

Understanding NetFlow Latency and Effectiveness in Detecting and Mitigating DDoS Attacks

HIGHLIGHTS

- NetFlow and IPFIX flow-based telemetry is the most efficient, scalable, accurate, and fastest way to detect DDoS attacks
- Flow-based export is up to 30x more efficient than sFlow
- Customers using Sightline and TMS who follow our recommended flow export best practices regularly report fast DDoS detection times of one second, and time to mitigation in as little as 10 seconds

NETSCOUT Recommended Settings for Flow Export

- Active flow timer: 60 seconds
 - Inactive flow timer: 5 seconds
 - Sampling rate: 1:1000 or 1:1024
 - Note: rates of 1:2048 or 1:4096 can work reasonably well if the router is unable to support faster sampling.
 - Tune flow cache size to keep it mostly full "running hot"
-

Recently some network operators have raised concerns about the use of flow data as a DDoS detection mechanism. The main concern is usually a perception that NetFlow export has high latency, i.e. that the attack will not be detected quickly because the NetFlow won't be sent to Sightline for a minute or so until after the attack has already caused an outage. There is also sometimes a concern that packet-based data such as sFlow provides better data than flow to detect and identify attacks.

While understandable for network operators who haven't worked with flow-based telemetry yet, these concerns are not accurate. While Sightline does support sFlow perfectly well if customers prefer to use it, flow-based telemetry (NetFlow, IPFIX) remains a more scalable, accurate, and fast option to detect DDoS attacks. Many of the perceived benefits of sFlow stem from a misunderstanding of how flow export works. With this FAQ, we hope to clear up these misunderstandings and false claims.

Isn't Flow Only Exported From the Router Once a Minute, so That DDoS Attacks Can't Be Detected for at Least a Minute?

Sightline using flow data can detect DDoS attacks in 1 second.

This is perhaps the most common concern that we hear, and it is understandable. With DDoS attacks, speed of detection is critical. However the perception that flow data is only exported once a minute, or with some longer latency, is not true for properly configured modern routers, and hasn't been true for a long time. Sometimes network operators have routers that are not correctly configured to export flow quickly, which results in unnecessary latency in flow export from the router, leading to this perception. With properly configured routers, flow records should be exported for DDoS attacks within a few seconds at most, and usually within 1 second.

How Does the Flow Export Process on a Router Work?

Routers sample packets to generate flow records. Flow records are maintained in the router's flow cache. When a router samples a packet, it checks to see if there is a flow record already in the cache for the packet, and if so updates it. If there isn't a flow record in the cache, then a new record is created. If there isn't room in the cache for the new flow record, an existing flow record (usually the oldest) is exported and cleared from the cache to make room. For this reason, the key to ensuring fast flow export is to ensure that the flow cache runs "hot" – i.e. full or nearly full all of the time.

How Should I Configure My Routers for Fast Flow Export?

NETSCOUT's recommends using these settings for router flow export:

Active Flow Timer: 60 seconds

Inactive Flow Timer: 5 seconds

Sampling rate: 1:1000 or 1024 (ideal, for some routers higher rates may be needed)

Flow cache size: Tune to a size that keeps the cache running "hot" (i.e. mostly full)

The inactive flow timer ensures that flows are exported quickly as soon as a TCP RST or FIN is seen. Keeping the flow cache size small enough that the cache remains fairly full ensures that flow records are constantly being exported by the router, rather than stored for long periods of time.

Network Operators experiencing long flow export latency typically have either set these timers to longer values, or have set the flow cache size to be too large. Reducing these values should fix the flow latency problem. The flow cache size that achieves this will depend on the sampling rate and the volume of traffic moving through the router.

If these settings are set correctly, then NETSCOUT® observes roughly 80% of the flow records exported will be for a single packet, and flow records generally will be sent within a second or so of the packet passing through the router. Your NETSCOUT Sales Engineer can further guide you on how to configure your routers for fast, efficient flow export.

Sampling rates of 1:2048 or 1:4096 can still work reasonably well if that is the best that the router can support. Higher sampling rates are not recommended as they lead to a loss of data granularity and increase the minimum DDoS attack size that can be accurately detected.

So With Flow Data I Can Detect DDoS Attacks in 1 Second?

Yes! Many NETSCOUT customers using Sightline and TMS who follow our recommended practices above regularly report fast DDoS detection times of 1 second, and time to mitigation of as little as 10 seconds (depending on BGP propagation times for diverting the traffic, which would be an issue for any diversion-based mitigation solution).

Doesn't Frequent Fast Flow Export Cause High Load on the Router?

Flow export has not caused load issues in modern routers for many years. The reason is that flow records are a very compact way to represent flow (and packet) data. Also, flow records are batched, with many flow records (up to 30) being sent per UDP packet. This makes the export process very efficient, especially if records are being exported frequently, since the router can batch them into the fewest packets possible. Modern CPUs used for the processing of flow export, and the fact that flow is batched into a smaller number of packets, helps keep the load on the router due to flow export lower.

Compare this to sFlow, where each sFlow packet can only store information about one packet seen by the router. **This means flow export is up to 30x more efficient than sFlow** for the router to send and the destination to receive and process.

Doesn't sFlow Provide More Data Than NetFlow?

This is also a very common concern. The perception is that sFlow is exporting "packet" data, and so would be more useful to understand the contents of the traffic and identify DDoS traffic. The reality is that sFlow only exports the first 128 bytes of a packet in most cases (some modern implementations may include more of the packet, but rarely the full payload). This is only enough to include full layer 4 headers (which are also included in flow records), and a fragment of application payload. For example, this is not enough data to include a full DNS Query in many cases, or the full DNS reply. It also can't include a full TLS handshake message. Other application traffic is likely encrypted (HTTP/s) and so a fragment of the encrypted payload is not helpful in any case.

These limitations mean that in practice, NetFlow and IPFIX provide the same quality and detail of data that an sFlow record does, and they do so much more compactly and efficiently, especially when using templated flow export such as NetFlow v9 and IPFIX.

Another concern is that sFlow export is frequently done in hardware on the line card where the packet enters the router, before the forwarding decision is made. This means that the sFlow record will not indicate the egress interface on the router where the packet will be forwarded, making traceback of DDoS attack traffic impossible. Because the flow record is generated as part of the forwarding process where the packet forwarding decision has been made by the router, Flow records almost always include both the ingress and egress ports on the router enabling flow data to fully report the path of traffic through the network.

I Hear You, but I Still Really Believe That sFlow Is Better. Do You Support sFlow?

Yes! While we believe that NetFlow or IPFIX data is more efficient and effective, Sightline fully supports ingesting sFlow data and has for over 15 years. Sightline provides full feature parity for sFlow data as it does with NetFlow or IPFIX.



Corporate Headquarters

NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information

Toll Free US: 800-309-4804
(International numbers below)

Product Support

Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us