



Virtualització de servidors, monitorització i control del trànsit en sistemes en xarxa

David Ortega Parrilla

Màster de Programari Lliure
Administració de xarxes i sistemes operatius

Consultor: Carlo Di Silvestre

Professor responsable de l'assignatura: Pierre Bourdin

Professor col·laborador: Miguel Martín Mateo

Gener de 2018



Aquesta obra està subjecta a una llicència de
Reconeixement-NoComercial-
SenseObraDerivada 3.0 Espanya de Creative
Commons

Títol del treball:	Virtualització de servidors, monitorització i control del trànsit en sistemes en xarxa
Autor:	David Ortega Parrilla
Consultor:	Carlo Di Silvestre
Professor responsable:	Pierre Bourdin
Professor col·laborador:	Miguel Martín Mateo
Data de lliurament:	01/2018
Titulació:	Màster de Programari Lliure
Àrea del Treball Final:	Administració de xarxes i sistemes operatius
Idioma del treball:	Català
Paraules clau:	virtualització, xarxes, monitorització

Resum del treball

La gestió dels recursos d'una xarxa corporativa és una de les principals tasques d'un administrador de xarxa. Una gestió eficient permetrà una milloria en la qualitat dels serveis oferits als usuaris, així com un millor control dels elements físics i lògics de la xarxa.

L'ús de sistemes d'encaminament i intermediaris personalitzats permet controlar l'ús dels recursos del sistema i millorar la seguretat de la xarxa.

Així mateix, i amb l'objectiu d'aconseguir un millor control de l'estat dels distints dispositius que formen la xarxa, es veu necessari l'ús de sistemes de monitorització.

El desenvolupament de les tecnologies de virtualització ofereix la possibilitat de desplegar sistemes de màquines virtuals amb els distints serveis requerits pel sistema. A més a més facilita les tasques de recuperació d'errades, còpies de seguretat, desplegament dels sistemes i aprofitament dels recursos de maquinari.

Les distintes solucions de programari lliure permeten la implementació d'aquests sistemes, oferint opcions que destaquen per la seua funcionalitat, popularitat i baix cost de desplegament.

A aquest article es detalla la implementació d'un d'aquests sistemes dins d'un cas real d'una xarxa corporativa de mitjana grandària. Dins d'aquesta implementació s'utilitzen màquines virtuals dins d'un sistema de virtualització **Proxmox**. Els serveis d'encaminament, intermediari i seguretat estan implementats en una màquina virtual basada en **pfSense**. Per últim els serveis de monitorització s'implementen en una màquina virtual **Ubuntu Server** amb **Icinga** com a sistema de monitorització.

Abstract

The management of the resources of a corporate network is one of the main tasks of an network administrator. Efficient management will allow an improvement in the quality of the services offered to users, as well as better control of the physical and logical elements of the network.

The use of customized routing and proxy systems allows controlling the use of system resources and improving network security.

Likewise, and with the aim of achieving a better control of the state of the different devices that make up the network, the use of monitoring systems is necessary.

The development of virtualization technologies offers the possibility of deploying virtual machine systems with the different services required by the system. It also facilitates the tasks of errors recovery, backups, deployment of systems and exploitation of hardware resources.

Free software solutions allow the implementation of these systems, offering options that stand out for its functionality, popularity and low deployment cost.

This article details the implementation of one of these systems in a real case of a medium-sized corporate network. Within this implementation, virtual machines are used within a **Proxmox** virtualization system. The routing, intermediary and security services are implemented in a virtual machine based on **pfSense**. Finally the monitoring services are implemented in a **Ubuntu Server** virtual machine with **Icinga** as a monitoring system.

Índex

1	Introducció.	1
2	Objectius.	1
3	Estat de l'art.	1
3.1	Documentació de la xarxa.	2
3.2	Servidor intermediari i d'encaminament.	2
3.3	Serveis de directori.	3
3.4	Sistemes de monitorització de xarxa.	3
3.5	Sistemes de virtualització.	4
4	Anàlisi de requeriments.	4
4.1	Documentació de la xarxa.	4
4.2	Optimització dels recursos de xarxa.	5
4.3	Millora en la seguretat d'accés a la xarxa.	5
4.4	Integració amb serveis LDAP.	5
4.5	Monitorització del trànsit i estat dels equips de la xarxa.	6
4.6	Virtualització dels serveis.	6
5	Anàlisi de viabilitat.	6
5.1	Viabilitat econòmica.	6
5.2	Viabilitat temporal.	7
5.3	Viabilitat personal.	7
6	Descripció del projecte.	7
6.1	Documentació de la xarxa.	8
6.2	Configuració d'un servidor proxy.	8
6.3	Optimització dels recursos de xarxa.	8
6.4	Sistema RADIUS.	9
6.5	Interconnexió amb serveis LDAP.	9
6.6	Monitorització del trànsit i estat dels equips de la xarxa.	9
6.7	Virtualització dels serveis i implantació.	9
6.8	Comprovació dels serveis i proves.	9
7	Arquitectura de xarxa del centre.	9
8	Disseny lògic del projecte.	10
9	Disseny físic del projecte.	12
10	Planificació del projecte.	12
10.1	Documentació de la xarxa.	14
10.2	Configuració d'un servidor proxy.	14
10.3	Optimització dels recursos de xarxa.	15
10.4	Sistema RADIUS.	15
10.5	Interconnexió amb serveis LDAP.	15
10.6	Monitorització del trànsit i estat dels equips de la xarxa.	16
10.7	Virtualització dels serveis i implantació.	16

10.8	Comprovació dels serveis i proves.	16
10.9	Seqüenciació i temporalització de les tasques.	16
11	Implementació del projecte.	18
11.1	Configuració d'un servidor proxy i d'encaminament.	18
11.2	Paràmetres de xarxa del servidor.	18
11.3	Procés d'instal·lació del servidor.	18
11.4	Configuració inicial del servidor.	18
11.4.1	Configuració en mode text.	18
11.4.2	Assistent web de configuració.	21
11.4.3	Configuració de noms d'interfícies.	21
11.4.4	Configuració de DHCP i DNS.	22
11.5	Configuració del tallafocs.	22
11.5.1	Configuració d'àlies.	22
11.5.2	Encaminament i NAT.	24
11.5.3	Tallafocs.	24
11.5.4	Limitadors d'amplària de banda.	25
11.6	Servidor proxy.	28
11.7	Servidor RADIUS.	29
11.8	Portal captiu.	29
11.9	Monitorització del trànsit i estat dels equips de la xarxa.	32
11.10	Virtualització dels serveis.	36
12	Valoració de les tasques desenvolupades.	38
13	Relació dels problemes plantejats.	40
14	Avaluació de les pràctiques i suggeriments de millora.	41
15	Resultats del projecte.	41
15.1	Configuració d'un servidor proxy i d'encaminament.	42
15.2	Optimització dels recursos de xarxa.	43
15.3	Control en l'accés a la xarxa.	43
15.4	Monitorització del trànsit i estat dels equips de la xarxa.	43
15.5	Virtualització dels serveis.	44
16	Valoració econòmica.	44
17	Conclusions.	45
18	Bibliografia.	45
19	Glossari.	46

Índex de figures

1	Esquema lògic de les xarxes del centre	11
2	Nou esquema lògic de xarxa del centre.	13
3	Planificació (1a part)	17
4	Instal·lació de pfSense (I).	19
5	Instal·lació de pfSense (II).	19
6	Pantalla d'inici pfSense (II).	20
7	Asistent Web pfSense (I).	21
8	Configuració d'interfície (I).	22
9	Configuració de DNS (I).	23
10	Configuració d'àlies (I).	24
11	Configuració d'àlies (II).	24
12	Configuració de NAT (I).	25
13	Configuració del tallafocs (I).	25
14	Configuració del tallafocs (II).	26
15	Configuració de limitadors (I).	26
16	Configuració de limitadors (II).	27
17	Configuració de limitadors (III).	28
18	Configuració de limitadors (IV).	28
19	Configuració de proxy (I).	29
20	Configuració de proxy (II).	30
21	Configuració de servidor RADIUS (I).	30
22	Configuració de servidor RADIUS (II).	30
23	Configuració de servidor RADIUS (III).	31
24	Configuració de portal captiu (I).	31
25	Configuració de portal captiu (II).	31
26	Instal·lació d'Ubuntu Server (I).	32
27	Configuració d'Ubuntu Server (I).	33
28	Configuració d'Icinga Web (I).	34
29	Configuració d'Icinga Web (II).	35
30	Configuració d'Icinga Web (III).	35
31	Configuració d'Icinga Web (IV).	36
32	Configuració d'Icinga Web (V).	37
33	Configuració de Proxmox (I).	37
34	Configuració de Proxmox (II).	38
35	Configuració de Proxmox (III).	39
36	Configuració de Proxmox (IV).	39
37	Configuració de Proxmox (V).	40

1 Introducció.

El següent projecte sorgeix de la necessitat de millora de les prestacions de la xarxa interna de l'IES Torrevigía.

L'IES Torrevigía és un centre educatiu d'ensenyament secundari i de formació professional, situat a la localitat alacantina de Torreveja. El centre disposa de 5 aules d'informàtica i ordinadors a la sala de professors, biblioteca i distints departaments. Així mateix el centre disposa de punts d'accés sense fils que permet la connexió des de dispositius mòbils a la xarxa.

El rendiment de la xarxa del centre no és l'òptim debut a l'elevat nombre d'usuaris simultanis existents i a un ús inadequat dels recursos. Aquesta situació és especialment acusada a les hores centrals del matí.

Resulta clara, per tant, la necessitat d'una millor gestió dels recursos de la xarxa. Aquesta millora haurà de centrar-se principalment a com fan ús de la xarxa sense fils els distints dispositius mòbils.

2 Objectius.

Els principals objectius del projecte són els següents:

- Completar la documentació de la xarxa, incloent dades i esquemes.
- Configurar un servidor **proxy** intern al centre que permeti un major control en l'administració de la xarxa del centre.
- Limitació de l'ús de la xarxa als equips i usuaris mitjançant sistemes **QoS** i/o de **portal captiu**.
- Millora a la seguretat de l'accés a la xarxa WiFi del centre mitjançant un servidor **RADIUS**.
- Integració dels paràmetres de configuració amb serveis **LDAP**.
- Monitorització del trànsit de la xarxa i de l'estat dels equips.
- Ús de sistemes de virtualització per a la instal·lació dels servidors, amb l'objectiu de millorar la seguretat i de facilitar la posterior administració del sistema implantat.

3 Estat de l'art.

Per dur a terme el present projecte s'utilitzarà una sèrie de programari d'administració de xarxes i servidors. Les llicències de tot aquest programari seran de tipus lliure. A tot projecte s'ha de fer un estudi previ de les distintes eines disponibles al mercat. D'aquesta manera es podrà triar el programa adequat a les nostres necessitats.

A continuació es detallaran les distintes opcions de programari existents per dur a terme les diverses tasques que componen el projecte.

3.1 Documentació de la xarxa.

Per a realitzar la tasca de documentació de la xarxa es necessitarà d'un procesador de textos. El programari lliure més famós d'aquest tipus és **LibreOffice** ¹. **LibreOffice** es troba disponible a multitud de sistemes operatius i és una solució adequada per a la redacció de majoria de tipus de documents.

Per contra, i com a valoració personal, **LibreOffice** no és la millor solució en la redacció de documents científics i tècnics. Per aquest motiu s'he utilitzarà **LaTeX** ², ja que es considera que proporciona una major qualitat en la maquetació final dels documents produïts. Existeixen multitud de distribucions de **LaTeX** disponibles. En concret s'utilitzarà **MacTeX** ³, amb llicència lliure i disponible al sistema operatiu **MacOS**.

Com a entorn de treball per a editar els documents **LaTeX** s'ha escollit **TeXstudio** ⁴. Aquest programa de llicència lliure està disponible a multitud de sistemes operatius i disposa de nombroses eines que faciliten l'escriptura de textos en **LaTeX**. De tota manera hi ha altres programes perfectament vàlids en aquest sentit: **Texmaker** ⁵, **TeXworks** ⁶, **TeXShop** ⁷...

Per últim, els distints esquemes gràfics de la xarxa es realitzaran mitjançant l'aplicació lliure **Dia** ⁸. Aquest programa compleix perfectament amb els requisits bàsics necessaris, encara que objectivament no arriba a la funcionalitat d'altres aplicacions privatives com ara **Microsoft Visio** ⁹.

3.2 Servidor intermediari i d'encaminament.

Qualsevol sistema operatiu lliure es pot configurar amb els programes i serveis necessaris per a implementar un servidor intermediari i d'encaminament. Aquest tipus d'aproximació té una dificultat de implantació mitja-alta ja que implica la realització de nombroses instal·lacions i configuracions manuals. Per aquest motiu es buscaran solucions lliures que inclouen els paquets i configuracions per defecte adequades per a una implementació ràpida de la solució requerida.

Entre les solucions existents orientades a la implementació de servidors intermediaris i d'encaminament s'ha escollit **pfSense** ¹⁰. **pfSense** és un sistema operatiu

¹<https://www.libreoffice.org>

²<https://latex-project.org/>

³<http://www.tug.org/mactex/>

⁴<http://www.texstudio.org/>

⁵<http://www.xmlmath.net/texmaker/>

⁶<http://www.tug.org/texworks/>

⁷<http://pages.uoregon.edu/koch/texshop>

⁸<http://wiki.gnome.org/Apps/Dia/>

⁹<http://visio.microsoft.com/>

¹⁰<https://www.pfsense.org/>

basat en **FreeBSD** ¹¹ orientat a aquestes tasques i que proporciona una configuració senzilla mitjançant una interfície web. L'ús d **pfSense** implicarà el coneixement del funcionament d'alguns aspectes de **FreeBSD**, els quals difereixen dels emprats a sistemes **Linux**.

Existeixen altres solucions lliures basades en **Linux**. Una de les més conegudes és **Mikrotik RouterOS** ¹². Aquesta solució disposa d'eines més avançades que **pfSense**. Per contra, si no s'adquireix una llicència, passades 24 hores es limita la funcionalitat del sistema.

Per a la implementació del projecte s'ha escollit **pfSense** com a sistema de base. A **pfSense** es troben disponible multitud de paquets que amplien les seues funcionalitats. Alguns d'aquests paquets seran necessaris al projecte, com ara **FreeRADIUS** ¹³.

3.3 Serveis de directori.

Al centre existeix implantat un servei de directori **OpenLDAP** ¹⁴. És per tant un requisit del projecte que funcione conjuntament amb **OpenLDAP** i no amb un altre servei de directori, sigui lliure o privatiu.

3.4 Sistemes de monitorització de xarxa.

La monitorització del trànsit i de la xarxa requereix de la instal·lació de nous serveis i servidors. La solució lliure més reconeguda és **Nagios** ¹⁵. Aquest sistema disposa d'una gran quantitat de documentació sobre la seua instal·lació i configuració. **Nagios** disposa d'una versió lliure i gratuïta que satisfarà les necessitats en quant a funcionalitat requerides pel projecte.

A aquest projecte s'utilitzarà **Icinga** ¹⁶ com a sistema de monitorització. **Icinga** és un programari derivat de **Nagios** i compatible amb els seus complements. En canvi, **Icinga** permet una configuració més senzilla que **Nagios**.

Cal no oblidar que **pfSense** també disposa d'eines que ens ajudaran en la monitorització del trànsit de la xarxa. Aquestes eines també podran ser utilitzades com a complement de les presents a **Icinga**.

Com a sistemes alternatius de monitorització de xarxa lliures estan disponibles **Cacti** ¹⁷ i **Pandora FMS** ¹⁸.

¹¹<https://www.freebsd.org/>

¹²<http://www.mikrotik.com/>

¹³<http://www.freeradius.org/>

¹⁴<http://www.openldap.org/>

¹⁵<http://www.nagios.org/>

¹⁶<http://www.icinga.com/>

¹⁷<http://www.cacti.net/>

¹⁸<http://pandorafms.com/>

3.5 Sistemes de virtualització.

En l'actualitat existeixen multitud de sistemes de virtualització disponibles. Com a sistemes privatis cal destacar **VMWare** ¹⁹ i **Microsoft Hyper-V** ²⁰. Ambdós solucions disposen d'un gran rendiment i eines de configuració i automatització.

Com a sistemes lliures es poden destacar **VirtualBox** ²¹, **Xen** ²² i **KVM** ²³. **VirtualBox** resulta una solució idònia a entorns de pràctiques ja que proporciona una configuració molt senzilla i intuïtiva. A més **VirtualBox** es troba disponible als principals sistemes operatius d'escriptori. En canvi, el seu rendiment i flexibilitat és inferior a altres solucions més orientades a l'àmbit professional.

Tant **Xen** com a **KVM** són hipervisores amb un gran rendiment i flexibilitat. Ambdós solucions s'inclouen únicament a sistemes **Linux**. S'ha triat **KVM** ja que és compatible amb un major número d'eines de virtualització.

En l'actualitat existeixen sistemes de virtualització basats en **KVM** que ofereixen facilitats a l'hora de la creació, configuració i automatització de màquines virtuals. Dos dels sistemes més coneguts són **oVirt** ²⁴ i **Proxmox** ²⁵. **oVirt** està creat per **RedHat** ²⁶ i proporciona un entorn potent de virtualització. Presenta una dificultat d'ús mitja i és una solució idònia a entorns de grandària mitjana-alta. **Proxmox**, en canvi, és un sistema basat en **Debian** ²⁷ molt popular i amb una dificultat d'aprenentatge relativament senzilla. **Proxmox** és una solució perfecta a entorns de grandària mitjana.

Al present projecte s'ha escollit **VirtualBox** en entorns de proves i **Proxmox** com a entorn final de producció.

4 Anàlisi de requeriments.

4.1 Documentació de la xarxa.

El centre educatiu disposa d'una infraestructura de xarxa de mitjana complexitat. Durant anys, la documentació d'aquesta xarxa ha sigut pràcticament inexistent. Actualment només existeix un gràfic de l'estructura física de la xarxa realitzat anys enrere i, per tant, obsolet. L'estructura lògica de la xarxa no disposa de cap tipus de documentació per escrit. Així, no hi ha cap registre sobre les direccions IP dels principals equips de la xarxa.

¹⁹<http://www.vmware.com/>

²⁰<https://www.microsoft.com/>

²¹<https://www.virtualbox.org/>

²²<http://www.xenproject.org/>

²³<http://www.linux-kvm.org/>

²⁴<http://www.ovirt.org/>

²⁵<http://pve.proxmox.com/>

²⁶<https://www.redhat.com/rhel>

²⁷<https://www.debian.org/>

Per aquest motiu, un dels primers objectius del projecte serà actualitzar aquest esquema a la realitat actual de la xarxa del centre.

De la mateixa manera, totes les noves configuracions i equips que s'implanten posteriorment al llarg del projecte han de ser documentades. Aquest és un requeriment important ja que el personal adscrit al centre canvia tots els anys. Per tant, la documentació a realitzar ha de ser de qualitat i gran detall, amb l'objectiu que els futurs treballadors al centre puguin conèixer l'estructura i el funcionament de la xarxa.

4.2 Optimització dels recursos de xarxa.

Molts dels usuaris de la xarxa, majoritàriament amb equips de connexions sense fils, fan un ús inadequat i excessiu de la mateixa. Per tant, és necessari per una banda optimitzar les connexions i d'altra limitar l'ús dels recursos de la xarxa per part dels usuaris.

Encara, que el problema d'ús dels recursos és extensible a tot tipus d'equips, és als equips sense fils on existeix una major problemàtica. Els usuaris de la xarxa sense fils utilitzen multitud de dispositius, en moltes ocasions més d'un alhora. Aquest fet produeix un alt consum dels recursos disponibles de la xarxa. Per tant, controlar i solucionar aquesta situació és el principal requeriment a assolir durant el desenvolupament del projecte.

El centre no té la possibilitat de gestionar el router que dona accés a Internet, ja que aquest es troba sota el control de l'administració central. Per tant, és requisit imprescindible la implementació d'un sistema de gestió interna que els administradors del centre puguin administrat amb total llibertat.

El control de l'ús dels recursos de la xarxa passen per implementar protocols **QoS** als sistemes de gestió implementats al projecte.

4.3 Millora en la seguretat d'accés a la xarxa.

En l'actualitat, l'accés a la xarxa sense fils, es controla mitjançant una única clau mestra **WPA2**. Aquest sistema de control és clarament insuficient. El descobriment d'aquesta clau per part de qualsevol alumne provocaria greus problemes en la xarxa, tant a nivell de rendiment com a de seguretat.

Així, s'exigeix un nou sistema de control d'accés que proporcione un major nivell de seguretat. En relació a aquest punt, es presenta com a una solució l'implementació d'un sistema de **portal captiu**, que a més permeti un major control de l'ús que fa cada usuari dels recursos de la xarxa.

4.4 Integració amb serveis LDAP.

Als ordinadors del centre existeix un sistema d'usuaris de xarxa que controla l'accés als equips i als serveis d'impressió. La implementació del sistema de portal

captiu descrit a l'anterior apartat milloraria la seguretat i el manteniment dels recursos de la xarxa. En canvi, incorporaria una duplicitat als nivells d'autenticació dels equips de xarxa.

El servidor LDAP del centre ha sigut implantat per una empresa externa. Per aquest motiu, i d'igual manera al router que proporciona la connexió a Internet, no es possible accedir a la configuració d'aquest servidor LDAP.

La integració entre ambdós sistemes d'autenticació és un requeriment important del projecte.

4.5 Monitorització del trànsit i estat dels equips de la xarxa.

Solucionats els principals requeriments del projecte i amb l'objectiu de millorar al control de l'ús dels recursos de la xarxa, resulta convenient la implantació de sistemes de monitorització.

Aquests sistemes de monitorització han de permetre el control d'ús dels recursos de la xarxa, a nivell d'equip i d'usuari. El seguiment d'aquestes eines proporcionarà als administradors de la xarxa les dades necessàries per a dur a terme futures noves implementacions i millores del sistema.

4.6 Virtualització dels serveis.

La virtualització de la implementació dels anteriors serveis descrits presenta beneficis a l'hora del manteniment de la xarxa. Encara que no és un requeriment imprescindible del projecte, la inclusió de sistemes virtualitzats ajudarà als administradors en tasques com ara la gestió de còpies de seguretat o la migració dels serveis a distints equips físics.

5 Anàlisi de viabilitat.

5.1 Viabilitat econòmica.

Els requeriments descrits amb anterioritat no exigeixen la utilització d'equips de grans prestacions, excepte en el cas que es vulguen virtualitzar diversos serveis a una mateixa màquina. No obstant això cal vigilar els recursos de xarxa disponibles per als serveis a implementar. Una assignació insuficient d'aquests recursos, com ara l'amplària de banda disponible per als serveis, pot produir problemes al rendiment de la xarxa.

Els recursos econòmics del centre són limitats. Per tant, tota adquisició de nou material necessari per a la implementació del projecte estarà molt controlada. D'aquesta manera es farà ús, sempre que siga possible, dels recursos materials ja disponibles, evitant noves despeses al centre. En conseqüència la viabilitat del projecte depèn de la capacitat de reciclatge d'equips i cablejat existents.

Remarcar, en aquest punt, que tot el programari utilitzat serà lliure i gratuït. Així, no serà necessari cap despesa en funció a l'adquisició de noves llicències de programari.

Ho descrit a l'anterior paràgraf suposaria un impediment insalvable a la majoria de les implementacions, però no faran impossible la realització del present projecte, debut als seus baixos requisits.

5.2 Viabilitat temporal.

Les principals limitacions imposades per a establir el termini de finalització del projecte venen imposades a nivell extern, pel calendari lectiu de la Universitat de Catalunya. En cas que no existiren aquestes limitacions, es podria dur a terme el projecte durant un major període de temps i d'aquesta manera augmentar les probabilitats d'èxit.

No obstant això el limit final d'implantació del projecte serà el present curs lectiu, abans del període estival, moment en el que molts dels treballadors canvien de centre educatiu.

5.3 Viabilitat personal.

El centre educatiu presenta un alt grau de temporalitat als contractes dels treballadors. Aquest fet implica que al finalitzar cada curs canvien gran part de la plantilla del centre. Per aquest motiu, resulta de gran complexitat emprendre qualsevol projecte de durades i envergadura àmplies.

Aquesta situació implica una limitació no només temporal, sinó també a l'hora de produir un projecte complet i ben documentat. Els administradors de la xarxa que continuen al centre al següent curs, poden no ser els mateixos que han dut a terme la implantació inicial.

En conseqüència, la documentació entregada al finalitzar el projecte ha de ser gran qualitat i detall. D'aquesta manera els futurs administradors de xarxa podran assolir els coneixements necessaris per a gestionar el sistema.

6 Descripció del projecte.

Amb l'objectiu de millorar el funcionament de la xarxa es pretén dur a terme les següents tasques:

- Completar la documentació de la xarxa, incloent dades i esquemes.
- Configurar un servidor proxy intern **pfSense** al centre que permeti un major control en l'administració de la xarxa del centre.
- Limitació de l'ús de la xarxa als equips i usuaris mitjançant sistemes **QoS** i/o de portal captiu.

- Millora a la seguretat de l'accés a la xarxa WiFi del centre mitjançant un servidor **RADIUS**.
- Integració dels paràmetres de configuració amb serveis **LDAP**.
- Monitorització del trànsit de la xarxa i de l'estat dels equips mitjançant programari com a **Icinga**.
- Ús de sistemes de virtualització com a **Proxmox** per a la instal·lació dels servidors, amb l'objectiu de millorar la seguretat i de facilitar la posterior administració del sistema implantat.

6.1 Documentació de la xarxa.

Primerament se procedirà a realitzar la documentació de la xarxa del centre. Aquesta és pràcticament inexistent actualment i necessita d'una organització i esquematització adequades. Amb la posterior introducció del servidor proxy, l'esquema es veurà modificat. Aquesta primera tasca es pot subdividir en els següents punts:

- Anotació de les direccions IP fixes dels distints servidors existents en la xarxa.
- Realització de l'esquema de l'estructura lògica de la xarxa.
- Elaboració de l'esquema de l'estructura física de la xarxa.
- Documentació del projecte.

6.2 Configuració d'un servidor proxy.

En aquest apartat es configurarà un servidor intermediari amb sistema operatiu **pfSense**. Aquest servidor proxy realitzarà les funcions d'encaminament i **NAT**, creant una segona xarxa interna on es situaran inicialment els equips amb connexió sense fil. A més es configuraran les regles del tallafoc necessàries per a la connexió d'aquesta segona xarxa amb l'exterior.

6.3 Optimització dels recursos de xarxa.

Els punts a realitzar en aquesta tasca serien:

- Configuració d'un sistema de memòria cau.
- Configuració d'un sistema de repart d'ús de la xarxa **QoS**. Es plantejarà l'establiment de quotes d'amplària de banda entre els usuaris.
- Implantació d'un sistema de portal captiu, la configuració de la qual serà realitzada en els següent apartat del projecte.

6.4 Sistema RADIUS.

En aquest apartat es completarà la configuració del sistema de portal captiu, instal·lant un accés per usuari i contrasenya. Aquest accés es basarà en la configuració d'un servidor **RADIUS**. **FreeRadius** ²⁸serà el sistema utilitzat, disponible per a la seua instal·lació en **pfSense**.

6.5 Interconnexió amb serveis LDAP.

En aquest apartat es contempla la interconnexió del servidor **LDAP** amb el servidor **RADIUS** implantat a l'anterior apartat. D'aquesta manera els usuaris de la xarxa sense fil podran accedir als serveis de connectivitat, carpetes de xarxa i impressió, amb un únic usuari i contrasenya.

6.6 Monitorització del trànsit i estat dels equips de la xarxa.

La monitorització del trànsit de la xarxa es pot realitzar en distints programes. **pfSense** inclou paquets que permeten un control de l'estat del trànsit de la xarxa. S'estudiarà en aquest punt si aquestes eines compleixen amb els requisits del centre o si es decideix per instal·lar alguna altra eina.

Així mateix, resulta interessant dur un control sobre l'estat dels principals equips de la xarxa. Per a dur a terme aquesta tasca s'instal·larà un servidor i distints clients **Icinga**. Com ja s'ha comentat anteriorment hi han servidors on els administradors de la xarxa no tenen control. Per tant, només es realitzarà aquesta tasca als ordinadors amb drets d'administració.

6.7 Virtualització dels serveis i implantació.

Per dur a terme aquesta tasca final s'ha decidit configurar un servidor de virtualització **Proxmox** on estaran les màquines virtuals del proxy i del servidor **Icinga**. Posteriorment serà necessari migrar els serveis configurats de l'entorn de pràctiques al servidor **Proxmox**.

6.8 Comprovació dels serveis i proves.

Per últim es realitzaran les proves pertinents per a comprovar el bon funcionament dels serveis implantats. Aquests serveis han de proporcionar un valor afegit a la xarxa i mai suposaran una disminució en les prestacions de la mateixa.

7 Arquitectura de xarxa del centre.

Al centre existeixen 2 xarxes internes separades entre sí i amb eixides a Internet dedicades.

²⁸<https://freeradius.org/>

La xarxa d'administració **10.20.30.0/24** abasta els equips de direcció i el personal administratiu. Els usuaris d'aquesta xarxa requereixen d'un alt rendiment a la seua connexió a Internet. Per aquesta raó existeix una línia dedicada a Internet per a un nombre reduït d'equips. A més a més, aquesta xarxa es troba aïllada de la resta del centre amb l'objectiu d'assegurar una major seguretat a aquests equips, els quals utilitzen informació confidencial. El router amb adreça **10.20.30.1** dóna accés a Internet als equips d'aquesta xarxa és propietat de Conselleria i els administradors del centre no tenen possibilitat d'accedir-hi per a la seua configuració.

La resta dels equips es connecten a una xarxa central **172.18.45.0/24**. És en aquesta xarxa on es troben els distints punts d'accés sense fils, així com els ordinadors de la sala de professors. A més es troben els distints servidors del centre, com ara els d'impressió, **LDAP** i **NAS**. Els servidors d'impressió i **LDAP** es troben allotjats al mateix servidor físic amb adreça **172.18.45.240**. El servidor **NAS** té l'adreça **172.18.45.210**. El router amb adreça **172.18.45.1** dóna accés a Internet a aquesta xarxa també és propietat de Conselleria. Aquest router fa de servidor **DHCP** amb un *pool* de direccions de **172.18.45.2-199**. Per tant es disposen el rang de direccions **172.18.45.200-254** per a assignar a equips amb adreça fixa.

Entre aquests equips estan els servidors d'aula, els quals realitzen funcions d'enca-minament i de **NAT** per a cadascuna de les aules d'informàtica existents al centre, així com a la sala de la biblioteca. Cadascuna de les 5 aules d'informàtica i la biblioteca disposen d'un servidor d'aula dedicat i formen xarxes separades amb adreça **10.2.1.0/24**. L'existència de múltiples xarxes amb la mateixa adreça deriva d'un disseny imposat anys enrere. Per a un futur es recomana crear adreces distintes per a cada xarxa d'aula i biblioteca.

La figura 1 mostra un esquema de l'estructura lògica de les xarxes del centre.

8 Disseny lògic del projecte.

Amb l'objectiu d'assolir un major control a l'hora de gestionar els recursos de xarxa, s'implantarà un servidor intermediari per a la xarxa sense fils. Aquest equip realitzarà diverses funcions: enca-minament, **proxy**, **NAT**, tallafocs, servidor **DHCP**, **QoS**, portal captiu... Aquest servidor es configurarà com a una màquina virtual amb sistema operatiu **pfSense**.

El servidor **pfSense** farà de porta d'enllaç a una nova xarxa **172.19.45.0/24** on es connectaran els equips sense fils. La idea és que en un futur s'afegeixen també equips amb connexions cablejades. En aquest cas es pot plantejar la creació de noves xarxes o l'ampliació de la màscara per a la xarxa **172.19.45.0**. Les adreces del servidor **pfSense** seran **172.18.45.253** i **172.19.45.253**, per a cadascuna de les xarxes a les que pertany.

El servidor virtual **pfSense** s'allotjarà a un servidor de virtualització **Proxmox** amb adreces **172.18.45.254** i **172.19.45.254**.

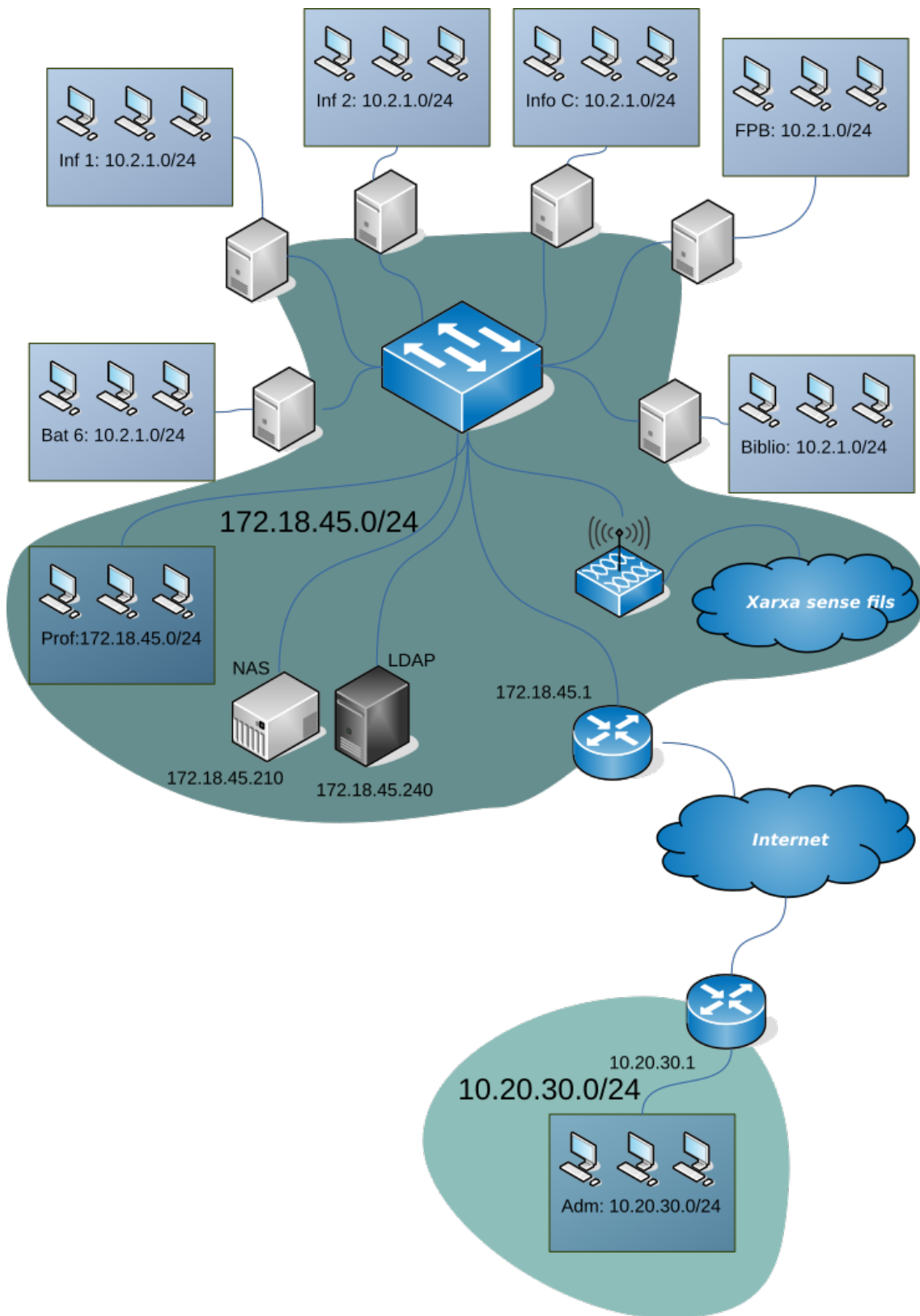


Figura 1: Esquema lògic de les xarxes del centre

La implantació de successius servidors virtuals es realitzarà assignant la següent adreça disponible, començant per la **172.X.45.253**, en ordre descendent.

La figura 2 mostra un esquema de l'estat final de les xarxes una vegada finalitzat la implementació del projecte.

9 Disseny físic del projecte.

La implantació d'un servidor intermedi per a un conjunt d'equips implica una sèrie de decisions a nivell físic, claus per a obtenir un rendiment òptim en el sistema de xarxa. Aquest servidor implementarà diverses funcions, les quals requeriran d'una sèrie de recursos de computació i xarxa.

En primera instància s'ha d'escollir un equip físic amb els recursos necessaris per a poder suportar la funcionalitat del servidor de virtualització i les màquines virtuals allotjades en ell. En aquest punt, cal aclarir que el centre no disposa de pressupost per a adquirir nous equips. D'aquesta manera serà necessari reciclar material present al centre i que no estiga sent utilitzat actualment. Els equips disponibles en el centre no són de grans prestacions i, per tant, disminuirà el rendiment del servidor de virtualització. Aquest fet limitarà en gran mesura el nombre de màquines virtuals que podrà suportar l'equip físic.

L'elecció de **pfSense** com a sistema operatiu per al servidor intermedi permet controlar els recursos necessaris per a la seua implantació. No obstant això serà necessari la migració en un futur del sistema a un equip de majors prestacions, el qual permeti la inclusió de nous serveis i a un major nombre d'equips clients.

La inclusió d'un servidor intermediari per a un grup d'equips exigeix d'uns recursos adequats a nivell de connectivitat de xarxa. Cal vigilar aquest punt ja que l'equip farà de porta d'enllaç a un nombre no menyspreable d'equips. Per aquest motiu es contempla la possibilitat de realitzar un *bond* de varis ports de xarxa. D'aquesta manera es poden unir diversos ports com a únic port de xarxa virtual, el qual serà utilitzat per **pfSense**. En conseqüència s'obté una major amplària de banda al sistema amb l'objectiu de donar un millor servei als equips clients. Per a realitzar el *bond* serà necessari configurar el switch gestionable on estarà connectat el servidor físic. Aquest switch és un **D-Link DGS-1210** de 48 ports.

L'esquema físic de la xarxa del centre es modificarà situant un nou switch gestionable on es connectaran els distints punts d'accés sense fils. Així mateix a aquest switch es connectarà el servidor físic. El nou switch realitzarà la connexió dels distints nodes que componen la xarxa **172.19.45.0/24**. Per una altra banda es connectarà el servidor al switch D-Link situat a la xarxa **172.18.45.0/24**.

10 Planificació del projecte.

La implementació del projecte es realitzarà mitjançant la subdivisió en tasques. Aquestes integraran de manera progressiva les distintes funcionalitats requerides

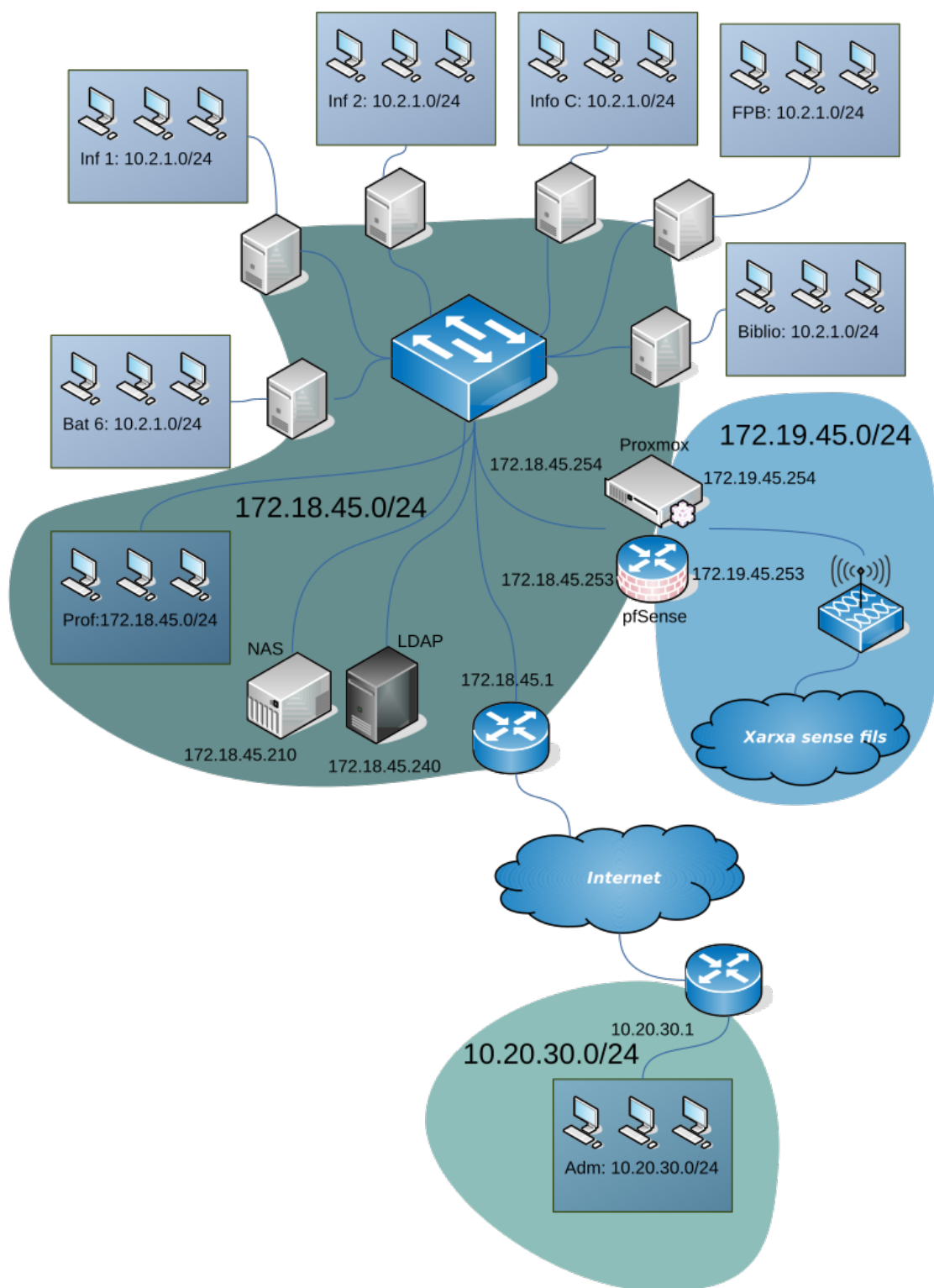


Figura 2: Nou esquema lògic de xarxa del centre.

pel projecte. Les tasques a realitzar ja han sigut descrites a anteriors apartats de la memòria i són les següents:

- Completar la documentació de la xarxa, incloent dades i esquemes.
- Configurar un servidor proxy intern **PfSense** al centre que permeti un major control en l'administració de la xarxa del centre.
- Limitació de l'ús de la xarxa als equips i usuaris mitjançant sistemes **QoS** i/o de portal captiu.
- Millora a la seguretat de l'accés a la xarxa WiFi del centre mitjançant un servidor **RADIUS**.
- Integració dels paràmetres de configuració amb serveis **LDAP**.
- Monitorització del trànsit de la xarxa i de l'estat dels equips mitjançant programari com a **Icinga**.
- Ús de sistemes de virtualització com a **Proxmox** per a la instal·lació dels servidors, amb l'objectiu de millorar la seguretat i de facilitar la posterior administració del sistema implantat.

10.1 Documentació de la xarxa.

Primerament se procedirà a realitzar la documentació de la xarxa del centre. Aquesta és pràcticament inexistente actualment i necessita d'una organització i esquematització adequades. Amb la posterior introducció del servidor proxy, l'esquema es veurà modificat. Aquesta primera tasca es pot subdividir en els següents punts:

- Anotació de les direccions IP fixes dels diferents servidors existents en la xarxa.
- Realització de l'esquema de l'estructura lògica de la xarxa.
- Elaboració de l'esquema de l'estructura física de la xarxa.

És important completar una primera versió de la documentació de la xarxa abans de continuar amb la següent tasca del projecte, ja que ajudarà a la implementació correcta dels diferents serveis. De tota manera, aquesta documentació podrà ser modificada i ampliada en les posteriors tasques, obtenint una versió final de la mateixa al moment de finalitzar el projecte.

10.2 Configuració d'un servidor proxy.

En aquest apartat es configurarà un servidor intermediari amb sistema operatiu **pfSense**. Aquest servidor proxy realitzarà les funcions d'encaminament i **NAT**, creant una segona xarxa interna on es situaran inicialment els equips amb connexió sense fil. A més es configuraran les regles del tallafoc necessàries per a la connexió d'aquesta segona xarxa amb l'exterior.

El procés de instal·lació, configuració i proves es realitzaran en entorns virtualitzats, amb l'objectiu de minimitzar l'impacte en el funcionament diari de la xarxa. Totes aquestes tasques es realitzaran amb un ordinador personal aïllat de la xarxa del centre. El programa de virtualització triat serà **VirtualBox**, sistema molt còmode en la realització d'entorns de pràctiques.

Les tasques descrites als següents apartats també es realitzaran dins d'aquest entorn de proves.

10.3 Optimització dels recursos de xarxa.

A aquest apartat es configurarà l'anterior servidor per a millorar les prestacions de la xarxa. Molts dels usuaris de la xarxa, majoritàriament amb equips de connexions sense fils, fan un ús inadequat i excessiu de la mateixa. Per tant és necessari per una banda optimitzar les connexions i d'altra limitar l'ús dels recursos de la xarxa per part dels usuaris. Els punts a realitzar en aquesta tasca serien:

- Configuració d'un sistema de memòria cau.
- Configuració d'un sistema de repart d'ús de la xarxa **QoS**. Es plantejarà l'establiment de quotes d'amplària de banda entre els usuaris.
- Implantació d'un sistema de portal captiu, la configuració de la qual serà realitzada en els següent apartat del projecte.

10.4 Sistema RADIUS.

En aquest apartat es completarà la configuració del sistema de portal captiu, instaurant un accés per usuari i contrasenya. Aquest accés es basarà en la configuració d'un servidor **RADIUS**. **FreeRadius** serà el sistema utilitzat, disponible per a la seua instal·lació en **pfSense**.

Aquest sistema d'accés permetrà una major seguretat en l'accés a la xarxa sense fil del centre, ja que en el moment depèn només d'una contrasenya mestra **WPA2**.

En primera instància es realitzaran proves per a comprovar el funcionament del servidor **RADIUS**, utilitzant usuaris i contrasenyes introduïdes en el servidor de manera manual. És en el següent apartat on es contemplarà la interoperabilitat entre aquest sistema i el servidor **LDAP** ja implantat en el centre.

10.5 Interconnexió amb serveis LDAP.

Actualment existeix un servidor **LDAP** al centre que gestiona els usuaris de xarxa, l'accés al servidor d'impressió i a les seues carpetes personals i compartides. Aquest servidor **LDAP** ha sigut implementat per una empresa externa al centre. Per aquest motiu els administradors de la xarxa no poden accedir a la configuració del servidor.

En aquest apartat es contempla la interconnexió del servidor **LDAP** amb el servidor **RADIUS** implantat a l'anterior apartat. D'aquesta manera els usuaris de la xarxa sense fil podran accedir als serveis de connectivitat, carpetes de xarxa i impressió, amb un únic usuari i contrasenya.

És possible que per a dur a terme aquesta tasca siga necessària la col·laboració amb l'empresa externa que controla el servidor **LDAP**.

10.6 Monitorització del trànsit i estat dels equips de la xarxa.

La monitorització del trànsit de la xarxa es pot realitzar en distints programes. **pfSense** inclou paquets que permeten un control de l'estat del trànsit de la xarxa. S'estudiarà en aquest punt si aquestes eines compleixen amb els requisits del centre o si es decideix per instal·lar alguna altra eina.

Així mateix, resulta interessant dur un control sobre l'estat dels principals equips de la xarxa. Per a dur a terme aquesta tasca s'instal·larà un servidor i distints clients **Icinga**. Com ja s'ha comentat anteriorment hi han servidors on els administradors de la xarxa no tenen control. Per tant, només es realitzarà aquesta tasca als ordinadors amb drets d'administració.

El servidor **Icinga** serà configurat a una màquina virtual en l'entorn privat de proves gestionat amb **VirtualBox**. **Icinga** s'instal·larà a un SO **Ubuntu Server**²⁹.

10.7 Virtualització dels serveis i implantació.

Una vegada comprovat el bon funcionament dels serveis configurats es procedirà a la implantació dels mateixos en la xarxa del centre.

Per dur a terme aquesta tasca final s'ha decidit configurar un servidor de virtualització **Proxmox** on estaran les màquines virtuals del proxy i del servidor **Icinga**. Posteriorment serà necessari migrar els serveis configurats de l'entorn de pràctiques al servidor **Proxmox**.

10.8 Comprovació dels serveis i proves.

Per últim es realitzaran les proves pertinents per a comprovar el bon funcionament dels serveis implantats. Aquests serveis han de proporcionar un valor afegit a la xarxa i mai suposaran una disminució en les prestacions de la mateixa.

10.9 Seqüenciació i temporalització de les tasques.

A la figura 3 es detalla la seqüenciació i temporalització de cadascuna de les tasques detallades a l'anterior secció del present document.

²⁹<https://www.ubuntu.com/server>

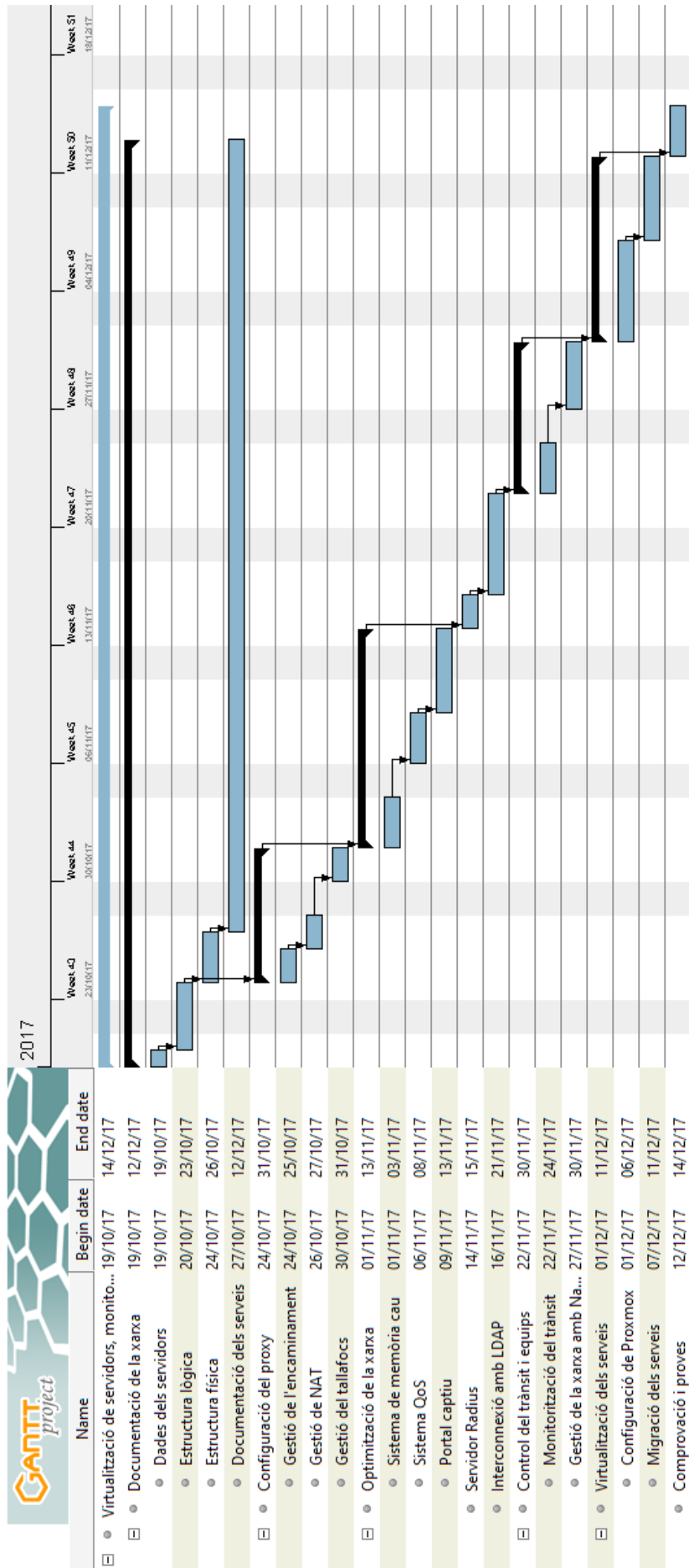


Figura 3: Planificació (1a part)

11 Implementació del projecte.

11.1 Configuració d'un servidor proxy i d'encaminament.

Aquest servei s'ha implementat en una màquina virtual amb el sistema operatiu **pfSense** 2.4. Es dediquen 4 GB de RAM, 2 CPUs i 32 GB d'espai de disc. Aquests recursos poden ampliar-se en un futur si les condicions ho requereixen.

11.2 Paràmetres de xarxa del servidor.

El servidor **pfSense** tindrà 2 interfícies de xarxa. El servidor realitzarà les tasques d'encaminament entre la xarxa original del centre **172.18.45.0/24** i la nova xarxa sense fil **172.19.45.0/24**. La interfície **WAN** de **pfSense** pertany a la xarxa original i tindrà una adreça fixa **172.18.45.253/24**. Per contra, la interfície **LAN** farà de porta d'enllaç als equips de la xarxa sense fil i tindrà una adreça fixa **172.19.45.253/24**.

Per defecte, **pfSense** utilitza la primera interfície (**em0**) connectada com a **WAN** i la segona (**em1**) com a **LAN**. Per aquest motiu es convenient seleccionar correctament el tipus d'interfície de xarxa en el gestor de virtualització *abans* de fer la instal·lació. A l'entorn de pràctiques es configurarà la interfície **LAN** com a de tipus **intern** i la **WAN** com a **NAT Network**. Es crearà per tant a **VirtualBox** una nova xarxa NAT **172.18.45.0/24** que simule la xarxa del centre.

Per contra, ambdós interfícies seran configurades de tipus pont o **bridge** a l'entorn real final.

Per a donar la possibilitat de connexió entre els equips de la xarxa cablejada i els de la xarxa sense fil es configurarà el servei **NAT** en **pfSense**. D'aquesta manera no serà necessari cap configuració extra als equips de la xarxa cablejada.

11.3 Procés d'instal·lació del servidor.

Durant el procés d'instal·lació de **pfSense** es seleccionaran les opcions per defecte del sistema. A les figures 4 i 5 es poden observar alguns dels passos de l'esmentat procés d'instal·lació.

Les credencials per defecte de l'usuari administrador de **pfSense** són:

- **Usuari:** admin
- **Contrasenya:** pfSense

11.4 Configuració inicial del servidor.

11.4.1 Configuració en mode text.

A l'opció 2 del menú de **pfSense** es configuraran la interfície **LAN** (**em1**) amb els següents paràmetres:

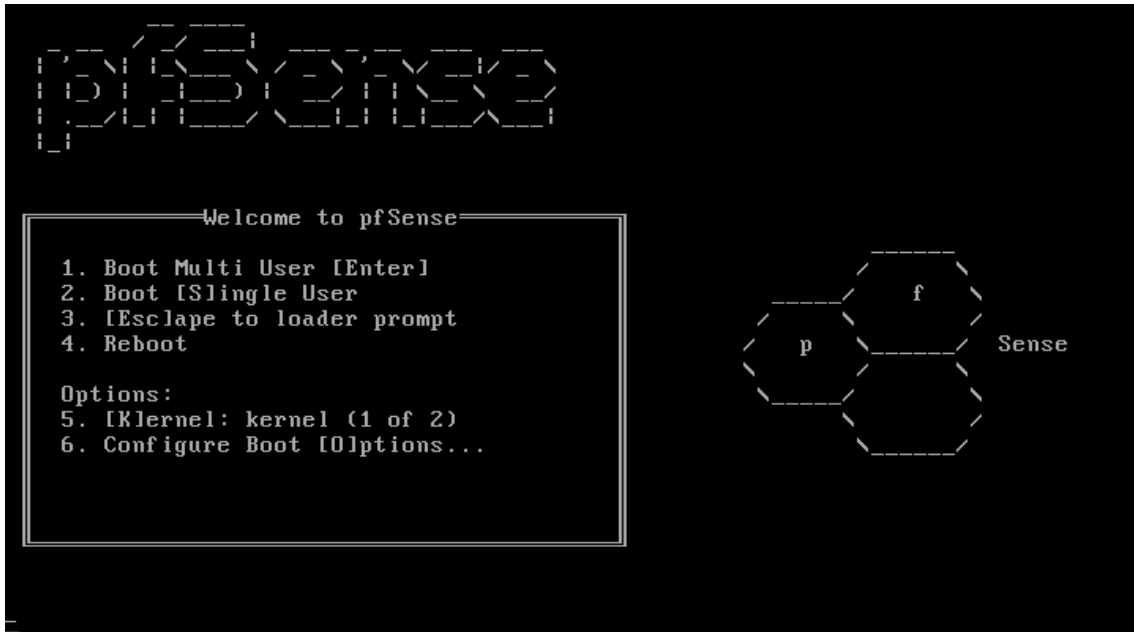


Figura 4: Instal·lació de pfSense (I).

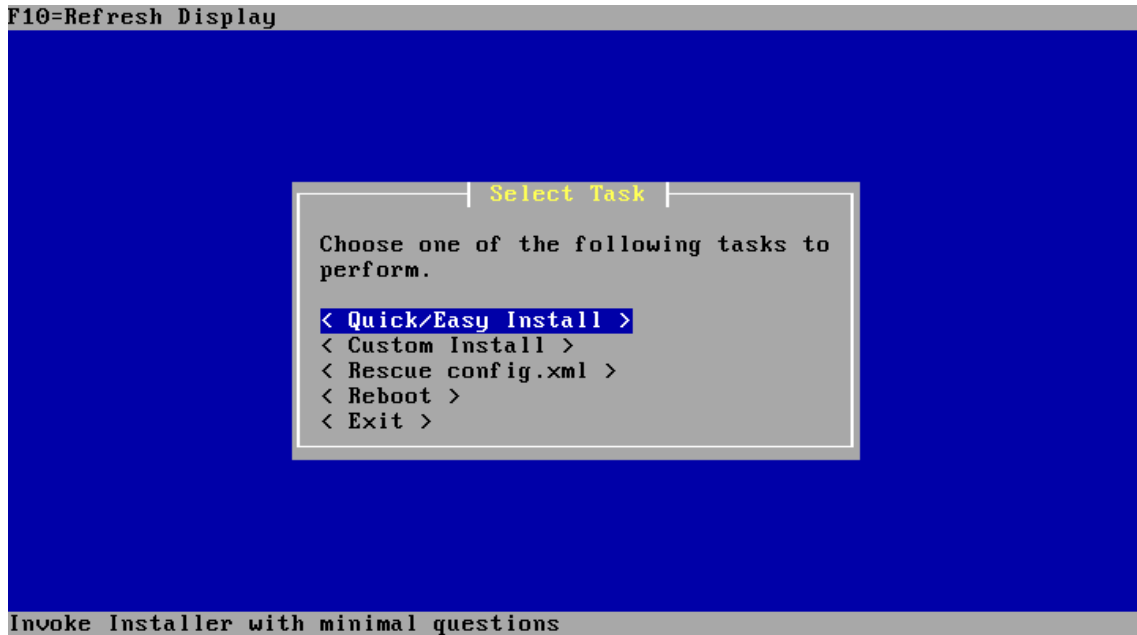


Figura 5: Instal·lació de pfSense (II).

```
FreeBSD/amd64 (pfSense.iestorrevisia) (ttyv0)
pfSense - Netgate Device ID: 2b92e382aa47042ee74e
*** Welcome to pfSense 2.4.2-RELEASE (amd64) on pfSense ***

WIRED (wan)      -> em0          -> v4: 172.18.45.253/24
WIRELESS (lan)  -> em1          -> v4: 172.19.45.253/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Dec  3 16:16:59 ...
pfSense php-fpm1659311: /index.php: Successful login for user 'admin' from: 172.18.45.5
```

Figura 6: Pantalla d'inici pfSense (II).

- IP: 172.19.45.253
- Màscara de xarxa: /24
- IP v6: No
- Servidor DHCP: Actiu
- Interval del servidor DHCP: 172.19.45.1-172.19.45.199
- Configuració d'interfície Web: HTTPS

I la interfície WAN (em1) amb els següents paràmetres:

- IP: 172.18.45.253
- Màscara de xarxa: /24
- Porta d'enllaç: 172.18.45.1
- IP v6: No
- Configuració d'interfície Web: HTTPS

Per últim és convenient activar el servidor **SSH** per a permetre l'accés remot al servidor. Per a realitzar-ho només caldrà triar l'opció 14 del menú.

La figura 6 mostra l'estat de la pantalla del menú una vegada realitzades totes les configuracions anteriors.

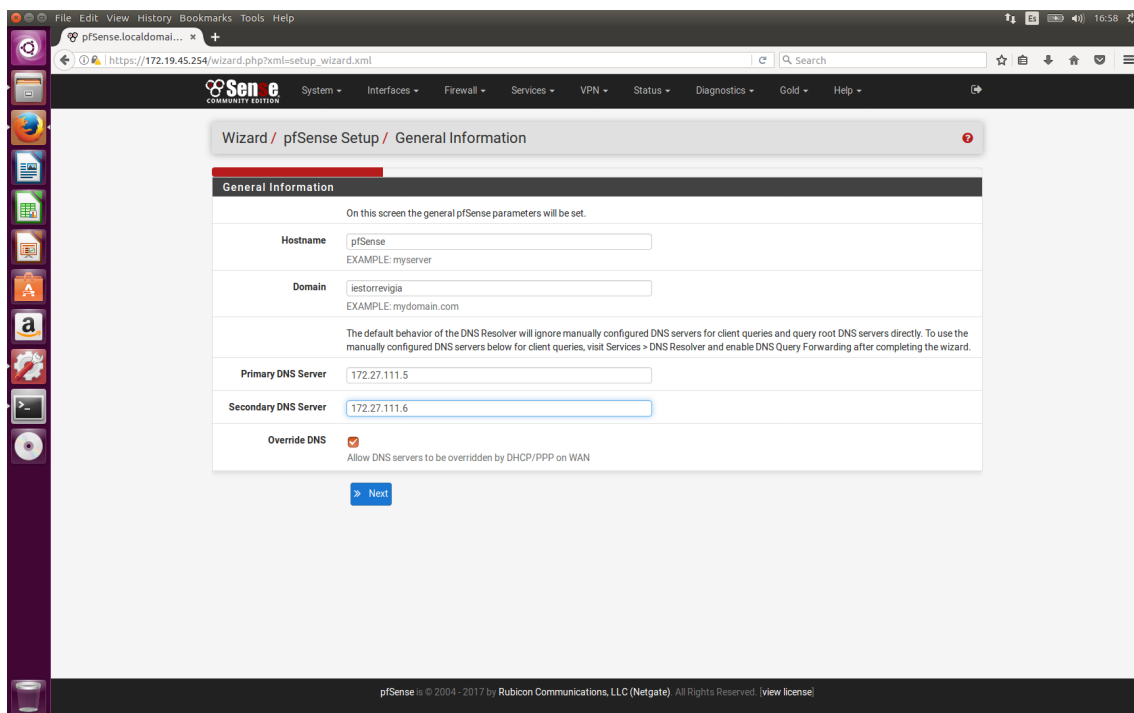


Figura 7: Asistent Web pfSense (I).

11.4.2 Assistent web de configuració.

Per a finalitzar es realitzaran unes últimes configuracions des de la interfície web de **pfSense**. Per a realitzar aquesta configuració s'accedirà des d'una màquina virtual **Ubuntu** client. Serà suficient amb introduir l'adreça **https://172.19.45.253** al navegador web, executar l'assistent i configurar els següents paràmetres, deixant la resta per defecte.

- **Equip:** pfSense
- **Domini:** iestorrevgia
- **Servidor DNS primari:** 172.27.111.5
- **Servidor DNS secundari:** 172.27.111.6
- **No DNS override**
- **Zona horària:** Europe/Madrid
- **Admin credencials:** NouPassword.

La figura 7 mostra un dels passos descrits anteriorment.

11.4.3 Configuració de noms d'interfícies.

Amb l'objectiu de simplificar les posteriors configuracions es canviaran els nom de les interfícies de xarxa. D'aquesta manera les interfícies LAN i WAN tindran com a nom **Wireless** i **Wired**, respectivament. Per a realitzar aquesta configuració s'he accedirà al menú **Interfaces**.

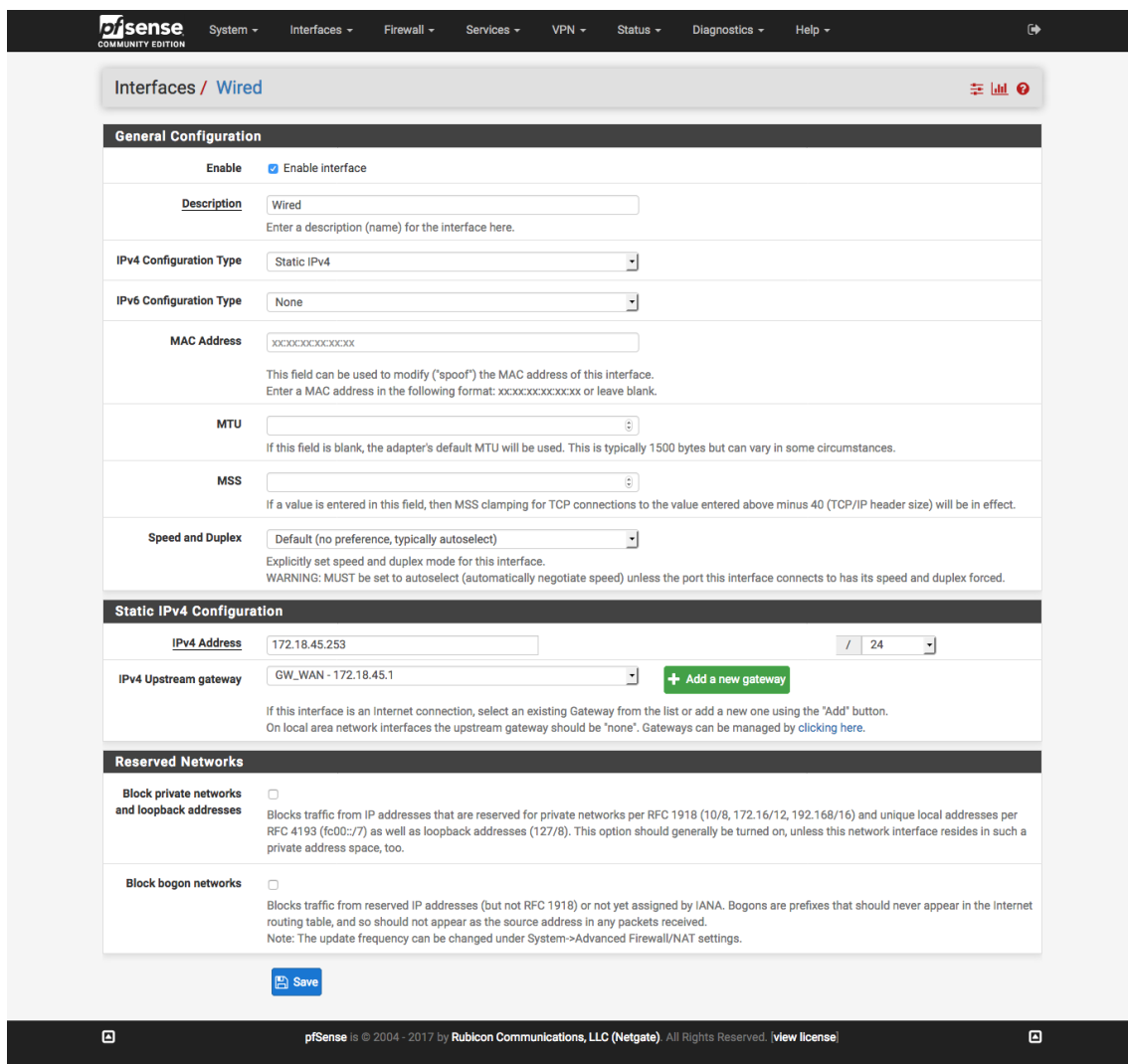


Figura 8: Configuració d'interfície (I).

A més es desactivarà el bloqueig a l'accés al sistema des de la interfície WAN. D'aquesta manera es podrà realitzar les tasques de configuració des de les 2 xarxes. La figura 8 mostra un exemple de la configuració d'una interfície.

11.4.4 Configuració de DHCP i DNS.

El servidor **DHCP** es configurarà anteriorment. En canvi és necessari realitzar canvis perquè els clients de la xarxa **Wireless** disposen dels servidors **DNS** correctes en el moment d'obtenir la configuració de xarxa. Al menú **Services...DNS Resolver...GeneralSettings** s'activarà l'opció **DNS Query Forwarding** (figura 9).

11.5 Configuració del tallafocs.

11.5.1 Configuració d'àlies.

Gràcies a la configuració d'àlies es podran crear regles al tallafocs que afecten a un conjunt de ports i d'equips. La configuració es realitza al menú **Fi-**

[System](#) - [Interfaces](#) - [Firewall](#) - [Services](#) - [VPN](#) - [Status](#) - [Diagnostics](#) - [Help](#)

[Services / DNS Resolver / General Settings](#)

[General Settings](#) [Advanced Settings](#) [Access Lists](#)

General DNS Resolver Options

Enable Enable DNS resolver

Listen Port

The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Network Interfaces

Interface IPs used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

Outgoing Network Interfaces

Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.

System Domain Local Zone Type

The local-zone type used for the pfSense system domain (System | General Setup | Domain). Transparent is the default. Local-Zone type descriptions are available in the unbound.conf(5) manual pages.

DNSSEC Enable DNSSEC support

DNS Query Forwarding Enable Forwarding Mode

If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under [System > General Setup](#) or those obtained via DHCP/PPP on WAN (if DNS Server Override is enabled there).

DHCP Registration Register DHCP leases in the DNS Resolver

If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS Resolver, so that their name can be resolved. The domain in [System > General Setup](#) should also be set to the proper value.

Static DHCP Register DHCP static mappings in the DNS Resolver

If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in [System > General Setup](#) should also be set to the proper value.

Display Custom Options

Host Overrides

Host	Parent domain of host	IP to return for host	Description	Actions
Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.				
<input type="button" value="+ Add"/>				

Domain Overrides

Domain	Lookup Server IP Address	Description	Actions
Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is treated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried.			
<input type="button" value="+ Add"/>			

pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [View license](#)

Figura 9: Configuració de DNS (I).

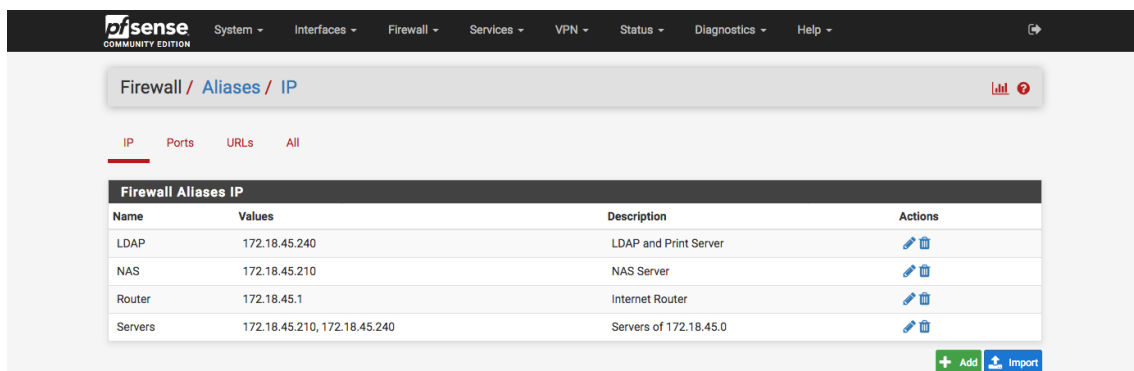


Figura 10: Configuració d'àlies (I).

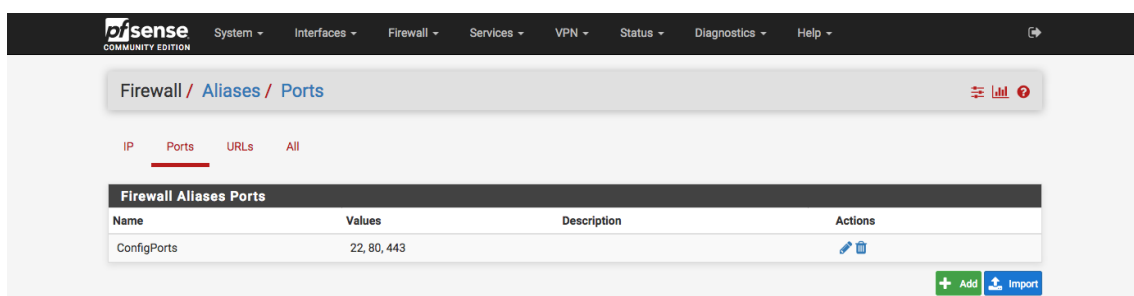


Figura 11: Configuració d'àlies (II).

rewall...Aliases. Els conjunt de ports definit contempla l'accés al sistema per **SSH**, **HTTP** i **HTTPS**. Les figures 10 i 11 mostren els equips servidors i els ports definits com a àlies.

11.5.2 Encaminament i NAT.

L'encaminament es realitzarà mitjançant **NAT**. D'aquesta manera no serà necessari configuracions extres d'encaminament als equips de la xarxa **Wired**. La configuració es realitzarà al menú **Firewall...NAT...Outbound** tal i com mostra la figura 12.

11.5.3 Tallafocs.

Les regles del tallafocs són les següents:

- Impedir l'accés des de la xarxa **Wired** a la xarxa **Wireless**.
- Permetre l'accés per **SSH**, **HTTP** i **HTTPS** a **pfSense**, des de les 2 xarxes.
- Permetre l'accés als servidors de la xarxa **Wired** des d'els equips de la xarxa **Wireless**.
- Impedir qualsevol altre accés des de la xarxa **Wireless** a la xarxa **Wired**.
- Permetre la resta de les connexions des de la xarxa **Wireless**. Aquesta regla permet l'accés dels equips de la xarxa **Wireless** a Internet.

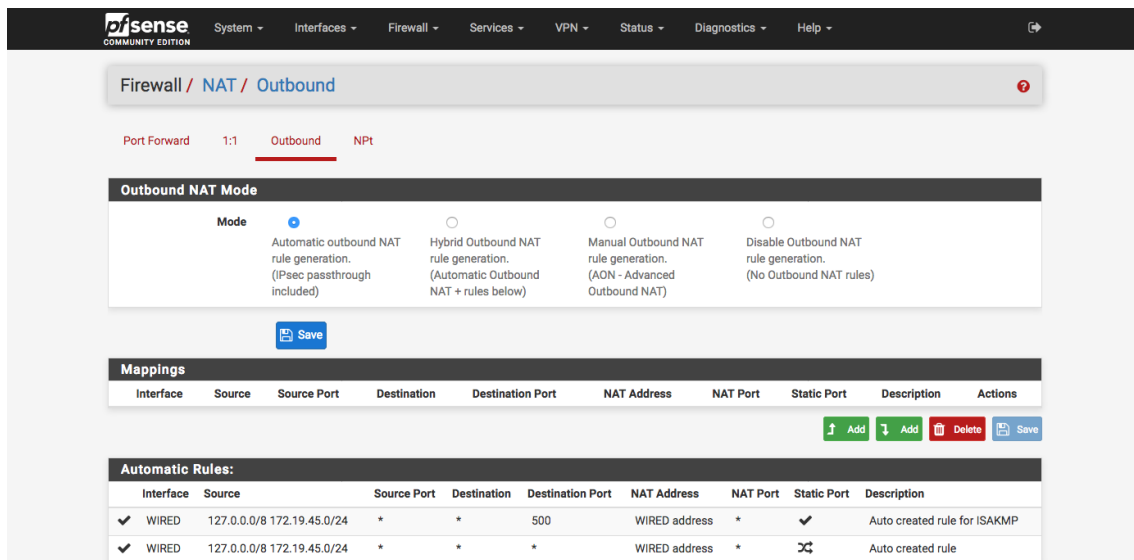


Figura 12: Configuració de NAT (I).

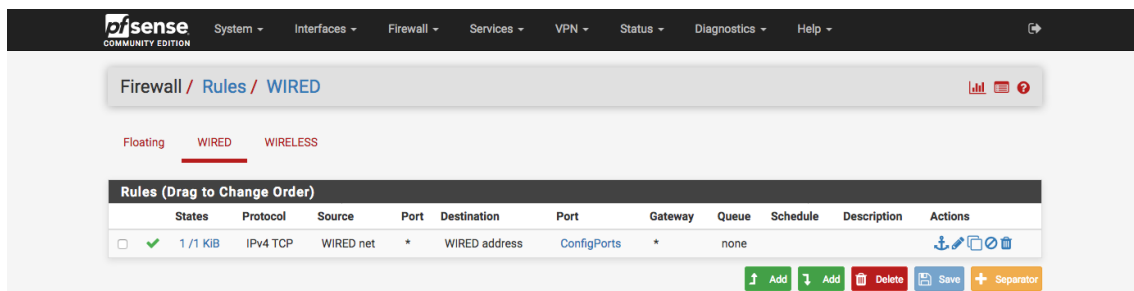


Figura 13: Configuració del tallafocs (I).

Les regles es defineixen al menú **Firewall...Rules** i les figures 13 i 14 mostren la seua configuració.

11.5.4 Limitadors d'amplària de banda.

El firewall de **pfSense** permet la configuració de distintes maneres d'establir sistemes **QoS**. S'ha escollit l'establiment de límits flexibles, els quals limiten el total de l'amplària de banda entre els clients existents en cada moment. El menú que permet la creació d'aquests límits es troba a **Firewall...Traffic Shapers...Limiters**.

Es crearan 4 canonades (*pipes*), 2 per a les connexions de pujada (**UploadIntranet**, **Upload**) i altres 2 per a les de baixada (**DownloadIntranet**, **Download**). Ací s'establirà l'amplària de banda diferenciada per a les connexions entre equips del centre i a Internet. És convenient deixar un marge d'amplària de banda disponible per a tasques importants d'administració de la xarxa. Les figures 15 i 16 mostra la configuració de dos d'aquestes canonades.

Cada canonada tindrà associada una cua (figura 17). Són aquestes cues les que posteriorment s'afegiran a les regles del tallafocs, dins de les opcions avançades d'edició (figura 18). La regla que controla l'accés als servidors tindrà associades les

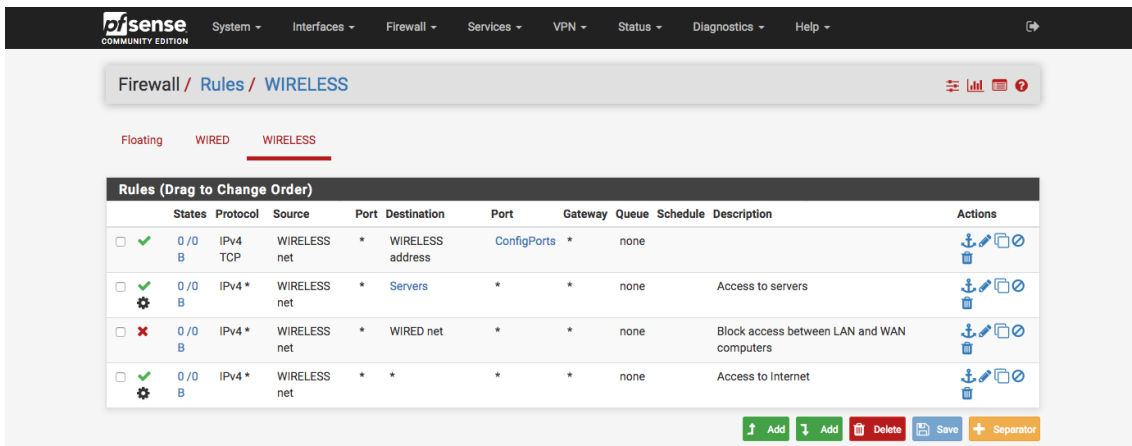


Figura 14: Configuració del tallafocs (II).

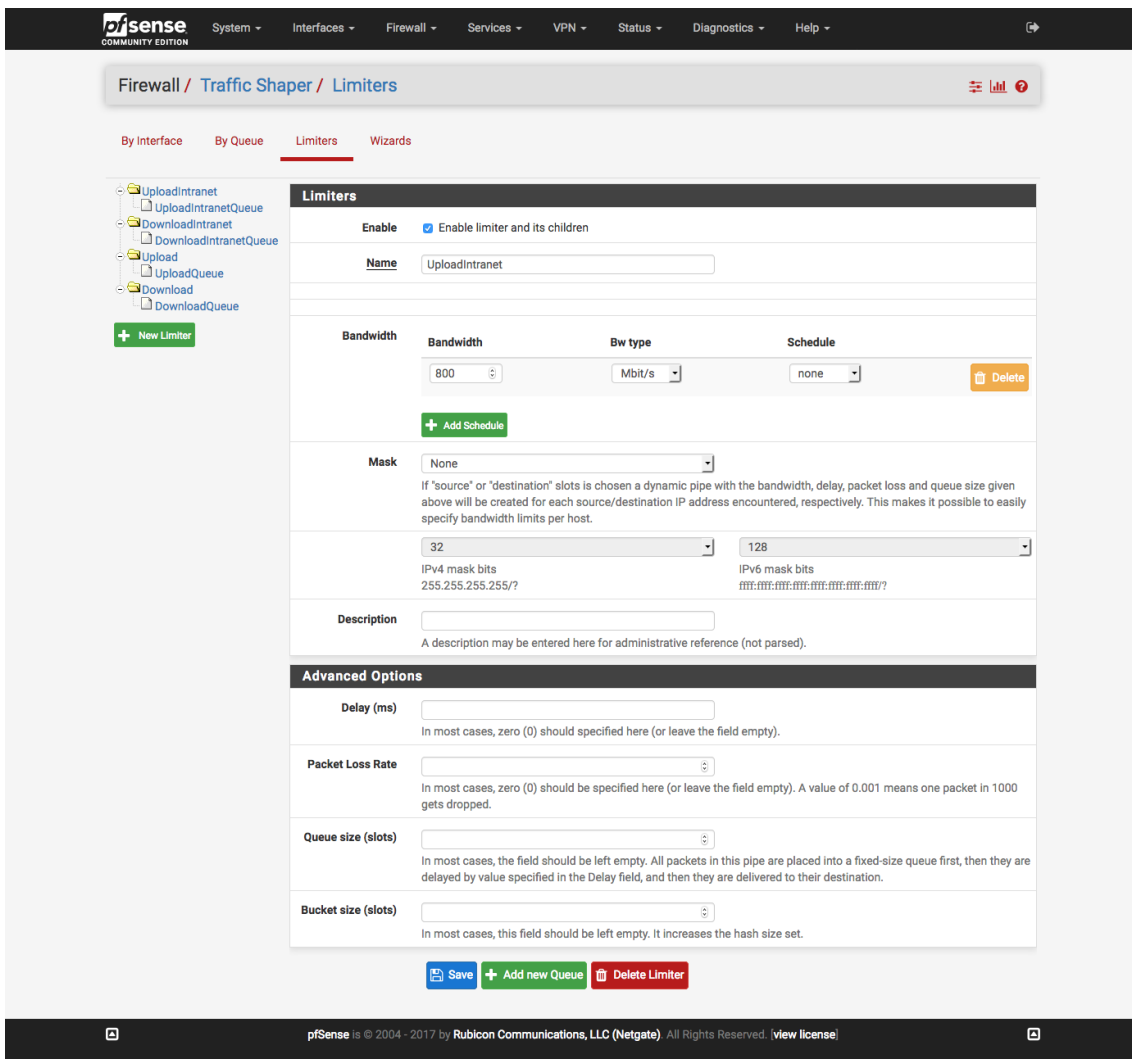



Figura 15: Configuració de limitadors (I).


 System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

Firewall / Traffic Shaper / Limiters

By Interface | By Queue | **Limiters** | Wizards

- UploadIntranet
 - UploadIntranetQueue
- DownloadIntranet
 - DownloadIntranetQueue
- Upload
 - UploadQueue
- Download
 - DownloadQueue

+ New Limiter

Limiters

Enable Enable limiter and its children

Name

Bandwidth	Bw type	Schedule	
200	Mbit/s	none	Delete
+ Add Schedule			

Mask

If "source" or "destination" slots is chosen a dynamic pipe with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host.

32	128
IPv4 mask bits 255.255.255.255/?	IPv6 mask bits fff:fff:fff:fff:fff:fff:fff:fff/?

Description

A description may be entered here for administrative reference (not parsed).

Advanced Options

Delay (ms)

In most cases, zero (0) should be specified here (or leave the field empty).

Packet Loss Rate

In most cases, zero (0) should be specified here (or leave the field empty). A value of 0.001 means one packet in 1000 gets dropped.

Queue size (slots)

In most cases, the field should be left empty. All packets in this pipe are placed into a fixed-size queue first, then they are delayed by value specified in the Delay field, and then they are delivered to their destination.

Bucket size (slots)

In most cases, this field should be left empty. It increases the hash size set.

Save
+ Add new Queue
Delete Limiter

pfsense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate) All Rights Reserved. [View license](#)

Figura 16: Configuració de limitadors (II).

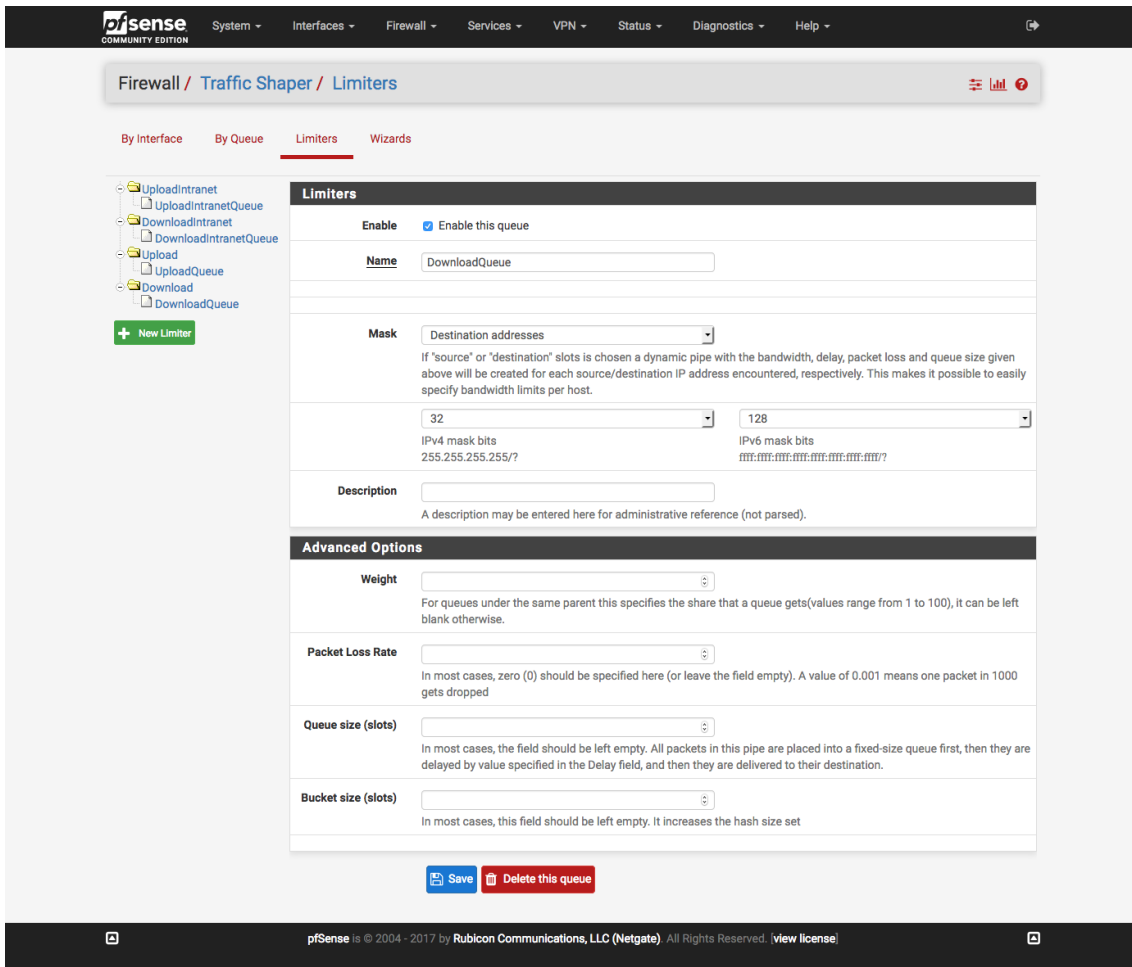


Figura 17: Configuració de limitadors (III).

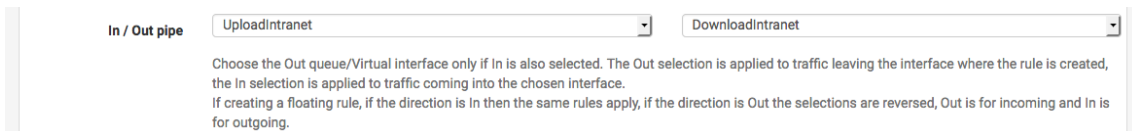


Figura 18: Configuració de limitadors (IV).

cues **UploadIntranet** i **DownloadIntranet**. La regla d'accés a Internet tindrà les cues **Upload** i **Download**.

11.6 Servidor proxy.

pfSense permet la instal·lació del paquet **squid** i així implementar un servidor proxy. Per a la instal·lació de nous paquets s'accedeix al menú **System...Package Manager...Available Packages**. Després de la instal·lació del paquet es procedeix a la configuració del servei al menú **Services...Squid Proxy Server**. Aquest proxy filtra tot el tràfic **HTTP**. En canvi no s'ha efectuat el filtrat dels continguts **HTTPS** ja que es necessitaria la configuració manual dels equips clients de la xarxa sense fil.

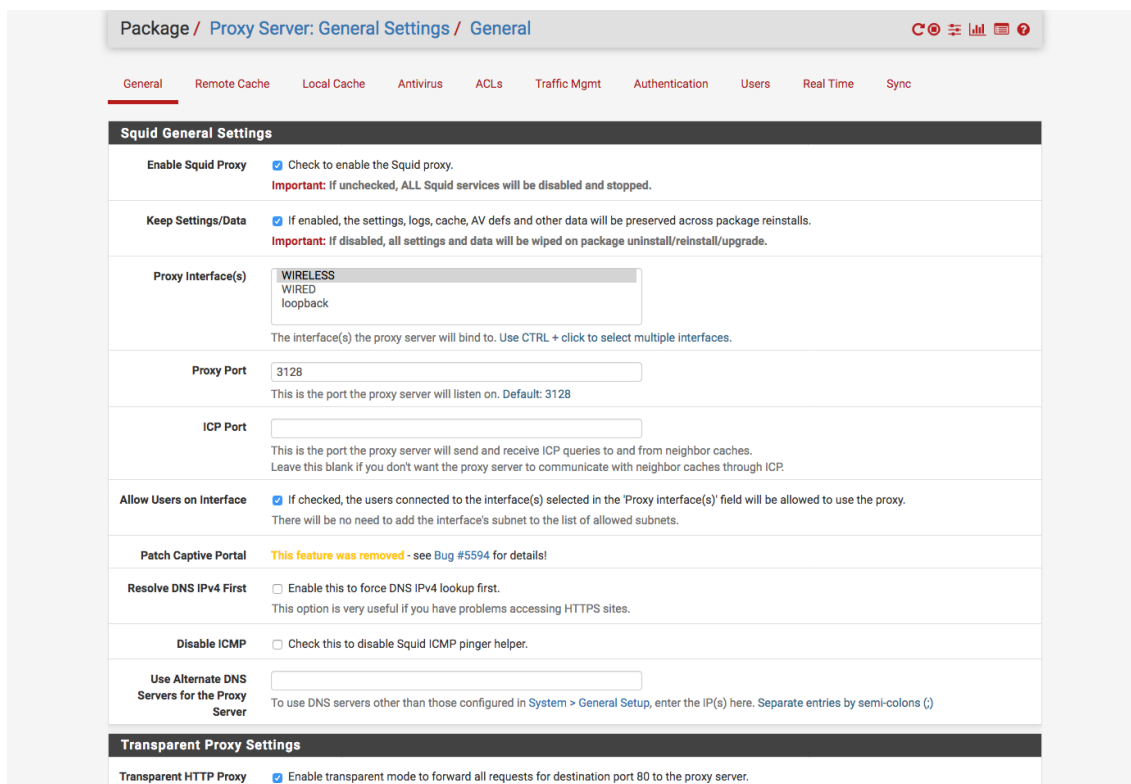


Figura 19: Configuració de proxy (I).

A més també s'activa un sistema antivirus **ClamAV**³⁰ integrat en **Squid**. La configuració del proxy es mostra a les figures 19 i 20.

11.7 Servidor RADIUS.

D'igual manera que amb **Squid**, el servidor **FreeRADIUS** pot ser instal·lat des de la secció **System...Package Manager...Available Packages**.

De **FreeRADIUS** es necessita configurar els següents elements:

- NAS/Clients (figura 21): s'especifiquen els clients que poden consultar al servidor **RADIUS**. En aquest cas s'indica la direcció del propi sistema **pfSense**, ja que serà el portal captiu qui realitzi les consultes.
- Interfaces (figura 22): s'activaran totes les interfícies del sistema per al servidor **RADIUS**.
- LDAP (figura 23): s'indicarà el servidor i les dades de l'usuari **LDAP** amb permisos de lectura.

11.8 Portal captiu.

El portal captiu es configura al menú **Services...Captive Portal**. Només caldrà activar el portal, habilitar l'accés per **HTTPS** (figura 24) i associar l'autenticació per **RADIUS** (figura 25).

³⁰<https://www.clamav.net/>

Package / Proxy Server: Antivirus / Antivirus

General Remote Cache Local Cache **Antivirus** ACLs Traffic Mgmt Authentication Users Real Time Sync

ClamAV Anti-Virus Integration Using C-ICAP

Enable AV Enable Squid antivirus check using ClamAV.

Client Forward Options
 Select what client info to forward to ClamAV.

Enable Manual Configuration
Warning: Only enable this if you know what you are doing.
 When enabled, the options below no longer have any effect. You must edit the configuration files directly in the 'Advanced Features'. After enabling manual configuration, click the button below **once** to load default configuration files. To disable manual configuration again, select 'disabled' and click 'Save'.

Redirect URL
 When a virus is found then redirect the user to this URL. Example: http://proxy.example.com/blocked.html
 Leave empty to use the default Squid/pfSense WebGUI URL.

Google Safe Browsing Enables Google Safe Browsing support.
 Google Safe Browsing database includes information about websites that may be phishing sites or possible sources of malware.
Warning: This option consumes significant amount of RAM.

Exclude Audio/Video Streams This option disables antivirus scanning of streamed video and audio.

ClamAV Database Update
 Optionally, you can schedule ClamAV definitions updates via cron. Select the desired frequency here.
Important: Set to 'every 1 hour' if you want to use Google Safe Browsing feature.
 Click the button below **once** to force the update of AV databases immediately. **Note: This will take a while.** Check freshclam log on the 'Real Time' tab for progress information.

Regional ClamAV Database Update Mirror
 Select a regional database mirror. Note: The default ClamAV database mirror performs extremely slow.
It is strongly recommended to choose a mirror here and/or configure your own mirrors manually below.

Figura 20: Configuració de proxy (II).

Package / FreeRADIUS: Clients / NAS / Clients

Users MACs **NAS / Clients** Interfaces Settings EAP SQL LDAP View config XMLRPC Sync

Client IP Address	Client IP Version	Client Shortname	Client Protocol	Client Type	Require Message Authenticator	Max Connections	Description
127.0.0.1	ipaddr	admin	udp	other	no	16	<input type="button" value="edit"/> <input type="button" value="delete"/>
172.19.45.253	ipaddr	admin	udp	other	no	16	<input type="button" value="edit"/> <input type="button" value="delete"/>

Figura 21: Configuració de servidor RADIUS (I).

Package / FreeRADIUS: Interfaces / Interfaces

Users MACs NAS / Clients **Interfaces** Settings EAP SQL LDAP View config XMLRPC Sync

Interface IP Address	Port	Interface Type	IP Version	Description
*	1812	auth	ipaddr	<input type="button" value="edit"/> <input type="button" value="delete"/>

Figura 22: Configuració de servidor RADIUS (II).

Package / FreeRADIUS: LDAP / LDAP ?

Users MACs NAS / Clients Interfaces Settings EAP SQL LDAP View config XMLRPC Sync

Enable LDAP Support - Server 1

LDAP Authorization Support Enable LDAP For Authorization
Enables LDAP in the authorize section. The ldap module will set Auth-Type to LDAP if it has not already been set. (Default: Disabled)

LDAP Authentication Support Enable LDAP For Authentication
Enables LDAP in the authenticate section. Note that this means "check plain-text password against the LDAP database", which means that EAP won't work, as it does not supply a plain-text password.

General Configuration - Server 1

Server Address
LDAP server FQDN or IP address. (Example: ldap.example.com)

Server Port
LDAP server port. (Default: 389)

Identity
LDAP ID for authentication. (Example: cn=admin,o=My Company Ltd,c=US)

Password
LDAP password for authentication. (Default: mypass)

Base DN
Base DN for LDAP search. (Example: o=My Company Ltd,c=US)

Filter
LDAP search filter. Default: `(uid=%{%Stripped-User-Name};-~%{User-Name})`

Base Filter
Default: `(objectclass=radiusprofile)`

Figura 23: Configuració de servidor RADIUS (III).

HTTPS Options

Login Enable HTTPS login
When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

HTTPS server name
This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in the certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.

SSL Certificate
If no certificates are defined, one may be defined here: [System > Cert. Manager](#)

HTTPS Forwards Disable HTTPS Forwards
If this option is set, attempts to connect to SSL/HTTPS (Port 443) sites will not be forwarded to the captive portal. This prevents certificate errors from being presented to the user even if HTTPS logins are enabled. Users must attempt a connection to an HTTP (Port 80) site to get forwarded to the captive portal. If HTTPS logins are enabled, the user will be redirected to the HTTPS login page.

Figura 24: Configuració de portal captiu (I).

Authentication

Authentication Method No Authentication Local User Manager / Vouchers RADIUS Authentication
Select an Authentication Method to use for this zone. One method must be selected.

RADIUS protocol PAP CHAP-MD5 MSCHAPV1 MSCHAPV2

Primary Authentication Source

Primary RADIUS server

Secondary RADIUS server
IP address of the RADIUS server to authenticate against. RADIUS port. Leave blank for default (1812) RADIUS shared secret. Leave blank to not use a shared secret (not recommended)

Figura 25: Configuració de portal captiu (II).

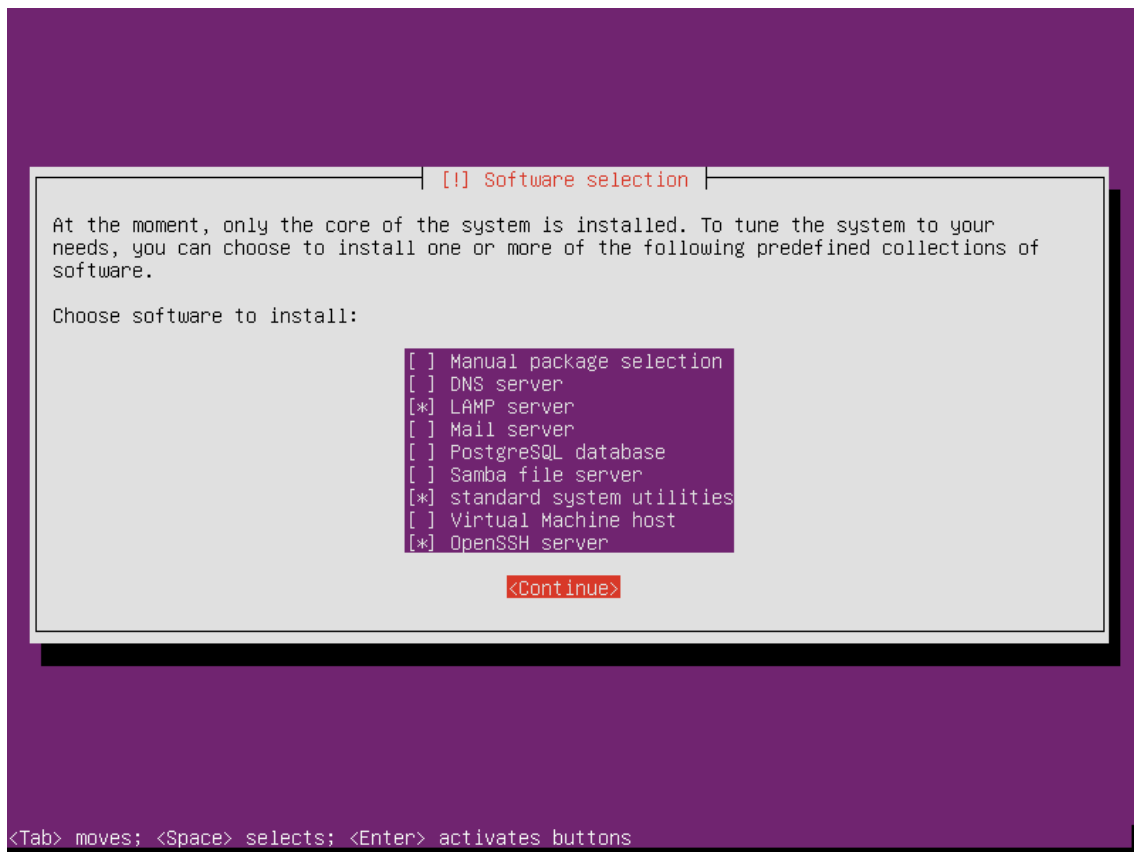


Figura 26: Instal·lació d'Ubuntu Server (I).

11.9 Monitorització del trànsit i estat dels equips de la xarxa.

La monitorització del trànsit es realitza al sistema **pfSense**. En canvi la comprovació dels equips principals de la xarxa es realitza a una màquina virtual **Ubuntu Server 16.04** amb el servei **Icinga**. Aquesta última màquina virtual disposa de 2 GB de RAM, 2 CPUs i 32 GB d'espai de disc. Aquests recursos poden ampliar-se en un futur si les condicions ho requereixen.

La instal·lació d'**Ubuntu Server** permet la selecció del programari necessari per a crear una plataforma **LAMP (Linux, Apache, MySQL i PHP)** (figura 26).

La màquina disposa de 2 interfícies de xarxa, cadascuna pertany a una xarxa distinta. Les dades de xarxa són les següents i es configuren a l'arxiu `/etc/network/interfaces` (figura 27):

- Interfície 1: 172.18.45.252/24, Gateway: 172.18.45.1 DNS: 172.27.111.5, 172.27.111.6
- Interfície 2: 172.19.45.252/24

Serà necessari la instal·lació dels paquets:

```
$ sudo apt-get install icinga2 nagios-plugins vim-icinga2
$ sudo apt-get install icinga2-ido-mysql icingaweb2
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
address 172.18.45.252
netmask 255.255.255.0
gateway 172.18.45.1
dns-nameservers 172.27.111.5 172.27.111.6

auto enp1s3
iface enp1s3 inet static
address 172.19.45.252
netmask 255.255.255.0
```

Figura 27: Configuració d'Ubuntu Server (I).

El següents comandaments configura l'emmagatzematge de les dades d'Icinga i activa mòduls necessaris per a l'administració.

```
$ sudo icinga2 feature enable ido-mysql
$ sudo icinga2 feature enable command
$ sudo systemctl restart icinga2
```

El següents comandaments permeten l'accés al port **HTTP** per a l'administració web i 5665 per a l'administració d'**Icinga**.

```
$ sudo iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
$ sudo iptables -A INPUT -p tcp -m tcp --dport 5665 -j ACCEPT
$ sudo iptables -save
```

El primer comandament afegeix l'usuari **nagios** al grup **www-data**. El segon genera un ticket necessari per al funcionament de la interfície web.

```
$ sudo usermod -a -G nagios www-data
$ sudo icinga2 pki ticket --cn 'pfSense.iestorrevigia'
```

Es finalitza la configuració d'**Icinga** amb el següent comandament:

```
$ sudo icinga2 api setup
```


Welcome to the configuration of Icinga Web 2!

This wizard will guide you through the configuration of Icinga Web 2. Once completed and successfully finished you are able to log in and to explore all the new and stunning features!

Setup Token ⓘ

Next

Generating a New Setup Token

To run this wizard a user needs to authenticate using a token which is usually provided to him by an administrator who'd followed the instructions below.

In any case, make sure that all of the following applies to your environment:

- A system group called "icingaweb2" exists
- The user "www-data" is a member of the system group "icingaweb2"

```
addgroup --system icingaweb2;
usermod -s -G icingaweb2 www-data;
```

If you've got the IcingaCLI installed you can do the following:

```
icingacli setup config directory --group icingaweb2;
icingacli setup token create;
```

In case the IcingaCLI is missing you can create the token manually:

```
su www-data -c "mkdir -m 2770 /etc/icingaweb2; chgrp icingaweb2 /etc/icingaweb2; head -c 12 /dev/urandom | base64 | tee /etc/icingaweb2
/setup.token; chmod 0660 /etc/icingaweb2/setup.token;";
```

Please see the Icinga Web 2 documentation for an extensive description on how to access and use this wizard.

Figura 28: Configuració d' Icinga Web (I).

A continuació resta iniciar la interfície web de **Icinga** (figura 28). Serà necessari editar l'arxiu `/etc/php.ini` amb la zona horària, així com instal·lar una sèrie de paquets extra (figura 29) i seleccionar com a backend d'autenticació un sistema de base de dades (figura 30).

```
$ sudo apt-get install php-intl php-xml php-imagick
$ sudo systemctl restart apache2
```

Per últim descarregarem i instal·larem el complement **NagVis** que permet la creació de gràfics d'estat dins d'**Icinga**.

```
$ sudo apt-get install graphviz
$ cd /usr/share/icingaweb2/modules
$ sudo git clone https://github.com/Icinga/icingaweb2-module-nagvis
$ sudo icingacli module enable nagvis
$ sudo systemctl restart apache2
$ sudo systemctl restart icinga
```

NagVis presenta un error en l'execució en sistemes **Ubuntu Server 16.04**. Es soluciona editant l'arxiu `/usr/share/nagvis/share/server/core/classes/objects/-NagiosService.php` (línea 103) i `/usr/share/nagvis/share/server/core/classes/objects/NagVisMapObj.php` (línea 247). A ambdós fitxer es substituirà les línies per aquesta:

```
function queueState($_unused_flag=true) {
```

Requirement	Description	Status
PHP Version	Running Icinga Web 2 requires PHP version 5.3.2. Advanced features like the built-in web server require PHP version 5.4.	You are running PHP version 7.0.22-0ubuntu0.16.04.1.
Default Timezone	It is required that a default timezone has been set using date.timezone in /etc/php/7.0/apache2/php.ini.	The PHP config 'date.timezone' is set to "Europa/Madrid".
Linux Platform	Icinga Web 2 is developed for and tested on Linux. While we cannot guarantee they will, other platforms may also perform as well.	You are running PHP on a Linux system.
PHP Module: OpenSSL	The PHP module for OpenSSL is required to generate cryptographically safe password salts.	The PHP module OpenSSL is available.
PHP Module: JSON	The JSON module for PHP is required for various export functionalities as well as APIs.	The PHP module JSON is available.
PHP Module: LDAP	If you'd like to authenticate users using LDAP the corresponding PHP module is required.	The PHP module LDAP is available.
PHP Module: INTL	If you want your users to benefit from language, timezone and date/time format negotiation, the INTL module for PHP is required.	The PHP module INTL is available.
PHP Module: DOM	To be able to export views and reports to PDF, the DOM module for PHP is required.	The PHP module DOM is available.
PHP Module: GD	In case you want views being exported to PDF, you'll need the GD extension for PHP.	The PHP module GD is available.
PHP Module: Imagick	In case you want graphs being exported to PDF as well, you'll need the ImageMagick extension for PHP.	The PHP module Imagick is available.
PHP Module: PDO-MySQL	To store users or preferences in a MySQL database the PDO-MySQL module for PHP is required.	The PHP module PDO-MySQL is available.
Zend database adapter for MySQL	The Zend database adapter for MySQL is required to access a MySQL database.	The Zend database adapter for MySQL is available.
PHP Module: PDO-PostgreSQL	To store users or preferences in a PostgreSQL database the PDO-PostgreSQL module for PHP is required.	The PHP module PDO-PostgreSQL is missing.

Figura 29: Configuració d'Icinga Web (II).

Authentication

Please choose how you want to authenticate when accessing Icinga Web 2. Configuring backend specific details follows in a later step.

Authentication Type:

[Back](#) [Next](#)

Figura 30: Configuració d'Icinga Web (III).

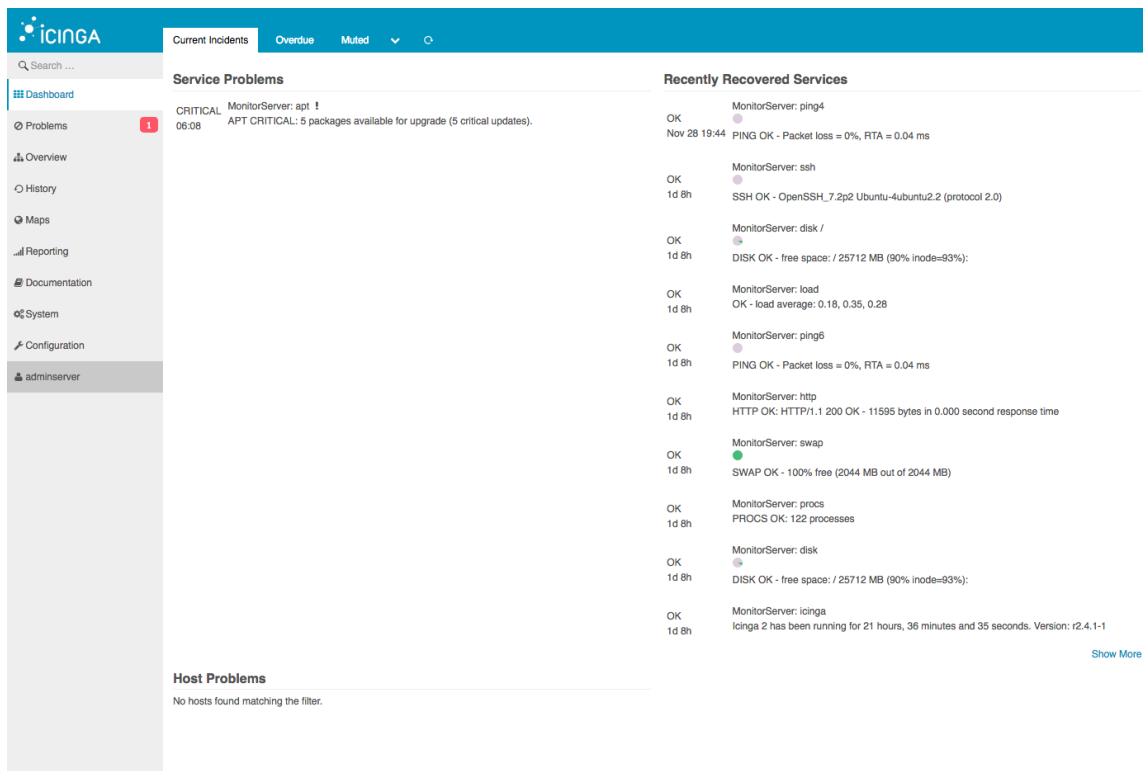


Figura 31: Configuració d'Icinga Web (IV).

Finalment es pot accedir tant a la **Icinga Web** (figura 31) com al complement **NagVis** (figura 32).

11.10 Virtualització dels serveis.

En una primera instància les proves es realitzaren a màquines virtuals dins del programari **VirtualBox**. Posteriorment es migraren els sistemes al hipervisor **Proxmox**.

La instal·lació de Proxmox suposa la destrucció de tot el contingut del disc dur que s'especifique, ja que realitza automàticament la partició d'aquest disc. Serà necessari a més indicar les dades de xarxa següents:

- Nom d'equip: proxmox.iestorrevigia
- IP: 172.18.45.254/24
- Gateway: 172.18.45.1
- DNS: 172.27.111.5, 172.27.111.6

Al finalitzar la instal·lació es pot accedir a la interfície web de **Proxmox** des de la direcció <https://172.18.45.254:8006> (figura 33).

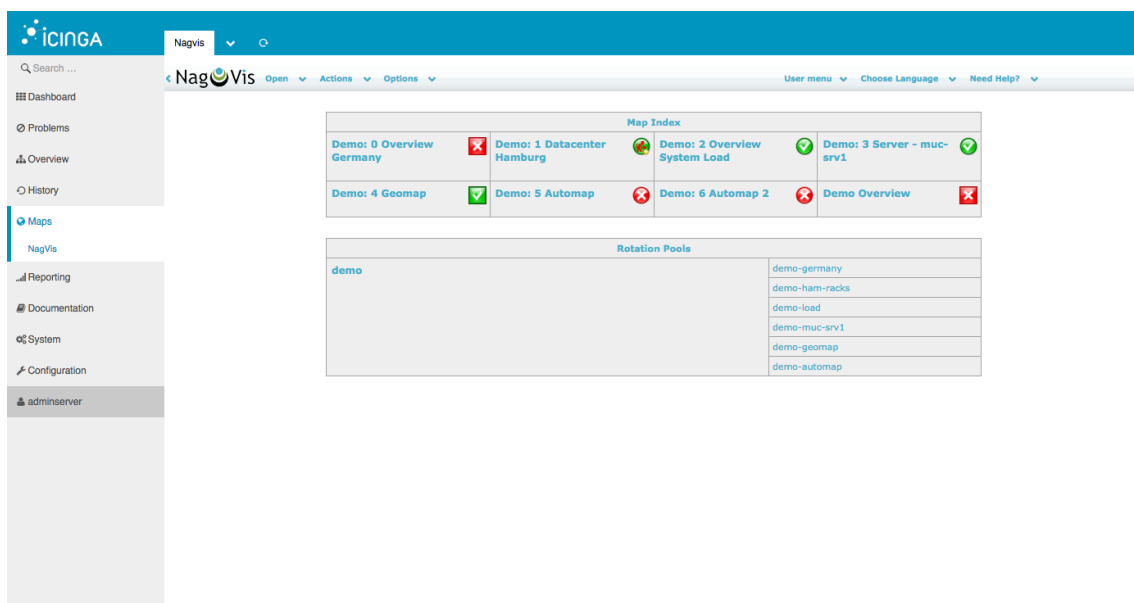


Figura 32: Configuració d'Icinga Web (V).

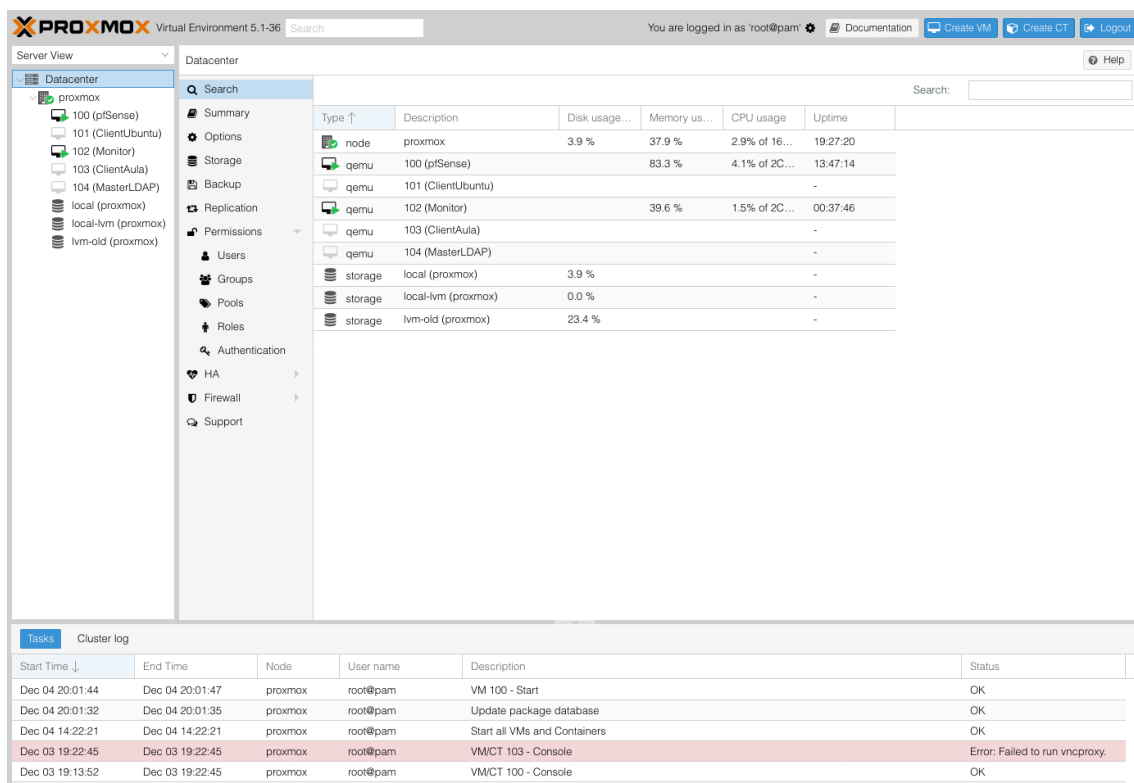


Figura 33: Configuració de Proxmox (I).

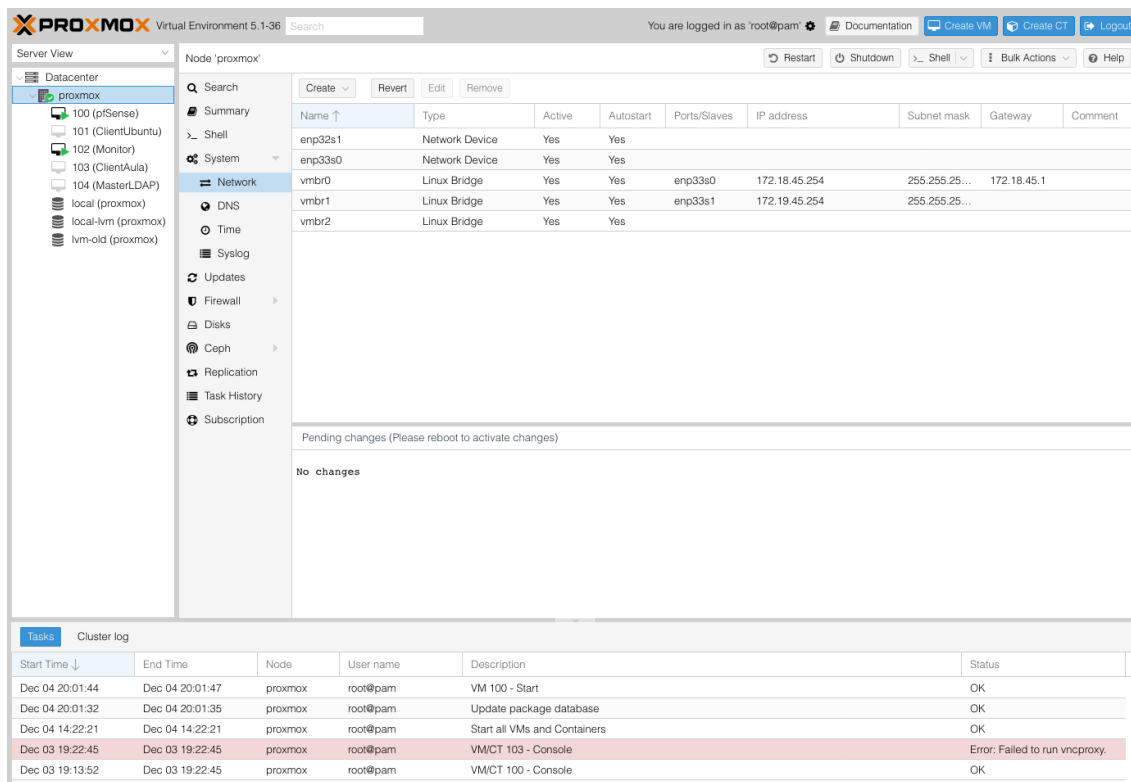


Figura 34: Configuració de Proxmox (II).

A l'hora de gestionar les interfícies de xarxa s'accedirà dins del node **proxmox** al menú **System...Network**. El servidor disposa de 2 interfícies de xarxa **enp32s0** i **enp32s1**, connectades a cada una de les xarxes. Associades a aquestes es creen 2 interfícies virtuals **vmbr0** i **vmbr1**, de tipus **bridge**, que seran les utilitzades per les màquines virtual. La interfície **vmbr2** serà de tipus interna i s'utilitza només en entorn de proves. La figura 34 mostra la configuració de la xarxa.

Proxmox crea automàticament dos volums **LVM**, **local** (emmagatzematge d'ISOs i backups) i **local-lvm** (emmagatzematge de discs durs virtuals). En la figura 35 es mostra un volum addicional **lvm-old** associat a un segon disc dur de major capacitat. La configuració es realitza a nivell de **Datacenter...Storage**.

La creació de màquines virtual és molt senzilla des del botó **Create VM** i és similar a les d'altres sistemes de virtualització (figura 36).

Per últim, en la figura 37 es pot comprovar les característiques de la màquina virtual **pfSense**.

12 Valoració de les tasques desenvolupades.

Les tasques desenvolupades a les pràctiques han reforçat les competències relacionades amb la gestió de xarxes i d'administració de servidors.

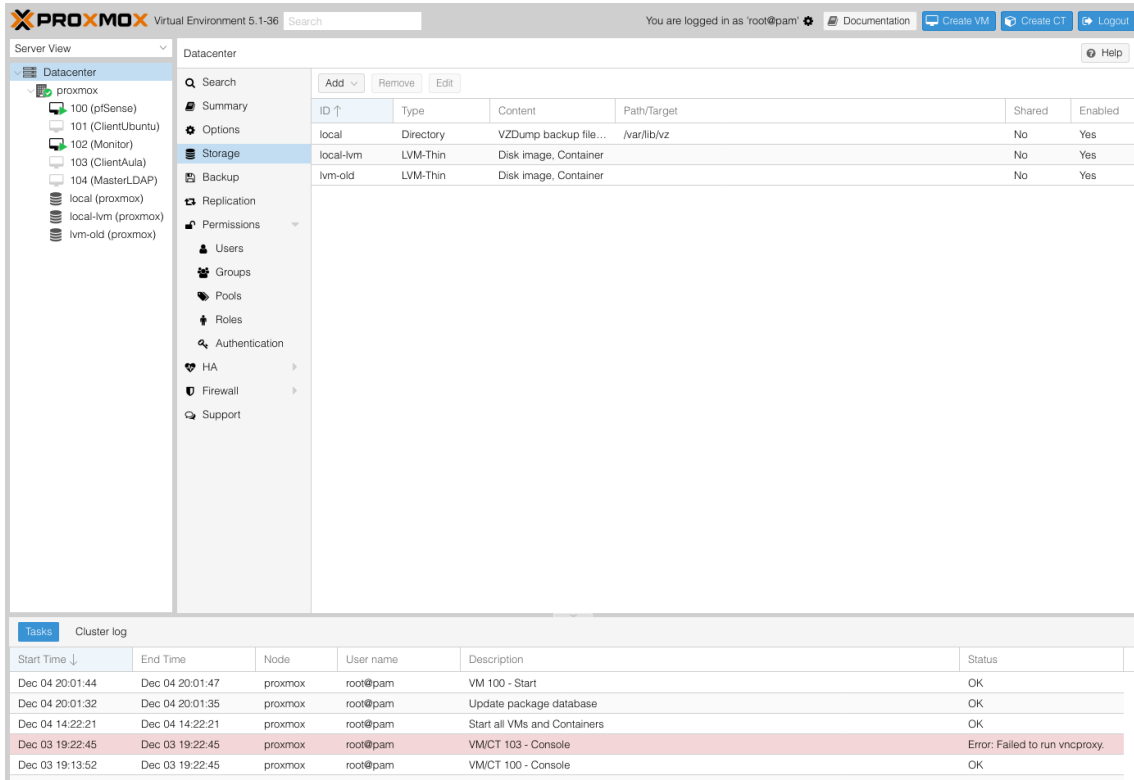


Figura 35: Configuració de Proxmox (III).

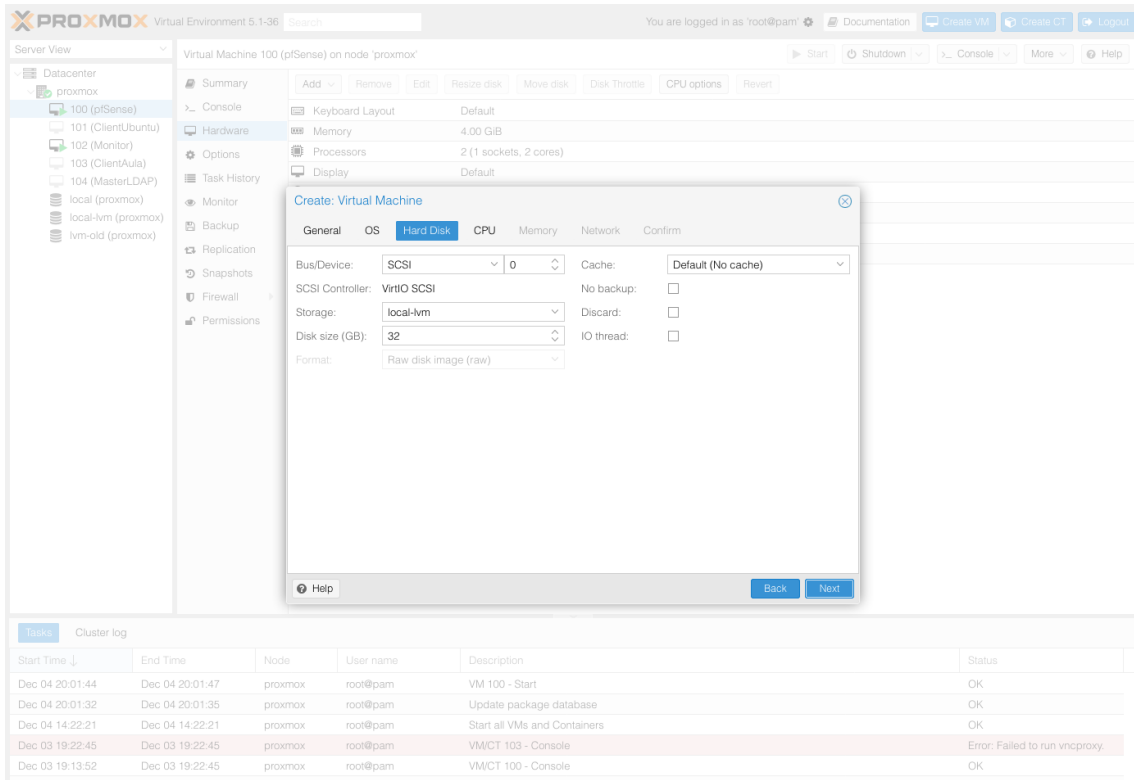


Figura 36: Configuració de Proxmox (IV).

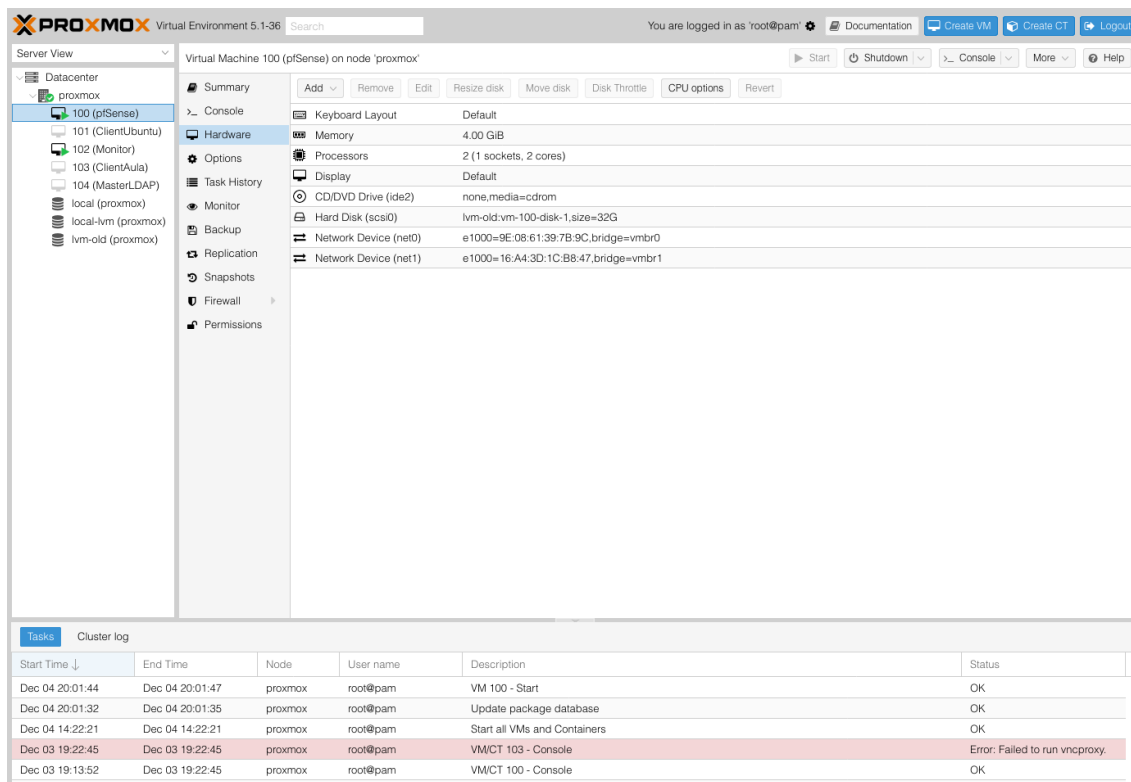


Figura 37: Configuració de Proxmox (V).

Les noves tecnologies involucrades en la virtualització de sistemes són de vital importància a l'hora de realitzar tasques d'administració. **Proxmox** és una solució de gran nivell dins del programari lliure. Les competències adquirides en aquest àmbit poden ser emprades a altres sistemes de virtualització, siguin o no solucions lliures.

pfSense resulta d'una utilitat a l'hora de gestionar un sistema de xarxa. Incorpora multitud d'eines i permet la incorporació senzilla de moltes més. Açò implica en una gran versatilitat i possibilitats d'ampliació futura. **FreeBSD** està basada en **FreeBSD** i permet ampliar les competències d'administració a altres sistemes lliures distints de **Linux**.

Icinga és un sistema complet de monitorització de sistemes de xarxa. Permet la instal·lació de multitud de complements compatibles amb **Nagios**. Aquest fet deriva en una gran de possibilitats en els mètodes de control dels equips i recursos de la xarxa.

13 Relació dels problemes plantejats.

El principal problema sorgit durant el desenvolupament de les pràctiques ha sigut la manca de recursos del servidor del centre. S'ha pogut finalitzar la implantació del sistema gràcies a l'ús d'un equip privat, propietat del treballador. S'ha realitzat un estudi de les despeses necessàries en l'adquisició d'un nou servidor. El cost total no és massa elevat i, per tant, es realitzarà la compra del servidor en un futur proper.

14 Avaluació de les pràctiques i suggeriments de millora.

Les pràctiques han suposat una ampliació en els coneixements del treballador. Aquestes pràctiques pertanyen a un àmbit del coneixement de gran interès per a un administrador de sistemes. Virtualització i gestió de xarxa són competències necessàries en el treball de l'administrador.

El treball realitzat durant aquestes pràctiques no finalitza en aquest punt. Les possibilitats de millora són nombroses:

- Agregació de tots els equips importants de la xarxa al sistema de monitorització.
- Establiment de nous paràmetres de monitorització als equips de xarxa.
- Integració del servidor proxy i els usuaris **LDAP**.
- Adquisició de noves targetes de xarxa i creació de bonds amb l'objectiu de multiplicar l'amplària de banda del sistema.
- Creació d'una **VPN** que permeti l'administració de la xarxa des d'altres localitzacions.
- Agregació d'un segon servidor **Proxmox** i la gestió de clusters de nodes virtualitzadors.

15 Resultats del projecte.

La implementació final del projecte es pot considerar com a una primera versió d'un sistema complet de gestió de la xarxa del centre. Durant els successius anys serà necessari l'ampliació gradual del sistema, incorporant noves variables a administrar, així com noves funcionalitats.

D'aquesta manera el sistema implementa l'esquelet on aniran acoblant-se els diferents mòduls que afegiran noves funcions així com millorar i completar les existents.

En la fase inicial del projecte es realitzaren les proves en un equip disponible del centre. Aquest servidor disposava de les següents característiques:

- **CPU:** AMD Athlon X4 620, amb 4 nuclis i 4 fils d'execució, amb una velocitat base de 2,6 GHz.
- **RAM:** 4 GB DDR3 1333 (2x2GB).
- **HD:** 2 Discs durs mecànics de 500 GB a 7200 rpm.
- **Xarxa:** 2 targetes de xarxa a velocitat de 1 Gbps.

El sistema s'ha implementat finalment en un servidor propi, amb l'objectiu de reduir el temps d'execució de les tasques a realitzar. La possibilitat de disposar del maquinari en qualsevol moment i a casa ha facilitat en gran grau el desenvolupament del projecte. Les característiques del maquinari del servidor emprat són les següents:

- **CPU:** AMD Ryzen 7 1700, amb 8 nuclis i 16 fils d'execució, amb una velocitat base de 3,7 GHz.
- **RAM:** 16 GB DDR4 3200 (2x8GB).
- **HD:** Disc dur mecànic de 320 GB a 7200 rpm.
- **Xarxa:** 2 targetes de xarxa a velocitat de 1 Gbps.

Les característiques d'aquest servidor personal són molt superiors a les de l'equip disponible al centre. De tota manera la migració dels serveis al servidor es pot realitzar en qualsevol moment. Les mancances en les prestacions es notaran en el número i velocitat dels nuclis disponibles per a les màquines virtuals, així com en la quantitat de RAM. La memòria RAM és de vital importància a serveis com el de servidor proxy. Aquest servei utilitza RAM i disc dur per a emmagatzemar la memòria cau. Les superiors velocitats de lectura/escriptura de la RAM front als del disc dur, implica que assignar una major quantitat de RAM al proxy és de vital importància per a assolir les millors prestacions del servei.

A continuació es detallen l'estat d'implantació dels distints serveis definits als objectius inicials del projecte.

15.1 Configuració d'un servidor proxy i d'encaminament.

Aquest servei s'ha implementat en una màquina virtual amb el sistema operatiu **pfSense** 2.4. Es dediquen 4 GB de RAM, 2 CPUs i 32 GB d'espai de disc. Aquests recursos poden ampliar-se en un futur si les condicions ho requereixen.

Els serveis d'encaminament i NAT funcionen correctament. Els usuaris de la xarxa sense fil poden accedir als servidors de la xarxa cablejada i a Internet. Qualsevol accés a un altre equip de la xarxa cablejada serà bloquejat pel tallafocs.

Així mateix s'ha configurat un servidor proxy transparent amb **Squid** ³¹. Aquest proxy filtra tot el tràfic **HTTP**. En canvi no s'ha efectuat el filtrat dels continguts **HTTPS** ja que es necessitaria la configuració manual dels equips clients de la xarxa sense fil. En una primera instància el servidor ha de provocar el menor impacte en el funcionament diari dels treballadors del centre, així que s'ha decidit implantar aquest segon filtrat més endavant.

El servidor proxy emmagatzemarà a la seua memòria cau el contingut de les pàgines web visitades pels treballadors, amb l'objectiu de reduir el volum del consum d'amplària de banda amb les connexions d'Internet.

³¹<http://www.squid-cache.org/>

Es deixa per a un futur el filtrat per part del proxy de l'accés d'algunes de les pàgines web que més trànsit generen, podem realitzar aquest filtrat només als moments de màxim ús de la xarxa.

15.2 Optimització dels recursos de xarxa.

Aquests serveis s'implementen al sistema **pfSense** anteriorment descrit.

Un dels serveis que permeten l'estalvi en el consum d'Internet és el sistema de memòria cau implantat en el servidor proxy.

Per una altra banda s'ha activat un sistema **QoS** que distribueix equitativament el total d'amplària de banda entre el total de les connexions existents en la xarxa sense fils. Aquest sistema no estableix un límit fixe per equip i, per tant, permet velocitats majors de connexió als clients quan hi han pocs equips accedint a la xarxa. Aquest sistema s'implementa gràcies al servei **TrafficShaper** inclòs a **pfSense**.

15.3 Control en l'accés a la xarxa.

Implantat en el sistema **pfSense**, permet accedir a la xarxa només als usuaris **LDAP** registrats. D'aquesta manera es protegeix l'accés a la xarxa, encara que es pugui veure compromesa la clau **WPA2** dels punts d'accés.

L'accés a la xarxa es realitza mitjançant un portal captiu que apareix en el moment d'intentar navegar per Internet. Aquest portal captiu està connectat a un servidor **FreeRadius** configurat en el propi **pfSense**. El servidor **RADIUS** realitza consultes al servidor **LDAP** del centre per a comprovar l'autenticació i autenticació dels usuaris.

Una altra possibilitat a l'hora de controlar l'accés passa per la configuració dels clients al moment de realitzar les connexions als punts d'accés. Això repercutiria en un major impacte als usuaris i obligaria a la configuració de tots els punts d'accés del centre. Es valorarà en un futur la migració a aquest nou sistema i eliminar el portal captiu, així es reduiria el consum de recursos del servidor.

15.4 Monitorització del trànsit i estat dels equips de la xarxa.

La monitorització del trànsit es realitza al sistema **pfSense**. En canvi la comprovació dels equips principals de la xarxa es realitza a una màquina virtual **Ubuntu Server 16.04** amb el servei **Icinga**. Aquesta última màquina virtual disposa de 2 GB de RAM, 2 CPUs i 32 GB d'espai de disc. Aquests recursos poden ampliar-se en un futur si les condicions ho requereixen.

pfSense disposa de funcionalitat bàsiques de monitorització que comproven l'ús de la xarxa. Així mateix també existeixen plugins que amplien aquestes funcionalitats. En el moment de la finalització d'aquest projecte s'ha decidit mantindre la

configuració per defecte que inclou **pfSense**. En un futur es plantejarà la possibilitat d'investigar algunes de les extensions disponibles en aquest àmbit.

Paral·lelament als recursos oferits per **pfSense** s'ha implantat a una màquina virtual **Ubuntu Server** un sistema de monitorització basat en **Icinga 2**. Aquest servei permet el control de l'estat dels distints equips de la xarxa i permet l'inclusió de multitud d'afegits compatibles amb **Nagios**. **Icinga 2** té un mòdul web que permet la visualització remota de l'estat de la xarxa. A més a més se li ha incorporat el mòdul **NagVis** que permet la creació de gràfics que mostren l'estat dels clients i serveis que l'administrador desitge.

15.5 Virtualització dels serveis.

En una primera instància les proves es realitzaren a màquines virtuals dins del programari **VirtualBox**.

Posteriorment es migraren els sistemes al hipervisor **Proxmox**. **Proxmox** permet una administració dels sistemes virtuals més avançada que **VirtualBox**, a més de major prestacions. **Proxmox** es basa en l'hipervisor **KVM** i li afegeix una interfície web d'administració molt completa.

16 Valoració econòmica.

A la vista dels resultats de la implantació del projecte es plantejarà la possibilitat de renovar el maquinari per a la confecció d'un equip de majors prestacions on allotjar el servidor de virtualització amb els distints serveis. Les característiques de l'equip personal són suficients per a aquest nou equip. Així i tot es recomana la incorporació d'un disc dur d'estat sòlid SSD on s'allotjaran el sistema operatiu i les màquines virtuals en execució. D'aquesta manera s'assoliria un increment en les prestacions de lectura/escriptura al disc. Es preveu així una millora substancial en la qualitat dels serveis oferits. Els discs durs mecànics actuals de l'equip s'utilitzarien per a emmagatzemar còpies de seguretat i imatges de disc necessàries per a assegurar els serveis.

Una millora recomanable seria la inversió en una targeta de xarxa gigabit amb més d'un port Gigabit. D'aquesta manera es podria augmentar l'amplària de banda de les connexions de xarxa. Els sistemes de virtualització com Proxmox permeten la creació de **bonds**, assignant una interfície virtual de xarxa a més d'un port físic real. Els switches de la xarxa local permeten l'agregació de ports i la creació de **VLANs**. Així es podria ampliar les característiques del sistema en un futur, millorant les prestacions dels serveis als usuaris.

Per tant es recomana l'adquisició d'un nou processador, placa base, RAM, disc dur SSD i targeta de xarxa de 2 ports Gigabit. La següent llista detalla la despesa econòmica necessària, atés al preu mitjà actual d'aquests components en el moment de la redacció del present document.

Componente	Modelo	Precio (euros)
CPU	AMD Ryzen 7 1700	283
RAM	G.Skill FlareX DDR4 3200 16GB 2x8GB	246
Disco SSD	Samsung 850 Evo SSD 500GB SATA3	152
Placa Base	MSI B350 Tomahawk	105
Tarjeta xarxa	Startech PCIe a Ethernet Gigabit	82
Total	-	868

Aquesta despesa es considera una inversió, ja que les característiques dels components són més que suficients per a la implantació dels presents i futurs serveis.

17 Conclusions.

El resultat final del projecte té els ciments necessaris per a implantar-se amb èxit a la xarxa del centre. A més conté l'estructura idònia per a ampliar la seua funcionalitat en un futur. La flexibilitat que ofereix els sistemes virtualitzats permet una administració dels serveis senzilla. Les noves funcionalitats es podrien provar en màquines virtuals no connectades al sistema real i fer la substitució immediata entre distintes *versions* dels serveis. En cas de funcionament erroni del sistema és molt fàcil el retorn a una versió de la màquina virtual anterior amb els serveis amb correcte funcionament.

La despesa en un millor maquinari per al servidor del centre és reduïda front als avantatges enunciats en aquest document, la qual cosa repercutiria en un millor funcionament dels recursos de la xarxa i, per tant, del treball diari dels usuaris d'aquesta.

18 Bibliografia.

- **pfSense 2 Cookbook** - Williamson, M. - Ed. Packt Publishing. 2011.
- **Mastering Proxmox** - Ahmed, W. - Ed. Packt Publishing. 2016.
- **Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud** - Stallings, W. - Ed. Addison-Wesley Professional. 2015.
- **Icinga Network Monitoring** - Mehta, V. - Ed. Packt Publishing. 2013.
- **Learning Nagios** - Beltowski, P. - Ed. Packt Publishing. 2016.
- **LDAP System Administration** - Carter, G. - Ed. O'Really Media, Inc. 2003.
- **Squid Proxy Server 3.1 Beginner's Guide** - Saini, K. - Ed. Packt Publishing. 2011.
- **FreeRADIUS Beginner's Guide** - van der Walt, D. - Ed. Packt Publishing. 2011.
- **Icinga2 Documentation**: <https://www.icinga.com/docs/>. 2017.

19 Glossari.

- **Agregació d'enllaços o network bonding:** Mètodes de combinació de múltiples connexions de xarxa en paral·lel amb l'objectiu d'augmentar l'amplària de banda i la resistència a errades.
- **Amplària de banda:** Mesura de dades i recursos de comunicació disponible o consumida expressades en bit/s o múltiples d'ell.
- **Conmutador o switch:** Dispositiu que interconnecta dos o més segments de xarxa.
- **DHCP:** (Dynamic Host Configuration Protocol). Protocol en el qual un servidor disposa d'una llista de direccions IP dinàmiques i les assigna als clients conform aquestes van quedant lliures.
- **DNS:** (Domain Name System). Sistema de noms jeràrquic que funciona sobre una base de dades distribuïda i que permet que qualsevol sistema connectat a Internet o a una xarxa informàtica privada obtingui informació associada als noms de domini.
- **Memòria cau web:** Memòria que emmagatzema documents web per a reduir l'amplària de banda consumida, la càrrega dels servidors i el retard en la descàrrega.
- **Monitorització de xarxes:** Ús d'un sistema que de manera contínua monitoritza una xarxa de computadores cercant components lents o fallits i després notifica a l'administrador de la xarxa en cas d'aparèixer cap comportament anòmal.
- **NAT:** (Network Address Translation). Mecanisme utilitzat per routers IP per a intercanviar paquets entre dos xarxes que assignen mútuament direccions incompatibles.
- **Portal captiu:** Programa o dispositiu d'una xarxa informàtica que vigila el trànsit HTTP i obliga als usuaris a passar per una pàgina especial si volen navegar per Internet de forma normal.
- **QoS:** (Quality of Service). Conjunt d'estàndards i mecanismes que realitza el control de reserves dels recursos de la xarxa, en el camp de les xarxes de commutació per paquets.
- **RADIUS:** (Remote Authentication Dial-In User Server). Protocol d'autenticació i autorització per a aplicacions d'accés a la xarxa o mobilitat IP.
- **Serveis de directori:** Aplicació o conjunt d'aplicacions que emmagatzema i organitza la informació sobre els usuaris d'una xarxa d'ordinadors i sobre els recursos de xarxa que permet als administradors gestionar l'accés d'usuaris als recursos d'aquesta xarxa.
- **Servidor d'encaminament o router:** Dispositiu que envia o encamina paquets de dades d'una xarxa a un altra, interconnectar distintes subxarxes.

- **Servidor intermediari o proxy:** Programa o dispositiu què fa d'intermediari entre les peticions de recursos que realitza un client a un altre servidor.
- **Tallafoc o firewall:** Element de maquinari o programari utilitzat en una xarxa d'equips informàtics per controlar les comunicacions, permetent-les o prohibint-les segons les polítiques de xarxa que hagi definit l'organització responsable de la xarxa.
- **Virtualització:** Creació mitjançant programari d'una versió virtual d'un recurs tecnològic, com una plataforma de maquinari, un sistema operatiu, un dispositiu d'emmagatzemament o altres recursos de xarxa.
- **VLAN:** Mètode per a crear xarxes lògiques independents dins una mateixa xarxa física.
- **Xarxa privada virtual o VPN:** Tecnologia de xarxa de computadores que permet una extensió segura de la xarxa d'àrea local sobre una xarxa pública o no controlada com Internet.
- **WiFi:** Mecanisme de connexió de dispositius electrònics sense fils.
- **WPA:** (Wi-Fi Protected Access). Sistema per a protegir les xarxes sense fils (Wi-Fi).