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

The most essential capabilities of any NAC solution must include the ability to detect a new element connecting to the network[1] 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.

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.

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 network[10].

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.