ISE 2.2 上での異常エンドポイントの検出と適用 の設定

内容

概要 <u>前提条件</u> <u>要件</u> 使用するコンポーネント <u>背景説明</u> 設定 <u>ネットワーク図</u> 設定 <u>手順1:異常の検出の有効化</u> <u>手順2:許可ポリシーの設定</u> 確認 トラブルシュート 関連情報

概要

このドキュメントでは、異常なエンドポイントの検出および強制適用について説明します。これ は、拡張的なネットワーク可視性を実現するため、Cisco Identity Services Engine(ISE)に導入 された新たなプロファイリング機能です。

前提条件

要件

次の項目に関する知識があることが推奨されます。

・スイッチの有線 MAC 認証バイパス(MAB)の設定

- ・ワイヤレス LAN コントローラ(WLC)のワイヤレス MAB 設定
- •両方のデバイスの認可変更(CoA)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 1. Identity Services Engine 2.2
- 2. ワイヤレス LAN コントローラ 8.0.100.0
- 3. Cisco Catalyst スイッチ 3750 15.2(3) E2

4. 有線およびワイヤレス アダプタを備えた Windows 10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

背景説明

異常なエンドポイント検出機能を使用すると、ISEは接続されたエンドポイントの特定の属性お よびプロファイルの変更を監視できます。変更が1つ以上の設定済みの異常動作ルールに一致する 場合、ISEはエンドポイントを異常としてマークします。検出されると、ISEは(CoAとともに)アクションを実行し、特定のポリシーを適用して、疑わしいエンドポイントのアクセスを制限 できます。 この機能の使用例の1つに、MACアドレススプーフィングの検出が含まれます。

注:この機能は、MACアドレスのスプーフィングに関する潜在的なシナリオすべてに対処するわけではありません。この機能でカバーされている異常のタイプを必ずお読みになり、ご使用のユースケースへの適用可能性を確認してください。

検出を有効にすると、ISE は既存の各エンドポイントに関して受信した新たな情報をモニタし、 以下の属性が変化したかどうかを調べます。

- 1. NAS ポート タイプ:このエンドポイントのアクセス方式が変更されたかどうかを判断しま す。たとえば、有線Dot1x経由で接続された同じMACアドレスが無線Dot1xに使用され、そ の逆も使用されます。
- 2. DHCP クラス ID: クライアントのタイプ、またはエンドポイントのペンダーが変更された かどうかを判断します。これは、DHCPクラスID属性に特定の値が入力された後、別の値に 変更された場合にのみ適用されます。エンドポイントにスタティックIPが設定されている場 合、DHCPクラスID属性はISEに設定されません。後で、別のデバイスがMACアドレスをス プーフィングしてDHCPを使用すると、クラスIDが空の値から特定の文字列に変更されます 。これにより、Anomols Behaviorの検出はトリガーされません。
- 3. **エンドポイントポリシ**ー:プリンタまたはIP Phoneからワークステーションによるエンドポ インプロファイルの変更。

上述のいずれかの変化が ISE によって検出されると、このエンドポイントに AnomalousBehaviour 属性が追加され、True に設定されます。この属性を後で、認証ポリシーの 条件として使用できます。これにより、以降の認証で、このエンドポイントによるアクセスを制 限できます。

強制適用を設定しておくと、このような変化が検出された時点で ISE は CoA を送信し、エンド ポイントに対して再認証またはポート バウンスを実行できます。この機能を有効化すると、設定 された認証ポリシーに基づき、異常なエンドポイントに対する検疫が実行されます。

設定

ネットワーク図



設定

スイッチおよび WLC に対し、単純な MAB および AAA 設定を行います。この機能を使用するに は、次の手順を実行します。

手順1:異常の検出の有効化

[Administration] > [System] > [Settings] > [Profiling] の順に選択します。

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	m 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		

最初のオプションでは、異常な動作がすべて検出されますが、CoA は送信されません(可視性の みのモード)。2番目のオプションでは、異常の動作が検出された時点で、CoA が送信されます (強制適用モード)。 図に示すように、認証ポリシーの条件として AnomIousBehaviour 属性を設定します。

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

確認

ワイヤレス アダプタを介して接続します。ipconfig /all コマンドを使用して、ワイヤレス アダプ タの MAC アドレスを特定します。次に、出力例を示します。

Wi	reless 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

イーサネット アダプタの MAC アドレスを、正常なユーザの MAC アドレスと一致するようにな りすますことで、悪意のあるユーザをシミュレーションできます。

eneral	Advanced	Driver	Details	Events	Power Manag	ement
he foll he prop n the r	owing proper perty you war ight.	ties are a nt to char	available for	or this net e left, and	work adapter. O then select its v	lick value
ropert	y:			Va	alue:	
Pv4 C	hecksum Off	load	^		C04A002149C2	
Jumbo Large Large	Packet Send Offload Send Offload	V2 (IPv V2 (IPv	4) 5)	ON	ot Present	
Log Lir Maxim Packe Receiv Receiv Speed TCP C TCP C TCP C Transn	nk State Ever um Number o t Priority & VL ve Buffers ve Side Scalir & Duplex hecksum Offl hecksum Offl nit Buffers	nt f RSS Q AN ng load (IPv load (IPv	4) 6)			

VD) 02574L Clash's Mature & Connection Departies

正常なユーザが接続すると、データベース内にエンドポイントのエントリが作成されます。この 後、悪意のあるユーザは、なりすました MAC アドレスを使用することで接続できます。

~

このレポートから、最初の接続が WLC から行われていたことが分かります。その後、悪意のあるユーザが接続し、10 秒後に CoA が送信されています。異常なクライアントが検出されたためです。グローバル CoA タイプが [Reauth] に設定されているため、エンドポイントは再度接続を 試みます。ISE ではすでに AnomalousBehaviour 属性が True に設定されているため、最初のルー ルとの照合に基づき、このユーザは拒否されます。

	Logged At	RADIUS St Deta	ails () Identity	3 Endpoint ID	Authorization Rule	Network Device
×	Match Alfogged At	✓ of the following rule	es. Enter Advanced Fi	Iter Nam Save		-
	Loaaed At	Ƴ Within	✓ Custom	✓ From 12/30/20	16 8:: 📅 To 12/30/20	16 8:38 🗰 🕂 📋 🛛 Filter
	2016-12-30 20:37:59.728	8	C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Anomalous Client	SW
	2016-12-30 20:37:59.704		<u>0</u>	C0:4A:00:21:49:C2		SW
	2016-12-30 20:37:49.614	×	C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	SW
	2016-12-30 20:22:00.193	~	C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	WLC

図に示すように、[Context Visibility] タブにはエンドポイントの詳細が表示されます。

C0:4A:00:21:49:C2	C 🗕				
MAC Address: C0:4A:0 Username: c04a00214 Endpoint Profile: TP-LI Current IP Address: 192 Location: Location	0:21:49:C2 9c2 INK-Device 2.168.1.38 All Locations				
Applications Attributes	Authentication	Threats	Vulnerabilities		
General Attributes					
Description					
Static Assignment false					
Endpoint Policy TP-LINK	-Device				
Static Group Assignment false					
Identity Group Assignment Profiled					
Custom Attributes					
				▼ Filter ▼	Q -
Attribute Name	Attribute Valu	ie		▼ Filter ▼	Q-
Attribute Name No data found. Add custom attribu	Attribute Valu tes here.	le		₹ Filter +	٥-
Attribute Name No data found. Add custom attribu	Attribute Valu tes here.	le		▼ Filter •	٥-
Attribute Name No data found. Add custom attribu Other Attributes	Attribute Valu tes here.	ie		▼ Filter •	٥-
Attribute Name No data found. Add custom attribu Other Attributes AAA-Server	Attribute Valu tes here. sth-nice	e		▼ Filter •	Q-
Attribute Name No data found. Add custom attribu Other Attributes AAA-Server AD-Last-Fetch-Time	Attribute Valu tes here. sth-nice 1483130280592	le		▼ Filter •	¢-
Attribute Name No data found. Add custom attribu Other Attributes AAA-Server AD-Last-Fetch-Time Acct-Input-Gigawords	Attribute Valu tes here. sth-nice 1483130280592 0	ie		▼ Filter ▼	Q
Attribute Name No data found. Add custom attribu Other Attributes AAA-Server AD-Last-Fetch-Time Acct-Input-Gigawords Acct-Output-Gigawords	Attribute Valu tes here. sth-nice 1483130280592 0 0	le		▼ Filter •	¢-
Attribute Name No data found. Add custom attribute Other Attributes AAA-Server AD-Last-Fetch-Time Acct-Input-Gigawords Acct-Output-Gigawords Airespace-Wlan-Id	Attribute Valu tes here. sth-niœ 1483130280592 0 0 3	le		▼ Filter ▼	Q
Attribute Name No data found. Add custom attribu Other Attributes AAA-Server AD-Last-Fetch-Time Acct-Input-Gigawords Acct-Output-Gigawords Airespace-Wlan-Id AllowedProtocolMatchedRule	Attribute Valu tes here. sth-nice 1483130280592 0 0 3 MAB	le		▼ Filter ▼	¢-

エンドポイントをデータベースから削除することで、この属性をクリアできます。

図に示すように、ダッシュボードには、異常な動作を示すクライアント数を表す新しいタブが追 加されます。

cisco	Identity S	ervices Engine	Home	Context Visibility	 Operations 	Policy	Administration	 Work Centers 		L	icense Warning 🔺	୍ୟ	0	•
	Summar	y Endpoints	Guests	Vulnerability	Threat	+								4
I		Total Endpo	ints O	ı <mark>1</mark> ,	Active Endpoin	ts 0		jected Endpoints O	0	Anomalous Be	havior © 1	•	Aut	- G

Filters: × Anomalous Endpoints

E	NDPOINTS [®] Type Profile	C (OUI OS Types	CATEGORIES Identity Group	0	0 9	NETWORK DEVIC	ES ⁹ Name	0 B		
1 Selec	homevices: [100%]	2	tp-li,ltd.: [100				locattions: [100%]	0	Rows/Page 🗌	1 ¥ H 4 1	•
c	+ 🛍 🗹 ANC -	Change Authorization - Clear	Threats & Vulnerabilities	Export - Impo	nt - MDM Actio	ns - Release R	ejected Revoke Certificat	e			
	MAC Address	Anomalous Behavior	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description	C	UI	05
×	MAC Address	true	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description		OUI	0
	C0:4A:00:21:49:C2	true	192.168.1.38	c04a002149c2		Location + All	TP-LINK-Device		т	P-LINK TECHNOLOGI	

トラブルシュート

トラブルシュートを実行するには、プロファイラのデバッグを有効化します。これには、 [Administration] > [System] > [Logging] > [Debug Log] [Configuration] の順に選択します。

dentity Services Engine	Home → Context Visibility → Operations → Policy → Administration → Work Centers							
▼System → Identity Management → Network Resources → Device Portal Management pxGrid Services → Feed Service → Threat Centric NAC								
Deployment Licensing + Certifica	es ▼Logging → Maintenance Upgrade Backup & Restore → Admin Access → Settings							
0								
Local Log Settings	Node List > sth-nice.example.com							
Remote Logging Targets	bebug Level configuration							
Logging Categories	/ Edit Reset 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							

ISE の Profiler.log ファイルを特定するには、図に示すように、[Operations] > [Download Logs] > [Debug Logs] の順に選択します。

dentity Services Engine Home	Context Visibility	Policy Administration	Work Centers
► RADIUS Threat-Centric NAC Live Logs ► TAC	ACS Troubleshoot + Adaptiv	e Network Control Reports	
Diagnostic 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	

これらのログには、**Profiling.log ファイルの一部を表すスニペットが表示されます。**図から分かる ように、ISE では NAS ポート タイプ属性の古い値と新しい値とを比較することで、MAC アドレ

ス C0:4A:00:21:49:C2 を持つエンドポイントがアクセス方式を変更したことを検出しています。 ここでは、アクセス方式がワイヤレスからイーサネットに変わっています。

2016-12-30 20:37:43,874 DEBUG [EndpointHandlerWorker-2-34-thread-1][] 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 強制適用が有効化されているため、ISE は規定のアクションを実行します。ここでのアクション は、上述のプロファイル設定で指定したグローバル設定に基づく、CoA の送信です。この例では 、CoA のタイプを再認証に設定しているため、ISE はエンドポイントを再認証し、設定されたル ールを再度チェックします。このエンドポイントは異常なクライアントのルールに適合したため 、拒否されます。 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

関連情報

• ISE 2.2 アドミニストレーション ガイド