



Déploiements de WALLIX Bastion

MAAOUFAL

Sommaire

1. Déploiement de Wallix Bastion

- 1.1 Démarrage de l'installation
- 1.2 Sélection de la langue et du clavier
- 1.3 Configuration initiale

2. Déploiement de Access Manager

- 2.1 Création de la machine virtuelle

3. Installation du Bastion Wallix

- 3.1 Première installation
- 3.2 Configuration des mots de passe :
 - wabadmin
- 3.3 Politique de sécurité des mots de passe

4. Configuration réseau du Bastion

- 4.1 Définition du hostname
- 4.2 Configuration du DNS
- 4.3 Définition du FQDN

5. Finalisation de l'installation

- 5.1 Accès au compte admin
- 5.2 Changement du mot de passe admin
- 5.3 Paramètres supplémentaires

6. Configuration des accès (Access Manager)

- 6.1 Création d'un groupe d'utilisateurs
- 6.2 Création d'un compte local
- 6.3 Création d'une cible (serveur)
- 6.4 Association d'un service
- 6.5 Création d'un groupe de cibles
- 6.6 Association des éléments

7. Gestion des accès aux serveurs

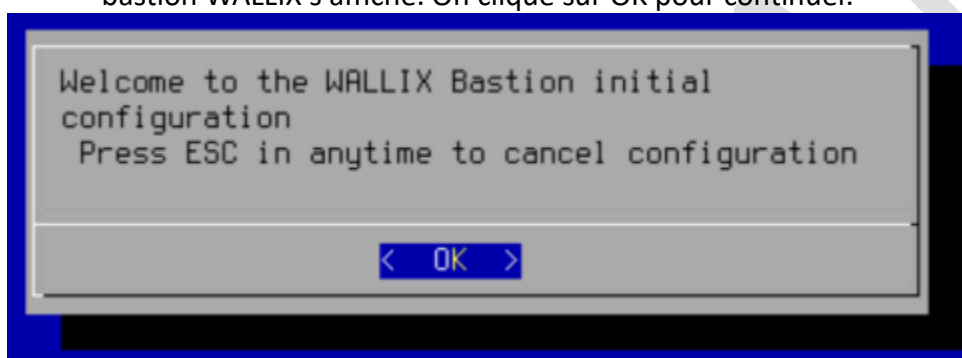
- 7.1 Association :
 - cible
 - service (SSH)
 - compte secondaire
- 7.2 Accès pour les utilisateurs

8. Connexion via WALLIX-PuTTY

- 8.1 Utilisation du fichier de session
- 8.2 Processus d'authentification :
 - authentification utilisateur
 - récupération du compte secondaire
 - connexion SSH vers la cible

DEPLOIEMENT DE WALLIX BASTION :

1. Au démarrage, un message de bienvenue pour la configuration initiale du bastion WALLIX s'affiche. On clique sur OK pour continuer.



2. Sélectionnez la langue et l'emplacement de la disposition de clavier souhaitée. (Français dans notre cas)

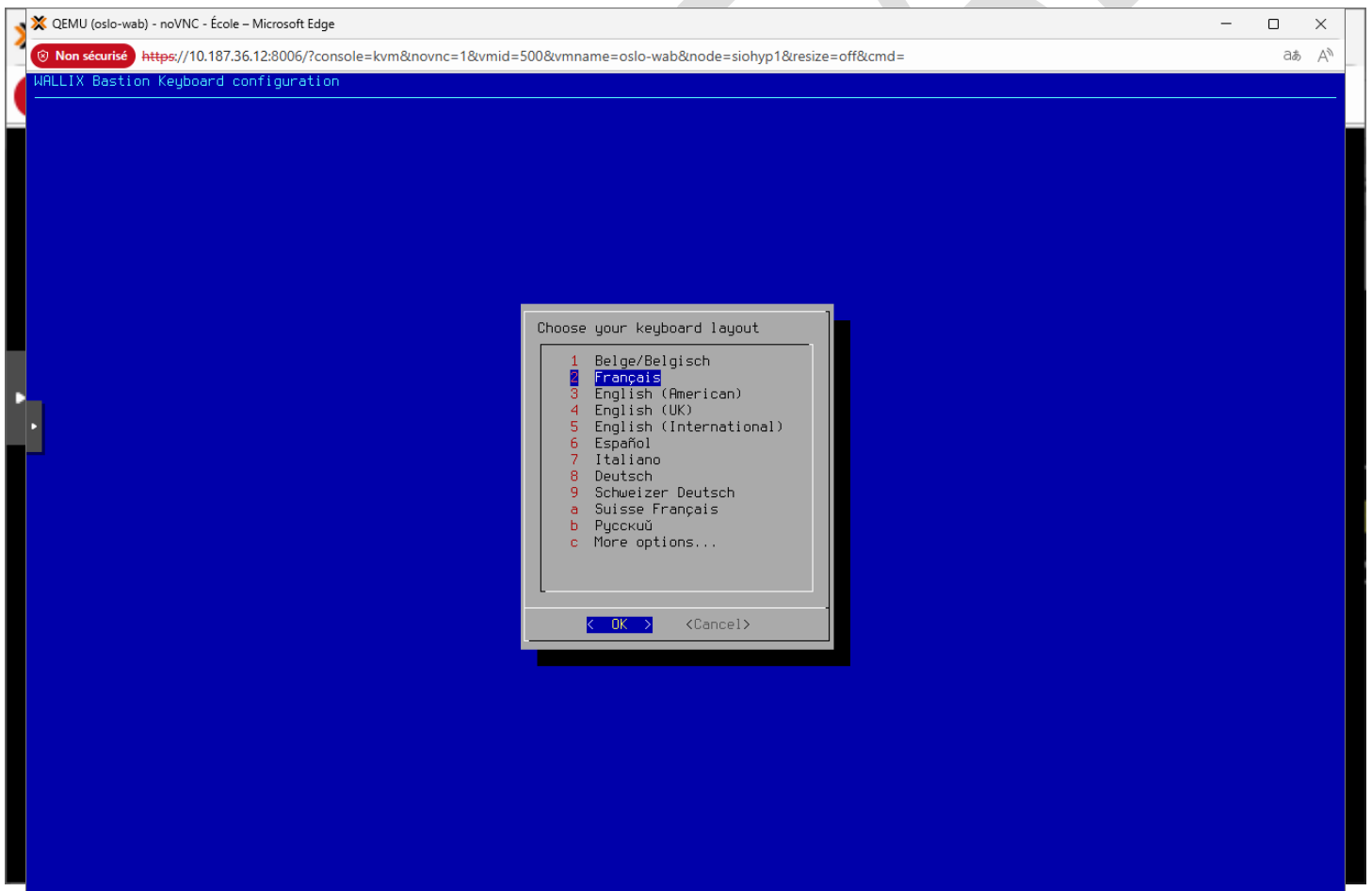


3. .

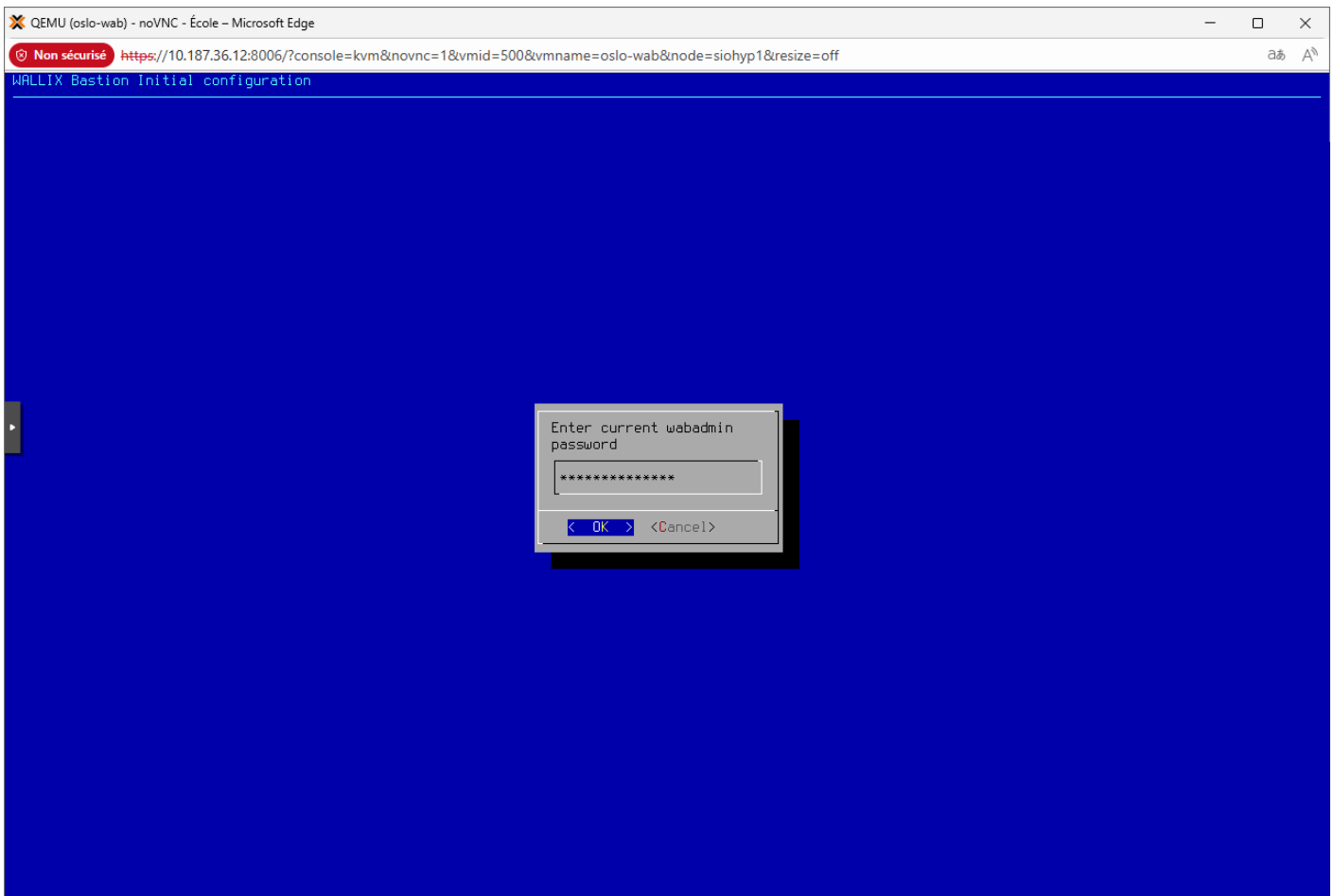
DEPLOIEMENT DE ACCESS MANAGER :

4. Création d'une VM :
- Nom : Access Manager
 - 2 cœurs
 - 4 Gio de RAM
 - 40 Gio de disque dur
 - 1 Interface réseau

CONFIGURATION DU BASTION WALLIX INSTALLATION DU BASTION 1RE INSTALLATION



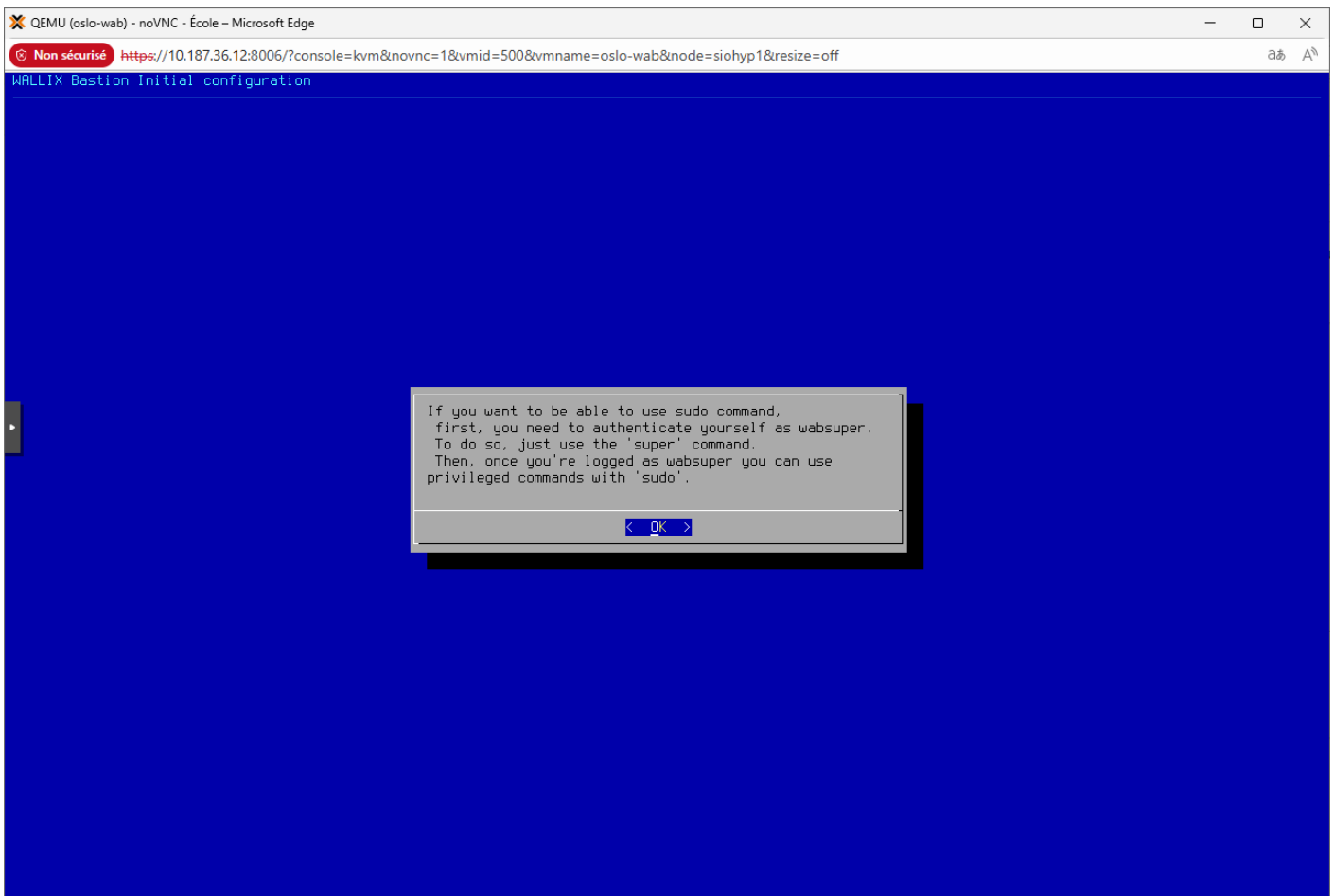
5. Saisir le mot de passe par défaut **SecureWabAdmin** du compte **wabadmin**



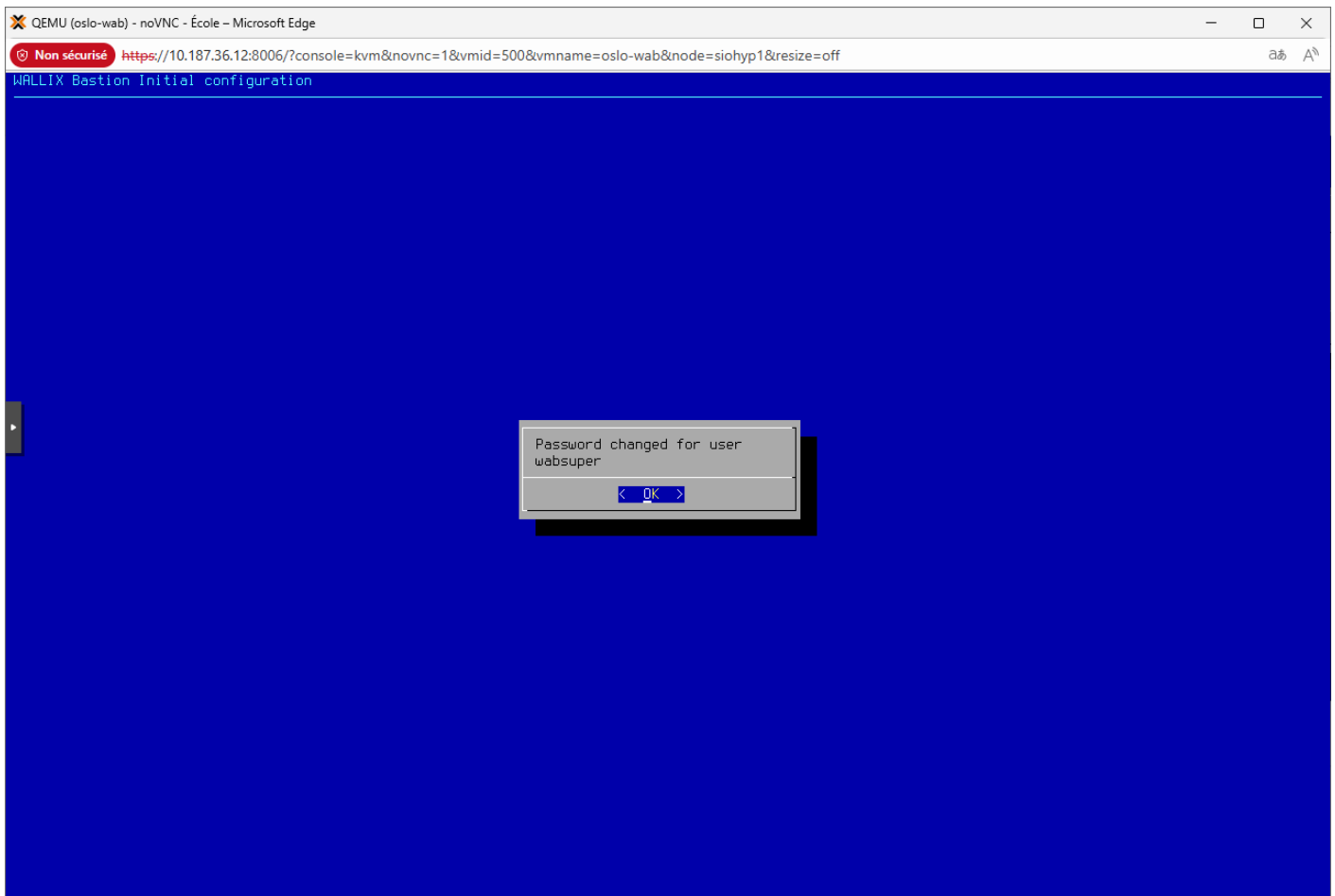
6. définir un nouveau mot de passe avec les caractéristiques suivantes :

- longueur minimale : 14
- caractère spécial : 1 minimum
- lettre majuscule : 1 minimum
- lettre minuscule : 1 minimum
- caractère numérique : 1 minimum

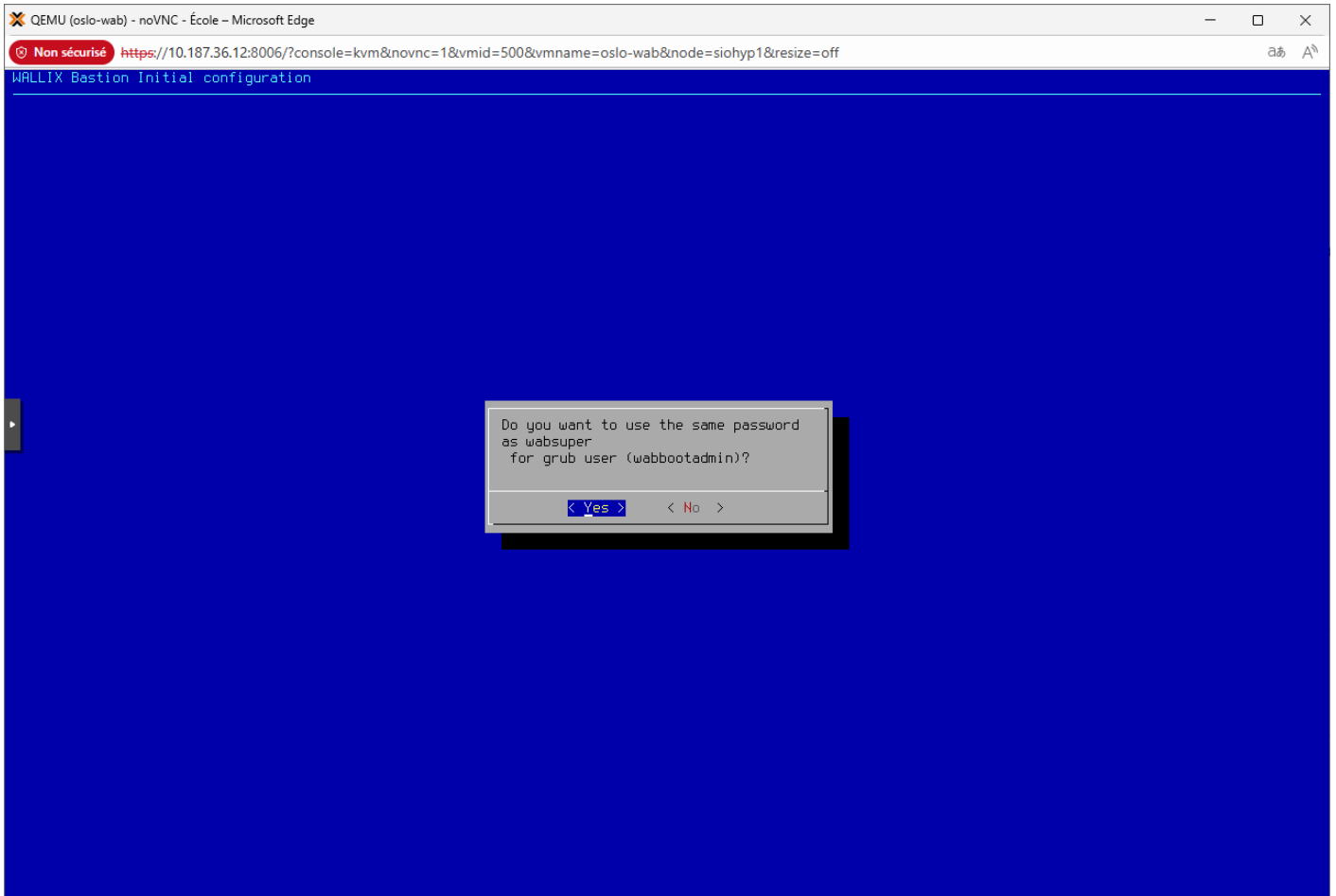
* => P@\$\$w0rd2025Secure



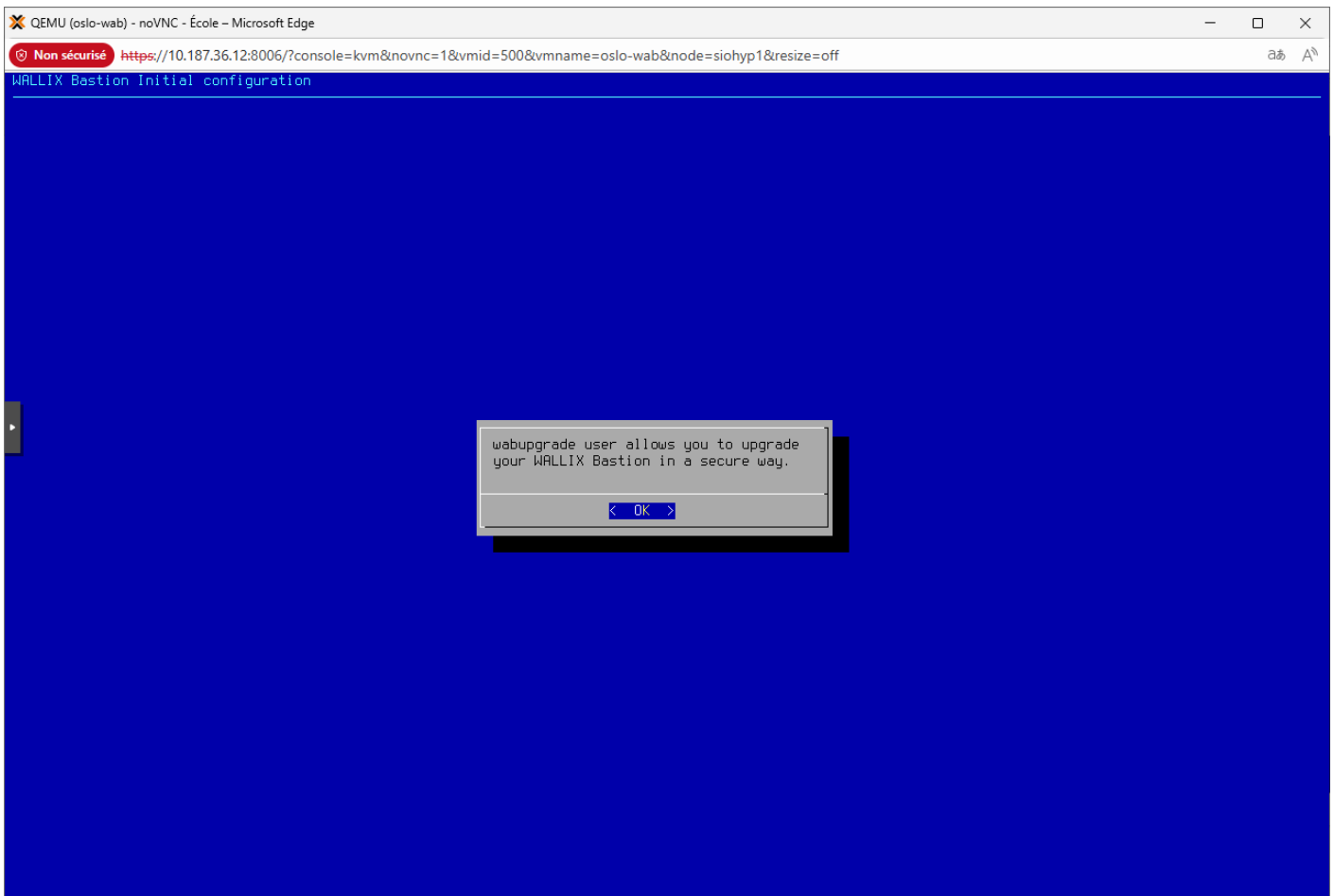
- Définir le mot de passe du compte **wabsuper** ⇒ P@\$swOrd2025Secure



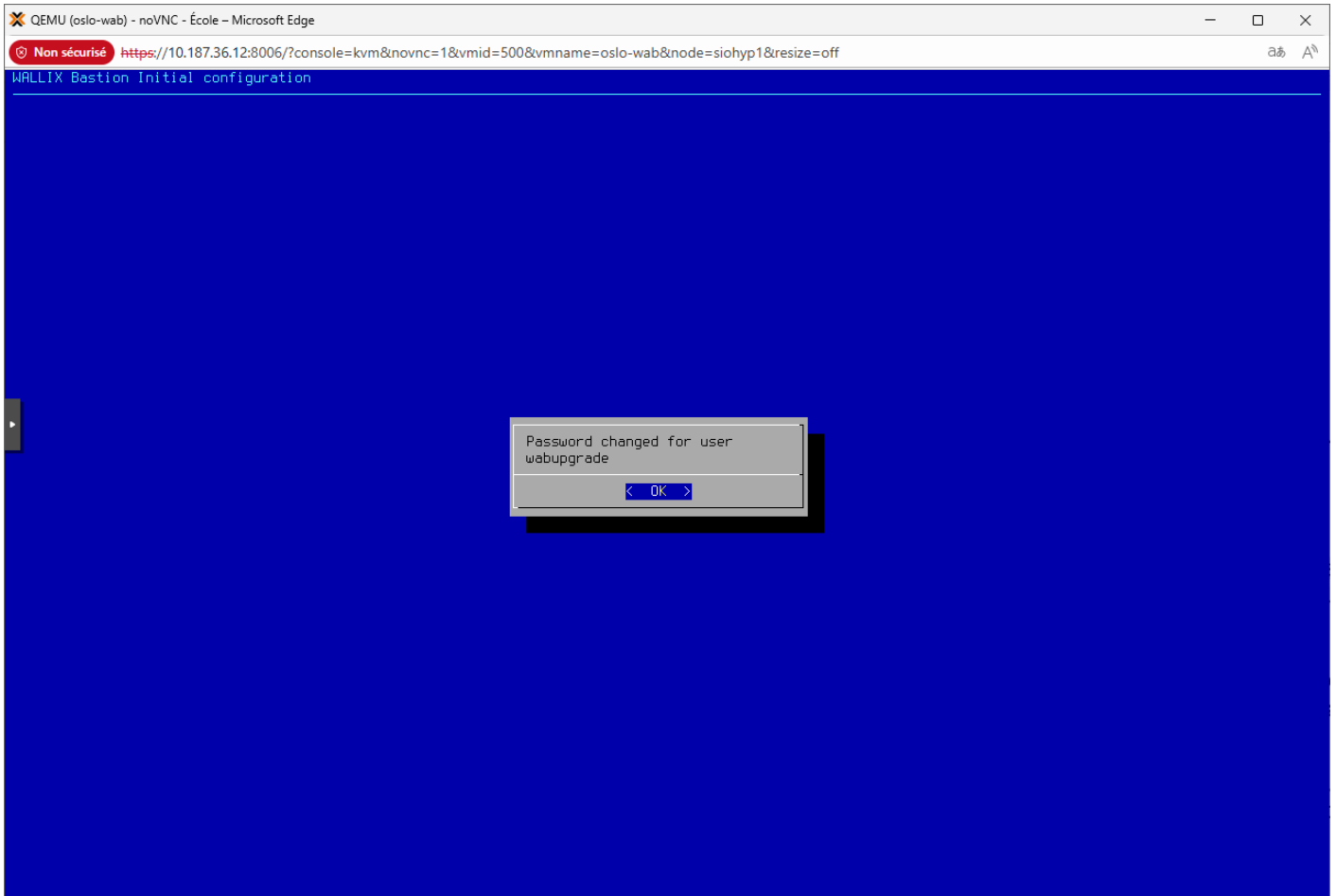
7. Définir le même mot de passe du compte **wabsuper** pour le compte **wabbootadmin** ⇒ P@\$\$w0rd2025Secure



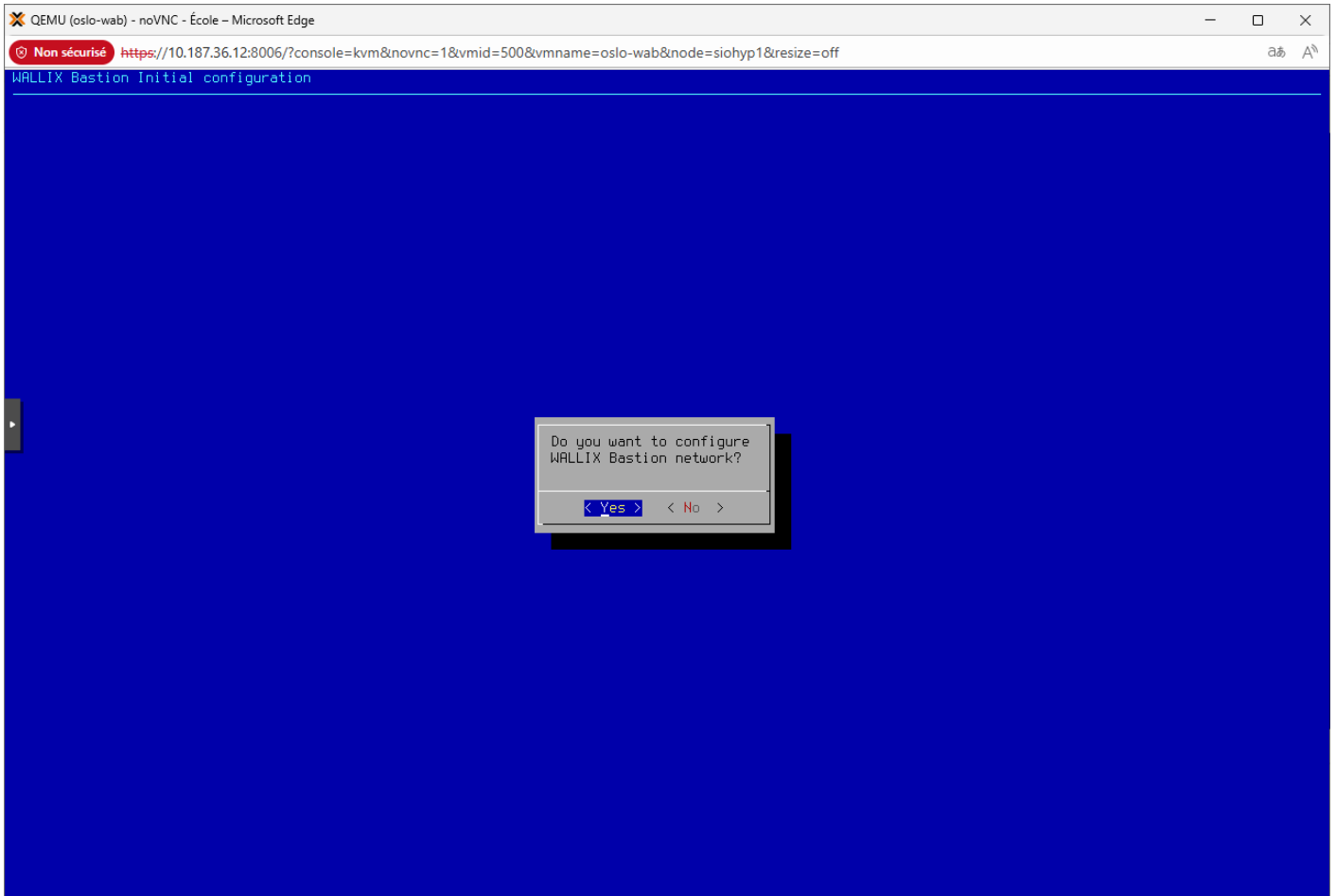
MAJ



8. Définir le mot de passe du compte **wabupgrade** ⇒ P@\$\$w0rd2025Secure



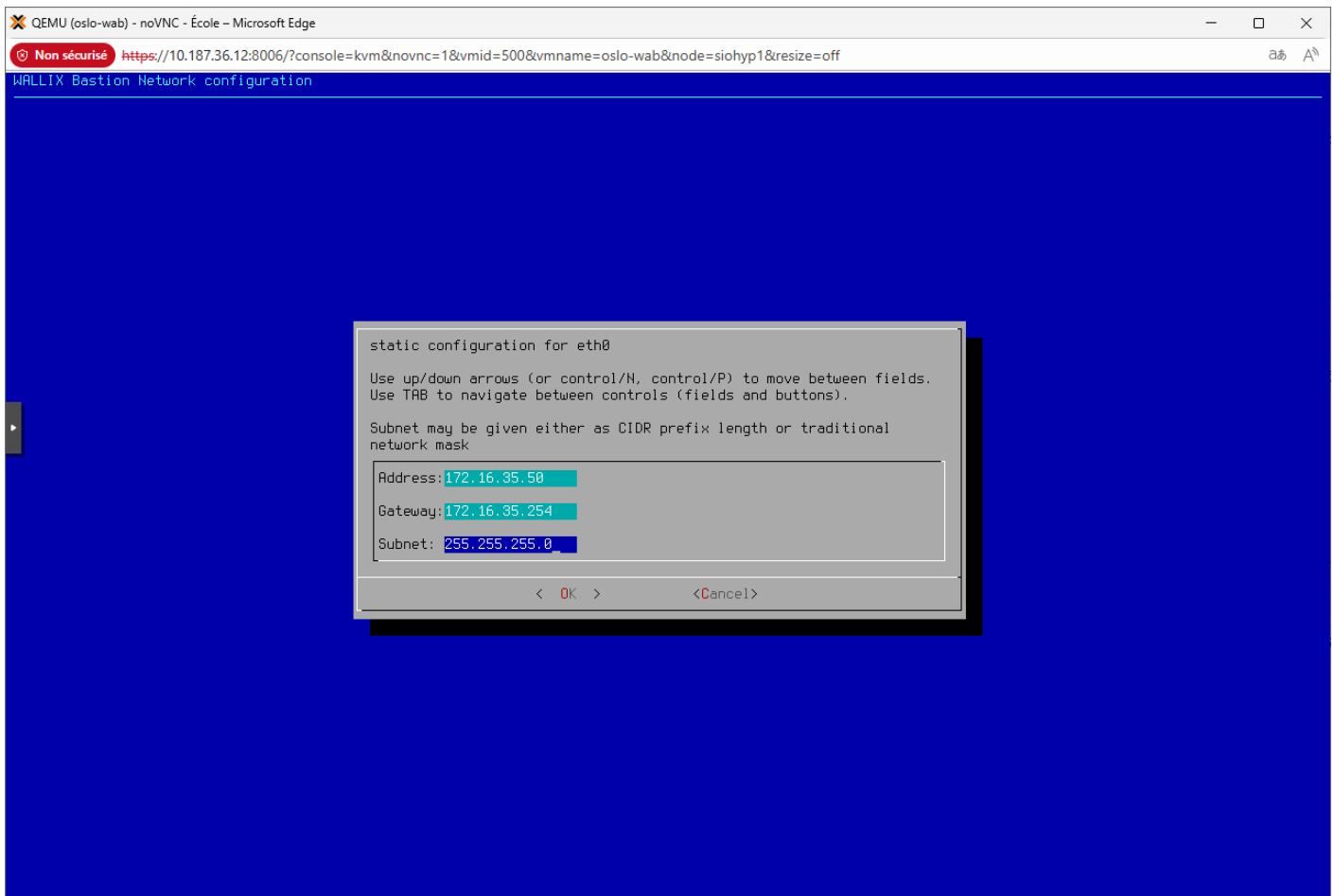
MAJ



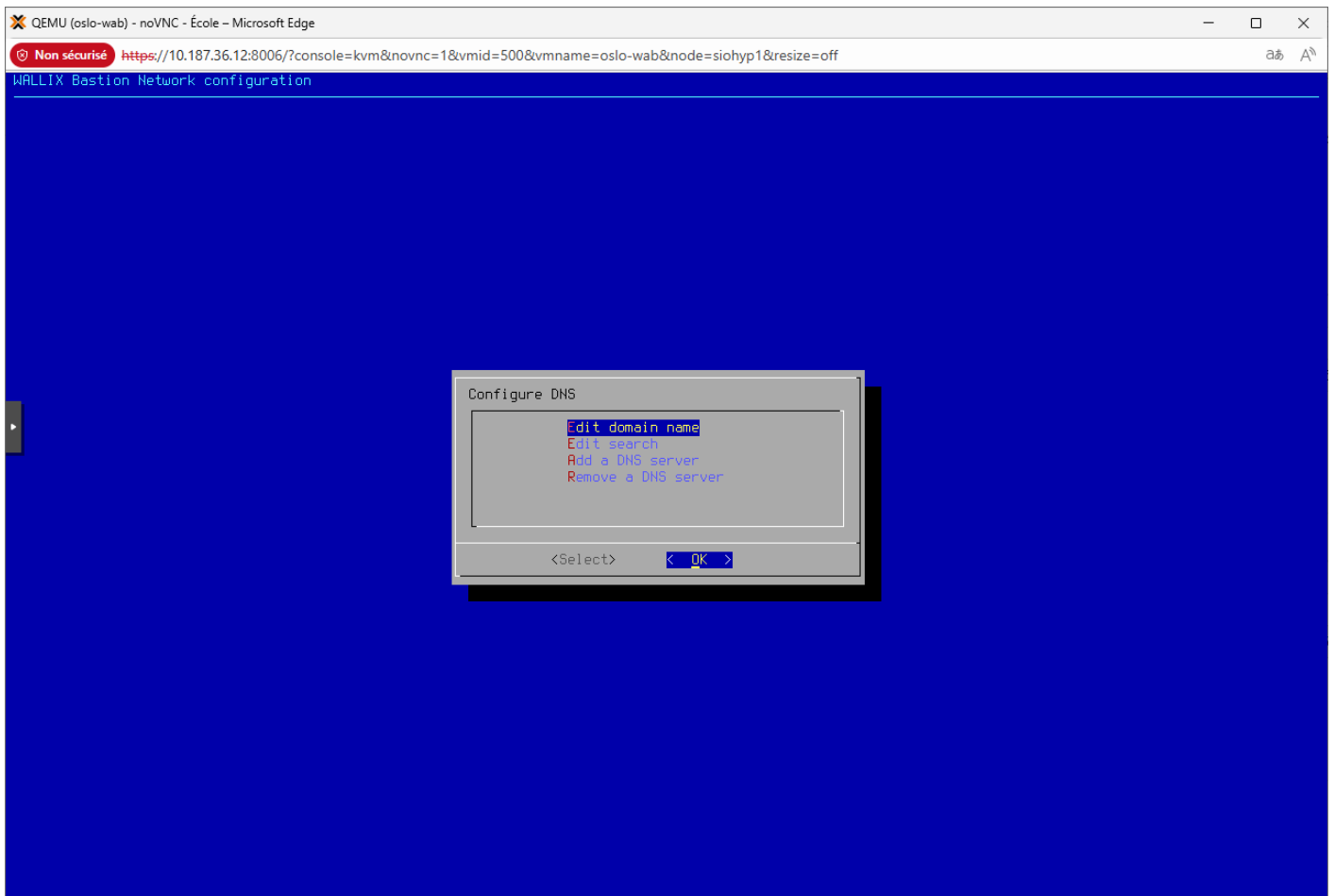
MAJ

CONFIGURATION RESEAU DU BASTION

DEFINITION DU HOSTNAME

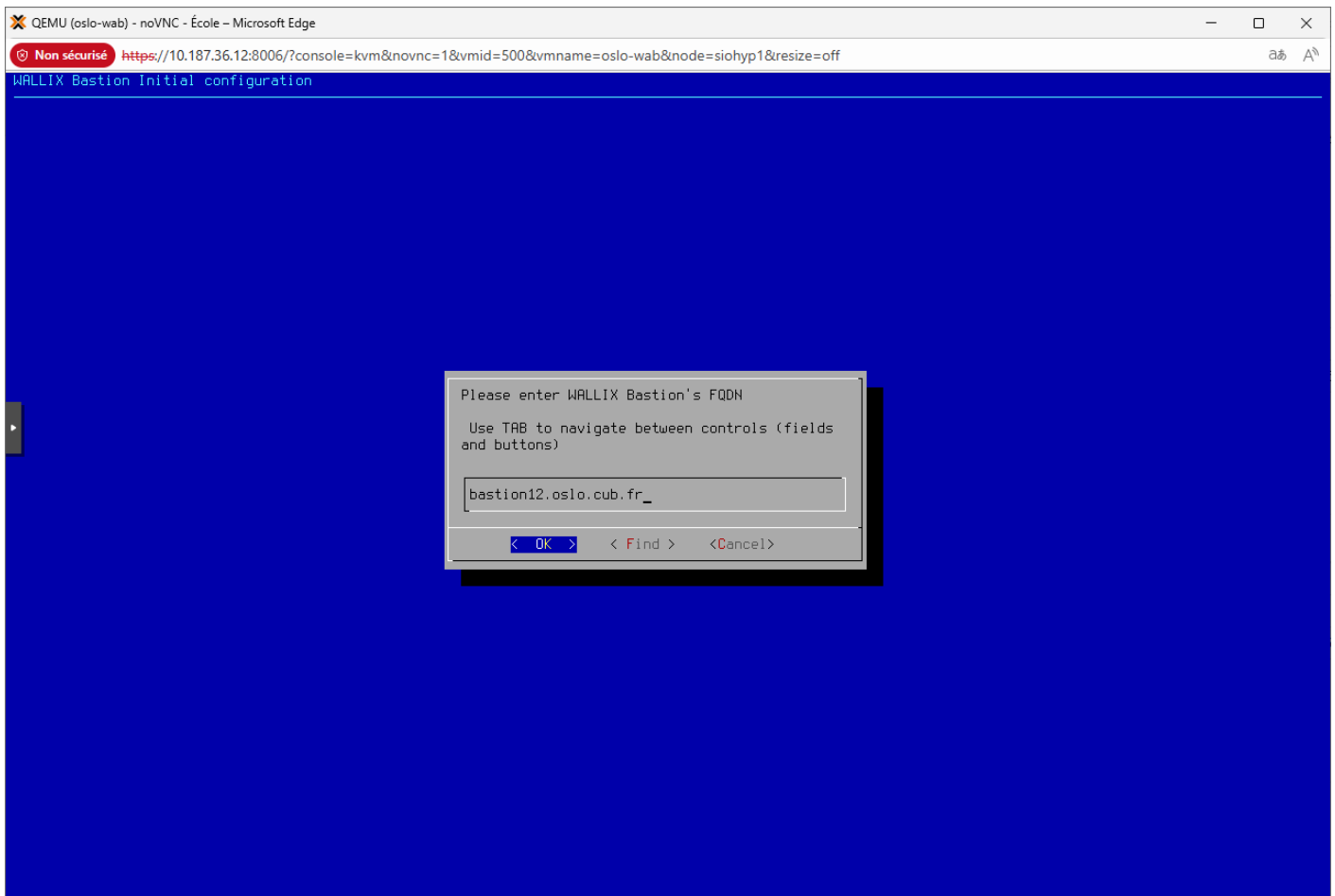


DEFINITION DU DNS

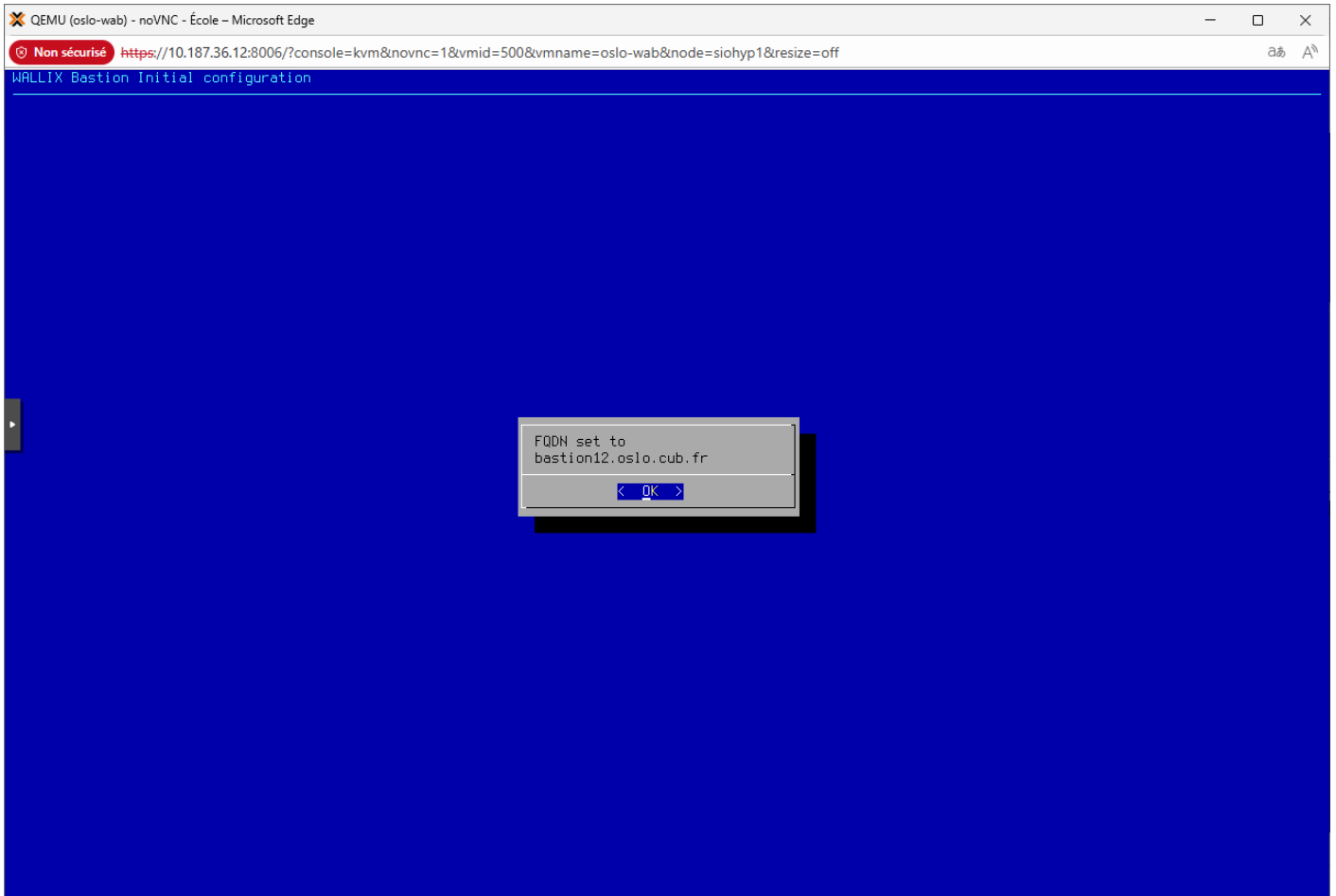


MAC

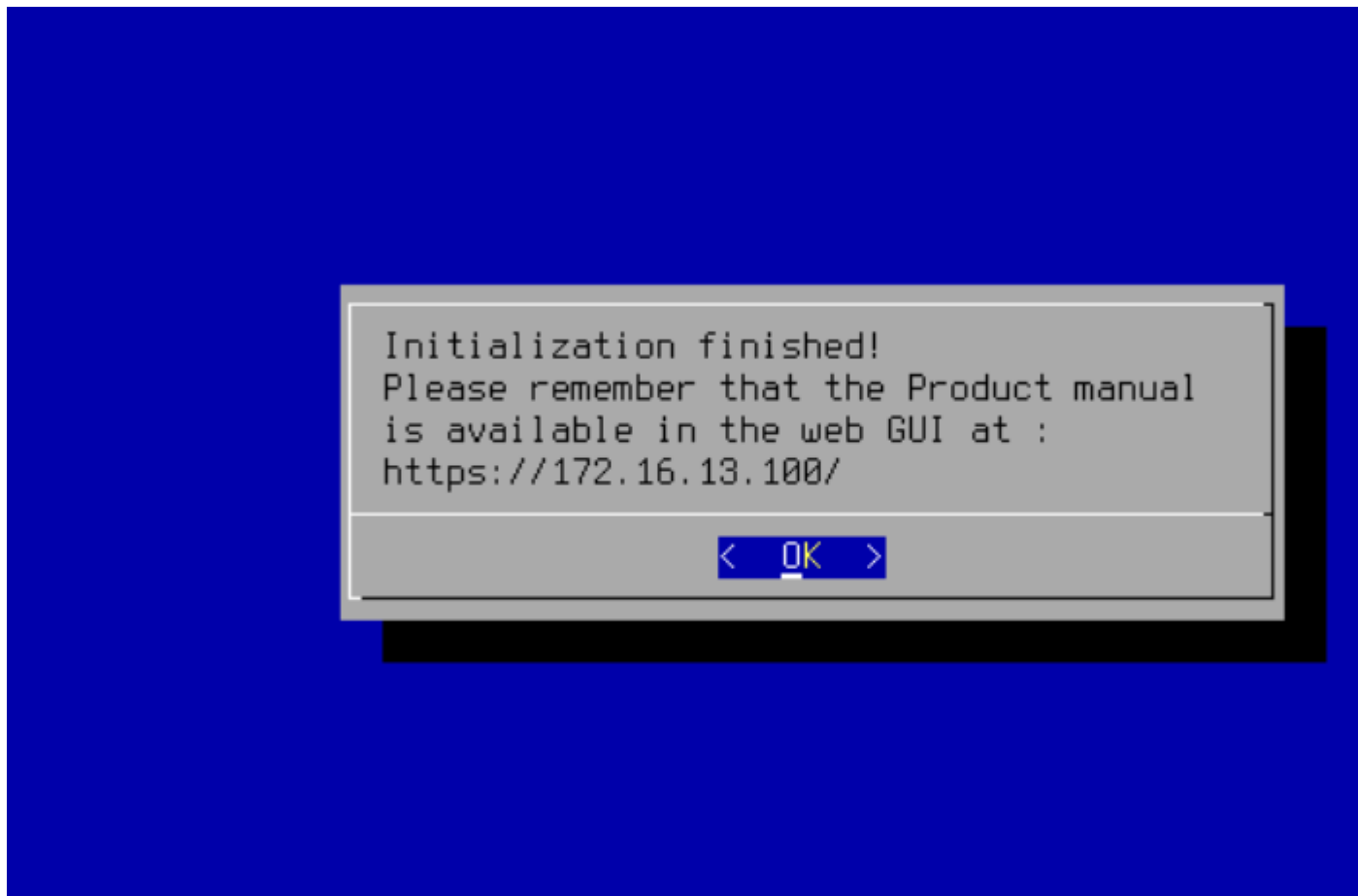
DEFINITION DU FQDN (FULLY QUALIFIED DOMAIN NAME):



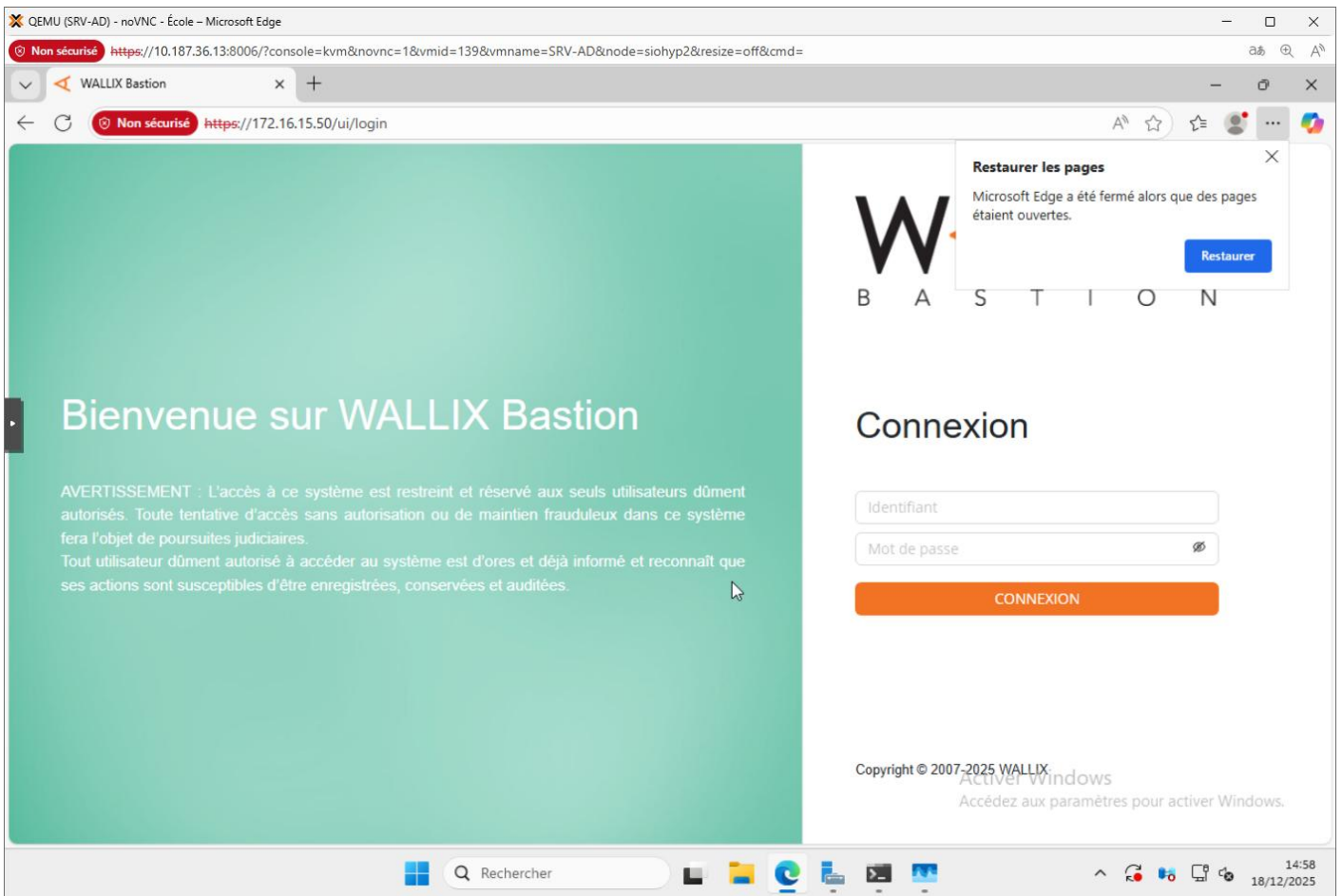
MAC



FIN DE LA 1RE PARTIE DE L'INSTALLATION



9. Saisir le mot de passe par défaut **admin** du compte **admin**



QEMU (SRV-AD) - noVNC - École - Microsoft Edge

Non sécurisé <https://10.187.36.13:8006/?console=kvm&novnc=1&vmid=139&vmname=SRV-AD&node=siohyp2&resize=off&cmd=>

WALLIX Bastion

Non sécurisé <https://172.16.15.50/ui/login>

Bienvenue sur WALLIX Bastion

AVERTISSEMENT : L'accès à ce système est restreint et réservé aux seuls utilisateurs dûment autorisés. Toute tentative d'accès sans autorisation ou de maintien frauduleux dans ce système fera l'objet de poursuites judiciaires.
Tout utilisateur dûment autorisé à accéder au système est d'ores et déjà informé et reconnaît que ses actions sont susceptibles d'être enregistrées, conservées et auditées.

Restaurer les pages

Microsoft Edge a été fermé alors que des pages étaient ouvertes.

Restaurer

Réinitialiser le mot de passe

En tant que **admin**

! Your password has been reset, you must change your password.

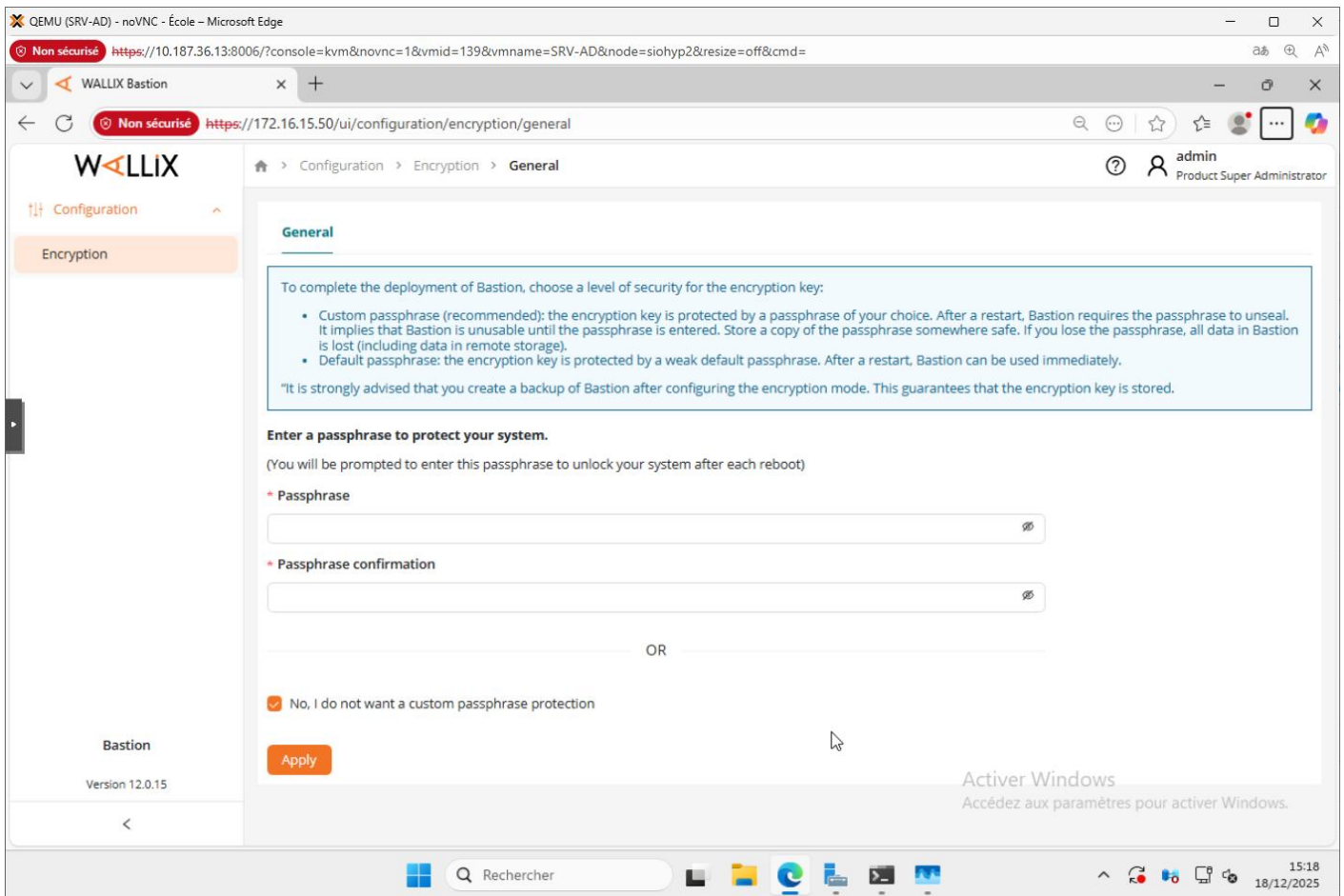
ANNULER OK

Copyright © 2007-2025 WALLIX

Active Windows
Accédez aux paramètres pour activer Windows.

15:10
18/12/2025

10. Définir le mot de passe du compte **admin** ⇒ P@\$\$w0rd2025Secure



- Ne pas saisir de passphrase
 - https://wallix.groupevalophis.fr/webhelp/fr/Bastion-user-guide/index.html#id-sect-ssh_putty.html
 - <https://github.com/wallix/WALLIX-PuTTY/releases>

-
-
-

La première étape a consisté à déployer les machines nécessaires à la solution :

Un conteneur Wallix Bastion ; une machine virtuelle Access Manager ; plusieurs conteneurs cibles à administrer ; un serveur Active Directory utilisé comme poste d'administration.

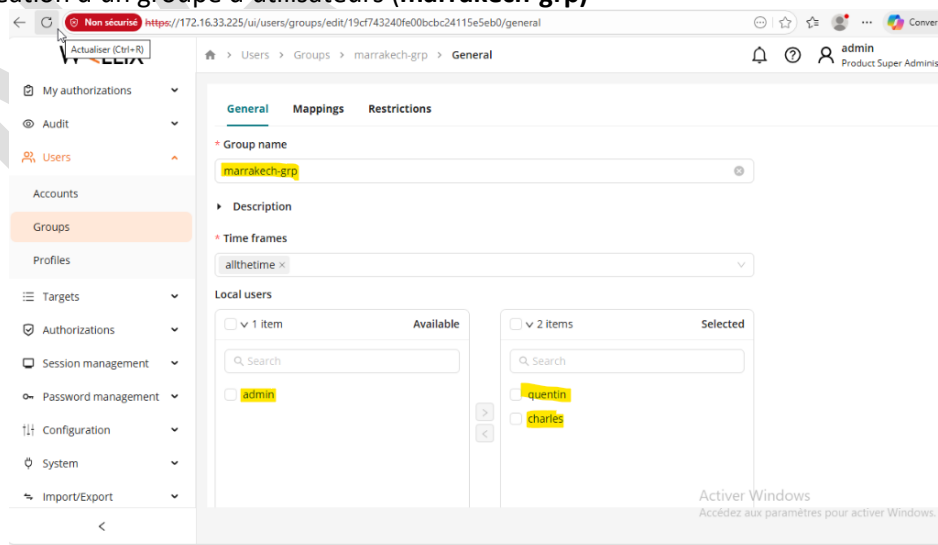
Une fois les machines déployées et accessibles sur le réseau, la configuration s'effectue via l'interface graphique du bastion.

Configuration des accès dans Access Manager :

La configuration des accès aux serveurs distants repose sur plusieurs objets : groupes d'utilisateurs, comptes locaux, cibles (serveurs), services d'accès, groupes de cibles

La mise en place a été réalisée selon les étapes suivantes :

1. Création d'un groupe d'utilisateurs (marrakech-grp)



Users > Groups

admin
Product Super Administrator

Add Delete

Name	Description	Time frames	Profile	Local
marrakech-grp	-	allthetime	-	2
Userlocal-grp	-	allthetime	-	0

1-2 of 2 entries < 1 > 20 / page

2. Création d'un compte local (nom de l'utilisateur, adresse e-mail,...)

Users > Accounts

admin
Product Super Administrator

Edit this user

User name: charles
Display name: --
Email: charles@oslo.cub.fr
Preferred language: fr
Source IP: --
Profile: user
Account expiration date: --
Locked: --
Disabled: --
Groups: marrakech-grp
Authentication and backup servers: local_password
Force password change: No
Password: ****
SSH public key: --
GPG fingerprint: --

Rights on GUI
 Authorizations on devices
 Authorizations on applications

Users > Accounts

admin
Product Super Administrator

Add a user

Show 10 entries Search:

User name	Display name	Profile	Authentication	Groups	Status	Last connection
admin	Product Super Administrator	product_administrator	local_password		✓	--
charles		user	local_password	marrakech-grp	✓	--
quentin	Quentin MAUJEAN	user	local_password	marrakech-grp	✓	2026-03-16 17:21:48

1 - 3 / 3

3. Création d'une cible (device, la machine sur laquelle l'administrateur souhaite se connecter)

4. Association d'un service à la cible

5. Création d'un groupe de cibles

6. Association de la cible, du service et du compte dans le groupe

La dernière étape consiste à associer les différents éléments créés :

la cible (serveur), le service SSH, le compte secondaire utilisé pour la connexion.

Cette association permet aux utilisateurs appartenant au groupe marrakech-grp d'accéder aux serveurs du groupe de cibles via le bastion.

Accès aux serveurs via WALLIX-PuTTY :

Une fois la configuration terminée, les utilisateurs peuvent se connecter aux machines distantes via WALLIX-PuTTY.

La connexion est effectuée à l'aide d'un fichier de session spécifique : WALLIX-PuTTY SSH Session File

- Ce fichier contient les informations nécessaires pour ouvrir une session SSH via le bastion.

Le processus de connexion est le suivant :

l'utilisateur s'authentifie sur le bastion avec son compte primaire, le bastion récupère le compte secondaire stocké dans le coffre sécurisé, la connexion SSH est établie vers la cible.