Échec du filtre d'URL CSC-SSM avec l'authentification par proxy cut-through configurée sur l'ASA en ligne

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Conventions
Conditions/environnement
Problème
Solution(s)
Informations connexes

Introduction

Ce document décrit le problème lorsque le filtre d'URL échoue sur le module CSC-SSM (Content Security and Control Security Services Module) lorsque l'authentification par proxy cut-through est configurée sur l'appliance ASA (Adaptive Security Appliance) ou un périphérique entre le port de gestion du module CSC-SSM et Internet.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Conditions/environnement

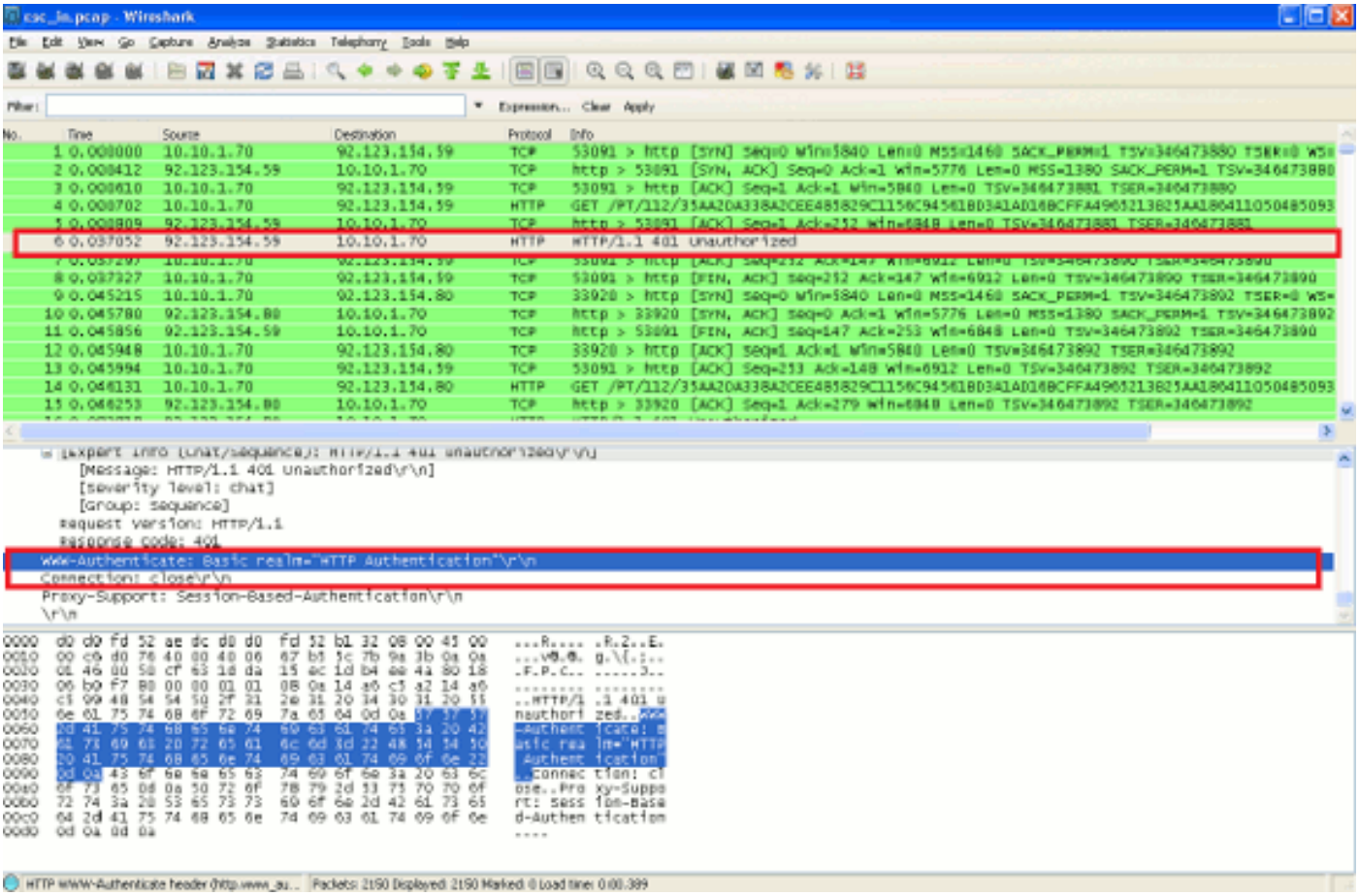
L'authentification par proxy cut-through AAA (Authentication, Authorization, and Accounting) est configurée sur un ASA qui se trouve sur le chemin entre le port Management du module CSC et Internet.

Problème

Les sites Web ne sont pas filtrés par URL via CSC-SSM et CSC-SSM HTTP. Les journaux affichent des messages similaires à ceux-ci :

```
2011/04/28 14:55:04 GMT+01:00  <6939-1376041904> Get URL Category returned [-1],
    with category 0 = [0] and rating = [0]
2011/04/28 14:55:04 GMT+01:00  <6939-1376041904> URLFilteringScanTask:PerformPreScanTask
    - URL rating failed, has to let it go
2011/04/28 14:55:04 GMT+01:00  <6939-1376041904> add result=1 server=
```

Le problème est facilement identifié une fois que les captures de paquets sont collectées à destination et en provenance du port de gestion du module CSC-SSM sur l'interface interne de l'ASA. Dans l'exemple ci-dessous, l'adresse IP du réseau interne est 10.10.1.0/24 et l'adresse IP du module CSC est 10.10.1.70. L'adresse IP 92.123.154.59 est l'adresse IP de l'un des serveurs de classification Trend Micro.



Lorsque le module CSC cherche à déterminer la catégorie dans laquelle se trouve une URL donnée, le module CSC doit demander aux serveurs de classification Trend Micro des informations sur cette URL spécifique. Le module CSC-SSM crée cette connexion à partir de sa propre adresse IP de gestion et utilise TCP/80 pour la communication. Dans l'écran ci-dessus, la

connexion en trois étapes s'est terminée correctement entre le serveur de classification Trend Micro et le module CSC-SSM. Le module CSC-SSM envoie maintenant une requête GET au serveur et reçoit un message « HTTP/1.1 401 Non autorisé » généré par l'ASA (ou tout autre périphérique réseau en ligne) qui effectue un proxy cut-through.

Dans cet exemple d'ASA, l'authentification par proxy cut-through AAA est configurée avec les commandes suivantes :

```
aaa authentication match inside_authentication inside AUTH_SERV
access-list inside_authentication extended permit tcp any any
```

Ces commandes exigent que l'ASA invite tous les utilisateurs internes (en raison de « tcp any any » dans la liste de contrôle d'accès d'authentification) à accéder à n'importe quel site Web. L'adresse IP de gestion du module CSC-SSM est 10.10.1.70, qui appartient au même sous-réseau que celui du réseau interne, est désormais soumise à cette politique. Par conséquent, l'ASA considère que le module CSC-SSM n'est qu'un autre hôte du réseau interne et le remet en question pour obtenir un nom d'utilisateur et un mot de passe. Malheureusement, le module CSC-SSM n'est pas conçu pour fournir une authentification lorsqu'il tente d'atteindre les serveurs de classification Trend Micro pour la classification des URL. Puisque l'authentification CSC-SSM échoue, l'ASA envoie un message « HTTP/1.1 401 Unallowed » au module. La connexion se ferme et l'URL en question n'est pas correctement classée par le module CSC.

Solution(s)

Utilisez cette solution pour résoudre le problème.

Entrez les commandes suivantes pour exempter l'adresse IP de gestion du module CSC-SSM de l'authentification :

```
access-list inside_authentication extended deny tcp host 10.10.1.70 any
access-list inside_authentication extended permit tcp any any
```

Le port de gestion du module CSC-SSM doit disposer d'un accès totalement libre à Internet. Il ne doit pas passer par des filtres ou des contrôles de sécurité susceptibles d'empêcher l'accès à Internet. En outre, il ne devrait pas avoir à s'authentifier, de quelque manière que ce soit, pour obtenir l'accès à Internet.

Informations connexes

- Support et documentation techniques - Cisco Systems