DAP和HostScan通过REST API从ASA迁移到 FDM

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> <u>许可</u> <u>功能限制</u> <u>配置</u> <u>验证</u> <u>从FTD GUI进行部署验证</u> <u>从FTD CLI进行部署验证</u> <u>故障排除</u>

简介

本文档介绍动态访问策略(DAP)和HostScan配置从思科自适应安全设备(ASA)迁移到由Firepower设备管理器(FDM)本地管理的思科Firepower威胁防御(FTD)。

先决条件

要求

Cisco 建议您了解以下主题:

- FDM上RA VPN配置的基本知识。
- •在ASA上运行DAP和Hostscan。
- REST API和FDM Rest API资源管理器的基本知识。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- •运行版本6.7.0的思科FTD
- •思科AnyConnect安全移动客户端版本4.9.00086
- 邮递员或任何其他API开发工具

注意:本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备最初均采 用原始(默认)配置。如果您的网络处于活动状态,请确保您了解任何配置更改的潜在影响。

背景信息

即使FTD具有远程访问VPN(RAVPN)配置支持,它也缺乏对DAP的支持。自版本6.7.0起,FTD上为 DAP添加了API支持。它旨在支持从ASA迁移到FTD的非常基本的使用案例。在其ASA上配置了 DAP且正在迁移到FTD的用户现在有了迁移其DAP配置及其RA VPN配置的路径。

要成功将DAP配置从ASA迁移到FTD,请确保以下条件:

- •配置了DAP/Hostscan的ASA。
- •从ASA访问TFTP/FTP服务器或从ASDM访问ASA。
- •运行版本6.7.0及更高版本的Cisco FTD,由Firepower设备管理器(FDM)管理。
- 在FTD上配置和运行RA VPN。

许可

- •FTD已注册到智能许可门户,并启用了导出受控功能(以允许启用RA VPN配置选项卡)。
- •任何一个AnyConnect许可证都已启用(APEX、Plus或仅VPN)。

要检查许可:导航至设备>智能许可证

Device Summary Smart License Go to Cisco Smart Software Manager D.	
Connected Last sync: 17 Nov 2020 05:21 AM Sufficient License Next sync: 17 Nov 2020 05:31 AM	Go to Cloud Services 🛛 🗘 🗸
SUBSCRIPTION LICENSES INCLUDED	
Threat ENABLE	Malware ENABLE
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 Policy	Includes: C File Policy
URL License ENABLE	RA VPN License Type PLUS ~ DISABLE
This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category 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 Reputation	Includes: RA-VPN

功能限制

- 仅通过FDM/FTD REST API接口支持这些功能。
- DAP名称不能包含REST API的空格字符。

配置

步骤1:将dap.xml从ASA复制到本地PC/TFTP服务器。实现这一目标有两种方法:

ASDM:

导航至工具>文件管理>文件传输>本地PC和闪存之间。

🖕 Back 🔿 Fwd 🛧 Up 🔇 Refresh 🍛 New 👔 Delete	Disk(s) Back + Fwd + Up Refresh A New Delete
 dev etc home Library net Network opt opt private sbin System tmp Users usr var Volumes .DS_Store installer.failurerequests .file 	<pre>asa941-13-lfbff-k8.SPA all_working_tunnels.txt asa953-6-lfbff-k8.SPA anyconnect-win-4.3.03086-k9.pkg backupconfig-1 lfbff.SSA.CSCvc55674.01192017.2 lfbff.SSA.CSCvc55674.01302017.1 hostscan_4.3.05017-k9.pkg dap.xml crash.txt anyconnect-win-4.4.01054-webdeploy-k9.pk anyconnect_rdp.xml asa981-lfbff-k8.SPA show_texh.txt lfbff.SSA.CSCve72227.06122017.1 working_1500_count.txt show_tech.txt</pre>

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

第二步:将主机扫描配置文件(data.xml)和主机扫描映像从ASA复制到本地设备。

ASDM:

导航至工具 >文件管理>文件传输>本地PC和闪存之间。



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

第三步: 获取dap.xml和data.xml的base64编码值。

在Mac上: base64 -i <file>

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

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTGlzdD4KPGRhcFJlY29yZD4 KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXB0YW1lPgo8ZGFwVmlld3NSZWxhdGlvbj4KPHZhbHV1PmFuZDwvdmFsdWU+Cj wvZGFwVmlld3NSZWxhdGlvbj4KPGRhcEJhc2ljVmlldz4KPGRhcFNlbGVjdGlvbj4KPGRhcFBvbGljeT4KPHZhbHV1Pm1hdGNoLWFueTwvdmFsd WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KP65hbWU+YWFhLmNpc2NvLnVzZXJuYW11PC9uYW11Pgo8dmFsdWU+Y2lzY288L3ZhbHV1Pgo8b3BlcmF0 aW9uPkVRPC9vcGVyYXRpb24+Cjx0eXB1PmNhc2VsZXNzPC90eXB1Pgo8L2F0dHI+CjwvZGFwU2VsZWN0aW9uPgo8ZGFWU2VsZWN0aW9uPgo8ZGF wUG9saWN5Pgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXBQb2xpY3k+CjxkYXBTdWJTZWx1Y3Rpb24+CjxkYXBQb2xpY3k+Cjx2YWx1ZT 5tYXRjaC1hbGw8L3ZhbHV1Pgo8L2RhcFBvbG1jeT4KPGF0dHI+CjxuYW11PmVuZHBvaW50LmFueWNvbm51Y3QucGxhdGZvcm08L25hbWU+cjx2Y Wx1ZT53aW48L3ZhbHV1Pgo8b3B1cmF0aW9uPkVRPC9vcGVyYXRpb24+CjwvYXR0cj4KPC9kYXBTdWJTZWx1Y3Rpb24+CjwvZGFwU2VsZWN0aW9u Pgo8L2RhcEJhc21jVmlldz4KPC9kYXBSZWNvcmQ+CjxkYXBSZWNvcmQ+CjxkYXBOYW1Pgo8dmFsdWU+YTwvdmFsdWU+CjwvZGFwTmFtZT4KPGR hcFzpZXdzUmVsYXRpb24+cjx2YWx1ZT5hbmQ8L3ZhbHV1Pgo8L2RhcFZpZXdzUmVsYXRpb24+CjwvZGFwUmVjb3JkPgo8L2RhcFJ1Y29yZExpc3 Q+Cg==

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

Windows PowerShell	-]	×
<pre>Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved. PS C:\Users\tazkhan> cd Desktop PS C:\Users\tazkhan\Desktop> certutil -encode dap.xml tmp.b64 ; findstr /v /c:- tmp.b64 > dap.b64 Input Length = 793 Output Length = 1150 CertUtil: -encode command completed successfully. PS C:\Users\tazkhan\Desktop></pre>			
	×		

对data.xml执行相同的步骤。

步骤4.在浏览器窗口中启动FTD的API浏览器。

导航至https://<FTD管理IP>/api-explorer

这包含FTD上可用的API的完整列表。它根据FDM支持的多个GET/POST/PUT/DELETE请求的主要 功能进行划分。

DAPXml和HostScanPackageFile是使用的API。

← → C ▲ Not Secure	10.197.224.82/#/api	-explorer										5	à 💿 🖬 G	27	* 🕲 🤇	Update
CISCO. Firepower Devic	ce Manager	题 Monitoring	Ø Policies	iiz: Objects	Device:	firepower		6.	٢	9	?	0	admin Administrato	r ~		
FTD REST API 🛛 🔶	DAPXml										Show	/Hide	List Operations	Expan	d Operation	15
ADI Evolorer	GET /	object/dapxml											Get th	e DAPXr	nl configure	d
AFTEXPIORE	POST /	object/dapxml											Create a new	DAPXml	configuratio	n
Error Catalog	DELETE	object/dapxml/{o	bjld}										Delete the	DAPXml	configuratio	in
	GET /	object/dapxml/{o	bjld}										Get th	e DAPXr	nl configure	d
	PUT /	object/dapxml/{o	bjld}										Update the	DAPXml	configuratio	in

第五步:为DAP添加Postman集合。

为集合**提**供名称。单击"**创建**",如下图所示。

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

reate

第六步:添加新请求 auth 创建到FTD的登录POST请求,以便获取令牌以授权任何 POST/GET/PUT请求。单击"**Save**(保**存)"**。