Bepaal de decryptie in SWA

Inhoud

Inleiding

Dit document beschrijft stappen om het percentage gedecrypteerd verkeer in Secure Web Applicatie (SWA) te berekenen dat voorheen bekend stond als WSA.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Physical of Virtual Secure Web Applicatie (SWA) geïnstalleerd.
- Licentie geactiveerd of geïnstalleerd.
- Secure Shell-client (SSH).
- De setup-wizard is voltooid.
- Administratieve toegang tot de SWA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Effect op decryptie-prestaties

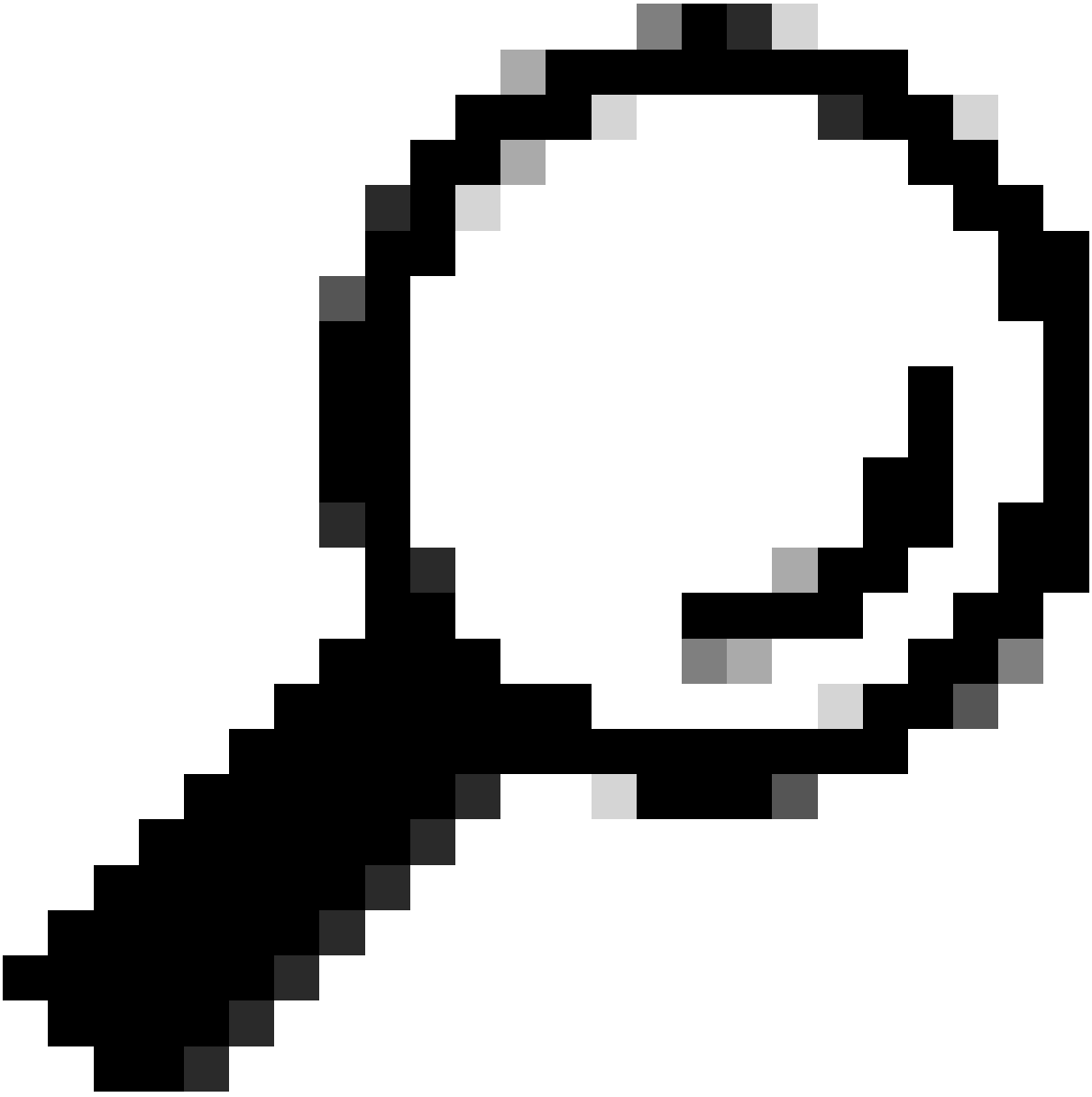
Van alle door de SWA uitgevoerde diensten is de evaluatie van HTTPS-verkeer (Hypertext Transfer Protocol Secure) het meest significant vanuit prestatieoogpunt.

Het percentage ontsleuteld verkeer heeft een directe invloed op de grootte van het apparaat. Een beheerder kan rekenen op ten minste 75% van het webverkeer als HTTPS.

Na de eerste installatie moet het percentage gedecrypteerd verkeer worden bepaald om er zeker van te zijn dat de verwachtingen voor de toekomstige groei nauwkeurig zijn ingesteld. Na plaatsing, moet dit aantal eens per kwartaal worden gecontroleerd.

Als de decryptie meer dan 30% is en SWA prestatiekwestie heeft, wordt geadviseerd om:

- Verwijder decryptie op diverse categorieën of vertrouwde URL's (zoals Microsoft Update of Antivirus Updates) in het decryptie beleid
- Taakverdeling over meer SWA's om de lading te verdelen



Tip: Voor meer informatie over het omzeilen van decryptie in SWA, bezoek: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/214746-how-

---

to-exempt-office-365-traffic-from-au.html

Stappen om het decryptie percentage te berekenen

Om het percentage HTTPS-verkeer te vinden dat in vergelijking met al het HTTPS-verkeer wordt gedecodeerd, kopieert u de access_logs van het SWA File Transfer Protocol (FTP).

U kunt eenvoudige Bash- of PowerShell-opdrachten gebruiken om dit nummer te verkrijgen. Hier zijn de stappen die voor elke omgeving worden beschreven:

1. Vind het aantal totale HTTPS-verbindingen (zowel expliciet als transparant):

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

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

2. Vind het aantal gedecrypteerde HTTPS-verbindingen:

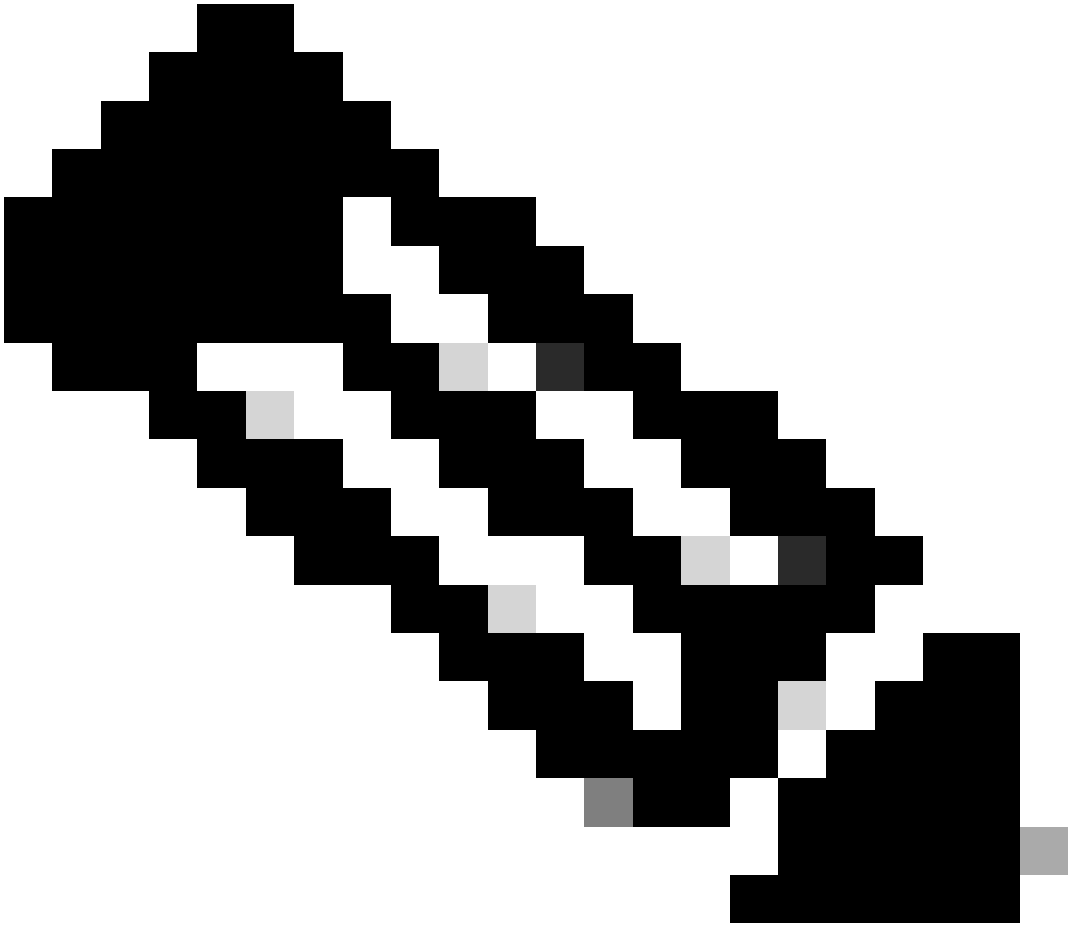
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

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

3. Verdeel de tweede waarde door de eerste waarde en vermenigvuldig met 100.

Algemene verkeersstatistieken van CLI

U kunt de verkeersstats in CLI bekijken, met de opdracht acceslogana lyzer die u kunt kiezen voor tijdbereik of de afgelopen N uur, voor uw rapport.



Opmerking: de uitvoertijd van de opdracht is afhankelijk van de geselecteerde tijdsperiode.

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

Gerelateerde informatie

Gebruikershandleiding voor AsyncOSAsyncOS voor Cisco SCisco Web Appliance - LD (LimLDed Implementation) - Cisco

Best practices voor UCS Web Applicatie - Cisco

Cisco Vrijgestelde Office 365 Traffic From Verification en Decryptie op Cisco WICiscocurity-applicatie (WSA) - WSAco

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.