Problemi di connessione dell'appliance ASA a Cisco Adaptive Security Device Manager

Sommario

Introduzione

Questo documento fornisce la metodologia di risoluzione dei problemi necessaria per esaminare i problemi incontrati quando si accede/si configura la Cisco Adaptive Security Appliance (ASA) con Cisco Adaptive Security Device Manager (ASDM). ASDM fornisce servizi di gestione e monitoraggio della sicurezza per le appliance di sicurezza attraverso un'interfaccia di gestione grafica.

Prerequisiti

Requisiti

Gli scenari, i sintomi e i passaggi elencati in questo documento vengono scritti per risolvere i problemi dopo la configurazione iniziale sull'appliance ASA. Per la configurazione iniziale, fare riferimento alla sezione Configurazione dell'accesso ASDM per gli accessori nella Guida generale alle operazioni ASDM della serie Cisco ASA, versione 7.1.

In questo documento viene usata la CLI di ASA per la risoluzione dei problemi, che richiede l'accesso all'ASA da parte di Secure Shell (SSH)/Telnet/Console.

Componenti usati

Le informazioni fornite in questo documento si basano su ASDM e ASA.

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.

Metodologia di risoluzione dei problemi

Il presente documento di risoluzione dei problemi è incentrato su tre punti di errore principali. Se si segue il processo generale di risoluzione dei problemi in questo ordine, il presente documento dovrebbe aiutare a determinare l'esatto problema con l'accesso o l'utilizzo di ASDM.

- **Configurazione ASA**
- **Connettività di rete**
- **Software applicativo**

Configurazione ASA

Per accedere correttamente all'ASDM, sono necessarie tre configurazioni essenziali sull'appliance ASA:

- Immagine ASDM in Flash
- Immagine ASDM in uso
- Restrizioni server HTTP

Immagine ASDM in Flash

Accertarsi che la versione richiesta dell'ASDM sia stata caricata sulla memoria flash. Può essere caricato con la versione corrente di ASDM o con altri metodi convenzionali di trasferimento dei file all'appliance ASA, ad esempio il protocollo TFTP.

Immettere **show flash** sulla CLI dell'ASA per ottenere un elenco dei file presenti sulla memoria flash ASA. Verificare la presenza del file ASDM:

```
ciscoasa# show flash --#--  --length--  -----date/time------  path

249 76267 Feb 28 2013 19:58:18 startup-config.cfg
250 4096 May 12 2013 20:26:12 sdesktop
251 15243264 May 08 2013 21:59:10 asa823-k8.bin
252 25196544 Mar 11 2013 22:43:40 asa845-k8.bin
253 17738924 Mar 28 2013 00:12:12 asdm-702.bin ---- ASDM Image
```

Per verificare ulteriormente se l'immagine presente sulla memoria flash è valida e non danneggiata, è possibile utilizzare il comando **verify** per confrontare l'hash MD5 memorizzato nel pacchetto software e l'hash MD5 del file effettivo presente:

```
ciscoasa# verify flash:/asdm-702.bin
Verifying file integrity of disk0:/asdm-702.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Done!
Embedded Hash MD5: e441a5723505b8753624243c03a40980
Computed Hash MD5: e441a5723505b8753624243c03a40980
CCO Hash      MD5: c305760ec1b7f19d910c4ea5fa7d1cf1
Signature Verified
Verified disk0:/asdm-702.bin
```

Questo passaggio permette di verificare la presenza dell'immagine e la sua integrità sull'appliance ASA.

Immagine ASDM in uso

Questo processo è definito nella configurazione ASDM sull'appliance ASA. La definizione di configurazione di esempio dell'immagine corrente utilizzata è simile alla seguente:

asdm image disk0:/asdm-702.bin

Per ulteriori verifiche, è possibile usare il comando **show asdm image**:

```
ciscoasa# show asdm image
Device Manager image file, disk0:/asdm-702.bin
```

Restrizioni server HTTP

Questo passaggio è essenziale nella configurazione ASDM, in quanto definisce le reti che hanno accesso all'ASA. Una configurazione di esempio è simile alla seguente:

```
http server enable
http 192.168.1.0 255.255.255.0 inside

http 64.0.0.0 255.0.0.0 outside
```

Verificare di disporre delle reti necessarie definite nella configurazione precedente. L'assenza di tali definizioni provoca il timeout dell'utilità di avvio ASDM durante la connessione e genera il seguente errore:

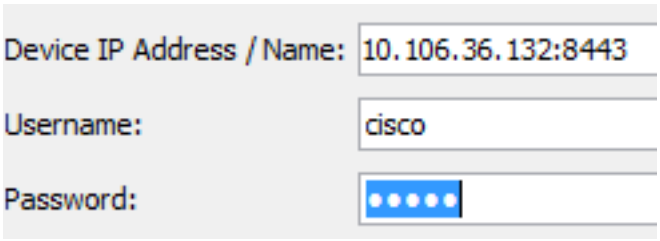
La pagina di avvio di ASDM (**https://<ASA IP address>/admin**) determina il timeout della richiesta e non viene visualizzata alcuna pagina.

Verificare inoltre che il server HTTP utilizzi una porta non standard per la connessione ASDM, ad esempio 8443. Questa condizione viene evidenziata nella configurazione:

cisco(config)# **show run http**

http server - abilita 8443

Se si utilizza una porta non standard, è necessario specificare la porta quando si esegue il collegamento all'ASA nell'utilità di avvio di ASDM come:



Ciò vale anche per quando si accede alla pagina di avvio di ASDM:
https://10.106.36.132:8443/admin

Altri possibili problemi di configurazione

Dopo aver completato i passaggi precedenti, se tutto funziona sul lato client, ASDM dovrebbe aprirsi. Tuttavia, se il problema persiste, aprire ASDM da un altro computer. Se il problema persiste, probabilmente è a livello di applicazione e la configurazione dell'ASA è corretta. Tuttavia, se il problema persiste, completare i seguenti passaggi per verificare ulteriormente le configurazioni lato ASA:

1. Verificare la configurazione di Secure Sockets Layer (SSL) sull'appliance ASA. ASDM utilizza SSL durante la comunicazione con l'appliance ASA. A seconda della modalità di avvio di ASDM, è possibile che i nuovi software del sistema operativo non consentano l'utilizzo di cifrature più deboli durante la negoziazione delle sessioni SSL.

   Verificare le cifrature consentite sull'appliance ASA e se sono state specificate versioni SSL specifiche nella configurazione con il comando **show run all ssl**:

   ```
   ciscoasa# show run all ssl
   ssl server-version any <--- Check SSL Version restriction configured on the ASA
   ssl client-version any
   ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1 <--- Check SSL ciphers
   permitted on the ASA
   ```

   Gli eventuali errori di negoziazione della cifratura SSL durante l'avvio di ASDM vengono visualizzati nei log ASA:

   ```
   %ASA-7-725014: SSL lib error. Function: SSL3_GET_CLIENT_HELLO Reason:
   no shared cipher
   %ASA-6-302014: Teardown TCP connection 3 for mgmt:64.103.236.189/52501 to
   identity:10.106.36.132/443 duration 0:00:00 bytes 7 TCP Reset by appliance
   ```

   Se vengono visualizzate impostazioni specifiche, ripristinarle ai valori predefiniti.

   Notare che la licenza VPN-3DES-AES deve essere abilitata sull'appliance ASA per fare in modo che le cifrature 3DES e AES vengano usate dall'appliance ASA nella configurazione. È possibile verificare questa condizione con il comando **show version** sulla CLI. L'output viene visualizzato nel modo seguente:

   ```
   ciscoasa#show version

   Hardware: ASA5510, 256 MB RAM, CPU Pentium 4 Celeron 1600 MHz
   Internal ATA Compact Flash, 64MB
   Slot 1: ATA Compact Flash, 32MB
   BIOS Flash M50FW080 @ 0xffe00000, 1024KB
   <snip>
   Failover            : Active/Active
   VPN-DES             : Enabled
   VPN-3DES-AES        : Enabled
   <snip>
   ```

   Una licenza VPN-3DES-AES può essere ottenuta senza costi aggiuntivi sul sito Web delle licenze Cisco. Fare clic su **Security Products**, quindi selezionare **Cisco ASA 3DES/AES License**.

   Nota: Nelle nuove piattaforme ASA 5500-X fornite con il codice 8.6/9.x, le impostazioni della cifratura SSL sono impostate su **des-sha1 per** impostazione predefinita, il che impedisce il funzionamento delle sessioni ASDM. Fare riferimento all'appliance ASA 5500-x: Per ulteriori informazioni, ASDM e altre funzioni SSL non funzionano correttamente.
2. Verificare che WebVPN sia abilitato sull'appliance ASA. Se è abilitato, è necessario usare questo URL (**https://10.106.36.132/admin**) per accedervi quando si accede alla pagina di avvio Web di ASDM.
3.
4. Verificare la configurazione NAT (Network Address Translation) sull'appliance ASA per la porta 443. In questo modo, l'appliance ASA non elabora le richieste ASDM, ma le invia alla rete/interfaccia per cui è stato configurato il protocollo NAT.
5.

6. Se si verifica tutto e il timeout dell'ASDM persiste, verificare che l'ASA sia configurata per l'ascolto sulla porta definita per ASDM con il comando **show asp table socket** sulla CLI dell'ASA. L'output dovrebbe mostrare che l'ASA è in ascolto sulla porta ASDM:

   ```
   Protocol  Socket    Local Address               Foreign Address         State
   SSL       0001b91f  10.106.36.132:443           0.0.0.0:*               LISTEN
   ```

   Se l'output non viene visualizzato, rimuovere e riapplicare la configurazione del server HTTP sull'appliance ASA per ripristinare il socket sul software ASA.
7.
8. Se si verificano problemi durante l'accesso o l'autenticazione ad ASDM, verificare che le opzioni di autenticazione per **HTTP** siano impostate correttamente. Se non è impostato alcun comando di autenticazione, è possibile usare la password di abilitazione ASA per accedere ad ASDM. Per abilitare l'autenticazione basata su nome utente/password, è necessario immettere questa configurazione per autenticare le sessioni ASDM/HTTP sull'appliance ASA dal database di nome utente/password dell'appliance:

   ```
   aaa authentication http console LOCAL
   ```

   Ricordarsi di creare un nome utente/password quando si abilita il comando precedente:

   ```
   username <username> password <password> priv <Priv level>
   ```

   Se nessuna di queste procedure consente di risolvere il problema, le opzioni di debug seguenti sono disponibili sull'appliance ASA per ulteriori informazioni:

   ```
   debug http 255
   debug asdm history 255
   ```

Connettività di rete

Se dopo aver completato la sezione precedente non è ancora possibile accedere ad ASDM, il passaggio successivo è verificare la connettività di rete all'appliance ASA dal computer da cui si desidera accedere ad ASDM. Per verificare che l'ASA riceva la richiesta dal computer client, è necessario eseguire alcune operazioni di base per risolvere i problemi:

1. **Test con ICMP (Internet Control Message Protocol)**.
   Eseguire il ping sull'interfaccia ASA da cui si desidera accedere ad ASDM. Il ping deve avere esito positivo se l'ICMP può attraversare la rete e non ci sono restrizioni al livello dell'interfaccia ASA. Se il ping ha esito negativo, è probabile che si sia verificato un problema di comunicazione tra l'ASA e il computer client. Tuttavia, questo non è un passo decisivo per determinare che c'è questo tipo di problema di comunicazione.
2.
3. **Confermare con l'acquisizione dei pacchetti**.
   Posizionare un'acquisizione di pacchetto sull'interfaccia da cui si desidera accedere ad ASDM. L'acquisizione deve mostrare che i pacchetti TCP destinati all'indirizzo IP dell'interfaccia arrivano con il numero della porta di destinazione 443 (impostazione predefinita).

   Per configurare un'acquisizione, utilizzare questo comando:

   ```
   capture asdm_test interface
   ```

```
For example, cap asdm_test interface mgmt match tcp host 10.106.36.132
eq 443 host 10.106.36.13
```

In questo modo viene acquisito tutto il traffico TCP proveniente dalla porta 443 sull'interfaccia ASA da cui ci si connette all'ASDM. A questo punto, connettersi tramite ASDM o aprire la pagina Web di avvio di ASDM. Quindi, usare il comando **show capture asdm_test** per visualizzare il risultato dei pacchetti acquisiti:

```
ciscoasa# show capture asdm_test

Three packets captured

   1: 21:38:11.658855 10.106.36.13.54604 > 10.106.36.132.443:
      S 807913260:807913260(0) win 8192 <mss 1260,nop,wscale 2,nop,nop,sackOK>

   2: 21:38:14.659252 10.106.36.13.54604 > 10.106.36.132.443:
      S 807913260:807913260(0) win 8192 <mss 1260,nop,wscale 2,nop,nop,sackOK>

   3: 21:38:20.662166 10.106.36.13.54604 > 10.106.36.132.443:
      S 807913260:807913260(0) win 8192 <mss 1260,nop,nop,sackOK>
```

Questa acquisizione mostra una richiesta di sincronizzazione (SYN) dal computer client all'appliance ASA, ma l'appliance ASA non invia alcuna risposta. Se l'acquisizione è simile a quella precedente, i pacchetti raggiungono l'ASA, ma l'ASA non risponde a queste richieste, isolando il problema dall'ASA stessa. Per ulteriori informazioni sulla risoluzione dei problemi, consultare la prima sezione di questo documento.

Tuttavia, se l'output del comando non è simile a quello precedente e non viene acquisito alcun pacchetto, è presente un problema di connettività tra l'ASA e il client ASDM. Verificare che non vi siano dispositivi intermedi che possano bloccare il traffico sulla porta TCP 443 e che non vi siano impostazioni del browser, ad esempio le impostazioni del proxy, che possano impedire al traffico di raggiungere l'appliance ASA.

In genere, l'acquisizione dei pacchetti è un buon modo per stabilire se il percorso all'appliance ASA è vuoto e se è necessario eseguire ulteriori operazioni di diagnostica per evitare problemi di connettività di rete.

Software applicativo

In questa sezione viene descritto come risolvere i problemi relativi al software di avvio ASDM installato sul computer client quando l'avvio/il caricamento non riesce. Il servizio di avvio ASDM è il componente che risiede sul computer client e si connette all'appliance ASA per recuperare l'immagine ASDM. Una volta recuperata, l'immagine ASDM viene in genere memorizzata nella cache e quindi acquisita finché non vengono notate modifiche sul lato ASA, ad esempio un aggiornamento dell'immagine ASDM.

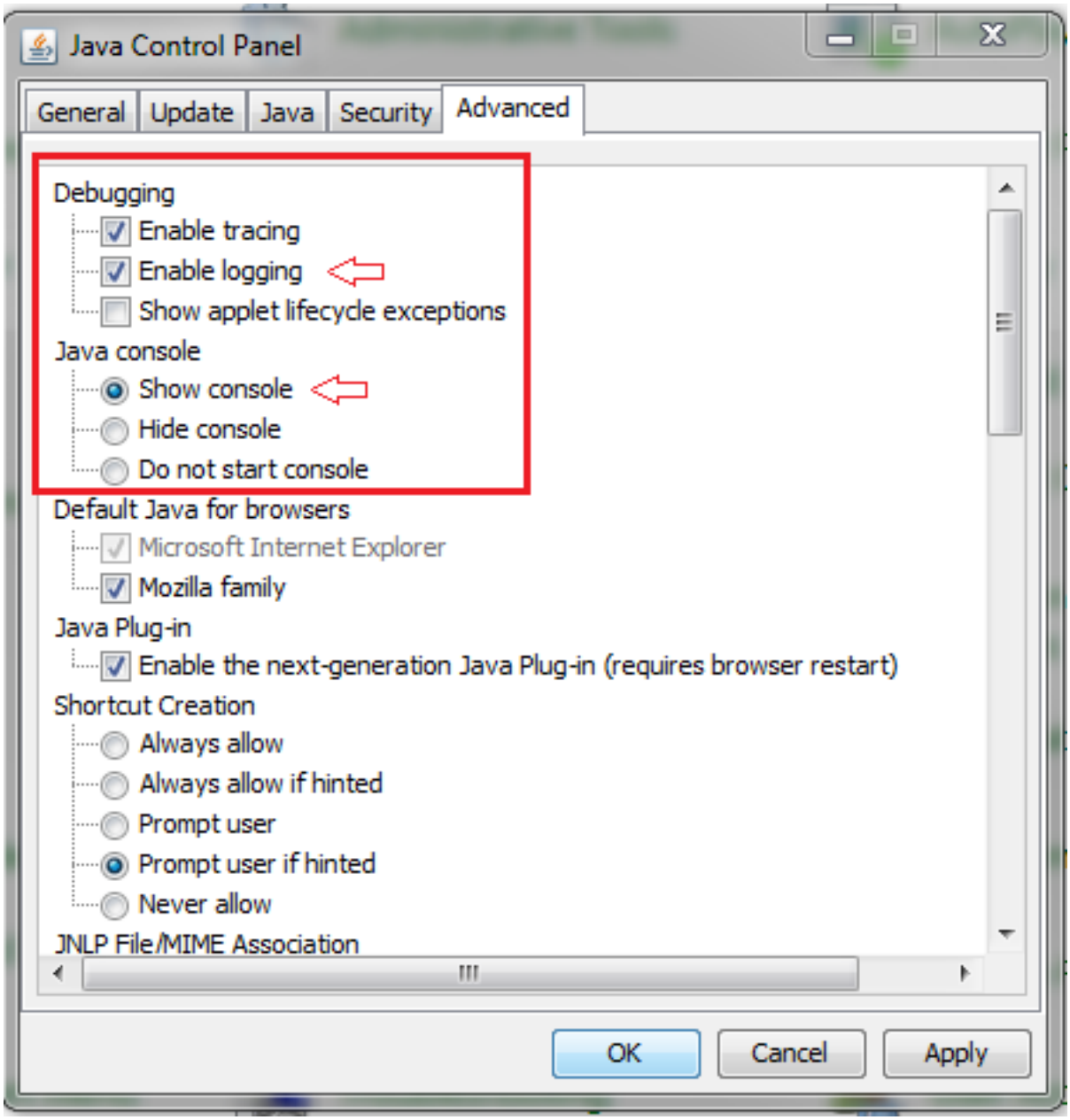
Per escludere eventuali problemi sul computer client, completare le seguenti operazioni di risoluzione dei problemi di base:

1. Aprire la pagina di avvio di ASDM da un altro computer. Se viene avviato, significa che il

problema riguarda il computer client in questione. Se l'operazione non riesce, seguire la guida alla risoluzione dei problemi dall'inizio per isolare i componenti interessati nell'ordine indicato.

2.
3. Aprire ASDM tramite il lancio sul Web e avviare il software direttamente da qui. Se l'operazione ha esito positivo, è probabile che si siano verificati problemi con l'installazione del servizio di avvio di ASDM. Disinstallare il software di avvio ASDM dal computer client e reinstallarlo dal Web di avvio ASA.
4.
5. Cancellare la directory cache di ASDM nella directory home dell'utente. In Windows 7, ad esempio, il percorso è il seguente: **C:\Users\<nomeutente>\.asdm\cache**. La cache viene cancellata quando si elimina l'intera directory **della cache**. Se l'ASDM viene avviato correttamente, è possibile cancellare la cache anche dal menu **File** ASDM.
6.
7. Verificare che sia installata la versione Java corretta. Le note di rilascio di Cisco ASDM elencano i requisiti per le versioni Java verificate.
8.
9. Cancellare la cache Java. Nel **Pannello di controllo Java**, scegliete **Generale > File Internet temporaneo**. Quindi, fare clic su **View** per avviare un **visualizzatore cache Java**. Eliminare tutte le voci che fanno riferimento o sono correlate ad ASDM.
10.
11. Se questi passaggi hanno esito negativo, raccogliere le informazioni di debug dal computer client per ulteriori informazioni. Abilitare il debug per ASDM con l'URL: **https://<indirizzo IP dell'appliance ASA>?debug=5, ad esempio https://10.0.0.1?debug=5**.

    Con Java versione 6 (detta anche versione 1.6), i messaggi di debug Java sono abilitati da **Java Control Panel > Advanced**. Selezionare quindi le caselle di controllo in **Debug**. Non selezionare **Non avviare console** nella **console Java**. Il debug Java deve essere abilitato prima dell'avvio di ASDM.



L'output della console Java viene registrato nella directory **.asdm/log** della home directory dell'utente. I log ASDM si trovano anche nella stessa directory. In Windows 7, ad esempio, i registri si trovano in **C:\Users\<nomeutente>/.asdm/log/**.

Esegui comandi con HTTPS

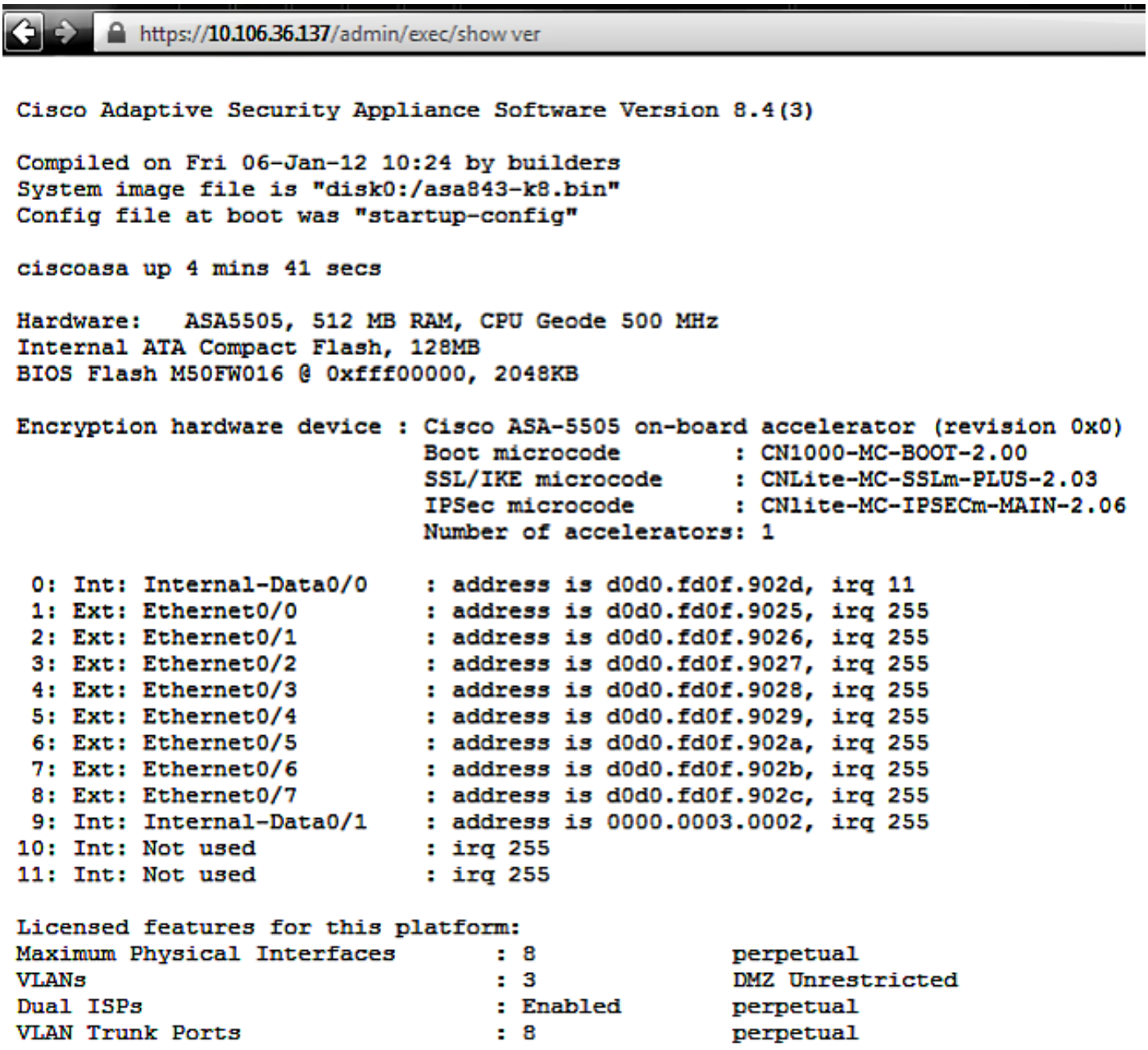
Questa procedura aiuta a determinare eventuali problemi di layer 7 per il canale HTTP. Queste informazioni si rivelano utili quando l'applicazione ASDM in sé non è accessibile e non è disponibile alcun accesso CLI per gestire il dispositivo.

L'URL usato per accedere alla pagina di avvio Web di ASDM può essere usato anche per eseguire qualsiasi comando a livello di configurazione sull'appliance ASA. Questo URL può essere usato per apportare modifiche alla configurazione di base dell'ASA, compresa la possibilità di ricaricare il dispositivo remoto. Per immettere un comando, utilizzare la seguente sintassi:

https://<indirizzo IP dell'appliance ASA>/admin/exec/<comando>

Se nel comando è presente uno spazio e il browser non è in grado di analizzare i caratteri spazio in un URL, è possibile utilizzare il segno **+** o **%20** per indicare lo spazio.

Ad esempio, **https://10.106.36.137/admin/exec/show ver** restituisce un output show version per il browser:



Questo metodo di esecuzione del comando richiede che il server HTTP sia abilitato sull'appliance ASA e che le restrizioni HTTP necessarie siano attive. Tuttavia, questa operazione NON richiede la presenza di un'immagine ASDM sull'appliance ASA.

Informazioni correlate

- Configurazione dell'accesso ASDM per gli accessori
- ASA 5500-x: ASDM e altre funzioni SSL non funzionano subito
- Note sulla release di Cisco ASDM
- Pagina delle licenze Cisco per ottenere una licenza 3DES/AES sull'appliance ASA
- Documentazione e supporto tecnico – Cisco Systems