Introduction

Almost every contemporary corporation and organization has acquired and deployed security solutions or mechanisms to keep its networks and data secure. Hardware and software tools such as firewalls, network-based intrusion prevention systems, antivirus and antispam packages, host-based intrusion prevention solutions, and vulnerability scanners have proven effective to a certain degree, but only if they are kept up to date. For example, classic virus attacks sent via e-mail attachments, such as netsky and MyDoom, can easily be detected and prevented by any up-to-date antivirus and antispam software package. The key to stopping host attacks is being able to proactively enforce security policies that ensure all hosts must be fully patched and have up-to-date security software running before allowing them full network access. Existing security solutions do not proactively stop a PC from entering the network if its security software and operating system software are not current. Frequently, users will manually disable their host security software because it either reduces the overall performance of their PC or prevents an application from installing. When antivirus and antispam packages are out of date or not running, the likelihood of PC virus infections increases. This in turn increases the overall security risk to the organization.

The same principle applies to OS hotfixes. Take Microsoft Windows as an example. If you fail to implement new Windows security hotfixes in a timely manner to address newly discovered vulnerabilities, the probability of those unpatched hosts being compromised, or "owned," greatly increases. This can result in a loss of productivity due to system downtime, theft of company and personal confidential information, or unauthorized access to sensitive information. Unfortunately, loss of a client's confidential information usually leads to financial losses for affected individuals and the organization.

Data security laws and regulations such as the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act, and the Peripheral Component Interconnect (PCI) standard are forcing organizations to implement and enforce tougher data security protection measures. Compliance regulations such as PCI speak directly to the antivirus and OS hotfix issues discussed previously. They make it mandatory that relevant hosts are kept up to date and run antivirus software, among other things. Increasingly, organizations are being forced by various data security laws and regulations to decrease their data security risk. Gone are the days when organizations had the flexibility to decide what their own data security risk tolerance and policy was. Given that many organizations used to choose to save money and time at the expense of data security, mandated security compliance is a welcome change for all.

The motivation for writing this book is to introduce the latest Cisco security technology, called Network Admission Control (NAC) Appliance. This security solution has proven to help minimize the chronic hard and soft dollar losses that corporations are experiencing due to security-related incidents. Additionally, it helps organizations enforce the use of already existing security investments such as antivirus software and patch management solutions. NAC brings to the table an innovative and proactive technique for improving the overall security posture of an organization's hosts and networks.

NAC allows organizations to enforce, for the first time, their previously unenforceable corporate host security policy. It works by authenticating users and posture assessing hosts before allowing them full network access. Hosts that fail the security posture checks (for example, if their OS or antivirus package is not up to date) are network quarantined and given remediation options. After the host is certified, it is

allowed on the network. A user, based on a successful authentication, is granted the level of network access privileges appropriate for that user's role.

The objectives of this book are to provide IT and security teams all the information needed to understand, design, configure, deploy, and troubleshoot the Cisco NAC Appliance solution.

Who Should Read This Book?

This book will be of interest to the following professionals:

- IT directors and managers
- Network administrators
- Network and security engineers
- Security analysts and consultants
- Operating systems administrators
- Application developers

How This Book Is Organized

This book is divided into six parts with 15 chapters and an appendix.

Part I, "The Host Security Landscape," discusses the security landscape and challenges faced by corporations and organizations today. It discusses how Cisco Network Admission Control solutions can help and includes the following chapters:

- **Chapter 1, "The Weakest Link: Internal Network Security,"** provides an explanation of why network attacks and intellectual property losses are originating from the internal network.
- **Chapter 2, "Introducing Cisco Network Admission Control Appliance,"** provides an overview of Cisco NAC offerings and how NAC can help to minimize network outages. NAC's return on investment is covered.

Part II, "The Blueprint: Designing a Cisco NAC Appliance Solution," covers the building blocks and components that make up NAC and how each component works to build a NAC design. Part II includes the following chapters:

- **Chapter 3, "The Building Blocks in a Cisco NAC Appliance Design,"** explains the requirements to deploy NAC and the components involved.
- **Chapter 4, "Making Sense of All the Cisco NAC Appliance Design Options,"** explains the various NAC designs, such as out-of-band versus in-band, and discusses the advantages and disadvantages of each one.
- **Chapter 5, "Advanced Cisco NAC Appliance Design Topics,"** discusses the user authentication methods including MAC address authentication, active directory single sign-on (AD SSO), virtual private network SSO, and wireless SSO. Best practices for VoIP integration and redundancy considerations are covered.

Part III, "The Foundation: Building a Host Security Policy," covers a very important fundamental step of developing a robust security policy. It explains the foundation of building a host security policy and how to assign the appropriate network access privileges for various user roles. Part III includes the following chapter:

- **Chapter 6, "Building a Cisco NAC Appliance Host Security Policy,"** explains what makes up a NAC host security policy; the types of antivirus, antispam, and OS checks required to perform a posture assessment; and the user roles assigned to users. User roles define which access privileges are given to each user.

Part IV, "Cisco NAC Appliance Configuration," provides details of how to set up and configure the NAC appliance solution. Part IV includes the following chapters:

- **Chapter 7, "The Basics: Principal Configuration Tasks for the NAM and NAS,"** provides detailed instructions on how to set up and configure NAC Appliance Manager and NAC Appliance Server for a new deployment.
- **Chapter 8, "The Building Blocks: Roles, Authentication, Traffic Policies, and User Pages,"** explains what and why roles are created and how to manage each role effectively.
- **Chapter 9, "Host Posture Validation and Remediation: Cisco Clean Access Agent and Network Scanner,"** explains the checks and rules that the NAC agent uses for posture validation and remediation. For non-agent devices, Nessus scanning is used to assess the vulnerability of each machine. In addition, reports can be produced.
- **Chapter 10, "Configuring Out-of-Band,"** explains how to configure out-of-band deployment for Layer 2 and Layer 3 networks.
- **Chapter 11, "Configuring Single Sign-On,"** provides step-by-step instructions on how to configure AD SSO, VPN SSO, and wireless SSO.
- **Chapter 12, "Configuring High Availability,"** explains how high availability works and how to deploy it.

Part V, "Cisco NAC Appliance Deployment Best Practices," focuses on the roll-out phases of the NAC appliance solution. Part V includes the following chapter:

- **Chapter 13, "Deploying Cisco NAC Appliance,"** discusses the testing, pilot, and deployment phases of NAC.

Part VI, "Cisco NAC Appliance Monitoring and Troubleshooting," focuses on common monitoring, maintenance, and troubleshooting tasks and procedures. Part VI includes the following chapters:

- **Chapter 14, "Understanding Cisco NAC Appliance Monitoring,"** explains how to read the summary, online users, event logs, SNMP, and other user event pages. Detailed information on NAM and NAS monitoring is also provided.
- **Chapter 15, "Troubleshooting Cisco NAC Appliance,"** provides information on how to troubleshoot common issues related to licensing, agents not connecting, DNS, policy, design (in-band and out-of-band), certificates, high availability, and so on. This is especially useful for support during the first 30 days of NAC appliance deployment.

The **Appendix, "Sample User Community Deployment Messaging Material,"** provides sample NAC appliance deployment templates (e-mails, posters, bulletin board signs, and letters) for customers preparing to deploy NAC. The sample messages are tailored for education institutions but can be modified for any other business.