A Review of Opensource Network Access Control (NAC) Tools for Enterprise Educational Networks

Henry Nunoo-Mensah
Department of Computer Engineering
Kwame Nkrumah University of Science and Technology

Emmanuel Kofi Akowuah
Department of Computer Engineering
Kwame Nkrumah University of Science and Technology

Kwame Osei Boateng
Department of Computer Engineering
Kwame Nkrumah University of Science and Technology

ABSTRACT
In enterprise networks, the concept of bringing your own devices (BYOD) to work and also allowing guest nodes to connect to the network is encouraged. As a factor the need to control access to the network is critical as visibility of nodes attached to the network is paramount in determining potential threats. The use of opensource technology is not mostly patronized by the corporate world because of the steep learning curve and the assumed complexities involved in the use of these software. This paper throws more light on the need for the use of opensource for enterprise networks especially for such networks for developing economies. Three major open source tools (OpenNAC, PacketFence and FreeNAC) are reviewed to provide a mechanism for assessing and selecting an opensource option for your educational network.

General Terms
Opensource Network Access Control Tools

Keywords
Opensource, Network Access Control (NAC), Enterprise Networks, Educational Networks, Developing Countries

1. INTRODUCTION
Educational networks can be undoubtedly categorized as an educational network because it follows the architecture of enterprise networks. Educational networks mainly for tertiary institutions are large and complex with a wide array of network contrivances found on them. It also has dynamic users of its network; this encourages the integration of seamless access to certain areas of the network. Enterprise networks have the ability to integrate all systems, such as Windows and Apple contrivances and operating systems, UNIX systems, mainframes and cognate contrivances like smartphones and tablets. A firmly incorporated enterprise network efficaciously conglomerates and uses different contrivance and system communication protocols.

The major challenge of enterprise networks is the lack of congruous overtness needed to comprehend what is running on the network, where it is being run and how to meritoriously troubleshoot and resolve performance quandaries when they transpire. Network management procedures and solutions were conventionally built around contrivance management, but that is no longer sufficient. Modern networks have grown in involution and must compete with incipient types of traffic such as streaming video and voice; which are very sensitive to latency. The exposure of private corporate networks to the public Internet has engendered incipient end-user engendered traffic and security issues. Thus, network monitoring must now incorporate everything from end-user activities, applications, network traffic, networking protocols, servers, and network contrivances [1]. This is essential so as to obtain a holistic end-to-end view of what is transpiring and where on the network it is transpiring.

Some security requirements pertaining to enterprise networks are the exposure of malicious software; any malicious software needs to be branded, removed or secluded. Auditing tools are needed to keep logs of all activities on the network, passwords must be hard to guess; there ought to be in place a one-way encryption form for application used on the networks and passwords should be changed at least once every six months. There should also be access control in place to give access rights and should be revised at regular interims, inactive accounts should be locked. Network access such as traffic inward and outward flow should be maintained.

Through Bring-Your-Own-Device (BYOD), individuals in an organization can use their own devices in business activities. It also helps in anticipating improved productivity, the main reason being that institutions do not burden themselves with the acquisition of contrivances and also most of these contrivances introduced onto the network are smart contrivances that have the ability to carry out productive or efficient work. In as much as it is beneficial it also comes with some security concerns. A major concern is corporate information leak since these personal contrivances have access to the internal network infrastructures of a company and due to frequent loss and theft coupled with the low security of these contrivances they become easy target for hacker wanting to attack our network. The Honey Stick project conducted by Symantec, discovered that access to internal company infrastructure through lost or stolen personal contrivances is occurring at a fast pace. Due to this [2] stated that establishing security is the topmost priority in introducing BYOD systems.

With the growing need to secure enterprise networks, educational networks especially those in developing countries are at the disadvantage due to their limited financial resources. The paper focuses on bringing to bear the strengths of opensource alternatives for authentication and conditioning contrivances before they are admitted onto the network. The investigations were carried out based on the following requirement metrics; posture analysis, contrivance authentication, bandwidth management, network vendor support, its support for both wireless and wired infrastructure, software integration, software community support, software administrative interface and reporting functionalities. The contribution of this paper is to provide an in-depth analysis of popular opensource tools used for Network Access Control. It further acts as a platform providing unbiased information to aid in the selection of NAC tools by network administrators. The tools being considered in the review are OpenNAC, PacketFence and FreeNAC; this is because they are the most widely used opensource tools being [3].

This paper has been divided into eight sections. Section two looks at the related work carried out in the field of NAC tools for enterprise networks. Section three explains the need to adapt opensource tools for use in critical projects. Section four explains some fundamental concepts and workings of Network Access Control (NAC). Section five briefly discusses OpenNAC, PacketFence and FreeNAC, section six depicts the requirements used in analyzing the tools listed in section five. Section seven explains NAC implementation strategies and finally section eight concludes the paper.

2. RELATED WORK

This section reviews related work carried out in the past. [4] carried out a work analyzing opensource architectures and requirements. [4] presented in-depth requirement analysis for NAC. Key design and implementation choices that are needed based on stakeholder requirements were also identified. Recommendations were further made to improve the security posture of the network. The analysis of the NAC products carried out in [4] was performed in the following areas; authentication, integrity measures, remediation, security, functional and non-functional, system administration and policy settings. The NAC products in the analysis were Cisco Network Admission Control, Microsoft Network Access Protection (NAP).

3. WHY OPENSOURCE

People prefer opensource software because they have more control over the software. They can examine the code to ascertain it's not doing anything they don't optate it to do, and they can transmute components of it they don't relish. Users who aren't programmers additionally benefit from open source software, because they can utilize this software for any purport they optate, not merely the way someone else cerebrates they should.

The active support by the opensource community on projects makes it the ideal software for important, long-term projects. Users can rely on software for crucial tasks knowing that their tools would not have discontinued support once their original developers discontinue work on them.

Others prefer opensource because it is considered as very secure and stable as opposed to proprietary software. This is because of the fact that the code is open and anyone can identify and correct bugs missed by the original creators of the software. It is stable because there are a lot of programmers that can work on it without seeking for permission from the originators of the software, this helps maintain it by keeping it fit generally fixed, updated and upgraded.

Additionally others like opensource software because it avails them to become enhanced coders. They can learn to make more preponderant software by studying the source code others have indited. Coders additionally share their work with others, welcoming comment and reproval. This spirit is self-motivating to always achieve or be the best.

Importantly it affords educational institutions, especially in developing economies to use world class software tools. This is because they get the service they would pay for free and still be able to compete with other institutions in the developed economies.

4. NETWORK ACCESS CONTROL (NAC) FUNDAMENTALS

Network Access Control (NAC) offers end-device management and compliance, identity management and utilization policy enforcement. NAC components as referenced as end-devices, enforcers and verifiers. Network Access Control (NAC), communications starts when an endpoint validates and provides a reliable platform characteristic to the verifier. The user and machine validation ought to be verified. Integrity measures are taken and are sent from the end-device to the verifier.

This is where the felicitous protocols and message handling practices are vital. Integrity measures are captured and provided to the verifier, it then decides if security policies are achieved. If policies are not realized, remediation is needed and the verifier issues instructions to the end-device on how it should connect for a remediation process. The end-device follows these instructions issued by the verifier to allow either limited network access or to be placed on a secluded network so that remediation can occur.

Also, after an end-device has been checked for integrity, the network administrator may need to apply policies to the end-device prior to its acceptance on the network. [4]

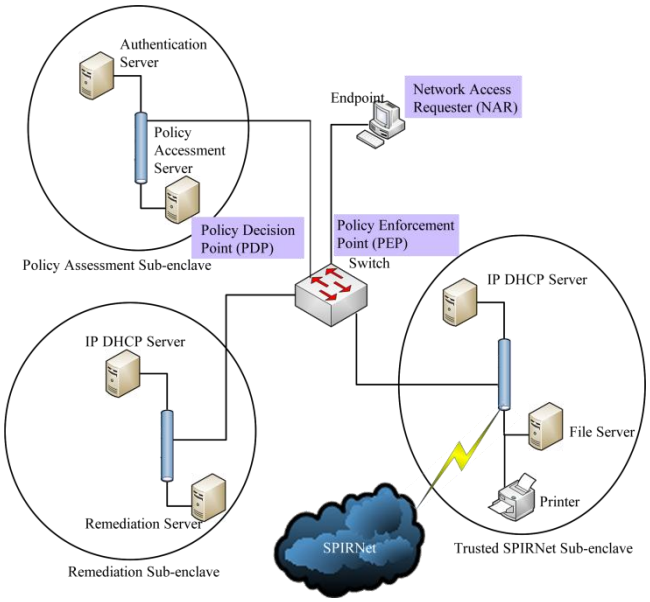

Fig 1: Network segregation used in NAC Solutions

5. REVIEW OF TOOLS

The opensource tools selected include OpenNAC, PacketFence and FreeNAC; these tools were chosen because of their popularity when it comes to opensource NAC tools.

5.1 OpenNAC

OpenNAC is an open source network access control tool that provides access for LAN/WAN. It works with a wide range of operating system clients (Windows, Linux, Mac, etc.) and network contrivances such as Extreme Networks, Cisco, 3Com and Alcatel. The software is developed based on well proven opensource components like FreeRadius, iTop, lcinga. It is very flexible as it allows for user to add new functionalities like accounting, asset management, and Network Intrusion Detection and authentication systems. OpenNAC is also ideal for network configuration and discovery, network contrivance configuration backup and network monitoring aside the inherent access control.

Other features of OpenNAC are that it enables authentication, authorization and audit policy-based access to the network; it also provides real time monitoring of users and contrivances on the network [5].

5.2 PacketFence

PacketFence is also a free and opensource NAC solution. It comprises a captive portal for registration and remediation, it additionally features a unified wired and wireless management, 802.1X support, layer-2 isolation of problematic contrivances. PacketFence additionally sanctions the integration of other applications. PacketFence can be habituated to efficaciously secure networks diminutive to prodigiously and sizably voluminous heterogeneous networks [6].

Other features of PacketFence are bandwidth accounting, detection of anomalous network activities, proactive susceptibility scans, and it provides a consummate verbal expression of health for the network [7, 8]. PacketFence annexes user accounts to contrivances accounts and examines the contrivances posture and authoritatively mandates the contrivance to perform self-remediation [4].

5.3 FreeNAC

FreeNAC provides, access control for LANs; it caters for all kinds of network contrivances. It also performs switch port management and documents patch cables. Both 802.1x and Cisco's VMPS port security modes are supported.

FreeNAC has redundancy and load-sharing for high availability as additional features, it provides flexible reporting, live inventory of end-to-end-devices on the network. FreeNAC is GPL opensource and thus entirely free, but also support is provided at a cost. The community edition is aimed at expert system administrators who are used to working with opensource.

6. REQUIREMENT ANALYSIS

The NAC requisites being considered in this paper are posture analysis, contrivance authentication, bandwidth management, and support for wired and wireless infrastructures, the network contrivance vendors fortified, software integrations, community support, administrative portal and reporting.

6.1 Posture Analysis

Please Posture refers to the amassment of attributes that are considered salubrious in order to admit an end-device that is endeavoring to access the network. Posture analysis is the act of applying a set of rules to the posture data to provide an assessment of the caliber of trust that you can place in an end-device.

6.1.1 OpenNAC

It does detection of antivirus updates, OS updates and patches and firewall of connected contrivances to enforce access policy.

6.1.2 PacketFence

PacketFence uses Statement of Health (SoH) protocol to perform complete posture analysis or assessment of connecting contrivance. This analysis is done while 802.1X user authentications are being carried out. An example is PacketFence verifying if an antivirus is installed and updated, if operating system patches are all applied. All this is done without an agent being installed on end-devices. Remediation is done through a captive portal; based on the end-devices current status, the user is redirected to the appropriate URL. In the case of violations, the user is presented with instructions for the exact situation he/she is in.

6.1.3 FreeNAC

FreeNAC is not currently designed to run a software agent on end-devices, this makes inherent posture analysis difficult. End-devices can only be verified through scans or querying of a server-side security assessment tool. This indicates that if McAfee EPO or MS-WSUS is used, it may be possible to verify the security of the end-devices before allowing access. EPO/WSUS information is currently utilized as an indication to the security administrator, but not to exclude end-devices from the network.

6.2 Contrivance Authentication

Contrivance authentication examines the mechanisms in place by these NAC tools to authenticate any contrivance before it access the network.

6.2.1 OpenNAC

There is authentication of 802.1X enabled devices, an authentication backend based on LDAP or Active Directory. It supports rogue devices using 802.1X or SNMP traps.

6.2.2 PacketFence

PacketFence authenticates contrivances by using MAC-Authentication-Bypass (MAB). It implements 802.1X port-based authentication is supported through a FreeRadius module. DHCP fingerprinting and user-agents are also authentication options available. Using MAC-Authentication-Bypass (MAB), contrivances like network printer or non-802.1X capable IP telephones can still gain access to the network. The contrivances, once authenticated are automatically registered. Access duration to the network can be controlled either absolutely or when the contrivance becomes inactive. Some authentication sources include; Microsoft Active Directory, Novell eDirectory, OpenLDAP, Cisco ACS and RADIUS.

6.2.3 FreeNAC

FreeNAC supports MAC address based authentication by using MAC-Authentication-Bypass for contrivances on the network. It also implements 802.1X authentication. MAC authentication bypass is an alternative to 802.1X that allows network access to contrivances, like printers and IP phones that do not have 802.1X supplicant capability. FreeNAC uses the authentication server FreeRadius which generates a VLAN Management Policy Server (VMPS) request for FreeNAC, and FreeNAC will decide if the device is authorized to join the network and also where to place it. FreeNAC enables expiry dates to be set for each MAC address; such that a visitor can be allowed for only a day or something. Finally it can automatically detect end-devices or ports not actively managed by FreeNAC; this ensures a complete list of end-devices on the network.

6.3 Bandwidth Management

For bandwidth management examinations were done to see if these tools have bandwidth analysis mechanisms in inbuilt or whether they rely on third party bandwidth management tools.

6.3.1 OpenNAC

OpenNAC does not keep track of bandwidth utilization. Its main focus is Network Access Control.

6.3.2 PacketFence

PacketFence automatically tracks the amount of bandwidth contrivances on the network consume. It can quarantine or change the access level of devices that are consuming too much bandwidth during a particular time frame. It also provides report on bandwidth utilization.

6.3.3 FreeNAC

FreeNAC does not inherently offer bandwidth monitoring of the network. It relies on other tools used for traffic monitoring and analysis like ntop for these functionalities; its main focus is on Network Access Control.

6.4 Network Vendor Support

Considering the increasing contrivances available from different vendors on enterprise networks, this section tries to examine the vendors supported by these tools. This is to provide a fair idea as to the vendor support base.

6.4.1 OpenNAC

OpenNAC supports these network devices; Cisco 2960, Cisco 2950, Cisco 3500XL, Cisco 3560, Cisco 1920, Cajun P120, Avaya P133 G2, 3COM HUB PS40, Enterasys vh4802 and AP 1242. The vendor support base is not as broad as expected; it only covers the above mentioned models.

6.4.2 PacketFence

PacketFence supports a host of hardware from several vendors. The creators of the software also invite new vendors that are not supported to contact them; this shows their preparedness to increase their current vendor base. Some of the vendors supported include; 3COM, Accton Allied Telisis, Amer, Avaya, Brocade, Cisco, Dell, D-Link, Enterasys, Extreme Network, HP, Intel, Juniper, NetGear, Nortel and SMC[9].

6.4.3 FreeNAC

FreeNAC supports multiple vendors from printers, servers, switches (managed and unmanaged), hubs and VoIP phones (AYA, Cisco).

6.5 Support for Wired and Wireless Infrastructure

Supports of these tools for wireless and wired technologies were examined. It is paramount because of the number of mobile users found on most enterprise networks.

6.5.1 OpenNAC

There is support for both wired and wireless infrastructure. It provides full control of users that access through wired or wireless. It also supports 802.1X.

6.5.2 PacketFence

PacketFence provides supports for wired and wireless infrastructure. It is equipped with centralized wired and wireless management and 802.1X support.

6.5.3 FreeNAC

FreeNAC supports both wired and wireless infrastructure. 802.1X support is available for wired LANS.

6.6 Software Integration

To be able to customize tools, tools were examined to know whether or not they have been inherently designed to support integration with other software. This is really important if you are looking at a complete software solution tool for your network.

6.6.1 OpenNAC

It is based on opensource components like FreeRadius and iTop. It is open to be integrated with platforms such as accounting, authentication, Intrusion Detection Systems (IDS) and asset management platforms.

6.6.2 PacketFence

PacketFence supports software integrations. Some integrated software includes Snort IDS for intrusion detection and Nessus vulnerability scanner for scanning for vulnerabilities. Its ability to easily integrate software makes it a Swiss knife NAC tool.

6.6.3 FreeNAC

FreeNAC supports Active Directory and other LDAP implementations, although some modifications may be relevant. Microsoft SMS (Software package/ system management) server can also be integrated but this feature is only available in the commercial version.

6.7 Community Support

The community base and the enthusiasm of the developers concerning the tool are very important. For every opensource tool the best place to start off is with the community; the communities and their contributions were examined.

6.7.1 OpenNAC

The OpenNAC has an online forum which is fairly active. It is difficult navigating through their documentations and there is very little explanation made the documentation; you need to be an expert or middle-level user to be able to comprehend the information put there. It is basically not too beginner friendly.

6.7.2 PacketFence

PacketFence is backed or supported by an online community. It provides a mailing list with an average of 8 posts daily to the PacketFence-users mail list. There is an archive where previously answered questions are stored [10]. There is also a well-documented documentation providing administration, configuration and installation guides.

6.7.3 FreeNAC

FreeNAC provides a well-documented documentation providing installation, user and technical guides. It has a forum or bulletin board that helps users post and discusses challenges being faced. The community is a little adamant based on the dates that the forums were last commented on or an issue posted. It has no registered user on the forum [11]. Commercial support for the software is available.

6.8 Administrative Interface

The administrative interface of the tool is also a very vital aspect to a software tool. With current network sizes and mobile administration, there is a need to make sure that the administrator can administer his network on any part of the network. This section examines the various administrative interfaces.

6.8.1 OpenNAC

The administration is done using a web based interface. Templates are available that can be used to do bulk configuration of hundreds or thousands of contrivances. It provides a real-time network contrivances status.

6.8.2 PacketFence

PacketFence is administered through a web-based interface; it also has command-line interfaces for all management tasks. There are different permission-levels for users and all users are authenticated using LDAP or Microsoft Active Directory

6.8.3 FreeNAC

FreeNAC is mainly administered, that is configured and monitored using a windows interface. A web GUI is also provided as an alternative to the windows GUI.

6.9 Reporting

Reports and audit are essential to any security tool. This section takes a look at the availability of reporting features in the tools under review.

6.9.1 OpenNAC

There is a reporting feature which has been integrated in order to review and audit network activities. It allows you to save results to CSV.

6.9.2 PacketFence

The reporting functionality for PacketFence allows you to see the entire contrivance activity when an IP or MAC address is entered. Active and inactive contrivances, registered and unregistered users, OS classes, Unknown fingerprints, open violations and probable static IPs can all be generated. Queries can also be filtered.

6.9.3 FreeNAC

There is a reporting feature which allows some standard reports to be generated, this reports can be optionally exported to excel. The reporting interface is very flexible which allows for the sorting and filtering; this allows custom reports to be generated.

Table 1.Comparison between OpenNAC, PacketFence and FreeNAC

Features	OpenNAC	PacketFence	FreeNAC
Posture Analysis	Fairly	Yes	Not Inherent
Contrivance Authentication	Yes	Yes	Yes
Bandwidth Management	No	Yes	No
Network vendor support	Multivendor	Multivendor	Multivendor
Wired and wireless support	Yes	Yes	Yes
Software Integration	Yes	Yes	Commercial
Community Support	Active	Active	Fairly active
Administrative Interface	Web Interface	Web Interface	Mainly window based
Reporting	Yes	Yes	Yes

With reference to table 1, it can be seen that PacketFence has the best edge over the other two opensource tools. PacketFence does posture analysis which is fairly done by OpenNAC but not done for FreeNAC. Posture analysis deals with the condition of a contrivance before it joins a network; it is done against a baseline, which helps to ascertain the operational level of the contrivance e.g. whether a contrivance has an updated antivirus and whether or not it meets some basic hardware requirements. PacketFence additionally does bandwidth accounting by automatically tracking the amount of bandwidth contrivances have consumed on the network; it can quarantine or change access level of contrivances that are consuming an inordinate amount of bandwidth during a particular time window. PacketFence additionally has reports on bandwidth consumption [8].

7. IMPLEMENTATION STRATEGIES

NAC is implemented with ardent consciousness of information that has to be protected and the kind of access policies that are necessary. An analysis of existing access controls performed by end-device and perimeter contrivances and the impact of adding NAC to the network is required.

Subsisting applications in utilization for anti-malware, anti-virus, intrusion detection and obviation and software updates may need to be integrated with the NAC solution. The solutions must be assessed punctiliously with IT staff because if optically discerned as a supplemental burden or degradation to network performance, the IT staff may shut key security features down. Auditing should be re-evaluated to include NAC auditable events. NAC can increment the life cycle of a subsisting network and preserve network administrators' man-hours by proactively ascertaining end-device integrity.

NAC requires the utilization of multiple subnets: pre-access, post access but remediation required, and a policy compliant network. VLAN containment can be acclimated to achieve this architecture with access restricted by numerous methods of identifying the end-device.

Either post or pre-admission is an option for implementation. It is not ideal to admit a user onto a network before integrity measures are taken. It is recommended that the integrity measures are matched to network policy at the point of admission before the user or contrivance is admitted onto the network.

8. CONCLUSION

The paper set out to review opensource tools for implementing Network Access Control (NAC) for Educational networks. Three opensource tools OpenNAC, PacketFence and FreeNAC were reviewed. OpenNAC fairly supports posture analysis. PacketFence was found to perform posture analysis and bandwidth monitoring. It also supported a wide array of vendors. FreeNAC has a load sharing and redundancy feature integrated. All the opensource features did authentication, supported both wired and wireless connections and has an active community backing. The paper has provided a mechanism for assessing and selection an opensource option for your educational network.

9. REFERENCES

[1] SolarWinds. "Choosing the right enterprise network management solution - white paper," Nov. 2009

[2] Kang D., Oh J. and Im C., "A study on abnormal detection in BYOD environment," International Journal of Environmental, Ecological, Geological and Mining Engineering Vol.: 7 No: 12, 2013

[3] "PacketFence: Testimonials", http://www.packetfence.org/about/testimonials.htm, retrieved on 03/10/2014

[4] Serrao, Gloria J., "Network access control (NAC): An open source analysis of architectures and requirements," IEEE International Carnahan Conference on Security Technology (ICCST), 2010

[5] OpenNac, http://sourceforge.net/projects/opennac, retrieved on 31/04/2014

[6] Annuar, H., Shanmugam, B., Ahmad, A., Idris, N.B., AlBakri, S.H.and Samy, G.N., "Enhancement of network access control architecture with virtualization," International Conference on Informatics and Creative Multimedia (ICICM), 2013

[7] "PacketFence: Overview" http://www.packetfence.org/about/overview.html, Retrieved on 31/04/2014

[8] "PacketFence: Advanced Features" http://www.packetfence.org/about/advanced_features.html, Retrieved on 31/04/2014

[9] "PacketFence: Supported Switches and APs", http://www.packetfence.org/about/supported_switches_and_aps.html#c1482, retrieved on 11/06/2014

[10] "PacketFence: Community", http://www.packetfence.org/support/community.html retrieved on 11/06/2014

[11] "FreeNAC", http://www.freenac.net/phpBB2, retrieved on 11/06/2014.