Fase 3 della risoluzione dei problemi relativi al percorso dei dati di Firepower: Security Intelligence

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 terza fase della risoluzione dei problemi relativi al percorso dati di Firepower, la funzionalità di intelligence di sicurezza.

Prerequisiti

- Questo articolo riguarda tutte le piattaforme Firepower attualmente supportate
- L'intelligence di sicurezza per URL e DNS è stata introdotta nella versione 6.0.0

Risoluzione dei problemi relativi alla fase Firepower Security Intelligence

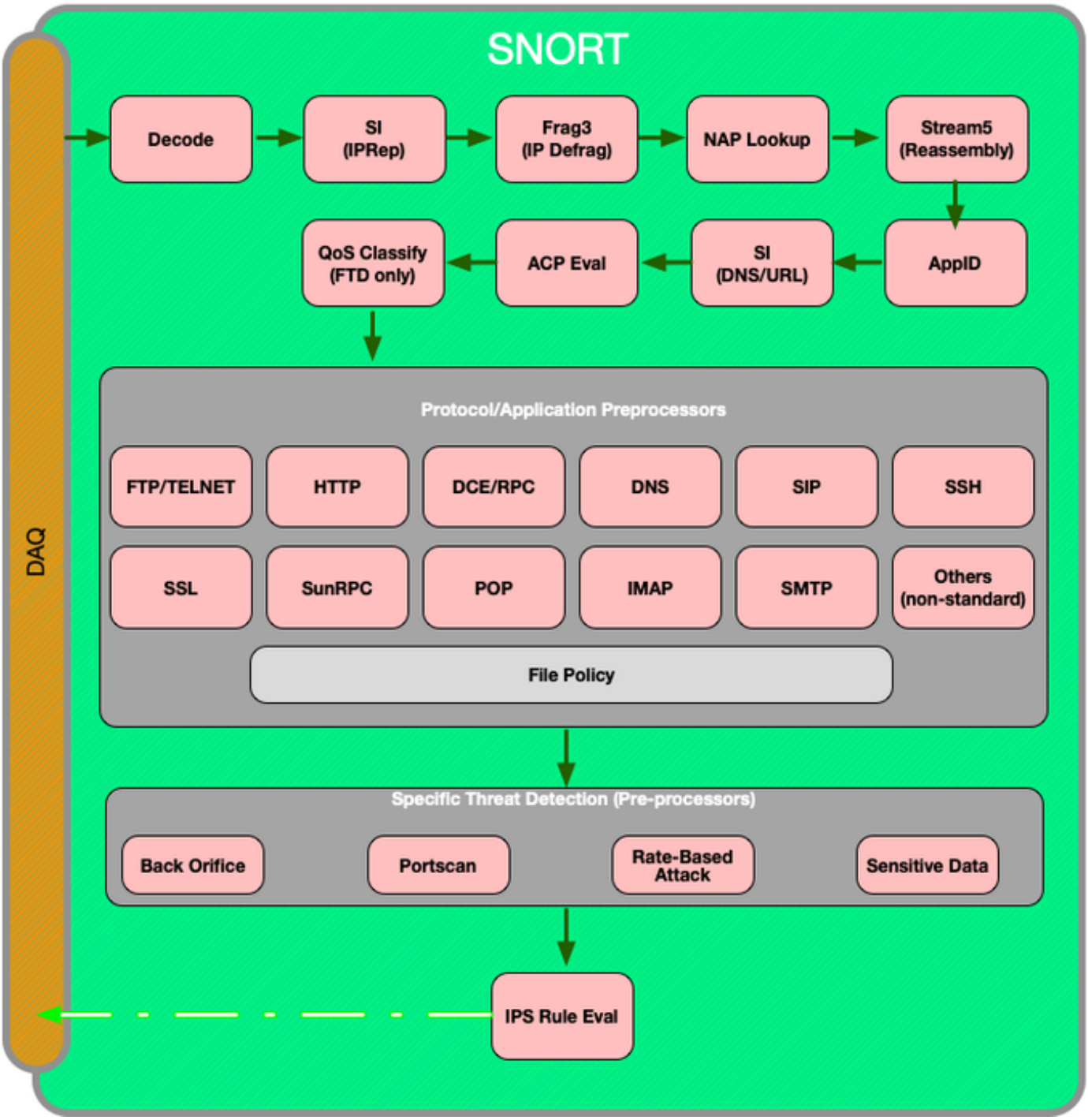
Security Intelligence è una funzione che esegue l'ispezione sia su liste nere che su liste bianche per:

- Indirizzi IP (noti anche come "reti" in alcune parti dell'interfaccia utente)
- URL (Uniform Resource Locator)

- Query DNS (Domain Name System)

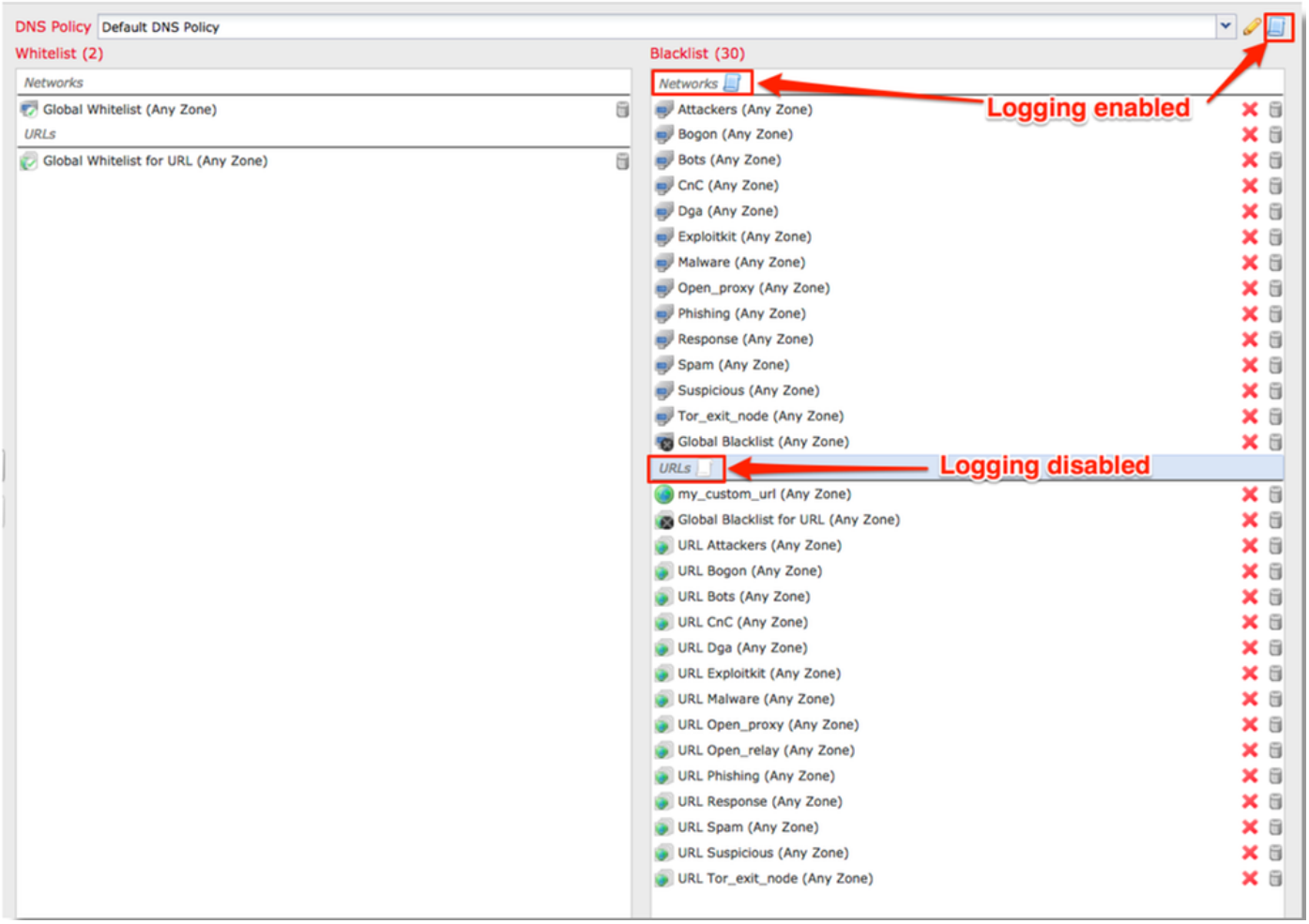
Gli elenchi all'interno della Security Intelligence possono essere popolati da feed forniti da Cisco e/o da elenchi e feed configurati dall'utente.

La reputazione di Security Intelligence basata su indirizzi IP è il primo componente di Firepower a ispezionare il traffico. L'intelligence di sicurezza URL e DNS viene eseguita non appena viene individuato il protocollo applicativo appropriato. Di seguito è riportato un diagramma che descrive il flusso di lavoro di ispezione del software Firepower.



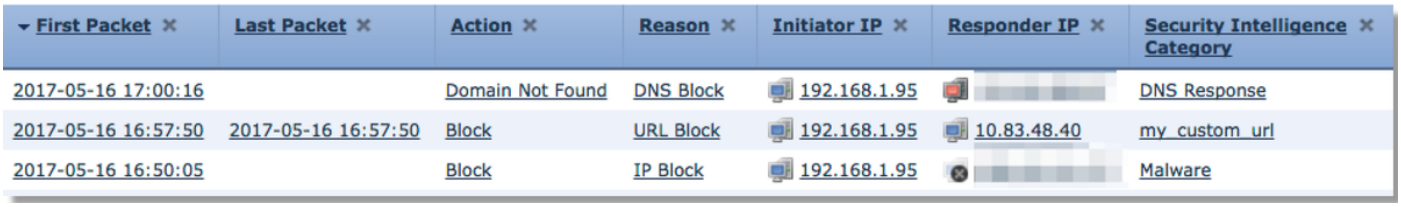
Verifica dell'abilitazione della registrazione per gli eventi di Security Intelligence

I blocchi a livello di Security Intelligence sono molto facili da determinare se la registrazione è abilitata. È possibile determinare questa condizione nell'interfaccia utente di Firepower Management Center (FMC) passando a **Criteri > Controllo di accesso > Criteri di controllo di accesso**. Dopo aver fatto clic sull'icona Modifica accanto al criterio in questione, passare alla scheda **Security Intelligence**.

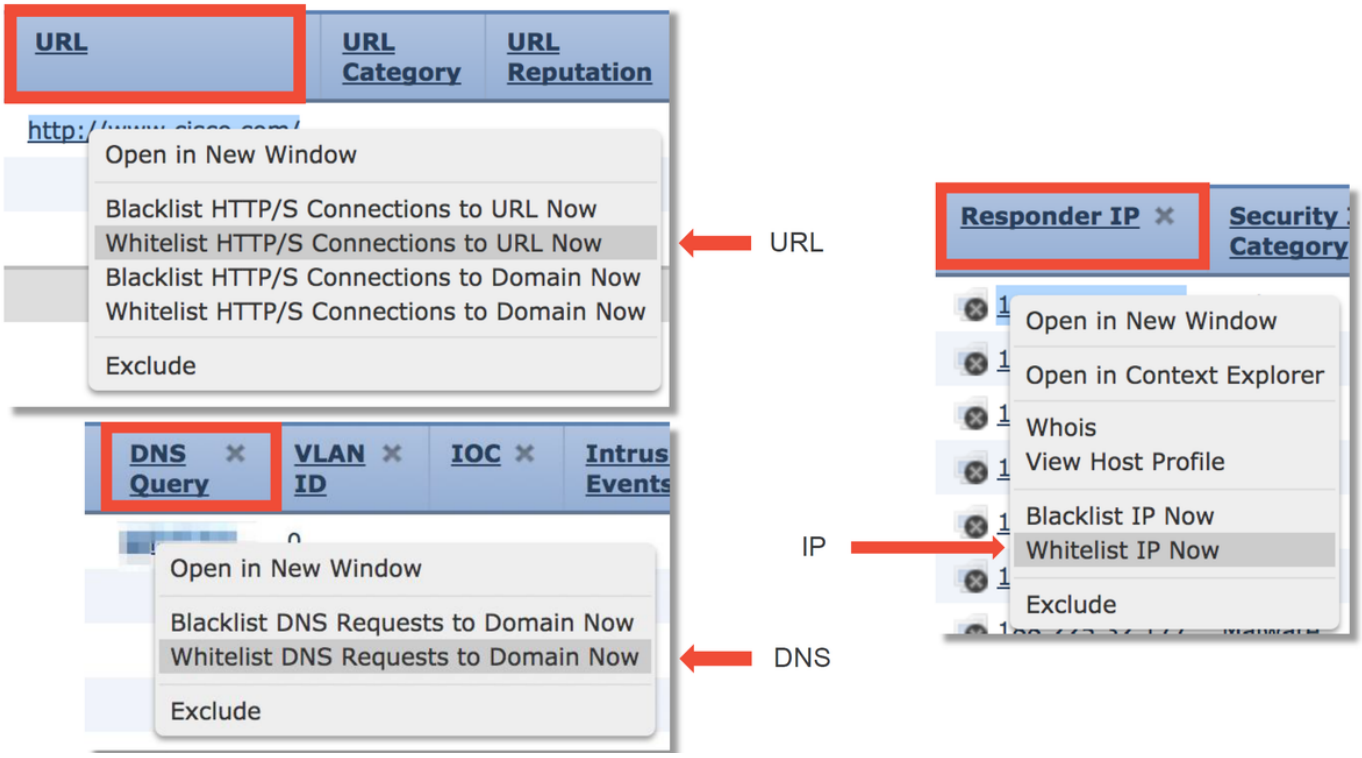


Verifica eventi di Security Intelligence

Una volta abilitata la registrazione, è possibile visualizzare gli eventi di Security Intelligence in **Analisi > Connessioni > Eventi di Security Intelligence**. Dovrebbe essere chiaro perché il traffico è bloccato.



Per ridurre rapidamente i rischi, è possibile fare clic con il pulsante destro del mouse sull'IP, l'URL o la query DNS bloccati dalla funzionalità di intelligence di sicurezza e scegliere un'opzione di elenco vuoto.



Se sospetti che qualcosa sia stato erroneamente inserito nella lista nera, o se vuoi richiedere di cambiare la reputazione, puoi aprire una richiesta direttamente con Cisco Talos al seguente link:

https://www.talosintelligence.com/reputation_center/support

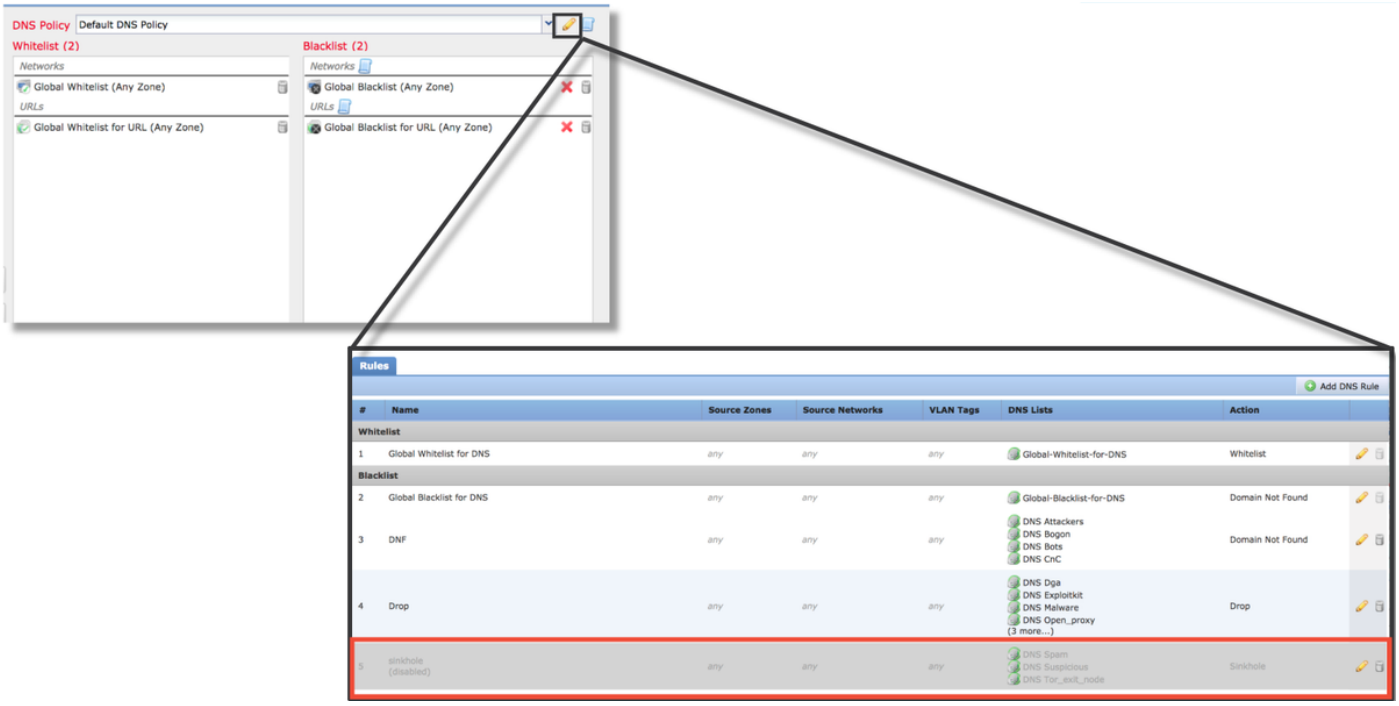
Èinoltre possibile fornire i dati al Cisco Technical Assistance Center (TAC) per verificare se un elemento deve essere rimosso dalla lista nera.

> **Nota:** L'aggiunta alla lista bianca consente di aggiungere solo una voce alla lista bianca Security Intelligence in questione, ovvero l'oggetto può superare il controllo Security Intelligence. Tuttavia, tutti gli altri componenti di Firepower possono ancora ispezionare il traffico.

Come rimuovere le configurazioni di Security Intelligence

Per rimuovere le configurazioni di Security Intelligence, passare alla scheda **Security Intelligence**, come indicato in precedenza. Ci sono tre sezioni; uno per reti, URL e criteri per DNS.

Da lì, gli elenchi e i feed possono essere rimossi facendo clic sul simbolo del cestino.



Nello screenshot precedente, tutte le liste di IP e URL Security Intelligence sono state rimosse ad eccezione della lista nera globale e della lista bianca.

Una delle regole è disabilitata all'interno dei criteri DNS, ovvero dove è archiviata la configurazione dell'intelligence di sicurezza DNS.

> **Nota:** Per visualizzare il contenuto delle liste nere globali e delle liste bianche, selezionare **Oggetti > Gestione oggetti > Security Intelligence**. Quindi fai clic sulla sezione di interesse (Rete, URL, DNS). La modifica di un elenco consente di visualizzare il contenuto, anche se la configurazione deve essere eseguita nell'ambito dei criteri di controllo di accesso.

Verifica della configurazione sul back-end

La configurazione della Security Intelligence può essere verificata sulla CLI con il comando **> show access-control-config**, che mostra il contenuto dei criteri di controllo dell'accesso attivi in esecuzione sulla periferica Firepower.

```
> show access-control-config

==================[ My AC Policy ]==================
Description             :
Default Action           : Allow
Default Policy           : SOC
Logging Configuration
   DC                  : Enabled
   Beginning            : Disabled
   End                 : Enabled
Rule Hits               : 0
Variable Set             : Default-Set

===[ Security Intelligence - Network Whitelist ]====
   Name                 : Global-Whitelist (List)
   IP Count             : 0
   Zone                 : any

===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Enabled
   DC                  : Enabled


--------------------[ Block ]---------------------
   Name                 : Attackers (Feed)
   Zone                 : any

   Name                 : Bogon (Feed)
   Zone                 : any
...[omitted for brevity]
```

Si noti che nell'esempio precedente, la registrazione è configurata per la lista nera della rete e almeno due feed sono stati inclusi nella lista nera (Attackers e Bogon).

Èpossibile determinare se un singolo elemento è incluso in un elenco di Security Intelligence in modalità Expert. Procedere come segue:

```
> expert
$ grep <ip.addr> /var/sf/iprep_download/*
/var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf:<ip.addr>

$ head -1 /var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf
#Cisco intelligence feed: Malware



$ grep <url> /var/sf/siurl_download/*
/var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf:<url>

$ head -1 /var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf
#URL object: my_custom_url



$ grep <dns.hostname> /var/sf/sidns_download/*
/var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf: <dns.hostname>

$ head -1 /var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf
#Cisco DNS and URL intelligence feed: DNS Response
```

IP SI lists are in /var/sf/iprep_download/

URL SI lists are in /var/sf/siurl_download/

DNS SI lists are in /var/sf/sidns_download/

Per ogni elenco di Security Intelligence è disponibile un file con un UUID univoco. Nell'esempio

precedente viene illustrato come identificare il nome dell'elenco tramite il comando **head -n1**.

Dati da fornire a TAC

Dati	Istruzioni
Risoluzione dei problemi relativi ai file dal FMC e dal dispositivo Firepower per il controllo del traffico	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techno
Schermate degli eventi (con timestamp inclusi)	Per istruzioni, vedere questo articolo
Output di testo da sessioni CLI	Per istruzioni, vedere questo articolo
Se si invia un caso falso positivo, fornire l'elemento (IP, URL, dominio) da contestare.	Fornire i motivi e le prove che giustificano l'esecuzione della controversia.

Passaggio successivo

Se è stato determinato che il componente di intelligence di sicurezza non è la causa del problema, il passaggio successivo consiste nella risoluzione dei problemi relativi alle regole dei criteri di controllo di accesso.

Fare clic qui per continuare con l'articolo successivo.