Net Optics xBalancer™ and McAfee Network Security Platform Integration

Solution Brief

Under the McAfee SIA Partner Program, Net Optics is integrating its xBalancer with the McAfee Network Security Platform (NSP). This partnership will enable mutual customers to realize the benefits of load balancing while achieving an unprecedented level of security and availability in their inline monitoring and access efforts.

Solving the Risk of Overburdened Tools: Load Balancing with the Net Optics xBalancer and McAfee Network Security Platform (NSP)

Many organizations now rely on inline monitoring tools to prevent attacks, ensure network protection, prevent information loss, and achieve regulatory compliance. With 10 Gigabit network links increasingly deployed to carry mission-critical business applications and data, voice, and video traffic, these inline security devices—Intrusion Prevention Systems (IPSs), Data Loss Prevention (DLP) devices, Web Application Firewalls (WAFs), Database Activity Monitors, (DAMs), Next-Generation Firewalls, and Application Performance Management tools—can become oversubscribed and lose the ability to perform effectively. Adding to the pressure, tools are becoming more complex and more demanding of processing power. The impact of this crisis raises a severe risk to network security and performance.

Postponing Expenses by Optimizing Tool Performance

Upgrading to a new generation of higher-performance tools may be ideal, but for business and other concerns this may not be a practical course at present. Fortunately, a quick, ingenious and cost-effective solution already exists to avoid oversubscribing inline monitoring tools. Network architects are increasingly turning to load balancing as a way to multiply tool throughput without the effort of locating, qualifying, and deploying new tools—not to mention incurring the costs of developing new procedures and retraining staff.

Load Balancing: A Cost-Effective Strategy to Relieve Oversubscription of Inline Monitoring Devices

In the case of an out-of-band tool becoming oversubscribed, it's a fairly straightforward task to replicate the tool and load-balance traffic. However, load balancing inline tools raises the stakes and presents unique challenges, since these can interfere with network traffic or even bring down a business critical link.

Because they deal with bidirectional traffic flows, conventional monitoring load balancers may not be able to meet inline load balancing requirements. To resolve these issues, Net Optics developed xBalancer—purpose-built for inline load balancing. xBalancer stands out among other load-balancing approaches for a number of innovative capabilities, including its linear scalability and superior cost-effectiveness. xBalancer enables replication of existing tools, with traffic load-balanced so that tools operate in parallel. This scheme enables two tools to perform twice the work; three tools to perform three times the work, and so forth. Scaling is linear, making the solution ideally cost-effective amid doubling and even quadrupling traffic volumes.

Solution Brief

Architecting for Optimal Load-Balancing Performance

Seven criteria must come together to ensure that this advanced load balancing technique works effectively.

1. Load balancing must be flow coherent, with symmetric forwarding. A "flow" refers to a stream of information passing between two endpoints, similar to a conversation between two people. All packets with the same source/destination address pair constitute a flow. In practice, flows may be defined by various criteria, depending on the application.

   In order for an IPS to make sense of traffic, it must "hear" all of it. A flow-coherent load balancer ensures that all packets in a flow are directed through the same tool, not spread across several tools. The load balancer accomplishes this by examining the source and destination address pair, and assigning all packets with like addresses to the same tool.

   Symmetric forwarding means that the flow moves through the tool in two directions, just as part of a conversation goes from you to the other person, while the rest returns from that person to you. A load balance with symmetric forwarding ensures that both directions of a flow are sent through the same IPS, so it can completely understand what is going on.

Net Optics xBalancer meets this criterion by performing flow-coherent inline load balancing with symmetric forwarding—ensuring that both directions of conversation flows are always directed through the same tool.

2. The load balancer must accommodate different definitions of flow. In many cases, a flow can be identified as all packets having an identical "5-tuple" (the five pieces of information that comprise each unique bidirectional TCP/IP connection). A 5-tuple must be specific to each connection in order to ensure that data goes to and from the correct places. For example, a 5-tuple may consist of the IP address pair, the TCP/UDP port pair, and the protocol. However—for some applications, a different definition of flow must be used. For example, non-IP traffic does not have IP addresses or ports, so it is better to define flows by the MAC address pair.

Net Optics xBalancer meets this criterion by supporting the 5-tuple definition of flows using the IP address pair, the TCP/UDP port pair, and the protocol, as well as allowing configuration to any mixture of those field plus MAC addresses, ethertype, and VLAN.

3. A load balancer must have filtering capabilities. Sending only the traffic of interest to the appropriate tool can alleviate oversubscription. For example, an IPS may need to look only at HTTP traffic—or it may be useful to exclude ARP traffic and allow it to bypass the IPS, saving IPS processing cycles.

Net Optics xBalancer meets this criterion by providing 4,000 layer 2-4 filters, plus a user-definable field that can reach all the way to layer 7 in some cases, enabling flexible and powerful selection of traffic of interest.

4. A load balancer should include aggregation and regeneration capability, because it may need to bring in traffic from multiple links or generate multiple copies of it. In fact, it should be able to "tool share," where it aggregates traffic from multiple links but logically keeps the traffic streams separate, so links act independently but share the same pool of monitoring tools. This

arrangement leads to greater efficiency than dividing up the tools into separate pools on each link, because the aggregate processing power of all the tools is available to whatever devices are running peak traffic loads from moment to moment.

Net Optics xBalancer meets this criterion with 24 SFP+ ports that can be configured in any port mapping—any to any, one to any, or any to one. It can combine traffic from multiple network links in straightforward aggregation, or in tool-sharing mode where the traffic on the links is kept separated.

5. The load balancer needs adequate bandwidth—not only to support immediate needs, but to accommodate growth. If you deploy a load balancer with 10 Gbps bandwidth today, and use it to balance traffic to two tools capable of processing 5 Gbps each, what happens when the traffic volume exceeds 10 Gbps? If the load balancer has plenty of headroom, you can simply add another copy of the tool and keep going, without interrupting traffic at all. If it doesn't, you'll need to deploy a new load balancer as well, probably needing to take down the link for a period while the unit is installed.

Net Optics xBalancer meets this criterion because its 480 Gbps backplane is totally non-blocking, even with 360 million 64-byte packets per second—the true measure of a switch's throughput. This is enough bandwidth to load balance traffic aggregated from six 10 Gbps links to a pool of six 10 Gbps inline monitoring tools.

6. The load balancer must provide 100 percent traffic visibility, just as if the IPS were deployed directly inline. The load balancer must not drop packets—even packets having CRC errors—under full-rated load.

Net Optics xBalancer meets this criterion because the backplane is totally non-blocking, so no packets are dropped even when the ports are all fully loaded.

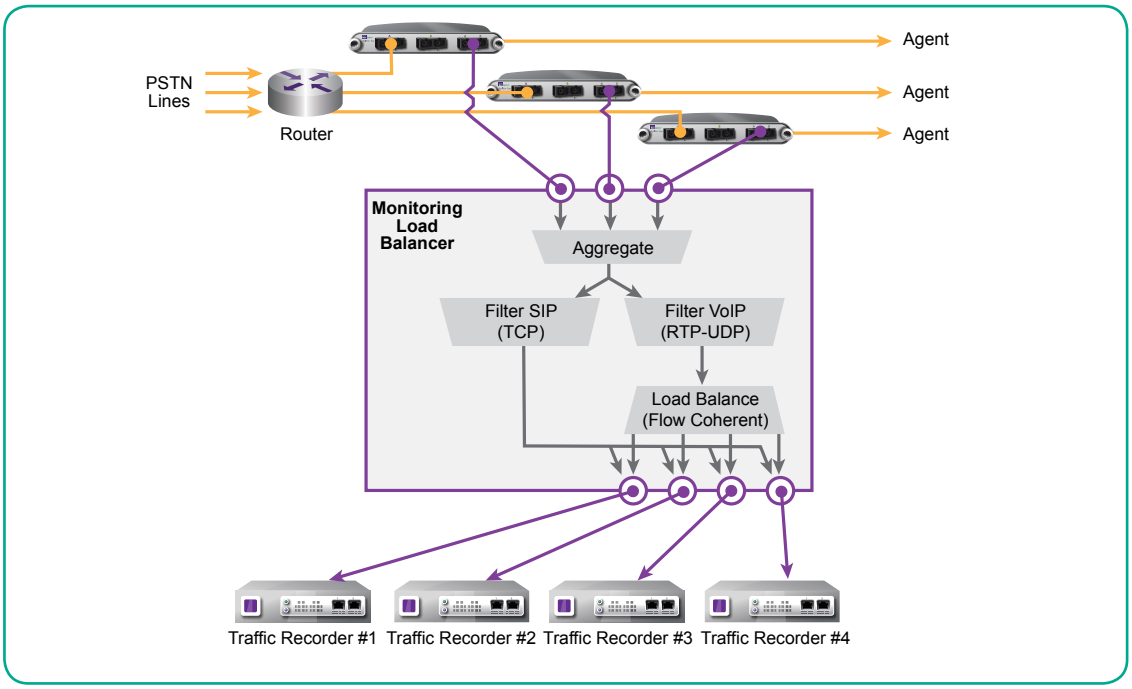
7. The solution must not introduce a single point of failure, which could have a severe impact on the network's reliability. Remember, if you deploy four copies of an IPS, the likelihood that one of them will fail is quadrupled. Fortunately, a monitoring load balancer can actually increase the overall network reliability if it supports N+M tool redundancy, where N tools are active and M tools act as warm spares, to which the load balancer can instantly transfer traffic if an active tool fails.

   The load balancer can also support other high-availability modes such as link-state awareness; in this case, when a tool goes down, traffic is automatically redistributed among the remaining active tools. To prevent the load balancer itself from becoming a single point of failure, it should support high availability modes that allow failover to a redundant load balancer.

Net Optics xBalancer meets this criterion with its ability to be configured for N+M tool redundancy, link-state awareness, device failover, and a variety of other High-Availability topologies.

Solution Brief

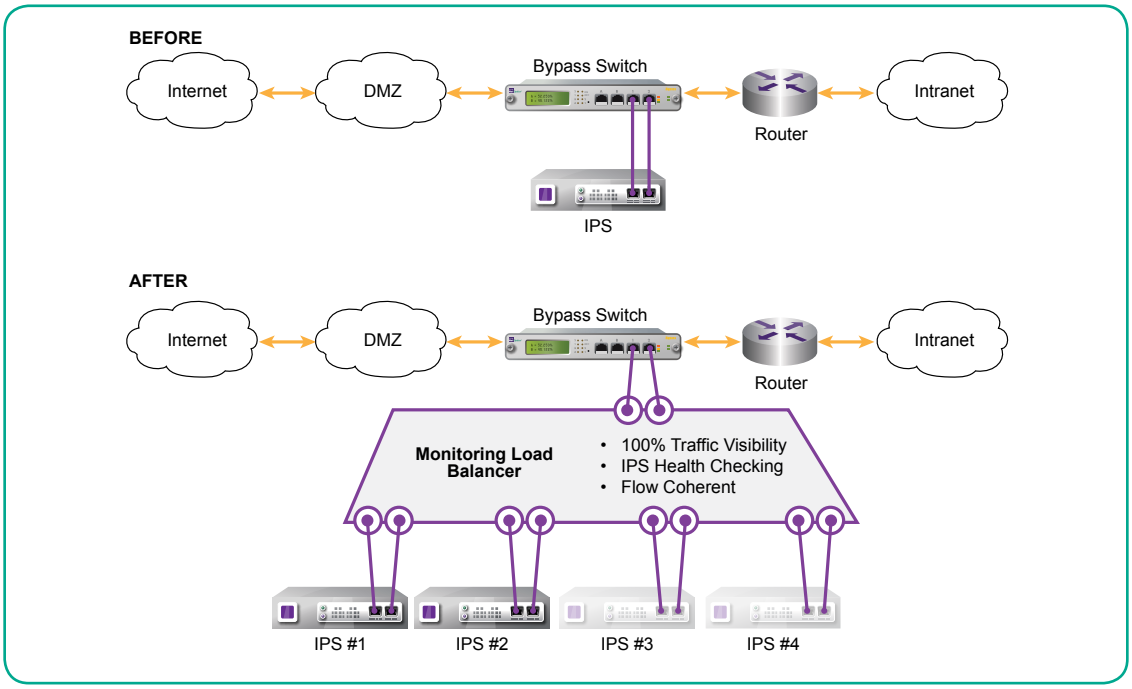
Use Case #1: xBalancer performing load balancing in a call center environment



A company must be able to pass links with the actual calls and bring these to a traffic recorder. The load balancer must be flow-coherent so that the entire traffic flow goes to the same recorder (the customer talking to the agent and the agent talking back to the customer). Here, the load balancer is able to recognize the traffic and send it to the same traffic recorder.

Solution Brief

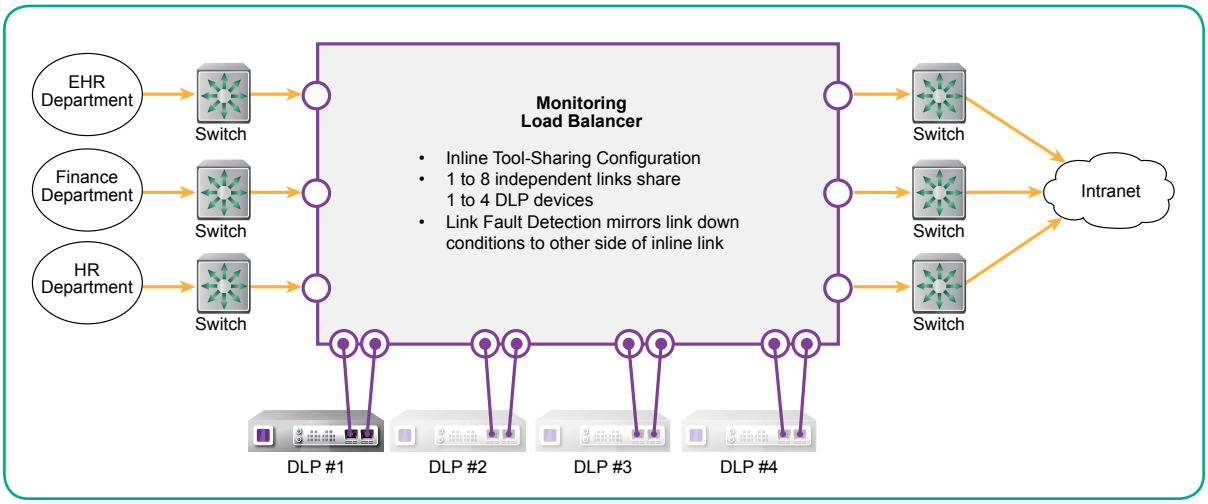
Use Case #2: Organizations using IPSs for reasons of network security



In this case, traffic must flow in through the IPS and into the company Internet so it can both analyze traffic and block inappropriate traffic. You can connect an IPS with a bypass switch from Net Optics (or other vendor) to create a fail-safe connection. If the IPS loses power and can't pass traffic, the Bypass switch clicks over into open mode and bypasses the IPS. However, as traffic gets faster, IPSs can run out of steam and get oversubscribed. High-performing IPSs can cost up to a half million dollars! And with mission-critical traffic to protect, load-balancing is a more pragmatic approach. Monitoring load balancers can also generate a heartbeat packet through each IPS, so they know if it has failed—in both directions. If it does fail, you can bypass the IPS or move traffic to a hot standby or more than one. It's important to plan for future capacity as traffic increases.

Solution Brief

Use Case #3: Dedicating tools to specific links can promote inefficiency and lead to IPS oversubscription



In some cases, tools are hardly being used at all, and for higher bandwidth requirements one can opt to share tools among links. In this case, a health clinic needing a Data Loss Prevention System for purposes of HIPAA compliance can also use it in finance and HR. In this way it is deployed more efficiently and enables the health clinic to gain a better ROI.

Net Optics xBalancer™ and McAfee Network Security Platform Integration

Solution Brief

In Summary

Load balancing with xBalancer can be the ideal approach for monitoring tools to avoid oversubscription. The solution is often the most cost-effective way to increase ROI on current tools. Organizations save CAPEX if they have spare tools that they can use in parallel to avoid investing in pricey new high-throughput tools. Or perhaps investing in a high-throughput tool might free up lower-performing tools that can be put to use for load-balancing. Load balancing also gives companies extra time to put off the investment in high-priced tools and yet still enjoy the ability to monitor just as efficiently using a number of current tools. This approach also saves on operations costs because the staff already understands how to use the tool and does not need additional training. Monitoring tools, combined with load-balancing solutions offer 100 percent visibility, flow coherence and the ability to tool share—all at a very practical cost.

For further information about xBalancer and all of Net Optics' Load Balancing solutions:

http://www.netoptics.com
Net Optics, Inc.
5303 Betsy Ross Drive
Santa Clara, CA 95054
(408) 737-7777
info@netoptics.com

Customer First!