WHITE PAPER

NETWORK ADMISSION CONTROL

EXECUTIVE SUMMARY

Network Admission Control (NAC), an industry initiative sponsored by Cisco Systems, uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from viruses and worms.

Using NAC, organizations can provide network access to endpoint devices such as PCs, PDAs, and servers that are verified to be fully compliant with established security policy. NAC can also identify noncompliant devices and deny them access, place them in a quarantined area, or give them restricted access to computing resources.

NAC is part of the Cisco Self-Defending Network. Its goal is to create greater intelligence in the network to automatically identify, prevent, and adapt to security threats.

WHY NAC?

Traditional identity management solutions can verify *who* a user is that is logging onto a network, and *what* the user is allowed to do, but do nothing to verify that an endpoint device conforms to security policy. As a result, networks are regularly compromised by the introduction of endpoint devices that do not conform to network security policy, which then spread viruses and worms throughout the networked environment. NAC addresses this issue by making sure that every endpoint device entering the network conforms to policy.

INTRODUCTION—RESPONDING TO THREAT EVOLUTION

Viruses and worms continue to disrupt business, causing system downtime, lost productivity, significant recovery costs, and expenses due to continual patching. The self-propagating nature of the latest computer attacks makes them especially virulent and damaging.

Security solutions that address this issue include antivirus software and intrusion prevention solutions. Existing antivirus solutions must be updated and maintained regularly, as they rely on current attack signatures in order to identify and mitigate attacks. Further, since they are unable to detect and contain “day-zero” viruses and the denial-of-service (DoS) attacks that they spawn, desktops and servers must also be hardened against attacks using intrusion prevention software such as the Cisco Security Agent. The installation and maintenance of these solutions is essential to any network security policy.

Servers and desktops not compliant with corporate security policy are common, and are difficult to detect, locate, contain, and cleanse. Locating and isolating these systems is time- and resource-intensive. Network availability is often unnecessarily compromised in order to protect computing resources while an infected device is located and repaired. Furthermore, infections can spread in such a way that remediation is extremely complex, often resulting in infections that appear to be removed from the corporate network but reappear at a later time.

Cisco Systems, Inc.
All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]

INFOEXPRESS, INC. - EX2413

The problem is compounded by the complexity of today's networked environment, which contains:

- Multiple types of end users—Employees, vendors, and contractors
- Multiple types of endpoints—Company desktop, home, and server
- Multiple types of access—Wired, wireless, VPN, and dialup
- Multiple types of services that can be compromised—Voice over IP (VoIP), e-commerce, B2B, Web servers

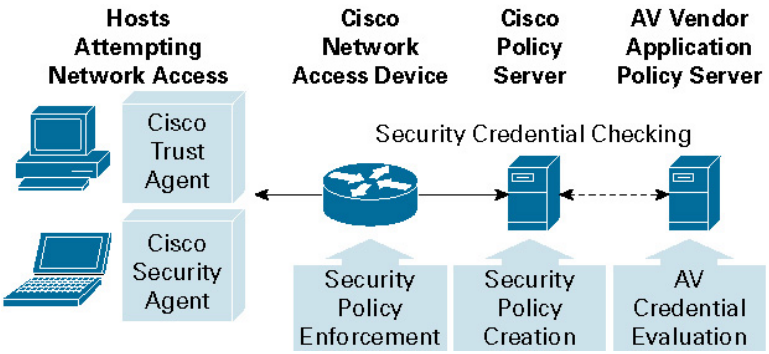
NAC counters newly evolved threats, addresses the environmental complexity of today's networks, and provides a real advance over point security technologies that have focused on the host, rather than global network availability and overall enterprise resiliency.

An Overview of Network Admission Control

The significant damage caused by recent worms and viruses demonstrates the inadequacy of existing safeguards. NAC provides a new, comprehensive solution that allows organizations to enforce host patch policies and to regulate noncompliant and potentially vulnerable systems by assigning them to quarantined environments for remediation. By combining information about endpoint security status with network admission enforcement, NAC enables organizations to dramatically improve the security of their computing infrastructures.

NAC allows network access to compliant and trusted endpoint devices (PCs, servers, and PDAs, for example), and restricts the access of noncompliant devices. Network access decisions can be based on such information as the endpoint's antivirus state, operating system version, operating system patch level, or Cisco Security Agent version and settings.

Figure 1
NAC



All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

NAC has the following components:

- Cisco Trust Agent—A software tool that resides on an endpoint system and collects security state information from security software solutions, such as antivirus and Cisco Security Agent clients, and communicates this to the network access device. Cisco Systems has licensed its trust agent technology to the NAC cosponsors—market-leading security software developers—in order to gather and report security state levels to the network policy server. Cisco Trust Agent is integrated with the Cisco Security Agent to provide endpoint security information such as operating system version, patch level, and Cisco Security Agent version and settings.
- Network access devices—Network devices that enforce admission control policy include routers, switches, wireless access points, and security appliances. These devices demand host security "credentials" and relay this information to policy servers, where NAC decisions are made. Based on customer-defined policy, the network will enforce the appropriate admission control decision—permit, deny, quarantine, or restrict.
- Policy server—Evaluates the endpoint security information relayed from the network access device and determines the appropriate access policy to be applied. Cisco Secure Access Control Server (ACS), an authentication, authorization, and accounting (AAA) RADIUS server, is the foundation of the policy server system. It works in concert with NAC cosponsor application servers, such as security policy servers that are able to provide deeper credential validation.
- Management system—CiscoWorks VPN/Security Management Solution (VMS) provisions NAC elements, while CiscoWorks Security Information Manager Solution (SIMS) provides monitoring and reporting tools. NAC cosponsors also provide management solutions for their endpoint security software.

Crucially, NAC uses existing investments in network infrastructure and host security technology by linking the two to provide a NAC facility. For example, organizations can ensure that the use of antivirus software is enforced by the Cisco network—routers, switches, wireless, and security appliances. In this way, NAC complements, rather than replaces, classic security technologies already widely used—firewalls, intrusion protection systems, user authentication, and communications security.

NAC in Action

An access control solution is only effective if it can identify and evaluate all of the devices seeking to access the network. NAC's unique implementation provides a flexible and ubiquitous solution capable of providing protection to all connected computing systems. NAC operates across all access methods that hosts use to connect to the network, including campus switching, wired and wireless, router WAN and LAN links, IP Security (IPSec) connections, remote access, and dialup links.

Cisco Systems, Inc.
All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

NAC deployment examples include:

- Branch-office compliance—NAC helps to ensure the compliance of hosts in remote or home offices attempting to connect to corporate computing resources, either over a private WAN or through a secure channel across the Internet. This includes performing compliance checks at the Cisco branch or main office router.
- Remote-access security—NAC helps to ensure that remote and mobile worker desktops and laptops have the latest antivirus and operating system patches before allowing them to access company resources through dialup, IPSec VPN, or other connections.
- Wireless campus protection—NAC checks hosts connecting to the network via wireless to ensure they are properly patched. The 802.1x protocol is used in combination with device and user authentication to perform this validation.
- Campus access and data center protection—NAC monitors desktops and servers within the office, helping to ensure that these devices comply with corporate antivirus and operating system patch policies before granting them LAN access. This reduces the risk of virus and worm infections spreading within an organization by expanding admission control to Layer 2 switches.
- Extranet compliance—NAC can be used to check the compliance of every system trying to obtain network access, not just those managed by IT. Managed and unmanaged hosts, including contractor and partner systems, may be checked for compliance with antivirus and operating system policy. If the Cisco Trust Agent is not present on the interrogated host, a default access policy can be enforced.

Benefits of NAC

- Dramatically improved security—NAC helps to ensure that all hosts comply with the latest corporate antivirus and operating system patch policies prior to obtaining normal network access. This provides proactive network protection against the proliferation of viruses and worms. Because only the network touches every device, NAC allows you to use the network for 100-percent auditing and enforcement of host security policies. Network segmentation services, via access control lists (ACLs) or VLANs, provide a powerful and efficient way to isolate and remediate vulnerable and noncompliant hosts, preventing them from spreading infection, or from being the targets of or the sources for worm and virus infections.
- Extending the existing network and security investment—NAC integrates with and increases the value of investments of both the Cisco network infrastructure and the host security technology.
- Increased resilience and availability—By taking information about endpoint security status and combining it with network admission enforcement, NAC enables customers to dramatically improve the security of their computing infrastructures. NAC provides comprehensive admission control access across all access methods, and ensures that all endpoints comply with corporate policy.

Availability and Use

Phase 1 of NAC, released in June, 2004, supports Cisco routers communicating with the Cisco Trust Agent to gather endpoint security credentials and enforce admission control policy. Router ACLs will restrict the communications between noncompliant hosts and other systems in the network—for example, only allowing communications to an antivirus server in order to download a new pattern file. NAC currently support endpoints running Microsoft Windows NT, XP, and 2000 operating systems.

Cisco Systems, Inc.
All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

"Recent worm and virus infections have elevated the issue of keeping insecure nodes from infecting the network and have made this a top priority for enterprises today," said Mark Bouchard, senior program director, META Group. "Many organizations were successful at stopping recent worm attacks at their Internet boundaries, yet still fell victim to the exploits when mobile or guest users connected their infected PCs directly to internal LANs. Eliminating this type of threat will require a combination of strengthened policies and NAC technology."

This first release of NAC addresses the two most pressing compliance tests required—antivirus software state and operating system information. This includes antivirus vendor software version, engine level, and signature file levels, as well as operating system type, patch, and hot fix. NAC is likely to first be used in monitoring mode, where host compliance will be assessed without any attempt to restrict network access. During this time, noncompliant systems may be updated as needed in order to reach desired compliance levels.

In Phase 2 of NAC, Cisco switches will be able to assign noncompliant hosts to quarantine VLAN segments on which only remediation servers reside. NAC will also support IPSec remote access platforms, such as the VPN 3000 concentrators, and expand support for additional endpoint operating systems. Cisco will also expand support beyond the initial NAC cosponsors in order to support an even broader range of access policy assessment and enforcement through the implementation of a broad API.

Future NAC releases will support additional access devices, such as firewalls and wireless access points, and continue to expand the platforms which it will support.

Conclusion—The Cisco Self-Defending Network

NAC is a crucial component of the Cisco Self-Defending Network, an innovative, multiphased security initiative that dramatically improves the ability of networks to identify, prevent, and adapt to security threats. The Cisco Self-Defending Network initiative significantly advances Cisco's strategy of integrating security services throughout IP networks by delivering new system-level network threat defense.

FOR MORE INFORMATION

For more information, visit: http://www.cisco.com/go/nac

Cisco Systems, Inc.
All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Catalyst, and Cisco IOS are registered trademarks or tradmarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

RD/LW 6416 06/04