



perfecting the art of network security

Benefits

- Enables IP based surveillance.
- Minimizes deployment time.
- Allows collection and filtering of application data at Gigabit speeds.
- Does not disrupt or degrade network services.
- Enables real time network monitoring.
- Preserves privacy requirements.

A high performance Layer 7 device used for access, filtering, and delivery of targeted IP data for monitoring and surveillance.

DCFD™ 3500 Meets Demand for IP Based Surveillance

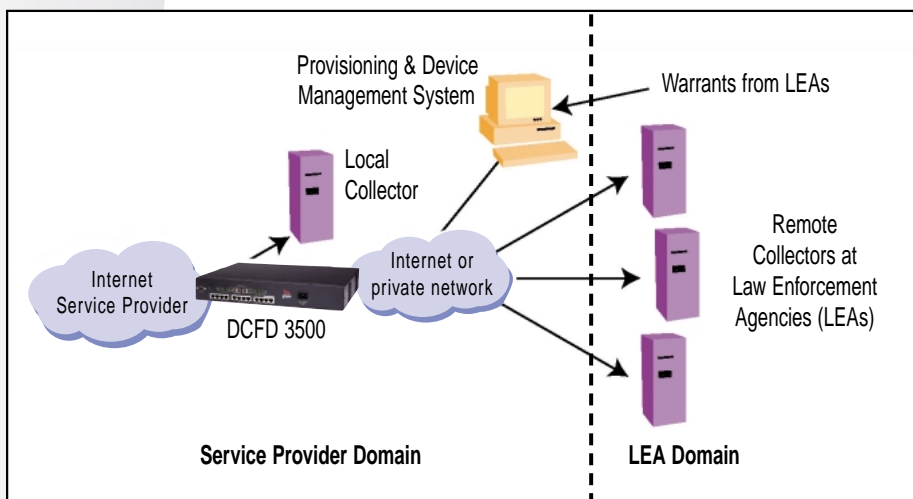
Lawfully authorized electronic surveillance (LAES - sometimes referred to as "wiretapping" or "lawful intercept") is a critically important law enforcement tool that police and other authorized government agencies use to investigate and prosecute criminals. LAES is the collection of (1) the contents of communications; and/or (2) communication identifying information. With the rapid growth of IP based networks (such as the Internet), criminals and terrorists have started using IP based applications for communications (email, chat, instant messaging, voice over IP, FTP etc) instead of voice. A clear need has emerged to create products and standards that can enable surveillance of IP based communications. Top Layer's richly constructed DCFD 3500 product line plays an important role in providing these services.

Precisely Extracts Application Information in Real-time without Disrupting Services

Until today, the technology to perform IP communication surveillance was either not available or too complex to implement due to the connectionless nature of IP traffic and the need to collect IP flows at the application level. Unlike voice traffic, IP traffic can flow through multiple routes and a suspect's IP traffic is usually intermixed with huge volume (Gbps speeds) of traffic aggregated from thousands, even millions of other users. Top Layer's advanced Layer 7 technology has an exceptional ability to precisely extract application information in real time from a busy IP network. Most importantly the DCFD 3500 is connected in the network in a non-intrusive mode, which does not disrupt or degrade the services offered to customers.

Optimal Granularity for Preserving Privacy

The DCFD 3500 can extract data flowing over the network based on an IP address, MAC address, email address, login user names, Instant Messenger handle, specific protocol, or application. Importantly, the device is designed to capture only the traffic to or from the entity listed on the warrant issued by the appropriate law enforcement agency. In so doing, the Top Layer solution preserves the privacy of all non-warrant defined IP traffic.



DCFD 3500 ISP Monitoring Architecture

Built for Speed

Because the DCFD 3500 device will be placed on critical high volume data paths and will be required to process all network traffic, extracting all the requested information is an essential part of the equation. The Top Layer DCFD 3500 ASIC-based solution is able to process packets at Gigabit speeds, thus enabling even the busiest network environment to be scanned for any traffic that meets the warrant defined criteria for surveillance.

Features

- Connects to the network in a non-obtrusive mode.
- Collects IP traffic from a variety of sources and filters out the extracted information requested by a provisioning system.
- Can filter application data based on the following parameters:
 - IP address
 - IP address range
 - MAC address using DHCP
 - MAC address
 - Cable modem ID
 - Email address (SMTP, POP3, using to, from, and cc fields)
 - Web-based email
 - RADIUS login name
 - Instant Messenger handle
- Can deliver data either to a collector directly attached or remotely connected over an IP network.
- Software Development Kit available for developers of provisioning and device management systems.
- Supports both full-content and summary (IRI) delivery.
- Formats and delivers filtered data to LEA collectors based on International standards.
- Available in both 12 10BASE-T/100BASE-TX ports (AS3551 model) and 12 10BASE-T/100BASE-TX with 2 1000BASE-SX ports (AS3552 model) configurations.

About Top Layer

Founded in 1997, Top Layer Networks develops network intrusion detection and prevention solutions enabling enterprises worldwide to protect against cyber threats and scale their infrastructure to meet new, ever increasing security demands. The Company's patented, ASIC-based products are engineered to block high-volume DoS and DDos attacks, HTTP worms, traffic anomalies and unknown attacks as well as improve the effectiveness of intrusion detection systems through intelligent balancing and distribution of traffic. Top Layer Networks is headquartered in Westboro, Massachusetts with sales and support presence in Australia, France, Germany, Japan, Korea, and the United Kingdom.

Top Layer Networks, Inc. 2400 Computer Drive • Westboro, MA 01581 USA • 508.870.1300 • Fax 508.870.9797

Designed for both Law Enforcement Agencies and Service Providers

The service provider IP surveillance architecture can be easily visualized as consisting of 3 components:

- The DCFD 3500 device that taps into the service provider's network and extracts precise information based on provisioned information (warrant defined information). It then delivers the collected information securely to the collector systems either directly attached or remotely at the law enforcement agencies that are connected over an IP network.
- A centralized provisioning system that converts the warrant information to instructions for the DCFD 3500 devices across the network.
- The collectors at the different law enforcement agencies that receive the formatted information sent by the DCFD 3500.

Top Layer has partnered with existing providers of voice monitoring provisioning and collector systems, who have added IP surveillance capabilities into their existing systems. This minimizes the investment required by service providers to enable IP monitoring in their networks.

Top Layer Helps Service Providers Comply with the Surveillance Laws

Top Layer's DCFD 3500 complies with current and emerging standards for IP surveillance (J-STD-025 XX, TIIT, ETSI etc.) and meets the surveillance requirements of various governments (such as CALEA in the U.S). Top Layer is working very closely with law enforcement agencies, other network/telecommunications equipment manufacturers and standards bodies to define and co-develop more IP surveillance standards. Working in concert with law enforcement agencies and suppliers of voice provisioning and collector systems, Top Layer's DCFD 3500 can be quickly and easily deployed either in new networks or existing networks that have other monitoring (such as voice or wireless) capabilities in place.

Specifications

Dimensions:

Height: 6.5 cm (2.55 in)
Width: 43.8 cm (17.25 in) without rack-mount brackets
48.6 cm (19.13 in) with rack-mount brackets
Depth: 33 cm (13 in)
Weight: 5kg (11 lbs).

Environmental:

Operating Temperature:
0° to 40° C
(32°F to 104°F)
Non-Operating Temperature: 25°C to 70°C
(-13°F to 158°F)
Relative Humidity: 5% to 95% non-condensing.

Power Requirements:

AC Input Voltage: 100 to 250 VAC auto ranging
AC Input Line Frequency: 47 to 63 Hz
AC Current Amps: 1.0 A
DC Output Voltage: 48 VDC +/-5%,
Watts: 48.00
Redundant Power Supply (optional)

International Compliance Approvals:

UL Listed
CUL
AS/NZS 3260
CE
FCC Class A
BSMI CNS 13438 Class A
VCC Class A
AS/NZS 3548 1995



perfecting the art of network security

www.TopLayer.com