GERENCIAMENTO DE USUÁRIOS E LDAP - PFSENSE

Responsável: João Pedro Toledo Gonçalves

Data: 26/01/2026

MANUAL TÉCNICO - GERENCIAMENTO DE USUÁRIOS E LDAP - PFSENSE

Código: ITGINF 0016/26 | **Classificação:** RESTRITO
Responsável: João Pedro Toledo Gonçalves | **Data:** 26/01/2026

1. HISTÓRICO DE REVISÃO

Data	Versão	Descrição	Autor
26/01/2026	**1.0**	**Criação Inicial**	**João Pedro Toledo Gonçalves**

2. OBJETIVO

Centralizar a autenticação de VPNs e acesso administrativo da WebGUI integrando o pfSense ao Active Directory (LDAP), eliminando a necessidade de criar usuários locais manualmente.

3. PRÉ-REQUISITOS

[ ] IP do Controlador de Domínio (DC).
[ ] Usuário de Serviço no AD (ex: `svc_pfsense`) com senha que não expira.
[ ] Grupo de Segurança no AD para Admins (ex: `G_TI_Admins`).

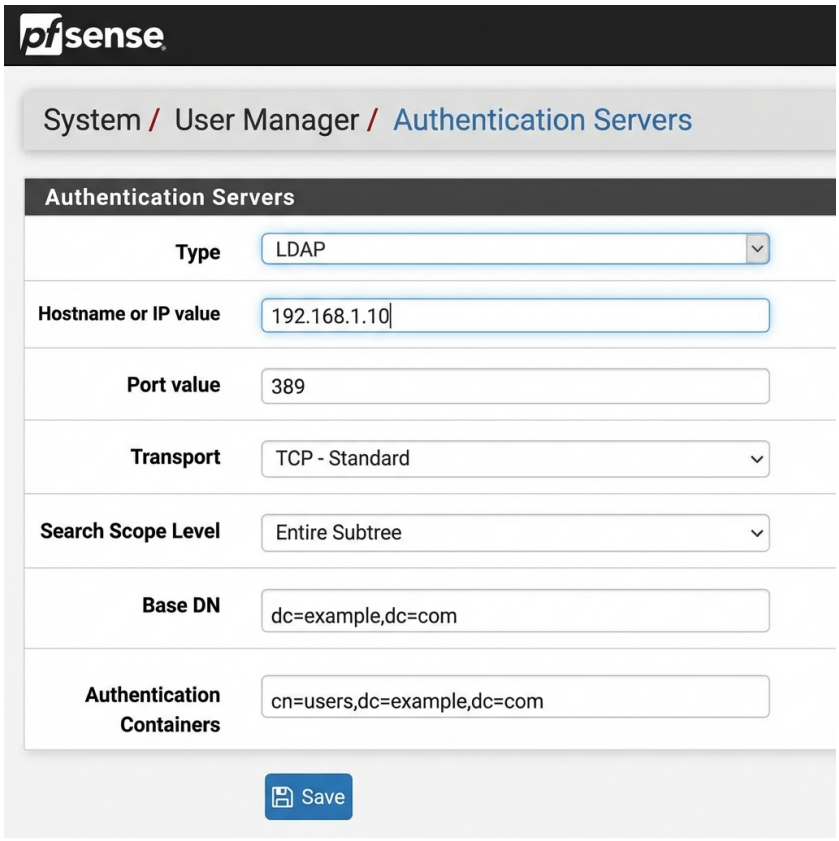
4. PASSO A PASSO (EXECUÇÃO)

Etapa 1: Configurar Servidor de Autenticação

1. [x] Acesse `System > User Manager > Authentication Servers`.
2. [x] Clique em **Add**.
3. [x] Preencha conforme abaixo:

• **Descriptive Name:** `AD_Principal`
• **Type:** `LDAP`
• **Hostname or IP address:** `{{IP_DC_PRINCIPAL}}` (ex: 192.168.0.10)
• **Port value:** `389` (TCP - Standard) ou `636` (SSL - Encrypted)
• **Transport:** `TCP - Standard` (Recomendado iniciar assim para teste, migrar para SSL depois).
• **Search Scope Level:** `Entire Subtree`
• **Base DN:** `{{BASE_DN}}` (ex: DC=itguys,DC=local).
• **Authentication Containers:** `{{USER_PC_CONTAINER}}` (ex: CN=Users,DC=itguys,DC=local).
• **Bind Credentials:**

- **User DN:** `CN=svc_pfsense,CN=Users,CD=itguys,DC=local`
- **Password:** Senha do usuário de serviço.
- **User Naming Attribute:** `samAccountName` (Padrão Microsoft AD).
- **Group Member Attribute:** `memberOf` (Padrão Microsoft AD).



4. [x] Clique em **Save**.

Etapa 2: Testar Autenticação

1. [x] Vá em `Diagnostics > Authentication`.
2. [x] Selecione o servidor `AD_Principal`.
3. [x] Digite um usuário e senha válidos do AD.
4. [x] Clique em **Test**.

- **Sucesso:** "User: johndoe authenticated successfully."
- **Falha:** Verifique logs em `Status > System Logs > Authentication`.

Etapa 3: Mapear Grupos e Permissões

Para que o usuário do AD possa logar na WebGUI, o grupo dele deve ter permissão no pfSense.

1. [x] Vá em `System > User Manager > Groups`.
2. [x] Crie um grupo **com o MESMO NOME** do grupo do AD (ex: `G_TI_Admins`).
3. [x] Em **Group Membership**, deixe vazio (os membros virão do AD).
4. [x] Clique em **Save**.
5. [x] Edite o grupo criado e vá em **Assigned Privileges**.

6. [x] Adicione a permissão `WebCfg - All pages` (para Admins).
7. [x] Salve.

Etapa 4: Configurar WebGUI para usar LDAP

1. [x] Vá em `System > User Manager > Settings`.
2. [x] Em **Authentication Server**, selecione `AD_Principal`.
3. [x] Salve e Teste.

5. SOLUÇÃO DE PROBLEMAS (TROUBLESHOOTING)

Problema 1: Erro "Bind failed"

- **Causa:** Usuário ou senha do Bind incorretos.
- **Solução:** Teste as credenciais do `svc_pfsense` com a ferramenta `ldp.exe` no Windows ou verifique se a conta não está bloqueada.

Problema 2: Usuário loga, mas vê "No page assigned to this user"

- **Causa:** O grupo do AD não foi criado no pfSense ou não tem privilégios.
- **Solução:** Revise etapa 3. O nome do grupo deve ser IDÊNTICO (Case Sensitive).

6. DADOS TÉCNICOS

Campo	Valor Recomendado	Descrição
LDAP Port	389 (Clear) / 636 (SSL)	Porta de conexão
Timeout	25	Tempo limite de conexão
Attribute	samAccountName	Identificador de Login AD

7. VALIDAÇÃO FINAL (DEFINIÇÃO DE PRONTO)

[ ] Teste de autenticação no Diagnostics OK?
[ ] Usuário do AD consegue logar na WebGUI?
[ ] Permissões administrativas aplicadas corretamente?