AS Path Length Violation

AS Path Length Violation

Detects when an AS path length for a configured prefix exceeds an upper or lower threshold. This alarm detects when an observed AS path falls below a lower threshold or exceeds an upper threshold for the AS Path Length.

The BGP AS path impacts the latency of prefixes, but is also an important tie-breaking step in BGP bestpath selection (the highest non-configurable attribute used in *bestpath* selection). Since shorter AS paths are preferred, this property can be exploited by a hijacker. You must configure an expected range for the AS path length for the monitored prefix. An advertised AS path length outside this range is a violating advertisement

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 hijacks. It can also help monitor latency of monitored prefixes.

Relevant Alarm Rule Configurations

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

- Thresholds
- Allowed AS path length range

Example

You create a Prefix policy with the **AS Path Length Violation** alarm rule and linked to prefixes 8.8.0.0/24 and 9.9.0.0/24. Prefix 8.8.0.0/24 is leaked by the user via a different peering point resulting in a shorter AS path which triggers the alarm. The alarm clears when prefix 8.8.0.0/24 is advertised via legitimate advertisements (a path length within the allowed range). Later, peering relationships change in the upstream path from prefix origin 9.9.0.0/24 (legitimately or due to a MITM attack) causing it to be advertised with a longer AS path. You might have little control of these upstream relationships and need to change the configured AS path range for the alarm to clear.