SUBSENTIO
To Notice Secretly

1G and 10G SAFE HARBOR PROBE

For Broadband, LTE, UMTS and VoIP Networks

The Safe Harbor Probe is an easy-to-install, self-contained system that provides interception, administration, and VPN security — all in one device — and is independent of the specific equipment used in the network. As an "out-of-line device," the probe can be connected to many different points in the network including network taps or span/mirror ports, the latter being viable if the load on the router or switch is low. Upon receipt of a court order, intercepts are configured or provisioned in the probe through a secure web browser interface.
The probe then examines network traffic and provides deep packet inspection capabilities that take special actions for certain protocols, such as DHCP, RADIUS, GTP, SIP and RTP. The probe can also discover and track dynamic IP assignments.

Features and Benefits of the Probe

- Provides CALEA compliance for Internet access providers, VoIP providers, LTE operators
- Supports ATIS and 3GPP CALEA standards
- Full IPv6 support
- 1G version – two to eight 1G "listening" inputs
- 10G version – up to 12 1G or six 10G "listening" inputs
- Integrated VPN reduces installation complexity
- Email alerts and notifications
- Buffering options selectable for each intercept
- Can operate alone or control separate sProbes
- Virtualized version can operate in cloud infrastructure environments

How the Probe Works

Data Intercepts: The Safe Harbor Probe performs data intercepts on broadband, LTE, and UMTS networks. A wide range of identifiers can be provisioned for a target, including:

- IPv4 static address or subnet
- IPv6 static address, prefix, interface identifier, or MAC-to-EIU-64 identifier
- DHCP identifiers (e.g., MAC address, client identifier
- RADIUS identifiers (user name, calling station ID, NAS port)
- PPPoE IPCP MAC address
- MSISDN, IMSI, IMEI
- S-VLAN and C-VLAN tags
- ERSPAN session identity

Case-by-case, the intercept can be specified as a pen register intercept or full content intercept, with optional location reporting and optional service separation (removing VoLTE/VoIP from a data intercept). For LTE, the probe is connected to

About Subsentio®

Subsentio, LLC. is trusted by both the private and the public sectors to perform lawful intercept. Based in Centennial, Colorado the company has national, regional and rural service provider clients.

Subsentio provides Lawfully Authorized Electronic Surveillance (LAES) and compliance services to a diverse community of communications service providers. From national carriers to ultra-small rural providers, our clients serve millions of subscribers with a wide range of communications services. These services are often complex, multi-vendor environments encompassing differing phases of evolution and technological approaches.

SUBSENTIO,
The CALEA Compliance Company™

© 2016 Subsentio, LLC.

the S5 interface, or the S11 and SGi interfaces. Also, because courts often require "service separation," meaning that VoLTE/VoIP cannot be included in a data intercept, the Probe has optional filtering functions to remove VoIP signaling and content from a data intercept.

VoIP Intercepts: Without reliance on any other network equipment, the Safe Harbor Probe also provides complete SIP/RTP VoIP intercepts, including over-the-top VoIP and VoLTE. The identifiers that can be provisioned for a VoIP or VoLTE intercept include:

- Phone numbers, including partial or wild-carded phone numbers
- URIs
- MSISDN, IMSI, IMEI

As it listens to SIP traffic, the probe looks for the provisioned identifiers in a number of possible places, such as To/From/Contact/P-Asserted-Identity headers. Options, which are typically specified in the court order, include DTMF (dialed digits) reporting and location reporting. Options exist to ask the probe to detect and remove duplicate calls.

Standards: For data intercepts, including LTE, the probe can be provisioned to generate the ATIS IAS V2 CALEA standard. Alternatively, for LTE, the 3GPP 33.108 standard can be used. For VoIP, the probe uses the ATIS 678 V3 standard. The probe supports the optional features of the standards embraced by law enforcement, such as surveillance start, stop, and continuation messages. The probe also supports, in conjunction with all of the above, the ATIS-1000069 standard, which allows the probe to report conditions such as failed delivery interface, input interface down, lost output, dropped input., and others to the collection system.

Email Alerts and Notifications: The probe can be provisioned to send periodic reports to designated email addresses, including overall status reports to operational personnel and intercept-case-specific reports to law enforcement. Additionally, certain events can be selected to trigger email messages.

Delivery: The Safe Harbor Probe contains a variety of mechanisms to maximize the robustness of the intercept delivery. One of these, buffering, prevents the loss of intercept information if anything fails on the upstream path. The buffering implemented in the probe is called "transparent buffering" because the file system used is not visible outside the probe and thus can be used with any law-enforcement collection system.

The probe integrates a site-to-site VPN capability, eliminating the need for a separate VPN appliance. The probe can deliver 400 Mbps of intercept output, or be enhanced for higher throughput either through multiple concurrent TCP connections or by "high-speed delivery" on the 10G probe.

Security: The probe has two interfaces – the provisioning interface and the delivery interface -- both of which are highly protected. The probe contains a firewall function that permits access to only a few services, and permits access from only a certain set of IP addresses. A specific client certificate is required to access the SSL-based provisioning interface. The delivery interface is typically protected using the built-in VPN capability. Certain information within the probe is encrypted, such as buffer files and the Probe's database.

Filtering: The probe provides an array of filtering capabilities to reduce the output traffic to law enforcement, if permitted by court order. The probe can "filter on" specific VLAN tags and "filter out." It also has heuristics to filter out specific services, such as Netflix and YouTube, and deliver metadata instead of the content streams of these services.

sProbe control: The probe can also control sProbes, a simpler device that is deployed at any number of points in a network to provide remote interception under direction from the probe.

Miscellaneous Functions: The Probe can also assist with installation and troubleshooting via capabilities such as viewable statistics by source, case, and sProbe; viewable log; and input traffic categorization (e.g., whether the probe is seeing SIP traffic, DHCP, LTE GTP).

1G Safe Harbor Probe Physical and Electrical Characteristics

- 1U, 16.9" deep
- Approximately 16 lbs
- Operating temperature: 10-35ºC
- One 1G system port (provisioning and delivery)
- Two to eight input ports, RJ-45 copper or LC MMF 62.5/50 um fiber
- Max input rate: 4Gb/s data, 2 Gb/s VoIP
- AC power, typical power 60w
- Remote management via BMC/IPMI

10G Safe Harbor Probe Physical and Electrical Characteristics

- 2U, 14" deep
- Approximately 25 lbs
- Operating temperature: 10-35ºC
- One 1G system port (provisioning and delivery), optionally 10G port for delivery
- Two to 12 input ports, 10G ports are SFP+. 1G ports are RJ-45 copper or LC MMF 62.5/50 um fiber
- Max input rate: 40 Gb/s
- AC or DC (48V) power, typical power 140w
- Remote management via BMC/IPMI

© 2016 Subsentio, LLC.