確定SWA中的解密速率

目錄

簡介

本文檔介紹計算安全網路裝置(SWA)（以前稱為WSA）中解密流量的百分比的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 已安裝物理或虛擬安全網路裝置(SWA)。
- 許可證已啟用或已安裝。
- 安全殼層(SSH)使用者端。
- 安裝精靈已完成。
- 對SWA的管理訪問。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。

解密效能影響

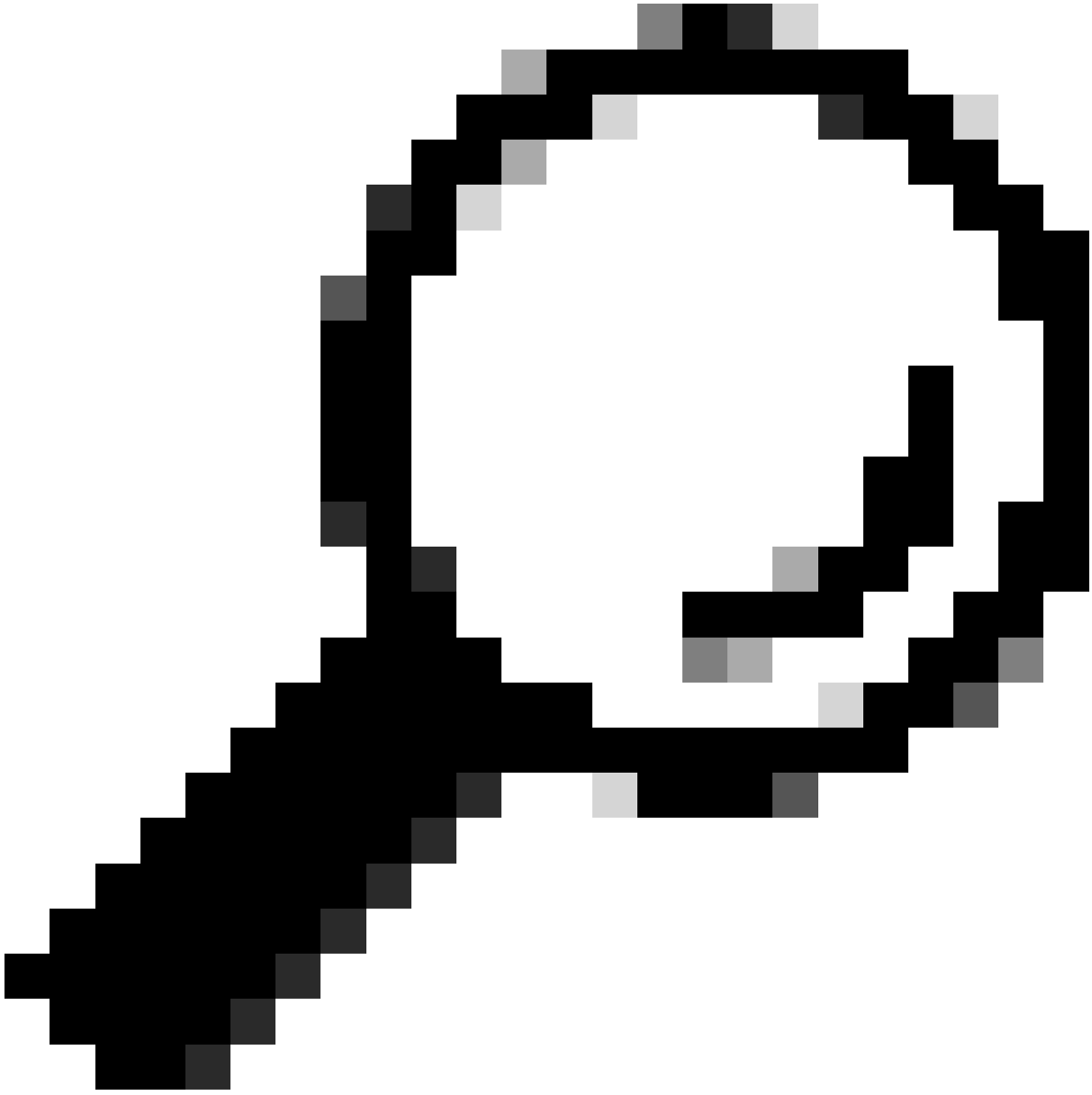
在SWA執行的所有服務中，從效能角度來看，超文本傳輸協定安全(HTTPS)流量的評估最為重要。

解密流量的百分比對裝置的大小有直接影響。管理員可以依靠至少75%的Web流量進行HTTPS。

在初始安裝之後，必須確定解密流量的百分比，以確保準確設定未來成長的預期。部署後，必須每季度檢查一次此數字。

如果解密率大於30%且SWA存在效能問題，建議執行以下操作之一：

- 移除解密策略中各種類別或受信任URL（例如Microsoft Update或Antivirus Updates）的解密
- 跨多個SWA進行負載平衡，以分配負載



提示：有關如何繞過SWA中解密的詳細資訊，請訪問：https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/214746-how-to-exempt-office-365-traffic-from-au.html

---

計算解密百分比的步驟

要查詢與所有HTTPS流量相比解密的HTTPS流量的百分比，請從SWA檔案傳輸協定(FTP)複製access_logs。

可以使用簡單的Bash或PowerShell命令來獲取此數字。以下是針對每個環境描述的步驟：

1. 查詢HTTPS連線總數（顯式和透明）：

```
Bash:
grep -cE 'tunnel://|TCP_CONNECT' aclog.current

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT').length
```

2. 查詢已解密HTTPS連線的數量：

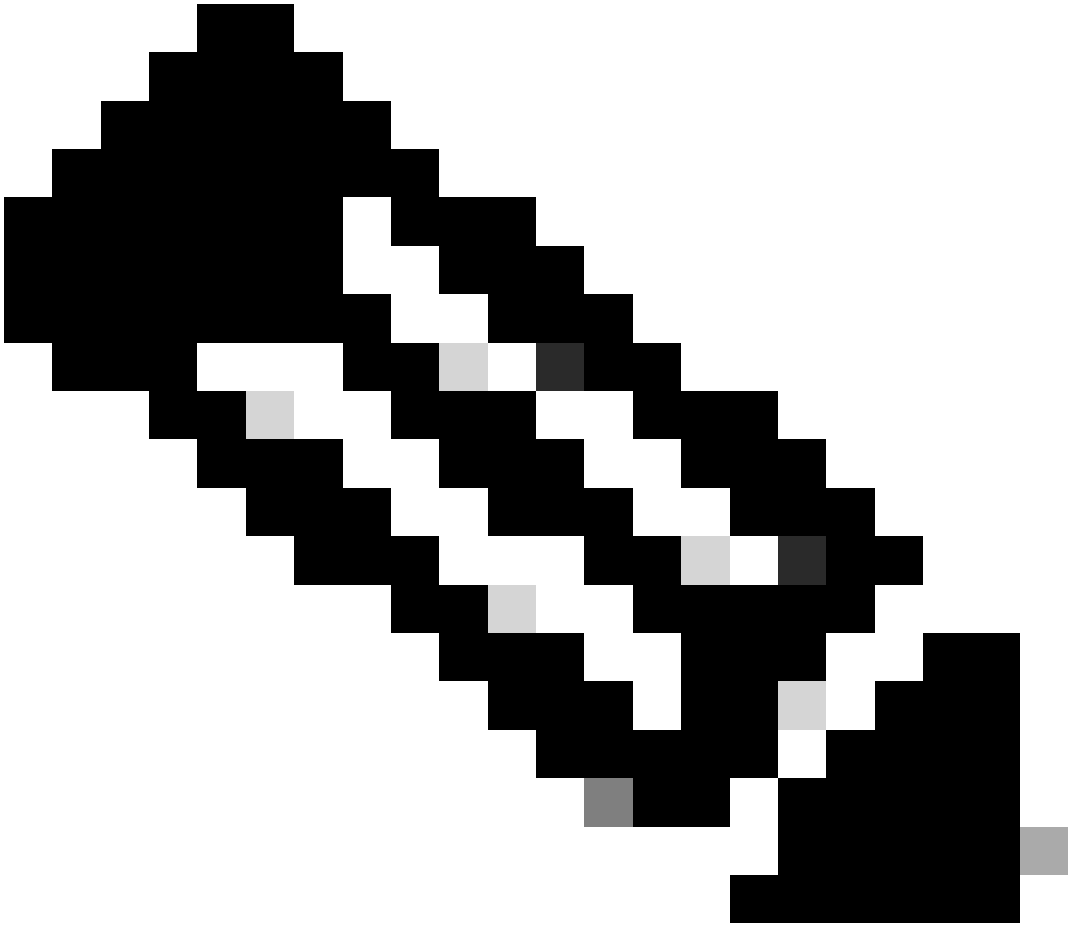
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT'| Select-String -Pattern 'DE
```

3. 將第二個值除以第一個值，再乘以100。

來自CLI的總體流量統計資訊

您可以使用accessloganalyzer命令在CLI中檢視流量統計資訊，該命令可以為您的報告選擇時間範圍或過去N小時。



注意：命令的執行時間取決於所選的時間段。

```
SWA_CLI> accessloganalyzer

Choose the option to define the time range:
- HOURS - Last N hours.
- RANGE - Time range with start and end specified in  MM/DD/YYYY HH:MM:SS format.
[]> HOURS

Analyze logs upto N hours old (oldest on this WSA is N = 312 hours). Enter N:
[]> 10

The log processing might take more than 15 secs. Do you want to continue: (Yes/No)
[No]> yes


-------------------------------------------------------------------------------------------------
                                       HTTP                HTTPS               Cumulative
---------------------------------------- ------------------- ------------------- --------------------
Num transactions                       1512509             4170261             5682770
```

Transaction/sec	42	115	157
Bandwidth (Mbps)	0.0001	0.0004	0.0003
Max Resp time (ms)	643269	285036670	285036670
Average Resp time(ms)	95663	141715	129458
Max Object size (KB)	92246	1215832	1215832
Avg Object size (Total Trans)(KB)	5	54	41
Avg Object size (Allowed Trans) (KB)	20	67	62
Methods			
GET	1295658	0	1295658
POST	34968	0	34968
CONNECT	0	4170261	4170261
Others	181883	0	181883
Status Codes			
1xx	0	0	0
2xx	319799	3351382	3671181
3xx	75011	0	75011
4xx	11697	115467	127164
5xx	1105999	703412	1809411

相關資訊

AsyncOSAsyncOS或Cisco Cisco Cisco Web裝置- LD使用手冊（LimLDed部署）-思科

UCiscoure Web裝置最佳實踐-思科

HCisco免除Office 365流量在Cisco WCiscocurity裝置(WSA)上進行身份驗證和解密- WSAco

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）。