

Construire un réseau informatique pour une petite structure

Le but de cette SAE est de construire un réseau informatique pour une petite entreprise. Pour ce faire nous allons utiliser gns3 pour simuler notre réseau et suivre les étapes suivante:

Configuration du routages inter-vlan.....	2
Configuration des commutateurs:.....	2
Configuration des vlans sous pfsense :.....	3
Configuration du dhcp sous pfsense.....	5
la plage d'adresse ip :.....	5
Attribution des adresses aux sous-interfaces.....	5
Activations du service DHCP :.....	6
Création de la DMZ.....	8
Création de l'interface:.....	8
Plan d'adressage de la DMZ:.....	8
Configuration du serveur FTP et WEB.....	9
configuration basique du serveur Proftpd :.....	9
mise en place des droits :.....	9
Installation minimal du serveur WEB :.....	10
Configuration de la deuxième sucursal.....	11
plage d'adresse ip :.....	11
Réutilisation de la première sucursal :.....	11
Mise en place des routes statiques :.....	11
Configuration vpn IPsec.....	13
Mise en place de IPsec:.....	13
Les règles de pare feux IPsec:.....	15
Configuration du pare-feu.....	17
Annexe.....	18
Topologie complète:.....	18
Scripte bash pour ajouter un utilisateur:.....	19

Configuration du routages inter-vlan

Configuration des commutateurs:

mise en place des vlans :

La réalisation ne diffère pas de Packet Tracer.

On peut commencer la configuration des Vlans et ça commence par leur donner un nom.

Vlan 10	Gi1/0-3
Vlan 20	Gi2/0-3
Vlan 30	Gi2/0-3

exemple de configuration:

```
switch(config)#vlan 10  
switch(config-vlan)#name commercial
```

Par la suite, nous avons attribué des interfaces aux Vlans.

Vlan 10	commercial
Vlan 20	gestion
Vlan 30	direction

exemple de configuration:

```
switch#config terminal  
switch(config)#interface range gi1/0-3  
switch(config-if-range)#switchport mode access  
switch(config-if-range)#no shutdown
```



la procédure est à réaliser sur tous les commutateurs.

Mise en place des trunk :

Pour les commutateurs :

Comme nous pouvons le voir les interfaces gi0/0,gi0/1 sur commutateur 1 et l'interface gi0/1 du commutateur 2 seront en mode trunk. On procède de la manière suivante.

```
switch(config)#interface <num interface>
switch(config-if)#switchport trunk encapsulation dot1q
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk allowed vlan 10,20,30
switch(config-if-range)#no shutdown
```

Configuration des vlans sous pfsense :

Pour faire cette opération, nous avons besoin d'accéder à l'interface web de pfsense.

login: admin

password: pfsense

Pour commencer, nous allons dans **interface > assignment**.

On active l'interface em2 puis nous allons dans la section vlan.

Une fois dans cette section, on clique sur **add**.

VLAN Configuration	
Parent Interface	<input type="text" value="em2 (0c:99:48:79:00:02) - opt1"/>
Only VLAN capable interfaces will be shown.	
VLAN Tag	<input type="text" value="10"/>
802.1Q VLAN tag (between 1 and 4094).	
VLAN Priority	<input type="text" value="0"/>
802.1Q VLAN Priority (between 0 and 7).	
Description	<input type="text" value="VLAN 10"/>
A group description may be entered here for administrative reference (not parsed).	









le numéro d'interface doit correctement être choisi lors de l'ajout de la vlan

On obtient le résultat suivant:




[Interface Assignments](#)
[Interface Groups](#)
[Wireless](#)
[VLANs](#)
[QinQs](#)
[PPPs](#)
[GREs](#)
[GIFs](#)
[Bridges](#)
[LAGGs](#)

VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions
em2 (opt1)	10		VLAN 10	 
em2 (opt1)	20		VLAN 20	 
em2 (opt1)	30		VLAN 30	 

Pour terminer, on repart dans **interfaces > assignment** et on rajoute des sous-interfaces.

On obtient le résultat ci-dessous.

Vlan10	VLAN 10 on em2 - opt1 (VLAN 10)	 Delete
Vlan20	VLAN 20 on em2 - opt1 (VLAN 20)	 Delete
Vlan30	VLAN 30 on em2 - opt1 (VLAN 30)	 Delete

La configuration du routage inter-vlan est terminée, mais il n'est pas encore fonctionnel.

Dans la prochaine partie, nous allons le rendre fonctionnel.

Pour ce faire nous allons mettre en place une plage d'adresse IPv4, attribuer une adresse aux sous interfaces de em2 et utiliser un serveur DHCP.

Configuration du dhcp sous pfsense

la plage d'adresse ip :

Pour cette étape, nous allons utiliser la méthode VLSM "Variable Length Subnet Mask".

Adresse réseau selon les vlan :

Vlan 10	172.22.1.0/27
Vlan 20	172.22.1.32/28
Vlan 30	172.22.1.48/29

Plage d'adresse valide par sous-réseaux :

adresse de réseau	plage valide	broadcast
172.22.1.0/27	172.22.1.1 / 172.22.1.30	172.22.1.31
172.22.1.32/28	172.22.1.33 / 172.22.1.46	172.22.1.47
172.22.1.48/29	172.22.1.49 / 172.22.1.54	172.22.1.55

Attribution des adresses aux sous-interfaces

Avec le terminal de pfsense :

Pour commencer la configuration choisit l'option 2 (set interfaces IP address)

```

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

```

On choisit le numéro de l'une des sous interface

```

7 - VLAN10 (em2.10
8 - VLAN20 (em2.20
9 - VLAN30 (em2.30

```

Par la suite on peut suivre les étapes suivantes:

- attribution de l'adresse
- choix du masque
- le reste ne nous intéresse. On passe à l'action suivante ou on choisit **no** si on a la possibilité.

Avec l'interface web de pfsense :

Il nous suffit d'aller sur l'interface web de pfsense, de sélectionner l'interface qui nous intéresse et de lui attribuer une ip.

General Configuration

Enable

☒ Enable interface

Description

Vlan10

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

Static IPv4 Configuration

IPv4 Address

172.22.1.1

/ 27

IPv4 Upstream gateway

None

+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

Activations du service DHCP :

Maintenant que nous avons attribué nos adresses au sous interfaces, on va pouvoir activer le service dhcp.

Pour ce faire nous allons sur l'interface web de pfsense. Puis dans le menu nous allons sélectionner **Service > DHCP server**.

On peut désormais activer le DHCP server sur les interfaces de nos VLAN en cochant la case **Enable DHCP server on VLAN"num vlan" interface**.

General Options

Enable ☒ Enable DHCP server on VLAN10 interface

Et enfin on définit le pool d'adresse.

Subnet	172.22.1.0	
Subnet mask	255.255.255.224	
Available range	172.22.1.1 - 172.22.1.30	
Range	<input type="text" value="172.22.1.2"/> From	<input type="text" value="172.22.1.30"/> To



Il faut faire attention à ne pas mettre l'adresse de l'interface dans le pool.

Il est important de souligner que nous avons choisi d'utiliser cette méthode pour la SAE 201 afin d'éviter toute coupure de service en cas de problème lié au serveur DHCP. Pour la deuxième succursale, cette méthode rend également les tests plus faciles. Cependant, il est également possible de configurer un serveur DHCP séparé et d'utiliser le pfsense comme relais DHCP.

Création de la DMZ

Création de l'interface:

Dans cette partie, nous allons simplement créer la DMZ.

Cette zone sera chargé d'accueillir notre serveur WEB,FTP et DNS (si disponible)

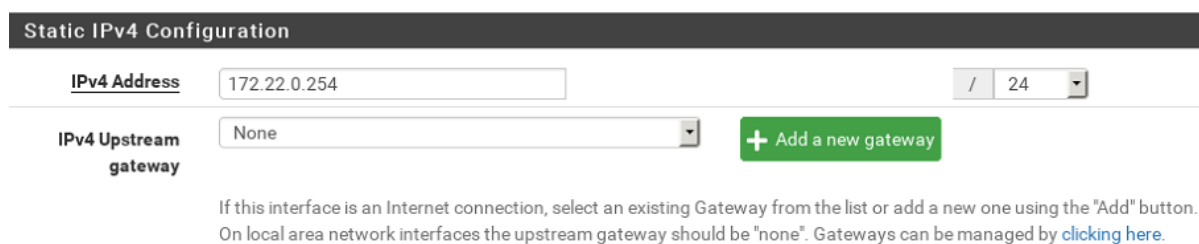
On ne va pas procéder à la configuration du pare-feu pour faciliter les tests.

On peut passer par l'interface web pour la création de la DMZ.

Pour ce faire, nous allons prendre l'une de nos interfaces non utilisées. On doit simplement l'activer et changer sa description pour qu'elle soit le plus clair pour nous.

Mais le plus important est son adresse IP. Pour simplifier la compréhension nous avons décidé de ne pas être dans le réseau 172.22.1.0/24, mais dans le réseau 172.22.0.0/24. Le but est simplement de mieux se repérer.

On à donc la configuration suivante.



Static IPv4 Configuration

IPv4 Address: 172.22.0.254 / 24

IPv4 Upstream gateway: None [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

Il aurait été possible de configurer la sécurité des commutateurs en utilisant la méthode VSM (Virtual Switching System). Cependant, nous avons décidé de ne pas l'utiliser pour le moment, car nous ne connaissons pas exactement les exigences de la SAE en matière de fourniture du serveur DNS et cela nous évitera également de modifier le plan d'adressage des VLANs.

Plan d'adressage de la DMZ:

WEB	172.22.0.1
FTP	172.22.0.2
DNS (si disponible)	172.22.0.3

Configuration du serveur FTP et WEB

configuration basique du serveur Proftpd :

Pour le serveur nous allons utiliser une appliance debian que nous pouvons retrouver sur le site de gns3.

Pour le serveur ftp nous allons utiliser **proftpd**, il nous suffit d'exécuter la commande suivante:

```
sudo apt install proftpd
```

Par la suite nous allons commencer par créer 4 groupes ftp-user, commercial, gestion et direction.

```
sudo groupadd ftp-user
sudo groupadd commercial
sudo groupadd direction
sudo groupadd gestion
```

Puis nous allons créer un répertoire ftp composé de 3 sous-répertoires commercial, gestion et direction.

```
sudo mkdir ftp && sudo mkdir ftp/commercial ftp/gestion
ftp/direction
```

mise en place des droits :

Maintenant, on doit procéder à la distribution des droits. Pour commencer nous allons faire en sorte que le répertoire ftp appartienne au groupe ftp-user.

```
sudo chown :ftp-user /var/ftp && sudo chmod -R 770 /var/ftp
```

Nous allons faire de même pour les répertoires commercial, gestion et direction.

```
sudo chown :commercial ftp/commercial && sudo chmod -R 770
ftp/commercial
sudo chown :gestion ftp/gestion && sudo chmod -R 770 ftp/gestion
sudo chown :direction ftp/direction && sudo chmod -R 770
ftp/direction
```

Maintenant qu'on en a fini avec les droits, on peut passer à la création des utilisateurs. Pour nous simplifier la vie, on va automatiser la tâche avec un script bash que vous pouvez trouver dans l'annexe..

on peut passer la modification des fichiers de configuration de proftpd. Plus précisément nous allons modifier le fichier **proftpd.conf** et on ajoute les lignes suivantes après le

commentaire sur le port 21.

```
Port 21
DefaultRoot /home/ftp
PassivePorts 5000 5100
```

Installation minimal du serveur WEB :

```
sudo apt install apache2
```

Pour cette SAE nous n'avons pas réellement de faire plus.

Configuration de la deuxième sucursal

plage d'adresse ip :

Pour cette étape nous allons utiliser la méthode VLSM "Variable Length Subnet Mask".

Adresse réseau selon les vlan :

Vlan 10	172.22.2.0/27
Vlan 20	172.22.2.32/28
Vlan 30	172.22.2.48/29

Plage d'adresse valide par sous réseaux :

adresse de réseau	plage valide	broadcast
172.22.2.0/27	172.22.2.1 / 172.22.2.30	172.22.2.31
172.22.2.32/28	172.22.2.33 / 172.22.2.46	172.22.2.47
172.22.2.48/29	172.22.2.49 / 172.22.2.54	172.22.2.55

Réutilisation de la première sucursal :

Pour cette partie, pour éviter de perdre du temps nous allons copier la configuration de la première succursale. Nous allons simplement changer les adresses des interfaces ainsi que le DHCP pour qu'il corresponde à la plage d'adresse donnée dans l'étape précédente. Pour ce faire il suffit de procéder de la même manière que pour le routeur 1.

Mise en place des routes statiques :

Maintenant que les deux succursales sont configurées il nous faut les relier. Pour commencer on va décider de la plage.

Nous avons décidé de changer le nom de l'interface WAN par Serial.

Interface serial R1 (WAN)	Interface serial R2 (WAN)
10.10.10.1/30	10.10.10.2/30

Maintenant on va se connecter à l'interface web du R1. Puis nous allons dans l'onglet **System>Routing** et nous cliquons sur **add** pour ajouter une nouvelle gateway.

Edit Gateway

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

Interface SERIAL
Choose which interface this gateway applies to.

Address Family IPv4
Choose the Internet Protocol this gateway uses.

Name serial
Gateway name

Gateway 10.10.10.2
Gateway IP address

Puis nous allons dans **System>Routing>Static routes** et nous cliquons sur **add** pour ajouter une nouvelle route static.

Edit Route Entry

Destination network 172.22.2.0 / 24
Destination network for this static route

Gateway serial - 10.10.10.2
Choose which gateway this route applies to or [add a new one first](#)

Disabled ☐ Disable this static route
Set this option to disable this static route without removing it from the list.

Description pfsense1 to pfsense2
A description may be entered here for administrative reference (not parsed).

Une fois cela fait, on doit faire de même pour la deuxième succursale avec les informations suivantes.

Gateways	Remote Networks
10.10.10.1	172.22.0.0/24

Ici nous n'avons pas trouvé pertinent de faire une route static vers le réseau 172.22.1.0/24. Nous voulions juste que les utilisateurs du réseau 172.22.2.0/24 puissent accéder à la DMZ.



Nous n'avons effectué cette manipulation mais on a remplacé par de l'IPsec

Configuration vpn IPsec

Le vpn nous permet d'établir une connexion site à site entre les deux succursales.

Mise en place de IPsec:


La configuration de l'IPsec est composée de 2 phases.

La phase 1 de IPsec est utilisée pour établir une connexion sécurisée entre les deux extrémités, en négociant les paramètres de sécurité pour la session. Cela inclut l'authentification, la méthode de chiffrement, la clé de chiffrement et la durée de vie de la session.

La phase 2 de IPsec est utilisée pour établir une connexion sécurisée pour le trafic réel, en utilisant les paramètres de sécurité négociés lors de la phase 1. Cette phase est également appelée la "session de données" et permet la transmission de données de manière sécurisée entre les deux extrémités.

configuration de la phase 1:

Pour commencer nous devons aller dans l'onglet **VPN>IPsec** et on clique sur **add P1**.

General Information	
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
Key Exchange version	<div>IKEv2</div> <div>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.</div>
Internet Protocol	<div>IPv4</div> <div>Select the Internet Protocol family.</div>
Interface	<div>WAN</div> <div>Select the interface for the local endpoint of this phase1 entry.</div>
Remote Gateway	<div>192.168.122.178</div> <div>Enter the public IP address or host name of the remote gateway. </div>
Description	<div>pfsense1 to pfsense2</div> <div>A description may be entered here for administrative reference (not parsed).</div>

On définit l'interface et l'adresse ip qui nous servira de gateway.



Il faut bien faire attention de bien spécifier l'adresse WAN de Pfsense cible.

Phase 1 Proposal (Authentication)

Authentication Method	Mutual PSK
Must match the setting chosen on the remote side.	
My identifier	My IP address
Peer identifier	Peer IP address
Pre-Shared Key	sae21
Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.	
Generate new Pre-Shared Key	

On doit aussi configurer les authentifications et on doit faire attention que ce champ soit le même sur l'autre routeur pfsense. Et on peut laisser le reste par défaut.

configuration de la phase 2:

Nous devons aller dans l'onglet **VPN>IPsec** et on clique sur **Show phase 2 Entries** puis on clique sur **add**.

General Information

Disabled	<input type="checkbox"/> Disable this phase 2 entry without removing it from the list.		
Mode	Tunnel IPv4		
Local Network	Network	172.22.0.0	/ 24
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	172.22.2.0	/ 24
Type		Address	
Remote network component of this IPsec security association.			
Description	dmz to pfsense2		
A description may be entered here for administrative reference (not parsed).			

Comme vous pouvez le voir le local network correspond à notre DMZ et le Remote network correspond au réseau distant ici celui de la deuxième succursale.

On peut faire la même configuration pour le pfsense 2 mais il faut juste changer le **remote gateways** dans la **phase 1** et le **local network**, le **remote network** dans la **phase 2**

Les règles de pare feux IPsec:

Pour que la connexion IPsec fonctionne correctement, on doit ajouter à minima des règles de pare-feu.

Il y a au moins deux règles de filtrage à implémenter : celles autorisant le trafic depuis la DMZ vers les réseaux du site distant ; et celles autorisant le trafic depuis le réseau du site distant vers la DMZ.

Pour Pfsense 1: :

Floating WAN LAN LOCAL SERIAL DMZ VLAN10 VLAN20 VLAN30 **IPsec**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/672 B	IPv4*	*	*	*	*	none			

↑ Add ↓ Add Delete Save + Separator

Pour Pfsense 2 :

Floating WAN LAN LOCAL SERIAL DMZ VLAN10 VLAN20 VLAN30 **IPsec**





Rules (Drag to Change Order)






	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/672 B	IPv4*	*	*	*	*	none			

↑ Add ↓ Add Delete Save + Separator

Floating WAN LAN OPT1 **VLAN10** VLAN20 VLAN30 OPT5 IPsec

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 2 KiB	IPv4 *	*	*	*	*	none			   

 Add  Add  Delete  Save  Separator

Pour le moment les règles sont très permissives et c'est volontaire. Cela nous permet dans un premier temps de vérifier le fonctionnement.

Par la suite nous devons nous rendre dans **Status>Ipsec** et démarrer la connexion sur les deux routeurs.

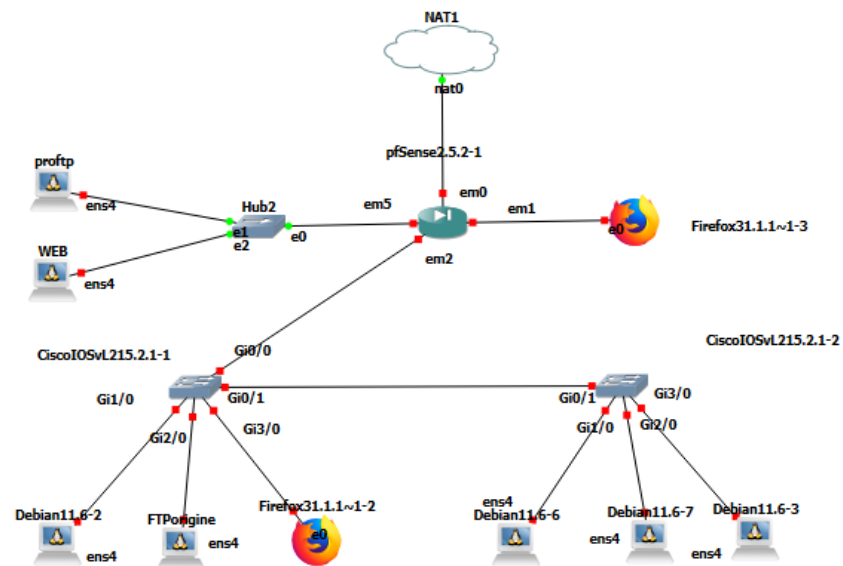
Configuration du pare-feu

Les règles de pare-feux :

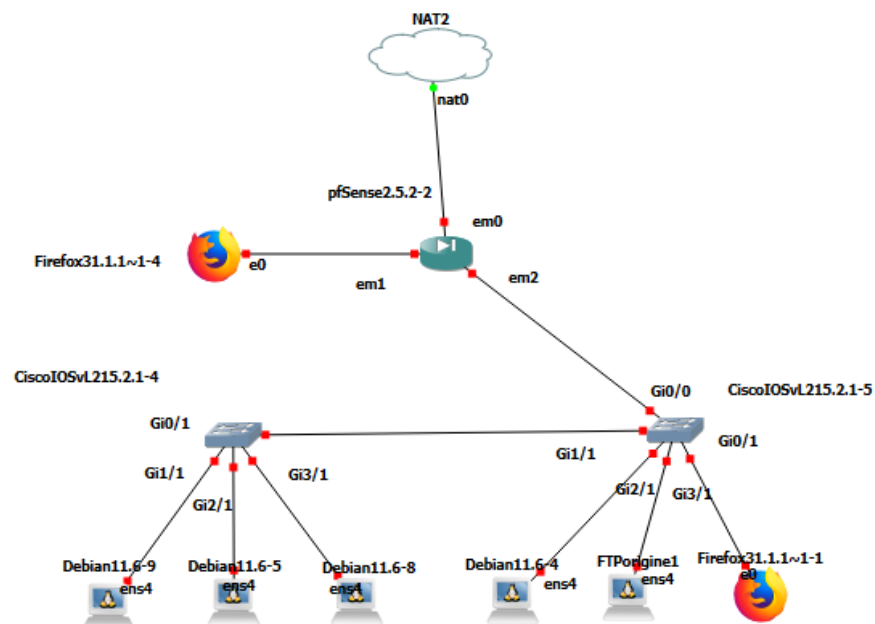
Annexe

Topologie complète:

Site 1:



Site 2:



Scripte bash pour ajouter un utilisateur:

```
#!/bin/bash

# Vérifie si l'utilisateur qui exécute le script est root.
if [ "$(id -u)" != "0" ]; then
    echo "Erreur : ce script doit être exécuté en tant que root" >&2
    exit 1
fi

# Demande le nom de l'utilisateur.
read -p "Nom de l'utilisateur : " username

# Demande le nom du groupe.
read -p "Nom du groupe : " groupname

# Vérifie si le groupe existe.
if ! getent group "$groupname" >/dev/null 2>&1; then
    echo "Erreur : le groupe $groupname n'existe pas" >&2
    exit 1
fi

# Crée le dossier de l'utilisateur dans le répertoire du groupe.
mkdir /home/ftp/$groupname/"$username"

# Crée l'utilisateur avec le groupe, sans dossier home et sans shell.
useradd -g "$groupname" -s /bin/false -M "$username"

# Définit le mot de passe de l'utilisateur comme étant égal au nom d'utilisateur.
echo "$username:$username" | chpasswd

# Ajoute l'utilisateur au groupe "ftp-users".
usermod -aG ftp-users "$username"

# Si le groupe est "direction", ajoute l'utilisateur aux groupes "gestion" et "commercial".
if [ "$groupname" == "direction" ]; then
    usermod -aG gestion "$username"
    usermod -aG commercial "$username"
fi

# Vérifie si l'utilisateur a été créé avec succès.
if [ $? -eq 0 ]; then
    echo "L'utilisateur $username a été créé avec succès"
else
    echo "Erreur : impossible de créer l'utilisateur $username" >&2
    exit 1
fi

# Notifie l'utilisateur que la configuration est terminée.
echo "La configuration pour l'utilisateur $username est terminée."

# Redémarre le service ProFTPD pour prendre en compte les modifications.
systemctl restart proftpd
```