http://infinite.barrel-of-knowledge.info/cryptoparty/ (Surface web)

https://yhfitd2wvrz3aybh.onion/cryptoparty/ (Deep web)

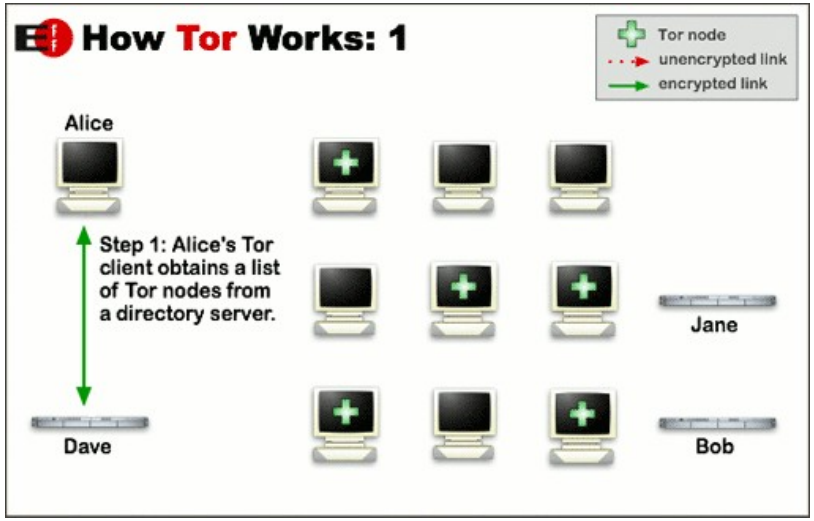
A Tor gatewayed platform for everyday use

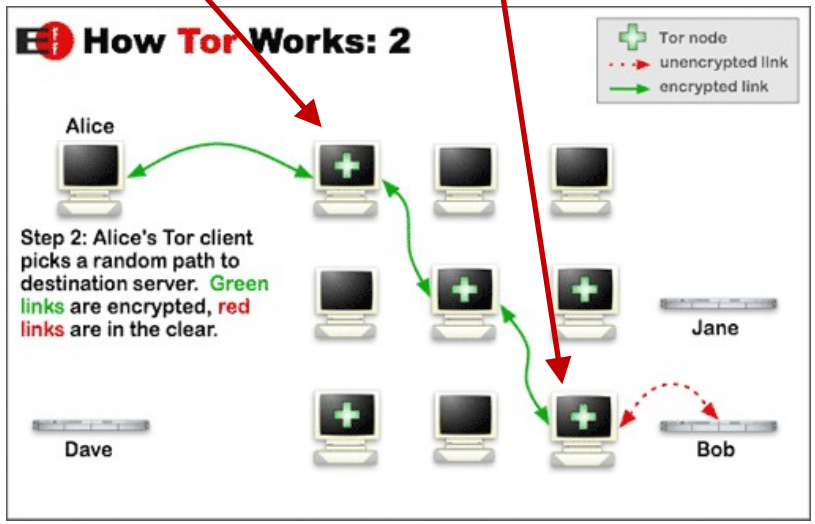
Using a virtual machine stack with it's own virtual LAN with all traffic routed into the Tor network

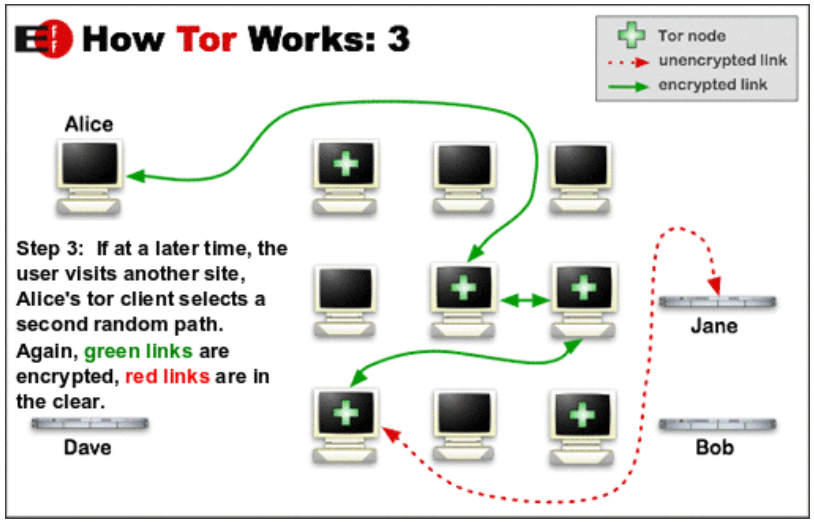
Per Foyer

per@foyer.se

What is Tor?







Previously short for The Onion Router

Clearnet = Internet

”Darknet” = Tor network

Surface web = Clearnet web

Deep web = Tor hidden service
(e.g. https://yhfitd2wvrz3aybh.onion/)

Why not simply...

...or Tor Browser?

Tails:

A USB stick based secure Tor gatewayed single entity platform.

- Very slow (access to data media)
- ”Amnesia” (by design)
- Not for everyday use
- Great for use ”on the road”

Qubes:

A virtualized platform with Tor traffic capabilities on top of a ”bare metal” hypervisor

- Demands high end machines with specific features
- Hungry for CPU and memory
- User communication awareness is crucial
- XEN server eliminates the need for a Host OS
- Tor traffic via two instances of Whonix (Linux) VMs

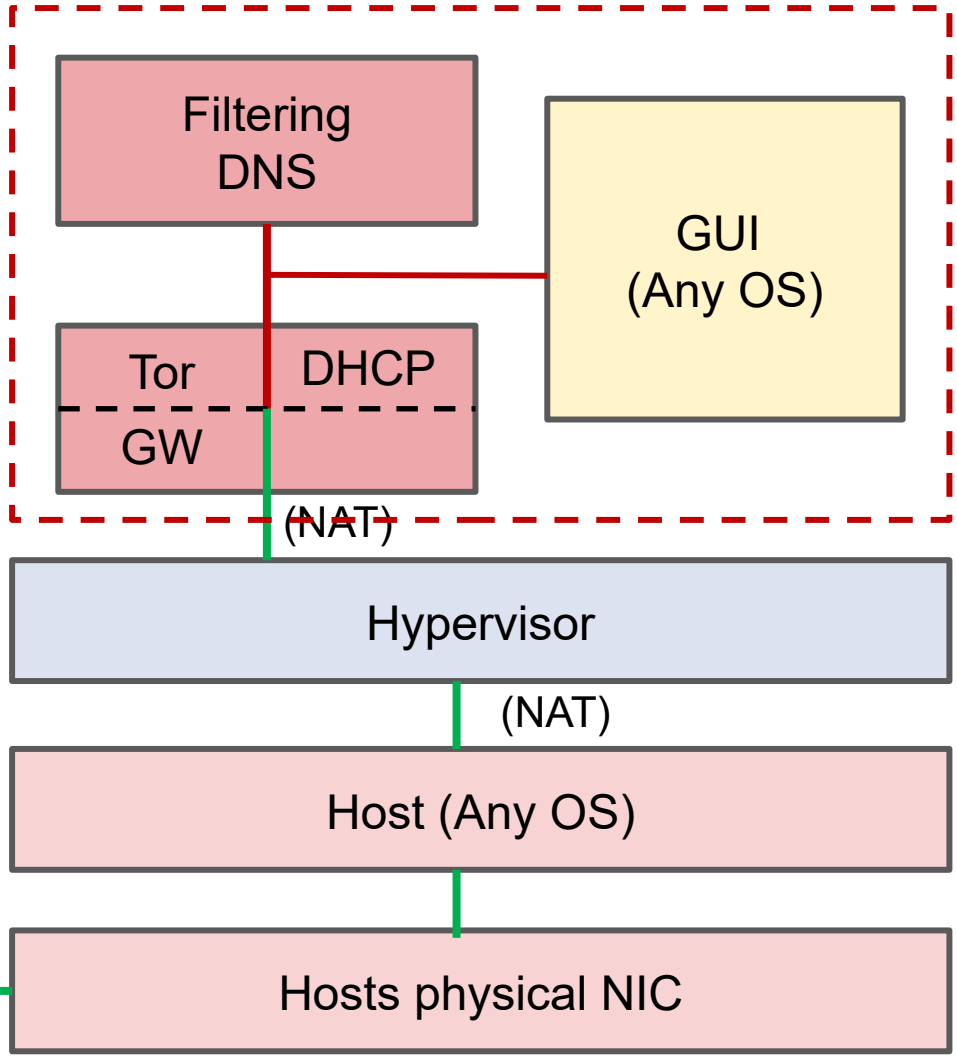
An easy to use VM based platform

Design goals:

- A nice GUI environment (OS) for daily use
- A filtering DNS to prevent requests to junk- and ad-domains etc (DNS sinkhole)
- A fully transparent Tor Gateway.
- The VMs should be able to run on any hypervisor and on any host OS:
  - ”bare bone”: VMware ESXi, XEN
    On host OS: VMware workstation, Virtual Box, qemu, …)
- No complicated configurations to get started.
- No need for user communication awareness

Architechture overview

VM LAN
IP range:
10.199.199/24

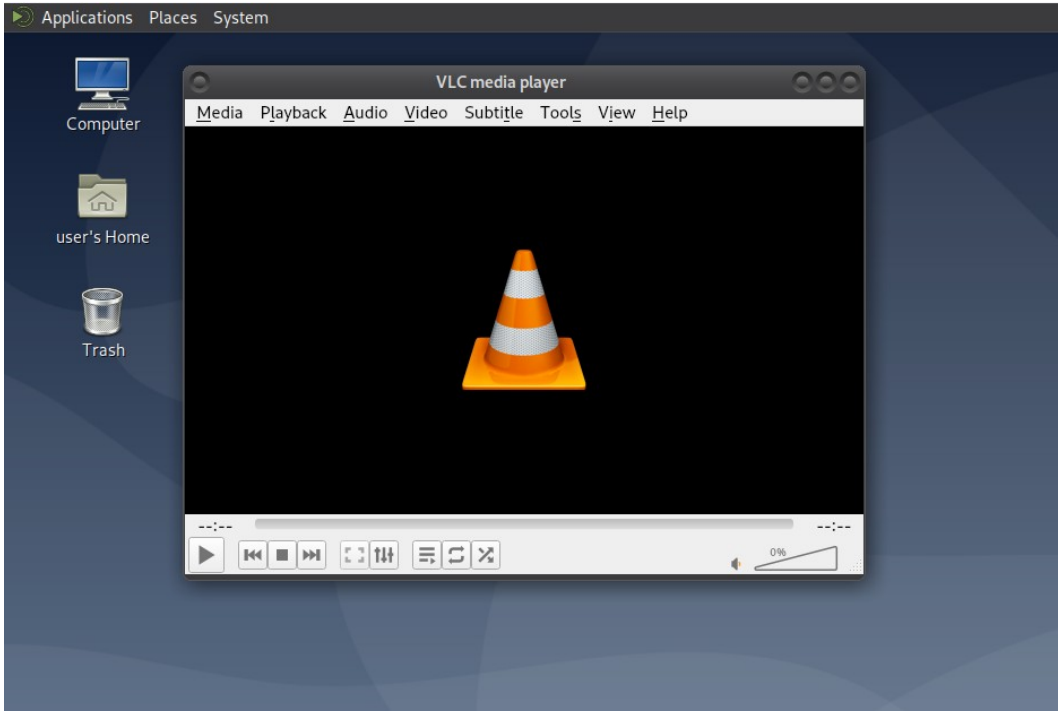


Tor tunnel through
”ClearNet”

Maximum host memory needed: Only 4 GB

GUI OS: The OS for everyday use

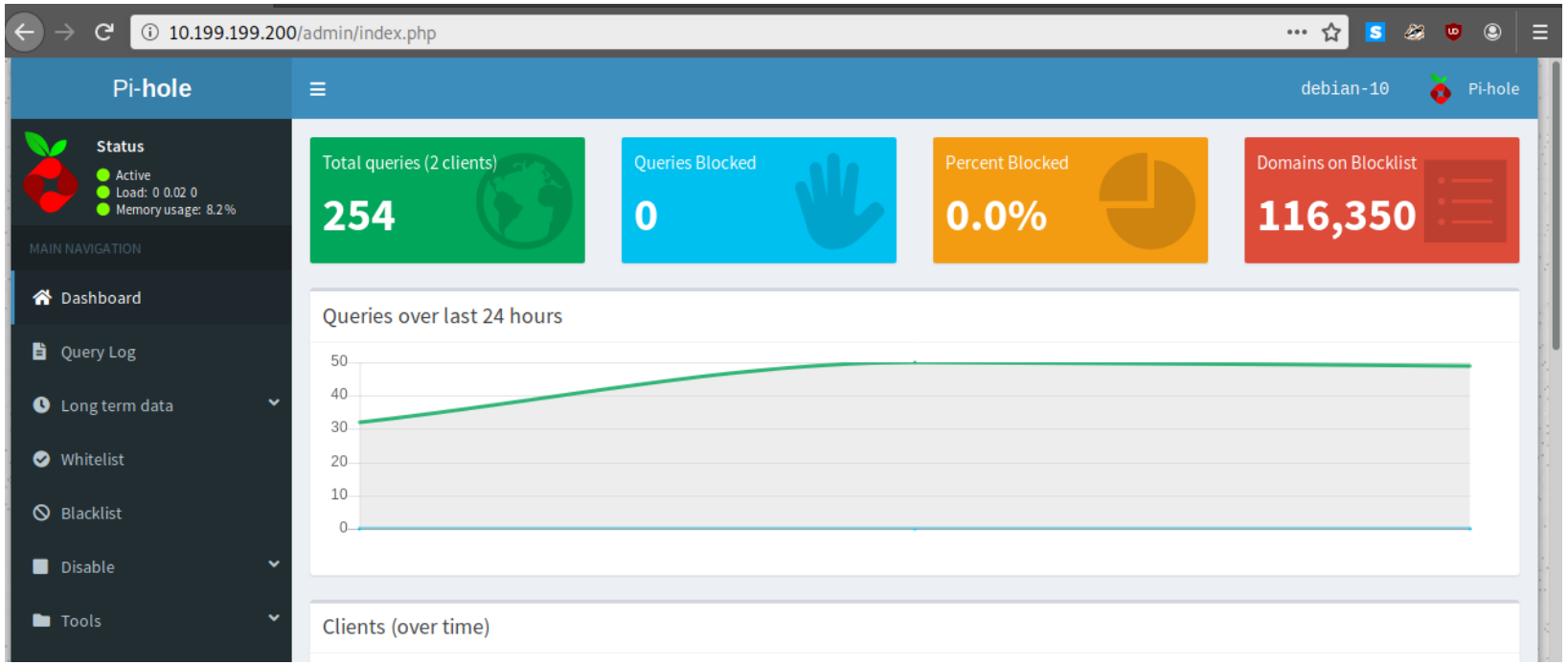
- Although possible to run any OS with GUI in the VM stack, choose an OS as free of unsolicited “phone homes” and telemetry as possible.
- Good choices are: Debian, OpenBSD, FreeBSD, NetBSD, ...
- A very bad choice is Windows 10 (“spyware” and a privacy nightmare)
- The GUI OS is installed like any ordinary installation. Nothing special to configure. IP via DHCP



The MATE desktop
(but you can use whichever desktop you like on Linux/BSD)

Filtering DNS: Pi-Hole

- Pi-hole (https://pi-hole.net) running ontop of a stock Debian 10.1.
- Acts both as an ordinary DNS and as a sinkhole
- More blocklists can be added at will.
- Fixed IP in the VM LAN: 10.199.199.200
- Upstream DNS: 10.199.199.1 (Tor Gateway)



The transparent Tor Gateway

- Running OpenBSD/i386 with two NICs (VM LAN / Host OS)
- DHCP server for the VM LAN (IP range 10.199.199.190 – 199)
- All traffic from and to the VM LAN is routed through the Tor server (localhost) via the hypervisor (NATed) to ”ClearNet”
- The Tor GW changes Tor entry nodes at regular intervals

```
root@torgw.local>netstat -n
Active Internet connections
Proto   Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp          0      0  10.0.2.15.36913        89.22.96.90.443        ESTABLISHED
tcp          0      0  10.0.2.15.40632        45.35.192.34.9001      ESTABLISHED
tcp          0      0  10.0.2.15.14662        144.76.91.184.9001     ESTABLISHED
Active UNIX domain sockets
Address    Type   Recv-Q Send-Q       Inode       Conn       Refs    Nextref Addr
0xd3356780 stream      0      0         0x0 0xd3356800        0x0        0x0
0xd37fa800 stream      0      0 0xd30a4d94        0x0        0x0        0x0 /var
/run/cron.sock
0xd37fa200 stream      0      0         0x0 0xd37fa180        0x0        0x0
0xd37fa180 stream      0      0         0x0 0xd37fa200        0x0        0x0
0xd3356b80 stream      0      0         0x0 0xd3356b00        0x0        0x0
0xd3356b00 stream      0      0         0x0 0xd3356b80        0x0        0x0
0xd3356800 stream      0      0         0x0 0xd3356780        0x0        0x0
0xd3356e00 dgram       0      0         0x0 0xd3356e80 0xd3356e80        0x0
0xd3356e80 dgram       0      0         0x0 0xd3356e00 0xd3356e00        0x0
0xd3356d80 dgram       0      0 0xd2fac7c4        0x0        0x0        0x0 /dev
/log
root@torgw.local>uname -a
OpenBSD torgw.local 6.5 GENERIC#3 i386
root@torgw.local>
```

Time for a Demo!

- All virtual machines (Desktop, DNS sinkhole and Tor GW) are available as easy to install images with no configuration needed:
- http://infinite.barrel-of-knowledge.info/cryptoparty/

…or if you like:

- https://yhfitd2wvrz3aybh.onion/cryptoparty/