GUIDA BRELDOITALIA WIREGUARD VPN

Per creare applicazioni VPN *(Site-to-Site / Client-to-Site)* come l'estensione della rete Lan aziendale, gestione di una singola o più periferiche di rete, BreldoItalia utilizza un nuovo protocollo VPN denominato 'Wireguard'.

CHE COS'E' WIREGUARD ?

WireGuard è un'applicazione e un protocollo di rete per la creazione di tunnel VPN criptati. Il software è gratuito con la licenza GPLv2 ed è disponibile su più piattaforme. WireGuard è scritto nei linguaggi "C" e "Go" e funziona con Windows, macOS, BSD, iOS e Android. WireGuard crea un tunnel criptato attraverso il quale vengono instradati i flussi di dati così protetti da accessi non autorizzati. Oltre all'attenzione per una crittografia avanzata, WireGuard offre ottimizzazioni per dispositivi e sistemi mobili "Internet of Things+ (IoT)". Dalla primavera del 2020, WireGuard è stato integrato direttamente nel kernel Linux. Dal momento che Linux opera come sistema operativo standard su miliardi di dispositivi collegati in tutto il mondo, WireGuard può essere utilizzato praticamente ovunque. Il suo utilizzo su larga scala è dovuto anche al fatto che il software è relativamente leggero e richiede solo bassi requisiti di hardware.

QUALI SONO LE CARATTERISTICHE DI WIREGUARD ?

La caratteristica principale del protocollo WireGuard è il cosiddetto Cryptokey Routing.Gli indirizzi IP consentiti all'interno di un tunnel vengono assegnati alla chiave pubblica di un partner di connessione che decifra i pacchetti in entrata. Dopo la decodifica, un pacchetto in entrata viene consegnato solo se proviene da un indirizzo IP corrispondente alla chiave, altrimenti viene scartato. A differenza degli stack di protocollo VPN IPsec e OpenVPN, WireGuard non è un protocollo agile: invece di negoziare singolarmente le basi crittografiche da utilizzare durante la fase di handshake quando si stabilisce una connessione, WireGuard si limita ad alcune opzioni solo in forma riassuntiva. Qualora una delle basi crittografiche risulti compromessa, viene pubblicata una nuova versione sicura del protocollo WireGuard che, se utilizzata da entrambi i partner di comunicazione, proteggerà il flusso di dati.

QUALI SONO I VANTAGGI DI WIREGUARD ?

Uno dei maggiori vantaggi di WireGuard sta nelle dimensioni del suo codebase. L'intero codice kernel è costituito da circa 4.000 linee di codice mentre il codice di un'implementazione di OpenVPN o IPsec ne contiene circa 100.00-600.000. Un codebase più piccolo è intrinsecamente più sicuro perché rende più facile trovare i bug e riduce al minimo la superficie di attacco. Grazie alla minore complessità del software, si possono ottenere maggiore sicurezza e prestazioni più elevate. Nei benchmark, WireGuard garantisce una velocità di trasmissione maggiore e una latenza minore rispetto ai protocolli concorrenti. Inoltre, WireGuard non è un protocollo "chiacchierone": ("it is not a chattyprotocol"): se l'utente non invia dati attraverso il tunnel, WireGuard è a riposo riducendo in questo modo la quantità di energia utilizzata, a beneficio della durata della batteria. L'efficienza energetica è molto importante per i dispositivi mobili e in questo settore WireGuard è ben posizionato per diversi aspetti. Ad esempio, questo protocollo supporta il roaming ovvero il passaggio automatico dalla rete Wi-Fi alla rete di telefonia mobile e viceversa. Questo significa che se si perde una connessione, WireGuard di solito si ricollega più velocemente rispetto ai protocolli concorrenti.

WIREGUARD MULTI-PIATTAFORMA

Wireguard è disponibile per i seguenti sistemi-operativi (Ne citiamo alcuni):

- Windows
- MacOS
- Ubuntu
- Android
- iOS
- Debian
- Fedora
- Mageia
- Arch
- OpenSuse

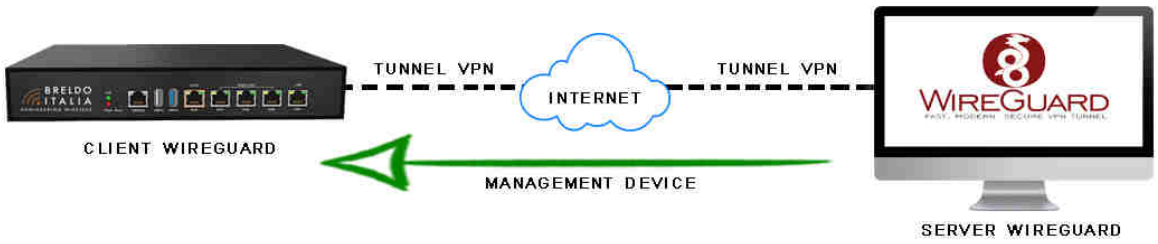
Link Download: https://www.wireguard.com/install/

MODALITA' DI UTILIZZO.

Come anticipato all'inizio di questa guida, BreldoItalia grazie al potente protocollo Wireguard VPN, permette di realizzare svariate applicazioni tunnel. Di seguito vi spiegheremo tutte le modalità di utilizzo di Wireguard con le soluzioni BreldoItalia.

COME CONNETTERSI AL GATEWAY BRELDOITALIA DA SOFTWARE WIREGUARD WINDOWS.

Questa prima applicazione ci permette di connetterci da qualsiasi posto nel mondo tramite il proprio PC sul Gateway BreldoItalia senza dover aprire le porte TCP/UDP sul Firewall dove è installato il Gateway. Tutto questo ci consente di eseguire manutenzione e configurazione sul Gateway BreldoItalia direttamente dal proprio PC/Notebook.



SERVER WIREGUARD:
- PC con O.S Windows
- Software Wireguard
- IP Interface: 192.168.1.4
- IP Tunnel: 10.14.0.2/32
- IP Pubblico: 2.237.17.52

CLIENT WIREGUARD:
- Gateway BreldoItalia
- Wireguard
- IP Tunnel: 10.14.0.1/32
- IP Lan: 192.168.88.1

Prima di passare alla configurazione del '**Software Wireguard Windows**' sul PC, si prega di creare una regola di **port-forwards** sul modem del proprio gestore telefonico. Tutto questo perchè il PC dove è installato il software wireguard windows viene utilizzato come **SERVER WIREGUARD VPN**.

- UDP 51820 Esterna/Interna su IP 192.168.1.4

IMPORTANTE:
- La PrivateKey e PublicKey sia su lato server *(PC)* che su lato client *(Gateway)* vengono generate automaticamente da Wireguard.

-- CONFIGURAZIONE DEL SOFTWARE WIREGUARD SU WINDOWS *(SERVER)*:

Aprire il programma ed eseguire i seguenti passaggi:
1) Click su "Aggiungi Nuovo Tunnel".
2) Inserire Nome del Tunnel (Esempio Hotel Verde).
3) Nel box bianco copiare quanto segue:

```
#####################################################################

[Interface]
PrivateKey = Non modificare.
ListenPort = 51820
Address = 10.14.0.1/32
DNS = 1.1.1.1

[Peer]
PublicKey = COPIARLA DAL GATEWAY BRELDOITALIA (CLIENT)
AllowedIPs = 10.14.0.2/32, 192.168.88.0/24

#####################################################################
```

LEGENDA:

Private Key: Esistente *(Non modificarla)*.
ListenPort: Porta di ascolto del Server Wireguard *(Obbligatorio).*
Address: Indirizzo IP del Server Wireguard *(Obbligatorio)*.
DNS: Server DNS che si vuole utilizzare (Obbligatorio) (Per aggiungere più di un un server DNS: 8.8.4.4, 8.8.8.8, 1.1.1.1).
Aggiungere il client [Peer]:
PublicKey: Inserire la PublicKey del Gateway BreldoItalia (Client) da gestire. *(Obbligatorio)*
AllowedIPs: Indirizzi IP che dal Server VPN possono essere chiamati tramite Tunnel. (Esempio: 192.168.88.4/32, 192.168.88.10/32)*(Obbligatorio)*

IMPORTANTE:
- Nel campo **AllowedIPs** inserire sempre l'indirizzo IP Tunnel del CLIENT*(Esempio: 10.14.0.2/32)*.
- La **Privatekey** viene generata al momento della creazione di un "Nuovo Tunnel".
  Si prega di non cancellarla. E' importante mantenerla segreta e non diffonderla a terzi.

-- CONFIGURAZIONE WIREGUARD SU GATEWAY BRELDOITALIA *(CLIENT)*:

Entrare nel Firmware ed eseguire i seguenti passaggi:
Click su **Network** ----------> **Interface** ----------> **Wireguard** ----------> **Edit**

Impostare i seguenti paramentri:

Protocol = WireGuard VPN.
PrivateKey = Non modificare.
ListenPort = Non necessaria.
IP Address = 10.14.0.2/32

Aggiungere il Server Wireguard nella sezione "**Peers**":

PublicKey = COPIARLA DAL SOFTWARE WIREGUAD WINDOWS *(SERVER)*
AllowedIPs = 10.14.0.1/32
Route Allowed IPs = Yes
Endpoint Host = 2.237.17.52
Endpoint Port = 51820
Persistent Keep Alive = 25

A parametri inseriti salvare la configurazione tramite il tasto: **Save & Apply**.

Per default l'interfaccia "Wireguard" è disabilita.
Per attivare il funzionamento di Wireguard bisogna abilitare l'interfaccia facendo click sul menù:
Physical Setting ----------> **Enable This Interface**

Per default le regole firewall impostate sul gateway consentono il collegamento tra PC (Server) e Gateway (Client)

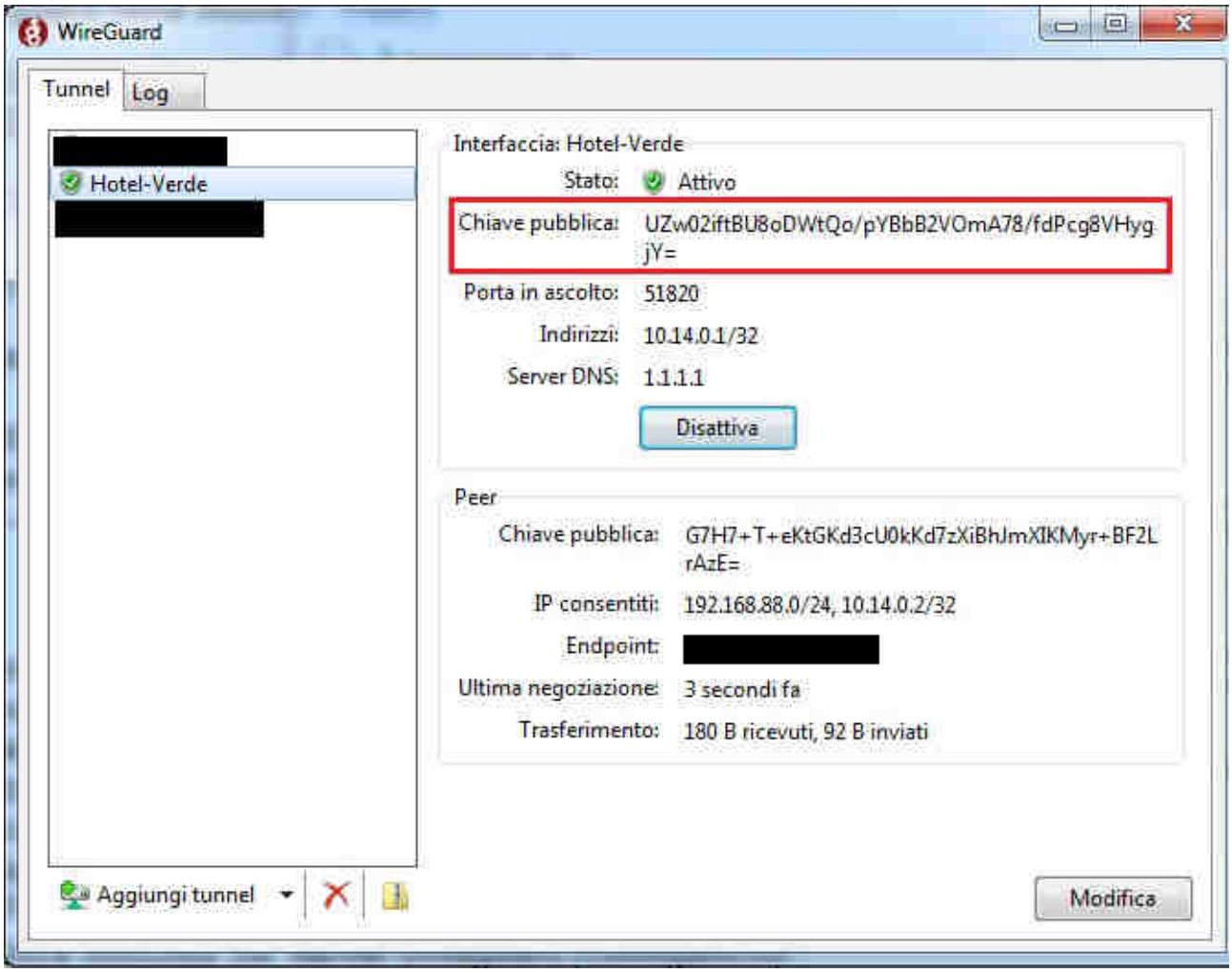
LEGENDA:

Private Key: Esistente *(Non modificarla)*.
ListenPort: Non necessaria *(La si può anche eliminare)*.
IP Address: Indirizzo IP del Client Wireguard *(Obbligatorio)*.
PublicKey: Inserire la PublicKey del Server Wireguard. *(Obbligatorio)*
AllowedIPs: Inserire l'indirizzo IP Tunnel del Server *(Esempio: 10.14.0.1/32)*.
Route Allowed IPs: Crea le route per gli indirizzi IP inseriti in "AllowedIPS". *(Obbligatorio)*
Endpoint Host: Indirizzo IP Pubblico del Server Wireguard *(Obbligatorio).*
Endpoint Port: Porta Pubblica utilizzata dal Server Wireguard *(Obbligatorio).*
Persistent Keep Alive: Espresso in secondi, è il tempo d'intervallo d'invio di un pacchetto al Server. *(Obbligatorio)*

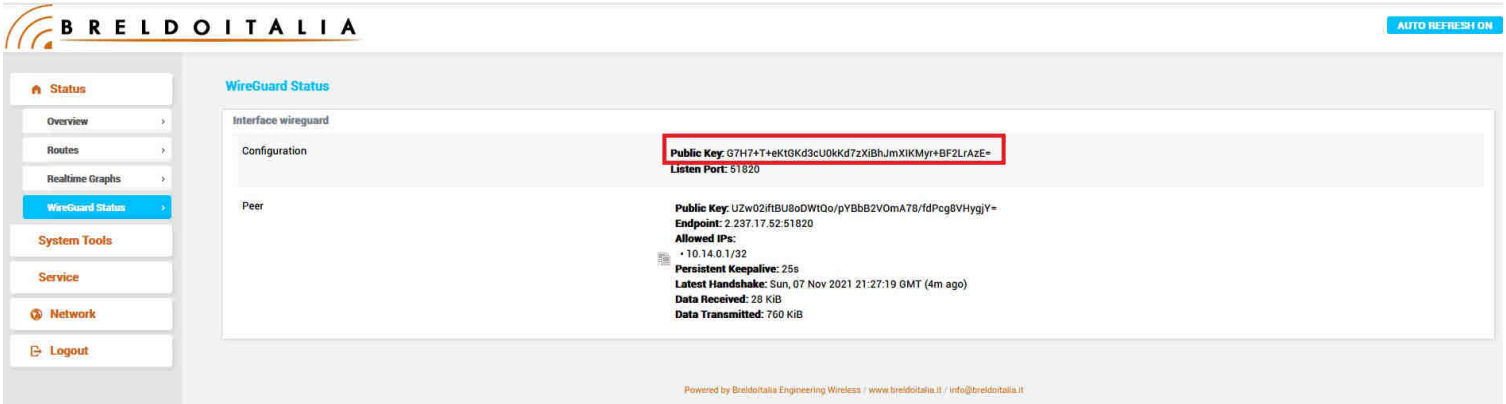
IMPORTANTE:
- Si prega 'd'inserire i dati nei campi dove è presente la voce "Obbligatorio" per permettere il corretto funzionamento VPN.
- La **Privatekey** è già presente sul gateway, si prega di non cancellarla. E' importante mantenerla segreta e non diffonderla a terzi.

DOVE VISUALIZZARE LA PUBLICKEY

-- SOFTWARE WIREGUARD (SERVER)



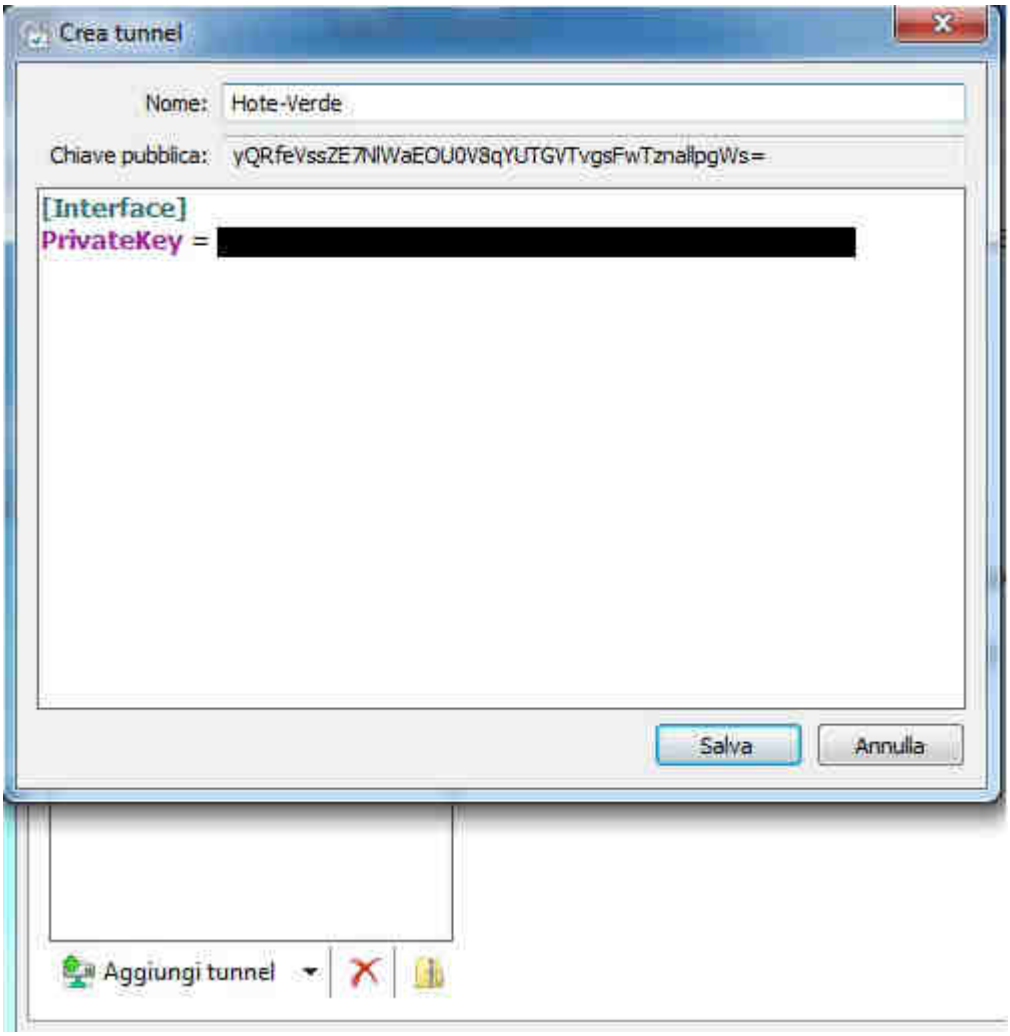
-- FIRMWARE GATEWAY (CLIENT)



TUTORIAL IMMAGINI:

-- SOFTWARE WIREGUARD (SERVER)

1) AGGIUNGI NUOVO TUNNEL

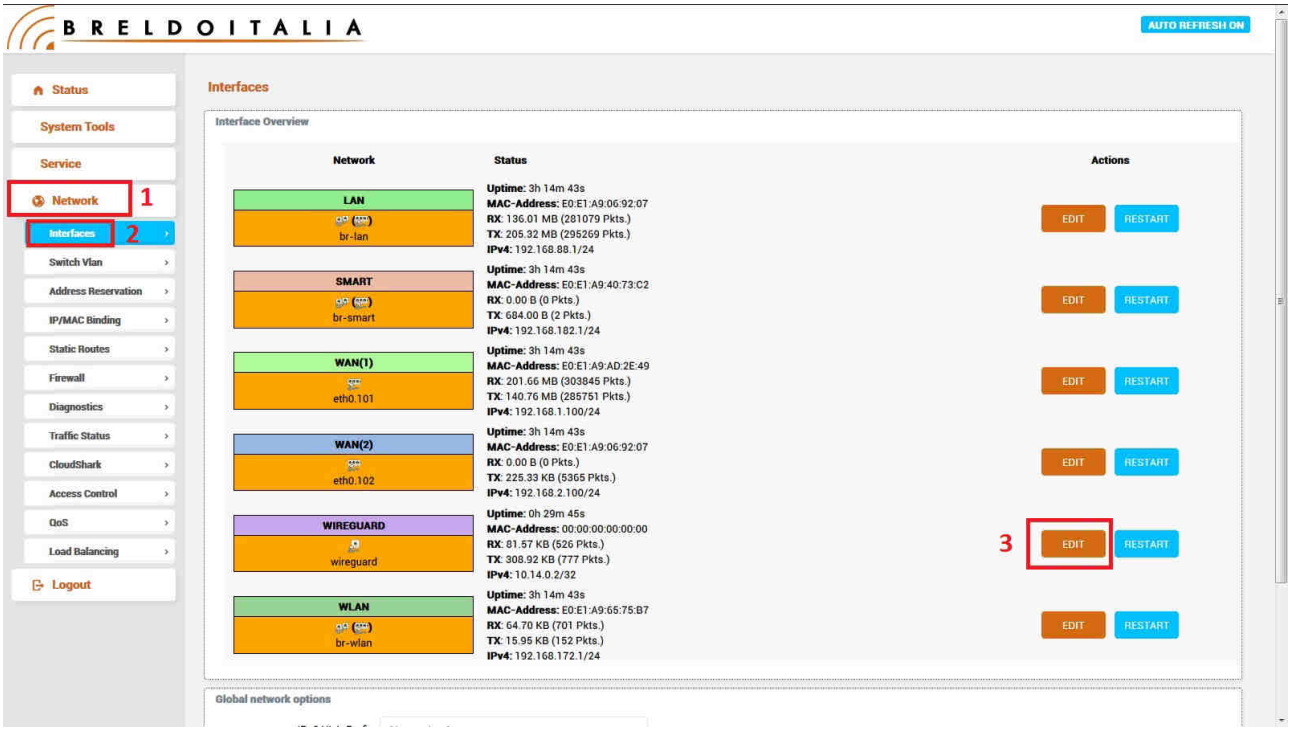


2) INSERIRE I PARAMENTRI NECESSARI PER CREARE IL SERVER VPN

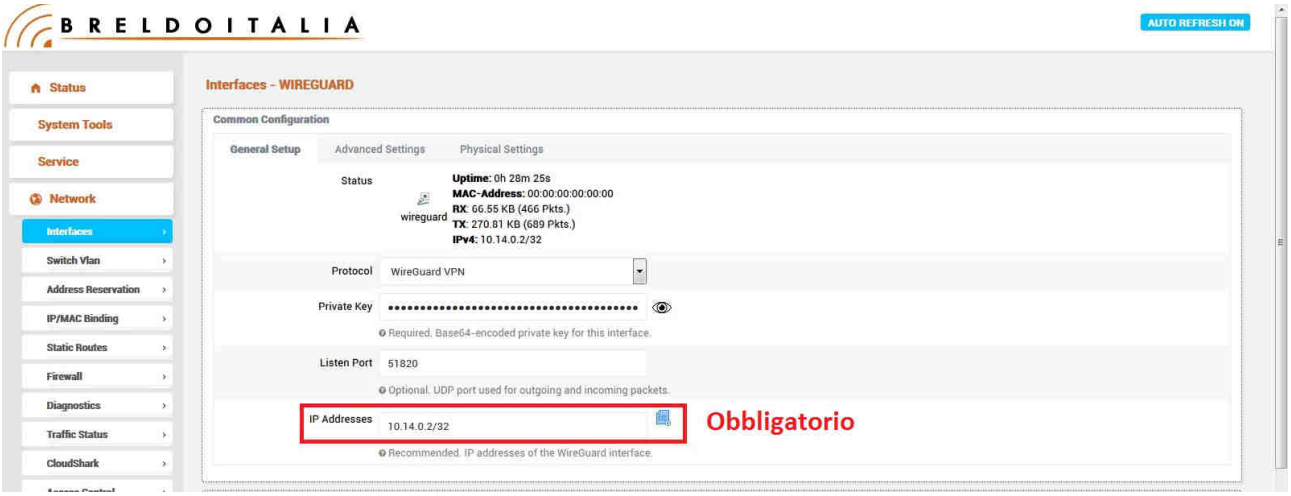
N.B: Si prega di seguire la spiegazione descritta nel capitolo precedente:
CONFIGURAZIONE DEL SOFTWARE WIREGUARD SU WINDOWS (SERVER)

-- FIRMWARE GATEWAY (CLIENT)

1) NETWORK ----> INTERFACES ---> WIREGUARD ---> EDIT



2) INSERIRE L'INDIRIZZO IP TUNNEL DEL CLIENT



3) INSERIRE I PARAMENTRI NECESSARI PER COLLEGARE IL GATEWAY (CLIENT) AL SERVER VPN

N.B: Si prega di seguire la spiegazione descritta nel capitolo precedente:
CONFIGURAZIONE WIREGUARD SU GATEWAY BRELDOITALIA (CLIENT)

4) ATTIVARE L'INTERFACCIA WIREGUARD