Comprendre le format de journal d'accès HTTPS dans l'appliance Web sécurisée

Table des matières

Introduction

Ce document décrit les journaux d'accès SWA (Secure Web Appliance) pour le trafic HTTPS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- SWA physique ou virtuel 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.

Informations générales

Les journaux de trafic HTTPS Cisco SWA dans les journaux d'accès sont différents du trafic HTTP normal.

Remarque : Les journaux dépendent du mode de déploiement du proxy. En mode de transfert explicite ou transparent, les journaux sont différés.

Mots clés dans les journaux d'accès

Voici quelques mots clés importants que vous pouvez voir dans les journaux d'accès :

TCP_CONNECT : Ceci montre que le trafic a été reçu de manière transparente (via WCCP, la redirection L4 ou d'autres méthodes de redirection transparentes)
CONNEXION : Ceci montre que le trafic a été reçu explicitement.
DECRYPT_WBRS : Indique que SWA a déchiffré le trafic en raison du score WBRS (Web Reputation Score).
PASSTHRU_WBRS : Ceci montre que SWA a un Passthrough du trafic en raison du score WBRS.
DROP_WBRS : Ceci montre que SWA a abandonné le trafic en raison du score WBRS

Journaux HTTPS dans les journaux d'accès

Lorsque le trafic HTTPS est décrypté, WSA consigne deux entrées.

- TCP_CONNECT tunnel:// ou CONNECT tunnel:// dépend du type de requête reçue, ce qui signifie que le trafic est chiffré (n'a pas encore été déchiffré).
- GET https:// a affiché l'URL déchiffrée.

Remarque : L'URL complète en mode transparent n'est visible que si SWA déchiffre le trafic.

```
1706174571.215 582 10.61.70.23 TCP_MISS_SSL/200 39 CONNECT tunnel://www.example.com:443/ - DIRECT/www.e
1706174571.486 270 10.61.70.23 TCP_MISS_SSL/200 1106 GET https://www.example.com:443/ - DIRECT/www.exam
```

Remarque : En mode transparent, SWA a l'adresse IP de destination initialement lorsque le trafic y est redirigé.

Voici quelques exemples de ce que vous voyez dans les journaux d'accès :`

Déploiement transparent - Trafic décrypté

1252543170.769.386.192.168.30.103 TCP_MISS_SSL/200 0 TCP_CONNECT 192.168.34.32:443/ - DIRECT/192.168.34.32 - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,5.0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-> - 1252543171.166 395 192.168.30.103 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - DIRECT/192.168.34.32 image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,0,-,-,-,-,-,-,-,-> -
Déploiement transparent - Trafic de transit
1252543337.373 690 192.168.30.103 TCP_MISS/200 2044 TCP_CONNECT 192.168.34.32:443/ - DIRECT/192.168.34.32 - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9.0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Déploiement transparent - Abandon
1252543418.175 430 192.168.30.103 TCP_DENIED/403 0 TCP_CONNECT 192.168.34.32:443/ - DIRECT/192.168.34.32 - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,-9.1.0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Déploiement explicite - Trafic déchiffré
252543558.405 385 10.66.71.105 TCP_CLIENT_REFRESH_MISS_SSL/200 40 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,5.0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-> - 1252543559.535 1127 10.66.71.105 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - DIRECT/www.example.com image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,0,-,-,-,-,-,-,-,-,-,-> -
Déploiement explicite - Trafic de transit
1252543491.302 568 10.66.71.105 TCP_CLIENT_REFRESH_MISS/200 2256 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9.0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Déploiement explicite - Abandonner
1252543668.375 1 10.66.71.105 TCP_DENIED/403 1578 CONNECT tunnel://www.example.com:443/ - NONE/- - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-NONE <Sear,-9.1,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-> -

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance - LD (Limited Deployment) - Troubleshooti...

- Configuration du paramètre de performance dans les journaux d'accès - Cisco

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.