Filtro URL CSC-SSM non riuscito con autenticazione proxy Cut-through configurata sull'appliance ASA in-line

Sommario

Introduzione

In questo documento viene descritto il problema quando il filtro URL sul Content Security and Control Security Services Module (CSC-SSM) ha esito negativo quando viene configurata l'autenticazione proxy cut-through sull'appliance ASA (Adaptive Security Appliance) o su un dispositivo tra la porta di gestione del CSC-SSM e Internet.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni

nei suggerimenti tecnici.

Condizioni/Ambiente

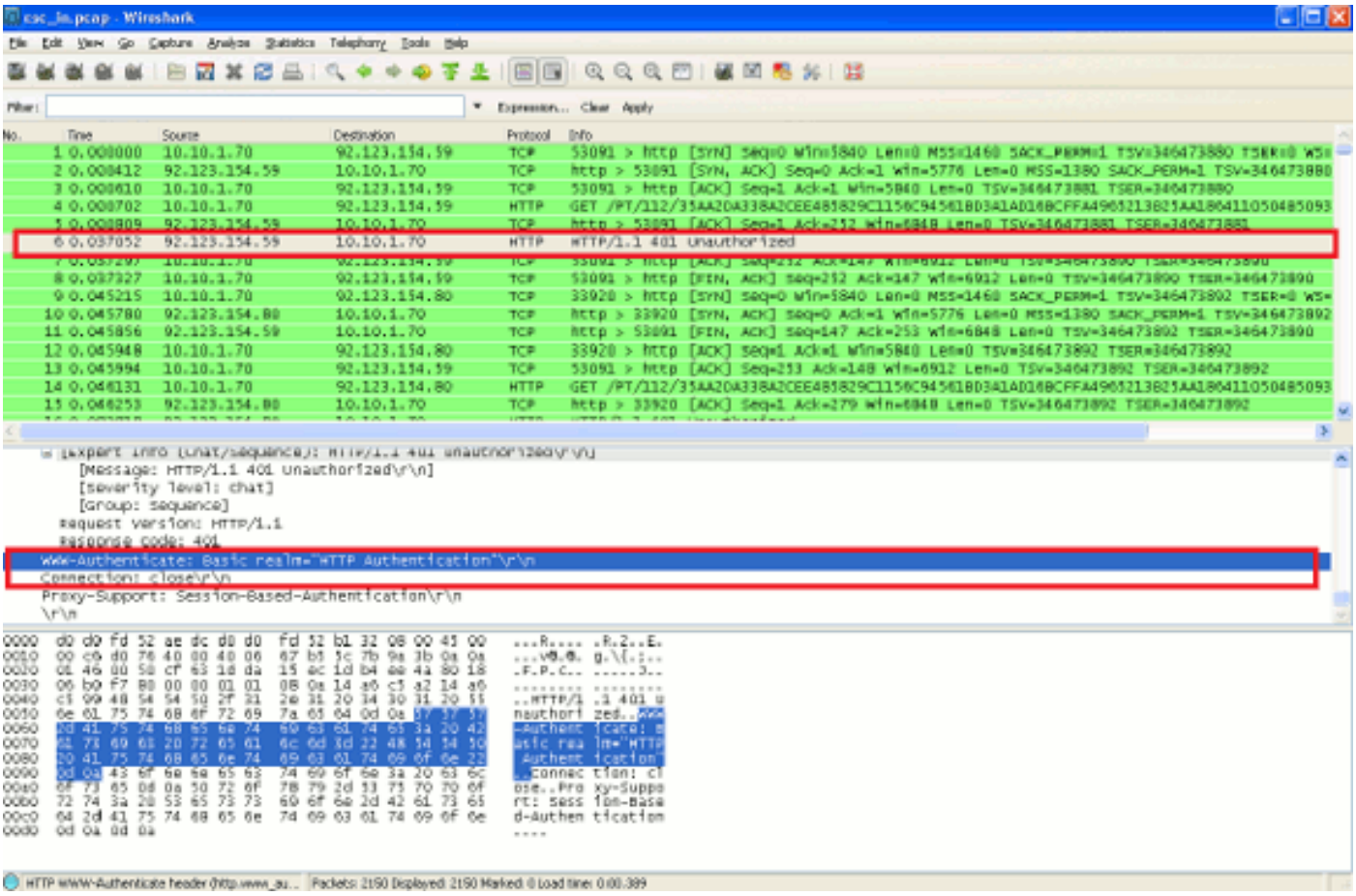
L'autenticazione proxy cut-through AAA (Authentication, Authorization, and Accounting) viene configurata su un'ASA situata nel percorso tra la porta di gestione del modulo CSC e Internet.

Problema

I siti Web non sono filtrati per URL tramite CSC-SSM e CSC-SSM HTTP. Nei log vengono visualizzati messaggi simili ai seguenti:

```
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=
```

Il problema viene facilmente identificato dopo che le acquisizioni dei pacchetti vengono raccolte da e verso la porta di gestione del CSC-SSM sull'interfaccia interna dell'ASA. Nell'esempio seguente, l'indirizzo IP della rete interna è 10.10.1.0/24 e l'indirizzo IP del modulo CSC è 10.10.1.70. L'indirizzo IP 92.123.154.59 è l'indirizzo IP di uno dei server Trend Micro Classification.



Quando il modulo CSC cerca di determinare la categoria in cui rientra un determinato URL, deve chiedere ai server di classificazione Trend Micro informazioni su tale URL specifico. Il CSC-SSM rileva questa connessione dal proprio indirizzo IP di gestione e utilizza il protocollo TCP/80 per la comunicazione. Nella schermata precedente, l'handshake a 3 vie viene completato correttamente

tra il server di classificazione Trend Micro e CSC-SSM. CSC-SSM invia una richiesta GET al server e riceve un messaggio "HTTP/1.1 401 Unauthorized" (HTTP/1.1.401 Non autorizzato) generato dall'ASA (o da un altro dispositivo di rete in linea) che invia un proxy cut-through.

Nell'esempio di ASA, l'autenticazione proxy AAA cut-through è configurata con questi comandi:

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

Per questi comandi, l'appliance ASA deve richiedere a tutti gli utenti all'interno (a causa di "tcp any" nell'ACL di autenticazione) di accedere a un sito Web. L'indirizzo IP di gestione di CSC-SSM è 10.10.1.70, che appartiene alla stessa subnet della rete interna ed è ora soggetta a questa policy. Di conseguenza, l'ASA considera il CSC-SSM solo un altro host nella rete interna e lo contesta per un nome utente e una password. Sfortunatamente, CSC-SSM non è progettato per fornire l'autenticazione quando cerca di raggiungere i server Trend Micro Classification per la classificazione degli URL. Poiché l'autenticazione CSC-SSM non riesce, l'ASA invia un messaggio "HTTP/1.1 401 Non autorizzato" al modulo. La connessione viene chiusa e l'URL in questione non è stato classificato correttamente dal modulo CSC.

Soluzione/i

Utilizzare questa soluzione per risolvere il problema.

Immettere questi comandi per escludere l'indirizzo IP di gestione di CSC-SSM dall'autenticazione:

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

La porta di gestione di CSC-SSM deve avere accesso a Internet senza ostacoli. Non deve passare attraverso filtri o controlli di sicurezza che potrebbero impedire l'accesso a Internet. Inoltre, non dovrebbe in alcun modo essere autenticata per ottenere l'accesso a Internet.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems