Why is Ezeelogin the most secure ssh gateway?

101 admin October 15, 2025 General, Security Features 10070

What makes Ezeelogin the most secure SSH gateway available?

Overview: This article explains how ezeelogin makes the most secure SSH gateway.

1. SSH User **password** and **security codes** are hashed using **CRYPT**(SHA512, SHA256, BLOWFISH . DES algorithms). So even in the unlikely scenario of the gateway server being rooted, access to all other servers would still be secure.
2. **Private keys/server root passwords/Critical information** are encrypted using **Asymmetric encryption** so it's almost impossible to get hold of the keys.
3. Two-factor authentication in the SSH gateway and for the web GUI (Authenticator applications (e.g., Google Authenticator, Microsoft Authenticator, and others) /Yubikey). This is especially useful when you outsource technical support and when you don't know how secure the tech's desktop is. So with the 2-factor authentication, there is an additional layer of security.
4. Access control to grant/deny SSH access to servers for individual users.
5. SSH logs including input and output of every key pressed or command executed on the server including live streaming of what tech is doing on the server.
6. Automated root password reset and password management.
7. Automated SUDO support so that you don't have to waste time with the su.
8. In the event that tech leaves the company, all the root passwords on all servers could be reset at the click of a button.
9. Command guard to filter commands like rm -rf / entered accidentally. Basically, you can create any command filters using regexp.

Related Articles:

Encryption Technologies used in Ezeelogin

Online URL: https://www.ezeelogin.com/kb/article/why-is-ezeelogin-the-most-secure-ssh-gateway-101.html