Cisco Network Admission Control (NAC)

At-A-Glance

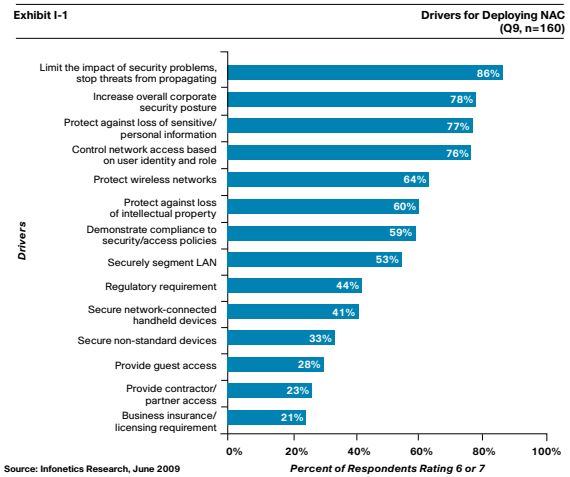
Stop Threats to Your Network from Unauthorized Access and Devices

Stop unauthorized or noncompliant devices and users from propagating threats into your network. Cisco® Network Admission Control (NAC) enforces your organization's security policies and posture on all devices and users seeking network access.

Current business mechanisms such as Web 2.0, social networking, and cloud computing increase the likelihood of sensitive data residing outside of company-owned devices. Traditional security products designed to protect closed environments with well-defined security boundaries are not effective in the new business environment.

Cisco NAC prevents loss of sensitive information by giving organizations a powerful, role-based method of allowing only compliant and authorized access and improving network resiliency. With Cisco NAC, only compliant and trusted endpoints—from PCs to printers, IP phones, and PDAs—are allowed onto the network, thereby limiting the potential damage from emerging security threats and risks.

Why do IT managers and CIOs look at NAC?



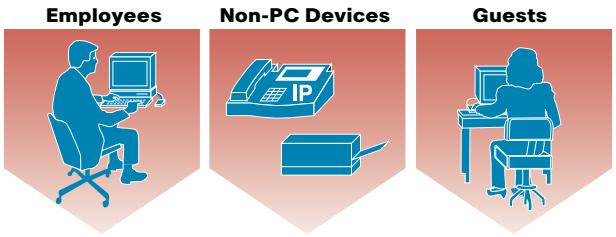
According to research conducted by Infonetics in June 2009, threat prevention from end devices is the number-one cause for considering NAC.

Why Cisco NAC?

1. **Collaborate with confidence.** Cisco NAC helps ensure that both employees and guest endpoints conform to your security policy, enabling you to collaborate with business partners while maintaining high security and compliance thresholds.
2. **The most comprehensive NAC solution.** Cisco NAC covers managed and unmanaged assets; deals with employee and non-employee devices; and helps ensure compliance of wireline and wireless-connected endpoints, VPN access, and guest users.

   With flexible deployment scenarios, Cisco NAC helps ensure that connected endpoints conform to your security policy.

Covers All Use Cases



Cisco NAC covers all use cases supporting employee and non-employee endpoints, managed and unmanaged assets, and Windows, non-Windows, and non-PC machines.

3. **The world's most trusted NAC solution.** Pioneering NAC in 2004 and with more than 4500 customers worldwide, Cisco is recognized as the world's leading NAC vendor, and has won numerous industry awards.

"Because network access control (NAC) is an embedded feature of so many network and security components, enterprises should look first within their existing vendor base to evaluate NAC solutions."

Gartner, Inc. Magic Quadrant for Network Access Control by Lawrence Orans, John Pescatore, Mark Nicolett, 27 March 2009

Cisco NAC's Main Capabilities

- **Role-based access control:** Controls access to authorized resources by verifying user privilege level. Cisco NAC provides full integration with wireless, VPN, and LAN switches.
- **Endpoint security, enforcement, and remediation:** Enforces security policies to an endpoint device during connection. Cisco NAC integrates with more than 350 antivirus and security applications from leading solution providers. Silent remediation, auto remediation, and other features help bring devices into compliance with little to no user impact.
- **Guest access and dynamic user provisioning:** Allows organizations to collaborate with confidence by providing secured guest access based on a user's role in the organization. Visitors and guests can stay in touch with their own companies without sacrificing the "host" organization's security.
- **Non-PC device support and data gathering:** Delivers automated non-PC device support by identifying, tracking, and placing the devices into pre-assigned network segments based on security policy requirements. This capability dramatically improves operational efficiency by freeing up IT personnel resources for other tasks.

Cisco Network Admission Control (NAC)

Cisco NAC Solution Components

CORE

Cisco NAC Manager: Provides a Web-based interface for creating security policies, establishing user roles, conducting compliance checks and remediation requirements, and managing online devices and users. Cisco NAC Manager communicates with and manages the Cisco NAC Server.

Cisco NAC Server: The enforcement component of Cisco NAC. Performs device compliance checks as users attempt to access the network. Cisco NAC Server can be implemented in band or out of band, in Layer 2 or Layer 3, and as a virtual gateway or as a real IP gateway. It can be deployed locally or around the world.

OPTIONAL

Cisco NAC Agent: Lightweight, read-only agent that performs deep inspection of security profiles on an endpoint device. Cisco NAC Agent is available as both a persistent agent and as a Web-based, dissolvable agent.

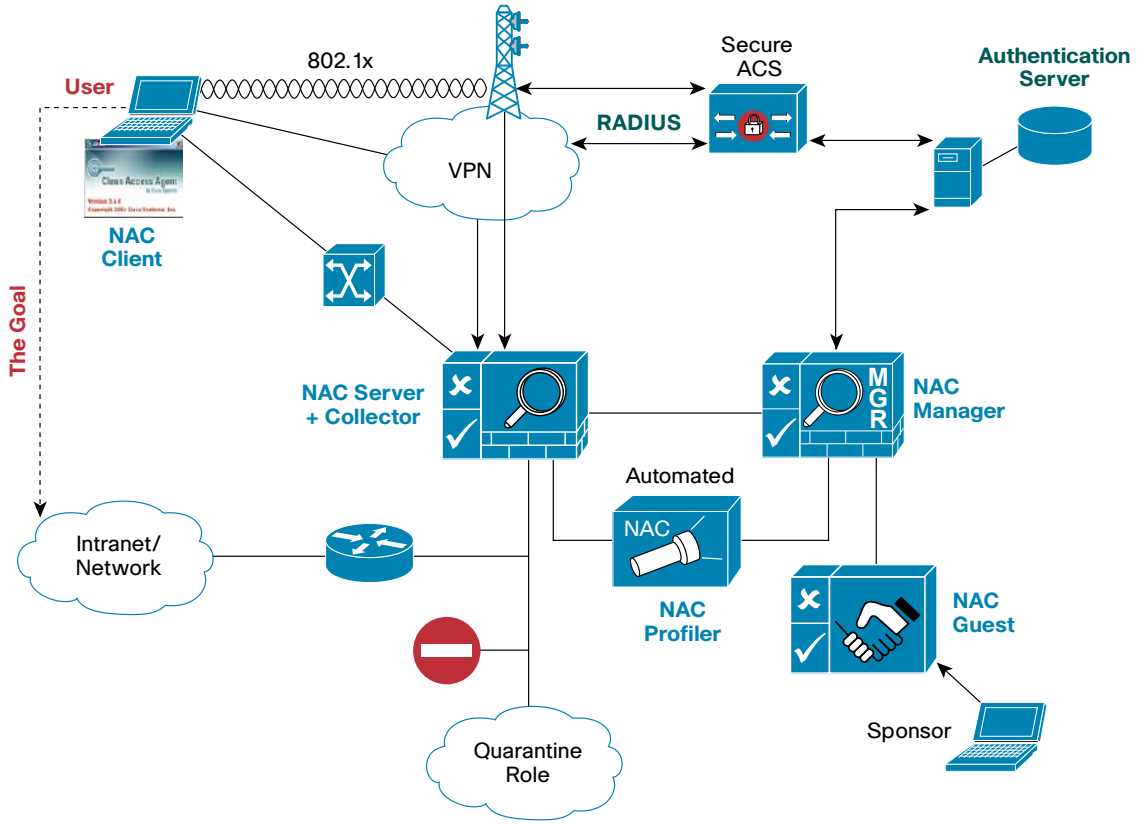
Cisco NAC Guest Server: Simplifies the provisioning, notification, management, and reporting of guest users on wired and wireless networks, offloading from IT staff many of the challenges commonly associated with supporting corporate visitors.

Cisco NAC Profiler: Provides non-PC device profiling by keeping a real-time, contextual inventory of all devices in a network, including non-authenticating devices such as IP phones, printers, and scanners. NAC Profiler discovers, tracks, and monitors the location, types, and behavior of all LAN-attached endpoints.

Cisco Secure Access Control System (ACS): The world's most trusted and widespread access control policy system provides Cisco NAC with 802.1x authentication support for wireless and VPN access. ACS is ideal when applying NAC to large corporate LANs.

Cisco NAC Implementations

- **Secure ACS-based implementation:** 802.1x is required. Role assignment is based on ACLs or VLANs. No immediate requirement for posture assessment
- **Direct NAC implementation:** Device security compliance required. Only VLAN role assignment needed. No 802.1x deployed.
- **Next-generation policy platform:** Both 802.1x and device security compliance will be available. TrustSec services available.



C45-542749-00 06/09