

IDS:

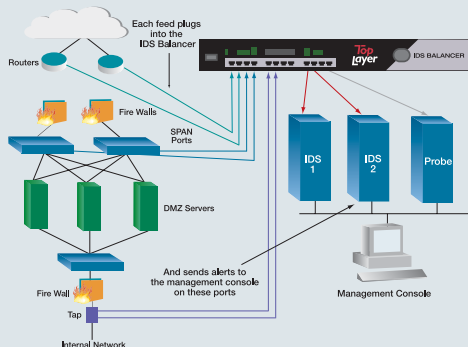
Increase network monitoring coverage while reducing cost?

Aggregation, Filtering and Load Balancing are the Answer.

Top Layer has a solution that can save you up to 80% on sensor costs while increasing your security level.

Network monitoring can get expensive!

To identify attacks and intrusions, security managers are asked to monitor 100% of their network, using network Intrusion Detection Systems (nIDS) and other monitoring systems. One way to do this is 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.) However, this approach comes with 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 IDS Balancer provides a cost-effective solution by aggregating multiple network segments, providing for redundancy, and scalable growth, as future traffic loads increase. The IDS Balancer also allows for other devices including Rmon probes, sniffers, and any vendors' nIDS systems to look at traffic.

The results can be catastrophic, since missed attacks and intrusions can cause millions of dollars in damages to the organization. Fortunately, there is an alternative solution which provides superior monitoring coverage at a fraction of the cost.

Aggregation can save up to 80%

Aggregating the traffic from multiple network segments provides immediate savings, since fewer nIDS sensors are required to examine the traffic. For example, if you want to monitor 6 GigE segments you can:

- use 6 GigE nIDS, or,
- use one "aggregation device"

(IDS Balancer) and one GigE nIDS.

In this simple example, the 6 to 1 aggregation saves 80% of the nIDS cost, while

providing the same coverage. Top Layer's family of high performance ASIC based IDS Balancers provides huge savings by offering aggregation for both Fast Ethernet and GigE networks.

Filtering and carbon copies

It is very common for enterprises to use two different types of IDS sensors, each one optimized for different types of traffic. The Top Layer IDS Balancer can filter the traffic by IP address and/or the type of application, thus enabling the nIDS sensors to be optimized. In addition the Top Layer IDS 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 an nIDS and a network analyzer, and it allows side-by-side comparisons.

Intelligent Load Balancing

When the amount of data to be monitored exceeds the sensor's capacity, the Top Layer IDS Balancer can be used to load balance the traffic to multiple sensors. This approach also offers N+1 sensor redundancy. 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 IDS sensor, and the rest going to a different one. Since IDS sensors monitor traffic by looking at the whole flow, this will cause the IDS to create a false alarm. The Top Layer IDS Balancer 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 phrase in the conversation, whereas a flow represents the whole conversation.

For IDS, Network Analyzers, Forensics, Rmon probes, and more.

Almost all monitoring devices (nIDS, Network Analyzers, Forensics Systems, Rmon probes and other devices) can see all the network traffic on the segment regardless of the source or destination address — this is termed promiscuous. The Top Layer IDS Balancer can be used for aggregation, filtering, and load balancing of traffic for any monitoring device that works in promiscuous mode.

The Top Layer IDS Balancer provides a true ROI, while helping you increase your network monitoring coverage.

There are several ways that you can capitalize on the benefits of using an IDS Balancer, such as:

- Reduce your capital, maintenance, and operations expenditure for all types of network monitoring solutions.
- Simplify the management of your monitoring solutions.
- Enable simultaneous monitoring for different applications (such as security and network troubleshooting).
- Scale your monitoring solutions, and enable the sensors to sustain the volume of traffic to be monitored.
- Add N+1 redundancy for your monitoring sensors.

Call Top Layer Networks at 508-870-1300, email at consult@toplayer.com, or register to attend an Educational Webinar on "Maximizing nIDS Performance and ROI" at www.TopLayer.com

**Top
Layer**

perfecting the art of network security