

Questions to Add to Your NAC RFP

Ofir Arkin
Chief Technology Officer
Insightix

Worldwide Headquarters

13 Hasadna Street
Ra'anana, Israel
+972.9.740.1667
info@insightix.com
www.insightix.com

Copyright © 2007-2009 - All Rights Reserved. This material is proprietary of Insightix. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited. This material is meant solely for the use by Insightix employees, and authorized Insightix customers.

About Insightix

Insightix is an innovator of real-time security intelligence and control solutions. Insightix patent-pending technologies are used to detect, identify, profile, audit and control ALL devices connected to your network, providing real-time network, endpoint and user intelligence. Insightix discovers an additional 20%- 50% of the devices residing on the enterprise network, devices that otherwise remain undetected, and automatically audits for the security configuration of endpoints based on the asset classification information collected.

The Insightix Business Security Assurance (BSA) solution suite provides a 360° view into the actual state of your network security effectively Bridging the Network Security Gap that exists between the actual security state of enterprise networks and what is known to IT.

For more information, please visit www.insightix.com.

Contents

- Abstract..... 1
- 1 Complete and Real-Time Network Access Control is Achievable 2
- 2 Recommendations for Your NAC RFP 3
 - Question #1 – How do you define NAC? 3
 - Question #2 – What are the prerequisites for implementing your NAC solution? 3
 - Question #3 – What is the architecture of your NAC solution?..... 3
 - Question #4 – How does your NAC solution perform element detection? 4
 - Question #5 – How does your NAC solution perform compliance checks 5
 - Question #6 – How does the quarantine mechanism of your NAC solution work? 5
 - Question #7 – How does your NAC solution provide enforcement?..... 6
- 3 Analyzing RFP Responses 7
 - Technology 7
 - Time-to-Value 7
 - Total Cost of Ownership..... 7

Abstract

When implemented properly, Network Access Control (NAC) allows only authorized and compliant devices to access and operate on a network. Complete and real-time NAC is achievable if you ask the right questions. This paper discusses the key factors to be considered in evaluating NAC solutions and recommends key questions for inclusion in any NAC Request for Proposal (RFP).

1 Complete and Real-Time Network Access Control is Achievable

Network Access Control (NAC) promises to allow only authorized and compliant devices to access and operate on a network. If implemented properly, NAC can lower the overall security risks faced by an enterprise.

The need for NAC is clear, although many NAC offerings today are still expensive propositions that require network re-architecture and are based on a complex set of bypassable technologies. At the same time, many vendors have jumped on the NAC bandwagon with products that appear to provide NAC-like features, although do not offer full network coverage and leave an enterprise exposed to significant security vulnerabilities.

The result is a confused marketplace.

Despite this, NAC is achievable. You can implement complete and real-time NAC with your existing network setup. Your NAC deployment can be accomplished within your budgetary and implementation expectations. You can ensure that all the devices connected to your network are and remain authorized and compliant throughout their lifecycle on your network.

2 Recommendations for Your NAC RFP

Asking the right questions when evaluating NAC solutions can help you make the correct buying decision. In order to select and implement a valuable NAC solution, it is recommended that the following questions be included in your Request for Proposal (RFP).

Question #1 – How do you define NAC?

NAC is a hot topic and is considered by many to be the *Next Big Thing* in the realm of IT security, thus many vendors are misusing the term NAC to gain extra visibility. As a result, there are many products available today claiming to offer NAC, although not all of them offer a complete solution to achieve coverage of an entire network and ensure that only authorized and compliant devices access and operate on the network.

As a first question, it is essential to ask – How do you define NAC? As an extension of this question, it is also important to understand what threats the NAC solution is designed to mitigate.

Question #2 – What are the prerequisites for implementing your NAC solution?

These prerequisites include the tasks that must be performed and the expenses that must be incurred in order for the NAC solution to be implemented and operate as advertised. The answer to this question can reveal potentially hidden costs and complexities associated with implementing the NAC solution.

Here are some additional questions to ask about the prerequisites of a NAC solution:

- Does the solution require changes to your network architecture?
- Does the solution rely on specialized networking gear? Are you going to need to purchase additional networking equipment from the vendor itself or a third-party vendor?
- Does the solution require the networking equipment to be upgraded or replaced?
- Does the solution require the installation of software agents?
- How are admission checks performed?

The answers to these questions enable you to calculate the total cost of ownership of the NAC solution, including deployment expenses, such as including labor and hardware (upgrades, replacements, additional appliances, or servers needed, and so on).

Question #3 – What is the architecture of your NAC solution?

You should ask the NAC vendor to describe the architecture of its NAC solution. Requesting a description of the NAC architecture and then asking specific questions regarding the various

techniques, methods, and technologies will help you determine the strengths and weaknesses of the proposed solution.

Question #4 – How does your NAC solution perform element detection?

Element detection is a core feature that must be supported by a NAC solution. This essential NAC feature provides the ability to detect in real-time a new element attempting to attach itself to the network.

If a NAC solution cannot perform element detection in real-time, then it does not provide a valuable line of defense for your network. In other words, if the NAC solution does not support real-time element detection, you cannot expect it to defend against devices that it is not aware of.

Additional questions that can be listed in this section of your RFP include:

- How does the solution detect the presence of a new element?
- Does the solution use agents for element detection?
If the answer is yes, then not all devices can be detected. Elements on which agents cannot be installed must have their MAC addresses white-listed. This leaves these types of devices open to MAC spoofing-based attacks. For example, the white-listed MAC address of a printer can be detached and replaced with a laptop spoofing the MAC address of the printer without attracting the attention of an agent-based NAC solution.
- Does the solution use the switch for element detection?
It is important to know that not all switches support this capability. Relying solely on the capability of a switch to provide information regarding new elements connecting to the network is not reliable.
- Is element detection performed in real-time?
If element detection is not performed in real-time, then there is a time gap during which a malicious insider can freely operate on the network without being detected by the NAC solution.
- Does the element detection include hosts other than Microsoft Windows-based elements?
If the answer is no, then a malicious insider using a non-Windows-based operating system can freely operate on the network without being blocked by the NAC solution.
- How does the information regarding the elements residing on the network stay current?
- Does the solution utilize DHCP for element detection?
If the answer is yes, then there may be other elements operating on the network that may not make use of DHCP. Any element that is configured with a static IP address may not be detected by the NAC solution.
- Does the solution utilize 802.1x for element detection?
If the answer is yes, all networking equipment must support 802.1x – and there may be additional prerequisites, such as the installation of a software agent. With such a solution, you

may need to white-list non-802.1x compatible devices, thereby exposing your network to MAC spoofing-based attacks.

Question #5 – How does your NAC solution perform compliance checks

In this section of your RFP, the following questions should be asked:

- What are the parameters that can be checked when an element is being admitted to the network?
- Is a software agent required when performing compliance checks?
If the answer is yes, then the deployment of the NAC solution becomes complicated. As the number of systems on which an agent should be installed increases, so does the complexity of the deployment.
- What operating systems are supported with compliance checks?
- To what degree can the solution assist the organization in meeting the requirements of compliance regulations, such as Sarbanes-Oxley, GLBA, PCI, and HIPA?
- Can custom compliance checks be defined?

Question #6 – How does the quarantine mechanism of your NAC solution work?

There are a variety of quarantine methods available, each with varying strengths and weaknesses. However, it is important for you to understand if the quarantine method of the NAC solution can be bypassed and if it allows a quarantined element to interact and infect other quarantined elements.

In this section of your RFP, the following questions should be asked:

- Does the quarantine method rely on specialized hardware or software?
- When an element is quarantined, can it be infected by other quarantined elements?
You need to evaluate whether the quarantine area is shared between the quarantined elements. If so, they are able to easily infect and penetrate each other.
- When an element is quarantined, can other quarantined elements try to penetrate it?
An attacker might use a shared quarantine area as its entry point to the network in order to infect the other quarantined elements with zero-day malware. Once readmitted to the network, these elements may allow the attacker to access other parts of the network and information it should not access.
- Is the quarantine performed at Layer 2 or Layer 3?
Layer 3 is problematic because elements are still able to interact with other devices on the local subnet. Layer 3 quarantining enables the local infection of quarantined elements by another

quarantined element. It enables a quarantined element to directly attack another quarantined element in an attempt to abuse a given vulnerability to gain unauthorized access to the network.

- Can the quarantine mechanism isolate virtual machines?
As virtualization becomes an integral part of data centers, as well as R&D and QA environments, this is an important feature to consider.
- Can elements connected by a non-managed switch to a hub be placed in quarantine?

Question #7 – How does your NAC solution provide enforcement?

- How is enforcement performed?
- Is the enforcement carried out at Layer 2 or Layer 3?
Layer 3 is problematic because elements are able to interact with other devices on the local subnet.
- Does the enforcement involve the networking gear? If so, how?
The answer to this question may unveil hidden costs, ways to circumvent the solution, and so on.
- Does the enforcement depend on specialized hardware?
If the answer is yes, then there maybe additional deployment costs that you need to consider.
- Does the enforcement depend on specialized software?
- Can you enforce your NAC policy on individual virtual machines (specifically against virtual guests)?

3 Analyzing RFP Responses

The answers to RFP questions allow you to analyze the technology of the NAC solution, its time-to-value, and overall total cost of ownership – all important factors to take into consideration when making your buying decision.

Technology

Learn whether the offered NAC solution meets your security requirements. Evaluate the weaknesses of the offered solution and determine if the NAC solution can be easily bypassed.

Time-to-Value

One of the important aspects of deploying a NAC solution is how much time is required to deploy the NAC solution throughout the entire enterprise. This is an important consideration when deploying a NAC solution.

Total Cost of Ownership

Calculating the *total* cost of implementing the NAC solution, not just the licensing fee, is important for your evaluation. For each NAC solution you evaluate, take into consideration the costs associated with deployment, as these may increase the cost of the solution beyond your expectation. Included in the overall costs are the NAC product itself, any networking gear upgraded and/or replacements, servers and appliances needed for the NAC product, and labor efforts required to implement and manage the solution.

Ultimately, you should choose the NAC solution that provides with strong technology together with short time-to-value – at a reasonable total cost of ownership.