opFlow and Cisco ASA NSEL NetFlows

Overview

opFlow version 3.0.6 and newer provide limited support for Cisco ASA NSEL NetFlow inputs. This document describes caveats and limitations of this interaction.

Cisco ASA devices from the 5500 series onwards support what Cisco calls 'NetFlow Security Event Logging' or short NSEL; this mechanism uses the NetFlow v9 data format (and custom 'templates') but transports somewhat different information than normal NetFlow exporters produce.

opFlow now makes use of the NSEL information where feasible and useful for its core purpose, visualizing traffic flows.

Only traffic events are handled

At this point, opFlow ignores NSEL events that indicate the creation or the denial of a connection. The only event types of potential relevance are the 'connection updated' and 'connection deleted' events, and for data consistency reasons opFlow currently handles exclusively the 'connection deleted' events. All other events are ignored and are tallied in the Operational Status report under the heading "Skipped Empty Flows".

NSEL flow information is usually delayed and not synchronous

According to the Cisco NSEL documentation, an ASA *may* send periodic "connection update" events with traffic counter updates (relative to an internal flow timer), but from our investigation of example data this information seems inseparable from and duplicated by the "connection deleted" events; the 'delete' events are mandatory while the generation of 'update' events is subject to various rules.

As of this time we're not aware of a mechanism that would let opFlow handle the "update" events (for minimum delay) without counting traffic twice (as the "delete" event duplicates the information); on the other hand, ignoring "delete" events would omit lots of data because for short-lived connections *no* update events are created at all.

For these reasons and to maximise robustness, opFlow 3.0.6 handles exclusively connection teardown/deletion events. This implies that opFlow will record NSEL traffic at connection termination.

NSEL flows are bi-directional

Typical NetFlow information is unidirectional whereas NSEL flow data includes 'internally assembled bidirectional' flow information covering both inbound and outbound traffic in a single flow.

As of version 3.0.6, opFlow does not split the inbound and outbound traffic counters from an NSEL input but rather records this as a single conversation with the sum of input and output byte traffic. (This behaviour will likely be reviewed and fine-tuned in future versions of opFlow.)