RAPIDS: Rogues, Triggers and Alerts

This article explains how rogue-related triggers and alerts work and the effect of acknowledging and deleting them.

There is only one type of trigger that applies to rogue devices: the *Rogue Device Classified* trigger. The definition of the *Rogue Device Classified* trigger contains a condition. The condition has to do with the RAPIDS classification of the rogue device. When the trigger is evaluated, an alert is generated if that condition is satisfied. All *Rogue Device Classified* triggers are evaluated any time the RAPIDS classification level of a rogue device increases.

The decision tree for generating a rogue-related alert is as follows:

Discovery event* (wired or wireless)
→ RAPIDS classification rules evaluated
→ If RAPIDS classification is higher than previous classification...
→ Each *Rogue Device Classified* trigger is evaluated
→ If the trigger condition is satisfied an alert is generated

*A device that is monitored by AMP reports another device that AMP does not recognize as one that it is monitoring.

Notice that there is no mention of acknowledged alerts or acknowledged rogues in the decision tree. This is because acknowledging an alert or a rogue has no effect on whether new alerts are generated for a particular rogue device. More on this below.

Likewise there is no mention of the pre-existence of alerts in the decision tree. This is because deleting alerts has no effect on whether new alerts are generated for a particular rogue device. More on this below.

Examples:

Define four RAPIDS rules (on the RAPIDS > Rules page), one for each of the following RAPIDS classifications:

- Valid
- Suspected Neighbor
- Suspected Rogue
- Rogue

(There is an excellent overview of RAPIDS rules in the *RAPIDS Best Practices Guide*.)

Next define four triggers (on the System > Triggers page) as follows:

Classification >= Valid
Classification >= Suspected Neighbor
Classification >= Suspected Rogue
Classification = Rogue

Case 1: Let's say an AP that is not monitored by AMP is heard by another AP that is monitored by AMP (wireless discovery) which satisfies a RAPIDS rule classifying the device as Suspected Rogue...

You should see 3 alerts:

Classification >= Valid
Classification >= Suspected Neighbor
Classification >= Suspected Rogue

(NOTE: Alert emails may contain more detail than the alert as seen in the web GUI.)

This rogue AP will be reported by a monitored AP that hears it every time the monitored AP or its controller is polled. The new discovery event will appear on the detail page for the rogue AP --replacing any previous discovery event by the same device. If the new discovery event does not cause the device to be re-classified (cause the device's RAPIDS classification to change) no new alert will be triggered.

Case 2: Let's say that same AP is then discovered in the Bridge Forwarding Table of a switch and is therefore re-classified as a Rogue (wired and wireless discovery)...

You should see 4 more alerts:

Classification >= Valid
Classification >= Suspected Neighbor
Classification >= Suspected Rogue
Classification = Rogue

The change in the device's RAPIDS classification causes all of the *Rogue Device Classified* triggers to be evaluated again. Because the classification of Rogue satisfies all of the trigger conditions, all four triggers generate alerts.

NOTE: Only a change in a device's RAPIDS classification will cause the *Rogue Device Classified* triggers to be evaluated. Multiple RAPIDS Rules at the same classification level will not trip the same trigger more than once, even if the threat level changes. The same trigger may be tripped multiple times for the same device, but only if the classification changes.

Case 3: Let's say a device has been classified as a Suspected Rogue due to signal strength. The *Rogue Device Classified* triggers are evaluated and the appropriate alerts are generated. Then, in a later discovery event, the device satisfies a different RAPIDS rule that classifies it as Suspected Rogue due to SSID. The device's classification has not changed so the *Rogue Device Classified* triggers are not evaluated and no alerts are generated.

Alerts: Acknowledging and Deleting

As mentioned above, in the case of a *Rogue Device Classified* alert, acknowledging or deleting alerts has no effect on whether a new alert will be generated. A change in RAPIDS classification is the event that causes *Rogue Device Classified* triggers to be evaluated. If the classification level of a device increases, all triggers will be evaluated, and if a given trigger's condition is satisfied, a new alert will be generated by that trigger.

Rogues: Acknowledging and Deleting

Acknowledging a rogue device has no effect on whether a new *Rogue Device Classified* alert will be generated. Acknowledging a rogue device does not stop alerts from being generated for that device. The same process for generating new alerts for a device is followed whether the rogue has been acknowledged or not. If a device is re-classified after being acknowledged, all *Rogue Device Classified* triggers will be evaluated, and if a given trigger's condition is satisfied, a new alert will be generated by that trigger.

If a rogue device is deleted, all associated alerts and discovery events are also deleted. If the device is discovered again, the process will begin as if the device is being discovered for the first time.