Benutzerdefinierte lokale Snort-Regeln in Snort2 auf FTD konfigurieren

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Konfigurieren
Netzwerkdiagramm
Konfiguration
Schritt 1: Snort-Version bestätigen
Schritt 2: Erstellen einer benutzerdefinierten lokalen Snort-Regel in Snort 2
Schritt 3: Benutzerdefinierte lokale Snort-Regel bestätigen
Schritt 4: Regelaktion ändern
<u>Schritt 5: Zuordnen einer Richtlinie für Sicherheitsrisiken zurZugriffskontrollrichtlinie (ACP)-</u> Regel
Schritt 6: Änderungen bereitstellen
Überprüfung
Benutzerdefinierte lokale Snort-Regel wird nicht ausgelöst
Schritt 1: Festlegen des Inhalts der Datei im HTTP-Server
Schritt 2: Erste HTTP-Anfrage
Benutzerdefinierte lokale Snort-Regel wird ausgelöst
Schritt 1: Festlegen des Inhalts der Datei im HTTP-Server
Schritt 2: Erste HTTP-Anfrage
Schritt 3: ConfirmIntrusion-Ereignis
Fehlerbehebung

Einleitung

In diesem Dokument wird das Verfahren zur Konfiguration benutzerdefinierter lokaler Snort-Regeln in Snort2 auf dem FTD (Firewall Threat Defense) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco FirePOWER Management Center (FMC)
- Schutz vor Bedrohungen durch Firewall (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FirePOWER Management Center für VMware 7.4.1
- Cisco FirePOWER 2120 7.4.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Benutzerdefinierte lokale Snort-Regel bezieht sich auf eine benutzerdefinierte Regel, die Sie innerhalb des Snort Intrusion Detection and Prevention Systems erstellen und implementieren können, das in die FTD integriert ist. Wenn Sie eine benutzerdefinierte lokale Snort-Regel in Cisco FTD erstellen, definieren Sie im Wesentlichen ein neues Muster oder eine Reihe von Bedingungen, auf die die Snort-Engine achten kann. Wenn der Netzwerkverkehr die in der benutzerdefinierten Regel festgelegten Bedingungen erfüllt, kann Snort die in der Regel definierte Aktion ausführen, z. B. eine Warnung generieren oder das Paket verwerfen. Administratoren verwenden benutzerdefinierte lokale Snort-Regeln, um bestimmte Bedrohungen zu bekämpfen, die nicht von den allgemeinen Regelsätzen abgedeckt werden.

In diesem Dokument wird erläutert, wie Sie eine benutzerdefinierte lokale Snort-Regel konfigurieren und überprüfen, die zum Erkennen und Verwerfen von HTTP-Antwortpaketen mit einer bestimmten Zeichenfolge (Benutzername) entwickelt wurde.



Vorsicht: Das Erstellen benutzerdefinierter lokaler Snort-Regeln und die Bereitstellung von Support hierfür fallen nicht unter den TAC-Support. Daher kann dieses Dokument nur als Referenz verwendet werden und Sie bitten, diese benutzerdefinierten Regeln nach eigenem Ermessen und mit eigener Verantwortung zu erstellen und zu verwalten.

Konfigurieren

Netzwerkdiagramm

In diesem Dokument wird die Konfiguration und Überprüfung der benutzerdefinierten lokalen Snort-Regel in Snort2 in diesem Diagramm vorgestellt.



Konfiguration

Dies ist die Konfiguration der benutzerdefinierten lokalen Snort-Regel zum Erkennen und Löschen von HTTP-Antwortpaketen, die eine bestimmte Zeichenfolge (Benutzername) enthalten.

Schritt 1: Snort-Version bestätigen

Navigieren Sie zu Geräte > Geräteverwaltung auf FMC, und klicken Sie auf die Registerkarte Gerät. Bestätigen Sie, dass die Snort-Version Snort2 ist.

Firewall Management Center Overview Analyst Devices / Secure Firewall Device Summary	is Policies Devices Objects Integration		Deploy	Q 🥝 🌣 🝘 admin 🗸 👘 SECU
FPR2120_FTD Cisco Firepower 2120 Threat Defense Device Routing Interfaces Inline Sets DHCP VTEP	SNMP			
General 🗸 ± +	License	/	System	0 G
Name: FPR2120_FTD	Essentials:	Yes	Model:	Cisco Firepower 2120 Threat Defense
Transfer Packets: Yes	Export-Controlled Features:	Yes	Serial:	UNPOT CECEUE
Troubleshoot: Logs CLI Download	Malware Defense:	Yes	Time:	2024-04-06 01:26:12
Mode: Routed	IPS:	Yes	Time Zone:	UTC (UTC+0:00)
Compliance Mode: None	Carrier:	No	Version:	7.4.1
TLS Crypto Acceleration: Enabled	URL:	No	Time Zone setting for Time	UTC (UTC+0:00)
	Secure Client Premier:	No	Inventory:	View
Device Configuration: Import Export Oownload	Secure Client Advantage:	No	inventory.	(Inv
OnBoarding Method: Registration Key	Secure Client VPN Only:	No		
Inspection Engine	Health		Management	/ 🕥
Inspection Engine: Snort 2	Status:	0	Remote Host Address:	1.1050.25

Snort-Version

Schritt 2: Erstellen einer benutzerdefinierten lokalen Snort-Regel in Snort 2

Navigieren Sie zu Objekte > Intrusion Rules > Snort 2 All Rules on FMC, und klicken Sie auf Create Rule (Regel erstellen).

Firewall Management Center Objects / Intrusion Rules / Snort 2 All Rules	Analysis Policies	Devices Objects Integration	Deploy Q 📀 🗱 🕢 admin ~ 🔤
Snort 2 All Rules Snort 3 All Rules			
< Intrusion Policy			Search Delete Local Rules Import Rules Create Rule
Group Rules By Category (62655)			
Category			

Benutzerdefinierte Regel erstellen

Geben Sie die erforderlichen Informationen für die benutzerdefinierte lokale Snort-Regel ein.

- Eindringen: custom_http_sig
- Aktion: alert
- Protokoll: TCP
- Fluss: etabliert, an Client
- Inhalt : Benutzername (Rohdaten)

Firewall Management Center Overview Analysis Objects / Intrusion Rules / Create Overview	Policies Devices Objects Integration	Deploy Q 🥥 🌣 🚱 admin
Snort 2 All Rules Snort 3 All Rules		Search Upload Update Intrusion
	Create New Rule	
	Message custom_http_sig	
	Classification Unknown Traffic	
	Action alert	
	Protocol too	
	Direction Ridirectional	
	Source De anu Source Dott	
	Destination for any Destination ford	
	Desenation Port any Desenation Port any	
	flow X	
	Established v To Client v	
	Case Insensitive Case I	
	HTTP Header	
	HTTP Raw URI	
	HTTP Raw Header	
	HTTP Raw Cookie	
	HTTP Client Body	
	HTTP Status Message	
	HTTP Status Code	
	Distance	
	Within	
	Offset	
	Depth	
	Use Fast Pattern Matcher	
	Fast Pattern Matcher Offset and Length	
	Content Add Uption Save As New	

Eingabe der erforderlichen Informationen für Regel

Schritt 3: Benutzerdefinierte lokale Snort-Regel bestätigen

Navigieren Sie zu Policies > Intrusion Policies on FMC, und klicken Sie auf die Schaltfläche Snort 2 Version.

Firewall Management Center Policies / Access Control / Intrusion / Intru	sion Policies Overview Ar	nalysis Policies Devices	Objects Integration	Deploy Q 📀 🔅 🕻	admin v dodh SECURE						
Intrusion Policies Network Analysis Policies											
Hide Snort 3 Sync status 🌒 🔍 Search by	Intrusion Policy, Description, or Base P	All IPS Rules	IPS Mapping 🜒 Comp	Create Policies							
Intrusion Policy Des	scription	Base Policy	Usage Information								
snort_test ✦ Snort 3 is in sync vith Snort 2. 2024-01-12		Balanced Security and Connectivity	1 Access Control Policy No Zero Trust Application Policy 1 Device	Snort 2 Version	Snort 3 Version 📝 🖥 🔃 🗑						

Benutzerdefinierte Regel bestätigen

Navigieren Sie zu Regeln > Kategorie > lokal auf FMC, und bestätigen Sie die Details der benutzerdefinierten lokalen Snort-Regel.

Firewall Management Policies / Access Control / Intru	Center Ov usion / Edit Policy	verview Analysis	Policies Devices	Objects Integration	De	ploy Q 🕝 🕴	¢ 0	admin v diala s	SECURE
Intrusion Policies Network Analy	lysis Policies								
Policy Information	Rules								< Back
Cisco Recommendations	Rule Configuration	Filter:							
> Advanced Settings	Category	Category:"local"							XØ
> Policy Layers	hle-pdf indicator-compromise indicator-obfuscation indicator-scan	0 selected rules of 1 Rule State • Event Fil	Itering • Dynamic State	 Alerting Comments 			Policy		•
	indicator-shellcode	GID SID	Message 4				-	• • • •	-
L	malware-backdoor	1 1000001	custom_http_sig				\rightarrow		
	malware-cnc								
	malware-tools	Hide details					IC C	1 of 1 >	X
	netbios os-linux	> Suppressions (0)					Add	^
	os-mohile	> Dynamic State	(0)					Add	
	Classifications Microsoft Vulnerabilities	Alerts (0)						Add SNMP Alert	
	Microsoft Worms Platform Specific	Comments (0)						Add	
	Preprocessors	 Documentation 	1						
	Priority Pula Lindata								
	nue opuate		rule alert top any ar	ny <> any any (sid:1000001; gld:1; flow:	established,to_client; content:"username"; rawbytes;	msg:"custom_http_sig"	; classtype:ur	iknown; rev:1;)	÷

Detail der benutzerdefinierten Regel

Schritt 4: Regelaktion ändern

Klicken Sie auf die Schaltfläche State (Status), legen Sie den Status auf Drop and Generate Events (Löschen und Generieren von Ereignissen) fest, und klicken Sie auf die Schaltfläche OK.

Firewall Managemen Policies / Access Control / Intr	t Center o rusion / Edit Policy	verview	Analysis	Policies	Devices	Objects	Integration		Deploy	Q	•	0	admin \sim	cisco S	ECURE
Intrusion Policies Network Ana	alysis Policies														
Policy Information	Rules														< Back
Cisco Recommendations > Advanced Settings	Rule Configuration Rule Content Category	Filter: Category	:"local"												ר
> Policy Layers	file-pdf indicator-compromise indicator-obfuscation indicator-scan	0 selected Rule State	0 selected rules of 1 Rule State + Event Filtering + Dynamic State + Alerting + Comments + GID SID Message +										Policy → ● ▼		-
	malware-backdoor malware-chor malware-tools netbios os-linux	. 1	1000001	custom_ht	state Disabled	tate for "cu	stom_http_sig" Ø								
	Classifications Microsoft Vulnerabilities Microsoft Worms Platform Specific				Generate Drop and Disabled	Events Generate Even	ts Cancel OK								

Ändern der Regelaktion

Klicken Sie auf die Schaltfläche "Richtlinieninformationen" und dann auf die Schaltfläche "Änderungen bestätigen", um die Änderungen zu speichern.

Firewall Managemen Policies / Access Control / In	nt Center Overview Analysis Policies Devices Objects Integration Deplo	» ९ ०	° 0	admin ~	sibialis cisco SECURE	
Intrusion Policies Network Ar	nalysis Policies					
Policy Information A Rules	Policy Information				< Back	
Cisco Recommendations > Advanced Settings	Drop when Inline					*
> Policy Layers	Base Policy Description of Changes O			🖌 Manage	e Base Policy	
	The base policy is up to date (Rule Update 2024-04-03-001-vr Change rule action)					
	This policy has 9958 enabled rules			/ N	Manage Rules	
	484 rules generate events Cancel OK OK				 View 	
	No recommendations have been generated. Click here to set up Cisco recommendations.					
	This policy contains enabled preprocessor rules. Please read the rule documentation to ensure the preprocessors have the correct settings for these rules					
		Discar	d Changes	Comm	nit Changes	

Änderungen bestätigen

Schritt 5: Zuordnen einer Richtlinie für Sicherheitsrisiken zur Zugriffskontrollrichtlinie (ACP)

Navigieren Sie zu Policies > Access Control on FMC, und ordnen Sie Intrusion Policy dem ACP zu.

1 Citing Rule ftd_acp			Mandatory 🛛 🖉 🗙
Name ftd_acp	Action C Allow	/ V Logging ON Time Ra	nge None V Rule Enabled
	Intrusion Polic	y snort_test X V	✓ File Policy None ✓
Q Zones (2) Networks Ports Application	s 🛕 Users URLs	Dynamic Attributes VLAN Tags	
Q Search Security Zone Objects	Showing 2 out of 2	Selected Sources: 1	Selected Destinations and Applications: 1
inside_zone (Routed Security Zone)		Collapse All Remove All	Collapse All Remove All
A outside_zone (Routed Security Zone)		ZONE V 1 Object	ZONE V 1 Object

Mit AKP-Regel verknüpfen

Schritt 6: Änderungen bereitstellen

Stellen Sie die Änderungen auf FTD ein.

Firewall Management Center Overview Analysis Policies Devices Objects Integration		Deploy Q Ø Ø admin v deuter	SECURE
→ Return to Access Control Policy Management acp-rule ✓	٩	Advanced Deploy All	Legacy UI Savo
Packets O Prefiter Rules O Decryption O Security Intelligence O Identity O Access Control O More	FPR2120_FTD	Ready for Deployment	1 device

Änderungen bereitstellen

Überprüfung

Benutzerdefinierte lokale Snort-Regel wird nicht ausgelöst

Schritt 1: Festlegen des Inhalts der Datei im HTTP-Server

Legen Sie den Inhalt der Datei test.txt auf der Seite des HTTP-Servers auf user fest.

Schritt 2: Erste HTTP-Anfrage

Greifen Sie vom Browser des Clients (192.168.10.1) auf den HTTP-Server (192.168.20.1/test.txt) zu, und bestätigen Sie, dass die HTTP-Kommunikation zulässig ist.

6	192.168.20.1/test.txt	×	+	-	٥	×
~	→ C ▲		192.168.20.1/test.txt	☆	Θ	:
use						

Erste HTTP-Anfrage

Benutzerdefinierte lokale Snort-Regel wird ausgelöst

Schritt 1: Festlegen des Inhalts der Datei im HTTP-Server

Legen Sie den Inhalt der Datei test.txt auf der Seite des HTTP-Servers auf username fest.

Schritt 2: Erste HTTP-Anfrage

Greifen Sie vom Browser des Clients (192.168.10.1) auf den HTTP-Server (192.168.20.1/test.txt) zu, und bestätigen Sie, dass die HTTP-Kommunikation blockiert ist.



B

Erste HTTP-Anfrage

Schritt 3: Angriffsereignis bestätigen

Navigieren Sie zu Analyse > Sicherheitsrisiken > Ereignisse in FMC, und bestätigen Sie, dass das Sicherheitsverletzungsereignis von der benutzerdefinierten lokalen Snort-Regel generiert wird.

Firewall Management Analysis / Intrusions / Events	Center	Verview	Analysis	Policies	Devices	Objects	Integration				Deplo	v Q	o o	ł 🕜 ad	imin v 👘	isco SEC	URE
							В	ookmark This Pa	ige Reporting	Dashboard	d View Bo	okmarks	Search	Predefin	ed Searche	s	•
Events By Priority and Classification (settle workflow)																	
Search Constraints (Edit Search Save Search)																	
Drilldown of Event, Priority, and Clas	sification Table	View of Eve	ents Pac	cets													
Jump to																	
🗌 🕹 Time X 🛛 Pric	rity X Impact X	Inline Result ×	Reason X	Source IP X	Source x	Destination IP X	Destination x Country	Source Port / ICMP X Type	Destination Port / ICMP X Code	SSL Status x	VLAN x	Messag	pe ×		Classifica	ation ×	Generat
▼ 2024-04-06 11:05:13 low	Unknow	Dropped		192.168.20.1		0 192.168.10.	1	80 (http) / tcp	50057 / tcp			custom	_http_sig	(1:1000001:1	I) Unknown	n Traffic	Standar

Intrusion-Ereignis

Klicken Sie auf die Registerkarte Packets, und bestätigen Sie die Details des Angriffsereignisses.

Firewall Management Center Overview Analysis / Intrusions / Events Objects Integration Deploy Q O 🌣 🕢 admin v relation	SECURE
Bookmark: This Page Reporting Dashboard View Bookmarks Search Predefined Searches	Ŧ
Events By Priority and Classification Institution for the section of the section	11:07:15 Expanding
Search Constraints (Edit Search)	
Drilldown of Event, Priority, and Classification Table View of Events Packets	
- Event Information	
Message custom_http_sig (1:100001:1) Time 2024-04-06 11:06:34	
Classification Unknown Traffic	
Priority low	
Ingress Security Zone outside_zone	
Egress Security Zone inside_zone	
Device FPR2120_FTD	
Ingress Interface outside	
Egress Interface inside	
Source IP 192.168.20.1	
Source Port / ICMP Type 80 (http) / tcp	
Destination IP 192.168.10.1	
Destination Port / ICMP Code 50061 / tcp	
HTTP Hostname 192.168.20.1	
HTTP URI /test.txt	
Intrusion Policy snort_test	
Access Control Policy acp-rule	
Access Control Rule ftd_acp	
Rule alert top any o⇔ any (sid:1000001; gid:1; flow:established.to_client; content:"username"; rambytes; msg:"custom_http_pig"; classtyme:unknown; rev:1;)	
► Actions	

Details des Angriffsereignisses

Fehlerbehebung

Führen Sie einen Befehl aussystem support trace, um das Verhalten auf FTD zu bestätigen. In diesem Beispiel wird der HTTP-Datenverkehr durch die IPS-Regel blockiert (gid 1, sid 1000001).

<#root>

```
>
```

system support trace

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.1
Please specify a client port:
Please specify a server IP address: 192.168.20.1
Please specify a server port:
```

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Firewall: allow rule, '

ftd_acp

', allow 192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0

IPS Event

:

gid 1

,

sid 1000001

, drop

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Snort id 3, NAP id 2, IPS id 1, Verdict BLOCKFLOW 192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 ===>

Blocked by IPS

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.