

### Why Should I Care About Network Admission Control?

Perimeter network security defenses alone and traditional network security products working independently are no longer sufficient to combat internal threats, rapidly propagating threats, and disappearing security boundaries. Organizations need more comprehensive, pervasive, and tightly integrated security solutions. Network Admission Control (NAC) offers a robust and comprehensive security solution.

### What Are the Main Functional Areas of Network Admission Control?

There are four main functional areas of a true NAC solution:

- **Policy compliance evaluation and verification (devices and users).** A NAC solution must be able to associate a device to its user (if any) and determine the appropriate security policies that apply. It should also evaluate and verify endpoint security posture information before the device gains network access. Solutions that cannot verify user credentials cannot protect against unauthorized access.
- **Policy enforcement and access control.** A NAC solution must be able to reliably deny, permit, or redirect (quarantine) network access depending on the level of policy compliance. Cisco NAC provides enforcement with the network infrastructure; it does not rely on client-based or DHCP-based mechanisms that are easily defeated by users. The network infrastructure represents the most robust enforcement point, as client-based or DHCP-based mechanisms are easily defeated by users.
- **Remediation.** A NAC solution must bring noncompliant devices into compliance. Remediation should be automatic, or it should guide the users through the tasks that achieve compliance. Shutting down ports on a network is not an effective remediation solution; it decreases productivity, increases the burden on the help desk, and does not address the root cause problem.

- **Flexible deployment and policy.** Networks often accommodate a variety of endpoint operating systems and owners as well as devices such as IP phones and networked printers. Consistent policy should apply to all these endpoints, regardless of whether they connect through VPNs, wireless access points, or hard-wired Ethernet ports. Few products on the market today can support all operating systems, all access methods, and policy exceptions in a scalable, manageable manner.

### What is Cisco NAC?

Cisco NAC is a solution that uses the network infrastructure to enforce security policies on all devices seeking to access network computing resources. Cisco NAC minimizes the risks associated with noncompliant devices—regardless of system type, ownership, or access methods—resulting in more resilient and secure networks. Its features fulfill the four main components of an effective, robust NAC solution.

### What Benefits Can Cisco NAC Provide?

Cisco NAC is a powerful security policy enforcement solution that addresses today's security challenges for organizations of all sizes. Cisco NAC provides a proactive, pervasive, and in-depth security defense throughout the network infrastructure and delivers several business benefits:

- **Secure both corporate and noncorporate assets.** Cisco NAC ensures that configuration standards are applied to all assets, whether they are corporate-owned or not. Effective asset management and controls result in lower total cost of ownership of the infrastructure and lower operational expenses.
- **Ensure policy compliance.** Cisco NAC provides security policy compliance enforcement at the network level. By enforcing security policies, Cisco NAC also assists organizations in adhering to privacy and regulatory compliance requirements, including Sarbanes-Oxley, HIPAA, and GLBA.
- **Proactively protect against worms and viruses.** Cisco NAC reduces and prevents large-scale infrastructure disruptions caused by vulnerability-based exploits. By eliminating the preconditions for these exploits and

attacks, organizations can achieve higher network availability and resiliency and radically lower the cost of fixing vulnerabilities and maintaining device compliance.

- **Integrate and collaborate with the Cisco Self-Defending Network.** Cisco NAC is a strategic element of the Self-Defending Network. Working together with other Self-Defending Network components such as the Cisco Security Agent and the Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS), Cisco NAC helps organizations achieve more accurate threat identification and prevention.

### How Do I Start with Cisco NAC?

For rapid deployment today, the Cisco NAC Appliance (formerly known as Cisco Clean Access) combines endpoint compliance assessment, user identity authentication, policy management and enforcement, and remediation services. The solution consists of the following components:

- **Cisco Clean Access Manager.** The Clean Access Manager provides a Web-based interface for creating security policies and managing online users. It can also act as an authentication proxy to authentication servers on the back end. Administrators can use it to establish user roles, compliance checks, and remediation requirements. The Clean Access Manager communicates with and manages the Cisco Clean Access Server, which is the enforcement component of the Cisco NAC Appliance.
- **Cisco Clean Access Server.** This security enforcement device is implemented at the network level. It can be implemented in-band or out-of-band, in Layers 2 or 3, as a virtual gateway or as a real IP gateway, and it can be deployed centrally or around the globe. The Cisco Clean Access Server performs device compliance checks as users attempt to access the network.
- **Cisco Clean Access Agent (optional).** This lightweight, read-only agent runs on an endpoint machine. It performs a deep inspection of a local machine's security profile by analyzing registry settings, services,

## At-A-Glance

and files. Through this inspection, it can determine whether a device has a required hotfix; and can then run the correct antivirus software version as well as other security software, such as Cisco Security Agents. For unmanaged assets, the Cisco Clean Access Agent can be downloaded as needed.

Cisco also offers the NAC Framework, which integrates an intelligent network infrastructure with solutions from more than 90 leading antivirus, security, and management software manufacturers. The Cisco NAC Framework provides the same security policy enforcement as the Cisco NAC Appliance. Representing an embedded approach, the Cisco NAC Framework allows security policy enforcement to be natively integrated into an organization's intelligent network infrastructure.

The Cisco NAC Framework may be more appropriate for some customers if one or more of the following conditions apply:

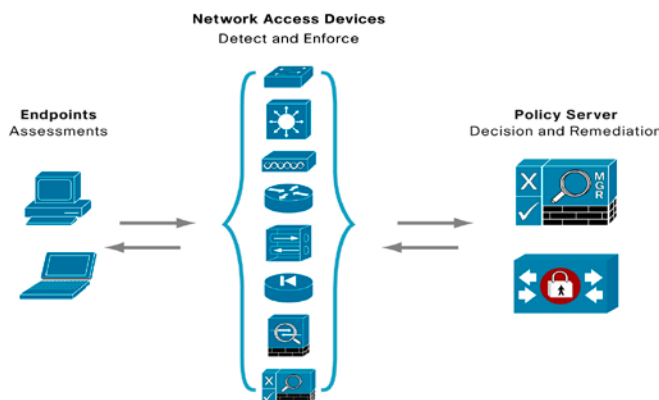
- (1) Deep NAC partner integration is a starting requirement
- (2) Deploying a NAC-compatible 802.1x solution is needed
- (3) Cisco Secure Access Control Server (ACS) is required as the central policy server

To speed your migration to NAC, Cisco Advanced Services can assist in the planning, design, and deployment of your NAC solution to help ensure that it integrates into your existing network infrastructure and that it supports future enhancements to NAC. Services include:

- NAC Readiness Assessment
- NAC Design Development
- NAC Implementation Engineering

**Figure 1. NAC Elements**

Cisco NAC solutions help you add more value to your network by taking advantage of your existing infrastructure without altering its topology.



### What Differentiates Cisco NAC from Other Solutions?

Since Cisco made the first NAC announcement in 2003, other vendors have started to bring similar products to the market. Many of these products are not able to fulfill the four functional areas of network admission control.

Furthermore, Cisco's approach to NAC provides distinct advantages over similar technologies:

- The Cisco NAC Appliance is the most widely deployed, market-tested NAC solution available today. Cisco's deep experience with all network environments results in a deployment timeframe of days rather than months.
- Cisco NAC Appliance and Framework solutions are both available now. No other vendor currently offers both an appliance and a framework solution.
- Only Cisco NAC offers a comprehensive span of control. Cisco NAC supports routers, switches, VPNs, wireless access points, wireless LAN controllers, and wireless client devices. It is also the only solution that supports cutting-edge deployment scenarios, including IP telephony.

- Cisco NAC provides 100-percent host and device compliance for the highest level of admission control effectiveness—without the need to install multiple servers.
- Cisco NAC provides solutions for managed, unmanaged, and guest endpoint devices and is the only solution that allows for the integration of both posture and identity for maximum control.
- With Cisco NAC, decisions regarding a device's policy compliance status are made at the network and not on the endpoint device itself; this limits users' ability to misrepresent their devices as "compliant" to the network.
- As interoperability improves between the Cisco NAC Appliance and the Cisco NAC Framework, the solutions will offer customers investment protection and a smooth integration path.
- Cisco Advanced Services consultants have expertise across all network security technologies and can help customers deploy a NAC solution that integrates with their existing network infrastructure, admission policy, endpoint security, and antivirus technologies.

### Cisco NAC and the Self-Defending Network

Although Cisco NAC can fit into any network environment, it works closely with the following Cisco products to help customers establish their Self-Defending Networks:

- Cisco Security Agent
- Cisco Secure ACS
- Cisco 3000 VPN Concentrator
- Cisco Security MARS
- Cisco adaptive security appliances
- Cisco wireless LAN controllers
- Cisco routers and switches

### For More Information

For more information, please contact your local Cisco sales representative or visit [www.cisco.com/go/nac](http://www.cisco.com/go/nac).