Top Layer™

perfecting the art of network security

Intelligence Distribution System Balancer

Aggregation, filtering & Load Balancing Appliance

Data Sheet

Top Layer IDSB

- *Up to 80% reduction in capital, maintenance, and operations expenditures for network monitoring solutions.*
- *Enables simultaneous operation of multiple monitoring applications at the same point in the network, effectively multiplying SPAN ports.*
- *Allows scaling the volume of monitored network activity beyond the capacity of a single sensor.*
- *Adds N+1 redundancy for monitoring sensors.*
- *Enables monitoring in asymmetrically routed networks.*
- *Works with all network sensors including:*
  - *Distributed network analyzers*
  - *Forensics systems*
  - *Content inspection engines*
  - *VoIP recorders*
  - *Network IDS*

Network Monitoring is Becoming Common Business Practice Across All Networks.

Network and security professionals monitor their networks for a variety of reasons:

- To improve network security.
- To improve network uptime, and thus provide access to business applications.
- For capacity planning and improving end user SLAs.

There are a variety of monitoring systems that customers use, such as:

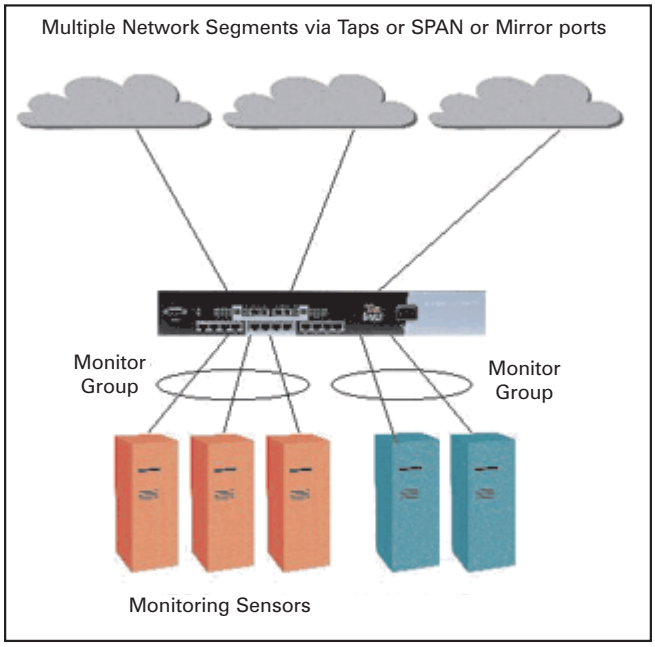
- **Forensics systems:** to identify the source of the intrusion, and possibly initiate legal action.
- **Content inspection:** to enforce corporate policy and prevent employees from accessing unauthorized web sites, such as pornographic web sites and gambling sites during work hours.
- **Network analyzers:** for network troubleshooting.
- **Intrusion Detection Systems**: to detect unauthorized intrusions and attacks (both external and internal) on the company's critical assets.
- **Rmon probes** (and other home grown systems)**:** for collecting data for capacity planning and improving end user SLAs.
- **VoIP Recorders:** for quality assurance and verbal transaction verifications.

Network monitoring provides significant benefits to organizations, however it comes with a high cost and a few deployment challenges.

High Cost of Traditional Network Monitoring

To get 100% network monitoring coverage, network and security managers could choose to install a monitoring sensor in each segment of the network (e.g. before the firewall, after the firewall at the DMZ, and at the internal segments).

This approach works well for small networks, but for larger networks there is a high price tag due to the large number of sensors needed. Restricted by tight budgets, some security managers are taking their chances, and choose to monitor only some segments in their network. The result in these cases can be catastrophic, since missed attacks and intrusions can cause millions of dollars in damages to the organization. The Top Layer Intelligence Distribution Balancer (IDSB) is an alternative solution that provides superior monitoring coverage at a fraction of the cost.



"The Top Layer Balancer fulfills a badly needed requirement in making the best use of valuable resources. It is easy to configure and manage."

— Network Computing

Additional Deployment Challenges of Network Monitoring

In addition to the high cost, network and security managers also have to deal with the following deployment challenges:

- Typically there are a limited number of "SPAN/Mirror" or tap ports in the network, and these have to be shared between the different monitoring applications.
- In many cases the monitoring sensors cannot keep up with large volumes of traffic.
- There is no easy way to add N+1 sensor redundancy.
- Most monitoring sensors cannot operate in asymmetrically routed networks. (Sensors need to see both sides of a flow to operate).

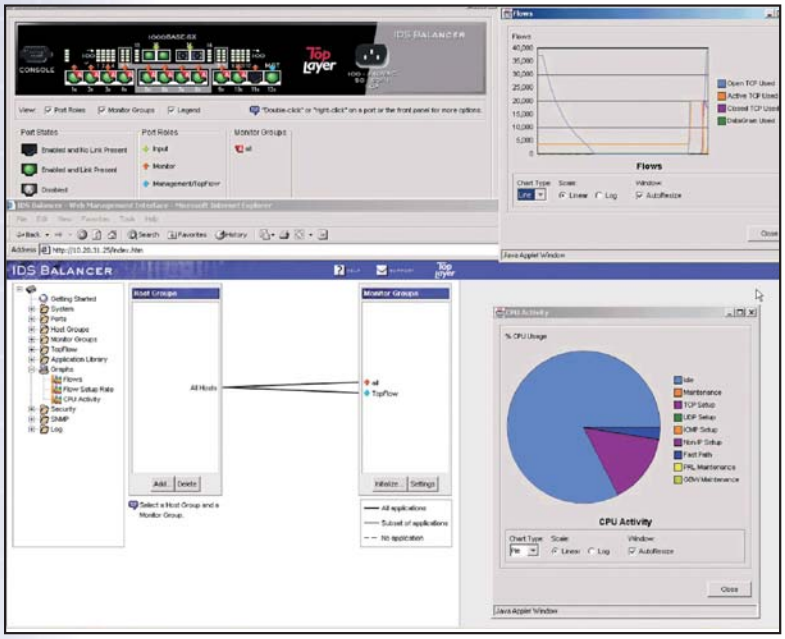
Aggregation Can Save up to 80% by Using Fewer Monitoring Sensors

The Top Layer IDSB aggregates the traffic from multiple network segments and thus it provides immediate savings — since fewer monitoring sensors are required to examine the traffic. For example, if you want to monitor 6 GigE segments you can:

a) Use 6 GigE attached monitoring sensors, or,

b) Use one Top Layer Balancer and one GigE attached monitoring sensor.

In this simple example, the 6 to 1 aggregation saves 80% of the monitoring sensor cost, while providing the same coverage. Top Layer's family of high performance ASIC-based Balancers provides huge savings by offering aggregation for both Fast Ethernet and GigE networks.



Top Layer IDSB Web Management Interface (WMI)

Investment Protection

If your network needs to be upgraded to handle increased traffic, using a Top Layer IDSB is a proven solution for maximizing your current investment in existing sensors and helping to extend their longevity.

When upgrading to Gigabit from Fast Ethernet, the Top Layer IDSB allows you the flexibility to continue to use your existing 100Mbit sensors while providing you with a cost-effective method for upgrading their performance.

Filtering and Multiple Copies of Traffic: No More Fighting for Shared SPAN/Mirror or Tap Ports.

It is very common for enterprises to use two or more different types of monitoring sensors, each one optimized for different types of applications and traffic. The Top Layer IDSB can filter the traffic by IP address and/or the type of application, thus enabling the monitoring sensors to be optimized. In addition, the Top Layer Balancer can create "carbon copies" of either the whole or portion of the traffic, which can be delivered to different sensor groups. This functionality is very useful for delivering the same traffic to two different sensors, such as a network IDS and a network analyzer, and it allows side-by-side comparisons. Because of its versatility, the Top Layer IDSB can also be used to simultaneously test the performance and functionality of various sensors and determine which will work best in your environment.

Intelligent Load Balancing Enables Scalability of Monitoring Solutions

Many monitoring sensors have trouble handling high amounts of traffic. Faced with this kind of overload, these sensors begin discarding traffic without checking it for attacks – a sure recipe for disaster. The Top Layer IDSB can be used to load balance the traffic to multiple sensors. Some balancing devices use "packet" based technology, balancing the traffic by looking at each packet and distributing the traffic to the various sensors. The problem with this approach is that you might end up with part of a flow going to one sensor, and the rest going to a different one. Since most sensors monitor traffic by looking at the whole flow, this will cause the sensor to malfunction and produce erratic results. The Top Layer IDSB is a stateful flow-based device, which load balances the traffic based on the flows (conversations between hosts on a network). The relationship between a packet and a flow as it relates to the communication between two systems, can be compared to the conversation between two people. A packet represents a word or phase in the conversation, whereas a flow represents the whole conversation.

High Availability by Adding Monitoring Sensor N+1 Redundancy

With a typical monitoring deployment, each sensor is installed singly, monitoring a separate portion of the network. When a sensor fails, attacks or intrusions on the portion of the network monitored by that sensor are missed.

The Top Layer IDSB distributes traffic across a group of sensors. If one monitoring sensor in the group fails, the remaining sensors pick up the load without impacting the monitoring operation.

Complete Network Coverage in Asymmetrically Routed Networks

In networks where asymmetric routes are present, placement of monitoring sensors creates an even more challenging problem. To be effective, a sensor needs to see the entire data flow between any two end points. When traffic enters via one route and leaves via another, the sensor will only see half of the communication, and a serious attack may go undetected, or protocol anomalies may be falsely reported.

The IDSB addresses this issue by using patented technology that matches both halves of the communication before passing the traffic to the sensor — providing complete network coverage.

Compatibility with Network Analyzers, Network IDSes, VoIP Recorders, Forensics, Content Inspection Engines, Rmon Probes, Network Detection Systems, and More

Almost all monitoring devices can see all the network traffic on the segment regardless of the source or destination address — this is termed promiscuous. The Top Layer IDSB has been tested and can be used for aggregation, filtering, and load balancing of traffic for any monitoring device that works in promiscuous mode.

Easy to Deploy and Use

The IDSB's Web Management Interface and configuration wizard makes the product simple to install and configure, and easy to use. Typically it takes less than fifteen minutes from beginning to end of installation.

IDSB Features

- *Aggregation of traffic.*
- *Filtering by IP address and application.*
- *Intelligent load balancing.*
- *Flow Mirror™ to intelligently distribute traffic in full context.*
- *Policy-based traffic distribution considers both the type and the source of the traffic.*
- *Wizard-based configuration, easy to use and deploy.*
- *802.1Q VLAN tag stripping for sensors that can't accommodate them.*
- *Flow Mirror traffic to multiple simultaneous groups to accommodate different types of sensors.*
- *Kill/reset packet forwarding.*
- *Preserves original MAC address information for Chain-of-Evidence forensics.*

"This is a great product! It is not very often that you come across a high-tech product that does exactly what it is supposed to do, and is very easy to use. I had it up and running the way I wanted within 30 minutes, pretty much without reading the documentation."

— Mike Iglesias

Intelligence Distribution System Balancer (IDSB)

Top Layer IDSB Family: Port Configurations

AS3531:
(12) 10BASE-T/ 100BASE-TX ports

AS3532:
(12) 10BASE-T/100BASE-TX ports
(2) 1000BASE-SX ports

TL4508:
(8) 10BASE-T/100 BASE-TX ports
(4) 1000BASE-SX ports
(4) GBIC ports (can either be 1000BASE-SX, 1000BASE-LX, or 1000BASE-TX)

Technical Specifications

The following table lists the system unit's technical specifications and compliance information.

Parameter	3500 Model Specifications	4500 Model Specifications
Physical Dimensions	Height: 6.5 cm (2.55 in) Width: 43.8 cm[1] (17.25 in) or 48.6 cm[2] (19.13 in) Depth: 33 cm (13 in) Weight: 5 kg (11 lbs)	Height: 8.8 cm (3.47 in) Width: 43.8 cm (17.25 in) Depth: 45.7 cm[3] (18 in) or 49.5 cm[4] (19.5 in) Physical Weight: with one power supply: 10 kg (22 lbs) with redundant power supply: 12 kg (26 lbs) Power Supply Weight: 2 kg (4.4 lbs)
Environmental Operating Temp Non-operating Temp Relative Humidity	 0°C to 40°C (32°F to 104°F) -25°C to 70° C (-13°F to 158°F) 5% to 95% non-condensing	 0°C to 40°C (32°F to 104°F) -25°C to 70° C (-13°F to 158°F) 5% to 95% non-condensing
Compliance to Safety	UL 60950, 3rd Edition CSA C22.2 No. 60950, 3rd Edition EN 60950/IEC 60950, 3rd Edition	UL 60950, 3rd Edition CSA C22.2 No. 60950, 3rd Edition EN 60950/IEC 60950, 3rd Edition
Compliance to EMC Emissions Immunity	FCC 47 CFR Part 15 Class A; EN55022: 1998 including CISPRR 22 3rd Edition; EN61000-3-2: A1: 1998 and A2: 1998; EN61000-3-3: 1995 EN55024: 1998 including CISPR24 1st Edition	FCC 47 CFR Part 15 Class A; EN55022: 1998 including CISPRR 22 3rd Edition; EN61000-3-2: A1: 1998 and A2: 1998; EN61000-3-3: 1995 EN55024: 1998 including CISPR24 1st Edition
International Compliance Approvals	UL Listed, CUL, AS/NZS 3260, AS/NZS 3548: 1995, CE, FCC Class A, BSMI CNS: 13438 Class A, VCCI Class A Common Criteria EAL2	UL Listed, CUL, AS/NZS 3260, AS/NZS 3548: 1995, CE, FCC Class A, BSMI CNS: 13438 Class A, VCCI Class A Common Criteria EAL2
Power Requirements AC Input Voltage AC Input Line Frequency AC Current Amps	 100 to 240 VAC Autoranging 50 to 60 Hz 1.0 A	 100 to 240 VAC Autoranging 50 to 60 Hz 3.0 A (maximum)
	1. without rack-mount brackets *2. with rack-mount brackets*	*3. Not including power supply handles* *4. Including power supply handles*

About Top Layer

Top Layer is dedicated to its role as a leading global provider of Network Intrusion Prevention Systems (IPS), developing and bringing to market network security infrastructure solutions that help commercial and government organizations protect their critical on-line assets from the losses and risks associated with cyber threats. Its family of IPS appliances is designed with “Three Dimensional Protection” that provides the most advanced protection capabilities against known and unknown attacks at the highest performance rates. Top Layer Networks is headquartered in Massachusetts, USA, with sales and support presence throughout North America, Europe, Asia, and Japan.

Top Layer™
perfecting the art of network security

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

www.TopLayer.com