

Subprefix Advertisement

- Subprefix Advertisement, on page 1

Subprefix Advertisement

A hijacker can redirect traffic for a portion of the IP space covered by the monitored prefix by installing a new subprefix (since a router will prefer the more specific route over a less specific one). The hijacker can also install a new route for an existing subprefix. To detect these hijack attempts, you can configure a list of allowed Origin ASNs of the subprefixes. For this alarm, the violating advertisement is when either the advertised *subprefix* and its peer threshold is in violation.

Possible Problem Detected

This alarm can help identify route leaks or the hijacking of a subprefix of the monitored prefix.

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 > Subprefix Advertisement**):

- Prefix subscription
- Thresholds per advertised subprefix (Peers to Resolve and Peers to Trigger)
- Allowed Origin ASNs

Note Toggle the **Use Origin ASNs** option to **No** to ignore the Origin ASNs list. An alarm will trigger for all ASNs if the Origin ASNs list is ignored.

- Max IPv4/IPv6 Length—Option to ignore subprefix masks longer than the configured **IPv4/IPv6 Max Length** is available. The maximum IPv4 length must be greater than 8 and the maximum IPv6 length must be greater than 16.

Example

You create a Prefix policy with the **Subprefix Advertisement** alarm rule and is linked to prefix 8.8.0.0/24. The following subprefix advertisements occur and triggers an alarm:

- An unexpected subprefix 8.8.0.5/30 is advertised. In this case, you had allocated this prefix to a new administrative organization and it is being advertised for the first time from a new origin AS. To clear this alarm, configure Crosswork Cloud Network Insights to subscribe to the *subprefix* 8.8.0.5/30, or its new origin AS should be added to the list of allowed Origin ASNs.
- An unexpected subprefix 8.8.0.4/30 is advertised. This may indicate either a route leak or a hijack. In order to clear this alarm, 8.8.04/30 should be withdrawn.