Configurar script LUA para evaluación de parámetros de certificado DAP

Contenido

Introducción

Este documento describe cómo configurar un script LUA para detectar los parámetros de certificado que los usuarios deben tener cuando intentan conectarse a la VPN.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Centro de gestión de firewall seguro (FMC)
- Configuración de VPN de acceso remoto (RAVPN)
- Codificación básica de scripts LUA
- Certificados SSL básicos
- Política de acceso dinámica (DAP)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Secure Firewall versión 7.7.0
- Secure Firewall Management Center versión 7.7.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

DAP es una potente función que permite a los administradores de red definir políticas de control de acceso granular basadas en diversos atributos de usuarios y dispositivos que intentan conectarse a la red. Una de las capacidades clave de DAP es la capacidad de crear políticas que evalúen los certificados digitales instalados en los dispositivos cliente. Estos certificados sirven como un método seguro para autenticar a los usuarios y verificar el cumplimiento de los dispositivos.

En la interfaz de Cisco Secure FMC, los administradores pueden configurar políticas DAP para evaluar parámetros de certificado específicos como:

- Asunto
- Emisor
- Nombre alternativo del asunto
- Serial Number
- Almacén de certificados

Sin embargo, las opciones de evaluación de certificados disponibles a través de la GUI de FMC se limitan a estos atributos predefinidos. Esta limitación significa que si un administrador desea aplicar políticas basadas en información de certificados más detallada o personalizada, como campos específicos dentro del certificado o extensiones personalizadas, esto no se puede lograr utilizando solamente la configuración DAP estándar.

Para superar esta limitación, Cisco Secure Firewall admite la integración de scripts LUA en DAP. Los scripts LUA proporcionan la flexibilidad de acceder y evaluar atributos de certificado adicionales que no se exponen a través de la interfaz FMC. Esta capacidad permite a los administradores implementar políticas de acceso más sofisticadas y personalizadas basadas en datos de certificados detallados.

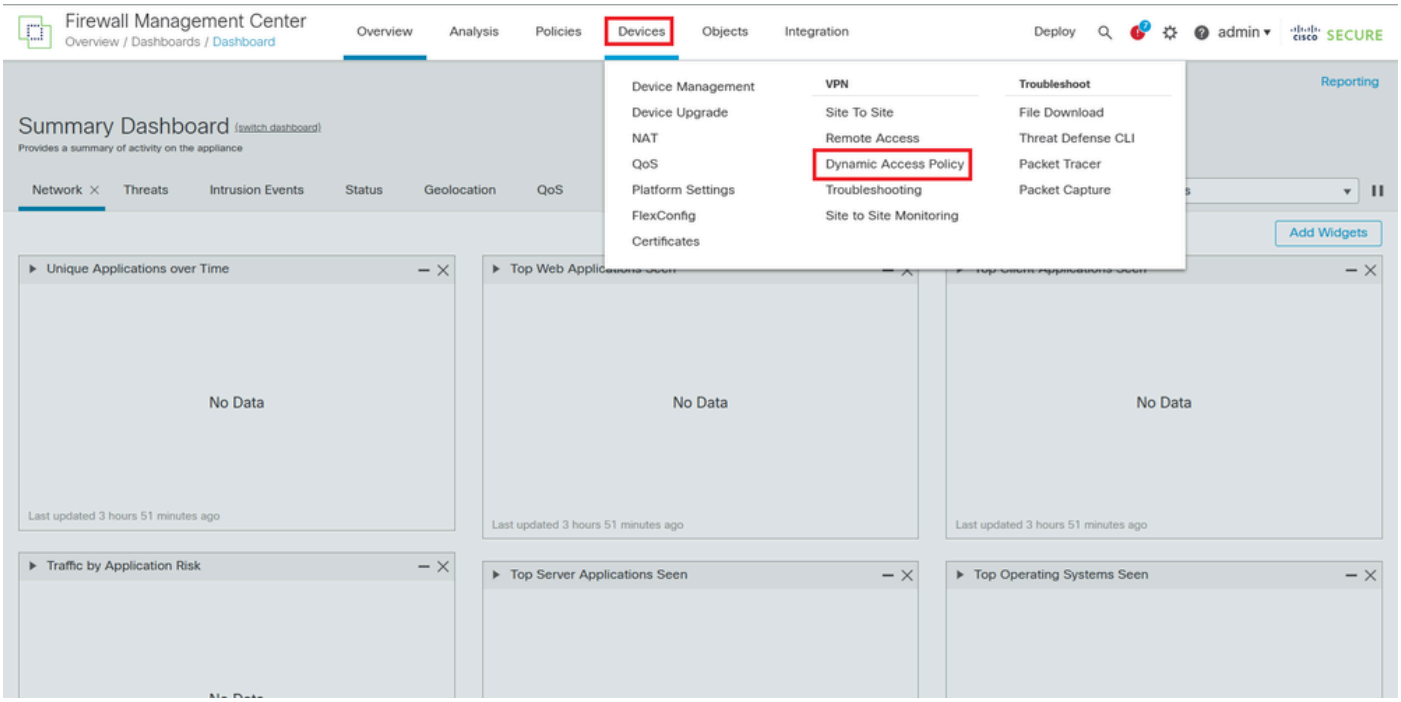
Al aprovechar la secuencia de comandos LUA, es posible analizar campos de certificado más allá de los parámetros predeterminados, como nombres de organizaciones, extensiones personalizadas u otros metadatos de certificado. Esta capacidad de evaluación ampliada mejora la seguridad al permitir que las políticas se adapten con precisión a los requisitos de la organización, garantizando que solo se conceda acceso a los clientes con certificados que cumplan criterios específicos y detallados.

Por lo tanto, en este documento, se configura una secuencia de comandos LUA para evaluar el parámetro Organization dentro de un certificado de cliente aprovechando las capacidades de secuencia de comandos LUA.

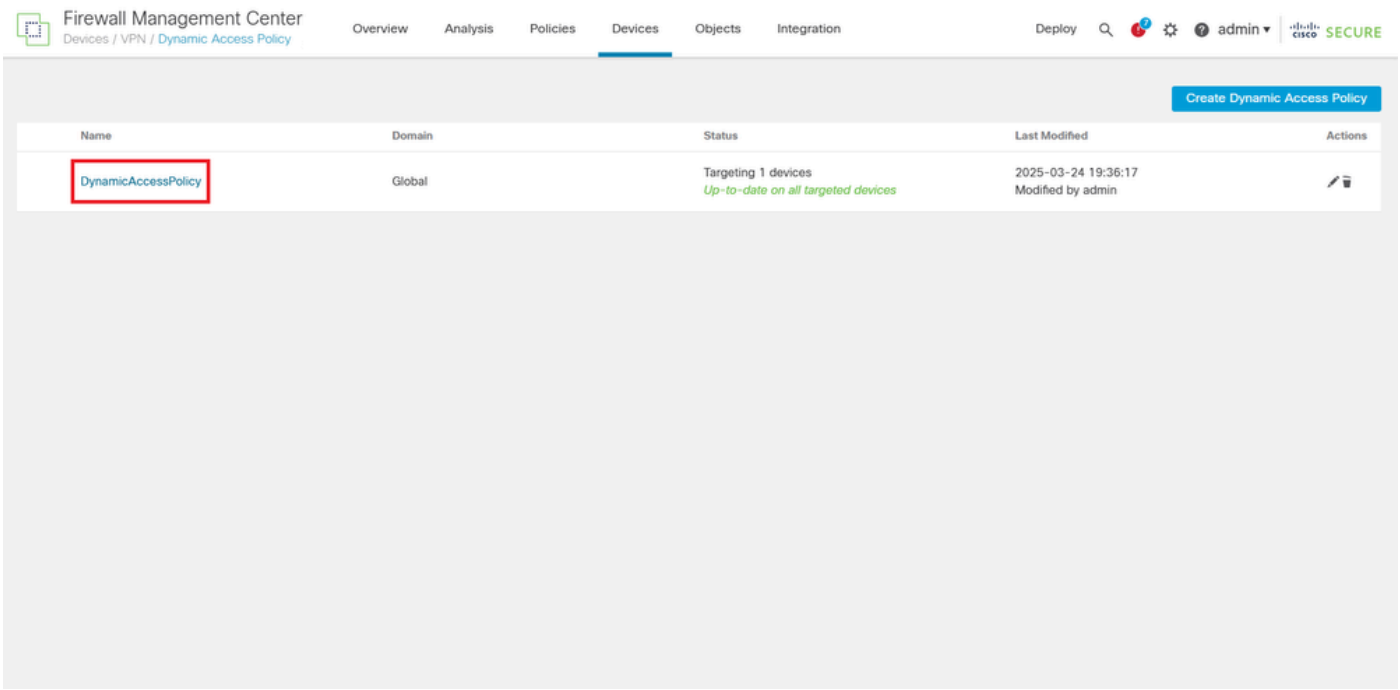
Configuración

1.Inicie sesión en la GUI de FMC y, a continuación, desde el panel, navegue hasta Devices

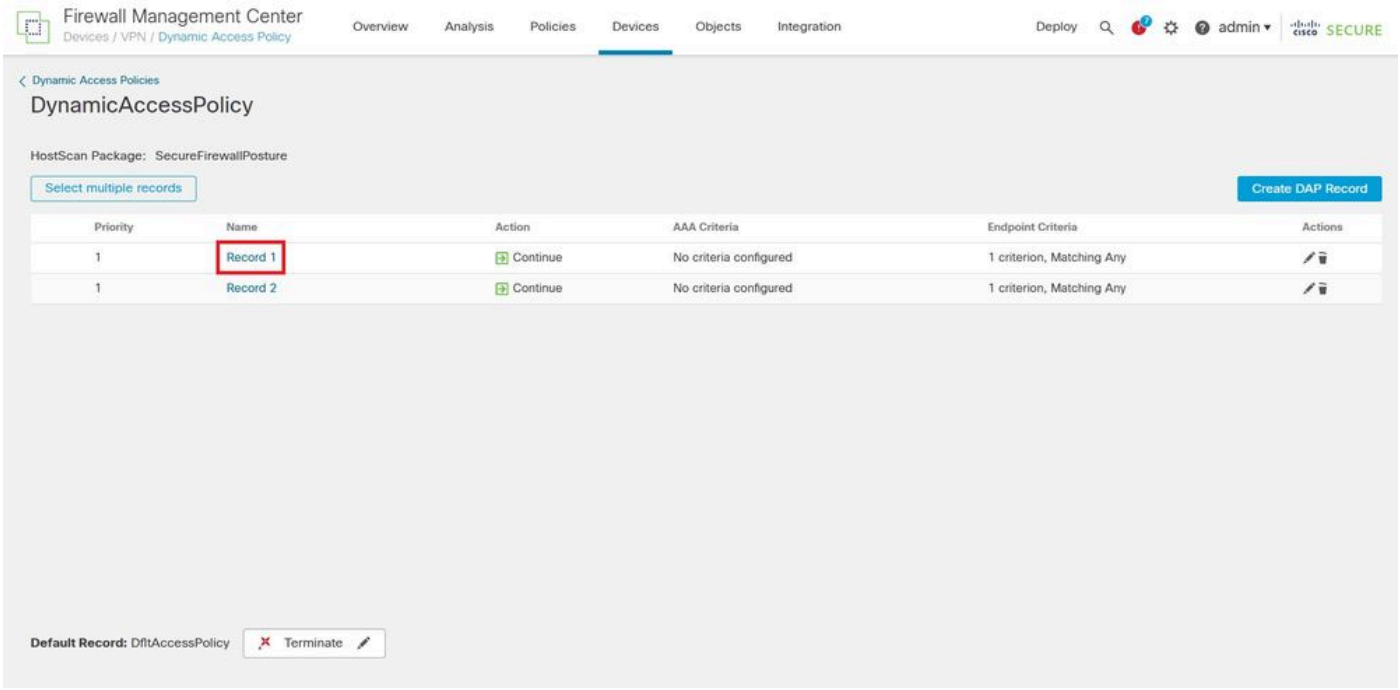
>Dynamic Access Policy (Dispositivos > Política de acceso dinámica) en el menú.



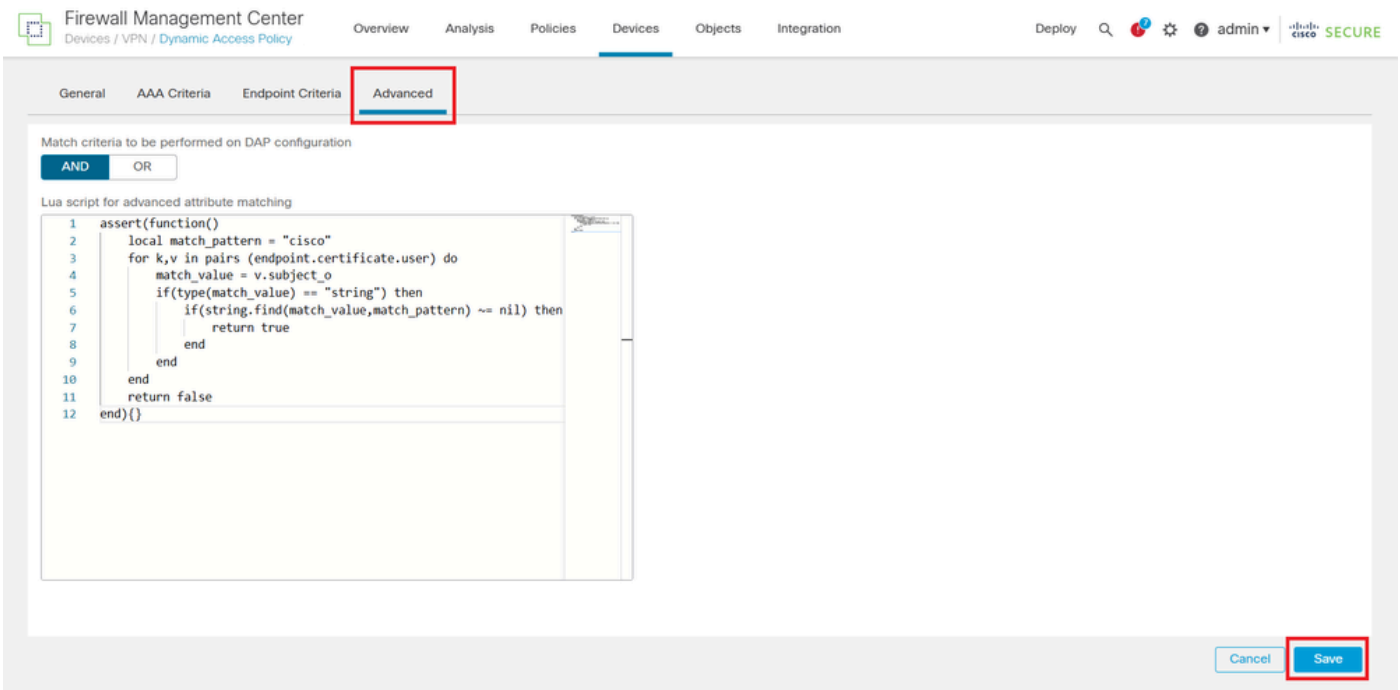
2. Abra la política DAP aplicada a la configuración RAVPN.



3. Edite el registro deseado para configurar el script LUA haciendo clic en el nombre del registro.



4. En el registro seleccionado, acceda a la pestaña Avanzado para introducir el archivo de comandos LUA que evalúa los parámetros de certificado necesarios. Después de configurar el script, haga clic en Guardar para aplicar los cambios. Una vez guardados los cambios en el registro DAP, implemente la política para enviar la configuración actualizada al dispositivo FTD.



Nota: El código presentado en este artículo está diseñado para evaluar los certificados instalados en el dispositivo cliente, verificando específicamente que hay un certificado cuyo parámetro Organization dentro del campo Subject (Asunto) coincide con el 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){}
```

- La secuencia de comandos define una variable match_pattern establecida en cisco, que es el nombre de la organización de destino que se va a buscar.
- Repite todos los certificados de usuario disponibles en el extremo mediante un bucle for.
- Para cada certificado, extrae el campo Organización (subject_o).
- Comprueba si el campo Organización es una cadena y, a continuación, busca el match_pattern que contiene.
- Si se encuentra una coincidencia, la secuencia de comandos devuelve true, indicando que el certificado cumple los criterios de la directiva.
- Si no se encuentra ningún certificado coincidente después de comprobar todos los certificados, la secuencia de comandos devuelve false, lo que hace que la directiva deniegue el acceso.

Este enfoque permite a los administradores implementar una lógica de validación de certificados personalizada más allá de los parámetros estándar expuestos por la GUI de FMC.

Verificación

Ejecute el comando more dap.xml para verificar que el código está presente en la configuración DAP en el 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) {}
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).