Software Freedom Day

PRIVACY & ANONYMITY OS

"El Anonimato no significa delincuencia.
Significa Libertad."

Intimidad, seguridad y anonimato en el internet.

Whonix es una distribución basada en **Debian GNU/Linux** enfocada a la seguridad.

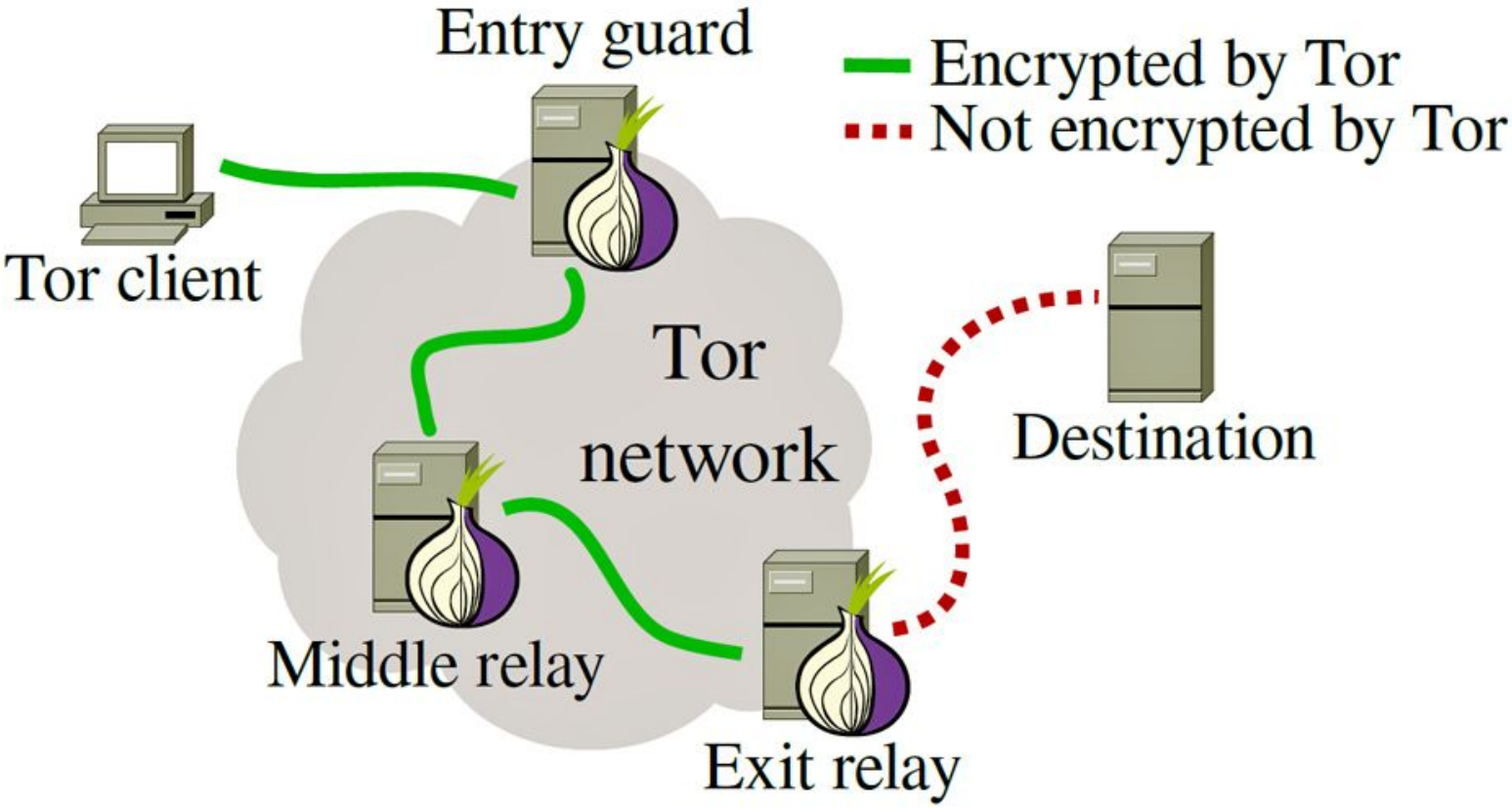
Es diferente a **Tails**. Whonix no es **"amnésico"**. Tanto el **gateway** como el **workstation** conservan su información en cada reinicio.

El no ser amnésico mejora la seguridad en la pasarela, al permitir al sistema de "entrada" de Tor elegir los nodos de entrada más antiguos en la red Tor, reduciendo la capacidad de adversarios para atrapar a usuarios utilizando nodos maliciosos.

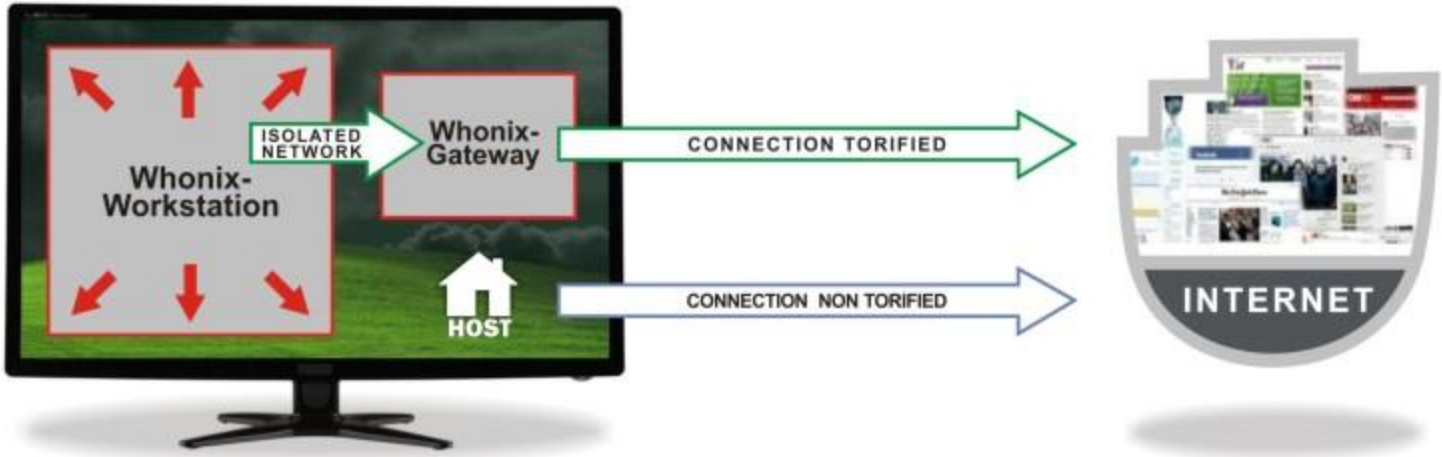
Whonix Está distribuido como dos imágenes de máquinas virtuales.

Whonix-Gateway es la responsable de ejecutar Tor, y tiene dos interfaces virtuales de red. Una de ellas está conectada a internet vía NAT en la VM, y es usada para comunicarse con la red Tor. La otra está conectada en una LAN virtual o **red interna** que puede conectar **Whonix-workstation**.

Todas las comunicaciones conectadas a la red interna están forzadas a pasar bajo la red de Tor.


Entry guard
Encrypted by Tor
Not encrypted by Tor
Tor client
Tor
network
Destination
Middle relay
Exit relay

Whonix
Anonymous Operating System



The red arow ↗ indicate that misbehaving / leaky applications can't break out of the **Whonix Workstation**.

All network connections ⇨ are forced to go through **Whonix Gateway** *where they are torified and routed to the Internet.*

	Whonix ™	Tails	Tor Browser
Focus on anonymity, privacy and security	Yes	Yes	Yes
Type	General purpose OS available as VM images and physical isolation	Live DVD / Live USB / Live SDCard	Portable browser
Supported hardware	x86 compatible and/or Virtual Machines + [4]	x86 compatible and/or Virtual Machines	Windows, Linux, Mac and Virtual Machines
Based on	Tor, Debian [5] and a Virtualizer [6] when not using Physical Isolation	Tor, Debian	Tor, Firefox
Gateway and torify any operating system [7]	Yes [8]	Not a torifying Gateway	Not a torifying Gateway
Live Mode	Yes [10]	Yes	No
Live DVD	No	Yes	No
Live USB	No	Yes	No
USB bootable	Yes [11]	Yes	Yes [11]
USB installer feature	No [12]	Yes [13]	?
Requires VirtualBox [14]	No	No	No
Requires VMware [14]	No	No	No
Requires Qubes OS [14]	No	No	No
System requirements	Higher	Lower	Lowest
Can run in VirtualBox	Yes	Yes, but not recommended. [15] Well documented [16]	Yes, but (?)
Can run in VMware	Yes, but not recommended and unsupported [18]	Yes, but not recommended [15]	Yes, but (?)
Can run in Qubes OS	Yes [20]	Yes [21]	Probably yes, but without security features provided by an Isolating Proxy
Persistence [22]	Full	Optional for Live USB	Yes [23]

Security [edit]

Network [edit]

Table: *Network Security*

	Whonix ™	Tails	Tor Browser
Responsibility for building Tor circuits	Tor client running on Whonix-Gateway ™	Tor client running on workstation	Tor client running on workstation
Protection against IP address / location discovery [28] on the Workstation [29]	Yes [30]	No [31]	No [31]
IP / DNS protocol leak protection	Full [33]	Depends [34]	Depends [34]
Workstation does not need to trust the Gateway	No	Not a gateway	Not a gateway
Takes advantage of entry guards [35]	Yes	No [36]	Yes

Fingerprint [edit]

Table: *Fingerprinting Issues*

	Whonix ™	Tails	Tor Browser
Network / web fingerprint	Whonix ™ fingerprint page	Tails fingerprint page	TBB traffic is tunneled through Tor. Host traffic passes over clearnet
Network fingerprint: ISP cannot trivially guess the project type [91]	Yes	Yes	Yes
Network fingerprint: ISP cannot guess that a non-persistent Tor directory is in use	Yes	No [93]	Yes
Clearnet traffic	All Whonix-Gateway ™ and Whonix-Workstation ™ traffic is tunneled through Tor. Host traffic [94] uses clearnet	None, unless other users sharing the same internet connection are not using Tails	TBB traffic is tunneled through Tor. Host traffic [95] uses clearnet
Network fingerprint: ISP cannot guess which anonymity software is in use due to the ratio of Tor and clearnet traffic	Unknown [97]	The ISP can guess a Tor live system is in use, unless... [98]	?
Network fingerprint: ISP cannot guess which anonymity software is in use because of tordate [100]	Yes, does not include tordate	No, if the clock is grossly inaccurate when booting [100]	No, not an operating system
Web fingerprint [101]	Same as TBB [102]	Not the same as TBB [103]	TBB [104]
Unsafe browser fingerprint [107]	[108]	[109]	?
Network time synchronization runs at randomized times during the session	Yes [110] [111]	Does not continuously run network time synchronization	Not an operating system, does not include network time synchronization
Connection wizard prevents unwanted / accidental connections to the public Tor network [112]	Yes	Yes	?
Includes Tor Browser from The Tor Project	Yes	Yes + patches	Yes
Privacy-enhanced browser [113]	Yes, Tor Browser	Yes, Tor Browser + patches [114] [103]	Yes, Tor Browser
Secure distributed network time synchronization	Yes [115]	Yes [116]	No

Host	Knowledge	Recommendation	OS	Virt	Status	Freedom
Windows	Newcomer	Windows (Download)			Production	FREE
Linux	Newcomer	VirtualBox (Download)			Production	FREE
macOS	Newcomer	macOS (Download)			Production	FREE
Qubes	Advanced	Qubes-Whonix ™ (Download)			Production	FREE
Linux	Advanced	KVM (Download)			Production	FREE
QEMU	Advanced	Unsupported			Experimental	FREE
VMware	Advanced	Unsupported			Experimental	FREE
Any	Advanced	Unsupported			Experimental	FREE
2 PCs, personal computer, notebook	Advanced	x86 compatible			Experimental	FREE
Raspberry Pi 3 B (RPI3)	Advanced	Whonix-Gateway ™ Raspberry Pi 3 B (RPI3)			Experimental	FREE
32-bit	Advanced	Whonix ™ 32 bit information			Production	FREE
Source Code	Advanced	Build Documentation (Download)			Production	FREE

Un método de alta seguridad para navegar en Internet

Basado en Tor

Proporciona una red de retransmisión abierta y distribuida para defenderse de la vigilancia de la red.

Aislamiento

Todas las conexiones del Whonix workstation, son forzadas a pasar por la red tor. Las fugas de DNS son imposibles, e incluso el malware con privilegios de root no puede descubrir la dirección IP real del usuario.

Compatibilidad

Está disponible para todos los principales sistemas operativos. Compatibilidad estable, para distintas arquitecturas.

Laboratorio:

Instalar VirtualBox
(virtualbox.org)

Obtener Whonix
(whonix.org)

Obtener Kali GNU/Linux
(offensive-security.com)

Importar Máquinas virtuales

Configurar red interna

Primeras pruebas