Port 22

Protocol 2

DebianBanner no

# === Logging

SyslogFacility AUTHPRIV

LogLevel VERBOSE

# === Authentication

PubkeyAuthentication no

AuthorizedKeysFile .ssh/authorized\_keys

UsePAM yes

PasswordAuthentication yes

KbdInteractiveAuthentication no

StrictModes yes

LoginGraceTime 60

PermitRootLogin no

KerberosAuthentication no

IgnoreRhosts yes

IgnoreUserKnownHosts yes

RhostsRSAAuthentication no

HostbasedAuthentication no

PermitEmptyPasswords no

ChallengeResponseAuthentication no

UseDNS yes

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none

#AuthorizedKeysCommandUser nobody

# === Session

MaxSessions 2

MaxAuthTries 2

MaxStartups 2

AcceptEnv LANG LC\_\*

PrintMotd no

PrintLastLog yes

TCPKeepAlive yes

ClientAliveInterval 30

ClientAliveCountMax 6

#MaxStartups 10:30:100

# === Features

AllowTcpForwarding no

GatewayPorts no

AllowStreamLocalForwarding no

PermitTunnel no

Compression no

PermitUserEnvironment no

AllowAgentForwarding no

X11Forwarding no

# === Cryptography

#HostKey /etc/ssh/ssh\_host\_rsa\_key

#HostKey /etc/ssh/ssh\_host\_ecdsa\_key

#HostKey /etc/ssh/ssh\_host\_ed25519\_key

#RekeyLimit default none

KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256

Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com

Subsystem sftp internal-sftp -f AUTH -l INFO