Fase 2 della risoluzione dei problemi del percorso dei dati di Firepower: Livello DAQ

Sommario

Introduzione Guida alla piattaforma Risoluzione dei problemi relativi alla fase DAQ di Firepower Acquisizione del traffico sul layer DAQ Come ignorare Firepower SFR - Attivare la modalità solo monitor per il modulo Firepower FTD (all) - Imposta set inline in modalità TAP Uso di Packet Tracer per risolvere i problemi relativi al traffico simulato SFR - Esegui Packet Tracer sulla CLI ASA FTD (all) - Esegui packet tracer sulla CLI FTD Uso di Acquisisci con traccia per risolvere i problemi relativi al traffico in tempo reale FTD (all) - Acquisizione con traccia in esecuzione sull'interfaccia utente di FMC Creazione di una regola Fastpath del prefiltro in FTD Dati da fornire a TAC Passaggio successivo

Introduzione

Questo articolo fa parte di una serie di articoli che spiegano come risolvere in modo sistematico i problemi relativi al percorso dei dati nei sistemi Firepower per determinare se i componenti di Firepower possono influire sul traffico. Per informazioni sull'architettura delle piattaforme Firepower e per i collegamenti agli altri articoli sulla risoluzione dei problemi relativi ai percorsi di dati, consultare l'<u>articolo</u> di <u>panoramica</u>.

In questo articolo verrà esaminata la seconda fase della risoluzione dei problemi relativi al percorso dati di Firepower: il livello DAQ (Data Aquisition).



Guida alla piattaforma

Nella tabella seguente vengono descritte le piattaforme descritte in questo articolo.

Nome codice piattaform a	Descrizione	Applicabile Hardware Piattaforme	Note
SFR	ASA con modulo Firepower Services	Serie ASA-5500-X	N/D

(SFR) installato.

FTD (tutto)	Si applica a tutte le piattaforme Firepower Threat Defense (FTD)	ASA serie 5500-X, piattaforme NGFW virtuali, FPR-2100, FPR-9300, FPR- 4100	N/D
FTD (non SSP e FPR- 2100)	Immagine FTD installata su un'ASA o una piattaforma virtuale	ASA serie 5500-X, piattaforme NGFW virtuali, FPR-2100	N/D
FTD (SSP)	FTD installato come dispositivo logico su uno chassis basato su Firepower eXtensible Operative System (FXOS)	FPR-9300 e FPR-4100	La serie 2100 non utilizza FXOS Chassis Manager

Risoluzione dei problemi relativi alla fase DAQ di Firepower

Il livello DAQ (Data Aquisition) è un componente di Firepower che converte i pacchetti in un formato che snort può comprendere. Gestisce inizialmente il pacchetto quando viene inviato allo snort. Pertanto, se i pacchetti in entrata ma non in uscita dall'appliance Firepower o la risoluzione dei problemi di entrata dei pacchetti non ha dato risultati utili, la risoluzione dei problemi tramite DAQ può essere utile.

Acquisizione del traffico sul layer DAQ

Per visualizzare la richiesta da cui eseguire l'acquisizione, è necessario prima connettersi con SSH all'indirizzo IP SFR o FTD.

Nota: Sui dispositivi FPR-9300 e 4100, immettere prima **connect ftd**, per terminare al secondo > prompt. Inoltre, è possibile eseguire il protocollo SSH sull'indirizzo IP di FXOS Chassis Manager, quindi immettere la **console del modulo di connessione 1** e **infine connettere il dispositivo ftd**.

In questo <u>articolo</u> viene spiegato come raccogliere le acquisizioni dei pacchetti a livello DQ di Firepower.

La sintassi è diversa da quella del comando **capture** usato sull'ASA e sul lato LINA della piattaforma FTD. Di seguito è riportato un esempio di acquisizione pacchetti DAQ eseguita da un dispositivo FTD:

> system support capture-traffic
Please choose domain to capture traffic from:
0 - br1
1 - Router
2 - my-inline inline set
Selection? 2
Please specify topdump 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

Come mostrato nella schermata precedente, un'acquisizione sul formato PCAP chiamata ct.pcap è stata scritta nella directory **/ngfw/var/common** (**/var/common** sulla piattaforma SFR). Questi file di acquisizione possono essere copiati dal prompt > della periferica Firepower utilizzando le istruzioni riportate nell'<u>articolo</u> sopra.

In alternativa, nel Firepower Management Center (FMC) di Firepower versione 6.2.0 e successive, selezionare **Dispositivi > Gestione dispositivi**. Quindi, fare clic sul pulsante accanto al dispositivo in questione, quindi selezionare **Advanced Troubleshooting > File Download**.

Èquindi possibile immettere il nome del file di acquisizione e fare clic su Download.

Overview Analysis Policies Device	s Objects A	MP Intelligence										Deploy 0 Sy	stem Help v	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 B	ack								

Come ignorare Firepower

Se Firepower rileva il traffico, ma è stato determinato che i pacchetti non stanno uscendo dal dispositivo o che esiste un altro problema con il traffico, il passaggio successivo consiste nell'ignorare la fase di ispezione di Firepower per confermare che uno dei componenti Firepower sta eliminando il traffico. Di seguito è riportata una descrizione del modo più veloce per evitare che il traffico ignori Firepower sulle varie piattaforme.

SFR - Attivare la modalità solo monitor per il modulo Firepower

Sull'appliance ASA che ospita l'SFR, è possibile configurare il modulo SFR in modalità di solo monitoraggio tramite l'interfaccia della riga di comando ASA (CLI) o Cisco Adaptive Security Device Manager (ASDM). In questo modo, solo una copia dei pacchetti live viene inviata al modulo SFR.

Per porre il modulo SFR in modalità di solo monitoraggio tramite la CLI di ASA, la mappa delle classi e la mappa dei criteri utilizzate per il reindirizzamento SFR devono essere determinate prima tramite il comando **show service-policy sfr**.

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

L'output mostra che la mappa dei criteri global_policy sta applicando l'azione di apertura degli errori della sfr sulla mappa delle classi "sfr".

Nota: "fail-close" è anche una modalità in cui può essere eseguito l'SFR, ma non è così comunemente utilizzato in quanto blocca tutto il traffico se il modulo SFR è inattivo o non risponde.

Per impostare il modulo SFR in modalità di solo monitoraggio, è possibile utilizzare questi comandi per negare la configurazione SFR corrente e accedere alla configurazione di solo monitoraggio:

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...

Una volta che il modulo è stato messo in modalità solo monitor, è possibile verificarlo nell'output del comando **show service-policy sfr**.

```
# 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
```

Nota: Per ripristinare la modalità in linea del modulo SFR, usare il comando no sfr fail-open monitor-only dal prompt (config-pmap-c)# mostrato sopra, seguito dal comando sfr {fail-open | fail-close}, comando originariamente presente.

In alternativa, è possibile configurare il modulo in modo che sia disponibile solo per il monitoraggio tramite ASDM selezionando **Configurazione > Firewall > Regole dei criteri di servizio**. Quindi, fare clic sulla regola in questione. Quindi, andare alla pagina **Azioni regola** e fare clic sulla scheda **ASA FirePOWER Inspection**. In questo modo, è possibile selezionare **solo monitor**.

Se il problema persiste anche dopo che è stato confermato che il modulo SFR è in modalità solo monitor, il modulo Firepower non lo causa. È quindi possibile eseguire Packet Tracer per diagnosticare ulteriormente i problemi a livello di ASA.

Se il problema persiste, il passaggio successivo consiste nella risoluzione dei problemi dei componenti software di Firepower.

FTD (all) - Imposta set inline in modalità TAP

Se il traffico passa attraverso coppie di interfacce configurate in set inline, il set inline può essere messo in modalità TAP. In questo modo, Firepower non interviene sul pacchetto live. Non si applica al router o alla modalità trasparente senza set in linea, in quanto il dispositivo deve modificare i pacchetti prima di inviarli all'hop successivo e non può essere impostato su una modalità bypass senza interrompere il traffico. Per la modalità instradata e trasparente senza set inline, procedere con il passaggio packet tracer.

Per configurare la modalità TAP dall'interfaccia utente di FMC, selezionare **Dispositivi > Gestione dispositivi**, quindi modificare il dispositivo in questione. Nella scheda **Insiemi in linea**, selezionate l'opzione **Modalità MASCHIO**.



Se la modalità TAP risolve il problema, il passaggio successivo consiste nella risoluzione dei problemi dei componenti software Firepower.

Se la modalità TAP non risolve il problema, il problema è esterno al software Firepower. È quindi

possibile utilizzare Packet Tracer per diagnosticare ulteriormente il problema.

Uso di Packet Tracer per risolvere i problemi relativi al traffico simulato

Packet Tracer è un'utilità che può aiutare a identificare la posizione in cui un pacchetto viene scartato. È un simulatore, quindi esegue una traccia di un pacchetto artificiale.

SFR - Esegui Packet Tracer sulla CLI ASA

Di seguito è riportato un esempio di come eseguire packet-tracer sulla CLI di ASA per il traffico SSH. Per informazioni più dettagliate sulla sintassi del comando packet tracer, consultare questa <u>sezione</u> della guida di riferimento dei comandi della serie ASA.



Nell'esempio precedente, vengono mostrati sia il modulo ASA che il modulo SFR che permette l'uso dei pacchetti, oltre a informazioni utili su come l'ASA gestirebbe il flusso dei pacchetti.

FTD (all) - Esegui packet tracer sulla CLI FTD

Su tutte le piattaforme FTD, il comando packet tracer può essere eseguito dalla CLI FTD.

> 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** Confia: 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

Nell'esempio, il tracer del pacchetto mostra il motivo della perdita. In questo caso, è la blacklist IP all'interno della funzionalità Security Intelligence di Firepower a bloccare il pacchetto. Il passaggio successivo consiste nella risoluzione dei problemi relativi al singolo componente software Firepower che causa la caduta.

Uso di Acquisisci con traccia per risolvere i problemi relativi al traffico in tempo reale

Il traffico in tempo reale può essere tracciato anche tramite la funzione di acquisizione con traccia, disponibile su tutte le piattaforme dalla CLI. Di seguito è riportato un esempio di esecuzione di un'acquisizione con traccia sul traffico SSH.

> capture ssh_traffic trac > show capture ssh_traff	e interface inside match tcp any any eq 22 ic
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	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,nop,timestamp< td=""></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,top,timestamp 1045829957="" 513898268=""></nop,top,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 7 packets captured 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< 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</nop,nop,timestamp<>	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: Application: 'SNORT Inspect'
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 Firewall: trust/fastpath rule, id 268435458, allow NAP id 1, IPS id 0, Verdict WHITELIST Snort Verdict: (fast-forward) fast forward this flow), vlan 0, sgt 65535, user 2, icmpType 0, icmpCode 0
Result: input-interface: inside input-status: up input-line-status: up Action: allow	

Nell'esempio riportato sotto, è stato tracciato il quarto pacchetto nell'acquisizione, poiché è il primo pacchetto con dati dell'applicazione definiti. Come mostrato nella figura, il pacchetto viene quindi reso bianco da uno snort, il che significa che non è necessaria un'ulteriore ispezione dello snort per il flusso, ed è consentito in generale.

Per ulteriori informazioni sulla sintassi di acquisizione con trace, consultare questa <u>sezione</u> della guida di riferimento dei comandi della serie ASA.

FTD (all) - Acquisizione con traccia in esecuzione sull'interfaccia utente di FMC

Nelle piattaforme FTD è possibile eseguire l'acquisizione con traccia nell'interfaccia utente di FMC. Per accedere all'utility, selezionare **Dispositivi > Gestione dispositivi**.

Quindi, fare clic sul pulsante a accanto al dispositivo in questione, quindi selezionare Advanced Troubleshooting > Capture w/Trace.

Di seguito è riportato un esempio di come eseguire un'acquisizione con trace tramite la GUI.

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							
SGT number:	0		(0_65525)					C	ickin	g Add Capture
Buffer:	U		(0-05555)					bu	utton	will display this
Packet Size:	1518	14-1522 bytes		oturo	7 T			pc	pup	window
Buffer Size:	524288	1534-33554432	 Stop when full 	Juie	Trace Count:	1000				
		bytes			Save	Cancel				
Advanced Troubleshoot IBAB.181.27 THE Download Threat Defense G Auto Refresh Sterver (seconds): [30 Rame Test	Ing CLI Packet Tracer Capitur Datie Auto Retreat	re tr/Trace Interface Inste	Type Trees Buffer Buf Hole Siz reardels √ jij 224	fer Packet B Length 208 1518	Buffar Protocol So Status Costuring TCP 192	arca Destination 1968.1.200 ery	C Adi		_	View of all current captures
Advanced Troubleshoo	ting									
File Download Threat Defens	e CLI Packet Tracer Cap	pture w/Trace								
G Packets Shown: S7/ Packets C Type: CATURE Subtype: Bustype: Bustype: Additional Information: MAC Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config Result: ALLOW Config Maditional Information: Maditional Information: Maditional Information: Mathematical Statematical Mathematical	aptured: 577 / Traces: 298						Format: Re		Exa sho	imple output ws the packet was
MAC Access list Phase: J Type: FLOW-LOOKUP Sobtype: Nesult: ALLOW Cooffig: Additional Information: Found flow with id 2672128, w Phase: 4	using existing flow									sked by chort
Type: EXTERNAL-INSPECT Subtype: Result: ALLOW Config: Additional Information: Application: 'SNORT Inspect'										
Phase: 5 Type: SNOT Subtype: Pesult: DROP Cosfig: Additional Information: Additional Snort Verdict: (block-packet)) drop this packet 🗲		- Snort Verd	dict: (k	olock-pac	:ket) drop	this pac	ket		
Result: input-interface: Inside input-status: up										
Last login on Thursday, 2017-05-11 at 14:5	4:07 PH from 10.151.32.47							cisco		

Se l'acquisizione con traccia indica la causa del rilascio del pacchetto, il passaggio successivo consiste nella risoluzione dei problemi dei singoli componenti software.

Se la causa del problema non è indicata chiaramente, procedere come segue per velocizzare il traffico.

Creazione di una regola Fastpath del prefiltro in FTD

Su tutte le piattaforme FTD è presente una Policy Pre-Filter, che può essere utilizzata per deviare il traffico dall'ispezione Firepower (snort).

Nel FMC, è disponibile in **Policy > Controllo di accesso > Prefiltro**. Impossibile modificare il criterio di prefiltro predefinito. È quindi necessario creare un criterio personalizzato.

In seguito, è necessario associare il nuovo criterio di filtro al criterio di controllo dell'accesso. Questa impostazione è configurata nella scheda Avanzate di Criteri di controllo di accesso della sezione Impostazioni criteri filtro preliminare.

Di seguito è riportato un esempio di come creare una regola Fastpath in un criterio di prefiltro e verificare il numero di accessi.

Name	fastpath 192.168.62	.60		🗹 Ena	abled	Insert	below rule		• 1						
Action	Fastpath		¥												
Inter	ace Objects Netwo	vLAN	N Tags Ports	s					Com	mment Loggi	ing				
vailable I	ietworks C		0	Source	e Networks (1)			Destination Net	tworks (0)						
			-	22 19	2.168.62.60			any							
any															
IPv4-Pr	vate-All-RFC1918												Clicki	ng Add Pre	filter
62 001	_181_1		Add	to									Dula	button will d	icolov
anv-in	4		Sour	ce									Rule	bullon will u	ispiay
any-in	5		Add	to									this po	obup windo	V.
IPv4-B	enchmark-Tests		Destine												
IPv4-Li	nk-Local														
IPv4-M	ulticast														
IPv4-Pr	ivate-10.0.0.0-8														
				Enter	an IP address		Add	Enter an IP add	ress		Add				
				criter			Aud	Lincer un ir uudi			AUU				
									Add	Cancel	5				
_		_					_		_		_				
Rules							🔾 Add	Tunnel Rule	Add Prefilter R	Rule Search Rule	les	×		View of all	rules i
#	Name	Rule Type	Source Interface	Destination Interface	Source Networks	Destination Networks	O Add Source Port	Tunnel Rule O Destination Port	Add Prefilter R	Rule Search Rule	les Tunnel Zo	×		View of all	rules i th test
# 1	Name fastpath 192.168.62.60	Rule Type Prefilter	Source Interface any	Destination Interface any	Source Networks	Destination Networks	Add Source Port any	Tunnel Rule O Destination Port any	Add Prefilter R VLAN Tag any	Rule Search Rule Action → Fastpath	les Tunnel Zo na	×	-	View of all the fastpa Prefilter po	rules i th test
# 1 Non-tunr	Name fastpath 192.168.62.60 eled traffic is	Rule Type Prefilter	Source Interface any	Destination Interface any	Source Networks	Destination Networks	Add Source Port any	Tunnel Rule O Destination Port any	Add Prefilter R VLAN Tag any	Rule Search Rule Action → Fastpath	ies Tunnel Zo na	×	-	View of all the fastpa Prefilter po	rules i th test blicy
# 1 Non-tunr	Name fastpath 192.168.62.60 eled traffic is	Rule Type Prefilter	Source Interface any	Destination Interface any	Source Networks	Destination Networks	Add Source Port any	Tunnel Rule O Destination Port any	Add Prefilter R VLAN Tag any	Rule Search Rule Action → Fastpath	les Tunnel Zo na	×	-	View of all the fastpa Prefilter po	rules i th test blicy
# 1 Non-tunr	Name fastpath 192.168.62.60 eled traffic is	Rule Type Prefilter	Source Interface any	Destination Interface any	Source Networks 2 192.168.62.6	Destination Networks 50 any	Add Source Port any	Tunnel Rule O Destination Port any	Add Prefilter R VLAN Tag any	Rule Search Rule Action → Fastpath	ies Tunnel Zo na	× • • •	-	View of all the fastpa Prefilter po	rules i th test blicy
# 1 Non-tunn	Name fastpath 192.168.62.60 eled traffic is	Rule Type Prefilter	Source Interface any	Destination Interface any	Source Networks ₽ 192.168.62.6	Destination Networks	Add Source Port	Tunnel Rule O Destination Port any	Add Prefilter R VLAN Tag any	Rule Search Rule Action → Fastpath	na	×	-	View of all the fastpa Prefilter po	rules i th test blicy
n non-tunn	Name fastpath 192.168.62.60 eled traffic is ter Policy:	Rule Type Prefilter <u>fastpal</u>	Source Interface any	Destination Interface any	Source Networks	Destination Networks	Add Source Port any	Tunnel Rule O Destination Port any	Add Prefilter R	Rule Search Rula Action → Fəstpəth	les Tunnel Zo na	×	-	View of all the fastpa Prefilter po	rules i th test blicy
non-tunn	Name fastpath 192.168.62.60 eled traffic is	Rule Type Prefilter <u>fastpal</u>	Source Interface any th test	Destination Interface any	Source Networks	Destination Networks	Add Source Port	Tunnel Rule O Destination Port any	Add Prefilter R	Ruie Search Ruli Action → Fastpath	les Tunnel Zo na	×		View of all the fastpa Prefilter po	rules i th test blicy
refil	Name fastpath 192.168.62.60 eled traffic is tter Policy: ilter Polic	Rule Type Prefilter fastpat	Source Interface any: th test	Destination Interface any	Source Networks	Destination Networks	کمی Add Source Port any	Tunnel Rule O Destination Port any	Add Prefilter R VLAN Tag any	Rule Search Ruli Action → Fastpath	ies Tunnel Zo na	×		View of all the fastpa Prefilter po	rules i th test blicy
refil	Name fastpath 192.168.62.60 eled traffic is iter Policy:	Rule Type Prefilter <u>fastpat</u>	Source Interface any	Destination Interface any	Source Networks	Destination Networks	Add Source Port απγ	Tunnel Rule O Destination Port any	Add Prefilter R VLAN Tag any	Rule Search Ruli Action → Fastpath	na	×		View of all the fastpa Prefilter po	rules i th tes t licy
refil Prefil The	Name fastpath 192.168.62.60 eled traffic is ter Policy: ilter Polic prefilter pol	Rule Type Prefilter <u>fastpat</u> Y icy per	source Interface any th test	Destination Interface any	Source Networks ⊇ 192.168.62.6	Destination Networks 10 any	Add Source Port any	Tunnel Rule Destination Port any	Add Prefilter R VLAN Tag any	Rule Search Ruli Action → Fastpath	ies Tunnel Zo na	×		View of all the fastpa Prefilter po	rules i th tes t blicy
Prefil Prefil The cha	Name fastpath 192.168.62.60 eled traffic is iter Policy: ilter Policy prefilter polication racteristics,	Rule Type Prefilter fastpat	source Interface any th test	Destination Interface any	Source Networks ⊇ 192.168.62.6 fic handl d encap	Destination Networks 10 ary	Add Source Port any g simp . (Firep	Tunnel Rule Destination Port any	Add Prefilter R VLAN Tag any ? X	Ruie Search Rule Action → Fastpath	Tunnel Zo			View of all the fastpa Prefilter po	rules i th test llicy
r Non-tunn Prefil Pref	Name fastpath 192.168.62.60 eled traffic is tter Policy: ilter Policy: prefilter polic racteristics, i ense only.)	Rule Type Prefilter fastpat y icy per includir	source Interface any th test forms ea ng non-ea	Destination Interface any	Source Networks ⊇ 192.168.62.6 provide the second secon	Destination Networks 50 ary 50 ary 10 ary 10 ary 10 ary 10 ary	• Add Source Port any g simp (Firep	Tunnel Rule Destination Port any denetworr power Thr	Add Prefilter R VLAN Tag any ? X	Rule Search Rule Action → Fastpath	les Tunnel Zo na	From	AC pol	View of all the fastpa Prefilter po	rules i th test llicy
non-tunn Prefil Prefi The cha Defi	Name fastpath 192.168.62.60 eled traffic la iter Policy: ilter Policy: prefilter policatoristics, ense only.)	Rule Type Prefilter <u>fastpat</u> y icy per includir	forms ea ng non-f	any	Source Networks ⊇ 192.168.62.6 fic handl d encap:	Destination Networks 30 ary ing using sulation.	Add	Tunnel Rule O Destination Port any	Add Prefilter R VLAN Tag any ? X k eat	Ruie Search Rula	les Tunnel Zo na	From	AC pol	View of all the fastpa Prefilter po licy make filter Policy	rules i th test blicy
rone units of the second secon	Name fastpath 192.168.62.60 eled traffic is ter Policy: ilter Polic prefilter pol racteristics, i ense only.)	Rule Type Prefilter fastpat y icy per includir	source Interface any th test forms ea ng non-e	any	Source Networks ⊇ 192.168.62.6 fic handl td encaps	Destination Networks 10 any ing using sulation.	g simp	Tunnel Rule O Destination Port any ble networ power Thr	Add Prefiter R VLAN Tag any ? × rk eat	Rule Search Rule	les Tunnel Zo na	From	AC pol	View of all the fastpa Prefilter po licy make filter Policy	rules i th test blicy
Prefil The cha Defi fas	Name fastpath 192.168.62.60 eled traffic is ter Policy: ilter Polic prefilter pol racteristics, ense only.) tpath test	Rule Type Prefilter fastpat	source Interface eny th test forms ea ng non-e	any	Source Networks ⊇ 192.168.62.6 fic handl cd encap:	Destination Networks 10 ary ing using sulation.	Add Source Port αηγ	Tunnel Rule	Add Prefilter P VLAN Tag any ? X *k reat	Rule Search Rule	Tunnel Zo	From	AC pol the Pre	View of all the fastpa Prefilter po licy make filter Policy custom	rules i th test blicy
Prefil The cha Defr fas	Name fastpath 192.168.62.60 eled traffic is iter Policy: ilter Polic prefilter pol racteristics, i ense only.) tpath test	Rule Type Prefilter fastpat	source Interface any th test forms ea ig non-f	arly traf	Source Networks ⊇ 192.168.62.6 fic handl d encap:	Destination Networks 50 ary ing using sulation.	Add <u>Source</u> Port any	Destination Port any ble networ power Thr	Add Prefilter R VLAN Tag any ? X rk reat	Rule Search Rule	les Tunnel Zo na	From sure is se Prefi	AC pol the Pre t to the Iter Poli	View of all the fastpa Prefilter po licy make filter Policy custom cy	rules in th test blicy
Prefil The cha Defi fas	Name fastpath 192.168.62.60 eled traffic is iter Policy: ilter Policy: prefilter polic racteristics, i ense only.) tpath test	Rule Type Prefilter fastpat y icy per includir	source Interface any th test forms ea ng non-e	Destination Interface any	Source Networks ⊇ 192.168.62.6 fic handl d encaps	Destination Networks 20 ary ing using sulation.	کمی میر و simp (Firep	Destination Port any	Add Prefilter R VLAN Tag any ? X rk reat	Rule Search Rule	les Tunnel Zo na	From sure is se Prefi	AC pol the Pre t to the lter Poli	View of all the fastpa Prefilter po licy make filter Policy custom cy	rules in th test blicy
Prefil Prefil Prefil The cha Defi	Name fastpath 192.168.62.60 eled traffic la iter Policy: ilter Policy: prefilter polic racteristics, ense only.) tpath test	Rule Type Prefilter fastpat y icy per includir	source Interface any th test forms ea ng non-f	any	Source Networks ⊇ 192.168.62.6 fic handl d encap:	Destination Networks 10 ary	Add	Tunnel Rule	Add Prefitter R VLAN Tag any ? X tk teat	Rule Search Rule	les na	From sure is se Prefi	AC pol the Pre t to the ter Poli	View of all the fastpa Prefilter po licy make filter Policy custom cy	rules i th test blicy

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

Fare clic qui per ulteriori dettagli sul funzionamento e la configurazione dei criteri di prefiltro.

Se l'aggiunta di un criterio PreFilter risolve il problema di traffico, è possibile lasciare la regola attiva. Tuttavia, non viene effettuata alcuna ulteriore ispezione di tale flusso. Sarà necessario eseguire ulteriori operazioni di risoluzione dei problemi del software Firepower.

Se l'aggiunta del criterio di prefiltro non risolve il problema, è possibile eseguire nuovamente il pacchetto con la fase di traccia per tracciare il nuovo percorso del pacchetto.

Dati da fornire a TAC

Istruzioni
Per istruzioni, vedere questo articolo
Per ASA/LINA: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-
asa-00.html
Per Firepower: <u>http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000</u> sourcefire-00.html
Accedere alla CLI di ASA e salvare la sessione terminale in un log. Immettere il comando she
della sessione terminale a TAC.
Questo comando consente di salvare il file su disco o su un sistema di storage esterno. show tech reindirizzare il disco0:/show_tech.log
http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techno

Passaggio successivo

Se è stato determinato che il problema è causato da un componente software Firepower, il passaggio successivo consiste nell'escludere sistematicamente ogni componente, a partire da Security Intelligence.

Fare clic <u>qui</u> per procedere con la guida successiva.