

Network Admission Control: Increase Organizational Security

What You Will Learn

Organizations today face many new security challenges. Cisco Network Admission Control (NAC) solutions can help organizations meet these new challenges. This overview explains how organizations can use Cisco NAC to achieve comprehensive, pervasive, and tightly integrated information security. We demonstrate how Cisco NAC delivers an array of advantages and benefits such as handling guests and unmanaged assets, providing identity-based access control, enforcing security policies, and improving an organization's overall security.

I. The Current Security Landscape

Organizations today face many information security threats and challenges. They include:

- **Financially motivated attacks and exploits.** A clear trend in the latest threat environment is a motivation shift from attention to financial gain. For the first time, financial fraud overtook virus attacks as the source of the greatest financial losses. The average annual loss per company has more than doubled. For details, see http://www.darkreading.com/document.asp?doc_id=133658.
- **New business environments with diminished security boundaries.** Several drivers are changing business environments from closed entities to open ones. Mobile users bring their laptops and handheld devices in and out of the office. Remote-access users connect from homes and public locations. Business outsourcing requires direct partner access into the internal network. Onsite visitors, vendors, and contractors may need physical access to the internal network to accomplish their work. Even "in-the-office" workers are subject to threats coming through Internet access, e-mail use, instant messaging, and peer-to-peer (P2P) activities. Traditional security products designed to protect closed environments with well-defined security parameters are no longer effective in the new business environment.
- **Rapid malware propagation.** Information security threats due to malware propagation remain as a major concern. The time between discovering a vulnerability and the availability of malware to exploit it has decreased from months and weeks to days or even hours. System downtime, recovery, and remediation efforts due to these threats are costly and unpredictable. Organizations are left with little time if they rely on reactive measures only.
- **Corporate governance and compliance.** Information security is not only a technology challenge, but also a corporate governance issue. Organizations must first create their business and security policies, and then take firm steps to implement effective controls based on these policies. Information security must become an integral part of core business decisions and operations. This is a continuous and incremental improvement process. Over time, organizations will be rewarded for mandating such consistent requirements with improved internal processes, reliable controls and greater operational efficiencies.

- **Limited resources.** Many organizations are facing a long list of security initiatives and goals, with only a limited number of qualified IT/security staff and constrained financial resources available. Adding to the challenge are the growing complexity and sophistication of new security threats, diverse user communities, mixed infrastructures, and often, less-than-efficient operations. Given a limited budget and headcount, organizations must aim to streamline work processes, lower operational costs, and reduce security incidents in order to address their high-priority security issues efficiently.

II. A Proven Winning Strategy

A comprehensive security strategy, time-tested and well-accepted in the industry, is to use a combination of people, processes, and best available technologies to address today's security challenges.

The people factor includes senior management support on security initiatives and policies (the "top-down" approach), understanding that security is accepted as everyone's responsibility, and consistent and lasting user awareness campaigns (the "bottom-up" approach). Together, they form a solid foundation for an organization's security program.

Strong IT and security governance, up-to-date security policies and standards, and streamlined and effective processes are the critical ingredients that allow organizations to be prepared and to execute both in their daily operations and during a crisis.

By applying the best-available technologies and products, implementing a well-designed architecture and infrastructure, and deploying a multilayered security defense, organizations can achieve a robust security posture.

To implement this kind of comprehensive strategy successfully, it is critical to have the ability to enforce necessary security policies and standards on all networked devices. For instance, the best host security software will not be useful if it is not installed and enabled on endpoint devices. Rather, an independent enforcement mechanism, applicable to not only corporate-owned devices, but to all devices that seek network access, would effectively ensure that the required host security software is enabled on the necessary devices. Cisco is the first to provide this solution, with NAC. Furthermore, Cisco NAC provides many practical and effective security services to help customers meet their real-world security challenges and improve their overall security.

III. The Cisco NAC Solution

The Cisco NAC solution enables the network to enforce security policy compliance on all users and devices seeking to access the network. Access is permitted only to users with proper credentials and compliant endpoint devices such as PCs, servers, IP phones, and printers. Cisco NAC can also redirect noncompliant devices to a quarantine and remediation area.

Cisco NAC is delivered through an appliance-based approach that can also interoperate with an architectural framework approach. The Cisco NAC Appliance provides rapid deployment, with endpoint compliance assessment, user identity authentication, policy management and enforcement, and remediation services. The Cisco NAC Appliance consists of the following components:

- **Cisco NAC Manager:** The Cisco NAC Manager provides a Web-based interface for creating security policies and managing online users. It can also act as an authentication proxy for authentication servers on the back end. Administrators can use the Cisco NAC Manager to establish user roles, compliance checks, and remediation requirements. It

communicates with and manages the Cisco NAC Server, which is the enforcement component of the Cisco NAC Appliance.

- **Cisco NAC Server:** This security enforcement device is implemented at the network level. It can be implemented in band or out of band, in Layer 2 or Layer 3, as a virtual gateway or as a real IP gateway, and it can be deployed locally or around the world. The Cisco NAC Server performs device compliance checks as users attempt to access the network.
- **Cisco NAC Agent (optional):** This lightweight, read-only agent runs on an endpoint device. It performs deep inspection of a local device's security profile by analyzing registry settings, services, and files. Through this inspection, it can determine whether a device has a required hotfix, runs the correct antivirus software version, and runs other security software, such as Cisco Security Agent. For unmanaged assets, the Cisco NAC Agent is available as a Web-based, dissolvable agent.

In addition to the core NAC functions of authentication, endpoint posture assessment, and roles-based access control, Cisco NAC also introduces a number of advanced NAC services that yield even greater operational benefits and network control. These additional services include:

- **Non-PC Device Profiling (optional).** The Cisco NAC Profiler keeps a real-time, contextual inventory of all devices in a network, including nonauthenticating devices such as IP phones, printers, and scanners. It facilitates the deployment and management of the Cisco NAC Appliance by discovering, tracking, and monitoring the location, types, and behavior of all LAN-attached endpoints. It also uses the information about the device to apply appropriate Cisco NAC policies.
- **Automated, Secure Guest Access (optional).** The Cisco NAC Guest Server vastly simplifies the provisioning, notification, management, and reporting of guest users on wired and wireless networks, offloading from IT staff much of the challenges commonly associated with supporting corporate visitors. The Secure Guest service enhances IT's ability to protect its own organization's assets, employees, and information from guests and their devices while providing secure and flexible network access to meet visitors' business needs

IV. Cisco NAC Benefits

Cisco NAC solutions are comprehensive and easily deployed. They integrate tightly with many additional components of a security strategy, and deliver an array of advantages and benefits not available through perimeter or point products.

Securing Both Managed and Unmanaged Assets

Cisco NAC provides a solid foundation for a secure infrastructure, helping to ensure that configuration standards are applied across all assets, both managed (by the organization) and unmanaged. Effective asset management and controls result in standardization, lower total cost of ownership of the infrastructure, and lower operational expenses.

Providing Guest Access and Preventing Unauthorized Access

Cisco NAC offers a Secure Guest service that allows authorized internal users to sponsor a guest and create the guest account in an efficient and secure manner. The Secure Guest service keeps track of the entire guest visit, including details of the guest network access history. Cisco NAC can assign different types of network access depending on user credentials so that, for example, onsite

visitors and guests may be provided with general Internet access without exposing the internal network to risk.

Cisco NAC can also control connections from a remote site. This is especially useful in dealing with partner connections, in which it is difficult, if not impossible, to determine who is sitting behind a connection at a remote partner site. Having the ability to control access after a user is authenticated provides a highly effective way to maintain security and protect an organization's confidential information.

Reducing Vulnerability-Based Exploits

Cisco NAC reduces and controls large-scale vulnerability-based exploits and attacks by ensuring that all endpoint devices enter the network with the proper protection installed and enabled (such as antivirus software, security fixes and updates, and personal firewalls). This is particularly useful for organizations in which corporate assets are individually controlled by the users to which they are assigned. These assets are easy targets for infections, which may substantially disrupt productivity if permitted to spread.

Host-based security software alone does not solve the "unmanaged asset" problem, due to lack of practical delivery mechanisms. Cisco NAC provides an effective solution by making policy compliance an enforceable requirement for all assets, regardless of whether they are managed by the organization. The end result is lower operational spending for repair and damage control, as well as higher employee productivity.

Ensuring Policy Compliance and Minimizing Inside Threats

Cisco NAC enhances control by providing security policy compliance enforcement at the network level. Policy compliance allows organizations to mitigate security threats caused by disappearing security boundaries, unauthorized access, and internal attacks. By enforcing security policies, Cisco NAC also assists organizations in adhering to privacy and regulatory compliance requirements, including Sarbanes-Oxley and HIPAA.

Cisco NAC enables users and their devices to achieve policy compliance so that they are proactively protected as they work in different environments. Cisco NAC quarantines noncompliant devices so that they are not compromised and used as a hiding place for malicious users to launch further attacks, and then updates the devices to bring them into compliance. The authentication capabilities of Cisco NAC can track and audit user activities. The log information can be used to assist incident response, and for forensics and analysis purposes.

Protecting Existing Security Investments and Providing Quantifiable Return on Investment (ROI)

Cisco is committed to helping customers protect their security investments. Cisco's convergence plan brings together appliance- and framework-based NAC technology, taking full consideration of customers' business priorities, security challenges, infrastructure needs, and operational requirements. In the converged Cisco NAC solution, Cisco NAC Appliance components become the foundation for NAC services while the Cisco infrastructure components provide the pillars for access authentication and network enforcement.

Cisco NAC can deliver a rapid and quantifiable return on investment. Customers can calculate their annual savings based on the threats and risks that an organization intends to address using NAC. For example, an enterprise customer who recently adopted Cisco NAC calculated that they were handling between 3000 and 4000 incidents annually related to PCs with uncontrolled access

to their network. Using their incident-costing model, they estimated that each incident costs between \$750 to \$1,000. Based on their calculations, their Cisco NAC solution will pay for itself in six to nine months, and will provide ongoing multimillion dollar savings annually by dramatically reducing such incidents. For details, see http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci1195099,00.html.

Integration and Collaboration 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 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 while increasing patch management efficiency.

In summary, Cisco NAC provides proactive security protection for an organization's infrastructure and greatly improves network resiliency. It enables pervasive and in-depth security defenses throughout an organization's infrastructure. Cisco NAC delivers many security and business benefits, including identity-based access control, guest access support, security policy enforcement, and security investment protection.



Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks 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. (0711R)