部署ASA DAP以確定AnyConnect的MAC地址

目錄
必要條件
<u>採用元件</u>
<u>背景資訊</u>
網路圖表
<u>ASA中的配置</u>
ASDM中的配置
<u>驗證</u>
案例1.僅匹配一個DAP
<u>案例2.預設DAP匹配</u>
<u>案例3.匹配多個DAP(操作:繼續)</u>
<u>案例4.匹配多個DAP(Action:Terminate)</u>
一般疑難排解
相關資訊

簡介

本文檔介紹如何透過ASDM配置動態訪問策略(DAP),以檢查用於AnyConnect連線的裝置的Mac地 址。

必要條件

需求

思科建議您瞭解以下主題: Cisco Anyconnect和Hostscan的配置

採用元件

本文中的資訊係根據以下軟體和硬體版本: ASAv 9.18 (4) ASDM 7.20 (1) Anyconnect 4.10.07073 Hostscan 4.10.07073 Windows 10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設

)的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

HostScan是一個軟體模組,可為AnyConnect安全移動客戶端提供在網路上實施安全策略的能力。 在Hostscan過程中,將收集有關客戶端裝置的各種詳細資訊並報告回自適應安全裝置(ASA)。這些 詳細資訊包括裝置作業系統、防病毒軟體、防火牆軟體、MAC地址等。動態訪問策略(DAP)功能允 許網路管理員基於每個使用者配置安全策略,DAP中的endpoint.device.MAC屬性可用於根據預定義 策略匹配或檢查客戶端裝置的MAC地址。

設定

網路圖表

下圖顯示本文檔示例中使用的拓撲。



圖表

ASA中的配置

這是ASA CLI中的最小配置。

tunnel-group dap_test_tg type remote-access tunnel-group dap_test_tg general-attributes default-group-policy dap_test_gp tunnel-group dap_test_tg webvpn-attributes group-alias dap_test enable

group-policy dap_test_gp internal group-policy dap_test_gp attributes vpn-tunnel-protocol ssl-client address-pools value ac_pool webvpn anyconnect keep-installer installed always-on-vpn profile-setting ip local pool ac_pool 172.16.1.11-172.16.1.20 mask 255.255.255.0

webvpn enable outside hostscan image disk0:/hostscan_4.10.07073-k9.pkg hostscan enable anyconnect image disk0:/anyconnect-win-4.10.07073-webdeploy-k9.pkg 1 anyconnect enable tunnel-group-list enable

ASDM中的配置

本節介紹如何在ASDM中配置DAP記錄。在本示例中,設定3個使用endpoint.device.MAC屬性作為 條件的DAP記錄。

·01_dap_test : endpoint.device.MAC=0050.5698.e608

- ·02_dap_test:endpoint.device.MAC=0050.5698.e605 = Anyconnect終端的MAC
- ·03_dap_test : endpoint.device.MAC=0050.5698.e609
- 1. 配置名為01_dap_test的第一個DAP。

導航到配置 > 遠端接入VPN > 網路(客戶端)接入 > 動態接入策略。點選Add,然後設定策略名稱 、AAA屬性、終端屬性、操作、使用者消息,如圖所示:

					ACL Priority:	D
ection Criteria efine the AAA and end elow and every endpo	dpoint attributes use int attribute has bee	ed to select this a en satisfied. The	access policy. A policy ese attributes can be o	y is used when a user's created using the tables	authorization attributes matc s below and/or by expanding	h the AAA attribute criteria the Advanced option to
ecify the logical expre Iser has ALL of the fol	ession text. llowing AAA Attribute	es values	$\overline{}$	and the following er	ndpoint attributes are satisfie	d.
AAA Attribute	Operation/V	alue	Add	Endpoint ID	Name/Operation/Value	Add
isco.grouppolicy	= dap_tes	st_gp	Edit	device	MAC["0050.5698.e608"] = true Edit
			Delete			Delete
						Logical Op.
Advanced	cy Attributes					
Advanced ess/Authorization Poli onfigure access/autho oup-policy hierarchy. Nat are not specified in Port Eorwardin	cy Attributes vization attributes fo The resulting VPN au DAP).	or this policy. At uthorization polic	tribute values specific cy is an aggregation o	ed here will override the of DAP attributes, AAA Secure Client	ose values obtained from the attributes, and group-policy l	AAA system and the hierarchy attributes (those
Advanced ess/Authorization Poli onfigure access/autho roup-policy hierarchy. nat are not specified in Port Forwardin Action	cy Attributes rization attributes fo The resulting VPN au n DAP). g Lists Bi Network AC	or this policy. At uthorization poli ookmarks CL Filters (client)	tribute values specifie cy is an aggregation o Access Method	ed here will override the of DAP attributes, AAA Secure Client Webtype AC	ose values obtained from the attributes, and group-policy l t Secure Clien CL Filters (dientless)	AAA system and the hierarchy attributes (those t Custom Attributes Functions
Advanced ess/Authorization Poli onfigure access/author oup-policy hierarchy. Iat are not specified in Port Forwardin Action Action Specify the message User Message:	cy Attributes rization attributes fo The resulting VPN an DAP). g Lists Ba Network AC e Quarantine that will be displaye dap_test	or this policy. At uthorization polic ookmarks 2. Filters (client)	tribute values specific cy is an aggregation of Access Method : • ord is selected.	ed here will override tho of DAP attributes, AAA Secure Client Webtype AC	ose values obtained from the attributes, and group-policy l t Secure Clien CL Filters (clientless)	AAA system and the hierarchy attributes (those t Custom Attributes Functions

配置第一個DAP

配置AAA屬性的組策略。

둴 Add AAA Attribute	2	×
AAA Attribute Type: Cisco		~
Group Policy:	= V dap_test_gp	\sim
Assigned IPv4 Address:	= ~	
Assigned IPv6 Address:	= ~	
Connection Profile:	= V DefaultRAGroup	\sim
Username:	= ~	
Username2:	= ~	
SCEP Required:	= 🗸 true	\sim
	OK Cancel Help	

配置DAP記錄的組策略

為終端屬性配置MAC地址。

Edit Endpoint Attribute		×
Endpoint Attribute Type: Device	= ~	
MAC Address:	- ~	0050.5698.e608
BIOS Serial Number:	= ~	
Port Number (Legacy Attribute):	= ~	
TCP/UDP Port Number:	= ~	TCP (IPv4) V
Privacy Protection:	= ~	None (equivalent to Host Scan only) $ \smallsetminus $
HostScan Version:	= ~	
Version of Endpoint Assessment (OPSWAT):	= ~	
ок са	ncel	Help

配置DAP的MAC條件

2. 配置名為02_dap_test的第二個DAP。

iption:					ACL Priority:	0
ction Criteria						
fine the AAA and end low and every endpoi ecify the logical expre	lpoint attribute int attribute ha ession text.	s used to select th s been satisfied. T	is access policy. A policy hese attributes can be c	r is used when a user's created using the tables	authorization attributes ma s below and/or by expandin	tch the AAA attribute criteria og the Advanced option to
ser has ANY of the fo	llowing AAA At	tributes values	\sim	and the following er	ndpoint attributes are satisf	fied.
AA Attribute	Operat	ion/Value	Add	Endpoint ID	Name/Operation/Valu	Je Add
sco.grouppolicy	= da	p_test_gp	Edit	device	MAC["0050.5698.e60	5"] = true Edit
			Delete			Delete
						Logical Op
Advanced ess/Authorization Polic	cy Attributes -	ter for this action		d l		
Advanced ess/Authorization Polic onfigure access/autho oup-policy hierarchy. at are not specified in	cy Attributes — rization attribu The resulting V DAP).	tes for this policy. PN authorization p	Attribute values specifie olicy is an aggregation o	d here will override the	ose values obtained from th attributes, and group-polic	e AAA system and the y hierarchy attributes (those
Advanced ess/Authorization Polic onfigure access/autho oup-policy hierarchy. at are not specified in Port Forwarding Action	cy Attributes rization attribu The resulting V DAP). g Lists Netwo	tes for this policy. PN authorization p Bookmarks rk ACL Filters (clier	Attribute values specifie olicy is an aggregation o Access Method nt)	d here will override the f DAP attributes, AAA Secure Client Webtype AC	ose values obtained from th attributes, and group-polic : Secure Clie 1. Filters (clientless)	e AAA system and the y hierarchy attributes (those ent Custom Attributes Functions
Advanced ess/Authorization Polix onfigure access/autho oup-policy hierarchy. at are not specified in Port Forwarding Action Action: O Continue Specify the message User Message:	cy Attributes	tes for this policy. PN authorization p Bookmarks rk ACL Filters (clier tine O Termina played when this re	Attribute values specifie olicy is an aggregation of Access Method nt) the (1) ecord is selected.	d here will override the f DAP attributes, AAA Secure Client Webtype AC	ose values obtained from th attributes, and group-polic : Secure Clie L Filters (dientless)	e AAA system and the y hierarchy attributes (those ent Custom Attributes Functions

配置第二個DAP

3. 配置名為03_dap_test的第三個DAP。

iption:					ACL Priority:	0
tion Criteria fine the AAA and er low and every endp	idpoint attribute oint attribute ha	s used to select this s been satisfied. The	access policy. A policy se attributes can be o	y is used when a user's created using the table	authorization attributes mate s below and/or by expanding	ch the AAA attribute criteria the Advanced option to
ser has ANY of the f	ollowing AAA At	tributes values	\sim	and the following e	endpoint attributes are satisfie	ed.
AA Attribute	Operat	tion/Value	Add	Endpoint ID	Name/Operation/Value	Add
sco.grouppolicy	= da	p_test_gp	Edit	device	MAC["0050.5698.e609	"] = true Edit
			Delete			Delete
Advanced ess/Authorization Po onfigure access/auth oup-policy hierarchy	licy Attributes – orization attribu . The resulting \	tes for this policy. At PN authorization poli	tribute values specific cy is an aggregation of	ed here will override th	lose values obtained from the A attributes, and group-policy	Logical Op AAA system and the hierarchy attributes (those
Advanced ess/Authorization Po onfigure access/auth oup-policy hierarchy at are not specified i	licy Attributes – orization attribu . The resulting V n DAP).	tes for this policy. At PN authorization poli	tribute values specific cy is an aggregation of	ed here will override th of DAP attributes, AAA	ose values obtained from the attributes, and group-policy	AAA system and the hierarchy attributes (those
Advanced ess/Authorization Po nifgure access/auth oup-policy hierarchy at are not specified i Port Forwardir Action	licy Attributes – orization attribu . The resulting V n DAP). ng Lists Netwo	tes for this policy. At PN authorization poli Bookmarks rk ACL Filters (client)	tribute values specific cy is an aggregation of Access Method	ed here will override th of DAP attributes, AAA Secure Clien Webtype Ad	ose values obtained from the A attributes, and group-policy It Secure Clier CL Filters (clientless)	AAA system and the hierarchy attributes (those it Custom Attributes Functions
Advanced ess/Authorization Po infigure access/auth oup-policy hierarchy at are not specified i Port Forwardir Action Action Specify the messag User Message:	licy Attributes – orization attribu . The resulting V n DAP). ng Lists Netwo ue Quarar e that will be dis dap_test	tes for this policy. At PN authorization poli Bookmarks rk ACL Filters (client) Itine Terminate played when this reco	tribute values specific cy is an aggregation of Access Method	ed here will override th of DAP attributes, AAA Secure Clien Webtype Ad	ose values obtained from the a attributes, and group-policy it Secure Clier CL Filters (clientless)	AAA system and the hierarchy attributes (those at Custom Attributes Functions

配置第三個DAP

4. 使用 more flash:/dap.xml 命令確認dap.xml中DAP記錄的設定。

在ASDM上設定的DAP記錄的詳細資訊儲存在ASA快閃記憶體中的dap.xml中。完成這些設定後,會在dap.xml中產生三個DAP記錄。 您可以在dap.xml中確認每個DAP記錄的詳細資訊。



注意:匹配的DAP的順序是dap.xml中的顯示順序。 預設的DAP (DfltAccessPolicy)是最後相符的專案。

<#root>

ciscoasa#

more flash:/dap.xml

<dapRecordList> <dapRecord> <dapName> <value>

01_dap_test

</value> <--- 1st DAP name </dapName> <dapViewsRelation> <value>and</value> </dapViewsRelation> <dapBas

dap_test_gp

< 1st DAP group policy <operation>EQ</operation> <type>caseless</type>
endpoint.device.MAC["0050.5698.e608"]
< 1st DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</operation>
02_dap_test
< 2nd DAP name <dapviewsrelation> <value>and</value> </dapviewsrelation> <dapbas< td=""></dapbas<>
dap_test_gp
< 2nd DAP group policy <operation>EQ</operation> <type>caseless</type>
endpoint.device.MAC["0050.5698.e605"]
< 2nd DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</operation>
03_dap_test
< 3rd DAP name <dapviewsrelation> <value>and</value> </dapviewsrelation> <dapbas< td=""></dapbas<>
dap_test_gp
< 3rd DAP group policy <operation>EQ</operation> <type>caseless</type>
endpoint.device.MAC["0050.5698.e609"]
<pre> < 3rd DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</operation></pre>

驗證

案例1.僅匹配一個DAP

1. 確保終端的MAC為0050.5698.e605,這與02_dap_test中的MAC條件匹配。

2.在終端上,運行Anyconnect連線並輸入使用者名稱和密碼。

🕥 Cisco	o AnyConne	ct 192.168.1.1	×
	Please enter	your username and password.	
_	Group:	dap_test ~	
	Username:	cisco	
	Password:	****	
		OK Cancel	
S Cisco	o AnyConne	ct Secure Mobility Client —	
	Plea 193	: se enter your username and password. 2.168.1.1 ~	Connect

輸入使用者名稱和密碼

3.在Anyconnect UI中,確認02_dap_test匹配。

Cisco AnyConnect	×				
Security policies were applied to your session, access to some resources may be blocked. Your system administrator provided the following		S Cisco AnyConnect Secure Mobility Client	-		×
information to help you understand and remedy the security conditions: 02_dap_test		Connected to 192.168.1.1. 192.168.1.1		Disconnec	t
ОК		00:00:13	1		IPv4

在UI中確認使用者訊息

4.在ASA系統日誌中,確認02_dap_test匹配。



注意:確保在ASA中啟用了debug dap trace。

<#root>

Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

0050.5698.e605

"] = "true"

Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001:

Selected DAPs

02_dap_test

Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Dec 30 2023 11:46:11: %ASA-4-711001: dap_process_selec selected 1 records

```
Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001:
```

案例2.預設DAP匹配

1.將02_dap_test中的endpoint.device.MAC值更改為與終端的MAC不匹配的0050.5698.e607。

2.在終端上,運行Anyconnect連線並輸入使用者名稱和密碼。

3. 確認Anyconnect連線被拒絕。

Cisco AnyConnect X	
Login denied. default	
ОК	
S Cisco AnyConnect Secure Mobility Client -	
VPN: Ready to connect. 192.168.1.1	Connect

在UI中確認使用者訊息

4. 在ASA syslog中,確認DfltAccessPolicy匹配。



注意:預設情況下,DfltAccessPolicy的操作為Terminate。

<#root>

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

"] = "true"

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 12:13:39: %ASA-4-711001: S Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Dec 30 2023 12:13:39: %ASA-4-711001: dap_process_select

selected 0 records

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 12:13:39: %ASA-4-711001:

Selected DAPs

:

DfltAccessPolicy

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 12:13:39: %ASA-4-711001: D

案例3.匹配多個DAP(操作:繼續)

1. 變更每個DAP中的作業與屬性。

·01_dap_test : dapSelection (MAC地址) = endpoint.device.MAC[0050.5698.e605] = Anyconnect終端的MAC 操作=繼續

 $\cdot 02_dap_test$:

dapSelection (主機名) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnect終端的主機名 操作=繼續 · 刪除03_dap_test DAP記錄

2. 在終端上,運行Anyconnect連線並輸入使用者名稱和密碼。

3. 在Anyconnect UI中,確認所有2個DAP都匹配



注意:如果連線與多個DAP匹配,則多個DAP的使用者消息將整合在一起並顯示在Anyconnect UI中。

Cisco AnyConnect	×						
Security policies were applied to your session, access to some resources may be blocked. Your system administrator provided the following information to help you understand and remedy the security conditions:		🕙 Cisco AnyCo	onnect Secure Mobility Client	_			×
01_dap_test 02_dap_test		ſ	VPN: Connected to 192.168.1.1.	~		Disconnect	
ОК		00:01:14			1	P	∿4

在UI中確認使用者訊息

4. 在ASA syslog中,確認所有2個DAP都匹配。

<#root>

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

0050.5698.e605

"] = "true" Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4-711001: endpoint.device.ho

DESKTOP-VCKHRG1

...

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:49:02: %ASA-4-711001: S

02_dap_test

,

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4-711001: dap_process_select

selected 2 records

```
Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:49:02: %ASA-4-711001: D
```

案例4.匹配多個DAP (Action : Terminate)

1. 變更01_dap_test的作業。

 ·01_dap_test : dapSelection (MAC地址) = endpoint.device.MAC[0050.5698.e605] = Anyconnect終端的MAC 操作=終止
·02_dap_test : dapSelection (主機名) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnect終端的主機名 操作=繼續

2. 在終端上,運行Anyconnect連線並輸入使用者名稱和密碼。

3. 在Anyconnect UI中,確認僅匹配01_dap_test。



註:一個連線與已設定為終止操作的DAP記錄匹配。終止操作後不再匹配後續記錄。



4. 在ASA syslog中,確認僅匹配01_dap_test。

<#root>

Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

0050.5698.e605

"] = "true"

Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.ho

DESKTOP-VCKHRG1

" Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:55:37: %ASA-4-711001:

01_dap_test

Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: dap_process_selec

selected 1 records

Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:55:37: %ASA-4-711001:

一般疑難排解

這些調試日誌可幫助您確認DAP在ASA中的詳細行為。

debug dap trace

debug dap trace errors

<#root>

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["0050.5698.e605"] = "true" Feb

Selected DAPs

: ,01_dap_test,02_dap_test Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4

相關資訊

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/108000-dap-deploy-guide.html#toc-hId-981572249

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。