FireSIGHT Management Center에서 AMP를 사용하여 연결 및 등록 문제 해결

목차

소개

구축의 FireSIGHT Management Center는 Cisco 클라우드에 연결할 수 있습니다. 클라우드에 연결하도록 FireSIGHT Management Center를 구성한 후 스캔, 악성코드 탐지 및 격리의 레코드를 수신할 수 있습니다. 레코드는 FireSIGHT Management Center 데이터베이스에 악성코드 이벤트로 저장됩니다. 기본적으로 클라우드는 조직 내 모든 그룹에 대한 악성코드 이벤트를 전송하지만, 연결을 구성할 때 그룹별로 제한할 수 있습니다. 이 문서에서는 FireSIGHT Management Center의 AMP(Advanced Malware Protection) 기능에 대한 다양한 문제 및 문제 해결 단계에 대해 설명합니다.

방화벽에서 포트 또는 서버가 차단됨

FireSIGHT Management Center에서 FireAMP Cloud Console에 연결할 수 없거나 악성코드 이벤트를 수신하지 못하는 경우, 필수 포트가 방화벽에 의해 차단되었는지 확인해야 합니다. FireSIGHT Management Center는 포트 443을 사용하여 FireAMP Console에서 엔드포인트 기반 악성코드 이벤트를 수신합니다. FirePOWER 어플라이언스가 Cisco 클라우드에서 악성코드 조회를 수행하려면 포트 32137이 필요합니다.

필요한 포트 번호 및 서버 주소에 대한 자세한 내용은 다음 문서를 참조하십시오.

- FireSIGHT System 작업에 필요한 통신 포트
- AMP 작업에 필요한 서버

사용 중인 MAC 주소

증상

프라이빗 클라우드에 FireSIGHT Management Center를 등록하고 초기 연결을 수행하려고 하면 MAC 주소가 이미 사용 중임을 알리는 메시지가 표시될 수 있습니다.

이유

하드웨어 장애로 인해 FireSIGHT Management Center를 교체하고, 교체용 장치가 클라우드에서 제대로 등록되지 않은 경우 이 문제가 발생할 수 있습니다.

솔루션

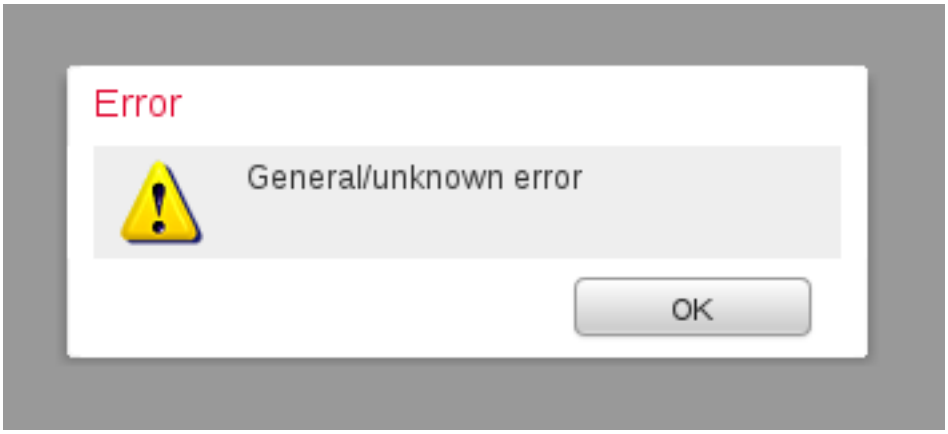
어플라이언스를 교체하기 전에 FireAMP Cloud에서 FireSIGHT Management Center 등록을 취소해야 합니다. 또한 FireAMP 클라우드에서 FireSIGHT Management Center를 제거해야 합니다. 이렇게 하면 MAC 주소가 사용 중인 것으로 인식되지 않습니다.

> **팁:** FireAMP Cloud에서 어플라이언스를 등록 취소하고 FireSIGHT Management Center에서 클라우드를 삭제하는 방법에 대한 세부 프로세스를 보려면 이 문서를 참조하십시오.

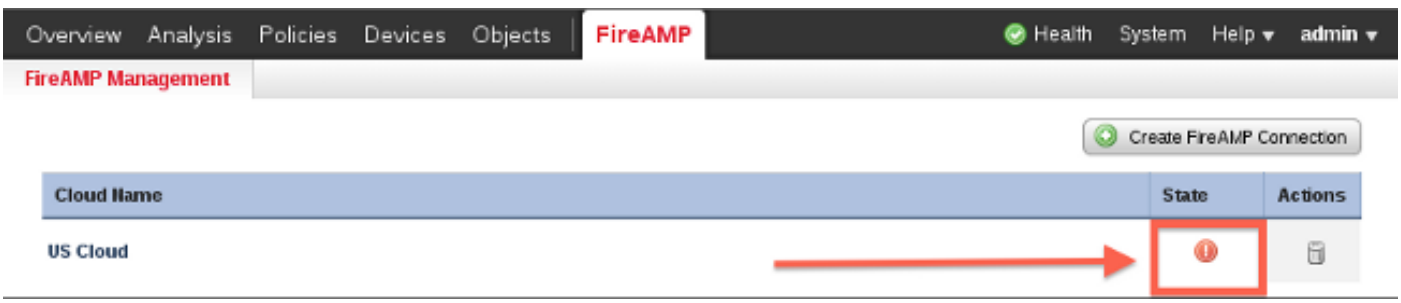
일반/알 수 없는 오류가 표시됩니다.

증상

이미지로 다시 설치되거나 교체된 FireSIGHT Management Center를 FireAMP Console에 연결하면 오류 메시지가 나타납니다. 일반/알 수 없는 오류가 표시됩니다.



General/unknown 오류 메시지가 나타나면 FireSIGHT Management Center의 FireAMP 연결 상태가 중요해집니다. 웹 인터페이스에 빨간색 아이콘이 표시됩니다.



이유

이 문제는 방금 이미지로 다시 설치되었거나 교체한 FireSIGHT Management Center의 MAC 주소가 FireAMP Console에 등록되어 있는 경우에 발생합니다.

솔루션

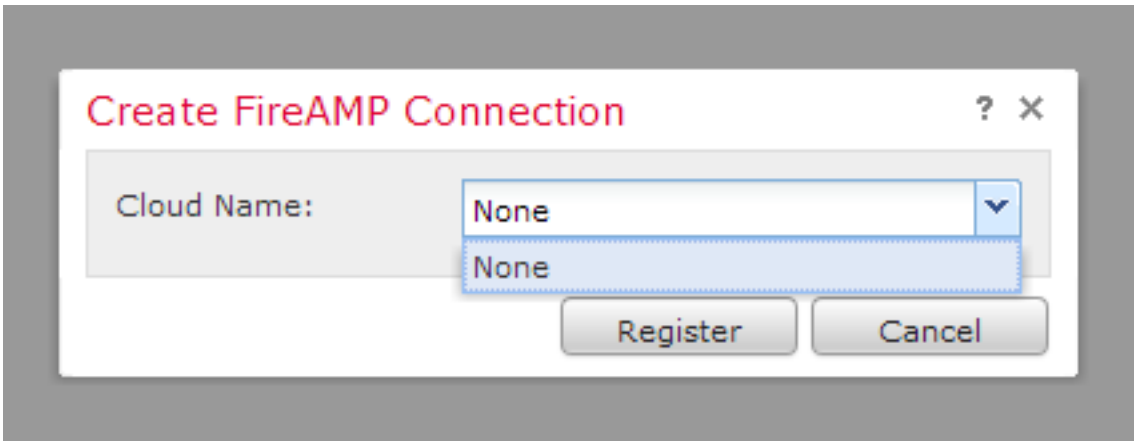
어플라이언스를 다시 이미징하거나 교체하기 전에 FireAMP Cloud에서 FireSIGHT Management Center 등록을 취소해야 합니다. 또한 FireAMP 클라우드에서 FireSIGHT Management Center를 제거해야 합니다. 이렇게 하면 MAC 주소가 사용 중인 것으로 인식되지 않습니다.

> **팁:** FireAMP Cloud에서 어플라이언스를 등록 취소하고 FireSIGHT Management Center에서 클라우드를 삭제하는 방법에 대한 세부 프로세스를 보려면 이 문서를 참조하십시오.

클라우드를 선택할 수 없음

증상

FireSIGHT Management Center에서 FireAMP Cloud Console로의 연결을 생성할 때 US 클라우드 또는 EU 클라우드에 대한 드롭다운 옵션이 없습니다.



이유

이 문제는 FireSIGHT Management Center에서 호스트 이름 api.amp.sourcefire.com을 확인할 수 없을 때 발생합니다.

문제를 확인하려면 FireSIGHT Management Center의 CLI에서 nslookup을 수행합니다. DNS 설정이 FireSIGHT Management Center에 올바르게 구성되어 있는지 확인합니다.

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

DNS에서 FireSIGHT Management Center의 호스트 이름을 확인할 수 없는 경우 다음 출력이 표시됩니다.

```
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
```

다음은 FireSIGHT Management Center에서 DNS가 올바르게 확인되는 경우의 출력입니다.

```
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
```

솔루션

- FireSIGHT Management Center에서 호스트 이름을 확인할 수 없는 경우 관리 센터의 DNS 설정이 올바른지 확인해야 합니다.
- FireSIGHT Management Center에서 호스트 이름을 확인할 수 있지만 방화벽을 통해 api.amp.sourcefire.com에 액세스할 수 없는 경우 방화벽 규칙 및 설정을 확인하십시오.

연결 생성 프로세스 중에 FireSIGHT Management Center에서 호스트 이름을 확인할 수 없는 경우 다음 오류 메시지가 httpsd_error_log에 기록됩니다.

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

예를 들어 다음 로그 출력은 Defense Center에서 api.amp.sourcefire.com에 대한 curl 명령을 완료하지 못한 것을 보여줍니다.

```
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/
```

연결 생성 프로세스 중에 다음 메시지가 오류 없이 httpsd_error_log에 로그인된 경우 FireSIGHT

Management Center에서 호스트 이름을 확인할 수 있음을 나타냅니다.

```
getCloudData completed
```

예를 들어, 다음 출력은 Management Center에서 api.amp.sourcefire.com에 curl 명령을 완료하는 것을 보여줍니다.

```
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/
```