insightix

Keep your network in sight

Bypassing Network Access Control Systems

Ofir Arkin
Chief Technology Officer
Insightix Ltd.

September 2006

United States

945 Concord Street
Framingham, MA 01701
1.508.620.4788

info@insightix.com
www.insightix.com

International

13 Hasadna Street
Ra'anana, Israel
+972.9.740.1667

Contents

By providing this document, Insightix is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice.

Abstract

The threat of viruses, worms, information theft and lack of control of the IT infrastructure has lead companies to implement security solutions to control the access to their internal IT networks. A new breed of software and hardware solutions from a variety of vendors has recently emerged. All are tasked with one goal – controlling the access to a network using various methods and solutions. This whitepaper examines the different strategies used to provide network access controls. The flaws associated with the different network access control (NAC) solutions are also presented. These flaws allow the complete bypass of each and every NAC mechanism currently offered on the market.

About Insightix

Insightix is the developer of the only complete, real-time and agentless IT infrastructure discovery and network access control solutions. Insightix solutions are simple to install, provide coverage for the entire network and deliver an immediate return-on-investment for IT operations, network security and regulation compliance. By providing comprehensive network visibility and access control, Insightix customers reduce the time, cost and complexity associated with IT management.

Insightix’s investors include Quest Software (NASDAQ: QSFT), several technology veterans and Blumberg Capital. The company's advisory members include industry leaders from IBM, Computer Associates, Citrix, Check Point, RSA, Comverse, ECI Telecom and AudioCodes.

1.0 Introduction to Network Access Control

An enterprise IT network is a complex and a dynamic environment that is generally described as a black hole by its IT managers.

The lack of network knowledge due to missing or partial information directly results in the inability to manage and secure the network in an appropriate manner.

This lack of knowledge regarding the enterprise network layout (topology), resources (availability and usage), elements residing on the network (devices, applications, their properties and the interdependencies among them) and users accessing the network and their resources (whether locally or remotely) lead to a situation in which the stability, integrity and regular operation of the IT network are in jeopardy.

In light of the inability to control the IT network and the increasing risk to the integrity and the regular operation of the IT network, a new set of technologies has been developed to enforce a certain predefined security policy as a prerequisite for network elements and users to connect to the network. This set of technologies is termed by many as Network Access Control (NAC) - a set of technologies and defined processes aimed at controlling access to the network.

1.1 NAC Capabilities

Although NAC is a valid technology that should play a key role with internal network security, a common criteria for NAC does not yet exist. As a result, the definition of what exactly a NAC solution does should be combined from vendors offering such solutions.

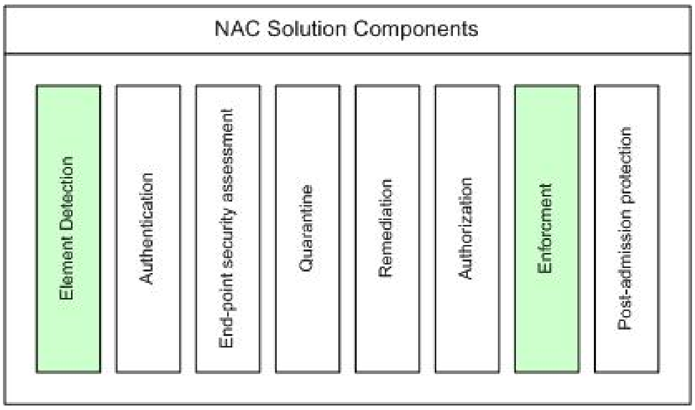

Figure 1: NAC Solution Components

The most essential capabilities of any NAC solution must include the ability to detect a new element connecting to the network1 and the ability to verify whether or not it complies with a defined security policy of the organization. If the element does not comply with the security policy, the NAC solution must restrict the access of element to the network.

The following is a list of functions that may or may not be included with a vendor's NAC offering:

- **Element Detection** – detecting new elements as they are introduced to the network.
- **Authentication** – authenticating each user accessing the network no matter where they are authenticating from and/or which device they are using.
- **Endpoint Security Assessment** – assessing whether a newly introduced network element complies with the security policy of the organization. These checks may include the ability to gather knowledge regarding an element's operating system, the list of installed patches, the presence of anti-virus software and its virus signature date, etc. In most cases, it involves the installation of client software on the end system.
- **Remediation** – quarantining an element that does not comply with the defined security policy until the issues causing it to be non-compliant are fixed. When quarantined, the element may be able to access a defined set of remediation servers allowing the user fixing the non-compliant issues and to be reintroduced, now successfully, to the network.
- **Enforcement** – restricting the access of an element to the network if the element does not comply with the defined security policy.
- **Authorization** – verifying access by users to network resources according to an authorization scheme defined in an existing authorization system, such as Active Directory, RADIUS servers, etc., allowing the enforcement of identity-based policies after an element is allowed on the network
- **Post-Admission Protection** – continuously monitoring users, elements and their sessions for suspicious activity (i.e. worms, viruses, malware, etc.). If detected, the action taken by a NAC solution may vary from isolating the offending system to dropping the session. Post-admission protection functions are similar to the functionality of Intrusion Prevention Systems (IPS).

Each function may be implemented using different technological approaches, which may vary from one vendor to another.

1.2 An Example of the Operation of a NAC Solution

When a new element is introduced to the network, a NAC solution must identify its presence.

A NAC solution relies on a certain element detection technique in order to detect the presence of the newly introduced element. Among the element detection techniques used, the following can be named:

[1] Although it may imply that a NAC solution must be aware of any element connected to the network, many NAC solutions do not maintain a complete, accurate and real-time inventory of all the elements connected to the network.

- **DHCP Proxy** – a NAC solution intercepts DHCP requests for network configuration information coming from elements operating on the network disclosing their presence.
- **Broadcast Listener** – a NAC solution listens to broadcast network traffic, such as ARP requests, DHCP requests, etc., generated by elements operating on the network disclosing their presence.
- **Listening to (sniffing) IP traffic** – IP packets passing through a certain monitoring location disclosing a certain element is connected to the network.
- **Client-Based Software** – some NAC solutions make use of client-based software as part of the solution architecture, which is used to perform endpoint security assessment in order to prevent an element from obtaining network configuration information until it is evaluated and to notify a centralized management console the element is on the network.
- **SNMP Traps** – some switches can be configured to send an SNMP trap when a new MAC address is registered with a certain switch port. The SNMP trap information details the MAC address and the network interface on which it was registered.

Most of the NAC solutions available today are using a single element detection technique, while a small number of NAC solutions are using multiple element detection techniques. Element detection has a key role for a NAC solution. If a NAC solution fails detecting an element connected to the network, the NAC solution can be then bypassed.

After a NAC solution has identified the existence of the new element, it then needs to determine if the element complies with the security policy of the organization. In order to do this, a NAC solution may use a set of checks that may include the ability to gather knowledge regarding an element's operating system, the list of installed patches, the presence of anti-virus software and its virus signature date, etc.

In order to perform endpoint security assessment, some NAC solutions require the installation of client-based software. Such client-based software usually is available only for Microsoft Windows operating systems (Microsoft Windows 2000 and later versions). A network element with NAC-based client software is known as a managed element. A network element without NAC-based client software is known as an unmanaged element.

Instead of installing client-based software, some NAC solutions use a vulnerability scanner in order to provide an endpoint security assessment of newly introduced elements.

The result of the checks performed by the endpoint security assessment process determines if the element in question should be allowed to access the network or if it should be isolated from the network until the appropriate software should be installed or the appropriate fixes should be applied.

When an element is isolated from the network, it is usually quarantined into a designated network without access to any resources on the enterprise network. In most cases, all quarantined elements share the same isolated network. In rare occasions, a quarantined element is placed into a private VLAN segregated from the enterprise resources and from any other quarantined element.

The only resource a quarantined element may access is a specified list of remediation servers. The role of these servers is to allow a user to easily remedy the issues that prevented its element from being allowed on the network, by installing the appropriate software stored on the remediation servers.

When the installation of the appropriate software is successfully performed, the element's compliance with the organization's security policy should be re-evaluated. If the element complies with the security policy, it is allowed access to the network.

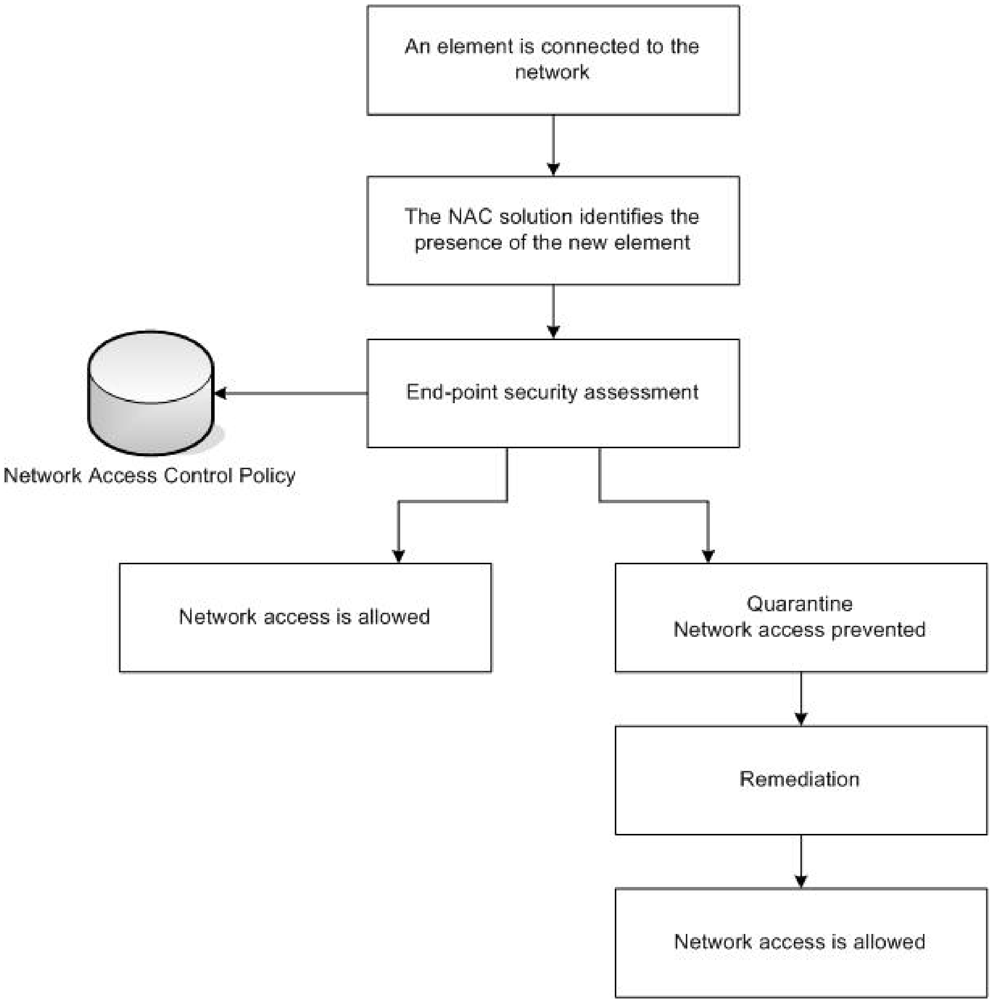
An element is connected to the network
The NAC solution identifies the presence of the new element
End-point security assessment
Network Access Control Policy
Network access is allowed
Quarantine
Network access prevented
Remediation
Network access is allowed

Figure 2: An Example for the operation of a NAC solution

2.0 Attack Vectors

NAC solutions can be attacked using a variety of different attack vectors. These attack vectors can be divided into several categories based on the way each can compromise the operation of a NAC solution:

- **Architecture** – the architecture of a NAC solution is usually combined from various elements, each responsible for one or more NAC function. Analyzing the architecture of a NAC solution may reveal a design flaw allowing weakening the NAC solution or even bypassing it.
- **Technology** – a NAC solution uses various technologies in order to provide NAC functionality. Each of these technologies may contain a weakness, which may allow bypassing the NAC solution.
- **Components** – a NAC solution is combined from various components, such as servers, client-side software, etc. A vulnerability that may be present with one or more of these components may allow the component to be controlled, which may facilitate the bypassing the NAC solution.

3.0 Architecture Flaws of NAC Solutions

Different NAC solutions suffer from various architectural design flaws associated with their architecture, design and operation.

3.1 Element Detection

3.1.1 Methods Used for Detecting Elements

The ability to detect new elements as they are introduced to the network is one of the key features a NAC solution must support.

Usually, a NAC solution listens to network traffic (sniffing) trying to detect a new element operating on the network by analyzing network traffic generated by the element. Element detection can be performed by analyzing traffic at different TCP/IP layers:

- Layer 2 network traffic (i.e. an ARP request)
- Layer 3 network traffic (i.e. SYN request)
- Any network traffic

When element detection depends on an IP packet (Layer 3) or a certain protocol to disclose the existence of an element on the network, there are ways to bypass the detection. This is due to the fact Layer 2 traffic and/or network traffic other then the designated protocol used for the element detection process can be used where the NAC solution is not be able to detect the presence of the element on the network.

The following are some examples:

- Element detection using DHCP proxy can be bypassed by assigning a static IP address.
- Element detection using a broadcast listener can be bypassed when an element is not generating broadcast network traffic.

- Element detection using a sniffer attached to a switch/router can be bypassed when elements communicate inside their network segment without sending their network traffic through the monitoring point2.

When an element is introduced to the network without being detected, it may be able to:

- Infect other elements on the network with a virus, a worm or a malware.
- Try penetrating other elements on the same local network segment using them as a launch pad for accessing other parts of the network it may not be allowed to access (abusing their network access rights).

3.1.2 Lack of Knowledge Regarding the Network Terrain

Currently available NAC solutions do not include network discovery capabilities, although they solely rely on their element detection capabilities in order to learn about the elements operating on the network.

The technology used by NAC solutions to perform element detection suffers from numerous flaws, preventing them from completely identifying the elements operating on the network, leaving unaccounted elements to freely operate on the network without being detected.

NAC solutions, whose aim is to control the access of elements to an enterprise network, do not have complete and accurate knowledge regarding the elements they need to operate against.

Information regarding the physical network topology of an enterprise network is an additional piece of missing information, which is not being collected by NAC solutions. This may allow elements to access the network using venues, which may exist, but are unknown to the NAC solution.

3.1.3 Masquerading and Virtualization

The technology limitations that prevent NAC solutions from detecting a rogue element are connected to the network behind a device providing it network address translation (NAT) services and access to the network from an allowed element. In this situation, the rogue element is given the same access rights as an allowed element.

Due to the fact the masquerading element is free to operate on the network without being detected by a NAC solution, virtualization solutions that provide NAT services should be a major concern for NAC solutions.

3.2 Managed vs. Unmanaged Elements

After a NAC solution has learned about the existence of a new element, it may need to determine if the element complies with the security policy of the organization. In order to do this, a NAC solution may use a set of checks that may include the ability to gather knowledge regarding an element’s operating system, the list of installed patches, the presence of anti-virus software and its virus signature date, etc.

[2] The location of the monitoring point determines the type of network traffic that is observed.

In order to perform endpoint security assessment, many NAC solutions require the installation of client-based software. Such client-based software is usually available only for Microsoft Windows operating systems (Microsoft Windows 2000 and later versions).

Research performed by various analyst groups has estimated that only 55% to 65% of the elements operating on an enterprise network may be identified by an active network discovery solution. The task of installing client-based software becomes a non-trivial issue where some of the elements the client-based software needs to be installed on are unknown to the organization.

Although the share amount of Microsoft Windows-based elements logon to an organizational Windows domain, a significant number of elements would operate outside an organizational Windows domain. In many cases, virtualized Microsoft Windows-based elements used for development, QA and related purposes are not part of the organizational Windows domain.

With many NAC solutions, only managed elements (a network element with NAC-based client software) go through the process of assessing their endpoint security, while unmanaged elements (a network element without NAC-based client software) is allowed on the network using exception rules. An exception rule identifies a certain element according to a unique characteristic, such as its MAC address, and allows the element to operate on the network without passing through any endpoint security assessment.

Due to the fact that many elements operating on an enterprise network are not accounted for, and the fact that elements running operating systems other then Microsoft Windows-based operating systems operate on the network, the number of unmanaged elements that connect to the network without endpoint security assessment is high.

Another concern is linked to the technology used by NAC solutions to perform element detection, which suffers from numerous flaws, preventing them from completely identifying the elements operating on the network, leaving unaccounted elements to operate freely without ever being detected.

3.3 Exception Rules

An exception rule identifies a certain element according to a unique characteristic, such as its MAC address and allows the element to operate on the network without passing through any endpoint security assessment.

An exception rule can be abused in order to introduce a rogue element to the network using a MAC address listed as an exception rule. For example, a printer can be disconnected from the network, while a rogue element can assume its MAC address and be given its network access rights.

A contributing factor that makes abusing exception rules even easier is the fact that except for the MAC address of an element, no other information regarding the properties of an element are discovered and saved with the exception rule.

3.4 Endpoint Security Assessment

3.4.1 Checked Information

Knowledge regarding an element's operating system, the list of installed patches, the presence of anti-virus software and its virus signature date are usually gathered as part of an endpoint security assessment process.

Organizations may not enroll a security patch as soon as it is released. The security patch is first tested and unless its installation will not cause any apparent damages, then and only then, is it installed. The matter of fact is that until this day many organizations still have not enrolled Microsoft Windows XP service pack 2.

As a result and in many cases, the barrier of entry for an element for entering the network might be lower then the desired one.

3.4.2 Falsifying Checked Information

In order to perform an endpoint security assessment, a NAC solution may use a set of checks that may include the ability to gather knowledge regarding an element's operating system, the list of installed patches, the presence of anti-virus software and its virus signature date, etc.

The information a NAC solution assess is stored in a Microsoft Windows operating system's registry. Any user with administrative privileges can override these registry settings to represent a different, falsified set of values, allowing an attacker to introduce an element to the network even if it does not actually have any of the required software.

3.4.3 Unmanaged Elements and the Usage of a Vulnerability Scanner

A recent trend with NAC solutions is the usage of a vulnerability scanner to perform an endpoint security assessment.

When client-based software is not available for or on a certain element, or a NAC solution claims to be agentless, a vulnerability scanner is used.

Due to the fact a high number of elements that operate on a network use a personal firewall, element scanning with a vulnerability scanner is in most cases useless.

3.5 Quarantine Type

The result of the endpoint security assessment process determines if an element in question should be allowed to access the network or if it should be isolated from the network until the appropriate software is installed or the appropriate fixes are applied.

When an element is isolated from the network, it is usually quarantined into a designated network, unable to access the enterprise network's resources.

The following are different strategies that can be used when quarantining an element:

- Layer 3
  - Placing an element into a quarantined network segment by assigning different network configuration information. Usually it is done by using an IP belonging to non-routable network segment or by using an ACL on routers in order to restrict the quarantined network segment's access.
- Layer 2
  - Placing an element into a designated quarantined VLAN.
  - Placing an element into a designated private VLAN (P-VLAN).
  - ARP mitigation using ARP spoofing to redirect an element to a quarantine corridor, including the element and the NAC solution server, which is able to determine the endpoint security status of the element as well as to provide remediation services.

The following are examples of how a quarantine method can be bypassed.

- When an element is quarantined into a network segment by assigning the element a different set of network configuration information (through DHCP for example), changing the configuration with parameters belonging to an allowed network then permits the element to detach itself from the quarantined network and regain access to the main enterprise network.
- When ARP mitigation is used to redirect an element to communicate only with the NAC solution, it can be bypassed by statically defining ARP entries on a newly introduced element.

3.6 Inside the Quarantine

When an element is isolated from the network, it is usually quarantined into a designated network without access to the resources of the organization. In most cases, all quarantined elements share the same isolated network.

The elements placed in quarantine shares a common characteristic - they do not comply with the security policy of the organizations. As such, they may be vulnerable to a certain number of viruses, worms and/or vulnerabilities.

If an infected element is placed into quarantine, it may infect other elements sharing the quarantine network.

Thus, the quarantine network opens a unique opportunity for an attacker. Instead of combating its way to bypass network access controls gaining access to the enterprise network, an attacker can intentionally place its element into the quarantined network. While on the quarantined network, the attacker can search for and compromise soft targets, ensuring access when they are reintroduced to the network3.

[3] Private VLAN segregated from the network resources and any other quarantined element

3.7 Access Restrictions while in Quarantine and Remediation

The only resource a quarantined element may access is a specified list of remediation servers. Their role is to allow a user to easily remedy the issues that had prevented its element from being allowed on the network by installing the appropriate software stored on the remediation servers.

Some NAC solutions allow quarantined elements to directly access some organizational resources for additional services. For example, access to DNS services requires access to a DNS server. While permitting access to such resources, the access restrictions imposed on the quarantined elements are not restrictive enough, allowing a quarantined element to access any element on the enterprise network by tunneling information through the allowed service.

3.8 Blinding Post-Admission Protection

The goal of post-admission protection is to continuously monitor allowed users, elements and their sessions for suspicious activity, such as worms, viruses, malware, abnormality and so. If a suspicious activity is detected, the action taken by a NAC solution may vary from isolating the offending system to dropping the session.

Post-admission protection relies on the ability to observe traffic coming from and going to elements against which the NAC system operates. This is also its main drawback. If network communications from and/or to an element does not pass through the monitoring point of the NAC solution, it is unable not to draw conclusions if a certain violation or an abnormality had occurred.

Communications between elements found on the same network segment is an example of a communication type that is usually not observed. Another example is with elements connected to the same Layer 2 switch that may communicate with each other without the knowledge of the NAC solution.

Another drawback that needs to be considered is the usage of encryption. If used between elements operating on the enterprise network as a means to securely communicate, it will “blind” the NAC solution.

3.9 No Bonding with Authorization

With many NAC solutions, after an element is granted access to the enterprise network, the element is free to perform any actions it may wish to take. This, without the supervision of a NAC solution monitoring the element’s actions tying it with authorization rights (if exists) prevent it access to resources it is not allowed to access.

4.0 Examples of Bypassing NAC Solutions

The following examples detail the operations of several NAC solutions and the ways to bypass them. These examples were gathered from different vendor offerings currently available on the market. The main issues with each NAC solution are also highlighted. Additional issues may exist.

The following NAC solutions are discussed in this section:

- Software
    - DHCP Proxy-based NAC solutions
    - Authenticated DHCP-based NAC solutions
    - Broadcast listeners-based NAC solutions
    - Cisco NAC Framework
- Hardware
    - Inline NAC devices
    - Out-of-band NAC devices

4.1 DHCP Proxy-Based NAC Solutions

4.1.1 Architecture Overview

A NAC solution using a DHCP proxy to perform element detection places a DHCP proxy server in front of the DHCP server (or as a replacement) of an organization, which is in charge of handing IP addresses and network configuration for DHCP clients.

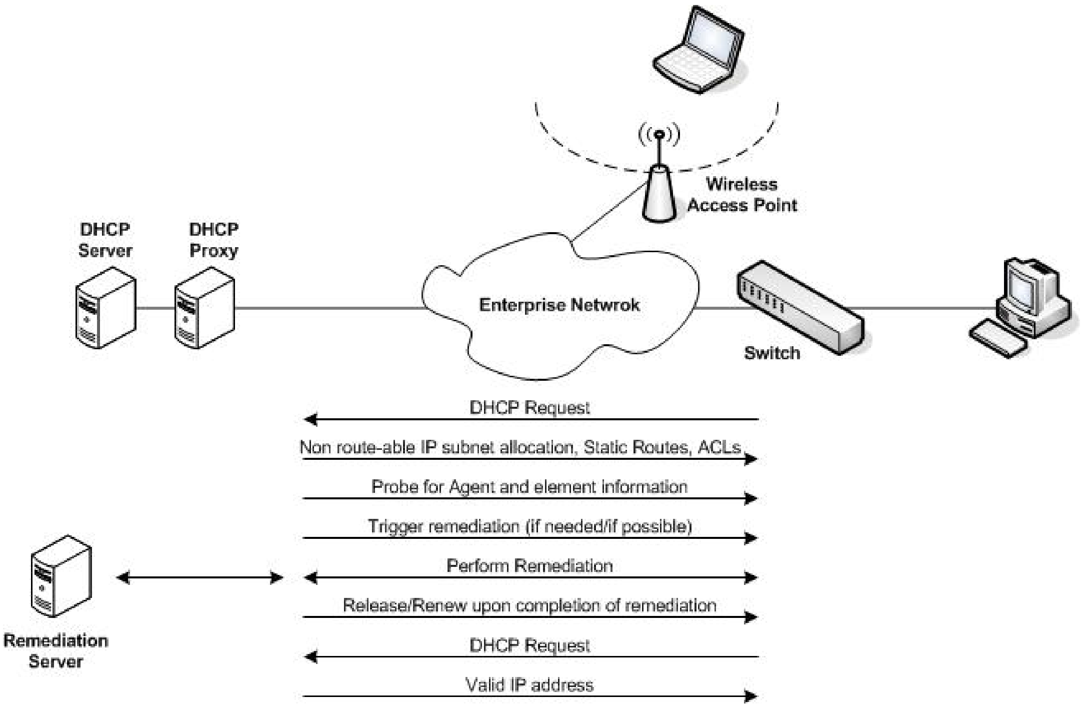
Wireless
Access Point
DHCP
Server
DHCP
Proxy
Enterprise Netwrok
Switch
DHCP Request
Non route-able IP subnet allocation, Static Routes, ACLs
Probe for Agent and element information
Trigger remediation (if needed/if possible)
Perform Remediation
Release/Renew upon completion of remediation
DHCP Request
Valid IP address
Remediation
Server

Figure 3: DHCP Proxy Information Exchange

The DHCP proxy intercepts DHCP requests coming from elements accessing the network. The NAC solution then quarantines an element sending a DHCP request into a non-routable network segment, assigning it network configuration information (IP address and static routes) aimed to restrict the access of the element to the main enterprise network. The network configuration information is handed to the element through the DHCP protocol.

After the element has been quarantined, the NAC solution probes the element for the presence of a client-based software agent, which had to be installed previously. When found, it gathers the information required for an endpoint security assessment. If the element does not comply with the security policy of the organization, the user is able to access a list of remediation servers to install the missing software.

The DHCP proxy assigns the IP settings for the element only for a short time period. This ensures the element re-sends a DHCP request, requesting an IP address allowing the process to repeat itself assessing whether or not the element can now be admitted to the network or remain in quarantine.

4.1.2 Strengths

The strengths associated with a NAC solution using a DHCP proxy are:

- Most organizations already use DHCP
- A DHCP proxy solution is easy to deploy

Implementing a DHCP-based NAC solution contains a low barrier-of-entry into organizations.

4.1.3 Weaknesses and Bypass

A DHCP proxy-based NAC solution has many different weaknesses contributing to several ways to bypass the solution.

4.1.3.1 Element Detection

A DHCP proxy-based NAC solution only detects elements using the DHCP protocol. Unfortunately, various elements residing on the enterprise network do no use the DHCP protocol, such as printers, servers and switches. Therefore, other elements may exist and operate on the enterprise network without the knowledge of the NAC solution. Furthermore, the DHCP proxy-based NAC solution can be simply bypassed by assigning an element a static IP address. The element would be granted access to at least the local network segment4.

4.1.3.2 Use of Client-Based Software

A DHCP proxy-based NAC solution must use client-based software in order to determine the endpoint security status of elements residing on the network. The client-based software is usually available only for

[4] This assuming a blocking gateway might also be present.

Microsoft Windows operating systems (Microsoft Windows 2000 and later versions). Thus, the endpoint security of any non-Windows operating system cannot be determined.

In order to allow non-Windows based elements to operate on the network, exception rules need to be defined.

4.1.3.3 Unmanaged Elements

The following quote was taken from a whitepaper titled "Network Access Control Technologies and Sygate Compliance on Contact" by Sygate (acquired by Symantec), which defines Sygate's DHCP proxy NAC solution's behavior regarding unmanaged elements:

> "Systems without agents can be granted network access two ways. First, a non-windows exception can be made that exempts non-windows clients from the NAC process. Second, a MAC address-based exemption list can be built. This MAC address list accepts wildcards, allowing the exemption of whole classes of systems such as IP phones using their Organizationally Unique Identifiers."

A rogue element can be introduced to the network spoofing the MAC address of an element with a defined exception rule. In the Sygate/Symantex example, this can be done by imposing any non-Windows based element that may reside on the network.

4.1.3.4 Breaking Out of the Quarantine

A user can bypass its element's quarantine by assigning the element a static IP address that belongs to the main enterprise network.

4.1.3.5 No User Authentication

With DHCP proxy-based NAC solutions, no form of user authentication exists. Theoretically, an attacker may be able to introduce a rogue element to the network by installing the client-based software used by the DHCP proxy-based NAC solution and comply with the security policy (i.e. making sure its Microsoft Windows based element has the appropriate hotfixes installed).

4.2 Authenticated DHCP

4.2.1 Architecture Overview

A NAC solution based on authenticated DHCP authenticates users before they are granted access to the network. In order to do so, a DHCP server as part of the authenticated DHCP NAC solution architecture is installed on the network.

The DHCP server answers DHCP requests coming from elements accessing the network (1). The NAC solution quarantines an element sending a DHCP request into a non-routable network segment, assigning it network configuration information (IP address and static routes) aimed to restrict the element's access to the main enterprise network (2). The network configuration information is handed to the element through the use of the DHCP protocol.

Among the configuration parameters sent from the DHCP server to elements requesting an IP address is the IP address of the DNS server the elements are to use. When an element attempts to browse on the Internet or the local network, the browser is redirected to an authentication portal (3). The redirection is performed when a user tries to browse the web and its element sends a DNS request to the DNS server it is set to use (the IP address of the DNS server is set to the IP address of the authentication portal5), in an attempt to resolve the web address of the web site it wishes to browse.

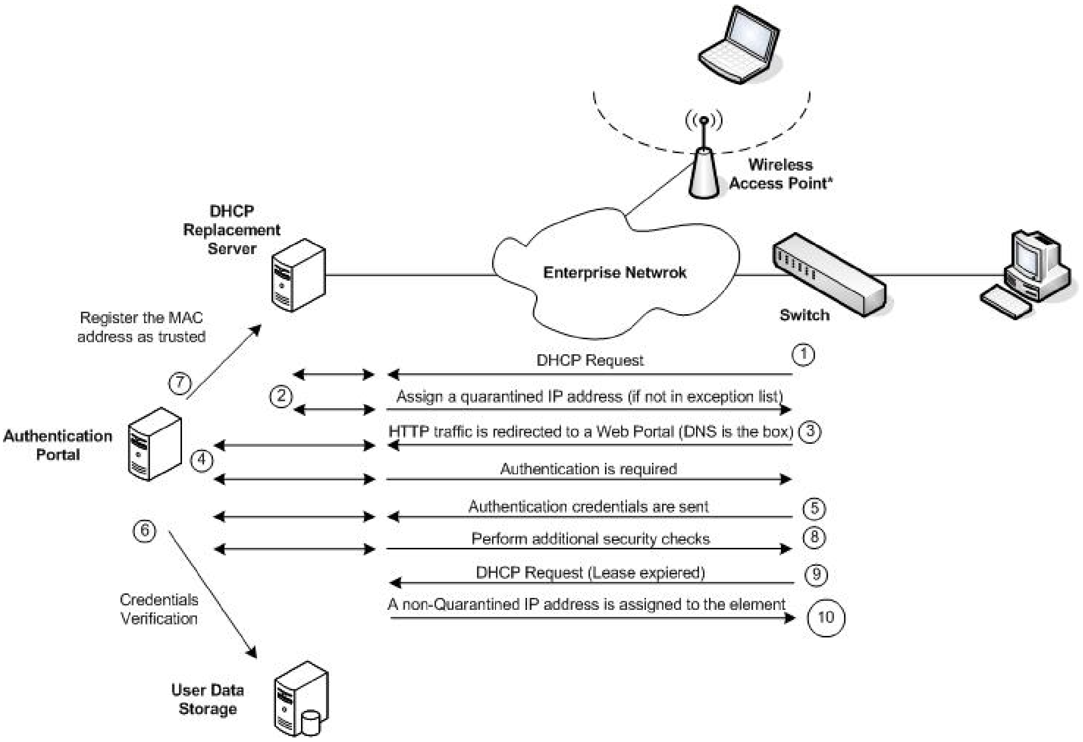
Wireless
Access Point*
DHCP
Replacement
Server
Enterprise Netwrok
Switch
Register the MAC
address as trusted
7
2
DHCP Request
1
Assign a quarantined IP address (if not in exception list)
Authentication
Portal
4
HTTP traffic is redirected to a Web Portal (DNS is the box)
3
Authentication is required
6
Authentication credentials are sent
5
Perform additional security checks
8
DHCP Request (Lease expiered)
9
Credentials
Verification
A non-Quarantined IP address is assigned to the element
10
User Data
Storage

Figure 4: Authenticated DHCP Information Exchange

The DNS server the element is set to use can be either set to the DHCP server, or to the authentication portal. The reply sent by the DNS server will resolve the web address of the web site to the IP address of the authentication portal.

The user is faced with an authentication page (4). The credentials the user should use are usually the user's username and password used to logon to a Windows domain belonging to the organization (although a separate username and password database can be built for this purpose).

[5] The DHCP server and the authentication portal may reside on the same element.

The authentication credentials sent to the authentication portal (5) are then verified against a data storage holding the username and password database (6).

If authentication is successful, the authentication portal registers the MAC address of the trusted element to the DHCP server (7).

A NAC solution supporting authenticated DHCP may choose to use additional checks against authenticated elements as part of the admission process (8). Some NAC solutions may use a patch management system and/or a vulnerability scanner to further determine the endpoint security status of authenticated elements.

The DHCP server assigns the IP settings for the element only for a short time period. This ensures the element in question re-sends a DHCP request (9) requesting an IP address, allowing the process to repeat itself assessing whether or not the element can now be admitted to the network or remain in quarantine.

4.2.2 Strengths

The strengths associated with an authenticated DHCP-based NAC solution, include:

- Most organizations already use DHCP
- An authenticated DHCP solution is easy to deploy
- Authenticates any user trying to access the network
- Operating system independent
- Clientless

Introducing an authenticated DHCP-based NAC solution has a low barrier of entry into organizations.

4.2.3 Weaknesses and Bypass

Unfortunately the authenticated DHCP-based NAC solution and the DHCP proxy-based NAC solution share most of their weaknesses and the methods that may be used to bypass these solutions (please see section 4.1.3 for more information)6.

Authenticated DHCP-based NAC solutions do contain some unique weaknesses.

4.2.3.1 Using a Rogue DHCP Server

An attacker is able to use a rogue DHCP server, intercepting DHCP requests and redirecting users to its own authentication portal for stealing user credentials.

An attacker can abuse a basic functionality with the DHCP protocol where the first DHCP reply reaching a host, after it sent a DHCP request, assigns the responding DHCP server to be used by the element.

[6] Please note that an authenticated DHCP does not use client-based software.

Therefore, even if several DHCP servers may answer a single DHCP request, only one DHCP server is then used.

An attacker can use the same techniques used by an authenticated DHCP-based NAC solution. The malicious user can assign, through the usage of DHCP, an IP address and network settings to the requesting element. The network setting places the element on a so-called quarantined network shared only between the rogue DHCP server and the attacked element. The DNS server's IP address assigned with the DHCP reply would be of the rogue DHCP server.

When a user on an attacked element would try to browse the Internet (or the local network) it is redirected to a rogue authentication server, which may have a look and feel similar to the real authentication server. The credentials submitted by the user, which may or may not be verified against the user data storage, allows the attacker not only to bypass the authenticated DHCP-based NAC solution, but also to penetrate deeper into the organization gaining access to its resources and data.

4.2.3.2 Performing Additional Endpoint Security Checks

Additional checks performed with a patch management system and/or vulnerability scanner may prove useless in many cases due to the increasing usage of personal firewalls inside organizations.

4.3 Broadcast Listeners

4.3.1 Architecture Overview

The architecture of a NAC solution utilizing broadcast listeners as its means to perform element detection includes multiple probes deployed at each and every network segment where network access control needs to be enforced. Each probe listens to broadcast network traffic (sniffs the network), which is usually generated as part of the regular TCP/IP communications in order to detect elements operating on the network.

The broadcast listener approach as a means to perform element detection builds on the fact that elements communicating on a network generates ARP requests (and other broadcast network traffic) when communicating with other elements on the same local network segment, learning about the physical address of an element to which they need to send their packets .

4.3.1.1 Managed Solution

A managed NAC solution utilizing broadcast listeners uses client-based software as part of its architecture.

When a broadcast listener probe identifies broadcast network traffic coming from a newly introduced element it probes the agent software for the status of its endpoint security before the element is granted access to the network.

Part of the client-based software role is to prevent the element from accessing the network until the endpoint security assessment process successfully ends. Another possibility is to quarantine the element into a specified VLAN until the process ends.

If the endpoint security assessment fails, the element is allowed to access remediation servers to remedy the issues preventing it from gaining access to the network. Only after these issues are resolved, the element is granted access to the network.

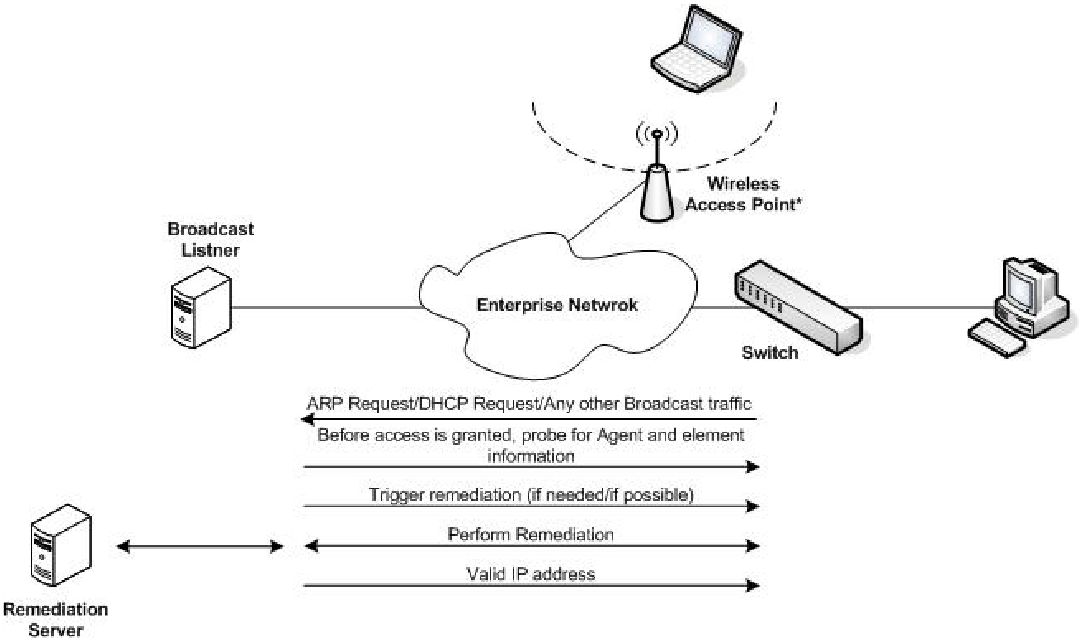
Wireless
Access Point*
Broadcast
Listner
Enterprise Netwrok
Switch
ARP Request/DHCP Request/Any other Broadcast traffic
Before access is granted, probe for Agent and element information
Trigger remediation (if needed/if possible)
Perform Remediation
Valid IP address
Remediation
Server

Figure 5: Broadcast Listener, Managed Elements Information Exchange

4.3.1.2 Unmanaged Solution

An unmanaged NAC solution utilizing broadcast listeners does not use any client-based software as part of its architecture.

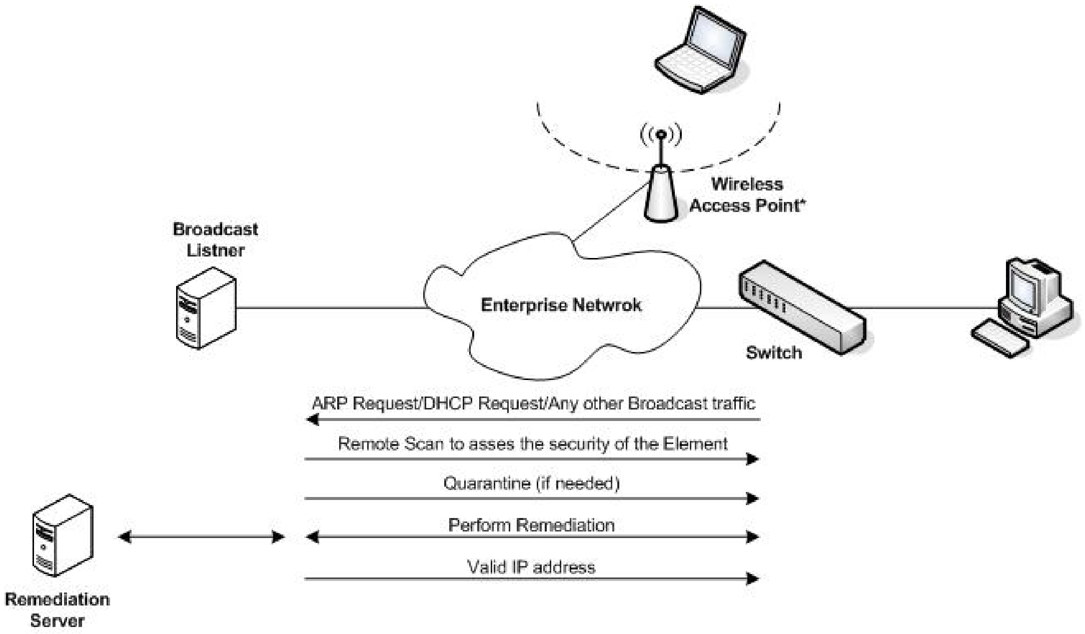

Figure 6: Broadcast Listeners, Unmanaged Solution Information Exchange

When a broadcast listener probe identifies broadcast network traffic coming from a newly introduced element, it remotely assesses the endpoint security status of the element by using a vulnerability scanner.

If the endpoint security assessment fails, the element is then quarantined and access is granted only to remediation servers in order to remedy the issues preventing it from gaining access to the network. Only after these issues are resolved, then the element is granted access to the network.

4.3.2 Weaknesses and Bypass

4.3.2.1 Deployment Issues

Broadcast listeners probes must be placed in each and every network segment of the enterprise. A lot of moving parts are involved with the solution, which makes it difficult to manage.

When deploying this NAC solution, prior knowledge regarding the enterprise network must be obtained. Such knowledge must include information regarding all of the network segments, which belongs to the enterprise network, the locations to place the probes, etc. In most cases the information is produced from a user’s knowledge, which in many cases is incomplete.

The managed broadcast listener-based NAC solution uses client-based software in order to determine the endpoint security status of elements residing on the network. Due to the fact the NAC solution does not have a mechanism to perform network discovery, detecting the elements, which its client-based software needs to be installed on, client-based software is not installed on all the necessary elements.

The client-based software is usually available only for Microsoft Windows operating systems (Microsoft Windows 2000 and later versions). Thus, the endpoint security status of any non-Windows operating system is determined using a vulnerability scanner.

4.3.2.2 Quarantine Issues

Quarantine can be performed only if the network the NAC solution operates in is configured to use VLANs. Without the use of VLANs, quarantining an element is impossible.

In order to quarantine elements the NAC solution must integrate with the switches operating on the network. This NAC solution lacks network discovery capabilities and does have information regarding these switches. The NAC solution must rely on a user’s input in order to receive the list of switches against which it needs to operate.

In some cases, switches are managed through a dedicated VLAN. Access is usually not granted from the main enterprise network to a management VLAN. Such access would have to be configured in order for the NAC solution to operate successfully.

4.3.2.3 Architecture Flaws with the Unmanaged Solution

A time gap exists between an element introduction to the network and the decision whether or not this element should be allowed on the network or be quarantined. This time gap may allow the element to access other elements on the network before its access is restricted. This time period may be enough for the element to infect, penetrate or abuse other elements on the enterprise network.

4.3.2.4 No Knowledge Regarding the Network Terrain

This NAC solution does not include network discovery capabilities although it solely relies on its element detection capabilities in order to learn about the elements operating on the network.

The technology used by the NAC solution to perform element detection suffers from numerous flaws, preventing it from completely identifying the elements operating on the network, leaving unaccounted elements to freely operate on the network without being detected.

The NAC solution aims to control the access of elements to an enterprise network, but does not have a complete and accurate knowledge regarding the elements it needs to operate against.

Information regarding the physical network topology of the enterprise network is not collected. This may allow elements to access the network using venues, which may exist, but are unknown to the NAC solution.

4.3.2.5 Using a Vulnerability Scanner against Unmanaged Elements

Due to the fact a high number of elements that operate on a network use a personal firewall, scanning an element with a vulnerability scanner is in most cases useless and does not produce valuable results for the endpoint security process.

4.3.2.6 Abusing Exception Rules

An exception rule identifies a certain element according to a unique characteristic, such as its MAC address and allows the element to operate on the network without going through any endpoint security assessment.

An exception rule can be abused in order to introduce a rogue element to the network using a MAC address listed as an exception rule. For example, a printer can be disconnected from the network, while a rogue element assumes its MAC address and be given its network access rights.

A contributing factor that makes abusing exception rules even easier is the fact that except for the MAC address of an element, no other information regarding the properties of an element are discovered and saved with the exception rule.

4.3.2.7 Virtualization and Masquerading

Technology limitations prevent the NAC solution from detecting a rogue element receiving network address translation (NAT) services and access to the network from an allowed element. The rogue element is given the same access rights as the allowed element.

Due to the fact masquerading elements are free to operate on the network without the ability of the NAC solution to detect their existence, virtualization solutions that provide NAT should be a major concern for the NAC solution.

4.3.2.8 Going below the Rader to Bypass Broadcast Listeners

In order to bypass the element detection performed by a broadcast listener probe, an attacker would have to alter its operating system from sending broadcast traffic to the network.

For example, an attacker can initiate communications directly with a host without broadcasting its ARP requests. The change involves sending the ARP request directly to the MAC address of the element it wishes to communicate with (i.e. instead of sending an ARP request with a destination MAC of the broadcast address, it should be replaces with the MAC address of the element with which the attacker wishes to communicate). This way the broadcast listener would not detect any broadcast network traffic coming from the attacker's element7.

[7] The knowledge regarding the MAC address of local elements can be gathered using various ways.

4.4 Cisco NAC Framework

4.4.1 Architecture Overview

Cisco's architecture for network admission control includes:

- Client-based software, Cisco Trust Agent (CTA)
- A Cisco Network Access Device (NAD) with NAC enabled on one or more interfaces for network access enforcement
- Cisco secure Access Control Server (ACS) for endpoint compliance validation
- A remediation server (optional)

Cisco supports three different NAC architectures:

- **NAC L3 IP** – the Cisco NAD is a Layer 3 device (i.e. router) with element detection triggered by IP packets passing through the router
- **NAC L2 IP** – the Cisco NAD is a Layer 2 device (i.e. switch) with element detection triggered by IP packet passing through the switch
- **NAC L2 802.1x** – the Cisco NAD is a Layer 2 device (i.e. switch) with element detection triggered by a data-link packet passing through the switch

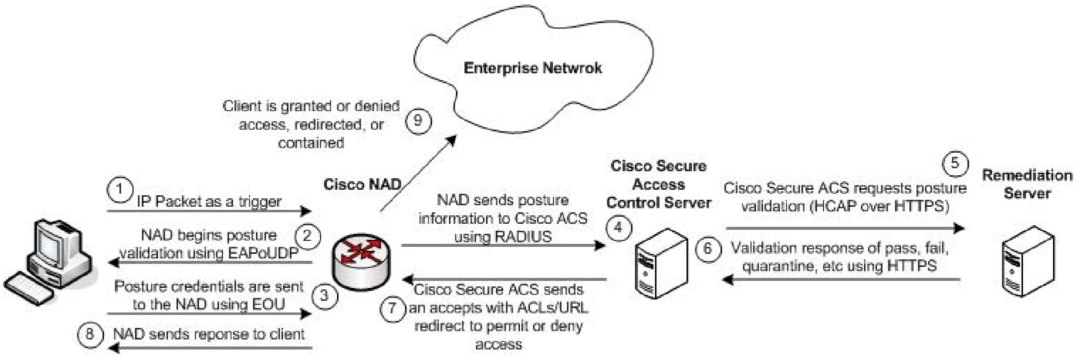
Enterprise Netwrok
Client is granted or denied access, redirected, or contained
9
Cisco NAD
Cisco Secure Access Control Server
Remediation Server
1
IP Packet as a trigger
NAD begins posture validation using EAPoUDP
2
Posture credentials are sent to the NAD using EOU
3
8
NAD sends reponse to client
NAD sends posture information to Cisco ACS using RADIUS
4
Cisco Secure ACS sends an accepts with ACLs/URL redirect to permit or deny access
7
5
Cisco Secure ACS requests posture validation (HCAP over HTTPS)
6
Validation response of pass, fail, quarantine, etc using HTTPS

Figure 7: Cisco L3 IP NAC Operation

4.4.2 Strengths

4.4.2.1 Cisco NAC L2 802.1x

The Cisco NAC L2 802.1x NAC solution can prevent elements from connecting to the network even before they are assigned an IP address. It employs not only standard endpoint security checks, but also includes user authentication as part of the NAC process.

4.4.3 Weaknesses and Bypass

4.4.3.1 Proprietary Solution

Cisco utilizes a proprietary protocol with its NAC framework, EAP over UDP (EAPoUDP), and as a result, the Cisco NAC framework does not work with non-Cisco elements.

An enterprise implementing Cisco NAC framework must ensure the networking gear it uses is Cisco only.

4.4.3.2 High Cost for an Implementation

The cost for implementing the Cisco NAC framework is high:

- Infrastructure upgrades to networking gear that either do not support NAC or that is not manufactured by Cisco is required
- Organizational resources for implementing the solution is required

4.4.3.3 Use of Client-Based Software

The Cisco NAC framework must use client-based software in order to assess the endpoint security status of elements residing on the network. The client-based software is available for Microsoft Windows operating systems (Microsoft Windows NT 4 and later versions) and for Red Hat Linux (Red Hat 9 and Red Hat Enterprise v3). Thus, the endpoint security of any non-Windows operating system and later versions of Red Hat Linux cannot be determined.

In order to allow non-Windows based elements to operate on the network, either a vulnerability scanner is used to determine their endpoint security status or exception rules needs to be defined.

4.4.3.4 Using a Vulnerability Scanner against Unmanaged Elements

Due to the fact a high number of elements that operates on a network use a personal firewall, scanning an element with Cisco's audit server (a vulnerability scanner solution) is in most cases useless and does not produce valuable results for the endpoint security process.

4.4.3.5 Abusing Exception Rules

The following is a quote from Cisco's NAC FAQ[8]:

> "Hosts that cannot run the CTA (Cisco Trust Agent) can be granted access to the network using manually configured exceptions by MAC or IP address on the router or ACS. Exceptions by device types such as Cisco IP phones can also be permitted using CDP on the router."

[8] http://www.cisco.com/go/nac/

An exception rule can be abused in order to introduce a rogue element to the network using a MAC address listed as an exception rule. For example, a printer can be disconnected from the network, while a rogue element assumes its MAC address and be given its network access rights.

A contributing factor that makes abusing exception rules even easier is the fact that except for the MAC address of the element, no other information regarding the properties of the element are discovered and saved with the exception rule.

4.4.3.6 Virtualization and Masquerading

Technology limitations prevent the Cisco NAC framework from detecting a rogue element receiving network address translation (NAT) services and access to the network from an allowed element. The rogue element is given the same access rights as the allowed element.

Due to the fact masquerading element is free to operate on the network without the ability of the NAC solution to detect their existence, virtualization solutions that provide NAT services should be a major concern for the NAC solution.

4.4.3.7 No Knowledge Regarding the Network Terrain

The Cisco NAC framework does not include network discovery capabilities and it solely relies on its element detection capabilities in order to learn about the elements operating on the network.

The technology used by the NAC solution to perform element detection suffers from numerous flaws, preventing it from completely identifying the elements operating on the network, leaving unaccounted elements to freely operate on the network without being detected.

The Cisco NAC framework aims to control the access of elements to an enterprise network, but does not have a complete and accurate knowledge regarding the elements it needs to operate against.

Information regarding the physical network topology of the enterprise network is not collected. This may allow elements to access the network using venues, which may exist but are unknown to the NAC solution.

4.4.3.8 No User Authentication

With Cisco NAC L3 IP and Cisco NAC L2 IP there is no user authentication involved with the NAC process.

4.4.3.9 Tunneling Data while In Quarantine

While in quarantine elements are able to exchange information with other elements on other parts of the enterprise network using selected allowed services. The ACLs, which are configured for quarantined elements, allow the tunneling of a number of protocols across the entire enterprise9. Examples include:

[9] Please see: Network Admission Control (NAC) Framework Configuration Guide, available from: http://www.cisco.com/go/nac

- DNS
- DHCP
- EAPoUDP

4.4.3.10 Abusing Cisco NAC L3 IP

Cisco NAC L3 IP allows elements to freely operate on a local segment without being detected, if these elements do not send their network traffic through the router that used to implement NAC L3 IP.

An element operating on a local network segment is then allowed to infect and/or penetrate other elements with which it shares the same local network.

By penetrating other elements on the local network segment, an attacker may abuse these as a launch pad to gain unauthorized access to other parts of the enterprise network.

4.5 Inline NAC Devices

4.5.1 Architecture Overview

Inline NAC solutions use dedicated hardware that is placed on the network usually between switches and their main switch/router. The inline device may offer multiple network interfaces allowing multiple connections/networks to be connected through the device.

The inline device performs passive element detection by listening to network traffic passing through the device. Element detection may be triggered by IP packets sent through the inline NAC device or by broadcast network traffic (if and only if the inline NAC solution is able to sniff network traffic at Layer 2).

Inline devices may or may not use client-based software. They may rely on a vulnerability scanner to perform the endpoint security assessment.

4.5.2 Weaknesses and Bypass

4.5.2.1 A Single Point of Failure

An inline NAC device represents a single point-of-failure. If the device fails it may not allow network traffic to go through the device.

4.5.2.2 Amount of Network Traffic that Can Be Handled

Inline NAC solutions may be limited by the amount of network traffic they may be able to process. Thus, multiple inline devices would have to be deployed throughout the enterprise network raising the cost associated with implementing the solution.

4.5.2.3 No Knowledge Regarding the Enterprise Network's Topology

Information regarding the physical network topology of an enterprise network may not be complete. Therefore, the deployment of an inline NAC solution may not cover the entire enterprise leaving unmonitored venues to access the network.

An inline NAC solution does not collect physical network topology information. This may allow elements to access the network using venues, which may exist, but are unknown to the NAC solution.

4.5.2.4 Network Re-Architecture

Deploying an inline NAC solution must involve significant changes to the architecture of the network.

4.5.2.5 Element Detection Is Partial and Incomplete

Due to the fact element detection is performed passively, technology limitations prevents the inline NAC solution from completely and accurately detecting all of the elements operating on the network10.

4.5.2.6 Abusing the Local Segment

An inline NAC solution allows elements to freely operate on their local segment without being detected if these elements do not send their network traffic through the inline device.

An element operating on a local network segment is free to infect and/or penetrate other elements with which it shares the same local network.

By penetrating other elements on the network, an attacker may abuse these as a launch pad to gain unauthorized access to other parts of the network.

4.5.2.7 Tunneling Data while In Quarantine

Some inline NAC solutions may allow quarantine elements to exchange information with other elements on other parts of the enterprise network using selected allowed services which may be required for the remediation process.

4.5.2.8 Using a Vulnerability Scanner against Unmanaged Elements

Due to the fact a high number of elements that operate on a network use a personal firewall, scanning an element with a vulnerability scanner is in most cases useless and do not produce valuable results for the endpoint security process.

4.5.2.9 Abusing Exception Rules

An exception rule identifies a certain element according to a unique characteristic, such as its MAC address, and allows the element to operate on the network without any endpoint security assessment.

[10] For more information please see: Ofir Arkin, "Risks of Passive Network Discovery Systems", June 2005. Available from: http://www.insightix.com/resources-currentwhitepaper.asp.

An exception rule can be abused in order to introduce a rogue element to the network using a MAC address listed as an exception rule. For example, a printer can be disconnected from the network, while a rogue element assumes its MAC address and be given its access rights to the network.

A contributing factor that makes abusing exception rules even easier is the fact that except for the MAC address of an element, no other information regarding the properties of an element are discovered and saved with the exception rule.

4.6 Out-of-Band Devices

4.6.1 Architecture Overview

An out-of-band NAC solution uses a span port on a switch to receive network traffic coming in and going out from networks against which it wishes to operate.

The NAC solution identifies elements operating on the network by analyzing the passive network traffic it receives from these networks.

4.6.2 Strengths

There are several considerable advantages for using an out-of-band NAC solution:

- Fast deployment
- Contains less moving parts
- Element detection is performed in real-time

4.6.3 Weaknesses and Bypass

4.6.3.1 Incomplete Discovery

Due to the fact element detection is performed passively, technology limitations prevents the inline NAC solution from completely and accurately detect all of the elements operating on the network11.

4.6.3.2 Abuse of the Local Segment

An out-of-band NAC solution allows elements to freely operate on a local segment without being detected, if these elements do not send their network traffic through the monitoring point the out-of-band NAC solution uses.

An element operating on a local network segment is allowed to infect and/or penetrate other elements with which it shares the same local network.

[11] For more information on this subject, please see: Ofir Arkin's whitepaper on “Risks of Passive Network Discovery Systems” (June 20050 available from: http://www.insightix.com/resources-currentwhitepaper.asp.

By penetrating other elements on the network, an attacker may abuse these as a launch pad to gain unauthorized access to other parts of the network.

4.6.3.3 No Knowledge Regarding the Enterprise Network's Topology

Information regarding the physical network topology of an enterprise network may not be complete. Therefore, the deployment of an out-of-band NAC solution may not cover the entire enterprise leaving unmonitored venues to access the network.

An out-of-band NAC solution does not collect physical network topology information. This may allow elements to access the network using venues, which may exist but are unknown to the NAC solution.

5.0 Conclusion

Network access control technology, which should be a vital part of internal network security, is still in its infancy.

NAC solutions, which aim to control the access of elements to an enterprise network, do not have a complete and accurate knowledge regarding the elements they need to operate against.

Nonetheless, some of the NAC solutions can be bypassed, allowing an attacker to freely access a network and its resources.

A NAC solution must have complete and accurate knowledge regarding the environment it operates in (i.e. topology, inventory), detect changes, and react to them in real-time. Without these capabilities, any NAC solution is destined to fail.

6.0 Resources

1. Ofir Arkin, "Risks of Passive Network Discovery Systems", June 2005. Available from: http://www.insightix.com/resources-currentwhitepaper.asp.
2. Ofir Arkin, "Deficiencies with Active Network Discovery Systems", June 2005. Available from: http://www.insightix.com/resources-currentwhitepaper.asp.
3. "Network Access Control Technologies and Sygate Compliance on Contact", by Sygate (now Symantec). Available from: http://www.sygate.com.
4. Cisco NAC framework. Available information from: http://www.cisco.com/go/nac.