

보안 클라이언트 AnyConnect VPN에 대한 강화 조치 구현

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[개념](#)

[Cisco Secure Firewall의 보안 클라이언트 강화 사례:](#)

[로그 및 Syslog ID를 사용하여 공격 식별](#)

[공격 확인](#)

[FMC 컨피그레이션 예](#)

[DefaultWEBVPNGroup 및 DefaultRAGroup 연결 프로파일에서 AAA 인증 비활성화](#)

[DefaultWEBVPNGroup 및 DefaultRAGroup에서 Hostscan/Secure Firewall Posture 비활성화\(선택 사항\)](#)

[그룹 별칭 사용 안 함 및 그룹 URL 사용](#)

[인증서 매핑](#)

[IPsec-IKEv2](#)

[ASA 컨피그레이션 예](#)

[DefaultWEBVPNGroup 및 DefaultRAGroup 연결 프로파일에서 AAA 인증 비활성화](#)

[DefaultWEBVPNGroup 및 DefaultRAGroup에서 Hostscan/Secure Firewall Posture 비활성화\(선택 사항\)](#)

[그룹 별칭 사용 안 함 및 그룹 URL 사용](#)

[인증서 매핑](#)

[IPsec-IKEv2](#)

[결론](#)

[관련 정보](#)

소개

이 문서에서는 원격 액세스 VPN 구현의 보안을 향상시키는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음과 같은 주제에 대해 숙지할 것을 권장합니다.

- Cisco Secure Client AnyConnect VPN

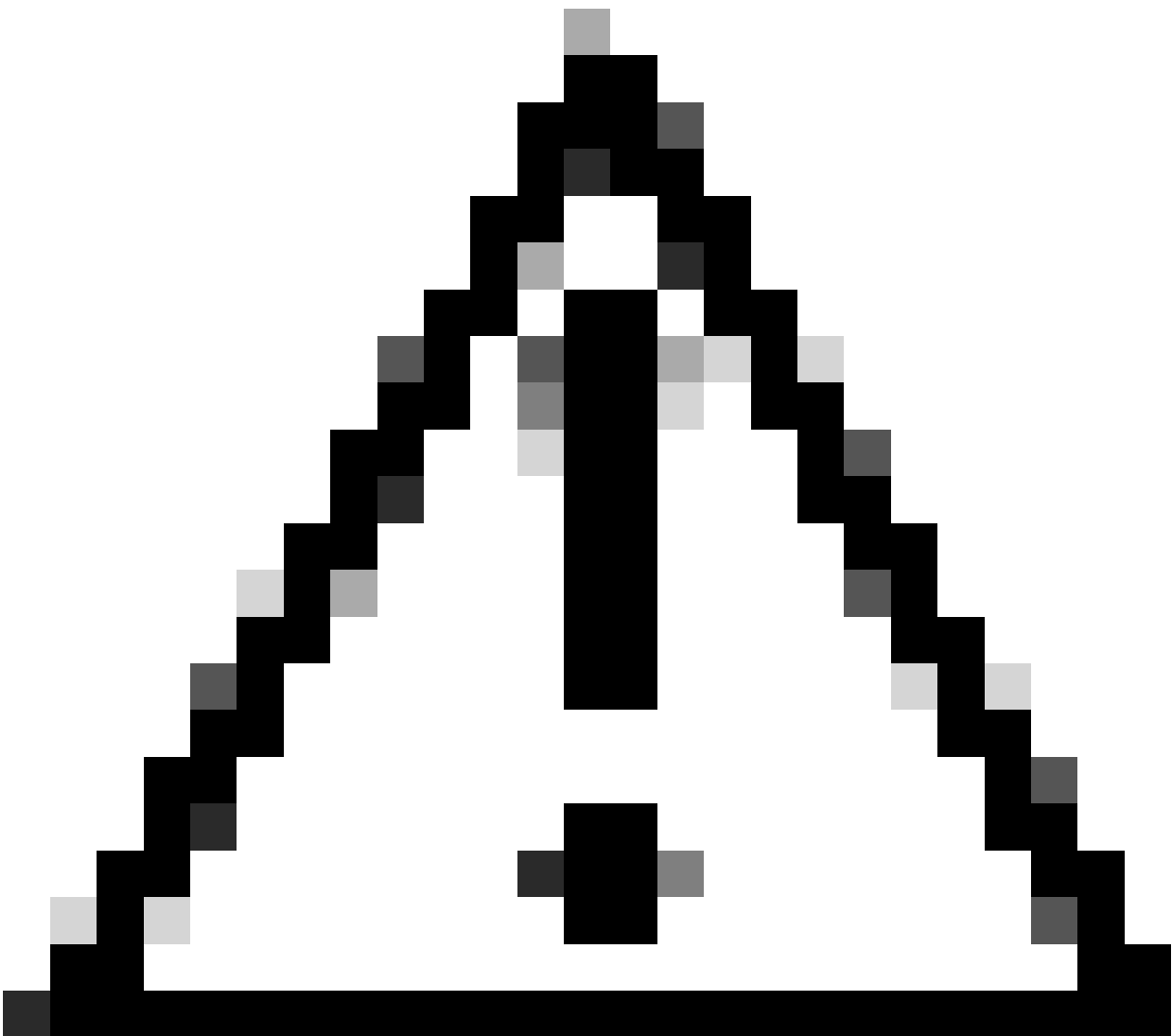
- ASA/FTD 원격 액세스 구성

사용되는 구성 요소

모범 사례 가이드는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.



주의: 이 문서에는 FDM(Firepower 장치 관리자) 단계가 포함되어 있지 않습니다. FDM은 DefaultWEBVPNGroup에서 인증 방법 변경만 지원합니다. 컨트롤 플레인 ACL 또는 FDM UI 내의 Remote Access VPN 'Global Settings' 섹션의 사용자 지정 포트를 사용하십시오. 필요한 경우 Cisco TAC(Technical Assistance Center)에 문의하여 추가 지원을 받으십시오.

배경 정보

이 문서의 목적은 Cisco Secure Client AnyConnect VPN 컨피그레이션이 사이버 보안 공격이 일반적인 현대 환경에서 보안 모범 사례를 준수하도록 하기 위한 것입니다.

무작위 대입 공격은 일반적으로 사용자 이름 및 비밀번호 조합을 사용하여 리소스에 대한 액세스를 얻으려는 반복적인 시도를 포함합니다. 공격자는 AAA 데이터베이스의 합법적인 조합과 일치할 경우 인터넷 브라우저, 보안 클라이언트 사용자 인터페이스 또는 기타 툴을 사용하여 여러 사용자 이름과 비밀번호를 입력하려고 합니다. 인증을 위해 AAA를 사용할 경우 연결을 설정하기 위해 최종 사용자가 사용자 이름과 비밀번호를 입력해야 합니다. 동시에 자격 증명을 입력할 때까지 사용자가 누구인지 확인하지 않습니다. 기본적으로 공격자는 다음과 같은 시나리오를 활용할 수 있습니다.

1. Cisco Secure Firewall의 정규화된 도메인 이름(특히 연결 프로파일에 그룹 별칭을 사용하는 경우) 노출:
 - 공격자가 VPN 방화벽의 FQDN을 검색할 경우 무차별 대입 공격을 시작할 그룹 별칭을 사용하여 터널 그룹을 선택할 수 있습니다.
2. AAA 또는 로컬 데이터베이스로 구성된 기본 연결 프로파일:
 - 공격자가 VPN 방화벽의 FQDN을 찾은 경우 AAA 서버 또는 로컬 데이터베이스를 무작위로 공격할 수 있습니다. 이는 그룹 별칭이 지정되지 않은 경우에도 FQDN에 대한 연결이 기본 연결 프로파일에 상주하기 때문에 발생합니다.
3. 방화벽 또는 AAA 서버의 리소스 소모:
 - 공격자는 대량의 인증 요청을 전송하고 DoS(Denial of Service) 조건을 생성하여 AAA 서버 또는 방화벽 리소스를 혼란에 빠뜨릴 수 있습니다.

개념

그룹 별칭:

- 방화벽이 연결 프로파일을 참조할 수 있는 대체 이름입니다. 방화벽에 대한 연결을 시작하면 사용자가 선택할 수 있도록 Secure Client UI의 드롭다운 메뉴에 이러한 이름이 표시됩니다. 그룹 별칭을 제거하면 Secure Client UI의 드롭다운 기능이 제거됩니다.

그룹 URL:

- 수신 연결이 원하는 연결 프로파일에 직접 매핑되도록 연결 프로파일에 연결할 수 있는 URL. 사용자가 Secure Client UI에 전체 URL을 입력하거나 XML 프로파일의 'Display Name'에 URL을 통합하여 사용자로부터 URL을 숨길 수 있으므로 드롭다운 기능은 없습니다.

여기서 차이점은 그룹 별칭이 구현되면 사용자가 `to vpn_gateway.example.com` 연결을 시작하고 연결 프로파일로 연결되는 별칭을 선택할 수 있는 별칭이 표시된다는 것입니다. group-URL을 사용하면 사용자가 `vpn_gateway.example.com/example_group`에 대한 연결을 시작하고 드롭다운 메뉴 옵션 없이 연결 프로파일로 직접 연결합니다.

Cisco Secure Firewall의 보안 클라이언트 강화 사례:

이러한 방법은 합법적인 사용자를 적절한 터널 그룹/연결 프로파일에 매핑하는 한편 악의적인 사용자는 사용자 이름 및 비밀번호 조합을 허용하지 않도록 구성하는 트랩 터널 그룹에 전송됩니다. 모든 조합을 구현해야 하는 것은 아니지만 권장 사항이 효과적으로 작동하려면 그룹 별칭을 비활성화하고 DefaultWEBVPNGroup 및 DefaultRAGroup의 인증 방법을 변경해야 합니다.

- 그룹 별칭을 비활성화하고 연결 프로파일 컨피그레이션에서 group-url만 사용하면 올바른 FQDN을 가진 클라이언트만 연결을 시작할 수 있으므로 공격자가 쉽게 검색하고 선택할 수 없는 특정 FQDN을 가질 수 있습니다. 예를 들어 vpn_gateway.example.com/example_group은 공격자가 vpn_gateway.example.com보다 검색하기가 더 어렵습니다.
- DefaultWEBVPNGroup 및 DefaultRAGroup에서 AAA 인증을 비활성화하고 인증서 인증을 구성하면 로컬 데이터베이스 또는 AAA 서버에 대해 무차별 대우(brute-force)가 발생하지 않습니다. 이 시나리오에서 공격자는 연결을 시도할 때 즉각적인 오류가 표시됩니다. 인증은 인증서를 기반으로 하므로 사용자 이름 또는 비밀번호 필드가 없으므로 무작위 대입 시도를 중지합니다. 또 다른 옵션은 악의적인 요청에 대한 싱크홀을 생성하기 위해 지원 컨피그레이션이 없는 AAA 서버를 생성하는 것입니다.
- 연결 프로파일에 대해 인증서 매핑을 활용합니다. 이렇게 하면 클라이언트 디바이스의 인증서에서 받은 특성을 기반으로 수신 연결을 특정 연결 프로파일에 매핑할 수 있습니다. 올바른 인증서를 가진 사용자는 올바르게 매핑되며, 매핑 기준에 실패한 공격자는 DefaultWEBVPNGroup으로 전송됩니다.
- SSL 대신 IKEv2-IPSec을 사용하면 터널 그룹이 XML 프로파일의 특정 사용자 그룹 매핑에 의존하게 됩니다. 최종 사용자 시스템에 이 XML이 없으면 사용자가 기본 터널 그룹으로 자동으로 전송됩니다.

참고: 그룹 별칭 기능에 대한 자세한 내용은 [ASA VPN 컨피그레이션 가이드](#)를 참조하고 '표 1'을 참조하십시오. SSL VPN에 대한 연결 프로파일 특성'

로깅 및 Syslog ID를 사용하여 공격 식별

무차별 대입 공격은 원격 액세스 VPN을 손상시키고 취약한 비밀번호를 악용하여 무단 진입을 유도하는 주요 방법을 나타냅니다. 로깅의 사용을 활용하고 syslog를 평가하여 공격의 징후를 인식하는 방법을 아는 것이 중요합니다. 비정상적인 볼륨에 발생한 경우 공격을 나타낼 수 있는 일반적인 syslogs ID는 다음과 같습니다.

```
%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

사용자 이름은 ASA에서 no logging hide username 명령이 구성될 때까지 항상 숨겨집니다.

참고: 참고: 이는 잘못된 IP로 인해 유효한 사용자가 생성되거나 알려진 경우 정보를 제공합니다. 그러나 사용자 이름이 로그에 표시되므로 주의하십시오.

Cisco ASA 로깅:

[보안 ASA 방화벽 사용 설명서](#)

Cisco Secure Firewall ASA Series General Operations CLI 컨피그레이션 가이드의 로깅 장

Cisco FTD 로깅:

[FMC를 통해 FTD에 로깅 구성](#)

Cisco Secure Firewall Management Center Device Configuration Guide의 Platform Settings 장에서 Syslog 구성 섹션

[firepower 장치 관리자에서 Syslog 구성 및 확인](#)

Firepower 디바이스 [관리자용](#) Cisco Firepower Threat Defense 컨피그레이션 가이드의 시스템 설정 장에서 시스템 로깅 설정 구성 섹션

공격 확인

확인하려면 ASA 또는 FTD CLI(Command Line Interface)에 로그인하고 show aaa-server 명령을 실행하여 구성된 AAA 서버에 대해 시도하거나 거부된 인증 요청 수를 조사합니다.

```
<#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#
```

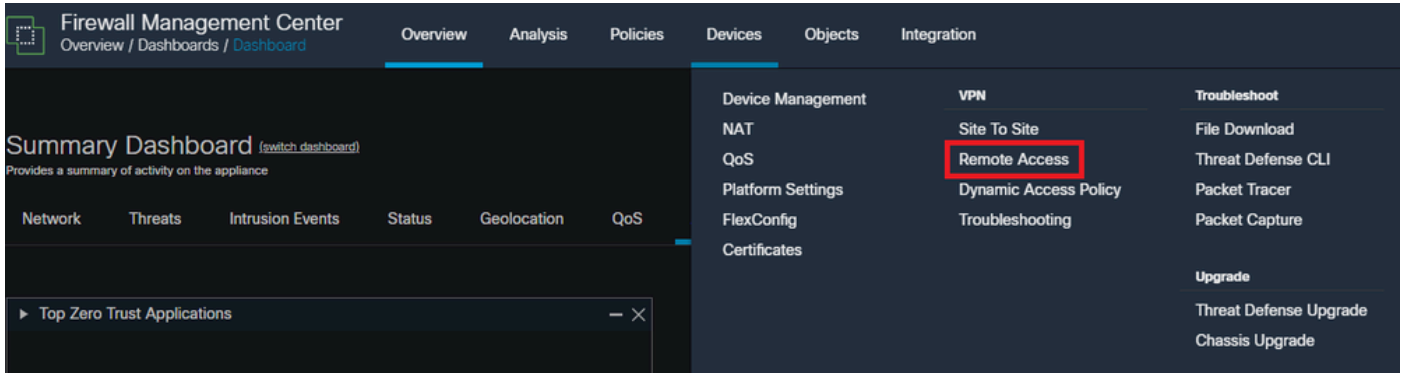
```
show aaa-server
```

```
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 컨피그레이션 예

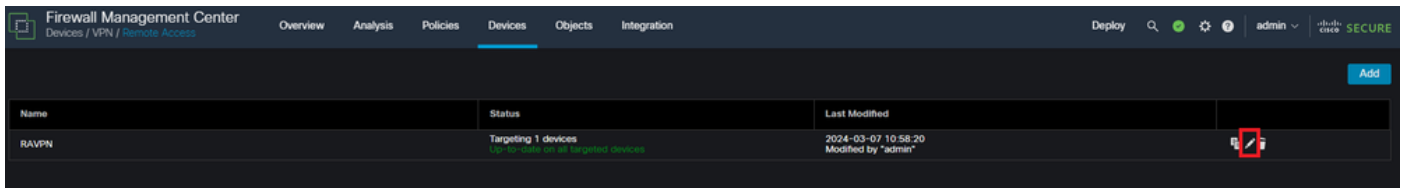
DefaultWEBVPNGroup 및 DefaultRAGroup 연결 프로파일에서 AAA 인증 비활성화

Devices(디바이스) > Remote Access(원격 액세스)로 이동합니다.



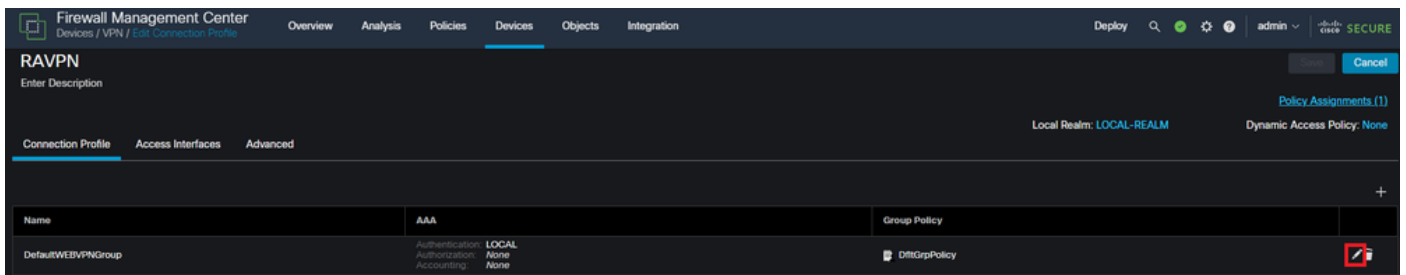
원격 액세스 VPN 정책 컨피그레이션에 연결하기 위해 FMC GUI 탐색을 표시합니다.

기존 원격 액세스 VPN 정책을 편집하고 'DefaultRAGroup'이라는 연결 프로필을 만듭니다.



FMC UI 내에서 원격 액세스 VPN 정책을 수정하는 방법을 표시합니다.

이름이 'DefaultWEBVPNGroup' 및 'DefaultRAGroup'인 연결 프로필을 편집합니다.



FMC UI 내에서 DefaultWEBVPNGroup을 편집하는 방법을 표시합니다.

AAA 탭으로 이동하여 Authentication Method(인증 방법) 드롭다운을 선택합니다. '클라이언트 인증서만'을 선택하고 저장을 선택합니다.

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

FMC UI 내의 DefaultWEBVPNGroup에 대해서만 클라이언트 인증서로 인증 방법을 변경합니다.

DefaultRAGroup을 편집하고 AAA 탭으로 이동하여 Authentication Method(인증 방법) 드롭다운을 선택합니다. '클라이언트 인증서만'을 선택하고 저장을 선택합니다.

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

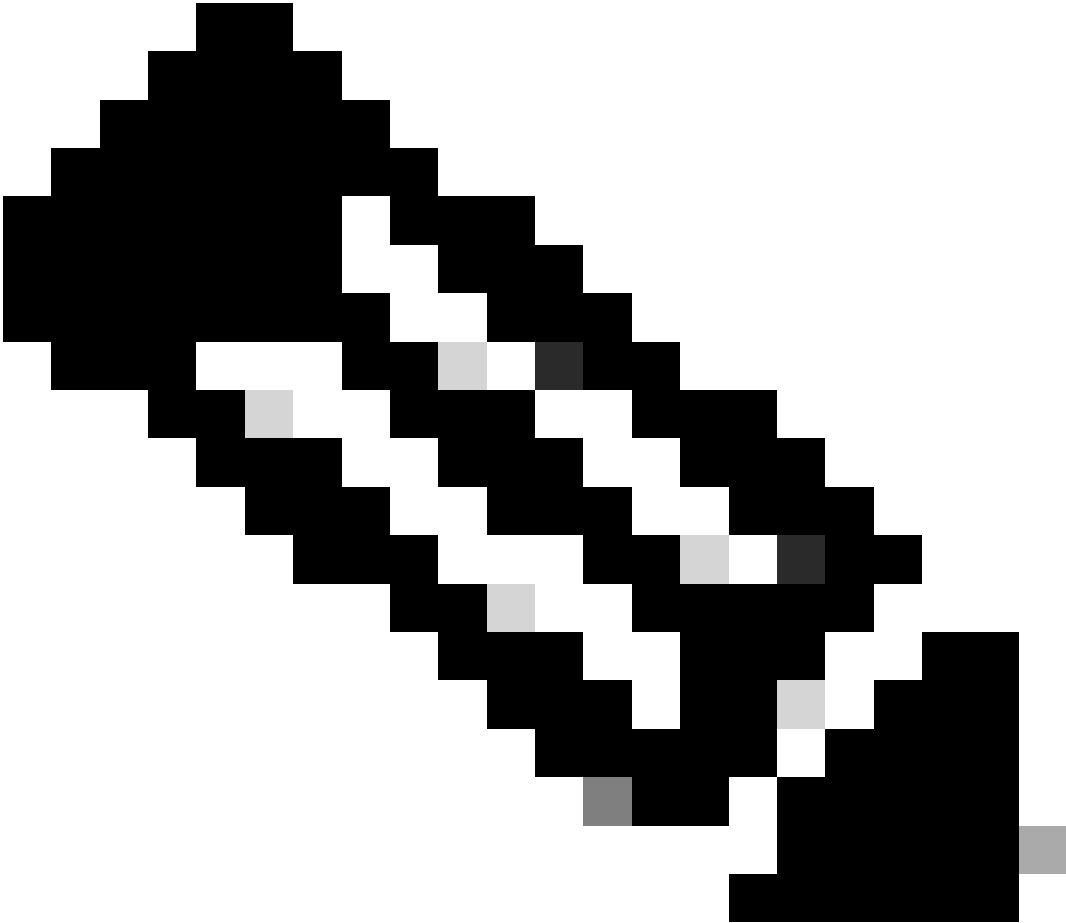
Accounting

Accounting Server:

Cancel

Save

FMC UI 내의 DefaultRAGroup에 대해서만 클라이언트 인증서로 인증 방법을 변경합니다.

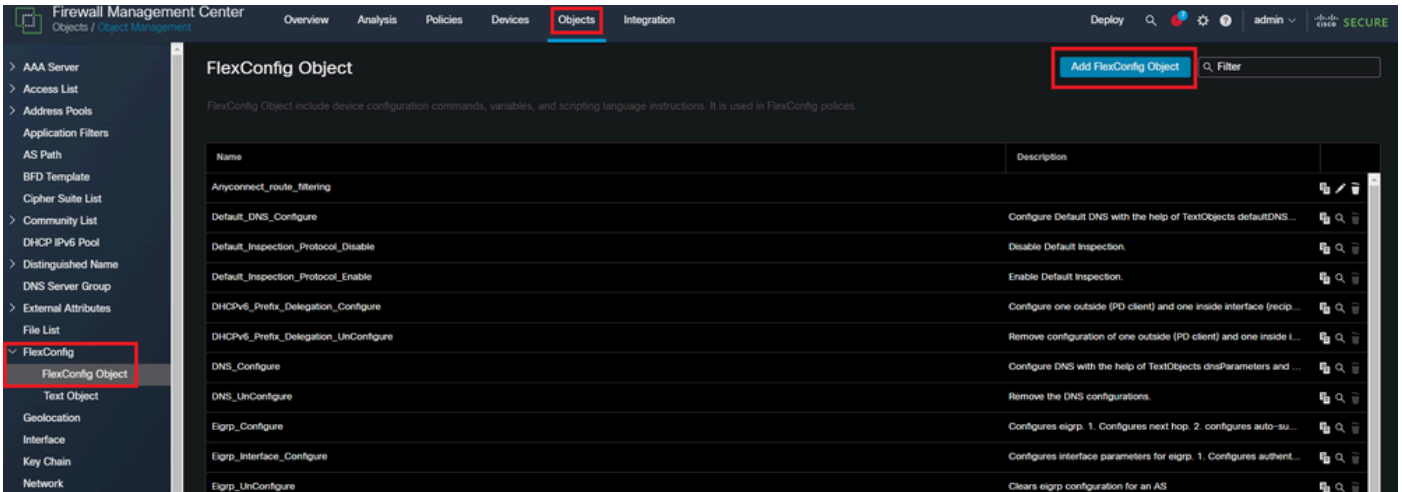


참고: 인증 방법은 싱크홀 AAA 서버일 수도 있습니다. 이 방법을 사용하는 경우 AAA 서버 컨피그레이션은 가짜이며 실제로 어떤 요청도 처리하지 않습니다. 변경 사항을 저장하려면 'Client Address Assignment(클라이언트 주소 할당)' 탭에도 VPN 풀을 정의해야 합니다.

DefaultWEBVPNGroup 및 DefaultRAGroup에서 Hostscan/Secure Firewall Posture 비활성화(선택 사항)

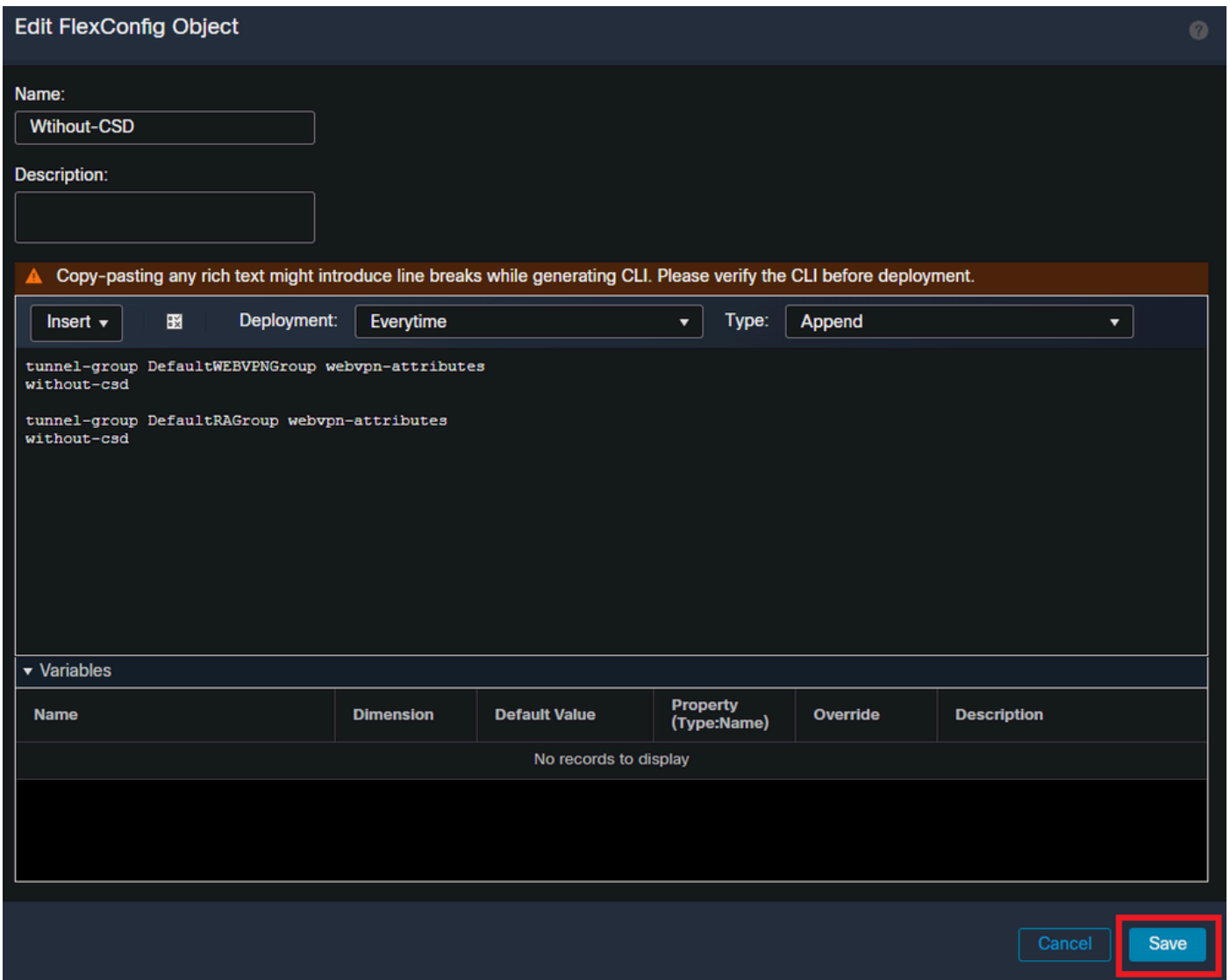
이는 해당 환경에 Hostscan/Secure Firewall Posture가 있는 경우에만 필요합니다. 이 단계에서는 공격자가 엔드포인트 검사 프로세스로 인해 방화벽의 리소스 사용률을 높이는 것을 방지합니다. FMC에서 이는 엔드포인트 검사 기능을 비활성화하기 위해 명령 `without-csd`를 사용하여 FlexConfig 객체를 생성함으로써 구현됩니다.

Objects(개체) > Object Management(개체 관리) > FlexConfig Object(FlexConfig 개체) > Add FlexConfig Object(FlexConfig 개체 추가)로 이동합니다.



FMC UI를 탐색하여 FlexConfig 개체를 만듭니다.

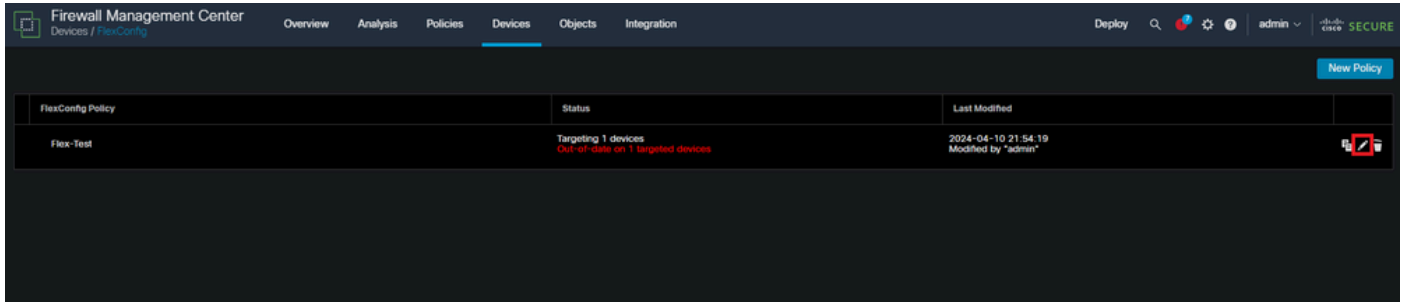
FlexConfig 개체의 이름을 지정하고 Append를 입력하여 구축을 Everytime으로 설정합니다. 그런 다음 표시된 것과 정확히 같은 구문을 입력하고 객체를 저장합니다.



'without-csd'로 FlexConfig 개체 만들기

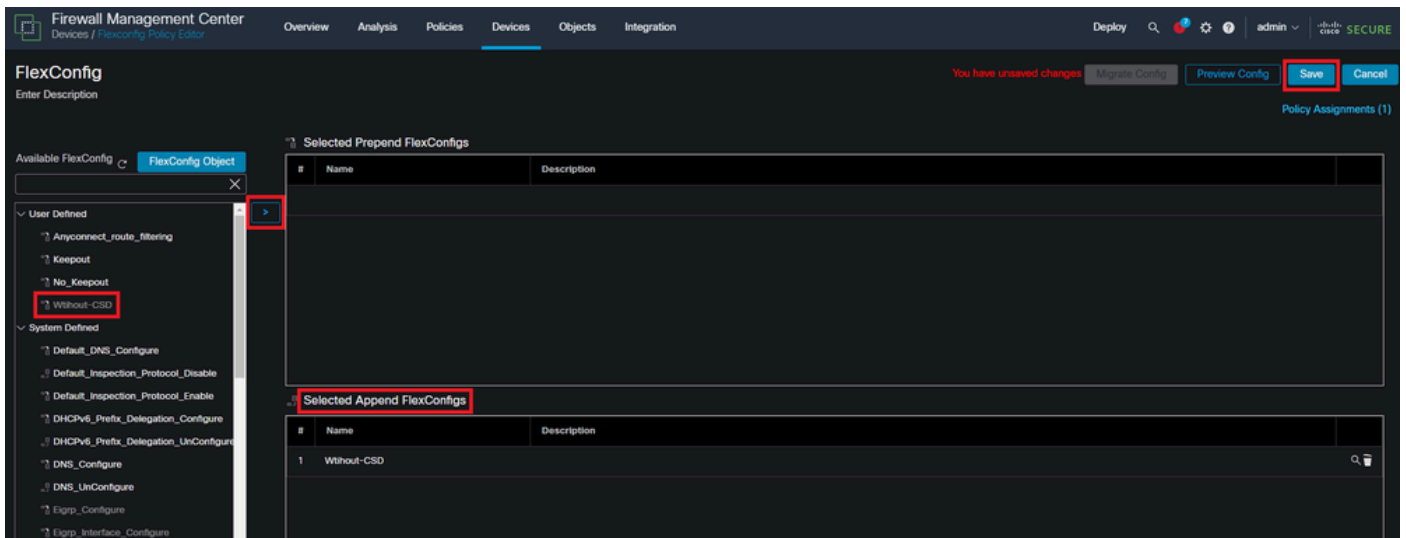
Devices(디바이스) > FlexConfig로 이동한 다음 Pencil(연필)을 클릭하여 FlexConfig 정책을 수정합

니다.



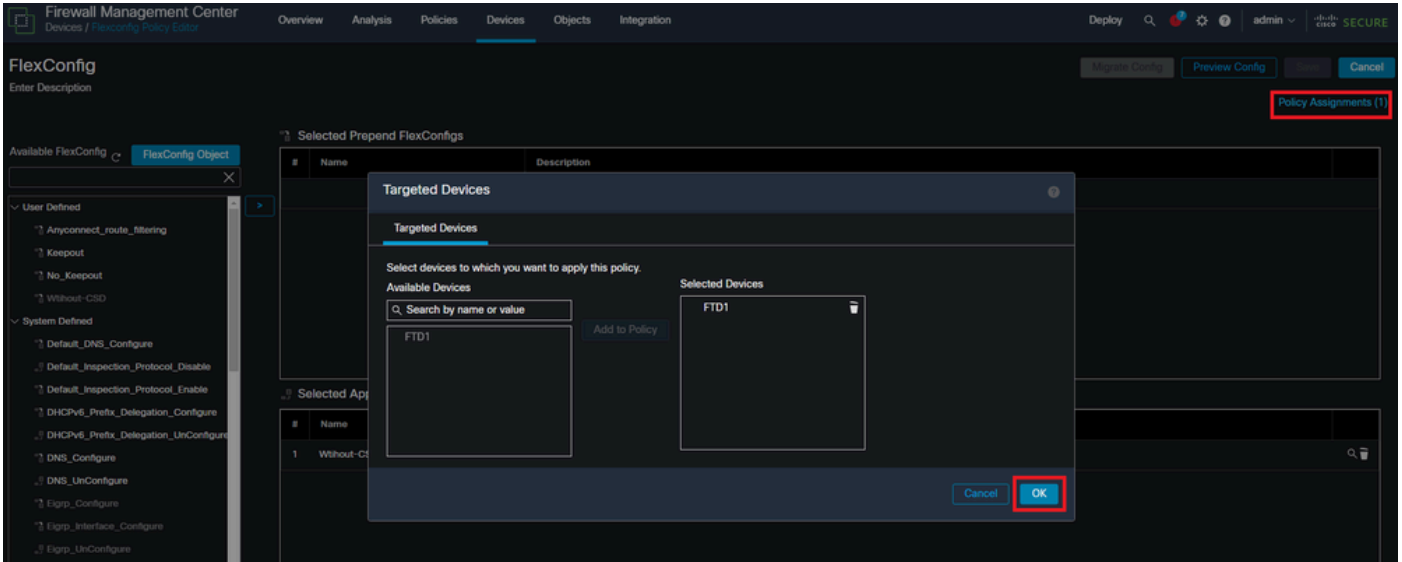
FMC 내에서 FlexConfig 정책 수정

사용자 정의 섹션에서 생성한 객체를 찾습니다. 그런 다음 화살표를 선택하여 Selected Append FlexConfigs에 추가합니다. 마지막으로 Save를 선택하여 FlexConfig 정책을 저장합니다.



FlexConfig 객체를 FlexConfig 정책에 연결합니다.

Policy Assignments(정책 할당)를 선택하고 이 FlexConfig 정책을 적용할 FTD를 선택한 다음 OK(확인)를 선택합니다. 새 FlexConfig 할당인 경우 Save(저장)를 다시 선택하고 변경 사항을 구축합니다. 구축이 완료되면



firepower 디바이스에 FlexConfig 정책을 할당합니다.

FTD CLI를 입력하고 DefaultWEBVPNGroup 및 DefaultRAGroup에 대해 show run tunnel-group 명령을 실행합니다. 컨피그레이션에 without-csd가 있는지 확인합니다.

```
<#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
```

그룹 별칭 사용 안 함 및 그룹 URL 사용

연결 프로필로 이동하여 '별칭' 탭을 선택합니다. 그룹 별칭을 비활성화하거나 삭제하고 더하기 아

이콘을 클릭하여 URL 별칭을 추가합니다.

Edit Connection Profile

Connection Profile:*

Group Policy:* +
[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	
-----	--------	--

FMC UI 내에서 터널 그룹에 대한 group-alias 옵션을 비활성화합니다.

URL 별칭에 대한 개체 이름을 구성하고 URL에 대한 방화벽의 FQDN 및/또는 IP 주소를 입력한 다음 연결 프로파일을 연결할 이름을 입력합니다. 이 예제에서는 'aaaldap'를 선택했습니다. 공격자가 FQDN을 가져왔더라도 전체 URL을 추측할 가능성이 낮으므로 모호할수록 안전합니다. 완료되면 저장을 선택합니다.

Edit URL Objects



Name

LDAP-ALIAS

Description

URL

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

Allow Overrides

Cancel

Save

FMC UI 내에서 URL-Alias 객체 생성

드롭다운에서 URL Alias(URL 별칭)를 선택하고 Enabled(활성화됨) 상자를 선택한 다음 OK(확인)를 선택합니다.

Add URL Alias



URL Alias:



Enabled

Cancel

OK

URL-Alias가 FMC UI 내에서 활성화되었는지 확인합니다.

그룹 별칭이 삭제되거나 비활성화되었는지 확인하고 URL 별칭이 활성화되어 있는지 확인한 후 저장을 선택합니다.


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:

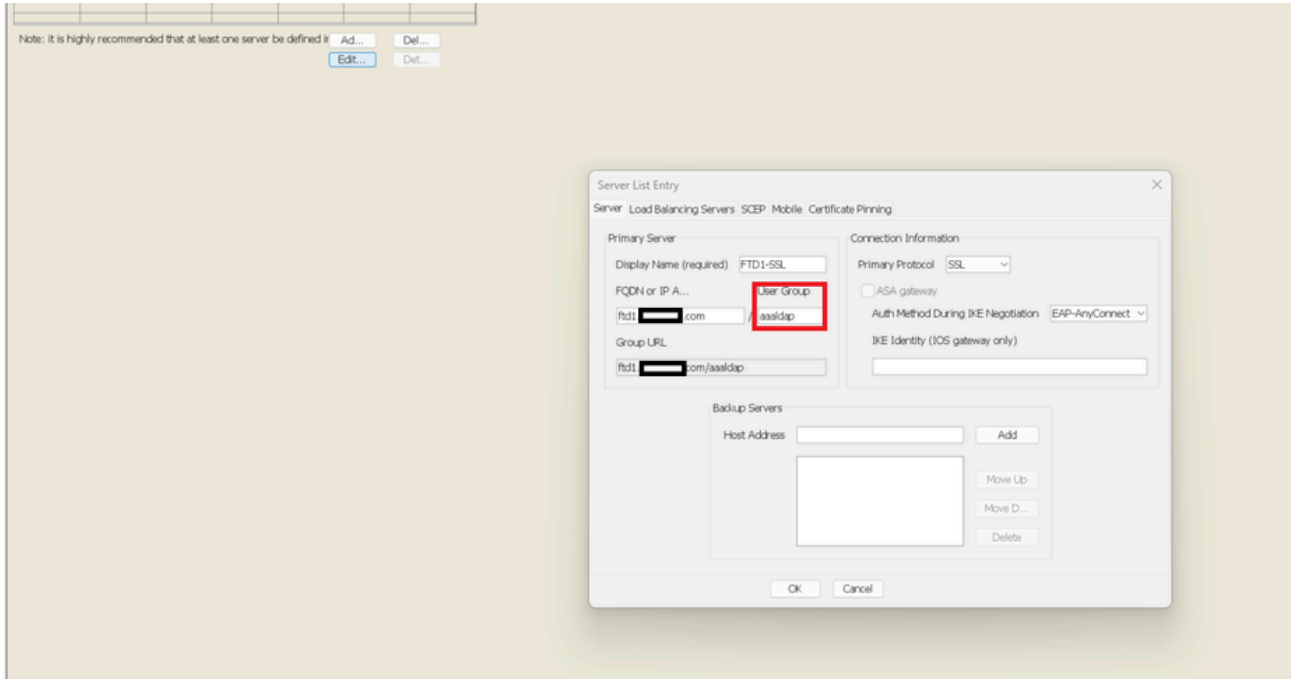
Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.

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

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

FMC UI 내에서 터널 그룹에 대해 URL-Alias 옵션을 활성화합니다.

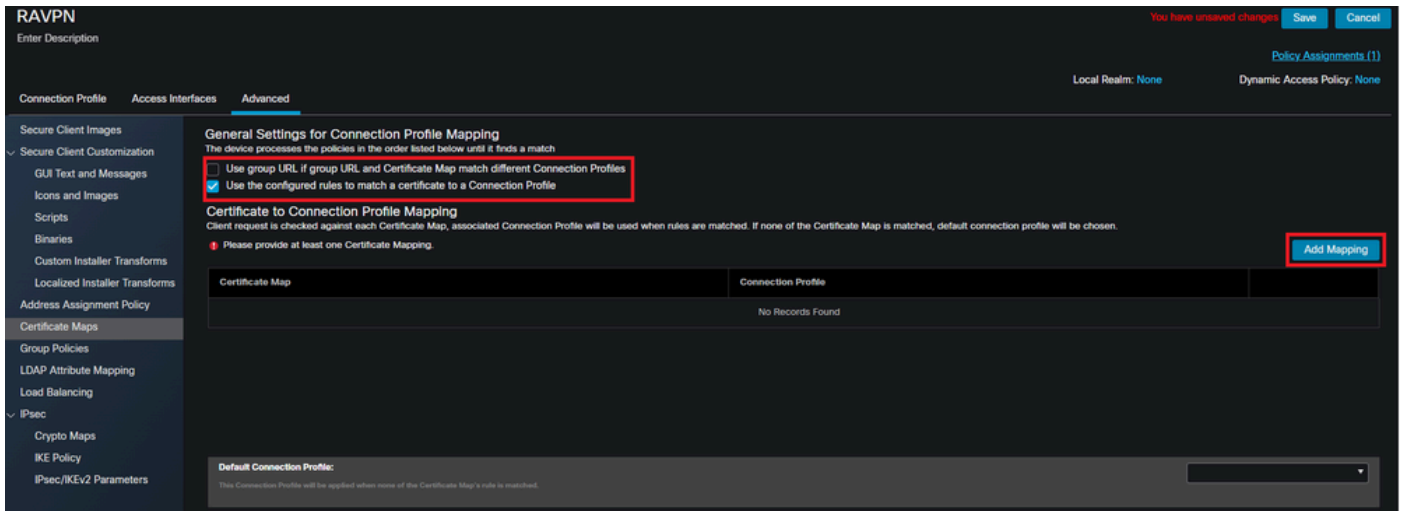
원하는 경우 URL 별칭도 XML의 일부로 푸시할 수 있습니다. 이는 VPN 프로파일 편집기 또는 ASA 프로파일 편집기를 사용하여 XML을 편집하여 수행할 수 있습니다. 이를 위해 Server List(서버 목록) 탭으로 이동하고 User Group(사용자 그룹) 필드가 SSL 사용 시 연결 프로파일의 URL 별칭과 일치하는지 확인합니다. IKEv2의 경우 User Group(사용자 그룹) 필드가 연결 프로파일의 정확한 이름과 일치하는지 확인합니다.



SSL 연결을 위한 URL 별칭을 갖도록 XML 프로파일 수정

인증서 매핑

Remote Access VPN Policy(원격 액세스 VPN 정책) 내의 Advanced(고급) 탭으로 이동합니다. 기본 설정에 따라 일반 설정 옵션을 선택합니다. 선택한 후 매핑 추가를 선택합니다.



FMC UI 내의 Advanced(고급) 탭으로 이동하여 FMC UI 내에 인증서 맵 객체를 생성합니다.

인증서 맵 객체의 이름을 지정하고 Add Rule을 선택합니다. 이 규칙에서는 사용자를 특정 연결 프로파일에 매핑하기 위해 식별하려는 인증서의 속성을 정의합니다. 작업을 마치면 OK(확인)를 선택한 다음 Save(저장)를 선택합니다.

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

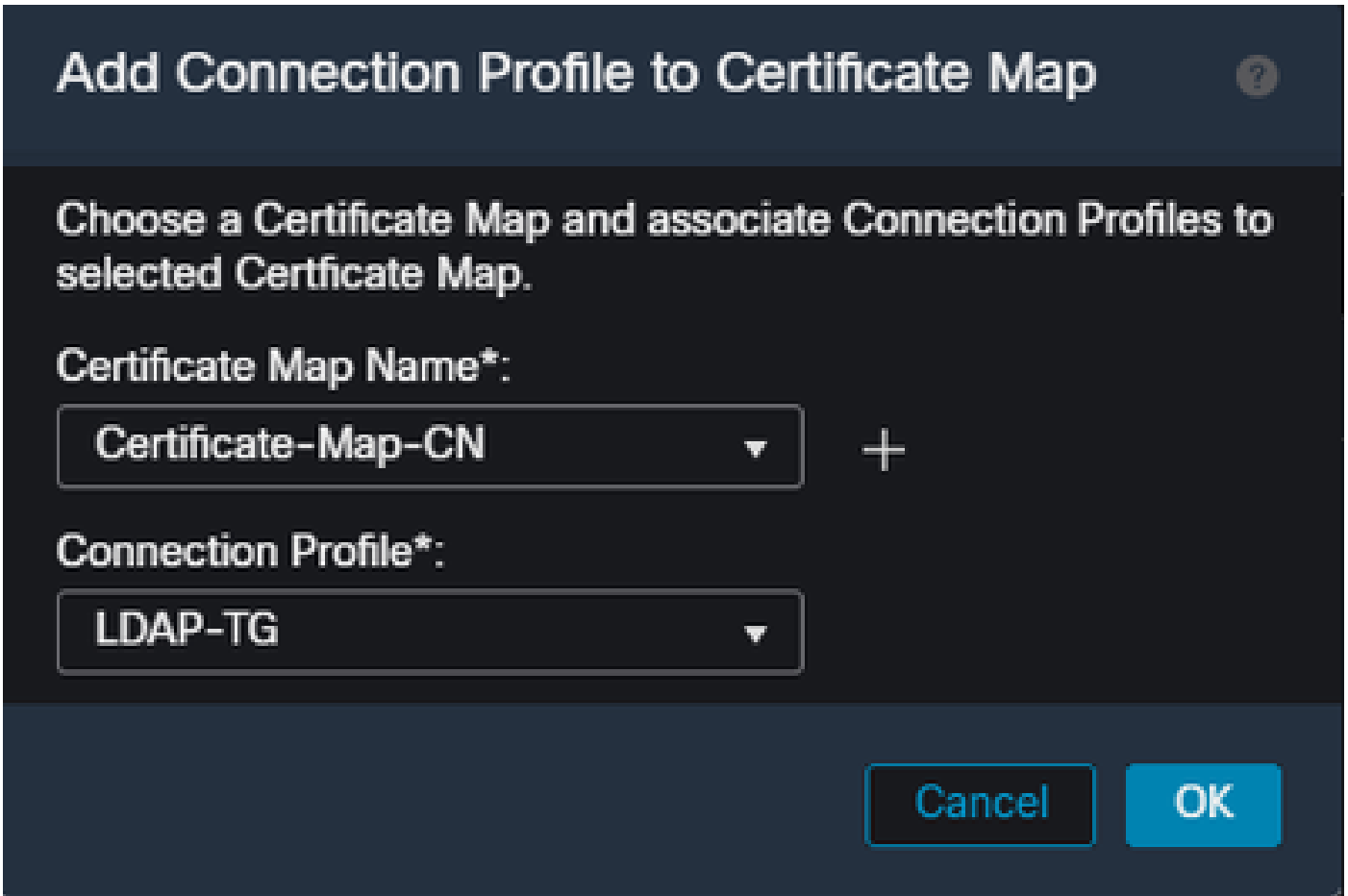
Cancel

Cancel

Save

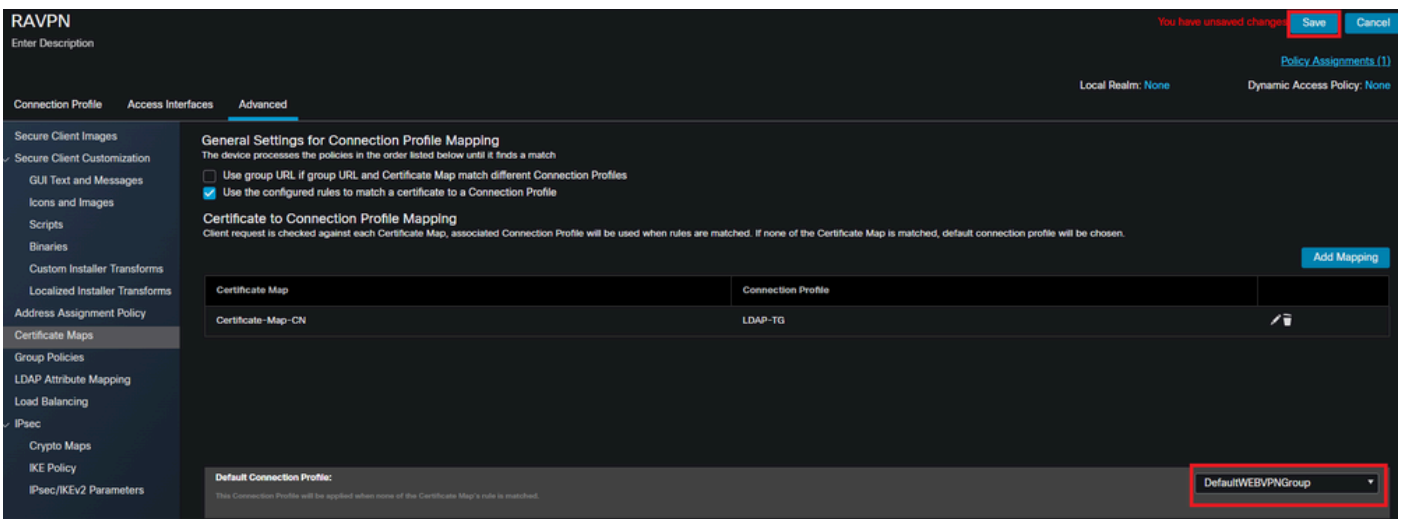
인증서 맵을 만들고 FMC UI 내에 맵 기준을 추가합니다.

드롭다운에서 인증서 맵 객체 및 인증서 맵을 연결할 연결 프로파일을 선택합니다. 그런 다음 확인을 선택합니다.



인증서 맵 객체를 FMC UI 내의 원하는 터널 그룹에 연결합니다.

사용자가 DefaultWEBVPNGroup으로 전송되는 매핑에 실패할 경우 기본 연결 프로파일이 DefaultWEBVPNGroup으로 구성되었는지 확인합니다. 완료되면 Save(저장)를 선택하고 변경 사항을 구축합니다.



인증서 매핑의 기본 연결 프로파일을 FMC UI 내의 DefaultWEBVPNGroup으로 변경합니다.

IPsec-IKEv2

원하는 IPsec-IKEv2 연결 프로파일을 선택하고 Edit Group Policy(그룹 정책 수정)로 이동합니다.

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	

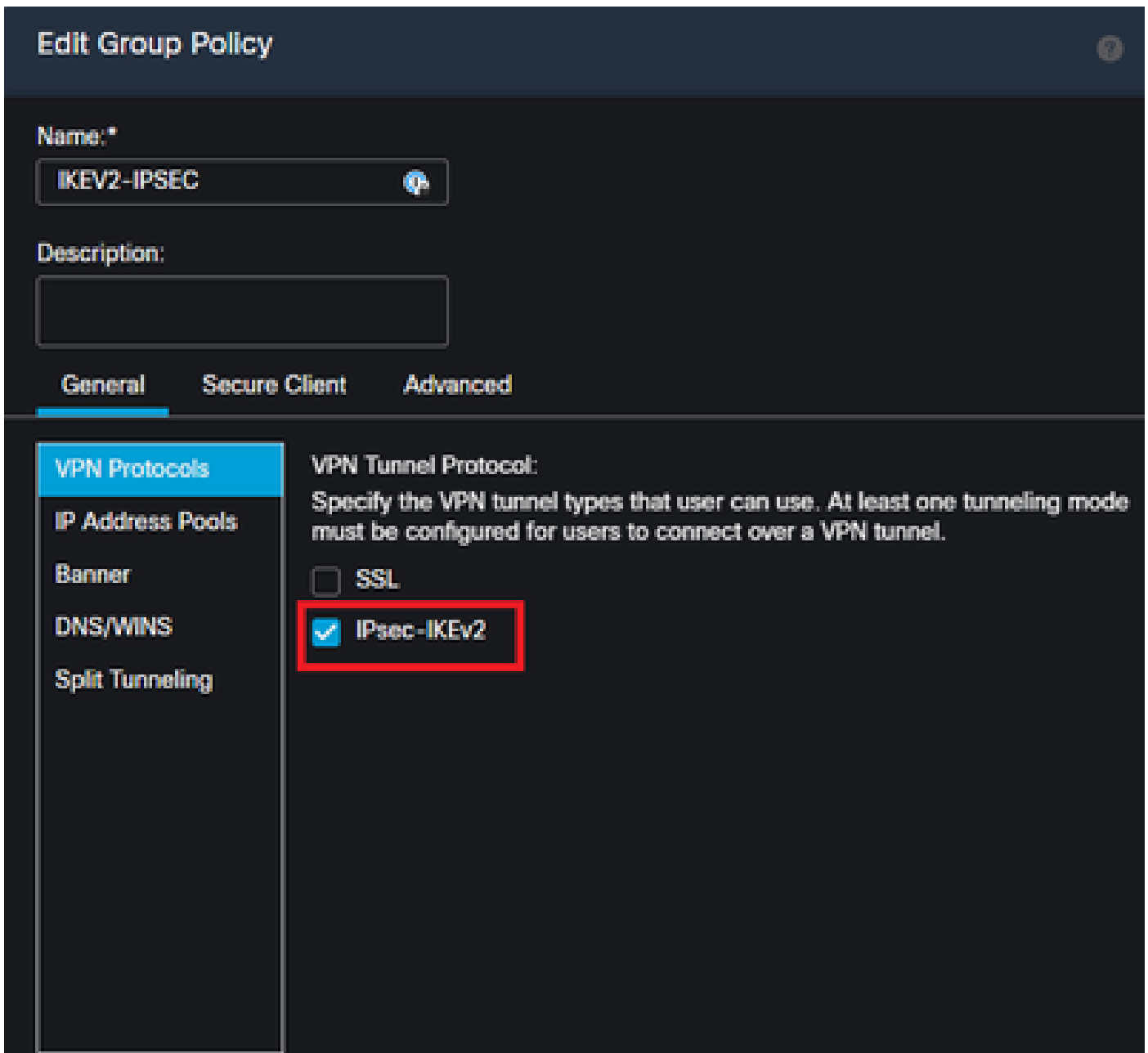
DHCP Servers: +

Name	DHCP Server IP Address	

Cancel Save

FMC UI 내에서 그룹 정책을 수정합니다.

General(일반) 탭에서 VPN Protocols(VPN 프로토콜) 섹션으로 이동하여 IPsec-IKEv2 상자가 선택되었는지 확인합니다.



FMC UI의 그룹 정책 내에서 IPsec-IKEv2를 활성화합니다.

VPN 프로파일 편집기 또는 ASA 프로파일 편집기에서 Server List(서버 목록) 탭으로 이동합니다. 사용자 그룹 이름은 방화벽의 연결 프로파일 이름과 정확히 일치해야 합니다. 이 예에서 IKEV2는 연결 프로파일/사용자 그룹 이름입니다. 기본 프로토콜은 IPsec으로 구성됩니다. 이 연결 프로파일에 대한 연결을 설정하면 의 '표시 이름'이 보안 클라이언트 UI에서 사용자에게 표시됩니다.

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 [] Add

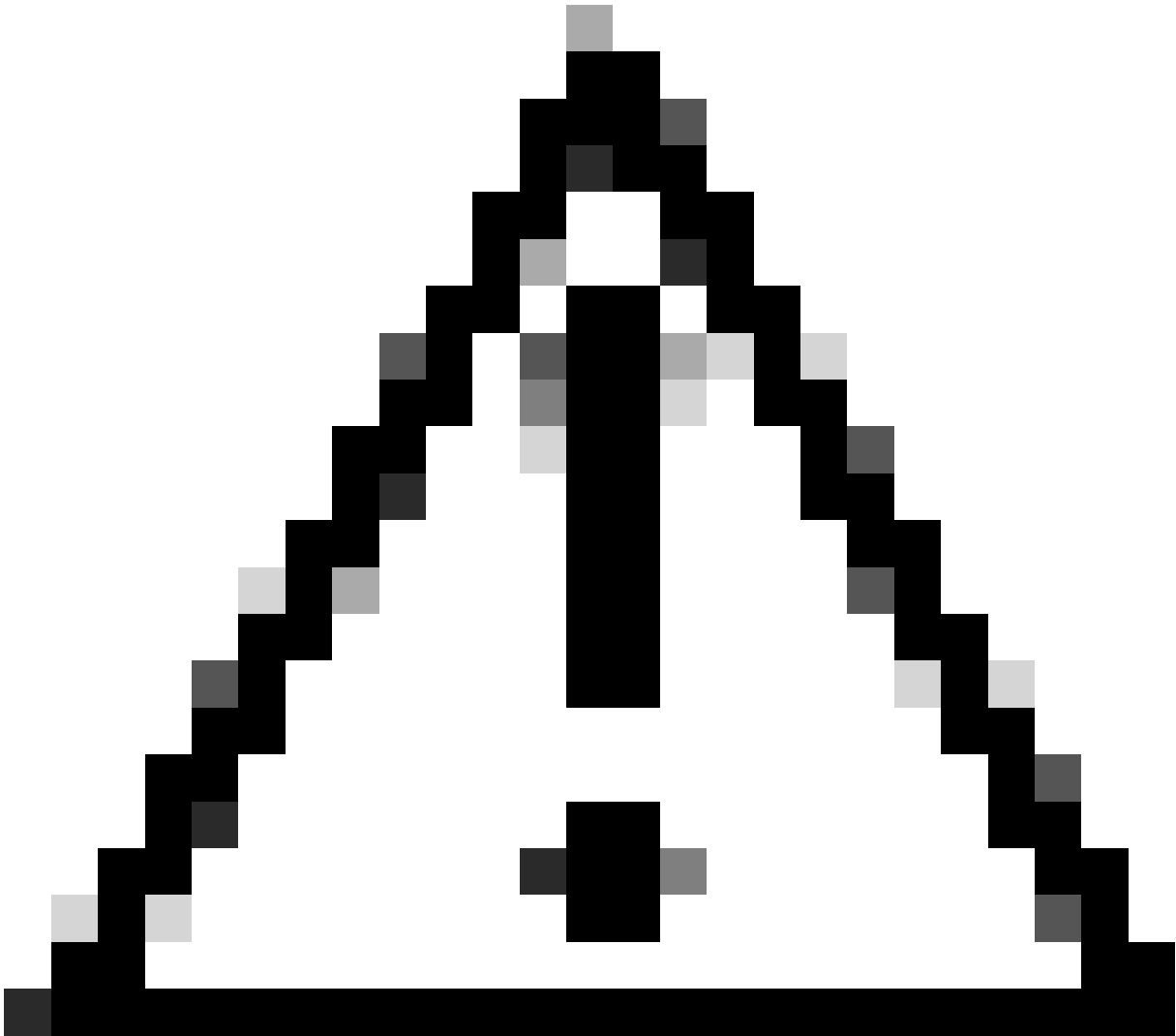
[] Move Up

[] Move D...

[] Delete

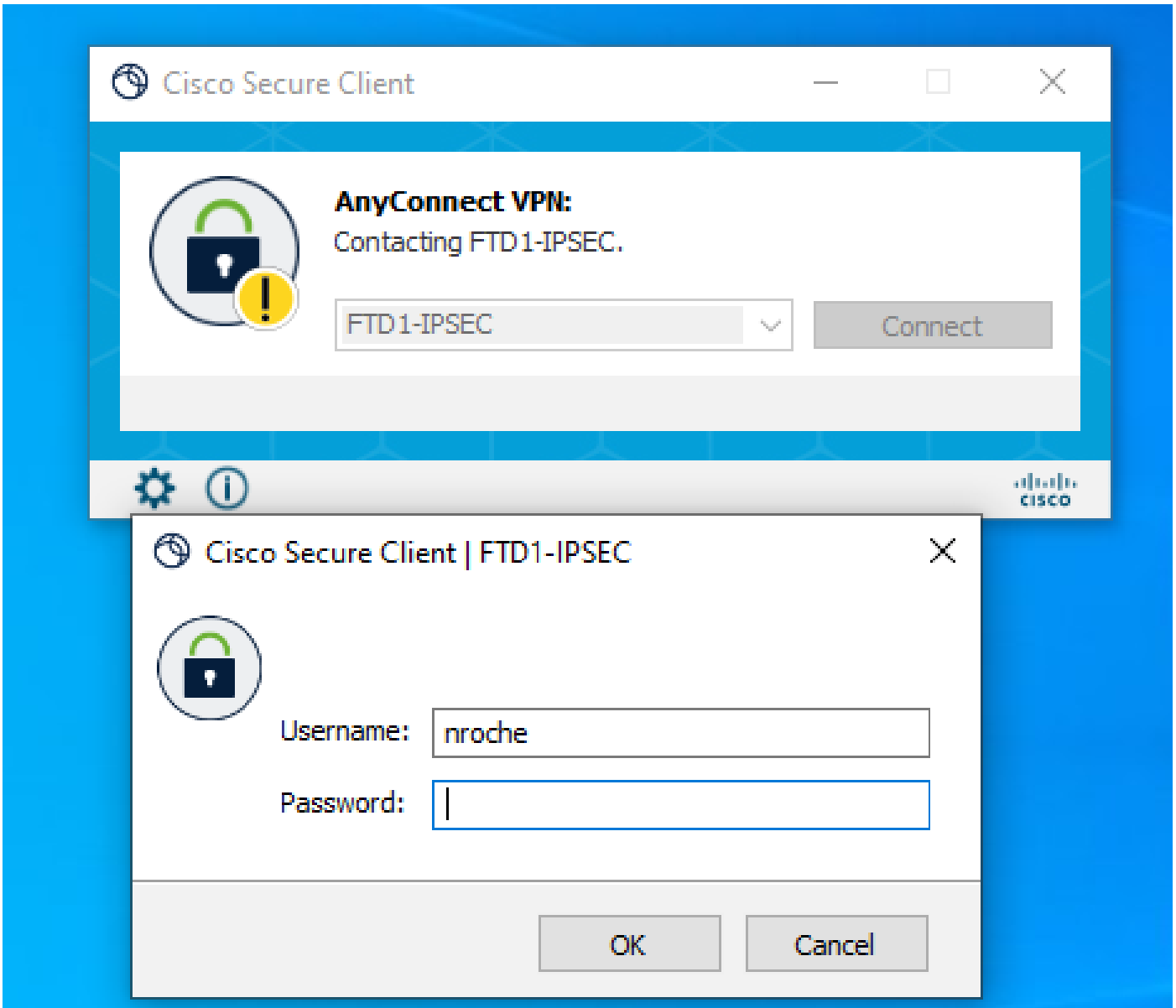
OK Cancel

기본 프로토콜이 IPsec이고 사용자 그룹이 연결 프로파일 이름과 일치하도록 XML 프로파일을 편집합니다.



주의: XML 프로파일을 방화벽에서 클라이언트로 푸시하려면 SSL 연결이 필요합니다.
IKEV2-IPsec만 사용하는 경우 XML 프로파일은 OOB(Out of Band) 방식을 통해 클라이언
트에 푸시되어야 합니다.

XML 프로파일이 클라이언트에 푸시되면 보안 클라이언트는 XML 프로파일의 사용자 그룹을 사용
하여 IKEV2-IPsec 연결 프로파일에 연결합니다.



IPsec-IKEv2 RAVPN 연결 시도에 대한 보안 클라이언트 UI 보기입니다.

ASA 컨피그레이션 예

DefaultWEBVPNGroup 및 DefaultRAGroup 연결 프로파일에서 AAA 인증 비활성화

터널 그룹 DefaultWEBVPNGroup에 대한 webvpn-attributes 섹션을 입력하고 인증서 기반으로 인증을 지정합니다. DefaultRAGroup에 대해 이 프로세스를 반복합니다. 이러한 기본 연결 프로파일에 속하는 사용자는 인증을 위해 인증서를 제시해야 하며 사용자 이름 및 비밀번호 자격 증명을 입력할 기회가 제공되지 않습니다.

```
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
```

DefaultWEBVPNGroup 및 DefaultRAGroup에서 Hostscan/Secure Firewall Posture 비활성화(선택 사항)

이는 해당 환경에 Hostscan/Secure Firewall Posture가 있는 경우에만 필요합니다. 이 단계에서는 공격자가 엔드포인트 검사 프로세스로 인해 방화벽의 리소스 사용률을 높이는 것을 방지합니다. DefaultWEBVPNGroup 및 DefaultRAGroup과 연결 프로파일에 대한 webvpn-attributes 섹션을 입력하고 without-csd를 구현하여 엔드포인트 검사 기능을 비활성화합니다.

```
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
```

그룹 별칭 사용 안 함 및 그룹 URL 사용

사용자가 연결 중인 터널 그룹을 입력합니다. 기존 그룹 별칭이 있는 경우 비활성화하거나 제거합니다. 이 예에서는 비활성화되어 있습니다. 완료되면 RAVPN 종료 인터페이스의 FQDN 또는 IP 주소를 사용하여 group-url을 생성합니다. group-url의 끝에 있는 이름은 모호해야 합니다. VPN, AAA, RADIUS, LDAP와 같은 일반적인 값을 사용하지 마십시오. 그러면 공격자가 FQDN을 얻을 경우 전체 URL을 쉽게 추측할 수 있습니다. 대신 터널 그룹을 식별하는 데 도움이 되는 내부 고유 이름을 사용합니다.

```
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
```

인증서 매핑

전역 컨피그레이션 모드에서 인증서 맵을 만들고 이름 및 시퀀스 번호를 할당합니다. 그런 다음 사용자가 매핑을 활용하기 위해 일치해야 하는 규칙을 정의합니다. 이 예에서 사용자는 "customvalue"와 같은 일반 이름 값의 기준과 일치해야 합니다. 그런 다음 webvpn 컨피그레이션을 입력하고 인증서 맵을 원하는 터널 그룹에 적용합니다. 완료되면 DefaultWEBVPNGroup을 입력하고 이 터널 그룹을 인증서 매핑에 실패한 사용자의 기본값으로 설정합니다. 사용자가 매핑에 실패하면 DefaultWEBVPNGroup으로 전달됩니다. DefaultWEBVPNGroup이 인증서 인증으로 구성된 경우, 사용자는 사용자 이름 또는 비밀번호 자격 증명을 전달할 수 있는 옵션이 없습니다.

```
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

전역 컨피그레이션 모드에서 기존 그룹 정책을 수정하거나 새 그룹 정책을 생성하고 해당 그룹 정책에 대한 특성을 입력할 수 있습니다. 특성 섹션에 있는 경우 IKEv2를 유일한 vpn 터널 프로토콜로 활성화합니다. 이 그룹 정책이 IPsec-IKEv2 원격 액세스 VPN 연결에 사용할 터널 그룹에 연결되어 있는지 확인합니다. FMC 단계와 마찬가지로 VPN 프로파일 편집기 또는 ASA 프로파일 편집기를 통해 XML 프로파일을 편집하고 ASA의 터널 그룹 이름과 일치하도록 User Group 필드를 변경하고 프로토콜을 IPsec으로 변경해야 합니다.

```
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
```

VPN 프로파일 편집기 또는 ASA 프로파일 편집기에서 Server List(서버 목록) 탭으로 이동합니다. 사용자 그룹 이름은 방화벽의 연결 프로파일 이름과 정확히 일치해야 합니다. 기본 프로토콜은 IPsec으로 구성됩니다. 이 연결 프로파일에 대한 연결을 설정할 때 표시 이름이 Secure Client UI에서 사용자에게 표시됩니다.

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

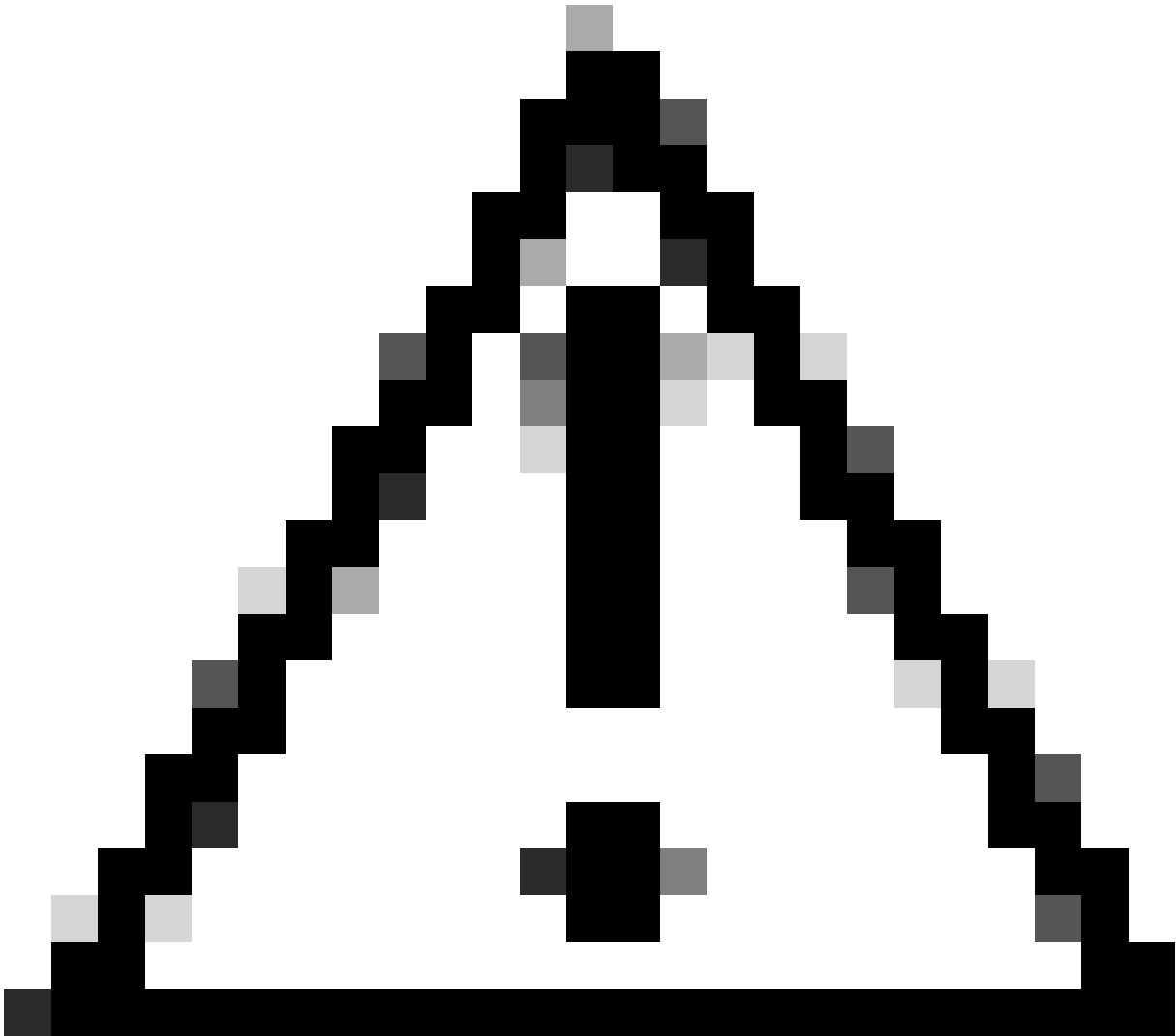
Move Up

Move D...

Delete

OK Cancel

기본 프로토콜 이름이 IPsec이고 사용자 그룹 이름이 IPsec-IKEv2 RAVPN 연결을 위한 ASA의 터널 그룹 이름과 일치하도록 XML 프로필을 수정합니다.



주의: XML 프로파일을 방화벽에서 클라이언트로 푸시하려면 SSL 연결이 필요합니다. IKEV2-IPsec만 사용하는 경우 XML 프로파일은 OOB(Out of Band) 방식을 통해 클라이언트에 푸시되어야 합니다.

결론

요약하면, 이 문서의 강화 방법은 공격자가 DefaultWEBVPNGroup 및 DefaultRAGroup으로 이동하는 동안 합법적인 사용자를 사용자 지정 연결 프로파일에 매핑하는 것입니다. 최적화된 컨피그레이션에서는 두 기본 연결 프로파일에 올바른 맞춤형 AAA 서버 컨피그레이션이 없습니다. 또한 그룹 별칭을 제거하면 공격자가 방화벽의 FQDN 또는 공용 IP 주소로 이동할 때 드롭다운 가시성을 제거하여 사용자 지정 연결 프로파일을 쉽게 식별할 수 없습니다.

관련 정보

[Cisco 기술 지원 및 다운로드](#)

[비밀번호 스프레이 공격](#)

[Unauthorized Access Vulnerability 2023년 9월](#)

[ASA 컨피그레이션 가이드](#)

[FMC/FDM 컨피그레이션 가이드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.