Fase 4 della risoluzione dei problemi relativi al percorso dei dati di Firepower: Policy di controllo dell'accesso

Sommario

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'articolo di panoramica.

In questo articolo viene descritta la quarta fase della risoluzione dei problemi relativi al percorso dati di Firepower, ovvero Access Control Policy (ACP). Queste informazioni sono valide per tutte le piattaforme e le versioni Firepower attualmente supportate.

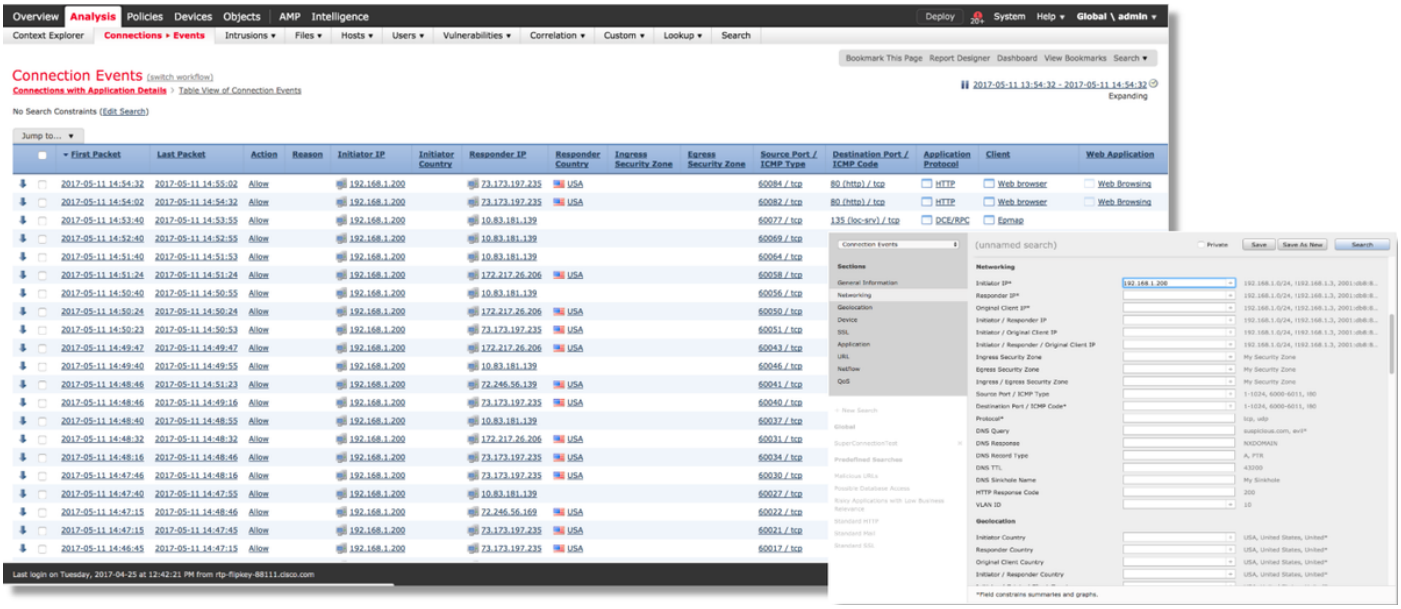
Risoluzione dei problemi relativi alla fase ACP (Access Control Policy)

In generale, determinare quale regola ACP corrisponde a un flusso dovrebbe essere piuttosto semplice. È possibile esaminare gli eventi di connessione per verificare quale regola/azione viene applicata. Se l'operazione non mostra chiaramente l'operazione del provider di servizi di audioconferenza con il traffico, è possibile eseguire il debug nell'interfaccia CLI (Command Line Interface) di Firepower.

Verifica eventi connessione

Dopo aver avuto un'idea dell'interfaccia in entrata e in uscita, il traffico dovrebbe corrispondere, così come le informazioni sul flusso, il primo passo per capire se Firepower sta bloccando il flusso è controllare gli eventi di connessione per il traffico in questione. È possibile visualizzarli in Firepower Management Center in **Analisi > Connessioni > Eventi.**

> **Nota:** Prima di controllare gli eventi di connessione, verificare che la registrazione sia abilitata nelle regole del provider di servizi di audioconferenza. La registrazione è configurata nella scheda "Registrazione" all'interno di ciascuna regola dei criteri di controllo di accesso e nella scheda Security Intelligence. Verificare che le regole sospette siano configurate per l'invio dei registri al "Visualizzatore eventi". Ciò vale anche per l'azione predefinita.



Facendo clic su "Edit Search" (Modifica ricerca) e filtrato da un indirizzo IP di origine univoco (Iniziatore), è possibile visualizzare i flussi rilevati da Firepower. Nella colonna Azione viene visualizzato "Consenti" per il traffico dell'host.

Se Firepower blocca intenzionalmente il traffico, l'azione conterrà la parola "Blocca". Facendo clic su "Table View of Connection Events" vengono forniti ulteriori dati. I seguenti campi negli eventi di connessione possono essere rivisti se l'azione è "Blocca":

- Motivo

- Regola di controllo di accesso

Attenuazione rapida

Per risolvere rapidamente un problema che si ritiene causato dalle norme ACP, è possibile effettuare le seguenti operazioni:

- Creare una regola con l'azione "Trust" (Considera attendibile) o "Allow" (Consenti) per il traffico in questione e collocarla al livello più alto del provider di servizi di audioconferenza o, soprattutto, delle regole di blocco.
- Disabilitare temporaneamente le regole con un'azione contenente la parola "Blocca"
- Se l'azione predefinita è impostata su "Blocca tutto il traffico", passare temporaneamente a "Solo individuazione rete"

Nota: Queste soluzioni rapide richiedono modifiche alle regole che potrebbero non essere possibili in tutti gli ambienti. Prima di apportare modifiche ai criteri, è consigliabile provare a utilizzare la traccia di supporto del sistema per determinare la regola che il traffico corrisponde.

Debug del provider di servizi di audioconferenza

Èpossibile eseguire ulteriori procedure di risoluzione dei problemi per le operazioni ACP tramite l'utility **> system support firewall-engine-debug** CLI.

Nota: Sulle piattaforme Firepower 9300 e 4100, è possibile accedere alla shell in questione tramite i seguenti comandi:

 # connetti console modulo 1
Firepower-module1**> connessione ftd**
>

Per le istanze multiple, è possibile accedere alla CLI del dispositivo logico con i seguenti comandi.
 # connect module 1 telnet
Firepower-module1**> connessione ftd ftd1**
Connessione alla console ftd(ftd1) del contenitore in corso... immettere "exit" per tornare alla CLI di avvio
>

L'utilità **system support firewall-engine-debug** ha una voce per ciascun pacchetto valutato dal provider di servizi di audioconferenza. Indica il processo di valutazione delle regole in corso e il motivo per cui una regola è associata o meno.

Nota: Nella versione 6.2 e successive, è possibile eseguire lo strumento di **traccia del supporto di sistema**. Vengono utilizzati gli stessi parametri ma vengono forniti ulteriori dettagli. Assicurarsi di immettere 'y' quando richiesto con "**Enable firewall-engine-debug too?"**.

Esempio 1: Il traffico corrisponde a una regola di trust

Nell'esempio seguente, la creazione di una sessione SSH viene valutata usando il **supporto di sistema firewall-engine-debug**.

Si tratta del punto ACP in esecuzione sul dispositivo Firepower.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Acti...
Mandatory - JG AC (all) (1-6)													
1	Trust ssh for host	Any	Any	192.168.0.7	Any	Any	Any	Any	Any	SSH	Any	Any	Trust
2	inspect	Any	Any	10.0.0.0/8	Any	Any	Any	Any	Any	Any	Any	Any	Allow
3	trust server backup	Any	Any	192.168.62.3	10.123.175.22	Any	Any	Any	Any	Any	Any	Any	Trust

L'ACP ha tre regole.

1. La prima regola è considerare attendibile il traffico proveniente da 192.168.0.7 con le porte di destinazione usate dal protocollo SSH.
2. La seconda regola controlla tutto il traffico originato da 10.0.0.0/8 in cui i criteri di rete corrispondono in base ai dati dell'intestazione XFF (come indicato dall'icona accanto all'oggetto di rete)
3. La terza regola considera attendibile tutto il traffico compreso tra 192.168.62.3 e 10.123.175.22

Nello scenario di risoluzione dei problemi, viene analizzata una connessione SSH da 192.168.62.3 a 10.123.175.22.

Ci si aspetta che la sessione corrisponda alla regola 3 dell'AC relativa al backup del server di trust. La domanda è: quanti pacchetti ci vogliono affinché questa sessione soddisfi questa regola? Sono necessarie tutte le informazioni nel primo pacchetto per determinare la regola AC o sono necessari più pacchetti, e in caso affermativo, quante?

Dalla CLI di Firepower, viene immesso quanto segue per visualizzare il processo di valutazione delle regole ACP.

```
>system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages
```

> **Suggerimento**: È consigliabile compilare il maggior numero di parametri possibile quando si esegue **firewall-engine-debug**, in modo che solo i messaggi di debug interessanti vengano stampati sullo schermo.

Nell'output del comando debug riportato di seguito vengono visualizzati i primi quattro pacchetti della sessione in fase di valutazione.

SYN

SYN,ACK

ACK

Primo pacchetto SSH (da client a server)

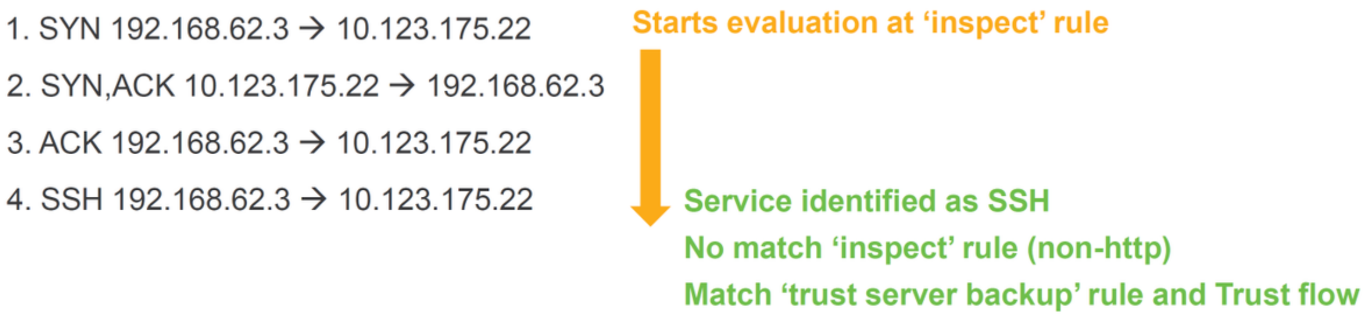
```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

Questo è un grafico che illustra ulteriormente la logica di debug.



Per questo flusso, sono necessari 4 pacchetti affinché il dispositivo soddisfi la regola.

Questa è una spiegazione dettagliata dell'output del comando debug.

- Il processo di valutazione del provider di servizi di audioconferenza inizia dalla regola "inspect" perché alla regola "trust ssh for host" non è stata associata alcuna corrispondenza poiché l'indirizzo IP non soddisfa il requisito. Questa corrispondenza è rapida perché tutte le informazioni necessarie per determinare se la regola deve corrispondere sono presenti nel primo pacchetto (IP e porte)
- Non è possibile determinare se il traffico soddisfa la regola "inspect" finché non viene identificata l'applicazione. Poiché le informazioni X-Forwarded-For (XFF) vengono trovate nel traffico dell'applicazione HTTP, l'applicazione non è ancora nota, in questo modo la sessione viene messa in sospeso per la regola 2, dati dell'applicazione in sospeso.
- Dopo aver identificato l'applicazione nel quarto pacchetto, la regola "inspect" determina una mancata corrispondenza, in quanto l'applicazione è SSH, anziché HTTP
- La regola "trust server backup" viene quindi soddisfatta in base agli indirizzi IP.

In breve, la connessione impiega 4 pacchetti per corrispondere alla sessione perché deve attendere che il firewall identifichi l'applicazione poiché la regola 2 contiene un vincolo per l'applicazione.

Se la regola 2 avesse solo reti di origine e non fosse XFF, sarebbe stato necessario 1 pacchetto per corrispondere alla sessione.

Èsempre consigliabile posizionare i livelli 1-4 delle regole al di sopra di tutte le altre regole nel criterio, quando possibile, poiché queste regole in genere richiedono un pacchetto per prendere una decisione. Tuttavia, è possibile notare che anche con i soli layer 1-4 delle regole, potrebbe essere necessario più di un pacchetto per soddisfare una regola AC e la ragione è l'intelligence di

sicurezza URL/DNS. Se si dispone di una di queste opzioni, il firewall deve determinare l'applicazione per tutte le sessioni valutate dal criterio AC perché deve determinare se si tratta di HTTP o DNS. Quindi, deve stabilire se consentire la sessione in base alle liste nere.

Di seguito viene riportato un output troncato del comando **firewall-engine-debug**, i cui campi sono evidenziati in rosso. Prendere nota del comando utilizzato per ottenere il nome dell'applicazione identificata.

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

[…omitted for brevity]

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust


[! How to map service/application ID to name]
> expert
$ grep "^846[^0-9]" /var/sf/appid/odp/appMapping.data
846 SSH 32 0 0 ssh
```

Esempio 2: Il traffico corrispondente a una regola di trust è bloccato

In alcuni scenari il traffico può essere bloccato nonostante la corrispondenza di una regola di trust nel provider di servizi di audioconferenza. Nell'esempio seguente viene valutato il traffico con gli stessi criteri di controllo di accesso e gli stessi host.

```
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Deleting session

[!Session was deleted because we hit a drop IPS rule and blacklisted the flow.
This happened before AC rule was matched (Intrusion policy before AC rule match dropped).
Firewall engine will re-evaluate from top of AC policy to find a rule for logging decision]

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline
sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user 9999997, icmpType 102, icmpCode 22
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 3, 'Trust ssh for host', src network and GEO
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Intrusion Events	Access Control Policy	Access Control Rule
Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp				JG AC (all)	trust server backup

Come illustrato sopra, l'output **firewall-engine-debug** mostra che il traffico corrisponde a un "Trust", mentre gli eventi di connessione mostrano l'azione di **blocco** a causa di una regola dei criteri per le intrusioni (determinata perché la colonna Motivo mostra il **blocco delle intrusioni**).

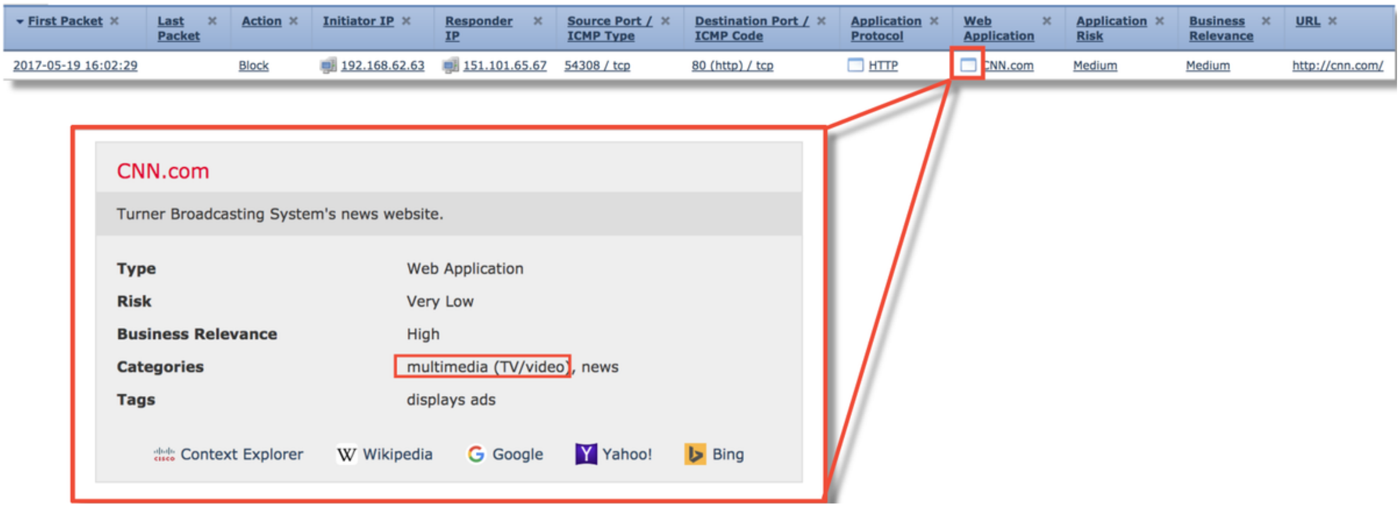
Ciò può verificarsi a causa del **criterio di intrusione utilizzato prima che venga determinata la regola di controllo di accesso** Impostazione nella scheda **Avanzate** del punto ACP. Prima che il traffico possa essere considerato attendibile in base all'azione della regola, il criterio intrusione in questione identifica una corrispondenza di schema e scarta il traffico. Tuttavia, la valutazione della regola del provider di servizi di audioconferenza determina una corrispondenza della regola di trust, poiché gli indirizzi IP non corrispondono ai criteri della regola di "trust server backup".

Affinché il traffico non venga sottoposto all'ispezione della policy sulle intrusioni, la regola di trust può essere posizionata al di sopra della regola di "ispezione", che sarebbe una buona pratica in entrambi i casi. Poiché l'identificazione dell'applicazione è necessaria per una corrispondenza e una mancata corrispondenza della regola "inspect", il **criterio di intrusione utilizzato prima della determinazione della regola di controllo di accesso** viene utilizzato per il traffico che viene valutato dalla stessa regola. Se si inserisce la regola "trust server backup" al di sopra della regola "inspect", il traffico corrisponderà alla regola quando viene visualizzato il primo pacchetto poiché la regola è basata sull'indirizzo IP, che può essere determinato nel primo pacchetto. Non è pertanto necessario utilizzare **i criteri per le intrusioni utilizzati prima della determinazione** della **regola di controllo di accesso**.

Scenario 3: Traffico bloccato dal tag dell'applicazione

In questo scenario gli utenti segnalano che cnn.com è bloccato. Tuttavia, non esiste una regola specifica che blocchi la CNN. Gli eventi di connessione, insieme all'output **firewall-engine-debug**, mostrano il motivo del blocco.

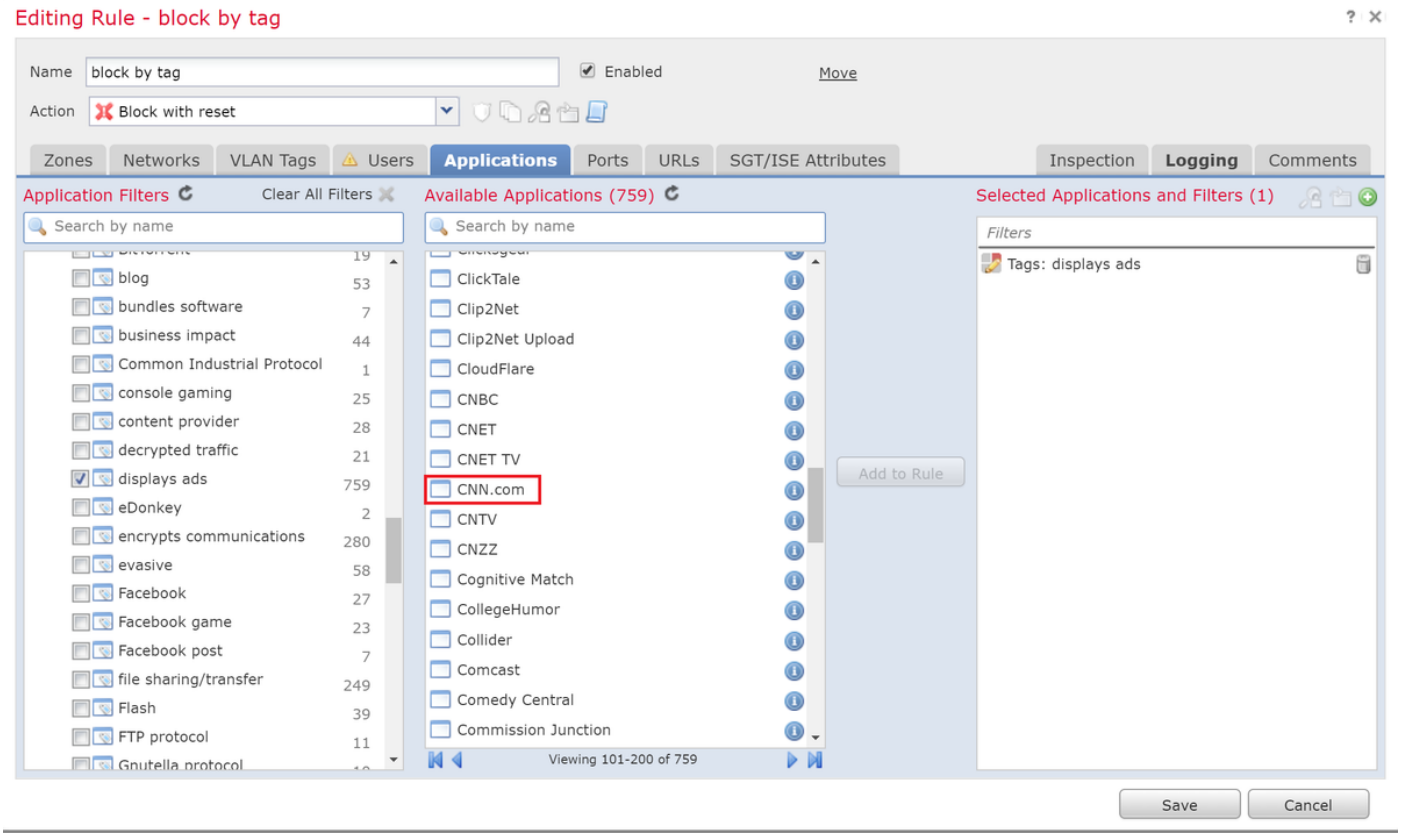
In primo luogo, accanto ai campi dell'applicazione è disponibile una casella di informazioni Eventi connessione che mostra le informazioni sull'applicazione e il modo in cui Firepower categorizza tale applicazione.



Tenendo presenti queste informazioni, il sistema esegue **firewall-engine-debug**. Nell'output del comando debug, il traffico viene bloccato in base al tag dell'applicazione.

```
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 New session
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1190, client 638, misc 0, user 9999997, url http://cnn.com/, xff
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 sending block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Deleting session
```

Anche se non esiste una regola che blocca esplicitamente http://cnn.com, la **visualizzazione degli annunci** contrassegnati viene bloccata nella scheda **Applicazioni** di una regola ACP.



Dati da fornire a TAC

Dati	Istruzioni
Risoluzione dei problemi relativi al file dal dispositivo Firepower per il controllo del traffico	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/1176
supporto di sistema - debug firewall-engine e output **system-support-trace**	Per istruzioni, vedere questo articolo
Esportazione criteri di controllo di accesso	Selezionare **Sistema > Strumenti > Importa/esporta**, selezionare la policy di controll pulsante **Esporta**

> **Attenzione:** Se il provider di servizi di audioconferenza contiene un criterio SSL, rimuovere il criterio SSL dal provider di servizi di audioconferenza prima dell'esportazione per evitare di divulgare informazioni riservate sull'infrastruttura a chiave pubblica

Passaggio successivo: Risoluzione dei problemi relativi al livello dei criteri SSL

Se è in uso un criterio SSL e la risoluzione dei problemi relativi al criterio di controllo dell'accesso non ha rilevato il problema, il passaggio successivo consiste nella risoluzione dei problemi relativi al criterio SSL.

Fare clic qui per continuare con l'articolo successivo.