排除SLIC通道关闭系统警报故障

目录

简介

先决条件

- 要求
- 使用的组件

步骤

- 常见错误日志
  - 连接超时
  - 找不到到所请求目标的有效证书路径
  - 握手失败
- 补救步骤
  - 步骤1.验证智能许可状态
  - 步骤2.检验域名系统(DNS)解析
  - 步骤3.检验与威胁情报源服务器的连接
  - 步骤4.禁用安全套接字层(SSL)检测/解密

相关问题

相关信息

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. 通过登录到Manager导航到Central Management(在您的浏览器地址字段中，键入https://和设备IP地址)。按Enter键。)
2. 从主菜单中选择Configure > Global > Central Management。
3. 点击设备的省略号图标。
4. 选择View Appliance Statistics。
5. 从主菜单中选择支持 > 浏览文件
6. 在“浏览文件”页面上，选择smc > logs > ，然后单击smc-core.log。
7. 将打开一个新选项卡，其中包含smc-core.log内容。通过搜索日志来查看此文件**SlicFeedGetter**。

常见错误日志

在与SLIC通道关闭警报相关的中**smc-core.log**，最常见的错误日志包括：

连接超时

```
2026-01-01 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.fl
```

找不到到所请求目标的有效证书路径

```
2026-01-01 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.SunCertP
```

握手失败

```
2026-01-01 20:00:50,227 ERROR [SlicFeedGetter] Getting Threat Feed update failed with exception.
javax.net.ssl.SSLHandshakeException: Handshake failed
```

补救步骤

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**是。

步骤2.检验域名系统(DNS)解析

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

步骤3.检验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

注意：如果不允许使用SNA Manager直接访问互联网，请确保已配置互联网访问的代理配置。

步骤4.禁用安全套接字层(SSL)检测/解密

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**Common Error Logs**时，可能会发生本部分所述的第二和第三错误。

为防止这种情况，请确保您的网络中没有对SNA Manager和部分中列出的威胁情报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**)。

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：

要创建数据包捕获用户，请使用设备控制台(SystemConfig)作为sysadmin用户。

1. 以sysadmin身份登录设备。
2. 选择Advanced > Packet Capture。如果没有现有的数据包捕获，您将直接进入数据包捕获配置菜单。如果有现有数据包捕获，请选择Create以创建新的数据包捕获。
3. 在Port Filter字段中输入TCP或UDP端口号。端口可以是源或目标。您可以将此字段留空以将过滤器设置为“任意”。SLIC使用tcp/443连接，因此在此字段中输入443。

4. 在Duration(900 Seconds Max)字段中，指定执行数据包捕获所需的秒数。



注意：请小心输入合理的时间量，因为超大的捕获文件可能会占用设备硬盘上的所有可用空间。此字段与Packets设置结合使用。捕获一直运行到达到持续时间或数据包数量为止。

5. 在Packets(100,000 max)字段中，指定在结束捕获之前要捕获的数据包数。此字段与“持续时间”设置结合使用。捕获一直运行到达到持续时间或数据包数量为止。
6. 点击OK开始数据包捕获。



提示：要突然停止数据包捕获，通常可以按Ctrl+C。

要查看数据包捕获文件，请下载并在本地查看它们。文件存储在/lancope/var/tcpdump中。

您可以直接登录设备或通过Central Manager资产>查看设备统计信息访问设备。转至Support > Browse Files以下载数据包捕获。

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)。联系时需要提供有效的支持合同：思科全球支持联系信息
- 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）。