

Cisco Firepower Device Manager에서 원격 액세스 VPN 서비스에 대한 위협 감지 구성

목차

소개

이 문서에서는 Cisco FDM(Firepower Device Manager)에서 원격 액세스 VPN 서비스에 대한 위협 감지를 구성하는 프로세스에 대해 설명합니다.

사전 요구 사항

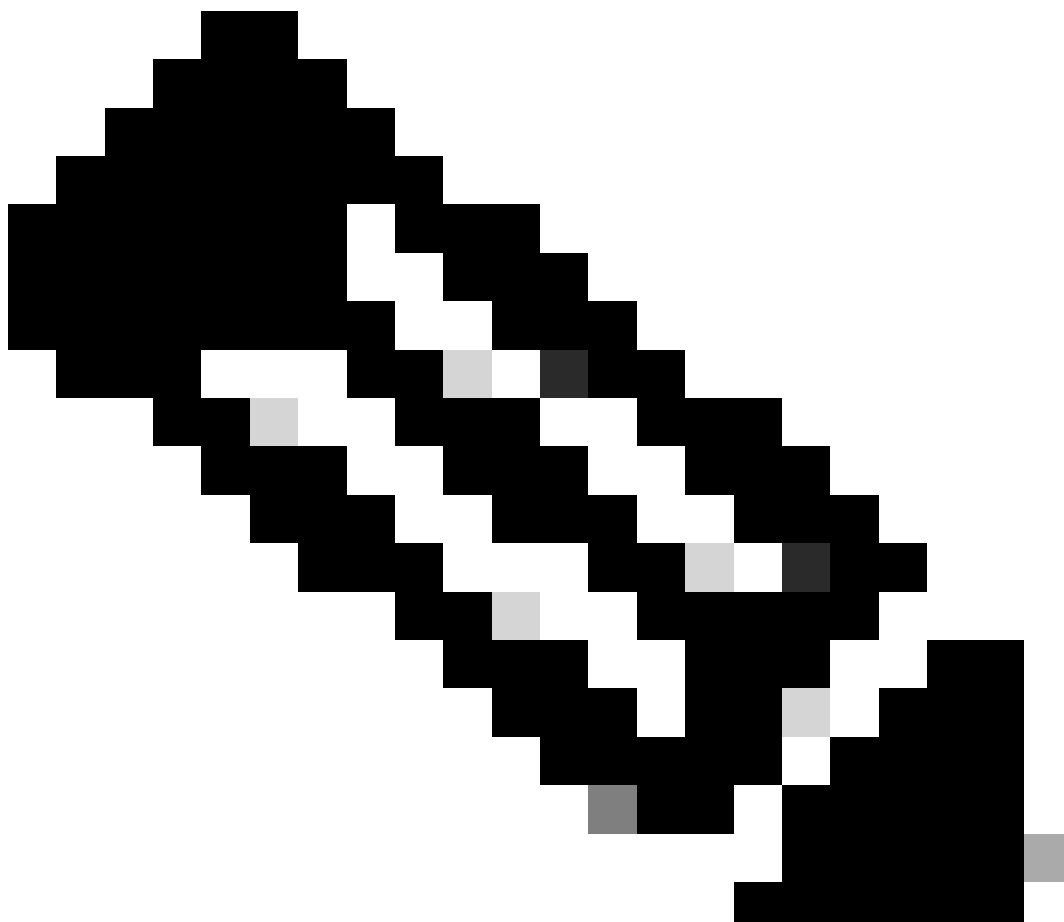
Cisco에서는 다음과 같은 주제에 대해 숙지할 것을 권장합니다.

- Cisco FTD(Secure Firewall Threat Defense).
- Cisco FDM(Firepower 장치 관리자).
- FTD의 원격 액세스 VPN(RAVPN).

요구 사항

이러한 위협 탐지 기능은 다음에 나열된 Cisco Secure Firewall Threat Defense 버전에서 지원됩니다.

- 7.0 버전 train->은(는) 이 특정 열차 내의 7.0.6.3 이상 버전에서 지원됩니다.
- 7.2 버전 train->은(는) 이 특정 열차 내의 7.2.9 이상 버전에서 지원됩니다.
- 7.4 버전 train->은(는) 이 특정 열차 내의 7.4.2.1 이상 버전에서 지원됩니다.
- 7.6 버전 train->은 7.6.0 이상 버전에서 지원됩니다.



참고: 이러한 기능은 버전 train 7.1 또는 7.3에서 현재 지원되지 않습니다.

사용되는 구성 요소

이 문서에 설명된 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Cisco Secure Firewall Threat Defense Virtual 버전 7.4.2.1

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.

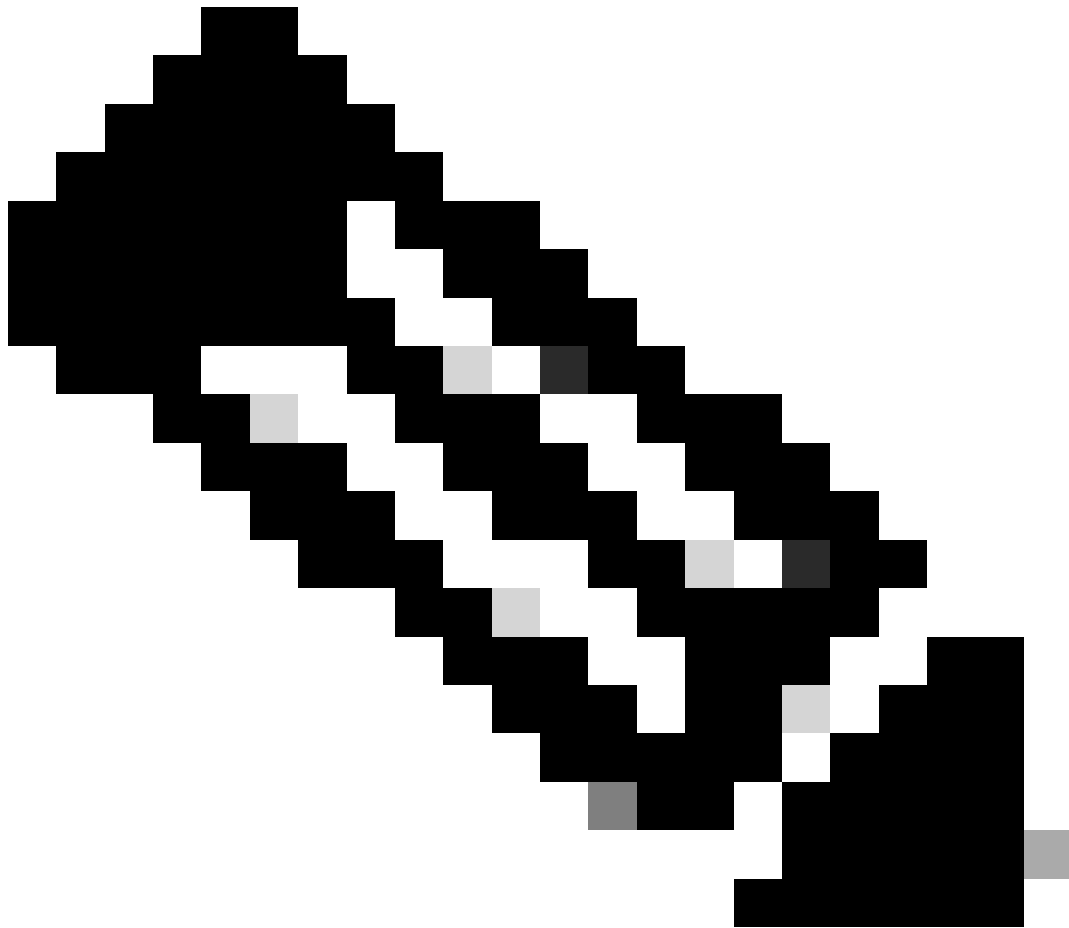
배경 정보

원격 액세스 VPN 서비스에 대한 위협 탐지 기능은 구성된 임계값을 초과하는 호스트(IP 주소)를 자동으로 차단하여 IP 주소의 차단 상태를 수동으로 제거할 때까지 추가 시도를 방지함으로써 IPv4 주

소에서 DoS(Denial of Service) 공격을 방지하는 데 도움이 됩니다. 다음 공격 유형에 사용할 수 있는 별도의 서비스가 있습니다.

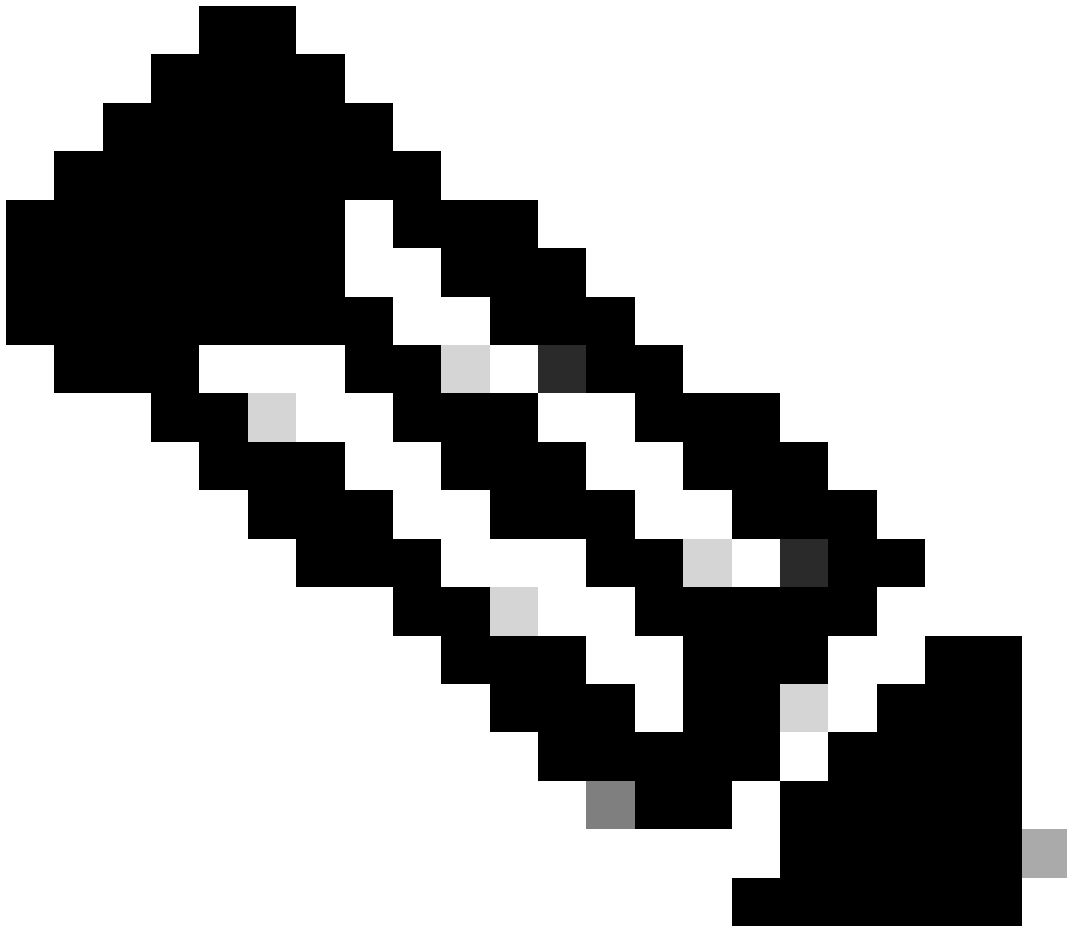
- 반복적으로 실패한 인증 시도: 원격 액세스 VPN 서비스에 대해 반복적으로 실패한 인증 시도 (무작위 대입 사용자 이름/비밀번호 스캔 공격).
- 클라이언트 시작 공격: 공격자가 시작하지만 단일 호스트에서 여러 번 원격 액세스 VPN 헤드 엔드에 대한 연결 시도를 완료하지 않는 경우.
- 연결이 잘못된 원격 액세스 VPN 서비스를 시도함: 공격자가 디바이스의 내부 기능만을 위해 특정 기본 제공 터널 그룹에 연결하려고 할 때 합법적인 엔드포인트는 이러한 터널 그룹에 연결을 시도하지 않습니다.

이러한 공격은 액세스 확보에 실패한 경우에도 컴퓨팅 리소스를 소비하고 유효한 사용자가 원격 액세스 VPN 서비스에 연결하는 것을 방지할 수 있습니다. 이러한 서비스를 활성화하면 방화벽은 구성된 임계값을 초과하는 호스트(IP 주소)를 자동으로 차단합니다. 이렇게 하면 IP 주소의 차단 (shun)을 수동으로 제거할 때까지 추가 시도를 방지할 수 있습니다.



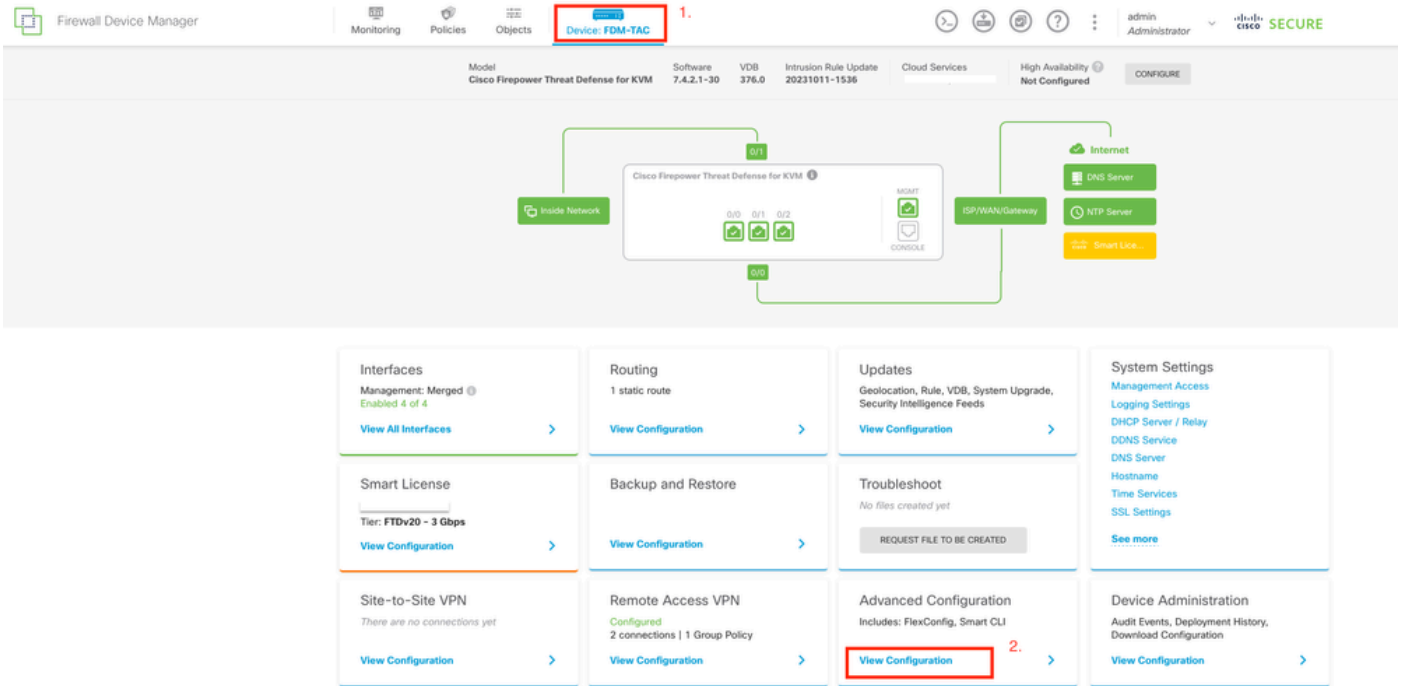
참고: 기본적으로 원격 액세스 VPN에 대한 모든 위협 감지 서비스는 비활성화되어 있습니다.

구성

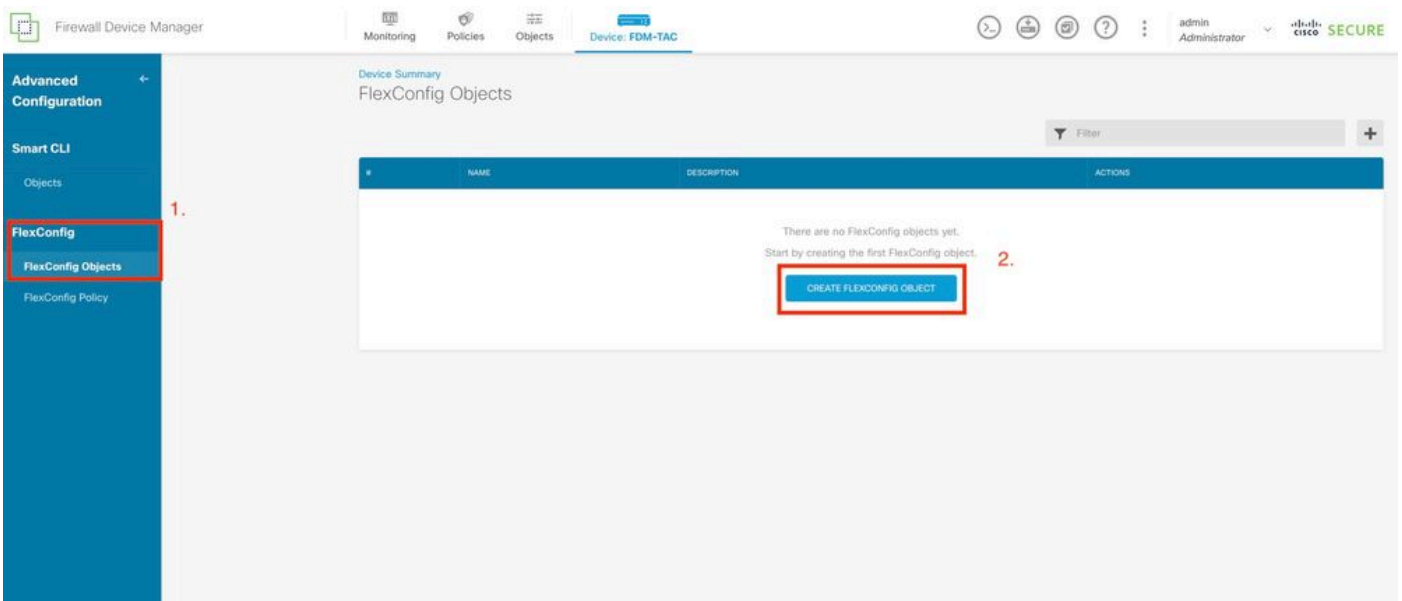


참고: Secure Firewall Threat Defense에서 이러한 기능의 컨피그레이션은 현재 FlexConfig를 통해서만 지원됩니다.

1. Firepower 장치 관리자에 로그인합니다.
2. FlexConfig 개체를 구성하려면 Device(디바이스) > Advanced Configuration(고급 컨피그레이션) > FlexConfig > FlexConfig Objects(FlexConfig 개체)로 이동한 다음 Create FlexConfig object(FlexConfig 개체 생성)를 클릭합니다.



FDM 홈 페이지에서 '고급 구성'을 편집합니다.



FlexConfig 개체를 만듭니다.

3. FlexConfig 개체 창이 열리면 원격 액세스 VPN에 대한 위협 탐지 기능을 활성화하는 데 필요한 구성을 추가합니다.

기능 1: 내부 전용(유효하지 않음) VPN 서비스에 대한 연결 시도에 대한 위협 감지

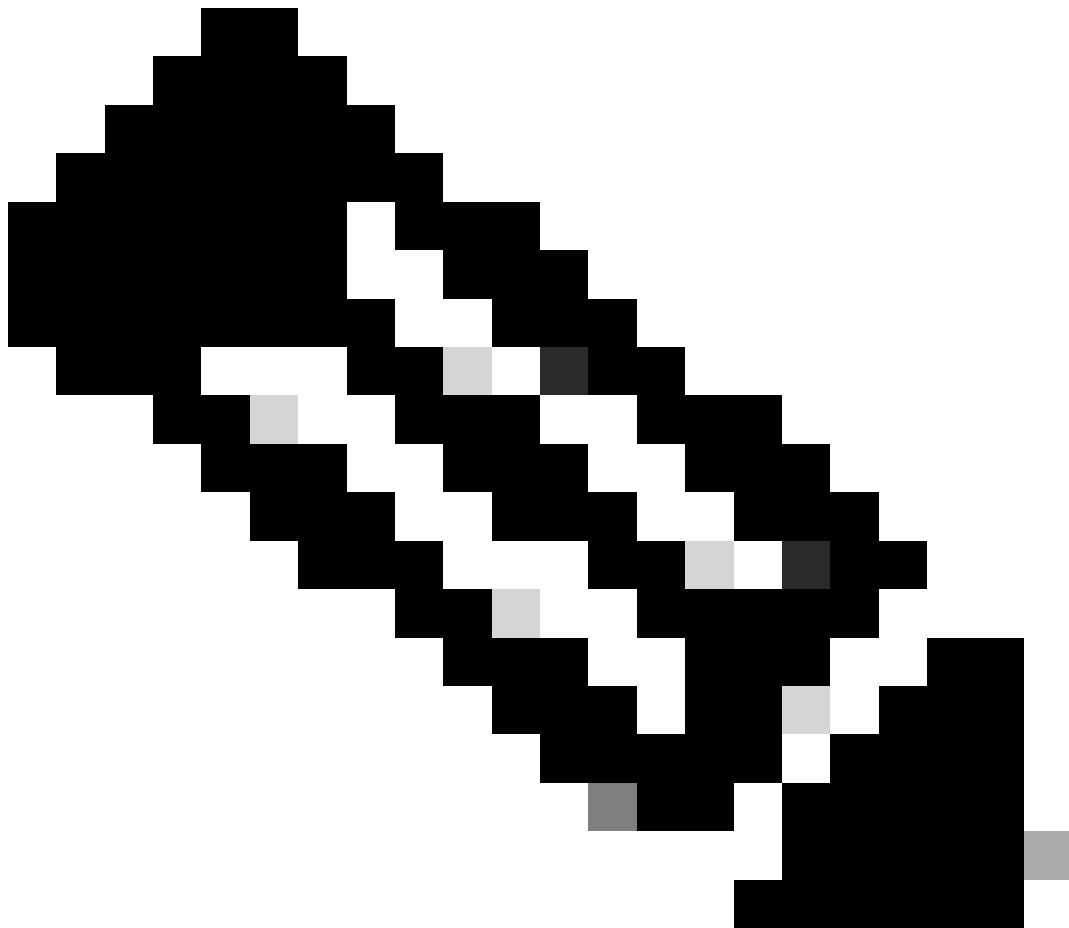
이 서비스를 활성화하려면 FlexConfig 개체 텍스트 상자에서 threat-detection service invalid-vpn-access 명령을 추가합니다.

기능 2: 원격 액세스 VPN 클라이언트 시작 공격을 위한 위협 감지

이 서비스를 활성화하려면 FlexConfig 개체 텍스트 상자에 threat-detection service remote-access-client-initiations hold-down <minutes> threshold <count> 명령을 추가합니다. 여기서

- hold-down <minutes>는 연속 연결 시도가 카운트되는 마지막 시작 시도 이후의 기간을 정의합니다. 연속 연결 시도 횟수가 이 기간 내에 구성된 임계값을 충족하면 공격자의 IPv4 주소가 차단됩니다. 이 기간은 1분에서 1440분 사이로 설정할 수 있습니다.
- threshold <count>는 중지를 트리거하는 데 필요한 연결 시도 횟수입니다. 임계값을 5~100으로 설정할 수 있습니다.

예를 들어, 보류 기간이 10분이고 임계값이 20이면 10분 범위 내에서 20회 연속 연결 시도가 있으면 IPv4 주소가 자동으로 차단됩니다.



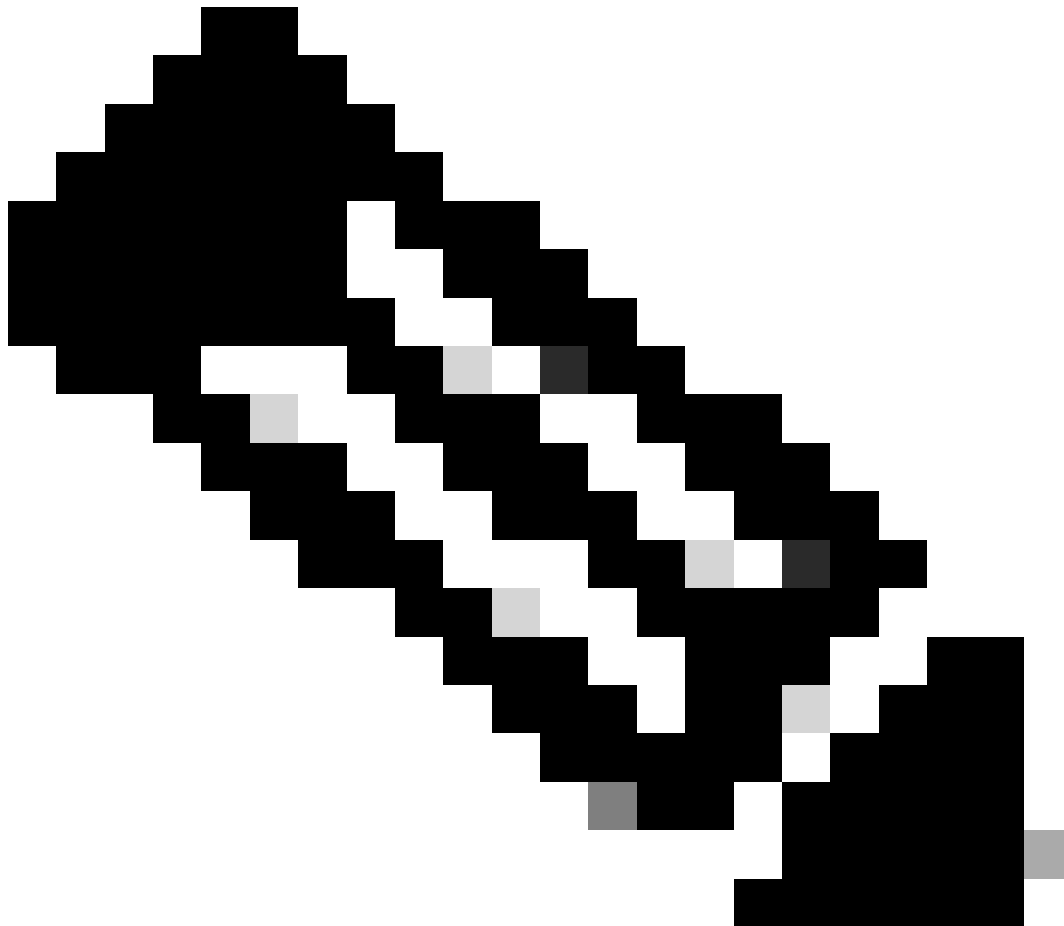
참고: 보류 및 임계값을 설정할 때 NAT 사용을 고려하십시오. 동일한 IP 주소에서 많은 요청을 허용하는 PAT를 사용하는 경우 더 높은 값을 고려하십시오. 이렇게 하면 유효한 사용자가 연결할 수 있는 충분한 시간이 확보됩니다. 예를 들어, 호텔에서는 수많은 사용자가 단기간에 연결을 시도할 수 있다.

기능 3: 원격 액세스 VPN 인증 실패에 대한 위협 감지

이 서비스를 활성화하려면 FlexConfig 개체 텍스트 상자에 `threat-detection service remote-access-authentication hold-down<minutes> threshold <count>` 명령을 추가합니다. 여기서

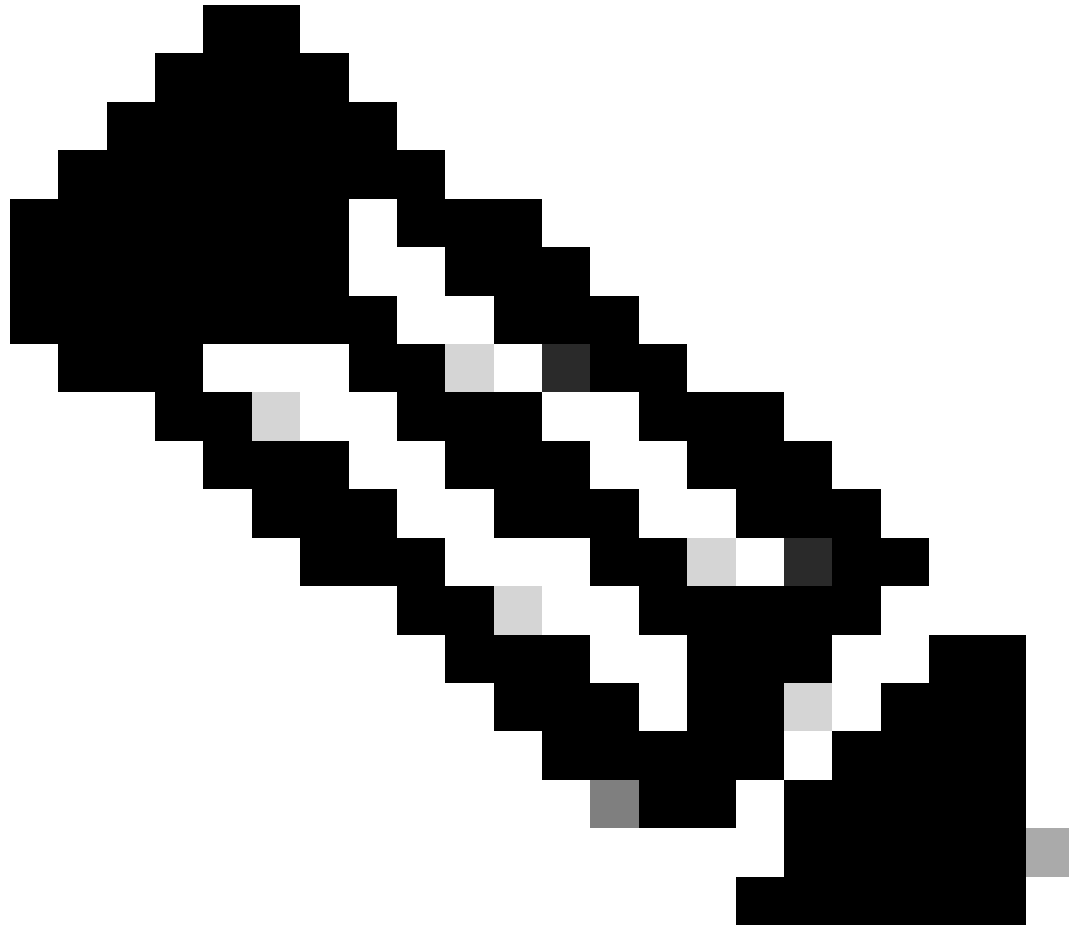
- `hold-down <minutes>`는 연속 실패가 계산되는 마지막 실패 시도 이후의 기간을 정의합니다. 연속 인증 실패 수가 이 기간 내에 구성된 임계값을 충족하면 공격자의 IPv4 주소가 차단됩니다. 이 기간은 1분에서 1440분 사이로 설정할 수 있습니다.
- `threshold <count>`는 중지를 트리거하기 위해 보류 기간 내에 필요한 실패한 인증 시도 횟수입니다. 임계값을 1에서 100 사이로 설정할 수 있습니다.

예를 들어, 보류 기간이 10분이고 임계값이 20이면 10분 범위 내에 연속 인증 실패가 20개 있는 경우 IPv4 주소가 자동으로 차단됩니다



참고: 보류 및 임계값을 설정할 때 NAT 사용을 고려하십시오. 동일한 IP 주소에서 많은 요청을 허용하는 PAT를 사용하는 경우 더 높은 값을 고려하십시오. 이렇게 하면 유효한 사용

자가 연결할 수 있는 충분한 시간이 확보됩니다. 예를 들어, 호텔에서는 수많은 사용자가 단기간에 연결을 시도할 수 있다.

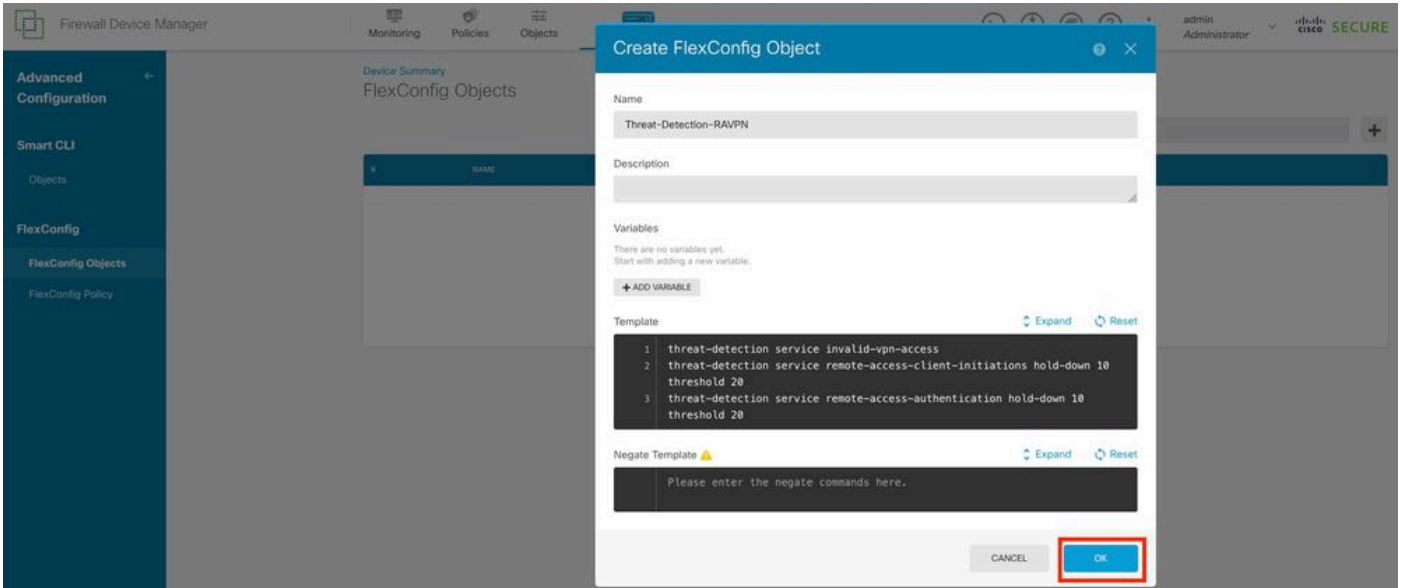


참고: SAML을 통한 인증 실패는 아직 지원되지 않습니다.

이 예제 컨피그레이션에서는 보류 기간이 10분이고, 클라이언트 시작 및 실패한 인증 시도에 대한 임계값이 20인 원격 액세스 VPN에 대해 사용 가능한 세 가지 위협 감지 서비스를 활성화합니다. 환경 요구 사항에 따라 보류 및 임계값을 구성합니다.

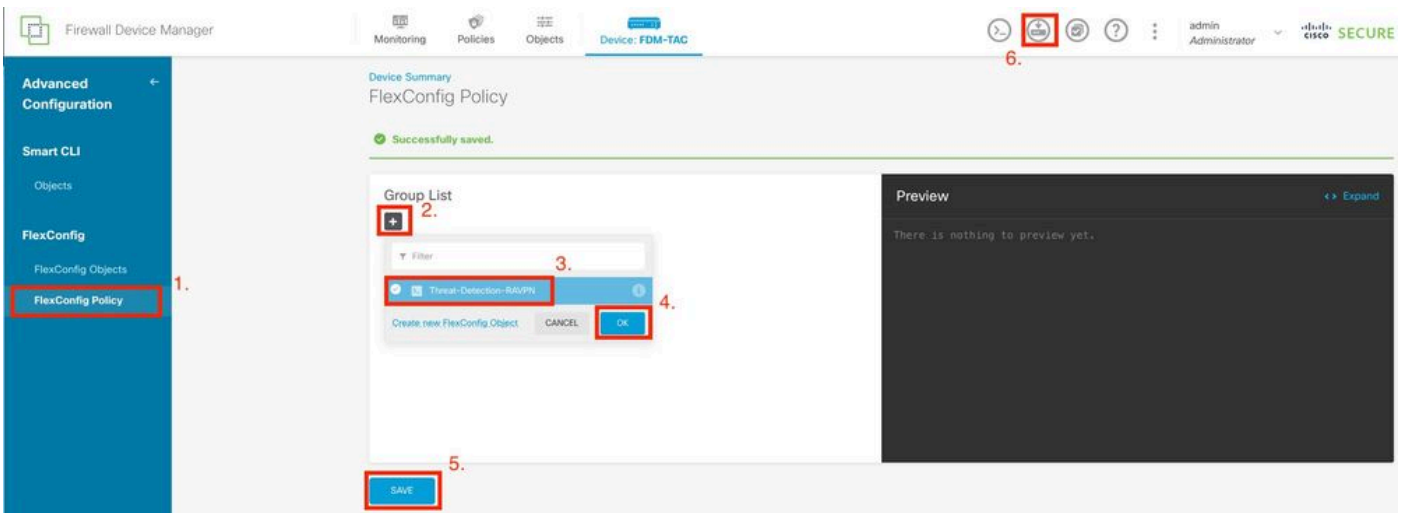
이 예에서는 단일 FlexConfig 개체를 사용하여 3개의 사용 가능한 기능을 활성화합니다.

```
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
```

FlexConfig 개체 기준을 정의합니다.

4. FlexConfig 개체가 생성되면 FlexConfig > FlexConfig Policy로 이동하여 Group List(그룹 목록) 아래의 더하기 기호를 찾습니다. RAVPN 위협 감지를 위해 생성한 FlexConfig 객체를 선택하고 OK(확인)를 클릭하여 해당 객체를 그룹 목록에 추가합니다. 이렇게 하면 명령의 CLI 미리 보기가 채워집니다. 이 미리 보기를 검토하여 정확한지 확인하십시오. SAVE(저장)를 선택하고 FTD(Firepower 위협 방어)에 대한 변경 사항을 구축합니다.



FlexConfig 정책을 수정하고 FlexConfig 개체를 할당합니다.

다음을 확인합니다.

위협 감지 RAVPN 서비스에 대한 통계를 표시하려면 FTD의 CLI에 로그인하고 show threat-detection service [service] [entries|details] 명령을 실행합니다. 여기서 서비스는 remote-access-authentication, remote-access-client-initiations 또는 invalid-vpn-access일 수 있습니다.

다음 매개변수를 추가하여 보기를 더 제한할 수 있습니다.

- `entries` — 위협 감지 서비스에서 추적하는 항목만 표시합니다. 예를 들어, 인증 시도가 실패한 IP 주소.
- `details` — 서비스 세부 정보와 서비스 항목을 모두 표시합니다.

활성화된 모든 위협 탐지 서비스의 통계를 표시하려면 `show threat-detection service` 명령을 실행합니다.

```
<#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
```

원격 액세스 인증 서비스에 대해 추적되는 잠재적 공격자에 대한 자세한 내용을 보려면 `show threat-detection service <service> entries` 명령을 실행합니다.

```
<#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.

특정 위협 감지 원격 액세스 VPN 서비스의 일반 통계 및 세부 정보를 보려면 `show threat-detection service <service> details` 명령을 실행합니다.

<#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.



참고: 항목은 위협 탐지 서비스에서 추적하는 IP 주소만 표시합니다. IP 주소가 차단 조건을 충족한 경우 차단 수가 증가하고 IP 주소가 더 이상 항목으로 표시되지 않습니다.

또한 VPN 서비스에 의해 적용된 차단을 모니터링하고 단일 IP 주소 또는 모든 IP 주소에 대한 차단을 다음 명령으로 제거할 수 있습니다.

- `show shun [ip_address]`

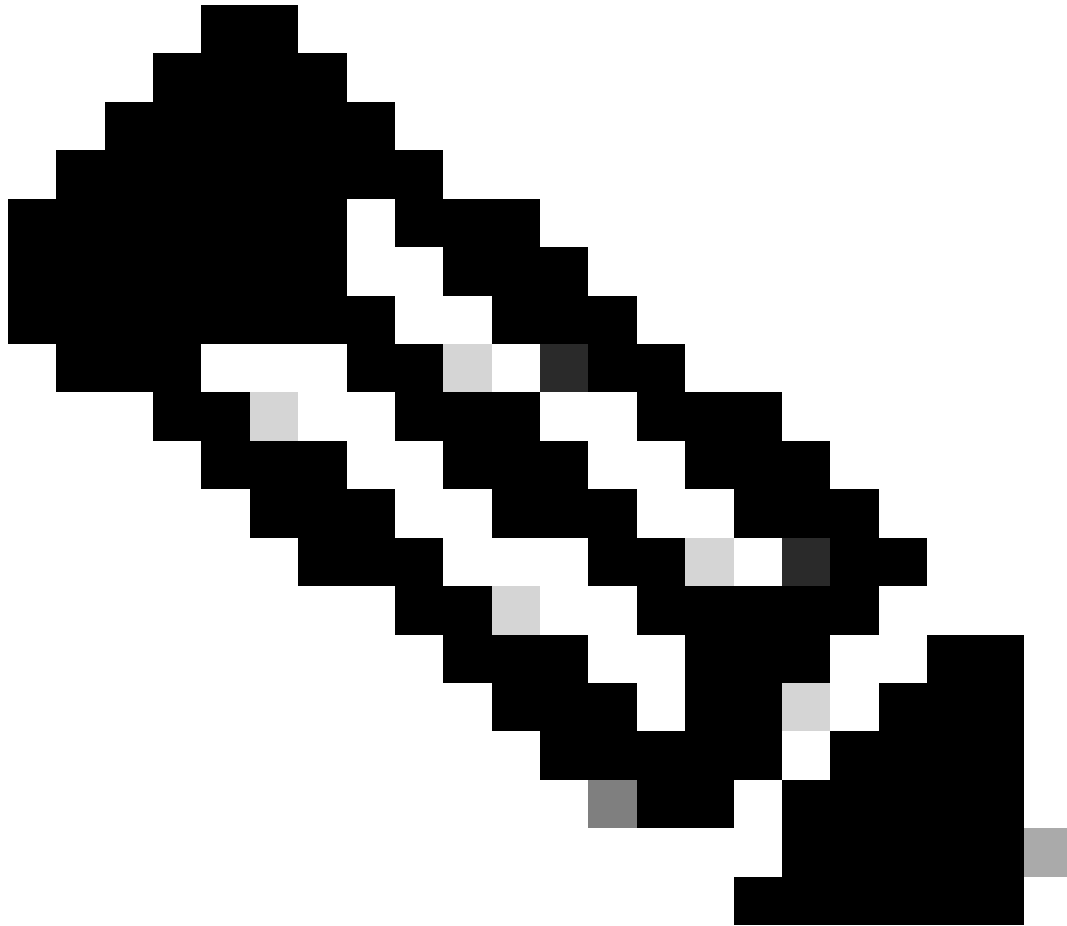
차단된 호스트를 표시합니다. 여기에는 VPN 서비스에 대한 위협 탐지에 의해 자동으로 차단되거나 `shun` 명령을 수동으로 사용하는 호스트가 포함됩니다. 선택적으로 보기를 지정된 IP 주소로 제한할 수 있습니다.

- `shun ip_address [interface if_name] 없음`

지정된 IP 주소에서만 `shun`을 제거합니다. 둘 이상의 인터페이스에서 주소가 차단되고 일부 인터페이스에서 `shun`을 그대로 두려는 경우 선택적으로 `shun`에 대한 인터페이스 이름을 지정할 수 있습니다.

- 맑은 쉐

모든 IP 주소 및 모든 인터페이스에서 shun을 제거합니다.



참고: VPN 서비스에 대한 위협 탐지로 차단된 IP 주소는 스캐닝 위협 탐지에만 적용되는 show threat-detection shun 명령에 나타나지 않습니다.

원격 액세스 VPN에 대한 위협 탐지 서비스와 관련된 각 명령 출력의 모든 세부 정보 및 사용 가능한 syslog 메시지를 읽으려면 [명령 참조 문서](#)를 참조하십시오.

관련 정보

- 추가 지원이 필요한 경우 TAC(Technical Assistance Center)에 문의하십시오. 유효한 지원 계약이 필요합니다. [Cisco Worldwide Support Contacts](#).
- [여기서](#) Cisco VPN Community를 방문할 수도 [있습니다](#).
- [Cisco 기술 지원 및 다운로드](#)

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.