2017-11-13 Unibank

Monday, November 13, 2017 12:13

Participants:
anna.kwayisi@unibankghana.com, christian.aborgeh@unibankghana.com, daniel.squire@unibankghana.com, emmanuel.sam@unibankghana.com, ibrahim.jibrilu@unibankghana.com, karen.ampoful@unibankghana.com, samuel.anakwa@unibankghana.com

john.tamakloe@ostecit.com, kwame.addo@comsecafrica.com,

Summary:

System was reviewed with the following findings:

- Current Portnox version is 3.0.2 no HF
- Switch 192.168.23.20 no longer exists - needs to be removed
- Switch 172.30.151.19 no longer exists - needs to be removed
- 192.168.10.20 read community is incorrect - to be fixed by customer
- UNI_SEC authentication has invalid credentials - to be fixed by customer
- Several alerts will be reviewed and handled by customer.
- Medina site was down and thus no communication was observed. After communication was restored, functionality returned.
- Although many switches are configured in monitor mode, currently piloting 2 switches (in enforce mode): 172.30.2.9, 172.30.2.10
- Rogue device on pilot switch was indicated as a test of rogue device. Search by IP and MAC was shown to locate the rogue device which is no longer connected (port is disabled by policy).
- 192.168.11.230 IP Helper has high latency (latency of ~900ms) - Portnox was able to retrieve IP address of devices. If any issue is found, a ticket should be opened with Portnox support to include Portnox logs (collected using Portnox Monitor app for the time of issue).
- Alerts are not closed automatically/immediately - issue escalated to be addressed in a future release. Alerts may be closed manually.
- Errors observed in Monitor: Duplicate entry in DB results in failure of query, SNMP trap packet error
    - Recommendation: install latest HF (HF7) and review errors
- Disable by policy wait period was raised for ability to change the value. This may be configured in Setup->Preferences to a different value (default is 300 minutes) as shown during the session
- Permissions and user role configuration reviewed and explained how to create new roles with custom permissions
- Solution functionality and benefits was explained to security team
- Role and functionality of IP Helper in Portnox was explained

Next step for Unibank:

- Address alerts found (update credentials, remove redundant switches, etc.)
- Install latest HF (by customer/reseller) – can be found in the following link: 3.0.2 HF07
- Schedule an additional session (up to 2 hours) for beginning of next week once alerts are addressed and HF is installed to review again