Migration DAP et HostScan d'ASA vers FDM via l'API REST

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Licence Limitations des fonctionnalités Configuration Vérification Vérification Vérification du déploiement à partir de l'interface utilisateur FTD Vérification du déploiement à partir de la CLI FTD Dépannage

Introduction

Ce document décrit la migration de la configuration DAP (Dynamic Access Policies) et HostScan des appliances de sécurité adaptatives Cisco (ASA) vers Cisco Firepower Threat Defense (FTD) gérée localement par Firepower Device Manager (FDM).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de la configuration VPN RA sur FDM.
- Fonctionnement de DAP et de Hostscan sur ASA.
- Connaissance de base de l'API REST et de l'Explorateur d'API FDM Rest.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco FTD version 6.7.0
- Client Cisco AnyConnect Secure Mobility version 4.9.00086
- Postman ou tout autre outil de développement d'API

Remarque : les informations de ce document ont été créées à partir de périphériques dans un environnement de travaux pratiques spécifique. All of the devices used in this document

started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de toute modification de configuration.

Informations générales

Même si FTD prend en charge la configuration RAVPN (Remote Access VPN), il ne prend pas en charge le DAP. Depuis la version 6.7.0, la prise en charge de l'API est ajoutée pour DAP sur le FTD. Il est destiné à prendre en charge le cas d'utilisation très basique de la migration d'ASA vers FTD. Les utilisateurs qui ont un DAP configuré sur leur ASA et qui sont en train de migrer vers les FTD ont maintenant un chemin pour migrer leur configuration DAP avec leur configuration VPN d'accès distant.

Afin de réussir la migration de la configuration DAP d'ASA vers FTD, assurez-vous que les conditions suivantes sont réunies :

- ASA avec DAP/Hostscan configuré.
- Accès au serveur TFTP/FTP depuis l'accès ASA ou ASDM à l'ASA.
- Cisco FTD version 6.7.0 et ultérieure gérée par Firepower Device Manager (FDM).
- VPN RA configuré et fonctionnant sur FTD.

Licence

- FTD enregistré sur le portail de licences Smart avec Export Controlled Features activé (afin d'autoriser l'activation de l'onglet de configuration VPN RA).
- Toutes les licences AnyConnect activées (APEX, Plus ou VPN uniquement).

Afin de vérifier la licence : Accédez à Périphériques > Licences Smart

vice Summary Mart License	Assigned Virtual Account: Export-controlled features: Enabled Go to Cisco Smart Software Manager (2.	
Connected Sufficient License	Last sync: 17 Nov 2020 05:21 AM Next sync: 17 Nov 2020 05:31 AM	Go to Cloud Services 🔅 🗸
SCRIPTION LICENSES INCL	UDED	
Threat Disabled by user	ENABLE	Malware ENABLE
This License allows you must have this license to license to apply file polic	to perform intrusion detection and prevention and file control. You o apply intrusion policies in access rules. You also must have this cies that control files based on file type.	This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.
Includes: 🍄 Intrusion P	olicy	Includes: C File Policy
ORL License	ENABLE	RA VPN License Type PLUS ~ DISABLE
This license allows you t than by individual URL al traffic based on categor	to control web access based on URL categories and reputations, rather lone. You must have this license to deploy access rules that filter web y and reputation.	Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.
Includes: URL Reputatio	n	Includes: RA-VPN

Limitations des fonctionnalités

- Ces fonctionnalités sont uniquement prises en charge via l'interface API REST FDM/FTD.
- Le nom DAP ne peut pas contenir de caractères d'espace avec l'API REST.

Configuration

Étape 1. Copiez **dap.xml** d'ASA vers votre ordinateur local / serveur TFTP. Il existe deux façons d'y parvenir :

ASDM :

Accédez à Outils > Gestion de fichiers > Transfert de fichiers > entre PC locaux et Flash.

Local Computer ← Back → Fwd ↑ Up	W Delete	Disk(s)
-------------------------------------	----------	---------

CLI :

ASA# copy flash: tftp:

Source filename []? dap.xml

Address or name of remote host []? 10.197.161.160

Destination filename [dap.xml]?

440 bytes copied in 0.40 secs

Étape 2. Copiez le fichier de configuration hostscan (data.xml) et l'image hostscan d'ASA vers le périphérique local.

ASDM :

Accédez à Outils > Gestion de fichiers >Transfert de fichiers >entre PC locaux et Flash.



CLI:

ASA# copy flash: tftp:

Source filename []? data.xml

Address or name of remote host []? 10.197.161.160

Destination filename [data.xml]?

500 bytes copied in 0.40 secs

ASA# copy flash: tftp:

Source filename []? hostscan_4.9.03047-k9.pkg

Address or name of remote host []? 10.197.161.160

Étape 3. Obtient la valeur encodée base64 de dap.xml et data.xml.

Sur Mac : base64 -i <fichier>

tazkhan@TAZKHAN-M-32A3 Desktop % base64 -i dap.xml

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTGlzdD4KPGRhcFJlY29yZD4 KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXBOYW1lPgo8ZGFwVmlld3NSZWxhdGlvbj4KPHZhbHV1PmFuZDwvdmFsdWU+Cj wvZGFwVmlld3NSZWxhdGlvbj4KPGRhcEJhc2ljVmlldz4KPGRhcFNlbGVjdGlvbj4KPGRhcFBvbGljeT4KPHZhbHV1Pm1hdGNoLWFueTwvdmFsd WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KPG5hbWU+YWFhLmNpc2NvLnVzZXJuYW11PC9uYW11Pgo8dmFsdWU+Y2lzY288L3ZhbHV1Pgo8b3BlcmF0 aW9uPkVRPC9vcGVyYXRpb24+Cjx0eXB1PmNhc2VsZXNzPC90eXB1Pgo8L2F0dHI+CjwvZGFwUZVsZWN0aW9uPgo8ZGFwUZVsZWN0aW9uPgo8ZGF wUG9saWN5Pgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXBQb2xpY3k+CjxkYXBTdWJTZWx1Y3Rpb24+CjxkYXBQb2xpY3k+Cjx2YWx1ZT 5tYXRjaC1hbGw8L3ZhbHV1Pgo8b3B1cmF0aW9uPkVRPC9vcGVyYXRpb24+CjwvYXR0cj4KPC9kYXBTdWJTZWx1Y3Rpb24+CjwvZGFwUZVsZWN0aW9uPgo8ZGF w2GFwUM9s2WNbPg08b3B1cmF0aW9uPkVRPC9vcGVyYXRpb24+CjwvYXR0cj4KPC9kYXBTdWJTZWx1Y3Rpb24+CjwvZGFwUZVsZWN0aW9uPgo8ZGF w2GFyXdzUmVsYXRpb24+Cjx2YWx1ZT5hbmQ8L3ZhbHV1Pgo8L2RhcFZpZXdzUmVsYXRpb24+CjwvZGFwUmVjb3JkPgo8L2RhcFJ1Y29yZExpc3 Q+Cg==

Sous Windows powershell : certutil -encode dap.xml tmp.b64 ; findstr /v /c :- tmp.b64 > dap.b64

27 Windows PowerShell		-	×
Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved.			
<pre>PS C:\Users\tazkhan> cd Desktop PS C:\Users\tazkhan\Desktop> certutil -encode dap.xml tmp.b64 ; findstr /v /c:- tmp.b64 > dap.b Input Length = 793 Output Length = 1150 CertUtil: -encode command completed successfully. PS C:\Users\tazkhan\Desktop></pre>	64		
ap - Notepad	_	×	
<pre>File Edit Format View Help PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9 InllcyI/Pg08ZGFwUmVjb33kTGlzdD4kPGRhcFJ1V29yZD4kPGRhcE5hbWU+Cjx2 YWx1ZT5baXNjbzwvdmFsdWU+CjwvZGFwTmFtZT4kPGRhcFZpZXdzUmVsYXRpb24+ Cjx2YWx1ZT5hbm08L3ZhbHV1Pg08L2RhcF2pZXdzUmVsYXRpb24+CjxkYXBCYXNp Y1ZpZX+CjxkYXBTZWx1Y3Rpb24+CjxkYXB0b2xpY3k+Cjx2YWx1ZT5tYXRjaC1h bnk8L3ZhbHV1Pg08L2RhcF8vbGljeT4kPGF0dHI+CjxuYW11PmFhYS5jaXNjby51 c2VybmFtZTmvbmFtZT4kPHZhbHV1PmNpc2NvPC92YWx1ZT4kPC9wZXJhdGlvbj5F UTwvb3B1cmF0aW9uPg08dH1wZT5jYXN1bGVzczwvdH1wZT4KPC9hdHRyPg08L2Rh cFN1bGVjdGlvbj4KPC9kYXBCYXNpY1ZpZX+CjwvZGFwUmVjb3JkPg08ZGFwUmVj b3JkPg08ZGFwTmFtZT4KPHZhbHV1PIRlc3Q8L3ZhbHV1Pg08L2RhcE5hbWU+Cjxk YXBWaWV3c1J1bGF0aW9uPg08dmFsdWU+YW5kPC92YWx1ZT4KPC9kYXBWaWV3c1J1 bGF0aW9uPg08ZGFwQmFzaWNWaWV3Pg08ZGFwU2VsZWN0aW9uPg08ZGFwUG9saWN5 Pg08dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXB02xPV3k+CjxhdHRyPg08 bmFtZT5hYWEUY212Y28udXN1cm5hbWU8L25hbWU+Cjx2YW1ZT50ZXN0PC92YWx1 ZT4KPC9hdHRyPg08L2RhcFN1bGVjdGlvbj4KPC9kYXBCYXNpY1ZpZXc+CjwvZGFw UmVjb3JkPg08L2RhcFJ1Y29yZExpc3Q+Cg==</pre>			

Suivez la même procédure pour data.xml.

Étape 4. Lancez l'Explorateur d'API du FTD dans une fenêtre de navigateur.

Accédez à https://<FTD Management IP>/api-explorer

Il contient la liste complète des API disponibles sur le FTD. Il est divisé en fonction de la fonction principale avec plusieurs requêtes GET/POST/PUT/DELETE prises en charge par le module FDM.

DAPXml et HostScanPackageFile sont l'API utilisée.

← → C ▲ Not Secure 10.19	07.224.82/#/api-explorer	🖈 😊 🖬 🍳 🔯 🏷 Update	
CISCO. Firepower Device M	anager Monitoring Policies Objects Device: firepower	(5.) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	
FTD REST API 🔶	DAPXml	Show/Hide List Operations Expand Operations	
ADI Evolarer	GET /object/dapxml	Get the DAPXml configured	
Artexplorer	POST /object/dapxml	Create a new DAPXml configuration	
Error Catalog	ottere /object/dapxml/{objid}	Delete the DAPXml configuration	
	7 /object/dapxml/{objld} Get the DAPXm		
	در /object/dapxml/{objid}	Update the DAPXml configuration	

Étape 5. Ajoutez une collection Postman pour DAP.

Indiquez un nom pour la collection. Cliquez sur Créer, comme illustré dans cette image.

CREATE A NEW (COLLECTION				×
Name					
DAP					
Description	Authorization	Pre-request Scripts	Tests	Variables	

This description will show in your collection's documentation, along with the descriptions of its folders and requests.

Make things easier for your teammates with a complete collection description.

Descriptions support Markdown

Cancel	Create

Étape 6. Ajouter une nouvelle demande authentification pour créer une requête POST de connexion au FTD afin d'obtenir le jeton pour autoriser toute requête POST/GET/PUT. Cliquez sur

Enregistrer.