Tactic LI System Package by Decision Group

For Cyber Investigation, Lab and Training of LEA

Contents

1. Introduction 1
2. Tactic LI Operation 2
3. Tactic LI Solution by Decision Group 3
3.1. Data Access at the Target Network 3
3.2. Target Traffic 3
3.3. Deployment 4
4. Assessment on Decision Group Tactic LI Solution 6
4.1. Advantages – 6
4.2. Disadvantages – 7
5. Customized Scope of Work 7
6. Decision Group LI Solution Package 8
7. Decision Group 9
Appendix 1: Estimated Finance Statement 11

1. Introduction

Tactic lawful interception operation is usually carried out by investigator for urgent and temporary action with definite targets for communication monitoring. The difference between tactic and permanent lawful intercept is the LI device used for tactic operation without acquisition capability of target provision data. So it can be used flexibly to link with TSP network facility without too much deployment concern.

TSP network assistance for a successful LI operation is a must when investigator request LI task, because there is no target provision data available. The monitoring period is normally for few days to one or two weeks, and sometimes it may be longer than one month by special approval from authorized organization, but it is not so often.

It is deployed by LEA investigator at the gateway network segment in TSP data center or in Internet Exchange Gateway (IEX) by the help of network management staff for locating target subscribers. Normally TSP will ask to separate its own network facility from Tactic LI system for security or network management concern by firewall.

The network provision data may not be available directly, but provision data of online services can be obtained through link analysis process on the target content of transportation layer from intercepted traffic. So, the capability of content reconstruction is very important for tactic LI system.

2. Tactic LI Operation

For a tactic LI operation carried out by both investigator and TSP, there are 3 major factors taken into account:

The first is the complete functionality of tactic LI system with data access, protocol decoding, content reconstruction and data analysis. Such system must be also equipped with good security mechanism for user access and data protection. Decision Group Tactic LI system set is a good choice for LEA to take tactic LI operation in the field.

The second is the target provision data availability by the help of TSP network management staff. Usually network management staff can filter out target traffic by its ID (ANI, IMSI…), and send all the target traffic to DG Tactic LI system for monitoring by authorization.

The third is quite important, because such operation between TSP and LEA should be authorized legally. That's approved warrant order from authorized organization with clear definition of period.

Sometimes, TSP will charge LEA by the intercepted traffic volume and service duration time. So before tactic LI operation, there is an SLA agreement between TSP and LEA.

3. Tactic LI Solution by Decision Group

Basically HTTPS interception is the core of DG Tactic LI system solution. It will be achieved by 2 different ways: forward proxy or transparent proxy. When this function is adopted in Tactic LI system, it is usually configured as transparent proxy for interception on HTTPS traffic, and works with E-Detective for non-HTTPS traffic.

It uses MiTM attack to intercept target HTTPS traffic for content reconstruction and service provision data availability (service CDR). It also provides certificate replacement control for intercepted traffic returned to TSP network in order to hide the LI operation from target subscribers.

All reconstructed data in the system will be saved with raw data for prosecution and judiciary purpose. There is primary data scoping utilities built-in to make portable MD5 hashed media for evidence submitted to court, and link analysis tool for identification on relationship among different targets.

For single system, the capability of HTTPS interception is at 300Mbps in term of system throughput.

3.1. Data Access at the Target Network

Though it is quite important for DG Tactic LI system to access target data from target network, it is quite flexible and quick to deploy it for different purpose – non-HTTPS or HTTPS interception. It is usually link with PDN gateway or toll gateway as transparency proxy in TSP network facility or as proxy with International Exchange gateway (IEX-GW) site for target HTTPS traffic interception.

By the assistance of network administrator, the target HTTPS traffic will be routed into Tactic LI system for interception and monitoring, and returned HTTPS with different certificate will be back to core network for continuing communication session.

There is one more thing taken into account: traffic volume. Since the maximum system throughput is 300Mbps, we need to add a traffic load balancer for more than 200 Mbps HTTPS traffic volume to multiple HTTPS interceptor modules inside Tactic LI system. So, appropriate site survey on the network traffic volume should be sized for deployment of Tactic LI system.

3.2. Target Traffic

There are 2 type of target traffic: non-HTTPS and HTTPS traffic. All must be directed to Tactic LI

system by the help of network administrator of TSP. For non-HTTPS traffic, network administrator can mirror the target traffic into Tactic LI system for interception, whereas HTTPS, as explained previously, is directed to transparent proxy module in Tactic LI system and returned to target network after intercepted.

The impact on the target network will be in the side of HTTPS interception. So, pay more attention on the routing and processing performance of HTTPS interceptor modules in Tactic LI system. It is quite important to check the sizing information for number of HTTPS interceptor modules inside Tactic LI system.

3.3. Deployment

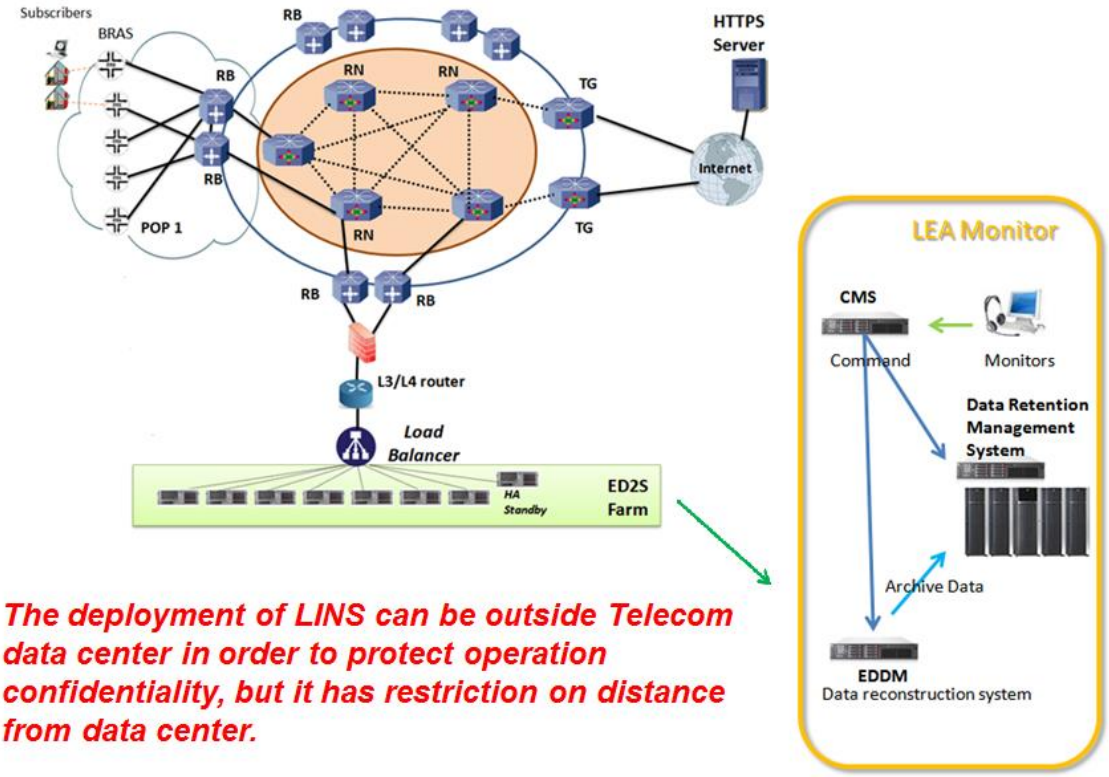
In DG Tactic LI system, there could be 2 to 3 sets of HTTPS interceptor module and 1 to 2 sets of E-Detective module for both HTTPS and non-HTTPS traffic interception. In order to distribute the high volume of target traffic, there can be deployed a traffic load balancer for fulfill this requirement. All system modules can be deployed together in the same rack mounted trolley as an independent LAN segment – Lawful Interception Network Segment (LINS).

For target non-HTTPS traffic, it will be mirrored from TSP network by the help of system administrator, whereas target HTTPS traffic will be directed from core network to LINS and reverted back to core router after HTTPS intercepted.

Between LINS and TSP network facility, there is firewall for network domain separation.

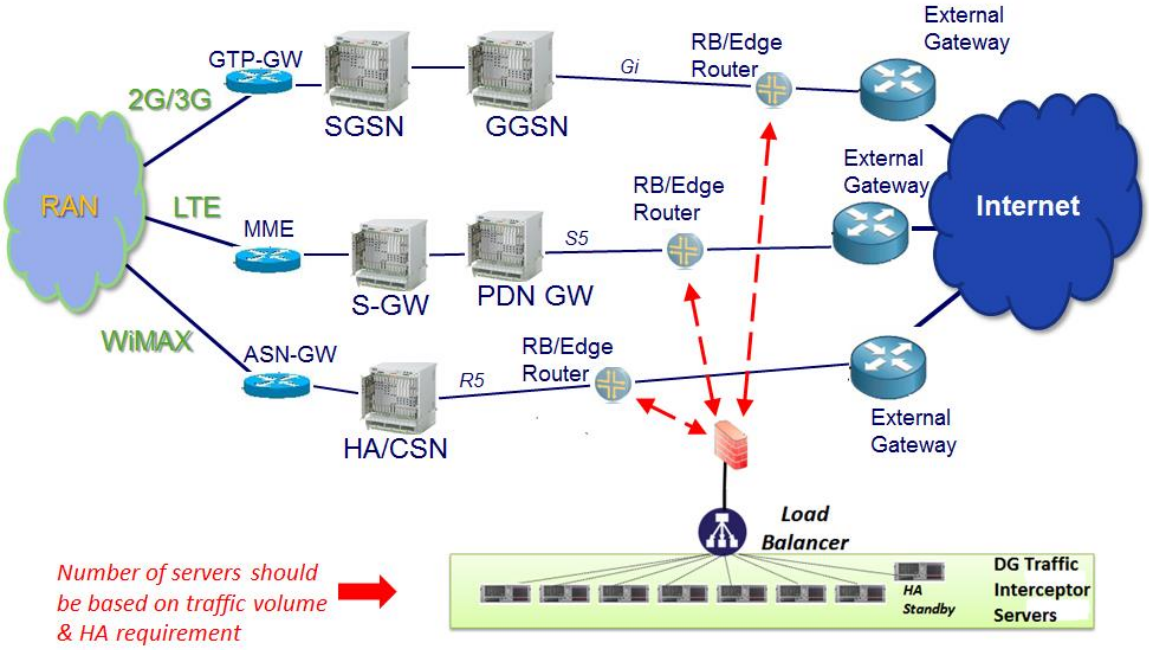
Below are 3 different types of deployment in fixed network, mobile networks and internet exchange gateway center. Please be aware of the below examples, which are only for explanation of deployment in different network instead of real deployment. For real deployment, we still need to conduct the site survey on the factors behind network infrastructure. In reality, LEA staff can also reference the below deployment for their use of Decision Group Tactic LI package.

For fixed network:

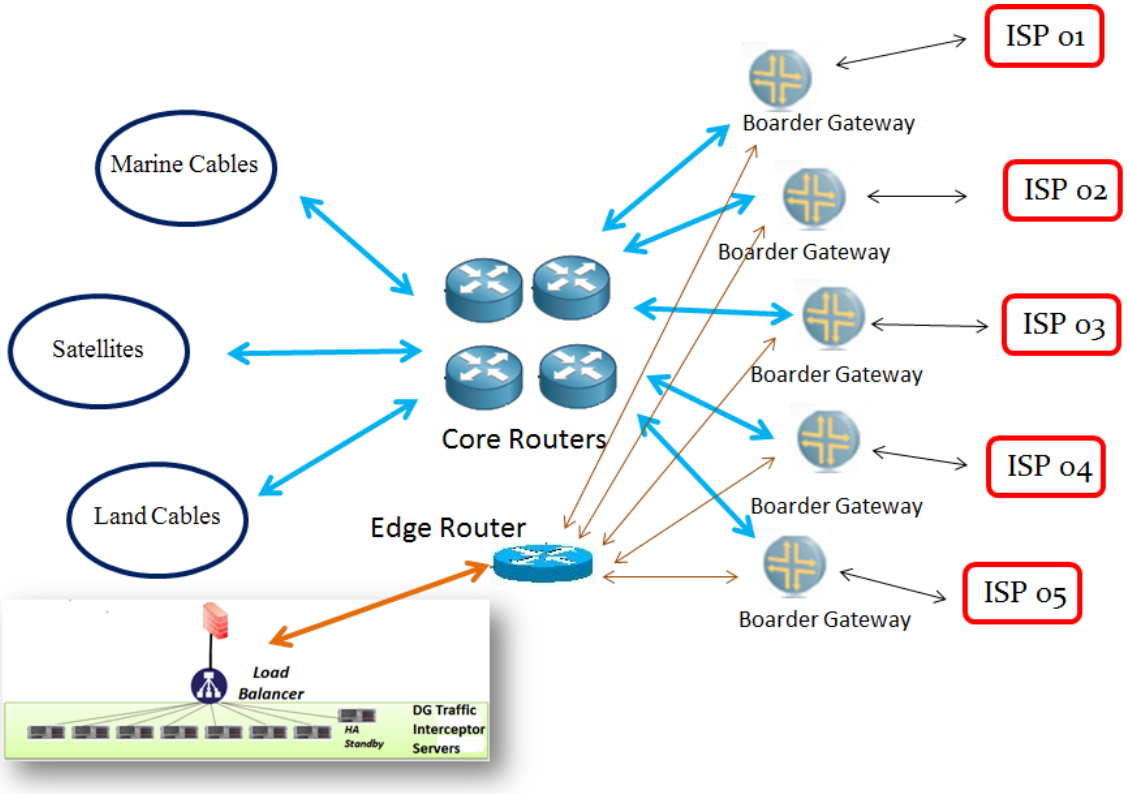


The deployment of LINS can be outside Telecom data center in order to protect operation confidentiality, but it has restriction on distance from data center.

For mobile networks:



For Internet Exchange Gateway Center:



4. Assessment on Decision Group Tactic LI Solution

There are big different between tactic LI operation and regular LI deployment in terms of deployment, standard operating procedure, data access, process auditing and authorization. The pros and cons of tactic LI operation compared with regular LI deployment are below:

4.1. Advantages –

1. It can provide functions of data access, protocol decoding, content reconstruction and data scoping within box, and process intercepted data seamless and quickly for urgent requirement.

2. It can perform interception on both non-HTTPS and HTTPS for monitoring as well as provide certificate replacement for completing communication between target subscribers and content service providers.

4.2. Disadvantages –

1. Operation is carried out for short period of time, usually few days to 2 weeks and no more than 60 days.
2. Operation must be relied on assistance of TSP network administrator for target provision availability.
3. For HI2 data availability if required, TSP must offer its provision data to Tactic LI system.

It can be deployed flexibly and quickly with network facility inside TSP data center.

5. Customized Scope of Work

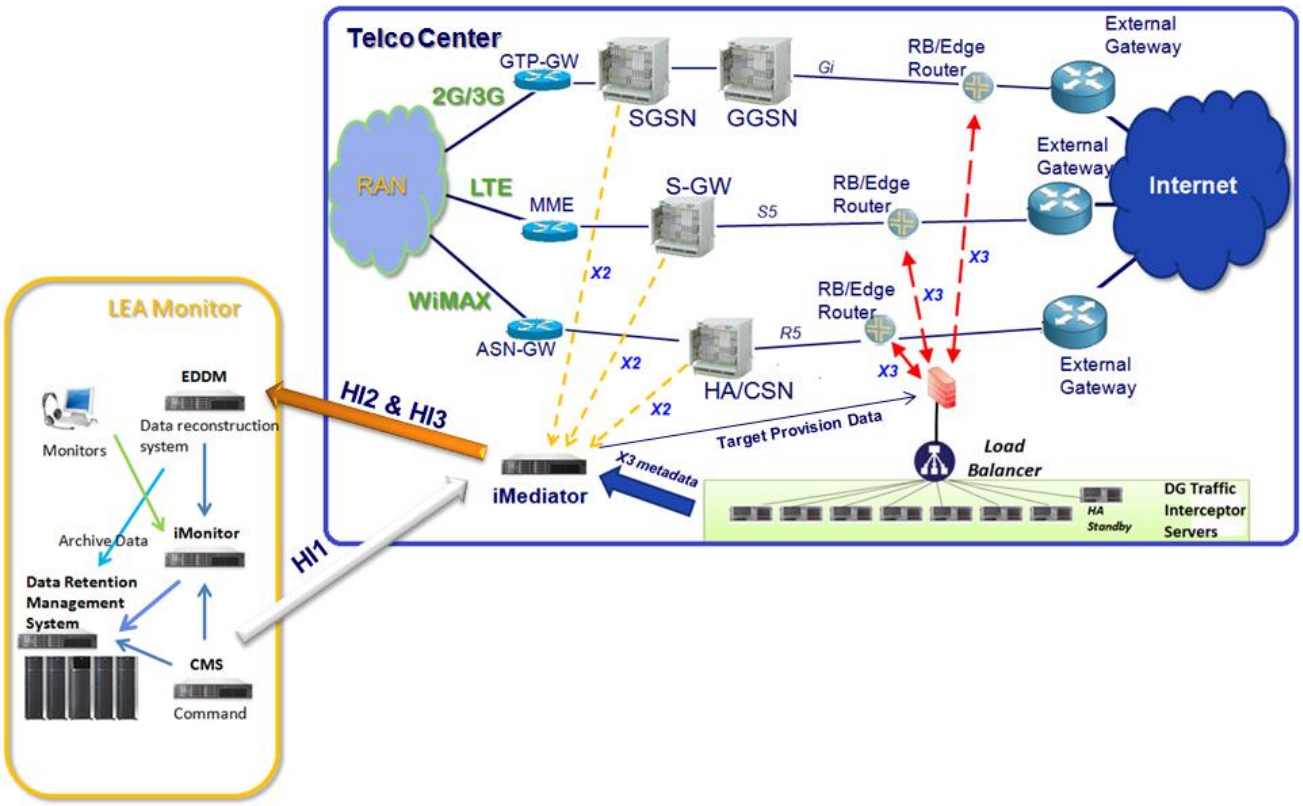
Tactic LI system is only for urgent and temporary operation, so there is no provision and warrant data available for its application. DG can provide customization service for provision data availability by customer requirement.

What Tactic LI system can get is the provision data of target subscribers online to access. Sometimes, the network provision data is available by the help of TSP. The formal investigation report must contain all provision data, which are both of network and online services, and warrant administration data with target ID, LI ID, TSP ID and LI operation date/time…etc. All these data can be input into system manually. DG provides a case management user interface for the above data entry.

For HTTPS interception, there must be state root trust certificate in target PC, laptop or mobile device for complete the HTTPS interception cycle.

It can be done to preload the provision data by mirroring AAA system into E-Detective for provision availability.

Below is shown how to upgrade tactic LI package into regular LI platform in mobile networks as an example by introducing Decision Group iMediator with Tactic LI Package:



6. Decision Group LI Solution Package

In order to provide an in-house design package, Decision Group provides a Tactic LI system package for target LEA customers in the field of cyber investigation, training and lab. LEA customers can also adjust the equipment in the package for the requirement of target environment flexibly.

The Tactic LI system package provided by Decision Group is accommodated in a movable trolley with rollers as an independent LI suite inside TSP data center and can be maintained remotely by LI staff through VPN network. The whole basic package is consisted of:

- 3 units of full function **E-Detective**, which provides interception capability of both non-HTTPS and HTTPS traffic and primary data link analysis tool, and these 3 unit can be adjusted to intercept non-HTTPS or HTTPS traffic separately,

- one unit of **data retention management system** (DRMS) with less than 6TB capacity storage, which can provide room for reconstructed data archiving from frontend E-Detective systems,
- one unit of **12 port switch**, which is for network link among E-Detective and DRMS systems,
- one unit of **traffic load balancer**, which is for incoming X3 traffic load dispatching to 4 units of E-Detective, and
- one unit of **router** with firewall function, which is for link with TSP network and remote login from LEA site,
- Options of UPS, 22U rack with rollers, tracking sensor (GPS or NFC), ventilation facility, security locks, cable management brace frame, monitor and KVM are available separately up to customer choice.

Form factor size of all equipment are around 12U height in 22U rack, in which there are 4 units of 2U server systems(HP DL380), 1U switch, 1U traffic load balancer, 1U router, and 1U sharable KMV unit inside mobile rack as LI system trolley for LEA investigator.

7. Decision Group

Decision Group is a company focusing on worldwide renowned DPI application of E-Detective. Decision Group, established in Taipei, Taiwan since 1986, is one of the leaders in manufacturing of PC-Based Multi-Port RS232/422/425 Serial Cards, Data Acquisition & Measurement Products and Industrial Automation and Control Systems.

Decision Group, since the year 2000, started new line of business involved in designing and development of equipment and software for Internet Content Monitoring and Forensics Analysis Solutions. Now Decision Group positions itself as a solution provider with full spectrum of product portfolio on network forensic and lawful interception. The excellent core network forensics products and training programs in our list are:

(i) **E-Detective** – work as strategic lawful interception device

(ii) **Wireless-Detective** - WLAN Internet Interception and Content Analysis Solution

(iii) **Lawful Interception Suite** –

a. **iMediator** – for lawful interception operation as mediation platform

b. **EDDM** – for lawful interception operation as content reconstruction and monitoring system in LEA Monitoring Center on packet switch telecom network

c. **iMonitor** – for warrant administration process and intercepted data presentation in TSP network center or LEA Monitoring Center

d. **iMedia Gateway** – for lawful interception on VoIP/SS7/ISUP signaling data of circuit switch telecom network

e. **Data Retention Management** – for long-term lawful interception data retention management with SAN or NAS system

f. **Tactic Lawful Interception Pack** –trolley system with integrated function of data access, collection, reconstruction and management for short term lawful interception operation of LEA

(iv) **HTTPS-Detective** – 2 types of HTTPS Interception Solution, and each for LAN (forward proxy) and Telecom networks – ED2S (transparency proxy)

(v) **Centralized Management System** – for centralized management on distributed frontend E-Detective, ED2S, EDDC, Data Retention Management systems

(vi) **EDDC** - Offline Internet Packet Reconstruction and backend data reconstruction engine Solution

(vii) **VoIP-Detective** - Voice over Internet Protocol (VoIP) Interception Solution

(viii) **NIT** - portable Network Investigation Toolkit

(ix) **FIT** - portable Forensics Investigation Tool (MS Windows based)

(x) **Knowledge base Platform (KbP)** – parallel indexing system for big data management with defined business rules built-in in the field of behavior pattern (modus operandi) analysis, text mining…etc.

In order to provide better service, Decision Group also provides several different level of training programs based on customer requirement. These programs are usually delivered by qualified local instructors, senior cybercrime investigators or scholars in university. These are listed below:

(i) **Network Packet Forensic Analysis Training (NPFAT)** - Network Packet Forensics Analysis Training

(ii) **Lawful Interception Training (LIT)** – on lawful interception planning, deployment and

delivery

(iii) **Cyber Intelligence Training (CIT)** – cyber intelligence deployment and delivery for national security

(iv) **Cybercrime Investigation Training (CCIT)** – co-work with National Taiwan Central Police University and Taiwan CIB on training of cybercrime investigation skill and theory for LEA staff

Besides the above products and training programs, Decision Group also provides consulting service on planning of lawful interception and cyber intelligence to our partners and customer. With lots of deployment experience in different countries, DG consultants will provide streamline lawful interception process from warrant authorization to data collection on telecom networks, and fully meet global and state mandates and regulation.

Head Quarter office of Decision Group is now in Taipei, Taiwan with 45 engineers in developing network forensic solutions and consulting service in network forensics division for more than 14 years. Decision Group Head Quarter owns copy right of all above highlighted product names and the blue world map logo for global sales marketing.

There are several sales and service points around the world for direct service to our partners and clients in Asia, Europe, North and Latin America, African and Middle East. All product service requests will be directly through Service Department in Decision Group Head Quarter for ensuring high standard of customer satisfaction, because we treat all customers as our VIP clients.

Please also check out our website: http://www.edecision4u.com for more product sales, technical and service information. Wherever you are, if you need more information about our products and services, please contact with decision@decision.com.tw. We'll be glad to give you our utmost support service.

Appendix 1: Estimated Finance Statement

Attached is the estimated generic finance statement for the above package. The final one will be submitted to you once we finished the site survey. You could still use this statement as your budget planning by proportional estimation. Please see the attachment for your information.