

Compte rendu technique
BTS SIO 2 – Année 2024-2025



1. Contexte de l'infrastructure

Ce projet consiste à mettre en place un serveur NTP interne basé sur pfSense. L'objectif est de fournir une synchronisation horaire fiable et identique pour tous les équipements du réseau : serveur Active Directory, serveur de fichiers, postes clients et switch Cisco. Une heure cohérente est indispensable au fonctionnement correct du domaine Active Directory, des journaux d'événements (logs) et de la sécurité réseau.

2. Tableau d'adressage

Ce tableau résume les adresses IP des équipements impliqués dans la synchronisation NTP.

Nom de l'équipement	Adresse IP	Masque	Passerelle
DEBIAN CLIENT	192.168.1.30	255.255.255.0	192.168.1.254
DEBIAN SRV	192.168.1.20	255.255.255.0	192.168.1.254
Oscar-GLPI	192.168.1.223	255.255.255.0	192.168.1.254
PC-CLIENT 1	192.168.2.10	255.255.255.0	192.168.1.254
PFsense	192.168.1.254	255.255.255.0	192.168.1.254
WIN-SRV-FICHER	192.168.1.2	255.255.255.0	192.168.1.254
WinSRV	192.168.1.10	255.255.255.0	192.168.1.254
Switch Externe	192.168.1.1	255.255.255.0	192.168.1.254

3. Pré-requis

- pfSense fonctionnel et accessible via son interface web.
- Un serveur Windows jouant le rôle de contrôleur de domaine.
- Postes clients intégrés au domaine.
- Switch Cisco accessible en CLI.
- Droits administrateur sur tous les systèmes.

4. Configuration NTP sur pfSense

Cette étape consiste à configurer pfSense pour qu'il agisse en tant que serveur NTP.

1. Aller dans Services → NTP.
2. Cocher « Enable NTP Server ».
3. Interface(s) → sélectionner LAN.
4. Ajouter les serveurs externes suivants :
 - 0.pool.ntp.org
 - 1.pool.ntp.org
 - 2.pool.ntp.org
5. Sauvegarder et appliquer.

NTP Server Configuration

Enable Enable NTP Server
You may need to disable NTP if pfSense is running in a virtual machine and the host is responsible for the clock.

Interface WAN
LAN
VLAN61
Localhost
Interfaces without an IP address will not be shown.
Selecting no interfaces will listen on all interfaces with a wildcard.
Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.

Time Servers	Prefer	No Select	Authenticated	Type	Delete
<input type="text" value="0.pool.ntp.org"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Pool	<input type="button" value="Delete"/>
<input type="text" value="1.pool.ntp.org"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Pool	<input type="button" value="Delete"/>
<input type="text" value="2.pool.ntp.org"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Pool	<input type="button" value="Delete"/>

Add

Active Windows

5. Configuration du pare-feu pfSense

Il est essentiel d'autoriser les clients à contacter pfSense via le port UDP 123.

Étapes :

1. Aller dans Firewall → Rules → LAN.
2. Ajouter une règle en haut de liste.
3. Action : Pass – Protocole : UDP.
4. Source : LAN net.
5. Destination : This Firewall (self).
6. Port : 123.
7. Sauvegarder et appliquer.

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 LAN
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 UDP
Choose which IP protocol this rule should match.

Source

Source Invert match LAN address Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Activer Windows

Projet AP2 – Serveur NTP interne

Destination	
Destination	<input type="checkbox"/> Invert match Any Destination Address /
Destination Port Range	From: NTP (123) Custom To: NTP (123) Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.	
Extra Options	
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	Autoriser à interroger NTP A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.
Advanced Options	Display Advanced
Rule Information	
Tracking ID	1762199588
Created	11/3/25 20:53:08 by admin@192.168.1.10 (Local Database)
Updated	11/3/25 20:53:08 by admin@192.168.1.10 (Local Database)

6. Configuration du contrôleur de domaine (AD)

Le contrôleur de domaine doit utiliser pfSense comme source de temps. Exécuter dans PowerShell (administrateur) :

```
w32tm /config /manualpeerlist:"192.168.1.254" /syncfromflags:manual /reliable:yes  
/update  
Restart-Service w32time  
w32tm /resync
```

Projet AP2 – Serveur NTP interne

```
PS C:\Users\Administrateur> w32tm /config /manualpeerlist:"192.168.1.254" /syncfromflags:manual /reliable:yes /update
La commande s'est terminée correctement.
PS C:\Users\Administrateur> restart-service w32time
PS C:\Users\Administrateur> w32tm /query /status
Indicateur de dérive : 0(Aucun avertissement)
Couche : 3 (Référence secondaire, synchronisée par (S)NTP)
Précision : -23 (119.209ns par battement)
Délai de racine : 0.0141369s
Dispersion de racine : 7.7793647s
ID de référence : 0xC0A801FE (IP de la source : 192.168.1.254)
Heure de la dernière synchronisation réussie : 13/11/2025 22:27:26
Source : 192.168.1.254
Intervalle d'interrogation : 6 (64s)

PS C:\Users\Administrateur> w32tm /query /source
192.168.1.254
PS C:\Users\Administrateur> w32tm /query /peers
Nb d'homologues : 1

Homologue : 192.168.1.254
État : Actif
Temps restant : 28.3716747s
Mode : 1 (Actif symétrique)
Couche : 2 (Référence secondaire, synchronisée par (S)NTP)
HomologueIntervalle d'interrogation : 15 (32768s)
HôteIntervalle d'interrogation : 6 (64s)
PS C:\Users\Administrateur>
```

Activer Windows
Accédez aux paramètres pour activer Windows.

7. Clients Windows

Les clients récupèrent l'heure du contrôleur de domaine.
Pour forcer une mise à jour :

```
gpupdate /force
w32tm /resync
w32tm /query /source
```

Projet AP2 – Serveur NTP interne

```
PS C:\Windows\system32> gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

PS C:\Windows\system32> w32tm /resync
Envoi de la commande de resynchronisation à l'ordinateur local
La commande s'est terminée correctement.
PS C:\Windows\system32> w32 /query /status
w32 : Le terme «w32» n'est pas reconnu comme nom d'applet de commande, fonction, fichier de script ou programme
exécutable. Vérifiez l'orthographe du nom, ou si un chemin d'accès existe, vérifiez que le chemin d'accès est correct
et réessayez.
Au caractère ligne:1 : 1
+ w32 /query /status
+ ~~~~
+ CategoryInfo          : ObjectNotFound: (w32:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Windows\system32> w32tm /query /status
Indicateur de dérive : 0(Aucun avertissement)
Couche : 4 (Référence secondaire, synchronisée par (S)NTP)
Précision : -23 (119.209ns par battement)
Délai de racine : 0.0173042s
Dispersion de racine : 9.8967080s
ID de référence : 0xC0A8010A (IP de la source : 192.168.1.10)
Heure de la dernière synchronisation réussie : 13/11/2025 22:33:56
Source : WIN-U7ENPFI6E6A.FRANCOIS.LOCAL
Intervalle d'interrogation : 10 (1024s)

PS C:\Windows\system32> w32tm /query /source
WIN-U7ENPFI6E6A.FRANCOIS.LOCAL
PS C:\Windows\system32>
```

Activer Window
Accédez aux paramè
Windows.

9. Configuration du switch Cisco

Configurer pfSense comme serveur NTP :

```
conf t
ntp server 192.168.1.254
end
write memory
```

Vérifications : show ntp status / show ntp associations

```
SW-OSCAR#show clock
21:44:30.645 UTC Thu Nov 13 2025
SW-OSCAR#show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.254
nominal freq is 119.2092 Hz, actual freq is 119.2080 Hz, precision is 2**18
reference time is ECC0CEF1.6D0D5AE3 (21:41:05.425 UTC Thu Nov 13 2025)
clock offset is 0.2294 msec, root delay is 15.34 msec
root dispersion is 3.33 msec, peer dispersion is 0.32 msec
SW-OSCAR#show ntp associations

      address          ref clock      st  when  poll reach  delay  offset  disp
*~192.168.1.254      79.143.250.33   2   232  1024  377    1.4   0.23   0.3
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
SW-OSCAR#
```

10. Vérifications globales

Sur pfSense : ntpq -p

Sur Windows : w32tm /query /status

Sur Cisco : show ntp status

```
PS C:\Users\Administrateur> w32tm /config /manualpeerlist:"192.168.1.254" /syncfromflags:manual /reliable:yes /update
La commande s'est terminée correctement.
PS C:\Users\Administrateur> restart-service w32time
PS C:\Users\Administrateur> w32tm /query /status
Indicateur de dérive : 0(Aucun avertissement)
Couche : 3 (Référence secondaire, synchronisée par (S)NTP)
Précision : -23 (119.209ns par battement)
Délai de racine : 0.0141369s
Dispersion de racine : 7.7793647s
ID de référence : 0xC0A801FE (IP de la source : 192.168.1.254)
Heure de la dernière synchronisation réussie : 13/11/2025 22:27:26
Source : 192.168.1.254
Intervalle d'interrogation : 6 (64s)

PS C:\Users\Administrateur> w32tm /query /source
192.168.1.254
PS C:\Users\Administrateur> w32tm /query /peers
Nb d'homologues : 1

Homologue : 192.168.1.254
État : Actif
Temps restant : 28.3716747s
Mode : 1 (Actif symétrique)
Couche : 2 (Référence secondaire, synchronisée par (S)NTP)
HomologueIntervalle d'interrogation : 15 (32768s)
HôteIntervalle d'interrogation : 6 (64s)
PS C:\Users\Administrateur>
```

Activer Windows
Accédez aux paramètres pour activer Windows.

11. Conclusion

La mise en place de ce serveur NTP interne permet de centraliser la distribution de l'heure au sein de l'infrastructure. Tous les équipements (pfSense, contrôleur de domaine, postes clients et switch Cisco) sont désormais synchronisés sur une même source fiable.

Cette synchronisation garantit un fonctionnement cohérent des services Active Directory, des journaux d'événements et des équipements réseau, tout en restant simple à administrer. La solution retenue, basée sur pfSense, est adaptée à un contexte professionnel et constitue une base solide pour de futures évolutions de l'infrastructure.