Small env.

Thursday, October 20, 2016 10:27

IdanK & Ben scheduled for onsite visit on Thursday to take care of the small environment.

Private VLAN

Thursday, October 20, 2016 10:27

Bug 20766 (Elbit): Elbit private vlan support. Contact Asaf to schedule portnox support addition for privet vlan on Cisco – you need to get all info needed from the switch and add it to the TFS. I strongly suggest to ask Vadim for his needs

2016: Virtualized Upgraded Servers

Tuesday, October 18, 2016 09:49

Setup

1. Prepare 2 new Virtual servers with OS, fully patched , according to resources (different IP addresses from production)-plan provided to Elbit
2. Backup existing DB
3. Export configuration and backup registry
4. Set system to Monitor (turn off enforcement)
5. Shutdown production for new virtual servers configuration (eliminate IP conflict)
6. Configure IP addresses of new servers to same IP addresses of old servers
7. Install Portnox with similar existing version on both servers do **NOT** run DB script
8. Update enforcer id for the new servers (DB+Registry)
9. Backup/snapshot new virtual servers
10. Sanity check ++ to make sure things are working properly
11. Freeze period for 2 weeks
12. Expect fine tuning due to use of default configuration (memory, queue, etc.)
13. Monitor performance to validate same/better performance (not worse)
14. Decision point – move on or roll back

Rollback

1. Shutdown virtual servers
2. Restore DB from backup
3. Turn on physical servers
4. Sanity check ++ to make sure things are working properly
5. Set enforcement

Upgrade

1. Backup existing DB (+manual export) + snapshot new virtual servers
2. Upgrade virtual servers to chosen new version (2.4 update3 latest HF or 2.5 latest) depending on status and date
3. Sanity check ++ to make sure things are working properly
4. Decision point – move on or roll back
5. Decide if we want to also move the physical DB server to virtual server.

2016-11-06

Sunday, November 6, 2016 14:21

- Once a week (used to be once a month) there is an issue where devices are blocked by the system using SSH authentication. Occurs on ports with IPPhone (unauthorized hub).
  Restart of the system solves the issue.
- Devices are blocked due to authentication failure with the domain while they are also connected via a different port (portable devices). Deployment Helper succeeds to authenticate.

★ Agreed to meet on Tuesday 2016-11-08. Check and document all issues according to priority and severity + create a plan with periodic followup

Elbit on site visit 2016-11-08

Tuesday, November 8, 2016 18:00

TSN (Alex)
V2.43

1. Unauthorized source and unknown trap
   Fixed in later version
2. Domain auth using second method (WMI after registry) fails
   Fixed in later version
3. In a specific domain, auth using registry fails but when manually retried it succeeds. Changed to rogue immediately.
4. Set VLAN fails (no response from srv). Switch changes VLAN but display is not updated (display is not updated for many actions).
5. (GUI) Choosing VLAN in "Set VLAN" takes very long to display vlan input box.
6. Nortel link up is not triggering portnox. Need assistance to configure Traps filter in Nortel.
   Please following KB article: https://support.portnox.com/support/solutions/articles/8000024988-nortel-passport-snmp-trap-definitions
7. Multiple domains exist in environment and policies are set to hive or vlan so multiple authentications are executed for same device.
   Error received: device is not member of the domain. Device is member of domain X where X is the same domain.
8. Adding unit for an existing switch requires remove+add switch and manually configuring all ports. This is very time consuming and impossible to work this way.
   Feature request raised to product management
9. Login to GUI from a different station and clicking update throws an error for non admin roles
10. Allow VM using role operator is disabled and requires permission to pages which should not be allowed for operator (switch permission)
    New UI is introduced in version 3.0

Shmura (Alex)
V2.43

1. Very small
2. Not in enforce
3. Network is being built and thus much more flexible to new/update configuration

BALMAS (Asaf)
V2.43

1. Load on DB:
   a. Redundant action found by Vadim during probe: (remove mac 120,000, set vlan 17,000, +more)
   b. High queue to DB found during stuck situations
   c. When there is no DB queue / load, the system is working perfect
2. Seems additional server is needed for the cluster:

Ne	Iph	Devices	Ports
140	23	10696	11978

326	35	12526	20878

3. Yellow ports get stuck (uncertain if the issue is due to DB queue or with execution on the device)
4. Service may be down on general operations (disable port, revalidate, etc.).
   Sometimes resolves by itself after a while.
   Sometimes restart is required.
5. GUI is slow and display update takes very long.
6. Fallback fails and auth using second method (WMI/Registry) happens in time (seems when system is loaded)
   Possible fix in v2.5 u1
7. Continue to block port after popup to end point
   Possible fix in v2.5
8. Report filter doesn't work (always returns everything)
   Possible fix in v2.5 u1

Test (Asaf)

V2.5

1. System was stuck and not operational
2. Logs showed constant hotswap
3. Memory configuration was updated from 1.2 to 3.5 out of 4 total as consumption was seen to be 3.4.

Feature requests

1. Expand auth limited: add per hive/location/vlan/etc. to allow limited on different port (both origination and destination need to be in allow change port for auth limited)
2. Add grace/limited for compliance
   Exists in later version using actions of compliance: wait+recheck
3. Script for vlan (instead of private vlan)
4. Add script per port
5. Set resident for device known in system but disconnected from port/not active
6. Allow adding/updating unit/ports

2016-12-07 Upgrade plan

Wednesday, December 7, 2016 18:35

Upgrade process

- Create 3 virtual servers with minimum as defined in **Technical Prerequisites** (verify DB is the same or later version from old system)
- Migrate DB (backup + restore) (logs DB?)
- Install version 2.42 (same as old) on 2 servers (Portnox services stopped)
- Move network elements to new servers
- Move devices from old enforcers to new
- Remove old servers from new system configuration (using cluster util)
- Verify IP addresses, hosts, certificates and licenses
- Set system to monitor (turn off enforce)
- Set all switches to monitor
- Upgrade to version 2.5u1
- Review general configurations
- Install another server in the cluster (3rd server)
- Move network elements required to server 3
- Monitor system
- Turn on enforce for the system
- Gradually move enforcement to new system while monitoring
    - Turn off switch enforce on old system
    - Turn on switch enforce on new system

Technical Prerequisites

Servers Required

- 3 X Portnox Servers
    - 3 for data ports
- 1 X Portnox DB server

Operating System

- Windows 2008/ 2012 64 bit R2 (including the latest service pack and hot fixes)
- Role of Web Server and Windows Process Activation

Portnox Servers + Backup servers – Virtual machine

- VMware or Hyper-V
- 8 CPU
- 12GB RAM
- 150GB free disk space

SQL Server instance

- MS SQL 2014 or MS SQL 2012 or MS SQL 2008
- Access from all Portnox servers to SQL instance
- Configuration Database – 500MB Size
- LOG Database - Database size depends on the retention policy.
  As a rule of thumb we recommend to have 100MB for each 1000 endpoints per month

2017-05-11

Thursday, May 11, 2017 17:44

- Switch down status not updated
- Switch arrow color not aggregated up to hive
- Unauthorized hub showing authorized hub although hub is not defined on port. Port history:
    - Unauthorized hub - many events
    - Authenticated devices - (NAS showing as green hub when port is not defined as hub).

- Trap receiver - default enforcer
- Wrapper log - ghost process EMPTY
- Switch timeout and retry to 20/2
- Query switch properties and IP Helpers related to it
- Unauthorized hub showing authorized hub although hub is not defined on port - could not reproduce in lab

- Check log retention since 14/5/2017

- FP authentication performance is degraded - Bug 29178:REGRESSION - OSFP authentication performance degraded substantially
- Switch is down but showing up - Bug 28011:Switch UP status not updated automatically
- Switch arrow color not aggregated up to hive - Bug 28013:Switch status is not aggregated to hive and above

2018-02-08 - Status

Thursday, February 8, 2018 11:10

Elbit is considering different solution for NAC in order to provide 1 solution in all of their networks and locations.
Alex Puziy is managing and centralizing the requirements.

Requirements:

- 1 system
- Centralized and unified system and system management
- ★ Stability is the most important factor
- Simple and quick to learn
- Flexible:
  - Allow different configurations in different locations/switches (e.g. heuristic engine)
  - Allow different authentications for different networks (802.1x, wmi…)
  - Allow grace for temporary failures (auth and compliance)
- Clear roadmap providing features and dates of release

Feature requests:

- Allow different configurations in different locations/switches (e.g. heuristic engine)
- Compliance limited (similar to auth limited)
- ACL management
- Private vlan (not raised in call)

Feedback about Portnox:

Positive (in order of severity):

- Portnox is simple to use and easy to learn
- Adi & Blum are always available and provide great service
- Critical issues always get the required attention

Negative/constructive (in order of severity):

- Old version was not stable to say the least and required repeated restarts and consumed 50% of Assaf's time
- New system (v2.51) is substantially more stable in a very good way but still has small issues which require occasional restart of a server
- Upgrade / HF is never easy and always requires vendor intervention
- Elbit is afraid to add existing functionality as it may break the system due to load or even the network
- Authentication (WMI/Remote Registry) and compliance checks occasionally fail due to unknown issue (and do not have a grace)
- UI is slow and does not allow ease of use
- Feature requests raised a year ago and 3 years ago were confirmed by Portnox to be good and valid but still no progress
- No clear roadmap
- Service - Elbit expects vendor to see them as strategic customer and to be proactively involved, review system periodically (even weekly), provide recommendation, help utilize additional/new features and adopt roadmap/solution/product to their requirements.
- None critical issue take a bit longer than expected (Alex small closed network only)

Elbit stated that it is not a lost cause and they are happy to raise are attention and will happy to meet.

Adi, please schedule a meeting with all recipients to discuss the above no later than next week.

2018-03-20 On Site visit

Tuesday, March 20, 2018 10:31

Guy Kopel (IT systems in abroad sub companies), Dima, Assaf, Alex, Moti
Omer, Idan K., Adi, Idan B

- Australia, Brazil, UK (Manchester), USA (Boston), Romania
  - Currently different domains, isolated but connected via site2site VPN in "subs" network
  - Roadmap to consolidate network and systems
- Central management (policy, rules, etc.) but locally enforced (in case of communication lost)
- Data center is in IL managing all sites

- 1 year ago, Portnox moved to new infrastructure and to virtual. Since then status is better but still requires some handling and monitoring (weekly instead of daily).
  Requirement is for the system to work without the overhead resources it currently requires.
  - Service stuck, multiple events without automatic changing to monitor mode.
  - System is consuming a lot of Assaf's time. Beyond the acceptable time.
  - Most events are of legit devices being blocked (false-positive)
- Email from 2016 raised items which all were confirmed by Portnox (Omer and more). Some were addressed but some still not.

- 802.1x is raised by malmab due to security requirement (for highly secured networks)
- 802.1x provides functionality that simplifies some of the operations (vlan assignment, moving devices…)

- In the past 6 months, system wide event happened 4 times
- To release the network and allow work, system is immediately restarted and logs investigation takes a long time and sometimes impossible.
  - Omer:
    - Thread handling mechanism/engine was rewritten to better manage and handle threads
    - Improved switch connection management
    - Constant improvement. Will continue to improve upon issues raised in weekly/bi-monthly/etc. status meetings
- Remediation needs to be executed automatically. User should be blocked as a last resort.
  - Omer:
    - VLAN remediation - need to understand the 2-3 exact scenarios solution is required
  - Compliance limited option raised to allow less strict policy and to continue blocking rogue devices but allow legit.
  - Less but still have noise due to authentication limited mechanism but is missing in compliance.
    - Omer:
      - Compliance state is definite thus allow Portnox to address issue and react accordingly
    - Assaf:
      - Event in compliance we see false positive (not due Portnox false)
    - Omer:
      - McAfee EPO allows sending Portnox alert/raise event of device not updated
- In secured areas, block is required immediately (before IP is received) - not possible in Portnox core
- ACL to deny 2 devices in same vlan from communicating between each other. e.g. private vlan /

deploy ACL at port (dynamic ACL)

- Dynamic VLAN is supported
- [ ] Resident/black list - device must be connected in order to add/remove from list. Need to allow offline device handling.
    - Omer:
- [ ] Voucher to device also requires device to be connected. **REGRESSION**
- Automatic identification of switch change (stack unit addition, etc.)
    - [ ] Omer: will check
- Support for new switch or switch OS
    - Needs to be raised to Portnox each time
- Upgrade requires Portnox engineer.
    - Always was complex and local attendance of Portnox engineer seems too heavy.
    - Requirement: improve upgrade process to not require Portnox resource and not be so stressful
- Expect to see Portnox as proactive. Vendor or Portnox.
    - Verify system version is up to date
    - Update about versions, new features, etc.
    - Expect to receive personalized notification regarding version upgrade (recommended to Elbit, known issues, etc.)
- Issue handling when logs cannot be sent or remote connection is not allowed
    - Blum: Integrator + raised to Portnox in cases where integrator is not capable
- HA/Cluster - proper solution
    - In roadmap
- [ ] Emergency Enforcement/Monitor change (red button)
- [ ] Respond to SOW document

- [ ] Immediate need for integrator in Melbourne (within less than 1 month)
- [ ]

2018-10-29 On site visit

Wednesday, 31 October 2018 16:00

- Elbit had a POC with ClearPass and Forescout
  - ClearPass provides good solution for their wireless but not for wired. They will keep using it for their wireless.
  - They were very impressed from Forescout and are replacing Portnox with Forescout in their small (secured) network managed by Alex
- Test environment (Windows 2012 R2) was upgraded to v3up2hf3
  - Their servers are not updated with Windows updates which required several Microsoft KBs installation in order to install .net framework 4.6.2
  - Blum to send Assaf link KB regarding installation on Windows 2016
- New switches: **(Blum need to check in Test env with latest version and open TFS if needed)**
  Purchased Arista
  In process of purchasing new switches. Considering and need confirmation of support for the following:
  - TP Link: T1500G-10PS
  - Netgear: MS510TX (or TXPP)
  - Netgear: GS105E (or EP), GS108E (or EP), GS116E (or EP)
- Follow up and new issues raised:
  - System still requires restart from time to time. Elbit usually restart before the system is stuck as they notice that memory usage of Portnox services increases to high usage.
  - False positive is still noticed and worked around by utilizing Authentication limited and removing heuristic engine. This is a workaround and is not accepted as a permanent solution.
    - Due to other issues raised this was not deeply investigated.
    - It was noticed that their IPPhones start in management vlan to pull configuration and then move to tagged. This causes the de vice to be authenticated limited if authentication starts before vlan change.
      Solution: Allow IPPhone on management vlan.
  - OTS version pending release will be installed on test environment.
    Prod installation is pending confirmation of stability from installations at other customers
  - FR: Compliance Limited is in design and will be developed and released per Elbit specific request. **Bug 40826:Compliance limited - allow grace for devices to complete compliance product update**
  - ACL solution for blocking communication between different elements within the network - relevant for small network (Alex) which is replaced with Forescout.
  - Remote sites solution
    - There are remote sites which have bad communication with high latency and interruptions. They cannot rely on a solution that requires constant communication from IL to remote sites.
    - FR: (exists at competitors) - **Bug 44945:Centralized management for isolated systems**
      Manager of manager allows deployment and management of policies from a single UI while all operation (monitor and enforcement is executed on local network only.
      Status is still available in the centralized UI.
  - FR: Private VLAN - **Bug 33342:Add support to change vlan on Cisco configure with private vlan**
    There are 4 required enforcement actions relating to set vlans:
    - From vlan to private vlan
    - From private vlan to another private vlan
    - From private vlan to vlan
    - From vlan to another vlan

    Assaf will provide details and commands to configure switch with primary vlan and 2 associated private vlans (verify type com munity or isolated) or as well as the commands required to change private vlan
  - Dynamic vlan to be implemented once issues resolved at test (**Blum to deply**)
  - Development request:
    - Ability to control access (not just read/admin) to setup/configurations. **Bug 44946:Newnox UI should include option of "None" in permissions of system configuration**
    - Ability to allow group of users to set system enforcement on/off only (without ability to see any other configuration) **Bug 44961:Newnox break down permission for configuration**
    - External application somewhat similar to Portnox monitor traffic light which after login indicates current enforcement status and allows disabling/enabling.
  - Lost functionality of executing action on a device that is not currently connected.
    e.g. adding a device to block list or removing voucher should not require the device to be connected at time of action **(check TFS as this was set for Q4 2018) Bug 44962:Allow actions on device when device is not connected**
  - FR: Automatic detection of switch change (e.g. added unit to a stack). No plan at the moment. **Need to raise to Tomer. Bug 11597:add the ability to identify adding new unit to switch stack automatically without the need to remove / add the switch**
  - Define periodic visits of PS at Elbit **(Blum to close with Adi and Assaf)**
  - New UI issues:
    - Filter of devices with voucher shows devices which had vouchers (expired/revoked) **Bug 44963:Devices view filter by voucher shows devices with revoked voucher**
    - Cannot set permissions for device revalidate **Bug 44964:Newnox missing ability to set permission for device revalidate**

2018-11-19 On site with Tomer

Monday, 19 November 2018 11:04

- Break point was when following an upgrade a bug caused hubs to be blocked as unauthorized hub and required manual granting of vouchers in public locations (conference rooms).
  This was the point of no return which created a stain in Elbit for Portnox which never went away.
- This created a feeling where Elbit is afraid of upgrading and experiencing new (regression) bugs
- Feature requests raised were not attended
- Monitoring system: Solarwinds
- Secured network required NAC with 802.1x and thus Forescout was chosen
- Clearpass exist on the wireless (guest + employee internet). No wireless exists in any of the internal networks (secured or none secured)
- Portnox advantages:
  - Simplicity of operations
  - Ease of operability for IT staff (understanding location of device/switch, etc.)
- Features required and pending proof by competitor (and afraid these will cause load/issues in Portnox):
  - Dynamic vlan
  - Automatic remediation
  - Change comp vlan without disconnecting phone (now open for discussion about Agent)
  - DR
- **Management targeted unified system across all Elbit network**
- **Assaf's network is pending budget approval for 2019 and understanding of implication to deploy a new system**
- **Current plan exists for upgrading Portnox**

Summary by Tomer:

Hi

Idan B. and I met Assaf from Elbit today.

Here is a short summary of the meeting and some conclusions:

- Meeting was very open and sincere. Assaf explained what happened in the past few years that contributed to our bad reputation, especially in the cyber team.
- Current version installed (2.5.1 HF11) is much more stable but still requires some attention (restart every couple of weeks).
- They chose FS for their 'classified' network and started to deploy it (he said it is mainly for their requirement to move that network to 802.1x, so maybe FS 802.1x support is not that bad).
- They also performed a pilot with FS on non-802.1x for their Large network (Balmas) and were happy with the results.
- In general, there is a directive to go with a single NAC solution.
- Although their networking team loves our product simplicity and daily operation (better than FS), their cyber team is presenting more and more requirements that are already supported and demonstrated by FS (Manager of managers for their growing remote branches, built in integrations with various 3rd party solutions, IoT, VLAN switching without disconnecting the device using an agent etc.)
- In general, their cyber team is taking the lead so maybe in the future, we should meet them as well (this is the team that thinks Portnox is a bad product due to past issues).

- A decision **was not** yet made to move to FS for the large network. It is mainly up for budget discussions. And even though from a feature-set perspective, FS are leading with flying colors, the budget aspect could kill it or postpone it to 2020. This is why Assaf still has plans to upgrade our system there in 2019 (with new UI training sessions to all field guys).

  Personal conclusion – adding one or two FR per their requests will not change the game (e.g. compliance limited, private VLAN, manager of managers). From a feature-set and reputation perspective, we already lost to FS (also in the non-802.1x comparison). HOWEVER, as the budget is a big driver, if we make the system stable and include the 2-3 high visibility defects, we could upgrade the system soon and make them happier….. Maybe happy enough to renew our solution for another year and postpone FS implementation. In the long run – if we want to stay in the game – we need to support features suitable for XL customers.

  Top priority items:

1. Stability (OTS- already in testing in Amdocs)
2. New UI privilege granularity (they have it today in classic UI and will not upgrade the system without it) – We will need to see why it was removed from NEWNOX.
3. Allow actions (black listing) on offline devices (currently planned to be fixed in HF5).
   The rest of the items below (including the false positive authentication limited) are not considered high priority.