SLIC 채널 중단 시스템 경보 문제 해결

목차

소개

이 문서에서는 SNA(Secure Network Analytics) "SLIC Channel Down" 시스템 경보의 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 기본 SNA 지식이 있는 것을 권장합니다.

SLIC는 "Stealthwatch Labs Intelligence Center"의 약자입니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

절차

"SLIC Channel Down" 경보는 SNA Manager가 이전에 SLIC였던 Threat Intelligence Server에서 피드 업데이트를 가져올 수 없을 때 트리거됩니다. 피드 업데이트가 중단된 원인을 더 잘 이해하려면 다음과 같이 진행합니다.

1. SSH를 통해 SNA Manager에 연결하고 **root** 자격 증명.
2. 분석 **/lancope/var/smc/log/smc-core.log** 파일 및 유형 로그 검색 **SlicFeedGetter**.

관련 로그를 찾은 후에는 이 경보가 트리거될 수 있는 여러 조건이 있는 경우 다음 섹션을 계속하십시오.

일반 오류 로그

에 표시되는 가장 일반적인 오류 로그 **smc-core.log** SLIC 채널 중단 알람과 관련된 사항은 다음과 같습니다.

연결 시간 초과

<#root>

```
2023-01-03 22:43:28,533 INFO [SlicFeedGetter] Performing request to get Threat Feed update file.
2023-01-03 22:43:28,592 INFO [SlicFeedGetter] Threat Feed Host 'lancope.flexnetoperations.com' resolves
2023-01-03 22:43:28,592 INFO [SlicFeedGetter] Threat Feed URL: /control/lncp/LancopeDownload?token=2019
2023-01-03 22:45:39,604
```

ERROR [SlicFeedGetter] Getting Threat Feed update failed with exception.

org.apache.http.conn.HttpHostConnectException: Connect to lancope.flexnetoperations.com:443 [lancope.fle

요청된 대상에 대한 유효한 인증 경로를 찾을 수 없습니다.

<#root>

```
2023-01-04 00:27:50,497 INFO [SlicFeedGetter] Performing request to get Threat Feed update file.
2023-01-04 00:27:50,502 INFO [SlicFeedGetter] Threat Feed Host 'lancope.flexnetoperations.com' resolves
2023-01-04 00:27:50,502 INFO [SlicFeedGetter] Threat Feed URL: /control/lncp/LancopeDownload?token=2019
2023-01-04 00:27:51,239
```

ERROR [SlicFeedGetter] Getting Threat Feed update failed with exception.

javax.net.ssl.SSLHandshakeException: PKIX path building failed: sun.security.provider.certpath.SunCertPa

핸드셰이크 실패

<#root>

```
2023-01-02 20:00:49,427 INFO [SlicFeedGetter] Performing request to get Threat Feed update file.
2023-01-02 20:00:49,433 INFO [SlicFeedGetter] Threat Feed Host 'lancope.flexnetoperations.com' resolves
2023-01-02 20:00:49,433 INFO [SlicFeedGetter] Threat Feed URL: /control/lncp/LancopeDownload?token=2019
```

2023-01-02 20:00:50,227 ERROR [SlicFeedGetter] Getting Threat Feed update failed with exception.

javax.net.ssl.SSLHandshakeException: Handshake failed

수행 단계

다른 조건으로 인해 위협 인텔리전스 피드 업데이트가 중단될 수 있습니다. 다음 검증 단계를 수행하여 SNA Manager가 요구 사항을 충족하는지 확인합니다.

1단계. Smart Licensing 상태 검증

탐색 **Central Management** > **Smart Licensing** Threat Feed 라이센스의 상태가 **Authorized.**

2단계. DNS(도메인 이름 시스템) 확인 확인

SNA Manager가 다음에 대한 IP 주소를 성공적으로 확인할 수 있는지 확인합니다
. **lancope.flexnetoperations.com** and esdhttp.flexnetoperations.com

3단계. 위협 인텔리전스 피드 서버에 대한 연결 확인

SNA Manager에 인터넷 액세스가 있고 다음에 나열된 위협 인텔리전스 서버에 대한 연결이 허용되는지 확인합니다.

포트 및 프로토콜	소스	대상
443/TCP	SNA 관리자	esdhttp.flexnetoperations.com lancope.flexnetoperations.com

참고: SNA Manager가 직접 인터넷 액세스를 허용하지 않는 경우 인터넷 액세스를 위한 프록시 컨피그레이션이 있는지 확인하십시오.

4단계. SSL(Secure Socket Layer) 검사/암호 해독 비활성화

에 설명된 두 번째 및 세 번째 오류 **Common Error Logs** 이 섹션은 SNA Manager가 올바른 ID 인증서 또는 위협 인텔리전스 피드 서버에서 사용하는 올바른 신뢰 체인을 수신하지 못할 때 발생할 수 있습니다. 이를 방지하려면 SNA Manager와 다음에 나열된 위협 인텔리전스 서버 간의 연결에 대해 네트워크 전체에서(지원되는 방화벽 또는 프록시 서버에 의해) SSL 검사/암호 해독이 수행되지 않는지 확인합니다. **Verify Connectivity to the Threat Intelligence Feed Servers** 섹션을 참조하십시오.

네트워크에서 SSL 검사/암호 해독이 수행되는지 확신할 수 없는 경우 SNA Manager IP 주소와 Threat Intelligence Servers IP 주소 간에 패킷 캡처를 수집하고 캡처를 분석하여 수신한 인증서를 확인할 수 있습니다. 이를 위해 다음과 같이 수행합니다.

1. SSH로 SNA Manager에 연결하고 **root** 자격 증명.
2. 다음에 나열된 두 명령 중 하나를 실행합니다(실행할 명령은 SNA 관리자가 인터넷 액세스에 프록시 서버를 사용하는지 여부에 따라 다름).

```
tcpdump -w /lancope/var/tcpdump/slic_issue.pcap -nli eth0 host 64.14.29.85
tcpdump -w /lancope/var/tcpdump/slic_issue2.pcap -nli eth0 host [IP address of Proxy Server]
```

3. 캡처를 2~3분 동안 실행한 다음 중지합니다.
4. 생성된 파일을 분석을 위해 SNA Manager에서 전송합니다. 이 작업은 SCP(Secure Copy Protocol)로 수행할 수 있습니다.

관련 결함

SLIC 서버와의 연결에 영향을 줄 수 있는 한 가지 알려진 결함이 있습니다.

- 대상 포트 80이 차단된 경우 SMC SLIC 통신이 시간 초과되어 실패할 수 있습니다. Cisco 버그 ID CSCwe를 참조하십시오08331

관련 정보

- 추가 지원이 필요한 경우 TAC(Technical Assistance Center)에 문의하십시오. 유효한 지원 계약이 필요합니다. Cisco 전 세계 지원 문의처.
- 여기서 Cisco Security Analytics Community를 방문할 수도 있습니다.
- 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.