Déterminer le taux de déchiffrement dans SWA

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Impact sur les performances de déchiffrement

Étapes De Calcul Du Pourcentage De Déchiffrement

- Statistiques de trafic globales à partir de CLI

Introduction

Ce document décrit les étapes pour calculer le pourcentage de trafic déchiffré dans l'appliance Web sécurisé (SWA) anciennement connu sous le nom de WSA.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appareil Web sécurisé physique ou virtuel (SWA) installé.
- Licence activée ou installée.
- Client Secure Shell (SSH).
- L'Assistant de configuration est terminé.
- Accès administratif au SWA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Impact sur les performances de déchiffrement

De tous les services fournis par le SWA, l'évaluation du trafic HTTPS (Hypertext Transfer Protocol Secure) est la plus importante du point de vue des performances.

Le pourcentage de trafic décrypté a un impact direct sur la manière dont l'appliance doit être

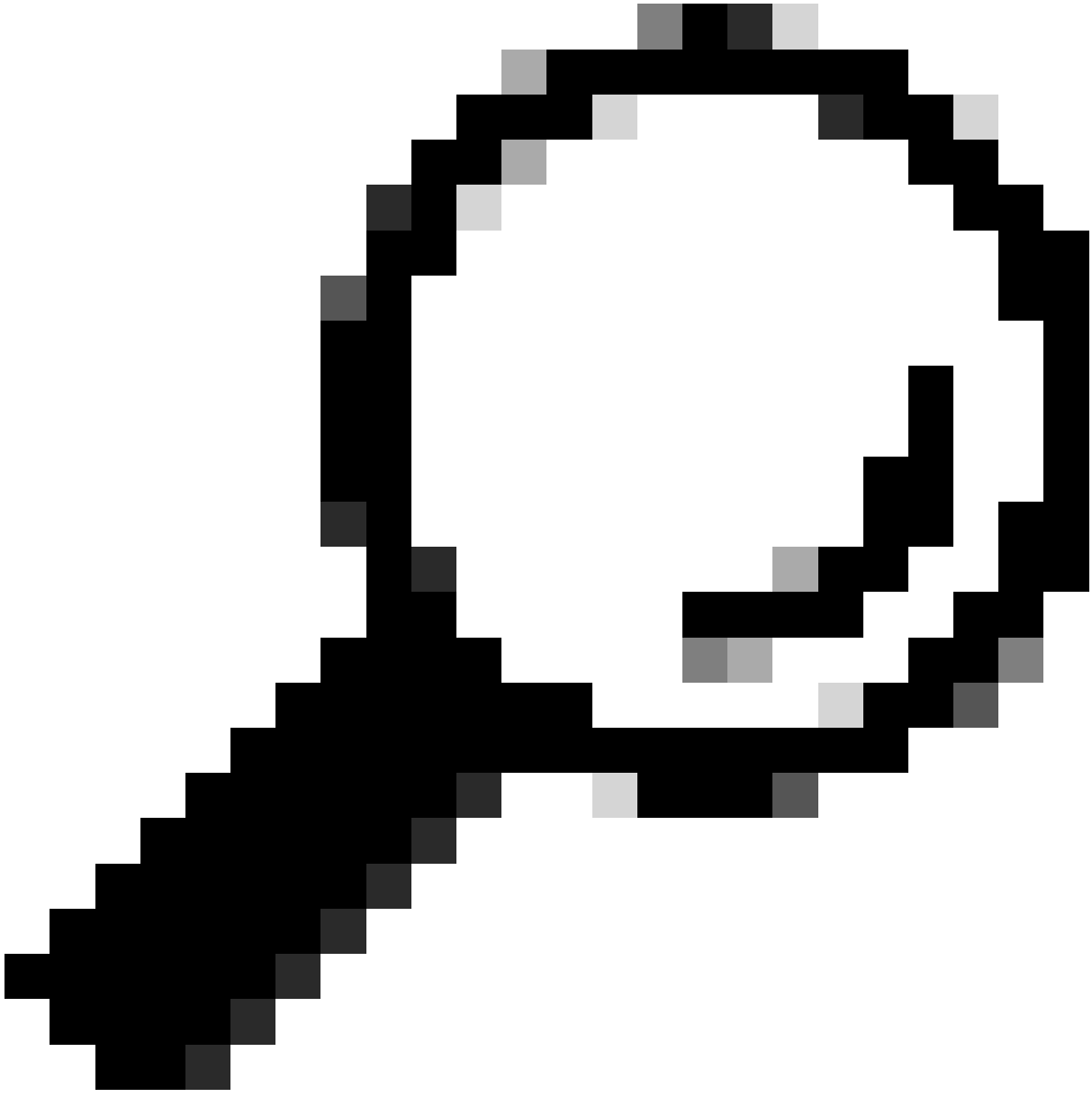
dimensionnée. Un administrateur peut compter sur au moins 75 % du trafic Web pour être HTTPS.

Après l'installation initiale, le pourcentage de trafic décrypté doit être déterminé afin de garantir que les prévisions de croissance future sont définies avec précision. Après le déploiement, ce nombre doit être vérifié une fois par trimestre.

Si le taux de décryptage est supérieur à 30 % et que SWA présente des problèmes de performances, il est conseillé de :

- Supprimez le déchiffrement sur diverses catégories ou URL approuvées (telles que Microsoft Update ou les mises à jour antivirus) dans les stratégies de déchiffrement
- Équilibrage de la charge sur plusieurs SWA pour répartir la charge

---



Conseil : pour plus d'informations sur la façon de contourner le déchiffrement dans SWA,

---

rendez-vous sur : https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/214746-how-to-exempt-office-365-traffic-from-au.html

Étapes De Calcul Du Pourcentage De Déchiffrement

Pour connaître le pourcentage de trafic HTTPS déchiffré par rapport à l'ensemble du trafic HTTPS, copiez access_logs à partir du protocole FTP (File Transfer Protocol) SWA.

Les commandes Simple Bash ou PowerShell peuvent être utilisées pour obtenir ce numéro. Voici les étapes décrites pour chaque environnement :

1. Recherchez le nombre total de connexions HTTPS (explicites et transparentes) :

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

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

2. Recherchez le nombre de connexions HTTPS déchiffrées :

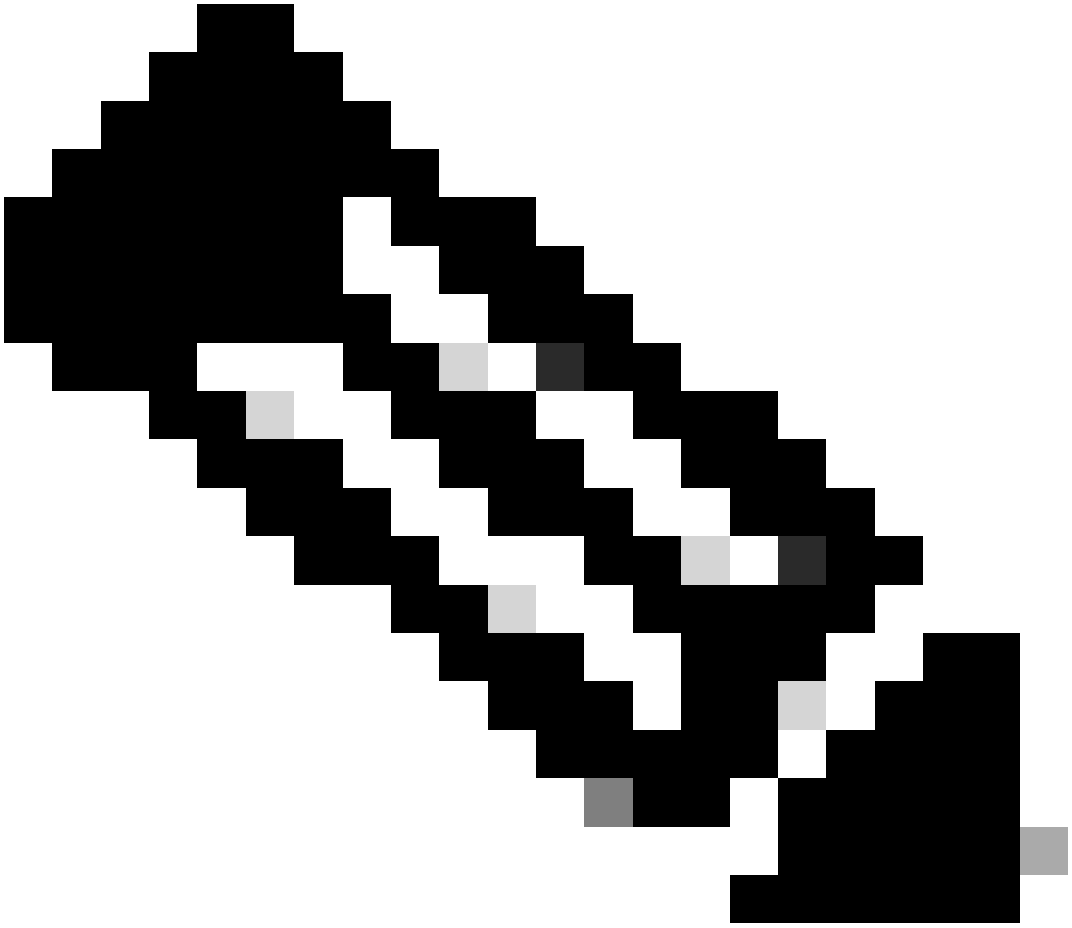
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

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

3. Divisez la deuxième valeur par la première valeur et multipliez par 100.

Statistiques de trafic globales à partir de CLI

Vous pouvez afficher les statistiques du trafic dans l'interface de ligne de commande, avec la commande accessloganalyzer qui vous permet de choisir une plage de temps ou les N heures passées, pour votre rapport.



Remarque : le temps d'exécution de la commande dépend de la période sélectionnée.

```
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

Informations connexes

Guide de l'utilisateur pour AsyncOSAsyncOS ou Cisco SCisco Web Appliance - LD (LimLDed Deployment) - Cisco

Meilleures pratiques des appliances Web Cisco UCiscocure - Cisco

Le trafic Cisco Office 365 est exempté de l'authentification et du déchiffrement sur Cisco WSA - WSAco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.