Troubleshoot SLIC Channel Down System Alarm

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Procedure

- Common Error Logs
  - Connection Timed Out
  - Unable to Find Valid Certification Path to Requested Target
  - Handshake Failed
- Remediation Steps
  - Step 1. Validate Smart Licensing Status
  - Step 2. Verify Domain Name System (DNS) Resolution
  - Step 3. Verify Connectivity to the Threat Intelligence Feed Servers
  - Step 4. Disable Secure Socket Layer (SSL) Inspection/Decryption

Related Defects

Related Information

Introduction

This document describes how to troubleshoot Secure Network Analytics (SNA) "SLIC Channel Down" system alarms.

Prerequisites

Requirements

Cisco recommends that you have basic SNA knowledge.

SLIC stands for "Stealthwatch Labs Intelligence Center"

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Procedure

The "SLIC Channel Down" alarm is triggered when the SNA Manager is unable to get feed updates from the Threat Intelligence Servers, formerly SLIC.

To better understand what caused the feed updates to be interrupted, proceed as follows:

1. Navigate to Central Management by logging in to the Manager (In your browser address field, type https:// and the appliance IP address. Press Enter.)
2. From the main menu, select Configure > Global > Central Management.
3. Click the Ellipsis icon for the appliance.
4. Select View Appliance Statistics.
5. From the main menu, select **Support** > **Browse Files**
6. On the Browse Files page select **smc > logs >** and then click **smc-core.log**.
7. A new tab opens with the smc-core.log contents. Review this file by searching for the **SlicFeedGetter** logs.

Common Error Logs

The most common error logs seen in the **smc-core.log** related to the SLIC Channel Down alarm are:

Connection Timed Out

```
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
```

Unable to Find Valid Certification Path to Requested Target

```
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
```

Handshake Failed

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

Remediation Steps

The Threat Intelligence Feed updates can be interrupted due to different conditions.

Perform the next validation steps to ensure your SNA Manager meets the requirements.

Step 1. Validate Smart Licensing Status

Navigate to **Central Management > Smart Licensing** and ensure that the status of the Threat Feed License is **Authorized.**

Step 2. Verify Domain Name System (DNS) Resolution

Ensure that the SNA Manager is successfully able to resolve the IP Address for **lancope.flexnetoperations.com** and esdhttp.flexnetoperations.com

Step 3. Verify Connectivity to the Threat Intelligence Feed Servers

Ensure that the SNA Manager has Internet access and that connectivity to the Threat Intelligence Servers listed next is allowed:

Port and Protocol	Source	Destination
443/TCP	SNA Manager	esdhttp.flexnetoperations.com lancope.flexnetoperations.com

Note: If the SNA Manager is not allowed to have direct internet access, please ensure that the Proxy configuration for internet access is in place.

Step 4. Disable Secure Socket Layer (SSL) Inspection/Decryption

The second and third errors described in the **Common Error Logs** section can occur when the SNA Manager does not receive the correct identity certificate or the correct trust chain used by the Threat Intelligence Feed servers.

To prevent this, ensure that no SSL Inspection/Decryption is performed across your network (by capable Firewalls or Proxy Servers) for connections between the SNA Manager and the Threat Intelligence servers listed in the **Verify Connectivity to the Threat Intelligence Feed Servers** section.

If you are unsure if SSL Inspection/Decryption is performed in your network, you can collect a packet capture between the SNA Manager IP address and the Threat Intelligence Servers IP address and analyze the capture to verify the certificate received. For this, perform as follows:

To create a packet capture user the appliance console (SystemConfig) as a sysadmin user.

1. Log in to the appliance as **sysadmin**.
2. Select **Advanced** > **Packet Capture**. If there are no existing packet captures, you are advanced directly to the packet capture configuration menu. If you have existing packet captures, select Create to create a new packet capture.
3. Enter a TCP or UDP port number in the **Port Filter** field. The port may be either source or destination. You can leave this field blank to set the filter to "Any". SLIC uses a tcp/443 connection so enter 443 in this field.
4. In the **Duration (900 Seconds Max)** field, specify the number of seconds to perform the packet

capture.



Note: Be careful to enter a reasonable amount of time because an extremely large capture file can potentially consume all the free space on the appliance's hard disk. This field works in conjunction with the Packets setting. The capture runs until either the Duration or number of Packets is reached.

5. In the **Packets (100,000 max)** field, specify the number of packets to capture before ending the capture. This field works in conjunction with the Duration setting. The capture runs until either the Duration or number of Packets is reached.
6. Click OK to start the packet capture.



Tip: To stop a packet capture abruptly, you can typically press Ctrl+C.

To view packet capture files, download them and view them locally. Files are stored in /lancope/var/tcpdump.

You can log directly into the appliance or access it through the Central Manager inventory > View Appliance Statistics. Go to Support > Browse Files to download the packet capture.

Related Defects

There is one known defect that can impact the connection to SLIC servers:

- SMC SLIC communication can timeout and fail if destination port 80 is blocked. See Cisco bug ID CSCwe08331

Related Information

- For additional assistance, please contact the Technical Assistance Center (TAC). A valid support contract is required: Cisco Worldwide Support Contacts.
- You can also visit the Cisco Security Analytics Community here.
- Technical Support & Documentation - Cisco Systems