SOLUTION BRIEF

Understanding How Feature Combinations Affect NPB Performance

Deployment Scenario: Out-Of-Band Visibility Architecture

Network packet brokers (NPBs) can provide a plethora of features and functionality. For instance, besides implementing Layer 2 through 4 packet filtering, you may want to perform Layer 7 filtering and combine with NetFlow generation and data masking. In another instance, maybe you want to support SSL data decryption and use load balancing to distribute the clear text data to multiple tools. The key point is that you bought a packet broker and want to use all of the functions, not just some of them.

Unfortunately, depending on the manufacturer and model, all of these functions may not work simultaneously because the manufacturer chose to use a blocking architecture within their device. This solution provides the methodology and objective data that you need to understand how your NPB will behave in real world situations and validate which features can run concurrently.

Solution Components

- Network Packet Brokers
- BreakingPoint
- PerfectStorm

Benefits

- Better understand how your NPB will behave under real-world conditions
- Help you understand if there are NPB-based monitoring limitations
- Reduce the financial cost of your monitoring solution by purchasing a solution that runs all desired features simultaneously

Solution Overview

This network visibility solution allows you to:

- Validate whether your NPB features can run simultaneously at line speed
- Understand if there are network monitoring trade-offs required due to NPB limitations
- Compare multiple NPB solutions for feature functionality

KEYSIGHT TECHNOLOGIES

Validation of Feature

To validate feature compatibility and non-blocking architectures, a traffic generator is required along with a packet capture (PCAP) analyzer to observe the output from the NPB under test.

Here is the basic process to validate your NPB performance:

1. Install IxNetwork, BreakingPoint, Wireshark, and the NPB in a lab
2. Set up BreakingPoint to send a mix of web traffic including Netflix media, static applications, dynamic applications, and SSL-encrypted traffic.
3. Set up the NPB to concurrently perform de-duplication, SSL decryption, and application monitoring with NetFlow data generation. Configure the Netflix traffic to forward to VLAN 100, so that you can easily separate it from the other traffic for application monitoring.
4. Set up two IxNetwork devices – one to generate Netflix traffic into the NPB and the second to observe the output port of the NPB to the NetFlow tool.
5. Set up Wireshark on an NPB output port to receive the packet captures, analyze them, and validate that they are correct.
6. Compare results between different NPBs to validate their operation
7. After performing this analysis, you will probably find that different vendors do indeed have architecture limitations that affect NPB performance and reduce the utility of their monitoring solutions.

After performing this analysis, you will probably find that different vendors do have architecture limitation that affect NPB performance and reduce the utility of their monitoring solutions.

After performing this analysis, you will probably find that different vendors do have architecture limitation that affect NPB performance and reduce the utility of their monitoring solutions.

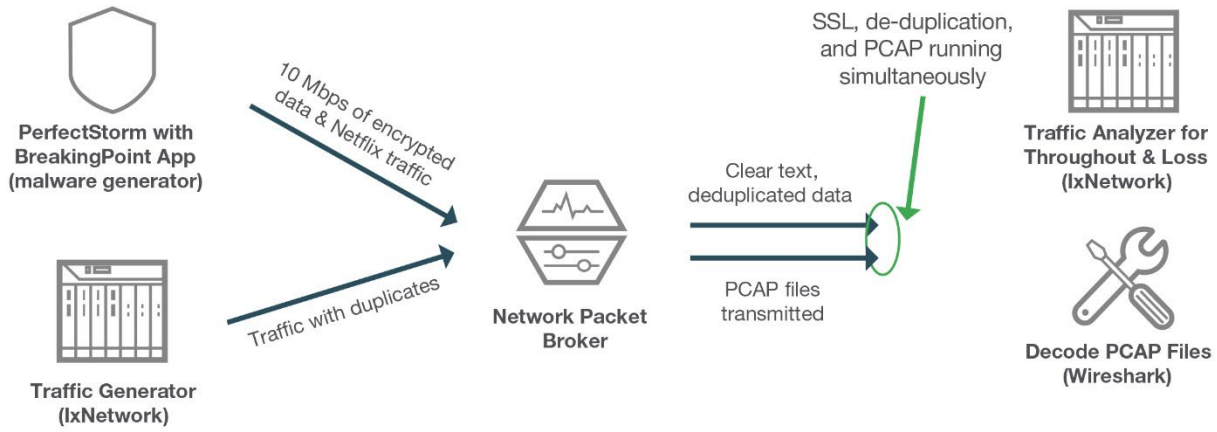

Figure 1. Configuration set-up

Summary

Understanding actual NPB performance is critical for any monitoring solution. One reason is that if the NPB has hidden architecture flaws (like a blocking architecture) or feature limitations, then this can have a direct impact on your solution by increasing (possibly significantly) your costs.

A second impact is that if the NPB has limitations, then the correct type and amount of monitoring data will not be passed on to the security and monitoring tools. This missing information can, and will, cause blind spots which can become very costly to an organization in terms of security breaches and troubleshooting efforts. Make sure you know now if there are network monitoring trade-offs required due to NPB limitations before you find out when it really matters.

Make sure you know now if there are network monitoring trade-offs required due to NPB limitations before you find out when it really matters.

Visibility Architecture Solutions from Keysight

Keysight's network packet brokers provide full-featured support at line rates up to 100 Gbps to security tool and monitoring tools. This includes de-duplication, load balancing, application filtering, SSL decryption, NetFlow, and many other features. Learn more about Keysight's Network Packet Brokers, BreakingPoint, IxNetwork, PerfectStorm, 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