Instal·lació i configuració d'una VPN amb Wireguard

Per tal de connectar-vos a la VPN i accedir a l'entorn eve-ng de manera remota, el primer pas és descarregar el client Wireguard i instal·lar-lo al vostre ordinador. Per fer-ho aneu a la web del projecte Wireguard (https://www.wireguard.com/install/) i descarregueu l'instal·lador pel vostre sistema operatiu, ja sigui Windows, MacOS o GNU/Linux. Un cop descarregat al vostre ordinador instal·leu-lo seguint la configuració per defecte.

Un cop instal·lat us caldrà la configuració per tal de connectar-vos al servidor VPN. La configuració d'una VPN amb Wireguard es basa en un fitxer de text que conté els camps `Interface` (la configuració del client) i `Peer` (la configuració del servidor), tal com es mostra a continuació:

```
[Interface]
PrivateKey = [Clau privada del client]
Address = [IP privada del client]

[Peer]
PublicKey = [Clau publica del servidor]
Endpoint = [IP:port del servidor]
AllowedIPs = [IPs permeses al túnel]
```

Wireguard utilitza un mecanisme d'autenticació entre client i servidor basat en un sistema de criptografia de clau pública. Així doncs, dins la secció `Interface` es defineix el camp `PrivateKey`, que és la clau privada del vostre ordinador. A partir d'aquesta clau privada es generarà una clau pública, que s'ha de copiar al servidor, i és el mecanisme que permetrà autenticar el client. De la mateixa manera, el servidor tindrà una clau privada a partir de la qual es generarà la clau pública. Aquesta clau pública és la que heu de posar a la secció `PublicKey` de l'apartat `Peer`. Això permetrà que el vostre client pugui autenticar els missatges del servidor.

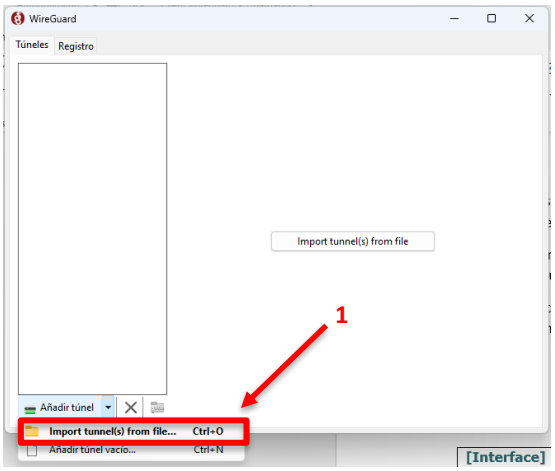
Un cop resolta l'autenticació, en el camp `Address` de l'apartat `Interface` cal indicar l'adreça IP que tindrà el vostre ordinador dins del túnel. Aquesta adreça ha d'estar dins del mateix rang que el servidor per tal que es puguin comunicar.

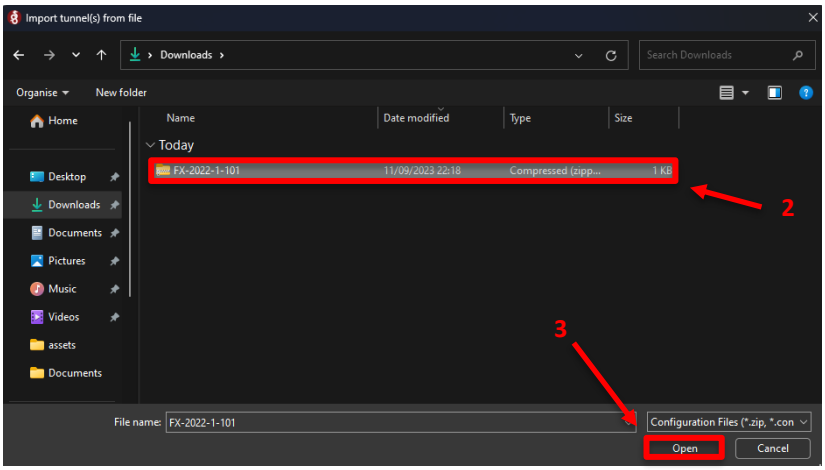
El següent pas és configurar el camp `Endpoint` de l'apartat `Peer`. Aquest camp indica quina és l'adreça IP i port UDP públics del servidor Wireguard. És a dir, és l'adreça IP i port UDP públics on el vostre client enviarà els paquets encriptats per tal d'accedir a la VPN.

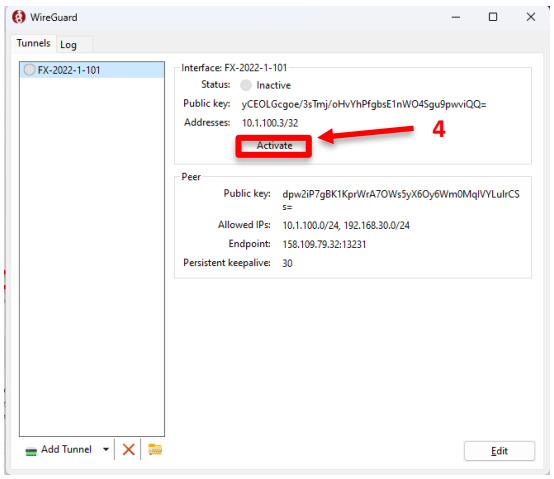
Finalment, el darrer camp a configurar és el `AllowedIPs` dins de l'apartat `Peer`. Aquest camp indica quines adreces IP poden circular a través del túnel entre el client i el servidor. Així es pot crear un `split tunel` o un `full tunnel`. En el cas de `split tunel` el client només envia a través del túnel aquells paquets que corresponguin a les adreces que hi ha a l'altre banda del túnel. En canvi, en el cas de `full tunel` el client envia tot el tràfic que genera a través del túnel, de manera que a l'altre banda s'ha de permetre la sortida cap a Internet en cas que sigui necessari. Així doncs, un valor `AllowedIPs=0.0.0.0/0` forçaria que tot el tràfic de la vostra màquina circulés a través del túnel. En canvi, un calor `10.0.0.0/30` forçaria que només el tràfic de la vostra maquina que va a la xarxa `10.0.0.0/30` circulés a través del túnel, mentre que la resta de tràfic sortiria cap a Internet sense problemes.

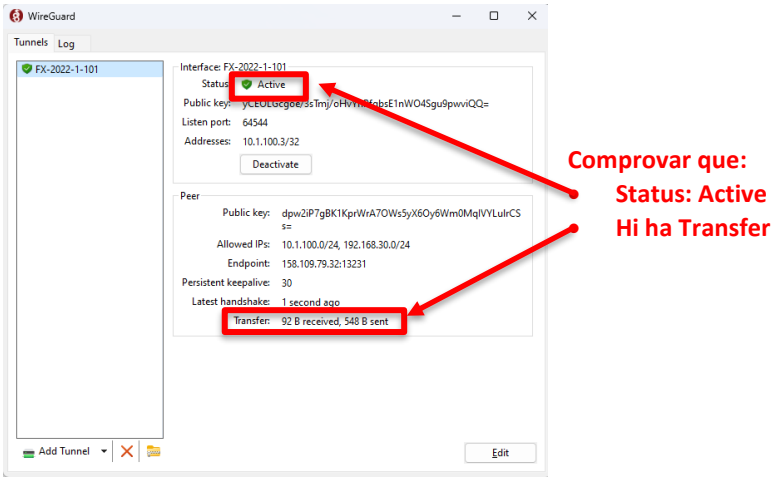
Així doncs, tenint en compte aquesta descripció funcional, en el correu us proporcionem la configuració que heu d'utilitzar en el vostre client. Per fer-ho us caldrà obrir el client Wireguard i seleccionar la opció "*Añadir tunel – Añadir tunel vacio*", tal com es mostra a la Figura següent

Un cop a la finestra de "*Añadir túnel vacio*" haureu d'enganxar la configuració que us hem fet arribar per correu, tal com es mostra a continuació.









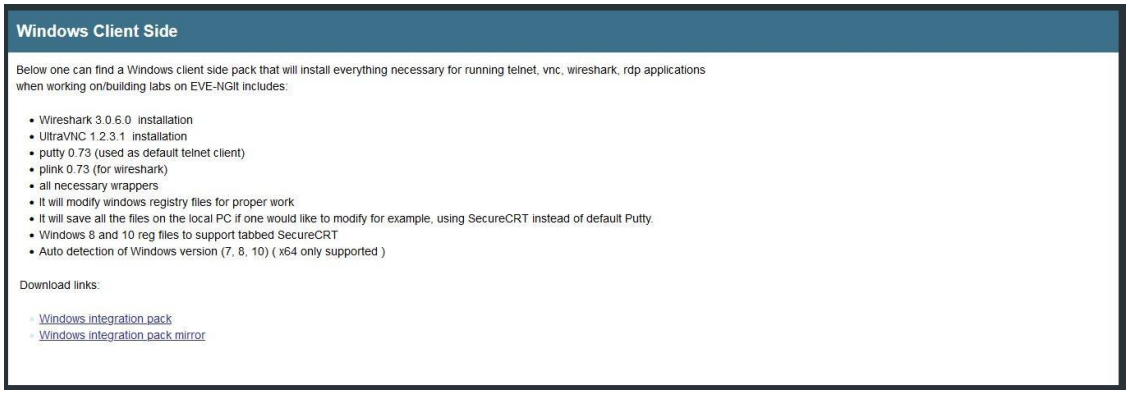
Un cop creat el nou túnel el podeu desar. Tingueu en compte que el nom que assigneu al túnel és irrellevant, i al resta de paràmetres dependran de la configuració que us hem proporcionat i que no heu de modificar en cap cas.

Finalment, us podeu connectar a la VPN activant el botó "Activar", tal com es mostra a continuació. Un cop connectats haureu de poder obrir un navegador i connectar-vos a l'entorn eve-ng utilitzant l'adreça http://10.0.n.2/, on n és el número de grup que teniu assignat. Recordeu que l'usuari i contrasenya de l'entorn eve-ng és usuari=**admin**, password=**eve**.

Instal·lació i configuració del client eve-ng

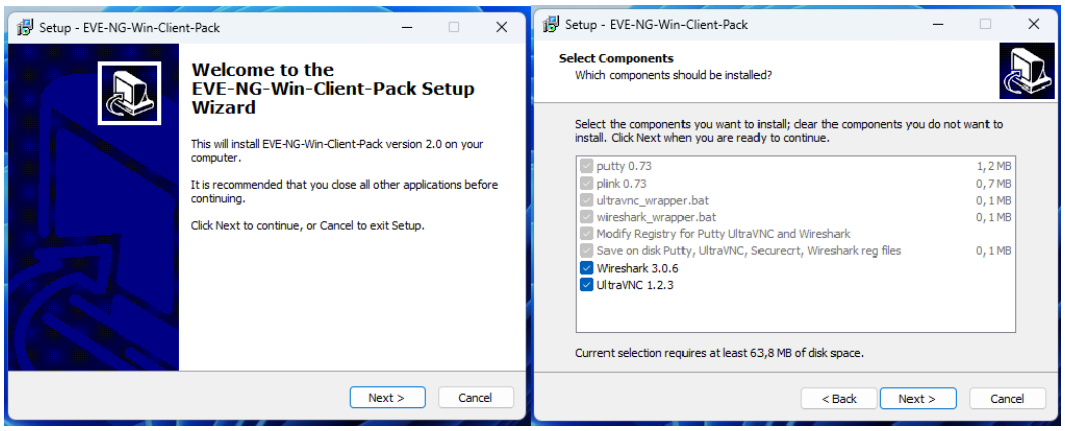
Un cop realitzada la instal·lació i configuració de la VPN amb Wireguard, el seguent pas és instal·lar i configurar el client eve-ng, que us permetra interaccionar amb les màquines de l'entorn virtual a través d'una consola de comandes, així com capturar tràfic de manera remota.

Per fer-ho, el primer pas és descarregar el client de la web d'eve-ng per al vostre sistema operatiu, ja sigui Windows, MacOS o GNU/Linux:

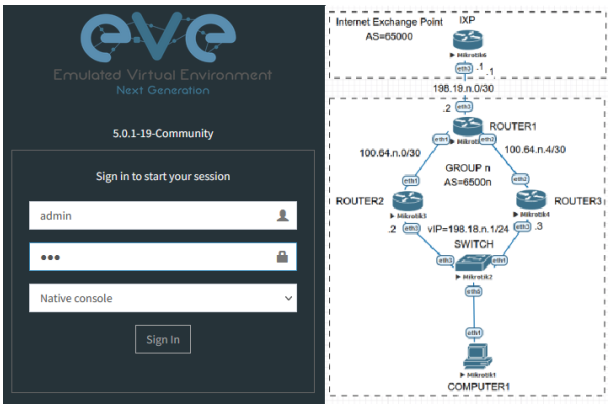


- https://www.eve-ng.net/index.php/download/#DL-WIN
- https://www.eve-ng.net/index.php/download/#DL-OSX
- https://www.eve-ng.net/index.php/download/#DL-LIN

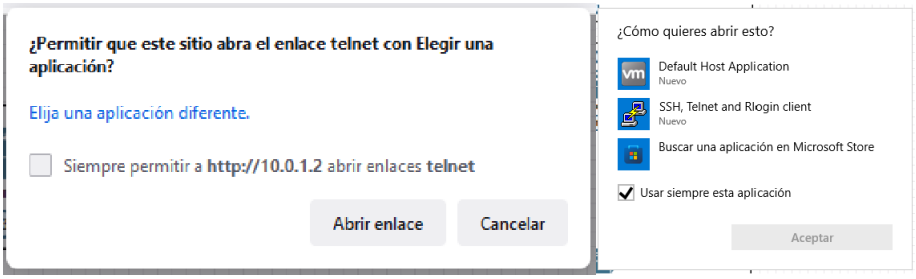
Un cop descarregat el client corresponent al vostre sistema operatiu, heu de realitzar-ne la instal·lació seguint els passos que es mostren a continuació, assegurant-vos d'instalar el client de telnet (PuTTY) i el sistema de captura de paquets (Wireshark), tal com es mostra a continuació.



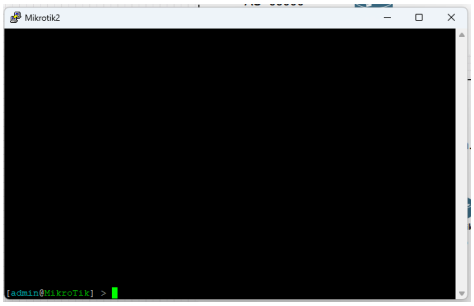
Un cop instal·lat el client podeu tornar a accedir a l'entorn eve-ng a través de l'adreça http://10.0.n.2/, on n és el número de grup que teniu assignat. Recordeu que l'usuari i contrasenya de l'entorn eve-ng és usuari=**admin**, password=**eve**. En aquest cas però, us caldrà seleccionar l'opció "**Native Console**", cosa que us permetrà fer servir el vostre ordinador per accedir directament l'entorn virtual d'eve-ng (routers, switch, etc.).



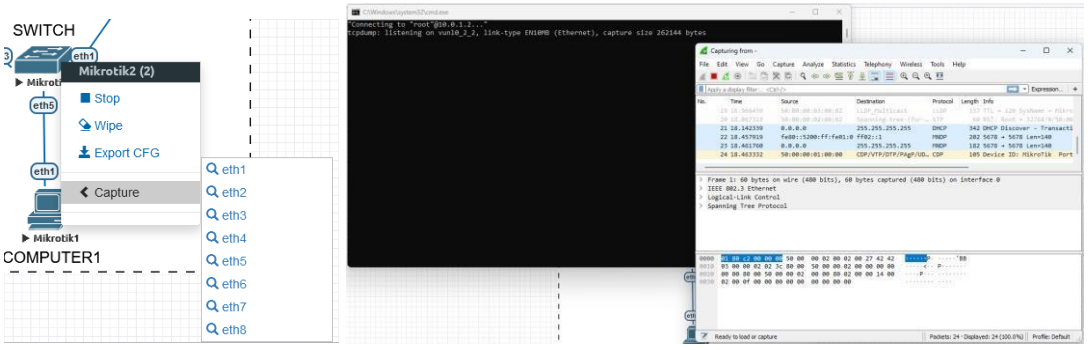
Un cop dins l'entorn eve-ng podeu fer click sobre qualsevol element de xarxa per tal d'obrir un terminal de configuració. Al fer-ho us apareixerà un menú contextual que heu d'acceptar (Abrir enlace) i, a continuació, seleccionar l'opció "SSH, Telnet and Rlogin client" (PuTTY).



Un cop acceptat us apareixerà un terminal de configuració PuTTY que us permetrà configurar l'equip seleccionat de manera remota, tal com es mostra a la Figura seguent.



Finalment, també podeu capturar el tràfic que circula entre qualsevol enllaç de la xarxa utilitzant l'eina Wireshark. Per fer-ho heu de clicar amb el botó dret sobre un dels nodes (router o switch) i, a continuació seleccionar l'opció "Capture" i la interfície de xarxa sobre la qual vulgueu fer la captura. Quan ho feu s'obrirà un menú contextual similar a l'anterior que, un cop acceptat, obrirà una instància de Wireshark on veureu el tràfic remot.



Usuari 1

```
[Interface]
PrivateKey = sJoCQ8HBqo7wFUXhqT8vGxEYFFTS7vbFFsEvEhvb0FU=
Address = 10.1.102.2/30

[Peer]
PublicKey = +3wY0LXoK2u56KtRVrbDbnNU7iXC2gwwtGCX9PtPpG8=
AllowedIPs = 10.1.102.0/30, 10.0.102.0/30
Endpoint = 213.73.43.41:13033
```