

**Global Consultancy Turns to Top Layer Networks for Checks and Balances****Solution Overview**

**Profile:** One of the largest consultancies in the world provides accounting services (audit, tax, advisory) and consultation projects (enterprise software implementations) to companies of all sizes, with customers in most countries. The company provides back office and administrative functions to its clients, and with access to confidential financial and competitive data must guarantee protection of its information and that of its clients from outside threats.

**Challenge:** The challenge for this consultancy was that when an intrusion or cyber threat exploded across its vast network, it was difficult to pinpoint infected hosts and sift through its extensive network. The existing Intrusion Detection Systems (IDS) that the company was using were overwhelmed due to the huge amount of traffic. It needed a solution that would help scale the existing IDSes, and monitor and analyze the traffic load, without the risk of missing intrusions and attacks. The company also wanted to add redundancy to its IDS solution and get the flexibility of adding additional monitoring sensors without disrupting the existing infrastructure.

**Solution:** The consultancy turned to Top Layer Networks due to the reputation of its Intelligence Distribution System Balancer (IDSB) product line. Initially the consultancy deployed four IDSBs to manage 28 network security monitoring sensors.

The IDSB allowed the IDS solution to be scaled and optimized by:

- Connecting to the various network segments via taps.
- Aggregating the traffic.
- Filtering the traffic as needed, based on user-configured parameters.
- Load balancing the traffic to multiple IDSes.

The consultancy is currently moving to the second phase of its rollout and is adding additional Top Layer IDSBs into its network.

**Benefits:** The IDSB enabled the consultancy to achieve non-stop Intrusion Detection monitoring, ensuring that all intrusions and attacks are detected and appropriate action taken immediately.

The Top Layer IDSB ensured that the consultancy's security infrastructure is able to provide unrelenting protection from the continuous onslaught of worms, viruses and other cyber threats – and able to do so without impacting network availability or speed.

The phased approach provided the consultancy with a bigger bang for its IT buck and enabled the IDSB technology to prove itself in the network. Moving to Phase II of the IDSB deployments, the consultancy will deploy more IDS probes across offices and within the data center for additional protection, with expectations that its satisfaction will even exceed that of Phase I.



# CASE STUDY - INTELLIGENCE DISTRIBUTION SYSTEM BALANCER

## Full Case Study

One of the largest consultancies in the world provides accounting services (audit, tax, advisory) and consultation projects (enterprise software implementations) to companies of all sizes, with personnel and clients in most countries. The company provides back office and administrative functions to its clients and in handling such sensitive financial and confidential data must guarantee protection of its information and that of its clients from outside threats.

With its global reach and extensive network, and with hundreds of thousands of devices accessing the network, security is a definite challenge and of utmost importance due to the sensitive financial and proprietary information that the company deals with on a daily basis. Access to this information for approved employees is critical to the company's continued success, and network availability and security around the globe are keys to ensuring that access.

The challenge for this consultancy was that when an intrusion or cyber threat exploded across its vast network, it was difficult to pinpoint infected hosts and sift through its extensive network. It needed a solution that would help monitor and analyze the traffic load effectively as the company's IT department worked through the network to fix any damage from each security event and handle the gigabit speeds the network demands.

## Impressing an Informed IT Department

The consultancy's IT staff is a very technically-adept team, yet sought a vendor who would support them when needed. The team keeps a close eye on the security products market, continually monitoring various technologies so they understand what is new and worth considering. When determining its needs for traffic balancing requirements, the team had its short list of vendors to evaluate. The consultancy's IT staff also knew it had the following requirements to satisfy:

- Needed 10/100/gigabit load balancing
- Lots of devices with different functions for a balancer to work with
- Needed to separate traffic by protocol or load balance.

The consultancy turned to Top Layer Networks due to the reputation of its IDSB product line and its ability to handle multi-gigabit speeds effectively. To that end, the IT Manager concluded, "Top Layer had the most mature and proven technology in the space to meet our needs, and the IDSB met all the claims that Top Layer made. We used it in a variety of ways, and didn't find any function that we needed that it didn't offer. The IDSB was a clear choice.

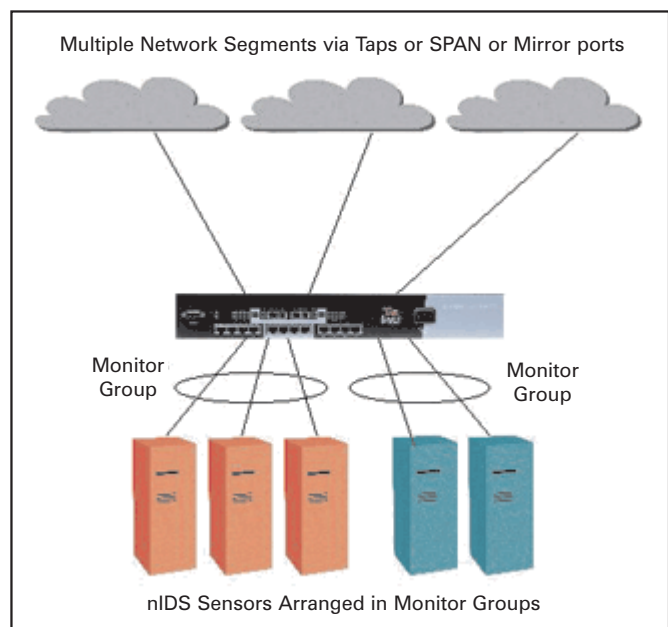
A key benefit that Top Layer brings to the consultancy is its commitment to client service and satisfaction. Top Layer brought in sharp engineers who saw flaws in our network planning. In one instance, we were evaluating our taps and traffic patterns. Top Layer presented an argument that clearly proved we were mistaken in our approach and that we didn't have a clear understanding of the number of taps we had in place – but we do now. You don't find that combination of intelligence and commitment often from vendors with as many customers as Top Layer has on its roster."

## Checks and Balances across the Networks

With its vast network, the consultancy deployed four IDSBs to manage 28 security appliances in one segment as the first step in a phased approach – so the technology could prove itself before being deployed across the entire network. The solution worked remarkably and now provides the consultancy with the analysis and correlation needs to identify activity across its network and properly deal with events or questionable traffic.

In one instance – an early encounter with MS Blast that previously would have taken up much of the consultancy's network resources – Top Layer's IDSB enabled the consultancy to maximize the value of its entire IDS system. This allowed the company to continue to operate without losing capacity or even a single packet of data.

As noted previously, the consultancy has a number of functions it requires of its load-balancing technology investments. One is to help with device upgrades due to the pure volume of devices on the network. The IDSB helps the consultancy execute its upgrades across network devices without losing functionality or protection – an added benefit that fulfills the consultancy's greater goal of continuous, effective security.



# CASE STUDY - INTELLIGENCE DISTRIBUTION SYSTEM BALANCER

For the consultancy, the IDS Balancer's patented Flow Mirror technology lets the IT team split the network traffic load to analyze it while not impacting traffic flow – a “huge value” according to the IT Manager. The company is utilizing the Top Layer products for its gigabit links that converge in front of its data center, providing the following functions:

- Distribution of traffic
- Serve as a primary and secondary path of gigabit network, so that traffic still comes into IDS sensors in the event of a failover
- Redundancy based on load shifts
- Enables non-stop IDS monitoring with the ability to adjust IDS units without loss of monitoring – whether to replace or upgrade them – because of its ability to switch traffic loads and not miss packets.

## Finding Needles in the Haystack

To optimize the consultancy's intrusion detection systems and ability to protect its clients and online assets, the organization employs a number of devices and probes to work with the Top Layer Balancer for complete analysis of traffic and security events. With the devices working together, the IDSB enables the consultancy to capture, log, analyze, and store days' worth of information, whereas other solutions only have the capacity to handle a few minutes. The monitoring function the IDS Balancer provides is key, as it shows glimpses of network activity that the consultancy would otherwise not be privy to during daily operations.

“This aspect has been extremely helpful. The Top Layer Balancers let us spread the traffic load and analyze it on the back end, effectively helping us identify troubled hosts and to set up triggers off of IP addresses and probes. With the ability to continuously capture traffic and trace over multiple days, we're able to find multiple needles in the network haystack and correct otherwise lingering and problematic situations,” stated the IT Manager.

The Top Layer Balancer ensures that the consultancy's security infrastructure is able to provide unrelenting protection from the continuous onslaught of worms,



viruses and other cyber threats – and do so without impacting network availability or speed.

## Encouraging Cross-Organizational Traffic Analysis

The flexibility of the devices also enables the IT Manager and his team to sell the IDSB's use into other business units for their traffic analysis and monitoring needs. Because the IT Manager did not use all of the ports on the IDSBs, other teams are able to plug into the open ports with various devices – Sniffers, Flukes and application performance monitoring devices – as needed without the need for expensive multi-port taps. The IDS Balancers can pre-filter traffic for other business units because of the spare ports available; this is key to aligning support for the consultancy's overall network monitoring and security goals.

Additionally, the IDSB's Flow Mirror technology provides the consultancy with the ability to plug devices in and out without disturbing the network. This means that as they install more IDSBs, there is no need to purchase costly multi-port taps. Instead, they can just use IDSBs with more ports, with the free ports available for other business units' traffic analysis and monitoring.

The phased approach provides the consultancy with a bigger bang for its IT buck, and enabled the IDSB technology to prove itself in the network. Moving to Phase II of the Top Layer Balancer deployments, the consultancy will be deploying more IDS probes across offices and within the data center for additional protection. The success the IT department realized with the IDSB in Phase I has made the shift to Phase II much easier to sell to company executives.

Finally, and most important, the security the IDSB provides helps the consultancy support the level of trust that practitioners promise to clients.