

AXS-2500 PASSIVE PROBE FOR IP INTERCEPT

Utilizing the industry leading AXS-2500 passive probe, Xcipio solves Lawful Intercept compliance issues for carriers whether they serve hundreds or millions of subscribers.

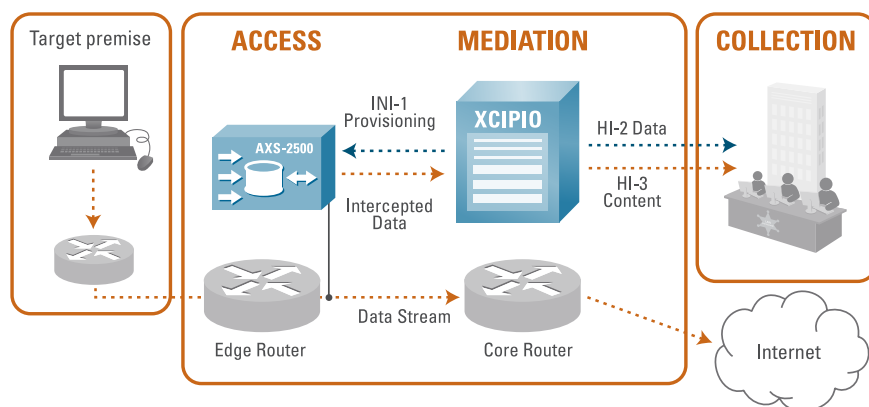
Europe was the early leader in packet intercept defining dedicated devices to handle the sensitive nature of lawful intercept and creating the first standard for packet intercept called TIIT (Transport of Intercepted IP Traffic). During this time SS8 was an active participant developing and testing solutions to comply with TIIT. In those early days of packet intercept things like SPAN ports and Remote Monitoring capabilities on routers were used to access and replicate a target's traffic but it quickly became apparent, with the explosion of IP services and protocols, that much more sophisticated capabilities were needed to identify, reconcile and deliver IP traffic to law enforcement. As the industry-leading, high-performance, filtering and capture device for passive communication intercept, the AXS-2500 provides those capabilities and much more. Purpose-built for this task it is based on stringent lawful intercept requirements pioneered in Europe; and is a field-proven solution with security mechanisms that ensure the integrity of the target data and provide protection against breaches in warrant security.

Lawful Intercept (LI) is performed in one of two ways, active or passive. Active intercept leverages the capabilities of the existing network elements (switches, routers, gateways etc.) to copy and forward the desired information to Xcipio. But when, for example, a network element doesn't have LI capability or maybe a portable solution is desired or if a single aggregation point exists, then a passive solution using the AXS-2500 probe can be an excellent choice.

Contrary to its description the AXS-2500 is anything but passive in operation. While it may only be passively attached to the network, as opposed to network elements that are actively switching calls and data, the AXS-2500 performs a very active role, examining and identifying packets at rates of up to 10 gigabits per second.

- Purpose-built appliance
- Based on COTS technology, providing continuity of supply and optimum pricing
- Filtering of ATM, MPLS, Ethernet and IP
- Filtering of user applications such as email, VoIP, chat, etc.
- Wide range of IP and telecom interfaces
- Passive VoIP intercept
- Powerful string search capability
- Full IP stream interception of all user data
- Encrypted software and file system
- Automatic target deletion on power down
- Secure, wire-speed filtering with no network degradation

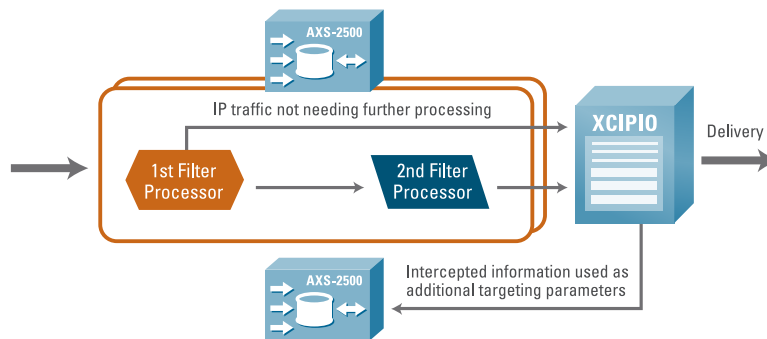
AXS-2500 in the Network



Architecture

The AXS-2500 is built on patented technologies that allow it to be deployed in the most secure and demanding environments. To ensure high performance several design techniques have been incorporated, including specially modified and tuned network card drivers for optimal performance and high capacity multistage buffering. This buffering technique allows the AXS-2500 to handle burst traffic from interception through delivery, ensuring accurate and complete collection of traffic with zero loss at wire speed.

For packet inspection a unique hierarchical and scalable filtering technique is used. A First Line Intercept Process filters traffic against IP address, protocol ID and TCP/UDP port number. Traffic targeted by IP address alone can be forwarded directly to the Xcipro Mediation Function. Traffic requiring further processing (SIP signaling, string searches, etc.) is passed to a Second Line Intercept Process for deep packet analysis. The first and second line processes are modular, allowing them to be hosted on a single platform or across multiple servers. This tiered approach, in conjunction with the buffering technique, keeps packets flowing while allowing deeper inspection to take place when necessary.



History Buffer

Experience has taught us that it is not always possible to immediately identify packets of interest, with this in mind the AXS-2500 contains a history buffer that allows searches to “go back in time” to retrieve packets that are deemed important after-the-fact. One example is in a VoIP environment where two independent packet streams (SIP and RTP) are created. While the AXS-2500 is examining the signaling information (SIP) to see if it belongs to a target, the corresponding RTP (voice) packets may have already started transmitting. But because of this unique buffer, as soon as the RTP traffic is deemed important, the AXS-2500 can back into the buffer and recover any initial RTP packets that might have been transmitted without being intercepted. A similar example is the case of a user logging onto a network (wireless, internet, etc.) and then transmitting data. In this case the AXS-2500 is examining the login protocol (I.e. RADIUS) for matches while simultaneously buffering the data packets in case they are needed. In a different example, when connectivity between elements is blocked, the history buffer, utilizing a combination of both RAM-based storage and the server’s hard drive, can be used to store information until connectivity is re-established

Core Functions Filters

While processing packets at high rates across various networks (wireless data, broadband, WiFi, etc.), the AXS-2500 needs guidance to determine what is important or relevant. This is where filters come into play; they are used to identify a target’s traffic and isolate it. Filters (IP address, IP address with port number, email address, SIP E.164, RADIUS login, text string, etc.) will vary based on the network technology, and the protocols in use. The AXS-2500 includes capacity for up to 5000 live targets (filters) and examines many different protocols (email, web surfing, chat, VoIP, instant messaging etc.) across many different transport types.

Targeting and Searching

The 5000 targets supported by the AXS-2500 can be configured using any combination of the following protocols/target identifiers:

- IP address
- TCP/UDP Port and IP address combination
- Email addresses from SMTP, POP3 or IMAP traffic
- POP3 and IMAP login usernames
- PPP username
- SIP E.164, URLs, Text ID, or all calls
- IRC nicknames, usernames or realnames
- ATM VPI and VCI
- String or keyword searches of all traffic at layer 7
 - 7 or 8 bit ASCII or binary strings
- Email address within email body

Media Agnostic

One of the core functions of the AXS-2500, and the thing that makes it so valuable to carriers, is the ability to support a variety of physical interfaces and connections; in essence, to be 'media agnostic'. As a media-agnostic device, the AXS-2500 supports multiple connectivity types, leaps over encapsulation layers to inspect the original payloads, compares data against thousands of filters and searches for strings across all kinds of protocols. These activities are supported across a wide range of networks and physical interfaces that include 10/100BASE-T, DS3 ATM, OC-3c ATM and GigE.

For Ethernet deployments, both copper and fiber are supported. For VLANs, automatic VLAN skipping is used to skip VLAN tags and inspect encapsulated IP packet payloads. In ATM environments, layer 2 inspection, VC filtering and IP over AAL5 is supported, along with application layer filtering of IP, SMTP, and TCP port traffic. MPLS filtering operates on both layer 2 and layer 3 and can automatically skip up to 3 levels of MPLS labels to inspect IP traffic.

Key Differentiators Application Aware

By being "application aware" and examining information at layer 7 of the OSI model, the AXS-2500 rapidly inspects traffic, matches it to filters and identifies the targets' traffic. This capability is significantly more precise than just grabbing packets going to and from an IP address and helps law enforcement pinpoint items of interest.

Some of the applications that the AXS-2500 is aware of include:

- SIP (Session Initiation Protocol) for passive intercept of Voice over IP (VoIP) phone calls
- email where the address portions of the email (To, CC) are searched for matching email addresses
- RADIUS for the identification of login names

Email searches that are application aware can avoid pulling all the traffic from the well-known "email" ports, for various protocols (SMTP, POP3, IMAP, etc.), and instead focus the search on the Source/Destination headers of the email, without having to do a string search which could produce false positives. And for application aware RADIUS searches, instead of reporting all RADIUS traffic the AXS-2500 examines the RADIUS traffic to find specific login names, identifies the IP address assigned to each login name and reports them so that they can be used for further intercept activities.

Keyword Search

Keyword searching in both ASCII and binary is a flexible capability limited to very few probes on the market today. This powerful feature in the AXS-2500 allows for free-form searches critical to intelligence and surveillance activities that not only spot keywords but also help identify patterns of usage.

Rapid Adoption of New Protocols

In addition keyword searches make the AXS-2500 "application independent", allowing it to immediately support the multitude of protocols constantly being introduced. By using keyword searches filters are set up immediately on new protocols without having to wait through a development cycle for full protocol support.

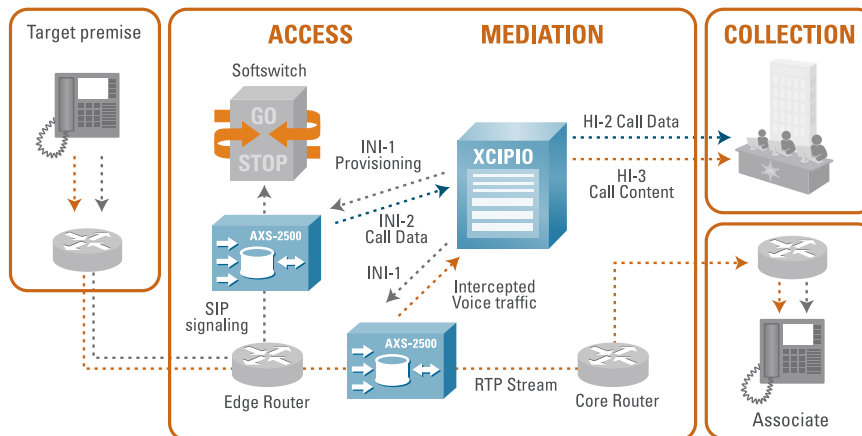
Flexible Deployment

One or more AXS-2500s can be deployed strategically throughout the network to capture traffic or relay signalling events. The captured data, voice and signaling are passed to the Xcipio mediation device for either further processing or delivery to the relevant agency managing the warrant. Delivery standards for both broadband data (ETSI TS 102.232,233,234 and ATIS T1.IAS) and voice (ETSI ES 201-671 and ANSI T1.678) are supported by Xcipio.

Passive VoIP

Utilizing a passive VoIP intercept solution can be a quick and efficient way of meeting regulatory obligations for VoIP providers. The AXS-2500 is a network-equipment agnostic solution that intercepts and interprets SIP signaling traffic in the network. It uses the information contained within the SIP control messages to create both call data messages and identify the RTP flow(s). Once the RTP flow is identified, any initial packets that may have been missed can be retrieved from the history buffer and all RTP packets transmitted from that point forward are intercepted. Xcipio collects information from all intercept access points in the network and delivers the information to law enforcement.

AXS-2500 Passive VoIP Intercept



Other Features Security

Security is always a concern when sensitive information is involved and the AXS-2500 has several built in features that protect the platform and the information within it. The first of these ensures target data never leaves the premises, upon any power down all target information is automatically deleted. In addition, the file systems are all encrypted and the software image itself is node-locked on the server. No run-time log files are exposed to general users, only explicit, predefined alarms are generated and finally, the server itself can be physically locked.

Cost Effectiveness

Uniquely scalable the AXS-2500 probes minimize both up-front investment and on-going operational costs. Modular hardware and software provide scalability in a common chassis with the flexibility to filter at the ATM, Ethernet or IP layers, all the way through to user applications (email, VoIP, chat, etc.). Powerful string search capabilities can be enabled allowing for free-form parsing of traffic streams without the need to develop expensive protocol interfaces. Use of commercial off-the-shelf (COTS) equipment reduces costs typically associated with proprietary chassis, servers and line cards. Multi-link line cards and quick software upgrades minimize time associated with maintenance and upgrades, reducing the total cost of ownership over the life of the product.

AXS-2500 Server Specifications

AXS-2500 Probes are based on two off-the-shelf server platforms. Both are 19" rack-mount servers designed for telecom environments with the DC version meeting the more stringent NEBS and ETSI requirements for central office deployments. In both cases, network interfaces may be upgraded or changed by simply swapping out the interface line-cards.

Server Platform – AC version

The AXS-2500 server-based platform provides high performance, real-time filtering of Internet data. This space saving, 1U high, AC powered server is a cost-effective solution that supports hot-plug dual redundant power supplies, Dual Core Intel processors, up to 8GB of RAM and a hard disk that can be used, in addition to the on-board RAM, for data buffering.

Server Platform – DC version

The DC version of the AXS-2500 is the Intel® Carrier Grade Server TIGW1U. It is a 1U, rack-mount server providing NEBS-3 and ETSI compliance along with industry leading CPU performance in a compact package. Built for the demanding telco environment, both the hard disk drives and the power supplies are hot-swappable, with a second power supply available for redundancy. The configuration includes an integrated four-port 10/100/1000 Mbps Ethernet card, a slim line CD/DVD drive and a lockable chassis.



SS8 Networks
750 Tasman Drive, Milpitas CA 95035
Tel: (408) 428-3600
WWW.SS8.COM

Some of the features listed may be under development. Please contact SS8 for feature availability schedule. This document does not create any express warranty by SS8 Networks or about its products or services. SS8 Network's sole warranty is contained in the written product warranty for each product. The end-user documentation shipped with SS8's products constitutes the sole specifications referred to in the product warranty. The customer is solely responsible for verifying the suitability of SS8's products for use in its network. Specifications are subject to change without notice.

Copyright © 2007 SS8 Networks, Inc. SS8 Networks, the SS8 Networks logo, and Xcipio are trademarks of SS8 Networks Inc. All other trademarks mentioned in this document are the property of their respective owners.