The Bastion

SSH

fichier de conf hardening ssh

nano /etc/ssh/sshd_config.d/ssh-hardening.conf

```
Port 60222
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
Protocol 2
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-512,hmac-sha2-256
AllowUsers sysadmin
#AllowGroups
X11Forwarding no
AllowAgentForwarding no
LoginGraceTime 1m
MaxAuthTries 3
ClientAliveInterval 300
ClientAliveCountMax 0
KexAlgorithms curve25519-sha256@libssh.org
LogLevel VERBOSE
```

création des clés ssh

```
Get-Service ssh-agent | Set-Service -StartupType Automatic

Start-Service ssh-agent

Get-Service ssh-agent
```

```
ssh-keygen -t ed25519 -C "mon_commentaire"

ssh-add $env:USERPROFILE\.ssh\id_ed25519
```

Alias ssh

il est possible de faire un fichier configuration qui permet de faciliter la connexion ssh

```
# Configuration globale
Host *
    ForwardAgent no
    ForwardX11 no
    IdentitiesOnly yes ## n'autorise les connexion qu'avec des clés ssh


# Alias pour un autre serveur avec clé spécifique
Host bssh
    HostName 192.168.0.25
    User bastion
    Port 60222
    IdentityFile ~/.ssh/bastion ## la clé privé
    Compression yes
    LogLevel INFO
```

ajout de de la clé ssh dans le authorized keys

rajouter la clé dans le dossier de l'utilisateur avec lequel vous voulez vous connecter

```
cd /home/sysadmin/.ssh

sudo nano authorized_keys

rajouter dans ce fichier votre clé publique
```

Qu'est-ce que The Bastion ?

The Bastion est un bastion (ou jump server) SSH conçu pour sécuriser et contrôler l'accès aux serveurs d'une organisation. Il agit comme un point central par lequel toutes les connexions SSH passent, permettant une surveillance et un contrôle stricts des accès.

Fonctionnalités principales :

1. **Contrôle d'accès centralisé** : The Bastion permet de centraliser et de gérer l'accès à tous les serveurs via SSH à partir d'un seul point d'entrée. Les utilisateurs doivent se connecter au bastion avant d'accéder aux serveurs finaux.
2. **Auditabilité** : Chaque connexion SSH passant par The Bastion est enregistrée, ce qui permet une traçabilité complète des actions des utilisateurs. Les logs détaillés facilitent les audits de sécurité et la conformité réglementaire.
3. **Sécurité renforcée** : En limitant les accès SSH directs aux serveurs, The Bastion réduit la surface d'attaque et ajoute une couche supplémentaire de sécurité. Il peut également appliquer des politiques de sécurité strictes, telles que l'authentification multifactorielle (MFA).
4. **Isolation des environnements** : The Bastion peut être configuré pour isoler différents environnements (production, développement, etc.), permettant ainsi de restreindre les accès en fonction des rôles des utilisateurs.
5. **Facilité d'utilisation** : Il fournit des outils conviviaux pour les utilisateurs finaux et les administrateurs, facilitant la gestion des accès sans compromettre la sécurité.

Comment fonctionne The Bastion :

1. **Connexion initiale** : L'utilisateur se connecte au bastion via SSH avec ses informations d'authentification.
2. **Vérification d'accès** : The Bastion vérifie les permissions de l'utilisateur et enregistre la tentative de connexion.
3. **Redirection sécurisée** : Une fois l'authentification réussie, l'utilisateur peut se connecter aux serveurs cibles via The Bastion. Toutes les connexions sont redirigées et surveillées.
4. **Enregistrement des sessions** : Les sessions SSH sont enregistrées pour audit et analyse. Les actions des utilisateurs peuvent être rejouées si nécessaire pour des vérifications postérieures.
5. **Déconnexion** : Lorsque l'utilisateur termine sa session, The Bastion enregistre la déconnexion et met à jour les logs.

Avantages de l'utilisation de The Bastion :

- **Sécurité accrue** grâce à la centralisation des accès et à la surveillance des sessions.
- **Auditabilité** facilitée par les logs détaillés et l'enregistrement des sessions.
- **Contrôle d'accès simplifié** grâce à la gestion centralisée des permissions.
- **Réduction de la surface d'attaque** en empêchant les accès SSH directs aux serveurs sensibles.

Image avec un petit dessin que j'aime bien pour son petit dessin en bas à gauche qui llustre bien le fonctionnement de the bastion

Pour mieux comprendre ce schéma, je vous invite à aller sur la page di lien ci-dessous
https://blog.ovhcloud.com/the-ovhcloud-bastion-part-1/

Installation de the bastion

Cette commande télécharge le code source de "The Bastion" depuis le dépôt GitHub officiel et le place dans le répertoire /opt/bastion sur le serveur

```
sudo git clone https://github.com/ovh/the-bastion /opt/bastion
```

Cette commande change le répertoire de travail en /opt/bastion et bascule le code sur le tag le plus récent du dépôt.

```
sudo git -C /opt/bastion checkout $(git -C /opt/bastion tag | tail -1)
```

Installation des paquets necessaires

Ce script vérifie les paquets nécessaires pour le bon fonctionnement de "The Bastion" et les installe si nécessaire.

> `/opt/bastion/bin/admin/packages-check.sh -i`

Installe ttyrec, un outil pour enregistrer les sessions de terminal.

> `/opt/bastion/bin/admin/install-ttyrec.sh -a`

Installe le Yubico PIV Checker, un outil pour vérifier les YubiKeys (dispositifs d'authentification physique).

> `/opt/bastion/bin/admin/install-yubico-piv-checker.sh -a`

Installe le helper mkhash pour la gestion des mots de passe et des hashes.

> `/opt/bastion/bin/admin/install-mkhash-helper.sh -a`

Chiffrement de la partition home

Ce script configure le chiffrement du dossier home pour protéger les clés SSH et autres données sensibles.

> `/opt/bastion/bin/admin/setup-encryption.sh`

Installation de The bastion

Lance le processus d'installation de "The Bastion" sur le système.

> sudo /opt/bastion/bin/admin/install --new-install

Revoir la configuration

Modifier le nom de votre bastion

> `sudo nano /etc/bastion/bastion.conf`

```
# bastionName (string)
#    DESC: This will be the name advertised in the aliases admins will give to bastion users, and also in the banner of>
# DEFAULT: "fix-my-config-please-missing-bastion-name"
"bastionName": "TheBastion",
#
```

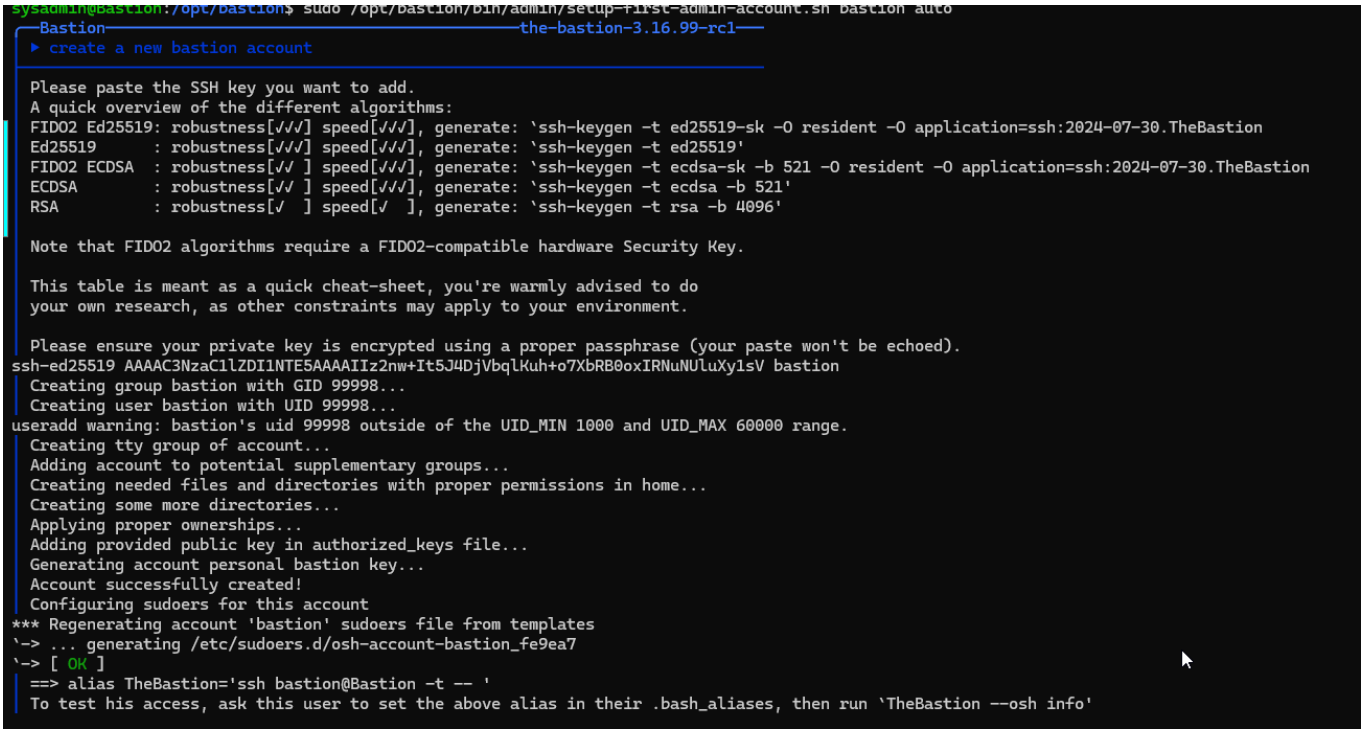
Vérifie les modules Perl nécessaires au bon fonctionnement de "The Bastion

> `/opt/bastion/bin/dev/perl-check.sh`

Crée son premier compte bastion

Ce script crée le premier compte administrateur sur "The Bastion". Le USERNAME doit être remplacé par le nom d'utilisateur souhaité

```
sudo nano /opt/bastion/bin/admin/setup-first-admin-account.sh USERNAME auto
```



Configuration d'une connexion ssh avec le bastion

Se connecter premièrement avec l'utilisateur crée avant sur le bastion

```
ssh bastion@192.168.0.49 -p 22 -i .\.ssh\bastion
```

Cette commande vérifie le bon fonctionnement du bastion et affiche ses informations général

bssh --osh info

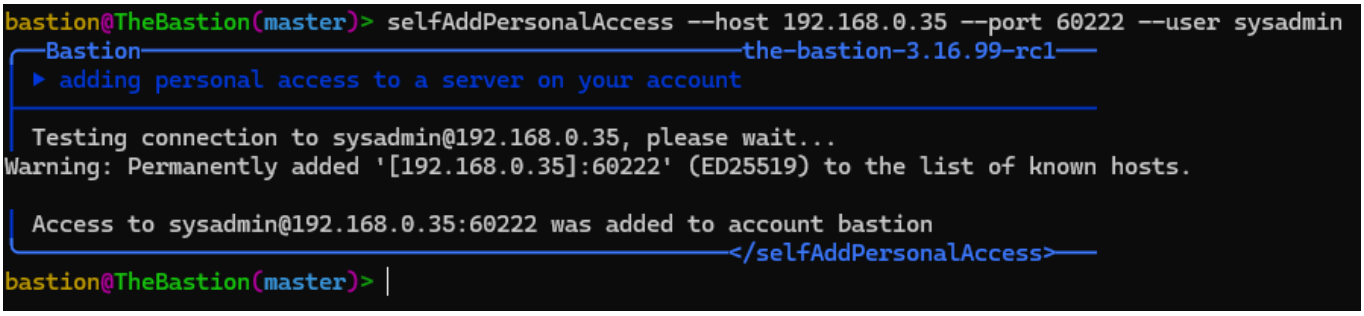
```
afin de récuperer la clé publique
```

selfListEgressKeys

- **Copier la clé publique**
- **Aller sur le client sur lequel on souhaite se connecter en ssh**
- **Rajouter la clé publique dans le authorized keys de votre utilisateur**

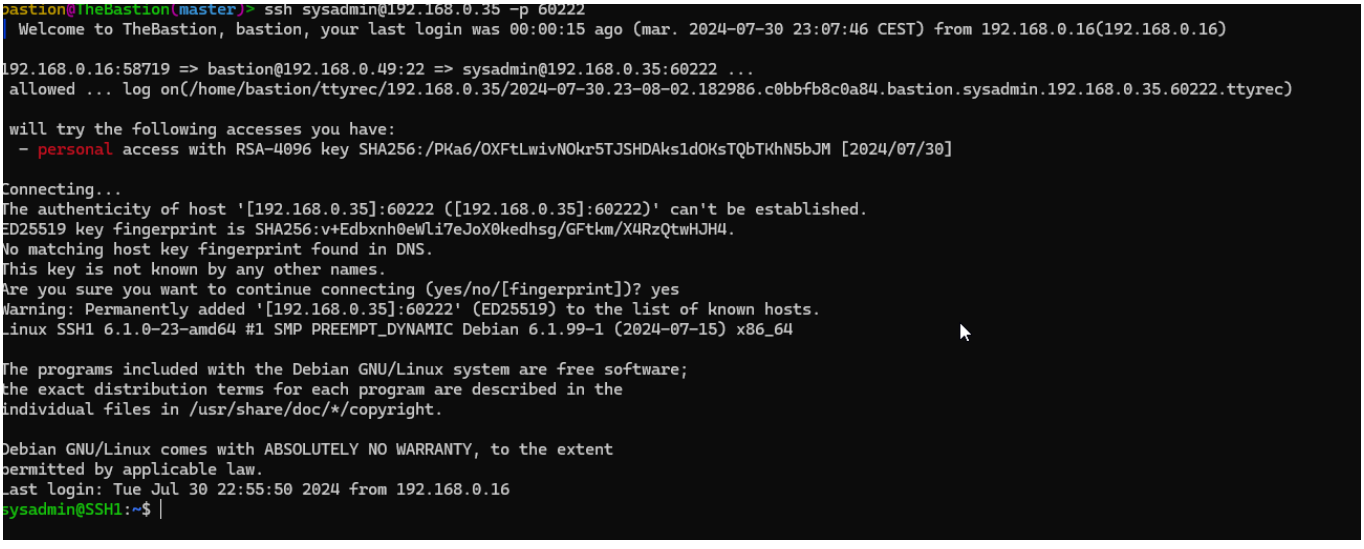
Maintenant, nous pouvons enregistrer la connexion dans the bastion

```
selfAddPersonalAccess --host 192.168.0.35 --port 60222 --user sysadmin
```



Connexion au client

```
ssh sysadmin@192.168.0.35 -p 60222
```



Utilisation de ttyrec

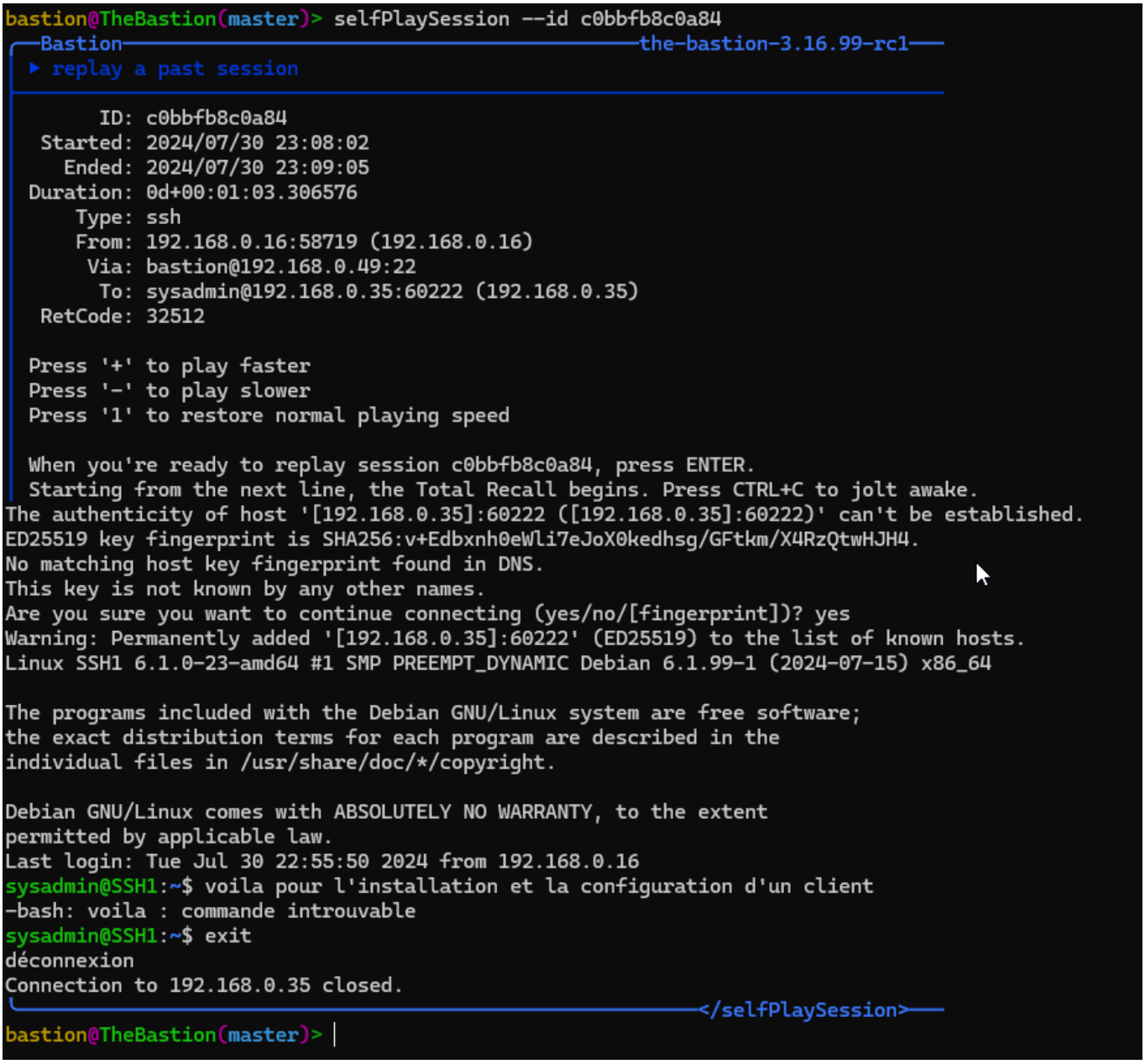
Cette outils va vous permettre d'enregistrer les sessions ssh effectués et de la regarder

Récupération de l'id de session ssh

```
selfListSessions --type ssh --detailed
```

Lancement de l'enregistrement de la session

```
selfPlaySession --id [id-de-votre-session]
```



Utilisateur et groupe

Lors de la création d'utilisateur ou de groupe, nous pouvons choisir d'utiliser une clé publique pour tout le groupe et d'en avoir pour chaque utilisateur

Création d'un groupe

> `groupCreate --group Tech --owner Test --encrypted --algo Ed25519`

Création d'un compte

`account Create --account Test --uid-auto --no-key`

> `accountCreate --account Test --uid-auto --public-key "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILkyp9jeTMvTv378WQUST9tJSZt3qAdOhqjFTn6pOsku SSH2"`

Suivant ce que vous avait chosi vous pouvez récuperer la clé publique de votre utilisateur ou de votre groupe et l'ajouter sur la machine sur laquelle vous souhaitez vous connecter

Maintenant, nous pouvons enregistrer la connexion dans the bastion

> `selfAddPersonalAccess --host 192.168.0.35 --port 60222 --user Test

Pour aller plus loin

il y a une grosse partie d'hardening de the bastion avec du MFA, chiffrement, PGP, Remote Backup.

Il est possible de mettre en place une connexion avec un mot de passe généré et stocké par the bastion si besoin.

Webographie

Lien de la documentation officiel de the bastion
https://ovh.github.io/the-bastion/