

# 監控並解決ASA效能問題

## 目錄

---

### [簡介](#)

#### [必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

#### [排除效能問題](#)

[速度和雙工設定](#)

[CPU使用率](#)

[記憶體使用率高](#)

[PortFast、通道和中繼](#)

[網路位址翻譯\(NAT\)](#)

[系統日誌](#)

[SNMP](#)

[反向DNS查詢](#)

#### [顯示命令](#)

[顯示CPU使用情況](#)

[顯示流量](#)

[顯示Perfmon](#)

[顯示區塊](#)

[顯示記憶體](#)

[顯示Xlate](#)

[顯示連線埠計數](#)

[顯示介面](#)

[顯示進程](#)

[命令摘要](#)

#### [相關資訊](#)

---

## 簡介

本文檔介紹用於監控和排除Cisco自適應安全裝置(ASA)效能故障的命令。

## 必要條件

## 需求

本文件沒有特定需求。

## 採用元件

本文檔中的資訊基於運行版本8.3及更高版本的思科自適應安全裝置(ASA)。

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。


## 慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

## 排除效能問題

若要對效能問題進行疑難排解，請檢查本節所述的基本區域。

---

 **注意：**如果您有來自Cisco裝置的show 命令的輸出，則可以使用[Cisco CLI Analyzer](#)顯示潛在問題和解決方法。Cisco CLI Analyzer支援某些show 指令。如果您使用思科CLI分析器，您必須是思科註冊使用者，必須登入您的思科帳戶，並且必須在瀏覽器中啟用JavaScript。

---

### 速度和雙工設定

安全裝置已預配置為自動檢測介面上的速度和雙工設定。但是，有幾種情況會導致自動交涉程式失敗，造成速度或雙工不相符 ( 和效

能問題)。對於任務關鍵型網路基礎設施，Cisco手動對每個介面的速度和雙工進行硬編碼，因此不會出錯。這些裝置通常不會移動，因此，如果正確配置它們，則不需要進行更改。

在任何網路裝置上，都可以感測連結速度，但必須交涉雙工。如果兩台網路裝置設定為自動交涉速度和雙工，它們會交換通告其速度和雙工功能的訊框（稱為快速連結脈衝或FLP）。對於不知道的鏈路夥伴而言，這些脈衝類似於常規10 Mbps幀。對於可以解碼脈衝的鏈路夥伴，FLP包含鏈路夥伴可以提供的所有速度和雙工設定。接收FLP的月台會確認訊框，且裝置會就各自可達到的最高速度和雙工設定達成一致。如果一台裝置不支援自動協商，另一台裝置將接收FLP並轉換為並行檢測模式。為了檢測對方的速度，裝置會偵聽脈衝長度，然後根據長度設定速度。雙工設定出現問題。由於必須協商雙工，因此設定為自動協商的裝置無法確定其他裝置上的設定，因此預設設定為半雙工，如IEEE 802.3u標準中所述。

例如，如果您將ASA介面配置為自動協商，並將其連線到為100 Mbps和全雙工硬編碼的交換機，則ASA會傳送FLP。但是，交換器沒有回應，因為它已對速度和雙工進行硬式編碼，而且不會參與自動交涉。由於未收到來自交換機的響應，因此ASA會轉換到並行檢測模式，並檢測交換機發出的幀中的脈衝長度。也就是說，ASA檢測到交換機設定為100 Mbps，因此它基於此設定介面速度。但是，由於交換機不交換FLP，因此ASA無法檢測交換機是否可以運行全雙工，因此ASA將介面雙工設定為半雙工，如IEEE 803.2u標準中所述。由於交換機硬編碼為100 Mbps和全雙工，並且ASA剛剛自動協商為100 Mbps和半雙工（就像現在一樣），因此可能導致雙工不匹配而導致嚴重的效能問題。

當相關介面上的錯誤計數器增加時，最常顯示速度或雙工不匹配。最常見的錯誤是幀、循環冗餘檢查(CRC)和殘幀。如果介面上的這些值增加，則可能發生速度/雙工不匹配或佈線問題。您必須先解決此問題，然後才能繼續。

## 範例

```
<#root>
```

```
Interface GigabitEthernet0/0 "outside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex), A
157 runts
, 0 giants
379 input errors, 107 CRC, 273 frame
, 0 overrun, 0 ignored, 0 abort 0 pause input, 0 resume input 0 L2 decode drops 121 packets output, 774
```

CPU使用率

如果您注意到CPU使用率較高，請完成以下步驟以進行故障排除：

- 確認show xlate count 中的連線計數較低。
- 驗證記憶體塊是否正常。
- 檢驗ACL的數量是否更高。
- 發出show memory detail命令並確認ASA使用的記憶體為正常使用率。
- 確認show processes cpu-hog和show processes memory中的計數正常。
- 安全裝置內部或外部的任何主機都可能生成惡意或大量流量，這些流量可以是廣播/組播流量，並導致CPU使用率較高。為了解決此問題，請配置一個訪問清單以拒絕主機之間的流量（端到端）並檢查使用情況。
- 檢查ASA介面中的雙工和速度設定。遠端介面設定不匹配會增加CPU利用率。

本示例顯示了因為速度不匹配而造成 *input error* 和 *overruns* 的值較大。請使用show interface 命令驗證錯誤：

```
<#root>
```

```
Ciscoasa#
```

```
sh int GigabitEthernet0/1
```

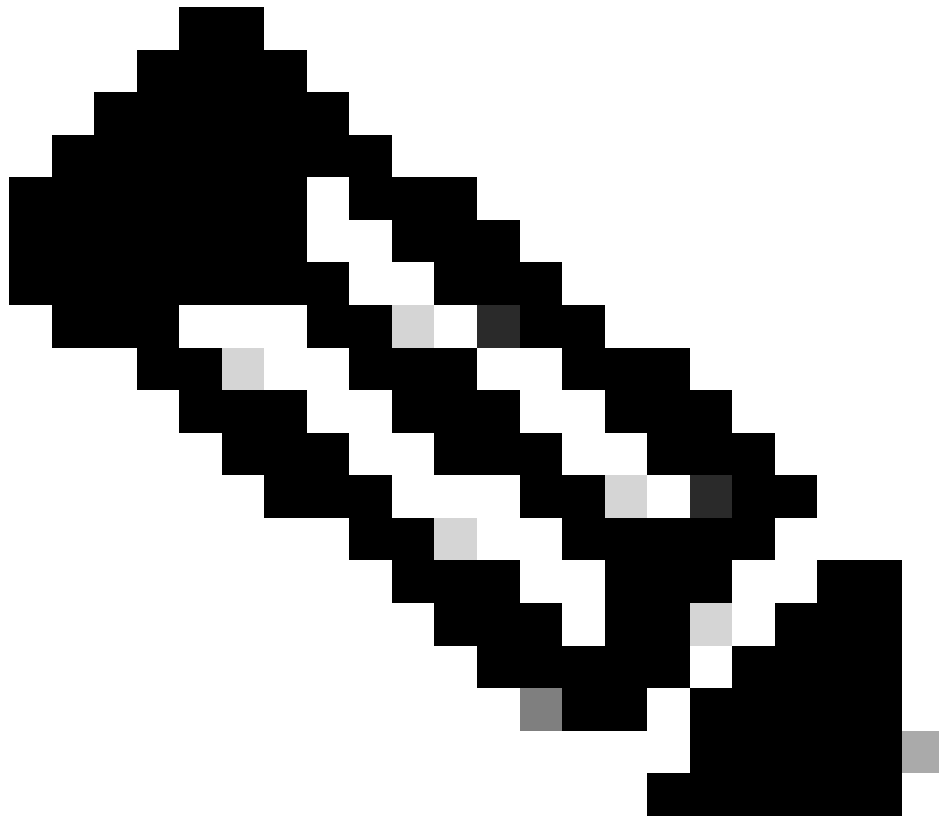
```
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 0013.c480.b2b8, MTU 1500
  IP address 192.168.17.4, subnet mask 255.255.255.0
  311981 packets input, 20497296 bytes, 0 no buffer
  Received 311981 broadcasts, 157 runts, 0 giants
```

```
7186 input errors, 0 CRC, 0 frame, 7186 overrun
```

```
, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  121 packets output, 7744 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 1 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops, 0 tx hangs
  input queue (blocks free curr/low): hardware (255/249)
  output queue (blocks free curr/low): hardware (255/254)
```

要解決此問題，請將相應介面的速度設定為 *auto*。

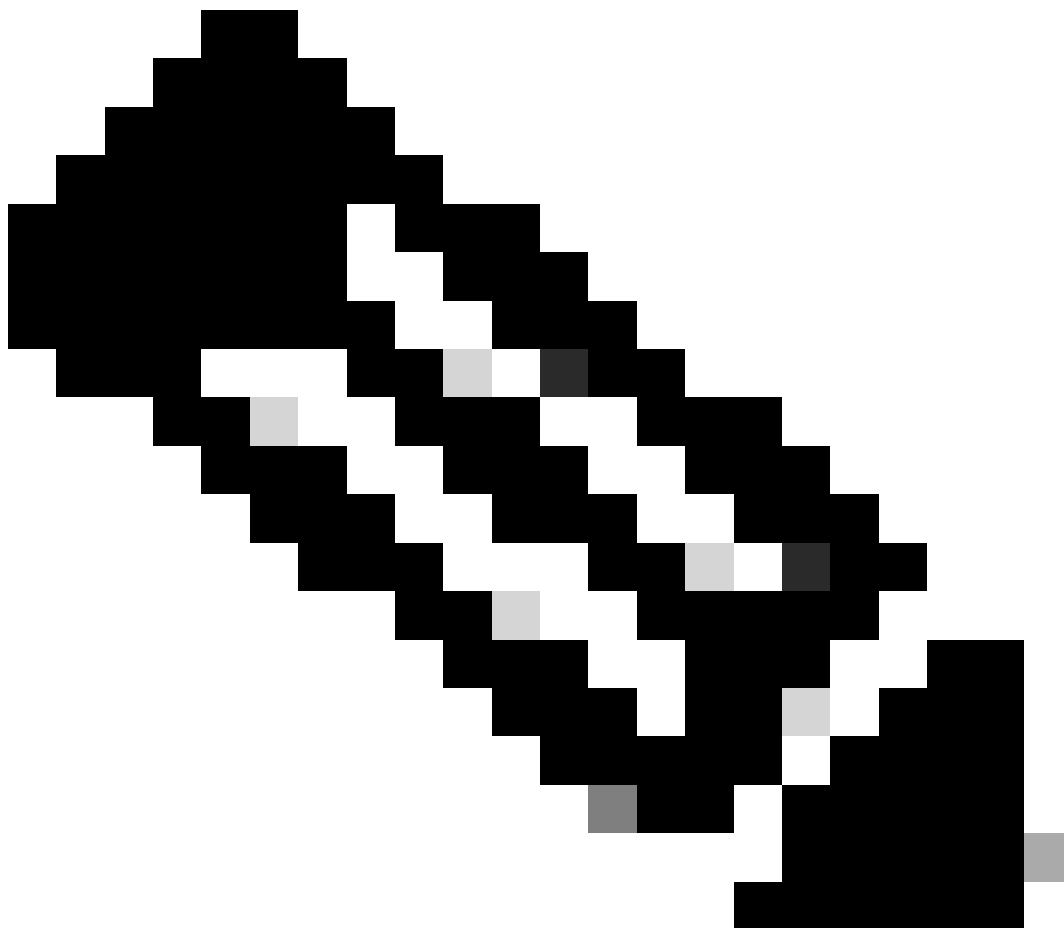
---



注意：Cisco建議您在所有介面上啟用 `ip verify reverse-path interface` 命令。這會導致沒有有效源地址的資料包被丟棄，從而減少CPU使用率。這適用於FWSM面臨高CPU問題時。

---


- 
- CPU使用率較高的另一個原因可能是由於多播路由過多。發出show mroute命令來檢查ASA是否收到過多組播路由。
  - 使用show local-host命令檢視網路是否受到了拒絕服務攻擊，該攻擊表明網路可能受到病毒攻擊。
  - 由於Cisco bug ID [CSCsq48636](#)（僅限註冊使用者），CPU使用率可能會很高。有關詳細資訊，請參閱思科漏洞ID [CSCsq48636](#)。
- 



---

注意：只有已註冊的思科使用者才能訪問內部思科工具和錯誤資訊。

---

 注意：如果之前提供的解決方案無法解決問題，請根據要求升級ASA平台。有關自適應安全裝置平台功能和能力的詳細資訊，請參閱[安全裝置的思科安全模組](#)。請與TAC([Cisco技術支援](#))聯絡以獲取更多資訊。

---

## 記憶體使用率高

以下是記憶體使用率高的一些可能原因與解決方法：

- **事件日誌記錄**：事件日誌記錄會消耗大量的記憶體。要解決此問題，請安裝所有事件並將其記錄到外部伺服器（例如syslog伺服器）。
- **記憶體洩漏**：安全裝置軟體中的一個已知問題可能導致高記憶體消耗。要解決此問題，請升級安全裝置軟體。
- **啟用除錯**：除錯會消耗大量的記憶體。為了解決此問題，請使用 `undebug all` 命令停用調試。
- **阻塞埠**：阻塞安全裝置外部介面上的埠會導致安全裝置消耗大量記憶體，以透過指定埠阻塞資料包。要解決此問題，請在ISP端阻止違規流量。
- **威脅檢測**：威脅檢測功能由針對各種威脅收集的不同級別的統計資訊和掃描的威脅檢測功能組成，這些功能可確定主機何時執行掃描。關閉此功能以減少記憶體消耗。


## PortFast、通道和中繼

預設情況下，許多交換機(例如運行Catalyst作業系統(OS)的Cisco交換機)設計為即插即用裝置。因此，當將ASA插入交換機時，許多預設埠引數是不可取的。例如，在運行Catalyst OS的交換機上，預設通道設定為自動，中繼設定為自動，並且PortFast處於停用狀態。如果將ASA連線到運行Catalyst OS的交換機，請停用通道功能，停用中繼並啟用PortFast。

通道（也稱為快速EtherChannel或Giga EtherChannel）用於繫結邏輯組中的兩個或多個物理埠，以提高整個鏈路的總體吞吐量。將連線埠設定為自動通道時，會在連結使用中時傳送連線埠聚合通訊協定(PAgP)訊框，以確定它是否為通道的一部分。如果另一台裝置嘗

試自動協商鏈路的速度和雙工，這些幀可能會出現問題。如果將連線埠上的通道化設定為「自動」，也可能會導致在連結啟動後，連線埠開始轉送流量之前額外延遲約3秒。

---


 **注意：**在Catalyst XL系列交換機上，預設情況下通道未設定為自動。因此，您必須停用連線到ASA的所有交換機埠上的通道。

---

中繼也稱為常用的中繼協定「交換機間鏈路」(ISL)或Dot1q，它在一個埠（或鏈路）上組合多個虛擬LAN (VLAN)。當兩台交換機上定義了一個以上的VLAN時，通常在兩台交換機之間使用中繼。當連線埠設定為自動主幹時，它會在連結啟動時傳送動態主幹通訊協定(DTP)訊框，以便判斷其連線的連線埠是否想要主幹。這些DTP幀可能導致鏈路的自動協商出現問題。如果交換機埠上的中繼設定為Auto，則會在鏈路接通後埠開始轉發流量之前增加約15秒的額外延遲。

PortFast也稱為快速啟動(Fast Start)，此選項可通知交換機第3層裝置已連線到交換機埠之外。埠不會等待預設的30秒（15秒進行偵聽，15秒進行學習）；相反，此操作會導致交換機在鏈路接通後立即將埠置於轉發狀態。請務必瞭解，啟用PortFast時，不會停用生成樹。該埠上的生成樹仍處於活動狀態。啟用PortFast時，只會通知交換器連結的另一端沒有連線其他交換器或集線器（僅限第2層裝置）。交換器會繞過正常的30秒延遲，同時嘗試判斷如果開啟第2層連線埠時是否會產生回圈。鏈路啟動後，仍然參與生成樹。連線埠會傳送橋接封包資料單元(BPDU)，而交換器仍會在該連線埠上偵聽BPDU。因此，建議您在連線到ASA的任何交換機埠上啟用PortFast。

---


 **注意：**Catalyst OS版本5.4及更高版本包含set port host <mod>/<port>命令，該命令允許您使用單個命令停用通道和中繼以及啟用PortFast。

---

## 網路位址翻譯(NAT)

每個NAT或NAT過載(PAT)會話會被分配一個稱為 *xlate* 的轉換插槽。即使在更改了影響它們的NAT規則之後，這些轉換仍可持續。這會導致轉換插槽或意外行為耗盡，或者兩者都耗盡進行轉換的流量。本節說明如何檢視和清除安全裝置上的xlate。

---

 **警告：**如果在安全裝置上全局清除xlate，則可能會暫時中斷透過裝置的所有流量。

---

使用外部介面IP地址的PAT的ASA配置示例：



```
object network OBJ_GENERIC_ALL subnet 0.0.0.0 0.0.0.0 nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface
```

流經安全裝置的流量最有可能經過NAT。要檢視安全裝置上所使用的轉換，請發出show xlate 命令：

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

```
5 in use, 5 most used Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice NAT
```

轉換插槽可以在進行關鍵更改後保留。要清除安全裝置上的當前轉換插槽，請發出clear xlate命令：

```
<#root>
```

```
Ciscoasa#
```

```
clear xlate
```

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

```
0 in use, 1 most used
```

clear xlate命令會從xlate表中清除所有當前的動態轉換。要清除某個特定的IP轉換，您可以結合使用clear xlate命令和global [ip

address]關鍵字。

以下是用於NAT的ASA配置示例：

```
object network inside-net subnet 0.0.0.0 0.0.0.0 object network outside-pat-pool range 10.10.10.10 10.10.10.100 nat (inside,outside) source dynamic inside
```

觀察show xlate的輸出，注意從內部10.2.2.2到外部全局10.10.10.10的轉換：

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

```
2 in use, 2 most used
```

```
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
```

```
TCP PAT from inside:10.2.2.2/1429 to any:10.10.10.10/64768 flags ri idle 62:33:57 timeout 0:00:30
```

```
TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri idle 62:33:57 timeout 0:00:30
```

清除10.10.10.10全局IP地址的轉換：

```
<#root>
```

```
Ciscoasa# clear xlate global 10.10.10.10
```

在本示例中，從內部10.2.2.2到外部全局10.10.10.10的轉換已不存在：

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

```
1 in use, 2 most used
```

```
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
```

```
TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri idle 62:33:57 timeout 0:00:30
```

## 系統日誌

系統日誌允許您對ASA上的問題進行故障排除。思科為Windows NT提供了一個名為ASA防火牆系統日誌伺服器(PFSS)的免費系統日誌伺服器。您可以從[思科技術支援和下載](#)下載PFSS。

其他多家廠商（例如Windows 2000和Windows XP）提供適用於各種Windows平台的系統日誌伺服器。預設情況下，多數UNIX和Linux電腦都安裝了Syslog伺服器。


設定系統日誌伺服器時，請配置ASA以向其傳送日誌。

舉例來說：

```
<#root>
```

```
logging on logging host <ip_address_of_syslog_server> logging trap debugging
```

---

 **注意：**此示例將ASA配置為將調試（第7級）和更重要的系統日誌傳送到系統日誌伺服器。由於這些ASA日誌是最詳細的，因此請僅在您對問題進行故障排除時使用。對於正常操作，請將日誌記錄級別配置為「警告」（級別4）或「錯誤」（級別3）。

---

如果遇到效能低的問題，請打開文本檔案中的系統日誌並搜尋與效能問題相關的源IP地址。（如果使用UNIX，則可以grep透過syslog獲取源IP地址。）檢查消息是否表明外部伺服器嘗試訪問TCP埠113上的內部IP地址（用於標識協定或Ident），但ASA拒絕了該資料包。訊息必須類似於以下範例：

```
%ASA-2-106001: Inbound TCP connection denied from 10.64.10.2/35969 to 192.168.110.179/113 flags SYN
```

如果您收到此消息，請向ASA發出service resetinbound命令。ASA不會以靜默方式丟棄資料包；相反，此命令會使ASA立即重置安全策略拒絕的任何入站連線。伺服器不會等候Ident封包逾時其TCP連線，而是會立即收到重設封包。

## SNMP

推薦的企業部署方法是使用SNMP監控思科ASA的效能。Cisco ASA透過SNMP版本1、2c和3支援此功能。

您可以將安全裝置配置為向網路管理伺服器(NMS)傳送陷阱，也可以使用NMS瀏覽安全裝置上的MIB。MIB是定義的集合，安全裝置維護每個定義的值資料庫。有關此項的更多資訊，請參閱[Cisco ASA 5500系列使用CLI 8.4和8.6的配置指南](#)。

Cisco ASA支援的所有MIB均可在ASA MIB支援清單中找到。從此清單中，以下MIB在監控效能時非常有用：

- CISCO-FIREWALL-MIB ----包含可用於故障切換的對象。
- CISCO-PROCESS-MIB ----包含對CPU利用率有用的對象。

- CISCO-MEMORY-POOL-MIB ----包含對記憶體對象有用的對象。

## 反向DNS查詢

如果您遇到ASA的效能低下，請驗證ASA使用的外部地址的授權DNS伺服器中是否有域名系統指標(DNS PTR)記錄（也稱為反向DNS查詢記錄）。這包括全局網路地址轉換(NAT)池中的任何地址（如果介面上過載，則為ASA外部介面）、任何靜態地址和內部地址（如果不使用NAT）。某些應用程式(例如檔案傳輸通訊協定(FTP)和Telnet伺服器)可以使用反向DNS查詢來判斷使用者來自何處以及它是否為有效主機。如果反向DNS查詢無法解析，則當請求超時時，效能會降低。

要確保這些主機的PTR記錄存在，請從您的PC或UNIX電腦上發出nslookup 命令；包括您用於連線到Internet的全局IP地址。

## 範例

<#root>

```
% nslookup 192.168.219.25  
10.219.133.198.in-addr.arpa name = www.cisco.com.
```

您必須收到回覆，其中包含指定給該IP位址之裝置的DNS名稱。如果您沒有收到響應，請聯絡控制您的DNS的人員，以請求為您的每個全局IP地址增加PTR記錄。

## 在介面上溢位

如果您有流量突發，當突發超過NIC和接收環緩衝區上FIFO緩衝區的緩衝容量時，就會發生資料包丟棄。如果為流量控制啟用暫停幀，可以緩解此問題。暫停(XOFF)和XON幀由NIC硬體根據FIFO緩衝區使用情況自動生成。當緩衝區使用量超過高水位標籤時，傳送暫停幀。若要啟用流量控制的暫停(XOFF)訊框，請使用以下命令：

```
<#root>
```

```
hostname(config)#
```

```
interface tengigabitethernet 1/0
```

```
hostname(config-if)#
```

```
flowcontrol send on
```

顯示命令

顯示CPU使用情況

show cpu usage命令用於確定在ASA CPU上放置的流量負載。在流量高峰期、網路激增或攻擊期間，CPU使用率可能會激增。

ASA具有單個CPU來處理各種任務；例如，它處理資料包並將調試消息列印到控制檯。每個進程都有其自己的用途，並且某些進程比其他進程需要更多的CPU時間。加密可能是CPU最密集的一個過程，因此，如果ASA透過加密隧道傳遞大量流量，則必須考慮速度更快的ASA，即專用VPN集中器，例如VPN 3000。VAC從ASA CPU解除安裝加密和解密，並在卡上的硬體中執行。這允許ASA使用3DES（168位加密）加密和解密100 Mbps的流量。

日誌記錄是另一個可能消耗大量系統資源的過程。因此，建議在ASA上停用控制檯、監控和緩衝區日誌記錄。您可以在對問題進行故障排除時啟用這些進程，但可以停用這些進程以進行日常操作，特別是當CPU容量用盡時。此外，還建議將系統日誌或簡單網路管理協定(SNMP)日誌記錄（日誌記錄）設定為第5級（通知）或更低級別。此外，您可以透過no logging message <syslog\_id> 命令停用特定Syslog消息ID。

Cisco Adaptive Security Device Manager (ASDM)還在Monitoring 頁籤上提供一個圖形，透過該圖形可以檢視ASA在一段時間內的CPU使用情況。您可以使用此圖形來確定ASA上的負載。

您可使用 show cpu usage 命令來顯示CPU利用率統計資訊。

範例

<#root>

Ciscoasa#

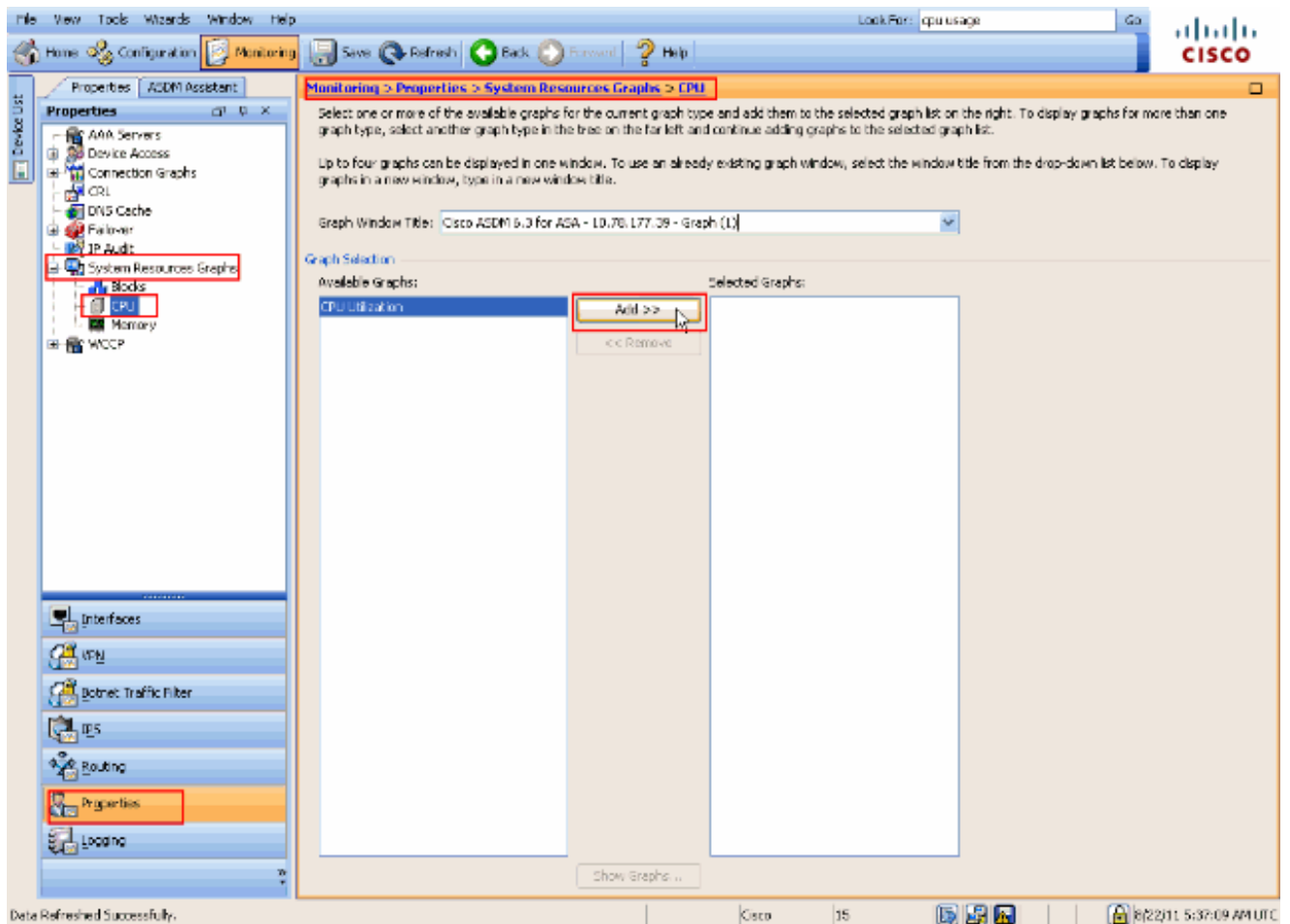
show cpu usage

CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%

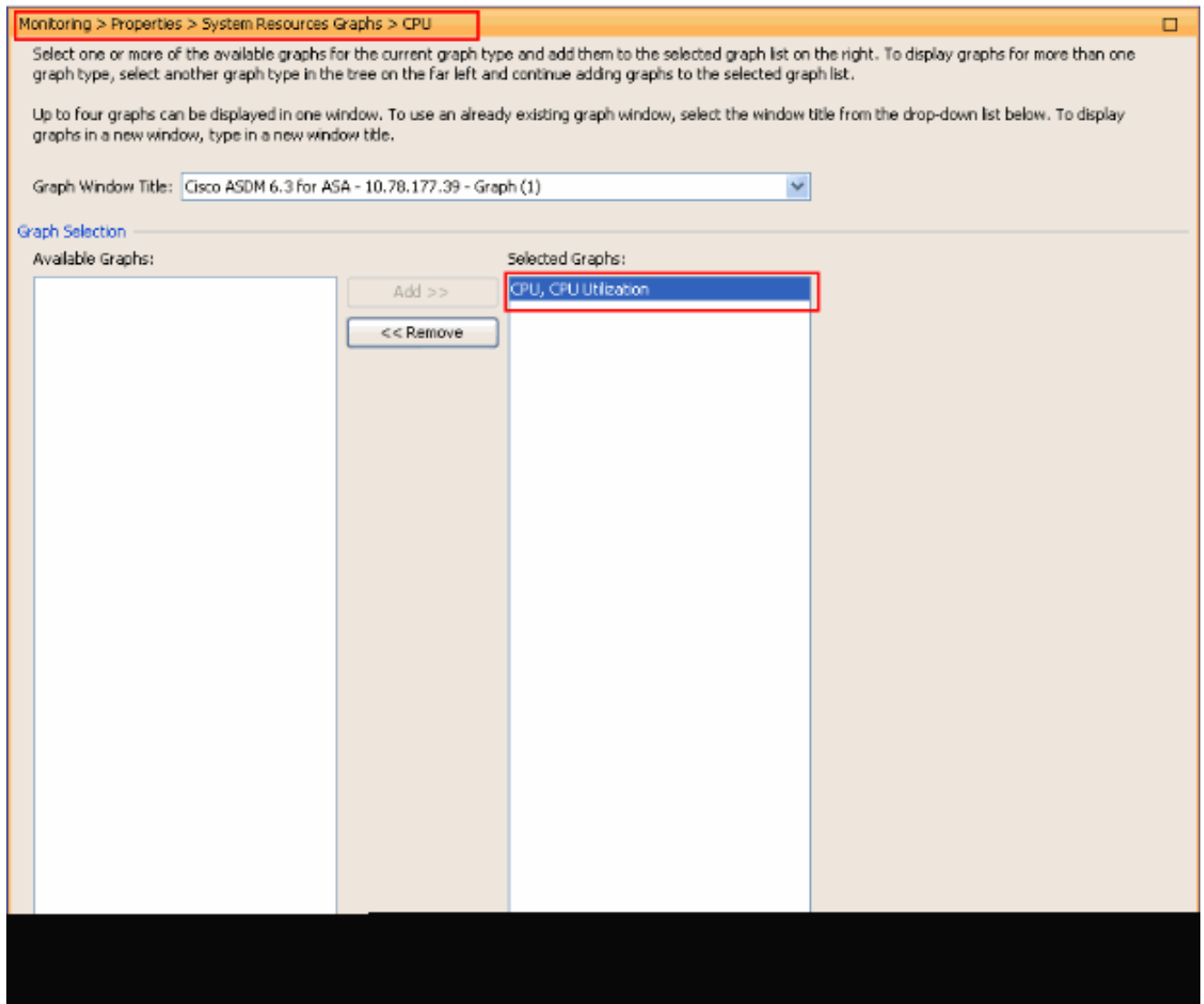
### 檢視ASDM上的CPU使用情況

要檢視ASDM上的CPU使用情況，請完成以下步驟：

- 轉到ASDM中的Monitoring > Properties > System Resources Graphics > CPU 並選擇圖形窗口標題。然後，從可用的圖形清單中選擇所需的圖表並點選增加，如圖所示。

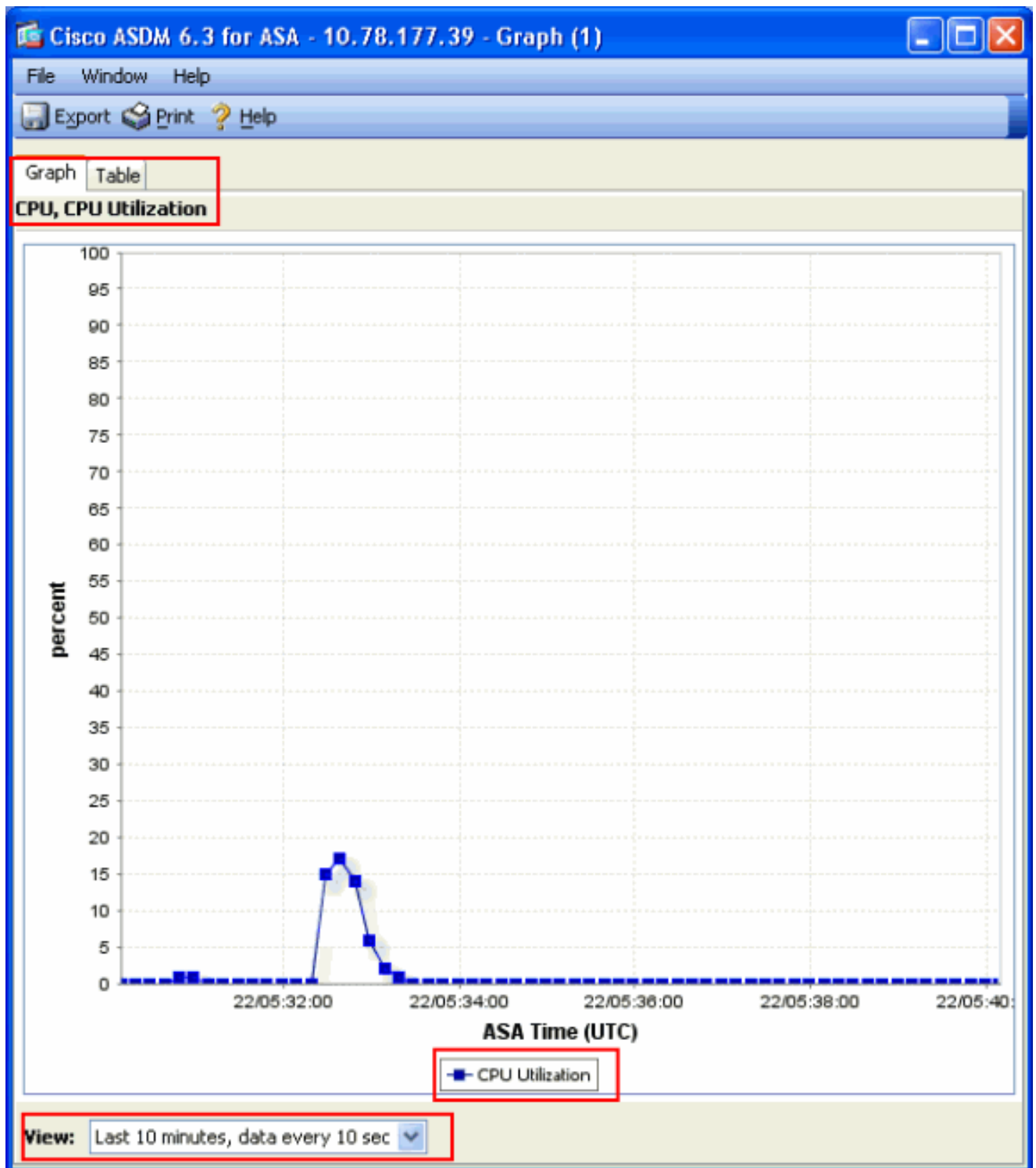


- 在選定圖形部分下增加所需的圖表名稱後，點選顯示圖形。



下一張圖顯示了ASDM上的CPU使用情況圖表。此圖形的不同檢視可供使用，且可在從「檢視」下拉式清單中選取檢視時加以變更。此輸出可根據需要列印或儲存到電腦。





#### 輸出說明

下表說明了 `show cpu usage` 輸出中的欄位。

| 欄位        | 說明                  |
|-----------|---------------------|
| 5秒的CPU使用率 | 過去五秒的CPU使用率         |
| 1分鐘       | 過去一分鐘內平均5秒的CPU使用率樣本 |
| 5分鐘       | 過去五分鐘內CPU使用率平均抽樣為5秒 |

## 顯示流量

show traffic 命令顯示了在給定時間段中有多少流量透過ASA。結果基於自上次發出命令以來的時間間隔。要想得到準確的結果，請先發出 **clear traffic** 命令，然後等待1-10分鐘，再發出show traffic 命令。您也可以發出show traffic命令，等待1-10分鐘，然後再次發出該命令，但是僅第二次命令的輸出有效。

您可使用show traffic命令來確定有多少流量透過ASA。如果您有多個介面，該命令可幫助您確定哪些介面傳送和接收的資料最多。對於具有兩個介面的ASA裝置，外部介面上的入站和出站流量的總和必須等於內部介面上的入站和出站流量的總和。

## 範例

```
<#root>
```

```
Ciscoasa#
```

```
show traffic
```

```
outside: received (in 124.650 secs): 295468 packets 167218253 bytes 2370 pkts/sec 1341502 bytes/sec tr
```

如果您在一個介面上接近或達到額定吞吐量，則需要升級到更快的介面或限制進出該介面的流量。否則可能導致資料包丟失。如 **show interface** 部分所說明的，您可以檢查介面計數器以查詢有關吞吐量的資訊。

## 顯示Perfmon

show perfmon命令用於監控ASA檢查的流量數量和型別。此命令是確定每秒轉換(xlates)和連線(conn)數目的唯一方法。連線進一步細分為TCP和使用者資料包協定(UDP)連線。有關此命令生成的輸出的說明，請參閱輸出說明。

## 範例

```
PERFMON STATS Current Average Xlates 18/s 19/s Connections 75/s 79/s TCP Conns 44/s 49/s UDP Conns 31/s 30/s URL Access 27/s 30/s URL Serve
```

## 輸出說明

下表說明了show perfmon 輸出中的欄位。

| 欄位           | 說明                                 |
|--------------|------------------------------------|
| Xlates       | 每秒建立的翻譯                            |
| 連線           | 每秒建立的連線                            |
| TCP連線        | 每秒TCP連線數                           |
| UDP連線        | 每秒UDP連線數                           |
| URL存取        | 每秒訪問的URL ( 網站 )                    |
| URL伺服器要求     | 每秒傳送到Websense和N2H2的請求(需要filter 命令) |
| TCP修正        | ASA每秒轉發的TCP資料包數                    |
| TCPIntercept | 每秒超過靜態設定之初期限制的SYN封包數目              |

|            |                                         |
|------------|-----------------------------------------|
| HTTP修正     | 每秒傳送到埠80的資料包數量(需要fixup protocol http命令) |
| FTP修正      | 每秒檢查的FTP命令                              |
| AAA Authen | 每秒身份驗證請求數                               |
| AAA作者      | 每秒授權請求                                  |
| AAA帳戶      | 每秒的記帳請求                                 |

#### 顯示區塊

您可以將show cpu usage命令與show blocks命令結合使用來確定ASA是否過載。

#### 封包區塊(1550和16384位元組)

當進入ASA介面時，會將資料包放在輸入介面隊列中，向上傳遞到作業系統，然後放入一個塊中。對於乙太網資料包，使用1550位元組塊；如果資料包在66 MHz Gigabit乙太網卡上進入，則使用16384位元組塊。ASA根據自適應安全演算法(ASA)確定資料包是被允許還是被拒絕，然後處理資料包到出站介面上的輸出隊列。如果ASA無法支援流量負載，則可用的1550位元組塊(或66 MHz GE的16384位元組塊)的數量會保持接近0 (如命令輸出的CNT列所示)。當CNT列達到零時，ASA會嘗試分配更多塊，最大塊數為8192。如果沒有其他可用塊，ASA將丟棄該資料包。

#### 故障切換和系統日誌塊 (256位元組)

256位元組塊主要用於有狀態故障切換消息。活動ASA生成資料包並將其傳送到備用ASA以更新轉換和連線表。在建立或中斷高連線率的突發流量期間，可用的256位元組塊數可以降為0。此丟棄表示一個或多個連線未更新到備用ASA。這通常是可以接受的，因為有狀態故障切換協定下一次會捕獲xlate或丟失的連線。但是，如果256位元組塊的CNT列長時間保持在或接近0，ASA將無法跟上同步的轉換和連線表，因為ASA每秒處理的連線數太多。如果這種情況持續發生，請將ASA升級到更快的型號。

從ASA傳送的系統日誌消息也使用256位元組塊，但通常不會以導致256位元組塊池耗盡的數量釋放。如果CNT列顯示256位元組塊的數量接近0，請確保您不以調試(第7級)登入到系統日誌伺服器。這由ASA配置中的日誌記錄陷阱行指示。建議您將「記錄」設為

「通知」(層級5)或更低層級，除非您需要其他資訊來進行除錯。

## 範例

```
<#root>
```

```
Ciscoasa#
```

```
show blocks
```

```
SIZE MAX LOW CNT 4 1600 1597 1600 80 400 399 400 256 500 495 499 1550 1444 1170 1188 16384 2048 1532 1
```

## 輸出說明

下表說明了show blocks輸出中的列。

| 欄   | 說明                                                                                               |
|-----|--------------------------------------------------------------------------------------------------|
| 大小  | 區塊池的大小(位元組)。每個大小代表一個特定的型別                                                                        |
| 最大  | 指定的位元組區塊集區可用的區塊數目上限。啟動時從記憶體中劃分出最大塊數。通常，最大塊數不會改變。但256和1550位元組塊除外，自適應安全裝置可以在需要時動態建立更多，最多可達8192位元組。 |
| 低   | 低水位標籤。此數字表示自自適應安全裝置通電以來，或者自上次清除塊(使用clear blocks命令)以來，此大小的塊的最低可用數量。LOW列中的零表示記憶體已滿的上一個事件。          |
| CNT | 該特定大小塊池的當前可用塊數。CNT列中的零表示記憶體現在已滿。                                                                 |

下表說明了show blocks輸出中SIZE行的值。

| 大小值   | 說明                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0     | 由dupb塊使用。                                                                                                                                                                                                                                                                                                                                                                                                  |
| 4     | 重複應用程式中現有的區塊，例如DNS、ISAKMP、URL篩選、uauth、TFTP和TCP模組。此外，代碼通常可以使用此大小塊將資料包傳送到驅動程式，以此類推。                                                                                                                                                                                                                                                                                                                          |
| 80    | 在TCP攔截中用於生成確認資料包和用於故障切換hello消息。                                                                                                                                                                                                                                                                                                                                                                            |
| 256   | 用於狀態故障切換更新、系統日誌記錄和其他TCP功能。這些塊主要用於有狀態故障切換消息。活動自適應安全裝置生成資料包並將其傳送到備用自適應安全裝置，以更新轉換和連線表。在突發流量中，高連線率被建立或斷開，可用塊的數量可以降為0。此情況表示一個或多個連線未更新到備用自適應安全裝置。有狀態故障切換協定會在下次捕獲丟失的轉換或連線。如果256位元組塊的CNT列長時間保持為或接近0，則自適應安全裝置會由於每秒處理的連線數而難以保持轉換和連線表的同步。從自適應安全裝置傳送的系統日誌消息也使用256位元組塊，但通常不會釋放這些數量以導致256位元組塊池耗盡。如果CNT列顯示256位元組塊的數量接近0，請確保您未在Debugging (第7級) 登入到系統日誌伺服器。這由自適應安全裝置配置中的日誌記錄陷阱行指示。除非您需要其他除錯資訊，否則我們建議您將「記錄」設為「通知」(層級5)或更低層級。 |
| 1550  | 用於儲存乙太網資料包，以便透過自適應安全裝置進行處理。當資料包進入自適應安全裝置介面時，它將被置於輸入介面隊列中，傳遞到作業系統，然後被置於一個塊中。自適應安全裝置根據安全策略確定資料包必須被允許還是被拒絕，並處理資料包到出站介面上的輸出隊列。如果自適應安全裝置難以跟上流量負載，可用塊的數量可以停留在接近0(如命令輸出的CNT列所示)。當CNT列為零時，自適應安全裝置會嘗試分配更多塊，最大塊數為8192。如果沒有其他可用塊，自適應安全裝置將丟棄該資料包。                                                                                                                                                                      |
| 16384 | 僅用於64位66 MHz千兆乙太網卡(i82543)。有關乙太網資料包的詳細資訊，請參閱1550的說明。                                                                                                                                                                                                                                                                                                                                                       |
| 2048  | 用於控制項更新的控制項或引導式影格。                                                                                                                                                                                                                                                                                                                                                                                         |

#### 顯示記憶體

show memory命令顯示了ASA的實體記憶體(或RAM)總量(或RAM)，以及當前可用位元組數。要使用此資訊，您必須首先瞭解ASA如何使用記憶體。當ASA啟動時，它將作業系統從快閃記憶體複製到RAM中，然後從RAM運行作業系統(就像路由器一樣)。

接下來，ASA從快閃記憶體複製啟動配置並將其放入RAM中。最後，ASA會分配RAM以建立show blocks部分所介紹的塊池。分配完成後，僅當配置增加時，ASA才需要額外的RAM。此外，ASA會將轉換和連線條目儲存在RAM中。

在正常運行期間，ASA上的空間記憶體必須更改得很少（如果有的話）。通常，只有當您受到攻擊且成千上萬個連線透過ASA時，您才需要運行記憶體不足的情況。為了檢查連線，請發出show conn count 命令，會顯示透過ASA的當前和最大連線數。如果ASA記憶體耗盡，它最終會崩潰。在崩潰之前，您可以在系統日誌(%ASA-3-211001)中看到記憶體分配失敗消息。

如果您由於受到攻擊而導致記憶體耗盡，請與[Cisco技術支援](#)團隊聯絡。

## 範例

```
<#root>
```

```
Ciscoasa#
```


```
show memory
```

```
Free memory: 845044716 bytes (79%) Used memory: 228697108 bytes (21%) ----- T
```

## 顯示Xlate

show xlate count命令顯示了透過ASA的當前和最大轉換數。轉換是內部地址到外部地址的對映，可以是一對一的對映，如網路地址轉換(NAT)，也可以是多對一的對映，如埠地址轉換(PAT)。此命令是show xlate命令的子集，會輸出透過ASA的每個轉換。命令輸出顯示轉換「使用中」，這是指發出該命令時ASA中的活動轉換數量；「最常用」是指自ASA通電以來，在ASA上見過的最大轉換數量。

---

 **注意：**單個主機可以有到多個到不同目標的連線，但只能有一個轉換。如果xlate計數遠遠大於內部網路上的主機數量，則可能是您的內部主機之一受到威脅。如果您的內部主機受到威脅，它會偽裝源地址並將資料包從ASA傳送出去。

---

---

 **注意：**當啟用vpncient配置，且內部主機發出DNS請求時，show xlate命令可以列出一個靜態轉換的多個xlate。

---

## 範例

```
<#root>
```

```
Ciscoasa#
```

```
show xlate count
```

```
84 in use, 218 most used
```

```
<#root>
```

```
Ciscoasa(config)#
```

```
show xlate
```

```
3 in use, 3 most used Flags: D - DNS, d - dump, I - identity, i - inside, n - no random, o - outside,  
TCP PAT from inside:10.1.1.15/1026 to outside:192.168.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30
```

```
UDP PAT from 10.1.1.15/1028 to outside:192.168.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30
```

```
ICMP PAT from inside:10.1.1.15/21505 to outside:192.168.49.1/0 flags ri idle 62:33:57 timeout 0:00:30
```

第一個條目是內部網路上主機埠(10.1.1.15、1026)到外部網路上的主機埠(192.168.49.1、1024)的TCP埠地址轉換。「r」標誌表示該轉換是埠地址轉換。「i」標誌表示該轉換適用於內部地址埠。

第二個條目是內部網路上的主機埠(10.1.1.15、1028)到外部網路上的主機埠(192.168.49.1、1024)的UDP埠地址轉換。「r」標誌表示該轉換是埠地址轉換。「i」標誌表示該轉換適用於內部地址埠。

第三個條目是內部網路上主機ICMP-id (10.1.1.15 , 21505)到外部網路上的主機ICMP-id (192.168.49.1 , 0)的ICMP埠地址轉換。「r」標誌表示該轉換是埠地址轉換。「i」標誌表示該轉換適用於內部地址-ICMP-id。

內部地址欄位顯示為資料包上的源地址，這些資料包是從較安全的介面傳輸到較不安全的介面。相反，在從安全性較低的介面傳輸到安全性較高的介面的資料包上，它們顯示為目標地址。



## 顯示連線埠計數

show conn count命令顯示了透過ASA的當前和最大連線數。連線是第4層資訊從內部地址到外部地址的對映。當ASA收到TCP會話的SYN資料包或UDP會話中的第一個資料包到達時，連線就會建立。當ASA收到最後一個ACK資料包時，連線將斷開，這發生在TCP會話握手關閉或UDP會話超時到期時。

極高的連線計數 ( 50-100倍於正常值 ) 表明您正遭受攻擊。發出show memory命令以確保較高的連線計數不會導致ASA記憶體耗盡。如果您受到攻擊，可以限制每個靜態條目的最大連線數，也可以限制初期連線的最大數量。此動作可保護您的內部伺服器，避免伺服器不堪重負。有關詳細資訊，請參閱[使用CLI 8.4和8.6的Cisco ASA 5500系列配置指南](#)。

## 範例

```
<#root>
```

```
Ciscoasa#
```

```
show conn count
```

```
2289 in use, 44729 most used
```

## 顯示介面

[show interface](#)命令可幫助您確定雙工不匹配問題以及電纜問題。它還可以提供有關介面是否超負荷的進一步資訊。如果ASA耗盡CPU容量，則1550位元組塊的數量會保持接近0。(請檢視66 MHz Gig卡上的16384位元組塊。) 另一個指標是介面上的「無緩衝區」增加。no buffers消息表明介面無法將資料包傳送到ASA OS，因為沒有資料包可用的塊，並且資料包被丟棄。如果no buffer的計數經常增加，請發出show proc cpu命令以檢查ASA上的CPU使用情況。如果CPU使用率因流量負載繁重而較高，請升級到能夠處理負載的更強大的ASA。

當資料包首次進入介面時，它會被放入輸入硬體隊列中。如果輸入硬體佇列已滿，封包會放在輸入軟體佇列中。封包會從其輸入佇列傳遞並置於1550位元組的區塊中(或66 MHz千兆位元組乙太網路介面上的16384位元組區塊中)。然後，ASA確定資料包的輸出介面，並將資料包放入相應的硬體隊列中。如果硬體隊列已滿，則資料包將被放入輸出軟體隊列中。如果任一軟體隊列中的最大塊數較大，則介面會溢位。例如，如果200 Mbps進入ASA並且都從單個100 Mbps介面輸出，則輸出軟體隊列會指示出站介面上的數字過高

, 這表示該介面無法處理流量。如果遇到這種情況, 請升級到更快的介面。

## 範例

```
<#root>
```

```
Ciscoasa#
```

```
show interface
```

```
Interface GigabitEthernet0/1 "inside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000
```

還必須檢查介面是否存在錯誤。如果您收到殘幀、輸入錯誤、CRC或幀錯誤, 則可能是雙工不匹配。電纜也可能有故障。有關雙工問題的詳細資訊, 請參閱[速度和雙工設定](#)。請記住, 每個錯誤計數器都代表由於該特定錯誤而被丟棄的資料包數量。如果您看到定期增加的特定計數器, 則ASA上的效能最有可能受損, 您必須找到問題的根本原因。


當您檢查介面計數器時, 請注意, 如果介面設定為全雙工, 您一定不會遇到任何衝突、延遲衝突或延遲資料包。反之, 如果介面設定為半雙工, 則您必須接收衝突、某些延遲衝突以及某些延遲封包。衝突、延遲衝突和延遲資料包的總數不得超過輸入和輸出資料包計數器總和的10%。如果您的衝突超過總流量的10%, 則表示鏈路使用過度, 您必須升級到全雙工或更快的速度 ( 10 Mbps到100 Mbps )。請記住, 10%的衝突意味著ASA丟棄透過該介面的資料包的10%; 必須重新傳輸這些資料包中的每一個資料包。

有關介面計數器的詳細資訊, 請參閱[Cisco ASA 5500系列自適應安全裝置命令參考](#)中的interface 命令。

## 顯示進程

ASA上的show processes命令顯示了執行此命令時在ASA上運行的所有活動進程。要確定哪些進程接收了過多的CPU時間, 哪些進程未接收任何CPU時間, 此資訊非常有用。為了獲得此資訊, 請發出 show processes 命令兩次; 每個例項之間等待約1分鐘。對於所討論的流程, 從第一個輸出中顯示的「運行時」值中減去第二個輸出中顯示的「運行時」值。此結果顯示在該時間間隔內, 進程接收的CPU時間 ( 以毫秒為單位 )。請注意, 某些處理作業已排定在特定間隔執行, 而某些處理作業只有在有資訊要處理時才會執行。577poll程式最有可能在所有程式中具有最大的執行階段值。這是正常現象, 因為577poll進程輪詢乙太網介面以檢視它們是否有任何需要處理的資料。

---

 **注意：**對每個ASA進程的檢查不在本文檔的討論範圍之內，但為了完整起見，稍作說明。有關ASA進程的詳細資訊，請參閱 [ASA 8.3及更高版本：監控和排除效能問題](#)。

---

## 命令摘要

總之，請使用show cpu usage命令來辨識ASA承受的負載。請記住，輸出是運行平均值；ASA的CPU使用率峰值可能會更高，但會被運行平均值掩蓋。一旦ASA達到80%的CPU使用率，透過ASA的延遲將緩慢增加到約90%的CPU。當CPU使用率超過90%時，ASA開始丟棄資料包。

如果CPU使用率較高，請使用show processes 命令確定佔用最多CPU時間的進程。使用此資訊可以減少密集型進程（如日誌記錄）所消耗的一些時間。

如果CPU使用率並不是很高，但是您發現資料包仍然被丟棄，請使用show interface命令來檢查ASA介面上是否沒有緩衝區以及ASA介面上是否存在衝突（這兩個問題很可能由雙工不匹配而造成）。如果無緩衝區計數增加，但CPU使用率並不低，則介面無法支援流經該介面的流量。

如果緩衝區正常，請檢查區塊。在1550位元組塊上(66 MHz Gig卡為16384位元組塊)，如果show blocks輸出中的當前CNT列接近於0，則ASA最有可能由於過於繁忙而丟棄乙太網資料包。這種情況下，CPU會達到峰值。

如果在建立透過ASA的新連線時遇到問題，請使用show conn count命令來檢查透過ASA的當前連線計數。

如果當前計數很高，請檢查show memory輸出來確保ASA不會耗盡記憶體。如果記憶體較低，請使用show conn 或 show local-host命令來檢查連線源以驗證您的網路是否遭到拒絕服務攻擊。

您可以使用其他命令來測量透過ASA的流量量。show traffic 命令顯示了匯聚資料包和每介面位元組，並且show perfmon會將流量分成不同型別的ASA檢查。

## 相關資訊

- [Cisco ASA 5500-X系列防火牆](#)
- [思科技術支援與下載](#)

## 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）。