Konfigurieren des LUA-Skripts für die Auswertung der DAP-Zertifikatparameter

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie ein LUA-Skript konfigurieren, um Zertifikatsparameter zu erkennen, die Benutzer benötigen, wenn sie versuchen, eine Verbindung mit dem VPN herzustellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Secure Firewall Management Center (FMC)
- Konfiguration des Remote Access VPN (RAVPN)
- Grundlegende LUA-Skriptcodierung
- Grundlegende SSL-Zertifikate
- Dynamic Access Policy (DAP)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Secure Firewall Version 7.7.0
- Secure Firewall Management Center Version 7.7.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

DAP ist eine leistungsstarke Funktion, mit der Netzwerkadministratoren präzise Zugriffskontrollrichtlinien definieren können, die auf verschiedenen Attributen von Benutzern und Geräten basieren, die eine Verbindung mit dem Netzwerk herstellen möchten. Eine der wichtigsten Funktionen von DAP ist die Erstellung von Richtlinien, die digitale Zertifikate auswerten, die auf Client-Geräten installiert sind. Diese Zertifikate dienen als sicheres Verfahren zur Authentifizierung von Benutzern und zur Überprüfung der Geräte-Compliance.

In der Cisco Secure FMC-Schnittstelle können Administratoren DAP-Richtlinien konfigurieren, um bestimmte Zertifikatparameter zu bewerten, z. B.:

- Betreff
- Emittent
- Betreff Alternativer Name
- Seriennummer
- Zertifikatsspeicher

Die über die FMC-GUI verfügbaren Optionen zur Zertifikatsbewertung sind jedoch auf diese vordefinierten Attribute beschränkt. Diese Einschränkung bedeutet, dass Richtlinien, die auf detaillierteren oder benutzerspezifischen Zertifikatinformationen basieren, z. B. bestimmte Felder im Zertifikat oder benutzerdefinierte Erweiterungen, von einem Administrator nicht mit der standardmäßigen DAP-Konfiguration allein durchgesetzt werden können.

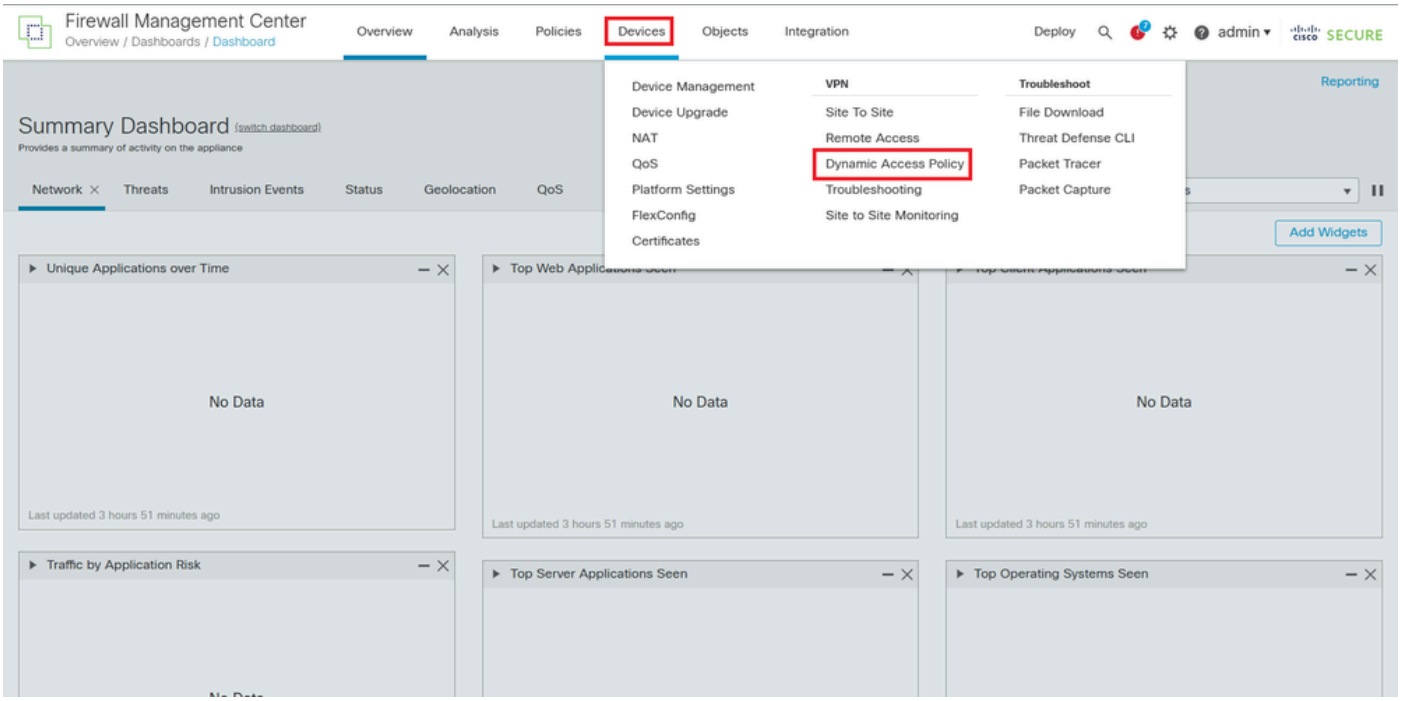
Um diese Einschränkung zu überwinden, unterstützt die Cisco Secure Firewall die Integration von LUA-Scripting in DAP. LUA-Skripte bieten die Flexibilität, auf zusätzliche Zertifikatattribute zuzugreifen und diese auszuwerten, die nicht über die FMC-Schnittstelle verfügbar gemacht werden. So können Administratoren differenziertere und individuell angepasste Zugriffsrichtlinien implementieren, die auf detaillierten Zertifikatsdaten basieren.

Durch die Verwendung von LUA-Scripting können Zertifikatfelder über die Standardparameter hinaus analysiert werden, z. B. Organisationsnamen, benutzerdefinierte Erweiterungen oder andere Zertifikatmetadaten. Diese erweiterte Evaluierungsfunktion erhöht die Sicherheit, da Richtlinien genau auf die Anforderungen der Organisation zugeschnitten werden können. So wird sichergestellt, dass nur Kunden mit Zertifikaten, die spezifische, detaillierte Kriterien erfüllen, Zugriff erhalten.

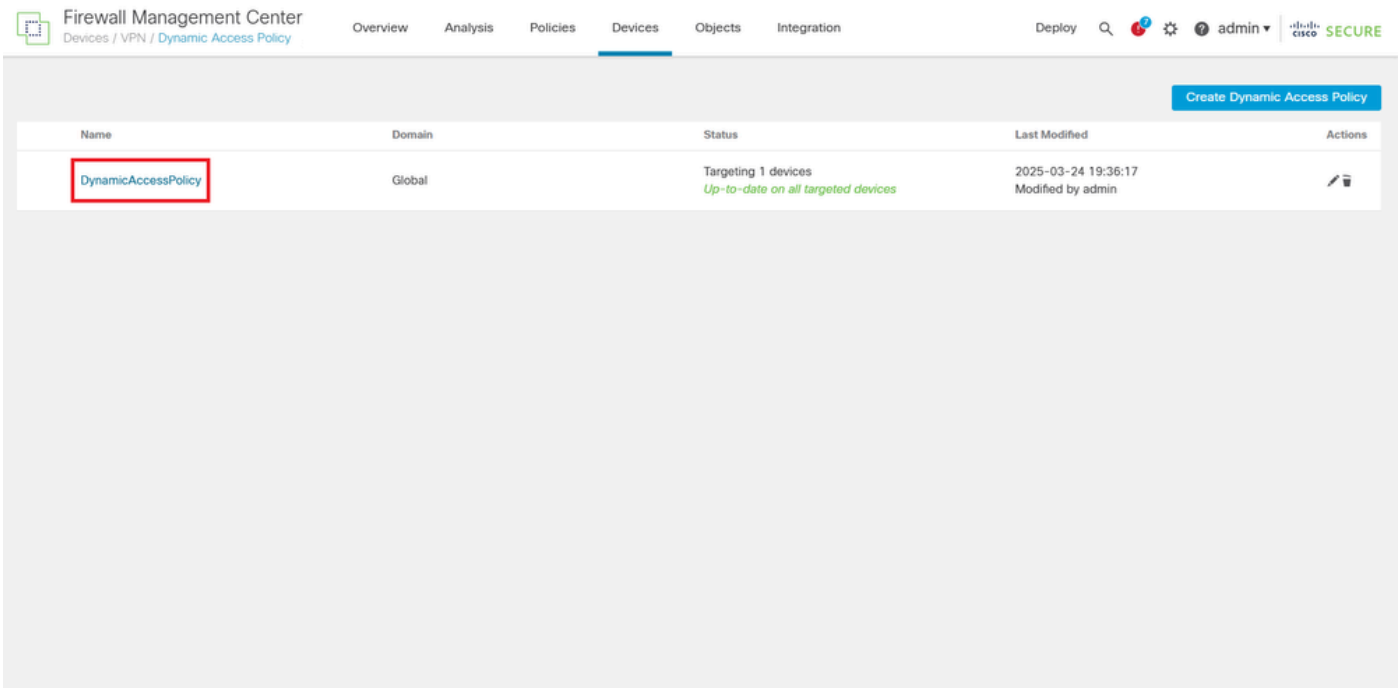
Daher wird in diesem Dokument ein LUA-Skript konfiguriert, um den Organisationsparameter in einem Clientzertifikat mithilfe von LUA-Skriptfunktionen auszuwerten.

Konfiguration

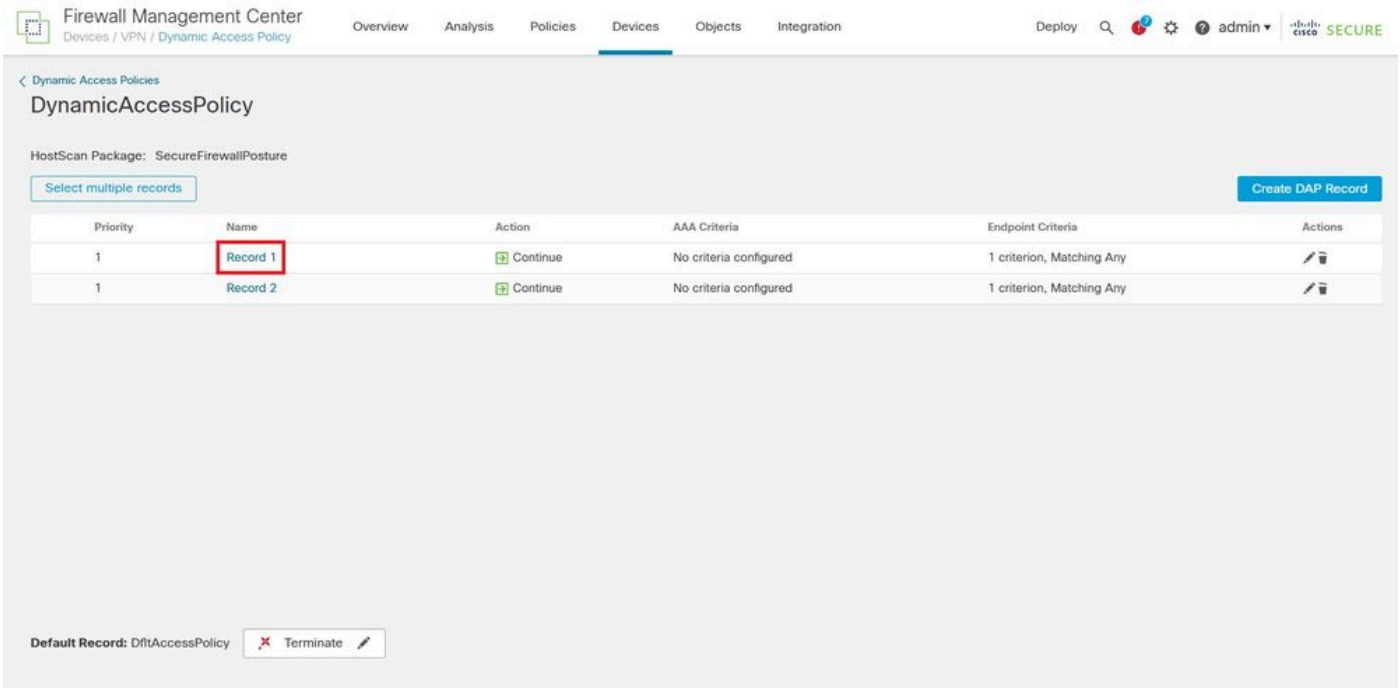
1.Melden Sie sich bei der FMC-GUI an, und navigieren Sie dann vom Dashboard aus im Menü zu Geräte > Dynamische Zugriffsrichtlinie.



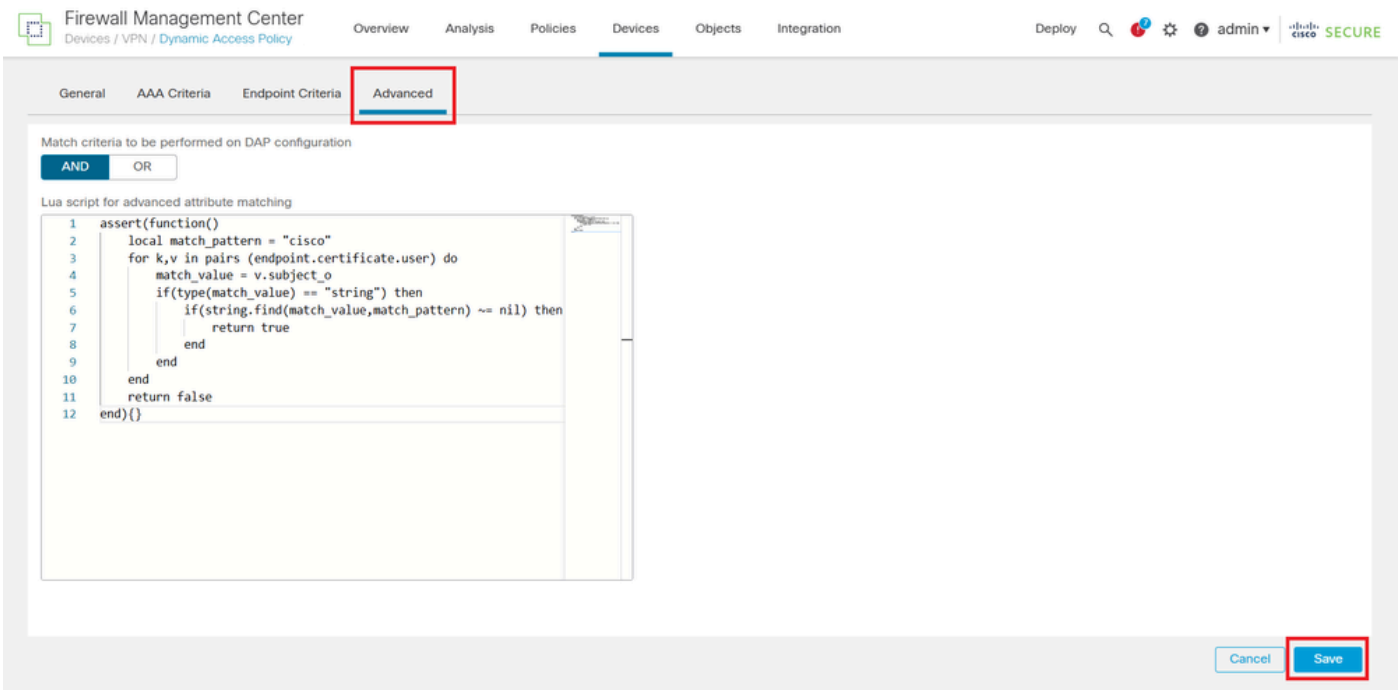
2.Öffnen Sie die DAP-Richtlinie, die auf die RAVPN-Konfiguration angewendet wird.



3. Bearbeiten Sie den gewünschten Datensatz, um das LUA-Skript zu konfigurieren, indem Sie auf den Namen des Datensatzes klicken.



4. Navigieren Sie innerhalb des ausgewählten Datensatzes zur Registerkarte Erweitert, um das LUA-Skript einzugeben, das die erforderlichen Zertifikatparameter auswertet. Klicken Sie nach der Konfiguration des Skripts auf Speichern, um die Änderungen zu übernehmen. Sobald die Änderungen im DAP-Datensatz gespeichert wurden, verwenden Sie die Richtlinie, um die aktualisierte Konfiguration auf das FTD-Gerät zu übertragen.



Anmerkung: Mit dem in diesem Artikel vorgestellten Code sollen die auf dem Clientgerät installierten Zertifikate ausgewertet werden. Insbesondere wird überprüft, ob ein Zertifikat vorhanden ist, dessen Organisationsparameter im Feld Betreff mit dem Wert cisco übereinstimmt.

<#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){}
```

- Das Skript definiert eine match_pattern-Variable, die auf cisco festgelegt ist, d. h. den zu suchenden Zielorganisationsnamen.
- Er durchläuft alle auf dem Endpunkt verfügbaren Benutzerzertifikate mithilfe einer for-Schleife.
- Für jedes Zertifikat wird das Feld Organisation (subject_o) extrahiert.
- Es überprüft, ob das Feld Organization eine Zeichenfolge ist, und sucht dann nach dem darin enthaltenen match_pattern.
- Wenn eine Übereinstimmung gefunden wird, gibt das Skript true zurück und gibt an, dass das Zertifikat die Richtlinienkriterien erfüllt.
- Wenn nach dem Überprüfen aller Zertifikate kein übereinstimmendes Zertifikat gefunden wird, gibt das Skript false zurück, wodurch die Richtlinie den Zugriff verweigert.

Mit diesem Ansatz können Administratoren eine benutzerdefinierte Zertifikatvalidierungslogik implementieren, die über die von der FMC-GUI angezeigten Standardparameter hinausgeht.

Überprüfung

Führen Sie den Befehl more dap.xml aus, um sicherzustellen, dass der Code in der DAP-Konfiguration auf dem FTD vorhanden ist.

<#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) {}
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.