Risoluzione dei problemi relativi al percorso dei dati di Firepower: Panoramica

Sommario

Introduzione

Lo scopo di questa guida è quello di aiutare a identificare rapidamente se un dispositivo Firepower Threat Defense (FTD) o un'appliance Adaptive Security (ASA) con servizi FirePOWER sta causando un problema con il traffico di rete. Inoltre, aiuta a ridurre i componenti di Firepower da esaminare e i dati da raccogliere prima di affidarsi al Cisco Technical Assistance Center (TAC).

Elenco di tutti gli articoli della serie Firepower Data Path Troubleshooting.

Fase 1 della risoluzione dei problemi relativi al percorso dei dati di Firepower: Pacchetto in ingresso

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214574-firepower-data-path-troubleshooting-phas.html

Fase 2 della risoluzione dei problemi del percorso dei dati di Firepower: Livello DAQ
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html

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

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html

Fase 4 della risoluzione dei problemi relativi al percorso dei dati di Firepower: Policy di controllo dell'accesso
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html

Fase 5 della risoluzione dei problemi del percorso dei dati di Firepower: Criterio SSL
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html

Fase 6 della risoluzione dei problemi relativi al percorso dei dati di Firepower: Autenticazione attiva
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html

Fase 7 della risoluzione dei problemi del percorso dei dati di Firepower: Policy anti-intrusione
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html

Fase 8 della risoluzione dei problemi del percorso dei dati di Firepower: Criteri di analisi della rete

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214610-firepower-data-path-troubleshooting-phas.html

Prerequisiti

- In questo articolo si presume che uno abbia una conoscenza di base delle piattaforme FTD e ASA.
- Èconsigliabile conoscere l'ascolto open source, anche se non è necessario.

Per un elenco completo della documentazione di Firepower, incluse le guide all'installazione e alla configurazione, visitare la pagina della roadmap della documentazione.

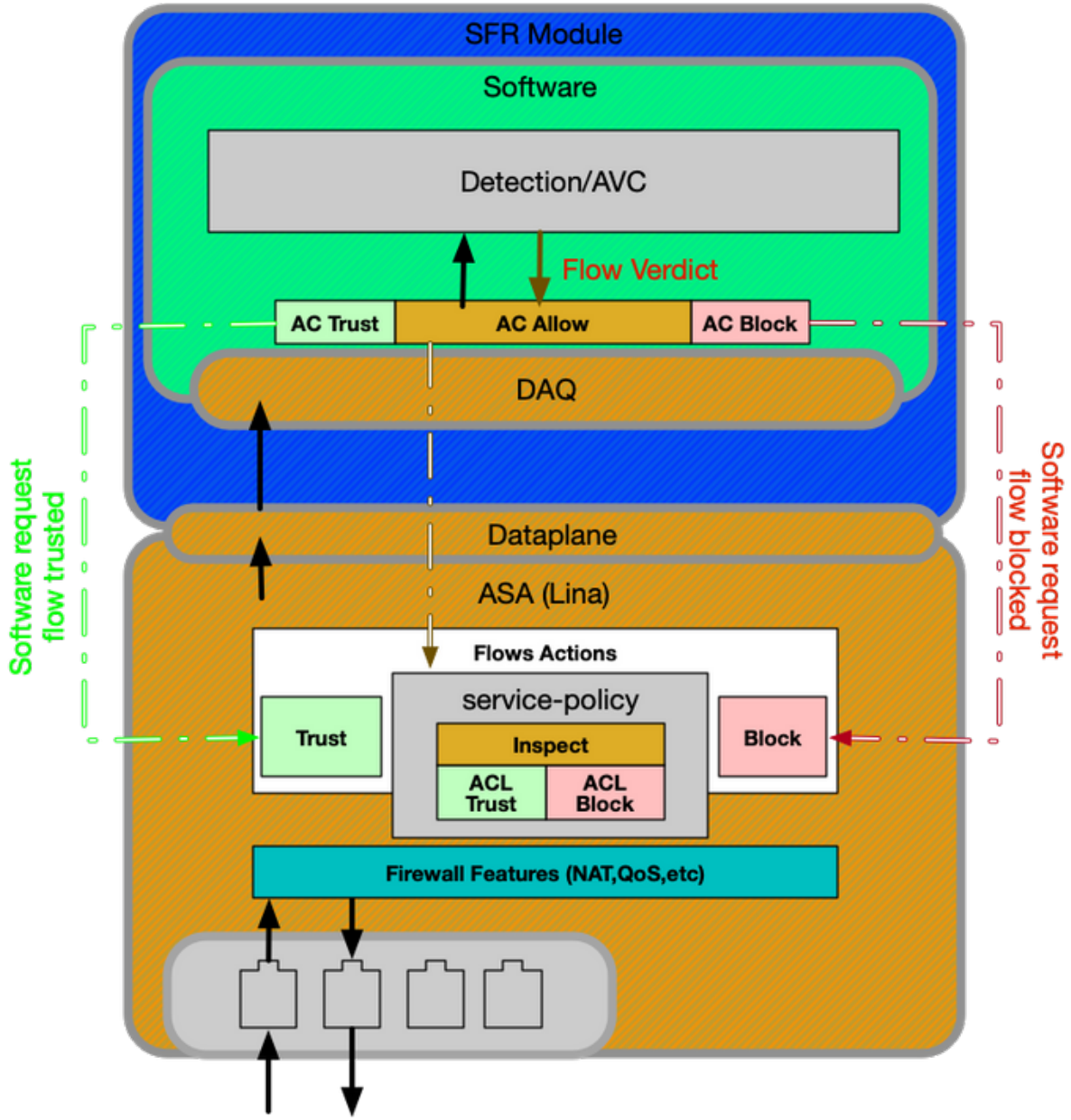
Panoramica dell'architettura del percorso dati

Nella sezione seguente viene analizzato il percorso dati dell'architettura per diverse piattaforme Firepower. Considerata l'architettura, verrà spiegato come determinare rapidamente se il dispositivo Firepower sta bloccando il flusso del traffico.

> **Nota:** Questo articolo non riguarda i dispositivi legacy Firepower serie 7000 e 8000, né la piattaforma virtuale NGIPS (non FTD). Per informazioni sulla risoluzione dei problemi relativi a tali piattaforme, visitare la pagina Note tecniche.

ASA con piattaforma FirePOWER Services (modulo SFR)

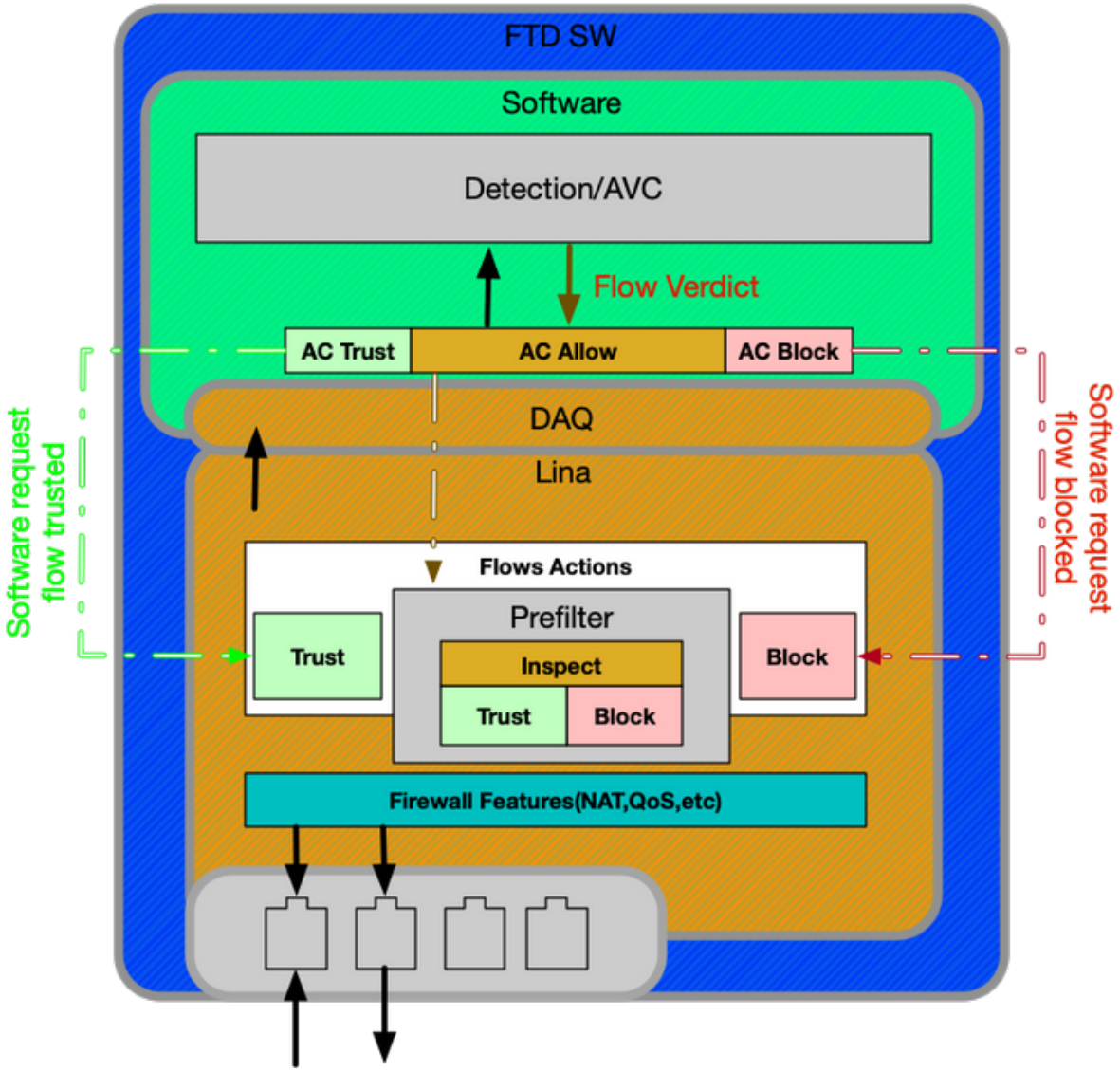
La piattaforma FirePOWER Services è anche nota come modulo SFR. Si tratta fondamentalmente di una macchina virtuale che viene eseguita su piattaforme ASA 5500-X.



La policy sui servizi sull'appliance ASA determina il traffico inviato al modulo SFR. Esiste un livello di corsia di dati che viene utilizzato per comunicare con il motore DAQ (Firepower Data Acquisition), che viene utilizzato per tradurre i pacchetti in modo comprensibile per gli snort.

Firepower Threat Defense su ASA500-X e piattaforma FTD virtuale

La piattaforma FTD è costituita da una singola immagine contenente sia il codice Lina (ASA) che Firepower. Una delle differenze principali tra questa e l'appliance ASA con piattaforma del modulo SFR è che vi sono comunicazioni più efficienti tra Lina e Snort.

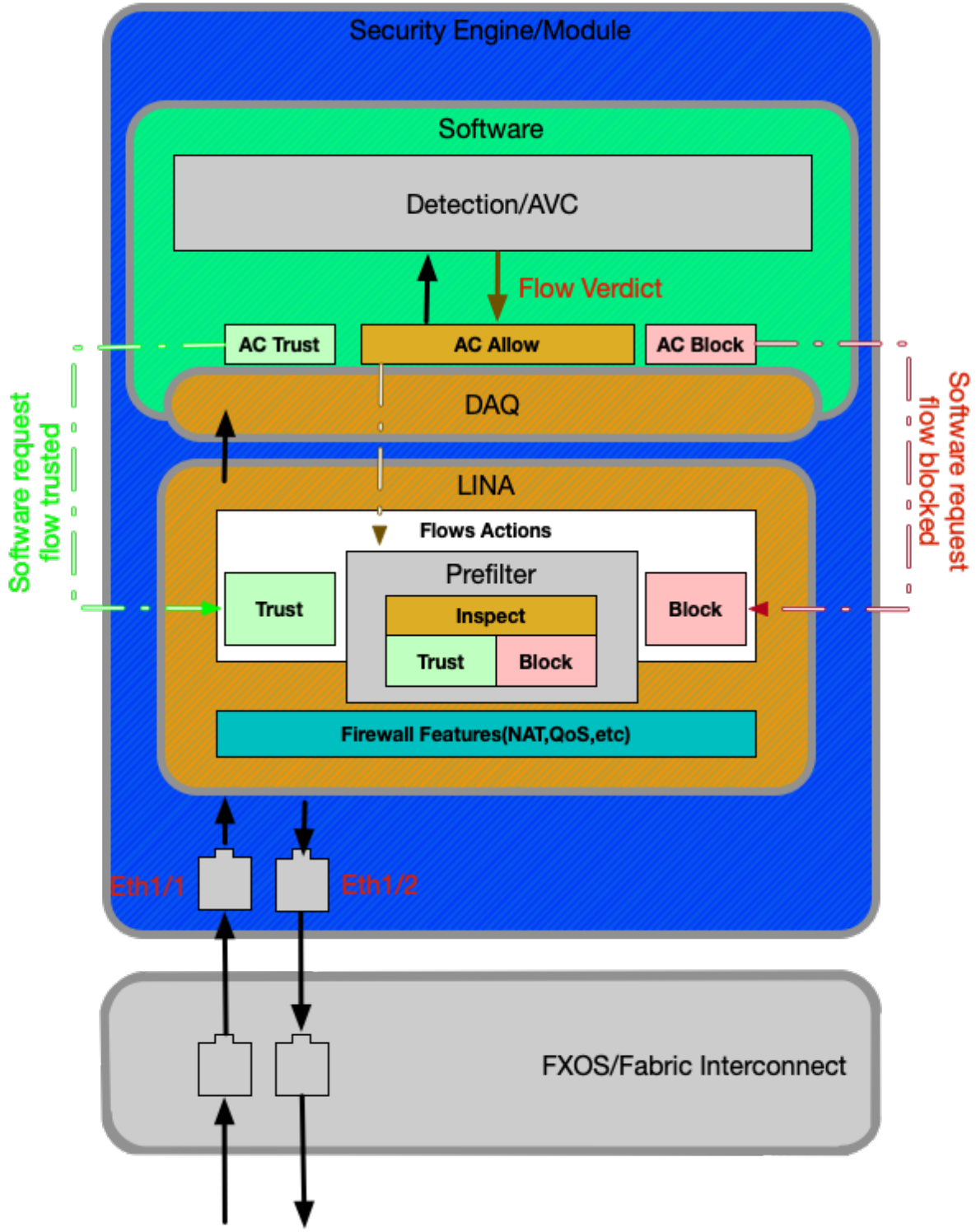


FTD su piattaforme SSP

Sui modelli SSP (Security Service Platforms), il software FTD viene eseguito sulla piattaforma Firepower eXtensible Operative System (FXOS), che è un sistema operativo sottostante utilizzato per gestire l'hardware dello chassis e ospitare diverse applicazioni note come dispositivi logici.

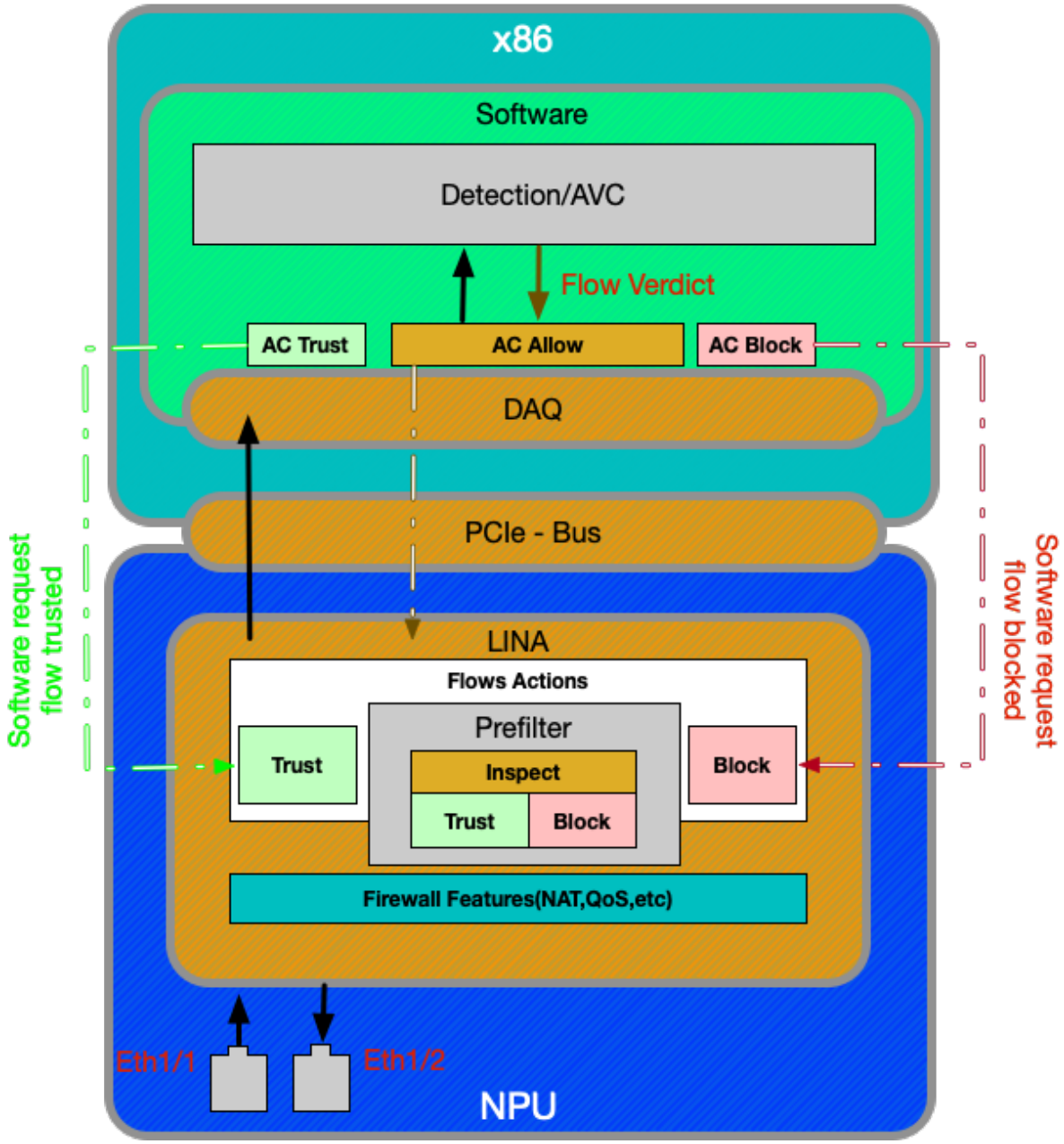
All'interno della piattaforma SSP esistono alcune differenze tra i diversi modelli, come illustrato nei diagrammi e nelle descrizioni seguenti.

Appliance Firepower 9300 e 4100



Sulle piattaforme Firepower 9300 e 4100, i pacchetti in entrata e in uscita vengono gestiti da uno switch con firmware FXOS (Fabric Interconnect). I pacchetti vengono quindi inviati alle interfacce assegnate al dispositivo logico (in questo caso, FTD). In seguito, l'elaborazione dei pacchetti è la stessa che viene effettuata sulle piattaforme FTD non SSP.

Appliance Firepower 2100



Il dispositivo Firepower 2100 funziona in modo molto simile alle piattaforme FTD non SSP. Non contiene lo strato di interconnessione del fabric presente sui modelli 9300 e 4100. Tuttavia, esiste una differenza importante tra i dispositivi della serie 2100 e gli altri dispositivi, ovvero la presenza del circuito integrato specifico dell'applicazione (ASIC). Tutte le funzionalità ASA tradizionali (Lina) vengono eseguite sull'ASIC e tutte le funzionalità NGFW (Next-Generation Firewall) (snort, filtro URL, ecc.) vengono eseguite sulla tradizionale architettura x86. Il modo in cui Lina e Snort comunicano su questa piattaforma è tramite un PCIe (Peripheral Component Interconnect Express) tramite una coda di pacchetti, a differenza delle altre piattaforme che utilizzano DMA (Direct Memory Access) per mettere in coda i pacchetti da sniffare.

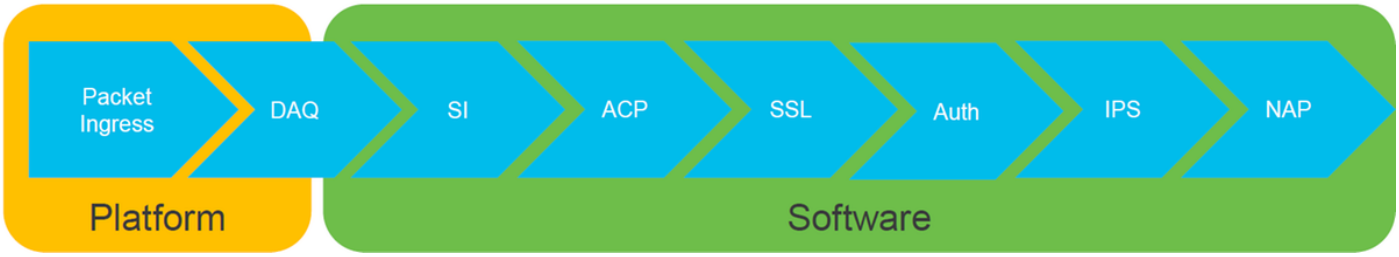
> **Nota:** Gli stessi metodi per la risoluzione dei problemi delle piattaforme FTD non SSP saranno seguiti sulla piattaforma FPR-2100.

Procedura consigliata per la risoluzione dei problemi relativi a Firepower Data-Path

Dopo aver descritto come identificare il traffico univoco e l'architettura del percorso dei dati di base

nelle piattaforme Firepower, vengono ora esaminati i punti specifici in cui i pacchetti possono essere scartati. Negli articoli relativi al percorso dati vengono descritti otto componenti di base, che possono essere risolti sistematicamente per determinare eventuali perdite di pacchetti. Tra queste:

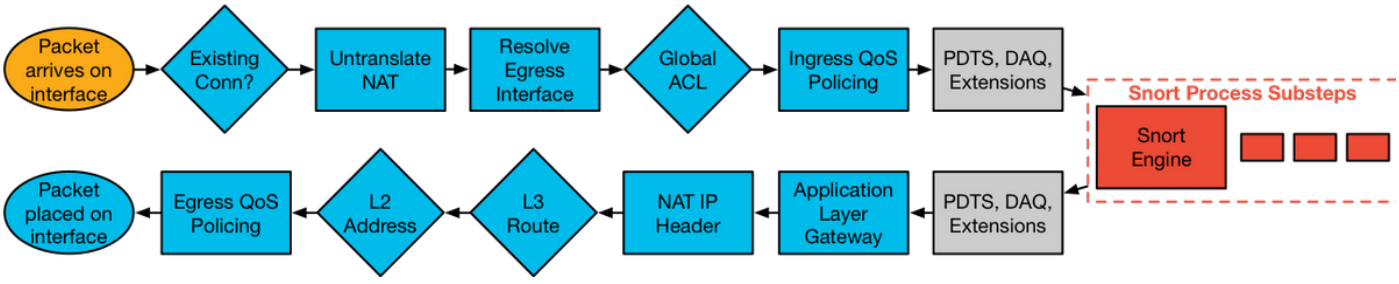
1. Pacchetto in ingresso
2. Firepower DAQ Layer
3. Security Intelligence
4. Policy di controllo dell'accesso
5. Criterio SSL
6. Funzionalità di autenticazione attive
7. Criteri per le intrusioni (regole IPS)
8. Criteri di analisi della rete (ignora le impostazioni del preprocessore)



Nota: Questi componenti non sono elencati nell'ordine esatto delle operazioni nell'elaborazione di Firepower, ma sono ordinati in base al flusso di lavoro di risoluzione dei problemi consigliato. Per il percorso effettivo del diagramma del pacchetto, vedere la figura seguente.

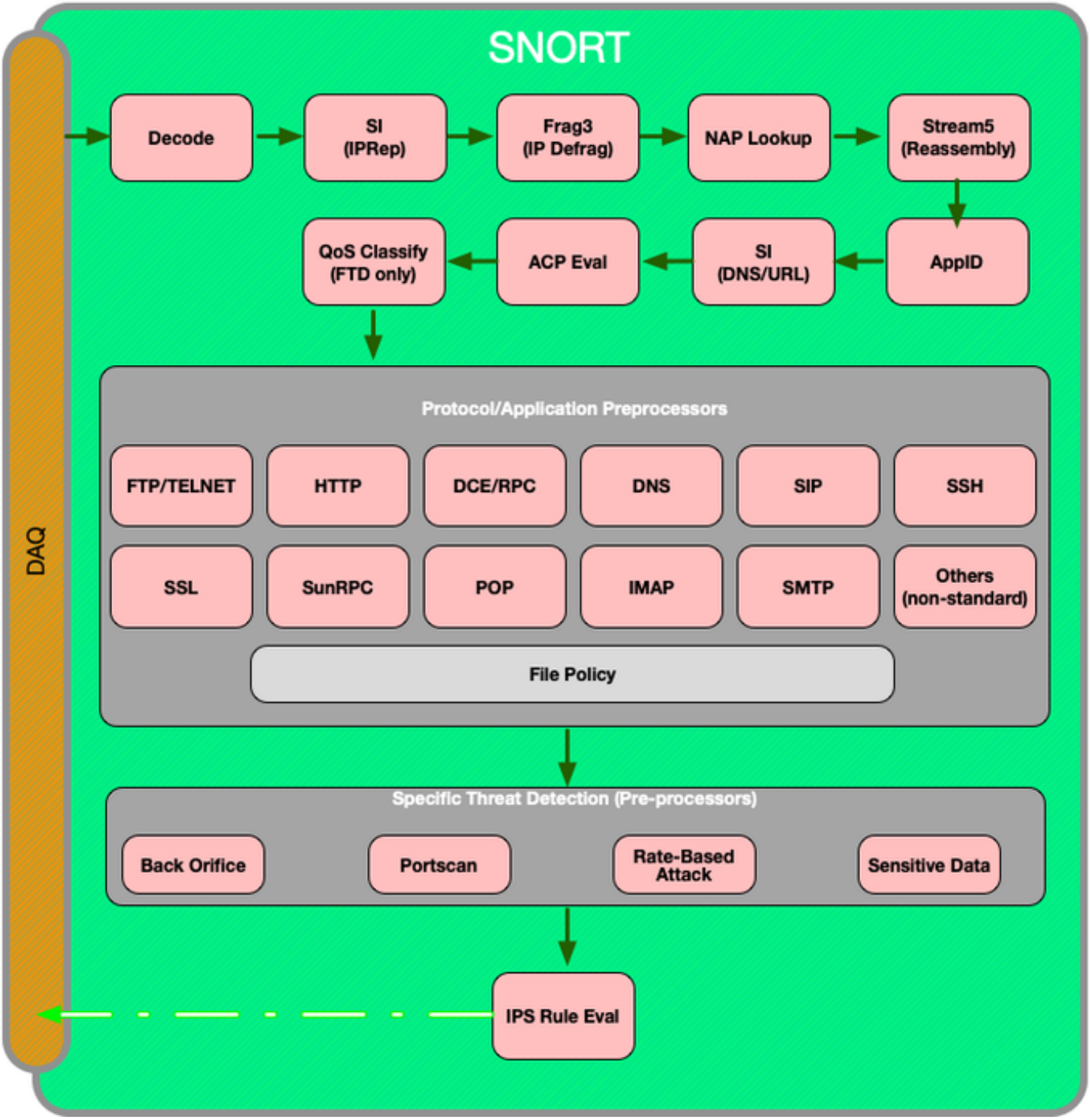
Percorso effettivo del pacchetto tramite FTD

L'illustrazione seguente mostra il percorso effettivo del pacchetto mentre attraversa l'FTD.



Ordina percorso pacchetto

La figura seguente mostra il percorso del pacchetto attraverso il motore Snort.



Pacchetti in entrata e in uscita

Il primo passaggio per la risoluzione dei problemi relativi al percorso dei dati consiste nell'assicurarsi che non si verifichino perdite in entrata o in uscita durante l'elaborazione dei pacchetti. Se un pacchetto è in entrata ma non in uscita, si può essere certi che il pacchetto venga scartato dal dispositivo in un punto qualsiasi del percorso dati.

In questo articolo viene spiegato come risolvere i problemi di ingresso e uscita dei pacchetti sui sistemi Firepower.

Firepower DAQ Layer

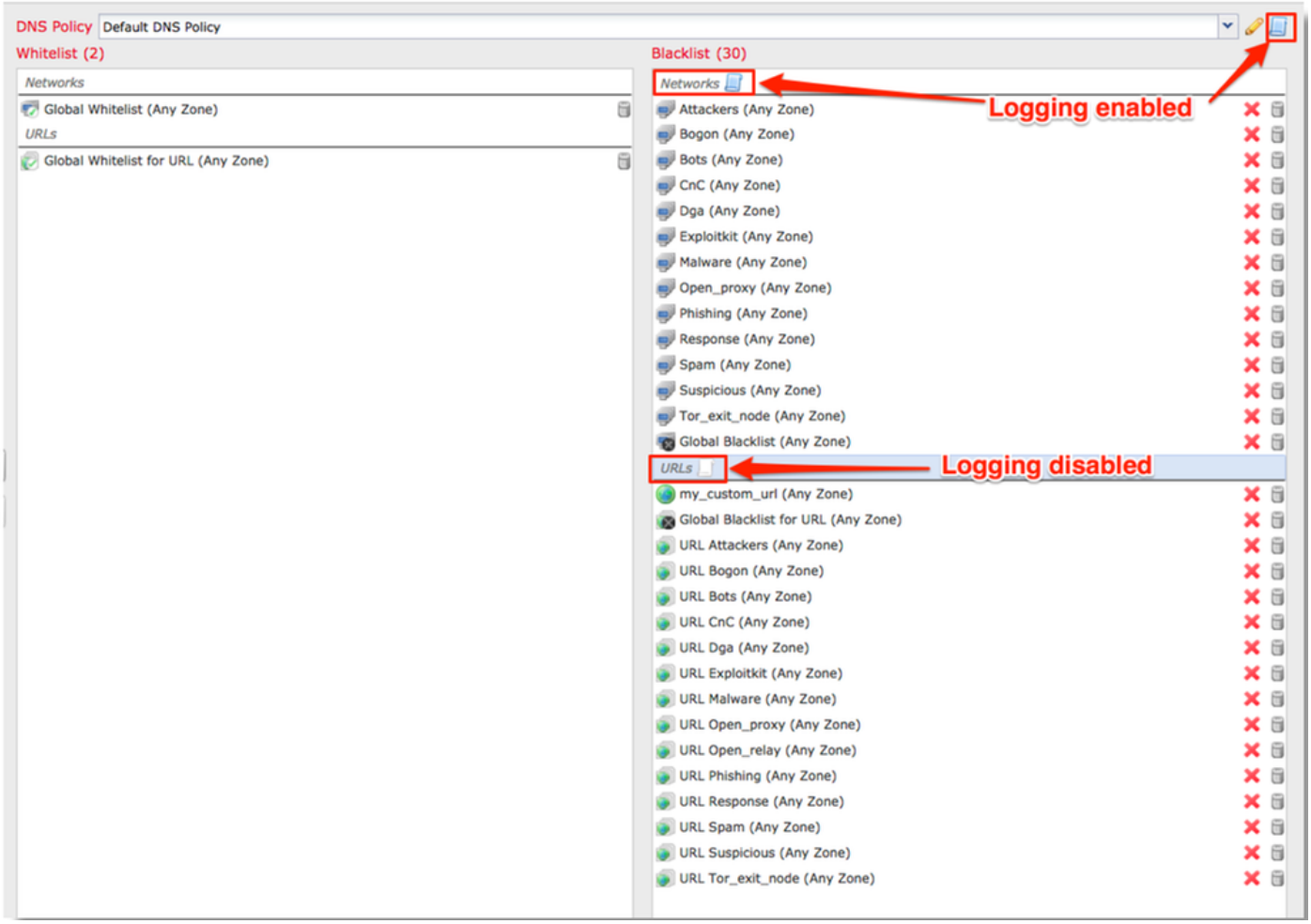
Se è stato determinato che il pacchetto è in entrata ma non in uscita, il passaggio successivo per la risoluzione dei problemi del percorso dati deve essere eseguito al livello Firepower DAQ (Data Acquisition) per essere certi che il traffico in questione venga inviato a Firepower per l'ispezione e, in caso affermativo, per verificare se viene scartato o modificato.

In questo articolo viene descritto come risolvere i problemi relativi alla gestione iniziale del traffico da parte di Firepower e al percorso che questo gestisce nell'accessorio.

Viene inoltre descritto come ignorare completamente il dispositivo Firepower per determinare se un componente Firepower è responsabile del problema di traffico.

Security Intelligence

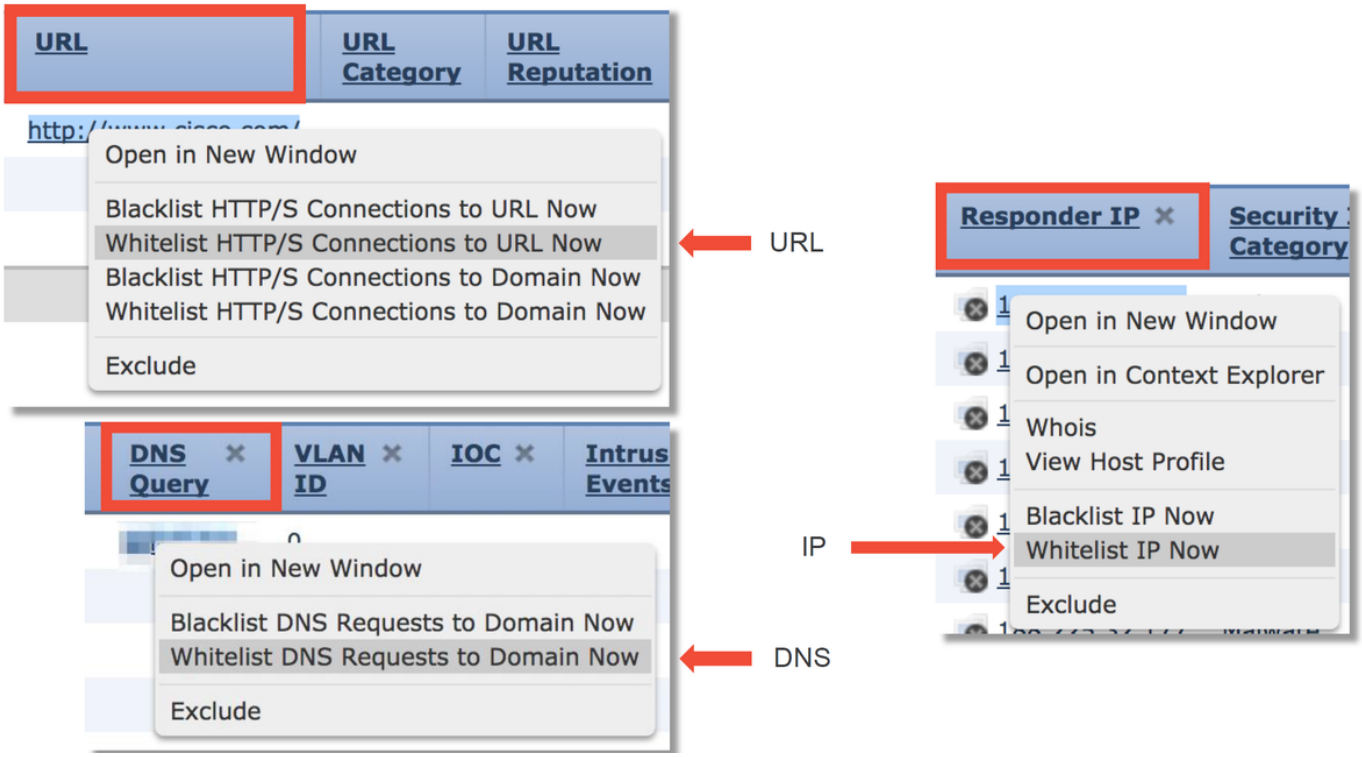
Security Intelligence è il primo componente di Firepower a ispezionare il traffico. I blocchi a questo livello sono molto facili da determinare se è abilitata la registrazione. È possibile determinare questa condizione dalla GUI di FMC selezionando **Policy > Controllo di accesso > Policy di controllo di accesso**. Dopo aver fatto clic sull'icona Modifica accanto al criterio in questione, passare alla scheda **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.

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

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 a TAC per segnalare ciò che viene bloccato e rimuovere eventualmente una voce da una lista nera.

Per una risoluzione approfondita dei problemi del componente Security Intelligence, consultare l'articolo relativo alla risoluzione dei problemi del percorso dati.

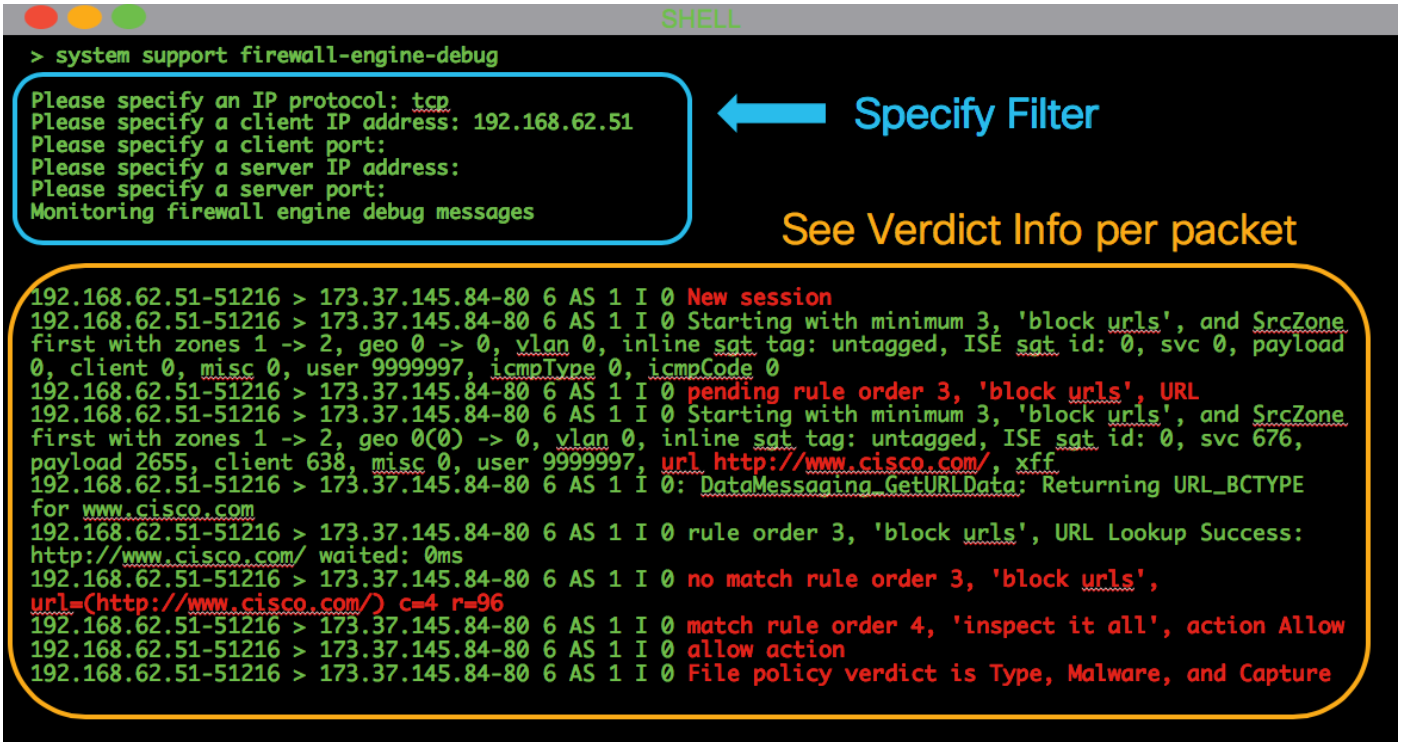
Policy di controllo dell'accesso

Se è stato determinato che la funzionalità di intelligence di sicurezza non blocca il traffico, il passaggio successivo consigliato consiste nella risoluzione dei problemi relativi alle regole dei criteri di controllo di accesso per verificare se una regola con un'azione 'Blocca' sta eliminando il traffico.

Si consiglia di iniziare a usare il comando "firewall-engine-debug" o acquisire con trace. In genere, questi strumenti consentono di ottenere immediatamente la risposta e di stabilire la regola per cui il traffico viene raggiunto e per quali motivi.

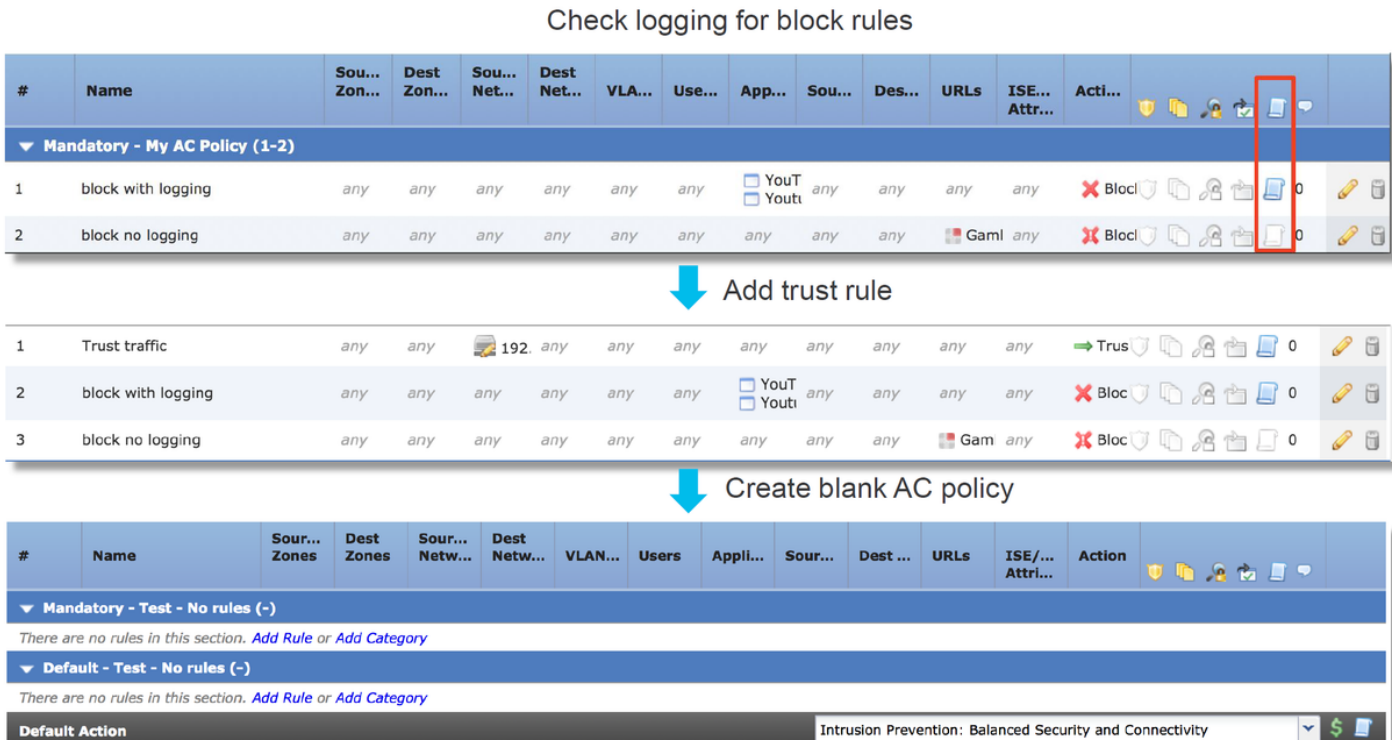
- Eseguire il debug sulla CLI di Firepower per verificare quale regola blocca il traffico (assicurarsi di immettere il maggior numero di parametri possibile) tramite il seguente comando: **> supporto sistema firewall-engine-debug**
- L'output del debug può essere fornito a TAC per l'analisi

Di seguito è riportato un output di esempio che illustra la valutazione delle regole per il traffico corrispondente a una regola di controllo di accesso con l'azione 'Consenti':



Se non è possibile determinare quale regola di controllo di accesso (ACL) viene soddisfatta o se non è possibile determinare se il criterio di controllo di accesso è il problema utilizzando gli strumenti sopra descritti, di seguito sono riportate alcune procedure di base per la risoluzione dei problemi relativi ai criteri di controllo di accesso (notare che queste opzioni non sono la prima in quanto richiedono modifiche/distribuzioni dei criteri):

- Abilitare la registrazione per qualsiasi regola con un'azione 'Blocca'
- Se gli eventi di connessione per il traffico non vengono ancora visualizzati e il traffico viene bloccato, creare una regola di trust per il traffico in questione come fase di mitigazione
- Se la regola di attendibilità per il traffico non risolve ancora il problema ma si sospetta che il criterio di controllo dell'accesso sia errato, creare un nuovo criterio di controllo dell'accesso vuoto, se possibile, utilizzando un'azione predefinita diversa da 'Blocca tutto il traffico'

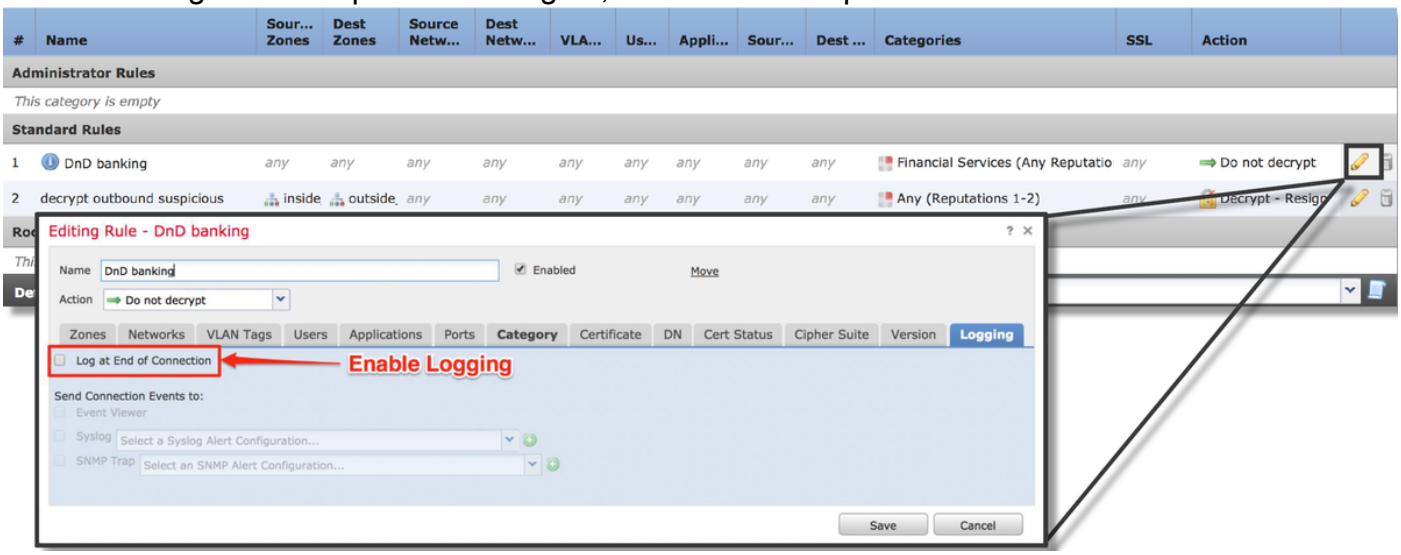


Per una risoluzione dettagliata dei problemi relativi ai criteri di controllo di accesso, consultare l'articolo sulla risoluzione dei problemi relativi al percorso dati.

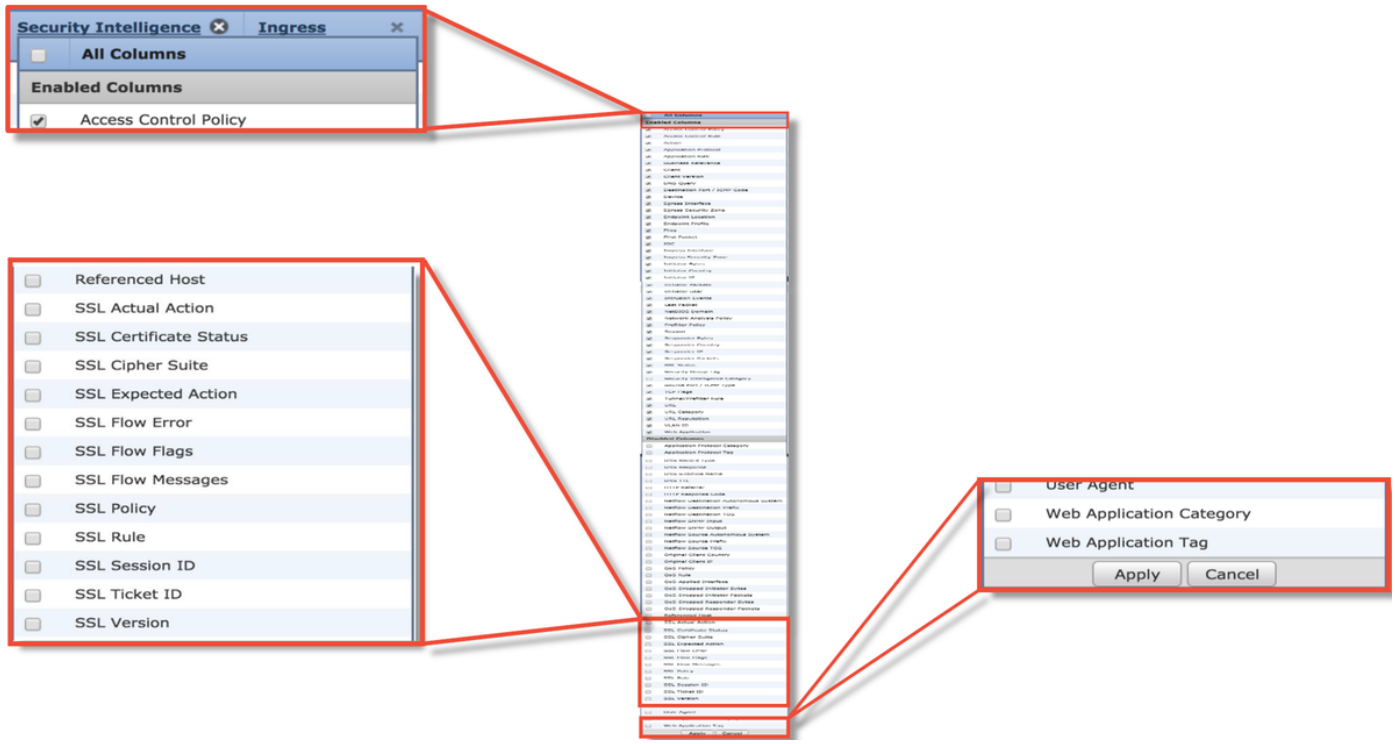
Criterio SSL

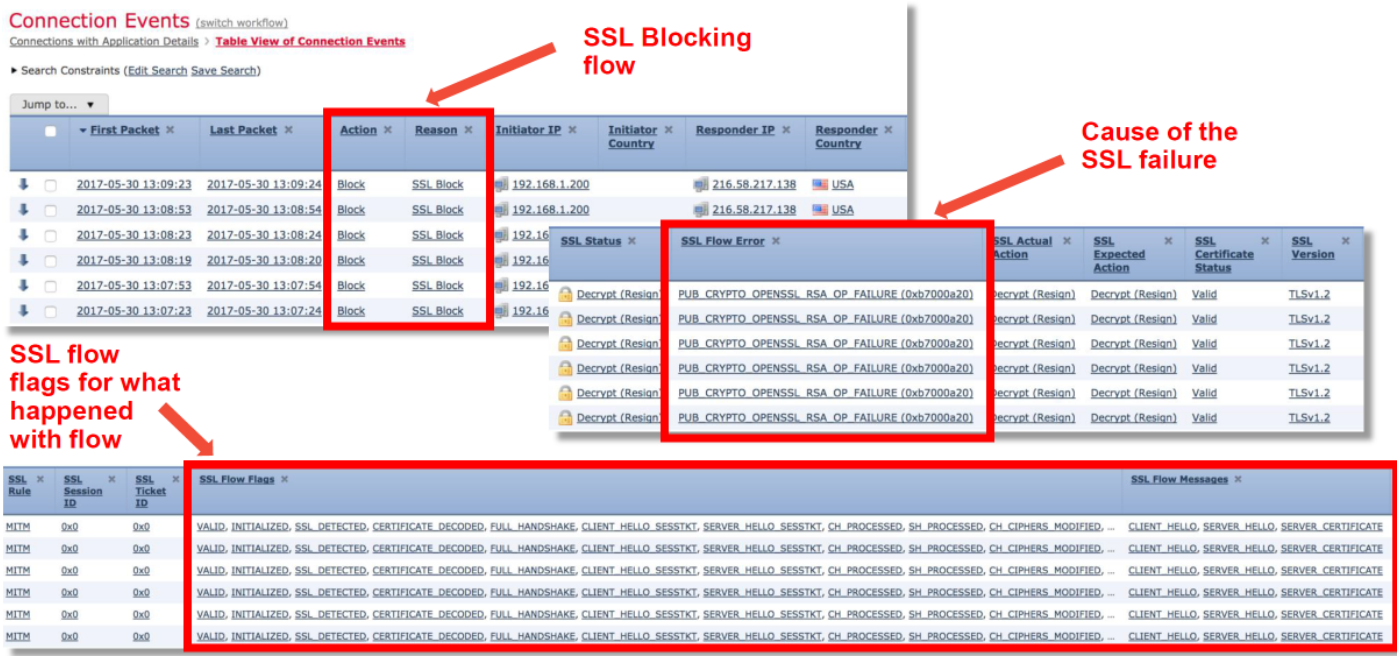
Se si utilizza il criterio SSL, è possibile che stia bloccando il traffico. Di seguito sono riportati alcuni passaggi di base per la risoluzione dei problemi relativi ai criteri SSL:

- Abilita registrazione per tutte le regole, inclusa l'azione predefinita



- Selezionare la scheda Azioni non decrittografabili per verificare se un'opzione è impostata per bloccare il traffico
- Nella sezione Eventi connessione selezionare tutti i campi con 'SSL' nel nome
  La maggior parte di essi è disattivata per impostazione predefinita e deve essere attivata nel visualizzatore degli eventi di connessione facendo clic sulla croce accanto al nome di una colonna





- Creare un criterio SSL vuoto con l'opzione Non decrittografare come azione predefinita come fase di mitigazione
- Rimuovere il criterio SSL dai criteri di controllo di accesso come fase di mitigazione
  Questa impostazione è specificata nella scheda Avanzate

Se si sospetta che il criterio SSL comporti la perdita di traffico, è possibile inviare a TAC gli eventi di connessione e la configurazione del criterio.

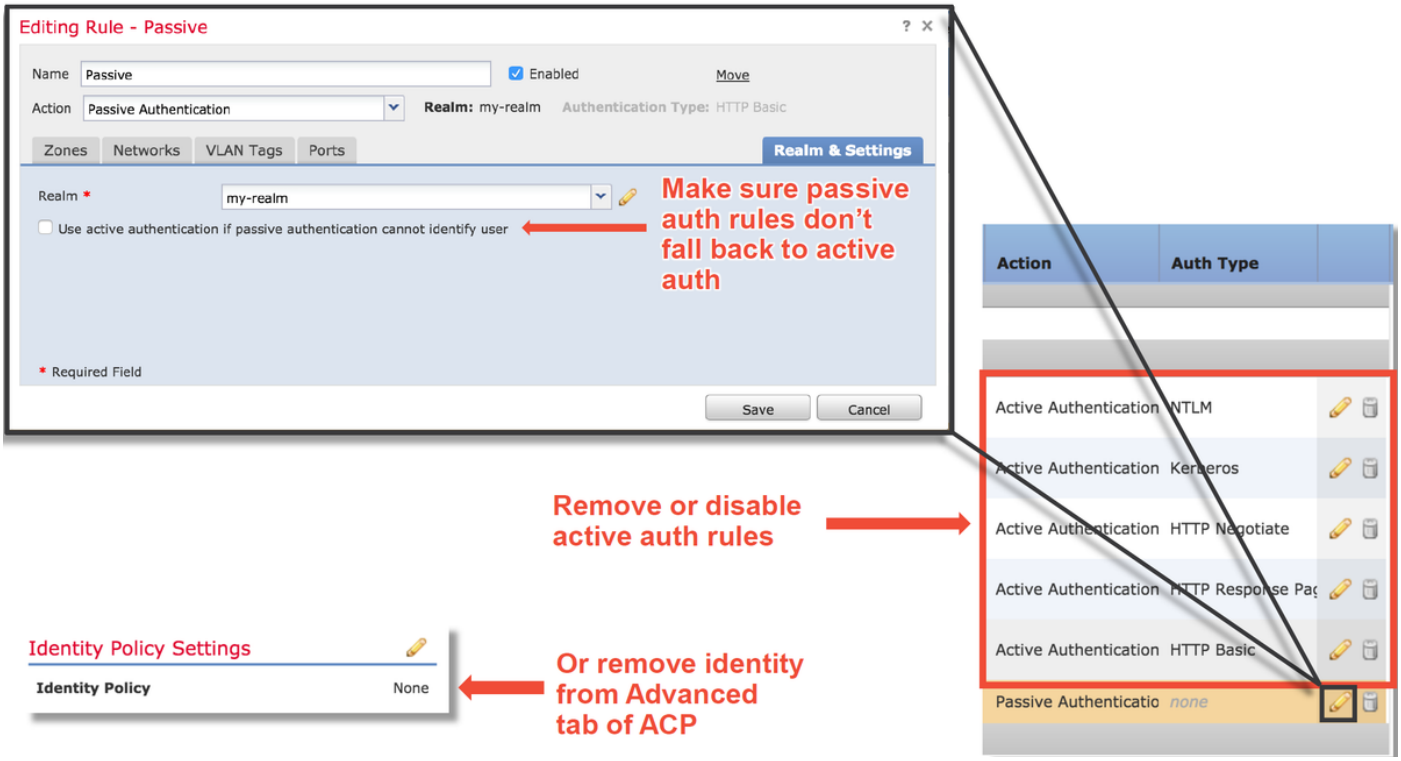
Per una risoluzione più dettagliata dei problemi relativi al criterio SSL, consultare l'articolo relativo alla risoluzione dei problemi del percorso dati.

Autenticazione attiva

Se utilizzata in un criterio di identità, l'autenticazione attiva consente di bloccare il traffico che dovrebbe essere autorizzato in caso di problemi. La stessa funzionalità di autenticazione attiva può avere un impatto diretto su tutto il traffico HTTP/HTTPS perché, se viene determinato che è necessario autenticare un utente, tutto questo avviene solo tramite il protocollo HTTP. Ciò significa che l'autenticazione attiva non deve influire su altri servizi di rete (come DNS, ICMP, ecc.) a meno che non si disponga di regole di controllo dell'accesso specifiche che si bloccano in base all'utente e gli utenti non siano in grado di eseguire l'autenticazione tramite i servizi di autenticazione attivi sull'FTD. Tuttavia, ciò non costituirebbe un problema diretto della funzionalità di autenticazione attiva, ma il risultato del fatto che gli utenti non sono in grado di autenticarsi e di disporre di un criterio che blocca gli utenti non autenticati.

Per ridurre rapidamente i rischi, è possibile disattivare qualsiasi regola all'interno dei criteri di identità con l'azione 'Autenticazione attiva'.

Verificare inoltre che per le regole con l'azione 'Autenticazione passiva' l'opzione 'Utilizza autenticazione attiva se l'autenticazione passiva non è in grado di identificare l'utente' non sia selezionata.



Per una risoluzione più approfondita dei problemi relativi all'autenticazione attiva, consultare l'articolo sulla risoluzione dei problemi relativi al percorso dati.

Policy anti-intrusione

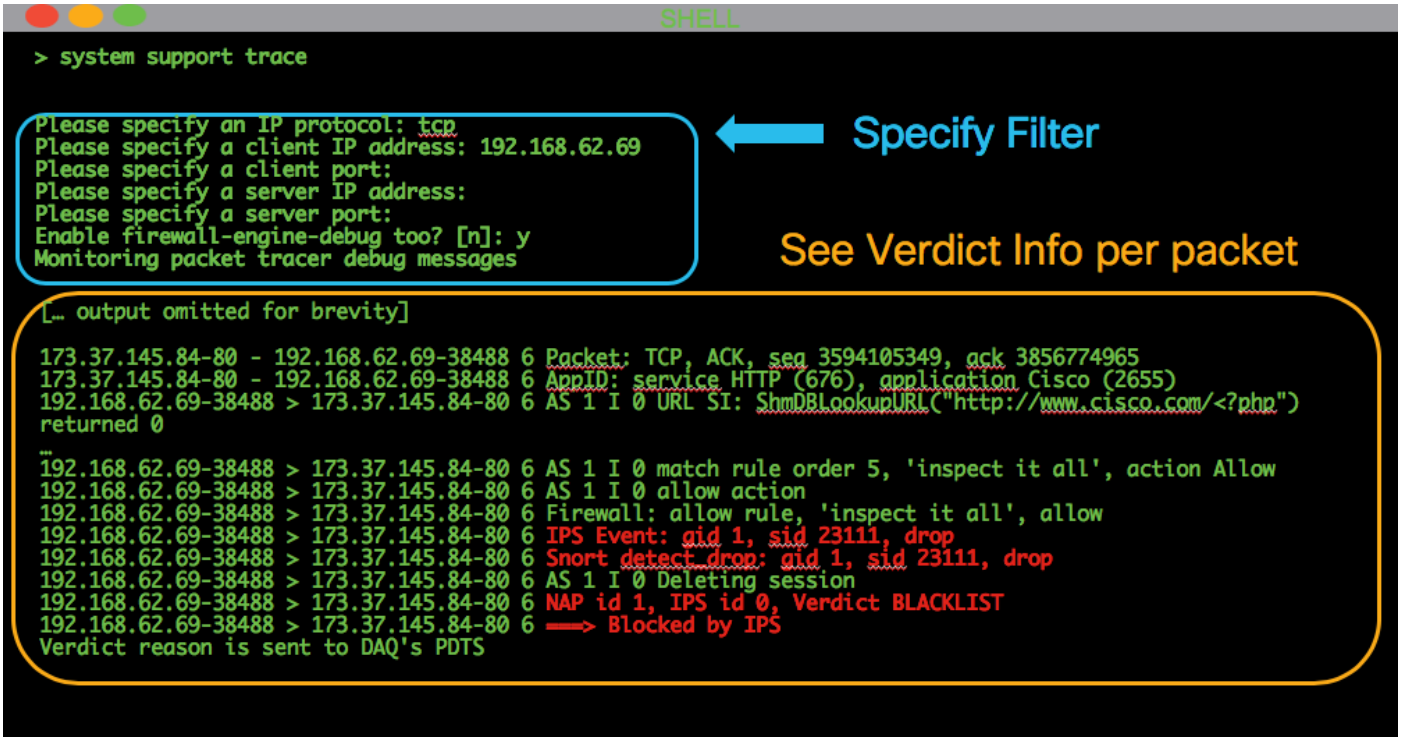
Un criterio di intrusione potrebbe causare la perdita di traffico o la latenza della rete. Un criterio di intrusione può essere utilizzato in una delle tre posizioni seguenti all'interno del criterio di controllo dell'accesso:

- In una regola di controllo d'accesso, nella scheda Ispezione
- Nell'azione predefinita
- Nella scheda Avanzate, nella sezione **Analisi di rete e criteri intrusione > Criteri intrusione utilizzati prima della determinazione della regola di controllo di accesso**

Per verificare se una regola dei criteri per le intrusioni blocca il traffico, passare alla pagina **Analisi > Intrusioni > Eventi** nel FMC. La **vista Tabella della** vista **Eventi di intrusione** fornisce informazioni sugli host coinvolti negli eventi. Per informazioni relative all'analisi degli eventi, consultare l'articolo relativo alla risoluzione dei problemi del percorso dati.

Per stabilire se una firma IPS (Intrusion Policy Signature) sta bloccando il traffico, si consiglia innanzitutto di utilizzare la funzione di **> traccia del supporto di sistema** dalla CLI dell'FTD. Questo comando debug funziona in modo simile a firewall-engine-debug e consente inoltre di abilitare firewall-engine-debug insieme alla traccia.

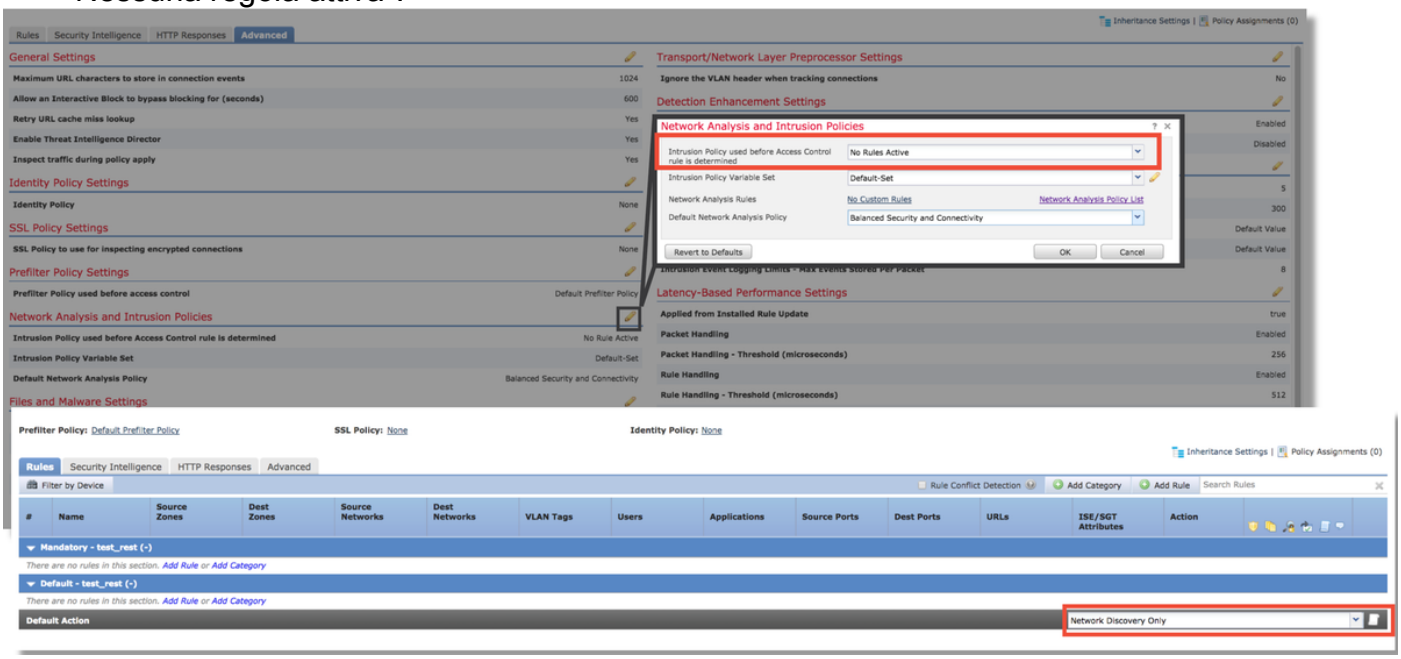
Nella figura seguente viene illustrato un esempio di utilizzo dello strumento di analisi del supporto di sistema in cui il risultato ha mostrato che un pacchetto era bloccato a causa di una regola di intrusione. In questo modo è possibile ottenere tutti i dettagli, quali il GID (Group Identifier), il SID (Signature Identifier), l'ID di Protezione accesso alla rete (Network Analysis Policy) e l'ID IPS, in modo da poter vedere esattamente quali criteri/regole bloccano il traffico.



Se non si è in grado di determinare che IPS blocca l'output di analisi, ma si sospetta che IPS stia eliminando a causa di un criterio di intrusione personalizzato, è possibile sostituire il criterio di intrusione con un criterio "Protezione e connettività bilanciate" o un criterio "Connettività su protezione". Si tratta di policy sulle intrusioni fornite da Cisco. Se si apporta questa modifica, il problema viene risolto, quindi il criterio di intrusione personalizzato utilizzato in precedenza può essere risolto da TAC. Se si usa già un criterio Cisco predefinito, è possibile provare a modificare il criterio predefinito in uno meno sicuro, in quanto contiene meno regole, in modo da restringere l'ambito. Ad esempio, se il traffico è bloccato e si utilizza un criterio bilanciato, si passa alla connettività tramite un criterio di sicurezza e il problema si risolve, è probabile che nel criterio bilanciato sia presente una regola che elimina il traffico che non è impostato per essere eliminato nel criterio di connettività tramite un criterio di sicurezza.

Le seguenti modifiche possono essere apportate all'interno dei criteri di controllo dell'accesso per eliminare tutte le possibilità di blocco delle ispezioni dei criteri per le intrusioni (si consiglia di apportare il minor numero possibile di modifiche in modo da non alterare l'efficacia della sicurezza; si consiglia pertanto di applicare regole CA specifiche per il traffico in questione, anziché disabilitare IPS nell'intero criterio):

- In tutte le regole di controllo d'accesso (o solo nelle regole corrispondenti a cui corrisponde il traffico specifico interessato), rimuovere i criteri per le intrusioni dalla scheda Ispezione
- Nella scheda Avanzate, nella sezione **Analisi di rete e criteri intrusione > Criteri intrusione utilizzati prima della determinazione della regola di controllo di accesso**, scegliere il criterio "Nessuna regola attiva".



Se il problema persiste, passare alla risoluzione dei problemi relativi ai criteri di analisi della rete.

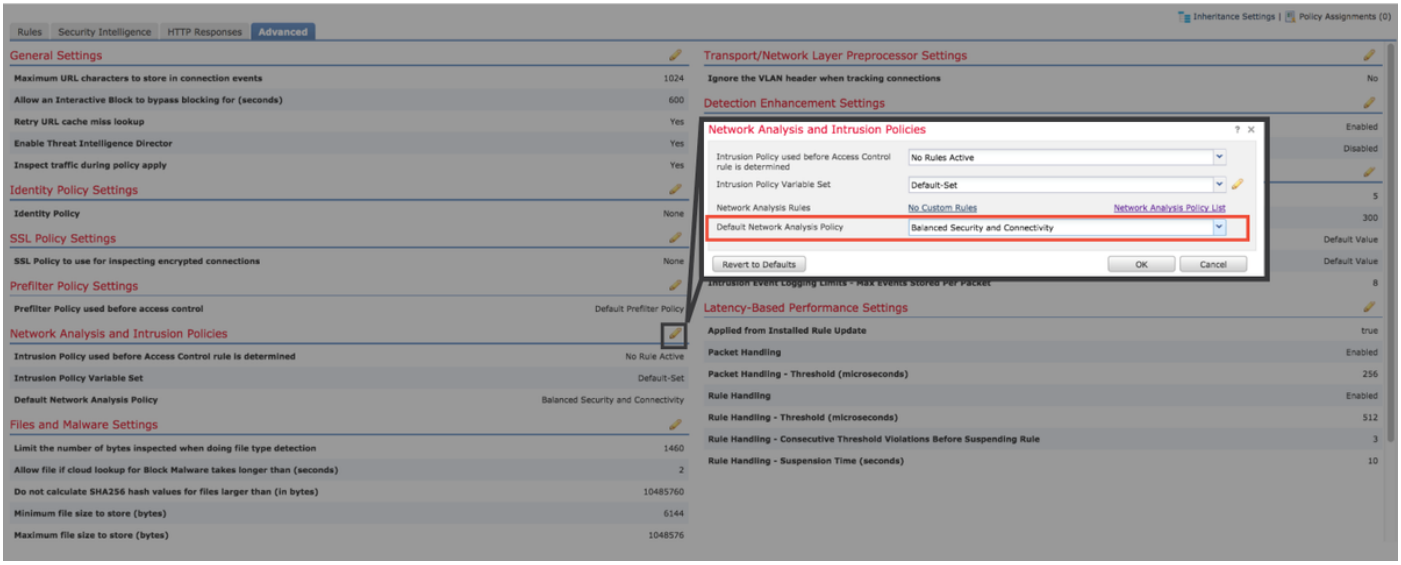
Risoluzione più approfondita dei problemi relativi alla funzionalità Intrusion Policy, consultare l'articolo relativo alla risoluzione dei problemi del percorso dati.

Criteri di analisi della rete

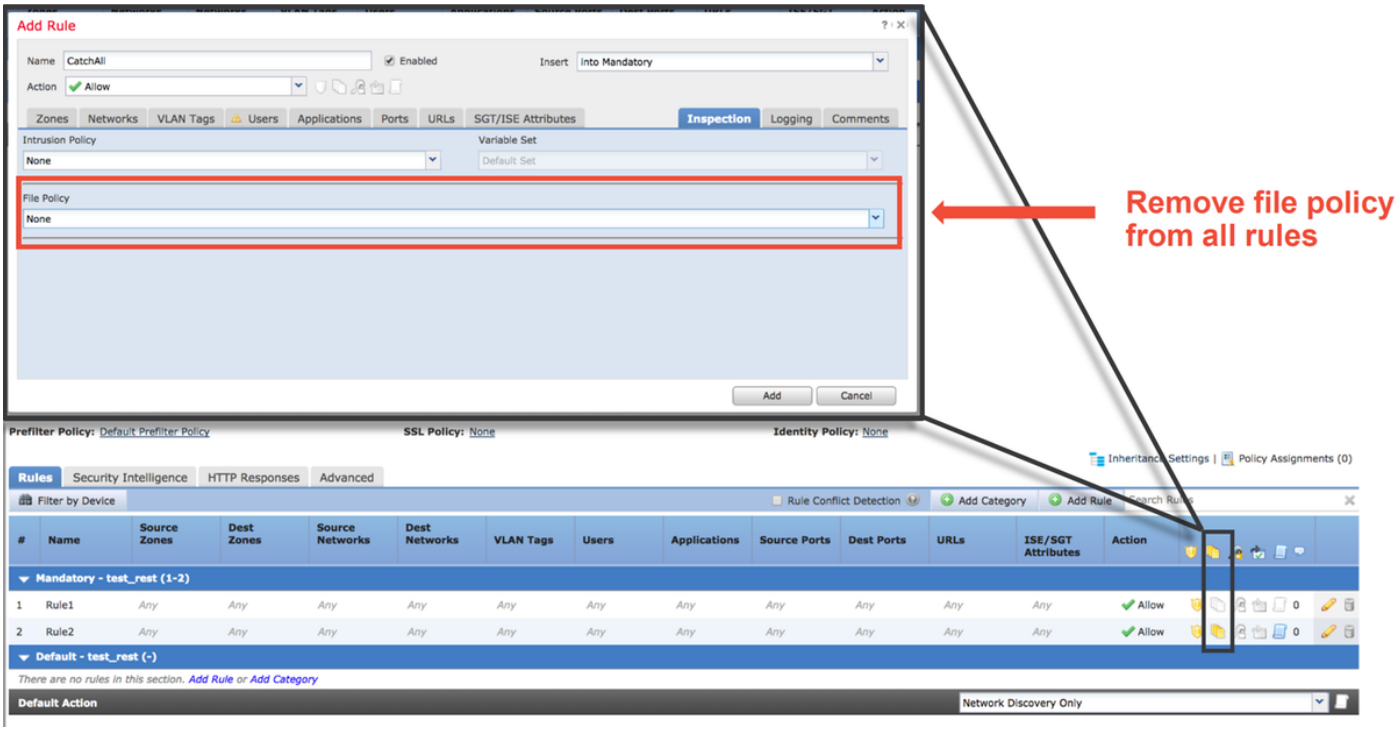
I criteri di analisi della rete contengono impostazioni del preprocessore Firepower, alcune delle quali possono causare la perdita di traffico. Il primo passaggio consigliato per la risoluzione dei problemi è lo stesso della risoluzione dei problemi IPS, che prevede l'utilizzo dello strumento di **> traccia del supporto di sistema** per cercare di individuare il problema che blocca il traffico. Per ulteriori informazioni su questo strumento e sull'utilizzo di esempio, vedere la sezione "Criteri intrusione".

Per ridurre rapidamente i possibili problemi di Protezione accesso alla rete, è possibile eseguire i passaggi seguenti:

- Se viene utilizzato un criterio di Protezione accesso alla rete personalizzato, sostituirlo con un criterio "Protezione e connettività bilanciate" o "Connettività su protezione"



- Se vengono utilizzate "regole personalizzate", assicurarsi di impostare Protezione accesso alla rete su uno dei valori predefiniti sopra indicati
- Se una regola di controllo d'accesso utilizza un criterio file, rimuoverlo temporaneamente come criterio file per abilitare le impostazioni del preprocessore sul backend che non verranno riflesse nella GUI



In questo articolo è possibile esaminare procedure più dettagliate per la risoluzione dei problemi relativi alla funzionalità Criteri di analisi della rete.

Informazioni correlate

Collegamenti alla documentazione di Firepower

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html