# Network Access Control

M.Roopesh
B.Tech, Department of CSE, Kalasalingam University, Krishnankoil ,India
roopesh.munnaluri1@gmail.com

G.Reethika
B.Tech, Department of CSE, Kalasalingam University, Krishnankoil ,India
garikamukku.reethika@gmail.com

B V Srinath
B.Tech, Department of CSE, Kalasalingam University, Krishnankoil ,India
srin71@gmail.com

A.Sarumathi
B.Tech, Department of CSE, Kalasalingam University, Krishnankoil ,India
a.sarumathi@klu.ac.in

***Abstract*— Traditional security systems running solitarily were no longer satisfying, as hazards are growing in complexity, diversity and performance. Usually mankind got habit of using computers in multiple kinds such as communication, tourism, purchasing in finger tips, online banking. In order to defend against threats we need more meshed security system and at the same time users should have access to any website worldwide. It is mandatory to have a security systems which prevents from all the threats. Even though systems get exposed to many threats like a malware, worms, data leakage , NAC firewall has proposed a new pose which coordinate as well as communicate security statistics to various network security components using a strategy. NAC governs the connection from outside while giving protection to every network passing through the firewall produced. It is used to unify end point security technology, user or authenticator and network security enforcement. This paper deals with NAC, problems in security systems, solutions and explains in detail about groups like Microsoft trusted group, juniper who are involved in developing the standards for NAC.**

***Key words:*** NAC, Malware, Threats, security

## I. INTRODUCTION

The security initiated by antivirus code which is a software from Symantec, Trend small[1], and McAfee working on end devices that uses client-server communication for updating the virus defining files. Antivirus code was governed by software-based personal firewalls from Microsoft, Norton, Trend small, and Zone Alarm which provides some accessing directories. Then code will be reworked to firewall devices, IPSec VPN devices and finally to affiliated SSL VPN devices with a growth in access over remote networks. The software ultimately acquired the design of the technology named by Network Access Management which provides additional layer of indemnity in contrast to potentially occurred security threats. NAC, in its original kind, was host pose check, quarantine, and restorative that create disturbance, client requesting access to a network. If the client did not receive recent OS patches or associated bugs along with an up-to-date virus definition running on that system, immediately the client would not be permitted for accessing the network despite would be moved to either a VLAN or quarantine (network) until it had been compliance with requirements stated by the network (remediation).As technology is evolving, NAC is not merely permitting access over network requested by staff, visitors, other than staff and protectively against security threats despite mutually authoritative to access anywhere the network supports the client's role. Access towards the network is acceptable, rejected, as well as supports the client's identity to a specific cluster.

[2]So what will a Network Access control ought to do with compliance? the solution is lots however to be clear, Network Access Control isn't a nostrum for acquiescence nothing is. From a network stand, acquiescence might be almost designed by the stated 5 needs. Certainly, stated needs are not thorough (many of our elders have for quiet larger list of needs), despite of them here goes:

- **Policies** – Rules followed previously was there is a need recorded security policies to forestall intrusion as well as to provide protection for personal info.
- **Authentication** – Validate a single request over access to sensitive info is that the one claimed.
- **Access management** – to ensure that circuitries, applications and data unit accessed simply by those accepted spare privileges.

- **Remediation** – abilities to acknowledge for a security instance, every reporting concentrated parties and assurance protecting area unit in situ to incorporate injury.
- **Audit** – Records and artifacts concerning the utilization of circuitry and implementation using personal information.

Authentication, access management and rectification square measure wherever NAC can include the foremost influence on your concession attempts. Let us strike them at a lapse of spin:

- **Authentication** – NAC will need number of various layers for validation in previous of producing usage over network. Major provisions will affiliate with prevailing LDAP directories, RADIUS servers and assist multiple-factor authentication. Score one for NAC.
- **Access management** –concluding for NAC will be nothing. Network access management conclusions will make sure about solely clients or groups providing some particular access will manage facilities. The square measures countless totally different social control implementations (inline, DHCP, 802.1x, VLAN, SNMP, etc.), however every arise towards the survey of concession requirements.
- **Remediation** – Once a problem is triggered, constant social control implementations dominant access are often took place at s situ to quarantine the "violators."

Audit is that the last piece of the puzzle, and NAC will become a major information supply for external log management and coverage mechanisms. NAC merchandise will log each request to access network resources, furthermore as once policies square measure profaned.

## II. BARRIERS

Network access management, that process as a mix of validation,[3] end-device reliability checking and usage management, evolved at a response for the matter of mobile finish clients involving infected personnel devices in return to the resource network. NAC was meant for unraveling actual issues and responding to real queries: which is interrelating to my network? Will the connection be secure? Can i monitor and govern their events? Will I could be able to disconnect or retrieve them from my network or power off their devices?

Typically in our business, merchandise tend to combine over time towards common approaches and customary feature sets. for instance, today's switches from totally different vendors are mostly substitutable. Swap out an Hp ProCurve switch for Enterasys and also the switch is perhaps aiming to add your network. however NAC hasn't found out that method. The merchandise bear little or no similarity to every different. With terribly close scrutiny, a network manager can be able to notice 2 or 3 merchandise which will be compared head-to-head. Despite finding comparable merchandise is troublesome, and doing therefore pre-supposes that the network manager already is aware of the feature set and capabilities that they need.

**Barrier No. 1: Politics gets within the manner**

A particularly troublesome issue is finding a product that may be compatible each politically and technically with the network. as a result of NAC combines options of security, network management and desktop management, a NAC preparation faces important structure challenges on prime of any technical challenges.

**Barrier No. 2: Too several merchant variations**

NAC's 3 parts are authentication, end-point security and access management, however vendors tend to deliver NAC product supported their explicit robust suits. This suggests NAC product tend to target one in all those 3 parts, typically ignoring the opposite two. as an example, once McAfee approaches NAC, they are doing thus from the context of their own end-point security management product, ePolicy arranger. However Juniper approaches North Atlantic Council from the context of their network security components: firewalls and, to some extent, switches.

**Barrier No. 3: ability woes**

When Network World tested NAC product head-to-head in 2007, we have a tendency to had to interrupt our tests up into separate components. One check checked out two council frameworks (Cisco and trusty Computing Group) and thirty product that worked in those frameworks. the opposite check checked out thirteen standalone NAC solutions. we have a tendency to had foreseen that by now, the frameworks would have unified and every NAC product would support them to one extent or another.

**Barrier No. 4: Deployment difficulties**

One perennial struggle for NAC vendors has been the issue of deployment. though several NAC merchandise we tend to tested are designed to permit gradual installation across enterprise networks, return one port protected by NAC will be a prolonged method. a lot of significantly, the installation of NAC will embody several important call points — and if those selections are modified down the road, the complete preparation might need to be restarted. easy queries, like "how am I getting to do authentication?" or "what mechanism can i exploit for access control?" are troublesome to answer with confidence while not some in-the-trenches expertise — however should be set before you'll be able to even begin rolling out NAC.

**Barrier No. 5:** Hidden measurability problems

One of the intense signs for NAC deployments that came out of our testing this year is that the relative lack of measurability and availableness problems. In previous NAC testing, we tend to uncovered performance issues caused by funneling an excessive amount of traffic through one management purpose. Early NAC merchandise were usually entirely "in-line," that means that you simply had to shop for a replacement appliance or device of some kind that sat in between devices you were dominant and therefore the remainder of the network.

## III. PROBLEMS

Even brilliant network access management systems do have some obstacles. Some of the difficulties encountered were**:**

**The CEO's view**

The NAC will be costly in terms of implementation as the prices are not simply describing about the council systems, we are in need of upgrading more number of network instrumentation which can be experimental in the council system.

NAC could enhance an expertise trials or hard work for attaining complete collaborator at every end devices. The considered action might replicate in extra operative outgoings in course of the personnel effort.

**The Net Administrator's view**

A NAC can embrace additional part of prospective loss to the network - doable poor management or misconfiguration for council system might produce greater issues

**The System Administrator's view**

A NAC can cause complexness in assimilation with alternative services (anti-virus, active directory, patch control) as well as can become a crisis of loss, if the council fails, the consequences about to occur will be a question?

**A client's view**

A NAC can produce immediate productivity consequences if the council misconceive at end-system's compliance. Giving the oaths for secured objectives at a situ, the correction of a likely happening occurs nearly minimum to 60 minutes.

## IV. PROS AND CONS OF EXISTING SECURITY SYSTEMS

**Pros and Cons of End point security system:[5]**

**Pros:**

- Centrally managed antivirus will determine work station without updated virus def initions
- Local firewall policy social control can't be disabled by end users

**Cons:**

- Anti-virus software package slows machine performance to the purpose wherever users disable automatic updates and stop scans. there's no way to prevent users from fixing the anti-virus software package.
- Only users with VPN access have the protection provided by native firewall policy social control.
- There is no anti-spyware or host intrusion bar resolution deployed.

**Pros and Cons of Network security system:**

**Pros:**

- Separate broadcast domains for sure internal users and
- Untrusted guest users – teams unable to speak directly
- Trusted internal PCs cannot contract viruses from untrusted guest PCs
- Untrusted guest users are unable to access personal internal servers
- Use of VLAN Trunking Protocol eases VLAN management

**Cons:**

- No measure to prevent untrusted guests from connecting to non-public ports
- Misconfiguration of a port can offer trustworthy network access
- Use of separate subnets ends up in inefficient use information processing address area
- Switches is also liable to attacks associated with raincoat flooding, tagging, multicast brute force, etc.

## V. POSSIBLE SOLUTIONS

**Improving End Point Security**

- Deploy a comprehensive end point resolution that has anti-virus, anti-spyware, and host intrusion interference capabilities
- Define and enforce policies that don't permit finish users to disable these protections
- Deploy personal firewall software system to any or all computers, not solely VPN enabled systems
- Design an worker education campaign stressing the importance of maintaining up thus far security software system definitions

**Improving Identity[6]:**

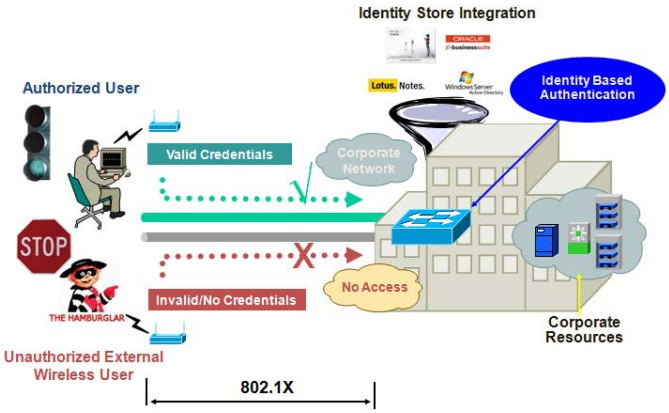


Fig.1 Solution by Improving Identity

**Comprehensive Solution**

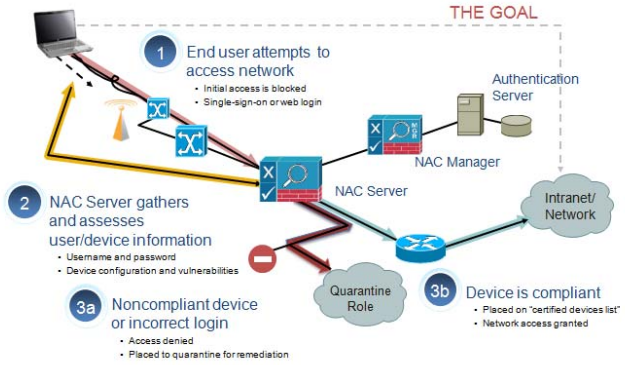


Fig.2 Providing Comprehensive solution

## VI. Recommended solution

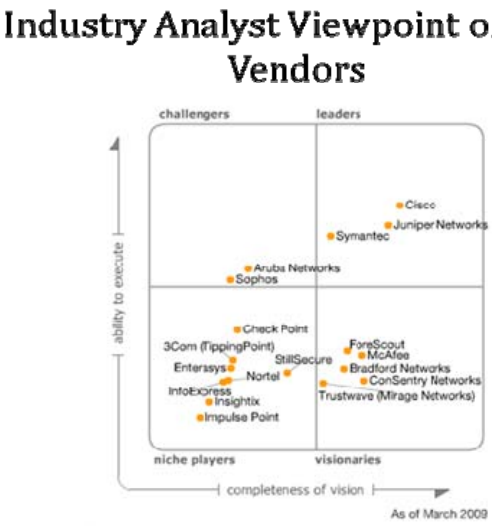


Fig.3 Analyst Report on NAC Vendors

### NAC Comparison Chart[6]:

Table 1 Comparisons Chart on Different Products of NAC

| | Aruba ClearPass Policy Management Platform | Bradford Networks' Network Sentry/NAC | Cisco Identity ServiceEngine (ISE) | ForeScout CounterACT | Pulse Secure - Policy Secure |
|---|---|---|---|---|---|
| Agentless Support | Yes | Yes | Yes | Yes | Yes |
| Extended Policy Capabilities | Yes | Yes | Yes | Yes | Yes |
| Onboarding Support | Yes | Yes | Yes | Yes | Yes |
| Extended Guest Management | Yes | Yes | Yes | Yes | Yes |
| Extended Profile Support | Yes | Yes | Yes (including sharing using pxGrid) | Yes | Yes |
| Extended Endpoint Compliance | Yes | Yes | Yes | Yes | Yes |
| Advanced Threat Protection and Mitigation | Yes (through ClearPass Exchange) | Yes (through Network Sentry/RTR) | Yes (through integration) | Yes (through ControlFabric) | Yes |
| Expanded Monitoring and Reporting | Yes | Yes | Yes | Yes | Yes |
| Extended System Integration and Interoperability | Yes (through ClearPass Exchange) | Yes | Yes (through Security Partner Ecosystem) | Yes (through ControlFabric) | Yes |

## VII. FEASIBILITY ANALYSIS

- Already a Cisco network, so NAC would simply be an add-on to current network
- Entry points can easily be identified
- Anti-virus and other end-point protections already deployed to users
- Non-compliance problems currently occur at a rate of 6 per day, indicating a positive ROI on a potential NAC investment

## VIII. CONCLUSION

Here goes finally state that a inclusive network access management system such as Cisco's Network Admission Control could be a better choice for investment rather than piecemeal improvements to the company's current network security systems. In future days the level of complexity of threats will increase, at the same time user needs a efficient mechanism to block those threats and have hassle free mechanisms to access all the websites. So a better integrated security systems could be developed using our recommended solution.

## REFERENCES:

[1] https://www.rivier.edu/journal/ROAJ-Fall-2007/J105-Sood.pdf
[2] http://searchsecurity.techtarget.com/tip/Network-access-control-Compliance-enabler-or-detractor
[3] http://www.networkworld.com/article/2209345/security/nac--what-went-wrong-.html
[4] http://searchsecurity.techtarget.com/tip/Integrated-security-suite-advantages-and-drawbacks
[5] https://en.wikipedia.org/wiki/Network_Access_Control
[6] http://www.tomsitpro.com/articles/network-access-control-solutions,2-916-2.html