Qualys Network Passive Sensor v1.x

Release Notes

Version 1.2.2

January 11, 2021

Here's what's new in Qualys Network Passive Sensor 1.2.2!

With this release, we've fixed an issue where users of the Global IT Asset Inventory were facing delay in processing of the assets in the "Unmanaged" Inventory because of issues in the Network Passive Sensor (PS) appliance.

PS appliance consumes high computing resources from the cloud servers because of certain traffic patterns in customer networks where it is deployed. These traffic patterns result in PS appliance reporting a larger number of traffic flows and also traffic with anomalously high number of open ports for some assets.

To address this issue, we've done following improvements in Network Passive Sensor:

- Hardened the identification of valid flows by the PS appliance. Extra checks are introduced to reject flows where no application content is exchanged. The hardening also rejects anomalous flows with unidirectional data resulting out of flaws in mirroring configuration that can result only in Tx or Rx data to be reported.
- Dropped ephemeral ports used for secondary data connections under a parent control flow. Certain protocols like FTP, TFTP, UPnP create temporary secondary connections for actual short lived data exchanges. These results in excessive open ports being assigned to many assets engaged in such data exchanges. Additionally the open port reporting is capped disallowing excessively high open ports from being recorded against any asset.
- Improvements in asset creation to handle a few corner cases which have a possibility of creating multiple assets/assetIds for the same physical asset.