Final Thesis

Comparative Study of Network Access Control Technologies

By

Hasham Ud-Din Qazi

LITH-IDA-EX--07/028--SE

2007-05-11

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]

Linköpings universitet
Department of Computer and Information Science

Final Thesis

Comparative Study of Network Access Control Technologies

By

Hasham Ud-Din Qazi

LITH-IDA-EX--07/028--SE

2007-05-11

Supervisor: Prof. Dr. Christoph Schuba

Examinator: Prof. Dr. Christoph Schuba

Avdelning, institution
Division, department

Institutionen för datavetenskap

Department of Computer
and Information Science

Datum
Date

2007-05-11

Linköpings universitet

Språk
Language

- [ ] Svenska/Swedish
- [X] Engelska/English
- [ ] _____

Rapporttyp
Report category

- [ ] Licentiatavhandling
- [X] Examensarbete
- [ ] C-uppsats
- [ ] D-uppsats
- [ ] Övrig rapport

_____

ISBN —

ISRN LITH-IDA-EX--07/028--SE

Serietitel och serienummer
Title of series, numbering

ISSN —

URL för elektronisk version

http://www.ep.liu.se/

Titel
Title

Comparative Study of Network Access Control Technologies

Författare
Author

Hasham Ud-Din Qazi

Sammanfattning
Abstract

This thesis presents a comparative study of four Network Access Control (NAC) technologies; Trusted Network Connect by the Trusted Computing group, Juniper Networks, Inc.'s Unified Access Control, Microsoft Corp.'s Network Access Protection and Cisco Systems Inc.'s Network Admission Control. NAC is a vision, which utilizes existing solutions and new technologies to provide assurance that any device connecting to a network policy domain is authenticated and is subject to the network's policy enforcement. Non-compliant devices are isolated until they have been brought back to a complaint status. We compare the NAC technologies in terms of architectural and functional features they provide.

There is a race of NAC solutions in the marketplace, each claiming their own definition and terminology, making it difficult for customers to adopt such a solution, resulting in much uncertainty. The NAC paradigm can be classified into two categories: the first category embraces open standards; the second follows proprietary standards. By selecting these architectures, we cover a representative set of proprietary and open standards-based NAC technologies.

This study concludes that there is a great need for standardization and interoperability of NAC components and that the four major solution proposals that we studied fall short of the desired interoperability. With standards, customers have the choice to adopt solution components from different vendors, selecting, what is commonly referred to as the best of breed. One example for a standard technology that all four NAC technologies that we studied did adopt is the IEEE's 802.1X port-based access control technology. It is used to control endpoint device access to the network.

One shortcoming that most NAC architectures (with the exception of Trusted Network Connect) have in common, is the lack of a strong root-of-trust. Without it, clients' compliance measurements cannot be trusted by the policy server whose task is to assess each client's policy compliance.

Nyckelord
Keywords

Network Access Control, Network Admission Control, Unified Access Control, Trusted Network Connect, Network Access Protection, The Trusted Computing Group, Trusted Platform Module, Posture Assessment, Endpoint security, compliance, Cisco, Microsoft, Juniper Networks, root of trust, Platform Authentication.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]

To my dear parents,

Badar ud-din Qazi and Shehnaz Badar,

and my homeland "Pakistan"!

ABSTRACT

This thesis presents a comparative study of four Network Access Control (NAC) technologies; *Trusted Network Connect* by the Trusted Computing group, Juniper Networks, Inc.'s *Unified Access Control,* Microsoft Corp.'s *Network Access Protection,* and Cisco Systems Inc.'s *Network Admission Control*. NAC is a vision, which utilizes existing solutions and new technologies to provide assurance that any device connecting to a network policy domain is authenticated and is subject to the network's policy enforcement. Non-compliant devices are isolated until they have been brought back to a complaint status. We compare the NAC technologies in terms of architectural and functional features they provide.

There is a race of NAC solutions in the marketplace, each claiming their own definition and terminology, making it difficult for customers to adopt such a solution, resulting in much uncertainty. The NAC paradigm can be classified into two categories: the first category embraces open standards; the second follows proprietary standards. By selecting these architectures, we cover a representative set of proprietary and open standards-based NAC technologies.

This study concludes that there is a great need for standardization and interoperability of NAC components and that the four major solution proposals that we studied fall short of the desired interoperability. With standards, customers have the choice to adopt solution components from different vendors, selecting, what is commonly referred to as the *best of breed*. One example for a standard technology that all four NAC technologies that we studied did adopt is the IEEE's 802.1X port-based access control technology. It is used to control endpoint device access to the network.

One shortcoming that most NAC architectures (with the exception of *Trusted Network Connect*) have in common, is the lack of a strong *root-of-trust*. Without it, clients' compliance measurements cannot be trusted by the policy server whose task is to assess each client's policy compliance.

ACKNOWLEDGEMENTS

First of all, I would like to thank ALLAH(God), without His will this thesis was not possible at all. His will lead me to its completion. May I keep on submitting to Him, as ALLAH guides those, who He wills.

I would like to show my gratitude to Mr. Christoph Schuba, a teacher, a supervisor, and a good friend. He is one of those people whom you talk to, and you believe that nothing is impossible, everything is possible. Whenever I was lost, he helped me, and showed me a vivid direction. I enjoyed the conversation we shared, his professional experiences, loads of sarcastic humor, and jokes, was very pleasant indeed. May God bless him and his family.

Lastly, I would like to thank my family and friends (especially Atif and Masroor) in Pakistan and Sweden, for their continuous support, which always helps me directly or indirectly, I value it a lot.

Also, I am grateful to the Swedish education system, for giving me an opportunity to learn at Linköping University, not just formal education but also ethics of life from the people of Sweden, which are very valuable to me. I was inspired and the experience helped in changing my perspective towards life.

Table of Contents

1 Introduction 1

1.1 Computing Trends 1
1.2 Network security at stake 3
1.3 Impact of Malware 4
1.4 Network Access Control 6
1.5 Editorial Comments 7

2 Problem Statement 9

2.1 Motivation 9
2.2 Research Definition 10

3 Network Access Control 13

3.1 Definition 13
3.2 NAC Functions 13
3.2.1 Node Detection 14
3.2.2 Authentication 16
3.2.3 Posture Assessment 16
3.2.4 Authorization 17
3.2.5 Policy Enforcement 18
3.2.6 Quarantine 19
3.2.7 Remediation 19
3.2.8 Post-Admission Control 20
3.3 NAC Components 20
3.3.1 Client 20
3.3.2 Enforcement Points 22
3.3.3 Policy Servers 25
3.3.4 Quarantine Network 25
3.3.3 Remediation Servers 26
3.4 NAC Flow 26

4 Trusted Network Connect by the Trusted Computing Group 29

4.1 Background 31

4.2 Trusted Network Connect 31
4.2.1 Introduction 31
4.2.2 Components of TNC 34
4.2.3 Architecture of TNC 36
4.2.4 Interfaces of TNC 38

5 Unified Access Control by Juniper Networks, Inc. 41

5.1 Background 41
5.2 Unified Access Control 42
5.2.1 Introduction 42
5.2.2 Architecture and Components of TNC 44
5.2.3 Interoperability Initiative 47

6 Network Access Protection by Microsoft Corp. 49

6.1 Background 49
6.2 Network Access Protection 50
6.2.1 Introduction 50
6.2.2 Architecture and Components of NAP 51

7 Network Admission Control by Cisco Systems Inc. 61

7.1 Background 61
7.2 Network Admission Control 62
7.2.1 Introduction 62
7.2.2 Cisco NAC Appliance 63
7.2.3 Cisco NAC Framework 65
7.2.3.1 Components of Network Admission Control Framework 65

8 Analysis and Comparison of NAC Technologies 71

8.1 Comparison Overview 72
8.2 Issues in NAC 75
8.2.1 Architectural Setup 75
8.2.2 Vendor Lock-In and Interoperability 77
8.2.3 802.1X Port-based Access Control 78
8.2.4 Post-Admission Control 80
8.2.5 Automatic Remediation 80
8.2.6 Cross Platform Support 81

8.2.7 Unmanaged Clients (Exceptions) 81
8.2.8 Posture Spoofing 82
8.2.9 What if NAC fails? 83
8.2.10 Unified Policy 83

9 Conclusions and Future Work 85

Bibliography 89

Appendices 95

Appendix A: Glossary of Terms.....95

List of Figures and Tables

FIGURE

1.1 Timeline of security solutions 3
3.1 Levels of enforcement 24
3.2 Basic message flow in a NAC paradigm 27
4.1 Components of TNC 34
4.2 Architecture of TNC 37
5.1 Infranet Controller with 802.1X enabled switch 43
5.2 Unified Access Control architecture and components 45
5.3 UAC architecture in terms of TCG's TNC 47
6.1 Network Access Protection architecture 53
6.2 NAP client sub-components 54
6.3 IPSec divisions 57
6.4 NPS sub-components 58
6.5 Communication between NPS and NAP servers 60
7.1 Core components of NAC Appliance 64
7.2 Core components of NAC Framework 66
7.3 Cisco Trust Agent architecture 67

TABLE

8.1 Comparison overview of architectural elements 73
8.2 Comparison overview of functional elements 74

1 Introduction

1.1 Computing Trends

Traditional network security places an emphasis on the protection of network perimeter. The number of repeated vulnerabilities is ever growing and new type of attacks can impersonate authenticated users and legitimate traffic. Network security lacks focus on endpoint devices connecting to the network policy domain. The compliance level of endpoint devices is not taken into account, which makes the network unaware of the compliance of endpoints. These endpoints may carry malware software, e.g., embedded in software distributed via peer-to-peer file sharing software packages, such as; Kazaa, Limewire, or any messaging software, etc.

Non-compliant machines are threat to business critical network assets. Osterman research referenced in article [3] states that, in 2004, 90% of organizations had employees using at least one of the chat-messaging software. It is not safe to assume that people connected on the Local Area Network (LAN) are trusted enterprise citizens. These users are present inside the network perimeter, working on managed desktop PCs. A survey of security professionals conducted by CSI/FBI shows that half of the attacks on enterprise networks start from inside [5].

The usage of mobile devices has affected the nature of computing by introducing innovation and standards such as Mobile IP, Virtual Private Networks (VPN), etc. There is an increase recorded in the adoption of mobile devices, mobile IP-

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 17 of 114

devices such as laptop computers, Personal Digital Assistants (PDA), tablet personal computers, smart phones, etc. With such popularity and adoption of mobile devices, the work model of companies is built around the idea of mobility.

With the privilege of mobility, employees can contribute by working at home and still being connected to their corporate network. Scenarios such as working in hotels, or wi-fi (wireless) spots available at airports, railway stations, cafes, affects and enhance the productivity of an organization. The popularity of mobility opens a new horizon for security concerns. With mobility, a mobile device may connect to a number of networks, every network may have different security requirements. There is a great probability that such mobile device may get compromised due to its weak protection against malicious software.

According to Gartner, Inc. [8], the major trend in computer purchase and usage has shifted to mobile devices and notebooks and makes up about 29% of computers sold in the United States of America and 31% of those sold worldwide. These figures are not only limited to laptops as a choice of computer but more and more IP-enabled devices are prevailing in, e.g., the increase adoption and usage of devices such as PDAs and mobile phones.

The widespread popularity and adoption of broadband and wireless networking has made mobile computing a standard. As computing trends move to a new working model, it also affects and jeopardizes the network security of an organization. This has created great challenges for IT and security industry for controlling and managing the access to resources of a corporate network.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 18 of 114

1.2 Network Security at Stake

As technology advances, the paradigm towards computer security also changes. There is a continuous cycle of exploitation and compromise of security technologies. Whenever a security solution is invented, eventually it is preceded by its exploit, e.g., the BlackHat community discovers vulnerabilities and display exploitation of these vulnerabilities in their conferences.

Controlling the devices accessing the network resources has progressively become more problematic. Figure 1.1, illustrates a time line of different security solutions available till now. If we go back in time, during the Microsoft-DOS era, the exchange of data through floppy disk drives was casual and carried great

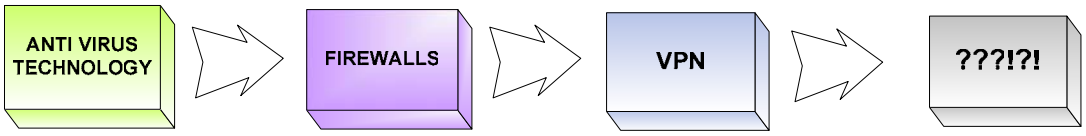

Figure 1.1 Timeline of security solutions

importance at that time. As it was the only standard to exchange data those days. Such method enabled a way for virus to break-in and spread from one computer to another. This created a need for an antivirus solution.

Likewise, when the concept of computer networks prevailed, that time demanded control of data flow at the perimeter of network, protecting network from outside intrusion. Thus firewall technology came into picture. A firewall creates a boundary around the trusted network separating it from other external networks

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 19 of 114

and thus monitoring the access to the network and corporate resources from unknown and unauthorized sources. Similarly, when Virtual Private Network (VPN) technology was introduced, there was great need of remote-access to corporate network through an inexpensive solution. The confidentiality and integrity of data was at stake, at that time the situation was handled through standards such as IP-Security (IPSec) and Secure Socket Layer (SSL)-based VPN.

Mobility makes the notation of *office* and *personal computer* indistinct. Complications arise when machines connect to various networks, protected and unprotected, and then connect back to their corporate networks. There is a high probability that such machines may be infected by some malware and thus are potential of infections that can spread within a corporate network. As users connecting to the corporate network have various different roles, as regular employees, as contractors, as guest users, as co-company employees, these scenarios create a constant threat to the protected network. A unified mechanism is required where it can be assured that any device connecting to the corporate network domain adopts the security policy.

1.3 Impact of Malware

There is a great increase in number of various attacks, malware such as viruses, worms, spyware, rootkits, backdoors, botnets, etc., having 35,000 different variations. Such massive growth in malware has infected more than 4,000,000 machines today [23]. A great deal of damage is done through these infections. Such loss can be categorized as following:

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 20 of 114

- When attacks occur, a corporation goes through a substantial amount of ***financial loss***. There is great delay in work process that might result in getting behind deadlines, decrease in company's revenue, etc., all sums up to financial loss.

- Such infections may also result in ***productivity loss***, as they hinder the work flow that might result in decline of productivity. As company's resources are compromised and consumed by such attacks.

- It takes a great amount of time for corporations to recover from infections to a compliant state. This includes ***recovery loss.*** As repairing and patching up of compromised systems consumes extra cost.

- Most importantly, compromise of security causes ***loss of reputation.*** Maintaining a high-profile of an organization is very pivotal. High level goals are built around it. If such loss occurs, the company is exposed in the media and hence the reputation of an organization is on stake.

PandaLabs (*a company having expertise in virus and intrusion prevention*) concluded in their research that there is an increase in new variants of malware categories, e.g., from 2005 to 2006, 57.6% of increase in new variants of Trojan is recorded, more than half of the new malware that appeared in 2006, pertained to this category. This was notable as compared to other categories of malware. Till 2007, such variants will increase up to 66.7% [18]. Malware is increasing every day there is a requirement of a unified access control mechanism.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 21 of 114

1.4 Network Access Control

Security products often have been quite tactical in nature, solving specific problems very well. Information Security is challenging in context of compliance of scenarios such as regular employees, remote users, telecommuters, guest users, etc. These usage scenarios affect the context of network security. Hence such endpoint devices, presents various paths for malware to penetrate, and such penetration becomes more trivial due to major reasons such as:

- *Out of date virus definitions*
- *Unpatched operating systems*
- *Defective configurations of firewall*
- *Out of date signatures for intrusion prevention*
- *Out of date security products*
- *Infected machines*

From the previous discussion in this chapter, it can be concluded that computer security is at stake, there is a requirement of a new security infrastructure that can control the access of endpoint devices connecting to the network, and by assuring that every endpoint device whether local or remote, complies with the corporate security requirements.

There is a requirement of a solution that protects the network security proactively rather than detection and recovery. Authentication of users is already present, but verifying the compliance level of a machine against corporate policy is not a common practice, which is very pivotal. As these machines are the potential sources for malware carrier and can compromise corporate resources.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 22 of 114

We defined Network Access Control as following:

"*Network access control is a vision, which utilizes existing solutions and new technologies to provide assurance that any device connecting to a network policy domain is authenticated, and is subject to the network's policy enforcement. Non-compliant devices are isolated until they have been brought back to a complaint status*".

1.5 Editorial Comments

In the printed copy of this thesis, the figures are likely to appear in grayscale. An electronic copy of this thesis, which contains these figures in high resolution and colored format, can be found at *http://www.ep.liu.se*.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 23 of 114

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 24 of 114

2 Problem Statement

2.1 Motivation

By the end of 2006, a number of companies and organizations have been creating their own Network Access Control (NAC) solutions. According to each of them, the solution they offer is complete. There is a race of such NAC solutions in the marketplace, claiming their own definition and terminology, making it difficult for the customers to evaluate and adopt such a solution, resulting in much uncertainty.

The NAC paradigm can be classified into two categories. The first category embraces open standards while the second follows proprietary standards. Although, considered amount of work has been put into creating NAC technology. The technology is still in early stages. While the need for NAC was generally realized by 2002, even by the end of 2006 there is no complete standardization of its unified vision. Every solution is confined to its vendor, lacking the incentive of a multi-vendor interoperable solution. Standardization of NAC architecture plays an important role and is the key to its success.

Forrester Research presents a timeline in [21], claiming that NAC solutions will converge to interoperability by 2008. It remains to be seen how accurate this prediction will turn out to be.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 25 of 114

2.2 Research Definition

This thesis presents a comparative study of the following four NAC technologies:

- *Trusted Network Connect* by the Trusted Computing Group.
- *Unified Access Control* by Juniper Networks, Inc.
- *Network Access Protection* by Microsoft Corp.
- *Network Admission Control* by Cisco Systems Inc.

The motivation for selecting these technologies is that, Cisco Systems Inc., Microsoft Corp., and the Trusted Computing Group are competitors of NAC architectures in the market place. Conover presents in [11] the results polled by 303 respondents, majority of the respondents confirmed that these architectures will play a significance role in standardization of the NAC vision. Cisco's and Microsoft Corp.'s approach to NAC are based on proprietary standards, while the Trusted Computing Group is working on Open standards. We are including Juniper Networks, Inc., in our NAC study because it is competitor with Cisco Systems Inc. Also, Juniper Networks, Inc. offers one of the first NAC platforms adhering to the Trusted Network Connect guidelines and is commercially available in the market. By selecting these four architectures, we cover a representative set of proprietary and open standards-based NAC technologies.

This thesis documents the contemporary issues related to these NAC technologies. The comparison is done in terms of architectural and functional features they provide, technology they focus on and the shortcomings they possess.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 26 of 114

This thesis work addresses following topics:

- Issues regarding the definition of a NAC solution. What are the ***requirements of a NAC technology***, a set of basic functions that makes up a complete NAC vision.

- The ***description of selected NAC solutions*** that are available in the current marketplace (till end of 2006), which as mentioned above are; *Trusted Network Connect, Unified Access Control, Network Access Protection, and Network Admission Control*.

- A ***comparative study and analysis*** of the selected solutions in terms of architectural and functional components they possess. This thesis will be a guideline for evaluating a NAC solution.

- An ***analysis of the future of NAC*** and the present factors affecting it in the marketplace.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 27 of 114

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 28 of 114

3 Network Access Control

3.1 Definition

In chapter 1 we referred to Network Access Control (NAC) as:

"*Network access control is a vision, which utilizes existing solutions and new technologies to provide assurance that any device connecting to a network policy domain is authenticated, and is subject to the network's policy enforcement. Non-compliant devices are isolated until they have been brought back to a complaint status*".

NAC is a unified vision that leverages from old and new technologies, so that companies can enhance their security infrastructure and secure their investments rather than restructuring their networking infrastructure. Replacing a company's existing infrastructure and laying down a new setup is a complex undertaking resulting in monetary concerns.

3.2 NAC Functions

In today's marketplace there are numerous NAC solutions available. Different companies have their own high level goals to define NAC. There is no unified standardization of NAC. NAC is supposed to go through three major phases, *a phase of NAC awareness, phase of standards* (proprietary and non-proprietary) and *interoperability of such standards*. Currently, NAC is somewhere in the

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 29 of 114

second phase, the phase of standards. As today's focus of the NAC market is on standards, people from various companies are collaborating to standardize NAC. One of the notable involved bodies is the Trusted Computing Group. We will discuss the common building blocks of a NAC mechanism, following are the minimum set of functionalities a NAC solution may have:

- ***Node Detection***
- ***Authentication***
- ***Posture Assessment (or Endpoint Security Assessment)***
- ***Authorization***
- ***Policy Enforcement***
- ***Quarantine***
- ***Remediation***
- ***Post-Admission Control***

3.2.1 Node Detection

The capability of node detection refers to the detection of element accessing the protected network. The function is very important to NAC. As the NAC should be aware of any node/element connecting to the intra-network, so that it can carry other NAC functions (such as authentication, posture assessment, authorization, enforcement, etc. *described below*).

There are a number of ways to detect a node accessing the corporate network. Node detection is done on various layers depending on the access method. Common access methods are; *wired LAN*, *wireless LAN*, *VPN*, and *dialup.*

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 30 of 114

Followings are the different ways to detect element connecting to the network:

- ***Address Resolution Protocol (ARP)*** needs to resolve an IP address to its MAC or Ethernet address. The node broadcasts an ARP request packet. This broadcast can be detected by the NAC equipment and hence the element is detected.

- In an ***802.1X*** port-based access control setup, a switch can detect an element requesting access to the corporate network, as the node sends ***Extended Authentication Protocol (EAP)*** request packets.

- Some switches have the capability to generate ***Simple Network Management Protocol (SNMP) traps,*** when they detect an Ethernet address is being registered to the switch.

- An element can also be discovered when a ***Dynamic Host Configuration Protocol (DHCP)*** request is broadcasted through out the network for requesting an IP address.

- ***Network-layer traffic*** (e.g., ICMP, IGMP, etc.) can be identified when passing through a particular network equipment (e.g., router).

- Through the usage of ***supplicant or endpoint software*** a node can be detected**.** In setups like 802.1X or a VPN, a supplicant software is present on the node which is required for the network connectivity. Whenever, the node connects to the protected network, this supplicant can notify the NAC about its presence.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 31 of 114

- ***Appliances (specialized hardware)*** can also detect a node, when specific traffic is passed through them, e.g., a firewall can detect traffic generated from an unidentified source when passing through it.

3.2.2 Authentication

A NAC system should be able to authenticate each and every user accessing the protected network. Currently authentication involves following methods (some are as following):

- *IEEE's 802.1X standard for wired and wireless networks (based on EAP types)*
- *Dynamic Host Configuration Protocol (DHCP)*
- *IPSec (IP security)*
- *Transport Layer Security/Secure Socket Layer (TLS/SSL)*
- *Virtual Private Network (SSL VPN or IPSec VPN)*
- *Point-to-Point protocol (PPP) in dial-up situations*
- *Secure HTTP (HTTPS)*

3.2.3 Posture Assessment

Posture assessment is a unique function of NAC which is responsible for inquiring the compliance of a device. In simple terms, it is the procedure of verifying the compliance of a device. As discussed in *chapter 1*, in practice users are only subject to authentication schemes, but compliance of the device is not taken into account and such endpoints can be major carriers of malware.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 32 of 114

Posture assessment is a procedure of running various tests on an endpoint device to collect observations (or measurements) and report this data to the policy servers (*discussed in 3.3.3)* to evaluate the compliance level of the machine. In the context of posture assessment we can consider "*compliance*" as an abstract word, it can be comprised of multiple specifications. For example, to:

- *Check the version number of softwares residing on the endpoint (e.g., operating system, antivirus, browser, etc.).*
- *Verify the presence of up-to-date patches.*
- *Collect and compare results of antivirus or anti-spyware scans with pre-defined policies*
- *Collect signature files for firewalls or intrusion prevention systems*
- *Collect and verify the list of trusted applications*
- *Validate digital certificates*

(*The discussion on posture assessment is further extended in 3.3.1)*

3.2.4 Authorization

When a user is connected to the protected network (after passing through the *authentication* and *posture assessment* step, and is considered compliant), afterwards, the NAC verifies each and every access of the user to the resources residing on the intra-network. Policy is defined on the basis of identity and measurements of posture assessment. Authorization step is usually implemented by the AAA system. Protocols used for AAA are RADIUS, DIAMETER, TACACS+, etc.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 33 of 114

3.2.5 Policy Enforcement

Policy enforcement is the function through which NAC enforces defined policies on endpoint machines. AAA system evaluates the policy for the machine (which is connecting to the private network) and forwards these decisions to the policy enforcement points (where policy can be enforced, *discussed in 3.3.2*). Common access scenarios are; access is denied, full access is granted, quarantine (*discussed below*) or limited access, the policy decision is enforced accordingly.

The technologies used for enforcing policy are as following:

- ***Access Control List (ACL)*** defines a list of permissions. The list specifies the access rules. The evaluated policy is formulated in the form of ACL(s) and is/are forwarded to the switch, router, or an appliance for enforcement of these policies.

- ***Virtual LAN (VLAN)*** is also used for enforcement of policies. According, to the formulated decisions, the user is subject to a particular VLAN, available with policy-specific resources (which is/ are defined by the policy).

- ***Firewalls*** can also enforce policies, on the basis of using different parameters, e.g., usage of defined rules, URL-lists, allowed ports, etc., depending on the capability of the firewall the policy is enforced accordingly. Firewall can be an appliance which enforces the policy on the private network or can be host-based firewall residing on the client machine enforcing policies locally.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 34 of 114

3.2.6 Quarantine

Quarantine function is a new model associated with the NAC vision. One of the goals of the NAC technology is to isolate non-compliant devices from the private (or protected) network, so that the network remains safe and unaffected from non-compliant machines. This is either done by a VLAN assignment to a specific and separate network, or a temporary IP address is assigned which can only communicate (or route messages) to specific resources such as *quarantine setup* (*discussed below in 3.3.4*).

3.2.7 Remediation

When a device is quarantined, the node is part of the quarantine network (or quarantine setup) and may be able to access a defined set of remediation resources. Remediation resources can allow the user to recover from non-compliant status to a compliant machine, so that the device can be re-connected to the private network. Remediation involves installing of patches, updating antivirus software, updating signatures for antivirus or intrusion prevention system, or enabling a firewall, etc., depending on the security requirements.

After the machine acquires all the updates as required by the policy, the device can once again go through the *posture assessment* step, if proved compliant, the device is admitted back to the private network, else quarantined again.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 35 of 114

3.2.8 Post-Admission Control

Post-admission control is similar to threat mitigation. When a device is considered compliant and is connected to the private network; users, nodes, and their sessions are monitored for any malware activity or policy violations. If such activity is detected, then the access of the user can be moderated either by quarantining or by dropping the session. Post-admission control works similar to the functionality of Intrusion Prevention Systems (IPS). Post-admission control defines procedures to mitigate threats from legitimate resources.

3.3 NAC Components

Following are the components involved in NAC:

- ***Client***
  - Agent-based Client
  - Agentless Client
- ***Enforcement Points***
- ***Policy Servers***
- ***Quarantine Network***
- ***Remediation Servers***

3.3.1 Client

A client is a machine which requests network access for the private or protected network. There are two categories of such clients which are specific to the NAC technology; one type of clients includes endpoint software running on them, and

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 36 of 114

is known as ***agent-based client***. In second category of clients, there is no endpoint software specific to the NAC paradigm installed on these machines, and is called ***agent-less client.***

- A client machine having a ***NAC-aware agent*** when requesting access to the private network, this agent can sense the request for connection and can perform posture assessment prior to any connectivity. In other case, the NAC can sense a machine requesting access for the protected network and can interact with the agent for posture information.

  Agent software is responsible for conducting posture assessment. Agent can itself or may collaborate additionally with other security software packages (specific to security applications such as antivirus, firewall, etc.) to collect posture of the machine (*discussed in 3.2.3*). Further on, the agent forwards these collected observations to the policy server(s). These servers are responsible for evaluating the compliance of machine and accordingly the policy is enforced at the enforcement points. Agent can also collaborate with security applications for post-admission control (*discussed above in 3.2.8*). Agent-based client can also act as an enforcement point (*by acting as a host-based firewall*).

- When an ***agentless client*** connects to the intra-network, the NAC can determine that there is no endpoint software installed on the machine. NAC can instantiate a dialogue with this client making it possible to download and install the agent software. In this case, the client will act as an agent-based client. If downloading of an agent is not possible, client's compliance is evaluated through browser integration that is through the usage of Java or ActiveX. Posture assessment is performed through web-

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 37 of 114

based agent and the collected information is communicated to the policy server. Agentless client can also be scanned through vulnerability scans by opening network connections to the client's machine. By using the web-based approach the browser should enable support for Java or ActiveX. Once, an agentless client is on the intra-network, for post-admission control monitoring, the network setup should integrate usage of firewalls or IPS.

3.3.2 Enforcement Points

Enforcements points in a NAC platform carry great importance, as clients communicate with these points to access the private network. Therefore through such points a NAC system have control over endpoint devices and hence can take any action specific to enforcement of policy. Following are the different enforcement points in the NAC setup:

- ***Switch***
- ***Router***
- ***VPN equipment (appliance or server)***
- ***Firewall***
- ***Enforcement Server***
- ***Agent-based Client***

- A network ***switch*** can enforce policies at the port-level (layer-2), which is possible through IEEE's 802.1X standard for wired and wireless LANs. Some switches have the capability of defining ACL by which traffic can be moderated.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 38 of 114

- A ***router*** can implement ACLs by which it can moderate traffic and enforce policy at IP-layer (layer-3).

- ***VPN*** equipment (server or appliance) used in remote setup can also be used to moderate the access to the private network. As these are the points from which the remote machines interact to connect to the private network. VPN supplicant software can also enforce limited policies.

- ***Firewall*** technology can also aid in moderating the access to the intra-network by defining rules according to the corporation's policy. Firewalls can enforce policies on the application or network layer by monitoring on going packets through a subnet and can collaborate with other enforcement technologies such as, switch, or router for enhanced security. Agent-based clients may also communicate with a firewall to enforce a policy. For example the agent software might detect a violation of policy and reports it to a firewall and can enforce policy accordingly.

- ***Enforcement Server*** category covers all sort of serving machines that have the capability to enforce a policy according to their designed function. For example, if we consider a DHCP server which is responsible for leasing IP addresses, can release an IP address on a policy violation, and further on can collaborate with a switch, router, or a firewall for the enforcement of policies. Likewise, a certificate granting server can invalidate a certificate on a policy infringement.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 39 of 114

- ***Agent-based Client (supplicant)*** can also act as a point of enforcement, as the agent software varies in terms of its functionality. On a policy violation it may not allow the client to communicate to the private network. This software can have the functionality of a firewall (host-based firewall) and may communicate with a firewall/IPS on the network for enforcement of policies.

From above we can identify three classifications of enforcement, as illustrated in the Figure 3.1.

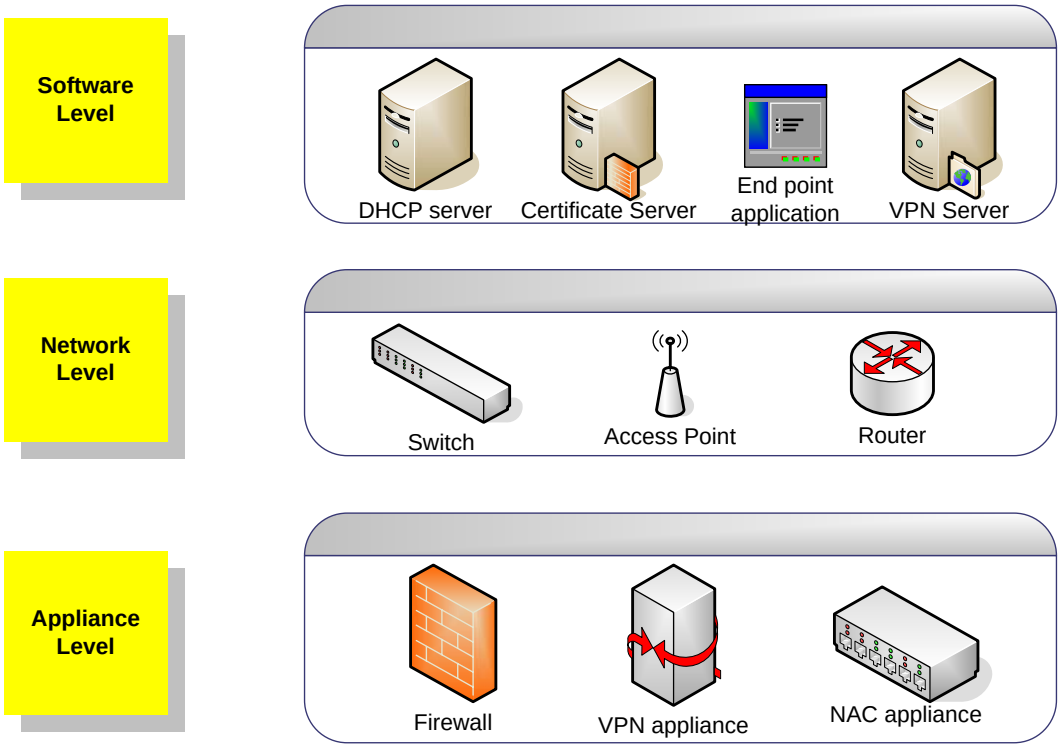

Figure 3.1 Levels of enforcement

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 40 of 114

3.3.3 Policy Servers

Policy servers are responsible for administering access control decisions. A policy server is a central server which is involved in defining, setting, and managing network security policies for the protected network. In practice, a policy server is a machine that supports Authentication, Authorization, and Accounting (AAA) architecture and usually implements Remote Authentication Dial-In User Service (RADIUS) protocol.

Policy servers collect the summary of compliance tests executed on a client machine (*refer to the posture assessment step 3.2.3*) and relate these results with pre-defined security policies, to determine access control decisions, and direct these decisions to enforcement points for enforcement of policies. In practice, for robust access control, policy servers may also interact with vendor-specific policy servers, specialized for a particular security domain.

3.3.4 Quarantine Network

A quarantine network is a separate security-hardened network where quarantine machines reside. Within this network a machine can communicate to a set of limited resources that mostly includes the remediation servers, DHCP server, etc. A machine stays in the quarantine network until its status remains *non-compliant*. The main purpose of the quarantine network is to keep the intra-network protected as much as possible and isolate affected machines effectively.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 41 of 114

3.3.5 Remediation Servers

Remediation servers are the resources which aid quarantined clients to recover theirselves to compliant statue. Hence, such machines can connect again to the protected network. Remediation servers can automatically or manually update endpoint software, operating system, antivirus, install patches, signatures for intrusion detection software, etc.

3.4 NAC Flow

The following Figure 3.2 presents typical flow of information during NAC process.

1. The user attempts to connect to the protected intra-network.
2. The NAC detects presence of a device (*element detection*), NAC inquires the client for admission control data (*authentication and posture assessment*).
3. The user provides the admission control data to the NAC components (switch, router, server, etc.).
4. Network components forward this data to the policy server(s) for access control decisions.
5. The policy server authenticates the client (*authentication*) and sends the posture data to the policy-vendor server(s).
6. Policy-vendor server(s) which is/are specific to a security application, verifies the posture data, and return their recommendation(s) to the policy server.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 42 of 114

7. Policy server decides the access decisions for the client and sends enforcement data to the enforcement pieces of the network (*authorization*).
8. Enforcement entities enforce the policy and respond to the client about the policy (*policy enforcement*); whether allowed, denied, or quarantined.
9. On the basis of policy decisions, the client is subject to the protected network or quarantine network.

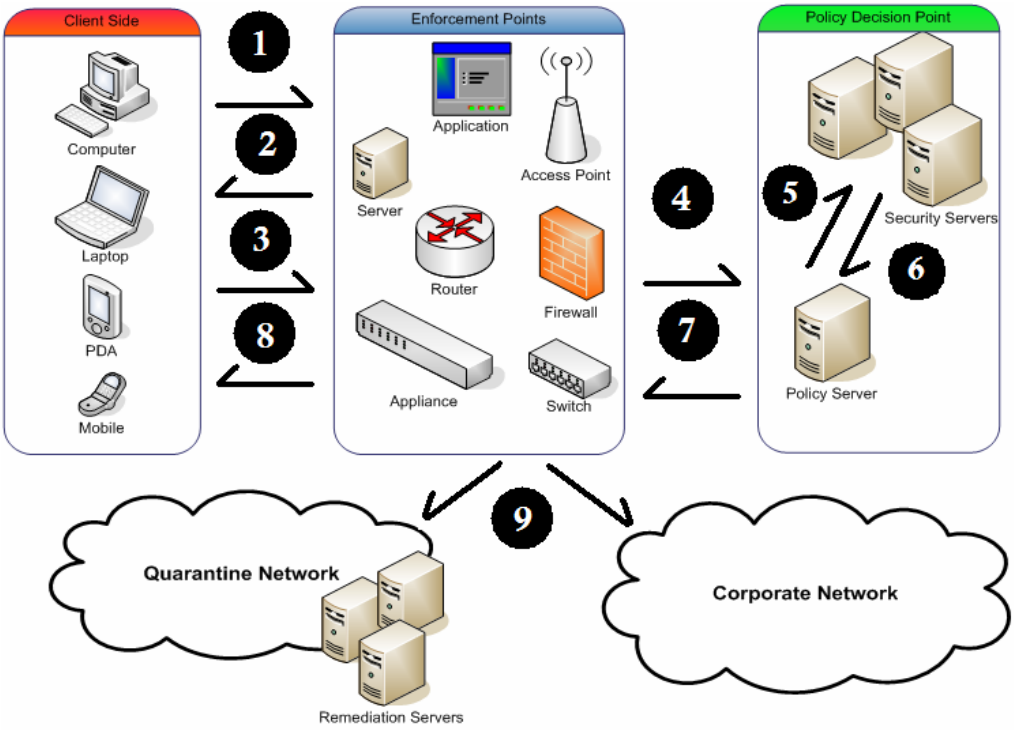

Figure 3.2 Basic message flow in a NAC paradigm

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 43 of 114

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 44 of 114

4 Trusted Network Connect

By the Trusted Computing Group

The Trusted Computing Group (TCG) is a non-profit organization formed to define, develop, and promote open standards for achieving *trusted computing* across multiple platforms. This consortium is led by AMD, Hewlett-Packard, IBM, Infineon, Intel, Lenovo, Microsoft Corp., Sun Microsystems, and others.

The term "*trusted computing*" refers that the computer will consistently behave in a specific manner and such behavior will be enforced through a set of specialized software and hardware. TCG proposes a number of security applications by which computer security can be improved, facilitating computers to be safe from viruses and malware threats [24].

The goal of *trusted computing* relies on the TCG's Trusted Platform Module (TPM) chip, which is an integrated circuit which allows achieving various trusted computing features defined by the TCG. The TPM chip is a microcontroller that can store and protect secret information such as keys, passwords, digital certificates, etc. It is typically attached to the motherboard of a machine or can be used in any computing device that requires such trusted computing features. The nature of the TPM chip ensures that the secret data is safely stored in a protected location until ready for reporting. TPM chip is designed is such a way that it is difficult to retrieve secret data by reverse engineering or any other method. TPM hardware aids in protection against external software attacks and physical theft of protected data.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 45 of 114

Additionally, one of the unique functions of TPM is establishing "*chain of trust*". In a chain of processes, there is an initial process, referred to as "*root-of-trust*", which is the core process by which other generated processes can be measured. *Roof-of-trust* is a trustworthy entity (or process) which must be trusted. There should be no means to measure the *root-of-trust* it is assumed to be trusted (due to the reason that it cannot be tampered or exploited due to the way it is designed). In a *chain of trust* the initial process measures the next executing process. The initial process (*root-of-trust* that is) verifies that whether the next process is trustworthy or not, if the process is not tampered or compromised, it concludes that the process can be trusted and hence provides the process with secret data, so that trustworthy process can measure other generating processes. Consequently, the trusted process can measure the process next to it. So this creates a chained process in which one process establishes trust with the next process in a transitive manner.

Application of *root-of-trust* can be integrated with the boot sequence process. The boot sequence can be verified in an incremental manner and can be halted/terminated if the boot sequence is not as expected. Such functionality can be verified or measured by the help of the TPM chip. Thus, introducing a security mechanism utilizing the idea of *transitive trust.* A strong hardware-protected *root-of-trust* is needed to ensure that any malware, compromised application, or improperly configured software fails to report an erroneous status.

The TCG is extending its specifications into a variety of related devices, including mobile devices, servers, peripheral devices, storage, infrastructure, and embedded systems, so that such trusted features can be incorporated and utilized.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 46 of 114

4.1 Background

One of the further initiatives of the TCG is related to the Network Access Control vision; this initiative is known as the "Trusted Network Connect", an architecture used to enable protection of the networking infrastructure. The Trusted Network Connect (TNC) architecture is based on open and non-proprietary standards, which makes this architecture unique. Open standards play a vital role in the computing world. Different companies are contributing to this architecture in a collaborative manner. The number of TCG members is increasing everyday, there are more than 100 members who are participating in trusted computing features.

4.2 Trusted Network Connect

4.2.1 Introduction

TNC specifications will enable application and enforcement of security requirements on endpoint machines requesting access to the corporate network. TNC guidelines are based on open and non-propriety standards. TNC architecture will facilitate IT organizations to enforce corporate security policies to prevent and detect malware outbreaks, as well as to avoid resulting security breaches and down time in multi-vendor network infrastructures.

TNC assists network administrators in protecting their networks by assessing compliance of endpoint devices and imposing enterprise security policies before any network connection is established. Hence, preventing unauthorized users to make connections to the private network.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 47 of 114

By TNC, a network infrastructure can be protected against various security outbreaks occurring through viruses, worms, Trojan horses, etc. TNC specifications focus on the collection of endpoint compliance measurements (also known as the "Posture Assessment" as discussed in Chapter 3) in conjunction with user authentication information. This posture is compared with a pre-defined set of organization policies defined for the network access to the protected network. Primarily, this creates a "secure" profile for a system. Secondly, evaluating the appropriate level of network access based on policy compliance, resulting in full access, partial access or directed access, or no access.

The TNC platform relies on the idea of "*integrity*" and "*identity*". The notation of *integrity* is used to describe the up-to-date state of an endpoint's "compliance" or posture. The notion of integrity allows the evaluation of the system, to confirm that whether a machine complies with pre-determined policies and to determine that the system is not engaged in any unusual or malicious behavior. Endpoint integrity policies may involve integrity parameters spanning a range of system components (hardware, firmware, software, and application settings), and may or may not include evidence of a Trusted Platform Module (TPM). On the other hand, the notion of *identity* ensures that systems are authenticated for authorized users only.

Identity and integrity are part of the concept of "*Platform Authentication*"; which is to verify the *proof of identity* (authenticate the identity) and *platform integrity* (authenticate integrity of the machine) using TPM module. Though the usage of TPM is optional but the TCG strongly recommends *platform-authentication* for the authorization of layer-2-based or layer-3-based network access, due to increased attacks on higher layers (Trojans, viruses, etc,). TPM offers additional security, as level of trust is established through hardware (in this case TPM chip).

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 48 of 114

The *transitive chain of trust* helps in preventing against passive and stealthy infections that are otherwise almost impossible to detect, e.g., root kits (a malware which gains root access, modifies the code of the application, and merges with it).

TNC is an excellent application for the TPM, it aids in establishing a secure link to a decision point where integrity measurements may be evaluated. Thus, it can protect the measurements from man-in-the-middle attacks that might occur anytime. For now the use of the TPM by TNC is optional. Products based on TNC architecture can operate in today's environments with and without TPM. TPM reports can be factored into Network Access Control decisions through "*Platform Trust Service*" specifications (IF-PTS) of the TCG, assuring that such reports are originated from the expected platform and are considered to be legitimate.

Another important aspect of TNC is its focus on heterogeneous networking environments. Environments comprising of products from a variety of vendors. TNC support for heterogeneity will enhance existing products to work with new technologies. Users can benefit easily and quickly adapt the TNC mechanism. TNC leverages from the existing infrastructure, utilizes products and standards that are already deployed on the network.

Companies currently providing compatible products to the TCG platform include Extreme Networks, HP ProCurve, Juniper Networks, Inc., Meru Networks, OpSwat, Patchlink, Q1 Labs, StillSecure, Wave Systems, General Dynamics and others. The pivotal aspect of Trusted Network Connect architecture is that it uses existing open industry standards, such as EAP, TLS, HTTPS, 802.1x specification and others. The architecture supports all commonly used enterprise access methods such as VPN-based or dial-up remote access; wireless networks; 802.1x infrastructures; and traditional LAN technologies.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 49 of 114

4.2.2 Components of TNC

Following Figure 4.1 illustrates the three main components of the Trusted Network Connect; Access Requestor (AR), Policy Enforcement Point (PEP) and Policy Decision Point (PDP):

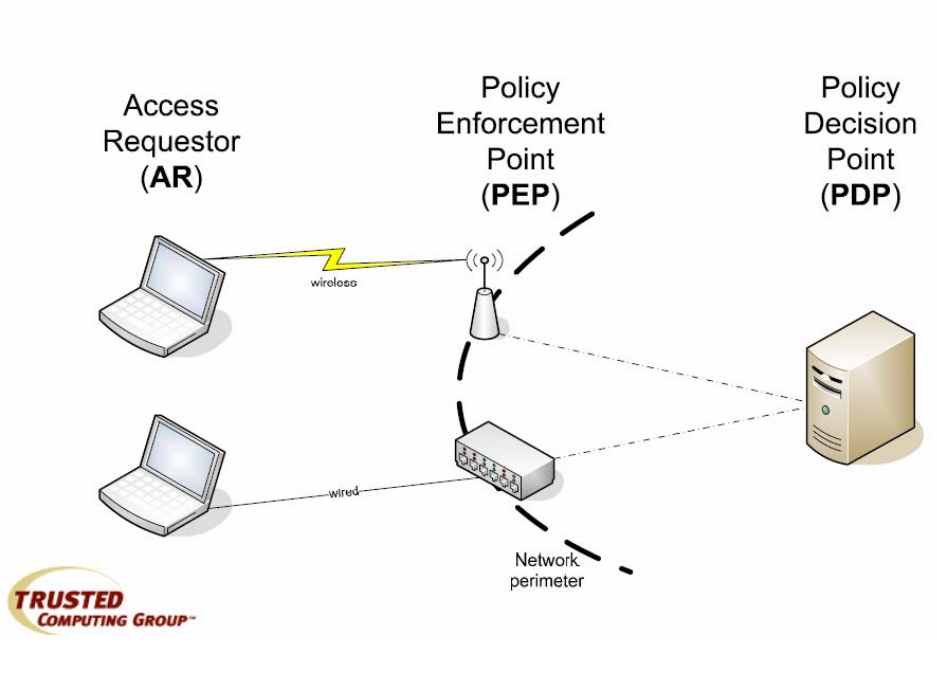

Figure 4.1 Components of TNC [23]

- ***An Access Requestor (AR)*** component is made up of three sub components: Network Access Requestor (NAR), Integrity Measurement Collector (IMC) and TNC Client (TNCC).

  Network Access Requestor (NAR) refers to the component which requests access to the network and is used to connect to the network. A supplicant in 802.1X setup or a software used in VPN setup are examples

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 50 of 114

of NAR. There might be several NARs present on a single AR responsible for handling connections to different networks.

Integrity Measurement Collector (IMC) is responsible for collecting "measurements of compliance" of a device, this component is responsible for collecting the security posture (same as "Posture Assessment" function discussed in Chapter 3) of the end-system on which it resides. The integrity measurements are transferred to TNC Client component.

TNC Client (TNCC) acts as a client broker (middleware); which is a layer between NAR and the IMC, it coordinates with IMC, helps in packaging integrity measurements (or posture data) and forwards it to the NAR component.

- ***Policy Enforcement Point (PEP)*** component of TNC is the simplest part in the TNC architecture. This is the point where policy is enforced. TNC is built on industry standards which are responsible for controlling access to a protected network. TCG enforcement points include support of IEEE 802.1X, HTTPS, and IPSec.

- ***Policy Decision Point (PDP)*** is analogous to AR. Likewise this component is divided into three sub-components. Network Access Authority (NAA), TNC Server (TNCS) and Integrity Measurement Verifier (IMV).

  Network Access Authority (NAA) is responsible for authentication and access control decisions, and communicating such decisions to PEPs. Practically NAA is an AAA (RADIUS or a DIAMETER server). Up to

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 51 of 114

current TCG specifications, TNC only supports integration with RADIUS server but later on will add support for DIAMETER and LDAP.

Integrity Measurement Verifier (IMV) is the counter part of IMC and is responsible for verifying a particular aspect of the AR's integrity. Verifiers and collectors correspond to each other, hence are in a paired form. They can communicate each other through their specified interface (IF-M described below).

TNC Server (TNCS) component acts as an agent between NAA and IMV, which coordinates with each other. It provides the aggregated measurements collected from the IMC(s) to corresponding IMV(s).

4.2.3 Architecture of TNC

Following Figure 4.2 is an illustration of Trusted Network Connect architecture, which shows the relation of various interfaces involved in this architecture:

All the entities in this architecture are logical not physical. In this architecture an entity can represent either a software or a hardware. It can be observed in Figure 4.2 that the architecture is divided into three abstract layers.

- Functions of ***Network access layer*** are related to network connectivity and security. This layer will involve variety of networking technologies (current support is for VPN [for remote access], 802.1X [for layer-2 access], PPP [for dial-up access]).

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 52 of 114

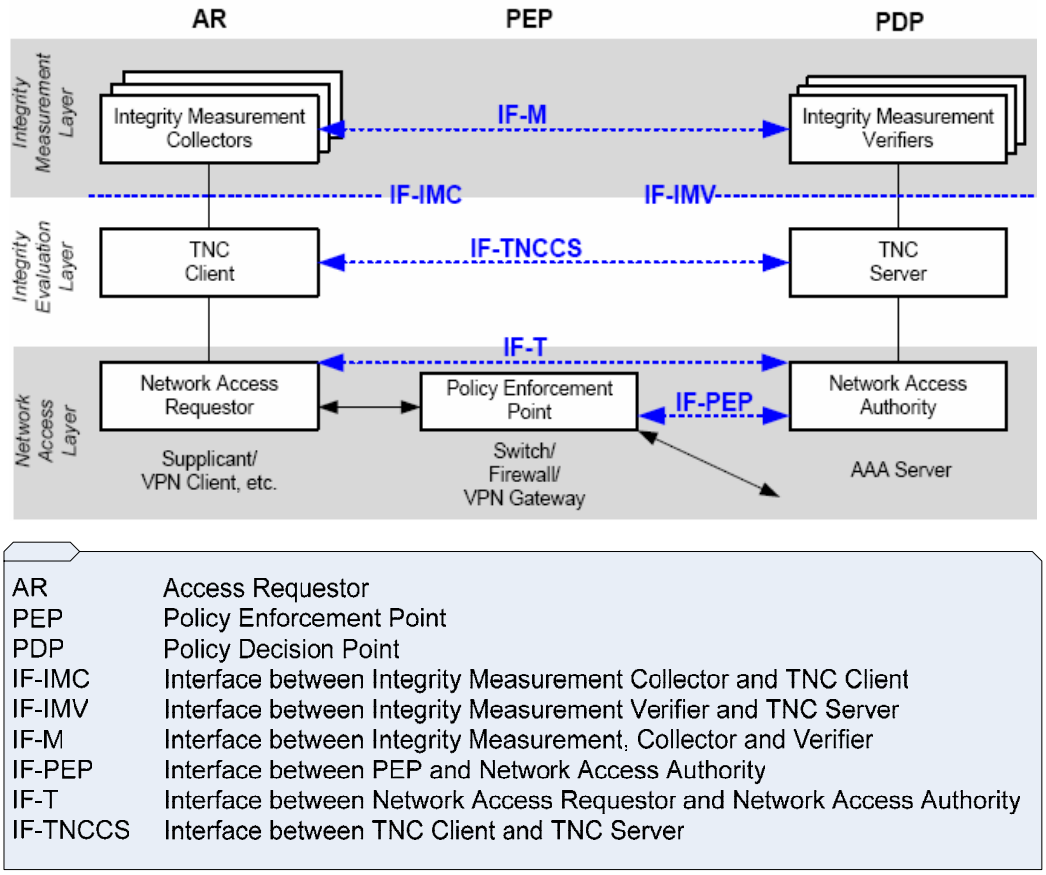

Figure 4.2 Architecture of TNC [24]

- The components of ***Integrity evaluation layer*** are responsible for evaluating the integrity of the AR according to access policies.

- ***Integrity measurement layer*** contains plug-in components which can correspond to different security applications (e.g., Antivirus, Operating system patch level, etc.) and is responsible for collecting and verifying integrity measurements

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 53 of 114

4.2.4 Interfaces of TNC

- ***IF-M:*** *Interface between IMC and IMV*

This is the protocol between the IMC's and IMV's, communicated over the IF-TNCCS interface (*discussed below*). Only a part of this interface will be standardized by the TCG, rest of it will be vendor specific and will be encapsulated in IF-TNCCS.

- ***IF-IMC:*** *Interface between IMC and TNCC*

This is the protocol for gathering integrity measurements (or "Posture Assessment") from the IMC(s) and forwards them to their corresponding IMV(s). This protocol also manages the message exchange between these two entities. Various IMC(s), specific to a application context (such as antivirus, firewall, etc.) can communicate with the TNCC through a set of API. So by this way the TNCC collects information from multiple sources such as software, firmware and hardware components and are further on delivered to corresponding IMV(s) through TNCS (using IF-TNCCS interface discussed below) [26].

- ***IF-IMV:*** *Interface between IMV and TNCS*

This protocol is the counter part of the interface IF-IMC, responsible for receiving integrity measurements from the TNCS (previously received through TNCC from IMC) and to forward them to their corresponding IMV(s). Also it provides its recommendations to TNCS on the basis of evaluation of posture or compliance measurements [27].

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 54 of 114

- ***IF-TNCSS:*** *Interface between TNCS and TNCC*

This interface specifies the protocol between the TNC Server and the TNC Client allowing interoperability between clients and servers from different vendors. The main responsibilities of this interface are to carry measurements between IMC(s) to IMV(s) (integrity measurements) and vice versa, and to synchronize messages between TNCC (TNC client) and TNCS (TNC server) as well as to manage session messages [30].

This interface is independent from transport type, can be carried over variety of transports. The TCG will standardize this interface in future, it will add on more TNC related information to the underlying protocols being used.

- ***IF-T:*** *Interface for Network Authorization Transport Protocol*

IF-T is the interface of tunneling for messages between network component NAR (part of AR entity) and component NAA (part of PDP entity). First it transports the information related to IF-TNCCS, then integrates TNC Handshake into IETF EAP thus allows TNC architecture to operate with a variety of network technologies that supports EAP authentication. TNC architecture will not standardize this protocol, but will provide bindings, showing how these messages can be carried over existing protocols, such as using EAP for IF-T within 802.1X. For now support is available for EAP-TTLS, EAP-FAST and EAP-PEAP [29].

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 55 of 114

- ***IF-PEP:*** *Interface between PEP and PDP*

This is the protocol which enables PDP to communicate network access decisions to PEP. For now, this enforcement protocol is only available for RADIUS enabled AAA server. The interface enables enforcement point to enforce access decisions based on endpoint's network traffic. Network access decision triggers enforcement action by the enforcement point, such actions are: *allow access, deny access, or grant limited access.*

Three types of enforcement are available: One method is the binary enforcement which either *allows* or *disallows*, second one isolates a machine by VLAN assignment also know as layer-2 isolation and the third one is based on layer-3 isolation, by filtering resources by User ID or IP (ACL's) [28].

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 56 of 114

5 Unified Access Control By Juniper Networks, Inc.

Juniper Networks, Inc. is one of the major companies in the telecommunication industry, developing solutions ranging from IP networking to security solutions. Juniper Networks, Inc. customers are service providers, enterprises, governments and research and educational institutions, situated worldwide. Juniper Networks, Inc. is directly in competition with companies such as Cisco Systems Inc. and Check Point Software Technologies Ltd. Today, Juniper Networks, Inc. plays a vital role in the telecommunication market. Juniper Networks, Inc. specializes in products such as:

- *Routers*
- *Firewalls*
- *Intrusion detection systems*
- *VOIP-based solutions*
- *SSL VPN*
- *Unified Access Control*

5.1 Background

The reason for selecting Juniper Networks, Inc. in our comparative study is very important. It is observed that Juniper's Network Access Control product "Unified Access Control (UAC)" holds a prominent place in the current marketplace. The reason for this is due to their support of the Trust Computing Group's (TCG) guidelines for Trusted Network Connect (TNC), and adoption of IEEE's 802.1X

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 57 of 114

standard (used for authenticating devices on wired and wireless LANs). As, TNC guidelines promotes open standards and interoperability. This makes Juniper's UAC one of the interoperable solution available in the market. UAC version 2.0 is also the first solution adhering to TCG-TNC guidelines.

Juniper's UAC is an appliance-based NAC which started off with their product UAC version 1.0. At that time Juniper's UAC was not an interoperable solution and was not following any of the TCG-TNC guidelines. Also, the policy enforcement relied on layer-3 by using capabilities of Juniper Networks, Inc. firewalls/VPN appliances. At the end of November 2006, Juniper Networks, Inc. released UAC version 2.0 which supports TCG-TNC guidelines and IEEE's 802.1X standard, making UAC version 2.0 a vendor agnostic technology. Enabling Juniper Networks, Inc. UAC version 2.0 to work with any 3rd party security application following TCG guidelines and, can work with switch available from any vendor supporting 802.1X capabilities.

In our report, our focus will be on UAC v2.0 (version 2.0) as it combines the functionality of UAC version 1.0 and it accumulates with TCG's TNC guidelines providing access control protection from layer-2 to layer-7.

5.2 Unified Access Control

5.2.1 Introduction

Unified Access Control secures the network from malicious users or machines by taking account of user identity (through authentication), device integrity (through posture assessment) and network location information (cases such as *employees,*

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 58 of 114

contractors and guests which categorize local and remote users*)* with session specific policy. UAC v2.0 is based on standards on which industry have agreed upon, standards such IEEE's 802.1X, RADIUS, etc. Juniper Networks, Inc. also follows the open standards of TCG-TNC, which makes UAC v2.0 an interoperable solution.

By supporting the IEEE 802.1X standard, UAC v2.0 can utilize existing switching infrastructure of a company, as it can operate with any vendor's switch or access point having 802.1X capabilities. Following Figure 5.1 illustrates the integration of UAC with 802.1X-enabled switch (using layer-2 access control). Enterprises using Juniper Networks, Inc. firewalls can also upgrade to UAC v2.0 and can enforce policy from layer-3 to layer-7. UAC v2.0 combined with 802.1X and Juniper Networks, Inc. firewalls provide access control from layer-2 to layer-7. UAC also have support for cross platforms; can work with platforms such as Windows, Linux (SuSe, fedora, Red Hat), Solaris and MAC.

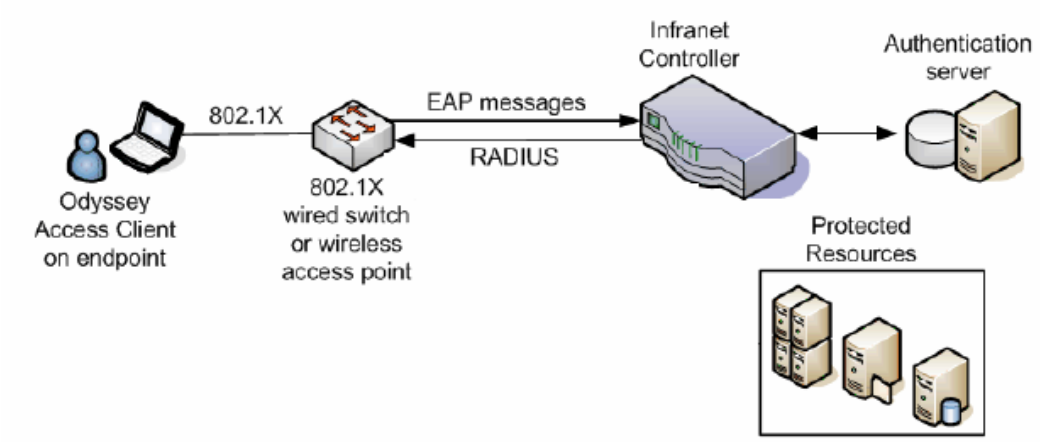

Figure 5.1 Infranet Controller with 802.1X enabled switch

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 59 of 114

UAC v2.0 assess the endpoint before and after the access of the network, performing endpoint assessment on intervals specified by the administrator, this is pivotal for providing complete and dynamic protection.

5.2.2 Architecture and Components of UAC

The following Figure 5.2 is an illustration which shows the relation among UAC components. Unified Access Control platform relies on the following components:

- ***The Infranet Controller*** is a component available in the form of an appliance which functions as a centralized security policy engine. The Infranet Controller also features integrated 802.1X functionality from SBR (Steel Belted Radius) server. SBR is a RADIUS/AAA policy management server, which is separate product of Juniper Networks, Inc. but also incorporated in the Infranet controller.

  Infranet controller works as an "*authentication server*" in an IEEE 802.1X setup. Infranet controller can also interface with the existing enterprise AAA infrastructure, support ranging from 802.1X, RADIUS, LDAP, etc.

  The UAC v2.0 can be run in both agent and agent-less modes to provide on-demand posture assessment of endpoints. One of the responsibilities of the Infranet controller is to dynamically push the *UAC Agent* (discussed below) to the host machine requesting network access, the UAC agent after being downloaded can initiate network access control process, such as "user authentication" and "posture assessment". The user agents are

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 60 of 114

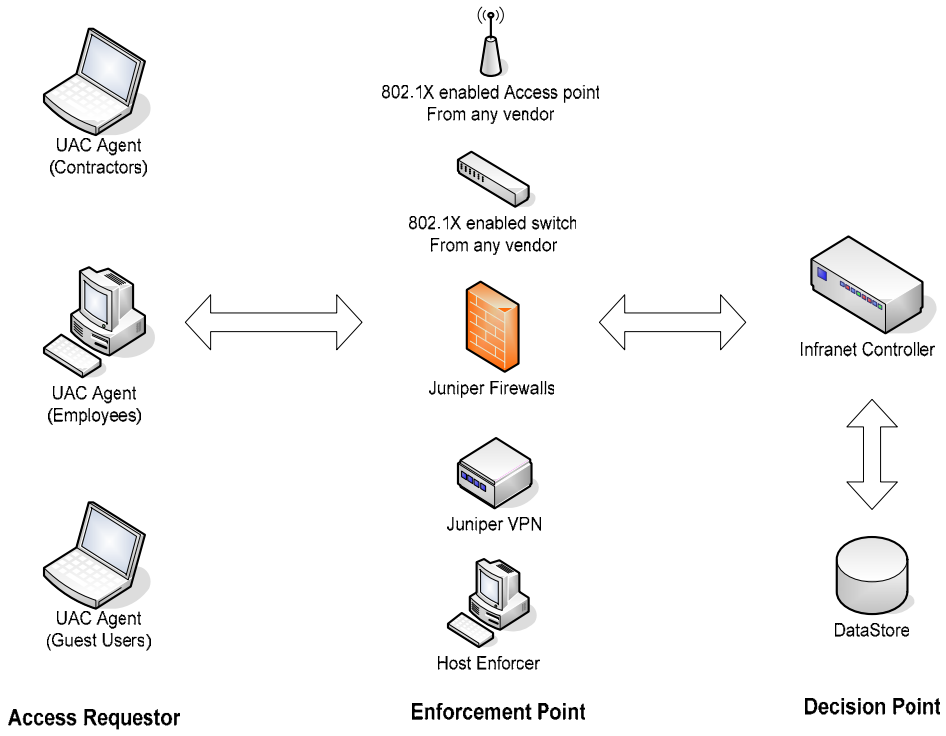

Figure 5.2: Unified Access Control architecture and components

always up to date to the latest version of software, minimizing operational costs of maintenance. In situations where the installation of agent is not possible on a client's machine e.g., guest access, network access control is initiated by the Infranet controller through browser based validation of user credentials by performing a set of vulnerability scans.

- ***The UAC Agent*** is a software, which can be dynamically pushed in real-time by the Infranet Controller to the device requesting access to the network resource, this can be done by browser supporting JAVA or ActiveX. The UAC agent provides security from layer-2 to layer-7. The

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 61 of 114

agent uses capability of OAC (Odyssey Access Client) to access the network at layer-2 (port level), OAC acts as *"supplicant"* in an IEEE 802.1X setup. For network access involving layer 3-7 the UAC agent uses a *Host Checker* and a *Host Enforcer* (which is a stateful personal firewall).

Host Checker enables the administrator to scan endpoints for various security evaluations such as antivirus, malware and status of firewalls.

Host Enforcer which a stateful personal firewall, is used for the dynamic enforcement of policies, it enforces policies on the endpoint. UAC agent is capable of checking registry values, network ports and can perform an MD5 checksum to verify application validity. Host checker can also communicate with other security applications designed by different vendors for more robust security *(discussed in 5.2.3)*.

- ***UAC Enforcement Points*** include any vendor's 802.1X-enabled wired or wireless switches which makes the UAC platform vendor agnostic. Additionally, the UAC enforcement points extend to all Juniper Networks, Inc. Firewall/VPN appliances. Machines having the UAC agent also consist of a Host Enforcer module, which is a small-functionality firewall, allows enforcing of policy local to the machine. Thus, UAC gives room to enforce policy from layer-2 to layer-7 providing stronger granular access control.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 62 of 114

5.2.3 Interoperability Initiative

The Figure 5.3 illustrates the UAC architecture in terms of TCG's TNC. Considering the Access Requestor (*refer Chapter 4*.2.2) component, the TNC client and Network Access requestor are built up in one component known as *UAC agent* (*discussed above in 5.2.2*). Likewise the Policy Decision Point component having the TNC Server and Network Access Authority are built up in the Infranet Controller component.

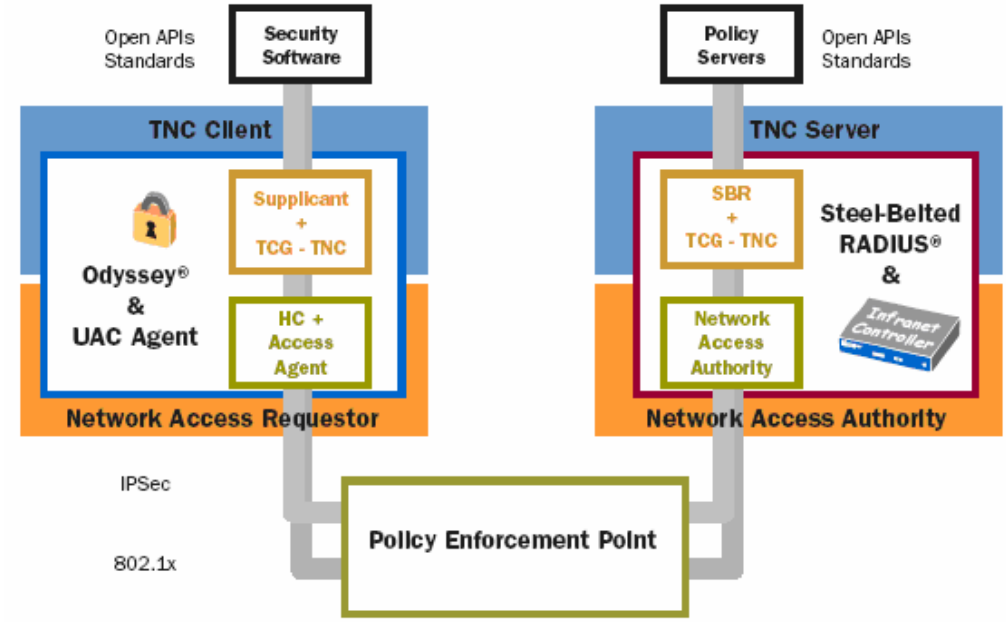

Figure 5.3: UAC architecture in terms of TCG's TNC [10]

The notion of interoperability in UAC is achieved through usage of open API standards, provided by TCG's TNC specifications (interfaces such as IF-IMC, IF-IMV and IF-M). By followings these open standard APIs, any vendor can plug-in

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 63 of 114

their security application with the UAC v2.0 (which was not possible with UAC 1.0, at that time Juniper Networks, Inc. made their own set of API for 3rd party integration). *Host checker* component is responsible for gathering "*posture measurements*" from 3rd party security applications and further on collaborates with Infranet controller to verify security policies with policy servers specific to security applications. Also, by following TCG's bindings for RADIUS, Juniper's UAC v2.0 can work with switch from any vendor.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 64 of 114

6 Network Access Protection

By Microsoft Corp.

Microsoft Corp. develops, manufactures, licenses and supports a wired range of products for computing devices. Microsoft Corp. is well known for their operating system, *Microsoft Windows*, and their word processing suite, *Microsoft office*. Microsoft Corp. have developed a line of server products for various technologies (Internet information Services, Internet Access Server, Active Directory etc), this also includes server edition of Microsoft windows operating system.

Recently, Microsoft Corp. is paying great attention on computer security. Development of their initiative "Security Centre", which is available in Microsoft Windows operating system, focuses on three security essentials; firewall technology, automatic updates (mostly patches and hotfixes), and virus protection software. By this Microsoft Windows can collaborate with such functions and make sure that they are up to date with security needs. Also, their recent products such as *Microsoft Defender* and *Microsoft Windows Malicious Software removal tool*, are new initiatives towards antivirus and antispyware products, which indicates that Microsoft Corp. is going to develop security products in the future.

6.1 Background

The reason for selecting Microsoft Corp. as subject in our study is that, Microsoft Corp. announced its new technology called "*Network Access Protection*" which is their product for Network Access Control. NAP (Network Access Protection) is one of the popular proprietary platforms available in the current market. Till Now,

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 65 of 114

NAP is not fully functional till their release of Microsoft Windows Server "Longhorn", at the time of this writing expected to be released in june/july 2007. NAP platform is based on software technology, which collaborates with other software or/and hardware functions to enforce network policy.

6.2 Network Access Protection

6.2.1 Introduction

Microsoft's NAP (Network Access Protection), addresses network access control by maintaining computer compliance of machines such as home computers, Intranet computers and traveling portable computers, keeping them safe from malicious attacks, enforces compliance according to system's compliance. NAP client is built into Microsoft Windows Server "Longhorn" and Microsoft Windows Vista™, also available as a separate client for Microsoft Windows XP with Service Pack 2.

NAP is comprised of client components and server components that allow you to create and enforce compliance policies for computers that connect to your network. NAP provides protection against non-compliant machines by centrally configuring a set of policies to define requirements for compliance, verify system's compliance before any access to secure resources by compliance requirements (or policy), limit the access of non-compliant computers to a restricted network containing remediation services, by using these services client machines can recover back on the secure network as a compliant machine (confirming to addressed policy). Through usage of Microsoft's API, 3rd party vendors can integrate with NAP to enhance validation and enforcement functions.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 66 of 114

NAP also provides ongoing health compliance while a compliant computer is connected to the network. By this NAP can identify any changes in compliance occurring at the client system, in terms of security applications, e.g., if an *automatic updates* option or a firewall functionality is turned off, NAP can detect this violation, and can quarantine the node immediately.

NAP incorporates the capability of automatic remediation; NAP can be configured for automatic remediation, so that NAP client components can automatically attempt to update the client computer when the client is noncompliant. In addition, NAP auto-remediation reduces the amount of time of a noncompliant computer for being prevented away from accessing the organization's network resources. Auto-remediation can rapidly update the computer using resources supplied in the restricted network (quarantine) allowing the non-compliant client to validate its corrected health state and obtain unlimited access to the network.

Microsoft's NAP is not designed to secure a network from malicious users, It is designed to help administrators maintain the compliance of computers on the network, which helps in maintaining the overall integrity of the network. NAP can not prevent an authenticated and authorized user with a compliant computer from spreading a malicious program to the private network or involving in other inappropriate activity [25]. It can do so by adding related functional components through its API.

6.2.2 Architecture and components of NAP

NAP architecture consists of following components, presented in Figure 6.1:

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 67 of 114

- ***NAP Client***
- ***NAP Server***
- ***NPS Server***
- ***Remediation Server***
- ***System Health Server***

NAP Client

NAP Clients are computers that support NAP platform, machines having Windows Server "Longhorn" or Windows Vista. A NAP client can be further divided into three more sub-components; Figure 6.2 illustrates the sub-components of a NAP client in a layered manner:

- ***Layer of SHA Components:*** SHA refers to System Health Agent. There can be one or more agents present on a NAP client. A SHA corresponds to specific security application and usually is in pair with System Health Validator (SHV, *discussed below in NAP Server section*) which is responsible for validating compliance requirements, e.g., SHA for antivirus, SHA for firewall, etc. On default, Microsoft Corp. provides its own SHA which is responsible for checking up with *Microsoft Security Centre* requirements (discussed above).

  One of the tasks of SHAs is to create Statements of Health (SOH) by analyzing the NAP client and pass these statements to the NAP agent component (*discussed below)*. The process is also known "posture assessment" (as discussed in chapter 3). A SOH is a unit corresponding to

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 68 of 114

a posture data (or measurement), e.g., A SHA for virus can produce a SOH stating, "ANTIVIRUS STATUS = ON" which indicates that the Antivirus software on the client is enabled.

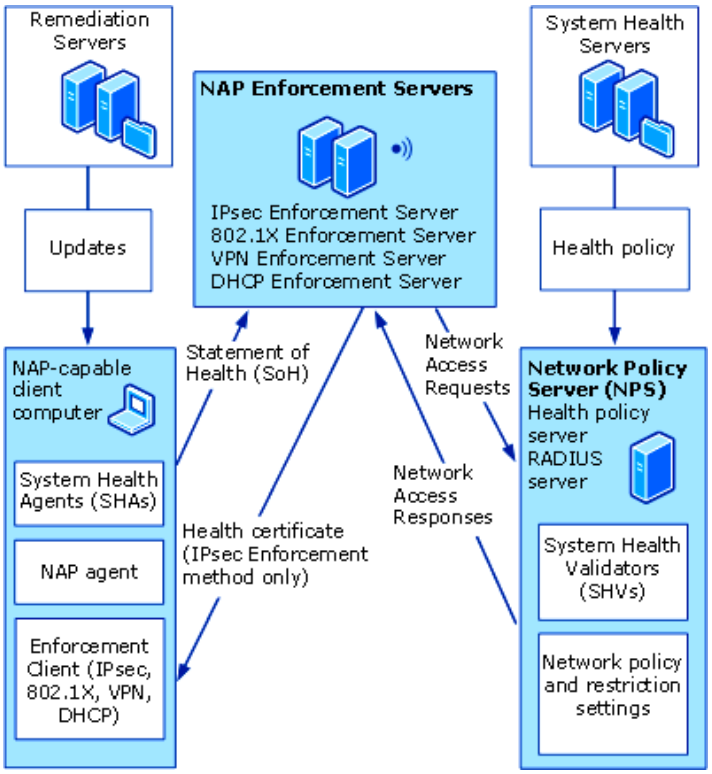

Figure 6.1 Network Access Protection architecture [25]

Secondly, the SHA is responsible for receiving *Statement of Response* (SOR), *discussed below*). These statements contains the remediation information for the NAP Client which are used for the remediation process. E.g., SOR may state, "ANTIVIRUS SIGNATURE=OLD", indicating that there is a requirement of a new antivirus signature. So SHA uses SORs to interact with the remediation resources for updating its

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 69 of 114

compliance. In this case it will install new signatures residing on the antivirus resource. 3rd party vendors can introduce new SHAs using the SHA API (*discussed below*) as add-ons to the NAP platform.

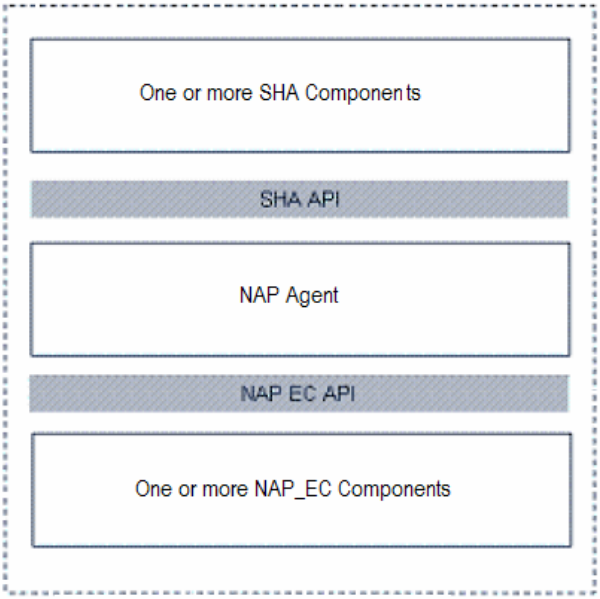

Figure 6.2 NAP client sub-components

- ***SHA API layer*** provides API for interaction between SHA components and NAP agent. NAP agent and SHA(s) communicate through this interface. SHA API provides functions, such as SHA(s) registering to the NAP agent, NAP agent querying SHA(s) for SOHs , SHAs passing SOHs to NAP agent, etc. It is also used for 3rd party vendors to integrate with new SHA(s) with the NAP Client.

- ***NAP agent*** maintains client's compliance by collecting SOHs from SHA(s) and further communicates this information to Enforcement Components (EC, *discussed below*).

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 70 of 114

- ***NAP EC API layer*** is an API for interaction between EC components (*discussed below*) and NAP agent. NAP agent and EC(s) communicate through this layer, providing functions, such as EC(s) registering to the NAP agent, EC(s) querying NAP agent for machine's compliance, EC(s) passing remediation information to NAP agent, etc. 3rd party vendors can use this API to introduce new EC components.

- ***Layer of EC:*** Enforcements Components (EC) are specific for the enforcement technology being used. By the use EC(s), health policy requirements are enforced on the NAC Client. This layer can consist of one or more Enforcement components. Till now, Following are the enforcement components available:

- *Internet Protocol security (IPsec)*
- *IEEE's 802.1X*
- *VPN*
- *Dynamic Host Configuration Protocol (DHCP)*

These components pair-up with Enforcement Server (ES, *discussed below*) components present on the NAP Server (*described below),* e.g., For DHCP enforcement, an EC will be the client component and an ES will be the server component. Microsoft Corp. defines *"enforcement"* API (for ES and EC component), so that 3rd party vendor(s) can integrate their enforcement technique(s) with NAP platform.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 71 of 114

NAP Server

NAP servers or NAP enforcement servers are computers that support NAP platform, i.e., machines having Windows Server "Longhorn". A NAP Server is comprised of one or more ES (Enforcement Server components), which corresponds to EC(s) present on a NAP Client.

A NAP ES component on a NAP server obtains the list of SOHs from its corresponding NAP EC on a NAP client and sends them to the NPS server. Likewise it receives list of SORs from NPS server and forwards it to its corresponding NAP EC(s) on the NAP client. The communication between NAP Server and NPS Server (*described below*) is done by RADIUS (Remote Authentication Dial-In User Service) protocol.

As discussed above, the enforcement services include; IPSec, VPN and DHCP but does not includes 802.1X, the 802.1X ES is implemented in the NPS component on the NPS server (described below). Also, in case of IPSec enforcement technology, ES component acts as a Health registration Authority (HRA) which is responsible for granting Health Certificates on the basis of client's compliance. In an IPSec enforcement setup the network is viewed as rings as presented in the following Figure 6.3, These rings are; *Secure Network, Boundary Network and Restricted Network.*

- ***Secure network:*** This area of the network is considered to be the most secure, it has long term health certificates. Incoming and outgoing communication within this area or outside of this area requires health certificates. This area contains NPS Servers (described below) and Health Policy Servers (described below).

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 72 of 114

- ***Boundary network:*** The communication between boundary network and restricted network does not require a health certificate because in the start the client needs to communicate with the HRA for acquiring a health certificate, or if a NAP client is non-compliant and is in the restricted network, it needs to interact with the remediation server for remediation. The communication between boundary and secure network requires Health Certificate. NAP servers and remediation servers are present on this layer.

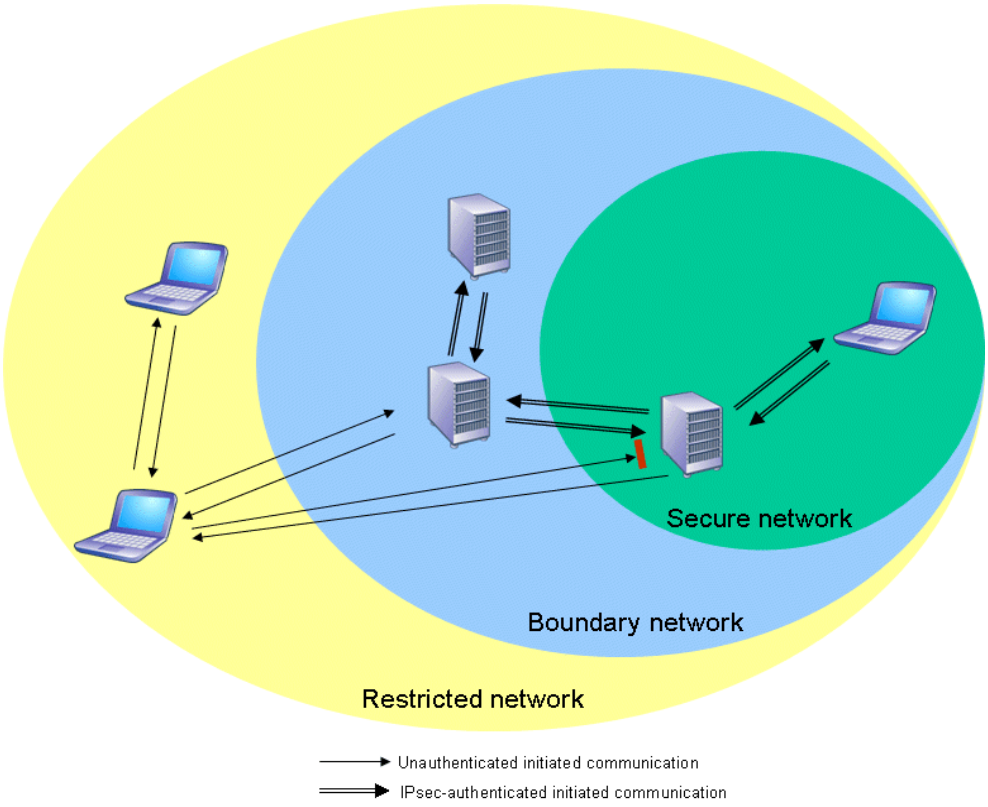

Figure 6.3 IPSec divisions [15]

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 73 of 114

- ***Restricted network:*** This area requires health certificates to communicate with the secure network.

NPS Server

Network Policy Servers (NPS) are computers that support NAP platform. That is machines having Windows Server "Longhorn". NPS is the Windows implementation of a RADIUS (AAA) server. NPS is the replacement for the Internet Authentication Service (IAS) in Windows Server 2003. Network access devices and NAP servers act as RADIUS clients to an NPS server (a RADIUS server). NPS performs authentication and authorization of a network connection attempt and, based on configured system health policies, determines computer health compliance and how to limit a noncompliant computer's network access. A NPS server can be further divided into more sub-components; the following Figure 6.3 illustrates the sub-components of a NPS server:

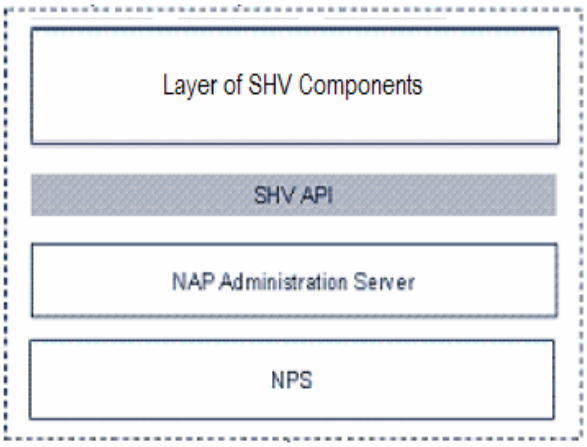

Figure 6.4 NPS sub-components

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 74 of 114

- ***Layer of SHV components*** is comprised of one or more SHV components. SHV refers to System Health Validator, there can be one or more validators present on this layer. SHV define system compliance requirements and validates Statements of Health (SOH) with corresponding policy servers (corresponding to antivirus, spyware, operating system patch, etc.). SHV-SHA pairs are specific to a security application.

- ***SHV API layer:*** This API defines the interaction between SHV components and NAP administration Server (*discussed below).* Works same as the NAP client's SHA layer; registers SHV(s) to the NAP Administration Server, etc. 3rd party vendors can use this API to integrate their SHV with the NAP platform.

- ***NAP administration server:*** This layer helps in communication between NPS and SHV(s) and performs system compliance analysis based on configured set of policies.

- ***NPS layer:*** This layer aids in communication between NAP server(s) and NAP administration server. This layer also integrates the EC component for 802.1X enforcement. Following Figure 6.5 elaborates the communication between NAP servers(s) and NAP administration server.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 75 of 114

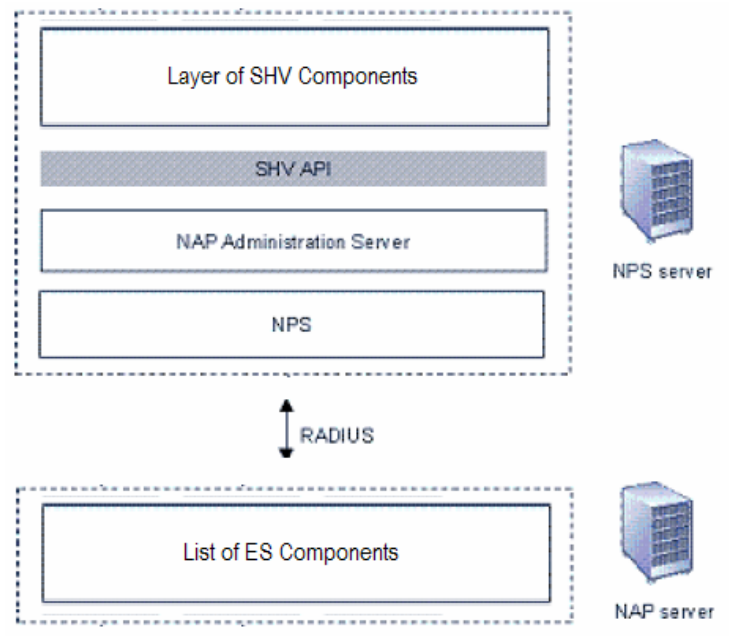

Figure 6.5 Communication between NPS and NAP servers[15]

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 76 of 114

7 Network Admission Control

By Cisco Systems Inc.

Cisco Systems Inc. is famous for manufacturing network and communication technology, Cisco Systems Inc. have provided their services for sectors such as; education, government, health care and more. Cisco Systems Inc. industrial solutions cover areas of switching, routing, wireless, IP telephony etc. According to a web article posted at ZDNet, a research carried by In-Stat shows that Cisco Systems Inc. controls 70% of enterprise router market [4]. Cisco Systems Inc. is direct competitors with Juniper Networks, Inc. and 3Com networks.

7.1 Background

Cisco Systems Inc. started off with their concept of "*self defending network*", which is to embed security features in the IP-network by delivering new network threat defense mechanisms, the idea is to integrate security throughout the networking infrastructure. Cisco's Network Admission Control (C-NAC) is part of phase-2 of self defending networks, which focuses on network access control. We wont be discussing "*self defending network*" in this study.

C-NAC is available in two forms; *Cisco NAC Appliance* and *Cisco NAC framework. NAC Appliance* is an appliance-based approach (i.e., "functionality in the box") and *NAC framework* focuses on complex network architectures and defines a vast range of security policies according to today's need. We have included both of these forms in our thesis report, to give a broader view of Cisco's approach towards network access control.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 77 of 114

7.2 Network Admission Control

7.2.1 Introduction

C-NAC, uses the network infrastructure to enforce security policies on all devices accessing the protected network. C-NAC ensures that all devices prior connecting to the network complies to the defined security policy and to isolate those devices which are not able to meet up with the policy. Devices which are non-compliant and are isolated (or “quarantined”) can remediate, and can come back to a "compliant" status by upgrading their machines with policy specific data and hence can be part of the secure network.

C-NAC emphasis on the enforcement of network policy to be implemented at the core network level (e.g., at switches or routers), instead of relying on hosts or softwares which are responsible for managing their selves (e.g., a software residing on the host enforcing policies). Also, Cisco's customers can utilize their existing network investments on security applications, as C-NAC collaborates with security solutions from Altiris, IBM, MCAFEE, SYMNATEC, TREND MICRO and more than 70 additional companies are partners with C-NAC framework approach, by this solutions from various vendors can be integrated to the C-NAC.

C-NAC considers network location and support access methods such as LAN, wireless, remote access and WAN. Cisco Systems Inc. offers to enforce policy on every device, whether unmanaged or guest access. C-NAC delivers vast range of compliance data, e.g., besides examining antivirus, firewall or security patches, it

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 78 of 114

can also check up with the encryption methods being used in VPN, ensuring that whoever remotely connects to the network, the confidentiality and integrity of the data is not compromised. Cisco Systems Inc. defines policy on basis of user-id and compliance level therefore decreasing the risk from non compliant and unknown devices.

Cisco Systems Inc. framework is built on standards such as Extensible Authentication Protocol (EAP), User Datagram Protocol (UDP), 802.1X Remote Authentication Dial In User Service (RADIUS), etc. In some cases these technologies require enhancement to support NAC, Cisco Systems Inc. is working with IETF for standardization of these extensions, and also standardizing of C-NAC technology.

7.2.2 Cisco NAC Appliance

The *Cisco NAC Appliance* (formerly known as Cisco Clean Access) provides rapid NAC deployment with self-contained endpoint assessment, policy management, and remediation services, including patching and updates from Microsoft Corp. and leading antivirus vendors. C-NAC Appliance-based approach reduces degree of complexity as NAC Appliance does not require change in prior network infrastructure, it can be deployed as an overlaying approach.

C-NAC appliance, have two server components, illustrated in Figure 7.1, *Clean access manager* and *Clean access server*.

- ***Clean Access Manager (CAM)*** centralizes management for administrators through HTML-based interface. It servers as an AAA RADIUS server, the

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 79 of 114

job of clean access manager is to define security requirement policies, remediation needs for the protected network.

- ***Clean Access Server (CAS)*** component performs device compliance checks as the user asks for the access to the network, Serves as an enforcement device for enforcing compliance requirements. This device initially opens a login page at the end-user, or the user can download the agent and access through the agent.

- ***Cisco Clean Access Agent (CAA)*** is an optional lightweight client which is responsible for deep inspection of the machine's security profile by analyzing registry settings, services etc. This agent makes sure that the client is fully equipped with security applications that comply with company's security policies. Users can also authenticate using this agent. CCA is support for windows and MAC (used only for authentication).

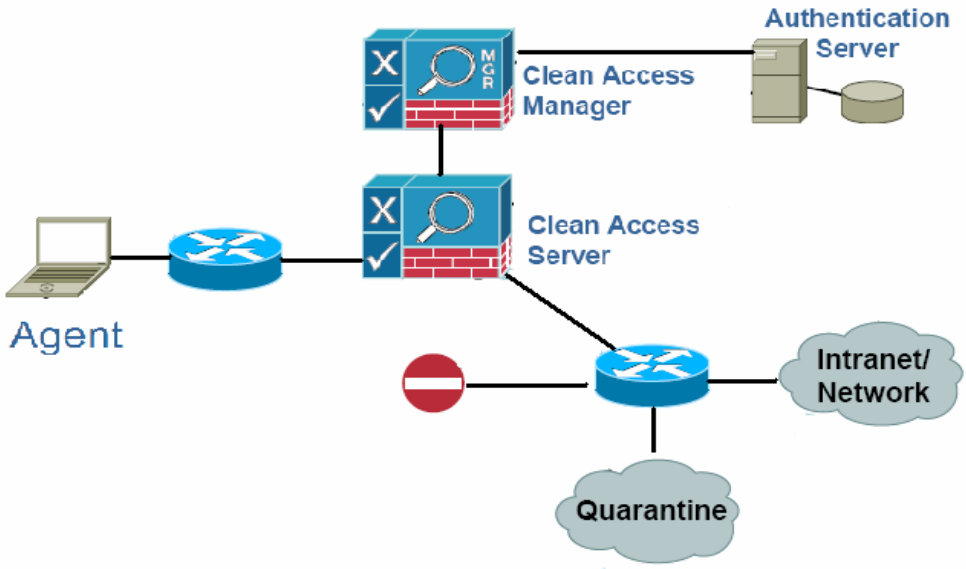

Figure 7.1 Core components of NAC Appliance [14]

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 80 of 114

7.2.3 Cisco NAC Framework

Cisco framework approach to NAC integrates the network infrastructure and products from third-party solutions to enforce security policy compliance on all endpoints. C-NAC framework is an initiative supported by more than 75 manufacturers of leading antivirus and other security and management applications. C-NAC framework uses new and existing network infrastructure for the enforcement of security requirements. Also, Cisco Systems Inc. has licensed endpoint software technology to NAC partners to enable to communicate with C-NAC.

Cisco Systems Inc. recommends NAC framework on the basis of the following checklist:

- *Extensive NAC partner integration is a starting requirement*
- *Deploying a NAC-compatible 802.1x solution is needed*
- *Cisco Secure Access Control Server (ACS) is required as the central policy server in the C-NAC deployment*

7.2.3.1 Components of Network Admission Control Framework

The following Figure 7.2 presents the architecture of C-NAC framework approach.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 81 of 114

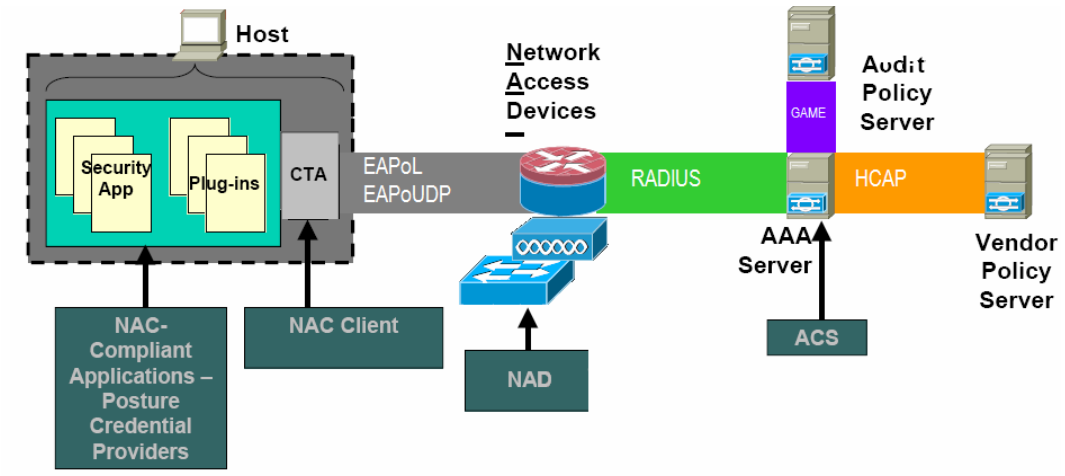

Figure 7.2 Core components of NAC Framework [6]

This includes *Cisco Trust Agent (CTA), Cisco Network Access Device (NAT), Cisco Secure Access Control Server (ACS), Vendor Policy Server (VPS)* and *Audit Policy Server (APS).*

- ***Cisco Trust Agent*** (CTA) is a software residing on the endpoint device, its presence on the client machine is compulsory. The job of CTA is to collect measurements related to posture of device and to communicate them further to the network. CTA is a core component of NAC, CTA coordinates with Cisco Security Agent (a separate product of Cisco Systems Inc. used for various security operations), antivirus software, or other required 3rd party vendor security application(s). CTA itself determines and communicates the OS version and patch level of the host. CTA includes the supplicant for 802.1X setup which is used for 802.1X-based connections. CTA can detect a change in posture and can request NAD for "posture assessment". Currently, CTA is available for Windows and Redhat Linux.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 82 of 114

Following Figure 7.3 illustrates the architecture of a Cisco Trust Agent, CTA is comprised of two components: *Posture Plugin* and *Posture Agent.*

- ***Posture Plugin*** is a software component (DLL) provided by a 3rd party vendor residing on the host machine responsible for providing posture credentials to the Posture Agent. There is one posture plugin for each vendor and/or application type.

- ***Posture Agent*** is also a software component residing on the host machine and acts like a broker responsible for collecting posture credentials from the *Posture Plugin* and to communicate it to the network. The agent uses *EAP over UDP* (EAPoUDP for NAC layer 2 IP enforcement method) or *EAP over 802.1X* (EAPoL for NAC Layer-2-based 802.1X enforcement method) to communicate with the network.

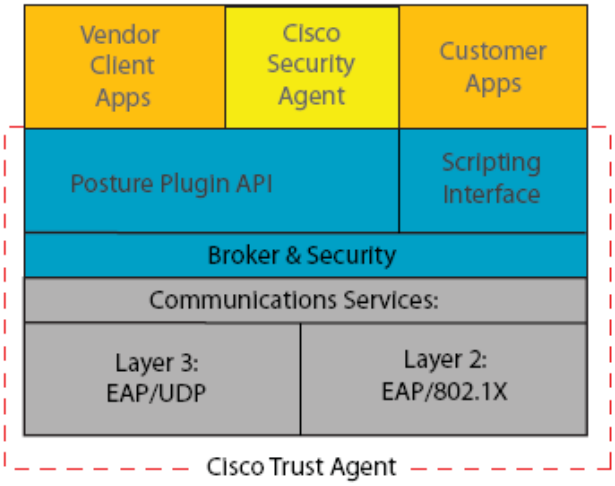

Figure 7.3 Cisco Trust Agent architecture [19]

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 83 of 114

- ***Cisco Network Access Device*** can be any device which is compatible with C-NAC, are used for network enforcement of security policies. NAD are Cisco Systems Inc. products which are C-NAC enabled and corresponds to network deployments such as LAN, WLAN, VPN remote access and MAN.

  Cisco Systems Inc. supports following enforcement methods:

- ***Layer-2, IP-based*** enforcement method does not involve identity-based authentication. An endpoint is assessed for its applications posture, by validating posture and applying the policy at the enforcement point in the form of Access Control List downloaded from the ACS server. Posture assessment is triggered when a network devices senses any ARP request or DHCP binding. Posture information is communicated to the network by EAP over UDP (EAPoUDP) protocol.

- ***Layer-2, 802.1X-based*** uses user identity, machine identity and machine posture for the validation of security policy. Uses EAPoL in a 802.1X setup. Cisco Systems Inc. has defined two EAP types for C-NAC, which provide security layer in EAP, one is EAP-FAST and the other one is EAP-TLV, both of these protocols are submitted in IETF as a draft for standardization.

- ***Layer-3, IP-based*** works the same way as layer-2-based approach, but instead of ARP requests it can only sense for DHCP bindings.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 84 of 114

- ***Cisco Secure Access Control Server (ACS)*** is a RADIUS server used for the management of policies and is responsible for endpoint compliance validation. It coordinates with policy servers provided by 3rd party vendor integration as illustrated above in Figure 7.3. The communication between vendor solutions is done through the Host Credential Authorization Protocol (HCAP). ACS forwards client EAP-based credentials to one or more vendor servers through HTTP(S) sessions, through these sessions the ACS then receives specific responses and optional notification messages from each vendor server. The ACS can also use Cisco's proprietary standard TACACS+ for communication, the communication of ACS is either RADIUS-based communication or TACACS+-based, but not both.

- ***Vendor Policy Server (VPS)*** is a server provided by a specific vendor which corresponds to a specific security application. The ACS can forward security-specific credentials to specific VPS for validation of specific posture. The communication between ACS and VPS is done by the HCAP protocol.

- ***Audit Policy Server (APS)*****:** ACS triggers the auditing of NAC Agentless Hosts through 3rd party vendor audit server. ACS then polls periodically for audit decisions. The audit server responds with a posture state when the audit is completed. Generic Authorization Message Exchange (GAME) protocol is used between ACS and APS, they communicate via HTTPS extending SAML (Security Assertion Markup Language).

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 85 of 114

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 86 of 114

8 Analysis and Comparison of NAC Technologies

The concept of Network Access Control (NAC) technology is a new initiative in network security genre. Cisco Systems Inc. first introduced NAC somewhere in 2003. NAC is comprised of different components and emerging technologies ranging from various hardware and software entities. According to Forrester research, some 40% of enterprises started adopting NAC initiatives in 2006 and about 52% of firms indicated the need for access control across all network mediums: wired, wireless and remote access [21]. This research indicates the adoption of NAC in the marketplace.

There is a great of need of standardization and interoperability of NAC. Companies need to secure their investments on network infrastructure. By adhering to standards, these investments can be utilized efficiently with NAC innovation. Without standards, the NAC world is an amalgam of technologies and will remain an obstacle for companies to adopt it. Following are the core issues that are obstacles for the wide adoption of NAC:

- Presence of ***numerous platforms*** makes the NAC market confusing. Every company is offering their solution with a particular set of functionality and with a unique architecture. Some are adhering to set of standards and some are following proprietary standards. No one is providing a complete NAC solution with all the required functions but only a subset of functions.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 87 of 114

- Currently, the NAC is in its standardization phase. NAC ***lacks interoperability*** among its functional and architectural pieces. Such obstruction locks up the customer with a particular vendor's approach to NAC. As solutions are not interoperable, customers are left with no choice, either they have to follow the same vendor or have to discard their existing infrastructure to replace it with vendor's setup, which is almost impractical and results in great financial loss. Customers need assurance that their investments are safe and are best utilized.

- ***Investment Issues:*** The NAC technology introduces new elements to the networking infrastructure. Some platforms leverage from existing infrastructure, some requires introduction of new entities with replacement of existing networking equipment, resulting in heavy investments. Companies should need to evaluate their motivation for NAC which includes the potential costs/benefits, as management and installation of new equipment raises monetary concerns. To determine the Return On Investment (ROI) of a security solution is a difficult task, before adoption of NAC companies should evaluate the cost involved in the installation of architectural and functional elements of NAC.

8.1 Comparison Overview

Following are the two tables, comparing architectural elements (Table 1.1) and functional elements (Table 1.2).

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 88 of 114

Architecture	***Trusted Network Connect***	***Unified Access Control***	***Network Access Protection***	***Network Admission Control Appliance***	***Network Admission Control Framework***
Vendor	***The Trusted Computing Group***	***Juniper Networks, Inc.***	***Microsoft Corp.***	***Cisco Systems, Inc.***	***Cisco Systems, Inc.***
Solution Type	Hardware Software	Appliance	Software (Servers)	Appliance	Appliance
Enforcement Points	802.1X Switch, 802.1X Access point, VPN Server	802.1X Switch, 802.1X Access point, Juniper Firewall	Machines having Windows Longhorn Server	Cisco clean access Server, Switch and Access point	Cisco-only equipment; Switch, Router, Firewall & VPN appliances
Deployment Setup	N/A	Inline Firewall, switch Out of band	N/A	Inline and Out of band	Out of band
TNC Support	N/A	Yes	Later	No	No
Cross Platform	Yes, any platform	Windows, Linux, MAC	Windows	Windows	Windows. Linux
Enforcement Technologies	802.1X VPN	802.1X IPSec SSL VPN	802.1X IPSec DHCP VPN	DHCP	802.1X DHCP

Table 8.1 Comparison overview of architectural elements

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 89 of 114

Architecture	***Trusted Network Connect***	***Unified Access Control***	***Network Access Protection***	***Network Admission Control Appliance***	***Network Admission Control Framework***
Vendor	***The Trusted Computing Group***	***Juniper Networks, Inc.***	***Microsoft Corp.***	***Cisco Systems, Inc.***	***Cisco Systems, Inc.***
User authentication	Yes	Yes	Yes	No	Yes
802.1X Support	Yes	Yes	Yes	No	Yes
TPM Chip Capability	Yes	No	No	No	No
Agentless Support	N/A	Yes, Infranet Controller	No	Yes, Cisco Clean Access Server	Yes, Audit Servers
Third Party Support	Yes	Yes	Yes	Limited	Yes
Post-Admission Control	N/A	Juniper Firewalls, 3rd party plugin	Not by default, 3rd party plugin	Not by default, 3rd party plugin	Requires additional components
Quarantine	VLAN, ACL	VLAN, ACL, Agent	VLAN, ACL	VLAN, ACL	VLAN, ACL
Auto Remediation	N/A	Yes, Limited	Yes, Limited	Yes, Limited	Yes, Limited

Table 8.2 Comparison overview of functional elements

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 90 of 114

8.2 Issues in NAC

Following are the set of issues we have discovered in our study:

8.2.1 Architectural Setup

- An ***inline*** appliance connects between the access switch and the core network. The traffic to the network passes through the inline device. Inline device can deeply inspect the packets which are passing through it. If the inline appliance detects any malicious packets/activity, packets are immediately dropped and the policy server is notified, and accordingly the policy is enforced. There are some *advantages* and *disadvantages* with this approach:

  One of the advantages of inline devices is that, it suits best for post-admission control. Once the devices are on the network, as the traffic generated by device passes through these inline setups, these appliances can deeply inspect packets for any malware activity. Inline appliances may vary in functionally ranging from layer-3 to layer-7 capabilities. Inspecting the traffic thoroughly gives granular access control (inspection on various layers).

  The disadvantage of inline appliance is that it provides a single point of failure. If an inline device fails, the network goes down. Also, the deployment and testing of such appliances require shutting down the intra-network, making it inflexible for deployment. Another disadvantage is that an appliance can only protect the traffic which passes through it. The

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 91 of 114

appliance may not be able to take account of the complete network topology, e.g., if an inline appliance is implemented near the network core and the responsibility of the appliance is to keep one network segment safe from another. In this scenario, a malicious host can infect other hosts attached to the same network segment, and may infect other neighboring segments which are not protected by an inline device.

In addition, such devices need to be highly efficient in terms of their processing capability, e.g., in an IP telephony setup, inline setup might produce jitter and delay in communication. In this case, inline devices may require high performance-based ASIC processors, which can be costly.

- In an ***out-of-band*** setup, the appliance usually connects with the mirror port of a switch. Such that, the traffic passes through the switch is replicated for the appliance, and the out-of-band appliance can inspect the traffic in a passive manner, causing no delays in the network traffic.

  Out-of-band appliances are easy to incorporate, as they do not introduce single point of failure, they only need to attach to the switch, making them easily deployable during working day. This makes the deployment of out of band appliances very flexible. Also, such systems require less processing power as compared to inline devices.

  The monitoring of out-of-band appliances relies on endpoint technologies or functionality of some other networking equipment like switch or router. Out-of-band appliances need to be aware of devices which are on the network. The problem of infecting local segment also holds for these appliances. As, the device may not be able to detect the infection within

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 92 of 114

the local network segment. Also, the network traffic does not pass through these devices, these appliances are not able to deeply inspect the network traffic, making them less capable for post-admission capabilities. Furthermore, debugging in such scenarios is problematic, it is difficult to determine where a problem occurred. The occurrence can be at the appliance or at the switch.

8.2.2 Vendor Lock-in and Interoperability

Most of the NAC solutions offered in the market are based on proprietary standards, standards such as Cisco's, Microsoft Corp.'s etc. E.g., Cisco's Network Admission Control framework requires all the networking equipment (switch, routers, etc.) to be exclusively from Cisco Systems Inc. Cisco's functionality for Virtual LAN or 802.1X-port-based access control can only work with equipment from Cisco Systems Inc. This includes Cisco switches and Cisco Access Control Server. By such approach Cisco Systems Inc. is putting customers in a vendor lock-in situation. Likewise Microsoft's Network Access Protection requires installing Windows Vista and Windows Longhorn on every machine present on the network. Such restructuring of infrastructure requires humble investment.

Till now, there is no solution which is completely built on open standards except the Trusted Computing Group's (TCG)-Trusted Network Connect (TNC) architecture. Even Juniper Networks, Inc. is adopting a part of TNC guidelines. Primarily, that any security application adopting TCG guidelines can communicate with Juniper's UAC agent and, secondly, Juniper Networks, Inc. can leverage from 802.1X enabled switch from any vendor. Juniper firewalls are not TCG-TNC compliant.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 93 of 114

8.2.3 802.1X Port-based Access Control

802.1X port-based access control have greatly affected the evolution of NAC. By 802.1X a user can be authenticated before the assignment of an IP address. This is only possible through IEEE's 802.1X port-based access control standard for wired and wireless LANs. There are advantages and disadvantages of 802.1X setup.

- ***Pros:*** 802.1X is more secure because a user is assessed before an IP address is assigned to it, i.e., before the user is part of the protected network. During an 802.1X session, 802.1X blocks the traffic on the port, only limited layer-2-based traffic is allowed. By deploying 802.1X setup, the chances of malware to affect the network are reduced. With strict port-based access control, 802.1X helps in preventing rogue devices to be part of the network.

- ***Cons:*** When the user is successfully authenticated through 802.1X, the user is assigned an IP address and, the port is opened for communication. If the user performs any malicious activity above layer-2, that activity is undetected by an 802.1X setup. Hence, an authenticated user can perform malicious activities by exploiting the above layers.

  802.1X requires installation of supplicant software on a machine to communicate with an 802.1X-based setup. Installing, configuring and managing of supplicant software on each and every device on the network are complex tasks. With 802.1X setup, quarantine is carried through VLAN assignment. 802.1X only works with switches implementing RFCs required for VLAN. VLAN management also requires the reconstruction

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 94 of 114

of network segments, e.g., introducing quarantine network to current network setup. Also, 802.1X introduces new attributes for authentication, the RADIUS server should be capable to support these new bindings.

802.1X standard will take time to prevail in the marketplace, as most of the switches being used today, do not support 802.1X functionality. According to Forrester Research mentioned in [2], "*…only about 15% of all enterprises are underway with 802.1x-enabled switches*." This is primarily because the cost involved in it 802.1X setup. "*Although Microsoft includes 802.1x in all versions of Windows XP, only 17% of enterprises have actually deployed Windows XP to all desktop PCs. Also Microsoft's supplicant is not robust enough for all enterprise as a result many enterprises will need to purchase a standalone 802.1x supplicant*".

802.1X-based connectivity requires supplicant software installed on the client's machine. Devices like printers, gaming consoles, etc., do not have the capability to install supplicant software. These devices can not communicate with an 802.1X-based setup and are usually exempted from the authentication process. This exemption is a potential source for malicious activities (*discussed below in 8.2.7*).

802.1X-setup is recommended by all the architectures that we have discussed in our thesis. But only relying on 802.1X control is not effective. 802.1X setup is only able to read traffic on layer-2, it cannot understand traffic from above layers. So, there is a requirement of a network entity which can analyze the traffic beyond layer-2 capability. E.g., Juniper Networks, Inc. firewalls play a vital role which performs deep inspection of traffic from layer-3 to layer-7.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 95 of 114

One of the advantages of the Juniper's UAC is that, it was initially built with Juniper Networks, Inc. firewalls and later on was extended to 802.1X capability. UAC with 802.1X capability and Juniper firewalls provide stronger access control, covering capabilities from layer-2 to layer-7.

8.2.4 Post-Admission Control

Most of the platforms lack proper post-admission Control. The architectures discussed in our thesis are based on pre-admission control and lack default capability of post-admission control. Post-admission control refers to the monitoring of devices on the network for any malicious activity (*discussed in chapter 3.2.8*). An exception is, Juniper's UAC, which includes Juniper Firewalls, which can play an important role in threat mitigation. Currently, post-admission control is achieved through software support, by integrating solutions from 3rd party vendors e.g., In Cisco's NAC, threat management is conducted by security agent software (which is a separate product), which also relies on the support from other security applications. The discussed architectures *by default* do not support post-admission control capabilities, requiring additional components.

8.2.5 Automatic Remediation

One of the effective features of NAC is automatic remediation, but the functionality is immature at the moment. Automatic remediation is not achievable in true sense, E.g., Automatic remediation offered by Microsoft Corp. NAP, Microsoft NAP can automatically only remediate their own security products, but they cannot auto-remediate clients having solutions available by other vendors. This can cause delay in network connectivity for employees. Increase of

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 96 of 114

investment on *helpdesk* department will be required as more number of users will be complaining about their connectivity problems.

8.2.6 Cross Platform Support

Most of the NAC marketplace is driven around Microsoft Windows technology. Less support is available for other platforms. Machines with platform other than Microsoft Windows are usually assessed through agentless vulnerability scans. As agent software is not available for these platforms. In most of the situations platforms beside Windows are declared as exceptions (*discussed in 8.2.7)* to the NAC.

Less support for other platforms beside Microsoft is a threat to the open source software community, in a way that if assessment is exercised on the basis of trusted applications, a set of open source applications might not be included in the list of trusted applications.

8.2.7 Unmanaged Clients (Exceptions)

Unmanaged clients are a set of machines present on the network like printers, gaming consoles, scanners, etc. These devices usually do not have support for any supplicant software, so for such devices exception rules are defined. On default, NAC is bypassed for such exceptions. These exception points may leave security holes in the network infrastructure. E.g., an attacker can disconnect the printer's cable, and by MAC spoofing, can spoof a printer's MAC address. By doing so, the device can connect to a network segment.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 97 of 114

In practice a printer might have access to limited resources. But, consider an IP-Phone which can connect to the internet. If MAC spoofing is performed in this case, the device can gain access to the internet or any other resources which are available to the IP-Phone.

NAC does not address exceptions very well. NAC architectures should have support for other available platforms. In some practical environments, open source software is more prevalent than Microsoft Windows, e.g., a university's intra-network. Usually, most of the machines have sun-solaris platform. NAC should cover a range of other platforms beside Microsoft Windows.

8.2.8 Posture Spoofing

One of the biggest problems of NAC is the "*lying client*", a machine which basically lies about its posture information and hence bypasses NAC. In March 2007, at the black hat conference, NAC client was demonstrated that lied about its posture assessment and bypassed the NAC. The study [13] was done by analyzing the traffic a CTA generates, and by reverse engineering the CTA, the researchers were able to determine where the posture data lied and how a user designed posture can be injected. In addition, a vulnerability was discovered in Clean Access Agent (Agent in Cisco NAC appliance), which exploits the TCP/IP stack and hence used to bypass NAC [1].

Reliance on agent software can be misleading, there should be a hardened process which relies on hardware security, TPM with its capability of "*root-of-trust*" can help in such scenarios, so that posture information is trusted and not spoofed. A number of laptop vendors including Dell, Fujitsu, Hewlett-Packard and Lenovo,

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 98 of 114

already include trusted hardware modules in their product lines. By adopting TPM capabilities, the environment can be protected from dangerous attacks such as root kits.

8.2.9 If NAC fails?

In the study of these Network Access Control technologies, not a single vendor specifies a real-time backup plan for a NAC failure. NAC should accommodate the failure of any component occurring in real time. NAC involves a number of architectural and functional components, debugging in such a setup might be problematic, it will be hard to detect where the error actually occurred. Additionally, it will be difficult to conclude the responsible authority for a NAC component failure, as NAC is comprised of numerous components.

8.2.10 Unified Policy

NAC involves people from network, security and administrative departments. Defining and configuring a unified policy for all the interfaces in a NAC platform is challenging requires intensive collaboration among administrative staff.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 99 of 114

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 100 of 114

9 Conclusions and Future Work

Network security provides mechanisms to offer confidentiality, integrity, and availability guarantees for the protected network. Which set thereof is desired in any given situation is defined by a security policy. Network Access Control technology (NAC) provides a set of mechanisms that can be used to enforce such policies. If, e.g., the network is not available, there would not be any business processes, there will be no inter-communication between customers and partners. If the integrity of the network is compromised there will be a lack of trust between customers and partners. Network downtime can cost a lot of money and can result in lost of productivity and revenue.

Today, to satisfy the security requirements of typical organizations and corporations, there is a need to protect the network not only at the perimeter, but also against inside threats. A comprehensive approach is required, so that the network remains safe and its ongoing operations can be guaranteed. The Network Access Control vision is instantiated with a set of technologies by which a network can be protected from non-compliant machines. From the discussion in earlier chapters, we conclude that the requirement for adopting NAC technologies is not an exception. Network infrastructures are dynamic in nature, causing traditional security management techniques to be insufficient to keep up with the ever constant change.

The goal of NAC is to control the access of endpoint devices to the network. NAC enforces endpoint device compliance in addition to other, traditional network security mechanisms, such as user authentication. One of the key issues with NAC is that it relies on collaboration of new technologies with existing network

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 101 of 114

and security paradigms. Such integration is evolving, and is in its early stages. Numerous companies have come up with their own NAC architectures and every company targets this approach with the same goal, i.e., to *control access to the protected network*.

With the popularity of IEEE's 802.1X standard, it establishes port-based access at the port-level. Although 802.1X enabled equipment is not yet pervasive in large-scale deployments, we expect network architectures to be converging toward a situation where endpoint admission is carefully guarded by employing 802.1X technology. 802.1X provides control over endpoint devices using layer-2 capabilities.

While the NAC market is overwhelmed by a large number of technologies that can solve parts of the NAC vision, they lack interoperability, often ignoring the need for standards. Consequently, we consider the NAC market to be very immature in nature and expect a consolidation of technologies. Eventually the movement for standardization will move on. For now, companies are providing appliance-based (*functionality in a box)* solutions, so that organizations can instantiate the NAC vision, by starting with limited access control capabilities and in future can upgrade to a comprehensive NAC technology.

In the future, we expect the Trusted Computing Group (TCG) to play a pivotal role in the NAC world. For example, Microsoft Corp. has agreed on following the TCG specifications. On the other hand, Cisco Systems Inc. is not interested in the TCG specifications at all, but recently is working with IETF for the standardization of their solution. IETF is also playing a part in standardizing the interfaces of NAC components, their initiative is known as Network Endpoint Assessment (NEA). NEA will be clear with their motives in the mid of 2007 [34].

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 102 of 114

Furthermore, Microsoft Corp. and Cisco Systems Inc. have also agreed on the interoperability of their NAC solutions. The details of these plans can expected to be revealed somewhere in summer of 2007 together with the release of Microsoft "Longhorn" server product. Companies are relying on the details of the Microsoft-Cisco collaboration, so that they are in a position to evaluate the directions of NAC vision. Some companies have decided to wait for the NAC industry to be more mature. There is no solution available in the market which adopts the functionality of a complete NAC. Currently companies can analyze and be prepared for the changes required in their network infrastructure. For instance, 802.1X integration require changes to the network infrastructure. Companies should be aware of such facts associated with the NAC vision, so that they can accommodate these requirements in the future.

Also, the TCG initiatives for *trusted computing* will also advance. The TPM chip technology is expected to gain further popularity. Kay states in [20] that it is predicted that until the end of 2010 there will be about 250 million TPM chips shipped globally. TPM technology will advance and play a pivotal role in achieving features of *trusted computing*. TPM chips with their *platform-authentication* capabilities can assist NAC in providing a strong *root-of-trust*. With this hardware based-*trust anchor* policy servers can trust clients' compliance measurements.

This thesis is limited to the analysis of four NAC schemes, though in the current marketplace (till end of May 2007), there are other NAC architectures available, implementing NAC functions in a unique way. In the future our comparative study could be extended to include other architectures as well as the dynamic developments of the NAC vision.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 103 of 114

Furthermore, detailed insights into the various different NAC technologies we studied could be gained by hands-on experimentation with these technologies and even more comprehensive details of NAC could be formulated after studying a representative set of organizations that are already using NAC technologies in their network deployments.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 104 of 114

Bibliography

[1] A. Gal and J. Feise, "Cisco NAC Appliance Agent Installation Bypass Vulnerability", Security Focus, Aug. 2006; http://www.securityfocus.com/archive/1/444737/30/0/threaded.

[2] A. Harding and R. Risser, "Secured and Assured Networking with an Enterprise Infranet", white paper, Juniper Networks; http://www.juniper.net/solutions/literature/white_papers/200144.pdf.

[3] A. Miller, "Leveraging your Networking Security For Unified Access Control", Juniper Networks; http://www.idgsecurityworld.com.sg/downloads_kl/ Juniper_Andy_Miller_slide_Malaysia_event.pdf.

[4] A. Moskalyuk, "Cisco Controls 70% of enterprise router markets", IT facts, ZDnet Research, 2006; http://blogs.zdnet.com/ITFacts/?p=12142.

[5] "Computer Crime and Security Survey", CSI/FBI, 2005; http://www.usdoj.gov/criminal/cybercrime/CSI_FBI.htm.

[6] D. D. Capite, *Self-Defending Networks: The Next Generation of Network Security*, Cisco Press, 2006.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 105 of 114

[7] D. Hendrickson, *Network Admission and Access Control, Product Selection Guide, Version 2.0.*, tech. report, Secure Access Central Security Portal, Apr. 2007; http://sslvpn.breakawaymg.com/breakaway/NAC%20PSG.php.

[8] **"**Getting the Knack of NAC: Understanding Network Access Control", A Mirage Networks Industry Report, white paper, Mirage Networks, Jan. 2006; http://www.miragenetworks.com/documents/white_papers/ MirageNAC_IndustryReport.pdf.

[9] *Introduction to Network Access Protection*, tech. report, Microsoft Corporation, June 2004; http://www.microsoft.com/technet/network/nap/napoverview.mspx.

[10] "Importance of Standards to Network Access Control", white paper, Juniper Networks, Nov. 2006; http://www.juniper.net/solutions/literature/white_papers/200205.pdf.

[11] J. Conover, *NAC vendors square off, Network Computing*, tech. report, July 2006; http://www.cisco.com/application/pdf/en/us/guest/netsol/ns617/c643/ cdccont_0900aecd80503ef7.pdf

[12] J. Prince, "Security appliances should be in-line rather than out of band", ConSentry Network, Network World, Jan. 2007; http://www.networkworld.com/columnists/2007/ 012907-guide-nac-faceoff-security-yes.html.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 106 of 114

[13] M. Thumann and D.R. Roecher, Hacking the Cisco NAC Framework, ERNW Wir leben IT-Security, Mar. 2007; http://www.ernw.de.

[14] *NAC Appliance (Cisco Clean Access) In-Band Virtual Gateway for Remote Access VPN configuration example*, tech. report, Cisco Systems, Inc.; http://www.cisco.com/warp/public/707/nac-inband-remote-vpn.pdf.

[15] *Network Access Protection Platform Architecture*, tech. report, Microsoft Corporation, June 2004; http://www.microsoft.com/technet/network/nap/naparch.mspx.

[16] "Network Admission Control, At-A-Glance", Cisco Systems, Inc.; http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c643/cdccont_0900aecd800fdd58.pdf.

[17] O. Arkin, "Bypassing Network Access Control Systems", white paper, Insightx Ltd., Sep 2006; http://www.insightix.com/files/pdf/Bypassing_NAC_Solutions_Whitepaper.pdf.

[18] *PandaLabs annual report 2006*, ann. report, Panda Software, 2006; http://research.pandasoftware.com/blogs/images/PandaLabs-2006.pdf.

[19] "Q&A, Cisco Network Admission Control", Cisco Systems, Inc; http://www.cisco.com/application/pdf/en/us/guest/netsol/ns617/c685/cdccont_0900aecd800fdd6f.pdf.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 107 of 114

[20] R. L. Kay, "The Future of Trusted Computing", (IDC 2005), 2005; https://www.trustedcomputinggroup.org/home/IDC_Presentation.pdf.

[21] R. Whiteley, *Demystifying NAC: Going Beyond Basic Admission Control*, tech. report, Forrester Research, Inc, Sept. 2006; http://www.forrester.com/Events/Content/0,5180,-1483,00.ppt.

[22] S. Buckley, "Combating the Evolution of Insider Attacks with Persistent LAN security", Feb. 2007; http://www.convergedigest.com/bp-sec/bp1.asp?ID=463&ctgy=.

[23] S. Hanna, "Putting Trust Into The Network, Securing Your Network Through Trusted Access Control", (ACSAS 2006*)*, Dec. 2006; https://www.trustedcomputinggroup.org/news/presentations/ SHanna_Talk_for_ACSAC_Dec_2006.pdf.

[24] *TCG Specification Architecture Overview*, V 1.3, The Trusted Computing Group, Apr. 2004; https://www.trustedcomputinggroup.org/groups/ TCG_1_3_Architecture_Overview.pdf.

[25] The Cable Guy, "Network Access Protection Platform Overview", *Microsoft TechNet*, Microsoft Corporation, July 2005; http://www.microsoft.com/technet/community/columns/cableguy/ cg0705.mspx.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 108 of 114

[26] *TNC IF-IMC Specification*, V 1.2, The Trusted Computing Group, Feb. 2007; https://www.trustedcomputinggroup.org/specs/TNC/TNC_IFIMC_v1_2_r8.pdf.

[27] TNC IF-IMV Specification, V 1.2, The Trusted Computing Group, Feb. 2007; https://www.trustedcomputinggroup.org/specs/TNC/TNC_IFIMV_v1_2_r8.pdf.

[28] TNC IF-PEP: Protocol Bindings for RADIUS, V 1.1, The Trusted Computing Group, Feb. 2007; https://www.trustedcomputinggroup.org/specs/TNC/TNC_IF-PEP_v1.1_rev_0.7.pdf.

[29] TNC IF-T: Protocol Bindings For Tunneled EAP Methods Specification, V 1.0, The Trusted Computing Group, May 2006; https://www.trustedcomputinggroup.org/specs/TNC/TNC_IFT_v1_0_r3.pdf.

[30] TNC IF-TNCCS Specification, V 1.1, The Trusted Computing Group, Feb. 2007; https://www.trustedcomputinggroup.org/specs/TNC/TNC_IF-TNCCS_v1_1_r15.pdf.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 109 of 114

[31] T.T.A. Dinh and M.D. Ryan, "Trusted Computing: TCG Proposals", Computer Security Lecture Notes, Nov. 2006; http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/TrustedComputingTCG.html.

[32] "Unified Access Control Solution V2.0: Infranet Controller, UAC Agent and UAC enforcement points", Juniper Networks, Nov. 2006; http://www.juniper.net/products/ua/dsheet/100137.pdf.

[34] "What is IETF NAC strategy?", white paper, 7 in a series, Interop Labs, May 2006; http://www.interop.com/lasvegas/exhibition/interoplabs/nac/IETFNACstrategy.PDF.

[35] "What is TCG's Trusted Network Connect?", white paper, Interop Labs, May 2006; http://www.interop.com/lasvegas/exhibition/interoplabs/nac/TCG.PDF.

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 110 of 114

Appendices

Appendix A: Glossary of Terms

802.1X:	IEEE Standard For Port-Based Access Control
AAA:	Authentication, Authorization and Accounting Protocol
API:	Application Programming Interface
AR:	Access Requestor (TCG Term.)
ACS:	Cisco Access Control Server (Cisco Term.)
CCA:	Cisco Clean Access Agent (Cisco Term.)
C-NAC:	Cisco's Network Admission Control (Cisco Term.)
CTA:	Cisco Trust Agent (Cisco Term.)
DHCP:	Dynamic Host Configuration Protocol
EAP:	Extended Authentication Protocol
EC:	Enforcement Component (Microsoft Term.)
ES:	Enforcement Server Component (Microsoft Term.)
HTTPS:	HTTP Security
IF-M:	Interface between IMC and IMV (TCG Term.)
IF-IMC:	Interface between IMC and TNCC (TCG Term.)
IF-IMV:	Interface between IMV and TNCS (TCG Term.)
IF-PEP:	Interface between PEP and PDP (TCG Term.)
IF-T:	Interface between NAA and NAR (TCG Term.)
IF-TNCCS:	Interface between TNCC and TNCS (TCG Term.)
IMC:	Integrity Measurement Collector (TCG Term.)
IMV:	Integrity Measurement Verifier (TCG Term.)
IPSEC:	Internet Protocol Security

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 111 of 114

NAC:	Network Access Control (Generic Term. Not specific to a vendor)
NAD:	Network Access Device (Cisco Term.)
NAP:	Network Access Protection (Microsoft Term.)
NPS:	Network Policy Server (Microsoft Term.)
OAC:	Odyssey Access Client (Juniper Networks Term.)
PDP:	Policy Decision Point (TCG Term.)
PEP:	Policy Enforcement Point (TCG Term.)
PPP:	Point-to-Point Protocol
RADIUS:	Remote Authentication Dial-In User Service Protocol
SHA:	System Health Agent (Microsoft Term.)
SHV:	System Health Validator (Microsoft Term.)
SNMP:	Simple Network Management Protocol
SOH:	Statement of Health (Microsoft Term.)
SOR:	Statement of Response (Microsoft Term.)
SSL:	Secure Socket Layer
TCG:	The Trusted Computing Group
TLS:	Transport Layer Security
TNC:	Trusted Network Connect (TCG Term.)
TNCC:	TNC Client (TCG Term.)
TNCS:	TNC Server (TCG Term.)
TPM:	Trusted Platform Module (TCG Term.)
UAC:	Unified Access Control (Juniper Networks Term.)
UDP:	User Datagram Protocol
Wi-fi:	IEEE 802.11 Wireless Standard
VPN:	Virtual Private Network

INFOEXPRESS, INC. - EX2447
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 112 of 114

LINKÖPING UNIVERSITY
ELECTRONIC PRESS

På svenska

Detta dokument hålls tillgängligt på Internet – eller dess framtida ersättare – under en längre tid från publiceringsdatum under förutsättning att inga extra-ordinära omständigheter uppstår.

Tillgång till dokumentet innebär tillstånd för var och en att läsa, ladda ner, skriva ut enstaka kopior för enskilt bruk och att använda det oförändrat för ickekommersiell forskning och för undervisning. Överföring av upphovsrätten vid en senare tidpunkt kan inte upphäva detta tillstånd. All annan användning av dokumentet kräver upphovsmannens medgivande. För att garantera äktheten, säkerheten och tillgängligheten finns det lösningar av teknisk och administrativ art.

Upphovsmannens ideella rätt innefattar rätt att bli nämnd som upphovsman i den omfattning som god sed kräver vid användning av dokumentet på ovan beskrivna sätt samt skydd mot att dokumentet ändras eller presenteras i sådan form eller i sådant sammanhang som är kränkande för upphovsmannens litterära eller konstnärliga anseende eller egenart.

För ytterligare information om Linköping University Electronic Press se förlagets hemsida http://www.ep.liu.se/

In English

The publishers will keep this document online on the Internet - or its possible replacement - for a considerable time from the date of publication barring exceptional circumstances.

The online availability of the document implies a permanent permission for anyone to read, to download, to print out single copies for your own use and to use it unchanged for any non-commercial research and educational purpose. Subsequent transfers of copyright cannot revoke this permission. All other uses of the document are conditional on the consent of the copyright owner. The publisher has taken technical and administrative measures to assure authenticity, security and accessibility.

According to intellectual property law the author has the right to be mentioned when his/her work is accessed as described above and to be protected against infringement.

For additional information about the Linköping University Electronic Press and its procedures for publication and for assurance of document integrity, please refer to its WWW home page: http://www.ep.liu.se/

© Hasham Ud-Din Qazi