



Màster Interuniversitari en Seguretat de les TIC
MISTIC

MEMÒRIA

“Oficina segura i mòbil”

Àrea: (M1.724 / M1.824)
Seguretat en sistemes operatius

Alumne: David Álvarez Valero
Director: Carles Estorach Espinós

23-06-2014

A la meva amiga, companya i mare del meu fill, Raquel.

*Aquest treball i tot el que he fet fins ara no hauria
estat possible sense la seva incalculable ajuda.*

Resum

Avui en dia els ginys són a tot arreu i amb aquest projecte s'ha intentat donar a aquests una funcionalitat dins l'empresa petita, com si d'una gran empresa es tractés, però amb un costos a la seva mida, utilitzant tot un programari lliure que hi ha a l'abast i que no per això deixa que el projecte sigui poc professional, tot el contrari, s'ha aconseguit el objectiu; una oficina segura, amb eines com un servidor cau i totalment mòbil, amb eines tan simples com una memòria USB o més complexes, com una xarxa privada virtual que juntament amb el xifratge de les dades, ens permet portar l'oficina casi a qualsevol lloc. Tot això queda ben explicat a la memòria que a continuació s'ha realitzat.

Summary

Today gadgets are everywhere and this project has tried to give such functionality within the small business as if it were a big company, but with a cost to its size, only using free software available that doesn't means the project is unprofessional, all the opposite, the objective has been achieved; a secure office, with a proxy server and fully mobile, with tools as simple as a USB drive or more complex, like a virtual private network with encryption of the data, that allows us to take office almost anywhere. All this is well explained in the report that has been done then.

Índex

Índex d'Il·lustracions	6
Índex de taules	6
1. PROJECTE.....	7
1.1. Descripció del projecte	7
1.2. Justificació del projecte	9
1.3. Motivacions per realitzar el projecte.....	9
1.4. Àmbit d'aplicació del projecte	10
1.5. Objectius del projecte	11
1.6. Desglossament de les tasques	12
1.7. Requisits.....	13
1.8. Planificació.....	14
2. Anàlisi, disseny i instal·lació, oficina central.....	16
2.1. Infraestructura inicial	16
2.1.1. Necessitats.....	16
2.1.2. Situació actual.....	17
2.1.3. Visió global	18
2.2. Configuració oficina central	20
2.2.1. Xarxa	20
2.2.2. Servidor.....	22
2.2.3. Servei cau.....	25
2.2.4. VPN, xarxa virtual i privada	26
2.2.5. Seguretat.....	28
3. Dispositius.....	30
3.1 Anàlisi	30
3.2 Instal·lació i configuració.....	31
3.3 Proves, anàlisi i millores.....	33
4. Manteniment, gestió i revisió.....	34
4.1 Consola d'administració	34
4.2 Selecció d'indicadors i control d'enregistrament	35
4.3 Còpies de seguretat.....	37

5. Formació	38
5.1 Manual d'usuari.....	38
5.2 Classes de formació.....	39
6. Valoració econòmica.....	40
6.1 Maquinari.....	40
6.1 Programari.....	41
7. Conclusions	42
7.1 Èxits	42
7.2 Problemes.....	43
7.3 Millores	43
8. Bibliografia	44
9. Annexes	45
9.1. Annex I. Certificació Zentyal	45
9.2. Annex II. Consola unificada de Zentyal.....	45
9.3. Annex III. Configuració Servei Cau.....	46
9.4. Annex IV. Configuració servei VPN	48
9.5. Annex V. Creació i configuració memòria USB.....	52
9.6 Annex VI. Manual de l'administrador	60
9.7 Annex VII. Manual de l'usuari	64

Índex d'Il·lustracions

Il·lustració 1. Visió global del projecte.....	19
Il·lustració 2. Esquema de xarxa.....	21
Il·lustració 3. Rols d'instal·lació de Zentyal.....	23
Il·lustració 4. Esquema model OSI.....	26
Il·lustració 5. Objectiu final.....	31
Il·lustració 6. Consola d'administració de Zentyal.....	34
Il·lustració 7. Dashboard de control al instant.....	35
Il·lustració 8. Manteniment registres a Zentyal.....	36
Il·lustració 9. Consola de Zentyal Remote.....	37
Il·lustració 10. Aula de formació.....	39
Il·lustració 11. Certificació ZeCa obtinguda al Setembre de 2012.....	45
Il·lustració 12. Consola gràfica d'administració de Zentyal.....	45
Il·lustració 13. Consola configuració ProxyHTTP.....	46
Il·lustració 14. ProxyHTTP regla d'accés.....	47
Il·lustració 15. Perfils de filtrat.....	47
Il·lustració 16. Panel de configuració servidor de OpenVPN de Zentyal.....	48
Il·lustració 17. Panel de configuració client de OpenVPN de Zentyal.....	50
Il·lustració 18. Creació d'un contenidor amb TrueCrypt.....	52
Il·lustració 19. Tipus de volum amb TrueCrypt.....	53
Il·lustració 20. Nom de fitxer del contenidor TrueCrypt.....	53

Índex de taules

Taula 1. Comparativa requisits de l'eina Zentyal.....	17
Taula 2. Configuració de xarxa.....	20
Taula 3. Comparativa de tecnologies possibles VPN.....	27
Taula 4. Llistat de programari i el seu cost.....	41

1. PROJECTE

1.1. Descripció del projecte

Avui en dia els dispositius intel·ligents, com els ultrabooks, els telèfons, les tauletes i també les memòries USB, s'han convertit en un giny que tothom fa servir, a més a més aquests estan arribant a les empreses com a eines amb un alt potencial, degut a la seva facilitat d'ús i les seves prestacions amb unes despeses poc elevades. Si a això afegim les possibilitats de les connexions sense fils a Internet amb tecnologies com; WI-FI, 3G o 4G que tothom té al seu abast, es pot arribar a obtenir una mobilitat de les dades personals o d'empresa sense precedents a més d'un accés a qualsevol tipus d'informació que es trobi a Internet independentment del lloc.

Totes les empreses posseeixen grups de treballadors, que realitzen cerques d'informació a Internet, des de l'ordinador de taula, i aquest conté dades com; programes de facturació i gestió, ofimàtica, etc. A més, s'ha de sumar la possibilitat de dotar de mobilitat a tot el personal, es a dir poder accedir remotament a les dades i eines de l'oficina. Llavors s'enfronten diàriament al perill d'anar a llocs no legítims o dubtosos i que podrien posar a l'abast de algú aquestes dades.

Tot això implica una facilitat a l'hora de desenvolupar la feina diària ja que permet l'accés al sistema des de qualsevol lloc. Tota aquesta mobilitat ha d'anar acompanyada d'una seguretat i en els temps que corren amb un costos assumibles. Per tant l'objecte d'aquest projecte es permetre al personal que desenvolupa feines mitjançant Internet, ho faci de la forma més segura possibles i des de qualsevol dispositiu que tingui connexió, del tipus ja esmentat, i independentment de si es troba fora o de dins l'oficina central.

Aquest escrit tracta de donar les pautes de com dotar al sistema d'una petita empresa, concretament una immobiliària, per protegir els

accessos a Internet i poder realitzar tasques remotes com; accés al programari de gestió i facturació i dades ofimàtiques de la xarxa interna.

Primer de tot es tindrà en compte les eines que ara utilitzen a la oficina. En segon lloc es dotarà al sistema actual d'una protecció d'accés Internet mitjançant un servidor cau a tota la xarxa. A continuació es farà servir una VPN, per protegir les comunicacions entre el sistemes remots i els serveis centrals. I per acabar s'ha de poder establir la connexió segura (Tallafores, IDS, encriptació de les dades) i independentment del proveïdor d'Internet i del dispositiu que s'utilitzi, ja sigui, ordinadors de taula, portàtils, tauletes tàctils o telèfons intel·ligents.

Així doncs, aquest treball es suporta en els conceptes introduïts en diverses matèries del Màster Interuniversitari en Seguretat de les TIC, fonamentalment en les assignatures: Seguretat en Sistemes Operatius i Seguretat de Xarxes, més de la certificació "ZeCA (Zentyal Certified Associate, veure annex I)", que acredita la capacitat en l'ús, configuració, instal·lació i manteniment de "Zentyal Linux Small Business Server" i de les seves eines associades, columna vertebral d'aquest projecte.

1.2. Justificació del projecte

Actualment els comercials desenvolupen tasques de recerca d'immobles on utilitzen Internet, xarxa d'àmbit públic i s'ha d'utilitzar amb compte. Per tant per protegir aquest ús s'implantarà un servidor cau.

A més d'Internet es realitzen tasques al carrer per captar nous immobles i per tant, donar d'alta nous clients. Actualment s'utilitza una fitxa de paper per omplir les dades i en molts del casos, tenen temps de traspàs al sistema llargs. Unes de les principals causes que provoquen aquests retards, són els desplaçaments físics a la oficina central per omplir la fitxa al programari de gestió. Si cada comercial tingués la possibilitat de desenvolupar la seva feina d'oficina, independentment del lloc, i només tenint com a requisit una connexió a internet, donaria com a resultat, una major celeritat a tot el procés i, com a conseqüència un servei més eficaç.

Llavors aquest projecte cerca la forma de millorar la seguretat i la mobilitat.

1.3. Motivacions per realitzar el projecte.

La major motivació per realitzar aquest TFM és configurar tot el sistema amb una eina que englobi tot, en una única consola i amb el mínim de recursos econòmics, ja que parlem d'una PIME i l'actual situació econòmica també ho requereix, aquesta eina és Zentyal.

Zentyal Technologies, és una empresa espanyola amb projecció internacional, que es dedica al desplegament de servidors Linux a les PIMEs. El seu producte estrella és la seva distribució GNU/Linux "Zentyal Linux Small Business Server". La distribució integra 30 eines de programari lliure de gestió de sistemes i xarxes.

El principal objectiu de Zentyal és reduir despeses de TI a empreses, principalment PIMEs, que compten amb un pressupost més ajustat.

Zentyal proporciona a totes aquestes organitzacions la gestió d'usuaris, infraestructura de xarxa, correu electrònic i altres serveis d'una manera senzilla, segura i a un preu (gratuït) imbatible.

Així doncs, tot fa que sigui molt atractiu, i, arrel d'això, al setembre de 2012 vaig obtenir la certificació ZeCA (Zentyal Certified Associate) que acredita la capacitat en l'ús, configuració, instal·lació i manteniment de Zentyal Linux Small Business Server i de les seves eines associades.

Finalment vaig decidir realitzar el meu projecte final de màster basat en la experiència durant el darrer any, on he realitzat proves del producte i totes les seves eines.

1.4. Àmbit d'aplicació del projecte

El projecte està basat, en la major part, en Zentyal i aquest integra una gran varietat d'eines (servidor cau, tallafoç, VPN, OpenSSL, integració amb AD, Monitorització dels serveis, etc.) que ens permet implementar-lo a molts àmbits. Com són la gestió d'usuaris que podran fer servir el sistema, la protecció de la xarxa, la gestió i servei de VPN, com a passarel·la entre Internet i la xarxa interna, així com també la monitorització de les connexions al sistema.

1.5. Objectius del projecte

Els principals objectius del projecte són:

- Instal·lar un servidor que permeti la configuració de l'eina Zentyal que donarà els serveis necessaris; servidor cau, per al control d'accés a Internet. VPN, per la connexió remota a la oficines central. I seguretat, Talla foc, IDS i Monitorització. S'haurà de aprofitar al màxim la infraestructura actual i estudiar quin sistema i protocol són més adients.
- Instal·lar i configurar els dispositius per realitzar les tasques remotes mitjançant la VPN. S'haurà de seleccionar l'eina més adient i portable. En aquest cas s'ha pensat en una unitat USB amb tot el programari necessari i en versions futures una tauleta tàctil configurada amb una connexió VPN.
- Realitzar proves de camp, per poder determinar i millorar tota la configuració feta per passar a la configuració definitiva.
- Formar als comercials per realitzar les tasques remotament, que actualment es fan a l'oficina central.
- Desenvolupar un sistema de manteniment i gestió de tots els serveis per controlar la seguretat.

1.6. Desglossament de les tasques

Les principals tasques del projecte són:

- Anàlisi de les necessitats dels comercials. S'han de conèixer quines aplicacions i dades de la oficina central són adients i indispensables tenir accés.
- Selecció de maquinari i programari per donar suport a les necessitats. La immobiliària actualment té una xarxa amb un servidor de domini AD de Microsoft i un servidor en proves, d'escriptori remot amb Ulteo.
- Instal·lació i configuració del servidor amb Zentyal. En aquest punt i donat que Zentyal integra diferents tecnologies VPN, és farà la configuració del sistema de connexió VPN més adient.
- Instal·lació i configuració dels dispositius remots, memòria USB encriptada o tauleta tàctil.
- Proves de camp per trobar mancances i intentar millorar el sistema. Amb els resultats s'han de configurar el dispositius definitivament i generar la documentació per la formació.
- Manteniment, gestió i revisió del sistema.
- Formació dels comercials i administrador del sistema. Es realitzarà formació a grups reduïts sobre l'ús del sistema, i se'ls dotarà amb un manual d'usuari.

1.7. Requisits

El requisits per poder arribar als objectius plantejats són:

- Un servidor on instal·lar l'eina de Zentyal. Com s'ha explicat aquesta es basa en Ubuntu LTS (actualment ZENTYAL 3.4 està suportada per Ubuntu Server 12.04 LTS). Això determinarà els mínims per aquesta màquina i, per estalviar, s'estudia elegir un ordinador que actualment ha deixat de tenir cap funció.
- Estudi de la Integració del servei cau amb el actual domini per realitzar un control més exhaustiu de l'accés a Internet.
- Una connexió d'alta velocitat, que actualment la immobiliària ja disposa. Es tracta d'una connexió de fibra del tipus 100Mb/10Mb amb adreça pública fixa. Aquest és un punt imprescindible, ja que els dispositius remots hauran de connectar-se a una adreça d'aquest tipus i la qualitat d'ample de banda és important.
- Per altra banda s'ha de posar en funcionament el servei de VPN. Per dur-ho a terme primer s'han d'estudiar les possibles tecnologies, PPTP, IPSEC I OpenVPN .
- Una vegada elegida la tecnologia, s'haurà d'elegir el programari més adient per portar a la memòria USB. Configurar aquest de tal forma que sigui segur i estable i es pugui connectar amb equips equipats de connexions a Internet.

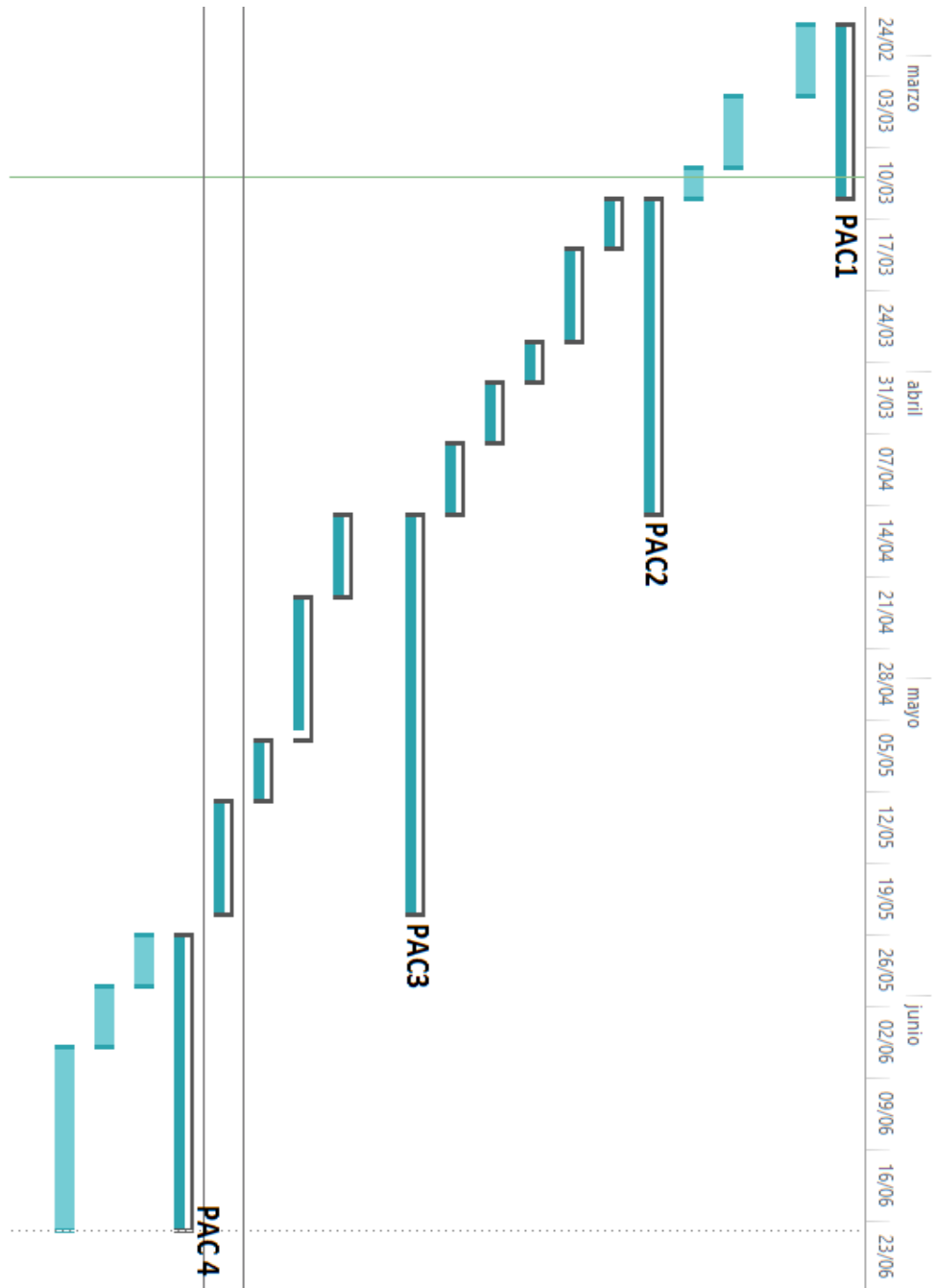
1.8. Planificació

Arribats a aquest punt podem exposar la planificació del projecte

Tasca	Duració	Inici	Fi
PAC1. Proposta Projecte	13 días	mié 26/02/14	vie 14/03/14
Descripció, Justificació, Motivació i Àmbits	5 días	mié 26/02/14	mar 04/03/14
Objectius, tasques, requisits	5 días	mié 05/03/14	mar 11/03/14
Planificació	3 días	mié 12/03/14	vie 14/03/14
PAC2. Anàlisi, Disseny i Instal·lació	22 días	sáb 15/03/14	lun 14/04/14
Necessitats i Infraestructura inicial	4 días	sáb 15/03/14	mié 19/03/14
Preparació reunió amb comercials i gerent	1 día	sáb 15/03/14	sáb 15/03/14
Reunió amb els comercials i gerent	1 día	lun 17/03/14	lun 17/03/14
anàlisi situació actual maquinari oficina	1 día	mar 18/03/14	mar 18/03/14
Revisió xarxa interna	1 día	mié 19/03/14	mié 19/03/14
Servidor	7 días	jue 20/03/14	vie 28/03/14
Selecció maquinari i de sistema operatiu	1 día	jue 20/03/14	jue 20/03/14
Instal·lació Ubuntu Server Zentyal Small Bussiness	6 días	sáb 22/03/14	vie 28/03/14
Servei cau	3 días	sáb 29/03/14	mar 01/04/14
Anàlisi i definició	1 día	sáb 29/03/14	sáb 29/03/14
Instal·lació servei	2 días	lun 31/03/14	mar 01/04/14
VPN	4 días	mié 02/04/14	lun 07/04/14
Anàlisi del protocols VPN	1 día	mié 02/04/14	mié 02/04/14
Instal·lació VPN	3 días	jue 03/04/14	lun 07/04/14
Seguretat	5 días	mar 08/04/14	lun 14/04/14
Anàlisi d'eines necessàries	1 día	mar 08/04/14	mar 08/04/14
Configuració Tallafoç , IDS, Monitorització	4 días	mié 09/04/14	lun 14/04/14
PAC3. Dispositius, proves, anàlisi i millores. Manteniment	29 días	mar 15/04/14	vie 23/05/14
Dispositius	6 días	mar 15/04/14	mar 22/04/14
Anàlisi i selecció	2 días	mar 15/04/14	mié 16/04/14
Instal·lació i configuració	4 días	jue 17/04/14	mar 22/04/14
Proves, anàlisi i millores	10 días	mié 23/04/14	mar 06/05/14
Proves des dispositius configurats, crear un manual usuari inicial	6 días	mié 23/04/14	mié 30/04/14
Anàlisi de les proves realitzades	2 días	mié 30/04/14	jue 01/05/14
Millores segon el resultat del anàlisi	2 días	vie 02/05/14	lun 05/05/14
Manteniment, gestió i revisió	4 días	mié 07/05/14	lun 12/05/14
Selecció d'indicadors i com es controlen	2 días	mié 07/05/14	jue 08/05/14
Activació de esdeveniment i registres de control	2 días	vie 09/05/14	lun 12/05/14
Formació	9 días	mar 13/05/14	vie 23/05/14
Creació de manual d'usuari	2 días	mar 13/05/14	mié 14/05/14
Creació de manual d'administració	3 días	jue 15/05/14	lun 19/05/14
Classes de formació	4 días	mar 20/05/14	vie 23/05/14

PAC4. Entrega Memòria i presentació.	21 días	lun 26/05/14	lun 23/06/14
Valoració econòmica	5 días	lun 26/05/14	vie 30/05/14
Conclusions: Èxits, problemes i millores	5 días	sáb 31/05/14	jue 05/06/14
Presentació: Elaboració de la presentació final	12 días	vie 06/06/14	lun 23/06/14

I amb un diagrama de Gantt es té una temporització més visual.



2. Anàlisi, disseny i instal·lació, oficina central

2.1. *Infraestructura inicial*

S'ha realitzat un anàlisi de les necessitats i de les eines que disposa la immobiliària per cobrir-les. A continuació es descriu tot el procés.

2.1.1. **Necessitats**

Per arribar als objectius assenyalats s'han de conèixer les necessitats dels usuaris i per tant s'ha realitzat una reunió amb el gerent i els comercials, i s'ha creat un equip de dos comercials, d'un total de catorze. De la reunió s'han obtinguts les necessitats que han de cobrir-se amb l'oficina segura i mòbil:

- Totes les consultes a Internet han de ser controlades: Es necessari un servidor cau que doni pas a Internet integrat amb el AD actual.
- Tractament de dades ofimàtiques: Textos, fulls de càlcul i PDF, consulta de document ubicats al servidor de forma remota.
- Accés al programari de gestió de la immobiliària: Gestió completa del programari independentment del lloc o del dispositiu.
- Enviament de dades al servidor central: Si es genera documentació nova al dispositiu remot (fotos, documents), que es puguin enviar fàcilment.
- Seguretat: totes les comunicacions així com l'accés al sistema remot han de ser el més segur possibles.

Una vegada definides les necessitats dels usuaris, és necessari analitzar la situació actual del sistema i quina serà la configuració més adient, que les cobrirà totes.

2.1.2. Situació actual

En l'actualitat l'economia marca el nivell d'inversió en TIC, i més encara si parlem de PIMES, aleshores unes de les premisses del projecte és que el costos s'han de minimitzar al màxim. Això és un punt determinant per a elegir el maquinari i el programari que s'ha d'utilitzar sense que això signifiqui una manca de serveis. Com s'ha introduït, tot el projecte es centra en l'eina Zentyal a continuació es mostres els seus requisits segons el tipus de perfils (veure al punt 2.2.2 els diferents perfils):

Taula 1. Comparativa requisits de l'eina Zentyal.

PERFIL DE ZENTYAL	USUARIOS	CPU	MEMORIA	DISCO	TARJETAS DE RED
Puerta de acceso	<50	P4 o superior	2G	80G	2 ó más
	50 ó más	Xeon Dual core o superior	4G	160G	2 ó más
Infraestructura	<50	P4 o superior	1G	80G	1
	50 ó más	P4 o superior	2G	160G	1
Oficina	<50	P4 o superior	1G	250G	1
	50 ó más	Xeon Dual core o superior	2G	500G	1
Comunicaciones	<100	Xeon Dual core o equivalente	4G	250G	1
	100 ó más	Xeon Dual core o equivalente	8G	500G	1

Per tant, s'han cercat les eines necessàries per cobrir els requisits establerts tant de maquinari, com de programari. L'empresa disposa de:

- Una màquina amb un Intel Core i3, 8Gb, un disc dur SATA de 250GB i 2 targetes de xarxa.
- Una xarxa interna amb un domini AD de Microsoft.
- Una connexió de fibra 100/10MB instal·lada amb un encaminador de Movistar independent de la xarxa interna.
- Un servidor d'aplicacions en terminal (Ulteo Open Virtual Desktop).
- Un servidor de fitxers i programari de gestió immobiliària.
- Deu portàtils amb connexió 3G.
- Catorze unitats de memòria USB.

2.1.3. Visió global

Tal com s'ha vist, tenim les necessitats definides i quina es la situació que té l'empresa per desenvolupar el sistema. A continuació es descriu una visió global del funcionament al qual es vol arribar.

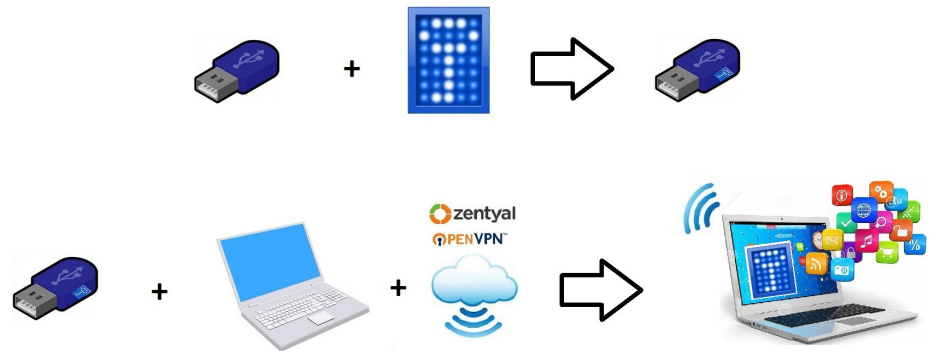
Tot el personal de l'empresa ha de realitzar les seves tasques de consulta a Internet de forma segura i controlada. Tots els equips tenen antivirus, però la millor manera de controlar els possibles intrusos provinents d'Internet, és controlar on es navega. Llavors el primer pas és integrar un servidor cau al domini existent que controli tota les peticions d'accés a Internet des de qualsevol ordinador de l'empresa.

Pel que fa a les comunicacions externes tot comercial ha de tenir un dispositiu de connexió (memòria USB amb programari) i un certificat digital que s'ha de introduir dins el client VPN que durà al dispositiu. Això permetrà al client VPN establir la connexió amb el servidor de l'oficina central d'una forma segura, encriptant les dades.

Una vegada connectat es podran utilitzar tots els serveis de l'oficina central com si es tractés d'un ordinador més d'aquesta, utilitzant una eina especialment dissenyada amb tot el necessari, paquet ofimàtic, programari de gestió d'empresa i explorador de fitxers.

Per acabar i afegir un nivell més de seguretat, tots el dispositius de memòria USB aniran encriptats amb una contrasenya per evitar, que en cas de pèrdua, es deixi un dispositiu l'abast de persones no autoritzades. A més d'això es configurarà un servei tallafoc per controlar els accessos externs i interns i la monitorització de tot el sistema amb un servei de registres tot controlat d'igual forma amb l'eina Zentyal.

En principi aquesta és la visió global de com ha de funcionar el sistema d'oficina segura i mòbil.



Il·lustració 1. Visió global del projecte

A continuació es descriu com s'ha arribat a aquesta solució, des de la configuració de la oficina central fins a la configuració de les memòries USB que contindran tot el necessari per connectar amb els portàtils amb 3G de forma segura i controlada.

2.2. Configuració oficina central

Una vegada definides les necessitats, descrits els recursos i vista la visió global, s'ha procedit a definir la configuració del sistema que s'ha instal·lat a l'oficina central.

2.2.1. Xarxa

La configuració de xarxa existent i la configuració que s'ha utilitzat per donar accés remot als serveis de l'empresa ha estat com segueix:

Taula 2. Configuració de xarxa

Xarxa interna	192.168.0.0/24
Xarxa perimetral	192.168.1.0/24
Xarxa VPN	192.168.170.0/24
Adreça IP pública	Ip fixa del proveïdor ISP

El perquè d'aquesta configuració es presenta a continuació.

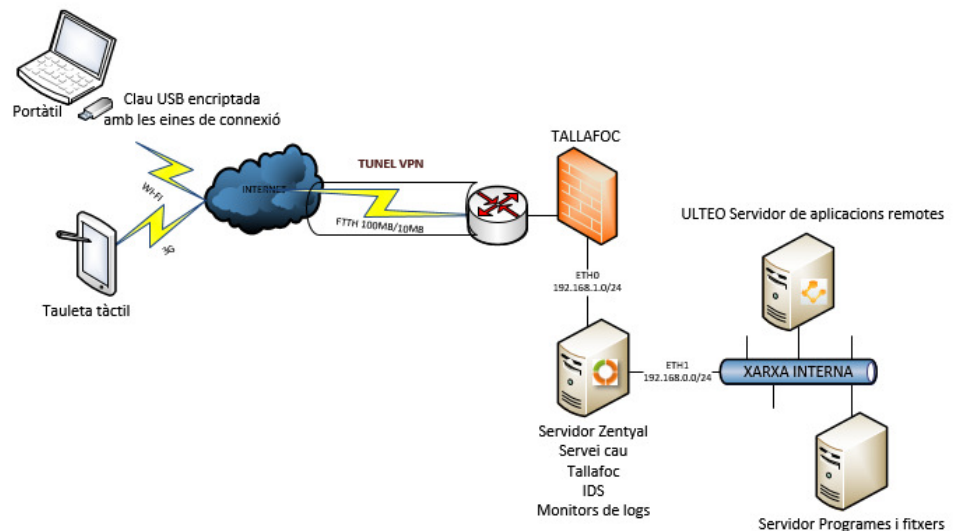
La xarxa interna, ja existent, conté els equips dels usuaris de la oficina central (domini AD), així com els servidors descrits anteriorment; el servidor de fitxers, de programari i el servidor d'escriptori remot.

La xarxa perimetral es crea com a resultat d'una configuració més segura, on anirà el tallafoc. Això s'ha realitzat així perquè sempre que es vulgui exposar un servei intern a una xarxa externa i conflictiva, en aquest cas Internet, s'ha d'evitar exposar la xarxa interna directament a l'externa per això es configura una xarxa intermèdia on s'instal·len els serveis que comuniquen la xarxa interior amb l'exterior, en aquest cas el servei de VPN.

La xarxa VPN és necessària per establir les connexions entre els dispositius externs i els serveis ubicats a la xarxa interna d'una forma segura. Amb aquesta xarxa es crea un túnel de connexió encriptat amb un certificat digital (s'ha decidit utilitzar OpenVPN) que permet enviar i rebre dades de l'oficina central d'una forma segura, fent servir una xarxa pública, com és Internet, però amb unes adreces que es comporten com internes. Cada equip que es connecta rep una adreça per DHCP que li proveeix el servidor amb Zentyal.

Per acabar, i com és lògic es necessari tenir una adreça pública per poder realitzar la connexió inicial al servei de VPN, ja esmentat, que vindrà donada per el proveïdor d'Internet. Dins el encaminador s'ha creat una regla DMZ que apunta a l'adreça IP perimetral del servidor Zentyal (aquest té dos targetes de xarxa). Aquesta serà l'única porta d'entrada des de l'exterior cap a tots els serveis de l'empresa.

Aquesta configuració es resumeix millor en l'esquema de xarxa següent:



Il·lustració 2. Esquema de xarxa

2.2.2. Servidor

Una vegada definida la configuració de xarxa s'ha passat a configurar el servidor, les característiques d'aquest servidor són:

- 1 processadors Intel Core i3
- 8Gb de RAM.
- 250GB de disc dur SATA.
- 2 targetes Gigabyte Ethernet.

Tal com s'ha introduït, el servidor realitza; de servei cau, de servei VPN, ha de permetre la connexió remota a les oficines centrals, i tot amb seguretat, tallafoc i monitorització. Aquest servidor és la porta d'entrada i sortida i com a tal, necessita un programari especialment dissenyat, que amb aquestes característiques de hardware, en tingui suficient. Hi ha dos possibles solucions accessibles, un servidor amb Windows Server 2012 o un servidor amb Linux.

Microsoft és un del sistemes operatius propietari més utilitzats al món, per tant molt consolidat. I pel que fa a la seva darrera versió, per a servidors, és més segura i estable que les anteriors, a més de tenir unes eines visuals que faciliten la seva administració i desplegament ràpidament. En canvi el seu cost és elevat per al projecte, ja que es necessita una llicència per servidor físic, a més de llicències de client (CAL), que per defecte no són suficients, ja que hi ha un total de vint-i-cinc usuaris a l'empresa. Amb la versió més econòmica, l'estàndard, necessitarien la compra de llicències extres, per tant queda descartat com a solució, principalment pel cost elevat.

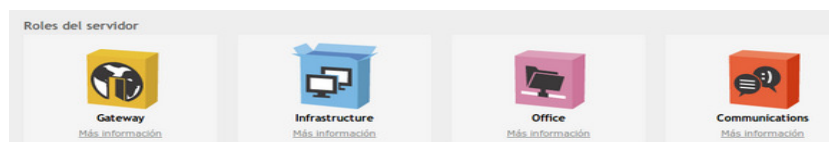
Com alternativa tenim Linux, un sistema operatiu OpenSource, per tant, en principi, no afegix un cost econòmic al projecte, però al contrari que el sistema operatiu de Microsoft, sempre ha estat un sistema més

difícil de administrar per la seva falta de una consola que centralitzi tot i que a més sigui gràfica, llavors implica un desplegament i integració més costosos, perquè requereix una major especialització.

Però això ha estat fins ara, amb l'aparició de l'eina Linux Zentyal Small Business Server que integra tot dins una única consola i d'una forma gràfica, permetent que el desplegament d'un servidor Linux amb tots els seus serveis (fins una trentena) sigui tant fàcil o més que amb Microsoft Windows. Llavors aquest serà el sistema elegit per al servidor, d'entrada gratuït, fàcilment desplegable i administrable.

Zentyal es divideix en quatre perfils, cada un d'ells amb el seu respectius serveis, i tot es configura amb una única consola per pàgina web. Aquest són cada un d'ells:

- Zentyal Gateway: Actua com a porta d'enllaç de la xarxa interna, oferint una connexió segura a Internet.
- Zentyal Infrastructure : Gestiona la infraestructura de la xarxa local amb els serveis bàsics: DHCP, DNS, NTP, servidor HTTP, A.C, VPN etc.
- Zentyal Office: Actua com servidor de recursos compartits, dominis i directori d'usuaris de la xarxa local: fitxers, impressores, calendari, contactes, perfils d'usuari i grups, etc.
- Zentyal Unified Communications: Es converteix en el centre de comunicacions de l'empresa, incloent correu, missatgeria instantània i plataformes de treball en grup.



Il·lustració 3. Rols d'instal·lació de Zentyal

Dels quatre perfils s'han elegit; Infraestructure i Gateway, perquè integren totes les eines necessàries per a configurar els serveis que es necessiten al servidor:

- HTTP PROXY(Cache and Filter): Per configurar i controlar tot l'accés a Internet des de els equips de la xarxa.
- DHCP: Per configurar les assignacions de adreces IP al clients de la xarxa VPN
- A.C. (Autoritat Certificadora): Per assignar els certificats utilitzats a cada dispositiu i així encriptar el túnel VPN amb el servidor.
- VPN: Per crear la xarxa VPN amb el dispositius externs.
- FIREWALL: Per controlar les connexions a les diferents xarxes.
- IDS/IPS: Per detectar possibles atacs o intents d'aquests, al servidor.
- Monitorització: Per auditar totes les connexions al servidor i el control de fallada d'algun servei.
- BACKUP: Per realitzar còpies de la configuració del sistema.

Una vegada instal·lats tots els serveis aquests es configuren amb una única consola, com ja s'ha indicat (*veure annex II*). A continuació s'han configurat cada un dels serveis instal·lats per obtenir com a resultat un accés a les consultes d'Internet més segura i una passarel·la de connexió entre els serveis centrals i els dispositius externs de forma segura fent servir una VPN i així arribar als objectius del projecte.

De tots aquests serveis ens centrarem al més importants que són el servei cau (HTTP PROXY), el de xarxa virtual privada (VPN) i aquells relacionats amb la seguretat de tot el sistema (FIREWALL, IDS/IPS, Monitorització i BACKUP).

2.2.3. Servei cau

El servei cau ofereix millorar la experiència de navegació, utilitzant una memòria cau i la possibilitat de controlar tots els accessos a Internet. Es pot restringir més o menys, segons es consideri des de, usuari per usuari, fins a un conjunt d'equips. I el tipus de control va, des de els continguts o la classificació de llocs que es permet, fins només deixar anar-hi a llocs en concret.

Dins els serveis que Zentyal integra hi ha HTTP-PROXY , un servei cau format per les eines “Squid” i “Dansguardian”, la primera té la funció de servidor cau i la segona control de continguts, entre totes dues es pot configurar tot el necessari per al nostre objectiu i com sempre des de la mateix consola (veure annex III).

El primer pas que s'ha realitzat per poder arribar a integrar el servidor cau amb el domini actual és modificar una política al AD¹ del domini per que a tots els equip tinguin al seu navegador configurat amb el servei cau, s'ha integrat el servidor cau amb el domini, de forma que si no és un usuari de domini no es pot navegar per Internet, utilitzant la propietat de “single sign-on”, descrita la l'annex III i que permet validar al usuari del domini davant el servei cau.

Arribats aquí s'ha definit que tots els usuaris de l'empresa navegaran només a les pàgines web que el gerent determini com a necessàries i les altres estaran prohibides. El control es durà a terme mitjançant l'eina de control que integra Zentyal i que es pot veure a l'annex III.

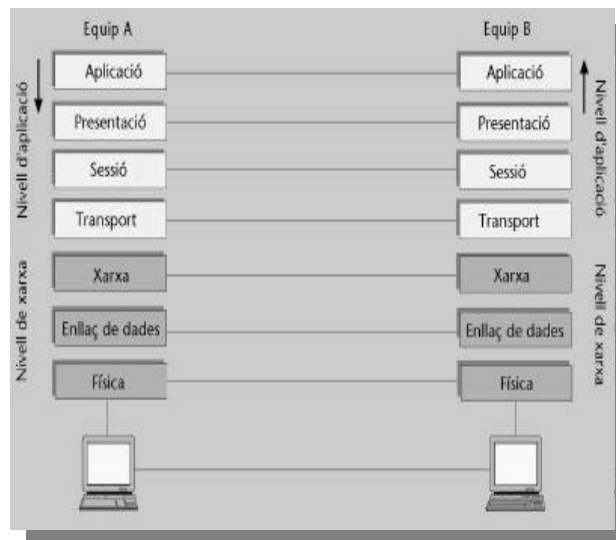
Amb tot s'ha arribat al primer objectiu i part d'altre, una navegació controlada i més segura. A continuació estudiarem com obtenir l'accés remot a les dades i de forma segura.

¹ Active Directory

2.2.4. VPN, xarxa virtual i privada

Cóm es pot utilitzar una xarxa pública com si d'una privada es tractés? . La resposta a aquesta pregunta és VPN, una xarxa privada perquè protegeix les dades d'usuaris no autoritzats mitjançant la criptografia i virtual perquè es comporta com si d'una LAN es tractés però utilitzant programari específic damunt una xarxa pública com és Internet.

Les VPN's que es poden trobar, s'implementen a diferents nivells del model OSI.



Il·lustració 4. Esquema model OSI

I dins totes les possibles opcions, OpenVPN és una excel·lent nova solució per a VPN que implementa connexions de capa 2 o 3, usa els estàndards de la indústria SSL/TLS per xifrar i combina totes les característiques de tecnologies anteriors com PPTP, L2TP o IPSec. A continuació la taula 3 mostra la comparativa entre les diferents implementacions de VPN que es poden trobar, extreta de la url: <http://es.giganews.com/vyprvpn/compare-vpn-protocols.html>

Taula 3. Comparativa de tecnologies possibles VPN

	PPTP	L2TP/IPsec	OpenVPN
Compatible.	Suport integrat per a equips de taula, dispositius mòbils i tauletes tàctils	Suport integrat per a equips de taula, dispositius mòbils i tauletes tàctils	Compatibilitat casi total amb qualsevol sistema d'escriptori, dispositius mòbils i tauletes tàctils.
Sistemes Operatius	Windows	Windows	Windows
	Mac OS X	Mac OS X	Mac OS X
	Linux	Linux	Linux
	iOS	iOS	iOS
	Android	Android	Android
	DD-WRT		
Xifrat	128 bits	256 bits	160 bits: més ràpid i segur
			256 bits: màxima seguretat però necessita més CPU
Seguretat	Xifratge bàsic	El major xifratge, revisió de integritat i encapsulament de les dades dues vegades.	Major xifratge, sense vulnerabilitats conegudes, i les dades son autenticades amb dos extrems mitjançant certificats digitals.
Estabilitat	Molt estable, acceptat per la majoria d'accessos Wi-Fi.	Estable, sempre que el dispositiu sigui compatible amb NAT.	La més estable versus fiable, inclús en xarxes no fiables i darrere encaminador Wi-Fi.
Configuració	Fàcil de configurar, integrat a la majoria de sistemes operatius.	Requereix una configuració personalitzada.	Fàcil de configurar amb programari.
Velocitat	Ràpid degut al nivell menor de xifratge.	Requereix un alt percentatge de CPU. Per tant no és tan ràpid, depenent del maquinari.	El millor desenvolupament. Ràpid, fins i tot en llarga distancia i amb connexions amb TTL alts.
Conclusió	Si OpenVPN no està disponible i les prioritats són la facilitat d'ús i la velocitat damunt la seguretat. En aquest cas és la millor elecció.	És més segur que PPTP però no tant ràpid i necessita d'una configuració més complexa. Si la seguretat és la prioritat i OpenVPN no està disponible és la millor elecció.	Ràpid, segur i fiable, i es pot instal·lar a qualsevol dispositiu dels que s'han d'utilitzar a la immobiliària.

El seu principal desavantatge, de moment, és que hi ha molt pocs fabricants de maquinari que l'integren en les seves solucions. De tota manera això no és un problema ja que amb l'eina Zentyal tenim la possibilitat d'implementar aquesta solució que pareix la més adient, considerant que és una solució multiplataforma que ha simplificat la configuració de VPN's deixant enrere les complicacions esmentades en la configuració de IPsec. A més, Zentyal genera tot el necessari fins i tot

per configurar els clients de tipus Windows, Linux, Mac i Android amb la generació de paquets d'instal·lació, per a cada sistema.

Arribats a aquest punt i una vegada analitzades les diferents opcions per implementar una VPN, s'ha decidit, per les raons exposades, que la solució serà OpenVPN. Tota la configuració del servei es pot veure a l'annex IV.

Ja instal·lat i configurat la xarxa virtual s'han assolit les necessitats d'accés a les dades ofimàtiques, al programari de gestió i al enviament de dades de forma remota, a continuació veurem com s'ha establert la seguretat de tot el sistema.

2.2.5. Seguretat

El sistema està del tot operatiu, malgrat això, tot sistema necessita seguretat i amb aquest objectiu s'han configurat els següents serveis:

- **FIREWALL:** Qualsevol equip, i sobretot, si aquest s'ha d'exposar a una xarxa externa, i a més pública, com és Internet, s'ha de protegir amb un tallafoc que controli totes les connexions possibles als serveis donats. Amb Zentyal el tallafoc es configura en mode "Fail Safe", tot denegat per defecte, per tant s'han d'obrir les connexions que es necessitin. Llavors en aquest cas i segons la configuració de xarxa donada, s'ha obert el port de connexió del servei VPN a qualsevol origen provinent d'Internet, damunt la interfície de connexió externa del servidor Zentyal, d'aquesta forma no es necessari obrir cap altre, ja que la xarxa VPN es considera com una xarxa interna i per tant tot el tràfic estarà permès.

- **IDS/IPS:** Un altre eina que permet millorar la seguretat del sistema perimetral es un IDS o sistema de detecció d'intrusos. En aquest cas s'ha configurat per detectar atacs a l'única eina exposada a l'exterior, el servei de VPN. A més, en cas de detecció d'un possible atac, s'ha activat l'enviament de un missatge de correu a l'administrador del sistema.
- **MONITORITZACIÓ:** la monitorització, és important auditar i registrar tots els esdeveniments del sistema relacionats amb els serveis configurats, d'aquesta forma en cas de fallada es pot trobar la raó d'aquesta més fàcilment. Llavors s'han activats l'enregistrament i enviament de missatge de correu amb l'esdeveniment de qualsevol fallada en els serveis instal·lats així com, l'enregistrament de totes les connexions al servei de VPN.
- **BACKUP:** El servidor ha de tenir una eina de còpies de seguretat per garantir que en cas de fallada total les dades es puguin recuperar. Zentyal ofereix des de la seva consola dos tipus de còpies; en primer lloc, una còpia de la configuració del sistema i en segon, còpia de les dades introduïdes al sistema. En aquest cas el servidor te com a principal funcionalitat la d'actuar com a passarel·la de connexió, no contindrà dades d'usuari i per tant, amb el primer tipus de còpies n'ha prou. Llavors es realitzaran les còpies manualment des de la consola cada vegada que es realitzi un canvi al sistema.

La configuració i administració de tots aquests serveis es tractarà més detalladament al apartat 4 i a l'annex VI, d'aquest document.

Ara el sistema a les oficines centrals està preparat per començar a donar accés a les connexions dels dispositius externs, sempre que suposem el següent punt com finalitzat.

3. Dispositius

3.1 Anàlisi

Avui en dia les possibilitats de dispositius mòbils són molt variades, des de telèfons, tauletes tàctils, portàtils, a memòries USB, a més d'això, s'ha de tenir en compte que cada vegada més, els empleats utilitzen els seus propis dispositius, i que està derivant en una tendència molt comú al món empresarial, el "BYOD", que traduït de l'anglès seria, dur el teu propi dispositiu (veure Bibliografia article "secure Mobile acces"), provant que els administradors de IT i seguretat s'hagin de preocupar de forma especial d'aquest tipus de noves eines a les empreses.

Llavors tenint en compte aquesta tendència i la necessitat de conèixer en tot moment qui s'ha connectat de forma remota a l'oficina central, s'ha decidit donar una unitat USB a cada comercial on hi hagi tot el necessari per poder realitzar la connexió remota, ja sigui utilitzant els ordinadors portàtils de l'empresa (recordem que només hi ha deu i ara són catorze comercials), o els seus propis, o fins i tot, com veurem a les millores del projecte s'ha estudiat la possibilitat de connexió des dels mòbils dels comercials o la compra de tauletes tàctils.

Una vegada decidit que el dispositiu ha de ser una unitat de memòria USB, s'han analitzat les eines que ha de dur per poder connectar-se des de qualsevol ordinador amb connexió a Internet (de l'empresa o no). Primer de tot aquest dispositiu ha de ser personal, només el pot utilitzar el comercial al qual ha esta assignat, a més d'això, ha de ser segur es a dir, que només el personal autoritzat el podrà utilitzar i en cas de pèrdua no ha de ser possible extreure cap tipus d'informació.

A continuació es veu com s'ha realitzat aquesta tasca i com s'ha configurat cada dispositiu.

3.2 Instal·lació i configuració

La seguretat és un dels primers objectius dins aquest projecte, juntament amb la cerca de les eines més adients i econòmiques. Per tant per proporcionar la seguretat d'accés al programari i les dades que es guarden a cada memòria USB, s'ha decidit encriptar totes les unitats amb una clau de pas, d'aquesta forma en cas de pèrdua no serà possible la seva lectura per part de personal no autoritzat.

Per dotar de encriptació a cada memòria USB s'ha estudiat al mercat del programari lliure quines possibilitats hi ha, quina és l'eina més adient per al projecte i s'han tingut en compte les següents característiques:

- Ha de permetre encriptar i desencriptar la informació independentment de si el programari està instal·lat o no al ordinador on es fa servir, llavors l'aplicació ha de ser del tipus "portable", i per tant no ha de requerir de cap instal·lació prèvia.
- El sistema de encriptació ha de garantir la seguretat de les dades, per això aquesta eina ha de ser compatible amb els algoritmes d'encriptació més segurs com; AES, SERPENT, TWOFISH o una barreja dels tres.
- Per últim i molt important, no ha de deixar rastre dins el ordinador on s'ha executat.

D'aquesta forma es pot arribar al objectiu marcat al inici, un dispositiu segur i que ha de permetre la connexió a l'oficina remotament.



Il·lustració 5. Objectiu final

Després d'una cerca minuciosa, s'han realitzat proves amb diferents eines; TrueCrypt, AxCrypt, DiskCryptor, BitLocker Drive Encryption, AES Crypt, Kruptos o Cryptainer LE. Com a conclusió i per tractar-se de l'eina que compleix totes les característiques i a més totalment gratuïta, s'ha elegit TrueCrypt.

A continuació i utilitzant aquesta eina s'ha decidit crear un volum encriptat a la memòria USB. Per aquesta tasca s'ha utilitzat l'algoritme AES, per ser el més ràpid i igualment segur, i una clau, que el propi comercial pot modificar a l'hora de rebre el seu dispositiu. Tota la instal·lació i configuració completa d'aquest es troba a l'annex V.

Arribats a aquest punt es disposa d'un contenidor segur on s'ha de introduir el programari necessari per realitzar la connexió VPN i l'accés a les eines de l'oficina central. En aquest cas s'ha creat, ja que el dispositiu ha de ser mòbil, i independent del programari necessari per establir la connexió, una versió adaptada, que faciliti al usuari la seva posta en funcionament.

A continuació es veu com s'ha arribat a la solució definitiva mitjançant proves i analitzant els resultats.

3.3 Proves, anàlisi i millores

Per arribar a la versió definitiva de que i com introduir programari a la memòria USB, s'han realitzat proves amb els dos comercials inicialment assignats al projecte. Després d'una setmana realitzant accessos remots, s'han agafat totes les indicacions dels comercials a l'hora de l'operativitat del sistema, ja que, ha estat el major dels problemes. S'ha arribat a la conclusió que ha de ser un procés senzill i ràpid, ja que l'operativitat ha de ser la mínima i molt clara davant dels clients.

Arribats a la fase final de les proves s'ha obtingut la versió definitiva. A aquesta el usuari només amb la inserció de la memòria USB al ordinador on vol realitzar la tasca remota, rep la petició de la seva clau i una vegada desencriptat el contenidor, pot iniciar una barra d'eines on realitzar qualsevol de les tasques necessàries fora de l'oficina:

- La connexió a la VPN.
- Entrada a les aplicacions mitjançant el sistema de escriptori remot Ulteo.
- Desconnexió i tancament del tot els sistema abans de retirar la memòria USB del ordinador.

Per a la realització d'aquest procediment s'ha afegit al l'annex V una explicació de tot el contingut del contenidor a més de crear un manual d'usuari, annex VII, que s'ha entregat als dos comercials que han realitzat les proves inicials dels dispositius i que una vegada revisat, és el manual que s'ha entregat a la formació de tots els comercials. (Veure apartat 5.)

En aquest punt del projecte tenim tot el sistema configurat i totes les eines preparades per utilitzar-lo. A continuació es veurà com es dur la gestió i manteniment de tot el conjunt utilitzant una única consola.

4. Manteniment, gestió i revisió

Al principi del projecte s'ha elegit el sistema operatiu Linux amb l'eina Zentyal per la seva facilitat d'ús, comparable o fins i tot, millor que les eines que Microsoft acostuma a tenir. Dons, a continuació es veurà com de fàcil i còmode és aquesta gestió, gràcies a que tot es gestiona amb una única consola amb la conseqüent millora en la seguretat, ja que tot està centralitzat.

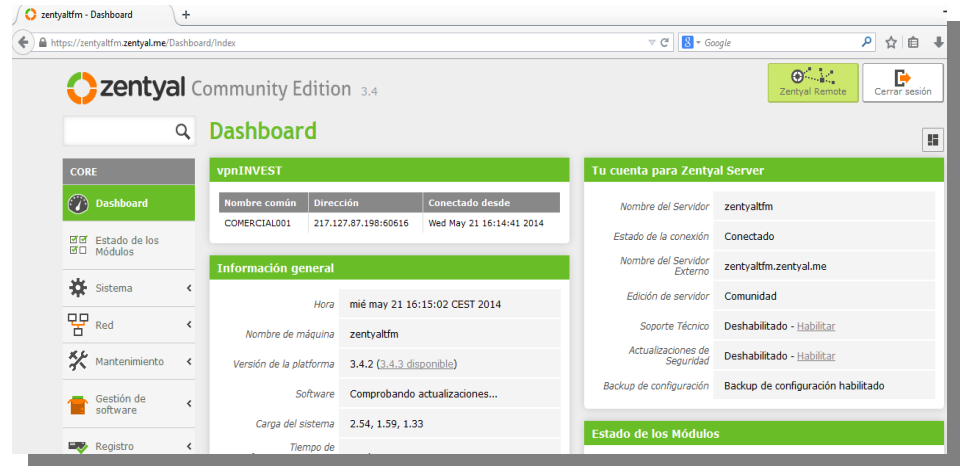
4.1 Consola d'administració

Zentyal otorga a l'administrador una única consola on centralitza tots els serveis del sistema englobats dins els quatre rols vist al punt 2.2.2 de la configuració del servidor. (Es pot veure un exemple de consola a l'adreça <https://zentyalrfm.zentyal.me> que conté el servidor de proves per al projecte)

Il·lustració 6. Consola d'administració de Zentyal.

Aquesta consola, de la il·lustració 6, es divideix en dos zones, una columna a l'esquerra, on podem elegir quin servei configurar i una a la part dreta, on es poden introduir els paràmetres dels diferents serveis. Només en el cas de no haver-hi de configurar cap servei, a la dreta,

apareix la “Dashboard”, un panel de control on es monitoritzen els diferents servei a temps real, com per exemple qui esta connectat a la VPN en aquest mateix moment, com es veu a l' il·lustració 7



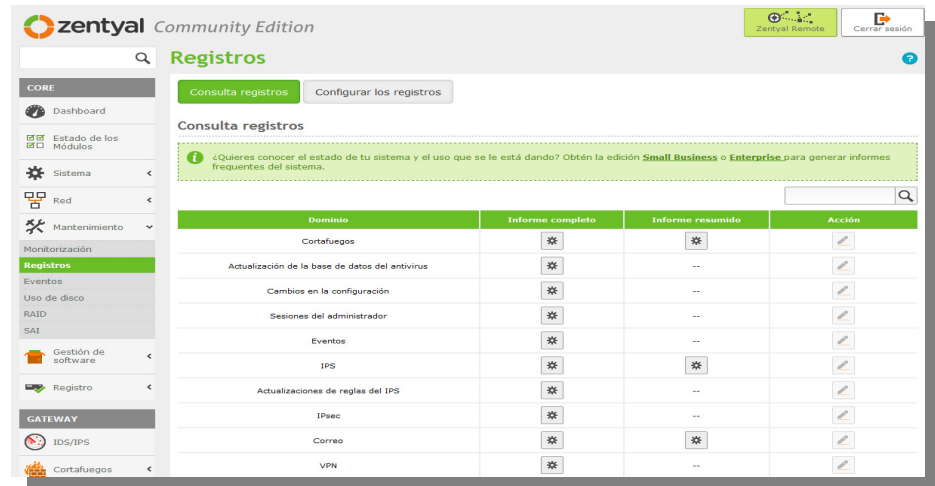
Il·lustració 7. Dashboard de control al instant.

Dins d'aquest panel de control, com s'ha dit, es controlen els serveis en temps real, però a l'hora d'administrar el servidor és molt important que hi hagi un registre del que passa al sistema i com s'ha de suposar aquesta tasca no es farà mirant contínuament el panel de control.

A continuació es presenta quins indicadors s'han configurat per realitzar aquest control i com es controlen tots aquests des de el apartat “Manteniment” on hi ha l'opció de “Registres” i “Esdeveniments”. Tot el necessari per realitzar aquesta tasca forma part del manual de l'administrador del sistema, que es pot veure a l'Annex VI.

4.2 Selecció d'indicadors i control d'enregistrament

Com ja s'ha dit, existeix un apartat de “Manteniment” a la consola de Zentyal, a l' il·lustració 8, es veu on es configurarà, quins registres es volen controlar i fins i tot, es pot crear una regla que enviï un missatge de correu en cas necessari.



Il·lustració 8. Manteniment registres a Zentyal

Segons les necessitats del projecte, interessa registrar:

- Totes les connexions VPN, ja que, aquest servei es la connexió amb l'exterior i per tant el punt d'entrada de tot el tràfic extern. En cas de produir-se qualsevol anomalia quedarà registrat tot el relacionat amb el servei.
- Si algun dels serveis actius, FIREWALL, IDS, VPN, AC... s'atura o falla.
- Si hi ha una entrada de tallafoc no permesa.
- O si el sistema IDS detecta algun atac sospitós.

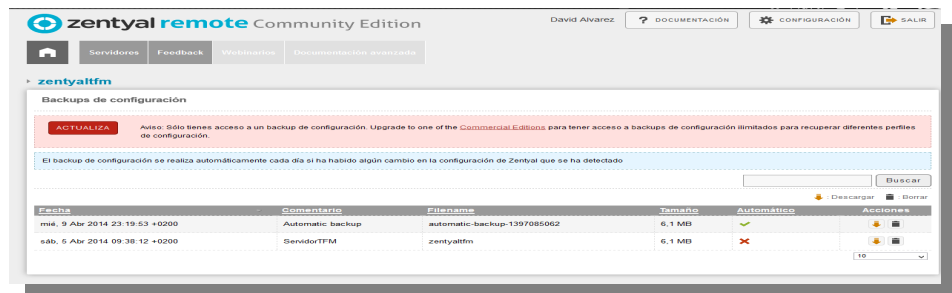
En tots els casos s'ha configurat que s'envii un avís per correu electrònic al administrador del sistema. Com sempre, tot es fa des d'una única consola, en aquest cas la consola mateixa de "Registres", veure manual del administrador annex VI.

Amb aquestes eines hi ha un control total davant possibles fallades, sempre recuperables, per que es poden reconèixer a temps però, en cas de un fallo greu del servidor, tenim un altre eina, les còpies de seguretat.

4.3 Còpies de seguretat

Les còpies de seguretat que es realitzen de forma local al servidor s'han vist a la configuració, al apartat 2.2.5, però en cas de fallada greu, el millor sistema de còpies es aquell que es troba fora del CPD on es troba el servidor, i en aquest sentit, Zentyal, també conté una solució.

Actualment amb la versió 3.4 de Zentyal Community Edition (versió gratuïta) l'empresa ofereix un servei de còpia remota de tota la configuració del sistema. Aquesta versió està limitada a només una còpia, però sempre conté les darreres modificacions fetes al sistema. Fins i tot, la còpia es realitza de forma automàtica, revisant diàriament si ha hagut algun canvi de la configuració i si ha estat així, es realitza una còpia al servei remot. Només s'ha de tenir registrat el servidor al núvol de Zentyal, ZentyalRemote, concretament a <https://remote.zentyal.com> on hi ha tota una consola, com a la il·lustració 9, que permet gestionar la còpia realitzada, descarregar-la i en cas de fallada greu es podria restaurar tot el sistema i la seva configuració amb aquesta.



Il·lustració 9. Consola de Zentyal Remote

Com a curiositat, a més de la còpia del sistema, zentyalRemote també ofereix un servei de DynamicDNS que permet registra el nostre servidor amb un nom públic i automàticament la nostra IP pública estarà associada aquest nom, del tipus “NomServidor.zentyal.me”. D'aquesta forma podem tenir accessible la consola d'administració, encara que no es tingui una adreça IP fixa.

5. Formació

Una vegada tenim tot el sistema preparat i provat, abans de posar a producció es necessari realitzar la formació de tot el personal que el farà servir, tant per l'administrador com pels comercials. Per dur a terme aquesta tasca s'ha creat un manual d'usuari i d'administrador a més de crear petites sessions de formació.

5.1 Manual d'usuari

Tal com començava aquest projecte avui en dia existeixen molts de ginys i l'accés a la oficina de forma remota utilitzant una memòria USB des de qualsevol equip amb connexió a Internet, pot afegir una dificultat extra a la feina diària del comercial, per aquesta raó s'ha intentat crea un manual d'usuari (*veure annex VII*) pensant en que no ha fet servir mai aquest tipus d'eines.

S'ha dividit en totes les funcionalitats que es necessiten:

- Descriptació de les dades al dispositiu.
- Barra d'eines única.
- Establiment connexió amb l'oficina.
- Accés al programari de l'oficina.
- Finalització de la feina.
- Canvi de contrasenya d'accés al dispositiu.

Amb tots aquest punts es dona suport al funcionament específic de la memòria USB per als comercials de la agència immobiliària que cobrirà totes les demandes sol·licitades per realitzar les tasques d'oficina remotament. S'ha de tenir en compte que el maneig del programari propi de l'empresa no està inclòs a aquest manual i que serà la pròpia empresa la que impartirà la formació específica.

5.2 Classes de formació

Tal com ja s'ha comentat la formació del personal es essencial per al correcte funcionament del projecte i es per això que s'ha creat aquest apartat, per a indicar quines han estat les pautes i eines utilitzades per a realitzar la formació de tots els comercials.



Il·lustració 10. Aula de formació

- El primer pas que s'ha fet és; crear grups reduïts de formació. Dos grups de cinc persones i un de quatre, d'aquesta forma els dubtes i comentaris són més fàcils de solucionar i es dona la formació més directa.
- El segon pas que s'ha realitzat ha estat; crear un entorn on poder simular el funcionament de les memòries USB damunt un ordinador de taula. Això ha permès poder presentar aquesta “simulació” a una pantalla de projecció i així poder mostrar el funcionament complet de totes les eines que s'han d'utilitzar de forma visual i real.

Una vegada feta la formació, s'ha realitzat l'entrega de la memòria USB (Annex V) a cada comercial, juntament amb el manual d'usuari (Annex VII).

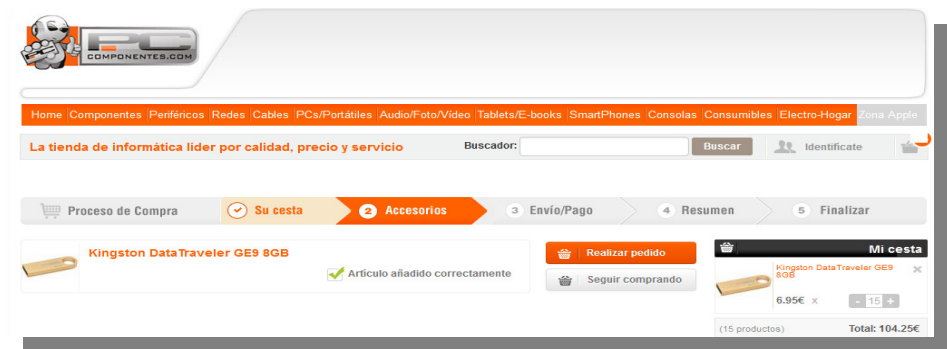
6. Valoració econòmica

Des de l'inici del projecte uns dels objectius ha estat arribar al final d'aquest amb el menor nombre de despeses. Als següents apartats s'estudia quina quantitat s'ha gastat, tant a nivell de maquinari, com de programari i també les hores de feina i quin cost aproximat tindria.

6.1 Maquinari

Pel que fa al maquinari, tot el necessari, a excepció de les memòries USB, ja el tenia l'empresa com s'ha vist al apartat 2.1.2, on s'ha analitzat la situació actual. Llavors l'única despesa en maquinari han estat les unitats USB.

Aquestes han tingut un valor per unitat de 6,95€, en total s'han comprat 15 memòries, una per a cada comercial més una de reserva, ja que el seu cost es petit. Llavors el total de despeses en maquinari ha estat de **104,25€**. (La compra s'ha efectuat a la plana web de l'il·lustració 11).



Il·lustració 11. Compra de memòries USB

El cost total del maquinari ha estat inusual per a un projecte, però amb el maquinari que existeix a l'empresa i només amb unes unitats USB s'ha pogut desplegar tot el necessari.

6.1 Programari

En programari, també s'ha estalviat, millor dit, no s'ha realitzat cap despesa, ja que s'ha utilitzat programari lliure o l'empresa ja disposa de llicències i programari propi, com el sistema de gestió d'immobles.

A continuació es llista la totalitat del programari que s'ha utilitzat, taula 4.

Taula 4. Llistat de programari i el seu cost

Programa	Preu UNITARI	TOTAL
TrueCrypt	0	0
Zentyal Community Edition	0	0
Client OpenVPN Portable	0	0
Yz Dock	0	0
Ulteo Comunnity Edition	0	0
TOTAL		0€

Com es pot apreciar s'ha aconseguit l'objectiu, les despeses totals han estat mínimes, amb només 104,25€ s'ha arribat al objectiu final, d'aquesta forma qualsevol empresa amb pocs recursos podria utilitzar aquesta tecnologia.

Com a cost d'un projecte que ha significat 150h de feina durant 90 dies hàbils, no ha estat molt elevat, però això ha estat sense tenir en compte les hores de feina, que si es comptabilitzessin, suposaria un cost aproximat de 4500€, en el supòsit, d'un cost de 30€ per hora. Llavors el total del projecte arribaria a un total de **4604,25€** .

Arribats a aquest punt només queda extreure conclusions de la totalitat del projecte.

7. Conclusions

Els èxits, problemes i millores de tot projecte es desenvolupen al llarg del temps, encara que durant el mateix trajecte de creació i posta en funcionament aquests es produeixen en major o menor mida. En aquest cas han estat els que segueixen.

7.1 Èxits

Si s'ha de parlar d'èxits, s'ha de dir que han estat gràcies a varies coses:

- Al sistema Zentyal.
- A la inversió mínima, només unes memòries USB.
- I a la Infraestructura prèvia.

Sense aquestes eines no s'haurien arribat a obtenir tots el objectius.

- Obtenir una accés més controlat i segur a la xarxa pública d'Internet.
- Tractament de dades pròpies de l'empresa mitjançant el programari de gestió d'immobles de forma remota i segura.
- Seguretat, totes les comunicacions així com l'accés les eines mitjançant l'enciptació de les memòries USB.

Llavors ha estat un èxit total i absolut la posta en funcionament del sistema Zentyal, també ha estat un èxit el sistema portable de connexió a la xarxa privada remota mitjançant dispositius tant econòmics. I per acabar dir que la integració de la xarxa interna amb la VPN ha estat possible a l'existència d'un serveis prèviament instal·lats i funcionant al màxim rendiment.

7.2 Problemes

A tot projecte es poden trobar obstacles i en aquest cas no ha estat una excepció. Uns dels principals ha estat trobar una tecnologia amb el nivell de seguretat necessari per establir una connexió externa, però després d'un estudi minucios de totes les possibilitats i gràcies a la integració d'aquesta al conjunt de l'eina Zentyal, el problemes han estat mínims. Falta veure, si ara que el sistema s'ha d'utilitzar per un nombre major d'usuaris això implicarà algun problema. Tot s'ha configurat per que no sigui així.

7.3 Millores

Recapitulant, tots els objectius s'han aconseguit, però com sempre tot es millorable i en aquest cas es podria:

- Augmentar la seguretat del sistema instal·lant un segon servidor Zentyal amb balanceig de carrega, per a que en cas de caiguda total del servidor hagués un segon que donés servei.
- Si hem de mantenir el servei accessible davant possibles caigudes, també seria convenient contractar una segona línia de fibra per realitzar un balanceig en cas de caiguda d'una de les dues.
- Realitzar un contracte amb l'empresa Zentyal per a rebre suport "Enterprise", d'aquesta forma es podrien millorar o adaptar eines de Zentyal al projecte en concret, com per exemple posar a la "Dashboard" un panell per controlar les connexions de VPN en temps real indicant usuari connectat i des de que xarxa s'ha connectat, això facilitaria les tasques de suport ja que es tindrien les dades de l'usuari al moment.

El sistema que s'ha utilitzat es pot portar a altres dispositius, com tauletes tàctils o els mòbils intel·ligents, ja que tota la tecnologia que s'ha utilitzat permet obrir una línia de feina per a crear un entorn polivalent.

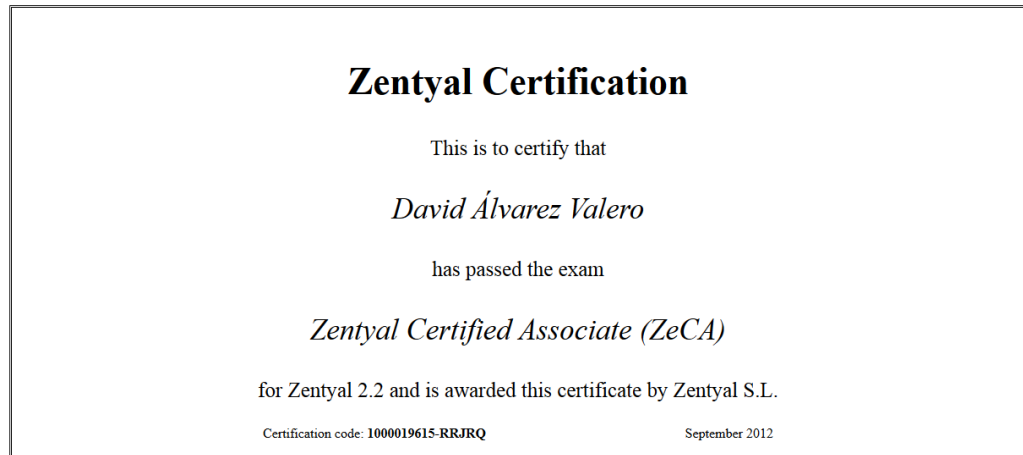
8. Bibliografia

Webs:

- Zentyal Documentació Oficial
<http://doc.zentyal.org/es/>
- Windows Server 2012 – Wikipedia
http://es.wikipedia.org/wiki/Windows_Server_2012
- OpenVPN – Viquipèdia
<https://ca.wikipedia.org/wiki/OpenVPN>
- Lista comparativa de protocolos VPN - PPTP vs L2TP vs OpenVPN
<http://es.giganews.com/vyprvpn/compare-vpn-protocols.html>
- OpenVPN : Conéctate a cualquier red de forma segura
<http://www.redeszone.net/redes/openvpn/>
- Secure Mobile acces : Estudi de la nova tendència el “BYOD”
<https://software.dell.com/docs/secure-mobile-access-whitepaper-14141.pdf>
- Estudi de diferents sistemes d’enciptació de les dades
<http://www.techshout.com/alternatives/2013/28/truecrypt-alternatives/>
- Documentació TrueCrypt
<http://www.truecrypt.org/docs/>

9. Annexes

9.1. Annex I. Certificació Zentyal



Il·lustració 12. Certificació ZeCa obtinguda al Setembre de 2012

9.2. Annex II. Consola unificada de Zentyal

Una única consola gràfica d'administració per a tots el sistema.

The screenshot shows the Zentyal Community Edition dashboard. The interface is divided into several sections:

- Navigation Menu (Left):** Includes CORE (Dashboard, Estado de los Módulos, Sistema, Red, Mantenimiento, Gestión de software, Registro) and GATEWAY (Proxy HTTP, Moldeo de tráfico, IDS/IPS).
- Dashboard (Top):** Features a search bar, the title "Dashboard", and buttons for "Zentyal Remote" and "Cerrar sesión".
- Interfaz de Red (Middle-Left):**
 - eth0:** Estado: activado, externo, enlace ok. Dirección MAC: 00:01:2e:4c:35:3f. Dirección IP: 192.168.1.7. Includes graphs for Bytes Tx (0-39 KB) and Bytes Rx (0-2 KB).
 - wlan0:** Estado: desactivado, interno. Dirección MAC: 0c:d2:92:0f:c7:79. Dirección IP: 192.168.2.7. Includes graphs for Bytes Tx (0-1 B) and Bytes Rx (0-1 B).
- Estado de los Módulos (Middle-Right):** A table listing various services and their status:

Módulo	Estado	Acción
Red	Ejecutándose	
Cortafuegos	Ejecutándose	
Antivirus	Ejecutándose	Reiniciar
Monitor de Ancho de Banda	Ejecutándose	Reiniciar
Autoridad de certificación	Disponible	
DHCP	Ejecutándose	Reiniciar
DNS	Ejecutándose	Reiniciar
Copia de seguridad	Ejecutándose	
Eventos	Ejecutándose	Reiniciar
IDS/IPS	Ejecutándose	Reiniciar
Registros	Ejecutándose	Reiniciar
Correo	Ejecutándose	Reiniciar
Filtro de correo	Ejecutándose	Reiniciar
Monitorización	Ejecutándose	Reiniciar

Il·lustració 13. Consola gràfica d'administració de Zentyal

9.3. Annex III. Configuració Servei Cau

A continuació es veu com s'ha realitzat tota la configuració del servei cau amb la consola de Zentyal. Al apartat de "Gateway" hi el menú de servei Proxy HTTP i de dins tot el necessari per configurar-ho.

La configuració es divideix en quatre seccions, però només s'han utilitzat:

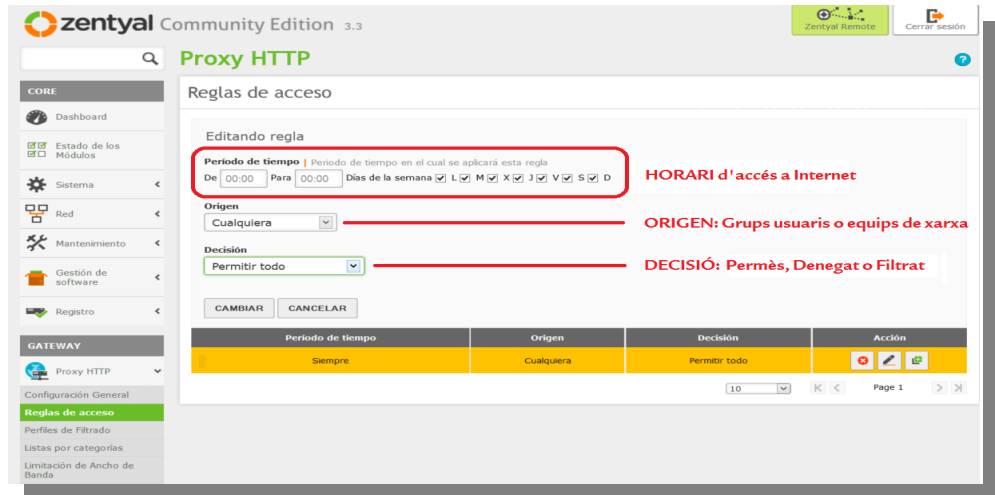
- Configuració General:



- Il·lustració 14. Consola configuració ProxyHTTP

Es pot definir si el proxy funciona en mode Proxy Transparent per forçar la política establerta o si per contra requereix configuració manual, però també te l'opció desitjada, "single sign-on". La característica "Activar Single Sign-On (Kerberos)" serveix per validar l'usuari automàticament usant el tiquet de Kerberos creat a l'inici de sessió del domini, per tant ens pot ser útil si estem usant proxy No Transparent, polítiques d'accés per grups i, per descomptat, un esquema d'autoritzacions basat en Kerberos i en el nostre cas es vol que només els usuaris validats al domini puguin navegar per internet, d'aquesta forma si algú es configura manualment el proxy no podrà utilitzar l'accés a Internet sense permís, per tant una connexió segura i controlada. Els altre paràmetres a tenir en compte en aquesta secció són el port de connexió, per defecte 3128, i la grandària de la memòria cau que el servei farà servir.

- Regles d'accés: Tal com es fa a un tallafoc el servei de cau també pot controlar a quina hora, qui pot accedir i amb quin permisos. Com sempre des de la mateixa consola:



Il·lustració 15. ProxyHTTP regla d'accés.

En el nostre cas qualsevol equip dins l'horari d'oficina podrà navegar per internet, però la decisió serà de tipus Filtrat perquè es vol indicar on està permès anar. Per definir els filtres tenim la següent secció.

- Perfils de filtrat: Ara s'ha d'indicar quin serà el perfil del filtre que volem aplicar per això tenim a la següent pantalla tot el necessari:



Il·lustració 16. Perfils de filtrat

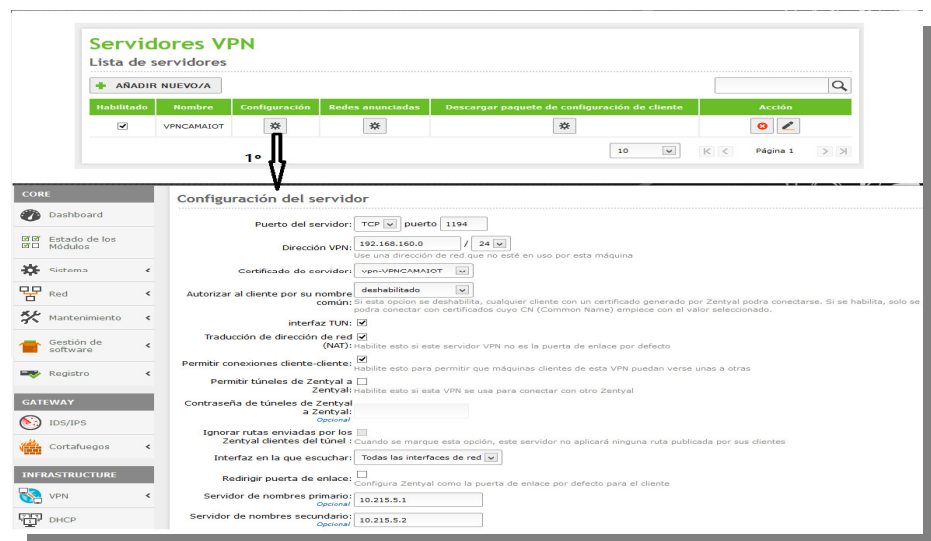
A la pestanya “Regles de dominis i URLs” de la il·lustració 9 podem decidir de forma estàtica quins dominis estaran permesos en aquest perfil. Podem decidir bloquejar llocs especificats només com a IP, per a evitar que algú pugui evadir els filtres de dominis aprenent les adreces IP associades. Així mateix amb l'opció “Bloquejar dominis i URLs no llistats” podem decidir si la llista de dominis de més a baix es comporta com una blacklist o com whitelist, és a dir, si el comportament per defecte serà acceptar o denegar una pàgina no llistada.

Una vegada instal·lat i configurat només queda crear la llista completa de llocs on està permès navegar i aplicar la nova política de seguretat al domini de l'empresa.

9.4. Annex IV. Configuració servei VPN

Com tot servei que ofereix Zentyal, la seva instal·lació i configuració es fa des de la mateixa consola i en el cas de OpenVPN, ocorre el mateix.

La configuració bàsicament es divideix en dos seccions, una part de servidor i l'altre de client.



Il·lustració 17. Panel de configuración servidor de OpenVPN de Zentyal

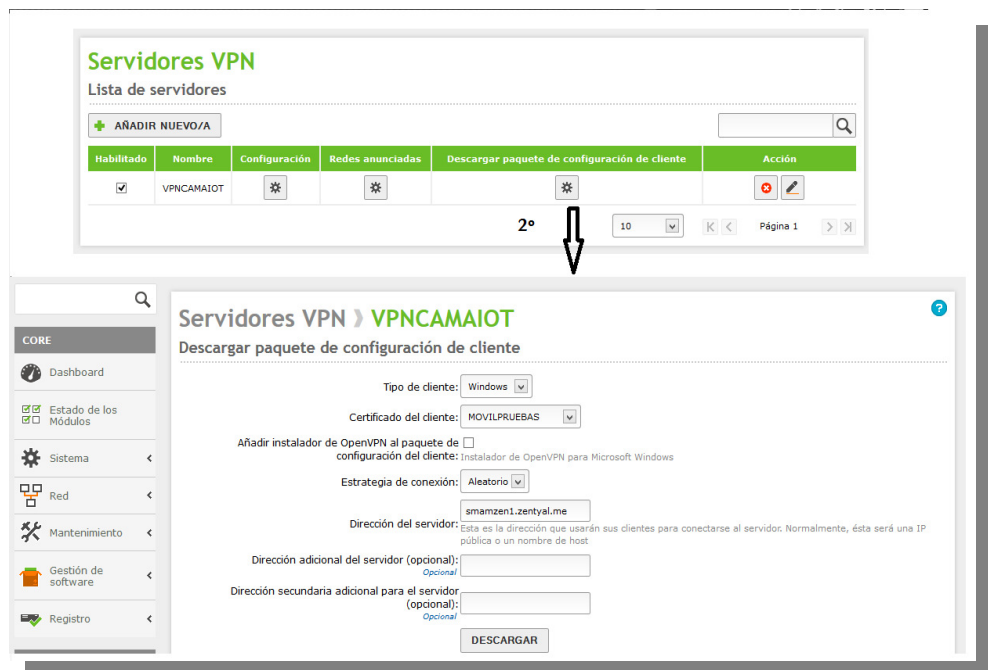
Servidor: Aquesta part és la més complicada, perquè intervenen un conjunt de paràmetres que s'han d'entendre, però una vegada aclarits, la seva configuració és realment senzilla i ràpida gràcies a la consola de Zentyal. Dins d'aquest paràmetres s'han de configurar els següents:

- Tipus i Port de connexió: es defineix quin port de connexió s'ha utilitzat, OpenVPN utilitza el 1194, per defecte. A més s'indica si la connexió serà fent servir datagrames TCP o UDP, en el nostre cas s'ha configurat UDP, ja que es més fort enfront d'atacs DoS i escanejos de ports (gràcies a que és no connectiu, no fiable i no orientat a connexió com TCP).
- Adreça xarxa VPN: S'ha establert la xarxa, segons la configuració indica per aquesta, 192.168.170.0/24, d'aquesta forma cada client connectat rebrà una adreça IP per DHCP.
- Certificat del Servidor: Pel que fa al xifratge de les comunicacions el nostre servidor necessita un certificat que s'ha emès des de la nostra pròpia C.A. per comprovar que els certificats dels clients són vàlids. Llavors amb l'instal·lació del servei OpenVPN, aquest certificat es genera automàticament, només queda seleccionar-lo.
- Interfaz TUN: Tal com s'ha explicat en l'anàlisi de implementacions de VPN tenim que OpenVPN pot implementar tant el transport per capa 2 com per capa 3 del model OSI. Llavors si s'activa aquesta interfície es realitza un túnel per capa 3 i per tant encapsula tot en datagrames IP i si no es fa actua com un pont de capa 2. En el nostre cas com que les dades seran de tipus IP, activarem la interfície, a més els dispositius mòbils suporten aquest i no l'altre.
- Traducció NAT: Es necessari activar aquesta opció del servei, ja que la porta d'enllaç per defecte dels clients no serà el servidor Zentyal, però

es vol que les peticions fetes a la xarxa interna siguin respostes al servidor Zentyal i no a la seva porta d'enllaç predeterminada.

- Interfície d'escolta: S'ha indicat la targeta de xarxa connectada al encaminador del nostre proveïdor d'Internet amb ip dins la xarxa perimetral, 192.168.1.0/24.
- Servidor de Nom Primari i Secundari: S'han configurat els servidors del domini intern, per a que els client externs puguin resoldre les adreces de la xarxa interna des de la xarxa de VPN.
- Domini: Aquest darrer paràmetre es opcional, però ajuda a resoldre els noms de xarxa interna.

Arribats a aquest punt es té configurat el servidor de VPN per a rebre connexions externes. A continuació només s'han de generar els paquets de connexió per als client, que amb la consola de Zentyal es fa d'una forma senzilla i còmoda. Només s'ha de crear un certificat des de la A.C. , per al dispositiu i usuari que es vulgui configurar.



Il·lustració 18. Panel de configuración client de OpenVPN de Zentyal

Clients: Des de la consola de configuració del servei de VPN i amb l'opció "Descarregar paquet de configuració de client" s'obté tot el necessari per configurar el client VPN.

Només s'han d'introduir els següent paràmetres:

- Tipus de client: Quin tipus de client es vol configurar, Windows, Linux o Mac i s'ha de conèixer que amb la configuració de Windows, es possible configurar client per Android i Iphone.
- Certificat: S'ha de seleccionar el certificat creat anteriorment.
- Instal·lador: Si s'activa aquesta opció, juntament amb els fitxers de configuració es descarrega el programari client de OpenVPN per al tres sistemes operatius indicats al principi, pel que fa a Android i Iphone s'han de descarregar de les seves respectives "stores".
- Estratègia de connexió: A l'hora de connectar amb el servidor de VPN s'ha d'indicar la seva Ip pública o una adreça pública i l'ordre de com es realitza pot ser aleatori o en ordre de introducció
- Adreça Ip/Nom públic: S'ha introduir l'adreça IP pública que ha assignat el nostre proveïdor de serveis d'Internet.

Una vegada introduïts els paràmetres es pot descarregar un paquet comprimit que contindrà tot el necessari per a instal·lar el client.

Finalment tenim el servidor de VPN completament configurat.

9.5. Annex V. Creació i configuració memòria USB

Amb aquest manual es descriu el procediment de creació del contenidor encriptat a la memòria USB i de les eines instal·lades per accedir per VPN. *(Sempre suposant que es farà servir a un ordinador amb sistema operatiu de Microsoft, encara que no es descarta la possibilitat en un futur de realitzar el mateix per a Mac o Linux).*

El primer de tot es crear el volum encriptat i per realitzar això s'han de utilitzar les eines de TrueCrypt, concretament la destinada a la creació de volums, exactament al menú "Volumes" s'ha d'agafar l'opció "Create New Volume..." i a continuació apareix:



Il·lustració 19. Creació d'un contenidor amb TrueCrypt

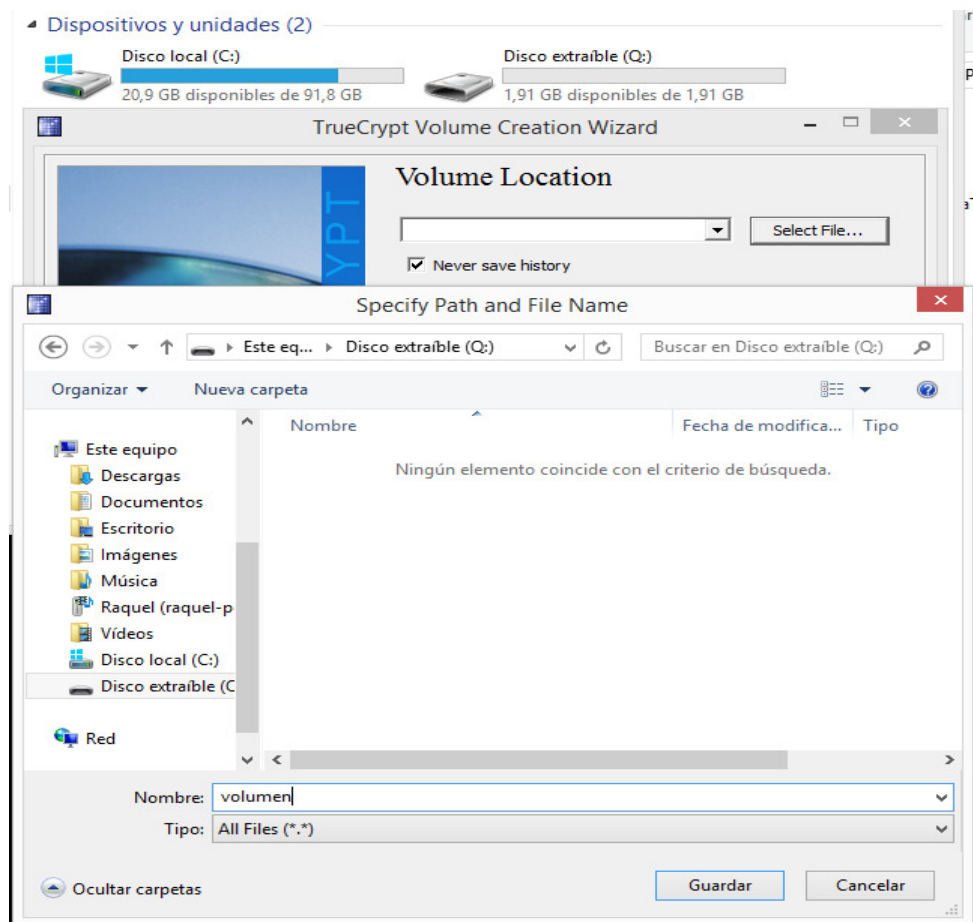
Com és pot veure tenim tres opcions i s'ha de seleccionar la primera de totes per crear el contenidor que volem posar a la nostra unitat USB, en aquest cas Q:\. A continuació hi la possibilitat d'ocultar el volum a crear

però en el nostre cas volem crear un contenidor , llavors elegirem la versió “Standard TrueCrypt volume” com es veu la il·lustració següent:



Il·lustració 20. Tipus de volum amb TrueCrypt

A continuació demana on es vol ubicar el volum encriptat, s’ha d’indicar el nom del fitxer, per exemple “volumen” :



Il·lustració 21. Nom de fitxer del contenidor TrueCrypt

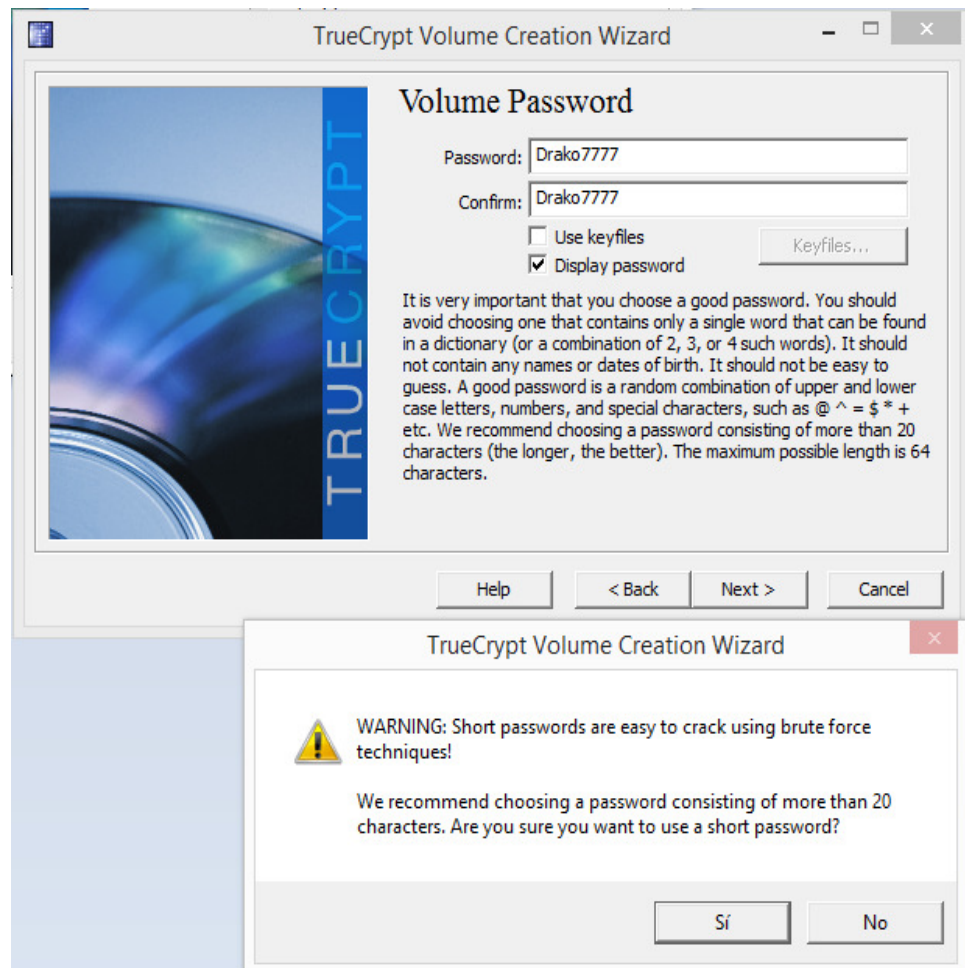
La següent passa és indicar el algoritme d'enciptació del contenidor, en aquest cas s'ha elegit AES que després d'estudiar les possibilitats dels diferents algoritmes aquest pareix que és el que millor rendiment dona i continua essent segur.



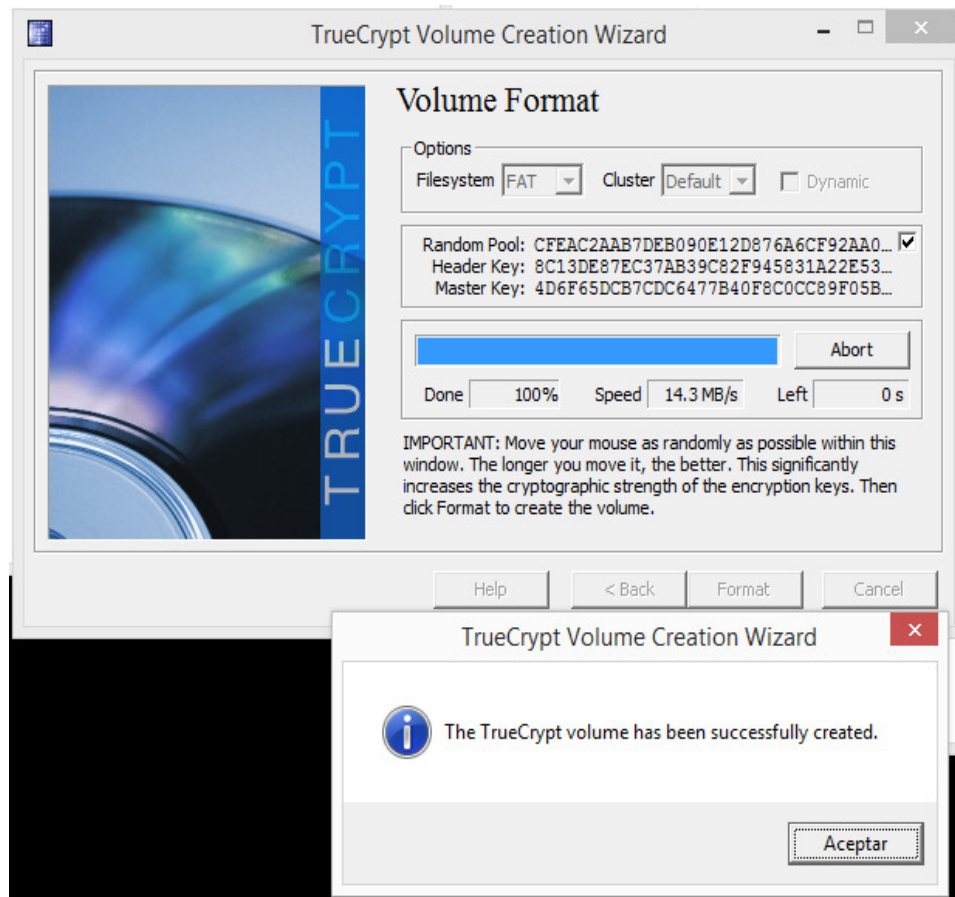
A continuació s'ha de indicar la grandària del contenidor, en el nostre cas s'ha analitzat la mida de les eines que han d'anar de dins i amb 100MB es suficient



Ara és el moment d'eleger la clau per descriptar les dades, en aquest punt es dona al comercial una clau i després amb el procediment explicat al manual d'usuari podrà canviar-la, també s'explica que ha d'introduir la seva clau amb un mínim de seguretat, es a dir, 8 caràcters o més i haurà números i lletres, d'aquesta forma la contrasenya serà mitjanament segura, encara que el sistema ens avisa de que hauria de ser millor. Per fer les proves en mostrat la contrasenya, per assegurar que és la que es vol. (drako7777).

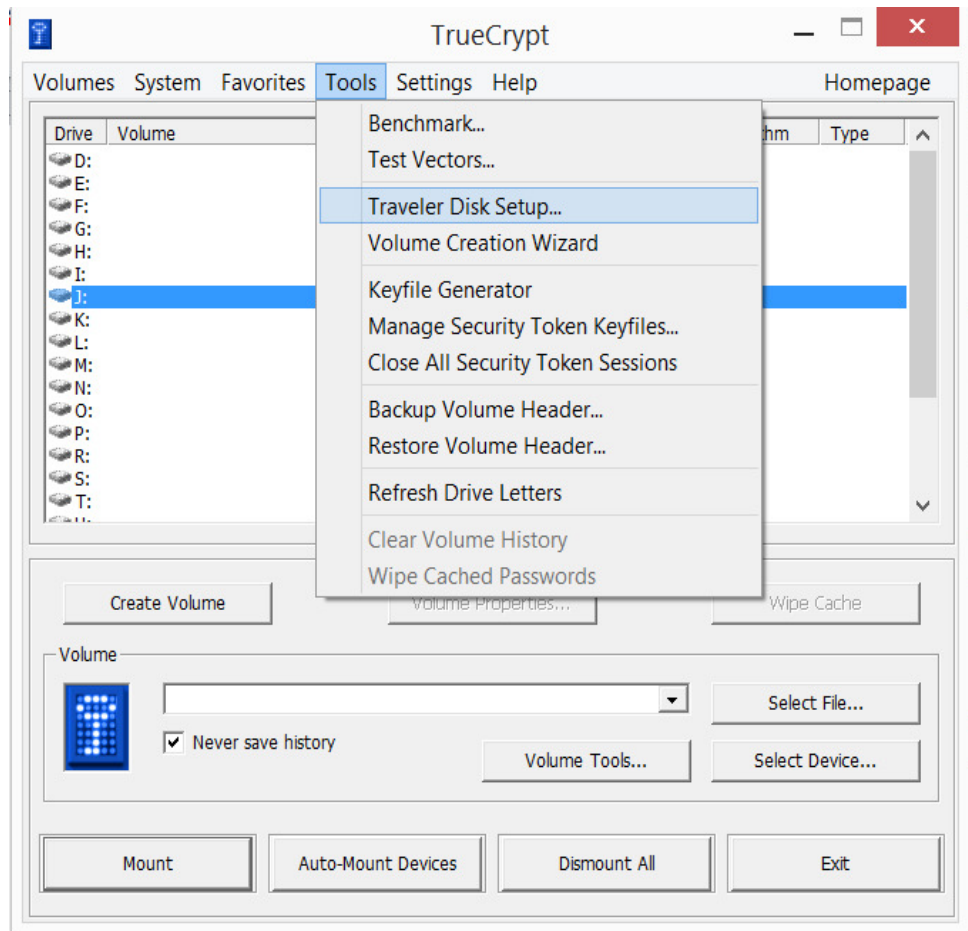


Per finalitzar només s’ha de donar “Format” al contenidor tal com es veu i ja tenim el volum creat al nostre USB.



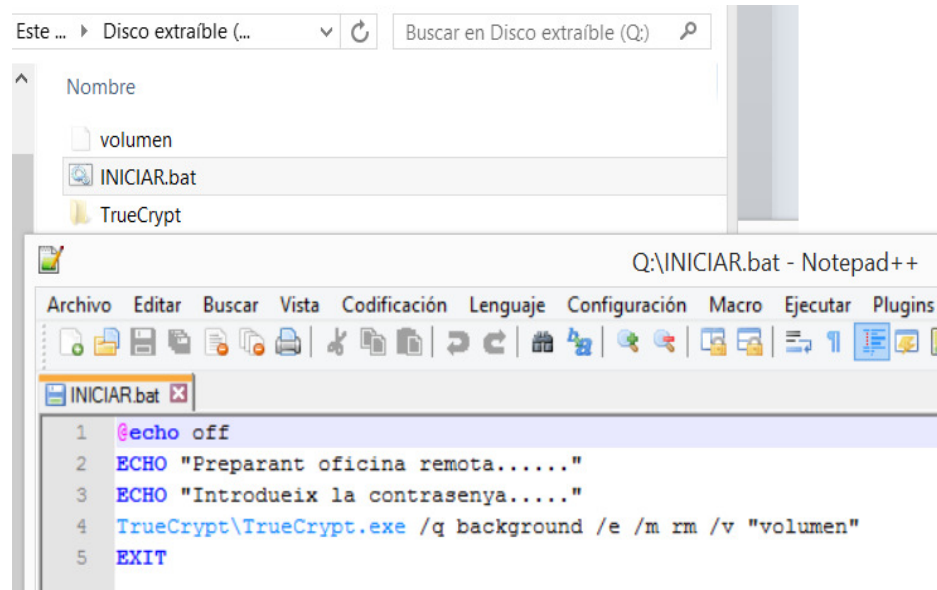
Ara per a que el procediment de posada en marxa sigui tal com s’ha demanat, ràpid i fàcil d’utilitzar, s’ha creat una petita automatització de posada en funcionament de les eines.

Primer de tot per descriptar el volum es necessari el programi Truecrypt instal·lat a la unitat USB, el que s’ha fet ha estat instal·lar aquest utilitzant l’eina que el propi TrueCrypt porta “Traveler Disk Setup”



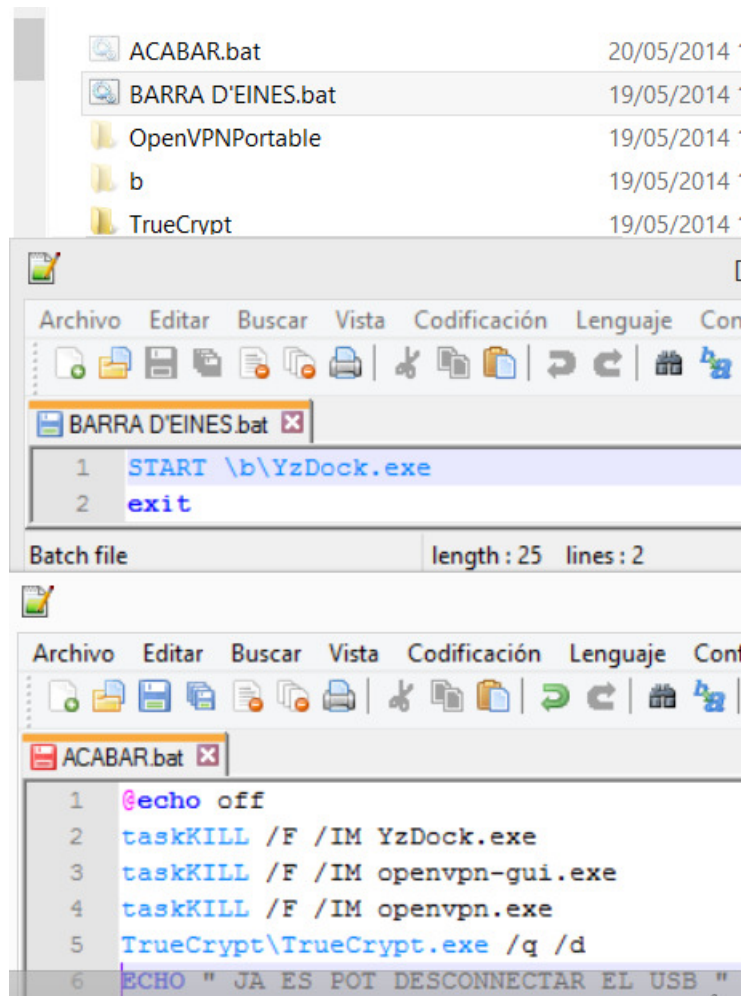
i així introduir el programari portable al arrel del USB, i per ocultar-lo s'han indicats als arxius que són ocults. Llavors la memòria USB conté:

- iniciar.bat : batch per iniciar el muntatge i descriptació del contenidor “volumen” on es troben les eines de connexió.
- volumen: contenidor creat al inici d'aquest manual on hi són les eines de connexió encriptades.
- TrueCrypt: programari portable de l'eina d'encriptació i descriptació.



Una vegada s'ha muntat el contenidor amb "INICIAR.BAT" aquest conté:

- BARRA D'EINES.BAT: batch que llança una barra d'eines que permet al usuari realitzar totes les tasques necessàries per iniciar la connexió a l'oficina remota, obrir el programari i eines d'accés al escriptori remot d'Ulteo, finalitzar i tancar tot el dispositiu.
- OPENVPNPORTABLE: conté el client portable de la vpn i el certificat del usuari que te assignat la memòria USB.
- B: conté la barra d'eines i la seva configuració, si es necessari més endavant introduir noves eines s'aniran afegint aquí.
- TrueCrypt: conte el client portable de TrueCrypt per poder desmuntar l'unitat i tornar a deixar-la inaccessible una vegada finalitzada la connexió.
- ACABAR.BAT: batch que finalitza totes les eines posades en funcionamet a la màquina, tant la connexió VPN com el volum descriptat es desactiven i no deixen rastre al ordinador.



```
ACABAR.bat 20/05/2014
BARRA D'EINES.bat 19/05/2014
OpenVPNPortable 19/05/2014
b 19/05/2014
TrueCrypt 19/05/2014
```

```
1 START \b\YzDock.exe
2 exit
```

```
1 @echo off
2 taskKILL /F /IM YzDock.exe
3 taskKILL /F /IM openvpn-gui.exe
4 taskKILL /F /IM openvpn.exe
5 TrueCrypt\TrueCrypt.exe /q /d
6 ECHO " JA ES POT DESCONNECTAR EL USB "
```

Una vegada arribats a aquest punt es té completament preparada la memòria USB per entregar al comercial assignat. Un exemple de proves es pot trobar a la següent adreça comprimiet en zip.



<https://zentyal.dradigit.com.es/owncloud/public.php?service=files&t=a3f9a2445000b56969949438625d502>

on es troba tot el que dur el dispositiu a l'arrel, tal com s'ha explicat.

9.6 Annex VI. Manual de l'administrador

Aquest manual va dirigit al administrador del sistema que serà l'encarregat de mantenir, gestionar i revisar-ho. Es descriu el procediment de configuració de tots els valors indicats al apartat 4.2

Començarem per el control del principal servei del servidor, les connexions VPN, encara que els altres serveis també es controlen dins la mateixa consola al mateix apartat “Manteniment”.

Una vegada seleccionat tenim l'opció de “Esdeveniments” on es controla quins registres es volen observar i per activar-ho només cal seleccionar l'opció

The screenshot shows the Zentyal Community Edition 3.4 interface. The main heading is 'Eventos'. There are two buttons: 'Configurar eventos' (highlighted in green) and 'Configurar emisores'. The 'Editando evento' section shows the following details:

- Habilitado**
- Nombre:** Observador de registros
- Descripción:** Notifica cuando un registrador (VPN, Sesiones del administrador, Cambios en la configuración, Cuarentena de Samba, Accesos a Samba, Virus en Samba, Proxy HTTP, Cortafuegos, Actualización de la base de datos del antivirus, IPS) ha registrado algo

Below the event details are two buttons: 'CAMBIAR' and 'CANCELAR'. A table lists the following events:

Habilitado	Nombre	Descripción	Configuración	Acción
<input checked="" type="checkbox"/>	Estado	Comprueba si Zentyal está actualmente en activo o inactivo	Ninguno	
<input type="checkbox"/>	Monitorización	Notificar cuando un valor en concreto ha llegado un cierto umbral		
<input type="checkbox"/>	Espacio de almacenamiento libre	Compruebe si alguna partición no tiene espacio de almacenamiento libre		
<input checked="" type="checkbox"/>	Copia de seguridad	Notificar el resultado de los respaldos programados.	Ninguno	
<input checked="" type="checkbox"/>	Servicio	Comprueba si algún servicio de Zentyal no está ejecutándose cuando debería estar haciéndolo	Ninguno	
<input type="checkbox"/>	RAID	Comprueba si algún evento ha ocurrido en el subsistema RAID	Ninguno	
<input type="checkbox"/>	WAN failover	Verifique si las puertas de enlace están conectadas o desconectadas.	Ninguno	
<input checked="" type="checkbox"/>	Observador de registros	Notifica cuando un registrador (VPN, Sesiones del administrador, Cambios en la configuración, Cuarentena de Samba, Accesos a Samba, Virus en Samba, Proxy HTTP, Cortafuegos, Actualización de la base de datos del antivirus, IPS) ha registrado algo		
<input checked="" type="checkbox"/>	Actualizaciones de seguridad	Comprueba si hay alguna actualización de seguridad	Ninguno	

At the bottom right of the table, there is a page indicator: '10' (with a dropdown arrow), navigation arrows, and 'Página 1'.

Després, a aquí mateix tenim el apartat de configuració on s'han d'indicar aquells registres que es volen observar.

Habilitado	Dominio	Filtrando	Acción
<input type="checkbox"/>	audit_sessions		
<input checked="" type="checkbox"/>	openvpn		
<input type="checkbox"/>	audit_actions		
<input type="checkbox"/>	samba_access		
<input type="checkbox"/>	samba_quarantine		
<input type="checkbox"/>	samba_virus		
<input type="checkbox"/>	squid_access		
<input type="checkbox"/>	av_db_updates		
<input checked="" type="checkbox"/>	firewall		
<input checked="" type="checkbox"/>	ips_event		

En el nostre cas es seleccionen el de VPN, el de tallafoc i el de IDS, que son els indicadors que en interessa observar. A més es poden filtrar, per exemple podem fer que als registre de VPN només observi les connexions i les desconexions, llavors es crea una regla i això és que el sistema registrarà.

Una vegada es tenen totes les regles definides es poden consultar fàcilment com al exemple següent.

zentyal Community Edition 3.4

Eventos > Observador de registros > VPN

Filtros a aplicar para notificar registros de VPN

+ AÑADIR NUEVOJA

Daemon	IP remota	Certificado remoto	Evento	Acción
..	..	NOMBRE CERTIFICAT	Cualquiera	[X] [E]

10 [K] [L] Página 1 [R] [X]

Llavors, per definir tots el registres s'ha de configurar com volem que es controlin, es a dir, si només es vol enregistrar per després voler realitzar una consulta o que en cas de trobar un dels esdeveniments filtrats, que envii un missatge de correu al administrador, per això tenim els emissors i en aquest cas activarem el de correu, com es mostra.

zentyal Community Edition 3.4

Eventos

Configurar eventos Configurar emissores

Habilitado	Nombre	Receptor	Configuración	Acción
<input type="checkbox"/>	RSS	Fichero RSS: Alerts	[*]	[E]
<input type="checkbox"/>	Zentyal Remote	Zentyal Remote	[*]	[E]
<input checked="" type="checkbox"/>	Registro	Fichero de registro	Ninguno	[E]
<input type="checkbox"/>	Jabber	Cuenta Jabber	[*]	[E]
<input checked="" type="checkbox"/>	Correo	Cuenta de correo	[*]	[E]

10 [K] [L] Página 1 [R] [X]

zentyal Community Edition 3.4

Eventos > Emisor de correo

El módulo Correo está desactivado. No olvide activarlo en la sección [Estado de los módulos](#) para que sus cambios se efectúen.

Configurar el emisor de correo

Asunto
Evento de Zentyal en zentyaltfm

Para
drako@uoc.edu

CAMBIAR

Per finalitzar amb aquest petit manual de control del sistema, podem veure com es poden consultar els registres per detectar o inspeccionar qualsevol activitat, al exemple que es mostra s'ha consultat quin usuaris s'han connectat a la VPN entre unes dates , i el resultat es mostra al final de la pantalla, d'aquesta mateixa forma es poden consultar tots el registres de tots el serveis monitoritzats.

The screenshot shows the Zentyal Community Edition 3.4 interface. The main content area is titled 'Consulta registros' and 'Informe completos'. It features a search form for VPN logs. The search criteria are as follows:

- Seleccione los informes completos disponibles:** VPN
- Desde la fecha:** 19 / Mayo / 2014 - 23 : 57
- To date:** 21 / Mayo / 2014 - 23 : 57
- Refresh logs:**
- Daemon:** [Empty field]
- IP remota:** [Empty field]
- Certificado remoto:** [Empty field]
- Evento:** Cualquiera

The search results are displayed in a table:

Fecha	Evento	Daemon	Tipo	IP remota	Certificado remoto
2014-05-20 08:10:26	Conexión a cliente terminada	vpnINVEST	server	217.127.87.198	COMERCIAL001
2014-05-20 08:05:08	Conexión a cliente iniciada	vpnINVEST	server	217.127.87.198	COMERCIAL001

Per qualsevol consulta o ampliació en l'àrea d'administració de la consola Zentyal tenim un manual en línia a la web següent:

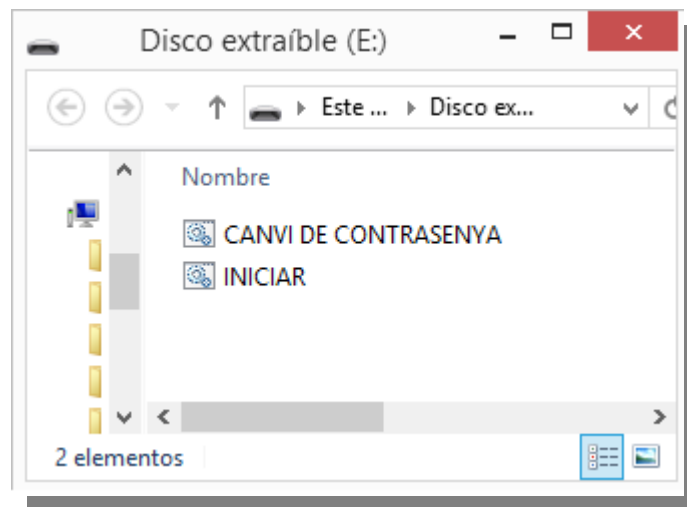
- <http://doc.zentyal.org/es/>

9.7 Annex VII. Manual de l'usuari

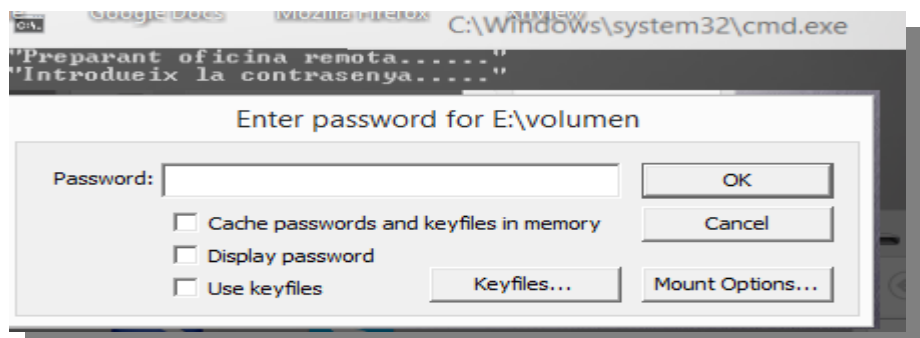
El manual descriu al usuari les passes necessàries per a posar en funcionament l'oficina mòbil que han estat indicades al apartat 5.1.

1. Descriptació de les dades al dispositiu.

El primer pas a realitzar una vegada connectada la memòria USB es anar a aquesta i dins es trobar el fitxer "INICIAR"



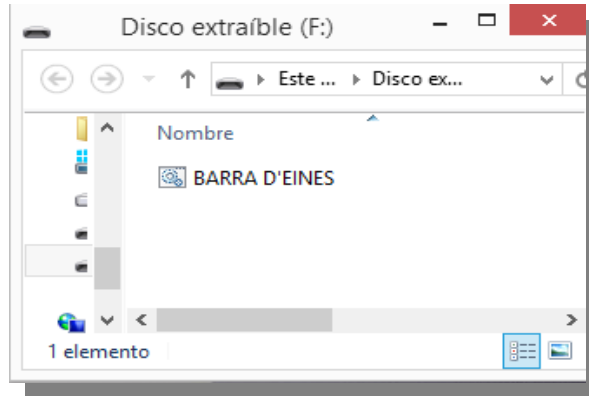
S'ha de pitjar doble clic i així s'inicia el procediment de descriptació i per tant demana la contrasenya d'accés, que inicialment és sa mateixa per a tots, després s'explicarà com es pot canviar.



Una vegada descriptat es dona accés a les eines de l'oficina remota

2. Barra d'eines única.

Per iniciar totes les eines apareix una finestra amb un fitxer anomenat “BARRA D'EINES” que posa en funcionament l'accés a totes les eines necessàries per establir la connexió i el maneig de les dades de l'oficina central.



Aquesta barra d'eines inicialment conté tres opcions possibles



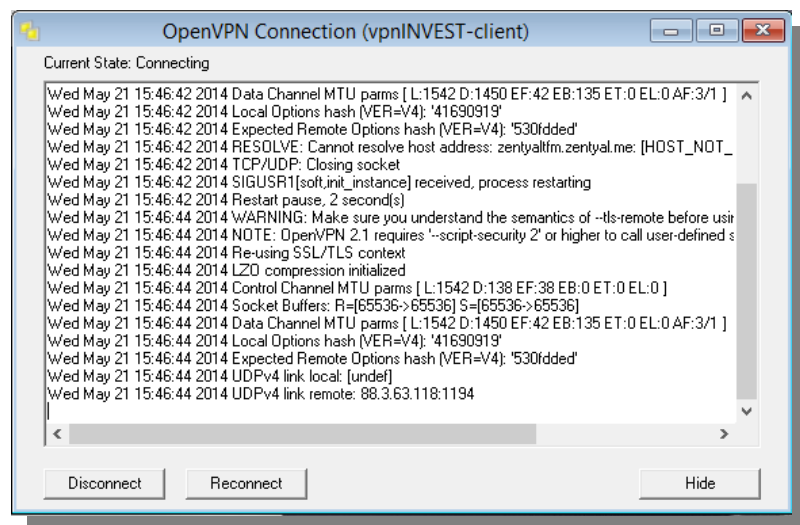
En cas necessari a aquesta barra es poden afegir més eines.

3. Establiment de connexió amb l'oficina.

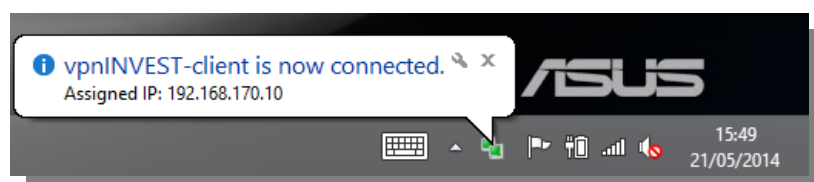
Ara ja està tot preparat per establir la connexió amb l'oficina utilitzant la xarxa privada virtual de l'empresa, només es necessari pitjar al primer icona "CONNECTA OFICINA" i això llençarà el client de connexió automàticament



i establirà la connexió.

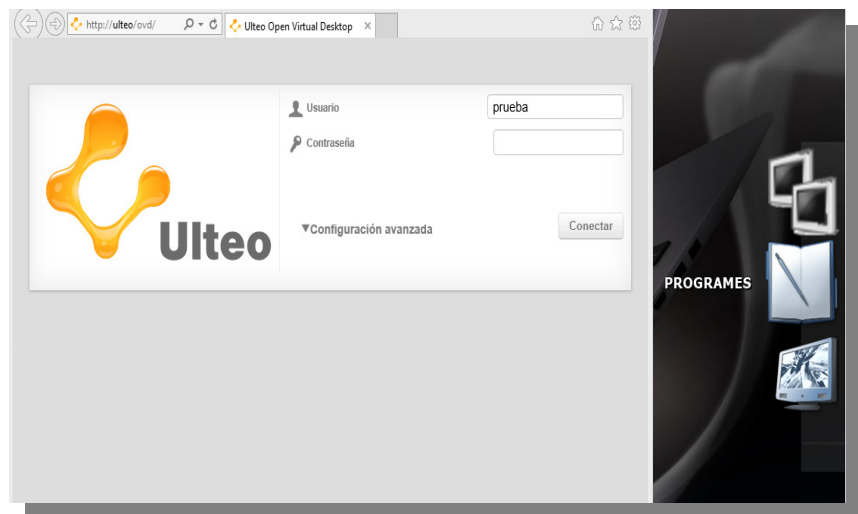


Una vegada acabat el procés apareix una finestra emergent aferrada a uns monitors de color verd, on indica que s'ha realitzat la connexió.



4. Accés al programari de l'oficina.

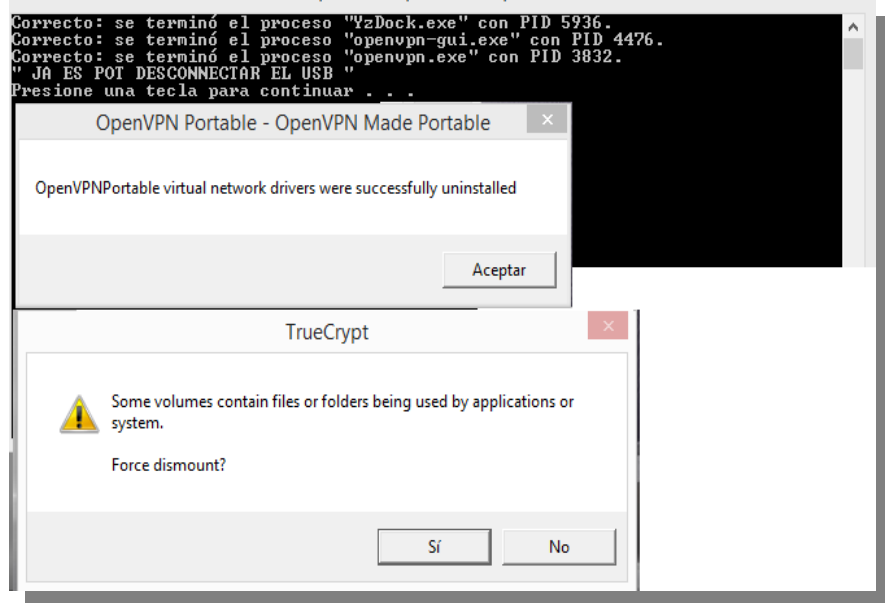
A partir de l'establiment de la connexió ja es pot anar a la barra d'eines i pitjar al icona de "PROGRAMES", i això obrirà la pàgina d'accés a aquest, on cada comercial s'ha de validar amb el seu usuari de domini, i el sistema Ulteo li mostrarà totes les eines definides per accedir remotament.



Ara el comercial pot realitzar les tasques necessàries com si estigues a l'oficina central, amb les mateixes eines i dades. Una vegada finalitzada la seva tasca ha de realitzar el procediment de finalització.

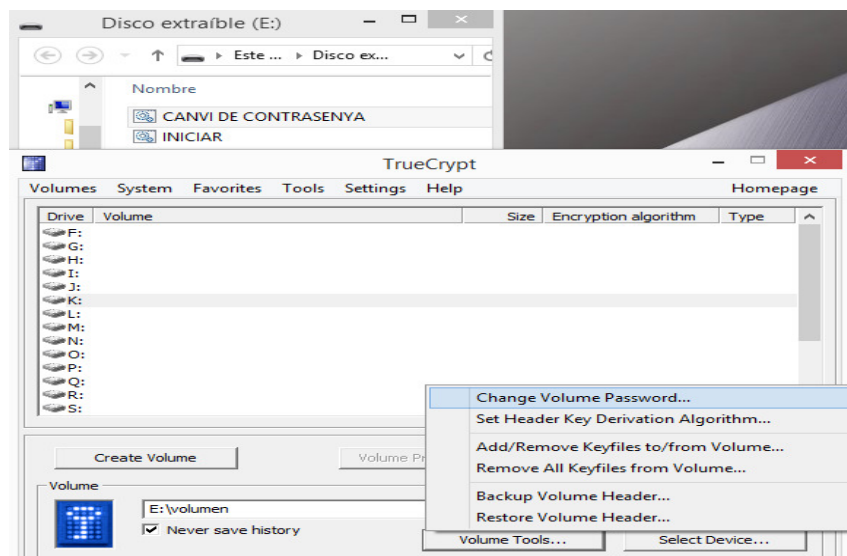
5. Finalització de la feina.

Per finalitzar la feina només s'ha de pitjar al icona de la barra d'eines "FINALITZAR", això desplega tot el necessari per tancar correctament tota la connexió i les eines habilitades des de la memòria USB, donant avisos amb finestres emergents de la seva finalització correcta.

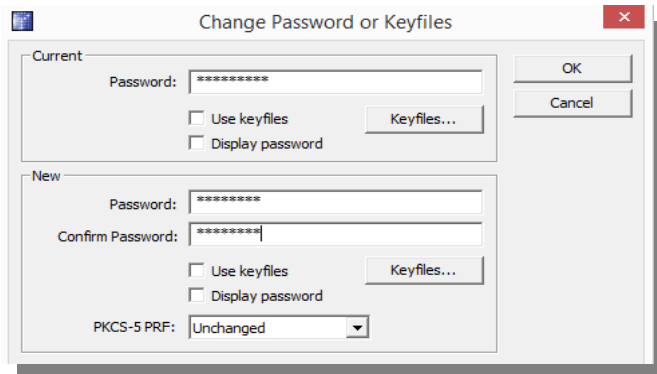


6. Canvi de contrasenya d'accés al dispositiu.

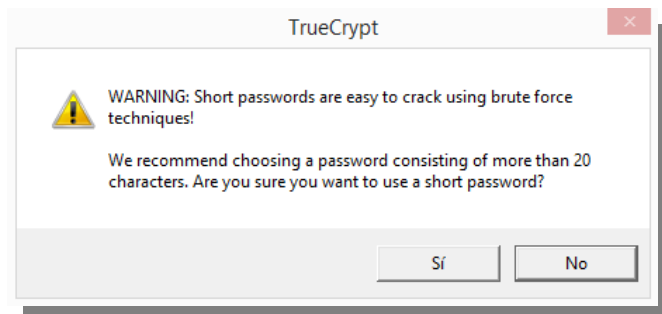
Per finalitzar dins de la memòria USB també es troba el fitxer “CANVI DE CONTRASENYA” que permet realitzar el canvi de contrasenya inicial i que permet accedir a la barra d'eines. Si es pitja a aquest s'obrirà l'eina de gestió i damunt l'opció “Volume Tools” s'ha de seleccionar “Change Volume Password”



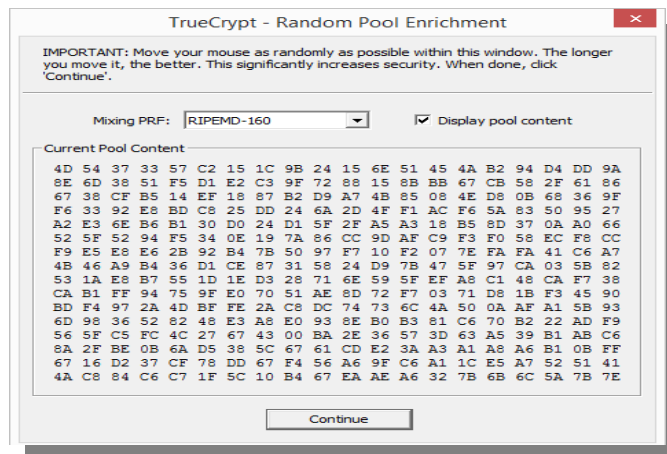
A continuació demana la contrasenya antiga i la introducció de la nova amb la confirmació d'aquesta.



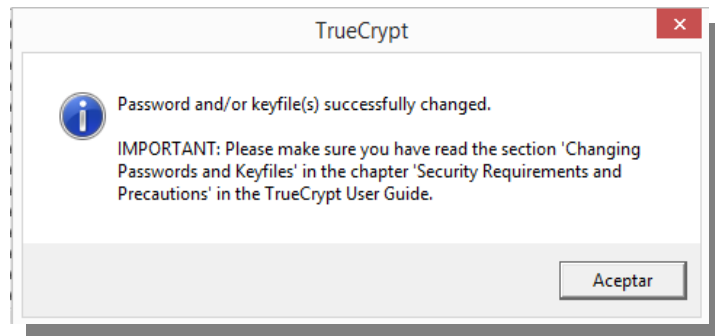
Després al pitjar “OK” a la finestra anterior apareix una finestra flotant advertint de la feblesa de la nostra clau, s’ha de respondre “sí” .



A continuació apareix una finestra de generació de codi aleatori amb el moviment del ratolí, només s’ha de pitjar “Continue”



Per acabar apareix una ultima finestra flotant que indica que el procés de canvi ha anat correctament.



Ara per inicia el sistema s'ha de utilitzar aquesta nova contrasenya