Activation de Secure Shell (SSH) sur un point d'accès (AP)

Contenu

Introduction

Ce document décrit comment configurer un point d'accès (AP) afin d'activer l'accès Secure shell (SSH).

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- La connaissance de la façon configurer Cisco Aironet aps
- Connaissance de base de SSH et de concepts relatifs de Sécurité

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gamme 1200 AP d'Aironet qui exécute la version de logiciel 12.3(8)JEB de Cisco IOS®
- PC ou ordinateur portable avec l'utilitaire de client SSH

Note: Ce document emploie l'utilitaire de client SSH afin de vérifier la configuration. Vous pouvez

employer n'importe quel tiers utilitaire client afin d'ouvrir une session à AP avec l'utilisation du SSH.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Accéder à l'interface de ligne de commande (CLI) sur l'Aironet AP

Vous pouvez employer l'un de ces méthodes afin d'accéder à l'interface de ligne de commande (CLI) sur l'Aironet AP :

- Le port de console
- Telnet
- SSH

Si AP a un port de console et vous avez accès physique à AP, vous pouvez employer le port de console afin d'ouvrir une session à AP et changer la configuration s'il y a lieu. Pour les informations sur la façon dont employer le port de console afin d'ouvrir une session à AP, référez-vous à *connecter aux Points d'accès de gamme 1200 localement la* section du document configurant le Point d'accès pour la première fois.

Si vous pouvez seulement accéder à AP par les Ethernets, employez le protocole Telnet ou le protocole de SSH afin d'ouvrir une session à AP.

Le protocole Telnet utilise le port 23 pour la transmission. Le telnet transmet et reçoit des données en texte clair. Puisque la communication de données se produit en texte clair, un pirate informatique peut facilement compromettre les mots de passe et accéder à AP. RFC 854 définit le telnet et étend le telnet avec des options par beaucoup d'autres RFC.

Le SSH est une application et un protocole qui fournit un remplacement sécurisé aux r-outils de Berkley. Le SSH est un protocole qui fournit un sécurisé, connexion distante à une couche 2 ou un périphérique de la couche 3. Il y a deux versions de SSH : Version SSH 1 et version SSH 2. Cette version logicielle prend en charge les deux versions SSH. Si vous ne spécifiez pas le numéro de version, AP se transfère sur la version 2.

Le SSH fournit plus de Sécurité pour des connexions distantes que le telnet en fournissant le cryptage fort quand un périphérique est authentifié. Ce cryptage est un avantage par rapport à une session de telnet, dans laquelle la transmission se produit en texte clair. Pour plus d'informations sur le SSH, référez-vous à la Foire aux questions de Protocole Secure Shell (SSH). La caractéristique de SSH a un serveur de SSH et un client intégré de SSH. Le client prend en charge ces méthodes d'authentification de l'utilisateur :

- RAYON (le pour en savoir plus, se rapportent au Point d'accès de contrôle Access avec la section de RAYON)
- Authentification locale et autorisation (le pour en savoir plus, se rapportent à configurer le

Point d'accès pour la section d'authentification locale et d'autorisation)

Pour plus d'informations sur le SSH, référez-vous à la partie, de *« autres fonctionnalités de sécurité »* dans le *guide de configuration de Cisco IOS Security pour la version 12.3.*

Note: La caractéristique de SSH dans cette version logicielle ne prend en charge pas la sécurité IP (IPSec).

Vous pouvez configurer des aps pour le SSH avec l'utilisation du CLI ou du GUI. Ce document explique les deux méthodes de configuration.

Configurez

Configuration CLI

Dans cette section, vous êtes présenté avec les informations pour configurer les caractéristiques décrites dans ce document avec l'utilisation du CLI.

Instructions pas à pas

Afin d'activer l'accès basé sur ssh sur AP, vous d'abord devez configurer AP en tant que serveur de SSH. Suivez ces étapes afin de configurer un serveur de SSH sur AP de CLI :

1. Configurez un nom d'hôte et un nom de domaine pour AP.
   ```
   AP#configure terminal
   !--- Enter global configuration mode on the AP. AP<config>#hostname Test
   !--- This example uses "Test" as the AP host name. Test<config>#ip domain name abc.com
   !--- This command configures the AP with the domain name "abc.com".
   ```
2. Générez une clé de Rivest, de Shamir, et d'Adelman (RSA) pour votre AP.La génération d'une clé RSA active le SSH sur AP. Émettez cette commande en mode de configuration globale :
   ```
   Test<config>#crypto key generate rsa rsa_key_size
   !--- This generates an RSA key and enables the SSH server.
   ```
   Note: La taille minimum recommandée de clé RSA est 1024.
3. Configurez l'authentification de l'utilisateur sur AP.Sur AP, vous pouvez configurer l'authentification de l'utilisateur pour utiliser la liste locale ou une authentification externe, une autorisation, et un serveur de comptabilité (AAA). Cet exemple emploie une liste localement générée afin d'authentifier les utilisateurs :
   ```
   Test<config>#aaa new-model
   !--- Enable AAA authentication. Test<config>#aaa authentication login default local none
   !--- Use the local database in order to authenticate users. Test<config>#username Test
   password Test123
   !--- Configure a user with the name "Test". Test<config>#username ABC password xyz123
   !--- Configure a second user with the name "ABC".
   ```
   Cette configuration configure AP pour exécuter l'authentification utilisateur avec l'utilisation d'une base de données locale qui est configurée sur AP. L'exemple configure deux utilisateurs dans la base de données locale, « test » et « ABC ».
4. Configurez les paramètres de SSH.
   ```
   Test<config>#ip ssh {[timeout seconds] | [authentication-retries integer]}
   !--- Configure the SSH control variables on the AP.
   ```
   Note: Vous pouvez spécifier le délai d'attente en quelques secondes, mais ne dépassez pas 120 secondes. Le par défaut est 120. Cette configuration s'applique à la phase de

négociation de SSH. Vous pouvez également spécifier le nombre de relances d'authentification, mais ne dépassez pas cinq relances d'authentification. Le par défaut est trois.

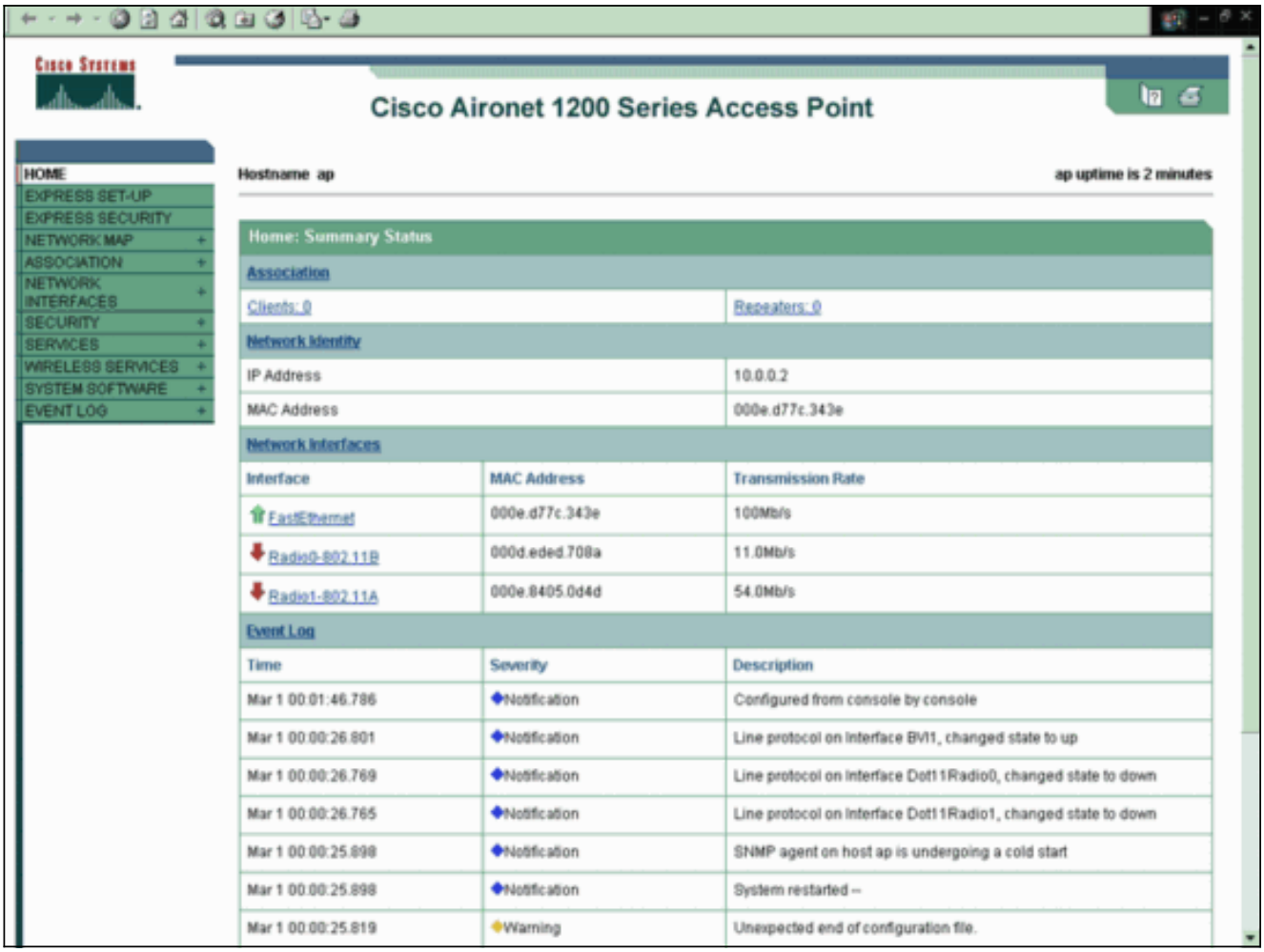
Configuration de la GUI

Vous pouvez également utiliser le GUI afin d'activer l'accès basé sur ssh sur AP.

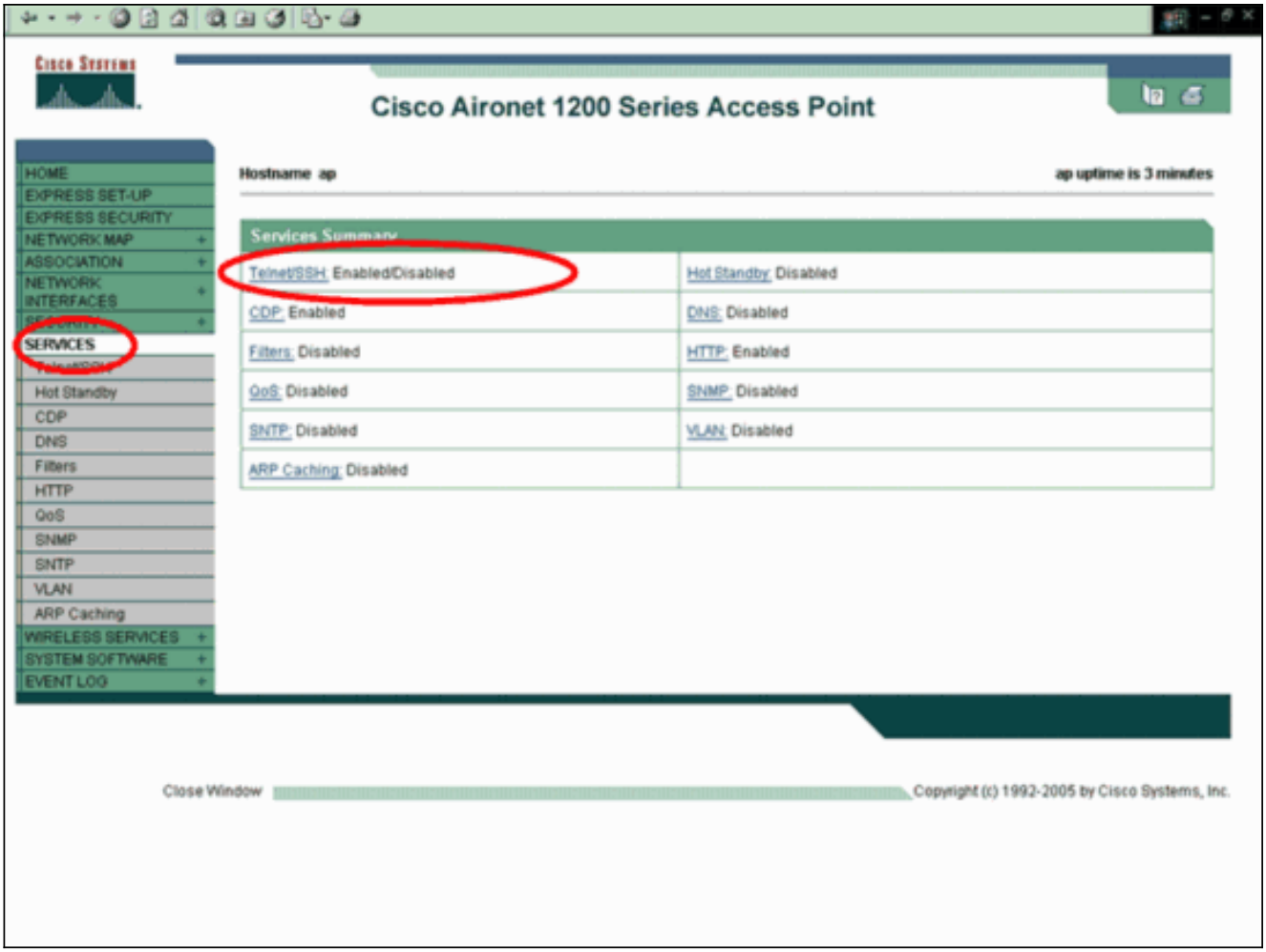
Instructions pas à pas

Procédez comme suit :

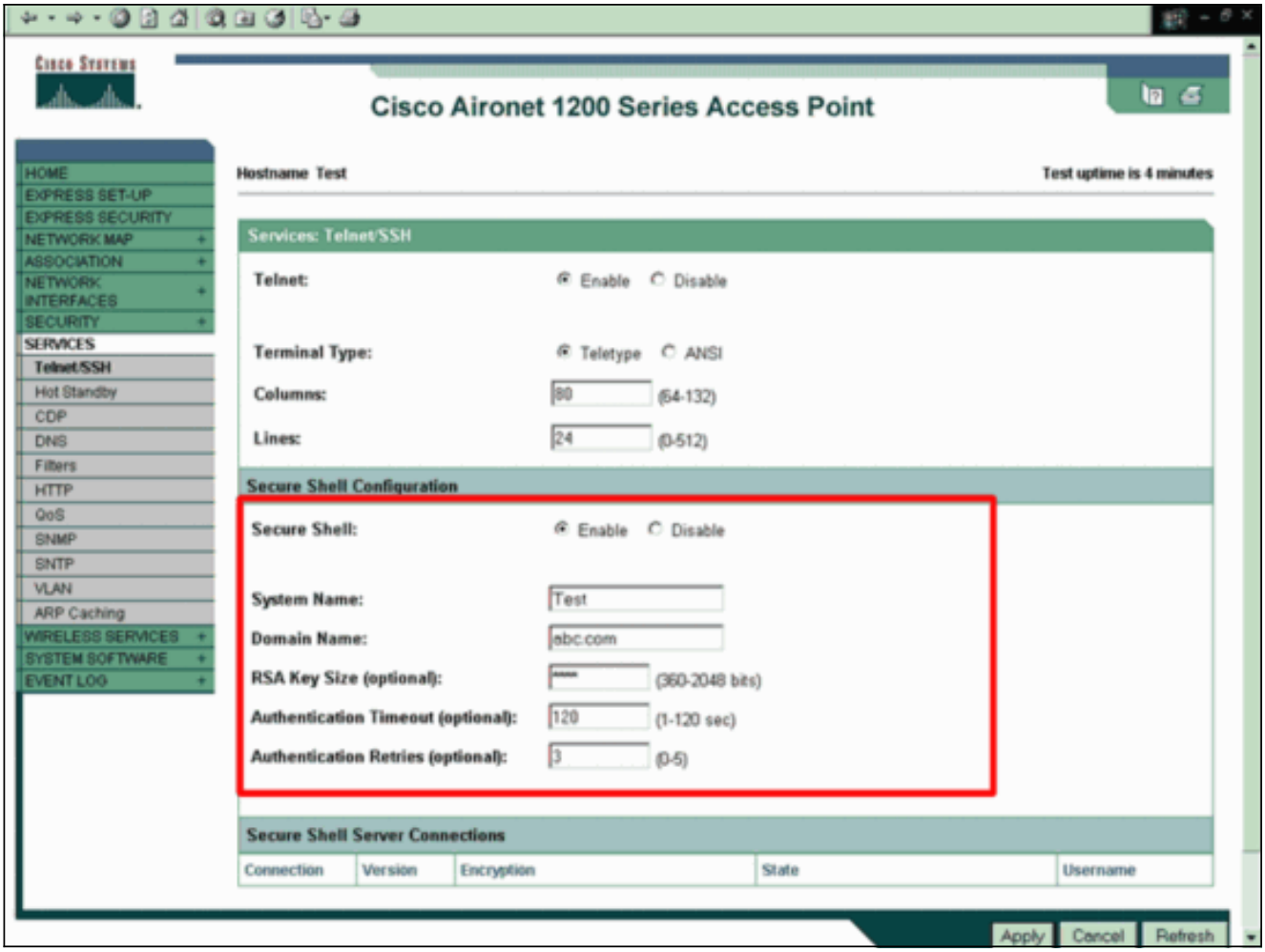
1. Procédure de connexion à AP par le navigateur.Les affichages de fenêtre Summary Status.



2. Cliquez sur les **services** dans le menu du côté gauche.Les affichages récapitulatifs de fenêtre de
services.



3. Cliquez sur **Telnet/SSH** afin d'activer et configurer les paramètres Telnet/SSH.Les services : Affichages de fenêtre Telnet/SSH. Faites descendre l'écran à la région sécurisée de configuration de shell. Cliquez sur l'**enable** près du shell sécurisé, et entrez dans le comme indiqué dans cet exemple de paramètres de SSH :Cet exemple utilise ces paramètres :Nom de système : TestNom de domaine : abc.comTaille de clé RSA : 1024Délai d'attente d'authentification : 120Relances d'authentification :
   3



4. Cliquez sur **Apply** afin de sauvegarder les modifications.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **show ip ssh** — Vous vérifie si le SSH est activé sur AP et permet de vérifier la version du SSH qui exécute sur AP. Cette sortie fournit un exemple

```
Test#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

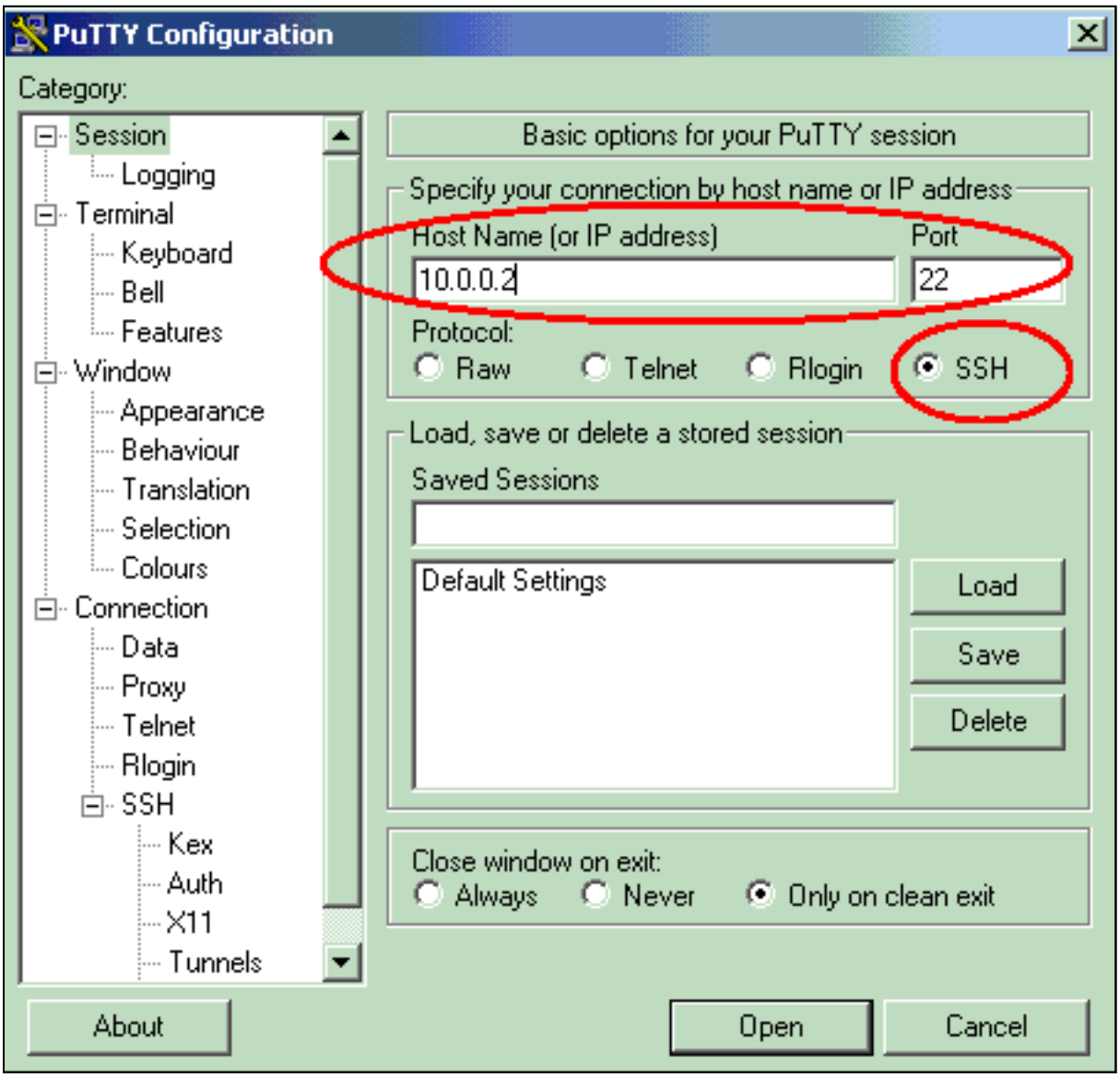
:

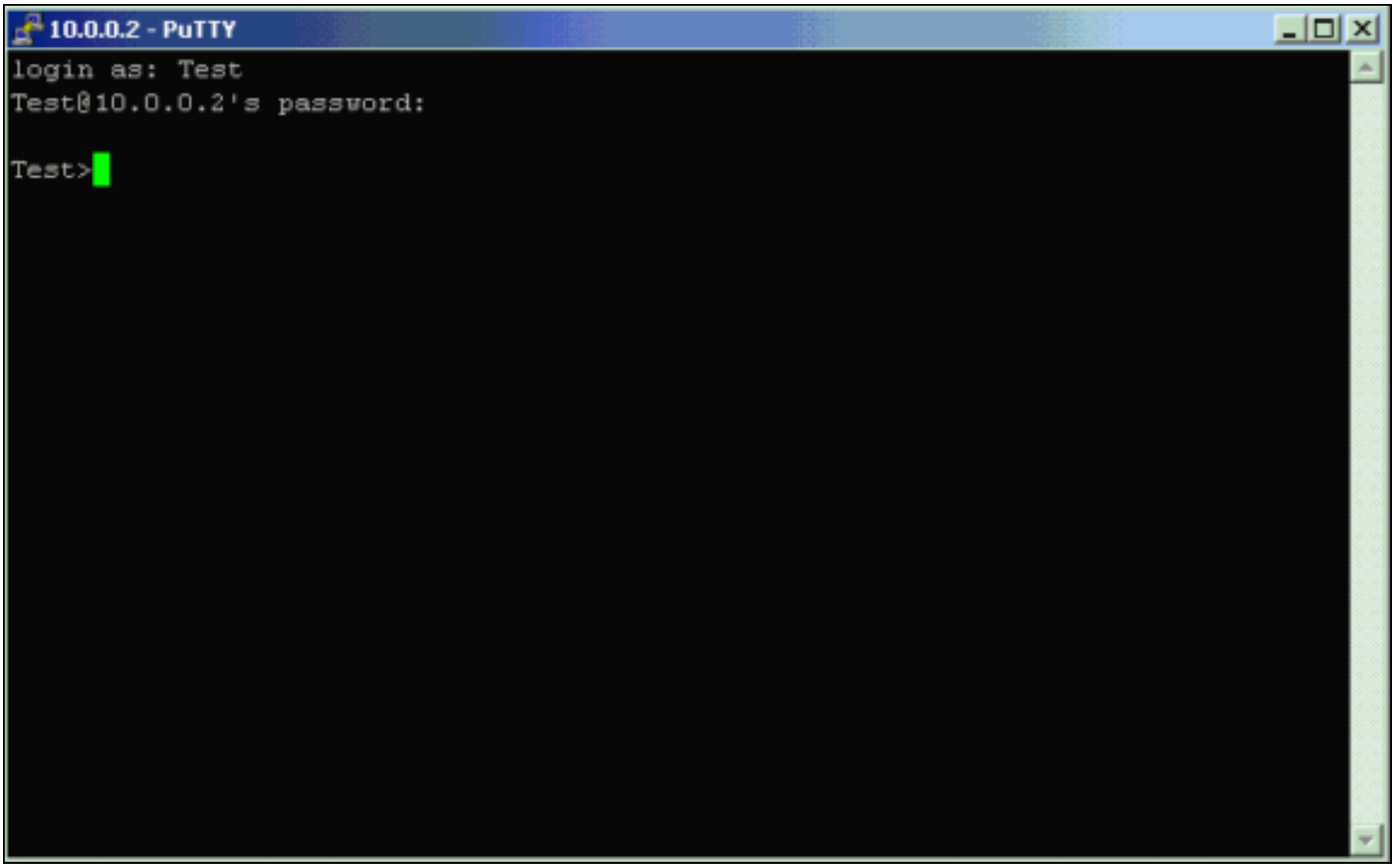
- **show ssh** — Te permet de visualiser le statut de vos connexions au serveur de SSH. Cette sortie fournit un exemple

```
Test#show ssh
Connection Version Mode Encryption  Hmac          State          Username
0          2.0     IN   aes256-cbc  hmac-sha1    Session started    ABC
0          2.0     OUT  aes256-cbc  hmac-sha1    Session started    ABC
```

:

Maintenant, initiez une connexion par un PC qui exécute le tiers logiciel de SSH et puis essayez d'ouvrir une session à AP. Cette vérification utilise l'adresse IP AP, 10.0.0.2. Puisque vous avez configuré le test de nom d'utilisateur, employez ce nom afin d'accéder à AP par le SSH :





Dépannez

Utilisez cette section pour dépanner votre configuration.

Si vos commandes de configuration de SSH sont rejetées en tant que commandes illégales, vous n'avez pas avec succès généré une paire de clés RSA pour votre AP. Référez-vous à la section de *conseils de dépannage du* document configurant le shell sécurisé pour une liste de possibles raison pour ce problème.

SSH de débronchement

Afin de désactiver le SSH sur AP, vous devez supprimer la paire RSA qui est générée sur AP. Afin de supprimer les paires RSA, émettez la commande de **crypto key zeroize rsa** en mode de configuration globale. Quand vous supprimez la paire de clés RSA, vous désactivez automatiquement le serveur de SSH. Cette sortie fournit un exemple :

```
Test(config)#crypto key zeroize rsa
% All RSA keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
```

Informations connexes

- Configurer le shell sécurisé

- Configuration d´un point d'accès pour la première fois
- Page de support de Protocole Secure Shell (SSH)
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems