Es posible utilizar los usuarios creados en un servidor LDAP para autenticarse en PFSense de forma que podamos conectar, por ejemplo, esa autenticación contra un servidor OpenVPN corriendo en el propio PFSense. Lo hacemos de la siguiente manera:

Primero, y antes que nada, vamos a crear en el Windows Server un usuario específico para realizar consultas LDAP en el servidor de Active Directory, de forma que si nos hackean el PFSesne, no tengan los datos de la cuenta del Administrador del dominio. Abrimos PowerShell como Administrador y ejecutamos:

```
$Password = ConvertTo-SecureString "P@ssw0rd" -AsPlainText -Force
New-ADUser -Name "ConsultorLDAP" -SamAccountName "ConsultorLDAP" -UserPrincipalName "ConsultorLDAP@example.com" -
AccountPassword $Password -Enabled $true -CannotChangePassword $true -PasswordNeverExpires $true -Description
"Usuario para consultas LDAP"
```

Para diagnosticar si la conexión es correcta podemos hacerlo conectándonos mediante SSH al PFSense, tocando 8 (para la shell) y ejecutando:

```
ldapsearch -x -H ldap://IPDelWindowsServer:Puerto -D "CN=ConsultorLDAP,CN=Users,DC=dominio,DC=com" -w
"ContraseñaDelAdmin" -b "DC=dominio,DC=com" "(objectClass=user)"
```

...o podemos ir a la web de configuración de PFSense >> «Diagnostics» >> «Authentication», indicamos que el «Authentication server» sea el servidor LDAP que tenemos creado y le metemos como usuario ConsultorLDAP y contraseña P@ssw0rd

En la web de configuración de PFSense vamos a «System» >> «User manager», pestaña «Authentication Servers» y pinchamos en el botón «Add».

MODO NORMAL

- **Descriptive name:** Algo (Obligatorio)
- **Type:** LDAP
- **Hostname or IP address:** La IP del servidor LDAP (Debe ser accesible desde PFSense)
- **Transport:** Standard TCP (el puerto cambiará automáticamente a 389)
- **Search scope level:** Entire Subtree
- **Base DN:** DC=dominio,DC=com
- **Authentication containers:** CN=Users,DC=dominio,DC=com (Le damos al botón y lo seleccionamos).
- **Bind anonymous:** Desmarcado.
- **Bind Credentials:** Usuario y contraseña de una cuenta con permiso para realizar búsquedas LDAP en el AD.
- **UTF8 encode:** Marcado
- **Allow unauthenticated bind:** Marcado

NOTA

MODO PARANOICO

Este modo activa el cifrado SSL/TLS y sólo deja conectarse a los usuarios que pertenezcan al grupo UsuariosVPN.

- **Descriptive name:** Algo (Obligatorio)
- **Type:** LDAP
- **Hostname or IP address:** La IP del servidor LDAP (Debe ser accesible desde PFSense)

- **Transport:** SSL/TLS Encrypted (el puerto cambiará automáticamente a 636)
- **Search scope level:** Entire Subtree
- **Base DN:** DC=dominio,DC=com
- **Authentication containers:** CN=Users,DC=dominio,DC=com (Le damos al botón y lo seleccionamos).
- **Extended query:** Marcado.
- **Query:** memberOf=CN=UsuariosVPN,OU=Groups,DC=dominio,DC=com
- **Bind anonymous:** Desmarcado.
- **Bind Credentials:** CN=ConsultorLDAP,CN=Users,DC=dominio,DC=com
- **Contraseña:** Contraseña de la cuenta que hemos puesto arriba.
- **Group member attribute:** CN=UsuariosVPN,OU=Groups,DC=dominio,DC=com
- **UTF8 encode:** Marcado
- **Allow unauthenticated bind:** Marcado.

Ahora deberemos agregar el certificado del servidor Windows a nuestro PFSense. Entonces, primero, en el servidor de Active Directory, ejecutamos como Administrador lo siguiente:

```
# Instalar el rol de Servicios de Certificados
  Install-WindowsFeature ADCS-Cert-Authority -IncludeManagementTools
# Configurar la CA como CA raíz empresarial
  Install-AdcsCertificationAuthority -CAType EnterpriseRootCA -CryptoProviderName "RSA#Microsoft Software Key
Storage Provider" -KeyLength 8192 -HashAlgorithmName SHA512 -ValidityPeriod Years -ValidityPeriodUnits 5
# Cargar el módulo de AD CS
  Import-Module AdcsAdministration
# Conectar al servidor de certificación
  $ca = Get-CertificationAuthority
# Duplicar la plantilla "Autenticación de Servidor"
  $sourceTemplate = Get-CATemplate -Name "Server Authentication"
  $newTemplate = $sourceTemplate.Duplicate()
# Configurar la nueva plantilla
  $newTemplate.DisplayName = "LDAPs Certificate"
  $newTemplate.SubjectNameFormat = "CommonName"
  $newTemplate.ValidityPeriod = 2 # En años
  $newTemplate.RenewalPeriod = 1 # En años
  $newTemplate.Extensions["KeyUsage"].IncludeKeyEncipherment = $true
  $newTemplate.Extensions["KeyUsage"].IncludeDigitalSignature = $true

# Publicar la nueva plantilla
  Add-CATemplate $newTemplate

# Emitir un Certificado para el Controlador de Dominio
  # Nombre del certificado y controlador de dominio
    $FQDN = (Get-WmiObject Win32_ComputerSystem).Domain
    $Subject = "CN=$($env:COMPUTERNAME).$FQDN"
  # Solicitar el certificado
    $Request = New-SelfSignedCertificate -DnsName $FQDN -CertStoreLocation "Cert:\LocalMachine\My" -KeyUsage
KeyEncipherment, DigitalSignature -Type SSLServerAuthentication
  # Exportar el certificado para su uso
    Export-Certificate -Cert $Request -FilePath "C:\LDAPs_Certificate.cer"

# Configurar el Servidor LDAPs para Usar el Certificado
  Get-ChildItem Cert:\LocalMachine\My
# Configurar Active Directory para usar el certificado generado
  certutil -dsmanage -viewstore "ldap"
```

Exporta el certificado raíz desde el almacén de certificados:

$RootCert = Get-ChildItem Cert:\LocalMachine\Root | Where-Object {$_.Subject -like «*RootCA*»}
Export-Certificate -Cert $RootCert -FilePath «C:\RootCA.cer»

Importa el archivo RootCA.cer en PFSense como una CA confiable desde System > Cert Manager > CAs.

6. Verificar LDAPS

Para asegurarte de que LDAPS está funcionando correctamente, utiliza Test-LDAP desde un cliente o usa el siguiente comando:

Test-LDAP -Server $FQDN -Port 636

Si necesitas herramientas como ldp.exe, también puedes verificar la conexión manualmente.

También deberemos crear el grupo UsuariosVPN en el servidor de Windows. Lo hacemos ejecutando lo siguiente como Administradores en Powershell:

```
New-ADGroup -Name UsuariosVPN -GroupScope Global
```

.