

Navegación Anónima ?



Navegación

ReD

Cofundador de Hacklabs
Apasionado de la tecnología
Defensor de la privacidad

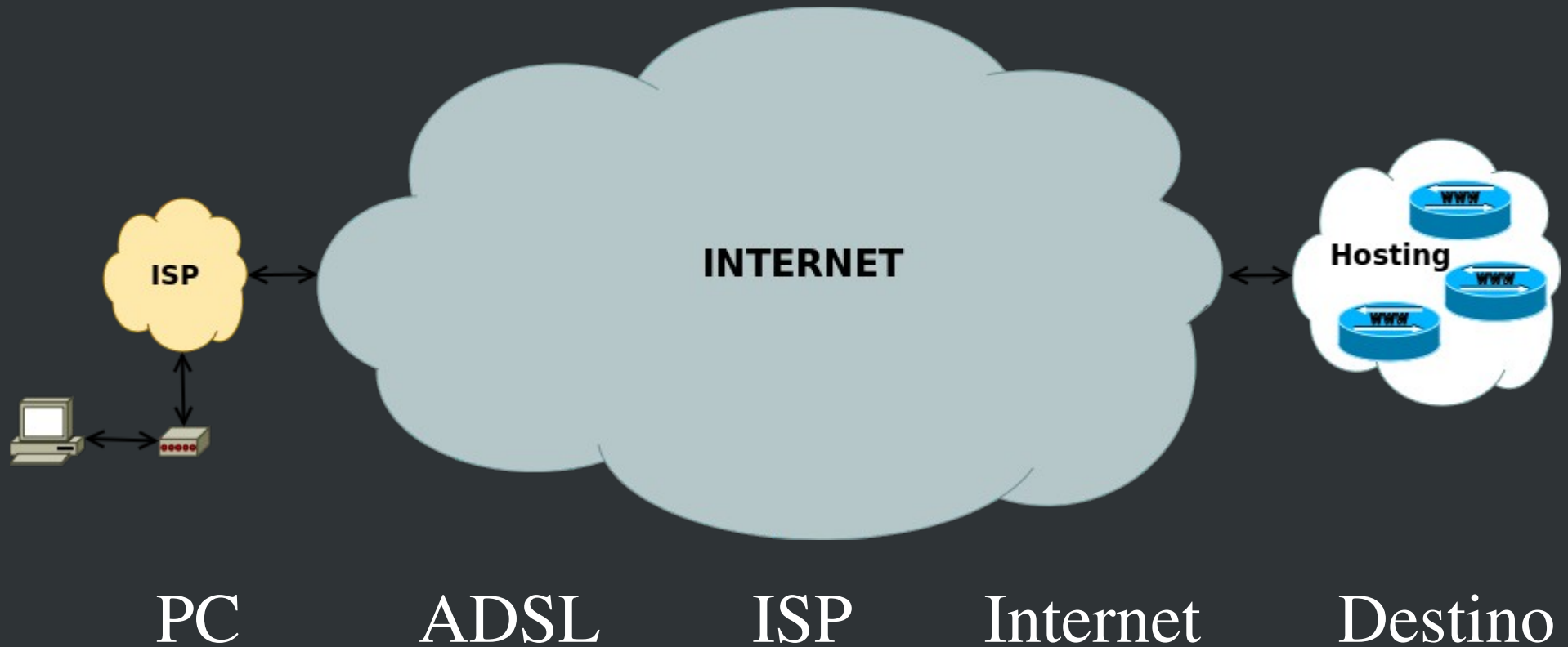


Navegación

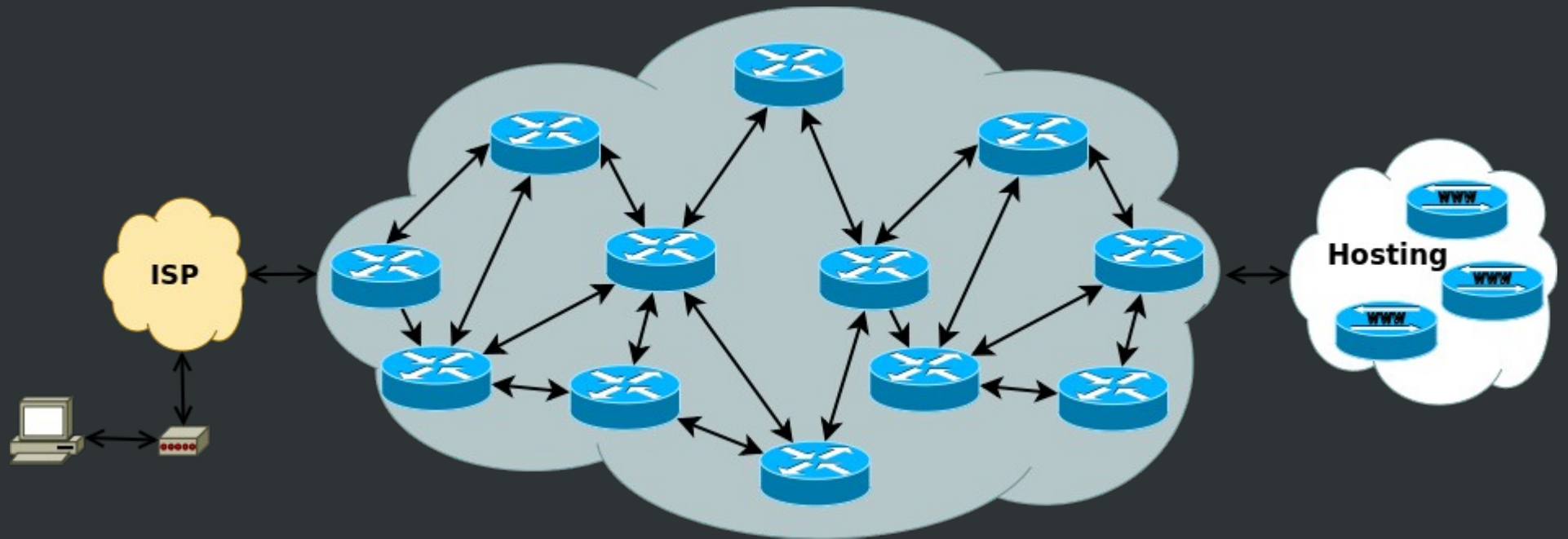
- Navegación
 - Mail
 - Voz IP
 - Mensajería instantánea
 - Etc.
- Navegación tradicional
- Navegación tradicional cifrada



Navegación tradicional

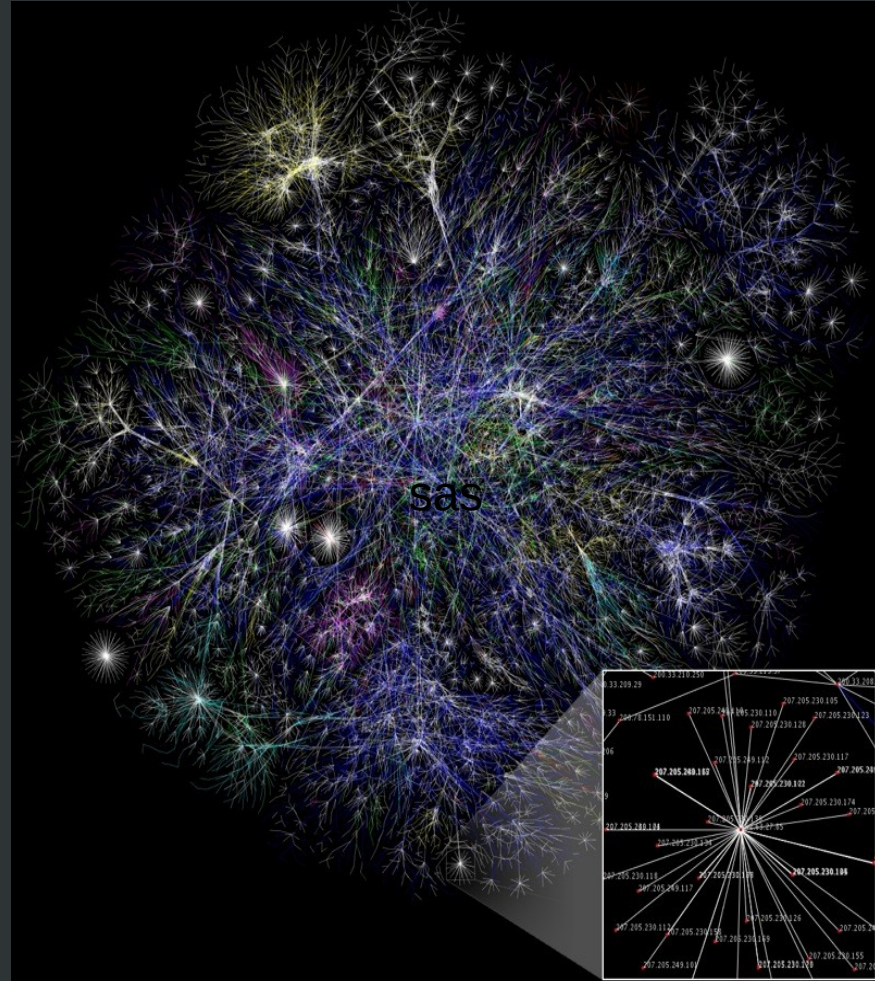


Navegación tradicional

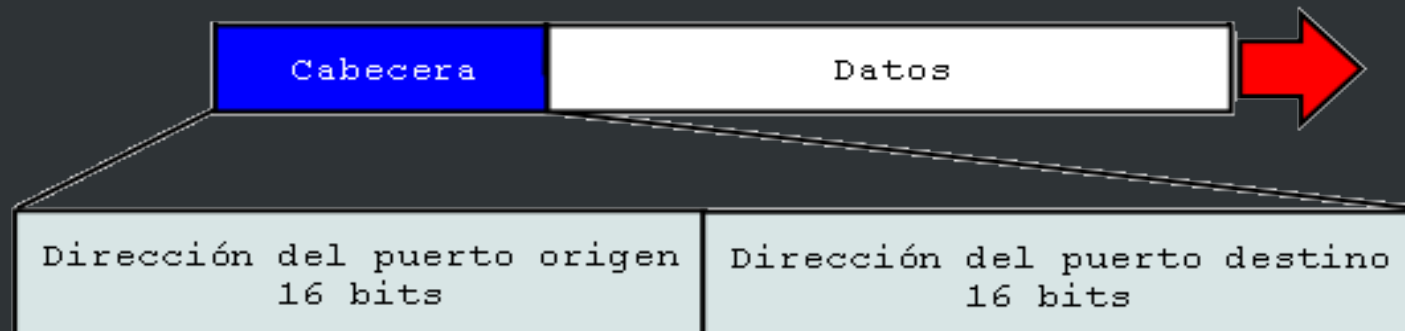
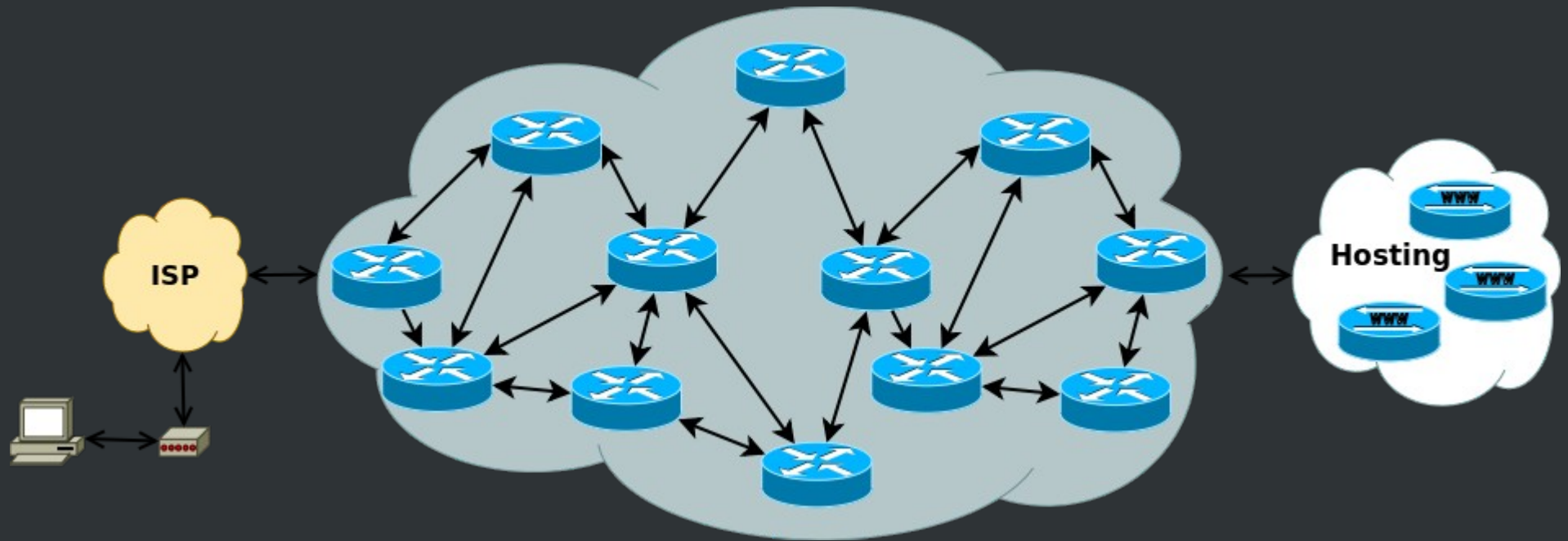


Navegación tradicional

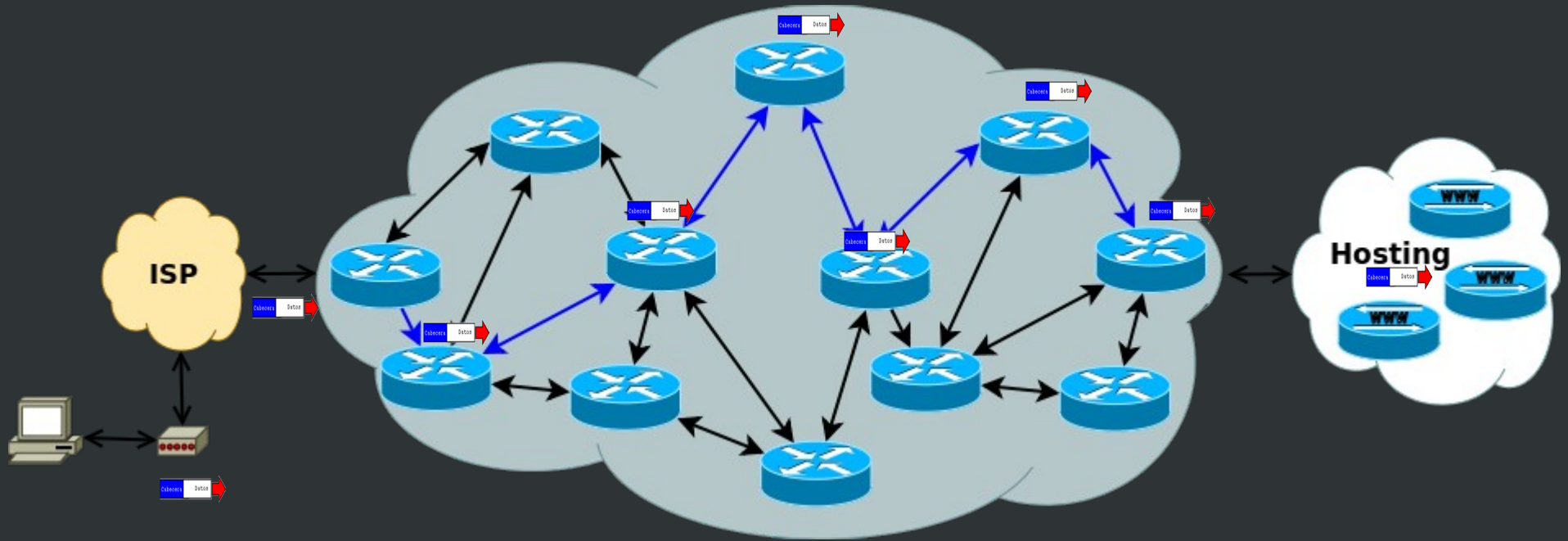
- Representación 30%
2005
- Internet
 - Países
 - Empresas



Navegación tradicional

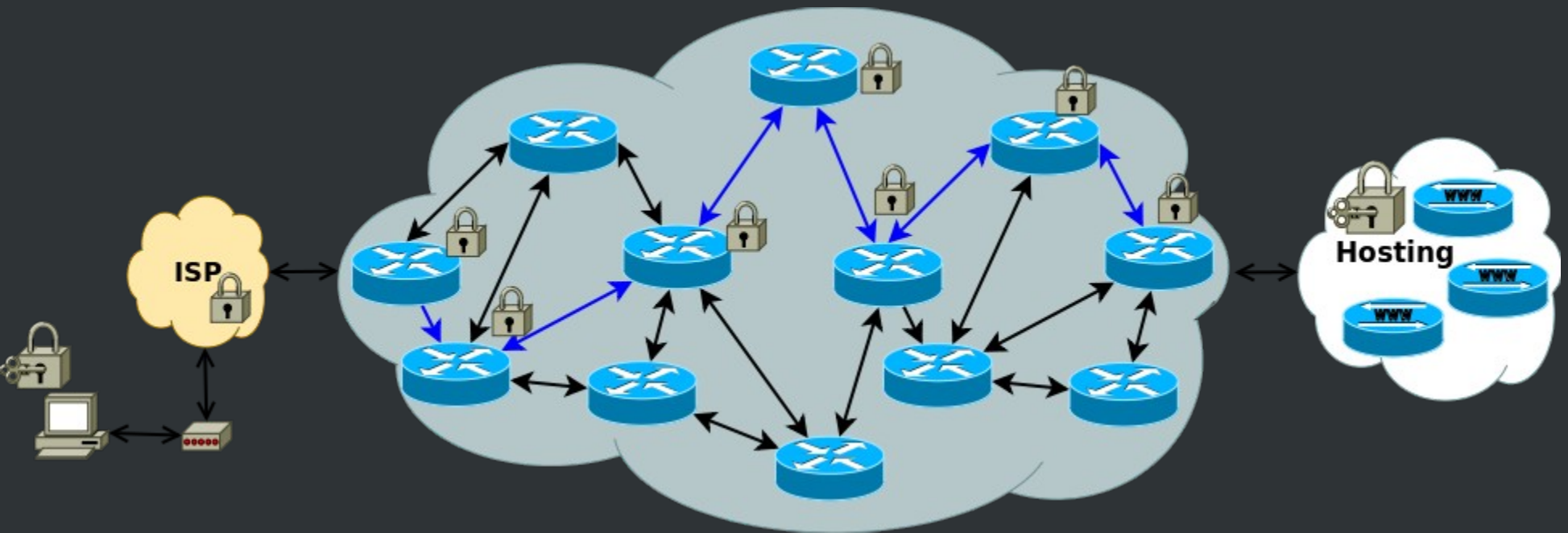


Navegación tradicional



Navegación tradicional

Cifrada

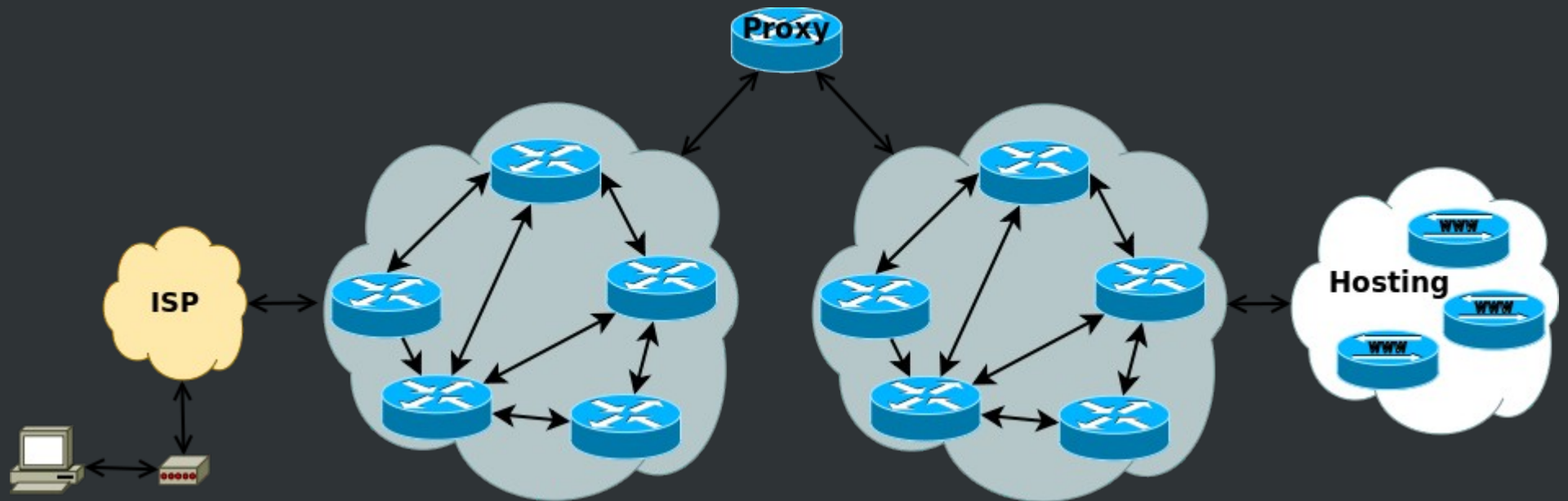


Proxys

- Realiza peticiones por nosotros
- La mayoría son transparentes
- La mayoría no están cifrados



Proxys



Proxys

Problemas

- Sitios con autenticación
- Acceso a información sensible
- Creación o compartición de contenidos
- Bancos, compra Online



Proxys

- Varios tipos de Proxys:
 - Proxy web
 - Proxys HTTP
 - Proxys socks



Proxys web

- Acceso a través de web
- Usan parámetros URL
- Lentos
- Con publicidad



Proxys web

- Seguros

- <https://www.ninjacloak.com/>
- <https://hidemyass.com>
- **SabzProxy** ("proxy verde")
<http://www.sabzproxy.com/>

- NO seguros

- <http://www.phpmyproxy.com/>
- <http://anonymouse.org/>



Proxys http/https

- Trabaja a un nivel más bajo
- Configurar navegador
- Servidor proxy (dirección y puerto)



Proxys web - Programas

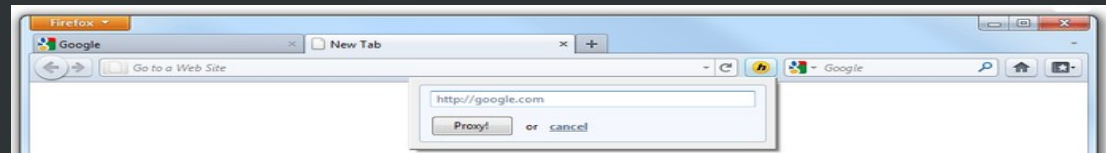
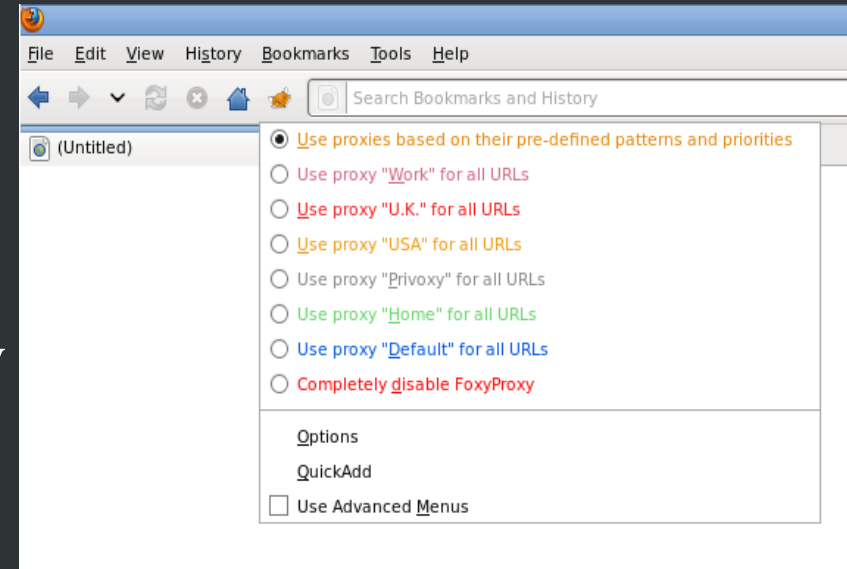
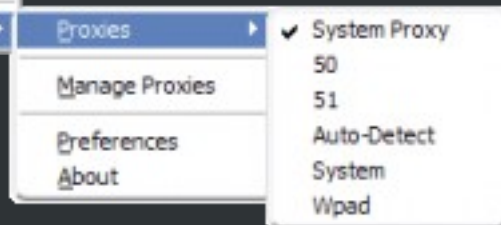
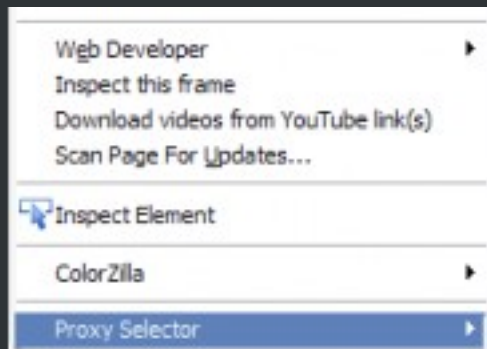
- Psiphon
 - Código abierto (GPL)
 - Distribuido
 - Nodos abiertos
 - Nodos con registro (invitación)

<http://www.psiphon.ca>



Proxys

- Extensiones
 - FoxyProxy Standard
 - Hide My Ass Web Proxy
 - Proxy Selector



Proxys socks

- Se puede conectar usando otros servicios
 - Mail
 - IRC
 -
- Tipos
 - Socks 4
 - Socks 4a
 - Socks 5 (más opciones de autenticación)



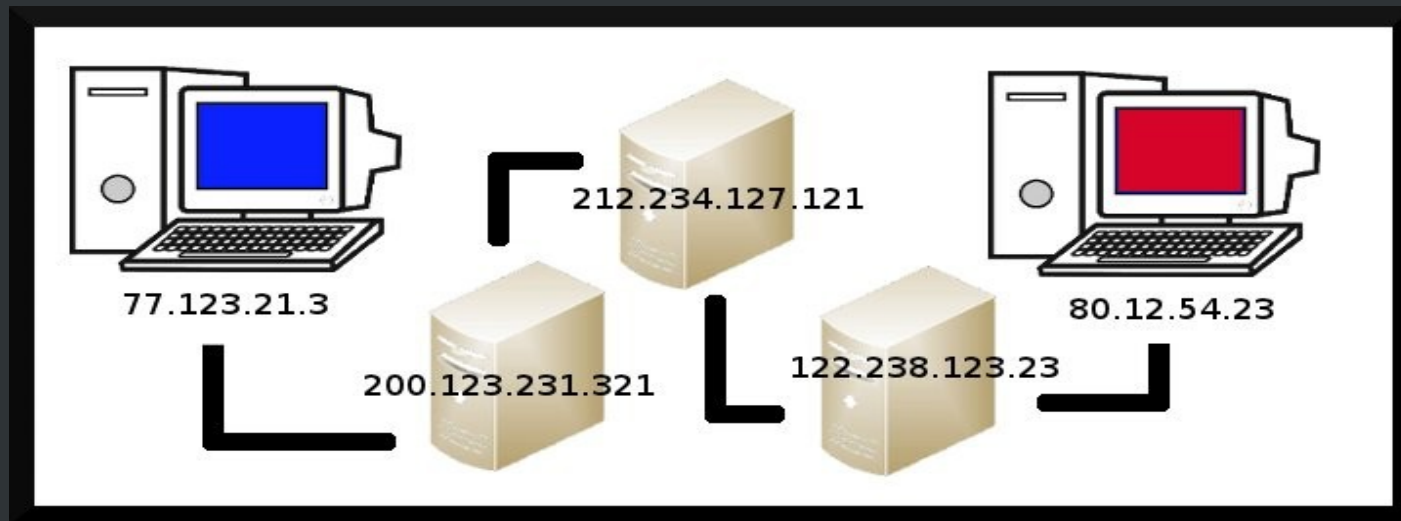
Proxys Herramientas

- Proxychains:
 - Puedes usar app sin configuración proxy
 - configuración de multiproxy
 - */etc/proxychains.conf*
 - *Descomentar “#dynamic_chain”*
 - *Añadir listado de proxy*
socks5 81.91.195.16 3128
socks5 234.125.139.116 3128
socks5 186.91.20.179 8080



Proxys Herramientas

- Proxychains (muliproxy)



Listado de Proxys

- <http://www.samair.ru/>
- <http://www.proxy-list.org/>
- <http://www.xroxy.com/>
- <http://www.workingproxies.org/>
- <http://www.proxy4free.com/>
- <http://www.proxylist.net>
- <http://www.atproxy.net>

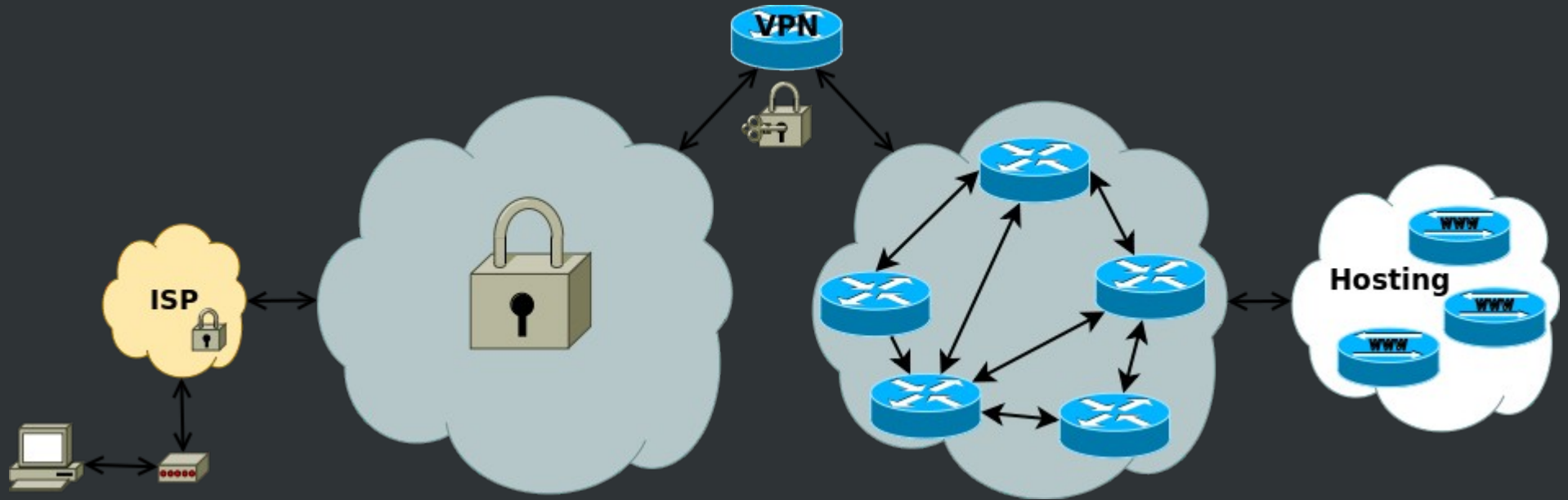


VPN

- Red privada virtual
- Une redes de forma cifrada
- Nueva IP pública
- Nueva interfaz de red
- Destino solo conoce la nueva IP
- ISP no conoce nuestro tráfico



VPN



VPN Disponibilidad

- VPN gratuitas
- VPN de pago
- Nuestra propia VPN



VPN Gratuitas

- Velocidad limitada
- Puntos de salida limitados
- Publicidad
- Instalación de soft
- Otros tipos de restricciones



VPN de pago

- Mayor ancho de banda
- Disponibilidad más punto de salida
- Elección de punto de salida
- Configuración
 - OpenVPN
 - PPTP
 - L2TP



VPN Nuestra

- Requiere mayor conocimiento técnico
- Contratar un servidor
- Montar servidor VPN

Ej. Open VPN server



VPN

- Más usados:

<http://www.anchorfree.com/>

<http://cyberghostvpn.com/es/>

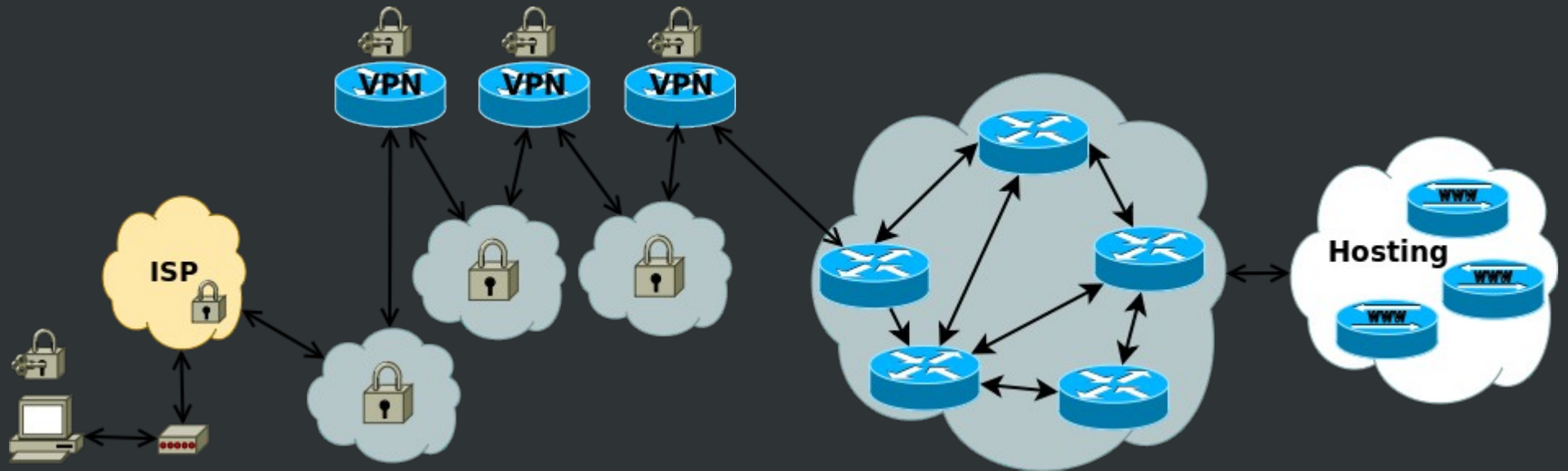
<http://www.securitykiss.com/>

- Listado de VPN gratuitas y de pago

<http://en.cship.org/wiki/VPN>



VPN Vuelta de tuerca



Remailers

- Datos enviados en un email:
 - Nombre de la máquina
 - IP de la máquina
 - Hora de envío
- 1º Remailer **Johan Helsingius** 1993
Para discutir de política y religión (USENET)



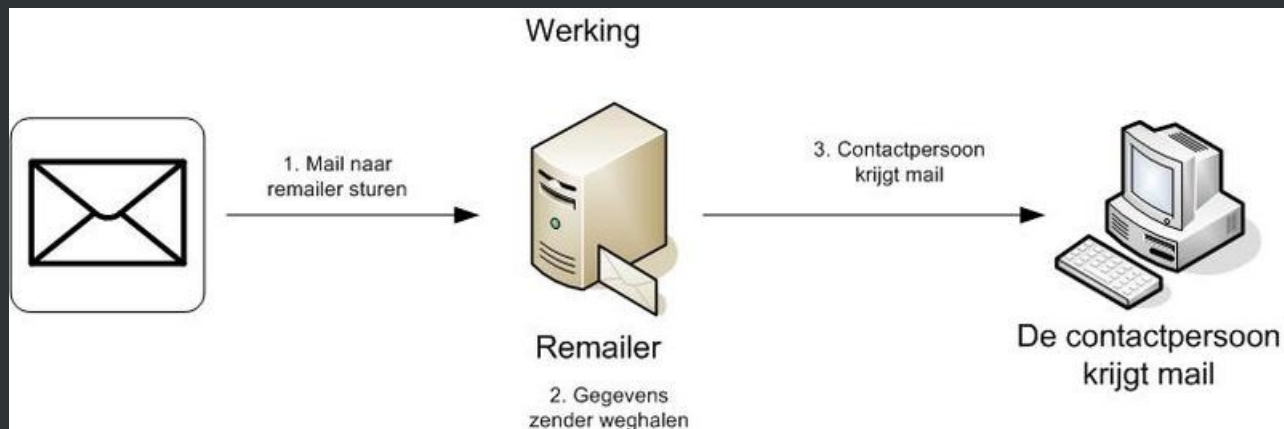
Remailers

- QUITAN cabeceras y nombres originales
- Reenvían el mail al destinatario original
- Reenvío en tiempo aleatorio
- Se pueden concatenar



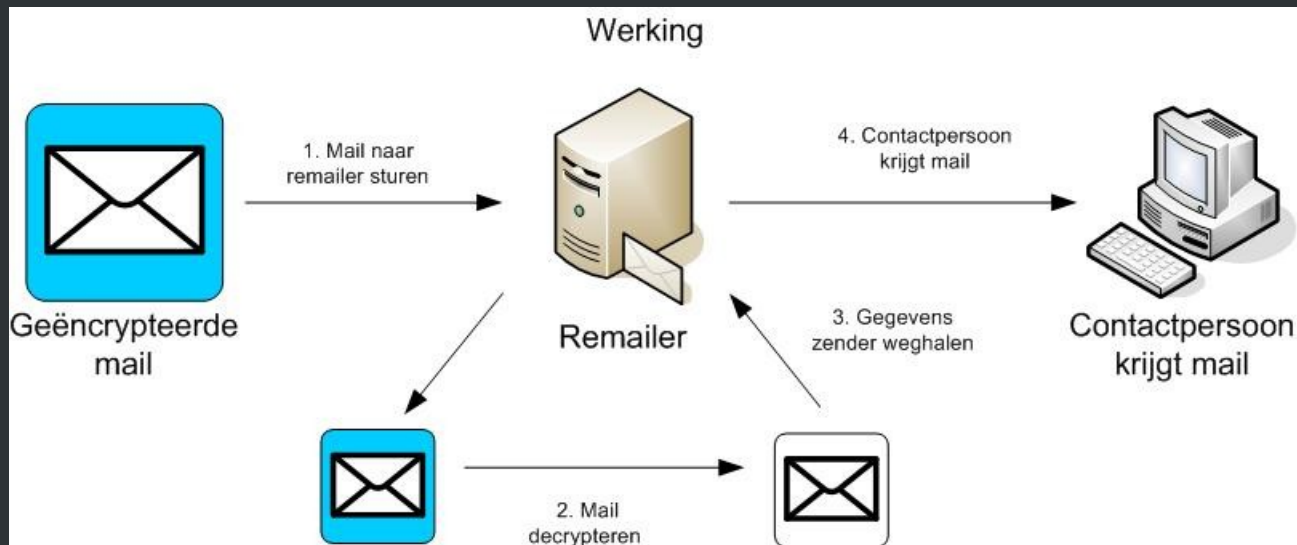
Remailers Tipo 1

- Tipo 1.1
 - Pseudo anónimos
 - Tienes 2º cuenta
 - Puedes recibir mails
- Tipo 1.2 (cypherpunk)



Remailers Tipo 2

- Tipo 2 (mixmaster)
 - Usan software en el lado cliente
 - Cifran y anonimiza



Remailers recursos

- Tipo 1.2

<https://www.cotse.net/cgi-bin/mixmail.cgi>

<https://www.awxcnx.de/mm-anon-email.htm>

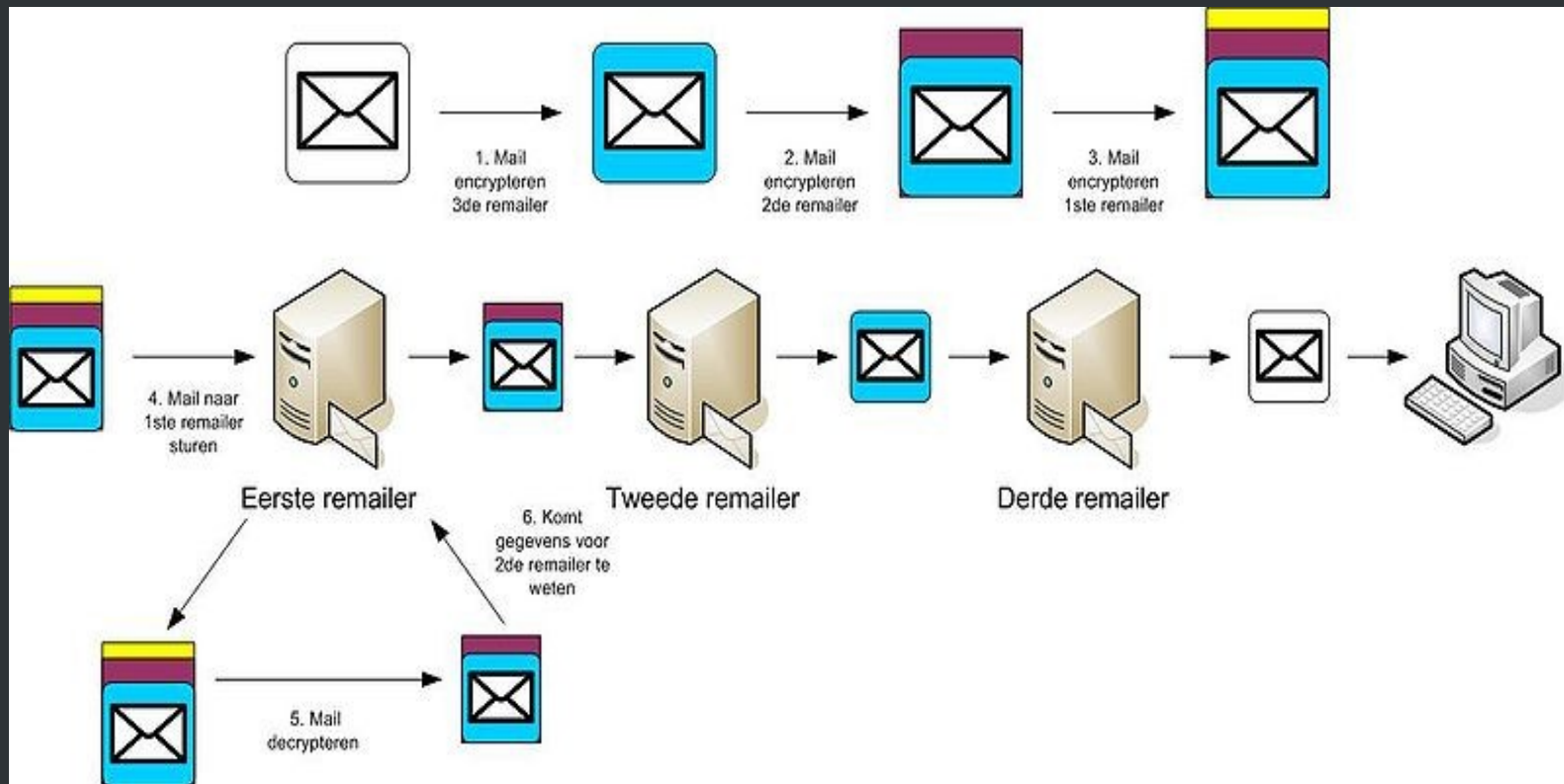
- Tipo 2

Prívate Idaho (<http://www.itech.net.au/pi/>)

- Echolot (<http://www.palfrader.org/echolot/>)
detecta estado y viabilidad de remailers



Remailers vuelta de tuerca



Pagos anónimos

- UKash
- Paysavecard
- Tarjetas de casino
- Bitcoin



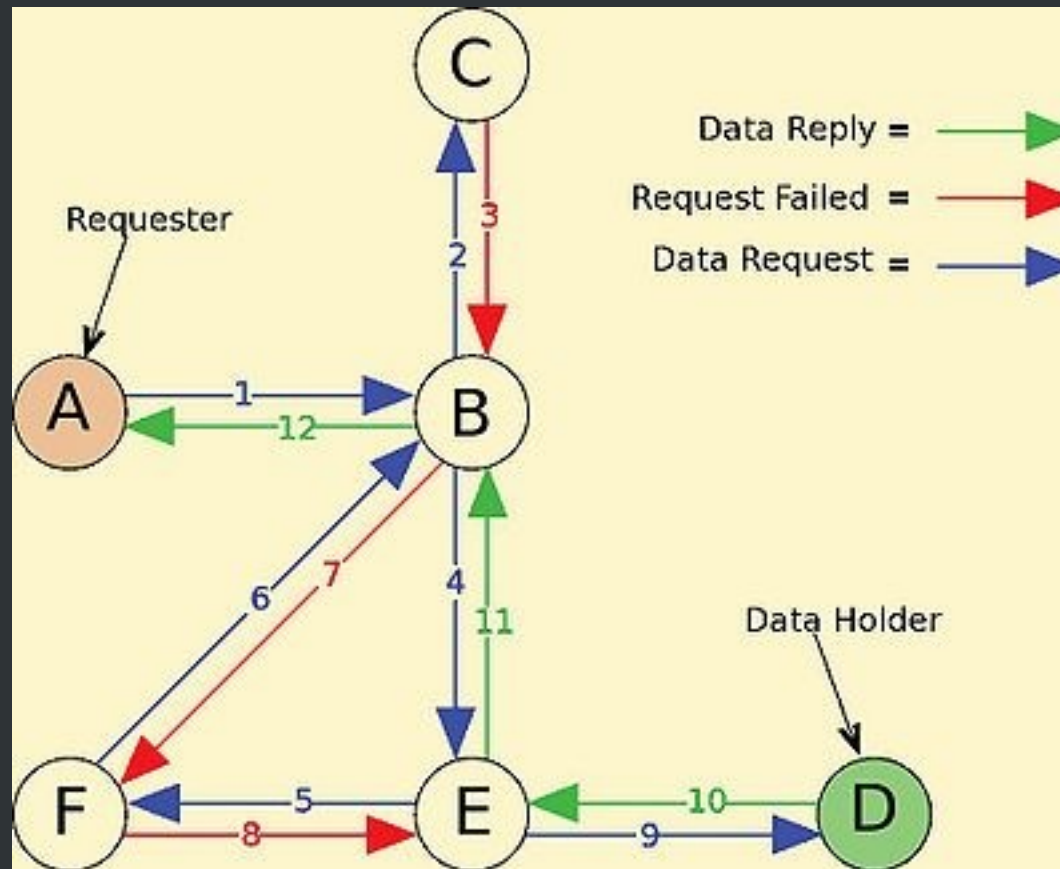
Freenet 0.75



- Red P2P descentraliza
- Cliente desarrollado en java (Java 6 jdk)
- Uso de ancho de banda y disco duro del usuario
- Datos cifrados (Data Store)
- Licencia GPL
- Multiplataforma
- Datos persistentes mientras se siga buscando



Freenet 0.75



Freenet Data Store



- Datos cifrados no accesibles por usuario
- Comprimido
- Ficheros 32KB
- Ficheros hasheados



Freenet Data Store



Claves de clasificación

- CHK (Content Hash Key)
Ficheros estáticos, hash
- SSK (Signed Subspace Key)
Ficheros que cambian, no repudio
- USK (Updatable Subspace Key)
Wrapper de SSK
- KSK (Keyword Subspace Keys)



Freenet 0.75



- Freesites; páginas de la red Freenet
- Página de ejemplo
- <http://localhost:8888/USK@0nnpnMrqZNKRCRoGojZV93UNHCMN-6UU3rRSAmP6jNLE,~BG-edFtdCC1cSH4O3BWdeIYa8Sw5DfyrSV-TKdO5ec,AQACAAE/fms/103/>
- Acceso configuración por web

NOTA: URI (Uniform Resource Identifier)



Freenet Darknet



- Darknet
 - Necesario 5 fiends
 - La "amistad" tiene que ser bidireccional
 - Todos los accesos Freenet son por friends
 - El tráfico entre "amigos" es cifrado
- <http://127.0.0.1:8888/friends/>



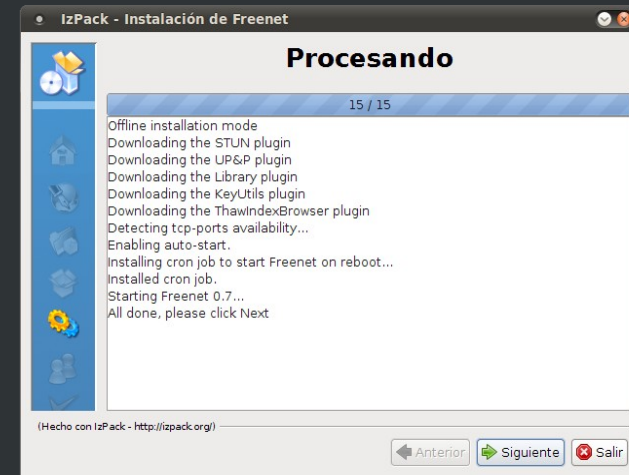
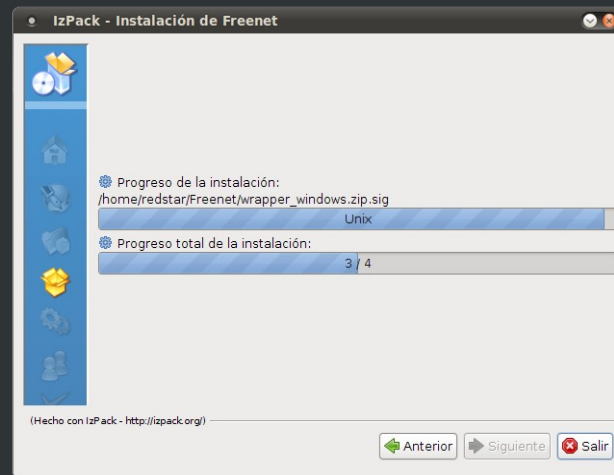
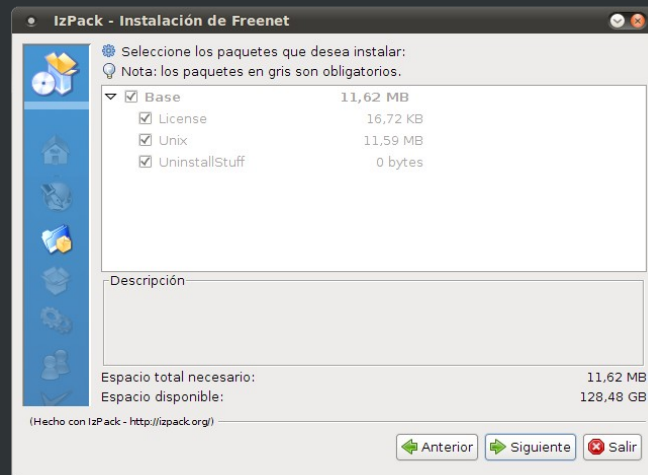
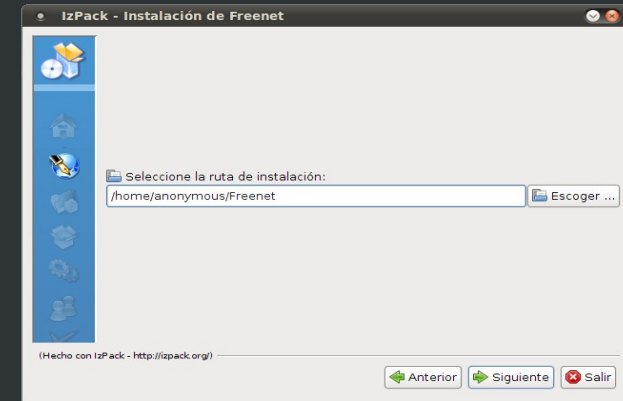
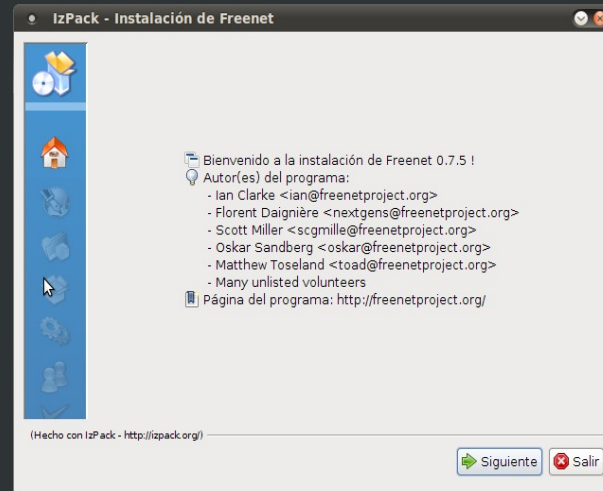
Freenet instalación



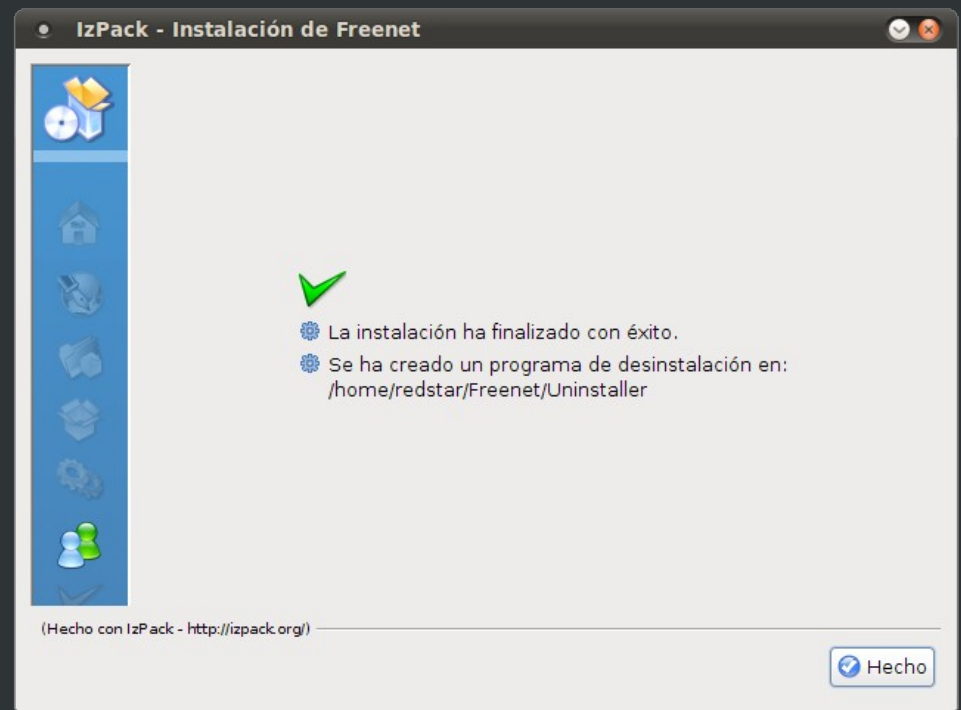
- Requisitos:
 - 1GHz de procesador
 - 1GB de Ram
 - 1GB al menos de disco duro.
- Inicio del asistente
 - `http://freenet.googlecode.com/files/new_installer_offline_1405.jar`
 - `java -jar new_installer_offline_1405.jar`
- Navegador nuevo con modo privado activado
- `http://127.0.0.1:8888/wizard/`



Freenet instalación



Freenet instalación



Freenet



- Low security usar vpn posible FBI...
- High security pocas fuentes

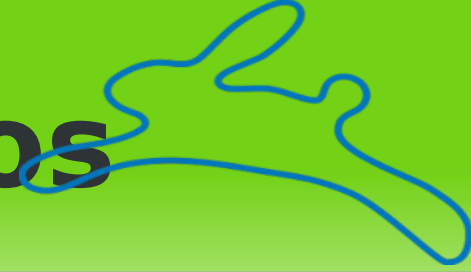
The screenshot shows a web browser window with the address bar displaying '127.0.0.1:8888/wizard/'. The page title is '¡Asistente para la primera vez en Freenet!'. Below the title, there are three columns of options for connecting to Freenet:

Connect to any Freenet user: (low security)	Connect only to friends: (high security)	Detailed settings: (custom)
If you live in a relatively free country where running Freenet is legal, you can choose this option. It is much safer than traditional P2P software like BitTorrent or Gnutella, but an attacker with moderate resources may be able to trace your activity on Freenet back to you. If you have friends who also run Freenet, you can improve security by adding them as Friends, then connecting only to them. Choose low security	If you know several people you want to connect to, this setting allows you to create your own Freenet darknet for vastly improved security. If you only have a few people it may not be very useful, but if some of them know others, or have low security set, you can have a very large network. Choose high security	If you want more fine-grained control, this option lets you set up Freenet according to your own privacy needs. It will take a bit longer than the other two options. Choose custom security

At the bottom of the form, there is a language selector set to 'Español' and a 'Submit Query' button.



Freenet Complementos



- Ejecución independiente

FCP2 (FreeNet Client Protocol 2)

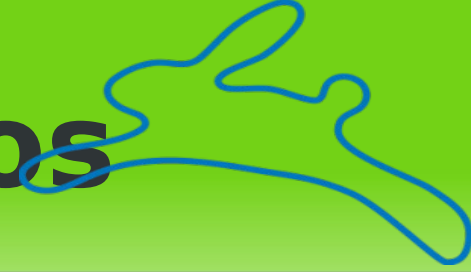
- Integrado como plugin

<http://localhost:8888/plugins/>

- Oficiales
 - No oficiales
- <https://freenetproject.org/tools.html>



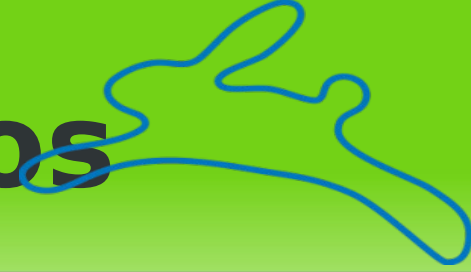
Freenet Complementos



- Frost; tablón de mensajes en freenet **IN**
- Fuqid; gestor de Download/Uploads (solo win)
- Thaw; otro gestor **IN**
- Jsite; crea, inserta y administra freesites. **IN**
- FMS; Freenet Message System **IN**



Freenet Complementos



- Freetalk; para chatear **OF**
- Web of trust (gestiona identidades) **OF**
- Freemail (correos anónimos) **OF**
- FlogHelper (blogs) **OF**
- Jfniki; Creación de wikis **NOF**



Freenet Otros



- Freenet API
- Text Mode Client Interface (TCMI)

`DIR_INS_FREENET/freenet.ini`

`console.enabled=true`

`console.directEnabled=true`



Tor



- Nodos de salida
- Nodos intermedios
- Nodos puente (Enrutable públicamente)

Listados públicos/listados privados

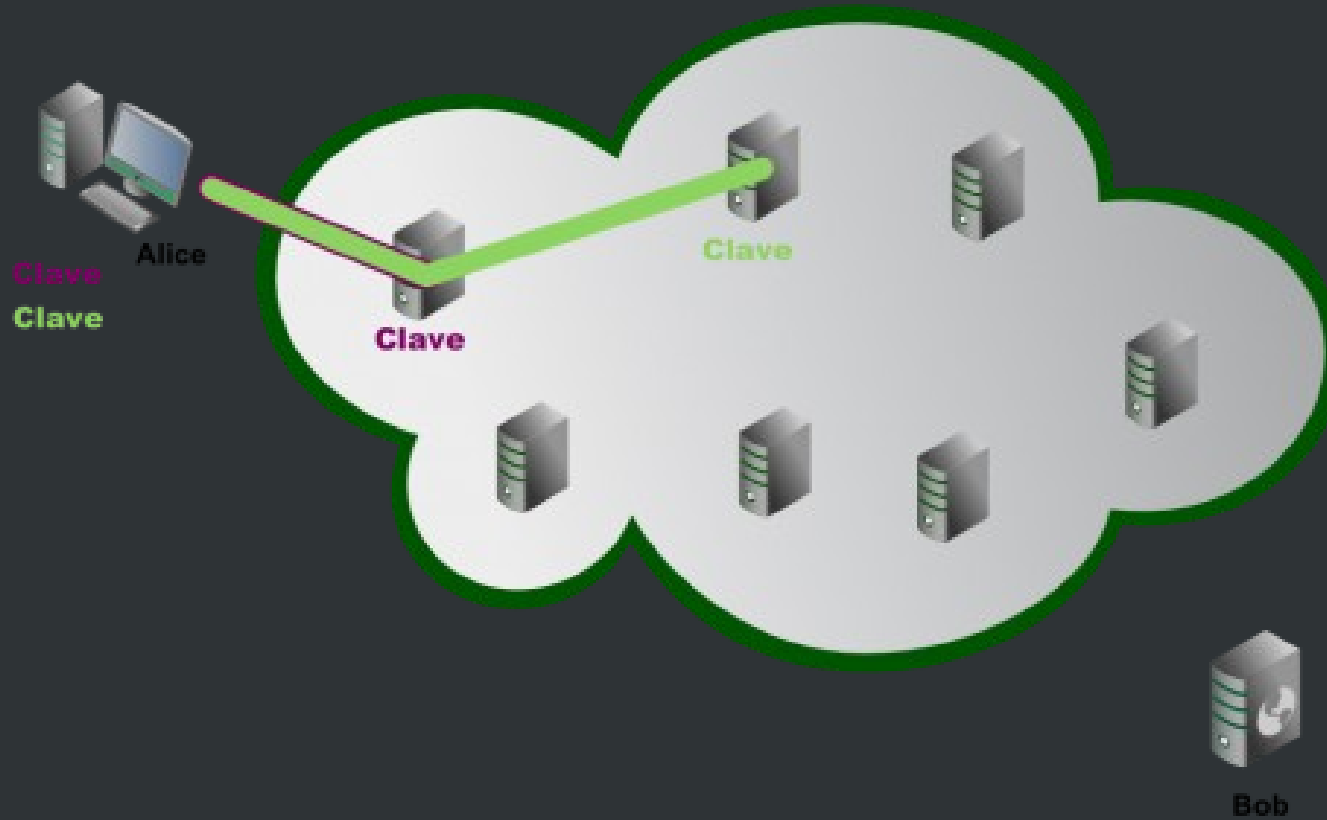
- <https://bridges.torproject.org/> Te dan 3
- bridges@torproject.org Subject y cuerpo
“get bridges”



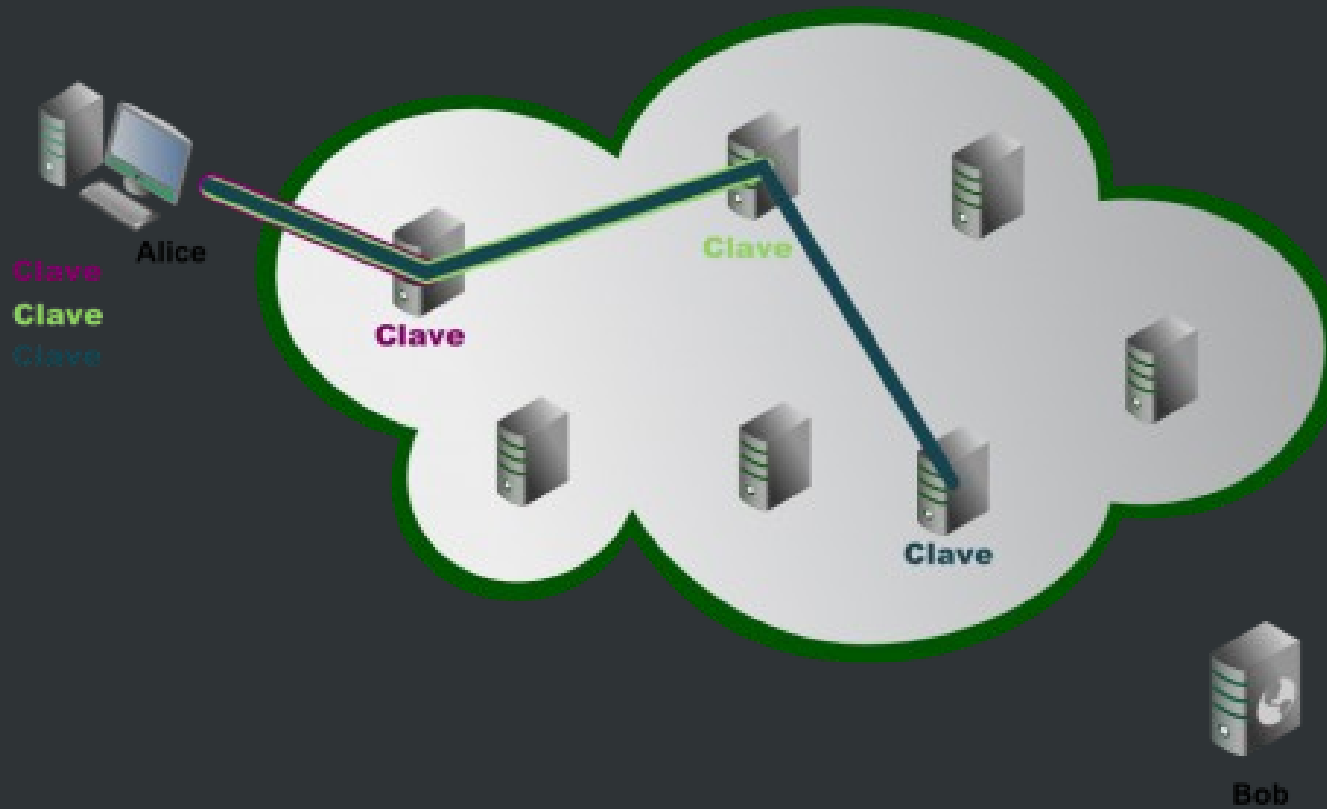
Tor



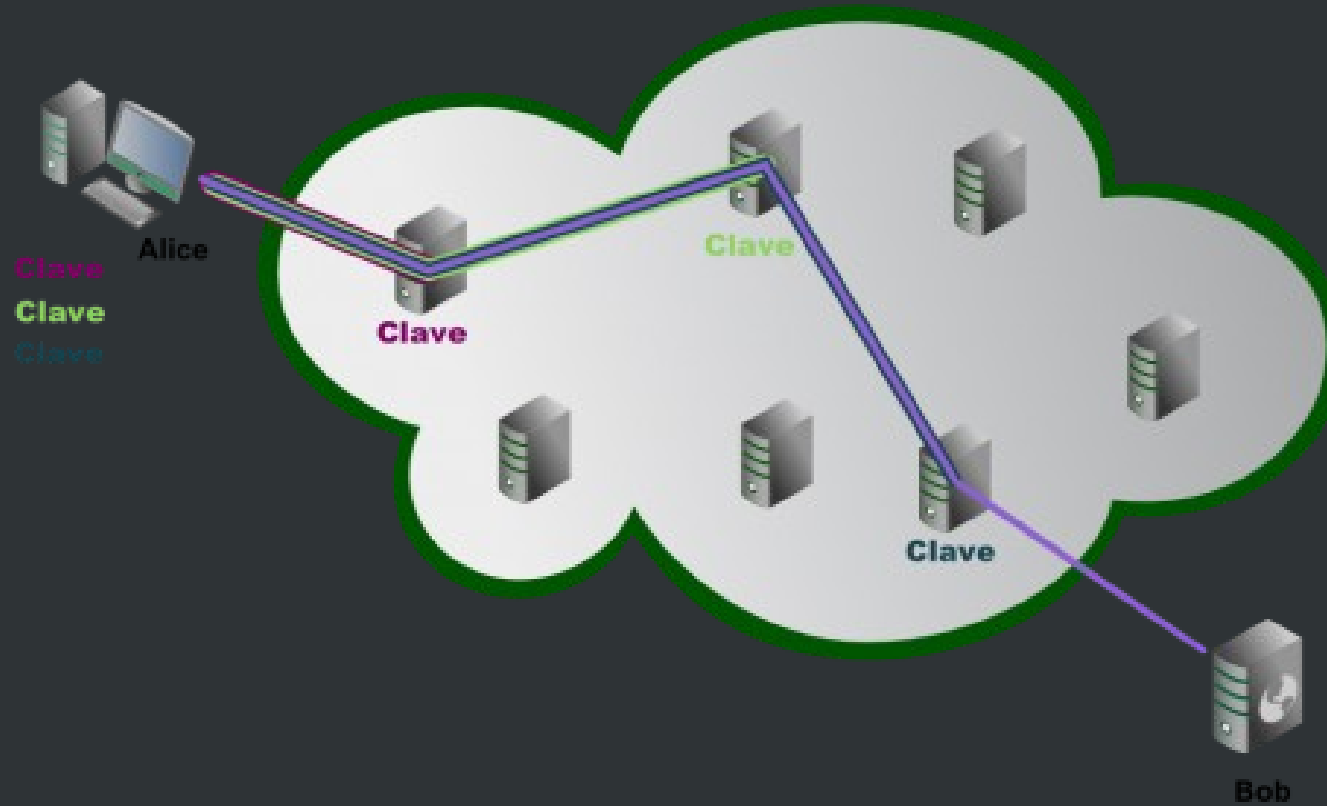
Tor



Tor



Tor



Tor



- Tor dar servicio en el puerto 9050
- Mínimo pasa por 3 nodos tor
- Nodos de tor
- <http://128.31.0.34:9031/tor/status/all>

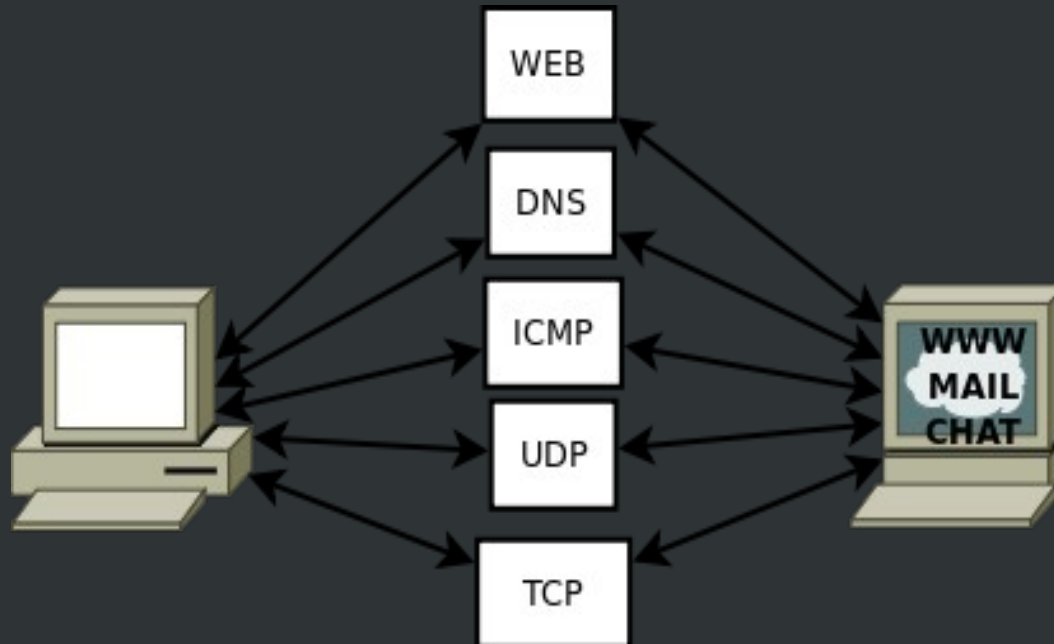
```
r LiPUR AYfjaGo6mVFG42IJ9qsu2ajKCrY ZC+f4qTK/dR6dwy3gYowz0aeYuk 2012-02-09 22:02:27 65.23.240.166 443 9030
s Fast Running V2Dir Valid
opt v Tor 0.2.2.35
r WesCSTor AZ7328jWfMynVRK09z0RjjgeCew cKlmbj6I+LCatj4pbbz0foRCPTo 2012-02-09 12:51:49 129.133.8.31 9001 9030
s Fast HSDir Named Running Stable V2Dir Valid
opt v Tor 0.2.2.35
```



Tor - Navegación



- DNS MAIL IRC IM JUEGOS...



Tor - Navegación web



- Tor Browser Bundle
 - Sin instalación (Portable)
 - Tor
 - Vidalia
 - Torbutton
 - Firefox (con algunas extensiones)
 - <https://check.torproject.org/>



Tor - Herramientas



- Torbutton

Control de fugas de información

- Plugins
- Java
- Flash
- Etc

Extensión Firefox

Cambio de user-agent

The screenshot shows the 'Preferencias de Torbutton' window. It has three tabs: 'Configuración del Proxy', 'Configuración de seguridad', and 'Mostrar configuración'. The 'Configuración del Proxy' tab is active. It contains the following options:

- ☒ Usar la configuración de proxy recomendada para mi versión de Firefox.
 - ☒ Usar Polipo
- ☐ Usar una configuración de proxy personalizada
 - Proxy HTTP: 127.0.0.1 Puerto: 8118
 - Proxy SSL: 127.0.0.1 Puerto: 8118
 - Proxy FTP: Puerto: 0
 - Proxy Gopher: Puerto: 0
 - Host SOCKS: 127.0.0.1 Puerto: 9050
 - ☐ SOCKS v4 ☒ SOCKS v5
 - No hay proxies para: 127.0.0.1

Below these options is a warning: 'Advertencia: Evite el uso de nombres de host por encima de'. Then there are two checkboxes:

- ☐ Torificación transparente (Requiere transproxy personalizado o router Tor)
- ☐ Deshabilitar el botón y las teclas directas para evitar cambios accidentales

At the bottom right is a 'Configuración de prueba' button. At the bottom left is a 'Restablecer valores predeterminados' button. At the bottom right are 'Cancel' and 'OK' buttons.

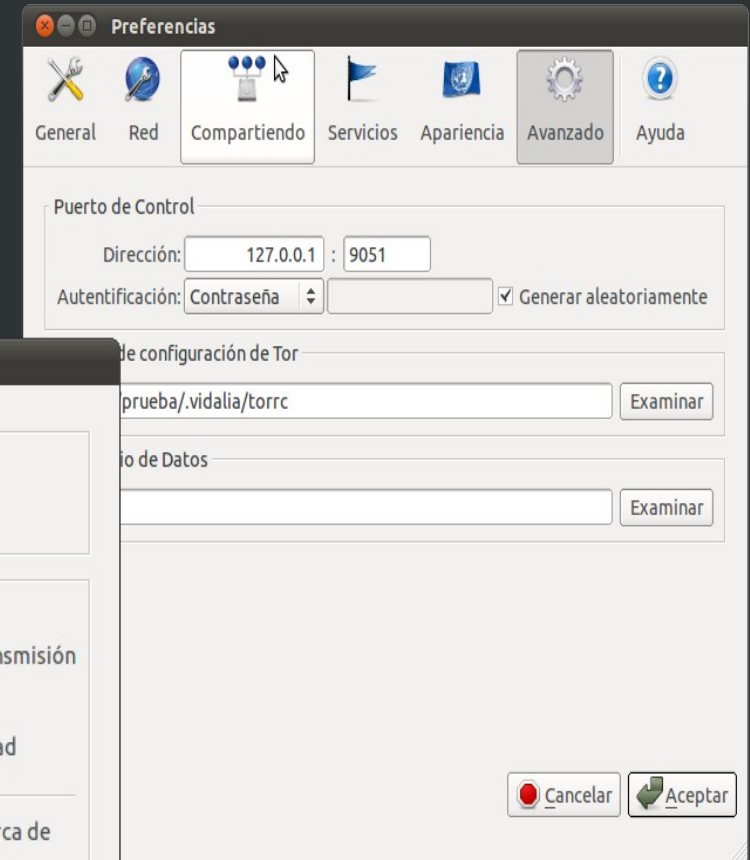
Tor - Herramientas



- Vidalia

Interfaz gráfica para TOR

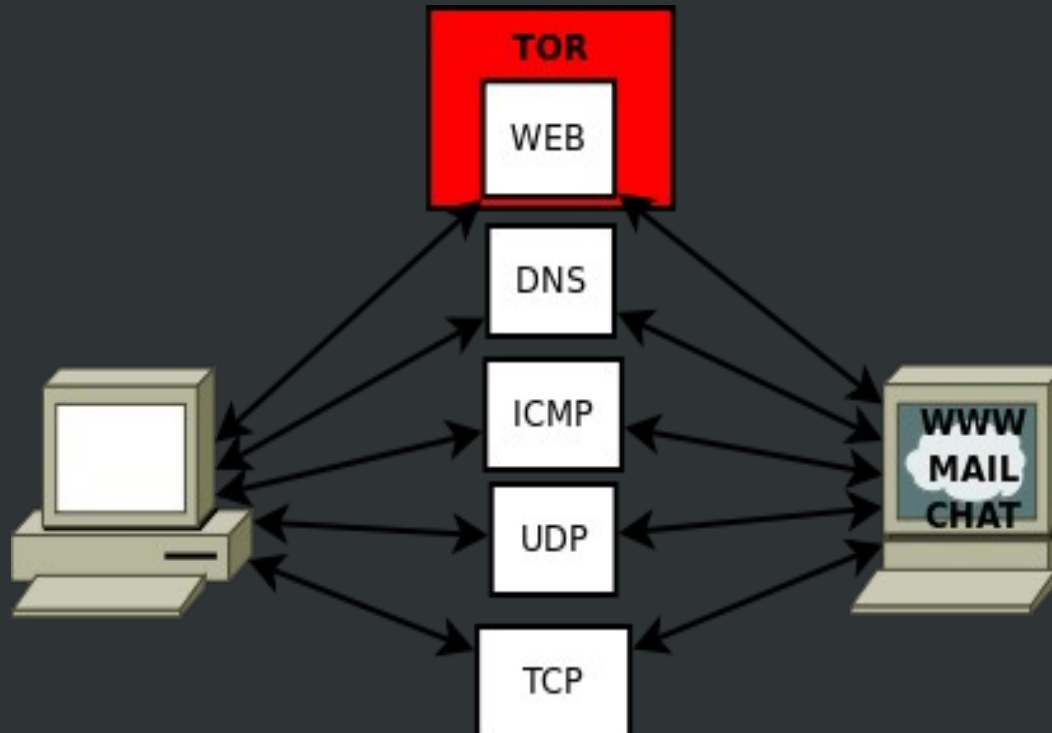
“mapa de red de Vidalia”



Tor - navegación



- Navegación “torificada”



Tor - Herramientas



TORIFICACIÓN

- Proxychains

proxy_dns (evita fuga de datos en DNS)

se traga los icmp

- TorTunnel (torproxy)

No 3 saltos, directos nodo salida

Más rápido

torproxy 8.8.8.8 (devuelve puerto del túnel)



Tor - Herramientas



TORIFICACIÓN

- Privoxy

Capacidades de filtrado

- Polipo

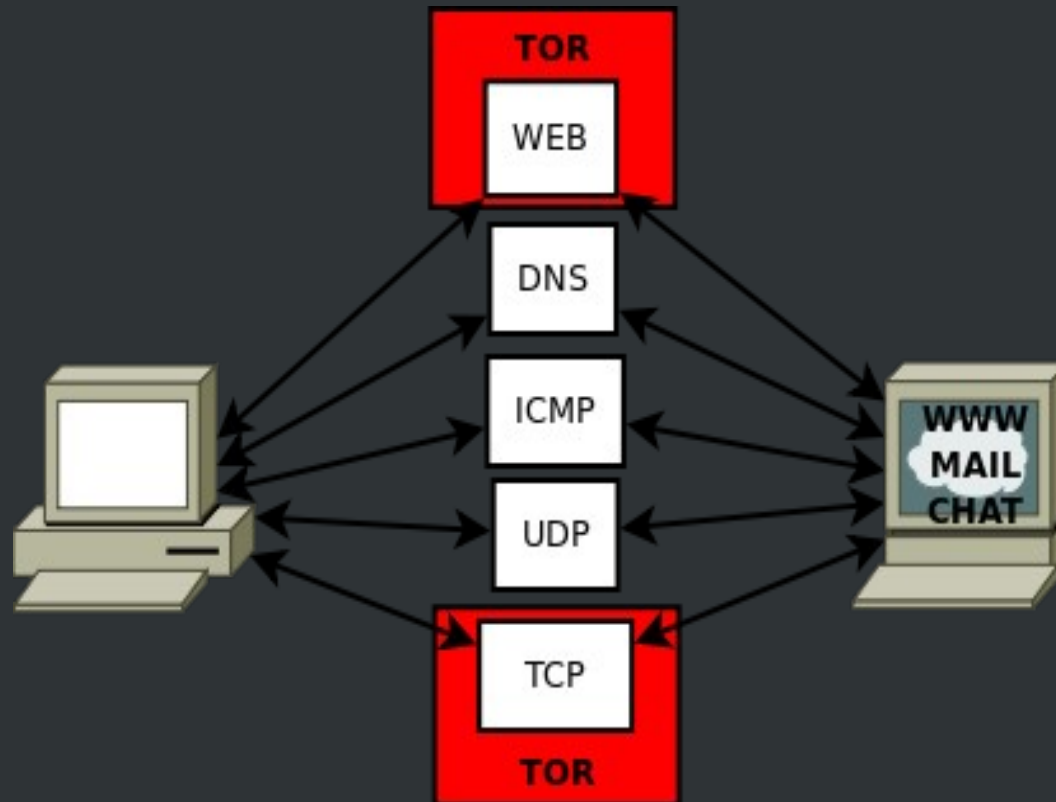
Más rápido HTTP 1.1

Peticiones agrupadas (HTTP 1.1)

Capacidades de filtrado



Tor - Navegación Torificada



Tor - Securitizar DNS



- Configuración

AutomapHostsOnResolve valor 1

AutomapHostsSuffixes “.” (todas las direcciones)

DNSPort

DNSListenAddress 127.0.0.1

ClientDNSRejectInternalAddress

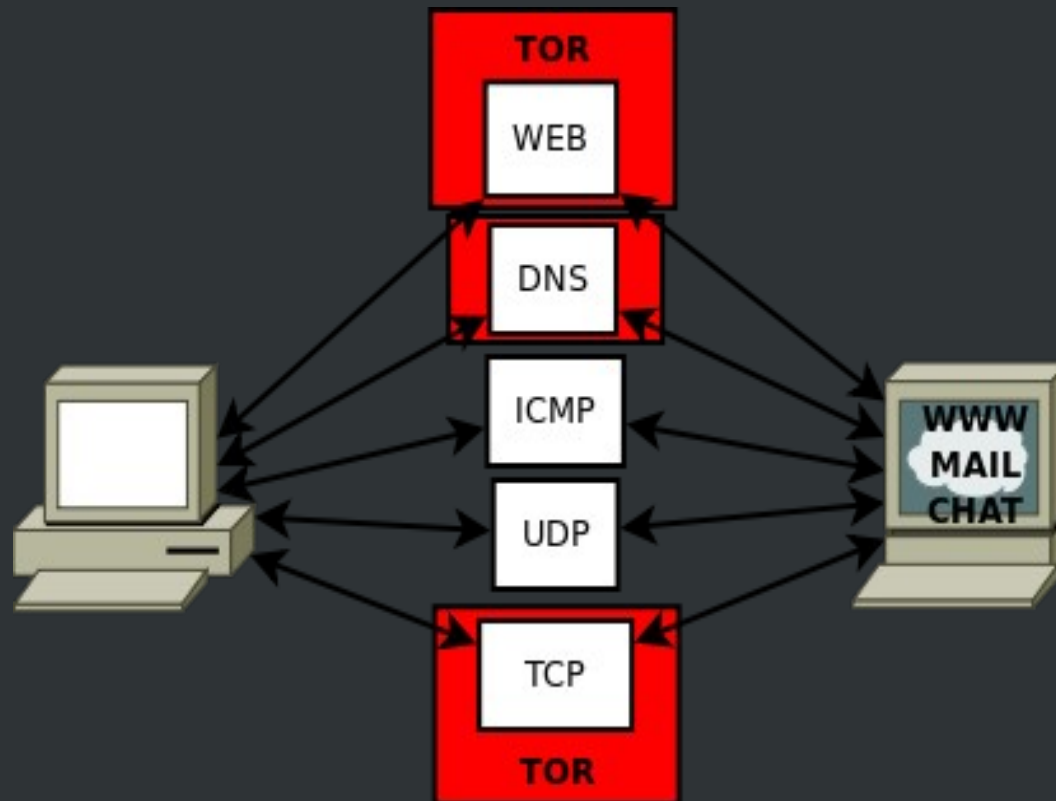
....

- Tor socks (reject UDP)
- Tor-resolve

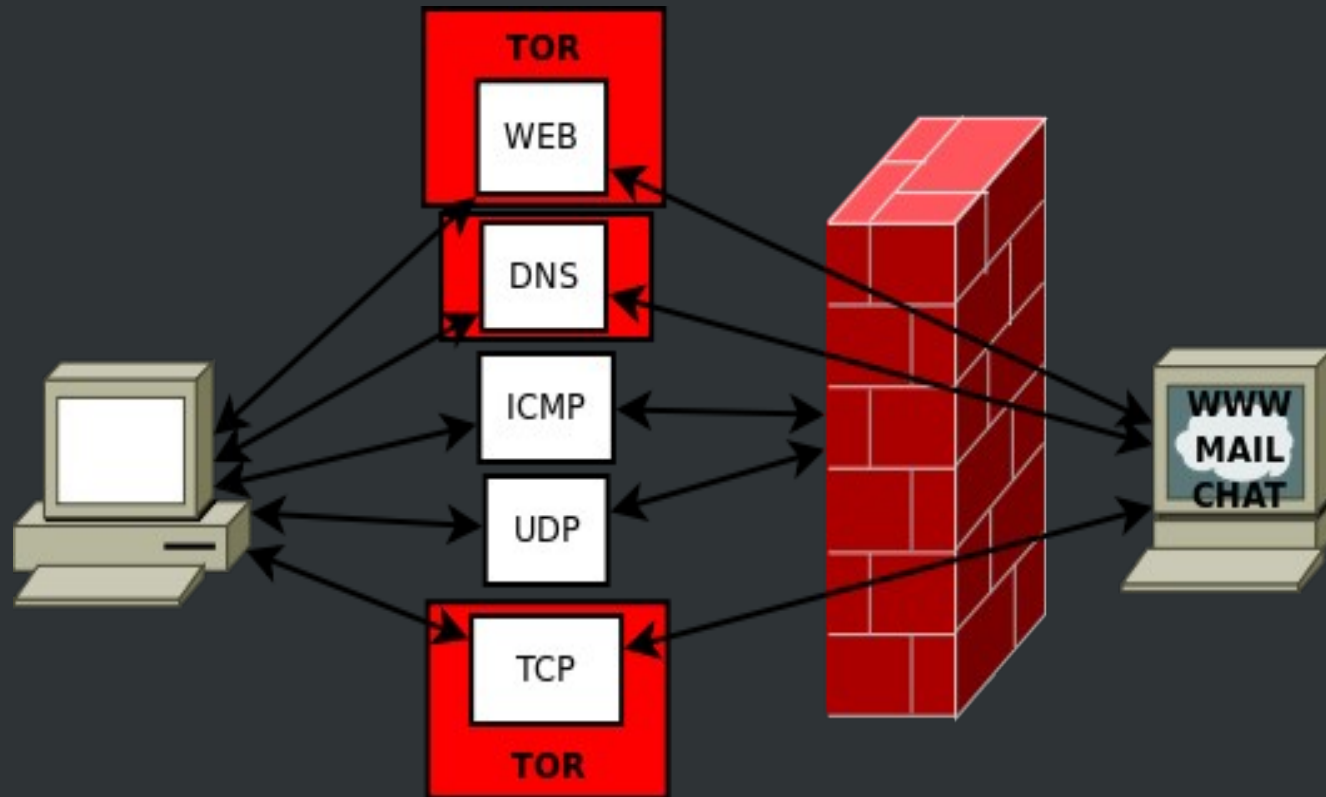
Tor-resolve www.analisisforense.com



Tor - Navegación Torificada/Filtrada



Tor - Navegación Torificada/Filtrada



Tor - Servicios ocultos

- Direcciones .onion
- Fichero torrc

HiddenServiceDir /direcoriodelservicio/

HiddenServicePort 80 127.0.0.1:8080

HiddenServicePort 110 127.0.0.1:110

- Se crearán dos ficheros: private y hostname



Tor - Servicios ocultos

WEBS

- TorDir

<http://eqt5g4fuenphqinx.onion/>

<http://dppmfxaacucguzpc.onion/index.php?sid=08e275eb2e787a41de379fa1fb9d2a21>

- DuckDuck Go

<http://3g2upl4pq6kufc4m.onion/>

- The Hidden Wiki

http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page



GRACIAS POR VUESTRA
ATENCIÓN

¿¿¿Preguntas???

red@nosoloaulas.com

