Firepower 데이터 경로 문제 해결 1단계: 패킷 인 그레스

목차

소개 플랫폼 가이드 패킷 인그레스 문제 해결 단계 해당 트래픽 식별 연결 이벤트 확인 인그레스 및 이그레스 인터페이스에서 패킷 캡처 SFR - ASA 인터페이스에서 캡처 FTD(비 SSP 및 FPR-2100) - 인그레스 및 이그레스 인터페이스에서 캡처 FTD(SSP) - 논리적 FTD 인터페이스에서 캡처 인터페이스 오류 확인 SFR - ASA 인터페이스 확인 FTD(비 SSP 및 FPR-2100) - 인터페이스 오류 확인 FTD(비 SSP 및 FPR-2100) - 인터페이스 오류 확인 FTD(SSP) - 인터페이스 오류를 찾기 위한 데이터 경로 탐색 Cisco TAC(Technical Assistance Center)에 제공할 데이터 다음 단계: Firepower DAQ 레이어 문제 해결

소개

이 문서는 Firepower 시스템의 데이터 경로 문제를 체계적으로 해결하여 Firepower의 구성 요소가 트래픽에 영향을 미치는지 여부를 확인하는 방법을 설명하는 일련의 문서 중 일부입니다. Firepower 플랫폼의 아키텍처에 대한 자세한 내용은 <u>개요 문서</u>를 참조하고 다른 데이터 경로 문제 해결 문서에 대한 링크를 참조하십시오.

이 문서에서는 Firepower 데이터 경로 문제 해결의 1단계인 패킷 인그레스 단계를 살펴봅니다.



플랫폼 가이드

다음 표에서는 이 문서에서 다루는 플랫폼에 대해 설명합니다.

플랫폼 코드 이름	설명	적용 가능 하드웨 어 플랫폼	참고
SFR	FirePOWER 서비스(SFR) 모듈이 설치된 ASA	ASA 5500-X 시 리즈	해당 없음
FTD(비 SSP 및 FPR-2100) FTD(SSP)	ASA(Adaptive Security Appliance) 또는 가상 플랫폼에 설치된 Firepower Threat Defense(FTD) 이미지 FXOS(Firepower eXtensible Operative	ASA-5500-X 시 리즈, 가상 NGFW 플랫폼 FPR-9300, FPR-	해당 없음 2100 시리즈는 FXOS

System) 기반 섀시에 논리적 디바이스로 설 치된 FTD 섀시 관리자를 사용하 지 않음

패킷 인그레스 문제 해결 단계

첫 번째 데이터 경로 문제 해결 단계는 패킷 처리의 인그레스 또는 이그레스 단계에서 삭제가 발생 하지 않는지 확인하는 것입니다. 패킷이 인그레스되고 있지만 이그레스되지 않는 경우라면 패킷이 데이터 경로 내의 특정 위치에서 디바이스에 의해 패킷이 삭제되고 있거나 디바이스가 이그레스 패 킷을 생성할 수 없는 것입니다(예: ARP 항목 누락).

해당 트래픽 식별

패킷 인그레스 단계의 문제를 해결하는 첫 번째 단계는 문제가 있는 트래픽과 관련된 플로우 및 인 터페이스를 격리하는 것입니다. 여기에는 다음 항목이 포함됩니다.

 플로우 정보
 인터페이스 정보

 프로토콜
 소스 IP 주소

 Source Port(소스 포트)
 인그레스 인터페이스

 대상 IP
 이그레스 인터페이스

 Destination Port(대상 포트)

예를 들면 다음과 같습니다.

TCP inside 172.16.100.101:38974 outside 192.168.1.10:80

팁: 소스 포트는 각 플로우에서 종종 다르기 때문에 정확한 소스 포트를 식별하지 못할 수도 있지만, 대상(서버) 포트로 충분합니다.

연결 이벤트 확인

플로우 정보뿐만 아니라 트래픽이 일치해야 하는 인그레스 및 이그레스 인터페이스에 대한 아이디 어를 얻은 후, Firepower가 플로우를 차단하고 있는지 여부를 확인하는 첫 번째 단계는 해당 트래픽 에 대한 연결 이벤트를 확인하는 것입니다. 이는 Firepower Management Center의 **분석 > 연결 >** 이벤트에서 확인할 수 있습니다.

참고: 연결 이벤트를 확인하기 전에 액세스 제어 정책 규칙에서 로깅이 활성화되어 있는지 확 인하십시오. 로깅은 각 액세스 제어 정책 규칙의 "로깅" 탭과 보안 인텔리전스 탭에서 설정합 니다. 의심스러운 규칙이 로그를 "이벤트 뷰어"로 전송하도록 설정되었는지 확인합니다.

ontext E	Analysis Polic	ies Devices Obje	acts / /	AMP Inte Files •	Higence Hosts • User	s Vuln	erabilities • Corr	elation •	Custom • Loo	kup • Search			Deploy	🤱 System Help 🕶	Global \ admin 🔻			
												Bookmark This Pa	ge Report Desi	gner Dashboard View Boo	kmarks Search •			
Connection Events (with workfree) ii 2017-05-11 13-54-32 O																		
> Search Constraints (<u>Sd:Search</u>)																		
Jump to •																		
	 First Packet 	Last Packet	Action	Reason	Initiator IP	<u>Lountry</u>	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application			
	2017-05-11 14:54:32	2017-05-11 14:55:02	Allow		192.168.1.200		73.173.197.235	JUSA			60084 / tcp	80 (http) / tcp	HTTP :	Web browser	Web Browsing			
	2017-05-11 14:54:02	2017-05-11 14:54:32	Allow		192.168.1.200		11 73.173.197.235	SA USA			60082 / tcp	80 (http) / tcp	HTTP	Web browser	Web Browsing			
- 0	2017-05-11 14:53:40	2017-05-11 14:53:55	Allow		192.168.1.200		10.83.181.139				60077 / tcp	135 (loc-srv) / tcp	DCE/RPC	Epmag				
	2017-05-11 14:52:40	2017-05-11 14:52:55	Allow		192.168.1.200		# 10.83.181.139				60069 / tcp							
	2017-05-11 14:51:40	2017-05-11 14:51:53	Allow		192.168.1.200		10.83.181.139				60064 / tcp	Connection Events		(unnamed search)		Private	Save Save As New	Search
	2017-05-11 14:51:24	2017-05-11 14:51:24	Allow		192 168 1 200		172 217 26 206	III USA			60058 / tro	Sections		Networking				
	2012 05 11 11 50 10	2012 05 11 14 50 55	Allow					1000 States			40054 (http://	General Information		Initiator IPa	192.168.1.200	+	192.168.1.0/24, 1192.168.1.3, 7	2001.108
· U	2017-02-11 14:50:40	2017-05-11 14:50:55	ALC:N		192.108.1.200		ME 10.83.181.139				950/20 / tcp	Networking		Responder IP*		*	192.168.1.0/24, 1192.168.1.3, 2	/001:db8
	2017-05-11 14:50:24	2017-05-11 14:50:24	Allow		192.168.1.200		172.217.26.206	usa usa			60050 / tcp	Device		Initiator / Responder IP			192.168.1.0/24, 1192.168.1.3, 4	2001.000
	2017-05-11 14:50:23	2017-05-11 14:50:53	Allow		192.168.1.200		73.173.197.235	USA USA			60051 / tcp	55L		Initiator / Original Client IP			192.168.1.0/24, 1192.168.1.3,	2001:08-8
	2017-05-11 14:49:47	2017-05-11 14:49:47	Allow		192.168.1.200		172.217.26.206	JUSA			60043 / tcp	Application		Initiator / Responder / Original Cli	ert IP		192.168.1.0/24, 1192.168.1.3, 7	2001.008
	2017-05-11 14:49:40	2017-05-11 14:49:55	Allow		192.168.1.200		10.83.181.139				60046 / tcp	URL		Ingress Security Zone		*	My Security Zone	
	2012.05.11.14.48.44	2012.05.11.14.51.22	Allow		102 168 1 200						60041 / http	Qe5		Egress Security Zone Ingress / Egress Security Zone			My Security Zone My Security Zone	
	2017-02-11 11:10:10	2017-02-11 14-21-12	Chinese .								5000TA / 500			Source Port / ICMP Type			1-1024, 6000-6011, 100	
• •	2017-05-11 14:48:46	2017-05-11 14:49:16	Allow		192.108.1.200		MB /3.1/3.19/.235	1050			50040 / tcp	+ New Search		Destination Port / ICMP Code*			1-1024, 6000-6011, 180	
	2017-05-11 14:48:40	2017-05-11 14:48:55	Allow		192.168.1.200		10.83.181.139				60037 / tcp	Global		Protocol* DNS Duery			top, udp suspicious.com. evil*	
	2017-05-11 14:48:32	2017-05-11 14:48:32	Allow		192.168.1.200		172.217.26.206	USA USA			60031 / tcp	SuperConnectionTest		DNS Response			NEDOMAIN	
	2017-05-11 14:48:16	2017-05-11 14:48:46	Allow		192.168.1.200		m 73.173.197.235	USA			60034 / tcp	Predefined Searches		DNS Record Type			A, PTR	
	2017-05-11 14:47:46	2017-05-11 14:48:16	Allow		192.168.1.200		# 73.173.197,235	usa			60030 / tcp			DNS TTL			43200	
	2012-05-11 14:47:40	2012-05-11 14-47-55	Allow		102 168 1 200		10 83 181 130				60027 / http	Possible Delabese Access		DNS Sinkhole Name HTTP Response Code			My Sinkhole 200	
• 0	2017-02-11 14:47:40	2017-02-11 14:47:55	ALC: N		B 124.168.1.200		98 10.02.181.139				930.27.7.900	Risky Applications with Lov	v business	VLAN ID			10	
• •	2017-05-11 14:47:15	2017-05-11 14:48:46	Allow		ME 192.168.1.200		團 72.246.56.169	USA			60022 / tcp			Geolocation				
	2017-05-11 14:47:15	2017-05-11 14:47:45	Allow		192.168.1.200		73.173.197.235	USA USA			60021 / tcp	Standard Hall		Initiator Country			USA, United States, United*	
	2017-05-11 14:46:45	2017-05-11 14:47:15	Allow		# 192.168.1.200		73.173.197.235	USA			60017 / tcp	Standard SSL		Responder Country			USA, United States, United*	
			_											Original Client Country			USA, United States, United*	
at login o	n Tuesday, 2017-04-25 at	12:42:21 PM from rtp-flipk	ey-88111.	cisco.com										Initiator / Responder Country			USA, United States, United*	

위의 예에서는 "검색 편집"을 클릭하고 고유한 소스(이니시에이터) IP를 필터로 추가하여 Firepower에서 탐지되고 있던 플로우를 확인합니다. 작업 열에 이 호스트 트래픽에 대해 "허용"이 표시됩니다.

Firepower에서 의도적으로 트래픽을 차단하는 경우 작업에 "차단"이라는 단어가 포함됩니다. "연결 이벤트의 테이블 보기"를 클릭하면 추가 데이터가 제공됩니다. 작업이 "차단"인 경우 연결 이벤트에 서 다음 필드를 확인하면 됩니다.

- 이유
- 액세스 제어 규칙

이는 해당 이벤트의 다른 필드와 함께 트래픽을 차단하는 구성 요소의 범위를 좁히는 데 도움이 될 수 있습니다.

액세스 제어 규칙 문제 해결에 대한 보다 자세한 내용을 보려면 <u>여기</u>를 클릭하십시오.

인그레스 및 이그레스 인터페이스에서 패킷 캡처

연결 이벤트에 "허용" 또는 "신뢰"라는 규칙 작업이 표시되었음에도 불구하고 이벤트가 없거나 여전 히 Firepower에서 차단하는 것으로 의심되는 경우, 데이터 경로 문제 해결을 계속합니다.

다음은 위에서 언급한 다양한 플랫폼에서 인그레스 및 이그레스 패킷 캡처를 실행하는 방법에 대한 지침입니다.

SFR - ASA 인터페이스에서 캡처

SFR 모듈은 단순히 ASA 방화벽에서 실행되는 모듈이므로 먼저 ASA의 인그레스 및 이그레스 인터 페이스에서 캡처하여 인그레스되는 동일한 패킷이 이그레스되는지 확인하는 것이 가장 좋습니다.

이 <u>문서</u>에는 ASA에서 캡처를 수행하는 방법에 대한 지침이 포함되어 있습니다.

ASA에 인그레스되는 패킷이 이그레스되지 않는 것으로 확인된 경우, 문제 해결의 다음 단계(DAQ 단계)를 계속 진행합니다.

참고: ASA 인그레스 인터페이스에서 패킷이 확인되면 연결된 디바이스를 확인하는 것이 좋습 니다.

FTD(비 SSP 및 FPR-2100) - 인그레스 및 이그레스 인터페이스에서 캡처

비 SSP FTD 디바이스에서의 캡처는 ASA에서의 캡처와 유사합니다. 그러나 CLI 초기 프롬프트에 서 직접 캡처 명령을 실행할 수 있습니다. 삭제된 패킷의 문제를 해결할 때 캡처에 "추적" 옵션을 추 가하는 것이 좋습니다.

다음은 포트 22에서 TCP 트래픽에 대한 인그레스 캡처를 설정하는 예입니다.

> capture <u>ssh_traffic</u> trace interface inside match <u>tcp</u> any any <u>ea</u> 22 > show capture <u>ssh_traffic</u>
7 packets captured
1: 01:17:38.498906 192.168.62.70.48560 > 10.83.180.173.22: S 4250994241:4250994241(0) win 29200 <pre>mss</pre>
2: 01:17:38.510898 10.83.180.173.22 > 192.168.62.70.48560: S 903999422:903999422(0) ack 4250994242 win
3: 01:17:38.511402 192.168.62.70.48560 > 10.83.180.173.22: . ack 903999423 win 229 <nop.nop.timestamp< td=""></nop.nop.timestamp<>
4: $01:17:38.511982$ 192.168.62.70.48560 > 10.83.180.173.22: P 4250994242:4250994283(41) ack 903999423 win
229 <nop.nop.timestamp 1043829957="" 5156982065<br="">5: 01:17:38.513294 10.83.180.173.22 > 192.168.62.70.48560: . ack 4250994283 win 140 <nop.nop.timestamp< td=""></nop.nop.timestamp<></nop.nop.timestamp>
6: 01:17:38.528125 10.83.180.173.22 > 192.168.62.70.48560: P 903999423:903999444(21) ack 4250994283 win
140 <nop.nop.timestamp 1045829957="" 513898282=""> 7: 01:17:38.528613 192.168.62.70.48560 > 10.83.180.173.22: . <u>ack</u> 903999444 win 229 <<u>nop.nop.timestamp</u> 1045829961 513898282></nop.nop.timestamp>

"추적" 옵션을 추가하면 시스템을 통해 추적할 개별 패킷을 선택하여 최종 판정에 도달한 방법을 확 인할 수 있습니다. 또한 NAT(Network Address Translation) IP 수정과 같이 패킷에 대한 적절한 수 정이 이루어지고 적절한 이그레스 인터페이스가 선택되었는지 확인하는 데에도 도움이 됩니다. > show capture ssh_traffic packet-number 4 trace 7 packets captured 4: 01:17:38.511982 192.168.62.70.48560 > 10.83.180.173.22 4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp 192.168.62.70.48560 > 10.83.180.173.22: P 1045829957 513898266> Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found flow with id 626406, using existing flow Phase: 4 Type: EXTERNAL-INSPECT Subtype: Result: ALLOW Config: Additional Information: pplication: 'SNORT Inspect Phase: 5 Type: SNORT Subtype: Result: ALLOW Config: Additional Information: Snort Trace: Packet: TCP, ACK, seg 4250994242, ack 903999423 AppID: service SSH (846), application unknown (0) Firewall: starting rule matching, zone 1 -> 2, geo 0 -> 0, vlan 0, sgt Firewall: Starting rule materials of a composed of the starting rule material of the start of th trust/fastpath rule, id 268435458, allow IPS id 0, Verdict WHITELIST ict: (fast-forward) fast forward this flow 1, I Verdi esult: nput-interface: inside nput-status: up nput-line-status: up : allow ction

위의 예에서는 트래픽이 Snort 검사로 이동하고 최종적으로 허용 판정에 도달하여 전체가 디바이스 를 통과했음을 확인할 수 있습니다. 트래픽이 양방향으로 표시될 수 있으므로 이 세션 동안 디바이 스를 통해 트래픽이 흐르는 것을 확인할 수 있어서 이그레스 캡처가 필요하지 않을 수 있지만, 추적 출력에 표시된 대로 트래픽이 적절하게 이그레스되는지도 확인하려면 이그레스 인터페이스에서도 캡처할 수 있습니다.

참고: 디바이스가 이그레스 패킷을 생성할 수 없는 경우 추적 작업은 여전히 "허용"이지만, 이 그레스 인터페이스 캡처에서 패킷이 생성되거나 표시되지 않습니다. 이는 FTD에 다음 홉 또 는 대상 IP에 대한 ARP 항목이 없는 매우 일반적인 시나리오입니다(마지막 항목이 직접 연결 된 경우).

FTD(SSP) - 논리적 FTD 인터페이스에서 캡처

위에서 언급한 것처럼 FTD에서 패킷 캡처를 생성하는 동일한 단계를 SSP 플랫폼에서 수행할 수 있 습니다. SSH를 사용하여 FTD 논리적 인터페이스의 IP 주소에 연결하고 다음 명령을 입력할 수 있 습니다.

Firepower-module1> connect ftd

다음 명령을 사용하여 FXOS 명령 프롬프트에서 FTD 논리적 디바이스 쉘(shell)로 이동할 수도 있 습니다.

connect module 1 console
Firepower-module1> connect ftd

>

Firepower 9300을 사용하는 경우 모듈 번호는 사용 중인 보안 모듈에 따라 달라질 수 있습니다. 이 러한 모듈은 최대 3개의 논리적 디바이스를 지원할 수 있습니다.

다중 인스턴스를 사용 중인 경우 인스턴스 ID를 "connect" 명령에 포함해야 합니다. Telnet 명령을 사용하여 동시에 다른 인스턴스에 연결할 수 있습니다.

connect module 1 telnet
Firepower-module1>connect ftd ftd1
Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI
>

인터페이스 오류 확인

인터페이스 레벨 문제도 이 단계에서 확인할 수 있습니다. 이는 인그레스 인터페이스 캡처에서 패 킷이 누락된 경우 특히 유용합니다. 인터페이스 오류가 표시되면 연결된 디바이스를 확인하는 것이 도움이 될 수 있습니다.

SFR - ASA 인터페이스 확인

FirePOWER(SFR) 모듈은 기본적으로 ASA에서 실행되는 가상 머신이므로 실제 ASA 인터페이스 에서 오류를 확인합니다. ASA의 인터페이스 통계 확인에 대한 자세한 내용은 ASA 시리즈 명령 참 조 가이드 <u>섹션</u>을 참조하십시오.

FTD(비 SSP 및 FPR-2100) - 인터페이스 오류 확인

비 SSP FTD 디바이스에서는 > show interface 명령을 초기 명령 프롬프트에서 실행할 수 있습니다. 관심을 둘 출력은 빨간색으로 강조 표시되어 있습니다.

> show interface
InterfaceGigabitEthernet0/0 "outside", is up, line protocol is up
Hardware is i82545EM rev01, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
Input flow control is unsupported, output flow control is off
MAC address 000c.2961.f78b, MTU 1500
IPS Interface-Mode: inline, Inline-Set: InlineSet
IP address unassigned
20686130 packets input, 8859847035 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
2312 input errors, 0 CRC, 0 frame, 12313 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
6485096 packets output, 1480276815 bytes, 0 underruns
0 pause output, 0 resume output
1341 output errors, 45635 collisions, 1 interface resets
U late collisions, U deferred
0 input reset drops, 0 output reset drops
Input queue (blocks free curr/low): hardware (509/362)
output queue (blocks free curr/low): nardware (511/415)
I ramic Statistics for "outside".
20000131 packets input, 0405159715 bytes
4702172 packets drapped
1 minute input rate 2 pt/ts/sec. 999 butes/sec
1 minute output rate 0 okts/sec. 78 bytes/sec
1 minute duput rate 0 pkts/sec, 70 bytes/sec
5 minute input rate 3 pkts/sec 1222 bytes/sec
5 minute output rate 1 pkts/sec 319 bytes/sec
5 minute drop rate 1 pkts/sec
o militate drop rate, i pitto see

FTD(SSP) - 인터페이스 오류를 찾기 위한 데이터 경로 탐색

9300 및 4100 SSP 플랫폼에는 패킷을 먼저 처리하는 내부 패브릭 인터커넥트가 있습니다.



초기 패킷 인그레스에서 인터페이스 문제가 있는지 확인하는 것이 좋습니다. 다음은 이러한 정보를 얻기 위해 FXOS 시스템 CLI에서 실행하는 명령입니다.

ssp# scope eth-uplink ssp /et-uplink # show stats 다음은 샘플 출력입니다.

ssp# scope eth-uplink tner Loss Stats: Time Collected: 2017-05-15T14:13:46.032 Monitored Object: fabric/lan/A/pc-44/loss-stats Suspect: No Single Collision (errors): 0 Multi Collision (errors): 0 Late Collision (errors): 0 Carrier Sense (errors): 0 Giants (errors): 0 Symbol (errors): 0 Ether Loss Stats: ssp /eth-uplink # show stats Ether Error Stats: Time Collected: 2017-05-15T14:13:46.032 Monitored Object: fabric/lan/A/pc-44/err-stats Suspect: No Rcv (errors): 0 Symbol (errors): 0 SQE Test (errors): 0 Align (errors): 0 Fcs (errors): 0 Xmit (errors): 0 Excess Collision (errors): 0 Thresholded: 0 Under Size (errors): 0 Out Discard (errors): 0 Int Mac Tx (errors): 0 Int Mac Tx (errors): 0 Int Mac Rx (errors): 0 Deferred Tx (errors): 0 Thresholded: Xmit Delta Min Time Collected: 2017-05-15T14:13:46.032 Monitored Object: abrir/Jan/A/pc-48/Joss-stats Suspect: No Single Collision (errors): 0 Multi Collision (errors): 0 Late Collision (errors): 0 Carrier Sense (errors): 0 Ciriate (cerrors): 0 Time Collected: 2017-05-15T14:13:46.032 Giants (errors): 0 Symbol (errors): 0 Monitored Object: fabric/lan/A/pc-48/err-stats Suspect: No Rcv (errors): 0 SQE Test (errors): 0 Excess Collision (errors): 0 Align (errors): 0 Fcs (errors): 0 Xmit (errors): 0 Under Size (errors): 0 Thresholded: 0 Out Discard (errors): 0 Int Mac Tx (errors): 0 Int Mac Rx (errors): 0 Deferred Tx (errors): 0 Thresholded: Xmit Delta Mi

인그레스되면 패브릭 인터커넥트에서 패킷을 처리한 후 FTD 디바이스를 호스팅하는 논리적 디바 이스에 할당된 인터페이스로 패킷을 전송합니다.

다음은 참조용 다이어그램입니다.



인터페이스 레벨 문제를 확인하려면 다음 명령을 입력합니다.

ssp# connect fxos ssp(fxos)# show interface Ethernet 1/7 다음은 출력 예입니다(발생 가능한 문제는 빨간색으로 강조 표시됨).

ssp# connect fxos

ssp(fxos)# show interface Ethernet 1/7 Ethernet1/7 is up **Dedicated Interface** Hardware: 1000/10000 Ethernet, address: 5897.bdb9.4080 (bia 5897.bdb9.4080) **Description: U: Uplink** MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec reliability 254/255, txload 1/255, rxload 1/255 [...Omitted for brevity] Last link flapped 14week(s) 4day(s) Last clearing of "show interface" counters never 2 interface resets 30 seconds input rate 1352 bits/sec, 1 packets/sec 30 seconds output rate 776 bits/sec, 1 packets/sec Load-Interval #2: 5 minute (300 seconds) input rate 728 bps, 0 pps; output rate 608 bps, 0 pps RX 3178795 unicast packets 490503 multicast packets 1142652 broadcast packets 4811950 input packets 3354211696 bytes 0 jumbo packets 0 storm suppression bytes 0 runts 0 giants 0 CRC 0 no buffer 44288 input error 0 short frame 44288 overrun 0 underrun 0 ignored 0 watchdog 0 bad etype drop 0 bad proto drop 0 if down drop 0 input with dribble 306404 input discard 0 Rx pause ТΧ 1974109 unicast packets 296078 multicast packets 818 broadcast packets 2271005 output packets 696237525 bytes 0 jumbo packets 0 output errors 0 collision 0 deferred 0 late collision 0 lost carrier 0 no carrier 0 babble 0 output discard 0 Tx pause

오류가 발견되면 실제 FTD 소프트웨어에서 인터페이스 오류도 확인할 수 있습니다.



FTD 프롬프트로 이동하려면 먼저 FTD CLI 프롬프트로 이동해야 합니다.

connect module 1 console Firepower-module1> connect ftd >show interface 다중 인스턴스의 경우:

connect module 1 telnet
Firepower-module1>connect ftd ftd1
Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI
>

다음은 출력 예입니다.

# connect module 1 console	
Firepower-module1> connect ftd	
> show interface InterfaceGigabitEthernet0/0 "outside", is up, line protocol is up Hardware is i82545EM rev01, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps) Input flow control is unsupported, output flow control is off MAC address 000c.2961.f78b, MTU 1500 IPS Interface-Mode: inline, Inline-Set: InlineSet IP address unassigned 20686130 packets input, 8859847035 bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants 2312 input errors, 0 CRC, 0 frame, 12313 overrun, 0 ignored, 0 abort 0 pause input, 0 resume input 0 L2 decode drops 6485096 packets output, 1480276815 bytes, 0 underruns 0 pause output, 0 resume output 1341 output errors, 45635 collisions, 1 interface resets 0 late collisions, 0 deferred 0 input reset drops, 0 output reset drops input queue (blocks free curr/low): hardware (509/362) output queue (blocks free curr/low): hardware (511/415) Traffic Statistics for "outside": 20686131 packets output, 1375761699 bytes 4702172 packets dropped 1 minute input rate 2 pkts/sec, 999 bytes/sec 1 minute output rate 0 pkts/sec, 78 bytes/sec 1 minute drop rate, 0 pkts/sec	
5 minute drop rate, 1 pkts/sec	

Cisco TAC(Technical Assistance Center)에 제공할 데이터

데이터	지침							
연결 이벤트 스크린샷 'show	지침은 이 문서를 참조하십시오.							
interface' 출 력	지침은 이 문서를 참조하십시오.							
ᆔᅱᆊᅮᅴ	ASA/LINA: <u>https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-ge</u> <u>firewalls/1180</u>							
패것 접서	Firepower: http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-s appliances/11777							
ASA Jahaw	ASA CLI에 로그인하여 터미널 세션을 로그에 저장합니다. show tech 명령을 입력한 다음, T							
ASA Show tech' 출력	파질을 제응합니다. 이 명령을 사용하여 이 파일을 디스크 또는 외부 스토리지 시스템에 저장할 수 있습니다. show tech redirect disk0:/show_tech.log							
트래픽을 검 사하는								
Firepower 디 바이스에서 파일 문제 해 결	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-tech							

다음 단계: Firepower DAQ 레이어 문제 해결

Firepower 디바이스가 패킷을 삭제하는지 여부가 확실하지 않은 경우, 모든 Firepower 구성 요소를 한 번에 배제하기 위해 Firepower 디바이스 자체를 우회할 수 있습니다. 이는 해당 트래픽이 Firepower 디바이스로 인그레스되지만 이그레스되지 않는 경우 문제를 완화하는 데 특히 유용합니 다.

계속하려면 Firepower 데이터 경로 문제 해결의 다음 단계인 Firepower DAQ를 검토하십시오. <u>여기</u> 를 클릭하여 계속하십시오. 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.