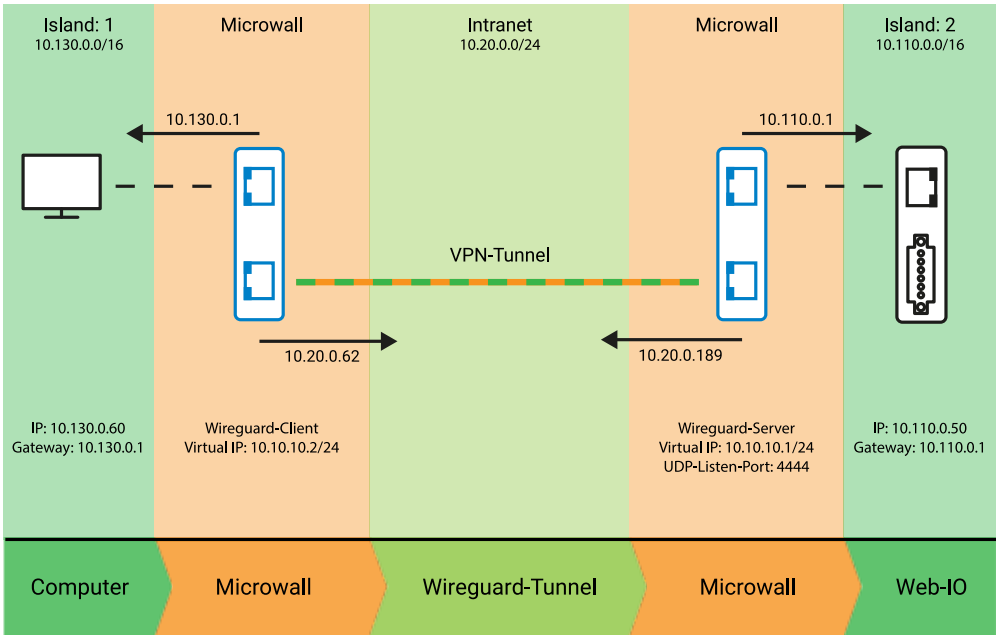
Tutorial:

Tunnel VPN WireGuard tra isole della rete

Tutti gli scenari VPN
Panoramica del prodotto
Panoramica dell'applicazione

L'obiettivo di questo esempio è che un PC nell'isola 1 può accedere attraverso il tunnel VPN al sito Internet (http/80) del Web-IO nell'isola 2. Ogni altra comunicazione tra le due isole non deve essere possibile.



Requisiti:

- I Microwall e i partecipanti delle due isole sono preconfigurati con i summenzionati parametri IP.
- Il Web based management dei due Microwall è raggiungibile nell'Intranet del cliente.

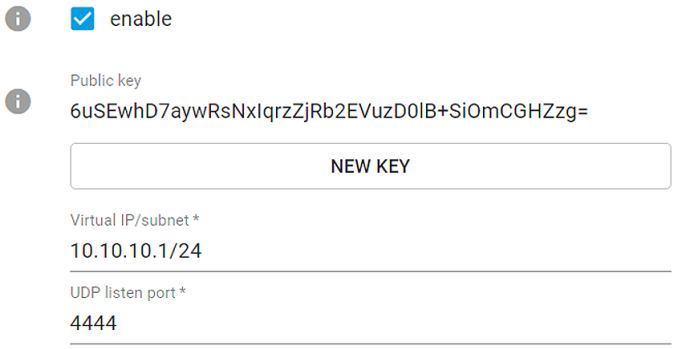
Nota: Nell'esempio qui descritto la configurazione del client VPN avviene per motivi di semplicità attraverso il Microwall. È qui contenuta anche la sensibile private key che autentifica il client. Per ambienti con requisiti di sicurezza aumentati, la produzione della key quindi deve avvenire sul client stesso e solo la public key acritica deve essere ceduta al microwall.

In sintesi i passi necessari:

1. Configurazione del Microwall server VPN
   - Impostare client VPN
   - Impostare regole di autorizzazione
2. Configurazione del Microwall client VPN
3. Test del collegamento VPN

1. Configurazione del Microwall server VPN

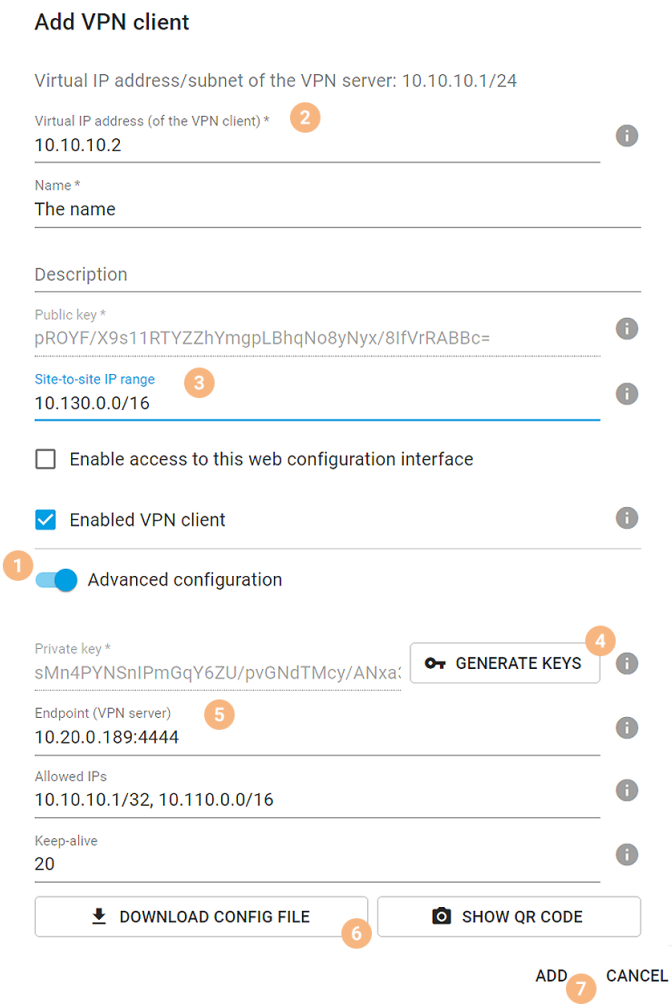
- Avviare nella LAN del cliente un browser e aprire un collegamento al Microwall tramite https che deve funzionare come server VPN (10.20.0.189).
- Navigare alla pagina *"Pagina iniziale"*, al *"Server VPN"* e all' *"Ambiente VPN"*.



- L'"IP virtuale" del server VPN e l'area IP del tunnel VPN può essere in gran parte selezionata liberamente. Tuttavia non può esserci alcun conflitto con le aree IP delle reti coinvolte (isola 1, isola 2, Intranet).
- Sulla porta UDP indicata il server VPN attende collegamenti in entrata dei client VPN.
- Salvare le modifiche e navigare attraverso *"Pagina iniziale"* e *"Server VPN"* a *"Inventario client"*.

Impostare client VPN

- Per l'allestimento di un nuovo client VPN cliccare prima di tutto sul simbolo Più. Per la messa in funzione semplificata qui descritta, nella quale il file di configurazione client viene creato dal Microwall del server, attivare l'interruttore a scorrimento *"Configurazione ampliata"* 1.

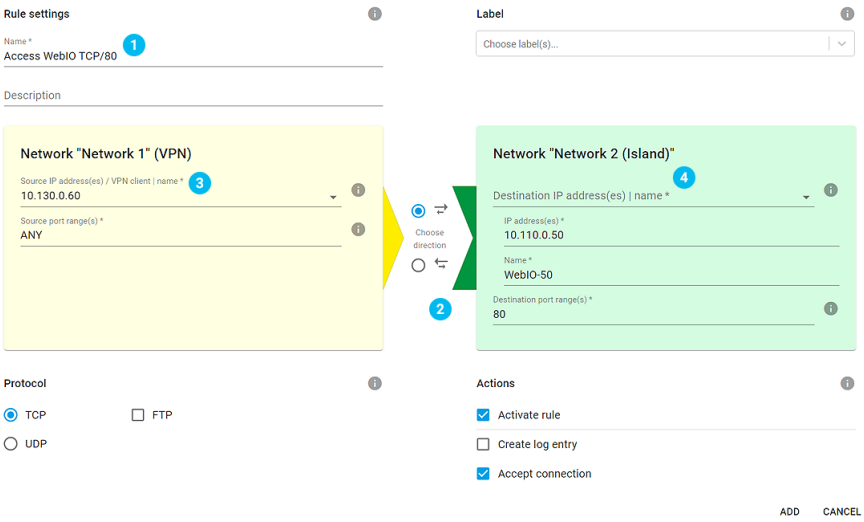


- Assegnare l'indirizzo IP del client VPN 2 dall'area del tunnel VPN e selezionare un nome per il client.
- Inserire alla voce "Area IP site-to-site" 3 la net-ID della rete isola presente nel client VPN rimossa.
- Fare clic su *"GENERA KEYS"* 4. Il Microwall genera una coppia public/private key per il client VPN. La Private-Key sensibile viene visualizzata dalla Microwall esclusivamente per la creazione del file di configurazione del client VPN e solo in questa finestra di dialogo. Non viene salvata.
- Le preimpostazioni del "terminale (server VPN)", "IP autorizzati" e "Keep alive" 5 possono essere riprese invariate in questo esempio applicativo.
- Con il tasto "Scarica file Config" 6 scaricate il file di configurazione e lo salvate. Tenete presente che questo file di configurazione contiene anche la private key riservata per il client VPN. Prendere le misure adeguate per proteggerlo da accessi non autorizzati.

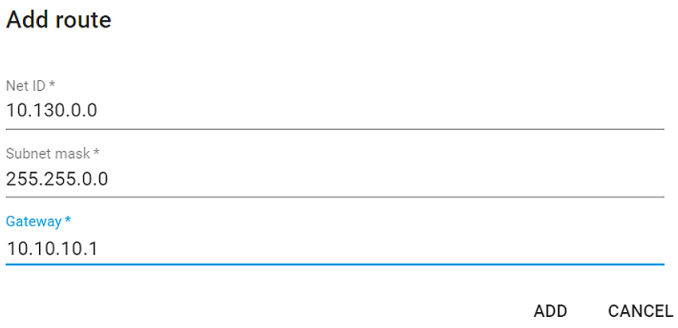
- Dopo il download del file Config cliccare su "Aggiungi" 7 per concludere la creazione del client VPN. Per salvarlo fare clic su "Salva" nella seguente panoramica dei client VPN.

Impostare regole di autorizzazione

- Per l'autorizzazione dell'accesso web del PC nell'isola 1 sui siti Internet del Web-IO nell'isola 2 è necessario impostare una regola di autorizzazione. A tal scopo navigare attraverso la pagina "Home" e "server VPN" alle "regole VPN". Per l'impostazione di una nuova regola di autorizzazione cliccare prima di tutto sul simbolo Più.

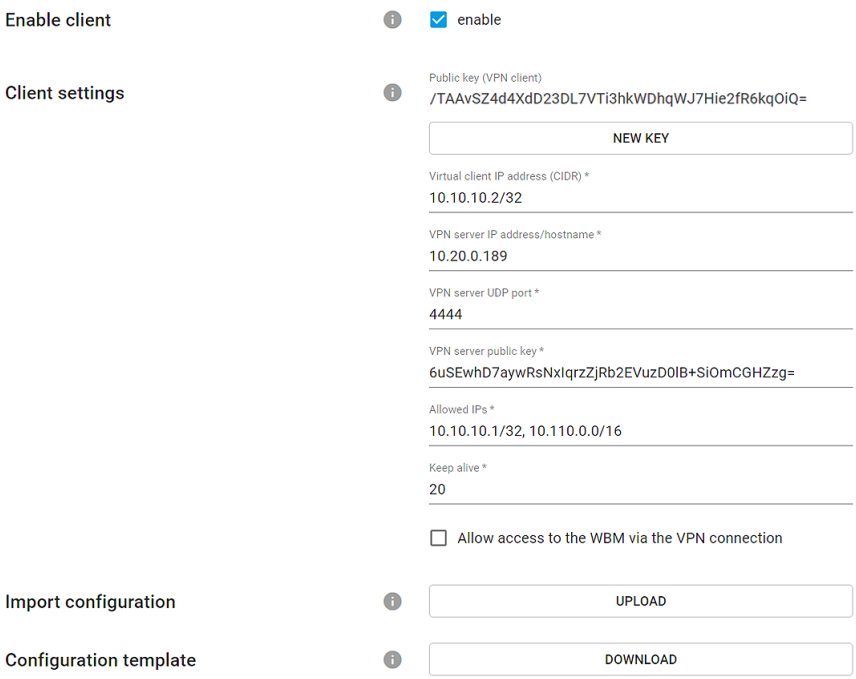


- Assegnare un nome selezionabile liberamente per la regola 1.
- Facendo clic sulla freccia di direzione 2 stabilite che si tratta di un collegamento in entrata nell'isola Web-IO.
- In "IP sorgente" 3 inserite l'indirizzo IP del PC rimosso (10.130.0.60) nell'isola 1 che dovrebbe accedere al Web-IO. Come porta sorgente selezionare "any" perché questa in genere viene determinata dinamicamente dal sistema lato client e non può essere stabilita.
- In "IP destinatario" 4 inserite l'indirizzo IP del Web-IO nell'isola 2 (10.110.0.50). Come "Porta di destinazione" inserite "80" come porta di default per il sito internet del Web-IO.
- Tutte le altre impostazioni rimangono in questo esempio come indicazioni standard. Per chiudere la finestra di dialogo fare clic su "Aggiungi" e poi nell'elenco inventario su "Salva".
- In conclusione è necessario comunicare al Microwall in forma di un itinerario statico che la rete dell'isola 1 è raggiungibile attraverso la connessione VPN. Passare al ramo menu "Rete" in "Impostazioni di base". Per l'impostazione di un nuovo itinerario cliccare in "Itinerari statici" sul simbolo Più. L'itinerario nella rete dell'isola 1 conduce attraverso i dati "Net-ID" e "maschera Subnet" attraverso l'interfaccia VPN 10.10.10.1 ("Gateway") del microwall. Attraverso "Aggiungi" e poi "Salva" chiudere la configurazione del microwall server VPN.

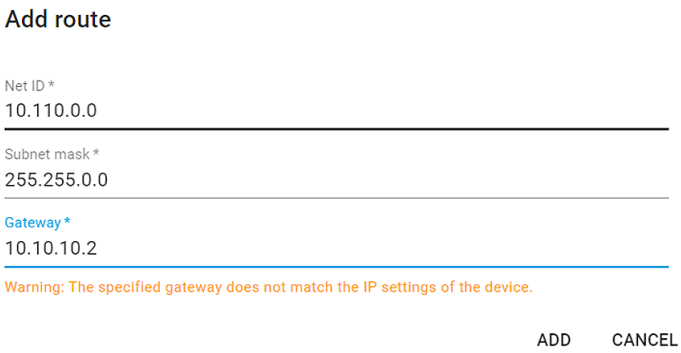


2. Configurazione del Microwall client VPN

- Avviare nella LAN del cliente un browser e aprire un collegamento al microwall che deve funzionare come client VPN (10.20.0.62).
- Navigare attraverso la "Home" alla pagina "client VPN" e fare clic in "Esegui configurazione" su "Carica". Selezionare il file di configurazione creato precedentemente sul server VPN e confermare l'upload.
- Attivare il client VPN, quindi fare clic su "Salva". Sotto l'opzione "Attivare client", dopo breve tempo lo stato del tunnel VPN deve cambiare ad "aperto".

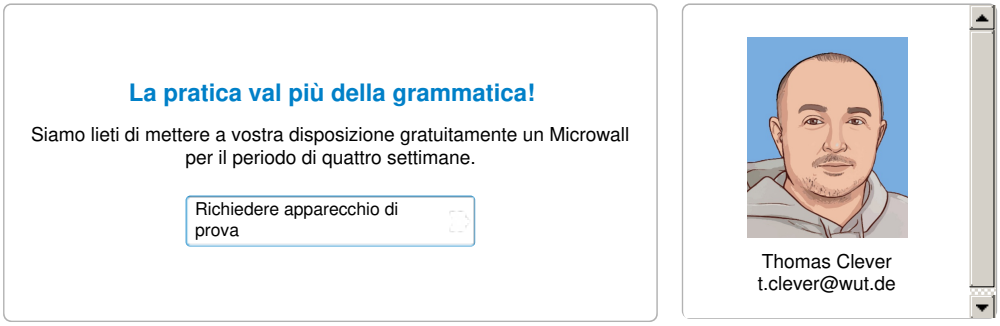


- In conclusione è necessario comunicare al microwall client VPN in forma di un itinerario statico che la rete dell'isola 2 a fianco è raggiungibile attraverso la connessione VPN. Attraverso "Impostazioni di base" passare al ramo del menu "Rete". Per l'impostazione di un nuovo itinerario cliccare in "Itinerari statici" sul simbolo Più. L'itinerario nella rete dell'isola 2 conduce attraverso i dati "Net-ID" e "maschera Subnet" attraverso l'interfaccia VPN 10.10.10.2 ("Gateway") del microwall. Attraverso "Aggiungi" e poi "Salva" chiudere la configurazione del microwall client VPN.



3. Test della connessione VPN

- Adesso è possibile accedere al sito internet del Web-IO 10.110.0.50 nell'isola 2 con un browser sul PC/10.130.0.60. Mediante il tunnel VPN Wireguard, accanto alla crittografia dei dati viene garantita anche la loro integrità e l'autenticazione del client VPN.



Potete contattare telefonicamente i nostri tecnici al numero +49 202/2680-110 (Lun-Ven. 8-17)

W&T
www.WuT.de

Saremo lieti di fornirvi una consulenza personalizzata!

Wiesemann & Theis
GmbH
Porschestr. 12
42279 Wuppertal
Tel.: +49 202/2680-110 (Lun-Ven. 8-17)
Fax: +49 202/2680-265
info@wut.de

errori, nessuna nostra informazione deve essere utilizzata senza essere stata verificata. Vi preghiamo di comunicarci tutti gli errori o gli equivoci che avete rilevato in modo tale che possiamo riconoscerli ed eliminarli quanto prima.

Protezione dei dati