SUBSENTIO
To Notice Secretly

Safe Harbor VNET

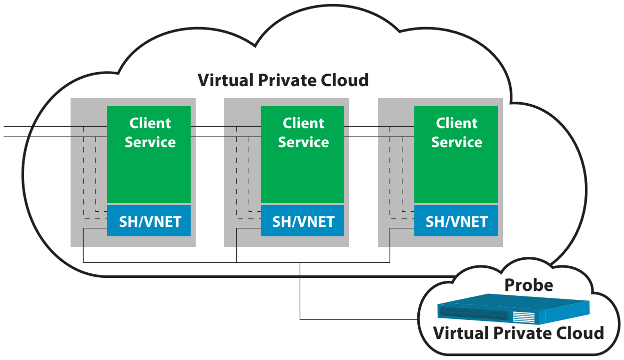
Networks today are experiencing exponential growth. Advances in cloud technology are moving traditional network infrastructure into cloud-based virtual solutions. For many situations, it is desirable for an interception probe to have remote intelligent surrogates that can extend the listening points of the probe beyond its traditional, hardware installation site. Subsentio's solution for these enhanced networks is our Safe Harbor VNET. The Safe Harbor VNET is a software module with an accompanying lawful-intercept architecture that provides a flexible solution tying a service- provider's network to a Subsentio Safe Harbor Probe. The VNET can be used in a variety of configurations, such as placed in virtual machines in a cloud-service environment (where physical taps are precluded); placed in network devices to be monitored, such as VoIP SBCs; or even placed alone in a physical device having network interfaces, allowing that device to be a remote surrogate of the probe, or a "subprobe."

KEY FEATURES & BENEFITS

- Supports broadband (e.g., IPv4, IPv6, DHCP-based, RADIUS-based) and VoIP (SIP and RTP) intercepts.
- Does intelligent target-identifier filtering under the direction of the probe to minimize network traffic from VNETs to probe
- Uses TLS for end-to-end encryption with the probe, thus eliminating any cleartext exposure of intercept data, and any need for VPNs
- Runs as a Linux process and uses no resources when no intercepts are active in the probe
- Provides the means to implement probe-based solutions in virtual environments such as Amazon Web Services (AWS) and Google Cloud.
- Up to 1500 VNETs can act as surrogates to one probe

Safe Harbor VNET Usage Models

In the Cloud. In the diagram to the right, in AWS terminology, virtual machines in the service provider's virtual private cloud (VPC) are being monitored by VNETs that are connected to a probe in a Subsentio VPC over an AWS peering connection.

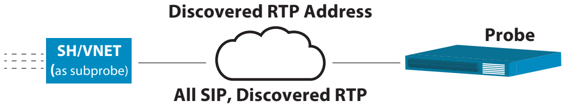


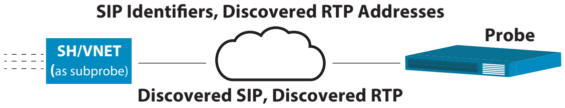
The probe interacts with the VNETs to provide a reliable and secure solution for VoIP and data intercepts.

As a VoIP Subprobe. The Safe Harbor VNET can be installed atop Linux in a server platform, and VNET's configuration file can tell it to tap certain of the interfaces and use another for the interface to the probe . Such a remote surrogate can be called a subprobe.

For VoIP intercept, Safe Harbor VNET has two alternate modes of operation. In one, if the probe has active VoIP intercept targets, it directs all the connected VNETs to send all SIP packets back to the probe for processing. When the probe determines that there is specific RTP media to be captured for an intercepted call, it sends the VNETs instructions to capture the specific RTP streams.

SUBSENTIO,
The CALEA Compliance Company™

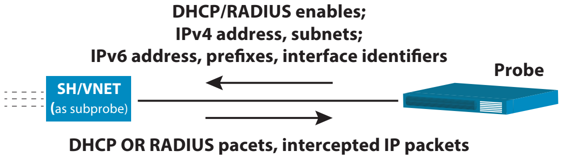



SIP Identifiers, Discovered RTP Addresses
SH/VNET
(as subprobe)
Probe
Discovered SIP, Discovered RTP

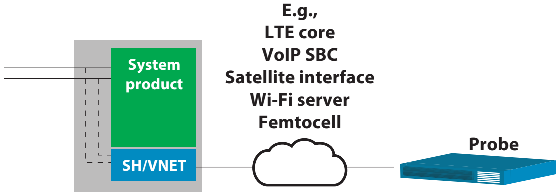
The second mode moves more of the processing to the VNET. Here the probe sends the identifiers (e.g., phone numbers) of the provisioned intercepts to the VNET, which then does the deep-packet inspection on SIP packets to determine a match and forwards them to the probe. The RTP processing occurs as before.

As a Data-Intercept Probe. For data intercepts, the behavior depends on the nature of active intercepts in the probe. If one or more intercepts are provisioned as dynamic IP addresses to be assigned by a DHCP server (e.g., intercept identifier is a MAC address that will appear in a DHCP request), the probe requests the VNETs to send all DHCP protocol packets to the probe so that the probe can do the discovery.

As the probe discovers dynamic IP address assignments to intercept targets, or if static IP addresses are being used for targeting, the probe provides the IP addresses (or subnets, etc) to the VNETs.


DHCP/RADIUS enables;
IPv4 address, subnets;
IPv6 address, prefixes, interface identifiers
SH/VNET
(as subprobe)
Probe
DHCP OR RADIUS pacets, intercepted IP packets

As an LI API. Another use is including the VNET in a manufacturer's network-equipment product to provide the LI capabilities required of manufacturers by the CALEA statute. This provides a solution without the oft-used proprietary interfaces to LI mediation systems..



Performance and Capability

Safe Harbor VNET performance is a function of the underlying system, the incoming traffic rates, the types of intercepts being performed, and the available bandwidth to the probe. Generally it can provide wire-speed performance. A VNET can deliver 1 Gb/s or more of intercepted traffic to the probe, providing, of course, that the network between VNET and probe supports this data rate.
When no intercepts are active, the VNET puts no load on its host system. When intercepts are active, it typically uses < 1% of the CPU resources of a typical multicore system.

VNET – Probe Communications

Running VNETs contact the probe periodically using routing information in their configuration files and thus are dynamically discovered by the probe. The probe can command each VNET to listen for (tap) certain traffic, enable or disable, and send statistics. Each VNET's configuration file tells it which network interfaces to listen on (tap).

Intercepted traffic is sent to the probe encapsulated in TCP for reliable delivery. Usually end-end encryption via TLS is enabled for this, although is can be turned off for troubleshooting.