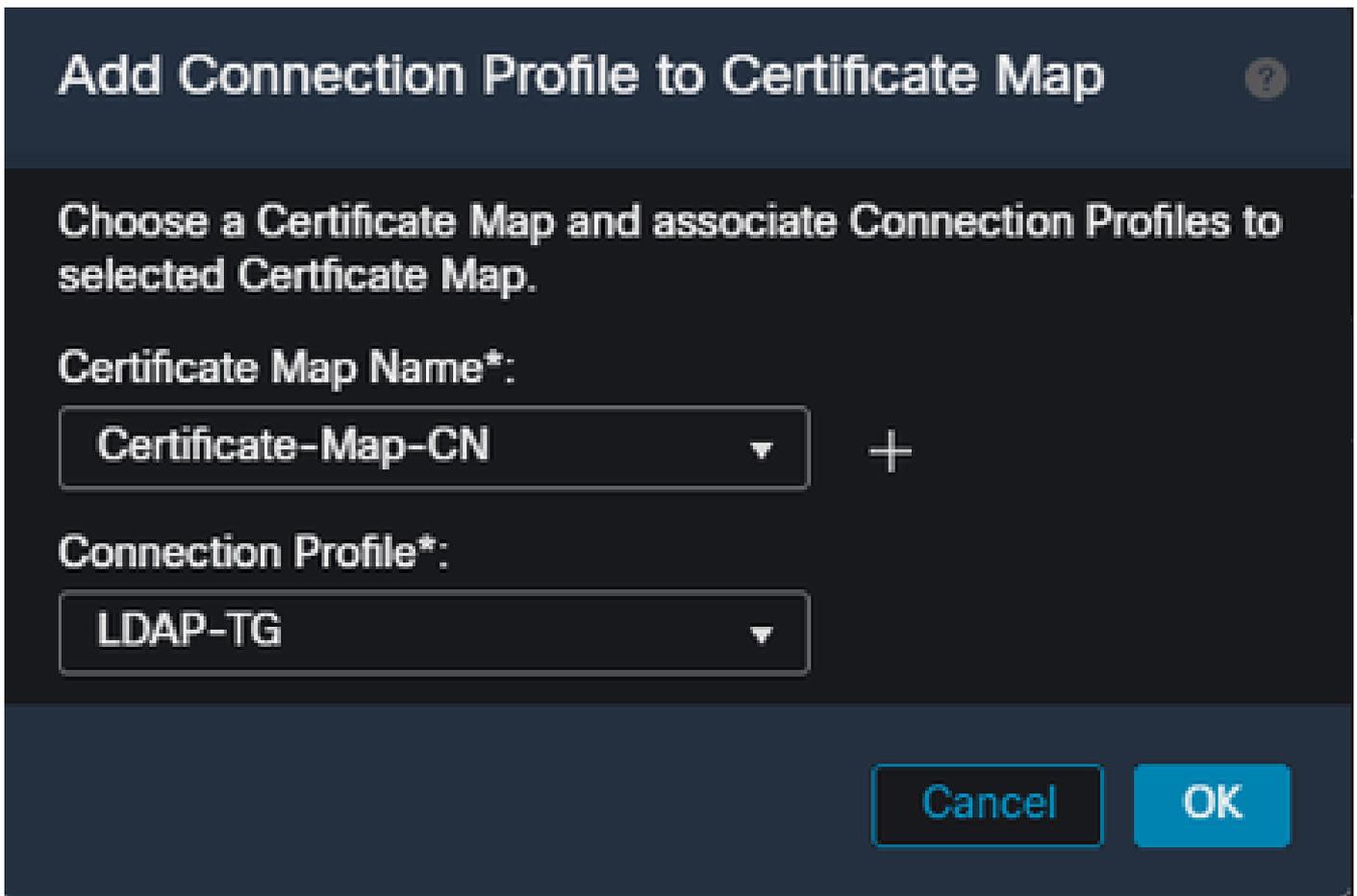
#	Field	Component	Operator	Value
1	Subject	CN (Common Name)	Equals	customvalue

OK Cancel

Cancel Save

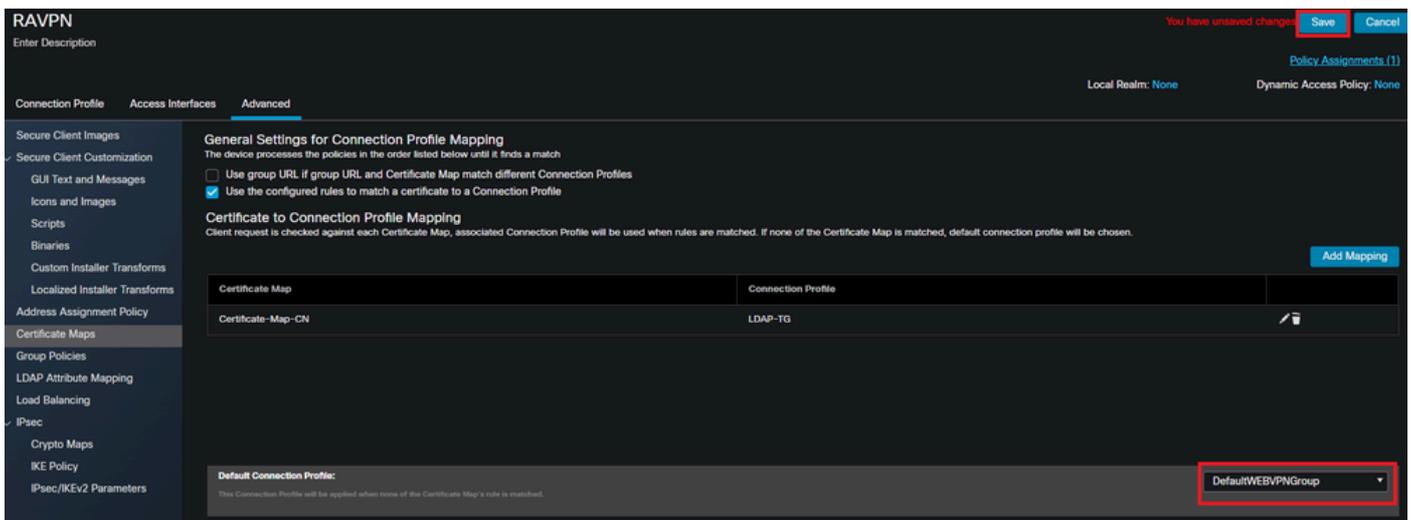
在FMC UI內建立證書對映並為對映增加條件。

從下拉選單中，選擇證書對映對象，以及希望與證書對映關聯的連線配置檔案。然後選擇OK。



將證書對映對象繫結到FMC UI中的所需隧道組。

確保將預設連線配置檔案配置為DefaultWEBVPNGroup，這樣，如果使用者對映失敗，則會將其傳送到DefaultWEBVPNGroup。完成後，選擇Save並部署更改。



更改證書對映到FMC UI中DefaultWEBVPNGroup的預設連線配置檔案。

IPsec-IKEv2

選擇所需的IPsec-IKEv2連線配置檔案，並導航到Edit Group Policy。

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	

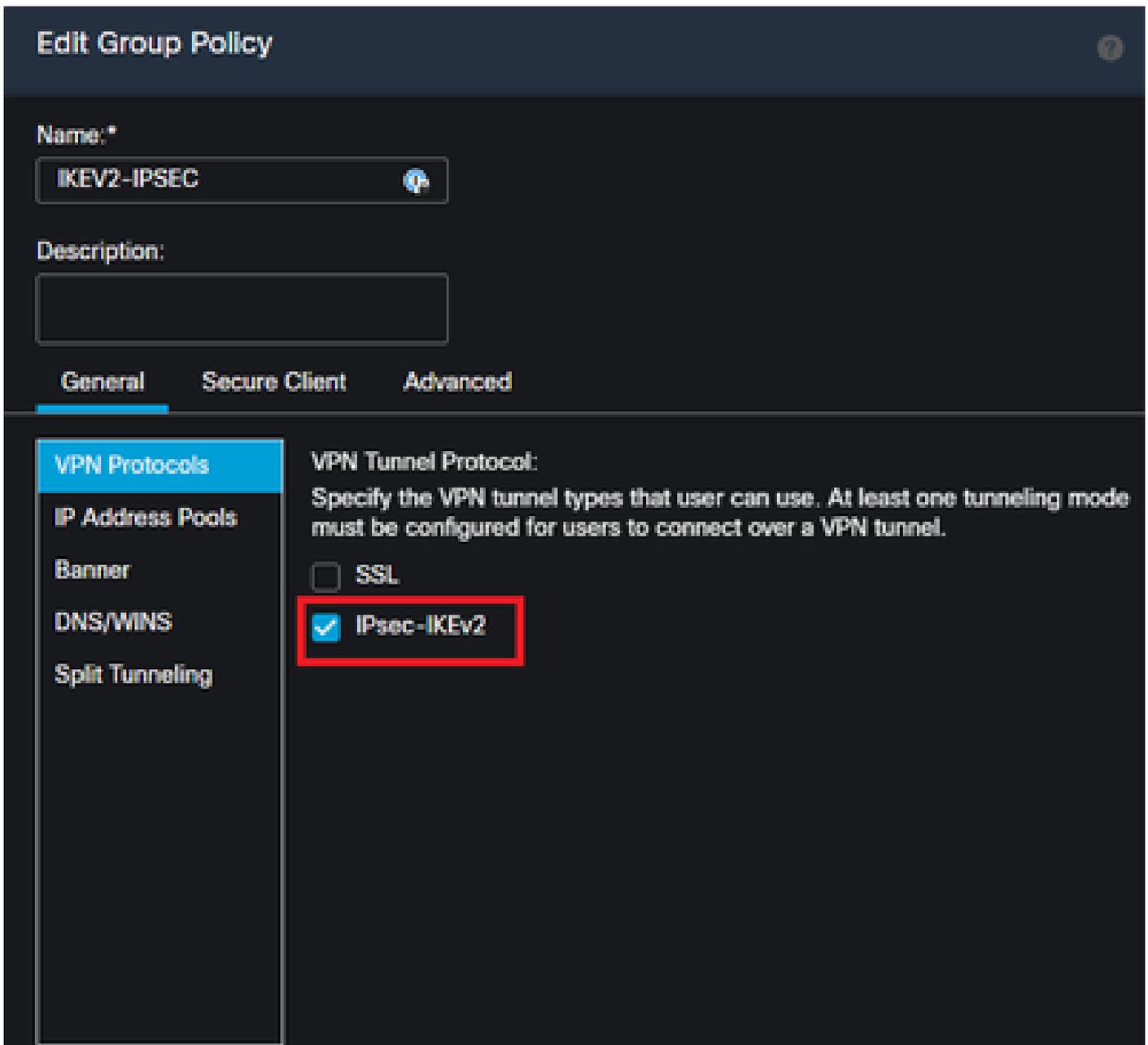
DHCP Servers: +

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

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

在FMC UI中編輯組策略。

在General頁籤中，導航到VPN Protocols部分並確保已選中IPsec-IKEv2框。



在FMC UI的組策略中啟用IPsec-IKEv2。

在VPN Profile Editor或ASA Profile Editor中，導航至Server List頁籤。使用者組名稱必須與防火牆上的連線配置檔名稱完全匹配。在本示例中，IKEV2是連線配置檔案/使用者組名稱。主協定配置為IPsec。當建立與此連線配置檔案的連線時，中的「顯示名稱」將顯示給安全客戶端UI中的使用者。

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) FTD1-IPSEC

FQDN or IP A... ftd1[redacted].com / User Group / 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 [text box] Add

[table area]

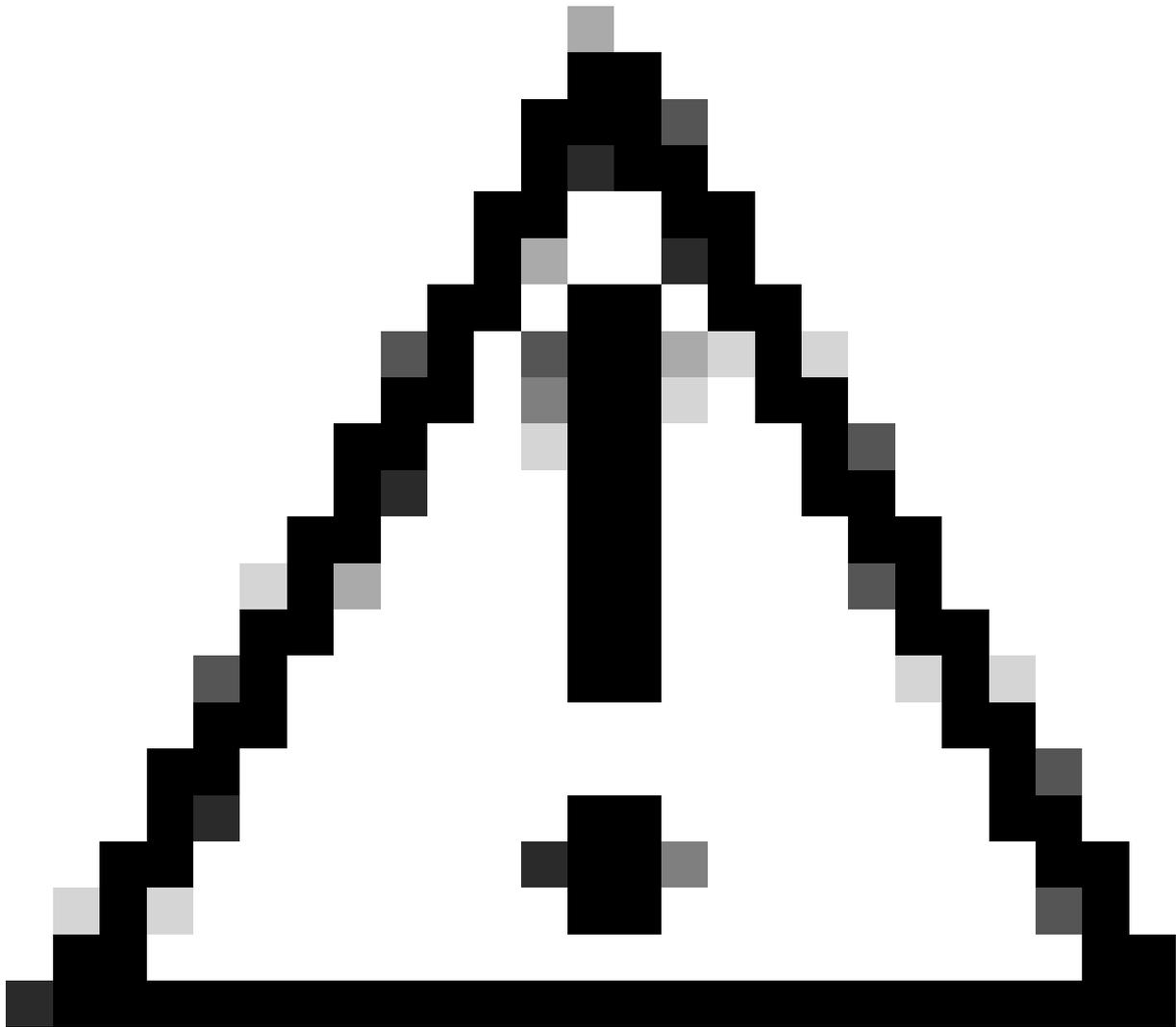
Move Up

Move D...

Delete

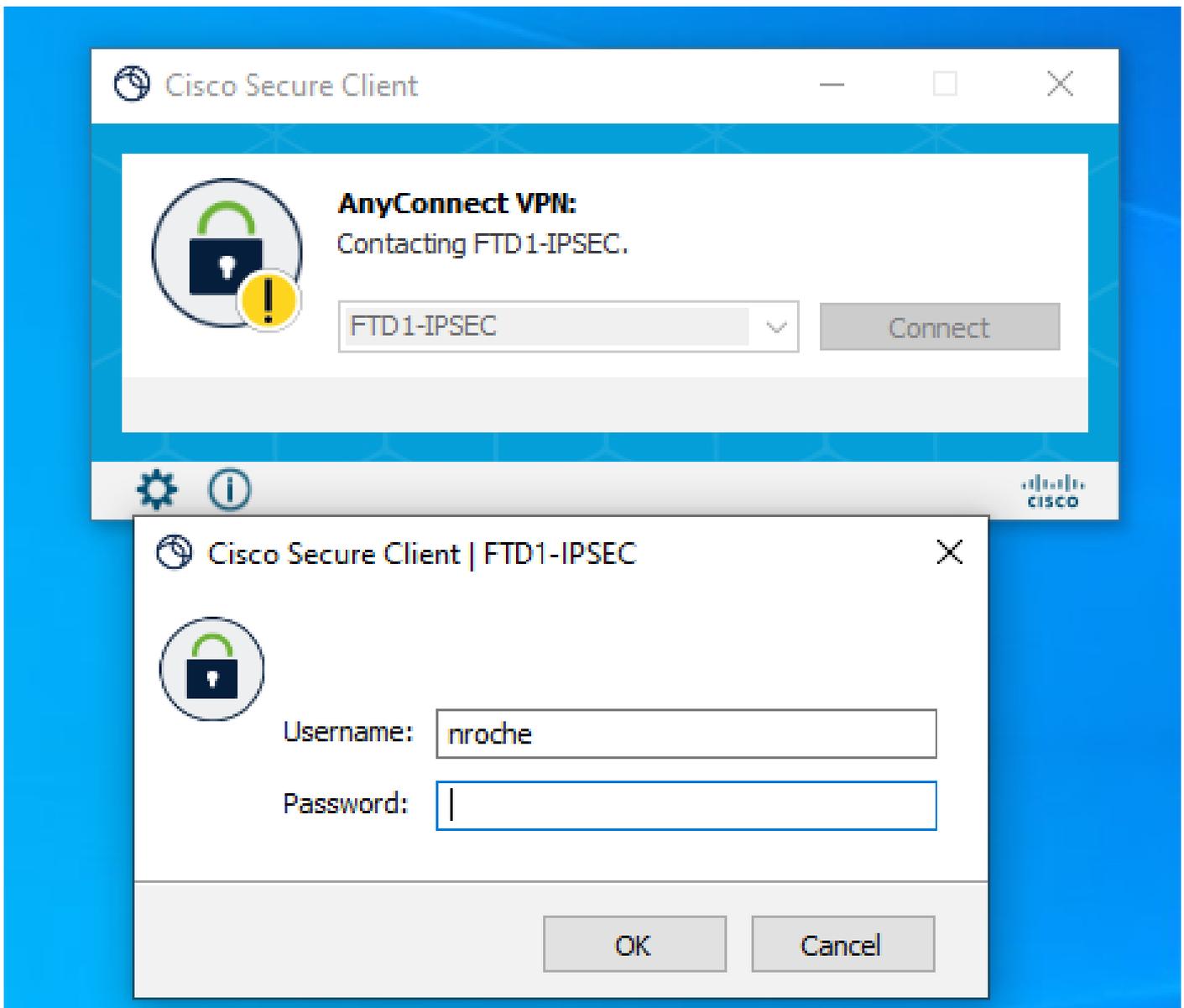
OK Cancel

編輯XML配置檔案，使主要協定為IPsec，並且使用者組與連線配置檔名稱匹配。



注意：需要SSL連線才能將XML配置檔案從防火牆推送到客戶端。如果僅使用IKEV2-IPsec，則必須透過帶外方法將XML配置檔案推送到客戶端。

將XML配置檔案推送到客戶端後，安全客戶端使用XML配置檔案中的使用者組連線到IKEV2-IPsec連線配置檔案。



IPsec-IKEv2 RAVPN連線嘗試的安全客戶端UI檢視。

ASA配置示例

停用DefaultWEBVPNGroup和DefaultRAGroup連線配置檔案中的AAA身份驗證

輸入tunnel-group DefaultWEBVPNGroup的webvpn-attributes部分並指定基於證書的身份驗證。對DefaultRAGroup重複此過程。登入這些預設連線設定檔的使用者必須出示驗證憑證，而且沒有機會輸入使用者名稱和密碼憑證。

```
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
```

在DefaultWEBVPNGroup和DefaultRAGroup上停用Hostscan/安全防火牆狀態（可選）

僅當您的環境中具有Hostscan/安全防火牆狀態時才需要執行此操作。此步驟可防止攻擊者增加由終端掃描進程引起的防火牆上的資源利用率。輸入DefaultWEBVPNGroup、DefaultRAGroup和連線配置檔案的webvpn-attributes部分並實現without-csd以停用端點掃描功能。

```
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
```

停用組別名並啟用組URL

輸入使用者要連線的隧道組。如果有現有的群組別名，請將其停用或移除。在本範例中，它處於停用狀態。完成後，使用RAVPN終止介面的FQDN或IP地址建立一個group-url。group-url末尾的名稱需要遮蔽。避免使用VPN、AAA、RADIUS、LDAP等通用值，因為這些值使攻擊者更容易在獲取FQDN的情況下猜測完整URL。相反，應使用內部有效名稱來幫助您辨識隧道組。

```
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
```

憑證對應

在全局配置模式下，建立證書對映並為其分配名稱和序列號。然後，定義使用者必須匹配的規則，以利用對映。在此範例中，使用者必須符合等於「customvalue」的通用名稱值的條件。接下來，輸入webvpn配置並將證書對映應用於所需的隧道組。完成後，請輸入DefaultWEBVPNGroup，並將此隧道組設定為證書對映失敗使用者的預設設定。如果使用者對映失敗，則會將其定向到DefaultWEBVPNGroup。當DefaultWEBVPNGroup設定為憑證驗證時，使用者沒有傳遞使用者名稱或密碼憑證的選項。

```
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

在全局配置模式下，您可以編輯現有組策略或建立新組策略並輸入該組策略的屬性。進入 attributes 部分後，啟用IKEv2作為唯一的vpn隧道協定。確保此組策略繫結到將用於IPsec-IKEV2遠端訪問VPN連線的隧道組。與FMC步驟相似，您必須透過VPN配置檔案編輯器或ASA配置檔案編輯器編輯XML配置檔案，並更改User Group欄位以匹配ASA上的隧道組的名稱，然後將協定更改為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
```

在VPN Profile Editor或ASA Profile Editor中，導航至Server List頁籤。使用者組名稱必須與防火牆上的連線配置檔名稱完全匹配。主協定配置為IPsec。建立與此連線設定檔的連線時，在Secure Client UI中向使用者顯示顯示名稱。

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

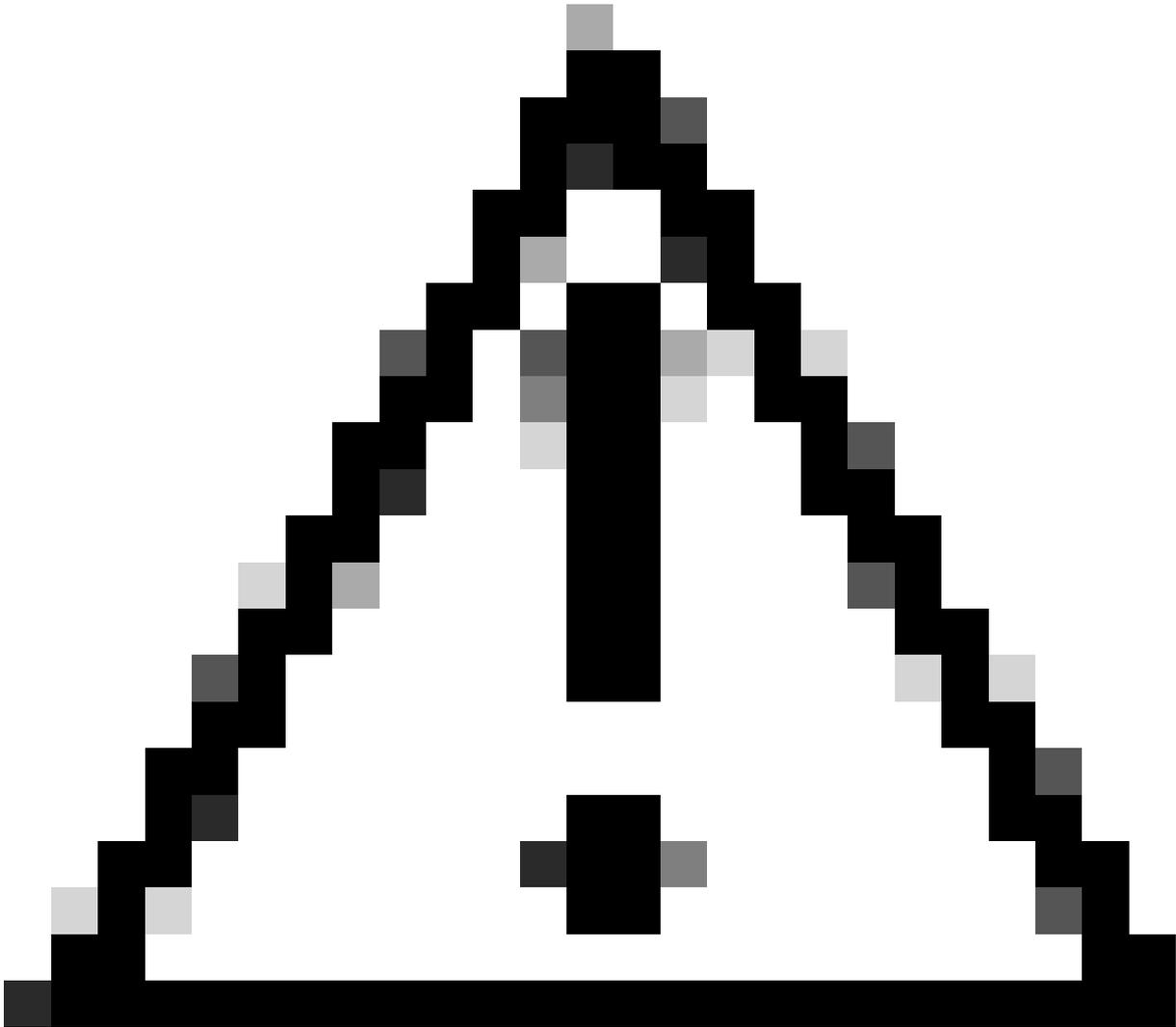
Move Up

Move D...

Delete

OK Cancel

編輯XML配置檔案，使主要協定名稱為IPsec，使用者組名稱與ASA的IPsec-IKEv2 RAVPN連線隧道組名稱匹配。



注意：需要SSL連線才能將XML配置檔案從防火牆推送到客戶端。如果僅使用IKEV2-IPsec，則必須透過帶外方法將XML配置檔案推送到客戶端。

結論

總之，本文檔中加強實踐的目的是將合法使用者對映到自定義連線配置檔案，同時攻擊者被強制使用DefaultWEBVPNGroup和DefaultRAGroup。在最佳化配置中，兩個預設連線配置檔案沒有任何合法的自定義AAA伺服器配置。此外，刪除組別名可防止攻擊者透過在導航到防火牆的FQDN或公共IP地址時刪除下拉可見性來輕鬆辨識自定義連線配置檔案。

相關資訊

[Cisco技術支援和下載](#)

[密碼噴霧攻擊](#)

[未經授權的訪問漏洞2023年9月](#)

[ASA配置指南](#)

[FMC/FDM組態指南](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。