ASA-Verbindungsprobleme mit dem Cisco Adaptive Security Device Manager

Inhalt

Einführung

Dieses Dokument enthält die erforderlichen Methoden zur Fehlerbehebung, um Probleme beim Zugriff auf/bei der Konfiguration der Cisco Adaptive Security Appliance (ASA) mit dem Cisco Adaptive Security Device Manager (ASDM) zu untersuchen. ASDM stellt Sicherheitsmanagement- und Überwachungsservices für Security Appliances über eine grafische Verwaltungsschnittstelle bereit.

Voraussetzungen

Anforderungen

Die in diesem Dokument aufgeführten Szenarien, Symptome und Schritte werden zur Behebung von Problemen nach der Erstkonfiguration auf der ASA geschrieben. Informationen zur Erstkonfiguration finden Sie im Abschnitt Konfigurieren des ASDM-Zugriffs für Appliances im Konfigurationshandbuch für allgemeine Betriebsabläufe der Cisco ASA-Serie, 7.1.

In diesem Dokument wird die ASA CLI zur Fehlerbehebung verwendet, die Secure Shell (SSH)/Telnet/Console-Zugriff auf die ASA erfordert.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem ASDM und der ASA.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Fehlerbehebungsmethode

Das Dokument zur Fehlerbehebung konzentriert sich auf drei wesentliche Fehlerbereiche. Wenn Sie sich an den allgemeinen Fehlerbehebungsprozess in dieser Reihenfolge halten, sollte dieses Dokument Ihnen helfen, das genaue Problem bei der Verwendung und beim Zugriff von ASDM zu ermitteln.

- **ASA-Konfiguration**
- **Netzwerkverbindungen**
- **Anwendungssoftware**

ASA-Konfiguration

Die ASA verfügt über drei grundlegende Konfigurationen, die für den erfolgreichen Zugriff auf das ASDM erforderlich sind:

- ASDM-Image in Flash
- Verwendung des ASDM-Image
- HTTP-Serverbeschränkungen

ASDM-Image in Flash

Stellen Sie sicher, dass die erforderliche ASDM-Version in den Flash-Speicher hochgeladen wird. Sie kann entweder mit der aktuell ausgeführten Version des ASDM hochgeladen werden oder mit anderen konventionellen Methoden zur Dateiübertragung an die ASA, z. B. TFTP.

Geben Sie **show flash** in der ASA-CLI ein, um die im ASA-Flash-Speicher vorhandenen Dateien aufzulisten. Überprüfen Sie, ob die ASDM-Datei vorhanden ist:

```
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
```

Um weiter zu überprüfen, ob das im Flash-Speicher enthaltene Bild gültig und nicht beschädigt ist, können Sie den Befehl **verify** verwenden, um den gespeicherten MD5-Hash im Softwarepaket und den MD5-Hash der tatsächlich vorhandenen Datei zu vergleichen:

```
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
```

Dieser Schritt sollte Ihnen helfen zu überprüfen, ob das Image vorhanden ist und ob es auf der ASA-Appliance integriert ist.

Verwendung des ASDM-Image

Dieser Prozess wird in der ASDM-Konfiguration auf der ASA definiert. Eine Beispielkonfigurationsdefinition des aktuellen Bildes, das verwendet wird, sieht wie folgt aus:

asdm image disk0:/asdm-702.bin

Sie können den Befehl **show asdm image** verwenden, um weitere Überprüfungen vorzunehmen:

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

HTTP-Serverbeschränkungen

Dieser Schritt ist für die ASDM-Konfiguration unerlässlich, da definiert wird, welche Netzwerke Zugriff auf die ASA haben. Eine Beispielkonfiguration sieht wie folgt aus:

```
http server enable
http 192.168.1.0 255.255.255.0 inside

http 64.0.0.0 255.0.0.0 outside
```

Stellen Sie sicher, dass die erforderlichen Netzwerke in der vorherigen Konfiguration definiert sind. Das Fehlen dieser Definitionen führt dazu, dass der ASDM-Launcher bei der Verbindung eine Zeitüberschreitung verursacht, und gibt diesen Fehler an:

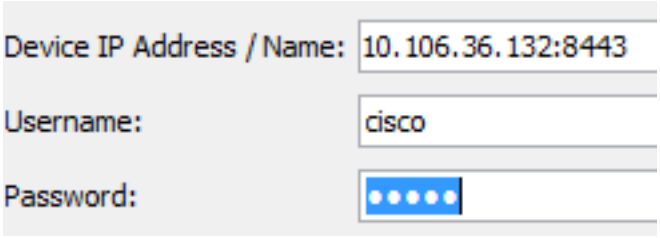
Die ASDM-Startseite (**https://<ASA-IP-Adresse>/admin**) veranlasst die Anforderung, das Zeitlimit zu überschreiten, und es wird keine Seite angezeigt.

Überprüfen Sie außerdem, ob der HTTP-Server einen nicht standardmäßigen Port für ASDM-Verbindungen wie 8443 verwendet. Dies wird in der Konfiguration hervorgehoben:

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

http-Server aktivieren 8443

Wenn ein nicht standardmäßiger Port verwendet wird, müssen Sie für die Verbindung mit der ASA im ASDM-Launcher Folgendes angeben:



Dies gilt auch für den Zugriff auf die ASDM-Startseite: **https://10.106.36.132:8443/admin**

Weitere mögliche Konfigurationsprobleme

Wenn Sie die vorherigen Schritte ausgeführt haben, sollte das ASDM geöffnet werden, wenn auf der Clientseite alles funktioniert. Wenn jedoch weiterhin Probleme auftreten, öffnen Sie das ASDM von einem anderen Computer aus. Wenn Sie erfolgreich sind, liegt das Problem wahrscheinlich auf der Anwendungsebene, und die ASA-Konfiguration ist in Ordnung. Falls es jedoch immer noch nicht gestartet werden kann, führen Sie die folgenden Schritte aus, um die ASA-seitigen Konfigurationen weiter zu überprüfen:

1. Überprüfen Sie die SSL-Konfiguration (Secure Sockets Layer) auf der ASA. ASDM verwendet SSL, während es mit der ASA kommuniziert. Je nachdem, wie ASDM gestartet wird, lässt neuere Betriebssystemsoftware bei der Aushandlung von SSL-Sitzungen möglicherweise die Verwendung schwächerer Chiffren nicht zu.

   Überprüfen Sie, welche Chiffren für die ASA zugelassen sind, und ob in der Konfiguration mit dem Befehl **show run all ssl** angegeben ist, ob bestimmte SSL-Versionen angegeben sind:

   ```
   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
   ```

   Wenn beim Start des ASDM Fehler bei der Aushandlung eines SSL-Verschlüsselungsschlüssels auftreten, werden diese in den ASA-Protokollen angezeigt:

   ```
   %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
   ```

   Wenn bestimmte Einstellungen angezeigt werden, setzen Sie sie auf die Standardeinstellung zurück.

   Beachten Sie, dass die VPN-3DES-AES-Lizenz auf der ASA für die 3DES- und AES-Verschlüsselungen aktiviert werden muss, die von der ASA in der Konfiguration verwendet werden. Dies kann mithilfe des CLI-Befehls **show version** überprüft werden. Die Ausgabe wird wie folgt angezeigt:

   ```
   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>
   ```

   Eine VPN-3DES-AES-Lizenz kann kostenlos von der Cisco Lizenzierungs-Website bezogen werden. Klicken Sie auf **Sicherheitsprodukte** und wählen Sie dann **Cisco ASA 3DES/AES-Lizenz aus**.

   Hinweis: Auf den neuen ASA 5500-X-Plattformen, die mit 8.6/9.x-Code ausgeliefert werden, sind die SSL-Verschlüsselungseinstellungen standardmäßig auf **des-sha1** festgelegt, wodurch die ASDM-Sitzungen nicht funktionieren. Weitere Informationen finden Sie unter ASA 5500-x: ASDM- und andere SSL-Funktionen sind für weitere Informationen nicht sofort einsatzbereit.
2. Überprüfen Sie, ob WebVPN auf der ASA aktiviert ist. Wenn diese Funktion aktiviert ist, müssen Sie diese URL (**https://10.106.36.132/admin**) verwenden, um auf sie zuzugreifen, wenn Sie auf die ASDM-Webseite zugreifen.
3.
4. Suchen Sie auf der ASA für Port 443 nach einer Network Address Translation (NAT)-Konfiguration. Dadurch verarbeitet die ASA die ASDM-Anfragen nicht, sondern sendet sie an

das Netzwerk bzw. die Schnittstelle, für die die NAT konfiguriert wurde.

5.
6. Wenn alles überprüft wird und das ASDM immer noch eine Zeitüberschreitung aufweist, stellen Sie sicher, dass die ASA so konfiguriert ist, dass sie den für ASDM definierten Port mit dem Befehl **show asp table socket** (**Tabelle anzeigen**) in der ASA CLI abhört. Die Ausgabe sollte zeigen, dass die ASA den ASDM-Port abhört:

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

Wenn diese Ausgabe nicht angezeigt wird, entfernen Sie die HTTP-Serverkonfiguration auf der ASA, und wenden Sie sie erneut an, um den Socket auf der ASA-Software zurückzusetzen.

7.
8. Wenn bei der Anmeldung beim ASDM Probleme auftreten, überprüfen Sie, ob die Authentifizierungsoptionen für **HTTP** korrekt eingerichtet sind. Wenn keine Authentifizierungsbefehle festgelegt sind, können Sie sich mit dem ASA-Aktivierungskennwort beim ASDM anmelden. Wenn Sie die Authentifizierung mit Benutzernamen/Kennwort aktivieren möchten, müssen Sie diese Konfiguration eingeben, um ASDM-/HTTP-Sitzungen der ASA über die Benutzername-/Kennwort-Datenbank der ASA zu authentifizieren:

```
aaa authentication http console LOCAL
```

Denken Sie daran, einen Benutzernamen/ein Kennwort zu erstellen, wenn Sie den vorherigen Befehl aktivieren:

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

Wenn keiner dieser Schritte hilft, stehen diese Debugoptionen auf der ASA für weitere Untersuchungen zur Verfügung:

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

Netzwerkverbindungen

Wenn Sie den vorherigen Abschnitt abgeschlossen haben und immer noch nicht auf das ASDM zugreifen können, besteht der nächste Schritt darin, die Netzwerkverbindung zu Ihrer ASA von dem Computer aus zu überprüfen, von dem aus Sie auf das ASDM zugreifen möchten. Es gibt einige grundlegende Schritte zur Fehlerbehebung, um sicherzustellen, dass die ASA die Anfrage vom Client-Computer erhält:

1. **Testen Sie mit dem Internet Control Message Protocol (ICMP)**.
   Pingen Sie die ASA-Schnittstelle, von der aus Sie auf das ASDM zugreifen möchten. Der Ping-Test sollte erfolgreich sein, wenn ICMP das Netzwerk durchlaufen darf und die ASA-Schnittstellenebene keine Einschränkungen aufweist. Wenn der Ping fehlschlägt, liegt dies wahrscheinlich daran, dass ein Kommunikationsproblem zwischen der ASA und dem Client-Computer vorliegt. Dies ist jedoch kein abschließender Schritt, um festzustellen, dass ein solches Kommunikationsproblem vorliegt.
2.
3. **Mit Paketerfassung bestätigen**.
   Platzieren Sie eine Paketerfassung auf der Schnittstelle, von der aus Sie auf den ASDM

zugreifen möchten. Die Erfassung sollte zeigen, dass TCP-Pakete, die an die IP-Adresse der Schnittstelle gerichtet sind, mit der Zielportnummer 443 eintreffen (Standard).

Verwenden Sie den folgenden Befehl, um eine Erfassung zu konfigurieren:

```
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
```

Dies erfasst jeglichen TCP-Datenverkehr für Port 443 der ASA-Schnittstelle, von der aus Sie eine Verbindung zum ASDM herstellen. Verbinden Sie sich zu diesem Zeitpunkt über ASDM, oder öffnen Sie die ASDM-Webseite. Verwenden Sie dann den Befehl **show capture asdm_test**, um das Ergebnis der erfassten Pakete anzuzeigen:

```
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>
```

Diese Erfassung zeigt eine SYN-Anfrage (Synchronize) vom Client-Computer an die ASA, aber die ASA sendet keine Antwort. Wenn Sie eine Erfassung sehen, die der vorherigen ähnelt, bedeutet dies, dass die Pakete die ASA erreichen, aber die ASA nicht auf diese Anfragen reagiert, wodurch das Problem an die ASA selbst isoliert wird. Weitere Informationen zur Fehlerbehebung finden Sie im ersten Abschnitt dieses Dokuments.

Wenn Sie jedoch keine Ausgabe ähnlich der vorherigen sehen und keine Pakete erfasst werden, bedeutet dies, dass ein Verbindungsproblem zwischen ASA und dem ASDM-Client-System besteht. Vergewissern Sie sich, dass keine zwischengeschalteten Geräte vorhanden sind, die den TCP-Port 443-Datenverkehr blockieren könnten, und dass keine Browsereinstellungen wie Proxy-Einstellungen vorhanden sind, die verhindern könnten, dass der Datenverkehr die ASA erreicht.

In der Regel ist die Paketerfassung eine gute Methode, um festzustellen, ob der Pfad zur ASA klar ist und ob möglicherweise keine weiteren Diagnosen erforderlich sind, um Netzwerkverbindungsprobleme auszuschließen.

Anwendungssoftware

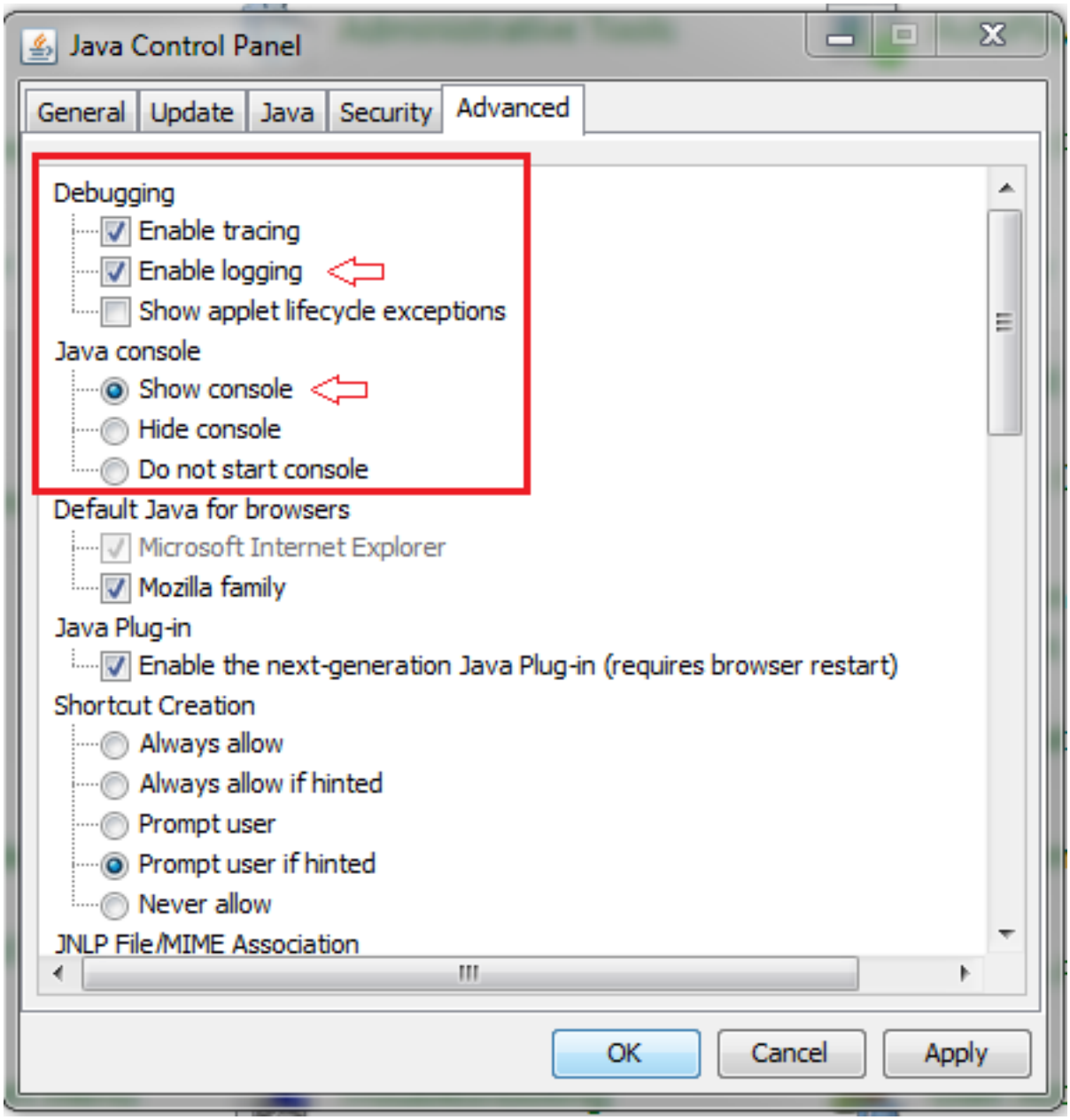
In diesem Abschnitt wird beschrieben, wie Sie die ASDM-Launcher-Software, die auf dem Client-Computer installiert wurde, beheben, wenn sie nicht gestartet/geladen werden kann. Der ASDM-Launcher ist die Komponente, die sich auf dem Client-Computer befindet und mit der ASA

verbunden ist, um das ASDM-Image abzurufen. Nach dem Abruf wird das ASDM-Image in der Regel im Cache gespeichert und von dort übernommen, bis auf der ASA-Seite alle Änderungen, z. B. ein ASDM-Image-Update, bemerkt werden.

Führen Sie die folgenden grundlegenden Fehlerbehebungsschritte aus, um Probleme auf dem Client-Computer auszuschließen:

1. Öffnen Sie die ASDM-Startseite von einem anderen Computer aus. Wenn es gestartet wird, bedeutet dies, dass das Problem mit dem betreffenden Client-Computer vorliegt. Wenn es fehlschlägt, folgen Sie dem Fehlerbehebungshandbuch von Anfang an, um die beteiligten Komponenten in der richtigen Reihenfolge zu isolieren.
2.
3. Öffnen Sie das ASDM über den Web-Launch, und starten Sie die Software direkt von dort. Wenn dies erfolgreich ist, gibt es wahrscheinlich Probleme mit der Installation des ASDM-Launchers. Deinstallieren Sie den ASDM-Launcher vom Client-Computer, und installieren Sie ihn vom ASA-Webstart selbst neu.
4.
5. Löschen Sie das ASDM-Cache-Verzeichnis im Hauptverzeichnis des Benutzers. In Windows 7 finden Sie sie beispielsweise hier: **C:\Users\<Benutzername>\.asdm\cache**. Der Cache wird gelöscht, wenn Sie das gesamte **Cache-**Verzeichnis löschen. Wenn der ASDM erfolgreich startet, können Sie den Cache auch im ASDM **File** Menü löschen.
6.
7. Überprüfen Sie, ob die korrekte Java-Version installiert ist. Die Cisco ASDM-Versionshinweise enthalten eine Liste der Anforderungen für getestete Java-Versionen.
8.
9. Löschen Sie den Java-Cache. Wählen Sie in der **Java-Systemsteuerung Allgemein > Temporary Internet File (Temporäre Internetdatei)**. Klicken Sie dann auf **Anzeigen**, um einen **Java Cache Viewer** zu starten. Löschen Sie alle Einträge, die sich auf ASDM beziehen bzw. damit zusammenhängen.
10.
11. Wenn diese Schritte fehlschlagen, sammeln Sie die Debuginformationen vom Client-Computer für weitere Untersuchungen. Debuggen für ASDM mit der URL aktivieren: **https://<IP-Adresse der ASA>?debug=5, z. B. https://10.0.0.1?debug=5**.

    Bei Java Version 6 (auch als Version 1.6 bezeichnet) werden Java-Debugmeldungen über **Java Control Panel > Advanced** aktiviert. Aktivieren Sie dann die Kontrollkästchen unter **Debuggen**. Wählen Sie **Konsole nicht starten** unter der **Java-Konsole aus**. Bevor ASDM gestartet wird, muss Java-Debugging aktiviert werden.



Die Ausgabe der Java-Konsole wird im Verzeichnis **.asdm/log** im Hauptverzeichnis des Benutzers aufgezeichnet. ASDM-Protokolle können auch im gleichen Verzeichnis vorhanden sein. In Windows 7 sind die Protokolle beispielsweise unter **C:\Users\<Benutzername>/.asdm/log/**.

Befehle mit HTTPS ausführen

Dieses Verfahren hilft bei der Ermittlung von Layer-7-Problemen für den HTTP-Kanal. Diese Informationen erweisen sich als nützlich, wenn Sie sich in einer Situation befinden, in der die ASDM-Anwendung selbst nicht zugänglich ist und für die Verwaltung des Geräts kein CLI-Zugriff verfügbar ist.

Die URL, die für den Zugriff auf die ASDM-Webseite verwendet wird, kann auch zum Ausführen von Befehlen auf Konfigurationsebene auf der ASA verwendet werden. Diese URL kann verwendet werden, um Konfigurationsänderungen auf einer grundlegenden Ebene an der ASA vorzunehmen, die ein erneutes Laden von Remote-Geräten beinhaltet. Um einen Befehl einzugeben, verwenden Sie die folgende Syntax:

https://<IP-Adresse der ASA>/admin/exec/<command>

Wenn der Befehl Leerzeichen enthält und der Browser Leerzeichen in einer URL nicht analysieren kann, können Sie das **+** Zeichen oder **%20** verwenden, um das Leerzeichen anzugeben.

https://10.106.36.137/admin/exec/show beispielsweise ergibt eine Ausgabe der Anzeigeversion für den Browser:


```
Cisco Adaptive Security Appliance Software Version 8.4(3)

Compiled on Fri 06-Jan-12 10:24 by builders
System image file is "disk0:/asa843-k8.bin"
Config file at boot was "startup-config"

ciscoasa up 4 mins 41 secs

Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xfff00000, 2048KB

Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                             Boot microcode         : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode      : CNLite-MC-SSLm-PLUS-2.03
                             IPSec microcode        : CNlite-MC-IPSECm-MAIN-2.06
                             Number of accelerators: 1

 0: Int: Internal-Data0/0    : address is d0d0.fd0f.902d, irq 11
 1: Ext: Ethernet0/0         : address is d0d0.fd0f.9025, irq 255
 2: Ext: Ethernet0/1         : address is d0d0.fd0f.9026, irq 255
 3: Ext: Ethernet0/2         : address is d0d0.fd0f.9027, irq 255
 4: Ext: Ethernet0/3         : address is d0d0.fd0f.9028, irq 255
 5: Ext: Ethernet0/4         : address is d0d0.fd0f.9029, irq 255
 6: Ext: Ethernet0/5         : address is d0d0.fd0f.902a, irq 255
 7: Ext: Ethernet0/6         : address is d0d0.fd0f.902b, irq 255
 8: Ext: Ethernet0/7         : address is d0d0.fd0f.902c, irq 255
 9: Int: Internal-Data0/1    : address is 0000.0003.0002, irq 255
10: Int: Not used            : irq 255
11: Int: Not used            : irq 255

Licensed features for this platform:
Maximum Physical Interfaces       : 8              perpetual
VLANs                             : 3              DMZ Unrestricted
Dual ISPs                         : Enabled        perpetual
VLAN Trunk Ports                  : 8              perpetual
```

Diese Befehlsausführungsmethode erfordert, dass der HTTP-Server auf der ASA aktiviert ist und die erforderlichen HTTP-Einschränkungen aktiviert sind. Es muss jedoch KEIN ASDM-Image auf der ASA vorhanden sein.

Zugehörige Informationen

- Konfigurieren des ASDM-Zugriffs für Appliances
- ASA 5500-x: ASDM und andere SSL-Funktionen Nicht sofort einsatzbereit
- Cisco ASDM Versionshinweise
- Cisco Lizenzseite für den Erhalt einer 3DES/AES-Lizenz auf der ASA
- Technischer Support und Dokumentation - Cisco Systems