

Comment le module de Services de sécurité ASA CSC agit-il en tant que proxy pour le trafic http ?

Contenu

[Introduction](#)

[Comment le module de Services de sécurité ASA CSC agit-il en tant que proxy pour le trafic http ?](#)

[Informations connexes](#)

Introduction

Ce document décrit comment le module de services de sécurité Cisco ASA Content Security and Control (CSC) peut agir en tant que serveur proxy pour le trafic http.

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Q. Comment le module de Services de sécurité ASA CSC agit-il en tant que proxy pour le trafic http ?

A. La compréhension des étapes impliquées en établissant une connexion HTTP par le module CSC vous aidera à comprendre d'autres questions (telles que des erreurs et des problèmes de performances de page) :

1. Quand les essais d'un utilisateur à connecter à un site, leur navigateur envoie un paquet de synchronisation à l'adresse IP de ce site.
2. Le module CSC, qui agit en tant que proxy, intercepte le paquet de synchronisation et répond avec un SYN-ACK au nom du site.
3. Le navigateur Web, qui ignore que le module CSC agisse en tant que proxy, répond avec un ACK, et une connexion est formée entre la machine cliente et l'engine de proxy HTTP de module CSC. **Remarque:** La première moitié de cette connexion désigné sous le nom du socket de côté client (CSS).
4. En ce moment, le navigateur pense que la connexion au site est en hausse et fonctionnelle, et elle envoie la requête HTTP GET.
5. La requête HTTP GET est traitée par le module CSC ; c'est-à-dire, il est vérifié contre les configurations du blocage URL/filtering/WRS. Si on permet la demande, le module CSC commence à établir une connexion au web server au site.
6. L'engine de proxy HTTP envoie un paquet de synchronisation de TCP avec une adresse IP source et le port de source qui apparie la synchronisation de TCP d'origine le client pense qu'il a envoyé au web server (comme reçu sur le CSS). Le web server répond avec une synchronisation ACK, et l'engine de proxy HTTP répond avec un ACK. En ce moment, le

socket de côté serveur (SSS) est en hausse.

7. L'engine de proxy HTTP envoie le HTTP du client OBTIENNENT au web server et le web server répond avec le contenu.
8. Ce contenu est balayé/vérifié. S'il est propre, le contenu est expédié de nouveau au client.
9. Ces mêmes étapes sont répétées pour n'importe quelle autre requête Web du client à n'importe quel web server.

Notez que le navigateur de client se connecte jamais vraiment au site ; il se connecte au module CSC qui feint pour être le site comme illustré dans cette image :

[Informations connexes](#)

- [Support et documentation techniques - Cisco Systems](#)