Problemas de conexión ASA al Cisco Adaptive Security Device Manager

Contenido

Introducción

Este documento proporciona la metodología de solución de problemas necesaria para examinar los problemas a los que se enfrenta al acceder/configurar Cisco Adaptive Security Appliance (ASA) con Cisco Adaptive Security Device Manager (ASDM). ASDM ofrece servicios de gestión y supervisión de seguridad para dispositivos de seguridad a través de una interfaz gráfica de gestión.

Prerequisites

Requirements

Los escenarios, síntomas y pasos enumerados en este documento se escriben para solucionar problemas después de que la configuración inicial se haya configurado en el ASA. Para la configuración inicial, refiérase a la sección Configuración del Acceso ASDM para Dispositivos de la Guía de Configuración de Cisco ASA Series General Operations ASDM, 7.1.

Este documento utiliza ASA CLI para la resolución de problemas, que requiere acceso Secure Shell (SSH)/Telnet/Console al ASA.

Componentes Utilizados

La información en este documento se basa en el ASDM y ASA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Metodología de solución de problemas

Hay tres puntos de falla principales en los que se centra este documento de troubleshooting. Si se adhiere al proceso general de resolución de problemas en este orden, este documento debe ayudarle a determinar el problema exacto con el uso/acceso de ASDM.

- **Configuración ASA**
- **Conectividad de red**
- **Software de aplicación**

Configuración ASA

Hay tres configuraciones esenciales presentes en el ASA que se necesitan para acceder correctamente al ASDM:

- Imagen ASDM en Flash
- Imagen ASDM en uso
- Restricciones del servidor HTTP

Imagen ASDM en Flash

Asegúrese de que la versión requerida del ASDM se cargue en la memoria flash. Se puede cargar con la versión ejecutada actualmente del ASDM o con otros métodos convencionales de transferencia de archivos al ASA, como TFTP.

Ingrese **show flash** en la CLI de ASA para ayudarlo a enumerar los archivos presentes en la memoria flash de ASA. Verifique la presencia del archivo 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
```

Para verificar más a fondo si la imagen presente en la memoria flash es válida y no está dañada, puede utilizar el comando **verify** para comparar el hash MD5 almacenado en el paquete de software y el hash MD5 del archivo real 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
```

Este paso debe ayudarle a verificar si la imagen está presente y su integridad en el ASA.

Imagen ASDM en uso

Este proceso se define en la configuración de ASDM en el ASA. Una definición de configuración de ejemplo de la imagen actual que se utiliza tiene el siguiente aspecto:

asdm image disk0:/asdm-702.bin

Para verificar más a fondo, también puede utilizar el comando **show asdm image**:

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

Restricciones del servidor HTTP

Este paso es esencial en la configuración de ASDM, porque define qué redes tienen acceso al ASA. Una configuración de ejemplo es similar a la siguiente:

```
http server enable
http 192.168.1.0 255.255.255.0 inside

http 64.0.0.0 255.0.0.0 outside
```

Verifique que tenga las redes necesarias definidas en la configuración anterior. La ausencia de esas definiciones hace que el punto de ejecución de ASDM se agote mientras se conecta y da este error:

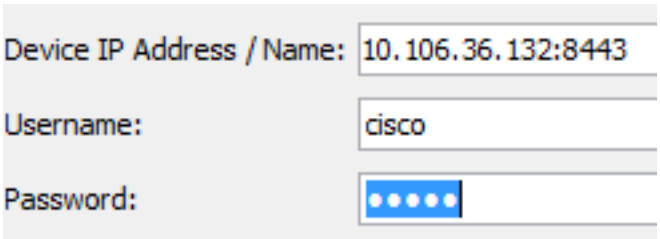
La página de inicio de ASDM (**https://<dirección IP de ASA>/admin**) hace que la solicitud se agote y no se muestra ninguna página.

Verifique además que el servidor HTTP utilice un puerto no estándar para la conexión ASDM, como 8443. Esto se resalta en la configuración:

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

http server enable 8443

Si utiliza un puerto no estándar, debe especificar el puerto cuando se conecta al ASA en el punto de ejecución ASDM como:



Esto también se aplica cuando se accede a la página de inicio de ASDM:
https://10.106.36.132:8443/admin

Otros problemas de configuración posibles

Después de completar los pasos anteriores, el ASDM debe abrirse si todo funciona en el lado del cliente. Sin embargo, si aún experimenta problemas, abra el ASDM desde otra máquina. Si tiene éxito, el problema probablemente se encuentre en el nivel de la aplicación y la configuración de ASA sea correcta. Sin embargo, si todavía no se inicia, complete estos pasos para verificar las configuraciones del lado de ASA:

1. Verifique la configuración de Secure Sockets Layer (SSL) en ASA. ASDM utiliza SSL mientras se comunica con ASA. Según la forma en que se inicie el ASDM, es posible que el software de sistema operativo más reciente no permita el uso de cifras más débiles cuando negocia sesiones SSL.

   Verifique qué cifras están permitidas en el ASA y si alguna versión SSL específica se especifica en la configuración con el 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
   ```

   Si hay algún error de negociación de cifrado SSL mientras se inicia el ASDM, se muestran en los registros de 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
   ```

   Si ve una configuración específica, vuelva a la predeterminada.

   Tenga en cuenta que la licencia VPN-3DES-AES debe estar habilitada en ASA para que los cifrados 3DES y AES sean utilizados por ASA en la configuración. Esto se puede verificar con el comando **show version** en la CLI. El resultado se muestra de la siguiente manera:

   ```
   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>
   ```

   Se puede obtener una licencia VPN-3DES-AES sin coste alguno del sitio web de licencias de Cisco. Haga clic en **Productos de seguridad** y luego elija **Licencia 3DES/AES de Cisco ASA**.

   Nota: En las nuevas plataformas ASA 5500-X que se envían con código 8.6/9.x, la configuración del cifrado SSL se establece en **des-sha1** de forma predeterminada, lo que hace que las sesiones ASDM no funcionen. Consulte el ASA 5500-x: ASDM y otras funciones SSL no funcionan desde el artículo de caja para obtener más información.
2. Verifique que WebVPN esté habilitado en el ASA. Si está habilitado, debe utilizar esta URL (**https://10.106.36.132/admin**) para acceder a ella cuando acceda a la página de inicio web de ASDM.
3.
4. Compruebe si hay una configuración de traducción de direcciones de red (NAT) en el ASA para el puerto 443. Esto hace que el ASA no procese las solicitudes de ASDM sino que las envíe a la red/interfaz para la cual se ha configurado la NAT.
5.
6. Si todo se verifica y el ASDM aún se agota, verifique que el ASA esté configurado para

escuchar en el puerto definido para ASDM con el comando **show asp table socket** en la CLI de ASA. El resultado debe mostrar que el ASA escucha en el puerto ASDM:

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

Si no se muestra este resultado, quite y vuelva a aplicar la configuración del servidor HTTP en el ASA para reiniciar el socket en el software ASA.

7.
8. Si experimenta problemas al iniciar sesión o autenticarse en el ASDM, verifique que las opciones de autenticación para **HTTP** estén configuradas correctamente. Si no se establece ningún comando de autenticación, puede utilizar la contraseña de habilitación de ASA para iniciar sesión en el ASDM. Si desea habilitar la autenticación basada en nombre de usuario/contraseña, debe ingresar esta configuración para autenticar las sesiones ASDM/HTTP al ASA desde la base de datos de nombre de usuario/contraseña de ASA:

   ```
   aaa authentication http console LOCAL
   ```

   Recuerde crear un nombre de usuario/contraseña cuando habilite el comando anterior:

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

   Si ninguno de estos pasos ayuda, estas opciones de depuración están disponibles en el ASA para una investigación adicional:

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

Conectividad de red

Si ha completado la sección anterior y aún no puede acceder al ASDM, el siguiente paso es verificar la conectividad de red a su ASA desde la máquina desde la que desea acceder al ASDM. Hay algunos pasos básicos de troubleshooting para verificar que el ASA recibe la solicitud del equipo cliente:

1. **Prueba con el protocolo de mensajes de control de Internet (ICMP)**.
   Haga ping en la interfaz ASA desde la que desea acceder al ASDM. El ping debe ser exitoso si se permite que ICMP atraviese su red y no hay restricciones en el nivel de interfaz ASA. Si el ping falla, probablemente se deba a un problema de comunicación entre el ASA y la máquina cliente. Sin embargo, este no es un paso decisivo para determinar que existe ese tipo de problema de comunicación.
2.
3. **Confirme con captura de paquetes**.
   Coloque una captura de paquetes en la interfaz desde la que desea acceder al ASDM. La captura debe mostrar que los paquetes TCP destinados a la dirección IP de la interfaz llegan con el número de puerto de destino 443 (predeterminado).

   Para configurar una captura, utilice este 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
```

Esto captura cualquier tráfico TCP que llegue al puerto 443 en la interfaz ASA desde la cual se conecta al ASDM. Conéctese a través de ASDM en este momento o abra la página de lanzamiento web de ASDM. A continuación, utilice el comando **show capture asdm_test** para ver el resultado de los paquetes capturados:

```
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>
```

Esta captura muestra una solicitud de sincronización (SYN) de la máquina cliente al ASA, pero el ASA no envía ninguna respuesta. Si ve una captura similar a la anterior, significa que los paquetes llegan al ASA pero el ASA no responde a esas solicitudes, lo que aísla el problema al propio ASA. Consulte la primera sección de este documento para resolver problemas adicionales.

Sin embargo, si no ve un resultado similar al anterior y no se captura ningún paquete, significa que hay un problema de conectividad entre el ASA y la máquina cliente ASDM. Verifique que no haya dispositivos intermedios que puedan bloquear el tráfico del puerto TCP 443 y que no haya ninguna configuración del navegador, como la configuración Proxy, que pudiera impedir que el tráfico llegue al ASA.

Por lo general, la captura de paquetes es una buena manera de determinar si la trayectoria hacia el ASA es clara y si es posible que no se necesiten más diagnósticos para descartar los problemas de conectividad de red.

Software de aplicación

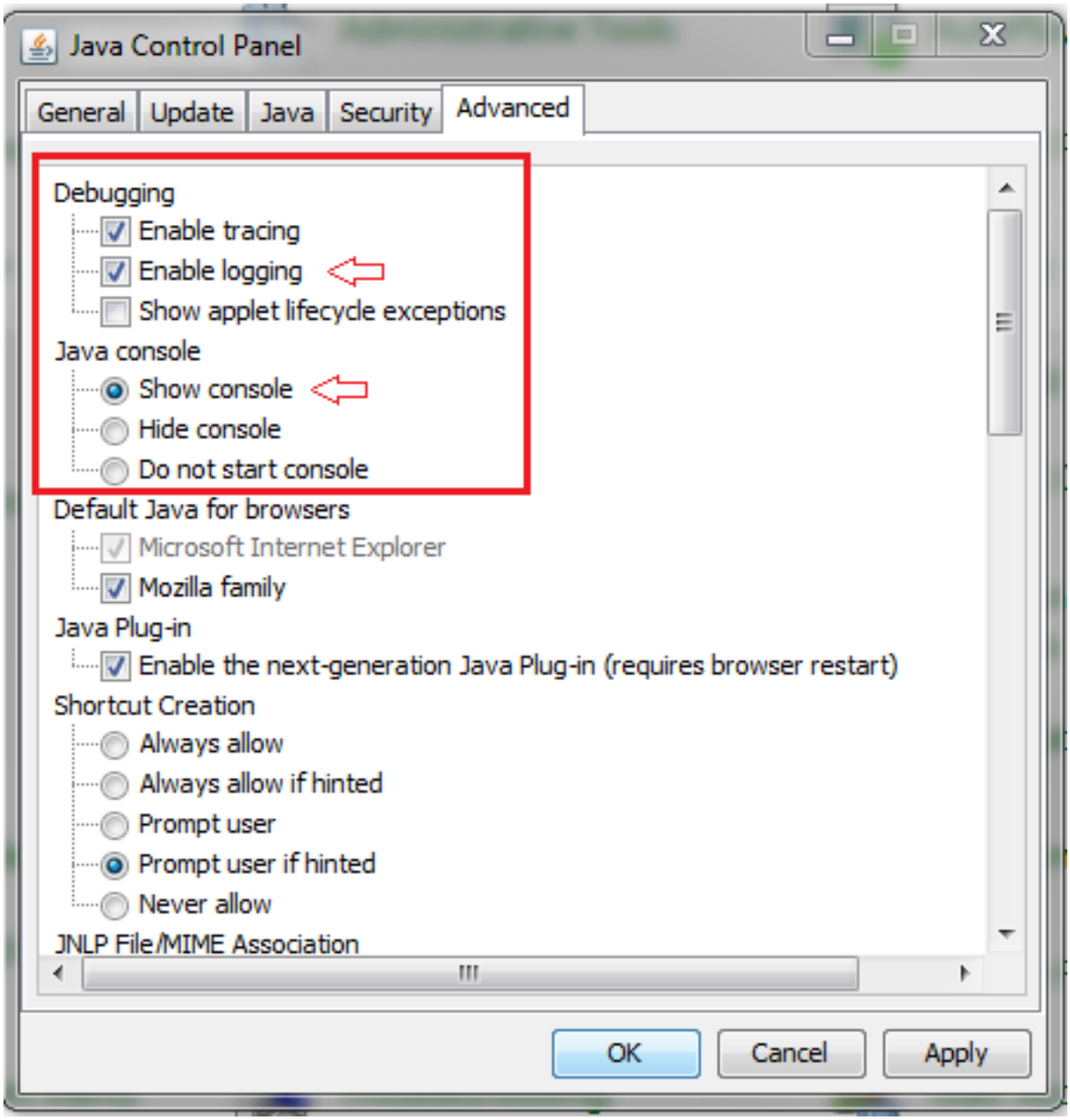
Esta sección describe cómo resolver problemas del software de punto de ejecución ASDM que se ha instalado en el equipo cliente cuando no se puede iniciar/cargar. El punto de ejecución ASDM es el componente que reside en la máquina cliente y se conecta con el ASA para recuperar la imagen ASDM. Una vez recuperada, la imagen ASDM se almacena generalmente en la memoria caché y se toma de ella hasta que se observa algún cambio en el lado ASA, como una actualización de la imagen ASDM.

Complete estos pasos básicos de troubleshooting para descartar cualquier problema en el equipo cliente:

1. Abra la página de inicio de ASDM desde otra máquina. Si se inicia, significa que el problema es con la máquina cliente en cuestión. Si falla, siga la guía de resolución de problemas desde el principio para aislar los componentes involucrados en orden.

2.
3. Abra el ASDM mediante el lanzamiento web e inicie el software directamente desde allí. Si tiene éxito, es probable que haya problemas con la instalación del punto de ejecución de ASDM. Desinstale el punto de ejecución ASDM del equipo cliente y vuelva a instalarlo desde el lanzamiento web de ASA.
4.
5. Borre el directorio de caché del ASDM en el directorio principal del usuario. Por ejemplo, en Windows 7, se encuentra aquí: **C:\Users\<username>\.asdm\cache**. La memoria caché se borra cuando elimina el directorio **caché** completo. Si el ASDM se inicia correctamente, también puede borrar la memoria caché desde el menú **Archivo** ASDM.
6.
7. Verifique que se haya instalado la versión Java adecuada. Las notas de la versión de Cisco ASDM enumeran los requisitos para las versiones de Java probadas.
8.
9. Borre la memoria caché de Java. En el **Panel de control de Java**, elija **General > Archivo de Internet temporal**. A continuación, haga clic en **Ver** para iniciar un **Java Cache Viewer**. Elimine todas las entradas que hacen referencia al ASDM o que están relacionadas con él.
10.
11. Si estos pasos fallan, recopile la información de depuración del equipo cliente para una investigación más detallada. Habilitar depuración para ASDM con la URL: **https://<dirección IP del ASA>?debug=5, por ejemplo https://10.0.0.1?debug=5**.

    Con Java Versión 6 (también llamada Versión 1.6), los mensajes de depuración de Java se habilitan desde **Java Control Panel > Avanzado**. A continuación, active las casillas de verificación en **Depuración**. No seleccione **No iniciar consola** en la **consola Java**. La depuración de Java debe estar habilitada antes de que se inicie ASDM.



La salida de la consola Java se registra en el directorio **.asdm/log** del directorio principal del usuario. Los registros ASDM también se pueden encontrar en el mismo directorio. Por ejemplo, en Windows 7, los registros se encuentran en **C:\Users\<username>/.asdm/log/**.

Ejecutar comandos con HTTPS

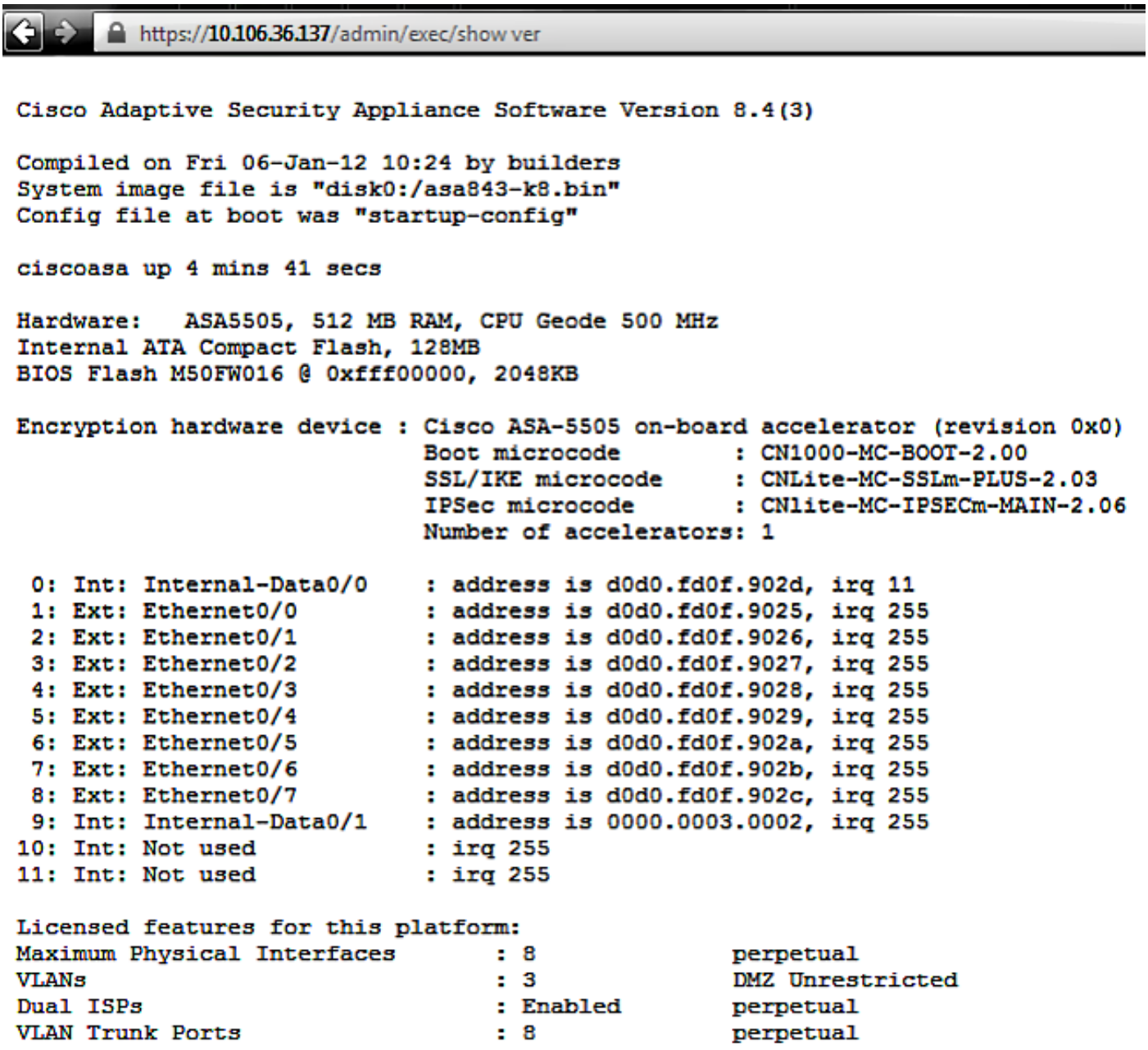
Este procedimiento ayuda a determinar cualquier problema de Capa 7 para el canal HTTP. Esta información resulta útil cuando se encuentra en una situación en la que la aplicación ASDM en sí no es accesible y no hay ningún acceso CLI disponible para administrar el dispositivo.

La URL que se utiliza para acceder a la página de inicio web de ASDM también se puede utilizar para ejecutar cualquier comando de nivel de configuración en el ASA. Esta URL se puede utilizar para realizar cambios de configuración a nivel básico en el ASA, que incluye una recarga de dispositivo remoto. Para ingresar un comando, utilice esta sintaxis:

https://<dirección IP del ASA>/admin/exec/<comando>

Si hay un espacio en el comando y el explorador no puede analizar los caracteres de espacio en una dirección URL, puede utilizar el signo **+** o **%20** para indicar el espacio.

Por ejemplo, **https://10.106.36.137/admin/exec/show ver** da como resultado un resultado de show version en el navegador:



Este método de ejecución de comandos requiere que el servidor HTTP esté habilitado en el ASA y tenga activas las restricciones HTTP necesarias. Sin embargo, esto NO requiere que una imagen ASDM esté presente en el ASA.

Información Relacionada

- Configuración del Acceso ASDM para Dispositivos
- ASA 5500-x: ASDM y otras funciones SSL no funcionan de forma inmediata
- Notas de la versión de Cisco ASDM
- Página de licencia de Cisco para obtener una licencia 3DES/AES en ASA
- Soporte Técnico y Documentación - Cisco Systems