

IP Network Surveillance using IP Fabrics' DeepProbe and DeepSweep



Kevin Graves
IP Fabrics

Table of Contents

Executive Overview	3
Network Surveillance Overview	4
Uses of Network Surveillance	4
IP Fabrics DeepProbe Network Surveillance System.....	7
DeepProbe System Features.....	7
IP Fabrics DeepSweep Network Surveillance System.....	11
DeepSweep System Features	11
DeepProbe and DeepSweep Technology	15
DeepProbe and DeepSweep Usage Examples.....	18
DeepProbe for Monitoring and Intercepting IP Traffic in a Comprehensive Surveillance Solution ..	18
DeepSweep used for Internet and VoIP Lawful Interception/US CALEA Compliance.....	20
DeepSweep used as a Tactical VoIP Intercept/Wiretap System	21
DeepSweep as Standalone Surveillance System.....	22
DeepProbe/DeepSweep as a Pre-filter for Existing Surveillance Devices.....	23
DeepProbe/DeepSweep as Insider Threat Detection/Mitigation	24
Summary – DeepProbe and DeepSweep Features and Benefits.....	26
Further Information.....	27

Executive Overview

DeepProbe™ and DeepSweep™ are a system-level products from IP Fabrics aimed at the emerging IP-based Network Surveillance market. Included in this market are application areas such as intelligence gathering for national security, lawful interception for criminal investigations, internal network abuse/misuse detection and capture, and general cyber crime surveillance.

DeepProbe is an intelligent probe, generally under the control of a separate surveillance element such as a mediation system. It is designed to be used in distributed surveillance environments, which are typically large, complex networks.

DeepSweep is stand-alone surveillance system which incorporates the intercept access point, mediation, and delivery functions. It is a particularly attractive solution for ISPs and VoIP providers now faced with complying with the FCC's recent broadband CALEA requirements.

Both systems excel in several areas. First, they both operate at 1Gbps and 10Gbps data rates, giving them the ability to be located in network aggregation points and thus providing the necessary visibility to a large amount of network traffic as the traffic traverses networks.

Second, they are easy to use and allow agents or analysts to configure surveillance/intercept filters at the application-level (e.g., based on criteria such as email/webmail addresses or login IDs) as opposed to the network protocol-level which require knowledge of network protocol fields.

Also, they provide best-of-breed Deep Packet Inspection (DPI) and Deep Application Protocol Inspection (DAPI) technology, allowing them to not only inspect the packet content in addition to the basic packet header fields, but to also decode and interpret which applications are using the packets. DPI is often compared to the Post Office looking inside each package shipped as opposed to simply looking at the To: and From: information, and DAPI can be compared to the Post Office looking inside a series of packages and inferring their relationship (e.g., what they would be used for).

The remainder of this paper will explore the features, underlying technology, and examples of the uses of the DeepProbe and DeepSweep Network Surveillance Systems.

Network Surveillance Overview

Uses of Network Surveillance

IP Fabrics' IP network surveillance systems are designed to meet the requirements of four market segments:

1. **National Security:** specific uses include intelligence gathering, counter-terrorism activities, and espionage.
2. **Criminal Investigations:** most notably lawful interception and US CALEA compliance.
3. **Cyber Crime:** Internet-based crimes, such as scams, phishing, child pornography, etc.
4. **Network Abuse:** such as detecting improper or illegal use of private or public networks.

Network surveillance is critical to each of the above application areas.

Stage I of Network Surveillance: Mass Interception for Target Identification

Conducting network surveillance often has two stages. The purpose of the first stage is to *identify targets*. This stage is often omitted because the target(s) may have been identified by other means (ie, physical surveillance, other intelligence, etc). When target identification is conducted via network surveillance, it is most commonly done using *mass interception*, performed at the application-level using content-based filters, such as inspecting all email and webmail for certain keywords or phrases, or looking for some abnormality in the amount or frequency of communications between networks, endpoints. This stage is often an iterative process (sometimes referred to as 'peeling the onion') to eventually isolate the surveillance to a set of targets.

Stage II of Network Surveillance: Target-based Interception

Which leads us to the second stage of the surveillance – target based surveillance. In this stage, we have a known set of targets and want to monitor or intercept their network traffic.

Target Discovery

The first component of target-based surveillance is the target *discovery*. This involves monitoring network traffic in an attempt to locate the traffic of a particular target. This is often a complex process that involves carefully inspecting every single packet at wire speed as it traverses the network and understanding how application use these packets. Due to the sheer volume of traffic, buffering/retaining all traffic isn't feasible, so the packets must be inspected 'on the fly'. It is critical to have the capability to inspect at wire speeds (meaning to process each packet before the next one arrives) since subsequent packets might need to be acted on based on information contained in the previous packet. Discovery is usually accomplished using one or more *filters* which are expressions of the discovery logic.

Target Interception/Action

The second component of target-based surveillance is acting on traffic of interest. Common options are to record specific packets or flows (conversations) or to keep the equivalent of call detail records (key statistics that characterize a conversation). Other options would be to retransmit those packets to other hosts or network devices or to keep key statistics on the occurrence of certain events.

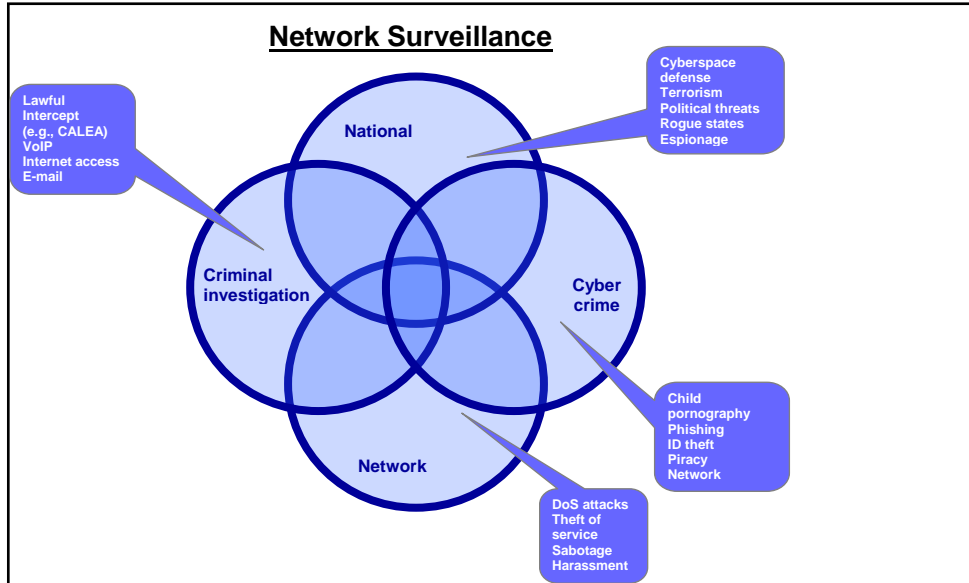


Figure 1. Network Surveillance Uses

Network Implementation of Network Surveillance

Network surveillance systems are generally viewed in two different manners. The first is as a 'probe'. In this case, they are often just one of many different forms of data being monitored/collected (other examples could be r/f signal capture, location data, etc) and are part of a broad intelligence collection aggregator and would typically feed into sophisticated analytic software.

The second is as a standalone system, potentially even portable, geared toward monitoring subjects in a very specific location/network. In some cases, the system will be rapidly and covertly deployed close to the targets location (e.g., apartment building, internet café, etc).

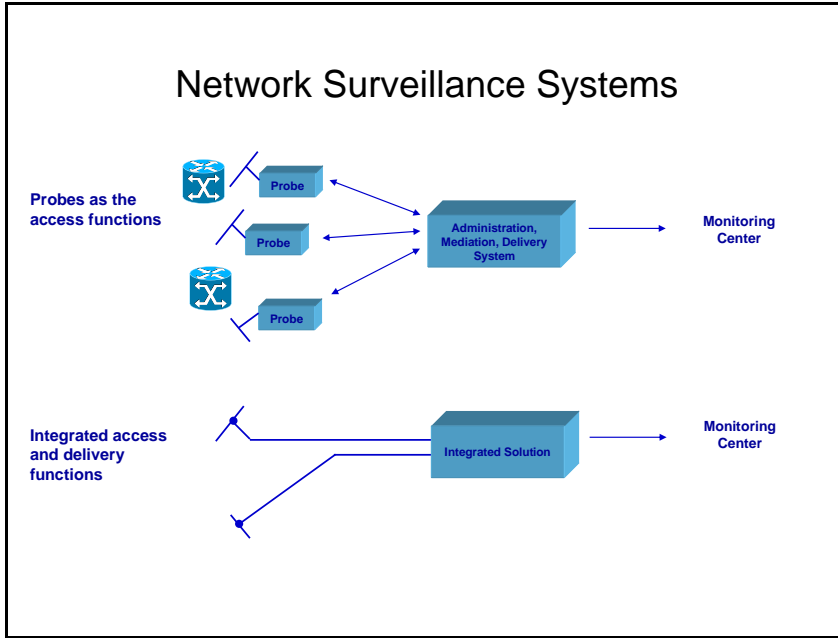


Figure 2. Network Surveillance Systems Architectures

IP Fabrics DeepProbe Network Surveillance System

DeepProbe System Features

As mentioned earlier, DeepProbe is an intelligent probe designed to be used in large, distributed, 1Gbps and 10Gbps networks. Multiple DeepProbes are often deployed in the same network and are provisioned, managed, and mediated by a centralized system, often called a mediation system.

DeepProbe has the capability to fully inspect every network packet and decode application-level protocols, so the controlling mediation systems don't need to rely on CMTSs, switches, routers or other probes for filtering and intercept. Using this approach provides several key benefits:

1. it eliminates any performance impact to the existing infrastructure by not requiring these systems to perform monitoring/intercept,
2. it provides enhanced intercept capabilities, since most existing network elements only inspect packet headers and don't have DPI or DAPI capability,
3. it reduces the processing and communications bandwidth required by the mediation systems

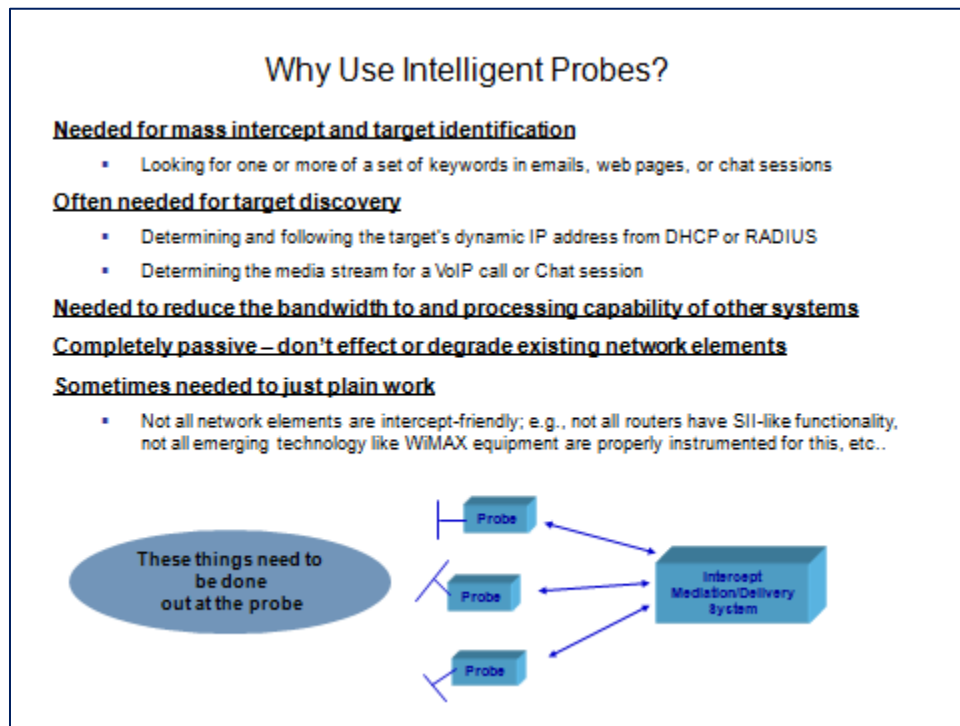


Figure 3. Benefits of Using Intelligent Probes

Management and Provisioning

The DeepProbe is typically provisioned and managed by a centralized mediation platform using secure ASN.1-formatted commands. Each provisioning command is reliably transmitted via TCP and securely authenticated to prevent use by unauthorized systems.

Target Identification and Discovery

Once provisioned, it identifies and/or discovers targets based on a sophisticated and flexible set of criteria, such as:

- DHCP or RADIUS dynamically assigned IPv4 or IPv6 addresses
- Email address or partial email address
- VoIP user name or phone number
- Webmail address or domain
- IM/Chat username
- Keyword/signature in a specific application (e.g., webmail, email, etc)

Target Intercept and Delivery

Once the target is discovered the DeepProbe can be configured to deliver varying amounts of intercepted information, including the complete application flow with related content such as attachments, a summary of the content, or just the application session events (i.e., IRI or Pen-Register equivalent). For IP traffic intercepts, the DeepProbe can qualify the intercepted traffic by layer 4 ports or application identifiers and will monitor all subsequent dynamic IP address (re)assignment. For email interception, the DeepProbe can deliver the entire email, even if the email address identifier was discovered after the first packet(s) in the email flow.

DeepProbe also incorporates sophisticated reconstruction logic to deliver only pertinent information when intercepting complex applications such as webmail and IM/chat, significantly reducing the processing required by the monitoring and analytic systems.

Figure 4 offers a summary of DeepProbe operations.

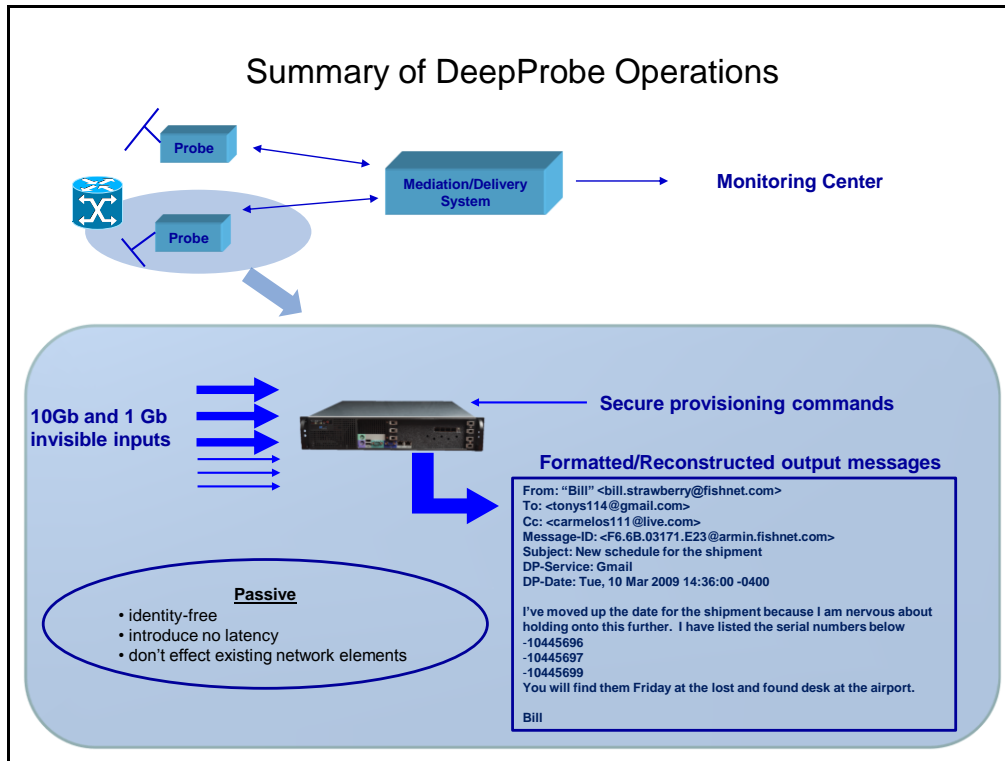


Figure 4. DeepProbe Operations

A Unique Discovery Approach

Discovery in the DeepProbe is provided via the innovative Surveillance Module™ architecture. To the user, Surveillance Modules (SMs) are a series of well-defined, secure ASN.1 commands, which are designed for specific surveillance techniques. For example, there are SMs for discovering webmail traffic, user-id login (e.g., radius or DHCP), and VoIP traffic. These are termed 'application-level' SMs, since they deal with specific target applications/usages.

Other SMs include those geared towards monitoring more generic flows (conversations) based on specific packet header or content characteristics. These are termed 'protocol-level' SMs since these require the user to be somewhat knowledgeable of specific packet header and/or content values. Table 1 provides a summary of the DeepProbe Surveillance Modules.

DeepProbe Surveillance Module	Description	Availability *
IP Traffic	IP traffic discovery and intercept. Discovery includes RADIUS, DHCP, DHCP option 82, and static IP/subnet	Now
VoIP Traffic	SIP-Based VoIP discovery and intercept	1H2010
Email Traffic	SMTP, POP3, and IMAP4-based email discovery and intercept	Now
Webmail	Application-level decode and intercept of Gmail, Hotmail/Live, Yahoo, and Mail.com webmail services	3Q2009
IM/Chat	Application-level decode and intercept of MS Live, yahoo, Google Talk, AIM, and Jabber	1H2010

IP Fabrics DeepProbe™ and DeepSweep™ Network Surveillance Systems

Webmail/Chat Keyword	Extensions to Webmail and IM/Chat SMS to discover users based on keywords in body, subject, and attachments. Keywords can be specified as simple strings, regex, or large signature databases.	2H1010
URL Keyword	Application-level intercept based on DNS and HTTP urls..	2H2010
Future SMS	Application-Level analysis for new, emerging, and other applications.	future

* Planned availability at the time of this writing. Actual availability may change

Table 1. DeepSweep Surveillance Modules

The DeepProbe-1 is a 'gigabit class' surveillance system that provides 4 or 8 Ethernet surveillance ports, each running at speeds up to 1Gbps. The system is packaged as a network appliance, in a 2U rack-mountable form factor.

The DeepProbe-10 is a '10Gbps-class' surveillance system that provides 4 10Gbps and 6 1Gbps surveillance ports. The system is packaged as a network appliance, in ATCA form factor.

IP Fabrics DeepSweep Network Surveillance System

DeepSweep System Features

IP Fabrics has created a best-of-breed, stand-alone, IP network surveillance system released under the product family name ‘DeepSweep’. The DeepSweep system is a powerful, configurable network system for monitoring and inspecting IP network traffic and taking actions on desired traffic. For example, DeepSweep could monitor all of the network activity on an organization’s network, searching for emails to a specific email address or for access to web sites content containing one of a large set of specific keywords/strings. Once traffic of this type was found, the system could then (as an example) record that traffic to a local hard disk as well as all subsequent traffic from the originator.

As mentioned earlier, there are two fundamental components to the system – the discovery and the actions.

DeepSweep Discovery

Similar to the DeepProbe, discovery in the DeepSweep is via SMs. To the DeepSweep user, SMs are a series of configurable web pages which are crafted for a specific surveillance technique. DeepSweep has both application-level and protocol-level SMs Table 2 provides a summary of the DeepSweep Surveillance Modules.

DeepSweep Surveillance Module	Description	Availability*
Packet Traffic	Layer 3-7 packet analysis at the network/protocol level	Now
Packet Flow	Layer 3-7 flow-based analysis at the network/protocol level	Now
Sub-IP	Layer 2-2+ (Ethernet, PPPoE, MPLS, shims) analysis	Now
User Connection	Application-Level analysis of various login and authentication protocols, including RADIUS, DHCP, and Diameter	Now
IAS (Broadband) CALEA Intercept	Application-Level analysis supporting lawful interception of Internet access and services per ATIS-1000013.2007(T1.IAS). Includes support for pen-register, tap-and-trace, and full content interception as well as standards compliance and interoperability with collection devices. Supports several delivery mechanisms, including streamed via UDP and TCP as well as buffered via ATIS-1000021.	Now
VoIP CALEA Intercept	Application-Level analysis supporting lawful interception of VoIP services per ATIS T1.682 version 2. Includes support for pen-register, tap-and-trace, and full content interception as well as standards compliance and interoperability with collection devices.	Now
CBIS CALEA Intercept	Application-Level analysis supporting lawful interception of broadband data per CableLabs CBIS standard. Includes support for pen-register, tap-and-trace, and full content interception as well as standards compliance and interoperability with collection devices.	Now
Future SMs	Application-Level analysis for new, emerging, and other applications.	future

* Planned availability at the time of this writing. Actual availability may change.

Table 2. DeepSweep Surveillance Modules

The IP Fabrics' DeepSweep SM architecture allows for multiple independent SMs to be run simultaneously and/or for SMs to be chained together for more complex logic. A simple example of this would be to have one protocol-level SM filter out traffic that wasn't from a known list of targets and to then chain the resultant traffic to an SM looking at specific email activity with specific keywords or other email values.

As one can see, the value of the SM Architecture lies in providing an interface that is both simple (via the application-level SMs) and yet allows complex discovery logic. Figure 5 illustrates one of the configuration screens for a protocol-level SM.

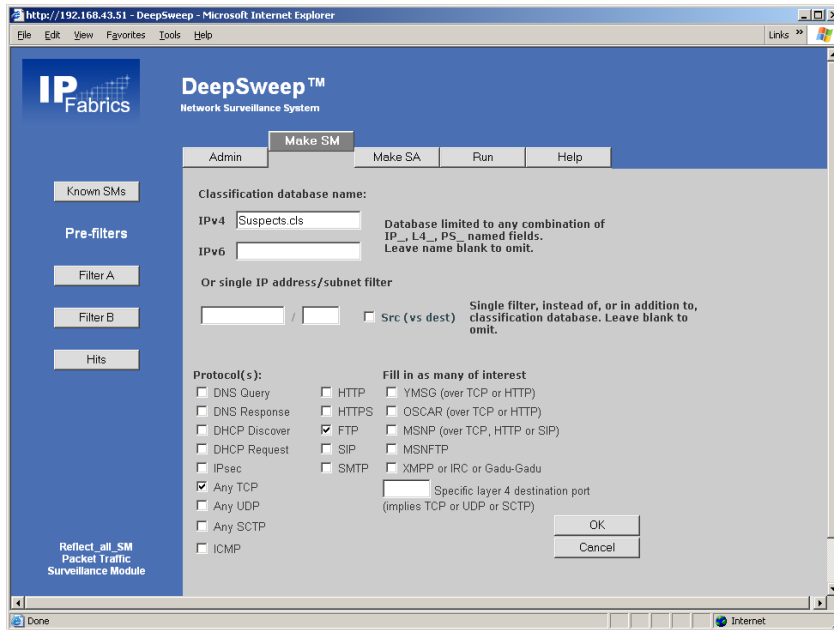


Figure 5. Sample DeepSweep protocol-level SM configuration interface

DeepSweep Actions

Now, on to the handling of network traffic that has been discovered. Each DeepSweep SM provides several options for how to handle traffic that has passed the discovery criteria:

1. **Record** The traffic is time-stamped and saved on the system's local disk drive in .pcap format.
2. **Gather Statistics** Statistics/Counters are kept, but the actual packets are not.
3. **Monitor in Real Time** Traffic is displayed in a scrolling, real time visualization
4. **Hand-Off to a Local User/Custom Application** Traffic is passed to a user-provided application running on the DeepSweep host processor (typically, a Linux user-mode application)
5. **Generate an SNMP Alert**

6. **Generate an Inter-DeepSweep Control/Update Message to other DeepSweeps** Here, the information learned from one DeepSweep can be communicated to another DeepSweep. This is particularly useful for user-id logins, dynamic IP address assignment, and connection-oriented protocols such as SIP (used in VoIP) among other things. Put simply, this allows one DeepSweep that has detected a target to inform the others what to look for.
7. **Reflect the Raw Traffic** The unmodified traffic is transmitted out a network port. This is useful when using the DeepSweep as a simple pre-filter.
8. **Transmit an External Record** Information, which may or may not include the raw or reformatted packet, is transmitted to another device. This may include encapsulation and/or other significant reformatting. This is useful for interoperating with other devices and/or complying with standards for traffic presentation.

Figure 6 summarizes the actions offered in DeepSweep.

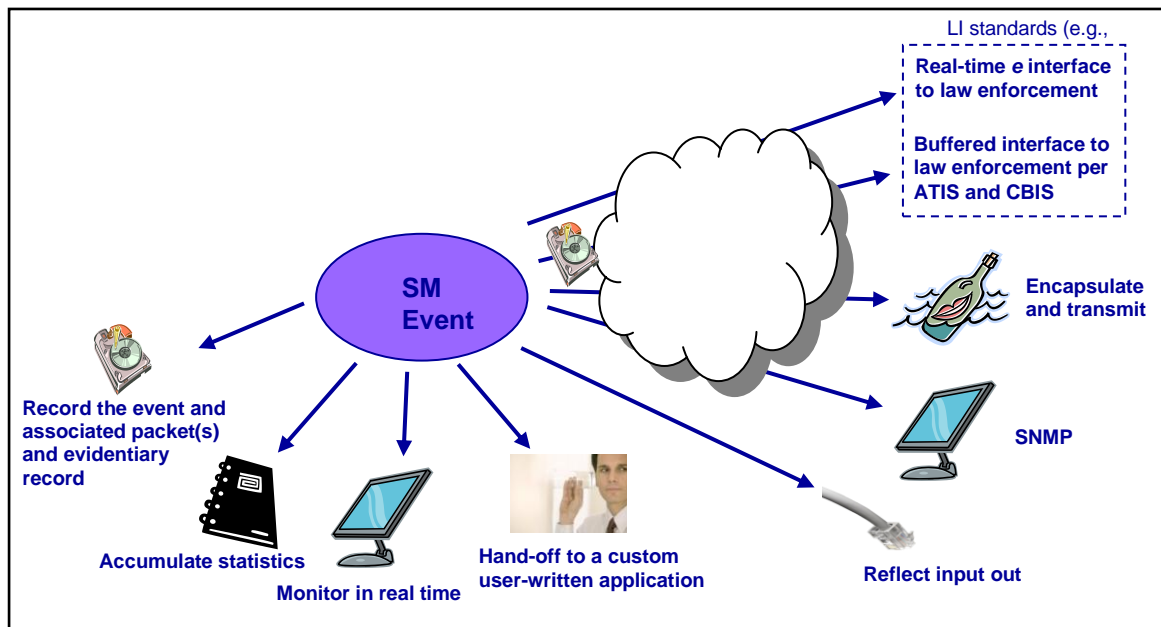


Figure 6. DeepSweep Actions

The DeepSweep family currently consists of two products, one generally available and the other under development with planned production availability in 2009.

The DeepSweep-1 is a 'gigabit class' surveillance system that provides 2, 4 or 8 Ethernet surveillance ports, each running at speeds up to 1Gbps. The system is packaged as a network appliance, in a 2U rack-mountable form factor. At the time of this writing, the DeepSweep-1 has been deployed by many service providers and government agencies.

The DeepSweep-10 is a '10Gbps-class' surveillance system that will provide 2 surveillance ports, each capable of monitoring 10Gbps Ethernet network links. The system is packaged as a

IP Fabrics DeepProbe™ and DeepSweep™ Network Surveillance Systems

network appliance, in ATCA form factor The DeepSweep-1 and DeepSweep-10 function the same, with the exception being the greater performance of the DeepSweep-10. The DeepSweep-10 system is currently under development and evaluation systems are planned to be available at the end of 2009.

DeepProbe and DeepSweep Technology

DeepProbe and DeepSweep systems are powered by IP Fabric's innovative multi-core DAPI/DPI engines and virtualization technology. This technology allows complex IP packet analysis to be parallelized (or, to run concurrently) across multi-core network processors, allowing wire-speed DAPI/DPI on 1Gbps and 10Gbps networks.

This approach has many benefits over more-traditional approaches (e.g., ASICs, FPGAs, general-purpose processors, etc.) including increased performance, increased capacities, and extensibility. This underlying technology facilitates the rapid introduction of new SMs by simply adding additional software modules that run on the multi-core network processors.

Deep Packet Inspection

At the core of the DeepSweep is a technology termed Deep Packet Inspection (DPI). Quite simply, DPI enables network devices to access portions of network traffic beyond the packet headers ("looking deeply into the packet"). Traditional networking devices such as routers and switches access only the packet headers to perform their networking function. Even early security devices (e.g., firewalls) only looked at packet headers. However, as communications are increasingly based on IP (e.g., VoIP, person-to-person communications, email, chat, etc) it is insufficient to simply inspect the information contained in packet headers. A common analogy is to equate network equipment that simply looks at packet headers to inspecting the packages carried in the US mail by simply looking at the 'TO:' and 'FROM:' labels on the package.

DPI fills this gap by enabling networking equipment to look at entire packets, including the payload (also called the content). Some common examples of important information contained in the content portion of packets are email addresses, user-ids used in logins, and text strings found inside of communications. To continue the prior analogy, DPI is equated to having the agency inspect the contents of each package. Figure 7 gives a short summary of deep packet inspection.

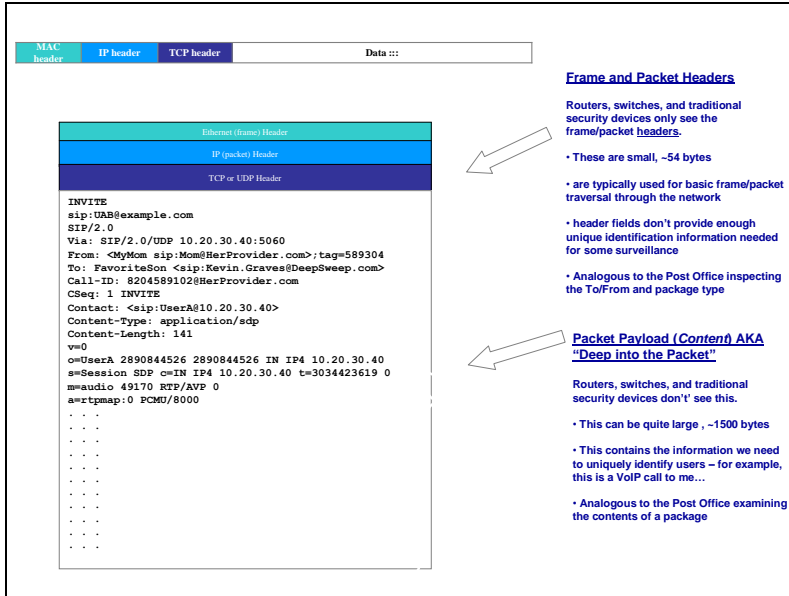


Figure 7. Deep Packet Inspection (DPI)

From a technical standpoint, DPI is a challenging subject since it potentially requires every byte contained in packets to be inspected at wire speeds (the maximum speed of packet arrival on a given network link). For example, on a gigabit Ethernet link, frames can arrive every 672ns. On a 10Gbps link, this time shrinks to ~57ns. In today's networking systems, the only viable method to accomplish DPI at speeds equal to or greater than 1Gbps is to use fixed-function ASICs, FPGAs, or multi-core processors (as are used in the DeepSweep).

Deep Application Protocol Inspection – Because Basic DPI isn't Good Enough

While DPI is a powerful technology, state-of-the-art surveillance systems need more sophisticated techniques for identifying, discovering, and intercepting targets. This is where DAPI comes in. In short, DAPI is the ability to inspect and understand how applications are communicating. This includes understanding an application's syntax and semantics to the extent users can be discovered and their subsequent communications can be decoded and pertinent traffic intercepted.

A good example of where DAPI is used is VoIP intercept. In simple terms, DPI can be used to locate a targets identity in the SIP call-setup message, but DAPI state machines must be used to monitor the subsequent SIP messages to determine the route of the resultant RTP stream.

Another more complex example is a typical webmail application, which might use a variety of layer 4 ports during a session and might gzip compress much of the communications, including the addressing information. While traditional DPI would have visibility to the pertinent packet bytes, it wouldn't understand what they mean. This is where the DAPI state machines and heuristics are used to piece together and decode the information from multiple packets.

There are several other interesting examples of where DPI falls short and DAPI is needed. Table 3 summaries a few of these.

Where DPI isn't Good Enough	Description
Layer 4 ports aren't reliable	Some applications don't use standard ports; others have fallback ports to use when primary ports are blocked.
Established conversations don't stick the initial ports used	Some applications cycle through a wide range of ports during a single session.
TCP sessions span multiple packets	Key data might be split across multiple packets, so looking at individual packets could result in missing required information.
Many hosted services use compressed or encoded data	This includes key addressing information and varies from service to service.
Many hosted applications are cluttered	Most of the data in webmail sessions is irrelevant – i.e., banners, advertisements, etc.

Table 3. Why DPI isn't Good Enough

DeepProbe and DeepSweep Usage Examples

DeepProbe for Monitoring and Intercepting IP Traffic in a Comprehensive Surveillance Solution

One common use of probes is in complex networks where there isn't a single aggregation point with visibility to all of the desired traffic. In this situation, multiple DeepProbes are distributed throughout the network in such a manner that at all interesting traffic is visible to at least one DeepProbe system.

In these configurations, the DeepProbe typically communicates with three other logical systems in the intercept system model:

- Administration/Provisioning system which provisions each DeepProbe (sometimes with assistance from the mediation systems) with the desired SMs using the DeepProbe's secure remote API
- Mediation systems, which update the various intercept access points (e.g., probes, intercept-capable network elements, etc.) and correlate intercepted data from various sources for delivery to the monitoring center
- Monitoring Center systems, which will sometimes directly receive intercepted data from DeepProbe (as opposed to an intermediate mediation system).

Note that in some cases several or all of these logical systems are implemented in a single physical system (for example, the IP Fabrics DeepSweep system functions as the Administration/Provisioning system and the Mediation system).

In these complex networks, the DeepProbe functions as the intercept access point – the system that is passively monitoring the network and intercepting the desired traffic. It is important to ensure that all of the key traffic is visible to at least one of the DeepProbes. For example, it would seem trivial to monitor all traffic at a single point in a case where there is a single gateway aggregating all traffic in/out of the network to be monitored (this could be a country gateway, or the gateway of a large institution). But conditions such as the following must be considered:

- *What about traffic that never leaves the network (e.g., country) or is hair pinned at the local ISP?*
- *Are there any networks or network segments that require special treatment due to the confidential data carried on them?*
- *Are there any unique application servers such as webmail, chat, conferencing, or IPTV that could require dedicated probes due to application-specific nature of their traffic or potential intermediate anonymizing servers between the end-user and the server?*

Conditions such as these in larger, complicated networks often require multiple probes to be distributed throughout the networks. Figure 8 summarizes the surveillance topology using distributed DeepProbes in a comprehensive intercept solution (for illustration purposes, the provisioning and mediation systems have been omitted).

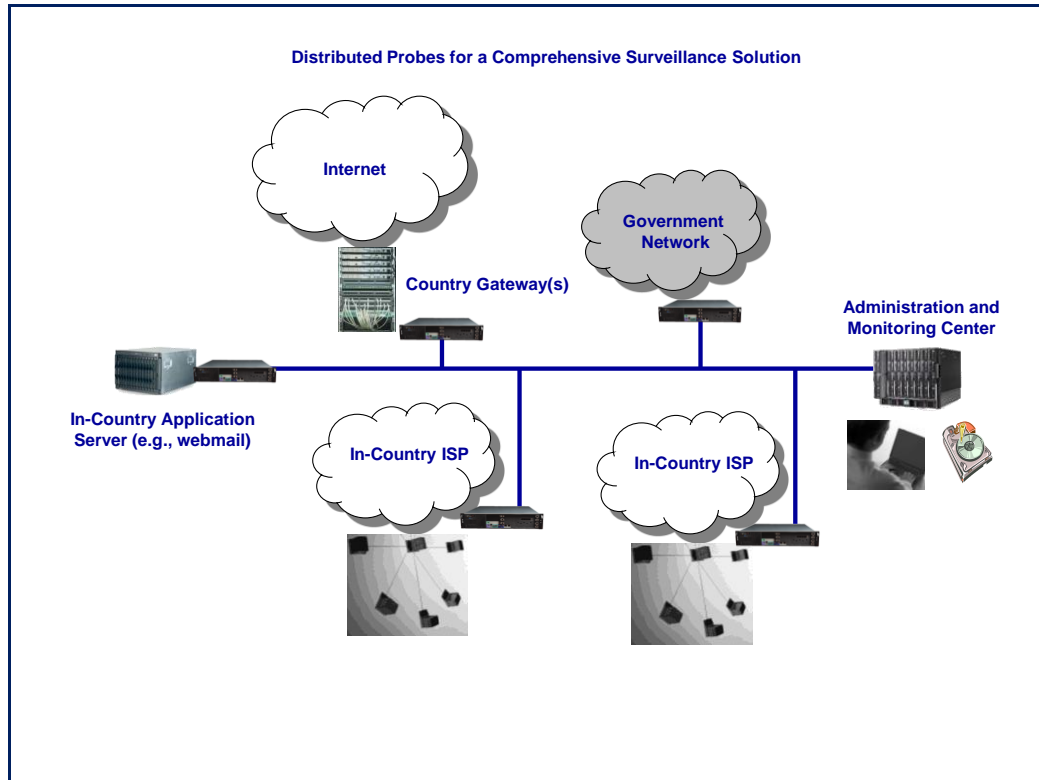


Figure 8. DeepProbe used as an intelligent probe in a distributed monitoring solution

For the entire solution to operate efficiently, it is important to reduce the amount of data as far out in the network as possible (as opposed to the other extreme, which would be to intercept every packet and deliver it to the monitoring center, which obviously is not a workable solution). The best approach for this is to deploy intelligent probes, such as DeepProbe. Intelligent probes greatly reduce the traffic delivered to mediation systems (or directly to monitoring centers) by doing the following:

- Using DAPI and DPI to discover targets, thus eliminating the signaling and application protocol traffic that would normally be delivered.
- Performing broad-based surveillance (mass interception) to help identify targets, reducing large amounts of traffic delivered to the analytic systems.
- Decoding application protocols and delivering only pertinent intercept data, such as in webmail, where only a small portion of the browser session is relevant.

DeepSweep used for Internet and VoIP Lawful Interception/US CALEA Compliance

One of the timeliest uses of DeepSweep is for the lawfully authorized electronic surveillance of Internet access and services (sometimes referred to as ‘broadband CALEA’) and VoIP. In this usage, DeepSweep performs the functions of discovery and forwarding of information to a law enforcement agency (LEA) collection device via some standardized message formats. A typical installation would have one or more DeepSweep systems attached to an Internet service providers (ISPs) network where dynamic IP address assignment/login/authentication (e.g., RADIUS, Diameter, DHCP) as well as user traffic are visible. Note that in some ISPs, everything will be visible at a single place in the network, whereas in others, multiple DeepSweeps would need to be installed.

Each DeepSweep system performs one or both of two key functions. The first function is implemented in the *controller SM* and is tasked with systematically inspecting every packet against one or more subjects associated with a surveillance warrant from an LEA. The second function is implemented in the *content SM*. Once a controller SM detects a subject event (ie, a subject logging in or getting a dynamic IP address assigned), it notifies all of the configured content SMs (located on the same or other DeepSweeps) and sends the LEA collection device(s) the appropriate messages. Once notified, the content SMs will monitor all traffic to/from the subject, and send the LEA(s) the appropriate information (the actual information varies with each warrant, some specifying that all content be sent to the LEA, whereas others, such as pen registers and trace-and-trap intercepts, require less information).

Figure 6 illustrates how this would be configured at a small ISP. At larger service providers, DeepSweep systems would most likely be used in conjunction with other intercept equipment (e.g., switches, routers, probes) and controlled via a centralized mediation device.

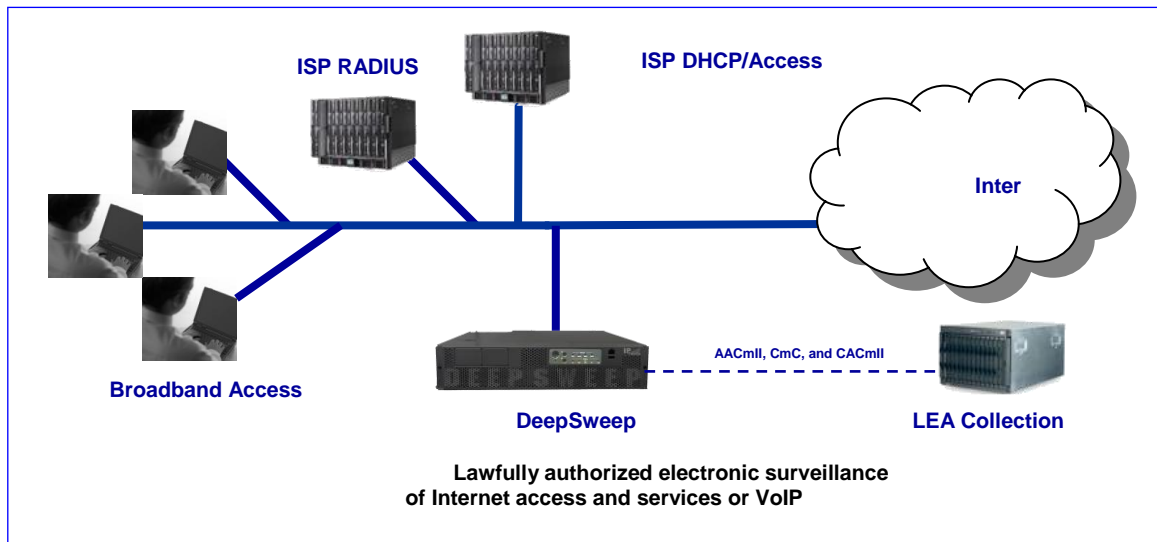


Figure 9. DeepSweep used for lawfully authorized electronic surveillance of Internet access and services in a small Internet service provider

DeepSweep used as a Tactical VoIP Intercept/Wiretap System

One challenge facing Law Enforcement Agencies (LEAs) is that many service providers haven't complied with CALEA and aren't able to execute court-ordered intercepts. This problem is most evident with IP-based service providers, and more specifically, ISPs and VoIP providers. When this occurs, the LEA is faced with taking action against the service provider to get them to become compliant (usually very time-consuming), just ignoring the intercept, or providing their own equipment and executing the intercept themselves – often called a tactical intercept.

The DeepSweep is an excellent solution for this type of tactical intercept for several reasons.

1. **The DeepSweep is Portable and Remotely Accessible:** packaged as a 2u rack-mount server, the DeepSweep can easily be transported to the service provider facilities and can be installed in existing racks, on top of other equipment, or placed on the floor. DeepSweep's are available with either AC or DC power supplies, and can be accessed/managed locally and remotely.
2. **The DeepSweep is Passive:** the DeepSweep surveillance interfaces are completely passive and don't affect the service provider's network traffic (e.g., don't add additional latency, don't degrade signal quality, etc).
3. **The DeepSweep is Self-Contained:** DeepSweep systems incorporate the probe/access point, mediation, and administration functions of the typical intercept system – all in the base DeepSweep system. Additionally, DeepSweep doesn't rely on service provider equipment such as routers or session border controllers to perform intercepts.

This last point is a critical one when dealing with VoIP wiretaps, especially in the case on non-managed VoIP services such as those offered by Vonage. In cases like these, there are two key complicating factors. First, inherent in VoIP is the likelihood that the signaling traffic (e.g., SIP) and the encoded voice (e.g., RTP) will traverse different network paths and in most cases both will not be routed through the non-managed VoIP providers facilities. Without altering the normal network routing (sometimes called a 'forced routing') the best place to perform the intercept is 'close to the user', which is normally at the user's ISP. To perform these intercepts, LEAs need tactical intercept systems that can be transported to the target's ISP, and, these systems need to be capable of intercepting VOIP calls. Since the ISP isn't offering the VoIP service, they most likely don't have 'VoIP-aware' equipment (e.g., session border controller, SIP server, etc) to assist in the intercept. So, the tactical intercept system needs to be completely self-contained and able to *discover* VoIP calls based on, for example, a phone number, and intercept the call per the court order. Since surveillance court orders are often pen-registers, the intercept system can't be simple packet recorder; it must adhere to the electronic surveillance laws and support pen-register, trap & trace, and full content intercepts, as well as deliver the content in 'near real time' to support LEA minimization guidelines.

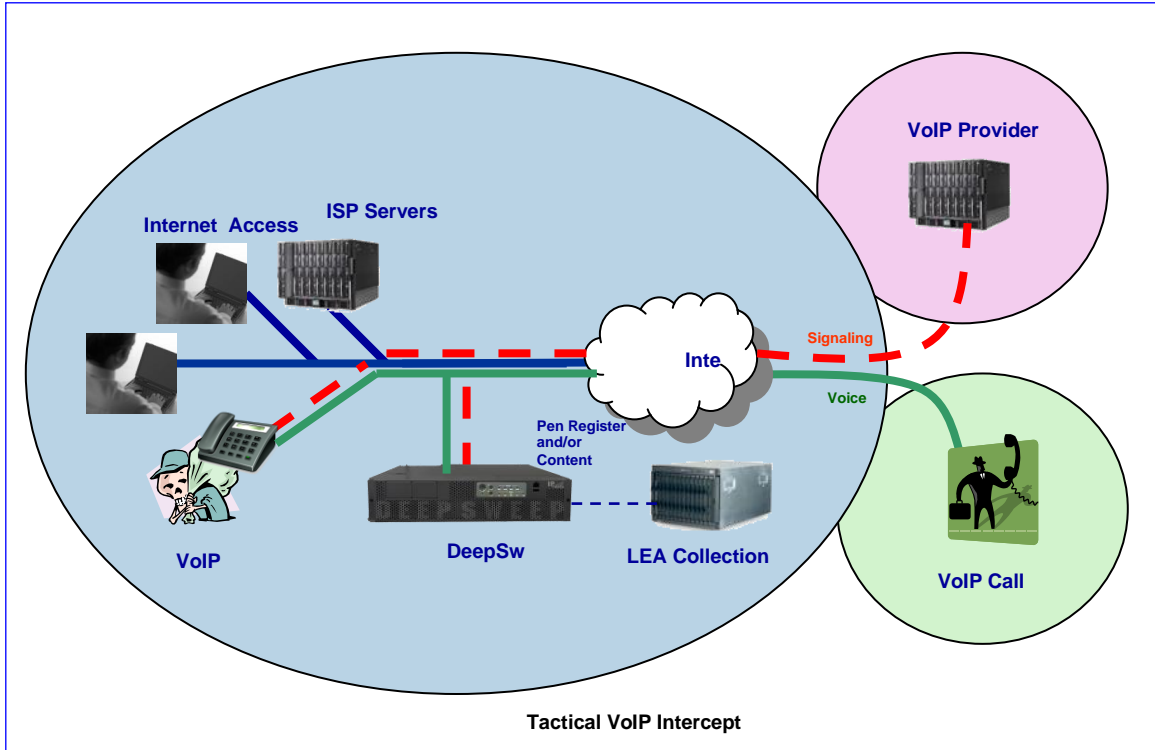


Figure 10. DeepSweep used as a tactical intercept system for VoIP

DeepSweep as Standalone Surveillance System

One common DeepSweep usage is as a standalone surveillance system. In this usage, the DeepSweep performs the complete functions of discovery and forensics/collection. A typical installation would have one or more systems attached to a network aggregation point (ie, a collection point in the network where the amount and breadth of traffic is maximized, for example, a location with visibility to multiple hosts, subnets, etc). Each system is systematically inspecting every packet against a set of criteria and if determined to be *interesting*, the packet (and potentially other related packets) are retained on the local hard drive for later analysis.

It is common to use off-the-shelf Ethernet taps to facilitate the physical connectivity to the target network links. These taps are completely identity-free (as are the DeepSweep surveillance ports) and can be detected only by visual identification. The tap serves the purposes of creating an identical data stream and presenting it to the DeepSweep. This has the benefit of having the DeepSweep act as a completely passive, out-of-band (ie, not inline) device.

The DeepSweep would commonly be configured to monitor DHCP IP address assignment or RADIUS user-id logins for specific targets and then to record all subsequent traffic to and from those targets. The recorded traffic could then be inspected/analyzed post-capture using other available analytic tools.

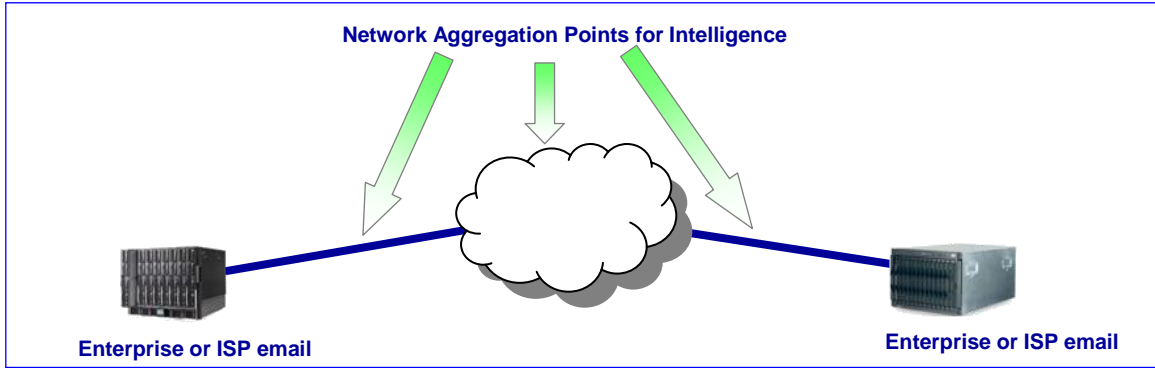


Figure 11. DeepSweep used for intelligence gathering as a standalone surveillance system

DeepProbe/DeepSweep as a Pre-filter for Existing Surveillance Devices

Another common DeepProbe/DeepSweep usage is to act as pre-filters for existing (and probably slower) equipment. This is particularly useful if the existing equipment has significant legacy value, such as a large number of agents trained to use it, required certifications, proprietary databases, or if it provides capabilities not supported by the IP Fabrics' systems.

In this usage, the DeepProbe/DeepSweep and the existing equipment are serialized/pipelined, with the DeepProbe/DeepSweep in a stage before the other equipment (logically 'in front of'). The primary role of the DeepProbe/DeepSweep is to inspect all network traffic and use broad filters to weed out the traffic known to be unimportant. The forwarded traffic may or may not necessarily be important, but if the overall amount of traffic has been significantly reduced, the next stage of the pipeline can perform the final processing. As a side note, this technique has been used with multiple DeepSweep systems for very complex surveillance logic.

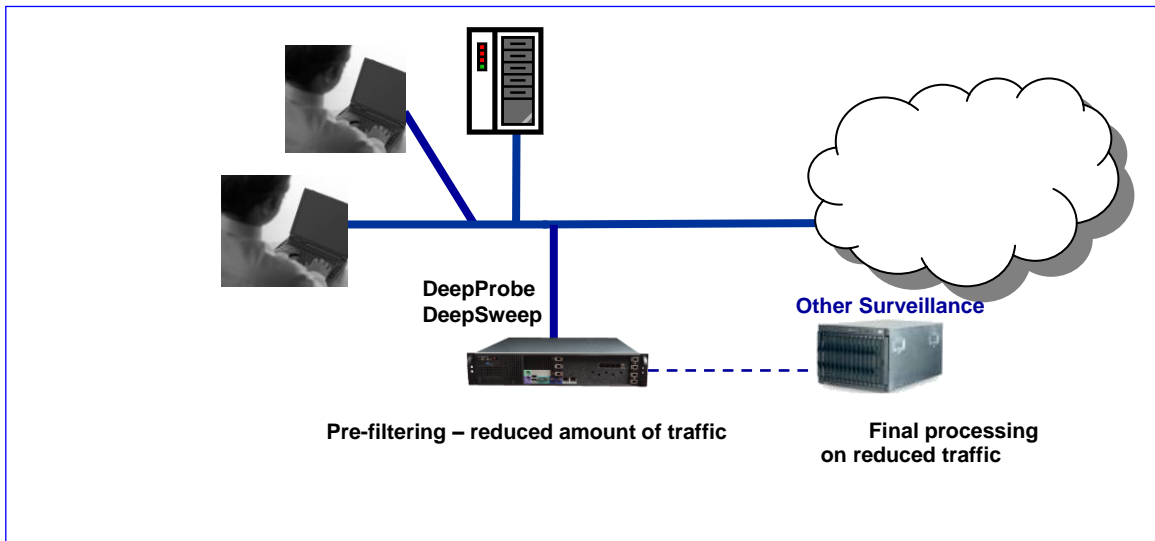


Figure 12. DeepProbe/DeepSweep used as a pre-filter for legacy equipment

DeepProbe/DeepSweep as Insider Threat Detection/Mitigation

In this usage, the DeepSweep or DeepProbe would be logically located on an organization's internal network with the goal to inspect the network traffic from internal users to ensure that the network isn't being abused or attacked from the inside (something traditional perimeter security device configurations using firewalls, intrusion detection systems and VPNs wouldn't prevent). Since many organizations' internal networks are 1Gbps and many internal server-to-server connections generate large amounts of network traffic, a standard PC-based system cannot be used.

The surveillance system will be configured to detect and intercept a variety of traffic at wire-speed, including:

- Emails to/from specific users
- Packets/flows containing any of a set of 'signatures' from a signature database
- Packets/flows from specific users triggered by the user log-ins
- Packets from IP addresses known to be invalid
- Packets from applications known to be invalid/not allowed

Since the threat would need to be mitigated in real time, the offending traffic would be sent to a user application running on the DeepSweep system or delivered by DeepProbe to the mediation system. For forensics purposes, the offending traffic would also be recorded and an evidentiary record (including things like log files, time of the system start, etc) could also be recorded.

The following figures illustrate the key aggregation points where wire-speed network surveillance systems would typically be located for intelligence gathering and insider threat detection purposes.

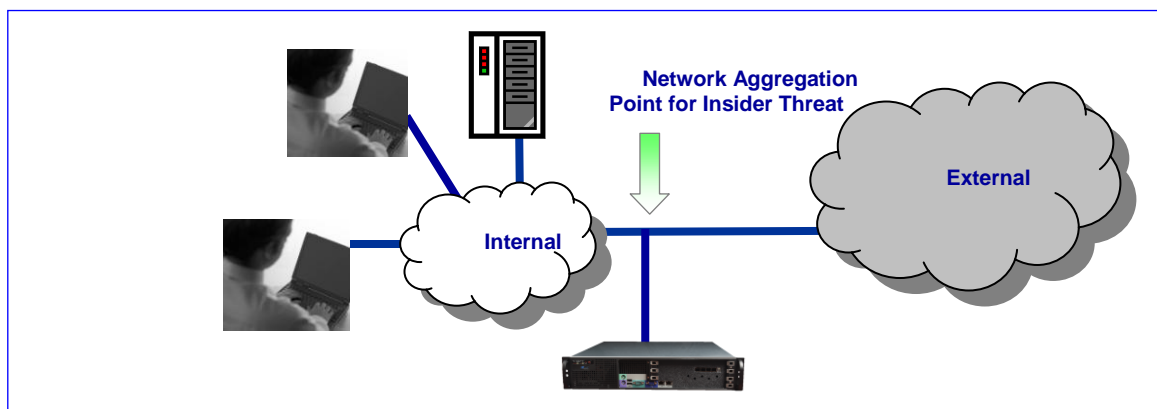


Figure 13. DeepProbe/DeepSweep when used for insider threat detection

Summary – DeepProbe and DeepSweep Features and Benefits

In short, IP Fabrics systems provide several important network surveillance features and resultant benefits. The table below summarizes these.

Feature	Benefit
High Performance	Supports multiple 1Gbps and 10Gbps Ethernet links, each optionally running multiple/different Surveillance Modules.
Broad Applicability	Supports a wide range of network surveillance needs, including intelligence gathering, national security, cyber crime mitigation, insider threat detection, lawful interception, and network abuse.
Surveillance Module Architecture	Allows application-level monitoring (e.g., webmail, chat, etc) and complex surveillance logic via Deep Application Protocol Inspection (DAPI) and Deep Packet Inspection (DPI).
Secure Provisioning and Delivery	Provisioning messages and responses are encrypted/authenticated; intercepted data is optionally authenticated and encrypted, preventing unauthorized use.

Table 4. DeepProbe and DeepSweep features and benefits summary

Further Information

For more information on IP Fabrics and DeepSweep, please visit the IP Fabrics web site, at www.ipfabrics.com

For the DeepProbeSweep product brief, please refer to:

<http://www.ipfabrics.com/pdf/DeepProbe.pdf>

For the DeepSweep product brief, please refer to:

<http://www.ipfabrics.com/pdf/DeepSweep.pdf>

For the DeepSweep model optimized for CALEA product brief, please refer to:

<http://www.ipfabrics.com/pdf/DeepSweepCALEA.pdf>