AS Origin Violation

AS Origin Violation

This alarm detects when any advertisement for the monitored prefix with origin AS is not in the **AS Origin List** list. This is a violating advertisement and could represent a prefix hijack attempt, especially if the AS path length in the advertisement is shorter than legitimate advertisements.

Note It is useful to know which of your peers may be doing something wrong (leaking route information or having some type of misconfiguration) so that you can address the problem right away. A **My Peers** rule is available for this alarm with certain Crosswork Cloud subscriptions. The **My Peers** option follows BGP updates *only* from your peers, whereas **All Peers** follow BGP updates from your peers *and* global peers. To configure this option, see Add Crosswork Cloud Network Insights Policies.

Possible Problem Detected

This alarm can help identify route leaks or a prefix hijack.

Relevant Alarm Rule Configurations

The following options should be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > AS Origin Violation**):

- Thresholds
- Allowed Origin ASNs

Example

You create a Prefix Policy with the **AS Origin Violation** alarm rule with for prefix 8.8.8.0/24 and it is configured with an AS Origin List field value of 15169. However, an observed BGP update is received with 8.8.8.0/24 and an origin AS of 109. This alarm triggers because AS 109 is not included in the AS Origin List.

AS Origin Violation