DAP 인증서 매개변수 평가를 위한 LUA 스크립트 구성

목차

소개

이 문서에서는 사용자가 VPN에 연결하려고 할 때 보유해야 하는 인증서 매개변수를 탐지하도록 LUA 스크립트를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC(Secure Firewall Management Center)
- 원격 액세스 VPN 구성(RAVPN)
- 기본 LUA 스크립트 코딩
- 기본 SSL 인증서
- DAP(동적 액세스 정책)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Secure Firewall 버전 7.7.0
- Secure Firewall Management Center 버전 7.7.0

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

DAP는 네트워크 관리자가 네트워크에 연결하려는 사용자 및 장치의 다양한 특성을 기반으로 세분화된 액세스 제어 정책을 정의할 수 있는 강력한 기능입니다. DAP의 주요 기능 중 하나는 클라이언트 장치에 설치된 디지털 인증서를 평가하는 정책을 만드는 기능입니다. 이러한 인증서는 사용자를 인증하고 디바이스 규정 준수를 확인하는 보안 방법으로 사용됩니다.

관리자는 Cisco Secure FMC 인터페이스 내에서 다음과 같은 특정 인증서 매개변수를 평가하도록 DAP 정책을 구성할 수 있습니다.

- 제목
- 발급자
- 주체 대체 이름
- 일련 번호
- 인증서 저장소

그러나 FMC GUI를 통해 사용할 수 있는 인증서 평가 옵션은 이러한 사전 정의된 특성으로 제한됩니다. 이러한 제한은 관리자가 인증서 또는 사용자 지정 확장의 특정 필드와 같이 더 자세한 인증서 정보 또는 사용자 지정 인증서 정보를 기반으로 정책을 적용하려는 경우 표준 DAP 컨피그레이션만으로는 이를 구현할 수 없음을 의미합니다.

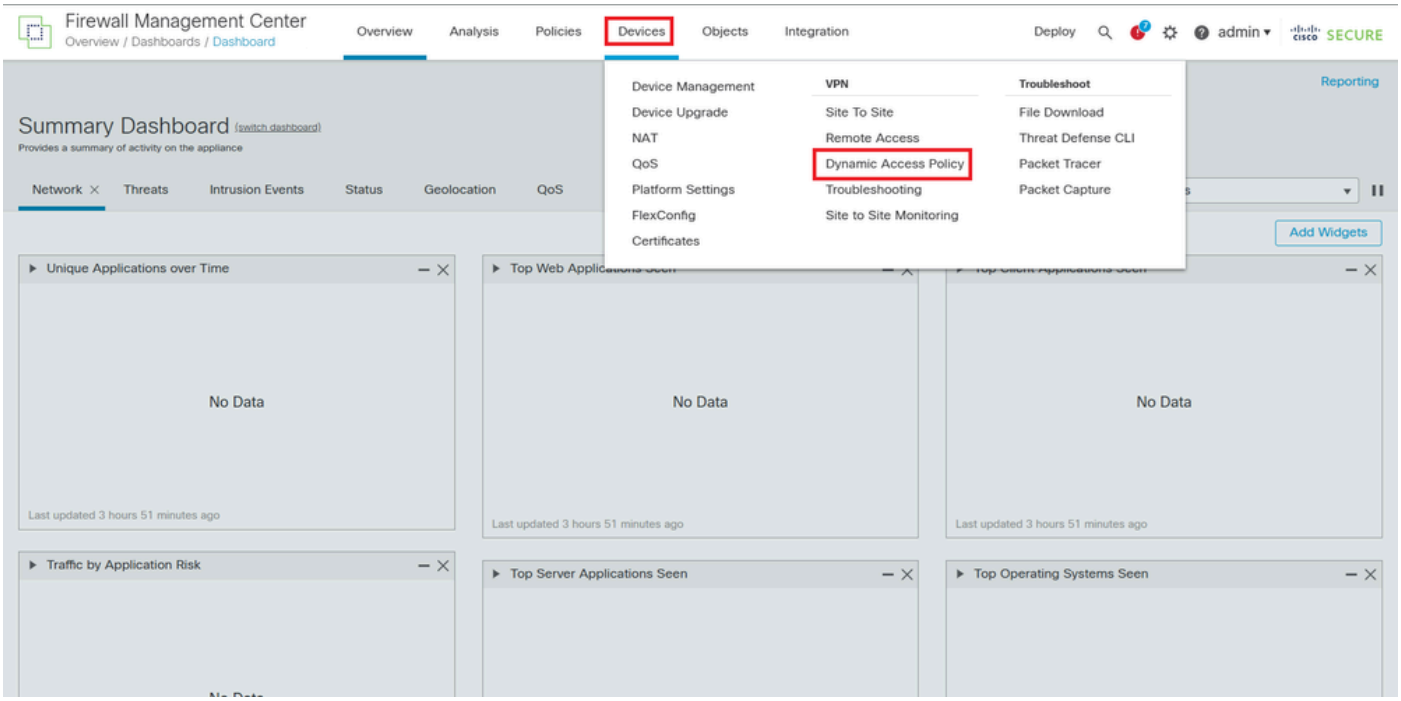
이러한 한계를 극복하기 위해 Cisco Secure Firewall은 DAP 내에서 LUA 스크립팅의 통합을 지원합니다. LUA 스크립트는 FMC 인터페이스를 통해 노출되지 않는 추가 인증서 특성에 액세스하고 평가할 수 있는 유연성을 제공합니다. 이 기능을 통해 관리자는 세부적인 인증서 데이터를 기반으로 더욱 정교하고 맞춤화된 액세스 정책을 구현할 수 있습니다.

LUA 스크립팅을 활용하면 조직 이름, 사용자 지정 확장 또는 기타 인증서 메타데이터와 같은 기본 매개변수 이외의 인증서 필드를 분석할 수 있습니다. 이 확장된 평가 기능은 조직의 요구 사항에 맞게 정책을 조정할 수 있도록 하여, 특정 세부 기준을 충족하는 인증서를 가진 클라이언트만 액세스 권한을 부여하도록 함으로써 보안을 강화합니다.

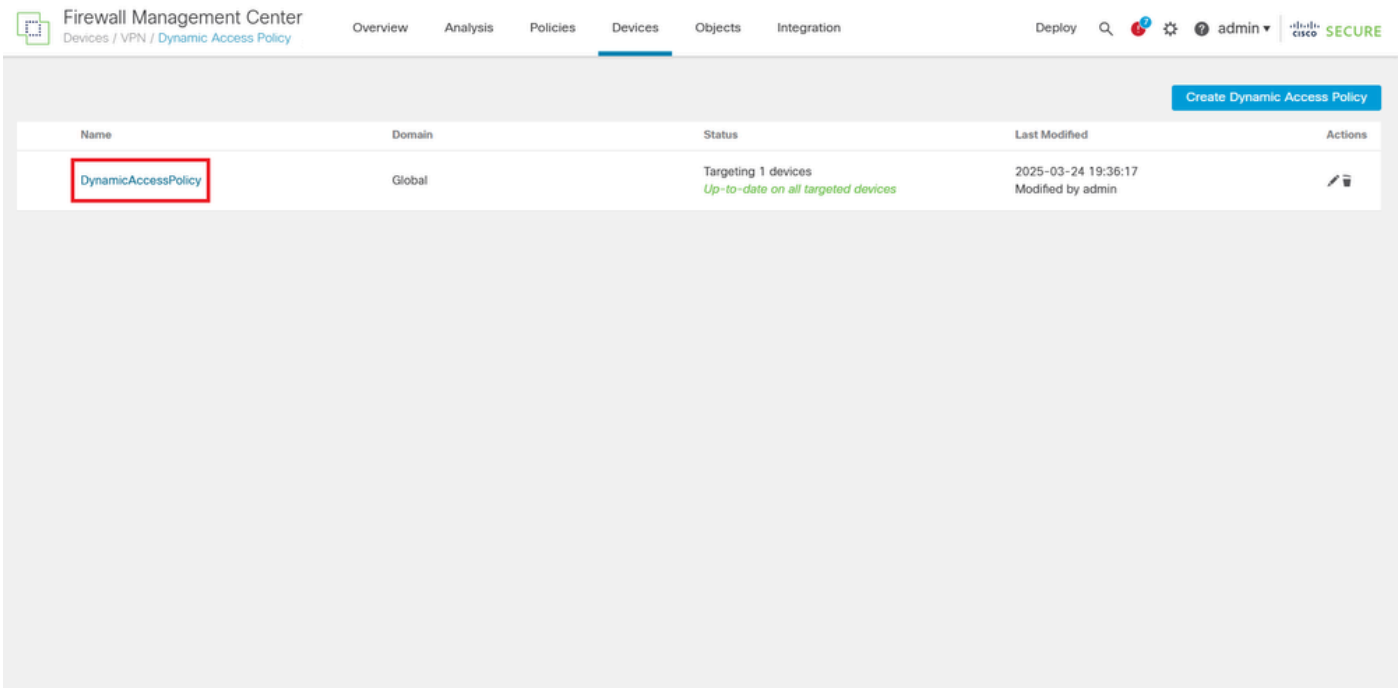
따라서 이 문서에서는 LUA 스크립팅 기능을 활용하여 클라이언트 인증서 내의 Organization 매개변수를 평가하도록 LUA 스크립트를 구성합니다.

설정

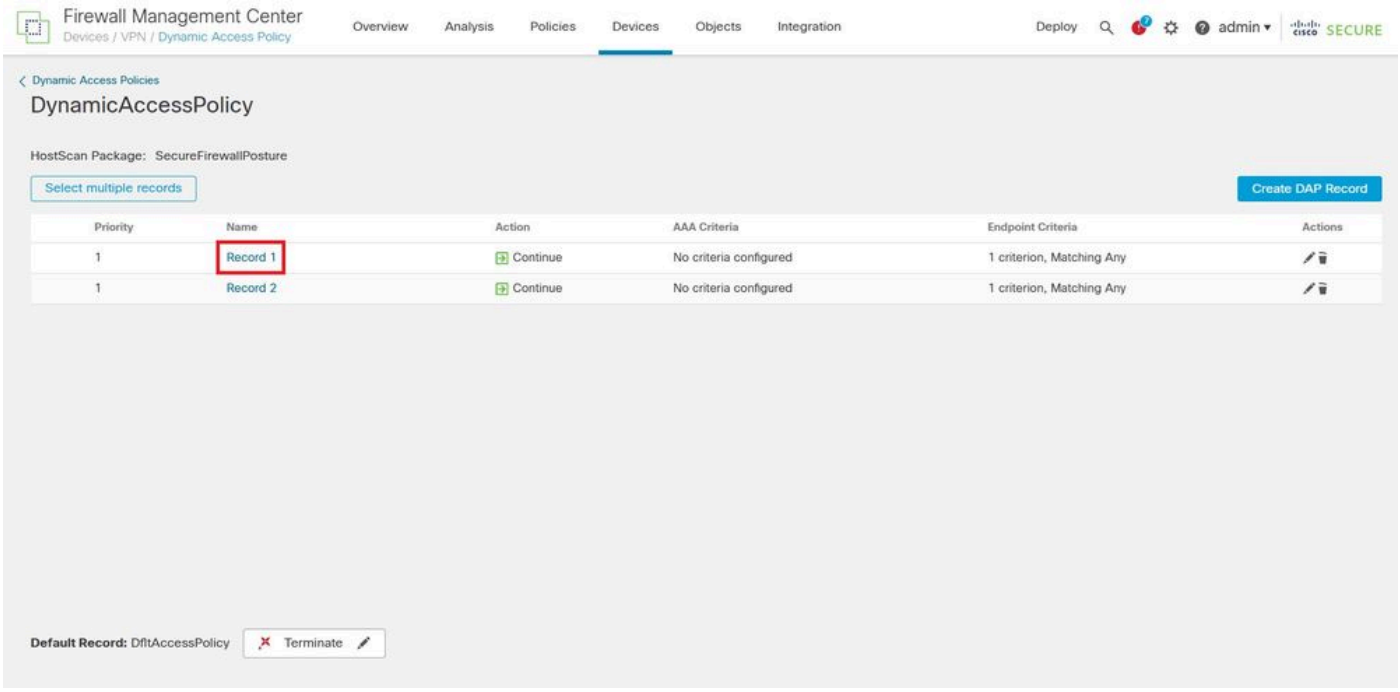
1. FMC GUI에 로그인한 다음 대시보드에서 메뉴의 Devices(디바이스) > Dynamic Access Policy(동적 액세스 정책)로 이동합니다.



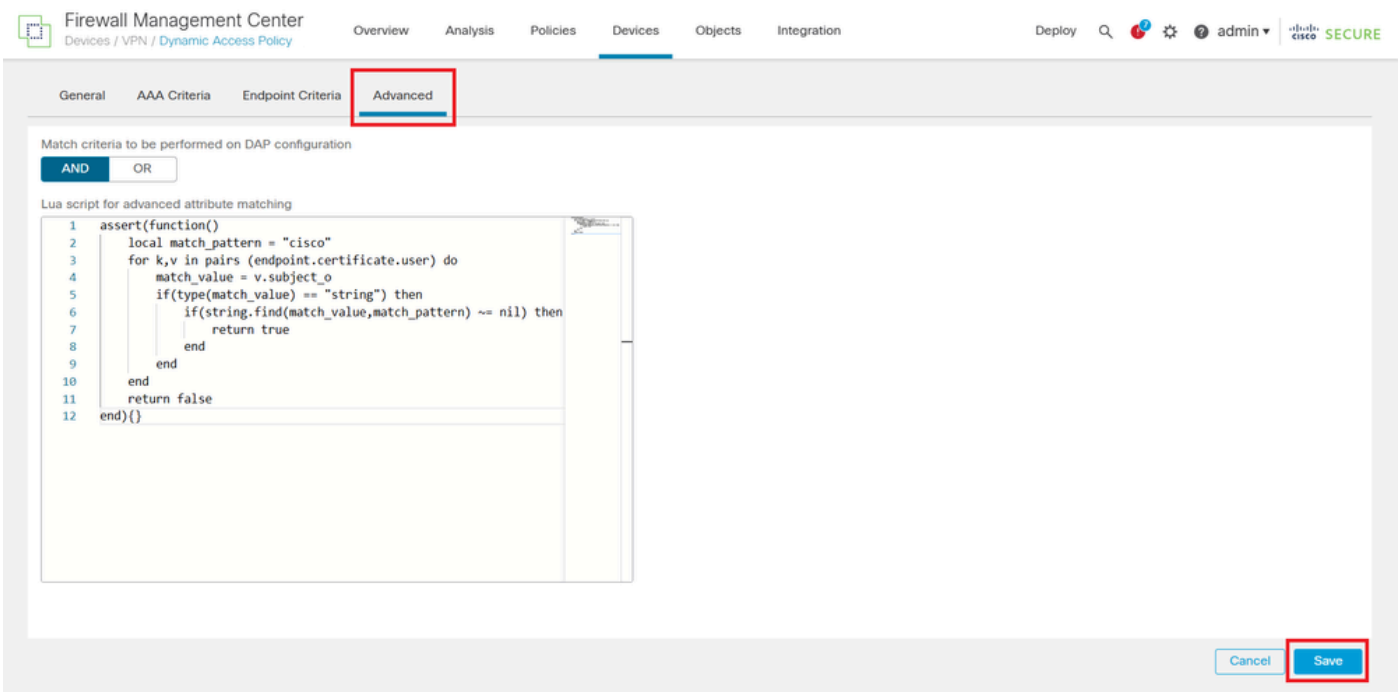
2. RAVPN 컨피그레이션에 적용된 DAP 정책을 엽니다.



3. 원하는 레코드를 편집하여 레코드 이름을 클릭하여 LUA 스크립트를 구성합니다.



4. 선택한 레코드에서 고급 탭으로 이동하여 필수 인증서 매개변수를 평가하는 LUA 스크립트를 입력합니다. 스크립트를 구성한 후 Save(저장)를 클릭하여 변경 사항을 적용합니다. 변경 사항이 DAP 레코드에 저장되면 정책을 구축하여 업데이트된 컨피그레이션을 FTD 디바이스에 푸시합니다 .



참고: 이 문서에 제시된 코드는 클라이언트 장치에 설치된 인증서를 평가하도록 설계되었으며 , 특히 Subject(주체) 필드 내의 Organization(조직) 매개변수가 cisco 값과 일치하는 인증서가 있는지 확인합니다.

<#root>

```
assert(function()
```

```
    local match_pattern = "
cisco
"
    for k,v in pairs (
endpoint.certificate.user
) do
        match_value =
v.subject_o
        if(type(match_value) == "string") then
            if(string.find(match_value,match_pattern) ~= nil) then

return true

            end
        end
    end
    return false
end){}
```

- 스크립트는 match_pattern 변수를 cisco로 설정하며, 이는 찾을 대상 조직 이름입니다.
- for 루프를 사용하여 엔드포인트에서 사용 가능한 모든 사용자 인증서를 반복합니다.
- 각 인증서에 대해 Organization 필드(subject_o)를 추출합니다.
- Organization(조직) 필드가 문자열인지 확인한 다음 그 안에서 match_pattern을 검색합니다.
- 일치 항목이 발견되면 스크립트는 true를 반환하여 인증서가 정책 기준을 충족함을 나타냅니다.
- 모든 인증서를 검사한 후 일치하는 인증서가 없으면 스크립트는 false를 반환하여 정책이 액세스를 거부하도록 합니다.

이 접근 방식을 통해 관리자는 FMC GUI에 의해 노출되는 표준 매개변수를 넘어 맞춤형 인증서 검증 논리를 구현할 수 있습니다.

다음을 확인합니다.

FTD의 DAP 컨피그레이션에 코드가 있는지 확인하려면 more dap.xml 명령을 실행합니다.

<#root>

```
firepower#
more dap.xml
```

Record 1

and

```
assert(function()
        local match_pattern = "cisco"
        for k,v in pairs (endpoint.certificate.user) do
                match_value = v.subject_o
                if(type(match_value) == "string") then
                        if(string.find(match_value,match_pattern) ~= nil) then
                                return true
```

```
                    end
                end
            end
            return false
end) {}
```

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.