TRAFFIC DISCOVERY AND VALIDATION TOOLKIT

Determine Precisely How Much Noise You Can Reduce From Your Network Tools Traffic

Irrelevant and unnecessary traffic to your network and security monitoring tools is a burdensome tax you pay in terms of unrealized performance and added costs. But much of this noise can be reduced or, in many cases, eliminated, by using traffic optimization.

Gigamon experts developed the Traffic Discovery and Validation Toolkit to prove how much irrelevant traffic or noise can be eliminated using traffic optimization techniques.

Now you can eliminate the guesswork on how much your network traffic can be optimized.

THE CONCEPT

The Traffic Discovery and Validation toolkit enables you to determine the exact noise reduction percent from your network traffic, as illustrated below, with the use of multiple traffic optimization capabilities. When you reduce the noise, you make your tools more efficient and enable longer usage before needing to purchase additional tool instances.
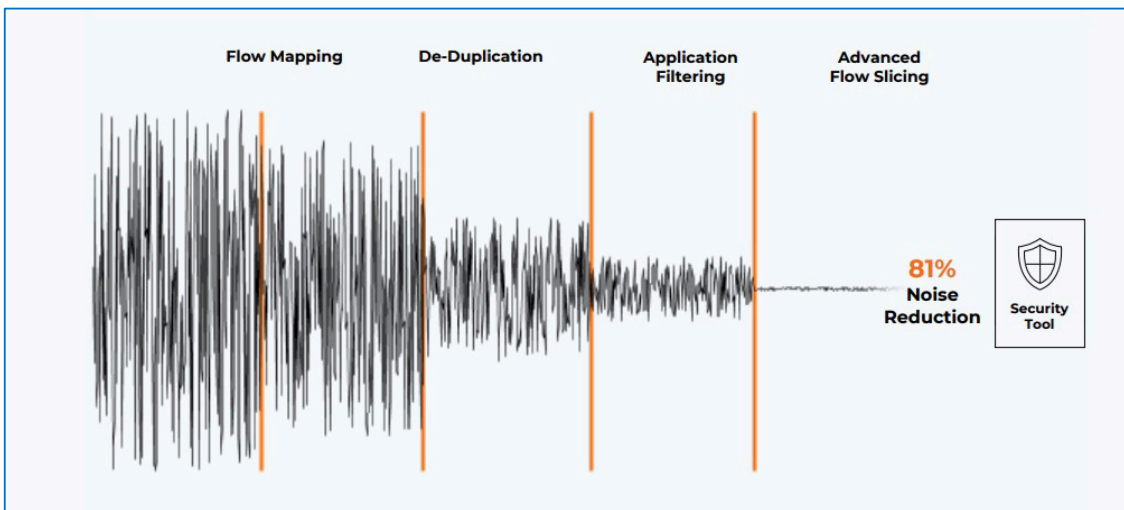

Figure 1. By applying proven traffic optimization techniques you significantly reduce efficiency-sapping noise.

Here is a step-by-step process, using the Traffic Discovery and Validation Toolkit, to determine precisely how much irrelevant traffic can be removed from your network traffic using various traffic optimization techniques.

STEP 1. APPLY DE-DUPLICATION TO YOUR TRAFFIC AND SEE THE IMPACT.

Why? Duplicate traffic is a "least effort" method to reduce 30–60 percent, typically, of noise to your tools. The toolkit dashboard below shows you the percent of duplicate traffic you can filter out.
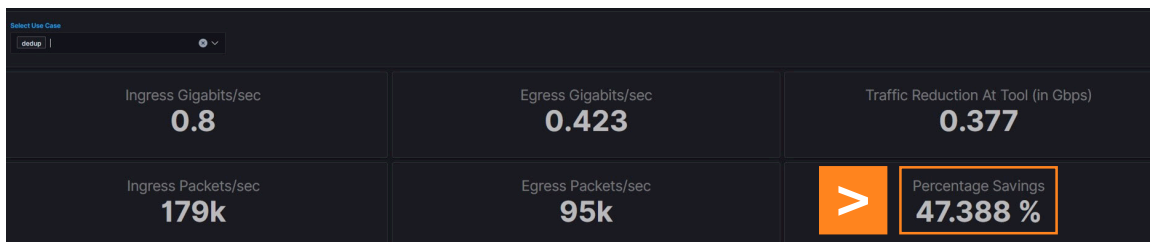

Figure 2. In this example, de-duplication by itself results in a 47.388 percent savings in traffic to tools.

STEP 2. FILTER OUT LOW-RISK, HIGH-BANDWIDTH APPLICATION TRAFFIC

Many organizations have budget constraints, but Gigamon Application Filtering Intelligence (AFI) helps you prioritize and filter tool traffic by application based on security risk, which can help you use your budget more effectively.

It's a straightforward process: The dashboard in Figure 3 lists the applications running based on traffic, and the associated bandwidth for each. You can then filter out low-risk, high-bandwidth application traffic, such as video streaming or windows updates. The dashboard in Figure 4 shows you the resultant impact.
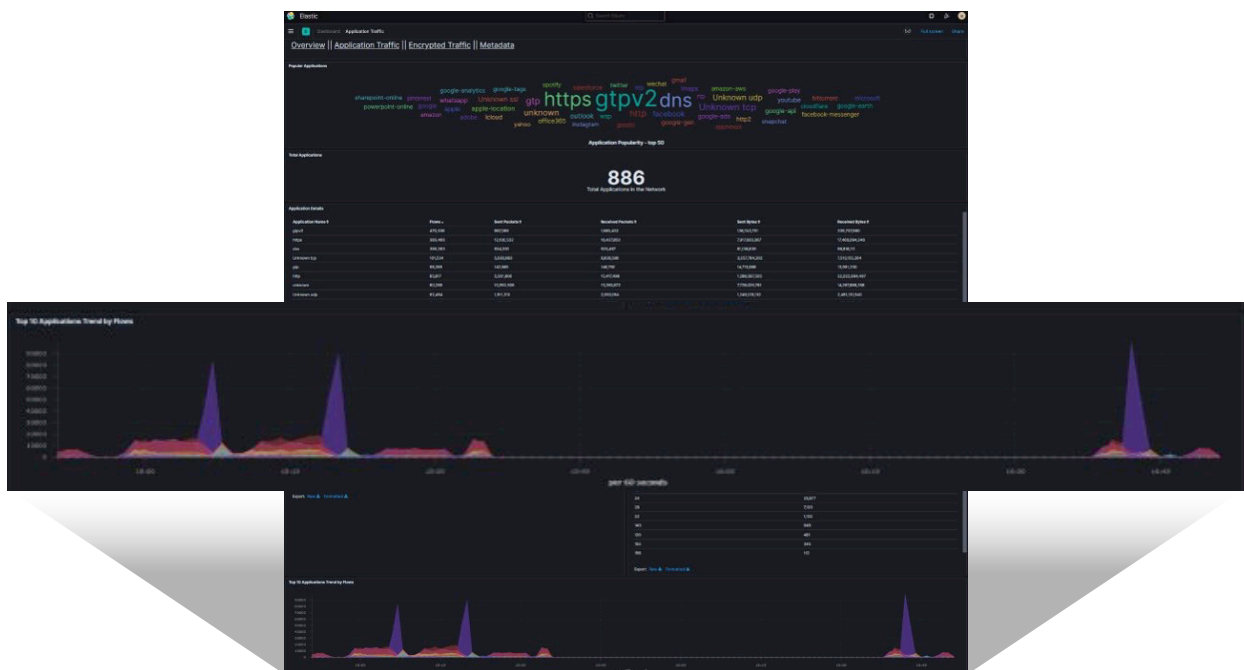

Figure 3. AFI lists applications and their bandwidth in your traffic, some of which is low-risk, high-bandwidth that you can safely filter out.
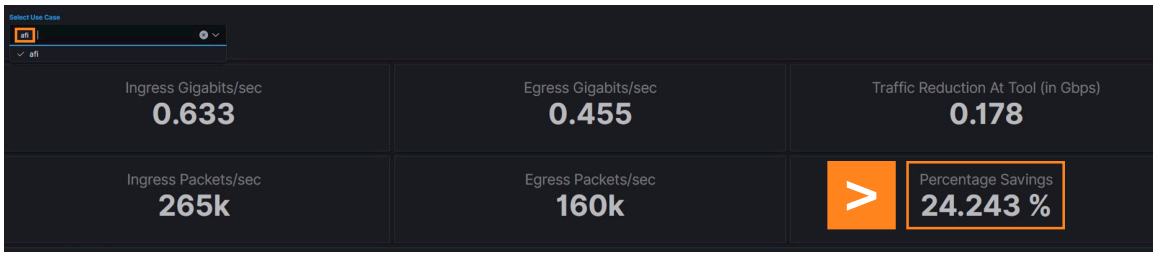
Figure 4. In this example, AFI eliminates 24.243 percent of traffic to tools.

STEP 3. USE FLOW MAPPING TO GET THE RIGHT TRAFFIC TO THE RIGHT TOOLS.

This is a fundamental feature to route certain traffic based on ports and other criteria to specific tools, typically enabling a 10–30 percent reduction in irrelevant traffic.
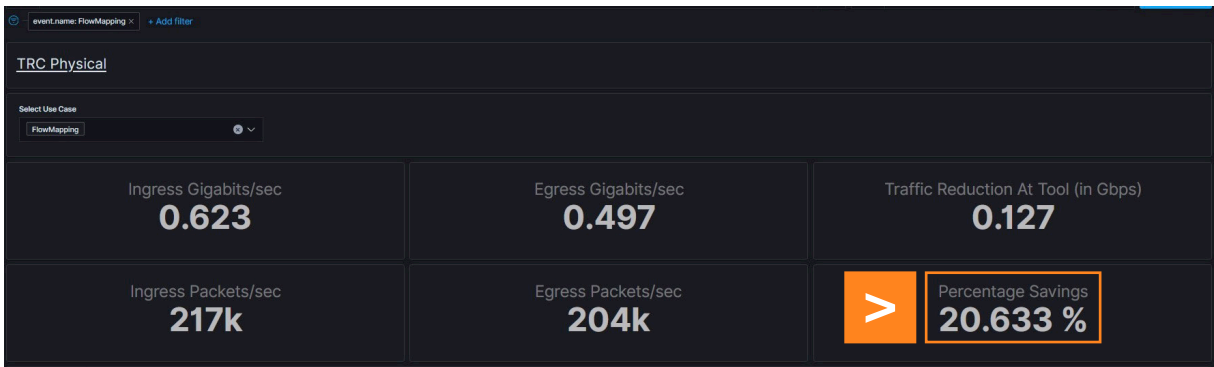

Figure 5. In this example, flow mapping provides an additional 20.633 percent savings in traffic to tools.

STEP 4. USE METADATA OR HANDSHAKE INFORMATION FOR TOOLS THAT DON'T REQUIRE PAYLOAD INFORMATION FOR EVERY PACKET IN A SESSION.

Next, take the opportunity to reduce expensive ingestion spend for SIEM tools, such as Splunk and others.

Gigamon Application Metadata Intelligence generates metadata from your traffic, while Gigamon Application Flow Slicing cuts the payload after the first 10–30 packets are ingested by your tools of choice (handshake information still gets sent to the tool).

The dashboard in Figure 6 below shows a reduction of tool traffic using Application Flow Slicing of over 90 percent, a very typical result.
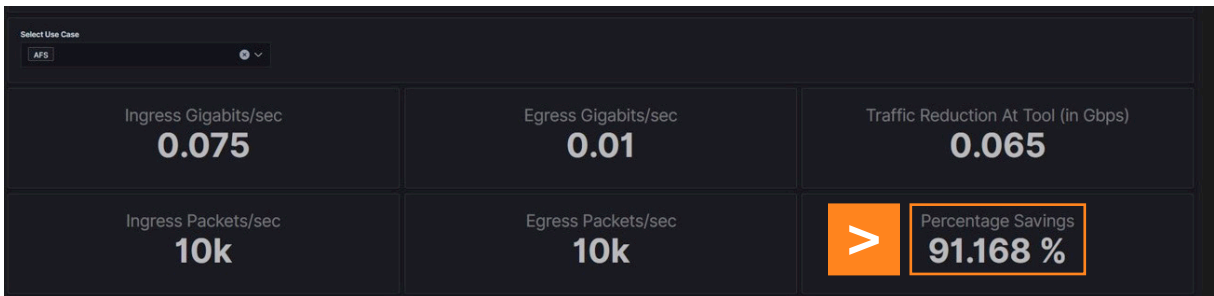

Figure 6. In this example, Gigamon Application Metadata Intelligence and Gigamon Application Flow Slicing combine to save 91.168 percent — a big reduction. How much could you save?

STEP 5. ADD UP THE COMBINED IMPACT OF ALL THE OPTIMIZATION TECHNIQUES.

You can see the combined impact of utilizing all the various techniques described above in one percentage. Many Gigamon customers worldwide have achieved 70–95 percent reduction to tools using capabilities in succession.

Figure 7. In this example, the combined reduction saves 80.738 percent.

How Much Noise Can You Reduce?

These results are common for those who try the Traffic Discovery and Validation Toolkit.

Schedule your complementary* analysis of your network traffic and we'll generate an annualized forecast of your tool spend and your savings.

Visit go.gigamon.com/NEAT.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

* Qualified organizations as determined in initial consultation (criteria includes size of organization and number of tool types deployed). Limited time deployment.

02.23_01