Networking

VPN Management.†

Fabrizio Valenti[a], Luca Ianniello[b], Giuseppe Nantista[b], Andrea Lora[b], Augusto Pifferi[b]

Il problema dell'accesso ad una rete in modalità sicura è uno degli argomenti che i sistemisti si trovano ad affrontare con maggior frequenza. In una rete di Campus come quella dell'Area della Ricerca RM 1 del Consiglio Nazionale delle Ricerche e di rilevante importanza che il personale, che spesso per motivi di lavoro, si trova in luoghi diversi dalla sede di servizio anche all'estero, possa collegarsi alla propria rete d'Istituto per accedere alle risorse hardware e software di cui ha necessità. In questo articolo sarà descritta la progettazione, la realizzazione ed il testing di un sistema di accesso VPN (Virtual Private Network) crossplatform di campus. Tale progetto nasce dall'esigenza di fornire ai dipendenti del C.N.R. un servizio che dia la possibilità di connettersi dalla propria utenza domestica, dal proprio smartphone o dal proprio tablet alla rete aziendale, instaurando un vero e proprio tunnel di comunicazione sicuro tra la rete esterna e il rispettivo istituto a cui l'utente afferisce.
L'analisi del problema è stata eseguita in maniera piuttosto dettagliata mettendo in luce i meccanismi di sicurezza e cifratura utilizzati per instaurare il tunnel, e le modalità di interfacciamento con le strutture interne (database e strutture gerarchiche) per consentire l'accesso sicuro tramite credenziali e lo scambio dei dati e/o informazioni. Inoltre si è scelto di implementare un'architettura VPN ad hoc, senza l'installazione e la configurazione di software commerciale esistente e disponibile sul mercato, in modo tale da rispondere direttamente ad esigenze partcolari qualora richieste.
Keywords: Virtual Private Network, VLAN, LDAP, L2TP, Open Source, Networking.

1 Introduzione

Le esigenze di connessione tra le sedi remote di un Ente o un'azienda e l'aumento costante del lavoro in mobilità sono cresciute di pari passo con la qualità e la velocità dei collegamenti a banda larga. La conseguenza logica dei questo scenario è l'utilizzo sempre più capillare dei collegamenti VPN. Questo acronimo significa: Virtual Private Network, rete privata virtuale. Generalizzando: l'utilizzo di infrastrutture "pubbliche" fuori dal proprio controllo (e gestione) per implementare un collegamento sicuro tra le diverse sedi di una azienda o tra un "road warrior" e la propria sede. La trattazione tecnica dell'argomento è vasta e complessa, le voci di Wikipedia inglese ed italiana offrono estese spiegazioni e parecchi link di approfondimento, in questo articolo viene descritta la soluzione implementata dai sistemisti dell'Istituto di Cristallografia sulla rete di Campus dell'Area della Ricerca RM 1 del CNR.

2 Virtual Private Network

Una VPN è un'estensione di una LAN (Local Area Network) privata che utilizza link forniti da reti pubbliche come internet o comunque condivise, assicurandone la cifratura e l'autenticazione. In pratica, una VPN emula le proprietà di una rete privata dedicata. Vengono emulate connessioni punto-punto attraverso l'uso del tunneling e l'accesso alla LAN viene assicurato attraverso l'uso di determinati protocolli. Le VPN permettono quindi ad un utente di lavorare a casa o in mobilità (albergo, aeroporto, clienti, ecc.) e connettersi con sicurezza ad un server aziendale remoto utilizzando le infrastrutture di instradamento di reti pubbliche come internet. L'utente vede la VPN come una connessione punto-punto dedicata e privata tra il proprio computer e il server aziendale. In alcune circostanze, i dati trattati da alcuni dipartimenti aziendali sono così riservati che la LAN dipartimentale può essere connessa al server VPN. Gli utenti della rete aziendale che sono dotati di opportune credenziali possono chiedere al VPN server il setup di una connessione virtuale per avere accesso alle risorse protette di un determinato dipartimento: in questo modo i dati sono protetti da meccanismi di crittografia e non possono essere soggetti a sniffing nella parte di rete non protetta; gli utenti

[a] *Elis Corporate School, Via Sandro Sandri 71 - 00159 Roma, Italia.*
[b] *C.N.R. Istituto di Cristallografia, via Salaria Km. 29,300, 00015 Monterotondo (RM), Italia.*

† Rapporto tecnico IC-RM 2017/06 protocollo n. 1226 del 12/07/2017
Questo lavoro è stato oggetto di una tesi di specializzazione nel corso di IT Systems Architect X edizione – Biennio 2011-2013 svolta dall'Ing. Fabrizio Valenti.

sprovvisti di credenziali d'accesso non vedranno neppure quella determinata LAN dipartimentale. È questo è il caso dell'area in cui si implementerà tale servizio, in cui gli utenti muniti di apposite credenziali chiederanno l'inizializzazione della connessione subito dopo essere stati riconosciuti e autenticati da un apposito server e connessi alla vlan di afferenza per accedere alle risorse condivise.

3 Il tunneling

Il tunneling (o encapsulation) consiste nel non inviare una frame nella sua forma originale, ma incapsularlo con un secondo header che protegge il contenuto e contiene le necessarie informazioni per il routing. Il percorso logico attraversato dal pacchetto incapsulato sulla rete si dice tunnel.

Il protocollo di tunnel si occupa sia di creare e mantenere il tunnel sia di traferire i dati nel tunnel stesso. Per creare il tunnel, sia il client che il server devono utilizzare lo stesso protocollo, nel nostro caso L2TP[1] (Layer 2 Tunneling Protocol). I due endpoints di un tunnel L2TP sono chiamati LAC (L2TP Access Concentrator) e LNS (L2TP Network Server). Tale tipo di protocollo utilizza la porta 1701 UDP per comunicare e non possiede alcun meccanismo di criptazione; essa avviene assicurata infatti utilizzando il protocollo di livello 3 IPSec. La combinazione di questi due protocolli è tipicamente nota come L2TP/IPSec. La creazione del tunnel è richiesta dal client ed è inviata al VPN server con una procedura simile al PPP: il VPN server richiede ai vari client di autenticarsi tramite le loro credenziali (con i metodi PAP, MS-CHAP, CHAP e EAP), la connessione viene autorizzata se e solo se l'utente viene riconosciuto dal sistema e può iniziare il trasferimento dei dati. Gli end point del tunnel sono legati da due indirizzi IP del client e del server, rilasciati dinamicamente da un pool di indirizzi precedentemente configurato. L2TP richiede anche una manutenzione del tunnel e le due entità terminali mantengono una reciproca conoscenza del loro stato, in genere attraverso una procedura keep-alive che interroga il corrispondente anche durante le pause del trasferimento dati; anche la fase di terminazione, in genere, è gestita attraverso una serie di messaggi di controllo. Quindi, una volta creato il tunnel, si possono inviare i dati incapsulati nell'header del protocollo di tunnel. Il VPN server riceve i pacchetti incapsulati, rimuove l'header di tunnel e inoltra i pacchetti al destinatario (e viceversa). Esistono due tipi di tunnel: voluntary e compulsory; questi ultimi possono essere static o dynamic, in base alla configurazione del client. I voluntary tunnel sono creati esplicitamente dall'utente client. I compulsory tunnel sono invece creati automaticamente senza un'esplicita richiesta dell'utente: in questo caso, il computer dell'utente non può essere considerato un client endpoint, ma un dispositivo di rete intermedio.

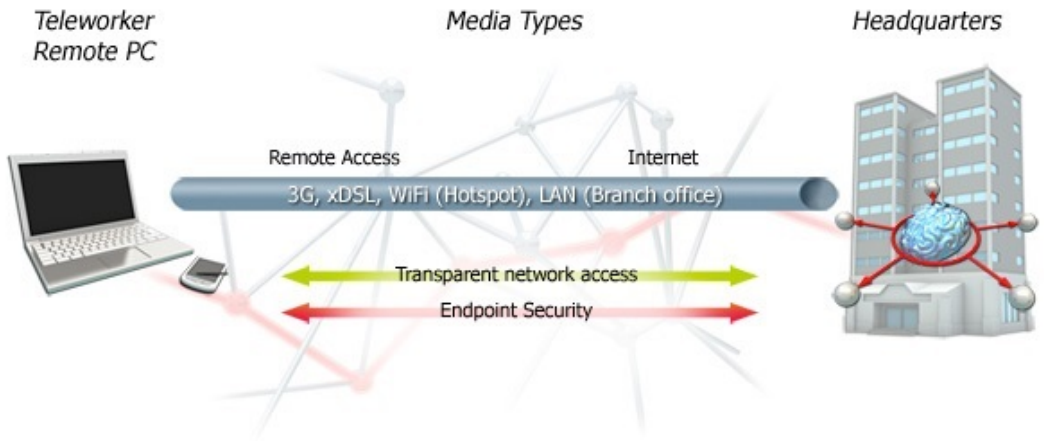

Fig. 1 Virtual Private Network tunneling

4 Creazione del tunnel e configurazione di L2TP/IPSec

Per la configurazione del server VPN, dopo aver installato una distribuzione Debian[2] Linux, su un elaboratore x86 dual-core, è stato utilizzato Openswan[3], implementazione del protocollo IPSec insieme a xl2tpd demone del protocollo di tunneling L2TP.

Nel server sono state installate due schede di rete: la prima eth1 (configurata con un indirizzo IP pubblico) che si interfaccia con l'esterno, favorendo quindi la comunicazione con i nodi remoti, mentre la seconda l'eth0 funge da trunk per consentire il traffico dei dati verso la rispettiva vlan dei vari istituti. Prima di configurare il server inoltre è stato configurato il firewall esterno in maniera tale da assicurare che il traffico UDP fosse consentito sulle porte 500 (IKE – Internet Key Exchange) e 4500 (IPSec Nat traversal). Successivamente è stato abilitato IP forwarding editando il file */etc/sysctl.conf* per configurare alcuni parametri del sistema operativo all'interno di Debian. In particolare i seguenti parametri:

```
net.ipv4.ip_forward = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
```

Il processo di creazione del tunnel L2TP/Ipsec segue i seguenti passi:

- Negoziazione di Ipsec security association (SA – insieme di elementi comuni utili ai due end per instaurare la connessione) che avviene attraverso lo scambio di una chiave (IKE);

- Creazione della comunicazione Encapsulating Security Payload (ESP – strumento che fornisce integrità, protezione e autenticità dei pacchetti). L'ip protocol number dell'ESP è il 50;

- Il processo di creazione e comunicazione del tunnel L2TP avviene attraverso la negoziazione dei parametri sul canale sicuro IPsec instaurato nella fase precedente.

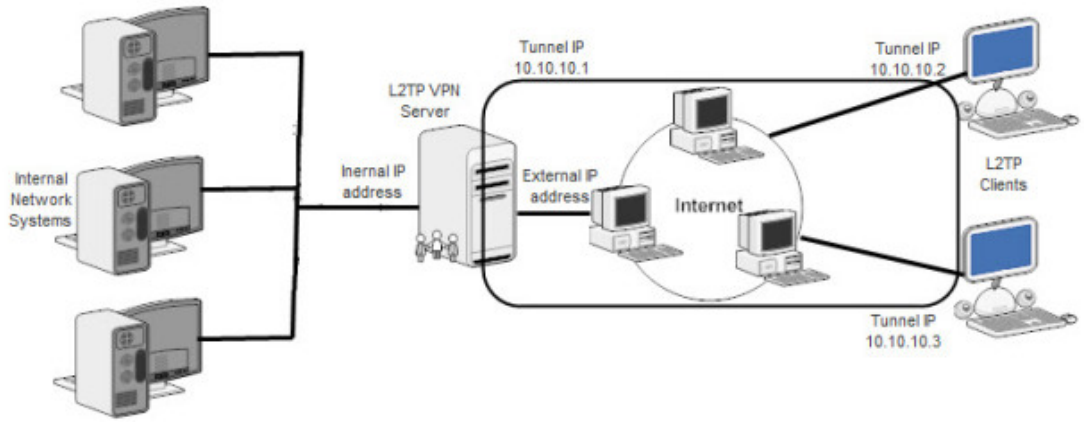

Fig. 2 L2TP "LAN"

5 Configurazione del protocollo IPSec

Subito dopo aver installato i packages attraverso il comando apt-get install openswan xl2tpd è stato configurato IPSec editando il principale file di configurazione di Openswan /etc/ipsec.conf nel seguente modo:

```
config setup
nat_traversal=yes virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12
oe=off
protostack=netkey
conn L2TP-PSK
authby=secret
pfs=no
auto=add
keyingtries=3
rekey=yes
ikelifetime=8h
keylife=1h
type=transport
left= "global ip-address"
leftnexthop=%defaultroute
leftprotoport=17/1701
right=%any
rightprotoport=17/%any
```

6 Discussione

Openswan, per individuare i nodi coinvolti in una connessione, utilizza i termini left e right piuttosto che utilizzare i termini locale e remoto. Il modo con cui i partecipanti alla comunicazione sono identificati come dispositivi left o right è arbitrario e viene stabilito attraverso un diagramma di rete prestabilito. In questo caso reale è stato individuato come dispositivo left il server VPN di Campus mentre come dispositivo right i vari client remoti che effettuano delle richieste. Inoltre è stato configurato un metodo di autenticazione basato su PSK (preshared key) per essere facilmente compatibile con i client che utilizzano differenti piattaforme. Altri meccanismi di autenticazione si basano su certificati (X.509) oppure su chiavi private RSA. Queste chiavi sono utilizzate da ipsec_pluto, il demone IKE di Openswan, affinché i client remoti siano autenticati. Per impostare la chiave PSK è necessario editatare il file /etc/ipsec.secrets aggiungendo per ogni utente che ottiene l'accesso al server la seguente voce:

```
Ip-address : PSK "chiave condivisa"
```

dove al posto del valore ip-address occorre scrivere l'indirizzo ip del collegamento punto-punto rilasciato al client e il campo chiave condivisa sarà modificato con una PSK scelta in fase di registrazione all'utente.

7 Configurazione del protocollo L2TP

Per configurare il demone del protocollo L2TP, precedentemente installato, si procede alla modifica del file di configurazione localizzato su */etc/xl2tpd/xl2tpd.conf* nella seguente maniera

```
[global]
ipsec saref = yes
listen-addr = "IP pubblico del server"
[lns default]
ip range = "pool di indirizzi da assegnare agli utenti remoti"
local ip = "ip dell'interfaccia locale"
refuse chap = no
refuse pap = yes
require authentication = yes
name= "nome del server VPN"
debug = yes
pppoptfile = /etc/ppp/options.xl2tpd
length bit = yes
```

Questo file contiene la configurazione per far siche il tunnel venga instaurato; all'attributo ip-range è stato dato un particolare pool di indirizzi che verranno assegnati successivamente ai vari client VPN nel momento in cui richiederanno la connessione al server VPN. Il local ip rappresenta il gateway locale con cui i vari client remoti comunicheranno quando verranno instaurati i collegamenti punto-punto. Infine per quanto riguarda i meccanismi di autenticazione al server VPN si è scelto di escludere il sistema di autenticazione utilizzando PAP (Password authentication protocol) in quanto poco sicuro permettendo invece altri schemi di autenticazione quali CHAP (challenge-handshake authentication protocol) e MS-CHAPv2. Dopo aver configurato questi file è necessario riavviare sia Openswan che xl2tpd con i seguenti comandi: */etc/init.d/ipsec restart* e */etc/init.d/xl2tpd restart*.

8 Sistema di autenticazione

Le tabelle possono includere o non includere linee verticali. Il modo con cui i nodi remoti vengono autenticati al server è gestito mediante un apposito file in grado di gestire e contenere le credenziali di accesso degli utenti autorizzati a usufruire di tale servizio VPN. Il file risiede in */etc/ppp/chap-secrets* e ha una struttura simile alla seguente:

```
# client    server    secret      IP-address
User1       vpn       password    static o dynamic address
```

Il campo client insieme al campo secret consentono di specificare lo username e la password richiesti prima di instaurare la connessione. Il campo server specifica il nome dato al server VPN all'interno del file */etc/xl2tpd/xl2tpd.conf*, mentre il campo ip-address permette di associare a quel relativo user un indirizzo ip statico, dinamicamente scelto tra un pool di indirizzi ben preciso oppure il simbolo "*" permette di attribuirgli un qualsiasi indirizzo disponibile del pool dichiarato all'interno del file */etc/xl2tpd/xl2tpd.conf*.

Per fare in modo che gli utenti si autentichino al sistema utilizzando le stesse credenziali adoperate per accedere ai portali e ai servizi interni all'area di ricerca è stato configurato un server RADIUS all'interno del server VPN con backend LDAP (Lightweight Directory Access Protocol – protocollo utilizzato per la gestione dei servizi di directory) già esistente. Inoltre in base al tipo di utente che ha richiesto l'acceso al server VPN uno script sarà istruito a eseguire un'operazione di NAT (spiegata nel paragrafo successivo) per fare in modo che l'utente navighi con un indirizzo ip appartenente alla sua vlan dipartimentale.

9 Configurazione interfacce VLAN

Per permettere a un nodo (client VPN) di essere identificato tramite un indirizzo IP appartenente alla vlan dipartimentale, sono stati individuati alcuni pool di indirizzi utilizzati esclusivamente per permettere tali collegamenti remoti. Inoltre per dare la possibilità a ciascun nodo remoto di interfacciarsi con l'esterno (internet) si è dovuto configurare l'interfaccia trunk (eth0) per far scorrere tutto il traffico tagged. Per eseguire tale operazione è stata aggiunta in */etc/modules* la voce *8021q* e alla sezione iface del file */etc/network/interfaces* il seguente parametro: *vlan-raw-device eth0*.

Inoltre ogni qualvolta un utente richiede di instaurare una connessione con il server VPN uno script in bash avrà il compito di inserire all'interno del file /etc/network/interfaces un'interfaccia vlan con il tag dell'istituto a cui l'utente afferisce; ad esempio:

```
ifconfig eth0.2310 indirizzo-ip netmask 255.255.255.0 broadcast broadcast up
```

Nel caso in cui la richiesta di connessione al VPN server provenga da più di un client appartenente alla stessa vlan lo script aggiungerà un alias di interfaccia che permetterà alla stessa di essere configurata con più indirizzi IP. Ciò avviene eseguendo il comando:

```
ifconfig eth0.2310:0 indirizzo-ip netmask 255.255.255.0 broadcast broadcast up
```

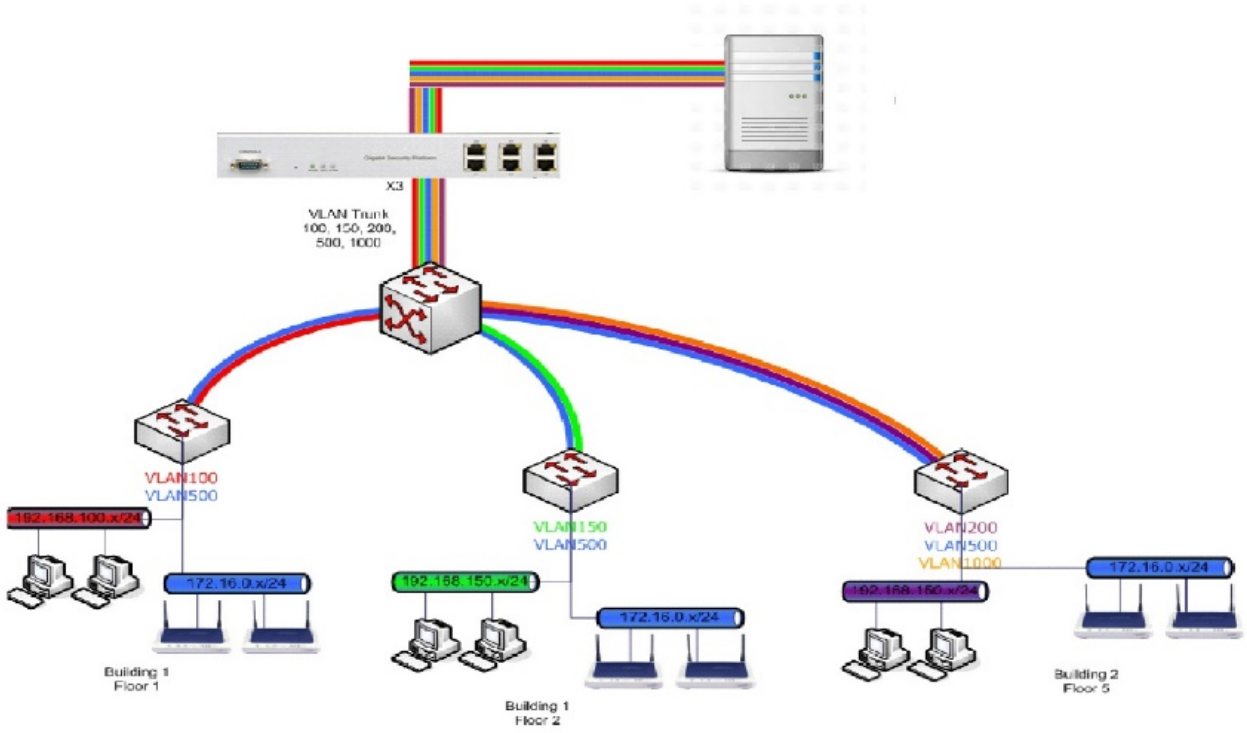

Fig. 3 Schema concentratore VPN

Per permettere al client remoto di essere raggiunto come se fosse all'interno del proprio istituto, è stato configurato il firewall iptables in maniera tale che l'indirizzo ip rilasciato al client (dal server nel momento in cui è stato instaurato il collegamento punto-punto attraverso l'interfaccia eth1) venga tradotto con l'indirizzo ip dell'interfaccia tagged vlan, eseguendo quindi un'operazione di NAT (network address traslation). Iptables è uno strumento fornito dal linux kernel firewall che svolge alcune funzionalità in grado di manipolare i pacchetti in ingresso e/o in uscita. Quindi, se ad esempio un client VPN ha ottenuto un indirizzo pari a 192.168.0.10/24 l'operazione di NAT viene eseguita aggiungendo una regola al file */etc/iptable/rule.v4* in grado di modificare l'indirizzo sorgente all'interno dell'header del pacchetto con quello del rispettivo alias d'interfaccia vlan. La regola da aggiungere è la seguente:

```
-A POSTROUTING -s source-address -o out-interface -j SNAT --to address
```

Infine per instradare i pacchetti al rispettivo gateway si è fatto in modo che esistano più di una tabella di routing all'interno del server VPN oltre alla main table o default table; in questo modo secondo l'ip sorgente del pacchetto è possibile scegliere una routing table piuttosto che un'altra. Per attivare questo routing avanzato dei pacchetti sui sistemi Debian è possibile installare il package iproute attraverso il comando *apt-get install iproute*; Per aggiungere delle secondary routing table è stato modificato il file */etc/iproute2/rt_table* nel seguente modo:

```
# reserved values
255     local
254     main
253     default
0       unspec
# local
2 istituto1
3 istituto2
...
```

In alternativa si possono aggiungere altre routing table attraverso il commando:

```
echo 2 istituto1 >> /etc/iproute2/rt_table
```

Dopo aver dichiarato le nuove routing table all'interno del precedente file si è proceduto alla configurazione, per ciascuna di esse, di una rotta di default attraverso il commando:

```
ip route add default via gw-address dev out-if table name
```

Per far si che esse vengano utilizzate in sostituzione della main routing table si è usato il comando *ip rule* per comunicare al kernel quale delle tante utilizzare in accordo con l'indirizzo sorgente contenuto all'interno del pacchetto ip. Per aggiungere una nuova regola si utilizza la seguente istruzione:

```
ip rule add from source-address lookup routing-table prio n-priority
```

Con il precedente comando è stata aggiunta una nuova regola per tutti i pacchetti che possiedono come indirizzo IP sorgente quello specificato dopo l'attributo *from*; in questo caso il pacchetto sarà processato a seconda delle voci presenti all'interno della tabella di routing dichiarata subito dopo l'attributo lookup. Per visualizzare l'insieme di tutte le regole impostate all'interno del server basta lanciare il comando *ip rule*.

10 Software lato client

L'utente dovrà installare sul proprio terminale (pc, desktop, laptop, mobile...) un client VPN. Tra i diversi software esistenti, quale client VPN, SoftEther2[4] è stato ritenuto il più userfriendly tra quelli disponibili gratuitamente. Il sistema si basa sul software opensource SoftEther, sviluppato dall'Università di Tsukuba, in Giappone. I suoi punti di forza sono essenzialmente due: In primo luogo, a differenza di altri software analoghi, SoftEther offre la possibilità di connettere il proprio PC da remoto direttamente alla LAN del proprio dominio di broadcast (nel nostro caso d'Istituto), con il vantaggio di condividere file e risorse come quando si è in ufficio. Sistemi simili "vincolano" l'utente remoto in una porzione di rete isolata, senza la possibilità di interagire direttamente con i PC presenti in ufficio. In secondo luogo la VPN utilizza la porta standard 443 (HTTPS) e quindi è possibile instaurare una VPN verso l'ufficio ogni qual volta si è connessi a una rete che consenta la semplice navigazione web. Altri sistemi richiedono l'utilizzo di porte speciali, come la porta 500 o 4500, che molte reti non consentono di usare se non dietro richiesta di assistenza. La porta HTTPS invece è sempre abilitata e non filtrata.

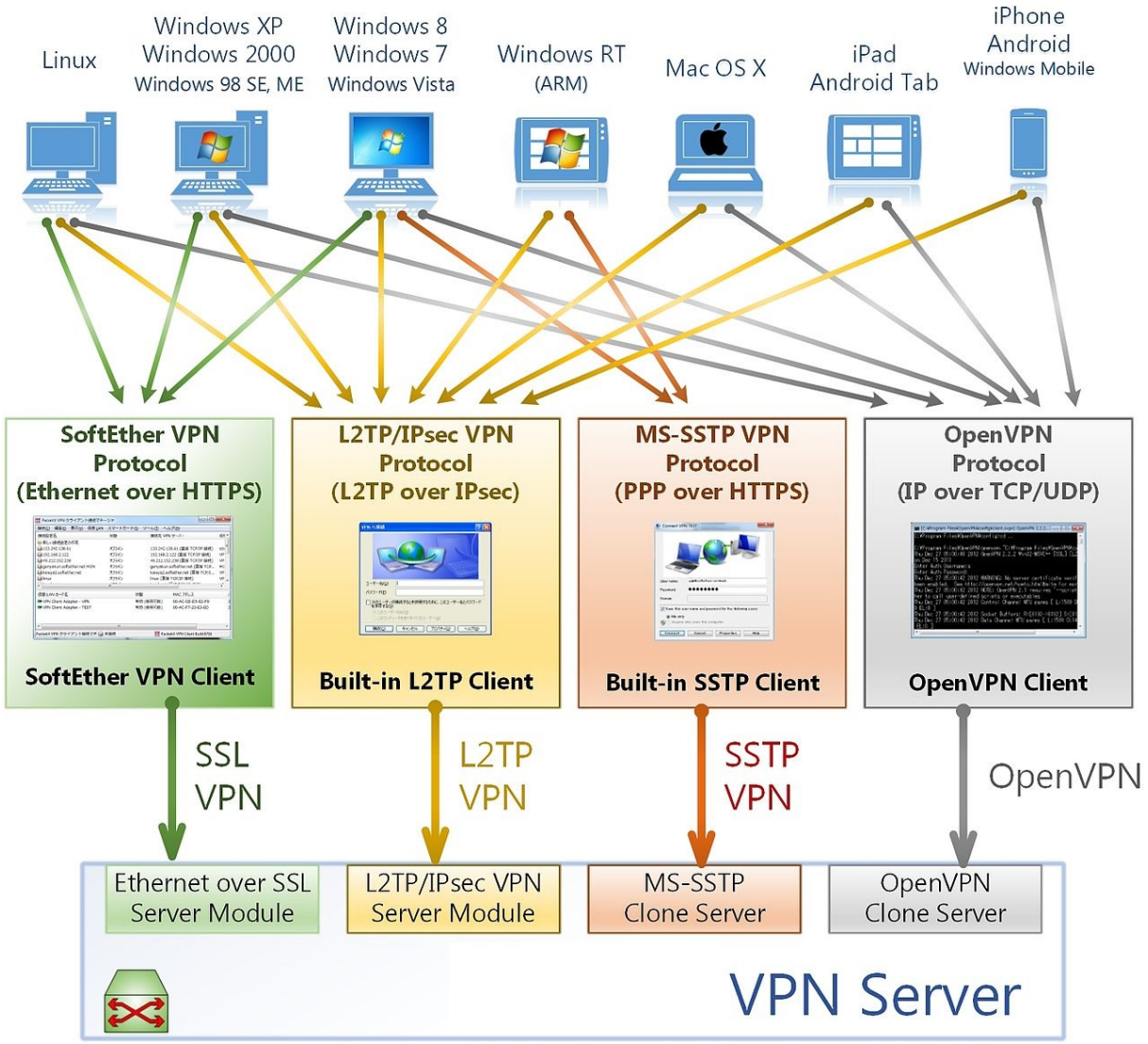

Fig. 4 Esempi di client VPN per dispositivi diversi

11 Conclusioni

Il servizio di VPN è stato attivato inizialmente per l'Istituto di Cristallografia e poi via via esteso anche ad altri istituti dell'area. Tra i vantaggi che si possono annoverare va sicuramente evidenziato quello di mantenere elevati i livelli di sicurezza per le risorse

presenti nelle reti di Istituto in quanto, grazie a questo sistema, queste risorse non vengono esposte nella rete pubblica,oltre a rendere disponibili le stesse risorse informatiche (storage, stampanti, PC collegati a strumentazione etc.). Un secondo notevole vantaggio è quello di poter consultare da remoto, in qualsiasi parte del mondo e collegati alla rete di un qualsiasi provider, le riviste in abbonamento dell'area che sono accessibili solamente se si ha un IP address incluso tra quelli abilitati a consultare le biblioteche on line per le quali il CNR ha stipulato contratti di abbonamento. Infine la sicurezza; ovunque si abbia accesso ad Internet (piazze digitali, Internet cafè, alberghi, reti wireless e cablate in genere) il proprio dispositivo dialoga con il server in modalità criptata rendendo impossibile l'intercettazione e il furto dei propri dati da parte di malintenzionati.

Riferimenti bibliografici

1 https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol.
2 www.debian.org/index.it.html.
3 www.openswan.org.
4 www.softether.org.