

NAC at the endpoint: control your network through device compliance

Protecting IT networks used to be a straightforward case of encircling computers and servers with a firewall and ensuring that all traffic passed through just one gateway. However, the increase in mobile workers, numbers and type of device and the amount of non-employees requiring network access, has led to a dissolving of that network perimeter. Access requests can come from anyone and anywhere, which is why organizations are turning to network access control (NAC) technologies. This paper discusses why NAC is important and how it should be implemented on the endpoint for maximum protection.

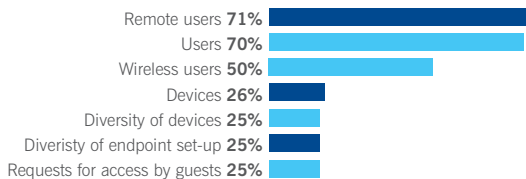
NAC at the endpoint: control your network through device compliance

Network protection in the past

Network protection used to be easy. Organizations erected a firewall around their IT assets and established just one route for inbound and outbound traffic. Employees and the computers they used were mostly office-based, and easily protected within this immovable perimeter from viruses, spyware and other malware. It was called the castle and moat approach; the castle being the office, the moat being the firewall¹.

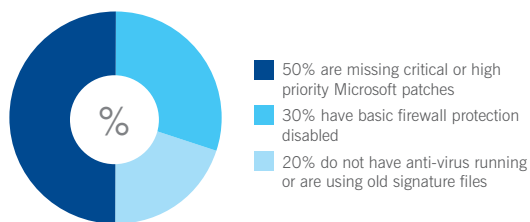
The changing business environment

However, technology and working practices have changed, and this has had a significant impact on the IT perimeter. Organizations also demand increasing mobility from employees – who in turn require network access while off-site – and need to open up their IT systems to contractors and guests. Research by the Aberdeen Group² shows that networks are encountering increasing numbers of devices, types of device, users and access requests (figure 1). As a result, network perimeters have dissolved and gaps in security have appeared.



Source: The Aberdeen Group, 2007

Figure 1: Where is your network use increasing?



Source: Sophos Endpoint Assessment Test, May 2008

Figure 2: Are your endpoint computers a security risk?

These gaps are significant. When assessing if their endpoint computers were a security risk³, organizations revealed a range of missing critical and basic security functions (figure 2). Such findings show that to better protect networks, IT teams need to concentrate on ensuring that each endpoint complies with their security needs, and enforcing that compliance where necessary.

How to control who uses the network

Organizations have increasingly turned to Network Access Control (NAC) technologies as a way of dealing with their ever shifting IT perimeters. In addition to the figures supplied by the Aberdeen Group, research by Forrester shows that network access is set to get even more complex, with 63 percent of North American enterprises planning an increase in their use of laptops⁴. This suggests that network boundaries will expand further, with many more workers requiring access from airports, cafes and their own homes.

As a result, NAC will become more central to corporate network defenses as it allows organizations to:

- Identify who is requesting network access
- Assess whether the user's computer has the correct security requirements
- Grant or refuse a request, or quarantine a computer until it complies with security requirements
- Ensure that users only visit that part of the network that their role or task requires.

Where to optimize control

The move away from the castle and moat approach has seen security vendors react with a range of hardware appliances and software solutions that address the problem of where access control should be deployed. There are currently three deployment choices:

- In the data path
- On the network
- At the endpoint.

NAC in the data path

This is called in-line enforcement and places a NAC appliance directly between the endpoint and the network. Data is unable to pass between the endpoint and the network without first being re-routed through the NAC appliance. Even though the data sent by the endpoint is scanned, in-line enforcement has drawbacks.

“

The best place for NAC is at the endpoint level as it ensures that the computer is automatically assessed before and during network connection.

”

Firstly, in order to provide comprehensive protection, NAC must reside at each physical location – such as every network entry point – which is costly as it requires additional hardware integration. Secondly, because it sits in the data path, in-line NAC appliances also add to data processing times, which lowers available bandwidth levels and reduces network speeds.

NAC on the network

Other NAC appliances work in what is termed “out-of-band”, in that they do not reside in the data path but are on the sidelines, watching as traffic passes by. They are called “post-connect” NAC appliances as they only scan data packets after the endpoint has connected to the network and begins to send traffic. These appliances typically look for abnormal behavior patterns in the data sent from the computer to determine whether it is infected. Again this requires substantial investment in additional hardware, since appliances need to be installed throughout a network.

NAC at the endpoint

The most effective deployment of NAC is to integrate it at the endpoint level, ensuring that the computer is automatically assessed before and during any connection to the network, at any time of the day or night. Importantly, this allows organizations to easily ensure that an individual endpoint is in compliance with their security requirements before it joins and (if out of compliance) compromises the network.

NAC at this level is entirely software-based. It has no impact on network processing speeds, and can easily be rolled out across an organization's existing complement of endpoint computers, plus any new devices as and when they are added to the network.

Endpoint NAC solutions are driven by centrally defined and managed security policies, which are able to cover every conceivable request and are easily updated. Updating in-line and out-of-band appliance policies are difficult, as they

suffer from being fragmented across the network, with separate pieces of hardware – possibly from different vendors – requiring their own policies.

For example, a NAC appliance at the gateway would need a policy to govern access for mobile workers, while one at a WLAN switch would need to cover office-based users. Any updates to an organization's overall policy would need to be replicated at each point, so that it remains consistent for employees who operate both on the road and in the office. Updating multiple policies is time-consuming and leaves open the possibility that one point in the network is overlooked, which can lead to a security hole or employees blocked from performing their normal duties.

NAC policies can be as specific as an organization requires and are flexible enough to react to changing organizational requirements. New individuals, groups or roles can quickly be added to ensure continued operational efficiency, while verification requests for the latest security patches can also be included.

Ensuring compliance

Placing NAC at the heart of their endpoint defenses allows IT administrators to control what many consider their greatest threat to network security: their own employees⁵.

An unintended consequence of providing employees with company-issued endpoint devices is configuration drift. Many organizations grant individual users administration rights over their device as a way of easing helpdesk enquiries and providing workers with a level of flexibility. Over time many users then change their device's configuration, so that it drifts away from the organization's security policy until it is out of compliance. Examples of configuration drift include the disablement of personal firewalls and the installation of Instant Message (IM) software – both of which cause significant security holes.

NAC can identify if an endpoint computer's configuration has altered since it was last

connected to the network, and then bring it back into compliance before access is granted. For example, firewalls are automatically switched back on and IM software disabled.

Who and what wants access?

Endpoint-based NAC works with both managed and unmanaged devices, and both known and unknown users.

Device and user types

- » **Managed device used by a known user.** This is a company-issued computer where the organization can dictate the software installed and the compliance policies.
- » **Unmanaged device used by a known user.** This is a guest – typically a contractor – who requires network access via their own computer. The organization has no right to install software, but certain types of application (e.g. anti-virus) can be mandated without specifying a vendor.
- » **Unmanaged device used by an unknown user.** This is an access request from a stranger, which can be restricted or blocked.

Managed devices

With a managed endpoint organizations install a NAC agent directly onto the device, which communicates directly with the NAC policy server. The agent is able to assess the device against the organization's security policy, and request updates from the server if the policy has been changed.

When a user travels and is not connected to the corporate network the NAC agent can stay in communication with the NAC policy server over the internet. If the policy server is not accessible, the agent uses the cached policy on the device's hard drive, ensuring that the endpoint remains consistent with the security policy, and protected until it next connects to the network.

Unmanaged devices

Non-employees requiring network access through their own endpoint computers is increasingly common, with examples including auditors undertaking annual audits, contractors contributing to projects and clients requiring internet access.

NAC deals with unmanaged computers by downloading a dissolvable agent to undertake pre-connection scanning. The device is checked to see:

- The type of security application, vendor and version number that is running
- Whether it has the latest operating system patches
- When it was last scanned for malware
- If its signature files are up-to-date.

Easy implementation

Software-based NAC solutions also reduce the impact of an implementation, as it can be rolled out in stages. Unlike NAC appliances, that require parts of the network to be disabled so they can be plugged in, software deployments allow organizations to assess their endpoints and ensure compliance without taking any of the IT infrastructure off line.

Such implementations have four stages:

- Define
- Assess
- Remediate
- Enforce.

Define the policy

Before any NAC solution is implemented organizations need to define exactly how a user's device needs to be configured in order to gain network access. It is at this point that policies are written. IT teams can ensure that certain applications not normally used for business operations, for example peer-to-peer applications, are not installed or running. They can also decide

on the type of user, group or role that should or should not be granted specific access privileges. For example, a solution could be set-up to allow a member of the sales team access to the sales server, but also to block any requests for non-sales servers and applications, such as information held by the HR department.

Policies can define network access requests against a range of criteria. In addition to the type of device and user, a policy might also define the request against where it is geographically originating from. For example, devices connecting remotely over a VPN may have different access privileges than a device connected to the LAN.

Assess the endpoint

NAC software can initially be implemented in a report-only mode. This allows organizations a network-wide view of how each endpoint device complies with policy, without interrupting its day-to-day operation. The solution runs in the background, while the endpoint continues its normal business.

From these reports IT teams can gauge how severe their non-compliance problem is and plan their response.

Remediate the problem

Many out of compliant situations on managed devices can be fixed automatically, reducing the administrative burden on the IT team and ensuring full network security.

Managed devices that, for example, lack up-to-date anti-malware signatures, have disabled firewalls, missing operating system patches or application security patches, will be updated by the NAC agent. The update will take place without the user or administrator needing to take any action, reducing the impact on IT resources and user workflow.

Unmanaged devices typically cannot be handled this way because they are not under an organization's direct control. Remediation is handled by sending the user a message, with instructions on what they need to do in terms of updating their endpoint computer in order to gain network access.

Enforce security

The final stage of implementation concerns endpoint devices that are unknown and have no business trying to gain network access privileges. Such computers present a clear security threat, and NAC software responds by simply blocking access to the network in coordination with the existing network infrastructure.

Summary

The IT network perimeter is dissolving and becoming increasingly difficult to secure. This is due to the growing number of devices and methods of access, such as employees working from home or on the road, and logon requests from contractors, clients and other guests. To manage who and what connects to their network, organizations are turning to NAC, which is best deployed at the endpoint level. Software-based NAC is proving superior to hardware-based solutions as it easily provides coverage for all existing endpoint devices and new ones as they are added. Software-based NAC can also be deployed across an organization in stages, ensuring minimal impact on infrastructure and IT resources.

Sophos solutions

Sophos provides NAC solutions for assessing and controlling all managed and unmanaged computers.

Endpoint Security and Control provides organization's with fundamental control of the security status of managed and unmanaged computers.

Sophos NAC Advanced allows greater control through more sophisticated policy definition and advanced reporting capabilities.

Sources

- 1 *NAC for Dummies*, Wiley Publishing, Inc., 2008
- 2 *Who's got the NAC? Best practices in protecting network access*. The Aberdeen Group, October 2007.
- 3 Sophos Endpoint Assessment Test, May 2008
- 4 *Client Management 2.0*. Forrester, March 2007.
- 5 Sophos web poll, September 2007.

About Sophos

Sophos enables enterprises worldwide to secure and control their IT infrastructure. Our network access control, endpoint, web and email solutions simplify security to provide integrated defenses against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage and compliance drift. With over 20 years of experience, we protect over 100 million users in nearly 150 countries with our reliably engineered security solutions and services. Recognized for our high level of customer satisfaction, we have an enviable history of industry awards, reviews and certifications. Sophos is headquartered in Boston, MA and Oxford, UK.

Boston, USA • Oxford, UK

© Copyright 2008. Sophos

*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