PROJECTE DE RECERCA BÀSICA O APLICADA PAC3 — TERCERA PROVA D'AVALUACIÓ CONTINUADA

Cognoms: *Boronat Pérez*
Nom: *Antonio*

RESPOSTES

TÍTOL

Anàlisi i proves de túnels en xarxes de guifi.net

AUTORS

Dr. Miguel Pérez Francisco
Antonio Boronat Pérez

DEPARTAMENT

Universitat Jaume I
Escuela Superior de Tecnología y Ciencias Experimentales
Departamento de Ingeniería y Ciencia de los Computadores
Campus de Riu Sec, Edifici TI - Castelló

RESUM

La xarxa lliure guifi.net s'utilitza com una infraestructura de comunicacions on es permet donar serveis en forma d'autoprestació o a tercers, en modalitats tant obertes, tancades o comercials, sent l'accés a Internet el més sol·licitat. El fet de tindre disponible la xarxa i donada la seua filosofia (basada en el moviment del programari lliure) està provocant noves necessitats tecnològiques entre els seus participants (ciutadans, empreses o administracions públiques). Una d'estes necessitats és la utilització de túnels. La necessitat de l'ús de túnels es dóna quan s'ha de connectar directament dos xarxes o adreces passant per altres subjacents. D'altra banda, vist que la major part de guifi.net funciona en forma sense fils, és desitjable que el tràfic del túnel siga xifrat. Guifi.net no assegura esta possibilitat quedant en mà dels usuaris i de moment no s'ha proposat cap solució concreta. Amb els túnels que es fan no es sap quin rendiment tenen ni la sobrecàrrega de CPU que suposen. Per tant, dels diferents tipus de túnels no es coneix quin és el millor per a cada escenari. Aquest treball analitza els túnels més populars que són suportats pel maquinari habitualment implantat a la xarxa guifi.net.

INTRODUCCIÓ

Guifi.net és una xarxa lliure usada com infraestructura de comunicacions on trobem nodes connectats de forma oberta o tancada, als quals es poden associar usuaris amb diferents necessitats. Alguns dels quals només requerixen accés a Internet, mentre que altres, a més accedixen a serveis oberts o privats proveïts a través d'aquesta xarxa. Així que dins d'aquest ventall d'escenaris en trobem alguns on es fa necessari disposar de mecanismes que garantisquen una connexió confidencial i fiable entre

xarxes o nodes interconnectats per guifi.net. Actualment, hi ha diferents solucions per a establir túnels o xarxes privades virtuals (VPN) entre elements enllaçats mitjançant una xarxa pública, al nostre cas guifi.net. Aplicar alguna d'estes solucions per a aconseguir un medi de comunicació segur i privat té un cost computacional als nodes que establixen el túnel, ja que hi ha un esforç de gestió, normalment s'apliquen tècniques de xifratge i/o compressió a la informació tramesa i a més s'introduïx una sobrecàrrega en la quantitat de bytes a enviar donat que els paquets de dades originals són encapsulats dins dels paquets enviats a través del túnel, de forma que a la grandària de les dades originals hi ha que afegir els bytes corresponents a les noves capçaleres dels paquets del túnel. Queda patent que en usar un túnel es produïx un augment del consum de recursos, bàsicament de consum de CPU i una reducció de l'ample de banda de transferència de dades entre els elements units pel túnel [Shashank Khanvilkar-Khokhar04] [Castro-Evans00]. Aquests requeriments fan necessari un estudi de les solucions aplicables per a crear túnels sobre el maquinari i sistemes emprats habitualment a la xarxa guifi.net, sent aquest l'objectiu del nostre treball.

Per a realitzar les proves en l'anàlisi de túnels aplicables a les necessitats de guifi.net, s'ha seleccionat un conjunt de maquinari característic en aquesta infraestructura, tenint en compte que siguen fàcils d'aconseguir i amb un preu assequible, però alhora amb una eficiència provada. D'altra banda, s'ha escollit el programari amb codi obert [Shashank Khanvilkar-Khokhar04] més usat en la implantació de túnels i que puga ser instal·lat sense problemes al maquinari de les proves amb l'objectiu d'avaluar el consum de CPU i la taxa de transferència obtinguda per a poder seleccionar la millor solució maquinari / túnel.

Els elements seleccionats per a les proves són:

- Ordinadors entre els quals s'establix el túnel, que poden actuar com encaminadors o bé elements finals entre els que es crea el túnel.
- Encaminadors Mikrotik RouterBoard
- Encaminadors amb accés sense fils TP-LINK
- Antenes per a enllaç sense fils Ubiquiti NanoStation.

I el programari per a implementar els túnels s'ha optat per les solucions més habituals per a túnels amb programari de codi obert i sense cost:

- PPTP (http://tools.ietf.org/html/rfc2637)
- L2TP + IPSEC (http://tools.ietf.org/html/rfc2661) + (http://tools.ietf.org/html/rfc4301)
- OpenSSH (http://www.openssh.com/)
- OpenVPN (http://openvpn.net/)

La resta del document detalla les proves realitzades per tal de mesurar el rendiments i comparar les diferents solucions.

ENTORN DE PROVES I EINES

Per a realitzar les proves de rendiment dels túnels sobre els diferents maquinaris hem emprat, dos ordinadors exactament iguals, tant en la configuració de maquinari com en el programari, són Toshiba Tecra Centrino Duo amb 2 GB de memòria RAM i amb sistema operatiu Lliurex 12.06 Escriptori, distribució de Linux basada en Ubuntu 10.04. Estos ordinadors han fet de servidor i client d'FTP i d'Iperf per a mesurar la velocitat de transferència de dades.
A les proves en les quals només intervenien els dos ordinadors connectats per cable s'han fet proves usant tant un hub Micronet SP508, com un switch Longshine LCS - 883R - SW800M+, però els resultats han estat semblants, no considerant-se estos elements de connexió determinants en els resultats. Les proves equivalents però amb connexió sense fils s'ha usat un punt d'accés Observa Telecom AW4062.
El maquinari seleccionat de guifi.net per a les proves de túnels ha estat:

- Dos encaminadors Mikrotik RouterBoard 750 GL amb sistema operatiu Router OS v 5.2.
- Dos encaminadors amb punt d'accés sense fils TP-LINK TL-WR740N amb sistema operatiu OpenWRT Backfire 10.03.
- Dos antenes per a connexió sense fils Ubiquiti NanoStation2 a 2,4 GHz.

Junt amb els sistemes descrits, s'ha usat el programari:

- Amb els ordinadors s'ha avaluat OpenSSH v. 5.3 p1 - OpenSSL 0.9.8 i OpenVPN v. 2.1.0.
- Per a la transferència de dades el servidor ProFTP v. 1.3.2, i la utilitat Iperf v. 2.0.4 que mesura la taxa de transferència, i amb l'ordre top s'ha recollit el consum de CPU en l'ús del túnel. En els encaminadors Mikrotik el consum de CPU s'ha mesurat amb /system resource monitor.
- Als encaminadors Mikrotik s'ha configurat tres tipus de túnel: PPTP, L2TP+IPSEC i OpenVPN usant els mòduls incorporats al sistema RouterOS.
- Per als encaminadors TP-LINK, només s'ha avaluat el túnel corresponent a OpenVPN. Els mòduls PPTP i L2TP+IPSEC no s'han configurat per que el rendiment d'aquests encaminadors és similar als de Mikrotik on s'ha comprovat que L2TP+IPSEC té un rendiment molt pobre comparat amb OpenVPN i a pesar que els túnels PPTP tenen un rendiment acceptable no s'aconsella el seu ús per la feblesa de l'algorisme xifratge RC4, ben documentada tant en publicacions com a Internet, especialment per ser el mateix xifratge que usa l'encriptació WEP a les xarxes sense fils. [Schneier05][Schneier99]

PROVES REALITZADES

Les proves realitzades en totes les configuracions per a mesurar la velocitat de transferència han consistit en:

- Obrir des del client una sessió d'ftp amb el servidor i realitzar cinc operacions put amb un fitxer i tancar la sessió. De cada prova es pren la velocitat de la transferència mesurada en 1000 bytes per segon (KB/s).
- Obrir dels del client una sessió d'ftp amb el servidor i realitzar cinc operacions get amb el mateix fitxer que al punt anterior i tancar la sessió. Es fan put i get per a mesurar la velocitat de transferència en els dos sentits de la connexió.
- Les dos proves anteriors es repetixen per a tots els fitxers emprats en l'estudi. Els fitxers són de dos grandàries, un de 100 MB i l'altre de 225 MB i de cada grandària hi ha de tres tipus:
  - Fitxers comprimits, un de 100 MB creat amb rar i un de 225 MB que conté vídeo xvid.
  - Fitxers amb contingut aleatori creats amb l'ordre dd i el dispositiu /dev/urandom.
  - Fitxers de text.

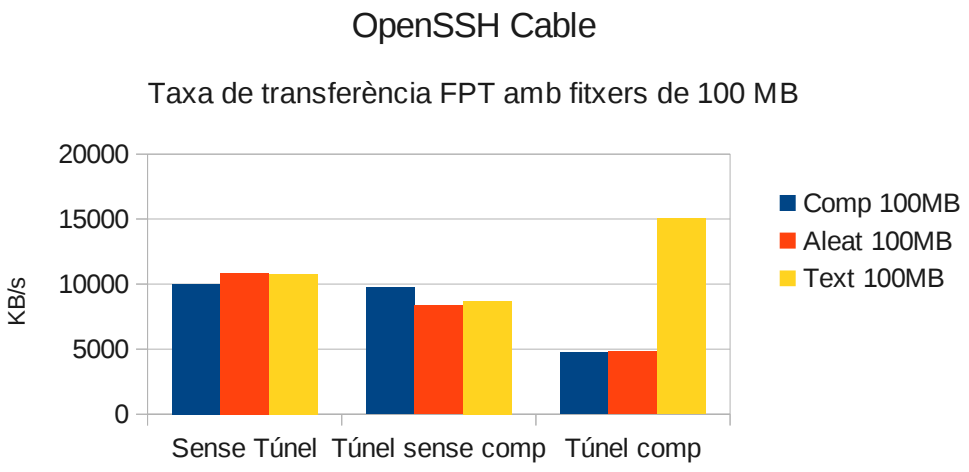
  L'objectiu d'usar diferents tipus de continguts als fitxers ha estat el poder avaluar l'efecte de la compressió sobre la taxa de transferència.
- Per a cada configuració s'ha executat tres vegades en cada sentit de la connexió la utilitat Iperf [Shashank Khanvilkar-Khokhar04] [Castro-Evans00] per a mesurar la taxa de transferència independentment de les proves d'ftp.
- Als tests executats amb els ordinadors com a gestors dels túnels i amb els encaminadors TP-LINK, durant les proves de transferència, s'ha executat l'ordre top (top -b > fitxer) per a recollir els consums de CPU. Als encaminadors Mikrotik esta informació s'ha recollit usant /system resource monitor.

Les configuracions emprades per a les proves han estat pensades amb l'objectiu de valorar l'aptitud dels diferents túnels per a aplicar-los a les necessitats plantejades en la implantació de la xarxa guifi.net. Les receptes usades sobre els sistemes estan detallades a l'últim punt del document.

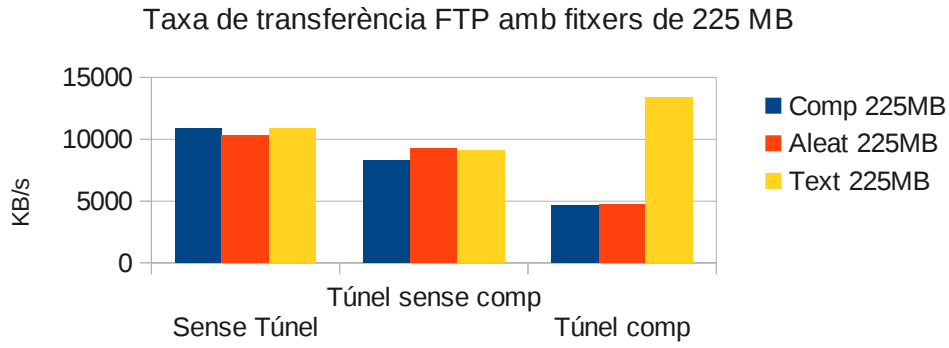
A continuació es mostren els resultats obtinguts pels diferents túnels provats:

Túnel OpenSSH sobre els ordinadors

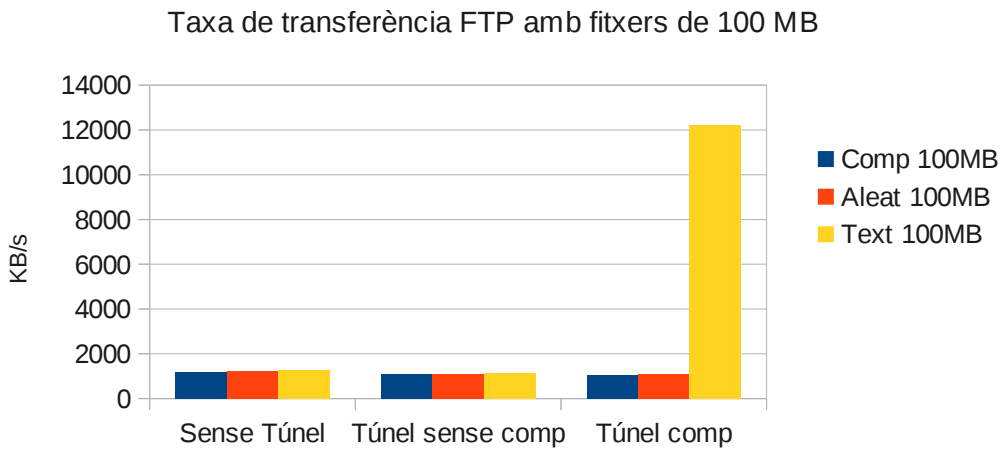
S'avaluen les connexions per cable i per punt d'accés sense fils.



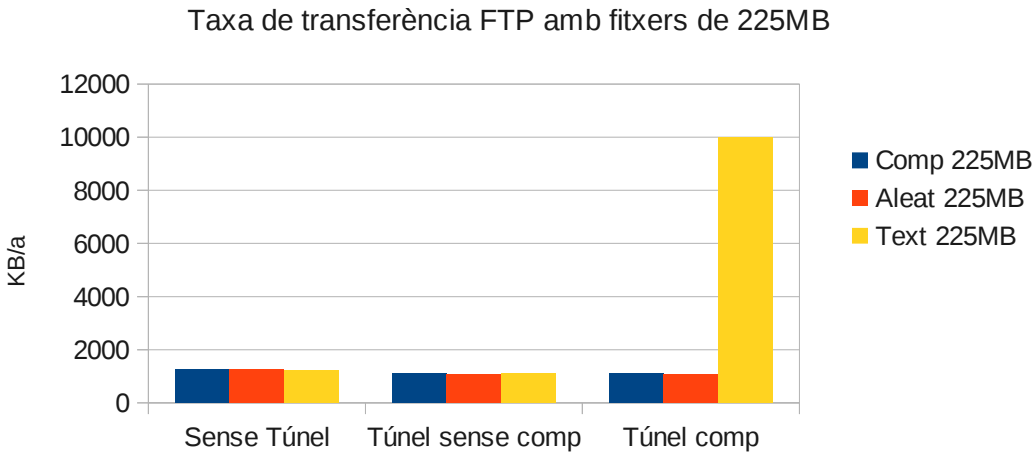
OpenSSH Cable

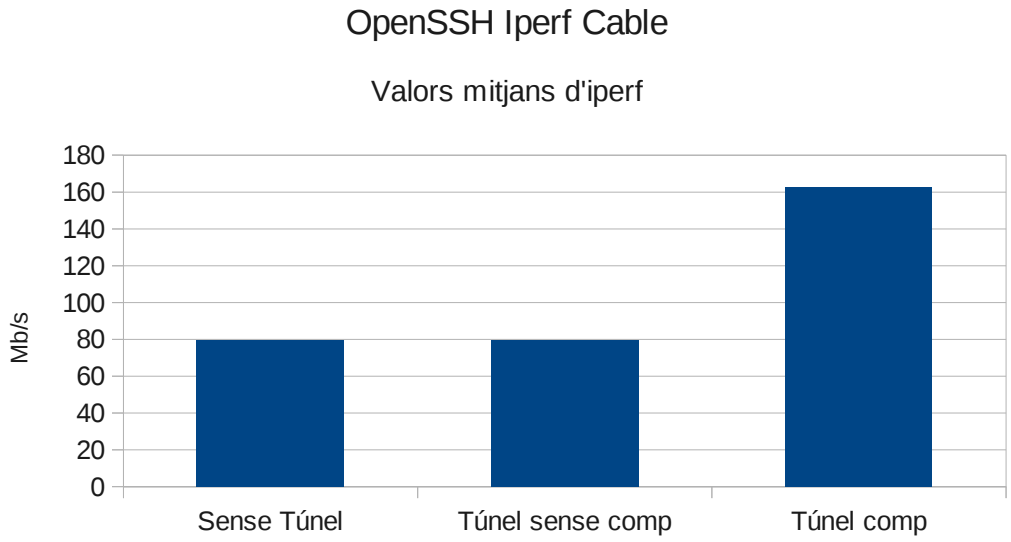


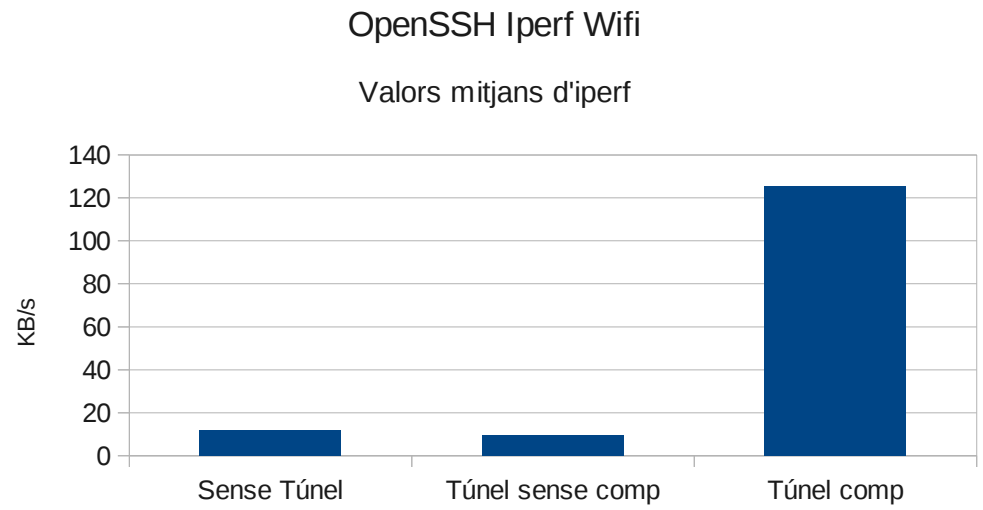
OpenSSH Wifi



OpenSSH Wifi







En primer lloc queda patent la reducció de rendiment en usar el túnel, cosa que s'accentua si a més s'activa la compressió de les dades, estes minves són les que justifiquen este estudi, de forma que comparant els resultats dels diferents túnels ajuden a decidir el més apropiat per als escenaris on són requerits pels usuaris de guifi.net.
Destaquem de les gràfiques que el pes d'usar el túnel es nota menys amb la connexió sense fils per ser més lenta i disposar de més temps en la tramesa per a realitzar les operacions requerides, està d'acord amb l'indicat a [Castro-Evans00] que compara una connexió ràpida com ethernet amb una lenta de tipus sèrie.
Pel que fa als resultats en la transferència dels fitxers de text i d'iperf es veu clarament l'impacte d'usar la compressió que millora ostensiblement les taxes de transferència.
Cal dir que este túnel s'ha col·lapsat diverses vegades, especialment en la transferència dels fitxers de 225 MBytes, no hem trobat un patró que facilite determinar la causa. Per comprovar si esta deficiència només es presentava a la versió emprada o per si es devia a alguna incompatibilitat del maquinari, hem provat els túnels sobre dos ordinadors diferents (Dell Inspiron amb Ubuntu 12.04 com client d'ftp i Hannspree amb Ubuntu 12.04 servidor de ProFTP v 1.3.4) i les versions usades han estat OpenSSH 5.9 p1 i OpenSSL 1.0.1, també hem sofert els mateixos col·lapses en la transferència. Direm que OpenSSH

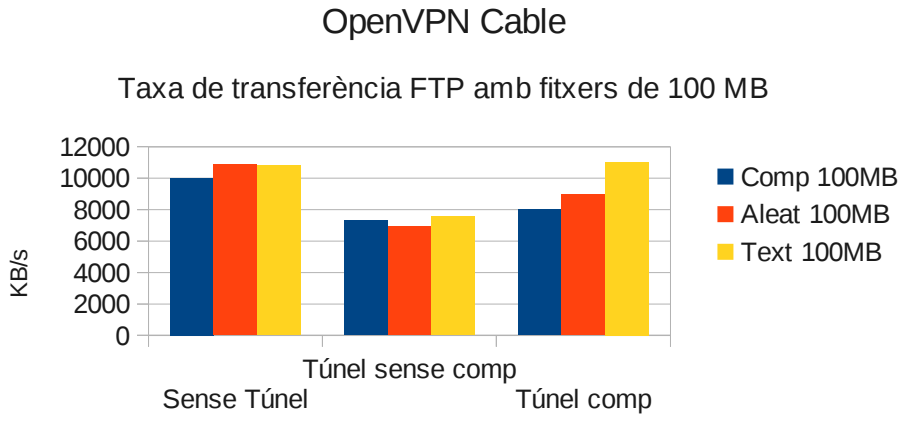
establix les seues connexions sobre TCP, de forma que es creen connexions TCP sobre connexions TCP, a la bibliografia hem trobat diverses referències on es destaca l'inconvenient d'aquesta pràctica, que en certes condicions pot produir una dràstica pèrdua de rendiment, generant un efecte anomenat *meltdown* [Honda], [Titz01], [Karlson-Habib10]. No podem afirmar que siga este el motiu, però el problema resta fiabilitat alhora de seleccionar esta solució

Els resultats obtinguts amb l'ordre top mostren una alta utilització de CPU especialment si apliquem compressió, arribant en el cas de la connexió per a cable fins al 100 % i sense fils al 99 %.
La taula següent mostra els consums màxims dels processos que intervenen en la transferència ftp, proftpd i sshd corresponen al servidor i ftp i ssh a client.

OPENSSH (% consum CPU)						
Procés	**Sense túnel + cable**	**Túnel + cable**	**Sense túnel + wifi**	**Túnel amb wifi**	**Túnel cable sense compressió**	**Túnel wifi sense compressió**
proftpd	23 %	55 %	10 %	42 %	25 %	9 %
sshd	No aplicable	100 %	No aplicable	97 %	82 %	20 %
ftp	19 %	36 %	11 %	33 %	6 %	1 %
ssh	No aplicable	100 %	No aplicable	99 %	19 %	13 %

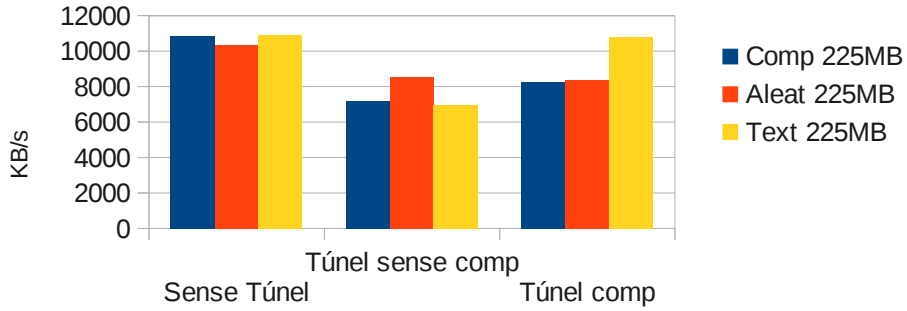
Túnel OpenVPN sobre els ordinadors

S'avaluen les connexions per cable i per punt d'accés sense fils.



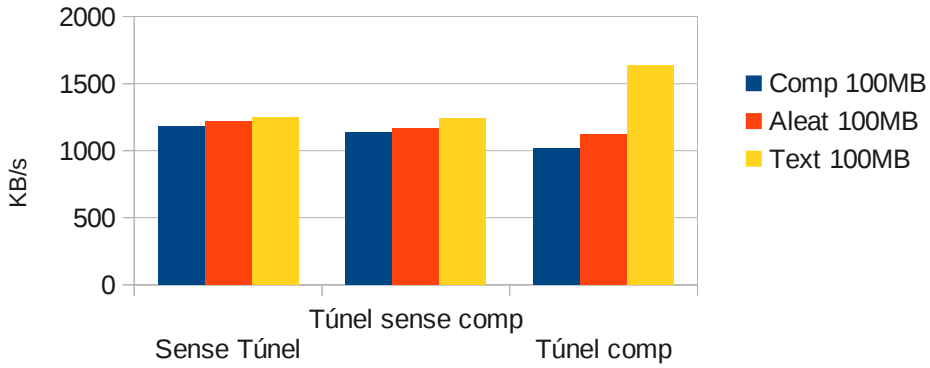
OpenVPN Cable

Taxa de transferència FTP amb fitxers de 225 MB



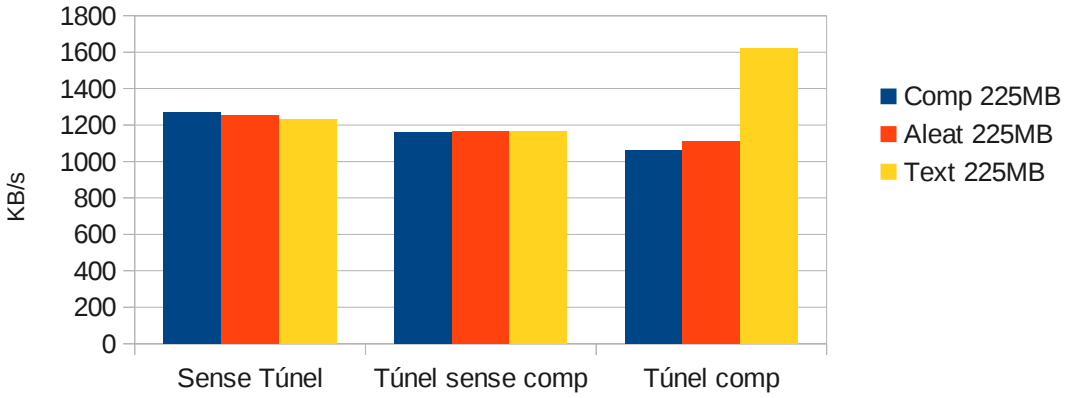
OpenVPN Wifi

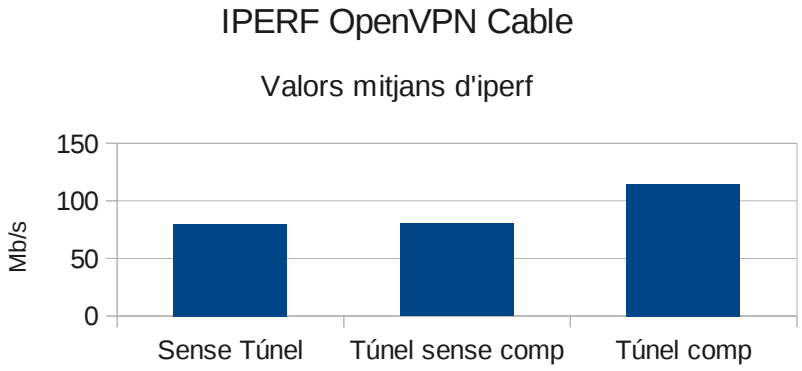
Taxa de transferència FTP amb fitxers de 100 MB

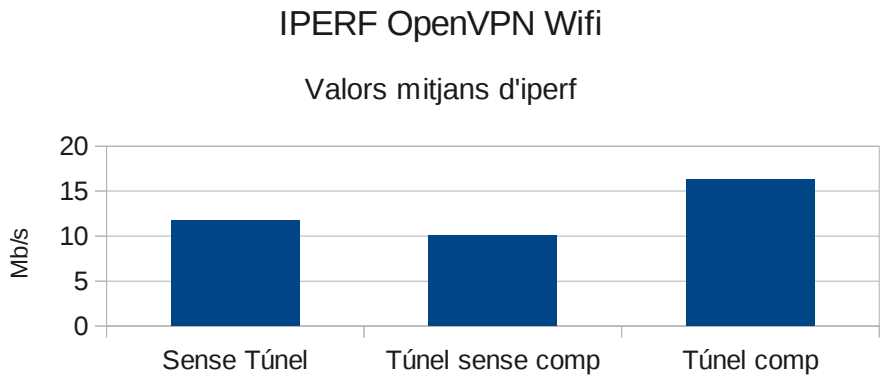


OpenVPN Wifi

Taxa de transferència FTP amb fitxers de 225 MB







Com era d'esperar i a l'igual que els resultats d'OpenSSH es produïx una reducció de la taxa de transferència, que millora amb l'ús de la compressió aplicada als fitxers de text i als resultats d'iperf, encara que no és tan exagerada com al cas anterior.
A diferència d'OpenSSH les proves amb OpenVPN no han sofert cap problema sent en tot moment els seus resultats homogenis. Destacarem que OpenVPN pot establir les seues connexions tant sobre TCP com sobre UDP, sent este últim protocol el seleccionat als fitxers de configuració per a les nostres proves.

Els resultats de l'ordre top han estat alts, especialment amb compressió, però no han arribat a ocupar completament la CPU amb un màxim del 90% tant en la connexió per cable com en la connexió sense fils.

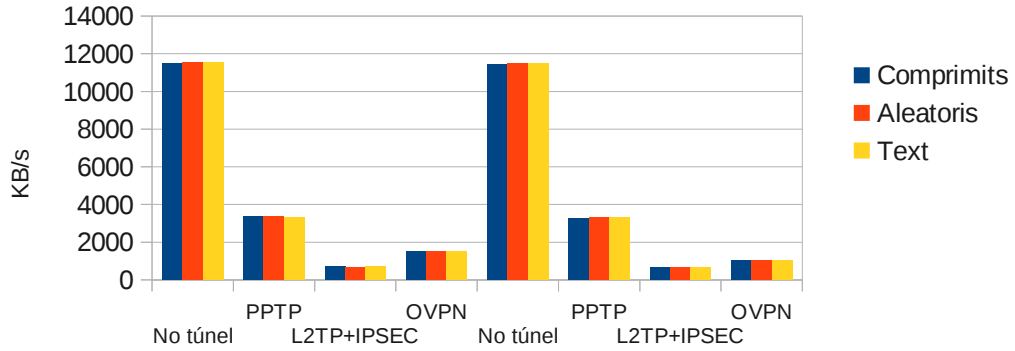
OPENVPN (% consum CPU)						
Procés	Sense túnel + cable	Túnel + cable	Sense túnel + wifi	Túnel amb wifi	Túnel cable sense compressió	Túnel wifi sense compressió
proftpd	23 %	48 %	10 %	5 %	48 %	11 %
openvpn	No aplicable	90 %	No aplicable	12 %	90 %	24 %
ftp	19 %	41 %	11 %	5 %	34 %	7 %
openvpn	No aplicable	90 %	No aplicable	22 %	85 %	23 %

Encaminadors Mikrotik de gama baxia

Els túnels realitzats amb els encaminadors Mikrotik connectats per cable han produït els resultats mostrats a les següents gràfiques:

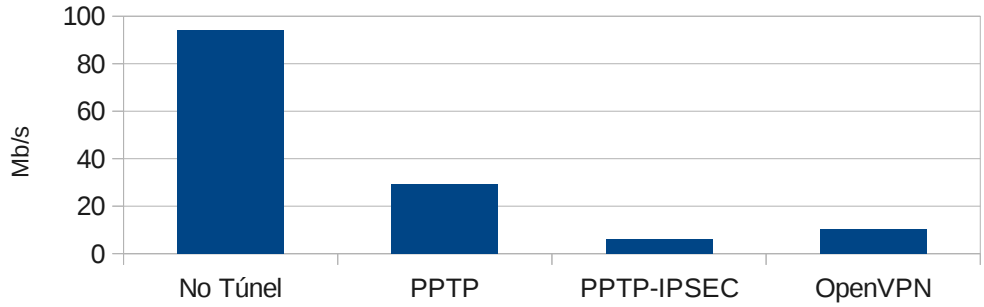
MIKROTIK RB750GL

Put / get de tots els túnels amb fitxers de 100MB (són similars als de 225MB)



IPERF MIKROTIK

Valors mitjans d'Iperf



Es pot comprovar el gran impacte que té l'ús dels túnels, menor per al túnel PPTP ja que usa un mecanisme de xifrat senzill. A més, es veu clarament el paral·lelisme de resultats d'ftp i iperf, la raó és que no aplica compressió que feia millorar els resultats d'iperf als túnels precedents.

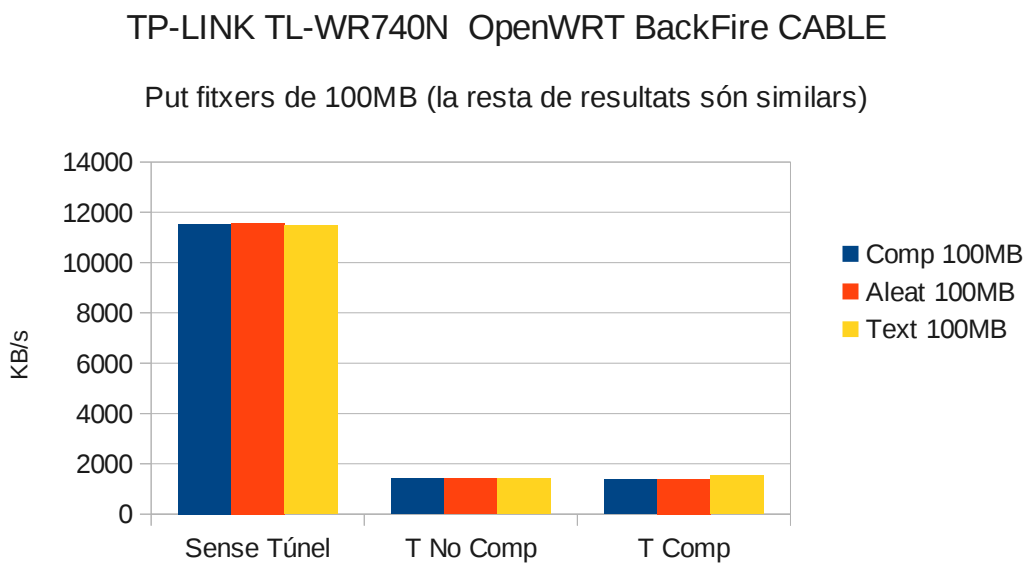
En les proves s'ha vist que quan la transferència s'establix des del costat del servidor del túnel el rendiment és inferior que si es fa des del costat client, esta diferència de rendiment és més accentuada en el cas del túnel OpenVPN on arriba a ser d'un terç inferior. Per a comprovar si el problema es presentava quan el servidor d'ftp estava connectat a l'encaminador servidor del túnel, hem repetit les proves connectant-li el client ftp, i la resposta ha estat la mateixa, per tant, podem dir que estos encaminadors realitzen major esforç al servidor del túnel.

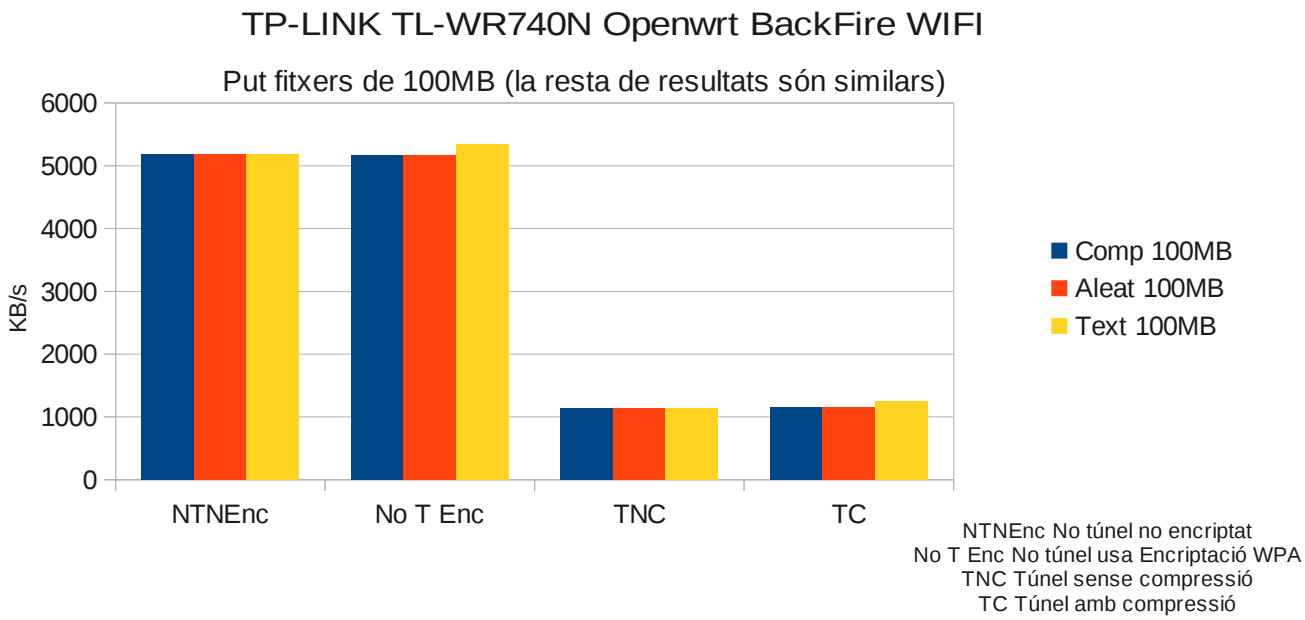
Respecte als túnels, com ja hem dit el PPTP, que oferix millor rendiment no s'aconsella per les vulnerabilitats que presenta, amb L2TP+IPSEC el rendiment és realment pobre i finalment OpenVPN amb una taxa de transferència entre els altres dos té els inconvenients: primer que la transferència es fa sense compressió ja que no està disponible en esta implementació del programari i que com hem vist que certs continguts millora el rendiment, en segon lloc l'asimetria de rendiment entre servidor i client del túnel no resulta desitjable si les operacions entre els extrems del túnel són equivalents i en tercer lloc la transferència la fa sobre TCP ja que no suporta el protocol UDP i com hem recollit de la bibliografia no sembla aconsellable. Per tant, de les tres la millor opció seria OpenVPN, però segons els objectius de l'estudi, la solució dels encaminadors Mikrotik no sembla massa atractiva.

Els resultats de consum de CPU recollits amb /system resource monitor són d'una alta ocupació, 100 % als túnels PPTP i L2TP+IPSEC, mentre que amb OpenVPN varia entre el 71 % i el 98 %.

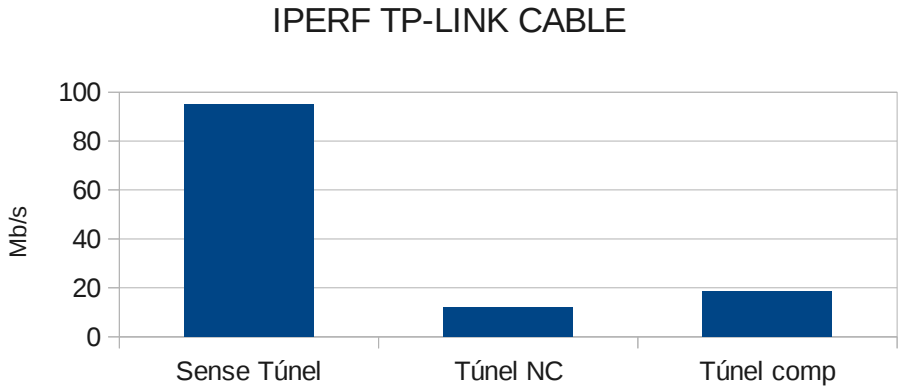
TP-LINK de gama baixa amb OpenWRT

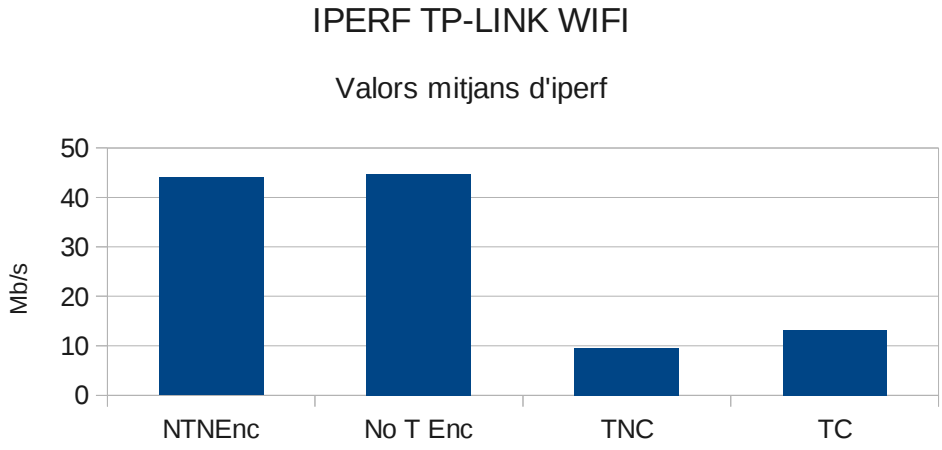
Els encaminadors i punts d'accés sense fils TP-LINK s'han avaluat en transferència per cable i sense fils.





NTNEnc No túnel no encriptat
No T Enc No túnel usa Encriptació WPA
TNC Túnel sense compressió
TC Túnel amb compressió





Els dispositius TP-LINK han permés avaluar els túnels amb connexió per cable i amb connexió sense fils, la qual cosa els dóna avantatge respecte als Mikrotik, a més poden funcionar amb el sistema operatiu OpenWRT que està basat en Linux facilitant a usuaris familiaritzats amb aquest sistema operatiu la seua configuració i adaptació a les necessitats, de fet el túnel provat ha estat OpenVPN, que es pot implantar de manera semblant a la usada amb els ordinadors.
Els resultats de les proves mostren la minva de rendiment esperada, presentant un patró semblant als obtinguts a la resta de sistemes, amb una lleugera millora a la taxa de transferència quan s'usa la compressió, recordem que la versió de OpenVPN sobre Mikrotik no oferia esta possibilitat.
Els túnels PPTP i L2TP+IPSEC no s'han avaluat amb els encaminadors TP-LINK per les raons següents:

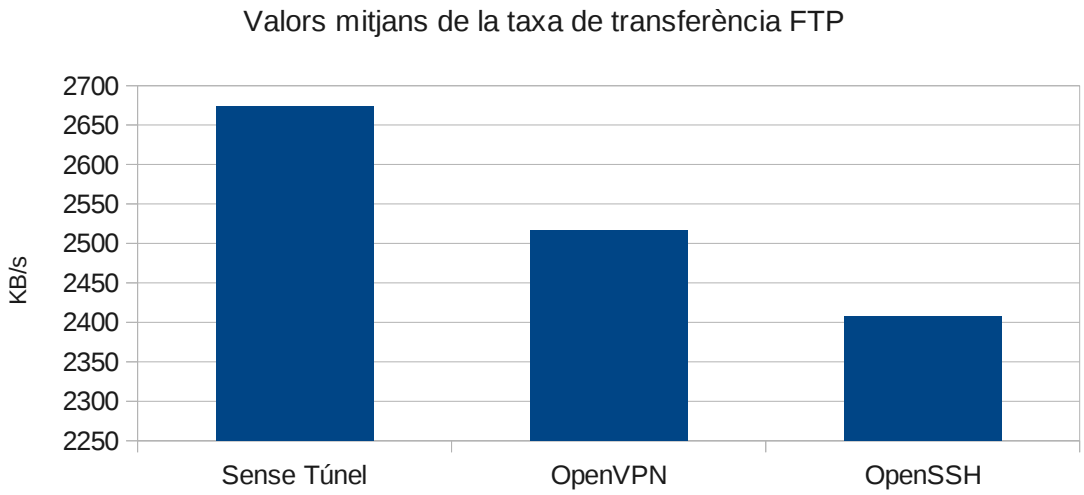
1. Al comprovar que els maquinaris de Mikrotik (CPU AR7161 668MHz i 64 MB de RAM) eren més potents que els de TP-LINK (CPU AR9330 400Mhz i 32 MB de RAM) i obtindre a les proves realitzades sobre OpenVPN uns resultats bastant similars no ens ha semblat que amb els túnels L2TP+IPSEC la diferència fora gaire interessant per als objectius de l'estudi.
2. El túnel PPTP presenta poca fiabilitat com s'ha esmentat abans.

Els resultats de l'ordre top mostren un elevat consum de CPU, voltant de la plena ocupació.

TPLINK OpenVPN (% consum CPU)				
Procés	Tunel cable	Túnel amb wifi	Tunel cable sense compressió	Túnel wifi sense compressió
Openvpn Servidor	98 %	98 %	94 %	97 %
Openvpn Client	98 %	98 %	94 %	98 %

Túnels entre ordinadors mitjançant enllaç sense fils amb antenes Nanostation 2 de Ubiquiti

Les proves amb les antenes Ubiquiti ens han donat uns resultats bastant satisfactoris per a la connexió de nodes mitjançant una xarxa sense fils. Les proves han estat fetes amb els túnels gestionats pels ordinadors i enllaçats a través de les antenes.



No hi ha grans diferències entre els túnels sense compressió, però queda clar que són molt més eficients que el punt d'accés sense fils, però més lentes que el cable. Este tipus d'antena és àmpliament usat a guifi.net, i aquesta prova les confirma com una bona opció.

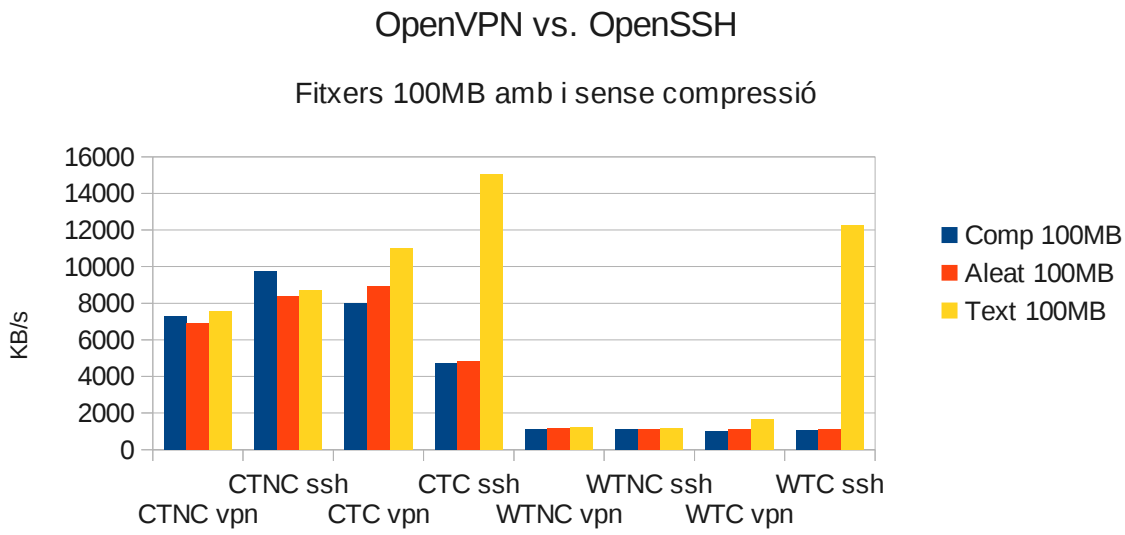
En estes proves no s'ha avaluat el consum de CPU ja que els túnels són gestionats pels ordinadors mentre que les antenes només han estat punt d'enllaç.

ANÀLISI DE RESULTATS

Túnels entre ordinadors. Comparació OpenSSH i OpenVPN

De les proves realitzades als túnels configurats sobre els ordinadors podem destacar que les dos solucions tenen uns resultats semblants, destacant els punts següents:

- La utilització de qualsevol dels túnels, de forma general, produïxen una reducció del rendiment, que per a la connexió per cable cau entre el 20 i el 25%, mentre que si la connexió és sense fils esta reducció queda en un 5 %. Només en el cas d'usar túnels amb compressió sobre els fitxers de text que són molts sensibles a esta operació el rendiment augmenta considerablement, cosa que també es reflexa als resultats de les proves d'iperf, sent realment bons per a OpenSSH, que per cable dobla la velocitat i sense fils la multiplica per sis.
- Si la connexió és per cable i no apliquem compressió, resulta més eficient OpenSSH, en canvi, en general amb l'ús de compressió OpenVPN resultat quasi el doble de ràpid, amb l'excepció de les proves sobre fitxers de text els quals són fàcilment comprimibles i OpenSSH obté uns resultats molt bons.
- Si la connexió és sense fils, tant amb compressió com sense ella OpenVPN és una mica més eficient, menys com s'ha dit abans, quan les proves són sobre fitxers de text, on la compressió d'OpenSSH oferix una velocitat fins a sis vegades superior.
- Cal dir que en algunes de les bateries de proves aplicades sobre OpenSSH, incloses aquelles en que provem les antenes Ubiquiti, ens hem trobat que la transferència pel túnel s'ha col·lapsat després de realitzar diverses operacions put o get, inclús alguna vegada amb les proves d'iperf. El problema fa que la transferència no finalitze (a l'avortar el procés amb Ctrl+c l'execució d'ftp, mostrava que la connexió funcionava a una velocitat ínfima, amb valors entre 17 i 57 KB/s quan hauria de ser de milers de KB/s), obligant a reiniciar els ordinadors per tal de restablir el túnel. La raó d'aquests col·lapses no l'hem pogut determinar ja que no hem trobat un patró que pogués donar-nos alguna pista per a solucionar-ho, però hem citat abans la possibilitat apuntada per diversos articles sobre els problemes que es poden presentar en usar una connexió TCP sobre una altra connexió TCP.
- Podem veure que bàsicament la diferència de rendiment entre OpenSSH i OpenVPN ve donada per la compressió aplicada, més eficient per al primer, però amb un major cost computacional que queda reflectit en el consum de CPU i en la taxa de transferència quan els continguts no faciliten esta característica. Les diferències en l'opció de compressió les trobem en que OpenSSH usa l'algorisme Deflate (el mateix que gzip) mentre que OpenVPN aplica la llibreria LZO i també pot radicar en el nivell de compressió que usa per defecte cada programari.

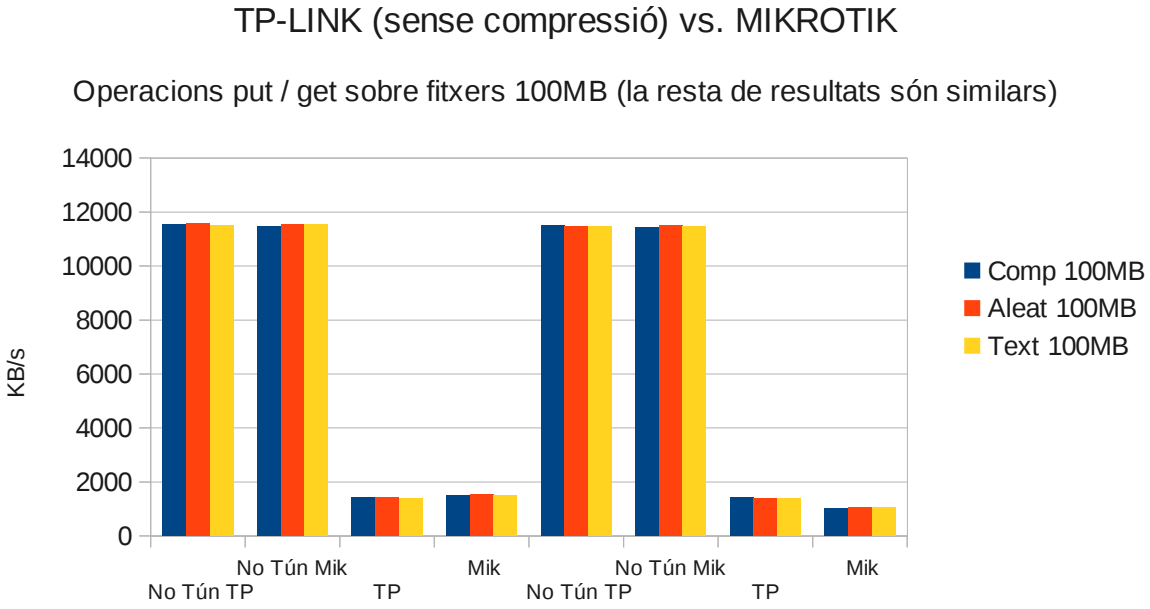


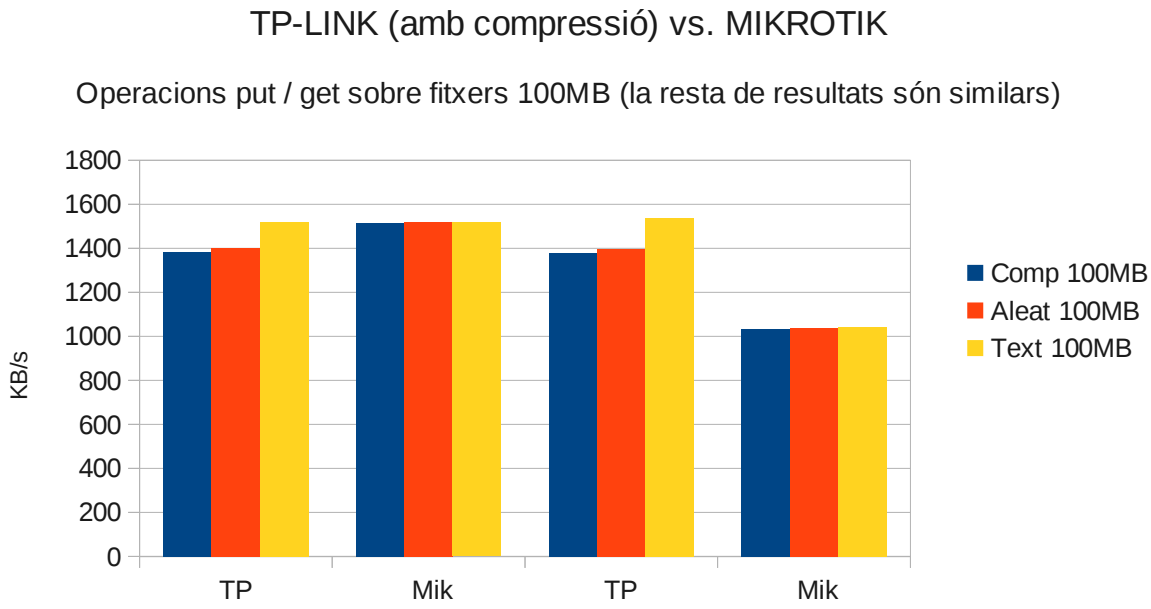
La gràfica compara amb els fitxers de 100MB, però els resultats són equivalents als de 225 MB. Les dos primeres són túnels amb cables sense compressió on es millor OpenSSH, després el mateix però amb compressió on clarament és superior OpenVPN i la resta corresponen a les mateixes proves però amb connexió sense fils.

Comparació Mikrotik front TP-LINK

Els resultats obtinguts amb els encaminadors Mikrotik han estat ben diversos en funció del túnel aplicat. Com en tots els casos, hi ha una caiguda de rendiment, però en aquests és molt major que amb els túnels implementats entre ordinadors, clarament deguda a la diferència de potència de càlcul entre uns maquinaris i altres.
Centrant-nos en els túnels, ens hem trobat una gran diferència entre el túnel PPTP, més del doble de ràpid que el següent en rendiment, l'OpenVPN. I OpenVPN és alhora doble de ràpid que la solució L2TP+IPSEC.
Les diferències de rendiment entre els dos primers les podem trobar en l'algorisme de xifratge, mentre que PPTP usa RC4, que és molt senzill però també vulnerable, OpenVPN pot usar Blowfish128, AES128, AES192 i AES256, més segurs però amb un major cost computacional. Finalment, el pobre rendiment de L2TP+IPSEC esdevé pel seu funcionament, ja que encapsula dos vegades les dades, en primer lloc el paquet de dades original s'encapsula en un paquet L2TP i després el nou paquet és encapsulat dins d'un paquet IPSEC on es xifren les dades mitjançant l'algorisme 3DES, que a pesar de tindre menor cost computacional que RC4 [Donta07], el conjunt d'operacions el fan més lent que els altres dos túnels [REF-L2TP+IPSEC].

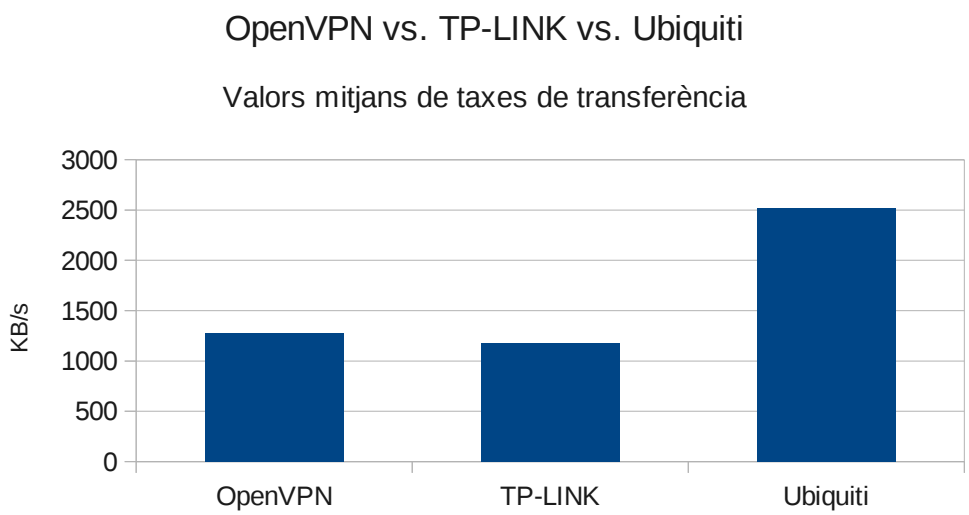
Amb els encaminadors i punt d'accés sense fils TP-LINK només hem avaluat el túnel OpenVPN per les raons detallades anteriorment. Al comparar els seus resultats amb els obtinguts per els Mikrotik, ens trobem que als Mikrotik el rendiment depén de si fan la connexió des del client del túnel o del servidor, recordem que amb ells hem obtingut una resposta asimètrica: si és des del client els Mikrotik resulten una mica més ràpids, mentre que si la connexió és des del servidor llavors els TP-LINK són millors.
De totes formes ja hem comentat que l'asimetria mostrada per els Mikrotik no era desitjable. També destacarem que amb els túnel OpenVPN dels TP-LINK tenim l'opció de compressió i d'usar tant el protocol UDP com TCP, opcions no suportades en els altres. A tot això cal afegir que el preu dels encaminadors TP-LINK és menys de la mitat que els Mikrotik. Quedant clar que la millor opció són els productes de TP-LINK.





Ordinadors amb OpenVPN, TP-LINK i Ubiquiti:

Si comparem els resultats d'OpenVPN entre ordinadors connectats per cable amb els de TP-LINK són quasi huit vegades més lents degut a la diferència en la potència de càlcul entre els maquinaris
Comparant ara els resultats de les proves amb connexió sense fils de les TP-LINK amb els resultats de les proves fetes amb ordinadors connectats per un punt d'accés sense fils amb OpenVPN han estat semblants, per tant ja no depén tant de la potència de càlcul com de la velocitat de la connexió, així que en este escenari podríem usar qualsevol de les dos solucions.
Si comparem els resultats anteriors amb els dels enllaços dels túnels amb ordinadors a través de les antenes Ubiquiti el rendiment obtingut per estes és més del doble de velocitat que l'obtinguda amb els punts d'accés o TP-LINK, per tant és una solució a mitat de camí entre la connexió per cable i els punts d'accés. Passa per tindre un preu més elevat, però obté unes prestacions molt millors.



Consum de CPU:

Pel que fa al consum de CPU els resultats varien en funció de si l'enllaç es fa per cable o per una connexió sense fils [Castro-Evans00], la segona és més lenta necessitant un menor flux de dades disponibles per a transmetre. També influïx si el túnel aplica o no compressió, sent l'opció amb major consum la d'OpenSSH com ja s'ha dit.
La taula següent detalla els consums de CPU en funció del tipus de connexió i si s'aplica compressió, hi apareix la solució amb major consum i el percentatge d'increment enregistrat respecte a l'altra solució:

	Cable	Wifi
Sense compressió	OpenVPN Servidor 8 % Client 65 %	OpenVPN Servidor 4 % Client 10 %
Amb compressió	OpenSSH Servidor 10 % Client 10 % Arriba a ocupar el 100 % de la CPU	OpenSSH Servidor 85 % Client 77 %

El consum de CPU en els encaminadors Mikrotik i TP-LINK és molt elevat arribant a ocupar el 100 % de la CPU, però és un resultat d'esperar sabent l'exigència de càlcul necessària en el procés de xifratge dels túnels i més si s'aplica compressió de dades com en el cas de les TP-LINK.

CONCLUSIONS

Les proves dels sistemes seleccionades en este estudi per a establir túnels segons les necessitats de guifi.net ens duen a les següents conclusions:

- Per a crear túnels entre nodes connectats a través d'una xarxa oberta, o bé per a establir un túnel entre dos xarxes on a cada extrem hi ha un ordinador que treballa com a passarel·la entre la xarxa i el túnel, la millor opció és OpenVPN, els rendiments són similars o superiors a OpenSSH, el consum de CPU és una mica menor, no ha presentat cap inestabilitat i a més, és una solució que trobem a tots els sistemes seleccionats, cosa que per a usuaris que tinguen que treballar amb els diferents sistemes, facilita la tasca a l'haver d'aprendre només un sol tipus de túnel.
- En el cas d'haver d'enllaçar xarxes, per rendiment queda clar que és preferible usar cable entre els ordinadors que establixen el túnel, però si és complicat, llavors la solució passa per usar un enllaç sense fils a través d'antenes Ubiquiti, tant per la distància de cobertura, com per la taxa de transferència sent molt major que si fem l'enllaç amb punts d'accés sense fils.
- Si la necessitat correspon per exemple a una xarxa domèstica que ha d'eixir a la xarxa pública per un túnel, tenim dos possibles solucions, una com el cas del primer punt on un ordinador fa de passarel·la entre la resta de nodes de la xarxa interna i el túnel, on este ordinador estarà connectat a un punt d'accés a través del qual accedix a la xarxa pública, de forma que usem dos elements, l'ordinador i l'element de connexió. L'altra solució seria usar un encaminador TP-LINK amb túnel OpenVPN de forma que siga este element l'únic necessari per a establir la connexió segura. Esta solució seria vàlida per a xarxes amb una càrrega de treball relativament reduïda, degut a les limitacions del maquinari, però presenta una solució molt simple.
- Per a crear túnels per cable sense haver de dedicar ordinadors a aquestes tasques tenim les opcions de crear el túnel entre dos TP-LINK o dos Mikrotik, l'elecció ha estat ben senzilla, TP-LINK. Els rendiments per cable eren similars, oferia l'opció de compressió, configuració com la d'un sistema Linux convencional, és punt d'accés de xarxa sense fils que encara que no es necessite pot donar flexibilitat en el futur i finalment el preu és la mitat que els dels Mikrotik.

Finalment, quedaria pendent per raons de limitació temporal i l'esforç dedicat a proves que finalment han resultat irrellevants per l'estudi, no s'han pogut realitzar proves de túnels implementats als ordinadors mitjançant Xl2tp + OpenSwan, solució basada en L2TP+IPSEC i Poptop + PPTP Client, que implementen túnels basats en el protocol PPTP. A més, pel que fa a maquinari ens ha faltat provar els túnels sobre plaques ALIX de PCEnguines i OpenWRT,. Quedant estes tasques per a treballs posteriors relacionats amb l'avaluació de túnels sobre xarxes obertes.

BIBLIOGRAFIA

Shashank Khanvilkar-Khokhar04: Shashank Khanvilkar and Ashfaq Khokhar, Virtual Private Networks: An Overviewwith Performance Evaluation, 2004
Castro-Evans00: C. Javier Castro Peiia and Joseph Evans, Performance Evaluation of Software Virtual Private Networks (VPN), 2000
Schneier05: Bruce Schneier, Microsoft RC4 Flaw, 2005
Schneier99: Bruce Schneier, Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2), 1999
Honda: Osamu Honda and Hiroyuki Ohsaki and Makoto Imase and Mika Ishizuka and JunichiMurayama, Understanding TCP over TCP: Effects of TCP Tunneling on End-to-End Throughput and Latency ,
Titz01: Olaf Titz, Why TCP over TCP is a bad idea, 2001
Karlson-Habib10: MAGNUS ULLHOLM KARLSSONMD. AHASAN HABIB, SSH over UDP, 2010
Donta07: Praveen Kumar Donta, Performance Analysis of Security Protocols, 2007
REF-L2TP+IPSEC: , http://technet.microsoft.com/es-es/library/cc771298%28v=ws.10%29.aspx,

ANNEX. CONFIGURACIONS

- OpenSSH:
  Configuració del túnel OpenSSH aplicada als ordinadors

```
Al servidor OpenSSH:

# mkdir /root/.ssh

/etc/ssh/sshd_config:

PermitedTunnel yes
PermitedRootLogin without-password

Comprovar que al servidor s'executa sshd.

Al client:

# ssh-keygen -t rsa (No posar res a la passphrase)
# cd .ssh
# scp id_rsa.pub root@192.168.1.1:.ssh/authorized_keys

Si no es posa als scripts d'arranc, per a crear el túnel executar cada vegada:

1 - CLIENT:

# modprobe tun
# ssh -f [-C] -w 0:0 192.168.xxx.yyy -N on: -C per usar compressió i la IP és la de l'ordinador servidor SSHD, pot demanar password de root del servidor.
# ifconfig tun0 10.10.10.2 pointopoint 10.10.10.1 netmask 255.255.255.252 on la primera IP del túnel és del client i la segona la del servidor.

2 - SERVIDOR:

# modprobe tun
# ifconfig tun0 10.10.10.1 pointopoint 10.10.10.2 netmask 255.255.255.252
```

- OpenVPN
  Configuració del túnel OpenVPN aplicada als ordinadors

Les passes estan extretes del document
https://help.ubuntu.com/11.10/serverguide/openvpn.html
Gestió de certificats creats amb "easy-rsa" i guardats als directoris corresponents del servidor i del client.
Per a arrancar els serveis openvpn a través de /etc/init.d/openvpn start al client i al servidor.
Comprovar les rutes per defecte amb ping -R i traceroute per a usar les IP del túnel.

```
################################################
# Sample OpenVPN 2.0 config file for multi-client server.

port 1194
proto udp
dev tun
ca ca.crt
cert 192.168.1.10.crt
key 192.168.1.10.key  # This file should be kept secret
dh dh1024.pem
server 10.10.10.0 255.255.255.0
```

```
ifconfig-pool-persist ipp.txt
keepalive 10 120
;comp-lzo Per a usa compressió llevar el comentari de la línia
persist-key
persist-tun
status openvpn-status.log
verb 3

################################################
# Sample client-side OpenVPN 2.0 config file for connecting to
multi-client server.     #

client
dev tun
proto udp
remote 192.168.1.10 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert 192.168.1.100.crt
key 192.168.1.100.key
ns-cert-type server
;comp-lzo Per a usa compressió llevar el comentari de la línia
verb 3
```

- Mikrotik

  Configuració del túnel per als encaminadors Mikrotik:

```
Configuracions bàsiques routers Mikrotik per a després crear els
túnels entre ells:

Router connectat al servidor ftp:

IP Lan --> 192.168.89.1/24 -- 192.168.89.0 ether2-master-local

Add new 192.168.90.1/24 ether 1-gateway

Afegir la ruta: 192.168.88.0 gw 192.168.90.2 (ip ether 1-gateway
de l'altre router)

Modificar tot el referen al seridor DHCP del router per que les
dades de xarxa i les IP que assigne als clients siguen de la
xarxa 192.168.89.0

Router connectat al client ftp:

Configuració bàsica per defecte: IP Lan --> 192.168.88.1/24

Add new 192.168.90.2/24 ether 1-gateway

Afegir la ruta: 192.168.88.0 gw 192.168.90.2 (ip ether 1-gateway
de l'altre router)

Als dos routers repassar les regles del TALLAFOCS i almenys
eliminar la que hi ha al NAT.

Les configuracions dels túnels segons els documents:

http://www.mikrotik.com/testdocs/ros/2.9/interface/pptp.php
L2TP + IPSEC Mikrotik routers
http://wiki.mikrotik.com/index.php?oldid=20333
OpenVPN Mikrotik  http://wiki.mikrotik.com/index.php?oldid=23366
```

- TP-LINK

  Configuració del túnel OpenVPN aplicada als encaminadors:

```
Als routers TP-LINK - OpenWRT s'ha creat les xarxes següents:
1) Xarxa Lan1 192.168.1.0 que enllaça un ordinador (servidor
FTP) amb el router TP-LINK --> 192.168.3.1 GW 192.168.2.2
2) Xarxa Lan2 192.168.3.0 que enllaça un ordinador (client FTP)
amb l'altre router TP-LINK --> 192.168.1.1 GW 192.168.2.1
3) Una xarxa que enllaça els dos routers primer a través de la
interfície WIFI i després amb la interfície WAN (per a cable):
    TP-LINK1  192.168.1.1  GW 192.168.2.1 LAN i 192.168.2.1  GW
192.168.2.2 wifi / wan
    TP-LINK1  192.168.3.1  GW 192.168.2.2 LAN i 192.168.2.2  GW
192.168.2.1 wifi / wan

Primer s'han fet les proves sense encriptació WIFI. Després
s'ha activar l'encriptació WPA2-PSK xifrat Auto-CCMP
Les proves del túnel s'ha fet amb encriptació activada, ja que
no hi havia diferència de rendiment.

Configuració d'OpenVPN als fitxer del LUCI /etc/config/openvpn
al servidor i al client:

Servidor:
     config openvpn 'lan'
             option enable '1'
             option port '1194'
             option proto 'udp'
             option dev 'tun'
             option ifconfig '10.0.0.1 10.0.0.2'
                 option option keepalive '10 60' (poden haver
canviat  per  que  el  servidor  si  no  treballava  perdia  la
connexió)
              option comp-lzo '1' o '0' (segon s'use compressió
o no respectivament)
             option verb '3'
             option secret '/etc/openvpn/static.key'


Client:
     config openvpn 'client_tun_ptp'
             option enable '1'
             option dev 'tun'
             list ifconfig '10.0.0.2 10.0.0.1'
             option remote '192.168.2.2 1194'
             option nobind '1'
              option comp-lzo '1' o '0' (segon s'use compressió
o no respectivament)
             option verb '3'
             option secret '/etc/openvpn/static.key'

Per a generar la clau (fet al client ftp):

 # openvpn --genkey --secret static.key

Per a copiar la clau:
 $scp root@192.168.3.1:static.key static.key
 Copiar-la a un pendrive
 $scp static.key root@192.168.1.1:static.key

Als dos routers modificar les taules de rutes per a que vaja
per el túnel:
```

```
1) Mirar si hi ha ruta per les IP 2.x en cada router per a
passar cap a l'altre, si és el cas eliminar-les.
2) route del default
3) Al client--> route add default gw 10.0.0.1 tun0
4) Al servidor --> route add default gw 10.0.0.2 tun0

Comprovar des dels ordinadors les rutes amb ping -R i
traceroute. Millor fer primer del client cap al servidor del
túnel.
```

- Ubiquiti
  Les antenes Ubiquiti s'han usat com a enllaç entre els ordinadors per a comprovar el seu rendiment amb connexió sense fils front a una connexió amb cable a una distància superior a la oferida per punts d'accés convencionals, per tant la configuració només correspon a l'enllaç entre elles (una Estació - Bridge i l'altra Punt d'Accés - Bridge).