排除SLIC通道关闭系统警报故障

目录

简介

本文档介绍如何对安全网络分析(SNA)“SLIC通道关闭”系统警报进行故障排除。

先决条件

要求

Cisco建议您掌握基本的SNA知识。

SLIC代表“Stealthwatch Labs Intelligence Center”

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

步骤

当SNA Manager无法从威胁情报服务器（以前称为SLIC）获取源更新时，会触发“SLIC通道关闭”警报。要更好地了解导致源更新中断的原因，请按以下步骤操作：

1. 通过SSH连接到SNA Manager，然后使用 **root** 凭证。
2. 分析 **/lancope/var/smc/log/smc-core.log** 文件并搜索类型的日志 **SlicFeedGetter**.

找到相关日志后，请继续下一部分，因为存在多种情况可能导致触发此警报。

常见错误日志

最常见的错误日志 **smc-core.log** 与SLIC通道关闭警报相关的有：

连接超时

<#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
```

找不到到所请求目标的有效证书路径

<#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
```

握手失败

<#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
```

执行的步骤

威胁情报源更新可能会由于不同情况而中断。执行后续验证步骤以确保SNA Manager符合要求。

步骤1:验证智能许可状态

导航至 **Central Management > Smart Licensing** 并确保威胁源许可证的状态为 **Authorized.**

第二步：验证域名系统(DNS)解析

确保SNA Manager能够成功解析 **lancope.flexnetoperations.com** and esdhttp.flexnetoperations.com

第三步：验证与威胁情报源服务器的连接

确保SNA Manager可以访问Internet，并允许连接到下面列出的威胁情报服务器：

端口和协议	来源	目的地
443/TCP	SNA管理器	esdhttp.flexnetoperations.com lancope.flexnetoperations.com

注：如果SNA Manager不允许直接访问互联网，请确保互联网访问的代理配置已就绪。

第四步：禁用安全套接字层(SSL)检测/解密

中所述的第二个和第三个错误 **Common Error Logs** 当SNA Manager未收到由Threat Intelligence Feed服务器使用的正确身份证书或信任链时，可能会出现此部分。要防止这种情况，请确保您的网络中没有为SNA Manager和Threat Intelligence服务器之间的连接执行SSL检查/解密（通过功能强大的防火墙或代理服务器）。 **Verify Connectivity to the Threat Intelligence Feed Servers** 部分。

如果您不确定是否在网络中执行SSL检查/解密，可以收集SNA Manager IP地址和Threat Intelligence Servers IP地址之间的数据包捕获，并分析该捕获以验证收到的证书。为此，请执行以

下操作：

1.通过SSH连接到SNA Manager，然后使用 **root** 凭证。
2.运行下面列出的两个命令之一（要运行的命令取决于SNA管理器是否使用代理服务器进行互联网访问）：

```
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.让捕获运行2-3分钟，然后停止捕获。
4.将生成的文件从SNA Manager中传输以进行分析。这可以通过安全复制协议(SCP)来实现。

相关问题

有一个已知缺陷可能会影响到SLIC服务器的连接：

- 如果目标端口80被阻止，则SMC SLIC通信可能会超时和失败。请参阅Cisco Bug ID CSCwe08331

相关信息

- 如需其他帮助，请联系技术支持中心(TAC)。需要有效的支持合同： 思科全球支持联系方式.
- 您还可以在此处访问思科安全分析社区。
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。