Comprendre Secure Shell Packet Exchange

Table des matières

Introduction

Ce document décrit l'échange au niveau paquet pendant la négociation Secure Shell (SSH).

Conditions préalables

Exigences

Cisco recommande que vous ayez une connaissance des concepts de sécurité de base :

- Authentification
- Confidentialité
- Intégrité
- Méthodes d'échange de clés

Composants utilisés

Ce document n'est pas limité à une version matérielle spécifique.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration.

Protocole SSH

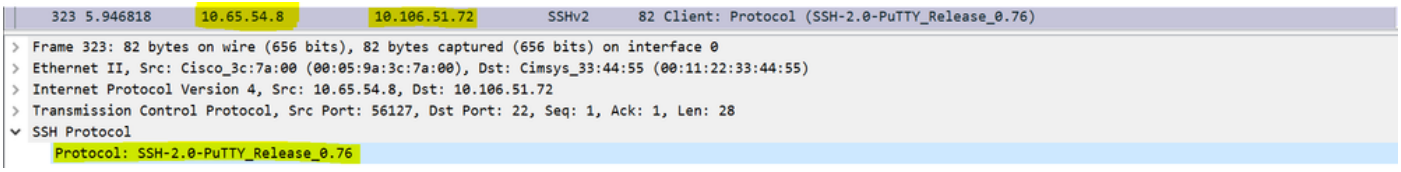
Le protocole SSH est une méthode de connexion à distance sécurisée d'un ordinateur à un autre. Les applications SSH sont basées sur une architecture client-serveur, connectant une instance de client SSH à un serveur SSH.

Échange SSH

1. La première étape de SSH est appelée Identification String Exchange.

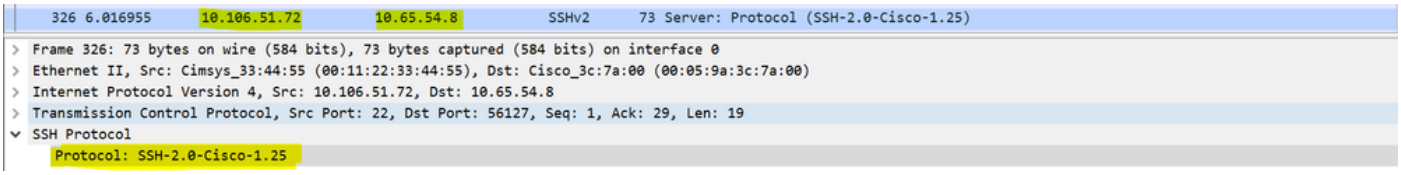
a. Le client construit un paquet et l'envoie au serveur contenant :

- Version du protocole SSH
- Version du logiciel



La version du protocole client est SSH2.0 et la version du logiciel est Putty_0.76.

b. Le serveur répond avec son propre échange de chaîne d'identification, y compris sa version de protocole SSH et sa version logicielle.

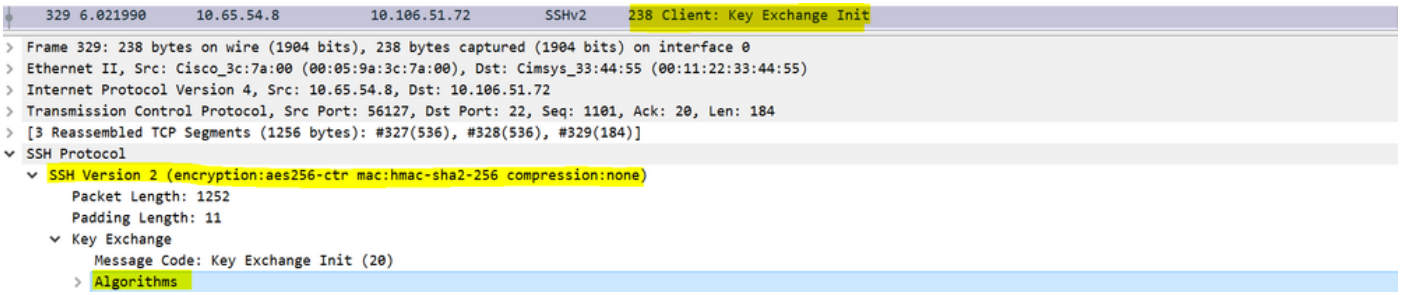


La version du protocole du serveur est SSH2.0 et la version du logiciel est Cisco1.25

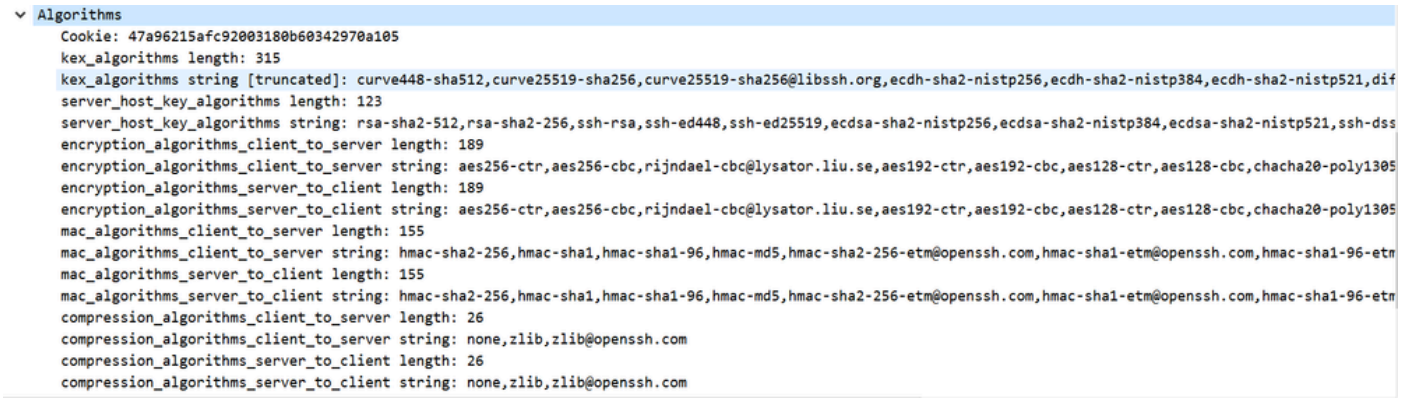
2. Étape suivante **Algorithm Negotiation**. Dans cette étape, le client et le serveur négocient les algorithmes suivants :

- Échange De Clés
- Chiffrement
- HMAC (Hash-based Message Authentication Code)
- Compression

1. Le client envoie un message d'initialisation d'échange de clés au serveur, en spécifiant les algorithmes qu'il prend en charge. Les algorithmes sont répertoriés par ordre de préférence.



Init d'échange de clés

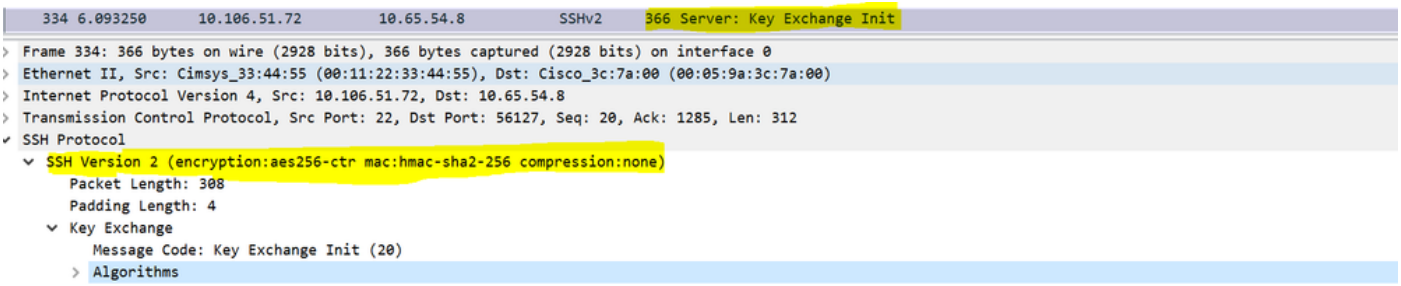


Algorithmes pris en charge par le client

b. Le serveur répond avec son propre message d'initialisation d'échange de clés, en répertoriant les algorithmes qu'il prend en charge.

c. Puisque ces messages sont échangés simultanément, les deux parties comparent leurs listes d'algorithmes. S'il existe une correspondance dans les algorithmes pris en charge par les deux côtés, ils passent à l'étape suivante. S'il n'y a pas de correspondance exacte, le serveur sélectionne le premier algorithme de la liste du client qu'il prend également en charge.

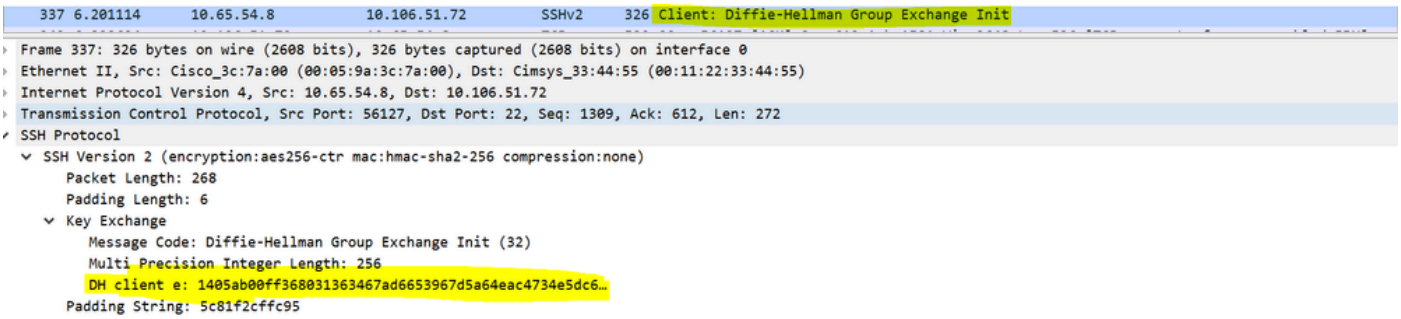
d. Si le client et le serveur ne parviennent pas à s'entendre sur un algorithme commun, l'échange de clés échoue.



Init Exchange de clé serveur

3. Ensuite, les deux parties entrent en phase de génération du secret partagé à l'aide de l'échange de clés DH et d'authentification du serveur **Key Exchange**:

a. Le client génère une paire de clésPublic and Privateet envoie la clé publique DH dans le paquet DH Group Exchange Init. Cette paire de clés est utilisée pour le calcul des clés secrètes.



Client DH Public Key & Diffie-Hellman Group Exchange Init

b. Le serveur génère sa propre Public and Private paire de clés. Il utilise la clé publique du client et sa propre paire de clés pour calculer le secret partagé.

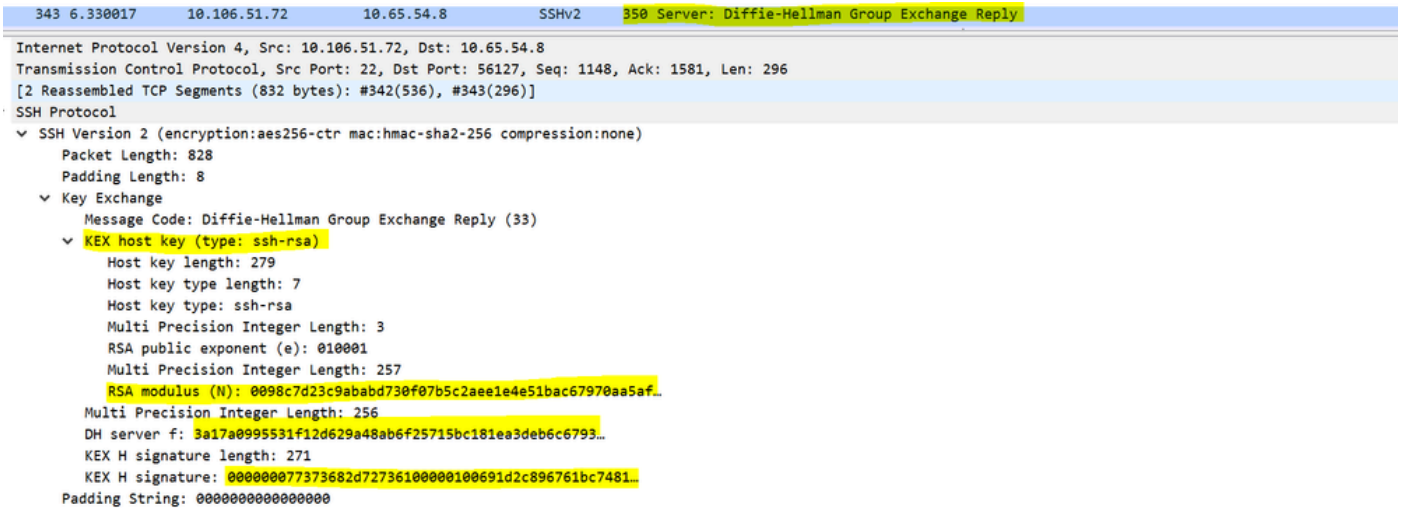
c. Le serveur calcule également un hachage Exchange avec les entrées suivantes :

- Chaîne D'Identification Des Clients
- Chaîne D'Identification Du Serveur
- Charge utile du client KEXINIT
- Charge utile du serveur KEXINIT
- Serveurs Clé publique à partir des clés d'hôte (Paire de clés RSA)
- Clé publique DH des clients
- Serveurs DH Clé publique
- Clé secrète partagée

d. Après avoir calculé le hachage, le serveur le signe avec sa clé privée RSA.

e. Le serveur construit un message DH_Exchange_Reply qui inclut :

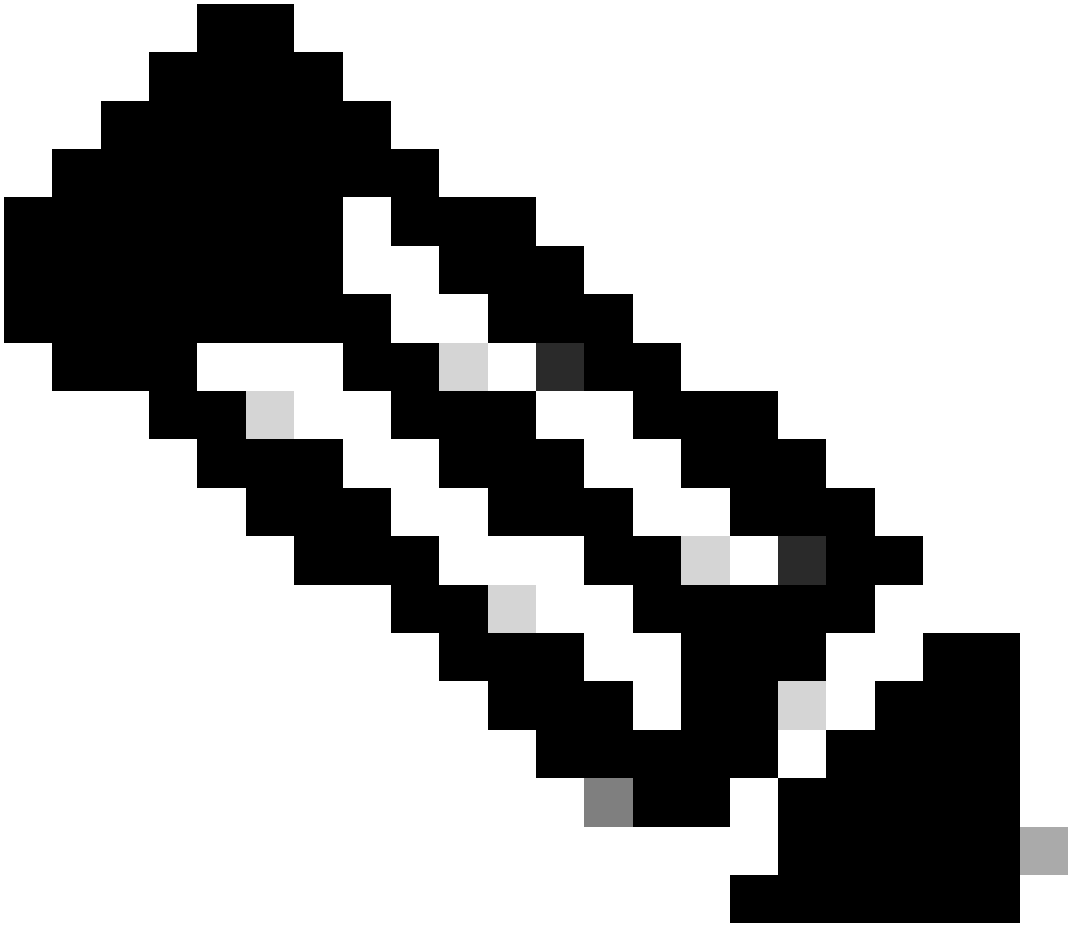
- RSA-Clé publique du serveur (pour aider le client à authentifier le serveur)
- DH-Clé publique du serveur (pour le calcul du secret partagé)
- HASH (pour authentifier le serveur et prouver que le serveur a généré le secret partagé, car la clé secrète fait partie du calcul de hachage)



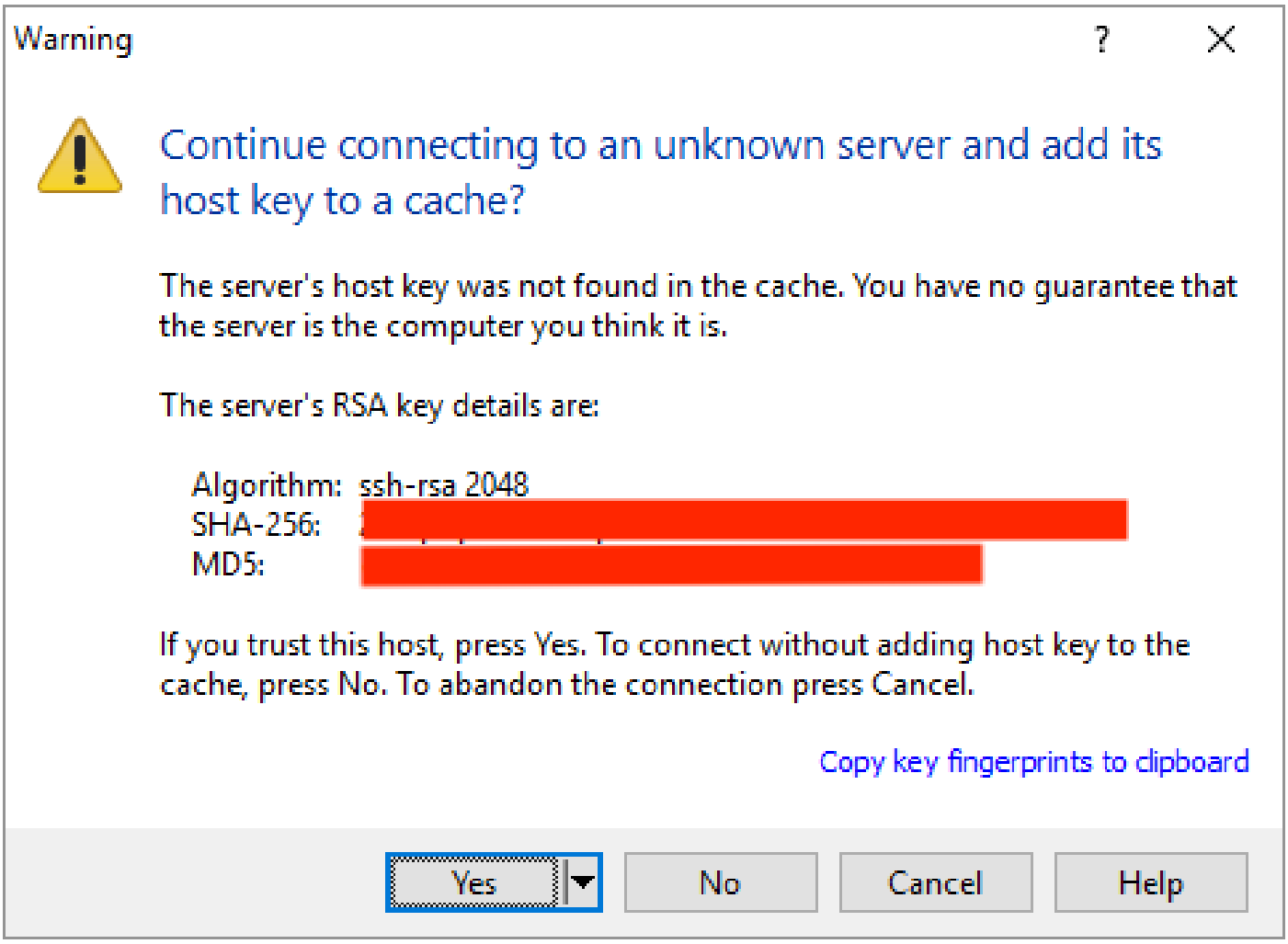
Server DH Public Key & Diffie-Hellman Group Exchange Réponse

f. Après réception de DH_Exchange_Reply, le client calcule le hachage de la même manière et le compare au hachage reçu, en le décryptant à l'aide de la clé publique RSA du serveur.

g. Avant de déchiffrer le HASH reçu, le client doit vérifier la clé publique du serveur. Cette vérification s'effectue au moyen d'un certificat numérique signé par une autorité de certification (AC). Si le certificat n'existe pas, c'est au client de décider d'accepter ou non la clé publique du serveur.



Remarque : lorsque vous accédez pour la première fois à SSH sur un périphérique qui n'utilise pas de certificat numérique, vous pouvez rencontrer une fenêtre contextuelle vous demandant d'accepter manuellement la clé publique du serveur. Pour éviter de voir cette fenêtre contextuelle chaque fois que vous vous connectez, vous pouvez choisir d'ajouter la clé d'hôte du serveur à votre cache.

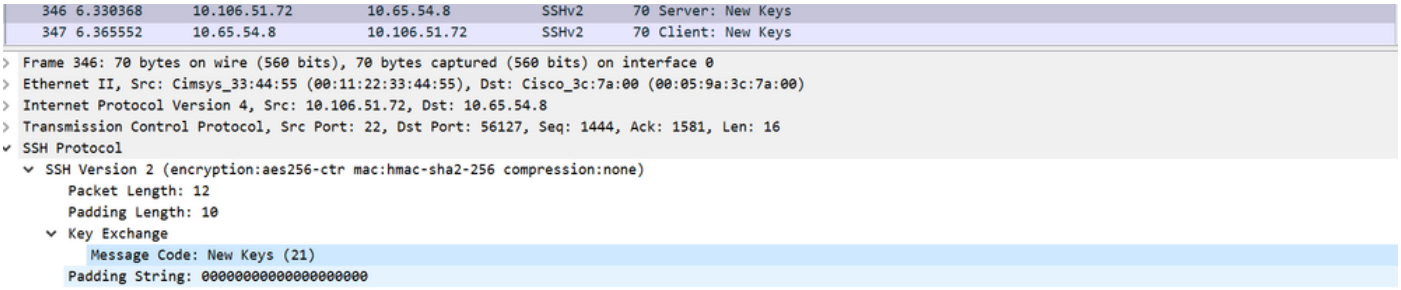


Clé RSA du serveur

4. Puisque le secret partagé est maintenant généré, les deux terminaux l'utilisent pour dériver ces clés :

- Clés de chiffrement
- IV Keys (Clés IV) : nombres aléatoires utilisés comme entrée dans des algorithmes symétriques pour améliorer la sécurité.
- Clés d'intégrité

La fin de l'échange de clés est signalée par l'échange du NEW KEYS message, qui informe chaque partie que tous les messages futurs seront chiffrés et protégés à l'aide de ces nouvelles clés .



Nouvelles clés client et serveur

5. La dernière étape est la demande de service. Le client envoie un paquet de demande de

service SSH au serveur pour lancer l'authentification de l'utilisateur. Le serveur répond avec un message d'acceptation de service SSH, invitant le client à se connecter. Cet échange se produit sur le canal sécurisé établi.

Informations connexes

- https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html
- https://datatracker.ietf.org/doc/html/rfc4253
- Assistance technique de Cisco et téléchargements

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.