Cisco Network Admission Control: Help Customers Improve Security

What You Will Learn

Many customers are facing increasing information security challenges, including:

- Financially motivated attacks
- An increase in vulnerability-based exploits and malicious activities
- Compliance requirements

Cisco® Network Admission Control (NAC) provides a timely solution tailored to meet these new challenges. This overview explains how organizations can use Cisco NAC to implement identity-based access control at the network level to protect valuable resources and assets; support guests and temporary workers; enforce security policies on all devices (managed and unmanaged); and help improve their overall security.

Introduction

Information security is difficult to define and manage. Technology advancements and new trends in business activities have created a fast-moving, amorphous security environment.

Diminished Security Boundaries and Financially Motivated Attacks

Few organizations today are closed entities with well-defined security perimeters. 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 to the internal network. Onsite visitors, vendors, and contractors may need physical access to the internal network to accomplish their work. Even traditional 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 acting independently, such as intrusion detection system (IDS) and intrusion prevention system (IPS) technology, antivirus measures, and firewalls, are no longer adequate in the new business environment.

In the meantime, malicious attackers have increasingly targeted valuable information assets to obtain financial gain. According to the recent annual Computer Security Institute (CSI) computer crime and security survey, for the first time financial fraud overtook virus attacks as the source of the greatest financial losses (average annual loss per company has more than doubled; for details, see http://www.darkreading.com/document.asp?doc_id=133658).

Rapid Threat Propagation

Information security threats are growing faster than ever. The time between discovery of 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 threats such as viruses and worms are costly and unpredictable. The demand to make business resources and information easily available corresponds to exposure to higher risks.

Corporate Compliance

Defining and enforcing organizationwide security policies is important in minimizing risks and meeting corporate and regulatory compliance requirements. IT staffs face the daunting task of helping ensure that all users and devices meet the defined requirements before accessing their designated resources. In addition, some compliance requirements dictate specific security programs, infrastructure, and control mechanisms. The challenge is compounded by diverse user communities and access methods. Just as many businesses have automated their processes to quickly meet the changing market requirements, so must IT to adopt new security tools that adapt to the changing corporate and regulatory compliance landscape.

Limited Resources

Most organizations create security programs that protect the confidentiality, integrity, and availability of their computing capabilities, online resources, intellectual property, and confidential information (financial, customer, legal, and business strategy). But few consider their other equally valuable assets: brand name, public image, reputation, and public trust. Physical assets must also be protected. For example, highly sensitive information is stored not only on central servers, but also on end-user devices. Organizations expect that information security investments will not only generate immediate benefits, but also continue to work within a long-term security strategy to meet future challenges. At the same time, organizations often have limited financial and human resources available to accomplish these goals. Given limited budgets and headcounts, organizations must aim to streamline work processes, lower operational costs, and reduce security incidents to address their high-priority security concerns efficiently.

Cisco NAC Solution

The Cisco NAC solution provides an effective answer to today's security challenges. Cisco NAC enables the network infrastructure to enforce security policy compliance on all devices seeking to access the network. Access is controlled based on device compliance status, device behavior, and user credentials. Cisco NAC can deny access to unauthorized users and noncompliant devices or redirect them to a quarantine and remediation area.

Cisco NAC fundamentally changes the way that security is implemented because it allows comprehensive security policies to be executed and enforced at the network level, resulting in a proactive approach that was not available before. Cisco NAC accomplishes this by adopting a scalable architecture with a central policy decision component, a distributed security enforcement component at the network level, and integration with additional security products and technologies.

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 Profiler (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.
- 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.

Cisco recommends the Cisco NAC Appliance to most customers as their initial Cisco NAC deployment option.

The Cisco NAC Appliance can also interoperate with Cisco NAC Framework deployments. The Cisco NAC Framework integrates an intelligent network infrastructure with solutions from more than 75 leading antivirus, security, and management software manufacturers. The Cisco NAC Framework provides the same security policy enforcement as the Cisco NAC Appliance. It allows security policy enforcement to be natively integrated into an organization's network infrastructure.

Role of Cisco NAC in Information Security

Cisco NAC delivers a powerful policy enforcement mechanism. For the first time, organizations can reliably implement security policies at the network level to help ensure that every endpoint device is in compliance before gaining network access, enabling organizations to align their security practices and policies based on business requirements and to implement them effectively.

Cisco NAC is comprehensive; it is also easily deployed, integrates tightly with many additional components of a security strategy, and delivers an array of advantages and benefits not available through perimeter or point products.

Rapid Deployment

Cisco NAC can be immediately deployed everywhere in an organization's network, or it can be deployed in focused areas (such as remote access or wireless access networks), first to resolve critical security concerns and later systematically across the network. Deployment of Cisco NAC enforces consistent security policies not just at the perimeter, but wherever network access takes place.

Holistic Integration

Cisco NAC enables tight security integration among multiple security products and technologies. Many host-based security solutions and patch management tools are building blocks of the specific security policies that Cisco NAC enforces. For example, the Cisco NAC Appliance ships with checks for all major antivirus and anti-spyware vendors, plus all current Microsoft updates. These checks can be updated as often as every hour. Today, Cisco NAC supports built-in policies

for more than 350 applications from leading antivirus and other security and management software solution providers. Cisco NAC provides strong integration with Microsoft products and Microsoft Network Access Protection (NAP). Microsoft Single Sign-On (SSO) service for Windows Server Active Directory, Windows Server Update Services (WSUS) automated remediation, and preconfigured critical hotfix checks are some of the major features that Cisco currently provides. Cisco NAC can be customized to add third-party application support. For instance, if laptop encryption is required to provide mobile user protection, Cisco NAC can enforce this requirement by adding custom checks. Such tight security integration achieves far more security benefits than do point solutions acting independently.

Cisco NAC integrates with advanced security technologies to deliver more security capabilities. Cisco NAC embodies the Cisco Self-Defending Network vision of integrated, collaborative, and adaptive security. For instance, Cisco NAC can be integrated with the Cisco Security Agent to enable the Trusted Quality-of-Service (QoS) feature that allows endpoints with different levels of trust to be identified and treated accordingly. Cisco NAC can also be integrated with the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS), which empowers an organization to identify, manage, and counter security threats. For instance, Cisco Security MARS can act as the centralized NAC Layer 2 and 3 reporting engine, and it can provide more advanced security features to integrate with Cisco NAC, such as enabling the 802.1x authentication capability to authenticate the endpoint device (in addition to authenticating the end user). Another example is an integrated Cisco NAC wireless solution. Cisco NAC delivers SSO for wireless access, providing user-transparent security. This integration allows a coherent Cisco NAC environment for both wired and wireless networks.

Overall, Cisco NAC reflects the Cisco Service-Oriented Network Architecture (SONA) concept that security should be built into every piece of an organization's infrastructure and should be delivered as a service along with applications, voice, and mobility.

Cisco NAC Benefits

Cisco NAC improves security in situations in which traditional security products are no longer sufficient. It can prevent unauthorized access, secure corporate and noncorporate assets, reduce vulnerability-based exploits, help ensure policy compliance, and minimize inside threats.

Prevent Unauthorized Access

Cisco NAC can be deployed in an otherwise open environment so that onsite visitors and guests must meet security requirements before they can connect. Cisco NAC can also use its role-based access feature to assign different types of network access depending on user credentials as well as device security postures, so that, for example, onsite visitors and guests can be provided with general Internet access without exposing the internal network to risk. Cisco NAC can also control connections from a remote site. This feature is especially useful in handling partner connections, where it is difficult, if not impossible, to determine who is sitting behind a connection at a remote partner site. Having the capability to control access after a user is authenticated provides a highly effective way to maintain security and protect an organization's confidential information.

Secure Corporate and Noncorporate Assets

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

Reduce Vulnerability-Based Exploits

Cisco NAC reduces and controls large-scale vulnerability-based exploits and attacks by helping ensure that all endpoint devices enter with the proper protection installed and enabled (such as antivirus software, security fixes and updates, and personal firewalls). This feature 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 because of the 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 result is less operational spending for repair and damage control, as well as increased employee productivity.

Help Ensure Policy Compliance and Minimize Inside Threats

Cisco NAC provides 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, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Gramm-Leach-Bliley Act of 1999 (GLBA).

Cisco NAC forces users and their devices to achieve policy compliance so that they are proactively protected as they work in different environments. Cisco NAC removes noncompliant devices from the network so that they are not compromised and used as hiding places for malicious users to launch further attacks. The authentication capabilities of Cisco NAC can track and audit user activities. The log information can be used for incident response, forensics, and analysis purposes.

Cisco NAC Adoption Considerations

The security industry and customers alike have realized the importance of network admission control. Using the experience of thousands of Cisco NAC customers as a basis, Cisco has assembled a list of required functions and implementation considerations.

For more information about Cisco NAC capabilities and to determine your organization’s network admission control requirements, see Table 1 at the end of this section. Use this table to review Cisco NAC functions. Determine how they serve your organization’s business and security needs, and compare Cisco NAC with alternatives you may be considering.

Minimum Functional Requirements

Cisco has identified the following basic requirements for network admission control.

Policy Compliance Evaluation and Verification (of Both Devices and Users)

A network admission control solution must be able to collect relevant security information before the user and the device gain network access. It must then be able to use the collected information to verify that the endpoint is in compliance with security policy requirements. In addition, it must also be able to provide user authentication support.

In comparison, some vendor products are based on network scanning alone. They suffer from two major deficiencies: they cannot provide policy compliance before a device gains network access, resulting in the exposure of an infected device to the network in the time between detection and

action; and they cannot collect and verify user credentials, which makes them incapable of countering unauthorized access.

Policy Enforcement

A network admission control 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. This approach is solid because organizations own and control the network infrastructure, not the end users.

If the point of enforcement is on the endpoint devices themselves, end users can easily defeat the enforcement mechanism. For instance, host-based Dynamic Host Configuration Protocol (DHCP) enforcement cannot prevent a malicious user who has administrator rights on a device from manually changing that device's IP address to gain unlimited network access. A practical example of such a scenario is guest access. Cisco NAC is effective, whereas host-based enforcement would not work because of the unmanaged devices.

Remediation

A network admission control solution must be able to help bring noncompliant devices into compliance, with the remediation method contingent on the user's role. For example, the remediation method of a contractor may substantially differ from that of an employee who has been issued a company-owned laptop. Ideally, remediation should be performed without user intervention; at minimum, users should be given a path to policy compliance. The solution should also allow ongoing compliance assistance in the form of automatic updating of compliant computers so that they adhere to ongoing adjustments and changes in security policy requirements.

Many network admission control products available today do not integrate with security software delivery. Instead, they simply shut off noncompliant endpoints without providing a way to bring them to compliance, resulting in unhappy users and an even greater workload for the IT department.

Flexible Deployment and Policy

Many organizations support a heterogeneous environment of operating systems, such as Windows, UNIX, Linux, and Macintosh. A network admission control solution must support all these OSs, plus devices without conventional operating systems, to provide consistent, effective protection. Similarly, there are different entry points to the network: remote access (VPN), wireless, Layer 2 and LAN (switches), and Layer 3 and WAN (routers). In addition, the network admission control solution must support certain type of nonauthenticating devices (such as IP phones and networked printers).

Few products available today can support all OS types, all access methods, and nonauthenticating devices in a scalable, manageable manner.

Desirable Functional Requirements

Beyond the basic requirements necessary for delivering the promise of network admission control, Cisco has identified several desirable functions that vastly improve the user experience and administrator manageability.

Identification of a Basic Level of Endpoint Security

A typical requirement is to support these components:

- Antivirus solution
- Personal firewall
- OS patches and updates
- Other required configurations, such as certain registry settings

The network admission control solution must verify not only that these components exist, but also that they are an approved version, are configured properly, and are enabled. Cisco NAC can perform this verification and can also help ensure that endpoints are running the correct corporate OS image.

Holistic Integration with Additional Security Technologies.

Cisco NAC has a mutually beneficial relationship with other security technologies, such as the following:

- Vulnerability scanning, to determine whether endpoint devices meet additional security requirements beyond base-level security
- Malware detection, which monitors the behavior of endpoint devices and quarantines them if they are suspected of running malware
- Customizable client scripts, which allows administrators to enforce more policy requirements of their choice beyond the default factory settings
- Integration with advanced security technologies such as Cisco Security Agent (for the Trusted QoS feature), and with analysis tools such as Cisco Security MARS (for event correlation)
- Effective data reporting, to help with planning, execution, and troubleshooting—critically important, especially with large-scale installations
- Security features to prevent bypass attempts, such as MAC address verification and periodic security posture reevaluation to prevent hijacked physical ports

Compatibility and Interoperability

Most organizations use numerous security products from different vendors. A network admission control solution must integrate these and remain interoperable with security products that organizations may consider in the near future. In addition, organizations need a network admission control solution that supports the existing network infrastructure. Cisco NAC addresses these challenges.

Scalability and Related Concerns

A network admission control solution should not require an organization to deploy a new security device on every segment of the network, and it should allow the use of existing infrastructure. The solution also should not create new single points of failure, cause performance degradation, or create high overhead for maintenance. Cisco NAC addresses these challenges, too.

Design and Deployment Considerations

Through its experience with thousands of Cisco NAC customers, Cisco realizes that implementing a network admission control solution represents a fundamental shift in the practice and experience of information security. Therefore, Cisco has identified some important considerations that can help smooth the deployment process.

- **Question 1: Which security risks are you trying to address?** What is the business case for employing network admission control? Identifying security risks that Cisco NAC can address will allow you to establish your delivery target and your project scope. Typical security risks identified by Cisco NAC customers include mobile endpoint devices because their security posture is often out of date. Risks also include wireless connections because of their ubiquitous presence.
- **Question 2: Does your organization already have existing business and security policies that would support Cisco NAC?** Does Cisco NAC fit into your overall security strategy? Any major security initiative needs to have senior management and policy support. Cisco NAC is no exception. Clear security policies need to be in place to establish that users and their devices must reach compliance before they will be allowed network access. In addition, precise security standards need to be published so that users understand the actual technical specifications for compliance. For example, an organization may establish a policy and its associated security standard to tell users in which infrastructure environment (remote access, wireless, etc.) Cisco NAC will be implemented, what operating systems will be affected, and what to do to reach compliance.
- **Question 3: Is your user population ready for the new security environment?** Are users ready to adjust their expectations because they understand the business values and benefits associated with Cisco NAC? Do they understand that they must meet certain security requirements before they can gain network access? Without thorough and persistent communication efforts, some users, especially those accustomed to unconditional network access, may not be ready for the change.
- **Question 4: What kind of Cisco NAC architecture do you need?** This question can be divided into three subquestions.
- **Question 4a. Where will you deploy Cisco NAC (where to start)?** The answer to this question depends on your answer to question 1. For instance, if mobile users are your major concern, you may want to deploy Cisco NAC for the remote-access segment first. If your main concern is the level of security protection at your branch offices because they lack onsite IT and security staff, allow unsupervised onsite visitors, etc., you may consider deploying Cisco NAC in those remote sites first. In most cases, Cisco recommends starting with a few small environments to gain knowledge and experience, followed by a more substantial deployment.
- **Question 4b. Which deployment approach will you use?** The Cisco NAC Appliance is a simple and effective solution for nearly all customers. The Cisco NAC Appliance allows rapid deployment for all environments, including remote-access gateways (VPN environments), wireless access points, remote and branch offices (WAN connections), and full-scale enterprise LANs. You can customize the Cisco NAC Appliance using a combination of Layer 2 and 3 and in-band and out-of-band designs to serve many organizations with different network characteristics and customer preferences. The Cisco NAC Appliance is the most efficient solution for quick deployment and immediate security benefits.

- **Question 4c. What subsequent technical decisions are necessary?** After high-level directions are chosen, you will have a series of detailed technical decisions to make. For example, how will you integrate the Cisco NAC policy decision component with the existing authentication, authorization, and accounting (AAA) infrastructure? How will you handle security software entitlement if you prefer not to give licensed software to visitors or contractors? Strategically, where should you deploy enforcement and management equipment? Where should you store collected data? How do you want to handle monitoring and reporting? You will need to consider your specific environment and requirements to design a plan that fits your business needs.

Table 1. Network Admission Control Solution Checklist

Security Function	Cisco NAC Offering	Competitive Offerings
Is a deployable solution available today?	Yes	To be useful, a security solution must be available and deployable today.
Security posture assessment: Collect and evaluate essential endpoint device security posture information (such as antivirus, personal firewall, and patch level).	Yes	This feature is required to determine a device's security policy compliance status.
Authentication: Collect and authenticate user identity and credentials.	Yes	This feature provides authentication as the user accesses the network. Products that use scanning as their only assessment method would fail here.
Remediation support: Provide a remediation path for client machines to achieve policy compliance.	Yes	Some vendors do not provide this support. They simply cut off noncompliant endpoints.
Quarantine and restricted-access support: Restrict or limit access until compliance is achieved.	Yes	Many scanning-based vendors can only permit (100%) or deny (0%) access; they do not offer a method to provide limited access.
OS support: Support most common endpoint operating systems (Windows, Linux, UNIX, and Mac OS X).	Yes	Many vendors support only a limited number of operating systems.
Network environment support: Implement network admission control for all entry points, including LAN, WAN, wireless, and remote access (VPN).	Yes	Not all vendors support most network environments.
Enforcement flexibility: Use either in-band or out-of-band enforcement.	Yes	Vendors that support in-band enforcement only would fail here.
Enforcement flexibility: Use either Layer 2 (switch level) or Layer 3 (router level) enforcement.	Yes	Many vendors do not have this flexibility.
Proactive protection: Mandate proactive protection before endpoints gain network access (deny a noncompliant device's access to the network until it conforms to the standard).	Yes	Products that use scanning as their only assessment method would fail here.
Reliable enforcement: Perform policy enforcement at the network level (not the host level).	Yes	Enforcement based on host security is easy to bypass; DHCP and other host-based enforcement techniques fail this test. In addition, host-based security alone fails on unmanaged assets.
Nonauthenticating device support: Provide scalable methods to support policies for certain types of devices (IP phones, networked printers, etc.).	Yes	
Advanced assessment: Collect and evaluate advanced endpoint security posture information (such as customized script execution and search results and audit server support).	Yes	This capability allows an organization to enforce endpoint security requirements beyond antivirus, personal firewall, and OS patches. An example of such a requirement is disk and file encryption.
Vulnerability assessment: Provide client vulnerability assessment by performing network-based scans.	Yes	Some scanning-based products excel here, but many vendors' products do not support this function.
Reactive protection: Provide malware detection and enforcement based on endpoint device traffic behavior.	Yes, Cisco NAC integrates with additional Cisco and third-party solutions to provide this function.	Many vendors' products fail here, except for products that actively monitor network traffic.

Security Function	Cisco NAC Offering	Competitive Offerings
Preservation of existing infrastructure: Integrate with products of a broad range of security product vendors.	Yes	
Bypass mitigation: Prevent users from bypassing network admission control.	Yes	
Scalability: Deploy the solution in organizations with large networks.	Yes	
Single sign-on: Provide the end-user benefit of SSO, for example, allowing one login activity to serve both network admission control and Windows Active Directory.	Yes	Many vendors cannot provide this feature

Conclusion

Security challenges have evolved from simple, isolated events to complex, multidimensional, and fast-changing threats. Financially motivated attackers use targeted attacks for personal gain and to cause financial damage to organizations. Expanding business needs and time-to-market pressures are pushing organizations to adjust constantly to better respond to market conditions and customer needs. Regulatory compliance requirements force organizations to implement secure infrastructure and consistent work processes.

Cisco NAC provides an effective solution to address today's business and security challenges. It implements identity-based access control to protect valuable resources and assets, handles guest access, and enforces security policies on all devices, managed and unmanaged, as they enter the network, regardless of access method, ownership, device type, application configuration, and remediation model. It provides proactive protection for the infrastructure and greatly improves network resiliency. Cisco NAC helps customers improve their overall security.

For More Information

Visit Cisco's NAC website at http://www.cisco.com/go/nac.

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, Inc.
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.**

Printed in USA

C22-438082-00 10/07