REST APIによるASAからFDMへのDAPおよび HostScanの移行

内容

概要前提条件要件使用するコンポーネント背景説明ライセンス機能制限コンフィギュレーション確認FTD GUIからの導入検証FTD CLIからの導入検証トラブルシュート

概要

このドキュメントでは、Cisco Adaptive Security Appliances(ASA)からFirepower Device Manager(FDM)によってローカルで管理されるCisco Firepower Threat Defense(FTD)へのダイナ ミックアクセスポリシー(DAP)およびHostScan設定の移行について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FDMでのRA VPN設定に関する基礎知識。
- ASAでのDAPおよびHostscanの動作。
- REST APIおよびFDM Rest APIエクスプローラの基礎知識。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・バージョン6.7.0が稼働するCisco FTD
- Cisco AnyConnect Secure Mobility Clientversion 4.9.00086
- Postmanまたはその他のAPI開発ツール

注:このドキュメントの情報は、特定のラボ環境のデバイスから作成されたものです。この ドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動して います。ネットワークが稼働中の場合は、設定変更による潜在的な影響について理解してお

背景説明

FTDではリモートアクセスVPN(RAVPN)の設定がサポートされていますが、DAPのサポートはありません。リリース6.7.0以降、FTDでDAPのAPIサポートが追加されました。これは、ASAから FTDへの移行の非常に基本的な使用例をサポートすることを目的としています。ASAでDAPが設定されており、FTDに移行する途中のユーザには、RA VPN設定とともにDAP設定を移行するパスが用意されています。

DAP設定をASAからFTDに正常に移行するには、次の条件を確認します。

- DAP/ホストスキャンが設定されたASA。
- •ASAまたはASDMからASAへのTFTP/FTPサーバアクセス。
- バージョン6.7.0以降を実行するCisco FTDは、Firepower Device Manager(FDM)によって管理されます。
- •FTDで設定され、動作しているRA VPN。

ライセンス

- [Export Controlled Features]を有効にしてスマートライセンスポータルに登録された FTD(RA VPN設定タブを有効にするために)。
- 有効になっているAnyConnectライセンス(APEX、Plus、またはVPN-Only)。

ライセンスを確認するには: [Devices] > [Smart Licenses]に移動します。

vice Summary mart License	Assigned Virtual Account: Export-controlled features: Enabled Go to Cisco Smart Software Manager (3.			
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 ENABL	E	
This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies 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 Po	olicy	Includes: Co File Policy		
URL License	ENABLE	RA VPN License Type PLUS ~ DISABU	E	
This license allows you to	o control web access based on URL categories and reputations, rather	Please select the license type that you purchased to enable remote access VPN. Note that	it	
than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.		Firepower Device Manager does not support any of the advanced features covered by the Apex license.)	
Includes: URL Reputatio	n	Includes: RA-VPN		

機能制限

- •これらの機能は、FDM/FTD REST APIインターフェイスでのみサポートされます。
- DAP名にREST APIの空白文字を含めることはできません。

コンフィギュレーション

ステップ1: ASAからロ**ーカルPC/**TFTPサーバにdap.xmlをコピーします。これを実現するには、次の2つの方法があります。

ASDM:

[Tools] > [File Management] > [File Transfer] > [Local PC and Flash]に移動します。



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

ステップ 2:ホストスキャン設定ファイル(data.xml)とホストスキャンイメージをASAからローカ ルデバイスにコピーします。

ASDM:

[Tools] > [File Management] > [File Transfer] > [Between Local PC and Flash] に移動します。



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

Mac:base64 -i <file>

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

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTGlzdD4KPGRhcFJlY29yZD4 KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXBOYW1lPgo8ZGFwVmlld3NSZWxhdGlvbj4KPHZhbHV1PmFuZDwvdmFsdWU+Cj wvZGFwVmlld3NSZWxhdGlvbj4KPGRhcEJhc2ljVmlldz4KPGRhcFNlbGVjdGlvbj4KPGRhcFBvbGljeT4KPHZhbHV1Pm1hdGNoLWFueTwvdmFsd WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KPG5hbWU+YWFhLmNpc2NvLnVzZXJuYW11PC9uYW11Pgo8dmFsdWU+Y2lzY288L3ZhbHV1Pgo8b3BlcmF0 aW9uPkVRPC9vcGVyYRpb24+Cjx0eXB1PmNhc2VsZXNzPC90eXB1Pgo8L2F0dHI+CjwvZGFwUZVsZWN0aW9uPgo8ZGFwUZVsZWN0aW9uPgo8ZGF wUG9saWN5Pgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXB0b2xpY3k+CjxKYXBTdWJTZWx1Y3Rpb24+CjxkYXBdb2xpY3k+Cjx2YWx1ZT 5tYXRjaC1hbGw8L3ZhbHV1Pgo8b2RhcFBvbG1jeT4KPGF0dHI+CjxuYW11PmVuZHBvaW50LmFueWNvbm51Y3QucGxhdGZvcm08L25hbWU+Cjx2Y Wx1ZT53aW48L3ZhbHV1Pgo8b3B1cmF0aW9uPkVRPC9vcGVyYXRpb24+CjwvYXR0cj4KPC9kYXBTdWJTZWx1Y3Rpb24+CjwvZGFwUZVsZWN0aW9u Pgo8L2RhcEJhc21jVmlldz4KPC9kYXBSZWNvcmQ+CjxkYXBSZWNvcmQ+CjxkYXB0YW11Pgo8dmFsdWU+YTwvdmFsdWU+CjwvZGFwTmFtZT4KPGR hcFZpZXdzUmVsYXRpb24+Cjx2YWx1ZT5hbmQ8L3ZhbHV1Pgo8L2RhcFZpZXdzUmVsYXRpb24+CjwvZGFwUmVjb3JkPgo8L2RhcFJ1Y29yZExpc3 Q+Cg=

Windows Powershellの場合: certutil -encode dap.xml tmp.b64 ;findstr /v /c:- tmp.b64 > dap.b64

🔁 Windows PowerShell			-	×
Windows PowerShell Copyright (C) Microsoft (Corporation. All rights reserved.			
PS C:\Users\tazkhan> cd U PS C:\Users\tazkhan\Deskt Input Length = 793 Output Length = 1150 CertUtil: -encode command PS C:\Users\tazkhan\Deskt	Desktop cop> certutil -encode dap.xml tmp.b64 ; findstr /v /c:- tmp.b64 d completed successfully. cop>	> dap.b64		
ap - Notepad		—	×	
File Edit Format View Hel PD94bWwgdmVyc2lvbj4 InllcyI/Pgo8ZGFwUm YWx1ZT5DaXNjbzwvdm1 Cjx2YWx1ZT5hbmQ8L3 Y1ZpZXc+CjxkYXBTZW bnk8L3ZhbHV1Pgo8L2 c2VybmFtZTwvbmFtZT4 UTwvb3B1cmF0aW9uPg cFN1bGVjdG1vbj4KPC9 b3JkPgo8ZGFwTmFtZT4 YXBWaWV3c1J1bGF0aW bGF0aW9uPgo8ZGFwQm Pgo8dmFsdWU+bWF0Y2f bmFtZT5hYWEuY21zY22 ZT4KPC9hdHRyPgo8L2 UmVjb3JkPgo8L2RhcF3	p p p p p p p p p p p p p p		~	
<			> .:i	

data.xmlについても同じ手順に従います。

ステップ4:ブラウザウィンドウでFTDのAPI Explorerを起動します。

https://<FTD Management IP>/api-explorerに移動します

これには、FTDで使用可能なAPIのリスト全体が含まれます。これは、FDMでサポートされている複数のGET/POST/PUT/DELETE要求を含む主機能に基づいて分割されます。

DAPXmlとHostScanPackageFileが使用されるAPIです。

← → C 🔺 Not Secure 10.197.224.82/#/api-explorer 🖄 😃 🗒 🖉 🚺				
CISCO. Firepower Devic	e Manager 🖗 🕅 🛱 👘 🖓 🛱 Monitoring Policies Objects Device: firepower	(>) (admin Administrator		
FTD REST API 🔶	DAPXml	Show/Hide List Operations Expand Operations		
ADI Explorer	GET /object/dapxml	Get the DAPXml configured		
AFTEXPIORE	Posr /object/dapxml	Create a new DAPXml configuration		
Error Catalog	otter: /object/dapxml/{objld}	Delete the DAPXml configuration		
	GET /object/dapxml/{objld}	Get the DAPXml configured		
	PUT /object/dapxml/(objid)	Update the DAPXml configuration		

ステップ5: DAPのPostmanコレクションを追加します。

コレクション**の名前**を指定します。次の図に示すように、[Create]をクリックします。

CREATE A NEW C	OLLECTION				×
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
--------	--------

手順 6:新しい要求の追加 AUTH トークンを取得してPOST/GET/PUT要求を認可するために、 FTDへのログインPOST要求を作成します。[Save] をクリックします。