WHITE PAPER

Load Balancing with McAfee Network Security Platform

Optimizing intrusion prevention system performance

WHITE PAPER

Load Balancing with McAfee Network Security Platform

Optimizing intrusion prevention system performance

McAfee® Network Security Platform is a uniquely intelligent security solution that discovers and blocks sophisticated threats in the network by using advanced detection and emulation techniques. This next-generation hardware platform scales to speeds of more than 40 Gbps with a single device to meet the needs of demanding networks. For larger enterprise environments that require additional performance, an individual intrusion prevention system (IPS) can be replaced with a cluster of IPS devices, easily scaling to achieve the desired throughput. In this scenario, network traffic is load balanced across the sensor cluster for fast, efficient inspection. In addition, multiple IPS sensors can be easily managed via a single pane of glass for efficiency. This paper describes several load balancing techniques to optimize performance across the sensors.

Key Advantages

- Scalable solutions for larger enterprise environments
- Flexible load balancing options optimize performance and reduce costs
- Easily manage multiple IPS sensors via a single pane of glass

Basic Configuration Considerations

The sensor needs to maintain flow information for proper IPS processing. This means all packets belonging to one flow should go to the same sensor. External devices need to be configured to ensure this condition is always satisfied. For example, all packets with the same source or destination address pair should pass through the same sensor.

IPS devices can be clustered to achieve throughput that exceeds that delivered by an individual device. Total throughput is limited by the capacity of the external devices, such as the load balancer or the switch.

Basic terminology

- **Link Aggregation:** There are various ways to increase individual-link bandwidth, like traffic policing and WAN optimization. Along with this, there are techniques to combine the bandwidth of all links, also known as Link Aggregation. As the name implies, it combines more than one network link logically in parallel to increase bandwidth between network devices. This may also be referred to as trunking.

Connect With Us

- **EtherChannel:** Cisco's proprietary aggregation scheme is built upon standards-based 802.3 Ethernet. This technology is composed of several Gigabit Ethernet links and is capable of load balancing traffic across those links. Unicast, broadcast, and multicast traffic is evenly distributed across the links, providing higher performance and redundant parallel paths. When a link fails, traffic is redirected to the remaining links within the channel without user intervention and with minimal packet loss. Load-balancing policy can be based on media access control (MAC) address (L2), IP address (L3), or port number (L4).
- **Link Aggregation Control Protocol (LACP):** This is the IEEE standard (defined in IEEE 802.3ad) for achieving link aggregation across multiple network links between two switches.
- **Port Aggregation Control Protocol (PAgP):** Cisco's proprietary protocol helps in automatic creation of EtherChannel links. PAgP packets are sent between EtherChannel capable ports to negotiate EtherChannel creation, but there are restrictions. Bundles aren't formed with dynamic VLAN-configured ports. In addition, all ports should be on the same VLAN and should operate at the duplex. Modes for PAgP include Off, Auto, and Desirable.

Load Balancing Solutions with McAfee Network Security Platform

Using a third-party load balancer

Third-party load balancers are supported with McAfee Network Security Platform. A cluster of McAfee Network Security Platform sensors can be used between properly configured load balancers on either side of IPS appliances to scale beyond single sensor limits. All the network-level functionalities are available, including stateful failover (Figure 1). Throughput of this solution depends on the load balancer selected by the customer. With use of a McAfee Network Security Platform NS-9300 sensor, in conjunction with a load balancer, throughput can scale above 300 Gbps. Load balancers need to be configured to ensure packets belonging to a flow are always received by the same sensor.

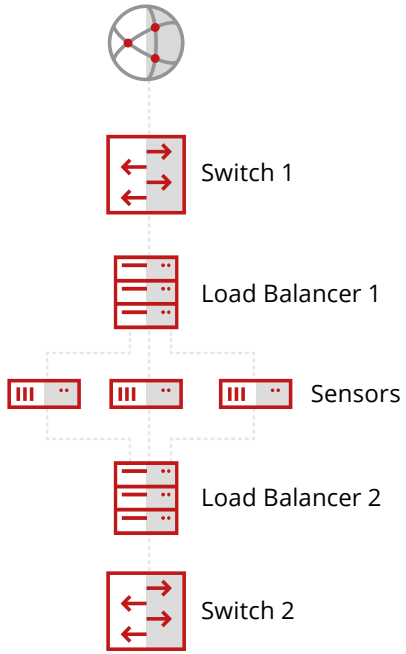

Figure 1. Load balancer configuration.

Configuring a firewall

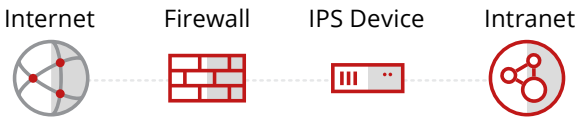

Figure 2. Inline IPS configuration residing behind a firewall.

Let's look at various forms of firewalls: application-based, packet-based, application proxy, and layer 2 firewalls. Since an IPS requires flow state to be maintained, application-based firewalls are more suitable here. The firewall can track all the IP packets bi-directionally to ensure that only packets from a valid session are passed through. Again, firewalls need to be configured to ensure that traffic pertaining to a flow are received by the same sensor and to distribute traffic evenly across different sensors. This means asymmetrical routing should not occur once flow connections are established through the sensors.

External Switches and McAfee Network Security Platform Cluster

OEM third-party switches

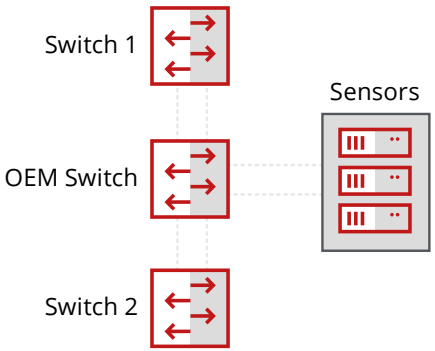

Figure 3. OEM switch configuration.

In this solution, a third-party switch can run as a load balancer by executing a load balancing algorithm and evenly distributing traffic across the sensors connected to the switch. Several IPS devices can be connected to the switch and are limited by port pair availability. This design is scalable and provides high port density.

Link aggregation of network switches

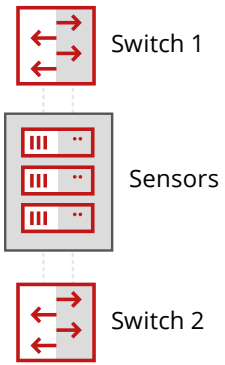

Figure 4. IPS sensors directly connected to switches.

Another approach is to configure switches so they are directly connected to the IPS devices. This requires configuring of the switches connected to the sensors to enable link aggregation, achieving both bandwidth increase and link fault tolerance.

Summary

The McAfee Network Security Platform delivers scalable solutions to meet the needs of enterprise organizations. For larger enterprise environments, individual IPS systems can be replaced with a cluster of IPS devices to achieve the desired throughput. In this scenario, multiple load balancing options are available to ensure that network traffic is optimized for cost-effective, fast inspection and data protection.

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com