Konfigurieren der Firepower 6.1 pxGrid-Problembehebung mit der ISE

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Netzwerkdiagramm Konfigurieren von FirePOWER ISE konfigurieren Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie die Firepower 6.1 pxGrid-Problembehebung mit der Identity Services Engine (ISE) konfiguriert wird. Das FirePOWER 6.1+ ISE-Sanierungsmodul kann zusammen mit dem ISE Endpoint Protection Service (EPS) verwendet werden, um Quarantäne-/Blacklisting von Angreifern auf dem Netzwerkzugriffs-Layer zu automatisieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ISE
- Cisco FirePOWER

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ISE Version 2.0 Patch 4
- Cisco FirePOWER 6.1.0
- Virtual Wireless LAN Controller (vWLC) 8.3.102.0

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Dieser Artikel behandelt nicht die Erstkonfiguration der ISE-Integration mit FirePOWER, die ISE-Integration mit Active Directory (AD) und die FirePOWER-Integration mit AD. Navigieren Sie für diese Informationen zu Referenzen-Abschnitt. Das FirePOWER 6.1-Sanierungsmodul ermöglicht dem FirePOWER-System die Nutzung von ISE-EPS-Funktionen (Quarantäne, Quarantäne, Port-Herunterfahren) als Problembehebung, wenn eine Korrelationsregel zugeordnet wird.

Hinweis: Für Wireless-Bereitstellungen ist keine Port-Abschaltung verfügbar.

Netzwerkdiagramm



Flussbeschreibung:

- 1. Ein Client stellt eine Verbindung zu einem Netzwerk her, authentifiziert sich mit der ISE und trifft eine Autorisierungsregel mit einem Autorisierungsprofil, das uneingeschränkten Zugriff auf das Netzwerk gewährt.
- 2. Der Datenverkehr vom Client fließt dann über ein FirePOWER-Gerät.
- 3. Der Benutzer startet eine schädliche Aktivität und trifft auf eine Korrelationsregel, die wiederum FirePOWER Management Center (FMC) veranlasst, die ISE-Beseitigung über pxGrid durchzuführen.
- 4. Die ISE weist dem Endpunkt eine EPSStatus-Quarantäne zu und löst einen RADIUS Change

of Authorization auf ein Netzwerkzugriffsgerät (WLC oder Switch) aus.

5. Der Client greift auf eine andere Autorisierungsrichtlinie zu, die einen eingeschränkten Zugriff zuweist (ändert SGT oder leitet den SGT an das Portal um oder verweigert den Zugriff).

Hinweis: Network Access Device (NAD) sollte so konfiguriert werden, dass RADIUS Accounting an die ISE gesendet wird, um der ISE IP-Adressinformationen zur Zuordnung der IP-Adresse zu einem Endpunkt bereitzustellen.

Konfigurieren von FirePOWER

Schritt 1: Konfigurieren einer pxGrid-Instanz zur Risikominderung

Navigieren Sie zu **Richtlinien > Aktionen > Instanzen**, und fügen Sie pxGrid Mitigation Instance hinzu, wie im Bild gezeigt.

Overview Analysis Policies Devices Objects AM	P		Deploy 🤇	System	Help 🔻	admin 🔻
Access Control Network Discovery Application Detectors	Correlation	Actions > Instances				
				Alerts F	emediation	s Groups
	Edit Instand	ce				
	Instance Name	ISE-NEW-INSTANCE				
	Module	pxGrid Mitigation(v1.0)				
	Description					
	Enable Logging	● On C Off				
		Create Cancel				

Schritt 2: Konfigurieren Sie eine Problembehebung.

Es stehen zwei Typen zur Verfügung: Ziel minimieren und Quelle minimieren. In diesem Beispiel wird Source Mitigation verwendet. Wählen Sie Sanierungstyp aus, und klicken Sie auf **Hinzufügen**, wie im Bild gezeigt:

Remediation Name	Remediation Typ	Description
No con	figured remediations	available
Add a new remediatio	on of type Mitigate D	estination 💌 🛛 Ad
Add a new remediatio	on of type Mitigate D Mitigate D	estination 💌 🗛

Weisen Sie der Problembehebung, wie im Bild gezeigt, eine Aktion zur Problembehebung zu:

Edit Remediation	
Remediation Name	QUARANTINE-SOURCE
Remediation Type	Mitigate Source
Description	
Mitigation Action	quarantine 🔽
Whitelist (an <i>optional</i> list of networks)	
	Create

Schritt 3: Konfigurieren einer Korrelationsregel.

Navigieren Sie zu **Policies > Correlation > Rule Management**, und klicken Sie auf **Create Rule Correlation (Regelkorrelation erstellen)**, um die Korrektur auszulösen. Korrelationsregel kann mehrere Bedingungen enthalten. In diesem Beispiel wird Correlation Rule **PingDC** getroffen, wenn ein Angriffsereignis auftritt und die Ziel-IP-Adresse 192.168.0.121 lautet. Für den Test wird eine benutzerdefinierte Intrusion-Regel konfiguriert, die mit der ICMP-Echoantwort übereinstimmt, wie im Bild gezeigt:

Overview Analysis Policies Devices Objects AMP	Deploy	. 00 System Help ▼ admin ▼
Access Control V Network Discovery Application Detectors Correlation Actions V		
		Alerts Remediations Groups
Policy Management Rule Management White List Traffic Profiles		
Rule Information Q Add User Qu	alification	O Add Host Profile Qualification
Rule Name PingDC		
Rule Description		
Rule Group Ungrouped		
Select the type of event for this rule		
If an intrusion event occurs 🔄 and it meets the following conditions:		
S Add condition		
X Destination IP is I192.168.0.121		
Rule Options		O Add Inactive Period
Snooze If this rule generates an event, snooze for 0 hours		
Inactive Periods There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".		

Schritt 4: Konfigurieren einer Korrelationsrichtlinie

Navigieren Sie zu **Richtlinien > Korrelation > Richtlinienmanagement**, und klicken Sie auf **Richtlinie erstellen**, fügen Sie der Richtlinie eine Regel hinzu, und weisen Sie der Richtlinie eine Antwort zu, wie im Bild gezeigt:

Overview Analysis Policies	Devices Objects AMP	Deploy 🍳 System Help 🔻 admin 🔻
Access Control Network Discover	ry Application Detectors Correlation Actions •	
		Alerts Remediations Groups
Policy Management Rule Ma	nagement White List Traffic Profiles	
Correlation Policy Information	n	You have unsaved changes Save Cancel
Policy Name ise_core	lation_policy	
Policy Description		
Default Priority None		
Policy Rules		O Add Rules
Rule	Responses	Priority
PingDC	QUARANTINE-SOURCE (Remediation)	Default 🖸 🧳 📋

Aktivieren Sie die Korrelationsrichtlinie, wie im Bild gezeigt:

Overview Analysis Policies Devices Objects AMP	Deploy	₽ ₁ s	System H	Help 🔻	admin 🔻
Access Control Network Discovery Application Detectors Correlation Actions Actions					
		A	Alerts Rem	nediations	s Groups
Policy Management Rule Management White List Traffic Profiles					
				😳 Crea	te Policy
Name			Sort	by State	2
ise corellation policy				10 🦉	D

ISE konfigurieren

Schritt 1: Konfigurieren der Autorisierungsrichtlinie

Navigieren Sie zu **Richtlinien > Autorisierung**, und fügen Sie eine neue Autorisierungsrichtlinie hinzu, die nach der Bereinigung aufgerufen wird. **Sitzung** verwenden: **EPSStatus EQUALS Quarantine** als Bedingung. Es gibt mehrere Optionen, die als Ergebnis verwendet werden können:

- Zulassen von Zugriff und Zuweisen eines anderen SGTs (Durchsetzung von Zugriffskontrollbeschränkungen auf Netzwerkgeräten)
- Zugriff verweigern (Benutzer sollte aus dem Netzwerk geworfen werden und nicht wieder eine Verbindung herstellen können)
- Umleitung zu einem Blacklist-Portal (in diesem Szenario ist hierfür ein benutzerdefiniertes Hotspot-Portal konfiguriert)

dentity Services Engin	e Home ▶ Operations		► Administration	▶ Work Centers	1	License Warning 🔺		Ø	1		
Authentication Authorization	Authentication Authorization Profiling Posture Client Provisioning > Policy Elements										
Authorization Policy Define He Authorization Policy by configuring rules based on identify groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page First Matched Rule Applies											
 Exceptions (3) 											
Status Rule Name	Co	nditions (identity groups and other cor	nditions)	Permissio	ons						
AssignSGTBloc	cOnFP If Set	ssion:EPSStatus EQUALS Quarantine	e	then Malicio	usUser AND Permi	tAccess		E	dit 🕶		
BlockOnISE	if S	ession:EPSStatus EQUALS Quaranti	ne	then Deny	Access			E	dit 🔻		
BlockOnISE	_copy if	Session:EPSStatus EQUALS Quarar	ntine	then bla	cklist_redirect			E	dit 🕶		

Benutzerdefinierte Portalkonfiguration

In diesem Beispiel wird das Hotspot-Portal als **Blacklist** konfiguriert. Es gibt nur eine Seite mit Richtlinien für akzeptable Nutzung (Acceptable Use Policy, AUP) mit benutzerdefiniertem Text, und es besteht keine Möglichkeit, die AUP zu akzeptieren (dies geschieht mit JavaScript). Um dies zu erreichen, müssen Sie zuerst JavaScript aktivieren und dann einen Code einfügen, der die Schaltfläche und Steuerelemente für die AUP-Anpassung in der Konfiguration der Portalanpassung verbirgt.

Schritt 1: Aktivieren Sie JavaScript.

Navigieren Sie zu Administration > System > Admin Access> Settings > Portal Customization. Wählen Sie Portal Customization mit HTML und JavaScript aktivieren und klicken Sie auf Save.



Schritt 2: Erstellen Sie ein Hotspot-Portal.

Navigieren Sie zu **Gastzugriff > Konfigurieren > Gastportale,** und klicken Sie auf **Erstellen**, und wählen Sie dann Hotspot-Typ aus.

diale Ident	ity Services Engine	Home	 Operations 	▶ Policy		► Administration	▶ Work Centers		1	License Warning 🔺			
✓ Configure	Manage Accounts	 Settings 											
Overview	Overview Guest Portals Guest Types Sponsor Groups Sponsor Portals												
Guest P	ortals												
Choose of	ne of the three pre-defin	ed portal types	, which you can eo	lit, customize, a	and authorize for gues	st access.							
Create	Edit Duplicate	Delete											

Schritt 3: Konfigurieren der Portalanpassung

Navigieren Sie zu **Portalseitenanpassung**, und ändern Sie Titel und Inhalt, um dem Benutzer eine entsprechende Warnung zu geben.

dentity Services Engine Home		➤ Administration → Work Centers	🚺 License Warning 🔺 ိ 🧔 🛔	\$
	or Groups Sponsor Portals			
Pages	Page Customizations			
✓ Pages	Browser Page Title RESTRICTED ACCESS		Preview Settings	
Acceptable Use Policy	Optional Content 1			
Authentication Success	Font Size X * [1] [2]	▲ • B I U ⊟ ⅓ ∅ •	cisco RESTRICTED ACCESS	
Error			RESTRICTED ACCESS You have been identified as a	
✓ Messages			malicious user and blocked.	
Error Messages				
	(text or HTML) Click Preview to test HTML render	ring.		
	Content Title			
	RESTRICTED ACCESS			
	Instructional Text			
	Font Size X → [□] ⊙	▲ • B I U ⋮ 號 Ø •		
	You have been identified as a malicious user an	nd blocked.		

Navigieren Sie zu **Option Content 2**, klicken Sie auf **HTML-Quelle umschalten**, und fügen Sie das Skript in Folgendes ein:

Klicken Sie auf HTML-Quelle deaktivieren.

Optional Content 2

Font	Size	<u>A</u> - B	Ι 및 Έ ξΞ ∅ ▼
X - 🗊 🖸			
<script></th><th></th><th></th><th></th></tr><tr><th>(function(){</th><th></th><th></th><th></th></tr><tr><th>jQuery('.cisco-i</th><th>se-aup-text').hide();</th><th></th><th></th></tr><tr><th>jQuery('.cisco-i</th><th>se-aup-controls').hide();</th><th></th><th></th></tr><tr><th>setTimeout(function</th><th>on(){ jQuery('#portal-sess</th><th>sion-timeout-popup-se</th><th>creen, #portal-session-</th></tr><tr><th>timeout-popup-po</th><th>pup, #portal-session-time</th><th>eout-popup').remove(</th><th>); }, 100);</th></tr><tr><th>})0;</th><th></th><th></th><th></th></tr><tr><th></script>			
<pre><br _moz_editor_<="" pre=""/></pre>	bogus_node="TRUE" />		
(hard an 1/TAU > 0/	- Construction for the state of		

(text or HTML) Click Preview to test HTML rendering.

Überprüfen

Verwenden Sie die Informationen in diesem Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

FirePOWER

Der Auslöser für die Problembehebung ist ein Treffer von Korrelationsrichtlinien/-regeln. Navigieren Sie zu **Analyse > Correlation > Correlation > Correlation Events**, und überprüfen Sie, ob ein Korrelationsereignis aufgetreten ist.

C	verviev	Analysis	Policies Dev	ices Obje	ects AMP							Deploy	. 🔒 System	Help 🖥	🗸 admin 🔻
С	ontext E	plorer Conne	ctions 🔹 In	rusions 🔻	Files Ho	osts 🔹 Users 🔻	Vulnerabilities	Correlation	Correlation Events	Custom 🔻	Lookup 🔻	Search			
										Bookr	nark This Page	e Report Designe	r Dashboard View	v Bookma	rks Search
0 0	Correlation Events														
N	Search (onstraints (<u>Edit Se</u>	rch)												
	Jump to.														
	Γ	▼ <u>Time</u> ×	Impact >	t <u>Inline</u> X <u>Result</u>	Source IP	× <u>Source</u> × <u>Country</u>	Destination × IP	Destination × Country	Security Intelligence × Category	Source User	×	Destination × User	Source Port / ICMP Type	×	Destination Po ICMP Code
		2017-02-16 13:2	:51 (1)		172.16.1	0.19	i 192.168.0.121						8 (Echo Request)	/ icmp	<u>0 / icmp</u>

ISE

Die ISE sollte dann Radius auslösen: CoA und erneute Authentifizierung des Benutzers. Diese Ereignisse können unter **Operation > RADIUS Livelog** verifiziert werden.

2017-02-16 13:26:22.894	_	0	alice	E4:B3:18:69:EB:8C	Windows10-Workst Default >> Dot1X >> D Default >> AssignSGT MaliciousUser,PermitAcc v	WLC
2017-02-16 13:26:21.040	~	à		E4:B3:18:69:EB:8C	v	WLC
2017-02-16 13:25:29.036	~	0	alice	E4:B3:18:69:EB:8C	Windows10-Workst Default >> Dot1X >> D Default >> Standard R PermitAccess,Administra v	WLC

In diesem Beispiel hat die ISE dem Endpunkt verschiedene SGT **MaliciousUser** zugewiesen. Im Falle eines **Deny Access** Authorization-Profils verliert der Benutzer die Wireless-Verbindung und kann keine Verbindung mehr herstellen.

Die Sanierung durch ein Blacklist-Portal. Wenn eine Behebungs-Autorisierungsregel für die Umleitung zum Portal konfiguriert ist, sollte sie aus Angreifersicht wie folgt aussehen:



Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Navigieren Sie zu Analyse > Korrelation > Status wie in diesem Bild gezeigt.



Die Ergebnismeldung sollte entweder **Erfolgreiche Beendigung der Problembehebung** oder eine bestimmte Fehlermeldung zurückgeben. Syslog überprüfen: **System > Monitoring > Syslog** und Filter Output with **pxgrid**. Die gleichen Protokolle können in **/var/log/messages** überprüft werden.

Zugehörige Informationen

- <u>https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-</u> <u>Troubleshoot-ISE-and-FirePOWER-Integrati.html</u>
- https://communities.cisco.com/docs/DOC-68284
- <u>https://communities.cisco.com/docs/DOC-68285</u>
- https://communities.cisco.com/thread/64870?start=0&tstart=0
- <u>http://www.cisco.com/c/en/us/td/docs/security/ise/2-</u> 0/admin_guide/b_ise_admin_guide_20.html
- http://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-configguide-v61.html