Regis University

ePublications at Regis University

Regis University Student Publications (comprehensive collection)

Regis University Student Publications

Fall 2007

Network Access Control: Disruptive Technology?

Craig Fisher
Regis University

Follow this and additional works at: https://epublications.regis.edu/theses

 Part of the Computer Sciences Commons

Recommended Citation

Fisher, Craig, "Network Access Control: Disruptive Technology?" (2007). *Regis University Student Publications (comprehensive collection)*. 94.
https://epublications.regis.edu/theses/94

This Thesis - Open Access is brought to you for free and open access by the Regis University Student Publications at ePublications at Regis University. It has been accepted for inclusion in Regis University Student Publications (comprehensive collection) by an authorized administrator of ePublications at Regis University. For more information, please contact epublications@regis.edu.

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

Network Access Control: Disruptive Technology?

Craig Fisher

Regis University

School for Professional Studies

Master of Science in Computer Information Technology

Abstract

Network Access Control (NAC) implements policy-based access control to the trusted network. It regulates entry to the network by the use of health verifiers and policy control points to mitigate the introduction of malicious software. However the current versions of NAC may not be the universal remedy to endpoint security that many vendors tout. Many organizations that are evaluating the technology, but that have not yet deployed a solution, believe that NAC presents an opportunity for severe disruption of their networks. A cursory examination of the technologies used and how they are deployed in the network appears to support this argument. The addition of NAC components can make the network architecture even more complex and subject to failure. However, one recent survey of organizations that have deployed a NAC solution indicates that the 'common wisdom' about NAC may not be correct.

Table of Contents

1 Introduction 1-1
1.1 What is the Problem 1-1
1.2 What is Network Access Control 1-4
1.3 Why use Network Access Control 1-5
1.4 Who is offering Network Access Control 1-6
1.5 Organization of Material 1-7
2 Terms 2-1
3 Research Methodology 3-1
4 Components of NAC 4-1
4.1 Network Access Policy 4-1
4.2 Secure Communications 4-1
4.2.1 OSI Reference Model 4-2
4.2.2 Encryption 4-3
4.2.3 Secure Sockets Layer (SSL) 4-12
4.2.4 Tunneling Protocols 4-14
4.2.5 Remote Authentication Dial-in User Service (RADIUS) 4-22
4.3 Infrastructure 4-24
4.3.1 IEEE 802.1x Standard 4-24
4.3.2 Virtual Private Network 4-25
5 Network Access Control 5-1
5.1 NAC Frameworks 5-1
5.2 NAC Appliances 5-4
6 Areas of Concern 6-1
6.1 Future Enterprise Network Infrastructure 6-1
6.2 Endpoint Control 6-1
6.3 Architectural Considerations 6-2
6.3.1 Nontechnical impact 6-2
6.3.2 Network Availability 6-3
6.3.3 Network Monitoring 6-3
6.3.4 New technologies 6-4
6.4 Complexity 6-4
6.5 Interoperability 6-5
7 Project Conclusions 7-1

7.1 Analysis of results 7-1
7.2 Project Summary 7-5
8 References 8-1
9 Supplemental Material 9-1
9.1 Network Access Control Frameworks 9-1
9.1.1 Cisco's Network Admission Control 9-1
9.1.2 Microsoft's Network Access Protection 9-8
9.1.3 TCG's Trusted Network Connect 9-26
10 Annotated Bibliography 10-1

Table of Figures

Figure 1-1 - Enterprise Network Perimeter 1-3
Figure 1-2 - Reduced Perimeter Network 1-4
Figure 4-1 - OSI Reference Model 4-2
Figure 4-2 - OSI and TCP networking models 4-3
Figure 4-3 - Symmetric encryption 4-5
Figure 4-4 - Asymmetric encryption 4-5
Figure 4-5 - Creating a digital signature 4-7
Figure 4-6 - Registration 4-9
Figure 4-7 - PKI Session 4-10
Figure 4-8 - TLS Session 4-14
Figure 4-9 - EAP exchange (Source: Aboba et al.) 4-19
Figure 4-10 - RADIUS infrastructure (Source: Harris) 4-23
Figure 4-11 - Typical 802.1x Network Environment (Source: Juniper Networks) 4-24
Figure 4-12 - Security Protocols and OSI Protocol Stack (Source: Disabato) 4-27
Figure 4-13 - Remote Access VPNs (Source: Young) 4-27
Figure 5-1 - IETF NAC Framework (Source: InteropLabs) 5-2
Figure 5-2 - IETF NAC Terms (Source: InteropLabs) 5-3
Figure 5-3 - Network Access Scenario 5-4
Figure 5-4 - In-band NAC Appliance (Source: Hanna) 5-5
Figure 5-5 - Out-of-band NAC Appliance (Source: Hanna) 5-6
Figure 7-1 - Regulatory Accountability (Source: Dornan) 7-2
Figure 9-1 - Cisco NAC Process (Source: InteropLabs) 9-4
Figure 9-2 - Cisco Access Scenario (Source: Cisco Systems) 9-4
Figure 9-3 - Microsoft NAP Process (Source: Microsoft) 9-9
Figure 9-4 - NAP Client Architecture (Source: Microsoft) 9-10
Figure 9-5 - NAP Enforcement Clients 9-11
Figure 9-6 - NAP Server Architecture (Source: Microsoft) 9-12
Figure 9-7 - NAP platform components interactions (Source: Microsoft) 9-14
Figure 9-8 - NAP-enabled Components (Source: Microsoft) 9-17
Figure 9-9 - IPsec enforcement logical networks (Source: Microsoft) 9-18
Figure 9-10 - How IPsec Enforcement Works 9-19
Figure 9-11 - How 802.1x Enforcement Works 9-21
Figure 9-12 - How VPN Enforcement Works 9-22
Figure 9-13 - How DHCP Enforcement Works 9-24
Figure 9-14 - TNC NAC Process (Source: Hanna) 9-27
Figure 9-15 - TCG TNC Framework (Source: Hanna) 9-28
Figure 9-16 - TNC Authentication Message Flow (Source: Hanna) 9-32

1 Introduction

Network Access Control (NAC) implements policy-based access control to the trusted network. It regulates entry to the network by the use of health verifiers and policy control points to mitigate the introduction of malicious software. A large number of vendors currently offer hardware or software solutions, with Cisco, Microsoft, and Juniper Networks providing comprehensive NAC frameworks. However the current versions of NAC may not be the universal remedy to endpoint security that many vendors tout. Some organizations that are evaluating the technology, but that have not yet deployed a solution, believe that NAC presents an opportunity for severe disruption of their networks. However this view is not shared by those who have deployed NAC solutions. Which group is correct?

This project addresses the proposition of NAC being a disruptive technology by:

- Explaining the need for NAC;
- Discussion of the components used by NAC;
- Explanation of the methods used to control network access;
- NAC frameworks and appliances;
- Areas of concern when deploying NAC;
- Observations and conclusions about the NAC impact to the network.

1.1 What is the Problem

To understand the problem that NAC solves it is helpful to talk about a real world issue that has existed for thousands of years. Almost since the time when people first collected in groups there has been a notion that some people were not welcome in some areas. Perhaps members of one tribe were excluded from another tribe's village. To enforce this exclusion, guards were posted at the perimeter of the village and anyone entering was examined for their identity to make sure they were welcome. During time of devastating sickness like plagues, each person entering the village or city might also be looked at for symptoms of the disease. Of course the purpose of both these checks was to protect the people within the enclosure from two things: malevolent or undesirable

people, and people who were ill. Both of these could have caused enormous damage to the population. There is a similar problem with a company's network.

If access is stopped at the client device (computer, PDA, Smartphone, etc.) then that device, and also the user of that device, are severely limited in the damage that can be perpetrated on the network resources. However, the problem with most organizations today is that the accessing device is allowed within the network perimeter while the rights of the device to be within the perimeter are ascertained. In the walled city analogy, this would be the same as allowing the person seeking admittance the freedom to roam about the city while their identity is examined.

One of the most dreaded security scenarios for many organizations is when a device accesses the trusted network and deposits a piece of malware that propagates to thousands of systems within a short period of time. Although security policy dictates that client systems must have the latest patches, current virus signatures, and that anti-malware software is current and operating, client systems may not be compliant with the policy, especially those devices that are not resident on the network all the time like telecommuters, mobile users, and employees working from a home system, guests, or clients. For this reason, it is also important that the health (its security posture) of the device be determined before access to the trusted network is allowed.

Maintaining a secure network begins when a user or system seeks access to the network. To prevent unauthorized access, to manage risk of noncompliance to security policy, and to control the spread of malicious software, enterprises must examine each endpoint (client device) before access is granted to network resources to ensure that the endpoint meets the enterprise's policies for network admission.

For the purpose of this paper, systems joining or existing at the ends of the enterprise network are referred to as endpoints. Technology advances have broadened the definition of what an endpoint system can be. Devices attempting to attach to the corporate network can include desktop computers, laptops, personal digital assistants, Smartphone, and other types of special equipment. Essentially any device that connects to the corporate network can be considered an endpoint device. Although servers and some similar systems do connect to the internal network, what is of primary concern are those systems that can be infected by malware from activities when detached from the internal network. These activities include email access, web browsing, instant messaging, and other activities performed through a public network (Mariwald, 2007, pp. 5-7).

Figure 1-1 illustrates a simplified view of an enterprise network that hosts a variety of employee and guest users, as well as remote users and other devices. The green area represents the internal or trusted network.

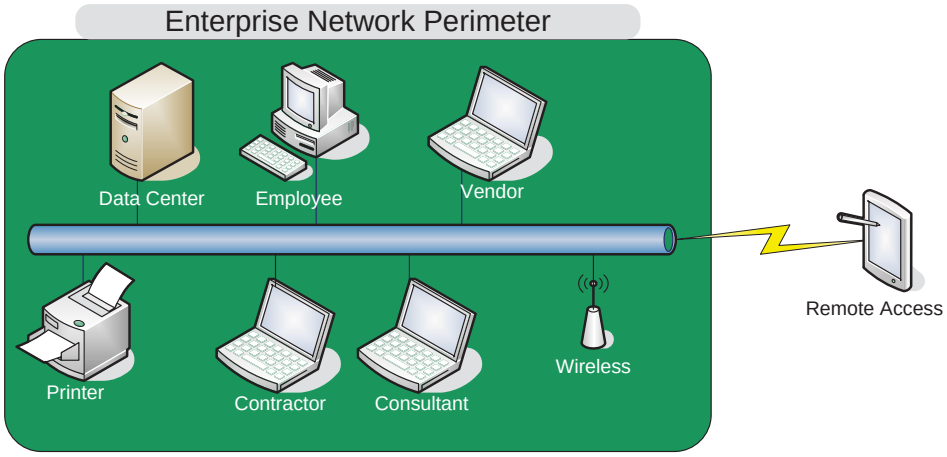


Figure 1-1 - Enterprise Network Perimeter

Organizations use multiple strategies to mitigate the problems of access from within the internal network. Organizational security policies mandate that endpoint systems have the latest operating system patches, the most current antivirus signatures, and perhaps personal firewalls installed on the client system. However, there is no assurance that employees, especially those whose systems may spend a great deal of time off the corporate network, or home systems used to access the internal network through a SSL VPN or dial-up, adhere to the policy.

This mobility of enterprise users, the addition of guest users such as contractors and vendors attaching to the internal network, must eventually shrink the perimeter of the internal network back to the datacenter in order to protect the core information assets of the enterprise. Figure 1-2 illustrates the new perimeter.

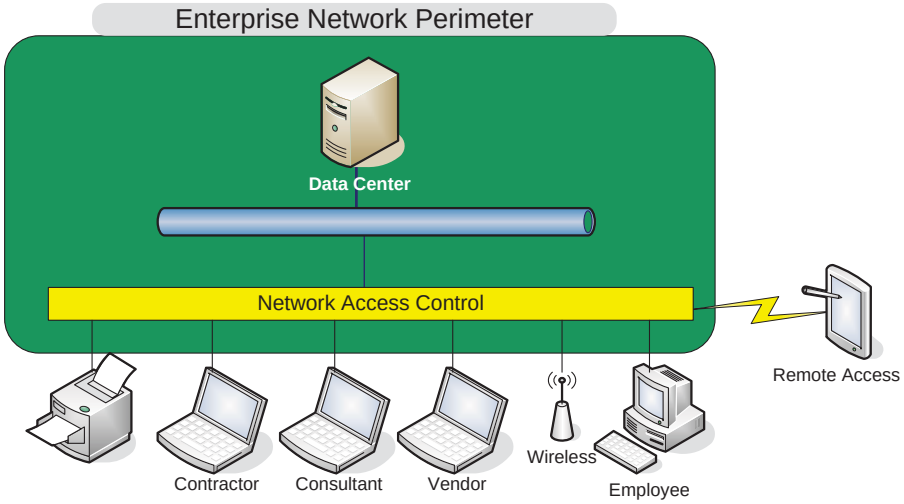


Figure 1-2 - Reduced Perimeter Network

To address this issue, corporations are focusing on ensuring that an endpoint is compliant with the organization's security policy at the time when it connects to the trusted network, and if it is not, to force remediation before allowing access. Access policy may require verification of the endpoint's posture (is it "healthy"?), its security assessment (does it have the latest patch level and virus signatures?), and does the endpoint meet the access policy criteria (user and device identity, location, time-of-day, and other access policy requirements). To address this issue, corporations are evaluating, and in some cases, deploying NAC solutions.

The Network Endpoint Assessment Group (NEA) of the Internet Engineering Task Force (IETF) states in their NAC requirements document that "…network operators need a proactive mechanism to assess the state of systems joining or present on the network to determine their status relative to network compliance policies" (NEA Overview and Requirements, 2007).

1.2 What is Network Access Control

NAC is a concept that controls network access and network resource usage "based on user authentication, endpoint behavior, and an assessment of the device's identity and security properties" (Mariwald, 2007, p. 6).

User authentication identifies the user requesting access to the network. Typically this is done today through a user identifier and password, but can involve other factors of authentication, such as fingerprint or a security token like a JavaCard.

The security posture (health) of the endpoint is another aspect of the network security policy. This check ensures that the endpoint device has the latest operating system and application patches, current anti-virus signatures, a personal firewall enabled, and perhaps a requirement may also exist to ensure that no unauthorized applications are on the device (Sturdevant, 2007). Other areas that may determine access to the internal network could be the user's group membership, the time of day, and the user's authorization to access the network.

Device identity and security properties may also govern the level of access and resources that are permitted. Before an endpoint is allowed onto the network, or the use of a network resource, its compliance to the network access-control security policy should be checked. The network access-control policy can cover a wide spectrum of control choices from a simple GO-NO GO decision on network access, or it can involve complex rules, such as the parts of the network accessible to the endpoint (Snyder, 2006).

When fully implemented, NAC will be able to apply policy across (1) the wired and wireless local area network (LAN), (2) SSL Virtual Private Network (VPN) remote access where a single user is executing IPsec or SSL VPN client, and (3) VPN-connected site-to-site (perhaps from a branch office) (Getting Started, 2006).

1.3 Why use Network Access Control

NAC is one attempt to reestablish the network perimeter. This control can occur before an endpoint device is allowed onto the network, and it can also be an ongoing evaluation of the endpoint during the time it is accessing the network. This is normally referred to as preadmission and postadmission assessment, respectively.

Enterprises have a strategic need to control access to their networks which by extension controls access to their information and application resources. NAC attempts to solve the following four problems:

- User and endpoint identification and authentication
- Security policy criteria for accessing network resources. This can include user identity, device configuration, or device security posture.
- Limit access or quarantine devices that do not meet security policy criteria
- Ability to remediate a device before allowing unrestricted access to network resources (Maiwald, 2007)

The most often stated reasons for deploying a NAC solution are:

- Restrict nonemployee access to network
- Restricting access based on the endpoint security posture (does it have a virus?)
- Regulatory compliance: Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), and other regulatory requirements
- Restrict user network access based on the "health" or security posture of the endpoint device (Maiwald, 2007, p. 7)

Universities have seen the greatest need for NAC solution because the students typically own their own computers, and in many cases these computers could be infected with viruses before joining the university network. In the past the university was not able to enforce network policy that would require anti-virus software but with NAC, this is changing. Arizona State University deployed Cisco's Clean Access technology to scan each computer before it joins the network to ensure that it adheres to network security policy. Non-compliant computers are quarantined until automated processes can bring the computer into compliance (Burger, 2007).

1.4 Who is offering Network Access Control

Three existing or emerging architectures address the problems described – Cisco's Network Admission Control (NAC), Microsoft's Network Access Protection (NAP), and The Trusted Computing Group's Trusted Network Connect (TNC) have products or proposals to address this issue with similar but different technology frameworks. Each has its supporters, and in many cases, many partners are hedging their bets by implementing support for each framework.

To help the interoperability of the different approaches, the IETF NEA Group is looking at defining a layer of communication to bridge the gaps between these competing architectures. Also to address the problem of interoperability, in 2006, Cisco and Microsoft agreed to have their two frameworks interoperate, and in May, 2007, TCG TNC and Microsoft introduced a change to the TNC specification to interoperate with Microsoft NAP.

In addition to the frameworks, there are a plethora of small companies offering NAC appliances that target some aspect of NAC but many of these are islands within the manageability ocean. Network administrators are often forced to have multiple tools to manage all of the devices on their network.

The absence of a single standard for NAC, and the fact that Microsoft will not release NAP until Windows Server 2008 timeframe, has many corporations either undecided about the correct direction or dealing with the complications of deploying in a world with multiple standards. A recent Forrester report indicated that "implementations are proving difficult and impractical" (Seltzer, 2007).

1.5 Organization of Material

The topic of this paper, policy-based network access control, is very complex and involves numerous aspects of network architecture. A building block approach to the topic is adopted so that each chapter lays a foundation for the discussion in succeeding chapters.

Chapter Four begins with a brief discussion of the important components used by NAC. This includes network policy, security protocols, and some key requirements of network infrastructure.

Chapter Five adds information about how network access can be controlled. This includes discussions about endpoint agents, Dynamic Host Control Protocol (DHCP), out-of-band security devices, in-band security devices, cryptographic overlays, and network infrastructure devices.

Chapter Six uses the information in Chapters Four and Five as a basis for the discussion for NAC frameworks and appliances.

With an understanding of the technologies involved and the complexities of NAC, Chapter Seven discusses the concerns with the current NAC solutions. This discussion begins with the level of control and ownership that an organization has over their network, followed by a discussion of agent-based endpoint control, network architectural considers, complexities associated with NAC follows, and concludes with a discussion on interoperability deficiencies.

In the final chapter, an analysis of the material and conclusions about the thesis are presented.

2 Terms

Term	Definition
preadmission assessment	An endpoint device is evaluated before admittance to the network is allowed. If the assessment is within the network policy, full control is normally allowed. If the device is not compliant with network policy, restricted access or forced remediation is normally the result.
postadmission assessment	Continuous assessment of endpoint devices after access to the trusted network. If the device fails to meet policy, a log of this event can be made or the endpoint's access can be revoked until the issue is corrected.
AAA	**Authentication, Authorization, and Accounting**. **Authentication** confirms that the user requesting access to network resources is a valid user. **Authorization** determines if the valid user making the request to use network resources or services has the rights to use those resources or services. **Accounting** tracks the consumption of resources by users.
Authentication or Log-in screen	A user-interface control that solicits and captures a user's credentials required for network authentication.
Authenticator	The authenticator acts as a gatekeeper that stands between the supplicant and authentication server and will only allow the supplicant to access the network once the supplicant has been successfully authenticated.
Authentication server	Provides an authentication service that performs for the actual authentication of the supplicant, user, or endpoint device.
CHAP	Challenge Handshake Authentication Protocol.
Cryptographic overlays	Appliances or endpoints use cryptographic mechanisms to limit access to network resources.
DHCP	**Dynamic Host Configuration Protocol.** A component of the TCP/IP protocol that assigns IP address.
DHCP enforcement	Enforces network policy at the time that an endpoint requests an IP address.
EAP	**Extensible Authentication Protocol**. A framework that facilitates the instantiation of security protocols within (on top of) the IPsec framework. Provides for additional authentication.
Endpoint agents	Software agents on the endpoint enforce connection policy.
Extranet	A network that allows access to trusted external users.
In-band security device	A device placed in the path of network traffic where it can monitor and make policy decisions to block network traffic.
Internet	A worldwide, publically accessible interconnection of business, academic, and government networks.
intranet	A trusted network that has the characteristics of the Internet but only allows access to trusted inside users.
LAN	**Local Area Network**. A computer network that covers a relatively small geographical area such as a home, office, or group of buildings.
Network infrastructure enforcement	Access policy decisions are enforced by network devices, such as an 802.1x Ethernet switch.
Network policy	Establishes the criteria for allowing an endpoint to access the network and typically contains (1) a set of usage rules, (2) an authorized user's specific set of parameters, or (3) network access criteria.
Network switch	Connects network segments by communicating a network packet a

	network device on one network segment to a network device on another network segment.
Network Switch Port	A network interface on a switch that provides for a single point of connection to the network.
Network packet	A block of data that is communicated over a computer network and consists of protocol control information (PCI), which contains source and destination addresses, checksums, and sequencing information. The packet also contains the user data that is often referred to as payload.
Out-of-band device	A device that monitors network traffic from outside the normal network traffic stream or responds to alert messages from network switches or other network infrastructure components.
PAP	**Password Authentication Protocol.** A simple protocol used to authenticate to a network access server.
PPP	**Point to Point Protocol**. Encapsulates TCP/IP and other traffic so that it can be transmitted over telephone lines.
Port-based authentication	An IEEE 802.1x mechanism that configures a network switch to allow access only to authorized users connecting through the port on the switch, and to deny access to all other users.
RADIUS	**Remote Authentication Dial-In Service**. Provides for centralized authentication and access control in a client / server environment.
Supplicant	The user or endpoint requesting authentication.
VLAN	**Virtual Local Area Network**. Segmentation of a physical network into one or more logical networks.
VPN	**Virtual Private Network.** A secure, private connection through a public unsecure network, which is typically the Internet.
WAN	**Wide Area Network**. A computer network that covers a wide geographical area.
WLAN	**Wireless Local Area Network**. A computer network that covers a relatively small geographical area such as a home, office, or group of buildings and links computers without the use of wires.

3 Research Methodology

This professional project used several research methods during its development. These methods can be broadly categorized into (1) search strategy, (2) evaluation, and (3) managing information (Hacker, 2003).

The search strategy used a systematic plan for locating sources. The search strategy consisted of searching the databases for academic and refereed journal articles. Examples of these databases are ACM Digital Library, ACM Portal, Computer Database, Computing Reviews, InfoTrac OneFile, and Wiley Interscience.

Additionally, consulting firms, such as the Barton Group, which specializes in information security and produces numerous research papers on the topic, was utilized.

Since this professional project topic is specific to three primary architectures of Network Access Control (NAC) frameworks and products, information posted on the Cisco, Juniper, and Microsoft web sites was also used. Information from the Trusted Computing Group's web site that relates to the Trusted Network Connection (TNC) framework and the Network Endpoint Assessment Group of the Internet Engineering Task Force was used in preparing this professional project.

Industry web sites, such as CIO, ComputerWorld, InfoWorld, and NetworkWorld were used to research the current trends and developments in NAC.

Book sources were used, and accessed primarily through Books24x7 and Regis Library Online.

In limited cases, online discussion, blogs, or other collaborative areas that contain expert information were used.

Government web sites such as NSA or other security-oriented organizations were referenced.

Lastly, Google and other search engines were extensively used to search the web for source material. Material found through this method was closely evaluated for impartiality and validity.

Source material must be relevant, scholarly, and current (the field is emerging and the latest information was used). Relevant material in many cases contained NAC, NAP, or TNC in the title or abstract. Scholarly material was from a recognized journal or educational site (recognized college / university) and the article was well-written and documented with footnotes and a bibliography (Hacker, 2003).

As information was evaluated, it was reviewed as to how well it applies to the thesis question, whether it was a primary or secondary source, if there was any bias in the article or source, and a careful assessment of the author's arguments was made (Hacker, 2003).

Since network access control is emerging technology, there is a great deal of information on the web, and this information covers the full spectrum, from very good to very bad. It was important to understand any agenda that the site had in promoting their viewpoint. For example, CISCO's web site is concerned with selling their network admission control approach to NAC. Their literature is biased toward their solutions. This isl not be a reason to dismiss this site as a source, only to weigh the information against any bias in the information. So Web sources were evaluated for authorship, sponsorship, purpose and audience, and currency (Hacker, 2003).

A great deal of information was collected, and a careful and accurate record as to the source of the information was maintained. It was important to maintain a bibliography, track source materials, and record information about the content of the source without plagiarizing. This professional project will use the APA format for its bibliography (Hacker, 2003).

Source materials were printed or photocopied and categorized in a three-ring binder. There are several benefits to this approach, but the main one is that the original material is always available to ensure that information has not been inadvertently plagiarized. Material from the Web was downloaded and stored locally.

The final stage of managing information was to record notes about the article. Recording notes can summarize information, paraphrase the information, or quote the information. Summarizing reduces the totality of an article or book chapter to a short paragraph or single sentence. While summarizing reduces the information to the key or important points, paraphrasing rewrites the information in different words. Key phrases that are used without change are quoted. In any event, information used directly from a source is quoted (Hacker, 2003).

4 Components of NAC

The current NAC implementations can use a broad array of technologies, which themselves rely on other basic and complex technologies. In this section some of these technologies are introduced.

The discussion begins with a brief overview of network policy as it relates to access control. The discussion continues with an overview of a few of the important security protocols used between network devices. As part of this discussion, an overview of encryption is introduced that explains the difference between public and private key encryption. The chapter concludes with a discussion about some key infrastructure components used by NAC.

4.1 Network Access Policy

Network Policy Enforcement establishes the criteria for allowing an endpoint to access the network. A policy can be (1) a set of usage rules, (2) an authorized user's specific set of parameters, or (3) network access criteria (Thayer, 2005).

The policy will be enforced using technology that can block access at the network entry point, or force access to a restricted network or remediation server until the endpoint meets the policy's minimum requirements.

The Network Policy Enforcement Point is as its name indicates: the place where the policy is enforced. This can be an in-band network device which may block all access or force an endpoint to a remediation infrastructure. It can also use 802.1x-aware switches, or access points, and 802.1x aware client systems to control the VLAN that an endpoint is assigned to. Lastly, it can use a web browser to redirect all endpoint traffic to a specific web portal until the endpoint is compliant (Thayer, 2005).

The Policy Enforcement Point will typically require a policy infrastructure that supports back-end authentication, a security event management mechanism, and a centralized policy store to control policy distribution. These can be a LDAP server, Active Directory, or policy data embedded in RADIUS data (Thayer, 2005).

4.2 Secure Communications

NAC solutions can make use of several different network communication protocols to facilitate the movement of information between devices. This is a huge subject that currently fills countless volumes so this section will focus on a limited number of areas that are used in many NAC implementations.

4.2.1 OSI Reference Model

Before beginning the actual discussion of the network protocols used, it is important to discuss what is meant by a network protocol. For this paper's purpose, a network protocol can be defined as a "standard set of rules that determines how systems will communicate across networks" (Harris, pg. 417).

In order to allow interoperability between various devices that communicate over the network, the International Standards Organization (ISO), a worldwide federation, established in the 1980s, defined an abstract framework. This is known as the Open Systems Interconnection Model, or more commonly referred to as OSI, and is described in ISO Standard 7498.



Each of the boxes in the graphic on the left represents a logical layer which has its own protocol where each one of these protocols has very specific responsibilities. Each layer can communicate with the layers above and below it, as well as the same layer in another device. As a message moves down the stack, control information is added to the contents from above. As a received packet or message moves up the stack, this control information is removed,

If there were two devices, device A and device B, the Application layer of device A would communicate to the Application layer of device B. The same is true for each of the other layers in the graphic.

Figure 4-1 - OSI Reference Model

Because computers and other devices that communicate over a network do so primarily through an electrical connection, a physical connection does not exist between say, application layer to application layer for two devices that are communicating. Instead, the connection exists at the physical layer and the layers above are encapsulated within a data package that is sent between two devices.

In a typical scenario, two devices want to communicate. The Application layer of device A constructs a message and passes it to the Presentation layer. It adds some information and passes it down to the next layer and

it adds some information. This continues until it reaches the Physical layer. The total data package is sent on the wire or by radio waves to device B. The package is received by the Physical layer on device B. This layer strips off the information added by device A's Physical layer and passes it up to the Data Link layer. It in turn takes off device A Data Link layer information and passes the package to the next higher layer. This repeats until it reaches the device B Application layer where what is received is the message from device A's Application layer.

While the OSI model is an abstract construct, one concrete protocol construct that will be referenced several times in this paper is the TCP/IP protocol stack.

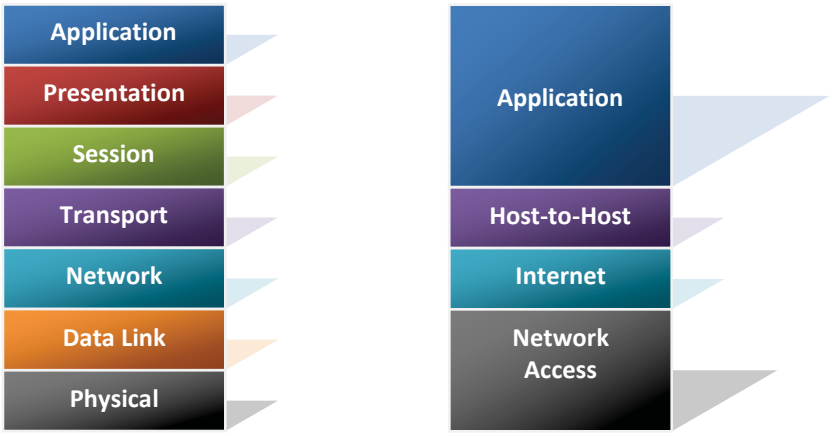


Figure 4-2 - OSI and TCP networking models

As can be seen from the comparison in Figure 4-2, the TCP/IP protocol stack does not contain all eight layers of the OSI model. The Application layer in TCP/IP performs the role of the Application, Presentation, and Session layers in the OSI model. Similarly the other layers of the OSI stack map to the layers shown in the TCP/IP model.

It is beyond the scope of this paper to provide a detail explanation of each layer, but the model should provide a helpful reference during the discussion of the protocols in this chapter.

Before examining the first protocol, however, it is important to discuss encryption.

4.2.2 Encryption

Encryption is a method of converting readable information, termed plaintext, into a form where the contents are no longer recognizable and may even appear to be random or scrambled. The words in a newspaper

story are plaintext, but if numbers were substituted for each letter of the alphabet, such that a '1' represented an 'A', and other numbers represented the remaining letters, then the newspaper story would no longer be readable and the jumble of numbers in the story would be termed ciphertext. So the essence of encryption is the process of converting plaintext into ciphertext.

When this technique is applied to a message from one person to another, then only the intended recipient can read the letter as long as the sender had previously communicated the method used to change the text. The method used to jumble the letters is referred to as an algorithm, which specifies the rules that instructs how to create the ciphertext and also how to retrieve the plaintext from the ciphertext.

While a clever algorithm may work in simple circumstances to hide a message, another element is needed in modern encryption systems to protect the contents of message from a determined effort to read the message, and this is called an *encryption key*.

It is helpful to draw a comparison between an algorithm, which is normally known by a large number of people, to that of a mechanical lock that is mass-produced and also used by a large number of people. The one aspect that makes the lock usable by so many is the fact that a different key is used to open each different lock. The same principal applies to encryption. A unique key is created that works with the algorithm to create an encrypted message. A key that someone else has will not reveal the contents of the encrypted message. Each key is different and a message encrypted by one key will not 'unlock' a message created by a different key.

4.2.2.1 Encryption Keys

There are two different types of encryption keys used in NAC implementations. To continue with the lock analogy, if for any given lock there was a single key that could lock and unlock it, that key could be thought of as *symmetric*, that is, the same key works for both locking and unlocking operations. If on the other hand, a special lock existed where it took one key to lock the lock, and a different one to unlock the lock, then these keys could be considered *asymmetric* because they would only perform one part of total functions required.

In the discussion about algorithms, only one type of key was considered, and this was a key that was used to encrypt and to decrypt a message. This type of algorithm would be considered a *symmetric algorithm* that uses a symmetric key. Figure 4-3 illustrates this concept.

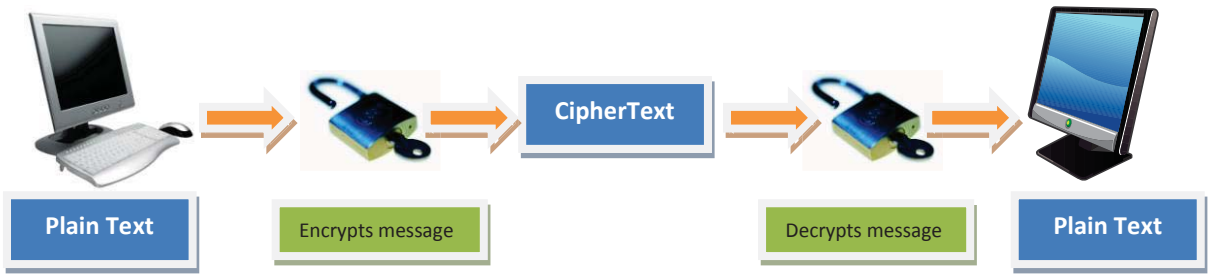


Figure 4-3 - Symmetric encryption

A second type of algorithm also exists. This is one where two keys are needed to perform the encryption and decryption. This algorithm is called an *asymmetric algorithm* and uses asymmetric keys, called public and private keys. In the first use case for asymmetric encryption, the public key encrypts a message and the receiver uses the private key to decrypt it. This provides message confidentiality. Figure 4-4 illustrates asymmetric encryption.

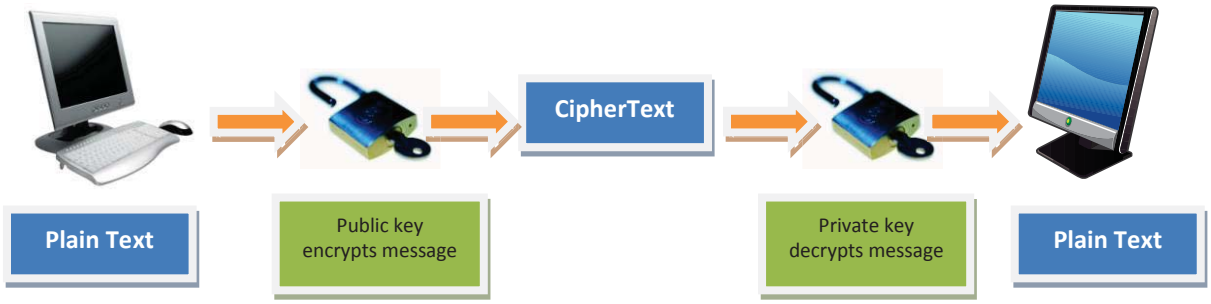


Figure 4-4 - Asymmetric encryption

In the second case, the private key encrypts the message and the receiver uses the sender's public key to decrypt it. In this case authenticity of the sender and nonrepudiation is the primary benefit. If it can be decrypted, then we can be assured that the message came from the sender. Of course this assumes that the sender is the only one with knowledge of the private key.

Each of these algorithms have strengths and weaknesses which make them ideal for different tasks as will be seen in the remainder of this paper. Symmetric encryption is faster and more secure than asymmetric encryption so it is typically used for large jobs like encrypting large amounts of text or data. On the other hand,

asymmetric encryption is better for distributing keys and provides for authentication and nonrepudiation (Harris, pg. 612).

The strengths of these two encryption methods can be linked to provide a secure key distribution system. Because symmetric encryption is much faster in processing large amounts of information than the asymmetric encryption, it should be used for encrypting the main traffic in any secure session. The problem is that the symmetric key must be present on both ends for this to work. To address this problem, asymmetric encryption is used to encrypt a symmetric key so that it can safely be transmitted to another site. Thus the strengths of both have been used to create a secure key distribution system. This will be discussed further.

4.2.2.2 Digital Signatures

A digital signature ensures that the contents of a message have not been modified since the signature was created. A digital signature employs a cryptographic hash function to create a unique value that represents the contents of the message.

For example, if I wanted to communicate the message, "The day is beautiful," but I also wanted the receiver of this message to be able to determine if the message had been changed, I could create a numerical value that the receiver could use to ensure that the message had not been changed to "The day is rainy." This numerical value used is referred to as a *hash value*.

A hash value creates a fixed-length value from a variable number of characters. It uses a special type of algorithm known as a one-way function. An interesting fact about a one-way function is that it relatively easy to compute in one direction, but almost impossible to do so in the opposite direction. The hash value is can also be referred to as a message digest.

When someone receives a message with an associated message digest, the receiver can compute a new message digest for the message and compare it to the received message digest. If these values are the same, then the receiver has some assurance that the message has not been changed. The exception to this is if a malicious party intercepted the message, changed it, and computed a new message digest on the changed message.

To prevent the changing of the message and the associated message digest, the message digest is encrypted with the sender's private key (the secret part of the asymmetric key pair) discussed in the previous

section. The encrypted message digest becomes a digital signature. Figure 4-5 describes the process for creating a digital signature.

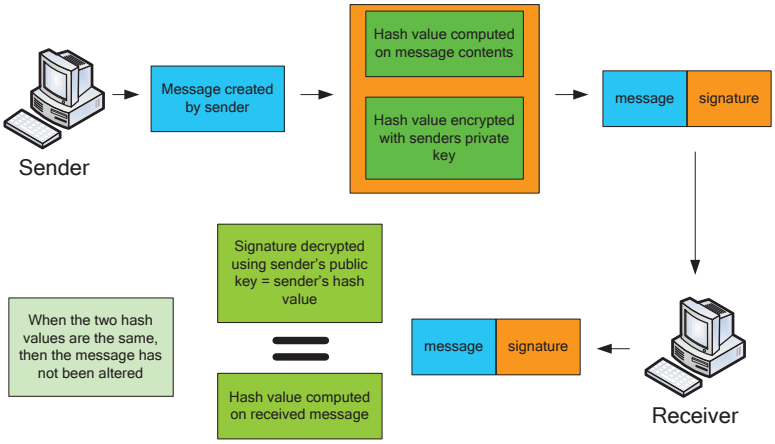


Figure 4-5 - Creating a digital signature

When the message and digital signature are received by a recipient, a new hash value (message digest) is computed for the received message. The sender's public key is used to decrypt the received digital signature. The decrypted hash value is compared to the computed hash value, and if they match, the sender knows that the message has not been altered and that it is from the expected sender.

A digital signature provides sender authentication, integrity checking, and prevents the sender from repudiating the message because the hash value was encrypted using the sender's private key. Signatures will be used in a future discussion about digital certificates.

4.2.2.3 Public Key Infrastructure

Public Key Infrastructure (PKI) is "the set of security services that enables the use of public key cryptography and X.509 certificates in a distributed computing system" (Diodati, p. 7). The current specification for PKI is published in Internet Certificate and CRL Profile RFC3280.

The impetus for public key cryptography was the ability to enable secure communication between parties in an open environment using an encryption key that can be conveyed over non-secure communications (Barr, 2004).

The parts of PKI can roughly be divided into the following areas: endpoints, Certification Authority, Registration Authority, Repository, and Certificate Revocation List (CRL) Issuer (Barr, 2004).

Endpoints can be anything that is the subject in a public key certificate. This can be an actual end-user, a device such as a router or server, or a software process (application). An endpoint can be either a consumer of PKI services or a provider.

For an endpoint to participate in PKI, it must have a digital certificate. The X.509 standard defines how a certificate is created. The certificate is issued by a trusted third party that is referred to as a Certificate Authority (CA). The certificate is a digital document that validates the sender's authorization and name, and contains the certificate holder's name, public key, and the Certification Authority's digital signature, which is used to authenticate the certificate. A certificate is only meaningful to another entity when the issuer of the certificate can be trusted.

To understand the basic workings of PKI, it can be helpful to relate the activities to a real world example like the passport system. When a person wants to acquire a passport, they must provide documentation that validates they are who they purport to be. If the proof is accepted by the registering authority (passport office) then their information is added to a list of valid passports (repository). Eventually a passport is created and given to the requestor by a different part of the passport service that certifies that the person described in the passport has proven their identity. In time, the passport may expire or the person may commit a crime that requires that their passport is invalidated. When this occurs, information is entered in the passport repository about the revoked status of the passport. The passport service can then create a list of invalid or revoked passports by looking in the repository. This list could be referred to as the passport revocation list and made available to organizations that use the passport as an assurance of identity, such as the custom service. PKI provides similar services with slightly different names.

When an endpoint requires a digital certificate, valid documentation is provided to a Certificate Registration Authority that proves the identity of the endpoint. This information is recorded in a repository, and a Certification Authority issues a digital certificate with the certificate holder's name and public key, along with the endpoint’s digital signature. Figure 4-6 illustrates this process.

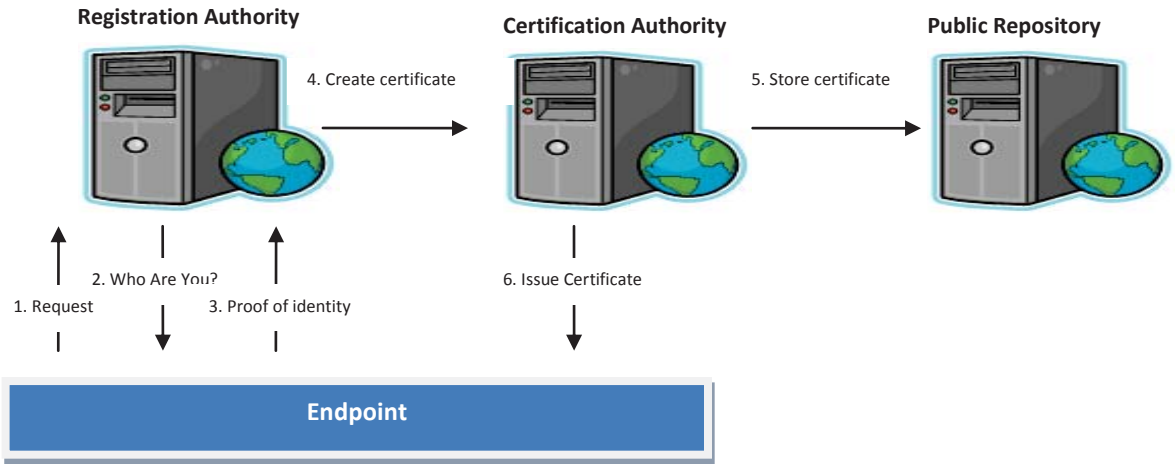


Figure 4-6 - Registration

When this certificate is presented to a PKI service, if it trusts the Certification Authority that issued the certificate, then the certificate is accepted as proof of the presenter's identity. Referring back to the passport scenario, this is analogous to a traveler presenting passport at the border of a country. If the country's custom service trusts the issuer of the passport, then the traveler is granted admittance.

Once a certificate is issued, it is critical that a record be maintained about the contents of the certificate. This is normally the role of a repository, which is a method for storing and retrieving PKI-related information, such as public key certificates and Certificate Revocation Lists (CRL). Practically, this can be something as low tech as a flat file or as robust as an implementation of a X.500-based directory with client access via the Lightweight Directory Access Protocol (LDAP).

Also important is the ability to revoke a certificate when it is no longer valid. In PKI this is accomplished through the use of the CRL. In most implementations, the CA is responsible for maintaining and providing a list of certificates that are no longer valid, but this can be optionally assigned to another service called Online Certificate Status Protocol (OCSP) that can check a CAs CRL during the certificate validation process. This of course would be equivalent to the customs service checking its repository to ensure that a presented passport is valid.

It will be illustrative at this point to discuss the major steps that take place during a PKI session, but before that happens a new term – session key – needs some explanation.

A simple definition for session key is a symmetric key that two endpoints use to encrypt messages. From our previous discuss of symmetric encryption you'll recall that the same key is used to encrypt and decrypt messages. One of the unique properties of a session key is that it is only used during a single session, and after that it is discarded. This provides for more secure exchange because the key will only exist for a relatively short time.

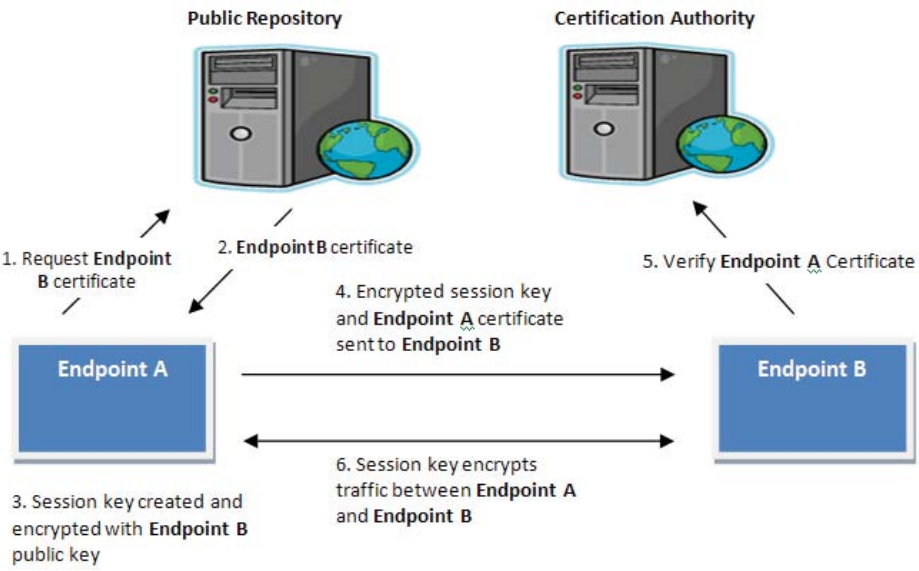


Figure 4-7 - PKI Session

Referring to the example in Figure 4-7 - PKI Session, there are two participants: Endpoint A and Endpoint B. Recall that an endpoint can be an end-user, a device, or a software process.

1. A session begins when Endpoint A requests Endpoint B's digital certificate from the PKI repository.
2. The Public Repository where certificates are stored returns Endpoint B's certificate, which also includes Endpoint B's public key.
3. Endpoint A creates a symmetric or session key that can only be used during the communication's session with Endpoint B. The session key is then encrypted with Endpoint B's public key.
4. The encrypted session key plus Endpoint A's digital certificate is sent to Endpoint B.
5. Using the information from Endpoint A's certificate, Endpoint B requests that the issuing CA verify that Endpoint A is who it says it is.

6. Once this is done, Endpoint A and Endpoint B have established a session, and the session key will be used to encrypt all traffic between them. Once the session is completed, the session key is discarded and the session infrastructure is disassembled. If these two endpoints need to communicate again, a new session will be created.

This represents one type of key exchange or key establishment. The other key establishment occurs when both parties contribute to the key generation. This is known as key agreement.

4.2.2.3.1 Benefits and Challenges

In the discussion thus far, several PKI benefits have been revealed. These include the ability to enable confidentiality of information, ensure data integrity, authenticate the parties in the exchange of information, and non-repudiation (remove the ability of one party to deny that an exchange took place).

From the description of so many moving parts, the careful reader has probably also determined that there may be some barriers to PKI deployment. These barriers are total cost of ownership (TCO), lack of maturity, complexity and uncertainty, repository issues, lack of industry standards, multi-vendor interoperability, and scalability and performance (Barr, 2004).

The TCO of PKI can be very significant because of the number of hardware components involved in a typical installation, the cost of software and support tools, the leveragability of the existing corporate IT infrastructure, the cost associated with planning, deployment, operation, and maintenance of infrastructure, the costs of defining policies and procedures needed with a PKI deployment, any additional facilities that are needed to support PKI, the training costs for PKI development, deployment and maintenance, the cost of administrative support, the problems or lack of interoperability with other vendor PKIs, and liability protection. While this list is not exhaustive, it does illustrate the many areas that must be considered when estimating the cost of PKI (2004).

There is not a consensus in the industry as to the maturity of PKI. Some believe that PKI is an emerging technology with all the problems that that entails, but others maintain that PKI is a must-have technology (2004).

Complexity and uncertainty should also be a concern for organizations considering PKI deployment. Many believe that PKI is too complicated and expensive to be viable. Because of this uncertainty, experts generally

recommend that small PKI pilots should be deployed first to address a small community or single application (2004).

Distribution and revocation of certificates, as well as other PKI-related information, from online repositories can also be problematic (2004).

The lack of industry standards for directory services that offer PKI services has also been a concern.

Lastly, because few large-scale PKI deployments have been completed, scalability and performance issues associated with repository services are unknown (2004).

This section has presented a brief description of Public Key Infrastructure and its major component parts. This was not meant to be an exhaustive treatment of the subject, but to only introduce the concept and complexities of PKI. As will become evident, PKI can be but one part of the complexity of a NAC solution.

4.2.3 Secure Sockets Layer (SSL)

Netscape Corporation developed Secure Sockets Layer (SSL) to facilitate the secure transmission of documents over the Internet. Today most browsers support SSL. Data encryption, integrity checking, server authentication, and optionally, client authentication, are supported by SSL.

SSL is composed of two protocols, where one works at the lower part of the OSI session layer, and the other works at the top of the OSI transport layer. The first protocol is SSL Record Protocol and the second is standard HTTP. Basic security and communication services are provided by SSL Record Protocol to the top layers of the SSL protocol stack. Standard Internet communication services are provided to the server and client by HTTP (Whitman and Mattord, pg. 376; Harris, pg. 667).

A SSL session is primarily divided into two parts. The first involves a handshaking exchange to setup the session and establish the security parameters that will be used. In the second part, data is securely exchanged using the environment established during handshaking. During a typical SSL session the following exchange will take place.

Handshaking:

1. Client attempts to access a secure web page on a site

2. Server offers SSL session
3. Client sends security parameters
4. Server compares received parameters against its own until a match is found
5. Server sends its digital certificate to client
6. Client evaluates certificate and decides to trust server
7. Optionally: Server requests client certificate

SSL session established:

8. Client generates a session key and encrypts it with server public key (**note**: only the server private key can descript the session key)
9. Encrypted key sent to server
10. Session Key used to encrypt data during session

In the typical session, only the server is authenticated. This normally occurs with Internet shopping today. When an SSL session is in effect, the user can confirm this by observing that the URL contains "HTTPS" and a padlock or key icon appears at the bottom corner of the browser. When the server does request the client certificate, this is referred to as client-side authentication (Hook, 2005; Harris, pg. 667).

4.2.3.1 Transport Layer Security (TLS)

Transport Layer Security (TLS) provides privacy, integrity, and proof of authenticity. Privacy is provided because the information between the client and server is encrypted within the session. Integrity is provided because any change to the content between client and server is immediately known. Proof of authenticity is provided when the client and server exchange certificates that can be verified with a trusted third-party certificate authority which can validate the authenticity of the endpoints involved (Hildebrandt and Koetter, 2005; Ciampa, pp. 210-211).

TLS version 1.0 was essentially the same as SSL version 3.0. While TLS 1.0 is derived from SSL 3.0, these two protocols don't interoperate easily. However, TLS 1.0 does contain the ability to regress to SSL 3.0 functionality (Oppliger, 2003).

Like the SSL protocol, TLS contains multiple protocols, but for the purposes of this discussion, these can be reduced to two primary areas. TLS Handshake Protocol is used to perform authentication between a server and a client, establish the encryption algorithm that will be used, and exchange the cryptographic key that will be used during the session (Oppliger, 2003; Johnston and Piscitello, 2006; Ciampa, pp. 210-211).

The TLS Record Protocol fragments messages into TLS records, computes a message authentication code (MAC) and appends this to the record, encrypts the combined result, and then transmits it (Oppliger, 2003; Johnston and Piscitello, 2006; Ciampa, pp. 210-211). MAC combines a cryptographic hash function and a symmetric key to produce a value that can be used to verify message integrity and authenticity (Oppliger, 2003). Figure 4-8 illustrates a typical TLS session.

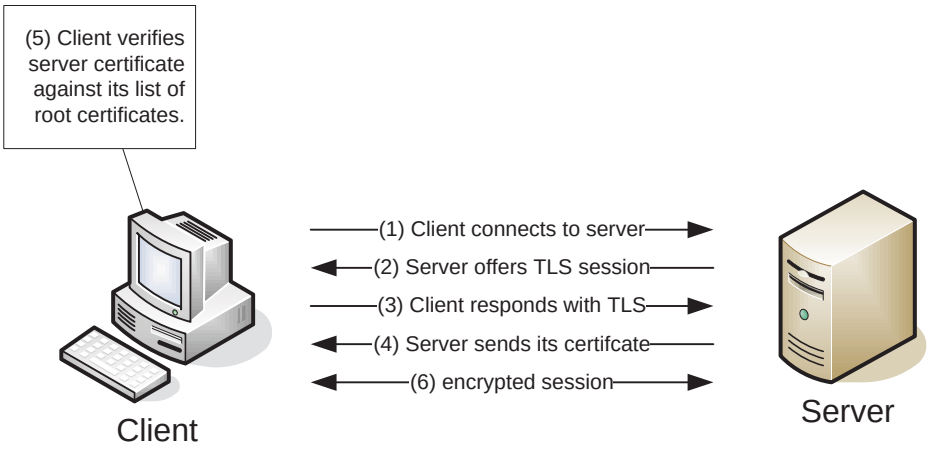


Figure 4-8 - TLS Session

A PKI is needed when either SSL or TLS is enabled in a web server environment. This requires that the client and server devices have certificate configuration (Schurman, Thomas, and Christian, 2006).

4.2.4 Tunneling Protocols

There is a class of protocols that are used to communicate other protocols over mediums where these protocols normally can't be used. This is accomplished by creating a virtual network path where protocol information or packets from one protocol are encapsulated within that of another protocol. Sometimes these encapsulated protocols are also encrypted. This is referred to as tunneling (Harris, p. 540).

For example, if network 1 wanted to communicate with network 2, but these two networks were not connected by a LAN, and the protocol on the network 1 only knew how to communicate over a LAN, then one way for the two networks to communicate would be over a telephone connection. But since the network protocols do not know how to communicate over a telephone line, another protocol could be used to wrap or encapsulate the network protocol as it travelled over the telephone network between the two networks.

In a sense it is like a letter sent through the postal service. The post office would not be able to deliver the contents of the letter without an envelope. The envelope protects the letter inside and also provides information that the postal service needs to move the letter from the sender to the receiver. The letter has been encapsulated by the envelope to allow this transference. When the receiver receives the envelope, the letter inside is removed and read by the receiver. This is also what happens when a message from the network 1 is transferred over the telephone network to network 2.

Four different tunneling protocols are discussed.

4.2.4.1 Point-to-Point Protocol

Point-to-Point Protocol (PPP) encapsulates TCP/IP and other traffic so that it can be transmitted over telephone lines. PPP is used when accessing the Internet through a dial-up connection that is hosted by an Internet Service Provider (ISP). PPP and ISP are important for corporate network access because an employee can dial into a local ISP instead of a possible long distance charge into the corporate facility. PPP will be used to facilitate three tunneling protocols: PPTP, L2TP, and IPsec (Harris, pp. 541-542).

4.2.4.2 Point to Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) was developed by Microsoft Corporation to allow a remote user to use the Internet securely by establishing a PPP connection to an ISP and then to create a secure virtual private network (VPN) or tunnel over the Internet to a destination. To secure the transmission of data, the PPP payload is encrypted by a key that is established during the authentication process. The user data is encapsulated within the PPP payload. PPTP allows the PPP data to be communicated over the Internet where PPP is not supported (Harris, pg. 543).

4.2.4.3 Layer 2 Tunneling Protocol

One limitation of PPTP is that it can only work over IP networks, but many other types of networks are used to move data. These include frame relay, X.25, and ATM links. To address this issue Cisco Corporation developed Layer 2 Tunneling Protocol (L2TP) which combines some of the best features of PPTP. L2TP encapsulates the PPP payload but does not provide for encryption of the payload. If this is required, then L2TP needs to be combined with IPsec, the next topic discussed (Harris, p. 544).

4.2.4.4 Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) is an open source protocol within the TCP/IP family of protocols used for secure communicates across an IP-based LAN, WAN, and Internet networks between two devices (two servers, two routers, client / server or possibly two gateways). IPsec is a creation of the IETF's IP Protocol Security Working Group and is normally used to establish virtual private networks (VPN) across the Internet between networks (Harris, p. 672; Whitman and Mattord, pg. 378).

Although IPsec has protocol in its name, it is normally considered more of a framework rather than a protocol. It defines the type of algorithms, keys, authentication requirements that must be used. Authentication Header (AH) and Encapsulating Security Payload (ESP) are the two protocols that IPsec uses. While ESP provides cryptographic means to provide source authentication, confidentiality, and message integrity, AH is only an authenticating protocol. A company will use AH when the source of the sender is required and when the integrity of the message information needs to be assured. ESP is used to gain the advantage of AH plus confidentiality, which is attained through encryption of the message information. For this reason, ESP is almost always used when setting up a VPN (Harris, p. 672; Whitman and Mattord, pg. 379).

The reader may wonder why AH would ever be used since ESP offers the same authentication and integrity services as AH. The use of one over the other is particular to the type of environment in which IPsec is used. Specifically, if the IPsec packet passes through Network Address Translation (NAT) device, then ESP must be used because NAT will modify the packet header when it changes the IP address of the packet. Because the packet contains an integrity check value (ICV), which computes a unique value depending of the contents of the IPsec packet, the changed ICV will cause the packet to be discarded by the receiver (Harris, 672, 674).

In addition to these two protocols, IPsec has two modes it can operate in. Transport mode protects the payload of a message and will be used when the network packet must pass through a NAT device, which allows the source and destination IP addresses to be visible (not encrypted). In transport mode intermediate nodes can read the IP headers but the actual IP data is encrypted (Whitman and Mattord, pp. 378-380; Ciampa, pp. 238-239; Harris, pp. 672-674).

In tunnel mode the message payload, header, and trailer information are protected. Tunnel mode is used when the source and destination IP addresses do not need to be visible, such as between gateways. In tunnel mode systems, the beginning and ending of a tunnel act as proxies to send and receive the fully encrypted packets which have been encapsulated in a new packet. The proxies will decrypt the packet and send it on to the destination in the original packet (Whitman and Mattord, pp. 378-380; Ciampa, pp. 238-239; Harris, pp. 672-674).

In order to manage the device configuration information during an IPsec connection, a security association (SA) is created for both the incoming connection and outgoing connection the device is using. Information contained in an SA will include the (1) lifetime of the SA, (2) mode (tunneling or transport), (3) ESP encryption algorithm and key, (4) ESP authentication algorithm and key, and other parameters needed to manage the connection between devices. The SA is referenced when an IPsec packet is received during a connection and the SA will define how the packet should be decrypted or authenticated (Harris, pp. 673-674).

To organize the various SAs during multiple communication sessions, the security parameter index (SPI) is used. Each IPsec packet contains a SPI value in its header information. This index is used to reference a security policy database where all the incoming and outgoing SAs are stored. The encrypted IPsec packet is decrypted and authenticated based on the parameters in the associated SA (p. 673).

The last aspect of IPsec discussed in this section is the management of keys. This can be accomplished manually or automated through a key management protocol. IPsec uses Internet Key Exchange (IKE) as its standard for key management. IKE uses an asymmetric-based key exchange and also negotiates security associations. IKE is a combination of two other protocols: Internet Security Association and Key Management Protocol (ISAKMP) and OAKLEY. ISAKMP defines a framework of exactly what can be negotiated during the establishment of an IPsec connection. This negotiation will include type of algorithm used, protocols used, modes, and keys. The OAKLEY

protocol actually performs the negotiation. These protocols operate at the network layer of the OSI reference model (Harris, pg. 674; Whitman and Mattord, p. 379).

The cryptosystems that IPsec uses in its operations are (Whitman and Mattord, p. 379):

- Diffie-Hellman key exchange: derives key material between peers on a public network
- Public key cryptography: guarantees identity of two parties through the signing of Diffie-Hellman exchanges.
- Symmetric encryption: bulk encryption algorithms like Data Encryption Standard (DES)
- Digital Certificates: signed by trusted certificate authority

4.2.4.5 Extensible Authentication Protocol (EAP)

Extensible Authentication Protocol (EAP) is a framework that facilitates the instantiation of security protocols within (on top of) the IPsec framework. By itself, EAP is made up of packet formats and a basic handshake which cannot address the authentication between two entities. However, EAP's real strength is that it can wrap authentication protocols in a common format without regard to the underlying communications medium (Hardjono and Dondeti, 2005). EAP is described in detail in the IETF 3748 document (Aboba et al., 2004).

EAP can be used on wired or wireless networks, and on switched or dedicated circuits. IEEE 802.1x describes EAP encapsulation on wired networks, and IEEE 802.11i describes EAP for wireless LANs.

EAP uses several terms to describe the primary entities involved in its operation (Aboba et al., 2004).

- The EAP peer or **supplicant** refers to the end of the link that responds to the authenticator.
- The **authenticator** represents the end of a link that initiates authentication. The authenticator specifies the authentication protocol that will be used. This term is also used in the IEEE 802.1x specification with the same meaning.
- The Authentication, Authorization, and Accounting (**AAA**) and backend authentication servers are the same entity in the EAP specification. This server provides an authentication service to an authenticator when present and executes EAP methods for the authenticator when the authenticator is operating in pass-through mode. RADIUS [IETF RFC3579] and Diameter [DIAM-EAP] typically provide the AAA protocols with EAP.

This paper will use the terms authenticator, supplicant, and AAA since these are common terms when referring to 802.1x implementations which will be discussed in a future section.

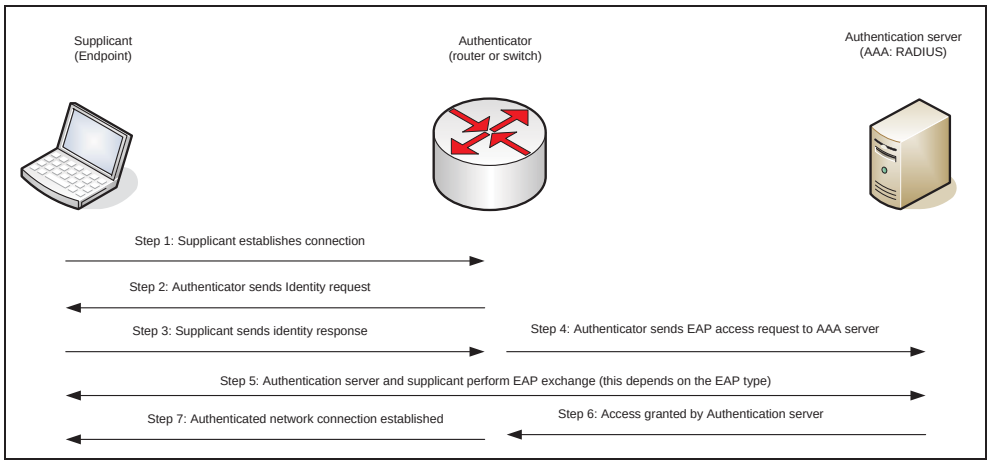


Figure 4-9 - EAP exchange (Source: Aboba et al.)

Figure 4-9 shows a typical EAP exchange. EAP exchanges occur between a supplicant, an authenticator, and an AAA (authentication) server. A typical exchange involves the exchange of request and response packets.

1. The supplicant establishes communications with the authenticator.
2. The authenticator sends a *request* to the supplicant. This may be a request for the supplicant's identity but it is not required.
3. The supplicant responds to the request packet with requested information.
4. The authenticator sends an EAP access request to the authentication server.
5. The supplicant and authentication server exchange EAP request / response (depends on the type of EAP type being used) until the authentication server can authenticate the supplicant.
6. If the authentication is successful, an EAP success response is returned to authenticator; otherwise, an EAP failure packet is returned.
7. Authenticator establishes network connection with supplicant.

Because EAP is essentially a peer-to-peer protocol, mutual authentication can also occur with simultaneous conversations (Hardjono and Dondeti, 2005; Aboba et al., 2004).

Authentication between authenticator and supplicant can be accomplished using passwords, a token card, one-time passwords, certificates, smart cards, public key authentication, or Kerberos. Additional authentication methods can also be added as needed (Harris, pp. 558-559; Chen and Wang, 2005).

The security protocols hosted by EAP for NAC can be any of the fifty-plus that are currently defined. However this paper will only describe a few that are relevant to this NAC discussion.

EAP-MD5 (Message Digest 5) is primarily based on a one-way hash. MD5 produces a 128-bit message digest from an arbitrary length message. This technique is used to convert a user's password to a hash that is stored in an authentication server. At login time, the supplicant converts the user entered password to a hash, transmits it over the network, and compares it with the stored hash value from the authentication server (Chen and Wang, 2005).

This is one of the most popular EAP types because of its ease of use. Also, because the message digest is transmitted over the network, this makes it a good choice for wired LANs because of low-risk of a man-in-the-middle and dictionary attacks, but is less attractive for wireless LANs because of an increased risk of someone capturing the message digest (Chen and Wang, 2005; Phifer, 2006).

EAP-TLS (Transport Layer Security) is based on Transport Layer Security protocol. EAP-TLS session begins with an authentication phase that establishes a session between the supplicant and authentication server. Once authenticated, the authenticator is notified and access to the network is granted to the supplicant. Certificates are used to perform a mutual authentication between supplicant and authentication server. This is both an advantage and disadvantage because it requires that clients hold digital certificates (What are your EAP Authentication Options, 2005; Harris, pp. 558-559).

Since the supplicant is able to authenticate the network, a forged Access Point (AP) could be detected in the case of a wireless network, but because both the supplicant and authentication server need valid PKI certificates, EAP-TLS can be difficult to manage (Chen and Wang, 2005; Robinson, 2006). EAP-TLS is included in Microsoft Windows XP and Server 2003 (Ciampa, p. 233). Because of the cost and complexity associated with PKI, this EAP type is generally considered the strongest available and the most costly to deploy (Phifer, 2006).

EAP-TTLS (Tunneled Transport Layer Security) was created by Funk Software (now part of Juniper Networks) and is also an IETF standard (Robinson, 2006). EAP-TTLS uses tokens and other advanced authentication methods (Ciampa, p. 233).

EAP-TTLS requires that additional information between the supplicant and authenticator be exchanged, which requires establishing a secure tunnel during TLS negotiations. In the *TLS handshake phase,* the supplicant authenticates the authentication server by using a server-side certificate. At the end of the handshake phase a secure tunnel is established (Chen and Wang, 2005).

In the *TLS tunnel phase* of the EAP-TTLS negotiations, the secure tunnel is used for client challenge / response exchanges. The authentication server will authenticate the supplicant using its username and password. Since the communication in this phase is through a secure tunnel, any non-EAP protocol can be used. These protocols typically include: PPP Authentication Protocols, PPP Challenge Handshake Authentication Protocol, Microsoft PPP CHAP Extensions, or Microsoft PPP CHAP Extensions, Version 2 (Chen and Wang, 2005). Once the authentication is complete and the session keys are delivered, the tunnel is disassembled (Phifer, 2006).

EAP-TTLS is more manageable because only the authentication server requires a certificate (Chen and Wang, 2005). EAP-TTLS is a good solution when legacy databases, such as LDAP, Active Directory, are used in a secure environment (Phifer, 2006).

PEAP (Protected EAP) was jointly developed by Microsoft and Cisco and is a draft IETF standard. It is one of the most popular methods because of its native support in the latest Microsoft operating systems (Robinson, 2006). EAP-PEAP is essentially the same as EAP-TTLS except that it can only use EAP protocols in the TLS Tunnel phase, such as EAP-Microsoft-Challenge Handshake Protocol-V2 (MS-CHAP) or EAP-Generic Token Card (Chen and Wang, 2005; Phifer, 2006). EAP-TTLS requires the same version of PEAP on the client and server (Phifer, 2006)

Enterprises that use legacy authentication methods such as username / password or token-based methods may select PEAP. Certificates and EAP-TLS are used to authenticate the server and to establish an encrypted tunnel. Once the tunnel is established, the client will use the tunnel to send username/password or token-card credentials to the server for authentication (What are your EAP Authentication Options, 2005; Robinson, 2006; Ciampa, p. 233; Harris, pp. 558-559).

Lightweight EAP (LEAP) was the first widely deployed EAP wireless authentication method. LEAP was developed by CISCO and is sometimes referred to as Cisco-EAP. A username/password is used to perform mutual authentication between server and client by using MS-CHAP version 1. A certificate is not required (Ciampa, p. 233; Harris, pp. 558-559; What are your EAP Authentication Options?, 2005; What is EAP-FAST?, 2005).

This method is vulnerable to dictionary attacks and must be installed where strong user passwords are used (What are your EAP Authentication Options, 2005; What is EAP-FAST, 2005; Phifer, 2006).

Flexible Authentication via Secure Tunneling (EAP-FAST) was created by Cisco Corporation to resolve some of the problems with LEAP (What is EAP-FAST, 2005). EAP-FAST can support tokens and establish an encrypted tunnel without a certificate from the supplicant (Ciampa, p. 233). A session will first establish a TLS tunnel by using a pre-shared Protected Authentication Credential (PAC) key. The secure tunnel is then used to carry a user authentication. A single master key on the authentication server is used to create each user PAC (What is EAP-FAST, 2005).

4.2.5 Remote Authentication Dial-in User Service (RADIUS)

The Remote Authentication Dial-in User Service (RADIUS) protocol provides for centralized authentication and access control in a client / server environment where relationships exist between the endpoint and Network Access Server (NAS) and between the NAS and RADIUS server. RADIUS was developed by Livingston Enterprises but was later published as RFC 2138 and RFC 2139 (Ciampa, pp. 234-235; Harris. pg. 173).

Corporations use RADIUS to assign pre-configured profiles for remote users that control the resources that the user can access. This provides a single administration point that standardizes security policy and tracks network usage. User credentials can be held in LDAP servers, text files or other databases (Harris, pg. 173).

Originally each NAS maintained a list of authorized user credentials (username and password), but with RADIUS infrastructure, NAS forwards access requests to a central RADIUS server for authentication. RADIUS can support Microsoft Active Directory, RSA Security SecureID, interface with NAS devices (e.g. dial-up servers), VPN concentrators, WLAN access points and firewalls (Ciampa, pp. 234-235; Harris. pg. 173; Robinson, 2004).

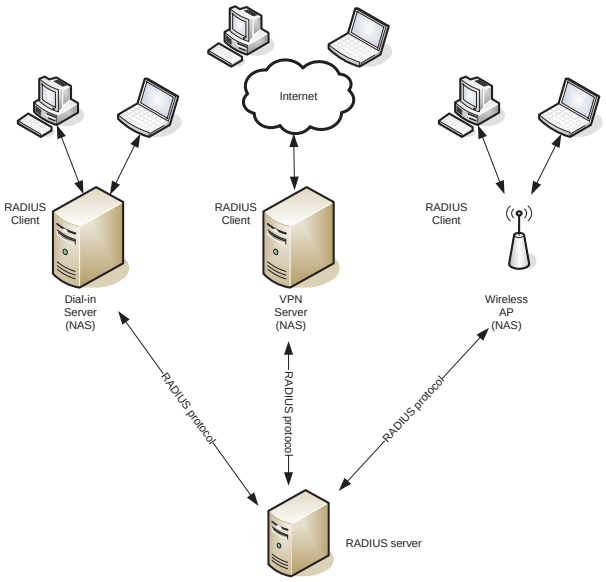


Figure 4-10 - RADIUS infrastructure (Source: Harris)

In Figure 4-10 an example RADIUS infrastructure is illustrated where the three access methods are shown: dial-in, VPN, and Wireless. The RADIUS client is installed on either the gateway servers or wireless access point. Information from the endpoints is routed through the RADIUS client to the RADIUS server, which then interacts with the network authentication server.

A typical RADIUS exchange uses the following steps:

1. Endpoint and NAS agree on authentication protocol (PAP, CHAP, or EAP).
2. Endpoint submits username and password. For dial-up, this communications occurs over PPP connection.
3. RADIUS protocol is used for communication between NAS and RADIUS servers. This combines both the authentication and authorization functionality.
4. Once the endpoint is authenticated, an IP address and connection parameters are given to endpoint.
5. Access to network is allowed.
6. NAS notifies RADIUS server at beginning and end of session and audit records are recorded (Harris, pg.173).

Access to the network in a WLAN environment is controlled by the RADIUS server and its data store or authentication backend. It can also supply Access Point (AP) and client keys, which are used to encrypt wireless traffic between the two. Communication to the RADIUS server should be restricted. The RADIUS server needs to communicate to the authentication backend (e.g. LDAP server) and to NAS, which in this case is the AP. This communication should be protected with encryption using either SSL or IPsec. SSL can easily be used between the RADIUS server and authentication backend and IPsec is available between RADIUS and APs. If IPsec cannot be used between RADIUS server and APs, then unique shared secrets must be selected for each AP (Lockhart, 2007).

4.3 Infrastructure

4.3.1 IEEE 802.1x Standard

IEEE 802.1x establishes a standard for supporting EAP over a wired or wireless LAN by packaging it in Ethernet frames. IEEE 802.1x is based on EAP and uses port-based authentication to restrict access to the network. With port-based authentication, the network switch restricts access to only authenticated users on a specific port. This prevents any access to network resources until the user has been authenticated (What is 802.1x, 2006; Ciampa, 2005; Harris, 2005). Like a glass front door, this allows someone to identify who is requesting entry before the door is opened to them.

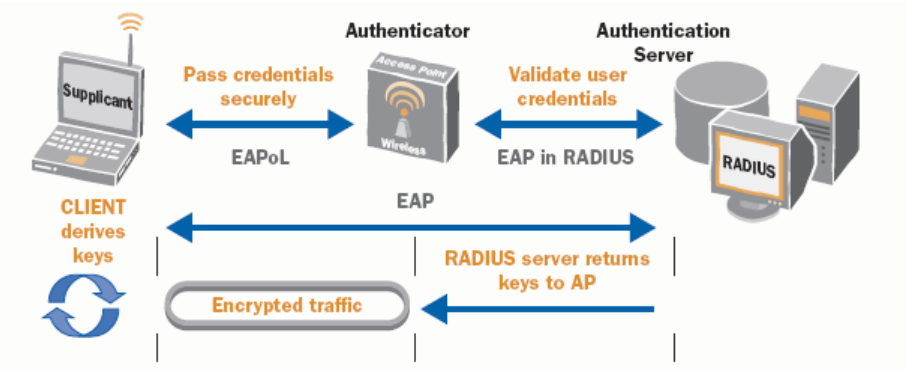


Figure 4-11 - Typical 802.1x Network Environment (Source: Juniper Networks)

Three parties are involved in wireless or wired LAN authentication: supplicant, authenticator, and authentication server. The supplicant is the user or endpoint requesting authentication. The authenticator acts as a gatekeeper that stands between the supplicant and authentication server and will only allow the supplicant to access the network once it has been successfully authenticated. The authentication server provides an

authentication service that performs the actual authentication (normally a RADIUS server). In situations where the authentication server does not exist, the authenticator can provide this functionality (Harris, 2005). EAP encapsulation over LAN (EAPOL) is the protocol used between the supplicant and authenticator, but CISCO will also encapsulate EAP over UDP in some situations. Figure 4-11 illustrates the interaction between supplicant, authenticator, and authentication server (What is 802.1x, 2006).

4.3.2 Virtual Private Network

A virtual private network (VPN) is a secure, private connection through a public unsecure network, which is typically the Internet. The connection is considered private because the confidentiality and integrity of the data is encrypted and uses a tunneling protocol. The protocols used are Point-to-Point Tunneling Protocol (PPTP), IPsec, and Level 2 Tunneling Protocol (L2TP) (Harris, pg. 539; Ciampa, pg. 240). VPN transmissions occur between endpoints, which are the ends of the VPN tunnel. Endpoints may be software on the user's computer, a VPN concentrator (aggregates multiple connections together), or a firewall (Ciampa, pg. 240).

VPNs are typically used to connect remotely (remote-access VPN) to a company network to gain access to e-mail, network resources, or corporate assets, or between two gateways, such as a branch office to the main office (site-to-site VPN), or even internal to a organization where VPN-enabled firewalls are located on the perimeter of the security domain and the incoming encrypted packets are decrypted before the firewall processes them (Harris, pg. 539; Ciampa, pg. 240).

In the remainder of this section, remote access VPNs, site-to-site VPNs and the issues associated with both will be discussed.

4.3.2.1 Remote Access VPN

The definition of remote users includes employees travelling that connect to the home office, telecommuters, employees that work from home over the Internet, and other mobile users (Disabato, 2007).

Many enterprises are collapsing their network perimeters such that all users are considered "hostile" and are required to use a secure VPN. Some organizations consider this a superior solution to the "heavy duty" network access control security where policy is enforced by 802.1x access network switches and routers with access control lists (ACL). In this context, remote can now mean an employee at his desk within the physical

confines of an enterprise accessing a server in the data center. Some of these changes have occurred because organizations fear business disruptions from natural events and pandemics that would limit mobility. In either of these cases employees could operate from just about any place with an Internet connection (Disabato, 2007).

Today, four types of VPNs exist that provide for a secure tunnel for remote access: direct clientless SSL VPN, appliance clientless SSL VPN, Layer 3 SSL VPN, and IPsec VPN (Disabato, 2007).

The **direct clientless SSL VPN** uses an application with SSL support and connects directly to a server that supports the application. Server examples include: Hypertext Transfer Protocol Secure (HTTPS), Secure Post Office Protocol (SPOP), Secure Internet Mail Access Protocol (SIMAP), and Secured File Transfer Protocol (SFTP). This VPN type operates between ISO layers 4 through 7. A common example of this type of user application is the Internet browser (Disabato, 2007).

The **appliance clientless SSL VPN** is the same as the **direct clientless SSL VPN** except instead of connecting directly to the server, the connection is made through a SSL VPN appliance (Disabato, 2007).

The **Layer 3 SSL VPN** type requires that a specialized software VPN client is installed on the user's device. The client software can also be installed automatically when the web browser, a Java applet, or ActiveX control accesses the enterprise web portal. The client software will establish a SSL connection tunnel to a VPN appliance from where multiple applications or servers can be accessed through the SSL tunnel from behind the VPN appliance. This is considered a "Layer 3" VPN because traffic can be routed through the tunnel from the user device to the VPN appliance. The user device will have two IP addresses. The "private" one is provisioned by the VPN appliance and is from the subnet behind the VPN appliance. The second is the external IP from the subnet where the device is located or from the Internet Service Provider (ISP) if the device is directly attached (Disabato, 2007).

The **IPsec VPN** requires that a specialized software VPN client installed on the user's device which establishes an IPsec connection tunnel from the user's device to the VPN appliance from where multiple applications or servers can be accessed from behind the VPN appliance. Like the **Layer 3 SSL VPN**, the user's device has both external and private IP addresses (Disabato, 2007).

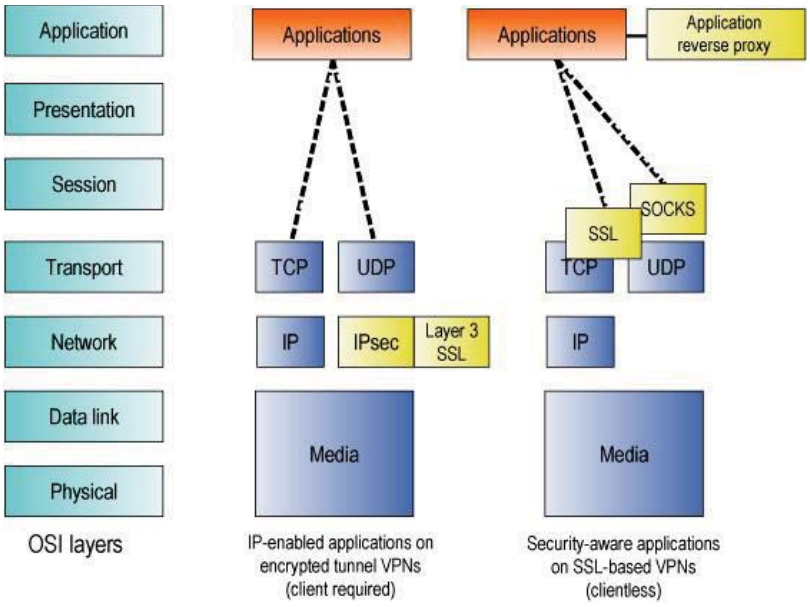


Figure 4-12 - Security Protocols and OSI Protocol Stack (Source: Disabato)

Figure 4-12 shows the relationship of the VPN security protocols to the Open Systems Interconnection (OSI) Protocol Stack while Figure 4-13 graphically shows the different VPN types discussed. **Layer 3 SSL VPN** and **IPsec VPN** are shown in the left of the diagram with the different Layer 3 Security accesses. **Direct clientless SSL VPN** and **Appliance clientless SSL VPN** are illustrated on the right of the diagram where the user client is typically a web browser.

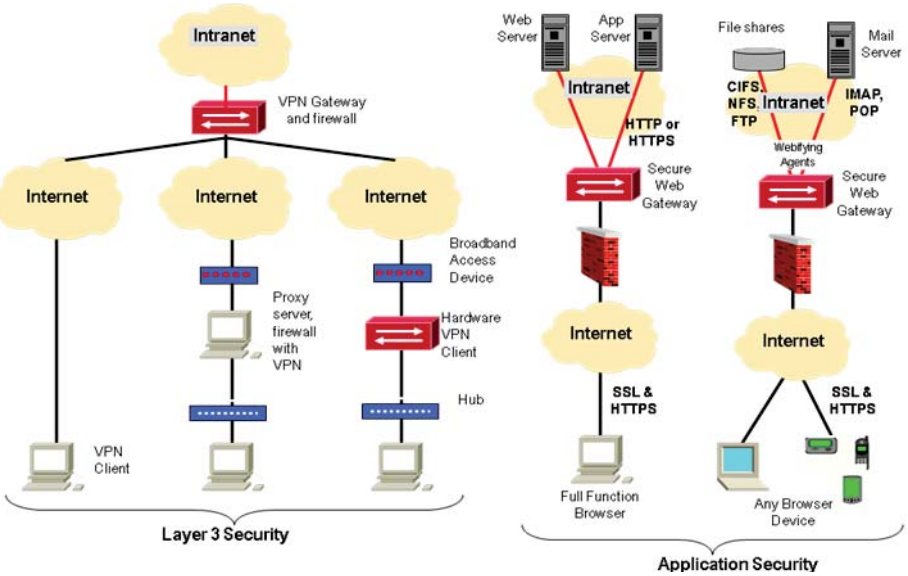


Figure 4-13 - Remote Access VPNs (Source: Young)

Authentication through each of these VPN types can be performed using several different authentication factors. Each of these, depending on the VPN vendor implementation, can support username/password, RSA SecureID, X.509 certificates, RADIUS, and LDAP directory data (Disabato, 2007).

4.3.2.2 Site-to-Site VPN

Enterprises use VPNs to build wide area networks (WAN) that connect the enterprise sites together. This is normally done in one of three ways: trusted VPN, secure VPN, and hybrid VPN (Young, 2006).

- **Trusted VPN** uses a dedicated service provider such as X.25, Frame Relay, or Asynchronous Transfer Mode (ATM) to protect their enterprise traffic between sites. The trusted VPN usefulness can depend on the carrier's coverage area.
- **Secure VPN** encrypts the traffic between enterprise sites to ensure privacy. The public Internet can be used to move this traffic. Site-to-site secure VPNs may offer the best overall solution for most enterprises because (1) they are available worldwide (or anyplace where Internet is), (2) have lower costs than trusted VPN, and (3) enterprise data is encrypted between VPN endpoints.
- **Hybrid VPN** will typically combine trusted and secure by encrypting traffic over a private service provider.

The technical details discussed in the remote-access VPN section may also apply to the discussion about site-to-site VPNs.

4.3.2.3 Issues with VPN

Issues with remote-access VPNs can be separated into five categories: security, application support, ease of deployment and management, scalability, and performance.

5 Network Access Control

Now that the primary component technologies of NAC have been described, the two main approaches to network access control will be discussed.

The **NAC Framework** is a comprehensive solution that controls network admission policies and provides for enforcement of network security compliance. This approach will generally require a significant investment in hardware, software, services, people resources, and changes to network infrastructure (Solution Profile: Cisco, 2007).

The **NAC Appliance** is normally a self-contained device that can assess endpoint security compliance, perform policy management and remediation services with minimum changes to network infrastructure (Solution Profile: Cisco, 2007).

5.1 NAC Frameworks

Three NAC frameworks exist today. These are Cisco's Network Assessment Control (C-NAC), Microsoft's Network Access Protection (NAP), and Trusted Computing Group Trusted Network Connection (TNC). Each of these is an independent solution where interoperability has been an issue until recently. In one effort to resolve the interoperability problem, the Network Endpoint Assessment group of the Internet Engineering Task Force (IETF) is defining a standard set of protocols that will allow these three frameworks to interoperate (What is the IETF NAC strategy, 2006).

In Figure 5-1 the main components of NAC are defined in terms of the IETF architecture. In an effort to establish a common set of terms, this section will map the IETF terms to the equivalent terms used by the three frameworks. A definition will also be provided for each functional component. The reader will notice a similarity with the 802.1x framework in some parts of the NAC framework.

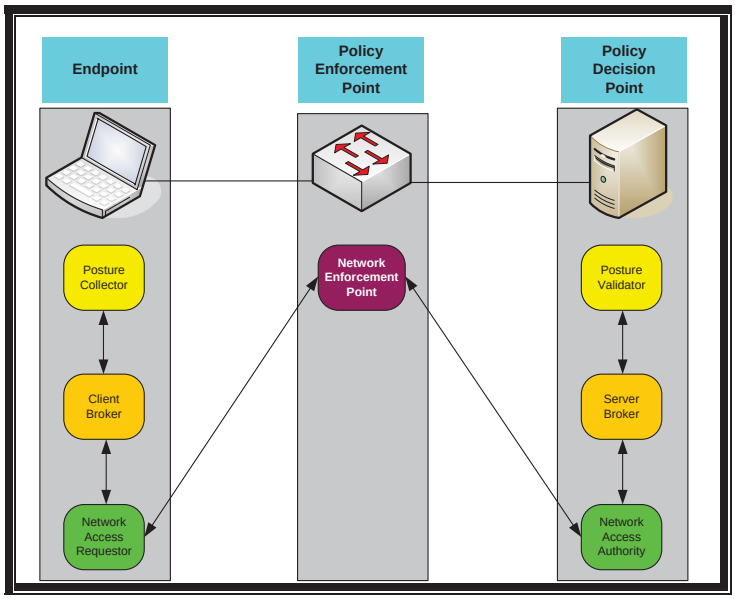


Figure 5-1 - IETF NAC Framework (Source: InteropLabs)

Three major groupings of functionality are present. The Endpoint contains posture collectors, a client broker, and a network access requestor. The Policy Enforcement Point (PEP) contains the Network Enforcement Point device. Lastly, the Policy Decision Point (PDP) contains posture validators, a server broker, and a network access authority. The Policy Decision Point functionality may not be restricted to a single server, but may be dispersed across multiple servers (InteropLabs, 2006).

The **Posture Collector** is third-party software that executes on the endpoint device and collects the security status of the device. This information can include information about the anti-virus version, the patch level of the operating system, and other information that reflects the 'health' of the client. There can be multiple posture collectors on the client (2006).

The **Client Broker** collects the information from the posture collectors. Once collected, the information is passed to the Network Access Requestor (2006).

The **Network Access Requestor** establishes network connectivity so the endpoint can be authenticated. It will also communicate the Endpoint Posture Collector data to the server side or policy decision point. This role is normally performed by an 802.1x supplicant or an IPsec VPN client (2006).

The **Network Enforcement Point** enforces network policy. This role can be performed by an 802.1x-capable switch, Wireless LAN, VPN gateway, or firewall (2006).

The **Posture Validator** is third-party software that is a complement to the Endpoint Posture Collector. The status information provided by the Endpoint Posture Collectors is evaluated against network policy and a status is passed to the Server Broker (2006).

The **Server Broker** performs a similar function to the Client Broker in that it provides an interface between the Posture Validators and the Network Access Authority (2006).

The **Network Access Authority** is a server that validates authentication and posture information. It also communicates policy information to the Network Enforcement Point (NEP) (2006).

In Figure 5-2 the IETF terms are mapped to the associated values for each of the three frameworks.

IETF Term	TCG TNC	Microsoft NAP	Cisco NAC
Posture Collector	Integrity Measurement Collector	System Health Agent	Posture Plug-in Applications
Client Broker	TNC Client	NAP Agent	Cisco Trust Agent
Network Access Requestor	Network Access Requestor	NAP Enforcement Client	Cisco Trust Agent
Network Enforcement Point	Policy Enforcement Point	NAP Enforcement Server	Network Access Device
Posture Validator	Integrity Measurement Verifier	System Health Validator	Policy Server Decision Points and Audit Server
Server Broker	TNC Server	NAP Administration Server	Access Control Server
Network Access Authority	Network Access Authority	Network Policy Server	Access Control Server

Figure 5-2 - IETF NAC Terms (Source: InteropLabs)

Although each of the frameworks has similar functionality, the segmentation and the implementation of that functionality does differ between each of the frameworks. To gain a better understanding of these differences, the reader is directed to Network Access Control Frameworks section in the Supplemental Material chapter at the end of this paper. To demonstrate the basic flow of control and workflow of information between the NAC parts, an abstracted access control flow is presented.

Figure 5-3 illustrates a possible network access scenario.

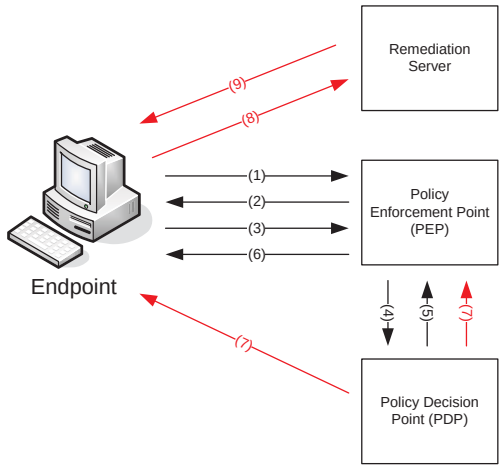


Figure 5-3 - Network Access Scenario

Step	Description
1.	Endpoint requests access to the network
2.	PEP requests security posture information from endpoint
3.	Endpoint sends consolidated posture information from all Posture Collectors to PEP
4.	PEP sends consolidated information to PDP
5.	PDP Posture Validators validate posture information against the security policy and sends instructions to PEP
6.	If endpoint is compliant, PEP allows full access to trusted network
7.	If endpoint is not compliant, PDP sends remediation instructions to PEP and endpoint
8.	Endpoint requests updates from remediation servers
9.	Remediation servers send updates to endpoint
10.	Access process restarts at step 1

5.2 NAC Appliances

NAC appliances have been referred to as "NAC-in-a-box" by some industry writers. These devices are filling the gap between the NAC infrastructures from Cisco, Microsoft, and TCG while these infrastructures mature. The NAC appliances are able to deliver benefits today on many of the promises made by the NAC infrastructures (Phifer, 2006).

According to an Infonetics Research report, manufacturers' revenue for NAC enforcement will grow from $323 million to $3.9 billion -- between 2005 and 2008. Most of this will be from network-integrated enforcement devices (Burger, 2007).

Arguably it can be easier and less expensive to insert one device in the network than it is to redesign and deploy new technologies to support network access control. Many NAC appliances try to avoid wholesale changes to the network infrastructure by augmenting what already exists (2006).

One way that they accomplish this is by minimizing dependencies on third-party systems by including as much of the required NAC functionality as possible (2006).

They also lower the total cost of ownership by not depending on any specific operating system functionality. In a practical sense, this means that they do not deploy endpoint agents but rather use scans to evaluate the endpoint systems (2006).

NAC appliances also integrate well with existing heterogeneous networks by connecting to Layer 2 and Layer 3 switches. The connection may be in-band or out-of-band (Phifer, 2006; Hanna, 2007).

In-band NAC appliances, shown in Figure 5-4, are inserted at critical points in the network. They combine assessment, enforcement, and remediation processes but enforcement is limited and the devices are expensive. For some, a separate user authentication is required (Hanna, 2007).

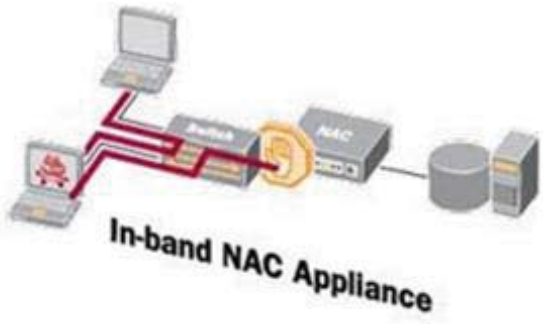


Figure 5-4 - In-band NAC Appliance (Source: Hanna)

Out-of-band NAC appliances, shown in Figure 5-5, integrate with networking devices such as routers, switches, DHCP servers, VPN gateways, wireless access points, firewalls, and others. Assessment and remediation are performed by the NAC appliance when the network device detects that a new endpoint as connected to the network. Advantages of out-of-band NAC appliance is that (1) it is less expensive than in-band device because a single NAC appliance can manage the whole network, and (2) more secure because it can stop an endpoint from joining the network sooner. But out-of-band NAC is more complex because it has to be integrated with the network devices (2007).

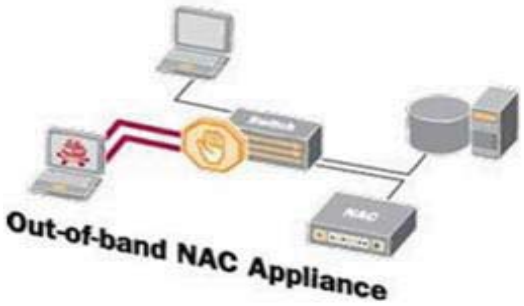


Figure 5-5 - Out-of-band NAC Appliance (Source: Hanna)

Proxying LAN access to an enterprise's existing Active Directory, LDAP, or RADIUS authentication servers is normally available. The results are then used to enforce network policies. To support VPN and 802.1x users, some NAC appliances also support certificates and two-factor authentication (Phifer, 2006).

Some NAC appliances also contain built-in policies that evaluate an endpoint's security posture and compare that posture against policy requirements, but may not be able to force the host to take remedial action. For example, a scan of an endpoint may reveal a threat, but the appliance may not be able to force the host to launch an anti-virus scan to correct the problem (2006).

Endpoint quarantine is available from most NAC appliances where the endpoint is placed on a VLAN or subnet where a remediation server can address the issues on the endpoint. This is one of the important cost justifications for NAC – reduction of help-desk intervention for simple changes (2006).

Most NAC appliances are product suites that include an assortment of assessment and enforcement devices tied to a central policy server (2006).

Appliances have the advantage of (1) integrating into an organization's current management systems, and (2) ensuring that the initial cost savings for the device is not offset by the ongoing administration costs. However, current appliances contain their own administrative and management interfaces that may not be compatible with existing datacenter management tools (Mohamed, 2007). Concerns expressed in technical polls on NAC usually point out that the top technical issues are uncompromised fault tolerance and undiminished network performance (Phifer, 2006).

One type of appliance is clientless endpoint security management (CESM). CESM can evaluate all aspects of endpoint activity. Some CESM advantages are: (1) more cost effective because there is no endpoint deployment,

(2) can identify unauthorized programs and changes on the endpoint, (3) repair and identify misconfigured endpoint services, and (4) is able to manage third-party security clients that may be disabled. As an added bonus, CESM provides pre-NAC functionality that can clean corporate endpoints before a full deployment of NAC (Tammam, 2007).

NAC and CESM are complementary because NAC blocks infected endpoints from entering the network and CESM monitors the endpoint after entry to ensure compliance to network policy. CESM tends to be a good single solution when guest users are not allowed on the trusted network and when remote access isn't used (2007).

The future of NAC appliances is expected to be integration with the larger NAC infrastructure solutions. Many appliance vendors are partnering with both Cisco NAC and Microsoft NAP. Companies with heterogeneous networks deploying NAC will benefit as the three NAC infrastructures move closer together and are able to interoperate effectively (Phifer, 2006).

The basic form of NAC, as exemplified by the all-in-one appliances, appears ready for use by a large number of organizations. These products have proven themselves by being able to verify endpoint integrity and to control network access. According to an evaluation performed on thirteen NAC products by Network World, vendor's are investing large sums in research and development to make their products integrate seamlessly within the existing network infrastructures (Andress, 2007).

6 Areas of Concern

There are many areas where NAC deployment can affect the operation of the enterprise network. Even the simplest changes add complexity to an already complex arrangement of devices, but when an enterprise deploys a NAC infrastructure such as Cisco NAC, Microsoft NAP, or a TCG TNC implementation, the possibility of a mistake that can severely impact the network can rise significantly.

6.1 Future Enterprise Network Infrastructure

The methods that an enterprise can select for their network infrastructure will depend on the level of control that the enterprise has over the network infrastructure (Maiwald, 2007).

For organizations that maintain complete control over their network infrastructure, then all of the NAC solutions discussed can be used. For organizations that do not have control of the client network but still maintain control of the data center network will be limited in the solutions that can be employed. These solutions will include in-band and out-of-band devices within the data center network, cryptographic appliances that arbitrate access to the data center network, and endpoint agents on those devices requesting access. For those organizations that will not have control of either the client or data center network, their options will be limited to solutions that install either endpoint enforcement agents or cryptographic agents on the endpoint (Maiwald, 2007).

Network acceleration technologies will also be a concern for organizational networks that deploy NAC. Many e acceleration technologies compress or tokenize information to an extent that the information will not be understood by the network monitoring devices. This will become an important consideration for the placement of In-band and out-of-band devices (Maiwald, 2007).

6.2 Endpoint Control

Who controls the endpoint is also an important consideration when deploying NAC. In the enterprise today, many endpoints are not managed by the organization. Some are employee home systems and some belong to consultants, contractors, and vendors. Each of these will probably have different policies that govern them, and

some may have policies that prevent them from installing an enterprise's agent. These systems will not have a permanent agent installed and even if a temporary agent is installed when these endpoints join the enterprise network, this may only address part of the problem. The other half of establishing a compliant endpoint may require remediation. If the enterprise does not manage an endpoint then its ability to remediate the endpoint may be limited (Maiwald, 2007; Discini, 2007).

6.3 Architectural Considerations

It appears to be a given that there will be an impact to the enterprise network architecture, regardless of the approach taken to implement NAC. While this impact may be minimized, perhaps through the deployment of a single NAC appliance, some of the solutions discussed thus far will be significant. Perhaps the least obvious, but certainly one of the biggest potential issues, is that of a denial of service condition for authorized employees. A configuration misstep can block access to the wrong endpoints (Maiwald, 2007).

6.3.1 Nontechnical impact

NAC deployment will also experience nontechnical impacts. The first concerns the non-personal computer devices like printers, mechanical devices, door locks, medical equipment, and other devices that access the organizational network. It is unlikely that these devices will have any type of agent installed that can respond to a request for user credentials or platform identification. And unless an exception process exists, these devices will be denied access to the network. To understand exceptions required, an organization must know what or who is accessing their network. Compiling this list should be completed before implementing any NAC solution (2007).

This concern for non-PC devices prevented Kaiser Permanente from implementing NAC because it couldn't help secure its medical devices. Kaiser Permanente believes that NAC must provide far more than pre-admission control which means it must have broad access control to corporate information. To protect devices, there must be a way to put the device in a role where access to the device can be controlled, and information from the device can be restricted. A challenge for IT is that security products don't allow them to implement controls using business logic. More control capabilities need to be embedded directly in the network infrastructure instead

of bolting on new appliances (McLean, 2007). So providing exceptions for these devices may still not be sufficient for every situation.

The second nontechnical problem area is the impact on the organization's helpdesk and problem resolution systems. As should be obvious by now, NAC adds additional complexity to an already complex arrangement of devices and software. The helpdesk personnel will need additional training in order to differentiate between NAC induced problems and other problem causes (Maiwald, 2007).

6.3.2 Network Availability

A NAC approach that uses in-band devices introduces a potential failure point in the network. If an in-band device fails, the network traffic stops. This problem can be addressed by high-availability configurations where two in-band devices are installed in parallel and spanning tree protocol is used between the devices. However, this is a major topological change to an organization's network that many companies are unwilling to make (2007).

A second area of concern for network availability is the proper configuration of the various network infrastructure devices. Today organizations experience configuration issues without a NAC solution installed. For example, according to a Forrester Research survey, in-house wireless local area networks (WLAN) provide access to corporate applications and networks for 63% of US companies. However, misconfiguration of these access points will result in 90% of WLAN security incidents over the next three years (Computer Weekly Reporter, 2007).

Switches and other network devices must have their configurations changed to support the different NAC approaches. To prevent significant outages, proper change control procedures and people with the proper expertise must exist (Maiwald, 2007).

6.3.3 Network Monitoring

The span or monitoring ports on network switches are used to monitor for unauthorized network traffic and for proper operation of the switch. Some enterprises have seen issues with network intrusion device use of these ports. If out-of-band devices are used in the NAC solution, similar issues may occur, but with potentially more dire consequences because the out-of-band devices are being used for network access control devices

instead of intrusion detection devices. If the out-of-band device is disconnected from the network then the network loses control of who is accessing in the network (2007).

6.3.4 New technologies

Some people believe that NAC will reduce the development and adoption of new technologies outside of the mainstream because of the lack of an agent. However others believe that this should not be a major impediment (Seltzer, 2007). Just as a video card manufacturer today must provide a driver for the various operating systems the card supports, a NAC agent or agents will be needed in the future for network devices to operate within a NAC solution.

6.4 Complexity

Since the network's primary responsibility is to stay on and available, Forrester's Natalie Lambert states that adding the complexity of NAC, such as policy servers, creates additional opportunities for the network to fail. To address this issue, she indicates that the network access control enforcement should move from the policy server to the endpoint security and management tools. Eventually big companies like Microsoft, Cisco, and Symantec will offer all the required functionality in one package, but until that happens, smaller company products will fill in the empty places (The Death of NAC, 2007).

Nathan McLain, product manager for LANDesk Software points out that NAC complexity results from the need to configure switches, servers, routers, or RADIUS servers in a NAC infrastructure. NAC products should provide multiple functions like antivirus, host intrusion prevention, and policy enforcement, and these should be managed through a single management console (The Death of NAC, 2007).

Rich Weiss, director of endpoint product marketing at Check Point Software, indicates that NAC products attempt to do too much and their management consoles fail to integrate with existing security products. He asserts that endpoints should control access through basic products (antivirus and desktop firewalls) with NAC capabilities. Weiss cautions that smaller company products may be immature, their long term viability questionable, may create integration challenges, and their product quality may be unknown (The Death of NAC, 2007).

6.5 Interoperability

A well-defined suite of NAC operation standards does not currently exist. These are needed to facilitate the interoperability of NAC products among multiple vendors. Interoperability will become even more critical in the future as NAC implementations become ubiquitous. Consider an individual that must connect at different times to an Internet service provider and a corporate network. Without a common standard, multiple agents installed on the accessing device may be required where as a single, standard agent would be all that is needed to allow enforcement of differing security policies (Schaffer, 2007).

The Internet Engineering Task Force (IETF) Network Endpoint Assessment working group and the TCG Trusted Network Connect work group are both attempting to define standards that are independent of vendor platform (Schaffer, 2007; Howell, 2007). However, Cisco has declined to participate in the TCG TNC effort but is a major player in IETF. It may be this forum where an industry standard is finally developed. The chair of the IETF Network Endpoint Assessment working group is shared by Cisco and Juniper Networks, which is also a co-chair of the TCG TNC (Howell, 2007).

Microsoft is working with its partners and standards organizations to create a cohesive protection strategy. This is primarily motivated by the dominance that Microsoft has in the client / server space and in fact that the vast majority of security-related attacks are directed toward Microsoft products (Schaffer, 2007).

Microsoft has taken two significant steps to improve the interoperability of NAP with other frameworks. In 2006, Cisco and Microsoft announced that their NAC solutions would be able to work together, and in May, 2007, TCG and Microsoft announced that their solutions would be interoperable. In addition to this, Cisco and Microsoft have both established large partner networks of vendors with products that will work with their solutions. Many of these partners are both Microsoft and Cisco vendors and will be able to support both Microsoft NAP and Cisco NAC (Schaffer, 2007; Howell, 2007).

At Interop exposition in Las Vegas in 2007, the NAC Interoperability Lab demonstrated a NAC system composed of equipment and software from multiple vendors. In one part of the lab equipment and methods from vendors using TNC and IETF initiatives were shown, while in another part, Microsoft's NAP and Cisco's NAC

configurations were operational (Schaffer, 2007). This bodes well for the future of NAC because it demonstrated that these different technologies can work together despite the lack of an overreaching standard.

An interoperability standard will eventually emerge if for no other reason than market pressure from NAC customers. In Network Computing survey of companies planning or deploying NAC solutions, a majority of respondents expressed the need for a single standard for NAC frameworks. While Cisco's NAC was rated as the favorite among respondents, the majority of respondents expressed no preference about who should win the framework standard battle, as long as in the end, there was only one standard (Dornan, 2007).

7 Project Conclusions

7.1 Analysis of results

Thus far, this presentation has briefly examined the complexities of the technologies and issues associated with NAC deployment. It would be fair to say that a disruption to an organization's network services should be expected. This would be the intuitive conclusion. This position is also supported by much of the press about NAC. However, in its second annual NAC survey, *Network Computing* found that the actual results from those that have deployed within the last year to be somewhat counterintuitive.

The 326 respondents categorized themselves as:

- 36 percent IT management
- 25 percent IT staff
- 25 percent C-level executives
- 14 percent as independent consultants and other positions (Dornan, 2007).

The survey found that 45% were currently deploying a NAC solution, 41% planned to deploy within 12 months, and 14% indicated no plans to deploy a NAC solution. This was down from 46% in the previous year's survey (Dornan, 2007).

The respondents indicated that the issues driving them toward NAC were:

- Address network security compliance requirements (65%)
- Controlling access to specific network resources (58%)
- Address specific regulatory compliance requirements (28%)
- Controlled access for unmanaged users (25%)
- Protect wireless computers (20%) (2007)

Even though specific regulatory compliance is third on the list of NAC drivers, many of the respondents are accountable for government and industry regulations. The distribution is fairly even across planners, deployers, and those with no plans as can be seen in Figure 7-1 (2007).

Regulation	Planners	Deployers	No plans
SOX	42%	44%	30%
HIPAA	41%	38%	42%
Payment Card Industry	22%	26%	25%
Gramm-Leach-Bliley	25%	20%	15%
DoD directives (8100.2, 8320.2, etc.)	12%	19%	11%

Figure 7-1 - Regulatory Accountability (Source: Dornan)

Branch office security and SOX compliance are driving larger NAC installations than what the current planners envisioned (2007). IDC estimates that the NAC market will grow to $.3.2 billion by 2010 from $526 million in 2005, and this growth will be driven by the finance, health care, and education areas addressing regulatory compliance requirements (McLaughlin and Ohlhorst, 2007).

Educational institutions, with 20% of all NAC initiatives, have a lot of unmanaged devices. It is also the fastest growing sector for NAC planners and deployers. However, the health-care industry with a great deal of specialized network-connected devices lacks the ability to participate in NAC because of the design of these devices (Dornan, 2007).

The good news is that the current press about NAC appears to be overly negative. For those companies and organizations that have implemented a NAC solution, they indicated that NAC is easier to deploy than thought, it was less disruptive than feared, it required fewer changes to network configurations than was assumed, and there was less impact to productivity than expected (2007).

However, some issues mar this positive news. There is little or no interoperability between the many solutions offered. No single solution solves all problems and the lack of interoperability between solutions means that users may have to log out of one application before they can access a different one. For those that have deployed a solution, the average cost is 12% of the entire enterprise budget. Even at that, these respondents felt it was well worth the expense. Like many security projects it is sometimes hard to quantify the actual return-on-investment for upper management (2007).

As with many things, once something has actually been done, opinions can change. The poll found that those who have actually deployed NAC had a higher opinion of NAC than the planners did, and surprisingly, 41% of deployers indicate that initial rollouts took less than three months. Those organizations that have deployed NAC

have higher revenue and more employees than average, which seems somewhat counterintuitive for early adopters (2007).

Interestingly, the early NAC deployers are less likely to have wireless networks in their organizations. This is viewed as an unnecessary risk factor to network security. However, for those that do have WLAN, they will typically have the 802.1x support that many NAC solutions need, which means that upgrades to the enterprise WLAN may not be required to support NAC (2007).

One of the pervasive perceptions about NAC is that wide-spread infrastructure changes are needed to deploy a solution. For those that responded to the survey, on average, one third expected upgrades would be required to their current IT devices, but those that were actually deploying NAC expected fewer upgrades. There was evidence that the reason for this difference between the perception and the results may be due to current NAC products being standalone appliances (2007).

"We looked at solutions that would require an upgrade of the infrastructure, and that would be close to 50 percent of our security budget," says a security engineer at a state university. Rather than selecting one of the framework solutions, the university used standalone products from three different vendors that were deployed on five campuses. The primary driver for this decision was the cost of the framework was more than the management cost of multiple enforcement points (2007).

Expectations of how much IT infrastructure would have to change for a successful NAC deployment showed a mean of 30 percent, where deployers had lower expectations for change than planners. Of the deployers, 15 percent performed no upgrades to their network while 26 percent had to upgrade more than a quarter of their network infrastructure (2007).

When asked how much of their networks were 802.1x-capable, both planners and deployers indicated 54 percent. However, the NAC deployers were actually running 802.1x over 33 percent of their network while the non-deployers were using 802.1x over just 23 percent of their network (2007).

For those willing to upgrade their network infrastructure, the most likely NAC upgrade was to add in-band appliances or extra enforcement points (firewalls) (2007).

The top two barriers to NAC adoption are cost and complexity, but impact on productivity is a growing concern because of the belief that NAC is incompatible with some applications like CRM, ERP, and remote-access

clients. For example, a NAC deployment that uses IPsec will break an application that requires direct access to the Internet. Those that have actually deployed NAC don't rate productivity impact as highly as the planners. At least one respondent believed that productivity had been increased because of the automatic quarantine and remediation features of NAC (2007).

One key area of complaint was the inability to "demonstrate clear benefits and ROI to internal stakeholders." Very high expectations contribute to this problem. The trend toward more stringent network-access policies is demanding more of NAC product capabilities (2007).

The highest rated technical issue for a NAC solution is its ability to easily integrate with other infrastructure components. This was classified as "very important" or "somewhat important" by all 179 people in the deployer group while one of the least important technical issues is the support for non-Windows operating systems like Linux and Apple Mac (2007).

Sixty-five percent of the respondents indicated that they were currently using either the Cisco NAC framework or appliances. This may be temporary until Microsoft releases NAP because more than one-third of the respondents indicated they were considering Microsoft NAP (2007).

This reader poll disclosed at least two very important results. The first is that NAC planners hold the common conception that NAC is complex, costly, and will affect productivity of their networks. The second is that for the organizations that have deployed NAC, it was easier than anticipated and provided productivity enhancements in some cases. While the deployers did spend on average 12% of their IT budget deploying NAC, they felt this was money well spent (2007).

I suspect that anyone examining a NAC solution would have the same impression of complexity and concern about the disruption to productivity. This appears intuitive. This, I believe, can be mitigated with a comprehensive deployment plan before the first configuration is changed or a new piece of hardware is plugged-in. And the plan needs to begin with a well thought out policy statement that leaves no doubt of what the organization's goals are. NAC success is anchored in a strong security practice with a properly architected network; once that is in place, then "it's all about policy" (McLaughlin and Ohlhorst, 2007).

The move toward NAC is underway. Some will wait until a single standard emerges before committing resources and time to deploying NAC. Others will ease into a NAC solution through all-in-one NAC appliances, and

others will adopt the framework as a comprehensive solution. But eventually most organizations will adopt NAC. In a recent IDC study, *Network Admission Control: Organizations Get the Knack for NAC*, IT executives agreed that an essential part of an overall enterprise security strategy would be based on NAC, and that the interoperability agreements between the primary NAC vendors and standards group are alleviating NAC adoption concerns (Tekrati, 2007).

7.2 Project Summary

This project has met all of my expectations and objectives. This subject was chosen because it is an significant and evolving component of one of the most important security challenges facing organizations today, especially educational institutions where a large population are attaching their unmanaged computer systems to the education network each day. It is vital that the institutions are able to identify the users, the devices, and to ensure that the devices are "healthy" with respect to the organizations security policies.

This project also satisfied my objective for the investigation of a new set of technologies. While much of the infrastructure of NAC has existed for sometime (e.g. switches, routers, firewalls, VPN) there are new technologies (e.g. NAC appliances) and new ways of marshalling them to protect the ever shrinking network perimeter.

This project also gave me the opportunity to apply the information studied in the master's program and to explore at a greater depth these technologies. As an example, while I had had a cursory exposure to 802.1x and Extensible Authentication Protocol (EAP), this project required that I explore this topic in more detail than my courses required. I had a similar experience in several other areas.

The key assertion of this project was that NAC was too complex and disruptive to deploy. To adequately address this assertion, an explanation of the technologies involved in NAC was needed as a prerequisite to answering this question. Attempting to balance the need for clear explanation of the NAC technologies and the depth of discussion about these technologies was an ongoing struggle. The question: *Has enough been explained?*, was always on my mind. To balance out the long narrative passages, a large number of graphical representations were used to simplify the concepts.

I was disappointed that there were so few scholarly articles and user surveys on this subject. This forced me to rely on articles from vendor sites, e-journals and e-magazines, as well as, companies that specialized in the topics covered in this paper. While these are important sources of information, there was always the possibility of bias. I always strived to find multiple sources to achieve a balanced view of a topic, but this was not always possible.

Although I spent far more time than recommended on the project, I feel that it achieved one of the key thesis goals of in-depth study on a specific topic. Network Access Control is an emerging technology and will probably not achieve its full potential for several years, especially since one of the biggest players, Microsoft, has not yet released its Network Access Protection product. Mobility of users has contributed to the shrinking of the network perimeter and this is a trend that is unlikely to abate. Corporate data centers have become the castle keeps without the traditional walls that have provided protection in the past. The most effective way to protect the most important asset of a company – its information – is to not allow someone access to that information in the first place. NAC provides an opportunity for achieving this goal.

8 References

(2005). Implementing Network Access Control Phase One Configuration and Deployment. Cisco Systems, Inc. Retrieved on August 4, 2007 from http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

(May, 2005). What is EAP-FAST? InteropNet Labs Full Spectrum Security Initiative. Retrieved on May 23, 2007, from www.opus1.com/nac/whitepapers-old/E-**EAPfast**-LV05.pdf

(May, 2005). What are your EAP Authentication Options? InteropNet Labs Full Spectrum Security Initiative. Retrieved on May 23, 2007, from www.opus1.com/www/whitepapers/8021x-**eap**-auth-types.pdf

(13 Oct 2005). Network Admission Control: Technical Overview. Cisco Systems, Inc. Retrieved on August 4, 2007, from http://www.cisco.com/application/pdf/en/us/guest/netsol/ns617/c664/cdccont_0900aecd80102f1b.pdf

(May, 2006). Getting Started with Network Access Control. Network Access Control Interoperability Lab. Retrieved on May 19, 2007, from http://www.interop.com/lasvegas/exhibition/interoplabs/nac/gettingstartedNAC.PDF

(May, 2006). What is the IETF NAC strategy? Network Access Control Interoperability Lab. Retrieved on May 19, 2007, from http://www.interop.com/lasvegas/exhibition/interoplabs/nac/IETFNACstrategy.PDF

(May, 2006). What is Cisco NAC? Network Access Control Interoperability Labs. Retrieved on May 23, 2007, from http://www.interop.com/lasvegas/exhibition/interoplabs/nac/CISCONAC.pdf

(May, 2006). What is Microsoft's Network Access Protection? Network Access Control Interoperability Labs. Retrieved on May 23, 2007, from http://www.interop.com/lasvegas/exhibition/interoplabs/nac/MSNAP.pdf

(May, 2006). InteropLabs Network Access Control Architecture v2. Network Access Control Interoperability Labs. Retrieved on June 2, 2007, from http://www.interop.com/lasvegas/exhibition/interoplabs/nac/NACoverview-color-v2.pdf

(May, 2006). What is the IETF NAC strategy? Network Access Control Interoperability Labs. Retrieved on June 2, 2007, from http://www.interop.com/lasvegas/exhibition/interoplabs/nac/IETFNACstrategy.PDF

(May, 2006). What is 802.1x. Interop Labs. Retrieved on May 23, 2007, from http://www.interop.com/lasvegas/exhibition/interoplabs/nac/8021X.PDF

(May, 2006). What is TCG's Trusted Network Connect? Network Access Control Interoperability Labs. Retrieved on May 23, 2007, from http://www.interop.com/lasvegas/exhibition/interoplabs/nac/TCG.PDF

(Nov, 2006). The Importance of Standards to Network Access Control. Juniper Networks. Retrieved on August 15, 2007 from http://www.juniper.net/solutions/literature/white_papers/200205.pdf

(Mar, 2007). 802.1x: Port-Based Authentication Standard for Network Access Control (NAC). Juniper Networks. Retrieved on August 17, 2007 from http://www.juniper.net/solutions/literature/white_papers/200216.pdf

(April 2007). Network Endpoint Assessment (NEA): Overview and Requirements. NEA Working Group of the The Internet Engineering Task Force. Retrieved on May 17, 2007 from http://tools.ietf.org/html/draft-ietf-nea-requirements-02

(25 April, 2007). Network Access Protection Platform Architecture. Microsoft Corporation. Retrieved on August 5, 2007, from http://www.microsoft.com/technet/network/nap/naparch.mspx

(25 April, 2007). Introduction to Network Access Protection. Microsoft Corporation. Retrieved on August 5, 2007, from http://www.microsoft.com/technet/network/nap/napoverview.mspx

(17 May 2007). NAC Competition: Start with a little TCG. NetworkWorld. Retrieved on June 7, 2007, from http://www.networkworld.com/research/2006/040306-nac-tcg.html

(25 May 2007). The Death of NAC? Security Options for the SME. Processor.com Retrieved on June 2, 2007, from http://www.processor.com/editorial/article.asp?article=articles/P2921/31p21/31p21.asp&guid=

(25 June 2007). Network Admission Control market to reach $3.2 billion by 2010, says IDC. Tekrati. Retrieved on August 25, 2007, from http://www.tekrati.com/research/News.asp?id=9047

(August, 2007). Solution Profile: Cisco NAC Framework. Breakaway Security Group. Retrieved on August 1, 2007, from http://www.secureaccesscentral.com/nac/ciscoNAC.php

Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and Levkowetz, H. (June 2004). RFC 3748 Extensible Authentication Protocol (EAP). Network Working Group. Retrieved on July 14, 2007 from http://www.ietf.org/rfc/rfc3748.txt

Andress, M. (30 July 2007). NAC alternatives hit the mark. NetworkWorld. Retrieved on August 19, 2007, from http://www.networkworld.com/reviews/2007/073007-test-nac-main.html?fsrc=rss-cisco

Barr, D. (December 2004). Public Key Infrastructure. Office of the Manager National Communications System. Technical Notes. Retrieved on June 30, 2007, from www.ncs.gov/library/tech_notes/tn_vol11n3.pdf

Burger, A.K. (June 1, 2007). Network Security, Part 2: NAC Moves Up the Architecture. TechNewsWorld. Retrieved on June 2, 2007, from http://www.technewsworld.com/story/57640.html

Ciampa, M. (2005). Security+ Guide to Network Security Fundamentals. Second Edition. Thomson Course Technology.

Chen, J. and Wang, Y. (2005). Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience. Retrieved on June 22, 2007, from http://wire.cs.nthu.edu.tw/wire1x/COMMAG-05-00270-post.pdf

Computer Weekly Reporter. (May 20, 2007). Meet the challenge of WLAN security. ComputerWeekly.com . Retrieved on June 15, 2007, from http://www.computerweekly.com/Articles/2007/05/29/224042/meet-the-challenge-of-wlan-security.htm

Cross, M., Johnson Jr., N.L., Piltzecker, T., Shimonski, R.J., Shinder, F.L. (2002). Security+ Study Guide and DVD Training System. Syngress Publishing Inc.

Diodati, M. and Blum, D. (September 2006). Public Key Infrastructure. Burton Group. Retrieved on July 6, 2007, from http://www.burtongroup.com/Client/Research/Document.aspx?cid=209

Disabato, M. (Jul 13, 2007). Remote Access VPNs: Not Just for Road Warriors. Burton Group. Retrieved on July 21, 2007, from http://www.burtongroup.com/Client/Research/Document.aspx?cid=1094

Discini, S. (May 29, 2007). NAC: The Hard Part. Enterprise IT Planet. Retrieved on June 7, 2007, from http://www.enterpriseitplanet.com/networking/features/article.php/3680196

Dornan, A. (May 14, 2007). NAC: More is More. Network Computing. . Retrieved on June 15, 2007, from http://www.networkcomputing.com/channels/security/showArticle.jhtml?articleID=199204304

Hacker, D. (2003). A Writer's Reference. Fifth Edition. Boston – New York: Bedford/ST. Martin's.

Hanna, S. Ed. (21 May 2007). TCG Trusted Network Connect TNC Architecture for Interoperability. Specification Version 1.2 Revision 4. Trusted Computing Group. Retrieved on August 11, 2007 from https://www.trustedcomputinggroup.org/specs/TNC/TNC_Architecture_v1_2_r4.pdf

Hanna, S. (April 24, 2007). Getting the NAC of Network Access Control. Enterprise Systems. Retrieved on June 7, 2007, from http://esj.com/security/article.aspx?EditorialsID=2554

Harris, S. (2005). CISSP All-in-One Exam Guide, Third Edition. McGraw Hill Osborn. New York

Hardjono, T. and Dondeti, L. R. (August 30, 2005). EAP, TLS, and Certificates. In Security in Wireless LANs and MANs. Artech House Publishers.

Hildebrandt, R. and Koetter, P. (2005). Understanding Transport Layer Security. In The Book of Postfix: State-of-the-Art Message Transport. No Starch Press.

Hook, D. (2005). SSL and TLS. In Beginning Cryptography in Java. Wrox Press.

Howell, D. (May 31, 2007). Cisco, Microsoft, Others Get Together on Security. Investor's Business Daily. Retrieved on June 7, 2007, from http://www.investors.com/editorial/IBDArticles.asp?artsec=17&artnum=1&issue=20070531

Johnston, A.B. and Piscitello, D. M.. (2006). Security Protocols. In Understanding Voice over IP Security. Artech House Telecommunications Library.

Kelly, D. (October, 2005). Vulnerability Management. Burton GROUP. Retrieved on July 27, 2007, from http://www.burtongroup.com/Client/Research/Document.aspx?cid=714

Lockhart, A. (May 7, 2007). Securing a RADIUS server. NetworkWorld. Retrieved on June 20, 2007, from http://www.networkworld.com/columnists/2007/050707-wireless-security.html

Maiwald, E. (Feb. 8, 2007). Architectural Alternatives for Enforcing Network Admission Requirements. Burton Group. Retrieved on May 17, 2007 from http://www.burtongroup.com/Client/Research/Document.aspx?cid=1000

McLaughlin, K, Ohlhorst, F.J. (23 Jul 2007). Network Access Control Made Easy. Channel Web Network. Retrieved on August 25, 2007, from http://www.crn.com/security/201002352

McLean, M. (May, 2007). Security as an After-Thought and (again!) What NAC Can Do for You. Mmclean-at-consentry-dot-com. Retrieved on June 2, 2007, from http://blog.consentry.com/blog/2007/05/security_as_an_.html

Mohamed, A. (June 5, 2007). The rise of the computing device. ComputerWeekly.com Retrieved on June 7, 2007, from http://www.computerweekly.com/Articles/2007/06/05/224539/the-rise-of-the-computing-appliance.htm

Oppliger , R. (2002). SSL and TLS Protocols. In Security Technologies for the World Wide Web. 2nd Ed. Artech House Publishers.

Phifer, L. (28 Mar 2006). Choosing the right flavor of 802.1x. SearchSecurity.com. Retrieved on July 16, 2007 from http://searchsecurity.techtarget.com/general/0,295582,sid14_gci1167608,00.html?track=wsland3

Phifer, L. (7 Nov 2006). NAC appliances: Shortcut to access control. SearchNetworking.Com. Retrieved on August 18, 2007 from http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1228704,00.html

Robinson III, C.W. (June 28, 2006). The Network Gatekeeper. Retrieved on June 22, 2007, from http://www.networkcomputing.com/showitem.jhtml?docid=1713crash

Robinson, F. (May 27, 2004). Review: Enterprise Radius Servers. NetworkComputing. Retrieved on June 16, 2007, from http://www.networkcomputing.com/showitem.jhtml?docid=1510f3

Schaffer, G. (August 2, 2007). Getting the NAC of futurology - A look at the evolution of NAC. Techworld. Retrieved on August 23, 2007, from http://www.techworld.com/networking/features/index.cfm?featureid=3579

Schurman, J., Thomas, R. and Christian, B. (2006). Introducing Microsoft Unified Communications. In Professional Live Communications Server. Wrox Press.

Seltzer, L. (May 15, 2007). Standards and the State of NAC. eWeek. Retrieved on May 17, 2007 from http://www.eweek.com/article2/0,1895,2129757,00.asp

Snyder, J. (04/03/06). What is NAC anyway? Network World. Retrieved on May 19, 2007, from http://www.networkworld.com/research/2006/040306-nac-primer.html

Snyder, J. (Apr 3, 2006). Opinion: An educated guess as to why NAC schemes abound. NetworkWorld. Retrieved on June 7, 2007, from http://www.networkworld.com/research/2006/040306-nac-opinion.html

Snyder, J. (30 July 2007). 6 tips for selecting the right all-in-one NAC product. NetworkWorld. Retrieved on August 19, 2007, from http://www.networkworld.com/reviews/2007/073007-test-nac-tips.html

Sturdevant, C. (2007, March 5). All-Access Pass? *eWeek.* Retrieved on May 12, 2007, from http://eweek.com/print_article2/0,1217,a=202367,00.asp

Tammam, A. (March 27, 2007). Why NAC Alone is Not Enough. Enterprise Systems. Retrieved on June 7, 2007, from http://www.esj.com/news/article.aspx?EditorialsID=2506

Thayer, R. (May, 2005). What is Network Policy Enforcement? InteropNet Labs Full Spectrum Security Initiative. Retrieved on May 23, 2007, from www.opus1.com/nac/whitepapers-old/06-**policy-enforcement**-lv05.pdf

Weaver, R. (2007). Guide to Network Defense and Countermeasures. Second Edition. Thomson Course Technology.

Whitman, M.E and Mattord, H.J. (2005). Principals of Information Security. Second Edition. Thomson Course Technology.

Young, J. (May 15/16, 2007). Secure VPNs: IPsec vs. SSL. Burton Group. Retrieved on June 30, 2007, from http://www.burtongroup.com/Client/Research/Download.aspx?cid=1145

Young, J. (June 6, 2006). Secure Site-to-Site VPNs: Real Privacy for Data Networks. Burton group. Retrieved on June 26, 2007, from http://www.burtongroup.com/Client/Research/Document.aspx?cid=389

9 Supplemental Material

Material in this chapter generally provides a more in-depth treatment of sections in the main document in order to provide the reader with additional clarity on aspects of network access control.

9.1 Network Access Control Frameworks

In this section a high level overview of the three NAC frameworks is presented. While not an exhaustive treatment of the subject, this nevertheless gives the reader some of the details pertinent to each framework.

9.1.1 Cisco's Network Admission Control

The Cisco Network Admission Control (CNAC) framework is the most comprehensive solution that is available today. All of the CNAC components are available either from Cisco or from one of its solution partners (Solution Profile, 2007).

A comprehensive implementation of CNAC includes multiple network systems, a NAC policy manager, one or more security posture validation servers, an audit server, a remediation server, and links to authentication stores. A broad number of endpoint security, audit, remediation servers, and secure access gateway vendors support Cisco NAC. All of these components represent a lot of moving parts that have to work together, which results in a great deal of infrastructure complexity. This can be one of the greatest challenges for any NAC implementation (Solution Profile, 2007).

The primary functions supported by the Cisco NAC Framework are (Solution Profile, 2007):

- Access to the network by a user is challenged with a authentication screen
- Device authentication using MAC addresses with a linkage to a user
- Quarantine device traffic to NAC-related (authentication, posture evaluation, and remediation) activities until authorization is completed
- Security policy compliance enforced by network- or agent-based scans
- Execute compliance checks on user and non-user devices (e.g. printers)
- Ability to use 3rd-party posture validation, audit, and remediation servers

- Use of quarantine LAN for non-compliant users who are notified of their status and action required to join trusted network and provide automatic remediation services
- Use of role-based policies to selectively control user access privileges

Cisco NAC requires that user and device authentication are performed with 802.1x Layer 2 LAN switches for either wired or wireless. However, this functionality is not available on Cisco Layer 3 switches, routers or VPN concentrators. The Cisco Layer 2 switches being produced today provide for this support, but older, installed Cisco switches do not. These will require an upgrade or replacement. In addition, an 802.1x supplicant must be installed on the endpoint and 802.1x support is required on the Layer 2 access switch for user authentication to take place (Solution Profile, 2007).

9.1.1.1 Client side

The IETF Network Access Requestor and Client Broker are contained in the Cisco Trust Agent. The posture collectors are vendor-supplied but Cisco does provide a host intrusion prevention functionality in its Cisco Secure Access (InteropLabs, 2006; Implementing Network Access Control – Cisco, 2005).

Policy Enforcement Points

Cisco's Network Access Devices are their policy enforcement points where access control enforcement uses VLAN separation (InteropLabs, 2006; Implementing Network Access Control – Cisco, 2005).

Policy Decision Points

ACS and vendor supplied policy servers, authentication servers, and audit servers provide the Policy Decision Point functionality. The ACS performs the role of Network Access Authority and Server Broker. Cisco's Policy Server Decision Points perform the role of Posture Verifiers and connects to ACS through Cisco proprietary protocols (InteropLabs, 2006; Implementing Network Access Control – Cisco, 2005).

To audit endpoint devices without the Cisco Trust agent installed, Cisco introduced an audit server, but it is still not clear how much useful information this will be able to collect (InteropLabs, 2006; Implementing Network Access Control – Cisco, 2005).

9.1.1.2 Operational Details

The key components in the Cisco NAC Framework are the Cisco Trust Agent (CTA), Posture Plug-In (PP), Network Access Device (NAD), Cisco Secure Access Control Server (ACS), and the Posture validation and remediation server (Implementing Network Access Control, 2005).

The endpoint hosts the CTA and PP. The PP provides the IETF functionality of Posture Collector. The posture collectors are vendor-supplied except for the Cisco Secure Access (Host Intrusion Prevention) posture collector (What is Cisco NAC, 2006). The CTA performs the role of IETF Client Broker and Network Access Authority. The PP communicates posture information to the CTA through a published Application Program Interface (API), and the CTA communicates posture information to the NAD (Implementing Network Access Control, 2005).

Cisco's NADs are their policy enforcement points where access control enforcement uses VLAN separation. Competitors maintain that an enterprise will have to replace all their switches with 802.1x compliant devices, but Cisco asserts that existing enterprise switches will work after a software upgrade (What is Cisco NAC, 2006).

NAD can be a NAC Layer 3 IP router or VPN, NAC Layer 2 IP switch, or NAC Layer 2 801.1x switch. Cisco supports both EAP-over-802.1x and EAP-over-UDP for endpoint communications. The former is used with 802.1x switches and the later when communicating through a VPN client or non-802.1x switches. With 802.1x, both authentication and endpoint posture information can be communicated; but with UDP only the posture information is available, authentication must be done in another system. As a result, endpoint access control is based on the endpoint posture, not the user credentials. Cisco has also defined a variation of EAP called EAP-FAST (Flexible Authentication via Secure Tunnel) to communicate both authentication and endpoint posture information. This is used with the L2 802.1x switch. The main thrust of the Cisco architecture at this time is for security posture verification. The Cisco Secure Access agent does not support wireless, which requires a different supplicant for that situation. Also a single enterprise policy server cannot be used when there is a mixture of 802.1x and UDP (What is Cisco NAC, 2006; NAC: Technical Overview, 2005).

The NAD sends the posture information or identity and posture information (802.1x) to the ACS which passes this on to the Posture Vendor Server (Policy Server Decision Point). The information is evaluated and then a

pass, fail, quarantine, or other posture response is forwarded through the ACS, NAD, and eventually to the client (Implementing Network Access Control, 2005).

ACS and vendor supplied policy servers, authentication servers, and audit servers provide the Policy Decision Point. The ACS performs the role of IETF Network Access Authority and Server Broker. Cisco's Policy Server Decision Points perform the role of Posture Verifiers and connects to ACS through Cisco proprietary protocols. To audit endpoint devices without the Cisco Trust Agent installed, Cisco uses an audit server, but how much useful information this will be able to collect is still an open question (What is Cisco NAC, 2006).

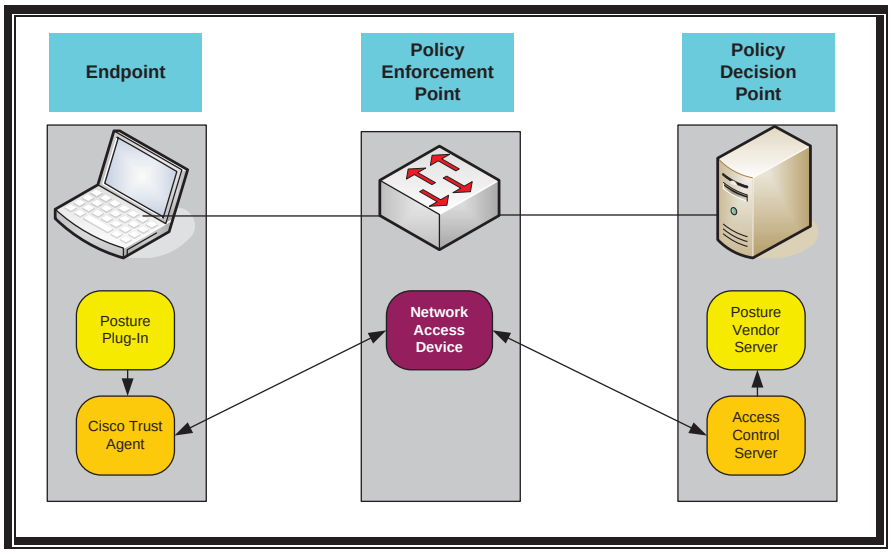


Figure 9-1 - Cisco NAC Process (Source: InteropLabs)

As can be seen in Figure 9-1 all the IETF framework basic functionality has been implemented but has been consolidated into fewer component parts. To better understand the actual operation, an example session describes a typical access request by an endpoint on a Cisco NAC network.

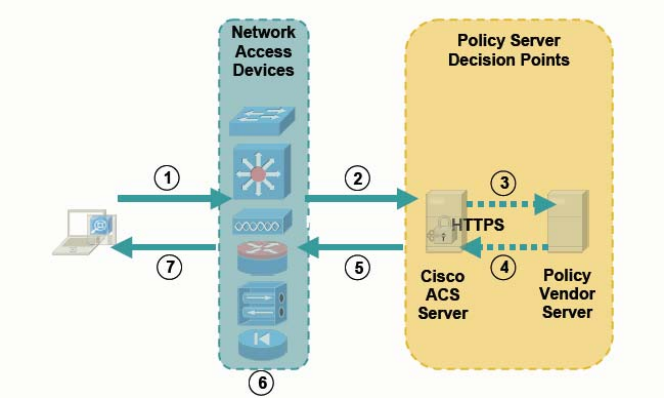


Figure 9-2 - Cisco Access Scenario (Source: Cisco Systems)

Figure 9-2 illustrates a typical access request session by an endpoint on CNAC.

1. The admission control process begins when the endpoint sends a network packet to the Network Access Device (Implementing Network Access Control, 2005; What is Cisco NAC, 2006).
2. The NAD starts the posture validation process. The Cisco Trust Agent (CTA) sends an identity of the endpoint to the NAD, which relays it to the Access Control Server (ACS). For non-802.1x sessions, the ACS then creates a Protected EAP (PEAP) session directly with CTA. PEAP requires a X.509 certificate. This certificate can be created from internal certificate authority (CA), if one exists, or the Cisco Secure ACS can generate a self-signed certificate. The CA certificate must be installed on the endpoint before requesting admission to the network. The CA certificate installation on the endpoint can occur automatically if the system is configured to do so. For 802.1x sessions, ACS uses EAP-FAST. The Posture Plug-In agents on the endpoint combine their information, which contains attributes that defines the current state of client software, with the CTA credential. This consolidated information is sent to the NAD, and then to ACS using EAPoRADIUS (Implementing Network Access Control, 2005; What is Cisco NAC, 2006).
3. ACS compares the received credential information against its policy database, or to an external server for validation. This external posture validator is used when the client software comes with an external validator. Communications between ACS and the external validator uses Host Credential Authorization Protocol (HCAP) over a HTTPS tunnel. Cisco's partners can provide an almost endless variety of posture checkers that can plug-in to CNAC Infrastructure. User authentication can be checked against a directory server (e.g. Active Directory). Posture validation can be anti-virus, anti-spyware, host intrusion detection system (HIDS), operating system patch levels, and application version control (Implementing Network Access Control, 2005; What is Cisco NAC, 2006).
4. The external posture validation server checks the received endpoint credentials and attributes against its internal policy database and sends a application posture token (APT) to the ACS. The APTs are collected from all internal and external validators and a system posture token (SPT) is

created. The SPT's value will be the value of the most restrictive APT (Implementing Network Access Control, 2005).

5. The value of the SPT dictates the network group membership of the endpoint. Each group has a specific set of access rights. Cisco categorizes the groups as Healthy, Checkup, Quarantine, Infected, or Unknown (Implementing Network Access Control, 2005; What is Cisco NAC, 2006; Network Admission Control, 2005).
    - **Healthy**: indicates that the endpoint has credentials that are current with the validator policies. For an anti-virus program this would mean that all signatures are up-to-date. No access restriction exists for the endpoint.
    - **Checkup**: indicates that some aspect of the validator is not current. For an anti-virus program, this would usually indicate that the signature files are out-of-date. This state may trigger an automatic update of the signature files. No access restriction exists for the endpoint.
    - **Quarantine**: indicates that some validator attribute requires immediate attention. The endpoint access control list (ACL) is changed to only allow access to a remediation server. This will effectively deny the endpoint access to any other network resource until the noncompliant condition is remedied.
    - **Infected**: a posture agent has detected a noncompliant condition, such as a virus infection, that must be resolved before allowing the endpoint on trusted network. Like the quarantine state, the endpoint is directed to a remediation server for any corrections.
    - **Unknown**: If an endpoint does not have CTA installed, is running an unsupported operating system, or is an IP device that does not support CNAC, the endpoint is normally assigned to this category. Access restrictions are enforced that are appropriate for the device.
6. NAD enforces policy based on rights assigned to client (Implementing Network Access Control, 2005; What is Cisco NAC, 2006).

7. Finally, the NAD sends the posture response to the endpoint. Endpoint is granted or denied access, redirected to a remediation server, or given limited access to resources. NAD will periodically check the endpoint to assess if its posture has changed or if the endpoint is different from the endpoint that was validated. If the endpoint does change state, or has been replaced by a different endpoint, the validation process is restarted. If no response is received during a validation session, then a restrictive policy is downloaded to the NAD that limits the network access of the endpoint (Implementing Network Access Control, 2005; What is Cisco NAC, 2006).

9.1.2 Microsoft's Network Access Protection

Microsoft Network Access Protection (NAP) provides components and an application programming interface in Vista and Windows XP SP2 that facilitate the enforcement of health (security posture) requirement policies for network access or communications. However, like the other NAC frameworks, NAP does not provide protection for the network against attacks from malicious users (Introduction to Network Access Protection, 2007).

The three distinct aspects of NAP are:

- **Health state validation**: Attempts by an endpoint device to access the network forces an evaluation of its health state against the current health requirement policies of the network. The NAP environment can be monitoring-only where any non-compliance is logged for later analysis, or non-compliant devices may have their access restricted. Compliant devices are allowed full access to the network.
- **Health policy compliance**: Endpoint device compliance can be ensured by forcing automatic updates or configuration changes on non-compliant systems. The NAP environment can be monitoring-only where any non-compliance is logged for later analysis, or non-compliant devices may have their access restricted until the endpoint device is compliant with health policies. For devices that are not NAP-capable, exceptions can be allowed in the health policies.
- **Limited access**: Access to network resources can be limited for non-compliant endpoint devices by either the amount of time allowed on the network or by the network resources that the non-compliant device can access (Introduction to Network Access Protection, 2007).

Health state can be examined on roaming laptops, desktop computers within an enterprise, visiting laptops, and unmanaged home computers (Introduction to Network Access Protection, 2007).

One of the primary differences between Microsoft and other NAC architectures is that NAP uses server enforcement instead of switch enforcement because Microsoft does not make switches or routers. The other major difference is that NAP is not a security system but is a system to identify and quarantine non-compliant endpoints on the enterprise LAN (What is Microsoft's Network Access Protection, 2006).

NAP provides the infrastructure components and an API that allows the creation of additional components that can evaluate an endpoint's health as well as enforcing network access and communications.

Figure 9-3 maps the Microsoft NAP terms into the IETF framework. Unlike CNAC, Microsoft NAP functionality is modularized in a similar way to the IETF functional modules.

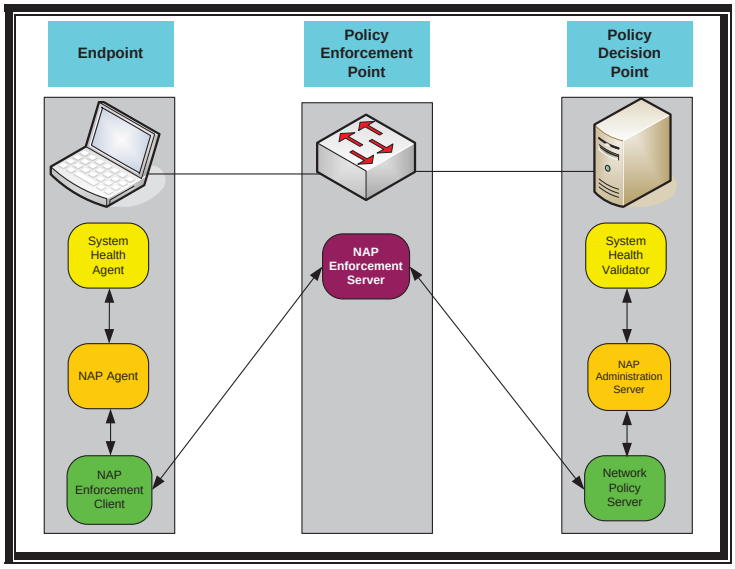


Figure 9-3 - Microsoft NAP Process (Source: Microsoft)

9.1.2.1 Client-side

The client is composed of System Health Agents, Network Access Protection Agent, and the Enforcement Clients. These can be used separately or together to limit non-compliant endpoint access or communications (What is Microsoft's Network Access Protection, 2006; Introduction to Network Access Protection, 2007).

Figure 9-4 shows the component parts of the NAP client architecture. This illustrates the multiple SHAs that are possible, as well as the different enforcement clients available.

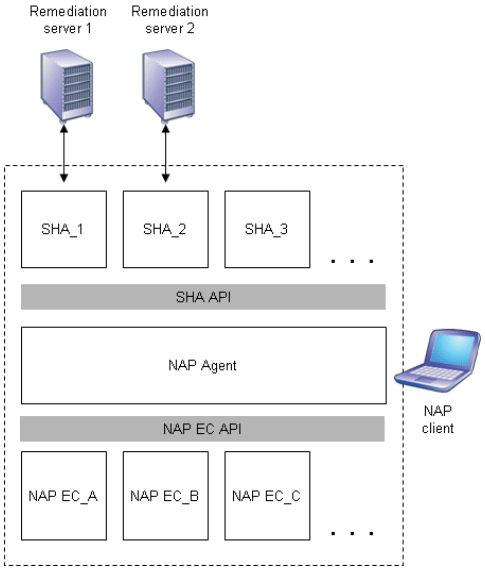


Figure 9-4 - NAP Client Architecture (Source: Microsoft)

System Health Agents (SHA) collects endpoint health information. These SHAs can be Microsoft supplied or from 3rd-party vendors. Microsoft provides a SHA that monitors the settings of the Windows Security Center (What is Microsoft's Network Access Protection, 2006; Introduction to Network Access Protection, 2007). Typically a SHA is matched to a specific System Health Validator (SHV) on the server side, but some are self-contained such as an SHA that ensures that the host-based firewall is enabled. A Statement of Health Response (SoHR) is provided by the SHV through the NAP EC and NAP Agent to the SHA. The SoHR indicates the actions the SHA must take to become compliant if it is not currently compliant. For example, a SoHR could direct an antivirus SHA to a specific anti-virus signature server for updates to its antivirus signature files (Network Access Protection Platform Architecture, 2007).

Network Access Protection Agent collects information from SHAs and facilitates communicates between the SHA and EC layers (What is Microsoft's Network Access Protection, 2006; Introduction to Network Access Protection, 2007; Network Access Protection Platform Architecture, 2007).

Enforcement Client (EC) enforces limited network access for non-compliant endpoint devices. The enforcement methods supported are Internet Protocol security (IPsec)-protected traffic, IEEE 802.1x-authenticated network connections, Remote access VPN connections, and Dynamic Host Configuration Protocol (DHCP) address configurations (What is Microsoft's Network Access Protection, 2006; Introduction to Network Access Protection,

2007). Microsoft provides the four ECs discussed here but third-party vendors also have the ability to create new ECs. An EC is normally matched with a specific NAP enforcement point such as DHCP EC with DHCP-based NAP enforcement point (Network Access Protection Platform Architecture, 2007).

Figure 9-5 summarizes the key information about each enforcement agent.

	IPsec-protected traffic	IEEE 802.1x-authenticated network connections	Remote access VPN connections	DHCP address configurations
Enforcement	Communications limited to compliant devices	Network access through 802.1x-authenticated network connection limited to complaint devices	Network access through remote access VPN connection limited to complaint devices	Only compliant devices can obtain an unlimited access IPv4 address from DHCP server
Components	Health Registration Authority and IPsec Enforcement Client	Network Policy Server and EAPHost Enforcement Client	Network Policy Server and VPN Enforcement Client	DHCP Enforcement Server and DHCP Enforcement Client
Method	X.509 certificates for compliant NAP clients. Used for IPsec-protected communications with other NAP clients.	Enforces health policies every time device attempts 802.1 x-authenticated network connection.	Enforces health policies every time device attempts remote access VPN connection.	Enforces health policies every time device attempts to lease or renew an IP address configuration.
Actively monitors NAP Client	No	Yes – applies restricted access profile to connection if client becomes non-compliant	Yes – applies IP packet filters for the restricted network to VPN connection if client becomes non-compliant	Yes - only renews for compliant devices.
Enforcement Strength	Strongest	Strong for all NAP clients accessing through an 802.1 x-authenticated network connection	Strong for all NAP clients accessing through a remote access VPN connection	Weakest because IPv4 address configuration can be overridden by a user

Figure 9-5 - NAP Enforcement Clients

Each SHA creates a Statement of Health (SoH) that reflects its specific health state. A SoH can include version information about the SHA and the date of its last update. This information is passed to the NAP Agent where SoHs from all SHAs are combined with the version of the NAP client into a System Statement of Health (SSoH) (Network Access Protection Platform Architecture, 2007).

9.1.2.2 Policy Enforcement

NAP Network Policy Server (NPS) is a Remote Authentication Dial-In User Service (RADIUS) server that provides authentication, authorization, and accounting (AAA) services for network access. Active Directory also verifies user or computer credentials, and provides device account properties for 802.1x-authenticated connection or a VPN connection (Introduction to Network Access Protection, 2007).

NAP will enforce network security policy by providing full access to an endpoint, no access, or limited access to a remediation service and quarantine network (What is Microsoft's Network Access Protection, 2006; Introduction to Network Access Protection, 2007).

9.1.2.3 Policy Decision Point

The NAP Server is composed of NAP Enforcement Server, NPS service, NAP Administration Server, and System Health Validator components (Network Access Protection Platform Architecture, 2007). This is shown in Figure 9-6.

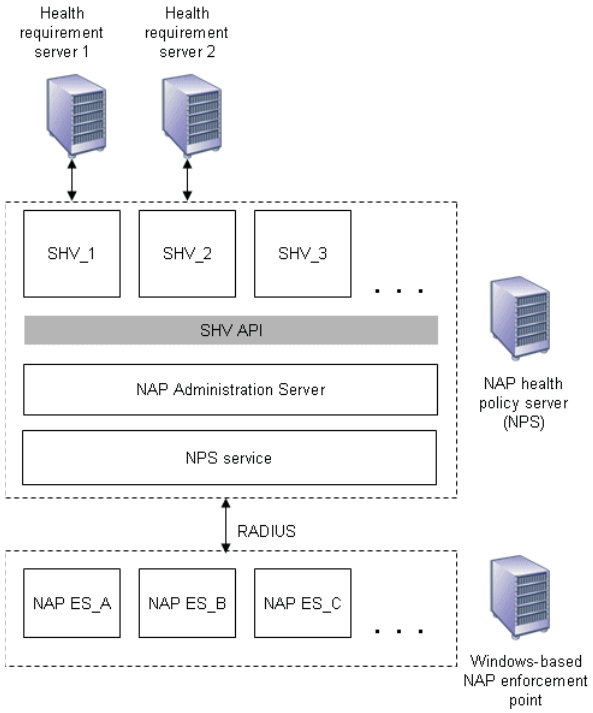


Figure 9-6 - NAP Server Architecture (Source: Microsoft)

NAP Enforcement Server (ES) facilitates the communications between NAP endpoint and NAP policy server, and in the case of a non-compliant NAP endpoint, can enforce limited network access. An IPsec NAP ES and a DHCP NAP ES are provided by Microsoft. Remote access VPN and 802.1x-authenticated connections use PEAP-TLV messages between NAP endpoints and the NAP health policy server. Enforcement for VPN and 802.1x network access device connections is accomplished by applying IP packet filters to the connection. In addition, a VLAN ID can be assigned to the 802.1x network access device to restrict network access (Network Access Protection Platform Architecture, 2007).

NPS service processes a RADIUS Access-Request message that contains the SSoH from the NAP endpoint, and passes this information to the NAP Administration Server. This service also aggregates the Statement of Health

Response (SoHR) from each SHV into a System Statement of Health Response (SSoHR) that indicates if the NAP endpoint device is compliant or non-compliant (Network Access Protection Platform Architecture, 2007).

NAP Administration Server is responsible for the following services (Network Access Protection Platform Architecture, 2007):

- Obtains the SSoH from the NAP ES by way of the NPS Service.
- SHV receive appropriate SoH that are in the SSoH.
- Aggregates the SoHRs from the various SHVs; conveys SoHRs to NPS service for examination.

System Health Validators (SHV) compares the SoH from a SHA against the required system health state. A Network Access Protection Administration server provides the SoH from the associated SHA to the SHVs. Using the antivirus example referred to earlier, the SHV will compare the antivirus file version in the SoH to determine if the latest antivirus signature files are being used on the NAP endpoint. As a result of this check, the SHV passes a SoHR to the NAP Administration Server that describes any remedial action that the SHA must take to become complaint (What is Microsoft's Network Access Protection, 2006; Introduction to Network Access Protection, 2007; Network Access Protection Platform Architecture, 2007).

Remediation actions bring a non-compliant endpoint device back into compliance. Remediation servers use a combination of servers, services, and other resources to update a non-compliant endpoint device so that it can be moved from a restricted network to the trusted network. For example, remediation for an endpoint device that does not contain the latest virus signatures would be to download the latest signatures to the device. The remediation server can communicate directly with the SHA or with the installed client software (Introduction to Network Access Protection, 2007).

NAP is unique among the NAC frameworks in that it uses a Web-based PKI server (Health Certificate Server) to create a digital certificate that can be used instead of a Statement of Health. The client proves it state of health by using System Health Agents and Statements of Health over HTTP/S connection and receives a digital certificate it can use at authentication time as a statement of health. This provides for a faster connection for the end user (What is Microsoft's Network Access Protection, 2006).

9.1.2.4 Operational Details

NAP can have many different interactions between the endpoint device, network devices, and servers of a NAP-enabled network. Figure 9-7 shows these interactions.

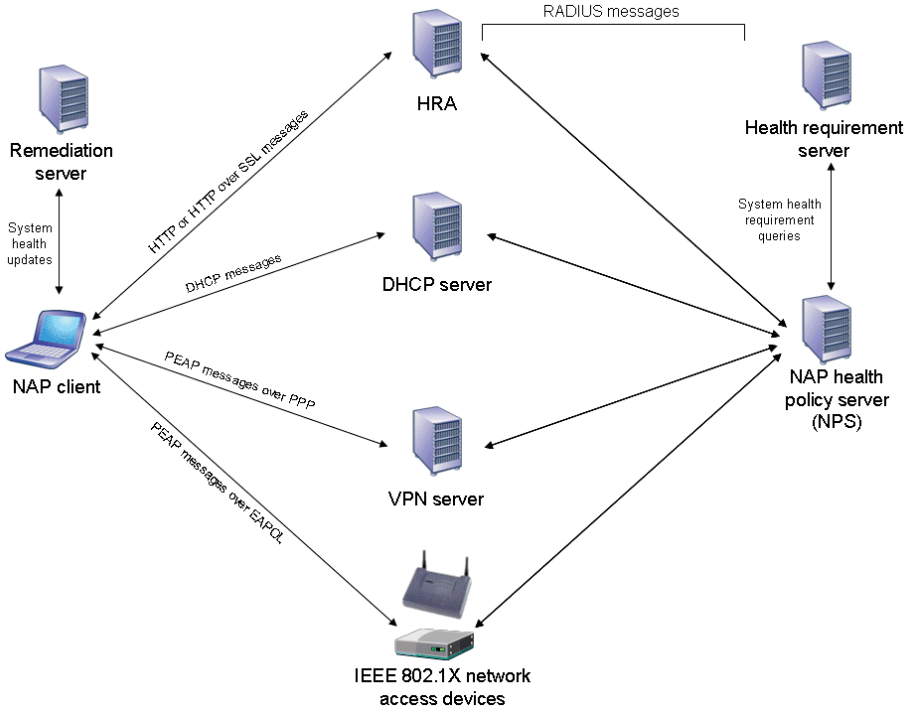


Figure 9-7 - NAP platform components interactions (Source: Microsoft)

The following brief descriptions illustrate these exchanges:

- **Between NAP client and an HRA**

The current system health state of the NAP client is sent to HRA using HTTP or HTTP over SSL protected session to request a health certificate. Remediation instructions or a health certificate is sent to the NAP client from the HRA (Network Access Protection Platform Architecture, 2007).

- **Between a NAP client and an 802.1x network access device**

PEAP messages sent over EAP over LAN (EAPOL) is used by a NAP client acting as a 802.1x supplicant to authenticate an 802.1x connection and communicate its system health state to NAP health policy server. Remediation instructions or authorization for unlimited network access is sent to the NAP client through an 802.1x network access device from the HRA (Network Access Protection Platform Architecture, 2007).

- **Between a NAP client and a VPN server**

Point-to-Point (PPP) messages are used by NAP client acting as a VPN client to establish a remote access VPN connection. The current health state is sent using PEAP messages over the PPP connection to the NAP health policy server. Remediation instructions or authorization for unlimited network access is sent to the NAP client using PEAP messages from the HRA. These messages are routed through the VPN server (Network Access Protection Platform Architecture, 2007).

- **Between a NAP client and a DHCP server**

DHCP messages are used by a NAP client acting as a DHCP client to obtain a valid IPv4 address configuration and to communicate its system health state to NAP health policy server. Remediation instructions are communicated using an IPv4 address configuration for the restricted network, or an IPv4 configuration for unlimited network access (Network Access Protection Platform Architecture, 2007).

- **Between a NAP client and a remediation server**

For NAP clients with unlimited intranet access, periodic communications are established with the remediation server to ensure that the NAP client is still compliant. Non-compliant NAP clients are allowed to communicate with the remediation server to become compliant. The NAP health policy server will instruct the NAP client as to what changes are needed to become compliant (Network Access Protection Platform Architecture, 2007).

- **Between an HRA and a NAP health policy server**

RADIUS messages are used to send the NAP client's system health state from the HRA to the NAP health policy server. The NAP health policy server responds with unlimited network access authorization or remediation instructions and authorization for limited network access. The HRA will issue a health certificate for unlimited network access and communicate the certificate to the compliant NAP client (Network Access Protection Platform Architecture, 2007).

- **Between an 802.1x network access device and a NAP health policy server**

PEAP messages from the NAP client acting as an 802.1x suppliant are sent from the 802.1x network access device using RADIUS messages. These messages from the NAP health policy server are used (1) to indicate that the NAP client has unlimited access, (2) that it has limited access, or (3) to send PEAP messages to the NAP client. Limited access for the NAP client is accomplished by a profile that consists of IP packet filters or a virtual LAN (VLAN) identifier. This confines the NAP client traffic to a restricted network until remediation is completed and the NAP client is compliant (Network Access Protection Platform Architecture, 2007).

- **Between a VPN server and a NAP health policy server**

PEAP messages from the NAP client acting as a VPN client are sent from the VPN server using RADIUS messages. These messages from the NAP health policy server are used (1) to indicate that the NAP client has unlimited access, (2) that it has limited access, or (3) to send PEAP messages to the NAP client. Limited access for the NAP client is accomplished by VPN connection IP packet filters (Network Access Protection Platform Architecture, 2007).

- **Between a DHCP server and a NAP health policy server**

RADIUS messages that contain the NAP client's health state are sent by the DHCP server to the NAP health policy server. These messages from the NAP health policy server are used (1) to indicate that the NAP client has unlimited access, or (2) that it has limited access (Network Access Protection Platform Architecture, 2007).

- **Between a NAP health policy server and health requirement server**

The NAP health policy server contacts a health requirement server to obtain the current requirements for system health. An example would be when the NAP health policy server contacts an antivirus server to determine the version of the most recent signature file (Network Access Protection Platform Architecture, 2007).

NAP has a great deal of flexibility in how the intranet is configured and will vary depending on an organization's network architecture. The remainder of this section discusses an example intranet that has been configured to support health state validation, health policy compliance, and a restricted network for non-compliant devices. All four methods of enforcement will be used on this example intranet: IPsec enforcement,

802.1x enforcement, VPN enforcement, and DHCP enforcement (Introduction to Network Access Protection, 2007). Figure 9-8 shows the various NAP-enabled components.

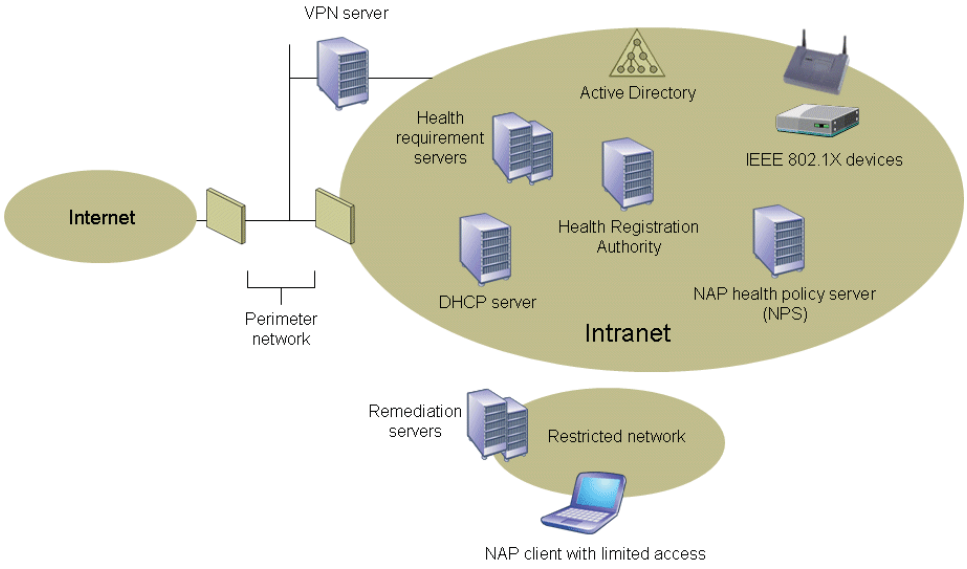


Figure 9-8 - NAP-enabled Components (Source: Microsoft)

For the purposes of the example, a NAP endpoint device is compliant when it meets all health policies and non-compliant when the device is deficient in one or more policies. Compliant devices are allowed unrestricted access on the intranet, and non-compliant devices are placed on a restricted network (Introduction to Network Access Protection, 2007).

The restricted network can be defined physically or logically by the use of filters, static routes, or a VLAN identifier. This information is stored on the endpoint device and will only provide connectivity to remediation servers (Introduction to Network Access Protection, 2007).

Since most intranets are typically a heterogeneous collection of endpoint devices, and there will be some devices on the network that cannot host the SHAs and enforcement clients, these can be exempted from health policy requirements. The exemption policy allows the device to operate on the unrestricted intranet (Introduction to Network Access Protection, 2007).

9.1.2.4.1 IPsec Enforcement

IPsec enforcement separates the physical network into three logical networks: secure, boundary, and restricted. The **secure network** contains endpoints and servers that must use health certificates for IPsec authentication. This will include most endpoints on a managed network that are members of the Active Directory domain. The **boundary network** contains endpoints and servers that have health certificates but that do not require other endpoints to have a health certificate for IPsec authentication. The **restricted network** includes endpoints that are not compliant, or running an operating system not supported by NAP and do not have a health certificate. Figure 9-9 graphically shows these three networks.

Information in this section was taken from Microsoft documents *Introduction to Network Access Protection* and Network *Access Protection Platform Architecture*.

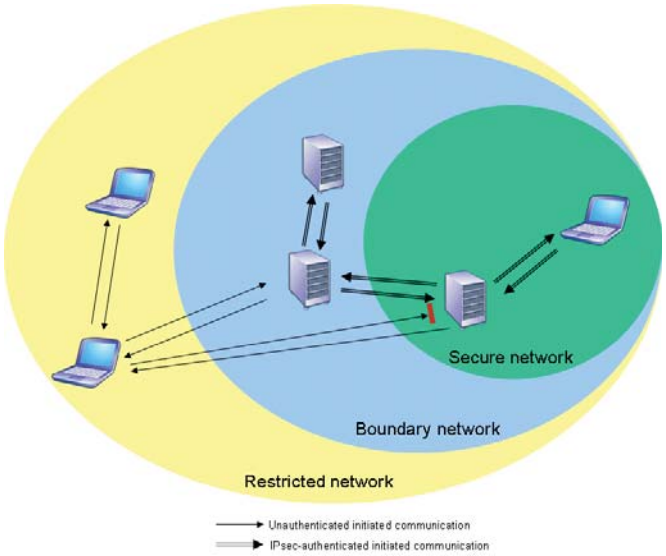


Figure 9-9 - IPsec enforcement logical networks (Source: Microsoft)

The IPsec enforcement process for an endpoint device requesting access on the example intranet is described in Figure 9-10.

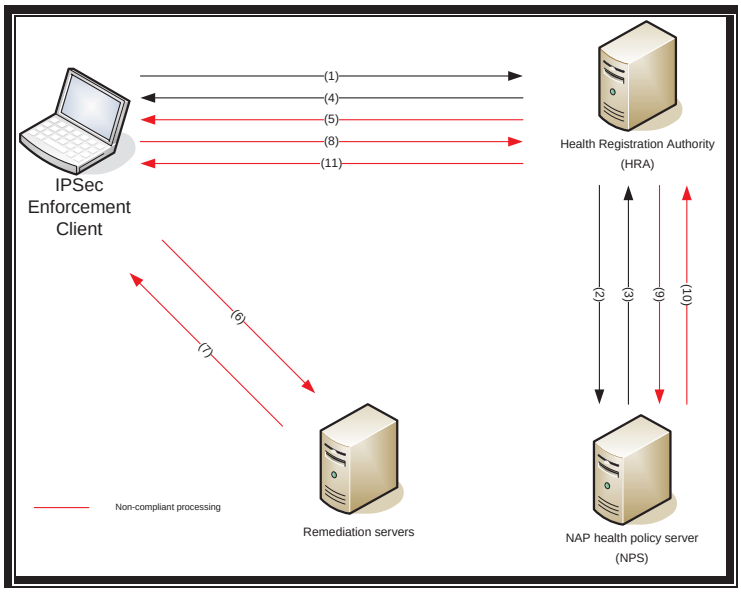


Figure 9-10 - How IPsec Enforcement Works

Compliant NAP endpoint

1. The IPsec EC on the endpoint device requesting access communicates its current health information to the HRA.
2. The HRA sends device health information to NAP health policy server
3. The NAP health policy server evaluates the system state of health information from the NAP endpoint to determine if the NAP endpoint is compliant. If it is, a system state of health response (SSoHR) is sent to the HRA. If the NAP endpoint is not compliant, remediation instructions are included in the response.
4. If the NAP endpoint is compliant, the HRA secures a health certificate for the NAP endpoint. The health certificate allows the endpoint to perform IPsec-protected communication with other compliant endpoints. The health certificate is used for IPsec authentication.

Non-compliant NAP endpoint

5. Remediation instructions are communicated to the NAP endpoint if it is not compliant. The NAP endpoint is restricted from initiating communications with other endpoints or servers that require a health certificate. However, this does not include the remediation servers.
6. Update requests are sent by the NAP endpoint to designated remediation servers.

7. The NAP endpoint is provisioned with the appropriate updates from the remediation servers to bring the NAP endpoint into compliance. These changes cause an update to the NAP endpoint health information.
8. Updated health information is sent from the NAP endpoint to the HRA.
9. The updated health information is sent by the HRA to the NAP health policy server.
10. If the NAP endpoint is now compliant, the NAP health policy server sends that result to the HRA.
11. The HRA secures a health certificate for the NAP endpoint. The health certificate is used for IPsec authentication and IPsec-protected communication with other compliant endpoints.

9.1.2.4.2 802.1x Enforcement

For 802.1x enforcement, the NAP endpoint's network traffic is controlled by a set of IP packet filters or a VLAN ID that restrict the NAP endpoint to resources on the restricted network until the NAP endpoint is verified compliant to the network health policies. For IP packet filtering, all other IP packets that do not conform to the configured packet filter are discarded by the 802.1x network enforcement device. For VLAN IDs, all packets exchanged between the NAP endpoint and the 802.1x network enforcement device have the VLAN ID applied to them, which prevents any of these packets from leaving the restricted network VLAN. Actual protocol sequences have been left out of the process description to facilitate clarity. The 802.1x enforcement access scenario is shown in Figure 9-11.

Information is this section was taken from Microsoft documents: *Introduction to Network Access Protection* and Network *Access Protection Platform Architecture*.

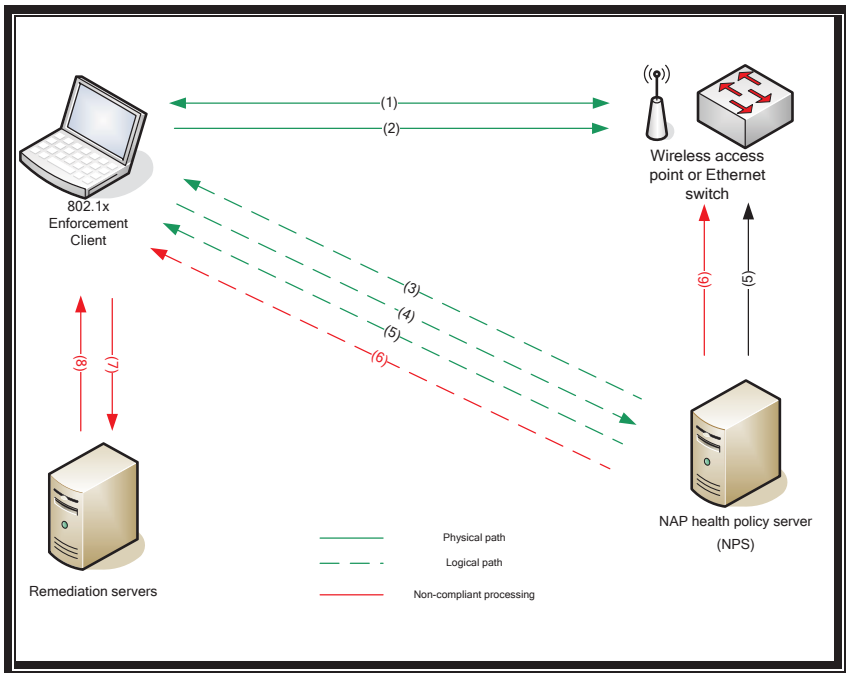


Figure 9-11 - How 802.1x Enforcement Works

Compliant NAP endpoint

1. Start 802.1x authentication sequence between NAP endpoint and 802.1x network enforcement device (Ethernet switch or wireless AP)
2. User or computer credentials sent by the NAP endpoint to NAP health policy server, which is also an AAA server.
3. Connection attempt is terminated if the authentication credentials are not valid; otherwise, the NAP health policy server requests the health state from the NAP endpoint.
4. NAP endpoint sends health state to NAP health policy server.
5. NAP health policy server evaluates the health state and sends the results to the 802.1x network enforcement device and NAP endpoint. The 802.1x network enforcement device completes the authentication and grants unlimited access to the NAP endpoint.

Non-compliant NAP endpoint

6. NAP health policy server sends results of evaluation with remediation instructions to NAP endpoint and a limited access profile to the 802.1x network enforcement device.

7. NAP endpoint requests updates from remediation servers.
8. Remediation server sends required updates for compliance to NAP endpoint, which updates its health state.
9. Access process restarts at step 1.

9.1.2.4.3 VPN Enforcement

For VPN enforcement, the NAP endpoint's network traffic is controlled by a set of IP packet filters that restrict the NAP endpoint to resources on the restricted network until the NAP endpoint is verified compliant to the network health policies. All other IP packets that do not conform to the configured packet filter are discarded by the VPN server. Actual protocol sequences have been left out of the process description to facilitate clarity. The VPN enforcement access scenario is shown in Figure 9-12.

Information is this section was taken from Microsoft documents: *Introduction to Network Access Protection* and Network *Access Protection Platform Architecture*.

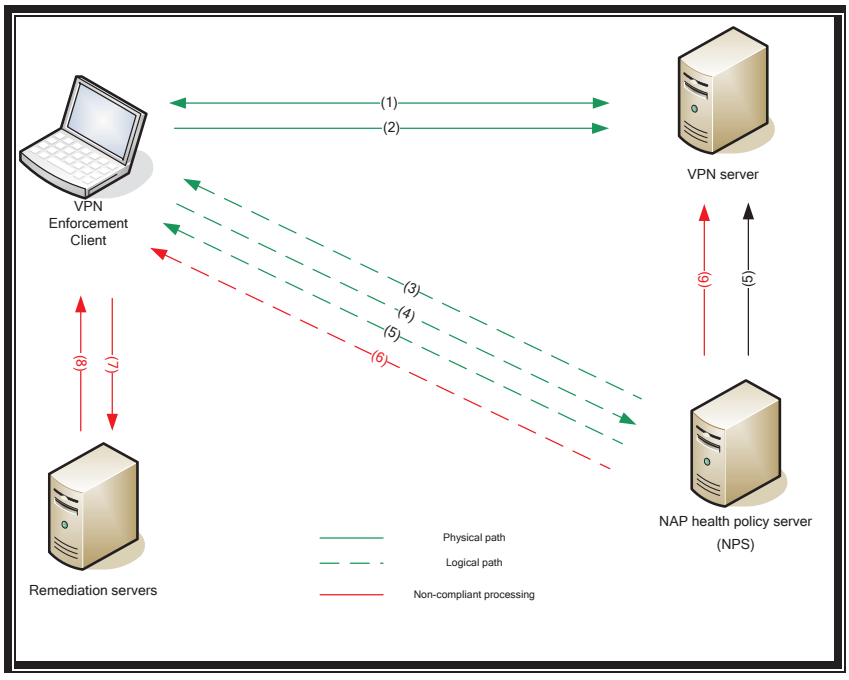


Figure 9-12 - How VPN Enforcement Works

Compliant NAP endpoint

1. A connection with the VPN server is initiated by the NAP endpoint.
2. User credentials from the NAP endpoint are sent to NAP health policy server, which is also an AAA server.
3. Connection attempt is terminated if the authentication credentials are not valid; otherwise, the NAP health policy server requests the health state from the NAP endpoint.
4. NAP endpoint sends health state to NAP health policy server.
5. NAP health policy server evaluates the health state and sends the results to the VPN server and NAP endpoint. The VPN server completes the authentication and grants unlimited intranet access to the NAP endpoint.

Non-compliant NAP endpoint

6. NAP health policy server sends results of evaluation with remediation instructions to NAP endpoint and a set of packet filters to the VPN server to restrict network access for NAP endpoint, which can only communicate with remediation servers.
7. NAP endpoint requests updates from remediation servers.
8. Remediation server sends required updates for compliance to NAP endpoint, which updates its health state.
9. Access process restarts at step 1.

9.1.2.4.4 DHCP Enforcement

Information is this section was taken from Microsoft documents: *Introduction to Network Access Protection* and Network *Access Protection Platform Architecture*. The IPv4 routing table is used for DHCP enforcement.

The following steps are taken for a non-compliant NAP endpoint:

- DHCP Router option value set to 0.0.0.0 (no default gateway)
- Subnet mask set to 255.255.255.255 (no route to attached subnet)
- Assign Classless Static Routes DHCP option (set of host routes to DNS and remediation servers on restricted network)

The NAP endpoint device is confined to the restricted network and any attempt to connect to an IP address other than those defined in the Classless Static Routes DHCP option will result in a routing error. It should be noted here that DHCP enforcement is only for IPv4 and does not apply to IPv6. The DHCP enforcement access scenario is shown in Figure 9-13.

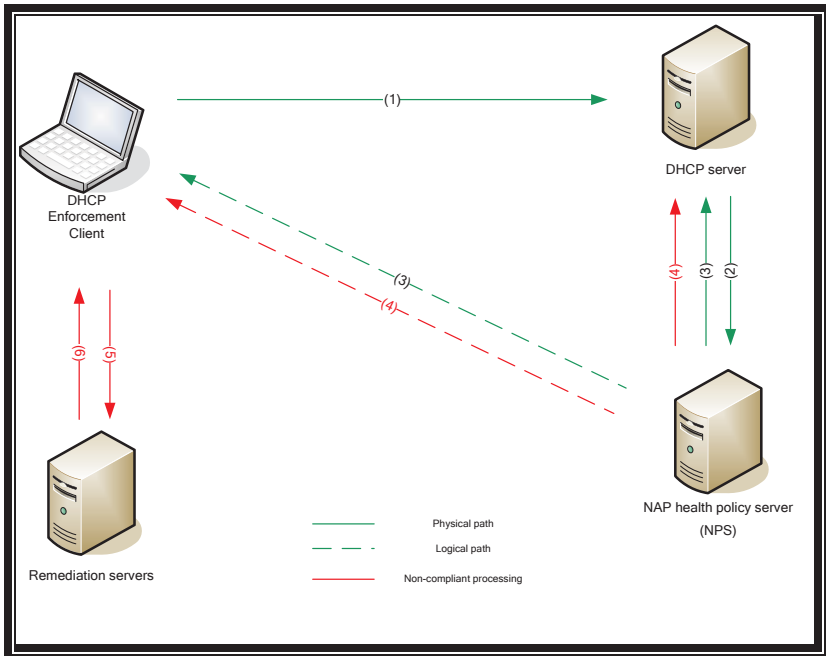


Figure 9-13 - How DHCP Enforcement Works

Compliant NAP endpoint

1. A DHCP request message with health state information is sent by the NAP endpoint to the DHCP server.
2. Health state information is sent to NAP health policy server by the DHCP server.
3. NAP health policy server evaluates the health state and sends the results to the DHCP server and NAP endpoint. For a compliant NAP endpoint, an IPv4 address configuration for unlimited network access is assigned to NAP endpoint by the DHCP server.

Non-compliant NAP endpoint

4. An IPv4 address configuration for restricted network access is assigned to NAP endpoint by the DHCP server and health remediation instructions are sent to NAP endpoint. The NAP endpoint can only communicate with the remediation servers on the restricted network.
5. NAP endpoint requests updates from remediation servers.

6. Remediation server sends required updates for compliance to NAP endpoint, which updates its health state.
7. Access process restarts at step 1.

9.1.3 TCG's Trusted Network Connect

The Trusted Computing Group's Trusted Network Connectivity (TNC), unlike the Cisco and Microsoft architectures, was designed by committee, and has at the time of this writing only been implemented by one large hardware vendor – Juniper Networks. According to the Juniper White Paper, *The Importance of Standards to Network Access Control*, "70 members [of the TCG] have participated in … the definition and specification of" TNC. The other unique aspect of the TNC is the optional use of the Trusted Platform Module (TPM).

The TPM is a hardware module typically located on the system's motherboard. Functionally it is similar to a SmartCard except that in addition to storing certificates and keys, it also can record the information about the state of the system. This state allows remote verification of the endpoint's hardware and software integrity. This provides a much more accurate and trustworthy evaluation of the endpoint than many other available solutions (The Importance of Standards, 2006). Microsoft currently uses the TPM in its Vista Secure Startup and BitLocker features to measure the pre-OS environment to determine if changes have occurred since the last system start up.

Trusted Network Connectivity (TNC) is concerned with the interoperability of network access control solutions, and the enhancement of security through the use of trusted computing. The security posture of an endpoint is determined through integrity measurements of hardware, firmware, software, and application settings. Based on these measurements an endpoint's suitability for joining the network is determined (Hanna, 2007).

TNC is concerned with "Platform-Authentication" which has two aspects. The first is proof of identity of the endpoint where this may or may not be related to a user's identity. This is accomplished by using a non-migratable key (e.g. Attestation Identity Key). The second aspect is integrity verification of the platform (Hanna, 2007).

The TNC architecture defines features that provide a framework to achieve a multi-vendor network standard that is interoperable. The key functionality is illustrated in Figure 9-14 (Hanna, 2007):

Platform-Authentication: verification of the endpoint identity and integrity.

Endpoint Policy Compliance (Authorization): ensures a desired state in the endpoint that establishes a level of 'trust' and network policy compliance.

Access Policy: authentication by an endpoint device and/or user and disclosure of an endpoint's security posture before access to the network is allowed.

Assessment, Isolation and Remediation: ability for a non-compliant endpoint to be isolated or quarantined from other compliant endpoints on the network, and to apply appropriate remediation to the endpoint.

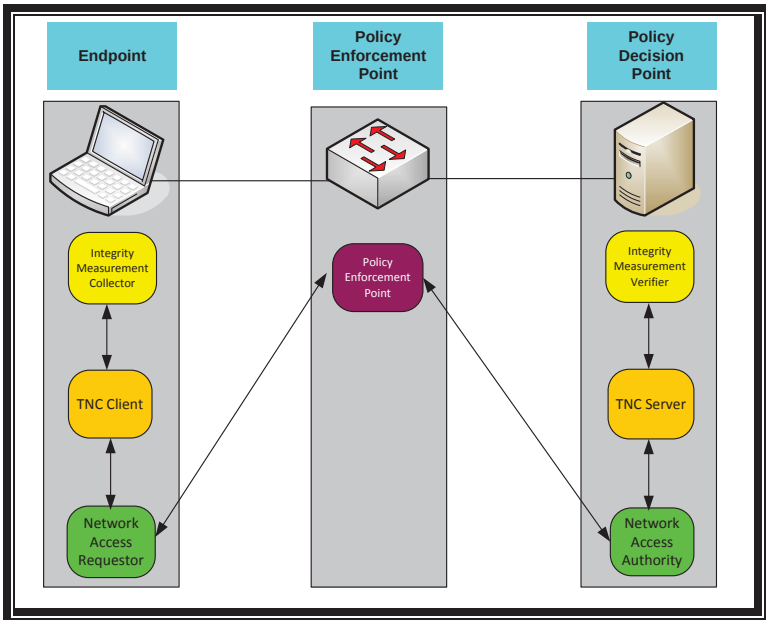


Figure 9-14 - TNC NAC Process (Source: Hanna)

As with the other architectures discussed, TNC has both vertical and horizontal relationships. Vertically there is the Access Requestor (AR), Policy Enforcement Point (PEP), and Policy Decision Point (PDP) (What is TCG's Trusted Network Connect, 2006, Hannah, 2007):

- **Access Requestor (AR)**: entity requesting access to network.
- **Policy Enforcement Point (PEP)**: enforces decisions by PDP for network access.
- **Policy Decision Point (PDP)**: evaluates the access request against the access policies grants or denies access.

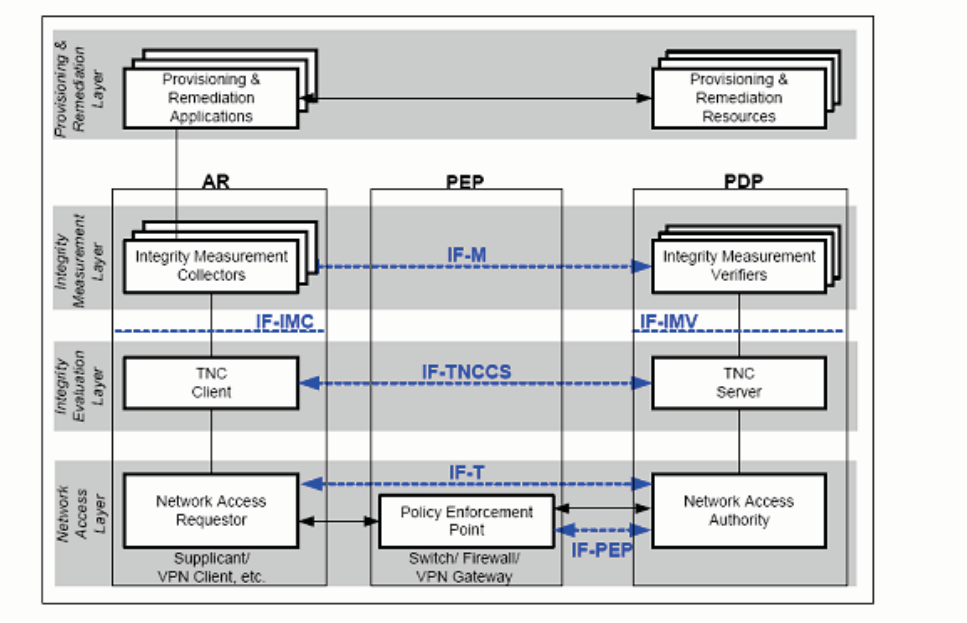


Figure 9-15 - TCG TNC Framework (Source: Hanna)

Horizontally three abstract layers group similar processing together (Hanna, 2007):

- **Network access layer**: Traditional network connectivity and security are defined at this level to support several different technologies like VPN, 802.1x, RADIUS, IPsec, EAP, and TLS/SSL. Network Access Requestor (NAR), Policy Enforcement Point (PEP), and Network Access Authority (NAA) are located at this layer.
- **Integrity evaluation layer**: Access Requestor integrity is evaluated against the access policies based on input from the integrity measurement layer.
- **Integrity measurement layer**: Security application plug-ins on the Access Requestor collects and verifies integrity-related information. Security verifiers on the PDP evaluate the integrity-related information.
- **Provisioning & Remediation Layer**: Applications, services, and other resources used to maintain an endpoint according to an organization's network access policies. The Provisioning and Remediation Application (PRA) may be implemented in several ways, but the goal is to bring the needed updates to the endpoint device through a connection to the Provisioning and

Remediation Resource (PRR). The PRR represents the source of integrity information that brings an endpoint into compliance. An example would be the latest anti-virus signature.

9.1.3.1 Client-side

Access Requestor executes on the endpoint and is divided into three parts: Network Access Requestor (NAR), TNC Client (TNCC), and Integrity Measurement Collectors (IMC).

- The NAR is software on the client that connects to network, requests access, and provides authentication. For 802.1x networks, NAR would be the 802.1x supplicant, and for IPsec VPN, the VPN client would have this function.
- IMCs evaluate the security posture of the client. Vendors will provide plug-ins to test if their part of the policy is in compliance.
- TNCC packages information from IMCs for the NAR that is sent to the PDP (What is TCG's Trusted Network Connect, 2006).

9.1.3.2 Policy Enforcement Point

The **Policy Enforcement Point (PEP)** enforces the network access control policy communicated to it from the PDP. This control is achieved through the configuration of the switch, firewall, or VPN that is performing the PEP function (What is TCG's Trusted Network Connect, 2006).

9.1.3.3 Policy Decision Point

The **Policy Decision Point** (PDP) is divided into three parts: Network Access Authority (NAA), TNC Server (TNCS), and Integrity Measurement Verifiers (IMV).

- NAA communicates to the authentication server and sends commands to PEP. NAA would normally be an AAA server such as RADIUS. An IMV is matched to an IMC on the Access Requestor.
- The IMC can communicate through a secure tunnel using a vendor-specific protocol and the results of the evaluation are passed to the PDP using a standard TCG protocol.

- TNCS provides an interface between the IMVs and NAA (What is TCG's Trusted Network Connect, 2006).

The TNC architecture relies on 802.1x authentication and tunneling mechanisms to get the various pieces to work. This becomes evident when 802.1 x terms are used in the diagram: NAR = 802.1x supplicant; PEP = 802.1x compatible switch or access point; NAA = 802.1x RADIUS server (What is TCG's Trusted Network Connect, 2006).

9.1.3.4 Operational Details

The Trusted Network Connect is composed of six protocols, but only two have been completely defined. The TNC specification was created in an open, vendor-neutral environment, making it a good basis for evaluating NAC. All existing NAC strategies can be mapped to the TNC but many vendors go beyond the current specification with the ability to control client firewalls, continuous checking of endpoint security, and functionality to handle guest devices accessing the network. (NAC Competition: Start with a little TCG, 2007).

Interfaces connect the logical components of the TCG TNC framework together, and protocols and messages are communicated between components using these interfaces. The following summarizes the purpose of each interface:

- **Integrity Measurement Collector Interface (IF-IMC)**: Software, firmware, and hardware components use this interface to communicate status information to the TNC Client component and then to the peer IMV through the TNC Server.
- **Integrity Measurement Verifier Interface (IF-IMV)**: This interface (1) communicates integrity measurements from the client-side IMCs to the peer IMVs, (2) enables message exchange between IMVs and IMCs, and (3) communicates remediation instructions from IMVs to IMCs.
- **TNC Client-Server Statement of Health Interface (IF-TNCCS-SOH)**: This interface defines a protocol between the TNC Client and TNC Server that communicates (1) IMC to IMV messages (e.g. integrity measurement batches), (2) IMV to IMC messages (e.g. remediation instructions or other requests), and (3) messages to manage the session between TNC Client and TNC Server. This interface was redefined in May, 2007 to facilitate the interoperability between TCG TNC and

Microsoft NAP. For Windows Vista and Windows XP systems, the NAP Agent will be used by TNC and NAP. Endpoint devices will be able to operate in either a TNC or NAP network.

- **Vendor-Specific IMC-IMV Messages (IF-M)**: These messages apply to vendor-specific information exchanges between the IMCs and IMVs.
- **Network Authorization Transport Protocol (IF-T)**: Transport of messages between the AR and the PDP.
- **Policy Enforcement Point Interface (IF-PEP)**: PDP to PEP communications that provides instructions for full or limited access for the endpoint device (Hanna, 2007).

The TCG TNC separates network access control into three phases.

- **Assessment**: Verification of the AR is performed by the IMVs based on the network access policies defined by the network administrator. If remediation is required, the instructions are communicated to the IMCs.
- **Isolation**: If the AR has failed the integrity-verification by the IMV, but has been authenticated and authorized for some level of access on the network, the PDP can instruct the PEP to redirect the AR to a restricted or isolation network where updates can be obtained to bring the AR into compliance.
- **Remediation**: This is the process where the AR receives updates to its current platform configuration and other policy-specific parameters. These changes bring the AR into compliance with the PDP's requirements for network access. Some examples have been mentioned previously: OS patches, anti-virus updates, etc (Hanna, 2007).

The following example network access scenario (graphically shown in Figure 9-16) involves **User Authentication** (is user authorized to access the network), **Platform Credential Authentication** (is the platform who it says it is), and **Integrity Check Handshake** (what is the security posture of the platform). This example flow was taken from *TCG Trusted Network Connect TNC Architecture for Interoperability* (Hanna, 2007).

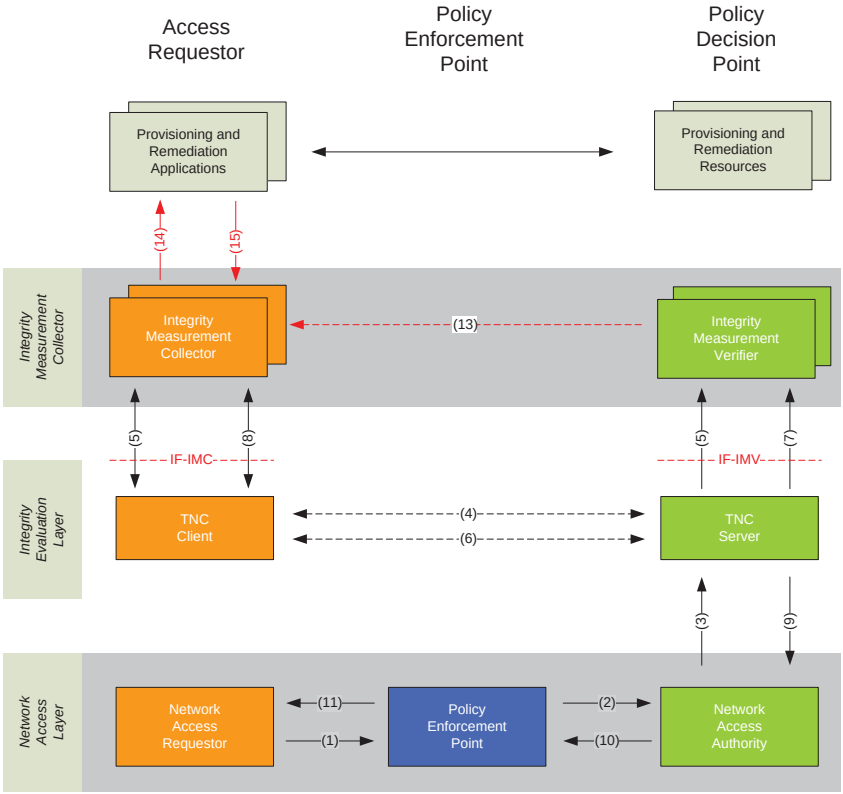


Figure 9-16 - TNC Authentication Message Flow (Source: Hanna)

Compliant TNC endpoint

1. Endpoint initiates a network connection request at the link and network layers.
2. NAA receives a network access decision request from the PEP.
    a. AR authenticates user to the NAA. If this fails, then the network access request is terminated.
3. NAA communicates connection request to TNCS.
4. TNCS performs **Platform Credential Authentication** with TNCC.
    a. This establishes the proof of identity for the platform. For a platform with a Trusted Platform Module (TPM), this could be valid Attestation Identity Key (AIK) credentials on the endpoint and server.
    b. If this fails, then the network access request is terminated.
5. TNCS communicates to IMV over the IF-IMV interface about the new connection request.
    a. On the AR the TNCC also communicates to the IMC that a new connection request has occurred.

   b. An **Integrity Check Handshake** request triggers several IMC-IMV messages between TNCC and IMCs across IF-IMC interface.

6. Integrity Check Handshake causes the exchange of integrity check messages between TNCC and TNCS. Logically these messages occur between the TNCC and TNCS but physically they are communicated through NAR, PEP, NAA, to TNCS. The messages continue until the AR integrity status has been fully verified.
7. TNCS passes the messages from IMC to its peer IMV through the IF-IMV interface. After analyzing the IMC messages, the IMV may exchange additional messages with the IMC.
   a. These may include remediation instructions for the IMC.
   b. The IMV may also communicate an IMV Action Recommendation or IMV Evaluation Result to the TNCS.
8. Messages from the IMVs are forwarded by the TNCC through the IF-IMC interface to the IMC.
9. A TNCS Action Recommendation is sent by the TNCS to the NAA once the Integrity Check Handshake has completed between the TNCC and TNCS.
   a. It is possible that if the AR has not met all security policy requirements but has passed the integrity check, the TNCS may still disallow access to the AR.
10. The network access decision is sent by the NAA to the PEP and to the TNCS.
    a. TNCS will communicate the decision to the TNCC.
11. PEP will typically indicate the decision execution to the NAR. An example would be that a port is open in 802.1x.

Non-compliant TNC endpoint

12. AR is placed on isolation network. This may entail using VLAN containment or IP Filters, which configures the PEP with the locations that the AR can access.
13. IMV sends results of evaluation with remediation instructions to IMC.
14. IMC requests remediation from Provisioning & Remediation Applications.

15. Remediation server sends required updates for compliance to IMC.

16. Access process restarts at step 1.

10 Annotated Bibliography

During the several months of research for this paper, I compiled several hundred pages of annotated bibliography. In order to keep this paper to a manageable length, I have only included a representative few in this section.

(13 Oct 2005). Network Access Control: Technical Overview. Cisco Systems, Inc. Retrieved on August 4, 2007, from http://www.cisco.com/application/pdf/en/us/guest/netsol/ns617/c664/cdccont_0900aecd80102f1b.pdf

The Cisco NAC Framework contains several key components. In the next Cisco graphic they have been divided into Subject (endpoints or NAC Clients), Enforcement (Network Access Devices), and Decision and Remediation (NAC Servers). From the left of the graphic, inputs are provided from devices on the LAN, WAN, or remotely. The access request is processed by the Enforcement section with the assistance of the Decision and Remediation section.

The endpoints will host the Cisco Trust Agent (CTA) and Posture Plug-In (PP). The CTA performs the role of IETF Client Broker and Network Access Authority. The PP provides the IETF functionality of Posture Collector. The PP communicates with the CTA through a published Application Program Interface (API), and the CTA communicates posture information to the Enforcement server.

The Network Access Device can provide different capabilities depending on the type of device used. For NAC Layer 3 IP routers and VPN, only EAPoUDP protocol is supported to communicate posture information only. This device also supports URL-Redirection, downloadable Access Control Lists (ACL), and posture status queries. NAC Layer 2 IP switches provides the same support as NAC Layer 3 IP with the exception that a NAC session is triggered by DHCP or ARP traffic, where as the NAC Layer 3 IP is triggered by a packet from the endpoint. Lastly, the NAC Layer 2 802.1x switch supports not only posture validation but also validates endpoint device identity, user identity, and VLAN assignment. EAP over 802.1x protocol is used instead of EAPoUDP. EAP-FAST is used for posture authorization.

Kelly, D. (October, 2005). Vulnerability Management. Burton GROUP. Retrieved on July 27, 2007, from http://www.burtongroup.com/Client/Research/Document.aspx?cid=714

Three types of scans are supported depending on the capabilities of the OOB (Kelly, 2005):

- **Uncredentialed scans**: Several different tests are performed on the endpoint by the OOB to determine if any open ports or services on the endpoint are vulnerable to known exploits.
- **Credentialed scans**: Performs the same type of external scan of the endpoint as the uncredentialed scan but will also examine details of the endpoint's system configuration by accessing the endpoint with administrator credentials.
- **Agent-based scans**: Agent software is installed on the endpoint to perform vulnerability assessment of the endpoint configuration, applications it is running, and any missing patches.

Blum, D. (May 9, 2007). VantagePoint 2007: Information Security Trends. Burton GROUP. Retrieved on June 7, 2007, from http://www.burtongroup.com/Client/Research/Document.aspx?cid=1078

For most large enterprises the single network perimeter has disappeared, and "re-perimerterization" is in progress with the ultimate goal of "de-perimeterization." These two terms have been coined by the Open Group Jericho Forum.

> *Members of the Forum recognize that over the next few years, as technology and business continue to align closer to an open, Internet-driven networked world, the current security mechanisms that protect business information will not scale to meet the increasing volumes of transactions and data of the future. A new*

approach is needed, to move from the traditional network perimeter down to the individual networked computers and devices—and ultimately to the level of the data being sent over the networks. This process has been described as "re-perimeterization" followed by ultimate "de-perimeterization" and Boundaryless Information Flow.

The trend toward mass collaboration with external business partners , outsourcing, and mobility are major factors in the erosion of the network perimeter. The trend is toward a greater dissolution of the boundaries but two factors will provide a counter-trend: cybercrime and regulatory compliance. The line between insiders and outsiders has blurred and security policy needs to reflect this.

In a web-based poll by the Burton Group, "[t]he single hard perimeter will be replaced by more effective distributed control points."

Re-perimeterization requires the deployment of more firewalls, intrusion detection services and devices, and other perimeter technologies. The protection is moving out to the ISPs and managed security providers (MSSP) that offer enterprise security services. These companies are doing more aggressive filtering of spam and malware as well as quarantining bots (compromised PCs) or limiting the effectiveness of distributed denial of service attacks.

These changes will occur slowly because boundaries will be needed around core areas like the data center, accounting departments, hospital floors, manufacturing lines, power plants, databases, military bases, and many other areas.

The enforcement of endpoint policies enables NAC to protect against vulnerabilities, but this will not be enough if a vulnerability exists but the patch to fix it isn't.

"Complexity is the enemy of security."

(May 29, 2007). 80% plan to enforce NAC in the network, says Infonetics in new study. Infonetics Research. Marketwire. Retrieved on June 2, 2007, from http://new.marketwire.com/2.0/rel.jsp?id=737569

Infonetics Research's study, "User Plans for Network Access Control: North America 2007," found that 80% of large organizations plan to enforce NAC in the network, and 51% plan enforcement at the client. Some will do both.

- The primary reason for NAC deployment is protection of corporate resources from unauthorized users and to limit impact from threats.
- 64% need to demonstrate policy compliance
- 54% need to demonstrate regulatory compliance
- 55% plan to use in-band NAC solutions
- In 2006, respondents spent 2/3 of their security budget on 802.1x-enabled switches

In summary, the study recommends that NAC vendors reduce cost on NAC products and provide a business case that appears to both corporate and technology buyers.

(25 April, 2007). Introduction to Network Access Protection. Microsoft Corporation. Retrieved on August 5, 2007, from http://www.microsoft.com/technet/network/nap/napoverview.mspx

Microsoft Network Access Protection (NAP) provides components and a application programming interface in Vista and Windows XP SP2 that facilitate the enforcement of health (security posture) requirement policies for network access or communications. However, NAP does not protect the network from malicious users.

The three distinct aspects of NAP are (1) health state validation, (2) health policy compliance, and (3) limited access.

- **Health state validation**: Attempts by an endpoint device to access the network forces an evaluation of its health state against the current health requirement policies of the network. The NAP environment can be monitoring-only where any non-compliance is logged for later analysis, or non-compliant devices may have their access restricted. Compliant devices are allowed full access of the network.
- **Health policy compliance**: Endpoint device compliance can be ensured by forcing automatic updates or configuration changes on non-compliant systems. The NAP environment can be monitoring-only where any non-compliance is logged for later analysis, or non-compliant devices may have their access restricted until the endpoint device is compliant with health policies. For devices that are not NAP-capable, exceptions can be allowed in the health policies.
- **Limited access**: Access to network resources can be limited for non-compliant endpoint devices by either the amount of time allowed on the network or by the network resources that the non-compliant device can access.

Health state can be examined on roaming laptops, desktop computers within a enterprise, visiting laptops, and the unmanaged home computers (Introduction to Network Access Protection, 2007).

NAP provides the infrastructure components and an API that allows the creation of additional components that can evaluate an endpoint device's health as well as enforcing network access and communications.

The client is composed of System Health Agents, Network Access Protection Agent, and the Enforcement Clients. These can be used separately or together to limit non-compliant device access or communications.

- **System Health Agents** collects endpoint health information. These SHAs can be Microsoft supplied or from 3rd-party vendors. Microsoft provides a SHA that monitors the settings of the Windows Security Center.
- **Network Access Protection Agent** collects information from SHAs.
- **Enforcement Clients** enforce limited network access for non-compliant endpoint devices. The enforcement methods supported are Internet Protocol security (IPSec)-protected traffic, IEEE 802.1x-authenticated network connections, Remote access VPN connections, and Dynamic Host Configuration Protocol (DHCP) address configurations.

Remediation actions will bring a non-compliant endpoint device back into compliance. Remediation servers use a combination of servers, services, and other resources to update a non-compliant endpoint device so that it can be moved from a restricted network to the trusted network. For example, remediation for a endpoint device that does not contain the latest virus signatures would be to download the latest signatures to the device. The remediation server can communicate directly with the SHA or with the installed client software.

(Nov, 2006). The Importance of Standards to Network Access Control. Juniper Networks. Retrieved on August 15, 2007 from http://www.juniper.net/solutions/literature/white_papers/200205.pdf

Trusted Network Connectivity (TNC) is concerned with the interoperability of network access control solutions, and the enhancement of security through the use of trusted computing. The security posture of an endpoint is determined through integrity measurements of hardware, firmware, software, and application settings. Based on these measurements an endpoint's suitability for joining the network is determined

(May 17, 2007). NAC Competition: Start with a little TCG. NetworkWorld. Retrieved on June 7, 2007, from http://www.networkworld.com/research/2006/040306-nac-tcg.html

The Trusted Network Connect is composed of six protocols, but only two have been completely defined. Specification created in an open, vendor-neutral environment, making it a good basis for evaluating NAC. All existing NAC strategies can be mapped to the TNC but many vendors go beyond the current specification with the ability to control client firewalls, continuous checking of endpoint security, and how to handle guest devices accessing the network.

TNC architecture is not complete enough to begin implementation.

(May, 2006). What is the IETF NAC strategy? Network Access Control Interoperability Labs. Retrieved on June 2, 2007, from http://www.interop.com/lasvegas/exhibition/interoplabs/nac/IETFNACstrategy.PDF

The Network Endpoint Assessment group of the Internet Engineering Task Force (IETF) is defining a standard set of protocols that will allow Cisco's Network Assessment Control, Microsoft's Network Access Protection, and TCG Trusted Network Connection to interoperate with each other.

Interface	Description
IF-PTT	Posture Transport Tunnel. EAP tunneling method used for authentication.
IF-PTC	Posture Transport Carrier. Protocol that carries EAP over 802.1x and EAP over RADIUS.
IF-PT	Posture Transport Interface. Composed of IF-PTT and IF-PTC.
IF-NAE	Network Access Enforcement interface. Defines the communications the Network Access Authority and the Network Enforcement Point and client. Typically RADIUS or DIAMETER.
IF-PB	Posture Broker Interface. Used to communicate posture information from the client broker to the server broker. Communicates the system posture result from the server broker to the client broker.
IF-PA	Posture Attribute interface. Communications between the Posture Collectors and Posture Validators. Passes collected posture information to Posture Validator, and returns the assessment results as well as remediation requirements.
IF-PV	Posture Validation interface. Communications between a Posture Validator and Server Broker.

(Mar, 2007). 802.1x: Port-Based Authentication Standard for Network Access Control (NAC). Juniper Networks. Retrieved on August 17, 2007 from http://www.juniper.net/solutions/literature/white_papers/200216.pdf

EAP over LAN (EAPoL) encapsulates EAP with an Ethernet header so that it can be transmitted over an Ethernet network. This is typically used on an 802.1x network between the Supplicant and Authenticator. A significant advantage of this protocol is the secure exchange of user and / or device credentials before an IP address is assigned. It operates at the Data Link or Layer 2 of the OSI model. Communications occurs between the supplicant and authenticator on an 802.1x network at the port level.

(May, 2006). What is 802.1x. Interop Labs. Retrieved on May 23, 2007, from http://www.interop.com/lasvegas/exhibition/interoplabs/nac/8021X.PDF

This article is a technical brief written for the 2006 Interop Labs conference. Explains that understanding 802.1x requires understanding: Extensible Authentication Protocol (EAP), IEEE 802.1x itself, and Tunneled Authentication.

EAP is part of PPP (point-to-point protocol) authentication protocol and is a framework for multiple authentication methods.

IEEE 802.1x establishes a standard for supporting EAP over a wired or wireless LAN by packaging it in Ethernet frames. For wireless, IEEE 802.1x establishes a method for the "access point and the wireless user to share and change encryption keys".

Three parties are involved in wireless or wired LAN authentication: supplicant, authenticator, and authentication server. The supplicant is the user or client requesting authentication. The authenticator is the device between the supplicant and authentication server. The authentication server performs the actual authentication (normally a RADIUS server). EAPOL (EAP encapsulation over LANs) is the protocol for 802.1x. NAC access is determined by the attributes returned from the Authentication server.

TTLS (Tunneled TLS) and PEAP (Protected EAP) are the two most important authentication protocols used for NAC and 802.1x. Both of these use certificates and TLS protocol. TLS (SSL) creates an encrypted tunnel between the server and client by authenticating the server side of the 802.1x transaction. The client uses the tunnel to send clear-text passwords, challenge-response passwords, or token-based authentication to authenticate to the server. NAC uses the tunnel to pass endpoint posture information between the client and authentication server.

CISO will also encapsulate EAP over UDP instead of Ethernet frames.

Howell, D. (May 31, 2007). Cisco, Microsoft, Others Get Together on Security. Investor's Business Daily. Retrieved on June 7, 2007, from http://www.investors.com/editorial/IBDArticles.asp?artsec=17&artnum=1&issue=20070531

NAC provides the most significant change to the way networks are secured since 1980s when firewalls emerged.

Infonetics Research: NAC enforcement manufacturer’s revenue is predicted to be $3.9 billion in 2008.

Cisco's Network Admission Control is different from TCG Trusted Network Connect. IETF may be able to address this.

Microsoft has commitment from more than 100 networking and security partners to support NAP. Windows Server 2008 will contain the NAP server. Microsoft currently has more than 100000 deployments of NAP on its own and partner networks.

Cisco has about 2,000 deployments of NAC currently.

OpenSEA (secure edge access) Alliance was formed to set a standard for the way vendor's products communicate with networks' NAC setups. Symantec, TippingPoint, Extreme Networks, Identity Engines, Infobox and Trapeze Networks are involved. This is based on 802.1x.

Andress, M. (30 July 2007). NAC alternatives hit the mark. NetworkWorld. Retrieved on August 19, 2007, from http://www.networkworld.com/reviews/2007/073007-test-nac-main.html?fsrc=rss-cisco

The basic form of NAC, as exemplified by the all-in-one appliances, appears ready for use by a large number of organizations. These products have proven themselves by being able to verify endpoint integrity and to control network access. According to an evaluation performed on thirteen NAC products by Network World, vendor's are investing large sums in research and development to make their products integrate seamlessly within the existing network infrastructures.