Migración de DAP y HostScan de ASA a FDM a través de la API REST

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Licencias Limitaciones de la función Configuración Verificación Verificación de la implementación desde la GUI de FTD Verificación de la implementación desde la CLI de FTD Troubleshoot

Introducción

Este documento describe la migración de las políticas de acceso dinámico (DAP) y la configuración de HostScan de Cisco Adaptive Security Appliances (ASA) a Cisco Firepower Threat Defense (FTD) gestionada localmente por Firepower Device Manager (FDM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración de VPN RA en FDM.
- Trabajo de DAP y HostScan en ASA.
- Conocimiento básico de la API REST y el Explorador de API Rest de FDM.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco FTD ejecutando la versión 6.7.0
- Cliente de Cisco AnyConnect Secure Mobility versión 4.9.00086
- Postman o cualquier otra herramienta de desarrollo API

Nota: La información de este documento se creó a partir de dispositivos en un entorno de laboratorio específico. All of the devices used in this document started with a cleared

(default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier cambio de configuración.

Antecedentes

Aunque FTD tiene compatibilidad con la configuración de VPN de acceso remoto (RAVPN), carece de compatibilidad con DAP. A partir de la versión 6.7.0, se agrega soporte de API para DAP en el FTD. Se ha diseñado para admitir el caso práctico más básico de la migración de ASA a FTD. Los usuarios que tienen DAP configurado en sus ASA y están en proceso de migrar a FTD ahora tienen una ruta para migrar su configuración DAP junto con su configuración de VPN RA.

Para migrar correctamente la configuración DAP de ASA a FTD, asegúrese de estas condiciones:

- ASA con DAP/HostScan configurado.
- Acceso al servidor TFTP/FTP desde ASA o ASDM al ASA.
- Cisco FTD que ejecuta la versión 6.7.0 y las versiones posteriores gestionadas por Firepower Device Manager (FDM).
- VPN RA configurada y funcionando en FTD.

Licencias

- FTD se registró en el portal de licencias inteligente con las funciones controladas de exportación activadas (para permitir que se habilite la ficha de configuración de VPN de RA).
- Cualquiera de las licencias de AnyConnect habilitadas (APEX, Plus o VPN-Only).

Para verificar la licencia: Vaya a **Dispositivos > Licencias inteligentes**



Limitaciones de la función

• Estas funciones solo se admiten a través de la interfaz API FDM/FTD REST.

• El nombre DAP no puede contener caracteres de espacio con la API REST.

Configuración

Paso 1. Copie dap.xml de ASA en su PC local / servidor TFTP. Hay dos maneras de lograr lo mismo:

ASDM:

Vaya a Herramientas > Administración de archivos > Transferencia > Entre PC local y Flash.

Local Computer Back Fwd Up Refresh New 1 O etc home Library net Network Opt private System System Users Users Users Users Volumes .DS_Store installer.failurerequests .file	Delete> < Help	Disk(s) Back Fwd Up Refresh New Delete 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
--	----------------	--

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

Paso 2. Copie el archivo de configuración de HostScan (data.xml) y la imagen de HostScan desde ASA al dispositivo local.

ASDM:

Vaya a Herramientas > Administración de archivos > Transferencia > Entre PC local y 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

Paso 3. Obtenga el valor codificado base64 de dap.xml y data.xml.

En Mac: base64 -i <file>

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==

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

<pre>Windows PowerShall Copyright (c) Microsoft Corporation. All rights reserved. PS C: Userstarkhan)Desktop> certuil -encode dep.xml tmp.b64 ; findstr /v /c:- tmp.b64 > dep.b64 Trupt Length = 733 CertUil: -encode command completed successfully. PS C: Userstarkhan)Desktop></pre>	ſ	E Windows PowerShell	-	×
		Mindows PowerShell Copyright (C) Microsoft Corporation. All rights reserved. PS C:\Users\tazkhan\Desktop> <mark>certutil -encode</mark> dap.xml tmp.b64 ; findstr /v /c:- tmp.b64 > dap.b64 Snput Length = 793 Dutput Length = 1150 SertUtil: -encode command completed successfully. PS C:\Users\tazkhan\Desktop>		
<		<pre>File Edit Format View Help PD94bWwgdmVyc212Vbj0iM54wIiB1bmNvZG1uZz0iVVRGLTgiIHN0YW5kYWxvbmU9 Inl1cyI/Pgo82GFwUmVjb3JkTG1zdD4KPGRhcFJ1Y29yZD4KPGRhcE5hbWU+Cjx2 YWx1ZT5bDaXNjbzwvdmFsdWU+CjwvZGFwTmFtZT4KPGRhcFZpZXdzUmVsYXRpb24+ Cjx2YWx1ZT5hbmQ8L3ZhbHV1Pgo8L2RhcFZpZXdzUmVsYXRpb24+CjxKYXBCYXNp Y1ZpZXc+CjxKYXBTY2Nx1Y3Rpb24+CjxKYXBQb2xPY3k+Cjx2Wx1ZT5tYXRjaC1h bnk8L3ZhbHV1Pgo8L2RhcFBvbG1jeT4KPGF0dHI+CjxUYW11PmFhYS5jaXNjby51 c2VybmFtZTaVvbmFtZT4KPHZhbHV1Pmbp22NvPC92YWx1ZT4KPC9hdHRyPgo8L2Rh cFN1bGVjdG1vbj4KPC9kYXBCYXNPY1ZpZXc+CjwvZGFwUmVjb33NFgo8ZGFwUmVj b33LPgo8ZGFwTmFtZT4KPHZhbHV1P1R1c3Q8L3ZhbHV1Pgo8L2RhcE5hbWU+Cjxk YXBWaW3c1J1bGF0aW9uPgo8dmFsdWU+YW5kPC92YWx1ZT4KPC9kYXBWaWV3c1J1 bGF0aW9uPgo8ZGFwQmFzaMNWaW3Pgo8ZGFwU29SzWN0aM9uPgo8ZGFwUC9saWN5 Pgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXBQ2xPY3k+CjxhdHRyPgo8 bmftzT5hYMEuY21zYZaudXNLm5hbWU81z5hbWU+Cjx2YWx1ZT5VRXDP22Xc+CjwvZGFw UmVjb3JkPgo8L2RhcFJ1Y29yZExpc3Q+Cg= </pre>		

Siga el mismo procedimiento para data.xml.

Paso 4. Inicie el Explorador de API del FTD en una ventana del explorador.

Vaya a https://<FTD Management IP>/api-explorer

Esto contiene la lista completa de API disponibles en el FTD. Se divide en función de la función principal con varias solicitudes GET/POST/PUT/DELETE que admite el FDM.

DAPXml y HostScanPackageFile son la API utilizada.

C 🔺 Not Secure 10.197.224.82/#/api-explorer x 🕹 🖶 Q 🔄 🕸 🥨 Updat x				
cisco. Firepower Device	e Manager 🖗 🔅 🛱 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		
Post /object/dapxml		Create a new DAPXml configuration		
Error Catalog otLete /object/dapxml/{objid}		Delete the DAPXml configuration		
Get the DAP				
	evr /object/dapxml/{objid}	Update the DAPXml configuration		

Paso 5. Agregue una colección Postman para DAP.

Proporcione un nombre para la colección. Haga clic en Crear, como se muestra en esta imagen.

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

Paso 6. Agregar una nueva solicitud **Autenticación** para crear una solicitud POST de inicio de sesión en el FTD para obtener el token para autorizar cualquier solicitud POST/GET/PUT. Haga

clic en Guardar.