Replay a Packet Using Packet Tracer Tool in FMC

Contents

Introduction

This document describes how you can replay a packet in your FTD device using FMC GUI Packet Tracer tool.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Firepower technology
- Knowledge of Packet flow through the Firewall

Components Used

- Cisco Secure Firewall Management Center (FMC) and Cisco Firewall Threat Defense (FTD) version 7.1 or later.
- Packet capture files in pcap format

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Replay the packet using packet tracer tool available on FMC

1. Login to FMC GUI. Go to Devices > Troubleshoot > Packet Tracer.

	Firewall Manager Devices / Troubleshoot /	ment Center / Packet Tracer	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	୍ 🚰 🌣 🔞	admin \vee	cisco SECURE
Trace History	New Trace 4 Select Device* Select the packet typ Protocol* Source Type* Source Port* Inline Tag	+ 10.197.224.9 to from the Protocol drop TCP V IPv4 Enter or select a port	o-down, and t or Solar number	✓ ✓ Hen specify t ta PCAP File ✓ ✓	he packet paran	Device M NAT QoS Platform FlexConf Certificat	tanagement Settings Ng Res	VPN Site To Remote Dynami Trouble	Site Access c Access Policy shooting		Troubleshoot File Download Fireat Defense CLI Packet Tracer Packet Capture Upgrade Threat Defense Upgrade Chassis Upgrade	CLI P:	scket Capture
	Bypass security checks for the simulated packet Treat the simulated packet as an IPsec/SSL VPN decrypted packet						Allow t	he simulated par	cket to transmit fro	om the d	evice	Reset	Trace
	Trace Result												€ ⊗ X

2. Provide the details of the source, destination, protocol, ingress interface. Click Trace.

Ð	Firewall Manage Devices / Troubleshoot	Ment Center Overview Analysis Policies D	Devices Objects	Integration	Deploy 🔍 🍄 🌣 🔞 adm	nin ~ diada SECURE					
Ш					File Download Threat Defense Cl	I Packet Capture					
Tra	New Trace	+									
ice His	Select Device*	10.70.73.44 ~	Ingre:	s Interface*	Select V C						
tory	Select the packet typ	pe from the Protocol drop-down, and then specify the packet parameter	ers. VLAN	ID	(1-4096)						
	Protocol*	ICMP v or Select a PCAP File v 0									
	Source Type*	IPv4 v 192.168.1.2	Destin	nation Type*	□Pv4 ∨ 10.197.226.1						
	Type*	8 (Echo Request) V	ID		(1-65535)						
	Code*	0 (0-255)									
	Inline Tag	(0-65533)									
	Bypass security	checks for the simulated packet	🗹 A	Allow the simulated packet to transmit from the device							
	Treat the simulat	ed packet as an IPsec/SSL VPN decrypted packet				Reset					
	Trace Result					n_ ∀ 11					

- 3. Use the option of Allow the simulated packet to transmit from the device to replay this packet from the device.
- 4. Observe that the packet was dropped because there is a configured rule in Access control policy to drop ICMP packets.

	Firewall Management Ce Devices / Troubleshoot / Packet Tra	enter Overview	Analysis	Policies	Devices	Objects	Integration	Deplo	y C	λ 💕	[∞] ¢	0	admin \vee	cisco	SECURE
													Reset		Trace
	Trace Result: 😑 DROP													F <u>B</u>	× ×
Trace History	 Packet Details: 11:59:51.233 PC(vrfid:0) ACCESS-LIST 	3 - 192.168.1.2 > 10.106.2	26.1 ICMP												
	> O INPUT-ROUTE-LOOKUP Re	ACCESS-LIST log DROP access-group CSM_FW, list CSM_FW_ACL_ rem	_ACL_ global ark rule-id 268	access-list C 3454920: ACG	SM_FW_ACL_ CESS POLICY: 1	advanced der Port-scan test	y object-group ICM Mandatory access-	IP_ALLOW ifc PC any ifc list CSM_FW_ACL_ ren	OUT ar ark rule	ny rule- e-id 26	-id 268 845492	45492 20: L4	20 event-log I RULE: block	flow-s	tart access-
	 Result: drop Input Interface: Input Status: Input Line Status: Output Interface: Output Status: Output Line Status: Action: Drop Reason: Drop Detail: OUT(vrfid:0) 	PC(vrfid:0) up OUT(vrfid:0) up drop (acl-drop) Flow is denie , Drop-location: frame 0	ad by configur x00000aaaca	red rule dc0eb0 flow (NA)/NA										

5. This packet tracer with TCP packets the final result of the trace (as shown).

þ	Firewall Management Center Devices / Troubleshoot / Packet Tracer	Overview A	analysis Policies	Devices	Objects In	ntegration		Deploy	۹ 💕	° (admin v	cisco SE	CURE
ш								File Dow	nload	Threat D	Defense CLI	Packet Cap	ture
z	New Trace +												
ace His	Select Device* 10.70.73.44		×.		Ingress Inter	face*	PC - Ethernet1/1			~ C			
tory	Select the packet type from the Protocol dr	rop-down, and then	specify the packet param	neters.	VLAN ID			(1-4096)					
	Protocol*	v or Select a l	PCAP File 🛛 🗸 🗿										
	Source Type* IPv4	Destination 1	Гуре*	IPv4 V	10.197.	226.1							
	Source Port* (0-65535)					Port*	443		- - 	(0-65535)			
	Inline Tag	(0-65533)											
	 Bypass security checks for the simulate 	ed packet			Allow the simulated packet to transmit from the device								
	 Treat the simulated packet as an IPsec/ 	SSL VPN decrypted	packet										
											Reset	Trac	е
	Trace Result: 🥑 ALLOW											¶∎ ⇒	\times
	Packet Details: 12:03:30.612 - 192.168	.1.2:1234 > 10.197.	226.1:443 TCP										
	PC(vrfid:0)												
	> O INPUT-ROUTE-LOOKUP Resolve Egres	s Interface											
	ACCESS-LIST log												
	> 📀 CONN-SETTINGS												

Replay the packets using PCAP file

You can upload the pcap file using the Select a PCAP File button. Then select the Ingress interface and click on Trace.

þ	Firewall Manage Devices / Troubleshoo	ement Center d t / Packet Tracer	Overview Anał	ysis Policies	Devices	Objects Inte	egration	Deploy	९ 🌮 ¢	admin 🗸	cisco SECURE		
 7	New Trace 3	+						File Down	load Thre	at Defense CLI	Packet Capture		
ace History	Select Device* Select the packet the Protocol*	10.197.224.9 ype from the Protocol drop-	fown, and then spe or Select a PCA	Cify the packet para	meters.	Ingress Interface* outside - GigabitEthernet0/1 VLAN ID (1-4096)							
	Source Type* Source Port* Inline Tag	IPv4	umber (0-65533)	✓ (0-65535)		Destination Ty Destination Po	ppe* IPv4 Enter or select	(0-65535)					
	Bypass security Treat the simula	r checks for the simulated pated packet as an IPsec/SSL	acket VPN decrypted par	cket		Allow the	simulated packet to tran	nsmit from the device	Đ	Reset	Trace		
	Trace Result										¶a ⊗ X		

Limitations of using this option

- 1. We can only simulate TCP/UDP packets.
- 2. The maximum number of packets supported in a PCAP file is 100.
- 3. Pcap file size must be less than 1 MB.

- 4. The PCAP file name must not exceed 64 characters (extension included) and must only contain alphanumeric, special characters (".", "-", "_"), or both.
- 5. Only a single flow packets are supported currently.

The Trace 3 is showing drop reason as invalid ip header

마	Firewall Managen Devices / Troubleshoot /	nent Center Packet Tracer	Overview	Analysis	Policies	Devices	Objects	Integration		D	eploy	۹ 💕	₽¢ (admin ~	cisco	SECURE
	Select the packet type from the Protocol drop-down, and then specify the packet parameters.							VLAN ID (1-4096)								
ш	Protocol*	UDP	or single	e2.pcap	\sim											
Trac	Source Type*	IPv4 v	192.168.2	9.58			Destinati	on Type*	IPv4	\sim	192.168	.29.160				
ен	Source Port*	60376		~ (0-65535)		Destinati	Destination Port* 161					V (0-	65535)		
istory	Inline Tag		(0-65533)													
Bypass security checks for the simulated packet																
	Treat the simulated packet as an IPsec/SSL VPN decrypted packet Reset Trace												Trace			
	Trace Result: 49 Erro	r: Some packets from	the PCAP file v	vere not replay	ved.										r <u>a</u>	× ×
	Packet 1: 11:58:21.8	75534 😼 Packe	t Details: 11:5	8:21.875534 1	92.168.29.58	3:60376 > 192.1	168.29.160:16	31 udp 80								
		Result Presult Presult Inp Inp Out Act Tirr Dro Dro Constant No Idde	(vrfid:0) : drop ut Interface: ut Status: ut Line Status: put Interface: ion: e Taken: p Reason: p Detail: entity Ifc	ins up up dro 0 n (in Dro	ide(vrfid:0) Identity Ifc yp s valid-ip-heac yp-location: fr	der) Invalid IP h Jarme 0x000055	eader f7cfb1b71b Ռ	ow (NA)/NA								

Related Documents

For more information on Packet captures and tracers, please refer Cisco Live Document.