AMP가 있는 ESA에서 "The File Reputation Service is not reachable" 오류 수신

목차

소개

이 문서에서는 AMP(Advanced Malware Protection)가 활성화된 Cisco ESA(Email Security Appliance)에서 서비스가 포트 32137 또는 파일 평판 443을 통해 통신할 수 없는 경우 발생하는 경고에 대해 설명합니다.

AMP에 대해 수신한 "파일 평판 서비스에 연결할 수 없습니다." 오류 수정

AMP는 AsyncOS Version 8.5.5 for Email Security에서 ESA에 사용하도록 릴리스되었습니다. ESA에서 AMP 라이센스가 부여되고 활성화된 경우 관리자는 다음 메시지를 받게 됩니다.

```
The Warning message is:

The File Reputation service is not reachable.

Last message occurred 2 times between Tue Jul 26 10:17:15 2015 and Tue Jul 26 10:18:16 2016.

Version: 12.5.0-066
Serial Number: 123A82F6780XXX9E1E10-XXX5DBEFCXXX
Timestamp: 07 Oct 2019 14:25:13 -0400
```

AMP 서비스가 활성화될 수 있지만 파일 평판을 위한 포트 32137을 통해 네트워크에서 통신하지는 않을 수 있습니다.

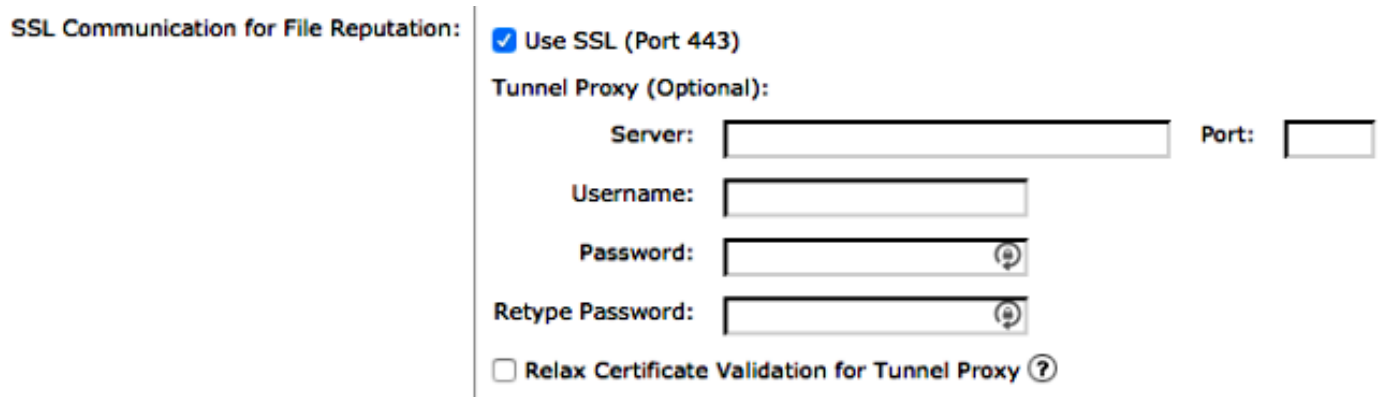
이 경우 ESA 관리자는 파일 평판이 포트 443을 통해 통신하도록 선택할 수 있습니다.

이렇게 하려면 CLI에서 ampconfig **> advanced**를 실행하고 **Y**가 *Do you want to enable SSL communication (port 443) for file reputation(파일 평판을 위해 SSL 통신(포트 443)을 활성화하시겠습니까?)에* 선택되어 *있는지 확인합니다. [N]>*:

```
(Cluster example.com)> ampconfig

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CACHESETTINGS - Configure the cache settings for AMP.
```

```
- CLUSTERSET - Set how advanced malware protection is configured in a cluster.
- CLUSTERSHOW - Display how advanced malware protection is configured in a cluster.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.cisco.com)
2. AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)
3. EUROPE (cloud-sa.eu.amp.cisco.com)
4. APJC (cloud-sa.apjc.amp.cisco.com)
5. Private reputation cloud
[1]>

Do you want use the recommended analysis threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>

Do you want to suppress the verdict update alerts for all messages that are not delivered to the
recipient? [N]>

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. EUROPE (https://panacea.threatgrid.eu)
3. Private analysis cloud
[1]>
```

GUI를 사용하는 경우 **Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석) > Edit Global Settings(전역 설정 수정) > Advanced(고급)(드롭다운)**를 선택하고 다음 그림과 같이 **Use SSL(SSL** 사용) 확인란이 선택되었는지 확인합니다.



컨피그레이션에 대한 모든 변경 사항을 커밋합니다.

마지막으로, 현재 AMP 로그를 검토하여 서비스 및 연결 성공 또는 실패를 확인합니다. **tail** amp를 사용하여 CLI에서 이를 수행할 수 **있습니다**.

ampconfig **> advanced**를 변경하기 **전**에 AMP 로그에서 이를 확인할 수 있었습니다.

```
Mon Jan 26 10:11:16 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
Mon Jan 26 10:12:15 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
Mon Jan 26 10:13:15 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
```

ampconfig > advanced(고급)를 변경하면 AMP 로그에서 다음 내용을 확인할 수 있습니다.

```
Mon Jan 26 10:19:19 2015 Info: amp stunnel process started pid [3725]
Mon Jan 26 10:19:22 2015 Info: amp The File Reputation service in the cloud
is reachable.
Mon Jan 26 10:19:22 2015 Info: amp File reputation service initialized
successfully
Mon Jan 26 10:19:22 2015 Info: amp File Analysis service initialized
successfully
Mon Jan 26 10:19:23 2015 Info: amp The File Analysis server is reachable
Mon Jan 26 10:20:24 2015 Info: amp File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Jan 26 10:20:24 2015 Info: amp Response received for file reputation query
from Cloud. File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown,
Malware = None, Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcdf403710098977
fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
```

이전 예에 표시된 amp_watchdog.txt 파일은 10분마다 실행되며 AMP 로그에서 추적됩니다. 이 파일은 AMP용 연결 유지 기능의 일부입니다.

File Reputation and File Analysis(파일 평판 및 파일 분석)에 대해 구성된 파일 유형의 메시지에 대한 AMP 로그의 일반 쿼리는 다음과 같습니다.

```
Wed Jan 14 15:33:01 2015 Info: File reputation query initiating. File Name =
'securedoc_20150112T114401.html', MID = 703, File Size = 108769 bytes, File
Type = text/html
Wed Jan 14 15:33:02 2015 Info: Response received for file reputation query from
Cloud. File Name = 'securedoc_20150112T114401.html', MID = 703, Disposition = file
unknown, Malware = None, Reputation Score = 0, sha256 = c1afd8efe4eeb4e04551a8a0f5
533d80d4bec0205553465e997f9c672983346f, upload_action = 1
```

이 로그 정보를 사용하여 관리자는 메일 로그의 메시지 ID(MID)를 상호 연결할 수 있어야 합니다.

문제 해결

방화벽 및 네트워크 설정을 검토하여 다음에 대해 SSL 통신이 열려 있는지 확인합니다.

포트	프로토콜	수신/발신	호스트 이름	설명
443	TCP	발신	Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석), Advanced(고급) 섹션에 구성된 대로.	파일 분석을 위한 클라 서비스 액세스
32137	TCP	발신	Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석), Advanced(고급) 섹션, Advanced(고급) 섹션, Cloud Server Pool(클라우드 서버 풀) 매개변수에 구성된 대로.	파일 평판을 얻기 위하 라우드 서비스에 액세 니다.

어플라이언스가 AMP 서비스, 파일 평판 및 파일 분석에 성공적으로 도달할 수 있도록 텔넷을 통해 443을 통해 ESA에서 클라우드 서비스로의 기본 연결을 테스트할 수 있습니다.

참고: File Reputation(파일 평판) 및 File Analysis(파일 분석)의 주소는 CLI에서 ampconfig > advanced(**고급)로 구성되거나** GUI에서 **Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석) > Edit Global Settings(전역 설정 수정) > Advanced(드롭다운)로 구성됩니다**.

참고: ESA와 파일 평판 서버 간에 터널 프록시를 사용하는 경우 터널 프록시에 대한 인증서 유효성 검사 완화 옵션을 활성화해야 할 수 있습니다. 이 옵션은 터널 프록시 서버의 인증서가 ESA에서 신뢰하는 루트 인증 기관에 의해 서명되지 않은 경우 표준 인증서 유효성 검사를 건너뛰도록 제공됩니다. 예를 들어, 신뢰할 수 있는 내부 터널 프록시 서버에서 자체 서명 인증서를 사용하는 경우 이 옵션을 선택합니다.

파일 평판 예:

```
10.0.0-125.local> telnet cloud-sa.amp.sourcefire.com 443

Trying 23.21.199.158...
Connected to ec2-23-21-199-158.compute-1.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

파일 분석 예:

```
10.0.0-125.local> telnet panacea.threatgrid.com 443

Trying 69.55.5.244...
Connected to 69.55.5.244.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

ESA에서 파일 평판 서버에 텔넷할 수 있고 연결의 암호를 해독하는 업스트림 프록시가 없는 경우 어플라이언스를 Threat Grid에 다시 등록해야 할 수 있습니다. ESA CLI에는 숨겨진 명령이 있습니다.

```
10.0.0-125.local> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> ampregister

AMP registration initiated.
```

관련 정보

- ESA AMP(Advanced Malware Protection) 테스트

- ESA 사용 설명서
- ESA FAQ: MID(Message ID), ICID(Injection Connection ID) 또는 DCID(Delivery Connection ID)란 무엇입니까?
- ESA에서 메일 로그를 검색하고 보려면 어떻게 해야 합니까?
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.