Fase 1 da solução de problemas de caminho de dados do Firepower: Entrada de pacote

Contents

Introduction Guia da plataforma Troubleshooting da Fase de Entrada de Pacotes Identificar o tráfego em questão Verificar eventos de conexão Captura de pacotes nas interfaces de entrada e saída SFR - Captura nas interfaces do ASA FTD (não SSP e FPR-2100) - Captura nas interfaces de entrada e saída FTD (SSP) - Captura nas interfaces lógicas FTD Verificar erros de interface SFR - Verificar interfaces do ASA FTD (não SSP e FPR-2100) - Verificar erros de interface SFR - Verificar interfaces do ASA FTD (não SSP e FPR-2100) - Verificar erros de interface FTD (SSP) - Navegando no caminho de dados para procurar erros de interface Dados a fornecer ao Cisco Technical Assistance Center (TAC) Próxima etapa: Solucionar problemas da camada DAQ do Firepower

Introduction

Este artigo faz parte de uma série de artigos que explicam como solucionar problemas sistematicamente no caminho de dados em sistemas Firepower para determinar se os componentes do Firepower podem estar afetando o tráfego. Consulte o <u>artigo Visão geral</u> para obter informações sobre a arquitetura das plataformas Firepower e links para outros artigos de solução de problemas de caminho de dados.

Neste artigo, examinaremos o primeiro estágio da solução de problemas de caminho de dados do Firepower, o estágio de entrada de pacote.



Guia da plataforma

A tabela a seguir descreve as plataformas abrangidas por este artigo.

Nome do código da plataforma	Descrição	Aplicável Hardware Plataformas	Notas
SFR	Módulo ASA com FirePOWER Services (SFR) instalado.	ASA-5500-X Series	N/A
FTD (não	İmagem do Firepower Threat Defense (FTD)	ASA-5500-X	N/A

SSP e FPR-2100)	instalada em um Adaptive Security Appliance (ASA) ou em uma plataforma virtual
	FTD instalado como um dispositivo lógico
FTD (SSP)	em um chassi baseado no Firepower
	eXtensible Operative System (FXOS)

Series, plataformas NGFW virtuais

FPR-9300, FPR-4100, FPR-2100 Manager

Troubleshooting da Fase de Entrada de Pacotes

A primeira etapa da solução de problemas do caminho de dados é garantir que não ocorram quedas no estágio de entrada ou saída do processamento de pacotes. Se um pacote estiver ingressando, mas não egressando, você pode ter certeza de que o pacote está sendo descartado pelo dispositivo em algum lugar no caminho de dados ou que o dispositivo não consegue criar o pacote de saída (por exemplo, uma entrada ARP ausente).

Identificar o tráfego em questão

A primeira etapa na identificação e solução de problemas na etapa de entrada de pacotes é isolar o fluxo e as interfaces envolvidas no tráfego de problemas. Isso inclui:

Informações de fluxo Informações da interface

Protocolo Endereço IP origem Porta de origem IP de Destino Porta de Destino

Por exemplo:

TCP inside 172.16.100.101:38974 outside 192.168.1.10:80

Tip: Você pode não ser capaz de identificar a porta de origem exata, pois ela é frequentemente diferente em cada fluxo, mas a porta de destino (servidor) deve ser suficiente.

Verificar eventos de conexão

Depois de obter uma ideia da interface de entrada e saída, o tráfego deve corresponder, bem como as informações de fluxo, a primeira etapa para identificar se o Firepower está bloqueando o fluxo é verificar os Eventos de Conexão para o tráfego em questão. Eles podem ser vistos no Firepower Management Center em **Analysis > Connections > Events**

Note: Antes de verificar Eventos de conexão, verifique se o registro está habilitado nas regras da Política de controle de acesso. O registro é configurado na guia "Registro" em cada regra da política de controle de acesso, bem como na guia Inteligência de segurança. Verifique se as regras suspeitas estão configuradas para enviar os registros para o "Visualizador de Eventos".

0v	Overview Analysis Policies Devices Objects AMP Intelligence Depicy 🚊 System Help + Global \ admin +																	
Co	ntext Ex	plorer Connectio	ins + Events Intri	usions +	Files •	Hosts • User	s • Vuin	erabilities • Corr	elation •	Custorn • Loc	ikup • Search					_		
													Bookmark This Pay	ge Report Desi	gner Dashboard View Bool	kmarks Search •		
C	onne	ction Events	switch workflow)												2017-05-11 13:54:32 - 201	7-05-11 14:54:32		
Co	nectio	is with Application De	tails > Table View of Co	nnection E	vents											Expanding		
No	Search (Constraints (Edit Search)																
	umo to																	
-	ump to.	First Realist	I and Bandard	a sel e s	Deserve	Total and a second	R Market	Deserved as 10	Recorder		F	Course David (Bastlandlan Bast /	Real Problem	Ollanda	Mark Annellandian		
		* First Packet	Last Packet	Accien	Reason	TURNATOR Th	Country	Responder 1P	Country	Security Zone	Security Zone	ICMP Type	ICMP Code	Protocol	Chens	Web Application		
- 8		2017-05-11 14:54:32	2017-05-11 14:55:02	Allow		192.168.1.200		13.173.197.235	SA USA			60084 / tcp	80 (http) / tcp	HTTP	Web browser	Web Browsing		
-3		2017-05-11 14:54:02	2017-05-11 14:54:32	Allow		192.168.1.200		73.173.197.235	SA USA			60082 / tcp	80 (http) / tcp	HTTP	Web browser	Web Browsing		
- 4		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	Epmap	_		
4		2017-05-11 14:52:40	2017-05-11 14:52:55	Allow		192.168.1.200		10.83.181.139				60069 / tcp	Concession Locate		(unnered second)		- P	
- 4		2017-05-11 14:51:40	2017-05-11 14:51:53	Allow		192.168.1.200		10.83.181.139				60064 / tcp			(unnamed search)		Private	Save Save AL New Search
-8		2017-05-11 14:51:24	2017-05-11 14:51:24	Allow		192.168.1.200		172.217.26.206	USA USA			60058 / tcp	Sections		Networking			
1		2017-05-11 14:50:40	2017-05-11 14:50:55	Allow		192.168.1.200		10.83.181.139				60056 / tcp	General Information		Initiator IPA	192.168.1.200	-	192.168.1.0/24, 1192.168.1.3, 2001:08:8.
		2017-05-11 14-50-24	2012.05.11.14.50.24	Allow		103 168 1 300						60050 / http	Geolocation		Original Client 3P*			192.168.1/0/24, 1192.168.1.3, 2001/dd8/8
		2017-03-11 14:30:24	2017-03-11 14:30:24	ALCON.		192.100.1.200		172.217.20.200	<u></u>			0000007.000	Device		Initiator / Responder IP			192.168.1.0/24, 1192.168.1.3, 2001:488.8
		2017-05-11 14:50:23	2017-05-11 14:50:53	Allow		192.168.1.200		BI 73.173.197.235	USA USA			60051 / tcp	851.		Initiator / Original Client IP			192.168.1.0/24, 1192.168.1.3, 2001:088:8-
-4		2017-05-11 14:49:47	2017-05-11 14:49:47	Allow		192.168.1.200		172.217.26.206	JUSA			60043 / tcp	URL		Initiator / Responder / Original Cle Incress Security Zone	NE IP		192.168.1.0/24, 1192.168.1.3, 2001.668.8 My Security Zone
- 4		2017-05-11 14:49:40	2017-05-11 14:49:55	Allow		192.168.1.200		10.83.181.139				60046 / tcp	Netflow		Egress Security Zone			Hy Security Zone
4		2017-05-11 14:48:46	2017-05-11 14:51:23	Allow		192.168.1.200		12.246.56.139	usa 🔜			60041 / tcp	QuS		Ingress / Egress Security Zone			My Security Zone
1		2017-05-11 14:48:46	2017-05-11 14:49:16	Allow		192.168.1.200		73.173.197.235	IUSA			60040 / tcp		_	Source Port / ICMP Type			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 / http	+ New Search		Protocol*			tep, udp
		2017-02-11 14:40:40	2017-02-11 14:40.22	CALINER.		124.139.1499						500027.7.558	Global		DNS Query			suspicious.com, evil*
		2017-05-11 14:48:32	2017-05-11 14:48:32	Allow		M 192.168.1.200		B 172.217.26.206	USA			600317 tcp	SuperConnectionTest		DNS Response			NEDOMAIN
-4		2017-05-11 14:48:16	2017-05-11 14:48:46	Allow		192.168.1.200		73.173.197.235	MA USA			60034 / tcp	Predefined Searches		DNS Record Type			A, PTR
- 4		2017-05-11 14:47:46	2017-05-11 14:48:16	Allow		192.168.1.200		73.173.197.235	💶 USA			60030 / tcp	Malicious URLs		DNS Sinkhole Name			Ny Sinkhole
4		2017-05-11 14:47:40	2017-05-11 14:47:55	Allow		192.168.1.200		10.83.181.139				60027 / tcp			HTTP Response Code			200
- 3		2017-05-11 14:47:15	2017-05-11 14:48:46	Allow		192.168.1.200		72.246.56.169	usa 🔜			60022 / tcp	Relevance		VLAN ID			10
		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			Geolocation			
		2012-05-11 14:46:45	2012-05-11 14:47:15	Allow		192 168 1 200		1 73 173 107 235	A 211			60017 / http			Initiator Country			USA, United States, United*
	0	NATIONAL INCOME	NAT-92-11 14 M7113	CLOCK R					- MAR			STATE A C. J. MAR			Original Client Country			USA, United States, United*
Las	login or	Tuesday, 2017-04-25 at	12:42:21 PM from rtp-flip	ey-88111.	disco.com										Initiator / Responder Country			USA, United States, United*
						_									"Tield constrains summaries and o	ranha.		

No exemplo acima, "Editar pesquisa" é clicado e um IP de origem (iniciador) exclusivo é adicionado como um filtro para ver os fluxos que estavam sendo detectados pelo Firepower. A coluna Ação mostra "Permitir" para este tráfego de host.

Se o Firepower estiver bloqueando intencionalmente o tráfego, a Ação conterá a palavra "Bloquear". Clicar em "Table View of Connection Events" fornece mais dados. Os seguintes campos nos Eventos de Conexão podem ser observados se a ação for "Bloquear":

-Razão

- Regra de controle de acesso

Isso, combinado com os outros campos no evento em questão, pode ajudar a restringir qual componente está bloqueando o tráfego.

Para obter mais informações sobre como solucionar problemas de regras de controle de acesso, clique <u>aqui</u>.

Captura de pacotes nas interfaces de entrada e saída

Se não houver nenhum evento ou o Firepower ainda tiver suspeita de bloqueio, apesar dos Eventos de Conexão exibirem uma ação de regra "Permitir" ou "Confiar", a solução de problemas do caminho de dados continuará.

Aqui estão instruções sobre como executar uma captura de pacote de entrada e saída nas várias plataformas mencionadas acima:

SFR - Captura nas interfaces do ASA

Como o módulo SFR é simplesmente um módulo em execução no ASA Firewall, é melhor capturar primeiro nas interfaces de entrada e saída do ASA para garantir que os mesmos pacotes que ingressam também estejam egressando.

Este artigo contém instruções sobre como executar as capturas no ASA.

Se for determinado que os pacotes que estão ingressando no ASA não estão egressando, continue na próxima fase da solução de problemas (a fase DAQ).

Note: Se os pacotes forem vistos na interface de entrada do ASA, pode valer a pena verificar os dispositivos conectados.

FTD (não SSP e FPR-2100) - Captura nas interfaces de entrada e saída

A captura em um dispositivo FTD que não seja SSP é semelhante à captura no ASA. Entretanto, você pode executar os comandos de captura diretamente do prompt inicial da CLI. Ao Troubleshoot pacotes descartados, é aconselhável adicionar a opção "trace" à captura.

Aqui está um exemplo de configuração de uma captura de entrada para o tráfego TCP na porta 22:

> 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. 1460.sack0K.timestamp 1045829951 0.pop.wscale 7></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 < <u>nop.nop.timestamp</u>				
4: $01:17:38.511982$ 192.168.62.70.48560 > 10.83.180.173.22: P 4250994242:4250994283(41) ack 903999423 win				
5: 01:17:38.513294 5: 01:17:38.513294 10.83.180.173.22 > 192.168.62.70.48560: . ack 4250994283 win 140 < <u>nop.nop.timestamp</u>				
513898268 1045829957> 6: 01:17:38.528125 10.83.180.173.22 > 192.168.62.70.48560: P 903999423:903999444(21) ack 4250994283 win				
140 < <u>nop.nop.timestamp</u> 513898282 1045829957> 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>				

Se você adicionar a opção "trace", poderá selecionar um pacote individual para rastrear pelo sistema para ver como ele chegou ao veredito final. Ele também ajuda a garantir que as modificações apropriadas sejam feitas no pacote, como a modificação de IP da Network Address Translation (NAT) e que a interface de saída apropriada tenha sido escolhida.

> 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

No exemplo acima, vemos que o tráfego chega à inspeção do Snort e que finalmente alcançou um veredito de permissão e, em geral, passou pelo dispositivo. Como o tráfego pode ser visto em ambas as direções, você pode ter certeza de que o tráfego está fluindo pelo dispositivo para esta sessão, portanto uma captura de saída pode não ser necessária, mas você também pode levar uma para lá para ter certeza de que o tráfego está egressando corretamente, como mostrado na saída de rastreamento.

Note: Se o dispositivo não puder criar o pacote de saída, a ação de rastreamento ainda será "permitir", mas o pacote não será criado ou visto na captura da interface de saída. Esse é um cenário muito comum em que o FTD não tem uma entrada ARP para o próximo salto ou IP de destino (se este último estiver diretamente conectado).

FTD (SSP) - Captura nas interfaces lógicas FTD

As mesmas etapas para gerar uma captura de pacote no FTD, como mencionado acima, podem ser seguidas em uma plataforma SSP. Você pode se conectar usando SSH no endereço IP da interface lógica FTD e inserir o seguinte comando:

```
Firepower-module1> connect ftd
>
```

Você também pode navegar até o shell de dispositivo lógico FTD a partir do prompt de comando FXOS com os seguintes comandos:

```
# connect module 1 console
Firepower-module1> connect ftd
>
```

Se um Firepower 9300 for usado, o número do módulo pode variar dependendo do módulo de segurança que está sendo usado. Esses módulos podem suportar até 3 dispositivos lógicos.

Se várias instâncias estiverem sendo usadas, a ID da instância deve ser incluída no comando "connect". O comando Telnet pode ser usado para se conectar a instâncias diferentes ao mesmo tempo.

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

Verificar erros de interface

Os problemas de nível de interface também podem ser verificados durante essa fase. Isso é especialmente útil se houver pacotes ausentes na captura da interface de entrada. Se forem observados erros de interface, a verificação dos dispositivos conectados pode ser útil.

SFR - Verificar interfaces do ASA

Como o módulo FirePOWER (SFR) é basicamente uma máquina virtual em execução em um ASA, as interfaces reais do ASA são verificadas quanto a erros. Para obter informações detalhadas sobre como verificar as estatísticas da interface no ASA, consulte esta <u>seção</u> do guia

FTD (não SSP e FPR-2100) - Verificar erros de interface

Em dispositivos FTD não SSP, o comando **> show interface** pode ser executado a partir do prompt de comando inicial. A saída interessante está realçada em vermelho.

> 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 000a 2961 f78b MTL 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 dreps, 0 output reset dreps	
input reset drops, 0 output reset drops input queue (blocks free curr/low): bardware (509/362)	
output queue (blocks free curr/low): hardware (505/502)	
Traffic Statistics for "outside":	
20686131 packets input, 8485139715 bytes	
6485096 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 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	

FTD (SSP) - Navegando no caminho de dados para procurar erros de interface

As plataformas 9300 e 4100 SSP têm uma interconexão de estrutura interna que manipula primeiro os pacotes.



Vale a pena verificar se há algum problema de interface na entrada inicial do pacote. Estes são os comandos a serem executados na CLI do sistema FXOS para obter essas informações.

ssp# scope eth-uplink
ssp /et-uplink # show stats
Esta é uma saída de exemplo.

ssp# scope eth-uplinkEther Loss Stats:ssp /eth-uplink # show statsTime Collected: 2017-05-15T14:13:46.032Ether Error Stats:Suspect: NoTime Collected: 2017-05-15T14:13:46.032Monitored Object: fabric/lan/A/pc-44/loss-statsSuspect: NoSingle Collision (errors): 0Rcv (errors): 0Late Collision (errors): 0Align (errors): 0Symbol (errors): 0Fcs (errors): 0Symbol (errors): 0Cult State (errors): 0Symbol (errors): 0Under Size (errors): 0Excess Collision (errors): 0Under Size (errors): 0Time Collected: 2017-05-15T14:13:46.032Under Size (errors): 0SQE Test (errors): 0Under Size (errors): 0Excess Collision (errors): 0Under Size (errors): 0Excess Collision (errors): 0Under Size (errors): 0Time Collected: 2017-05-15T14:13:46.032Monitored Object: fabric/lan/A/pc-48/loss-statsSuspect: NoSuspect: NoSingle Collision (errors): 0Time Collected: 2017-05-15T14:13:46.032Monitored Object: fabric/lan/A/pc-48/loss-statsDeferred Tx (errors): 0Carrier Sense (errors): 0Time Collected: 2017-05-15T14:13:46.032Monitored Object: fabric/lan/A/pc-48/loss-statsSuspect: NoSingle Collision (errors): 0Time Collected: 2017-05-15T14:13:46.032Monitored Object: fabric/lan/A/pc-48/loss-statsSuspect: NoSingle Collision (errors): 0Time Collected: 2017-05-15T14:13:46.032Monitored Object: fabric/lan/A/pc-48/loss-statsSuspect: NoSingle Collision (errors): 0Carrier Sense (errors): 0 </th <th></th> <th></th>		
	ssp# scope eth-uplink 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 Align (errors): 0 Cout Discard (errors): 0 Under Size (errors): 0 Under Size (errors): 0 Int Mac Tx (errors): 0 Deferred Tx (errors): 0 Thresholded: Xmit Delta Min Time Collected: 2017-05-15T14:13:46.032 Monitored Object: fabric/lan/A/pc-48/err-stats Suspect: No Rcv (errors): 0 Align (errors): 0 Suspect: No Cout Discard (errors): 0 Under Size (errors): 0 Under Size (errors): 0 Int Mac Tx (errors): 0 Under Size (errors): 0 Int Mac Tx (errors): 0 Int Mac Tx (errors): 0 Int Mac Tx (errors): 0 Int Mac Tx (errors): 0 Thresholded: Xmit Delta Min	Ether 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 Late Collision (errors): 0 Carrier Sense (errors): 0 Giants (errors): 0 SQE Test (errors): 0 Excess Collision (errors): 0 Time Collected: 2017-05-15T14:13:46.032 Monitored Object: fabric/lan/A/pc-48/loss-stats Suspect: No Single Collision (errors): 0 Multi Collision (errors): 0 Late Collision (errors): 0 Giants (errors): 0 Symbol (errors): 0 Symbol (errors): 0 Symbol (errors): 0 Symbol (errors): 0 SQE Test (errors): 0 Symbol (errors): 0 SQE Test (errors): 0 Symbol (errors): 0 SQE Test (errors): 0 SQE Test (errors): 0 Symbol (errors): 0 SQE Test (e

Depois que a interconexão de estrutura manipula o pacote na entrada, ele é enviado para as interfaces que são atribuídas ao dispositivo lógico que hospeda o dispositivo FTD.

Aqui está um diagrama para referência:



Para verificar se há problemas no nível da interface, insira os seguintes comandos:

ssp# connect fxos
ssp(fxos)# show interface Ethernet 1/7
Este é um exemplo de saída (possíveis problemas destacados em vermelho):

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

Se algum erro for detectado, o software FTD real também poderá ser verificado quanto a erros de interface.



Para chegar ao prompt do FTD, é primeiro necessário navegar até o prompt do FTD CLI.

connect module 1 console
Firepower-module1> connect ftd
>show interface
Para várias instâncias:

connect module 1 telnet
Firepower-module1>connect ftd ftd1
Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI
>
Este é um exemplo de saída.

# 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 input, 4485139715 bytes 6485096 packets output, 1375761699 bytes 4702172 packets dropped 1 minute input rate 2 pkts/sec, 78 bytes/sec 1 minute output rate 0 pkts/sec 5 minute drop rate, 0 pkts/sec, 1222 bytes/sec 5 minute output rate 1 pkts/sec, 319 bytes/sec	
5 minute drop rate, 1 pkts/sec	

Dados a fornecer ao Cisco Technical Assistance Center (TAC)

Dados Capturas	Instruções
de tela do evento de conexão	Consulte este artigo para obter instruções
'show interface'	Consulte este artigo para obter instruções
Capturas de pacotes	Para ASA/LINA: <u>https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-firewalls/1180</u> Para Firepower: <u>http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000</u> appliances/11777
Saída 'show tech' do ASA	Faça login no ASA CLI e salve a sessão do terminal em um log. Digite o comando show tech de saída da sessão de terminal ao TAC. Esse arquivo pode ser salvo em disco ou em um sistema de armazenamento externo com es show tech l redirecionar disco0'/show tech log
Solucionar problemas do	
dispositivo Firepower que inspeciona	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technot

Próxima etapa: Solucionar problemas da camada DAQ do Firepower

Se não for claro se o dispositivo Firepower está descartando pacotes, o próprio dispositivo Firepower pode ser ignorado para excluir todos os componentes do Firepower de uma só vez. Isso é especialmente útil para mitigar um problema se o tráfego em questão estiver entrando no dispositivo Firepower, mas não no egresso.

Para prosseguir, revise a próxima fase da solução de problemas de caminho de dados do Firepower; O Firepower DAQ. Clique <u>aqui</u> para continuar.