Designing, Implementing, and Managing

Security on Windows Server 2012 R2

Includes Real-World Scenarios,
Hands-On Labs and Exercises

Esmaeil Sarabadani

Designing, Implementing, and Managing Security on Windows Server 2012 R2

Esmaeil Sarabadani

Cover Design: Golnar Shishehgaran

First published: September 2014

About the Author

Esmaeil Sarabadani is a technology professional with numerous years of experience managing small to global scale IT infrastructure projects for multiple companies. Since the very first days he got his personal computer, he found an interest in the field of information security and began his exploration in gaining more knowledge in this area. Since then, he has worked in different companies as a system and security consultant and is currently working as a project manager on global projects implementing Microsoft latest technologies and systems.

Esmaeil is an active conference speaker and has given deep-dive technical talks in many well-known Microsoft events and conferences on the topic of security. As a Microsoft Certified Trainer for more than four years, he provided training on the latest IT courses in the market and coming from that background he decided to write his first technical book dedicated thoroughly to the topic of security on the latest Windows server platform.

TABLE OF CONTENTS

CREATING AND DEPLOYING SECURITY POLICIES USING SECURITY CONFIGURATION WIZARD (SCW)

CONFIGURATION ACTION
SECURITY CONFIGURATION DATABASE
ROLE-BASED SERVICE CONFIGURATION

Server Roles
Client Features
Administration and Other Options
Additional Services
Handling Unspecified Services

NETWORK SECURITY

Windows Firewall with Advanced Security

REGISTRY SETTINGS

Require SMB Security Signatures
Require LDAP Signing
Outbound Authentication Methods

AUDIT POLICY

WHAT'S NEW IN SERVICE ACCOUNTS

GROUP MANAGED SERVICE ACCOUNTS
EXERCISE: CONFIGURING GROUP MANAGED SERVICE ACCOUNTS

USER ACCOUNT CONTROL

USER ACCOUNT CONTROL MECHANISM
USER ACCOUNT CONTROL MODES
EXERCISE: CONFIGURING USER ACCOUNT CONTROL

LAB 1-B: CONFIGURING SECURITY ON WINDOWS SERVER 2012 R2

Exercise 1: Creating and applying security policies using Security Configuration Wizard
Exercise 2: Configuring Enhanced Mitigation Experience Toolkit (EMET)

LAB 1-B ANSWERS: CONFIGURING SECURITY ON WINDOWS SERVER 2012 R2

Exercise 1: Creating and applying security policies using Security Configuration Wizard
Exercise 2: Configuring Enhanced Mitigation Experience Toolkit (EMET)

CHAPTER 2: CONFIGURING FILE ACCESS AUTHORIZATION AND ENCRYPTION

OVERVIEW OF NTFS PERMISSIONS
IMPLEMENTING AND CONFIGURING NTFS PERMISSIONS

ACCESS CONTROL LIST (ACL), ACCESS CONTROL ENTRY (ACE)

Adding and Removing NTFS Permissions for users/Groups
Advanced Permissions

Cumulative Permissions
NTFS Permissions Inheritance
Files/Folders Ownership
Effective Access

EXERCISE: CONFIGURING NTFS PERMISSIONS

OVERVIEW OF SHARE PERMISSIONS
BEST PRACTICES ON COMBINING NTFS AND SHARE PERMISSIONS

EXERCISE: COMBINING NTFS AND SHARE PERMISSIONS

OVERVIEW OF ENCRYPTING FILE SYSTEM (EFS)

PRIVACY
EFS OPERATION
DATA RECOVERY

Private Keys Location

IMPLEMENTING AND CONFIGURING ENCRYPTING FILE SYSTEM (EFS)

HOW EFS IS USED AND OPERATED
CIPHER COMMAND-LINE UTILITY
BACK UP AND RESTORE ENCRYPTED FILES
DISABLE EFS
EXERCISE: CONFIGURING ENCRYPTING FILE SYSTEM

LAB 2-A: CONFIGURING FILE ACCESS AUTHORIZATION AND ENCRYPTION ON WINDOWS SERVER 2012 R2

Exercise 1: Configuring and combining NTFS and Share permissions
Exercise 2: Performing Encrypting File System (EFS) Recovery

LAB 2-A ANSWERS: CONFIGURING FILE ACCESS AUTHORIZATION AND ENCRYPTION

Exercise 1: Configuring and combining NTFS and Share permissions
Exercise 2: Performing Encrypting File System (EFS) Recovery

INTRODUCTION TO BITLOCKER
IMPLEMENTING BITLOCKER ON SERVERS

BITLOCKER COMMAND-LINE TOOLS AND WINDOWS POWERSHELL CMDLETS

Manage-bde
Repair-bde

BITLOCKER WINDOWS POWERSHELL CMDLETS
EXERCISE: CONFIGURING BITLOCKER ON WINDOWS SERVER 2012 R2
BACKING UP BITLOCKER OR TPM RECOVERY KEY IN ACTIVE DIRECTORY DOMAIN SERVICES

LAB 2-B: CONFIGURING BITLOCKER DRIVE ENCRYPTION AND RECOVERY

Exercise 1: Backing up/Restoring BitLocker recovery information to/from Active Directory

Lab 2-B Answers: Configuring BitLocker Drive Encryption and Recovery

Exercise 1: Backing up/Restoring BitLocker recovery information to/from Active Directory

CHAPTER 3: IMPLEMENTING DEFENSE IN DEPTH

Introduction to Designing Perimeter Networks

Planning and Designing Security for Perimeter Networks

DMZ Design Objectives
Basic Design (Three-Legged Firewall)
Moderate Design (Back-to-Back Firewalls)
Advanced Design (Back-to-Back and Three-Legged Firewalls)

Planning and Implementing Active Directory Domain Services in Perimeter Network

No Active Directory Domain Services
Isolated Forest Model
Extended Forest
Forest Trust Model

DNS Security on Windows Server 2012 R2

Overview of DNSSEC
DNSSEC Mechanism
NSEC3 and Authenticated Denial-of-Existence
DNSSEC Key Management

Key Signing using DNSSEC
Key Signing Key (KSK)
DNSSEC on the Client Side
Name Resolution Policy Table

DNS Security Common Practices

Zone Transfer Restriction
Secure Dynamic Updates
Global Query Block List
Discretionary Access Control List (DACL)
Socket Pool
Cache Locking
DNS Server Interface Restriction
Disabling Recursion
Zone Transfer using IPSec
Exercise: Configuring Security for DNS on Windows Server 2012 R2

Introduction to IPSec

Traffic Filtering
End-to-End Transmission Security

Securing the Traffic Passing through Network Address Translator (NAT)
Secure Servers
L2TP over IPSec (L2TP/IPSec)
Site-to-Site IPSec Tunneling with Non-Microsoft IPSec Gateways

IPSec Operation Modes

Tunnel Mode
Transport Mode

IPSec Encryption Methods

Encapsulating Security Payload (ESP)
Authentication Header (AH)

Introduction to Defense in Depth
Overview of Domain and Server Isolation Model
Planning and Implementing Domain and Server Isolation

Isolation Scope

Hosts to be isolated
Servers to be isolated
Firewalls

Planning Phase
Deployment Phase

Things to consider when designing domain and server isolation
Risks that cannot be mitigated

Exercise: Configuring IPSec Policy using Group Policies

Overview of Windows Firewall with Advanced Security

Firewall Types

Network Firewalls
Host-Based Firewalls
Location-aware host-based firewalls

New Functionalities in Windows Server 2012/2012 R2
Exercise: Configuring Windows Firewall with Advanced Security

Lab 3: Configuring Defense in Depth

Exercise 1: Configuring IPSec policies
Exercise 2: Configuring security for DNS

Lab 3 Answers: Configuring Defense in Depth

Exercise 1: Configuring IPSec policies
Exercise 2: Configuring security for DNS

CHAPTER 4: IMPLEMENTING AND CONFIGURING NETWORK POLICY AND ACCESS SERVICES

OVERVIEW OF NETWORK POLICY AND ACCESS SERVICES

NETWORK POLICY SERVER (NPS)
HEALTH REGISTRATION AUTHORITY (HRA)
HOST CREDENTIAL AUTHORIZATION PROTOCOL (HCAP)
NEW AND CHANGED FUNCTIONALITIES IN WINDOWS SERVER 2012 R2

INTRODUCTION TO NETWORK POLICY SERVER (NPS)

RADIUS SERVER
RADIUS PROXY
NETWORK ACCESS PROTECTION (NAP)
EXERCISE: INSTALLATION AND BASIC CONFIGURATION OF NETWORK POLICY AND ACCESS SERVICES ON WINDOWS SERVER 2012 R2

CONFIGURING NETWORK POLICY SERVER (NPS)

UDP Port Configuration on NPS
Disabling NAS Notification Forwarding
Exporting and Importing NPS Configuration
Registering an NPS Server in another Domain
Creating and Using Templates in NPS
Managing RADIUS Clients
Managing Network Policies
Rules Processing Order
VLAN Configuration for Remote Users on NPS
Managing Accounting

EXERCISE: CONFIGURING NETWORK ACCESS SERVER AND NETWORK POLICY SERVICE

INTRODUCTION TO NETWORK ACCESS PROTECTION (NAP)

EXERCISE: CONFIGURING NAP INTEGRATION WITH DHCP

LAB 4: IMPLEMENTING AND CONFIGURING NETWORK POLICY AND ACCESS SERVICES

Exercise 1: Configuring VPN and Network Policy and Access Services
Exercise 2: Configuring and Integrating VPN with Network Access Protection

LAB 4 ANSWERS: IMPLEMENTING AND CONFIGURING NETWORK POLICY AND ACCESS SERVICES

Exercise 1: Configuring VPN and Network Policy and Access Services
Exercise 2: Configuring and Integrating VPN with Network Access Protection

CHAPTER 5: IMPLEMENTING DYNAMIC ACCESS CONTROL

INTRODUCTION TO DYNAMIC ACCESS CONTROL ON WINDOWS SERVER 2012 R2
OVERVIEW OF FILE CLASSIFICATION INFRASTRUCTURE (FCI)

FILE SERVER RESOURCE MANAGER

Exercise: Configuring security on Hyper-V

APPENDIX

LAB PREPARATION

Sample Lesson

Introduction to Designing Perimeter Networks

Perimeter network, also known as the DMZ (Demilitarized Zone), is one of the most critical parts of the network infrastructure which is more than any other parts exposed to the Internet. As the name suggests, it is a specific zone placed between the internal network and the Internet providing services to users from outside the company network.

Any company or organization has remote users, remote offices, customers and partners who may need to access services offered internally. The availability of these services is vital to the type of business these companies provide and that is why they need to be always accessible. The perimeter network is in fact a section in the network where these services reside. The servers hosting such services are in most cases assigned public IP addresses. A server with a public IP address can be easily accessible from the Internet. In fact a server with a public IP address is part of the Internet with the difference that it is only placed behind the company's firewall boundary. The firewall boundary helps protect the services from all sorts of attacks coming from the Internet.

Services placed in DMZ are mostly critical and need to be always available for people inside and outside the network. An important point here is even if specific services are not placed in DMZ, there might be connections to them from the services in DMZ. An example here is a domain controller which we might not prefer to place in DMZ but almost any service is dependent on it for authentication and authorization of their users.

There are different designs of the perimeter network depending on your network infrastructure and the ultimate goal of a proper design is to never put security at stake for the sake of availability and also never underestimate the possibility of security threats imposed on your whole internal infrastructure in case your DMZ is penetrated. In this chapter, different scenarios will be discussed to help you design a secure and reliable perimeter network.

Planning and Designing Security for Perimeter Networks

In the previous section of this chapter, you got an idea of what DMZ is and why we need it. Today with this fast growth of networks and with different types of services offered to users, it is no more the question of whether we need a DMZ but more the question of how we need to design it. There are different approaches in designing the DMZ but it takes a great amount of smartness and creativity to create a really secure design. Having mentioned that, there are still rules and goals to follow to make sure the basic requirements are met.

DMZ Design Objectives

The main goal in designing a reliable DMZ, as mentioned before, is the segmentation of services, devices, systems and, of course data in your network based on the risk. So before going about the design, one thing to make sure about is to really well classify the importance of such resources in your network and also identify up to which level each of the services needs to be accessible. This actually means whatever services, systems or data which will be placed in your DMZ will need to be segregated by the operating system, data classification schemes, trust levels or business unit. You need to know the risk imposed on the services in DMZ, internal network and in general the whole company if one of your services were attacked. With this analysis, you will have a good understanding of how many layers of security your DMZ will require in order to protect your critical services and data. For instance, in most designs you can see the web application and the database are separated and placed in different segments in the DMZ. Now let's have a closer look at different DMZ designs:

Basic Design (Three-Legged Firewall)

This design, which is unfortunately quite popular among network engineers, is the most basic way of implementing your perimeter network. In this design, you will use a single firewall as the only secure gateway to both your perimeter and internal networks. The firewall is connecting on one side to your internal LAN and on the other two sides to your perimeter and external networks. The downside of having such a design is first of all you have one single point of protection which, if successfully penetrated, will not only put the servers in DMZ at stake but also your internal network and all your confidential data on your internal servers. It is never suggested to have one single firewall protecting your whole infrastructure.

The other problem with such a design is that your internal network is only one hop away from the Internet. In simple words, in case of an intrusion of the firewall, attackers would easily access your internal LAN and servers. Illustration 3.1 below shows what a three-legged firewall design looks like:

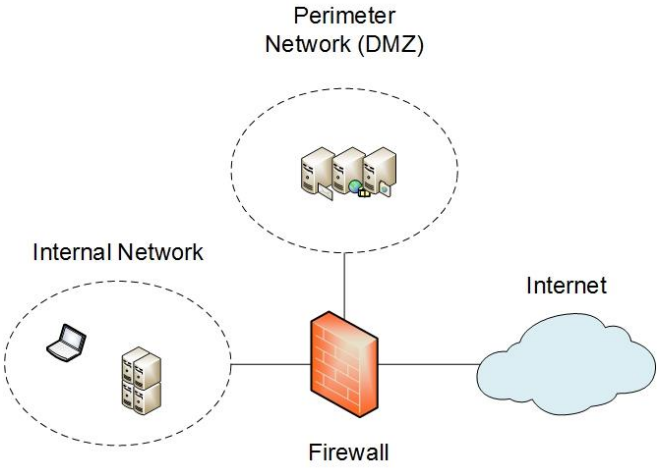

Illustration 3.1: Three-Legged Firewall Design

There is also another variation to our basic design where we will have only one firewall but in a slightly different setup. In this design, there will be multiple DMZ zones connected to the firewall and the firewall will no more be connected to only three networks. Depending on the criticality of the services in DMZ, they are placed in different zones. In this design, none of the aforementioned problems with the three-legged firewall will be tackled as they are almost similar in design but it will bring some more benefits to make it a better choice when it comes to a very basic design.

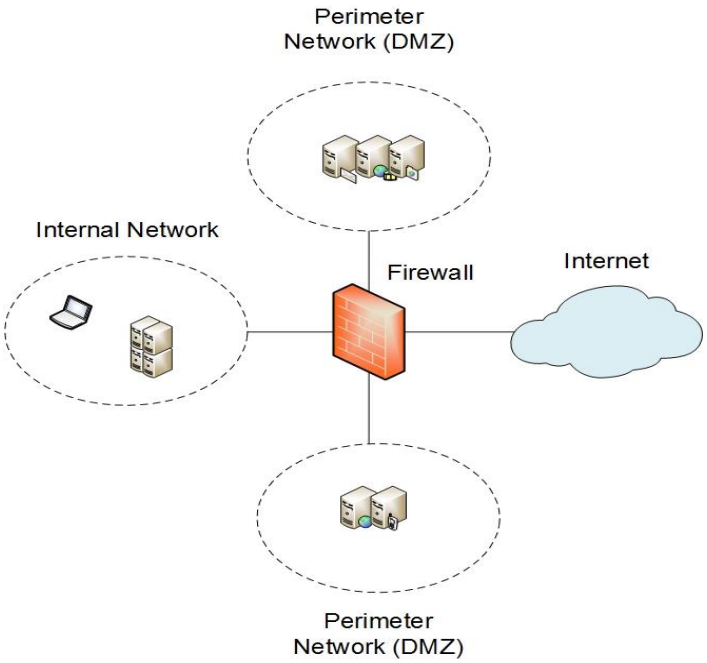

Illustration 3.2: Basic Firewall Design

One of the benefits is the segregation of services even in the DMZ. With such separation, you could configure the firewall in a way that only specific requests are routed to the critical DMZ zone while the other zone is open to all sorts of requests from the Internet. This design can also be of great benefit when it comes to the communication of the servers in the DMZ with the ones in the internal network. You can place the servers that do not need to communicate with the internal hosts in a separate zone and remove any network routes set on the firewall between that zone and the internal network. In this way, you will be reducing the risk of access to your internal network through your DMZ zone.

As mentioned before, to a large extent, it depends on how creative you are with your design and how efficiently you can reduce the risk of penetration into your network. Another downside to this variation of firewall design could come from the complexity that might exist when you have a lot of static routes defined on your firewall. This could potentially complicate troubleshooting and lead to mistakes.

Moderate Design (Back-to-Back Firewalls)

In this design we will have an added layer of protection to our internal network as well as DMZ by adding one more firewall. In the back-to-back firewall scenario, we will have more flexibility since we can connect our one or multiple DMZ zone(s) to one of the two firewalls and create more advanced setups. However in this section we will not go deep into more advanced implementations and we will just cover an ordinary setup of a back-to-back firewall design.

In a back-to-back firewall scenario, as the picture below shows, there is a firewall which on one side is directly connected to the internet and on the other side is connected to a second firewall. The second firewall then connects the perimeter network to the internal network. As it is clear in illustration 3.3, the perimeter network is placed between the two firewalls where all the servers which need to be publicly accessible are located.

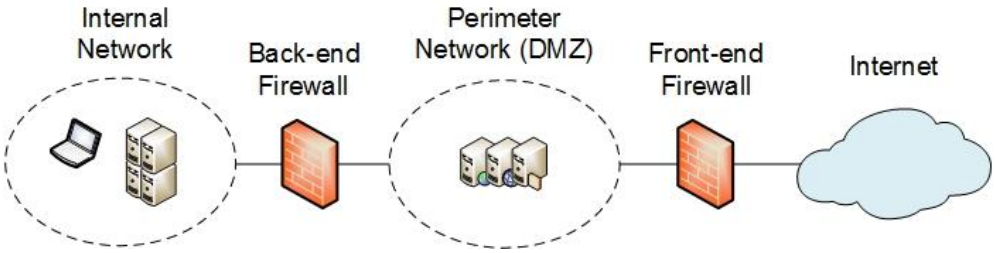

Illustration 3.3: Back-to-Back Firewall Design

The advantage this design has over the basic DMZ design is the fact that the internal network is two hops away from the internet and therefore there are two layers of protection guarding the internal network against possible attacks. The DMZ itself is also behind the first firewall protecting it from any possible intrusion. For any sort of communication between the DMZ servers and the internal hosts, static routes can be created on the back-end firewall. This design

is more tolerant to mistakes and is very popular and widely-practiced in many networks around the world.

Advanced Design (Back-to-Back and Three-Legged Firewalls)

Now that you have a solid understanding of the previous two designs, we can dig a bit deeper into a more advanced DMZ setup which combines the three-legged and back-to-back firewall implementations. The idea behind this design is to place both the internal and perimeter networks behind two firewalls. In the simple back-to-back firewall model discussed previously, the perimeter network was defined in the area between the two firewalls but in this new design we still keep the back-to-back setup the same way it was, however we will use our back-end firewall in a three-legged design connected to the internal network on one side and to the DMZ on the other side and finally its third adapter connects it to the front-end firewall.

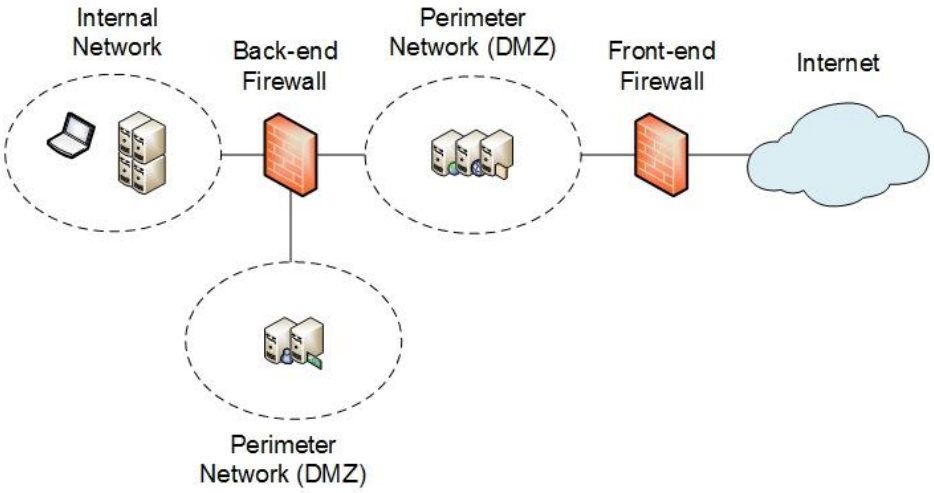

Illustration 3.4: Advanced Firewall Design

This design is very secure because firstly we have two firewalls protecting our DMZ and internal network and secondly we are flexible in creating even more advanced setups. One of the best techniques used to mislead attackers is creating honeypots and placing them in a segment connected directly to the front-end firewall. Honeypots are fake replicas of the production servers placed somewhere on the network and they are used to confuse attackers by making them think they are the production servers so that they will spend plenty of their time working on penetrating into these servers. As the picture below shows, the network segment between the two firewalls is the best place for placing the honeypot servers and in case intruders manage to break in to the first firewall, they only manage to get to the honeypot servers and it gives you more time to detect the attack and get them off your network.

Planning and Implementing Active Directory Domain Services in Perimeter Network

In this section, we will discuss the deployment of Active Directory within perimeter network or DMZ. Many people believe deploying Active Directory in perimeter network is not the right decision because of the security risks which could be potentially imposed on the organization's directory service. In this section we will discuss different deployments of Active Directory in perimeter network. Below is an illustrated and descriptive list of different designs:

No Active Directory Domain Services

This simply means that we do not create any connectivity between the directory service in the network and any of the other services. You may prefer using the servers' SAM (Security Accounts Manager) database file which stores the local user and group accounts but that creates management inconvenience. There are many other disadvantages such a design could bring about like the lack of security and central management and, so more.

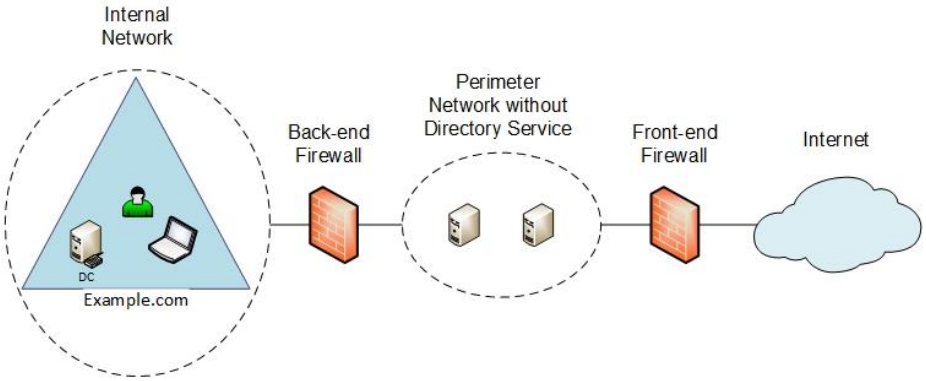

Illustration 3.5: Perimeter Network without Directory Service

Isolated Forest Model

As illustration 3.6 shows, it is possible to create two separate Active Directory forests for the internal and the perimeter networks. In this way we have the directory service in the perimeter network but it is still isolated from the rest of the network meaning that any update on the directory services in the internal network such as adding or modifying user accounts, will not affect the directory services in the perimeter network and vice versa. And the disadvantage with this design is that you need to place a writable domain controller of the perimeter forest in the perimeter network, so there is always a risk the Domain Controller could get penetrated. A disadvantage to this design is that there is no connectivity between the forests and if the domain users in the internal network require access to any of the resources in the perimeter network, it is not possible to give them such an access since there is no connectivity between the forests.

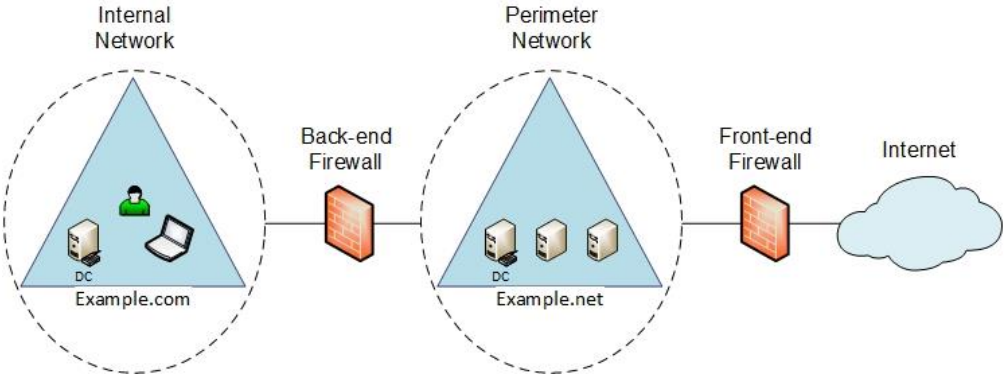

Illustration 3.6: Perimeter Network Design – Isolated Forest

Extended Forest

In this design there will be one single forest covering both the internal and the perimeter networks. If you place a writable Domain Controller in the perimeter network, any changes by a hacker on the DC could be replicated to all the other DCs inside the internal network.

The good choice is using an RODC (Read-Only Domain Controller) inside the perimeter network which is in replication with the DCs inside the internal network. This way if by any chance one of the DCs in the DMZ is at risk of getting penetrated, the data is not at risk of getting changed and then replicated to the entire domain or forest.

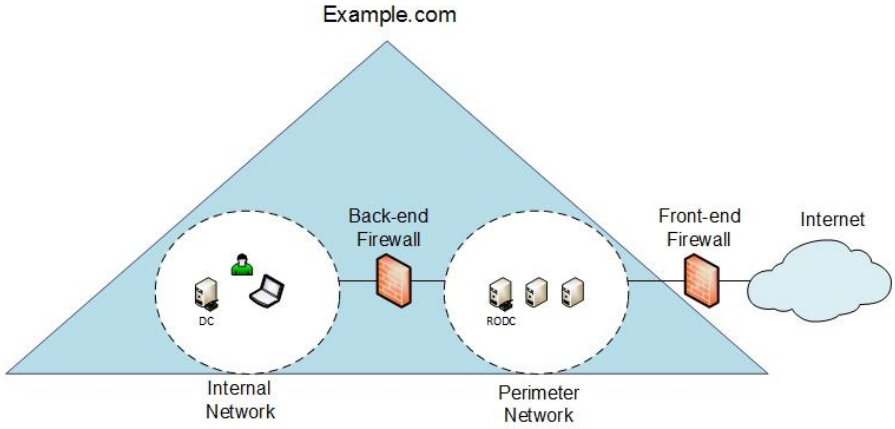

Illustration 3.6: Perimeter Network Design – Isolated Forest

Below are some of the benefits of placing Read-Only Domain Controllers in the DMZ:

- Reducing the attack surface by placing an RODC instead of a writable domain controller.
- Giving directory service to applications that require access to Active Directory and are located in the perimeter network
- Decreasing the type of the traffic passing from the DMZ to the LAN and vice versa

You have to keep in mind that the clients and member servers running in the perimeter network need to be Windows Vista and Windows Server 2008 and above, otherwise a hotfix called RODC compatibility pack needs to be applied to them. You can download the hotfix from here.

Forest Trust Model

This is one of the best designs where there is a separate forest for both the perimeter and the Internal networks just like the Isolated Forest Model but there is a forest trust between the two.

The trust could be unidirectional meaning that we can only let the internal users access the resources inside the perimeter network. For example, if you have a SQL server in your perimeter network and you want both your internal and external users to access it, you could follow this model to have two forests and make a unidirectional trust between them making the server in the DMZ accessible to the internal users but still preventing the outside users in the perimeter network to access any resources inside the internal network. A drawback to this model is the administration cost of two different forests.

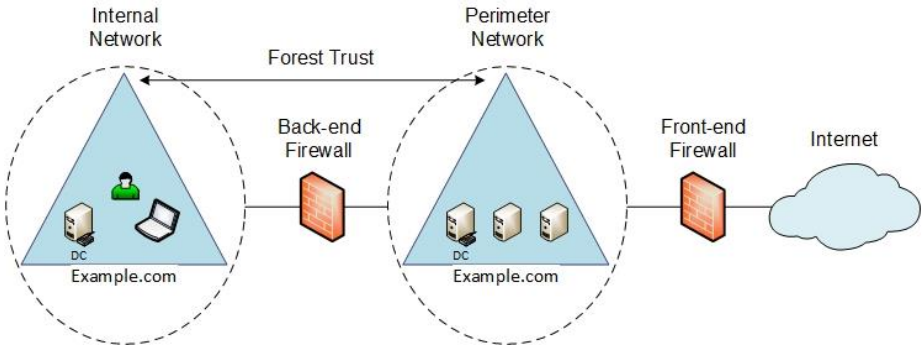

Illustration 3.7: Perimeter Network Design – Forest Trust

Sample Exercise

Exercise: Configuring Security for DNS on Windows Server 2012 R2

Exercise 1.1

In this exercise you will learn how to configure secure dynamic updates and also zone transfers for a zone on a Windows Server 2012 R2 DNS server:

1. Log on to **Example-Server01** using the following credentials:
- Username: **Example.com\Administrator**
- Password: **P@ssw0rd**
2. On the **Start** screen type **DNS** and press **Enter**.
3. Expand **Example-Server01** and right click **Forward Lookup Zones** and click **New Zone** to open the **New Zone Wizard**.
4. On the **Welcome to the New Zone Wizard** page, click **Next**.
5. On the **Zone Type** page, select **Secondary zone** and click **Next**.
6. On the **Zone Name** page, type **Example.com** in the **Zone name** textbox and click **Next**.
7. On the **Master DNS Server** page, in the **Master Servers** box type **Example-DC01** and click **Next**.
8. On the **Completing the New Zone Wizard** page, click **Finish**.
9. Log on to **Example-DC01** using the following credentials:
- Username: **Example.com\Administrator**
- Password: **P@ssw0rd**
10. On the **Start** screen type **DNS** and press **Enter**.
11. On the **DNS Manager** Console tree expand **Example-DC01** > **Forward Lookup Zones** and right click **Example.com** and click **Properties**.
12. On the **Example.com Properties** window select the **Zone Transfers** tab.
13. Check the box next to **Allow zone transfers** and then click **Only to servers listed on Name Servers tab.**
14. Select the **Name Servers** tab and click **Add**.
15. On the **New Name Server Record** window, type **Example-Server01.Example.com** for the **Server fully qualified domain name (FQDN)** and click **Resolve** and then **OK** twice.
16. Go back to **Example-Server01** and right click **Example.com** zone and click **Transfer from Master**.
17. Right click again on the **Example.com** zone and click **Refresh** and all the transferred records will be visible.
18. Go back to **Example-DC01** and right click the **Example.com** zone and click **Properties**.
19. Select the **General** tab and at the bottom of the window, click the drop-down menu next to **Dynamic updates** and select **Secure only**.
20. Click **OK** to close the **Example.com Properties** window.

Exercise 1.2

In this exercise you will learn how to enable and update the global query block list on a Windows Server 2012 R2 with the DNS service installed:

1. Log on to **Example-DC01** using the following credentials:
- Username: **Example.com\Administrator**
- Password: **P@ssw0rd**
2. Open a **command prompt** window and type the following command and press **Enter** to enable the global query block list:

```
Dnscmd Example-DC01.Example.com /config /enableglobalqueryblocklist 1
```

3. Type the following command and press **Enter** to update the global query block list with the specified hostname:

```
Dnscmd Example-DC01.Example.com /config /globalqueryblocklist wpad.Example.com
```

4. Type the following command and press **Enter** to see the global query block list:

```
Dnscmd Example-DC01.Example.com /info /globalqueryblocklist
```

Exercise 1.3

In this exercise you will learn how to enable cache locking, disable recursion and configure a DNS socket pool on a Windows Server 2012 R2 with the DNS service installed:

1. Log on to **Example-DC01** open a **command prompt** window and type the following command and press **Enter** to enable cache locking:

```
Dnscmd /config /CacheLockingPercent 100
```

Note: Cache locking is configured as a percent value. For example, if it is configured as 50, then the DNS server will not overwrite a cached entry for half of the duration of the TTL. The default value is 100.

2. Type the following command and press **Enter** to disable recursion:

```
Dnscmd Example-DC01.Example.com /config /NoRecursion 1
```

3. Type the following command and press **Enter** to configure a **socket pool size of 5000** with an **excluded port range of 1-1500**:

```
Dnscmd /config /SocketPoolSize 5000
Dnscmd /config SocketPoolExcludedRanges 1-1500
```

Sample Lab Scenario

w/ Answers

Lab 4: Implementing and Configuring Network Policy and Access Services

In these lab exercises we will configure different components of Network Policy and Access services and will learn how to integrate them with the other services in our environment. Through the exercises in this lab you will acquire a deep knowledge and understanding on how to strengthen security in your environment using Network Policy and Access services.

Objectives

After completing this lab, you will be able to:

- Understand the different components of Network Policy and Access services
- Configure network policies to restrict access to the network
- Configure Network Access Protection
- Integrate the remote access server with Network Access Protection

Prerequisites

The following virtual machines are necessary to complete this lab:

- Example-DC01
- Example-Server01
- Example-Server02
- Example-Client01

Exercise 1: Configuring VPN and Network Policy and Access Services

Scenario

You are working as a security consultant in a consulting firm based in Kuala Lumpur. The company has hundreds of consultants working for them and some of them work also on international projects which requires them to travel abroad. While working for customers in different countries, these consultants require access to the company network to access files and reports saved on the file servers. Some of these reports are very confidential and apart from the security and access permissions set on the file servers, the company needs to ensure any remote connection to the network is secured and only specific people with specified requirements are able to connect to the network and access the resources.

The security team has been assigned the task of securing remote access connections to the network and for this purpose the team has decided to implement Network Policy and Access services.

Exercise Overview

In this exercise you will need to perform following four tasks:

- Task 1: Configure a VPN server for the network

1. Log on to **Example-Server02** using the following credentials:
   - Username: **Example.com\Administrator**
   - Password: **P@ssw0rd**
2. Configure **Routing and Remote Access Service** to work as a remote VPN server.
3. Redirect the authentication traffic to **Example-Server01** which will be configured in Task 2 as a RADIUS server.

- Task 2: Create a new Active Directory group for remote access users

1. Log on to **Example-DC01** using the following credentials:
   - Username: **Example.com\Administrator**
   - Password: **P@ssw0rd**
2. Create two new Active Directory groups named **Example-Remote-Access-Users** and **Example-Remote-Access-Computers.**
3. Add the Active Directory user **Mikem** to the group **Example-Remote-Access-Users**.

- Task 3: Configure a RADIUS server and network policies

1. Log on to **Example-Server01** using the following credentials:
   - Username: **Example.com\Administrator**
   - Password: **P@ssw0rd**
2. Create a shared folder named **Example_Reports** to contain sample reports and documents.
3. Configure **Network Policy and Access Services** on **Example-Server01** to work as a RADIUS server and serve requests sent from **Example-Server02**.

4. Create **network policies** to grant access to users with the following requirements:

- Users must be a member of Active Directory **Example-Remote-Access-Users** group.
- Users must be able to connect to the network **on any day** and **at any time** during the 24 hours.
- Users must only use **MS CHAP v2** authentication method.
- Users must be allowed **full network access**.

➢ Task 4: Configure clients to connect to network using VPN

1. Log on to **Example-Client01** using the following credentials:

- Username: **Example.com\Mikem**
- Password: **P@ssw0rd**

2. Change the IP address on **Example-Client01** to be in the same range with the external network interface of **Example-Server02**.
3. Create a **VPN connection** to connect to **Example-Server02** and ensure **MS CHAP v2** has been specified as the authentication method.
4. Try accessing the **Example_Reports** shared folder on **Example-Server01**.

Exercise 2: Configuring and Integrating VPN with Network Access Protection

The company needs to add an additional layer of security to their remote access users by implementing Network Access Protection. The security team needs to ensure remote VPN computers' health status is validated using Network Access Protection and Protected Extensible Authentication Protocol (PEAP) is used as the authentication method. This requires the existence of a Certificate Authority (CA) to issue the required certificates.

Exercise Overview

In this exercise you will need to perform following four tasks:

- Task 1: Configure a VPN server for the network

1. Log on to **Example-Server02** and configure **Routing and Remote Access Service** to work as a remote VPN server.
2. Redirect the authentication traffic to **Example-Server01** which will be configured as a RADIUS server.
3. Ensure **Protected Extensible Authentication Protocol (PEAP)** is used as the authentication method.

- Task 2: Configure the Certificate Authority (CA) server and issue PEAP certificate

1. Log on to **Example-DC01** and create a new **certificate template** for the remote access server and ensure the right security permissions are set on the template.
2. Create a new Active Directory group named **Example-Remote-Access-Computers** and add **Example-Client01** to it.

- Task 3: Configure Network Access Protection and create network policies

1. Log on to **Example-Server01** and request and **install a new certificate** on **Example-Server01** from the certificate template created in task 2.
2. Configure **Network Access Protection** to integrate with the VPN server (**Example-Server02**)
3. Configure **Protected Extensible Authentication Protocol (PEAP)** to be used as the main method to authenticate remote clients.
4. Ensure the following requirements are considered when creating network and health policies:

- **Only NAP-capable client computers** are able to connect to network.
- Client is **NAP VPN compliant** only if **it passes all the SHV (System Health Validation) checks**.
- Client is **NAP VPN noncompliant** if **it fails one or more SHV checks**.
- Ensure **Windows System Health Validator** includes the following setting:
- A **firewall** is enabled for all network connections.

- Task 4: Configure clients to connect to network using VPN

1. Log on to **Example-DC01** and create a new GPO named **Clients NAP Policy** at the domain level and apply it only to the members of **Example-Remote-Access-Computers**.
2. Edit the **Clients NAP Policy** GPO to enable **EAP Quarantine Enforcement Client** on the GPO.
3. Log on to **Example-Client01** and create a **VPN connection** to connect to **Example-Server02**.
4. Ensure **Protected Extensible Authentication Protocol (PEAP)** is selected as the authentication method and also **Network Access Protection** is enforced.
5. Enable **Windows Firewall** on **Example-Client01** and try connecting to the network using the VPN connection.
6. Try the same while **Windows Firewall** is **disabled**.

Lab 4 Answers: Implementing and Configuring Network Policy and Access Services

Exercise 1: Configuring VPN and Network Policy and Access Services

➢ Task 1: Configure a VPN server for the network

1. Log on to **Example-Server02** using the following credentials:
- Username: **Example.com\Administrator**
- Password: **P@ssw0rd**
2. Open the **Start** screen, type **Routing and Remote Access** and press **Enter**.
3. On the **Routing and Remote Access** console, right click **Example-Server02** on the left pane and click **Disable Routing and Remote Access** to remove the configuration from the last exercises.
4. Right click **Example-Server02** again on the left pane and click **Configure and Enable Routing and Remote Access**.
5. On the **Welcome to the Routing and Remote Access Server Setup Wizard** page, click **Next**.
6. On the **Configuration** page, leave **Remote access (dial-up or VPN)** selected and click **Next**.
7. On the **Remote Access** page, select **VPN** and click **Next**.
8. On the **VPN Connections** page, click **Ethernet 2** and click **Next**.
9. On the **IP Address Assignment** page, select **From a specified range of addresses** and click **Next**.
10. On the **Address Range Assignment** page, click **New** and on the **New IPv4 Address Range** window enter a range within the internal IP address range. i.e. 192.168.0.30-192.168.0.45 and then click **Next**.
11. On the **Managing Multiple Remote Access Servers** page, select **Yes. Set up this server to work with a RADIUS server** and click **Next**.
12. On the **RADIUS Server Selection** page, enter **Example-Server01.Example.com** as the **Primary RADIUS server** and **$har3d$3cr3t** as the **Shared secret** and click **Next**.
13. Click **Finish** to finish the configuration.

➢ Task 2: Create a new Active Directory group for remote access users

1. Log on to **Example-DC01** using the following credentials:
- Username: **Example.com\Administrator**
- Password: **P@ssw0rd**
2. Open the **Start** screen and type **Active Directory Administrative Center** and then press **Enter**.
3. In the left pane of the **Active Directory Administrative Center**, click **Example (local)** and then on the middle pane double click **Users**.
4. On the **Tasks** pane click **New** and then click **Group**.

5. On the **Create Group** window, type **Example-Remote-Access-Users** for **Group name** and click **OK**.
6. Right click the user **Mike Mayer** and click **Properties**.
7. On the left pane click **Extensions** and then click the **Dial-in** tab on the right pane and then in the **Network Access Permission** section select **Allow access** and then click **OK**.
8. Right click **Example-Remote-Access-Users** group and click **Properties**.
9. On the left pane click **Members** and then click **Add**.
10. Type **mikem** in the textbox and click **Check Names** and then click **OK**.

- Task 3: Configure a RADIUS server and network policies

1. Log on to **Example-Server01** using the following credentials:
2. Username: **Example.com\Administrator**
3. Password: **P@ssw0rd**
4. Create a new shared folder in **partition C** and name it **Example_Reports.**
5. Right click **Example_Reports** and click **Properties**.
6. Select the **Sharing** tab and click **Advance Sharing**.
7. On **Advance Sharing** window, select **Share this folder**. Leave the **Share name** as default and click **Permissions** to open the permissions window.
8. Select **Everyone** in the list of **Group or user names** and in the permissions entry list select **Allow** for **Full Control**.
9. Click **OK** three times to close all windows.
10. Create a new text document in **Example_Reports** and name it **Sample_Doc1.txt** and then open it with **NotePad** editor, add the following line to it: *"This is a sample document."* and then **save** before closing it.
11. Click **Start**, type **nps.msc** to open the **NPS** console.
12. In the NPS console, double-click **RADIUS Clients and Servers**. Click **RADIUS Clients** and then on the right pane **delete** all the existing RADIUS clients you created in the previous exercises.
13. Right-click **RADIUS Clients**, and then click **New**.
14. In **New RADIUS Client**, verify that the **Enable this RADIUS client** check box is selected.
15. In **New RADIUS Client**, in **Friendly name**, enter **Example-Server02** as the name for the remote access server. In **Address (IP or DNS)**, enter the **Example-Server02.Example.com**. To verify the FQDN, click **Verify**.
16. In **New RADIUS Client**, in **Vendor**, specify the manufacturer of the Remote Access Server you are using. If you are not sure of it, select **RADIUS standard**.
17. In the **Shared secret** section, ensure that **Manual** is selected, and then in **Shared secret**, enter **$har3d$3cr3t**. Retype the shared secret in **Confirm shared secret**.
18. Click **OK**. Your VPN Server will be listed as a RADIUS client configured on the NPS server.
19. On the **NPS** condole expand **Policies**, right click **Network Policies** and then click **New** to open the **New Network Policy** wizard.

20. On the **Specify Network Policy Name and Connection Type** page, type **VPN Users Policy** as the **Policy name** and select **Remote Access Server (VPN-Dial up)** as the **Type of network access server** and then click **Next**.
21. On the **Specify Conditions** page, click **Add** to open the **Select condition** window.
22. Select **User Groups** and then click **Add**.
23. On the **User Groups** window click **Add Groups** and then type **Example-Remote-Access-Users** in the textbox below **Enter the object name to select** and click **Check Names** and click **OK** twice.
24. Click **Add** again to open the **Select condition** window.
25. Select **Authentication Type** and click **Add**.
26. On the **Authentication Method** window, select **MS-CHAP v2** and then click **OK** and then click **Next**.
27. On the **Specify Access Permission** page, select **Access granted** and then click **Next**.
28. On the **Configure Authentication Methods** page, select **Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)** and **User can change password after it has expired** and then click **Next**.
29. On the **Configure Constraints** page, click **Next**.
30. On the **Configure Settings** page, click **Next**.
31. On the **Completing New Network Policy** page, click **Finish**.

- Task 4: Configure clients to connect to network using VPN

1. Log on to **Example-Client01** using the following credentials:
2. Username: **Example.com\Mikem**
3. Password: **P@ssw0rd**
4. Open the **Start** screen and type **Control Panel** and press **Enter** on the keyboard.
5. On the **Control Panel** window, click **View network status and tasks** under **Network and Internet** to open the **Network and Sharing Center** window and then on the left menu click **Change adapter settings**.
6. On the **Network Connections** window right click the network adapter and click **Properties** and when prompted for credentials, enter **Example.com\Administrator** for the username and **P@ssw0rd** for the password and then press **OK**.
7. On the network adapter properties window, click **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.
8. On the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, click **Use the following IP address** and then enter an IP address in the same range with **Example-Server02**'s external network adapter IP address. Enter a subnet mask of 255.255.255.0 and no default gateway.
9. Select **Use the following DNS server addresses** and then enter the IP address of **Example-Server02**'s external network adapter as the **Preferred DNS server** and then click **OK** twice.

10. Go back to the **Network and Sharing Center** window and click **Set up a new connection or network**.
11. On the **Set UP a Connection or Network** page, select **Connect to a workplace** and click **Next**.
12. On the **Connect to a workplace** page, click **Use my Internet connection (VPN)** and then click **I'll set up an Internet connection later**.
13. On the **Type the Internet address to connect to** page, enter the IP address of **Example-Server02**'s external network adapter in the **Internet address** textbox and in the **Destination name** textbox enter **Example VPN Connection** and click **Create**.
14. On the **Network and Sharing Center** window, click **Change adapter settings** on the left menu.
15. On the **Network Connections** window, right click **Example VPN Connection** and click **Properties**.
16. Select the **Security** tab and click **Allow these protocols** and then select **Microsoft CHAP Version 2 (MS-CHAP v2)** and click **OK**.
17. Double click **Example VPN Connection** and then on the right side bar click **Example VPN Connection** and click **Connect**.
18. Once prompted for credentials, enter **Example.com\Mikem** as the username and **P@ssw0rd** as the password.
19. Once the connection is established, open the **Start** screen and type \\Example-Server01.Example.com\Example_Reports and then make sure you can open **Sample_Doc1.txt** and view the content.

Exercise 2: Configuring and Integrating VPN with Network Access Protection

- Task 1: Configure a VPN server for the network

1. Log on to **Example-Server02** and keep the configuration as-is from **exercise 1.1**.
2. Open the **Routing and Remote Access console** and right click **Example-Server02** and click **Properties**.
3. Select the **Security** tab and click **Authentication Methods**.
4. On the **Authentication Methods** window, only select **Extensible authentication protocol (EAP)** and click **OK** twice.

- Task 2: Configure the Certificate Authority (CA) server and issue PEAP certificate

1. Log on to **Example-DC01** and open the **Start** screen and type **Certification Authority** and press **Enter**.
2. On the **Certification Authority** window, expand the **Example-Example-DC01-CA** node and then right click **Certificate Templates** and click **Manage**.
3. On the **Certificate Templates Console** window, right click **RAS and IAS Server** and click **Duplicate Template**.
4. On the **Properties of New Template** window, select the **General** tab and enter **NPS Certificate** as the **Template display name** and then select **Publish certificate in Active Directory**.
5. Select the **Security** tab and in the **Group or user names list** click **Domain Admins** and ensure they have **Allow Full Control** permission.
6. Click **Add** and enter **RAS and IAS Servers** in the textbox below **Enter the object names to select** and then click **Check Names** and then **OK**.
7. Make sure **RAS and IAS Servers** also are assigned **Allow Full Control** permission.
8. Click **OK** to create the template and then close the **Certificate Template Console**.
9. On the **Certification Authority** window, right click **Certificate Templates** and click **New** and then **Certificate Template to Issue**.
10. On the **Enable Certificate Template** window, select **NPS Certificate** and then click **OK** to add it to the list of available certificate templates.
11. Open the **Start** screen and type **Active Directory Administrative Center** and then press **Enter**.
12. In the left pane of the **Active Directory Administrative Center**, click **Example (local)** and then on the middle pane double click **Users**.
13. On the **Tasks** pane click **New** and then click **Group**.
14. On the **Create Group** window, type **Example-Remote-Access-Computers** for **Group name** and click **OK**.
15. Right click **Example-Remote-Access-Computers** and click **Properties**.
16. On the right pane click **Members**.
17. Click **Add** and then click **Object Types** and select **Computers** and click **OK**.

18. Enter **Example-Client01** in the textbox below **Enter the object names to select** and then click **Check Names** and then click **OK** twice.
19. Right click **RAS and IAS Servers** and click **Properties**.
20. On the right pane click **Members**.
21. Click **Add** and then click **Object Types** and select **Computers** and click **OK**.
22. Enter **Example-Server01** in the textbox below **Enter the object names to select** and then click **Check Names** and then click **OK** twice.

- Task 3: Configure Network Access Protection and create network policies

1. Log on to **Example-Server01** and open the **Start** screen and type **mmc** and press **Enter**.
2. On the **Microsoft Management Console** window, click **File** and then **Add/Remove Snap-in**.
3. On the **Add or Remove Snap-ins** window, from the list of **Available snap-ins** on the left select **Certificates** and then click **Add**.
4. On the **Certificates snap-in** window select **Computer account** and click **Next** and then click **Finish**.
5. Click **OK** to add the snap-in to the console.
6. Expand **Certificates (Local Computer)** and right click **All Tasks** and then **Request New Certificate** to open the **Certificate Enrollment** wizard.
7. Click **Next** twice and on the **Request Certificates** page, select **NPS Certificate** and then click **Enroll** and then **Finish**.
8. Expand **Personal** > **Certificates** to ensure the certificate has been added.
9. Open the **Start** screen and type **NPS** and press **Enter**.
10. On the **NPS** console, expand the **RADIUS Clients and Servers** and click **RADIUS Clients**.
11. On the right pane right click **Example-Server01.Example.com** and click **Properties**.
12. On the **Example-Server01.Example.com Properties** window, click the **Advanced** tab and then select **RADIUS client is NAP-capable** and then click **OK**.
13. Expand the **Policies** node and click **Network Policies** and on the right pane delete all the policies created in the previous exercises.
14. On the **NPS** console, click **NPS (local)** and on the right pane click **Configure NAP**.
15. On the **Select Network Connection Method for Use with NAP** page, select **Virtual Private Network (VPN)** as the **Network connection method** and enter **NAP VPN** as the **Policy name** and then click **Next**.
16. On the **Specify NAP Enforcement Servers Running VPN Server** page, ensure **Example-Server01.Example.com** is listed under the **RADIUS clients** and click **Next**.
17. On the **Configure User Groups and Machine Groups** page, click **Add** in the **Machine Groups** section.
18. Enter **Example-Remote-Access-Computers** in the textbox below **Enter the object names to select** and then click **Check Names** and then **OK**.
19. Click **Add** in the **User Groups** section.
20. Enter **Example-Remote-Access-Users** in the textbox below **Enter the object names to select** and then click **Check Names** and then **OK** and then click **Next**.

21. On the **Configure an Authentication Method** page, ensure the certificate added in this task has been automatically selected by clicking **View** and checking the details of the certificate. Click **Next** twice.
22. On the **Define NAP Health Policy** page, uncheck **Enable auto-remediation of client computers** and ensure **Windows System Health Validator** has been selected and then click **Next**.
23. Click **Finish**.
24. Expand the **Policies** node and click **Network Policies** and on the right pane right click **NAP VPN Non Nap-Capable** and click **Properties**.
25. On the **NAP VPN Non Nap-Capable Properties** select the **Overview** tab and in the **Access Permission** section, select **Deny access. Deny access if the connection request matches this policy** and then click **OK**.
26. Click **Health Policies** node on the left pane and on the right pane double click **NAP VPN Compliant** and on the **NAP VPN Compliant Properties** window, ensure **Client passes all SHV checks** has been selected for **Client SHV Checks** and then click **OK**.
27. Double click **NAP VPN Noncompliant** and on the **NAP VPN Noncompliant Properties** window, ensure **Client fails one or more SHV checks** has been selected for **Client SHV Checks** and then click **OK**.
28. On the **NPS** console, expand **Network Access Protection > System Health Validators > Windows Security Health Validator** and click **Settings** and then on the right pane double click **Default Configuration**.
29. On the **Windows System Health Validator** window, ensure **Windows 8/Windows 7/Windows Vista** on the left pane is selected and then on the right pane only **A firewall is enabled for all network connections** is selected.
30. Click **OK**.

- Task 4: Configure clients to connect to network using VPN

1. Log on to **Example-DC01** and open the **Start** screen and type **Group Policy Management** and then press **Enter**.
2. Expand the following nodes **Forest: Example.com > Domains > Example.com.**
3. Right-click **Group Policy Objects** and click **New**.
4. In the **New GPO** dialog box, type **Clients NAP Policy** as the name for your new GPO in the **Name** field. Click **OK**.
5. Right-click **Clients NAP Policy**, and then click **Edit**.
6. In the **Group Policy Management Editor** window, expand the following nodes **Computer Configuration > Policies > Windows Settings > Security Settings > System Services.**
7. In the details pane, double-click **Network Access Protection Agent** and on the **Network Access Protection Agent Properties** window, select the **Define this policy setting** check box, select **Automatic**, and then click **OK**.
8. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Network Access Protection > NAP Client Configuration > Enforcement Clients.**
9. In the details pane, right click **EAP Quarantine Enforcement Client**, and then click **Enable**.

10. Close the **Group Policy Management Editor** window and on the middle pane and in the **Security Filtering** section click **Authenticated Users** and click **Remove** and on the **Group Policy Management** dialog box click **OK**.
11. Click **Add** and then enter **Example-Remote-Access-Users; Example-Remote-Access-Computers** in the textbox below **Enter the object names to select** and then click **Check Names** and then click **OK**.
12. Right click **Example.com** and then click **Link an Existing GPO**.
13. On the **Select GPO** dialog box, select **Clients NAP Policy** and click **OK**.
14. Log on to **Example-Client01** using the following credentials:

- Username: **Example.com\Mikem**
- Password: **P@ssw0rd**

15. Open the **Start** screen and type **CMD** and then press **Enter**.
16. On the command prompt window enter the following command to update the policies on Example-Client01: **gpupdate /force**
17. Enter the following command to ensure **EAP Quarantine Enforcement Policy** is enabled: **netsh nap client show grouppolicy**
18. Enter the following command to ensure the **Initialized** status of the **EAP Quarantine Enforcement Client** is set to **Yes**: **netsh nap client show state**
19. Open the **Start** screen and type **Windows Firewall** and then click to open it.
20. On the left menu click **Turn Windows Firewall on or off** and enter the **Example.com\Administrator** credentials. Make sure **Turn on Windows Firewall** is selected for **Domain**, **Private** and **Public** networks and click **OK**.
21. Open the **Start** screen and type **Control Panel** and press **Enter** on the keyboard.
22. On the **Control Panel** window, click **View network status and tasks** under **Network and Internet** to open the **Network and Sharing Center** window and then on the left menu click **Change adapter settings**.
23. Do not remove the **Example VPN Connection** you created in **exercise 1.1** and right click on it and click **Properties**.
24. Select the **Security** tab, select **Use Extensible Authentication Protocol (EAP)** and choose **Microsoft: Protected EAP (PEAP) (encryption enabled)** and then click **Properties** and select **Validate server certificate** and then select **Enforce Network Access Protection** option. Click **OK** twice.
25. Double click **Example VPN Connection** and then on the right side bar click **Example VPN Connection** and click **Connect**.
26. Once prompted for credentials, enter **Example.com\Mikem** as the username and **P@ssw0rd** as the password.
27. Once the connection is established, open the **Start** screen and type \\Example-Server01.Example.com\Example_Reports and then make sure you can open **Sample_Doc1.txt** and view the content.
28. Disconnect the VPN connection and then go back to **Windows Firewall** and this time make sure **Turn off Windows Firewall (not recommended)** is selected for all **Domain**, **Private** and **Public** networks and then try again establishing the VPN connection.