在ISE 2.2上配置異常端點檢測和實施

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>設定</u> <u>網創態</u> <u>步驟1.啟用異常檢測。</u> <u>步驟2.配置授權策略。</u> <u>驗證</u> <u>疑難排解</u> <u>相關資訊</u>

簡介

本文檔介紹異常端點檢測和實施。這是思科身份服務引擎(ISE)中引入的新分析功能,用於增強網路 可視性。

必要條件

需求

思科建議您瞭解以下主題:

- 交換器上的有線MAC驗證略過(MAB)組態
- •無線LAN控制器(WLC)上的無線MAB組態
- •兩台裝置上的授權(CoA)組態變更

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 1. 身分識別服務引擎2.2
- 2. 無線LAN控制器8.0.100.0
- 3. Cisco Catalyst交換器3750 15.2(3)E2
- 4. 帶有線和無線介面卡的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。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

背景資訊

異常端點檢測功能允許ISE監控對連線端點的特定屬性和配置檔案的更改。如果更改匹配一個或多 個預配置的異常行為規則,ISE會將終端標籤為異常。檢測到後,ISE可以採取行動(使用CoA)並 實施某些策略以限制對可疑端點的訪問。 此功能的一個使用案例包括檢測MAC地址欺騙。

• 附註:此功能不會處理MAC地址欺騙的所有可能情況。請務必閱讀此功能所涵蓋的異常型別,以確定其是否適用於您的使用案例。

啟用檢測後,ISE會監控收到的現有終端的任何新資訊,並檢查這些屬性是否已更改:

- NAS-Port-Type 確定此端點的訪問方法是否已更改。例如,如果通過有線Dot1x連線的同一 MAC地址用於無線Dot1x,反之亦然。
- 2. DHCP類ID -確定端點的客戶端/供應商型別是否已更改。僅當使用特定值填充DHCP類ID屬性 並將其更改為其他值時才適用。如果終端配置了靜態IP,則不會在ISE上填充DHCP類ID屬性 。稍後,如果另一台裝置偽裝MAC地址並使用DHCP,則類ID將從空值變為特定字串。這不會 觸發Anomouls行為檢測。

3. 終端策略 — 終端配置檔案從印表機或IP電話更改為工作站。

一旦ISE檢測到上述更改之一,AnomalyBehavior屬性將新增到終端並設定為True。稍後可以將此作 為授權策略中的條件使用,以限制終端在將來身份驗證中的訪問。

如果配置了Enforcement,ISE可以在檢測到更改後傳送CoA以重新驗證或執行終端埠彈回。如果有效,它可以隔離異常終端,具體取決於配置的授權策略。

設定

網路圖表



組態

在交換器和WLC上執行簡單的MAB和AAA設定。要使用此功能,請執行以下步驟:

步驟1.啟用異常檢測。

導航到管理>系統>設定>分析。

Profile	r Configuration		
	* СоА Туре:	Reauth	
	Current custom SNMP community strings:	•••••	Show
	Change custom SNMP community strings:		(For NMAP, comma separated. Field will be cleared on successful saved change.)
Confir	n changed custom SNMP community strings:		(For NMAP, comma separated. Field will be cleared on successful saved change.)
	EndPoint Attribute Filter:	Enabled (i)	
	Enable Anomalous Behaviour Detection:	Enabled 👔	
	Enable Anomalous Behaviour Enforcement:	Enabled	
Save	Reset		

第一個選項允許ISE檢測任何異常行為,但不會傳送CoA(僅可視性模式)。 第二個選項允許ISE在 檢測到異常行為後傳送CoA(實施模式)。

步驟2.配置授權策略。

將Anomlousbehavior屬性配置為授權策略中的條件,如下圖所示:

Exceptions (1)										
	Status	Rule Name Conditions (identity groups and other conditions)								
	 	Anomalous Client	if	(EndPoints:AnomalousBehaviour EQUALS true AND DEVICE:Location EQUALS All Locations)	then	DenyAccess				
Sta	indard									
	Status	Rule Name		Conditions (identity groups and other conditions)		Permissions				
	~	Normal Client	if	DEVICE:Location EQUALS All Locations	then	PermitAccess				

驗證

使用無線介面卡連線。使用命令ipconfig /all查詢無線介面卡的MAC地址,如下圖所示:

Wir	eless LAN adapter Wi-Fi:		
	Connection-specific DNS Suffix .		
	Description	:	802.11n USB Wireless LAN Card
	Physical Address		C0-4A-00-21-49-C2
	DHCP Enabled		Yes
	Autoconfiguration Enabled	:	Yes
	Link-local IPv6 Address		fe80::1c54:884a:33c0:bcf1%4(Preferred)
	IPv4 Address		192.168.1.38(Preferred)
	Subnet Mask		255.255.255.0
	Lease Obtained		Friday, December 30, 2016 5:17:12 AM
	Lease Expires		Friday, December 30, 2016 6:17:12 AM
	Default Gateway		192.168.1.1
	DHCP Server		192.168.1.1
	DHCPv6 IAID		46156288
	DHCPv6 Client DUID		00-01-00-01-1F-F3-74-5F-C0-4A-00-21-49-C2
	DNS Servers	:	fec0:0:0:ffff::1%1
			fec0:0:0:ffff::2%1
			fec0:0:0:ffff::3%1
	NetBIOS over Tcpip		Enabled

要模擬惡意使用者,您可以偽裝乙太網介面卡的MAC地址以匹配普通使用者的MAC地址。

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right. Property: IPv4 Checksum Offload Jumbo Packet Large Send Offload V2 (IPv4) Large Send Offload V2 (IPv6) Locally Administered Address Log Link State Event Maximum Number of RSS Queues Packet Priority & VLAN Receive Buffers Receive Side Scaling Speed & Duplex TCP Checksum Offload (IPv4) TCP Checksum Offload (IPv6) Transmit Buffers	eneral	Advanced	Driver	Details	Events	Power Manage	ement
Property: Value: IPv4 Checksum Offload Jumbo Packet Large Send Offload V2 (IPv4) Large Send Offload V2 (IPv6) Locally Administered Address Log Link State Event Maximum Number of RSS Queues Packet Priority & VLAN Receive Buffers Receive Side Scaling Speed & Duplex TCP Checksum Offload (IPv4) TCP Checksum Offload (IPv6) Transmit Buffers ✓	The foll he prop on the r	owing proper berty you war ight.	ties are a nt to char	vailable fo nge on the	or this net e left, and	twork adapter. Cl then select its v	lick alue
IPv4 Checksum Offload Jumbo Packet Large Send Offload V2 (IPv4) Large Send Offload V2 (IPv6) Localy Administered Address Log Link State Event Maximum Number of RSS Queues Packet Priority & VLAN Receive Buffers Receive Side Scaling Speed & Duplex TCP Checksum Offload (IPv4) TCP Checksum Offload (IPv6) Transmit Buffers ✓	roperty	y:			Va	alue:	
Jumbo Packet Large Send Offload V2 (IPv4) Large Send Offload V2 (IPv6) Locally Administered Address Log Link State Event Maximum Number of RSS Queues Packet Priority & VLAN Receive Buffers Receive Buffers Receive Side Scaling Speed & Duplex TCP Checksum Offload (IPv4) TCP Checksum Offload (IPv6) Transmit Buffers ✓	IPv4 C	hecksum Off	load	^		C04A002149C2	
Localy Administered Address Log Link State Event Maximum Number of RSS Queues Packet Priority & VLAN Receive Buffers Receive Side Scaling Speed & Duplex TCP Checksum Offload (IPv4) TCP Checksum Offload (IPv6) Transmit Buffers	Jumbo Large Large	Packet Send Offload Send Offload	V2 (IPv4 V2 (IPv6	4) 5)	ON	ot Present	
	Maxim Packe Receiv Receiv Speed TCP C TCP C TCP C Transn	IN State Even um Number o t Priority & VL ve Buffers ve Side Scalir & Duplex hecksum Offl hecksum Offl hit Buffers	nt f RSS Q AN ng load (IPv oad (IPv	4) 6)			

普通使用者連線後,您就可以看到資料庫中的終端條目。之後,惡意使用者使用偽造的MAC地址進 行連線。

V.

在報告中,您可以看到來自WLC的初始連線。之後,惡意使用者進行連線,10秒後,由於檢測到異 常客戶端,會觸發CoA。由於全域性CoA型別設定為**Reauth**,端點將嘗試再次連線。ISE已將 AnomalyBehavior屬性設定為True,因此ISE匹配第一個規則並拒絕使用者。

					• • • • • •			
	Logged	At	RADIUS St	Details	Identity	Endpoint ID	Authorization Rule	Network Device
×	Match	Altogged At	✓ of the following	ng rules.	Enter Advanced Filt	er Nam Save		-
		Loaded At	✓ Within		✓ Custom	✓ From 12/30/20:	16 8:: 🗰 To 12/30/20	16 8:38 🗰 🕇 💼 🛛 Filter
	2016-12	-30 20:37:59.728	0	0	C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Anomalous Client	SW
	2016-12	-30 20:37:59.704		0		C0:4A:00:21:49:C2		SW
	2016-12	-30 20:37:49.614	~	Q	C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	SW
	2016-12	-30 20:22:00.193	~	0	C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	WLC

如圖所示,您可以在「Context Visibility」頁籤中檢視端點下的詳細資訊:

C0:4A:00:21:49:C2	3								
MAC Address: C0:4A: Username: c04a0021 Endpoint Profile: TP- Current IP Address: 1 Location: Location =	:00:21:49:C2 149c2 LINK-Device 92.168.1.38 ▶All Locations								
Applications Attribute	Authentication	Threats	Vulnerabilities						
General Attributes									
Description									
Static Assignment false									
Endpoint Policy TP-LIN	K-Device								
Static Group Assignment false									
Identity Group Assignment Profiled									
Custom Attributes									
				▼ Filter ▼	۰.				
Attribute Name	Attribute Va	alue		🔻 Filter 👻	۰.				
Attribute Name No data found. Add custom attrib	Attribute Va	alue		▼ Filter -	0-				
Attribute Name No data found. Add custom attrib	Attribute Va outes here.	alue		▼ Filter -	٥-				
Attribute Name No data found. Add custom attrib Other Attributes	Attribute Va outes here.	alue		▼ Filter -	Q				
Attribute Name No data found. Add custom attrib Other Attributes AAA-Server	Attribute Va outes here. sth-nice	alue		▼ Filter -	0				
Attribute Name No data found. Add custom attrib Other Attributes AAA-Server AD-Last-Fetch-Time	Attribute Va outes here. sth-nice 1483130280592	alue		▼ Filter -	Q				
Attribute Name No data found. Add custom attrib Other Attributes AAA-Server AD-Last-Fetch-Time Acct-Input-Gigawords	Attribute Va outes here. sth-nice 1483130280592 0	alue		▼ Filter -	0				
Attribute Name No data found. Add custom attributes Other Attributes AAA-Server AD-Last-Fetch-Time Acct-Input-Gigawords Acct-Output-Gigawords	Attribute Va putes here. sth-nice 1483130280592 0 0	alue		▼ Filter -	0				
Attribute Name No data found. Add custom attributes Other Attributes AAA-Server AD-Last-Fetch-Time Acct-Input-Gigawords Airespace-Wlan-Id	Attribute Va putes here. sth-nice 1483130280592 0 0 3	alue		▼ Filter -	0-				
Attribute Name No data found. Add custom attrib Other Attributes AAA-Server AD-Last-Fetch-Time Acct-Input-Gigawords Airespace-Wlan-Id AilowedProtocolMatchedRule	Attribute Va putes here. sth-nice 1483130280592 0 0 3 MAB	alue		▼ Filter -	0 -				

您可以看到,可以從資料庫中刪除端點以清除此屬性。

如圖所示,控制面板包含一個新頁籤,顯示出現此行為的客戶端數量:



Filters: × Anomalous Endpoints

E	Type Profile	Ø	OUI OS Types	CATEGORIES Identity Group	0	0 9	NETWORK DEVIC	ES ⁰ Name	0 9		
	(`		C							
	homevices: [100%]		tp-li,ltd.: [100	%]			locattions: [100%]				
1 Sele	cted								Rows/Page	1 🔽 🗟 🗍	÷
c	+ 🛍 🗹 ANC -	Change Authorization - Clear	Threats & Vulnerabilities	Export - Impo	ert - MDM Actio	ons - Release R	ejected Revoke Certificat	e			
	MAC Address	Anomalous Behavior	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description	0	UI	05
×	MAC Address	true	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description		UI	0
	C0:4A:00:21:49:C2	true	192.168.1.38	c04a002149c2		Location + All	TP-LINK-Device		TF	P-LINK TECHNOLOGI	

疑難排解

要排除故障,請啟用Profiler調試,同時導航到Administration > System > Logging > Debug Log Configuration。

dentity Services Engine	Home	ations	✓Administration
▼ System → Identity Management	Network Resources Device Portal Ma	anagement pxGrid Se	ervices
Deployment Licensing + Certificat	es -Logging + Maintenance Upgr	ade Backup & Resto	ore + Admin Access + Settings
0			
Local Log Settings	Node List > sth-nice.example.com Debug Level Configuration		
Remote Logging Targets	Debug Level configuration		
Logging Categories	/ Edit CReset to Default		
Message Catalog	Component Name	Log Level	Description
Debug Log Configuration	O portal-web-action	INFO	Base Portal debug messages
	O posture	INFO	Posture debug messages
Collection Filters	O previewportal	INFO	Preview Portal debug messages
	• profiler	DEBUG 🔻	profiler debug messages
	O provisioning	INFO	Client Provisioning client debug messages Save Cancel

要查詢ISE Profiler.log檔案,請導航至**操作>下載日誌>調試日誌**,如下圖所示:

ahaha Ide	lentity Services Engine	Home	▶ Cont	ext Visibility	~ 0	perations	▶ Policy	Administration	▶ Work Centers
▶ RADIU	JS Threat-Centric NAC Live L	Logs 🕨 T	ACACS	→ Troublesh	oot	Adaptive N	Vetwork Contr	ol Reports	
▶ Diagn	ostic Tools Download Logs								

Appliance node list	Support Bundle	Debug Logs	
sth-nice			
	Debug Log Type	Log File	Description
		prrt-server.log.7	
		prrt-server.log.8	
		prrt-server.log.9	
	profiler		Profiler debug messages
		profiler.log	

這些日誌顯示**Profiling.log**檔案中的某些片段。您可以看到,ISE通過比較NAS-Port-Type屬性的舊 值和新值,檢測到MAC地址為C0:4A:00:21:49:C2的終端已更改了訪問方法。它是無線的,但已更 改為乙太網。 cisco.profiler.infrastructure.profiling.ProfilerManager -: Profiling: - Classify hierarchy C0:4A:00:21:49:C2 2016-12-30 20:37:43,874 DEBUG [MACSpoofingEventHandler-52-thread-1][] profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -: ProfilerCollection: - Received AttrsModifiedEvent in MACSpoofingEventHandler MAC: C0:4A:00:21:49:C2 2016-12-30 20:37:49,618 DEBUG [MACSpoofingEventHandler-52-thread-1][] profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -: ProfilerCollection: - Received AttrsModifiedEvent in MACSpoofingEventHandler MAC: C0:4A:00:21:49:C2 2016-12-30 20:37:49,618 INFO [MACSpoofingEventHandler-52-thread-1][] com.cisco.profiler.api.MACSpoofingManager -: ProfilerCollection: - Anomalous Behaviour Detected: C0:4A:00:21:49:C2 AttrName: NAS-Port-Type Old Value: Wireless - IEEE 802.11 New Value: Ethernet 2016-12-30 20:37:49,620 DEBUG [MACSpoofingEventHandler-52-thread-1][] cisco.profiler.infrastructure.cache.EndPointCache -: ProfilerCollection:- Updating end point: mac - C0:4A:00:21:49:C2 2016-12-30 20:37:49,621 DEBUG [MACSpoofingEventHandler-52-thread-1][] cisco.profiler.infrastructure.cache.EndPointCache -: ProfilerCollection:- Reading significant attribute from DB for end point with mac C0:4A:00:21:49:C2 2016-12-30 20:37:49,625 DEBUG [MACSpoofingEventHandler-52-thread-1][] profiler.infrastructure.probemgr.event.EndpointPersistEventHandler -: ProfilerCollection: - Adding to queue endpoint persist event for mac: C0:4A:00:21:49:C2 因此,ISE會執行操作,因為已啟用實施。此處的操作是根據上述「分析」設定中的全域性配置傳 送CoA。在我們的示例中,CoA型別設定為Reauth,這允許ISE重新驗證終端並重新檢查配置的規 則。這一次,它匹配異常客戶端規則,因此被拒絕。 2016-12-30 20:37:49,625 INFO [MACSpoofingEventHandler-52-thread-1][] profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -: ProfilerCollection:- Taking mac spoofing enforcement action for mac: C0:4A:00:21:49:C2 2016-12-30 20:37:49,625 INFO [MACSpoofingEventHandler-52-thread-1][] profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -: ProfilerCollection:- Triggering Delayed COA event. Should be triggered in 10 seconds 2016-12-30 20:37:49,625 DEBUG [CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -: ProfilerCoA:- Received CoAEvent notification for endpoint: C0:4A:00:21:49:C2 2016-12-30 20:37:49,625 DEBUG [CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -: ProfilerCoA:- Configured Global CoA command type = Reauth 2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -: ProfilerCoA:- Received FirstTimeProfileCoAEvent for endpoint: C0:4A:00:21:49:C2 2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -: ProfilerCoA:- Wait for endpoint: C0:4A:00:21:49:C2 to update - TTL: 1 2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -: ProfilerCoA:- Setting timer for endpoint: C0:4A:00:21:49:C2 to: 10 [sec] 2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -: ProfilerCoA:- Rescheduled event for endpoint: C0:4A:00:21:49:C2 to retry - next TTL: 0 2016-12-30 20:37:59,644 DEBUG [CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -: ProfilerCoA:- About to call CoA for nad IP: 10.62.148.106 for endpoint: C0:4A:00:21:49:C2 CoA Command: Reauth 2016-12-30 20:37:59,645 DEBUG [CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -: ProfilerCoA:- Applying CoA-REAUTH by AAA Server: 10.48.26.89 via Interface: 10.48.26.89 to NAD: 10.62.148.106

2016-12-30 20:37:43,874 DEBUG [EndpointHandlerWorker-2-34-thread-1][]

相關資訊

• ISE 2.2管理指南