# SSH-Tunneling mit Proxy

```
 % GIT_TRACE=1 GIT_CURL_VERBOSE=1 git push
21:32:14.216308 exec-cmd.c:139          trace: resolved executable path from Darwin stack: /Applications/Xcode
21:32:14.216594 exec-cmd.c:238          trace: resolved executable dir: /Applications/Xcode.app/Contents/Devel
21:32:14.216949 git.c:460               trace: built-in: git push
21:32:14.218655 run-command.c:655       trace: run_command: unset GIT_PREFIX; ssh git@github.com 'git-receive-
Everything up-to-date
```

Ich habe langsame `git push`-Operationen erlebt, bei denen Verzögerungen während der `ssh git@github.com`-Phas

Um `corkscrew` für SSH-Tunneling zu verwenden, müssen Sie es zuerst installieren. Auf macOS können Sie Homebre

`~/.ssh/config`:

```bash
Host *
    UseKeychain ja
    AddKeysToAgent ja
    IdentityFile ~/.ssh/id_rsa
    ProxyCommand corkscrew localhost 7890 %h %p
```

Protokoll:

“‘bash % ssh root@138.201.174.0 -vvv  **Proxyeinstellungen erkannt:** - HTTP_PROXY: http://127.0.0.1:7890 - HTTPS_PROXY: http://127.0.0.1:7890

OpenSSH_9.8p1, LibreSSL 3.3.6 debug1: Reading configuration data /Users/lzwjava/.ssh/config debug1: /Users/lzwjava/.ssh/config Zeile 1: Applying options for *debug1: Reading configuration data /etc/ssh/ssh_config debug1: /etc/ssh/ssh_config Zeile 21: include /etc/ssh/ssh_config.d/* matched no files debug1: /etc/ssh/ssh_config Zeile 54: Applying options for *debug2: resolve_canonicalize: hostname 138.201.174.0 is address debug3: expanded UserKnownHostsFile ‘~/.ssh/known_hosts’-> ‘/Users/lzwjava/.ssh/known_hosts’debug3: expanded UserKnownHostsFile ‘~/.ssh/known_hosts2’-> ‘/Users/lzwjava/.ssh/known_hosts2’debug1: Authenticator provider $SSH_SK_PROVIDER did not resolve; disabling debug3: channel_clear_timeouts: clearing debug1: Executing proxy command: exec corkscrew localhost 7890 138.201.174.0 22 debug1: identity file /Users/lzwjava/.ssh/id_rsa type 0 debug1: identity file /Users/lzwjava/.ssh/id_rsa-cert type -1 debug1: Local version string SSH-2.0-OpenSSH_9.8 debug1: Remote protocol version 2.0, remote software version OpenSSH_9.6p1 Ubuntu-3ubuntu13.5 debug1: compat_banner: match: OpenSSH_9.6p1 Ubuntu-3ubuntu13.5 pat OpenSSH* compat 0x04000000 debug2: fd 5 setting O_NONBLOCK debug2: fd 4 setting O_NONBLOCK debug1: Authenticating to 138.201.174.0:22 as ‘root’debug3: record_hostkey: found key type ED25519 in file /Users/lzwjava/.ssh/known_hosts:164 debug3: record_hostkey: found key type RSA in file /Users/lzwjava/.ssh/known_hosts:165 debug3: record_hostkey:

found key type ECDSA in file /Users/lzwjava/.ssh/known_hosts:166 debug3: load_hostkeys_file: loaded 3 keys from 138.201.174.0 debug1: load_hostkeys: fopen /Users/lzwjava/.ssh/known_hosts2: No such file or directory debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory debug3: order_hostkeyalgs: have matching best-preference key type ssh-ed25519-cert-v01@openssh.com, using HostkeyAlgorithms verbatim debug3: send packet: type 20 debug1: SSH2_MSG_KEXINIT sent debug3: receive packet: type 20 debug1: SSH2_MSG_KEXINIT received debug2: local client KEXINIT proposal debug2: KEX algorithms: sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com debug2: host key algorithms: ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256 debug2: ciphers ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: ciphers stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
debug2: MACs ctos: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com
sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hm
sha2-256,hmac-sha2-512,hmac-sha1 debug2: MACs stoc: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: compression ctos: none,zlib@openssh.com,zlib debug2: compression stoc: none,zlib@openssh.com,z
debug2: languages ctos: debug2: languages stoc: debug2: first_kex_follows 0 debug2: reserved 0 debug2: peer server KEXINIT proposal debug2: KEX algorithms: sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-s,kex-strict-s-v00@openssh.com debug2: host key algorithms: rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519 debug2: ciphers ctos: chacha20-poly1305@openssh.com,aes
ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: ciphers stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: MACs ctos: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: MACs stoc: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hm
sha2-256,hmac-sha2-512,hmac-sha1 debug2: compression ctos: none,zlib@openssh.com debug2: compression stoc: none,zlib@openssh.com debug2: languages ctos: debug2: languages stoc: debug2: first_kex_follows 0 debug2: reserved 0 debug3: kex_choose_conf: will use strict KEX ordering

debug1: kex: algorithm: sntrup761x25519-sha512@openssh.com debug1: kex: host key algorithm: ssh-ed25519 debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: compression: none debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: compression: none debug3: send packet: type 30 debug1: expecting SSH2_MSG_KEX_ECDH_REPLY debug3: receive packet: type 31 debug1: SSH2_MSG_KEX_ECDH_REPLY received debug1: Server host key: ssh-ed25519 SHA256:+5SaMkJXG9yZrsYjXgxFfRZpvb6qjc/arFG2Nk4Vv48 debug3: record_hostkey: found key type ED25519 in file /Users/lzwjava/.ssh/known_hosts:164 debug3: record_hostkey: found key type RSA in file /Users/lzwjava/.ssh/known_hosts:165 debug3: record_hostkey: found key type ECDSA in file /Users/lzwjava/.ssh/known_hosts:166 debug3: load_hostkeys_file: loaded 3 keys from 138.201.174.0 debug1: load_hostkeys: fopen /Users/lzwjava/.ssh/known_hosts2: No such file or directory debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory debug1: Host '138.201.174.0'is known and matches the ED25519 host key. debug1: Found key in /Users/lzwjava/.ssh/known_hosts:164 debug3: send packet: type 21 debug1: ssh_packet_send2_wrapped: resetting send seqnr 3 debug2: ssh_set_newkeys: mode 1 debug1: rekey out after 134217728 blocks debug1: SSH2_MSG_NEWKEYS sent debug1: Sending SSH2_MSG_EXT_INFO debug3: send packet: type 7 debug1: expecting SSH2_MSG_NEWKEYS debug3: receive packet: type 21 debug1: ssh_packet_read_poll2: resetting read seqnr 3 debug1: SSH2_MSG_NEWKEYS received debug2: ssh_set_newkeys: mode 0 debug1: rekey in after 134217728 blocks debug2: KEX algorithms: sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com debug2: host key algorithms: ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256 debug2: ciphers ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: ciphers stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: MACs ctos: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: MACs stoc: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: compression ctos: none,zlib@openssh.com,zlib debug2: compression stoc: none,zlib@openssh.com,zlib debug2: languages ctos: debug2: languages stoc: debug2: first_kex_follows 0 debug2: reserved 0 debug3: send packet: type 5 debug3: receive packet: type 7 debug1: SSH2_MSG_EXT_INFO received debug3: kex_input_ext_info: extension server-sig-algs debug1: kex_ext_info_client_parse: server-sig-algs=<ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-

ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256> debug3: kex_input_ext_info: extension publickey-hostbound@openssh.com debug1: kex_ext_info_check_ver: publickey-hostbound@openssh.com=<0> debug3: kex_input_ext_info: extension ping@openssh.com debug1: kex_ext_info_check_ver: ping@openssh.com=<0> debug3: receive packet: type 6 debug2: service_accept: ssh-userauth debug1: SSH2_MSG_SERVICE_ACCEPT received debug3: send packet: type 50 debug3: receive packet: type 7 debug1: SSH2_MSG_EXT_INFO received debug3: kex_input_ext_info: extension server-sig-algs debug1: kex_ext_info_client_parse: server-sig-algs=<ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256> debug3: receive packet: type 51 debug1: Authentications that can continue: publickey,password debug3: start over, passed a different list publickey,password debug3: preferred publickey,keyboard-interactive,password debug3: authmethod_lookup publickey debug3: remaining preferred: keyboard-interactive,password debug3: authmethod_is_enabled publickey debug1: Next authentication method: publickey debug3: ssh_get_authentication_socket_path: path '/private/tmp/com.apple.launchd.cTjjogIh4V/Listeners'debug1: get_agent_identities: bound agent to hostkey debug1: get_agent_identities: agent returned 3 keys debug1: Will attempt key: /Users/lzwjava/.ssh/id_rsa RSA SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 explicit agent debug1: Will attempt key: lzwjava@Zhiweis-MacBook-Air.local RSA SHA256:ibpUGVDyOYKOQArPUs5ZSnp0oECaZJWSPWAthOYBX/8 agent debug1: Will attempt key: /Users/lzwjava/Downloads/LightsailDefaultKey-ap-northeast-1.pem RSA SHA256:AQCwUpsEP8cawJtCQ agent debug2: pubkey_prepare: done debug1: Offering public key: /Users/lzwjava/.ssh/id_rsa RSA SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 explicit agent debug3: send packet: type 50 debug2: we sent a publickey packet, wait for reply debug3: receive packet: type 60 debug1: Server accepts key: /Users/lzwjava/.ssh/id_rsa RSA SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 explicit agent debug3: sign_and_send_pubkey: using publickey-hostbound-v00@openssh.com with RSA SHA256:bF6g9+hPW6crim36xewb/
debug3: sign_and_send_pubkey: signing using rsa-sha2-512 SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 debug3: send packet: type 50 debug3: receive packet: type 52 Authenticated to 138.201.174.0 (via proxy) using "publickey". debug1: channel 0: new session [client-session] (inactive timeout: 0) debug3: ssh_session2_open: channel_new: 0 debug2: channel 0: send open debug3: send packet: type 90 debug1: Requesting no-more-sessions@openssh.com debug3: send packet: type 80 debug1: Entering interactive session. debug1: pledge: filesystem debug3: client_repledge: enter debug3: receive packet: type 80 debug1: client_input_global_request: rtype hostkeys-00@openssh.com want_reply 0 debug3: client_input_hostkeys: received RSA key SHA256:iw5lLSMAuL30RZCUe+w7sbdXV0DI/gJ+Jwua+mmBVGw debug3: client_input_hostkeys: received ECDSA key SHA256:XKwEiSX70VqFOFCxJ0sUl/Au0bbyOSUaaQz/9WSe8Gc debug3: client_input_hostkeys: received ED25519 key SHA256:+5SaMkJXG9yZrsYjXgxFfRZpvb6qjc/arFG2Nk4Vv48 debug1: client_input_hostkeys: searching /Users/lzwjava/.ssh/known_hosts for 138.201.174.0 / (none) debug3: hostkeys_foreach: reading file "/Users/lzwjava/.ssh/known_hosts"debug3: hostkeys_find: found ssh-ed25519 key at /Users/lzwjava/.ssh/known_hosts:164 debug3: hostkeys_find: found ssh-rsa key at /Users/lzwjava/.ssh/known_hosts:165 debug3: hostkeys_find: found ecdsa-sha2-nistp256 key at /Users/lzwjava/.ssh/known_hosts:166 debug1: client_input_hostkeys: searching /Users/lzwjava/.ssh/known_hosts2 for 138.201.174.0 / (none) debug1: client_input_hostkeys: hostkeys file /Users/lzwjava/.ssh/known_hosts2 does not exist debug3: client_input_hostkeys: 3 server keys: 0 new, 3 retained, 0 incomplete match. 0 to

remove debug1: client_input_hostkeys: no new or deprecated keys from server debug3: client_repledge: enter debug3: receive packet: type 4 debug1: Remote: /root/.ssh/authorized_keys:1: key options: agent-forwarding port-forwarding pty user-rc x11-forwarding debug3: receive packet: type 4 debug1: Remote: /root/.ssh/authorized_keys:1: key options: agent-forwarding port-forwarding pty user-rc x11-forwarding debug3: receive packet: type 91 debug2: channel_input_open_confirmation: channel 0: callback start debug2: client_session2_setup: id 0 debug2: channel 0: request pty-req confirm 1 debug3: send packet: type 98 debug1: Sending environment. debug3: Ignored env TERM_SESSION_ID debug3: Ignored env SSH_AUTH_SOCK debug1: channel 0: setting env LC_TERMINAL_VERSION = “3.4.19”debug2: channel 0: request env confirm 0 debug3: send packet: type 98 debug3: Ignored env COLORFGBG debug3: Ignored env ITERM_PROFILE debug3: Ignored env XPC_FLAGS debug3: Ignored env PWD debug3: Ignored env SHELL debug3: Ignored env __CFBundleIdentifier debug1: channel 0: setting env LC_CTYPE = “UTF-8”debug2: channel 0: request env confirm 0 debug3: send packet: type 98 debug3: Ignored env TERM_PROGRAM_VERSION debug3: Ignored env TERM_PROGRAM debug3: Ignored env PATH debug1: channel 0: setting env LC_TERMINAL = “iTerm2”debug2: channel 0: request env confirm 0 debug3: send packet: type 98 debug3: Ignored env COLORTERM debug3: Ignored env COMMAND_MODE debug3: Ignored env TERM debug3: Ignored env HOME debug3: Ignored env TMPDIR debug3: Ignored env USER debug3: Ignored env XPC_SERVICE_NAME debug3: Ignored env LOGNAME debug3: Ignored env ITERM_SESSION_ID debug3: Ignored env __CF_USER_TEXT_ENCODING debug3: Ignored env SHLVL debug3: Ignored