NETWORK ACCESS CONTROL

Arti Sood*
Graduate Student, M.S. in Computer Science Program, Rivier College

Abstract

Computers connected to the Internet are very much part of every day life. People now use their computers in many different ways, such as online banking, online shopping, email, travel planning, news gathering, etc. It has provided users convenience and the ability to search for things on a moment's notice. However, by being able to easily log in to and access almost any worldwide site on the Internet, this has also exposed them to software called Malware, such as worms, viruses, Trojans, spy ware, data leakage and identity theft. Additionally, it places their networks at risk to which these computers are connected if they become infected. With an increased remote workforce, businesses also face these issues when their workers attempt to connect to the corporate network through Virtual Private Networks (VPN), or through a growing deployment of wireless technologies and mobile computing with devices, such as smart phones and PDAs. All these factors make Network Access Control (NAC) an important tool to have for today's businesses.

NAC controls the connections coming from the outside and also provides protection from every network connection coming from within the corporate firewall. It also provides security and controls for those, who has access to the network and its resources.

This paper describes what NAC is, what prerequisites are required to implement it, and its implementation process. It also introduces the larger network environment by discussing its main players, such as: Cisco, Microsoft, Trusted Network Group, and Juniper, who are involved in developing the technology and standards.

INTRODUCTION

The security started with antivirus software from Symantec, Trend Micro, and McAfee running on end devices which uses client server communication to update the virus definition files. Antivirus software was followed by software-based personal firewalls from Microsoft, Norton, Trend Micro, and ZoneAlarm which provided some access control. The software then transformed into firewall devices, IPSec VPN devices, and SSL VPN devices with an increasing need to access remote networks. This software finally took the form of the technology called Network Access Control which added another layer of protection against potential security threats. NAC, in its original form, was host posture check, quarantine, and remediation which involved a user seeking access to a network. If the user hadn't received recent OS patches or antivirus with an up-to-date virus definition running on its system, then the user would not be allowed in the network but instead would be placed on a VLAN or network (quarantine) until it was compliant with requirements of the network (remediation).

As technology is developing, NAC is not only granting access to the network sought by employees, guests, non employees, and protecting it against security threats but also controlling the access all over the network based on the user's role. The access to network is permitted, denied, or restricted based on the user's identity or membership to a particular group [4].

Copyright © 2007 by Arti Sood. Published by Rivier College, with permission.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

1 OVERVIEW

Network access control should perform five fundamental functions: pre-admission host posture checking; quarantine and remediation; identity aware and policy based authentication, resource access control, and post–admission check along with ongoing threat analysis and containment. No single vendor has solution that addresses all five NAC areas but customers are attempting to solve only portions of network access control problems. A few players in network access control technology are: Microsoft with its Network Access Protection (NAP) technology works through Windows Operating Systems; Cisco has Network Admission Control (NAC), which depends on Cisco's switching infrastructure; Trusted Network Group has standard based Trusted Network Connect (TNC); and Juniper has Unified Access Control (UAC), which uses TNC open standard specification. It is clearly becoming evident that network access control is moving towards framework architecture where various components work together to implement network access control [5].

2 TYPES OF NAC APPROACHES

As per the Garner's report [2], NAC solutions can take three main approaches or any combination of them. They are described below.

2.1 Software Agent

Software agent based solutions rely on the software residing permanently or temporarily on endpoint devices. This software communicates with and authenticates to a server in the network or an appliance.

2.2 Standalone Appliances (Inline and Out-of-band Appliances)

The inline solutions, such as, appliances, switches, firewall, and SSL VPN, work inline with network traffic and examine all the traffic and manage access as required. Though they offer mitigation options, they degrade the network performance and add a single point of failure.

Out-of-band solutions are adjunct to network infrastructure and require software agents on endpoint devices that direct traffic to the appliances as the user comes on network. This approach does not add a single point of failure but relies on existing network infrastructure to deal with policy violations.

2.3 Infrastructure-based NAC Capabilities

Infrastructure-based NAC capabilities integrated on switches or the software itself provide posture check and built-in authentication. This may require existing hardware to upgrade to enable NAC capabilities or upgrade to OS software to be perform network access control.

3 NAC FRAMEWORK AND FUNCTIONS

The key functional aspects of network access controls are: Posture assessment, Access control, Identity based resource control, Quarantine/Remediation, and Threat Assessment. They are performed by different components of the NAC framework (see Figure 1). The NAC products grant access to network based on factors like host assessment, host and user authentication, patch level, location, and even time of] day after undertaking four steps of assessment, decision, validation, and enforcement [7]. The laptop or client seeking access to the network sends over the assessment data required by the policy server. The

policy server validates the assessment data, consults the patch manager and the user directory, and grants limited or full access to the client based on the data.

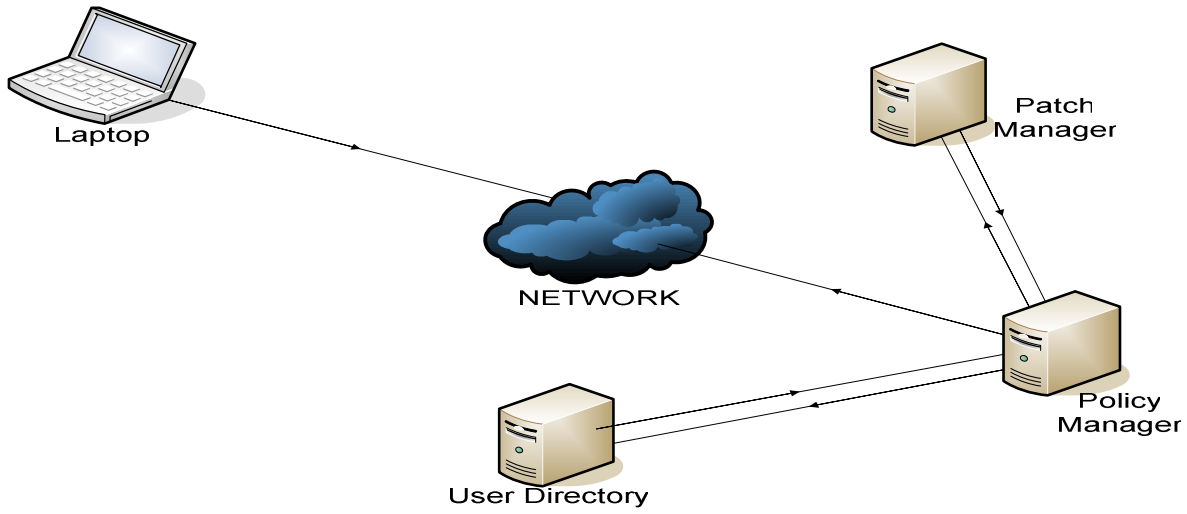

Figure 1: Network Access Control Framework

3.1 Posture Assessment

This is the first and foremost step in the NAC cycle and it requires pre-admission assessment and post admission assessment. NAC products consider various data points, such as, antivirus and anti spam status, patch level, firewall status and policy, authentication, logged-in users, access methods, and location as defined by IP address, to assess the state of host using the client software. The client software (called agent) uses different strategies, such as, persistent agent, dissolvable agent, remote procedural call, vulnerability scan, and passive monitoring to assess the health of the host seeking access. The software agent installed on the system performs the assessment. These are called **persistent agents** and need special privileges to be installed. There may another piece of software which gathers all the required data and reports to this software agent. The agents may be "on demand" installed on the PC only when the PC tries to access the network. They may be JavaScript or Active-X control (which are very useful in the case of unmanaged systems as used by guests or contractors), also called client less or **dissolvable agents**. These are mostly for unmanaged devices but they have limitation as they need appropriate permissions to run on the system [8]. There is the true agent-less method, where an agent is stored in a temporary directory until the endpoint is rebooted. It can be used to test endpoints without impacting the endpoint, since no install or download is required to obtain testing results. This method is useful for managed endpoints and networks with a centralized user-management system.

The server scans the computer seeking access to the network using the remote procedural call or WMI (Windows Management instrumentation). Although no software is required, however, the server needs administrative access to the machine to scan. The vulnerability assessment scan is again performed by the server to determine the OS and services running on the system. Finally, passive monitoring can perform intrusion detection and monitor authentication requests and responses on the system. The post-admission assessment occurs after the network access has been granted.

3.2 Access Control

The data collected about the host is sent to the **policy server** using the protocols, such as, 802.1x, EAP or other proprietary protocols, which makes the decision of allowing the access and enforcement to be done through devices, such as, switches, routers, or other methods that can use IPSec, 802.1x, VPN, or DHCP for host authentication. The policy selection is crucial for a successful NAC deployment. The policy that governs the system may have a more up-to-date signature file or OS patches installed on the system.

3.3 Identity-based Resource Control

The access is allowed to a specific part of the network depending on the identity of the user provided by means of username/password, software token, hardware token (e.g. RSA token, smartcards, or biometrics) after it has been authenticated against the **authentication server** which may be RADIUS, LDAP, Microsoft's Active Directory, Novell's eDirectory, etc. The network admission policies may be determined not only on the basis of user identity but also on the basis of the resource being accessed, user/group role in organization, group membership device health, device location, device type, and time of the day.

3.4 Quarantine/ Remediation

In case the host fails the policy, it may be placed in VLAN where the user is redirected to a website to download the latest version of antivirus or OS patch or **AV and patch manager** to bring it into compliance.

3.5 Threat Assessment

This is the ongoing effort after the host has been granted the access to the network. The host may be continuously checked for the posture by means of 802.1X re-authentication, a scheduled reassessment, or passive monitoring.

4. NAC MODES OF OPERATIONS

4.1 VLAN Steering

This moves the host and switch ports onto specific virtual VLAN like guest VLAN and may be used just to give Internet access to visitors.

4.2 802.1x

IEEE 802.1x standard manages port-based access. It authenticates devices attached to LAN ports by initiating the connections and requesting login details. Access is prevented if the user fails authentication. IEE 802.1x attaches EAP to both wired and wireless media and supports multiple authentication methods, such as, tokens cards, one-time passwords, certificates, and public key authentication. It was designed to accommodate and allow network control at port level, authentication, authorization, accounting technology, public network security, and distribution of dynamic encryption keys.

The key elements of the framework are supplicant, port, authenticator, Extensible Authentication Protocol, EAP over LAN, and RADIUS (see Figure 2).

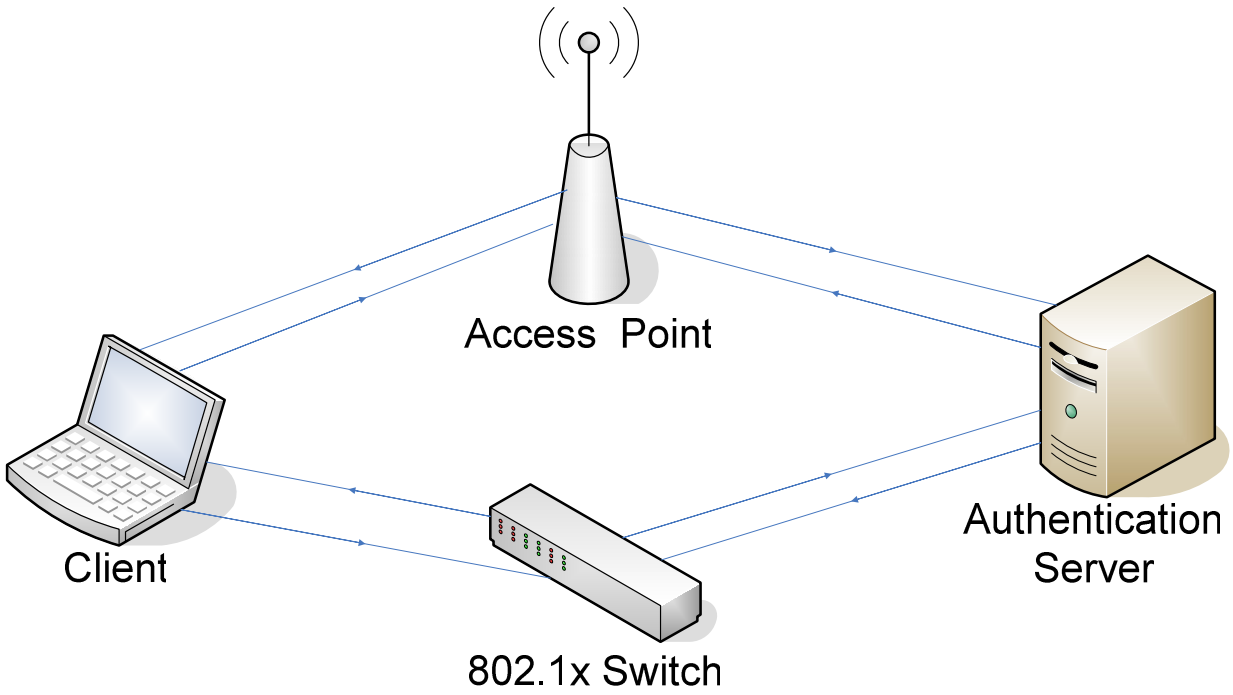

Figure 2: 802.1x Authentication

The supplicant is the client that grants the network access and use EAP over LAN (EAPoL) messages for management functions, such as, start, log off, and key distribution. The port is where the device is attached either directly into a 802.1x switch or wireless access point. The wireless access point is called authenticator and it acts as a go between supplicant and authentication server. RADIUS server manages the database of users, provides authentication by verifying username and password provides authorization, such as, dynamic VLAN assignment, and provides accounting information about how long a user was connected and how much data they transferred.

This is the most secure network access control technology.

4.3 DHCP

DHCP sever passes out leases and host configuration information. The access can be controlled by controlling the issuing of the IP address.

4.4 VPN

VPN can be used to restrict access by rejecting non-VPN traffic, thus disallowing traffic from an infected host or attacker. The VPN servers may also be able to handle encryption and decryption.

5. NAC VENDORS

There are many vendors in the network access control arena but few are chief contenders because they have too much at stake due to a large portfolio of products. This forms fabric of a network for Cisco, Juniper, and Microsoft.

5.1 Cisco NAC (Network Admission Control)

Started as Self-Defending Network Initiative (SDNI) to dramatically improve the network's capability to identify, prevent, and adapt to threats. The initiative had plans to make every piece of Cisco gear a security enforcement point, where client machines must meet security and policy criteria to access a router or switch port [9]. Cisco partnered with Trend Micro, Symantec, and Network Associates to make client-side anti-virus software work with Cisco's Trust Agent, a PC-based software agent that communicates client security status to Cisco network equipment and security servers.

NAC Phase I was planned to use message based on Extensible Authentication Protocol (EAP), running over User Datagram Protocol (UDP) or at Layer 3. Access control lists (ACL) on routers set to block all traffic except EAP over UDP (see Figure 3). NAC phase II was planned to provide access control for wireless devices at a time when authentication scheme was moved to EAP over 802.1X to offer NAC support for Layer 2 switches. Recently, Cisco launched a NAC appliance which offers Layer 2 support using EAP using 802.1X framework. It was made possible by an acquisition of a Portsmouth-based company called meeting house (see Figure 4). Though it is moving from proprietary strategy and towards appliance, a self contained NAC solution, called Cisco‘s Clean Access NAC appliance, Cisco still lacks a strong policy tool [10].

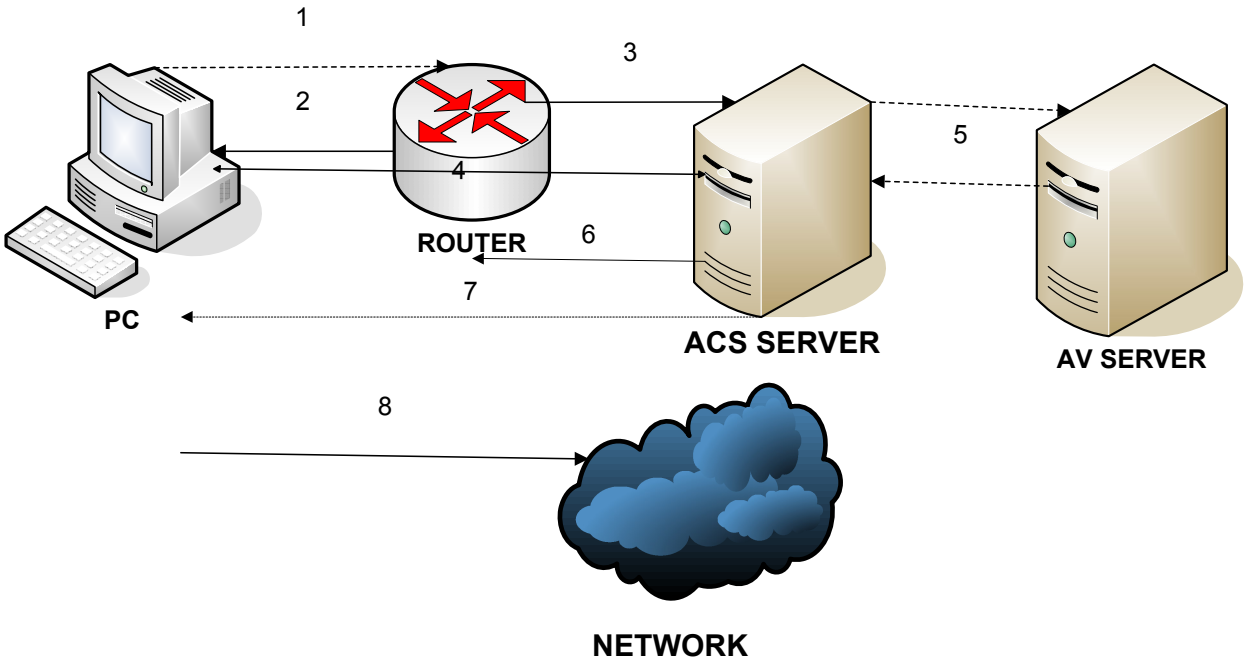

Figure 3: NAC L3/L2 IP Architecture Overview

As per step one, the endpoint sends a packet through the router on to its destination. The packet matches the *Intercept ACL* applied to the router's interface, which initiates the NAC-L3-IP posture-validation process. The second step involves setting a tunnel between the agent on the endpoint and the ACS server. The third step involves establishing a secure tunnel RADIUS tunnel between the router and the ACS server. The fourth step involves PEAP or a Protected Extensible Authentication Protocol tunnel between the endpoint and ACS server to exchange the posture credentials. The posture credentials may be passed on to the Antivirus server, as per step five, for further validation using the Host Credentials Authorization Protocol (HCAP). As per step six, the host is assigned a security posture by the ACS server based on the results of the rules defined by administrator on the ACS server. As per step seven, the user's browser may be directed to a remediation server if the host is deemed unhealthy; otherwise, it is permitted full access as per step eight.

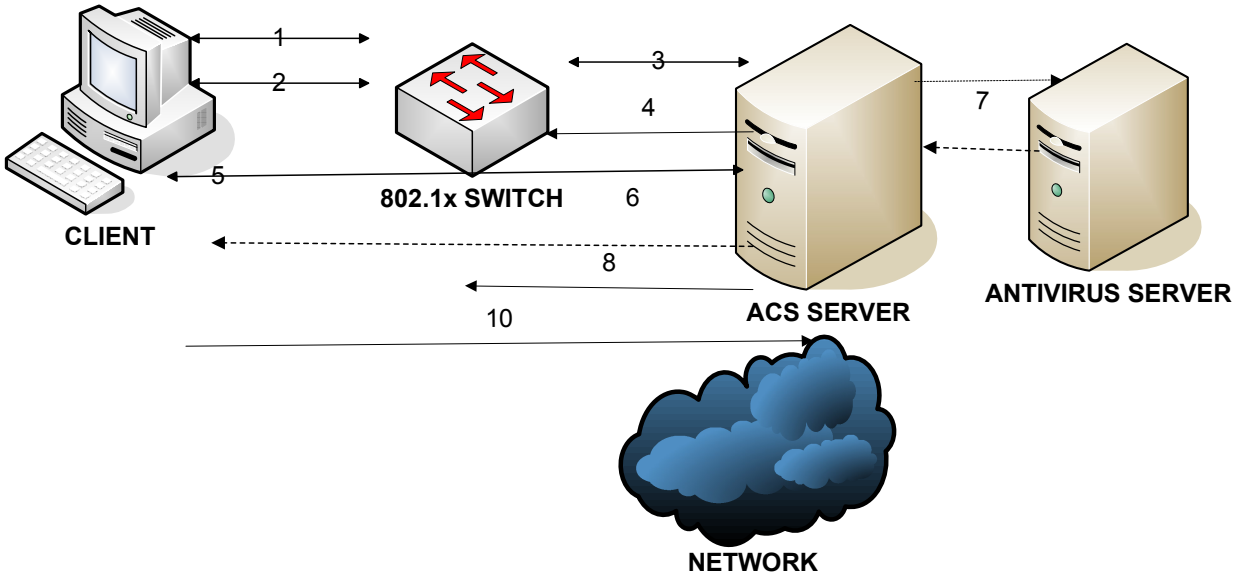

Figure 4: NAC L2 Architecture Overview

As per step 1, endpoint is attached to a switch port. As soon as step 2, the link comes up and 802.1X supplicant sends an authentication request to the 802.1x switch. In step 3, the user credentials are passed to the ACS server via RADIUS. Step 4 has the ACS server authenticating the user. In step 5, there is a FAST tunnel established between the agent on the machine and the ACS server over the sessions established by 802.1x switch and RADIUS. As per step 6, user credentials are requested by the ACS server. Step 7 is optional where the ACS server proxies posture credentials for extra validation to the AV server using HCAP. In step 8, as defined by the security policy on the ACS server to posture credentials, the posture is applied to a host which is further applied to the port to which the machine is connected. In step 9, the ACS server can send a message to the host to redirect it to the remediation server. Finally, in step 10, the host is granted or denied access to the network based on its posture and VLAN assignment [11].

5.2 Microsoft NAP (Network Access Protection)

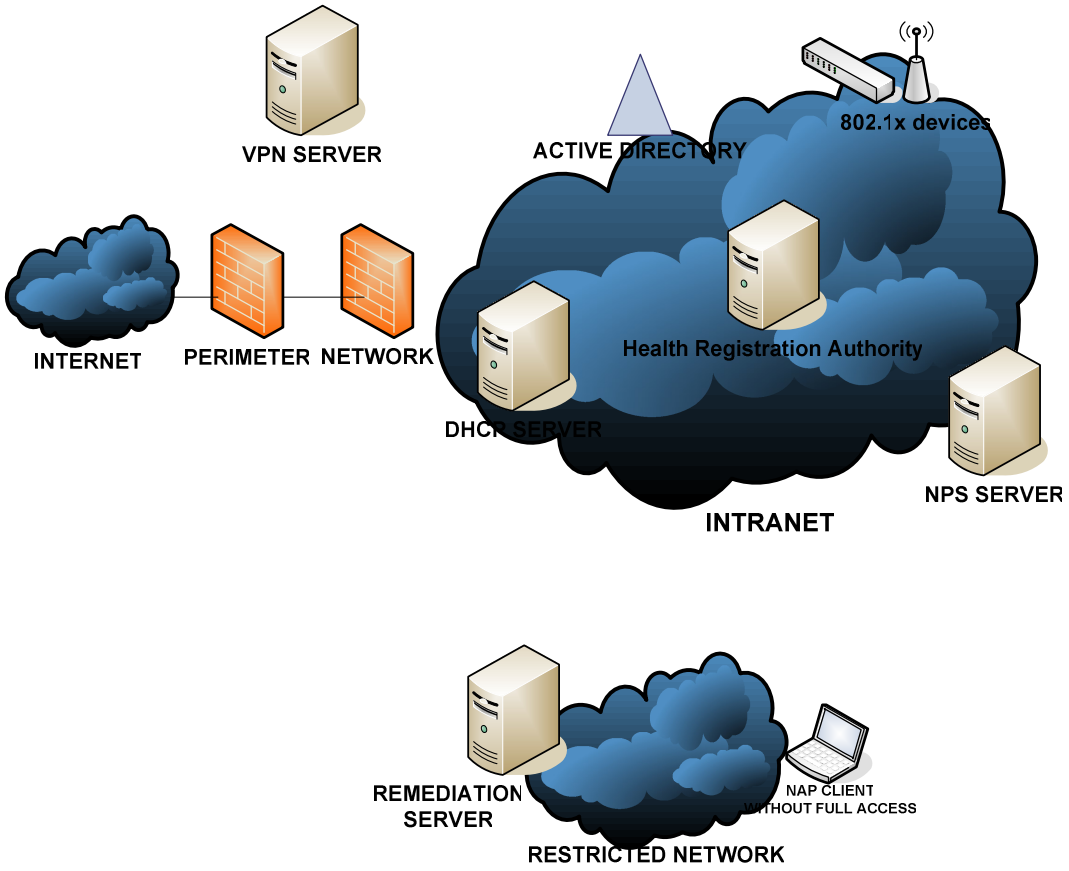

Figure 5: NAP Framework

NAP was announced as a set of extensions for the Windows Server 2003 and Microsoft Windows XP [12]. NAP is software only framework and Windows-specific that includes Active Directory, a server called Network Policy Server (NPS), a NAP agent that will be shipped with Longhorn, Vista, and as an upgrade to XP SP2. The framework also has SHAs (System Heath Agents) which includes desktop firewalls, antivirus scanners, and patch management systems. The status reports referred to as Statements of Health (SoH) are sent by SHA to another server called HRA (Health Registration Authority). The IAS server will be also required if remote access is required. The NPS integrates with external authorities like antivirus and patch management servers to retrieve the current configuration information. The endpoints are issued Health Certificates by the HRA or directed for remediation if they fail the health check. In the NAP framework, the client connects to the 802.1X switch to pass authentication and present Health Certificates to NPS. Following the authentication, an appropriate VLAN is provided for access, quarantine, or remediation. The other components of the NAP framework include the 802.1x devices (Access points and switches), DHCP server, Remediation servers handling the clients with limited access, and Active Directory maintaining the user information. See Figure 5 for NAP framework components.

5.3 Juniper UAC (Unified Access Control)

UAC is delivered as a complete solution based on TNC standard which interoperates with any vendor‘s 802.1x enabled switch or access point, any platform (Solaris, Windows, Macintosh or Linux), and works for any type of user contractor, employee, or guest, allowing them appropriate resources. The solution works with existing infrastructure with or without 802.1X. The solution comes with a centralized policy server referred to as an Infranet Controller (IC). All details, such as, user identity, device state, and network location can be determined by dynamically deployable agents, as well as, through an agentless mode where it is not feasible to install the software client. The solution forces policy at Layer 2 (Data Link layer of 7 layer OSI model) with any vendor‘s 802.1x enabled switch or wireless access point. It also enforces at layers 3 through 7 using Juniper‘s firewalls. It has dynamic endpoint assessment and seamless interaction with AAA backbone. The various components are: policy enforcer Infranet Controller (IC), 802.1x supplicant Odyssey Access client (OAC), and Steel-Belted Radius Server (SBR) (see Figure 6).

The agent also includes the Host Checker functionality which enables scanning of the endpoints for a variety of security applications, such as, personal firewalls, antivirus, and malware. It also includes custom checks of registry, port status, and MD5 checksum to verify an application’s validity. UAC allows network access to users to only those resources for which the user has been authorized.

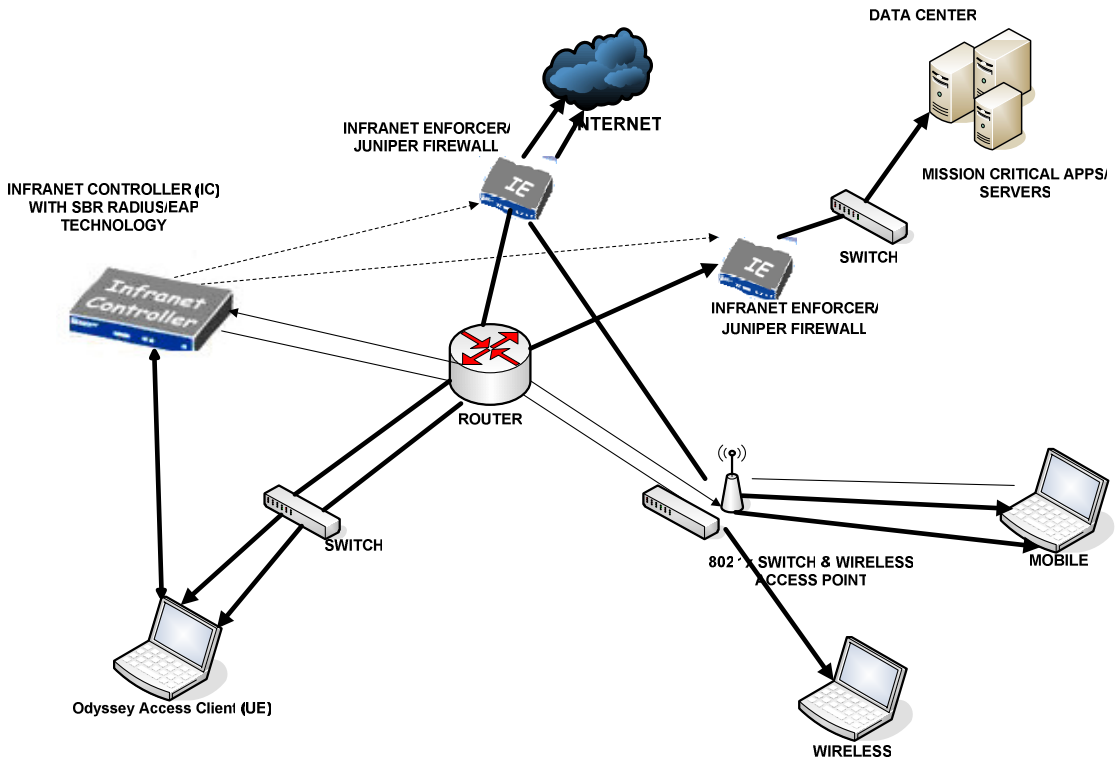

Figure 6: Unified Access Control Version 2.0

By adhering to the open standard by TNC, UAC allows organizations to leverage their existing heterogeneous network by quickly and effectively applying network access control. It enables high flexibility and return on investment for the organization (see Figure7). A TNC client on the agent side

runs on the endpoint which communicates with the TNC sever running on the Infranet Controller responsible for authentication. The TNC client provides the update to the server about the posture of the client [17].

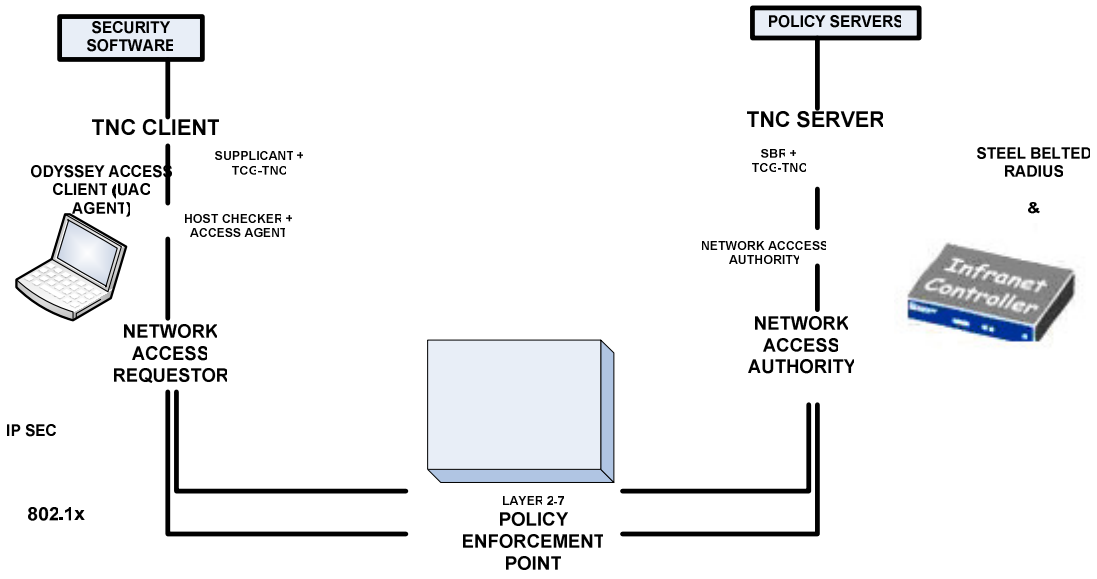

Figure 7: UAC – TNC implementation

6. NAC STANDARDS

The proprietary solutions tie the user to one vendor, today‘s networks have networking equipment from wide range of vendors, therefore only open, multi-vendor NAC standards can achieve inoperability and meet challenges of borderless networks.

6.1 Trusted Networking Group (Trusted Network Connect)

Trusted Networking Group (TNG) formed in 2003, lays out Trusted Network Connect specifications, defining an open access control method similar to proprietary efforts from Cisco Systems and Microsoft Corp. It has more than 135 members with expertise in antivirus, firewall products; switches, routers and hubs; network security; systems management; and operating systems. Originally, every one except Cisco, worked together to define on open architecture for network security and endpoint integrity.

TNC builds on work from the IEEE's 802.1x authentication group, and the IETF's Extensible Authentication Protocol, TLS, and RADIUS, but adds higher-layer functions for policy definition and policy enforcement. Network clients, called "supplicants" in 802.1x parlance, use the flash memory-based TPM to gather statistics known as integrity measurement collectors (IMC) in the TNC model [13][15]. The policy enforcement occurs at the switch, firewall, or VPN gateway device that have 802.1x and EAP support automatically support TNC. TNC NAC architecture is implemented by Access Requestor (AR), the Policy Enforcement Point (PEP), and the Policy Decision Point (PDP). The PEP consults PDP to grant the access to AR when it attempts to access the network protected by PEP. There are three layers: Network Access Layer, Integrity Evaluation Layer, and Integrity Measurement Layer. In each layer, the AR and PDP have components.

The network access layer has Network Access Requestor (NAR) on endpoints (network nodes) which negotiate and establish network access along with implementing security, such as, 802.1x supplicants, VPN clients, and web browsers initiating SSL, are all NARs for Access Requestor. The PEP is the network infrastructure device, such as, switch, wireless AP, or a VPN concentrator which can control the access. The PEP is controlled by PDP which determines whether the endpoint should be admitted to network and the level of access to be granted. The PDP is Network access Authority (NAA) which may be RADIUS server.

The integrity evaluation layer has a TNC client that collects integrity measurements from Integrity Measurement Collectors (IMCs), which are plug-in modules. It reports the health of the endpoint and delivers reports [Integrity Measurements (IMs)] to a TNC server in PDP component. The TNC server delivers the IM to Integrity Measurement Verifiers (IMV), which checks the state of the endpoint against the policy.

The integrity measurement layer has IMC(s) and IMV(s). Additionally, there are interfaces or plug-in APIs, such as: IF-IMC between the TNC client and IMC, IF-IMV between TNC server and IMV, IF-TNCCS between TNC client and server, and IF-T for Tunneled EAP Methods, such as, EAP-TTLS, EAP-FAST, and EAP-PEAP allowing the TNC architecture to work with networking technologies that support EAP authentication like 802.1x and IKEv2. Finally IF-PEP or RADIUS specifies the usage of the RADIUS protocol between NAA (AAA/RADIUS server) and PEP.

CONCLUSION

Though this paper has concentrated on three popular vendors, the NAC market is exploding with various product offerings from companies like Trend Micro, Symantec, Enterasys, and McAfee. **Infonetics Research** estimates that worldwide annual sales of NAC enforcement systems will reach **almost $3 billion by the start of 2009**. There will be continuous debate in the future about using the network integrated devices, network enforcement applications, or the SSL VPN for network access control. This will become better defined as the market matures [16].

GLOSSARY

AAA Server: Authentication Authorization Accounting Server
API: Application Programming Interface
DHCP: Dynamic Host Configuration Protocol
EAP: Extensible Authentication Protocol
EAP-FAST: EAP Flexible Authentication via Secure Tunneling
EAP-PEAP: EAP Protected Extensible Authentication Protocol
EAP-TTLS: EAP Tunneled Transport Layer Security Protocol
IEEE: Institute of Electrical and Electronics Engineers
IETF: Internet Engineering Task Force
IKE: Internet Key Exchange Protocol
IPSec: Secure Internet Protocol
LDAP: Lightweight Directory Access protocol
OS: Operating system
SSL: Secure Socket Layer
VLAN: Virtual Local Area Network
VPN: Virtual Private Network

REFERENCES

[1] Network Access Control: An Introduction. Retrieved from http://www.itsecurity.com/features/introduction-network-access-control-120506/ on April 12, 2007.

[2] Network Access Control: Securing the Perimeter. Retrieved from http://www.networksecurityjournal.com/features/network-access-control-securing-the-perimeter-031607/ on April 12, 2007.

[3] Network Access Control Decision Framework. Retrieved from www.cisco.com/global/ES/pdfs/2006_10_gartner-NAC_decision_fr.pdf on April 22, 2007.

[4] Defending an Expansive Definition of NAC. Retrieved from http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci1226473,00.html on April 12, 2007.

[5] NAC and Endpoint Security Frameworks: Which Way to Go? Retrieved from http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci1228723,00.html on April 22, 2007.

[6] NAC Vendors vie Over Architecture, Product Direction. Retrieved from http://www.networkcomputing.com/gswelcome/showArticle.jhtml?articleID=197000856 on April 22, 2007.

[7] Analysis: Network Access Control. Retrieved from http://www.networkcomputing.com/channels/security/showArticle.jhtml?articleID=193101592 on April 12, 2007.

[8] NAC underneath the Covers: Endpoint Health Assessments. Retrieved from http://searchnetworking.techtarget.com/general/0,295582,sid7_gci1228598,00.html on April 14, 2007.

[9] Cisco to Unleash Security Plan. Retrieved from http://www.infoworld.com/article/04/06/18/HNcisonet_1.html on April 23, 2007.

[10] NAC Enforcement Tools Fall Short. Retrieved from http://www.networkworld.com/reviews/2007/041907-nac-intro.html on April 23, 2007.

[11] NAC Solution and Technology Overview Retrieved from http://www.informit.com/articles/article.asp?p=680828&rl=1 on April 24, 2007.

[12] Network Access Protection Platform Architecture, Microsoft Corporation. Retrieved from http://www.microsoft.com/technet/network/nap/naparch.mspx on April 12, 2007.

[13] Trusted Net Specifications Gain Broad Support. Retrieved from http://www.eetimes.com/showArticle.jhtml;jsessionid=M1YA00UUKGPT0QSNDLOSKHSCJUNN2JVN?articleID=187200845 on April 25, 2007.

[14] Remote User Dial-In User Service. Retrieved from http://www.faqs.org/rfcs/rfc2865.html on April 12, 2007.

[15] Build Borderless Networks You Trust. Retrieved from http://www.networksystemsdesignline.com/showArticle.jhtml;jsessionid=5VJAEIBNIFAF0QSNDLRSKH0CJUNN2JVN?articleID=187002030 on April 25, 2007.

[16] What You Should Know About Network Admission Control. Retrieved from http://sslvpn.breakawaymg.com/eps/NAC.php on April 25, 2007.

[17] Juniper Unified Access Control 2.0. Retrieved from http://www.juniper.net/products_and_services/unified_access_control/ on April 26, 2007.

---

* **ARTI SOOD** received her Bachelor's degree in Science and Education from Punjab University, India. After obtaining P.G. Diploma in Computer Science, she worked as database application developer. She moved to the U.S. in 1996 and worked with Emerging Markets, Inc., and Gambit Communications, Inc. on web development and network simulation tools till 2005. Arti works currently as Senior Quality Assurance Engineer at Juniper Networks, Inc. developing security products and pursuing M.S. in Computer Science at Rivier College.