

PuTTYgen Generation of SSH Authorized Keys and RSA Authentication on Cisco Secure IDS Configuration Example

Document ID: 61864

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure

- Configure PuTTYgen

Verify

- RSA Authentication

Troubleshoot

Related Information

Introduction

This document explains how to use the Key generator for PuTTY (PuTTYgen) to generate Secure Shell (SSH) authorized keys and RSA authentication for use on Cisco Secure Intrusion Detection System (IDS). The primary issue when you establish SSH authorized keys is that only the older RSA1 key format is acceptable. This means that you need to tell your key generator to create an RSA1 key, and you must restrict the SSH client to use the SSH1 protocol.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Recent PuTTY – February 7, 2004
- Cisco Secure IDS

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

This section presents you with the information to configure the features this document describes.

Note: Use the Command Lookup Tool (registered customers only) to find additional information on the commands this document uses.

Configure PuTTYgen

Complete these steps to configure PuTTYgen.

1. Launch PuTTYgen.
2. Click the **SSH1** key type and set the number of bits in the generated key to **2048** in the Parameters group at the bottom of the dialog box.
3. Click **Generate** and follow the instructions.

The key information is displayed in the upper section of the dialog box.

4. Clear the Key Comment edit box.
5. Select all the text in Public key for pasting into authorized_keys file and press **Ctrl-C**.
6. Type a passphrase in the Key passphrase and Confirm passphrase edit boxes.
7. Click **Save private key**.
8. Save the PuTTY private key file into a directory private to your Windows login (in the Documents and Settings/(userid)/My Documents subtree in Windows 2000/XP).
9. Launch PuTTY.
10. Create a new PuTTY session as seen here:
 - ◆ **Session:**
 - ◆ **IP Address:** IP address of the IDS sensor
 - ◆ **Protocol:** SSH
 - ◆ **Port:** 22
 - ◆ **Connection:**
 - ◆ **Auto-login username:** cisco (can also be the login you use on the Sensor)
 - ◆ **Connection/SSH:**
 - ◆ **Preferred SSH version:** 1 only
 - ◆ **Connection/SSH/Auth:**
 - ◆ **Private key file for authentication:** Browse to the .PPK file stored in step 8.
 - ◆ **Session:** (back to the top)
 - ◆ **Saved sessions:** (enter the sensor name, click **Save**)
11. Click **Open** and use password authentication to connect to the Sensor CLI, since the public key is not on the Sensor yet.
12. Enter the **configure terminal** CLI command and press **Enter**.
13. Enter the **ssh authorized-key mykey** CLI command, but do not press Enter at this time. Make sure and type a space at the end.
14. Right-click in the PuTTY terminal window.

The clipboard material copied in step 5 is typed into the CLI.
15. Press **Enter**.
16. Enter the **exit** command and press **Enter**.
17. Confirm the authorized key is entered properly. Enter the **show ssh authorized-keys mykey** command and press **Enter**.
18. Enter the **exit** command to quit the IDS CLI and press **Enter**.

Verify

RSA Authentication

Complete these steps.

1. Launch PuTTY.
2. Locate the Saved Session created in step 10 and double-click on it. A PuTTY terminal window opens and this text appears:

```
Sent username "cisco"  
Trying public key authentication.  
Passphrase for key "":
```

3. Type the private key passphrase you created in step 6 and press **Enter**.

You are automatically logged in.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [Network Intrusion Detection Technical Support Pages](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 24, 2008

Document ID: 61864
