

## Understanding Network Access Control: What it means for your enterprise

Network access control is a term that is highly used, but not clearly defined. By understanding the reasons for pursuing a network access control solution, by assessing what needs to be accomplished, and by determining how the solution is to be implemented and used, organizations give themselves a much better chance of uncovering the right technology for their environment. Through a comprehensive series of business and technical questions, this paper helps you define and understand your organization's needs in relation to network access control.

# Understanding Network Access Control: What it means for your enterprise

## Overview

In Information Technology and Security there are multiple terms that mean different things to different people. For example, consider the phrase “policy compliance.” Many vendors use this phrase to market their wares while paying little or no attention to what it means to the enterprise. Compliance with policy can mean regulatory compliance, internal physical security compliance, legal compliance, internet-use compliance, network-use compliance, endpoint security compliance, and much more. A quick Google search alone shows the number of sponsored links for the term policy compliance, many of them devoted to vendor solutions. In truth, policy compliance has many facets and needs further distillation to be useful to an enterprise.

Another term that gets bandied about is “network access control” (NAC). In a young market, this term has become over used and highly misunderstood. NAC solutions encompass everything from intrusion detection systems, authenticated DHCP solutions, two-factor authentication, patch management solutions, network hardware, and security suites. These variations confuse the market and cause enterprises to compare apples to oranges when looking for a NAC solution.

The key to finding a good solution for NAC is first understanding what the terms involved mean to the enterprise, and then matching those expectations with what a vendor can provide. The assessment

questions that follow will help you with this task, enabling you to understand your organization’s needs in relation to NAC.

## Establishing a baseline understanding

To establish a baseline understanding, this document assumes that a NAC solution has four integral functions.\*

### 1 Definition and management of endpoint security policies

Setting up and managing a policy on who a user is and what needs to be running/not running on their machine to deem them safe and permit them access to the enterprise network.

### 2 Assessment of endpoint security policies

Providing a mechanism to assess the state of adherence to the endpoint security policies.

### 3 Enforcement of endpoint security policies

Providing/using a mechanism to automatically enforce endpoint security policies.

### 4 Reporting, alerting, and auditing

Providing a means to monitor the endpoints and the solution.

\* This simple framework is designed to keep the scope of this paper focused by removing from the equation aspects like intrusion detection, anti-virus applications, and personal firewalls.

## Assessment: Network Access Control and your enterprise

Many vendors have defined themselves as providing a complete NAC solution or a key component of NAC. However, it is important for an organization both to determine exactly what the vendor means by network access control and to assess what it means in the context of the problems that the organization is trying to solve.

By developing a greater understanding of NAC and endpoint policy enforcement, you can better determine how to approach a project. Answering the questions below will enable you to begin to define what access control means for your organization and start to shape a plan of attack. The next step will be to find the solutions that are available and to determine what questions you should pose to the solution vendors.

Each section contains space for you to add your own criteria. There are also more discursive questions where you can add your thoughts and relevant information.

### Section I Business issues

This section explores commonly raised NAC-related business issues, including questions about the reasons for pursuing a project, the potential costs/benefits, and who should be involved. While these are questions that every enterprise intuitively asks, agreeing upon and recording the answers often provides much needed direction in a NAC project.

What are the main problems we hope to solve via a NAC solution?

- Stemming the tide of worms and viruses that proliferate in the network.
- Securing corporate information by protecting our endpoints.
- Ensuring the return on investment of prior security applications – making sure they are all being used properly by all my users.
- Stopping rogue/unauthorized use of my network and mitigating the risk it imposes.
- Meeting internal or external regulations.
- Managing guest access to the network.
- Ensuring that my patch operation system is operating correctly and that necessary patches are installed on all my machines.
- Ensuring that every user on the network is identified.
- Protecting the enterprise by ensuring no file-sharing or peer-to-peer applications are operating on connected endpoints.
- \_\_\_\_\_

**Note**

*Security ROI is a difficult thing to measure accurately, as investing in security is much like investing in insurance. You need it to be there, you're more comfortable when it's there, and you're hardest hit when it is not. However, it is always best to take a look at what the current state is costing the enterprise by using various methods, such as cost of network downtime, cost of help desk response to security related incidents, and high and low-end estimated risk cost versus actual solution cost ratios.*

Why are we trying to solve these problems?

- Internal pressure to make proactive security a priority.
- External regulatory pressure.
- Risk of our data being compromised.
- Risk of bad publicity due to a security breach.
- Need to decrease the time, money, and effort spent on security problems.
- Experienced a recent security event and need to make sure it doesn't happen again.
- \_\_\_\_\_

Can we quantify what this problem costs our enterprise? Can we estimate what solving this problem is worth to us?

---

---

Do we currently know our risk levels associated with the endpoints using our network? Do we have independent mechanisms to audit them? Are we confident in those mechanisms?

---

---

What groups in our enterprise should be involved in a decision on NAC?

- Information security
- Network operations
- Desktop support
- Privacy/Compliance management
- \_\_\_\_\_

Who are the individuals in our organization that need to be involved in a NAC decision?

---

## Section II Technical issues

This section explores technical issues. The questions are designed to uncover the high-level technical needs of an organization, based loosely upon the technology for NAC available in the market today.

In our environment, we have people accessing the network via different means. What access methods do we need to control?

- Remote via VPN
- LAN via wired connections
- LAN via wireless connections
- \_\_\_\_\_

Are there segments of our user population that we would like to cover first? Are these segments based on types of users, types of access, or both?

---

---

---

How many users do we need to cover? How many network segments do we need to cover? How important is a scalable solution?

---

---

---

What methods for access control would be acceptable in our enterprise?

- Appliance based – Placing appliances at every access point.
- Software based – Leveraging current and future enforcement technologies with a software solution.
- A combination – Placing appliances in the network and placing software on each machine.
- Cisco standardization – All Cisco NAC-compliant hardware, Cisco Trust Agent, Cisco management solution.
- Microsoft standardization – All upgraded Microsoft OS, Microsoft servers throughout environment.
- Open standards based – Trusted Computing Group standards based technology.
- \_\_\_\_\_

When a corporate laptop or desktop accesses our network, what do we need to ensure before granting them access?

- They are a member of the corporate directory.
- Their machine is running a corporate standard image.
- Their security applications are running and properly updated.
- Their operating system is patched to the level I deem appropriate.
- They are not running any blacklisted software – e.g. Kazaa or Skype.
- They are running required corporate software.
- \_\_\_\_\_

When a non-corporate laptop attempts to access our network, what action do we want to take?

- Allow them access to the network.
- Quarantine their access to Internet only access.
- Block their access altogether.
- Quarantine them until they pass a health check.
- Be notified of the access attempt.
- \_\_\_\_\_

What is our preferred means of assessing each machine?

- "Agentless" – ActiveX- or Java-based deep assessment of a machine.
- "Agentless" – Access credentials needed for a deep remote assessment of each machine.
- "Agentless" – Monitoring traffic to/from each machine is sufficient.
- Agent-based – An agent that actively searches for elements placed in policy.
- Agent-based – An agent that listens to other elements that report in via APIs.
- A combination, dependent on type of user accessing the network.
- \_\_\_\_\_

Should a machine be assessed prior to granting connection or is it acceptable that a machine is assessed after making connection with the network?

---

---

What type of policy management should our NAC solution have?

- We would like to manage different policies for different user groups.
- We would like to manage policy centrally.
- We would like to script policy.
- We would like to manage policy via an intuitive GUI.
- We would like to have security applications and patches pre-populated for us to potentially use in policy.
- We would like the ability to write custom checks.
- \_\_\_\_\_

Do we want one central place to manage all access policies, or do we want to manage different types of users and different types of access points separately?

---

---

What technologies have already been placed in our network that we can leverage to quarantine and re-direct users?

- 802.1x on wireless LAN
- 802.1x on wired LAN
- DHCP
- "Registered" DHCP
- Cisco NAC-compliant routers and switches
- SSL VPN
- IP Sec VPN
- We don't want to leverage current infrastructure.
- \_\_\_\_\_

What is our deployment schedule? When do we want to achieve NAC throughout the enterprise?

- |   |  |
|---|--|
| <input type="checkbox"/> We needed it yesterday | <input type="checkbox"/> 1 year            |
| <input type="checkbox"/> 0-6 months             | <input type="checkbox"/> 2 years or longer |
| <input type="checkbox"/> 6-12 months            |  |

What type of NAC technology best fits our deployment schedule? What types of solutions have we been effective at deploying in this timeframe in the past?

- Appliance based – Placing appliances at every access point.
- Software based – Leveraging current and future enforcement technologies with a software solution.
- A combination – Placing appliances in the network and placing software on each machine.
- Cisco standardization – All Cisco NAC-compliant hardware, Cisco Trust Agent, Cisco management solution.
- Microsoft standardization – All upgraded Microsoft OS, Microsoft servers throughout environment.
- \_\_\_\_\_

What type of information do we want to gather from our access control and endpoint policy enforcement solution?

- Authentication information only.
- The state of each machine in relation to policy.
- The number of access attempts.
- How the enterprise looks as a whole in relation to security policies.
- The presence of rogue or guest devices attempting to access the network via standard methods.
- The presence of rogue devices attempting to access the network via more sophisticated methods (e.g. spoofing an IP address).
- \_\_\_\_\_

What type of remediation options do we want to offer to people who are out of compliance with policy?

- None.
- Access to the internet to download the necessary patches and updates.
- Messaging and specific directions based on their compliance with policy.
- Integration with our patch management solution.
- \_\_\_\_\_

What do we want our corporate end-user experience to be with a NAC and endpoint policy enforcement solution? What would best meet our business needs?

- Totally transparent for all machines attempting access.
- Transparent for compliant machines only.
- Very noticeable for all – we want users to be highly aware their machines must be in compliance and they play a large part in keeping them up to date.
- Different experiences for different groups.
- \_\_\_\_\_

What do we want our non-corporate/rogue end-user experience to be with a NAC and endpoint policy enforcement solution? What would best meet our business needs?

- Totally transparent for all machines attempting access.
- Transparent for compliant machines only.
- Very noticeable for all – we want users to be highly aware their machines must be in compliance, recognizing they are a guest on our network, and they play a large part in keeping it up to date.
- Different experiences for different groups of guests.
- \_\_\_\_\_

## The Sophos solution

Sophos NAC is a software solution that works with an organization's current networks to control access of all users based on who they are, where they are accessing the network, and the security state of their computer as dictated by the organization's policies. By supporting current network hardware and all security applications, using standards to prepare for tomorrow's networks, and providing a solution that is scalable and configurable to meet specific business needs, Sophos NAC is a market leader and the only truly independent and enterprise-ready software solution on the market today. Sophos is a member of the Cisco NAC partner program, the Microsoft NAP partner program (Microsoft Gold Certified), and the Trusted Computing Group's Trusted Network Connect program. In our deployments in global Fortune 100 companies, Sophos has shown we have the people, processes, and product in place to meet enterprises' network access control needs.

**To find out more about Sophos products and how to evaluate them, please visit [www.sophos.com](http://www.sophos.com)**

## About Sophos

Sophos is a world leader in integrated threat management solutions purpose-built for business, education and government. With 20 years' experience and consolidated anti-virus, anti-spyware and anti-spam expertise SophosLabs protects even the most complex networks from known and unknown threats. Our reliably engineered, easy-to-operate products protect over 35 million users in more than 150 countries from viruses, spyware, intrusions, unwanted applications, phishing, spam and email policy abuse. Round-the-clock vigilance has resulted in our increasingly rapid international growth, expanding user base and continuous profitability. Our instant response to new threats is matched by business-focused, 24/7 technical support, and has led to the highest levels of customer satisfaction in the industry.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France  
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2007. Sophos Plc.

*All registered trademarks and copyrights are understood and recognized by Sophos.  
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.*

**SOPHOS**  
[WWW.SOPHOS.COM](http://WWW.SOPHOS.COM)