为DAP证书参数评估配置LUA脚本

目录

简介

本文档介绍如何配置LUA脚本以检测用户尝试连接到VPN时必须具有的证书参数。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全防火墙管理中心(FMC)
- 远程访问VPN配置(RAVPN)
- 基本LUA脚本编码
- 基本SSL证书
- 动态访问策略(DAP)

使用的组件

本文档中的信息基于以下软件版本：

- 安全防火墙版本7.7.0
- 安全防火墙管理中心版本7.7.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

DAP是一项强大的功能，允许网络管理员根据尝试连接到网络的用户和设备的各种属性定义精细访问控制策略。DAP的主要功能之一是能够创建策略，评估客户端设备上安装的数字证书。这些证书用作验证用户身份和验证设备合规性的安全方法。

在Cisco Secure FMC界面中，管理员可以配置DAP策略以评估特定证书参数，例如：

- 主题
- 签发方
- 主题备用名
- Serial Number
- 证书存储

但是，通过FMC GUI可用的证书评估选项仅限于这些预定义属性。此限制意味着，如果管理员希望基于更详细的或自定义的证书信息（例如证书或自定义扩展中的特定字段）实施策略，则无法仅使用标准DAP配置来实现此限制。

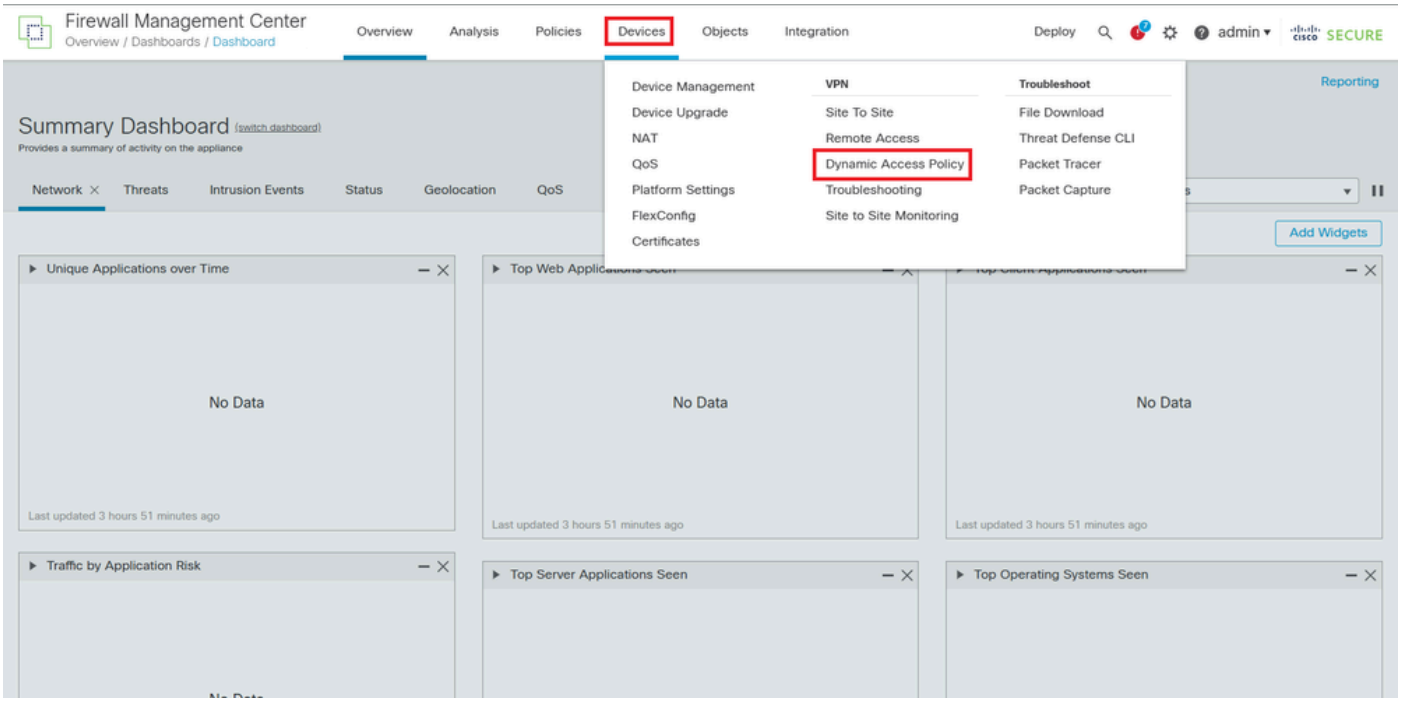
为了克服此限制，思科安全防火墙支持在DAP中集成LUA脚本。LUA脚本可以灵活访问和评估未通过FMC界面公开的其他证书属性。此功能使管理员可以根据详细的证书数据实施更复杂的自定义访问策略。

通过利用LUA脚本，可以分析默认参数之外的证书字段，例如组织名称、自定义扩展名或其他证书元数据。这种扩展的评估功能允许策略根据组织的要求进行精确调整，从而确保只有证书符合具体详细标准的客户才能获得访问权限，从而增强安全性。

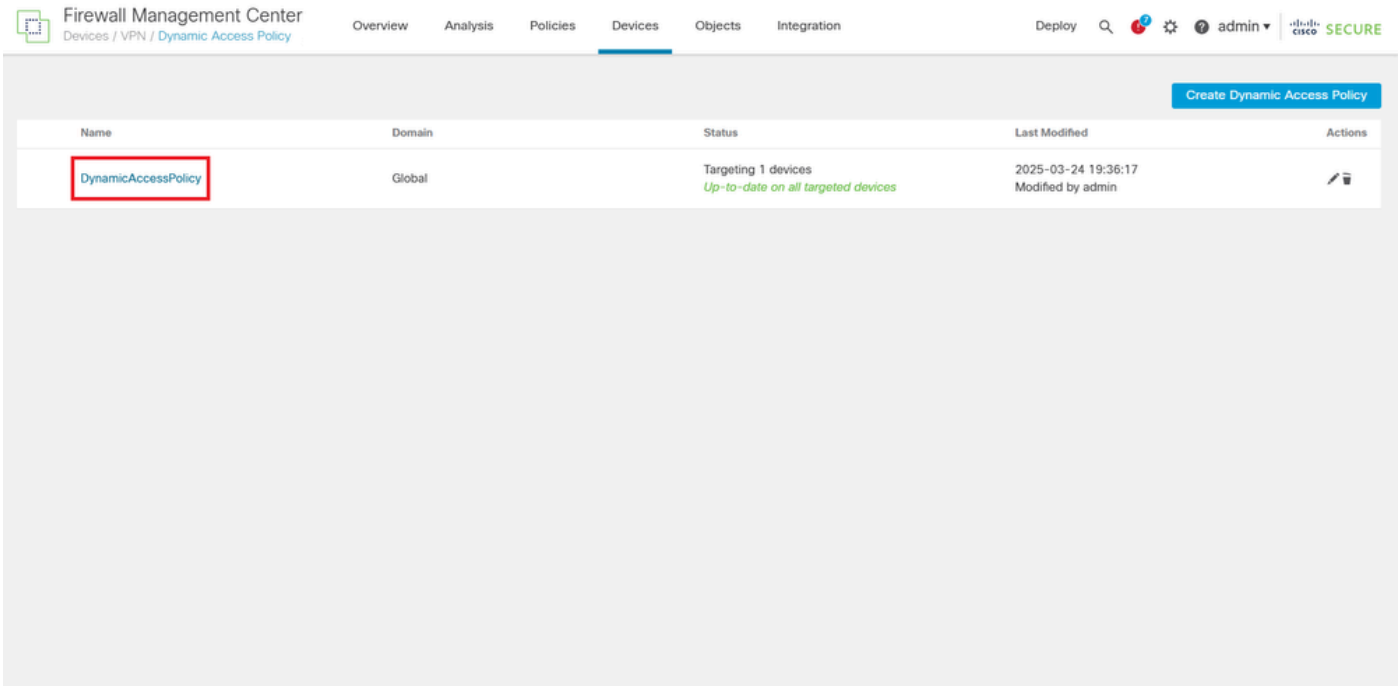
因此，在本文档中，LUA脚本配置为利用LUA脚本功能评估客户端证书中的Organization参数。

配置

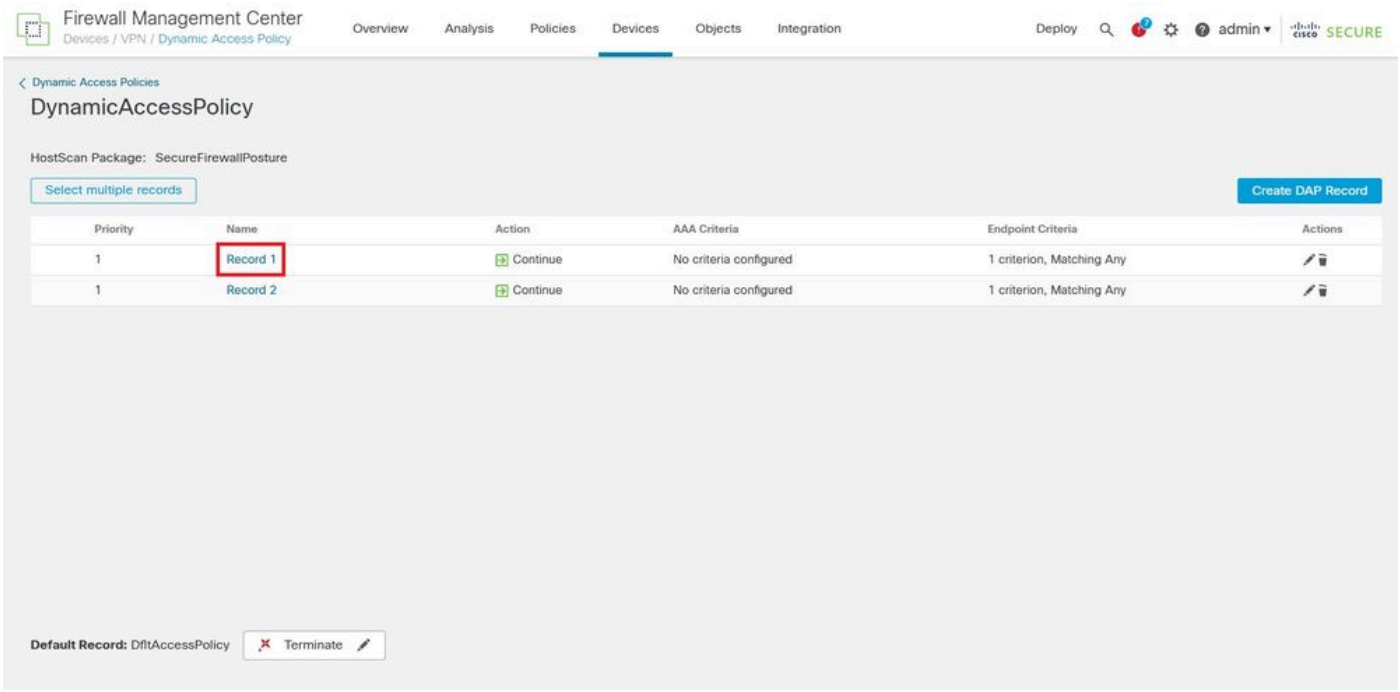
1.登录到FMC GUI，然后从控制面板导航到菜单中的设备>动态访问策略。



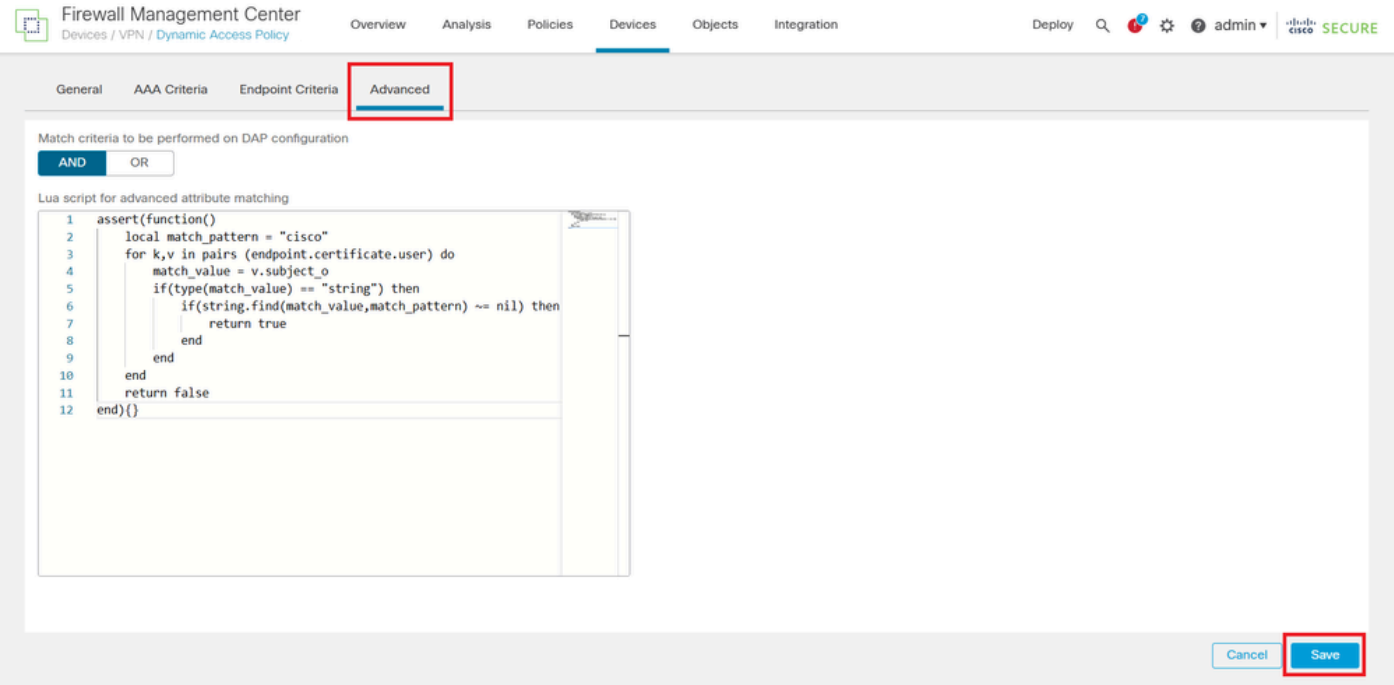
2.打开应用于RAVPN配置的DAP策略。



3.通过单击记录名来编辑所需的记录，以配置LUA脚本。



4.在选定记录中，定位至高级标签以输入用于评估所需证书参数的LUA脚本。配置脚本后，单击Save应用更改。在DAP记录中保存更改后，部署策略以将更新的配置推送到FTD设备。



注意：本文介绍的代码用于评估客户端设备上安装的证书，具体是验证是否存在其主题字段中的Organization参数与cisco值匹配的证书。

<#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){}
```

- 该脚本定义一个设置为cisco的match_pattern变量，这是要查找的目标组织名称。
- 它使用for循环对终端上的所有可用用户证书进行迭代。
- 对于每个证书，它提取组织字段(subject_o)。

- 它检查Organization字段是否为字符串，然后在其中搜索match_pattern。
- 如果找到匹配项，脚本将返回true，表示证书符合策略条件。
- 如果在检查所有证书后未找到匹配的证书，脚本将返回false，导致策略拒绝访问。

此方法允许管理员在FMC GUI显示的标准参数之外实施自定义的证书验证逻辑。

验证

运行命令more dap.xml以验证FTD上的DAP配置中是否存在该代码。

<#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) {}
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。