Demande d'accès CLI Cisco Cloud Email Security

Table des matières

Introduction

Ce document décrit comment demander l'accès à leur CLI de sécurité de messagerie électronique cloud (CES).

Informations générales

Les clients Cisco CES ont le droit d'accéder à l'interface de ligne de commande de leurs ESA et SMA par le biais d'un proxy SSH utilisant l'authentification par clé. L'accès à l'interface de ligne de commande de vos appareils hébergés doit être limité aux personnes clés de votre entreprise.

Utilisateurs Linux et Mac

Pour les clients Cisco CES :
Instructions pour un script shell utilisant SSH afin de rendre l'accès CLI via le proxy CES.

Conditions préalables

En tant que client CES, vous devez avoir engagé l'intégration/les opérations CES ou le centre d'assistance technique Cisco pour que les clés SSH soient échangées et placées :

1. Générez des clés RSA privées/publiques.
2. Fournissez à Cisco votre clé PublicRSA.
3. Attendez que Cisco enregistre et vous informe que vos clés ont été enregistrées sur votre compte client CES.
4. Copiez et modifiez le script connect2ces.sh.

Comment créer des clés RSA privées/publiques ?

Cisco recommande d'utiliser « ssh-keygen » sur le terminal/CLI pour Unix/Linux/OS X. Utilisez la commande ssh-keygen -b 2048 -t rsa -f ~/.ssh/<NOM> .

Remarque : Pour plus d'informations, visitez le site https://www.ssh.com/academy/ssh/keygen.
Assurez-vous que vous protégez l'accès à vos clés privées RSA à tout moment.
N'envoyez pas votre clé privée à Cisco, seulement la clé publique (.pub).
Lors de l'envoi de votre clé publique à Cisco, identifiez l'adresse e-mail/prénom/nom auquel la clé est destinée.

Comment ouvrir une demande d'assistance Cisco pour fournir ma clé publique ?

Accédez à ce lien.

Assurez-vous que vous avez correctement identifié le SR comme « Configuration SSH/CLI client Cisco CES », etc.

Configuration

Pour commencer, opencopiez le script fourni et utilisez l'un de ces hôtes proxy pour le nom d'hôte.

Assurez-vous de choisir le proxy approprié pour votre région (c'est-à-dire, si vous êtes un client CES des États-Unis, afin d'atteindre le data center et les appareils F4, utilisez le f4-ssh.iphmx.com. Si vous êtes un client CES de l'UE et que vous possédez un appareil en Allemagne, utilisez f17-ssh.eu.iphmx.com.).

AP (ap.iphmx.com)
f15-ssh.ap.iphmx.com
f16-ssh.ap.iphmx.com

CA (ca.iphmx.com)
f13-ssh.ca.iphmx.com

f14-ssh.ca.iphmx.com

UE (c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

UE (eu.iphmx.com) (Allemagne DC)
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

États-Unis (iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com

Que faire si je souhaite me connecter à plusieurs appareils de sécurité de la messagerie (ESA) ou appareils de gestion de la sécurité (SMA) ?

Copiez et enregistrez une deuxième copie de connect2ces.sh, telle que connect2ces_2.sh.

Remarque : Vous devez modifier le paramètre « cloud_host » pour qu'il corresponde à l'appliance supplémentaire à laquelle vous souhaitez accéder.
Vous voudrez modifier le 'local_port' pour qu'il soit AUTRE que 2222. Si ce n'est pas le cas, un message d'erreur « WARNING: L'IDENTIFICATION DE L'HÔTE DISTANT A CHANGÉ ! »

Comment puis-je configurer mon ESA ou SMA pour me connecter sans demander de mot de passe ?

Lisez ce guide.

À quoi cela ressemblera-t-il une fois que les conditions préalables seront remplies ?

joe.user@my_local > ~ ./connect2ces
[-] Connexion à votre serveur proxy (f4-ssh.iphmx.com)...
[-] Connexion proxy réussie. Désormais connecté à f4-ssh.iphmx.com.
[-] Proxy exécuté sur le PID : 31253
[-] Connexion à votre appliance CES (esa1.rs1234-01.iphmx.com)...

Dernière connexion : Lun Avr 22 11:33:45 2019 à partir de 10.123.123.123
AsyncOS 12.1.0 pour Cisco C100V build 071

Bienvenue dans l'appliance virtuelle de sécurité de la messagerie Cisco C100V

NOTE: Cette session expirera si elle reste inactive pendant 1 440 minutes. Toute modification de

configuration non validée sera perdue. Validez les modifications de configuration dès qu'elles sont effectuées.

(Ordinateur esa1.rs1234-01.iphmx.com)>
(Ordinateur esa1.rs1234-01.iphmx.com)> exit

La connexion à 127.0.0.1 est fermée.
[-] Fermeture de la connexion proxy...
[-] Terminé.

connect2ces.sh

Remarque : assurez-vous de choisir le proxy approprié pour votre région (c'est-à-dire, si vous êtes un client CES des États-Unis, afin d'atteindre le data center et les appareils F4, utilisez le f4-ssh.iphmx.com. Si vous êtes un client CES de l'UE et que vous possédez un appareil en Allemagne, utilisez f17-ssh.eu.iphmx.com.).

```
# !/bin/bash

#-- MODIFIEZ LES VALEURS CI-DESSOUS ----------------------
# Les valeurs suivantes doivent déjà être établies avec CES :
# cloud_user="nom d'utilisateur"
# cloud_host="esaX.CUSTOMER.iphmx.com" ou "smaX.CUSTOMER.iphmx.com"
## [ASSUREZ-VOUS QUE VOUS DISPOSEZ DU DATACENTER CES RÉGIONAL APPROPRIÉ !]
# private_key="CHEMIN_LOCAL_VERS_SSH_PRIVATE_RSA_KEY"
# proxy_server="SERVEUR_PROXY" [N'EN SÉLECTIONNEZ QU'UN !]
#
## Pour 'proxy_server', il s'agit de proxys SSH :
##
## AP (ap.iphmx.com)
## f15-ssh.ap.iphmx.com
## f16-ssh.ap.iphmx.com
##
## CA (ca.iphmx.com)
## f13-ssh.ca.iphmx.com
## f14-ssh.ca.iphmx.com
##
## EU (c3s2.iphmx.com)
## f10-ssh.c3s2.iphmx.com
## f11-ssh.c3s2.iphmx.com
##
## EU (eu.iphmx.com)(Allemagne DC)
## f17-ssh.eu.iphmx.com
## f18-ssh.eu.iphmx.com
```

```
##
## US (iphmx.com)
## f4-ssh.iphmx.com
## f5-ssh.iphmx.com

cloud_user="nom d'utilisateur"
cloud_host="esaX.CUSTOMER.iphmx.com"
private_key="CHEMIN_LOCAL_VERS_SSH_PRIVATE_RSA_KEY"
proxy_server="SERVEUR_PROXY"

#-- LAISSER CES VALEURS TELLES QUELLES ----------
# 'proxy_user' ne doit pas changer
# « remote_port » reste 22 (SSH)
# 'local_port' peut être défini sur une valeur différente, si nécessaire

proxy_user="utilisateur-dh"
remote_port=22
port_local=2222

#-- NE PAS MODIFIER SOUS CETTE LIGNE ----------

proxycmd="ssh -f -L $local_port:$cloud_host:$remote_port -i $private_key -N
$proxy_user@$proxy_server"

printf "[-] Connexion à votre serveur proxy ($proxy_server)...\n"
$proxycmd >/dev/null 2>&1
if nc -z 127.0.0.1 $local_port >/dev/null 2>&1 ; puis
printf "[-] Connexion proxy réussie. Maintenant connecté à $proxy_server.\n"
autre
printf "[-] Échec de la connexion proxy. Arrêt en cours...\n"
sortie
fi

# Rechercher le processus ssh proxy
proxypid=`ps -xo pid,commande | grep "$cloud_host" | grep "$proxy_server" | head -n1 | sed "s/^[
\t]*//" | cut -d " " -f1`
printf "[-] proxy exécuté sur le PID : $proxypid\n"

printf "[-] Connexion à votre appliance CES ($cloud_host)...\n\n"
ssh -p $local_port $cloud_user@127.0.0.1

printf "[-] Fermeture de la connexion proxy...\n"
kill $proxypid

printf "[-] Terminé.\n"

#-- Vous voulez éviter d'avoir à taper un mot de passe à chaque fois ?
#-- Voir : https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118305-
technote-esa-00.html
```

#-- Besoin d'un accès à plusieurs ESA ou SMA ? Copiez le même script et renommez-le en connect2ces_2.sh ou similaire.

Document d'origine : https://github.com/robsherw/connect2ces.

Utilisateurs Windows

Instructions pour l'utilisation de PuTTY et de SSH afin de rendre l'accès CLI via le proxy CES.

Conditions préalables

En tant que client CES, vous devez avoir fait appel à l'intégration/opérations CES ou au centre d'assistance technique Cisco pour que les clés SSH soient échangées et placées :

1. Générez des clés RSA privées/publiques.
2. Fournissez à Cisco votre clé publique RSA.
3. Attendez que Cisco enregistre vos clés et vous informe qu'elles ont été enregistrées sur votre compte client CES.
4. Configurez PuTTY comme détaillé dans ces instructions.

Comment créer des clés RSA privées/publiques ?

Cisco recommande d'utiliser PuTTYgen (https://www.puttygen.com/) pour Windows.

Pour plus d'informations : https://www.ssh.com/ssh/putty/windows/puttygen.

Remarque : Assurez-vous que vous protégez l'accès à vos clés privées RSA à tout moment.
N'envoyez pas votre clé privée à Cisco, seulement la clé publique (.pub).
Lors de l'envoi de votre clé publique à Cisco, identifiez l'adresse e-mail/le prénom/le nom pour lequel la clé est utilisée.

Comment ouvrir une demande d'assistance Cisco pour fournir ma clé publique ?

Accédez à ce lien.

Assurez-vous que vous avez correctement identifié le SR comme « Configuration SSH/CLI client Cisco CES », etc.

Comment puis-je configurer mon ESA ou SMA pour me connecter sans demander de mot de passe ?

Lisez ce guide.

Configuration PuTy

Afin de commencer, ouvrez PuTTY et utilisez l'un de ces hôtes proxy pour les noms d'hôtes :

Assurez-vous de choisir le proxy approprié pour votre région (c'est-à-dire, si vous êtes un client CES des États-Unis, afin d'atteindre le data center et les appareils F4, utilisez le f4-ssh.iphmx.com. Si vous êtes un client CES de l'UE et que vous possédez un appareil en Allemagne, utilisez f17-ssh.eu.iphmx.com.).

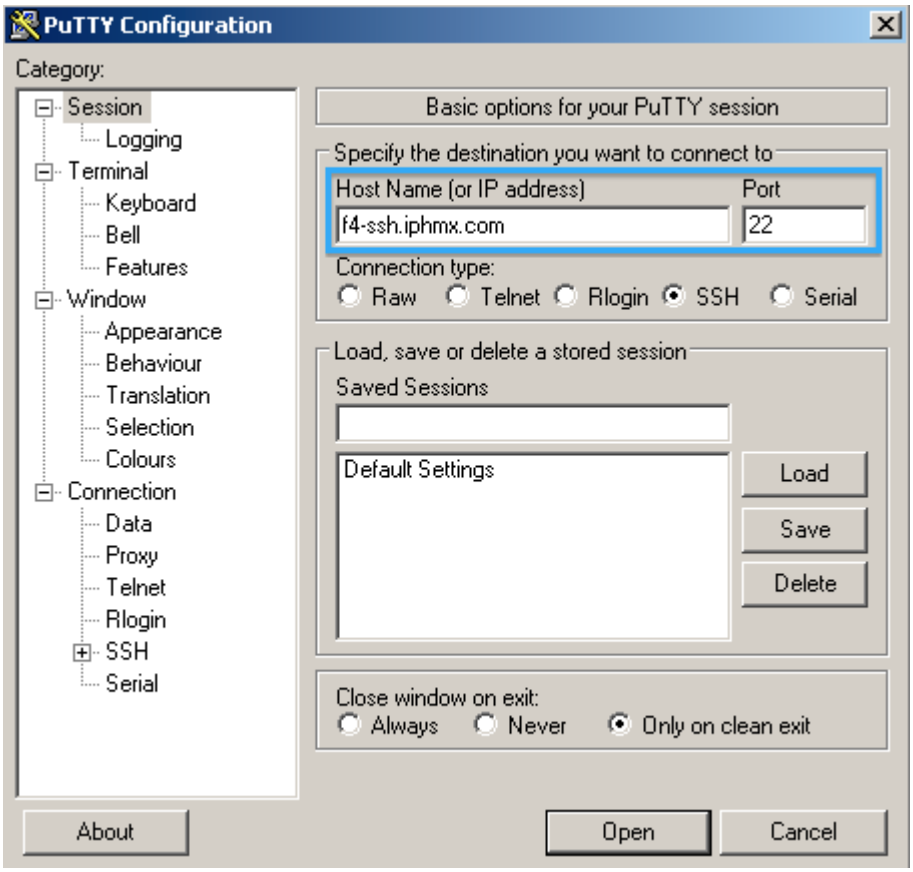
AP (ap.iphmx.com)
f15-ssh.ap.iphmx.com
f16-ssh.ap.iphmx.com

CA (ca.iphmx.com)
f13-ssh.ca.iphmx.com
f14-ssh.ca.iphmx.com

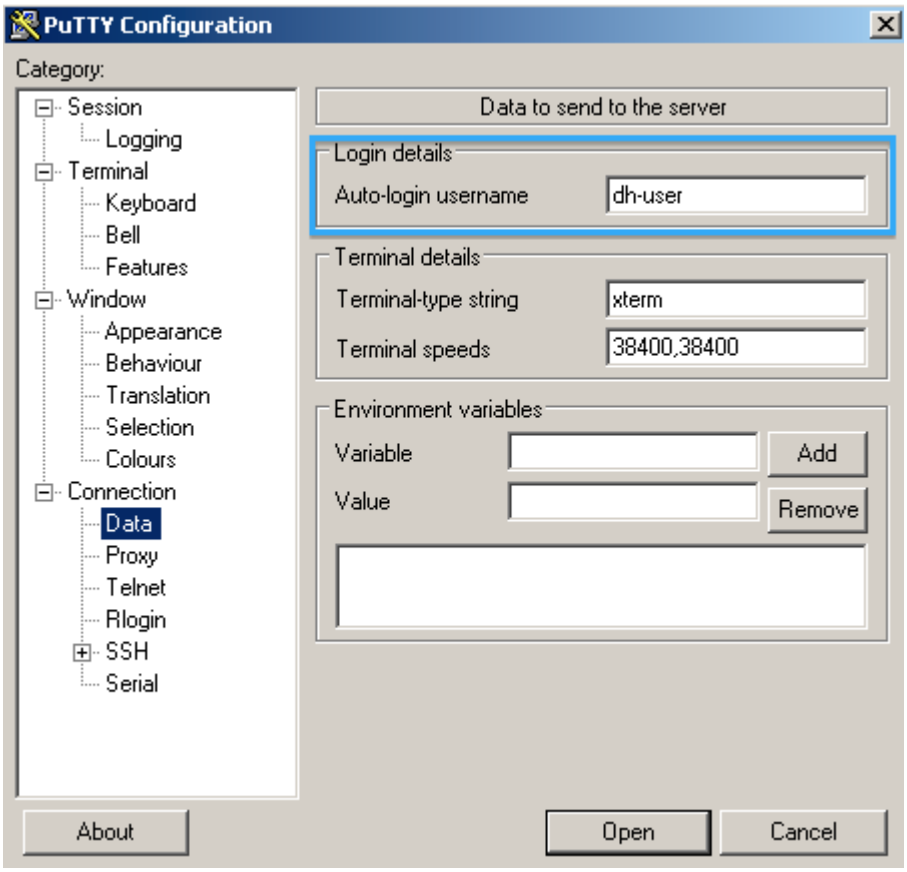
UE (c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

UE (eu.iphmx.com) (Allemagne DC)
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

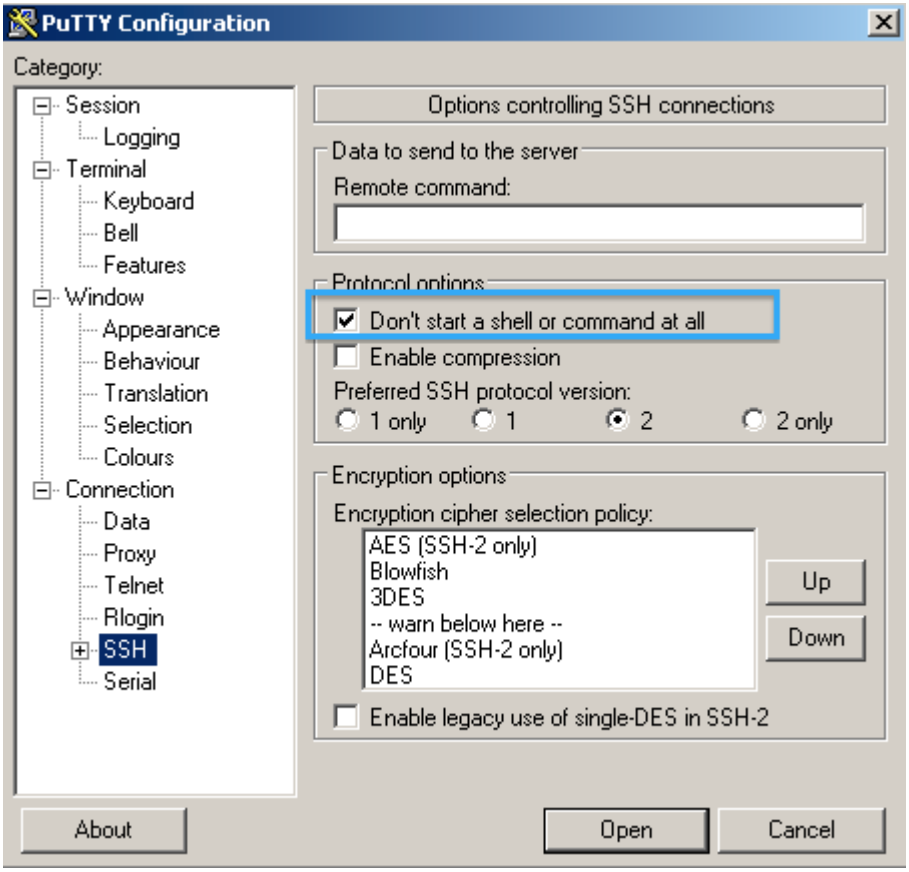
États-Unis (iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com



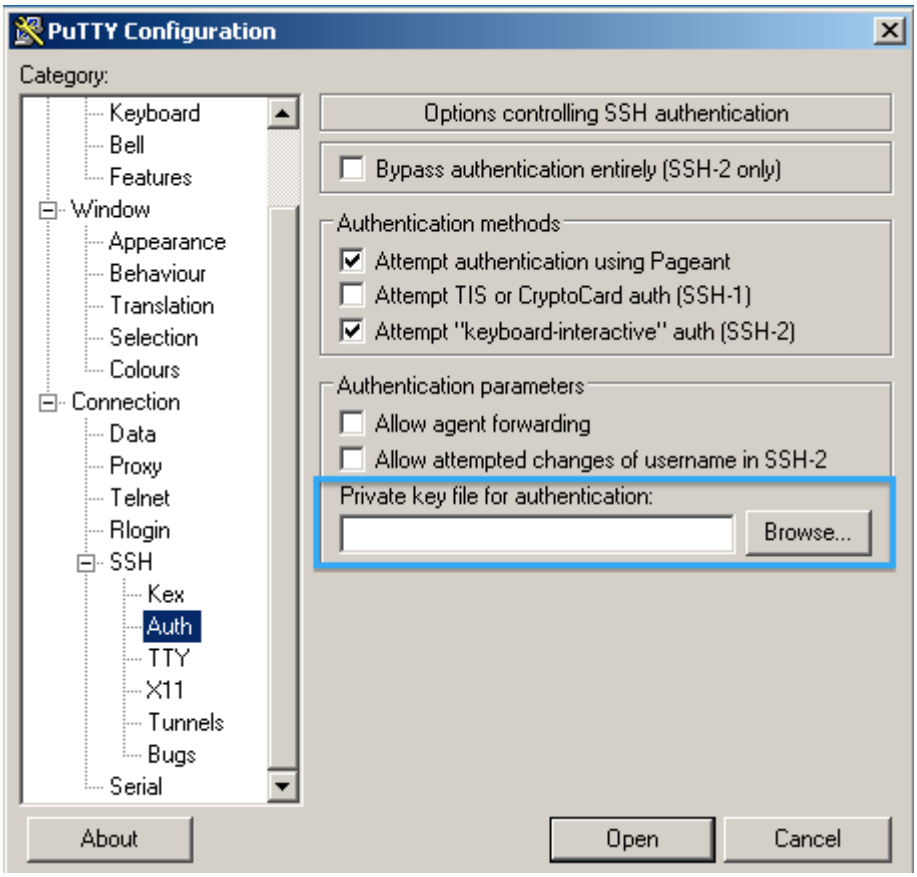
Cliquez surData et pour obtenir les détails de connexion, utilisez le nom d'utilisateur de connexion automatique et entrez dh-user.



Choisissez SSH et cochez Ne pas démarrer un shell ou une commande du tout.

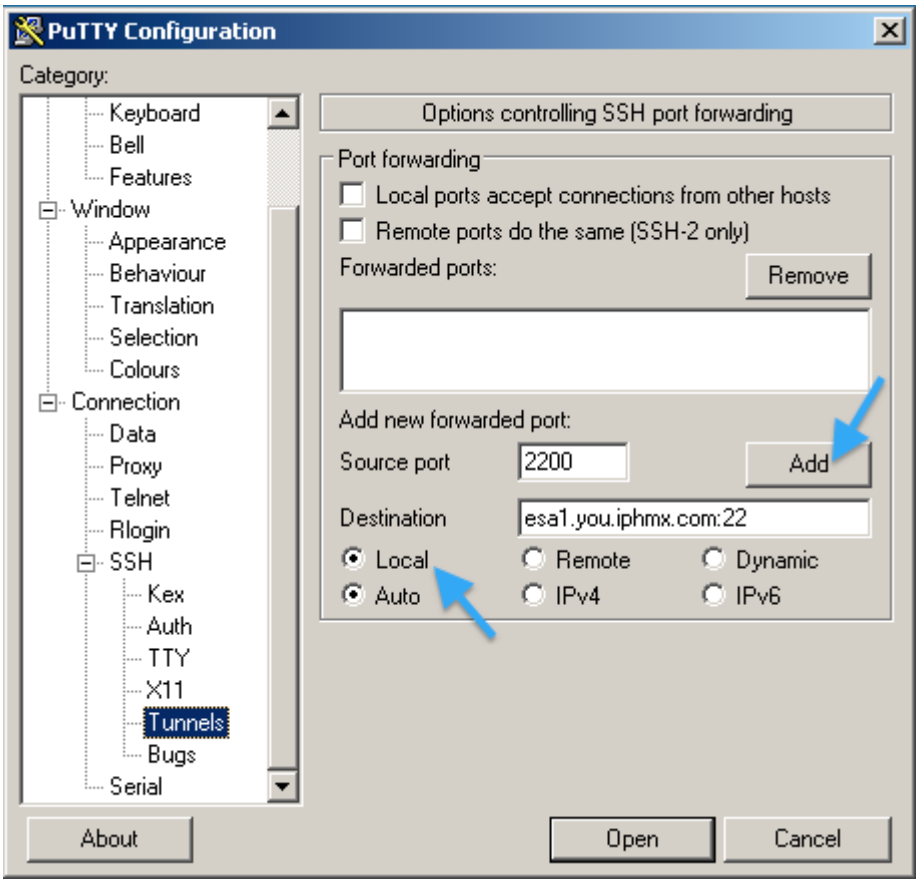


Cliquez sur Authand for Private key file for authentication, parcourez et choisissez votre clé privée.

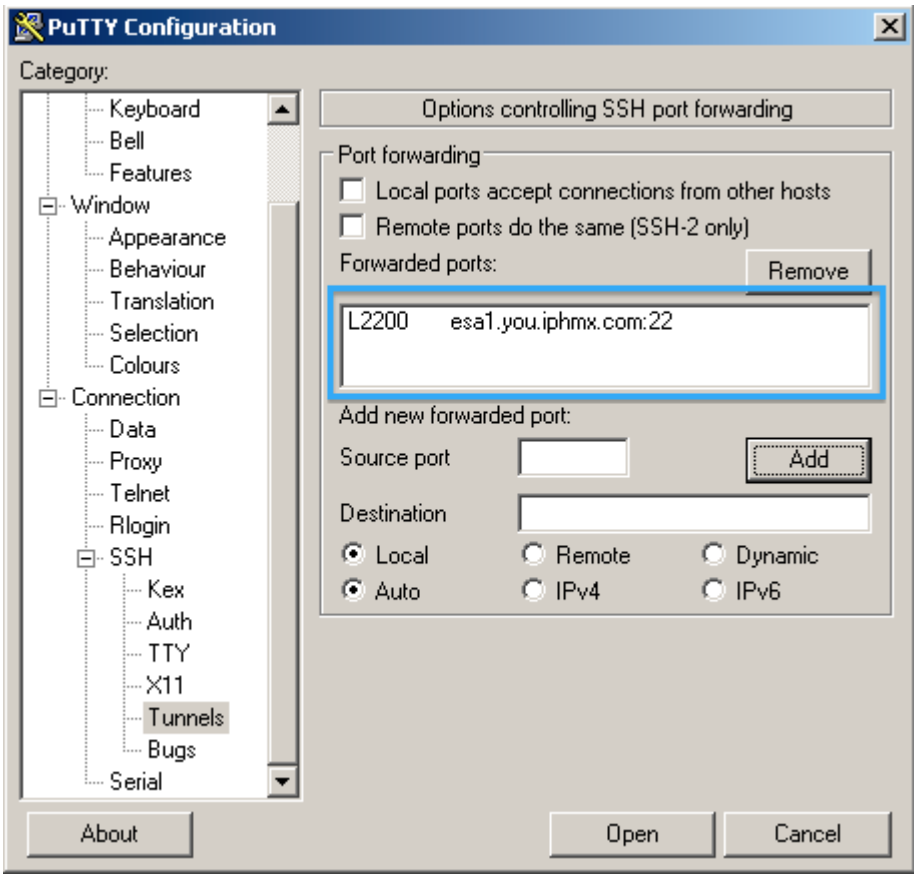


Cliquez sur Tunnels.
Entrez un port source ; il s'agit d'un port arbitraire de votre choix (l'exemple utilise 2200).

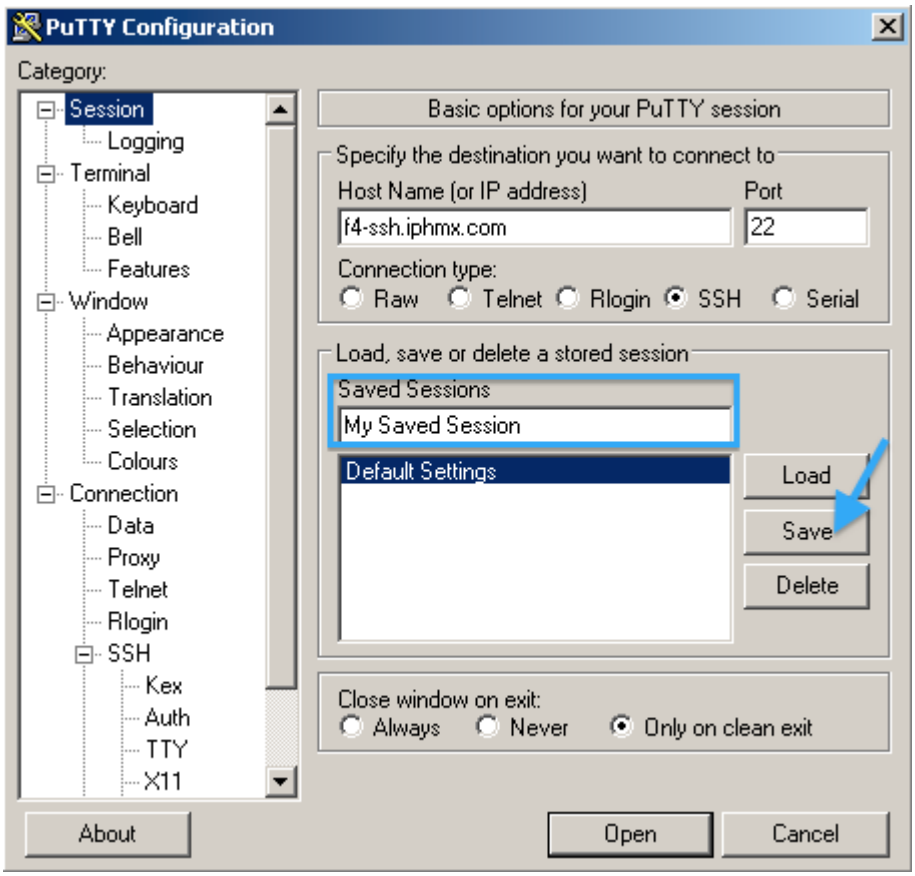
Entrez une destination ; il s'agit de votre ESA ou SMA + 22 (en spécifiant la connexion SSH).



Une fois que vous avez cliqué sur Add, il doit ressembler à ceci.

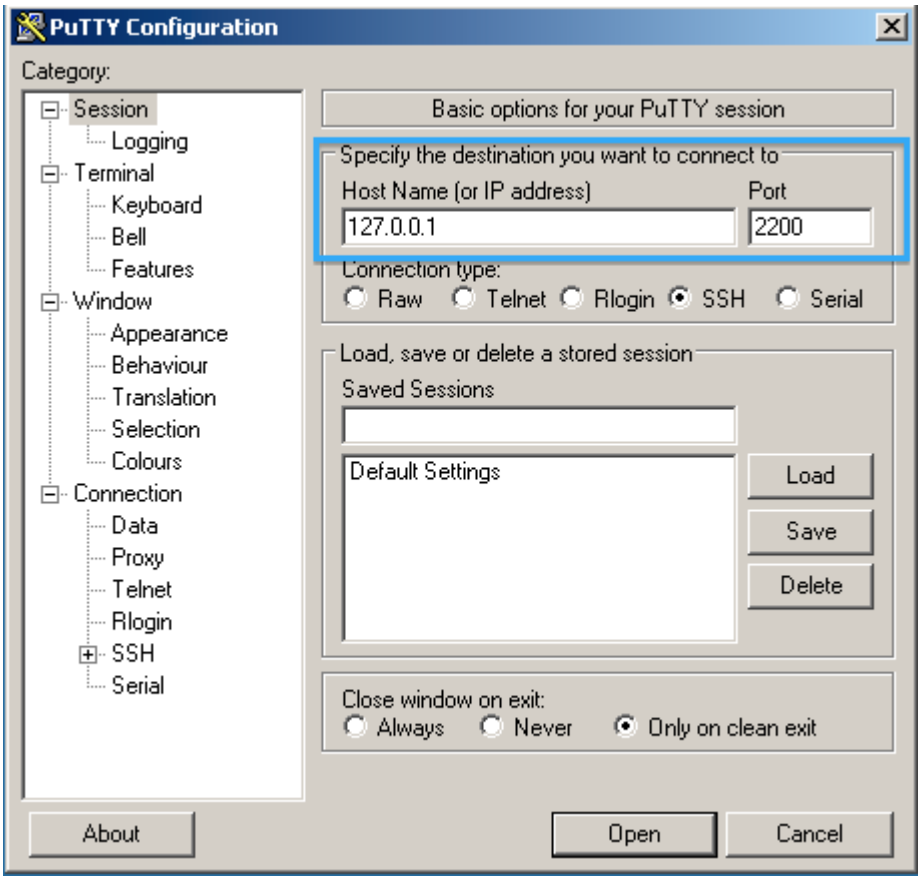


Afin d'enregistrer la session pour une utilisation future, cliquez sur Session.
Entrez un nom pour votre « session enregistrée », puis cliquez sur Enregistrer.



À ce moment-là, vous pouvez cliquer sur Open et lancer la session proxy.
Il n'y aura pas d'invite de connexion ou de commande. Vous devez maintenant ouvrir une deuxième session PuTTY sur votre ESA ou SMA.

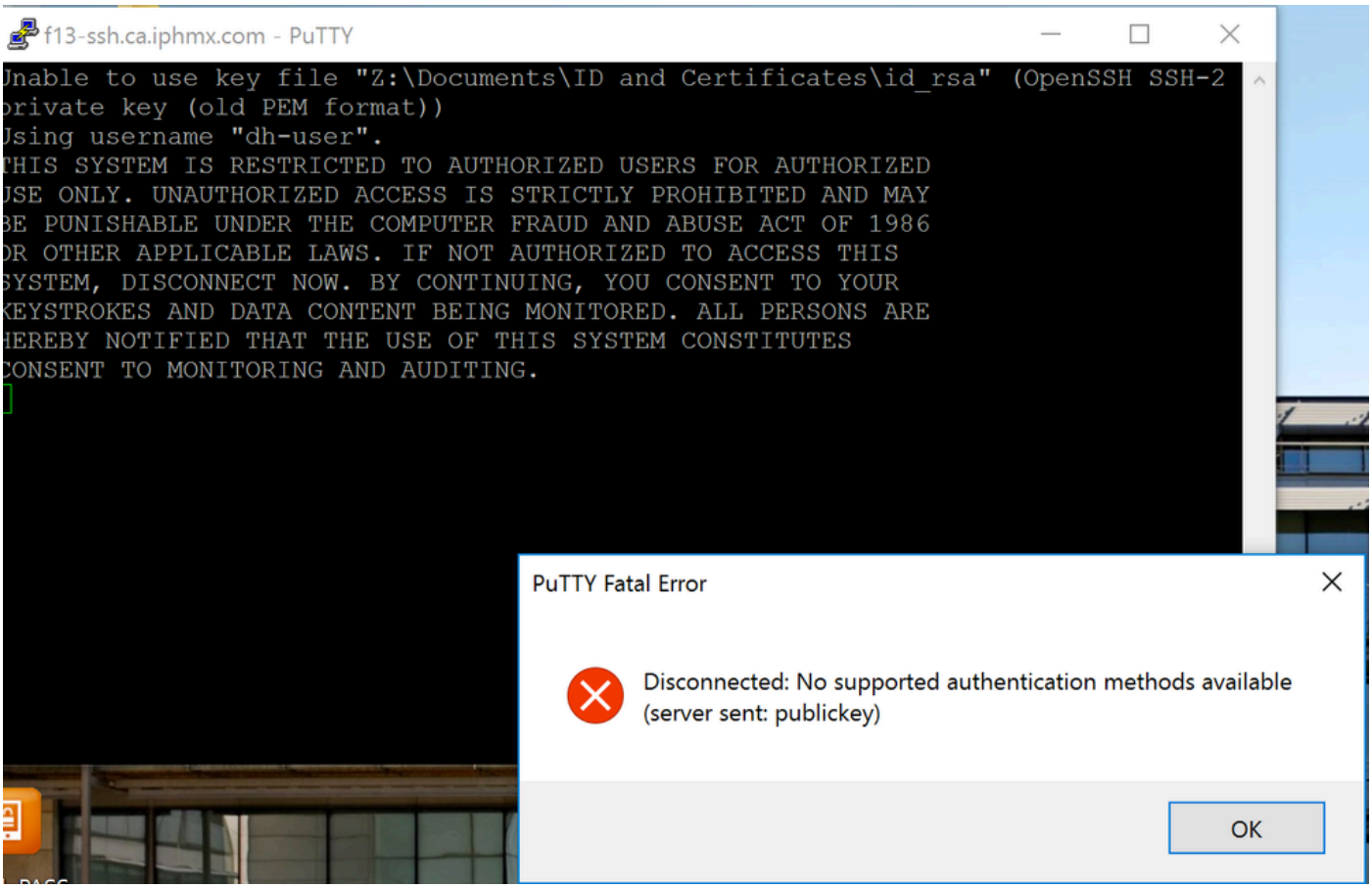
Utilisez le nom d'hôte 127.0.0.1 et le numéro de port source dans la configuration de tunnel présentée précédemment.
Dans cet exemple, 2200 est utilisé.
Cliquez sur Ouvrir pour vous connecter à votre appliance.



Lorsque vous y êtes invité, utilisez le nom d'utilisateur et le mot de passe de votre appliance, comme pour l'accès à l'interface utilisateur.

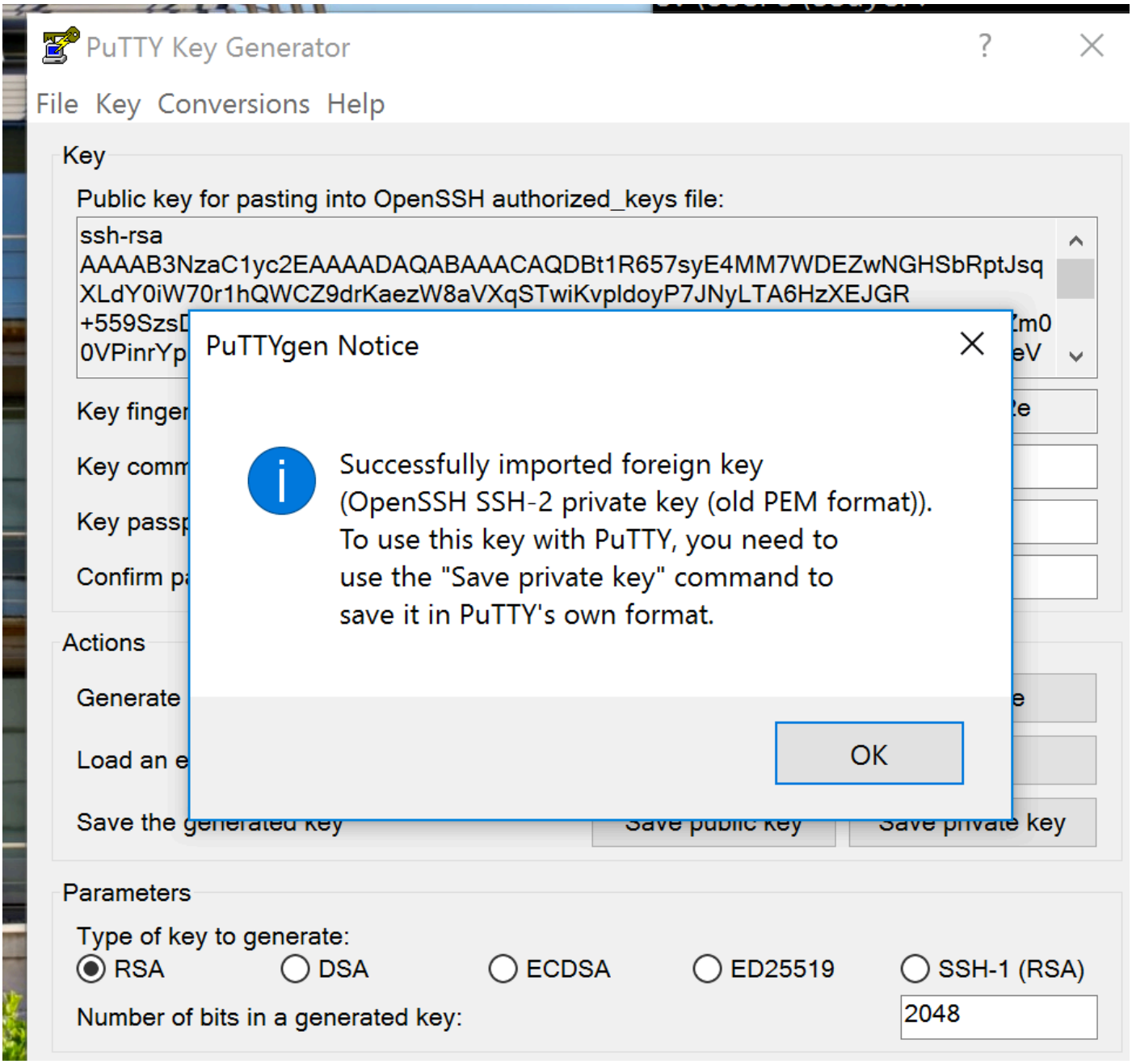
Dépannage

Si votre paire de clés SSH a été générée à l'aide d'OpenSSH (non-PuTTy), vous ne pouvez pas vous connecter et une erreur « old PEM format » s'affiche.



La clé privée peut être convertie à l'aide du générateur de clé PuTTY.

- Ouvrez PuTy Key Generator.
- Cliquez sur Chargement pour parcourir et charger votre clé privée existante.
- Vous devez cliquer sur la liste déroulante et sélectionner Tous les fichiers (.) afin de localiser la clé privée.
- Cliquez sur Ouvrir une fois que vous avez trouvé votre clé privée.
- Puttygen fournira un avis comme dans cette image.



- Cliquez sur Enregistrer la clé privée.
- À partir de votre session PuTTY, utilisez cette clé privée convertie et enregistrez la session.
- Essayez de vous reconnecter avec la clé privée convertie.

Vérifiez que vous pouvez accéder à vos appareils via la ligne de commande.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.