Determinare il traffico gestito da una specifica istanza di snort

Sommario

Introduzione

Questo documento descrive come determinare il traffico gestito da un'istanza Snort specifica in un ambiente Cisco Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti prodotti:

- Secure Firepower Management Center (FMC)
- Secure Firepower Threat Defense (FTD)
- Syslog e SNMP
- API REST

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

1. Uso dei comandi CLI

Usando l'interfaccia della riga di comando (CLI) sul dispositivo FTD, è possibile accedere a informazioni dettagliate sulle istanze Snort e sul traffico che gestiscono.

- Questo comando fornisce i dettagli relativi all'esecuzione dei processi Snort.

show snort instances

Di seguito è riportato un esempio per l'output del comando.

> show snort instances

Total number of instances available - 1 +----------+----------+ | INSTANCE | PID | +----------+----------+ | **1** | **4765** | <<< One instance available and its process ID +----------+----------+

- Per informazioni più dettagliate sulle statistiche del traffico gestite dalle istanze Snort, è possibile utilizzare questi comandi. Vengono visualizzate varie statistiche, tra cui il numero di pacchetti elaborati, scartati e gli avvisi generati da ogni istanza di Snort.

show snort statistics

Di seguito è riportato un esempio per l'output del comando.

> show snort statistics Packet Counters: Passed Packets 3791881977 Blocked Packets 707722 Injected Packets 87 **Packets bypassed (Snort Down) 253403701** <<< Packets bypassed **Packets bypassed (Snort Busy) 0** Flow Counters: Fast-Forwarded Flows 294816 Blacklisted Flows 227 Miscellaneous Counters: Start-of-Flow events 0 End-of-Flow events 317032 Denied flow events 14230 Frames forwarded to Snort before drop 0 Inject packets dropped 0 TCP Ack bypass Packets 6412936 TCP Meta-Ack Packets 2729907 Portscan Events 0 Packet decode optimized 21608793 Packet decode legacy 6558642

show asp inspect-dp snort

Di seguito è riportato un esempio per l'output del comando.

> show asp inspect-dp snort

SNORT Inspect Instance Status Info Id Pid Cpu-Usage Conns Segs/Pkts Status tot (usr | sys) -- ----- ---------- ---------- ---------- -- -------- 0 16450 8% (7%| 0%) 2.2 K 0 READY 1 16453 9% (8%| 0%) 2.2 K 0 READY 2 16451 6% (5%| 1%) 2.3 K 0 READY 3 16454 5% (5%| 0%) 2.2 K 1 READY 4 16456 6% (6%| 0%) 2.3 K 0 READY 5 16457 6% (6%| 0%) 2.3 K 0 READY 6 16458 6% (5%| 0%) 2.2 K 1 READY 7 16459 4% (4%| 0%) 2.3 K 0 READY 8 16452 9% (8%| 1%) 2.2 K 0 READY **9 16455 100% (100%| 0%) 2.2 K 5 READY** <<<< High CPU utilization 10 16460 7% (6%| 0%) 2.2 K 0 READY -- ----- ---------- ---------- ---------- ---------- Summary 15% (14%| 0%) 24.6 K 7

-

Utilizzo di Firepower Management Center (FMC)

Se si gestiscono i dispositivi FTD tramite FMC, è possibile ottenere informazioni dettagliate e rapporti sul traffico e sulle istanze Snort tramite

l'interfaccia Web.

- Controllo

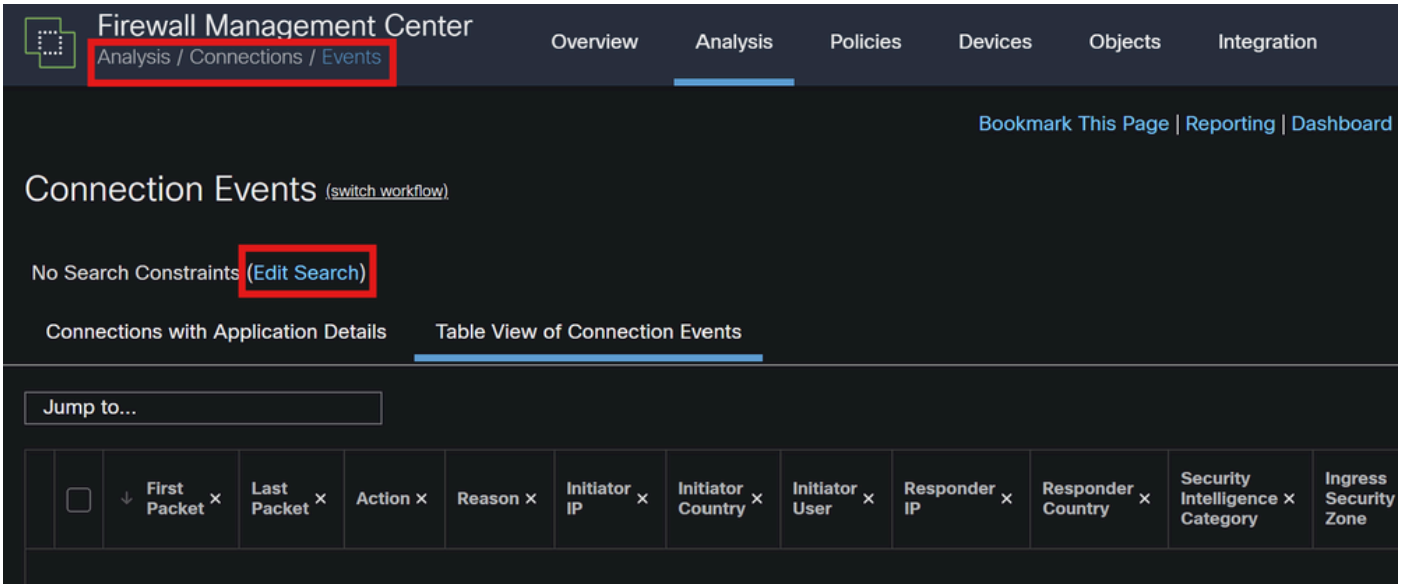
Dashboard di FMC: passare al dashboard in cui è possibile visualizzare una panoramica dello stato del sistema, incluse le istanze Snort.

Monitoraggio dello stato: nella sezione Monitoraggio dello stato è possibile ottenere statistiche dettagliate sui processi di snort, incluso il traffico gestito.

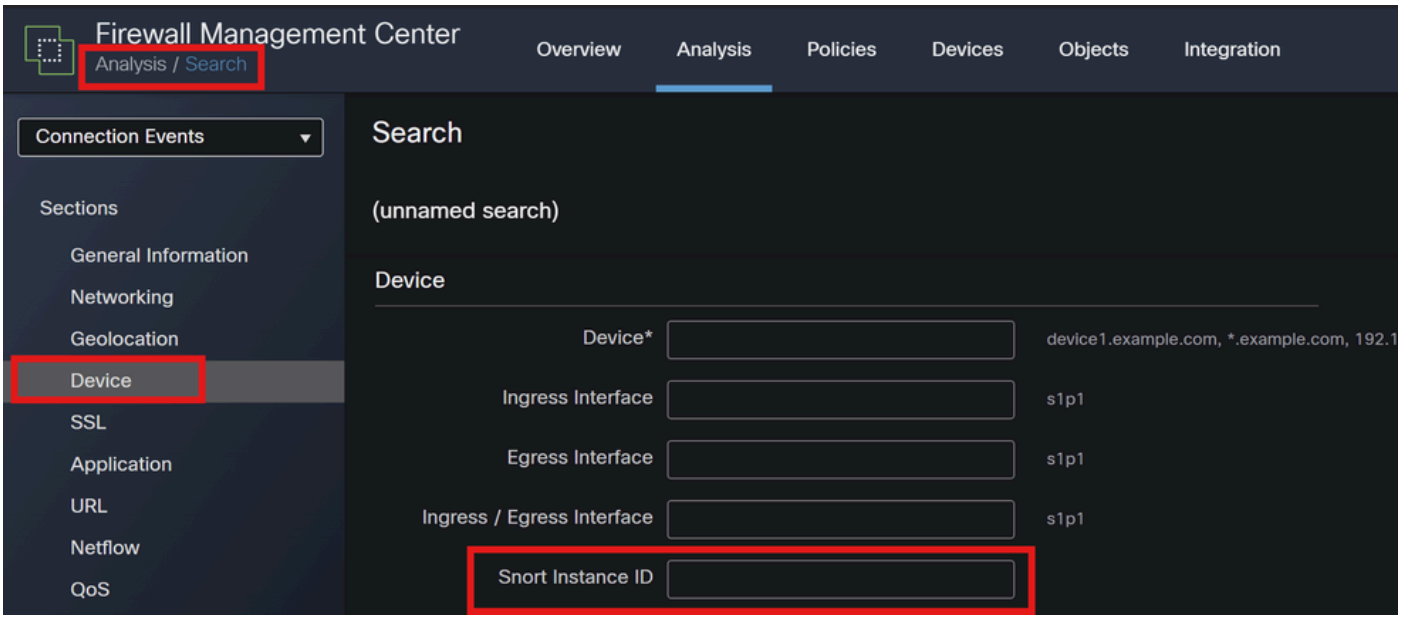
- Analisi

Analisi: passare ad **Analisi > Eventi connessione**.

Filtri: utilizzare i filtri per limitare i dati all'istanza Snort o al traffico a cui si è interessati.



Eventi connessione



ID istanza snort

-

Uso di Syslog e SNMP

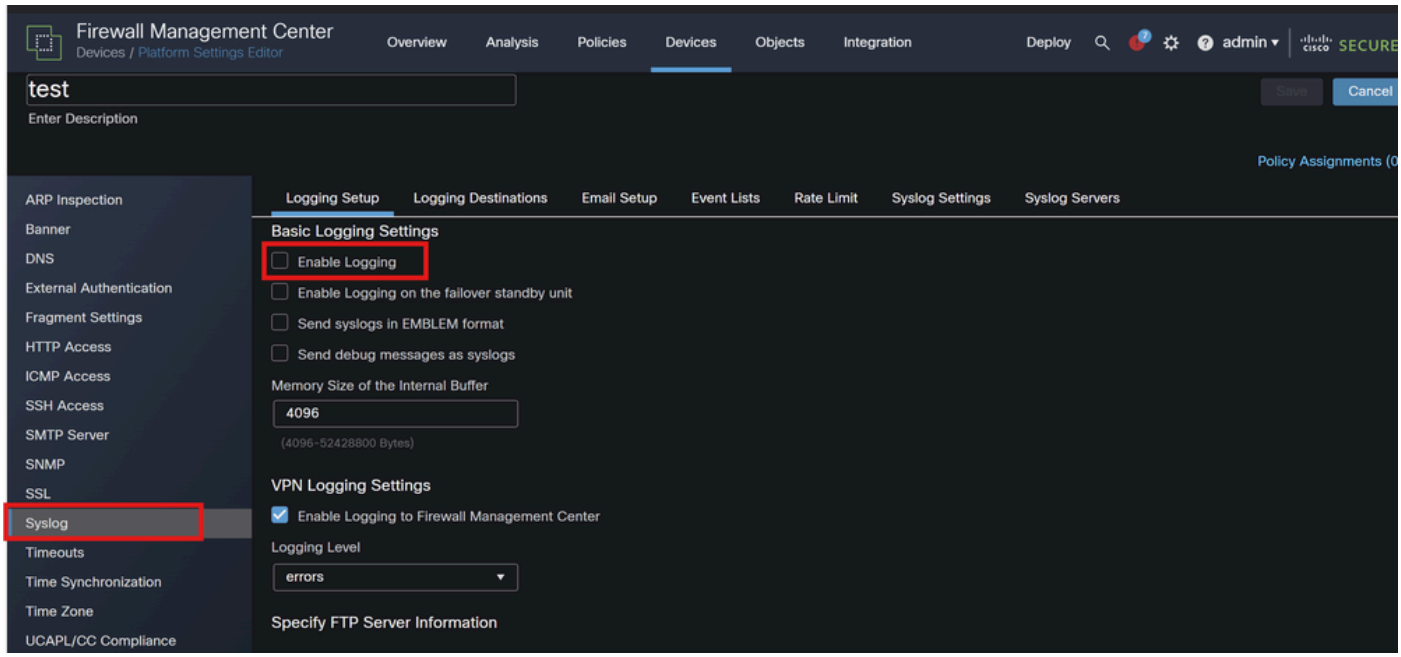
È possibile configurare l'FTD in modo che invii messaggi syslog o trap SNMP a un sistema di monitoraggio esterno dove è possibile analizzare i dati del traffico.

- Configurazione Syslog

Dispositivi: in FMC, selezionare **Dispositivi > Impostazioni piattaforma**.

Creare o modificare un criterio: scegliere il criterio di impostazioni della piattaforma appropriato.

Syslog: configurare le impostazioni syslog in modo da includere gli avvisi e le statistiche Snort.

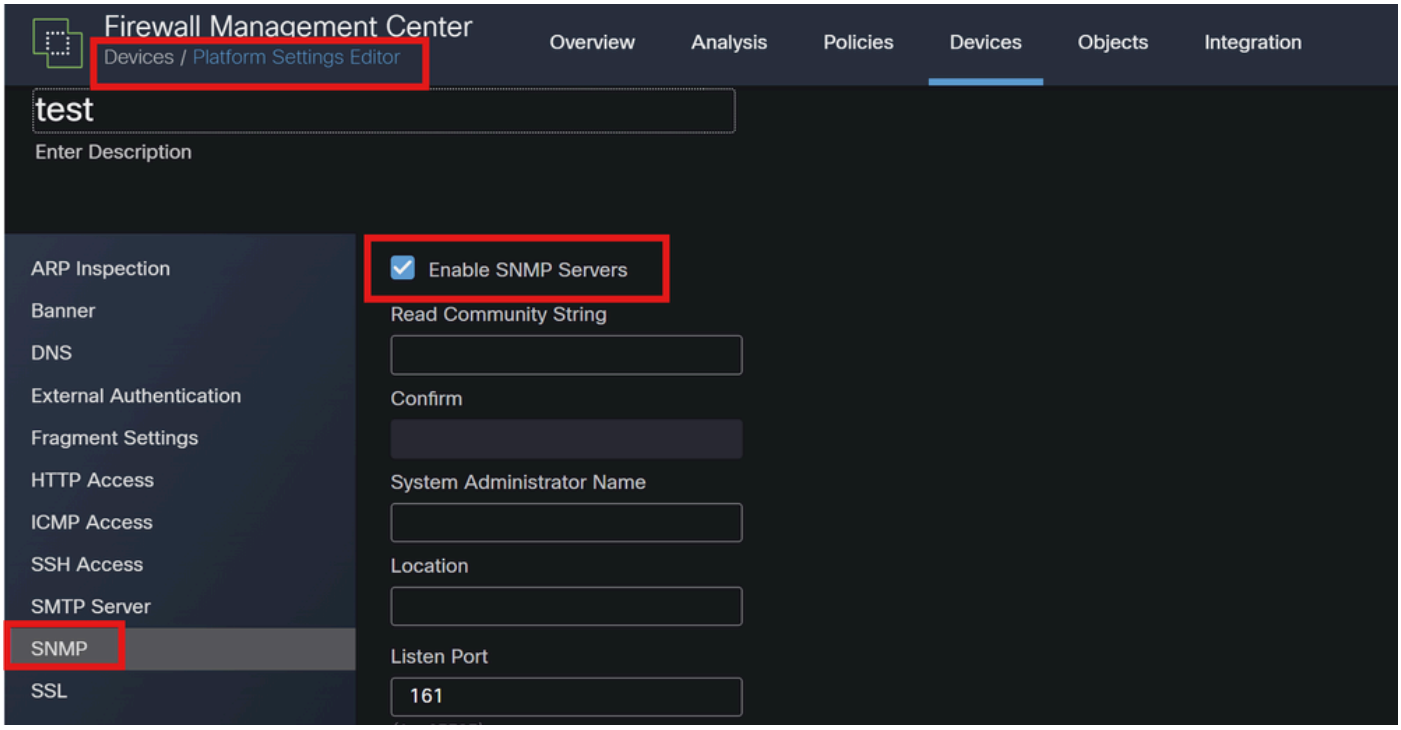


Configurazione Syslog

- Configurazione SNMP

Impostazioni SNMP: come in syslog, configurare le impostazioni SNMP in **Dispositivi > Impostazioni piattaforma**.

Trap: verificare che le trap SNMP necessarie siano abilitate per le statistiche delle istanze Snort.



Configurazione SNMP

4. Uso degli script personalizzati

Per gli utenti avanzati, è possibile scrivere script personalizzati che utilizzano l'API REST FTD per raccogliere statistiche sulle istanze Snort. Questo approccio richiede una certa familiarità con gli script e l'utilizzo delle API.

- API REST

Accesso API: verificare che l'accesso API sia abilitato nel CCP.

Chiamate API: utilizzare le chiamate API appropriate per recuperare le statistiche e i dati sul traffico relativi allo snort.

In questo modo vengono restituiti i dati JSON che è possibile analizzare e analizzare per determinare il traffico gestito da specifiche istanze Snort.

Combinando questi metodi, è possibile ottenere una comprensione completa del traffico gestito da ciascuna istanza Snort nell'implementazione Cisco FTD.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).