CSC-SSM-URL-Filter schlägt fehl, wenn Cut-Through-Proxy-Authentifizierung auf der In-Line-ASA konfiguriert ist

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Bedingungen/Umgebung
Problem
Lösung(en)
Zugehörige Informationen

Einführung

Dieses Dokument beschreibt das Problem, wenn der URL-Filter im CSC-SSM (Content Security and Control Security Services Module) fehlschlägt, wenn die Cut-Through-Proxy-Authentifizierung auf der Adaptive Security Appliance (ASA) oder einem Gerät zwischen dem Management-Port des CSC-SSM und dem Internet konfiguriert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips

Conventions (Technische Tipps zu Konventionen von Cisco).

Bedingungen/Umgebung

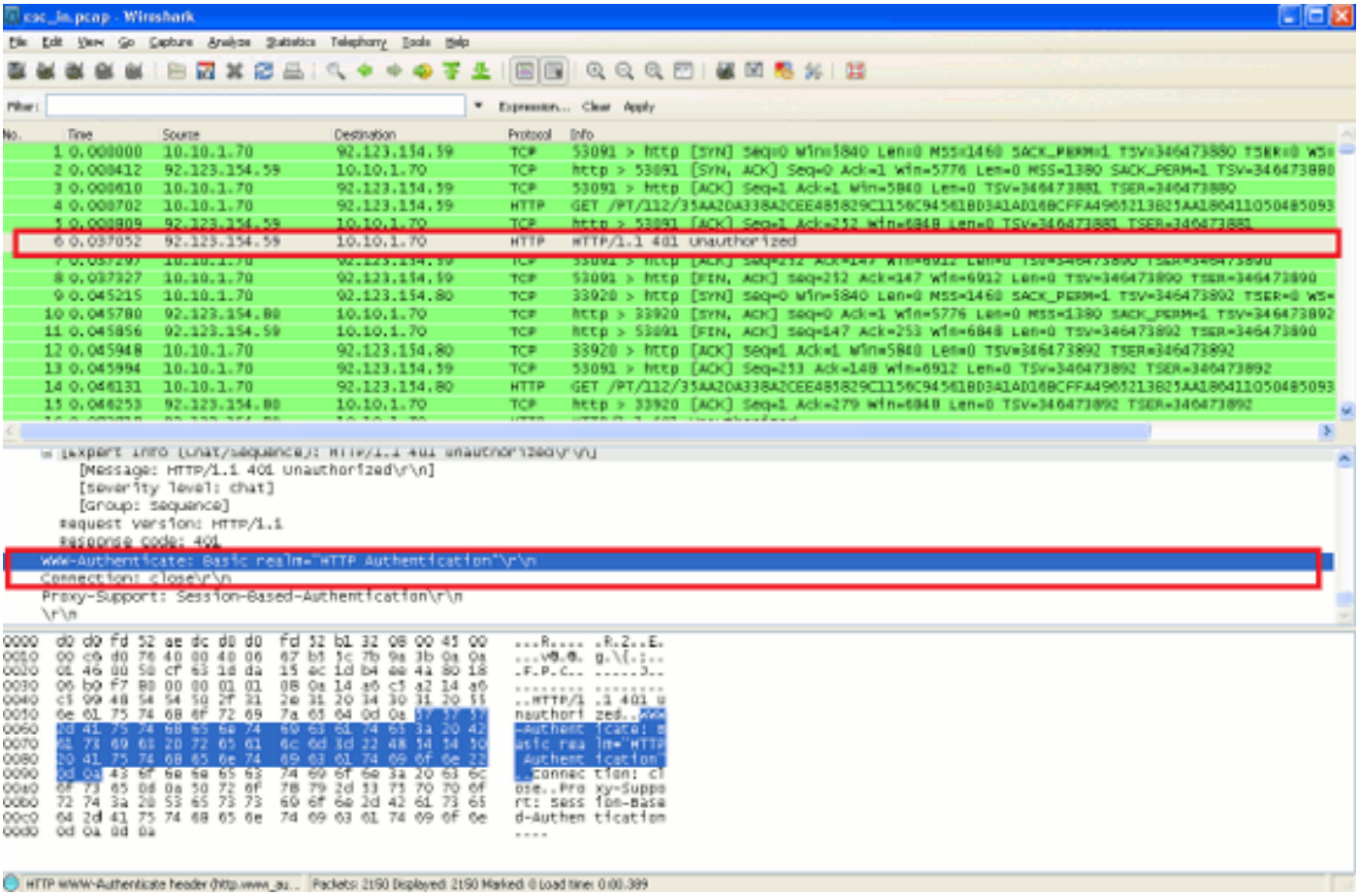
Die AAA-Cut-Through-Proxy-Authentifizierung (Authentication, Authorization, Accounting) wird auf einer ASA konfiguriert, die sich im Pfad zwischen dem Management-Port des CSC-Moduls und dem Internet befindet.

Problem

Die Websites werden nicht über den CSC-SSM und das CSC-SSM HTTP URL-gefiltert. Die Protokolle zeigen ähnliche Meldungen an:

```
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=
```

Das Problem lässt sich leicht identifizieren, nachdem die Paketerfassung für den Management-Port des CSC-SSM auf der internen ASA-Schnittstelle erfasst wurde. Im folgenden Beispiel lautet die interne IP-Adresse des Netzwerks 10.10.1.0/24, und die IP-Adresse des CSC-Moduls lautet 10.10.1.70. Die IP-Adresse 92.123.154.59 ist die IP-Adresse eines der Trend Micro Classification-Server.



Wenn das CSC-Modul nach der Kategorie sucht, in die eine bestimmte URL fällt, muss das CSC-Modul die Trend Micro Classification-Server nach Informationen über diese spezifische URL

fragen. Der CSC-SSM bezieht diese Verbindung von seiner eigenen Management-IP-Adresse und verwendet TCP/80 für die Kommunikation. In der Anzeige oben wird der Drei-Wege-Handshake zwischen dem Trend Micro Classification-Server und dem CSC-SSM erfolgreich abgeschlossen. Der CSC-SSM sendet jetzt eine GET-Anforderung an den Server und empfängt eine Nachricht "HTTP/1.1 401 Unauthorized" (HTTP/1.1 401 Unauthorized), die von der ASA (oder einem anderen In-Line-Netzwerkgerät) generiert wird und einen Cut-Through-Proxy ausführt.

In diesem Beispiel wird die AAA-Cut-Through-Proxy-Authentifizierung mit folgenden Befehlen konfiguriert:

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

Diese Befehle erfordern, dass die ASA alle Benutzer im Inneren auffordert (aufgrund von "tcp any any" in der Authentifizierungs-ACL), damit die Authentifizierung zu einer beliebigen Website führt. Die IP-Adresse des CSC-SSM für die Verwaltung lautet 10.10.1.70. Diese Adresse gehört zum gleichen Subnetz wie das des internen Netzwerks und unterliegt nun dieser Richtlinie. Daher betrachtet die ASA das CSC-SSM als einen weiteren Host im internen Netzwerk und fordert ihn auf, einen Benutzernamen und ein Kennwort einzugeben. Leider ist das CSC-SSM nicht dafür ausgelegt, eine Authentifizierung bereitzustellen, wenn versucht wird, die Trend Micro Classification-Server zur Klassifizierung von URLs zu erreichen. Da die Authentifizierung des CSC-SSM fehlschlägt, sendet die ASA eine Nachricht "HTTP/1.1 401 Unauthorized" (HTTP/1.1 - Nicht autorisiert) an das Modul. Die Verbindung wird geschlossen, und die betreffende URL wird vom CSC-Modul nicht erfolgreich klassifiziert.

Lösung(en)

Verwenden Sie diese Lösung, um das Problem zu beheben.

Geben Sie die folgenden Befehle ein, um die IP-Adresse des CSC-SSM-Managements von der Authentifizierung auszunehmen:

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

Der Management-Port des CSC-SSM muss einen vollständig ungehinderten Zugriff auf das Internet haben. Es sollte keine Filter oder Sicherheitsprüfungen durchlaufen, die den Zugriff auf das Internet verhindern könnten. Außerdem sollte es sich in keiner Weise authentifizieren müssen, um Zugang zum Internet zu erhalten.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems