

NAC: Managing unauthorized computers

Unauthorized endpoint computers pose significant security risks to organizations. Where underlying network-based enforcement is available, network access control (NAC) solutions provide detection and implementation of security policies to minimize these risks. However, in some environments the network cannot provide this enforcement. This paper looks at how a complete NAC solution can protect the network from unauthorized access from unknown computers or people with malicious intent.

NAC: Managing unauthorized computers

Overview

Having an enterprise-level strategy for security compliance and access control is essential to protecting the organization from possible threats. The core infrastructure and network-based resources must be protected using multiple safeguards at multiple access points throughout the enterprise. Well-integrated, multilayered security systems are the best methods for controlling threats to those resources.

Effective enterprise NAC solutions rely on the ability of the network to positively enforce compliance and affirmatively block or quarantine access to computers that are unauthorized.

Network access control (NAC) solutions enable organizations to reduce vulnerabilities by defining and managing security policies, and introducing assessment capabilities and enforcement methods to control access to the network. The best NAC solutions permit regulated access for known and secure/compliant users while also disabling or controlling the use of high-risk applications on those users' computers. Additionally, leading NAC solutions can be configured to prevent or quarantine access by unauthorized or unknown computers. Although most users do not have malicious intentions, unauthorized computers pose a big security risk to organizations.

The key requirement of a complete NAC solution is to identify and block such rogue computers, such as a user who is intentionally bypassing standard network connection methods, and may be malicious.

How NAC handles rogue computers

NAC solutions permit access to authorized computers by evaluating and enforcing the computers' security state based on whether they comply with the organization's security policy. Endpoint computers are permitted access to network resources when they conform to policy, and are denied or quarantined from access when they do not conform. These functions are performed most effectively by using a combination of network- and client-based enforcement points, such as DHCP, 802.1X, wireless LAN, SSL or IPsec VPN, and client-based enforcement.

Effective enterprise NAC solutions rely on the ability of the network to positively enforce compliance and affirmatively block or quarantine access to unauthorized computers, i.e. those that are either non-compliant or unknown. In most cases, the network or client software provides the necessary enforcement and quarantine mechanisms. However, there are scenarios where certain network-based enforcement mechanisms cannot fully enforce compliance, and where no client is present that can provide client-based enforcement.

Where there is no network enforcement

Scenarios where network-based enforcement does not provide 100% coverage include DHCP networks or where the endpoint is using local, statically assigned IP addresses for network access and a quarantine agent is not installed on the endpoint. Although an enterprise can use DHCP to assign a combination of dynamic and static IP addresses, this case refers to those clients that are not using DHCP to obtain that address.

“Organizations need to protect their networks from intelligent users that deliberately try to evade security enforcement when accessing network resources.”

In this instance, the risk arises from an intelligent user deliberately trying to evade enforcement when accessing network resources. The number of unauthorized computers trying to access the network constitutes a small percentage of overall network use, but because of the nature of the method of access and unknown intent, administrators need to be alerted to the threat and be able to mitigate the risk. The damage to a network from just one rogue computer could be immense.

Fitting NAC into a typical environment

Once an organization has identified the need for a NAC solution, and implemented and rolled it out to all or part of its end users, additional requirements become apparent, such as protecting against unauthorized computers connecting to the network.

A complete NAC solution must do the following:

- Integrate with existing network configurations with minimal impact and cost of upheaval.
- Provide comprehensive support for the organization's security strategies and have the ability to create and manage policies that support those strategies.

Network considerations

Today's commonly deployed enterprise networks share characteristics that make them vulnerable to certain kinds of malware and unauthorized users:

- Open, collaborative environments allow many different types of user to access information and services, including employees, customers, prospects, vendors, contractors, and suppliers.
- Increased access by trusted individuals can result in a higher risk of non-trusted parties accessing the network, potentially putting the business at risk.

Therefore, a NAC solution must ensure that the network is adequately protected.

- Remain flexible enough to meet new strategies as they inevitably arise.
- Offer capabilities beyond standard network-based enforcement, and identify and provide protection against all classes of users trying to access the network – both known and unknown.

While 802.1X can provide robust enforcement, many network switches in use today do not support 802.1X, and organizations are averse to the disruption and cost of upgrading. Furthermore, 802.1X must be applied to the whole user base – any area without enforcement remains vulnerable. The majority of organizations today want to get the best from their existing enforcement mechanism, which in most cases is DHCP. The biggest risk is that of a rogue computer using a static IP address to access the network.

A NAC solution that delivers enforcement around the existing deployed network infrastructure will drastically reduce risk levels, but the addition of a method to identify and stop unauthorized computers becomes critical to an enterprise when completing its NAC capabilities.

The ideal NAC solution

A complete NAC solution ideally extends the capability of DHCP-based enforcement, providing the following:

- Real-time alerting of the MAC and IP addresses, with no false positives, so that administrators can take immediate action when an unauthorized endpoint computer connects to the enterprise network.
- An ability to be deployed in enterprises of all sizes, with built-in redundancy for reliability and extra security.
- Centralized, simplified administration that allows administrators to exempt computers from alerting by MAC address or prefix, or by IP address, subnet, or range.
- Integration with network-based enforcement to automate the process for known, compliant computers.
- Comprehensive reporting for easy ongoing administration, including multiple reports for rogue endpoints, exempt endpoints, and alert information.

The solution should monitor the network passively without interfering with normal network communications, detecting and alerting the administrator when unauthorized computers attempt to connect. Low-level ARP (Address Resolution Protocol) monitoring allows all IP communications to be detected. Even if a computer evades DHCP or 802.1X network-based enforcement, the computer cannot communicate and spread infections throughout the network without using ARP. By monitoring ARP, identifying which computers are attempting IP connections, and comparing the computer with the list of approved, compliant, and registered computers, it is possible to tell if an unauthorized computer is using the network.

Once a rogue computer is identified, the administrator can be alerted with the computer's MAC or IP addresses. The administrator can then identify its network location and take appropriate security actions.

Summary

Organizations need to employ total network access control, not just to ensure compliance of known computers – whether managed or unmanaged – but also to exclude unauthorized computers. A complete NAC solution must fit into the current network environment, and support security initiatives as they evolve. By implementing a flexible and dynamic strategy, an enterprise can combat today's threats and still remain nimble enough for tomorrow's potential threats. ◆

The Sophos solution

Sophos NAC Informant uses a combination of passive network monitoring and advanced correlation and alerting systems to provide early warning when unknown or unauthorized computers attempt to connect to the network, giving administrators the time and critical information required to isolate them.

Sophos NAC and **Sophos NAC Informant** together provide complete protection against all classes of computers that can access the network, including managed, unmanaged, and unauthorized computers.

To find out more about Sophos products and how to evaluate them, please visit www.sophos.com

See also

- 1 NAC: Bridging the network security gap. Sophos white paper, April 2007
www.sophos.com/security/whitepapers/sophos-nac-bridging-the-gap-wpus.pdf

About Sophos

Sophos is a world leader in IT security and control. We offer complete protection and control to business, education and government organizations – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, and policy abuse, and providing comprehensive network access control (NAC). Our reliably engineered, easy-to-operate products protect over 100 million users in more than 150 countries. With over 20 years' experience and a global network of threat analysis centers, the company responds rapidly to emerging threats and achieves the highest levels of customer satisfaction in the industry. Sophos is a global company with headquarters in Boston, MA., and Oxford, UK.

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