Troubleshoot "buffer" Configuration Under Lawful Interception Context in StarOS

Contents

Introduction

This document describes how to troubleshoot the "buffer" configuration under lawful interception context in StarOS.

Prerequisites

Requirements

Cisco recommends that you have knowledge of StarOS.

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.

Abbreviations

LI	Lawful Intercept
LEA	Law Enforcement Agency
AF	Access Function
MF	Mediation Function
DF	Delivery Function
CF	Control Function
IRI	Intercept Related Information
CC	Content of Communication

AF could be any StarOS node. CF resides in LEA premises or Administrative Domain.

Problem

At the time of the configuration of the buffering option under lawful interception module, it is observed that the parameter related to event/content-based buffering option was not available in the CLI configuration list.

This option helps to define the buffer value of default 5000 IRI records and 1000 CC records per LI context.

The only option available in the configuration list was "dest-addr".

```
[li-context]<hostname>(config-ctx)# lawful-intercept tcp event-delivery
dest-addr - Destination IP address where the intercepted information needs to be forwarded.
```

Ideally, it should show the "buffer" keyword along with the "dest-addr" option in the previously mentioned list of options.

Lawful Intercept

> **Note**: Lawful Intercept is a license-enabled feature. The Basic Lawful Intercept license supports UDP as a transport protocol for call content (CC) interception for active subscribers. Event (IRI) interception and TCP as a transport protocol for delivery are not supported under the Basic license. The Enhanced Lawful Intercept license supports all of the Basic LI license functionality plus Event (IRI) Interception and TCP as a transport protocol for delivery of intercepted packets.

The Lawful Intercept functionality provides the network operator the capability in order to intercept control and data messages of the targeted mobile users. In order to invoke this support, the LEA will request the network operator to start the interception of a particular mobile user. This request will be supported by a court order or warrant. There are different standards followed for Lawful Intercept in different countries.

A typical Lawful Intercept process includes these sequence of events:

1. The LEA requests the TSP to start intercepting a session of a particular individual, which usually must be supported by a Court Order or Warrant. Information to identify the individual will be provided (such as Phone Number or Name/Address etc).
2. The Telecommunication Service Provider (TSP) administrator configures the TSP Access Function/Delivery Function to start intercepting Control/Data events of the targeted subscriber. If the Subscriber Session is already in progress, the interception will occur immediately. Otherwise,

the Access Function must wait until the Subscriber Session connects.
3. The Access Function sends a copy of the Control/Data events for the intercepted session to the Delivery Function.
4. The Delivery Function sends the intercepted information to one or more Collection Functions, which are in the LEA's administrative domain. A Collection function analyzes and stores the intercepted information.
5. When the LEA requests to stop the interception, the TSP administrator configures the Access Function and Delivery Function to stop interception for that particular subscriber session.

A Command Line Interface (CLI) over SSH session is used by the DF for LI provisioning and de-provisioning of the target identity, as well as to monitor the LI statistics.

These protocols/modes (IPv4 and IPv6) are supported on the StarOS to deliver LI events and content to the DF:

- UDP (Un-ack) Mode: The address of DF2 and DF3 is provided at the time of provisioning for UDP Un-acknowledged mode.
- TCP Mode: For TCP Mode, the configuration provides the peer address only. All intercepted event delivery (IRI) is sent to DF2 and all the intercepted data (CC) delivery is sent to DF3.

Troubleshoot

StarOS configuration should have a proper license for this feature.

```
[local]<hostname># show license information | grep -i lawful
Monday December 10 01:54:13 UTC 2018
Lawful Intercept [ ASR5K-XX-CSXZZLI ]
+ Enhanced Lawful Intercept [ ASR5K-XX-CS0ZZELI / ASR5K-00-CS00XZI ]
Persistent Lawful Intercept [ ASR5K-XX-CS1ZZPLI ]
Segregating Lawful Intercept Context based on Count [ ASR5K-XX-PWXZZICS ]
```

StarOS also should have “segregated li-configuration”.

With this feature, only "li-administrator" will be able to view and edit the LI interface integration details in a dedicated li context.

The LI admin user should be mapped to li-administration in the configuration.

```
administrator liadmin encrypted password *** ftp li-administration
```

But still, it was found that StarOS did not allow to define the "buffer" option under the lawful-intercept configuration module.

```
[local]<hostname># context li
[li]<hostname># config
[li]<hostname>(config-ctx)# lawful-intercept tcp event-delivery
dest-addr - Destination IP address where the intercepted information needs to be forwarded.
====> customer do see only this option

[li]<hostname>(config-ctx)# lawful-intercept tcp event-delivery buff
Unknown command - "buff", unrecognized keyword
```

Ideally one should see an option with keyword "buffer" to complete the CLI like this for the buffer configuration.

```
configure
context
lawful-intercept tcp event-delivery buffer max-limit <1000 ... 50000>
end
```

Resolution

In order to get the li-admin rights for any StarOS user, that user should be defined under li context with admin privileges. It is the li-admin user that need to log in from an external server (from LEA) in order to enable this "buffer" option. Any other administrator user who tries to login into node under local context will not be allowed to define this "buffer" option.

Here are the steps in order to achieve the requirement in getting the "buffer" option in StarOS under LI module.

1. Log in to the node with local admin user.
2. Create li context (as there was no dedicated li context there).
3. Create li user with li-admin privileges in the local context.
4. Create li user with li-admin privileges in li context.
<<we removed li-admin from the local context to add dedicated li which will help us to enable the segregate the li context from local context >>
5. Remove the li user with the li-admin privilege from the local context.
6. Create a dedicated-li context in order to enable segregate li configuration.
7. Define access-list under li context.
8. Logout from node.
9. Log in into node again with “li” user who has privileges as li-admin.
10. Configure the buffer option that is required, it should allow you to configure it.

Configuration

```
configure
context
lawful-intercept tcp event-delivery buffer max-limit <1000 ... 50000>
end
```

For example, after you log in with the use of the li-admin user, you can see all the options that we need:

```
<local-node><hostname>$ ssh li-admin@li@<local context IP of node>
Cisco Systems QvPC-SI Intelligent Mobile Gateway
li-admin@li@aa.bb.cc.dd's password:
Last login: Wed Jan 23 17:32:31 -0500 2019 on pts/2 from 10.xx.yy.zz.
Cisco Systems QvPC-SI
Lawful Intercept Interface

No entry for terminal type "xterm-256color";
using dumb terminal settings.
[li]<hostname># configure
Warning: One or more other administrators may be configuring this system
[li]<hostname>(config-ctx)# lawful-intercept tcp event-delivery
```

buffer - This is used to configure the LI buffering >>>>>>> **We can see the buffer option now.**

dest-addr - Destination IP address where the intercepted information needs to be forwarded.