# 在FMC中使用Packet Tracer工具重新運行資料包

### 目錄

 簡介

 必要條件

 蓋求

 採用元件

 使用FMC中提供的Packet Tracer工具重新運行資料包

 使用PCAP檔案重新執行封包

 使用此選項的限制

 相關檔案

### 簡介

本檔案介紹如何使用FMC GUI Packet Tracer工具在FTD裝置上重新執行封包。

### 必要條件

需求

思科建議您瞭解以下主題:

- Firepower技術知識
- 瞭解透過防火牆的資料包流

採用元件

- Cisco Secure Firewall Management Center (FMC)和Cisco Firewall Threat Defense (FTD) 7.1或更高版本。
- PCAP格式的資料包捕獲檔案

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設) )的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

# 使用FMC中提供的Packet Tracer工具重新運行資料包

1. 登入FMC GUI。轉至Devices > Troubleshoot > Packet Tracer。

	Firewall Management Center Overview Devices / Troubleshoot / Packet Tracer	Analysis Policies	Devices Objects Integ	ration	Deploy Q 🚱 🌣 🛛	admin ~ citethe SECURE
Trace History	New Trace       +         Select Device*       10.197.224.9         Select the packet type from the Protocol drop-down, and         Protocol*       TCP       or         Source Type*       IPv4	elect a PCAP File (0-65535) (0-65535)	Device Management NAT QoS Platform Settings FlexConfig Certificates	VPN Site To Site Remote Access Dynamic Access Policy Troubleshooting	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture Upgrade Threat Defense Upgrade Chassis Upgrade	CLI Packet Capture
	Treat the simulated packet as an IPsec/SSL VPN deep Treat the simulated packet as a sec of the simulated packet	crypted packet				Reset
	Trace Result					¶a ⊗ ⊠

### 2. 提供源、目標、協定、入口介面的詳細資訊。按一下「追蹤」。

마	Firewall Manager Devices / Troubleshoot /	Packet Tracer Overview Analysis Policies Devices	Objects Integration Deploy Q 🌍 🌣 🚱 admin 🗸 👘 SECURE
Ш			File Download   Threat Defense CLI   Packet Capture
Tra	New Trace +	-	
ice His	Select Device*	10.70.73.44 🗸	Ingress Interface* Select V C
story	Select the packet type	e from the Protocol drop-down, and then specify the packet parameters.	VLAN ID (1-4096)
	Protocol*	ICMP V or Select a PCAP File V	
	Source Type*	IPv4 v 192.168.1.2	Destination Type* IPv4 V 10.197.226.1
	Type*	8 (Echo Request)	ID (1-65535)
	Code*	0 (0-255)	
	Inline Tag	(0-65533)	
	<ul> <li>Bypass security c</li> </ul>	hecks for the simulated packet	Allow the simulated packet to transmit from the device
	Treat the simulate	ed packet as an IPsec/SSL VPN decrypted packet	Reset
	Trace Result		R ×

3. 使用Allow the simulated packet to transmit from the device選項,從裝置重新執行此資料包。 4. 請注意,資料包被丟棄,因為訪問控制策略中有已配置的丟棄ICMP資料包的規則。

D	Firewall Management Co Devices / Troubleshoot / Packet Tr	enter Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	6003	¢ 0	admin $\vee$	cisco	SECURE		
													Reset	Т	race		
	Trace Result: ODROP											¶a ⊗ ≫					
Tra	Packet Details: 11:59:51.23	3 - 192.168.1.2 > 10.106.2	26.1 ICMP														
ce His	PC(vrfid:0)																
tory	> 🤣 ACCESS-LIST																
		esolve Egress Interface															
	- O ACCESS-LIST   log																
	Type:	ACCESS-LIST															
	Subtype:	log															
	Result:	O DROP															
	Config:	access-group CSM_FW list CSM_FW_ACL_ rem	_ACL_ global ark rule-id 268	access-list C 8454920: AC	SM_FW_ACL_ CESS POLICY:	advanced der Port-scan tes	ny object-group ICM t Mandatory access-	MP_ALLOW ifc PC -list CSM_FW_AC	any ifc OU CL_ remark	T any rule-i	rule-id 2 d 26845	684549 4920: L	20 event-log 4 RULE: block	flow-sta ICMP	art access-		
	Additional Information																
	🗸 😑 Result: drop																
	Input Interface:	PC(vrfid:0)															
	Input Status:	up															
	Input Line Status:	up															
	Output Interface:	OUT(vrfid:0)															
	Output Status:	up															
	Output Line Status:	up															
	Action:	drop															
	Drop Reason:	(acl-drop) Flow is denied	ed by configur	red rule													
	Drop Detail:	, Drop-location: frame 0	x000000aaac	dc0eb0 flow (	(NA)/NA												
	OUT(vrfid:0)																

#### 5. 使用TCP資料包的此Packet Tracer將獲得跟蹤的最終結果(如圖所示)。

þ	Firewall Management Center         Overview         Analysis         Policies         Devices	Objects Integration Deploy Q 🌮 🛠 🕢 admin 🗸 👘 SECURE
 ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	New Trace +	File Download   Threat Defense CLI   Packet Capture
ace History	Select Device*     10.70.73.44       Select the packet type from the Protocol drop-down, and then specify the packet parameters.       Protocol*       TCP       or       Select a PCAP File	Ingress Interface*         PC - Ethermet1/1         C           VLAN ID         (1-4096)
	Source Type*         IPv4         192.168.1.2           Source Port*         1234         (0-65535)           Inline Tag         (0-65533)	Destination Type*         IPv4         I0.197.226.1           Destination Port*         443         (0-65535)
	Bypass security checks for the simulated packet Bypass security checks for the simulated packet Treat the simulated packet as an IPsec/SSL VPN decrypted packet	Allow the simulated packet to transmit from the device           Reset         Trace
	Trace Result: O ALLOW	¶u ⊗ ×
	PC(vrfid:0) PC(vrfid:0) OTE-LOOKUP   Resolve Egress Interface	
	> Ø ACCESS-LIST   log > Ø CONN-SETTINGS	

### 使用PCAP檔案重新執行封包

您可以使用「選取PCAP檔案」按鈕來上傳pcap檔案。然後選擇Ingress介面並按一下Trace。

	Firewall Manage Devices / Troubleshoot	ement Center t / Packet Tracer	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 💧	<b>*</b> ¢ (	admin	cisco	SECURE
 7	New Trace 3	+								File Down	nload	Threat D	efense CLI	Packet Ca	apture
ace History	Select Device* Select the packet ty Protocol*	10.197.224.9 ppe from the Protocol dr	op-fown, and t	hen specify the	packet parar	neters.	Ingress I VLAN ID	nterface*	outside - GigabitEthern	net0/1 (1-4096)		∨ C			
	Source Type* Source Port* Inline Tag	IPv4	ort number (0-65533)	~ (0	)-65535)	]	Destinati Destinati	on Type* on Port*	IPv4 ~	number		<ul><li>✓ (0-</li></ul>	65535)		
	<ul> <li>Bypass security</li> <li>Treat the simula</li> </ul>	checks for the simulate	d packet SSL VPN decry	pted packet			Allow	v the simulate	ed packet to transmit from	n the device	e		Res	et Tr	ace
	Trace Result													¶a ⊗	×

# 使用此選項的限制

- 1. 我們只能模擬TCP/UDP資料包。
- 2. PCAP檔案中支援的最大資料包數為100。
- 3. Pcap檔案大小必須小於1 MB。

- 4. PCAP檔案名稱不得超過64個字元(包括副檔名),且只能包含英數字元、特殊字元(「。」
  - 、「-」、「\_」)或同時包含兩者。
- 5. 目前僅支援單一流量封包。

#### 跟蹤3將丟棄原因顯示為無效IP報頭

(ch	Firewall Managem	nent Center	Overview Anal	sis Policies	Devices Obje	cts Integration		Deploy Q	¢ 😜	admin ~	cise	SECURE
	Select the packet type	from the Protocol dro	op-down, and then spe	city the packet par	rameters. VI	LAN ID		(1-4096)				
ш	Protocol*	UDP ~	v or single2.pcap	~								
Tra	Source Type*	IPv4 V	/ 192.168.29.58		De	estination Type*	IPv4 🗸	192.168.29.16	0			
ce Hi	Source Port*	60376		✓ (0-65535)	De	estination Port*	161		~ (	0-65535)		
story	Inline Tag		(0-65533)									
	Bypass security ch	ecks for the simulated	d packet			Allow the simulate	d packet to transmit fron	n the device				
	Treat the simulated	i packet as an IPsec/S	SSL VPN decrypted pa	ket								
										Reset		Trace
	Trace Result:										F <u>la</u>	$\approx$ ×
	Packet 1: 11:58:21.875534 Packet Details: 11:58:21.875534 192.168.29.58:60376 > 192.168.29.160:161 udp 80											
		inside	e(vrfid:0)									
		🗸 😑 Result:	t: drop									
		Inpu	out Interface: aut Status:	inside(vrfid:0)								
		Inpu	ut Line Status:	up								
		Out	tput Interface:	NP Identity Ifc								
		Acti	tion: ne Taken:	drop								
		Dro	op Reason:	(invalid-ip-hea	ader) Invalid IP header							
		Dro	op Detail:	Drop-location:	frame 0x000055f7cfb1	b71b flow (NA)/NA						
		NP Ide	entity Ifc									
			oney no									

### 相關檔案

有關資料包捕獲和跟蹤器的詳細資訊,請參閱<u>Cisco Live文檔</u>。

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。