Global Information Assurance Certification Paper

Challenges to Implementing Network Access Control

GIAC GCIA Gold Certification

Author: Joseph F. Matthews, joseph.matthews@pccairfoils.com
Advisor: Dave Hoelzer
Accepted: August 23rd 2017

Abstract

Network Access Control had always offered the hope of solving so many network security problems but has proven quite difficult to implement. NAC was to solve the issues of visibility, control, and compliance enforcement. This paper seeks to demonstrate through research and implementation an effective and practical way for small to medium-sized businesses to move to NAC and take advantage of the security benefits of a 3-6 month implementation plan.

1. Introduction

1.1. NAC Explained

Designed to improve security on networks, Network Access Control, also known as NAC, restricts access and resource availability to only authorized devices. Many companies use NAC to manage guest and contractor access. NAC provides data and resource restriction aiding in meeting compliance requirements. Additionally, NAC pushes organizations to have a complete device inventory for asset management ("Network access control: Security advice for enterprise CIOs," n.d.).

The basis of this paper, including the research and the elements presented, is based on real-life testing and Proof of Concept (POC) implementation within a singular environment with long-term planned deployment across the company. The POC will determine the feasibility of implementing each proposed NAC solution. The scope of this research is an analysis of the selections, considerations of the preferences within this environment, to show why these decisions for a NAC implementation might be beneficial elsewhere. Where possible and practical, implementation steps and instructions will be included to aid in successful duplication and implementation of the NAC technology.

1.2. History of NAC

NAC was originally just an authentication technology solution and now has advanced to become a security integrator. Bradford Networks' white paper, "The Evolution of Network Access Control," states that NAC has evolved into a broader Security Automation and Orchestration (SA&O) solution. Companies are facing stronger regulatory requirements such as HIPAA, SEC/SOX, PCI DSS, and others. These requirements include strict network access control and data protection. Companies must secure all endpoints or possibly face hefty fines that can reach millions of dollars per violation; this can be achieved through the utilization of NAC. Figure 1 below, shows the evolution of NAC graphically. NAC 1.0's focus was the onboarding of company owned devices. NAC 2.0 focused on network protection while allowing the use of BYOD (Bring Your Own Device). NAC's current phase of evolution into an SA&O now coordinates endpoint visibility, control, and automated response to reduce threat response time.

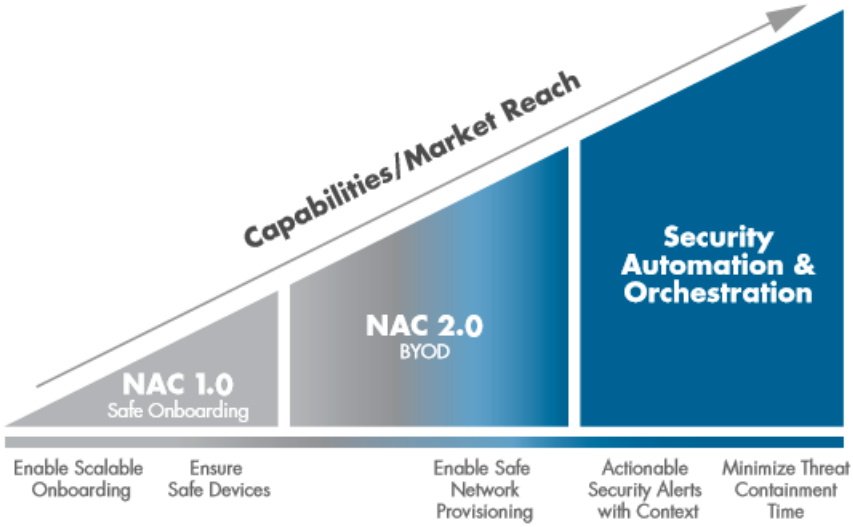

Figure 1: Evolution of NAC

The new SA&O systems verify the user and device identity and check the system for risk. Then, the systems will assign network rights based on predefined policies as shown in Figure 2. The four levels shown are No Access, Guest Access, Restricted Access and Unrestricted access. The SA&O system periodically re-verifies the risk level and automatically adjusts the devices access level based on the risk.

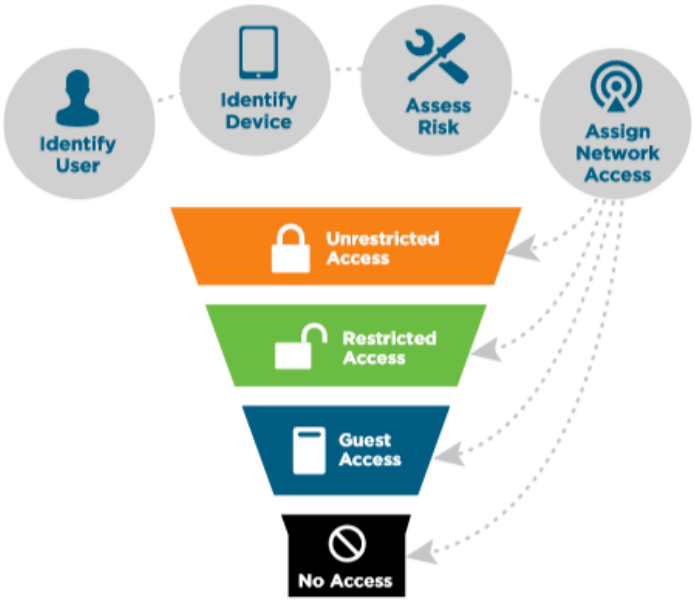

Figure 2: Trust-based policies

NAC has evolved from an authentication solution into an advanced security integrator solution. BYOD and IOT have forced the growth and the need for automation provided by an SA&O system.

2. Implementation

2.1. Requirements

The Center for Internet Security (CIS) Critical Security Controls Version 6.1's, Control Number 1 is Inventory of Authorized and Unauthorized Devices. The control recommends to "actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access" ("Center for Internet Security," 2016). NAC is one solution to the implementation of Control Number 1. Figure 3 below shows Control Number 1 and its recommended steps.

Critical Security Control #1: Inventory of Authorized and Unauthorized Devices		
System	1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.
System	1.2	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.
System	1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
System	1.4	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.
System	1.5	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.
System	1.6	Use client certificates to validate and authenticate systems prior to connecting to the private network.

Figure 3: Critical Security Control #1

The requirements for the Proof of Concept NAC implementation include:

- 100% view of all devices on the network, or ones attempting to connect to the network
- Central management of the NAC solution
- Ease of use through automation
- The solution cannot be labor intensive
- Granular rule enforcement and control
- Automatic onboarding of new systems and guests
- Confirm compliance control of company owned equipment
- Must be able to handle printers, IOT, BYOD, VoIP, etc.

2.2. Vendors

The three vendors picked for evaluation are Portnox, Cisco and Bradford Networks. Each vendor offers differing approaches to the Network Access Control problem and represents different quadrants of the Gartner Magic Quadrant report as shown in Figure 4 below from 2014. The Gartner Magic Quadrant report is based Gartner's research and ranks businesses based on "Completeness of Vision" and their "Ability to Execute" their proposed solution.

Figure 4: Gartner Magic Quadrant for Network Access Control

2.2.1. Portnox:

Founded in 2007, Portnox (http://www.portnox.com/portfolio/nac/) is a vendor that is focused solely on NAC solutions that operates mainly in the Americas and EMEA. Portnox offers a solution that is agentless and based primarily on endpoint discovery. After a device connects to the network, Portnox checks the OS type. Then Portnox applies the appropriate policy to the network access point – for example, a port on a LAN switch, a WLAN controller or a VPN gateway.

Portnox Clear is Portnox's cloud-based offering. Portnox Core is their on-premises solution. Portnox Clear enables cloud deployment of 802.1X, including RADIUS server and certificate authority functionality. The Clear app runs on Windows,

IOS, Android, and macOS. Clear includes an onboard configuration for 802.1X supplicants. A supplicant is software required on endpoints that allow them to participate in the 802.1X authentication process. It also calculates a risk score for devices based on attributes, including applications, encryption, open ports, and updates. Clear operates as a standard/simple app and not an MDM profile; it allows administrators to identify the device, its owner, its compliance status. Clear also allows administrators to see all visited Wi-Fi networks. The Core solution can also enforce NAC policies in wired, wireless VPN, VMware environments. Core monitors and graphically represents the number of VMs in use, as well as policy enforcement for these VMs by blocking or allowing access to virtual switches. Portnox Clear and Core support visibility, control and management of all devices and users in the network. (Neiva & Orans, 2017)

Portnox proposes a solution to NAC with implementation at the switch and wireless controller level instead of requiring a supplicant. Since a supplicant is not required, fewer device resources are utilized. Portnox Core Solution creates a template of each item and aligns it to a signature. Therefore, 802.1x is not a requirement for their proposed solution. The licensing model of the Core product is determined by the number of ports monitored, not by the number of endpoints or devices connected to the environment. Compliance verification for the company-owned computers is through WMI calls. Core requires an account with enough rights to collect WMI information. An additional requirement is the Portnox Core manager must have access to all computer systems to extract the compliance information. The Portnox Dashboard shown below in figure 5 is the initial information screen within Portnox Core. The dashboard contains information on the number of switches, ports, access points, management segments, virtual switches and failure events within Portnox Core.

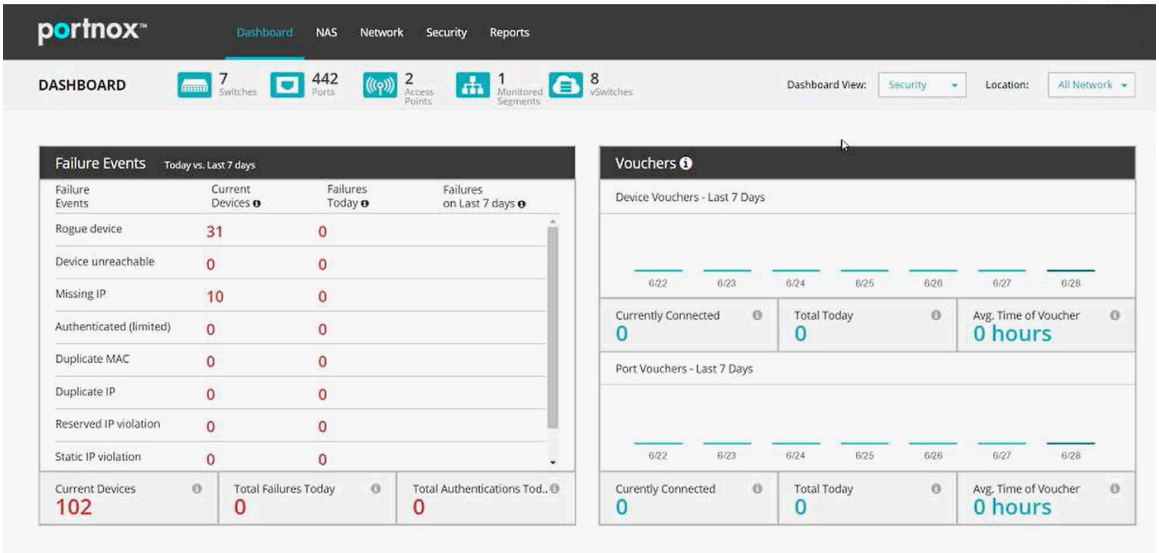

Figure 5: Portnox Dashboard View

2.2.2. Cisco:

Cisco Identity Services Engine also is known as Cisco ISE is located at (http://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html)(ISE). ISE is a policy server that is RADIUS- and Terminal Access Controller Access Control System Plus (TACACS+)-based, allowing Cisco to support authentication and device administration in heterogeneous network environment. ISE is available on two platforms hardware appliances and virtual servers. Their profile feed service updates the device-profiling capability. Profiling provides endpoint classification and reports on devices connected to the network.

Cisco ISE uses the pxGrid framework, allowing ISE to integrate with Cisco's security products and third-party technologies. Cisco packages its NAC posture agent with baseline capabilities in its AnyConnect endpoint bundle. The agent aids in the unification of additional capabilities, such as VPN, NetFlow, MACsec, Supplicant, Cisco Umbrella and Advanced Malware Protection (AMP). Certificate authority ability and Active Directory multi-domain are new capabilities within ISE. (Neiva & Orans, 2017).

Cisco's offering of ISE is very complex and robust; companies can add modules and additional integration points to enhance the product. As with most Cisco products, each additional items or additional functionality added requires an additional license.

Their “Base” license allows device authorization to utilize ISE. For printers that do not support a supplicant the addition of a "Plus" license is a Cisco license requirement. For endpoint compliance, the initial "Base" license and an additional "Apex" license is a Cisco requirement. Below is Cisco ISE's console view, it contains several items including a system summary, endpoint breakdown, how many authentications are occurring and how many network devices ISE is managing. The view is customizable per user; this allows a network admin to tailor their view differently than an incident response team member.

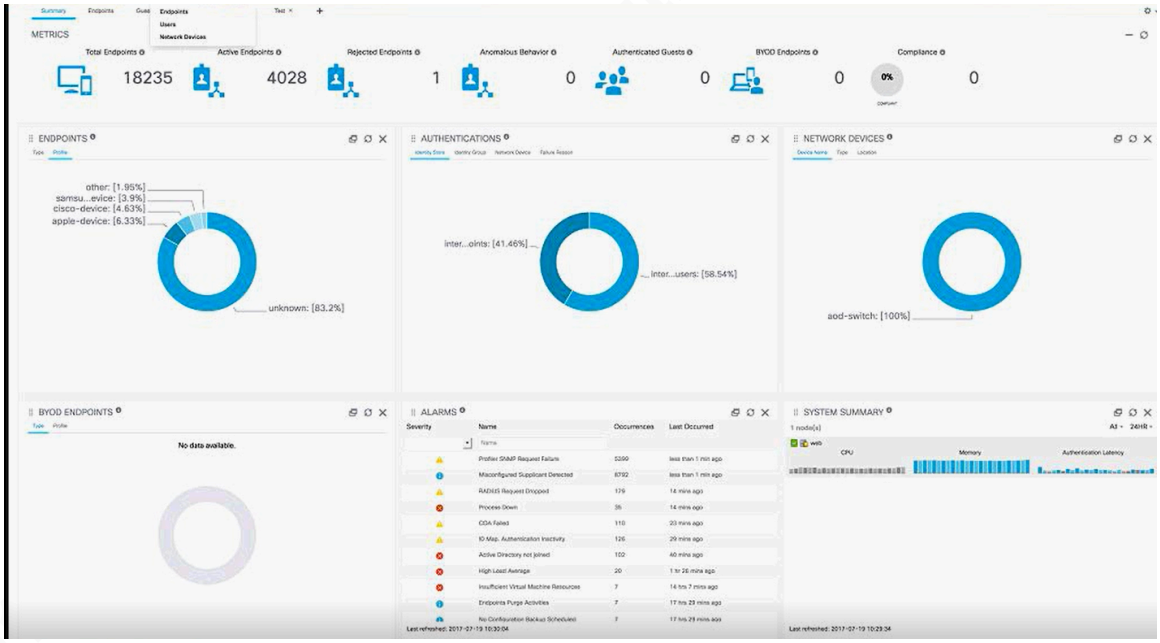

Figure 6: Cisco Console View

2.2.3. Bradford Networks:

Bradford Networks is based in Boston and is a privately held company. Bradford has been delivering NAC solutions since 2001. Network Sentry is their premier product. More information is available at (https://www.bradfordnetworks.com/products/network-sentry/). Network Sentry is a RADIUS-based solution available in hardware, virtual appliances and as a cloud service. Network Sentry comes in three versions – Secure Enterprise Advanced (SEA), Secure Enterprise Response (SER) and Secure Enterprise Premier (SEP). All three version include the ability to share contextual information about endpoints and provides tools for security analysts to respond to alerts. Their SEP product

includes Automated response workflow. Bradford Networks' also offers a mobile application that can perform limited mobile device management (MDM) capabilities. It includes jailbreak, device and OS detection.

Bradford added integration with Tenable in 2016. The integration with Tenable allows sharing of vulnerability data with Network Sentry's correlation engine. The integration helps by increasing the number of trust factors and assigns priority to enforce policy-based threat containment. Sentry and Cyphort are integrated, which enables automated malware analysis, and threat triage and response. Network Sentry's security parser supports many third-party security solutions. Bradford Networks is securing network and facilities infrastructure devices on top of a myriad of vendor network switching environments. (Neiva & Orans, 2017).

Bradford Network's solution is similar to the Portnox solution; a connection to all switches is one requirement. Network Sentry polls and collects connection information via SNMP. To manage and control port access, Network Sentry uses Secure Shell Version 2 (SSH2) and Command Line Interface (CLI). Endpoint inventory and classification occurs by fingerprinting the devices. MDM, AD, LDAP integration for additional device information is available. The more information and classification points used, the harder it becomes for an attacker to spoof a device. Bradford also offers a dissolvable agent for BYOD devices. The dissolvable agent is temporarily installed from a web portal; it performs user and device authentication and additional checks. Once the dissolvable agent performs all necessary checks, it uninstalls. No agent or software is left in place on the users BYOD device. Dissolvable agents are used in place of the permanent agent recommended by Cisco, or the WMI calls utilized by Portnox. Bradford Networks Sentry can also collect compliance information by utilization of their executable at login. The executable call integrates into in a login script. Execution time is minimal during the login process. Bradford's use of the login script gives them a slight advantage over Portnox and Cisco because they do not require a known username and password like Portnox and do not require and additional client installation as Cisco does. Below is the Dashboard view for Bradford's Network Sentry. The dashboard contains alarms, network and host summaries and performance information, giving a quick consolidated view of the environment.

Figure 7: Bradford Networks Dashboard View

3. NAC Challenges

3.1. Non-authenticating Assets

Modern NAC solutions utilize profile-based authorization for non-authenticating assets. Full network visibility is the goal; without full visibility, attackers have an open door into the network. All three of the vendors Portnox, Cisco and Bradford Networks take the same approach for non-authenticating assets by classifying a trust level with data that populates automatically and compares the gathered information against the authorization profile.

3.2. Implementation Approach

Companies and organizations should consider which implementation approach is the best for their particular environments by answering the following questions: Will a full implementation of NAC or a phased implementation be the best approach? Would it be best to start with the Guest environment and then gradually bring in other areas, or would it be best to implement fully across the environment? What are the benefits of each? What are the drawbacks of each? What impact will it have on the network and the user base?

Portnox's getting started guide, version 2.5, recommends that regardless of the size and breadth of the network to separate the deployment into several steps. It does not matter if the network is small and composed of just a few switches and a router or if it is a larger enterprise network. The network can be a standard LAN, wireless LAN, or WAN. It could be using public and private cloud or other external services. Virtual servers or VoIP enabled, it does not matter, break it into steps, start with a representative sample and expand from that point.

Bradford and Cisco both recommend implementing their products in a learning mode. Learning mode allows the products to gather all switch information across the environment. After initial data collection, classification of the devices that are connected would occur then the configuration of pre-connect rules followed by configuration of post connect rules. Signature/behavior based activity triggers the post network connect policies, agent and security rules.

All three vendors recommend a phased approach that has minimal impact on the user base. The only drawback would be the time delay in completing each phase. Based on the information and recommendation from all three vendors, a full implementation from day one with full lockdown would create significant disruption to the environment and offer no benefit except an accelerated deployment timeline. Therefore, the best approach is a phased implementation.

3.3. NAC Technology Types

Companies and organizations should consider which NAC technology is the best for their respective environments by comparing and contrasting the following:

a. Out-of-band
b. In-line
c. Appliance

Out-of-band devices do not sit directly inline with network traffic. The out-of-band device eliminates the worry of taking the network down when the device becomes overloaded. Another benefit of out-of-band is there is no chance the device will start blocking traffic based on a false positive.

In-line devices sit directly in line. They must be able to handle the maximum throughput of the network segment. One advantage of in-line is no traffic passes without first being inspected. The primary concern with in-line is it can take the network segment offline if it encounters issues.

Appliances can be either out-of-band or in-line. They can also be a hybrid of both. The advantage of an appliance deployment is the vendor will pre-configure all settings and ship the appliance to the customer. The customer must connect the device to their network to complete the installation process.

Below are three examples of each of the implementation methods available with explanations provided for the specific choice.

Central Michigan University (CMU) used an appliance-based, out-of-band approach to implementing NAC within their environment. Bradford Networks provided the solution. CMU's main concern was placing a device inline and possibly disrupting access for their students and faculty.

Ball State University went with a different approach. They chose a software-based solution and utilized Microsoft Network Access Protection (NAP). NAP comes as a feature of Windows Server 2008 since Ball State is already a Microsoft shop, so the only costs incurred were setting up five new servers. Ball State estimates a savings of about $75,000 per year in support and maintenance.

The University of San Francisco chose a hybrid NAC solution. They deployed an in-line NAC solution from Cisco for their dorms. Later Pereira's team expanded the

deployment, adding an out-of-band system for the dorms. Their primary concern was that the dorms have the highest network traffic and potentially the most infected computers. They are now using the original inline system on their wireless network. ("Network access control: Security advice for enterprise CIOs," n.d.)

The three vendors that were chosen and reviewed for this research all now offer Virtual Machine (VM) solutions that are out-of-band. Either the vendor can provide a VM image, or as Portnox suggests, the company can create their own VM and install the Core application. The VM's use SNMP and CLI to control the switches in a network environment. Mirror or Span ports are no longer required. By directly communicating with the switches, this eliminates the possibility of a bottleneck slowing network traffic. All three vendors provided the same advice, to utilize their virtualized solutions.

4. Portnox POC

4.1. Preparation

In preparation for the POC a server, meeting the minimum specs shown previously in Figure 4, had to be set up and configured. The next step was to configure the test switch to output SNMP traps to the static IP address configured on the server.

Windows 2008 R2 standard edition (64 bit)
or
Windows 2012 or Windows 2012 R2

Enabled Roles:

Role of Web Server

Enabled features:

Window Process Activation (accept the default)

Microsoft Internet Explorer 7/0 or later

Hardware or Virtual Machine:

At least 2 CPUs Dual core Xeon 3.x GHz or equivalent (one core for each 60 switches)

Min of 4GB RAM

72 GB of disk space (recommended raid 5)

Single network adapter 100/1000

Additional considerations:

The server must have a static IP address.

Figure 8: Portnox Server Requirements

4.2. Installation and Use

After the pre-configuration steps, the next procedure is to start the software setup. The software had several prerequisites; these are on the ISO provided and installed automatically. After installation of the prerequisites, the system required a reboot before continuing the installation process. During the installation, the technician should record the administrator password and the ports utilized. Installation is straightforward and relatively quick. The systems required another reboot.

After installation, utilize the Portnox monitor to confirm that all services are running as shown in Figure 9. Then it is time to define the first switch and start device identification.

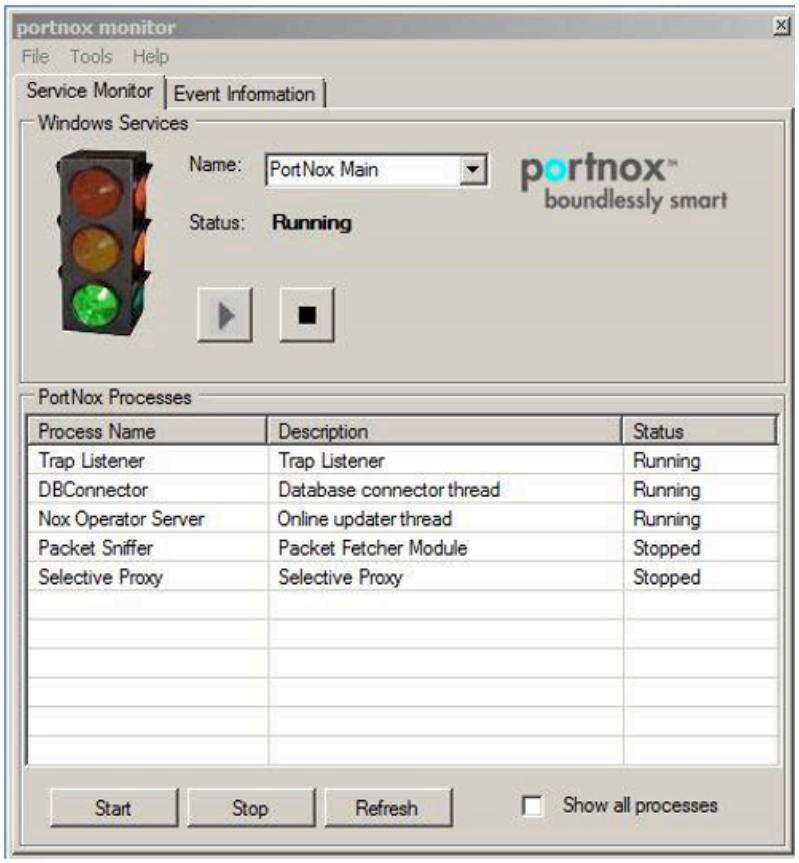

Figure 9: Portnox Monitor

Control and management of the Portnox environment are through their management web page as shown in Figure 10 below.

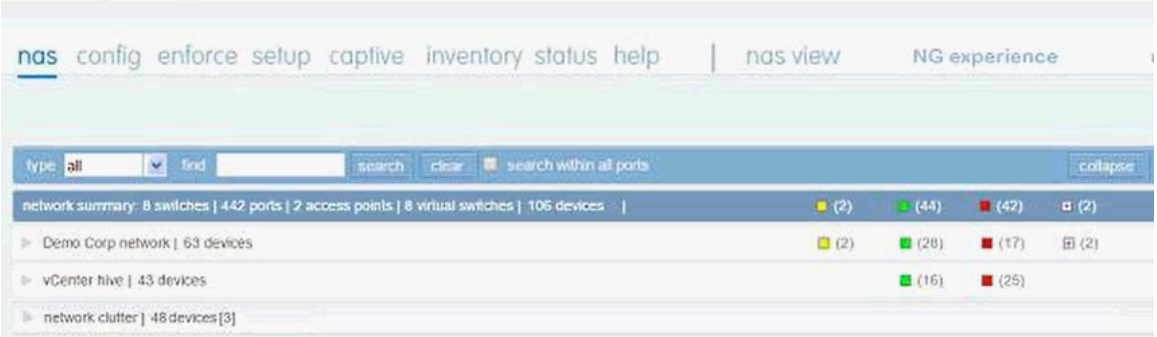

Figure 10: Portnox Management Page

Figure 11 shows the switch view; each port is clickable to go directly to the configuration and management page for the specific port. Information includes the details of the device and whether it passed or failed the compliance check. Granting access for failed devices to meet specific needs occurs at the port management page.

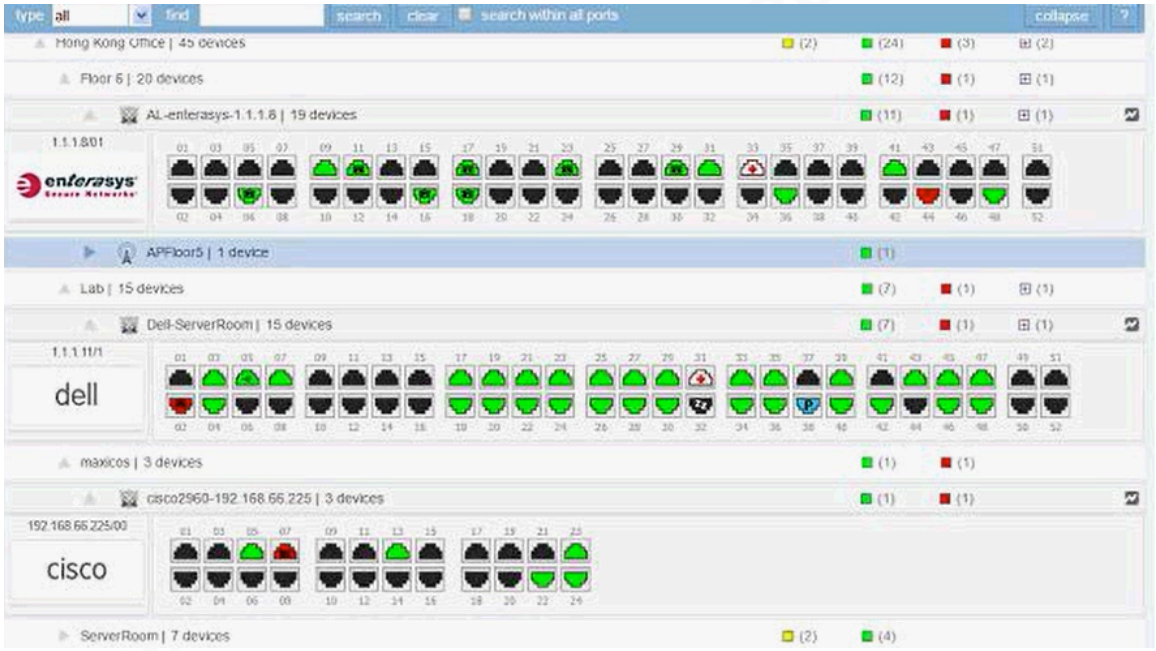

Figure 11: Portnox Switch Status View

5. Conclusion

Research and review of three vendors and their premiere solutions Portnox Core, Cisco Identity Services Engine and Bradford Networks Network Sentry occurred. The vendors were compared and evaluated based on the POC and NAC implementation requirements specified below. Each of the three vendors quickly scheduled demonstrations after initial contact. Each vendor received the requirements for the POC and NAC implementation. These include:

- 100% view of all devices on the network, or attempting to connect to the network

- Central management of the NAC solution
- Ease of use through automation
- The solution cannot be labor intensive
- Granular rule enforcement and control
- Automatic onboarding of new systems and guests
- Confirm compliance control of company owned equipment
- Must be able to handle printers, IOT, BYOD, VoIP, etc.

Chart 1 below shows a side by side comparison of how each vendor rated based on the requirements.

	Portnox Core	Cisco ISE	Bradford Networks Sentry
100% view of all devices on the network, or attempting to connect to the network	5, Core receives its information from the switches, any connection or attempted connection is known	3, Cisco depends on its supplicant	5, Sentry receives its information from the switches, any connection or attempted connection is known
Central management of the NAC solution	5, Screens are manageable, needed information is consolidated to one location	4, Screens are too busy, have to go through multiple layers to complete a single task	5, Screens are manageable, needed information is consolidated to one location
Ease of use through automation	5, Fully automatable	5, Fully automatable	5, Fully automatable
The solution cannot be labor intensive	5, Fully automatable, rules can trigger any event needed by the administrator	4, Fully automatable, ruleset is limited to what Cisco provides	5, Fully automatable, rules can trigger any event needed by the administrator
Granular rule enforcement and control	5, Rules are very granular. Management roles are very granular.	5, Rules are very granular. Management roles are very granular.	3, Rules are very granular. Management roles are limited.
Automatic onboarding of new systems and guests	5, Onboarding process is automatic.	4, Onboarding is automatic for known device types	5, Onboarding process is automatic.
Confirm compliance control of company owned equipment	5, all devices on the network are reported	4, all devices on the network that a license is available for are reported	5, all devices on the network are reported
Must be able to handle printers, IOT, BYOD, VoIP, etc.	5, All devices are handle by profiles. The profile feed is updated regularly.	4, All devices are handle by profiles. The profile feed is updated regularly. Requires additional licenses.	5, All devices are handle by profiles. The profile feed is updated regularly.
Scale from 1 to 5, with 5 being the best			

Chart 1: Vendor ratings

After reviewing all three vendors, Portnox was the vendor chosen to perform the POC based on cost, integration, usability, and manageability. Their product is very

simple to acquire, deploy, configure and start auditing. After the initial phase, policies are required to utilize enforcement. Portnox is very granular in the ability to perform almost any task after triggering a rule or alert. Initial NAC implementation is possible in a large environment in less than 30 days with Portnox. Achieving full policy and compliance enforcement within 60 days is possible.

Matthews, Joseph

References

Andrus, F. (2012, July 7). Understanding the Difference Between 802.1x and NAC | Bradford Networks. Retrieved from https://www.bradfordnetworks.com/understanding-the-difference-between-802-1x-and-nac/

Boscolo, C. (2008). How to implement network access control. Retrieved from http://www.computerweekly.com/opinion/How-to-implement-network-access-control

Center for Internet Security. (2016, August 31). Retrieved from https://www.cisecurity.org/critical-controls.cfm

Cisco Network Admission Control (NAC) Solution Data Sheet - Cisco. (2017, January 23). Retrieved from http://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html

Hickey, A. R. (2006, November 3). Network access control: Should you implement now? Retrieved from http://searchnetworking.techtarget.com/news/1228311/Network-access-control-Should-you-implement-now

NAC Framework Configuration Guide. (n.d.). Retrieved from http://www.cisco.com/en/US/solutions/ns340/ns394/ns171/ns466/ns617/net_design_guidance0900aecd8040bbd8.pdf

Neiva, C., & Orans, L. (2017, May 9). Market Guide for Network Access Control. Retrieved from https://www.gartner.com/doc/3708117?ref=SiteSearch&sthkw=market%20guide%20for%20network%20access%20control&fnl=search&srcId=1-3478922254

Network access control -- More than endpoint security. (n.d.). Retrieved from http://searchnetworking.techtarget.com/report/Network-access-control-More-than-endpoint-security?offer=briefcase

Network access control: Security advice for enterprise CIOs. (n.d.). Retrieved from http://searchcio.techtarget.com/Network-access-control-Security-advice-for-enterprise-CIOs

Network Admission Control Software Configuration Guide - Cisco Systems. (n.d.). Retrieved from http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_configuration_guide09186a00805764fd.html

Snyder, J. (2010, May 24). NAC: What went wrong? | Network World. Retrieved from http://www.networkworld.com/article/2209345/security/nac--what-went-wrong-.html

Snyder, J. (2010, May 24). Cisco's NAC goes off track, customers taken aback | Network World. Retrieved from http://www.networkworld.com/article/2209367/security/cisco-s-nac-goes-off-track--customers-taken-aback.html

Wilkins, S. (2012, March 7). Switchport Security Configuration. Retrieved from https://www.pluralsight.com/blog/it-ops/switchport-security-configuration

Wilkins, S. (2012, February 22). Switchport Security Concepts. Retrieved from https://www.pluralsight.com/blog/it-ops/switchport-security-concepts