

Prohibited IP Prefix

- Prohibited IP Prefix, on page 1

Prohibited IP Prefix

This alarm detects if a monitored peer has a prohibited prefix in the public IP routing space installed in its Routing Information Base (RIB) or the monitored peer is forwarding it.

Bogons are IP address blocks that are not public, either because they are reserved or have not been allocated to a Regional Internet Registry (RIR). *Full bogons* also include address blocks that have been assigned to the RIRs but are not allocated by the RIR to a specific network. It is good practice for routers to filter advertisements for a prohibited prefix. A user can choose to be alerted only for bogon advertisements using this alarm.

Possible Problem Detected

This alarm can help identify DoS attacks on routers.

Relevant Alarm Rule Configurations

Select **Bogons** or **Full Bogons** when adding this alarm rule to a Peer policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Peer Policy > Add Rule > Prohibited IP Prefix**).

Example

You create a Peer Policy with the **Prohibited IP Prefix** alarm rule with option **Bogons** and linked to Peer RTR1. The alarm activates when RTR1 advertises 10.0.0.0/24 (Bogon per RFC1918) to Crosswork Cloud Network Insights but not when 2001:221::/32 (Full Bogon) is advertised.

Prohibited IP Prefix