

DAP証明書パラメータ評価用のLUAスクリプトの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[コンフィギュレーション](#)

[確認](#)

はじめに

このドキュメントでは、ユーザがVPNに接続しようとするときに必要な証明書パラメータを検出するようにLUAスクリプトを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアファイアウォール管理センター(FMC)
- リモートアクセスVPNの設定(RAVPN)
- 基本的なLUAスクリプトコーディング
- 基本的なSSL証明書
- ダイナミックアクセスポリシー(DAP)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Secure Firewallバージョン7.7.0
- Secure Firewall Management Center(FMC)バージョン7.7.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

DAPは、ネットワーク管理者が、ネットワークに接続しようとしているユーザとデバイスのさまざまな属性に基づいてきめ細かなアクセスコントロールポリシーを定義できるようにする強力な機能です。DAPの主要な機能の1つは、クライアントデバイスにインストールされたデジタル証明書を評価するポリシーを作成する機能です。これらの証明書は、ユーザを認証し、デバイスのコンプライアンスを確認するための安全な方法として機能します。

Cisco Secure FMCインターフェイスでは、管理者は次のような特定の証明書パラメータを評価するようにDAPポリシーを設定できます。

- Subject
- Issuer
- サブジェクトの別名
- シリアル番号
- 証明書ストア

ただし、FMC GUIで利用できる証明書評価オプションは、これらの事前定義済み属性に限定されています。この制限は、管理者が、証明書内の特定のフィールドやカスタム拡張など、より詳細なカスタム証明書情報に基づいてポリシーを適用する場合、標準DAP設定だけではポリシーを適用できないことを意味します。

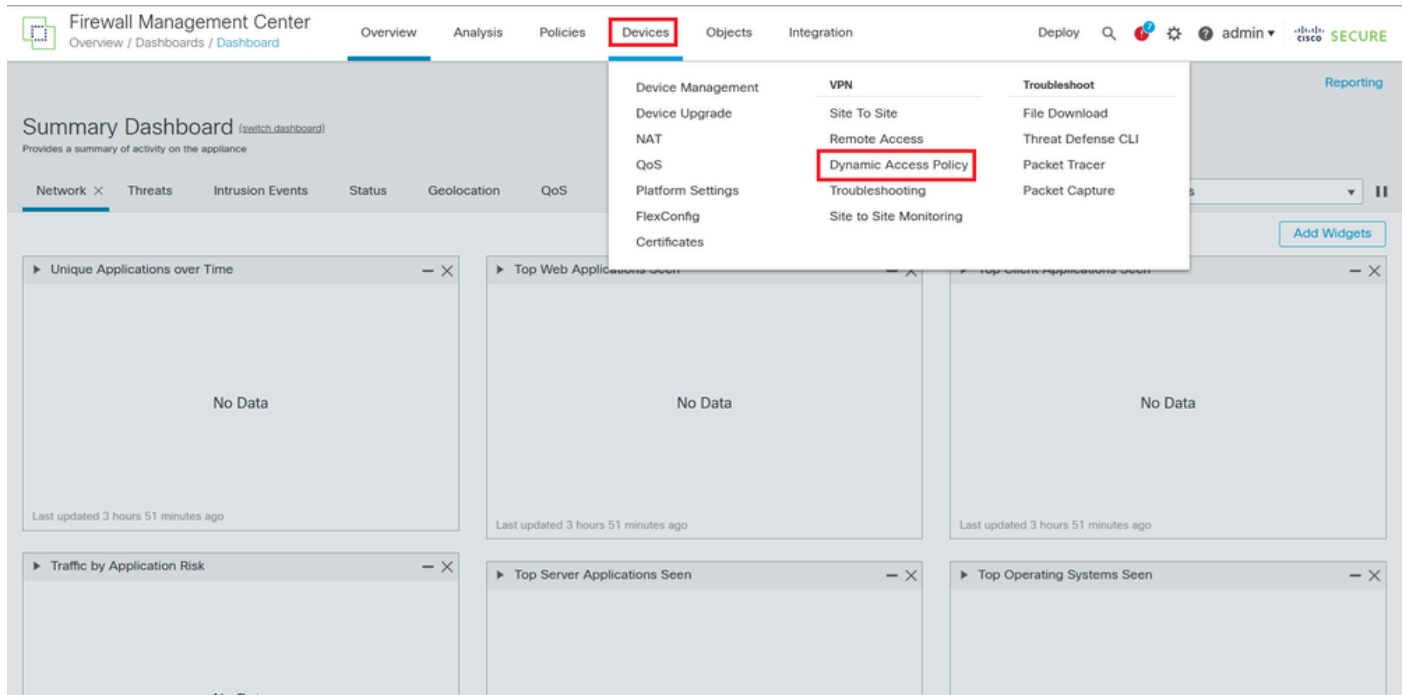
この制限を克服するために、Cisco Secure FirewallはDAP内でのLUAスクリプトの統合をサポートしています。LUAスクリプトは、FMCインターフェイスを介して公開されない追加の証明書属性にアクセスして評価するための柔軟性を提供します。この機能により、管理者は詳細な証明書データに基づいて、より高度でカスタマイズされたアクセスポリシーを実装できます。

LUAスクリプトを利用することで、組織名、カスタム拡張、またはその他の証明書メタデータなど、デフォルトのパラメータを超える証明書フィールドを分析できるようになります。この拡張された評価機能により、組織の要件に合わせてポリシーを正確に調整できるようになり、特定の詳細な基準を満たす証明書を持つクライアントだけがアクセスを許可されるようになります。

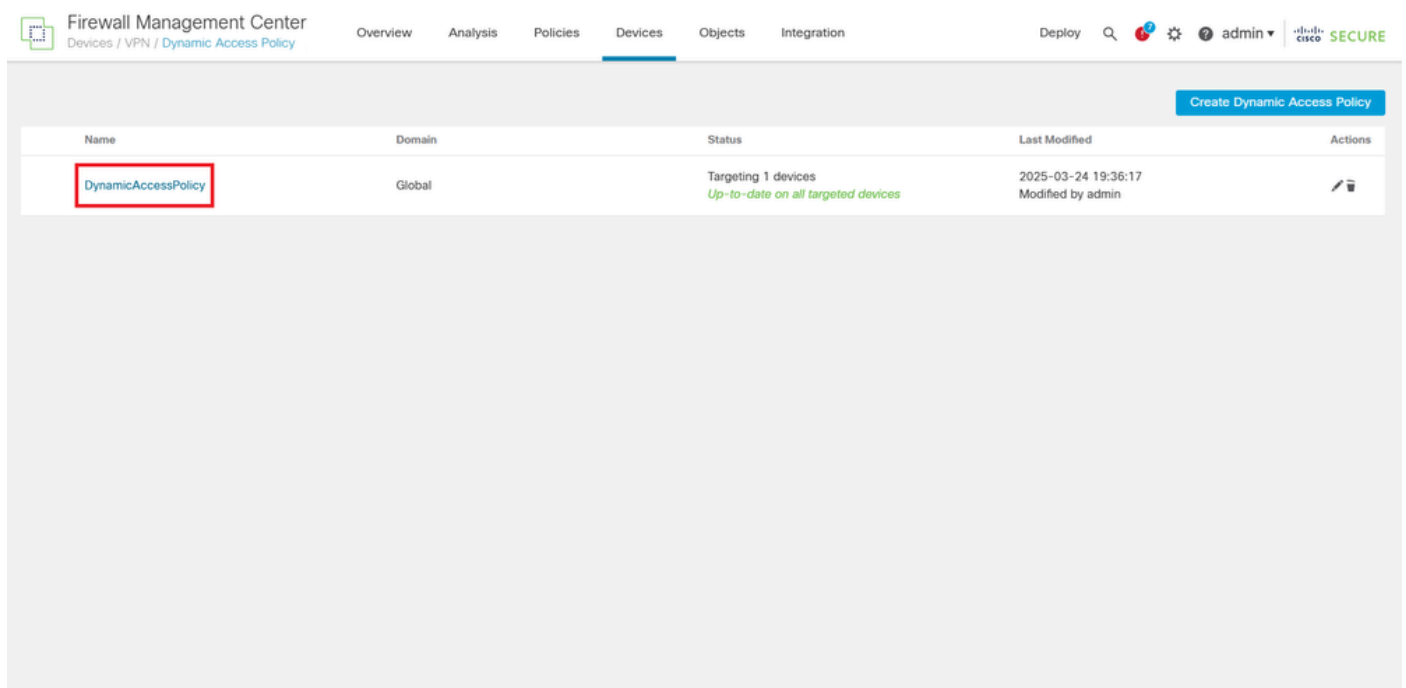
したがって、このドキュメントでは、LUAスクリプト機能を利用してクライアント証明書内のOrganizationパラメータを評価するようにLUAスクリプトを設定します。

コンフィギュレーション

1. FMCのGUIにログインし、ダッシュボードでメニューからDevices > Dynamic Access Policyの順に選択します。



2. RAVPN設定に適用されたDAPポリシーを開きます。



3. 目的のレコードを編集し、レコード名をクリックしてLUAスクリプトを設定します。

Firewall Management Center
Devices / VPN / Dynamic Access Policy

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

< Dynamic Access Policies

DynamicAccessPolicy

HostScan Package: SecureFirewallPosture

Select multiple records Create DAP Record

Priority	Name	Action	AAA Criteria	Endpoint Criteria	Actions
1	Record 1	Continue	No criteria configured	1 criterion, Matching Any	
1	Record 2	Continue	No criteria configured	1 criterion, Matching Any	

Default Record: DfltAccessPolicy ✖ Terminate

4. 選択したレコード内で、「拡張」タブにナビゲートし、必要な証明書パラメータを評価する LUA スクリプトを入力します。スクリプトを設定したら、Save をクリックして変更を適用します。変更が DAP レコードに保存されたら、更新された設定を FTD デバイスにプッシュするようにポリシーを展開します。

Firewall Management Center
Devices / VPN / Dynamic Access Policy

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

General AAA Criteria Endpoint Criteria **Advanced**

Match criteria to be performed on DAP configuration

AND OR

Lua script for advanced attribute matching

```

1  assert(function()
2    local match_pattern = "cisco"
3    for k,v in pairs (endpoint.certificate.user) do
4      match_value = v.subject_o
5      if(type(match_value) == "string") then
6        if(string.find(match_value,match_pattern) ~= nil) then
7          return true
8        end
9      end
10   end
11   return false
12 end)()

```

Cancel **Save**

注：この記事のコードは、クライアントデバイスにインストールされている証明書进行评估することを目的としています。具体的には、Subject フィールドの Organization パラメータが値 cisco に一致する証明書があることを確認することが目的です。

<#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){}

```

- このスクリプトは、ciscoに設定されたmatch_pattern変数を定義します。これは、検索する対象組織名です。
- forループを使用して、エンドポイントで使用可能なすべてのユーザ証明書を繰り返します。
- 各証明書について、組織フィールド(subject_o)を抽出します。
- Organizationフィールドが文字列かどうかを確認し、その中でmatch_patternを検索します。
- 一致が見つかった場合、スクリプトはtrueを返し、証明書がポリシーの基準を満たしていることを示します。
- すべての証明書を確認した後で一致する証明書が見つからなかった場合、スクリプトはfalseを返し、ポリシーがアクセスを拒否します。

このアプローチにより、管理者は、FMC GUIによって公開される標準パラメータを超えて、カスタマイズされた証明書検証ロジックを実装できます。

確認

more dap.xmlコマンドを実行して、FTDのDAP設定にコードが存在することを確認します。

```

<#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) {}
```

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。