CSC-SSM URL Filter faalt met cut-by Proxy verificatie ingesteld op Inline ASA

Inhoud

Inleiding

Dit document beschrijft het probleem wanneer het URL-filter niet voldoet aan de CSC-SSM (Content Security and Control Security Services Module) wanneer doorsnede-proxy-verificatie is geconfigureerd op de adaptieve security applicatie (ASA) of een apparaat tussen de CSC-SSM beheerpoort en het internet.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Voorwaarden/milieu

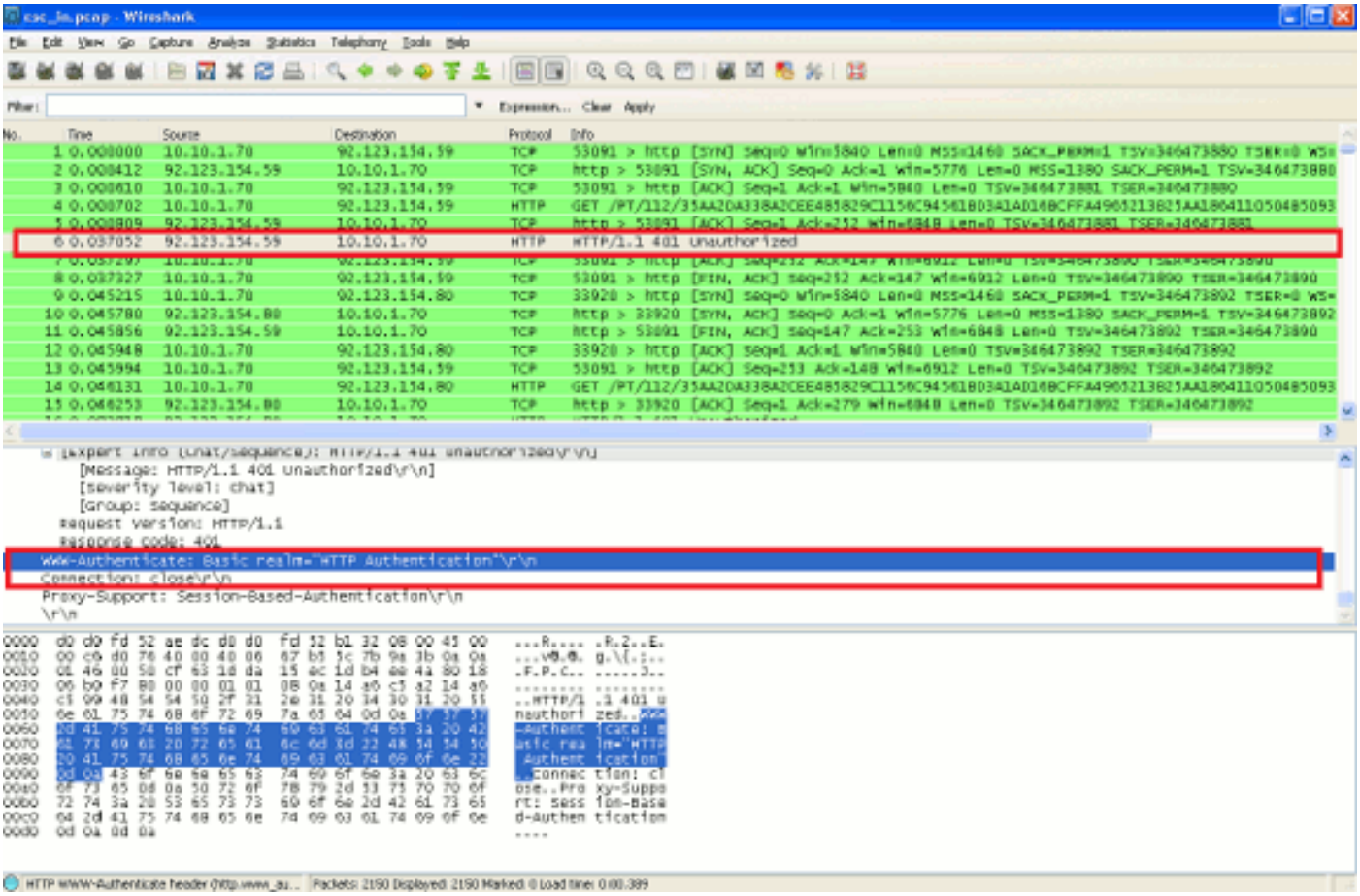
Verificatie, autorisatie en accounting (AAA) doorgesneden proxy-verificatie is ingesteld op een ASA die in het pad tussen de beheerpoort van de CSC-module en het internet ligt.

Probleem

De websites zijn niet URL-gefilterd door CSC-SSM en CSC-SSM HTTP. De blogs tonen soortgelijke berichten:

```
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=
```

Het probleem wordt gemakkelijk geïdentificeerd nadat de pakketvastlegging van en naar de beheerpoort van CSC-SSM op de ASA binneninterface is verzameld. In het onderstaande voorbeeld is het IP-adres van het binnennetwerk 10.10.1.0/24 en is het IP-adres van de CSC-module 10.10.1.70. Het IP-adres 92.123.154.59 is het IP-adres van een van de Trend Micro Classifier-servers.



Wanneer de CSC-module de categorie wil bepalen waarin een bepaalde URL valt, moet de CSC-module de Trend Micro Classifier-servers om informatie vragen over die specifieke URL. CSC-SSM bronnen deze verbinding van zijn eigen IP-adres en het gebruikt TCP/80 voor communicatie. In het bovenstaande schermdisplay wordt de 3-voudige handdruk voltooid tussen de Trend Micro Classifier-server en de CSC-SSM. Het CSC-SSM stuurt nu een GET aanvraag naar de server en

ontvangt een "HTTP/1.1 401 onbevoegd" bericht dat gegenereerd is door de ASA (of ander inline netwerkapparaat) dat doorsnijproxy heeft.

In dit voorbeeld ASA, wordt AAA cut-through proxy authenticatie ingesteld met deze opdrachten:

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

Deze opdrachten vereisen dat de ASA alle gebruikers binnenin (door "tcp any" in de authenticatie ACL) vraagt om verificatie naar een website te gaan. Het beheer-IP-adres van CSC-SSM is 10.10.1.70, dat tot dezelfde vorm van netwerk behoort als dat van het binnennetwerk is nu aan dit beleid onderworpen. Als resultaat hiervan, beschouwt de ASA CSC-SSM als slechts een andere host in het binnennetwerk en daagt deze uit voor een gebruikersnaam en wachtwoord. Helaas is het CSC-SSM niet ontworpen om authenticatie te bieden wanneer het probeert de Trend Micro Classifier-servers te bereiken voor classificatie van URL's. Aangezien CSC-SSM niet-verificatie heeft plaatsgevonden, stuurt de ASA een "HTTP/1.1 401 onbevoegd" bericht naar de module. De verbinding sluit en de URL in kwestie wordt niet met succes geclassificeerd door de CSC Module.

Oplossing(en)

Gebruik deze oplossing om het probleem op te lossen.

Voer deze opdrachten in om het IP-adres van het beheer van CSC-SSM van verificatie te vrijwaren:

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

De beheerpoort van CSC-SSM moet volledig onbelemmerde toegang tot het internet hebben. Het moet geen filters of veiligheidscontroles doorlopen die de toegang tot het internet kunnen verhinderen. Ook mag het op geen enkele wijze een authenticatie van het internet behoeven.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems