

# 確定特定Snort例項處理的流量

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[使用命令列介面命令](#)

[使用Firepower管理中心\(FMC\)](#)

[使用系統日誌和SNMP](#)

---

## 簡介

本檔案介紹如何判斷在Cisco Firepower威脅防禦(FTD)環境中特定Snort執行個體處理的流量。

## 必要條件

### 需求

思科建議您瞭解以下產品：

- 安全Firepower管理中心(FMC)
- 安全Firepower威脅防禦(FTD)
- 系統日誌和SNMP
- REST API

### 採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

#### 1. 使用命令列介面命令

使用FTD裝置上的指令行介面(CLI)，您可以存取有關Snort例項及其處理流量的詳細資訊。

- 此命令提供有關正在運行的Snort進程的詳細資訊。

```
show snort instances
```

以下是指令輸出的範例。

```
> show snort instances
```

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

- 有關Snort例項處理的流量統計資訊的詳細資訊，可以使用以下命令。這會顯示各種統計資訊，包括已處理、丟棄的資料包的數量，以及每個Snort例項生成的警報。

```
show snort statistics
```

以下是指令輸出的範例。

```
> 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
```

以下是指令輸出的範例。

```
> 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
```

- .

## 使用Firepower管理中心(FMC)

如果您透過FMC管理FTD裝置，則可透過Web介面取得有關流量和Snort執行處理的詳細見解和報告。

- 監控

FMC儀表板：導航至儀表板，您可以在其中檢視系統狀態的概覽，包括Snort例項。

運行狀況監控：在運行狀況監控部分，您可以獲取有關Snort進程的詳細統計資訊，包括已處理的流量。

- 分析

分析：導航到分析>連線事件。

過濾器：使用過濾器將資料縮小到您感興趣的特定Snort例項或流量。

Firewall Management Center

Analysis / Connections / Events

Overview Analysis Policies Devices Objects Integration

Bookmark This Page | Reporting | Dashboard

### Connection Events (switch workflow)

No Search Constraints **(Edit Search)**

Connections with Application Details **Table View of Connection Events**

Jump to...

<input type="checkbox"/>	↓ First Packet ×	Last Packet ×	Action ×	Reason ×	Initiator IP ×	Initiator Country ×	Initiator User ×	Responder IP ×	Responder Country ×	Security Intelligence × Category	Ingress Security Zone
--------------------------	------------------	---------------	----------	----------	----------------	---------------------	------------------	----------------	---------------------	----------------------------------	-----------------------

連線事件

Firewall Management Center

Analysis / Search

Overview Analysis Policies Devices Objects Integration

Connection Events

### Search

(unnamed search)

Sections

- General Information
- Networking
- Geolocation
- Device**
- SSL
- Application
- URL
- Netflow
- QoS

Device

Device\*  device1.example.com, \*.example.com, 192.1

Ingress Interface  s1p1

Egress Interface  s1p1

Ingress / Egress Interface  s1p1

**Snort Instance ID**

Snort例項ID

- 

使用系統日誌和SNMP

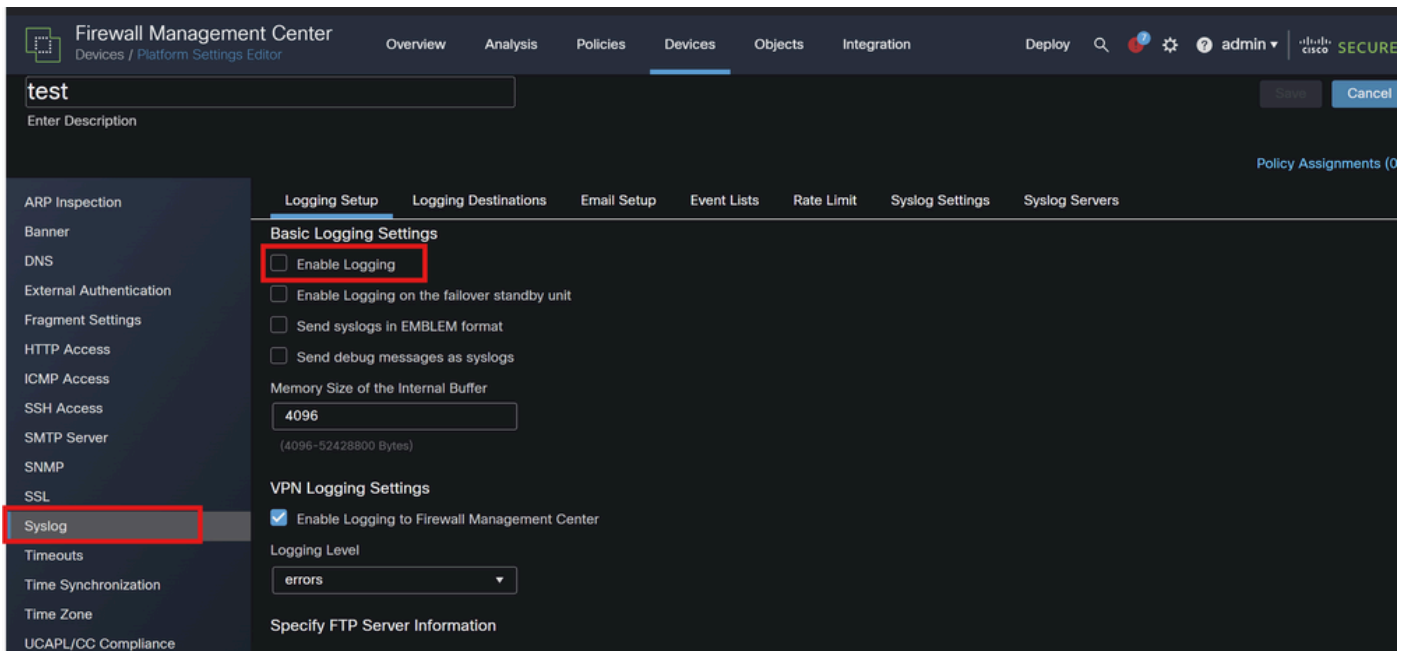
您可以將FTD設定為將系統日誌訊息或SNMP陷阱傳送到外部監控系統，以便分析流量資料。

- 系統日誌配置

裝置：在FMC中，導航到裝置>平台設定。

建立或編輯策略：選擇適當的平台設定策略。

系統日誌：配置系統日誌設定以包括Snort警報和統計資訊。

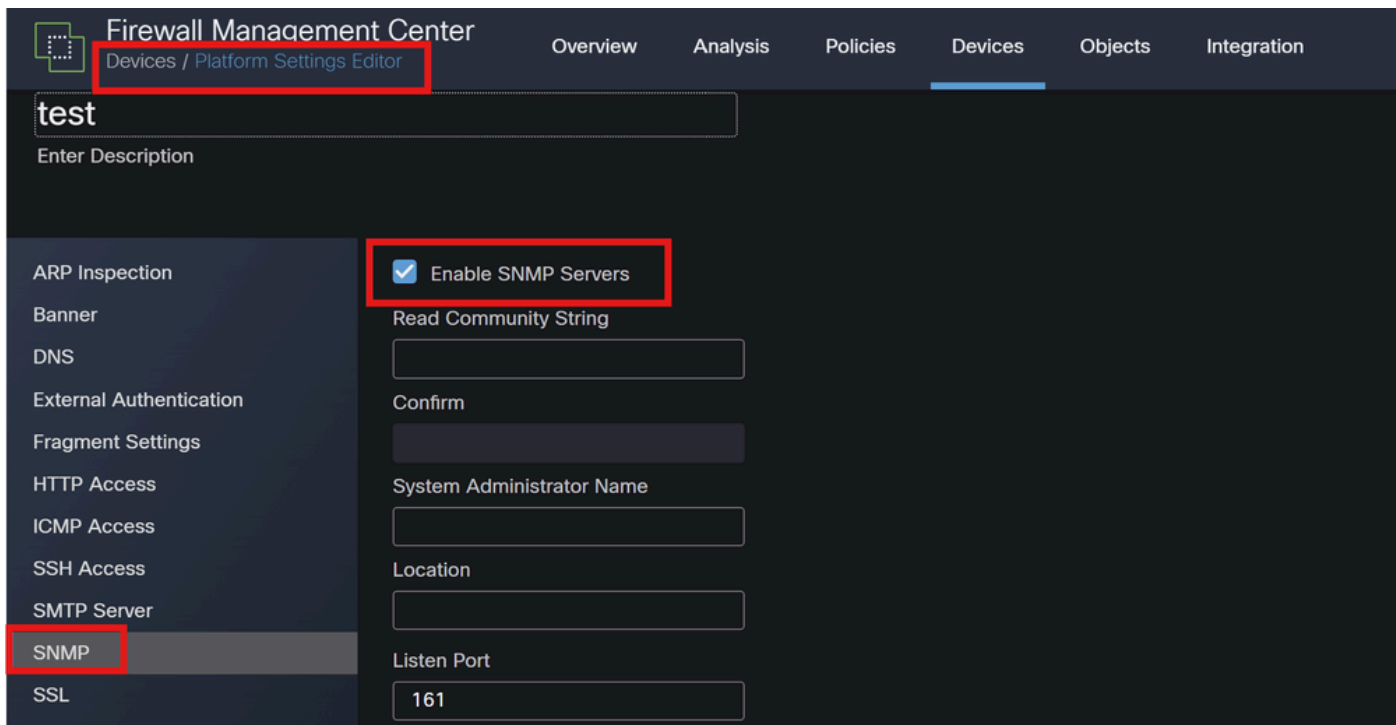


## 系統日誌配置

- SNMP配置

SNMP設定：與syslog相似，請在Devices > Platform Settings下配置SNMP設定。

陷阱：確保為Snort例項統計資訊啟用必要的SNMP陷阱。



## SNMP配置

### 4. 使用自訂指令集

對於高級使用者，您可以編寫使用FTD REST API來收集有關Snort例項的統計資訊的自定義指令碼。此方法需要熟悉指令碼和API用法。

- REST API

API訪問：確保在FMC上啟用API訪問。

API呼叫：使用相應的API呼叫獲取Snort統計資訊和流量資料。

這會返回您可以解析和分析的JSON資料，以確定由特定Snort例項處理的流量。

透過結合這些方法，您可以全面瞭解Cisco FTD部署中每個Snort執行處理所處理的流量。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。