2017-02-01

Wednesday, February 1, 2017 12:37

- Portnox remote
- Amdocs - new people without experience
- DB - Portnox to do
- [x] Unmanaged vlan in a specific server (e.g. India) but same vlan is managed in other location (e.g. US)
  - Configure policy per hive and vlan
- Migration
  - [x] Authentication needed as passwords are not known - Manual recover passwords
  - [x] Policies - none exist
  - [x] Switches - export + import with noxcli
  - [x] IP Helper - export + import with noxcli
- [x] HA between locations - Manual failover
  - 2 DBs in different locations
  - Enforcers?
- Latency
  - IL-US: 120-180
  - IL-IN: 180-220

Hi Idan,

As discussed on call kindly check the requirements which we have raised.

- What are possibilities of managing/un-managing different region same VLAN.
- How we can use more than one database for replication? Also If one database goes down is it possible automatically switching to 2nd database.
- Is it possible to have central management with same current architecture (5 Servers and 4 Database)?
- How Authentication and policy migration can be done without adding manually to new setup?
- Suggest if you have any other architecture which will suffice our requirement.

Let me know if you need any further information.

Regards,
Suryakant Patil

2017-02-27

Monday, February 27, 2017 08:56

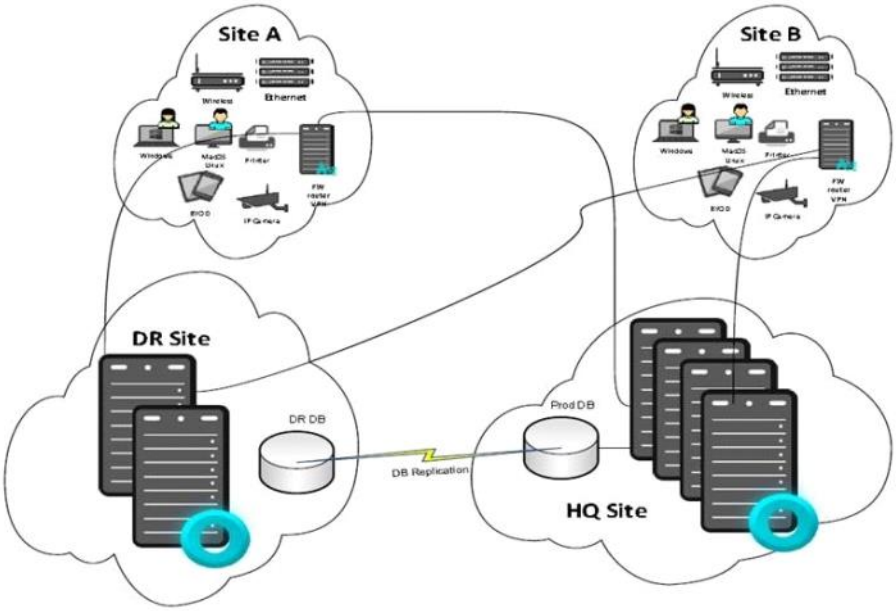
- Architecture stories (different architectures and customer stories) + white papers + technical papers
- Formula to calculate the traffic per event and per server + ports
    - Enforcer to DB - changes per environment, depends on configuration (switches, ip helpers, protocols, auths, policies, compliances, etc.). Over 150ms latency risks stability.
    - Information received from ip helpers, snmp traps, etc. by a specific enforcer will be sent to other enforcers
    - Web action to distant network will update DB + update relevant enforcer (WCF between enforcers)
    - Backups communicate with all enforcers and DB.

2017-04-19 Architecture

Wednesday, April 19, 2017 15:39

Idan,

Please find attached a diagram for the Architecture.
This was finalized during the discussion between portNox , Amdocs Info-Sec & Amdocs DB teams.



Short explanation

Two complete replicas in active-passive mode.
one in Israel and one London , Israel site is active, London is passive.
At Each site, we place the following configuration:

a. 5 enforcement servers (for WW)
b. 1 enforcement Backup Server
c. 1 DB Server
d. **All** Enforcement servers in same site, see **only** the local DB server (Connection string to local db)

An SQL Replication between both DB servers, Israel --->London , with no listener in London.

Use cases

1. **An Enforcer malfunctions in Israel**
   a. The backup server in Israel takes its place
2. **Database crash in Israel**
   a. Database in London automatically goes live (SQL Server functionality)
   b. We bring the servers at London up
3. **Connectivity from Israel to WW is lost**
   a. Database in London automatically goes live (SQL Server functionality)
   b. We bring the servers at London up

We now need to set up the Israel (Active) site , 5 enforcers + 1 backup enforcer.
The Database server is still being provisioned.

Regards,
Vignesh Kamath
Network Engineer
Business Technologies Group, IT
Amdocs GO

2091 54526 (Internal)
+ 91 020 4015 4526 (External)

2017-05-09

Tuesday, May 9, 2017 10:55

- Servers installed:
  - 1-5 Active in IL - Up
  - 6 backup in IL - currently down
  - 7-11 Active in UK - Down
  - 12 backup in UK - Down
  - Servers were installed using the IL DB address.
  - Need to do:
    - Confirm DB installed in UK with synch from IL.
    - Change DB connection string for all UK servers using DB Util and verify registry and web.config were updated

2017-05-18

Thursday, May 18, 2017 12:49

- Bulk hive update for switches (and create hive)
- IPHelpers update name using DB update command

2018-05-02

Wednesday, May 2, 2018 17:58

- Jehuda to work with Vignesh K tomorrow on the following :
    - Compliance implementation -> Create a script to force a machine to update itself - windows patch , SEP (testing is pending)
    - Compliance Implementation -> Start Auto Blocking actions for UAT Hive
    - Feasibility check -> Last installed patch is not more than 50 days old
    - Feasibility check -> Move blacklisted devices back to separate VLAN and back to previous VLAN
    - Policy Implementation -> Exclude entire VLAN from enforcement for particular hive
    - Feasibility check -> Whitelist for MAC (Like resident block list) , use of skip authentication
    - Feasibility Check -> Logged in user is a part of Domain check
    - Discussion -> How TCP fingerprint works , DB table which has header for fingerprint data to be demonstrated
    - Discussion -> Compliance Totals not adding UP to same count

- Points Pending with Idan :
    - Feasibility Check -> Is it possible to generate a report for eLAN compliance failures that also has product and failure reason (Status) column in it
    - Discussion -> Hive Name column in report for rogue devices
    - Discussion -> Voice VLAN Change on IP Phone rogue
    - Discussion -> DR implementation procedure and timing (Pending 3 DB Scripts for Failover, cluster_util , failing back)

- Following Points have been discussed :
    - Agent for Microsoft Monitor Agent is known to impact the service and increases CPU utilization on server
    - Feasibility Check -> Workgroup Authentications , can Portnox use a username other than built in Administrator ? Yes
    - Feasibility check -> Can we sort the Cluster ID , what is the Impact - possible but not recommended (Too many references in the DB)
    - Feasibility Check -> Screensaver is active on the Domain authenticated machine check - Not possible
    - Feasibility Check -> Is it possible to search for not connected devices ? by IP or MAC - Possible , but some events (Like new device connected in place of old one) may remove this data
    - Discussion -> How WMI works -Portnox checks only the last patch installed date , not last successful update check time
    - Discussion -> Portnox availability and escalation (Sunday to Thursday 9 AM to 6 PM Israel time) , issues may be escalated to idan.blum@portnox.com if no update on ticket

2018-05-28

Monday, May 28, 2018 10:07

Preventing go live:

Amdocs:

- 9390 - Fingerprints authentication fails - No TFS
- 9281 - IP Helpers - IP seen but cannot authenticate (missing IP)- No TFS
- 9264 - Compliance could not connect - Bug 38676:compliance check - could not connect

Portnox:

- Compliance to be handled in next phase
- 9230 - India Juniper switches - Bug 39140:Switch failed to be enable several times and after enabled shows 0 devices

Time limits

- Vignesh will be available only on June 4 and after

Action Items:

- Deadline: by mid of June
- Resolve Auth issues
  - Daily status for 2 issues raised by Vignesh
- Review policy and 400 rules
- Idan to send invites
- Provide deadlines of issues to be resolved
- Provide due date for compliance

2018-08-21

Tuesday, August 21, 2018 10:11

- Could not connect status reduced from ~700 devices to ~150
  - Devices are actually failing due to not updated but elan shows old status
- Rogue devices increased
  - Device in example given was not authenticated for a long time (seems was rogue for quite a while)
- Classic UI is extremely slow
  - NAS View takes very long time to load and open
  - Policy takes very long to load
  - Edit rule never ends
- NG Experience device view takes very long time to open

2018-09-16

Sunday, 16 September 2018 10:03

Danny, Michael, David

- Slowness of portal : searching a device got better than previous but there are still some segments where we are observing slowness.
- ~~Mismatch in Rogue count of GUI and DB. We need to make both in sync.~~
- As phone won't get blocked even if it gets identified as rogue, do we have any mechanism to block them?
  - Set vlan applies to native vlan only. For voice, block action should be configured to block the port.
- Servers having Multiple VM's are getting identified as "Unauthorized hubs", do we have any fix for this?
- Enforcement timeout in new GUI is less, we need a fix for this
  - Newnox has rstriction for 20 sec timeout
  - Classic cannot enable switch (operation fails/times out)

➔ Script to Whitelist/Voucher for bulk devices.

- ~~Slow - whitelisting takes ~20 minutes~~
- ~~Mismatch of rogue device count~~

- Verify there is TFS for:
  - ~~Voucher issue~~
  - Rulebase performance - not seen
  - Stuck threads - OTS
  - Switch timeout is limited to 20 sec in newnox

    Bug 42664:Switch timeout setting in newnox is limited to 20 seconds
  - Switch is marked down + switch commander does not open

    Bug 43481:Switch initial probe never completes

2018-09-17 - Internal meeting summary

Monday, 17 September 2018 19:13

Participants: Ofer, Idan K., Vadim, Idan B.

Summary:
Amdocs are at a delay of moving to enforcement. Original date was beginning of August which was postponed a few times and today postponed again due to the issues they have.
Status has been escalated to Amdocs management and management status meetings with Idan B. take place on a weekly basis due to the urgency and focus this has at Amdocs.
Amdocs DB is available in Blum's lab on SQL Express and on Alex Ryzhov lab on SQL Standard.

Issues:

1. Stuck threads – all authenticators are found stuck on at least 2 servers. Oleg participated in the session today and expects the OTS to resolve the issue observed. Hot swap was raised as an option that may be needed. Option to enable hot swap needs to be checked internally.
2. Operations such as grant voucher take ~20 minutes while screen is frozen.
3. Any operation / update related to rule base fails in the classic UI and takes a very long time in newnox.

Decisions / AIs:

1. Stuck threads:
    a. **Vadim** to check option to enable hot swap and provide instruction to Blum.
    b. OTS will be released during Sukot and to be implemented in Amdocs with follow up session.
        i. **Blum** to coordinate deployment
        ii. **Vadim** to allocate Oleg as required for deployment, follow up sessions and fixes
2. **Blum** to review grant voucher issue with customer on Thursday, take logs, open a TFS and communicate to Vadim (and Alex Ryzhov) - no longer exists
3. **Blum** to review rule base performance issues with customer on Thursday, take logs, open TFS and communicate to Alex Ryzhov

2018-10-24 Amdocs management meeting

Wednesday, 24 October 2018 15:41

Participants:

Amdocs:

David (owner), Ronen (manager) - Responsible for Portnox
Daniel, Michael - Security team
Golan Remi - VP

Portnox:

Idan Blum - Support and Technical Services manager
Ofer Amitai - CEO

Summary:

Amdocs:

- System installed over 1 year
- Very good service, listening and provide patches but still system is not functioning
- Enforcement planned for Aug.

Portnox:

- DB issues delayed beginning of project until resolved
- Vignesh disappeared and replaced by Vipin after 3 weeks
- MS monitor agent delayed project until was disabled but recently found to be enabled again

AI:

- Amdocs to provide updated excel with priority and indication if show stopper
- Management status update every 2 days until going into enforcement
- Stop MS Monitor Agent to verify impact and allow going into production asap.
  Amdocs stated they are not the only organization to use MS Monitor Agent and thus this should be resolved
- Compliance checks agreed to be none show stopper with lowest priority as it was set for phase 2

2018-10-31

Wednesday, 31 October 2018 11:10

Schedule session with Amdocs monitoring team to investigate MS Agent Issue

- What needs to be monitored
- How it is done
- What configurations are available
- Amdocs to update time (mid November)
- Will be tested on 1 server and once resolved

Pending session to align servers (IL6 and IN7)

2018-11-13

Tuesday, 13 November 2018 12:44

- Server 1:
  - Registry settings:
    HKEY_LOCAL_MACHINE\SOFTWARE\AccessLayers\PortNox\DeviceDiscovery
    FirstProbeMaxTime Need to change to 120 and then 60. This parameter regulates maximum wait time (in seconds) for first probe for switches with connectivity problems
    InitSwitchPingTimeout Need to change to 5000. This parameter regulates maximum wait time (in milliseconds) for tcp ping to switch on first probe
  - switches disabled to allow service start:
    10.19.18.81
    10.19.18.82
    10.19.18.137
    10.19.18.145
    10.19.18.146
    10.85.0.100
- Action items:
  - Change default server
    Server 1 is most loaded and thus should not be set as default (possibly 8 will be good for default)
  - Continue finding the problematic switches where partial communication causes the service to be stuck and eventually restart
  - After services are up. Install new OTS version already released to handle thread issue and switch timeout settings in NG Experience.

2018-12-26

Wednesday, 26 December 2018 10:30

19/12/2018 - Conference call

Agreed to work together on resolving issues found.
Define 2 initial sites to go into enforcement.
Amdocs expect Portnox to be on Amdocs site to work with Amdocs personnel in Amdocs offices.

20/12/2018 - Call between David Friedman (Amdocs) and Idan Blum (Portnox).

Amdocs does not have a technical project manager allocated for the project at this time and thus request Portnox to do whatever is needed. Allocation is being checked internally at Amdocs and answer expected next week.
Amdocs person allocated for the project is Vipin who is working from India and thus there is no need or benefit for Portnox to be on Amdocs site.
Due to holidays, Amdocs will be available only on Dec. 26.

26/12/2018 - web session

Participants:

Amdocs: Vipin
Portnox: Idan Blum, Vadim, Oleg

Summary

- Thailand have issue with local support thus replaced by China for first sites to set enforcement
- 2 sites to set enforcement
  - China BMCC
  - Malaysia
- Current status
  - China BMCC:
    - 3 Switches are configured in Portnox
    - 66 devices (46 rogue)
    - Search threads running for a long time (investigated by Portnox R&D)

Action Items for next session (Monday, Dec. 31)

Description	Impact	AI	Owner	Comment
Portnox switch configuration	None blocking	Verify all switches are configured in Portnox for both sites	Amdocs	Vipin
Many rogue devices (IP Phones)	Blocking	Verify IP Phones configuration and authentication	Amdocs	Vipin to handle with local team
Search threads	May block	Analyze to locate root cause (bug/environment/3rd party)	Portnox	Portnox R&D
Amdocs technical PM	None blocking	Allocation	Amdocs	

2018-12-31

Monday, 31 December 2018 10:13

China BCC

- 3 switches
- 50-60 devices computers and phones
- 5-6 IP Cameras and Printers
- Printers, Cameras and IP Phones are on the wrong vlan and set with static IP thus cannot be changed to correct vlan
    - Vipin to work with local team to change to DHCP and update to correct vlan
    - Possible temporary workaround if Vipin is not able to resolve is to set voucher for these devices until issue will be resolved
- IP Phone stuck in not authenticated
    - Issue found at vlan configuration in Portnox fixed

Malaysia

- 4 switches, 80 devices (15 rogue devices)
- 10.220.204.210 has no communication in Portnox. Checked manual ping from Portnox server 3 and ping times out.
- 15 rogue devices need to be checked
- Some devices (all are voice) are stuck in Not Authenticated. Verify voice VLAN is defined as voice in Portnox and devices IP subnet is defined for the vlan. Pending check and log analysis.

Server 03

- Performance is very low. Search in files is very slow (local disk read is at ~1MB) although resource consumption is not even at 50%.
- Portnox services are running with no issue. Threads are running without any issue.

Server 02

- Portnox services are running with no issue. Threads are running without any issue.

Server 01

- Services are running, no apparent stuck threads pending additional health check for verification

Scheduled another session for 01/01/2019 but was cancelled to Amdocs request.
Idan Blum will not be available until 13/01/2019 and Jehuda will take over during this time.
Vipin and Jehuda to schedule upon next availability.

Action Items for **next session**

Description	Impact	AI	Owner	Comment
Portnox switch configuration	None blocking	Verify all switches are configured in Portnox for both sites	Amdocs	Vipin
Many rogue devices (IP Phones)	Blocking	Verify IP Phones configuration and authentication	Amdocs	Vipin to handle with local team
Rogue devices (IP Phones, Printers, IP Cameras)	Blocking	Update configuration of devices to DHCP to allow change to correct vlan	Amdocs	Vipin to handle with local team
Amdocs technical PM	None	Allocation	Amdocs	

	blocking			
Switch state down	May block	Verify switch is up and responsive + communication is available between Portnox and switch	Amdocs	Vipin to handle with local team
Server 1 status	None blocking	Verify state of server 1 before future expansion of enforcement to India and US	Portnox + Amdocs	Joint session Amdocs and Portnox R&D
Server 2 performance Performance is very low. Search in files is very slow (local disk read is at ~1MB) although resource consumption is not even at 50%.	May block	Verify Server 2 resources and performance	Amdocs	Vipin to handle with local team

- Reinstall takes a long time in newnox and policies never end loading in classic
- SC is not usable due to communication attempt with all switches defined in DB (none defined in registry)
- Status "Under Authentication" is updated in classic UI only and not in newnox (showing not authenticated until authenticated)
- IP is NA in classic but available in Newnox

2019-01-29

Wednesday, 2 January 2019 13:56

Subject: IT Threats - NAC weekly sync dated 29-Jan-19 Summary

Participants: David F., Raya C., Idan B., Gautam K-V., Vipin T., Michael H.

Summary and Action Items:

1. Vipin walked us throw the latest list of open issues with PortNox that were raised on the meeting dated 24-Jan – see below:

- ~~Vipin: In my past meeting with Yossi on 21st Jan, he had collected the logs. I am not sure if they have relevant data or not. If you need something more, will fetch logs again and share along.~~
  ~~Idan: I have the screenshot and text file with macs but logs zip file is empty. Could you please upload the logs and notify once uploaded?~~
  ~~**AI – Vipin**: To provide the relevant logs to PortNox. **Due date: 30-Jan**.~~
  [Idan] This is part of old system and is NOT part of this project
- Vipin: As I understand, portnox only changes access vlan and keeps voice vlan as it is. What I observed is, ***access vlan*** of port where phone was connected, got moved to phase vlan when enforced, but when rolled back, it didn't change. This is not the expected behavior. Shouldn't the access vlan change back to its original vlan?
  Idan: This is the expected behavior! Changing system to Monitor does not initiate any action. Furthermore, it will actually cause "return to lan" action (return to original vlan) to not occur.
  AI – Idan: ~~PortNox to investigate this phenomena that appears once the system is switched back to Monitoring~~. **Due date: 4-Feb**.
  [Blum] Amdocs to provide logs and details of the 2 incident types for Portnox to investigate
- Vipin: In past, with Vignesh, the enforcement with same write snmp community with view permissions was tested successfully. This time it failed. We will need to check together why it failed this time.
  Idan: Failure is on the switch side and not at Portnox side. Please check with switch support why switch does not allow change with such configuration.
  AI – Idan & Vipin: ~~Check together this phenomena. Results on next meeting~~. **Due date: 5-Feb**.
  [Idan] Portnox to provide OIDs used in Cisco switch integration for Amdocs to work with switch support to allow action on switch
- Vipin: For servers general health, Amdocs server team checked it from their end found nothing. They are ready to have a call with Portnox if you have some recommendations to improve the health from applications perspective.
  Idan: Issue observed at session did not have anything to do with app but rather simple file management operations on server took very long time. Portnox cannot manage, support or provide recommendation for Amdocs servers. It is Amdocs responsibility to verify that the server is in good health and performance.
  ~~**AI – Idan**: To check again the slowness issue, which is defined by Amdocs as a **Showstopper**. According to Idan, the next SW upgrade should resolve the slowness – planned for **mid Feb-19** (Idan will try to be ready earlier for this upgrade – will notify)~~
  [Idan] Amdocs responsible to verify server health. If Portnox will notice the issue recurred, a flag will be raised.

1. Additional items discussed:

a. ~~**AI – Idan**: To provide a process for immediate (urgent) rollback. To be presented on the next status meeting, **5-Feb**.~~
   [Idan] Process of manual rollback explained. Amdocs raised a question for FR of automated rollback. FR to be discussed between Amdocs and Portnox in order to define and raise to Portnox PM

b. Next steps: Target to start China Site Enforcement about 1 week after the next SW upgrade - **~~21-Feb~~** (not final). Actually, the site is ready for enforcement. ~~Just need PortNox stability~~.***[Idan]*** **Amdocs decided to wait for next version with UI performance enhancement so upgrade will not require change request**
c. **AI – Idan**: To provide Amdocs with specifications for establishing a lab. **Due date: 4-Feb**.
d. **AI – David**: To hold an internal discussion regarding the next sites plan for Enforcement, including timelines, and publish. **Due date: 7-Feb**.

1. **Reminder to Yaniv T. / Michael H**.: Please publish the process coordinated with SD and SOC teams for handling rouge devices. It became urgent.

   Next meeting on **5-Feb**.

Tuesday, 5 February 2019 13:08

- Plan by David:
  - No real showstopper except waiting for new version + 1 week to set enforcement
  - After 1 week set compliance
  - After 1 week plan for big site (Gurgaon)
- Weekly meetings required until end of full deployment

- FR: Automated rollback on switch operations due to Portnox enforcement
  - Currently manual selecting all rogue devices and revalidating

- OID for Cisco enforcement actions
- Choose enforcer when adding switch
- Switch does not recover connectivity
- Compliance report per hive (site)

2019-03-27

Wednesday, 27 March 2019 10:06

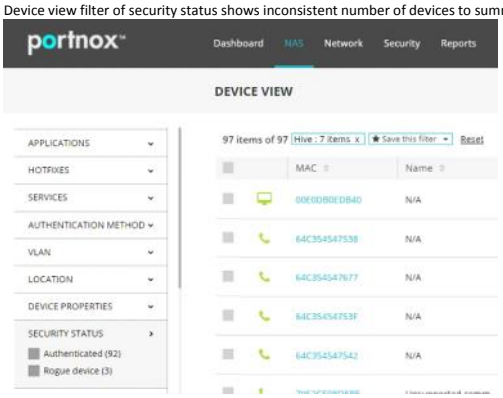
- Server 6 was added to cluster and backup order set for all backup servers
- Server 6 in India is missing it's certificate (different certificates were found installed by Amdocs). Instruction for installation will be sent to Vipin.

Classic UI

- NAS view takes very long time to open (was fast before upgrade)
- Port is displayed in yellow although device not exists / device authenticated
- Policy rule edit never ends (does not open the edit page)

Newnox

- NAS view
  - (BMCC China) Devices stuck on not authenticated - error stating different vlan
    - Subnet belongs to 2 vlans. TFS: Bug 50449:Device is not authenticated when subnet is defined on 2 vlans
    - VLAN subnet cannot be changed from newnox due to duplicate but does not indicate issue (classic shows reason for failure).
- Device view takes 2-10 seconds to open (improved from 2 minutes)
- Open device details - does not open (Open as new tab works). Bug 50026:Endless spinning wheel when access Device details
- Update switch (even deleting disabled switch) takes very long time (several minutes) and ends with exception.
  - Registry: CoreModules->Operator timeout was checked but still takes a long time
    - **Alex to update**
- Servers 5 and 8 are missing from Network page filter even though they have network entities they manage.
  - **Alex to update**
- Switches displayed as offline
  - None are related to current sites in scope.
  - This needs to be checked that switch is responsive to all snmp queries from the Portnox server managing it.
- Security page
  - Sometimes takes several seconds to load
  - Changing policy takes time to update
  - Need logs from server 8 time 10:20-10:30 user: vipint + send to Vadim/Dima
- Device view filter of security status shows inconsistent number of devices to summary:



  - Alex explained to customer it is due to under authentication. Customer and I do not accept it. Needs to show all devices and all statuses
  - Revalidate all rogue devices (50 devices) - takes a long time (couple of minutes) and results in change of device counter in filter 1 by 1. This is **regression** as it used to update all at once and seems to have been broken when added support to action done for large number of devices.

- Server 6 was added to cluster and backup order set for all backup servers
- Server 6 in India is missing it's certificate (different certificates were found installed by Amdocs). Instruction for installation provided to Vipin.
- (BMCC China) Devices stuck on not authenticated - error stating different vlan
  - Subnet belongs to 2 vlans. Once removed from incorrect vlan, **issue was resolved.**
- Device view takes 2-10 seconds to open (improved from 2 minutes).
  - Vipin raised 10 seconds to be too long.
- Open device details did not open
  - Open as new tab resolves the issue.
- Servers 5 and 8 are missing from Network page filter (not impacting current sites in scope).
  - Amdocs to provide logs and DB backup.
- Update switch (even deleting disabled switch) takes very long time .
  - Registry: CoreModules->Operator timeout updated.
- Switches displayed as offline (not impacting current sites in scope)
  - Issue needs to be checked if switch is responsive to all snmp queries from the Portnox server managing it.
- Security page
  - Changing policy takes time to update
    - Amdocs to provide logs from server 8 time 10:20AM-10:30AM
- Device view filter of security status shows inconsistent number of devices to summary:
  - Explanation provided due to temp status such as under authentication.
- Revalidate rogue devices (50 devices) - results in change of device counter in filter 1 by 1.
  - Vipin provided expectations of behavior. Portnox will review and raise to PM.

Additional session will be schedule:

- Assistance with collecting required data
- Assistance to check switches response from Portnox servers
- Investigate port displayed red with no MAC