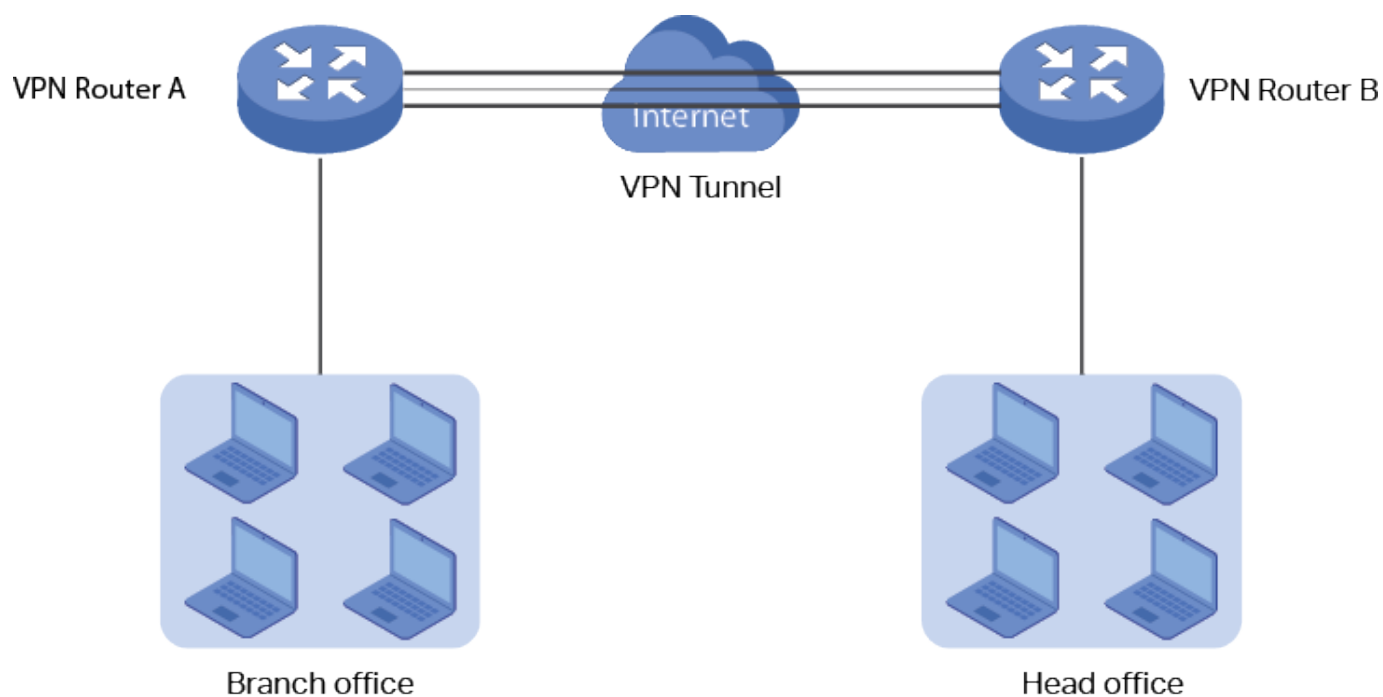


TP Tunnel Host To Lan IPsec & AD



Table des matières

1-	Création de l'autorité de certification	3
2-	VPN – IPSec.....	6
3-	Règles de Firewall	8
4-	Authentication AD dans le Pfsense	10
5-	L'UO Pfsense dans l'AD.....	11
6-	Test Final	12



1- Création de l'autorité de certification

Dans l'onglet Sytem/Certificate Manager/CAs on commence par le nommer et vérifier le Digest Algorithme (sha256) Pour une meilleure sécurité.

System / Certificate Manager / CAs / Edit

CAs

Certificates

Certificate Revocation

Create / Edit CA

Descriptive name

CAPFSENSE

Method

Create an internal Certificate Authority

Internal Certificate Authority

Key length (bits)

2048

Digest Algorithm

sha256

NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days)

3650

Common Name

PFSense-IPsec

The following certificate authority subject components are optional and may be left blank.

Country Code

None

State or Province

e.g. Texas

City

e.g. Austin

Organization

e.g. My Company Inc

Organizational Unit

e.g. My Department Name (optional)

Save

3

Nous allons ensuite dans l'onglet certificates ou l'ont précise autorité de certification ainsi que le nom du certificat.

CA's **Certificates** Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name LANPfsense10

Internal Certificate

Certificate authority CAPFSENSE

Key length 2048

Digest Algorithm sha256
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days) 3650

Common Name PFSense-ipsecd

The following certificate subject components are optional and may be left blank.

Country Code None

State or Province e.g. Texas

City e.g. Austin

Organization e.g. My Company Inc

Organizational Unit e.g. My Department Name (optional)

On choisi le type de certificat (ici « Server Certificate »)
Et enfin on ajoute l'adresse IP de la carte WAN du serveur.

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type Server Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names

Type	Value
IP address	10.12.1.20

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add + Add

Save

Puis on refait un autre certificat en entrant cette fois-ci l'adresse du second serveur.


Certificate Attributes


Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type Server Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names IP address 10.12.1.10
Type Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add 



On exporte ensuite le premier certificat vers le second serveur.

Certificat & Clé :



 LANPfSenseH.key	19/05/2021 10:58	Fichier KEY	2 Ko
 LANPfSenseH.crt	19/05/2021 10:58	Certificat de sécur...	2 Ko
 CAipsPfSense.crt	19/05/2021 10:58	Certificat de sécur...	2 Ko


Le certificat sur le second serveur :

System / Certificate Manager / CAs

CA's Certificates Certificate Revocation

Certificate Authorities





Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CAPFSENSE	✗	self-signed	1	CN=PFsense-20 Valid From: Wed, 19 May 2021 13:24:22 +0200 Valid Until: Sat, 17 May 2031 13:24:22 +0200	IPsec Tunnel	 




System / Certificate Manager / Certificates

CA's Certificates Certificate Revocation

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (608bfc4e8d69d) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-608bfc4e8d69d Valid From: Fri, 30 Apr 2021 14:47:10 +0200 Valid Until: Wed, 21 Oct 2026 14:47:10 +0200	webConfigurator	 
LANPfSense10 CA: No Server: Yes	CAPFSENSE	CN=PFsense-ipsec-10 <div>Serial: 1 Signature Digest: RSA-SHA256 SAN: DNS:PFsense-ipsec-10, IP Address:10.12.1.10 KU: Digital Signature, Key Encipherment EKU: TLS Web Server Authentication, IP Security IKE Intermediate</div> Valid From: Wed, 19 May 2021 13:26:03 +0200 Valid Until: Sat, 17 May 2031 13:26:03 +0200	IPsec Tunnel	 



2- VPN – IPSec

On se rend dans VPN/IPSec pour ajouter sur les deux serveurs Pfsense un tunnel pointant vers le réseau WAN de chacun.

On précise la version Key Exchange, la gateway du serveur distant, la méthode d'authentification (Mutual RSA) ainsi que le certificat précédemment créé et l'autorité de certification.

The screenshot displays the Pfsense VPN/IPSec configuration interface. At the top, there are tabs for 'Tunnels', 'Mobile Clients', 'Pre-Shared Keys', and 'Advanced Settings'. The 'Tunnels' tab is selected, showing a list of tunnels. Below this, the 'General Information' section is expanded, showing fields for 'Disabled' (a checkbox), 'Key Exchange version' (set to IKEv2), 'Internet Protocol' (set to IPv4), 'Interface' (set to WAN), 'Remote Gateway' (set to 10.12.1.20), and 'Description' (set to Tunnel). Below the 'General Information' section, the 'Phase 1 Proposal (Authentication)' section is expanded, showing fields for 'Authentication Method' (set to Mutual RSA), 'My identifier' (set to My IP address), 'Peer identifier' (set to Peer IP address), 'My Certificate' (set to LANPfsense10), and 'Peer Certificate Authority' (set to CAPFSENSE).

General Information	
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
Key Exchange version	IKEv2 Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.
Internet Protocol	IPv4 Select the Internet Protocol family.
Interface	WAN Select the interface for the local endpoint of this phase1 entry.
Remote Gateway	10.12.1.20 Enter the public IP address or host name of the remote gateway.
Description	Tunnel A description may be entered here for administrative reference (not parsed).

Phase 1 Proposal (Authentication)	
Authentication Method	Mutual RSA Must match the setting chosen on the remote side.
My identifier	My IP address
Peer identifier	Peer IP address
My Certificate	LANPfsense10 Select a certificate previously configured in the Certificate Manager.
Peer Certificate Authority	CAPFSENSE Select a certificate authority previously configured in the Certificate Manager.

On reproduit ensuite la même manipulation sur le second serveur.

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Disabled ☐ Set this option to disable this phase1 without removing it from the list.

Key Exchange version IKEv2
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol IPv4
Select the Internet Protocol family.

Interface WAN
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway 10.12.1.10
Enter the public IP address or host name of the remote gateway.

Description Tunnel
A description may be entered here for administrative reference (not parsed).

Phase 1 Proposal (Authentication)

Authentication Method Mutual RSA
Must match the setting chosen on the remote side.

My identifier My IP address

Peer identifier Peer IP address

My Certificate LANPfsense20
Select a certificate previously configured in the Certificate Manager.

Peer Certificate Authority CAPFSENSE
Select a certificate authority previously configured in the Certificate Manager.

Puis on créer une « Phase » sur chacun des serveurs.

VPN / IPsec / Tunnels / Edit Phase 2

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Disabled ☐ Disable this phase 2 entry without removing it from the list.

Mode Tunnel IPv4

Local Network LAN subnet / 0
Type Address
Local network component of this IPsec security association.

NAT/BINAT translation None / 0
Type Address
If NAT/BINAT is required on this network specify the address to be translated

Remote Network Network 192.168.1.0 / 24
Type Address
Remote network component of this IPsec security association.

Description LAN
A description may be entered here for administrative reference (not parsed).

3- Règles de Firewall

Sur les deux serveurs on ouvre les ports any-any-any pour les règles WAN/LAN et IPSec.

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match.

any

Source Address

/

Destination

Destination

☐ Invert match.

any

Destination Address

/

Les règles :

Firewall / Rules / WAN

Floating

WAN

LAN

IPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	1/106 KiB	IPv4 *	*	*	*	*	none			Anchor Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

Floating

WAN

LAN

IPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	1/29.52 MiB	*	*	LAN Address	443	*	*		Anti-Logout Rule	Edit
<input type="checkbox"/>	✓	2/34 KiB	IPv4 *	*	*	*	*	none			Anchor Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

Firewall / Rules / IPsec

Floating

WAN

LAN

IPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	*	*	*	*	none			Anchor Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

Pour que tout fonctionne nous avons dû ouvrir le port 500 sur le routeur.
le pare-feu (pour équipements IPv6).

TCP ▼



pfSense ▼

Toutes

Créer

00

IP externes autorisées

	Port	Protocole	Équipement	Adresse IP externe	
	500	UDP/TCP	pfSense	Toutes	
	500	UDP/TCP	pfSense-1	Toutes	

4- Authentication AD dans le Pfsense

On indique dans la configuration d'authentification du serveur l'adresse IP de ce dernier ainsi que le Bind Crédential qui permettra au Pfsense de s'authentifier dans l'AD, l'authentification containers où l'ont indique l'OU qu'il utilisera pour identifier les utilisateurs et enfin le certificat.

The screenshot shows the PfSense web interface for configuring an LDAP authentication server. The breadcrumb trail is System / User Manager / Authentication Servers / Edit. The 'Authentication Servers' tab is selected. The configuration is divided into 'Server Settings' and 'LDAP Server Settings'.

Server Settings

- Descriptive name:** WinServAD
- Type:** LDAP

LDAP Server Settings

- Hostname or IP address:** 10.0.0.201
NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.
- Port value:** 389
- Transport:** Standard TCP
- Peer Certificate Authority:** CA-Me
This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.
- Protocol version:** 3
- Server Timeout:** 25
Timeout for LDAP operations (seconds)
- Search scope:** Level
Entire Subtree
- Base DN:** DC=rah, DC=local
- Authentication containers:** OU=pfsense,DC=rah,DC=local
Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users,DC=example,DC=com or OU=Staff,OU=Freelancers
- Extended query:** ☐ Enable extended query
- Bind anonymous:** ☐ Use anonymous binds to resolve distinguished names
- Bind credentials:** CN=Administrateur,CN=Users,DC=rah,DC=local
- User naming attribute:** cn
- Group naming attribute:** cn
- Group member attribute:** memberOf
- RFC 2307 Groups:** ☐ LDAP Server uses RFC 2307 style group membership
RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).
- Group Object Class:** posixGroup
Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".
- Shell Authentication Group DN:**
If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login. Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com
- UTF8 Encode:** ☐ UTF8 encode LDAP parameters before sending them to the server.
Required to support international characters, but may not be supported by every LDAP server.
- Username Alterations:** ☐ Do not strip away parts of the username after the @ symbol
e.g. user@host becomes user when unchecked.
- Allow unauthenticated bind:** ☒ Allow unauthenticated bind
Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.

At the bottom, there is a 'Save' button.

5- L'UO Pfsense dans l'AD

Nous pouvons voir ici les utilisateurs dans l'UO utilisé par Pfsense pour accorder l'accès au Vpn.

The screenshot shows the Windows Server Management console. The left sidebar indicates the path: **Gestionnaire de serveur** > **Services Bureau à distance** > **Collections** > **RDP/TSE**. The main area is divided into several panes:

- PROPRIÉTÉS**: Shows properties for the collection, including 'Session' (Programmes RemoteApp) and 'Groupe d'utilisateurs' (RAH.Utilisateurs du domaine).
- PROGRAMMES REMOTEAPP**: A table with columns 'Nom du programme RemoteApp', 'Alias', and 'Visible dans l'Accès'. It lists 'Connexion Bureau à distance' with alias 'mstsc' and 'Oui'.
- SERVEURS HÔTES**: A table with columns 'Nom du serveur', 'Type', 'Bureaux virtuels', and 'Autoriser les nouvelles collections'. It lists 'WINSERV16' as a 'Hôte de session Bureau à distance' with 'N/A' for virtual desktops and 'Vrai' for allowing new collections.
- Utilisateurs et ordinateurs Active Directory**: A window showing a list of users. The table has columns 'Nom', 'Type', and 'Description'. The users listed are: alexandre (Utilisateur), didier (Utilisateur), Hugo (Utilisateur), Rayan (Utilisateur), and test (Utilisateur).
- CONNEXIONS**: A pane showing connection details, including a filter and a table with columns: État de la session, Heure d'ouverture de session, Heure de déconnexion, and Durée d'inactivité.

6- Test Final

Nous pouvons enfin tester la connectivité entre les deux Pfsense :

Status / IPsec / Overview

Overview

Leases

SADs

SPDs

IPsec Status

IPsec ID	Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
con1000: #1	Tunnel	10.12.1.10	10.12.1.10	10.12.1.20	10.12.1.20	IKEv2 responder	27079 seconds (07:31:19)	AES_CBC HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	ESTABLISHED 986 seconds (00:16:26) ago <div>Disconnect</div>

Show child SA entries

Status / IPsec / Overview

Overview

Leases

SADs

SPDs

IPsec Status

IPsec ID	Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
con1000: #1	Tunnel	10.12.1.20	10.12.1.20	10.12.1.10	10.12.1.10	IKEv2 initiator	26519 seconds (07:21:59)	AES_CBC HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	ESTABLISHED 1006 seconds (00:16:46) ago <div>Disconnect</div>

Show child SA entries

Diagnostics / Authentication

User hugo authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server

LDAP DC1

Select the authentication server to test against.

Username

hugo

Password

Test

12