

Whonix: sistema operativo anonimo (parte 1 e 2)

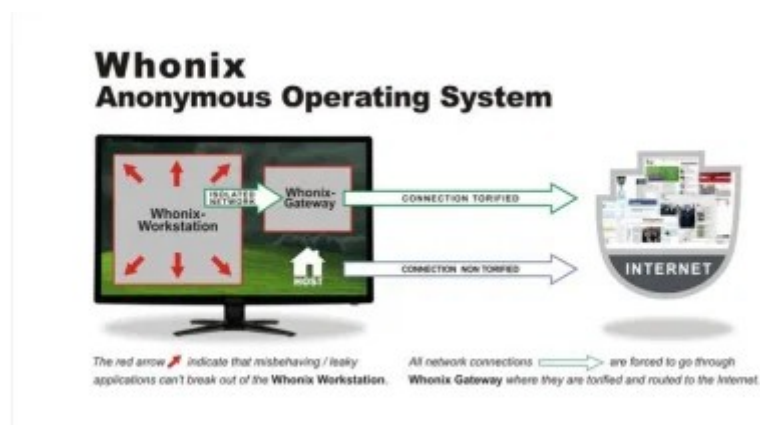
<https://technoblitz.it/whonix-sistema-operativo-anonimo/>

Whonix: un metodo sicuro ed efficace per navigare anonimi

Whonix è un sistema operativo per PC progettato avere un'elevata sicurezza e privacy anche su internet.

Deriva da Debian/Linux e l'architettura su cui si basa è ben diversa dalla classica installazione Desktop, infatti necessita di due macchine virtuali: una Workstation (Whonix-Workstation), questa è la macchina su cui l'utente installerà le applicazioni che tramite una rete isolata comunica con l'esterno esclusivamente tramite l'altra VM chiamata Gateway (Whonix-Gateway) che, come suggerisce il suo nome, instrada tutto il traffico dati (di qualsiasi applicazione) tramite Tor. Questa suddivisione rende impossibile a qualsiasi malware di risalire all'indirizzo IP iniziale.

Dal sito ufficiale abbiamo una schematizzazione del funzionamento:



Come funziona:

La workstation e il gateway Whonix sono configurati per utilizzare una rete privata sul computer host. La workstation indirizza tutto il suo traffico al gateway, che utilizza la rete Tor per accedere a Internet. Tutte le attività di rete eseguite sulla workstation vengono eseguite tramite Tor. Il gateway implementa l'isolamento del flusso per garantire che le diverse applicazioni sulla workstation abbiano percorsi diversi attraverso Tor. Per la massima sicurezza possibile, gli utenti possono scegliere di eseguire le macchine virtuali Whonix sulla piattaforma Qubes. Qubes è un

hypervisor (virtualizer) basato su Xen che gira sul bare metal dell'hardware invece che all'interno di un sistema operativo host.

Poiché viene eseguito su macchine virtuali, può essere utilizzato come sistema operativo guest in Windows, OSX, BSD e Linux.

Come installare il Gateway e la Workstation

Primo step sarà ovviamente avere installato VirtualBox, è possibile scaricarlo da qui, dopo aver installato VirtualBox dovremmo importare le due macchine virtuali scaricate da qui.

Per importarli seguire la procedura classica :

Fare clic su File> Importa...

Fare clic su "Scegli" e seleziona il file del Gateway scaricato.

Fare clic su Avanti e quindi su "Importa" senza modificare nessuna delle impostazioni.

Attendere che la barra di avanzamento completi l'importazione.

Ripeti questi passaggi per il file della Workstation

Ora avviare sia Whonix-Gateway (prima) che Whonix-Workstation (seconda)

Per il primo utilizzo è necessario eseguire una procedura di installazione rapida, quindi attendere la ricerca e la successiva installazione degli aggiornamenti necessari.

Approfondiremo questi passaggi con degli screenshot nel prossimo tutorial.

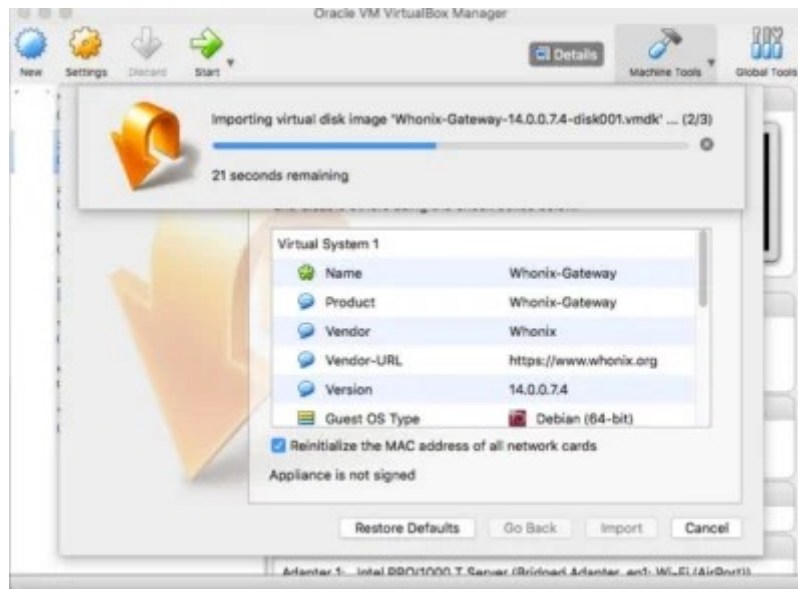
Seconda parte

<https://technoblitz.it/whonix-guida-alluso-e-approfondimenti/>

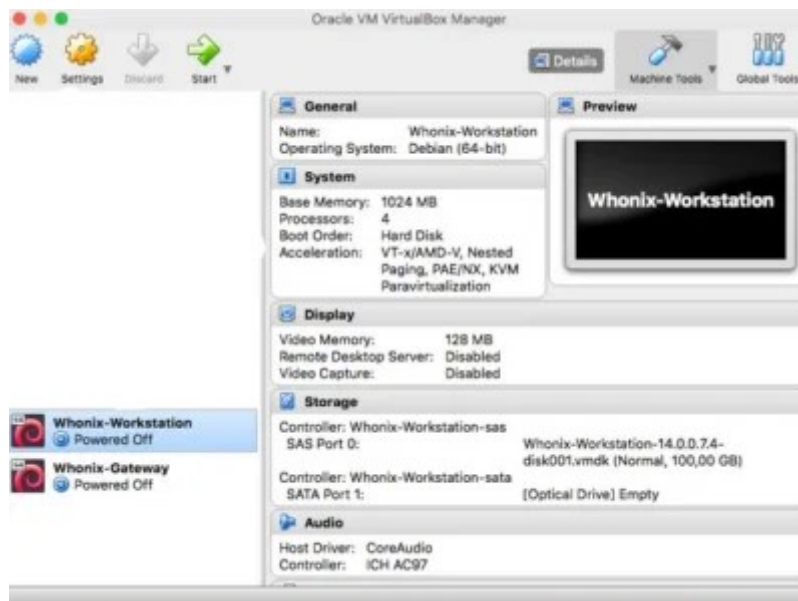
Whonix: guida all'uso

Questa è la seconda parte del nostro tutorial su Whonix: il sistema operativo derivato da Debian con la privacy e l'anonimato come obiettivo principale. Se vi fosse persi la prima parte: ecco qui il link.

A questo punto dovremmo aver già installato ed importato le macchine (se così non fosse i link per il download e gli step da seguire sono nella prima parte, vi consiglio di dargli una lettura prima di proseguire):



Quindi aprendo Virtualbox ci troviamo davanti alle due icone:



Ora dobbiamo avviare le macchina virtuali importate il Gateway e dopo la Workstation, sempre in questo ordine, per gli utenti Windows è possibile fare doppio click sull'icona di Whonix. Al primo avvio ci sarà un'installazione guidata e non dovrete far altro che dare sempre conferma di procedere. Dopo di che è sempre meglio verificare che il sistema sia aggiornato: su entrambe le macchine aprendo la Konsole e scriviamo:

```
sudo apt-get update && sudo apt-get dist-upgrade
```

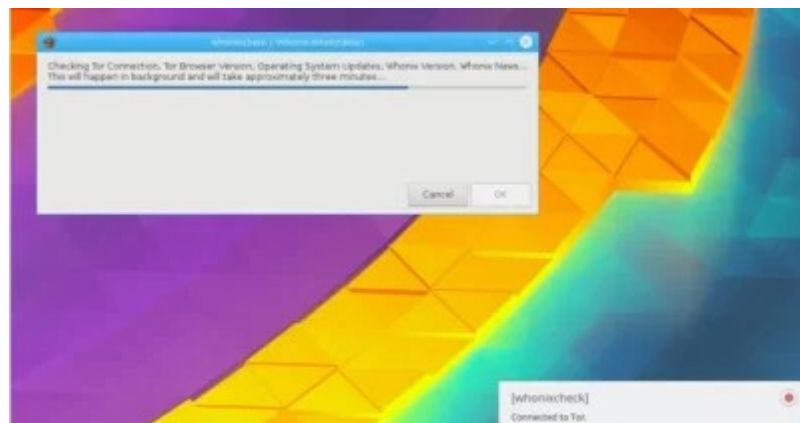
La password di default è changeme, ma anche qui è buona norma cambiarla tramite il comando:

```
sudo su
```

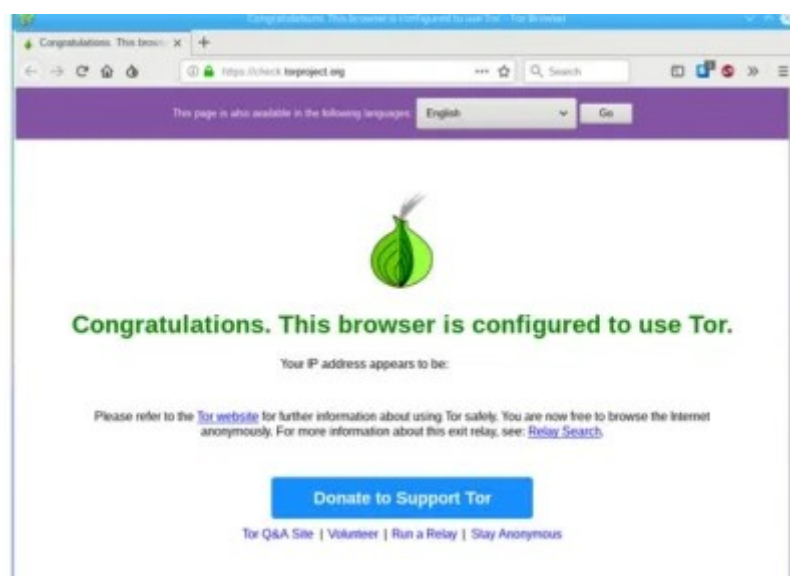
seguito dal

```
/home/user# passwd
```

Ora che il sistema è pronto, verifichiamo la connessione alla rete Tor tramite il tool WhonixCheck:

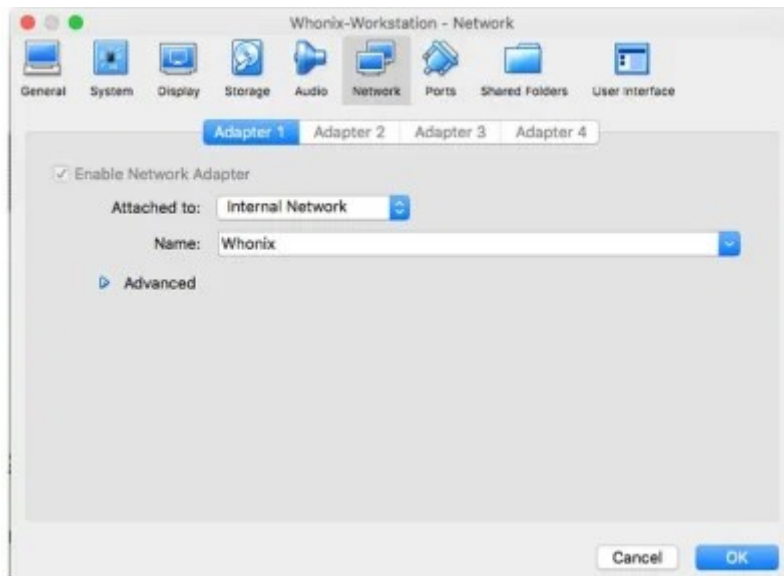


Ovviamente se il check va a buon fine siamo pronti per la nostra navigazione anonima.



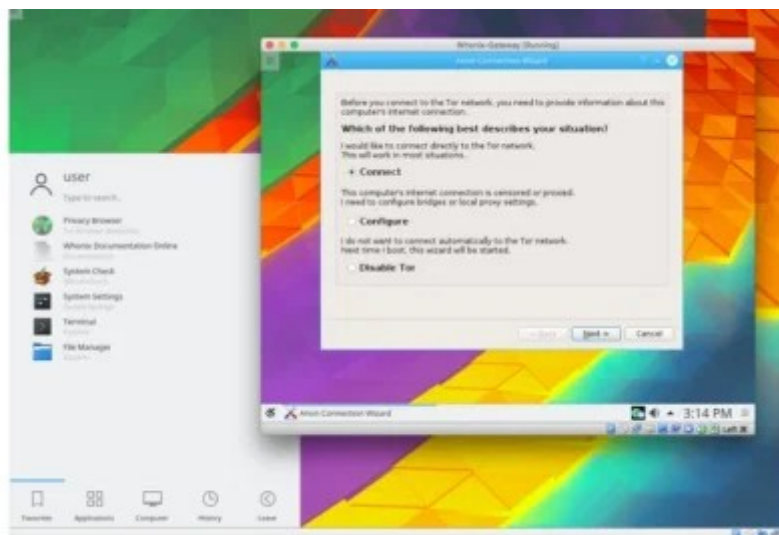
Approfondimenti:

Controlliamo che la workstation sia connessa al gateway dalle opzioni di VBox:

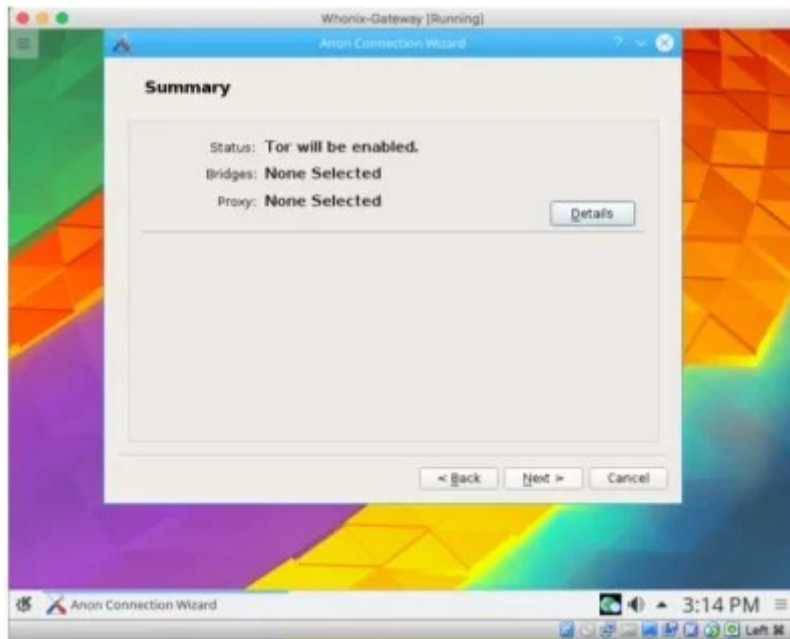


È possibile controllare la connessione a Tor sul Gateway utilizzando il tool Anon Connection Wizard:

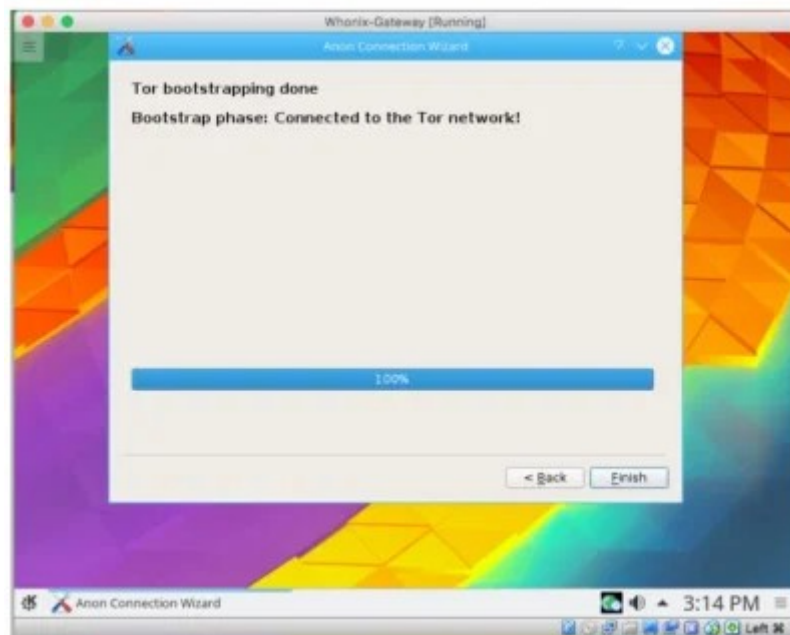
normalmente basterà premere next e lasciare la configurazione automatica, oppure disabilitarlo o invece addentrarsi nella configurazione manuale ogni volta che si accede alla macchina.



riassunto della configurazione:



Connessione riuscita: bootstrapping done!



Conclusioni

Come ogni strumento è bene conoscerlo a fondo, la possibilità di navigare in maniera anonima su internet è importante e spesso utile per non essere tracciati durante le nostre ricerche. È però giusto sapere che non si è mai completamente nascosti su internet!