Le filtre URL CSC-SSM échoue avec l'authentification de proxy de cut-through configurée sur l'ASA intégrée

Contenu

Introduction

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

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à

Conventions relatives aux conseils techniques Cisco.

Conditions/environnement

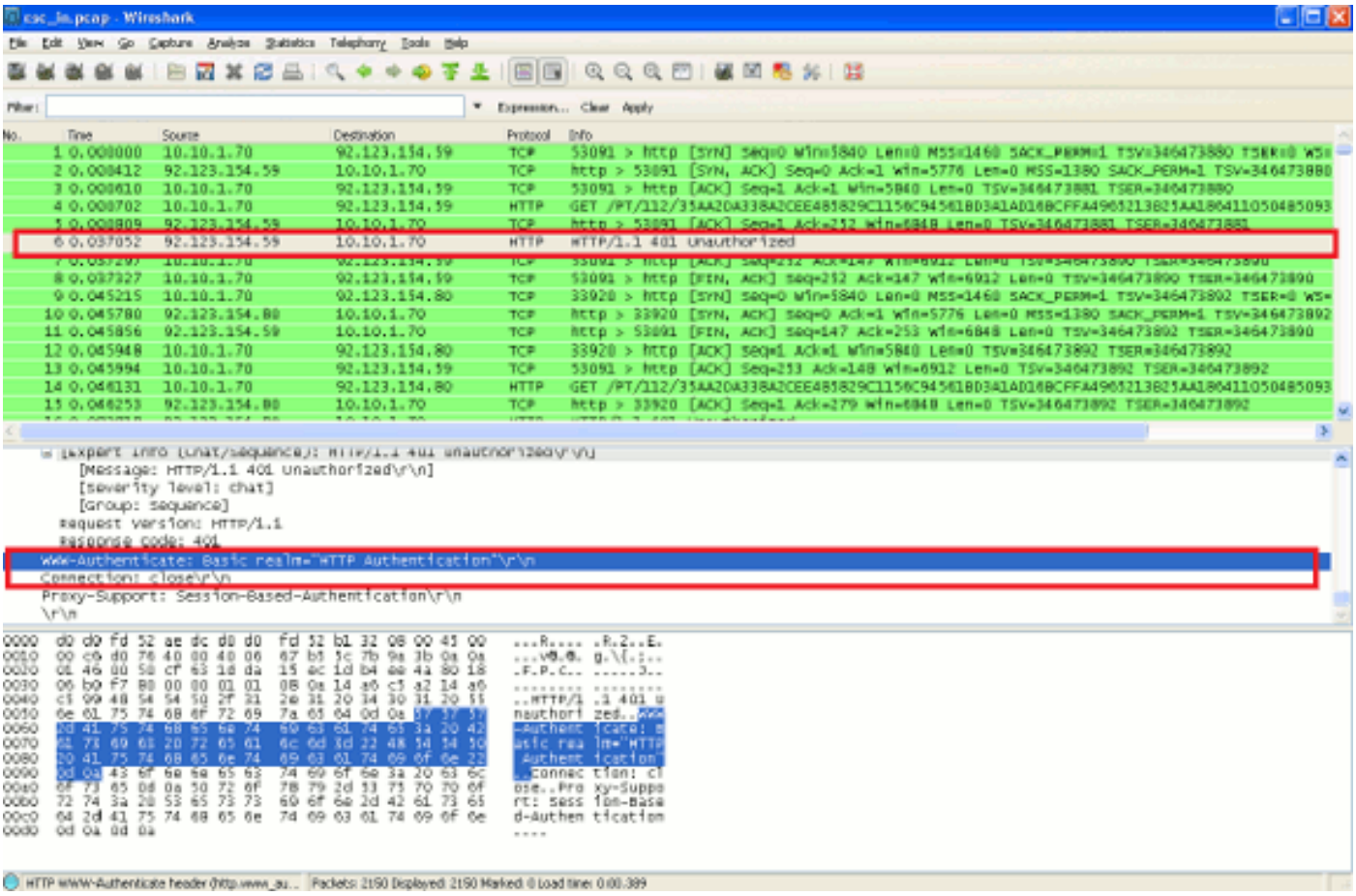
L'authentification de proxy de cut-through d'Authentification, autorisation et comptabilité (AAA) est configurée sur une ASA qui est dans le chemin entre le port de gestion du module CSC et l'Internet.

Problème

Les sites Web URL-ne sont pas filtrés par le CSC-SSM et le HTTP CSC-SSM. Les messages d'exposition de logs semblables à ces derniers :

```
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 après que des captures de paquet soient collectées à et du port de gestion du CSC-SSM sur l'interface interne ASA. Dans l'exemple ci-dessous, l'adresse IP intérieure de réseau 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 d'un des serveurs Trends Micros de classification.



Quand le module CSC regarde pour déterminer la catégorie qu'un certain URL tombe dans, le module CSC doit interroger les serveurs Trends Micros de classification pour information au sujet de cet URL de particularité. Les sources CSC-SSM cette connexion de sa propres adresse IP et elle de Gestion utilise TCP/80 pour la transmission. Dans l'affichage de l'écran ci-dessus, la prise

de contact à trois voies se termine avec succès entre le serveur Trend Micro de classification et le CSC-SSM. Le CSC-SSM envoie maintenant une demande GET au serveur et il reçoit un » message "HTTP/1.1 401 non autorisé généré par l'ASA (ou tout autre périphérique intégré de réseau) qui fait le proxy de cut-through.

Sur cet exemple ASA, l'authentification de proxy de cut-through d'AAA est configurée avec ces commandes :

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

Ces commandes exigent de l'ASA d'inciter tous les utilisateurs sur l'intérieur (dû au « TCP tout » dans l'ACL d'authentification) pour que l'authentification aille à n'importe quel site Web. L'adresse IP de la Gestion Du CSC-SSM est 10.10.1.70, qui appartient au même sous-réseau que ce du réseau intérieur est sujette maintenant à cette stratégie. En conséquence, l'ASA considère comme étant le CSC-SSM juste un autre hôte dans le réseau intérieur et le conteste pour un nom d'utilisateur et mot de passe. Malheureusement, le CSC-SSM n'est pas conçu pour fournir l'authentification quand il essaye d'atteindre les serveurs Trends Micros de classification pour la classification de l'URLs. Puisque le CSC-SSM échoue authentification, l'ASA envoie un » message "HTTP/1.1 401 non autorisé au module. La connexion se ferme et l'URL en question n'est pas avec succès classifié par le module CSC.

Solutions

Utilisez cette solution pour résoudre le problème.

Sélectionnez ces commandes d'exempter l'adresse IP de la Gestion du 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 CSC-SSM doit avoir l'accès à Internet complètement sans difficulté. Il ne devrait pas ne passer par aucuns filtres ou contrôle de Sécurité qui pourraient empêcher l'accès à Internet. En outre, il ne devrait pas devoir authentifier, de quelque façon, pour obtenir l'accès à Internet.

Informations connexes

- Support et documentation techniques - Cisco Systems