

---

**Review - Cisco Network Admission Control**  
**Volume I: NAC Framework Architecture and Design**  
**A guide to endpoint compliance enforcement**

Denise Helfrich, Lou Ronnau, Jason Frazier, Paul Forbes

Cisco Press, 2007

ISBN: 1-58705-241-5

List Price: \$55.00

If you don't worry about the integrity and security of your network and networked applications - you should! Malware and other malicious code bring every system you own to its knees - and your business with them.

Threats can arise not only from outside intruders, but also from your own systems that have already been comprised or systems of your customers, vendors or other business partners. What to do? Implement Network Admission Control.

Network Admission Control protects your network by enforcing corporate security software compliance policy for network endpoints. Endpoints can include - servers, network devices and user computers. That means not only can you ensure that malware hasn't invaded your servers and server-based applications, it also means that you can ensure that user computers have up to date security software in place before they enter the network (ensure they won't spread any malware around!).



In this first or two volumes, the authors explain what Network Admission Control is, why you need it, and the explain how to architect a Network Admission Control architecture for your business that will protect it the network and business systems - and your operation. (In the second volume which we'll review next month, they explain how to implement and troubleshoot Network Admission Control.)

This book is designed for businesses already employing Cisco Systems-based networking equipment, but can also serve as a good "baseline" for understand the whys and wherefores of Network Admission Control. A worthy, and much needed reference, for a world filled with malware and other threats posed by sneaky, malicious code - check it out.

**Table of Contents (in brief)**

<b>Chapter 1</b>	<b>Network Admission Control Overview</b>
	What is Network Admission Control?
	Cisco NAC Technology Progression
	Accessing a Network That Does Not Implement NAC
	Accessing a NAC Network
	NAC Benefits

---

- NAC Framework Components
- NAC Framework Requirements
  - NAD Requirements
    - Router Support
    - Switch Support
    - VPN Concentrator Support
    - Wireless Support
  - Cisco Secure ACS Requirements
  - Cisco Trust Agent Requirements
  - Summary of Requirements
- NAC Framework Operational Overview
- NAC Framework Deployment Scenarios
- Summary
- Resources
- Review Questions

## Chapter 2

- Understanding NAC Framework**
- NAC Framework Authorization Process
- Posture Token Types
- Using Information from the Host for the Admission Decision
  - Host Credential Information
    - Arbitrary Information Collection with Cisco Trust Agent Scripting
- Dealing with Hosts That Are Not NAC Capable
  - Static Exemptions for NAH
  - NAC Agentless Auditing
- NAC Modes of Operation
  - NAC-L3-IP and NAC-L2-IP Overview
  - NAC-L2-802.1X Overview
- NAC Communication Protocols
  - EAP Primer
  - Client-Side Front-End Protocols
    - EAP over UDP (EoU)
    - EAP over 802.1X (EAPo802.1X)
  - RADIUS and EAP over RADIUS
  - Server-Side Protocols
    - Host Credential Authorization Protocol (HCAP)
    - Generic Authorization Message Exchange (GAME)
    - Vendor-Specific Out-of-Band Protocols
- NAC L3-IP and NAC-L2-IP Posture Validation and Enforcement Process
  - NAC-L3-IP and NAC-L2-IP Status Query
  - NAC-L3-IP and NAC-L2-IP Revalidation
- NAC-L2-802.1X Identity with Posture Validation and Enforcement Process
- NAC Agentless Host Auditing Process

---

- Authorization and Enforcement Methods
  - ACL Types
    - PACL
    - RACL
    - VACL
  - VLANs and Policy-Based ACLs (PBACLs)
  - Cisco Trust Agent and Posture Plug-in Actions
- NAH and Exception Handling
- Summary
- Resources
- Review Questions

### Chapter 3

- Posture Agents**
  - Posture Agent Overview
  - Cisco Trust Agent Architecture
    - Posture Agent Plug-in Files
    - Cisco Trust Agent Logging
    - Operating System Support
  - Posture Plug-in Functionality
  - Vendor Application Example: Cisco Security Agent
    - Cisco Trust Agent Protection
    - NAC State Awareness
    - Trusted Quality of Service
    - Bundling Cisco Trust Agent for Deployment
- Summary
- Resources
- Review Questions

### Chapter 4

- Posture Validation Servers**
  - Posture Validation Servers
    - Cisco Secure Access Control Server
    - NAC Framework Solution with External Policy Servers
      - Trend Micro OfficeScan
      - McAfee Policy Enforcer
  - Audit Servers
    - The QualysGuard Appliance
    - McAfee Policy Enforcer
    - Altiris
- Posture Policy Planning and Policy Rules
  - Posture Policy Rules
  - Policy Evaluation and Choosing a Posture Token
- NAC Agentless Hosts and Whitelisting
- Authorization

---

Enforcement Actions  
RADIUS Authorization Components  
Posture Plug-in Actions  
Summary  
Review Questions

**Chapter 5**

**NAC Layer 2 Operations**  
IEEE 802.1X Technology Overview  
802.1X Framework  
Supplicant  
Authenticator  
Default Security of 802.1X  
Authentication Server  
IEEE 802.1X Operational Overview  
Multicast MAC Addressing  
EAP Data Frames  
RADIUS  
EAP Negotiation  
End-to-End EAP  
Tunneled Method  
Authorization and Enforcement  
VLAN Assignment  
Integration Issues When Using 802.1X  
Default Operation  
The Guest-VLAN  
IP Telephony  
Management Utilities  
Supplemental Authentication Techniques  
NAC-L2-802.1X Identity with Posture Validation and Enforcement  
Periodic Posture Reassessment  
NAC Supplicants for 802.1X  
EAP-FAST  
Leveraging an Authenticated Identity  
Accounting  
Summary  
Resources  
Review Questions

**Chapter 6**

**NAC Layer 3 Operations**  
EAPoUDP Framework  
Posture Trigger Mechanisms for NAC-L3-IP and NAC-L2-IP  
Session Initiation Process  
Credential Validation

---

- EAPoUDP Operational Overview
  - RADIUS
    - Authorization
  - Cisco Trust Agent
  - Policy Enforcement
    - Status Query Techniques
    - Agentless Hosts
- Voice Integration
  - Impact of Trust Agent Disappearing
  - Voice Integration Summary
- Exceptions to NAC Posture
- Summary
- Resources
- Review Questions

## Chapter 7 Planning and Designing for Network Admission Control Framework

- NAC Framework Lifecycle Process
  - Preparation Phase
    - Define Your Corporate Security Policy
      - Information Security Policy
      - Acceptable Use Policy
      - Network Access Control Policy
      - Security Management Policy
      - Incident-Handling Policy
  - Planning Phase
    - NAC Solution Objectives
    - Documenting Your Existing Infrastructure
      - Surveying Your Network
    - Integration Strategy
    - Operational Strategy
      - Policy Compliance
      - Project Information Sharing
      - Monitoring and Support Strategy
    - Proof of Concept
    - Migration Strategy
    - Cost Considerations
      - Software Costs
      - Hardware Costs
      - Installation/Operation Costs
  - Design Phase
    - Network Admission Policy Definition
      - Policy Definition
      - Credential Definition

---

- Identity Definition
- Network Virtualization and Isolation
- Quarantine and Remediation Services
- NAC Agentless Host (NAH) Definition
- Solution Scalability and High-Availability Considerations
  - Scalability Considerations
  - High-Availability Considerations
- Implementation Phase
  - Staging Implementation
    - Phase 1 Migration Strategy Sample
    - Migration Strategy Summary
  - Communication to Users
- Operation and Optimization Phases
- Summary
- Resources
- Review Questions

**Chapter 8**    **NAC Now and Future Proof for Tomorrow**  
Policing Your Information Highway  
Begin by Laying the Framework

- Asset Protection
- Detecting Misbehavior and Dealing with It

Value Is in the NAC Partners  
Examples of Admission Control Uses

- Tracking and Managing Company Assets
- Enforcing Use of Corporate-Approved Software
- Enforcing Operating System Access Control
- Enforcing Physical Identification for Higher Security Clearance
- Enforcing a Business Policy or Rule
- Enforcing Regulatory Compliance
- Enacting Roles-Based Provisioning
- Enforcing Data Restriction When External Media is Detected
- Using Customized Shared Resources

Summary

**Appendix A**    **Answers to Review Questions**

Index

January, 2007