在FTD的Snort2中配置自定义本地Snort规则

目录

<u>简介</u>

<u>先决条件</u>

<u>要求</u>

<u>使用的组件</u>

<u>背景信息</u>

<u>配置</u>

<u>网络图</u>

<u>配置</u>

<u>步骤1:确认Snort版本</u> <u>第二步:在Snort 2中创建自定义本地Snort规则</u> <u>第三步:确认自定义本地Snort规则</u> <u>第四步:更改规则操作</u> <u>第五步:将入侵策略与访问控制策略(ACP)规则相关联</u> <u>第六步:部署更改</u>

<u>验证</u>

 未触发自定义本地Snort规则

 步骤1:设置HTTP服务器中的文件内容

 第二步:初始HTTP请求

 触发自定义本地Snort规则

 步骤1:设置HTTP服务器中的文件内容

 第二步:初始HTTP请求

 第二步:初始HTTP请求

 第三步:初始HTTP请求

 第三步:确认入侵事件

<u>故障排除</u>

简介

本文档介绍在防火墙威胁防御(FTD)的Snort2中配置自定义本地Snort规则的过程。

先决条件

要求

Cisco 建议您了解以下主题:

- 思科Firepower管理中心(FMC)
- 防火墙威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科VMWare Firepower管理中心7.4.1
- 思科Firepower 2120 7.4.1

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

自定义本地Snort规则是指用户定义的规则,您可以在集成到FTD的Snort入侵检测和防御系统中创 建和实施。当您在思科FTD中创建自定义本地Snort规则时,您实际上是在定义Snort引擎可以监视 的新模式或条件集。如果网络流量匹配自定义规则中指定的条件,Snort可以采取规则中定义的操作 ,例如生成警报或丢弃数据包。管理员使用自定义本地Snort规则解决一般规则集未涵盖的特定威 胁。

本文档介绍了如何配置和验证旨在检测和丢弃包含特定字符串(用户名)的HTTP响应数据包的自 定义本地Snort规则。



注意:创建自定义本地Snort规则并为其提供支持不属于TAC支持范围。因此,本文档只能

用作参考,并要求您自行决定并自行负责创建和管理这些自定义规则。

配置

网络图

本文档介绍此图中Snort2中的自定义本地Snort规则的配置和验证。



配置

这是用于检测和丢弃包含特定字符串(用户名)的HTTP响应数据包的自定义本地Snort规则的配置 。

步骤1:确认Snort版本

导航到FMC上的设备 > 设备管理,点击设备选项卡。确认Snort版本为Snort2。

Firewall Management C Devices / Secure Firewall Device S	enter Overview Analysis Summary	Policies Devices Objects Integ	ration	Deploy	Q 🥝 🌣 🚱 admin 🗸 🖓
FPR2120_FTD Cisco Firepower 2120 Threat Defense Device Routing Interfaces	Inline Sets DHCP VTEP SN	МР			
General	1 ± +	License	1	System	Ø G
Name:	FPR2120_FTD	Essentials:	Yes	Model:	Cisco Firepower 2120 Threat Defense
Transfer Packets:	Yes	Export-Controlled Features:	Yes	Serial:	JAPPT 1707U2
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	based Rules:	
Device Configuration:	Import Export Download	Secure Client Advantage:	No	Inventory:	View
OnBoarding Method:	Registration Key	Secure Client VPN Only:	No		
Inspection Engine		Health		Management	/ 🔍
Inspection Engine:	Snort 2	Status:	0	Remote Host Address:	1.10%0.25

第二步:在Snort 2中创建自定义本地Snort规则

在FMC上导航到对象 > 入侵规则 > Snort 2所有规则,点击创建规则按钮。

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)		

创建自定义规则

输入自定义本地Snort规则的必要信息。

- 入侵:custom_http_sig
- 操作:警报
- 协议:tcp
- 流:已建立,到客户端
- 内容:用户名(原始数据)

Firewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🙋 🌣 🕢 admin 🗸 diada SECURE
	Search Upload Update Intrusion
Snort 2 All Rules Snort 3 All Rules	
Create New Rule	
Message custom_http_sig	
Classification Etr Classifications	
Action alert •	
Protocol top •	
Direction Bidirectional •	
Source IPs any Source Port any	
Detection Ontione	
flow X	
Established • To Client •	
content ×	
Case Insensitive	
Not Rave Data	
HTTP Header	
HTTP Raw Header	
HTTP Raw Cookle	
HTTP Claim Body	
HTTP Status Message	
HTTP Status Code	
Distance	
VOTEIN	
Offset	
Use Fast Patient Matcher Chi	
Fast Pattern Matcher Offset and Length	
content V Add Option Save As New	

输入规则的必要信息

第三步:确认自定义本地Snort规则

在FMC上导航到策略 > 入侵策略,点击Snort 2版本按钮。

Firewall Management Center Policies / Access Control / Intrusion / Intrusion Policies	Overview Analysis Policies Devices	Objects Integration D	eploy Q 🥝 🔅 🕼 admin ~ 🖞									
Intrusion Policies Network Analysis Policies												
Hide Snort 3 Sync status () Q. Search by Intrusion Policy,	Description, or Base Policy	All IPS Rules	PS Mapping () Compare Policies Create Policy									
Intrusion Policy Description	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 🖌 🖥 🔃 🗑									

确认自定义规则

在FMC上导航到规则 >类别>本地,确认自定义本地Snort规则的详细信息。

Firewall Management Center Policies / Access Control / Intrusion / Edit Policy	Overview Analysis	Policies Devi	ces Objects	Integration	Deploy Q 🥝 🕯	admin ~ admin SECURE						
Intrusion Policies Network Analysis Policies												
Policy Information Rules						< Back						
Cisco Recommendations Rule Configuration > Advanced Settings Category	Filter: Category:"local"	ilter: Category:"local"										
Policy Layers Policy Layers indicator-compromise indicator-obfuscation indicator-scan	O selected rules of 1 Rule State Event	Filtering + Dynamic	State - Alerting	✓ Comments ▼		Policy •						
indicator-shellcode	GID SID	Message + custom_http_sig				→ @▼○ 9 ₩						
malware-onc malware-other malware-tools netbios	Hide details	(0)	_			< < 1 of 1 > > Add ▲						
os-inux os-mohile Classifications	Dynamic Stat	e (0)				Add						
Microsoft Vulnerabilitie Microsoft Worms Platform Specific	> Alerts (0) > Comments (0)				Add SNMP Alert						
Preprocessors Priority Rule Update	✓ Documentatio	rule aiert to	p any any <> any any (s	d:1000001; gid:1; flow:established.to_client; content:"u	isername"; rawbytes; msg:"custom_http_sig"	; classtype:unknown; rev:1;)						

自定义规则详细信息

第四步:更改规则操作

单击State按钮,将State设置为Drop and Generate Events,然后单击OK按钮。

Firewall Manageme Policies / Access Control / In	nt Center ntrusion / Edit Policy c	verview	Analysis	Policies	Devices	Objects	Integration			Deploy	۹	•	0	admin \sim	cisco S	SECURE
Intrusion Policies Network A	nalysis Policies															
Policy Information Rules	Rules															< Back
Cisco Recommendations > Advanced Settings	Rule Configuration Rule Content Category	Filter: Category	ler: Category:"local"												XO	
> Policy Layers	file-pdf indicator-compromise indicator-obfuscation indicator-scan indicator-shellcode	0 selected Rule State	0 selected rules of 1 Rule State • Event Filtering • Dynamic State • Alerting • Comments •							Policy ▼						
	malware-backdoor malware-other malware-other malware-other malware-other malware-other malware-other malware-other malware-other malware-other malware-other malware-other malware-other malware-other malware-other malware-other Microsoft Vulmerabilities Microsoft Worms Platform Specific Provoncesore		1000001	custom_htt	Set rule st State Disabled Drop and C Disabled	ate for "cus vents ionorate Event	tom_http_sig" @						-			

更改规则操作

依次单击Policy Information 按钮和Commit Changes 按钮以保存更改。



提交更改

第五步:将入侵策略与访问控制策略(ACP)规则相关联

导航到FMC上的策略 > 访问控制,将入侵策略与ACP关联。

Editing Rule ftd_acp	Mandatory 🛛 🗙
Name ftd_acp	w 🗸 🖞 Logging ON 🛛 🐻 Time Range None 🗸 Rule Enabled (
Intrusion Po	cy snort_test X V Default-Set X V Shore V
Q Zones (2) Networks Ports Applications 🛕 Users URLs	Dynamic Attributes VLAN Tags
Q Search Security Zone Objects Showing 2 out of 2	Selected Sources: 1 Selected Destinations and Applications: 1
diside_zone (Routed Security Zone)	Collapse All Remove All Collapse All Remove All
A outside_zone (Routed Security Zone)	ZONE V 1 Object Image: state sta

与ACP规则关联

第六步:部署更改

将更改部署到FTD。



部署更改

验证

未触发自定义本地Snort规则

步骤1:设置HTTP服务器中的文件内容

将HTTP服务器端的test.txt文件的内容设置为用户。

第二步:初始HTTP请求

从客户端浏览器(192.168.10.1)访问HTTP服务器(192.168.20.1/test.txt),并确认允许HTTP通信。

6	3	192.	168.2	20.1/	/test.t	xt		×	+	-	٥	×
÷	-	\rightarrow	С		▲				192.168.20.1/test.txt	☆	θ	:
use	r											

初始HTTP请求

触发自定义本地Snort规则

步骤1:设置HTTP服务器中的文件内容

将HTTP服务器端的test.txt文件的内容设置为用户名。

第二步:初始HTTP请求

从客户端浏览器(192.168.10.1)访问HTTP服务器(192.168.20.1/test.txt),并确认已阻止HTTP通信。

) 192.168.20.1	×	+	_	٥	×
\leftrightarrow \rightarrow \times	(i) 192.168.20.1/test	txt		Θ	:

똅

初始HTTP请求

第三步:确认入侵事件

在FMC上导航到分析 > 入侵 > 事件,确认入侵事件由自定义本地Snort规则生成。

Firewall Manageme Analysis / Intrusions / Even	ent Center	Ove	rview	Analysis	Policies	Devices	Objects In	tegration				Deploy	۹	0	¢ 0	admin	i ∨ situalu S	ECURE
								Вс	ookmark This Pa	ge Reporting	Dashboard	View Bo	okmarks	Searc	h Pre	defined	Searches	•
Events By Priority and Classification (metch workfow)																		
II 2024-04-06 09:41:20 - 2024-04-06 11:00:04 Expanding																		
Drilldown of Event, Priority, and	Classification	Table Vi	iew of Ever	nts Paci	kets													
Jump to	_																	
			Inline			Source		Destination	Source	Destination	SSL	VLAN						
• fime x	Priority X Im	npact X	Result ×	Reason X	Source IP X	Country X	Destination IP X	Country	Type	Code	Status X	ID X	Messag	10 X		_	Glassification X	Generab
 2024-04-06 11:05:13 	low 0	Unknown	Dropped		92.168.20.1		9192.168.10.1		80 (http) / tcp	50057 / tcp			custom	_http_s	ig (1:1000	0001:1)	Unknown Traffic	Standar

单击Packets选项卡,确认入侵事件的详细信息。

Firewall Manage Analysis / Intrusions / E	Iment Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🤣 🌣 🚱 admin 🗸 secure
	Bookmark This Page Re	porting Dashboard View Bookmarks Search Predefined Searches V
Events By Priority	and Classification (patient workford)	
		II 2024-04-06 09:41:20 - 2024-04-06 11:07:15 Expanding
Search Constraints (Edit S	earch Save Search)	
Drilldown of Event, Priority,	and Classification Table View of Events Packets	
Event Information		
Message	custom_http_sig (1:100001:1) 2024_04-06 11 06:34	
Classification	Likensen Traffic	
Priority		
Ingress Security Zone	catale 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.bxt	
Intrusion Policy	snort_test	
Access Control Policy	acp-rule	
Access Control Rule	ftd_acp	_
Rule	alert top any any ⇔ any any (sid:1000001; gid:1; flow:established,to_client; content:"username"; rambytes; msg:"custom_http_sig"; classtyme:unknown; rev:1;)
 Actions 		

入侵事件的详细信息

故障排除

运行system support trace命令以确认FTD上的行为。在本示例中,HTTP流量被IPS规则阻止(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

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)。