FMCのパケットトレーサツールを使用したパケ ットのリプレイ

内容
 はじめに
 前提条件
 要件
 使用するコンポーネント
 FMCで使用可能なパケットトレーサツールを使用してパケットをリプレイします。
 PCAPファイルを使用してパケットを再生します。
 このオプションの使用に関する制限
 関連資料

はじめに

このドキュメントでは、FMC GUIのPacket Tracerツールを使用して、FTDデバイスでパケットを リプレイする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FirePOWER の知識
- ファイアウォールを通過するパケットフローの知識

使用するコンポーネント

- Cisco Secure Firewall Management Center(FMC)およびCisco Firewall Threat Defense(FTD)バージョン7.1以降
- pcap形式のパケットキャプチャファイル

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

FMCで使用可能なパケットトレーサツールを使用してパケット をリプレイします。 1. FMC GUIにログインします。Devices > Troubleshoot > Packet Tracerの順に選択します。

	Devices / Troubleshoot	/ Packet Tracer	Overview	Analysis	Policies	Devices	Objects	Integration	D	eploy	ର୍ 🚱 🔅 🔞	admin ~ doubt SECURE
 =	New Trace	÷				Device I	Management	VPN Site To Site	9	Trou	bleshoot Download	CLI Packet Capture
ace History	Select Device* Select the packet typ Protocol* Source Type*	10.197.224.9 be from the Protocol driver of the Protocol drivero driver of the Protocol dri	op-down, and	then specify the specify the specify the specify the specify the specific s	ne packet paran	QoS Platform FlexCon Certifica	n Settings fig ites	Remote Ac Dynamic A Troublesho	ccess occess Palicy noting	Pack Pack Upgr Three	ket Tracer ket Capture rade eat Defense Upgrade	
	Source Port* Inline Tag Bypass security o	Enter or select a po checks for the simulate ed packet as an IPsec/	ort number (0-65533) ed packet SSL VPN decr) ypted packet	(0-65535)		Allow	the simulated packet	t to transmit from	Cha	e	Reset
	Trace Result											¶a ⊗ X

2. 送信元、宛先、プロトコル、入力インターフェイスの詳細を入力します。[トレース]をクリ ックします。

	Firewall Manager Devices / Troubleshoot /	nent Center c	Overview Analysi	s Policies	Devices	Objects	Integration		Deploy	۹ 🕻	P 0	admin ~	cisco SECUR	E
н Т	New Trace +	-							File Dow	mload	Threat De	efense CLI	Packet Capture	
ace History	Select Device* Select the packet type	10.70.73.44 e from the Protocol drop-(v down, and then specif) y the packet para	meters.	Ingress In VLAN ID	nterface*	Select	(1-4096))	√ C			
	Protocol* Source Type*	ICMP ~	or Select a PCAP	File 🗸 🕻		Destinatio	on Type*	IPv4 ~	10.197.	226.1	_			
	Type*	8 (Echo Request)	~	Ĵ		ID			(1-6553	5)				
	Code* Inline Tag	0	(0-255) (0-65533)											
	 Bypass security cl Treat the simulate 	hecks for the simulated particle of the simu	acket VPN decrypted packe	t		Allow	the simulate	ed packet to transmit fror	n the devie	ce		Rese	t] Trace	
	Trace Result												₽ <u></u>	9

- 3. Allow the simulated packet to transmit from the device to replay this packet from the deviceのオプションを使用します。
- 4. アクセスコントロールポリシーにICMPパケットをドロップするための設定済みルールがあ るため、パケットがドロップされたことを確認します。

Fir	rewall Management C vices / Troubleshoot / Packet T	enter Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	6 ⁰⁰ ¢	0	admin ~	cisco	SEC	URE
													Rese		Trace	
1	frace Result: 😑 DROP													F2	\approx	×
B	Packet Details: 11:59:51.23	33 - 192.168.1.2 > 10.106.2	26.1 ICMP													
	PC(vrfid:0)															
» 🥑	ACCESS-LIST															
» 🥑	INPUT-ROUTE-LOOKUP R	esolve Egress Interface														
~ 0	ACCESS-LIST log															
- T	Type:	ACCESS-LIST														
	Subtype:	log														
	Result:	O DROP														
	Config:	access-group CSM_FW list CSM_FW_ACL_ rem	ACL_ global // ACL_ global	access-list C 8454920: AC	SM_FW_ACL_ CESS POLICY:	advanced de Port-scan tes	ny object-group ICMF t Mandatory access-I	P_ALLOW ifc PC list CSM_FW_AC	any ifc OL L_ remark	T any i rule-i	rule-id 2 d 268454	684549 920: L	20 event-log 4 RULE: bloc	g flow-s k ICMP	tart a	ce
	Additional Information															
~ 0	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 deni	ed by configu	red rule												
	Drop Detail:	, Drop-location: frame (0x000000aaac	dc0eb0 flow	NA)/NA											
	OUT(vrfid:0)															

5. TCPを使用したこのパケットトレーサは、トレースの最終結果をパケット化します(図を参

	Firewall Manager	Packet Tracer Ove	rview Analysis	Policies Dev	vices Objects	Integration	Deploy Q	6 😳 🗘 🕜 admin 🗸	cisco SECURE
 , ,	New Trace	-					File Download	d Threat Defense CLI	Packet Capture
n Hi	Select Device*	10.70.73.44	×		Ingress Int	erface* PC - Ethernet1		~ C	
story	Select the packet typ	e from the Protocol drop-dov	wn, and then specify th	e packet parameters	VLAN ID		(1-4096)		
	Protocol*	TCP v or	Select a PCAP File	× 0					
	Source Type*	IPv4 ~ 1	92.168.1.2		Destination	n Type* IPv4	√ 10.197.226.	1	
	Source Port*	1234	~	(0-65535)	Destination	n Port* 443		(0-65535)	
	Inline Tag	(0-	-65533)						
	Bypass security of the secu	hecks for the simulated pack	et		Allow t	the simulated packet to trans	mit from the device		
	Treat the simulate	ed packet as an IPsec/SSL VP	N decrypted packet					Reset	Trace
	Trace Result: 🕑 AL								₽ ≈ ×
	Packet Details: 12	:03:30.612 - 192.168.1.2:12	34 > 10.197.226.1:443	3 TCP					
	PC(vrfid:0)								
>	INPUT-ROUTE-LO	OKUP Resolve Egress Interfa	ace						
>	ACCESS-LIST Io	9							

PCAPファイルを使用してパケットを再生します。

pcapファイルをアップロードするには、[PCAPファイルを選択]ボタンを使用します。次に、入力 インターフェイスを選択して、Traceをクリックします。

þ	Firewall Manag Devices / Troublesho	ement Center Overview	Analysis Policies D	Devices Objects	Integration	Deploy Q	🌮 🌣 🛛 🛛	admin ~ dudu cisco	SECURE
 _	New Trace 3	+				File Downloa	d Threat Defe	nse CLI Packet C	apture
ace History	Select Device* Select the packet Protocol* Source Type* Source Port*	10.197.224.9 type from the Protocol drop - town, and or Se IPv4 - Enter or select a port number	d then specify the packet parameter Hect a PCAP File (0-65535)	Ingress I ers. VLAN ID Destinati Destinati	on Type* IPv4 On Port* Enter or sele	gabitEthernet0/1 (1-4096)	✓ C ✓ (0-65	535)	
	Inline Tag Bypass securit Treat the simul	(0-6553) y checks for the simulated packet lated packet as an IPsec/SSL VPN dec	3) crypted packet	Allov	v the simulated packet to tra	insmit from the device		Reset	race ∞ ×
								_	

このオプションの使用に関する制限

- 1. TCP/UDPパケットのみをシミュレートできます。
- 2. PCAPファイルでサポートされるパケットの最大数は100です。
- 3. Pcapファイルのサイズは1 MB未満にする必要があります。
- 4. PCAPファイル名は64文字(拡張子を含む)以内で、英数字、特殊文字(「。」、「-」、 「_」)、またはその両方を含める必要があります。
- 5. 現時点では、単一のフローパケットのみがサポートされています。

トレース3に、ドロップの理由が無効なIPヘッダーとして表示されています

þ	Firewall Manager Devices / Troubleshoot /	ment Center Packet Tracer	Overview Analysi	s Policies Devices	Objects Integration		Deploy Q 🍪 🛱	admin ~ "livelit" SECURE
	Select the packet typ	e from the Protocol drop	o-down, and then speci	y the packet parameters.	VLAN ID		(1-4096)	
m	Protocol*		or single2.pcap	\sim				
Trac	Source Type*	IPv4 🗸	192.168.29.58		Destination Type*	IPv4 🗸	192.168.29.160	
ен	Source Port*	60376	``	(0-65535)	Destination Port*	161	~	(0-65535)
story	Inline Tag		(0-65533)					
	Bypass security of	hecks for the simulated	packet		Allow the simulated	d packet to transmit from	m the device	
	Treat the simulate	ed packet as an IPsec/SS	SL VPN decrypted pack	et				Reset Trace
	Trace Result: 🤑 Err	or: Some packets from th	he PCAP file were not re	played.				¶a ☆ ×
I	Packet 1: 11:58:21.	875534 Packet Packet Packet Packet Packet Inpu Inpu Outp Actit Time Drop Drop Drop	t Details: 11:58:21.8755 vrfid:0) drop t Interface: t Status: t Line Status: out Interface: on: a Taken: p Reason: b Detail: ntity Ifc	34 192.168.29.58:60376 > 19 inside(vrfid:0) up NP Identity Ifc drop 0 ns (invalid-ip-header) Invalid I Drop-location: frame 0x0000	92.168.29.160:161 udp 80 P header 955f7cfb1b71b flow (NA)/NA			

パケットキャプチャとトレーサの詳細については、<u>Cisco Liveドキュメント</u>を参照してください 。 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。