FMC에서 Packet Tracer Tool을 사용하여 패킷 재 생

목차

소개

이 문서에서는 FMC GUI Packet Tracer 툴을 사용하여 FTD 디바이스에서 패킷을 재생하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- firepower 기술에 대한 지식
- 방화벽을 통과하는 패킷 흐름에 대한 지식

사용되는 구성 요소

- Cisco FMC(Secure Firewall Management Center) 및 Cisco FTD(Firewall Threat Defense) 버 전 7.1 이상
- pcap 형식의 패킷 캡처 파일

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

FMC에서 사용 가능한 패킷 추적기 툴을 사용하여 패킷 재생

1. FMC GUI에 로그인합니다. Devices > Troubleshoot > Packet Tracer로 이동합니다.

	Firewall Management Center Overview Analysis Policies Devices / Troubleshoot / Packet Tracer	Devices Objects Inte	egration	Deploy Q 🚱 🌣 🕼	admin ~ thethe SECURE
Trace History	New Trace + Select Devloe* 10.197.224.9 Select the packet type from the Protocol drop-down, and then specify the packet part Protocol* TCP Source Type* IPv4 Source Port* Enter or select a port number Inline Tag (0-65535) Bypass security checks for the simulated packet	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 decrypted packet				Reset
	Trace Result				¶a ⊗ ⊠

2. 소스, 목적지, 프로토콜, 인그레스 인터페이스에 대한 세부사항을 제공합니다. Trace(추적)를 클릭합니다.

þ	Firewall Managen Devices / Troubleshoot /	nent Center Packet Tracer	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	Q	¢ 🧠	admin	 diala secure 	
111	New Trace +									File Dow	nload	Threat	Defense CLI	Packet Capture	
race History	Select Device* Select the packet type	10.70.73.44 e from the Protocol drop	p-down, and t	✓ hen specify the	e packet parar	neters.	Ingress II VLAN ID	nterface*	Select	(1-4096)	√ C			
	Protocol* Source Type*	ICMP ~	or Select	t a PCAP File	~ 0		Destinati	on Type*	IPv4 V	10.197	.226.1				
	Type*	8 (Echo Request)		~			ID			(1-6553	5)				
	Code*	0	(0-255)												
	Inline Tag		(0-65533)												
	Bypass security checks for the simulated packet						Allow	the simulate	ed packet to transmit from	n the devi	ce				
	Treat the simulate	d packet as an IPsec/S	SL VPN decry	pted packet									R	eset Trace	
	Trace Result													≞ ∀ 55	

- 3. 시뮬레이션된 패킷이 디바이스에서 전송되도록 허용 옵션을 사용하여 디바이스에서 이 패킷을 재생합니다.
- 4. ICMP 패킷을 삭제하도록 액세스 제어 정책에 구성된 규칙이 있으므로 패킷이 삭제되었는지 확인합니다.

Dev	rices / Troubleshoot / Packet Tr	racer Overview	Analysis	Policies	Devices	Objects	Integration	D	eploy	Q	6 ¢	0	admin y	et	Trace	CUR
															muco	~
т	race Result: 😑 DROP													6	\approx	\times
1	Packet Details: 11:59:51.23	33 - 192.168.1.2 > 10.106.	226.1 ICMP													
	PC(vrfid:0)															
» 🥑	ACCESS-LIST															
> 🥑	INPUT-ROUTE-LOOKUP R	esolve Egress Interface														
~ 0	ACCESS-LIST log															
1	Type:	ACCESS-LIST														
	Subtype:	log														
		-														
	Result:	DROP														
	Result: Config:	DROP access-group CSM_FV list CSM_FW_ACL_ ren	/_ACL_ global nark rule-id 268	access-list CS 8454920: ACC	SM_FW_ACL_ CESS POLICY:	advanced der Port-scan tes	ny object-group ICMP_ Mandatory access-lis	ALLOW ifc PC any t CSM_FW_ACL_	y ifc OUT remark	⊺any n rule-id	ule-id 26 268454	84549 920: L4	20 event-l RULE: blo	og flow-: ock ICMF	start a	aco
	Result: Config: Additional Information	DROP access-group CSM_FV list CSM_FW_ACL_ ren	V_ACL_ global nark rule-id 268	access-list C 8454920: ACC	SM_FW_ACL_ CESS POLICY:	advanced der Port-scan tes	ny object-group ICMP_ t Mandatory access-lis	ALLOW ifc PC any t CSM_FW_ACL_	y ifc OUT remark	f any n rule-id	ule-id 26 268454	84549 920: L4	20 event-l RULE: blo	og flow-: ock ICMF	start a	acc
~ 0	Result: Config: Additional Information Result: drop	DROP access-group CSM_FV list CSM_FW_ACL_ rer	V_ACL_ global nark rule-id 268	access-list C 8454920: ACC	SM_FW_ACL_ CESS POLICY:	advanced der Port-scan tes	ny object-group ICMP_ Mandatory access-lis	ALLOW ifc PC any t CSM_FW_ACL_	y ifc OUT remark	⊺any n rule-id	ule-id 26 268454	84549 920: L4	20 event-l RULE: blo	og flow-: ock ICMF	start a	aco
~ 😑	Result: Config: Additional Information Result: drop Input Interface:	DROP access-group CSM_FV list CSM_FW_ACL_ ren PC(vrfid:0)	V_ACL_ global nark rule-id 268	access-list CS 8454920: ACC	SM_FW_ACL_ CESS POLICY:	advanced der Port-scan tes	ny object-group ICMP_ Mandatory access-lis	ALLOW ifc PC any t CSM_FW_ACL_	y ifc OUT remark	f any n rule-id	ule-id 26 268454	84549 920: L4	20 event-l RULE: bk	og flow-: ock ICMF	start a	ace
~ 0	Kesuit: Config: Additional Information Resuit: drop Input Interface: Input Status:	DROP access-group CSM_FV list CSM_FW_ACL_ ren PC(vrfid:0) up	V_ACL_ global nark rule-id 26/	access-list C 8454920: ACC	SM_FW_ACL_ CESS POLICY:	advanced der Port-scan tes	ny object-group ICMP_ Mandatory access-lis	ALLOW ifc PC any t CSM_FW_ACL_	y ifc OUT remark	Γany n rule−id	ule-id 26 268454	84549 920: L4	20 event-I I RULE: bk	og flow-: ock ICMF	start a	acc
~ 0	Kesuit: Config: Additional Information Resuit: drop Input Interface: Input Status: Inout Line Status:	DROP access-group CSM_FV list CSM_FW_ACL_rer PC(vrfid:0) up up	V_ACL_ global nark rule-id 26i	access-list CS 8454920: ACC	SM_FW_ACL_ CESS POLICY:	advanced der Port-scan tes	ny object-group ICMP_ Mandatory access-lis	ALLOW ifc PC any t CSM_FW_ACL_	y ifc OUT remark	⊺any n rule-id	ule-id 26 268454	84549 920: L4	20 event-l	og flow-: ock ICMF	start a	aco
~ 0	Result: Config: Additional Information Result: drop Input Interface: Input Status: Input Line Status: Output Interface:	DROP access-group CSM_FV list CSM_FW_ACL_ ren PC(vrfid:0) up UD OUT(vrfid:0)	V_ACL_ global nark rule-id 26i	access-list CS 8454920: ACC	SM_FW_ACL_ CESS POLICY:	advanced der Port-scan tes	ny object-group ICMP_ Mandatory access-lis	ALLOW ifc PC any t CSM_FW_ACL_	y ifc OUT remark	⊺any n rule-id	ule-id 26 268454	84549 920: L4	20 event-I	og flow-: ock ICMF	start a	acc
~ 0	Result: Config: Additional Information Result: drop Input Interface: Input Status: Input Line Status: Output Interface: Output Status:	DROP access-group CSM_FV list CSM_FW_ACL_ren PC(vrfd:0) up UP OUT(vrfd:0) up	V_ACL_ global nark rule-id 26i	access-list C 8454920: ACC	SM_FW_ACL_ CESS POLICY:	advanced der Port-scan tes	ty object-group ICMP_ Mandatory access-lis	ALLOW ifc PC any t CSM_FW_ACL_	y ifc OUT remark	⊺any n rule-id	ule-id 26 268454	84549 920: L4	20 event-I	og flow-: ock ICMF	start a	aco
~ 0	Result: Config: Additional Information Result: drop Input Interface: Input Status: Output Interface: Output Interface: Output Status: Output Status:	DROP access-group CSM_FV list CSM_FW_ACL_ ren PC(vrfid:0) up OUT(vrfid:0) up UUT(vrfid:0) up up	V_ACL_ global nark rule-id 26i	access-list C3 8454920: ACC	SM_FW_ACL_ CESS POLICY:	advanced der Port-scan tes	ny object-group ICMP_ Mandatory access-lis	ALLOW ifc PC any t CSM_FW_ACL_	y ifc OUT remark	f any n rule-id	ule-id 26	84549 920: L4	20 event-l	og flow-: ock ICMF	start a	acc
~ 🖸	Result: Config: Additional Information Result: drop Input Interface: Input Status: Input Line Status: Output Interface: Output Status: Output Status: Output Line Status: Action:	DROP access-group CSM_FV list CSM_FW_ACL_ ren PC(vrfid:0) up OUT(vrfid:0) up OUT(vrfid:0) up drop	V_ACL_ global nark rule−id 26i	access-list C3	SM_FW_ACL_ CESS POLICY:	advanced der Port-scan tes	ny object-group ICMP_ Mandatory access-lis	ALLOW ifc PC any	y ifc OUT remark	⊺any n rule-id	ule-id 26	84549 920: L4	20 event-1 I RULE: bk	og flow-:	start a	acc
~ 0	Result: Config: Additional Information Result: drop Input Interface: Input Status: Input Line Status: Output Status: Output Status: Output Status: Output Line Status: Action: Drop Reason:	DROP access-group CSM_FV list CSM_FW_ACL_rer PC(vrfd:0) up up OUT(vrfd:0) up up drop (acl-drop) Flow is den	V_ACL_ global nark rule-id 26i	access-list CS 8454920: ACC	SM_FW_ACL_ CESS POLICY:	advanced der Port-scan tes	ıy object-group ICMP_ Mandatory access-lis	ALLOW ifc PC any	y ifc OUT remark	⊺any n rule-id	ule-id 26	84549 920: L4	20 event-I	og flow-:	start a	acc

5. 이 패킷 추적기는 TCP 패킷과 함께 추적의 최종 결과입니다(표시된 대로).

œ	Firewall Managen Devices / Troubleshoot /	nent Center Overview Analysis Policies	Devices Objects Integration Deploy C	k 🍪 🌣 🕲 admin 🗸 🖓 secure
ш	New Trace +		File Downlo	ad Threat Defense CLI Packet Capture
Trace History	Select Device*	10.70.73.44 V e from the Protocol drop-down, and then specify the packet para	Ingress Interface* PC - Ethernet1/1 meters. VLAN ID (1-4096)	~ C
	Protocol* Source Type* Source Port*	TCP or Select a PCAP File 0 IPv4 192.168.1.2 (0-65535)	Destination Type* IPv4 v 10.197.226 Destination Port* 443	3.1 (0-65535)
	Inline Tag Bypass security cl Treat the simulate	(0-65533) hecks for the simulated packet d packet as an IPsec/SSL VPN decrypted packet	Allow the simulated packet to transmit from the device	
	Trees Decute			Reset Trace
3	Trace Result: ALL Packet Details: 12: PC(vrfid:0) OINPUT-ROUTE-LOC OACCESS-LIST log OCONN-SETTINGS	203:30.612 - 192. I68.1.2:1234 > 10.197.226.1:443 TCP DKUP Resolve Egress Interface		*8 ⊗ X

PCAP 파일을 사용하여 패킷 재생

Select a PCAP File(PCAP 파일 선택) 버튼을 사용하여 pcap 파일을 업로드할 수 있습니다. 그런 다 음 Ingress 인터페이스를 선택하고 Trace(추적)를 클릭합니다.

þ	Firewall Management Center Devices / Troubleshoot / Packet Tracer Overview Analysis Policies Device	s Objects Integration Deploy Q 🌮 🌣 🍘 admin 🗸 👘 SECURE
 	New Trace 3 +	File Download Threat Defense CLI Packet Capture
ace History	Select Device* 10.197.224.9 Select the packet type from the Protocol drop- fown, and then specify the packet parameters. Protocol* TCP Source Type* IPv4 Source Port* Enter or select a port number Inline Tag (0-65533)	Ingress Interface* outside - GigabitEthernet0/1 VLAN ID (1-4096) Destination Type* IPv4 V Destination Port* Enter or select a port number 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
	Trace Result	¶a ⊗ X

이 옵션 사용의 제한 사항

- 1. TCP/UDP 패킷만 시뮬레이션할 수 있습니다.
- 2. PCAP 파일에서 지원되는 최대 패킷 수는 100입니다.
- 3. Pcap 파일 크기는 1MB 미만이어야 합니다.
- 4. PCAP 파일 이름은 64자(확장자 포함)를 초과할 수 없으며 영숫자, 특수 문자(".", "-", "_") 또는 둘 다만 포함해야 합니다.
- 5. 현재 단일 플로우 패킷만 지원됩니다.

추적 3에서 삭제 이유를 잘못된 ip 헤더로 표시하고 있습니다.

þ	Firewall Manager Devices / Troubleshoot / F	ent Center Packet Tracer	Overview Analys	is Policies Devices	Objects Integration	Deploy Q 🂕	admin ~ distribution SECURE
	Select the packet type	from the Protocol dro	p-down, and then spec	ty the packet parameters.	VLAN ID	(1-4096)	
ш	Protocol*	UDP ~	or single2.pcap	~			
Trac	Source Type*	IPv4 v	192.168.29.58		Destination Type*	IPv4 ∨ 192.168.29.160	
e His	Source Port*	60376		(0-65535)	Destination Port*	161 🗸	(0-65535)
tory	Inline Tag		(0-65533)				
	Bypass security ch	ecks for the simulated	l packet		Allow the simulated	d packet to transmit from the device	
	Treat the simulated	I packet as an IPsec/S	SL VPN decrypted pack	et			Reset
	Trace Result: 🔒 Error	: Some packets from	the PCAP file were not r	eplayed.			¶a ☆ ≫
	Packet 1: 11:58:21.87	75534 😼 Packe	et Details: 11:58:21.875	534 192.168.29.58:60376 > 19	2.168.29.160:161 udp 80		
		Result Inpi Inpi Inpi Out Act Tim Dro Dro	(vrfid:0) : drop ut Interface: ut Status: ut Line Status: iput Interface: ion: the Taken: the Taken	inside(vrfid:0) up up NP Identity Ifc drop 0 ns (invalid-ip-header) Invalid IF Drop-location: frame 0x0000	P header 55f7cfb1b71b flow (NA)/NA		

관련 문서

패킷 캡처 및 추적기에 대한 자세한 내용은 <u>Cisco Live Document를 참조하십시오.</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.