Istruzioni configurazione e utilizzo servizio VPN per utenti TIFPA/UniTN

Il servizio VPN si basa su crittografia SSL e consente l'accesso da postazioni internet alle risorse interne della rete d'Ateneo e ad alcuni servizi dedicati TIFPA. Inoltre, transita attraverso il tunnel anche il traffico diretto verso i server nazionali di licenza per i software di cui il TIFPA è sottoscrittore (Mathematica, Autodesk, Ansys). Ciò permette di utilizzare tali software anche quando non ci si trova connessi alla rete INFN.

Per la configurazione e l' uso è necessario installare il client Pulse Secure, visitare la sezione corrispondente al proprio sistema operativo:

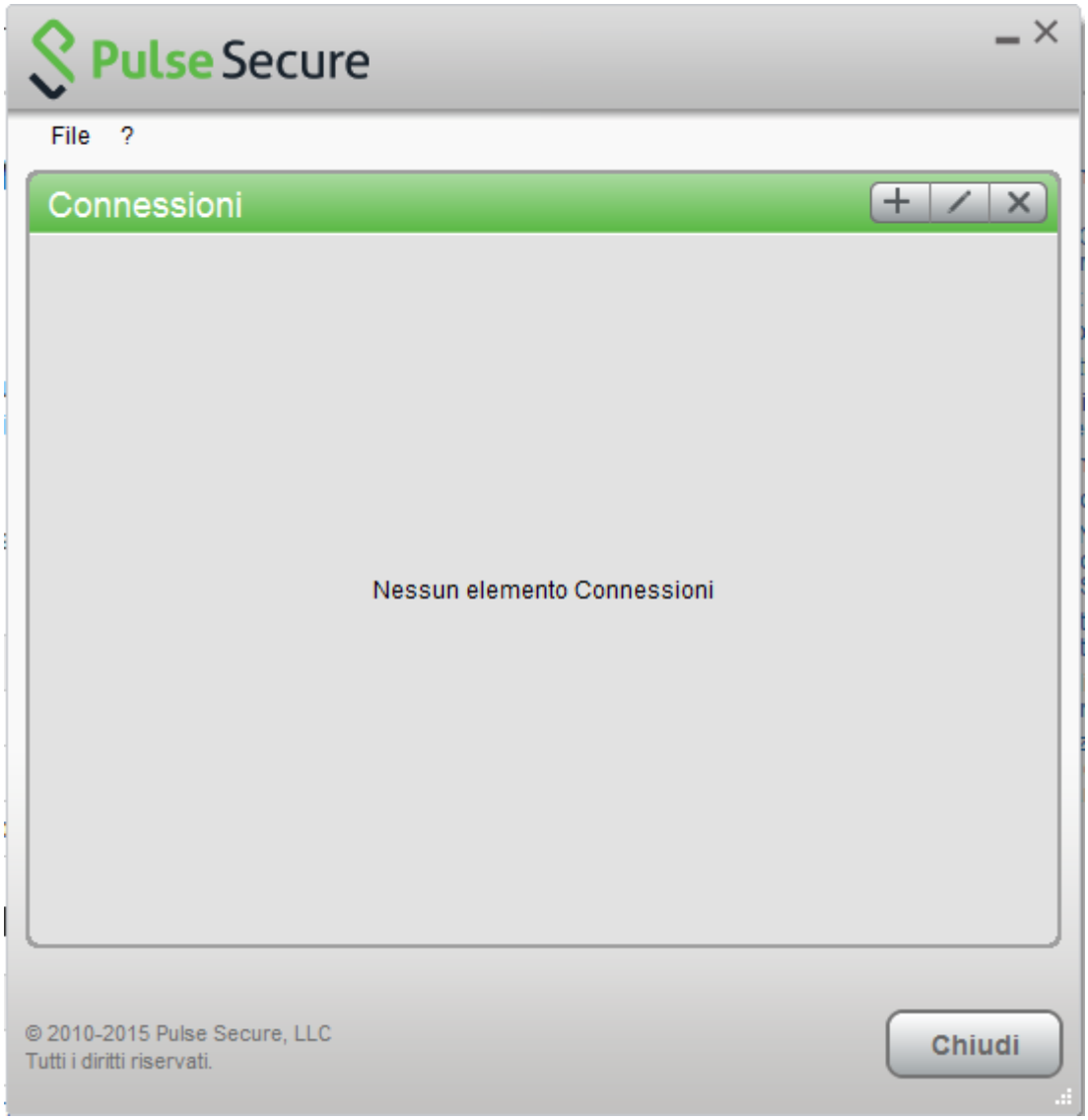
Sistema Operativo	Client consigliato	Istruzioni
Windows, Macosx	Pulse Secure	Pulse Secure Desktop
Linux	Pulse Secure	Pulse Secure Linux
Dispositivi Mobili (Smartphone & Tablet)	Pulse Secure	Pulse Secure Mobile

MACOSX, Windows (Pulse Secure)

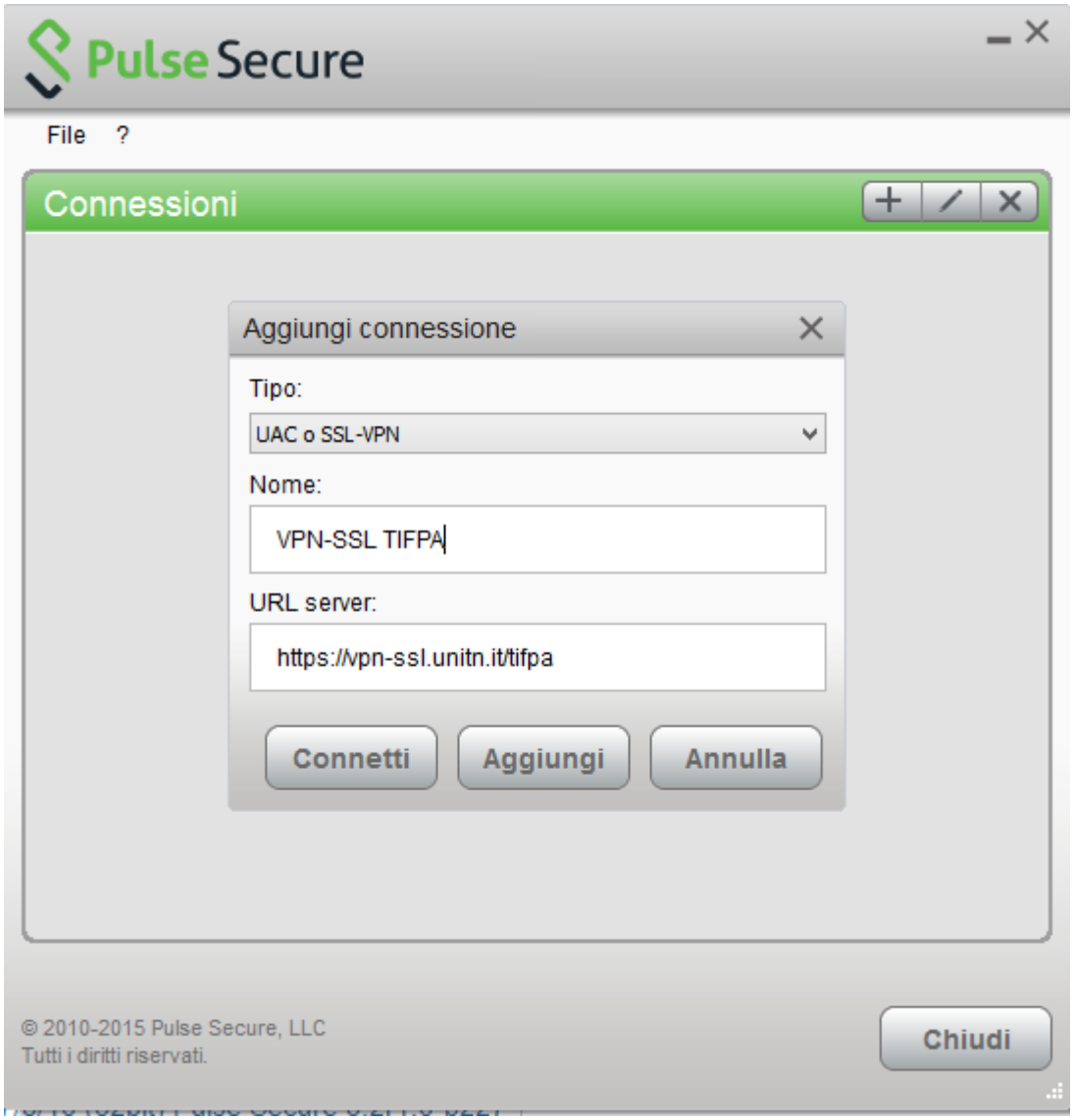
Junos Pulse Download
MACOSX (>= 10.6) Pulse Secure 5.2r1.0-b227
Windows XP, Vista and Windows 7/8/10 (32bit) Pulse Secure 5.2r1.0-b227
Windows XP, Vista and Windows 7/8/10 (64bit) Pulse Secure 5.2r1.0-b227

Per Mac: Attenzione!!! Se viene usato il client Safari: al file .dmg viene appeso un'estensione .exe che va rimossa per poter ulilizzare il file, oppure effettuare un salva con nome “pulse.dmg”. Per client Firefox o Chrome non sono state riscontrate anomalie nel download.

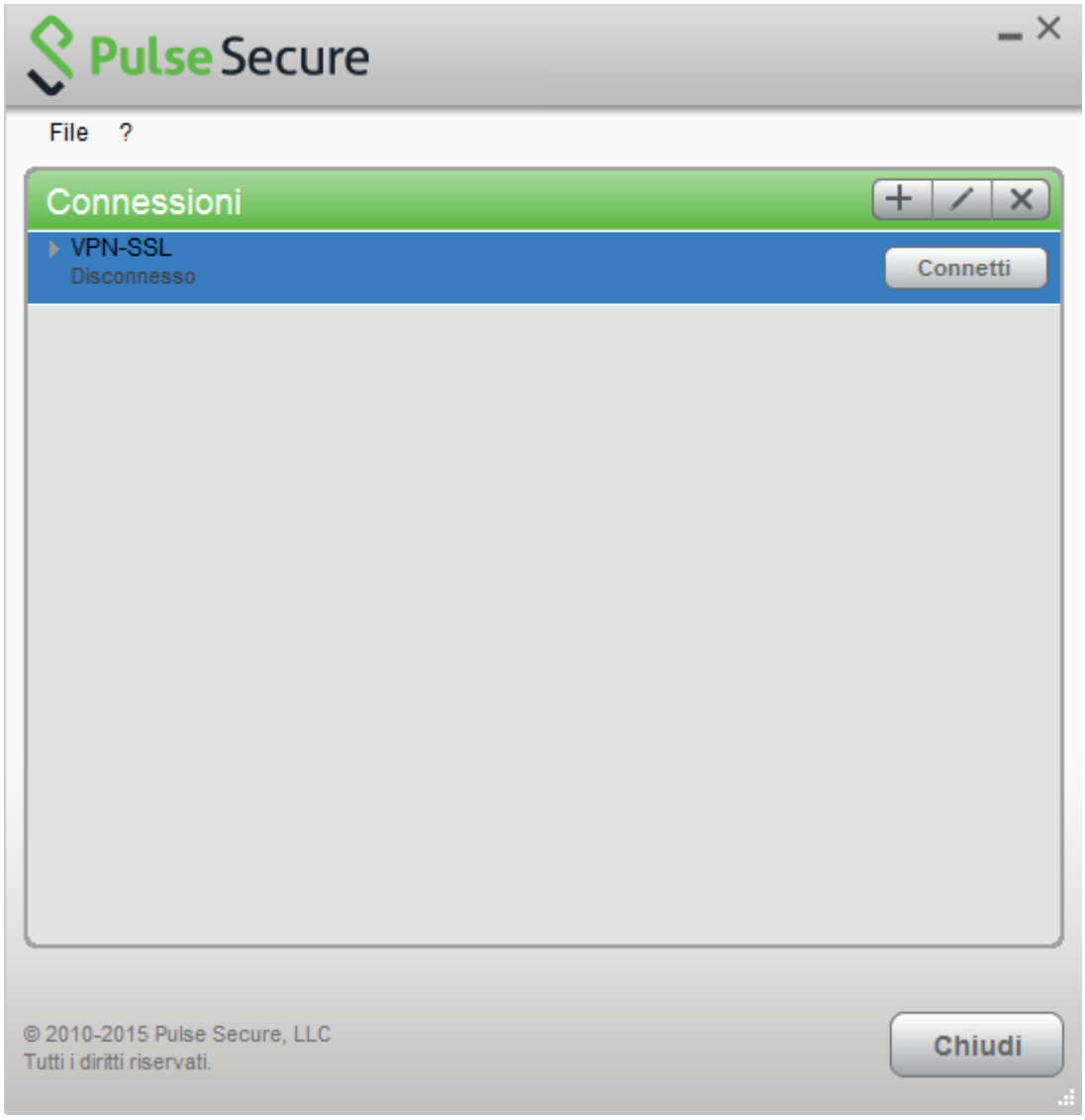
Dopo averla installata, lanciare l' Applicazione Pulse Secure, appare la schermata principale:



Creare quindi una nuova connessione cliccando su '+' e inserendo i parametri corretti:

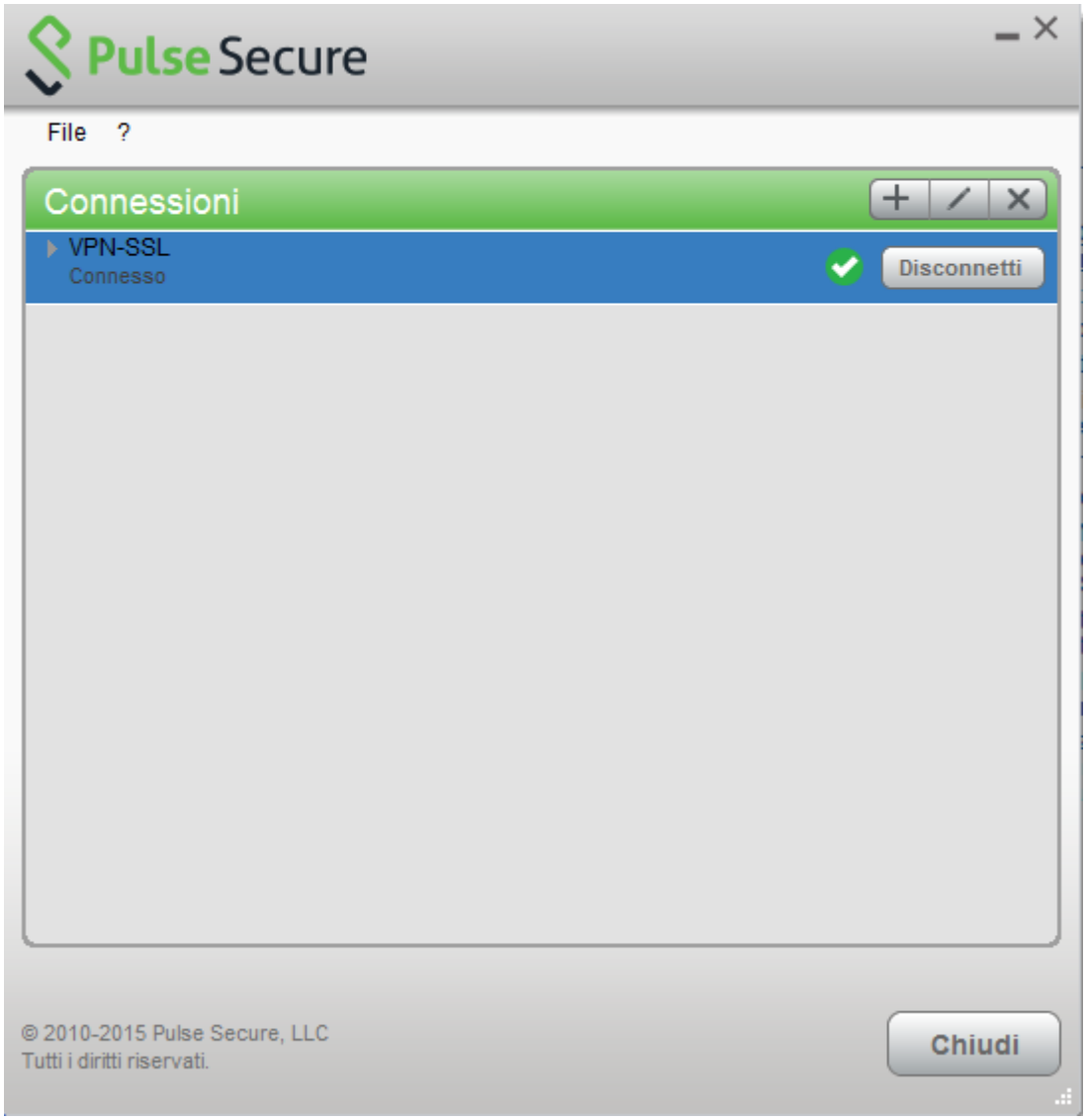


Per far partire la connessione cliccare su <Connetti>



Inserire nome utente (@unitn.it) e password ed eventualmente memorizzare le credenziali

La connessione è stabilita, per disconnettere cliccare su <Disconnetti>



Notare l'icona di Pulse Secure nell' area di notifica

E' possibile visualizzare una finestra di stato da File→Connessioni→Dettagli avanzati di connessione...

Linux Pulse Secure Client

Pulse Secure per Linux Download
Linux CentOS Pulse Secure 8.1r7.0-b41041
Linux Ubuntu (> 14.04) Pulse Secure 8.1r7.0-b41041

Scaricare il pacchetto, aprire un terminale e installare Pulse Secure con il comando:

Debian-based Linux (ad esempio Ubuntu):

dpkg -i <package name>

RPM-based Linux (ad esempio CentOS):

rpm -ivh <package name>

Per esempio, se Pulse Secure è stato salvato in /$HOME/Downloads su Ubuntu, il comando di installazione sarà:

```
sudo dpkg -i /$HOME/Downloads/ps-pulse-linux-8.1r7.0-b41041-ubuntu-debian-installer.deb
```

Lo script di installazione eventualmente indicherà quali pacchetti vanno installati sul sistema (in questo caso libc6-i386 e lib32z1):

```
user@host:~$ sudo dpkg -i /$HOME/Downloads/ps-pulse-linux-8.1r7.0-b41041-ubuntu-debian-installer.deb
```

```
(Reading database ... 154703 files and directories currently installed.)
Preparing to replace pulse 8.1 (using
.../ps-pulse-linux-8.1r7.0-b41041-ubuntu-debian-installer.deb) ...
Unpacking replacement pulse ...
Setting up pulse (8.1) ...
 Please execute below commands to install missing dependent packages
apt-get install libc6-i386
apt-get install lib32z1
Please refer /usr/local/pulse/README for instructions to launch the Pulse
Client
```

E' poi necessario scaricare il certificato della VPN con il comando:
NB: questa operazione va effettuata SOLO una volta

```
user@host:~$ openssl s_client -connect vpn-ssl.unitn.it:443 -showcerts <
/dev/null 2> /dev/null | openssl x509 -outform der > /$HOME/Downloads/vpn-
ssl.crt
```

Oppure scaricare il certificato da qui: vpn-ssl.zip e scompattarlo con:

```
user@host:~$ unzip /%HOME/Downloads/vpn-ssl.zip
```

A questo punto possiamo lanciare il client con il comando (ci verrà chiesta la password UniTN):

```
/usr/local/pulse/PulseClient.sh -h vpn-ssl.unitn.it -u nome.cognome@unitn.it
-f /usr/local/pulse/vpn-ssl.crt -U https://vpn-ssl.unitn.it/tifpa -r AR-
unitn-ldap-ad-tifpa
```

Ad Esempio:

```
user@host:~$ /usr/local/pulse/PulseClient.sh -h vpn-ssl.unitn.it -u
username@unitn.it -f /$HOME/Downloads/vpn-ssl.crt -U
https://vpn-ssl.unitn.it/tifpa -r AR-unitn-ldap-ad-tifpa
Reading package lists... Done
Building dependency tree
Reading state information... Done
lib32z1 is already the newest version.
libc6-i386 is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 557 not upgraded.
executing command : /usr/local/pulse/pulsesvc -h vpn-ssl.unitn.it -u
username@unitn.it -f /$HOME/Downloads/vpn-ssl.crt -U
https://vpn-ssl.unitn.it/tifpa -r AR-unitn-ldap-ad-tifpa
VPN Password:
```

Dopo pochi secondi la connessione viene stabilita ed è possibile monitorare lo stato da un' altra finestra terminale con il comando:

```
user@host:~$ /usr/local/pulse/PulseClient.sh -S

Connection Status :
```

```
        connection status : Connected
        bytes sent : 1722
        bytes received : 2586
        Connection Mode : ESP
        Encryption Type : AES128/SHA1
        Comp Type : None
        Assigned IP : 10.31.110.80
```

Per terminare la connessione digitare il comando:

```
user@host:~$ /usr/local/pulse/PulseClient.sh -K
```

Riferimenti - Documentazione ufficiale:
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40126/?q=linux&l=en_US&fs=Search&pn=1&atype=

Dispositivi Mobili

REQUISITI

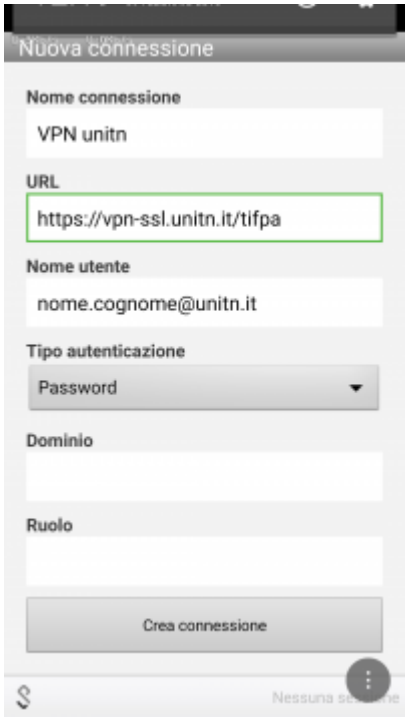
- iPhone, iPod Touch, iPad
- Android devices 4.0 o superiori
- Windows Mobile 6.5

ISTRUZIONI: (screenshots relativi alla versione Android 5)

- installare l'app “Pulse Secure” dall' App Store o da Google Play
- avviare l' applicazione “Pulse Secure”

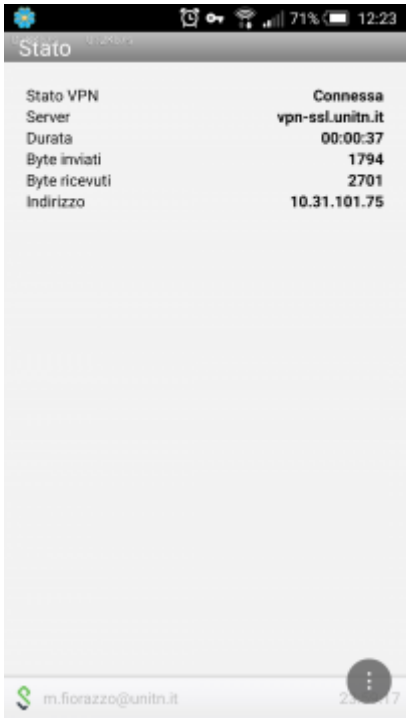
- Creare una nuova connessione inserendo:

- “Nome connessione” (a scelta)
- “URL”: https://vpn-ssl.unitn.it/tifpa
- “Nome utente” (nella forma nomeutente@unitn.it)
- toccare su “Crea connessione”



- toccare su “Connetti”, inserire la password e selezionare “Sign In” (eventualmente accettare la richiesta di considerare l' applicazione attendibile)

- a questo punto viene stabilita la connessione, verificabile tramite un tocco su “Stato”



- al termine della sessione, per terminare la connessione, toccare su “Disconnetti”

Caratteristiche servizio vpn-ssl

Indirizzo IP assegnato al client

Ai client connessi in vpn viene assegnato un ip nel range che va da 10.31.110.10 a 10.31.110.254

Funzionalità "split-tunnel"

La connessione VPN prevede che il traffico diretto agli IP dell'Ateneo transiti lungo il tunnel VPN mentre il traffico verso altre reti (p.e. internet) esce dalla connessione standard del client (p.e. ADSL di casa). Inoltre, transita attraverso lo split-tunnel anche il traffico diretto verso i server nazionali di licenza per i software di cui il TIFPA è sottoscrittore (Mathematica, Autodesk, Ansys). Ciò permette di utilizzare tali software anche quando non ci si trova connessi alla rete INFN.

NB: il routing NON viene modificato per le connessione già attive al momento della connessione vpn

Requisiti Firewall lato utente

Il traffico VPN è crittografato in SSL ed usa la porta destinazione TCP 443. Per la modalità ESP (che aumenta le prestazioni) è necessario aprire la porta destinazione UDP 4500.