

Table des matières

| | |
|--|---|
| <i>En ligne de commandes</i> | 3 |
| <i>Avec Cyberduck sur macOS</i> | 4 |
| <i>Avec WinSCP sur Windows</i> | 7 |

Public : utilisateurs de SSH et SCP

Copier des fichiers à travers un bastion SSH

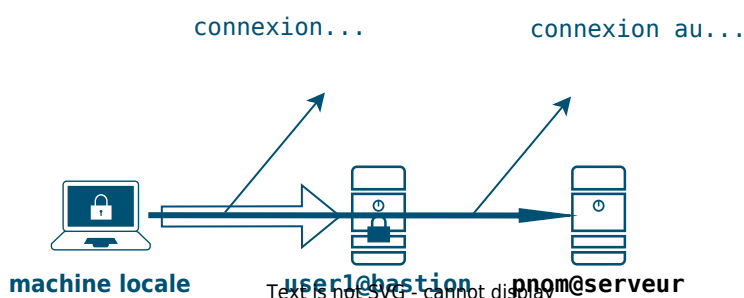
← [Accès distants](#)

Dans toute la suite, on suppose connue la page [Utiliser SSH](#), en particulier la section [utilisation d'une machine de rebond avec ProxyJump](#).

En ligne de commandes

En reprenant les noms (bastion bastion, serveur final serveur) de la situation :

```
$ ssh -J user1@bastion pnom@serveur
```



et la configuration suggérée dans `$HOME/.ssh/config`, à savoir :

```
Host bastion
  User user1

Host srv
  ProxyJump bastion
  Hostname serveur
  User pnom
```

il suffit d'indiquer :

```
$ scp path/to/local/file srv:path/to/destination
```

pour copier file dans path/to/destination sur serveur. Sans l'option ProxyJump, utiliser aussi `-J user1@bastion` avant les indications de la source et de la destination :

```
$ scp -J user1@bastion path/to/local/file pnom@serveur:path/to/destination
```

Évidemment, il suffit d'inverser les arguments pour copier un fichier depuis le serveur vers le poste local. L'option `-r` permet la copie « récursive » (*i.e.* d'un répertoire et de l'ensemble de son contenu).

NB : la commande `sftp(1)` permet l'échange interactif de fichiers et se comporte de la même manière :

```
$ sftp -J user1@bastion pnom@serveur
sftp>
```

Avec Cyberduck sur macOS

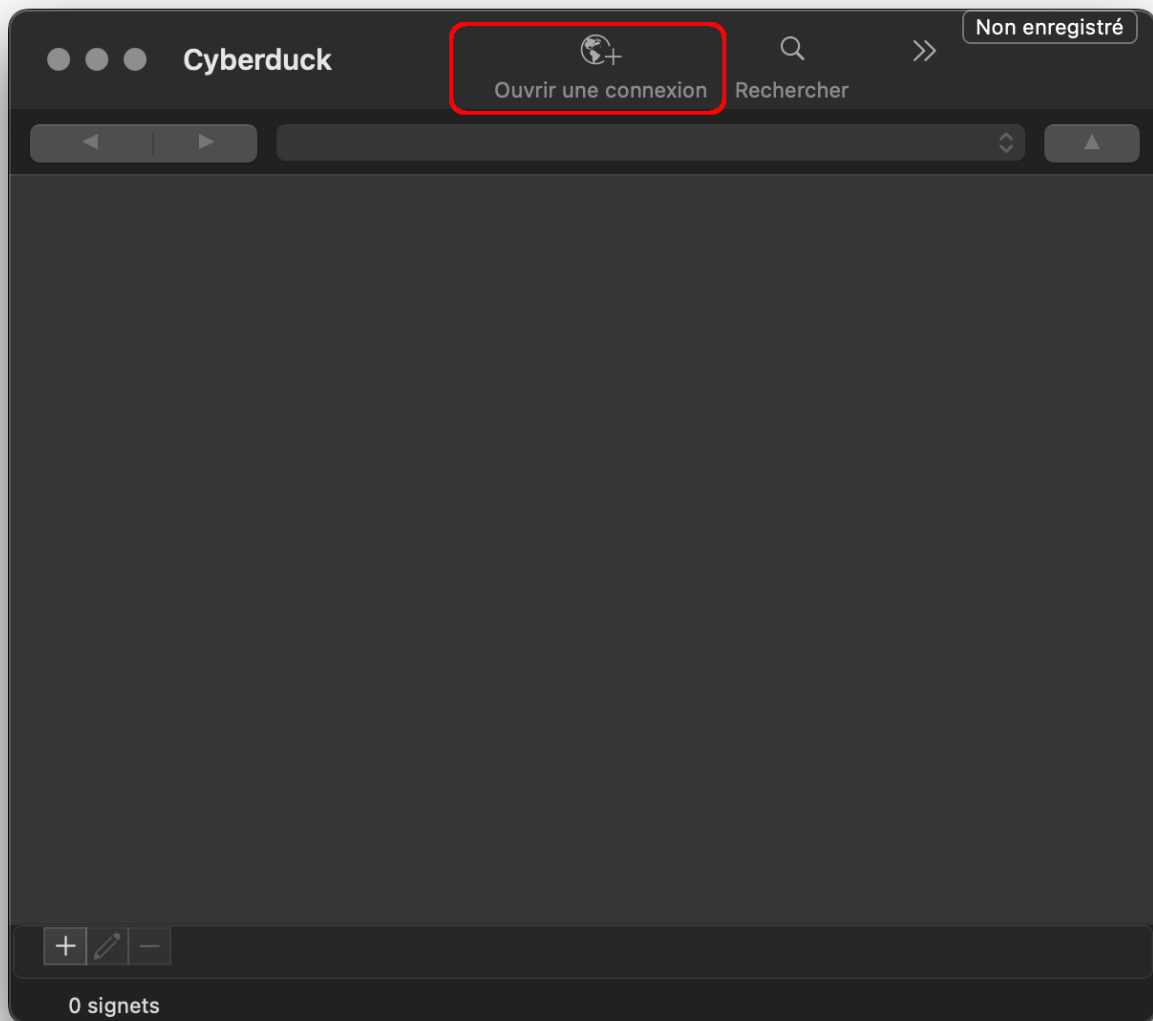
[Cyberduck](#) est un logiciel libre (qui propose de participer au financement du projet mais qui reste gratuit) disponible sur macOS et sur Windows. Sur macOS, il s'intègre avec OpenSSH *i.e.* il utilise les réglages dans `~/.ssh/config`.

S'assurer que `~/.ssh/config` contient la configuration pour le bastion et pour le serveur :

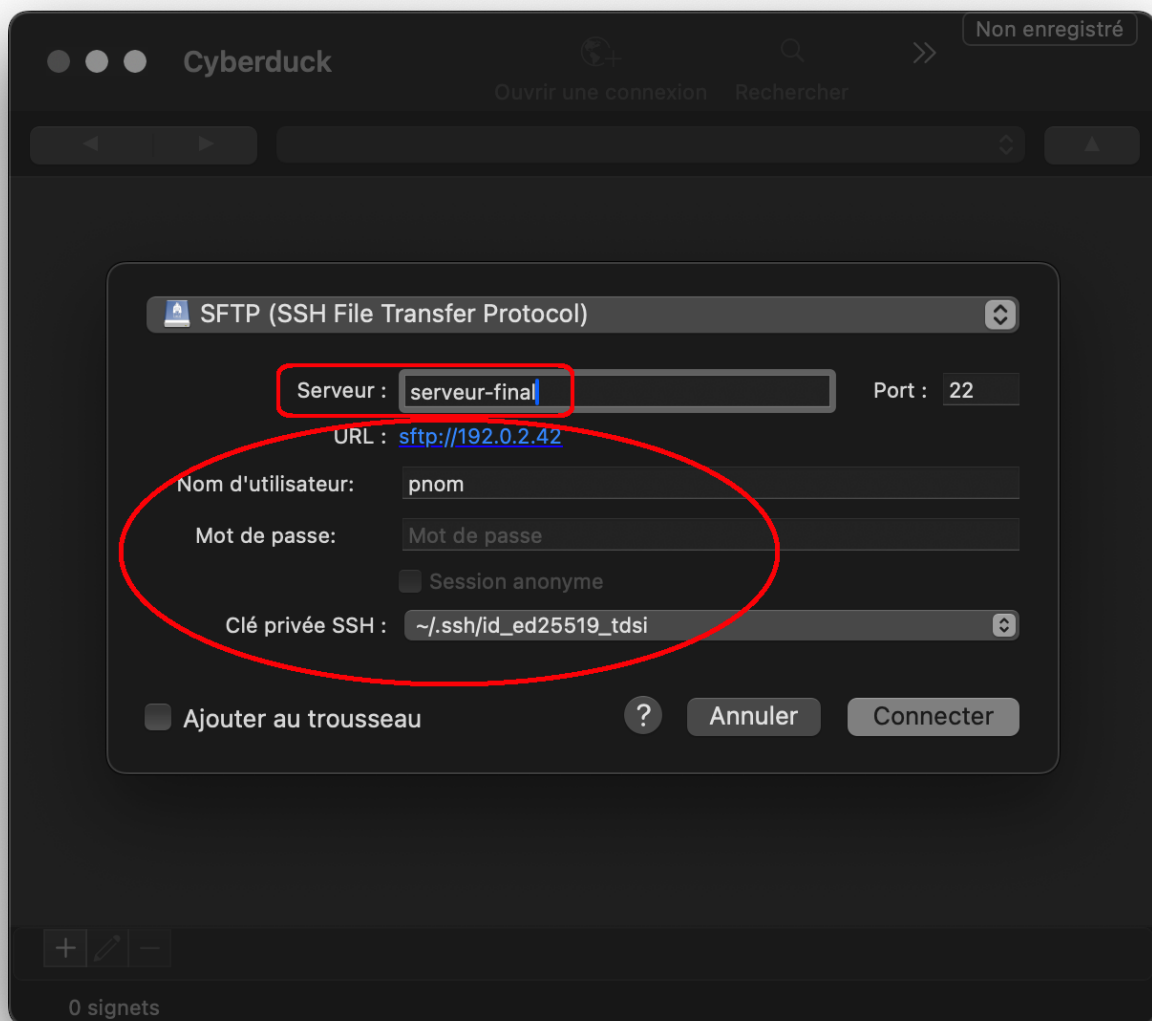
```
Host bastion
  User user
  IdentityAgent ~/.ssh/ssh-agent.sock
  IdentityFile ~/.ssh/id_ed25519
  Hostname nom.dns.du.bastion

Host serveur-final
  User user
  Hostname nom.dns.du.serveur
  IdentityAgent ~/.ssh/ssh-agent.sock
  IdentityFile ~/.ssh/id_ed25519
  ProxyJump bastion
```

Lancer Cyberduck et créer une connexion :



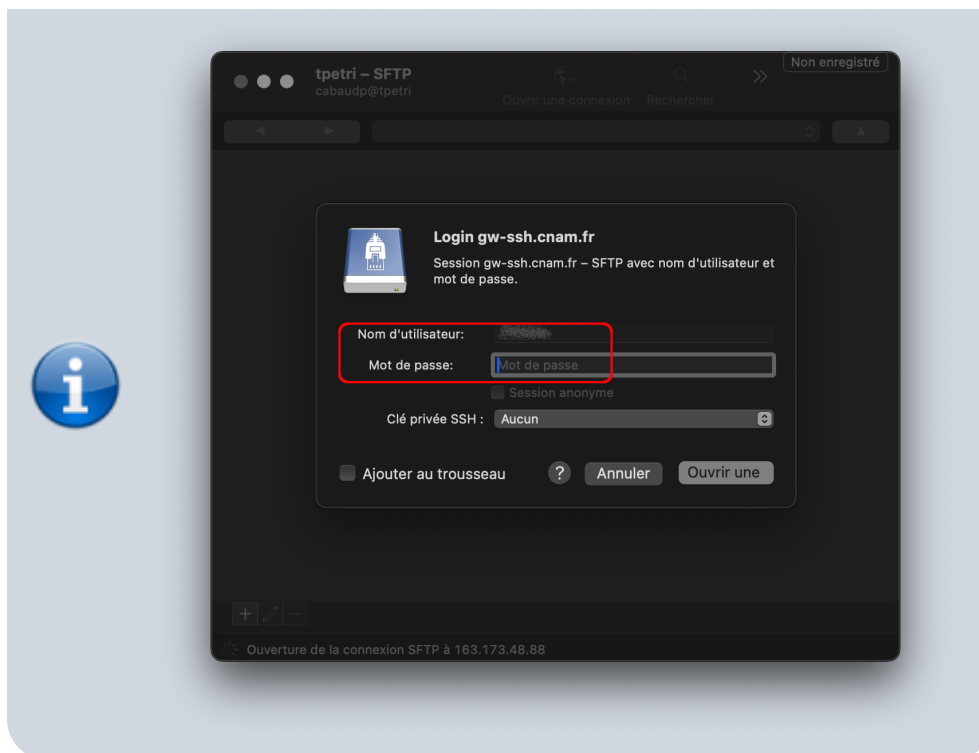
Dans le cartouche server, saisir le nom `serveur-final` comme renseigné dans `~/ .ssh/config`, Cyberduck remplit alors les autres champs :



Les empreintes des clefs des serveurs (le bastion puis le serveur final) doivent être validées.

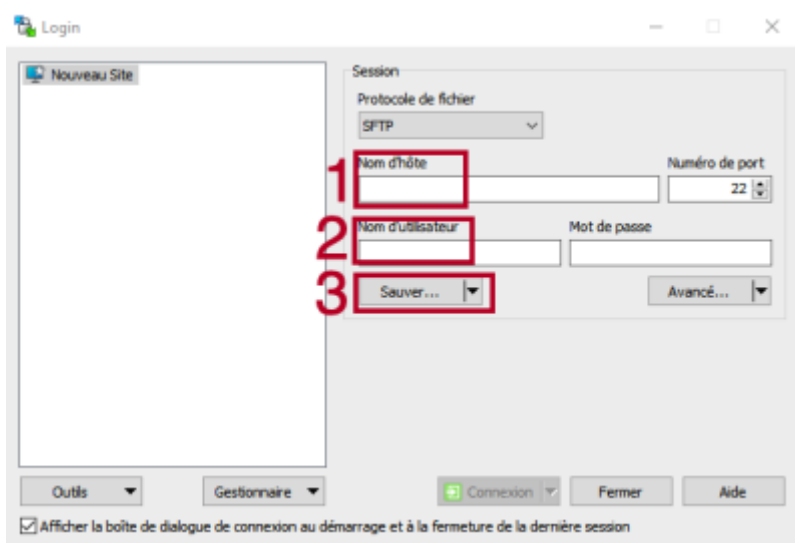
Avec la passerelle `gw-ssh.cnam.fr`, **avant** la connexion il faut avoir lancé `ssh-agent (1)` et avoir chargé la clef SSH avec `ssh-add (1)`. Lors de la connexion, la saisie du mot de passe est requise :





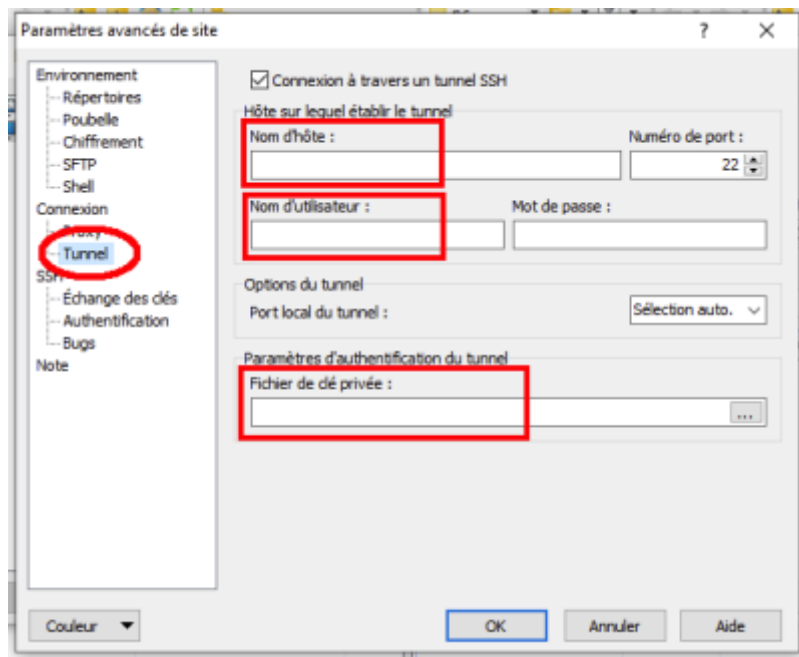
Avec WinSCP sur Windows

WinSCP est un client SCP graphique populaire sous Windows ; il se télécharge (c'est un logiciel libre et gratuit) sur le site officiel : <https://winscp.net/eng/download.php>. Après installation, le lancer. Configurer un « Nouveau site » en paramétrant le serveur final avec son nom DNS et le nom d'utilisateur ; enregistrer.



Dans le menu « Outils », on retrouvera les outils Pageant (agent SSH) et PuTTYgen (création de clef)¹⁾. Ils sont documentés sur la page [Utiliser SSH](#).

Charger ce site et cliquer sur « Avancé ». Cliquer sur l'onglet « Tunnel » et paramétrer le nom DNS du bastion et le nom d'utilisateur sur le bastion ; si une clef SSH est attendue, paramétrer le chemin :



Cliquer sur les ... à droite du cartouche et sélectionner le fichier de clé créé avec PuTTYgen et chargé avec Pageant.

Il ne reste qu'à se connecter.



Avec la passerelle `gw-ssh.cnam.fr`, **avant** la connexion il faut avoir lancé Pageant et avoir chargé la clé SSH.

← [Accès distants](#)

1)

En effet, ils sont fournis avec WinSCP.

From:

<https://assistancedsi.cnam.fr/> - **Assistance DSI**

Permanent link:

<https://assistancedsi.cnam.fr/kb/1202>

Last update: **2024/11/12 07:27**

