

Navegación segura

SEGURA NO : Cómo navegar dejando menos rastro.

¡ No hay nada 100% seguro !

Itinerario colectivo de autodefensa digital

- 14 de Febrero : Introducción a GNU/Linux y uso básico de Freeptto
- 28 de Febrero : Navegación segura: TOR , certificados, VPN
- 14 de Marzo : Correo seguro y chat seguro: GPG, SSL , servidores autogestionados
- 28 de Marzo : Publicación de contenidos online : streaming de video y audio, publicación de contenidos

Internet

- Muchas redes unidas
- Las redes 'hablan' para comunicarse
- Pertenece a estados y empresas
- Ofrecen servicios: web, tv, teléfono,...
- No es gratis, tiene coste y tú lo pagas
- Video datacenter Facebook 2:27

Nos ponemos en contexto

- Sociedad interconectada con tecnología
- Generamos datos
- Para empresas: consumidores
- Para estado: posibles delincuentes
- Tecnología pertenece a empresas
- Control = Beneficio

Privacidad

- La privacidad y la intimidad no se respeta
- Evidencias de control y seguimiento por gobiernos y empresas (NSA, PRISM)
- ... y no pasa nada de nada

Hay que defenderse

Caso teórico del taller

- Denuncia ciudadana anónima por agresiones racistas
- Entorno conflictivo
- Miedo a represalias
- Es necesario anonimato

FREEPTO



Freepto en 1 minuto



- Sistema Operativo GNU/Linux
- Arranca desde USB
- Almacenamiento cifrado
- Herramientas de privacidad y anonimato
- Es Software Libre

Arranca tu Freepto



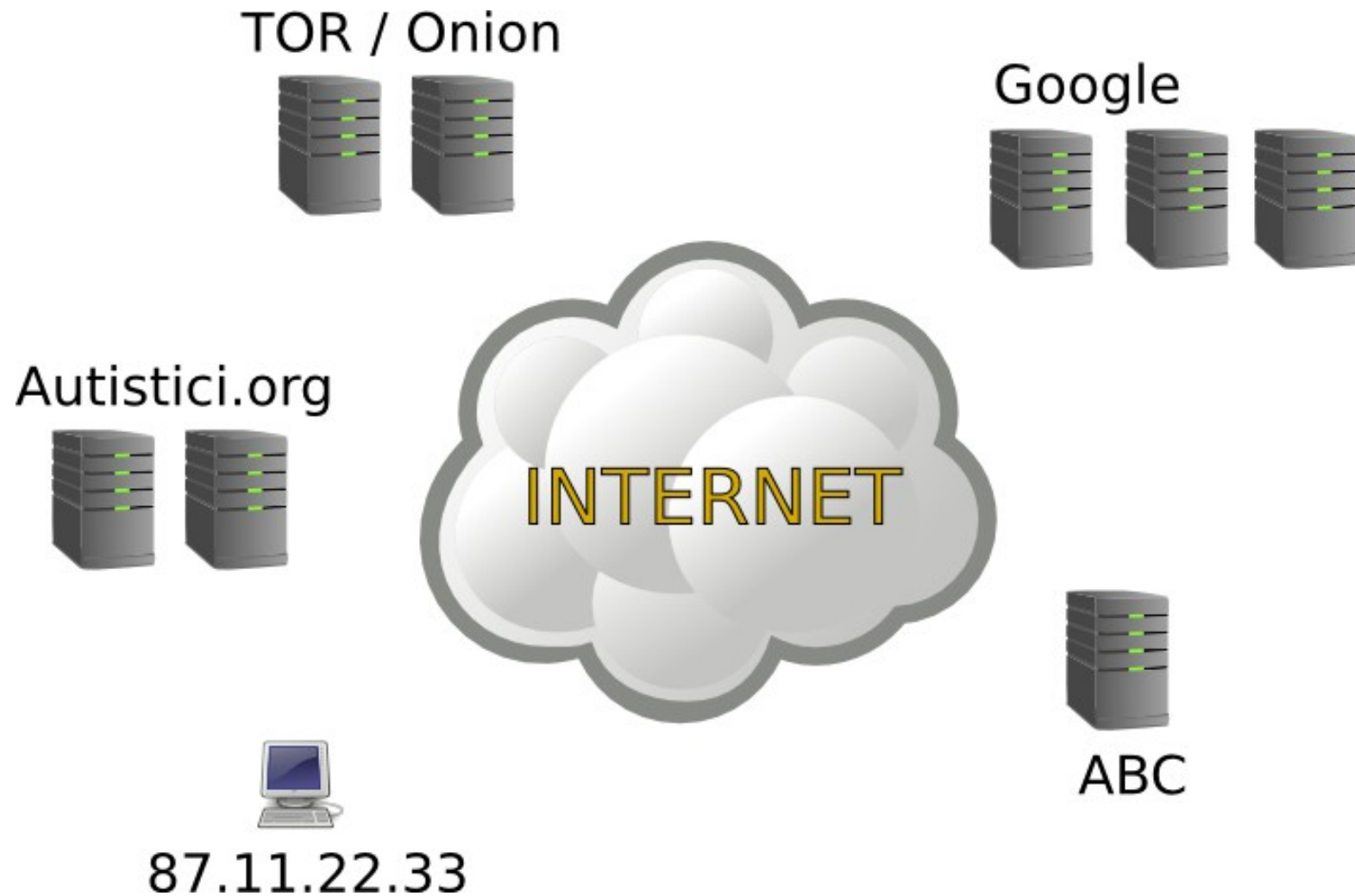
- Arranca Freepto y configura la conexión a la red
- Ver IP Local y chequear la ip en un servicio externo

Identificación: No somos anónimos

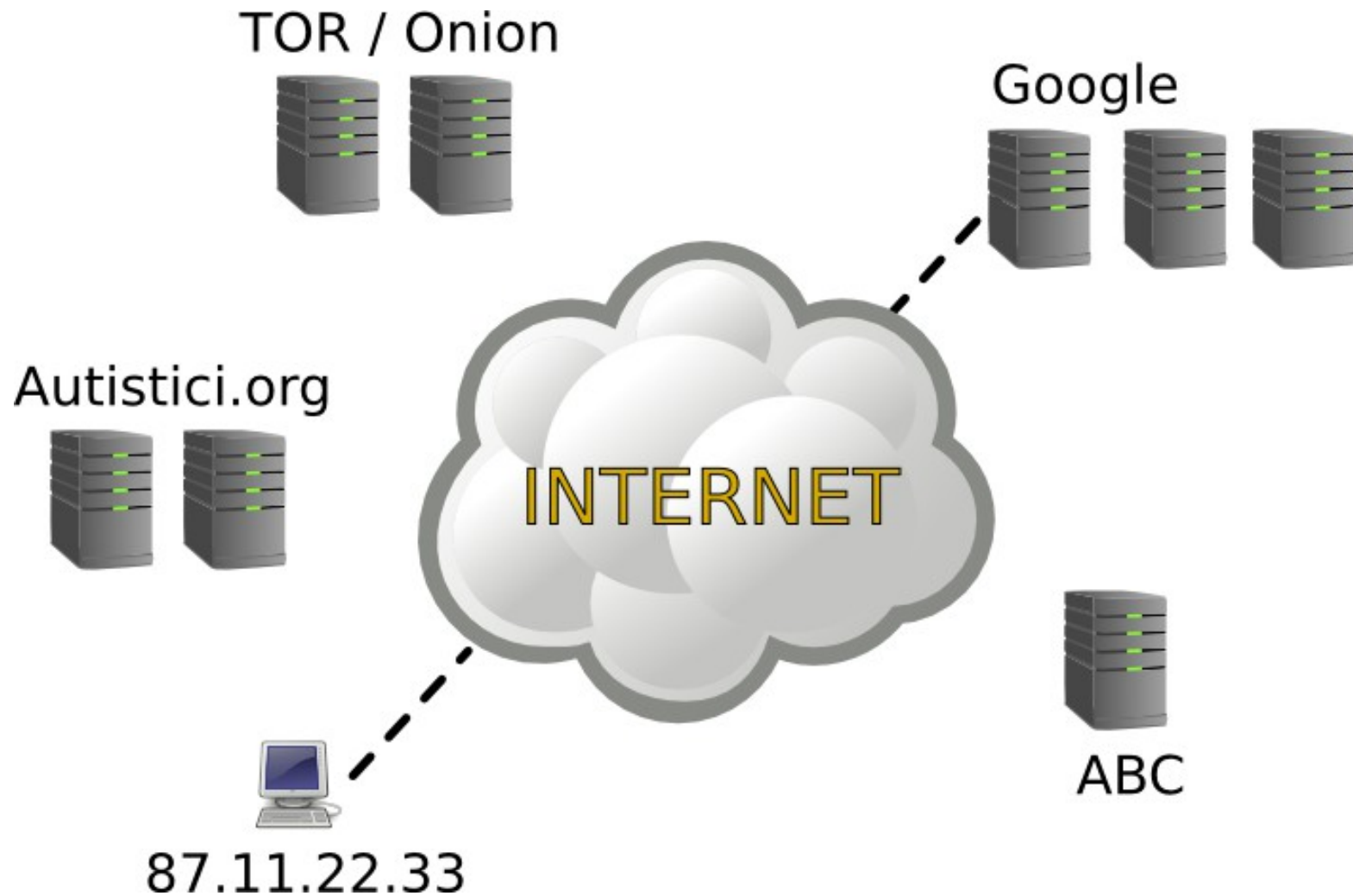
Identificación

- Orden judicial
- Solicitud de registros a la empresa
- Solicitud de registros al operador
- Identificación de la persona

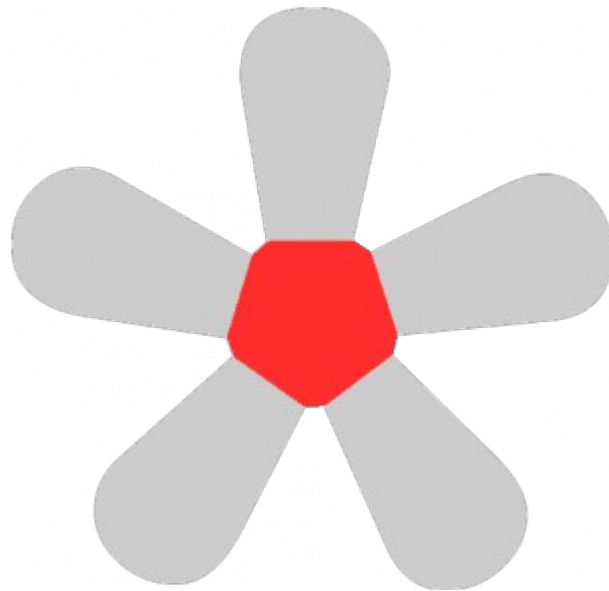
Redes y routers



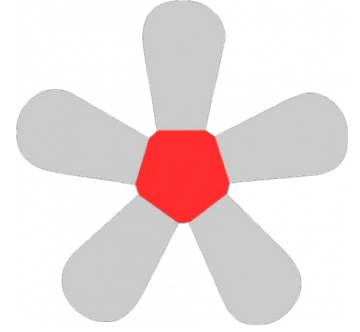
Redes y routers



AUTISTICI / INVENTATI
SERVICIO VPN

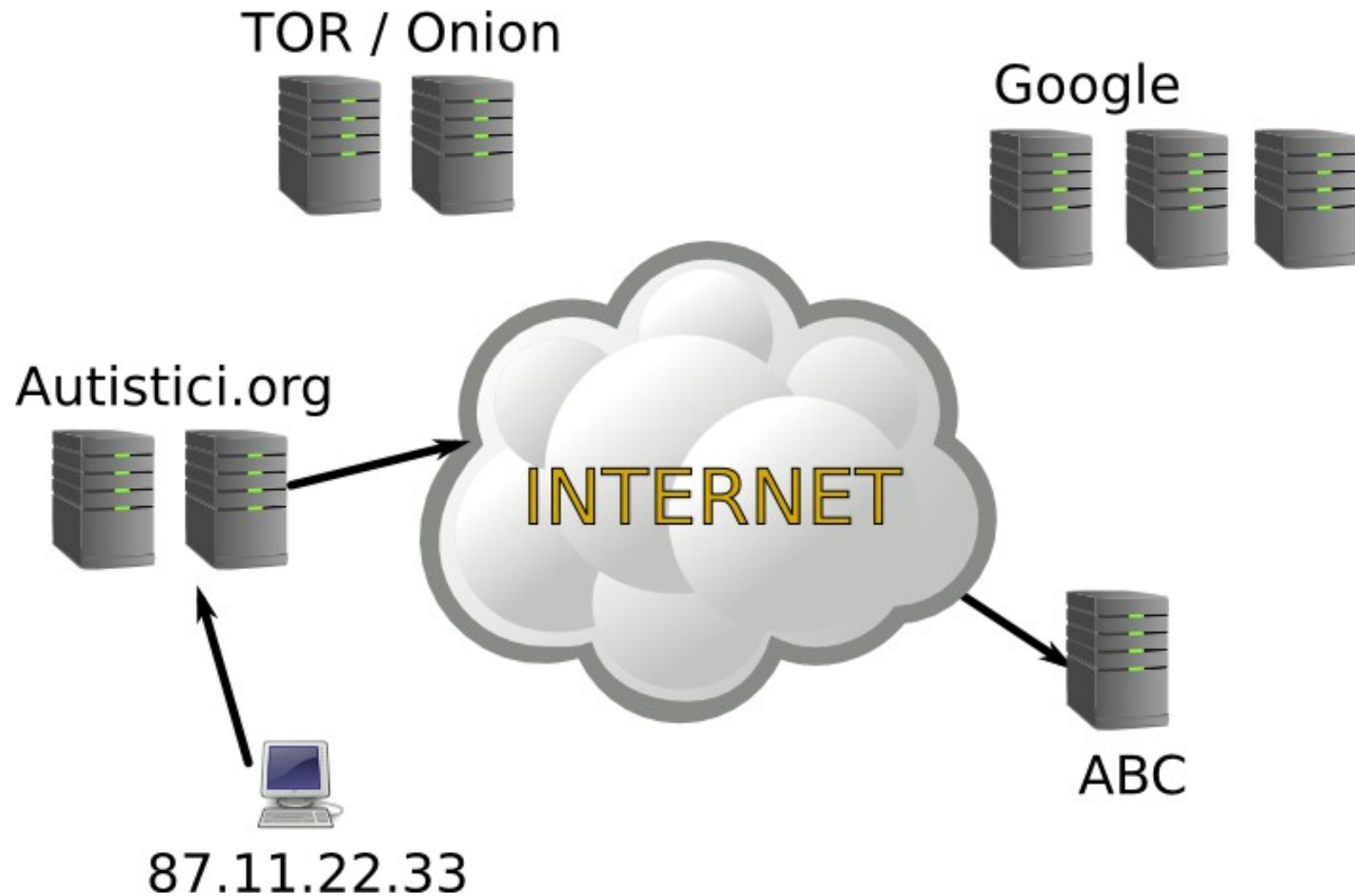
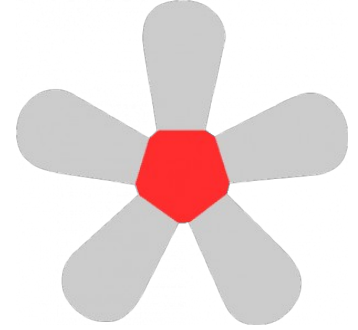


A/I VPN

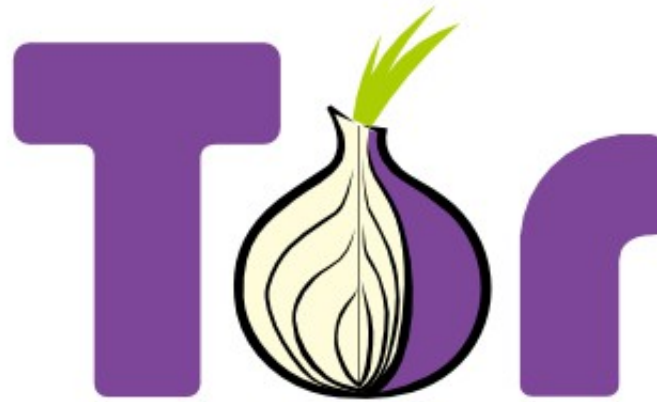


- Necesitas cuenta en autistici
- Genera un certificado para 10 días
- Configurararlo en Freepto

A/I VPN



TOR / Onion



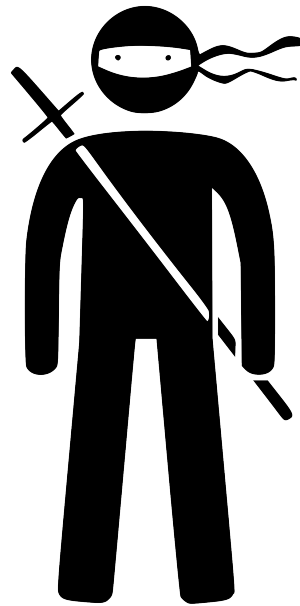
TorProject.org

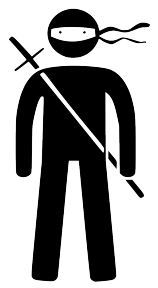
- Individuos ponen servidores con TOR
- La información se transmite cifrada
- No se sabe por donde va a ser emitida
- Por ahora parece seguro
- Se usa un plugin en firefox
- Paquete TORBrowserBundle
- Muy sencillo de usar

Esto no sirve de mucho

- Esto no nos proporciona anonimato
- Tenemos que usar protocolos seguros HTTPS
- Usar otra identidad
- Evitar javascripts, trackers, etc...
- Sentido común

Sé un ninja





HTTPS y Certificados

- Usar HTTPs evita que capturen las comunicaciones (tampoco es seguro)
- WARNING: certificado no válido



Secure Connection Failed

login.new.facebook.com uses an invalid security certificate.

The certificate is only valid for www.facebook.com

(Error code: ssl_error_bad_cert_domain)

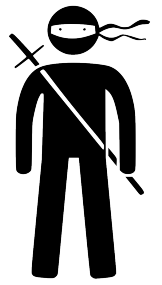
- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

[Or you can add an exception...](#)



- Algunos scripts javascript son maliciosos
- Empresas trackean usuarios con js





- No usar tus datos personales
- Usa cuentas de 'usar y tirar'
- Usa el sentido común.

Resumen

- Ocultar nuestra IP
- No dejar rastros de nuestra identidad
- No ignorar alertas
- Usar Cifrado