Module 7: Configuring and Troubleshooting Security Settings

Lab: Configuring and Troubleshooting Security Settings

**Scenario**

A user has been assigned a new computer. You decide to verify the security settings on the device before delivering it to the user. You start by configuring Windows Defender Firewall. You also create a connection security rule to enable secure communications between a group of computers. Having delivered the computer, a user reports a problem to the helpdesk which is escalated to you. The user cannot sign-in, and the helpdesk have been through the obvious things with no success. You investigate.

Objectives

After completing this lab, you will be able to:

* Configure Windows Defender Firewall.
* Configure a connection security rule.
* Resolve a sign-in issue.

Exercise 1: Configuring Windows Defender Firewall

**Scenario**

When communications occurs over a network, it's important to manage the specific nature of that communications. A host firewall, like Windows Defender Firewall, enables you to configure rules that allow or block network traffic based on its characteristics.

The main tasks for this exercise are as follows:

1. Create and test an inbound firewall rule.

Task 1: Create and test an inbound firewall rule

1. On [**LON-DC1**](urn:gd:lg:a:select-vm), sign in as [**Adatum\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. In Server Manager, click **Tools**, and then click **Windows Defender Firewall with Advanced Security**.
3. In Windows Defender Firewall with Advanced Security, click **Inbound Rules**, right-click **Inbound Rules**, and then click **New Rule**.
4. In the **New Inbound Rule Wizard**, on the **Rule Type** page, select **Custom** and click **Next** twice.
5. On the **Protocol and Ports** page, in the **Protocol type** list, select **ICMPv4** and click **Next** twice
6. On the **Action** page, click **Allow the connection** and click **Next** twice.
7. On the **Name** page, in the **Name** text box, enter [**ICMP**](urn:gd:lg:a:send-vm-keys) and click **Finish**.
8. On [**LON-CL1**](urn:gd:lg:a:select-vm), sign in as [**Adatum\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
9. Open **Windows Terminal (admin)**.
10. On the **Administrator: Windows Powershell** tab, in the command prompt, type **ping LON-DC1** and press Enter. This is successful as the rule is configured to allow inbound ICMP traffic.
11. ping LON-DC1
12. On [**LON-DC1**](urn:gd:lg:a:select-vm), in the **Inbound Rules** folder, double-click **ICMP**.
13. Click **Block the connection** and click **OK**.
14. On [**LON-CL1**](urn:gd:lg:a:select-vm), repeat the **ping LON-DC1** command. This fails as the rule now blocks ICMP traffic.
15. ping LON-DC1

**Results** : After completing this exercise, you should successfully created an inbound firewall rule.

Exercise 2: Configuring a connection security rule

**Scenario**

You can create connection security rules that enable authenticated connections between configured devices to provide for additional security.

The main tasks for this exercise are as follows:

1. Create and test a connection security rule.

Task 1: Create and test a connection security rule

1. Switch to [**LON-DC1**](urn:gd:lg:a:select-vm), in **Windows Defender Firewall with Advanced Security**, click the **Connection Security Rules** node, right-click **Connection Security Rules**, and then click **New Rule**.
2. In the **New Connection Security Rules Wizard**, select **Server-to-server** and click **Next** twice.
3. On the **Requirements** page, click **Require authentication for inbound connections and request authentication for outbound connections** and click **Next**.
4. On the **Authentication Method** page, click **Advanced**.
5. Click **Customize**, and then, under the **First authentication** heading, click **Add**.
6. Select **Preshared key (not recommended)**, and enter the password of [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys). Click **OK** twice, and then click **Next** twice.
7. On the **Name** page, enter the name [**Adatum Secure**](urn:gd:lg:a:send-vm-keys) and click **Finish**.
8. Switch to [**LON-CL1**](urn:gd:lg:a:select-vm), and open **Windows Defender Firewall with Advanced Security**.
9. In **Windows Defender Firewall with Advanced Security**, click the **Connection Security Rules** node, right-click **Connection Security Rules**, and then click **New Rule**.
10. In the **New Connection Security Rules Wizard**, select **Server-to-server** and click **Next** twice.
11. On the **Requirements** page, click **Require authentication for inbound connections and request authentication for outbound connections** and click **Next**.
12. On the **Authentication Method** page, click **Advanced**.
13. Click **Customize**, and then, under the **First authentication** heading, click **Add**.
14. Select **Preshared key (not recommended)**, and enter the password of [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys). Click **OK** twice, and then click **Next** twice.
15. On the **Name** page, enter the name [**Adatum Secure**](urn:gd:lg:a:send-vm-keys) and click **Finish**.
16. On [**LON-DC1**](urn:gd:lg:a:select-vm), in the **Inbound Rules** folder, double-click **ICMP**.
17. Click **Allow the connection if it is secure** and click **OK**.
18. On [**LON-CL1**](urn:gd:lg:a:select-vm), in Windows Terminal, repeat the **ping LON-DC1** command. This succeeds as ICMP traffic is allowed if its secured.
19. ping LON-DC1
20. To examine the Main Mode Security Associations (SAs), at the Windows PowerShell command prompt, type the following cmdlet, and then press Enter:
21. Get-NetIPsecMainModeSA
22. Review the result.
23. To examine the Quick Mode SAs, at the command prompt, type the following cmdlet, and then press Enter:
24. Get-NetIPsecQuickModeSA
25. Review the result.

**Results** : After completing this exercise, you should successfully created and tested a connection security rule.

Exercise 3: Resolving a Sign-In Issue

**Scenario**

Art, one of the senior managers, has called the help desk to report that he has an issue when trying to sign in. You are assigned to resolve this issue. He has called the help desk twice since his initial call, so it is urgent that you resolve the issue.

| **Incident Record** |
| --- |
| **Incident Reference Number:** 823423 |
| Date and time of call: October 6, 13:47 |
| User: Art Odum (Manager) |
| Status: OPEN |
| **Incident Details** |
| Art called to report an issue with signing in. It has been determined that several management teams are experiencing the same issue, and receive an error message that displays: "There are currently no logon servers available to service the logon request." |
| **Additional Information** |
| The management team's computers connect to a private subnet that has a private local domain controller, LON-DC1. |
| Some of the management team can sign in, but most cannot. |
| You might need the local account, LON-CL1\Admin (password is Pa55w.rd), to sign in atMr. Odum's computer. |
| A few network-related issues were reported in that subnet this morning, with failure to locate resources by URL name. |
| **Plan of Action** |
| **Resolution** |

Task 1: Review the help-desk Incident Record for incident 823423

* Review the help-desk Incident Record 823423 in the Student Handbook exercise scenario.

Task 2: Update the Plan of Action section of the Incident Record

1. Review the **Additional Information** section of the incident record in the Student Handbook exercise scenario.
2. Update the **Plan of Action** section of the incident record with your recommendations:

a. Visit the management subnet.

b. Attempt a local sign-in at Mr. Odum's computer.

c. Sign in by using a local administrator's account to attempt resolution.

Task 3: Simulate the issue

1. Switch to [**LON-CL1**](urn:gd:lg:a:select-vm) and login as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys)
2. Run the **D:\Labfiles\Mod07\Scenario1.cmd** script at an elevated Windows Terminal command prompt.
3. D:\Labfiles\Mod07\Scenario1.cmd
4. Wait while **LON-CL1** restarts.

Task 4: Attempt to resolve the issue

1. Switch to [**LON-CL1**](urn:gd:lg:a:select-vm) and login as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys)
2. Notice that you are unsuccessful.
3. Sign in by using the following credentials:
   * Username: [**.\Admin**](urn:gd:lg:a:send-vm-keys)
   * Password: [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys)
4. Switch to [**LON-DC1**](urn:gd:lg:a:select-vm) send the [**CTRL+ALT+DEL**](urn:gd:lg:a:send-vm-key-combo) command and login as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys)
5. In Server Manager, select **Tools**, and then select **Services**.
6. Double-click **DNS Server**.
7. Click **Start**, and then click **OK**.
8. Switch to [**LON-CL1**](urn:gd:lg:a:select-vm)
9. On the desktop, right-click **Start**, point to **Shut down or sign out**, and then click **Restart**.
10. Sign in by using the following credentials:
    * Username: [**Adatum\Art**](urn:gd:lg:a:send-vm-keys)
    * Password: [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys)
11. Sign out of **LON-CL1**.
12. Notice that you are now able to sign in, and then sign out.
13. Update the **Resolution** section of the incident record.

a. Signed in as a local administrator.

b. Switched to the domain controller, and then restarted the Domain Name System (DNS) service, which had stopped.

c. Restarted Mr. Odum's computer.

d. Tested signing in as Mr. Odum. This was successful.

e. Lack of DNS service meant no domain controller could be located for sign-in.

**Results**: After you have completed this exercise, you should have resolved the sign-in issue.

**Congratulations!** You have now completed this lab. To continue to the next lab click End Lab in the Tools Menu . If you wish to contiue with this lab at a later date ensure you save the lab environment rather than ending it.