[Date]

Infrastructure à clés publiques (PKI) - Identité & Certificat ssh

Stormshield

Mamadou CAMARA
[NOM DE LA SOCIETE]

Table des matières

1. Contexte :

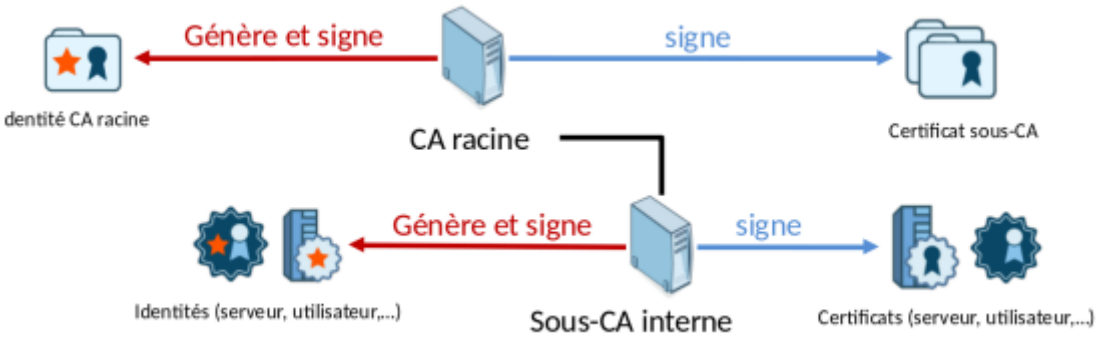
Les activités consistent :

- à mettre en oeuvre une **infrastructure à clé publique (PKI)** avec un pare-feu Stormshield ;

  créer et utiliser :

- des **certificats utilisateurs** signés pour s'authentifier sur un serveur Debian distant et pour l'interface d'administration du SNS Stormshield.
- Un certificat racine ca

2. Présentation



CA interne

Cette fonctionnalité de gestion d'une infrastructure à clés publiques permet de répondre à un grand nombre de cas d'usage :

• **Le pare-feu agit en tant qu'autorité de certification racine (root CA**) : le boîtier SNS permet de définir les chaînes de confiance nécessaires à une authentification par certificat. Des autorités par défaut sont disponibles pour signer les certificats utilisés par le proxy SSL ou livrer les certificats nécessaires au fonctionnement du VPN SSL. Son certificat d'autorité est auto-signé. Les fonctions proposées par le boîtier SNS permettent de répondre pleinement au rôle d'autorité de certification (création de certificat de différentes natures, signature de CSR, révocation de certificat et gestion de CRL).

• **Le pare-feu agit en tant que sous-autorité de certification** : il est possible de définir un boîtier SNS comme étant une sous-autorité de certification d'une CA parente (gérée obligatoirement sur le même boîtier). Le certificat de la sous-autorité est signé par l'autorité parente (pas nécessairement une autorité racine), laquelle est une autorité interne ou externe. Cela permet d'organiser plus finement la répartition et la distribution des identités, par usages ou par entités d'une même entreprise.

3. Création de l'autorité de certification ca, certificat et autorité utilisateur sur Stormshield

3.1 L'autorité de certification ca

Se rendre au menu CONFIGURATION / OBJETS / Certificats et PKI Cliquer sur Ajouter puis sélectionner **Autorité racine**.

Ensuite :

Renseigner un CN (obligatoire) : il s'agit d'un nom permettant d'identifier votre autorité racine, dans la limite de 64 caractères. Ce nom peut faire référence à une organisation, un utilisateur, un serveur, une machine, etc.

Renseigner un Identifiant (facultatif) : vous pouvez ici indiquer un raccourci de votre CN, utile pour vos lignes de commande.

renseigner les attributs de l'autorité. Ces informations seront présentes dans le certificat de l'autorité ainsi que dans les certificats qu'elle émettra :

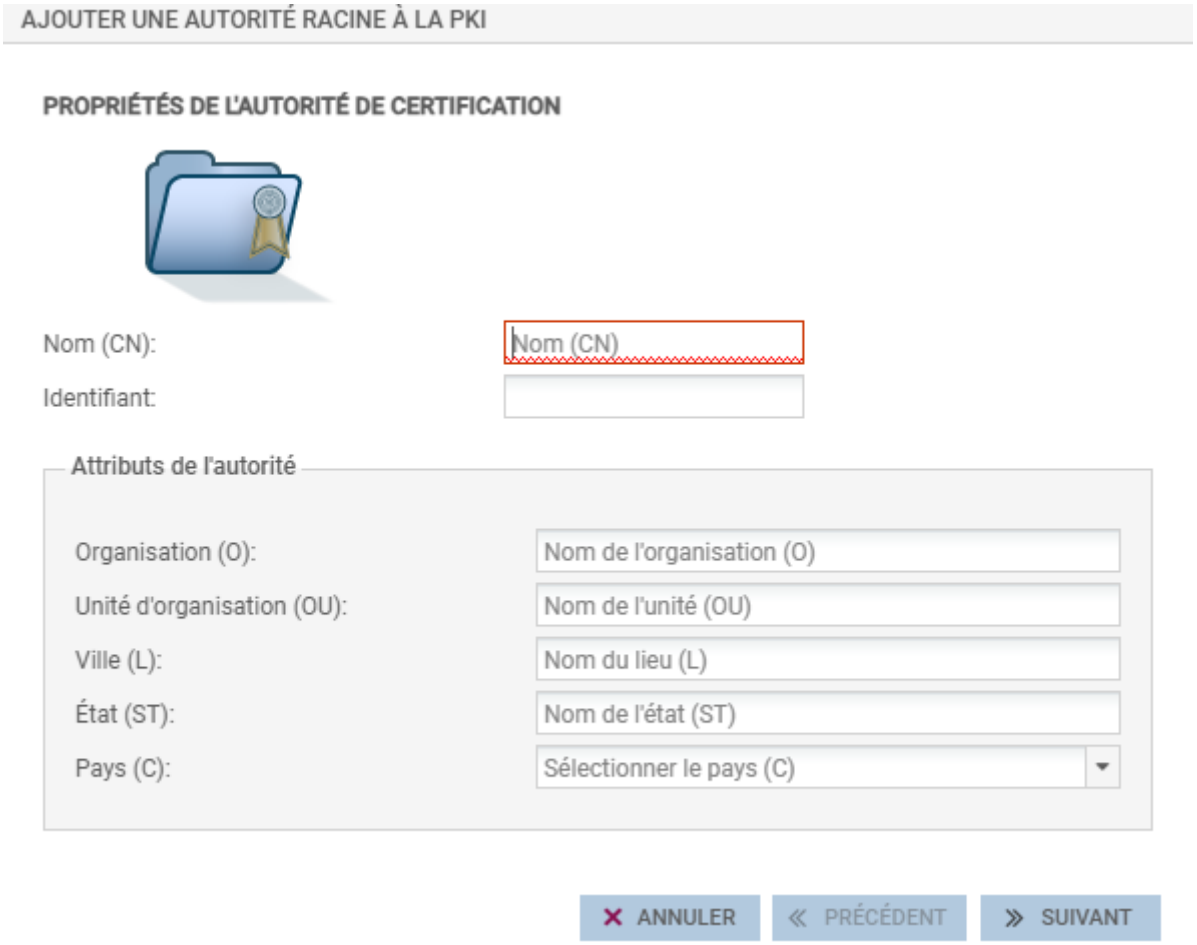
• Organisation (O) : nom de votre société.

• Unité d'organisation (OU) : "branche" de votre société.

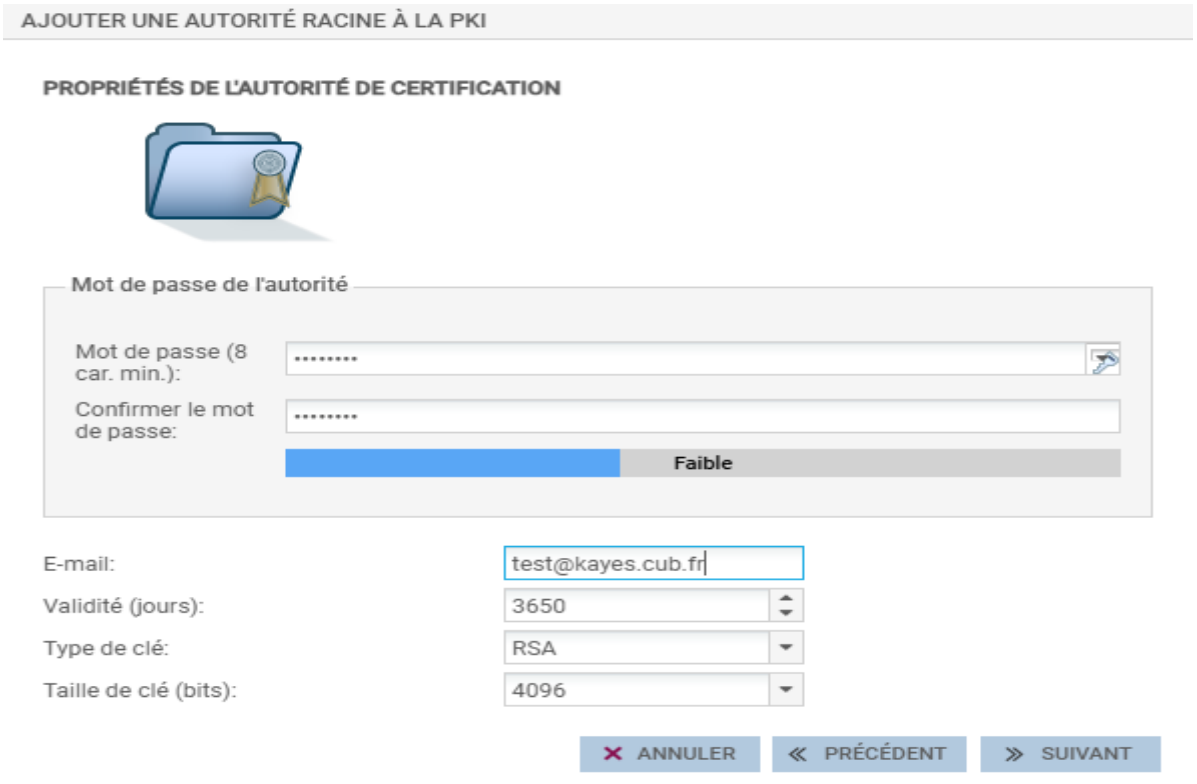
• Lieu (L) : ville dans laquelle est située votre société

• État ou province (ST) : département géographique de votre société.

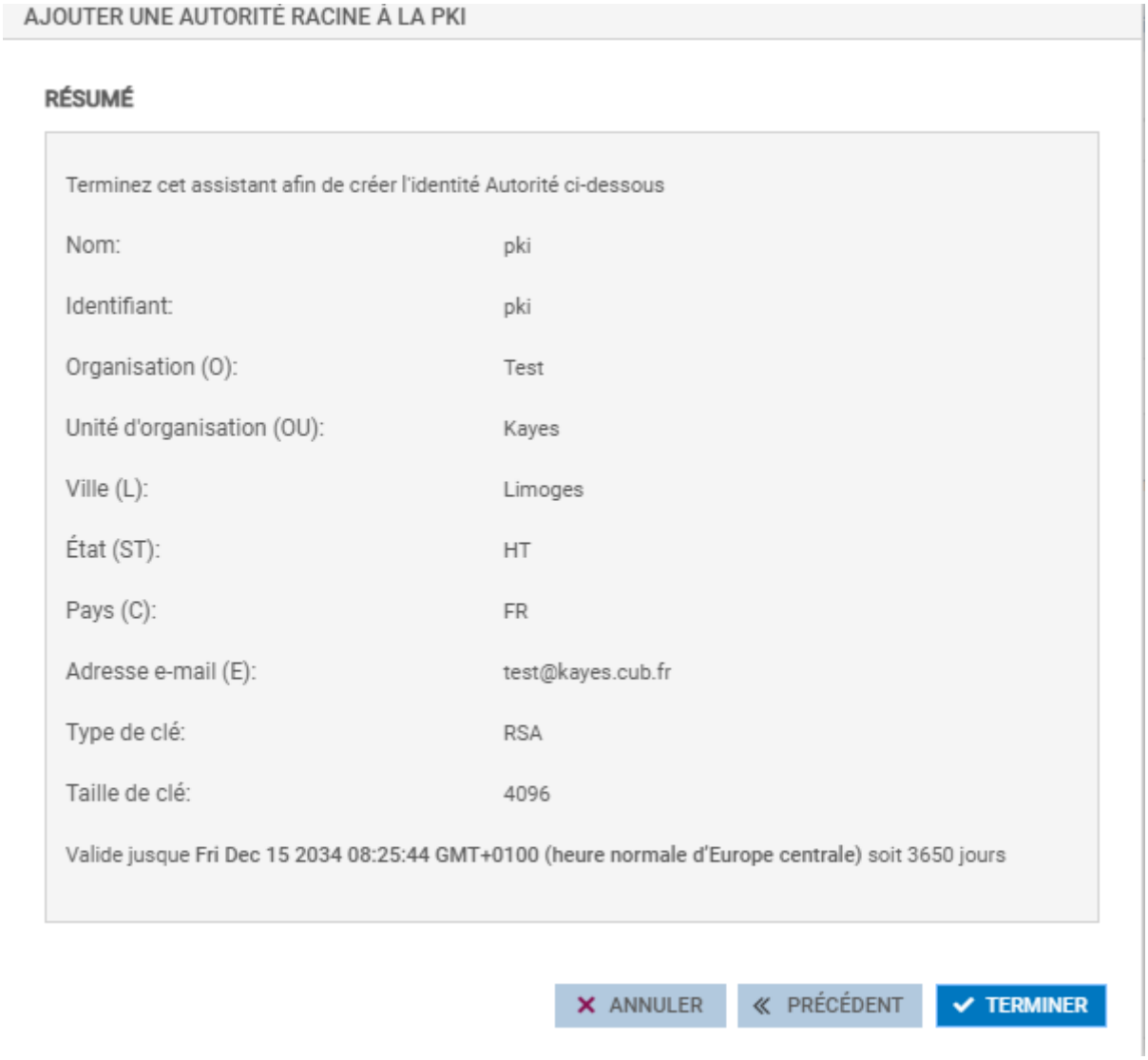
• Pays (C) : pays dans laquelle est située votre société Cliquer sur Suivant



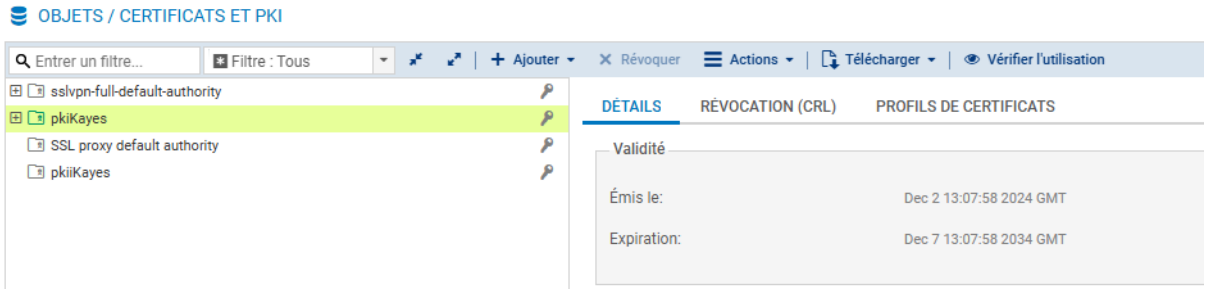
Cliquer sur suivant :



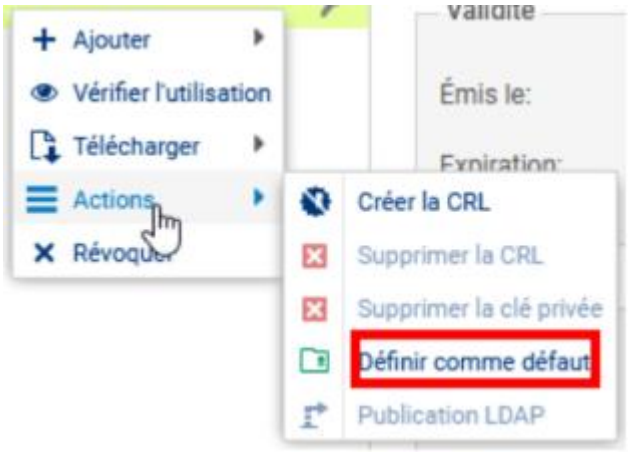
Le ca est crée



L'autorité est automatiquement ajoutée à l'arborescence des autorités, identités et certificats définis sur le firewall.



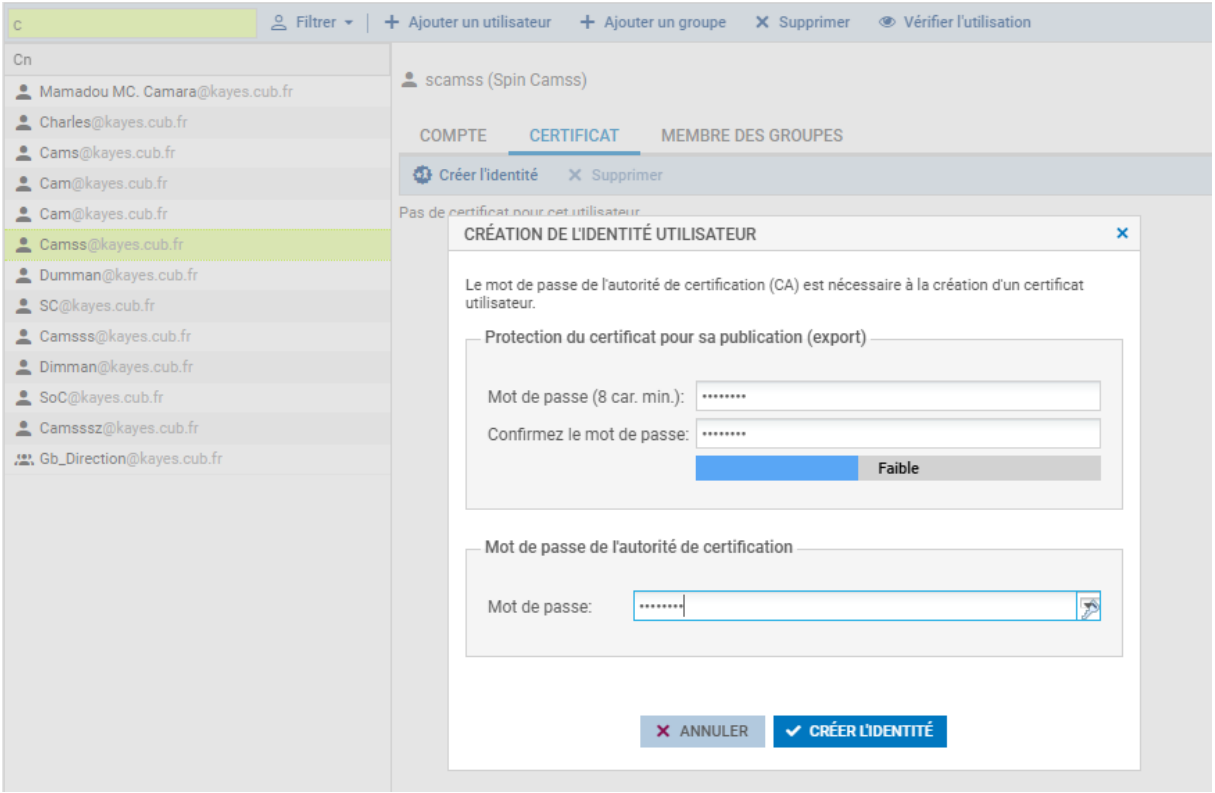
- Définir éventuellement par défaut l'autorité de certification :



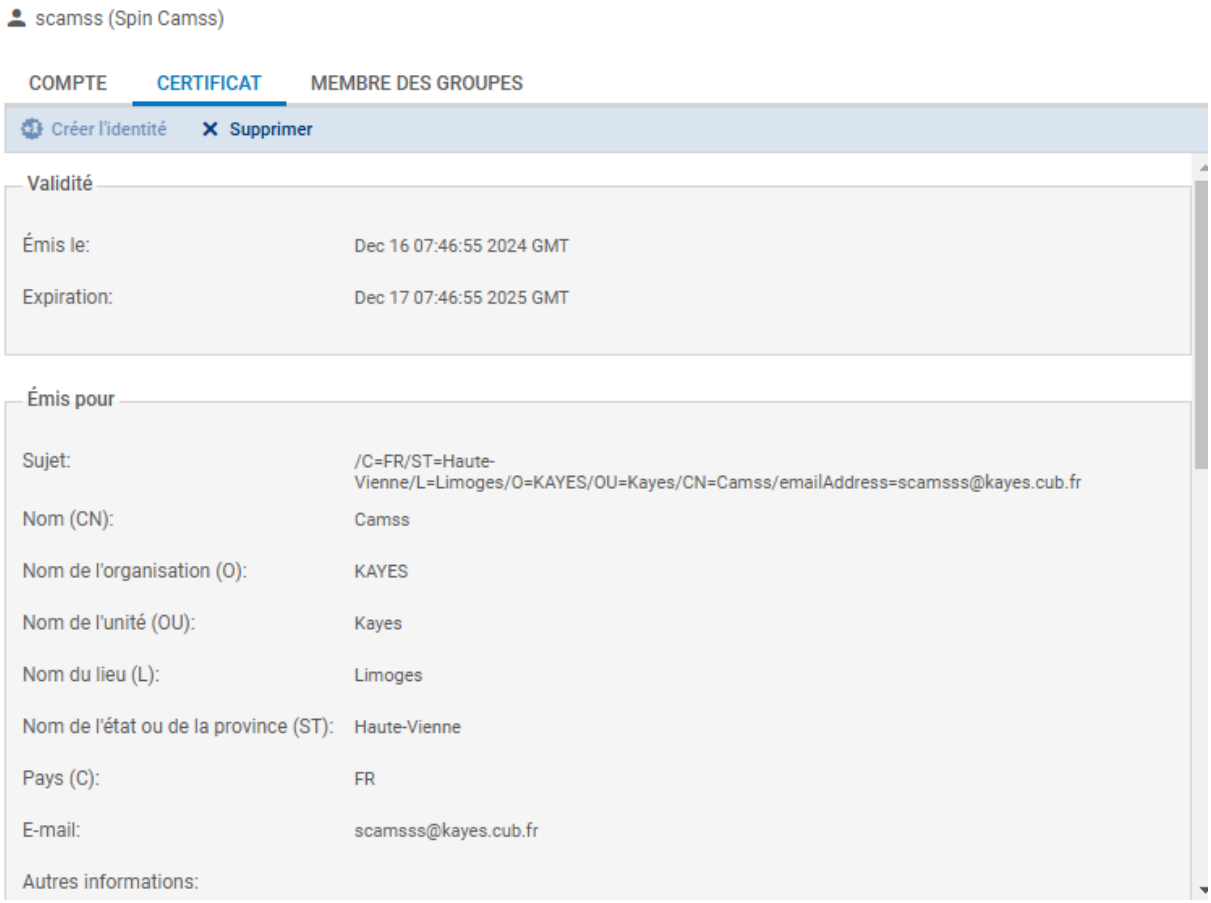
-

3.2 Identité utilisateur

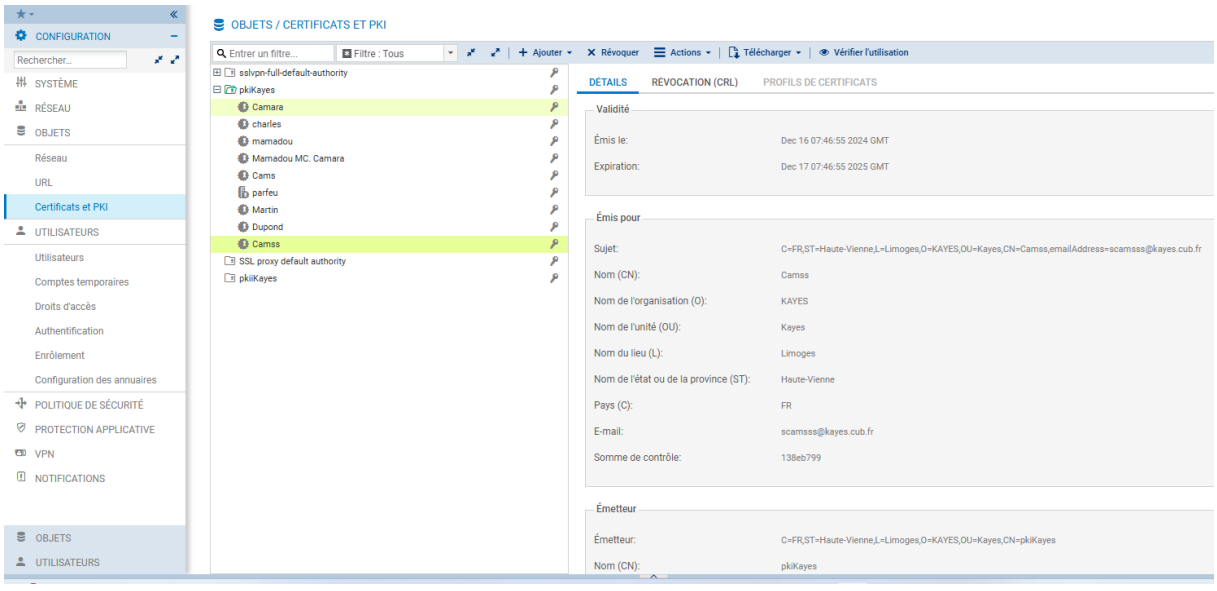
Première méthode à partir d'un utilisateur créé dans l'annuaire LDAP externe du firewall.il est possible de générer une identité utilisateur directement depuis l'annuaire LDAP du firewall. Dans ce cas, le choix de l'autorité signataire se porte automatiquement sur la CA désignée par défaut. Se rendre au menu **CONFIGURATION / UTILISATEURS / Utilisateurs** Sélectionner l'utilisateur puis cliquer sur CERTIFICAT puis Créer l'identité



Cliquer sur « Créer l'identité » Le certificat de l'utilisateur s'affiche



Il est également visible via le menu **OBJETS / CERTIFICATS et PKI**



Deuxième méthode

Se rendre au menu **CONFIGURATION / OBJETS / Certificats et PKI** Cliquer sur **+Ajouter** puis Identité Utilisateur.

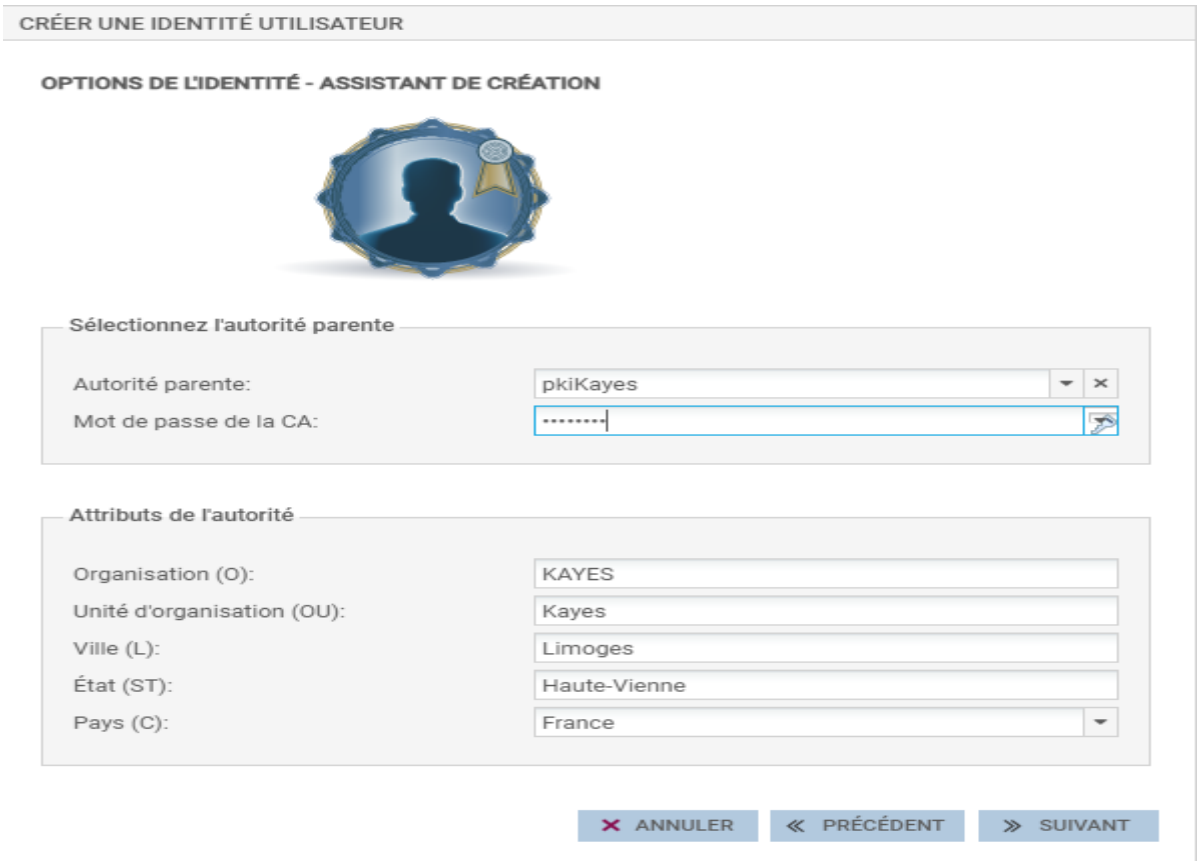
Renseigner : un CN (obligatoire) : nom permettant d'identifier l'utilisateur dans la limite de 64 caractères. 2. un Identifiant (facultatif) : vous pouvez ici indiquer un

raccourci de votre CN, utile pour vos lignes de commande (exemple : si le CN est un couple Prénom+Nom, l'identifiant peut correspondre aux initiales du CN).

l’adresse e-mail (obligatoire) de l'utilisateur pour lequel vous créez une identité.
Cliquer sur Suivant.

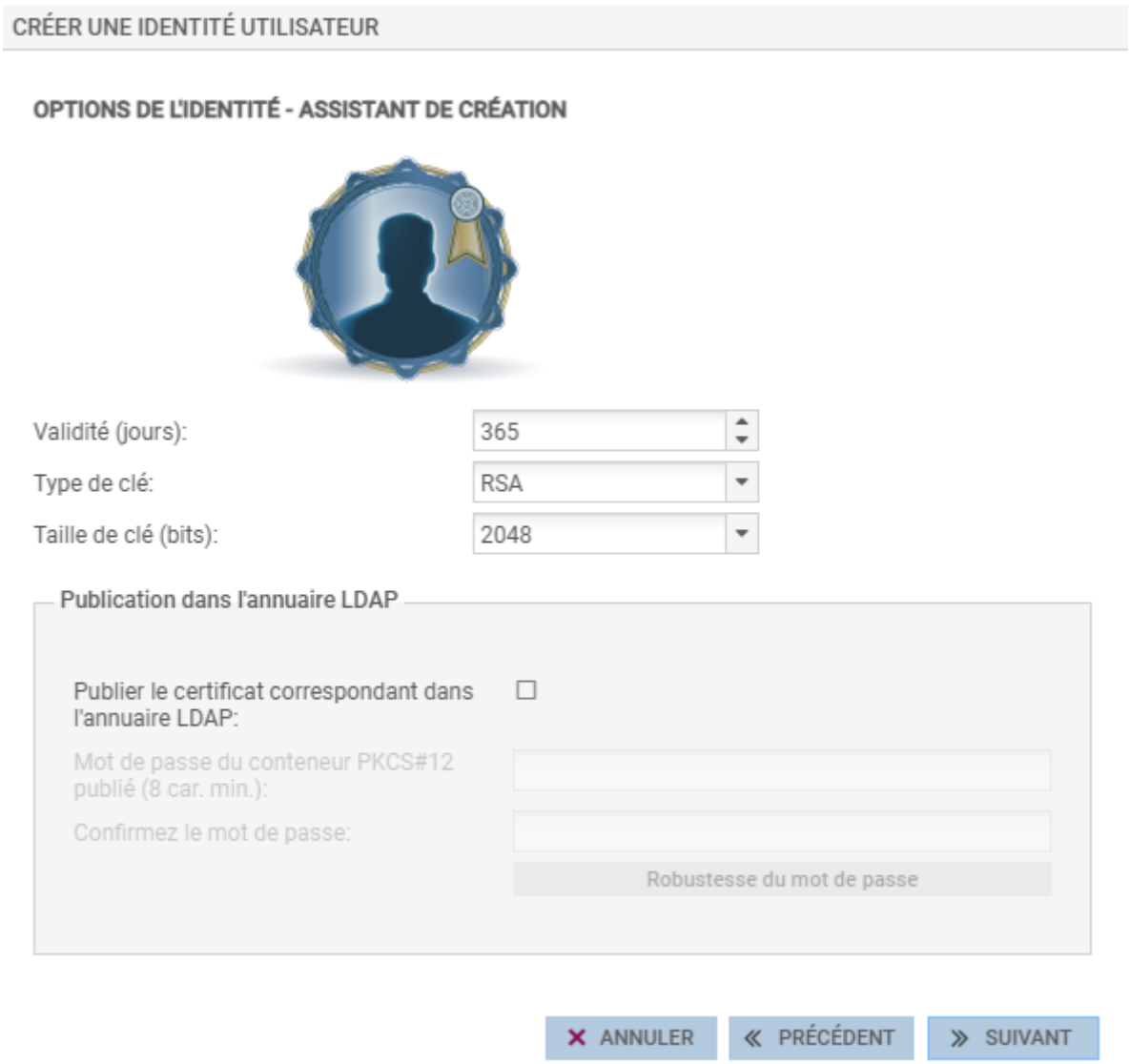
Sélectionner l'Autorité parente destinée à signer le certificat de l'identité.
Renseigner le Mot de passe de l'autorité parente.

Les attributs de l'autorité sont automatiquement ajoutés. Ils seront présents dans le certificat utilisateur.

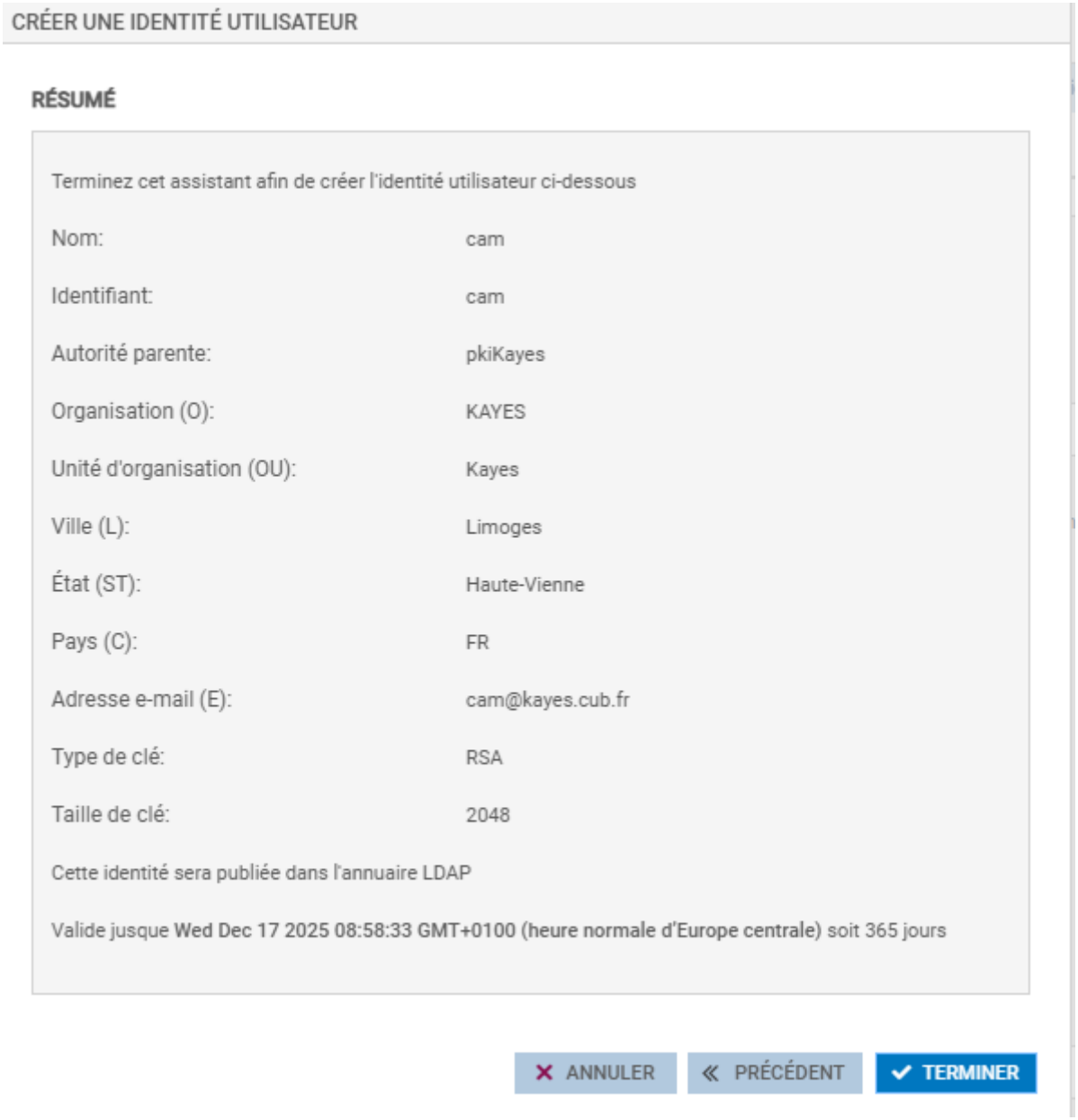


Cliquer sur suivant

Si l'autorité utilisée pour générer le certificat est l'autorité par défaut du firewall ET si un utilisateur déclaré dans l'annuaire LDAP référence la même adresse e-mail que celle précisée à l'étape 3, vous pouvez associer automatiquement cette identité à l'utilisateur correspondant : Cocher la case **Publier cette identité dans l'annuaire LDAP**, Saisissez deux fois un mot de passe destiné à protéger le conteneur PKCS#12 de l'identité. Cliquer sur Suivant



Un résumé des informations saisies vous est présenté. ⇒ Cliquer sur Terminer



L'identité est automatiquement ajoutée à l'arborescence des autorités, identités et certificats définis sur le firewall, sous son autorité parente.

4. Gestion des identités et certificats

Menu Télécharger

Certificat : le format d'export contient des données en base64 (.pem) ou des données binaires (.der). Le fichier exporté contient le certificat du porteur mais également les certificats des autorités présentes dans la chaîne de confiance de ce certificat.

Identité : l'identité, puisqu'elle contient une clé privée, est sensible et son export doit être protégé par un mot de passe, lequel permet de chiffrer la clé privée qu'il contient. L'identité est pour rappel constituée de la clé privée du porteur, de son certificat (qui

contient sa clé publique), et des certificats de la chaîne de confiance. Le fichier d'export est un container .pem ou un container PKCS#12 (ou .p12).

2.1 Connexion ssh en utilisant l'identité utilisateur sur un serveur distant

- Télécharger l'identité utilisateur crée sur Stormshiel au format p12 :
- Puisque l'identité contient une clé privée qui est sensible et son export doit être protégé par un mot de passe, lequel permet de chiffrer la clé privée qu'il contient.
- Indiquer le mot de passe :

-
- Ensuite téléchargé l'identité :

2.2 Extraction des clés privée et publique du fichier identité de charles

Avec la commande **ssh-keygen -f /fichieridentité**

```
PS C:\Users\camar\Downloads> ssh-keygen -f .\identité_charles.pem
Generating public/private ed25519 key pair.
.\identité_charles.pem already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in .\identité_charles.pem
Your public key has been saved in .\identité_charles.pem.pub
The key fingerprint is:
SHA256:c8bDsoXlZ59Eji1238suZ9XO6CINijk8qDG9elI10VE camar@Mamadou
The key's randomart image is:
+--[ED25519 256]--+
|       ..oE      |
|      . .        |
|       .  .   .  |
|      o  *   =   |
|     . .S O * = .|
|    ..    B.= = o+|
|  o..o o.. o  o++|
|  .oo.* . . o.oo+|
|  o=.  o   . o*+ |
+----[SHA256]-----+
```

On renomme les clés générées : id_rsa est la clé privée et id_rsa.pub est la clé publique

```
+----[SHA256]-----+
PS C:\Users\camar\Downloads> ren .\identité_charles.pem id_rsa
PS C:\Users\camar\Downloads> ren .\identité_charles.pem.pub id_rsa.pub
```

On copie la clé publique dans **.ssh/autorized_key du client windows**

```
    + FullyQualifiedErrorId : FileOpenFailure,Microsoft.PowerShell.Commands.OutFileComm

PS C:\Users\camar\Downloads> cat id_rsa.pub >> ~/.ssh/autorized_key
PS C:\Users\camar\Downloads>
```

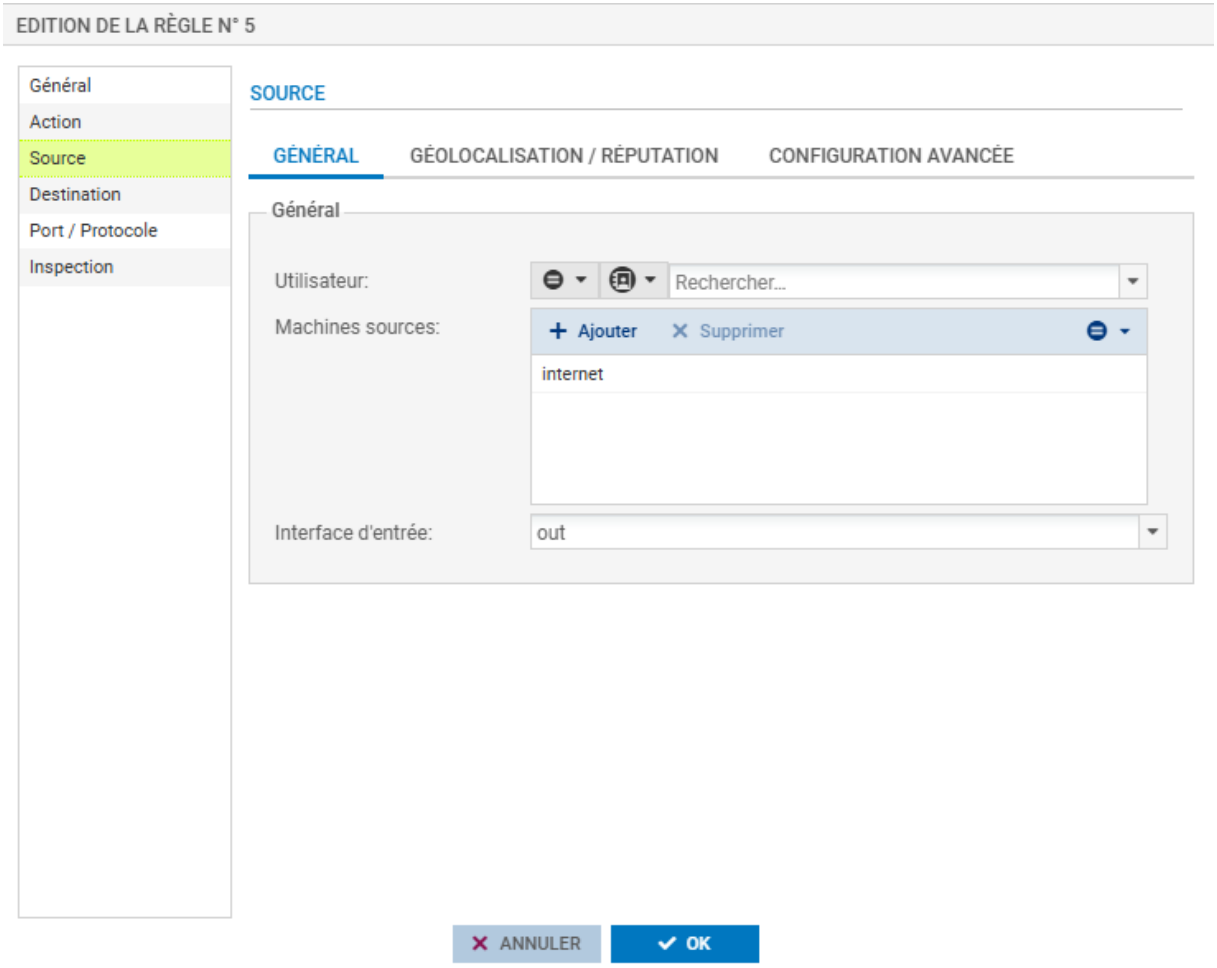
On copie les deux clé publique/Privée dans **.ssh/** du Windows

```
PS C:\Users\camar\Downloads> cp .\id_rsa C:\Users\camar\.ssh\
PS C:\Users\camar\Downloads> cp .\id_rsa.pub C:\Users\camar\.ssh\
```

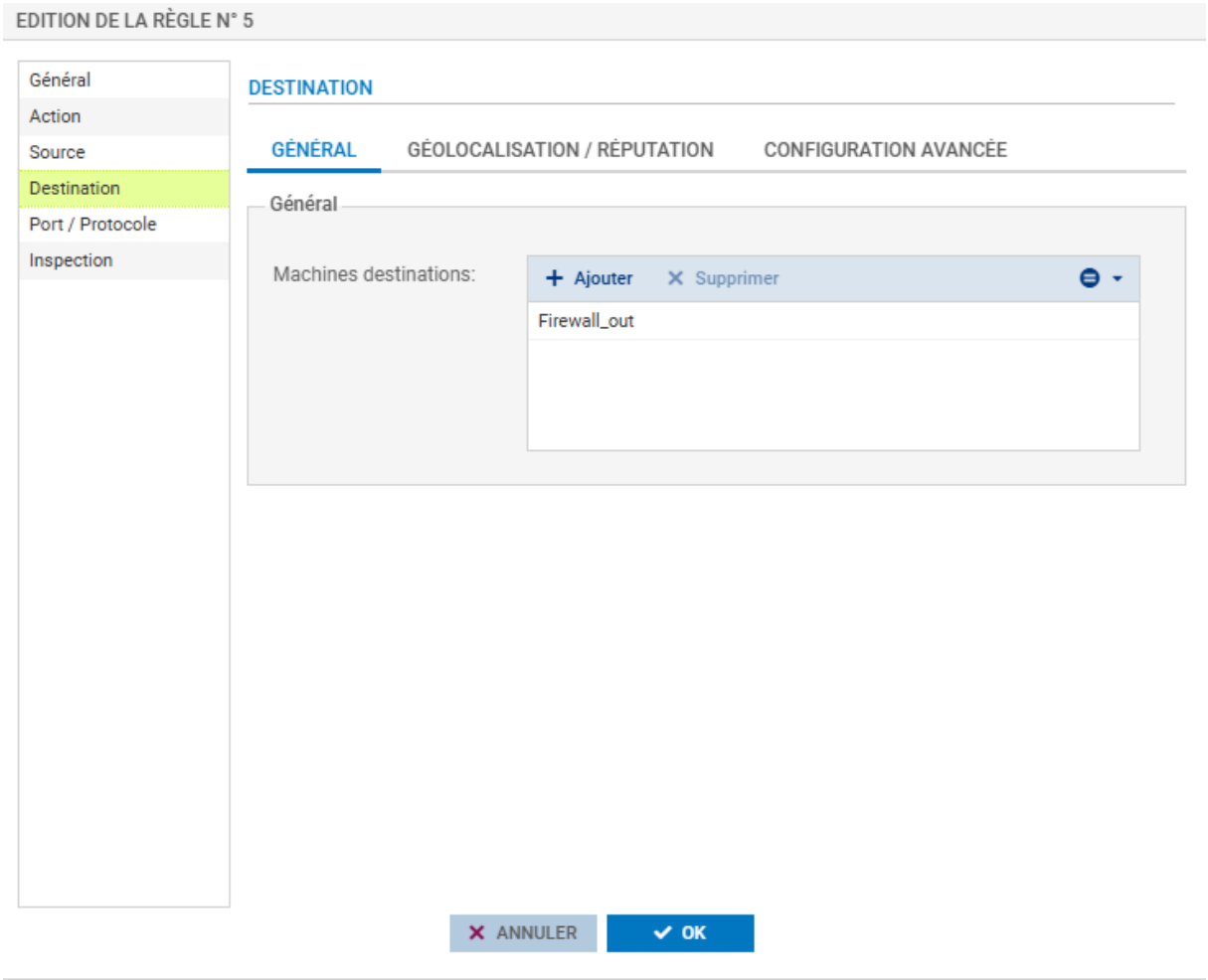
On copie la clé publique sur le serveur distant

NB : Pour pouvoir se connecter au serveur distant depuis internet, on fait une redirection de port :

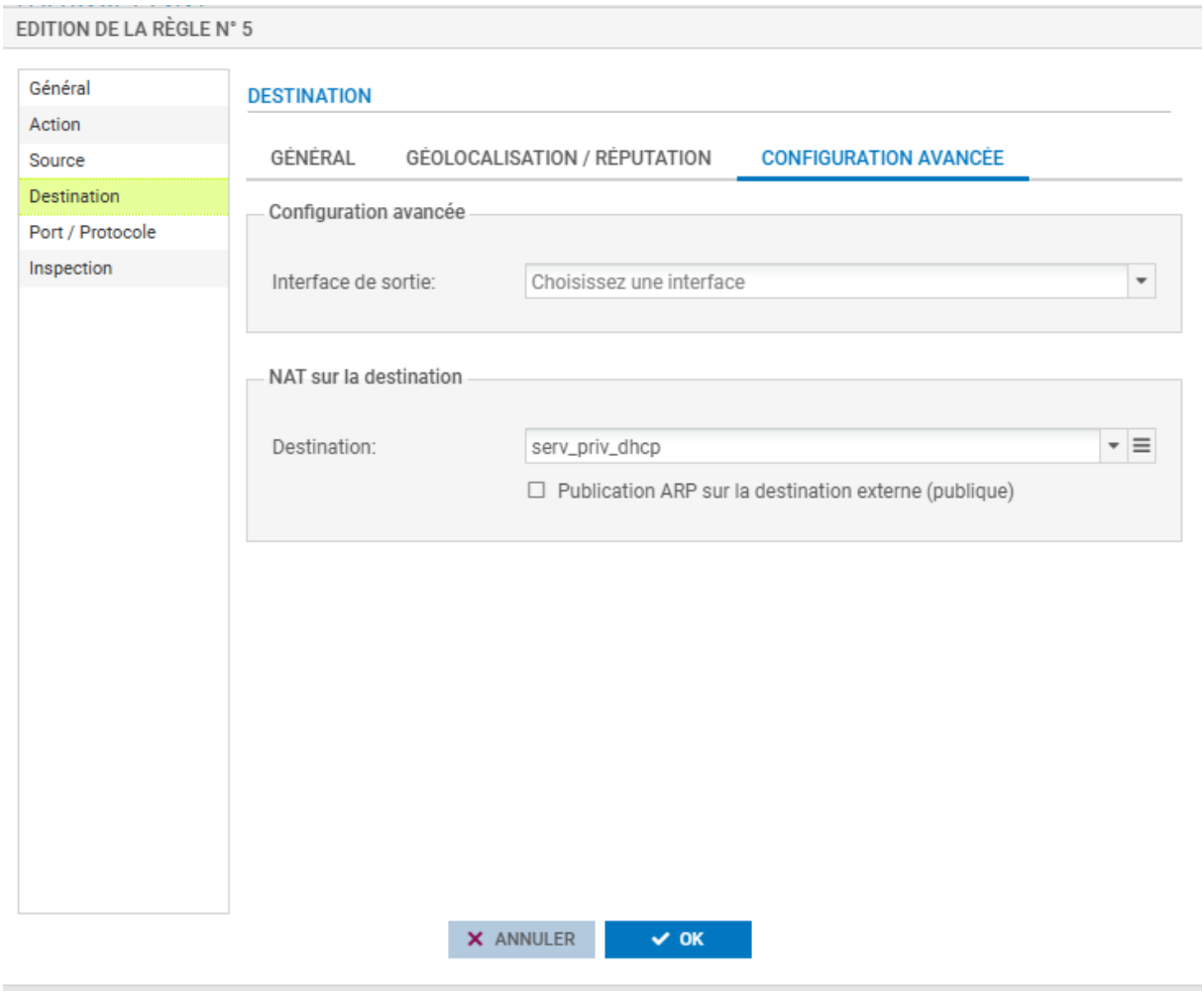
- Source : Internet



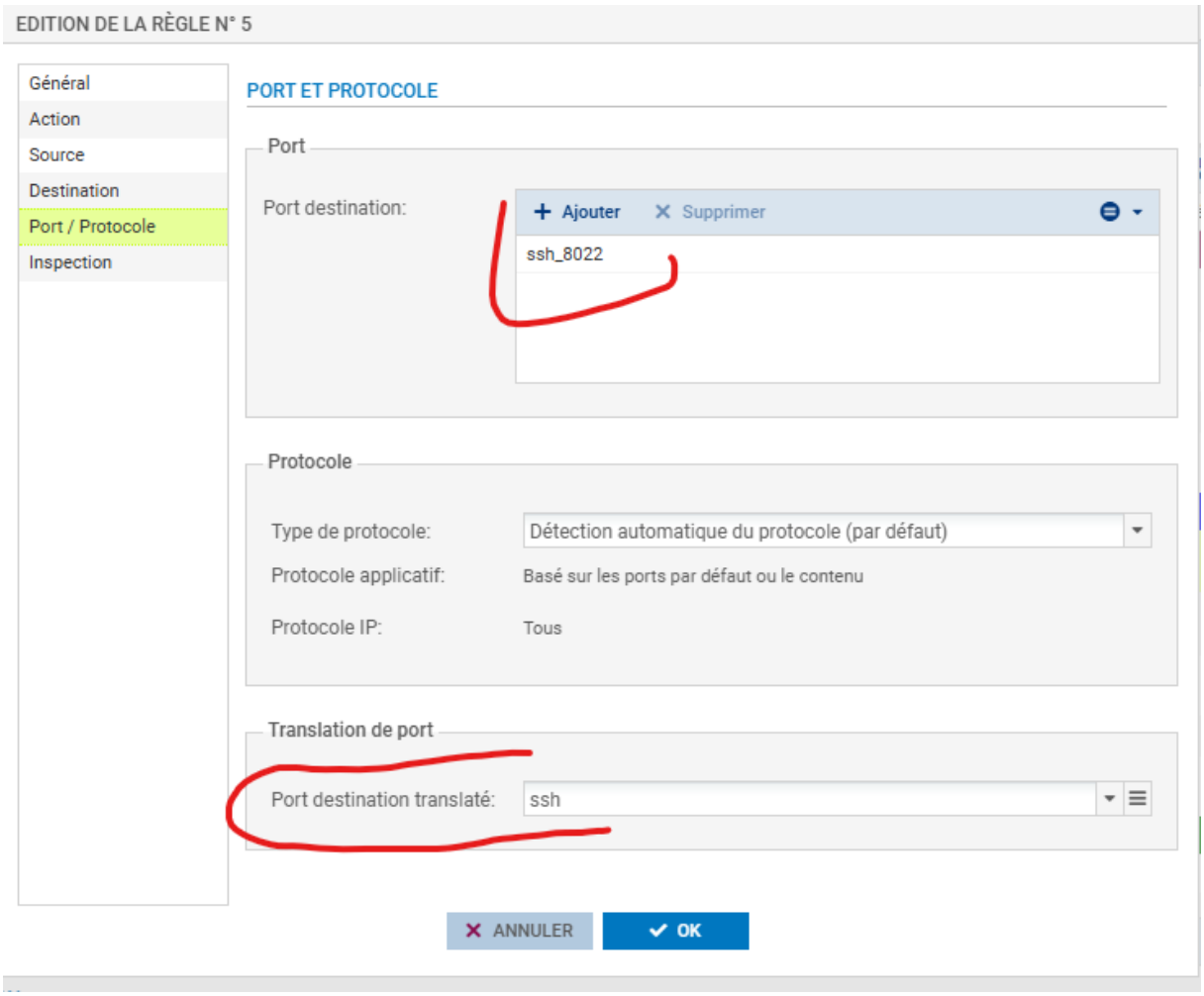
- Deestination : l'interface OUT du pare feu



-Dans Configuration avancée, on indique l'adresse ip de notre serveur distant (NAT Destination):



- Dans l'onglet Port/Protocole :
- Pour **le Port Destination**, on choisi un port disponible, **ici 8022** pour pouvoir se connecter au serveur via ssh port **22** (**port de translation**)



-

On copie la clé publique sur le serveur distant via la commande :

Scp -P 8022 fichierIdentite.pub compte@192.168.229.36:/home/compte

-P : indique le port de destination

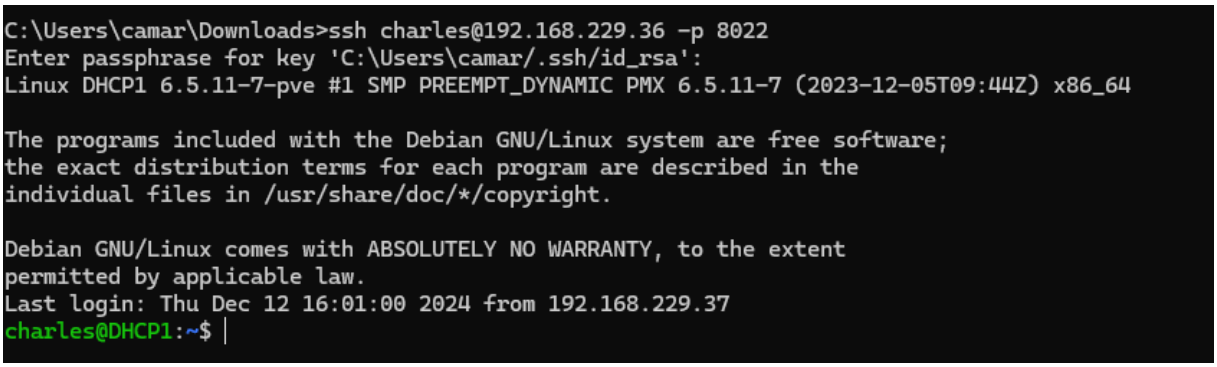
```
C:\Users\camar\Downloads>scp -P 8022 id_rsa.pub charles@192.168.229.36:/home/charles/.ssh
charles@192.168.229.36's password:
id_rsa.pub                                    100%   96    13.4KB/s   00:00

C:\Users\camar\Downloads>
```

On copie en suite la clé dans autorized_keys avec la commande

Cat id_rsa.pub >> autorized_keys

2.3 Test :



5. Configuration du client ssh sous Windows

Configuration du client SSH

Sur le client LWindows, le fichier C:**Users\.ssh\config** permet de configurer les **paramètres globaux** du client pour toutes les connexions vers des serveurs **ssh**.

Pour chaque compte utilisateur, une configutation personnalisée se fait créant/modifiant le fichier **config** situé dans le répertoire utilisateur **.ssh** (C:\Users\[nom_utilisateur]\.ssh\config sous Windows)

Exemple :

On crée un fichier **config** dans le dossier **.ssh,** on ajoute les information suivantes **:**

Host dhcp

Hostname 192.168.229.X

Port 8022

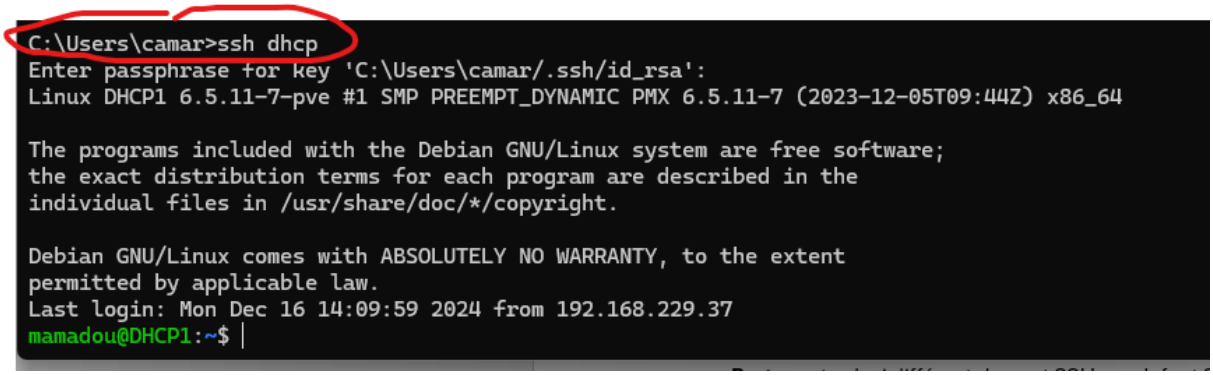
User mamadou

Explication :

- **Host** : défini un nom pour le serveur ssh
- **Hostname** adresse IP ou nom DNS du serveur
- **Port** : port ssh si différent du post SSH par defaut 22
- **User** : précise le nom de connexion

Utilisation :

Pour se connecter au serveur DHCP via ssh, il suffit d'indiquer le nom définit dans le fichier de configuration C:\Users\[nom_utilisateur]\.ssh\config



6. Certificat :

On met le ca dans **: /usr/local/share/ca-certification**

Puis on tape la commande update-ca-certificates