How to secure SSH jump server / SSH bastion host / SSH gateway

103 admin November 23, 2024 Getting Started, Security Compliances, Tweaks & Configuration 20852

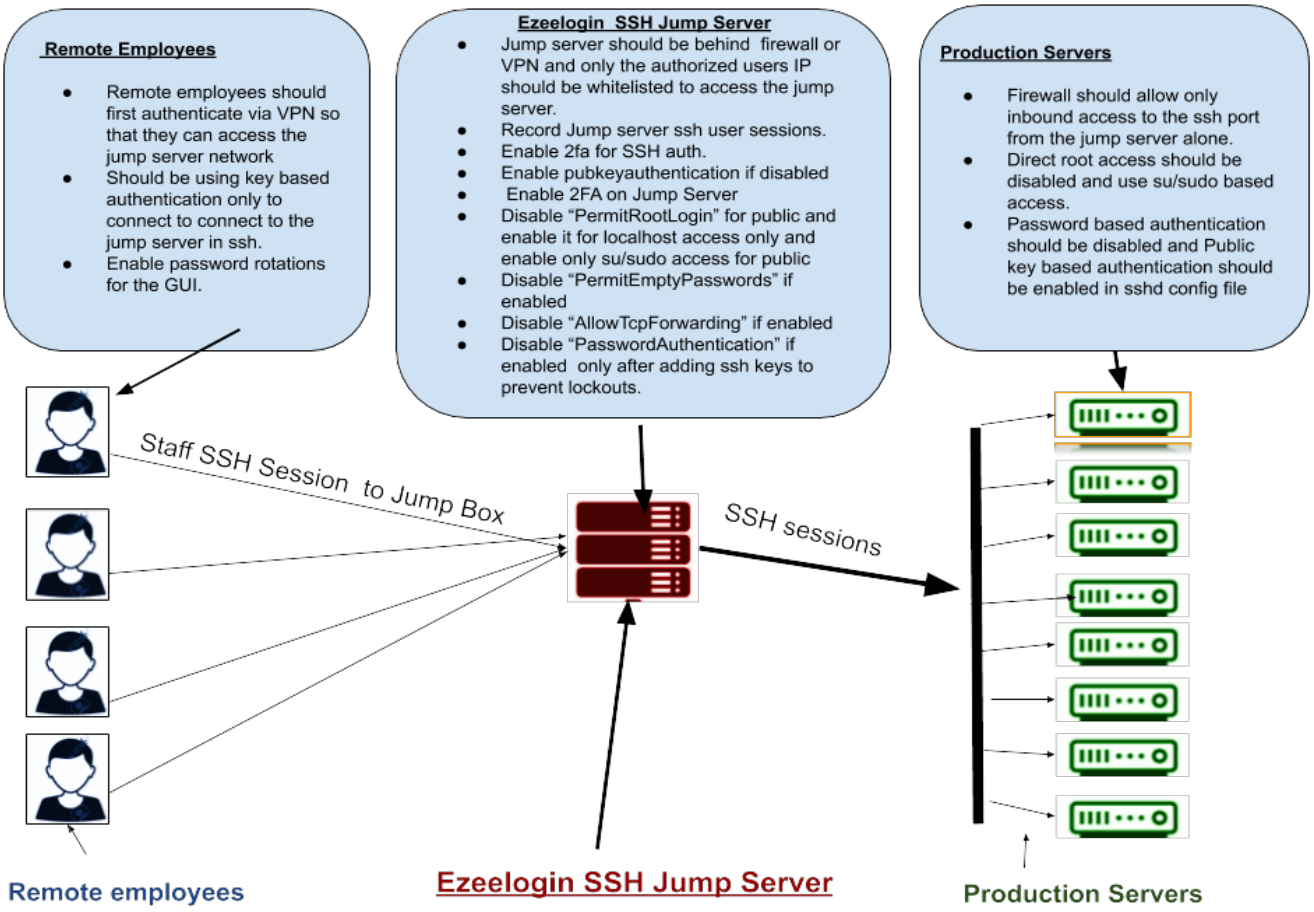
How to secure SSH jump server ?

Overview: This article defines what an SSH bastion host is and how to secure an SSH jump server.

What is an SSH Bastion Host?

SSH Bastion host is simply a single, hardened server that you "jump" through in order to access other servers or devices on the inner network. It's simply a server that all of your users can log into and use as a relay server to connect to other Linux servers, Routers, Switches, and more. Find more about the SSH bastion host.

Security measures to harden Ezeelogin Linux SSH Jump server.



---

1. Two-factor authentication:

Enforce 2-factor authentication like Google 2FA auth or Yubikey 2FA or DUO Security so that both the Ezeelogin web GUI and SSH interface have an additional layer of protection.

2. SSL For HTTPS:

Enable SSL and access your web GUI using HTTPS only. You would need to install your SSL certificate for the GUI and then enable SSL mode in Ezeelogin settings.

3. Enable Captcha:

Enable reCaptcha for the web GUI in the Ezeelogin settings.

4. Hardening SSH Server Daemon configuration file:

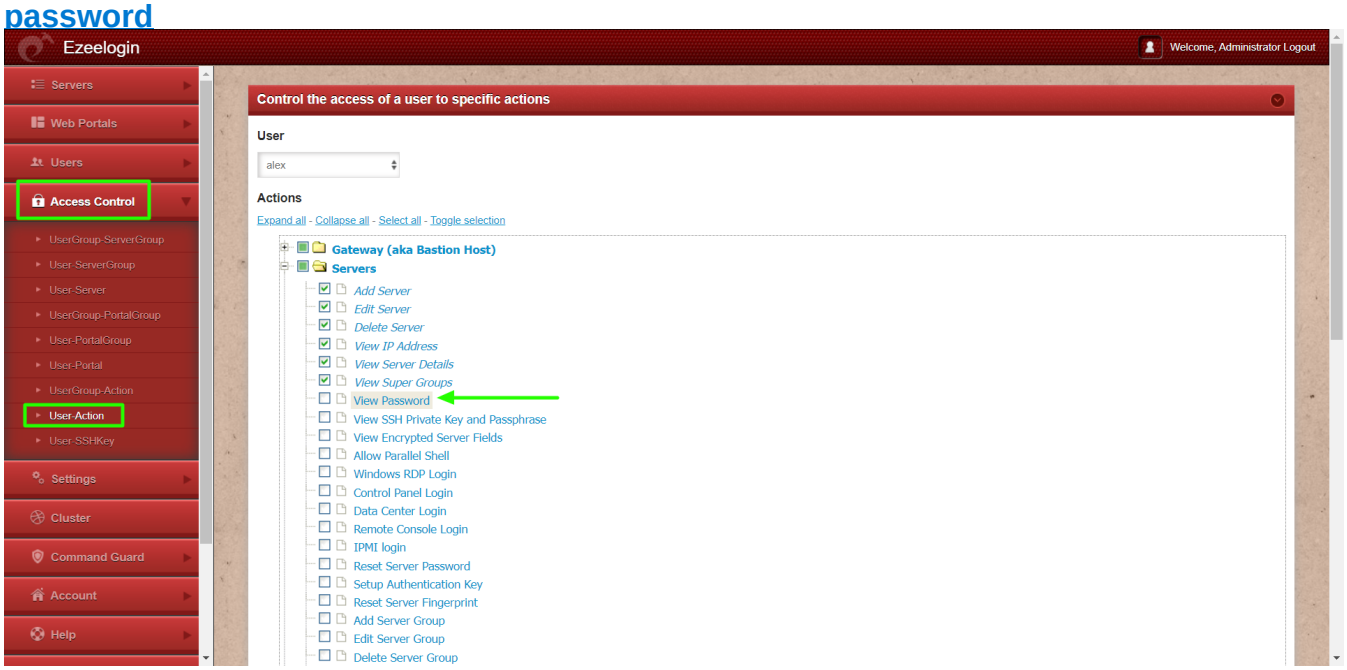
Disable password authentication, Disable AllowTCPForwarding, and Disable Password Authentication as Public key-based authentication is recommended

```
root@gateway:~# vi /etc/sshd/sshd_config


#Allow Key-based authentication as its harder to brute-force or sniff than a password

Pubkeyauthentication yes
```

```
#Disable password authentication to the jump server as key-based authentication is much more secure. Make sure to enable this under localhost section below.
#Make sure to add in your SSH Public key before you disable password authentication to prevent lock outs.
PasswordAuthentication no

#Disable Tcp Forwarding on the jump server

AllowTcpForwarding no

#Disable direct root logins to servers and instead login as non privileged user and switch to root
#Make sure that a non privileged user can ssh and switch to become a root user before disabling direct root login.

PermitRootLogin no



#SSHD localhost settings. ( Note the rules under the following section will apply only to localhost ( 127.0.0.1) )

Match Address 127.0.0.1

PermitRootLogin yes

PubkeyAuthentication yes
PasswordAuthentication yes



#Do a syntax check of sshd configuration file as shown below

root@gateway:~# sshd -T

# restart sshd daemon

root@gateway:~# service sshd restart
```

5. Disable the view server password **field in Ezeelogin GUI:**

Login to Ezeelogin GUI and navigate to **Access control** -> **User action** -> **disable view password**



6. Enable Firewall and Lockdown access:

Always, restrict the ips from which staff are allowed to ssh from. You should be allowing only your IPs, employees ips and the default rule should block SSH for everyone and should be granted explicitly. You can achieve this using iptables or setting up rules in host.allow/hosts.deny files.

Refer article to grant SSH access only from the gateway IP to the remote server

7. SSH Gateway behind VPN is Very Good:

Having the SSH Jump server behind a VPN is very good as it prevents unauthorized traffic. This is highly recommended.

Related Articles:

Grant SSH access only from an IP to a server

Setup and configure Jump Server

Online URL:
https://www.ezeelogin.com/kb/article/how-to-secure-ssh-jump-server-ssh-bastion-host-ssh-gateway-103.html