AgentP roll out proc

Tuesday, August 28, 2018 13:02

Below you will find the general process for Change Management related to AgentP. Please confirm that we are good to go with this. Thanks.

General

1. Victory will be notified when a new build of AgentP is available
a. The MSI file will be supplied
b. Release notes to be supplied alongside; an informal list of changes/fixes/enhancements is fine as well
2. Victory will test the new version and roll-out to a controlled group (20 or so users)
3. Victory will run the new version for a period of up to 2 weeks to ensure there are no introduced issues
a. Victory may choose an accelerated roll-out if there is a fix or enhancement that is desired in a quicker timeframe
4. Victory will inform Portnox once we are ready to release the new build to all users

Deployment

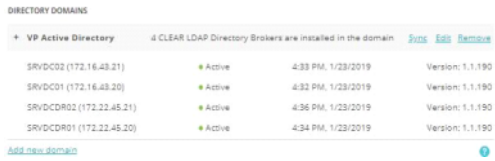
1. The roll-out will be performed via GPO by Victory
2. Cloud-based updates should never be enabled until Victory notifies Portnox that it is ready to roll out the new version
a. Is it possible to disable the cloud update for us?
b. We are OK with always deploying via GPO as it gives us the control we are looking for

2019-01-23

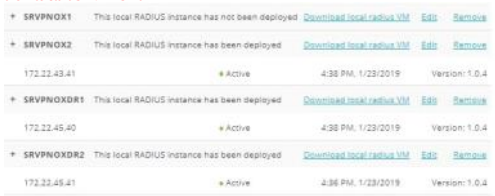
Thursday, 24 January 2019 11:33

Current VP settings: Weds Jan 23 – 2019

VP Adbroker DC servers:



VP Local Radius: SVPNOX01 looks to be down currently → Gord to contact VP and get them to start SRVPNOX01



Victory Packaging utilizes Portnox Clear for VPN, Wireless and Wired Validation.

Four Local Radius Servers are configured at Victory Packaging.

SRVPNOX1 – 172.22.43.40
SRVPNOX2 - 172.22.43.41
SRVPNOXDR1 – 172.22.45.40
SRVPNOXDR2 – 172.22.45.41

Adbroker is installed on Four Servers at Victory Packaging.

SRVDC01 – 172.16.43.20
SRVDC02 – 172.16.43.21
SRVDCDR01 – 172.22.45.20
SRVDCDR02 – 172.22.45.20

Houston - DR External NAT - 65.121.169.66
Phoenix - Production External NAT - 67.128.161.51

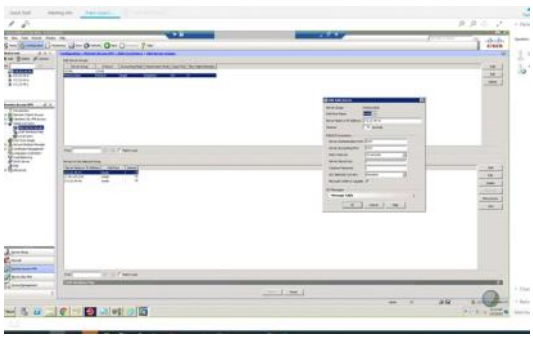
Portnox CLEAR Radius:
USA - 13.90.229.234 Auth port 10132 Acct port 10133
Europe - 52.232.122.157 Auth port 10006 Acct Port 10007

VPN in use - Cisco AnyConnect

Summary of issue:

1) VP identified "AgentP strong factor validation timeout" on **Oct 31 – 2018** - at that time the default VPN connection was via their production ASA 172.23.43.5 which pointed to Local radius 172.22.43.41 as primary Local radius .
   a. Phoenix - Production External NAT - 67.128.161.51
2) This issue was re-identified by VP on Dec 11 2018 when VP changed to route all VPN users to connect to Houston DR(Disaster Recovery) ASA 172.22.45.31 using local radius 172.22.45.41.

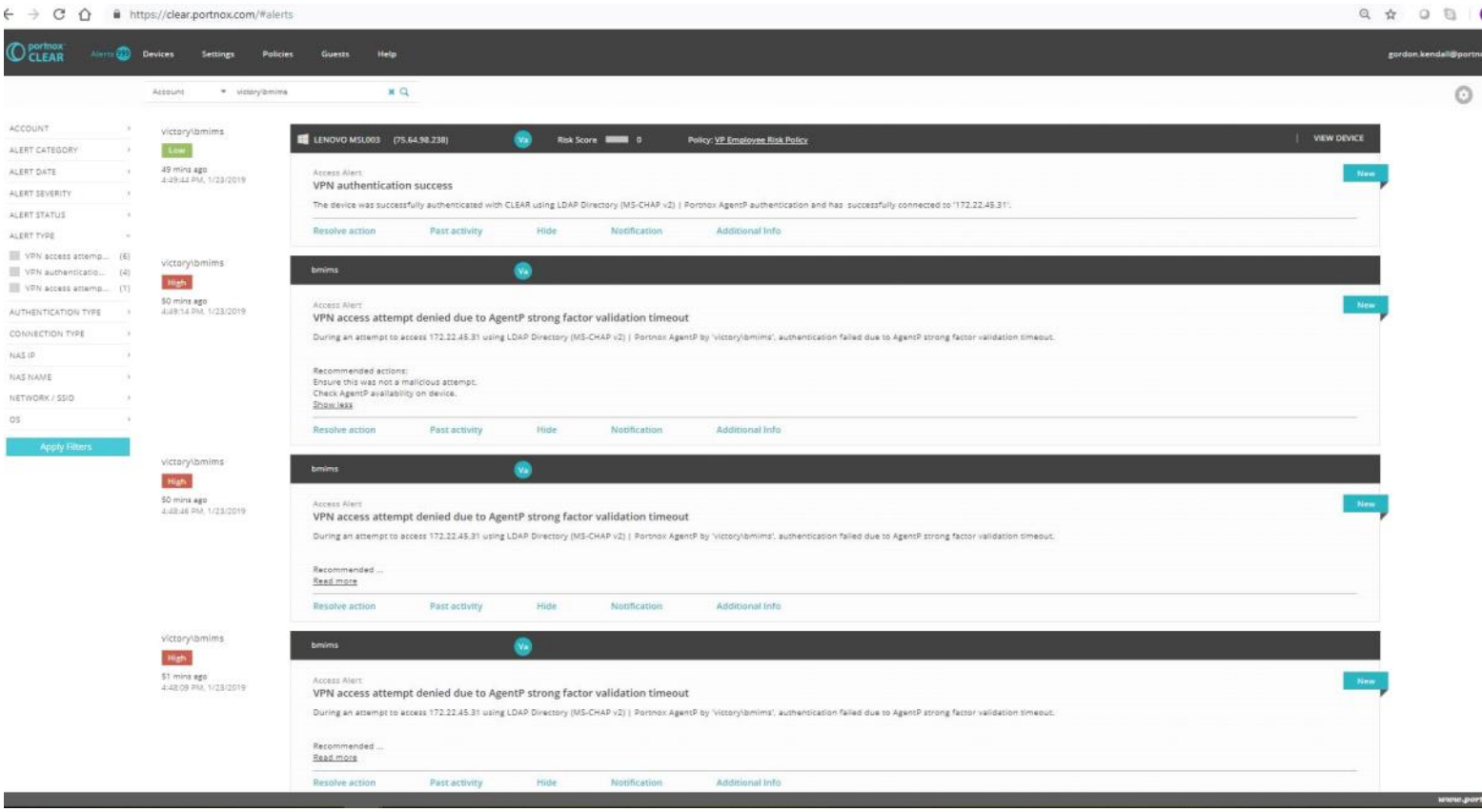
a) Houston - DR External NAT - 65.121.169.66



   a. VP switched to DR as default VPN concentrator so they could deploy Force Point VPN as production VPN and migrate all users to the new Force Point VPN from the Phoenix location.

Victory Packaging VPN Connection Flow– Jan 23 – 2019 :

1) Client device initiates VPN connection request -→ to Houston DR ASA
2) Houston ASA forwards to Portnox Local radius server 172.22.45.41 (Local Radius should be in Houston) (timeout=75 seconds).
3) Portnox Local Radius server relays request to Portnox Cloud Radius – North America 13.90.229.234
4) Radius request makes it to the Portnox clear services and times out on AgentP validation (sometimes? Or at least a message is generated?)
5) Notification email is sent to Victory packaging administrators and to VP end users causing concern.
6) Connection may or may not be successful regardless of "AgentP Strong factor validation failure" message
7) After a few retries (multiple minutes) user is authenticated.


https://clear.portnox.com/#alerts
portnox CLEAR
Devices
Settings
Policies
Guests
Help
ACCOUNT
ALERT CATEGORY
ALERT DATE
ALERT SEVERITY
ALERT STATUS
ALERT TYPE
AUTHENTICATION TYPE
CONNECTION TYPE
NAS IP
NAS NAME
NETWORK / SSID
OS
Apply Filters
victory\bmims
Low
49 mins ago
LENOVO MSL003 (75.64.98.238)
Risk Score 0
Policy: VP Employee Risk Policy
VIEW DEVICE
Access Alert
VPN authentication success
The device was successfully authenticated with CLEAR using LDAP Directory (MS-CHAP v2) | Portnox AgentP authentication and has successfully connected to '172.22.45.31'.
New
Resolve action
Past activity
Hide
Notification
Additional Info
High
50 mins ago
bmims
VPN access attempt denied due to AgentP strong factor validation timeout
During an attempt to access 172.22.45.31 using LDAP Directory (MS-CHAP v2) | Portnox AgentP by 'victory\bmims', authentication failed due to AgentP strong factor validation timeout.
Recommended actions:
Ensure this was not a malicious attempt.
Check AgentP availability on device.
Show less
51 mins ago