ASA Connection Problems to the Cisco Adaptive Security Device Manager

Document ID: 116403

Contributed by Ishwinder Cheema and Jay Johnston, Cisco TAC Engineers.
Jul 31, 2013

Contents

Introduction
Prerequisites
- Requirements
- Components Used

Troubleshooting Methodology
- ASA Configuration
  - ASDM Image in Flash
  - ASDM Image in Use
  - HTTP Server Restrictions
  - Other Possible Configuration Issues
- Network Connectivity
- Application Software

Run Commands with HTTPS
Related Information

Introduction

This document provides the troubleshooting methodology necessary to examine issues faced when you access/configure the Cisco Adaptive Security Appliance (ASA) with Cisco Adaptive Security Device Manager (ASDM). ASDM delivers security management and monitoring services for security appliances through a graphical management interface.

Prerequisites

Requirements

The scenarios, symptoms, and steps listed in this document are written for troubleshooting issues after the initial configuration is set up on the ASA. For the initial configuration, refer to the Configuring ASDM Access for Appliances section of the Cisco ASA Series General Operations ASDM Configuration Guide, 7.1.

This document uses the ASA CLI for troubleshooting, which requires Secure Shell (SSH)/Telnet/Console access to the ASA.

Components Used

The information in this document is based on the ASDM and 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.

Troubleshooting Methodology

There are three major failure points on which this troubleshooting document focuses. If you adhere to the general troubleshooting process in this order, this document should help you to determine the exact problem with ASDM use/access.

- ***ASA Configuration***
- ***Network Connectivity***
- ***Application Software***

ASA Configuration

There are three essential configurations that are present on the ASA that are needed in order to successfully access the ASDM:

- ASDM Image in Flash
- ASDM Image in Use
- HTTP Server Restrictions

ASDM Image in Flash

Make sure that the required version of the ASDM is uploaded to the flash. It can either be uploaded with the currently run version of the ASDM or with other conventional methods of file transfer to the ASA, such as TFTP.

Enter ***show flash*** on the ASA CLI in order to help you list the files present on the ASA flash memory. Check for the presence of the ASDM file:

```
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
```

In order to further verify if the image present on the flash is valid and not corrupt, you can use the ***verify*** command in order to compare the stored MD5 hash in the software package and the MD5 hash of the actual file present:

```
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
```

This step should help you verify if the image is present and its integrity on the ASA.

ASDM Image in Use

This process is defined under the ASDM configuration on the ASA. A sample configuration definition of the current image that is used looks like this:

asdm image disk0:/asdm−702.bin

In order to further verify, you can also use the ***show asdm image*** command:

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

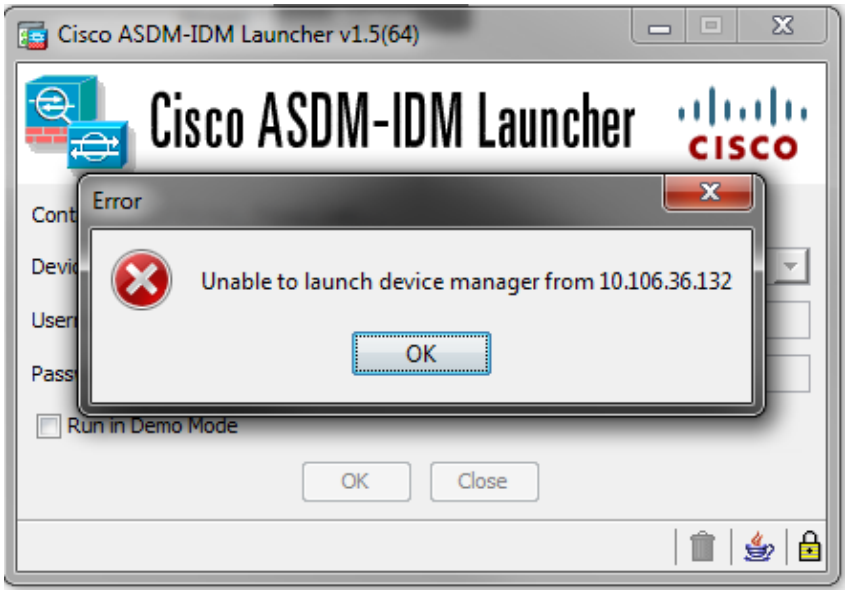
HTTP Server Restrictions

This step is essential in the ASDM configuration, because it defines which networks have access to the ASA. A sample configuration looks like this:

```
http server enable
http 192.168.1.0 255.255.255.0 inside

http 64.0.0.0 255.0.0.0 outside
```

Verify that you have the necessary networks defined in the previous configuration. The absence of those definitions causes the ASDM launcher to time out while it connects and gives this error:



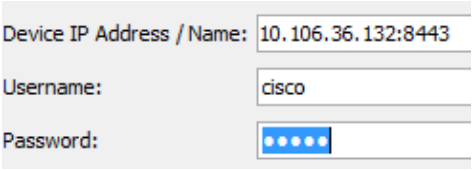
The ASDM launch page (***https://<ASA IP address>/admin***) causes the request to time out and no page is displayed.

Further verify that the HTTP server uses a non−standard port for ASDM connection, such as 8443. This is highlighted in the configuration:

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

http server enable 8443

If it uses a non−standard port, you need to specify the port when you connect to the ASA in the ASDM launcher as:



This also applies for when you access the ASDM launch page: ***https://10.106.36.132:8443/admin***

Other Possible Configuration Issues

After you complete the previous steps, the ASDM should open if everything is functional on the client side. However, if you still experience issues, open the ASDM from another machine. If you succeed, the issue is is probably at the application level, and the ASA configuration is fine. However, if it still fails to launch, complete these steps to further verify the ASA−side configurations:

1. Verify the Secure Sockets Layer (SSL) configuration on the ASA. ASDM uses SSL while it communicates with the ASA. Based on the way ASDM is launched, newer OS software might not allow usage of weaker ciphers when it negotiates SSL sessions.

   Verify which ciphers are allowed on the ASA, and if any specific SSL versions are specified in the configuration with the ***show run all ssl*** command:

   ```
   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
   ```

   If there are any SSL cipher negotiation errors while the ASDM launches, they display in the ASA logs:

   ```
   %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
   ```

   If you see specific settings, revert them to the default.

   Notice that the VPN−3DES−AES license needs to be enabled on the ASA for the 3DES and AES ciphers to be used by the ASA in the configuration. This can be verified with the ***show version*** command on the CLI. The output displays like this:

   ```
   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>
   ```

   A VPN−3DES−AES license can be obtained without any cost from the Cisco licensing website. Click ***Security Products***, and then choose ***Cisco ASA 3DES/AES License***.

Note: In the new ASA 5500−X platforms that ship with 8.6/9.x code, the SSL cipher settings are set to ***des−sha1*** by default, which causes the ASDM sessions to not work. Refer to the ASA 5500−x: ASDM and other SSL function do not work out of the box article for more information.

2. Verify that WebVPN is enabled on the ASA. If it is enabled, you need to use this URL (***https://10.106.36.132/admin***) in order to access it when you access the ASDM web launch page.

3. Check for a Network Address Translation (NAT) configuration on the ASA for port 443. This causes the ASA to not process the requests for ASDM but rather send them to the network/interface for which the NAT has been configured.

4. If everything is verified and the ASDM still times out, verify that the ASA is set up to listen on the port defined for ASDM with the ***show asp table socket*** command on the ASA CLI. The output should show that the ASA listens on the ASDM port:

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

   If this output does not display, remove and reapply the HTTP server configuration on the ASA in order to reset the socket on the ASA software.

5. If you experience issues when you log in/authenticate to the ASDM, verify that the authentication options for ***HTTP*** are set up correctly. If no authentication commands are set, you can use the ASA enable password to log in to the ASDM. If you want to enable username/passoword−based authentication, you need to enter this configuration in order to authenticate ASDM/HTTP sessions to the ASA from the ASA's username/password database:

   ```
   aaa authentication http console LOCAL
   ```

   Remember to create a username/password when you enable the previous command:

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

   If none of these steps helps, these debug options are available on the ASA for further investigation:

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

Network Connectivity

If you have completed the previous section and are still unable to access the ASDM, the next step is to verify the network connectivity to your ASA from the machine from which you want to access the ASDM. There are a few basic troubleshooting steps in order to verify that the ASA receives the request from the client machine:

1. ***Test with Internet Control Message Protocol (ICMP)***.
   Ping the ASA interface from which you want to access the ASDM. The ping should be successful if ICMP is allowed to traverse your network and there are no restrictions on the ASA interface level. If the ping fails, it is probably because there is a communication issue between the ASA and the client machine. However, this is not a conclusive step to determine that there is that type of communication issue.

2. ***Confirm with packet capture***.
   Place a packet capture on the interface from which you want to access the ASDM. The capture should show that TCP packets destined to the Interface IP address arrive with destination port number 443 (default).

   In order to configure a capture, use this command:

   capture asdm_test interface <name of the ASA interface> match tcp host <IP address of the interface> eq 443 host <IP address of the client machine>
   For example, cap asdm_test interface mgmt match tcp host 10.106.36.132 eq 443 host 10.106.36.13

   This captures any TCP traffic that comes for port 443 on the ASA interface from which you connect to the ASDM. Connect via ASDM at this point or open the ASDM web launch page. Then use the ***show capture asdm_test*** command in order to view the result of the packets captured:

   ```
   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>
   ```

   This capture shows a synchronize (SYN) request from the client machine to the ASA, but the ASA sends no response. If you see a capture similar to the previous one, it means that the packets reach the ASA but the ASA does not respond to those requests, which isolates the issue to the ASA itself. Refer to the first section of this document in order to troubleshoot further.

   However, if you do not see output similar to the previous and no packets are captured, it means that there is a connectivity problem between the ASA and the ASDM client machine. Verify that there are no intermediary devices that might block TCP port 443 traffic and that there are no browser settings, such as Proxy settings, that could prevent the traffic from reaching the ASA.

   Typically, packet capture is a good way to determine if the path to the ASA is clear, and if further diagnostics might not be needed to rule out network connectivity problems.

Application Software

This section describes how to troubleshoot the ASDM launcher software that has been installed on the client machine when it fails to launch/load. The ASDM launcher is the component that resides on the client machine and connects to the ASA in order to retrieve the ASDM image. Once retrieved, the ASDM image is usually stored in cache and is taken from there until any changes are noticed on the ASA side, such as an ASDM image update.

Complete these basic troubleshooting steps in order to rule out any issues on the client machine:

1. Open the ASDM launch page from another machine. If it launches, it means that the issue is with the client machine in question. If it fails, follow the troubleshooting guide from the beginning to isolate the involved components in order.

2. Open the ASDM via web launch, and launch the software directly from there. If it succeeds, it is likely that there are issues with the ASDM launcher installation. Uninstall the ASDM launcher from the client machine, and reinstall it from the ASA web launch itself.

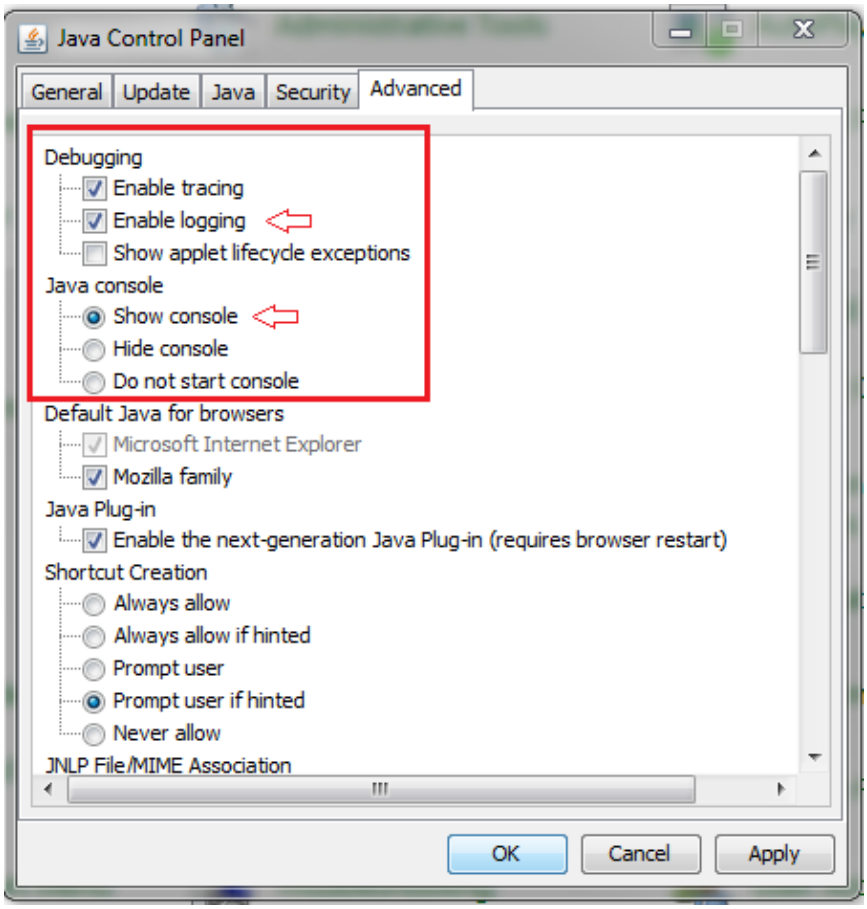
3. Clear the ASDM's cache directory in the user's home directory. For example, in Windows 7, it is located here: ***C:\Users\<username>\.asdm\cache***. The cache is cleared when you delete the entire ***cache*** directory. If the ASDM starts successfully, you can also clear the cache from within the ASDM ***File*** menu.

4. Verify that the proper Java version is installed. The Cisco ASDM Release Notes list the requirements for tested Java versions.

5. Clear the Java cache. In the ***Java Control Panel***, choose ***General > Temporary Internet File***. Then, click ***View*** in order to launch a ***Java Cache Viewer***. Delete all entries that refer to or are related to ASDM.

6. If these steps fail, collect the debugging information from the client machine for further investigation. Enable debugging for ASDM with the URL: ***https://<IP address of the ASA>?debug=5 e.g. https://10.0.0.1?debug=5***.

   With Java Version 6 (also called Version 1.6), Java debugging messages are enabled from ***Java Control Panel > Advanced***. Then select the check boxes under ***Debugging***. Do not select ***Do not start console*** under the ***Java console***. Java debugging must be enabled before ASDM starts.



The Java console output is recorded in the ***.asdm/log*** directory of the user's home directory. ASDM logs might also be found in the same directory. For example, in Windows 7, the logs are under ***C:\Users\<username>/.asdm/log/***.

Run Commands with HTTPS

This procedure helps determine any Layer 7 issues for the HTTP channel. This information proves useful when you are in a situation where the ASDM application itself is not accessible, and there is not any CLI access available to manage the device.

The URL that is used to access the ASDM web launch page can also be used to run any configuration−level commands on the ASA. This URL can be used in order to make configuration changes at a basic level to the ASA, which includes a remote device reload. In order to enter a command, use this syntax:

https://<IP address of the ASA>/admin/exec/<command>

If there is a space in the command and the browser is unable to parse space characters in a URL, you can use the **+** sign or ***%20*** to indicate the space.

For example, ***https://10.106.36.137/admin/exec/show ver*** results in a show version output to the 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
```

This method of command execution requires that the HTTP server is enabled on the ASA and has the necessary HTTP restrictions active. However, this does NOT require an ASDM image to be present on the ASA.

Related Information

- ***Configuring ASDM Access for Appliances***
- ***ASA 5500−x: ASDM and Other SSL Function Do not Work out of the Box***
- ***Cisco ASDM Release Notes***
- ***Cisco License Page to Obtain a 3DES/AES License on the ASA***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Jul 31, 2013 Document ID: 116403