Determinazione della velocità di decrittografia in SWA

Sommario

Introduzione

In questo documento viene descritto come calcolare la percentuale di traffico decrittografato in Secure Web Appliance (SWA), precedentemente noto come WSA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Installazione di Physical o Virtual Secure Web Appliance (SWA) completata.
- Licenza attivata o installata.
- Client Secure Shell (SSH).
- Installazione guidata completata.
- Accesso amministrativo all'SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Impatto sulle prestazioni della decrittografia

Tra tutti i servizi forniti dall'SWA, la valutazione del traffico HTTPS (Hypertext Transfer Protocol

Secure) è la più importante dal punto di vista delle prestazioni.

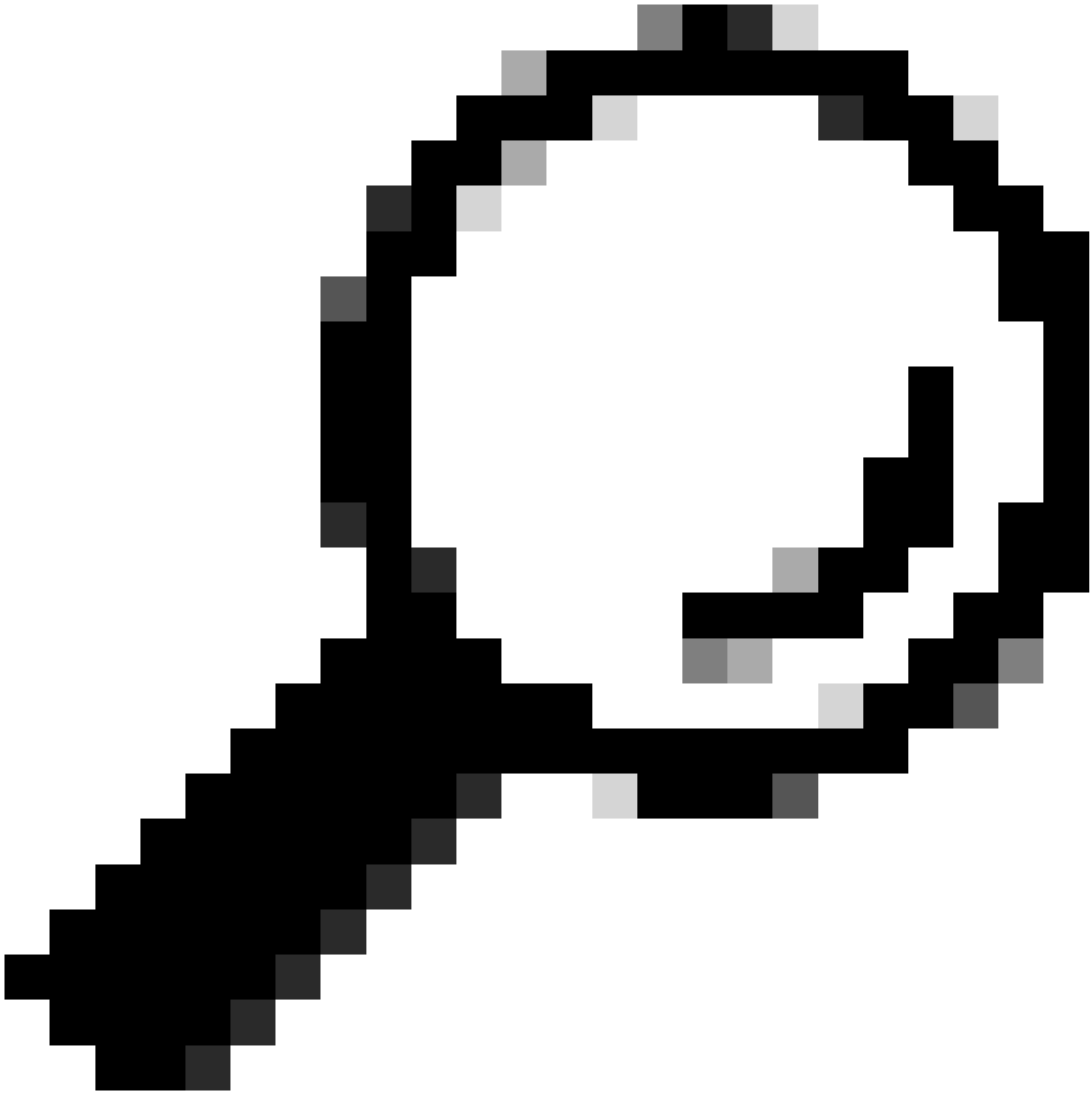
La percentuale di traffico decrittografato influisce direttamente sulle dimensioni dell'accessorio. Un amministratore può contare su almeno il 75% del traffico Web come HTTPS.

Dopo l'installazione iniziale, è necessario determinare la percentuale di traffico decriptato per garantire che le aspettative di crescita futura siano impostate correttamente. Dopo la distribuzione, questo numero deve essere controllato una volta a trimestre.

Se la velocità di decrittografia è superiore al 30% e lo SWA presenta problemi di prestazioni, si consiglia di:

- Rimuovere la decrittografia in varie categorie o URL attendibili (ad esempio Microsoft Update o Aggiornamenti antivirus) nei criteri di decrittografia
- Bilanciamento del carico tra più SWA per distribuire il carico

---



Suggerimento: per ulteriori informazioni su come evitare la decrittografia in SWA, visitare: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/214746-how-to-exempt-office-365-traffic-from-au.html

Passaggi Per Calcolare La Percentuale Di Decrittografia

Per trovare la percentuale di traffico HTTPS decrittografato rispetto a tutto il traffico HTTPS, copiare access_logs dal protocollo FTP (SWA File Transfer Protocol).

Per ottenere questo numero è possibile utilizzare i comandi Simple Bash o PowerShell. Di seguito sono riportati i passaggi descritti per ogni ambiente:

1. Trovare il numero totale di connessioni HTTPS (sia esplicite che trasparenti):

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

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

2. Trovare il numero di connessioni HTTPS decrittografate:

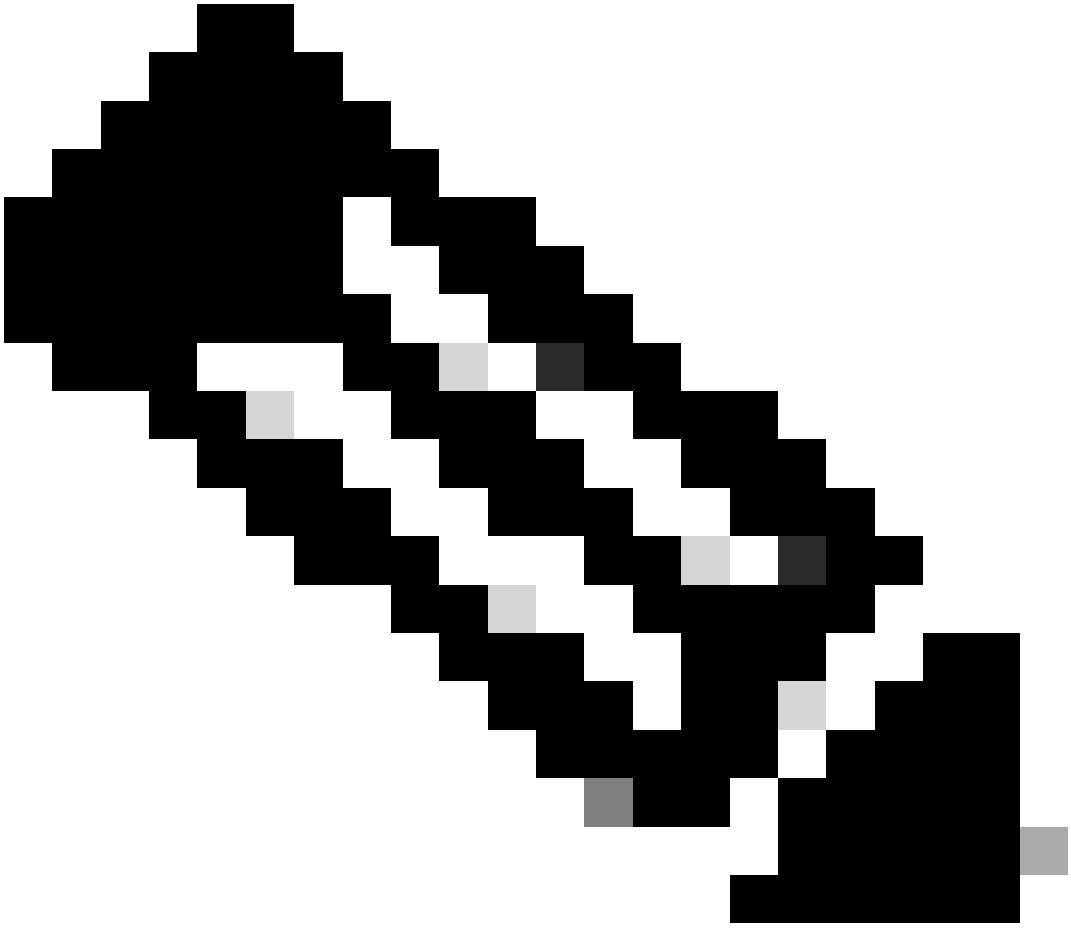
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

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

3. Dividere il secondo valore per il primo e moltiplicarlo per 100.

Statistiche globali del traffico dalla CLI

È possibile visualizzare le statistiche del traffico nella CLI, con il comando accessloganalyzer che consente di scegliere l'intervallo di tempo o le ultime N ore per il report.



Nota: il tempo di esecuzione del comando dipende dal periodo di tempo selezionato.

```
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
-------------------------------------------------------------------------------------------------------
```

Informazioni correlate

Guida per l'utente di AsyncOSAsyncOS o Cisco SCisco Web Appliance - LD (LimLDed Deployment) - Cisco

Best practice per UCiscoure Web Appliance - Cisco

Traffico di Office 365 esente da autenticazione e decrittografia per Cisco WSA (Cisco WCiscourity Appliance) - WSAco

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).