

LNF-06/02 (NT)
15 Gennaio 2006

VPN AT LNF – USER GUIDE

Angelo Veloce

INFN-Laboratori Nazionali di Frascati Via E. Fermi 40, I-00044 Frascati, Italy

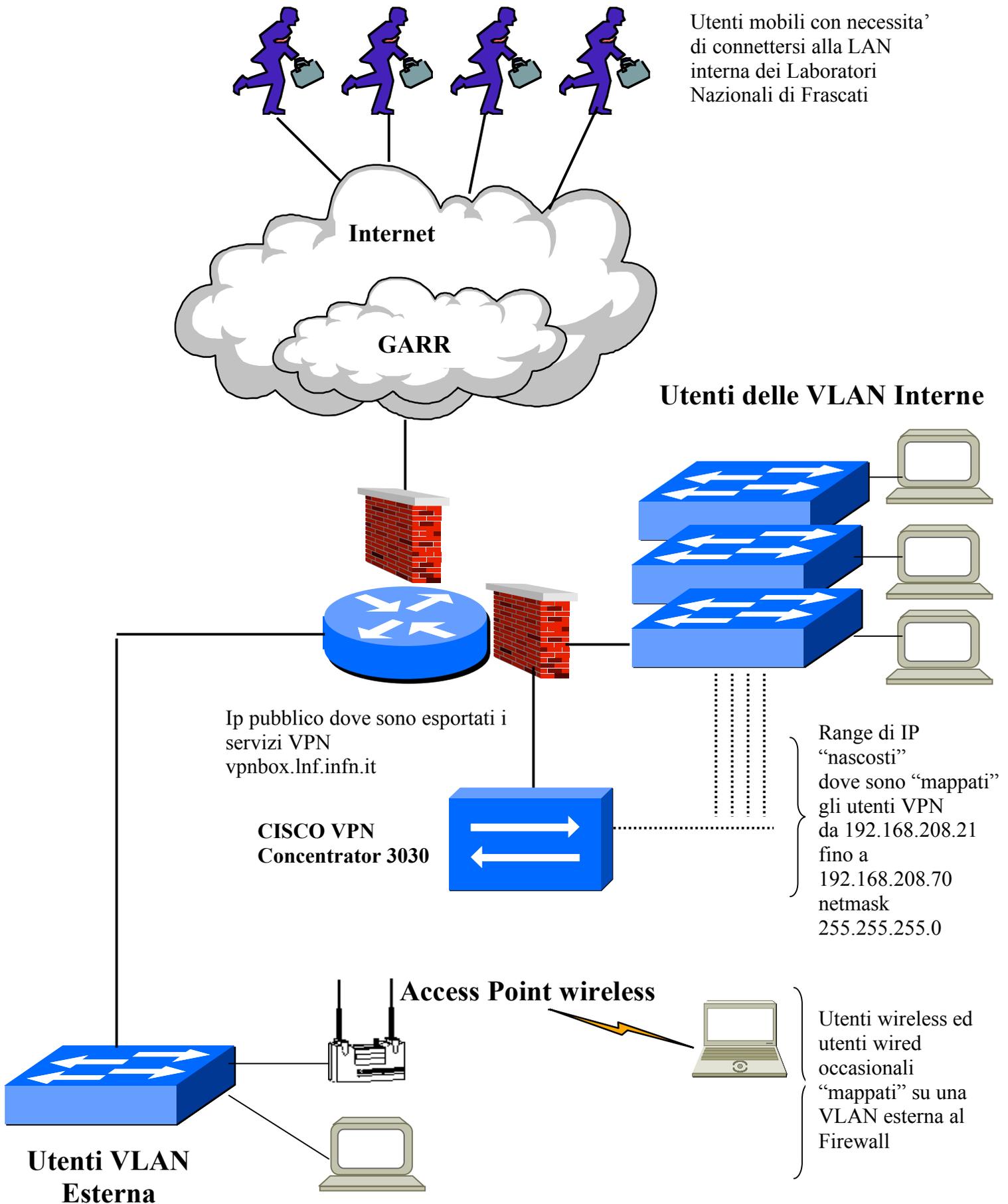
Abstract

La presente nota tecnica rappresenta una guida per l'utente affinché possa connettersi alla Local Area Network (LAN) dei Laboratori Nazionali di Frascati utilizzando un CISCO VPN Concentrator 3030. L'obiettivo è quello di permettere ad utenti "mobili" di accedere in modo "trasparente" alle risorse della propria LAN superando access-list o firewall presenti sul Router di frontiera ad Internet. Le modalità di accesso implementate sono due: attraverso l'uso di IPSec ed attraverso SSL, soluzione denominata WebVPN.

Indice:

- 1 Infrastruttura di rete - pag. 3**
- 2 Introduzione Virtual Private Network (VPN) – pag. 4**
- 3 Implementazione della VPN – pag. 4**
- 4 IPSec – pag. 4**
- 5 Secure Sockets Layer (SSL) – pag. 5**
- 6 Certificate Authority (CA) – pag. 6**
 - 6.1 Infrastruttura delle CA – pag. 7**
 - 6.2 Regole di match scelte per l'autenticazione attraverso certificato - pag. 8**
- 7 Configurazione del CISCO VPN Client con autenticazione attraverso certificato digitale – pag. 8**
 - 7.1 Configurazione del client Windows – pag. 8**
 - 7.2 Configurazione del client Linux – pag. 15**
 - 7.3 Configurazione del client Macintosh – pag. 16**
- 8 Configurazione del client windows con autenticazione attraverso username e password – pag. 18**
- 9 Configurazione WebVPN – pag. 18**
 - 9.1 Servizi esportabili con il WebVPN - pag. 19**
 - 9.2 Esempio connessione WebVPN su piattaforma windows – pag. 19**
- 10 Performance dichiarate dal costruttore – pag. 23**
- 11 Conclusioni finali – pag. 24**

1 INFRASTRUTTURA DI RETE



2 INTRODUZIONE VIRTUAL PRIVATE NETWORK (VPN)

Nel passato le aziende o le istituzioni pubbliche utilizzavano per permettere la connessione alla propria rete LAN delle “batterie” di modem a cui si potevano connettere i propri dipendenti, consulenti o rappresentanti commerciali.

Con l’evoluzione delle reti domestiche verso connessioni sempre piu’ veloci quali ADSL, UMTS, GPRS e il proliferare del Wi-Fi nelle stazioni ed aeroporti, diventa necessario dotarsi di tecnologie che permettano di creare dei tunnel sicuri attraverso Internet per raggiungere le LAN aziendali.

Una VPN e’ una rete logica privata che connette attraverso dei tunnel due o piu’ nodi connessi fisicamente in un mezzo untrusted (rete internet).

3 IMPLEMENTAZIONE DELLA VPN

Per garantire l’integrita’ dei dati che transitano in internet si e’ scelto di utilizzare alternativamente due soluzioni:

- 1) Il protocollo IPSec con autenticazione tramite certificati. In questo caso e’ richiesta l’installazione di un client su tutti gli host che vogliono connettersi al VPN concentrator. Il vendor CISCO Systems garantisce, gratuitamente con l’acquisto del VPN Concentrator, il client per le seguenti piattaforme:
 - a. Windows
 - b. Linux
 - c. MacOS X
 - d. Solaris
- 2) Il protocollo SSL, Secure Socket Layer, con autenticazione gestita localmente dal VPN Concentrator. Questa soluzione clientless anche chiamata WebVPN permette di connettersi al VPN concentrator, attraverso un web browser.

4 IPSec

L’Internet Protocol Security (IPSec) e’ una suite dei protocolli al livello di rete che stende l’IP offrendo meccanismi di autenticazione, confidenzialita’ ed integrita’ alle comunicazioni via IP. Con l’uso di IPSec, una sessione di comunicazione fra due host puo’ essere cifrata in modo trasparente alle applicazioni che girano su tali host.

IPSec ha due protocolli di sicurezza che possono essere implementati separatamente o insieme:

- Authentication Header (AH) : esegue solo l’autenticazione del mittente. L’autenticazione puo’ essere effettuata con Message Digest 5 (MD5), Hash-Based Message Authentication Code (HMAC) o Secure Hash Algorithm-1 (SHA-1).
- Encapsulating Security Protocol (ESP): Esegue sia l’autenticazione del mittente che del destinatario e la crittografia dei dati. L’autenticazione puo’ essere effettuata con gli algoritmi precedentemente citati mentre la crittografia e’ affidata a Digital Encryption Standard (DES), triple DES (3DES) ed altri algoritmi.

La crittografia di IPsec può essere implementata in due modi differenti:

- Transport mode, viene cifrato solo il payload (la parte dati) del pacchetto, mentre l'header resta in chiaro. Questa soluzione può essere utilizzata per la comunicazione diretta fra due host.
- Tunnel mode, sia l'header che il payload del pacchetto vengono cifrati. Questa soluzione può essere utilizzata fra gateway per proteggere le comunicazioni fra macchine che non sono in grado di utilizzare IPsec.

Per stabilire una Security Association (SA) di IPsec fra due host, questi devono precedentemente aver condiviso una chiave (segreta o pubblica) o un certificato digitale. La gestione delle chiavi in IPsec è affidata al protocollo Internet Key Exchange (IKE), talvolta referenziato come ISAKMP/Oakley.

5 Secure Sockets Layer (SSL)

SSL è un protocollo sviluppato da Netscape Communications per consentire il trasferimento sicuro di informazioni sensibili o private, come i numeri di carta di credito, attraverso un mezzo intrinsecamente insicuro: Internet. Si sono succedute diverse versioni di SSL fino a SSL v3, che ha costituito la base del protocollo Transport Layer Security (TLS) descritto nella RFC 2246.

SSL lavora al livello di trasporto della suite di protocolli TCP/IP. Il funzionamento di SSL consiste in una combinazione di crittografia a chiave pubblica e a chiave segreta che offre riservatezza dei dati mediante cifratura. I certificati digitali e le coppie di chiavi pubbliche e private usate in SSL sono generate mediante l'algoritmo a chiave pubblica RSA.

Prendiamo HTTPS come esempio: quando il browser Web di un client vuole collegarsi a un server web che adopera SSL, il client usa una URL che inizia con https:// per iniziare la procedura di handshaking SSL con il server. Questo handshaking viene usato per negoziare l'algoritmo crittografico a chiave segreta che entrambi le parti adopereranno per cifrare le informazioni scambiate tra loro durante la sessione. Le informazioni iniziali inviate dal client al server includono un elenco degli algoritmi crittografici che il client supporta e una stringa di challenge casuale usata più avanti nell'handshake.

Una volta che il client ha inviato la challenge al server, questo risponde restituendo una copia del suo certificato server, un certificato digitale da esso usato per provare la propria identità a terzi. Perché SSL funzioni, il server deve aver precedentemente ottenuto un certificato da una Certification Authority (CA) come Verisign. Insieme al certificato, il server include anche una sua stringa di challenge casuale e sceglie l'algoritmo crittografico da usare, dall'elenco inviatogli prima del client. Esempi di algoritmi crittografici a chiave segreta supportati da SSL sono RC4 e DES.

Il client verifica quindi il certificato inviato dal server usando la chiave pubblica di quello, per assicurarsi di stare effettivamente parlando con il server con cui vuole parlare. Il client ottiene la chiave pubblica del server estraendola dal suo certificato ricevuto al passo precedente. Il client genera quindi un'altra stringa casuale chiamata premaster secret, che verrà usata nel processo di generazione della chiave di sessione. Il client cifra il premaster secret usando la chiave pubblica del server e glielo invia, insieme a un hash dei messaggi di handshaking e a un master secret. Questo hash aiuta a garantire che i messaggi di handshaking non siano stati manomessi da un intruso che tenta di dirottare la sessione. La chiave usata per l'hash è derivata dalle due stringhe casuali precedentemente inviate da ciascuna parte e dal master secret.

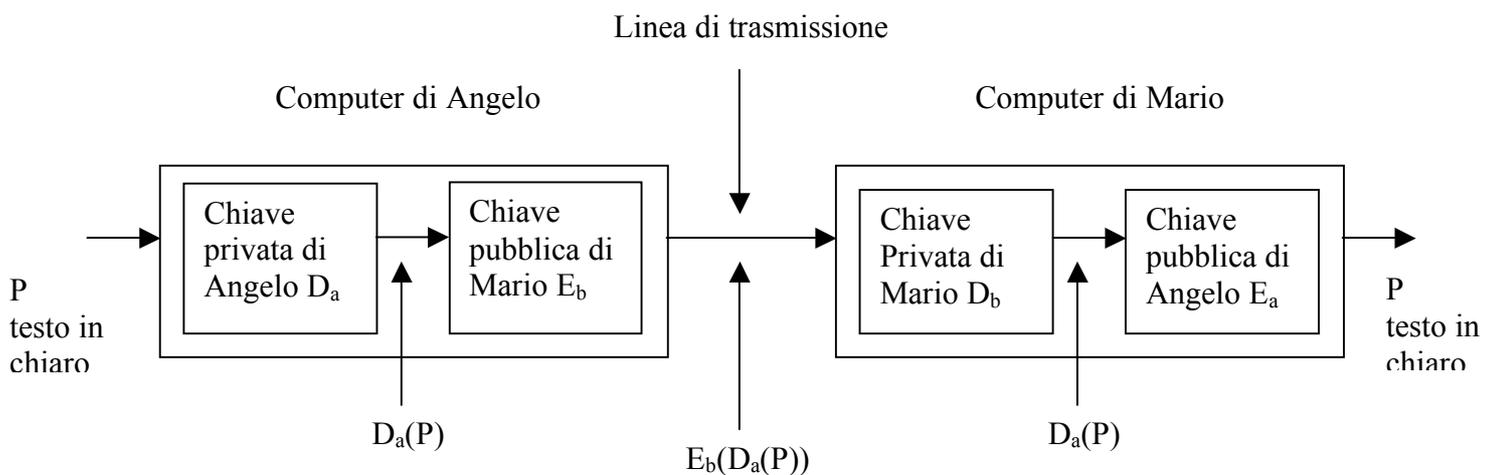
Infine il server completa la procedura inviando al client un hash di tutti i messaggi di handshaking scambiati fino a questo punto. Entrambe le parti derivano quindi la chiave di sessione dai vari valori casuali e dalle chiavi scambiate, mediante una complessa operazione matematica.

Tutti i dati scambiati tra client e server nel corso della sessione vengono cifrati mediante la chiave di sessione che viene poi scartata quando la sessione stessa termina o scade.

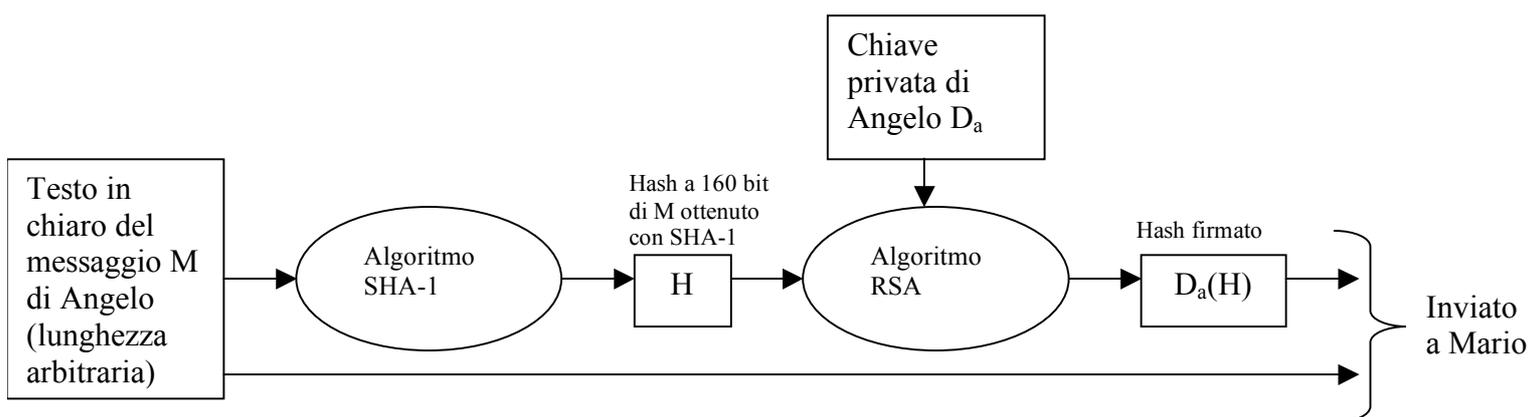
6 Certificate Authority (CA)

La crittografia a chiave pubblica consente la comunicazione sicura fra persone che non condividono una chiave comune senza che sia necessaria una terza parte fidata. Le firme digitali usando la crittografia a chiave pubblica tipo RSA garantiscono l'autenticazione e la segretezza.

Questo può essere facilmente riassunto nel seguente schema:



I message digest garantiscono l'autenticazione con l'integrità dei messaggi ma non la segretezza. Di seguito riportiamo un esempio di comunicazione utilizzando i Message digest con tecnologia SHA-1



Anche questo esempio mostra che è necessario un repository per le chiavi pubbliche.

L'idea è quella di non avere un centro di distribuzione delle chiavi pubbliche online a tutte le ore, ma di avere una organizzazione che certifica le chiavi pubbliche che appartengono a persone o organizzazioni.

Una organizzazione che certifica le chiavi pubbliche è chiamata Certificate Authority o autorità di certificazione.

In generale una CA emette un certificato che potrebbe avere ad esempio il seguente formato:

Certifico che la chiave pubblica:

```
30 82 01 0a 02 82 01 01 00 cb ae 0d 92 6e 88 80 3f 52 91 0f 17 16 ac 4e 75 41 4a 2f c5 2d 66 68
74 f8 92 14 53 4d 5d 17 27 ac 2a d3 1b 84 09 bb 52 41 09 cb 0d 12 cf a0 74 94 7b 7b 43 00 53 c4
18 73 9c fa 6e 27 17 e3 f3 f5 75 18 c2 f4 0e e3 93 ef a2 94 b0 1d 7f b4 96 71 1a 69 30 5d 1b 0d
2d fa ec a2 64 97 6b f7 80 41 13 35 10 91 a2 37 93 26 70 ea ac ca a0 9f f7 5c e1 91 f9 ed 25 b8
06 3c aa ed c2 1c fd 18 27 c7 05 07 09 40 13 b6 a4 e4 0c 23 0a a0 ef 73 a9 f2 dd ae ca e8 ce 20
d4 73 08 09 ab 9c 6b 31 09 d4 24 ce 70 33 7c da 42 e2 55 30 fc 3e 54 fe 03 b9 ce bc 73 b9 ce d2
d8 0e 08 46 0b e3 7c 21 49 91 7b 13 94 07 4f 03 1d 5e 46 b1 94 8a a9 c3 68 88 a5 58 00 d2 09 32
43 d0 68 69 64 a3 d3 3a b7 04 6f 20 89 fb 4a c2 81 6b 0f 3b f9 a2 cb 52 aa 30 fc 04 d7 c9 f4 6a
cc 4d 7b 2c f0 59 c5 04 ad 02 03 01 00 01
```

Appartiene a :

Angelo Veloce

LNF

INFN

IT

Emesso il: 8 Marzo 2005

Scade: 8 Marzo 2006

Hash SHA-1 del certificato di cui sopra firmato con la chiave private della CA:

La CA accertatasi dell'identita' di Angelo emette un certificato che contiene la chiave pubblica di Angelo piu' i suoi dati anagrafici. Al certificato viene aggiunta una estensione che e' l'hash SHA-1 del certificato firmata con la chiave privata della CA.

I certificati sono stati successivamente standardizzati nel formato X.509.

6.1 Infrastruttura delle CA

Le CA sono organizzate in una struttura chiamata PKI (Public Key Infrastructure).

I componenti base sono:

- a. Gli utenti
- b. Le CA
- c. Directory

Le CA hanno una organizzazione gerarchica al vertice c'e' root che certifica le CA di secondo livello chiamate RA (Regional Authorities), queste a loro volta certificano le vere e proprie CA che rilasciano certificati ad organizzazioni o privati.

Ad ogni livello della gerarchia PKI la relativa CA ha un certificato pubblico approvato dalla CA di gerarchia immediatamente superiore. In generale un utente conosce quanto meno la chiave pubblica di root perche' i produttori di Browser inseriscono questa al loro interno. Comunque per superare il problema della gestione di una singola root nei browser sono presenti le chiavi pubbliche di piu' root chiamate anche trust anchors.

Le Directory nascono dall'esigenza della memorizzazione dei certificati e delle loro catene fino a qualche trust anchor conosciuta.

Una soluzione e' quella che ogni utente memorizzi i propri certificati, ci sono pero' proposte per usare LDAP per contenere questo tipo di informazioni.

Con i certificati nasce anche l'esigenza della gestione delle CRL (Certificate Revocation List) che contengono la lista di tutti i certificati revocati dalla CA per comportamento illecito dell'utente. Sfortunatamente per un utente con l'introduzione delle CRL questo deve controllare la possibile revoca del certificato presso la CA prima di usarlo.

6.2 Regole di match scelte per l'autenticazione attraverso certificato.

Per l'autenticazione attraverso certificato e' necessario stabilire dei criteri di selezione degli utenti possessori dei certificati emessi dalla INFN CA.

In particolare ho voluto permettere l'accesso alla LAN attraverso connessioni VPN ai soli utenti dei Laboratori Nazionali di Frascati. Per soddisfare questa esigenza e' possibile utilizzare il campo L (locality) del certificato come criterio per consentire l'autenticazione solo ai client possessori di certificato della CA INFN facenti capo ai Laboratori Nazionali di Frascati (LNF).

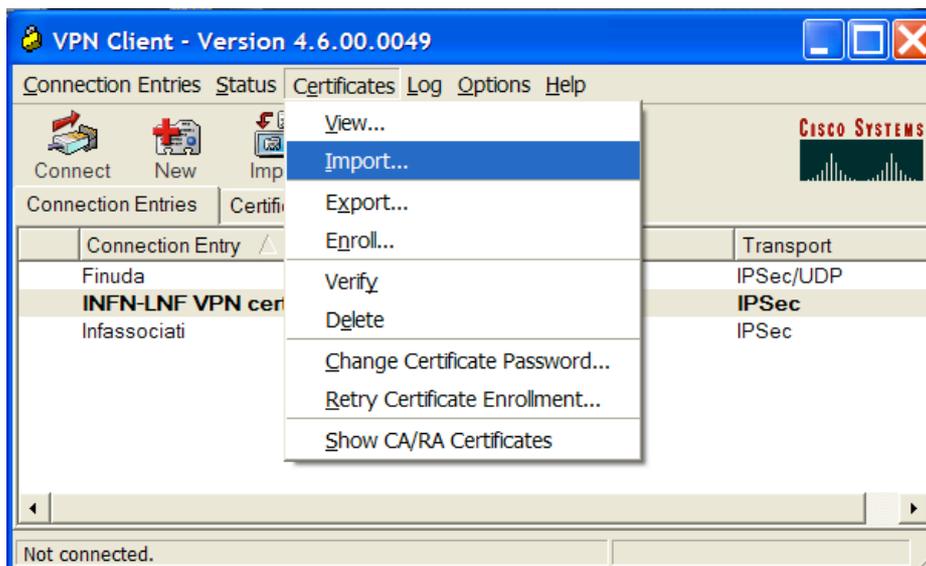
7 Configurazione del CISCO VPN Client con autenticazione attraverso certificato digitale

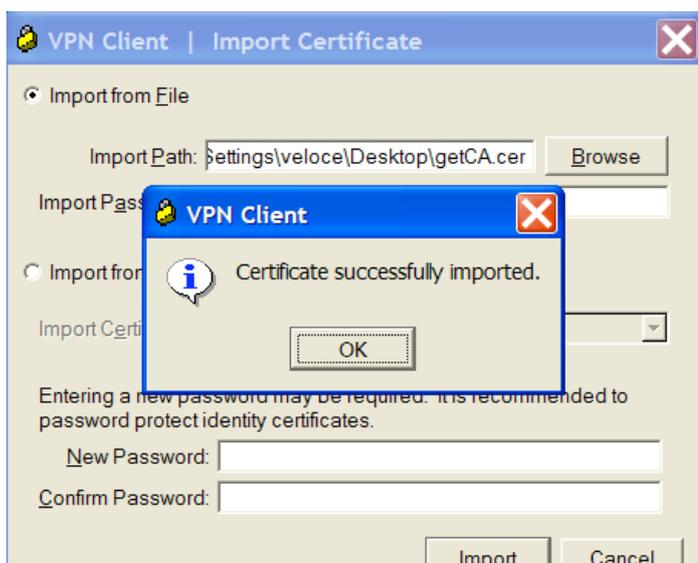
Come abbiamo gia' detto e' necessaria l'installazione di un software sul client, tipicamente il notebook. E' stato testato questo client sulle piattaforme Windows XP, Scientificlinux e MacOS 10.3. Il client del Cisco VPN Concentrator e' fornito gratuitamente con l'acquisto dell'appliance.

Tutto il software e' disponibile sul sito: <http://www.lnf.infn.it/computing/networking/> accessibile dalle sole sedi INFN.

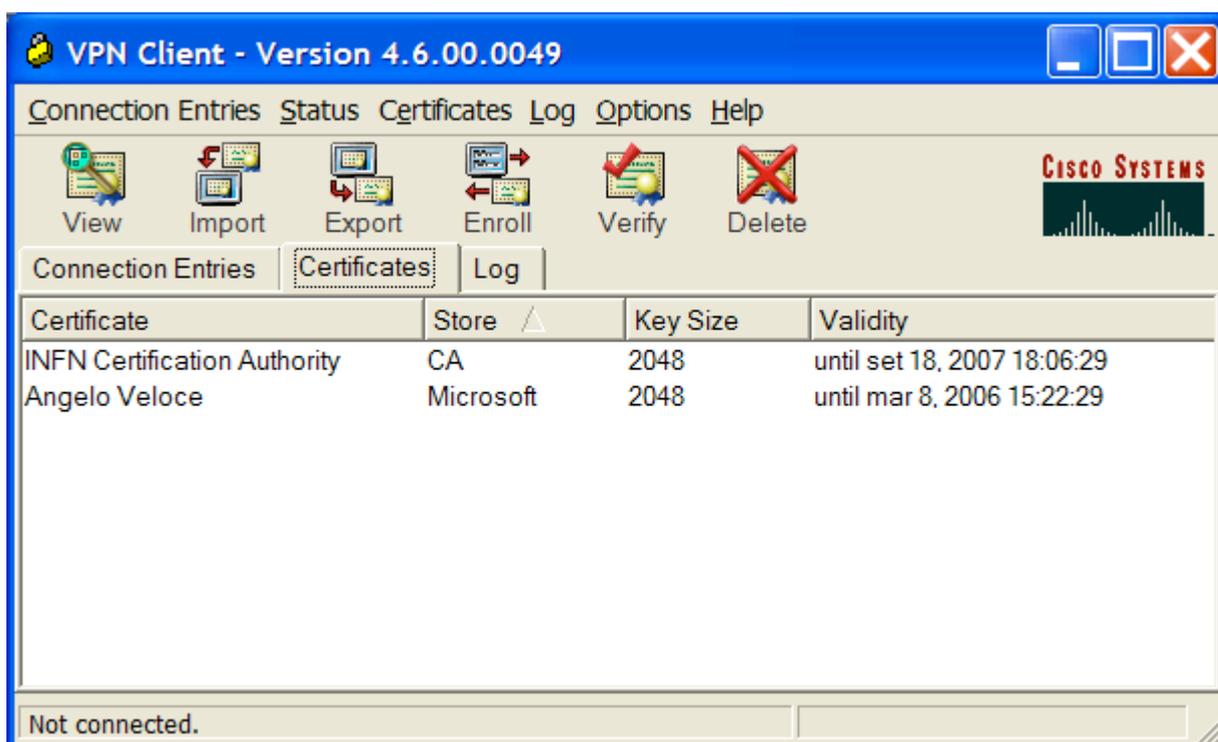
7.1 Configurazione del client Windows

Eseguita l'installazione come una normale applicazione windows si procede alla configurazione. Se desideriamo l'accesso con autenticazione attraverso certificato e' necessario importare il certificato personale e quello dell'INFN CA (<http://security.fi.infn.it/CA/>). Se tutto questo e' gia' stato importato con il browser Internet Explorer il software del Client Cisco automaticamente li importa. Altrimenti si possono importare entrambi i certificati attraverso il software Cisco, come di seguito riportato:



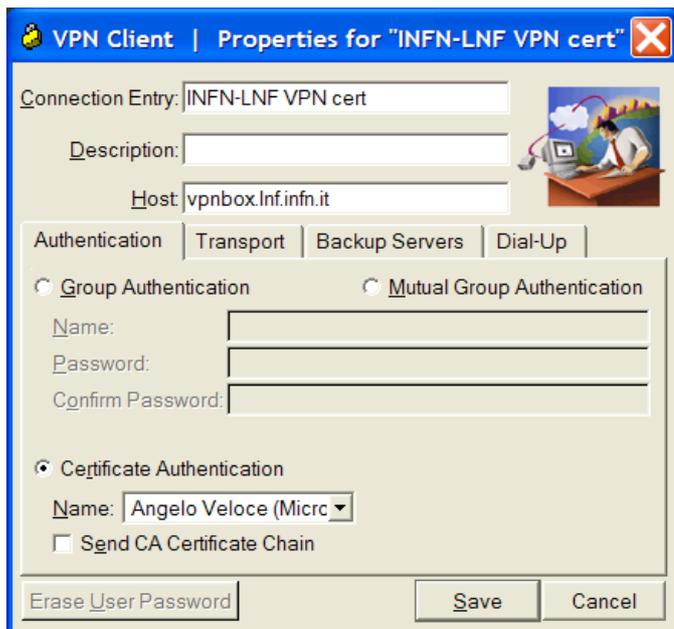


E' possibile verificare i certificati importati come di seguito indicato:

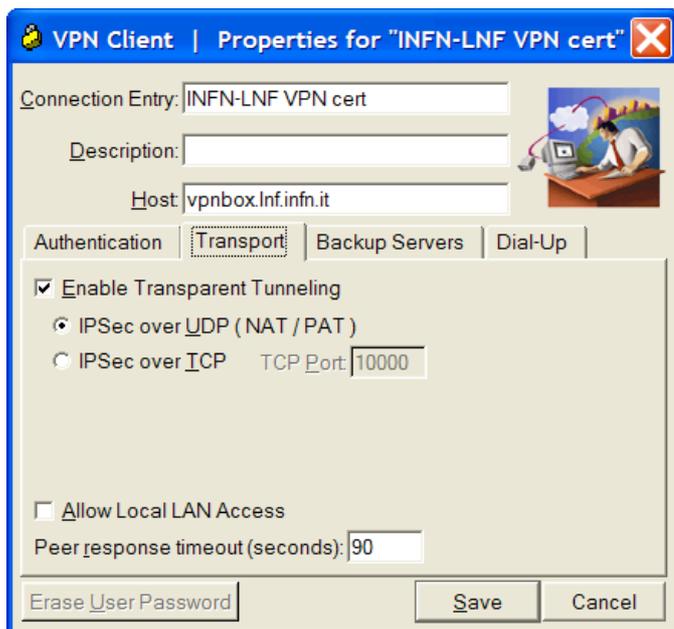


Il passo successivo e' la configurazione di una nuova connessione dove dovra' essere specificato:

- Connection Entry:, il nome della connessione;
- Host:, il nome DNS dell'interfaccia pubblica del VPN Concentrator che esporta i servizi agli utenti remoti;
- Scegliere l'autenticazione, che nel caso di accesso attraverso certificato avverra' attraverso il certificato personale selezionabile nel menu' a tendina.



Molto importante e' il tab Transport relativo alle diverse modalita' di connessione possibili, a seconda della configurazione di rete offerta dal proprio provider. Il default e' quello di seguito riportato:



E' bene mettere in evidenza che il successo di una connessione VPN dipende molto dalle impostazioni della rete del provider a cui si e' connessi.

Spesso i provider offrono la connettivita' internet fornendo indirizzi IP nascosti. Ogni organizzazione privata o pubblica puo' utilizzare sulla propria LAN dei gruppi di indirizzi IP nascosti:

Spazi di indirizzamento nascosti non ruotati assegnati dall'Internet Assigned Numbers Authority (IANA)	
Classe A	Da 10.0.0.0 a 10.255.255.255
Classe B	Da 172.16.0.0 a 172.31.255.255

Classe C	Da 192.168.0.0 a 192.168.255.255
----------	----------------------------------

L'utente connesso dal proprio provider con indirizzi nascosti sarà visibile in Internet con una operazione di traslazione con altri indirizzi pubblici. Le tecnologie che permettono queste operazioni sono: Network Address Translation (NAT) e Port Address Translation (PAT). Tutto questo "complica" l'instaurazione di una connessione VPN. Inoltre spesso i provider "filtrano" il traffico in uscita dalla propria LAN non permettendo ad esempio i protocolli utilizzati da IPsec:

- Encapsulating Security Payload (ESP) protocol 50;
- UDP 500 per l'Internet Key Exchange.

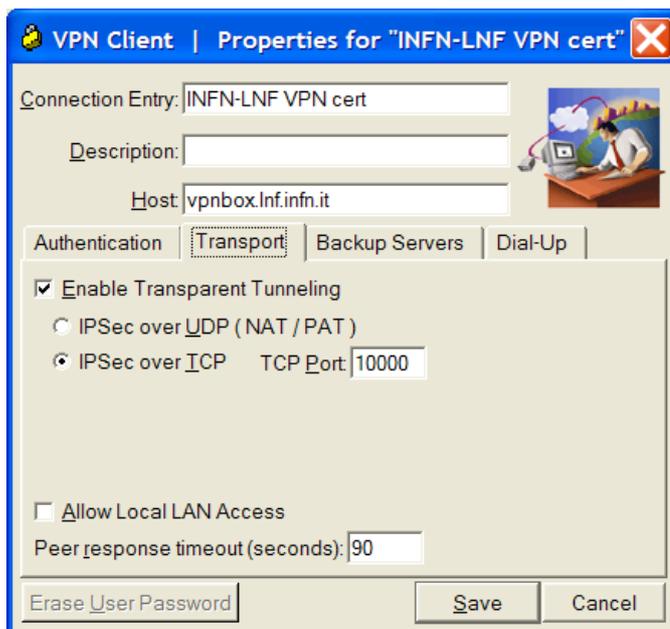
Per superare i problemi che derivano da eventuali reti con NAT, PAT o firewall si utilizzano tre tecnologie:

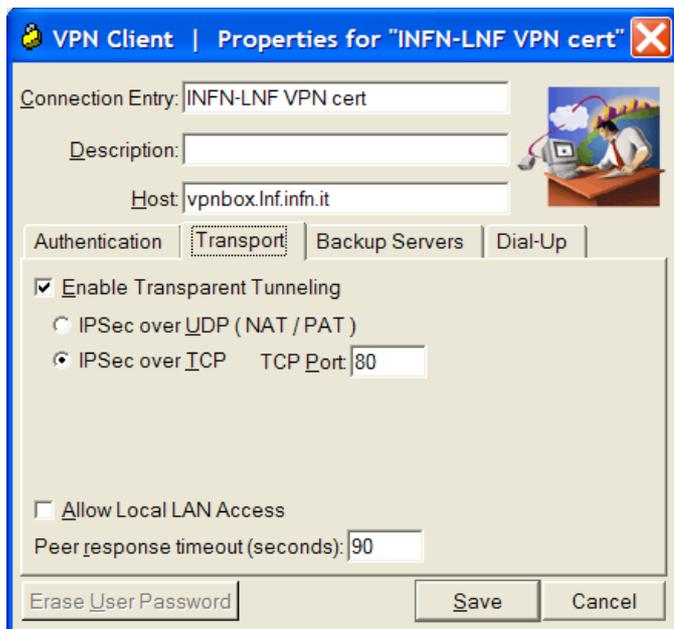
- IPsec over UDP (soluzione proprietaria)
- IPsec over UDP (NAT-T standard)
- IPsec over TCP (soluzione proprietaria)

In particolare, utilizzando l'impostazione di default, Enable Transparent Tunneling e IPsec over UDP (NAT/PAT) si utilizza la soluzione standard NAT-T.

Con questa soluzione tutto il pacchetto IPsec viene incapsulato in un nuovo pacchetto IP che utilizza allo strato di trasporto la porta UDP 4500.

Se il provider a cui si è connessi blocca questo tipo di traffico e' possibile usare alternativamente le seguenti impostazioni:





E' importante esaminare le differenze sulla impostazione della rete prima e dopo l'apertura della connessione VPN:



Dopo l'apertura della connessione VPN

```

Prompt dei comandi

Scheda PPP universita2:

Suffisso DNS specifico per connessione:
Descrizione . . . . . : WAN (PPP/SLIP) Interface
Indirizzo fisico . . . . . : 00-53-45-00-00-00
DHCP abilitato . . . . . : No
Indirizzo IP . . . . . : 160.80.21.191
Subnet mask . . . . . : 255.255.255.255
Gateway predefinito . . . . . : 160.80.21.191
Server DNS . . . . . : 160.80.2.5
                          160.80.1.8
NetBIOS su TCPIP . . . . . : Disabilitato

Scheda Ethernet Connessione alla rete locale (LAN) 3:

Suffisso DNS specifico per connessione: Inf.infn.it
Descrizione . . . . . : Cisco Systems UPN Adapter
Indirizzo fisico . . . . . : 00-05-9A-3C-78-00
DHCP abilitato . . . . . : No
Indirizzo IP . . . . . : 192.168.208.24
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . :

C:\Documents and Settings\veloce>

```

E' possibile notare che viene aperta una sub-interface attraverso la quale passa il traffico cifrato verso il VPN Concentrator. A questo punto ci si puo' chiedere ma quale traffico passa?

Bene in una sezione del VPN Concentrator, e' possibile impostare la tabella di Routing che verra' scaricata sul Client. In particolare il gruppo servcal, che e' quello degli utenti che si autenticano attraverso certificato, utilizzano la sub-interface della connessione VPN per inoltrare il traffico delle seguenti Network dei Laboratori Nazionali di Frascati:

Reti sulle quali e' inoltrato il traffico del VPN	Descrizione
193.206.80.0 / 0.0.7.255	Range di IP pubblici utilizzati dai Server e Desktop
192.84.128.0 / 0.0.3.255	Range di IP pubblici utilizzati dai Server e Desktop
192.135.25.0 / 0.0.0.255	Range di IP pubblici utilizzati dall' esperimento Kloe
192.135.26.0 / 0.0.0.255	Range di IP pubblici utilizzati dall' esperimento Kloe
192.168.130.0 / 0.0.0.255	Range di IP nascosti utilizzati per le stampanti AC
192.168.132.0 / 0.0.0.255	Range di IP nascosti utilizzati per le stampanti LNF
192.168.140.0 / 0.0.0.255	Range di IP nascosti utilizzati per strumenti e field point
192.168.161.0 / 0.0.0.255	Range di IP nascosti utilizzati per strumenti e laboratorio Master
192.168.192.0 / 0.0.0.255	Range di IP nascosti utilizzati per controllo DAFNE
192.168.195.0 / 0.0.0.255	Range di IP nascosti utilizzati per laboratorio DAFNE
192.168.197.0 / 0.0.0.255	Range di IP nascosti utilizzati per esperimento SPARC
192.168.199.0 / 0.0.0.255	Range di IP nascosti utilizzati per esperimento FINUDA
192.168.208.0 / 0.0.0.255	Range di IP nascosti utilizzati per utenti VPN

Impostare questa tabella e' importante affinche' solo il traffico effettivamente diretto alle Network dei laboratori vengano inoltrate nella sub-interface con canale IPSec. Quindi il traffico esterno alle Network dei Laboratori utilizzeranno il normale canale di comunicazione del proprio provider. Tutto questo e' dimostrato nelle immagini di seguito riportate:

```
Prompt dei comandi
C:\Documents and Settings\veloce>
C:\Documents and Settings\veloce>tracert www.larepubblica.it

Rilevazione instradamento verso locutus.e-solutions.it [80.247.78.231]
su un massimo di 30 punti di passaggio:

  1   136 ms   160 ms   130 ms   pppstudTS-02.stud.uniroma2.it [160.80.21.19]
  2   150 ms   159 ms   130 ms   160.80.2.1
  3   140 ms   140 ms   140 ms   160.80.246.2
  4   150 ms   140 ms   140 ms   rc-uniromaII.rm.garr.net [193.206.131.77]
  5   159 ms   159 ms   159 ms   rt-rm1-rt-mi2.mi2.garr.net [193.206.134.229]
  6   340 ms   159 ms   170 ms   levelip.mix-it.net [217.29.66.74]
  7   169 ms   160 ms   149 ms   80.247.66.20
  8   150 ms   159 ms   170 ms   e-solutions.it [80.247.78.231]

Rilevazione completata.
C:\Documents and Settings\veloce>
```

```
Prompt dei comandi
C:\Documents and Settings\veloce>
C:\Documents and Settings\veloce>tracert www.lnf.infn.it

Rilevazione instradamento verso www.lnf.infn.it [193.206.84.219]
su un massimo di 30 punti di passaggio:

  1   238 ms   230 ms   220 ms   upnbox.lnf.infn.it [193.206.84.7]
  2   231 ms   209 ms   230 ms   192.168.208.1
  3   218 ms   230 ms   219 ms   www1.lnf.infn.it [193.206.84.219]

Rilevazione completata.
C:\Documents and Settings\veloce>
```

```
Prompt dei comandi
C:\Documents and Settings\veloce>
C:\Documents and Settings\veloce>tracert dante100

Rilevazione instradamento verso dante100.lnf.infn.it [192.168.192.100]
su un massimo di 30 punti di passaggio:

  1   204 ms   210 ms   220 ms   upnbox.lnf.infn.it [193.206.84.7]
  2   220 ms   210 ms   210 ms   192.168.208.1
  3   220 ms   230 ms   209 ms   swlat-80.lnf.infn.it [193.206.80.10]
  4   240 ms   230 ms   230 ms   192.168.192.100

Rilevazione completata.
C:\Documents and Settings\veloce>
```

7.2 Configurazione del client Linux

La versione testata e' la 4.6.03, Cisco fornisce il file da installare `vpnclient-linux-x86_64-4.6.03.0190-k9.tar`. Questa versione puo' essere installata sulle seguenti piattaforme:

- Linux per Intel, con le seguenti caratteristiche:
 - versioni RedHat 6.2 o superiori;
 - versioni glibc 2.1.1-6 o superiori;
 - versione di kernel 2.2.12 o superiore;
- Solaris UltraSPARC 5;
- SunBlade.

Nel mio caso ho provato l'installazione con la distribuzione Scientificlinux che e' una derivazione di RedHat 9.

Per l'installazione viene creata una directory `vpnclient` dove ho eseguito lo script `vpn_install`. Nel passo successivo si carica il modulo `cisco_ipsec` eseguendo lo script `vpnclient_init start` nella cartella `vpnclient`. Dopo l'installazione troveremo i file di configurazione nella directory `/etc/CiscoSystemsVPNClient/Certificates/Profiles/`. Mentre per l'autenticazione e' necessario installare i certificati nel percorso di seguito indicato:

```
[root@dyn17 Certificates]# cd /etc/CiscoSystemsVPNClient/Certificates
[root@dyn17 Certificates]# ls
getCA.cer      angelo2005linux.pfx
```

E' necessario che il proprio certificato sia nel formato `.pfx`. Normalmente il proprio certificato e' nel formato `pkcs12`, per esportarlo in formato `pfx` si puo' usare ad esempio l'export di Internet Explorer.

Per quanto riguarda il file di configurazione va copiato ed editato il file `sample.pcf`. Di seguito riporto la configurazione necessaria per il nostro tipo di connessione:

```
[root@dyn17 root]# cd /etc/CiscoSystemsVPNClient/Profiles/
[root@dyn17 Profiles]# more ip sec-cert.pcf
[main]
Description=ServizioVPNLNF
Host=vpnbox.lnf.infn.it
AuthType=3
GroupName=servcal
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=cert_user
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableLocalLAN=1
EnableNat=0
CertStore=1
CertName=Angelo Veloce
CertPath=/etc/CiscoSystemsVPNClient/Certificates
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
UserPassword=
enc_UserPassword=
```

Di seguito riporto un esempio di connessione:

```
[root@dyn17 root]# vpnclient connect ipsec-cert
Cisco Systems VPN Client Version 4.6.03 (0190)
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.21-27.0.2.EL #1 Tue Jan 18 19:45:27 CST 2005 i686
Config file directory: /etc/opt/cisco-vpnclient

Enter Certificate password:
Initializing the VPN connection.
Contacting the gateway at 193.206.84.7
Negotiating security policies.
Securing communication channel.

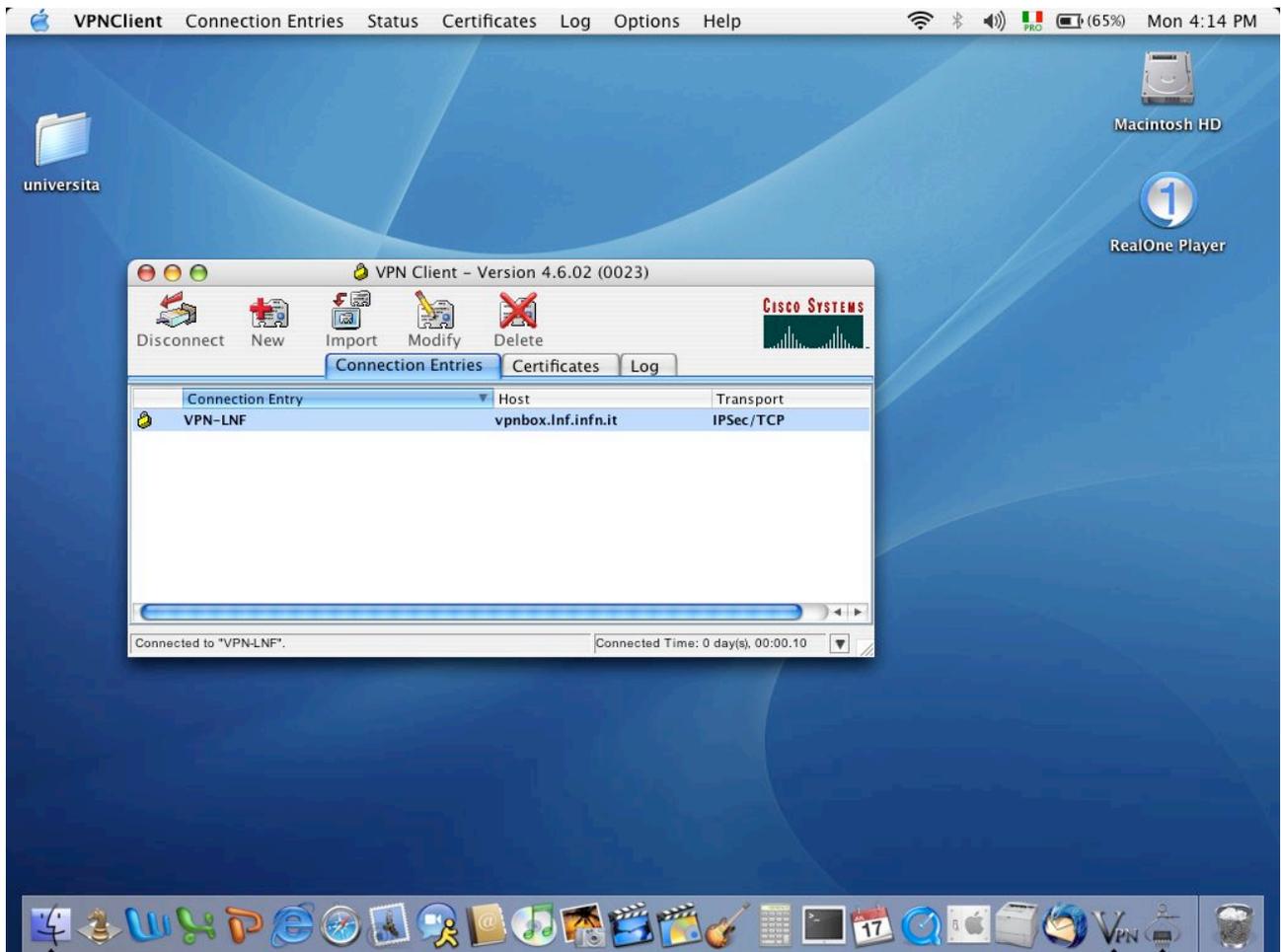
Your VPN connection is secure.

VPN tunnel information.
Client address: 192.168.208.22
Server address: 193.206.84.7
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is inactive
Local LAN Access is disabled
```

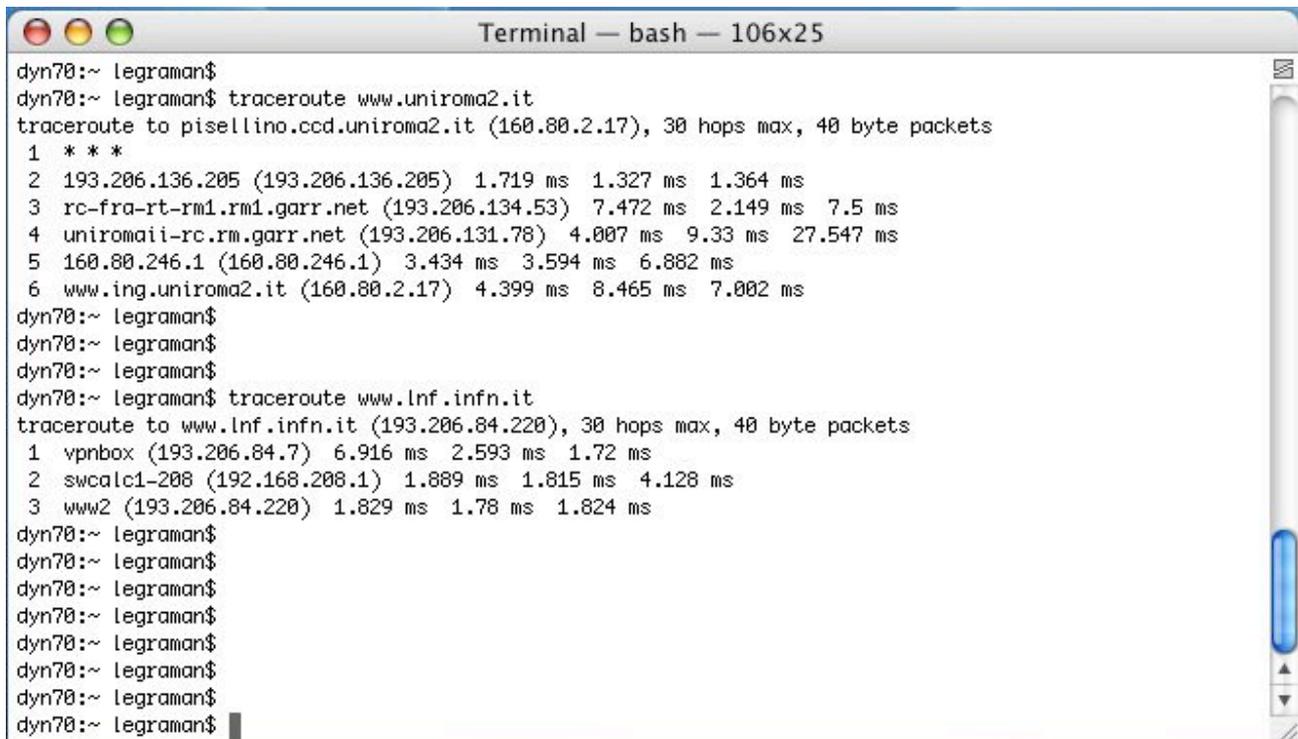
7.3 Configurazione del client Macintosh

La versione testata e' la vpnclient-darwin-4.6.02.0023-GUI-k9.dmg per MacOS 10.3. L'installazione e' molto semplice, i certificati vengono importati direttamente attraverso il client Cisco. L'interfaccia di configurazione e' molto simile a quella windows e valgono i medesimi criteri di configurazione.





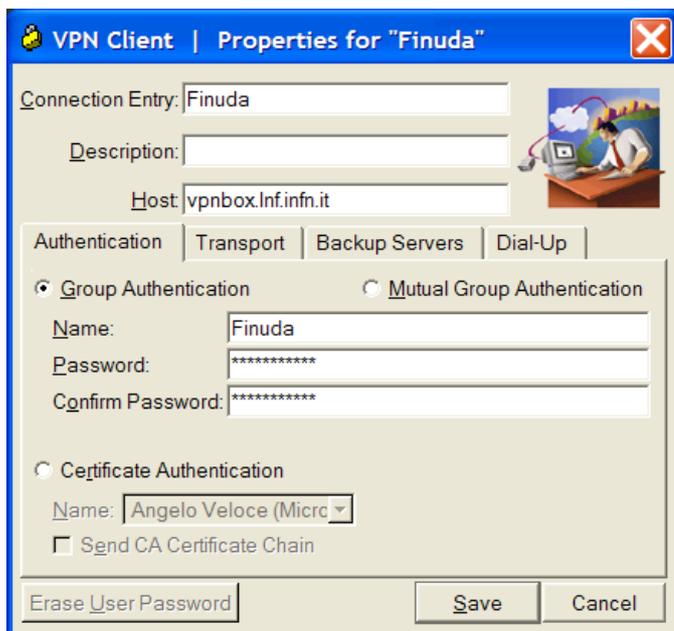
Le politiche di routing sono medesime a quelle già illustrate per i client windows.



8 Configurazione del client windows con autenticazione attraverso username e password

Questa soluzione e' quella adottata principalmente per i collaboratori esterni dei Laboratori Nazionali di Frascati. Per questi tipi di utenti l'accesso sara' limitato alle sole risorse di rete di cui hanno bisogno, cio' significa che la tabella di routing scaricata sul client potra' essere limitata.

Di seguito riporto un esempio di configurazione del client windows per gli utenti che si autenticano con username e password:



Questo esempio e' relativo al gruppo sperimentale Finuda, la Password inserita in questa maschera e la IKE Pre-shared Keys utilizzata durante la prima fase di instaurazione del canale IPsec. Il tab Transport potra' essere configurato come precedentemente indicato.

La username e la password proprie dell'utente verranno richieste nel momento di una connessione. Il routing per il gruppo Finuda e quindi l'accesso alle risorse della LAN LNF e' limitato alla sola VLAN di Finuda e ad alcuni siti WEB normalmente chiusi; ad esempio il sito WEB del magazzino.

9 Configurazione WebVPN

WebVPN permette di stabilire connessioni sicure con il VPN 3000 Concentrator usando un web browser. La tecnologia utilizzata per queste connessioni sicure e' Secure Socket Layer (SSL) ed il suo successore Transport Layer Security (TLS1). Il WebVPN supporta le connessioni HTTPS degli utenti aventi i seguenti browser:

- Su Microsoft Windows:
 - Internet Explorer version 6.0 SP1 (SP2 richiesta per Windows XP)
 - Netscape version 7.2
 - Mozilla version 1.73
 - Firefox 1.0
- Su Linux:
 - Netscape version 7.2
 - Mozilla version 1.73
 - Firefox 1.0

- Su Macintosh OS X:
 - Safari version 1.24
 - Firefox 1.0
- Su Solaris:
 - Netscape version 7.2
 - Mozilla version 1.73

Per supportare il port forwarding e' necessaria l'installazione della Java Runtime Environment (JRE) che e' una parte del J2SE versione 1.4.1.

Per l'autenticazione degli utenti WebVPN ho scelto l'utilizzo del server di autenticazione interno del VPN Concentrator. Questo permette di gestire un massimo di 500 utenti.

9.1 Servizi esportabili con il WebVPN

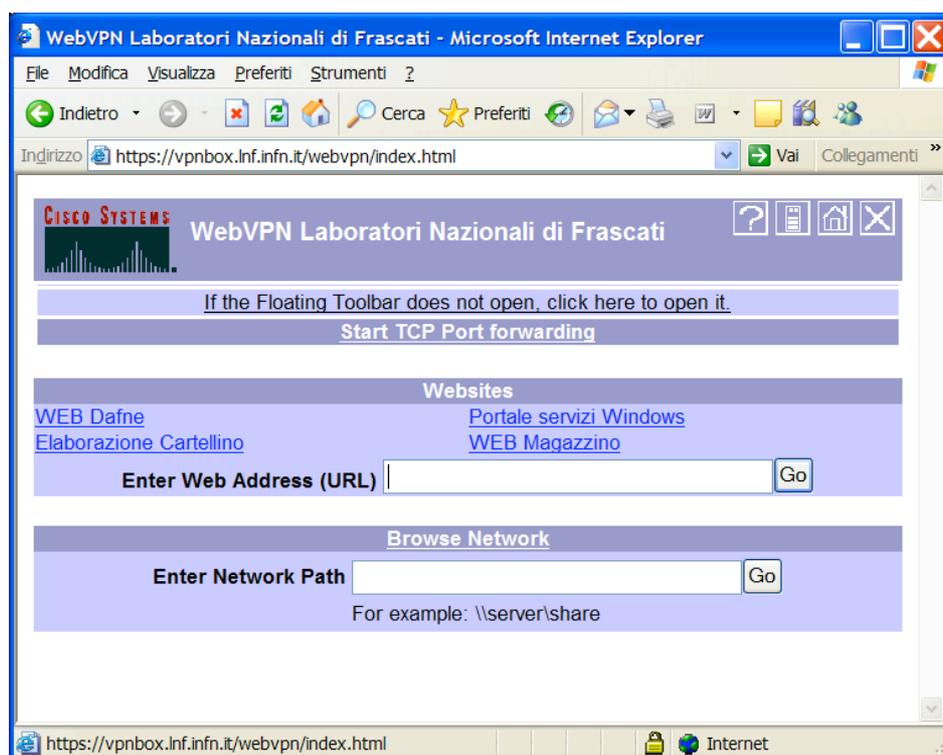
Il WebVPN e' sicuramente una soluzione valida nel mio caso per tutti quegli utenti occasionali come borsisti, ricercatori associati o collaboratori esterni che richiedono un accesso limitato ad alcune risorse della LAN. I servizi disponibili sono:

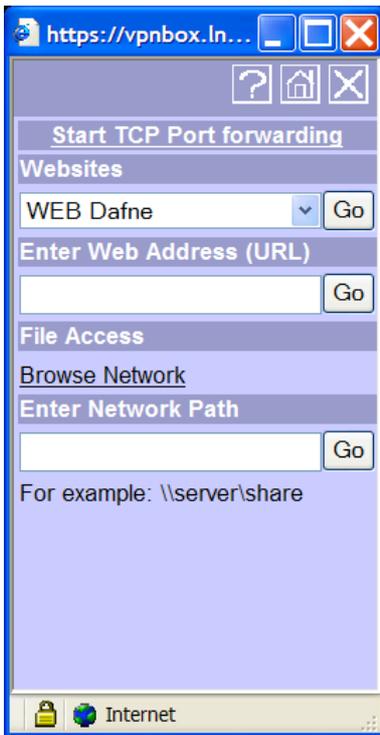
- Esportare dei siti web normalmente non visibili dalla WAN;
- Permettere il browsing NetBIOS della rete;
- Abilitare il Port Forwarding.

Sicuramente le due funzionalita' piu' interessanti sono la possibilita' di vedere siti WEB normalmente filtrati ed il Port Forwarding.

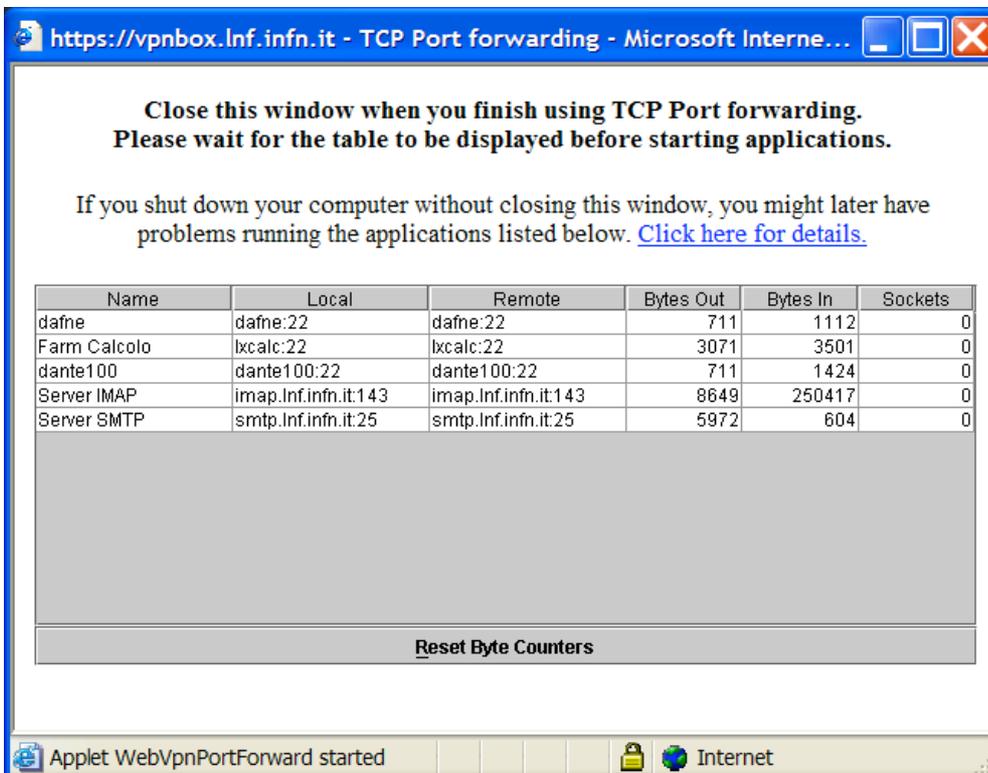
10 Esempio connessione WebVPN su piattaforma windows

Per aprire una connessione WebVPN basta connettersi al sito (<https://vpnbox.lnf.infn.it>). Dopo l'autenticazione attraverso username e password si apriranno le seguenti maschere:





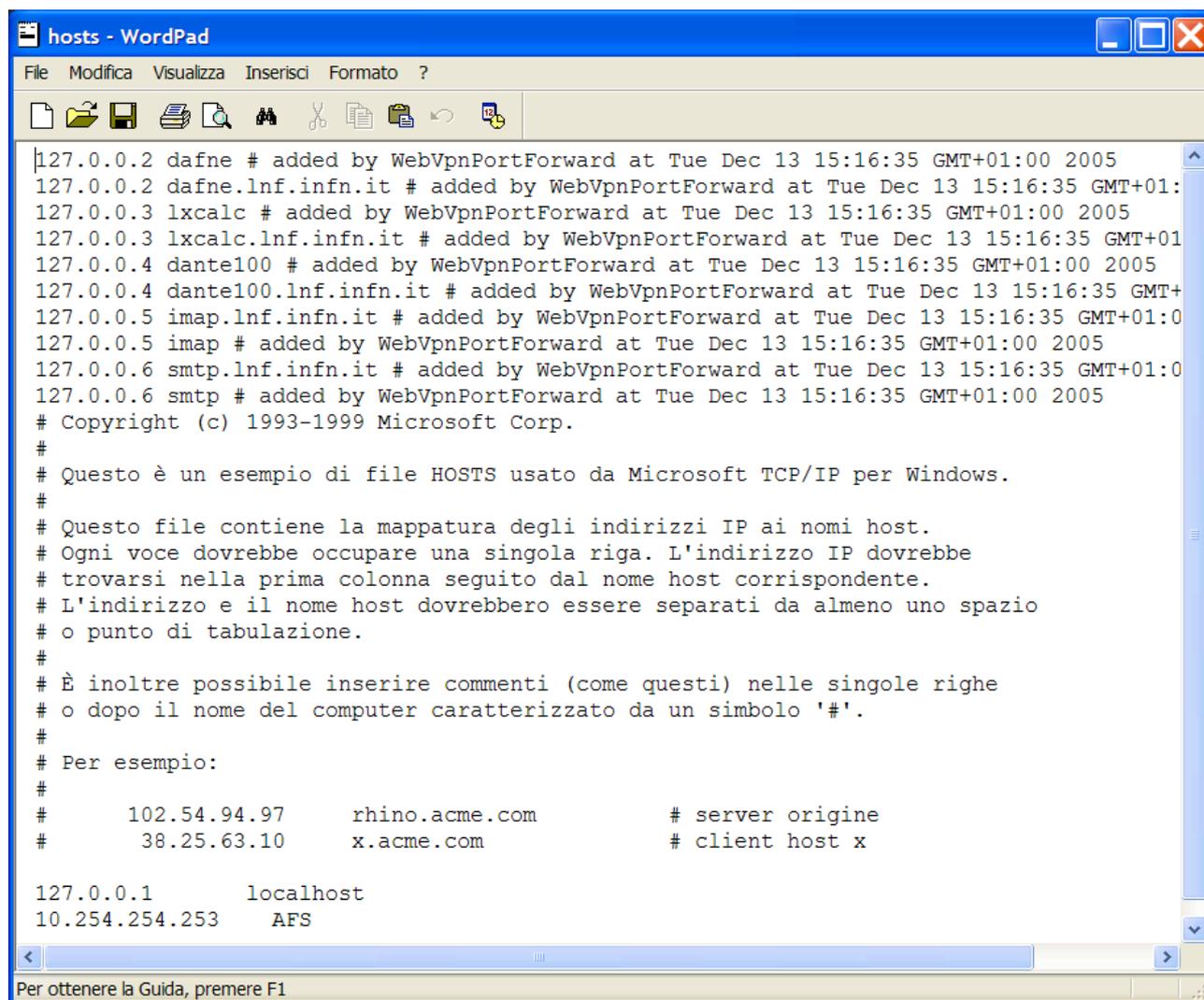
Selezionando lo Start TCP Port forwarding, e' possibile abilitare il forwarding nel tunnel SSL dei servizi configurati. Se non gia' installato, verra' proposta l'installazione della JAVA 2 runtime environment standard edition (J2RE), versione 1.4.2_10 o superiore. Una volta selezionato lo Start TCP Port forwarding dovra' essere confermata l'accettazione del certificato del VPN Concentrator.



Nel nostro esempio l'utente una volta stabilita questa sessione SSL potrà, in maniera trasparente eseguire le seguenti attività:

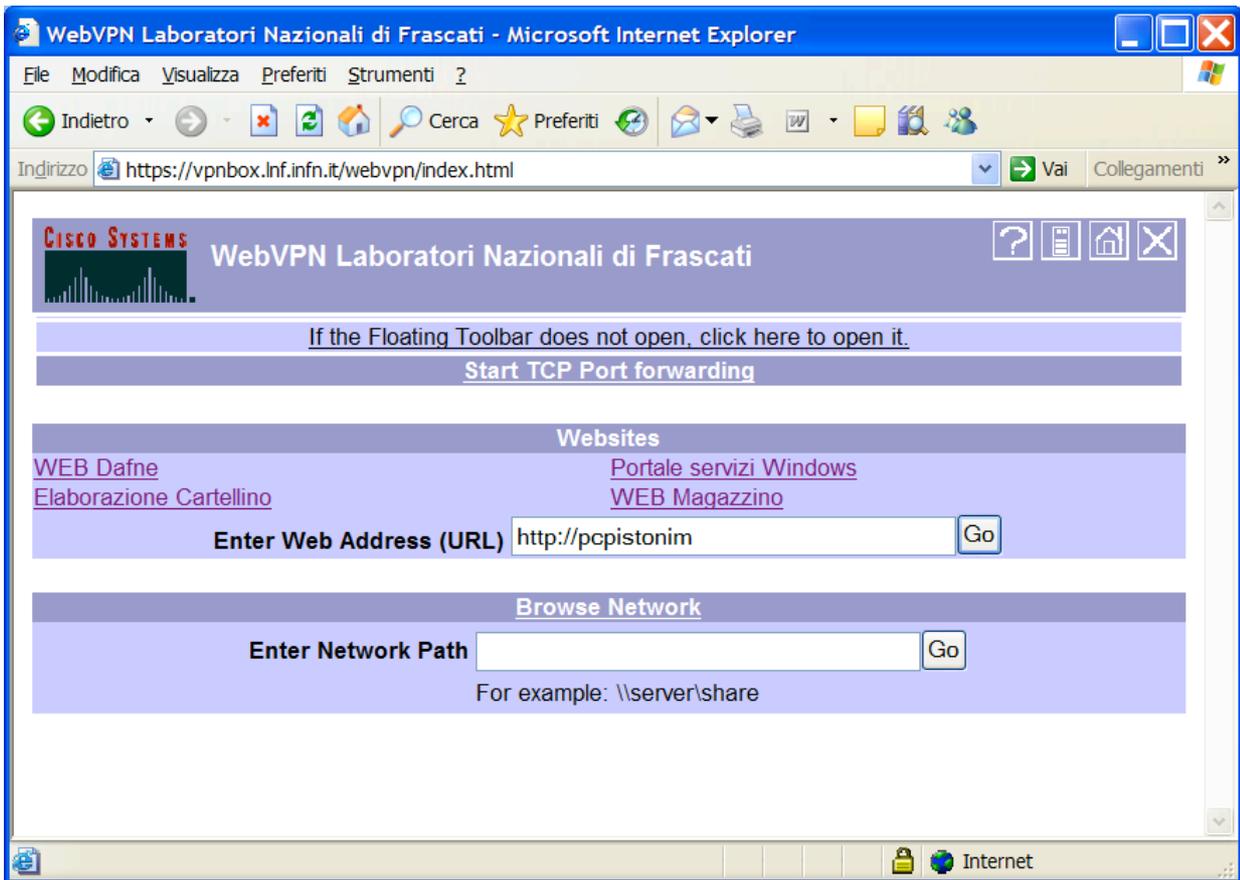
- a. Aprire una connessione SSH con il server dafne normalmente non visibile nella WAN;
- b. Aprire una connessione SSH con la farm di calcolo denominata lxcalc;
- c. Aprire una connessione SSH con il server dante100 avente un indirizzo nascosto;
- d. Aprire il client di posta, configurato con imap.lnf.infn.it e smtp.lnf.infn.it, ed accedere alla posta personale.

Tutto questo è trasparente all'utente, il quale continua ad utilizzare i nomi DNS per accedere a queste risorse. Questo è possibile perché l'applicazione Java edita il file hosts:

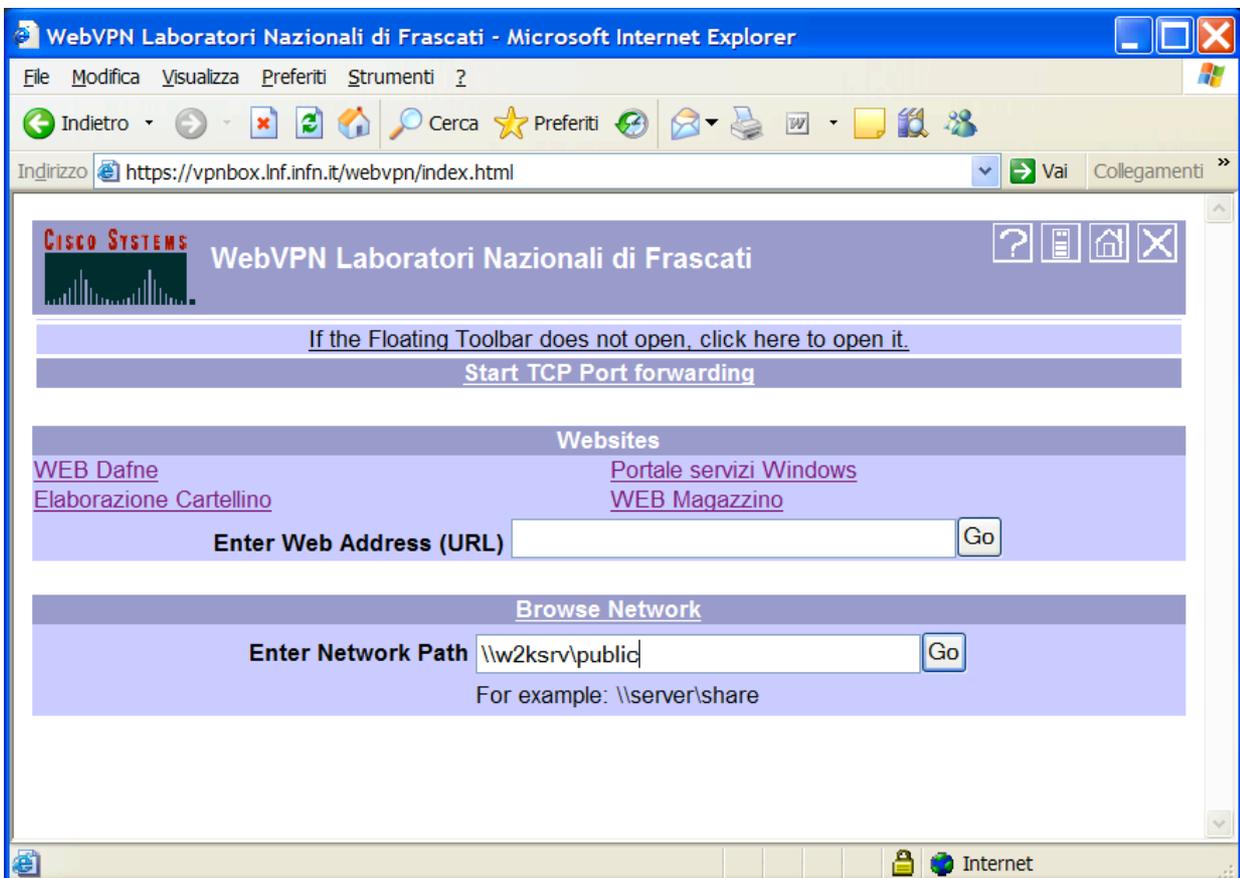


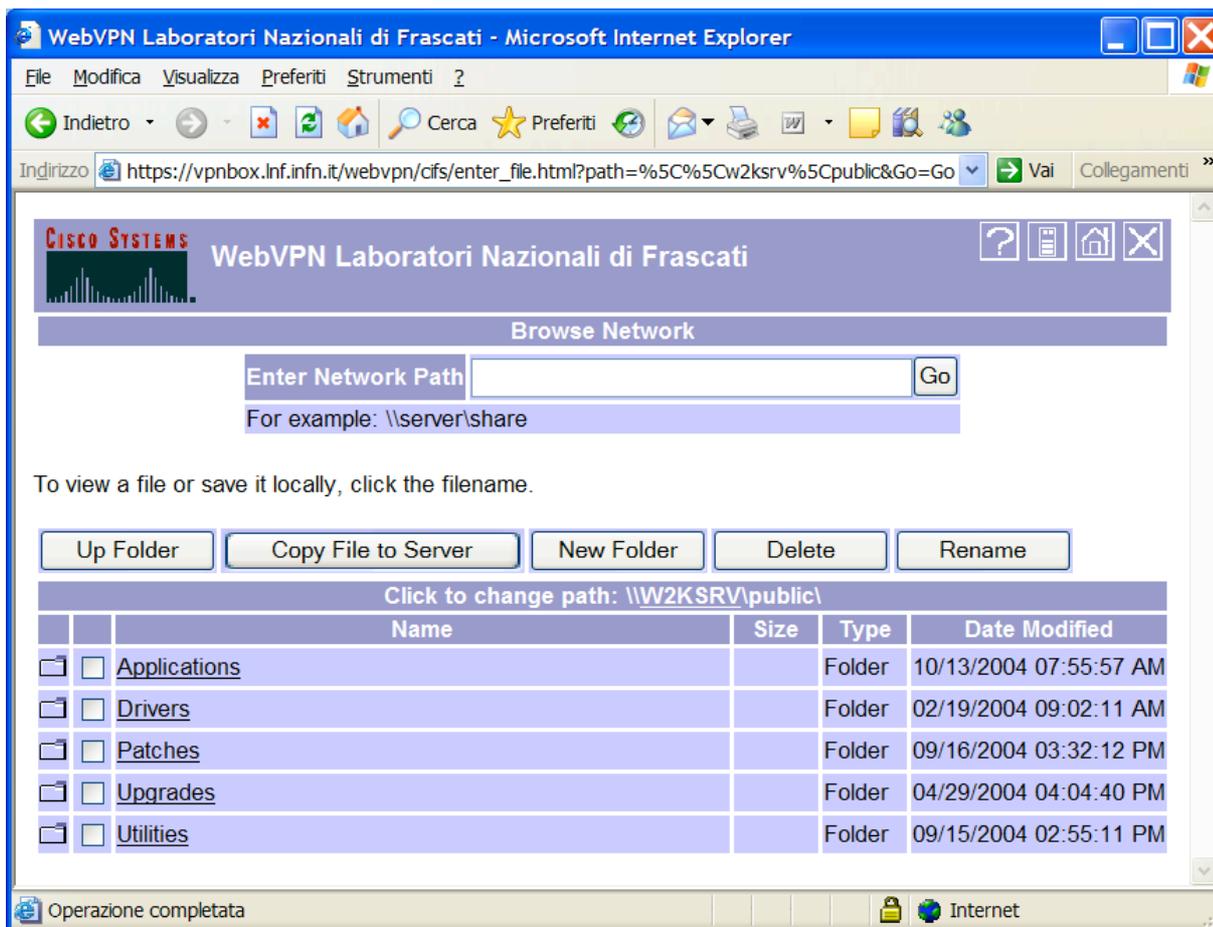
```
hosts - WordPad
File Modifica Visualizza Inserisci Formato ?
|127.0.0.2 dafne # added by WebVpnPortForward at Tue Dec 13 15:16:35 GMT+01:00 2005
127.0.0.2 dafne.lnf.infn.it # added by WebVpnPortForward at Tue Dec 13 15:16:35 GMT+01:
127.0.0.3 lxcalc # added by WebVpnPortForward at Tue Dec 13 15:16:35 GMT+01:00 2005
127.0.0.3 lxcalc.lnf.infn.it # added by WebVpnPortForward at Tue Dec 13 15:16:35 GMT+01
127.0.0.4 dante100 # added by WebVpnPortForward at Tue Dec 13 15:16:35 GMT+01:00 2005
127.0.0.4 dante100.lnf.infn.it # added by WebVpnPortForward at Tue Dec 13 15:16:35 GMT+
127.0.0.5 imap.lnf.infn.it # added by WebVpnPortForward at Tue Dec 13 15:16:35 GMT+01:0
127.0.0.5 imap # added by WebVpnPortForward at Tue Dec 13 15:16:35 GMT+01:00 2005
127.0.0.6 smtp.lnf.infn.it # added by WebVpnPortForward at Tue Dec 13 15:16:35 GMT+01:0
127.0.0.6 smtp # added by WebVpnPortForward at Tue Dec 13 15:16:35 GMT+01:00 2005
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Questo è un esempio di file HOSTS usato da Microsoft TCP/IP per Windows.
#
# Questo file contiene la mappatura degli indirizzi IP ai nomi host.
# Ogni voce dovrebbe occupare una singola riga. L'indirizzo IP dovrebbe
# trovarsi nella prima colonna seguito dal nome host corrispondente.
# L'indirizzo e il nome host dovrebbero essere separati da almeno uno spazio
# o punto di tabulazione.
#
# È inoltre possibile inserire commenti (come questi) nelle singole righe
# o dopo il nome del computer caratterizzato da un simbolo '#'.
#
# Per esempio:
#
#      102.54.94.97      rhino.acme.com      # server origine
#      38.25.63.10     x.acme.com         # client host x
127.0.0.1      localhost
10.254.254.253  AFS
Per ottenere la Guida, premere F1
```

È possibile visualizzare altri siti WEB interni ai Laboratori attraverso la pagina mostrata inizialmente dal vpn concentrator.



Altra funzionalità supportata dal tunnel SSL e' la visualizzazione di cartelle condivise in rete da host windows.





Una funzionalità non operativa è il Browse Network ovvero Sfoglia rete perché non è operativo un server WINS.

11 Performance dichiarate dal costruttore

Il VPN Concentrator supporta sessioni IPsec, PPTP, L2TP/IPsec e WebVPN, ciascuna singolarmente o combinate. L'hardware del VPN Concentrator determina il massimo numero di sessioni supportate. Il costruttore per il modello esaminato dichiara le seguenti performance per il massimo numero di connessioni WebVPN, senza nessun altro tipo di connessioni:

- 500 sessioni WebVPN usando encryption 3DES;
 - Ciascun utente ricerca una pagina web attraverso il WebVPN ogni 60 secondi;
 - Il contenuto delle pagine web include testo in chiaro, file .gif, file .jpg, URLs e file Javascript;
 - Throughput 9Mbps.

Il massimo numero di sessioni IPsec, PPTP & L2TP senza nessuna connessione WebVPN dichiarato dal costruttore è pari a:

- 1500 sessioni con un throughput di 18 Mbps

12 Conclusioni finali

Il VPN Concentrator CISCO rappresenta una valida soluzione per permettere l'accesso alle risorse aziendali normalmente protette da firewall. Il prodotto e' ben documentato ed aggiornato sul sito web Cisco.

Delle due soluzioni studiate IPSec e SSL WebVPN sicuramente la soluzione IPSec e' quella che presenta performance maggiori. Di contro la soluzione WebVPN ha il grande vantaggio di essere clientless.