# DAP- en Host Scan-migratie van ASA naar FDM via REST API

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Licentie Functiebeperkingen Configuratie Verifiëren Implementatie-verificatie van FTD GUI Implementatie-verificatie van FTD CLI Problemen oplossen

# Inleiding

Dit document beschrijft de migratie van Dynamic Access Policy (DAP) en HostScan-configuratie van Cisco adaptieve security applicaties (ASA) naar Cisco Firepower Threat Defense (FTD), die lokaal wordt beheerd door Firepower Apparaatbeheer (FDM).

# Voorwaarden

# Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van RA VPN-configuratie op FDM.
- Werken van DAP en Hostscan op ASA.
- Basiskennis van REST API en FDM Rest API Explorer.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco FTD-versie 6.7.0
- Cisco AnyConnect Secure Mobility Clientversie 4.9.0086
- Postman of een ander API-ontwikkelingsmiddel

**Opmerking:** de informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg ervoor dat u de

# Achtergrondinformatie

Hoewel FTD ondersteuning heeft voor de configuratie van Remote Access VPN (RAVPN), biedt het geen ondersteuning voor DAP. Vanaf release 6.7.0 wordt API-ondersteuning voor DAP op de FTD toegevoegd. Het is bedoeld ter ondersteuning van het zeer fundamentele gebruiksgeval van migratie van ASA naar FTD. Gebruikers die DAP op hun ASA's hebben geconfigureerd en die momenteel naar FTD's migreren hebben nu een pad om hun DAP-configuratie samen met hun RA VPN-configuratie te migreren.

Om de DAP-configuratie van ASA naar FTD te kunnen migreren, moet u deze voorwaarden waarborgen:

- ASA met DAP/Hostscan ingesteld.
- TFTP/FTP-servertoegang van de ASA- of ASDM-toegang tot de ASA.
- Cisco FTD-versie 6.7.0 en hoger, beheerd door FirePOWER Apparaatbeheer (FDM).
- RA VPN geconfigureerd en werkt aan FTD.

## Licentie

- FTD geregistreerd op het slimme licentiepatroon met Door export gecontroleerde functies ingeschakeld (om het tabblad RA VPN in te schakelen).
- AnyConnect-licenties zijn ingeschakeld (APEX, Plus of VPN-alleen).

Zo controleert u de vergunningen: Navigeren in naar apparaten > Smart-licenties

vice Summary mart License	Assigned Virtual A Export-controlled Go to Cisco Smar Last sync: 17 Nov 2020 05:21 AM	Account: features: Enabled t Software Manager [2].			Go to Clou	ud Services 🗘 🗸
Sufficient License	Next sync: 17 Nov 2020 05:31 AM	0				
BSCRIPTION LICENSES INCL	UDED					
Threat		ENABLE	Malware			ENABLE
Disabled by user			Disabled by user			
This License allows you must have this license to license to apply file polic	to perform intrusion detection and prevent o apply intrusion policies in access rules. Yr ies that control files based on file type.	ion and file control. You ou also must have this	This License allows you to perform Cisco Firepower and AMP Threat Grid. You mus and block malware in files transmitted ov	Advanced Malware Pro st have this license to ap er your network.	otection (AMP) oply file policie	with AMP for s that detect
Includes: 🌯 Intrusion Pe	olicy		Includes: Cy File Policy			
URL License		ENABLE	RA VPN License	Туре	PLUS V	DISABLE
Disabled by user			Senabled			
This license allows you to than by individual URL al traffic based on category	o control web access based on URL categ ione. You must have this license to deploy y and reputation.	jories and reputations, rather access rules that filter web	Please select the license type that you po Firepower Device Manager does not sup Apex license.	urchased to enable remo port any of the advanced	ote access VPI d features cov	N. Note that ered by the

# Functiebeperkingen

• Deze functies worden alleen ondersteund via FDM/FTD REST API-interface.

• De DAP-naam kan geen ruimtetekens met REST API bevatten.

# Configuratie

**Stap 1.** Kopieer **dap.xml** van ASA naar uw lokale PC / TFTP Server. Er zijn twee manieren om hetzelfde te bereiken:

ASDM:

Navigeren in op Gereedschappen>Bestandsbeheer > File Transfer >tussen lokale pc en Flash.

Local Computer Back → Fwd ↑ Up  Refresh  New     let     etc     home     Library     net     Network     opt     private     sbin     System     funp     Users     usr     var     Volumes     .DS_Store     installer.failurerequests     .file	Delete> < Help Clo	Disk(s) Back  Fwd  Up  Refresh  New  Delete as a941-13-Ifbff-k8.SPA all_working_tunnels.txt as a953-6-Ifbff-k8.SPA anyconnect-win-4.3.03086-k9.pkg backupconfig-1 Ifbff.SSA.CSCvc55674.01192017.2 Ifbff.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 as a981-Ifbff-k8.SPA show_texh.txt Ifbff.SSA.CSCve72227.06122017.1 working_1500_count.txt show_tech.txt toreat-deleteet#II=C00000014
---	--------------------	---

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

**Stap 2.** Kopieert het bestand hostscan Setup (data.xml) en hostscan afbeelding van ASA naar het lokale apparaat.

#### ASDM:

Navigeer naar tools > File Management > File Transfer >tussen lokale pc en 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

Stap 3. Ontvang de basis64-gecodeerde waarde van dap.xml en data.xml.

Op Mac: base64-i <bestand>

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

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTGlzdD4KPGRhcFJlY29yZD4 KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXBOYW1lPgo8ZGFwVmlld3NSZWxhdGlvbj4KPHZhbHV1PmFuZDwvdmFsdWU+Cj wvZGFwVmlld3NSZWxhdGlvbj4KPGRhcEJhc2ljVmlldz4KPGRhcFNlbGVjdGlvbj4KPGRhcFBvbGljeT4KPHZhbHV1Pm1hdGNoLWFueTwvdmFsd WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KPG5hbWU+YWFhLmNpc2NvLnVzZXJuYW11PC9uYW11Pgo8dmFsdWU+Y2lzY288L3ZhbHV1Pgo8b3BlcmF0 aW9uPkVRPC9vcGVyYXRpb24+Cjx0eXB1PmNhc2VsZXNzPC90eXB1Pgo8L2F0dHI+CjwvZGFwUZVsZWN0aW9uPgo8ZGFwUZVsZWN0aW9uPgo8ZGF wUG9saWN5Pgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXB0b2xpY3k+CjxkYXBTdWJTZWx1Y3Rpb24+CjxkYXBQb2xpY3k+Cjx2YWx1ZT 5tYXRjaC1hbGw8L3ZhbHV1Pgo8b2RhcFBvbG1jeT4KPGF0dHI+CjxuYW11PmVuZHBvaW50LmFueWNvbm51Y3QucGxhdGZvcm08L25hbWU+Cjx2Y Wx1ZT53aW48L3ZhbHV1Pgo8b3B1cmF0aW9uPkVRPC9vcGVyYXRpb24+CjwvYXR0cj4KPC9kYXBTdWJTZWx1Y3Rpb24+CjwvZGFwUZVsZWN0aW9u Pgo8L2RhcEJhc21jVmlldz4KPC9kYXBSZWNvcmQ+CjxkYXBSZWNvcmQ+CjxkYXBOYW11Pgo8dmFsdWU+YTwvdmFsdWU+CjwvZGFwTFtZT4KPGR hcFzpZXdzUmVsYXRpb24+Cjx2YWx1ZT5hbmQ8L3ZhbHV1Pgo8L2RhcFZpZXdzUmVsYXRpb24+CjwvZGFwUmVjb3JkPgo8L2RhcFJ1Y29yZExpc3 Q+Cg==

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

<pre>Nindows PowerShell copyright (c) Microsoft Corporation. All rights reserved. P5 C:Users\tashhan/Desktop&gt; certufil =encode dap.xml tmp.b64 ; findstr /v /c:= tmp.b64 &gt; dap.b64 Input Length = 733 Output Length = 733 Output Length = 735 C:Users\tashhan/Desktop&gt; P5 C:Users\tashhan/Desktop&gt; P5 C:Users\tashhan/Desktop&gt; P5 C:Users\tashhan/Desktop&gt; P5 C:Users\tashhan/Desktop&gt; P094bWwgdmVyc21vbj0HS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5KYWxvbmU9 Inllcy1/Pgo8Z6FwUmvjb31kTGlzd04PCR6RhcF21V29yZ04KPGRhcE5hbWU-6jx2 YWk1ZTSShaNjb2wdmEskUWL6jwvZErWTmFtZ14KPGRhcF2DxZdzUmVsYXRpb24+ C;kzYWk1ZTShbmQBL3ZhbHV1Pgo8L2RhcF2DzZdzUmVsYXRpb24+c;kxYXBCYXNp Y12pZxc+jkxYRB7bw/JY3Rb24C+jkxYRB02kw73k+c;jxXWXIZTSfvKRja2Lh bnk8L3ZhbHV1Pgo8L2RhcF8b4Glj=T4KPGF0dHI+c;xuVM11PmFhYS5jaXhjby51 czVybmFtZTwvbmftZ14KPHZhbHV1PmNpc2NvPC92YWk1ZT4KPC9hdHkyPgo8L2Rh cFhl6Gvj6Glw5GeWmsY12pZxc-c;wvZGFwUmvjb3JkPgo8ZGFwUmvj Y3B1kPgo8ZGFwUmc72ltvWSDFQ2VWk1ZT4KPC9hdHkyPgo8L2Rh cFhl6Gvj6Glw9BeUPgo8dHiwZT5jYXNlbCVzczwdHlwZT4KPC9hdHkyPgo8 bmftZTShVWEuY21tvZ8udXNlcm5hbWU-6;xzWwk1ZT6SFbWWU-6;kx YXWBaWV3c11bCF0aH9uPgo8dFr5dWu-YWSkPC92YWk1ZT4KPC9kYXBMW3c111 bGF0aH9uPgo8dErsdWu-YWSkPC92YWk1ZT4KPC9kYXBMW3c111 bGF0aH9uPgo8dErsdWu-YBSCFGrWUC9zCWx1ZT6BZCHwUG928MWS Pgo8dmFsdWU-bWF0Y2trWSFC92YWk1ZT4KPC9kYXBQ2kpY3k-c;jxkVZHM1 ZT4KF0SMzHv21tvZ8udXNlcm5hbWUCjx2WkX1ZT6KPC92YWk1Z T4KF0SMzHWEyz21vZ8udXNlcm5hbWUCjx2WkX1ZT6KPC92YWk1Z T4KF0SMzHWEyz21vZ8udXNlcm5hbWUCjx2WkX1ZT6ZCHUG92xWk1 ZT4KF0SMzHWEyz21vZ8udXNlcm5hbWUCjx2WkX2C+XypY1ZpZxc+cjwzGFw Umvjb3JkPgo8L2RhcFJ1V29yZExpc3Q+cg=</pre>	Windows PowerShell	_	×
Image: Antipage: Control of the second se	<pre>Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved. PS C:\Users\tazkhan\Desktop PS C:\Users\tazkhan\Desktop&gt; certutil -encode dap.xml tmp.b64 ; findstr /v /c:- tmp.b64 &gt; dap.b64 Input Length = 793 Output Length = 1150 CertUtil: -encode command completed successfully. PS C:\Users\tazkhan\Desktop&gt;</pre>		
	<pre>Pierce And And And And And And And And And And</pre>		

Volg dezelfde procedure voor data.xml.

Stap 4. Start de API-verkenner van de FTD op een browser.

### Navigeren in naar https://<FTD Management IP>/API-verkenner

Dit bevat de volledige lijst van API's die op de FTD beschikbaar is. Het is verdeeld op basis van de hoofdfunctie met meerdere GET/POST/PUT/DELETE verzoeken die door de FDM worden ondersteund.

DAPXml en HostScanPackageFile worden gebruikt voor API.

← → C ▲ Not Secure   10.197.224.	.82/#/api-explorer	🖈 😊 🖶 🍳 🛃 🏇 🛞 Updat
Firepower Device Manage	er Monitoring Policies Objects Device: firepower	S₂ (a)
FTD REST API 🔶 D/	APXml	Show/Hide   List Operations   Expand Operations
ADI Evolorer	GET /object/dapxml	Get the DAPXml configured
P	vosr /object/dapxml	Create a new DAPXml configuration
Error Catalog	/object/dapxml/{objid}	Delete the DAPXml configuration
	GET /object/dapxml/{objld}	Get the DAPXml configured
	vut /object/dapxml/{objid}	Update the DAPXml configuration

Stap 5. Voeg een Postmanverzameling toe voor DAP.

Geef een naam op voor de verzameling. Klik op Maken, zoals in deze afbeelding wordt getoond.

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
--------	--------

**Stap 6.** Een nieuw verzoek toevoegen **Auth** om een loginlogPOST-aanvraag bij de FTD te maken om de token te hebben voor het autoriseren van POST/GET/PUT-aanvragen. Klik op **Opslaan**.