Upstream AS Change

Upstream AS Change

A BGP operator has control over their peering relationships through outbound policies (for example, which upstream ASs can propagate a prefix). This alarm detects a route leak to an existing peer, who should not propagate the prefix. The user must configure a list of allowed Upstream ASNs. Any advertisement for the monitored prefix with 1-hop left ASN in the upstream AS path that is not in the list, 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 of a monitored prefix.

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 > Upstream AS Change**):

- Thresholds
- Allowed Upstream ASNs

Example

You create a Prefix policy with the **Upstream AS Change** alarm rule with allowed Upstream ASNs [293,1221] and linked to prefixes 8.8.0.0/24. Prefix 8.8.0.0/24 is advertised by a peer or peers with AS path [2711, 1299, 3356]. Subject to thresholding, the alarm triggers because AS1299 is not an allowed upstream ASN. The

alarm clears when the route with the offending AS path is withdrawn or you add AS1229 to the list of allowed upstream ASNs.