Microsoft

Designing and Implementing an Server Infrastructure

Second Edition

Exam Ref 70-413

Paul Ferrill
Tim Ferrill

Microsoft

Designing and Implementing an Enterprise Server Infrastructure

Exam Ref 70-413

Paul Ferrill
Tim Ferrill

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2014935079
ISBN: 978-0-7356-8540-6

Printed and bound in the United States of America.

First Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at http://www.microsoft.com/learning/booksurvey.

Acquisitions Editor: Anne Hamilton
Developmental Editor: Karen Szall
Editorial Production: Box Twelve Communications
Technical Reviewer: Brian Svidergol
Cover: Twist Creative • Seattle

Contents

This page intentionally left blank

Introduction

This book is written for IT professionals who want to earn the MCSE: Server Infrastructure certification for Windows Server 2012 R2. This certification requires that you've passed the following three exams, which have already earned you the MCSA: Windows Server 2012 certification:

- **70-410** Installing and Configuring Windows Server 2012
- **70-411** Administering Windows Server 2012
- **70-412** Configuring Advanced Windows Server 2012 Services

Alternatively if you hold one of the qualifying certifications from the Windows Server 2008 certification track, you can take the following exam in order to upgrade your existing certification to the MCSA: Windows Server 2012:

- **70-417** Upgrading Your Skills to MCSA Windows Server 2012

The 70-417 exam is basically a consolidation of the three exams required for the MCSA certification, primarily focused on changes and new features. Once you've achieved the MCSA: Windows Server 2012 certification, two additional exams must be passed in order to gain the MCSE: Server Infrastructure certification:

- **70-413** Designing and Implementing a Server Infrastructure
- **70-414** Implementing an Advanced Server Infrastructure

This book is primarily focused on the 70-413 exam, which indicates a couple of things. You can safely assume that the knowledge tested in the first three exams contain some prerequisite information for the 70-413 exams. In fact much of the content in this book (and the 70-413 exam) will draw directly upon the information you've already learned, but will require you to utilize this knowledge specifically from a design perspective. One thing you should pay special attention to throughout this book are requirements, as they will often drive what you can and can't do in certain situations.

As you are probably aware, the Windows Server 2012 R2 release introduced several major features, as well as updates and changes to existing features in Windows Server 2012. Both Windows Server 2012 and Windows Server 2012 R2 will be tested in the 70-413 exam, and you should be ready to answer questions asking which version is required to enable a certain feature.

The 70-413 exam tests your understanding of five domains and 20 objectives, encompassing critical services and features that form the basis of an enterprise server infrastructure.

For the purpose of this book, the focus is primarily on new features and capabilities in both Windows Server 2012 and Windows Server 2012 R2, though many of the core features and services have existed in previous versions of Windows Server. Because the 70-413 exam

is focused on the design phase of building an enterprise infrastructure, this book emphasizes the theory behind effective design—not the step-by-step or hands-on knowledge you'll likely find in the other exams.

While we've made every effort to cover all of the information being tested in the 70-413 exam, only the Microsoft exam team has access to the exam questions. This makes it impossible to cover each question or exam topic individually. Additionally, Microsoft commonly adds new questions to the exam, and some of the technologies covered here (such as those pertaining to Microsoft Azure or Windows PowerShell) are receiving updates at an ever-increasing frequency. For up-to-date information on these fast-moving technologies, both real-world and for the exam, use the resources provided by Microsoft at MSDN and TechNet.

This book is not a replacement for real-world experience; you will want to get your hands dirty and work with some of the services and tools covered in this book in order to fully understand how they function. If you don't have a lab environment available for your use, TechNet offers virtual labs, which can be an indispensable tool for getting hands-on time with the roles and features.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO **ALL MICROSOFT CERTIFICATIONS**

For information about Microsoft certifications, including a full list of available certifications, go to *http://www.microsoft.com/learning/en/us/certification/cert-default.aspx*.

Acknowledgments

Paul Ferrill To my wife, Sandy, for your tireless support of me and of our family. I could not have done this without you. You truly are a precious gift. To our children, not the least of which is my co-author Tim. It has been a joy to get to work together with my son on this project and I appreciate his taking on the bulk of the writing.

Thanks to the Microsoft Press team for the quality support and consistent professional approach to a tough process. Writing a book is hard work and this book would not have been completed without the efforts of Karen Szall, Anne Hamilton, and the project management of Jeff Riley. Brian Svidergol's technical expertise made a tremendous difference in the communication of a multitude of topics.

Tim Ferrill This book would never have been possible without the frequent and consistent assistance from the Microsoft Press team. The clarity, professionalism, and attention to detail made this process much smoother than it could have been. Thanks to Anne Hamilton for her assistance in getting everything rolling and answering any questions along the way. To Karen Szall for her patience, and for her communication skills and tact when she had to pass along the news that we had more work to do. To Jeff Riley for his willingness to help a beginner along, and his constant support when I started to become overwhelmed. A special thanks to Brian Svidergol, whose knowledge and experience with Windows Server and the enterprise is twice what I could ever hope to obtain.

I'd also like to thank my parents, Paul and Sandy Ferrill. Dad shared his love of technology with me, the passion to try new things, and the propensity to push buttons to see what happens. Mom was my teacher. This book is due, in part, to the English papers that came back bloodied and bruised from her crrection (sic) pen.

Finally, this book could never have happened without my beautiful wife, Jodi, being the ultimate example of patience. Not only did she give up her own time with me, she provided time to write while she was corralling five kids and going through a pregnancy. Jodi is my hero.

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

http://aka.ms/ER413R2

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at mspinput@microsoft.com.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *http://support.microsoft.com*.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority and your feedback is our most valuable asset. Please tell us what you think of this book at:

http://aka.ms/tellpress

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. While there is no substitution for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you round out your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Exam Ref and another study guide for your "at home" preparation and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you.

CHAPTER 3

Design and implement network access services

With how integral to our business lives our computers, files, and applications have become, much of our daily work requires access to network resources. The obvious trade-off of this scenario is the potential of not being able to accomplish certain aspects of our daily routine without having access to the network resources we count on.

This chapter delves into the tools available in Windows Server 2012 R2 that allow you to provide network access to users who do not have physical access to your network. Several solutions are supported that will provide different types of access depending on the type of resource and security required. The remote access features available in Windows Server 2012 R2 range from the traditional (VPN), to the modern (DirectAccess), to the cutting-edge (Web Application Proxy). Each of these features can be used in your enterprise to support a different kind of user, or you can pick and choose to meet the needs of your users.

A large part of the remote access discussion centers on security. Virtual private network (VPN) connections and remote access are particular areas of concern for security professionals because the purpose of the solution is to allow corporate resource access to users throughout the world. Ensuring that only authorized users access your network is key, and several techniques to help your network to remain safe will be discussed. We also discuss how to protect your network clients, both internal and through VPN, by using Network Access Protection (NAP) and Network Policy Server (NPS).

Scalability is also a topic of interest for remote access, particularly when discussing site-to-site VPN used to link corporate locations into a single logical network. Ensuring that your remote access solution is resilient and highly available is a crucial aspect of maintaining a corporate network that spans multiple locations.

Objectives in this chapter:

- Objective 3.1: Design a VPN solution
- Objective 3.2: Design a DirectAccess solution
- Objective 3.3: Design a Web Application Proxy solution
- Objective 3.4: Implement a scalable remote access solution
- Objective 3.5: Design and implement a network protection solution

Objective 3.1: Design a VPN solution

A VPN connection has been the solution for accessing resources on the corporate network while outside the bounds of the physical network. Several protocols are available for VPN communication, each with different levels of security and configuration requirements. Even though VPN has been around for years, do not mistake its longevity for obsolescence. Most corporations still use VPN solutions to support legacy or third-party clients, and will continue to do so for the foreseeable future.

One area that is relatively new to the discussion is the use of a VPN to connect to resources in Microsoft Azure. Using a site-to-site VPN, you can ensure secure communication between corporate resources in the cloud and on-premises resources. Service providers large and small can provide similar functionality to their customers—secure connectivity to their own applications—using the new multitenant site-to-site VPN feature in Windows Server 2012 R2.

This objective covers how to:

- Deploy certificates
- Configure firewalls
- Use client/site-to-site connections
- Understand bandwidth requirements
- Understand protocol implications
- Connect to Microsoft Azure IaaS
- Use the Connection Manager Administration Kit (CMAK) for VPN deployment configurations

Deploying certificates

Several aspects of VPN configuration either have the option to use certificates to improve security or an outright requirement for certificates to be used. Three standard VPN tunneling protocols are supported by Windows Server 2012 R2: PPTP, L2TP, and SSTP. Each of these protocols supports certificate-based authentication and encryption of some sort, as shown in Table 3-1.

TABLE 3-1 VPN protocol support for certificate-based authentication and encryption

VPN protocol	Authentication method
PPTP	EAP-TLS
L2TP	IPsec
SSTP	SSL

With certificate-based authentication, a key aspect is ensuring that the client trusts the server performing the authentication. There are multiple ways to achieve this trust relationship between client and server. For domain clients, an internal Certificate Authority (CA) allows you to configure computers to trust the corporate CA as well as enable autoenrollment for client certificates. If a public CA is used, a client-server trust typically exists already, but authentication using client certificates becomes difficult. A hybrid certificate deployment, in which your enterprise CA uses a root certificate from a trusted third party, allows you to combine the strengths of both options: automatic enrollment of domain members and inherent trust from external clients. Figure 3-1 shows an example of a hybrid certificate deployment.

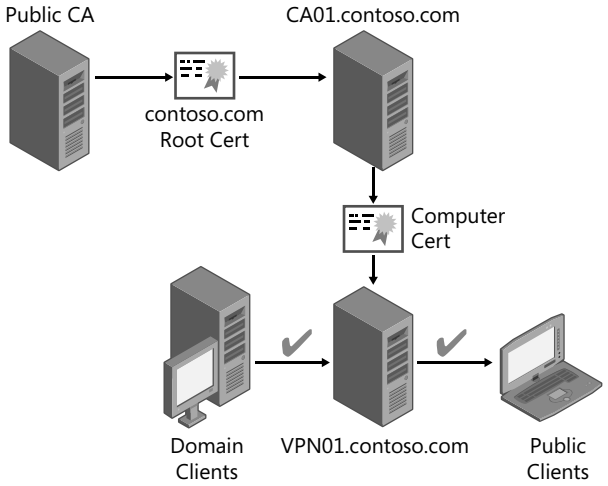

FIGURE 3-1 A hybrid certificate deployment

Client certificate enrollment can be accomplished in a number of ways. Typically, Group Policy is used for clients to automatically obtain certificates from the CA without any user intervention or knowledge. For clients that are not domain members, web-based enrollment can be used to obtain the necessary certificates to authenticate.

EXAM TIP

Certificates are used heavily throughout remote access. Some use cases call for certificates issued by an internal enterprise CA; others are best served using a certificate from a public CA. Knowing when and where to use certificates from different CAs is critical.

Configuring firewalls

Firewall rule configuration is important for enabling VPN traffic to reach remote access servers on your network. In addition to allowing incoming traffic on these ports, there is the potential for remote access servers to also function as VPN clients for site-to-site connections.

In this case, outbound traffic on these ports might need to be enabled as well. Rules enabling client traffic to traverse internal firewalls should also be created when the remote access server is hosted in a perimeter network (also known as a demilitarized network or DMZ). Table 3-2 contains a list of the ports used for VPN connectivity.

TABLE 3-2 Network ports used by VPN protocols

Port	Protocol	Use
TCP 1723	PPTP	PPTP tunnel
GRE (value 47)	PPTP	PPTP pass-through
UDP 500	L2TP	IKEv1/IKEv2 (IPsec)
UDP 4500	L2TP	IKEv1/IKEv2 (IPsec)
TCP 1701	L2TP	L2TP tunnel
ESP (value 50)	L2TP	IPsec
TCP 443	SSTP	SSTP tunnel

Besides the VPN protocols, various other protocols used for address translation and transition technologies might also need to be allowed to traverse the firewall. When using the 6to4 protocol, port 41 must be allowed through the edge firewall. If the public IPv6 address space is used for remote access, both TCP port 50 and UDP port 500 must be allowed through to the remote access server.

Using client/site-to-site connections

Over the years, VPN connections have evolved from a technology primarily used to connect clients to their workplace into one often used to secure corporate traffic between locations. Through the use of site-to-site VPN, illustrated in Figure 3-2, Internet-based connectivity can be used instead of dedicated network infrastructure to allow network traffic between sites and branches.

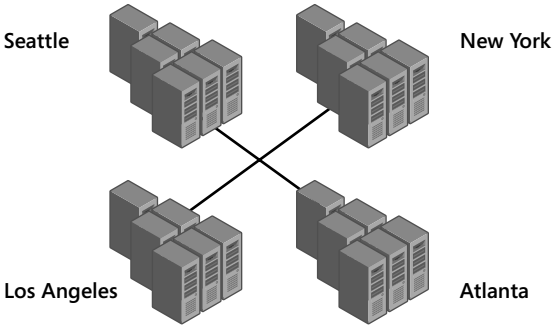

FIGURE 3-2 Site-to-site VPN allows you to link multiple sites into a single logical network

Windows Server 2012 R2 extends the capabilities for VPN connectivity by allowing for multitenant site-to-site or remote access connectivity. This functionality is designed for hosting environments or service providers with a need to provide secure connectivity directly from remote clients to individual Hyper-V virtual networks or virtual local area networks (VLANs).

EXAM TIP

Multitenant site-to-site VPN is a crucial piece of the Microsoft hybrid cloud strategy and is a new feature in Windows Server 2012 R2. Windows 8.1 also introduces auto-triggered VPN, which can be used to allow modern apps to automatically make a VPN connection. These and other new remote access features can be seen on the exam. More information on new remote access features in Windows Server 2012 R2 and Windows 8.1 can be found here: *http://technet.microsoft.com/en-us/library/dn383589.aspx*.

Understanding bandwidth requirements

Some requirements for remote access are simply intuitive. The bandwidth requirements are proportional to the number of clients you expect to use the remote access solution and how heavy you expect the usage to be. Particular attention should be paid to the differentiation between upload and download speeds provided by your Internet connection. Because many Internet providers provide high download speeds with a fraction of the available upload bandwidth, it can become problematic for users trying to access resources from outside the corporate network.

When designing your VPN solution, consider the Internet connections available within each site and within the organization as a whole. If one site has a significantly more robust Internet connection (see the New York location in Figure 3-3), it might make sense to centralize remote access servers to that site. If remote access traffic is expected to be heavy, it might make sense to have a dedicated Internet connection for remote access purposes to provide optimal performance. Users of site-to-site VPN might consider the use of rate limiting to prevent the Internet connection from being saturated by VPN traffic.

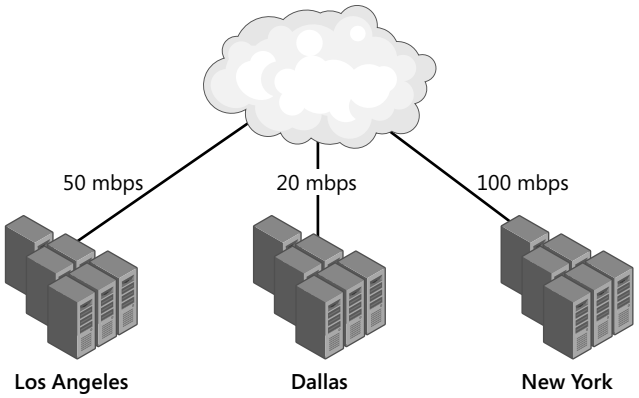

FIGURE 3-3 The bandwidth available to individual sites might dictate where your VPN infrastructure should be deployed

Understanding protocol implications

Several factors contribute to the decision about which VPN protocols to support in an organization. Security is always important, and in remote access scenarios both the authentication process and the VPN tunnel must be considered. Compatibility with clients is another important point to evaluate because newer VPN protocols might not be supported by all VPN clients. Additionally, some protocols handle firewall and NAT traversal better than others, making them better suited for clients connecting through networks found in homes, hotels, or even coffee shops. Performance can also be affected by the choice of protocol and should be a key aspect of any remote access design process.

Security is an important aspect of your VPN infrastructure, largely because it bypasses any physical security measures you might have in place. As already stated, both the authentication process and the VPN tunnel must be secured. Each protocol handles these factors differently; although each offers strong security, understanding the differences and requirements is important. Point to Point Tunneling Protocol (PPTP) supports Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication using certificates. Encryption of the PPTP tunnel is accomplished with Microsoft Point-to-Point Encryption (MPPE), which uses keys generated by the EAP-TLS authentication process. PPTP does not provide data confidentiality, so data can be modified in transit without being discovered. Layer 2 Tunneling Protocol (L2TP)/Internet Protocol security (IPsec) relies on IPsec for authentication, data integrity, and encryption using Data Encryption Standard (DES) or Triple DES (3DES) with keys generated through the Internet Key Exchange (IKE) negotiation process. IPsec requires a public key infrastructure (PKI) to issue computer certificates for client-server authentication, adding some complexity to an L2TP/IPsec deployment. Secure Socket Tunneling Protocol (SSTP) relies on the Secure Sockets Layer (SSL) for encryption, data integrity, and encapsulation while using EAP-TLS for authentication. Of the three traditional VPN protocols mentioned here, only SSTP supports two-factor authentication such as smart cards.

For clients to connect to your VPN implementation, they must support the protocol you choose. SSTP supports only clients using Windows Vista Service Pack 1 (SP1) or later, making it the most restrictive of the three options. L2TP/IPsec and PPTP both support clients using Windows XP and later.

Additional compatibility factors are the networking aspects of the three choices. The SSTP use of SSL makes it the best option for traversing Network Address Translation (NAT) or firewall devices. L2TP/IPsec supports NAT traversal, but might encounter problems on networks with more restrictive firewalls. PPTP requires a NAT device with a NAT editor capable of properly translating and routing the VPN tunnel.

Performance differences between the three VPN protocols discussed here have much to do with the type of encryption and encapsulation being used. Because PPTP uses the least amount of encryption and encapsulation, there is less overhead on both client and server to handle these processor-intensive operations. L2TP/IPsec encapsulates each packet four to six times, resulting in increased overhead on each end of the tunnel and making the processor performance of the remote access server critical.

Connecting to Microsoft Azure IaaS

Microsoft Azure enables you to connect your cloud-based virtual machines (VMs) and applications to your local network through the use of an Azure virtual network and site-to-site VPN connectivity. This functionality is very similar to the multitenant site-to-site VPN connectivity introduced in Windows Server 2012 R2. Not only can you name the connection and specify the VPN information but you can also configure local IP address pools and IP subnets. Point-to-site connectivity is also supported for scenarios in which only a few devices require connectivity to the virtual network, rather than an entire site.

A critical requirement for connecting your organization to an Azure virtual network is a public IPv4 address (public IPv6 addresses are not currently supported). A virtual network is configured using the Azure management portal, shown in Figure 3-4, or manually through the use of network configuration files.

Configuration of a virtual network using network configuration files typically involves exporting an existing virtual network configuration, making modifications to the XML file, and importing the network configuration file. Using manual configuration is an efficient way to rapidly deploy multiple virtual networks with similar configurations.

MORE INFO **NETWORK CONFIGURATION FILES**

Using network configuration files involves manually editing the XML files exported from the Azure management portal. More information on this process can be found here: *http://msdn.microsoft.com/en-us/library/azure/jj156097.aspx*.

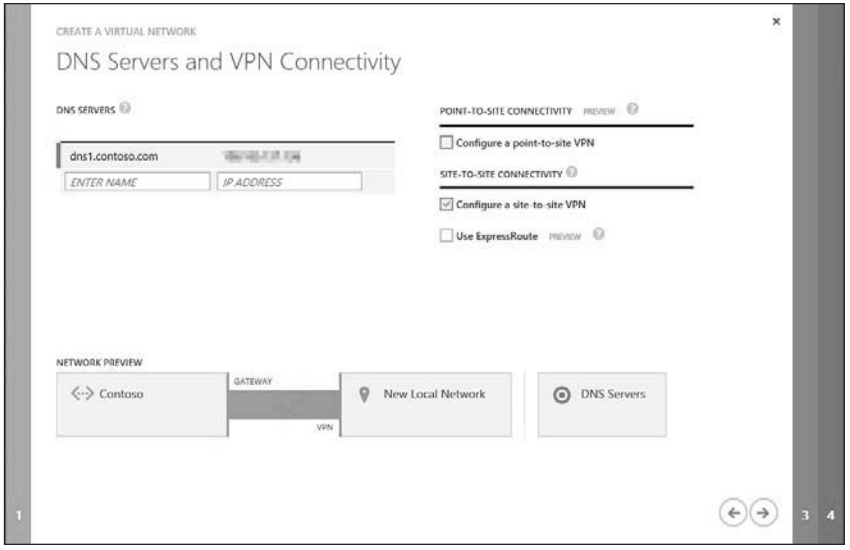

FIGURE 3-4 Site-to-site VPN can be used to create a private connection to a virtual network on Azure

EXAM TIP

Hybrid clouds and Azure are focal points in Windows Server 2012 and for Microsoft in general. Expect at least one question on connecting your corporate location to Azure using a site-to-site VPN.

Using the Connection Manager Administration Kit (CMAK) for VPN deployment configurations

The Connection Manager Administration Kit (CMAK) is a tool that allows an administrator to create a simplified method for users to create and initiate a VPN connection. By using CMAK, you can predefine the remote access server information, protocol options, and authentication method to be used. Even corporate branding and custom support numbers can be included. The result is a tool that can be made available to users to automate the VPN client configuration process.

CMAK is made available by installing the RAS Connection Manager Administration Kit (CMAK) feature in Windows Server 2012 and Windows 8. After it is installed, the Connection Manager Administration Kit Wizard (see Figure 3-5) guides you through the process of creating a Connection Manager profile. Options presented during the creation of a Connection Manager profile include configuring supported operating systems, naming for the profile and the executable, realm (domain) name, VPN connection types, proxy settings, and customization of graphics and support information.

FIGURE 3-5 The Connection Manager Administration Kit Wizard is used to create a Connection Manager profile that users can use to configure their VPN connection

The end product of the Connection Manager Administration Kit Wizard is an executable file that automates the process of creating and configuring a connection profile for end users, requiring minimal user interaction and reducing the support workload. Distributing this executable file can be accomplished through Group Policy, physical media such as CD or USB storage, or through a corporate website. After the end user runs the executable, a VPN connection profile is created, as shown in Figure 3-6, allowing connection to the corporate network.

FIGURE 3-6 Users can easily create connection profiles using the executable created by CMAK

Thought experiment

Designing a corporate VPN solution

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

Your company is working toward implementing a single integrated network throughout the nationwide corporate footprint. Each branch site should connect back to the datacenter at corporate headquarters. Answer the following questions regarding how your corporation's network unification goals can be achieved:

1. **The first step of connecting sites throughout the country/region is to create a connection to the corporate datacenter. What type of VPN connection can be used for this scenario?**
2. **Your corporate network, including VPN connections, will be encrypted using IPsec. What type of CA should be used to provide certificates for IPsec authentication?**
3. **Remote clients with work-issued computers will use DirectAccess to connect to the corporate network. What firewall rules need to be configured to allow this traffic to the remote access server at corporate headquarters?**
4. **To increase flexibility, your CIO wants to explore the possibility of shifting some corporate application servers to the cloud. What capabilities are offered with Azure to enable cloud functionality while maintaining connectivity to on-premises resources and ensuring the security of your corporate data?**

Objective summary

- Certificates are integral to securing VPN and remote access solutions, and can be used to authenticate users or computers with the remote access server. Depending on usage, either a public CA or an internal CA can be used.
- Some firewall configuration is required for VPN to allow the chosen protocol to reach the remote access server. Additional rules are required for 6to4 translation or use of public IPv6 addresses.
- VPNs can be created for either client-server or site-to-site communication, depending on the need. Windows Server 2012 R2 introduces the ability to support multitenant site-to-site VPNs for hosting providers to provide clients with secure access to their applications.
- Lack of necessary bandwidth to support the VPN workload can affect users and prevent access to corporate resources. Bandwidth should be considered during the design phase to determine which Internet connection to use and whether upgrades are needed.

- Each VPN protocol has different strengths and weaknesses related to security, compatibility, and performance. They should be considered when choosing the protocol to support.
- Workloads in Azure can be connected to on-premises networks through the use of VPN and Azure-based virtual networks.
- CMAK is used to create VPN connection profiles for end users, which enable simple configuration of the VPN client for end users.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. What type of server is required to use IPsec authentication?
   - **A.** Public CA
   - **B.** Enterprise CA
   - **C.** Stand-alone CA
   - **D.** Remote access server
2. Which firewall ports must be opened to enable L2TP traffic?
   - **A.** TCP 1701
   - **B.** TCP 1723
   - **C.** TCP 443
   - **D.** TCP 80
3. What feature in Windows Server 2012 R2 enables the deployment of a remote access solution allowing clients to connect directly to their own virtual networks within your datacenter?
   - **A.** Site-to-site VPN
   - **B.** Multisite VPN
   - **C.** Multitenant site-to-site
   - **D.** Microsoft Azure Virtual Network
4. Which VPN solution supports 3DES encryption?
   - **A.** PPTP
   - **B.** L2TP/IPsec
   - **C.** SSTP
   - **D.** All of the above

5. Which VPN protocol supports smart cards for authentication?
   - **A.** PPTP
   - **B.** L2TP/IPsec
   - **C.** SSTP
   - **D.** All of the above
6. What is the primary advantage of SSTP over PPTP and L2TP/IPsec?
   - **A.** NAT traversal
   - **B.** Security
   - **C.** Performance
   - **D.** Client compatibility
7. Which is not part of the Azure virtual network creation process?
   - **A.** Private DNS addresses
   - **B.** On-premises IP address pool configuration
   - **C.** Local IP subnet definition
   - **D.** VPN server IP address
8. What is the purpose of CMAK?
   - **A.** Manage VPN connection permissions for users
   - **B.** Deploy and configure remote access servers
   - **C.** Create preconfigured VPN profiles for end users
   - **D.** Create a site-to-site VPN connection with an Azure virtual network
9. How is CMAK installed?
   - **A.** The Windows feature must be installed.
   - **B.** CMAK must be downloaded from the Microsoft website.
   - **C.** CMAK is included on the Windows Server 2012 installation media.
   - **D.** CMAK is installed by default on both Windows 8 and Windows Server 2012.

Objective 3.2: Design a DirectAccess solution

DirectAccess is a remote access solution for Windows clients that allows for automatic, always-on connections to the corporate network. Introduced in Windows Server 2008 R2, DirectAccess is an improved method of providing remote connectivity to domain-joined computers. Typically deployed in conjunction with a more traditional VPN option, DirectAccess supports only client operating systems using Windows 7 or later. In addition to providing clients the ability to remain connected to corporate resources while outside the scope of the company network,

DirectAccess provides the ability to join computers to the domain while outside the bounds of the physical network, and a means to manage computers while they are outside the corporate network.

A big aspect of DirectAccess has to do with requirements. DirectAccess in Windows Server 2012 R2 is extremely flexible, capable of being configured in multiple topologies, and offers several new features. Each of these configuration topologies and features comes with its own set of requirements, which you will need to know to effectively design a DirectAccess deployment.

This objective covers how to:

- Understand DirectAccess deployment topology
- Migrate from Forefront UAG
- Use One-Time Password (OTP)
- Use enterprise Certificate Authority (CA) certificates

Understanding deployment topology

A major limitation of DirectAccess in Windows Server 2008 R2 was the inability to use the same server for both DirectAccess and traditional VPN through the use of routing and remote access. Windows Server 2012 unifies these capabilities in the Routing and Remote Access Service (RRAS) role.

Several of the new features in Windows Server 2012 have to do with support for different deployment topologies for DirectAccess. Windows Server 2008 R2 DirectAccess servers were required to have two network connections: one to the public Internet and one to the private network. Windows Server 2012 supports placement of remote access servers behind a NAT device and removes the requirement for multiple network connections. This greatly increases the flexibility of your network topology when planning for placement of your remote access server. Figure 3-7 shows the difference between these two topologies and exemplifies the increased flexibility offered by placing the DirectAccess server behind a NAT device.

Topologies featuring connectivity to both internal and external networks are still supported, but they are no longer the only option. The network topology can be configured in the Remote Access Server Setup Wizard, shown in Figure 3-8. Windows Server 2012 also removes the requirement for multiple public IPv4 addresses. ISATAP for IPv6 to IPv4 address translation is not supported with DirectAccess.

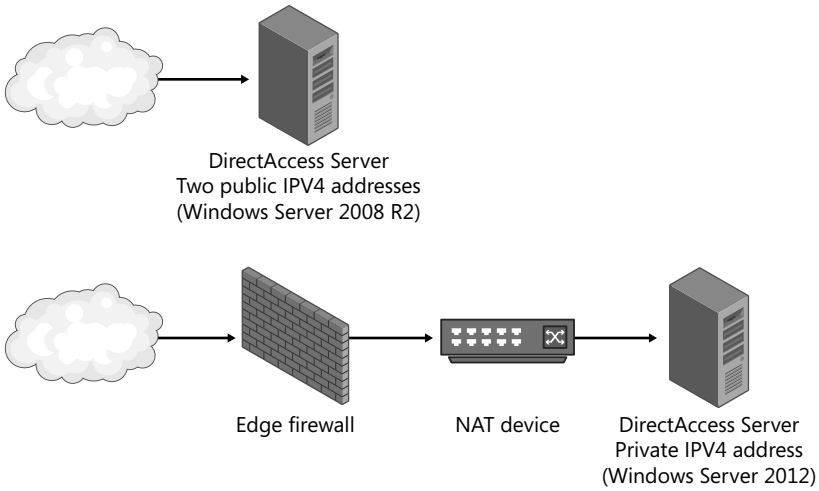

FIGURE 3-7 DirectAccess in Windows Server 2008 R2 required a direct connection to the Internet and at least two public IP addresses; Windows Server 2012 supports deployment behind a NAT device, adding much needed flexibility to the deployment topology

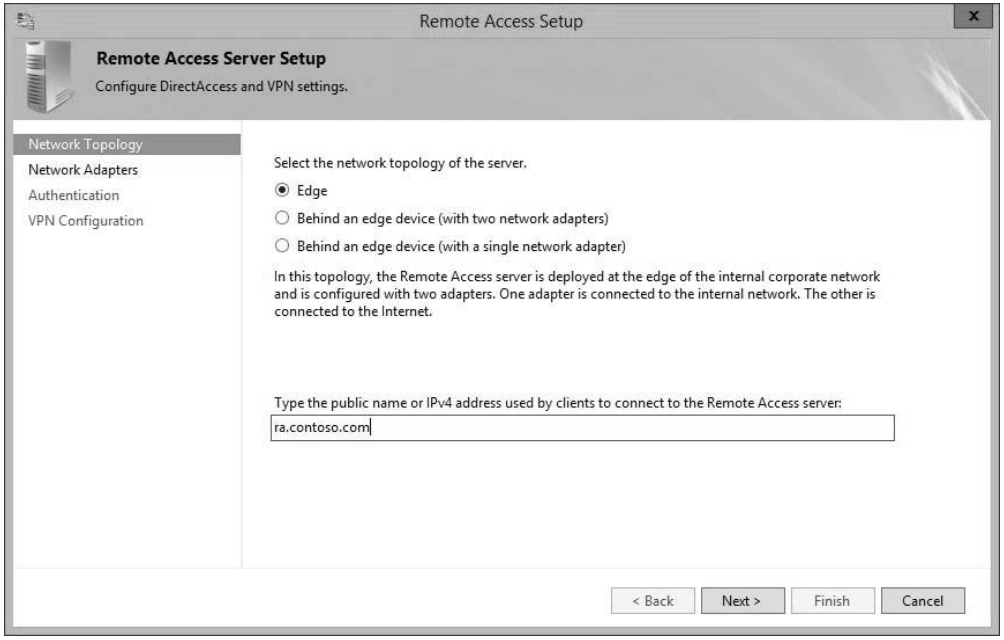

FIGURE 3-8 Windows Server 2012 supports placement of a remote access server behind a NAT device

Windows Server 2012 introduced support for Network Load Balancing (NLB) for remote access servers, which allows you to provide high availability in your remote access as well as improve scalability for large implementations.

In addition to the requirements for DirectAccess changing in Windows Server 2012, different topologies also have unique requirements. A single remote access server deployed using the Getting Started Wizard supports only clients running Windows 8 Enterprise or Windows 8.1 Enterprise. PKI is not required for a single remote access server deployed using the wizard, but two-factor authentication is not supported. DirectAccess clients cannot be configured in force tunnel mode (shown in Figure 3-9) when deployed using the Getting Started Wizard, resulting in only traffic destined for the corporate network being routed through the DirectAccess connection.

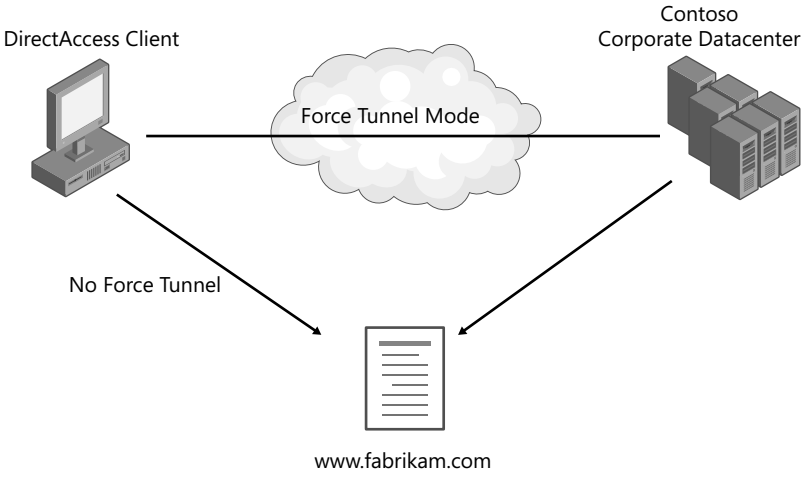

FIGURE 3-9 Force tunnel mode requires all traffic to go through the DirectAccess server and the associated corporate infrastructure; without force tunnel mode, only traffic destined for the corporate network goes through the DirectAccess connection

When a single remote access server is deployed using the Remote Access Setup Wizard, several requirements are different than when the Getting Started Wizard is used. (The two configuration options are shown in Figure 3-10.) Clients running Windows 7 or later are supported in this scenario, and a PKI is a requirement. Force tunnel mode is supported, but not when using KerbProxy authentication.

A multisite DirectAccess deployment enables automatic site selection for Windows 8–based VPN clients. However, Windows 7 clients can be configured to connect only to a single site. Multisite DirectAccess requires both IPv6 and a PKI.

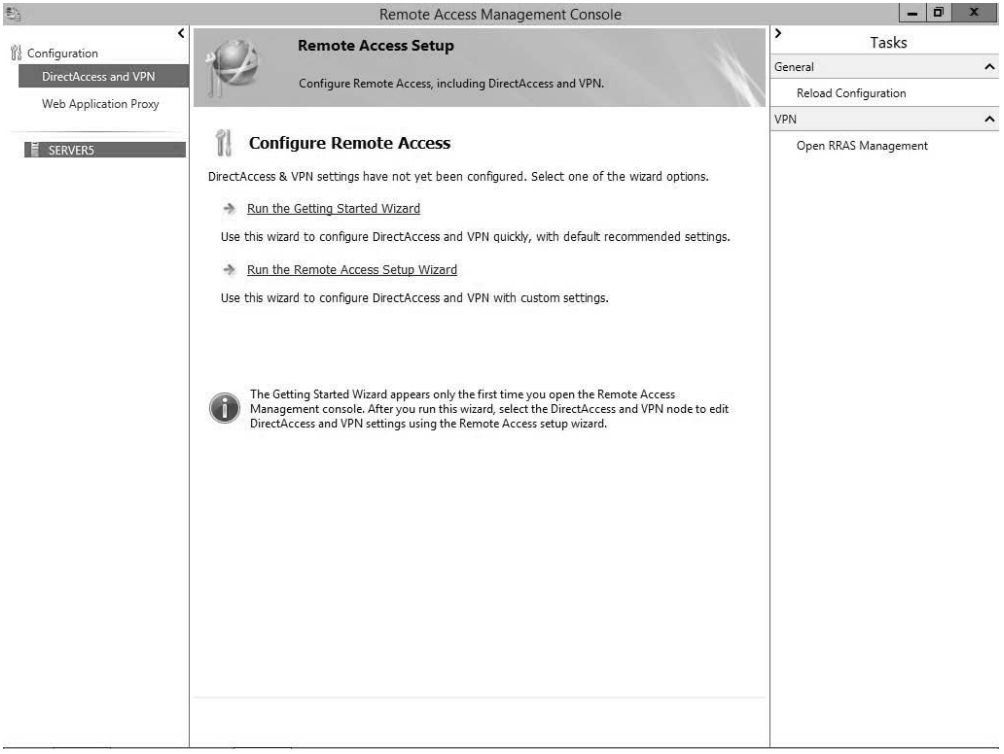

FIGURE 3-10 The two wizards presented in the Configure Remote Access page offer very different end results

EXAM TIP

The topology changes in DirectAccess are reason enough for many users to start implementing DirectAccess in their organizations. Support for a DirectAccess server behind a NAT device was introduced in Windows Server 2012, so make sure you understand the differences between the options.

Migrating from Forefront UAG

Migration from an existing Forefront Unified Access Gateway (UAG) DirectAccess server to a Windows Server 2012 R2 remote access server is supported, but there are several steps in the migration process that you should know. Two migration methods are supported: a side-by-side migration allows you to continue to serve clients throughout the migration process; an offline migration results in some downtime. Side-by-side migrations add complexity because some duplication of configuration options is required (such as fully qualified domain names [FQDNs] and IP addresses) because these settings must be unique to each server.

Prior to beginning the migration of your DirectAccess configuration, there are three prerequisites. First, the Forefront UAG server must be at SP1 before you can perform a migration. Also, ISATAP is not supported on the internal network, so it is recommended that native IPv6 be used. Finally, if the UAG server is also operating as a Network Policy Server (NPS) for Network Access Protection (NAP), this function cannot operate on the same server as the remote access server.

A side-by-side migration from Forefront UAG to a Windows Server 2012 remote access server involves exporting the DirectAccess settings using the Forefront UAG export feature, reconfiguring DirectAccess Group Policy Objects (GPOs), configuring new infrastructure and server settings, and deploying DirectAccess. Side-by-side migrations allow you to provide continuous DirectAccess service throughout the migration, which can be untenable for organizations requiring full-time availability from their DirectAccess servers. A side-by-side configuration adds complexity in the duplication required by supporting services and network configuration. FQDNs of the servers must be unique, as do IP addresses. Because both DirectAccess servers coexist for a time, these settings cannot be reused in a side-by-side migration, as shown in Figure 3-11. Due to the changes in the server's FQDN, certificates must be reissued for the new servers as well.

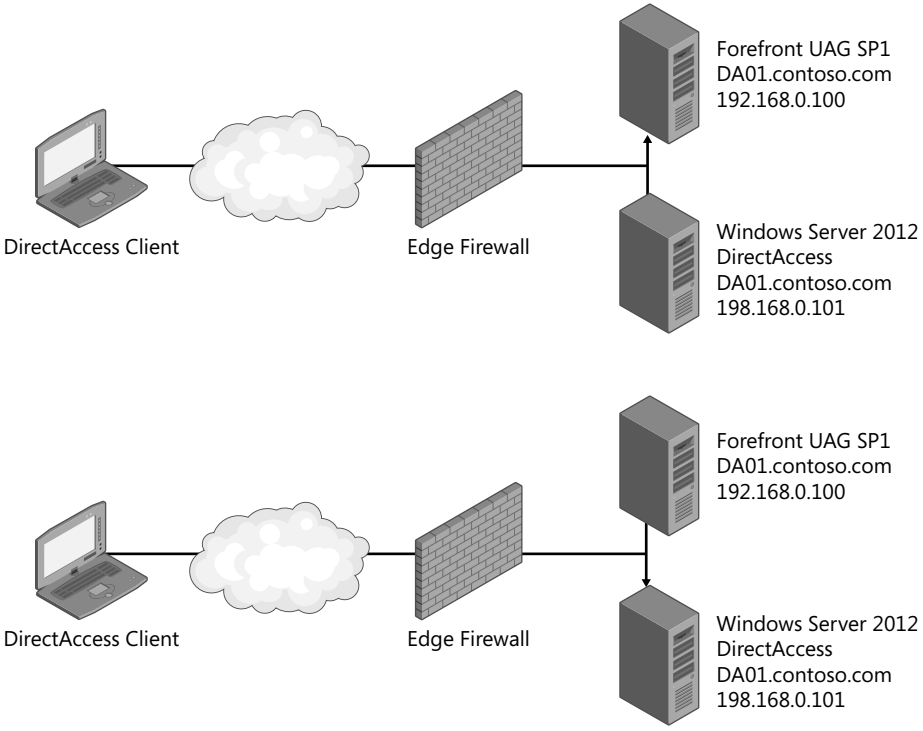

FIGURE 3-11 A side-by-side migration from Forefront UAG results in both the FQDN and IP address of the remote access server changing, which in turn requires that new certificates be issued

An offline migration involves configuring the new remote access server and reconfiguring the necessary GPOs. Offline migrations require some downtime because the new servers will typically reuse the same FQDN, IP address, and certificates, resulting in a trade-off between the procedural ease of the transition and the required downtime. Figure 3-12 shows an example of an offline migration, in which the Windows Server 2012 DirectAccess server is brought online and configured only after the Forefront UAG server is disconnected.

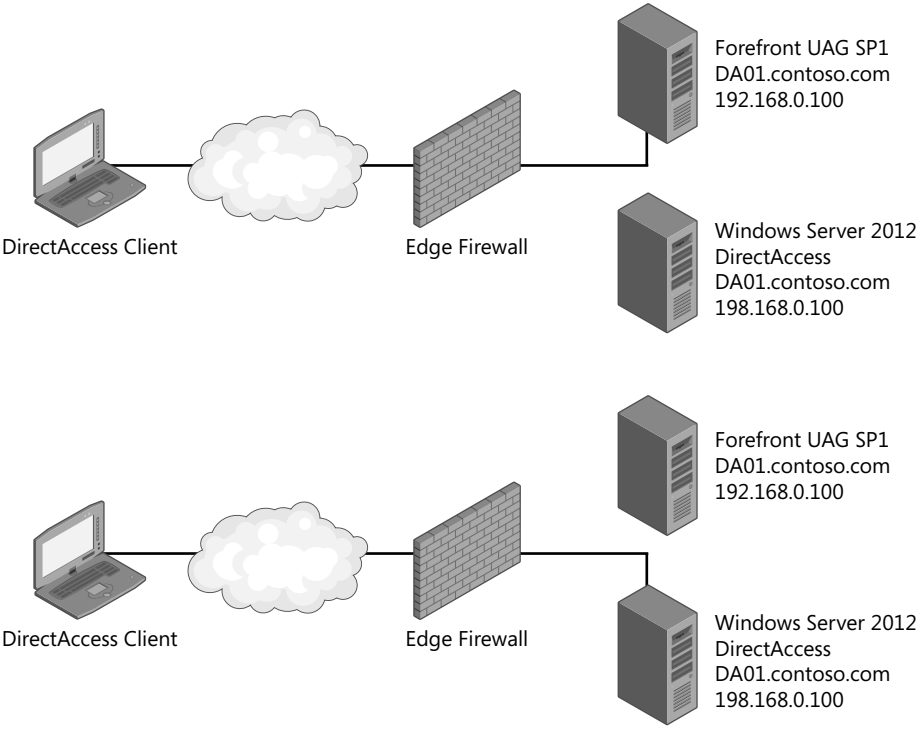

FIGURE 3-12 An offline migration simplifies the process as the FQDN, IP address, and certificate can be reused; downtime is required, however

MORE INFO **MIGRATING FROM FOREFRONT UAG**

Migrating from Forefront UAG to Windows Server 2012 DirectAccess is a complex process. For complete instructions on the full process, go to *http://technet.microsoft.com/en-us/library/hh831658.aspx*.

Using One-Time Password (OTP)

DirectAccess in Windows Server 2012 supports One-Time Password (OTP) two-factor authentication, providing increased security for remote access connections. Two-factor authentication was supported in Windows Server 2008 R2, but only by using smart cards. Support for OTP vendor solutions such as RSA SecurID enables existing enterprise security

systems to be used in conjunction with DirectAccess. DirectAccess also can be used with Trusted Platform Module (TPM)–based virtual smart cards to perform two-factor authentication. The option for OTP can be selected in the Authentication page of the Remote Access Server Setup Wizard, as shown in Figure 3-13. Windows 7 clients support DirectAccess with OTP authentication, but must use the DirectAccess Connectivity Assistant (DCA) 2.0.

To support OTP, an internal PKI must be available to issue certificates to DirectAccess clients. A Remote Authentication Dial-In User Service (RADIUS) server must also be configured to perform authentication. (RADIUS will be discussed in more detail in Objective 3.5).

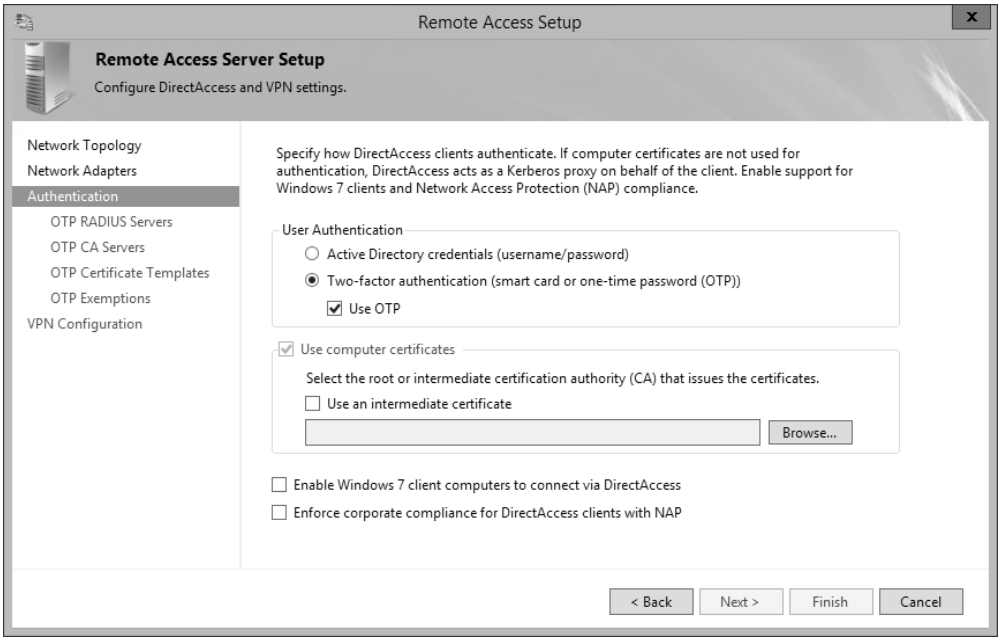

FIGURE 3-13 Two-factor authentication using OTP can be configured for remote access connections

MORE INFO **PKI AND CERTIFICATE CONFIGURATION FOR OTP**

For specifics on configuration of certificate templates, enrollment, and CA configuration for OTP, visit this page: *http://technet.microsoft.com/en-us/library/jj134161.aspx*.

Using enterprise Certificate Authority (CA) certificates

Certificates are central to several aspects of DirectAccess, and a PKI is required for some features such as OTP or smart card authentication. You must also have a PKI in place to support Windows 7 clients or to use a force tunnel configuration. Although many aspects of DirectAccess require certificates, it is no longer a requirement of DirectAccess as a whole in Windows Server 2012, which is a significant change from DirectAccess in Windows Server 2008 R2.

With DirectAccess, both the remote access server (IP-HTTPS) and the network location server require certificates. IP-HTTPS requires an HTTPS website certificate configured with the public IPv4 address or FQDN of the remote access server. The Certificate Revocation List (CRL) distribution point for the certificate issued for IP-HTTPS must be available to external clients, either by using a certificate issued by a public CA or by making the CRL from an internal CA available from outside the corporate network. The network location server also requires a website certificate, but because the network location server will be available only to clients already accessing the internal network, the CRL used to validate this certificate needs to be available only to the internal network.

MORE INFO **DIRECTACCESS CERTIFICATE REQUIREMENTS**

For information on the certificate prerequisites for the different DirectAccess deployment topologies, visit: *http://technet.microsoft.com/en-us/library/dn464273.aspx*. For more detail on the certificate needs of individual servers in your DirectAccess infrastructure, visit: *http://technet.microsoft.com/en-us/library/jj134148.aspx*.

Thought experiment

Planning a DirectAccess deployment

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You have been tasked with briefing management on the options available for improving your corporate remote access solution. Of specific importance are the security and manageability of remote clients. Management also wants to know the best method for migrating from the existing DirectAccess solution on a Forefront UAG server.

1. **One of the questions presented to you by corporate management has to do with the requirements for managing remote clients through DirectAccess. Can remote management through DirectAccess be enabled without permitting remote access to resources in the corporate network? How would you configure DirectAccess for only remote management?**
2. **A key requirement of any remote access solution is the ability to limit the clients that can connect remotely as well as the application servers that they can access remotely. Are these options configurable using DirectAccess in Windows Server 2012 R2?**
3. **What options are available for migrating from the Forefront UAG DirectAccess server? Are there any benefits of using one method over the other? What similarities are there in the two procedures?**

Objective summary

- In addition to supporting both DirectAccess and traditional VPN solutions on the same server, Windows Server 2012 improves the flexibility of the network location of the remote access server. Deployment behind a NAT device is now fully supported in Windows Server 2012.
- Two methods of migration from a Forefront UAG–based DirectAccess deployment are supported. A side-by-side migration eliminates downtime due to the migration, but requires duplication of FQDNs and IP addresses; an offline migration provides a simplified deployment, but requires some downtime.
- OTP support allows third-party OTP solutions to be integrated with your remote access solution. Virtual smart cards enabled by TPM chips are also supported.
- Although DirectAccess does not require a PKI in Windows Server 2012, different topologies and features require that a PKI be implemented. Additionally, both IP-HTTPS and the network location server require website certificates to be validated by DirectAccess clients.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which of the following remote access configuration options is used to enable placement of the DirectAccess server behind a NAT device? (Choose all that apply.)
   - **A.** Edge topology
   - **B.** Behind an edge device (with two network adapters)
   - **C.** Behind an edge device (with one network adapter)
   - **D.** DirectAccess for remote management only
2. Which options are not available when DirectAccess is configured using the Getting Started Wizard? (Choose all that apply.)
   - **A.** Force tunnel mode
   - **B.** Two-factor authentication
   - **C.** Placement behind an edge device
   - **D.** DirectAccess for remote management only

3. Which of the following is a newly supported method of authentication for DirectAccess in Windows Server 2012? (Choose all that apply.)

   A. OTP

   B. Smart card

   C. User name and password

   D. Virtual smart card

4. What prerequisite must be met before migrating from a Forefront UAG DirectAccess server to one based on Windows Server 2012?

   A. Public and private IPv6 support.

   B. Forefront UAG SP1 must be installed.

   C. A PKI must be deployed.

   D. Additional public IPv4 addresses must be available.

5. What benefit is provided by performing a side-by-side migration from Forefront UAG DirectAccess to Windows Server 2012?

   A. IP addresses and FQDNs can be reused.

   B. The migration process is automated.

   C. New certificates do not need to be issued.

   D. No downtime is required.

6. What requirement must be met for Windows 7 clients to use OTP for authentication to DirectAccess?

   A. PKI

   B. DCA 2.0

   C. RADIUS

   D. Windows 7 SP1

7. Which of the following certificate requirements is best served by a certificate issued from a public CA?

   A. Client computer certificate for IPsec

   B. Server computer certificate for IPsec

   C. SSL certificate for a network location server

   D. SSL certificate for an IP-HTTPS server

Objective 3.3: Design a Web Application Proxy solution

As cloud-based applications become more prolific, there is a need to provide similar flexibility with on-premises applications that reside within the corporate network. Although a solution such as DirectAccess provides simplified connectivity to internal network resources, DirectAccess is not a good fit when multiple device types or non-domain-joined computers are used.

Web Application Proxy is a new feature in Windows Server 2012 R2 that allows you to provide access to web applications within your internal corporate network through the use of a reverse proxy. Authentication requests can be passed from the Web Application Proxy to internal web applications to provide access to client devices that might not otherwise be able to gain access to resources on the corporate network.

The Web Application Proxy feature makes heavy use of Active Directory Federation Services (AD FS) and was previously known as AD FS 2.0 proxy. AD FS is covered in the 70-414 exam, as is the integration between Web Application Proxy and AD FS, but you need to know the basics for this exam as well.

This objective covers how to:

- Plan for applications
- Use authentication and authorization
- Use Workplace Join
- Use devices
- Use multifactor authentication
- Use multifactor access control
- Use Single Sign-On (SSO)
- Use certificates
- Plan access for internal and external clients

Planning for applications

The process of making web applications available through Web Application Proxy is known as publishing. Published applications can be accessed by remote clients using a number of different methods, including a standard web browser, Microsoft Office applications, or a Windows Store app. The device used does not require any additional software to access the application, and it does not have to be joined to the Active Directory domain.

A primary role of a Web Application Proxy is to facilitate authentication between the remote client and the application. Several forms of application authentication can be used

through Web Application Proxy, including claims-based, integrated Windows authentication; Microsoft Office Forms Based Authentication (MS-OFBA); and OAuth 2.0 authentication from Windows Store apps. Some examples of applications that can be published through Web Application Proxy are Microsoft SharePoint Server, Microsoft Exchange Server, and Microsoft Lync Server.

Using authentication and authorization

Authentication, which is the primary functionality offered by Web Application Proxy, affects the publication process significantly. Web Application Proxy also provides an additional layer in the authentication and authorization process for external clients, allowing you to limit access to applications from outside the network to only clients meeting certain requirements.

Access to a web application through a Web Application Proxy is enabled using AD FS. The connection to an AD FS server is configured using the Web Application Proxy Configuration Wizard, as shown in Figure 3-14. Preauthentication occurs to prevent any unauthorized traffic from reaching the internal web application. Several security mechanisms can be used to provide authentication and authorization to published web applications, many of which are discussed throughout this chapter.

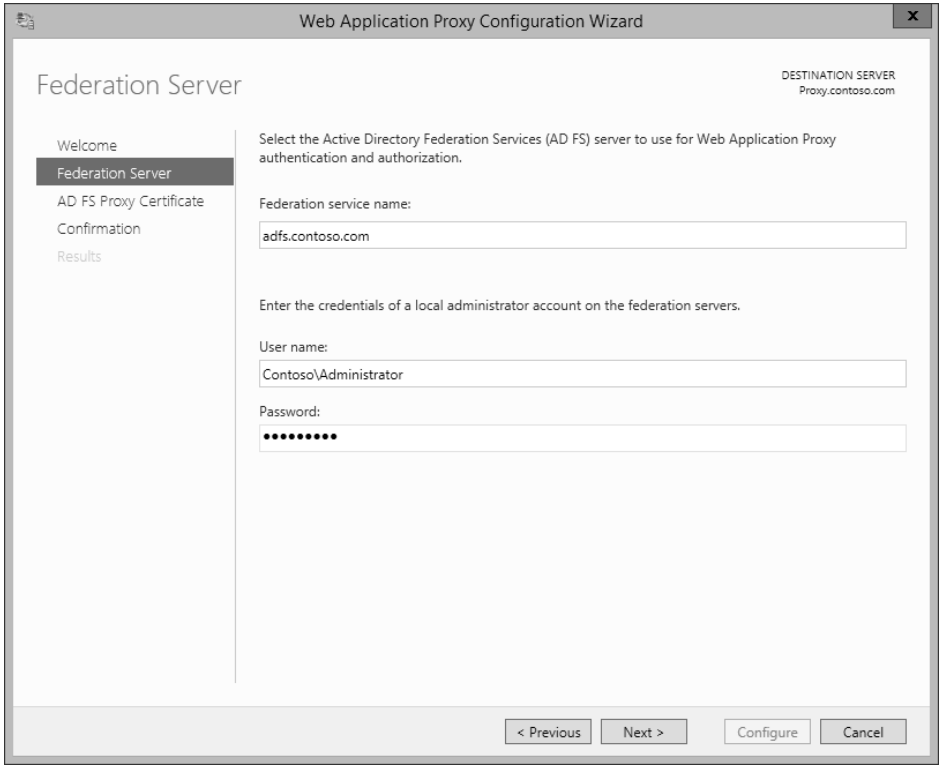

FIGURE 3-14 AD FS is used to perform the authentication process for Web Application Proxy

Preauthentication in Web Application Proxy comes in two forms: AD FS preauthentication and pass-through preauthentication. With AD FS preauthentication, a user is required to authenticate in some way prior to accessing the application, ensuring that only authorized users can reach the application. AD FS preauthentication is required for applications to make use of Workplace Join and multifactor authentication, both of which are discussed in this chapter.

Pass-through authentication does not require any user interaction before being directed to the application. In most cases, pass-through authentication is used only when the application performs authentication and authorization.

Using Workplace Join

A new feature in both Windows Server 2012 R2 and Windows 8.1, Workplace Join allows devices to be registered with the Active Directory Domain Services (AD DS) using the Device Registration Service (DRS) with AD FS. To support the DRS, the Active Directory Forest must be at the Windows Server 2012 R2 functional level, a process that extends the Active Directory schema to contain references to registered devices.

To enable the DRS, you must run the Initialize-ADDeviceRegistration command once for the forest from a federation server. The Enable-AdfsDeviceRegistration command must also be run once on each federation server. The DRS is automatically published to the Web Application Proxy when the proxy is deployed to make it available to external users. If the DRS is enabled after the Web Application Proxy has been deployed, you can run the Update-WebApplicationProxyDeviceRegistration command on the Web Application Proxy server to publish the DRS and make it available to external users.

Both Windows 8.1 and iOS devices can be connected using Workplace Join. By requiring registered users within AD FS (see Figure 3-15), device registration using Workplace Join can be configured as a requirement for accessing published applications.

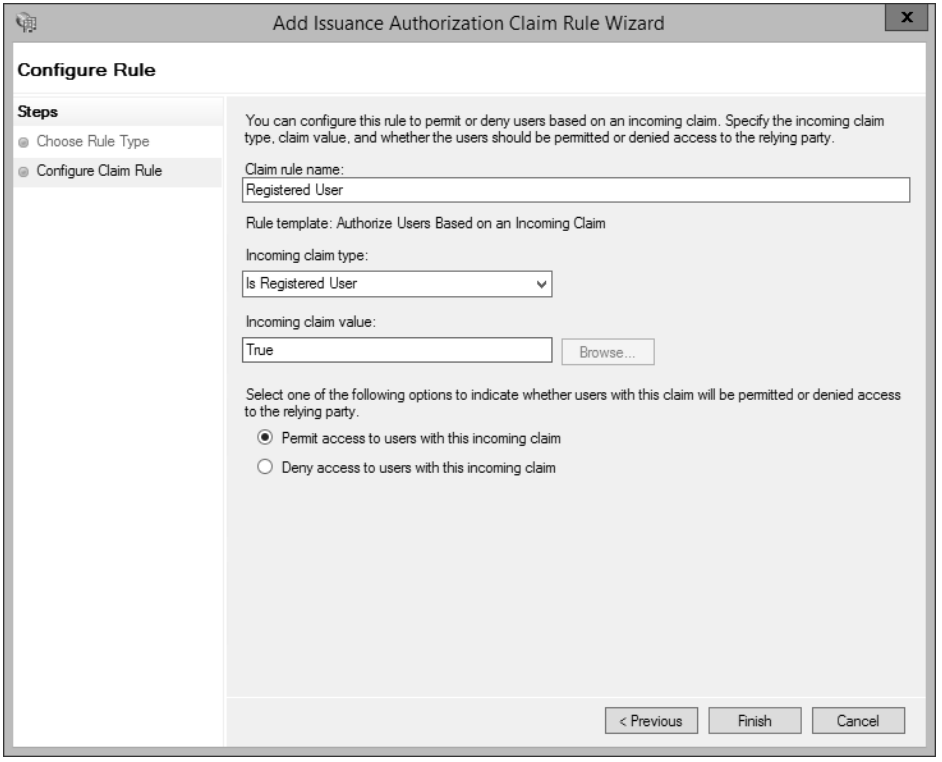

FIGURE 3-15 Configuring AD FS to require registration

Using devices

One of the major benefits of using Web Application Proxy is that it enables you to allow users to access internal web applications using whatever device they have available, whether it be a company-issued laptop or tablet, or even a personal device. The risk of allowing personal and unmanaged devices to connect to the corporate network is mitigated because an internal network connection is not required. As mentioned in the previous section, only Windows 8.1 and iOS devices currently support Workplace Join.

Using multifactor authentication

In addition to being able to limit access to applications to only those devices that are connected using Workplace Join, Web Application Proxy can require multifactor authentication through the use of certificates, smart cards, or OTP. Workplace Join is also a form of multifactor authentication because the device must be registered in addition to the user providing credentials.

Using multifactor access control

With AD FS preauthentication in Windows Server 2012 R2, access control can be managed using multiple factors such as user, device, location, or authentication data. Any of these claim types can be required to gain access to applications through the Web Application Proxy. For example, you could configure a multifactor access control policy to require members of certain Active Directory groups to perform authentication using a smart card before gaining access to an application through the Web Application Proxy.

Using Single Sign-On (SSO)

A Web Application Proxy can provide Single Sign-On (SSO) only if the Web Application Proxy is a member of an Active Directory domain. AD FS preauthentication is used to allow SSO to published applications. After a user authenticates to the Web Application Proxy, AD FS attaches an SSO cookie to further requests, ensuring that the user continues to have access to published applications.

EXAM TIP

There are many similarities between some of the different authentication types available for use with AD FS and Web Application Proxy. You should have a good understanding of the options and how they differ.

Using certificates

Web Application Proxy depends heavily on SSL certificates to secure traffic with remote clients. Because these clients are not required to be domain joined, the certificates used are usually issued by an external CA. Single-name certificates, subject alternative name (SAN) certificates, and wildcard certificates are supported. Multiple certificates might be required to support multiple published applications.

In addition to the Web Application Proxy server, AD FS relies on certificates for the services it provides. The certificates used for AD FS must also be from an external CA. AD FS requires a SAN certificate because both the <federation service name>.<domain suffix> and enterpriseregistration.<domain suffix> FQDNs must be supported.

Planning access for internal and external clients

The intent of deploying Web Application Proxy is to enable external clients to access internal web applications. Using FQDNs that resolve to the application internally and the Web Application Proxy externally enables users to access their applications without having to remember a unique external URL. Web Application Proxy can facilitate this process through the use of URL translation, shown in Figure 3-16, which is configured during the application publishing process.

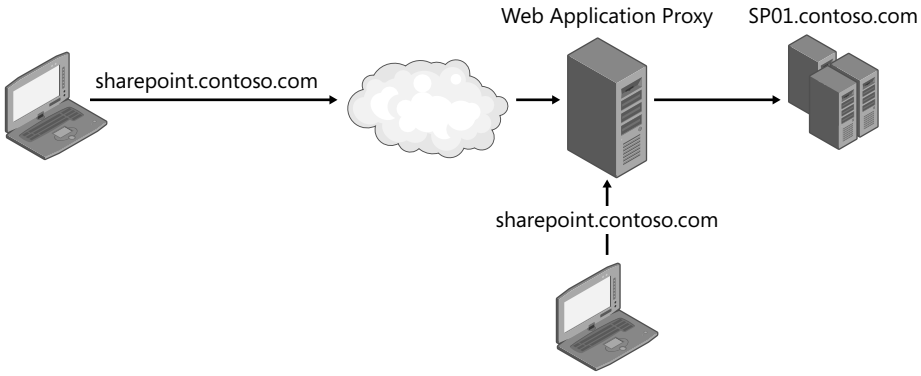

FIGURE 3-16 URL translation is used to allow users to access applications using the same URL from both internal and external clients

EXAM TIP

Web Application Proxy is one of the important new features in Windows Server 2012 R2. You should have a solid grasp of the requirements for the feature, the different options available, and how these options affect potential users and devices.

Thought experiment

Planning a Web Application Proxy deployment

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

Your company is considering allowing users to access web applications hosted within the corporate network using devices they have available. Answer the following questions for the corporate management team regarding Web Application Proxy:

1. **Is there a way to allow access to internal web applications from devices that are not domain joined, but still require a device registration process? What limitations should be in place if you implement such a solution?**
2. **Passwords and other authentication methods can be problematic and awkward on tablet devices. We certainly want users to authenticate to our web applications, but allowing them to authenticate once and then access any application they have access to would be the best solution. Are there capabilities to do this using Web Application Proxy? What requirements would have to be met for SSO?**
3. **What certificate needs are introduced by implementing Web Application Proxy? Can these needs be met using an internal CA?**

Objective summary

- Web Application Proxy provides external clients with access to internal web applications enabled through the publishing process.
- AD FS is used to provide multiple authentication methods for Web Application Proxy.
- Applications published in Web Application Proxy are accessible through a standard web browser, Microsoft Office applications, or Windows Store apps.
- Web Application Proxy supports AD FS preauthentication, which allows you to ensure that clients are allowed to access an application prior to serving the application. AD FS preauthentication also allows you to use Workplace Join and multifactor authentication.
- Workplace Join can be used with Web Application Proxy to provide access only to devices that have completed the registration process.
- Any device with a web browser can access applications through the Web Application Proxy, although only Windows 8.1 and iOS devices support Workplace Join.
- Multifactor authentication can be used with AD FS preauthentication to require authentication by using certificates, smart cards, or OTP.
- Multifactor access control allows you to design policies to gain more control over the authentication process through a Web Application Proxy.
- Published applications can make use of SSO within Web Application Proxy.
- To secure communication with external clients, certificates from an external CA are required for the Web Application Proxy and AD FS servers.
- Web Application Proxy uses URL translation to allow both internal and external clients to access applications using a consistent FQDN.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which service does Web Application Proxy interact with to perform authentication?
   - **A.** AD FS
   - **B.** AD DS
   - **C.** AD CS
   - **D.** AD FS Proxy

2. What is required of a device to access an application through a Web Application Proxy?
   - **A.** Membership in an Active Directory domain
   - **B.** Registration through Workplace Join
   - **C.** Windows 8.1 operating system
   - **D.** Web browser, Microsoft Office application, or compatible Windows 8.1 app
3. Which of the following relies exclusively on the application to authenticate users?
   - **A.** AD FS preauthentication
   - **B.** SSO
   - **C.** Pass-through authentication
   - **D.** Multifactor access control
4. What benefits are offered by using Workplace Join as an authentication method for a Web Application Proxy? (Choose all that apply.)
   - **A.** It does not require devices to be domain members.
   - **B.** It allows the use of any device with a web browser.
   - **C.** It requires device registration.
   - **D.** It ensures that devices meet corporate security requirements.
5. Which operating systems support Workplace Join? (Choose all that apply.)
   - **A.** Windows 8
   - **B.** iOS
   - **C.** Windows 8.1
   - **D.** UNIX
6. What allows you to require members of a specific group to authenticate using a smart card?
   - **A.** SSO
   - **B.** Workplace Join
   - **C.** Multifactor authentication
   - **D.** Multifactor access control
7. What are the requirements to use SSO with Web Application Proxy?
   - **A.** The client must be connected using Workplace Join.
   - **B.** The client must be joined to the domain.
   - **C.** The Web Application Proxy server must be domain joined.
   - **D.** The client must be using a Windows 8.1 or iOS device.

8. What aspect of Web Application Proxy allows both internal and external clients to access applications using the same URL?

   A. DNS CNAME records

   B. URL translation

   C. Pass-through authentication

   D. Workplace Join

Objective 3.4: Implement a scalable remote access solution

As businesses rely more extensively on remote access solutions, it is important to know the options available to increase scalability and fault tolerance for remote access. Whether you support traditional VPN services, site-to-site connectivity, DirectAccess, or Web Application Proxy, reliability and performance are critical. Fortunately, Windows Server 2012 R2 includes capabilities to support high availability and expansion of the remote access services throughout your enterprise.

This objective covers how to:

- Configure site-to-site VPNs
- Configure packet filters
- Implement packet tracing
- Implement multisite remote access
- Configure remote access clustered with Network Load Balancing (NLB)
- Implement an advanced DirectAccess solution
- Configure multiple RADIUS server groups and infrastructure
- Configure Web Application Proxy for clustering

Configuring site-to-site VPNs

Site-to-site VPN meets many of the requirements formerly met only through dedicated network connectivity between corporate locations. Through site-to-site VPN connections, an enterprise can link multiple physical locations across the globe into a single logical network, which improves access to applications, shared resources, and services critical to the corporate infrastructure. As mentioned earlier in this chapter, site-to-site VPN connections can also be used to create a secure tunnel to cloud services such as Azure. Windows Server 2012 supports either the PPTP or L2TP/IPsec protocol for creation of site-to-site connections, with all the implications related to security and performance applying.

Site-to-site VPN can be enabled through the Remote Access Management Console by clicking the Enable Site-to-Site VPN link in the Tasks panel. After the configuration is complete, the RRAS has to be restarted.

Configuring packet filters

Packet filters are similar to network firewall rules in that they are used to restrict certain types of network traffic. The Routing and Remote Access console allows you to manage the types of network traffic allowed to traverse a network interface. Both inbound and outbound filters can be configured, and IPv4 and IPv6 traffic are both supported. Packet filters can be configured to pass or drop packets that meet the configured filters.

To configure packet filters, navigate to the General node under either IPv4 or IPv6 in the Routing and Remote Access console. Within the properties for a network interface are buttons labeled Inbound Filters and Outbound Filters. The Inbound Filters window is shown in Figure 3-17.

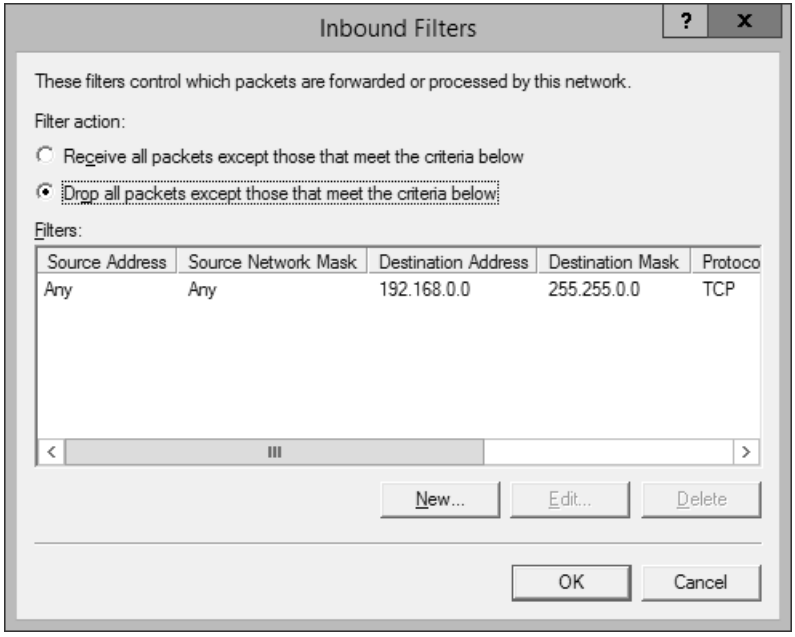

FIGURE 3-17 Inbound packet filters are used to control the flow of traffic through a remote access server

MORE INFO **PACKET FILTERING**

For more detailed directions on configuring packet filters in the Routing and Remote Access console, visit: *http://technet.microsoft.com/en-us/library/dd469754(v=WS.10).aspx*.

Implementing packet tracing

Packet tracing enables troubleshooting of network connections by logging traffic, which can be monitored and analyzed to pinpoint configuration problems. Packet tracing can be enabled in the Dashboard section of the Remote Access Management Console by clicking the Start Tracing link in the Tasks panel, which displays the window shown in Figure 3-18. New logs can be created, existing logs can be appended to, and existing logs can be overwritten using circular logging. Packet tracing is useful for troubleshooting network or firewall problems, or for tracking security concerns.

Packet tracing is resource-intensive, using both processor and storage resources. The tracing feature should be enabled only for troubleshooting purposes and should be disabled after diagnostics are complete.

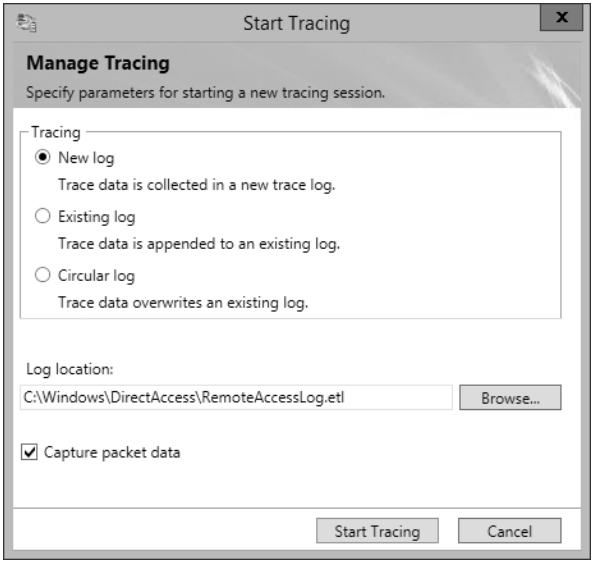

FIGURE 3-18 Packet tracing can be used to create log files detailing remote access traffic

Implementing multisite remote access

A multisite remote access deployment enables users to connect directly to any site containing a remote access server configured as an entry point. The decision about which site to connect to can be fully automatic for Windows 8 clients, it can be the site with the best possible connectivity (as shown in Figure 3-19), or the user can be allowed to decide which site to use. Even a global load balancer can be used for users to be automatically directed to another site if one site is unavailable. Windows 7 users are restricted to a single site, so if the remote access server at the predefined site is unavailable, they must wait until the remote access server returns to service.

Multisite remote access can be used to deploy endpoints to every corporate location or only those that serve as central hubs. In addition to providing optimal performance between remote users and the remote access server, consider the location of corporate resources being accessed through the remote access connection; it might affect your deployment of remote access endpoints through your corporate infrastructure.

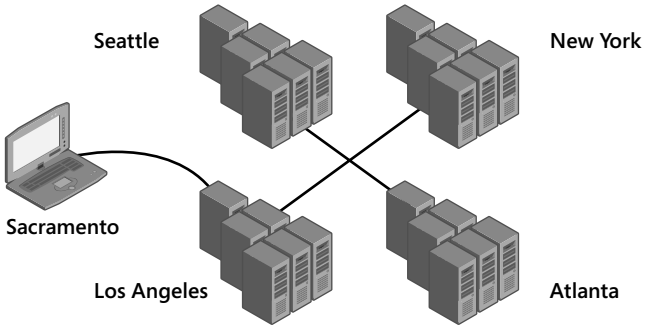

FIGURE 3-19 Multisite remote access makes possible automatic connection to the location with the best connectivity

There are a couple of requirements for multisite remote access. First, Web Application Proxy cannot be installed on the same remote access server. IPsec authentication must be configured for the remote access server, and both the network location server and the IP-HTTPS server must use certificates from a CA (they cannot be self-signed).

Two wizards govern the use of multisite remote access. The Enable Multisite Deployment Wizard is used to configure the initial multisite deployment, including the selection of the first entry point for the multisite deployment. During multisite deployment, you can configure global load balancing and support for Windows 7 clients. Additional entry points are created through the Add An Entry Point Wizard, which is run on the DirectAccess server being added.

Configuring remote access clustered with NLB

To provide high availability, remote access can be configured as an NLB cluster. Prior to configuring NLB for remote access, the NLB feature must be installed using the Add Roles And Features Wizard.

Executing the Enable Load Balancing Wizard allows you to specify IPv4 and IPv6 prefixes for use with the NLB cluster. Because each server in the NLB cluster must be able to authenticate as the IP-HTTPS server, the HTTPS certificate must be deployed to each server in the cluster.

MORE INFO **IMPLEMENTING NLB FOR DIRECTACCESS**

For complete details on deploying DirectAccess in an NLB cluster, visit *http://technet.microsoft.com/en-us/library/jj134175.aspx*.

Implementing an advanced DirectAccess solution

Upon initial deployment of a remote access server, you have the choice of running a Getting Started Wizard or the Remote Access Setup Wizard. Although the Getting Started Wizard helps you get DirectAccess up and running with minimal effort, it does not give you the options required to configure the more advanced aspects of DirectAccess and does not support implementing these options at a later date without completely reconfiguring DirectAccess.

If you plan to use OTP or smart cards for authentication immediately or in the future, you must use the Remote Access Setup Wizard because the CA must be configured as well as RADIUS and certificates for OTP. The same is true for multisite DirectAccess: If not configured, using the Remote Access Setup Wizard multisite is not supported, and the DirectAccess server must be reconfigured. Support for Windows 7 also requires configuration using the Remote Access Setup Wizard because support for Windows 7 clients also requires computer certificates issued by a root or intermediate CA. NAP enforcement and RADIUS authentication are also enabled with the Remote Access Setup Wizard.

Configuring multiple RADIUS server groups and infrastructure

Both DirectAccess and traditional VPN connections can be authenticated through a RADIUS server such as a Windows Server 2012 R2–based NPS. RADIUS gives you increased control over the authentication process through policies and centralized management, and it also allows you to use other authentication types such as OTP with Web Application Proxy.

Another benefit of using RADIUS for authentication is the ability to manage authentication traffic, distributing it across a RADIUS server group. The Remote Access Setup Wizard allows for RADIUS authentication on the VPN Configuration page. One or more RADIUS servers can be configured and prioritized in a list. RADIUS server groups can then be configured, as shown in Figure 3-20, to handle these authentication requests as they are routed to the RADIUS servers. (NPS and RADIUS are discussed in more detail in Objective 3.5.)

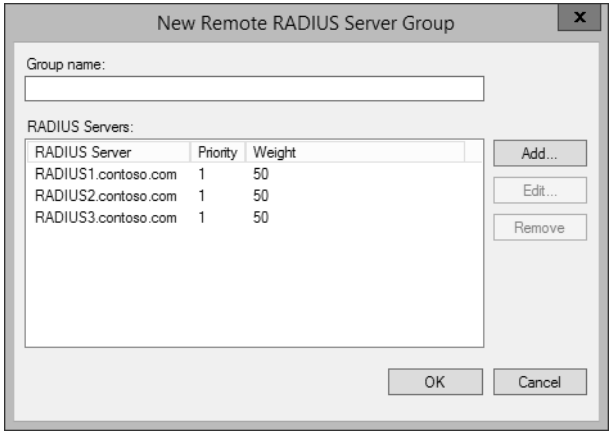

FIGURE 3-20 RADIUS server groups are used to load balance, prioritize, and provide high availability for RADIUS authentication

Configuring Web Application Proxy for clustering

To provide optimal performance and high availability, it might be necessary to deploy multiple Web Application Proxy servers. Configuration information for Web Application Proxy servers is stored within AD FS. Additional Web Application Proxy servers are configured automatically using this configuration information during deployment through the use of the Web Application Proxy Configuration Wizard.

Thought experiment

Configuring a scalable remote access implementation

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You have been tasked with implementing a modern remote access solution for your corporation, replacing the existing VPN solution. With the modernization of the internal corporate network and application infrastructure, the remote access solution must be able to provide seamless access to these applications.

1. **Your company has begun to expand to other locations, and maintaining access to network resources regardless of corporate location is critical for users. What remote access tool allows you to link corporate locations into a single logical network?**
2. **In addition to linking corporate locations into a single network, a solution that allows users to automatically create a remote access connection to the closest corporate location has been requested. What option in Windows Server 2012 supports this functionality?**
3. **Is there any functionality in Windows Server 2012 R2 that allows you to create a high-availability solution to provide remote access to internal web applications? What configuration steps are required to implement this solution in a clustered environment?**

Objective summary

- Site-to-site VPNs can be used to create a single logical network out of multiple physical locations.
- Using the Routing and Remote Access console, packet filters can be configured to allow or disallow certain types of traffic over a specific network interface.
- Packet tracing is a troubleshooting tool that allows you to log diagnostic information about network traffic as it passes through your remote access server.

- Multisite remote access in Windows Server 2012 can be used to automatically connect Windows 8 users to the site offering the best connectivity.
- Remote access servers can be made highly available and can distribute the workload across multiple servers using NLB clusters.
- Several features in remote access can be used only when they are configured using advanced settings: multiple servers, multisite, two-factor authentication, and force tunneling.
- RADIUS servers provide increased flexibility for authenticating remote access connections, including the capability to create RADIUS server groups to provide improved performance and fault tolerance.
- Web Application Proxy servers can be clustered to provide high availability and improve performance.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Your users can connect to your remote access server, but cannot access network resources. What might be the cause of this problem?
   - **A.** Packet filtering on the Internet connection
   - **B.** Packet filtering on the intranet connection
   - **C.** Packet tracing is enabled
   - **D.** Packet tracing is disabled
2. What is the minimum required client operating system supported for a user to automatically connect to the optimal remote access server?
   - **A.** Windows Vista SP1
   - **B.** Windows 7
   - **C.** Windows 8
   - **D.** Windows 8.1
3. Which of the following allows Windows 8 clients to automatically connect to the closest remote access server?
   - **A.** DirectAccess
   - **B.** Web Application Proxy cluster
   - **C.** Site-to-site VPN
   - **D.** Multisite remote access

4. What feature allows you to create a highly available remote access solution?
   - **A.** Remote access cluster using NLB
   - **B.** RADIUS server groups
   - **C.** Web Application Proxy clusters
   - **D.** Site-to-site VPN
5. What capabilities are provided by RADIUS server groups?
   - **A.** Distribution of the authentication workload
   - **B.** The ability to remotely access internal web applications using devices that are not domain joined
   - **C.** Automatic connection to the nearest remote access entry point
   - **D.** Enforcement of network policies prior to establishing a remote access connection

Objective 3.5: Design and implement a network protection solution

The NPS role includes features that allow you to authenticate clients attempting to connect to the network and enforce policies prior to allowing clients to fully access the corporate network. There are several aspects of implementing a network protection solution, including deploying NPS, managing network policies, creating a remediation network, choosing an enforcement method, and configuring network clients.

One aspect of network protection is NAP, a feature that allows clients to be evaluated for health before being allowed to connect to the network. NAP is deprecated in Windows Server 2012 R2, so the functionality is still fully supported for both Windows Server 2012 R2 and Windows 8.1, but will likely be removed in future product versions. Microsoft recommends using its System Center Configuration Manager to perform health policy enforcement and remediation going forward.

As with any security measure in your network, NPS can result in significant network issues if misconfigured, even to the point of lost network connectivity. Proper planning, testing, and a phased implementation are highly recommended.

This objective covers how to:

- Configure NAP enforcement methods for DHCP, IPSec, VPN, and 802.1x
- Plan capacity
- Plan for server placement
- Understand firewall considerations
- Deploy Network Policy Server (NPS)
- Create a remediation network
- Configure NAP enforcement for IPsec and 802.1x
- Monitor for compliance

Configuring NAP enforcement methods

NAP can be a powerful tool for network protection because it enables you to evaluate network clients based on health criteria such as antivirus definitions, software updates, and firewall configuration. Two things must be in place for this enforcement to occur: NAP client software on the client computer and an enforcement method used to refer network clients to the NPS.

The NAP client on Windows computers can be managed in several ways. The NAP Client Configuration MMC snap-in can be accessed by entering **NAPCLCFG.MSC** at the Run prompt. (The NAP Client Configuration window is shown in Figure 3-21.) NAP clients for domain member computers can also be configured using Group Policy, which is always the preferred method for multiple computers in an enterprise environment. Finally, the NETSH command-line tool allows you to configure NAP client enforcement using NETSH NAP CLIENT. Each enforcement method used on your network must be enabled within the NAP client, and the Network Access Protection Agent service must be started for NAP enforcement to perform correctly.

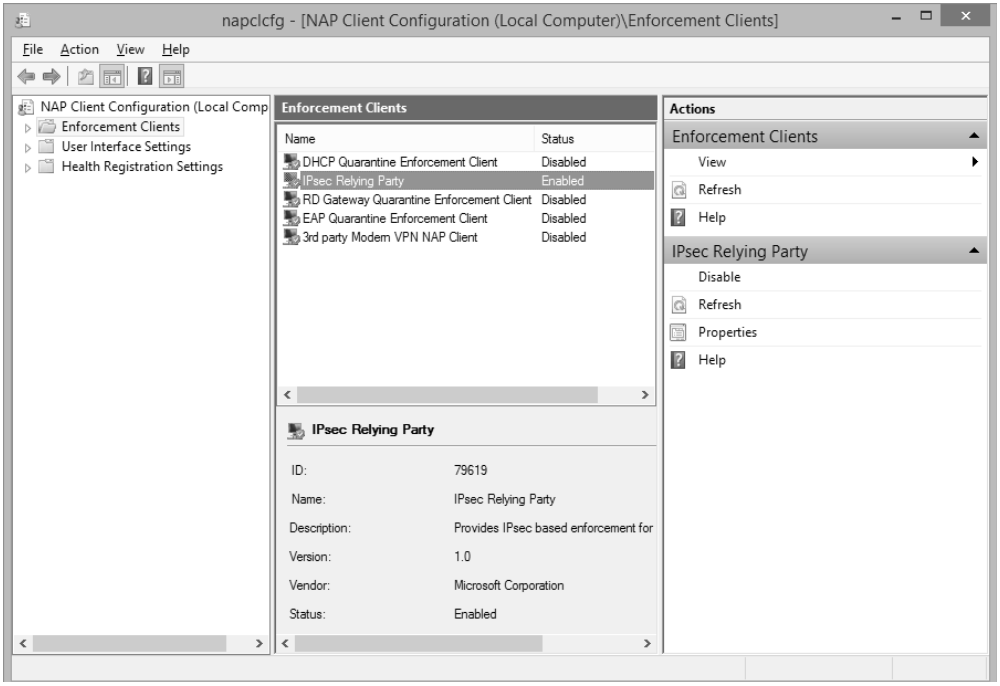

FIGURE 3-21 The NAP Client Configuration console allows you to enable individual enforcement clients and configure user interface settings shown during the NAP enforcement process

NAP policies are enforced by segregating clients that do not meet the health policies of the network, as well as those that cannot be validated, from computers that meet the health policies. Each enforcement method handles this segregation in a different way, but the common thread is that each method is capable of performing or facilitating a health evaluation prior to giving the client access to the network.

DHCP

DHCP servers using Windows Server can be used to provide NAP enforcement for DHCP clients if the server also performs the NPS role. The NPS role can either perform authentication locally or be configured as a RADIUS proxy to forward requests to the NPS performing the authentication. NAP enforcement can be enabled for individual DHCP scopes or for all scopes configured on the DHCP server.

DHCP is a weak NAP enforcement method because it can only prevent clients from gaining an IP address through DHCP. Network clients with a static IP address or an automatically configured IP address such as an automatic private IP address (APIPA) or IPv6 autoconfiguration can still access the network.

IPsec

IPsec, along with 802.1x, is one of the preferred methods of NAP enforcement of internal network clients. Enforcement occurs by configuring computer certificate issuance so that only computers that meet the requirements of the network policy receive a computer certificate, which enables communication with other computers on the network. When used as a NAP enforcement method, the IPsec client configuration must be configured to require IPsec for all network traffic. Only computers placed in the remediation network should be allowed to communicate to clients without using IPsec. As with NAP client enforcement, Group Policy can be used to configure IPsec policies on domain-joined computers.

NAP enforcement using IPsec requires heavy use of Active Directory Certificate Services (AD CS), including the capability to automatically issue computer certificates. The IPsec enforcement method also uses the Health Registration Authority (HRA), which is installed as a feature. The HRA must also be an NPS, either performing authentication or forwarding requests to an authenticating NPS.

VPN

Remote access clients can be evaluated by NAP and NPS when initiating a remote access connection to the corporate network. The NPS role must be installed on the remote access server and can be configured to operate as a RADIUS proxy or to handle authentication requests locally. When using the VPN NAP enforcement, the Extensible Authentication Protocol (EAP) enforcement method must be enabled on the NAP client.

NAP enforcement of VPN clients can be configured in conjunction with a corporate PKI using Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS) or EAP-TLS with AD CS.

802.1x

Unlike other NAP enforcement methods, 802.1x relies on physical networking hardware such as switches and wireless access points to initiate RADIUS authentication and health evaluation. These network hardware devices are configured as RADIUS clients during policy configuration. The result is that having 802.1x-capable networking hardware is a requirement for using this enforcement method. In the 802.1x enforcement method, noncompliant network clients are segregated from healthy computers, either through IP filtering or VLANs. Similar to VPN-based enforcement, NAP clients must be configured to use the EAP enforcement method. 802.1x enforcement can also work with your corporate PKI using EAP-TLS, or PEAP-TLS and AD CS.

EXAM TIP

Even though NAP is deprecated in Windows Server 2012 R2, it is still covered on the exam. At a minimum, you need to know the enforcement methods, what they require, and how they segregate compliant from noncompliant computers.

Designing an NPS infrastructure

The design of your NPS infrastructure is critical for high availability and performance reasons. Authentication traffic can be routed through your network using RADIUS proxies, and high availability for authentication can be managed using RADIUS server groups. The NAP infrastructure must include remediation of noncompliant computers, ideally offering a path to update antivirus signatures or to acquire system updates.

Planning capacity

There are several aspects of your NPS infrastructure that should be evaluated and monitored for performance problems. Each step in the health evaluation and authentication process should be assessed to ensure optimal performance.

Enforcement servers for the DHCP, IPsec, and VPN enforcement methods should be analyzed to ensure that the additional workload from NAP enforcement does not affect their capability to respond to client requests. In the case of DHCP and VPN, high-availability options for those services can be used to distribute the workload across additional resources. In the case of IPsec enforcement, the HRA server should be monitored to ensure that it can respond to health certificate requests in a timely manner. Enforcement servers can be configured to perform validation or forward the authentication request to a RADIUS server group (see Figure 3-22).

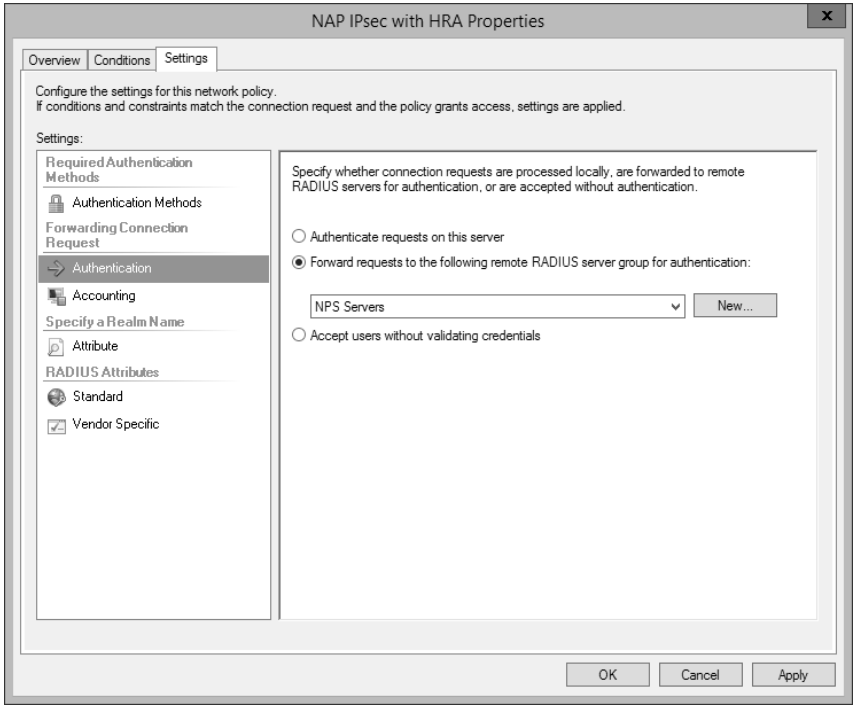

FIGURE 3-22 By configuring the network policy on a NAP enforcement server, you can forward authentication requests to a RADIUS server group of your choosing

NAP health policy servers can be load balanced using RADIUS server groups, as shown in Figure 3-23, which allows you to distribute RADIUS authentication requests to multiple NPS servers on your network. Load balancing allows you to set priority and weight values to manage the distribution of the authentication workload and to configure the circumstances under which a RADIUS server should be considered unavailable.

Capacity should be a consideration for remediation servers such as Windows Server Update Servers (WSUS). Many criteria determine the load for remediation servers, including the number of clients, the level of enforcement, and whether the same servers are used to update compliant and noncompliant computers.

Planning for server placement

Regardless of the NAP enforcement method, some network services must be available to both compliant and noncompliant computers. Health policy servers must be able to accept authentication requests from clients, but must also be able to authenticate users and computers to an Active Directory domain controller.

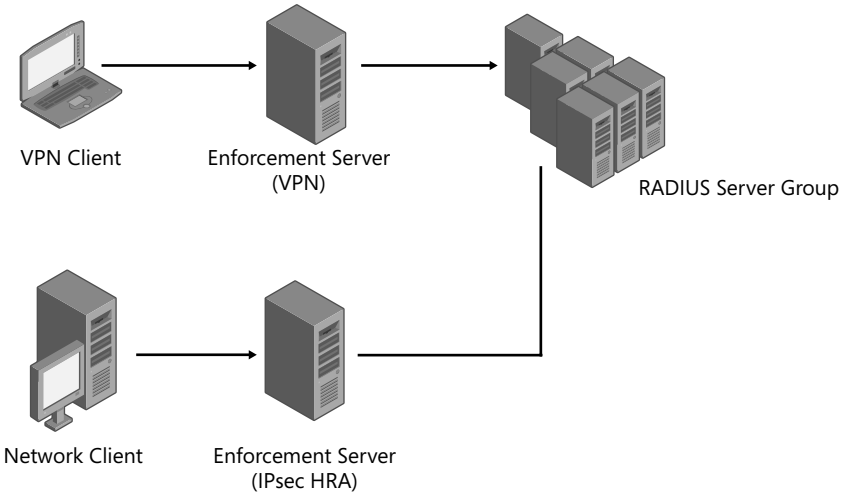

FIGURE 3-23 RADIUS server groups can be used to provide improved performance and fault tolerance for authentication traffic

Enforcement servers such as DHCP, VPN, or HRA servers must be able to communicate with all clients, regardless of policy compliance. Servers used for remediation are not required to be able to communicate across compliance levels, but having separate update mechanisms adds unnecessary complexity to your network.

Understanding firewall considerations

The Windows Firewall should automatically create exceptions for ports used by NPS and RADIUS traffic, including User Datagram Protocol (UDP) ports 1812, 1813, 1645, and 1646.

Other firewalls external to NPS servers have to be configured to allow these ports through to the server for authentication to occur.

Deploying a Network Policy Server (NPS)

The primary piece in a network protection infrastructure is one or more NPS servers, which forward RADIUS authentication requests, analyze authentication requests for compliance, and manage the policies used to determine compliance. NPS policies and enforcement can be initiated using the Configure NAP Wizard. Each of the three policy types can also be created or modified manually by editing the properties of individual policies, as shown in Figure 3-24.

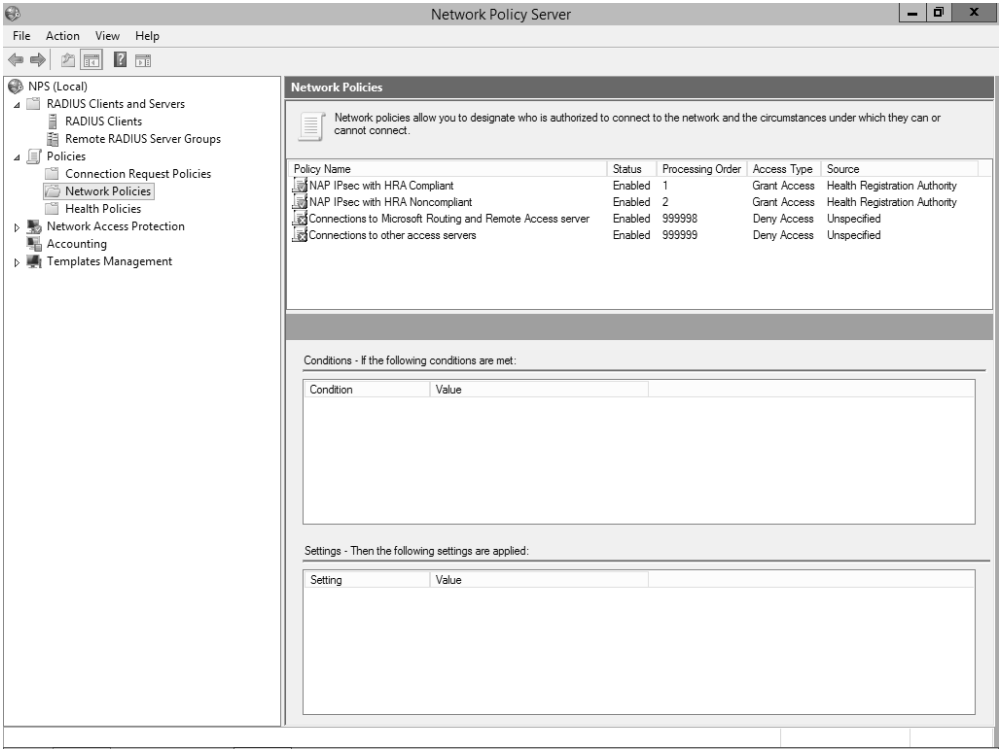

FIGURE 3-24 Policies can be manually edited by modifying their properties in the Network Policy Server management console

Connection Request Policies allow you to identify and route incoming authentication traffic, choose the enforcement method and other criteria such as time or IP address range, and then either forward to another RADIUS server to perform the authentication or handle it internally.

Network Policies determine whether clients meet the requirements to be authenticated and allowed into the network. NAP clients are evaluated by their health, resulting in the client being allowed or denied network access.

The final policy type configured on the NPS is the Health Policy, which is used to refer to one or more system health validators (SHVs). Only the default Windows SHV (shown in Figure 3-25) is included with NPS in Windows Server 2012, but third-party SHVs can be integrated and enforced. The Windows SHV allows you to evaluate configuration and status of Windows updates, antimalware protection, and the Windows Firewall.

FIGURE 3-25 The Windows Security Health Validator is the only SHV provided by default

Creating a remediation network

With NAP and NPS, you can provide limited network connectivity to noncompliant network clients. This connectivity can be used to prevent access to sensitive systems and healthy clients, or as a remediation network to provide a way to become compliant with network policies (see Figure 3-26).

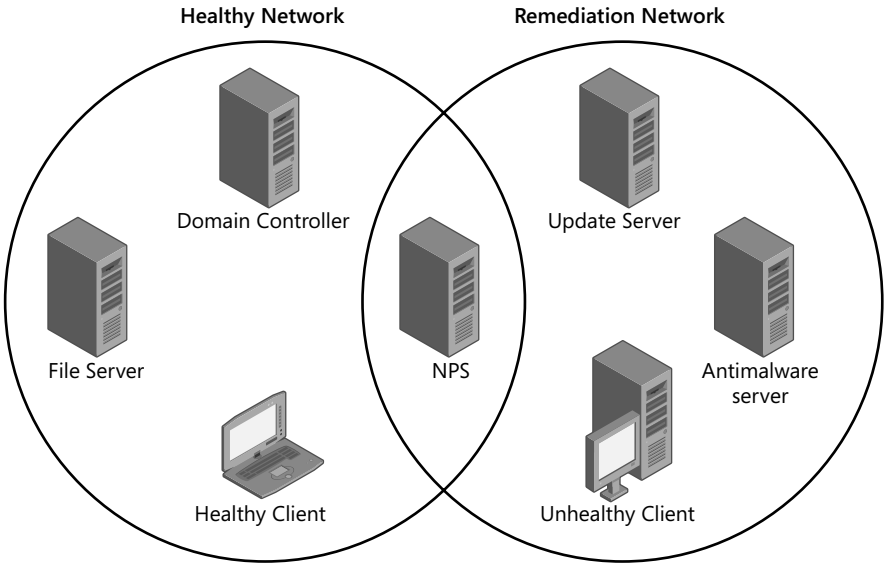

FIGURE 3-26 A remediation network provides a way for unhealthy computers to join the healthy network

To allow noncompliant computers to access servers offering system or antivirus updates, some additional configuration of these servers is needed to prevent network traffic from being blocked. The method to enable this network traffic through depends on the enforcement method used, but it can be as easy as assigning a static IP address (for DHCP enforcement) or configuring less-restrictive IPsec policies using a GPO.

Configuring NAP enforcement for IPsec and 802.1x

For enforcing NAP compliance on an internal network, there are only two recommended enforcement options. IPsec enforces compliance through the use of IPsec policies that require computer certificates to authenticate network communication. 802.1x enforces NAP at the network hardware level, assigning computers to different VLANs based on client health. Both of these solutions are strong options for protecting your network, but the configuration of each option is quite different.

Enforcing IPsec

The core of the IPsec enforcement method includes configuring computer certificate autoenrollment and IPsec policies using Group Policy. The next step is to configure the NPS server with the appropriate policies. The NAP policies configured within the NPS determine which clients are issued certificates. Figure 3-27 shows a healthy client requesting a certificate

from a CA, which is also the HRA. In this scenario, the HRA forwards the authentication request to another NPS, which validates the client's health, and the HRA issues the certificate. After the client receives the certificate, it can then communicate with the file server using IPsec authenticated using the computer certificate.

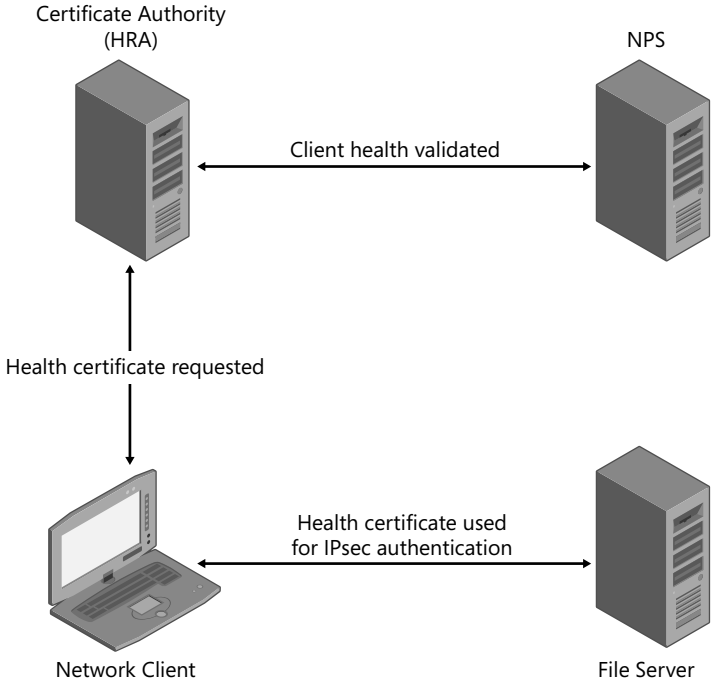

FIGURE 3-27 The IPsec enforcement method relies heavily on computer certificates that are used to facilitate IPsec authentication between healthy computers; computers that cannot be validated do not receive certificates and cannot communicate with healthy computers

To configure IPsec enforcement on your NPS, launch the Configure NAP Wizard and choose the IPsec With Health Registration Authority (HRA) option. The next page allows you to identify remote HRA servers as RADIUS clients. If the same server is performing both HRA and NPS roles, you can skip this step. The Configure Machine Groups page allows you to specify security groups containing computers to which the policy will apply. To enforce NAP on all computers, leave the Machine Groups list empty. The final step of enforcing NAP policies using IPsec is to choose the SHVs to use for enforcement and determine whether clients are automatically remediated when possible. Figure 3-28 shows a fully configured network policy, enforcing NAP using IPsec.

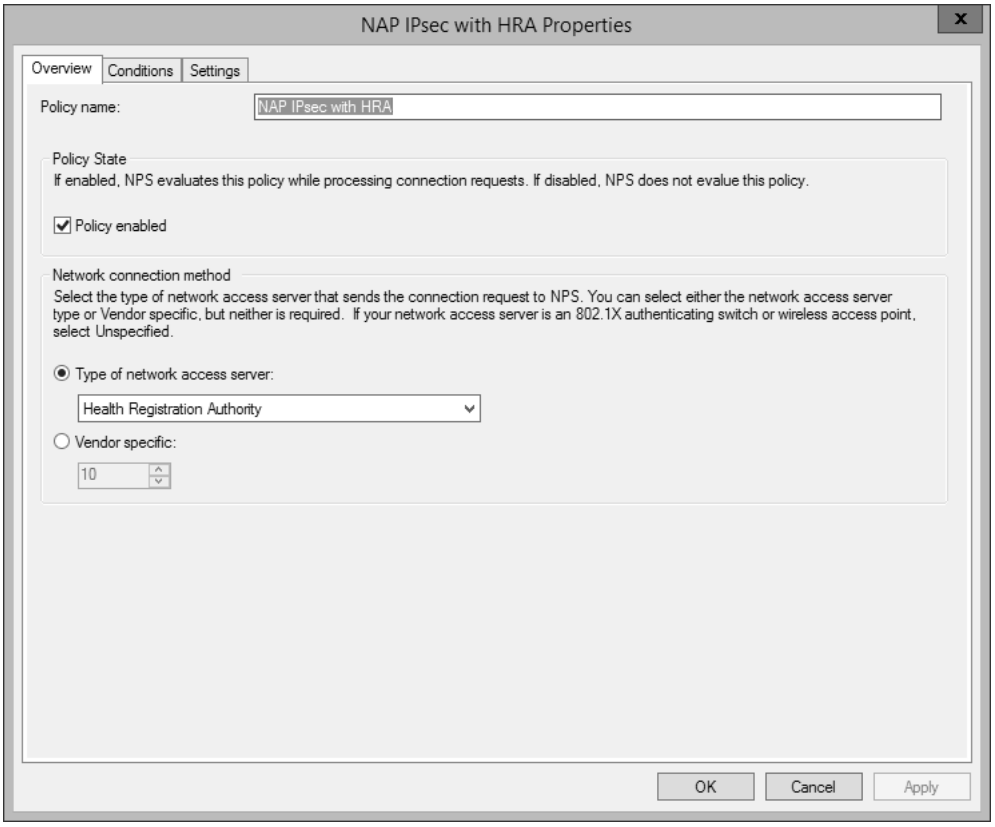

FIGURE 3-28 The IPsec enforcement method uses the Health Registration Authority network access server

Enforcing 802.1x

For NAP enforcement, 802.1x wired and wireless enforcement are configured separately. The Configure NAP Wizard allows you to choose one type of 802.1x client to configure before continuing with the wizard (see Figure 3-29). Regardless of the network connection, the remainder of the wizard is the same for both wired and wireless clients.

The second page of the Configure NAP Wizard requires you to identify RADIUS clients. For wired 802.1x configuration, this list should include 802.1x authenticating switches; for wireless networks, you have to list 802.1x wireless access points. On the Configure User Groups And Machine Groups page, you can identify groups of users or computers that should be authenticated using 802.1x. NAP enforcement using 802.1x uses PEAP for authentication, which can be configured by choosing a server certificate and EAP type in the Configure An Authentication Model page.

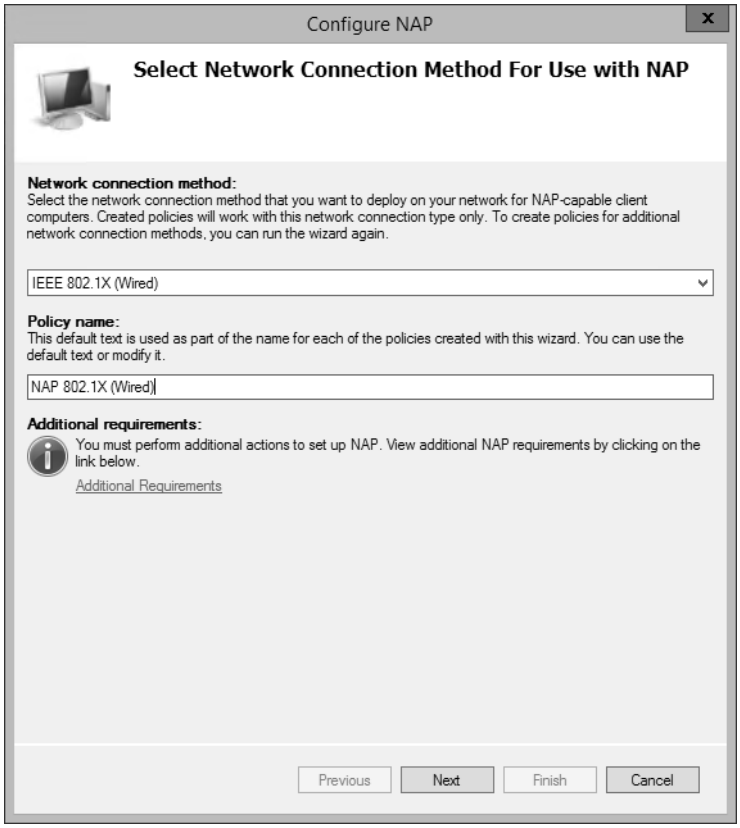

FIGURE 3-29 802.1x enforcement of NAP must be configured individually for wired and wireless clients

Traffic controls are used by 802.1x to segregate traffic between compliant and noncompliant systems. There are several options that can be used for traffic control, some of which are dependent on the vendor of your networking hardware. Finally, you can configure the SHVs to be used to determine compliance with the corporate health policy. You can also configure how to handle clients that do not support NAP, either by allowing them full access to the network or restricting them to a restricted network.

Figure 3-30 shows the 802.1x authentication process at work. When the network client first makes a physical connection to the 802.1x switch, an authentication request is passed to the NPS. After the client health is validated, the switch places the network client on the corporate VLAN, allowing it to communicate to the file server.

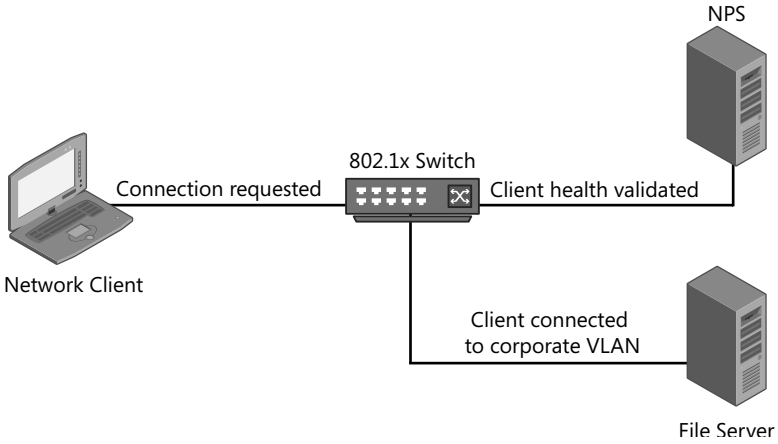

FIGURE 3-30 The 802.1x enforcement method uses VLANs or IP filtering to segregate healthy computers from those that do not meet the health requirements

Monitoring for compliance

One aspect of NAP that should be considered either as a long-term solution or part of the testing phase is the ability to configure NAP in logging-only mode. In this configuration, clients are not restricted from gaining access to the network, but their compliance status is monitored and logged. Logging-only mode allows you to ensure that clients are being validated properly prior to fully enforcing NAP policies.

NAP logging, also known as RADIUS accounting, can be configured to write to a file on the local hard drive or to a Microsoft SQL Server database (which can be configured in the Accounting options). Another vital configuration step is to determine what action should be performed if the NPS cannot write to a log file, specifically whether incoming connection requests should be discarded or allowed.

Thought experiment

Enforcing network protection

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

Your corporation is interested in ramping up the security of its network. NPS and NAP have been identified as possible tools to improve the overall security of the network, but much is undecided as far as an implementation strategy. You will make recommendations based on answers to the following questions:

1. **What aspects of your corporate infrastructure should be evaluated to determine which enforcement methods should be used?**
2. **If capacity becomes a concern due to the size of the corporate network, what methods are available to handle a large number of authentication requests?**
3. **Is there any way to offer noncompliant computers a method to achieve compliance with network policies without exposing healthy computers to potential network security risks?**

Objective summary

- NPS supports four enforcement methods, DHCP, IPsec, VPN, and 802.1x.
- RADIUS, a standard protocol used for network authentication, is used with NPS to enforce authentication policies, including client health.
- Because DHCP enforcement can be easily bypassed through the use of a static IP address, it is not recommended for use in secure environments.
- IPsec enforcement uses policies requiring certificate-based authentication to prevent noncompliant computers from connecting with compliant systems.
- VPN connections can use network protection to ensure that remote computers meet local network policies.
- The 802.1x enforcement method uses techniques such as IP filtering or VLANs to segregate network traffic.
- RADIUS proxy and RADIUS server groups can be used to manage the authentication workload by spreading requests across multiple servers.

- NPS servers should be placed in network locations that perform NAP enforcement, specifically VPN servers or an HRA.
- Network and host-based firewalls must be configured to allow RADIUS authentication traffic to pass.
- The NPS server functions as a RADIUS server, authenticating clients and performing policy validation.
- A remediation network can be implemented to assist clients in taking the corrective actions necessary to achieve full connectivity to the network.
- IPsec and 802.1x enforcement are the preferred options for internal corporate networks. IPsec uses computer certificate–based authentication to segregate network traffic. The 802.1x enforcement method uses network infrastructure devices to route authentication traffic to a RADIUS server for validation, and separates clients using VLANs or IP filtering.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which is the weakest NAP enforcement method?
   - **A.** DHCP
   - **B.** IPsec
   - **C.** VPN
   - **D.** 802.1x
2. What authentication standard is performed by an NPS?
   - **A.** 802.1x
   - **B.** RADIUS
   - **C.** IPsec
   - **D.** VPN
3. What enforcement method uses compatible networking hardware?
   - **A.** DHCP
   - **B.** IPsec
   - **C.** VPN
   - **D.** 802.1x

4. What enforcement method uses computer certificates to restrict network communication between clients?

   A. DHCP

   B. IPsec

   C. VPN

   D. 802.1x

5. What types of servers would typically be contained in a remediation network? (Choose all that apply.)

   A. Windows Server Update Server

   B. Active Directory domain controller

   C. Corporate file server

   D. Antimalware update server

6. What type of enforcement server is specifically used with the IPsec enforcement method?

   A. HRA

   B. RADIUS

   C. DHCP

   D. NPS

Answers

This section contains the solutions to the thought experiments and answers to the lesson review questions in this chapter.

Objective 3.1: Thought experiment

1. Site-to-site VPN connections allow you to connect remote locations to the same logical network.
2. An internal enterprise CA is used to allow automatic enrollment for computer certificates to facilitate IPsec authentication on a network.
3. The required firewall rules depend on the infrastructure and its configuration. DirectAccess uses IP-HTTPS on port 443, the 6to4 protocol uses port 41, the network location server uses port 62000, and IPv6 uses TCP port 50 and UDP port 500.
4. Web Application Proxy enables you to allow remote clients to connect to web applications on the internal network. Web Application Proxy makes use of AD FS and supports PKI, OTP, and multifactor authentication.

Objective 3.1: Review

1. **Correct answer:** B
   - A. **Incorrect:** Public CAs provide certificates for public-facing applications, not internal computers.
   - B. **Correct:** An enterprise CA enables you to configure your certificates to allow computers to automatically enroll, making possible the process of configuring IPsec using computer certificates.
   - C. **Incorrect:** A stand-alone CA lets you create certificates for use on the internal network, but does not allow you to use autoenrollment of computer certificates.
   - D. **Incorrect:** Remote access servers are not required to use IPsec authentication.
2. **Correct answer:** A
   - A. **Correct:** Port 1701 is used by L2TP traffic.
   - B. **Incorrect:** PPTP uses port 1723.
   - C. **Incorrect:** HTTPS traffic uses TCP port 443.
   - D. **Incorrect:** Port 80 is used by standard HTTP traffic.

3. **Correct answer:** C

   A. **Incorrect:** Site-to-site VPN allows disparate locations to connect into a single logical network.

   B. **Incorrect:** Multisite VPN allows Windows 8 clients to connect to the optimal remote access server in your organization.

   C. **Correct:** Multitenant site-to-site VPN allows hosting providers to create virtual networks for individual clients, ensuring that they are connected only to the network segment containing their applications.

   D. **Incorrect:** Azure virtual networks offer similar functionality to multitenant site-to-site VPNs, but not on-premises datacenters.

4. **Correct answer:** B

   A. **Incorrect:** PPTP uses MPPE.

   B. **Correct:** 3DES is supported only by L2TP/IPsec.

   C. **Incorrect:** SSTP uses SSL to encrypt its tunnel.

   D. **Incorrect:** Only L2TP/IPsec supports 3DES.

5. **Correct answer:** C

   A. **Incorrect:** PPTP supports certificate-based authentication, but not smart cards.

   B. **Incorrect:** L2TP/IPsec also uses certificates for authentication, but smart cards are not supported for authentication.

   C. **Correct:** Smart card authentication is supported using SSTP.

   D. **Incorrect:** Of the traditional VPN protocols supported in Windows Server 2012, only SSTP supports authentication with smart cards.

6. **Correct answer:** A

   A. **Correct:** Because SSTP uses port 443, which is rarely blocked by network firewalls, it is the best solution for traversing NAT devices.

   B. **Incorrect:** SSTP provides strong security for both authentication and encryption, as does L2TP/IPSec.

   C. **Incorrect:** PPTP provides the best performance of the traditional VPN protocols.

   D. **Incorrect:** SSTP requires Windows 7 clients or later, whereas both PPTP and L2TP/IPsec support older client operating systems.

7. **Correct answer:** A
   A. **Correct:** Local DNS servers are not part of the Azure virtual network creation process, but they can be used by resources contained within the Azure virtual network.
   B. **Incorrect:** On-premises IP address pools are one aspect of the Azure virtual network creation process.
   C. **Incorrect:** Azure virtual networks allow you to define subnets within your local network.
   D. **Incorrect:** The VPN server IP address is part of the site-to-site VPN creation process.
8. **Correct answer:** C
   A. **Incorrect:** CMAK does not affect user permissions for VPN.
   B. **Incorrect:** Remote access servers are deployed using the Add Roles And Features Wizard and the Remote Access Management Console.
   C. **Correct:** CMAK is used to create VPN profiles that are easy for end users to deploy on their own computers.
   D. **Incorrect:** Site-to-site VPN connections with Azure are created using the new virtual network creation wizards in Azure.
9. **Correct answer:** A
   A. **Correct:** CMAK is installed through the RAS Connection Manager Administration Kit (CMAK) feature.
   B. **Incorrect:** CMAK does not need to be downloaded from the Microsoft website.
   C. **Incorrect:** The Windows Server 2012 installation media do not contain the CMAK setup files.
   D. **Incorrect:** CMAK is not installed by default on either Windows 8 or Windows Server 2012.

Objective 3.2: Thought experiment

1. DirectAccess can be configured for remote access and remote management, or just for remote management.
2. The DirectAccess Client Setup Wizard allows you to select security groups containing users that should be allowed to connect remotely, whereas the DirectAccess Application Server Setup page is used to select security groups containing application servers to which these users should be allowed to connect.

3. Migration from Forefront UAG DirectAccess to Windows Server 2012 DirectAccess can be accomplished side-by-side or in offline mode. A side-by-side migration allows you to continue to service DirectAccess clients throughout the process, but requires some duplication of DNS records and IP addresses during the migration. Both methods require configuration of the new remote access server and relevant GPOs.

Objective 3.2: Review

1. **Correct answers:** B, C
   - A. **Incorrect:** An edge topology is used when the remote access server has a direct connection to the Internet.
   - B. **Correct:** The option for behind an edge device (with two network adapters) can be used when a NAT device is used on the network.
   - C. **Correct:** When a NAT device is providing address translation, the option for behind an edge device (with one network adapter) can be used.
   - D. **Incorrect:** NAT has no relation to DirectAccess for remote management.
2. **Correct answers:** A, B
   - A. **Correct:** Force tunnel mode requires configuration using the Remote Access Setup Wizard.
   - B. **Correct:** Two-factor authentication is not supported when DirectAccess is configured using the Getting Started Wizard.
   - C. **Incorrect:** The wizard used to configure DirectAccess has no impact on the placement of the DirectAccess server.
   - D. **Incorrect:** Either configuration option supports DirectAccess for remote management only.
3. **Correct answers:** A, D
   - A. **Correct:** OTP is a new feature for authentication in DirectAccess on Windows Server 2012.
   - B. **Incorrect:** Smart card authentication was supported in previous versions of DirectAccess.
   - C. **Incorrect:** Authentication using a user name and password have always been supported for remote access.
   - D. **Correct:** Using Trusted Platform Modules, Virtual Smart Cards are a new feature in DirectAccess for Windows Server 2012.

4. **Correct answer:** B

   A. **Incorrect:** IPv6 support is not required for migration of DirectAccess from Forefront UAG to Windows Server 2012.

   B. **Correct:** Forefront UAG SP1 must be installed before migration of DirectAccess can occur.

   C. **Incorrect:** A PKI is not a requirement for migration of DirectAccess from Forefront UAG to Windows Server 2012.

   D. **Incorrect:** Because Windows Server 2012 does not require public IPv4 addresses, additional public addresses are not required.

5. **Correct answer:** D

   A. **Incorrect:** In a side-by-side migration of DirectAccess, IP addresses and FQDNs cannot be reused because both DirectAccess servers must be connected to the network at the same time.

   B. **Incorrect:** Side-by-side migration and offline migration do not support automated migration.

   C. **Incorrect:** New certificates must be issued in a side-by-side migration because the FQDN of the DirectAccess server changes.

   D. **Correct:** No downtime is required in a side-by-side DirectAccess migration from Forefront UAG to Windows Server 2012.

6. **Correct answer:** B

   A. **Incorrect:** A PKI is required for Windows 7 clients to connect to DirectAccess, but it does not enable support for OTP.

   B. **Correct:** The DirectAccess Connectivity Assistant 2.0 is required for Windows 7 clients to use OTP for DirectAccess authentication.

   C. **Incorrect:** A RADIUS server is required to support the use of OTP, but it does not enable support for Windows 7 clients.

   D. **Incorrect:** Windows 7 SP1 does not bring OTP support to Windows 7 DirectAccess clients.

7. **Correct answer:** D

   A. **Incorrect:** Using certificates from a public CA is not practical for client computer certificates.

   B. **Incorrect:** Computer certificates, even for servers, are best served by an internal enterprise CA.

   C. **Incorrect:** The network location can use a certificate from a public CA, but an internal CA is supported, provided that the CRL is accessible.

   D. **Correct:** It is recommended to use an SSL certificate from a public CA for the IP-HTTPS server because some remote access clients might not be domain joined.

Objective 3.3: Thought experiment

1. Workplace Join allows you to support Web Application Proxy while still requiring a device registration process. Workplace Join is supported only on Windows 8.1 and iOS devices at this time.
2. Although SSO is supported with Web Application Proxy, it requires AD FS.
3. Certificates from a public CA are required for both the Web Application Proxy and AD FS.

Objective 3.3: Review

1. **Correct answer:** A
   - **A. Correct:** Web Application Proxy requires an AD FS server, and uses AD FS heavily for authentication and authorization.
   - **B. Incorrect:** Although ultimately AD DS contains the security principals used to authenticate users and computers, AD FS is the service that performs the authentication requests against AD DS for the Web Application Proxy.
   - **C. Incorrect:** Certificates are used extensively with Web Application Proxy, but AD CS does not perform authentication.
   - **D. Incorrect:** AD FS Proxy is the precursor to Web Application Proxy.
2. **Correct answer:** D
   - **A. Incorrect:** Domain membership is not a requirement for client access through a Web Application Proxy.
   - **B. Incorrect:** Workplace Join can be configured as an authentication requirement for access to applications through a Web Application Proxy, but it is not mandatory.
   - **C. Incorrect:** Windows 8.1 is one of the supported operating systems for Workplace Join, but is not required to use Web Application Proxy.
   - **D. Correct:** Web Application Proxy supports clients that have a web browser, Microsoft Office application, or compatible Windows 8.1 app.
3. **Correct answer:** C
   - **A. Incorrect:** AD FS preauthentication requires authentication prior to the client being referred to the application.
   - **B. Incorrect:** SSO is used by Web Application Proxy to allow users to authenticate once, but this is still handled by the Web Application Proxy, not the application.
   - **C. Correct:** Pass-through authentication forwards users to the application they have requested without performing any authentication at the Web Application Proxy level.
   - **D. Incorrect:** Multifactor access control is performed at the Web Application Proxy level.

4. **Correct answers:** A, C

   A. **Correct:** Workplace Join allows supported nondomain devices to be registered with the AD DS using the DRS within AD FS.

   B. **Incorrect:** Workplace Join does not support all device types; only Windows 8.1 and iOS devices are supported.

   C. **Correct:** Registration with AD DS is required for Workplace Join.

   D. **Incorrect:** Workplace Join cannot be used to verify that clients meet network security policies.

5. **Correct answers:** B, C

   A. **Incorrect:** Windows 8 does not support Workplace Join.

   B. **Correct:** Devices using iOS support Workplace Join.

   C. **Correct:** Windows 8.1 clients can be registered using Workplace Join.

   D. **Incorrect:** Registration of UNIX devices using Workplace Join is not supported.

6. **Correct answer:** D

   A. **Incorrect:** SSO allows users to maintain a session after authenticating once.

   B. **Incorrect:** Workplace Join does not allow you to conditionally require smart cards for authentication.

   C. **Incorrect:** Multifactor authentication can be configured for all users, but not conditionally without using multifactor access control.

   D. **Correct:** Multifactor access control allows you to create rules for authentication, including the ability to require smart cards for certain groups of users.

7. **Correct answer:** C

   A. **Incorrect:** SSO is supported for any device that can use Web Application Proxy.

   B. **Incorrect:** Client computers do not have to be domain joined to use SSO.

   C. **Correct:** The Web Application Proxy must be domain joined to support SSO.

   D. **Incorrect:** Client devices do not have to be running Windows 8.1 or iOS to support SSO.

8. **Correct answer:** B

   A. **Incorrect:** DNS CNAME records can be created to make the same FQDN resolve to the same host for both internal and external clients, but this is not a function of Web Application Proxy.

   B. **Correct:** URL translation, which is part of the application publishing process in Web Application Proxy, allows both internal and external clients to use the same URL to access applications.

   C. **Incorrect:** Pass-through authentication bypasses authentication at the Web Application Proxy level, but does not affect the URL used to access the application.

   D. **Incorrect:** Workplace Join has no bearing on the URL used to reach a published application.

Objective 3.4: Thought experiment

1. A site-to-site VPN connects multiple corporate locations into the same logical network.
2. Multisite remote access supports clients automatically, discovering the best entry point to connect to remotely.
3. Web Application Proxy can run in a multiserver environment. All configuration information for Web Application Proxy is contained within AD FS, so installing additional servers automatically configures them for this scenario.

Objective 3.4: Review

1. **Correct answer:** B

   A. **Incorrect:** Misconfigured packet filtering on the Internet connection would probably prevent clients from connecting to the remote access server.

   B. **Correct:** Packet filtering on an intranet connection would constrain traffic from the remote access server to internal network resources.

   C. **Incorrect:** Packet tracing only monitors network traffic; it does not restrict network traffic.

   D. **Incorrect:** Packet tracing being disabled would have no effect on remote access.

2. **Correct answer:** C

   A. **Incorrect:** Windows Vista clients cannot use automatic server selection in a multisite DirectAccess.

   B. **Incorrect:** Windows 7 does not support the automatic selection of a DirectAccess server in a multisite deployment.

   C. **Correct:** Windows 8 clients can automatically choose the optimal DirectAccess server with which to connect in a multisite configuration.

   D. **Incorrect:** Windows 8.1 clients fully support multisite DirectAccess autoconfiguration, but it is not the minimum.

3. **Correct answer:** D

   A. **Incorrect:** DirectAccess is the remote access protocol used, but it does not allow this by default.

   B. **Incorrect:** Web Application Proxy in a cluster provides high availability and is not a full remote access solution.

   C. **Incorrect:** Site-to-site VPN allows two or more locations to communicate with each other and does not support client failover.

   D. **Correct:** Windows 8 clients can automatically connect to the best DirectAccess server in a multisite deployment.

4. **Correct answer:** A

   A. **Correct:** NLB allows you to create a highly available remote access solution.

   B. **Incorrect:** RADIUS server groups provide high availability for RADIUS authentication, but not remote access.

   C. **Incorrect:** Web Application Proxy is not a full remote access solution.

   D. **Incorrect:** Site-to-site VPN is used to connect multiple network locations to the same logical network.

5. **Correct answer:** A

   A. **Correct:** RADIUS server groups are used to distribute authentication workload, providing high availability and scalability.

   B. **Incorrect:** Remote access to internal web applications is best served by Web Application Proxy.

   C. **Incorrect:** Automatic connection to the optimal remote access entry point is a function of multisite remote access.

   D. **Incorrect:** Network policy enforcement is a function of NPS and NAP.

Objective 3.5: Thought experiment

1. Enforcement decisions need to be made by determining what enforcement methods are needed and what options are already available. If VPN or DirectAccess are used, the VPN enforcement method is probably needed. The decision between 802.1x and IPsec for the internal network would probably come down to which is easier to manage: the enterprise CA and computer certificates or the 802.1x configuration for network switches and wireless access points.
2. RADIUS server groups can be used to add scale and high availability to your NPS deployment.
3. A remediation network is the best way to provide noncompliant computers the capability to meet the network policies.

Objective 3.5: Review

1. **Correct answer:** A
   - **A. Correct:** DHCP enforcement of NAP can be bypassed by configuring a static IP address, making it the weakest enforcement method by far.
   - **B. Incorrect:** IPsec is a strong enforcement method that uses computer certificates to authenticate network communication.
   - **C. Incorrect:** VPN connections can be enforced effectively by using NPS in conjunction with the remote access server.
   - **D. Incorrect:** The 802.1x enforcement method is a strong enforcement method, effectively segregating network clients into separate logical networks.
2. **Correct answer:** B
   - **A. Incorrect:** 802.1x uses RADIUS authentication provided by the NPS, but does not perform the authentication.
   - **B. Correct:** RADIUS authentication is a standard for network authentication and is performed by the NPS server.
   - **C. Incorrect:** IPsec is not an authentication method.
   - **D. Incorrect:** VPN is not an authentication method.

3. **Correct answer:** D

   A. **Incorrect:** DHCP enforcement uses DHCP request negotiation to segregate computers.

   B. **Incorrect:** IPsec uses computer certificates and IPsec policies to prevent noncompliant computers from communicating with compliant computers.

   C. **Incorrect:** VPN enforcement is done at the remote access server.

   D. **Correct:** 802.1x compatible network hardware can be used to enforce NAP policies.

4. **Correct answer:** B

   A. **Incorrect:** DHCP enforcement provides IP leases so that noncompliant computers cannot communicate with those that are compliant.

   B. **Correct:** IPsec enforcement of NAP uses computer certificates to authenticate compliant computers, allowing them to communicate.

   C. **Incorrect:** NAP enforcement of VPN connections segregates noncompliant computers into their own logical network.

   D. **Incorrect:** Enforcement using 802.1x uses hardware-level networking features such as VLANs or IP filtering.

5. **Correct answers:** A, D

   A. **Correct:** A Windows Server Update Server is typically included on a remediation network to provide system updates to noncompliant computers.

   B. **Incorrect:** An Active Directory domain controller should be protected from vulnerable computers and should not be included in a remediation network.

   C. **Incorrect:** Corporate file servers can contain protected information and should be left on a protected network segment.

   D. **Correct:** Antivirus and other antimalware updates should be provided on the remediation network when possible.

6. **Correct answer:** A

   A. **Correct:** An HRA is the NPS role used to request client health certificates for the IPsec enforcement method.

   B. **Incorrect:** RADIUS servers and the RADIUS authentication protocol are used throughout NAP enforcement, regardless of the method used.

   C. **Incorrect:** The DHCP enforcement method uses DHCP servers to forward authentication requests to the NPS.

   D. **Incorrect:** NPS servers function as RADIUS servers and are used in each enforcement method.

Index

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

This page intentionally left blank

About the authors

PAUL FERRILL has a BS and MS in Electrical Engineering and has been writing in the computer trade press for over 25 years. He serves as CTO for Avionics Test and Analysis Corporation, a woman-owned small business specializing in providing engineering expertise to help solve complex data analysis problems. He's written hundreds of articles over the years for publications like Datamation, Federal Computer Week, Information Week, InfoWorld, Network Computing, Network World, PC Magazine and is the author of two books.

TIM FERRILL is a system administrator and writer living in Southern California with his wife, Jodi, and their five kids. Over the years Tim has written for a number of publications such as WPCentral.com, MaximumPC, and InfoWorld. Tim's love of technology encompasses Windows Server, Windows Phone, scripting, web and graphic design, and gadgets of all shapes and sizes. Tim holds several industry certifications, including the MCSE on Windows Server 2003, the MCITP: Enterprise Administrator on Windows Server 2008, and a Security+ from CompTIA.