6. Pivot

> You can use the standard apt repos if you don’t need to do any modifications, e.g. bypassing Applocker or CLM.

```
sudo apt install ligolo-ng ligolo-ng-common-binaries -y
```

Basic tunnel

1. start `ligolo-proxy`

```
sudo ligolo-proxy -selfcert
```

1. Connect the agent
2. enter session and list network configuration

   ```
   #in ligolo-ng
   sessions
   ifconfig
   ```

3. set route
   1. 1 hop

      ```
      autoroute
      start
      ```

   2. 2 hops

AV evasion

1. Clone the repository

   ```
   git clone <https://github.com/nicocha30/ligolo-ng.git>
   ```

2. Edit the `ignoreCertificate` and `serverAddr` variables in the following file `/ligolo-ng/cmd/agent/main.go`
3. Compile the `agent.exe` using the following command

```
GOOS=windows go build -o agent.exe cmd/agent/main.go
```

4. Compile as `x64` and give the name `ApplockerBypassExternalBinary.exe` - Github Repo
5. Encode the file created above with certutil

```
certutil.exe -encode .\\ApplockerBypassExternalBinary.exe AppLockerBypassLigolo.txt
```

6. Rename the `agent.exe` to `ligolo-agent.exe`
7. Serve the files (`ligolo-agent.exe` and `AppLockerBypassLigolo.txt`
8. Upload the files to the target

Revision #1
Created 2026-01-08 18:54:43 UTC by Vlad Birgauanu
Updated 2026-01-08 18:56:12 UTC by Vlad Birgauanu