The power of technology. The worth of safety.

rcs

AGT ADVANCED GERMAN TECHNOLOGY

Technical Proposal to SCT

Index

Figures

1 RCS / AGT Proposal to SCT

This document has been prepared to be a proposal according to SCT requirements. RCS /AGT reserves the right to review this proposal should this assumption be incorrect. The system proposed in this document is a comprehensive telecom monitoring solution to be implemented in order to provide a monitoring coverage of SCT Internet Service Provider, with particular regards to the Satellite one way connectivity.

The proposed system is ready for future expansion, upgrade and adding of optional capabilities and functions.

The proposed system is based on the state of the art solution

Ø AM (Administration Module – Element Manager)

Ø IVS (Internet Visualization System)

Ø TIP (Tactical IP Probe).

Key points of these products are:

ü Flexibility

They can be used over any kind of IP networks -including tunnelized networks- conveyed by several different media (including Satellite)

ü Scalability

The solution (HW and/or SW) can easily be upgraded to manage an increasing requirements in terms of number of Interceptions, bandwidth, depth of analysis.

ü Ease of use

The solution has been designed with an advanced GUI in order to be extremely user-friendly.

1.1 Overview

The following Figure 1 "RCS Layered solution" shows how RCS covers layered structure (as per RCS Model of Unified LI System) to provide solution to SCT.

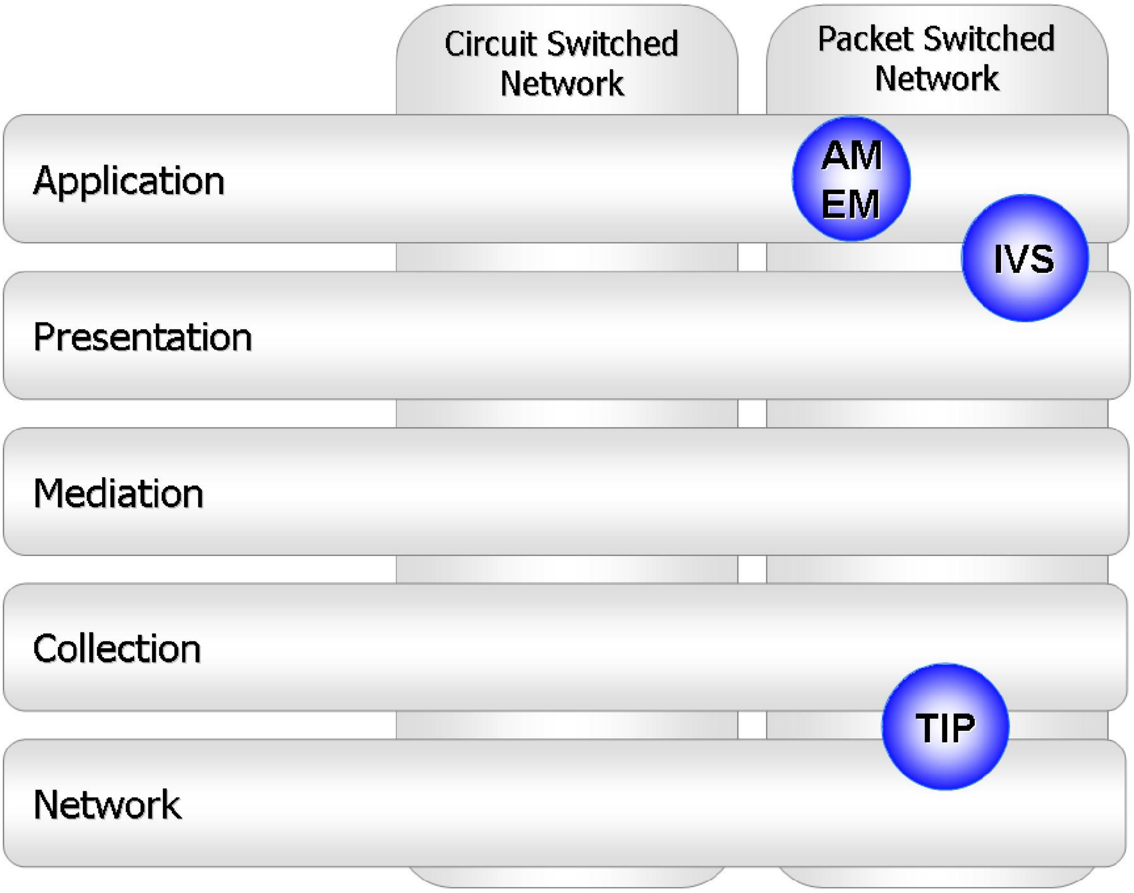

Figure 1 “RCS Layered solution”

- **Application** – Warrant processing, target setup, network management., information collection & analysis.
- **Presentation** – Modifying all data and communications protocols and formats into a form understood by the application layer and vice-versa
- **Mediation** – Communication and interfacing with the collection and presentation layers to control and manage the diverse network elements that would form the core of the unified solution
- **Collection** – Collecting the required data and information from the targets identified within the diverse operator and service provider networks
- **Network** – Equipment that interfaces and connects into the service provider or operator network.

1.2 RCS Capability

RCS products, described below, are deployed in many countries. RCS has many years of experience in not only supplying equipment, but also wide range of services:

- Consultancy on LI solutions
- Site survey & site preparation (provided by RCS engineers or certified local companies)
- Installation, configuration test and commissioning (provided by RCS engineers or certified local companies)
- Training on customer site (provided by RCS trainers)
- Support
- Maintenance
- Security audit
- Project management

1.3 Solution Deployment

RCS designed the solution here detailed granting the best trade-off in terms of

- Security
- Scalability
- Cost effectiveness

1.4 Network Scenario

The project has been designed taking into account information provided by SCT reported in the Figure 2 “Network Scenario”.
RCS reserves the right to review the proposal should this assumption be incorrect.

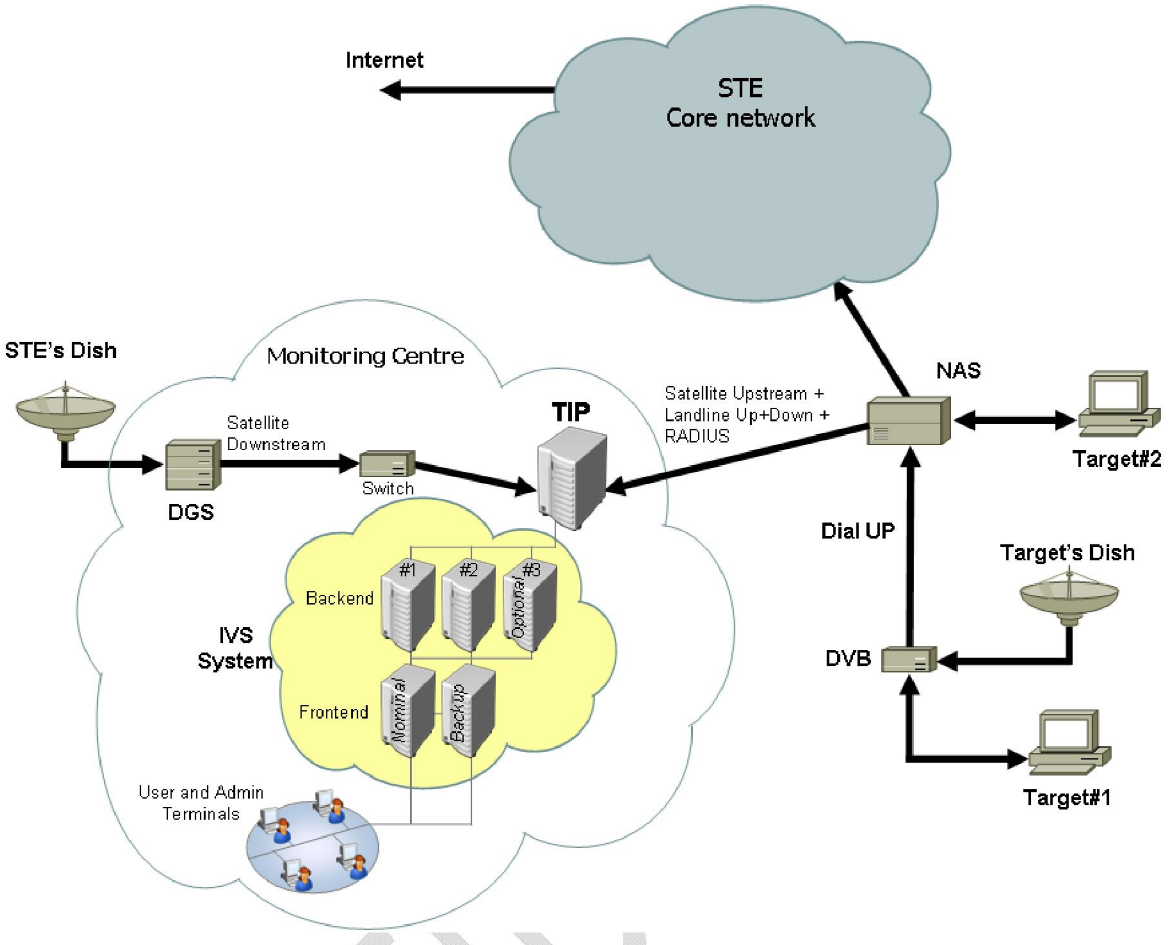

Figure 2 "Network Scenario"

1.5 Logical Architecture

The proposed solution is designed to analyze and eventually intercept the traffic exchanged by SCT's subscribers: all the traffic is analyzed at wire-speed by the ***Probing Subsystem*** and the relevant one is saved in standard PCAP files when the content match with one or more configured interception rules.

Seized traffic is delivered in realtime to the ***Monitoring Subsystem***, where PCAP files are recorded, stored and decoded.

2 Probing Subsystem

The proposed probing subsystem lean on the well established RCS's Tactical IP Probe (TIP), a 1+1Gbps single server software based interception Probe already used in many contests. RCS's TIP runs over COTS [Commercial-Off-The-Shelf] hardware (see the following paragraph §4.2 for details) with Linux operative system, allowing an easy system management with scripts or standard software.

RCS's TIP includes the following capabilities:

ü Network sniffing

ü Wire-speed packet filtering and collection

ü Mediation to the Monitoring Subsystem

The probe is connected in a passive way, receiving a copy of the "to be monitored" packet streams. The traffic replication can be done by mean of a mirror (span) port or through physical "tapping" (optical or electrical) of the identified connection.

The proposed TIP probe are ready to receive Ethernet packets, meaning that wiretapping over different transport network –such as ATM or SONET- require a review of the current offer. Moreover, they are able to handle both L2TP-tunnelized and not-tunnelized (plain) IP packets, allowing to intercept targets belonging to "hosted ISPs".

Packets are saved in PCAP standard format with precise timestamp: for this reason, TIP servers periodically synchronize the internal clock to a master NTP server.

2.1 AM Element Manager

The proposed administration solution, is based on RCS's AM Element Manager modules.

This software module is hosted by the TIP server, and is accessed as a secured website through a normal web browser.

Included functionalities are:

- Provisioning of the interception targets
- Diagnostic and alarms
- Management and maintenance

An authentication system guarantee both the security and the desired visibility of data: different users can be configured to have access only to the desired function (provisioning, monitoring, administration…), maybe from different clients located in different premises: for example an investigator can access the system from the LEA client for provisioning purposes -without having access to the network configuration page-, while a technician is accessing the system from a local client for monitoring the CPU usage -without seeing any target-related data-.

2.2 Provisioning

The administration system includes the capability to configure the interception elements (Probes and IVS) in order to provide the interception of targets.

The system has two classes of interception targets: **user** and **content**

The following paragraph describes the Target allocation for all the target types supported by the system.

2.2.1 Static-IP

Triggers interception upon any IP-level parameter match. Typical applications :

- Interception of static IP-address users, a range of IP-addresses, some specific IP-ports over a certain IP-address range.

AND+OR chains of rules can be easily implemented.

2.2.2 Keyword

Triggers interception upon keyword match on reconstructed IP flows Typical applications:

- interception of keyword spotted emails, web pages, webmails, chats.

Keywords can be strings or regular expressions ("bomb", info@easygain.com, [Ff]errari, any word...) Flow reconstruction and keyword search are done upon a pre-filtered subset of the whole traffic: pre-filtering rules are specified using "Static-IP" parameters. unmatching flows are discarded after they reach a settable threshold (typical: 512KByte)

2.2.3 VoIP

Triggers IP/RTP interception upon SIP/H.323 user match: URI, alias. Typical applications:

- interception of the VoIP calls from/to a VoIP number, a country/area...

2.2.4 User:

Triggers IP interception upon Radius authentication parameter match: username, NAS-port-ID (line identifier). Typical applications:

- interception of an ADSL user, a Dialup user

2.2.5 DHCP

Triggers IP interception upon MAC-address or Modem-ID match. Typical applications:

- Interception of a cable-modem user

2.2.6 DNS

Triggers IP interception upon Server-Name match. Typical applications:

- interception of an Internet Server regardless if its address is static or not

RCS is available to provide separate quotation for any further requirements issued by SCT.

2.3 Diagnostic and alarms

The administration solution includes a diagnostic system that collect all the alarms gathered from the TIP. The alarms can be:

- System alarms (i.e. HW failure)
- Performance alarms (i.e. input bandwidth exceed the nominal one)
- Activity alarms (i.e. one specific interception target log in)

The notification can be by SMS, email or the AM alarm console.

2.4 Management and maintenance

The administration solution includes a management system that enables to check the performance of the interception system and allows maintenance activity.

3 Monitoring Subsystem

The Monitoring Subsystem is the central Law Enforcement Monitoring Facilities from which the LEA intends to decode and inspect the intercepted data. The proposed solution is based on IVS (Internet Visualization System) that is a client server architecture, and both clients and servers have conveniently been located into the Monitoring Center, but other combination are suitable, provided that the necessary network connectivity (may be a VPN) between sites is guaranteed.

The main functionalities implemented in the Monitoring Subsystem are:

- IP traffic reception;
- IP traffic decoding;
- IP traffic presentation;
- Production of forensic archival copies of the traffic;
- IP traffic storage;

3.1 Architecture

The proposed Monitoring Subsystem is a Client-Server system that stores all the target-based intercepted data on the server storage for security and privacy reasons.

The clients are MS-Windows based Personal Computer and they retain only the web-based application needed to browse decoded contents. Data are dynamically downloaded from the IVS and they remain present in the client workstation only for the time needed to view it.

Firmly based upon RCS experience in investigative activity, IVS is a scalable modular platform which follows the development of Internet applications.

The current proposal include five IVS server, the characteristics of which are described in the following paragraph §4.3.

3.2 IP Traffic reception

Data sent by TIP probe, is received by IVS in standard PCAP format. The transfer can be in realtime (streaming ETSI) or as batch file transfer.

The recording speed is the one allowed by the network connection.

3.3 IP Traffic decoding

The system is able to identify thousands of different IP protocols and decode the most popular and relevant of them.

More than 4000 internet protocols are recognized and classified (tagged), while the following are decoded:

3.3.1 Web

- HTTP
- MMS (.mms file + multimedia contents)

3.3.2 Email

- SMTP
- POP3
- IMAP4
- NNTP
- EML (.EML files - RFC_822)
- WEBMAIL:
    - Hotmail
    - Yahoo!
    - Gmail
    - All standard webmail are presented as Web pages

3.3.3 Chat

- MSN
- IRC
- YAHOO
- ICQ
- C6
- Paltalk
- Volano (web chat)
- Terra (web chat)
- Lycos (web chat)
- Gtalk (web chat)

3.3.4 File transfer

- FTP
- EMULE
- MSN
- IRC
- YAHOO
- ICQ

- C6
- Paltalk

3.3.5 Audiovideo

- H323
- SIP
- MSN Video Call
- YAHOO Video Call
- Paltalk Audio
- Paltalk Video
- Icq Audio

3.4 IP Traffic presentation

Designed to fit the requirements of users with different technological skills, IVS is a flexible tool whose employment is within occasional users reach but, at the same time, ensures full support to skilled users.

After decoding, the operator’s access to the intercepted communications may be carried out in any of two supported methods:

- Offline Browsing, that allows to review all the data accumulated for a given target (or set of targets);

- Online browsing, that allows to observe the activities of a single target in real-time (the display window follows the actual activities of the target whenever he is connected to the Internet)

The decoded data are immediately graphically displayed as though the operator was in front of the target’s monitor.

When the investigation is run by qualified personnel, this effortless usability accelerates the analysis, enabling the operator to find quickly on screen the most important pieces of the IP communication.

At the same time IVS can also present detailed views of the same traffic enabling the analysts to examine the deep structure of gathered information.

IVS client application allow the user to manage Investigation activity providing a suite of useful tools like as:

- ü Search function
- ü Possibility to set a relevance for any Item and Session
- ü Possibility to edit a Digest for any Item
- ü Fast filtering and sorting on different Item Types
- ü Report generation for export or printout

Beside IVS's client application functionalities, Windows's standard tools are available for saving, printing, playing any kind of resources.

3.5 Production of forensic archival copies of the traffic

The system provides the functionality of archiving the traffic data from any IVS workstation by every user that has the needed right (interception administrator), based on authentication.

The archiving is made by optical disks that contain the raw and decoded data, in a format that can be easily browsed by any browser (i.e. without the need of a any special application, and over any platform like MS-Windows, Linux, MAC-OS…), providing a kind of GUI similar to the online IVS.

3.6 Authentication

The access authentication for the workstations, both users and administrative, is by username/password, or optionally by smartcard.

3.7 IP traffic storage

All the received data are stored as raw PCAP files in the server storage, as well as the decoded resources (web pages, audio files, images…). IVS keeps both the raw and decoded data for matching two binding requirements:

- realtime responses to user queries on decoded data
- possibility to reprocess (re-decode) raw traffic after a decoder update.

4 Physical Arrangement

4.1 Target number

Based on RCS' 20 years of experiences in the LI solutions provider, and having many of the top worldwide countries as clients, we can confirm that the size of a monitoring system has to be calculated following two main concepts:

- ü Target/Subscriber ratio (also known as "interception rate")
- ü Target/Operators ratio

For the interception rate, the maximum value ever seen in all European and Extra-European countries is 1:2000 (i.e.: 1 target each 2000 subscribers). Considering the special context of this project, with the need of content-oriented monitoring, we considered for this project a very safe ratio of 1:1000.

The sizing of this project has been calculated considering a forecast of 5000 subscribers and 400 Mbps of sniffed traffic, which lead to a need of 50 target.

As it's easily understandable, beside the amount of subscribers, the number of target should be proportional to the monitoring stations and the operators that are going to work on such stations: according to RCS' experience in broadband users monitoring, we can say that a correct Target/Operator ratio is 5, meaning that each Operator can profitably work on not more than 5 targets.

This lead to the conclusion that at least 10 operators will be required for handling the amount of information collected by 50 targets: in order to realize the correctness of this figure, please note that, according to the estimated protocol distribution and to RCS' experience, 50 broadband targets will generate up to:

- ü Number of HTML pages accumulated per day: 1500
- ü Number of chat lines accumulated per day: 37000
- ü Number of email accumulated per day: 1800
- ü Number of other items accumulated per day: 20000
- ü Total number of Items to be checked per day: **30000**

For the reasons explained above, the system has been dimensioned to guarantee the capability of handling more than the proposed bandwidth (up to 2Gbps) and monitoring 50 targets with 100 rules, using 10 client stations.

Anyway is also important to understand that the mentioned values are not rigid limitations on the system: due to the modular architecture, RCS' system can be easily scaled up whenever there is the need.

4.2 TIP

The proposed TIP probe have the following features:

TIP Features

- ***Probe Platform:*** *one Dual Xeon Intel server (DELL PE2950)*
- ***Input Interfaces:*** 2*1GbE (electrical)
- ***Filtering Throughput:*** wire-speed
- ***Pre-processor Forwarding:*** 50Mbps max.
- ***Keyword/email/chat search capability:*** 20Mbps max.
- ***Targets:*** 75 max.
- ***Keyword search Targets:*** 20 max.
- ***Rules:*** 100 max
- ***Alerting:*** email and SMS support for both alarms and interception events

4.3 IVS distributed system

As depicted in Figure 2 "Network Scenario", the IVS architecture is split in two layers:

ü Backend IVS:

ü Frontend IVS

Let's go through the distinction between the two layers.

4.3.1 Backend IVS

It's a processing server hosting the recording and decoding functionalities. Each server can handle up to 25 targets. The recorded file and the decoded resources are stored in the Frontend IVS storage, like so the database information that are remotely stored inside the Frontend IVS database.

The Backend IVS does not keep any stored information, so it doesn't need to be backupped.

Backend IVS Features:

- ***Platform:*** Dual Xeon Intel server (DELL PE2950)
- ***Number of Targets:*** 25 max

4.3.2 Frontend IVS

It's the server hosting the database and the presentation functionalities (WAS). A single server can handle up to 75 targets and 15 operator clients.

The Frontend IVS do store sensitive data, so in order to increase the availability of the service, it should be backupped by an hot-standby IVS Frontend Backup server.

The Backup server is autonomously responsible to keep its storage aligned to the Master server's one.

Frontend IVS Features

- ***Platform:*** Dual Xeon Intel server (DELL PE2950)
- ***Number of Targets:*** 75 max

- ***Number of Clients:*** 15 max

- ***Direct attached storage:*** 3TByte

4.4 Clients

- ***IVS client:*** "state of the art" PC with DVD reader/writer

4.5 Physical arrangement

The proposed system consists in:

- 1 (one) TIP probe with AM - Element Manager

- 1 IVS System composed by

    - 2 (two) IVS Backend servers: working in load sharing on up to 50 targets (expandable to three servers, for managing up to 75 targets)

    - 2 (two) IVS Frontend servers: one as Master, one as hot-standby with storage backup

- 10 IVS Clients access capability