Configura script LUA per la valutazione dei parametri del certificato DAP

Sommario

Introduzione

In questo documento viene descritto come configurare uno script LUA per rilevare i parametri del certificato che gli utenti devono avere quando tentano di connettersi alla VPN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Centro gestione firewall protetto (FMC)
- Configurazione VPN di accesso remoto
- Codifica script LUA di base
- Certificati SSL di base
- Criteri di accesso dinamico (DAP)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Secure Firewall versione 7.7.0
- Secure Firewall Management Center versione 7.7.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

DAP è una potente funzione che consente agli amministratori di rete di definire criteri granulari di controllo dell'accesso basati su vari attributi di utenti e dispositivi che tentano di connettersi alla rete. Una delle funzionalità chiave di DAP è la capacità di creare criteri che valutino i certificati digitali installati nei dispositivi client. Questi certificati rappresentano un metodo sicuro per autenticare gli utenti e verificare la conformità dei dispositivi.

All'interno dell'interfaccia Cisco Secure FMC, gli amministratori possono configurare i criteri DAP per valutare parametri di certificato specifici, quali:

- Oggetto
- Emittente
- Nome soggetto alternativo
- Numero di serie
- Archivio certificati

Tuttavia, le opzioni di valutazione dei certificati disponibili tramite l'interfaccia GUI del CCP sono limitate a questi attributi predefiniti. Questa limitazione significa che se un amministratore desidera applicare criteri basati su informazioni di certificato più dettagliate o personalizzate, ad esempio campi specifici all'interno del certificato o estensioni personalizzate, non è possibile utilizzare solo la configurazione DAP standard.

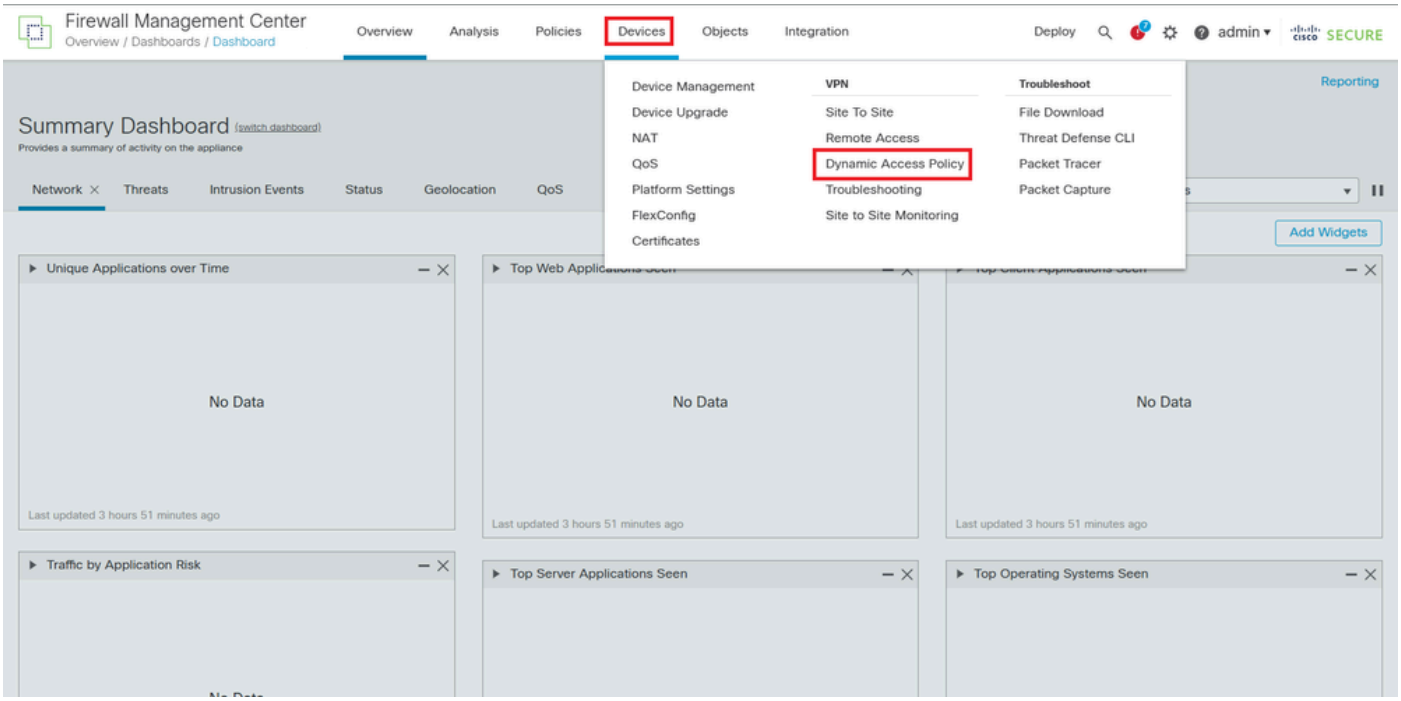
Per superare questo limite, Cisco Secure Firewall supporta l'integrazione degli script LUA in DAP. Gli script LUA offrono la flessibilità necessaria per accedere e valutare attributi di certificati aggiuntivi non esposti tramite l'interfaccia FMC. Questa funzionalità consente agli amministratori di implementare regole di accesso più sofisticate e personalizzate basate su dati di certificato dettagliati.

Utilizzando gli script LUA, è possibile analizzare i campi dei certificati oltre i parametri predefiniti, ad esempio i nomi delle organizzazioni, le estensioni personalizzate o altri metadati dei certificati. Questa capacità di valutazione estesa migliora la sicurezza consentendo di adattare le politiche in base ai requisiti dell'organizzazione, garantendo l'accesso solo ai client con certificati che soddisfano criteri specifici e dettagliati.

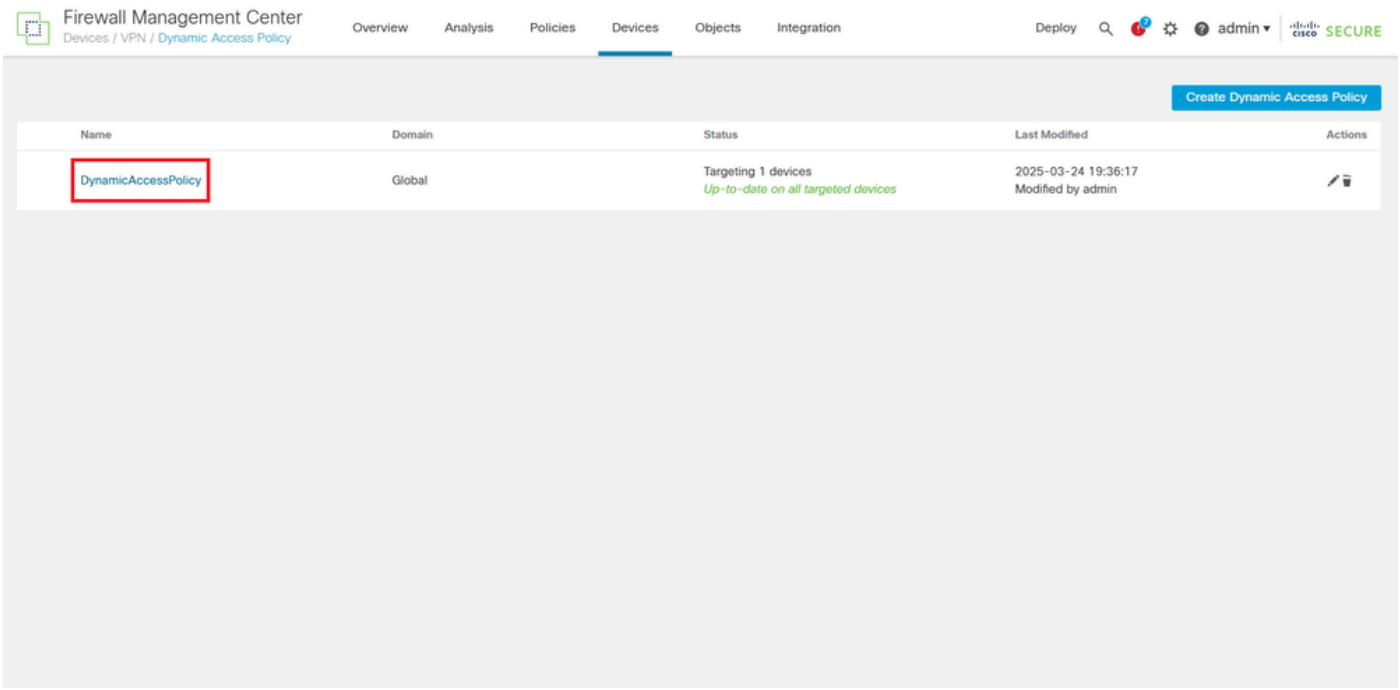
Pertanto, in questo documento, viene configurato uno script LUA per valutare il parametro Organization all'interno di un certificato client utilizzando le funzionalità di scripting LUA.

Configurazione

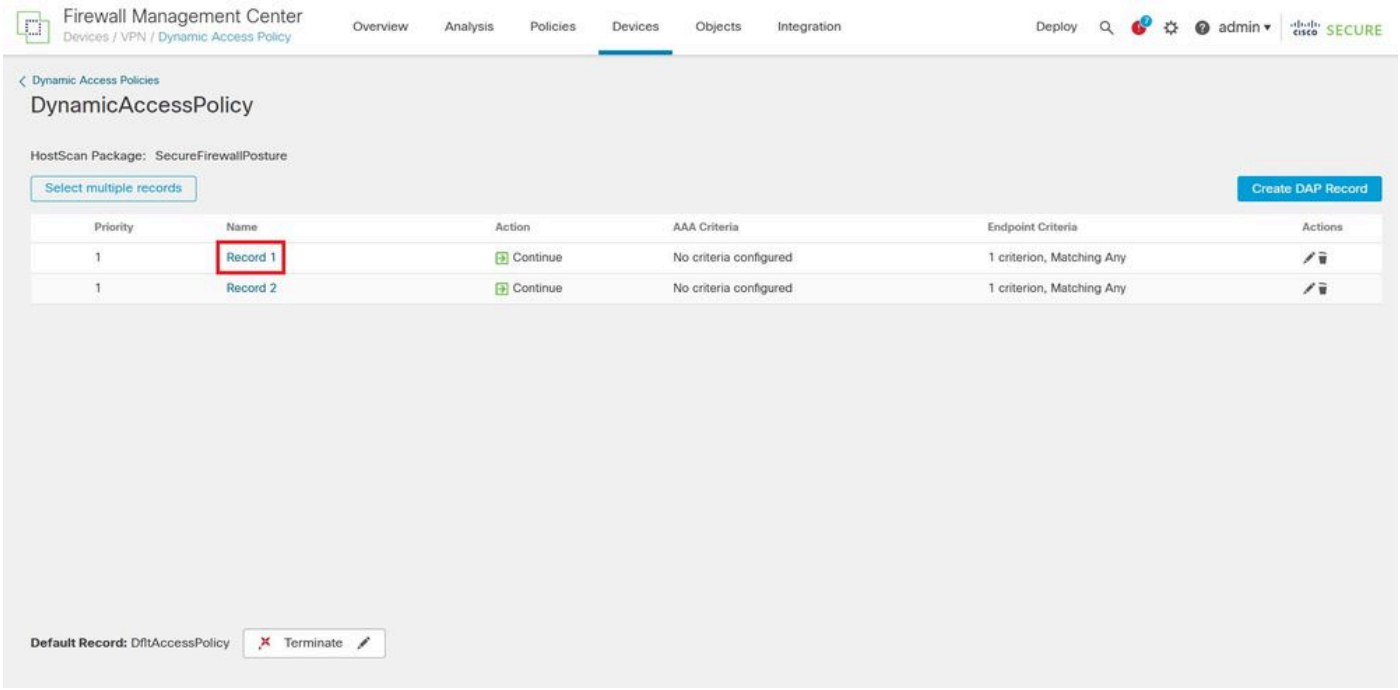
1. Accedere all'interfaccia utente di FMC, quindi dal dashboard passare a Devices >Dynamic Access Policy nel menu.



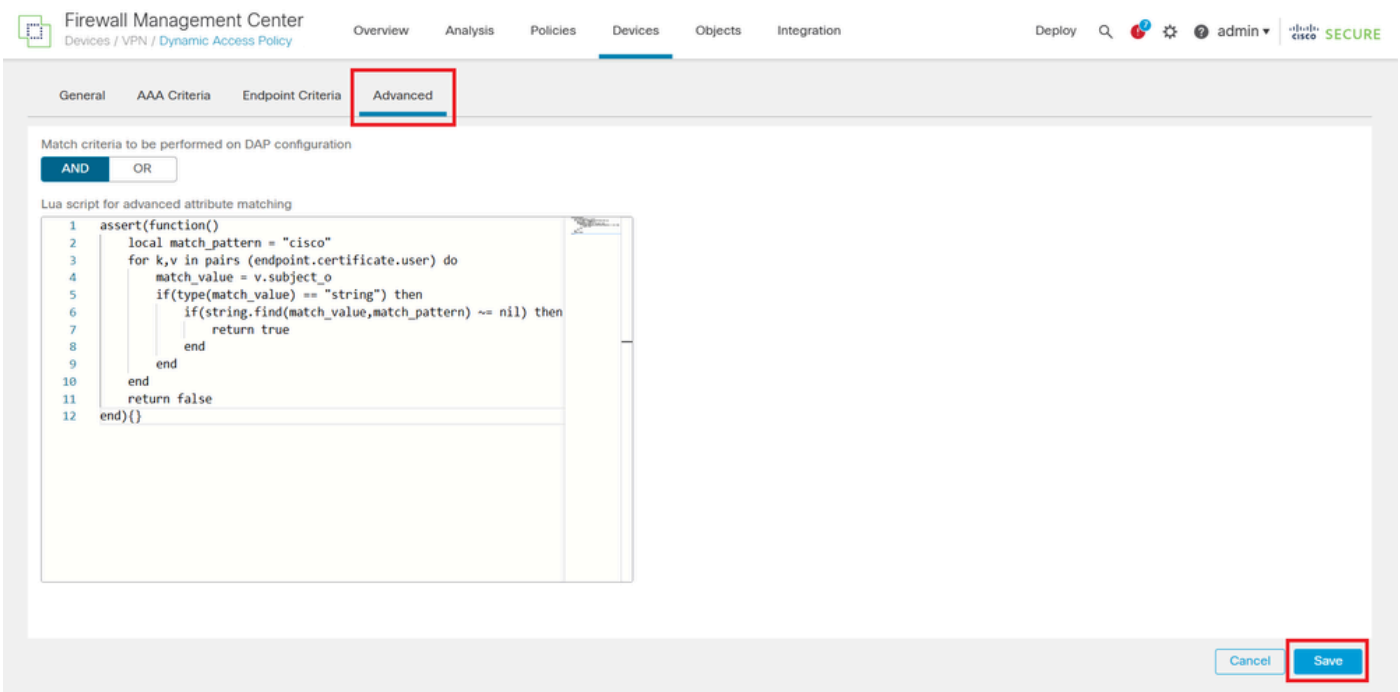
2. Aprire il criterio DAP applicato alla configurazione RAVPN.



3. Modificare il record desiderato per configurare lo script LUA facendo clic sul nome del record.



4. All'interno del record selezionato, passare alla scheda Avanzate per immettere lo script LUA che valuta i parametri obbligatori del certificato. Dopo aver configurato lo script, fare clic su Salva per applicare le modifiche. Una volta salvate le modifiche nel record DAP, distribuire il criterio per trasferire la configurazione aggiornata al dispositivo FTD.



Nota: Il codice presentato in questo articolo è progettato per valutare i certificati installati nel dispositivo client e verificare in particolare che esista un certificato il cui parametro Organization nel campo Subject corrisponda al valore 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){}
```

- Lo script definisce una variabile match_pattern impostata su cisco, che è il nome dell'organizzazione di destinazione da trovare.
- Esegue l'iterazione su tutti i certificati utente disponibili nell'endpoint utilizzando un ciclo for.
- Per ogni certificato viene estratto il campo Organizzazione (subject_o).
- Viene verificato se il campo Organizzazione è una stringa e quindi viene eseguita la ricerca di match_pattern al suo interno.
- Se viene trovata una corrispondenza, lo script restituisce true, a indicare che il certificato soddisfa i criteri.
- Se non viene trovato alcun certificato corrispondente dopo aver controllato tutti i certificati, lo script restituisce false, determinando la negazione dell'accesso da parte del criterio.

Questo approccio consente agli amministratori di implementare una logica di convalida dei certificati personalizzata che vada oltre i parametri standard esposti dall'interfaccia utente grafica (GUI) di FMC.

Verifica

Eseguire il comando more dap.xml per verificare che il codice sia presente nella configurazione DAP sull'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) {}
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).