



## NETWORK SOLUTIONS for Internet service providers and companies

### Lawful interception requirements for Internet service providers

Across the globe governments are putting legislation in place that requires Internet service providers (ISPs) to provide interception facilities to law enforcement agencies (LEAs). When an ISP receives a legal order from a LEA, the order should be provisioned on the ISP's lawful interception equipment. All communication as detailed in the order would then be intercepted, and delivered in the specified electronic format to the LEA by the lawful interception equipment.

Some challenges ISPs might face are:

- Hefty penalties for not complying.
- Lawful interception equipment should not have negative effect on performance and stability of the network infrastructure.
- Restrict access to lawful interception equipment to authorized parties.
- Respect the privacy of an ISP user.
- Simple and effective to manage, even with various LI devices at different locations.
- A non-standard implementation of the network infrastructure might require customizations.

## Lawful Interception

*Crovanto's non-intrusive lawful interception solution for Internet service providers offers a full range of interception services from the interception of traffic to the mediation and delivery of intercepted traffic to lawful enforcement agencies. The solution is fully compliant with international ETSI standards for lawful interception and can intercept IP, Radius, e-mail (SMTP, POP, IMAP) and VoIP (SIP, H.323) traffic.*

### Benefits of Crovanto Lawful Interception for Internet service providers

- Crovanto Lawful Interception is compliant with the ETSI standards for lawful interception and covers the full scope of lawful interception legislation for ISPs in the countries Crovanto operates in.
- Crovanto Lawful Interception is non-intrusive and uses passive taps or port mirroring to minimize the effect on the performance and stability of the network infrastructure.
- Various user roles can be defined and sensitive information is encrypted to ensure that only authorized users can access and manage lawful interception equipment.
- Crovanto respects the privacy of ISP network users. We took various steps to ensure that only communication as detailed in the legal order is intercepted and that only the relevant LEA gets access to the intercepted communication.

(continue)

## Detailed specifications

### GENERAL

- Compliant with ETSI TS 101-232-1, ETSI TS 102-232-2, ETSI TS 102-232-3 and ETSI TS 102-232-5 standards
- Cover full scope of local legislation for ISPs
- Inline or non-intrusive solution (with passive taps or port mirroring)
- Forward intercepted communication to law enforcement agencies (LEAs)

### INTERCEPTION PROBES AND MEDIATION DEVICES

- Intercept IP, Radius, e-mail (SMTP, POP3, IMAP) and VoIP (SIP, H.323) traffic
- Identify interception targets using Radius user names, IP addresses, e-mail addresses, SIP URIs and various other criteria
- Support multiple simultaneous interception flows and/or targets
- Buffer Radius traffic to enable interception of users that are already logged in
- Match Radius and e-mail interception targets using wildcards
- Match interception against predefined virtual ISPs
- Filter IP traffic using port ranges and/or protocols
- Activate interception using time schedules
- Support encrypted e-mail logins (base64 encryption)

### REMOTE CONSOLE

- For the management of interception targets
- For monitoring of interception activities and devices
- Supports multiple roles of user access
- Provides detailed event logs and online performance counters

### INTERCEPTION VIEWER (for testing purposes)

- View intercepted traffic in native ASN.1 structures
- Exports intercepted traffic to Libpcap format
- Decodes e-mail (SMTP, POP3, IMAP) traffic

(continued)

- All lawful interception equipment deployed on the network infrastructure can be managed remotely within a single console.
- Detailed event logs and online performance counters are available with notification services to ensure the equipment runs fault free. The equipment can also be put into debug mode to reveal even more information when troubleshooting problems.
- Crovanto Lawful Interception is built on the Crovanto networking framework for deep packet inspection and manipulation solutions. As the framework is software-based, additional functionality and customization could be added to the lawful interception equipment with ease.

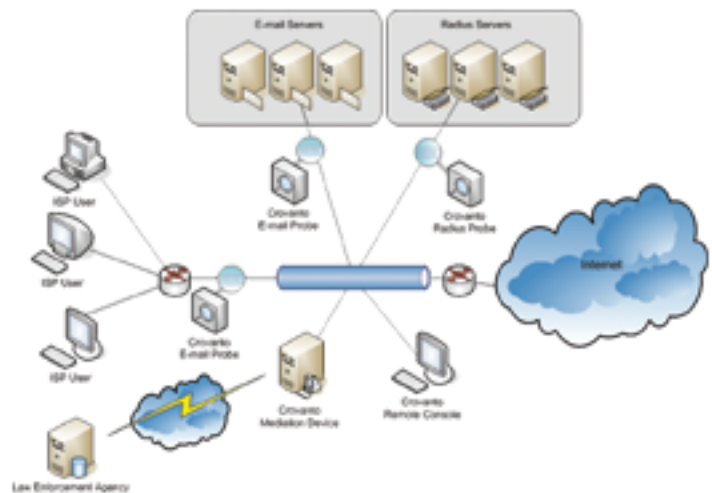


Figure 1: Possible set-up scenario at ISP

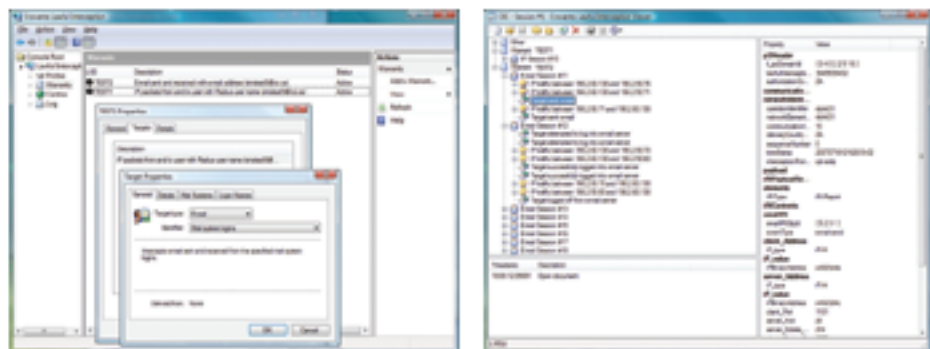


Figure 2: Screenshots of Remote Console and Interception Viewer