Firepowerデータパスのトラブルシューティング フェーズ1:パケット入力

内容

概要 プラットフォームガイド パケット入力フェーズのトラブルシューティング 問題のトラフィックの特定 接続イベントの確認 入力および出力インターフェイスでのパケットのキャプチャ SFR:ASAインターフェイスでのキャプチャ FTD(非SSPおよびFPR-2100):入力および出力インターフェイスでのキャプチャ FTD(SSP):論理FTDインターフェイスでのキャプチャ インターフェイスエラーのチェック SFR:ASAインターフェイスの確認 FTD(非SSPおよびFPR-2100):インターフェイスエラーの確認 FTD(非SSPおよびFPR-2100):インターフェイスエラーの確認 FTD(SSP)-インターフェイスエラーを検索するためのデータパスの移動 Cisco Technical Assistance Center(TAC)に提供するデータ 次の手順:Firepower DAQレイヤのトラブルシューティング

概要

この記事は、Firepowerシステムのデータパスを体系的にトラブルシューティングし、 Firepowerのコンポーネントがトラフィックに影響を与えているかどうかを判断する方法を説明す る一連の記事の一部です。Firepowerプラットフォームの<u>アーキテクチャに</u>関する情報や、その他 のデータパスのトラブルシューティングに関する記事へのリンクについては、概要記事を参照し てください。

この記事では、Firepowerのデータパスのトラブルシューティングの最初の段階であるパケット入 力の段階について説明します。



プラットフォームガイド

次の表では、この記事で扱うプラットフォームについて説明します。

プラットフ ォームコー ド名	説明	該当 ハードウェ ア プラットフォ ーム	注意事項
SFR	ASA with FirePOWER Services(SFR)モジュ ールがインストールされている。	ASA-5500-Xシリ ーズ	N/A
FTD(非	適応型セキュリティアプライアンス(ASA)ま	ASA-5500-Xシリ	N/A

SSPおよび	たは仮想プラットフォームにインストール	ーズ、仮想	
FPR-	されたFirepower Threat Defense(FTD)イメ	NGFWプラット	
2100)	ージ	フォーム	
FTD(SSP)	Firepower eXtensible Operational System(FXOS)ベースのシャーシに論理デバ イスとしてインストールされるFTD	FPR-9300、 FPR-4100、 FPR-2100	2100シリーズでは、 FXOS Chassis Managerは使用されま せん

パケット入力フェーズのトラブルシューティング

最初のデータパスのトラブルシューティング手順は、パケット処理の入力または出力ステージで ドロップが発生していないことを確認することです。パケットが入力されていても出力されない 場合は、パケットがデータパス内の任意の場所でデバイスによってドロップされているか、また はデバイスが出力パケットを作成できないことが確認できます(ARPエントリの欠落など)。

問題のトラフィックの特定

パケット入力段階のトラブルシューティングの最初のステップは、問題のトラフィックに関係す るフローとインターフェイスを切り分けることです。これには、次のような特徴があります。

 フロー情報
 インターフェイス情報

 プロトコル
 送信元 IP アドレス

 送信元ポート
 入力インターフェイス

 宛先 IP
 出力インターフェイス

以下に、いくつかの例を示します。

TCP inside 172.16.100.101:38974 outside 192.168.1.10:80

ヒント:送信元ポートは各フローで異なることが多いため、正確な送信元ポートを特定できない場合がありますが、宛先(サーバ)ポートで十分です。

接続イベントの確認

トラフィックが一致する必要がある入力および出力インターフェイスとフロー情報を確認した後 、Firepowerがフローをブロックしているかどうかを確認する最初のステップは、該当するトラフ ィックの接続イベントを確認することです。これらはFirepower Management Centerの[Analysis] > [Connections] > [Events]で表示できます

注:接続イベントを確認する前に、アクセスコントロールポリシールールでロギングが有効 になっていることを確認してください。ロギングは、各アクセスコントロールポリシールー ルの[Logging]タブおよび[Security Intelligence]タブで設定します。疑わしいルールが「イベ ントビューア」にログを送信するように設定されていることを確認します。

Overview Analysis Policies Devices Objects AMP Intelligence Depicy & System Heip + Global \ admin + Context Explorer Connections + Events Intrusions + Files + Hosts + Users + Vulnerabilities + Correlation + Custom + Lookup + Search																			
Connection Events (matra workfree) Connection Events (matra workfree) Connection with Application Datains) Table View of Connection Pients Connection Pients (add Search) No Search Constraints (<u>dd Search</u>)																			
Jum	p to	• First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application	Client	Web Application			
-		2017-05-11 14:54:32	2017-05-11 14:55:02	Allow		192,168,1,200		73,173,197,235	USA .			60084 / trn	80 (http) / tcp	HTTP	Web browser	Web Browsing			
		2017 05 11 14 54 02	2012 05 11 14 54-22	Allow					100 A			(0000) / http	00 (http://www.		- High homes	Web Dependen			
		2017-03-11 14:34:02	2017-05-11 14:54:32	ALIGHT .		192.108.1.200		MI 73.173.197.235	<u>1000</u>			000027.000	eu (nitip) / tcp		web browser	web browsing			
•		2017-05-11 14:53:40	2017-05-11 14:53:55	Allow		192.168.1.200		10.83.181.139				50077 / 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		H 10.83.181.139				60069 / tcp	Connection Events		(unnamed search)		C Private	Save Save As New Search	
+		2017-05-11 14:51:40	2017-05-11 14:51:53	Allow		192.168.1.200		10.83.181.139				60064 / tcp	Sections		Meteoretine				
4		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	General Information		Initiates 104	100 168 1 000			
4		2017-05-11 14:50:40	2017-05-11 14:50:55	Allow		192.168.1.200		10.83.181.139				60056 / tcp	Networking		Responder IP*	197.109.1.200		192.168.1.0/24, 1192.168.1.3, 2001:008:8	
4		2017-05-11 14:50:24	2017-05-11 14:50:24	Allow		192.168.1.200		172.217.26.206	usa 🔜			60050 / tcp	Geolocation		Original Client 37*			192.168.1.0/24, 1192.168.1.3, 2001:db8:8	
		2012-05-11 14-50-23	2017-05-11 14-50-53	Allow		102 168 1 200		73 173 107 235	IICA			60051 / tro	Device		Initiator / Responder IP			192.168.1.0/24, 1192.168.1.3, 2001:088.8	1
			2017-02-11 14.20.22	COLUMN I					MAD			5000.00.00.00.00	NSL Application		Initiator / Original Client IP Initiator / Responder / Original Clie	eri 19		192.168.1.0/24, 1192.168.1.3, 2001:088.8 192.168.1.0/24, 1192.168.1.3, 2001:088.8	1
		2017-05-11 14:49:47	2017-05-11 14:49:47	Allow		B 192.168.1.200		B 172.217.26.206	<u>1054</u>			600437tcp	URL		Ingress Security Zone			My Security Zone	11
+		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	1
4		2017-05-11 14:48:46	2017-05-11 14:51:23	Allow		192.168.1.200		72.246.56.139	JUSA			60041 / tcp	QuS		Ingress / Egress Security Zone			Hy Security Zone	
4		2017-05-11 14:48:46	2017-05-11 14:49:16	Allow		192.168.1.200		73.173.197.235	JUSA			60040 / tcp		_	Source Port / ICMP Type Destination Bost / ICMP Code*			1-1024, 6000-6011, 180	
4		2017-05-11 14:48:40	2017-05-11 14:48:55	Allow		192,168,1,200		10.83,181,139				60037 / tcp			Protocol*			tcp, udp	
		2012.05.11 14:48:32	2017-05-11 14-48-32	Allow		102 168 1 200		172 217 26 206				60031 / http	Global		DNS Query			suspicious.com, evil*	
		2017-02-11 14:40:32	2017-02-11 14:40:32	PUIVA		172.100.1.200		MB 172.217.20.200	<u></u>			200247.00	SuperConnectionTest		DNS Response			INDOMAIN	
+		2017-05-11 14:48:16	2017-05-11 14:48:46	Allow		192.168.1.200		3.173.197.235	USA USA			600.34 / tcp	Predefined Searches		DNS Record Type DNS TTL			43200	
+		2017-05-11 14:47:46	2017-05-11 14:48:16	Allow		192.168.1.200		73.173.197.235	SA USA			60030 / tcp	Malicious URLs		DNS Sinkhole Name			My 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	
4		2017-05-11 14:47:15	2017-05-11 14:48:46	Allow		192.168.1.200		12.246.56.169	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			60021 / trp			Geolocation				
1		2012 05 11 14 46 45	2012.05.11.14.47.15	Allow		102 168 1 200						60017 / No			Initiator Country			USA, United States, United*	
•		2017-05-11 14:46:45	2017-05-11 14:47:15	SUDW.		m 194.108.1.200		m /3.1/3.197.235	U20			956177 SCD			Responder Country Drinknal Claust Country			USA, United States, United*	
Last lo	gin on	Tuesday, 2017-04-25 at 1	12:42:21 PM from rtp-flipk	ey-88111.	disco.com										Initiator / Responder Country			USA, United States, United*	
_						_			_						Theid constrains summaries and o	anta.			

上の例では、[Edit Search]をクリックし、一意のソース(イニシエータ)IPをフィルタとして追加して、Firepowerによって検出されたフローを確認します。[Action]列には、このホストトラフィックの[Allow]が表示されます。

Firepowerが意図的にトラフィックをブロックしている場合、アクションには「ブロック」という 単語が含まれます。 [接続イベントのテーブルビュー]をクリックすると、さらに多くのデータが 表示されます。アクションが「ブロック」の場合、接続イベントの次のフィールドに注意してく ださい。

-原因

- アクセスコントロールルール

このフィールドは、問題のイベントの他のフィールドと組み合わされて、トラフィックをブロックしているコンポーネントを絞り込むのに役立ちます。

アクセスコントロールルールのトラブルシューティングの詳細については、ここをクリック<u>して</u> <u>ください</u>。

入力および出力インターフェイスでのパケットのキャプチャ

接続イベントで「許可」または「信頼」のルールアクションが表示されているにもかかわらず、 イベントが存在しない場合やFirepowerがブロックの疑いがある場合は、データパスのトラブルシ ューティングが続行されます。

上記のさまざまなプラットフォームで入力および出力パケットキャプチャを実行する方法を次に 示します。

SFR:ASAインターフェイスでのキャプチャ

SFRモジュールは単にASAファイアウォールで実行されるモジュールであるため、最初にASAの 入力インターフェイスと出力インターフェイスでキャプチャし、入力と同じパケットが出力され ていることを確認することをお勧めします。

この記事では、ASAでキャプチャを実行する方法について説明します。

ASAに着信しているパケットが出力されていないと判断された場合は、トラブルシューティングの次のフェーズ(DAQフェーズ)に進みます。

注:ASA入力インターフェイスでパケットが見られる場合は、接続されたデバイスを確認す る価値があります。

FTD(非SSPおよびFPR-2100):入力および出力インターフェイスでのキャプチャ

非SSP FTDデバイスでのキャプチャは、ASAでのキャプチャと同様です。ただし、CLIの初期プロンプトからcaptureコマンドを直接実行できます。ドロップされたパケットのトラブルシューティングを行う場合は、キャプチャに「trace」オプションを追加することを推奨します。

次に、ポート22でTCPトラフィックの入力キャプチャを設定する例を示します。

> capture <u>ssh_traffic</u> trace interface inside match <u>tcp</u> any any <u>eq</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 ⊲mss.
2: 01:17:38.510898 10.83.180.173.22 > 192.168.62.70.48560: S 903999422:903999422(0) ack 4250994242 win
17896 < <u>mss</u> 1380,sackOK,timestamp 513898266 1045829951,nop,wscale 7> 3: 01:17:38.511402 192.168.62.70.48560 > 10.83.180.173.22: . <u>ack</u> 903999423 win 229 < <u>nop.nop.timestamp</u>
1045829956 513898266> 4: 01:17:38.511982 192.168.62.70.48560 > 10.83.180.173.22: P 4250994242:4250994283(41) <u>ack</u> 903999423 win
229 <nop.nop.timestamp 1045829957="" 513898266=""> 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>
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 < nop. nop. timestamp 513898282 1045829957> 7: 01-17:38 528613 102 168 62 70 48560 > 10 83 180 173 22; ack 903999444 win 229 < nop. nop. timestamp
1045829961 513898282>

"trace"オプションを追加すると、システムをトレースする個々のパケットを選択して、最終的な 判定がどのように行われたかを確認できます。また、ネットワークアドレス変換(NAT)のIP変更 などのパケットに対して適切な変更が行われ、適切な出力インターフェイスが選択されているこ とを確認することもできます。 > 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

上記の例では、トラフィックがSnort検査に到達し、最終的に許可の判定に達し、デバイス全体が 通過していることがわかります。トラフィックは両方向で確認できるため、このセッションのデ バイスを通過するトラフィックを確認できます。そのため、出力キャプチャは必要ない可能性が ありますが、トレース出力に示すように、トラフィックが正しく出力されていることを確認する こともできます。

注:デバイスが出力パケットを作成できない場合、トレースアクションは「allow」のまま ですが、パケットは出力インターフェイスキャプチャで作成または表示されません。これは 、FTDにネクストホップまたは宛先IPのARPエントリがない(この最後のエントリが直接接 続されている場合)非常によく見られるシナリオです。

FTD(SSP):論理FTDインターフェイスでのキャプチャ

上記と同じ手順で、FTDでパケットキャプチャを生成できます。この手順は、SSPプラットフォ ームでも実行できます。SSHを使用してFTD論理インターフェイスのIPアドレスに接続し、次の コマンドを入力できます。

Firepower-module1> connect ftd

次のコマンドを使用して、FXOSコマンドプロンプトからFTD論理デバイスシェルに移動することもできます。

connect module 1 console
Firepower-module1> connect ftd

>

Firepower 9300が使用されている場合、使用されているセキュリティモジュールによってモジュール番号が異なる場合があります。これらのモジュールは、最大3つの論理デバイスをサポートできます。

マルチインスタンスを使用する場合は、「connect」コマンドにインスタンスIDを含める必要があ ります。Telnetコマンドを使用すると、異なるインスタンスに同時に接続できます。

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

インターフェイスエラーのチェック

このフェーズでは、インターフェイスレベルの問題も確認できます。これは、入力インターフェ イスキャプチャでパケットが欠落している場合に特に役立ちます。インターフェイスエラーが表 示される場合は、接続されているデバイスを確認すると便利です。

SFR:ASAインターフェイスの確認

FirePOWER(SFR)モジュールは基本的にASAで実行される仮想マシンであるため、実際のASAインターフェイスでエラーがチェックされます。ASAのインターフェイス統計情報の確認の詳細については、次の「ASAシリーズコマンドリファレンスガイド」セクションを参照<u>してください</u>。

FTD(非SSPおよびFPR-2100):インターフェイスエラーの確認

SSP以外のFTDデバイスでは、**> show interfaceコマンド**を初期コマンドプロンプトから実行でき ます。対象となる出力は赤で強調表示されています。



FTD(SSP) – インターフェイスエラーを検索するためのデータパスの移動

9300および4100 SSPプラットフォームには、最初にパケットを処理する内部ファブリックイン ターコネクトがあります。



最初のパケット入力にインターフェイスの問題があるかどうかを確認する価値があります。この 情報を取得するには、FXOSシステムCLIで実行するコマンドを次に示します。

ssp# scope eth-uplink ssp /et-uplink # show stats 次に出力例を示します。

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 Align (errors): 0 Under Size (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 Cound Size (errors): 0 Monitored Constantiation (errors): 0 Align (errors): 0 Align (errors): 0 Cound Size (errors): 0 Int Mac TX (errors): 0 Deferred 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 Multi Collision (errors): 0 Carrier Sense (errors): 0 Symbol (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 SQE Test (errors): 0 SQE Test (errors): 0 SQE Test (errors): 0 Thresholded: 0

ファブリックインターコネクトは、入力時にパケットを処理した後、FTDデバイスをホストする 論理デバイスに割り当てられたインターフェイスに送信されます。

次の図を参照してください。



インターフェイスレベルの問題を確認するには、次のコマンドを入力します。

ssp# connect fxos ssp(fxos)# show interface Ethernet 1/7 次に出力例を示します(赤で強調表示されている問題の可能性があります)。

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 interta 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

エラーが見つかった場合は、実際のFTDソフトウェアでもインターフェイスエラーをチェックで きます。



FTDプロンプトに移動するには、まずFTD CLIプロンプトに移動する必要があります。

connect module 1 console
Firepower-module1> connect ftd
>show interface
マルチインスタンスの場合:

connect module 1 telnet Firepower-module1>connect ftd ftd1 Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI > 次に出力例を示します。

# 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, 1375761699 bytes 4702172 packets dropped 1 minute input rate 2 pkt/sec, 999 bytes/sec 1 minute drop rate, 0 pkts/sec 5 minute drop rate, 0 pkts/sec	
5 minute drop rate, 1 pkts/sec	

Cisco Technical Assistance Center(TAC)に提供するデータ

Data	手順
接続イベントのスクリーンショット	手順については、
「show interface」出力	手順については、
	ASA/LINAの場合
パケット キャプチャ	firewalls/1180 C
	Firepowerの場合
	appliances/11777
	ASA CLIにログイ
ASA Φ [show tooh · Ψ]	ナルセッション出
	このファイルは、
	show tech redire
トラフィックを検査するFirepowerデバイスからのファイルのトラブルシューティング	http://www.cisco.d

次の手順: Firepower DAQレイヤのトラブルシューティング

Firepowerデバイスがパケットをドロップしているかどうかがわからない場合は、Firepowerデバ イス自体をバイパスして、すべてのFirepowerコンポーネントを一度に除外できます。これは、問 題のトラフィックがFirepowerデバイスに入り込んで出てこない場合の問題を軽減するのに特に役 立ちます。

続行するには、Firepowerデータパスのトラブルシューティングの次のフェーズを確認してください。Firepower DAQ。続行するに<u>はここ</u>をクリックします。