

La VPN con il FRITZ!Box – parte I

Descrizione

Ogni utente di Internet può scambiare dati ed informazioni con qualunque altro utente della rete.

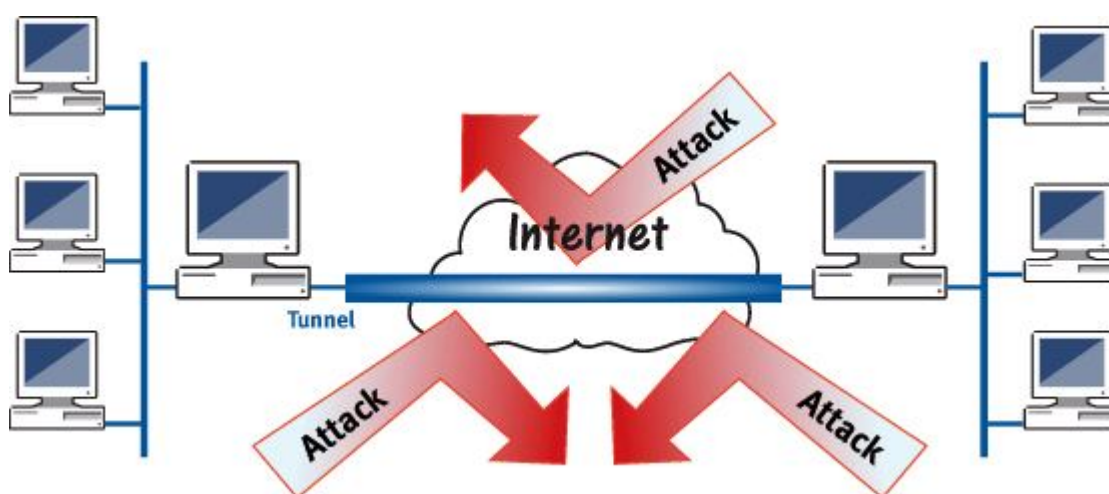
I dati scambiati viaggiano nella nuvola attraverso una serie di connessioni che trasportano le informazioni da un punto all'altro.

Di norma all'interno della nuvola i dati viaggiano senza una reale protezione: se questo approccio può non essere fonte di problemi in molti casi pratici (pensiamo ad esempio alla visualizzazione di un filmato in streaming o alla consultazione di quotidiani online), in altri ambiti si corre il rischio di esporre le proprie informazioni ad attacchi fraudolenti, che potrebbero comprometterne la riservatezza e l'integrità dei dati stessi.

Per questa ragione se abbiamo la necessità, ad esempio, di scambiare dati tra due uffici dislocati su sedi remoti potrebbe essere opportuno utilizzare una connessione sicura e protetta.

Una *VPN*, Virtual Private Network, consiste in una sorta di tunnel in grado di collegare tra loro due o più punti remoti della rete, attraverso una connessione sicura, protetta da crittografia dei dati e con il vantaggio di poter accedere da un punto all'altro del tunnel come se appartenessero alla stessa rete locale.

In questo modo, ad esempio, solo gli utenti della vostra rete aziendale, opportunamente autorizzati, potranno avere accesso alla VPN.



Esistono diverse tecnologie per realizzare un tunnel VPN: AVM ha scelto di implementare questa funzionalità sui FRITZ!Box attraverso il protocollo IPSec standard.

Questo protocollo, di più recente sviluppo, si configura come tra i più sicuri tra le tecniche utilizzate per la realizzazione dei tunnel VPN.

Grazie all'ausilio di IPSec, il FRITZ!Box è in grado di supportare l'accesso remoto di singoli utenti alla rete di un sito tramite tunnel VPN (modalità client-to-site) o di mettere in comunicazione due o più siti con le loro reti (modalità site-to-site), sempre tramite opportuni tunnel VPN.

Per maggiori approfondimenti sulla tecnologia vi suggeriamo di consultare il nostro portale dedicato alle VPN, al seguente:

<http://www.avm.de/de/Service/Service-Portale/Service-Portal/index.php?portal=VPNen>

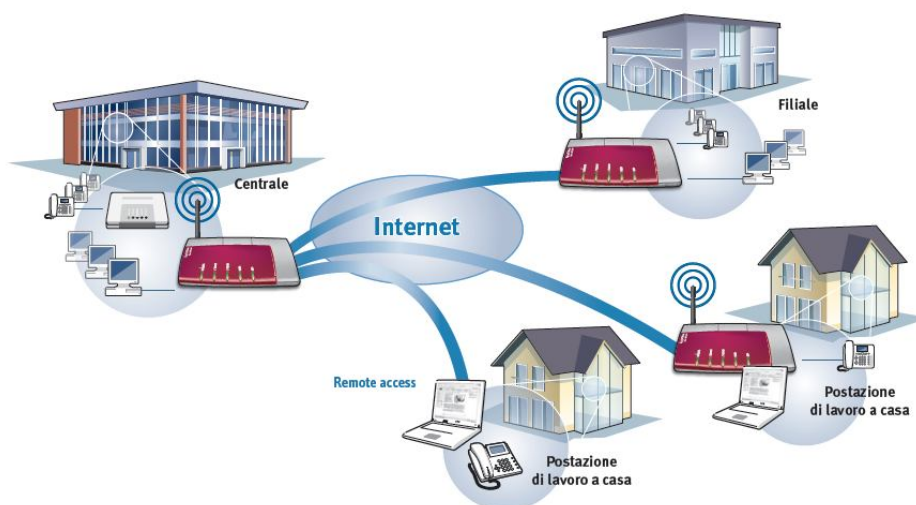
Configurazione

Sebbene supporti un protocollo standard, AVM ha sviluppato per i propri clienti un software molto semplice da utilizzare e disponibile per gli utenti senza costi aggiuntivi, con l'obiettivo di agevolare la configurazione di tunnel VPN con il FRITZ!Box.

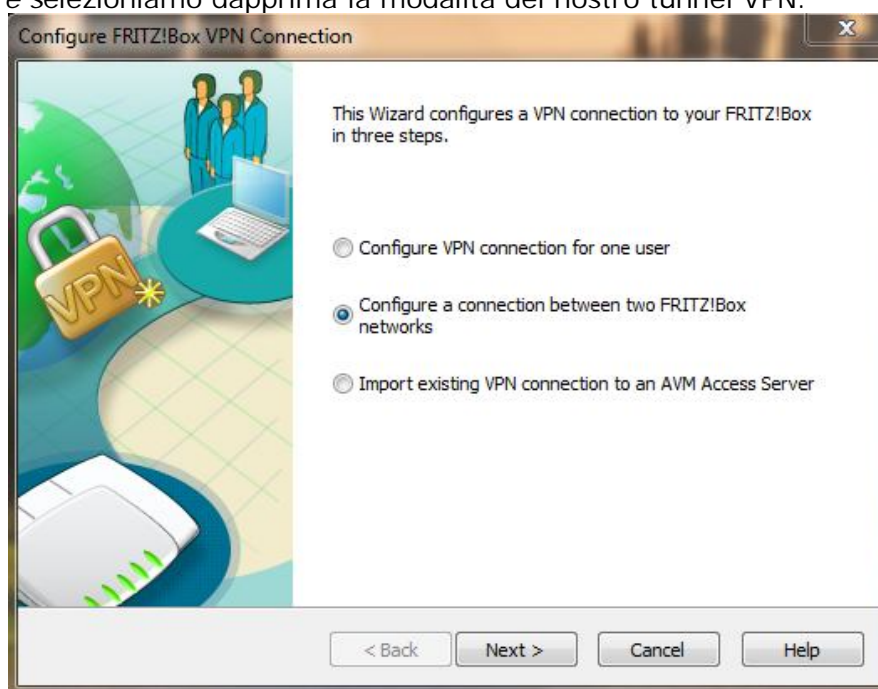
Il programma può essere scaricato tramite il collegamento riportato in precedenza.

Come anticipato sopra, il FRITZ!Box supporta due modalità di VPN: client-to-site e site-to-site. In questa prima parte vediamo come configurare i dispositivi per utilizzare una VPN tra due siti, ad esempio tra due uffici della stessa società.

Nella configurazione di esempio che vi proponiamo, supponiamo che un sito sia dotato di un indirizzo IP pubblico dinamico con la registrazione al servizio Dynamic DNS (di cui abbiamo trattato in un'altra mini-guida), mentre l'altro di un indirizzo IP pubblico statico (cioè assegnato a tempo indeterminato).

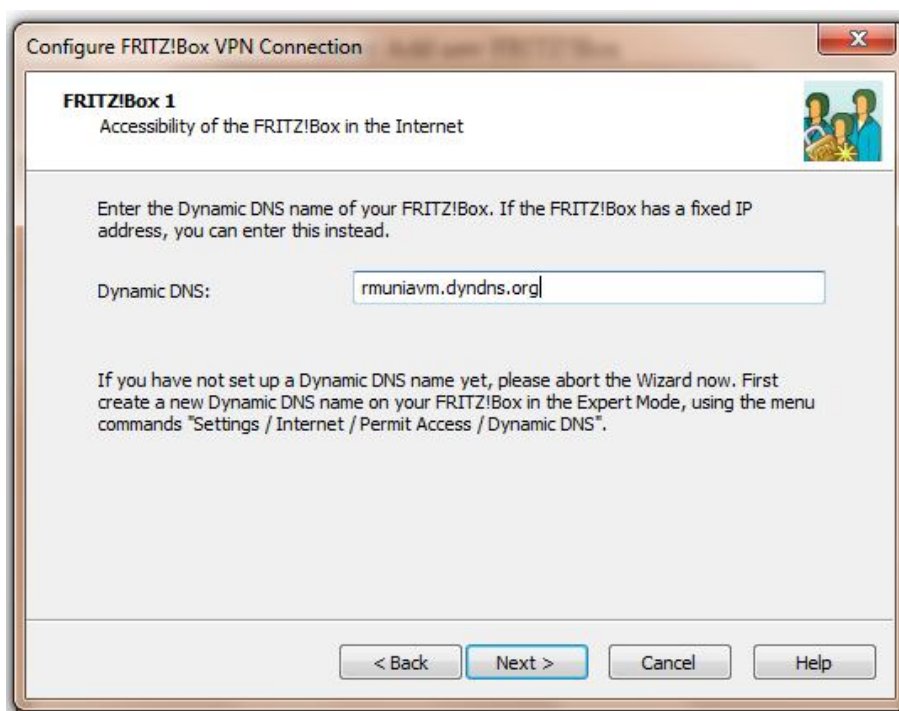


Avviamo dunque il software per la configurazione delle VPN: *Configure FRITZ!Box VPN Connection* e selezioniamo dapprima la modalità del nostro tunnel VPN:

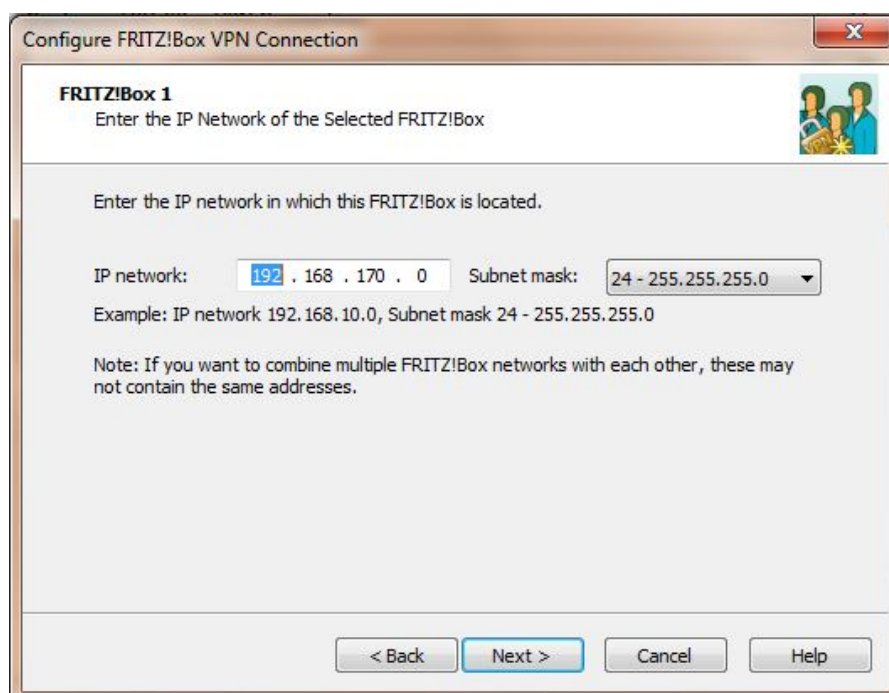


La VPN con il FRITZ!Box

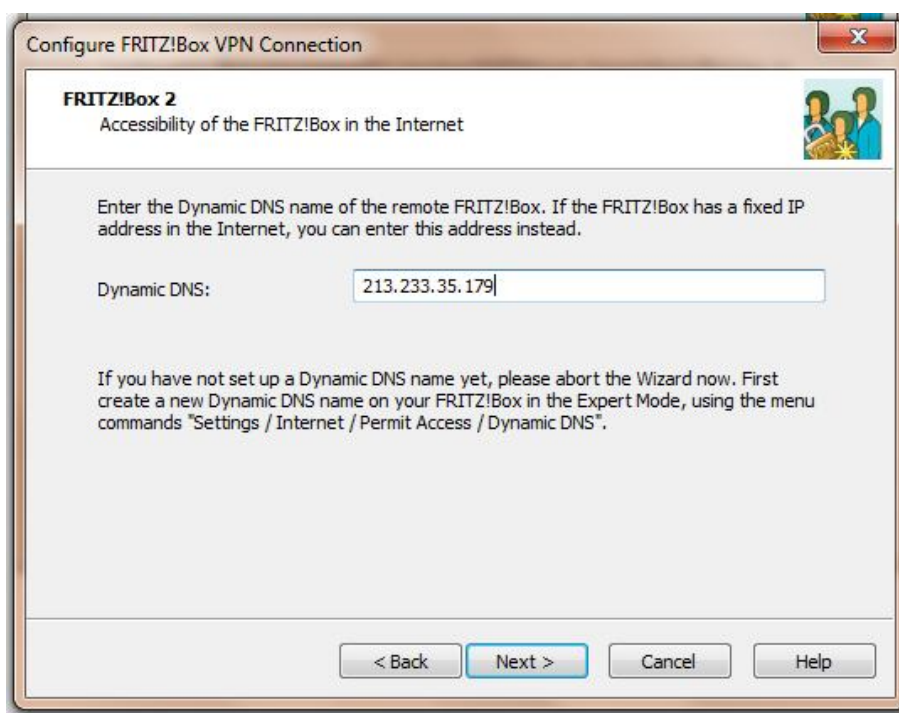
Il software di configurazione si comporta come una sorta di assistente alla configurazione, proponendo passo dopo passo le informazioni da inserire. Procediamo quindi inserendo il nome DNS del sito A, precedentemente registrato:



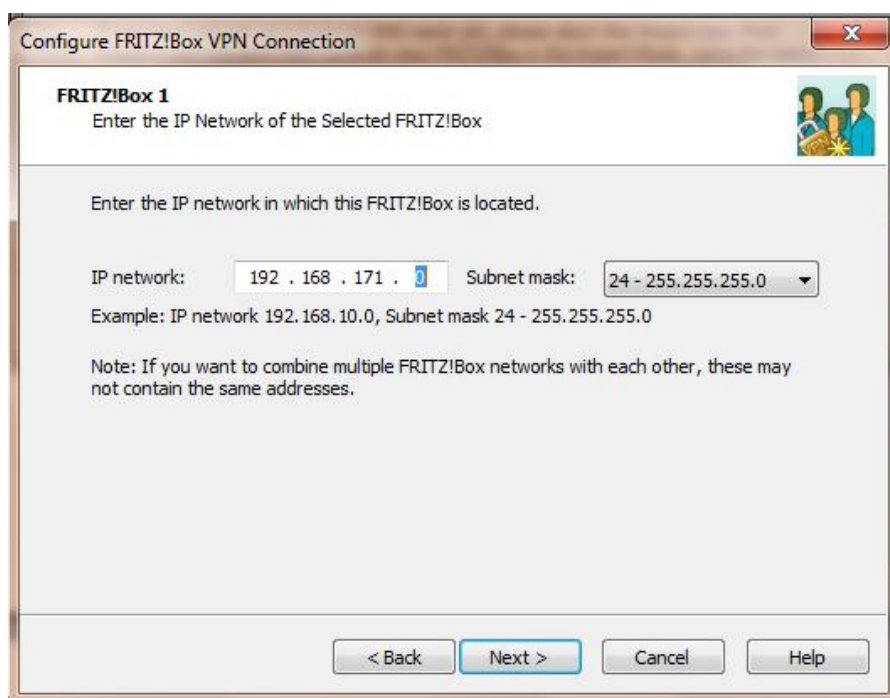
Configuriamo quindi le rete locale della sede A, inserendo l'indirizzo IP privato della rete e la maschera della sottorete:



Passiamo dunque alla configurazione del sito B, inserendo in questo caso l'indirizzo IP pubblico



Successivamente, configuriamo la rete privata del sito B con le informazioni analoghe a quelle inserite per il sito A:



Nota: nella scelta del piano di indirizzamento privato delle due sedi è bene tenere a mente che non possiamo utilizzare la rete privata di default 192.168.178.0 utilizzata di norma dai FRITZ!Box, e che le due reti private devono avere piani di indirizzamento diversi.

A questo punto, completiamo la configurazione salvando i due file che il software ha prodotto e che dovranno essere successivamente importati nei FRITZ!Box presenti nei due siti.

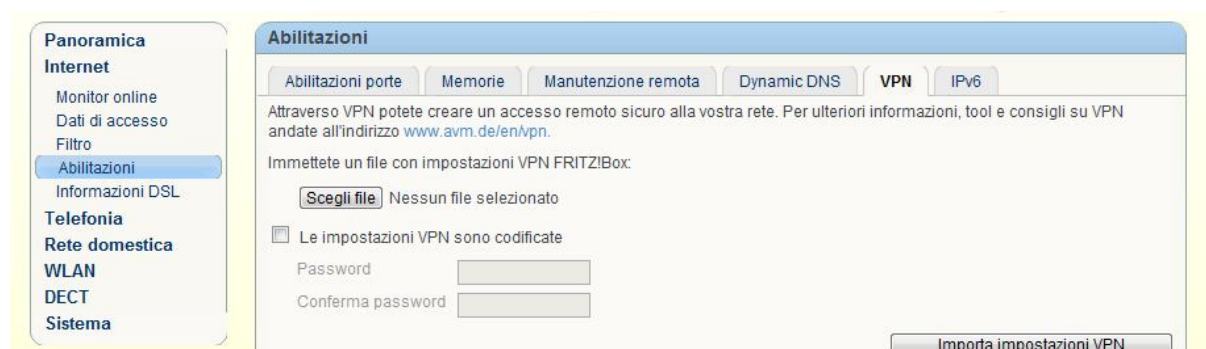
In fase di salvataggio è possibile proteggere la configurazione della VPN inserendo un'apposita password.

Utilizzo

Completata la fase di configurazione, non resta che applicarla ai dispositivi che operano da *access gateway* nei nostri due siti A e B.

Per fare questo entriamo nella interfaccia grafica di utente (GUI) del FRITZ!Box del sito A, utilizzando un browser.

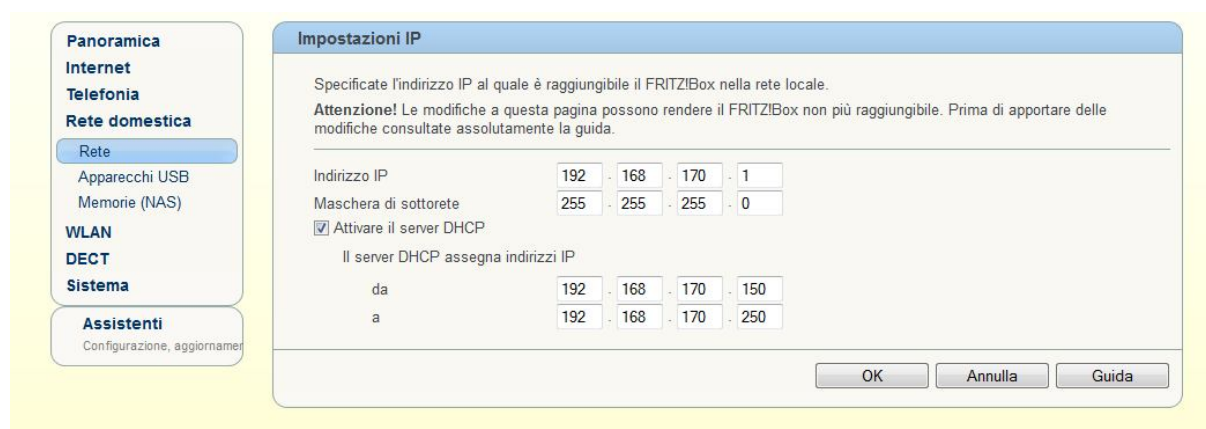
Accediamo quindi al menu "Internet" → "Abilitazioni" → "VPN".



Selezioniamo il file in precedenza salvato per il sito A, inseriamo la password per decriptare, nel caso, il file di configurazione e clicchiamo infine su **Importa impostazioni VPN**.

Questo passaggio va ripetuto in maniera del tutto analoga per il FRITZ!Box presente nel sito B.

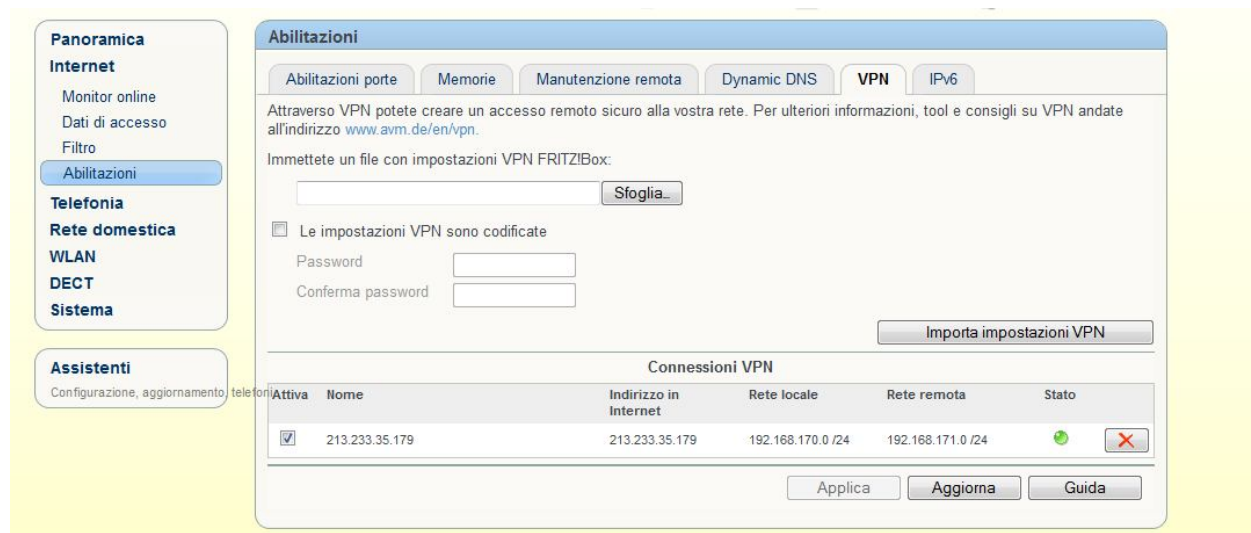
Poiché in fase di configurazione della VPN è stata indicata anche una rete privata specifica per ciascun sito, per rendere effettiva la configurazione della VPN è necessario modificare opportunamente le impostazioni IP dei due access gateway, come nell'esempio illustrato nella figura sotto.



La VPN con il FRITZ!Box

Accediamo dunque nella sezione "Rete domestica" → "Rete" → "Impostazioni IP" della GUI e modifichiamo l'indirizzo IP della rete locale: questa operazione va effettuata per ciascun sito.ⁱ

Ultimata l'attivazione della funzionalità con le modifiche alla rete locale, possiamo controllare che la VPN sia attiva e funzionante tramite il pannello presente nel menu "Internet" → "Abilitazioni" → "VPN" o nella sezione "Panoramica" del prodotto.



Per rendere funzionante la VPN potrebbe essere necessario, ad esempio, provare ad accedere ad un terminale da una sede remota all'altra. La VPN si attiverà automaticamente con il traffico tra le due sedi remote

Nell'esempio riportato nella figura sotto, effettuiamo un comando *ping* di test

```
C:\windows\system32\cmd.exe
Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : fritz.box
Link-local IPv6 Address . . . . . : fe80::f9bb:48e1:17e4:5437%15
IPv4 Address. . . . . : 192.168.170.20
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.170.1

Ethernet adapter Local Area Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : fritz.box

Tunnel adapter isatap.{A87C9C6B-514A-4C3E-9AB5-65588BF82D4A}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Tunnel adapter isatap.fritz.box:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : fritz.box

Tunnel adapter Teredo Tunneling Pseudo-Interface:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2001:0:4137:9e76:18df:3d0:3f57:55eb
Link-local IPv6 Address . . . . . : fe80::18df:3d0:3f57:55eb%17
Default Gateway . . . . . :

C:\Users\fpatri>ping 192.168.171.1

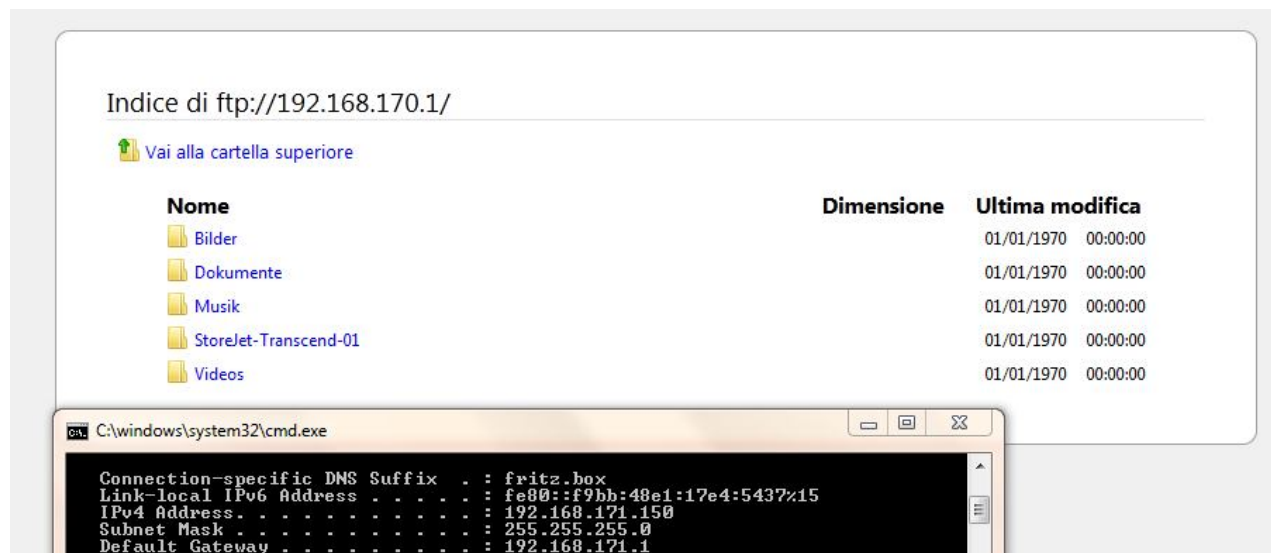
Pinging 192.168.171.1 with 32 bytes of data:
Reply from 192.168.171.1: bytes=32 time=14ms TTL=63
Reply from 192.168.171.1: bytes=32 time=13ms TTL=63
Reply from 192.168.171.1: bytes=32 time=15ms TTL=63
Reply from 192.168.171.1: bytes=32 time=13ms TTL=63

Ping statistics for 192.168.171.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 15ms, Average = 13ms
```

La VPN con il FRITZ!Box

Il risultato mostrato è che un computer del sito A, con indirizzo IP 192.168.170.1 effettua con successo un ping verso l'access gateway del sito B, il cui indirizzo privato è 192.168.171.1

Un altro esempio di utilizzo pratico è riportato nell'immagine sotto.



In questo caso, un PC del sito B, con indirizzo IP 192.168.171.150, accede via ftp ad un NAS configurato nel sito A (per approfondimenti vi invitiamo a leggere la mini-guida NAS e Multimedia), come farebbe un qualunque altro PC appartenente alla rete locale del sito A.

Nota: su ogni FRITZ!Box è possibile configurare fino ad 8 tunnel VPN.

Inoltre, utilizzando il protocollo IPsec standard, il file di configurazione che viene prodotto dal software di AVM per le VPN può essere eventualmente editato con un file editor e quindi successivamente importato anche in dispositivi di terze parti che supportano questo standardⁱⁱ.

In questo modo risulta possibile instaurare dei tunnel VPN basati su IPsec anche utilizzando un FRITZ!Box in combinazione con access gateway di terze parti.



La VPN con il FRITZ!Box

Vi ricordiamo che la funzionalità è disponibile per:

Prodotto	Dati	Voce
FRITZ!Box WLAN 3270	Si	-
FRITZ!Box Fon WLAN7390	Si	Si
FRITZ!Box Fon WLAN7330	Si	Si
FRITZ!Box Fon WLAN7270	Si	Si

Link Video:

http://www.avm.de/de/Service/FRITZ_Clips/start_clip.php?clip=fritz_clip_vpn_en

ⁱ Il cambio di indirizzo IP potrebbe causare una disconnessione temporanea in attesa che il DHCP Server rilasci al vostro PC un nuovo indirizzo.

ⁱⁱ Adattamenti successivi potrebbero essere necessari per una nuova importazione del file nel FRITZ!Box