ALTRON
DEVELOPMENT AND PRODUCTION

EAGLE EYE - IP TAP

Passive Network Application
Platform for Lawful Interception
and Network Monitoring

EAGLE EYE
IP TAP

1. Introduction

The Eagle Eye - IP tap is a passive IP network application platform for lawful interception and network monitoring. Designed to be used in distributed surveillance environments, the Eagle Eye - IP tap is ideal for monitoring various networks – from small business network to large complex networks.

The Eagle Eye - IP tap enables to perform inspection and classification of network packets with subsequent decoding of application-level protocols without necessity of preliminary filtration at switches, routers or other probes. This capability eliminates any performance impact to the existing infrastructure and provides enhanced interception capabilities.

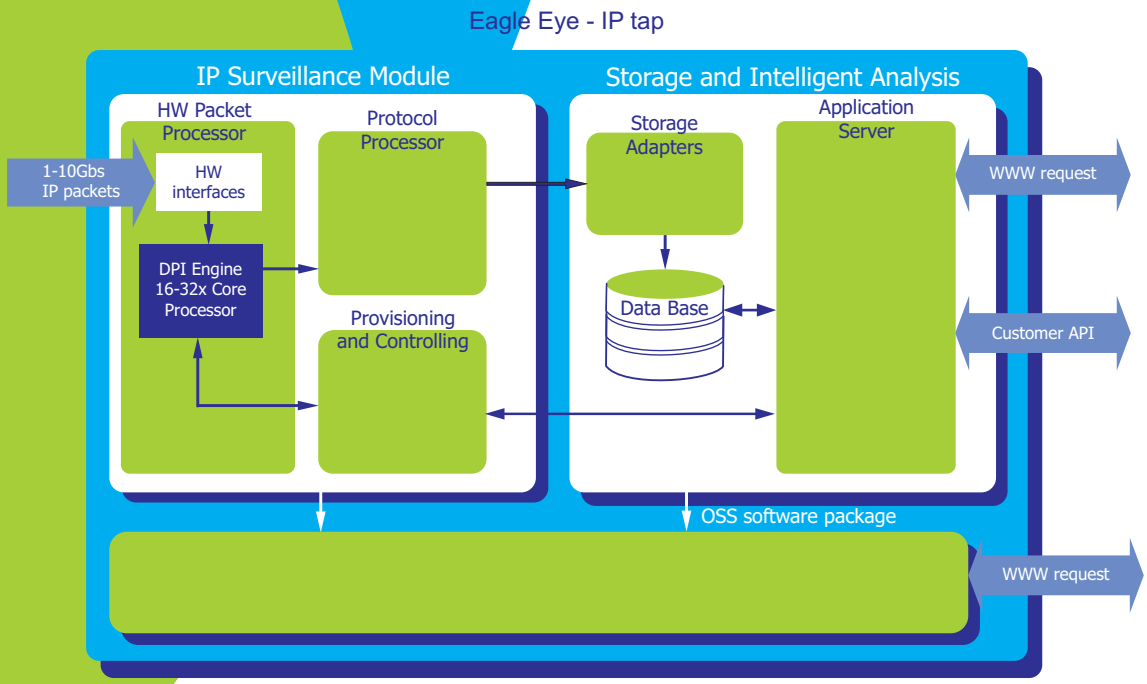
The Eagle Eye - IP tap offers flexible interception options, including the ability to deliver entire data stream, level 7 application's data stream, IRI/Pen-Register information, IPDR/CDR records, and/or key session events, that enable the Eagle Eye - IP tap to provide a full range of interception solutions and data retention.

The Eagle Eye - IP tap also incorporates sophisticated reconstruction logic to deliver only pertinent information when intercepting complex applications such as webmail and IM/chat, reducing processing required by the monitoring and analytic systems.

2. Architecture

The Eagle Eye - IP tap consists of three basic software-hardware modules:

- IP Surveillance Module is intended for direct filtering and analysis of network packets. Internal host processors and multi-core packet inspection accelerators of this module make it possible to monitor multiple 1Gbps and 10Gbps Ethernet links at true real wire-speed with full deep application protocol inspection (DAPI) and deep packet inspection (DPI) capabilities.
- Storage and Intelligent Analysis Module is intended for a long-term storage of intercepted information, for accessing recorded information, analysis of data related to operators authentication and authorization.
- Operations Support System (OSS) is intended for administration, management, and collection of information on health status.



The Eagle Eye - IP tap can be supplied to the Customer in three types of configuration:

- A standalone solution for monitoring small networks with 10/100/1000 Mbs bandwidth (from 1 to 4 ports). In this configuration the Eagle Eye - IP tap includes a software for recording and intelligent analysis of the captured traffic that is to be installed on the same server-based platform, where data interception is performed.
- A distributed solution for monitoring enterprise networks with 1-10Gbs bandwidth (4 ports or more). IP Surveillance Module and Storage and Intelligent Analysis Module are installed on dedicated platforms. Additionally, several IP Surveillance Modules can interact with one Storage and Intelligent Analysis Module that enables flexibly increase capacity of the system in general.
- IP probe devices as an integral part of the MC that ensures processing of network traffic. In this configuration the role of the Storage and Intelligent Analysis Module is performed by the Eagle Eye MC software.

3. Features

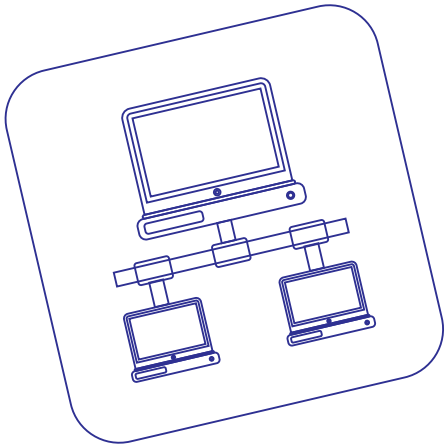
- Passive mode Interception.
- Operation in 100Mb/1Gb/10Gb networks.
- Interception of network traffic from 1 to 4 channels in a standalone solution.
- Processing of unlimited quantity of channels in a distributed version.
- Processing of IPv4 and IPv6 protocols.
- Identifying and filtering of layer-7 traffic with using integrated real-time DPI engine.
- Intercepting based on application content specified by a set of simple strings, complex strings, regular expression, or pattern/signature database.
- Intercepting of specified subscribers enabled by the system's capability to process the RADIUS and DHCP protocols.
- Extraction of application layer metadata and full reconstruction of content.
- Full generation of IPDR and CDR for all network flows and events.
- Intercepting and decoding of GRE and GTP tunneling protocols.
- Storing of captured content and metadata in a local DB and its transfer to a remote monitoring center.
- Web-based graphical user interface.

Intercepted Protocols	Metadata and Criteria for Subject Filtering	Intercepted Content
Discovery and Interception of SMTP, POP3, and IMAP-based Email	Targets can be specified as localname@domainname, localname (at any domain), @domainname (any localname on this domain), @ (all email). Additionally, targets can be specified as: to (including cc and bcc), from, or both, email subject, attachment type, keyword in email body	Full email with attachments, just the email text, summary information, or the email session events
VoIP	VoIP calls are discovered and captured based on the analysis of SIP and H.323 signaling protocols. Targets can be specified as: user@host, user@IPv4/IPv6 address, phone_number@host, host, phone number@IPv4/IPv6, telephone_number, hostname, or IPv4/IPv6 address	Voice content and information about occurrence of signaling events
HTTP	The HTTP traffic is intercepted based on URL, HTTP header, or IPv4/IPv6 address. Additionally, webmails (non encrypted Gmail, Hotmail, Yahoo and etc.) can be intercepted based on the email address or the webmail domain	Web-pages, images, email, and etc.

Intercepted Protocols	Metadata and Criteria for Subject Filtering	Intercepted Content
IM/chat services	IM/chat sessions are discovered and intercepted based on the subject's username. The IM/chat session, including advanced features such as audio, video, and file sharing are captured and decoded with the pertinent information extracted and delivered	Presence information, text messages, video, files, summary information, and events
FTP	IPv4/IPv6 address, username	Files, summary information, and events
Layer 4 IP Traffic Discovery and Interception	IP traffic is discovered and captured based on IPv4 or IPv6 address, layer-4ports, and application classifications. IP addresses can be static IPv4/IPv6 addresses or subnets, DHCP-assigned via MAC address, option 82 (remote ID, circuit id or both) or RADIUS login (username or NAS port ID). Layer-4 ports can be specified be as singular, a range, a set, or a 'not' condition	Delivered traffic can be all packets, packet summary, or IPDR
Layer 2 Traffic Discovery and Interception	Discovery and Intercept of the following Data Link Layer protocols: Ethernet, ARP and etc.	All packets, packet summary and events

4. Benefits

- Possibility to create small standalone systems for interception in IP networks and distributed system for interception and analysis of information in 2G(GPRS)/3G/ISP networks.
- Possibility to create both target centric interception systems and systems for massive interception of information in IP networks.
- Processing of metadata and information on network events enabled by Complex Event Processing technology.
- Definition of triggers for combinations of network events with an opportunity to start business processes.
- Integration into the Customer's business structure enabled by ESB and BPEL technology.
- Integration into the Customer's existing interception systems by using API.



ALTRON
DEVELOPMENT AND PRODUCTION

EAGLE EYE - IP TAP

6, Kostomarovskaya str.
61002 Kharkov, Ukraine
Tel./Fax: +38 (057) 766-13-63
e-mail: post@altron.ua
http://www.altron.ua