Cisco Network Admission Control (NAC) Executive Overview

Introduction

As collaboration and globalization change how workplaces function, new information security challenges emerge. Organizations must adopt effective and practical security solutions to meet these challenges and to safeguard their valuable information assets. Cisco® Network Admission Control (NAC) helps organizations to achieve these goals.

This overview explains how organizations can use Cisco NAC to strengthen their security. It discusses how Cisco NAC is integrated into the business lifecycle in terms of supporting role-based access control, enforcing device security compliance, and providing visibility and intelligence for better business decisions. This document also details the return on investment for customers deploying a Cisco NAC solution.

I. The Current Security and Business Environment

The Internet has generated tremendous technology advancements for organizations, resulting in improved business efficiencies and productivity gains. Security threats such as viruses and remote attacks have kept pace with the growing adoption of Internet-related technologies. A recent trend is the shift to financially motivated attacks and exploits: The 2008 CSI Computer Crime and Security Survey shows that the most expensive computer security incidents were those involving financial fraud.

Increased collaboration and globalization introduce further security challenges. Mobile users bring their laptops and handheld devices in and out of the office. Remote-access users connect from their homes and from public locations. Business outsourcing requires direct partner access into the internal network. Onsite visitors, vendors, and contractors may need 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. Web 2.0 applications, social networking technology, and cloud computing all increase the likelihood that sensitive data may no longer reside on a typical company-owned data server only. Traditional security products designed to protect closed environments with well-defined security boundaries are not effective in the new business environment.

Most IT and security departments also face budgetary and personnel resource constraints. 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. Organizations must streamline work processes, improve operational efficiency, and reduce security incidents and financial losses to remain competitive.

II. NAC Lifecycle

To effectively protect the new open and dynamic business environment, organizations need to address several key security questions, including:

- Do you have full control over who is accessing your network and where each user is permitted to go?
- Do you have the ability to implement security policies on endpoints—before they connect?
- Do you have user activity information for analysis, planning, and other purposes?

The Cisco NAC solution addresses these issues by providing complete business activity support. The NAC lifecycle includes:

- Role-based access control
- Endpoint security policy enforcement and remediation support
- Guest access and dynamic user provisioning
- Non-PC device support and data gathering

Role-Based Access Control

Cisco NAC helps reduce the potential loss of sensitive information by enabling organizations to verify a user's privilege level before granting network access. This helps prevent unauthorized access via the wired, wireless, or remote-access network. Cisco NAC provides full integration with wireless, VPN, and 802.1X, and can be implemented in a single-sign-on (SSO) manner to maximize security benefits and minimize user impact.

Endpoint Security Policy Enforcement and Remediation Support

As users carry their laptops to external locations, it is critical that the security protection on each endpoint device is up to date. The security policy is applied when an endpoint device attempts to connect to the internal network. Cisco NAC provides comprehensive policy enforcement and support. Cisco NAC integrates with a wide range of endpoint security applications. It supports built-in policies for more than 350 applications from leading antivirus and other security and management software solution providers. Many user-friendly capabilities, such as silent remediation and auto-remediation, help bring devices into compliance without causing user impact.

Guest Access and Dynamic User Provisioning

Cisco NAC helps organizations improve operational efficiency and productivity by providing secured guest access and assigning internal user access based on a user's role in the organization. Secure guest access allows visitors and guests to stay in touch with their own companies without sacrificing the "host" organization's security. Assigning internal user access based on their role in the organization provides a powerful way to ensure that employees, contractors, and temporary workers can access the required resources to complete their work while maintaining a high level of security standard.

Non-PC Device Support and Data Gathering

In a typical customer network, many non-PC endpoint devices are not associated with user identities. Examples of these devices include IP phones, printers, or scanners. It is usually a labor-intensive process to locate, track, and provide security protection for these devices. Cisco NAC delivers automated non-PC device support by identifying and tracking these devices and placing

them into pre-assigned network segments based on the security policy requirement. This device profiling technology dramatically improves operational efficiency by freeing up IT personnel resources for other tasks. In addition, Cisco NAC gathers rich network user and device activity data for organizations to perform analysis, planning, and other functions.

III. Cisco NAC Product Family

The Cisco NAC solution comprises several core components, with additional optional components for enhanced capabilities.

Cisco NAC Appliance Components

Following are the components of the Cisco NAC Appliance.

- **Cisco NAC Manager**: 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 Cisco NAC Manager to establish user roles, compliance checks, and remediation requirements. Cisco NAC Manager communicates with and manages the Cisco NAC Server, which is the enforcement component of Cisco NAC.
- **Cisco NAC Server:** Cisco NAC Server performs device compliance checks as users attempt to access the network. This security enforcement device is deployed at the network level. 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.
- **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. Cisco NAC Agent is available as both a persistent agent and as a Web-based, dissolvable agent.

Additional NAC Services

Beyond the core Cisco NAC Manager and Server functions of user authentication, device compliance assessment, and role-based access control, several advanced Cisco NAC services are available that yield even greater operational benefits and policy control. These additional services include:

- **Cisco NAC Profiler:** The optional 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. 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 Guest Server**: The optional Cisco NAC Guest Server 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.

- **Cisco Secure Access Control System (ACS) (optional):** Cisco Secure ACS is an 802.1X access policy system that enables Cisco NAC to support 802.1X network authentication. This type of implementation is ideal when applying NAC to large corporate LANs.
- **Cisco 802.1X supplicant (optional):** Although Cisco NAC supports any 802.1X supplicant on the client device side, it is most commonly deployed with Cisco Secure Services Client (802.1X supplicant), or the embedded Windows supplicant.

IV. Cisco NAC Return on Investment

The Cisco NAC solution integrates tightly with many additional security technologies and provides numerous benefits.

Threat Containment

By closely monitoring the security protection on endpoint devices and enforcing security policies, Cisco NAC effectively mitigates virusand malware-based security threats. Benefits to customers include fewer infections, fewer help desk calls, and a more resilient network. For instance, Virginia Commonwealth University has enjoyed a 90-percent reduction in infections on the school's resident student network since implementing a Cisco NAC solution. To learn more, read the case study at http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/case_study_univ_virtually_eliminates_infections_v3.pdf.

Access Control

Cisco NAC assigns different types of network access based on user credentials and a user's role in the organization. Customers benefit from increased security protection, which is reflected in fewer security incidents and a reduction in the loss of sensitive data.

Compliance

Many organizations are under various regulatory or industrial compliance requirements, such as Sarbanes-Oxley (business and financial data), HIPAA (patient health information), and PCI DSS (credit card information). With a Cisco NAC solution, organizations can demonstrate to their stakeholders and auditors that they are putting effective security control and protection in place to address compliance requirements. Direct customer benefits include improved security as well as more reliable audit and enforcement capabilities.

Operational Efficiency

Cisco NAC can help organizations improve their operational efficiencies. By providing secure guest access services, Cisco NAC Guest Server helps to free up IT and help desk resources. Cisco NAC Profiler automates the labor-intensive process of identifying and tracking non-PC devices on the network, therefore saving significant IT resources. Cisco NAC can help improve business results by ensuring that configuration standards are applied across all assets, both managed (internal) and unmanaged (guest). Effective asset management and controls result in standardization, lower total cost of ownership of the infrastructure, and lower operational expenses.

In summary, customers can use Cisco NAC to protect their critical information assets and infrastructure proactively. Cisco NAC delivers many security and business benefits to help customers increase their network resiliency and improve their business results.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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 C22-521628-00 02/09