Aktivieren von Secure Shell (SSH) auf einem Access Point (AP)

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie einen Access Point (AP) konfigurieren, um SSH-basierten Zugriff (Secure Shell) zu aktivieren.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie diese Konfiguration ausprobieren:

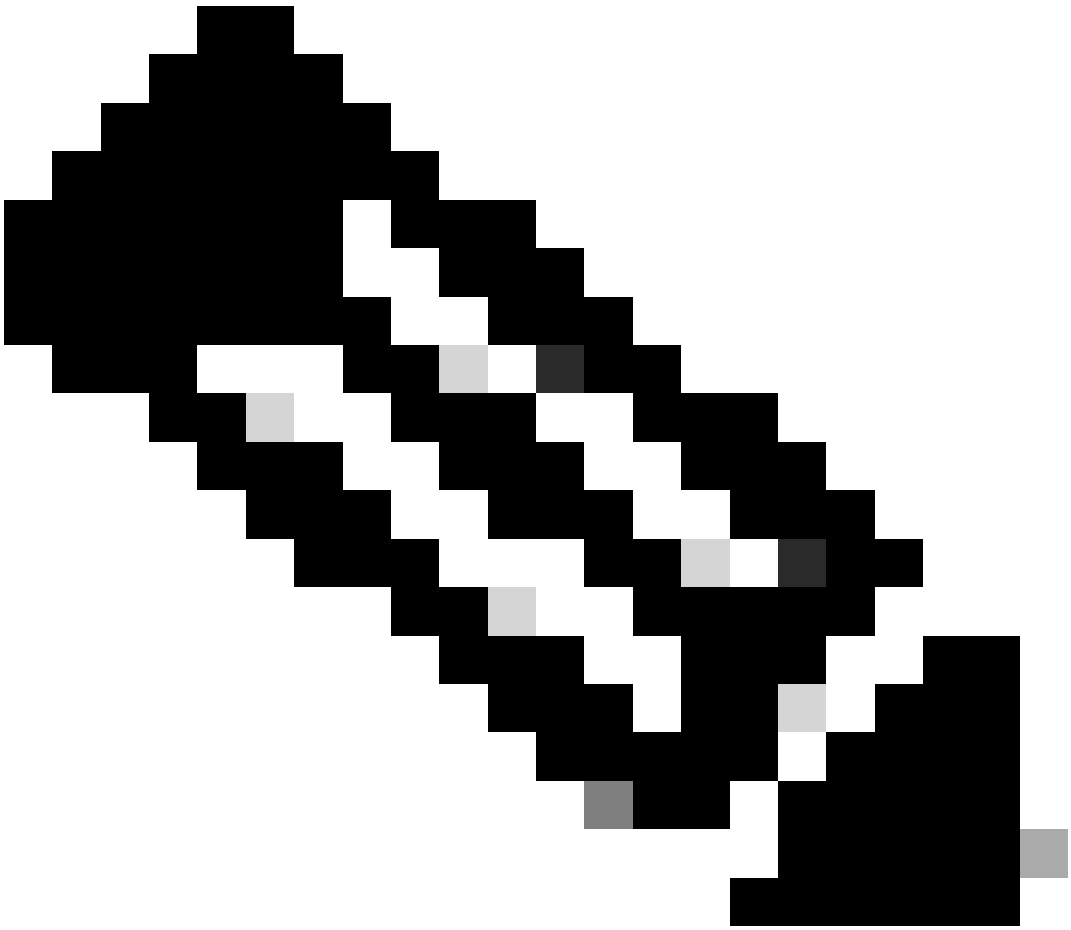
- Kenntnisse der Konfiguration von Cisco Aironet APs
- Grundkenntnisse von SSH und verwandten Sicherheitskonzepten

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Aironet AP der Serie 1200 mit Cisco IOS® Software, Version 12.3(8)JEB

- PC oder Laptop mit SSH-Client-Dienstprogramm



Hinweis: In diesem Dokument wird das SSH-Client-Dienstprogramm zum Überprüfen der Konfiguration verwendet. Sie können ein beliebiges Client-Dienstprogramm eines Drittanbieters verwenden, um sich mit SSH beim Access Point anzumelden.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Zugreifen auf die Befehlszeilenschnittstelle (CLI) des Aironet AP

Sie können eine der folgenden Methoden verwenden, um auf die Kommandozeilenschnittstelle (CLI) des Aironet AP zuzugreifen:

- Konsolen-Port
- Telnet
- SSH

Wenn der Access Point über einen Konsolenport verfügt und Sie physischen Zugriff auf den Access Point haben, können Sie sich über den Konsolenport beim Access Point anmelden und die Konfiguration bei Bedarf ändern. Weitere Informationen zur Verwendung des Konsolenports für die Anmeldung am Access Point finden Sie im Abschnitt Verbindung mit lokalen Access Points der Serie 1200 herstellen im DokumentErstkonfiguration des Access Points.

Wenn Sie nur über das Ethernet auf den AP zugreifen können, verwenden Sie entweder das Telnet-Protokoll oder das SSH-Protokoll, um sich beim AP anzumelden.

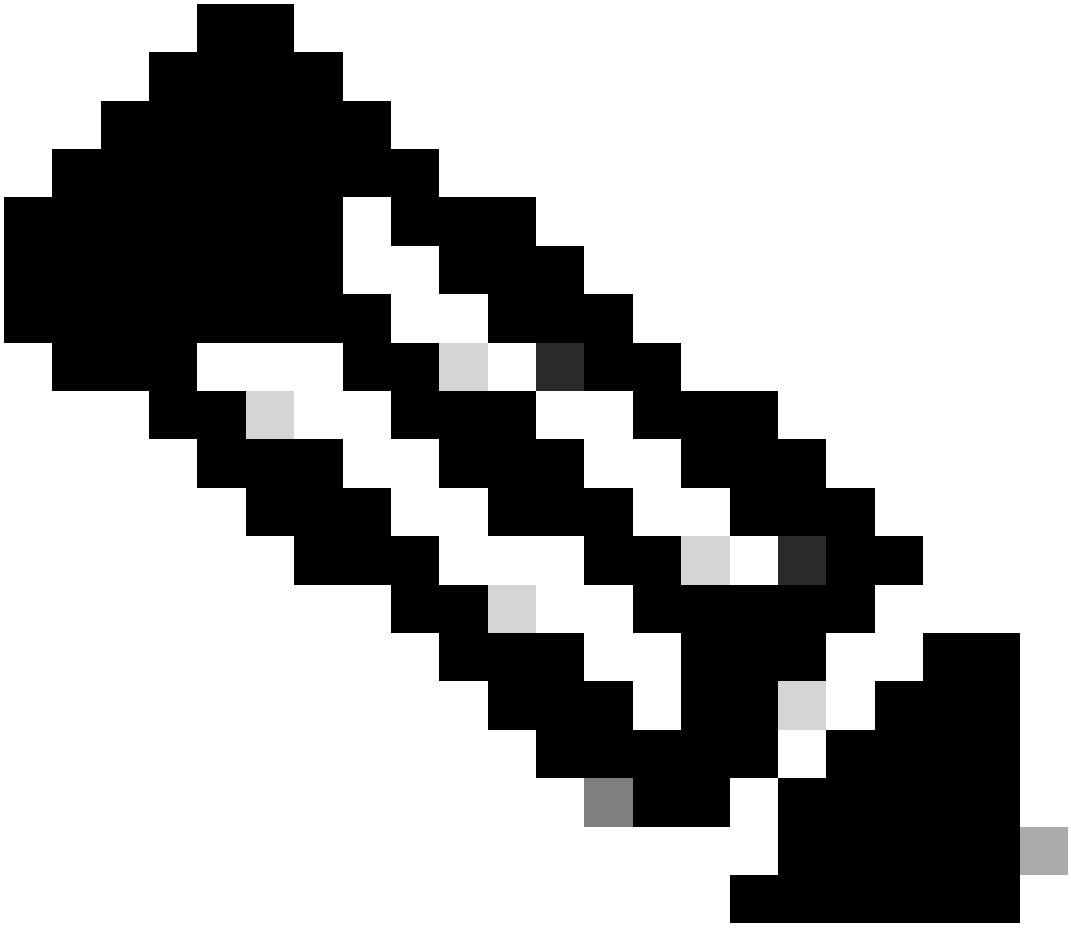
Das Telnet-Protokoll verwendet Port 23 für die Kommunikation. Telnet überträgt und empfängt Daten in Klartext. Da die Datenkommunikation im Klartext erfolgt, kann ein Hacker leicht die Passwörter kompromittieren und auf den AP zugreifen. RFC 854 definiert Telnet und erweitert Telnet mit Optionen von vielen anderen RFCs.

SSH ist eine Anwendung und ein Protokoll, die einen sicheren Ersatz für die Berkley r-tools. SSH ist ein Protokoll, das eine sichere Remote-Verbindung zu einem Layer 2- oder Layer 3-Gerät bereitstellt. Es gibt zwei SSH-Versionen: SSH Version 1 und SSH Version 2. Diese Softwareversion unterstützt beide SSH-Versionen. Wenn Sie die Versionsnummer nicht angeben, wird die Standardversion 2 verwendet.

SSH bietet mehr Sicherheit für Remote-Verbindungen als Telnet, da es eine starke Verschlüsselung bei der Authentifizierung eines Geräts bietet. Diese Verschlüsselung ist ein Vorteil gegenüber einer Telnet-Sitzung, bei der die Kommunikation im Klartext erfolgt. Weitere Informationen zu SSH finden Sie unter Secure Shell (SSH) FAQ. Die SSH-Funktion verfügt über einen SSH-Server und einen integrierten SSH-Client.

Der Client unterstützt folgende Benutzerauthentifizierungsmethoden:

- RADIUS
- Lokale Authentifizierung und Autorisierung



Hinweis: Die SSH-Funktion in dieser Softwareversion unterstützt IP Security (IPSec) nicht.

Sie können APs für SSH mithilfe der CLI oder GUI konfigurieren. In diesem Dokument werden beide Konfigurationsmethoden erläutert.

Konfigurieren

CLI-Konfiguration

Dieser Abschnitt enthält Informationen zum Konfigurieren der Funktionen mithilfe von CLI.

Schritt-für-Schritt-Anleitung

Um den SSH-basierten Zugriff auf dem WAP zu aktivieren, müssen Sie den WAP zunächst als SSH-Server konfigurieren. Gehen Sie folgendermaßen vor, um über die CLI einen SSH-Server auf dem Access Point zu konfigurieren:

1. Konfigurieren Sie einen Host- und einen Domänennamen für den Access Point.

<#root>

```
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 domain

!--- This command configures the AP with the domain name "domain name".
```

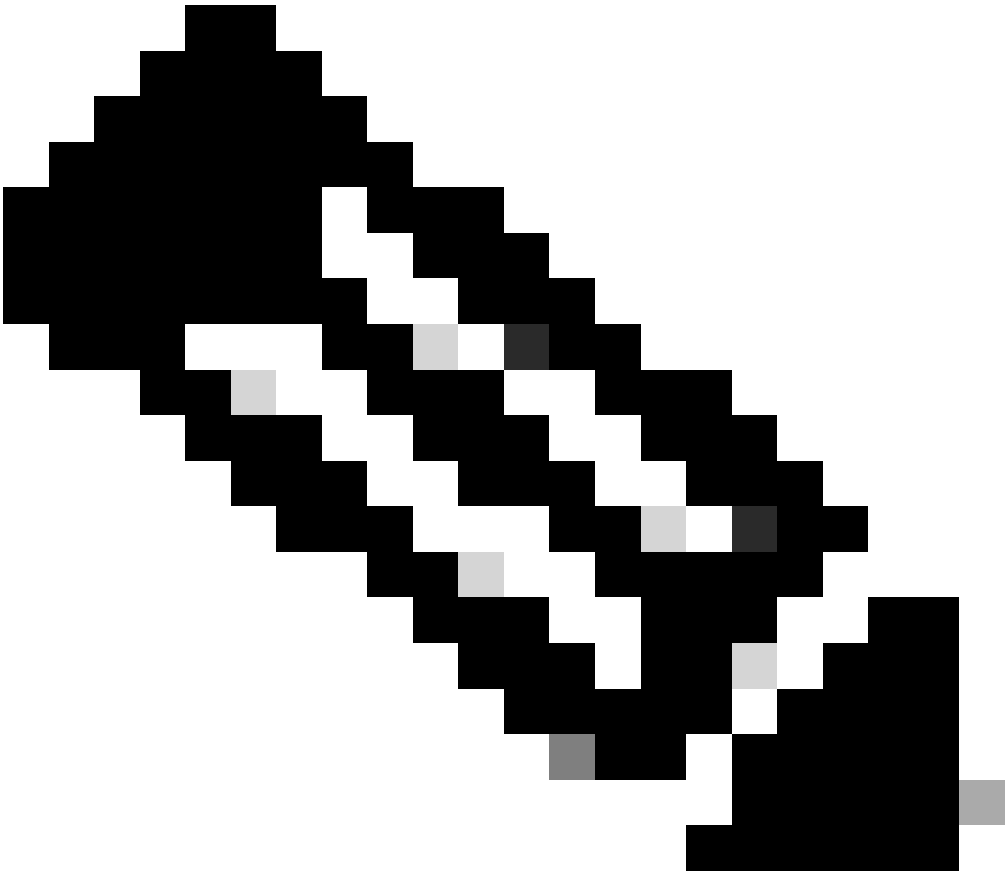
2. Erstellen Sie einen Rivest-, Shamir- und Adelman-Schlüssel (RSA-Schlüssel) für Ihren AP.

   Die Generierung eines RSA-Schlüssels aktiviert SSH auf dem AP. Geben Sie diesen Befehl im globalen Konfigurationsmodus ein:

<#root>

```
Test<config>#
crypto key generate rsa rsa_key_size

!--- This generates an RSA key and enables the SSH server.
```



Hinweis: Die empfohlene Mindestgröße für einen RSA-Schlüssel beträgt 1024.

3. Konfigurieren Sie die Benutzerauthentifizierung auf dem Access Point.

   Auf dem AP können Sie die Benutzerauthentifizierung so konfigurieren, dass entweder die lokale Liste oder ein externer AAA-Server (Authentication, Authorization, Accounting) verwendet wird. In diesem Beispiel wird eine lokal generierte Liste verwendet, um die Benutzer zu authentifizieren:

   <#root>

   ```
   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 "Domain".
```

Durch diese Konfiguration wird der Access Point so konfiguriert, dass er eine benutzerbasierte Authentifizierung unter Verwendung einer lokalen Datenbank durchführt, die auf dem Access Point konfiguriert ist. In diesem Beispiel werden zwei Benutzer in der lokalen Datenbank konfiguriert: "Test" und "ABC".

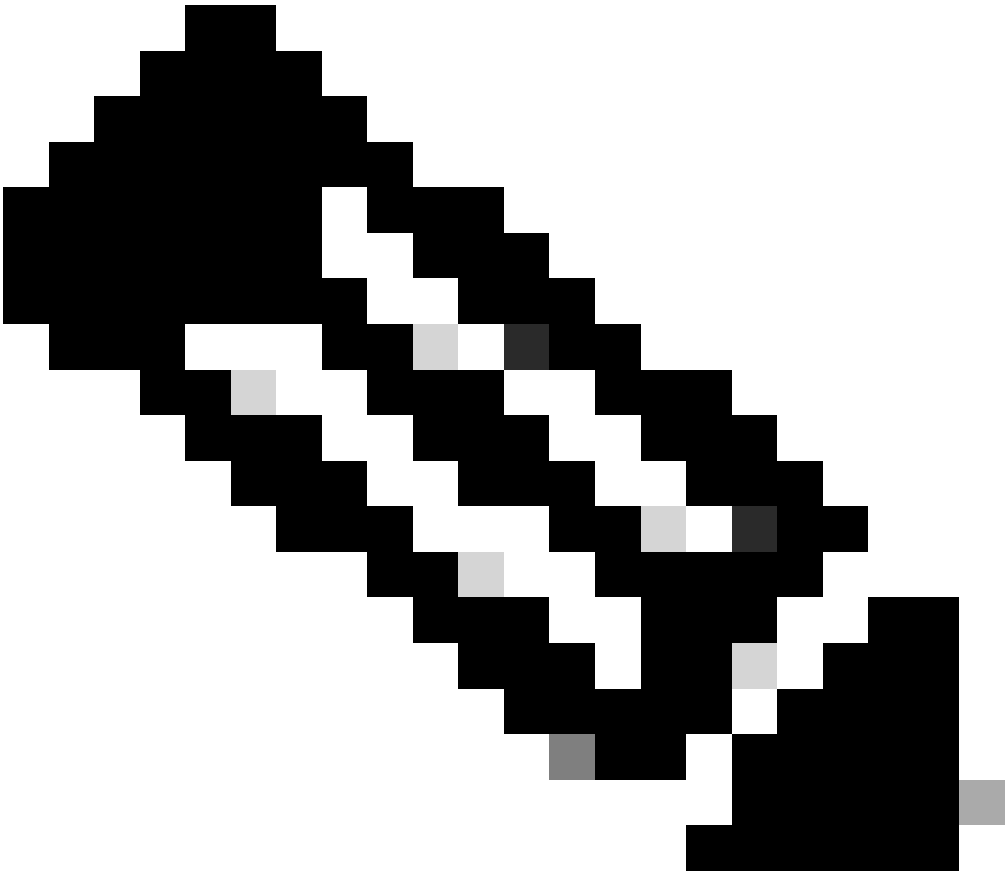
4. Konfigurieren der SSH-Parameter

<#root>

```
Test<config>#

ip ssh {[timeout seconds] | [authentication-retries integer]}


!--- Configure the SSH control variables on the AP.
```



Hinweis: Sie können das Timeout in Sekunden angeben, aber nicht mehr als 120 Sekunden. Der Standardwert ist 120. Dies ist die Spezifikation, die für die SSH-Aushandlungsphase gilt. Sie können auch die Anzahl der Authentifizierungsversuche angeben, jedoch nicht mehr als fünf Authentifizierungsversuche. Der Standardwert ist drei.

GUI-Konfiguration

Sie können die grafische Benutzeroberfläche auch verwenden, um den SSH-basierten Zugriff auf dem Access Point zu aktivieren.

Schritt-für-Schritt-Anleitung

Führen Sie diese Schritte aus:

1. Melden Sie sich über den Browser beim Access Point an.

   Das Fenster "Summary Status" wird angezeigt.

2. Klicken Sie im Menü links auf Services.

   Das Fenster "Service-Übersicht" wird angezeigt.

3. Klicken Sie auf Telnet/SSH, um die Telnet/SSH-Parameter zu aktivieren und zu konfigurieren.

   Das Fenster Dienste: Telnet/SSH wird angezeigt. Blättern Sie nach unten zum Bereich Secure Shell Configuration. Klicken Sie neben Secure Shell auf Enable (Aktivieren), und geben Sie die SSH-Parameter ein, wie in diesem Beispiel gezeigt:

   In diesem Beispiel werden folgende Parameter verwendet:

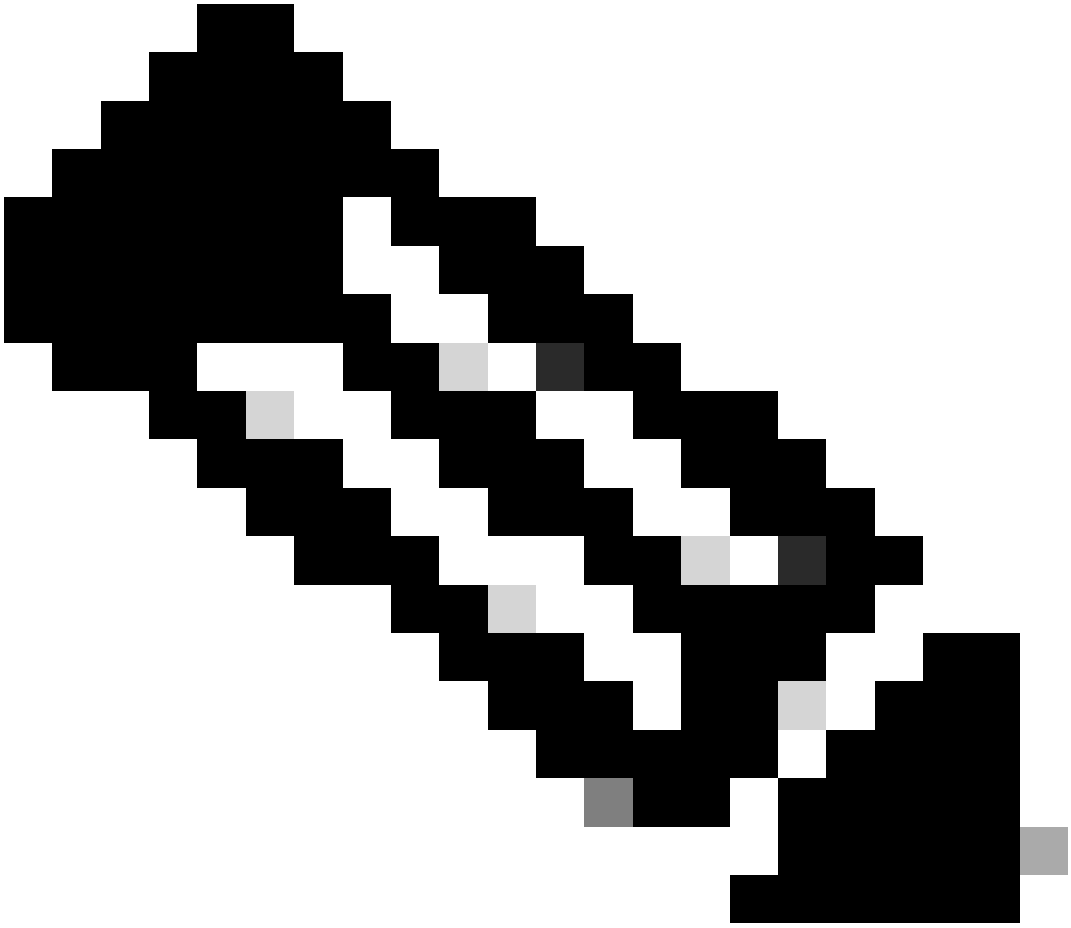
   - Systemname: Test
   - Domänenname: DOMÄNE
   - Größe des RSA-Schlüssels: 1024
   - Authentifizierungs-Timeout: 120
   - Authentifizierungsversuche: 3

4. Klicken Sie auf Apply, um die Änderungen zu speichern.

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (OIT) unterstützt bestimmte show-Befehle. Verwenden Sie das OIT, um eine Analyse der show-Befehlsausgabe anzuzeigen.



Hinweis: Nur registrierte Cisco BenutzerInnen können auf interne Cisco Tools und Informationen zugreifen.

- show ip ssh: Überprüft, ob SSH auf dem WAP aktiviert ist, und ermöglicht Ihnen, die Version von SSH zu überprüfen, die auf dem WAP ausgeführt wird. Diese Ausgabe enthält ein Beispiel:
- show ssh: Ermöglicht die Anzeige des Status Ihrer SSH-Serververbindungen. Diese Ausgabe enthält ein Beispiel:

Stellen Sie jetzt eine Verbindung über einen PC her, auf dem SSH-Software von Drittanbietern ausgeführt wird, und versuchen Sie dann, sich beim Access Point anzumelden. Bei dieser Überprüfung wird die IP-Adresse des Access Points 10.0.0.2 verwendet. Da Sie den Benutzernamen Test konfiguriert haben, verwenden Sie diesen Namen, um über SSH auf den Access Point zuzugreifen:

Fehlerbehebung

Verwenden Sie diesen Abschnitt, um Probleme mit Ihrer Konfiguration zu beheben.

Wenn Ihre SSH-Konfigurationsbefehle als ungültige Befehle zurückgewiesen werden, haben Sie kein RSA-Schlüsselpaar für Ihren Access Point erfolgreich generiert.

SSH deaktivieren

Um SSH auf einem Access Point zu deaktivieren, müssen Sie das auf dem Access Point generierte RSA-Paar löschen. Um das RSA-Paar zu löschen, geben Sie den Befehl crypto key zeroize rsa im globalen Konfigurationsmodus ein. Wenn Sie das RSA-Schlüsselpaar löschen, deaktivieren Sie automatisch den SSH-Server. Diese Ausgabe enthält ein Beispiel:

Zugehörige Informationen

- Support-Seite für Secure Shell (SSH)
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.