* Por padrão, o daemon sshd ouve na porta TCP 22. A mudança da porta reduz a exposição do sistema a ataques baseados em varredura automatizada da rede e, assim, aumenta a segurança através da obscuridade. Você pode especificar a porta usando a diretiva Port no arquivo de configuração /etc/ssh/sshd\_config.

Você também tem que atualizar a política padrão da SELinux para permitir o uso de uma porta não inadimplente. Para fazer isso, utilize a ferramenta semanage do pacote policycoreutils-python-utils:

# **semanage port -a -t ssh\_port\_t -p tcp *port\_number***

Além disso, atualizar a configuração firewalld:

# **firewall-cmd --add-port *port\_number*/tcp**

# **firewall-cmd --runtime-to-permanent**

Nos comandos anteriores, substituir *port\_number* pelo novo número de porta especificado usando a diretiva Port.

Ex. para a porta 2222

/etc/ssh/sshd\_config

**Alterar**

Port 2222

SAIR

**Liberar nas politicas de segurança**

semanage port -a -t ssh\_port\_t -p tcp 2222

**Liberar no Firewall**

firewall-cmd --add-port 2222/tcp

firewall-cmd --runtime-to-permanent

**Reiniciar o Serviço**

**systemctl reload sshd**

<https://access.redhat.com/documentation/pt-br/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/making-openssh-more-secure_using-secure-communications-between-two-systems-with-openssh>