Managing Centralized Authentication

Scenario

RADIUS permits centralized authentication. In this activity, you will rely on Active Directory (on DC1) as the authentication server. It will also act as the RADIUS server – the point where all authentication attempts get forwarded. The pfSense security appliance VM, will be configured as a RADIUS client. It will pass authentication attempts to DC1. In this scenario, RADIUS is being used to authenticate administrative users who manage the pfSense firewall appliance itself, rather than authentication of remote access VPN or wireless users.

Objectives

This activity is designed to test your understanding of and ability to apply content examples in the following CompTIA Security+ objectives:

- 3.8 Given a scenario, implement authentication and authorization solutions.

Lab

- DC1 VM
- pfSense VM

Task 1

Register RADIUS client

RADIUS can be used with VPN, wireless, and appliance authentication. In Windows Server, the RADIUS role is configured using Network Policy Server (NPS). Use NPS to configure pfSense VM as an authorized RADIUS client of DC1.

1. Select the **DC1** VM, send **CTRL+ALT+DEL**, and log on with the credentials **CONTOSO\ Administrator** and **Pa$$w0rd**.

2. In **Server Manager**, select **Tools > Network Policy Server**.

3. Expand **RADIUS Clients and Servers** to select **RADIUS Clients**. Right-click **RADIUS Clients** and select **New**.

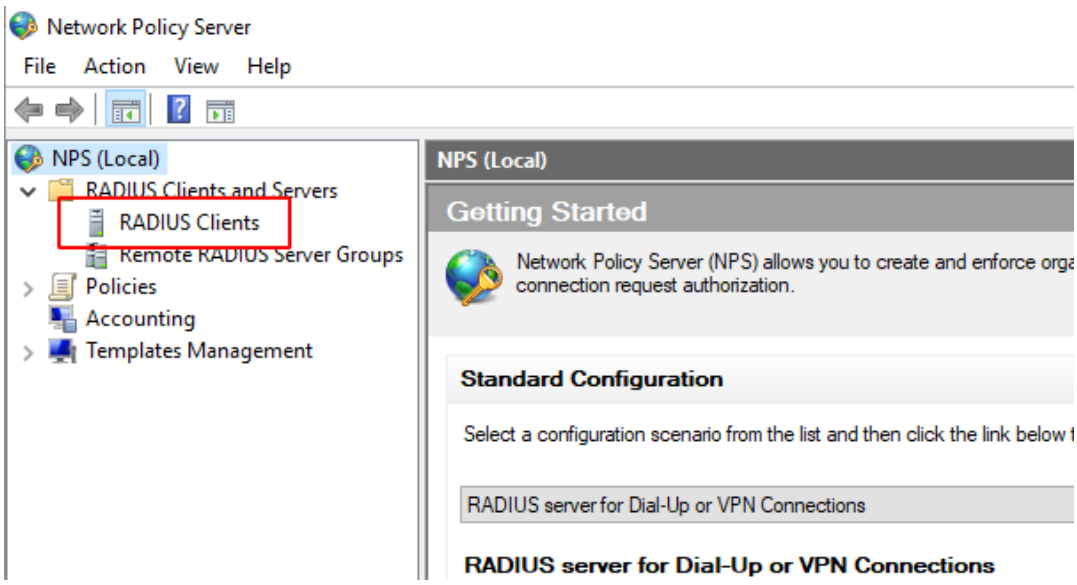

Figure 1.1 – Network Policy Server console.

The RADIUS client is the network appliance accepting the user's credentials (in this case, the pfSense VM).

4. In the New RADIUS Client dialog box, in the Friendly name box, enter **pfsense.contoso.local**.

5. In the Address box, type **192.168.1.254**.

6. Under Shared Secret, select the **Generate** radio button, then select the **Generate** button.

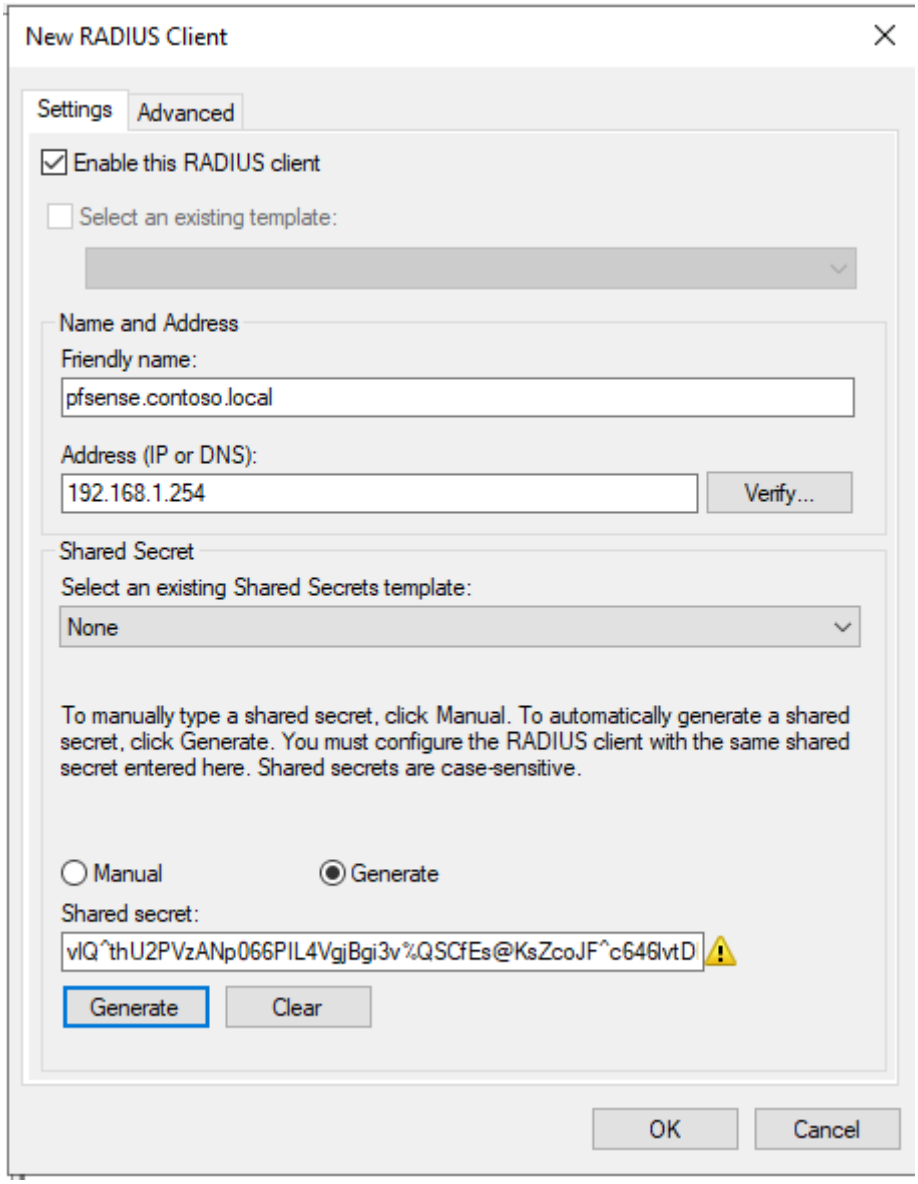

Figure 1.2 – New RADIUS Client configuration window.

7. **Copy** the shared secret string.

TIP: You need to keep this value on the Clipboard for a while – alternatively, you can paste it into a Notepad file.

8. Select **OK** to close the dialog box.

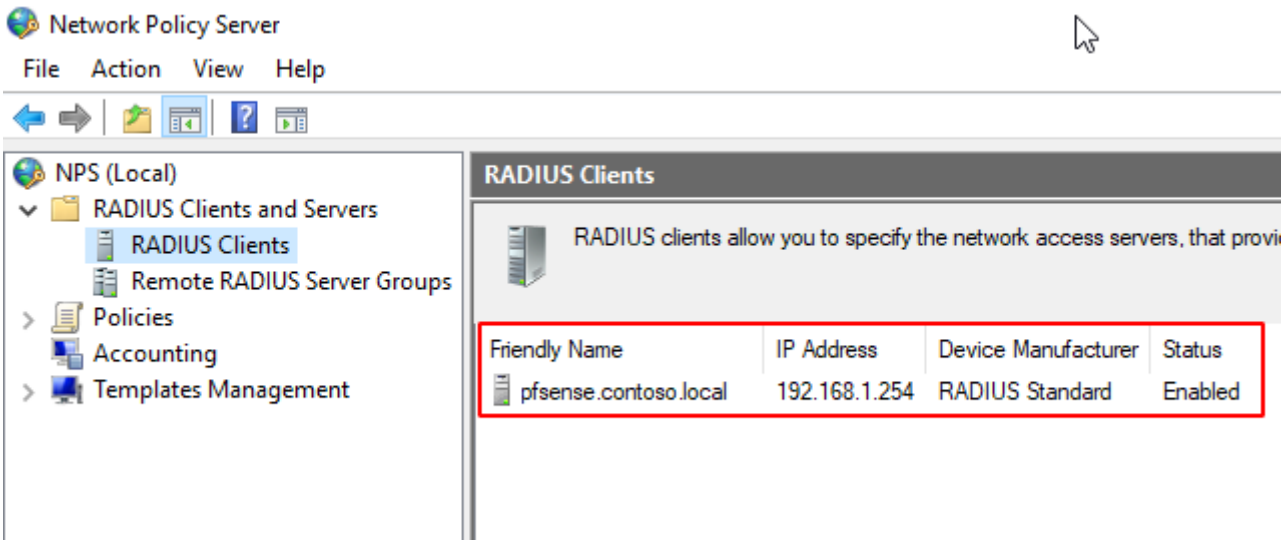

Figure 1.3 – The RADIUS clients pane in Network Policy Server.

Task 2

Configure network policy

Configure a policy that allows users in the LocalAdmin security group to authenticate with pfSense by using unencrypted authentication. Use the Class attribute to transmit the LocalGroup property from the RADIUS server to the RADIUS client when a user authenticates.

1. In the Network Policy Server console, expand **Policies** to select **Network Policies**, Right-click **Network Policies** and select **New**.

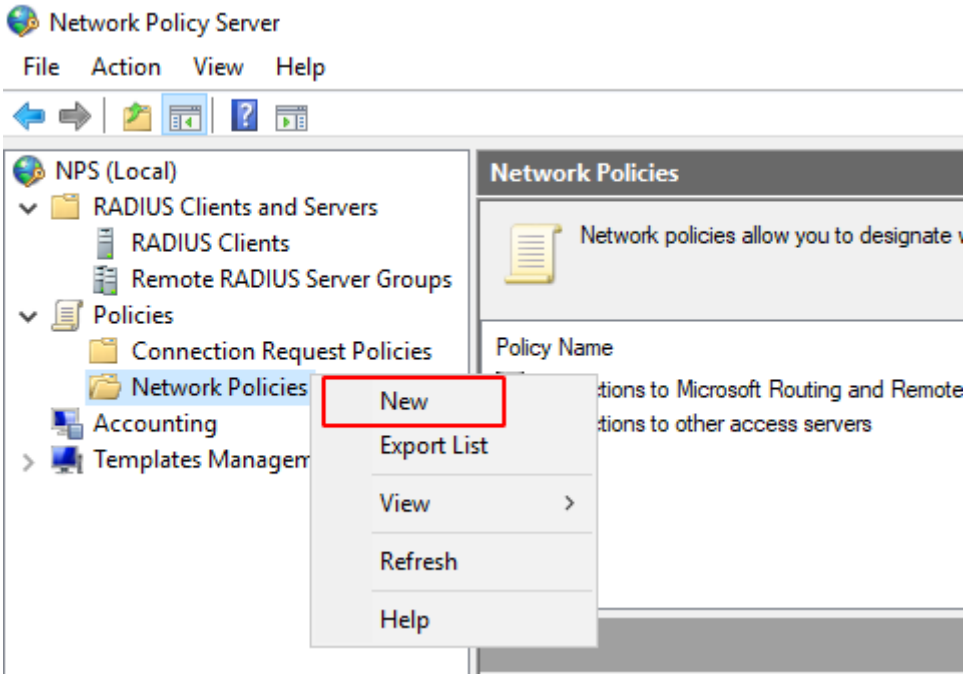

Figure 2.1 – Creating a New Network Policy.

2. In Policy name, type **pfSense Network Security Appliance Administration**.

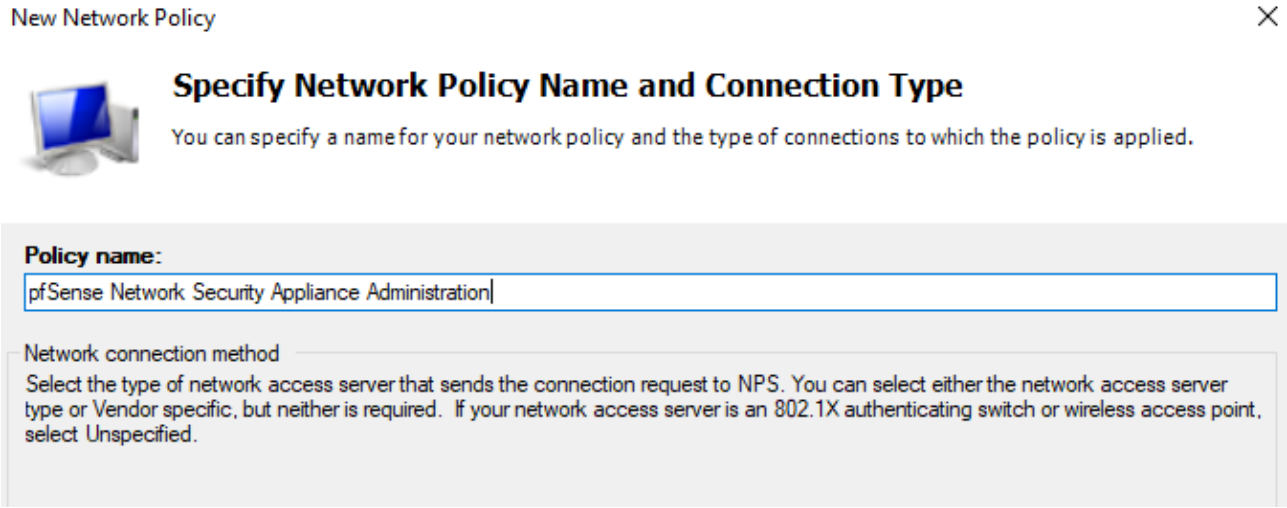

Figure 2.2 – Specify a Network Policy Name.

3. Select **Next**, On the Specify conditions page, select the **Add** button.

4. Select **Windows Groups** and select **Add**.

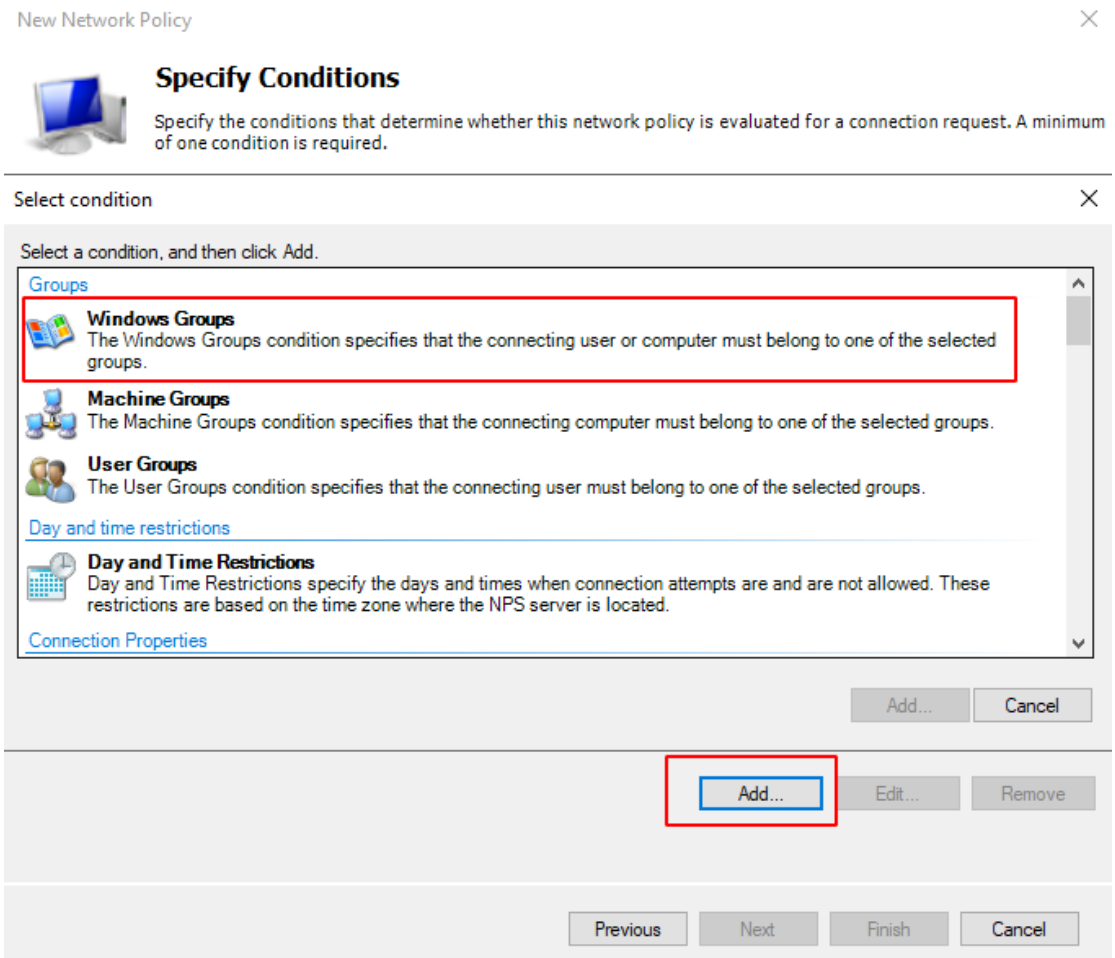

Figure 2.3 – Specifying the conditions and Groups.

5. Select the **Add Groups** button then type **localadmin** and select the **Check Names** button.

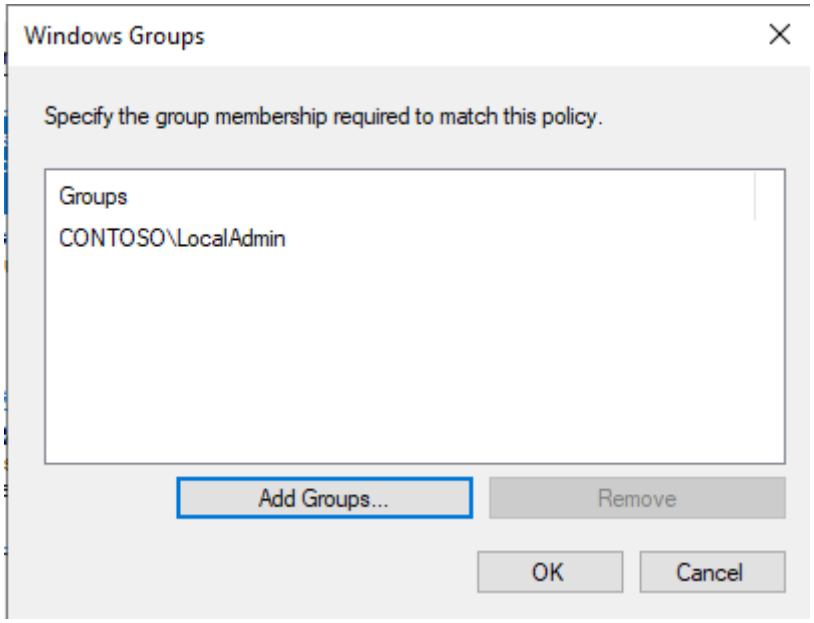

Figure 2.4 – Selecting LocalAdmin group.

6. Select **OK** then select **OK** again to confirm the Windows Groups dialog box.

7. Select **Next**.

8. On the **Specify Access Permissions** page, leave **Access granted** selected and select **Next**.

9. On the **Configure Authentication Methods** page, leave the existing **MS-CHAPv2** and **MS-CHAP** boxes selected, as shown in this screenshot.

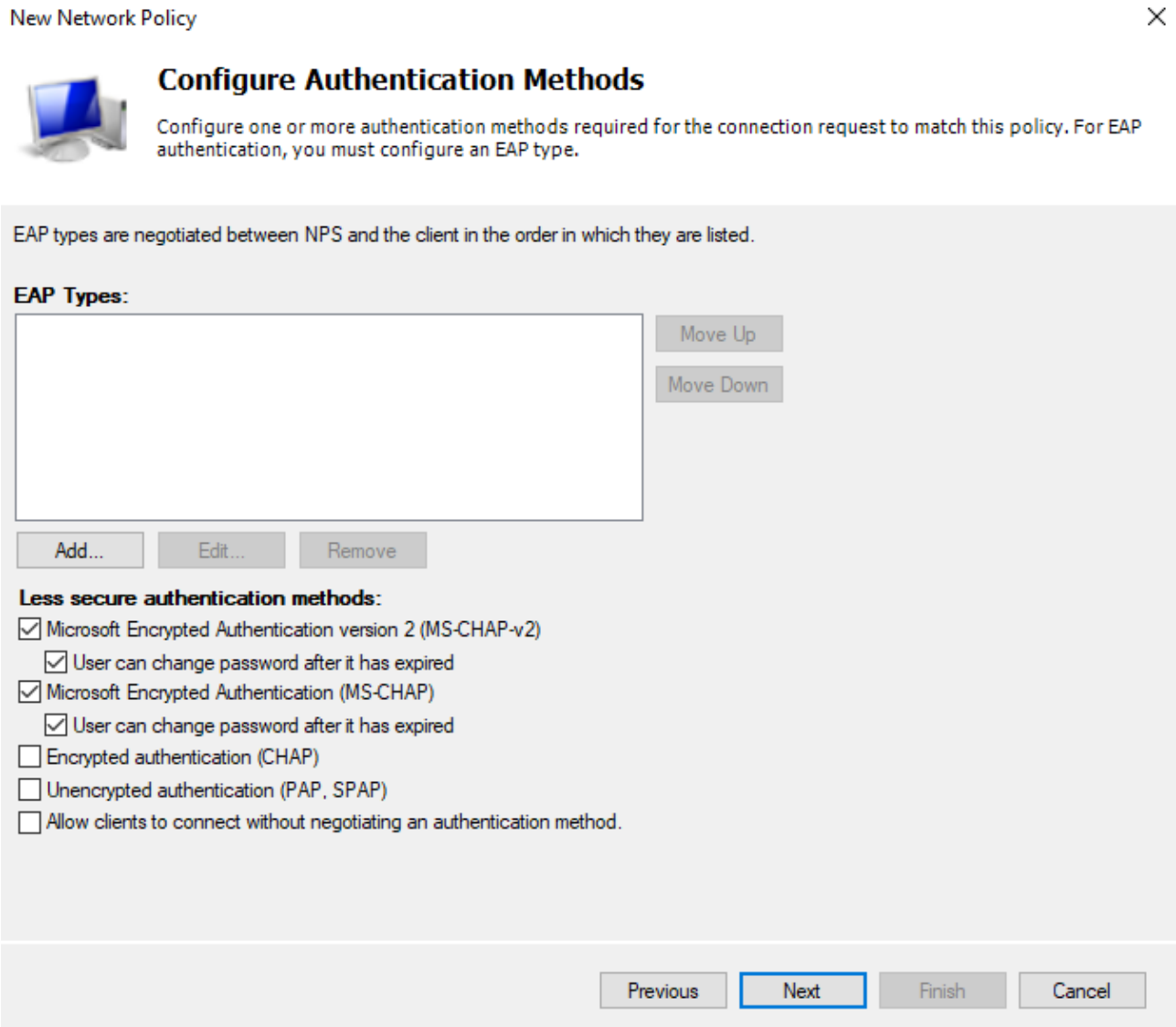

Figure 2.5 – Configure authentication methods.

10. Select **Next**.

TIP: We are not implementing it for this lab, but because the credential is being passed using **weak MS-CHAP encryption**, you must configure the management interface to use HTTPS encrypted connection security rather than plain HTTP. You would achieve this by installing a trusted root certificate to the pfSense appliance and disabling HTTP-only access.

11. On the **Configure Constraints** page, select **Next**.

12. On the **Configure Settings** page, with **Standard** selected, select the **Add** button.

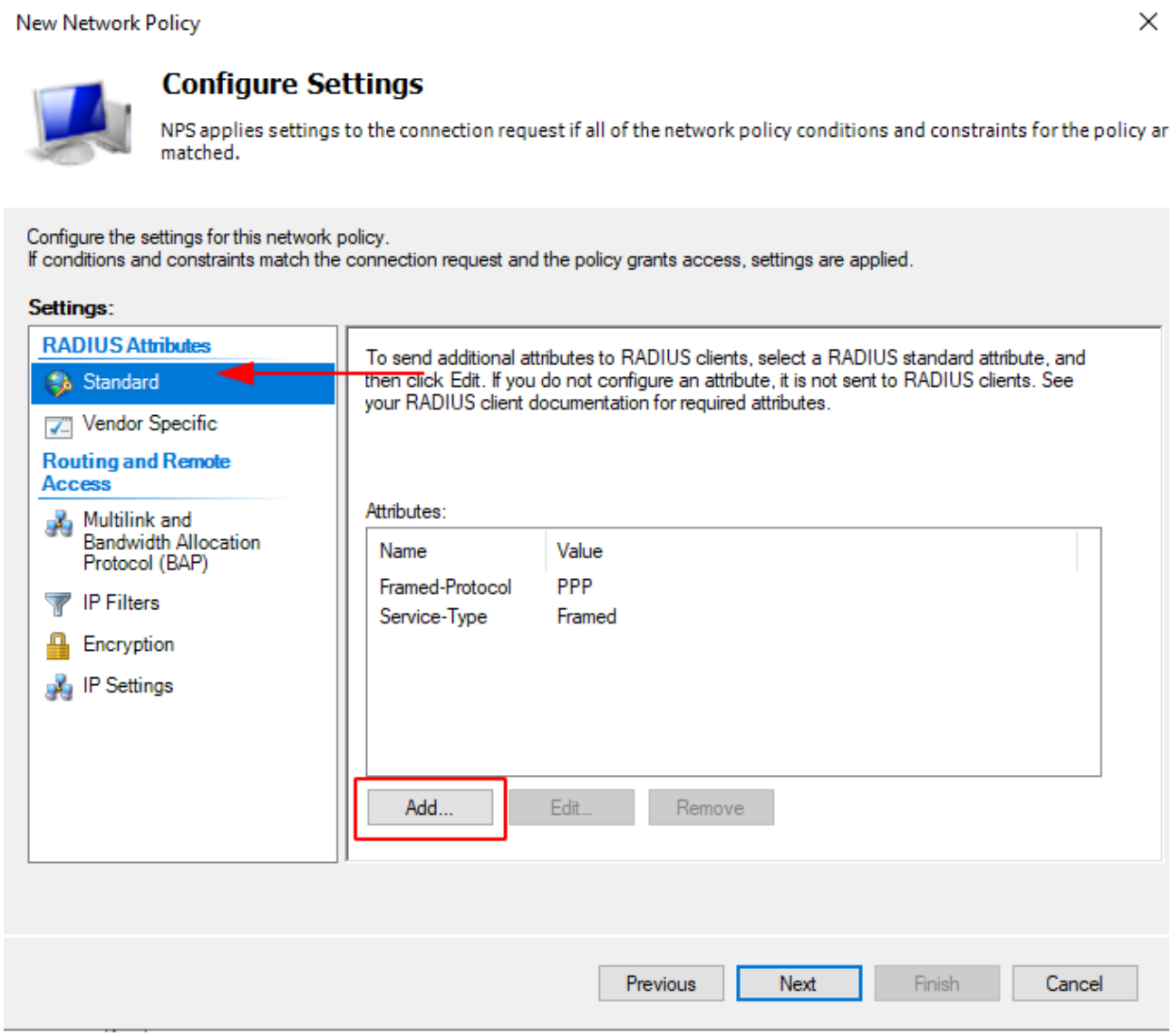

Figure 2.6 – Configure Settings window.

13. In the **Add Standard RADIUS Attribute** dialog box, from the **Attributes** box, select **Class**, Select the **Add** button.

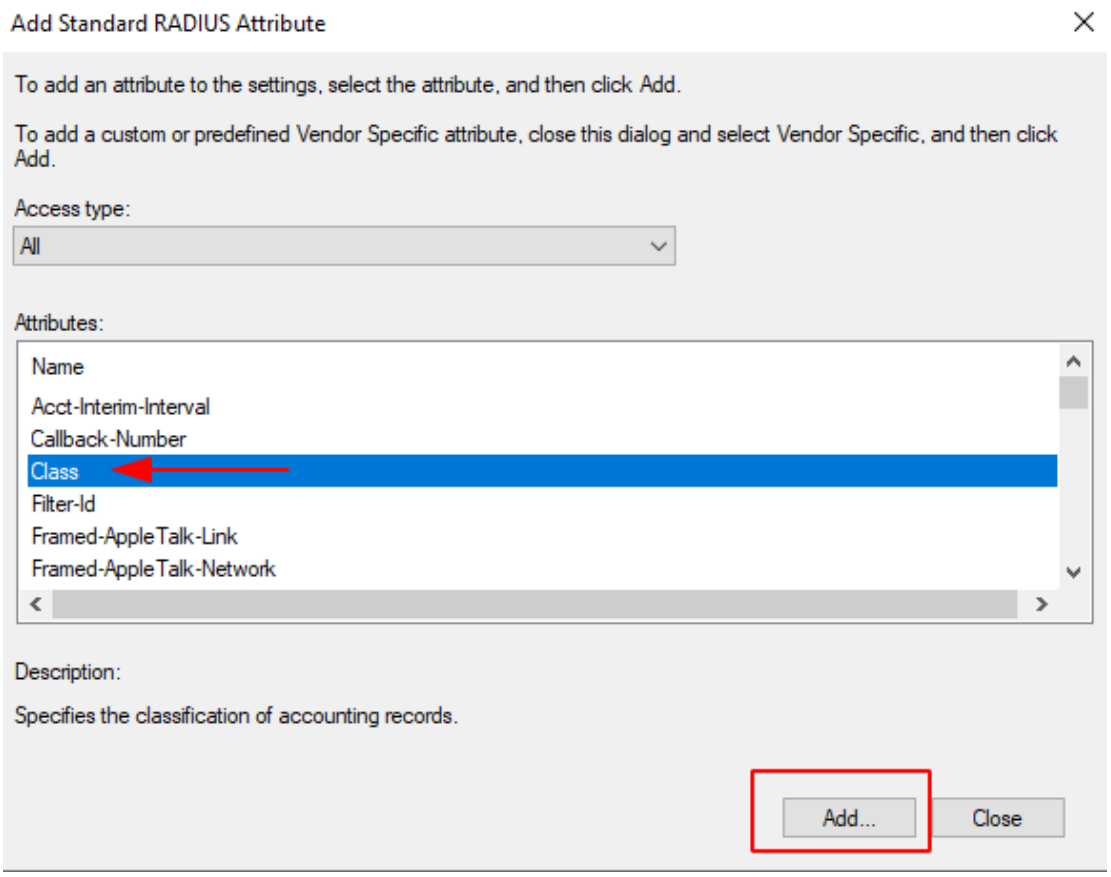

Figure 2.7 – Adding Class attribute.

14. Type **LocalAdmin** in the box and select **OK**. Select **Close**. pfSense uses the Class attribute to communicate group membership.

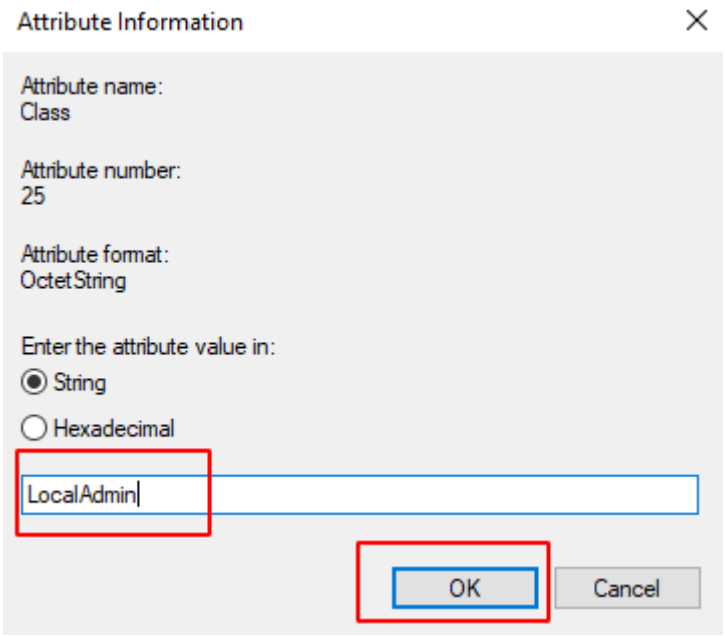

Figure 2.8 – Attribute information window.

15. Select **Next** then **Finish**.

16. Right-click the policy and **Move Up** to have **Processing Order** of **1**.

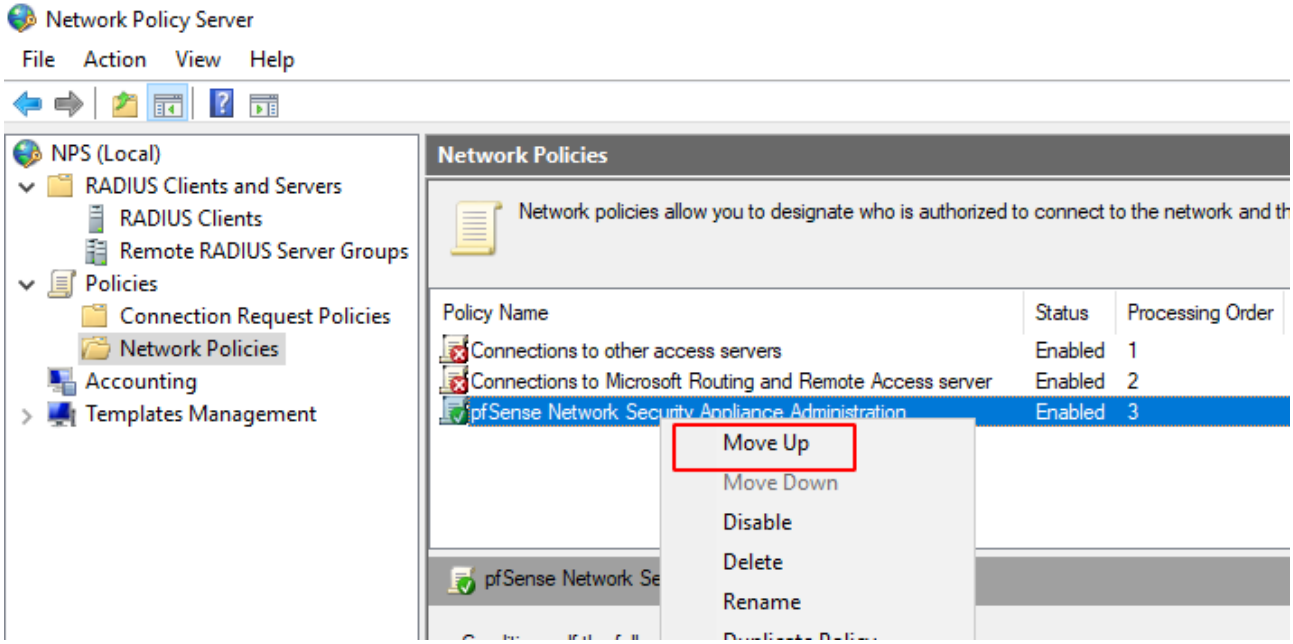

Figure 2.9 – Moving UP the policy to have a Processing Order of 1.

Task 3

Configure RADIUS client

Configure the pfSense VM as a RADIUS client by inputting the RADIUS server details. This permits pfSense to forward authentication requests to DC1.

1. Still on the **DC1** VM, open h**ttp://192.168.1.254** in the browser.

You will be connected to the pfSense virtual machine.

2. Log on with the credentials **admin** and **Pa$$w0rd**. When prompted to save the password, select **Not for this site**.

3. Maximize the browser window. select **System > User Manager**. Select the **Authentication Servers** tab, then select the **Add** button.

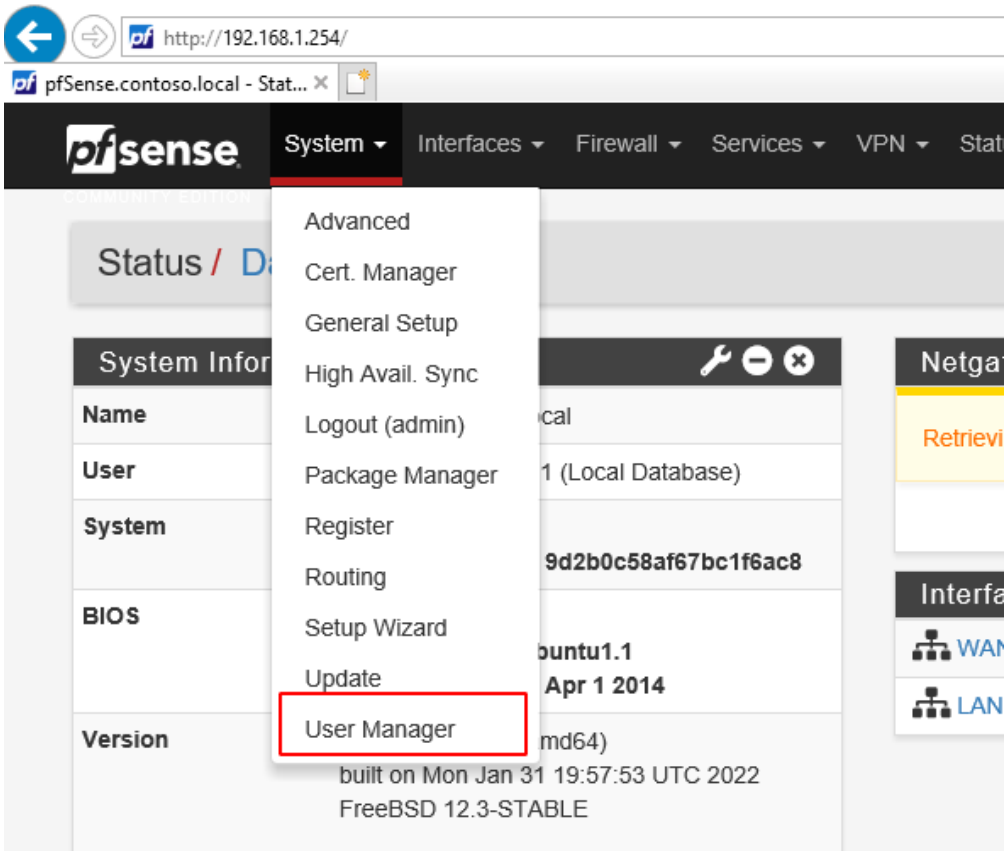

Figure 3.1 – pfSense System > User Manager.

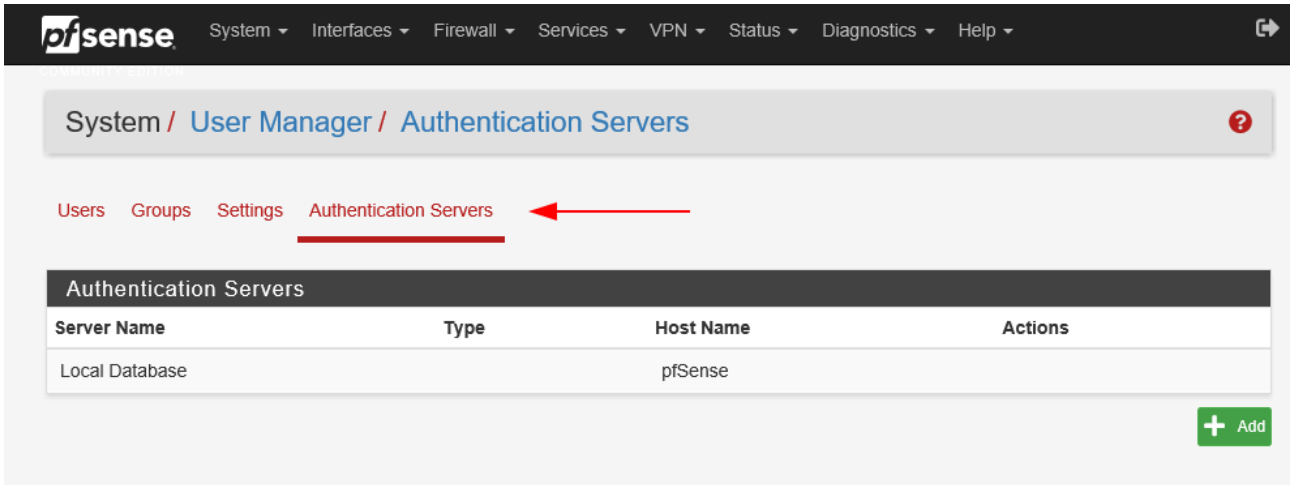

Figure 3.2 – User Manager > Authentication Servers Tab.

4. In the Descriptive name box, type **Contoso Support AD**.

5. From the Type list, select **RADIUS**.

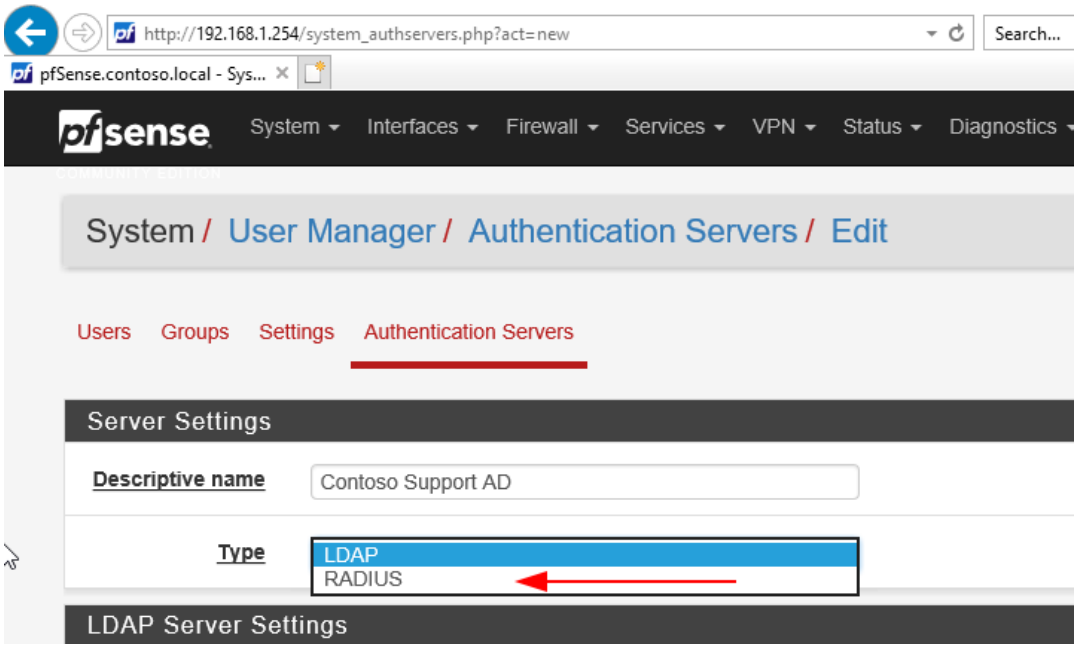

Figure 3.3 – pfSense > User Manager > Authentication Servers > Type – RADIUS selection.

6. Under RADIUS Server Settings, note that the Protocol is set to MS-CHAPv2 by default. This is the authentication protocol that determines the format for the user credential. The RADIUS server and the client must be able to match at least one authentication method.

7. In the **Hostname or IP address** box, enter **192.168.1.1**.

8. In the **Shared Secret** box, **paste the Clipboard contents**.

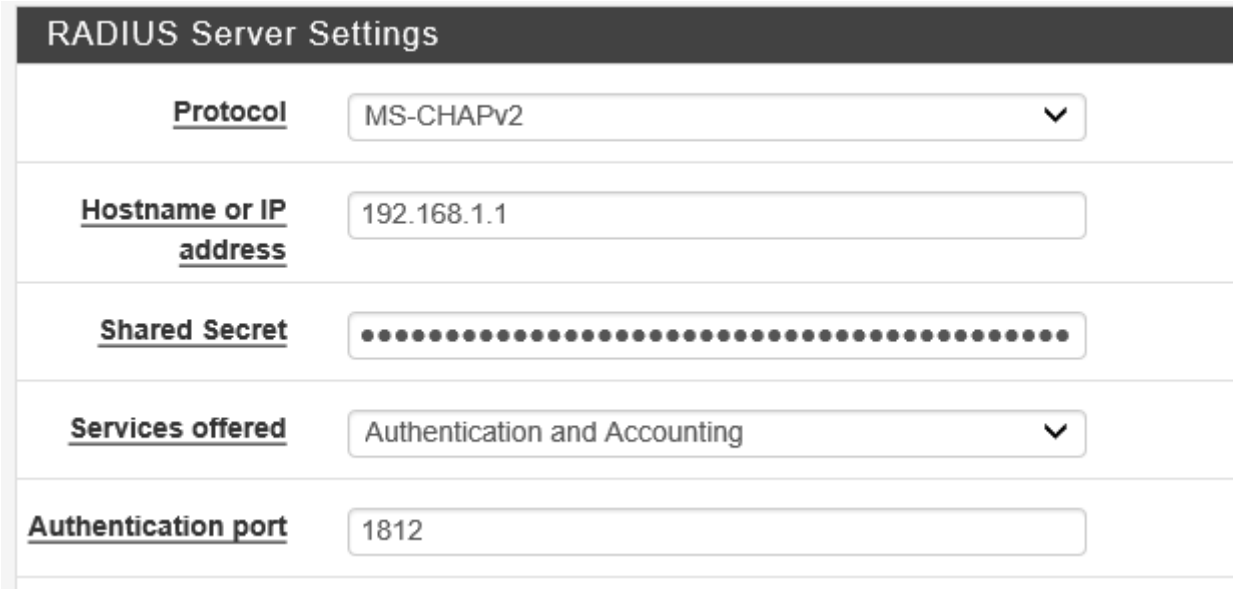

Figure 3.4 – RADIUS Server Settings.

You are **pasting** in the **shared secret** generated on **DC1** in an earlier task.

9. Select the **Save** button.

Task 4

Configure role-based permissions

Configure a basic least permissions role for the LocalGroup security group account so that users do not have access to advanced system configuration pages.

1. Select the **Groups** tab, then select the **Add** button.

2. In the **Group name** box, type **LocalAdmin**.

3. Select the **Save** button.

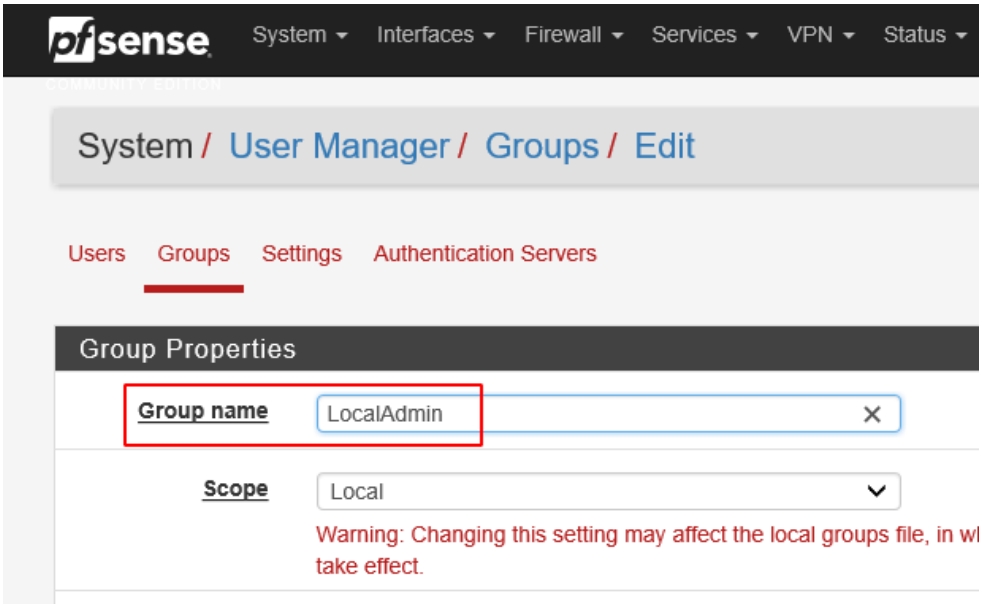

Figure 4.1 – System > User Manager Groups > Edit.

4. In the **Actions** column, select the **Edit group** pencil icon to edit the **LocalAdmin** group.

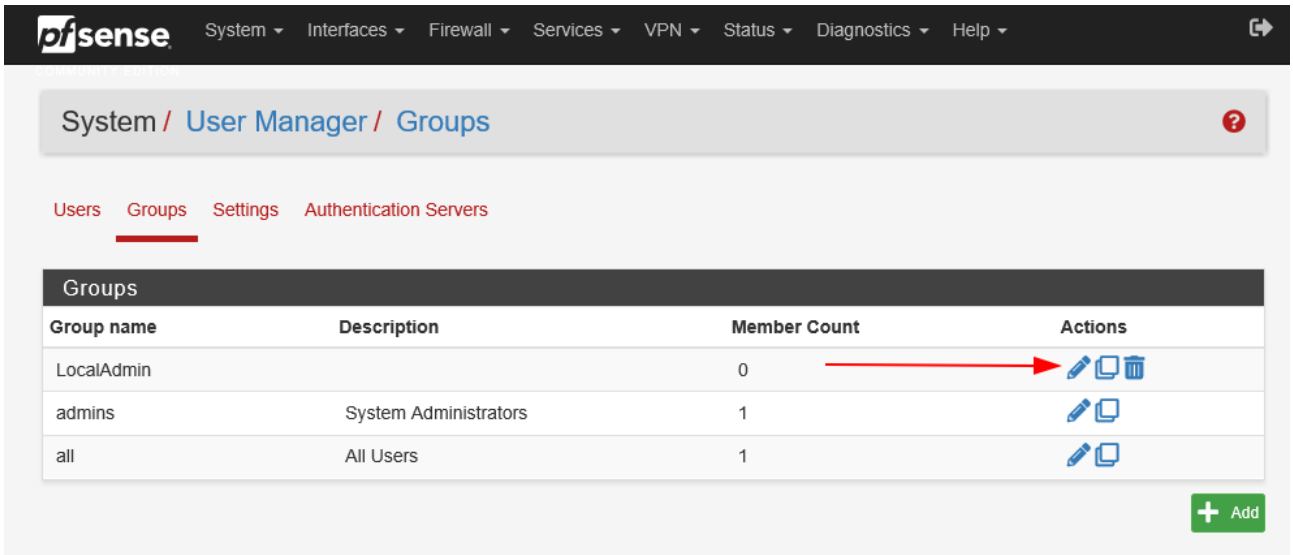

Figure 4.2 – Edit LocalAdmin group by clicking the pencil icon.

5. Under the **Assigned Privileges** section, select the **Add** button.

6. **SHIFT-click** to select from **WebCfg—Dashboard (all)** down to the last **WebCfg—Status: UpnP Status** item.

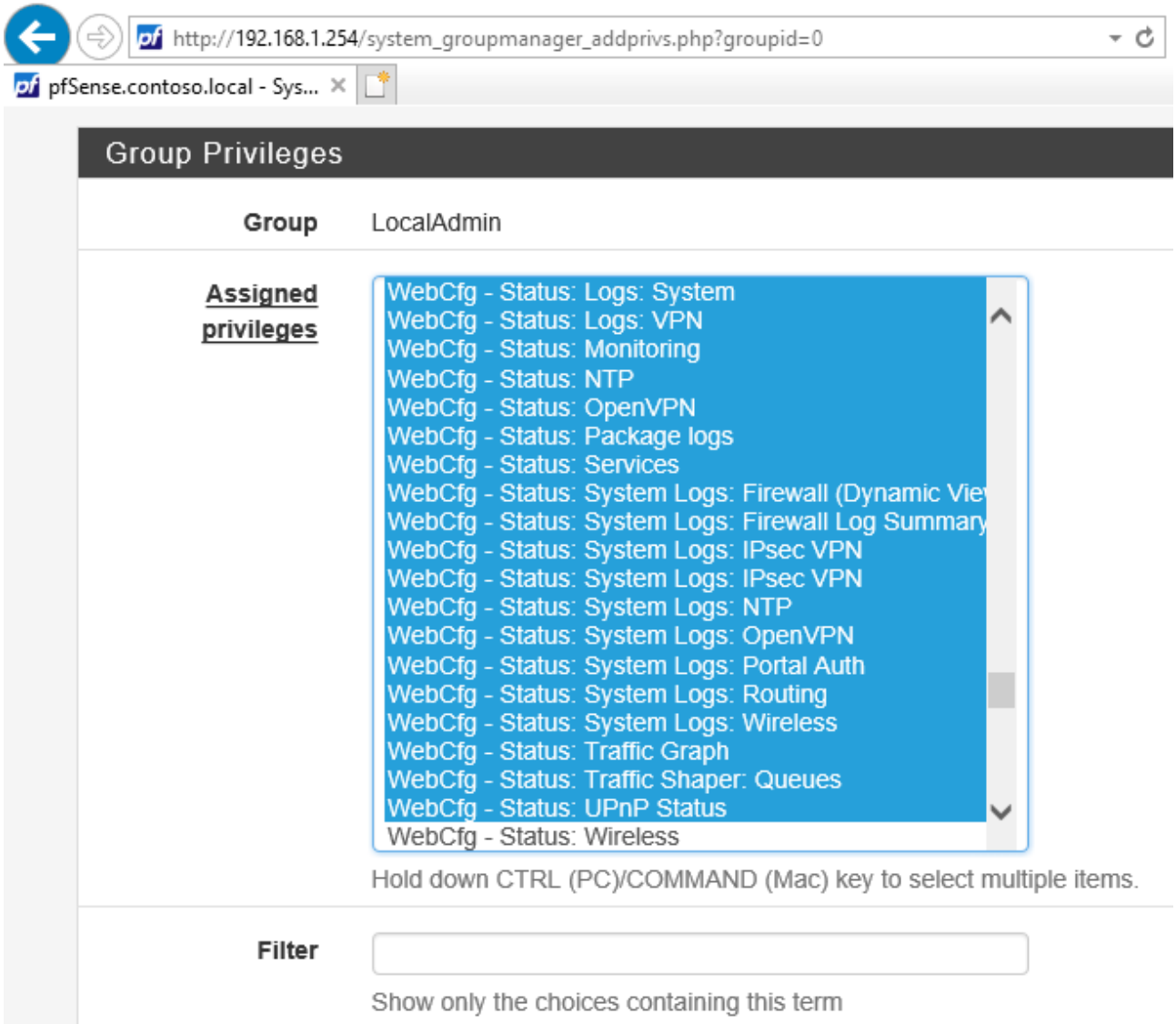

Figure 4.3 – Selecting Assigned Privileges.

This is a very long list of privilege names!

7. Locate the item **WebCfg—pfSense wizard subsystem** and **CTRL+click** to **deselect** it.

8. Select the **Save** button.

TIP: If you scroll down you will see the privileges selected.

9. Select the **Settings** tab, then from the **Authentication Server** box, select **Contoso Support AD**. Select the **Save** button.

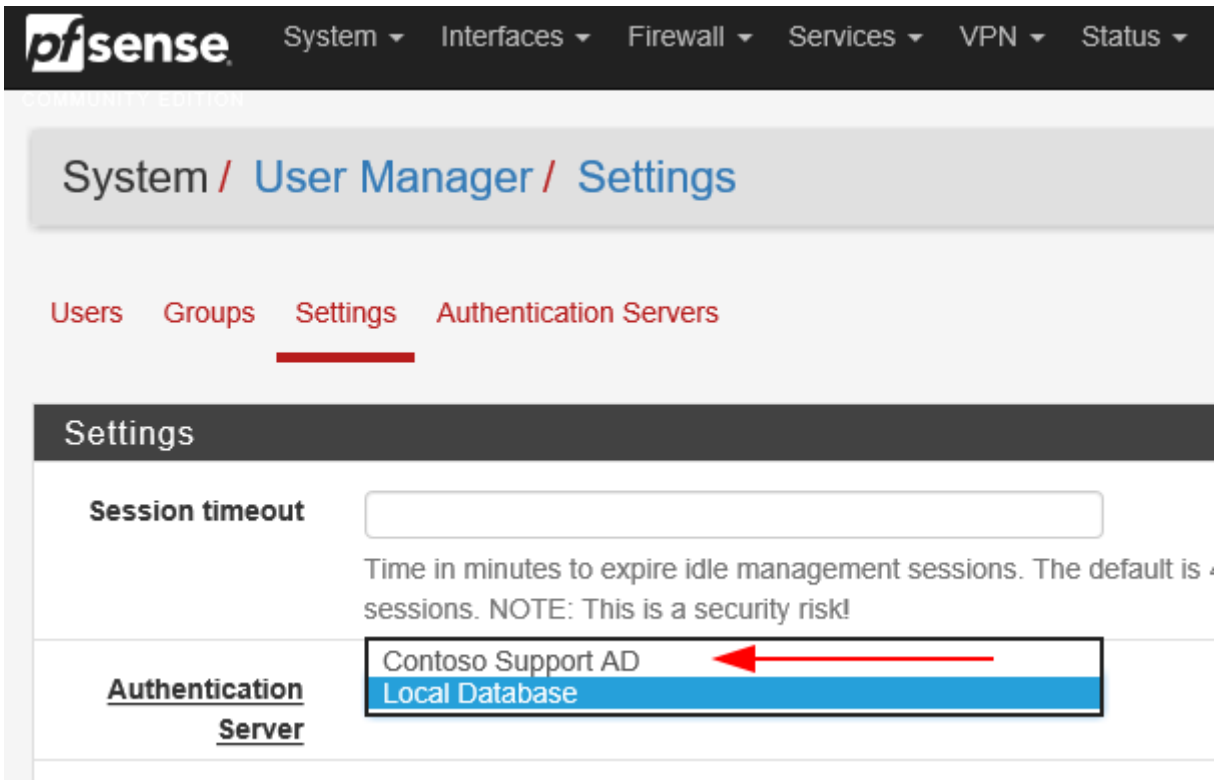

Figure 4.4 – Selecting Authentication Server.

10. From the **upper right corner** of the page, select the **Logout** button.

Task 5

Test the credentials

To test that pfSense is passing credentials to Active Directory, you will now log on to the pfSense device with a non-administrator account. The account is stored in AD. This allows you to exercise the privileges granted in the previous task.

1. Log on with the credentials **support** and **Pa$$w0rd**.

Now when you log on, the pfSense VM passes the credentials you have submitted to the RADIUS server for validation.

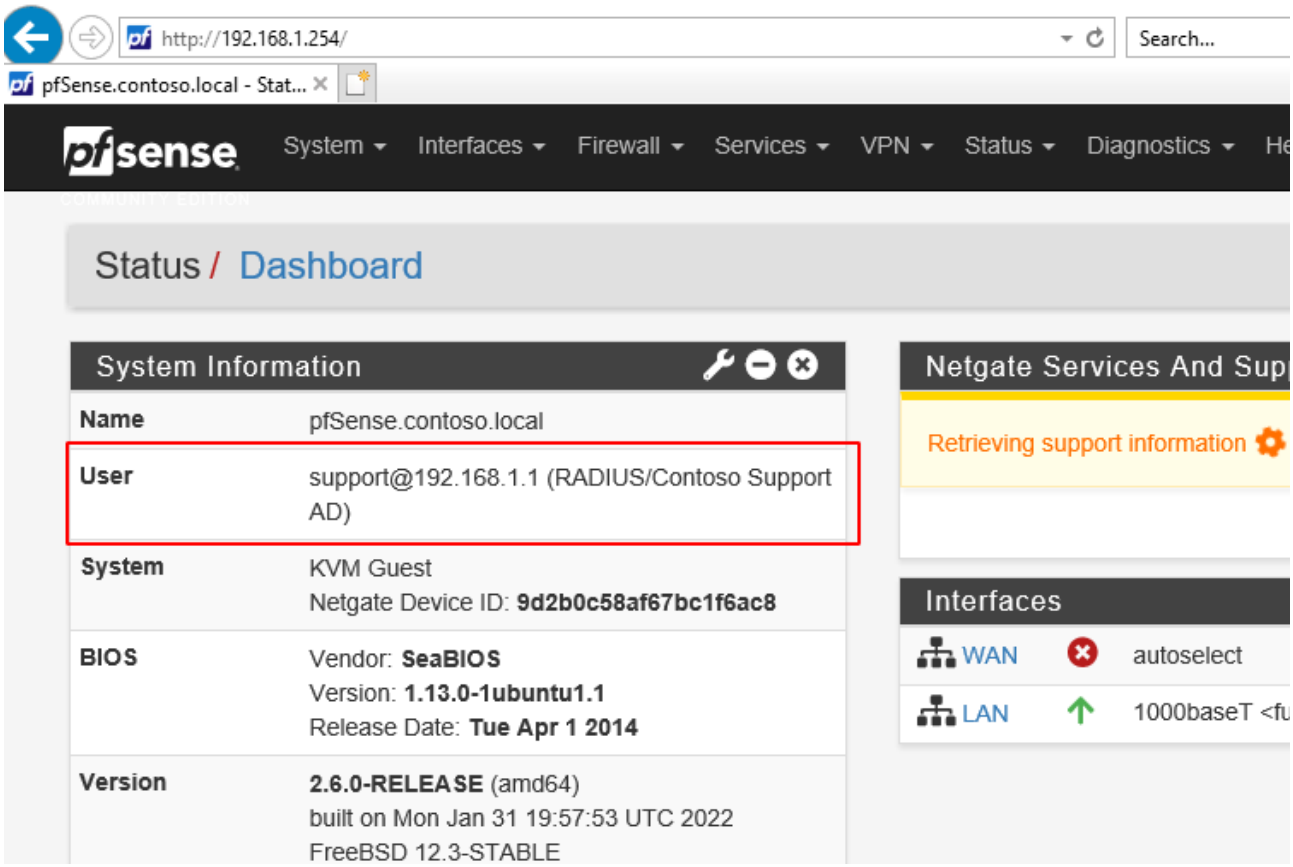

Figure 5.1 – pfSense showing Dashboard information with the support account.

NOTE: On DC1, you can open **Active Directory Users and Computers**, and then Browse to the **Users** container to find **Support** account. His group memberships will be displayed in the **Member Of** tab in the accounts properties.

2. Observe that you can configure most things but cannot adjust system settings to change the user accounts or root admin password.

Ideally, you would create role-based groups with more fine-grained privileges for different tasks.