Configurar regras locais personalizadas de Snort no Snort2 no FTD

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configurar
Diagrama de Rede
<u>Configuração</u>
Etapa 1. Confirmar versão do Snort
Etapa 2. Crie uma regra de Snort local personalizada no Snort 2
Etapa 3. Confirmar regra de Snort local personalizada
Etapa 4. Ação da regra de alteração
Etapa 5. Associar Política de Intrusão à Regra de Política de Controle de Acesso (ACP)
Etapa 6. Implantar alterações
Verificar
A regra de Snort local personalizada não é acionada
Etapa 1. Definir Conteúdo do Arquivo no Servidor HTTP
Etapa 2. Solicitação HTTP inicial
A regra de Snort local personalizada é acionada
Etapa 1. Definir Conteúdo do Arquivo no Servidor HTTP
Etapa 2. Solicitação HTTP inicial
Etapa 3. Evento de Intrusão de Confirmação
Troubleshooting

Introdução

Este documento descreve o procedimento para configurar as Regras locais personalizadas de Snort no Snort2 no Firewall Threat Defense (FTD).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Firepower Management Center (FMC)
- Firewall Threat Defense (FTD)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Firepower Management Center para VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Regra de Snort Local Personalizada refere-se a uma regra definida pelo usuário que você pode criar e implementar no sistema de detecção e prevenção de intrusão Snort integrado ao FTD. Ao criar uma regra Snort local personalizada no Cisco FTD, você está essencialmente definindo um novo padrão ou conjunto de condições que o mecanismo Snort pode observar. Se o tráfego de rede corresponder às condições especificadas em sua regra personalizada, o Snort poderá executar a ação definida na regra, como gerar um alerta ou descartar o pacote. Os administradores usam regras locais personalizadas do Snort para lidar com ameaças específicas não cobertas pelos conjuntos de regras gerais.

Neste documento, você é apresentado como configurar e verificar uma Regra de Snort Local Personalizada projetada para detectar e descartar pacotes de resposta HTTP contendo uma string específica (nome de usuário).



Cuidado: a criação de regras locais personalizadas de Snort e o fornecimento de suporte a elas não faz parte da cobertura de suporte do TAC. Portanto, este documento pode ser usado apenas como referência e peça que você crie e gerencie essas regras personalizadas a seu próprio critério e responsabilidade.

Configurar

Diagrama de Rede

Este documento introduz a configuração e a verificação da Regra de Snort Local Personalizada no Snort2 neste diagrama.



Configuração

Esta é a configuração da Regra de Snort Local Personalizada para detectar e descartar pacotes de resposta HTTP contendo uma string específica (nome de usuário).

Etapa 1. Confirmar versão do Snort

Navegue até Devices > Device Management no FMC e clique na guia Device. A confirmação da versão de snort é Snort2.

Specific Dependence Specific Dependence Our met faces in line Sets DHCP VEP SMP Our met faces in line Sets DHCP VEP SMP Our met faces in line Sets DHCP VEP SMP Our met faces in line Sets DHCP VEP SMP Our met faces in line Sets DHCP VEP SMP Our met faces in line Sets DHCP VEP SMP Our met faces in line Sets DHCP VEP SMP Our met faces in line Sets DHCP VEP SMP Our met faces in line Sets DHCP VEP SMP Section S	Firewall Management C Devices / Secure Firewall Devices	Center Overview Analysis Summary	Policies Devices Objects	Integration	Deploy	Q 🥥 🌣 🕼 admin 🗸 "divide SEC
General Image: Constraint of the second of the secon	FPR2120_FTD Cisco Firepower 2120 Threat Defense Device Routing Interfaces	Inline Sets DHCP VTEP SN	MP			
Name: FPR2120_FDT Transfer Packets: Yes Troubleshoot: Coop CL Controlled Features: Yes Mode: Routed Compliance Mode: None TLS Crypto Acceleration: Enabled Device Configuration: Emort Controllent Fremier: No Device Configuration: Registration Key Inspection Engine: Snot 2	General	/±∓	License	1	System	8 G
Transfer Packets: Yes Troubleshoot: Tog CL Dominant Mode: Routed Compliance Mode: None TLS Crypto Acceleration: Enabled Device Configuration: Engistration Key Inspection Engine: Snot 2 Packets: Yes Secure Client VPN Only: Status: South 2 Status: South 2 Secure Client VPN Only: South 2 <td>Name:</td> <td>FPR2120_FTD</td> <td>Essentials:</td> <td>Yes</td> <td>Model:</td> <td>Cisco Firepower 2120 Threat Defense</td>	Name:	FPR2120_FTD	Essentials:	Yes	Model:	Cisco Firepower 2120 Threat Defense
Troubleshoot: Logi CL Downsolf Malware Defense: Yes Time: 2024-04-06 01:26:12 Mode: Routed IPS: Yes Time: 2024-04-06 01:26:12 Compliance Mode: None Carrier: No Time: 2024-04-06 01:26:12 T.S. Crypto Acceleration: Enabled URL: No Version: 7.4.1 Device Configuration: Emore Teport Downsolf Secure Client Premier: No No Time Zone setting for Time Dut C (UTC+0:00) Secure Client Premier: No Secure Client Advantage: No No Inventory: View Inspection Engine Snot 2 Status: Status: Status: Management Renote Host Address: 1.1010.0.20	Transfer Packets:	Yes	Export-Controlled Features:	Yes	Serial:	JAPATTERUS
Mode:RoutedIPS:YesTime Zone:UTC (UTC+0:00)Compliance Mode:NoneCarrier:NoVersion:7.4.1TLS Crypto Acceleration:EnabledURL:NoTime Zone setting for Time based Rules:UTC (UTC+0:00)Device Configuration:Imort Tiport CommonderSecure Client Premier:NoInventory:Version:Secure Client Advantage:NoSecure Client Advantage:NoInventory:ViewInspection EngineSnot 2Status:Status:ManagementRenote Host Address:1.1010.0.20	Troubleshoot:	Logs CLI Download	Malware Defense:	Yes	Time:	2024-04-06 01:26:12
Compliance Mode: None Carrier: No Version: 7.4.1 TLS Crypto Acceleration: Enabled URL: No Secure Client Premier: No Device Configuration: Import Icont Control Secure Client Premier: No No OnBoarding Method: Registration Key Secure Client VPN Only: No No Inspection Engine: Snot 2 Status: Status: Status:	Mode:	Routed	IPS:	Yes	Time Zone:	UTC (UTC+0:00)
TLS Crypto Acceleration: Enabled URL: No Time Zone setting for Time UTC (UTC+0:00) Device Configuration: Import Icont Secure Client Premier: No No Inventory: View OnBoarding Method: Registration Key Registration Key No No No No Inspection Engine: Snot 2 Status: Status: Status: Management Remote Host Address: 1.101/J.C.C.	Compliance Mode:	None	Carrier:	No	Version:	7.4.1
Device Configuration: Import Configuration: Secure Client Premier: No Inventory: View OnBoarding Method: Registration Key Secure Client VPN Only: No Management View Inspection Engine: Snot 2 Status: Status: Secure Client Address: 1.101:0.0000000000000000000000000000000	TLS Crypto Acceleration:	Enabled	URL:	No	Time Zone setting for Time	UTC (UTC+0:00)
Device Configuration: Import Leport Configuration: Inventory: No OnBoarding Method: Registration Key Secure Client Advantage: No Inspection Engine Health Management Inspection Engine: Snot 2 Status: Import Leport			Secure Client Premier:	No	based Rules:	1 million
OnBoarding Method: Registration Key Secure Client VPN Only: No Inspection Engine Health Management Inspection Engine: Snort 2 Status: Ø	Device Configuration:	Import Export Download	Secure Client Advantage:	No	inventory:	view
Inspection Engine Health Management Inspection Engine: Short 2 Status: Image: Status:	OnBoarding Method:	Registration Key	Secure Client VPN Only:	No		
Inspection Engine Health Management Imagement Inspection Engine: Snort 2 Status: Imagement Remote Host Address: 1.1010.020						
Inspection Engine: Short 2 Status: O Remote Host Address: 1.1010.020	Inspection Engine		Health		Management	/ 🔍
	Inspection Engine:	Snort 2	Status:	0	Remote Host Address:	1.105.0.25

Versão do Snort

Etapa 2. Crie uma regra de Snort local personalizada no Snort 2

Navegue até Objects > Intrusion Rules > Snort 2 All Rules no FMC, clique no botão Create Rule.

Firewall Management Center Objects / Intrusion Rules / Snort 2 All Rules	Analysis Policies	s 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			

Criar Regra Personalizada

Insira as informações necessárias para a Regra de Snort Local Personalizada.

- Intrusão : custom_http_sig
- Ação : alerta
- Protocolo : tcp
- fluxo : Estabelecido, Para o cliente
- conteúdo : nome de usuário (dados brutos)

Firewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🥝 🌣 🚱 admin 🗸 👶 SECURE
Snort 2 All Rules Snort 3 All Rules	Search Upload Update Intrusion
Create New Rule	

Inserir informações necessárias para a regra

Etapa 3. Confirmar regra de Snort local personalizada

Navegue para Policies > Intrusion Policies no FMC, clique no botão Snort 2 Version.

Firewall Management Center Policies / Access Control / Intrusion / Intrusion Policies	Overview Analysis Policies Devices	Objects Integration	Deploy Q 🥝 🌣 🕻	admin v diada SECURE
Intrusion Policies Network Analysis Policies				
Hide Snort 3 Sync status 🜒 🔍 Search by Intrusion Polic	y, Description, or Base Policy	All IPS F	Rules IPS Mapping 🜒 Com	pare Policies Create Policy
Intrusion Policy Description	Base Policy	Usage Information		
snort_test → Snort 3 is in sync with Snort 2. 2024-01-12	Balanced Security and Connectivit	1 Access Control Policy No Zero Trust Application Policy 1 Device	Snort 2 Version	Snort 3 Version 📝 🖥 🔃 🗑

Confirmar regra personalizada

Navegue até Rules > Category > local no FMC e confirme os detalhes de Custom Local Snort Rule.

Firewall Manageme Policies / Access Control / I	ent Center o Intrusion / Edit Policy	Overview Analysis	Policies Devices	Objects Integration	Dept	oy Q 👩 🕴	¢ 0	admin v disto S	ECURE
Intrusion Policies Network A	Analysis Policies								
Policy Information	Rules								< Back
Cisco Recommendations	Rule Configuration	Filter:							
> Advanced Settings	Category	Category:"local"							XØ
> Policy Layers	hle-pdf indicator-compromise indicator-obfuscation	0 selected rules of 1 Rule State Event Fi	iltering - Dynamic State	e ▼ Alerting ▼ Comments ▼			Policy		•
	indicator-scan indicator-shellcode	GID SID	Message 4				+		-
	local malware-backdoor	1 1000001	custom_http_sig				\rightarrow		
	malware-cnc								
	malware-tools	Hide details					KK	1 of 1 >	21
	netbios os-linux	> Suppressions	(0)					Add	^
	< mohile	> Dynamic State	(0)					Add	
	Classifications Microsoft Vulnerabilities	Alerts (0)						Add SNMP Alert	
	Microsoft Worms Platform Specific	Comments (0)						Add	
	Preprocessors	 Documentation 	n						
	Priority Dulo Update								- 0
	Rule Opdate		rule alert top any a	any <> any any (sid:1000001; gid:1; flow:	established,to_client; content:"username"; rawbytes; m	sg:"custom_http_sig"	; classtype:u	nknown; rev:1;)	*

Detalhes da regra personalizada

Etapa 4. Ação da regra de alteração

Clique no botão State, defina o estado como Drop and Generate Events e clique no botão OK.

Firewall Manageme Policies / Access Control / I	ent Center c	Verview	Analysis	Policies	Devices	Objects	Integration	Deplo	y Q	0	° 0	admin v	cisco	SECURE
Intrusion Policies Network A	Analysis 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 r Rule State	rules of 1 • Event F	Filtering v	Dynamic State	 Alerting 	Comments +				Polic	/		¥
	indicator-shellcode local malware-backdoor	_ GID	SID 1000001	Message custom_h	+ nttp_sig								Y 0 (
	malware-cnc malware-other malware-tools				Set rule s	tate for "cu	stom_http_sig" 🕜							
	os-linux os-mobile				State Disabled		¥							
	Classifications Microsoft Vulnerabilities Microsoft Worms				Generate Drop and Disabled	Events Generate Even	nts Cancel OK							
	Platform Specific Preprocessors													

Alterar a ação da regra

Clique no botão Informações da política, clique no botão Confirmar alterações para salvar as alterações.



Confirmar alterações

Etapa 5. Associar Política de Intrusão à Regra de Política de Controle de Acesso (ACP)

Navegue para Policies > Access Control no FMC, associe Intrusion Policy ao ACP.

1 Citing Rule ftd_acp	Mandato	iry 🛛 🗙
Name [ftd_acp 1 Action C Allow	r V Logging ON K Time Range None V Rule Enable	ed 💽
Intrusion Polic	y snort_test X V Default-Set X V Kone	
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	1
inside_zone (Routed Security Zone)	Collapse All Remove All Collapse All Rem	move All
dutside_zone (Routed Security Zone)	ZONE • 1 Object inside_zone • 1 Object	
Associar à Regra de ACP		

Etapa 6. Implantar alterações

Implante as alterações no FTD.

Firewall Management Center Overview Analysis Policies Devices Objects Integration		Deploy Q 🙆 🌣 🕢 admin v dada.	SECURE
⇒ Return to Access Control Policy Management acp-rule ✓	۹	Advanced Deploy All Ignore warnings Deploy All	Legacy UI Save
Packets → Prefitter Rules → Decryption → Security Intelligence → Identity → Access Control More	FPR2120_FTD	Ready for Deployment	1 device

Implantar alterações

Verificar

A regra de Snort local personalizada não é acionada

Etapa 1. Definir Conteúdo do Arquivo no Servidor HTTP

Defina o conteúdo do arquivo test.txt no lado do servidor HTTP como usuário.

Etapa 2. Solicitação HTTP inicial

Acesse o Servidor HTTP (192.168.20.1/test.txt) a partir do navegador do cliente (192.168.10.1) e confirme se a comunicação HTTP é permitida.

J	0	192.1	68.20.1	1/test.txt	×	+	-	٥	×
	←	\rightarrow	G	▲		192.168.20.1/test.txt	☆	θ	:
ι	iser								

Solicitação HTTP inicial

A regra de Snort local personalizada é acionada

Etapa 1. Definir Conteúdo do Arquivo no Servidor HTTP

Defina o conteúdo do arquivo test.txt no lado do servidor HTTP como nome de usuário.

Etapa 2. Solicitação HTTP inicial

Acesse o Servidor HTTP (192.168.20.1/test.txt) a partir do navegador do cliente (192.168.10.1) e confirme se a comunicação HTTP está bloqueada.





Solicitação HTTP inicial

Etapa 3. Confirmar evento de intrusão

Navegue para Analysis > Intrusions > Events no FMC, confirme se o evento de intrusão é gerado pela regra de snort local personalizada.

Firewall Management Analysis / Intrusions / Events	Center o	werview	Analysis	Policies	Devices	Objects Ir	ntegration				Deploy	Q	0 ¢ (adm	in ~ cisco SE	CURE
							B	ookmark This Pa	ge Reporting	Dashboard	I View Bo	okmarks	Search	Predefine	d Searches	Y
Events By Priority and Classification (seatch workford)																
Search Constraints (Edit Search S	Search Constraints (Edit Search Save Search)															
Drilldown of Event, Priority, and Cla	ssification Table	View of Even	nts Pack	ets												
Jump to]															
🗌 🕹 Time X 🛛 Pri	ority 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	e ×		Classification X	Generab
▼ 2024-04-06 11:05:13 lov	O Unknown	Dropped		9192.168.20.1		0 192.168.10.1		80 (http) / tcp	50057 / tcp			custom	_http_sig (1:1	1000001:1)	Unknown Traffic	Standar

Evento de intrusão

Clique na guia Packets e confirme os detalhes do Intrusion Event.

Firewall Manage Analysis / Intrusions / E	errent Center Overview Analysis Policies Devices Objects Integration Deploy Q 📀 🌣 🚱 admin - v viewe SECURE
	Bookmark: This Page Reporting Dashboard View Bookmarks Search Predefined Searches •
Events By Priority	and Classification (netro, montrail)
Search Constraints (Edit S	earch Save Search)
Drilldown of Event, Priority,	and Classification Table View of Events Packets
- Event Information	
Message	custom_intp_sej (1:100001:1) 2924-04-061 106:34
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	Aest.txt
Intrusion Policy	snort_test
Access Control Policy	acp-rule
Access Control Rule	fid_acp
Rule	alert top any any ⇔ any sid:1000001; gid:1; flor:established.to_client:`usernaee": rawbytes: msg:`custom_http_pig`; classtyse:unknown; rev:1;)
 Actions 	

Detalhes do evento de intrusão

Troubleshooting

Execute system support trace o comando para confirmar o comportamento no FTD. Neste exemplo, o tráfego HTTP é bloqueado pela regra IPS (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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.