SOLUTION BRIEF

Load Balancing Reduces Costs While Increasing Reliability

Deployment Scenario: Inline and Out-Of-Band Visibility

In today's 24x7, "always on" world, the company's data network must be as reliable as possible. Otherwise, revenue reduction and productivity losses are not only possible, but probable. This includes the inline security and monitoring tools which can become a single point of failure. One option to increase network reliability is to deploy n+1 survivability using network packet brokers (NPBs) to create load balancing for those devices. This provides a cost-effective alternative to full component redundancy.

Another use case for NPB-based load balancing is to deploy it for out-of-band monitoring and security tools. Data from a 2016 Enterprise Management Associates survey shows that 32% of enterprise tools are underutilized. In this instance, load balancing is used to increase the utilization of your existing tools by pooling them and then load balancing traffic across them. This solution brief describes how to implement both capabilities.

Solution Components

- Keysight Network Packet Brokers
- NetStack

Benefits

- Reduce network risk by deploying component survivability
- Create n+1 solutions that deliver survivability at a lower cost than High Availability
- Reduce CAPEX by reducing the amount of required security and monitoring devices

Solution Overview

This network visibility solution allows you to:

- Improve inline security and monitoring tool deployments by using NPBs to load balance traffic to create an n+1 survivability option
- Create a more cost effective alternative to high availability while still improving system reliability
- Pool your resources and then load balance across them to increase tool utilization
- Perform media speed conversion of high rate data to extend the life of your existing lower rate devices

KEYSIGHT TECHNOLOGIES

What is Load Balancing?

Load balancing is the ability to take incoming traffic and dynamically spread that traffic across multiple output ports. This functionality has a couple fundamental use cases including n+1 survivability and increasing tool utilization. One of the easiest ways to deploy load balancing is to use an NPB. The NPB has the ability to split the traffic by bandwidth. For instance, incoming traffic at 40 Gbps could be distributed to either one 40 Gbps device, two 20 Gbps device, four 10 Gbps device, or some other combination of devices to process the required data.

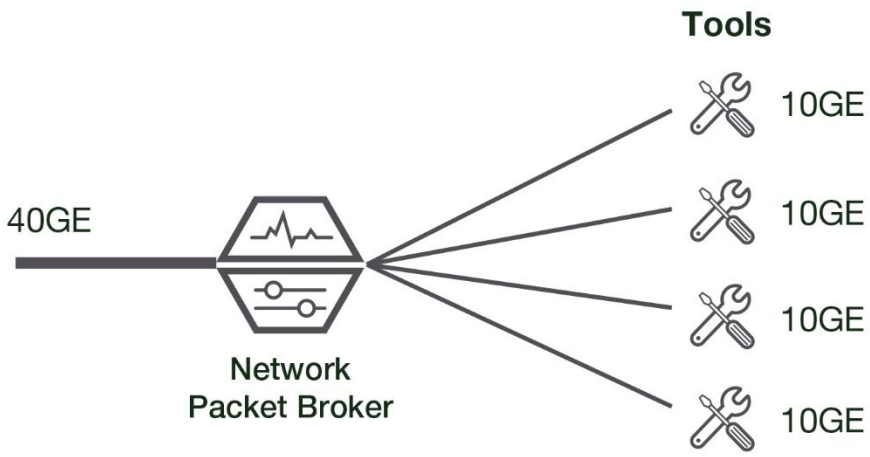

Figure 1. Load Balancing example

Security and monitoring tool survivability is often thought about in terms of fully redundant devices, especially in the case of inline deployments. However, an alternative is to implement an n+1 option for component redundancy.

Achieving N+1 Survivability with Load Balancing

Security and monitoring tool survivability is often thought about in terms of fully redundant devices, especially in the case of inline deployments. However, an alternative is to implement an n+1 option for component redundancy. In this situation, you don't have a complete set of spare units waiting in a standby mode to take over should the primary equipment fail, just one or two. At the same, you don't have to spend double the costs for a redundant solution like you do with full redundancy. In addition, this n+1 solution can be applied to both inline or out-of-band architectures, depending upon your needs.

In this scenario, security and monitoring tools are allocated to a specific port group on a network packet broker. Based upon the necessary criteria, data traffic is then spread evenly across the port group. Should a heartbeat message (for inline solutions) or a Link Failure message (for out-of-band) solutions be received, the data is spread out across the remaining tools in the port group by the packet broker. Once the device becomes available again, the NPB will resume routing traffic to it.

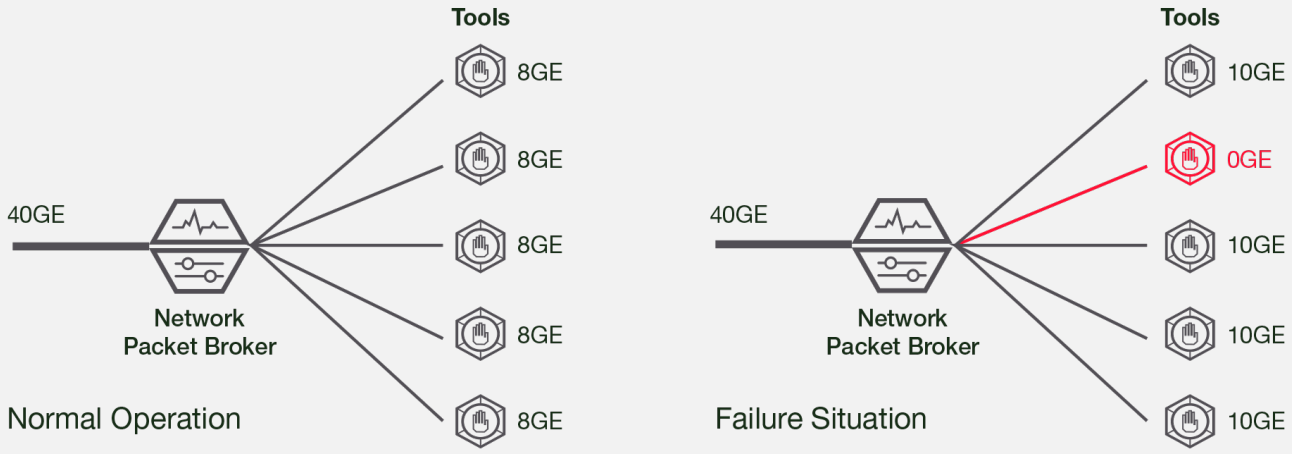

Figure 2. N+1 survivability with Load Balancing

For example, let's say you need four IPS appliances to process your inline network traffic. In this case, you would add a fifth IPS. The packet broker would then load balance the traffic across all 5 IPS appliances. Should any one of the appliances fail, the packet broker can load balance the full load across any of the remaining four IPS'. This provides a reasonable level of survivability at a fraction of the cost of a fully redundant system.

If you would like to have more survivability, like an n+2 situation, you can do that as well—all the way up to a fully redundant set of tools. It just depends upon the level of risk you feel comfortable with and your budget.

Increasing Tool Utilization While Decreasing Costs

There are a couple clear examples of how load balancing can help most enterprises decrease costs. The first example is media speed reduction. Network traffic increases, along with traffic speed increases, are a very common occurrence. But what about the monitoring impacts of the bandwidth upgrades? For instance, if you upgrade your network core from 1GE to 10GE, you will now need 10GE tools to properly monitor the network. While 10GE devices may be plentiful and cost-effective, what if you upgrade to 40GE or 100GE? There may be few, to no, monitoring tools available at those data rates. And available solutions at those data rates can be very expensive.

Packet brokers provide the aggregation and load balancing capabilities needed. Data coming into the packet broker can be broken down into lower rate streams of data and then sent to the proper monitoring devices. For instance, load balancing of 40 GE data allows you to spread the monitoring traffic across multiple 10 GE tools. Note, this obviously assumes you have enough 10 GE devices for the load. Once you implement this functionality, you can extend the life of those devices a little longer until you have enough budget to purchase more expensive tools that can handle the higher data rates. For example, you might be able to implement the network upgrade you want to this year and then purchase additional higher rate monitoring solutions later. This helps you align your capital expenditures with your technology updates.

A second scenario is to pool your tools in one location and feed them the data they need from a packet broker. Some architectures use individual devices spread out across the network. This may have some minor access advantages, but (as mentioned earlier) these devices are often underutilized which means additional and unnecessary costs. Centralization and load balancing allows you to pool your tools to increase device utilization. You can often postpone purchases of additional devices until the utilization factor reaches a high level. This allows you to postpone security and monitoring solution purchases until you have enough CAPEX budget.

Summary

Load balancing is a powerful feature of network packet brokers that can be used to increase both system availability and reliability while decreasing the costs required for additional security and monitoring tools.

Specifically, a visibility architecture with an NPB can perform the following:

- Reduce network downtime risk by deploying a component survivability option
- Provide a cost-effective alternative to full component redundancy in regards to network survivability
- Increase device utilization by spreading the data processing load across multiple, similar tools
- Perform media speed conversion to extend the life of your existing solution

Visibility Architecture Solutions from Keysight

Keysight's network visibility solution involves using NPBs in conjunction with application intelligence and taps. Learn more about Keysight's Network Packet Brokers, PacketStack, AppStack, and SecureStack Technology.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES