Configurar Script LUA para Avaliação de Parâmetros de Certificado DAP

Contents

Introdução

Este documento descreve como configurar um script LUA para detectar parâmetros de certificado que os usuários devem ter quando tentam se conectar à VPN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Centro de gerenciamento seguro de firewall (FMC)
- Configuração de VPN de acesso remoto (RAVPN)
- Codificação de script de LUA básica
- Certificados SSL básicos
- Política de acesso dinâmico (DAP)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Secure Firewall versão 7.7.0
- Secure Firewall Management Center versão 7.7.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O DAP é um recurso poderoso que permite aos administradores de rede definir políticas granulares de controle de acesso com base em vários atributos de usuários e dispositivos que tentam se conectar à rede. Um dos principais recursos do DAP é a capacidade de criar políticas que avaliem certificados digitais instalados em dispositivos clientes. Esses certificados servem como um método seguro para autenticar usuários e verificar a conformidade do dispositivo.

Na interface do Cisco Secure FMC, os administradores podem configurar políticas DAP para avaliar parâmetros de certificado específicos, como:

- Assunto
- Emissor
- Nome Alternativo do Assunto
- Serial Number
- Repositório de Certificados

No entanto, as opções de avaliação de certificado disponíveis através da GUI do FMC estão limitadas a esses atributos predefinidos. Essa limitação significa que, se um administrador quiser aplicar políticas baseadas em informações de certificado mais detalhadas ou personalizadas, como campos específicos dentro do certificado ou extensões personalizadas, isso não poderá ser obtido usando apenas a configuração DAP padrão.

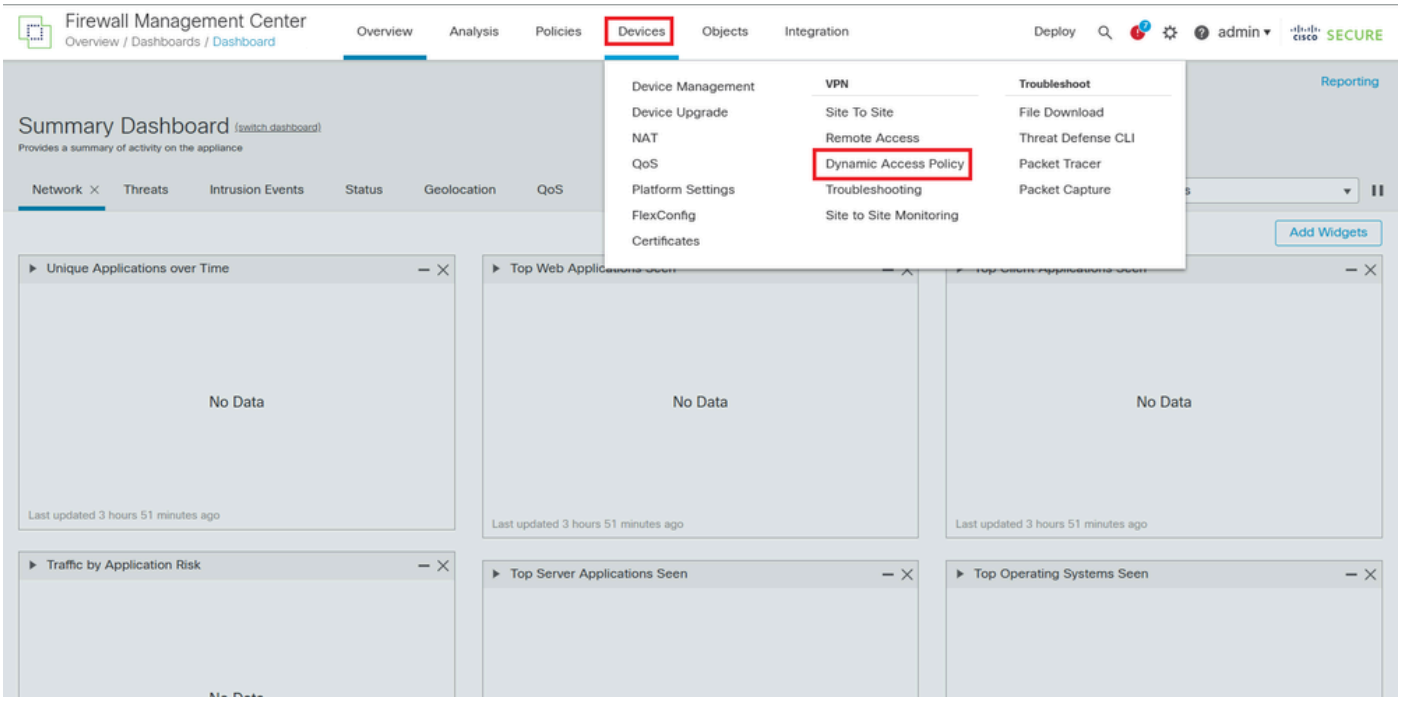
Para superar essa limitação, o Cisco Secure Firewall suporta a integração de scripts LUA dentro do DAP. Os scripts LUA oferecem a flexibilidade de acessar e avaliar atributos de certificado adicionais que não são expostos através da interface FMC. Esse recurso permite que os administradores implementem políticas de acesso mais sofisticadas e personalizadas com base em dados de certificado detalhados.

Aproveitando o script LUA, torna-se possível analisar campos de certificado além dos parâmetros padrão, como nomes de organização, extensões personalizadas ou outros metadados de certificado. Esse recurso de avaliação ampliado aumenta a segurança, permitindo que as políticas sejam ajustadas precisamente aos requisitos da organização, garantindo que somente os clientes com certificados que atendem a critérios específicos e detalhados tenham acesso.

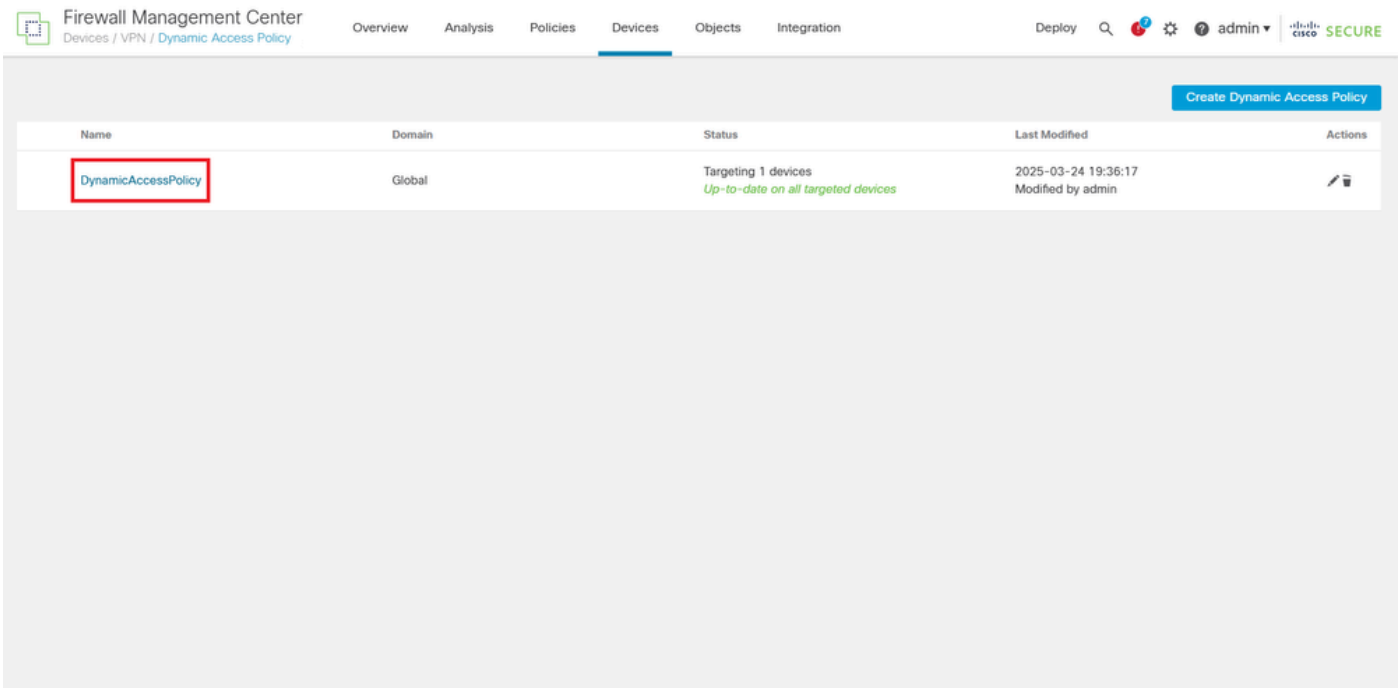
Portanto, neste documento, um script LUA é configurado para avaliar o parâmetro Organization (Organização) dentro de um certificado de cliente, aproveitando os recursos de script LUA.

Configuração

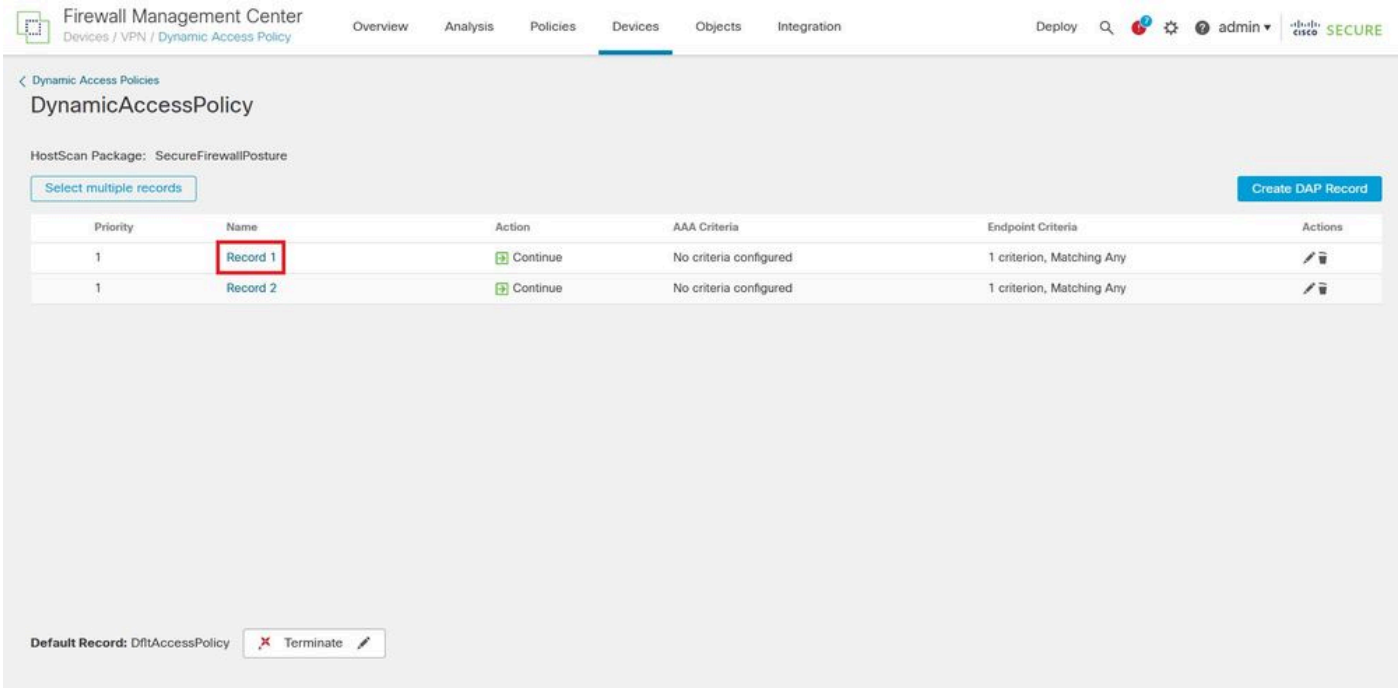
1.Faça login na GUI do FMC e, em seguida, no painel, navegue até Devices >Dynamic Access Policy no menu.



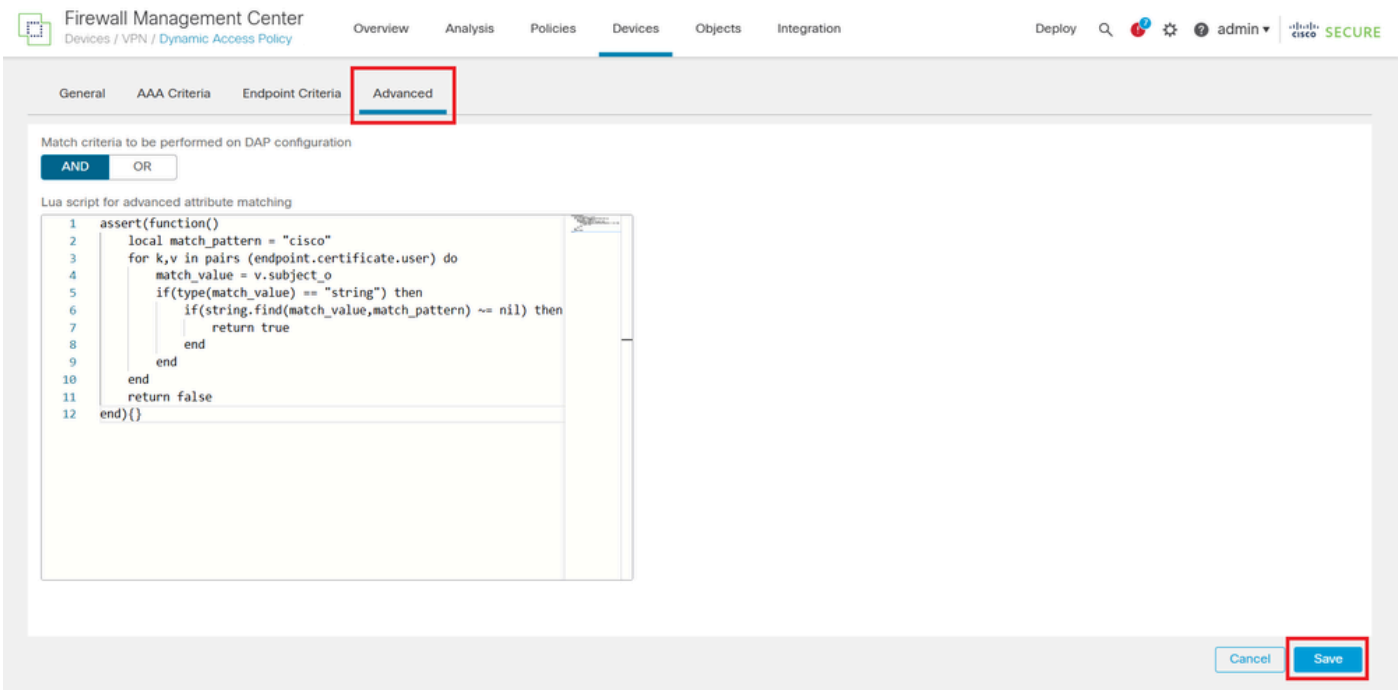
2.Abra a política DAP aplicada à configuração RAVPN.



3. Edite o registro desejado para configurar o script LUA clicando no nome do registro.



4. No registro selecionado, navegue até a guia Avançado para inserir o script LUA que avalia os parâmetros de certificado necessários. Após configurar o script, clique em Salvar para aplicar as alterações. Depois que as alterações forem salvas no registro DAP, implante a política para enviar a configuração atualizada para o dispositivo FTD.



Note: O código apresentado neste artigo é projetado para avaliar os certificados instalados no dispositivo cliente, verificando especificamente se há um certificado cujo parâmetro Organização no campo Assunto corresponde ao valor 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){}
```

- O script define uma variável match_pattern definida como cisco, que é o nome da organização de destino a ser localizado.
- Ele repete todos os certificados de usuário disponíveis no endpoint usando um loop for.
- Para cada certificado, ele extrai o campo Organização (subject_o).
- Ele verifica se o campo Organização é uma string e procura o match_pattern dentro dele.
- Se uma correspondência for encontrada, o script retornará verdadeiro, indicando que o certificado atende aos critérios da política.
- Se nenhum certificado correspondente for encontrado após a verificação de todos os certificados, o script retornará falso, fazendo com que a política negue o acesso.

Essa abordagem permite que os administradores implementem uma lógica de validação de certificado personalizada além dos parâmetros padrão expostos pela GUI do FMC.

Verificar

Execute o comando more dap.xml para verificar se o código está presente na configuração DAP no 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) {}
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.