# PALI™ - PineApp™ Lawful Interception Whitepaper

## Introduction

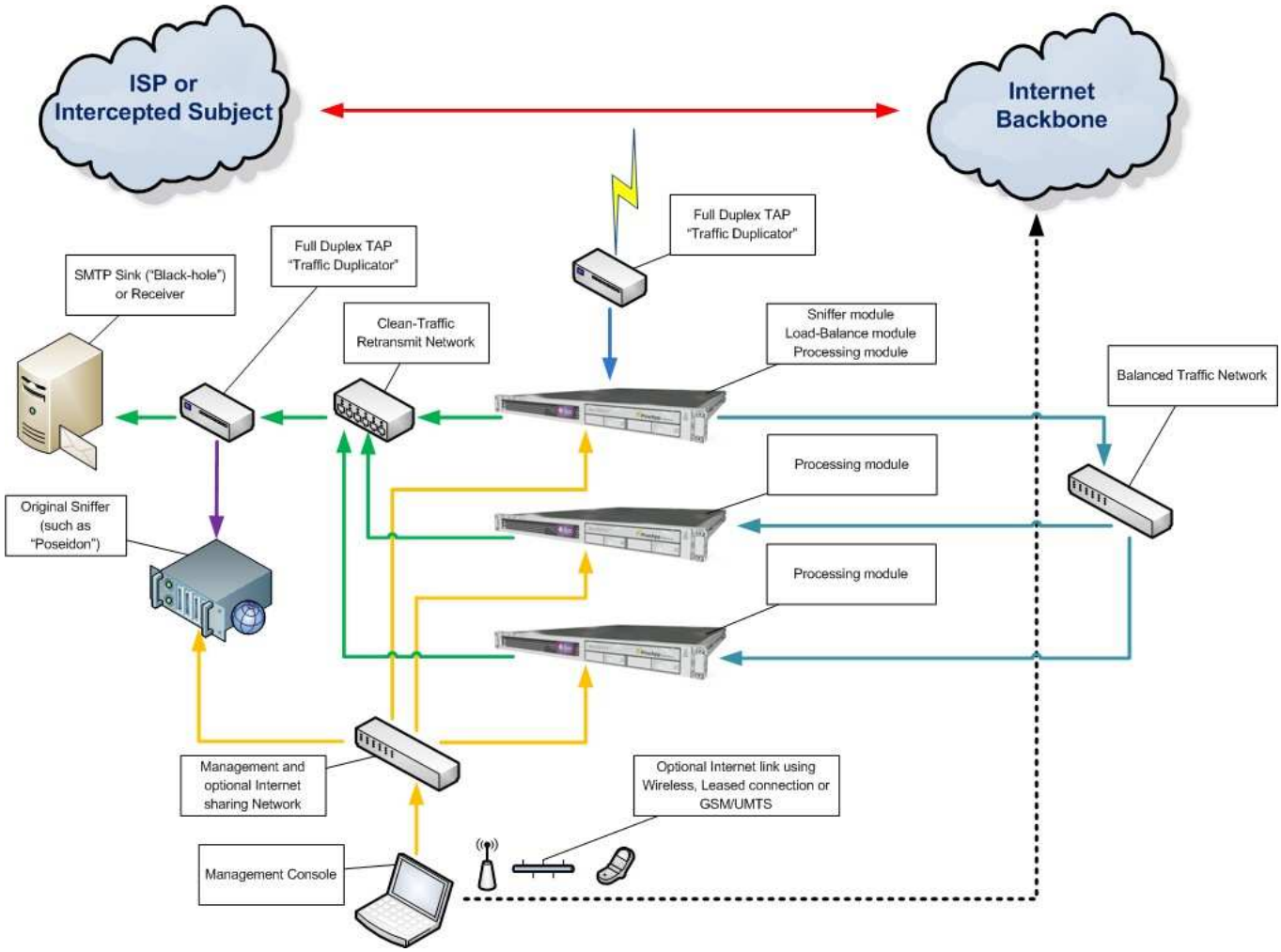
Lawful interception is the interception of telecommunications by law enforcement agencies (LEA's) and intelligence services, in accordance with local law and after following due process and receiving proper authorization from competent authorities.

The biggest challenge in email lawful interception resides in the fact that more than 90% of the email traffic is invalid: Spam, Phishing & Viruses. Due to this fact, it has become almost impossible to extract information in real-time as most of the processing time is wasted on analyzing irrelevant content. To make it even harder, using standard anti-spam/anti-virus devices is impossible since the traffic is not directed to the unit, but rather "captured".

Based on the award winning Mail-SeCure product, PineApp Lawful Interception Solution – PALI™ – offers a complete and flexible end-to-end solution for any infrastructure, filtering all the non-relevant content, thus providing pinpointed and accurate processing of the relevant information. Furthermore, Mail-SeCure enables real-time content analysis of mail traffic, in-addition or instead of existing content extraction systems.

## Infrastructure

The following diagram illustrates a typical PALI™ infrastructure:



## How does it work?

**Components:**

• **Mail-SeCure** – the base component of the solution; Mail-SeCure is used to filter and categorize the sniffed traffic. Furthermore, it is used as the platform for the PALI™ components.
• **PALI™ Sniffer module –** a dedicated SMTP sniffer; has the ability to "capture" all SMTP conversation and format it in a form suitable for processing by Mail-SeCure.
• **PALI™ Load-Balance module –** a weighted-round-robin load-balancer, responsible for balancing the "captured" traffic between the Mail-SeCure units, provides scalability and achieves a higher processing performance. This component is optional and is not needed on a stand-alone environment (when only one Mail-SeCure unit is used).
• **PALI™ Processing module –** is responsible for queuing the captured messages into Mail-SeCure's regular scanning-queue system. On large clusters, it is not recommended to enable this module on the unit which is responsible for the sniffing of the traffic.
• **TAP device/"Traffic duplicator"** (not provided by PineApp) – is used to duplicate the traffic without intervening with the original traffic and to allow capture of the SMTP protocol. In some devices, definition of port-mirroring or usage of a hub (instead of a switch) may be enough.
• **SMTP Sink or "Receiver"** (by default, not provided by PineApp) – acts as a "black-hole" for the SMTP traffic, since on some occasions PALI™ is added to an existing solution which has only the ability to sniff/capture the traffic but not to receive a direct SMTP session. Therefore, Mail-SeCure units retransmit the traffic towards the SMTP Sink in order to allow the information to be recaptured.
• **Switching devices** (not provided by PineApp) – are used to interconnect the devices.
• **Management console** (not provided by PineApp) – is used to control the entire infrastructure and optionally to share the Internet connection.

Workflow of a typical clustered solution:

• Red – the original traffic of the subject to be intercepted, a TAP device is connected to this link and the traffic is duplicated.
• Blue – the TAP device which is connected to the intercepted network in one end is connected to a Mail-SeCure unit which captures the SMTP traffic using the PALI™ Sniffer module. The Mail-SeCure parses the captured information and then distributes the traffic between the entire traffic using the PALI™ Load-Balance module. Part of the traffic which is directed for local processing is processed by the PALI™ Processing module.
• Cyan – the Mail-SeCure with the PALI™ Sniffer module distributes the traffic using an encrypted dedicated network to achieve maximum security and best performance. PALI™ processing module within the rest of the Mail-SeCure units, detects new messages and queues them into Mail-SeCure system for processing.
• Green – clean traffic is retransmitted from Mail-SeCure units towards the SMTP Sink/Receiver component to allow analysis of clean traffic only. An alternate TAP device is connected to the retransmit network in one end and to the original capturing device on the other (represented in Magenta) thus providing content extraction by the original device which most commonly works on capture-mode only.
• Orange – this dedicated network allows management of the devices without intervention of the normal operation of the system. In addition, since Mail-SeCure requires Internet connection for best filtering results, the management console can be used to share the Internet connection using any media such as wireless, GSM/UMTS or any other (represented in dotted Black).