Relire un paquet à l'aide de l'outil Packet Tracer dans FMC

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Relire le paquet à l'aide de l'outil Packet Tracer disponible sur FMC
Rediffusion des paquets à l'aide du fichier PCAP
Limites de l'utilisation de cette option
Documents associés

Introduction

Ce document décrit comment vous pouvez relire un paquet dans votre périphérique FTD à l'aide de l'outil Packet Tracer de l'interface graphique FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la technologie Firepower
- Connaissance du flux de paquets dans le pare-feu

Composants utilisés

- Cisco Secure Firewall Management Center (FMC) et Cisco Firewall Threat Defense (FTD) version 7.1 ou ultérieure.
- Fichiers de capture de paquets au format pcap

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Relire le paquet à l'aide de l'outil Packet Tracer disponible sur FMC

1. Connectez-vous à l'interface FMC. Accédez à Périphériques > Dépannage > Packet Tracer.

ഥ	Firewall Manag Devices / Troubleshor	ement Center at / Packet Tracer	Overview	Analysis	Policies	Devices	Objects	Integrati	on	Depl	ay (Q 🚱 🌣 🔞	admin ∨	cisco SECURE
ш Та	New Trace	+				Device I NAT OpS	Management		VPN Site To Site Remote Access		Troubl File D Threa	leshoot Jownload at Defense CLI	CLI Pr	acket Capture
ice Hi	Select Device*	10.197.224.9		~		Platform	Settings		Dynamic Access Policy		Packe	et Tracer		
story	Select the packet type from the Protocol drop-down, and then specify the packet param					FlexCon	FlexConfig Troubleshooting			Packe	et Capture	1		
	Protocol* TCP v or			Select a PCAP File 🛛 🗸		Certificates					Upgra	ade		
	Source Type*	IPv4	~								Threa	at Defense Upgrade		
	Source Port*	Enter or select a	port number	~ ((0-65535)						Chase	sis Upgrade		
	Inline Tag		(0-65533)											
	Bypass security checks for the simulated packet				Allow the simulated packet to transmit from the device									
	Treat the simulated packet as an IPsec/SSL VPN decrypted packet													
													Reset	Trace
	Trace Result													n ⊹ × .

2. Fournissez les détails de la source, de la destination, du protocole et de l'interface d'entrée. Cliquez sur Trace.

þ	Firewall Management Center Overview Analysis Policies Devices	Objects Integration Deploy Q 6 admin V (the SECURE					
ш	New Trace +	File Download Threat Defense CLI Packet Capture					
Trace Histor	Select Device* 10.70.73.44 Select the packet type from the Protocol drop-down, and then specify the packet parameters.	Ingress Interface* Select VI AN ID (1-4096)					
~	Protocol* ICMP or Select a PCAP File Image: Comparison of the select a processing of the sel	Destination Type* IPv4 V 10.197.226.1					
	Type* 8 (Echo Request)	ID (1-65535)					
	Code* 0 (0-255) Inline Tag (0-65533)						
	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						

- 3. Utilisez l'option Autoriser le paquet simulé à transmettre à partir du périphérique pour relire ce paquet à partir du périphérique.
- 4. Notez que le paquet a été abandonné car une règle configurée dans la stratégie de contrôle d'accès permet d'abandonner les paquets ICMP.



5. Ce traceur de paquets avec des paquets TCP génère le résultat final du suivi (comme illustré).

(C)	Firewall Management Center Devices / Troubleshoot / Packet Tracer Overview Analysis Policies Device	s Objects Integration Deploy Q 🚱 🌣 🕢 admin V 🖓
 ₹	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 O	Ingress Interface* PC - Ethermet1/1 VLAN ID (1-4096)
	Source Type* IPv4 I122.168.1.2 Source Port* 1234 (0-65535) Inline Tag (0-65533)	Destination Type* IPv4 V 10.197.226.1 Destination Port* 443 V (0-65535)
	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: ALLOW Ib Packet Details: 12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP Ib PC(vrfid:0) PC(vrfid:0) PC(vrfid:0) Ib PC(vrfid:0)	%

Rediffusion des paquets à l'aide du fichier PCAP

Vous pouvez télécharger le fichier PCAP à l'aide du bouton Sélectionner un fichier PCAP. Sélectionnez ensuite l'interface d'entrée et cliquez sur Trace.

P	Firewall Manag Devices / Troubleshoo	ement Center Overview Analysis Policies Devi	es Objects Integration Deploy Q 崎 🋱 🍘	admin ~ doub SECURE
111	New Trace 3	+	File Download Threat Do	fense CLI Packet Capture
ace History	Select Device* Select the packet t Protocol* Source Type* Source Port* Inline Tag	10.197.224.9 ype from the Protocol drop-fown, and then specify the packet parameters. TCP IPv4 Enter or select a port number (0-65533)	Ingress Interface* outside - GigabitEthernet0/1 VLAN ID (1-4096) Destination Type* IPv4 (0-6 Destination Port* Enter or select a port number (0-6	35535)
	Bypass securit Treat the simul	y checks for the simulated packet ated packet as an IPsec/SSL VPN decrypted packet	Allow the simulated packet to transmit from the device	Reset Trace
	Trace Result			na ⊗ ×

Limites de l'utilisation de cette option

- 1. Nous ne pouvons simuler que des paquets TCP/UDP.
- 2. Le nombre maximal de paquets pris en charge dans un fichier PCAP est de 100.
- 3. La taille du fichier Pcap doit être inférieure à 1 Mo.
- 4. Le nom du fichier PCAP ne doit pas dépasser 64 caractères (extension incluse) et ne doit contenir que des caractères alphanumériques, des caractères spéciaux («.», «-», «_») ou les deux.
- 5. Actuellement, un seul flux de paquets est pris en charge.

Le Trace 3 affiche la raison de suppression comme en-tête IP non valide

	Firewall Managem Devices / Troubleshoot / F	nent Center Packet Tracer	Overview	Analysis	Policies Devices	Objects Integration		Deploy Q 🍄 🕻	admin v dialia	SECURE		
	Select the packet type	from the Protocol drop	p-down, and the	in specify the p	packet parameters.	VLAN ID		(1-4096)				
ш	Protocol*	UDP ~	or single2	.рсар	\sim							
Trac	Source Type*	IPv4 🗸	192.168.29.	58		Destination Type*	IPv4 🗸	192.168.29.160				
ie His	Source Port*	60376		~ (0-	65535)	Destination Port*	161	~	(0-65535)			
story	Inline Tag		(0-65533)									
	Bypass security ch	ecks for the simulated	packet			Allow the simulated packet to transmit from the device						
	Treat the simulated	d packet as an IPsec/SS	SL VPN decrypte	ed packet								
									Reset	frace		
	Trace Result: 🕴 Error: Some packets from the PCAP file were not replayed.											
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(vrfid:0) Result: drop Input Interface: inside(vrfid:0) Input Line Status: up Input Line Status: up Output Interface: NP Identity Ifc Action: drop Time Taken: 0 ns Drop Reason: (Invalid-ip-head Drop Detail: Drop-location: fr NP Identity Ifc					header i5f7cfb1b71b flow (NA)/NA						

Documents associés

Pour plus d'informations sur les captures de paquets et les traceurs, veuillez vous reporter au document <u>Cisco Live Document.</u>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.