Problemas de conexão do ASA com o Cisco Adaptive Security Device Manager

Contents

Introduction

Este documento fornece a metodologia de solução de problemas necessária para examinar problemas enfrentados ao acessar/configurar o Cisco Adaptive Security Appliance (ASA) com o Cisco Adaptive Security Device Manager (ASDM). O ASDM oferece serviços de gerenciamento e monitoramento de segurança para dispositivos de segurança por meio de uma interface gráfica de gerenciamento.

Prerequisites

Requirements

Os cenários, sintomas e etapas listados neste documento são escritos para solução de problemas após a configuração inicial no ASA. Para obter a configuração inicial, consulte a seção Configurando o acesso ASDM para dispositivos do Guia de Configuração ASDM de Operações Gerais do Cisco ASA Series, 7.1.

Este documento usa a CLI do ASA para solução de problemas, que exige acesso de Shell Seguro (SSH)/Telnet/Console ao ASA.

Componentes Utilizados

As informações neste documento são baseadas no ASDM e no 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.

Metodologia de solução de problemas

Há três pontos principais de falha nos quais este documento de solução de problemas se concentra. Se você aderir ao processo geral de solução de problemas nesta ordem, este documento deve ajudá-lo a determinar o problema exato com o uso/acesso do ASDM.

- **Configuração do ASA**
- **Conectividade de rede**
- **Software de aplicativo**

Configuração do ASA

Há três configurações essenciais que estão presentes no ASA necessárias para acessar o ASDM com êxito:

- Imagem ASDM em Flash
- Imagem ASDM em uso
- Restrições de Servidor HTTP

Imagem ASDM em Flash

Certifique-se de que a versão necessária do ASDM esteja carregada na memória flash. Ele pode ser carregado com a versão atualmente executada do ASDM ou com outros métodos convencionais de transferência de arquivos para o ASA, como o TFTP.

Insira **show flash** no ASA CLI para ajudá-lo a listar os arquivos presentes na memória flash do ASA. Verifique a presença do arquivo 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 se a imagem presente na memória flash é válida e não está corrompida, você pode usar o **verify** para comparar o hash MD5 armazenado no pacote de software e o hash MD5 do arquivo 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
```

Esta etapa deve ajudá-lo a verificar se a imagem está presente e sua integridade no ASA.

Imagem ASDM em uso

Esse processo é definido na configuração do ASDM no ASA. Um exemplo de definição de configuração da imagem atual que é usada é semelhante a este:

asdm image disk0:/asdm-702.bin

Para verificar melhor, você também pode usar o comando **show asdm image**:

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

Restrições de Servidor HTTP

Essa etapa é essencial na configuração do ASDM, pois define quais redes têm acesso ao ASA. Um exemplo de configuração é semelhante a:

```
http server enable
http 192.168.1.0 255.255.255.0 inside

http 64.0.0.0 255.0.0.0 outside
```

Verifique se você tem as redes necessárias definidas na configuração anterior. A ausência dessas definições faz com que o iniciador ASDM exceda o tempo limite enquanto se conecta e apresenta este erro:

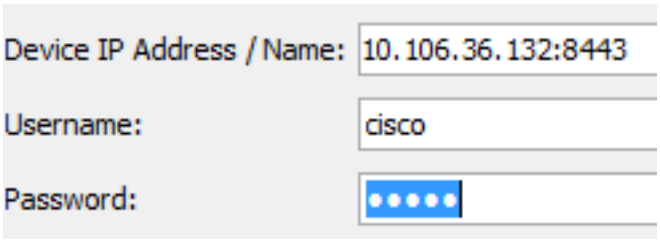
A página de lançamento do ASDM (**https://<endereço IP do ASA>/admin**) faz com que o tempo limite da solicitação seja excedido e nenhuma página é exibida.

Verifique ainda se o servidor HTTP usa uma porta não padrão para a conexão ASDM, como 8443. Isso é destacado na configuração:

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

http server enable 8443

Se ela usar uma porta fora do padrão, você precisará especificar a porta quando se conectar ao ASA no iniciador ASDM como:



Isso também se aplica a quando você acessa a página inicial do ASDM:
https://10.106.36.132:8443/admin

Outros possíveis problemas de configuração

Depois de concluir as etapas anteriores, o ASDM deverá abrir se tudo estiver funcionando no lado do cliente. No entanto, se ainda tiver problemas, abra o ASDM de outra máquina. Se você for bem-sucedido, o problema provavelmente está no nível do aplicativo e a configuração do ASA está boa. No entanto, se ainda não for iniciado, faça o seguinte para verificar ainda mais as configurações do ASA:

1. Verifique a configuração SSL (Secure Sockets Layer) no ASA. O ASDM usa SSL enquanto se comunica com o ASA. Com base na forma como o ASDM é iniciado, o software de SO mais recente pode não permitir o uso de cifras mais fracas quando negocia sessões SSL.

   Verifique quais cifras são permitidas no ASA e se alguma versão SSL específica é especificada na configuração com o 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
   ```

   Se houver algum erro de negociação de cifras SSL enquanto o ASDM é iniciado, eles serão exibidos nos registros do 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 você vir configurações específicas, reverta-as para o padrão.

   Observe que a licença VPN-3DES-AES precisa ser habilitada no ASA para os cifras 3DES e AES a serem usados pelo ASA na configuração. Isso pode ser verificado com o comando **show version** na CLI. A saída é como esta:

   ```
   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>
   ```

   Uma licença VPN-3DES-AES pode ser obtida sem nenhum custo do site de licenciamento da Cisco. Clique em **Produtos de segurança** e escolha **Cisco ASA 3DES/AES License**.
   Note: Nas novas plataformas ASA 5500-X fornecidas com código 8.6/9.x, as configurações de cifra SSL são definidas como **des-sha1** por padrão, o que faz com que as sessões ASDM não funcionem. Consulte o ASA 5500-x: O ASDM e outras funções SSL não funcionam no artigo original para obter mais informações.
2. Verifique se a WebVPN está habilitada no ASA. Se estiver ativado, você precisará usar este URL (**https://10.106.36.132/admin**) para acessá-lo quando acessar a página de inicialização da Web do ASDM.
3.
4. Verifique a configuração de NAT (Network Address Translation, tradução de endereço de rede) no ASA para a porta 443. Isso faz com que o ASA não processe as solicitações do ASDM, mas as envie para a rede/interface para a qual o NAT foi configurado.
5.
6. Se tudo for verificado e o ASDM ainda expirar, verifique se o ASA está configurado para ouvir na porta definida para ASDM com o comando **show asp table socket** na CLI do ASA. A saída deve mostrar que o ASA escuta na porta ASDM:

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

Se essa saída não for exibida, remova e reaplique a configuração do servidor HTTP no ASA para redefinir o soquete no software ASA.

7.
8. Se você tiver problemas ao fazer login/autenticar no ASDM, verifique se as opções de autenticação para **HTTP** estão configuradas corretamente. Se nenhum comando de autenticação estiver definido, você poderá usar a senha de ativação do ASA para fazer login no ASDM. Se quiser habilitar a autenticação baseada em nome de usuário/senha, você precisa inserir esta configuração para autenticar sessões ASDM/HTTP para o ASA a partir do banco de dados de nome de usuário/senha do ASA:

   aaa authentication http console LOCAL

   Lembre-se de criar um nome de usuário/senha ao habilitar o comando anterior:

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

   Se nenhuma dessas etapas ajudar, essas opções de depuração estão disponíveis no ASA para investigação adicional:

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

Conectividade de rede

Se você tiver concluído a seção anterior e ainda não puder acessar o ASDM, a próxima etapa será verificar a conectividade de rede com o ASA da máquina a partir da qual deseja acessar o ASDM. Há algumas etapas básicas de Troubleshooting para verificar se o ASA recebe a solicitação da máquina cliente:

1. **Teste com o ICMP (Internet Control Message Protocol)**.
   Faça ping na interface ASA da qual você deseja acessar o ASDM. O ping deve ser bem-sucedido se o ICMP tiver permissão para atravessar sua rede e não houver restrições no nível de interface do ASA. Se o ping falhar, provavelmente é porque há um problema de comunicação entre o ASA e a máquina cliente. No entanto, essa não é uma etapa conclusiva para determinar se há esse tipo de problema de comunicação.
2.
3. **Confirme com a captura de pacotes**.
   Coloque uma captura de pacote na interface da qual deseja acessar o ASDM. A captura deve mostrar que os pacotes TCP destinados ao endereço IP da interface chegam com o número de porta destino 443 (padrão).

   Para configurar uma captura, use 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
```

Isso captura todo o tráfego TCP que vem para a porta 443 na interface ASA a partir da qual você se conecta ao ASDM. Conecte-se via ASDM neste momento ou abra a página de inicialização da Web do ASDM. Em seguida, use o comando **show capture asdm_test** para ver o resultado dos pacotes 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>
```

Essa captura mostra uma solicitação de sincronização (SYN) da máquina cliente para o ASA, mas o ASA não envia resposta. Se você vir uma captura semelhante à anterior, significa que os pacotes chegam ao ASA, mas o ASA não responde a essas solicitações, o que isola o problema para o próprio ASA. Consulte a primeira seção deste documento para fazer troubleshooting adicional.

No entanto, se você não vir uma saída semelhante à anterior e nenhum pacote for capturado, isso significa que há um problema de conectividade entre o ASA e a máquina cliente ASDM. Verifique se não há dispositivos intermediários que possam bloquear o tráfego da porta TCP 443 e se não há configurações do navegador, como configurações de Proxy, que possam impedir que o tráfego acesse o ASA.

Geralmente, a captura de pacotes é uma boa maneira de determinar se o caminho para o ASA está limpo e se não será necessário mais diagnósticos para excluir problemas de conectividade de rede.

Software de aplicativo

Esta seção descreve como solucionar problemas do software iniciador do ASDM que foi instalado na máquina cliente quando ele falha ao iniciar/carregar. O iniciador ASDM é o componente que reside na máquina cliente e se conecta ao ASA para recuperar a imagem do ASDM. Depois de recuperada, a imagem do ASDM é geralmente armazenada em cache e é tirada de lá até que qualquer alteração seja percebida no lado do ASA, como uma atualização de imagem do ASDM.

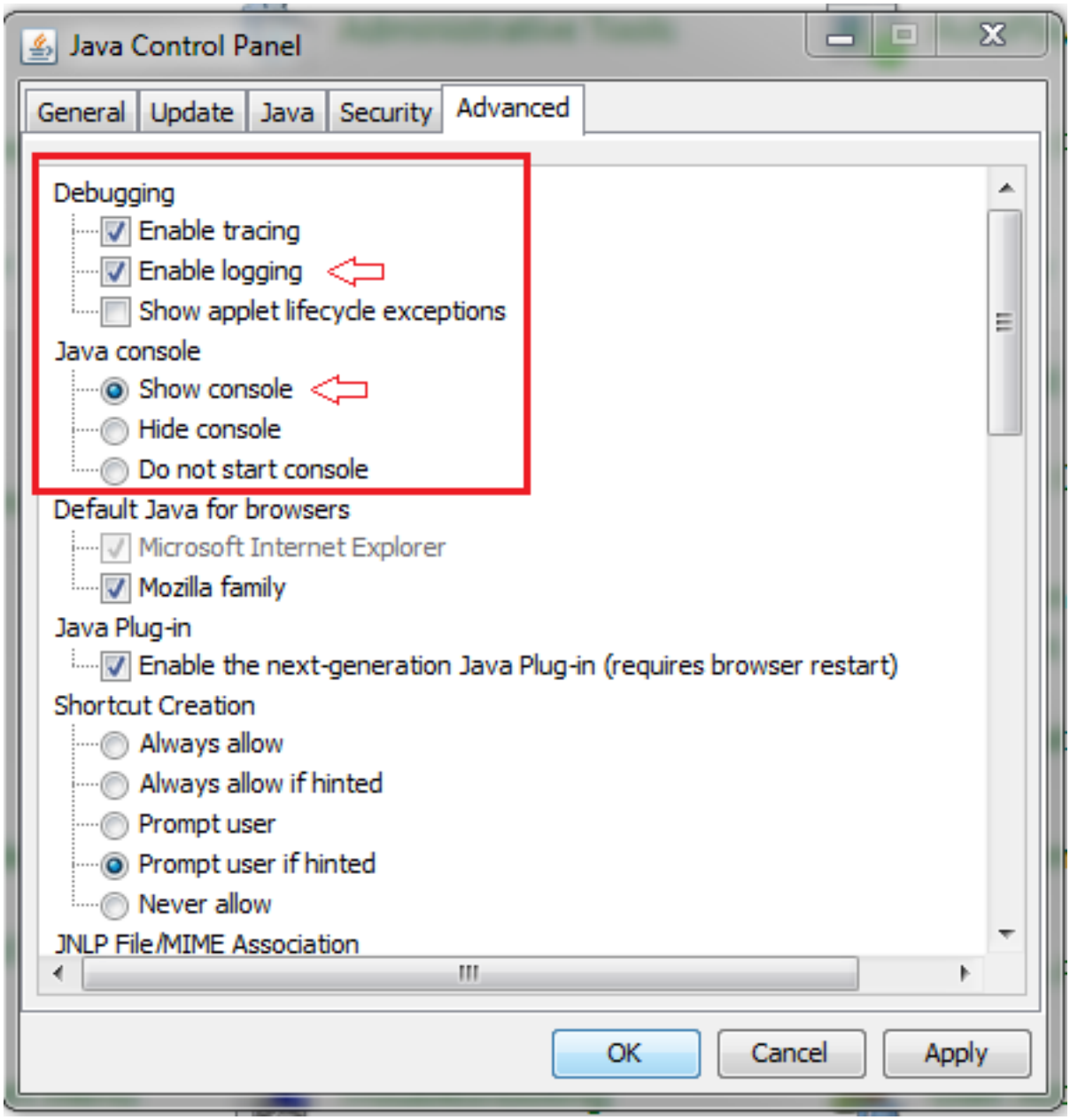
Conclua estas etapas básicas de solução de problemas para excluir quaisquer problemas na máquina cliente:

1. Abra a página de lançamento do ASDM de outra máquina. Se for iniciado, significa que o problema está na máquina cliente em questão. Se falhar, siga o guia de solução de problemas desde o início para isolar os componentes envolvidos na ordem.
2.
3. Abra o ASDM por meio do lançamento na Web e inicie o software diretamente a partir daí. Se for bem-sucedido, é provável que haja problemas com a instalação do iniciador ASDM. Desinstale o iniciador do ASDM da máquina cliente e reinstale-o a partir do próprio

lançamento da Web do ASA.

4.
5. Limpe o diretório de cache do ASDM no diretório inicial do usuário. Por exemplo, no Windows 7, ele está localizado aqui: **C:\Users\<nome de usuário>\.asdm\cache**. O cache é limpo quando você exclui todo o diretório **do cache**. Se o ASDM for iniciado com êxito, você também poderá limpar o cache no menu **Arquivo** ASDM.
6.
7. Verifique se a versão Java correta está instalada. As Notas de versão do Cisco ASDM listam os requisitos para versões de Java testadas.
8.
9. Limpe o cache Java. No **Painel de controle Java**, escolha **Geral > Arquivo temporário de Internet**. Em seguida, clique em **View** para iniciar um **Java Cache Viewer**. Exclua todas as entradas referentes ao ASDM ou relacionadas a ele.
10.
11. Se essas etapas falharem, colete as informações de depuração da máquina cliente para uma investigação mais detalhada. Ative a depuração para ASDM com o URL: **https://<endereço IP do ASA>?debug=5, por exemplo, https://10.0.0.1?debug=5**.

    Com o Java Versão 6 (também chamado de Versão 1.6), as mensagens de depuração do Java são ativadas a partir do **Painel de Controle do Java > Avançado**. Em seguida, marque as caixas de seleção em **Debugging (Depuração)**. Não selecione **Não iniciar console** no **console Java**. A depuração do Java deve ser ativada antes do ASDM iniciar.



A saída do console Java é gravada no diretório **.asdm/log** do diretório home do usuário. Os registros ASDM também podem ser encontrados no mesmo diretório. Por exemplo, no Windows 7, os registros estão em **C:\Users\<username>/.asdm/log/**.

Executar comandos com HTTPS

Este procedimento ajuda a determinar quaisquer problemas da Camada 7 para o canal HTTP. Essas informações se mostram úteis quando você está em uma situação em que o aplicativo ASDM em si não está acessível e não há nenhum acesso CLI disponível para gerenciar o dispositivo.

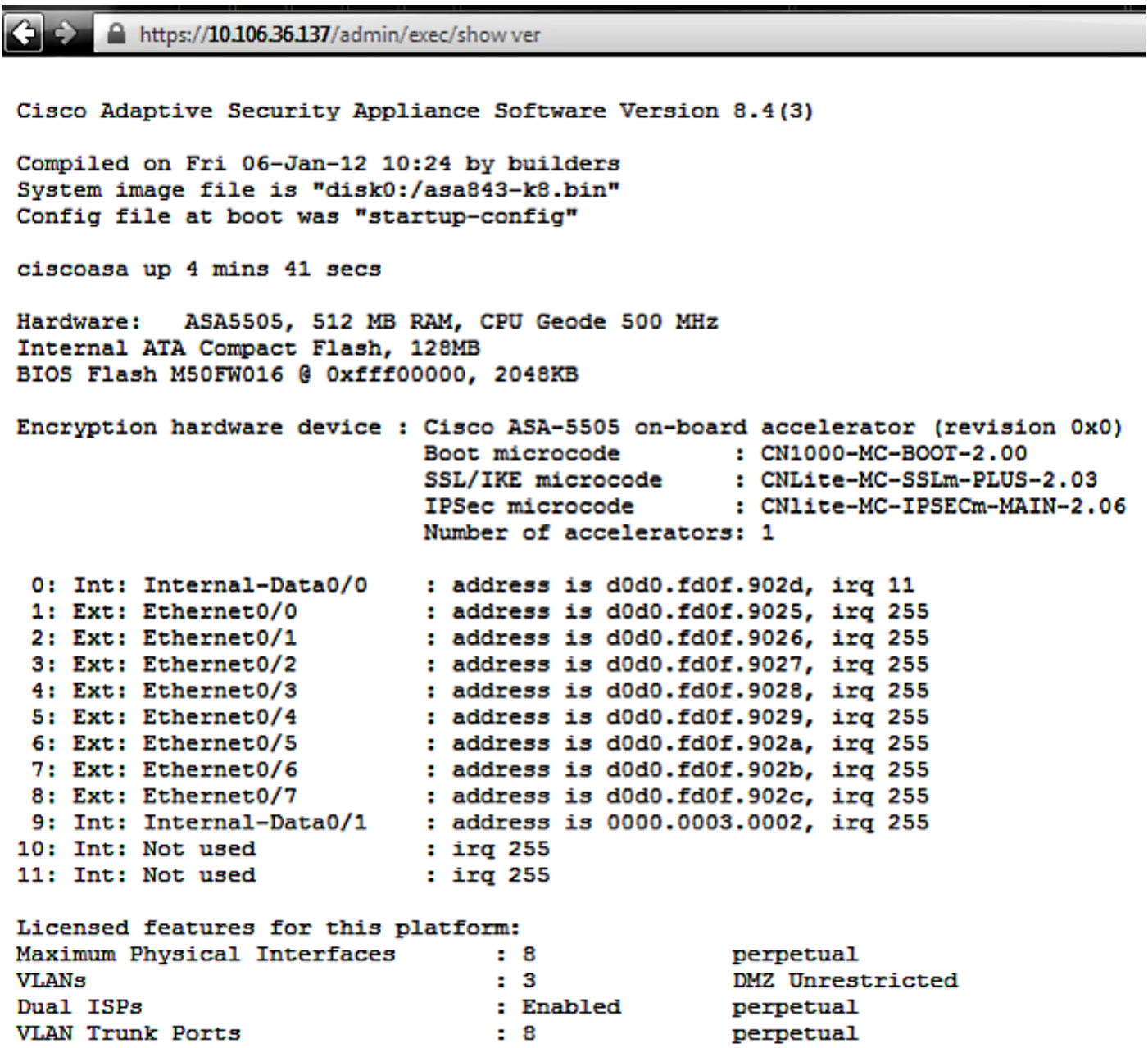
O URL usado para acessar a página de lançamento da Web do ASDM também pode ser usado para executar qualquer comando de nível de configuração no ASA. Esse URL pode ser usado para fazer alterações de configuração em um nível básico no ASA, que inclui um recarregamento de dispositivo remoto. Para inserir um comando, use esta sintaxe:

https://<endereço IP do ASA>/admin/exec/<comando>

Se houver um espaço no comando e o navegador não puder analisar caracteres de espaço em

uma URL, você poderá usar o **+** sinal ou **%20** para indicar o espaço.

Por exemplo, **https://10.106.36.137/admin/exec/show** resulta em uma saída show version para o navegador:



Esse método de execução de comando exige que o servidor HTTP esteja ativado no ASA e tenha as restrições HTTP necessárias ativas. No entanto, isso NÃO exige que uma imagem ASDM esteja presente no ASA.

Informações Relacionadas

- Configurando o acesso ASDM para dispositivos
- ASA 5500-x: A função ASDM e outras funções SSL não funcionam fora da caixa
- Notas da versão do Cisco ASDM
- Página de licença da Cisco para obter uma licença 3DES/AES no ASA
- Suporte Técnico e Documentação - Cisco Systems