PertSol®
Simple Solutions for Complex World

WHITE PAPER

ILD iNterception

Lawful Interception & Monitoring System For IPLC Network

NEED FOR LI

For IPLC

With the advancement in communication technologies, the way organised crime syndicates operate throughout the world have changed drastically. While many technological advances have been exploited for conducting criminal activities, none has likely had greater impact or influence than the internet. This exploitation of the Internet has not only given rise to a completely new form of crime but is also facilitating criminality across other crime areas. Therefore in order to combat such illicit operations, Law Enforcement Agencies (LEAs) must have access to suspicious communications that allows them to nip the bud at an early stage. To enable access to such communications, Governments across the globe have made it mandatory for the Telecommunication Service Providers to intercept communications and transmit to LEAs for further analysis. Lawful Interception (LI) is one of the regulatory requirements that the telecommunication service providers must satisfy as a legal obligation towards the national security of the country in which they are operating their businesses.

IP private leased line turnout to be an important medium for internet data transmission with in countries-contenents To rectify and monitor the traffic going outside the national border every service provider shall implement Lawful Interception System so as to facilitate the interception of all kinds of IP interfaces over which Leased Line services are provided by the operator based on the criteria defined by Law Enforcement Agencies like IP Addresses, Url etc.

iNterceptor

Lawful Interception of IPLC Network

PertSol iNterceptor is a unified Lawful Interception System for network operators and service providers which is fully compliant to the international standards and has a proven track record. It is a complete solution which is capable of handling both circuit switch and packet switch traffic from both legacy as well as latest telecom technologies including PSTN, 2G, 3G, 4G, 5G, NGN, IMS, IPLC and others.

The core purpose of iNterceptor is to intercept the traffic and convert intercepted traffic into a format suitable for delivery to the National Authorities or Law Enforcement Agencies, over a secure network. It can also retain the intercepted traffic for future use by the LEAs.

PertSol iNterceptor platform along with iNteliProbes intercept the IPLC traffic using the probes that capture the data & intercept the required information & transmit it towards the LEA through LI Mediator & Management platform situated at central monitoring location. The mediator server carries out reconstruction of entire TCP traffic for various protocols including HTTP, Telnet, FTP, POP3, SMTP, NNTP & many other un-encrypted protocols. SSL decoding is also supported wherein private keys are available.

iNterceptor solution is designed to change and adapts as per latest network upgradation & technologies. It protects investments through its modular setup, accommodating network expansion as well as network changes. It can also integrate with existing Lawful Interception solution incorporating it in a centrally managed unified solution.

Interception Criteria

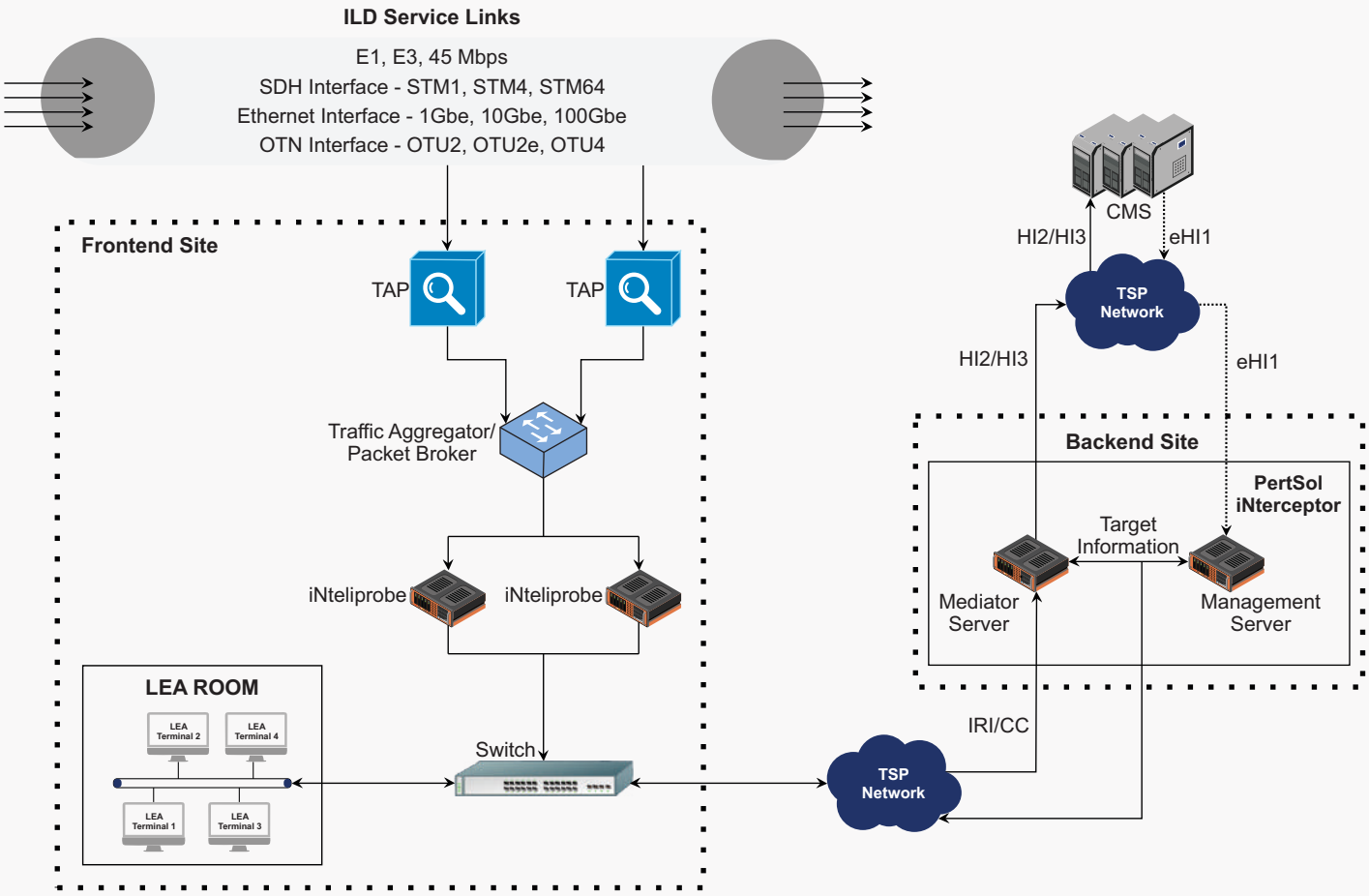
iNterceptor is capable of intercepting content using the criteria below:

MAC Address	ATM Address/X25Address (If in network)	L2VPNIdentifier
Source IP (IPv4, Ipv6)	Destination IP (IPv4, Ipv6)	VOIP Identifier
Subnet IP Address	LL Circuit Number	LL Channel Number
L3 VPN Identifier	TCP Port number & range	UDP Port number & range
SCTP Range	Radius, AAA & DHCP username	Chat Nickname – For unencrypted traffic if available
Email Address (SMTP, POP3, IMAP4)	Web mail (To, From, CC)	URL Address
IM Group	Keyword (case Insensitive)	User Group (i.e. Yahoo user group)
Phone number (including VOIP)	SIP (URI/Phone/Email)	Leased Line (Circuit/Channel Number)
MPLS Tag (RD/RT+IP address)	STM Link ID	Customer Location
STM Channel Number	IM-ID	

iNterceptor can intercept content using any combination of the above-mentioned criteria which includes boolean condition (AND, OR, NOT etc.). It is also possible to group targets on the basis of the following rules:

- Packets originating from or destined to an IP - Sub-network
- Packets between two specific IP – Sub-network
- Packets originating from a specific IP address (client or server) and port-range
- Packets destined to a specific IP address (client or server) and port-range

IPLC - LIMS Architecture



Supported

Technical Specification & Parameters

Standards & Regulations

ETSI TS 101 331: " Lawful Interception (LI);

Requirements of Law Enforcement Agencies"

ETSI TS 102 232-01: "Lawful Interception (LI);

Handover specification for IP delivery".

ETSI TS 102 232-03: "Lawful Interception (LI);

Service-specific details for internet access services"

ETSI TS 101 671: "Lawful Interception (LI);

Handover interface for the Lawful Interception of telecommunications traffic"

ISP Traffic Legal Intercept and Monitoring

System – SD/IMC-01/01. MAR 04 (India Specific)

IPLC Traffic Lawful Interception & Monitoring System

GR/IPLC-01/01 JUL 2007 (India Specific)

Network Interface

E1, E3 interface as per ITU-T recommendation G.703	STM-1 interface as per ITU-T recommendations G.703 or G.783	10/100 Mbps Auto sensing Ethernet as per IEEE 802.3
OTU-2/OTU-2e/OTU-4	45 Mbps as per ITU-T recommendation G.703	STM-4/64 Optical interface mono-mode/Long haul/short haul
10G/100G Ethernet		

Audio Codecs

✓ Common Codecs

G.711 PCM mue law, G711 PCM A-law	Audio Codec G.722/G.722.1/ G.722.1 (Siren14)	G.723/G.729
MPEG-4 AAC-LC/MPEG-4 ACC-LD	SPEEX	Vorbis, ADPCM

GSM Codecs

GSM-EFR	GSM-HR	GSM-abis

3GPP Codecs

AMR - NB Rates: 4.75, 5.15, 5.9, 6.7, 7.4, 7.9, 10.2, 12.2	AMR - WB Rates: 6.6, 8.85, 12.65, 14.25,15.85, 18.25, 19.85, 23.05, 23.8

Video Codecs

H261/H263/H263+/H264 Standard video implementation	x264, FFH264, OPUS codec, Vc1	JPEG Compression Video
Dirac, DV Demultiplexing support	Zlib compression base videos	Video Codecs implemented using H264 standard over dynamic RTP payload type values
VP series Codecs Vp3, VP5, VP6, VP6A	Theora	WMV series video codec decoding
Encrypted Video traffic sent over RTP with keys available in SDP (i.e. SRTP)		

Traffic for Interception

IP Traffic

Our solution discovers and collects data based on IPv4 or Ipv6 internet access. IP access can be static Ipv4/IPv6 addresses or subnets, DHCP assigned via MAC address or RADIUS login.

VoIP Traffic

Our solution can discover and collect data on VoIP calls that use:

ITU-T H.323, H.248, G.711, G.722.2, G.723.1, G.726, G.728, G.729AB	SIP + RTP	SIP + SRTP

SIP over TLS + RTP	SIP over TLS and SRTP	RTP header Compression systems with and without extensions
Packetized GSM and Data Traffic over TDM and IP	De-multiplexing of voice sent over IP with and without RTP header	De-multiplexing of Bundling of Multiplexed IP traffic which contains TCP, UDP, SCTP etc, traffic over fixed ports

It is capable of identifying and extracting the signalling parameters as well as voice payload.

✔ Email Traffic

Our solution can discover and collect data based on target's email activity. It supports email based on SMTP, POP3 and IMAP4. The monitored traffic can be all emails or can be specified as target email id like abc@domainname, local name (at any domain), @domainname (any local name on this domain). Targets can be specified as receiver of emails (including CC & BCC) or sender of email or both. Our system collects the email session, the full email and its attachments.

Our solution can also monitor and collect data from webmail. The webmail session is captured and decoded with the information extracted and delivered in RFC822 format (email text, folders, drafts) and byte stream with metadata (attachments).

Some of the supported email protocols are SMTP, POP3, IMAP4, Windows Live Email, QQ mail, Lotus Notes, Thunderbird mail system and other commonly used systems.

✔ IM/Chat Traffic

Our solution is capable of collecting data for all IM/Chat activity. Options for delivered traffic includes key IM/Chat events, or the full IM/Chat session, including (when possible) advanced features such as audio, video, and file sharing, formatted using RFC 3920/3921 XMPP for IM/Chat text and presence information, video files, summary information, and events.

✔ HTTP/HTTPS and DNS Traffic

Our solution can detect and collect based on DNS domain lookups and HTTP/HTTPS traffic based on URL,

HTTP header and SSL handshakes. Traffic can be discovered and collected for all web activity or can be specified with targeting information including the client, a website or a specific type of traffic.

File Transfer/Sharing Traffic

Our solution can detect and collect data based on file transfer activity such as FTP, BitTorrent, Gnutella, SMB V1/V2 and others.

Fax Over IP

Supports fax over IP that use ITU-T T.37, T.38

Encrypted Traffic

Our solution can detect and collect encrypted information such as certificates, Public Key, Encryption, Authentication & integrity algorithms, Server Key & Session key information. Some of the encrypted algorithms supported by our system are DES, 3DES, AES-128, AES-256. It also supports SIP over SSL, POP3 over SSL, HTTPS, OpenSSL, Openswan & other encrypted traffic provided their keys are available.

BENEFITS OF iNterceptor

Solution With Excellent Capabilities

High Performance Mediation - iNterceptor is capable of handling network with very high throughput requirements. It can handle multiple 100 Gbps links and is capable of selecting required traffic from these links.

Integrity Check Mechanism - The integrity check mechanism periodically checks the network elements and if required correct the erroneous states. It will query the network element for the placed intercepts and add missing intercepts, remove invalid intercepts, etc. This mechanism is used to detect and correct both network flaws as well as tampering with the interception solution. In case of correction of an erroneous state, this will be notified to the operator.

Extensive Interface Adapters – iiNterceptor has a vast range of Input/Output adapters which makes itcompatible with all the available access technologies and network equipment of all the major equipment providers. By allowing multiple Input and Output Adapters to be combined in one system, iNterceptor can be configured to support any situation, even mixing circuit switched and packet switched technologies in the same system. If required, customer specific Input or Output adapters can be developed. Because of the true modularity of the iNterceptor, these specificallybdeveloped adapters can generally be offered at the same price as a standard license. Due to its design philosophy, iNterceptor can support hybrid networks with equipment from different vendors on same server. When networks grow or change, iNterceptor can easily be extended to cater for the growth in traffic volumes or new types of network elements.

Compliance - Unified solution for all interception requirements of a service provider which is compliant to international standards like 3GPP, ETSI, ATSI, ANSI, CALEA and others. It also complies with local LI regulations of many countries across the world.

Proven Field Record - PertSol's LI is a proven and mature solution that continues to benefit from functional enhancement & feature evolution. It has been deployed in varied networks, enabling TSPs / Law Enforcement Agencies to benefit.

PertSol®

Simple Solutions for Complex World

Reach us at

INDIA

Corporate Office:
720 Midas Sahar Plaza, J.B. Nagar,
Andheri East, Mumbai 400059,
Maharashtra, India

+91 224 023 5503

Sales Office:
Unit No: 05-012, 5th Floor, Tower-B,
Emaar Digital Greens, Sector-61,
Gurugram-122011, Haryana, India

+91 124 427 3777

USA

Sales Office:
6379 Clark Ave.
Suite 260 Dublin CA 94568,
USA

contact@pertsol.com

www.pertsol.com