

# Contents at a Glance

---

<b><i>Introduction</i></b> .....	<b>1</b>
<b><i>Part I: Unlocking the Mysteries of NAC</i></b> .....	<b>7</b>
Chapter 1: Developing a Knack for NAC .....	9
Chapter 2: Knowing Why You Want NAC.....	35
Chapter 3: The NAC Lifecycle.....	51
Chapter 4: NAC Components.....	63
Chapter 5: SSL VPNs .....	77
<b><i>Part II: NAC in Your Network</i></b> .....	<b>101</b>
Chapter 6: Writing a Corporate Security Policy.....	103
Chapter 7: Herding the Cattle.....	119
Chapter 8: Identifying Who's On My Network.....	143
Chapter 9: Verifying that a PC Is Safe.....	155
Chapter 10: Deciding Where to Enforce.....	175
Chapter 11: Flipping the Switch .....	197
<b><i>Part III: NAC in the Real World</i></b> .....	<b>213</b>
Chapter 12: AC Architectures.....	215
Chapter 13: The Role of Standards.....	241
Chapter 14: Extending NAC .....	259
<b><i>Part IV: The Part of Tens</i></b> .....	<b>277</b>
Chapter 15: Ten Best Practices .....	279
Chapter 16: Ten Steps to Planning Your NAC Implementation.....	285
Chapter 17: Ten Online Information Sources .....	291
Chapter 18: Ten Definitions .....	295
<b><i>Index</i></b> .....	<b>301</b>



# Table of Contents



<b><i>Introduction</i></b> .....	<b>1</b>
About This Book .....	2
Something You Should Know About This Book .....	3
What You're Not to Read .....	3
Foolish Assumptions .....	3
How This Book Is Organized .....	4
Part I: Unlocking the Mysteries of NAC .....	4
Part II: NAC in Your Network .....	4
Part III: NAC in the Real World .....	4
Part IV: The Part of Tens .....	4
Icons Used in the Book .....	4
Where to Go from Here .....	5
<b><i>Part I: Unlocking the Mysteries of NAC</i></b> .....	<b>7</b>
<b>Chapter 1: Developing a Knack for NAC</b> .....	<b>9</b>
NAC's Evolving Description .....	10
What NAC is and what it does .....	12
AAA .....	14
Control freak .....	15
Evolving on the job .....	15
The last word .....	17
A Diagram Is Worth a Thousand Descriptions .....	18
Appliance-based NAC solutions: Inline or out-of-band .....	18
Switch- or network equipment-based NAC solutions .....	22
Client- or host-based NAC solutions .....	23
Clientless NAC solutions .....	25
Types of deployment .....	25
Layer 2 or Layer 3 enforcement deployment .....	26
The Best NAC Approach .....	28
Do your NAC homework .....	29
Must-have traits of your NAC solution .....	30
Leveraging What You Have Today .....	33
Standards .....	33
Reuse policies .....	33
Interface with existing systems .....	34
Reporting .....	34



<b>Chapter 2: Knowing Why You Want NAC</b> .....	<b>35</b>
What Are the Reasons for NAC? .....	35
That's Why They're Called Trojan Horses .....	36
Where Have You Been? .....	37
Wireless Networks and NAC .....	38
NAC and Compliance .....	40
The difficult news .....	40
The good news .....	42
Be Our Guest .....	43
Off-shoring and Outsourcing .....	45
Insider Access and Threats .....	47
Keeping Business Running .....	48
Continuity .....	48
Telecommuting and remote access .....	49
Merger or acquisition readiness .....	49
<b>Chapter 3: The NAC Lifecycle</b> .....	<b>51</b>
Policy and the NAC Lifecycle .....	51
Taking Inventory .....	53
User and machine identity .....	54
Clean machines .....	55
How's the weather? .....	55
Putting the Pieces Together .....	56
Not So Fast . . . ..	57
Let Me In! .....	58
We're Watching You .....	59
<b>Chapter 4: NAC Components</b> .....	<b>63</b>
Creating Policy .....	63
Controls .....	64
Continuous monitoring .....	66
Location .....	66
Oh, one more thing . . . ..	67
Dealing with Clients .....	68
Client functions .....	68
Not-so-secret agents .....	69
Left behind .....	72
Enforcement Time .....	72
Endpoint .....	73
802.1X .....	73
Inline .....	75
IPSec .....	76
Remediation .....	76

<b>Chapter 5: SSL VPNs</b> .....	<b>77</b>
In the Beginning, There Were SSL VPNs .....	77
User identity with SSL VPN.....	78
Endpoint security with SSL VPN.....	80
Remote access policy enforcement.....	90
So . . . NAC to Get In.....	95
SSL VPN Use Cases .....	97
Mobile users .....	98
Fixed telecommuters.....	99
Mobile users on a kiosk or home machine.....	99
Business partners or customers on their own machines.....	99

## ***Part II: NAC in Your Network***..... **101**

<b>Chapter 6: Writing a Corporate Security Policy</b> .....	<b>103</b>
What Policies Do You Need? .....	103
Acceptable use policy .....	104
Antivirus policy.....	104
Data backup policy .....	104
E-mail use policy .....	105
Extranet policy .....	105
Mobile device usage policy .....	105
Network access control policy.....	106
Password policy.....	106
Physical security policy .....	107
Remote access policy.....	107
Security configuration change policy.....	107
You Want Me to Do What?.....	108
Being reasonable.....	108
Book 'em, Danno! .....	110
Impressing the big wigs .....	110
Coercing your colleagues .....	111
Training the masses .....	111
A Living Document: The Security Policy Lifecycle.....	114
Up to date .....	115
In sync .....	115
Getting Started: Standards and Web Resources.....	116
Writing Your Own Security Policy.....	116
<b>Chapter 7: Herding the Cattle</b> .....	<b>119</b>
Analyzing the Terrain.....	119
Authentication.....	120
Endpoint checking .....	121
Clients and agents.....	121
Scanning the NAC terrain.....	121

A Team Security Blanket.....	122
It's our policy.....	123
The billing of rights .....	123
The team job description.....	124
Networking Social.....	126
You gotta have heart.....	127
Don't tread on me .....	128
Use your phasers .....	129
A Clean Desk(top).....	130
Not-so-secret agents.....	132
Compliant with Compliance.....	133
Antivirus (and Anti-malware).....	134
Authentication.....	135
Identity .....	135
Access control.....	135
Encryption .....	136
Audits .....	136
Other Players .....	137
1 + 1 = 3?.....	138
Help! (Desk).....	139
User-bility .....	140
Remote users.....	141
Contractors.....	142
The Cattle Corral .....	142
<b>Chapter 8: Identifying Who's On My Network .....</b>	<b>143</b>
Hey, It's Me.....	143
Identity Authentication.....	144
Collecting identity.....	145
Transporting credentials .....	149
Identity validation.....	151
Authorizing the Workforce.....	153
<b>Chapter 9: Verifying that a PC Is Safe .....</b>	<b>155</b>
All PCs Are Not Created Equal.....	156
Which Device Gets the Trust?.....	159
Endpoint security applications.....	159
Operating system and application patches.....	162
Machine identity: Who's on first? .....	163
Get your certificate.....	164
Known vulnerabilities .....	165
Custom policies.....	166
Third-party verification.....	167
Help! My Machine Is Infected! .....	167
Remediate .....	168
Make mine an automatic.....	169
To quarantine or not to quarantine, that is the question.....	169
Get Scanned in Mid-Stream .....	172

**Chapter 10: Deciding Where to Enforce . . . . . 175**

- Operating Modes ..... 175
  - Evaluate only ..... 175
  - Enforcement ..... 176
  - Decision making ..... 179
- Endpoint/Software Enforcement ..... 180
  - Host-based ..... 180
  - Server-based ..... 182
- Inline Appliances ..... 182
  - Firewalls ..... 183
  - NAC appliances ..... 184
- Network Infrastructure ..... 185
  - VLANs ..... 186
  - 802.1X ..... 188
  - MAC authentication ..... 190
  - SNMP and CLI ..... 191
- Other Enforcement ..... 192
  - DHCP ..... 192
  - IPSec ..... 193
  - ARP ..... 194

**Chapter 11: Flipping the Switch . . . . . 197**

- Gearing Up for the Deployment ..... 197
  - The proof is in the pudding ..... 198
  - The pilot implementation ..... 199
  - Sample pilot test plan ..... 201
- Evaluation Before Enforcement ..... 205
- What Are Your Best Practices? ..... 207
  - On location ..... 207
  - Role playing ..... 208
  - Wireless, rather than wired ..... 209
  - Function first ..... 210
- Professional Services and Consulting ..... 210

***Part III: NAC in the Real World . . . . . 213***

**Chapter 12: NAC Architectures . . . . . 215**

- Cisco Network Admission Control (Cisco NAC) ..... 216
  - Cisco Trust Agent (CTA) ..... 217
  - Cisco Access Control Server (Cisco ACS) ..... 217
  - Network Access Device (NAD) ..... 218
  - Third-party servers ..... 218
  - How Cisco NAC works ..... 219

Microsoft Network Access Protection (NAP) .....	220
Microsoft NAP Agent .....	221
System Health Agents (SHAs) & System Health Validators (SHVs) .....	222
Microsoft NAP enforcement components .....	222
Microsoft Network Policy Server (NPS) .....	225
Third-party remediation servers .....	225
Third-party policy servers .....	225
How Microsoft NAP Works .....	226
Trusted Network Connect (TNC) .....	227
What is the TNC architecture? .....	228
Integrity and identity .....	229
Open interfaces .....	232
Working with the TNC Architecture .....	232
Extensibility and architectural options .....	233
Internet Engineering Task Force (IETF) Network Endpoint Assessment (NEA) .....	235
Working Together .....	236
Microsoft NAP–Cisco NAC framework .....	236
Microsoft NAP and TNC .....	238
<b>Chapter 13: The Role of Standards .....</b>	<b>241</b>
Making the Case .....	242
Costs .....	242
Integration .....	242
Organization linking .....	243
Filling the roles .....	243
IETF Standards .....	245
RADIUS: Completing the circle .....	245
The simplicity of SNMP .....	246
The lowdown on DHCP .....	248
I see IPsec .....	250
IEEE Standards .....	251
The 411 on 802.1X .....	251
EAP — we've been framed .....	252
EAP-speak .....	252
Putting it all together in 802.1X .....	254
Open NAC Standards .....	255
Trusting TNC .....	255
In the know on NEA .....	257
<b>Chapter 14: Extending NAC .....</b>	<b>259</b>
Learning from Your Network .....	259
IDP/IPS integration .....	260
Security incident and event management integration .....	261

Network antivirus integration .....	263
Network inventory/device classification integration .....	263
Extending NAC Enforcement .....	265
Firewall enforcement .....	266
IDP/IPS enforcement .....	267
Network antivirus enforcement .....	268
URL/Web-filtering enforcement .....	269
VPN enforcement .....	270
Application enforcement .....	270
Extending NAC on the Endpoint .....	271
Disk encryption integration .....	272
Data leakage prevention integration .....	272
Peripheral protection suite integration .....	273
Virtual sandbox desktop virtualization integration .....	274
Patch management and remediation integration .....	275
Backup software integration .....	275
Custom application integration .....	276

***Part IV: The Part of Tens* ..... 277**

**Chapter 15: Ten Best Practices ..... 279**

Have a Complete Plan for NAC .....	279
Leverage Existing Authentication .....	280
Endpoint Compliance .....	280
Policy Enforcement .....	281
Management .....	281
Logging, Reporting, and Auditing .....	282
Helpdesk Support .....	282
Day-to-Day Operation .....	283
Maintenance and Upgrades .....	283
Future Expansion .....	284

**Chapter 16: Ten Steps to Planning Your NAC Implementation . . . . 285**

Understand NAC .....	285
Create (or Revise) Your Corporate Security Policy .....	286
Build a Cross-Functional Team .....	286
Seek Vendor Info and RFPs .....	287
Test a Proof of Concept .....	287
Implement a Pilot .....	287
Rollout a Limited Production .....	288
Deploy the Full Production and Evaluate Policies .....	288
Deploy Full Production with Policy Enforcement .....	289
Assess and Re-Evaluate at Regular Intervals .....	289

<b>Chapter 17: Ten Online Information Sources</b> .....	<b>291</b>
Network World on NAC.....	291
Trusted Computing Group .....	291
IETF NEA .....	292
Gartner NAC Marketscope.....	292
Forrester NAC Wave.....	293
Cisco NAC .....	293
Juniper Networks UAC.....	293
Microsoft NAP .....	293
Symantec NAC.....	294
Bradford Networks NAC .....	294
<b>Chapter 18: Ten Definitions.</b> .....	<b>295</b>
802.1X.....	295
AAA.....	296
Endpoint Integrity.....	296
Policy Decision Point .....	297
Policy Enforcement Point.....	297
Statement of Health.....	298
Trusted Network Connect .....	298
Juniper Networks Unified Access Control.....	298
Microsoft Network Access Protection .....	299
Cisco's Network Admission Control .....	299
<b><i>Index</i></b> .....	<b>301</b>