Managing Centralized Authentication

(CompTIA Security + SY – 601)

Objectives:

- To implement authentication and authorization solution

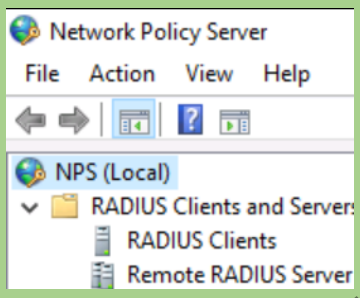
Resources:

- Windows VM (DC1)
- pfSense VM

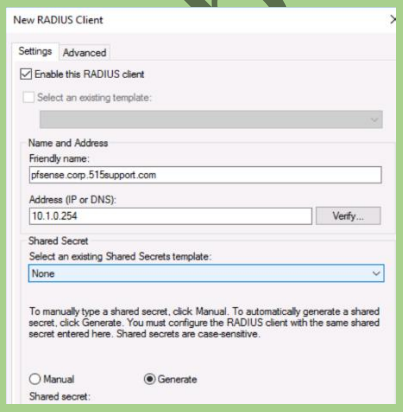
Instructions:

Register RADIUS client

- Log-in to DC1 VM
- In the Server Manager, select **Tools > Network Policy Server**
- Expand RADIUS Clients and Servers to select **RADIUS Clients**. Right-click **RADIUS Clients** and select New



- In the New RADIUS Client dialog box in the Friendly name box enter: **pfSense.corp.515support.com**
- In the address box, type **10.1.0.254**

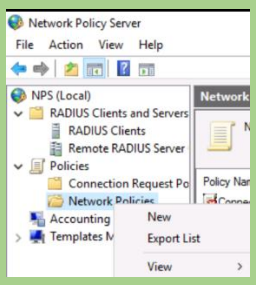


- Under Shaved Secret, Select the **Generate** radio button, then select the **Generate** button

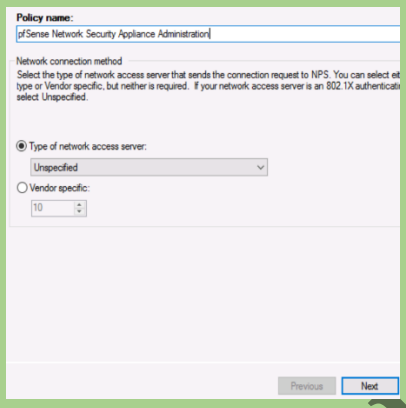
- Copy the shared secret string

Configure network policy

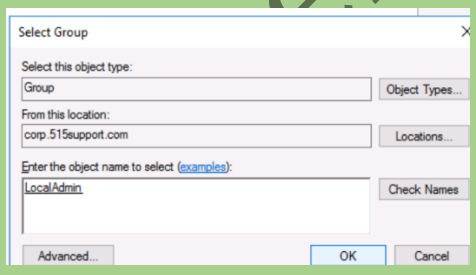
- In the Network Policy Server console, expand Policies to select **Network Policies**. Right-Click **Network Policies** and Select **New**



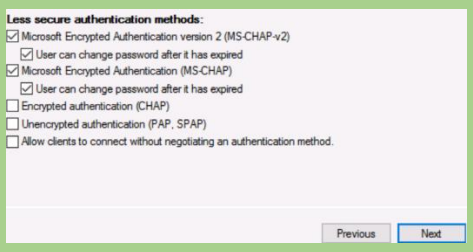
- In policy name, type pfSense Network Security Appliance Administration
- Select **Next**. On the Specify conditions page select the **Add** button



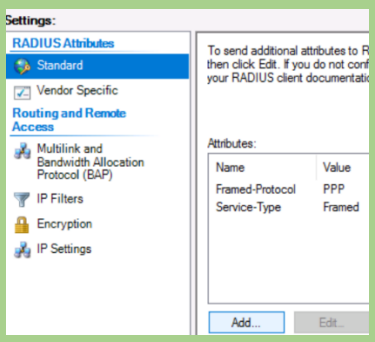
- Select **Windows Groups** and select **Add**
- Select the Add Groups button, then type **localadmin** and select Check Names
- Select OK then select OK again to confirm the Windows Group dialog box



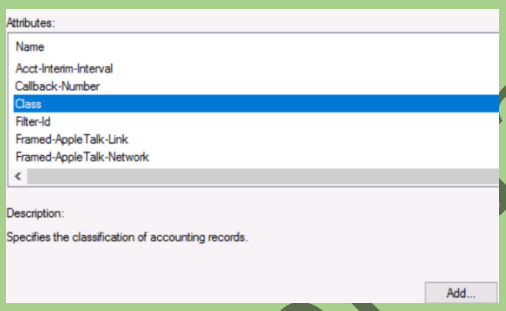
- Select **Next**
- On the Specify Access Permission page, leave **Access granted** selected and select **Next**
- On the Configure Authentication Methods page leave the existing MS-CHAPv2 and MS-CHAP boxes selected



- Select **Next**
- On the configure Constraints page, select **Next**
- On the configure Settings page, with **Standard** selected, select the **Add** button



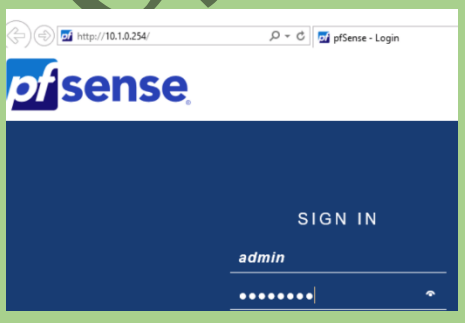
- In the Add Standard RADIUS Attribute dialog box from the Attributes box, select **Class**, select the **Add** button



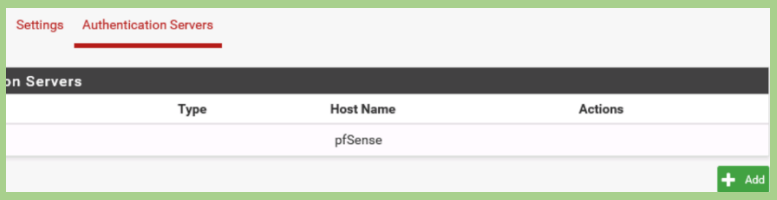
- Type **LocalAdmin** in the box and select **OK**. Select Close. pfSense uses the Class attribute to communicate group membership

Configure RADIUS client

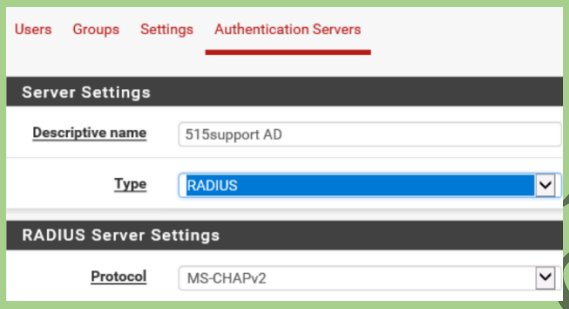
- Still on the DC1 VM, open https://10.1.0.254 in the browser



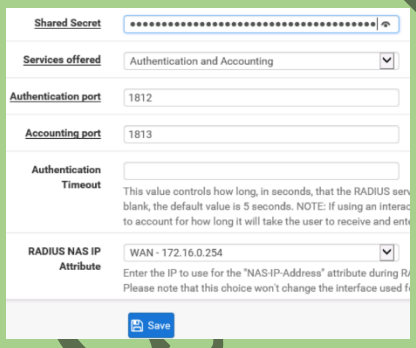
- Log on with the credentials: **admin** and **Pa$$w0rd**. When prompted to save the password, select **Not for the site**
- Maximize the browser window, select System > **User Manager**, Select the **Authentication Servers** tab, then select the **Add** button



- In the Descriptive name box, type **515supportAD**
- From the Type list, select RADIUS
- 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 client must be able to match at least one authentication method



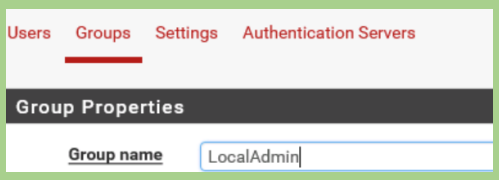
- In the **Hostname or IP address** box enter 10.1.0.1
- In the **Shared Secret** box paste the Clipboard contents



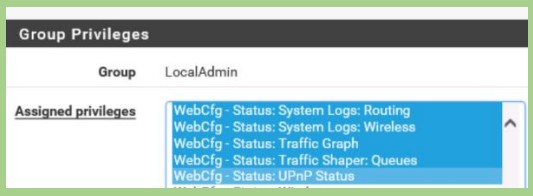
- Select the **Save** button

Configure role-based permission

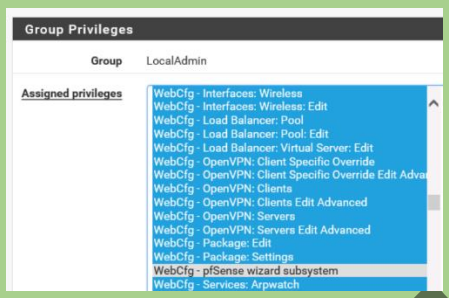
- Select the **Groups** tab, then select the **Add** button
- In the Group name box, type **LocalAdmin**



- Select the **Save** button
- In the **Actions** column, select the Edit group pen icon to edit the **LocalAdmin** group
- Under Assigned Privileges, select the **Add** button
- **SHIFT**-click to select from WebCfg-Dashboard (all) down to the last WebCg-Status: UPnP Status item.



- Locate the item WebCfg-pfSense wizard subsystem and **CTRL+click** to de-select it



- Select the **Save** button
- Select the Settings tab from the Authentication Server box, select **515supportAD**. Select the **Save** button

Test the Credentials

- Log back on with lobby and Password
- Observe that you can configure most things but cannot adjust system settings to change the user accounts or root admin password

Observations:

- **RADIUS Client Registration**:

- Registered pfSense as a RADIUS client on the DC1 VM.
- Generated and copied the shared secret string.

- **Network Policy Configuration**:

- Created a network policy for pfSense administration.
- Configured Windows Groups and access permissions.

- **RADIUS Client Configuration**:

- Configured RADIUS settings on pfSense.
- Set authentication server and shared secret.

- **Role-Based Permission Setup**:

- Created and assigned privileges to the LocalAdmin group on pfSense.

- **Credential Testing**:

- Tested login with lobby account.
- Verified restricted access to critical system settings.

Results:

- Successfully configured and tested centralized authentication with RADIUS and pfSense.
- Confirmed role-based permissions restricting access to sensitive settings.

Conclusion:

- Centralized authentication and role-based access control were implemented effectively.
- Demonstrated the importance of secure and structured user management.

Future Work:

- **Enhance Security Policies**:

- Regularly update and review authentication policies.

- **Regular Audits**:

- Perform periodic audits to ensure compliance and security.

- **User Training**:

- Train users on the importance of secure login practices.