Dépannage des problèmes de connexion ASA sur ASDM

Table des matières

Introduction

Ce document décrit la méthodologie de dépannage nécessaire pour examiner les problèmes rencontrés lorsque vous accédez à/configurez Cisco ASA avec Cisco ASDM.

Conditions préalables

Exigences

Les scénarios, symptômes et étapes répertoriés dans ce document sont écrits pour le dépannage des problèmes après la configuration initiale sur l'appliance de sécurité adaptative (ASA). Pour la configuration initiale, référez-vous à la section Configuration de l'accès ASDM pour les appareils du Guide de configuration de Cisco ASA Series General Operations Adaptive Security Device Manager (ASDM), 7.1.

Ce document utilise l'interface de ligne de commande ASA pour le dépannage, qui nécessite un accès SSH (Secure Shell)/Telnet/Console à l'ASA.

Composants utilisés

Les informations de ce document sont basées sur l'ASA et l'ASDM.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

ASDM fournit des services de gestion et de surveillance de la sécurité pour les appliances de sécurité via une interface de gestion graphique.

Méthodologie de dépannage

Ce document de dépannage se concentre sur trois points de défaillance majeurs. Si vous respectez la procédure de dépannage générale dans cet ordre, ce document peut vous aider à déterminer le problème exact de l'utilisation/de l'accès ASDM.

- Configuration ASA
- Connectivité réseau
- Application logicielle

Configuration ASA

Trois configurations essentielles sont présentes sur l'ASA et sont nécessaires pour accéder avec succès à l'ASDM :

- Image ASDM dans Flash
- Image ASDM utilisée
- Restrictions du serveur HTTP

Image ASDM dans Flash

Assurez-vous que la version requise de l'ASDM est téléchargée dans la mémoire flash. Il peut être téléchargé avec la version en cours d'exécution de l'ASDM ou avec d'autres méthodes classiques de transfert de fichiers vers l'ASA, telles que TFTP.

Entrez show flash sur l'interface de ligne de commande ASA afin de vous aider à répertorier les fichiers présents sur la mémoire flash ASA. Vérifiez la présence du fichier ASDM :

<#root>

```
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
```

Afin de vérifier si l'image présente sur la mémoire flash est valide et non corrompue, vous pouvez utiliser la commande verify afin de comparer le hachage MD5 stocké dans le package logiciel et le hachage MD5 du fichier réel présent :

<#root>

```
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
```

Cette étape peut vous aider à vérifier si l'image est présente et son intégrité sur l'ASA.

Image ASDM utilisée

Ce processus est défini dans la configuration ASDM sur l'ASA. Un exemple de définition de configuration de l'image actuelle utilisée ressemble à ceci :

asdm image disk0:/asdm-702.bin

Afin de vérifier davantage, vous pouvez également utiliser la commande show asdm image :

<#root>

```
ciscoasa# s
```

how asdm image

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

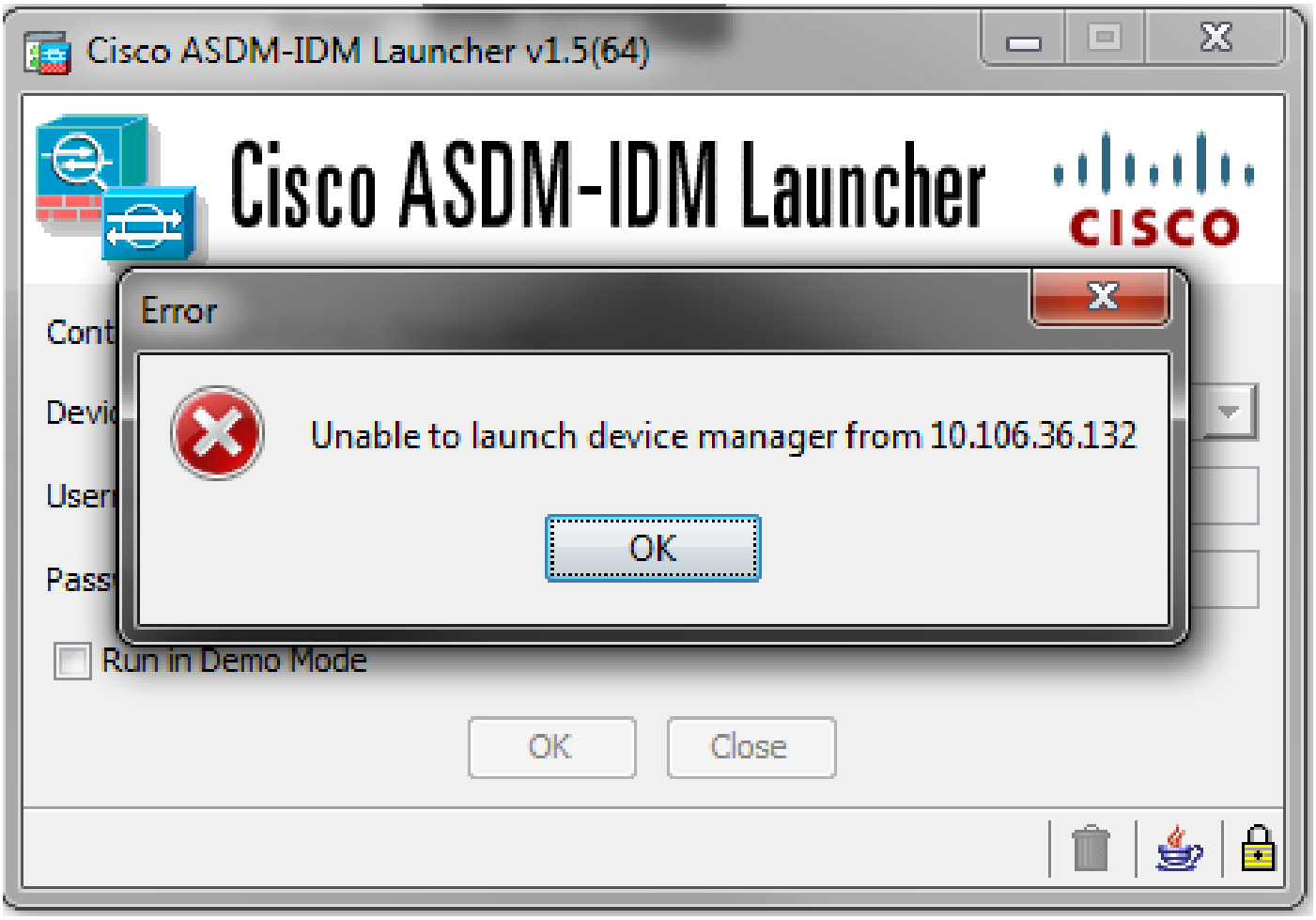
Restrictions du serveur HTTP

Cette étape est essentielle dans la configuration de l'ASDM, car elle définit quels réseaux ont accès à l'ASA. Voici un exemple de configuration :

```
http server enable
http 192.168.1.0 255.255.255.0 inside

http 10.0.0.1 255.0.0.0 outside
```

Vérifiez que vous disposez des réseaux nécessaires définis dans la configuration précédente. L'absence de ces définitions provoque le dépassement du délai d'attente du lanceur ASDM lors de la connexion et donne cette erreur :

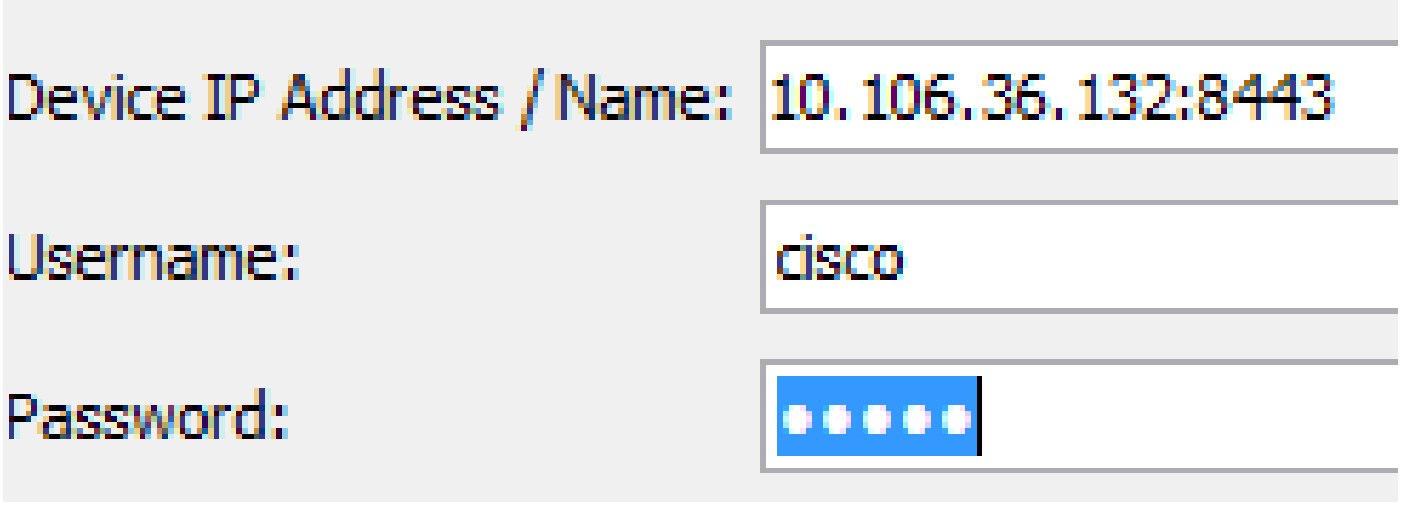


La page de lancement d'ASDM (https://<adresse IP ASA>/admin) provoque le dépassement du délai d'attente de la demande et aucune page ne s'affiche.

Vérifiez également que le serveur HTTP utilise un port non standard pour la connexion ASDM, tel que 8443. Ceci est mis en évidence dans la configuration :

ciscoasa(config)# show run http
http server enable 8443

S'il utilise un port non standard, vous devez spécifier le port lorsque vous vous connectez à l'ASA dans le lanceur ASDM comme suit :



Ceci s'applique également lorsque vous accédez à la page de lancement d'ASDM : https://10.106.36.132:8443/admin

Autres problèmes de configuration possibles

Une fois que vous avez terminé les étapes précédentes, l'ASDM peut s'ouvrir si tout est fonctionnel côté client. Toutefois, si vous rencontrez toujours des problèmes, ouvrez l'ASDM à partir d'une autre machine. Si vous réussissez, le problème se situe probablement au niveau de l'application et la configuration ASA est correcte. Toutefois, si le démarrage échoue toujours, procédez comme suit pour vérifier les configurations côté ASA :

1. Vérifiez la configuration SSL (Secure Sockets Layer) sur l'ASA. L'ASDM utilise SSL lorsqu'il communique avec l'ASA. D'après la façon dont ASDM est lancé, le nouveau logiciel du système d'exploitation ne peut pas autoriser l'utilisation de chiffrements plus faibles lorsqu'il négocie des sessions SSL. Vérifiez quels chiffrements sont autorisés sur l'ASA, et si des versions SSL spécifiques sont spécifiées dans la configuration avec la commande show run all ssl :

   <#root>

   ```
   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
   ```

   S'il y a des erreurs de négociation de chiffrement SSL pendant le lancement de l'ASDM, elles s'affichent dans les journaux 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:10.103.236.189/52501 to
   identity:10.106.36.132/443 duration 0:00:00 bytes 7 TCP Reset by appliance
   ```

Si des paramètres spécifiques s'affichent, rétablissez-les à leur valeur par défaut. Notez que la licence VPN-3DES-AES doit être activée sur l'ASA pour les chiffrements 3DES et AES à utiliser par l'ASA dans la configuration. Vous pouvez vérifier cela à l'aide de la commande show version sur l'interface de ligne de commande. Le résultat s'affiche comme suit :

```
<#root>

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>
```

Une licence VPN-3DES-AES peut être obtenue gratuitement sur le site Web de licence Cisco. Cliquez sur Security Products, puis choisissez Cisco ASA 3DES/AES License.

Remarque : sur les nouvelles plates-formes ASA 5500-X livrées avec le code 8.6/9.x, les paramètres de chiffrement SSL sont définis sur des-sha1 par défaut, ce qui empêche les sessions ASDM de fonctionner. Pour plus d'informations, reportez-vous à l'article ASA 5500-x : ASDM and other SSL function do not work out of the box.

---

2. Vérifiez que WebVPN est activé sur l'ASA. Si elle est activée, vous devez utiliser cette URL (https://10.106.36.132/admin) afin d'y accéder quand vous accédez à la page de lancement Web d'ASDM.
3. Recherchez une configuration NAT (Network Address Translation) sur l'ASA pour le port 443. Cela amène l'ASA à ne pas traiter les demandes d'ASDM, mais plutôt à les envoyer au réseau/à l'interface pour lequel la NAT a été configurée.
4. Si tout est vérifié et que l'ASDM expire toujours, vérifiez que l'ASA est configuré pour écouter sur le port défini pour l'ASDM avec la commande show asp table socket sur l'interface de ligne de commande ASA. Le résultat peut montrer que l'ASA écoute sur le port ASDM :

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

Si ce résultat ne s'affiche pas, supprimez et réappliquez la configuration du serveur HTTP sur l'ASA afin de réinitialiser le socket sur le logiciel ASA.

5. Si vous rencontrez des problèmes lorsque vous vous connectez/authentifiez l'ASDM, vérifiez

que les options d'authentification pour HTTP sont correctement configurées. Si aucune commande d'authentification n'est définie, vous pouvez utiliser le mot de passe enable ASA pour vous connecter à l'ASDM. Si vous voulez activer l'authentification basée sur le nom d'utilisateur/mot de passe, vous devez entrer cette configuration afin d'authentifier les sessions ASDM/HTTP à l'ASA à partir de la base de données de nom d'utilisateur/mot de passe de l'ASA :

<#root>

```
aaa authentication http console LOCAL
```

N’oubliez pas de créer un nom d’utilisateur/mot de passe lorsque vous activez la commande précédente :

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

Si aucune de ces étapes n'aide, ces options de débogage sont disponibles sur l'ASA pour une étude plus approfondie :

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

Connectivité réseau

Si vous avez terminé la section précédente et que vous ne parvenez toujours pas à accéder à l'ASDM, l'étape suivante consiste à vérifier la connectivité réseau à votre ASA à partir de la machine à partir de laquelle vous souhaitez accéder à l'ASDM. Il existe quelques étapes de dépannage de base afin de vérifier que l'ASA reçoit la requête de l'ordinateur client :

1. Testez avec le protocole ICMP (Internet Control Message Protocol).
   Envoyez une requête ping à l'interface ASA à partir de laquelle vous souhaitez accéder à l'ASDM. La requête ping peut aboutir si ICMP est autorisé à traverser votre réseau et s'il n'y a aucune restriction au niveau de l'interface ASA. Si la requête ping échoue, c'est probablement parce qu'il y a un problème de communication entre l'ASA et la machine cliente. Cependant, il ne s'agit pas d'une étape concluante pour déterminer qu'il y a ce type de problème de communication.
2. Confirmez la capture des paquets.
   Placez une capture de paquets sur l'interface à partir de laquelle vous souhaitez accéder à l'ASDM. La capture peut montrer que les paquets TCP destinés à l'adresse IP de l'interface arrivent avec le numéro de port de destination 443 (par défaut).

Afin de configurer une capture, utilisez cette commande :

<#root>

capture asdm_test interface

match tcp host

eq 443 host

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

Cela capture tout trafic TCP qui arrive pour le port 443 sur l'interface ASA à partir de laquelle vous vous connectez à l'ASDM. Connectez-vous via ASDM à ce stade ou ouvrez la page de lancement Web ASDM. Utilisez ensuite la commande show capture asdm_test afin de visualiser le résultat des paquets capturés :

<#root>

```
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>
```

Cette capture montre une requête de synchronisation (SYN) de l'ordinateur client vers l'ASA, mais l'ASA n'envoie aucune réponse. Si vous voyez une capture similaire à la précédente, cela signifie que les paquets atteignent l'ASA, mais l'ASA ne répond pas à ces requêtes, ce qui isole le problème à l'ASA lui-même. Reportez-vous à la première section de ce document afin de poursuivre le dépannage.

Cependant, si vous ne voyez pas de sortie similaire à la précédente et qu'aucun paquet n'est capturé, cela signifie qu'il y a un problème de connectivité entre l'ASA et la machine cliente ASDM. Vérifiez qu'aucun périphérique intermédiaire ne peut bloquer le trafic du port TCP 443 et qu'aucun paramètre de navigateur, tel que les paramètres de proxy, ne peut empêcher le trafic d'atteindre l'ASA.

En général, la capture de paquets est un bon moyen de déterminer si le chemin vers l'ASA est libre et si d'autres diagnostics ne peuvent pas être nécessaires pour éliminer les problèmes de connectivité réseau.

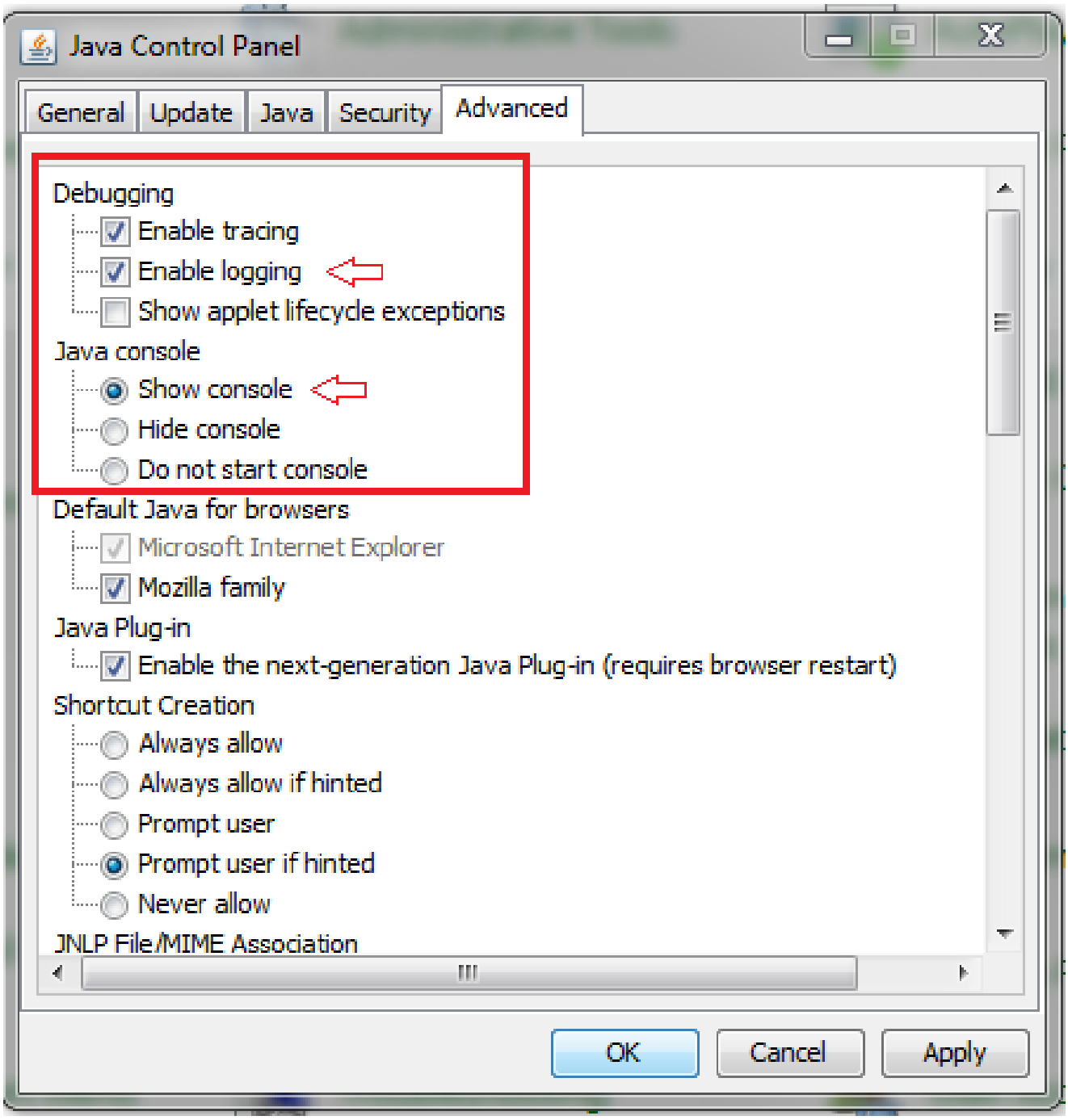
Application logicielle

Cette section décrit comment dépanner le logiciel de lancement ASDM qui a été installé sur la machine cliente lorsque le démarrage/chargement échoue. Le lanceur ASDM est le composant qui réside sur la machine client et se connecte à l'ASA afin de récupérer l'image ASDM. Une fois récupérée, l'image ASDM est généralement stockée dans le cache et est prise à partir de là jusqu'à ce que des modifications soient remarquées côté ASA, telles qu'une mise à jour d'image ASDM.

Effectuez ces étapes de dépannage de base afin d'éliminer tout problème sur l'ordinateur client :

1. Ouvrez la page de lancement d'ASDM à partir d'une autre machine. S'il est lancé, cela signifie que le problème est lié à la machine client en question. En cas d'échec, utilisez le guide de dépannage depuis le début pour isoler les composants concernés dans l'ordre.
2. Ouvrez l'ASDM via le lancement Web et lancez le logiciel directement à partir de là. En cas de succès, il est probable que l'installation du lanceur ASDM présente des problèmes. Désinstallez le lanceur ASDM de l'ordinateur client et réinstallez-le à partir du lancement Web ASA lui-même.
3. Effacez le répertoire cache de l'ASDM dans le répertoire de base de l'utilisateur. Le cache est effacé lorsque vous supprimez l'intégralité du répertoire cache. Si l'ASDM démarre correctement, vous pouvez également effacer le cache à partir du menu Fichier ASDM.
4. Vérifiez que la version Java appropriée est installée. Les notes de version de Cisco ASDM répertorient les exigences relatives aux versions testées de Java.

5. Effacez le cache Java. Dans le Panneau de configuration Java, sélectionnez Général > Fichier Internet temporaire. Cliquez ensuite sur View afin de lancer un Java Cache Viewer. Supprimez toutes les entrées qui font référence à l'ASDM ou qui lui sont associées.
6. Si ces étapes échouent, collectez les informations de débogage à partir de l'ordinateur client pour un examen plus approfondi. Activez le débogage pour ASDM avec l'URL : https://<adresse IP de l'ASA>?debug=5 par exemple, https://10.0.0.1?debug=5.
   Avec Java Version 6 (également appelé Version 1.6), les messages de débogage Java sont activés à partir de Java Control Panel > Advanced. Activez ensuite les cases à cocher sous Débogage. Ne sélectionnez pas Ne pas démarrer la console sous la console Java. Le débogage Java doit être activé avant le démarrage d'ASDM.



La sortie de la console Java est enregistrée dans le répertoire .asdm/log du répertoire

d'accueil de l'utilisateur. Les journaux ASDM se trouvent également dans le même répertoire.

Exécuter des commandes avec HTTPS

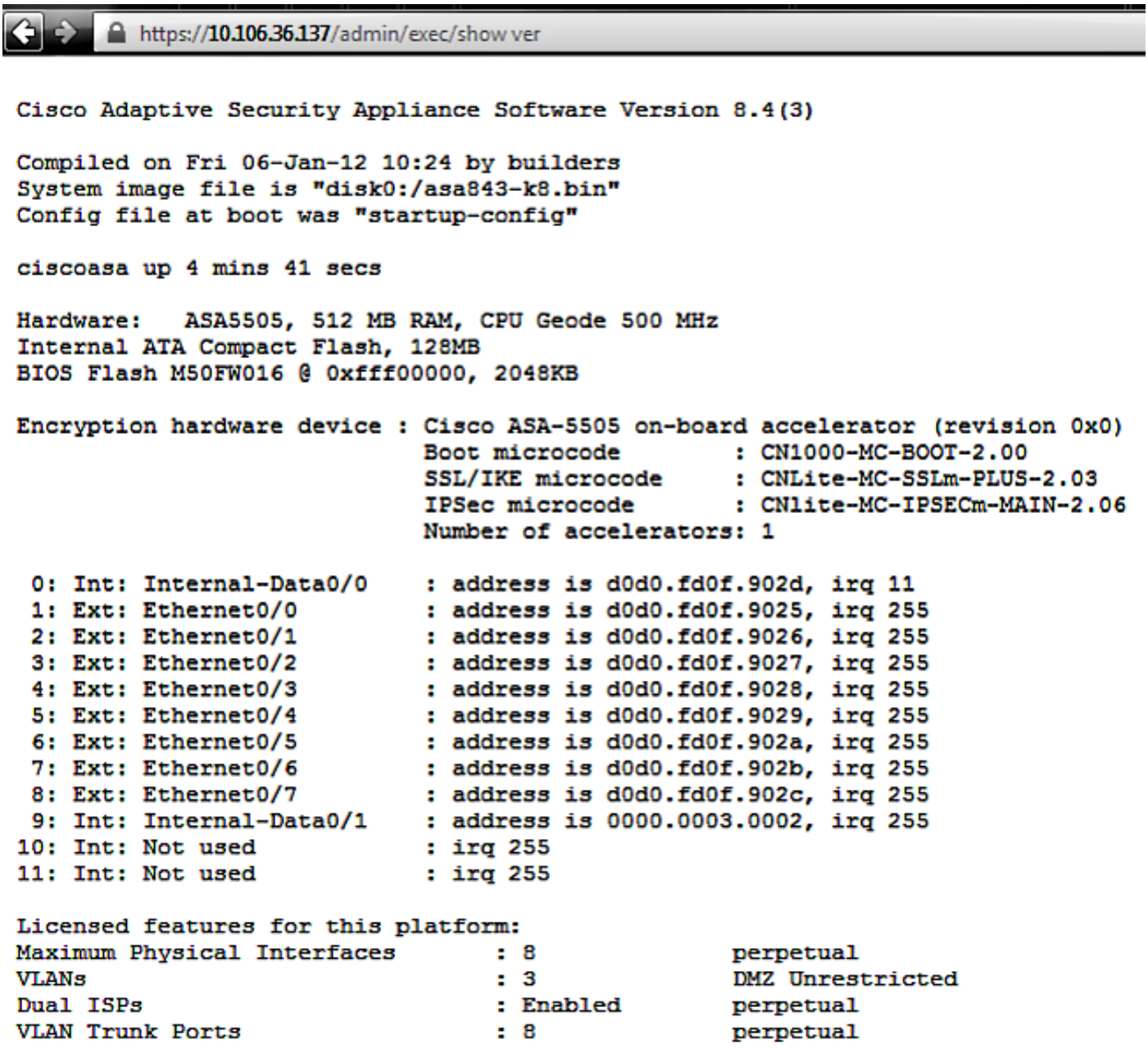
Cette procédure permet de déterminer les problèmes de couche 7 pour le canal HTTP. Ces informations s'avèrent utiles lorsque vous vous trouvez dans une situation où l'application ASDM elle-même n'est pas accessible et où aucun accès CLI n'est disponible pour gérer le périphérique.

L'URL utilisée pour accéder à la page de lancement Web d'ASDM peut également être utilisée pour exécuter n'importe quelle commande de niveau de configuration sur l'ASA. Cette URL peut être utilisée afin d'apporter des modifications de configuration de base à l'ASA, ce qui inclut un rechargement de périphérique distant. Afin d'entrer une commande, utilisez cette syntaxe :

https://<adresse IP de l'ASA>/admin/exec/<commande>

Si la commande contient un espace et que le navigateur ne parvient pas à analyser les caractères d'espace dans une URL, vous pouvez utiliser le signe + ou %20 pour indiquer l'espace.

Par exemple, https://10.106.36.137/admin/exec/show ver génère une sortie show version dans le navigateur :



Cette méthode d'exécution de commande nécessite que le serveur HTTP soit activé sur l'ASA et que les restrictions HTTP nécessaires soient actives. Cependant, cela ne nécessite PAS la présence d'une image ASDM sur l'ASA.

Informations connexes

- Configuration de l'accès ASDM pour les appareils
- ASA 5500-x : l'ASDM et d'autres fonctions SSL ne sont pas prêtes à l'emploi
- Notes de version de Cisco ASDM
- Page Licence Cisco pour obtenir une licence 3DES/AES sur l'ASA
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.