Troubleshoot Connectivity and Registration Issues with AMP on FireSIGHT Management Center

Contents

Introduction

A FireSIGHT Management Center in your deployment can connect to the Cisco cloud. After you configure a FireSIGHT Management Center to connect to the cloud, you can receive records of scans, malware detections, and quarantines. The records are stored in the FireSIGHT Management Center database as malware events. By default, the cloud sends malware events for all groups within your organization, but you can restrict by group when you configure the connection. This document discusses various issues and troubleshooting steps on Advanced Malware Protection (AMP) feature of a FireSIGHT Management Center.

Port or Server is Blocked in Firewall

If a FireSIGHT Management Center is unable to connect to the FireAMP Cloud Console, or not receiving malware events, you must check if the required ports are blosked by the firewall. A FireSIGHT Management Center uses port 443 to receive endpoint-based malware events from the FireAMP Console. The port 32137 is required for FirePOWER appliances to perform malware lookups in the Cisco Cloud.

In order to learn more about the required port numbers and server addresses, read the following documents:

- Required communication ports for FireSIGHT System operation
- Required servers for AMP operation

MAC Address in Use

Symptom

When you attempt to register a FireSIGHT Management Center to a private cloud and perform the initial connection, you may receive a message indicating that the MAC address is already in use.

Reason

When a FireSIGHT Management Center is replaced due to a hardware failure, and the replacement unit is not properly unregistered from the cloud, you may experience this issue.

Solution

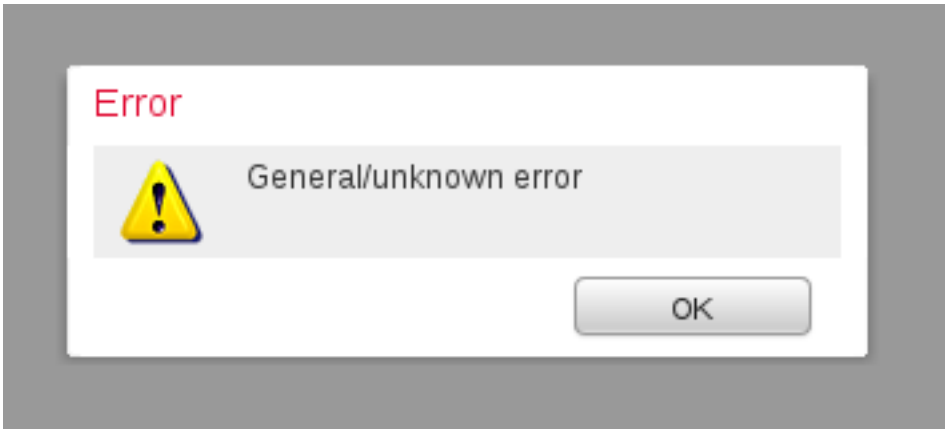
Before you replace an appliance, you must deregister the FireSIGHT Management Center from the FireAMP Cloud. You should also remove your FireSIGHT Management Center from the FireAMP cloud. This prevents a MAC address from being perceived as in use.

> **Tip**: Read this document to learn the detail process on how to deregister an appliance from the FireAMP Cloud and delete a cloud from the FireSIGHT Management Center.

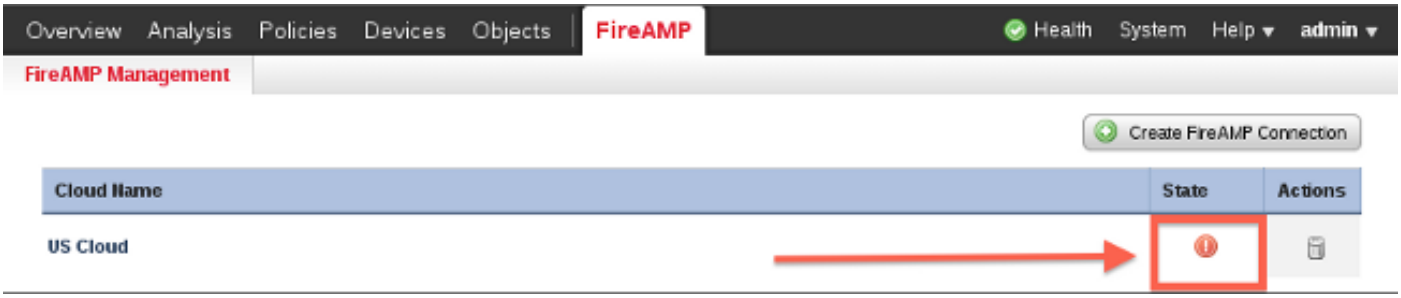
General/Unknown Error is Displayed

Symptom

When connecting a reimaged or replacement FireSIGHT Management Center to a FireAMP Console, an error message appears. It displays a `General/unknown error.`



When the `General/unknown error` message appears, the state of the FireAMP connection on FireSIGHT Management Center becomes critical. The web interface displays a red icon.



Reason

This issue occurs when a MAC address of a FireSIGHT Management Center, which has just been reimaged or replaced is still being registered to a FireAMP Console.

Solution

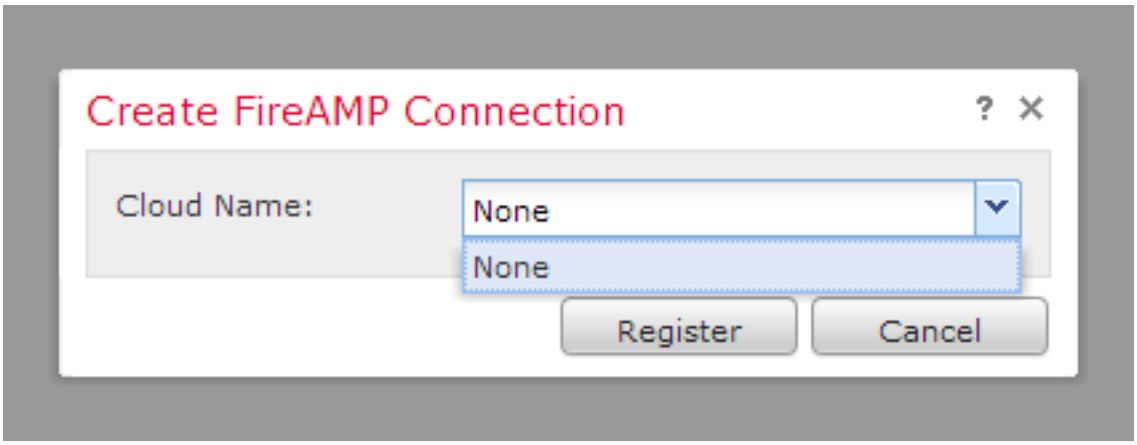
Before you reimage or replace an appliance, you must deregister the FireSIGHT Management Center from the FireAMP Cloud. You should also remove your FireSIGHT Management Center from the FireAMP cloud. This prevents a MAC address from being perceived as in use.

> **Tip**: Read this document to learn the detail process on how to deregister an appliance from the FireAMP Cloud and delete a cloud from the FireSIGHT Management Center.

Unable to Select a Cloud

Symptom

When creating a connection from a FireSIGHT Management Center to the FireAMP Cloud Console, there is no drop down options found for US Cloud or EU Cloud.



Reason

This issue occurs when a FireSIGHT Management Center is unable to resolve the hostname `api.amp.sourcefire.com`.

In order to verify the issue, perform an `nslookup` on the CLI of FireSIGHT Management Center. Check if the DNS Settings are properly configured on the FireSIGHT Management Center:

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com
```

The following output is displayed when DNS is unable to resolve the hostname on the FireSIGHT Management Center:

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com

Server:         192.168.45.2
Address:        192.168.45.2#53

** server can't find api.amp.sourcefire.com
```

Below is the output if DNS is properly resolved on the FireSIGHT Management Center:

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com
Server:         192.168.45.1
Address:        192.168.45.1#53

Non-authoritative answer:
api.amp.sourcefire.com
Name:   xxxx.xxxx.xxxx
Address: xx.xx.xx.xx
```

Solution

- If a FireSIGHT Management Center is unable to resolve the hostname, you need to verify if the DNS Settings on the Management Center are correct.
- If a FireSIGHT Management Center is able to resolve the hostname, but unable to access `api.amp.sourcefire.com` through a firewall, check the firewall rules and settings.

During connection creation process, if a FireSIGHT Management Center is unable to resolve the hostname, the following error message is logged in the `httpsd_error_log`:

```
Error attempting curl for FireAMP: System
```

For example, the following log output shows the Defense Center failing to complete the `curl` command to `api.amp.sourcefire.com`:

```
admin@Sourcefire3D:~$ tail -f /var/log/httpd/httpsd_error_log

[Thu Jul 18 12:38:13.433765 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
getCloudData start... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1778., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:38:14.338174 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --
sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H Accept:
application/vnd.sourcefire.fireamp.dc+json; version=1 https://api.amp.sourcefire.com/clouds at
/usr/local/sf/lib/perl/5.10.1/SF/System.pm line 7491., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352374 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
Error attempting curl for FireAMP: System (/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L
--max-redirs 5 --max-filesize 104857600 --sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H
Accept: application/vnd.sourcefire.fireamp.dc+json; version=1
https://api.amp.sourcefire.com/clouds) Failed at /usr/local/sf/lib/perl/5.10.1/SF/System.pm line
7499., referer: https://192.168.45.45/ddd/
```

```
[Thu Jul 18 12:38:24.352432 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
No cloud data returned at /usr/local/sf/lib/perl/5.10.1/SF/FireAMP.pm line 145., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352478 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
getCloudData completed... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1780., referer:
https://192.168.45.45/ddd/
```

During connection creation process, if the following message is logged in the `httpsd_error_log` without an error, it indicates that the FireSIGHT Management Center is able to resolve the hostname:

```
getCloudData completed
```

For example, the following output shows that a Management Center completes a `curl` command to `api.amp.sourcefire.com`:

```
admin@Sourcefire3D:~$ tail -f /var/log/httpd/httpsd_error_log

[Thu Jul 18 12:42:54.949461 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
getCloudData start... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1778., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:42:55.856432 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --
sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H Accept:
application/vnd.sourcefire.fireamp.dc+json; version=1 https://api.amp.sourcefire.com/clouds at
/usr/local/sf/lib/perl/5.10.1/SF/System.pm line 7491., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:42:55.931106 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
getCloudData completed... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1780., referer:
https://192.168.45.45/ddd/
```