Firepowerデータパスのトラブルシューティング フェーズ2:DAQレイヤ

内容

<u>概要</u>

プラットフォームガイド Firepower DAQフェーズのトラブルシューティング DAQレイヤでのトラフィックのキャプチャ Firepowerをバイパスする方法 SFR:Firepowerモジュールをモニタ専用モードにします FTD(すべて): インラインセットをTAPモードに配置 Packet Tracerを使用したシミュレーショントラフィックのトラブルシューティング SFR:ASA CLIでのPacket Tracerの実行 FTD(すべて):FTD CLIでパケットトレーサを実行します。 トレースによるキャプチャを使用したライブトラフィックのトラブルシューティング FTD(すべて):FMC GUIでのトレースによるキャプチャの実行 FTDでのPreFilter Fastpathルールの作成 TACに提供するデータ 次のステップ

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データパスのトラブルシューティングの2番目の段階について説明しま す。DAQ(データ収集)レイヤ



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。

ノフット 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	ASA-5500-Xシリーズ	N/A

されている。

	すべてのFirepower	ASA-5500-Xシリーズ、仮想	
FTD(す	Threat	NGFWプラットフォーム、	N/A
べて)	Defense(FTD)プラッ	FPR-2100、FPR-9300、	N/A
	トフォームに適用	FPR-4100	
FTD(非	ASAまたは仮想プラ	▲SA-5500-Xシリーズ 仮相	
SSPおよ	ットフォームにイン	NGFWプラットフォーム	N/A
びFPR-	ストールされた	FPR-2100	
2100)	FTDイメージ	111(2100	
	Firepower eXtensible		
	Operational		
	System(FXOS)べー		2100シリーズでは、FXOS Chassis
FID(SSF)	スのシャーシに論理	FFR-9300, FFR-4100	Managerは使用されません
	デバイスとしてイン		
	ストールされるFTD		

Firepower DAQフェーズのトラブルシューティング

DAQ(データ収集)レイヤは、パケットをSnortが理解できる形式に変換するFirepowerのコンポ ーネントです。Snortに送信されると、最初にパケットが処理されます。したがって、パケットが 入力されていてもFirepowerアプライアンスから出力されていない場合、またはパケット入力のト ラブルシューティングで有用な結果が得られなかった場合は、DAQのトラブルシューティングが 役立ちます。

DAQレイヤでのトラフィックのキャプチャ

キャプチャを実行するプロンプトを表示するには、まずSSHを使用してSFRまたはFTDのIPアド レスに接続する必要があります。

注:FPR-9300および4100デバイスで、**connect ftd**を最初に入力し、2番目の>プロンプトで 終了します。また、FXOS Chassis Manager IPにSSH接続し、**connect module 1 console**、 **connect ftdの順**に入力することも**できます**。

```
この記事<u>では</u>、Firepower DAQレベルでパケットキャプチャを収集する方法について説明します
。
```

構文は、FTDプラットフォームのLINA側だけでなく、ASAで使用される**captureコマンドと同じ**で はないことに注意してください。FTDデバイスから実行されるDAQパケットキャプチャの例を次 に示します。

> system support capture-traffic	
Please choose domain to capture traffic from:	
0 - br1	
1 - Router	
2 - my-inline inline set	
Selection? 2	
Please specify tcpdump options desired.	
(or enter '?' for a list of supported options)	
Options: -s 1518 -w ct.pcap	
> expert	
admin@ciscoasa:~\$ ls /ngfw/var/common/	
ct.pcap	

上のスクリーンショットに示すように、ct.pcapというPCAPフォーマットのキャプチャが /ngfw/var/commonディレクトリ(SFRプラットフォームで/var/common)に書き込まれました。 こ れらのキャプチャファイルは、上記の記事の指示に従って、>プロンプトからFirepowerデバイス からコピー<u>すること</u>ができます。

または、Firepowerバージョン6.2.0以降のFirepower Management Center(FMC)で、[デバイス (Devices)] > [デバイス管理(Device Management)]に移動します。次に、 ※ アイコンをクリック し、その後に[Advanced Troubleshooting] > [File Download]をクリックします。

キャプチャファイルの名前を入力し、[Download]をクリックします。

Overview Analysis Policies Devic	es Objects Al	MP Intelligence										Deploy 0g Sys	stem Help 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses •	Health > Monitor	Monitoring •	Tools •
Advanced Troubleshooting														
File Download Threat Defense CLI	Packet Tracer	Capture w/Trace												
			File	ct.pcap										
					Download	Back								

Firepowerをバイパスする方法

Firepowerがトラフィックを検出しているものの、パケットがデバイスから出ていないか、トラフィックに別の問題があると判断された場合は、次のステップとしてFirepower検査フェーズをバイパスし、Firepowerコンポーネントの1つがトラフィックをドロップしていることを確認します。 次に、さまざまなプラットフォームでFirepowerをバイパスするトラフィックの最も高速な方法の 内訳を示します。

SFR:Firepowerモジュールをモニタ専用モードにします

SFRをホストするASAで、SFRモジュールをモニタ専用モードにするには、ASAコマンドライン インターフェイス(CLI)またはCisco Adaptive Security Device Manager(ASDM)を使用します。 こ れにより、ライブパケットのコピーだけがSFRモジュールに送信されます。

ASA CLIを使用してSFRモジュールをモニタ専用モードにするには、show service-policy sfrコマ ンドを実行して、SFRリダイレクトに使用するクラスマップとポリシーマップを最初に決定する 必要があります。

show service-policy sfr

Global policy: Service-policy: global_policy Class-map: sfr

SFR: card status Up, mode fail-open

packet input 10000, packet output 9900, drop 100, reset-drop 0

この出力は、global_policyポリシーマップが「sfr」クラスマップに対してsfr fail-openアクション を実行していることを示しています。

注:「fail-close」はSFRを実行できるモードですが、SFRモジュールがダウンしたり応答し なくなると、すべてのトラフィックがブロックされるため、一般的には使用されません。

SFRモジュールをモニタ専用モードにするには、次のコマンドを発行して、現在のSFR設定を無効にし、モニタ専用の設定を入力します。

configure terminal (config)# policy-map global_policy (config-pmap)# class sfr (config-pmap-c)# no sfr fail-open (config-pmap-c)# sfr fail-open monitor-only

INFO: The monitor-only mode prevents SFR from denying or altering traffic.

(config-pmap-c)# write memory
Building configuration...

モジュールがモニタ専用モードになると、show service-policy sfrの出力で確認できます。

sh service-policy sfr

Global policy: Service-policy: global_policy Class-map: sfr SFR: card status Up, mode fail-open monitor-only packet input 0, packet output 100, drop 0, reset-drop 0

注:SFRモジュールをインラインモードに戻すには、上に示す(config-pmap-c)#プロンプト からno sfr fail-open monitor-onlyコマンドを発行し、その後にsfr {fail-open | fail-close}コマン ドを使用します。

または、[Configuration] > [Firewall] > [Service Policy Rules]の順に移動して、ASDMを介してモジ ュールをモニタ専用に配置す**ることもできます。**次に、対象のルールをクリックします。次に、 [Rule Actions]ページ**に移動**し、[ASA FirePOWER Inspection]タブを**クリック**します。その後、 [Monitor-only]を選択できます。

SFRモジュールがモニタ専用モードであることが確認された後もトラフィックの問題が解決しない場合は、Firepowerモジュールが問題の原因ではありません。その後、Packet Tracerを実行して、ASAレベルでさらに問題を診断できます。

問題が解決しない場合は、次のステップとして、Firepowerソフトウェアコンポーネントのトラブ ルシューティングを行います。

FTD(すべて):インラインセットをTAPモードに配置

トラフィックがインラインセットで設定されたインターフェイスペアを通過する場合は、インラ インセットをTAPモードにすることができます。これにより、Firepowerはライブパケットに対し てアクションを実行しなくなります。デバイスはパケットをネクストホップに送信する前にパケ ットを変更する必要があり、トラフィックをドロップせずにバイパスモードに設定することはで きないため、インラインセットのないルータや透過モードには適用されません。インラインセッ トのないルーテッドモードおよびトランスペアレントモードの場合は、パケットトレーサの手順 に進みます。

FMCユーザインターフェイス(UI)からTAPモードを設定するには、[デバイ**ス] > [デバイス管理]に移動**し、該当するデバイスを編集します。[インラインセ**ット]タブ**で、[TAPモード]オプションを **オフにします**。

Devices	Routing	Interfaces	Inline Sets	DHCP	
Name	Interfa	ace Pairs			
my_inline	inline1.	<->inline2			🥟 🛅
E	dit Inline General	Set dvanced			1
	Tap Mode:				
	Propagate Lir	nk State:			
	Strict TCP En	forcement:			

TAPモードで問題が解決した場合、次のステップはFirepowerソフトウェアコンポーネントのトラ ブルシューティングです。

TAPモードで問題が解決しない場合、問題はFirepowerソフトウェアの対象外になります。その後、パケットトレーサを使用して、問題をさらに診断できます。

Packet Tracerを使用したシミュレーショントラフィックのトラ ブルシューティング

Packet Tracerは、パケットドロップの場所を特定するのに役立つユーティリティです。シミュレ ータであるため、人工パケットのトレースを実行します。

SFR:ASA CLIでのPacket Tracerの実行

SSHトラフィック用にASA CLIでパケットトレーサを実行する方法の例を次に示します。packet tracerコマンドの構文の詳細については、『ASA Series Command Reference guide』のこの項を <u>参照し</u>てください。

asa# packet-tracer input inside tcp 192.168.62.60 10000 10.10.10.10 ssh Phase: 1 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase: 2 Type: ROUTE-LOOKUP Subtype: Resolve Egress Interface Result: ALLOW Config: Additional Information: found next-hop 10.151.37.1 using egress ifc outside Phase: 3 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information:	Phase: 4 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 5 Type: SFR Subtype: Result: ALLOW Config: class-map inspection_default match any policy-map global_policy class inspection_default sfr fail-open service-policy global_policy global Additional Information:
Phase: 6 Type: INSPECT Subtype: np-inspect Result: ALLOW Config: class-map inspection_default match any policy-map global_policy class inspection_default inspect icmp service-policy global_policy global Additional Information: Phase: 7 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Phase: 8 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information:	Phase: 9 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 756, packet dispatched to next module Result: input-interface: inside input-interface: inside input-status: up output-line-status: up output-interface: outside output-status: up output-line-status: up Action: allow

上記の例では、ASAとSFRモジュールの両方がパケットを許可し、ASAによるパケットフローの 処理方法に関する有用な情報が表示されています。

FTD(すべて):FTD CLIでパケットトレーサを実行します。

すべてのFTDプラットフォームで、packet tracerコマンドはFTD CLIから実行できます。

> packet-tracer input inside tcp 192.168.62.60 10000 10.10.10.10 ssh

Phase: 1 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list

Phase: 2 Type: ROUTE-LOOKUP Subtype: Resolve Egress Interface Result: ALLOW Config: Additional Information: found next-hop 192.168.100.1 using egress ifc outside Phase: 3 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_global access-list CSM_FW_ACL_advanced permit ip any any rule-id 268434433 access-list CSM_FW_ACL_remark rule-id 268434433: ACCESS POLICY: My_AC_Policy - Mandatory access-list CSM_FW_ACL_remark rule-id 268434433: L7 RULE: Block urls Additional Information: This packet will be sent to snort for additional processing where a verdict will be reached Phase: 4 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default

match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:

Phase: 5 Type: NAT Subtype: Result: ALLOW Config: object network 62_network nat (inside,outside) dynamic interface Additional Information: Dynamic translate 192.168.62.60/10000 to 192.168.100.51/10000

Phase: 6 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information:

Phase: 7 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 8 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information:

Phase: 9 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information:

Phase: 10 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 612016, packet dispatched to next module Phase: 11 Type: EXTERNAL-INSPECT Subtype: Result: ALLOW Config: Additional Information: Application: 'SNORT Inspect'

Phase: 12 Type: SNORT Subtype: Result: DROP Config: Additional Information: Snort Trace: Packet: TCP, SYN, seq 1821549761 Reputation: packet blacklisted, drop Snort: processed decoder alerts or actions queue, drop IPS Event: gid 136, sid 1, drop Snort detect_drop: gid 136, sid 1, drop NAP id 1, IPS id 0, Verdict BLACKLIST, Blocked by Reputation Snort Verdict: (black-list) black list this flow

この例では、パケットトレーサはドロップの理由を示しています。この場合、これはFirepowerの セキュリティインテリジェンス機能のIPブラックリストであり、パケットをブロックしています 。次のステップは、ドロップの原因となる個々のFirepowerソフトウェアコンポーネントのトラブ ルシューティングです。

トレースによるキャプチャを使用したライブトラフィックのトラ ブルシューティング

ライブトラフィックは、トレース機能を使用してキャプチャをトレースすることもできます。この機能は、CLIですべてのプラットフォームで使用できます。次に、SSHトラフィックに対する トレースを使用してキャプチャを実行する例を示します。

<pre>> capture ssh_traffic traf > show capture ssh_traf</pre>	ce interface inside match tcp any any eq 22 ffic
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 1045829951<="" 1460,sackok,timestamp="" th=""></mss>
0,nop,wscale 7>	
2: 01:17:38.510898	10.83.180.173.22 > 192.168.62.70.48560: S 903999422:903999422(0) ack 4250994242 win 17896 <mss 1380,sackok,timestamp<="" td=""></mss>
513898266 1045829951	1,nop,wscale 7>
3: 01:17:38.511402	192.168.62.70.48560 > 10.83.180.173.22: . ack 903999423 win 229 <nop,nop,timestamp 1045829956="" 513898266=""></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,timestamp< td=""></nop,timestamp<>
1045829957 513898266	3>
5: 01:17:38.513294	10.83.180.173.22 > 192.168.62.70.48560: . ack 4250994283 win 140 <nop.nop.timestamp 1045829957="" 513898268=""></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 513898282<="" td=""></nop.nop.timestamp>
1045829957>	
7:01:17:38.528613	192.168.62.70.48560 > 10.83.180.173.22: . ack 903999444 win 229 <nop,nop,timestamp 1045829961="" 513898282=""></nop,nop,timestamp>

> show capture ssh_traffic packet-number 4 trace Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW 7 packets captured 4: 01:17:38.511982 192.168.62.70.48560 > 10.83.180.173.22: P Config: Additional Information 50994242:4250994283(41) ack 903999423 win 229 < nop, nop, timestamp 1045829957 513898266> Found flow with id 626406, using existing flow Phase: 1 Type: CAPTURE Phase: 4 Type: EXTERNAL-INSPECT Subtype Result: ALLOW Subtype Result: ALLOW Config: Additional Information: Config: MAC Access list Additional Information: RT Ins Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase: 5 Type: SNORT Subtype: **Result: ALLOW** Config: Additional Information: Snort Trace: Packet: TCP, ACK, seq 4250994242, ack 903999423 AppID: service SSH (846), application unknown (0) Firewall: starting rule matching, zone 1 -> 2, geo 0 -> 0, vlan 0, sgt 65535, user 2, icmpType 0, icmpCode 0 Firewall: trust/fastpath rule, id 268435458, allow NAP id 1, IPS id 0, Verdict WHITELIST Snort Verdict: (fast-forward) fast forward this flow

Result: input-interface: inside input-status: up input-line-status: up Action: allow

この例では、アプリケーションデータが定義された最初のパケットであるため、キャプチャの4番目のパケットがトレースされました。図に示すように、パケットはsnortによってホワイトリスト に表示されます。つまり、フローに対してこれ以上snort検査が必要なく、全体が許可されます。

トレース構文を使用したキャプチャの詳細については、『ASA Series Command Reference guide』の<u>このセクショ</u>ンを参照してください。

FTD (すべて):FMC GUIでのトレースによるキャプチャの実行

FTDプラットフォームでは、トレースによるキャプチャをFMC UIで実行できます。このユーティリティにアクセスするには、[Devices] > [Device Management]に移動します。

次に、 **※** アイコンをクリックし、次に[Advanced Troubleshooting] > [Capture w/Trace]をクリッ クします。

次に、GUIを介してトレースを使用してキャプチャを実行する方法の例を示します。

Add Capture						? ×			
Name*:	Test		Interface*:	Inside		~			
Match Criteria:									
Protocol*:	ТСР	~							
Source Host*:	192.168.1.200		Source Network:	255.255.2	255.255				
Destination	any		Destination						
Host*:			Network:					Click	king Add Capture
SGT number:	0		(0-65535)					butto	on will display this
Buffer:								popu	up window
Packet Size:	1518	14-1522 bytes	Continuous Cap	ture	Trace		1		
Buffer Size:	524288	1534-33554432 bytes	 Stop when full 		Trace Count:	1000			
					Save	Cancel			
Advanced Troubleshoot 10.83.181.27 File Download Threat Defense C Auto Refresh Interval (seconds): 10 Name Test	CLI Packet Tracer Capture	e w/Trace Interface Imice	Type Trace Buffer Buf Mode Size raw-data of a 32	fer Packet Length 158 1518	Buffer Protocol Sourc Status Caduring TCP 192.1	ce Destination	Add Capture Status Running 2 5 2 1		View of all current
Advanced Troubleshoo	bting]	
File Download Threat Defens	se CLI Packet Tracer Cap	ture w/Trace							
C Packets Shown: 577 / Packets C Type: CAPTURE Subtypes Result: ALCOM Config: Additional Information: MCACCess List Dabtype: Packet 2 Type: ACCESS-LIST Booking Results ALCOM Packet 2 Type: Thomas Configuration Results ALCOM Additional Information MCACcess List	laptured: 577 / Traces: 298			*			Format: Raw	Esb	xample output hows the packet was locked by Snort
Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found flow with id 2672128, u	using existing flow								
Phase: 4 Type: EXTERNAL-INSPECT Subtype: Result: ALLOW Config: Additional Information: Application: 'SNORT Inspect'									
Phase: 5 Type: SNORT Subtype: Result: DROP Config: Additional Information: Snort Verdict: (block-packet)) drop this packet 🔶		- Snort Verd	lict: (b	olock-pacl	ket) drop	this packe	et	
Result: input-interface: Inside input-status: up				V.		· · · · · · ·			
Last login on Thursday, 2017-05-11 at 14:5	54:07 PH from 10.151.32.47							-ili-ili- cisco	

トレースを使用したキャプチャがパケット廃棄の原因を示している場合は、次のステップとして 個々のソフトウェアコンポーネントのトラブルシューティングを行います。

問題の原因が明確に示されていない場合は、次のステップとしてトラフィックの高速パスを設定 します。

FTDでのPreFilter Fastpathルールの作成

すべてのFTDプラットフォームには、Pre-Filter Policyがあり、Firepower(snort)インスペクション からトラフィックを転送するために使用できます。

FMCでは、[Policies] > [Access Control] > [**Prefilter**]の下**にあります**。デフォルトのプレフィルタ ポリシーは編集できないため、カスタムポリシーを作成する必要があります。

その後、新しく作成したPrefilter Policyをアクセスコントロールポリシーに関連付ける必要があり ます。これは、[プレフィルタポリシーの設定]セクションの[アクセスコントロールポリシー]の[**詳** 次に、プレフィルタポリシー内でFastpathルールを作成し、ヒットカウントを確認する方法の例 を示します。

Name Action	ter rules perform early har fastpath 192.168.62. Fastpath	odling of traffi	c based on simpl	le network cha	racteristics. Fastp	athed traffic by	below rule	control and Qo	× 1					
Inter Available any IPv4-f 2 10_83 62_ne any-ig 2 IPv4-f IPv4-f 1 IPv4-f 2 IPv4-f	rface Objects Networks C Networks C Private-All-RPC1918 [_181_1 twork w4 w4 w5 Benchmark-Tests Jink-Local Multicast Yrivate-10.0.0.0-8	rks VLAN	Add to Destinat	o e tion Enter	e Networks (1) 32.168.62.60 an IP address		Add	Destination 1 any	Con letworks (0) ldress	nment I	Logging		Clicki Rule this p	ng Add Prefilter button will display opup window.
fastp Enter Der Rules	ath test scription	Pule Type	Source	Destination	Source	Destination	Add	Tunnel Rule	Add Prefilter R VI AN Tag	Action	ch Rules	Save Cancel		View of all rules i
1 Non-tur	fastpath 192.168.62.60	Prefilter	any	any	Networks	Networks	Port	Port	any	→ Fastp	ath na			the fastpath test Prefilter policy
-							_			_				
Prefi	iter Policy:	fastpat	<u>:h test</u>						? ×					
Prefi Pref	Iter Policy: ilter Policy e prefilter poli rracteristics, i fense only.) stpath test	fastpat y icy perf ncludir	<u>th test</u> forms ea ng non-e	arly traf	fic handl ed encap	ling usin sulation	g simp . (Firep	ole netwo power Th	? X prk ireat			From sure is set	AC po the Pre	licy make filter Policy custom

View of connection events matching prefilter rule

	▼ <u>First Packet</u> ×	Last Packet ×	Action ×	<u>Reason</u> ×	Initiator IP ×	Responder × IP	Source Port / X ICMP Type	Destination Port / × ICMP Code	Prefilter × Policy	<u>Tunnel/Prefilter</u> × <u>Rule</u>
↓ □	2017-05-15 16:05:14	2017-05-15 16:05:14	Fastpath		192.168.62.60	10.83.180.173	<u>48480 / tcp</u>	22 (ssh) / tcp	fastpath test	fastpath 192.168.62.60

<u>プレフィルタポ</u>リシーの操作と構成の詳細については、ここをクリックしてください。

PreFilterポリシーを追加してトラフィックの問題を解決した場合は、必要に応じてルールを残す ことができます。ただし、そのフローに対する検査は行われません。Firepowerソフトウェアの詳 細なトラブルシューティングを実行する必要があります。

Prefilter Policyを追加しても問題が解決しない場合は、トレースステップを含むパケットを再度実 行して、パケットの新しいパスをトレースできます。

TACに提供するデータ

Data コマンド出力

パケット キャプチャ

ASAの「show tech」出力

手順 手順については、 ASA/LINAの場合 <u>configure-asa-00</u> Firepowerの場合 <u>technote-sourcefi</u> ASA CLIにログイ 出力ファイルを扱 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.o

次のステップ

Firepowerソフトウェアコンポーネントが問題の原因であると判断された場合は、次のステップとして、セキュリティインテリジェンスから始めて、各コンポーネントを体系的に除外します。

ここをク<u>リック</u>して、次のガイドに進みます。