Windows Server 2012
Security from End to Edge
and Beyond
Save 30% on Syngress books and eBooks

- Save 30% on all Syngress books and eBooks at the Elsevier Store when you use promo code CW3013.
- Free shipping on all orders. No minimum purchase.
- Offer valid only on Syngress books sold by the Elsevier store until 31 December 2014.

Click here to order a copy of: Windows Server 2012
Security from End to Edge and Beyond

How it works:

1. Choose a Syngress title.
2. Add the title to your shopping cart.
3. Click on “Enter Discount Code” in your shopping cart.
4. Enter code CW3013 to obtain your discount and click apply.
Contents

ACKNOWLEDGMENTS ........................................................................................................... xiii
ABOUT THE AUTHORS ................................................................................................. xv
ABOUT THE TECHNICAL EDITOR ............................................................................... xix
FOREWORD ..................................................................................................................... xxi

CHAPTER 1   Planning Platform Security ................................................................. 1
Reviewing the Core Security Principles ......................................................... 2
Planning a Secure Platform from End to Edge and Beyond ...................... 4
   Understanding Business Requirements .................................................. 5
   Perform Risk Analysis ........................................................................ 6
   Review Policies, Procedures, Standards, and Guidelines .................. 7
   Security Awareness Training .............................................................. 7
   Determine Access Control .................................................................... 8
   Secure Software Development Strategy ........................................... 9
   Network Security ...................................................................................... 9
   Operating System Security ................................................................. 10
From End to Edge and Beyond Chapter Previews ................................... 11
   Chapter 1—Planning Platform Security .......................................... 11
   Chapter 2—Planning Server Role in Windows 8 ............................... 12
   Chapter 3—Deploying Directory Services and Certificate Services .......................... 12
   Chapter 4—Deploying AD FS and AD RMS in Windows Server 2012 ......................... 13
   Chapter 5—Patch Management with Windows Server 2012 ................... 14
   Chapter 6—Virtualization Security ...................................................... 14
   Chapter 7—Controlling Access to Your Environment with Authentication and Authorization .............................. 16
Chapter 8—Endpoint Security ..................................................... 17
Chapter 9—Secure Client Deployment with Trusted Boot and BitLocker ..................................................... 17
Chapter 10—Mitigating Application’s Vulnerabilities ........... 18
Chapter 11—Mitigating Network Vulnerabilities .................... 18
Chapter 12—Unified Remote Access and BranchCache .......... 19
Chapter 13—DirectAccess Deployment Scenarios .................. 19
Chapter 14—Protecting Legacy Remote Clients ....................... 20
Chapter 15—Cloud Security ....................................................... 20
Summary .................................................................................. 20

CHAPTER 2 Planning Server Role in Windows Server 2012 ............ 21
Server Role and Security Considerations ................................. 21
  Using Security Configuration Wizard to Harden the Server .......... 22
  Using Server Manager to Add a New Role or Feature ............... 36
Using Security Compliance Manager to Hardening Servers .......... 43
  Planning Before Hardening Your Server with SCM .................. 46
  Staying Up to Date with SCM .................................................. 47
Administrator’s Punch List ......................................................... 48
Summary .................................................................................. 48

CHAPTER 3 Deploying Directory Services and Certificate Services ......................................................... 49
Evolving Threats Against Certificates ...................................... 50
Implementing Directory Services on Windows Server 2012 ......................... 51
  Installing the Active Directory Domain Services Role .............. 54
  Creating a New Forest with the Windows Server 2012 Server Manager ......................................................... 56
Implementing Certificate Services on Windows Server 2012 ......................... 70
  Planning AD CS Implementation ............................................ 71
  Installing AD CS Role .......................................................... 75
  Installing AD CS Using Server Manager ................................. 77
Site-Aware Certificate Enrollment .......................................... 85
  Configuring CA Site ............................................................ 86
  Renew with the Same Key .................................................... 86
Validate Your Knowledge in AD CS ........................................ 89
Administrator’s Punch List ......................................................... 89
Summary .................................................................................. 89
CHAPTER 4  Deploying AD FS and AD RMS in Windows
Server 2012................................................................. 91
Planning for Active Directory Federation Services.......... 91
Deploying Active Directory Federation Services .......... 96
  Installing AD FS Role Service Using PowerShell .......... 97
  Installing and Deploying AD FS Using Server Manager .. 98
Troubleshooting Active Directory Federation Services .... 107
Active Directory Rights Management Services ............. 110
  General Considerations When Planning to Deploy
  AD RMS ............................................................ 111
  Installing and Deploying Active Directory Rights
  Management Services ........................................... 113
  Validate Your Knowledge in AD RMS .................... 119
Summary .................................................................. 119

CHAPTER 5  Patch Management with Windows Server 2012....... 121
Why Should You Have a Patch Management Strategy
in Place?................................................................ 121
Planning WSUS Deployment on Windows
Server 2012................................................................. 122
  Planning WSUS on Windows Server 2012 ............... 124
Deploying WSUS ....................................................... 129
Managing Updates with WSUS ................................ 135
  Configure Synchronization .................................... 135
  Configure Target Group ........................................ 136
  Review and Approve Updates ................................. 138
Using Group Policy to Configure WSUS ................. 140
  Validating the Configuration .............................. 144
Administrator’s Punch List ....................................... 147
Summary .................................................................. 148

CHAPTER 6  Virtualization Security.................................... 149
Considerations Regarding Virtualization Security
in Microsoft Platform................................................. 150
Understanding and Deploying Windows Server 2012
Hyper-V Security Capabilities .................................. 152
  ARP Poisoning/Spoofing Protection ....................... 152
  DHCP Guard Protection ...................................... 154
  Port ACLs .......................................................... 155
  Network Traffic Monitoring ................................. 158
Isolated Private VLAN (PVLAN) ............................. 163
High Availability for Virtualization Security.............. 164
## Contents

Beyond the Hypervisor ................................................................. 174
Scenario: Virtualization Security Considerations for
a Cloud Infrastructure ................................................................. 175
  Private Cloud Security ............................................................ 177
Administrator's Punch List ............................................................. 185
Summary .................................................................................... 185

### CHAPTER 7
Controlling Access to Your Environment with Authentication and Authorization ........................................ 187
Planning Authentication, Authorization, and Access Control ................................................................. 188
  Data Classification .................................................................. 188
  Data Control .......................................................................... 188
  Auditing ................................................................................. 188
Understanding Dynamic Access Control ................................. 189
  DAC Requirements ................................................................ 189
  Planning for DAC .................................................................. 191
Planning Authentication ............................................................... 191
  KDC Proxy ............................................................................ 191
  Resource-Based Constrained Delegation ................................. 192
  Picture Password .................................................................. 194
  Setting Up Picture Password .................................................. 196
  Logging on with Picture Password ........................................... 197
  Picture Password Management Issues ................................. 199
Configuring Dynamic Access Control ........................................ 200
Summary .................................................................................... 210

### CHAPTER 8
Endpoint Security ........................................................................... 211
Considerations Regarding Endpoint Security ........................................... 212
Planning Endpoint Security ........................................................... 212
Windows 8 Security Enhancements ................................................. 214
  Windows Defender ................................................................. 215
  Windows SmartScreen .............................................................. 229
  Action Center ....................................................................... 234
Encrypting File System ................................................................ 235
Administrator's Punch List ............................................................. 237
Summary .................................................................................... 237

### CHAPTER 9
Secure Client Deployment with Trusted Boot and BitLocker ................................................................. 239
Security Considerations for Mobile Users ........................................ 240
  Data Breaches: A Growing Problem ........................................ 240
  Consequences of a Data Breach ................................................ 242
  Protecting Against Data Breaches ............................................. 243
Understanding the Trusted Boot Process ........................................ 243
How UEFI Enables Secure Boot ...................................................... 244
Windows 8 and UEFI .................................................................. 245
Windows 8 Boot Hardening Features ............................................. 246
Understanding BitLocker Full Volume Encryption .......................... 248
FVE vs. File/Folder Encryption ..................................................... 249
How BitLocker Works Together with Other Technologies to Protect Mobile Users .......................................................... 249
How BitLocker Works ................................................................. 250
Deploying BitLocker .................................................................. 252
Troubleshooting, Recovery, and Repair ......................................... 265
Summary .................................................................................. 265

CHAPTER 10 Mitigating Application’s Vulnerabilities .................. 267
Living in the World of Apps .......................................................... 267
Windows App Store Security ....................................................... 268
Browser Protection .................................................................... 270
A Sandbox Called AppContainer ................................................ 270
SmartScreen .............................................................................. 272
The Old Friends Are Still Here: UAC and AppLocker .................. 276
Hardening Application Environment ............................................ 278
Extra Tools ................................................................................ 285
SDL Threat Modeling Tool ............................................................ 285
Attack Surface Analyzer ............................................................... 287
Enhanced Mitigation Experience Toolkit ...................................... 288
Security Tools Community Edition .............................................. 288
Summary .................................................................................. 288

CHAPTER 11 Mitigating Network Vulnerabilities ....................... 289
Understanding Windows Firewall with Advanced Security .......... 290
Evolution of the Windows Firewall ............................................... 291
Deploying and Managing the Windows Firewall with Advanced Security ............................................................ 294
What Is New in Windows 8 and Windows Server 2012 .................. 294
Configuring the Windows Firewall with Advanced Security ......... 295
Controlling the Windows Firewall Through Group Policy ............. 309
Managing the Windows Firewall with PowerShell and Netsh ......... 318
Troubleshooting the Windows Firewall with Advanced Security .... 320
CHAPTER 13 DirectAccess Deployment Scenarios ......................... 381
  The Simplified DirectAccess Server Test Lab .................. 384
  Create a Security Group for DirectAccess Clients on DC1 .................................................. 387
  Install the Unified Remote Access Server Role on EDGE1 .................................................. 389
  Run the Getting Started Wizard on EDGE1 .................. 391
  Setup and Test Client1 for DirectAccess Connectivity .......... 408
  Overview of Traditional DirectAccess Single Server Deployment .................................................. 419
  Administrator’s Punch List ............................................. 436
  Summary ..................................................................... 437

CHAPTER 14 Protecting Legacy Remote Clients ....................... 439
  Virtual Private Networking with Windows Server 2012 ...... 440
    Brief History of Windows VPN Protocols ..................... 440
    The RRAS Unified Server Role .................................. 444
    Deploying a VPN Server on Windows Server 2012 via the GUI .................................................. 445
    Installing Remote Access Services on Windows Server 2012 via PowerShell .................................. 475
    Deploying Network Access Protection (NAP) Through Network Policy and Access Services ................ 476
      NAP Overview ..................................................... 477
      Deploying NAP on Windows Server 2012 .................. 479
    Summary ................................................................... 489

CHAPTER 15 Cloud Security ..................................................... 491
  General Considerations for Cloud Security (SaaS) .......... 491
  Cloud Security Readiness Tool .................................... 494
  General Considerations for Cloud Security (IaaS) .......... 497
    Network Security .................................................... 497
    Compute Security ................................................. 504
    Guest Compute Security ........................................ 504
    Host Compute Security .......................................... 505
    Building a Private Cloud with Windows Server 2012 ...... 506
  Summary ..................................................................... 510

INDEX ........................................................................... 511
After about 30 books and thousands of articles and millions of words written, you’d think the task of writing would get easier. This book was a yearlong effort shared among Yuri Diogenes, Deb Shinder, and myself. Hundreds of hours of research and testing went into this book. There are a number of people I’d like to thank and acknowledge for their efforts, encouragement, and motivation in making this book come to fruition. First, thanks to Yuri Diogenes for staying upbeat and positive in spite of long hours and multiple responsibilities—without Yuri’s “Outlook,” we would never have been able to complete this book. I want to thank my beautiful wife Deb Shinder for her willingness to step in and take on some of the heavy lifting while we were in midstream—without her exceptional quality input, this book would have been much less than it is today. John Dawson receives my utmost appreciation for motivating us to be all that we can be and encouraging us to reach down for that extra effort needed to bring this effort across the wire. I want to extend a special thanks for Adina Hagege for recruiting me to work for Microsoft. It’s been a wild ride and there’s never a boring day. The opportunities for growth and learning and pushing the boundaries make me look forward to going to work in the morning. Kudos and many thanks go to Richard Hicks for providing an amazingly helpful and actionable technical edit on this book. A big high five for Tim Rains for his gracious contribution to the foreword of this book. Thanks and gratitude go to Bill Gates, Paul Allen, and Steve Ballmer for changing the world for the better—I owe more than I can put into words. Finally, I thank God for all the blessings that He’s given me, including the strength, the intelligence, and the will to complete this and all my other projects.

Tom Shinder

Every book is a new journey, and this one couldn’t be different. I’m fortunate to have the full support of my wife Alexandra Diogenes and my beautiful daughters Yanne and Ysis throughout this journey—I love you. I’m also glad that I could once more have my friend Tom Shinder sharing this project with me; this is our fourth book together, and as always it is an enormous privilege.
to write with such a great person. I also would like to thank Deb Shinder for joining (literally hit the ground running) this project; it was great to partner with you on that. To our technical reviewer for precisely going through each chapter and suggesting improvements, thanks Richard Hicks. To wrap up this team of great minds, I would like to thank our friend Tim Rains for writing the foreword of this book; Tim, I truly appreciate all your support, thanks.

There were many people indirectly involved on this project that I would like to thank for. Some friends keep inspiring me even after leaving the IT field to pursue a new journey. Yes, Jim Harrison, I’m talking about you, buddy. Thanks for sharing your knowledge, your experience, and your friendship. To my close friends that were able to understand the times that I couldn’t meet them for a party because I was busy writing: Alexandre Hollanda, Marcelo Fartura, Wilson Souza, Jose Moreira, and Marcus Paulino. Thanks, guys! Also, to all my coworkers (new and former); they were responsible for helping shape my knowledge: Gershon Levitz, Nathan Bigman, Jess Huber, Steve Dodson, Dan Watson, Mohit Saxena, Daniel Mauser, Eddie Bowers, Andrew Davis, Dan Herzog, Thomas Detzner, Jamir Correa, Vandy Rodrigues, and Phillip Sand.

When you have great leaders at work, new challenges become easy to deal with. I’m fortunate to have great leaders that keep inspiring us to do better; thanks for Adina Hagege and John Dawson for leading us to great places.

Last, but certainly not least, I would like to thank God for guiding me daily and for enabling me to do what I love.

Yuri Diogenes

Writing a book is always a journey that takes you into unexpected places. Coauthoring a book with others makes the process easier in many ways and sometimes more challenging in others. Sometimes you get lucky and get to work with people who smooth the way. It helps when those people are not just random colleagues, but folks you know and like. So I want to extend a big “thank you” to my husband, Tom Shinder, and my good friend, Yuri Diogenes, who were my constant companions on this particular trip from outline to printed text. In addition, I thank those at Syngress for the opportunity to participate in this project, and my colleagues and readers in the IT security community, from whom I’ve learned so much over the years.

Deb Shinder

The authors would also like to thank Adina Hagege, John Dawson, Jose Barreto, Yigal Edery, Travis Plunk, Josh Adams, Frank Simorjay, Jose Maldonado, Cecilia Cole, Tim Springer, Ned Pyle, Joe Davis, Steve Dodson, Jim Harrison, Kim Ditto-Ehlert, Greg Marshall, Starr Anderson, Jim Dial, Jason Jones, Mohit Kumar, Pat Fetty, David Cross, Kathy Watanabe, Bryon Surace, Mike Truitt, John Morello, Ben Bernstein, Joe Davies, Bala Natarajan, Ben Ari, Pat Telford, Tam Viet Pham, Tom Roughley, Jeff Lilleskare, Dana Knipp, Shawn Aebi, and Billy Price.
Dr. Thomas W. Shinder is a 17-year veteran of the IT industry. Prior to entering IT, Tom graduated from the University of Illinois College of Medicine with a Doctor of Medicine degree and was a practicing neurologist with special interests in epilepsy and multiple sclerosis. Tom began his career in IT as a consultant and has worked with many large companies, including Fina Oil, Microsoft, IBM, HP, Dell, and many others. He started his writing career toward the end of the 1990s and has published over 30 books on Windows, Windows Networking, Windows Security and ISA Server/TMG, UAG, and Microsoft DirectAccess. For over a decade, ISA Server and TMG were Tom’s passions, and he ran the popular Web site www.isaserver.org, in addition to writing eight books on ISA/TMG. Tom joined Microsoft in December of 2009 as a member of the UAG DirectAccess team and started the popular “Edge Man” blog that covered UAG DirectAccess. He is currently a Principal Knowledge Engineer in the Server and Cloud Division Information Experience Group Solution’s Team and his primary focus now is private cloud—with special interests in private cloud infrastructure and security.

Yuri Diogenes started working in the IT field as computer operator back in 1993 using MS-DOS 5.5 and Windows 3.1. In 1998, he moved to a Microsoft Partner where he was instructor for computer classes and also wrote internal training materials on topics such as Windows NT 4 and Networking Essentials. His initial experience with security started in 1998 when he had to set up the Internet security connectivity using Microsoft Proxy 2.0 and Cisco routers. In 2001 Yuri released his first book (in Portuguese) about Cisco CCNA Certification. In 2003, Yuri accepted the offer to be a Professor in the University in Brazil where he taught operating system and computer network classes. In December 2003, he moved to United States to work for Microsoft as a contractor in the Customer Service and Support for Latin America messaging division.

Yuri returned to Microsoft as a full-time employee in 2006 to work again on the Customer Service and Support for Latin America, but at this time to be dedicated to the platform division. There he was responsible for primarily supporting Windows Networking and ISA Server (200/2004/2006) for enterprise customers from Latin America. In 2007, he joined the Customer Services and Support Security Team as a Security Support Engineer where he was dedicated to work with Edge protection (ISA Server and then TMG). In 2010 Yuri cowrote the Forefront Administrator’s Companion book and also three other Forefront books in partnership with Thomas W. Shinder. During this time, Yuri also wrote articles for his own blog (blogs.technet.com/yuridiogenes), TechNet Magazine, ISSA Journal, and other Security magazines in Brazil.

Nowadays, Yuri works as a senior technical writer for the Server and Cloud division Information Experience Team where he writes articles about cloud infrastructure with security functionalities baked in. In his current role, he also delivers presentations at public events such as TechED US, Europe, Brazil, and internal Microsoft conferences such as TechReady. Currently, Yuri is also working on his master degree in Cybersecurity Intelligence & Forensics at UTICA while also writing the second edition of his Security+ book (in Portuguese).

Yuri holds several industry certifications, including CISSP, E|CEH, E|CSA, CompTIA, Security+, CompTIA Cloud Essentials Certified, CompTIA Network+, CASP, MCSE, MCTS, MCT, and many other Microsoft certifications. You can follow Yuri on Twitter@yuridiogenes.

**Debra Littlejohn Shinder** is a technology consultant, trainer, and writer who has authored a number of books on computer operating systems, networking, and client and server security over the past 14 years. These include *Scene of the Cybercrime: Computer Forensics Handbook*, published by Syngress, and *Computer Networking Essentials*, published by Cisco Press. She is coauthor, with her husband, Dr. Thomas W. Shinder, of the best-selling *Configuring ISA Server 2000, Configuring ISA Server 2004*, and *ISA Server and Beyond.*

Deb has been a tech editor, developmental editor, and contributor on over 20 additional books on networking and security subjects, as well as study guides for Microsoft’s MCSE exams, CompTIA’s Security+ exam, and TruSecure’s ICSA certification. She formerly edited the Element K *Inside Windows Server Security* journal. She authored a weekly column
for TechRepublic’s Windows blog, called *Microsoft Insights* and a monthly column on Cybercrime, and is a regular contributor to their Security blog, Smart Phones blog, and other TR blogs. She is the lead author on Windowssecurity.com and ISAServer.org, and her articles have appeared in print magazines such as Windows IT Pro (formerly Windows &.NET) Magazine. She has authored training material, corporate whitepapers, marketing material, webinars, and product documentation for Microsoft Corporation, Intel, HP, DigitalThink, GFI Software, Sunbelt Software, CNET, and other technology companies.

Deb specializes in security issues, cybercrime/computer forensics, and Microsoft server products; she has been awarded Microsoft’s Most Valuable Professional (MVP) status in Enterprise Security for 8 years in a row. A former police officer and police academy instructor, she has taught many courses at Eastfield College in Mesquite, Texas, and sits on the board of the Criminal Justice Training Center there. She is a fourth-generation Texan and lives and works in the Dallas–Fort Worth area.
Richard Hicks is a network and information security expert specializing in Microsoft technologies. An MCP, MCSE, MCITP Enterprise Administrator, CISSP, and four-time Microsoft Most Valuable Professional (MVP), he has traveled around the world speaking to network engineers, security administrators, and IT professionals about Microsoft edge security and remote access solutions. A former information security engineer for a Fortune 100 financial services company in the United States, he has nearly two decades of experience working in large-scale corporate computing environments. He has designed and deployed perimeter defense and secure remote access solutions for some of the largest companies in the world. Richard has served as a technical reviewer on several Windows networking and security books, and is a contributing author for http://WindowsSecurity.com and http://ISAserver.org. He’s an avid fan of Major League Baseball and, in particular, the Los Angeles Angels (of Anaheim!), and also enjoys craft beer and single-malt Scotch whisky. Born and raised in Southern California, he still resides there with Anne, the love of his life and wife of 27 years, along with their four children. You can keep up with Richard by visiting http://www.richardhicks.com/.
The threat landscape has evolved dramatically over the past 10 years in ways that have been challenging for organizations to understand, manage, and predict. In the wake of the successful mass worm attacks of 2003 (SQL Slammer and Blaster), organizations and information technology (IT) professionals began adapting to the rapidly changing threat level of the Internet. Host-based firewalls, security update deployment tools, and antivirus solutions became the primary ways in which organizations managed threats. IT professionals expanded their skill sets by learning about a whole new category of features, functionality, tools, and products that would help them manage the security of the infrastructure they were entrusted with.

For many, the new security requirements were painfully hard to understand, implement, and maintain. IT professionals were required to understand vulnerability details included in security bulletins, use this information to make thoughtful deployment decisions, and deploy security updates in large environments using rudimentary tools, all without disrupting the business they supported.

During this time, I was the technical lead on Microsoft’s customer facing security incident response team. My team helped many customers get through these dark days. In times like those, an IT professional’s best friend was well-written technical documentation and guidance that was accurate, authoritative, and from a trusted source. Understanding precisely how to configure, deploy, and manage security-related technologies and updates, and what to do if things didn’t operate as expected, was invaluable.

Fast forward now 10 years to 2013. Things have changed dramatically. The threat landscape can no longer be characterized as a place where relatively simple worms with benign payloads run wild. Organized crime is now borrowing advanced vulnerabilities and threats reportedly developed by government espionage and cyber-warfare programs to attack organizations and governments. IT professionals, now with the aid of Chief Information Security Officers (CISOs) and professional risk managers, are defending critical infrastructures against
targeted attacks perpetrated by determined adversaries who will use every dirty trick they can devise to compromise IT environments and steal information. Hacktivists focused on drawing attention to their political causes are also targeting organizations that IT professionals are expected to protect. The types of threats that IT professionals are now faced with are far more insidious than in the past, making the IT professional’s job more challenging and important than ever before.

One thing that has not changed over the past 10 years is the need for well-written technical documentation and guidance that is authoritative, accurate, and from a trusted source. This is where Tom Shinder, Yuri Diogenes, and Debra Littlejohn Shinder have made some significant contributions over the years, and now in their latest book, *Windows Server 2012 Security from End to Edge and Beyond*. Within Microsoft, I have watched Tom and Yuri roll up their sleeves on a number of occasions over the past several years to become respected figures within the technical security community at Microsoft. I have seen Debra, a Microsoft Security MVP, work tirelessly to help IT professionals understand security-related technologies. Together they have produced a comprehensive book to provide IT professionals with the information they need to know about modern-day, cutting-edge security technologies. They didn’t take the easy route and write about technologies that are relatively easy to understand and administer. They tackled some of the most complex security technologies that IT professionals typically look for help with, including Certificate Services, ADFS and ADRMS, and DirectAccess, to name a few. This book will help you understand the newest security technologies that are built into the latest operating systems from Microsoft that will be in IT environments for the next 5–10 years.

Tim Rains
Director, Trustworthy Computing
Microsoft Corporation
CHAPTER 1

Planning Platform Security

**CONTENTS**

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Planning Platform Security</td>
</tr>
<tr>
<td>2</td>
<td>Planning Server Role in Windows 8</td>
</tr>
<tr>
<td>3</td>
<td>Deploying Directory Services and Certificate Services</td>
</tr>
<tr>
<td>4</td>
<td>Deploying AD FS and AD RMS in Windows Server 2012</td>
</tr>
<tr>
<td>5</td>
<td>Patch Management with Windows Server 2012</td>
</tr>
<tr>
<td>6</td>
<td>Virtualization Security</td>
</tr>
<tr>
<td>7</td>
<td>Controlling Access to Your Environment with Authentication and Authorization</td>
</tr>
<tr>
<td>8</td>
<td>Endpoint Security</td>
</tr>
<tr>
<td>9</td>
<td>Secure Client Deployment with Trusted Boot and BitLocker</td>
</tr>
<tr>
<td>10</td>
<td>Mitigating Application’s Vulnerabilities</td>
</tr>
<tr>
<td>11</td>
<td>Mitigating Network Vulnerabilities</td>
</tr>
<tr>
<td>12</td>
<td>Unified Remote Access and BranchCache</td>
</tr>
<tr>
<td>13</td>
<td>DirectAccess Deployment Scenarios</td>
</tr>
<tr>
<td>14</td>
<td>Protecting Legacy Remote Clients</td>
</tr>
<tr>
<td>15</td>
<td>Cloud Security</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
</tr>
</tbody>
</table>

**CHAPTER POINTS**

- Reviewing the core Security Principles
- Planning a Secure Platform from End to Edge and Beyond
- From End to Edge and Beyond Chapter Previews
REVIEWING THE CORE SECURITY PRINCIPLES

Information security has evolved throughout the years, there is no more room for “band aid” solutions, and security must be integrated with all layers in order to better protect your data. The attacks that happened in the past years proved that investing only in technology in order to secure the data without educating the end user imposes a high security risk to the company. The most recommended formula is to keep the balance and make sure to mitigate all potential vulnerabilities, be vigilant to rapidly identify flaws, and have an incident response in place to reactive in a structured manner. But what this has to do with Windows Server 2012? Well, everything! The operating system is the main door to good and bad users to have access to your data. You might protect all other windows in your house, have a alarm system that alert you if something happens, have secure cameras all around the house, but if you fail to protect the main door, the whole investments in other security measures will not matter.

Windows 8 brings a new user experience with a radical change in the UI (User Interface) and also on the way that applications are presented to the end user. With the advent of social networks, it is clear that Windows 8 make it easier for the end user to get connected with others, share information, and socialize. While this is a natural trend for nowadays needs, the security concerns around this new era of information sharing are higher than in the past. We do not want to reinvent the wheel and we believe that the core security principles must remain intact, which means that we will focus on addressing the traditional security triad: Confidentiality, Integrity, and Availability.

In a nutshell, we believe that if you address this core security principle you will be answering the major concerns around data protection. As the operating system is the main door to access your data, we shall use the same approach to protect the operating system and how the users will use it to access the data (Figure 1.1).

Now you add to this landscape the fact that the data are not on your data center anymore, that is the way cloud computing starts introducing new challenges to data protection. The threat landscape that throughout the years companies were trying to tackle now is about to change with the adoption of cloud computing. Windows 8 is an operating system that was build with cloud computing in mind. There are many areas of improvement in this version that are related with how well Windows can be used to not only provide a great user experience while using cloud resources but also be the main platform to deploy a cloud infrastructure.

The core security principles must be applied to the whole infrastructure and that is why we have been using the phrase (which is the name of our Security Talk Show\textsuperscript{1}): \textit{From End} (security from endpoint) \textit{to Edge} (regardless
Reviewing the Core Security Principles

of your infrastructure edge protection is still important) and Beyond (beyond on-premises we mean, cloud resources). This also reinforce the use of the defense in depth approach in this new era of cloud computing. Figure 1.2 summarizes how we should use this approach while planning the overall security strategy.

FIGURE 1.1 Evaluating user’s needs while leveraging core security principles to address security concerns.

FIGURE 1.2 Defense in depth approach while moving to the cloud.

1You can access the episodes of our Security Talk Show at http://blogs.technet.com/b/security_talk.
As we previously mentioned, the first step toward a better secure environment is to ensure your end users are well trained. They need to understand the risks and implications of their actions not only when they are using a corporate asset to access a resource but also when he is exposing company information in a social network. It is key to have a good security policy in place, but having a security policy without enforcing it does not really work. It is necessary to leverage technology to enforce security policy; Windows 8 provides a great flexibility and granularity on this respect. It is quite possible that your company will have some service running on the cloud while keeping others on-premises. Data will move from on-premises to the cloud and vice versa, and this imposes some risks. You cannot relax the on-premises security, because if you do, this will be your weakest point in the chain; keeping security consistent across the board is the key.

From the cloud perspective, the reality shows that many businesses will only migrate to the cloud if the cloud provider meets the compliance and regulatory requirements for the company. It is very important to be including this in the overall security plan because even knowing that is not you that will manage the compliance and regulatory needs; you are still accountable to ensure that your data are protected according to the required standards. You also need to understand the cloud provider security program. Is important to understand what this provider is doing to keep your data secure, What is security certificates do they have? Who is handling the data? We will go further on this conversation in Chapter 15, Cloud Security.

NOTE

Windows Server 2012 allows you to build your own cloud infrastructure, and this is a built-in feature in this release. Throughout the Beta timeframe, we wrote a set of documents that explains in more details how to build this cloud infrastructure.²

PLANNING A SECURE PLATFORM FROM END TO EDGE AND BEYOND

In order to take full advantage of the security feature set that Windows Server 2012 has built in, you should plan your security strategy in a way that security is baked in all process and procedures that exist in your company. The foundation platform that we propose is presented in Figure 1.3.

Before we present the foundation in which you could build your security strategy upon, it is important to emphasize that it is out of the scope of this book to provide further details on how to plan all elements of Phase 1 and Phase 2. Our core goal here is to expose those phases and as we explain and demonstrate the Windows Server 2012 security feature set, we will refer to this diagram for a better understanding of the overall security strategy. It is also important to clarify that these are core elements that should be present on the overall security strategy, which framework you will be use to implement that is also out of the scope of this book.

**Understanding Business Requirements**

The main goal in creating a security strategy is to address the overall business requirements regarding information security. Different company sizes will require different approaches as they will have different budget available to deal with information security. What it is really important here is that you can bring to the table a solid value proposition that will address the company’s needs while stay on budget. The table below has a decision matrix sample:

As previously mentioned, this is only an example of how you can leverage the Windows 8 built in technology to address security business needs (Table 1.1).
### Table 1.1

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Business Requirements</th>
<th>Proposed Solution</th>
</tr>
</thead>
</table>
| Small-medium business company with an overall limited budget without legacy applications | ■ Data must be highly available for end users with a low maintenance cost  
■ No budget for physical security  
■ Limited budget to maintain its own IT infrastructure | Migrate to a public cloud infrastructure. This will address all core business needs. We will discuss more about Public Cloud in Chapter 15 |
| Large enterprise that needs better control of the data, capability of rapid expansion and resource automation | ■ Internal IT must be in control of the data  
■ Departments should be logically isolated from each other  
■ Reduce the amount of physical servers that are in use today | Migrate to a Windows Server 2012 Private cloud. This will meet all business requirements. We will discuss more about Private Cloud in Chapter 15 |
| Large enterprise that needs to allow remote users to securely access internal resources in a transparent manner | ■ Remote users should be able to access applications that are in the local network  
■ The solution must be transparent to the user, in order words; they should have the same experience as they have when accessing the data internally | Migrate to Windows 8 DirectAccess Solution. This will allow users to securely access internal resources without manual intervention. We will discuss more about DirectAccess in Chapter 13 |
| Large enterprise that has roaming users using laptops on the field and connecting to untrusted networks | ■ Roaming users should be inspected for malware in all phases of a computer startup  
■ Remediation actions should be done in order to fix potential issues | Migrate to Windows Server 2012 and use Platform Integrity in order to take advantage of the Trusted Boot feature. We will discuss more about Platform Integrity in Chapter 9 |

### Perform Risk Analysis

How can you justify the security safeguards if you do not know the real risk? Well, that is what the risk analysis is for. It will be the tool that you will use to define and justify to upper management why those countermeasures should be in place. It always boils down to answering two questions:

- How much it cost if you have a breach and your data are compromised?
- How much it cost to mitigate this issue?
This is a huge subject and a deeper analysis of all variants is a book by itself. Just keep in mind that whatever you are going to propose as solution, you should have a concrete business case that was built upon a solid risk analysis.

**Review Policies, Procedures, Standards, and Guidelines**

No, they are not the same thing and that is why you really should understand the boundaries of each one in order to correctly plan and implement it. A company must have a security policy in place to determine the function that security will have in the organization. Different departments within the company will have different procedures in order to accomplish a specific goal. IT might have a procedure that explains how to restore a server in case of a completed failure, while HR will have a hiring process procedure that detailed explain how to hire a new employee. In both situations, there are security concerns that must be addressed. A company also needs a standard to ensure that specific needs are met before anything else. For example, a company might have a standard to always acquire hardware with at least 8 GB or RAM (for desktops), that is the standard desktop memory. Guidelines are general recommendations that the company will have for all users.

When planning your Windows Server 2012 deployment strategy, you should be aware of the overall PPSG (Policies, Procedures, Standards, and Guidelines). You should leverage technology as much as you can to assist policy enforcement. The table 1.2 exemplifies this approach:

<table>
<thead>
<tr>
<th>Company Policy</th>
<th>How to Enforce this Policy</th>
<th>Reference Chapters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users must change passwords every three months</td>
<td>■ Use Windows Group Policy to implement that</td>
<td>7</td>
</tr>
<tr>
<td>It is important to have a cleanup process during the provision/deprovision operation in order to avoid data leakage</td>
<td>■ Use Windows Server 2012 automation for Cloud Technologies</td>
<td>15</td>
</tr>
<tr>
<td>All computers must be running the latest updates no later than five days after the update was released</td>
<td>■ Use Windows Update Services (WSUS) role in Windows Server 2012</td>
<td>5</td>
</tr>
<tr>
<td>Certificates issued by the company’s CA must alert the administrator that the expiration date is approaching</td>
<td>■ Use Certificate Lifecycle in Windows Server 2012</td>
<td>3</td>
</tr>
</tbody>
</table>

**Security Awareness Training**

Users must be aware of the new techniques that hackers are using to attack users by enticing them to open a malicious email or even leveraging social
engineering on-premises to give them an infected USB drive. The famous RSA Attack in 2011\(^3\) was done using a phishing e-mail that looked so legitimate that the user moved from the Junk Mail folder to the Inbox and opened the infected file. Is very important that users are well trained and upon finishing the training they should acknowledge that this training was successfully finished.

**NOTE**


When deploying a new operating system to the users, they must be trained on how to use it and this basic training should teach security best practices so that they can securely use the features available for them. One important point about Security Awareness Training is that it can be the old passive way to teach, you cannot just send out an email with tips on how to get protected. Users should be able to learn how to differentiate from a phishing e-mail to a legitimate e-mail; they should be able to interactively practice what they learned. Most of the security awareness training focuses only on teaching terminologies instead of making the users experience a real social engineering attack. What will happen if someone walks in to the receptionist, dressing like a mail man and deliver a piece of hardware where the destination is the CEO of the company saying it is a gift from Company C but it is actually full of malware? Will this receptionist validate the package? While this might sound like tales from movies,\(^4\) it is not, social engineering is something that will bypass most of the technologies in place because it deals with the psychological side of the human, the most vulnerable element in the enterprise chain.

**Determine Access Control**

The core premises here are least privilege and need to know. Each user or group should have access to only the set of documents that they need to and always assume that he doesn’t needs access to it until his manager proves otherwise. It is important to use this step within Phase 2 to also determine the level of authentication and authorization that must be provided to the user. This could (and mostly will) vary between data access and application access. Not all users within the same group will need to access the same set of application.


\(^4\)Read this post and you see some social engineering techniques recently used to spy individuals at [http://arstechnica.com/tech-policy/2013/01/the-bizarre-tale-of-john-mcafee-spymaster/](http://arstechnica.com/tech-policy/2013/01/the-bizarre-tale-of-john-mcafee-spymaster/).
This is also true when you are planning your cloud infrastructure; the same person that will demand a new virtual machine might not be the same that has authorization to release it. This means that role-based access control plays a very important role in such scenario. The table 1.3 has some other sample scenarios and how you can leverage Windows Server 2012 to address those needs:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Solution</th>
<th>Chapters that Cover this Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users must be authenticated on-premises in order to have access to public cloud resources</td>
<td>Use ADFS on Windows Server 2012</td>
<td>4</td>
</tr>
<tr>
<td>Users must be part of the Cloud Operators group in order to provision a new resource</td>
<td>Use Windows Server 2012 Cloud Infrastructure</td>
<td>15</td>
</tr>
</tbody>
</table>

### Secure Software Development Strategy

Most companies have their own development team to develop their custom applications that will be used internally. If security is not part of the software development strategy for those applications, chances are that all investment that was done in infrastructure and personnel training will be compromised by a security breach in the application. It is very important that security is part of the development plan. The development team must be aware of how to design their solution without compromise data’s confidentiality, integrity, and availability. Microsoft has its own software development strategy called SDL (Security Development Lifecycle). We encourage you to learn more about at [www.microsoft.com/sdl](http://www.microsoft.com/sdl).

### Network Security

The path from end to edge and beyond always will use some sort of connection: wired or wireless. Such connection will always use a communication protocol. This means that from the security standpoint it is very important to understand your network profile. What are the protocols that are in transit in your network? Do you have a network baseline? Do you know what protocols and ports the applications that you use will leverage? Please do not tell me: everything is encrypted, so I do not care about ports. While encryption is important to avoid data leakage in transit, you should still have a clear understanding of what it is in transit within your network.

---

It becomes vital to have this network profile done prior to deploy Windows Server 2012, mainly because of the built in firewall that Windows has. If you do not know what ports the applications will use, how can you configure a standard host firewall profile for your corporate computers? You might argue that you can do it via executable file; however if this executable file is a piece of malware that replaced the original program, then you are not in a good position. At that point, the malicious program might send request in ports that are not supposed to be authorized to use, but since it was released from the program context, it will have complete access. Sure we can mitigate that; we can use software restriction policy and only run programs that are authorized. What this really means is that you need to address the different variants of your choice (using protocol/port or using executable file name). We will discuss network vulnerabilities in more details in Chapter 11.

**Operating System Security**

Without a doubt, this is the main area that we will cover on this book, the Windows 8 operating system security functionality. It was very important to go over all the aspects that are part of this security foundation. You do not want to start building your house in a broken foundation, do you? Same thing applies to an operating system deployment. You do not want to deploy without planning and you do not want to plan without considering security aspects of the overall solution. Once you realize that all those pieces are part of the same puzzle is because your security maturity level has achieved the level that we want.

As explained before, Windows Server 2012 brings a new set of features that allows the operating system to be prepared for nowadays security challenges. In order to leverage the security capabilities offered by this release, you must understand that security will be used as a wrapper as shown in Figure 1.4.

![Figure 1.4 Using security around the entire solution.](image-url)
Each chapter will tackle the operating system in a different security perspective with the ultimate goal of allowing you to securely deploy and maintain a Windows Server 2012 infrastructure on-premises or in the cloud.

**FROM END TO EDGE AND BEYOND CHAPTER PREVIEWS**

This book takes a deep dive approach into a collection of Windows 8 platform technologies that are related to security. We focus on platform security technologies for a reason: the cloud. As cloud computing becomes ever more important in the data center, the need to bring security closer to the service and the data hosted by the service increases. This is why Microsoft is no longer investing in standalone security products. Instead of investing in standalone security products, Microsoft is working toward bringing the security protection and controls into the core Windows platform.

This book is comprised of the following chapters:

- Chapter 1—Planning Platform Security
- Chapter 2—Planning Server Role in Windows Server 2012
- Chapter 3—Deploying Directory Services and Certificate Services
- Chapter 4—Deploying AD FS and AD RMS in Windows Server 2012
- Chapter 5—Patch Management with Windows Server 2012
- Chapter 6—Virtualization Security
- Chapter 7—Controlling Access to your Environment with Authentication and Authorization
- Chapter 8—Endpoint Security
- Chapter 9—Secure Client Deployment with Trusted Boot and BitLocker
- Chapter 10—Mitigating Application’s Vulnerabilities
- Chapter 11—Mitigating Network Vulnerabilities
- Chapter 12—Unified Remote Access and BranchCache
- Chapter 13—DirectAccess Deployment Scenarios
- Chapter 14—Protecting Legacy Remote Clients
- Chapter 15—Cloud Security

**Chapter 1—Planning Platform Security**

Planning considerations must always take place before you being to consider the security technologies that you want to employ. What are your security requirements? What constraints do you have? What security controls do you need to apply and how do you need to apply them? How will you manage your security controls? How will you monitor them? What capabilities do you require are part of your security architecture and design? You need to be able to answer these questions before you begin your quest for finding technologies that meet your requirements. You will find that many of your security requirements will be met
by the platform technologies you will learn about in this book. However, there will be other requirements that are not met by Windows 8 and you will need to look for other options. This book will provide you with an in-depth look at those technologies so that you can make an informed decision.

Chapter 2—Planning Server Role in Windows 8
Similar to Windows Server 2008 R2, Windows Server 2012 enables you to install only the server roles that you require. In order to decide which role is appropriate for the server, you need to have an understanding of the roles and features available to you. Each of the roles and features included with Windows Server 2012 are installed with default best practices security settings. However, there may be times when you want to adjust those settings. We will talk about those adjustments and how to make them in subsequent chapters. You can see a page from the Windows Server 2012 Add Roles and Features Wizard in Figure 1.5.

Chapter 3—Deploying Directory Services and Certificate Services
Windows Server 2012 is designed to be a comprehensive cloud operating system. One of the core requirements of any cloud-based system is identity management. The cloud introduces a number of challenges when it comes to identity, and Windows Server 2012 aims to help solve some of those challenges. Windows

![Figure 1.5 New Add Roles and Features Wizard in Windows Server 2012.](image-url)
Server 2012 includes significant enhancements in a number of the Active Directory-related services and roles. The next version of Active Directory Federation Services will make it easier than ever to federate your corporate identities with partners and cloud-based identity providers. Active Directory Certificate services have also been greatly improved so that it is easier than ever to deploy and manage certificates in your private and public cloud. In this chapter, we will talk about how to deploy the Active Directory roles and features and describe how they solve problems in identity management in your next-generation data center.

Figure 1.6 shows an example from the improved Active Directory Administration Center.

Chapter 4—Deploying AD FS and AD RMS in Windows Server 2012

In the future, your private cloud datacenter will likely be connected to public cloud resources and those public cloud resources may need to be able to consume identities managed in your private cloud. How do you connect your
identity management system so that private and public clouds can be accessed seamlessly by your users? You can do this by taking advantage of federation services. Windows Server 2012 includes a new version of the Active Directory Federation Services (ADFS) that makes it possible for you to easily federate your corporate identities with cloud server providers and with partners.

As cloud pushes security closer to the services and the data managed by the services, it is that access controls need to also be pushed back as far as possible. The ideal security scenario is when you can protect your information, even after the network, operating system, and application has been compromised. This is where Active Directory Right Management Services comes in. With Active Directory RMS, you can apply flexible access controls over documents so that only authenticated and authorized personnel can access that information. You can also apply other policies to protected documents, such as the ability to copy or paste, or alter the document, or create an “auto destruct” time for the document.

This chapter will discuss where ADFS and ADRMS fit into your overall security architecture, how to deploy and manage these services, and how to get the most out of these critical cloud enabling security technologies.

Chapter 5—Patch Management with Windows Server 2012

Patch management is an unfortunate fact of life. No matter how well-architected and designed software might be, that software is created by humans and humans are not, and will never be, perfect. However, Microsoft continues to improve security in its platform and works on the principle of continuous improvement. One of the major improvements in the area of patch management is the new version of Windows Server Update Services (WSUS) included in Windows 8. You will see improved reporting and control of updates applied to both servers and clients in your organization. Figure 1.7 shows an example of one of the screens in the new WSUS feature. In this chapter, we will talk about what is new in WSUS, how to deploy the Windows Server 2012 WSUS, and how to get the most out of your advanced WSUS deployment (Figure 1.8).

Chapter 6—Virtualization Security

While not an essential characteristic of cloud computing, virtualization is a critical component of any cloud deployment. Virtualization enables many of the essential characteristics of cloud computing. However, as data centers continue to migrate from physical to virtual, new security challenges introduced by virtualization need to be addressed. Some of these can be solved by properly managing your virtual infrastructure, but many of them require technical solutions to enable the key security principle of isolation. Windows Server 2012 includes literally dozens of new
**FIGURE 1.7** New look and feel for AD RMS.

**FIGURE 1.8** WSUS now fully integrated with Windows Server 2012.
technologies aimed at securing the compute, network, and storage components of a private cloud infrastructure. In this chapter, we will introduce you to these new technologies and explain how to deploy them so that you can reach levels of security in a virtualized environment that you never thought possible.

**Chapter 7—Controlling Access to your Environment with Authentication and Authorization**

Authentication and Authorization are two core elements of any security policy. While the old approach of creating groups and adding users to the groups is something that can still be used to better manage authorization of resources, there are much more variables that should be consider before authorize an user to have access to a resource. In Windows Server 2012, a new feature called Dynamic Access Control (DAC) was introduced to better reflect the diversity of scenarios that companies are facing nowadays. Active Directory Group Policy has been with us since Windows 2000 Server, and with each version of Windows, it just keeps getting better and better. The pace of improvement does not slow with Windows Server 2012. While the interface for configuring Group Policy has not changed a ton, there are a few very handy new features that help you make the most out of GPOs (Figure 1.9).

![Group Policy Management Editor](image)

**FIGURE 1.9** New policies were added in Windows Server 2012.
Chapter 8—Endpoint Security
As discussed earlier, this book is about security from end, to edge and beyond! The end is the endpoint—the client or server that connects to your valuable resources and interacts with other network devices. As cloud computing makes borders ever more porous, the issue of endpoint security becomes job number one for security administrators. In this chapter, we will present key questions that you will need to ask yourself about how to best secure your endpoints and help you map out these requirements to platform technologies included in Windows 8 (Figure 1.10).

Chapter 9—Secure Client Deployment with Trusted Boot and BitLocker
Mobile client systems are now the norm. This is great for employee productivity but puts your information at serious risk because of the high rate of lost or stolen mobile devices. You need to be able to prevent data leakage from these compromised devices. Windows Server 2012 includes a new feature called “Trusted Boot.” The Windows Server 2012 boot process is signed and measured, helping to protect the PC from malware or viruses. Trusted Boot validates the integrity of the entire boot process, including the hardware, boot loader, kernel, boot-related system files, and drivers. Antimalware is loaded in advance of all non-critical Windows components. This means that malware, such as rootkits, is less able to hijack the boot process or hide from antimalware software.

FIGURE 1.10 Windows Defender now plays a bigger role in the overall platform security.
BitLocker encrypts volumes using strong AES encryption. It also prevents intruders from using off-line attacks to get access to the data on the encrypted hard disk—thus keeping the data on the stolen device safe from theft. Windows Server 2012 includes a number of BitLocker improvements, such as support for encrypted hard drives (where encryption is performed on the entire disk, not just disk volumes) and network unlock. In this chapter, we will discuss how to plan and deploy these key Windows Server 2012 security features.

Chapter 10—Mitigating Application’s Vulnerabilities
It does not matter how careful and assiduous you are, there are going to be flaws and weaknesses to all applications. However, this does not mean you have to put up with it and do clean up after the inevitable attacks! In this chapter, we will talk about the threat landscape that evolves as clients are getting more connected via apps and downloading them direct from Windows Store. What are the implications of this new window of opportunities and how a company can mitigate potential vulnerabilities on this space. This chapter will also cover some aspects related to security enhancements on Internet Explorer 10 and review some tools that can assist users to operate in a more safer way, some old technologies that were introduced in Windows Vista, such as User Account Control and other out of band tools such as Enhance Mitigation Experience.

Chapter 11—Mitigating Network Vulnerabilities
Whether you deploy a private cloud or run a traditional data center, you will need to have controls in place thatmitigate network vulnerabilities. With the increasing openness seen in corporate network infrastructures due to the proliferation of mobile devices, the ability to protect data on the wire is just as important as protecting data during processing and at rest. Windows 8 includes a number of new enhancements that help you in your mission of protecting in-flight information. One of these new improvements is SMB 3 encryption. With little or no overhead, SMB connections to file shares can be encrypted without any special efforts required by the clients connecting to the file servers. Windows Firewall with Advanced Security is improved and can be centrally managed using Group Policy to protect the endpoints from network-based exploits. Microsoft Security Essentials also helps against network attacks by incorporate IDS/IPS components. In addition, you can use IPsec not only to encrypt data on the wire but also to make sure that only trusted computers can communicate with each other (Figure 1.11).

If you are running a private cloud, or just a virtualized data center, then Windows 8 will definitely help you secure the network components of your virtual infrastructure. New features included in the Hyper-V virtual switch include port ACLs, bandwidth control, DHCP protection, router advertisement protection, and more work together to protect your virtual infrastructure from network attacks. In this chapter, we will discuss how to make best use of these technologies and how to deploy them to enhance your network level security.
Chapter 12—Unified Remote Access and BranchCache

One of the essential characteristics of cloud computing is broad network access. People need to be able to get the information they need from anywhere, and from any device. While this is often connected with the public cloud, the fact is that your users will need to access information in your private cloud, and they have the same expectations that they will be able to get to that information regardless of their current location, and regardless of type of device they are using. You will need to think about how you can provide secure remote access to your users. You will need to consider authentication and authorization, you will need to think about device state assessment, you will need to consider performance and reliability of connections, and what remote access methods work with what devices. In this chapter, we will go into the planning considerations you will need to make that will enable you to choose the right combination of Windows 8 technologies to enable the essential cloud characteristic of broad network access.

Chapter 13—DirectAccess Deployment Scenarios

Once you have put together your remote access plan and considered your options, you are ready to deploy that plan. In this chapter, we will take a look at the new and improved routing and remote access feature that integrates...
remote access deployment and configuration for remote access VPN client connections, site to site VPN connections, and DirectAccess connectivity. Windows Server 2012 introduces a number of improvements in DirectAccess, including support for NAT64/DNS64, the ability to put a DirectAccess server behind a NAT device, higher performance for IP-HTTPS connections and more. We will cover the deployment considerations and how to manage Windows Server 2012 DirectAccess technologies.

Chapter 14—Protecting Legacy Remote Clients
While DirectAccess is the ideal secure remote access solution for Windows 7 and Windows 8 clients, you will still need to be able to provide access to resources on your corporate network. Windows 8 includes integrated VPN services that enable legacy clients secure remote access to your network. We will discuss how to design a VPN solution using the Network Policy and Access Services role and how to perform endpoint health detection using remote access control options.

Chapter 15—Cloud Security
Windows Server 2012 is designed to be the consummate private cloud operating system. Literally hundreds of new features and capabilities have been introduced in the new operating system to make the best choice for creating the infrastructure foundation for your private cloud. However, with the advantages that you can accrue by deploying a private cloud, there are new and different security challenges that are introduced by private cloud. In this chapter, we will discuss these challenges and how you can build a framework for protecting and militating against them.

SUMMARY
In this chapter, we discussed key issues in information security and the importance of architecting and planning a secure network, server, and application infrastructure. Only after the due diligence planning is completed, you can be ready to move on to the next step, which is to investigate the products and technologies that will fulfill your security requirements. Windows Server 2012 is built from the ground up with a large collection of platform technologies that will help enable you meet many of your security requirements. We then completed the discussion with a chapter over that will help you understand what to expect as you move forward in this book.

In the next chapter, we will take a look at the Server Roles and Features available in Windows Server 2012 and focus on those that have direct and indirect impact on security issues in the Windows Server 2012 platform.
Index

Note: Page numbers followed by f indicate figures and t indicate tables.

A
Access control determination
auditing, 188–189
authentication and authorization
level, 8
cloud infrastructure, 9
data classification, 188
data control, 188
description, 188
Access Control List (ACL)
Get-VMNetworkAdapterAcl
cmdlet, 157
IPv4 port, 155
IPv6 port, 155
MAC port, 155
ACL. See Access Control List (ACL)
Action Center, Windows 8
architecture, 234
Change Action Center Settings,
234, 235f
third-party security-related
programs, 234
Windows Security Center
Service, 234
Active Directory Based Activation
(AD BA), 53–54
Active Directory Certificate Service
(AD CS)
arguments, 76, 76f
CA, 72–73
CEP and CES, 74–75
certificate authority web
enrollment, 78, 79f
confirmation, 80, 81f
confirm installation selections, 78
credentials page, 78
cryptography, 79, 80f
dashboard, roles and features, 77
destination server, 77, 78
trace
enterprise CA, 79
Get-WindowsFeature command,
75, 76, 76f
individual services installation, 76
installation progress, 78
installation, Server Manager, 77
NDES, 74
OCSP, 73–74
PowerShell/Server Manager, 75
private key, 79
progress and results, 80, 81f
role-based/feature-based
installation, 77
roles and features, 80, 82f
root CA, 79
Server Manager, 78, 78f
server roles, 77
Service Account, CES, 83, 83f
services, 82, 82f
SSL encryption, 83, 84f
validation, knowledge, 89
web enrollment, 73
Web Server Role (IIS), 78
Windows integrated
authentication, 83
Windows Server 2012, 71
Active Directory Domain Services
(AD DS)
add roles and features, 58, 58f
add servers, 56, 56f, 57
configuration, deployment, 63, 64f
confirmation, 61, 62f
credentials, built-in administrator
account, 63–64
Dcpromo.exe, 55
deployment, 55
DNS Server, 64, 65, 66f
domain controller
configuration, 55
DS Restore Mode Password
option, 65
failure, promotion and
administrative information,
68, 70f
features and services, 58, 60f
forest and domain functional
levels, 64, 65f
IncludeManagementTools, 58, 60f
installation, 68, 69f
Install-WindowsFeature, 57, 57f
management workstation, 55
NetBIOS, 65, 66f, 67
Paths page, 67, 67f
Prerequisites Check, 68, 69f
Remote Desktop Services
scenario-based installation,
58, 59f
requirements and practices, 61, 62f
results, 61, 63f
Review Options, 67–68, 68f
select features, 61, 61f
Server Manager and Windows
PowerShell, 54, 55f
Server Selection, 58, 59f
server to domain controller link, 63
WsmProvHost.exe, 61
Active Directory Federation Services
(AD FS)
analytic and debug logs, 108
certificate planning, 94–95
descriptions, 101
confirm installation selections, 99
Debug node and Enable Log, 109
deployment, 103–104
description, 13–14
ETW, 107
features, 97
goals, 91–92
Active Directory Federation Services (AD FS) (Continued)
hybrid cloud resources, 96, 96f
installation, 97
installing and deploying, 98–107
LDAP attribute column, 106
partner’s application, 92
planning phase, 92–93
planning role services, 94
PowerShell, 97
review core infrastructure, 93–94
role services, 99
SCW, 95–96
stand-alone/farm deployment, 101
URL, 104
Web server Role, 99
WIF, 97
Windows Server 2012 Beta, 52
XML, 104

Active Directory Rights Management Services (AD RMS)
cluster key storage, 114
confirm installation selections, 114
Cryptographic Mode 2, 114
delegation support, 111
deployment, 111–112
features, 110
infrastructure integration enhancement, 111
Licensor Certificate, 116
Microsoft Test Lab Guide, 119
perform additional configuration, 114
Protect Document, 117
Server Manager and PowerShell, 111
support, crypto, 111
Windows 8, 113
Windows Azure RMS, 111

AD BA. See Active Directory Based Activation (AD BA)

AD CS. See Active Directory Certificate Service (AD CS)
Address Space Layout Randomization (ASLR), 270

AD DS. See Active Directory Domain Services (AD DS)

AD FS. See Active directory federation services (AD FS)

AD RMS. See Active Directory Rights Management Services (AD RMS)

Advanced Encryption Standard (AES)
BitLocker, 250
SMB encryption, 332

AES. See Advanced Encryption Standard (AES)

AIK. See Attestation Identity Key (AIK)

AppLocker
Modern Apps, 281
reference computer, 284

ASLR. See Address Space Layout Randomization (ASLR)

Attestation Identity Key (AIK), 247

B

BitLocker
Active Directory, 252
AES, 250
boot device order, 252
deployment, enterprise, 261–262
encryption, 251
fixed data drives, 261
group policy settings, 259
mobile/desktop system, 249
operating system drive, 255–256
operating system installation, 262–264
OS, 251–252
removable data drives, 261
setup wizard, 253–255
tool, repair-bde, 265
trust measurement, 252
VM, 253
Windows Vista, 248

BranchCache deployment
access controls, 363
BitLocker, 364
caching modes, 363
configuration, clients, 377–379
content information, 363
content-related activity, 363
certification server configuration, 365–375
distributed mode, 362
firewall settings, 378
hosted cache server configuration, 375–376
hosted mode, 362–363
metadata, 363
preloading, hosted cache servers, 376–377
requirements, 364
security, 363
server types, 363
WAN bandwidth optimization technology, 362

Browser protection
AppContainer sandbox, 270–272
SmartScreen, 272–276

C

CA. See Certificate Authority (CA)
CEP. See Certificate Enrollment Policy Web Server (CEP)
Certificate Authority (CA), 72–73, 73f
Certificate Enrollment Policy Web Server (CEP), 74–75, 75f
Certificate Enrollment Policy Web Services (CES), 74–75, 75f
Certificate renewal, keys
add/remove Snap-ins, 86
authority, 87, 87f
Duplicate Template, 86f, 87
MMC, 86
recipient, 87, 87f
request handling, 87, 88f
templates, 86–87
Windows Server 2012, 86

Certificate services (CS) deployment
AD CS. See (Active Directory Certificate Service (AD CS))
description, 12–13, 13f
features, deployment, 70, 71f
CES. See Certificate Enrollment Policy Web Services (CES)
CLIENT1, DirectAccess connectivity alternate port number, 410–411, 412f
client connectivity, 409
Collect Logs, 413, 413f
ConnectedLocally, 411, 412f
ConnectedRemotely, 412, 412f
Connection Details section, 415–417, 418f
Connection Security Rules, 415, 417f
Files shared folder, 414, 415f
Generate Report link, 417
Get-DnsClientNdptPolicy and hit ENTER, 410–411, 411f
Get-NetIPAddress, 414, 416f
Get-NetIPITPSConfiguration and hit ENTER, 415, 416f
Group Policy settings, 408–409
to Internet subnet, 412
to launch IE, 413, 414f
ping app1.corp.endtoedge.com and hit ENTER, 413, 414f
Protocol, Port, and IP Address, 417–418
Server Load Statistics, 419, 420f
Workplace Connection, 413, 413f
Cloud infrastructure
Cluster/CSV traffic, 182
Compute Security, 179–180
deprovisioning, 184
Hyper-V, 175
Live Migration traffic, 182
management traffic, 183
Networking Security, 180–183
Private Cloud Principles, 176
Private Cloud Security, 177–184
storage traffic, 183
traditional data center, 178
virtualized infrastructure, 176
Windows Server 2012, 178
workload administrator, 176
Cloud security
description, 20
design, infrastructure, 506–507
IaaS. See (Infrastructure as a Service (IaaS))
installation process, 507
OEM vendors, 507
presentations, 507
SaaS. See (Software as a Service (SaaS))
Compute security, IaaS
description, 504
guest, 504–505
host, 505–506
Connection Manager Administration
Kit (CMAK), 472, 474f
Connection security rules, WFAS
authentication method, 326, 328f
command-line netsh, 329
properties sheet, 327, 329f
remote computers, 329
types, connection security rules, 325, 326f
Content server configuration
file servers. See (File servers)
Web and BITS application servers, 365–366
Control Panel Interface
Add an app window, 296
configuration, apps and features, 296, 296f
network types, 296
system and security, 295–296
Windows Firewall management
console, 297
Cross-Site-Request-Forgery (CSRF), 272
CSRF. See Cross-Site-Request-Forgery (CSRF)
DAC. See Dynamic access control (DAC)
Data breaches, security
approaches, protection, 243
c confidential/sensitive company
data, 240
first-party cyber insurance, 242
methods, 240
Data Recovery Agent (DRA), 236
DCs. See Domain controller (DCs)
Digital Subscriber Line (DSL)
analog technology, 343
direct point-to-point connection, 343
internet access, 343
line conditioner, 343
DirectAccess deployment
access security solutions, 381
administrator’s punch list, 436–437
c omputer certificate authentication, 350
double encryption, 354
Getting Started Wizard, EDGE1, 391–408
intranet resources, 358
IP-HTTPS, 357
IPsec tunnels, 351
IPv6 to IPv4 protocol, 351–353
Kerberos Proxy service, 351
multiple domains, 354–355
multiple sites, 358
NAP Integration, 355
network location server, 350
OTP, 355
PKI, 382
planning requirements, 361–362
public IP addresses, 353, 382
real high availability, 354
Remote Domain Offline Join, 359–360
RRAS, 349–350
security group, 387–389
setup and test, CLIENT1, 408–419
simplified DirectAccess management, 350
simplified DirectAccess wizard, 382
split/force tunneling, 356–357
Support for Server Core, 359
Test Lab. See (Test Lab Guides, simplified DirectAccess server)
UAG DirectAccess, 382
Unified Remote Access Server role, EDGE1, 389–391
Web site certificate, 350
and Windows, 360–361
Windows DirectAccess, 358
Windows Server 2008 R2, 381
DirectAccess server (EDGE1)
going started wizard
add roles and features page, 392, 392f
configuration process, 401
configure accounting, 405, 405f, 406f, 407f
configure remote access getting
started wizard, 395, 395f
configure remote access page, 392–393, 393f
DAClients, 395, 396f
Dashboard entry, 403, 404f
DirectAccess Connection, 396, 397f
operations status, 401, 403
Remote Access Review, 395
396f, 397f–398, 398f
Remote Access server, 393–394, 394f
Remote Client Status node, 408, 410f
Reporting node, 408, 409f
tasks section, 405, 405f
wizard settings page, 398, 399f, 400f
unified Remote Access
Confirmation screen, 390, 392f
installation, 390–391
Role Services page, 390, 391f
in Select Server Roles dialog box, 389, 391f
in Server Manager, 389, 390f
steps, 389
Directory services deployment
AD BA. See (Active Directory Based Activation (AD BA))
AD DS. See (Active Directory Domain Services (AD DS))
AD FS integration, Windows
Server 2012 Beta, 52
description, 12–13, 13f
dynamic access control, 53
FAST, 54
Directory services deployment
(Continued)
fine-grained password policy user interface, 53
identity management system, 51
KCD, 54
off-premises domain, 52
recycle bin user interface, 53
Server Manager, AD DS integration, 52
virtualized DCs. See (Domain controller (DCs))
Windows and non-Windows networks, 51
Windows PowerShell history viewer, 53
Domain controller (DCs) cloning, 51
support and safe, 52
DRA. See Data Recovery Agent (DRA)
DSL. See Digital Subscriber Line (DSL)
Dynamic Access Control (DAC) components, 189
domain controller configuration, 201
domain perspective, 190
features, 189
File Server configuration, 207
File Server perspective, 190
Kerberos protocol and claims, 189
locations, 200
planning, 191
requirements, 189–190
validation, 208
in Windows Server 2012, 191

E
EAP. See Extended Authentication Protocol (EAP)
Early Launch Antimalware (ELAM), 246
ECC. See Elliptic curve cryptography (ECC)
EFI. See Extensible Firmware Interface (EFI)
EKU. See Enhanced key usage (EKU)
ELAM. See Early Launch Antimalware (ELAM)
Elliptic curve cryptography (ECC), 235
Encapsulating Security Payload (ESP), 324
Endpoint security
compny’s goals, 213–214
compny’s priorities, 212–213
consumerization, IT, 214
d-end-point client machines, 237
policy enforcement, 214
security chain, 212
Windows 8 enhancements, 214–237
Enhanced key usage (EKU), 246
Enhanced Protected Mode (EPM)
Internet Explorer functions, 270
remote access connections, 272
EPM. See Enhanced Protected Mode (EPM)
ESP. See Encapsulating Security Payload (ESP)
ETW. See Event Tracing for Windows (ETW)
Event Tracing for Windows (ETW), 107
Evolving threats vs certificates
Certificate Infrastructure model, 50
core components, 51
defense, depth approach, 50–51
HTTPS, Web transactions, 50
Extended Authentication Protocol (EAP), 345
Extensible Firmware Interface (EFI), 244

F
FAST. See Flexible Authentication Secure Tunneling (FAST)
FDE. See Full Disk Encryption (FDE)
File servers
Active Directory Users and Computers, 369, 370f
BC file servers, 369, 371f
BranchCache Hash Publication, 372, 373f
BranchCache, Network Files, 368, 369f
Enable Hash Publication, 368–375
File and iSCSI Services, 367, 368f
Group Policy Management Editor console, 372, 374f
new file servers, 367
Organizational Unit, 369, 371f
Fine-Grained Password Policy User Interface, 53
Flexible Authentication Secure Tunneling (FAST), 54
Force tunneling
automated support, 349
DirectAccess clients, 356
IPsec rules, 356
FQBN. See Fully Qualified Binary Name (FQBN)
FQPN. See Fully Qualified Path Name (FQPN)
Full Disk Encryption (FDE), 248
Full volume encryption (FVE)
BitLocker. See (BitLocker)
vs. file/folder encryption, 249
parallel installation attack, 249
Fully Qualified Binary Name (FQBN), 280
Fully Qualified Path Name (FQPN), 280
FVE. See Full volume encryption (FVE)

G
Getting started wizard and remote access, VPN
configuration settings, 455
configuring IP address assignment, 456, 458f
default settings, 455, 456f
Finish button, 456
IP address/public name, 455, 455f
modifying Remote Access settings, 456, 457f
RADIUS authentication, 456, 458f
Tasks Details box, 453, 454f
Globally unique identifiers (GUIDs), 295
GPMC. See Group Policy Management Console (GPMC)
GPO. See Group Policy Object (GPO)
Group policy
Add/Remove Snap-ins, 313
firewall rules/settings, 313–314
network isolation controls, Windows Store Apps
address space, intranet network, 314
configuration, proxy addresses, 314
Create Custom Firewall Rules, 315–316
WFAS settings, 309–311
Windows Firewall behavior, 316–318
Group Policy Management Console (GPMC), 316
Group Policy Object (GPO)
Configure Windows Smart Screen, 233, 233f
firewall rules/settings, 313
policy enforcement., 237
Guest compute security
integration services, 505
RBAC, 505
virtual machines, 505
GUIDs. See Globally unique identifiers (GUIDs)

H
Health Registration Authority (HRA)
administrative tool, 478–479, 479f
authentication requirements, 486–487
certification authority (CA), 487
description, 478–479
issuance of health certificates, 479
request policy, 487
Host compute security, 505–506
HRA. See Health Registration Authority (HRA)
Hyper-V architectural model
Extensible Switch, 152
features, 151
security enhancements, 151
Hypervisor
Core Operating System, 175
networking, 174–175
storage, 175

I
IaaS. See Infrastructure as a Service (IaaS)
ICMP. See Internet Control Message Protocol (ICMP)
Infrastructure as a Service (IaaS)
cloud service models, 497
compute security. See (Compute Security, IaaS)
enterprise infrastructure, 497
network security, 497–504
service solutions, 497
Integration, Identity and Access (IIA), 492
Internet Control Message Protocol (ICMP), 316
Internet Information Services (IIS)
  Web Server, VPN
  confirm installation selection, 450, 452f
  information, 450, 451f
  roles and server groups section, 453, 453f
  selection, 450, 452f
Internet Key Exchange version 2 (IKEv2)
IPsec Tunnel Mode, 443
policies, 444
Ports node, 466, 467f
Internet Protocol Security (IPsec)
  connection security rules, 324
  and ESP, 324
  and SSL, 324
  and TLS, 324
Interprocess communication (IPC), 268–269
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 351
IPC. See Interprocess communication (IPC)
IPsec. See Internet Protocol Security (IPsec)
IPV6 to IPv4 protocol, DirectAccess
DirectAccess server setup
Wizard, 352
name resolution mapping service, DNS64, 352
translator, “NAT64”", 352
ISATAP. See Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
Isolated Private VLAN (PVLAN) classification, 163
Hyper-V Switch, 163
and ports, 163, 163f
Layer 2 Tunneling Protocol (L2TP)
connection security, 470
and IPsec combination, 441–442
ports, 466, 467f
in RRAS, 468–469
Layer 2 Tunneling Protocol over IPsec (L2TP/IPsec), 345
Legacy remote clients
NAP. See (Network Access Protection (NAP))
VPN. See (Virtual Private Networking (VPN))

M
MAPS. See Microsoft Active Protection Service (MAPS)
Microsoft Active Protection Service (MAPS), 226
Microsoft Antimalware Engine
Scan, 216–217
Spyware Removal, 217
Update, 217–218
Microsoft Management Console (MMC), 317
Mitigation, application’s vulnerabilities
Attack Surface Analyzer, 287–288
Browser protection, 270–276
Enhanced Mitigation Experience Toolkit, 288
Microsoft Security Development Lifecycle, 267–268
SDI. Threat Modeling Tool, 285–286
UAC and AppLocker, 276–285
Windows App store security, 268–270
Windows SmartProtection, 268
Windows system, 268
MMC. See Microsoft Management Console (MMC)

N
NAP. See Network Access Protection (NAP)
NAT64
destination server, 341
DirectAccess client, 353
domain name resolution, 353
hit, 353
types, records, 353
National Security Agency (NSA), 235
NDES. See Network Device Enrollment Service (NDES)
Network Access Protection (NAP) components, 477, 478
Connection Request Policies, 481
description, 476
health policies, 477, 481
health status information, 477
HRA. See (Health Registration Authority (HRA))
with legacy clients, 477
network policies, 481, 483f
NPS. See (Network Policy Server (NPS))
protecting remote legacy, 477–478
role services, 476
on Windows Server 2012, 479–489
Network Device Enrollment Service (NDES), 74
Network Inspection System (NIS), 219
Network Location Awareness (NLA) domain networks, 330
guest/public networks, 330
private networks, 330
types, firewall policies, 331
Network Policy Server (NPS) components, 478
configuring VPN servers, 482–486
description, 478
and HRA, 478–479
PowerShell, 480–481, 481f
Server Manager, 480
types of policies, 481
Network security, IaaS aggregation, bandwidth, 503
bandwidth control and requirements, 500–502
datacenter networks, 503
Ethernet broadcast boundaries, 502
infrastructure, 504, 504f
network access control, 499–500
NVA, 497–498
physical infrastructure, 497
private cloud IaaS infrastructure, 498
remote access and administration methods, 504
scalability and performance, 502–504
virtual networks, 499
VLAN tagging/virtual NICs, 502–503
vulnerability assessment, 497, 498f
Network traffic monitoring external switch, 160
Hyper-V Switch, 160–163
internal switch, 160–161
port mirroring, 159, 159f
PowerShell cmdlet, 161
private switch, 161
Windows Server 2012, 159
Network vulnerability assessment (NVA), 497–498
NLA. See Network Location Awareness (NLA)
NPS. See Network Policy Server (NPS)
NSA. See National Security Agency (NSA)
NVA. See Network vulnerability assessment (NVA)
OCSP. See Online Certificate Status Protocol Responder (OCSP)
Online Certificate Status Protocol Responder (OCSP), 73–74
Patch management description, 121–122
WSUS. See (Windows Update Services (WSUS))
PCRs. See Platform Configuration Registers (PCRs)
Perform risk analysis, 6–7
Personal identification number (PIN), 256
Picture password description, 194
Desktop Experience, 194–195
gestures, 197
logging, 197–199
management issues, 199
PC Settings application, 196
PIN. See Personal identification number (PIN)
Planning authentication constrained delegation, 192–194
deployment, 194
KDC Proxy, 191–192
Kerberos, 191
picture password, 194–195
requirements, 193
Planning endpoint security, 17, 17f
Planning server roles, Windows 8, 12, 12f
Platform Configuration Registers (PCRs), 246–247
Platform security planning access control determination, 8–9
ADFS and ADRMS deployment, 13–14
application’s vulnerabilities, 18
broad network access, cloud computing, 19
business requirements, 5
cloud security, 20
compliance and regulatory requirements, company, 4
computing, cloud, 2–3, 3f
confidentiality, integrity and availability, 2
core elements, 5
core security principles, 2–3
description, 11–12
directory and certificate services, 12–13, 13f
environment with authentication and authorization, 16, 16f
foundation platform, 4, 5f
information security, 2
legacy remote clients, 20
network security, 9–10
network vulnerabilities, 18, 19f
operating system, 2, 3f
patch management with WSUS role, Windows 8, 14
perform risk analysis, 6–7
planning endpoint security, 17
planning server roles, Windows 8, 12, 12f
resources, cloud, 2
review policies and procedures, 7
risks and implications, 4
seamless and secure connection, DirectAccess, 19–20
secure client deployment, trusted boot and BitLocker, 17–18
secure software development strategy, 9
security awareness training, 7–8
standalone security products, 11
standards and guidelines, 7
system security operation, 10–11
virtualization security, 14–16
Point-to-point protocol (PPP), 344
Point-to-Point Tunneling Protocol (PPTP) communications, 441
connections, 471
description, 441 and L2TP, 441–442 vulnerabilities, 441
PowerShell and Netsh administration, 318–319 commands, WFAS, 318
PPP. See Point-to-point protocol (PPP)
PPTP. See Point-to-Point Tunneling Protocol (PPTP)
Protected Mode Internet Explorer (PMIE), 277–278
Q
Quality of service (QoS) technologies
IaaS cloud infrastructure, 501
network utilization, 501
SLA, 501
R
RBAC. See Role-based access control (RBAC)
Real-time protection, Windows Defender
availability, 218
detection, 218–219
Spyware Removal, 219
Remote Access
Active Directory Users, 471
additional features, 448, 449f
add roles and features wizard, 446, 446f, 447f
CMAK, 472, 474f
collection, 457, 460f
Connection Manager profile, 471
dial-in access, 471, 472f
and Getting Started Wizard, 453–457
install, 446, 448, 448f, 449f
installation type, 446, 447f
RAMgmtUI.exe, 457
setting up, dial-up/VPN connection, 471, 473f
Start Screen, 457, 459f
Remote Access Services (RAS)
DirectAccess and VPN Services, 448–450
Point-to-point protocol (PPP), 344–441
VPN connections, 440
Role-based access control (RBAC), 505
Routing and Remote Access Service (RRAS)
completing, RRAS setup wizard, 466, 466f
description, 466, 468f
installing, 448, 450f
packet filters, configuration, 468–469, 468f
Ports node, 466, 467f
and routing, 461, 462f
server, configuration, 466, 467f
setting up, VPN server, 461, 463f
unified server role, 444–445
RRAS. See Routing and Remote Access Service (RRAS)
Secure client deployment, mobile users
BitLocker full volume encryption, 248–265
data breaches, 240–242
portable devices, 240
trusted boot process, 243–248
Secure Sockets Tunneling Protocol (SSTP)
configured, 443
description, 442
Ports node, 466, 467f
and routing, 461, 462f
server, configuration, 466, 467f
setting up, VPN server, 461, 463f
unified server role, 444–445
Secure client deployment, mobile users
BitLocker full volume encryption, 248–265
data breaches, 240–242
portable devices, 240
trusted boot process, 243–248
Security Configuration Wizard (SCW)
Additional Services, 28
Administration selection, 26–28
auditing options, 32, 34f
Audit Policy, 32
core requirements, 22
feature selection, server’s role, 26, 27f
hardening, AD FS deployment, 95–96
name addition, security policy, 33, 35f
network security, 29
option category selection, 28, 28f
outbound authentication methods, 31–32
processing, 25
type of operation, 23, 24f
Windows configuration, unspecified service, 28–29
Windows Firewall rules, 29, 30f
XML file, 34
Security group, DirectAccess clients
Active Directory Administrative Center, 387, 387f
Create Group dialog box, 389, 389f, 390f
Group Policy, 387
steps, 387
Tasks pane, 387, 388f
users, 387, 388f
WMI filter approach, 387
Security identifiers (SIDs), 295
configure remote access wizard, 422, 423f
on directaccess application
server setup page, 433–434, 435f
DNS configuration page, 431–432, 432f
on DNS suffix search list page, 432, 433f
full DirectAccess, 422, 423, 424f
getting started wizard, 421–422, 422f
Groups page, 423–424
infrastructure servers, 430, 430f
management servers, 432, 433f
on network adapters screen, 427–428, 428f
Network Connectivity Assistant page, 424–425, 425f
on Network Location Server page, 430–431, 431f
on Network Topology page, 426–427, 428f
Operations Status, 434, 436f
on prefix configuration page, 429, 429f
in remote access review dialog, 434, 435f
remote clients and
configuration, 422, 423f
for remote management, 422
server configuration, 419–420
tools and remote access
management, 421, 421f
trusted boot process
code signing, 243
standard antimalware tools, 243
UEFI, 244–245
trusted platform module (TPM)
antimalware driver, 246–247
EKU, 246
group policy, 256–257
hardware test, 259
PCRs, 246–247
PIN, 256
startup key, 258
tool, Manage-bde, 257
user logs, 255
uac. see user access control (UAC)
UEFI. see unified extensible firmware interface (UEFI)
UIPI. See User Interface Privilege Isolation (UIPI)
Unified Extensible Firmware Interface (UEFI)
categorization, computers, 244
EFI, 244
industry standard firmware interface, 244
and Windows 8, 245–246
Windows 8 Boot hardening features, 246–248
Unified Remote Access
broadband Internet, 342
computer security, 343
computing device, 346
corporate network, 343
DirectAccess. See (DirectAccess deployment)
EAP, 345
EDGE1. See (DirectAccess server (EDGE1))
high-speed Internet connections, 343–344
L2TP/IPsec protocol, 345
Microsoft, 344
modem speeds, 342
packet fragmentation, 345
phone coupler-based modem, 342
PPP, 344
tunneling protocols, 346
universal firewall protocols, 345
VPN networking, 344
Web proxy, 348
User Access Control (UAC)
AppLocker Packaged App Rule, 280–284
installation and execution, Modern apps, 280
PMIE, 277–278
UIPI, 277–278
Windows 8, 280
Windows Vista, 276–277
User Interface Privilege Isolation (UIPI), 277–278
Virtual Desktop Infrastructure (VDI), 348
Virtualization security capabilities, 150, 150f
cloud computing, 14–16
Create Virtual Switch, 166
feature leverage, 164
Hyper-V architectural model, 150
Hyper-V Manager, 170
mono-lithic hypervisor, 151
Planned Failover dialog box, 172
service availability, 164
Settings dialog box, 168
Windows Firewall, 165
Windows Server 2012, Hyper-V, 151
Virtual machine (VM), 253
Virtual Private Networking (VPN) block PPTP connections, 471
DirectAccess and VPN Services, 448–450
firewall configuration, 469–470
install certificates, 470
and NAP. See (Network Access Protection (NAP))
planning process, 445
and PowerShell, 475–476, 475f
Remote Access. See (Remote Access)
remote workers, 440
RRAS. See (Routing and Remote Access Service (RRAS))
steps to deploying, 445
telecommuting team members, 440
Web Server (IIS) role, 450–453
Windows VPN protocols, 440–443
VM. See Virtual machine (VM)
VPN. See Virtual Private Networking (VPN)
Windows Defender, Windows 8 client-side configuration configuration interface, 220, 220f
excluded files and locations, 222, 224f
excluded file types, 223–224
excluded processes, 224
local configuration interface, 220
MAPS, 226
pornography, 222
real-time protection, 222, 223f
Windows Updates, 220, 221f
definition updates, 219
Group Policy Settings, 228–229
Microsoft Antimalware Engine, 216–218
Microsoft Security Essential, 216
NIS, 219–220
real-time protection, 218–219
security solution, 216
signature-based antimalware system, 219
Window Server Update Services (WSUS)
Microsoft Antimalware Engine Update, 217–218
patch management, 14, 15f
Windows Firewall with Advanced Security (WFAS)
Checking Status of Services, 320
control, group policy. See (Group policy)
Custom Log Files, 323
custom logging settings, profile, 300, 300f
disabling and modifying rules, 307–308
Event Logs, 320–321
exporting and importing policies, 309
filtering rules, 306–307
Firewall Log Text Files, 321–323
general settings, profile type, 298, 299f
inbound rule/outbound rule ICMP rules, 302, 303f
integrity and authentication, 305
IP addresses, 302, 304f
network types, 306, 309f
protocol/port-specific rules, transport protocol, 304, 306f
W
Web enrollment, 73
WIF. See Windows Identity Foundation (WIF)
Windows App store security access levels, 269, 269t
data leakage prevention, 269
IPC, 268–269
Windows Store app data storage, 269
User Interface Privilege Isolation (UIPI), 277–278
V
Validating configuration, WSUS
GPO, 144
MMC, 145
VDI. See Virtual Desktop Infrastructure (VDI)
Windows Firewall with Advanced Security (WFAS) (Continued)
rule types, 301, 301f
services and programs., 302, 302f
software/network equipment, 305
types, connections, 304, 307f
types, protocols, 302, 303f
IPSec connection security rules, 297
monitoring node, 300, 300f
operating systems and applications, 290
PowerShell and Netsh, 318–319
protected network connections, 298
Restoring Default Settings, 324
Rule merging, 298
rule types, 301, 301f
server and domain isolation, 331
Vista, 291
Windows 7, 291–292
Windows 8. See (Windows 8 Server)
Windows Identity Foundation (WIF), 97
Windows Management Instrumentation (WMI), 317
Windows PowerShell History Viewer, 53
Windows 8 Server
Action Center, 234
control panel, 292, 292f
domain networks, 292
Encrypting File System, 235–237
firewall rules, 295
group policy, 293–294
guest/public networks, 292
MMC, 293, 293f
private networks, 292
spectrum of components, 213–214, 213f
Windows Defender, 215–229
Windows Server 2012
home/work network, 295
internet, 295
IPSec transport mode, 294
network isolation controls access, 294
Windows PowerShell cmdlets for Windows Firewall, 294
Windows Store app network isolation, 294
Windows SmartScreen, 229–233
Windows Server 2012
ARP poisoning/spoofing protection, 152–153
deployment, NAP
client computers configuration, 488–489
Connection Request Policies, 481
Health Policies, 481
HRA configuration, 486–487
IPv6 configuration, 480
Network Policies, 481, 483f
Network Policy and Access Services role, 479–480
RADIUS servers, 477
using PowerShell, 480–481, 481f
using Server Manager, 480
VPN Servers, 482–486
DHCP guard protection, 154–155
Hyper-V, 152
port ACLs, 155–158
VPN. See (Virtual Private Networking (VPN))
Windows Server Update Services (WSUS), 14, 365
Windows SmartScreen, Windows 8 application reputation service, 229
GPO, 233
settings, 230
UAC, 232
Windows Update Services (WSUS)
Choose Upstream Server, 134
components, 126
configure synchronization, 135–136
configure target group, 136–138
confirm installation selections, 131
database considerations, 125
deployment, 129–135
design considerations, 128–129
design high availability, cluster environment, 129
enabled client-side targeting, 144
group policy, configure, 140–147
installation progress, 132
Microsoft Update Improvement Program, 132
PowerShell cmdlets, 126
PowerShell options, 138
Proxy Server, 134
role placement consideration, 125
security update, 122–123
Team Blog, 129–130
update options and target computers, 127
updates, 138–140
vendor releases, 123
Windows Server 2012, 124–129
Windows Server Update Services Wizard, 132
Windows VPN protocols
IPSec Tunnel Mode with IKEv2, 443
and L2TP/IPsec, 441–442
and PPTP, 441
and RRAS, 440–441
and SSTP, 441
WMI. See Windows Management Instrumentation (WMI)
WSUS. See Window Server Update Services (WSUS)