LUA-script configureren voor evaluatie van DAP-certificaatparameters

Inhoud

Inleiding

In dit document wordt beschreven hoe u een LUA-script configureert om certificaatparameters te detecteren die gebruikers moeten hebben wanneer ze proberen verbinding te maken met de VPN.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Veilig Firewall Management Center (FMC)
- Remote Access VPN-configuratie (RAVPN)
- Basis LUA-scriptcodering
- Standaard SSL-certificaten
- Dynamisch toegangsbeleid (DAP)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Secure Firewall versie 7.7.0
- Secure Firewall Management Center versie 7.7.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

DAP is een krachtige functie waarmee netwerkbeheerders granulair toegangscontrolebeleid kunnen definiëren op basis van verschillende kenmerken van gebruikers en apparaten die proberen verbinding te maken met het netwerk. Een van de belangrijkste mogelijkheden van DAP is de mogelijkheid om beleid te maken dat digitale certificaten evalueert die op clientapparaten zijn geïnstalleerd. Deze certificaten dienen als een veilige methode om gebruikers te verifiëren en de naleving van de apparaatvereisten te controleren.

Binnen de Cisco Secure FMC-interface kunnen beheerders DAP-beleid configureren om specifieke certificaatparameters te beoordelen, zoals:

- onderwerp
- uitgever
- Alternatieve naam onderwerp
- serienummer
- certificaatarchief

De opties voor certificaatevaluatie die beschikbaar zijn via de FMC GUI zijn echter beperkt tot deze vooraf gedefinieerde kenmerken. Deze beperking houdt in dat als een beheerder beleid wil afdwingen op basis van meer gedetailleerde of aangepaste certificaatinformatie, zoals specifieke velden in het certificaat of aangepaste extensies, dit niet kan worden bereikt met alleen de standaard DAP-configuratie.

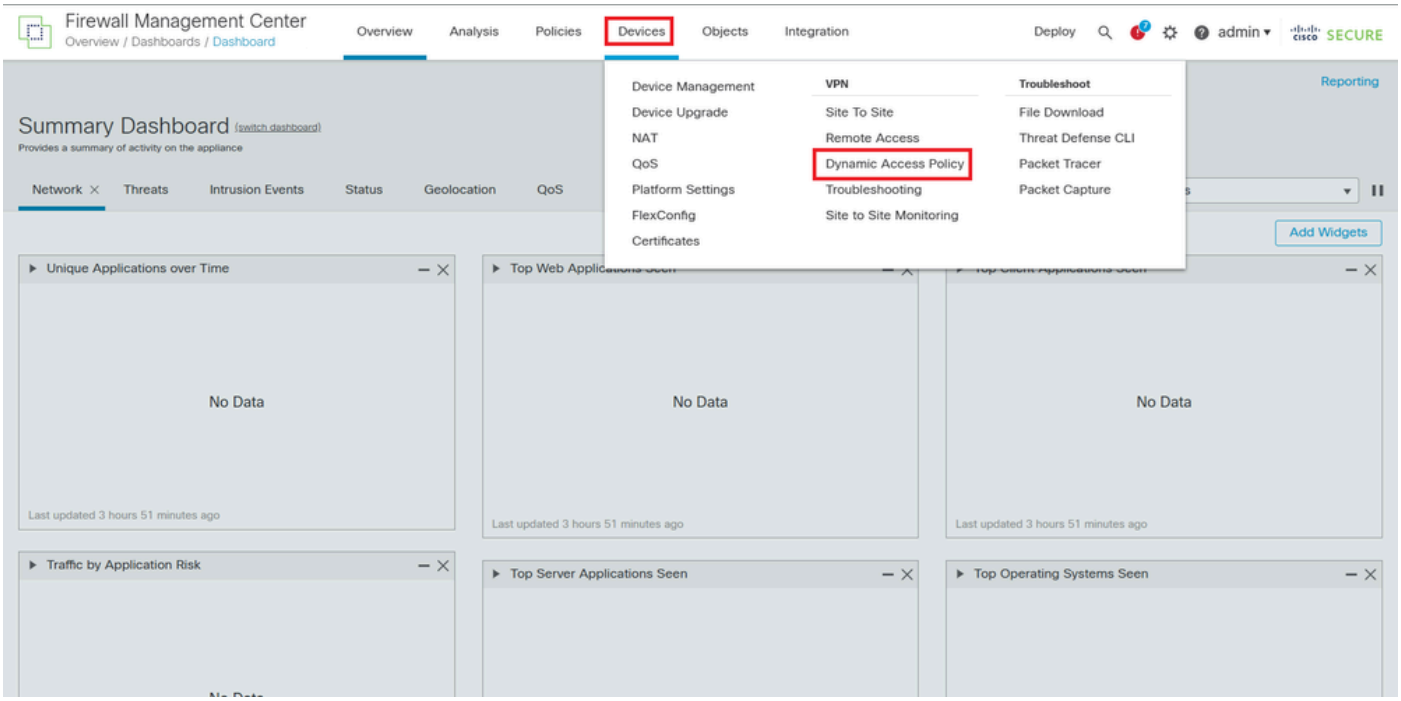
Om deze beperking te overwinnen, ondersteunt Cisco Secure Firewall de integratie van LUA-scripting binnen DAP. LUA-scripts bieden de flexibiliteit om toegang te krijgen tot aanvullende certificaatkenmerken die niet via de FMC-interface worden weergegeven en deze te evalueren. Met deze mogelijkheid kunnen beheerders geavanceerdere en aangepaste toegangsbeleidsregels implementeren op basis van gedetailleerde certificaatgegevens.

Door gebruik te maken van LUA-scripts wordt het mogelijk om certificaatvelden te analyseren die verder gaan dan de standaardparameters, zoals organisatienamen, aangepaste extensies of andere certificaatmetagegevens. Deze uitgebreide evaluatiecapaciteit vergroot de veiligheid doordat het beleid nauwkeurig kan worden afgestemd op de vereisten van de organisatie, zodat alleen klanten met certificaten die voldoen aan specifieke, gedetailleerde criteria toegang krijgen.

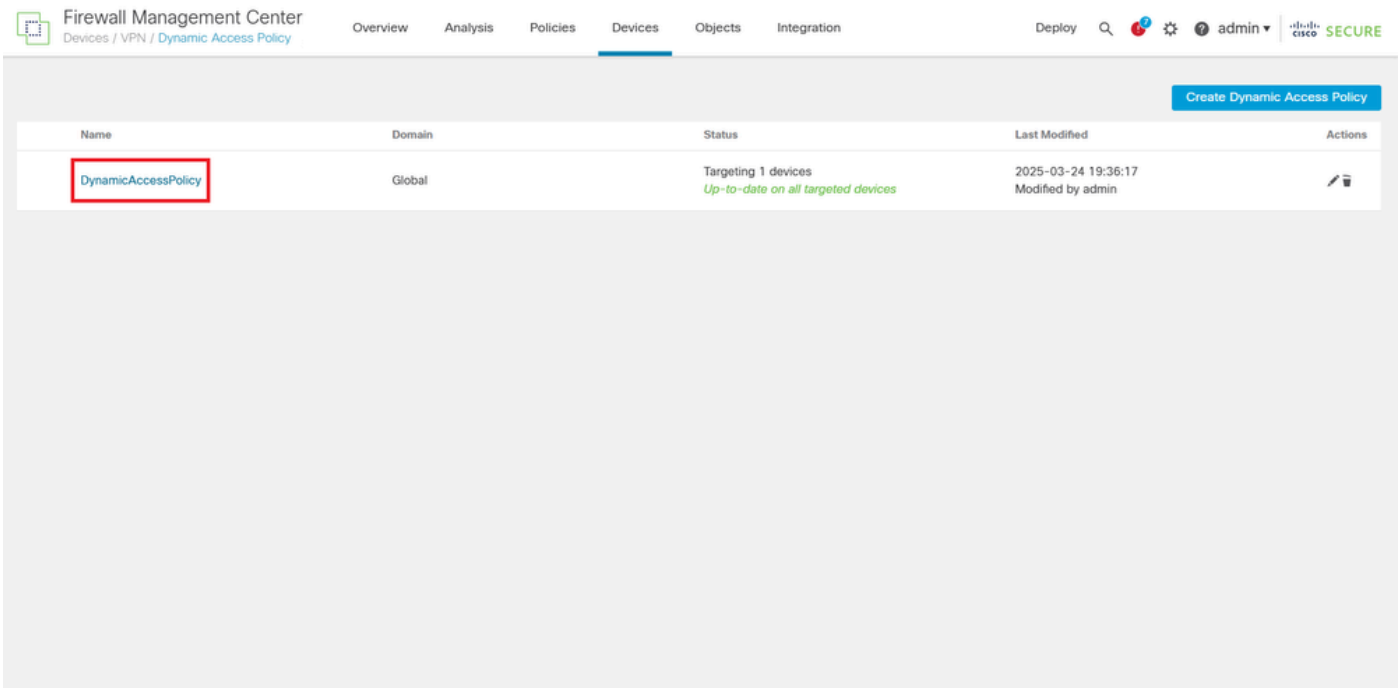
Daarom wordt in dit document een LUA-script geconfigureerd om de parameter Organization binnen een clientcertificaat te evalueren door gebruik te maken van LUA-scriptmogelijkheden.

Configuratie

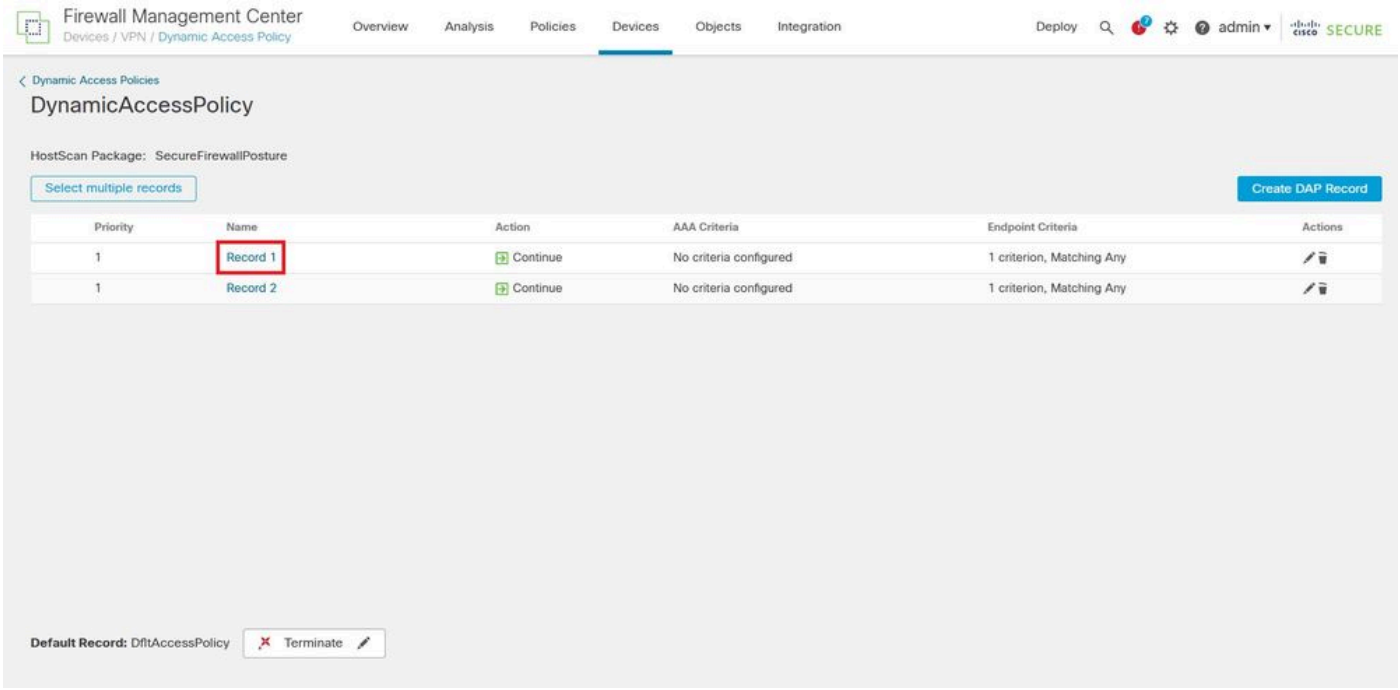
1.Log in op de FMC GUI en navigeer vervolgens vanuit het dashboard naar Apparaten > Dynamisch toegangsbeleid in het menu.



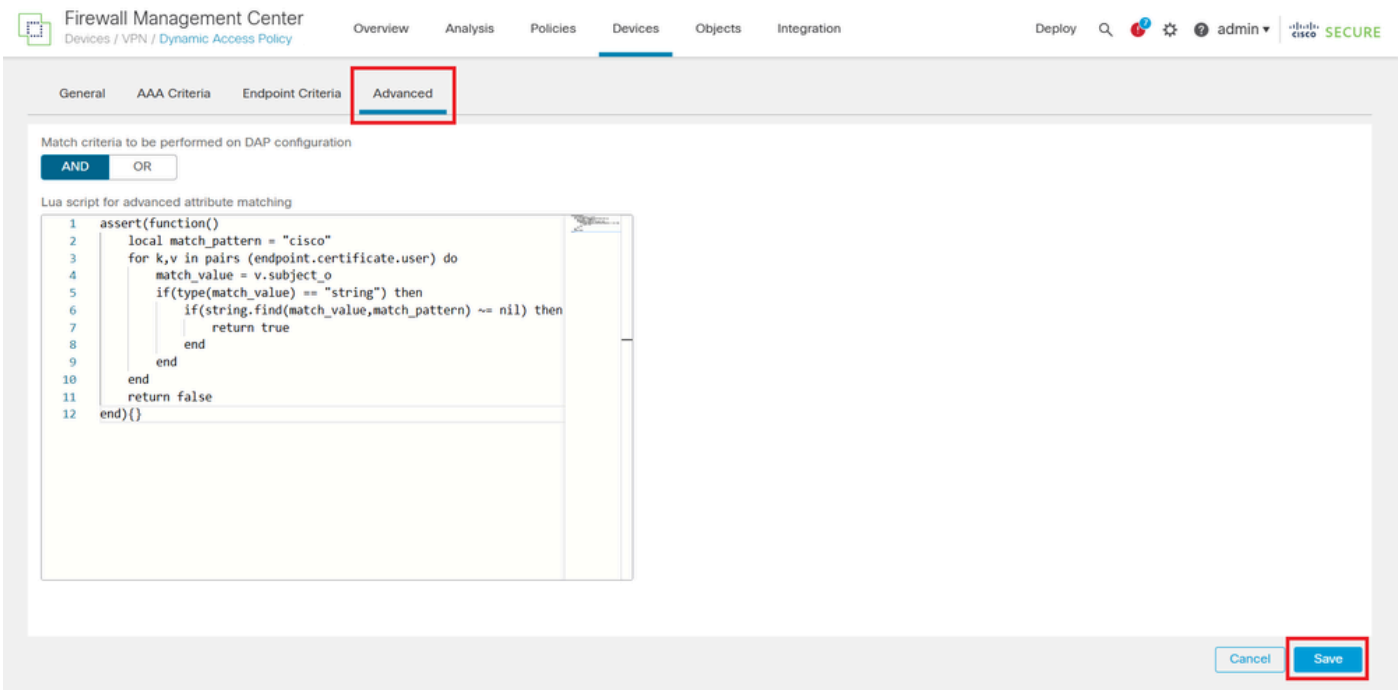
2.Open het DAP-beleid dat is toegepast op de RAVPN-configuratie.



3. Bewerk de gewenste record om het LUA-script te configureren door op de naam van de record te klikken.



4. Navigeer binnen de geselecteerde record naar het tabblad Geavanceerd om het LUA-script in te voeren dat de vereiste certificaatparameters evalueert. Nadat u het script hebt geconfigureerd, klikt u op Opslaan om de wijzigingen toe te passen. Zodra de wijzigingen zijn opgeslagen in het DAP-record, implementeert u het beleid om de bijgewerkte configuratie naar het FTD-apparaat te pushen.



Opmerking: de code in dit artikel is bedoeld om de certificaten te evalueren die op het clientapparaat zijn geïnstalleerd, waarbij specifiek wordt gecontroleerd of er een certificaat is waarvan de parameter Organisatie in het veld Onderwerp overeenkomt met de waarde cisco.

<#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){}
```

- Het script definieert een match_pattern variabele ingesteld op cisco, dat is de naam van de doelorganisatie te vinden.
- Het herhaalt alle gebruikerscertificaten die beschikbaar zijn op het eindpunt met behulp van een for-lus.
- Voor elk certificaat wordt het veld Organisatie geëxtraheerd (subject_o).
- Het controleert of het veld Organisatie een tekenreeks is en zoekt vervolgens naar het match_pattern erin.
- Als een overeenkomst wordt gevonden, retourneert het script true, wat aangeeft dat het certificaat voldoet aan de beleidscriteria.
- Als er na het controleren van alle certificaten geen overeenkomend certificaat wordt gevonden, retourneert het script false, waardoor het beleid toegang weigert.

Met deze aanpak kunnen beheerders aangepaste certificaatvalidatielogica implementeren die verder gaat dan de standaardparameters die door de FMC GUI worden weergegeven.

Verifiëren

Voer de opdracht meer dap.xml uit om te controleren of de code aanwezig is in de DAP-configuratie op de FTD.

<#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) {}
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.