pfSense admin logins via RADIUS using Active Directory Accounts

https://community.spiceworks.com/how_to/128944-pfsense-admin-logins-via-radius-using-active-directory-accounts

This guide will allow you to setup RADIUS authentication to log into your pfSense firewall.

It assumes you have already installed the Network Policy Server role. If you have not already installed this role, do this now through the Add Roles and Features Wizard. I usually install this role on a domain controller.

If a setting is not mentioned throughout this guide, leave the setting at its default.

This will only work on pfSense v 2.3.1 or later.

Section 1 is Windows configuration. Section 2 is pfSense configuration.

6 Steps total

Step 1: Section 1.1 Create an AD group

How to step

Image not found or type unknown

Expand

Create a new local group that will be used to grant members access to pfSense. Add the members who should have access.

I have called the group pfSense.

Step 2: Section 1.2 Network Policy Server RADIUS Clients

How to step

Image not found or type unknown

Expand

First we need to define a new RADIUS client. pfSense will be the client that queries active directory (via RADIUS) to authenticate the login. The RADIUS client and server use a matching key pair to authenticate communication with each other.

-Server Manager – Tools – Network Policy Server – RADIUS Clients and Servers – RADIUS Clients – Action - New

-Settings tab --Friendly name: Enter a name for this client. I have used the DNS name of the firewall. --Address: Enter the IP address of your pfSense firewall --Select an existing Shared Secrets template: None --Generate: Generate a shared secret and copy this to notepad, we will need this again later. --Click OK to finish.

Step 3: Section 1.3 Network Policy Server Network Policies

How to step

Image not found or type unknown

Expand

Create the policy used to grant access to members of the AD group.

-Server Manager – Tools – Network Policy Server – Policies – Network Policies – Action – New

This starts the New Network policy wizard

-Specify Name and connection type --Policy Name: Enter a name for the policy. I have used ‘shr-gw1 Policy’. --Type of network access server: Unspecified --Next

-Specify Conditions --Add.. – Windows Groups – [select the group you created] --Add.. – Client IPv4 Address – [enter the IP address of pfSense] --Next

-Specify Access Permission --Access granted --Next

-Configure Authentication Methods --Unencrypted authentication (PAP, SPAP) – enabled --All other types off -Next

-Configure Constraints --No changes --Next

-Configure Settings --RAIDUS Attributes – Standard – Add… - Class – Add… - String – [enter the name of the AD Group you created] – OK (Note: the class string will be parsed back to pfSense where a matching group name to this string must exist. For simplicity I have used the same group name in AD and in pfSense, therefore the Class string matches both)

--Next --Finish

Step 4: Section 2.1 Authentication Servers

How to step

Image not found or type unknown

Expand

Add the RADIUS server.

-pfSense – System – User Manager – Authentication Servers – Add --Descriptive Name: Name of the RADIUS Server --Type: RADIUS --Hostname or IP address: Enter the DNS name or IP address --Shared Secret: Enter the secret you copied to notepad in an earlier step --Services Offered: Authentication and Accounting --Save

Step 5: Section 2.2 Groups

How to step

Image not found or type unknown

Expand

Add a shadow group to pfSense with the same name as the AD group you created.

-pfSense – System – User Manager – Groups – Add --Group Name: [enter the same name as the AD group, this is where the class string parsed from the RADIUS server looks for this group name] --Scope: Local (I tested with Remote and it worked with that setting too) --Group membership: no members need to be added --Assigned Privileges – Add – ‘WebCfg - All pages’ --Save

Step 6: Section 2.3 Settings

How to step

Image not found or type unknown

Expand

Enable the RADIUS server as the authentication method

-pfSense – System – User Manager - Settings --Athentication Server: [choose your authentication server] --Save

You should now be able to add users to the AD group and login using your AD credentials with full access.

You can use this same method to create multiple groups in pfSense with various levels of access. To do this, create a new AD group, a new Network Server Policy with a different ‘Class’ string to parse back to pfSense, then create a pfSense group of the same name and give the group only access to the pages you wish them to have.

Revision #1
Created 5 January 2024 04:55:24 by ColtM
Updated 5 January 2024 04:55:53 by ColtM