部署ASA DAP以识别AnyConnect的MAC地址

日求	
<u>先决条件</u>	
<u>要求</u>	
使用的组件	
<u>背景信息</u>	
<u>网络图</u>	
<u>ASA中的配置</u>	
<u>ASDM中的配置</u>	
<u>验证</u>	
场景1.仅匹配一个DAP	
<u>场景2.默认DAP匹配</u>	
<u>场景3.匹配多个DAP(操作:继续)</u>	
<u>场景4.多个DAP (Action :Terminate)匹配</u>	
<u>一般故障排除</u>	
相关信息	

简介

- -

本文档介绍如何通过ASDM配置动态访问策略(DAP),以检查用于AnyConnect连接的设备的Mac地 址。

先决条件

要求

Cisco 建议您了解以下主题: Cisco Anyconnect和Hostscan的配置

使用的组件

本文档中的信息基于以下软件和硬件版本: ASAv 9.18 (4) ASDM 7.20 (1) Anyconnect 4.10.07073 Hostscan 4.10.07073 Windows 10

本文档中的信息都是基于特定实验室环境中的设备编写的。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,请确保您了解所有命令的潜在影响。

背景信息

HostScan是一个软件模块,可让AnyConnect安全移动客户端在网络上实施安全策略。在 Hostscan过程中,将收集有关客户端设备的各种详细信息并向自适应安全设备(ASA)进行报告。这 些详细信息包括设备操作系统、防病毒软件、防火墙软件、MAC地址等。动态访问策略(DAP)功能 允许网络管理员基于每个用户配置安全策略,DAP中的endpoint.device.MAC属性可用于根据预定义 策略匹配或检查客户端设备的MAC地址。

配置

网络图

下图显示本文档示例中使用的拓扑。



图解

ASA中的配置

这是ASA CLI中的最低配置。

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

本节介绍如何在ASDM中配置DAP记录。在本示例中,设置3个使用endpoint.device.MAC属性作为 条件的DAP记录。

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

·02_dap_test:endpoint.device.MAC=0050.5698.e605 = Anyconnect终端的MAC

·03_dap_test : endpoint.device.MAC=0050.5698.e609

1. 配置名为01_dap_test的第一个DAP。

导航到配置 > 远程接入VPN > 网络(客户端)接入 > 动态接入策略。点击Add,然后设置Policy Name、AAA Attribute、endpoint attributes、Action、User Message,如图所示:

ription:				ACL Priority: 0	
ection Criteria efine the AAA and end elow and every endpoi	point attributes used to select nt attribute has been satisfied.	this access policy. A polic These attributes can be	y is used when a user's a created using the tables	authorization attributes match below and/or by expanding th	the AAA attribute criteria ne Advanced option to
Jser has ALL of the foll	owing AAA Attributes values	\sim	and the following en	dpoint attributes are satisfied.	
AAA Attribute	Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
isco.grouppolicy	= dap_test_gp	Edit	device	MAC["0050.5698.e608"]	= true Edit
		Delete			Delete
					Logical Op.
Advanced	ry Attributes			an unit of a fact that A	:
Advanced ess/Authorization Polic onfigure access/author roup-policy hierarchy. at are not specified in Dest Ecouverdian	y Attributes ization attributes for this policy The resulting VPN authorization DAP).	/. Attribute values specific policy is an aggregation of	ed here will override those of DAP attributes, AAA a	se values obtained from the A attributes, and group-policy his	AA system and the erarchy attributes (those
Advanced ess/Authorization Polic onfigure access/author oup-policy hierarchy. at are not specified in Port Forwarding Action	y Attributes ization attributes for this policy The resulting VPN authorization DAP). Lists Bookmarks Network ACL Filters (di	y. Attribute values specific policy is an aggregation Access Method ent)	ed here will override thos of DAP attributes, AAA a Secure Client Webtype ACL	se values obtained from the A attributes, and group-policy hi Secure Client (Filters (clientless)	AA system and the erarchy attributes (those Custom Attributes Functions
Advanced ess/Authorization Polic onfigure access/author roup-policy hierarchy. Iat are not specified in Port Forwarding Action Action: O Continue Specify the message User Message:	y Attributes ization attributes for this policy The resulting VPN authorization DAP). Lists Bookmarks Network ACL Filters (di Quarantine Termi that will be displayed when this ap_test	y. Attribute values specifi policy is an aggregation of Access Method ent) nate record is selected.	ed here will override thos of DAP attributes, AAA a Secure Client Webtype ACL	se values obtained from the A attributes, and group-policy hie Secure Client (Filters (clientless)	AA system and the erarchy attributes (those Custom Attributes Functions
Advanced ess/Authorization Polic onfigure access/authon roup-policy hierarchy. at are not specified in Port Forwarding Action Action: O Continue Specify the message User Message:	y Attributes ization attributes for this policy The resulting VPN authorization DAP). Lists Bookmarks Network ACL Filters (di Quarantine Termi that will be displayed when this ap_test	 Attribute values specific policy is an aggregation of Access Method ent) nate () record is selected. 	ed here will override thos of DAP attributes, AAA a Secure Client Webtype ACL	se values obtained from the A attributes, and group-policy his Secure Client (Filters (clientless)	AA system and the erarchy attributes (those Custom Attributes Functions

配置第一个DAP

配置AAA属性的组策略。

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记录的组策略

为终端属性配置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条件

2. 配置第二个名为02_dap_test的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 h		
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

配置第二个DAP

3. 配置名为03_dap_test的第三个DAP。

ection Criteria efine the AAA and en elow and every endpo	dpoint attributes used to select this bint attribute has been satisfied. Th	s access policy. A policy lese attributes can be c	is used when a user's a reated using the tables	authorization attributes match th below and/or by expanding the	e AAA attribute criteria Advanced option to
ecify the logical expr	ession text. ollowing AAA Attributes values	~	and the following en	dpoint attributes are satisfied.	
AAA Attribute	Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
sco.grouppolicy	= dap_test_gp	Edit	device	MAC["0050.5698.e609"] =	true Edit
		Delete			Delete
					Logical Op.
ess/Authorization Pol onfigure access/author oup-policy hierarchy.	icy Attributes orization attributes for this policy. A The resulting VPN authorization po	Attribute values specifie Nicy is an aggregation o	d here will override tho f DAP attributes, AAA a	se values obtained from the AAA attributes, and group-policy hiera	system and the archy attributes (those
ess/Authorization Pol onfigure access/autho oup-policy hierarchy, at are not specified in Port Enruradio	icy Attributes orization attributes for this policy. A The resulting VPN authorization po n DAP).	Attribute values specifie licy is an aggregation o	d here will override tho f DAP attributes, AAA a	se values obtained from the AAA attributes, and group-policy hiera	a system and the archy attributes (those
ess/Authorization Pol onfigure access/autho oup-policy hierarchy, at are not specified ir Port Forwardin Action	icy Attributes orization attributes for this policy. A The resulting VPN authorization po n DAP). g Lists Bookmarks Network ACL Filters (client	Attribute values specifie dicy is an aggregation o Access Method t)	d here will override tho f DAP attributes, AAA a Secure Client Webtype ACI	se values obtained from the AAA attributes, and group-policy hiera Secure Client Cu Filters (clientless)	system and the archy attributes (those stom Attributes Functions

配置第三个DAP

4. 使用 more flash:/dap.xml 命令确认dap.xml中DAP记录的设置。

在ASDM上设置的DAP记录的详细信息以dap.xml形式保存在ASA闪存中。完成这些设置后,将以dap.xml形式生成三个DAP记录。您可以在dap.xml中确认每个DAP记录的详细信息。



注意:DAP的匹配顺序是dap.xml中的显示顺序。 最后匹配默认DAP (DfltAccessPolicy)。

<#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>

验证

场景1.仅匹配一个DAP

1. 确保终端的MAC地址为0050.5698.e605,这与02_dap_test中的MAC条件匹配。

2.在终端上,运行Anyconnect连接并输入用户名和密码。

🕙 Cisco	o AnyConne	ct 192.168.1.1 ×	
	Please enter	your username and password.	
_	Group:	dap_test ~	
	Username:	cisco	
	Password:	*****	
		OK Cancel	
S Cisc	o AnyConne	ct Secure Mobility Client — 🔲 🖸	×
	Plea 192	enter your username and password. 2.168.1.1 Connect	

输入用户名和密码

3.在Anyconnect UI中,确认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		VPII: Connected to 192.168.1.1. 192.168.1.1	D	isconnect	
ОК		00:00:13		I	Pv4

在UI中确认用户消息

4.在ASA syslog中,确认02_dap_test匹配。



注意:确保在ASA中启用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:

场景2.默认DAP匹配

1.将02_dap_test中的endpoint.device.MAC值更改为不匹配终端的MAC的0050.5698.e607。

2.在终端上,运行Anyconnect连接并输入用户名和密码。

3. 确认Anyconnect连接被拒绝。

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

在UI中确认用户消息

4. 在ASA syslog中,确认DfltAccessPolicy匹配。



注意:默认情况下,DfltAccessPolicy的操作为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

场景3.匹配多个DAP(操作:继续)

1. 更改每个DAP中的操作和属性。

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

 $\cdot 02_dap_test$:

dapSelection (主机名) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnect终端的主机名 操作=继续 ·删除03_dap_test DAP记录

2. 在终端上,运行Anyconnect连接并输入用户名和密码。

3. 在Anyconnect UI中,确认所有2个DAP都匹配



注意:如果连接匹配多个DAP,则多个DAP的用户消息将集成并一起显示在Anyconnect UI中。

Cisco AnyConnect	×
Security policies were applied to your session, access to some resource may be blocked. Your system administrator provided the following information to help you understand and remedy the security conditions:	🕙 Cisco AnyConnect Secure Mobility Client — 🗆 🗙
01_dap_test 02_dap_test	VPI: Connected to 192.168.1.1. 192.168.1.1 V Disconnect
OK	00:01:14 IPv4

在UI中确认用户消息

4. 在ASA syslog中,确认所有2个DAP均匹配。

<#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

01_dap_test

02_dap_test

,

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

场景4.多个DAP (Action: Terminate)匹配

1. 更改01_dap_test的操作。

 ·01_dap_test: dapSelection (MAC地址) = endpoint.device.MAC[0050.5698.e605] = Anyconnect终端的MAC 操作=终止
 ·02_dap_test: dapSelection (主机名) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnect终端的主机名 操作=继续

2. 在终端上,运行Anyconnect连接并输入用户名和密码。

3. 在Anyconnect UI中,确认仅匹配01_dap_test。



注意:连接与已设置为终止操作的DAP记录匹配。终止操作后不再匹配后续记录。



4. 在ASA syslog中,确认仅匹配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:

一般故障排除

这些调试日志可帮助您确认ASA中DAP的详细行为。

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

相关信息

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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。