Incorporació de mecanismes de seguretat a la xarxa de l'empresa

Projecte Final de Màster de Programari Lliure

Autor: Beatriz Simó Martí
Consultor: Miquel Martín Mateo
Tutor extern: Ernest Juanico Soler
Palma, 31 de Decembre 2013

Llicència

Resum

Idiso es una empresa de serveis de distribució hotelera amb una plataforma que aconsegueix que la formalització d'una reserva en qualsevol tipus d'hotel sigui factible i efectiva pels tur-operadors, agents de viatge on i offline o usuaris finals.

Actualment, es una empresa full PCI DSS Complience(Payment Card Industry Data Security Standard), que vol dir això, que l'empresa tracta i custodia adequadament les dades de targetes de dèbit/crèdit dels clients que s'aloja en els hotels als que prestam serveis de reserves. A rel d'aquesta normativa, Idiso, necessita un control de seguretat perimetral i de la seguretat dels accessos a la xarxa, es obligat la observació de procediments de gestió del canvi i l'emmagatzemament de uns logs de tots aquest canvis. Degut a la mobilitat dels equips la quantitat de canvis necessaris en la configuració dels routers es massa alta i les tomes de xarxa també.

Per una altra banda l'aparició de múltiples dispositius particulars que se desitgen puguin ser connectats a la xarxa corporativa, dificulta encara més la gestió, d'aquest routers, amb un NAC, es pretén poder definir pol.lítiques i oblidar-se de realitzar canvis de manera manual i a més es pretén automatitzar els procediments i els log que es requereixen PCI DSS.

Idiso, amb aquest projecte pretén implantar l'eina de software lliure Packetfence amb la que gestionarem els punts de xarxa corporativa de manera automàtica. Se pretén instal.lar i configurar una NAC(Network Access Control) de manera que la configuració d'un determinat punt de xarxa depengui únicament del dispositiu que se connecti en aquell punt. De les possibles sol.solucions actuals en el mercat, s'ha optat per aquesta per la seva transparència en l'usuari, solució basada amb Linux i d'altres empreses que l'han feta servir el hi han donat bon resultats.

Taula de Continguts

1. Introducció

1.1. Motivació

Actualment, Idiso, és una empresa full PCI DSS Complience a rel d'aquesta normativa necessita un control de seguretat perimetral i de la seguretat dels accessos a la xarxa, es obligat la observació de procediments de gestió del canvi i l'emmagatzemament de uns logs de tots aquest canvis. Degut a la mobilitat dels equips la quantitat de canvis necessaris en la configuració dels routers es massa alta i les tomes de xarxa també.

Per una altra banda l'aparició de múltiples dispositius particulars que se desitgen puguin ser connectats a la xarxa corporativa, dificulta encara més la gestió d'aquest routers, amb una NAC(Network access control), es pretén poder definir pol.lítiques, certes regles i categories, oblidar-se de realitzar canvis de manera manual i a més es pretén automatitzar els procediments i els log que es requereixen PCI DSS.

La xarxa d'Idiso està dividida en diferents segments o subxarxes. Depenent del segment o de la subxarxa a la que es connecta un dispositiu, els firewalls limitaran la visibilitat que tindrà aquest dispositiu de la xarxa. Finalment, és als switchos on hi ha la definició dels segments accessibles des de un determinat punt de la xarxa.

Malauradament les configuracions de les boques de xarxa varien amb massa freqüència. Per exemple: Les boques de xarxa de les sales de reunions sols tenen sortida a Internet i la resta de la xarxa no és visible, però en cas de certes reunions o formacions es necessari canviar la configuració de les boques per a que tenguin visibilitat de la xarxa i en acabar aquestes reunions o formacions es necessari tornar a deixar les boques de xarxa com estaven.

La normativa PCI DSS obliga a tenir un control exhaustiu de tots aquests canvis, avui per avui aquest control es manual així com l'aplicació d'aquests canvis. A més, la normativa requereix emmagatzemar els registres de canvis i per a cada canvi requereix que s'especifiqui el motiu del mateix.

Amb un NAC es pretén passar a un model de perfils. Al final, és una persona la qui té la

necessitat de connectar el seu dispositiu a la xarxa, aleshores ha d'esser el perfil d'aquesta persona qui especifica el segment al que ha d'estar connectat. A més aquesta persona disposa d'un equipament informàtic facilitat per l'empresa i és amb aquest equipament amb el que s'ha de connectar a la xarxa.

Una solució NAC permet controlar quins dispositius es connecten a la xarxa i a quins segments ha d'estar connectats aquest dispositius. Amb aquesta informació el NAC es capaç de detectar quin dispositiu s'ha connectat a quin punt de xarxa i es capaç de canviar la configuració del punt de xarxa de manera automàtica d'acord a informació de que disposa. Per altre banda, el NAC deixa dins un log tots el canvis de configuració dels punts de xarxa que realitza.

Finalment un NAC és capaç d'examinar el dispositiu connectat i situar-lo a un segment de xarxa molt restringit en cas de detectar malware, versions no actualitzades del software instal·lat etc.

Amb un NAC es simplificarà la tasca de configuració de switchos, podrem passar a un model de perfils i quedarà mecanitzat el registre canvis que requereix la normativa PCI DSS.

1.2. Objectius

Els objectius son:

- Implantar una eina de Software Lliure, Packetfence, per gestionar els punts de xarxa corporativa de manera automàtica, es pretén instal.lar i configurar un NAC.
- Definir pol.lítiques, automatitzar procediments i logs.
- Desenvolupament d'integració de Qualys amb Packetfence.

1.3. Estructura de la memòria del projecte.

L'estructura de la memòria sira la següent:

- ***Introducció***, on es detalla la motivació i els objectius d'aquest projecte.
- ***L'estudi de viabilitat i els requeriments***, s'explica quines són les necessitats de l'empresa, la

situació actual d'aquesta, quines polítiques s'han de seguir, quines solucions se poden aplicar.

- Els ***fonaments teòrics***, en aquest apartat, s'explica el que es una NAC.
- Les ***fases***, s'explicarà les fases que te el projecte, les seves tasques i la durada d'aquestes amb el diagrama de Gant.
- El ***disseny*** i la **implementació**, definició de l'arquitectura del sistema, especificacions d'estàndards, casos d'us real, especificacions de desenvolupament i proves, implantació.
- ***Costos economics***, detall de l'esforç econòmic que suposa implantar una NAC.
- ***Conclusions***, en aquest apartat es comentaran els resultats, les conclusions i possibles millores.
- **Referències bibliogràfiques**.
- **Annexes**. En aquest apartat estirà la documentació adicional que sirà la llicència, el laboratori, la instal.lació del software, etc.

2. Estudi de viabilitat i requeriments

A rel de la norma PCI DSS(Data Security Standard), que consisteix en una serie d'estàndards de seguretat que inclouen:

- Requeriments per administrar la seguretat.
- Les polítiques.
- Els procediments
- L'arquitectura de les xarxes.
- El disseny de software
- Altres mesures critiques de protecció de la informació.

L'empresa necessita un control de seguretat perimetral i de la seguretat d'accessos a la xarxa, es obligat l'observació de procediments de gestió de canvis i l'emmagatzemament d'uns logs de tots aquests canvis. Degut a la mobilitat dels equips la quantitat de canvis necessaris en la configuració dels routers es massa alta i les tomes de xarxa també.

Per una altra banda l'aparició de multiples dispositius particulars que se desitgen puguin ser connectats a la xarxa corporativa, dificulta encara més la gestió d'aquests routers, amb un NAC es pretén poder definir pol.lítiques i oblidar-se de realitzar canvis de manera manual i a més es pretén automatitzar els procediments i els logs que es requereixen per PCI DSS.

2.1. Necessitats i requeriments del client

El principal requeriment d'Idiso és implantar una eina NAC, per gestionar tots els punts de xarxa corporativa de manera automàtica.

El NAC ha d'esser capaç de:

• Tenir un inventari de les MACs dels dispositius de l’empresa, tant de Palma com de Madrid.

• Detectar que un dispositiu es connecta a la xarxa i situar-lo al segment de xarxa que pertoqui.

• Canviar la configuració dels switchos de manera automàtica per tal d'aconseguir el punt anterior.

• Enregistrar a un totes les accions realitzades a un log.

2.2. Anàlisi de la situació actual

2.2.1. Diagrama de xarxa

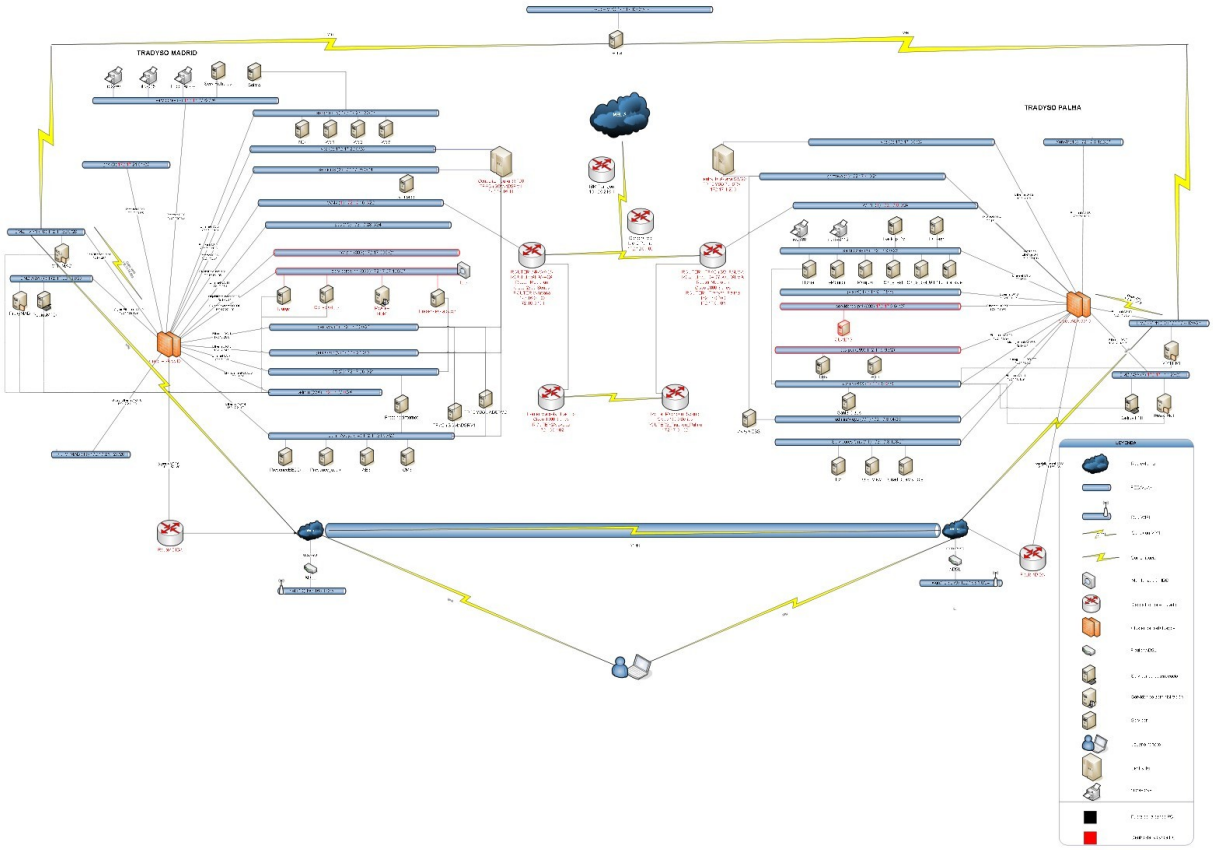

Ilustración 1: Diagrama de xarxa de l'empresa

2.2.2. Descripció i configuració dels diferents switches.

La topología de la xarxa física de Madrid i Palma es en anell amb STP(Spanning Tree Protocol) habilitat mode PVSTP(Per-VLAN Spanning Tree), la topologia de xarxa lógica es amb estrella. A Palma hi ha 7 switches funcionant, i a Madrid ni ha 8.

No hi ha una arquitectura en 3 nivells de: access, distribució i nucli. Els switchos nous

que arriven es configuren i se conecten a la xarxa.

En la xarxa tenim dos models diferents de software CISCO:

• Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Version 12.2(55)SE1, RELEASE SOFTWARE (fc1)

• Cisco IOS Software, C2960 Software (C2960-UNIVERSALK9-M), Version 12.2(55)SE5, RELEASE SOFTWARE (fc1).

Tots els switches tenen 48 ports, excepte el sw7pmi que te 24, admiteixen PoE.

La configuració admeteix enrutament de capa 3 però no se utilitza, se configura manualment els ports d'access en funció de la necessitat de cada usuari per el mateix port del software que s'utilitza per access.

Tots els ports d'access estan configurats com port-fast i en la configuració global està habilitat com PortFast BPDU Guard Default, lo que impideix injectar BPDU(Bridge Protocol Data Unit) en els ports d'accèss i modificar la topologia STP(Spanning Tree Protocol).

Alguns ports tenen habilitat port-security, per exemple, els de les sales de reunió, per protegir la xarxa de vou.

L'autentificació dels usuaris es remota contra un servidor Radius(FreeRadius).

2.3. Definició dels requeriments del sistema

2.3.1. Polítiques de seguretat a implementar

Seguint les guies de hardenització de Idiso, el servidor a on instal.lem el NAC haurà d'aplicar les següents polítiques:

• Deshabilitar protocols insegurs en aquest cas per gestió(HTTP, Telnet, SNMPv1 ó SNMPv2, SSHv1).

• Utilitzar criptografia robusta.

• Control de canvis.

• Reenviar logs en el servidor centralitzat.

• Registre de logs d’accès i accions administratives damunt del software.

• Sincronització del relotge mitjançant NTP intern.

• Eliminar serveis innecessaris.

• Escanejos trimestrals mitjançant l’eina Qualys amb la finalitat de no tenir vulnerabilitats amb CVSS.

• La gestió del software unicament es pot fer mitjançant una subxarxa administrativa i l’usuari ha d’estar donat d’alta en el servidor Radius i pertanyer un determinat grup administrador de switches.

• Revisió semestral dels serveis habilitats.

• Revisió semestral de usuaris amb accès al software.

• Canvi de valors predeterminats pels proveïdors abans d’instal.lar un sistema a la xarxa.

2.3.2. Polítiques de retenció de logs

Segons PCI DSS, respecte als logs:

• Retenció de logs en el servidor centralitzat.

• Aquests logs s’han de retenir durant un periode d’un any complet, disponible per la consulta immediata dels darrers 3 mesos.

• Control d’access al registre de logs emmagatzemats-

• Mecanisme de protecció davant de qualsevol canvi damunt d’aquest fitxers de logs emmagatzemats.

• Revisió diaria automatizada dels fitxers de logs.

Idisio disposa d'una solució de centralització de logs, i es requeriment d'aquest projecte, habilitar els mecanismes necessaris per tal de que els logs generats per Packet Fence arribin a la solució de centralització de logs existent.

2.4. Estudi d'alternatives de solució

Hem estudiat les següents alternatives de software de NAC, tenim com se pot veure a la taula següent:

Producte	*URL*
Packetfence	http://www.packetfence.org
Symantec Network Access	Symantec Network Access
Cisco Network Admission Control	Cisco Network Admission Control

2.4.1. Valoració i elecció de les possibles sol.lucions

PacketFence, es una solució Open Source, de control d' acces de xarxa(NAC). Es una distribució linux configurada per proporcionar un complet sistema de control d'acces de xarxa.

Característiques:

• Portal cautiu per autentificar i registrar els dispositius que demanen acces a la xarxa.

• Suport de 802.1x(FreeRadius inclòs).

• Gestió centralitzada de les xarxes: cabletjada e inalàmbrica.

• Integració amb Snort i Nessus.

• Suport VLAN i aillament de xarxes.

• Autentificació, suport per (Microsoft Active Directory, Novell eDirectory, OpenLDAP, CISCO ACS Radius(FreeRadius, Radiator, etc), Local user File).

Estàndars suportats:

• 802.1x

• Simple Network Management Protocol(SNMP).

• Estàndar SNMP managament information base(MIB) com BRIGE-MIB, Q-BRIGE-MIB, IF-MIB, IEEE8021-PAE-MIB

• Radius

• Network/IPFIX

• Wireless ISP Roaming(WISPR)

Les novetats de la darrera versió 4.0.6, son:

• Millora de la visualització dels filtres i de les fonts(DynamicTable) a l'editor de perfils del portal.

• Assegureu-vos que l'esquema de noms de VLAN s'estableix en l'arrencada.

• Quan no hi ha cap font d'autentificació s'associa amb el perfil predeterminat del portal, s'utilitzen totes les fonts disponibles.

• El nombre telefònic es arà editable de l'editor dels usuaris.

• Emprentes digitals actualitzades del dispositius de joc(Xbox).

• Mogut pfmon a un dimoni d'un sol procés i s'afegeix la capacitat de reiniciar en cas d'error.

• Afegit nou test eina bin / Pfvariedad sotmesa a assaig

• Millora de la consulta SQL en pf :: node quan coincideixen amb un MAC vàlida

• Permetre el canvi de propietari en editor de nodes (amb auto-realització) gestió iptables per PacketFence ara és opcional

• Permetre cerca avançada d'usuaris i nodes de notes (# 1701)

• Va afegir millor error / missatges d'advertència quan s'afegeix una violació amb pfcmd

• Sortida de la Identificació violació de violació pfcmd afegir ordres quan es subministra l'opció json.

Symantec Network Access Control (SNAC), es una solució privativa, una solució de control d'accés de xarxa d'extrem a extrem que permet que les organitzacions tenguin l'accés eficient i segur en les seves xarxes corporatives amb les actuals infraestructures de xarxes.

Principals aventatges de SNAC, son:

• Reducció de la propagació de codis maliciosos com virus, cucs, spyware,etc.

• Pèrfil de risc baix a través d'un major control de punts finals no gestionats i administrats amb l'accés a xarxes corporativa.

• Major disponibilitat de xarxa i reducció de la interrupció dels serveis.

• Verificació de les inversions en seguretat de punt final com antivirus i firewalls degudament habilitats.

• Integració amb Symantec Endpoint protection.

Les característiques son:

• Symantec proporciona una funcionalitat de control extrem a extrem sense requerir solucions externes. A més integra altres tecnologies de control d'accés a la xarxa.

• Independentment de la metodologia de la aplicació, els administradors poden estar segurs de que tenen amplia cobertura i control.

• Descobreix i avalua els punts finals.

• Provisió d'accés a xarxa.

• Remeiar els punts finals que no compleixen.

• Supervisa de manera pro-activa el compliment.

Symantec NAC, inclou suport per a assignació de VLAN de CISCO cable i sense fils,, commutadors Alcatel-Lucent, Foundry, HP, Nortel i switches Extreme, aixi com controladors sense fil Aironet.

Tambe inclou suport per Mac basat amb autenticació (per telèfons VoIP e impresores).

La fixació de preu per a l'aparell 11 NAC comença a $12.732, que inclou Symantec Network Access Coontrol Started Edition 11.0, un Symantec Enforcer NAC Appliance i un

any de suport essencial.

Cisco Network Admission Control, solucions basades en una iniciativa de la industria patrocinada per Cisco, utilitza la infraestructura de la xarxa per fer complir la política de seguretat en tots els dispositius que pretenen accedir als recursos informàtics de la xarxa, limitant aixins el dany causat per amenaces emergents contra la seguretat. Es una arquitectura propietaria, que en el costat del client es compon d'un agent anomenat Cisco Trust Agent, software gratuit descarregable des de la pàgina del fabricant, i la funció es la de rebre la informació de l'estat de la seguretat de l'equip a connectar a la xarxa proporcionant tota la informació recollida, per recopilar aquesta informació es poden utilitzar aplicacions de diferents fabricants o una propietària de Cisco, el Cisco Secure Access. Els clients que usen NAC tenen la capacitat de permetre que accedeixin a la xarxa nomes dispositius de punt terminal fiables que compleixin les polítiques de seguretat i poden limitar l'accés dels dispositius que no les compleixen.

Pel Trust Agent Cisco ha desenvolupat un protocol propietari l'EAP, en dues versions: una sobre UDP i una altra sobre 802.1X. La diferència entre ambdues és que sobre UDP es fa nomes validació i en 802.1X es fa validació i autenticació. A més no tots els equips Cisco suporten tots els escenaris possibles a través del protocol EAP.

La tecnologia NAC Appliance, basada en la línia de productes Cisco Clean Access, permet una ràpida implementació amb serveis incorporats d'avaluació de punts terminals, administració de polítiques i serveis correctius.

La tecnologia NAC Framework, a traves del programa de control d'admissió a la xarxa de Cisco, integra una infraestructura de xarxa intel·ligent amb solucions de més de 75 dels principals fabricants d'antivirus i altres solucions de programari de seguretat i gestió.

Conclusió, de totes les opcions estudiades, hem triat Packetfence, perquè dins un marc de reducció de costos i control dels mateixos, l'adquisició d'una eina comercial no és plantejable, a més es pretén demostrar que el valor de les eines open source poden

aportar.

3. Fonaments teòrics

3.1. NAC.

NAC, control d'accèss a xarxa, s'utilitza en la infraestructura de xarxa per fer complir la política de seguretat en tots els dispositius que busquen l'accés als recursos de xarxa. Un NAC, permet als administradors de xarxa autenticar i autoritzar als usuaris i avaluar i posar remei a les màquines corresponents abans que se'ls concedeixi accéss a la xarxa.

Els diferents tipus de solucions NAC inclouen:

- Applience-based, dividit per si l'aparell està en línea o fora de banda.
- Basad amb equips de xarxa o switch
- Client/servidor.
- Agentless o Clientless, no ha de menester cap software instal.lat en el dispositius.
- Client-based, s'ha de instal.lar un component de software en els dispositius per poder assistir al proces de NAC.

Els diversos tipus de mètodes d'implementació de NAC inclouen:

- Integrat amb, o com una superposició a, la xarxa o la infraestructura de seguretat.
  Si s'implementa una solució NAC com a part integrant d'una xarxa o com una capa superposada a la xarxa d'infraestructura de seguretat, en la seva major part, depèn del tipus de solució NAC que seleccioni.
  Generalment, s'ha de tractar amb NAC integrat quan s'utilitza qualsevol tipus de solució NAC que aprofita una caixa de xarxa. Si vostè no necessita un dispositiu o component de xarxa, llavors en general no ha de preocupar-se per la integral contra l'elecció d'implementació de superposició.

- Capa 2 o Capa 3 d'autenticació, es refereix a les capes OSI(Open System Interconnection) de xarxa.
  La capa d'enllaç de dades (Capa 2) facilita les comunicacions i la transferència d'informació entre els components de la xarxa. (L'estàndard IEEE 802.1x per al control d'accés a la xarxa basat en port també opera a la capa 2. Molts switches Ethernet i punts d'accés sense fil desplegats en xarxa en tot el treball d'avui donen suport l'estàndard 802.1x).

Capa 3, la capa de xarxa en el model de referència OSI bàsica, proporciona els mitjans de transferència de dades des d'un origen a una destinació a través d'una o més xarxes. A més, l'enrutament de xarxa es produeix a la capa 3. Algunes solucions NAC utilitzen Layer 3 el model d'aplicació de polítiques de seguretat i accés. Aquest model típicament aprofita un firewall o routers assegurances com a punt d'aplicació de la NAC, l'aplicació de les decisions basades en polítiques sobre com manejar certs usuaris, dispositius, i fins i tot el tràfic de xarxa.

4. Fases

El projecte esta compost de quatre fases que se descriuran a continuació i se poden veure planificades a la il.lustració següent amb el diagrama de Gant.

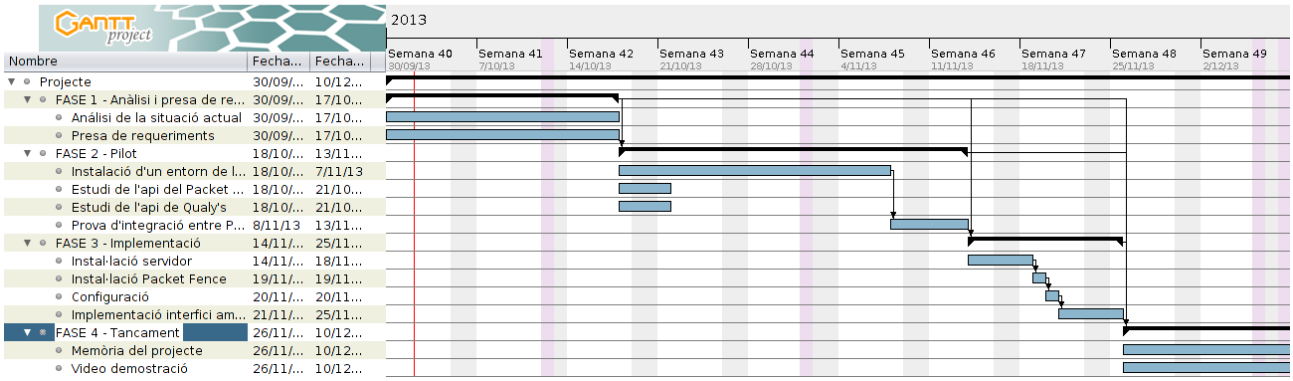

Ilustración 2: Diagrama de Gant del projecte de incorporació de mecanismes de seguretat

Aquestes fases se descriuen a continuació a la següent taula:

Fase 1. Anàlisis i presa de requeriments	**Anàlisi de la situació actual.** És necessari conéixer i documentar la situació actual: * Obtenir diagrama de la xarxa * Obtenir descripció i configuració dels diferents switches
	Presa de requeriments. Obtenir els requeriments d'implementació: * Polítiques de seguretat a implementar * Polítiques de retenció de logs

Fase 2. Desenvolupar un Pilot	**L'entorn de laboratori s'implementara sobre una màquina virtual**. L'objectiu d'aquesta tasca és descobrir: * Dependències de paquets. * Característiques necessàries del servidor. * Usuaris del sistema que el producte necessita. En definitiva es tracte de recollir tots els punts a tenir en compte quan s'instal·li la versió final.
	Estudi de l'API de PacketFence El Packet Fence s'integra amb diferents detectors de vulnerabilitats. Un dels objectius del projecte és desenvolupar d'integració amb Qualy's, servei de detecció de vulnerabilitats utilitzat a l'empresa. La finalitat d'aquesta tasca és tenir ben els mecanismes que Packet Fence ofereix per poder fer aquest tipus d'integracions.
	Estudi de l'API de Qualys La finalitat d'aquesta tasca es estudiar i documentar l'API que ofereix Qualy's per automatitzar els anàlisis devulnerabilitats amb altres sistemes.
	Integració entre PacketFence i Qualy's 1. La finalitat d'aquesta tasca és desenvolupar la més senzilla de les

	integracions per tal de: 2. * Descobrir els possibles problemes que poguem trobar. * Assegurar la viabilitat d'integració
Fase 3. Implementació	**Instal.lació del servidor.** Estara compost per les tasques de instalació, hardenització i actualització de paquets de la darrera versió.
	Instal.lació PacketFence. Seguint com a guió l'instal.lació que s'ha fet en la fase pilot, s'instal.larà el producte**.**
	Configuració. Tenint en conte els resultats de la presa de requeriments, es procedirà a fer la configuració del producte final.
	Implementació d'interfici amb Qualys. Tenguent en conte els resultats finals de l'instal.lació pilot, es desenvoluparan les darreres integracions amb Qualys.
Fase 4. Tancament del Projecte	**Memoria.** Se farà la documentació del projecte.
	Vídeo del projecte. Se farà un vídeo de demostració del desenvolupament del projecte i el seu resultat final.

5. Disseny e implementació

5.1. Disseny de la sol.lució e implementació.

La sol.lució adoptada ha estat implementar una NAC(Network Access Control), per gestionar tots els punts de xarxa corporativa de manera automàtica.

Aquesta sol.lució s'implantará amb l'eina, PacketFence, és una solució Open Source, de control d' acces de xarxa(NAC). Es una distribució linux configurada per proporcionar un complet sistema de control d'acces de xarxa.

Característiques:

• Portal cautiu per autentificar i registrar els dispositius que demanen acces a la xarxa.

• Suport de 802.1x(FreeRadius inclòs).

• Gestió centralitzada de les xarxes: cabletjada e inalàmbrica.

• Integració amb Snort i Nessus.

• Suport VLAN i aillament de xarxes.

• Autentificació, suport per (Microsoft Active Directory, Novell eDirectory, OpenLDAP, CISCO ACS Radius(FreeRadius, Radiator, etc), Local user File).

Estàndars suportats:

• 802.1x

• Simple Network Management Protocol(SNMP).

• Estàndar SNMP managament information base(MIB) com BRIGE-MIB, Q-BRIGE- MIB, IF-MIB, IEEE8021-PAE-MIB

• Radius

• Network/IPFIX

• Wireless ISP Roaming(WISPR)

5.2. Definició de l'arquitectura del sistema.

A continuació descriurem l'arquitectura del sistema, está definida en dos nivells un funcional i l'altre lògic.

5.2.1. Arquitectura funcional.

En la Ilustració 3, es veuen els blocs dels sistema, sense entrar en detall e identificant les relacions entre ells, és útil per tenir una visió global del sistema.

El client(workstations), se connecta a la xarxa i proporciona un conjunt de credencials que es validen per autentificar i autoritzar el nivell apropiat d'accessos a la xarxa. Aquestes credencials del client inclouen credencials d'identificació d'usuari i equip, a més de les credencials en bon estat, després dels escaneigs. Els clients que compleixen se posen en quarantena, se tracten de manera similar abans de concedir-lis l'accés normal a la xarxa, en el nostre cas se'ls posara fora de la xarxa administrativa, aniran directament a la xarxa d'aïllament, que es internet.

Segons els tipus d'autentificació que podrá ser: 802.1x i EAP, portal captiu, o basad amb mac. El switch envia les dades del client que es vol connectar al servidor packetfence, EAP sobre radius, les credencials de l'usuari es validen en la base de dades d'autentificació, el servidor del packetfence, redireccionar l'usuari que es vol identificar a la VLAN que li pertoqui en funció de si aquest usuari compleix les regles establertes.

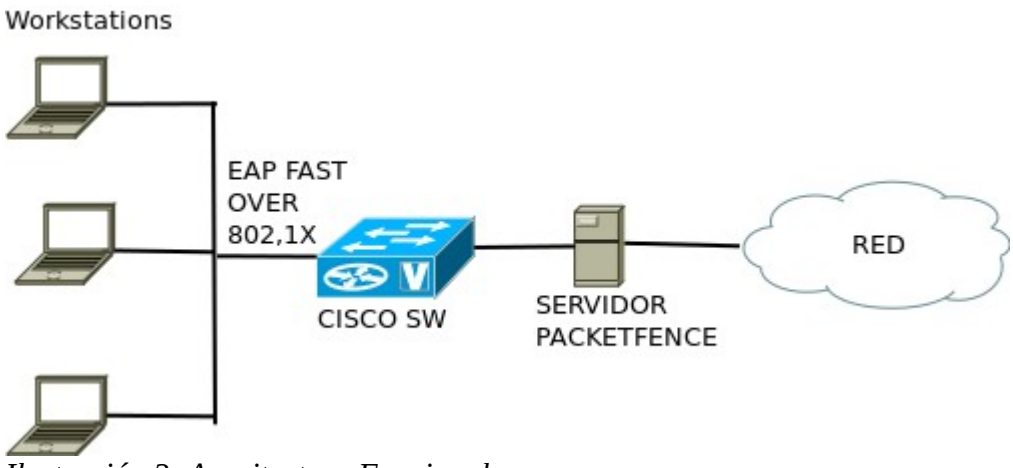

Ilustración 3: Arquitectura Funcional

5.2.2. Arquitectura lógica.

En l'arquitectura lógica, de la ilustració 4, detalla l'anterior i incorpora els detalls de la interacció de

cada un dels subsistemes(blocs), que permetran a cada desenvolupador trevallar preocupant-se només de la feina encarregada.

El packetfence es pot configurar com VLAN Enforcement o Inline:

- VLAN enforcement es per assignar les diferents vlans als usuaris en funció de les regles establertes.
- Inline, es per el cas de que vulguem que funcioni el packetfence com un gateway o router.

En aquest cas, treballara amb les tècniques d'assignació de Vlan, estarà configurat com a Vlan Enforcement, això vol dir que Packetfence es el servidor que assigna les VLAN a cada dispositiu. Aquestes VLANs poden ser les nostres o una especial que el packetfence tengui el portal captiu per autentificar-se els usuaris.

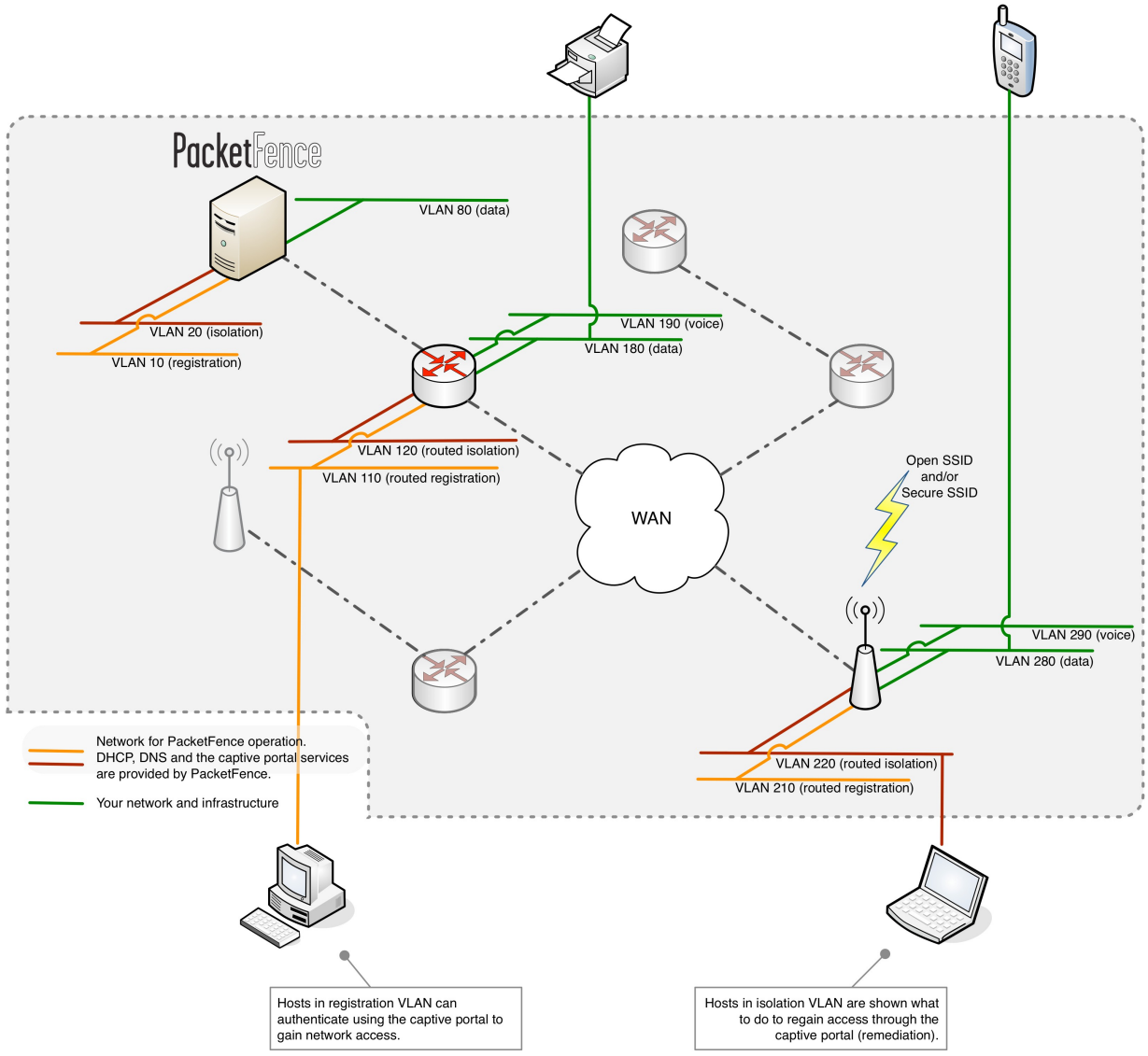

Ilustración 4: Arquitectura lógica

5.3. Especificacions d'estàndards, normes de disseny i construcció

En un directori comú de l'empresa, tenim definides unes series de carpetes, on es pot trobar tota la informació de les plantilles que s'han de seguir per fer els documents de projecte, siguin aquets:

- Document de requeriments i anàlisi.
- Document de seguiment de projecte.
- Document de disseny.
- Diagrames de disseny.

- Documentació tècnica.

Cal dir que tots aquets documents i carpetes cumpleixen l'estandar de l'empresa, amb la nomenclatura definida.

Està compost per la següent estructura de directoris, aixins com les plantilles a utilitzar:

- DES - Desenvolupament
  - ASA – Anàlisi del Sistema Actual
    - _DESASA_Anàlisi del sistema actual
  - ERP – Evaluació i Recomendacions de Productes
    - RFP - Request For Proposals
      - _DESERPRFP_RequestForProposal
    - IRP - Informe Recomendació Producte
      - _DESERPIRP_InformeRecomendacióProducte
    - DCE - Definició Criteris Evaluació
      - _DESERPDCE_DefinicióCriterisEvaluació
    - DAP - Documentació Aportada Proveedor
      - _DESERPDAP_DocumentacióAportadaProveedor
    - ADP - Análisi Detallat Producte
      - _DESERPADP_AnàlisiDetallatProducte
  - AIP Adquisició e Instalació de Productes
  - ANS - Análisis Necesitats Sistema
    - EFN - Especificació Funcions Negoci
      - _DESANSEFS_EspecificacióFunciónNegoci
    - MAA - Model Arquitectura Aplicacions
      - _DESANSMAA_DefinicióInterficiLògica
      - _DESANSMAA_ArquitecturaAplicacions
        - _DESANSMER_ModelEntitatRelació
        - _DESANSMPN_DiagramaProcesNegoci
        - _DESANSREQ_CatálegRequeriments
        - DFS - Diseny Funcional Sistema
        - _DESDFSEFS_EspecificacióFunciónNegoci
        -
        - _DESDFSMAA_DefinicióInterfaceLògica
        - _DESDFSMAA_ArquitecturaAplicacions
        - _DESDFSMER_ModelEntitatRelació
        - _DESDFSMPN_DiagramaProcesNegoci
        - _DESDFSMCD_PlanMigracióConversió
        - _DESDFSMCD_DefinicióProcesMigració
        - _DESDFSREQ_CatálegRequeriments
        - _DESDFSDFD_Diagrama de fluxe de dades
        - PAI - Planificació Arquitectura Tecnológica e Infraestructura
        - _DESPAIMAT_InfraestructuraTecnológica
        - _DESPAIMAT_ConfiguracióArquitectura

- _DESPAIPSA_Seguretat i Acces
- _DESPAIRAL_RelacióAspectesLegals
- DPO - Desarrollo Procediments Operació
- _DESDPODPC_DefinicióPlansContingència
- _DESDPOMDU_ManualsDeUsuari
- _DESDPOPOE_ManualExplotació
- _DESDPOPOE_ProcedimentOperació
- DTS - Diseny Técnic Sistema
- _DESDTSDTI_DefinicióInterfaceFísica
- DESDTSDVS - DefinicionFinestresSistema
- DESDTSDPS - DefinicióFuncions-ProcedimentsSistema
- DESDTSDNV - DiagramaNavegacióFinestres
- ESDTSDIS - DefinicióInformesSistema
- _DESDTSMDF_ModelDadesFísic
- _DESDTSDMD_DefinicióMigracióDades
- DCS – Desenvolupament Components Sistema
- PCP – Paramertrització i Configuració del Producte
  _DESPCP_ConfiguracióDelProducte
- PAS - Proves Aceptació
- _DESPASCPR_CasosProva
- _DESPASIEP_InventariErrorsPrograma
- _DESPASJPR_JocsProva
- _DESPASPPR_PlaProves
- IMP – Implantació
- _DESIMPPIS_PlaImplantacióSistema
- _DESIMPPMS_PlaManteniment
- _IMPSGU_Alta Usuaris SAP
- _IMPSGU_Baja Usuaris SAP
- _IMPSGU_Modificació Usuaris SAP

El nom de cada un dels nous documents a registrar dins de l'estructura de carpetas deu de complir els estándars de nomenclatura fixats en SS.II.

5.4. Identificació dels subsistemes.

En el nostre cas tenim com components o subsistemes tenim:

- 7 switches funcionant a Palma i a Madrid ni ha 8.
- Switch Cisco Catalytic 3560 i 2960.
- Administrats via SNMP v3
- Que configuren les N xarxes de l'empresa
- Servidor de RADIUS, encara que al laboratori hem utilitzat el que ve amb el paquet.
- Servidor Active Directory (LDAP de MHI).
- Servidor (actualment de laboratori) a on hem instalat el NAC Open source
    - Centos 6.x.
    - Packet Fence versió 4.0.6
    - Servidor configurat com a trunk amb les següents interficíes: VLAN6 és la VLAN "normal" (1), VLAN400 és la VLAN “registre”(2), VLAN9 és la VLAN “Isolation”(3) d'aillament, VLAN404 és la VLAN “MAC detection”(5), VLAN 4 s'ha de definir en tots els switches que no soporten port-security, VLAN 666 és la VLAN “management” (4).
    - El servidor DHCP se encarregarà de la distribució d'adreçes IP en la VLAN 2 y 3.
    - El servidor DNS se fará carrec de la resolució de dominio en xarxer VLAN 2 y 3.
- Equips de Windows XP de l'empresa on es conectaran per autentificar-se mitjançant el portal captiu a la xarxa.
- Equips portàtils de clients que venguin a l'empresa i s'autentifiquin per conectar-se a la xarxa de l'empresa, ja sigui mitjançant el portal captiu, mitjançant 802.1x, o mac.

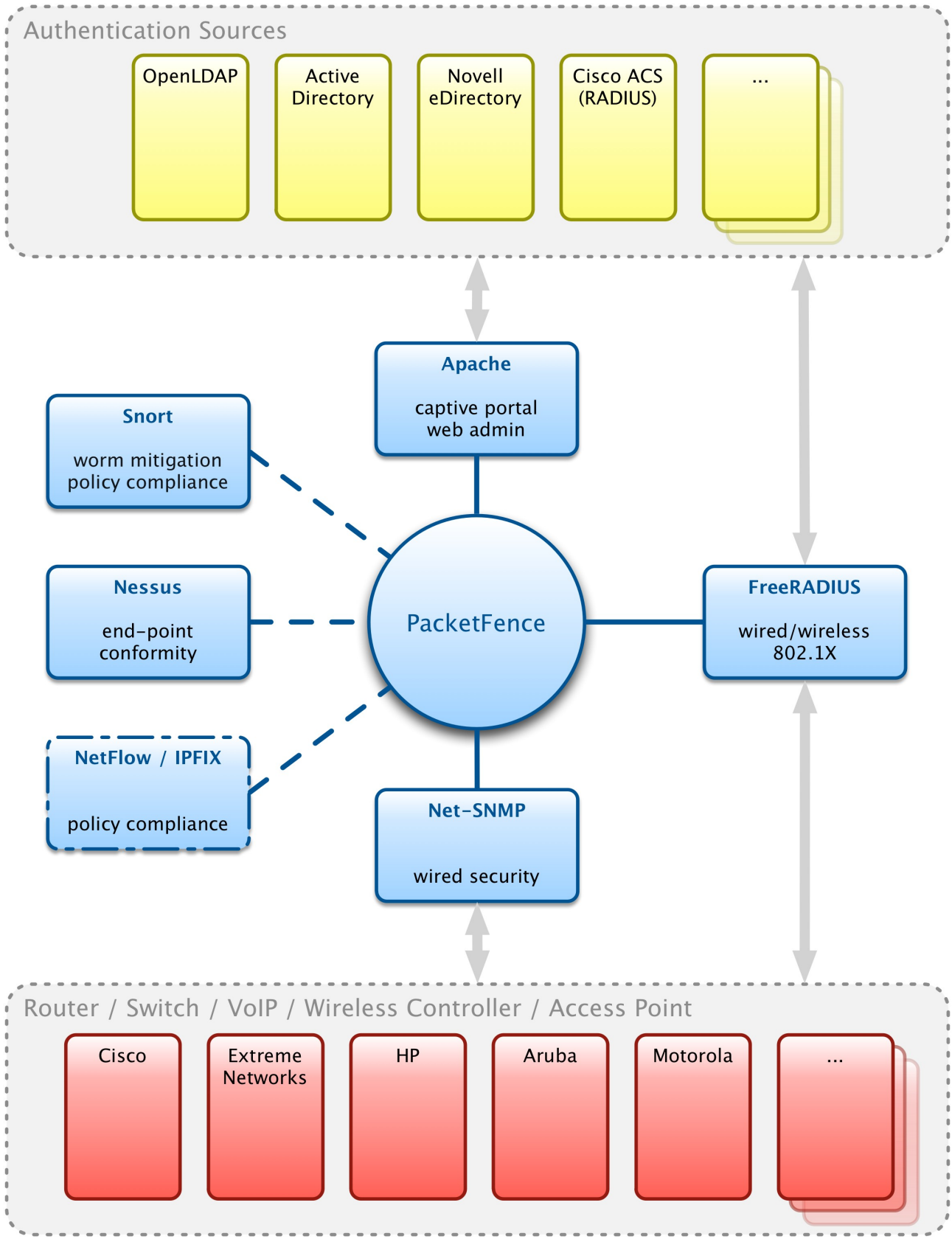

Ilustración 5: Components del Packetfence

5.5. Casos d'us real

Els casos d'us real es poden veure en els vídeos pujats a l'eina Present@:

Cas 1. Dispositiu no reconegut que s'identifica contra autenticació local i queda a la xarxa de convidats. L'usuari es connecta a la xarxa de l'empresa, el NAC detecta a aquest usuari, el força a registra mitjançant el portal captiu, en el portal haurà de posar el usuari de "guest", i accedir a la xarxa corresponent pels convidats.

Cas 2. Dispositiu no reconegut que s'identifica contra autenticació LDAP i queda connectat a la xarxa d'empleats. L'usuari es connecta a la xarxa de l'empresa, el NAC detecta a aquest usuari però en lloc d'entrar com usuari convidat entra com usuari empleat, se comprava que pertanys a l'empresa aquest usuari mitjançant el LDAP, i entra a la xarxa d'empleats.

Cas 3. Dispositiu reconegut que es reconnecta a la xarxa i aleshores l'assignació de VLAN es automàtica. L'usuari empleat, ja està registrat i no cal tornar a identificar-se una vegada ja s'han emmagatzemat l'usuari/password ja que el reconeix, i segons les regles no cal que es torni a identificar fins que arribi la data d'expiració amb lo que automàticament et deixa a la xarxa d'empleats.

5.6. Especificacions de desenvolupament i proves.

Seguint les guies de hardenització de l'empresa, el servidor a on instal.lem el NAC haurà d'aplicar les següents polítiques:

- Deshabilitar protocols insegurs en aquest cas per gestió(HTTP, Telnet, SNMPv1 ó SNMPv2, SSHv1).
- Utilitzar criptografia robusta.
- Control de canvis.
- Reenviar logs en el servidor centralitzat.
- Registre de logs d'accés i accions administratives damunt del software.

• Sincronització del rellotge mitjançant NTP intern.

• Eliminar serveis innecessaris.

• Escanejos trimestrals mitjançant l’eina Qualys amb la finalitat de no tenir vulnerabilitats amb CVS.

• La gestió del software unicament es pot fer mitjançant una subxarxa administrativa i l’usuari ha d’estar donat d’alta en el servidor Radius i pertànyer un determinat grup administrador de switches.

• Revisió semestral dels serveis habilitats.

• Revisió semestral de usuaris amb accés al software.

• Canvi de valors predeterminats pels proveïdors abans d’instal.lar un sistema a la xarxa.

En el nostre cas es tracta de montar un petit laboratori, per no cometre errades que puguin tirar enterra la xarxa de l'empresa, amb lo que se tendran que crear dues vlans noves i configurar un switch que ara mateix no es fa servir:

- PC, que sigui un trunk amb lo que s'ha de configurar com a tal, se li definira les següents eth(ethernet): eth0, eth0:6, eth0:666, eth0:400, eth0:9, eth:404.
- S'haura de tenir configurat un switch adicional per fer les proves, pel laboratori, hem posat en marxa un switch que estarà configurat amb les vlans que ha de menester per la configuració, ja que el packetfence, obliga a tenir definides cinc tipus de vlan:
    1. vlan de registre(vlan 400): la vlan de registre és on es coloquen els dispositius no registrats automàticament per el packetfence, com un àrea d'espera fins que estiguin registrats i validats per un conjunt de normes i requeriments.
    2. vlan de isolation(vlan 9): és la vlan on les màquines que no cumpleixen les regles que hem establert estiran.
    3. vlan de managament(vlan 666): aquesta es la vlan d'administració.
    4. vlan normal. (vlan 6): aquesta es la vlan de pc's.
    5. Vlan mac detection (vlan 404) : aquesta es la de detecció de mac.

El cas que ens ocupa es la configuració VLAN enforcement, ja que noltros no farem servir la Inline enforcement.

Abans de configurar l'eina de Packetfence, tenim que configurar les vlans que hem de

manester i el switch.

Una vegada configurada l'eina tal com se detallarà en l'apartat de manual de l'usuari que s'afeguirà com annexe d'aquesta memoria. Es tracta de fer proves amb les conexions del nodes que volem authentificar i redirigir aquests en funció dels rols d'usuari definits en els perfils.

La infraestructura de xarxa del laboratori esta formada:

- Switch Cisco Catalytic 3560.
- VLAN6 és la VLAN "normal" (1) - els usuaris amb el rol de "default" s'asignaran a la mateixa.
- VLAN400 és la VLAN “registre”(2)- els dispositius no registrats seràn posats en aquesta VLAN.
- VLAN9 és la VLAN “Isolation”(3) d'aillament – els dispositius aisllats seràn posats en aquesta VLAN.
- VLAN404 és la VLAN “MAC detection”(5)
- VLAN 404 ha de definir en tots els switches que no soporten port-security.
- VLAN 666 és la VLAN “management” (4).
- El servidor DHCP se encarregarà de la distribució d'adreçes IP en la VLAN 2 y 3.
- El servidor DNS se fará carrec de la resolució de dominio en xarxer VLAN 2 y 3.

Taula de Configuració de Xarxa – Servidor PacketfenceLab.

VLAN ID	VLAN Name	Subnet	Gateway	PacketFence Address
Vlan6 (1)	Normal(Default)	172.17.9.128/25	172.17.9.129	172.17.9.134
Vlan400 (2)	Registration	192.168.2.0/24		192.168.2.3
Vlan9 (3)	Isolation	192.168.1.0/24		192.168.1.2
Vlan666 (4)	Management	172.17.8.0/26		172.17.8.24
Vlan404 (5)	MAC Detection	-	-	-

La tècnica d'assignació de la VLAN per defecte que s'utilitza en Packetfence es per switch. La VLAN per defecte correcta per una MAC donada se determina basant-se en el role(guest o treballador) del Packetfence durant el proces de registre per al dispositiu, o dinàmicament durant una autenticació 802.1x.

Els roles es defineixen en el PacketFence, des de la Interfície Administrativa, tal com es mostren en la següent il·lustració:

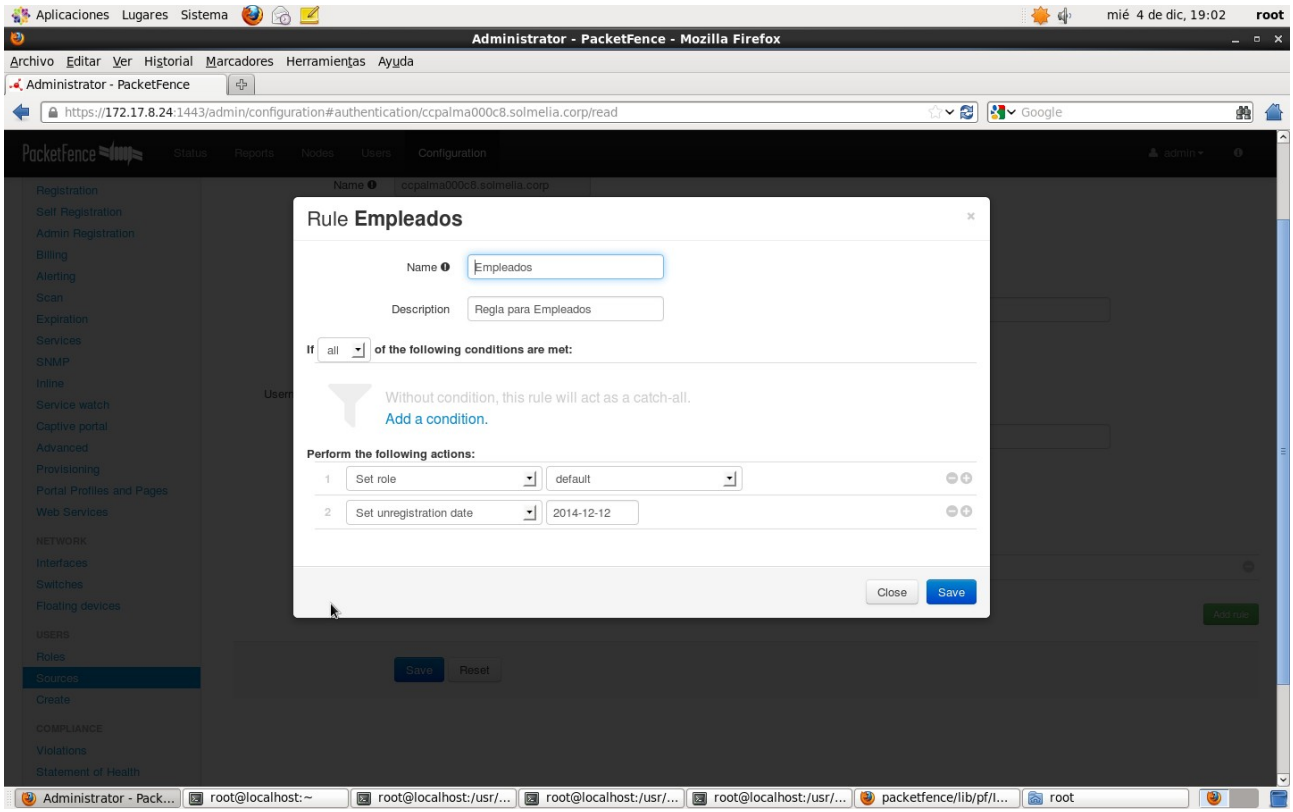

Ilustración 6: Roles d'usuaris que siguin empleats

En el projecte es defineixen dos roles, els de usuaris empleats, i els d'usuaris convidats(guests).

L'usuari convidat tindrá el role guest, que el que te asignat es la VLAN 9, que es la d'aillament i una vegada autentificat te sortida directa cap a internet. En la següent ilustració se detalla la definició de l'usuari guest:

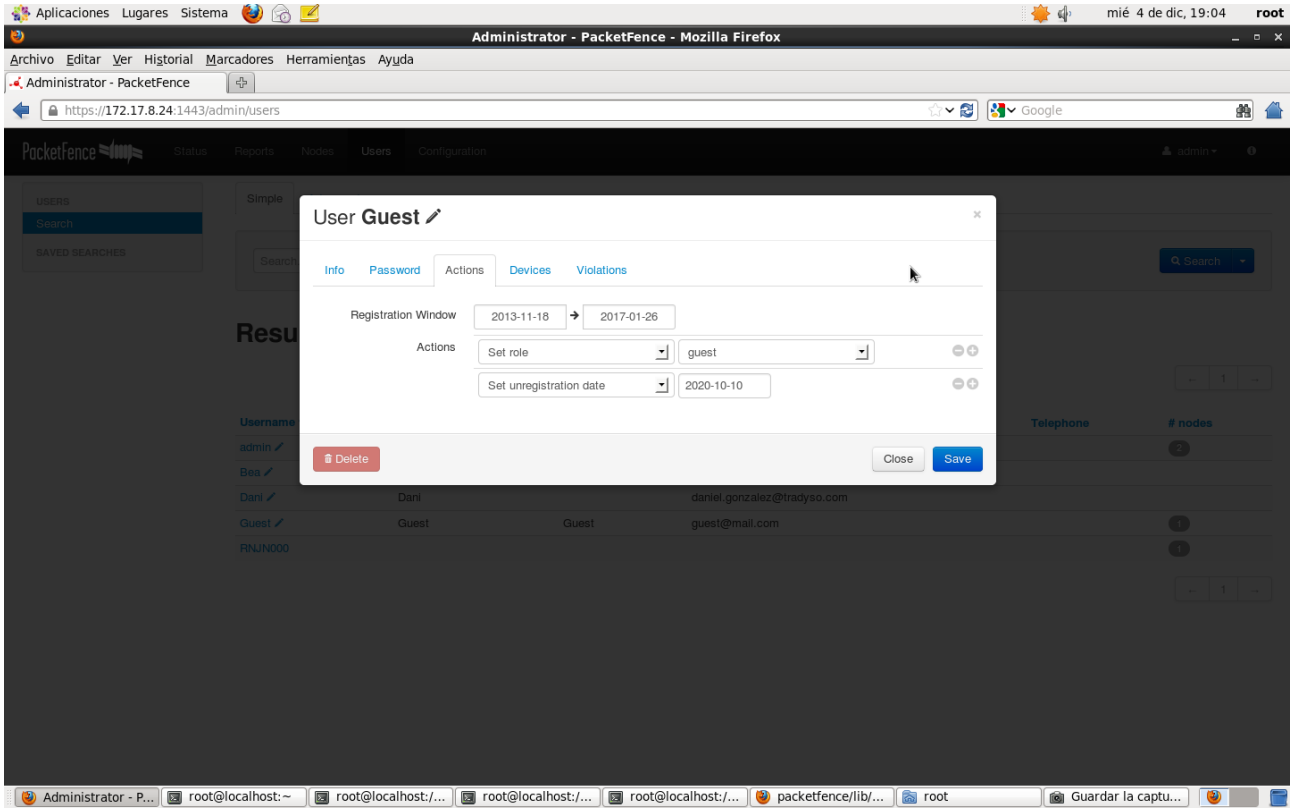

Ilustración 7: Definició d'usuari Guest

En la configuració del switch s'estableix una asociació amb els roles que hi ha definits per cada VLAN.

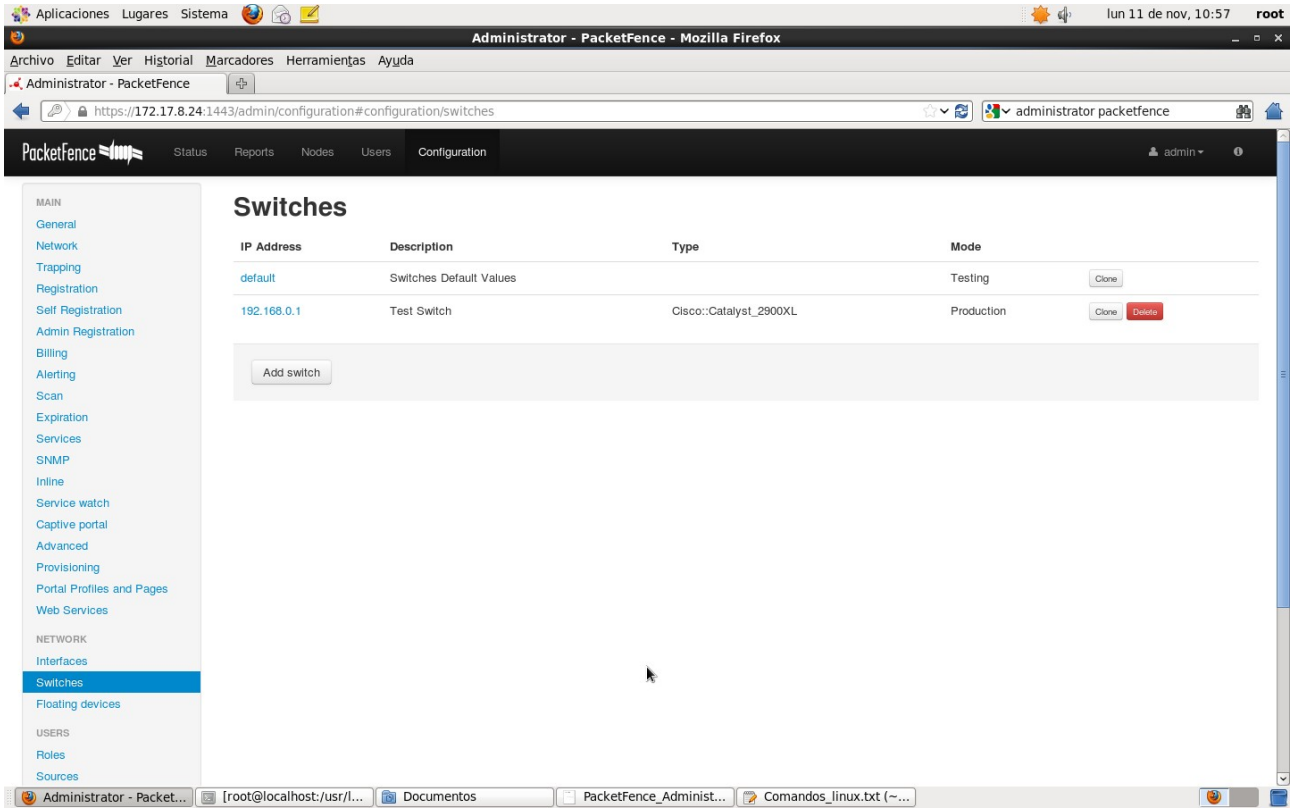

Ilustración 8: Configuració del switches

Per autentificar els usuaris empleats mitjançant LDAP i els usuaris convidats(guests) en la base de dades interna del Packetfence, tot dos mitjançant el portal captiu. S'ha de crea el source de l'usuari, seleccionant OpenLDAP tal com es mostra a l'ilustració següent:

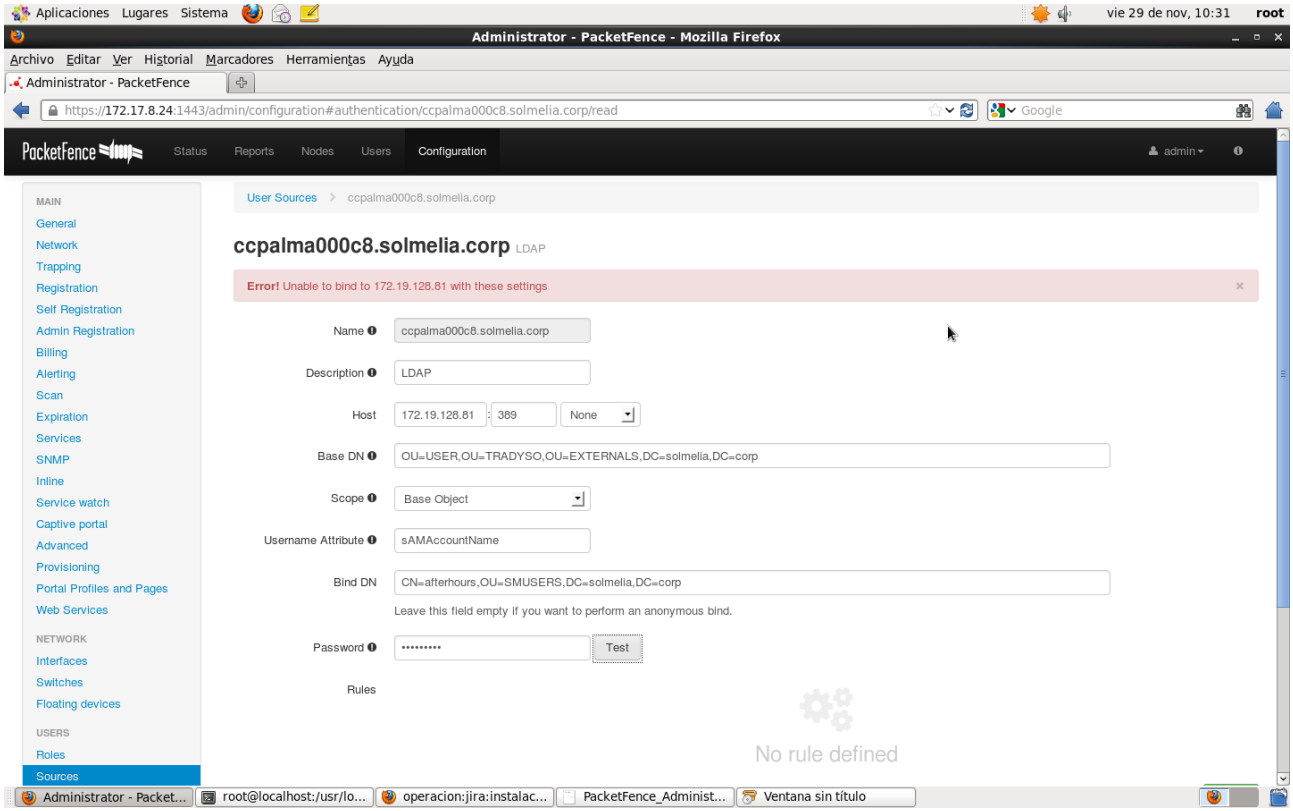

Ilustración 9: Afegir source LDAP

S'ha de facilitar la següent informació:

- Nom del source.
- Descripció
- Host
- Base DN
- Scope: Subtree
- Username atributte
- Bind DN
- Password

Apart de LDAP, també hi ha definit el source de Apache htpasswd file.

5.7. Requisits d'implantació.

En en el nostre cas per la implantació tindrem en conta els components o subsistemes que s'han esmentat en l'apartat 5.4. Identificació dels subsistemes.

Els requisits d'implantació seràn els que hauran de complir per cada component quan es treballa en l'entorn real, s'han de determinar les condicions de l'entorn en el qual s'implantarà la NAC.

Aleshores, els requisits per implantar el laboratori a la xarxa de l'empresa siràn:

- Definir les VLANs que s'han de menester, en el nostre cas són vlan normal, la d'aillament, la de management, i la de registre.
- Instal.lar el packetfence en un servidor, configarar-ho amb les vlans esmentades abans, segons els documents annexats.
- Configurar el switch, Switch Cisco Catalytic 3560.
- Instal.lar els certificats en el servidor del packetfence.
- Tenir usuari per validar contra LDAP de l'empresa, per aquest pas, s'ha de customitzar el packetfence, ja que per defecte no ve amb la opció de validar contra directory actiu. Les customitzacions fetes estan al manual técnic d'usuari annexat a la memòria.
- Definir les regles dels usuaris per empleats i guest.
- Establir condicions per l'acces d'aquests usuaris.
- Tenir inventari de les macs de l'empresa, i els usuaris creats per asociar-ho a aquestes macs. L'inventari de les macs s'obte, executan des del servidor de packetfence, un script tal que:

  import-node-csv.pl

  aquest script li pases un fitxer amb la informació de les macs, el nom d'usuaris, etc, i quan s'executa s'importen les macs dels usuaris creats previament en el packetfence.

6. Recursos Econòmics.

Es important determinar l'esforç econòmic que pot suposar el realitzar la implementació d'una Nac i contrastar-ho amb el cost que suposaria un sistema íntegrament compost de software privatiu.

El que millor reflexarà el cost econòmic sirà el TCO, Total Cost of ownership, defineix el cost total de propietat d'una tecnologia concreta sobre el periode de vida útil.

Els components que formen el TCO son tots aquells costos que se produeixen com conseqüència de la introducció d'una tecnologia. A grans trets se pot xerrar de dos tipus de costos, els directes e indirectes. Els costos directes, normalment, son aquells costos coneguts i que impliquen una contraprestació econòmica. Per una altra banda, els costos indirectes son els que no tenen una contraprestació econòmica coneguda i no son tan fàcilment identificables com els costos directes.

6.1. Costos Directes.

6.1.1. Llicències i suport de software.

En aquest apartat, donat que emplearem una aplicació de software lliure, el cost de la llicència sirà null, ja que el PacketFence, es basa en una llicència GNU General Public *License* version 2.0 (GPLv2). En aquest cas el suport depen completament de la comunitat de software lliure i del personal ben qualificat del que disposa en plantilla l'empresa.

6.1.2. Costos de hardware.

La major part de distribucions linux son capaçes d'executar-se sobre hardware vell, depenguen de les necessitats i exigencies del software que hem de fer servir, però aixi i tot, els requisits de memòria son minims i es poden fer servir màquines velles.

En el nostre cas hem fet servir per les proves del laboratori un pc vell, que s'havia donat de baixa, on s'ha instal.lat el Centos, que te llicència lliure, i no cal pagar llicència. A més s'ha fet servir, un switch Cisco 3560 que ja teniem, i que no s'utilitzaba.

Si que cal dir que per la posta en producció s'haurà de comprar un servidor.

6.1.3. Costos de soport.

L'empresa te un departament de noves tecnologies ben qualificat, amb el que pot donar soport per el manteniment de l'aplicació i la seva gestió.

6.1.4. Costos de formació.

Els costos de formació serán les despeses de redactar l'anexe pels usuaris, i explicar com poden aquests conectar-se.

6.1.5. Costos de personal.

El projecte s'ha duit a terme, amb el personal del departament de Sistemes de Informació, que s'ha encarregat de la posta en marxa de la NAC de Packetfence, de la seva configuració i administració.

6.2. Costos indirectes.

Aquest tipus de costos son els més impredecibles. De totes maneres podriem dir que un cost indirecte siria la inoperativitat del sistema.

Existeixen moltes causes per les que el sistema pot queda inoperatiu, però direm que si no se configura adequadament l'eina de Packetfence, el sistema de xarxes pot queda inoperatiu, i aleshores, no tendriem conexions de xarxes segures pels usuaris, això implicaria que no es podria gestionar la seguretat de l'empresa correctament.

Es pot donar el cas de que:

- no autentifiqui els usuaris contra LDAP.
- no accedesqui a la vlan que li correspongui segons les regles establertes.
- que se'n vagi la corrent, el SAI caigui, i aleshores el servidor no estigui operatiu.
- Al actualitzar el software se desconfiguri la NAC i no funcioni correctament.

6.3. Total costos.

Costos Incorreguts			
Concepte	***Hores***	***Import***	***Despeses***
Hores i Despeses de SS.II.	260	38,39	9981,4
Maquinari (nou servidor)			2000
Entorn de desenvolupament(tarifa porrateada)	260	6,7	1742

Totals			
Total Hores i despeses fetes			4990,7
Total Hores i despeses pendents			8732,7
Total Inversió fins finalització			13723,4

Hem de dir que si haguessim triat una aplicació privativa per portar a terme el projecte, com per exemple Symantec Network Access Control (SNAC) , s'ha de contactar amb el departament de ventes per sebre el cost de la llicència extra del producte, i del suport. Això implicaria un cost adicional al calculat en la taula de costos.

7. Conclusions

7.1. Resultats

Els resultats obtinguts fins al moment son els següents:

- Tenim un inventari de les MACs dels dispositius de l'empresa, tant de Palma com de Madrid.
- Detectar que un dispositiu es connecta a la xarxa i situar-lo al segment de xarxa que pertoqui.
- Canviar la configuració dels switchos de manera automàtica per tal d'aconseguir el punt anterior.

En quan respecte als mecanismes d'autentificació actualment s'aconsegueix autentificar per:

- 802.1x
- Mac Detection.
- Combinació de tot dos.

PacketFence pot autenticar als usuaris que es registrin els dispositius a través del portal captiu utilitzant diversos mètodes. Entre els mètodes admesos hem probat:

- Apache htpasswd file .
- LDAP (autentificar els usuaris contra LDAP.

El projecte pretenia dur-se a terme en un plaç de dos mesos, en els quals a part de muntar el

laboratori e implementar-ho, també es pretenia implementar la NAC en producció a la xarxa corporativa de Palma i Madrid, a més integrar l'eina de qualys amb packetfence.

Hem aconseguit demostrar que posar en marxa el laboratori es factible, que seria una eina de software lliure customitzada pel requisits que ha de menester l'empresa per ser complir la normativa PCI DSS de seguretat.

Tenim penden implementar-ho en producció, tot depen de les decisions finals dels caps de seguretat, però estan contents amb el que s'ha aconseguit.

La integració de l'API de qualys amb packetfence, esta pendent, no s'ha pogut dur a terme perque se tenia que customitzar els escanetjos, per defecte te deixa configurar i customitzar el Packetfence amb OpenVas i Nessus.

7.2. Conclusions

De les posible solucions actuals en el mercar, s'ha optat amb aquesta perque es la més econòmica, es una solució basada amb Linux i d'altres empreses que l'han fet servir els hi han donat bons resultats. A més ha quedat demostrat que després de les proves fetes en el laboratori cumpleix els nostres objectius principals independenment que estiguen en proves de qualque punt.

Cal dir que el soport s'obte de la comunitat d'usuaris en el cas de que un no trobi la sol.lució dels seus problemes en la guia de l'administrador, i això comporta un poc de retràs ja que depen de la bona intenció dels usuaris de la comunitat el que t'atenguin ràpid i et donin el soport tècnic adequat.

Reconec que hi ha manca documentació, ja que hi ha casos que en la guia de l'administrador del packetfence no se comenten, i et diu “to be contributed”.

Comentar que els desviaments de les tasques s'han degut principalment a falta de recursos, de documentació, vaig perdre temps en la configuració del laboratori, ja que per instal.lar el sistema operatiu, vaig començar amb Ubuntu, però després d'una serie d'errors vaig triar Centos, amb això me vaig retrasar una setmana. Després amb la configuració del servidor Packetfence, també vaig tenir problemes per configurar-ho i customitzar-ho ja que no hi havia documentació sobre l'autentificació contra LDAP. Respecte a les qüestions que vaig obrir en la comunitat d'usuaris, tinc que dir que me varen anar contestant però no varen resoldre tots els meus dubtes, tinc que dir que

amb una de les meves darreres consultes me varen suggerir d'instal.lar la darrera versió del PacketFence, que va sortir el 11 desembre, la versió 4.1.0., però vist que durant la primera setmana, tot eren problemes per fer l'update de la darrera versió, no me vaig veure amb anim de provar de instal.lar-la , ja que això implicaria més retràs en el projecte, degut a que has de tornar a customitzar els programes, del Packetfence, i a part, has de resoldre nous problemes.

El projecte m'ha aportat els següents coneixements de configurar un NAC, el radius, els traps, les interficies, la xarxa, el switch, sebre instal.lar els certificats, gestionar un projecte, entendre que no sempre se pot arribar a l'abast del projecte, depenen dels problemes que sorgeixen, sebre quin carreg ocupa els companys, millor comunicació.

Satisfacció per veure que hi ha gent interesada amb aquest projecte i que si se poguès posar en producció se podria dur a terme a altres sectors, encara que hi hagi companys que només afegeixen problemes al seu desenvolupament i posada en producció .

7.3. Posibles millores.

En aquest apartat es veuran possibles millores que podrien fer-se a l'eina de Packetfence, com al projecte en general:

- Configurar i customitzar els escanetgos amb Qualys, en lloc d'utilitzar Nesus i Openvas.
- A part, d'implementar el NAC a l'empresa, es podria suggerir d'implantar als hotels, ja que s'ha donat el cas, de que en els hotels connecten dispositius que poden col·lapsa la xarxa de l'empresa o tirar-la enterra.

8. Referències bibliogràfiques

Bibliogràfica

- Guía del segundo año de CISCO System.(CCNA).
- Implementing NAP and NAC Security Technologies by Hoffman Daniel V.
- PacketFence_Administration_Guide-4.0.6.pdf
- QualysGuard_API_v2_User_Guide.pdf
- PacketFence_Network_Devices_Configuration_Guide-4.0.6.pdf

Fonts web

http://www.packetfence.org/ pàgina oficial de Packetfence

http://www.cisco.com/ pàgina oficial de Cisco

http://www.symantec.com/ pàgina oficial de Symantec

9. Annexes

9.1. Manual técnic d'usuari.

9.1.1. Requisits mínim d'instal.lació del Packetfence

Requisits mínims del sistema:

Hardware

Llista de requisits mínims de hardware del servidor:

- Intel o AMD CPU 3 Ghz
- 4 GB de RAM
- 100 GB spai de disc
- 1 tarjeta de xarxa

Sistema Operatiu suportat

PacketFence suporta els següents sistemes operatius en arquitectures i386 o x86_64:

- Red Hat Enterprise Linux 6.x Server
- Community ENTerprise Operating System (CentOS) 6.x

- Debian 7.0 (Wheezy)
- Ubuntu 12.04 LTS

En el projecte s'ha fet servir Centos 6.4. per arquitectura i386.

9.1.2. Instal.lació del Packetfence.

S'ha d'instal.lar una distribució mínima sense paquets addicionals. S'ha de tenir deshabilitat el següent:

- Firewall

El sistema ha d'estar actualitzat, per tant, abans de començar amb la instal.lació hem de fer un:

```
yum update
```

S'ha d'instal.lar els següents repositoris en yum:

- Repoforge
- EPEL
- OpenFusion

```
#wget http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.2-2.el6.rf.i686.rpm
#wget http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm
#wget http://rpms.famillecollet.com/enterprise/remi-release-6.rpm
#sudo rpm -Uvh remi-release-6*.rpm epel-release-6*.rpm
# rpm -Uvh http://repo.openfusion.net/centos6-i386/openfusion-release-0.6.2-1.of.el6.noarch.rpm
Retrieving http://repo.openfusion.net/centos6-i386/openfusion-release-0.6.2-1.of.el6.noarch.rpm
warning: /var/tmp/rpm-tmp.21ssfQ: Header V4 DSA/SHA1 Signature, key ID 2a6b914a: NOKEY
Preparing...                ########################################### [100%]
   1:openfusion-release     ########################################### [100%]
[root@smtmobile572068 ~]# ls /etc/yum.repos.d/
CentOS-Base.repo       mirrors-rpmforge-extras
CentOS-Debuginfo.repo  mirrors-rpmforge-testing
CentOS-Media.repo      openfusion.repo
CentOS-Vault.repo      remi.repo
epel.repo              rpmforge-release-0.5.2-2.el6.rf.i686.rpm
epel-testing.repo      rpmforge.repo
mirrors-rpmforge

# ls -1 /etc/yum.repos.d/epel*

/etc/yum.repos.d/epel.repo

/etc/yum.repos.d/epel-testing.repo
```

```
/etc/yum.repos.d/openfusion.repo
/etc/yum.repos.d/rpmforge.repo
```

Aleshores deshabilitam els repositories per defecte. En el directori /etc/yum.repos.d/ editam el fitxer rpmforge.repo, epel.repo i openfusion.repo i posam enable=0 en cada secció.

```
enabled= 0
```

S'exclou perl-Apache-Test del reposiroti rpmforge i penfusion

```
#  Vi /etc/yum.repos.d/rpmforge.repo
```

S'afegeix la linea exclude = perl-Apache-Test* en la seció rpmforge

```
#  Vi /etc/yum.repos.d/openfusion.repo
```

S'afegeix la linea exclude = perl-Apache-Test*

Aleshores, s'ha de crear el fitxer anomenat Packetfence.repo en el directori :

```
   /etc/yum.repos.d/PacketFence.repo
```

amb el contingut següent:

```
name=PacketFence Repository
baseurl=http://inverse.ca/downloads/PacketFence/RHEL$releasever/$basearch
gpgcheck=0
enabled=0
```

Instal.lam el PacketFence amb totes les seves dependencies:

```
yum groupinstall --enablerepo=PacketFence,epel,rpmforge,of Packetfence-complete
```

A continuació se detalla com se configura el PacketFence. El PacketFence utilitza MySQL, Apache, ISC DHCP, iptables i FreeRADIUS. Tots aquests components han d'executar-se en el mateix servidor que el Packetfence.

9.1.3. Configuració del Packetfence.

Configuram el Packetfence, en la url següent https://@ip_of_packetfence:1443/configurator.

Pas 1. Enforcement.

Seleccionam el tipus de xarxa que tindrem:

- Inline enforcement.
- Vlan enforcement.

En el nostre cas serà vlan enforcement, ja que tenim una xarxa composta per n vlans.

PacketFence no se iniciarà a menys que tengui al menys una interfaç interna, per lo que necessita per crear el registre local(tipus xarxa register) i VLANs aillament(tipus isolation), inclus si no tenim intenció de fer-los servir. A mes, les interficis internes son les úniques en les que dhcpd escolta, per lo que el registre remot i subxarxes d'aisllament deuen senyalar amb el helper-address DHCP a les IPs particulars. Després s'ha de proporcionar la informació de xarxes enrutades a PacketFence. Aquest se pot fer mitjançant la interficie gràfica d'usuari en xarxes d'administració.

Pas 2. Network.

En aquest pas hi ha que configurar les vlan que tenim, en el nostre cas, son:

- vlan 9. Tipus guest, e isolation.
- vlan 400. Tipus registro.
- Vlan 6. Tipus normal.
- Vlan 666. Tipus management.

Pas 3. Base de Dades.

En aquesta finestra se te que posar l'usuari/password de mysql, crear la BBDD de packetfence, i la conta.

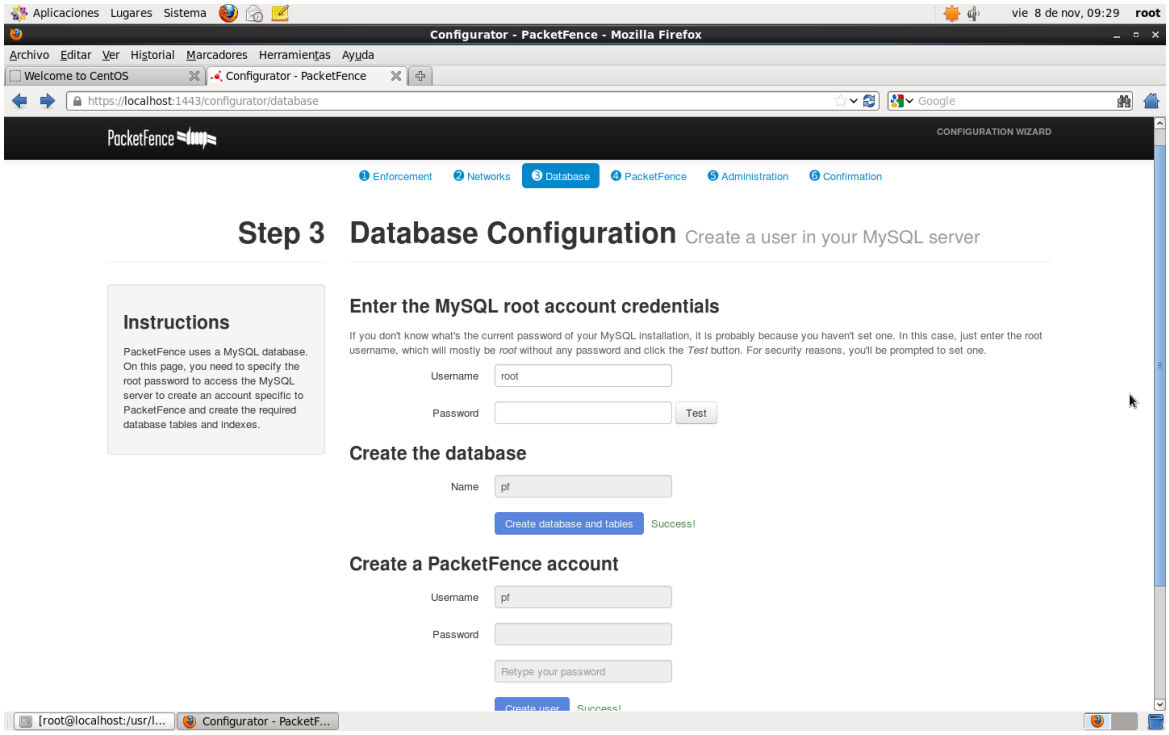

Ilustración 10: Configurar_BBDD_PacketFence

Pas 4. Configuració PacketFence.

Introduim les sigüents dades per configurar el NAC:

- nom del domini.
- Hostname.
- DHCP server.
- email per les alertes.

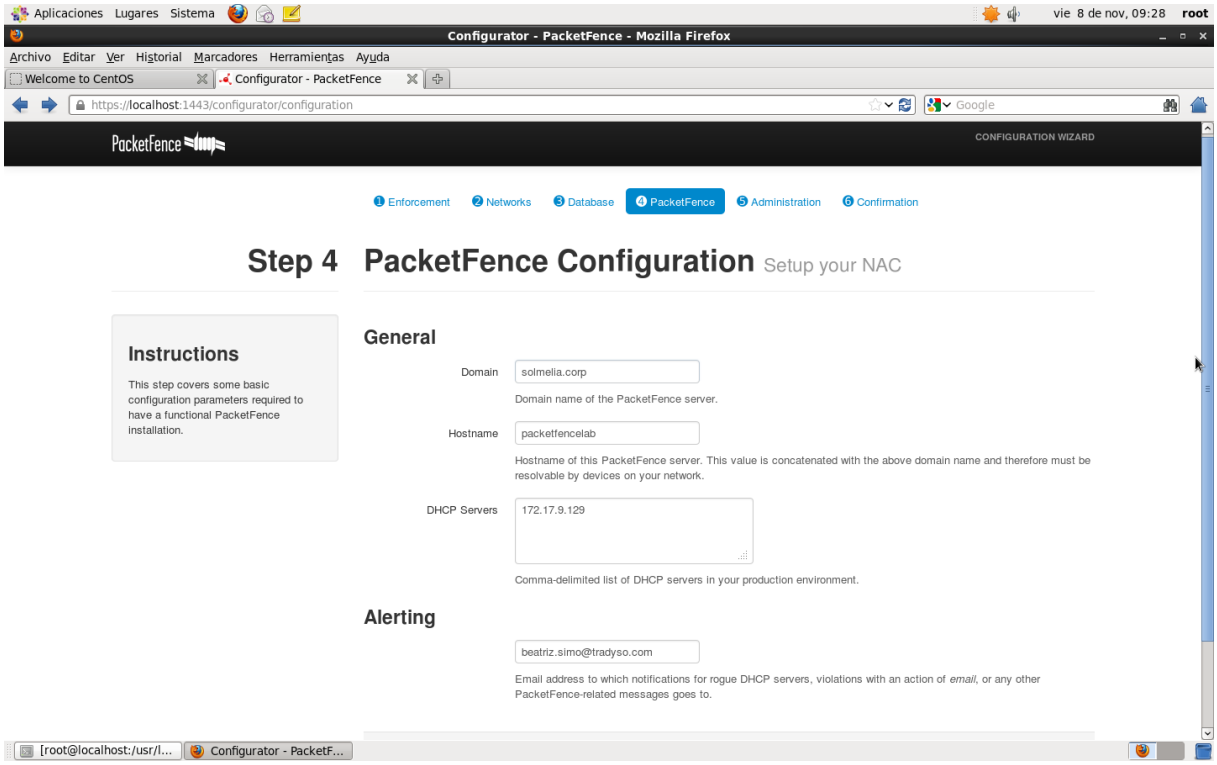

Ilustración 11: PacketFence

Pas 5. Administració

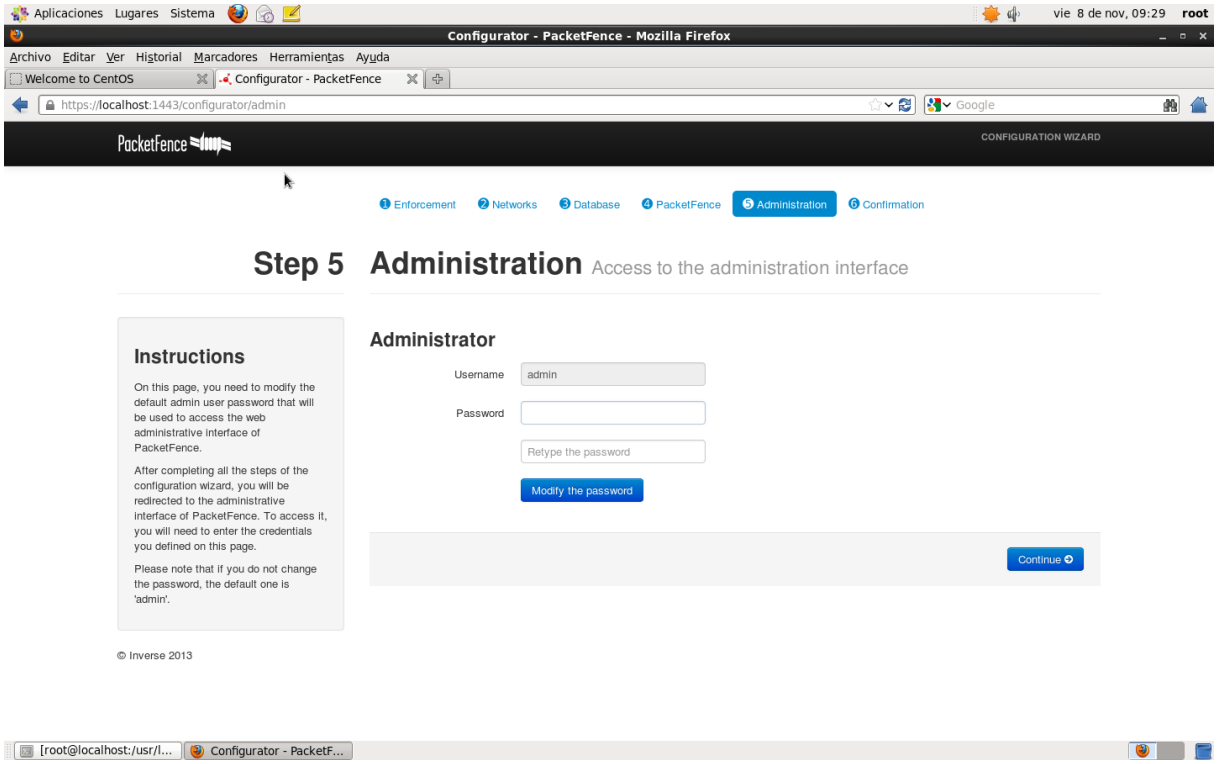

Ilustración 12: Administration to acces to administration interface

Paso 6. Confirmació.

S'han de posar en marxa els següents serveis que utilitza el packetfence aquest son:

- Web server (httpd)
- FreeRadius server(radiusd)
- Snort/suricata network IDS.
- Firewall (iptables).

Donam al botó de “Start Services”, es posaran en marxa tots els serveis i haurem configurat packetfence, aquest ens redirigirà a la url de l'Administrador que es la següent:

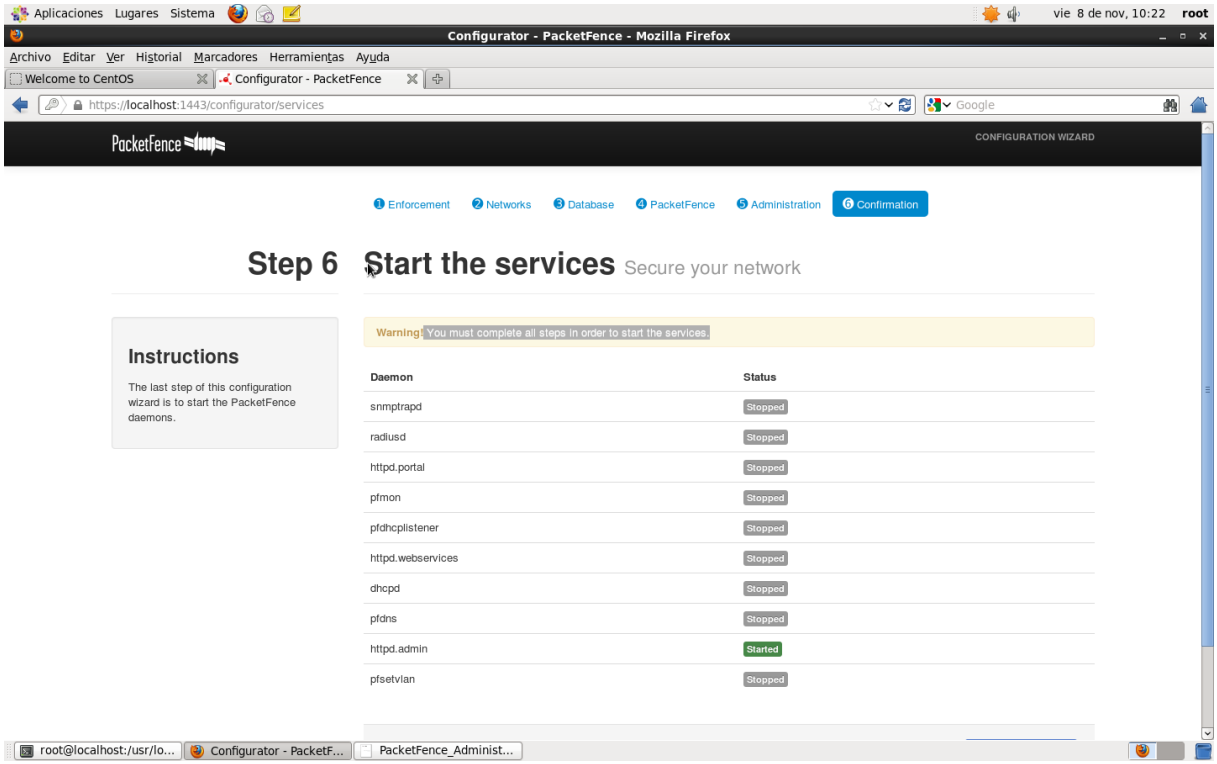

Ilustración 13: Paso 6. Start the services

9.1.4. Laboratori:

La infraestructura de xarxa del laboratori esta formada:

- Switch Cisco Catalytic 3560.
- VLAN6 és la VLAN "normal" (1) - els usuaris amb el rol de "default" s'asignaran a la mateixa.
- VLAN400 és la VLAN “registre”(2)- els dispositius no registrats seràn posats en aquesta VLAN.

- VLAN9 és la VLAN “Isolation”(3) d'aillament – els dispositius aisllats seràn posats en aquesta VLAN.
- VLAN404 és la VLAN “MAC detection”(5)
- VLAN 4 s'ha de definir en tots els switches que no soporten port-security.
- VLAN 666 és la VLAN “management” (4).
- El servidor DHCP se encarregarà de la distribució d'adreços IP en la VLAN 2 y 3.
- El servidor DNS se fará carrec de la resolució de dominio en xarxer VLAN 2 y 3.

Taula de Configuració de Xarxa – Servidor PacketfenceLab.

VLAN ID	VLAN Name	Subnet	Gateway	PacketFence Address
Vlan6 (1)	Normal(Default)	172.17.9.128/25	172.17.9.129	172.17.9.134
Vlan400 (2)	Registration	192.168.2.0/24		192.168.2.3
Vlan9 (3)	Isolation	192.168.1.0/24		192.168.1.2
Vlan666 (4)	Management	172.17.8.0/26		172.17.8.24
Vlan404 (5)	MAC Detection	-	-	-

Interficis definides al Packetfence.

Els NICs d'inici de Packetfence estàn en:

/etc/sysconfig/network-scripts/ifcfg-eth0:

```
DEVICE=eth0
HWADDR=
ONBOOT=yes
BOOTPROTO=static
NM_CONTROLLED=no
TYPE=Ethernet
```

/etc/sysconfig/network-scripts/ifcfg-eth0.6:

```
DEVICE=eth0.6
VLAN=yes
ONBOOT=yes
BOOTPROTO=static
NM_CONTROLLED=no
IPADDR=172.17.9.134
NETMASK=255.255.255.128
GATEWAY=172.17.9.129
```

/etc/sysconfig/network-scripts/ifcfg-eth0.400:

```
DEVICE=eth0.400
VLAN=yes
```

```
ONBOOT=yes
BOOTPROTO=static
NM_CONTROLLED=no
IPADDR=192.168.2.3
NETMASK=255.255.255.0
```

/etc/sysconfig/network-scripts/ifcfg-eth0.9:

```
DEVICE=eth0.9
VLAN=yes
ONBOOT=yes
BOOTPROTO=static
NM_CONTROLLED=no
IPADDR=192.168.1.2
NETMASK=255.255.255.0
```

/etc/sysconfig/network-scripts/ifcfg-eth0.666:

```
DEVICE=eth0.666
VLAN=yes
ONBOOT=yes
BOOTPROTO=static
NM_CONTROLLED=no
IPADDR=172.17.8.24
NETMASK=255.255.255.192
```

/etc/sysconfig/network-scripts/ifcfg-eth0.404:

```
DEVICE=eth0.404
VLAN=yes
HWADDR=
ONBOOT=yes
NM_CONTROLLED=no
```

Configuració dels Traps dins paquetfence (receptor de captures)

Packetfence utilitza snmptrapd per els traps. Se guarda en la configuració del switch en el directori /usr/local/pf/conf/switches.conf:

```
[default]
SNMPCommunityTrap = public
```

Configuració del switch de laboratori.

Hem habilitat linkUp/linkDown per el switch Switch Cisco Catalytic 3560. Se pot consultar la configuració del switch Cisco Catalytic 3560 en el document de packetfence anomenat “PacketFence_Network_Devices_Configuration_Guide-4.0.6.pdf”

```
sw6pmi#sh run
Building configuration...

<omitido>

!
aaa group server radius packetfence
 server 172.17.8.24 auth-port 1812 acct-port 1813
!

<omitido>

!
aaa authentication login default group ldiso local line
aaa authentication dot1x default group packetfence
aaa authorization exec default local group ldiso
aaa authorization network default group packetfence

!

<omitido>

!
dot1x system-auth-control
!

<omitido>

!
interface FastEthernet0/1
 description "none"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,6,9,666,999
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 description "PF_PruebaAcceso"
```

```
 switchport access vlan 404
 switchport mode access
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 10800
 authentication timer reauthenticate 7200
 mab
 dot1x pae authenticator
 dot1x timeout quiet-period 2
 dot1x timeout tx-period 3
!

<omitido>

!
interface FastEthernet0/24
 description "PF_trunk"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 6,9,400,404,666
 switchport mode trunk
 switchport nonegotiate
 ip access-group 100 in
!
interface GigabitEthernet0/1
 description "none"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,3,6,666,999
 switchport mode trunk
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description "none"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,3,6,666,999
```

```
 switchport mode trunk
 switchport nonegotiate
 shutdown
!

<omitido>

no cdp run
no cdp tlv location
no cdp tlv app

<omitido>

snmp-server community TraPub RO
snmp-server community TraPriv RW
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move threshold
snmp-server host 172.17.8.24 version 2c TraPub  mac-notification snmp

<omitido>

radius-server host 172.17.8.24 auth-port 1812 acct-port 1813 timeout 2 key 7 **********************
radius-server vsa send authentication
!

<omitido>

mac address-table notification change interval 0
mac address-table aging-time 3600
end

sw6pmi#
```

En packetfence, la configuració del switch se pot fer utilizant la GUI d'Administrador de Web, https://iphostpacketfence:1443:admin/configuration#configuration

o editant el fitxer /usr/local/pf/conf/switches.conf

```
[172.17.8.20]
mode=production
SNMPCommunityRead=TraPub
SNMPCommunityWrite=TraPriv
defaultVlan=6
deauthMethod=SNMP
description=sw6pmi
type=Cisco::Catalyst_3560
macDetectionVlan=404
VoIPEnabled=N
isolationVlan=9
radiusSecret=VU8A!Lxm-xIw7rF9Bf
SNMPVersion=2c
registrationVlan=400
defaultRole=default
guestVlan=9
guestRole=guest
```

Configuració global del Packetfence.

La configuració global del Packetfence està en el directori /usr/local/pf/conf/pf.conf

Tots aquest paràmetres se poden configurar per la Web administradora, recordar que quan se modifiquen aquest paràmetres hi ha que reiniciar els serveis del packetfence.

```
[general]
#
# general.domain
#
# Domain name of PacketFence system.
domain=solmelia.corp
#
# general.hostname
#
# Hostname of PacketFence system.  This is concatenated with the domain in Apache rewriting
rules and therefore must be resolvable by clients.
hostname=packetfencelab
#
# general.dnsservers
#
# Comma-delimited list of DNS servers.  Passthroughs are created to allow queries to these servers
from even "trapped" nodes.
dnsservers=62.187.216.107
#
# general.dhcpservers
#
# Comma-delimited list of DHCP servers.  Passthroughs are created to allow DHCP transactions
from even "trapped" nodes.
dhcpservers=172.17.9.129
#
# general.locale
#
# Locale used for message translation
# more than 1 can be specified
locale=es_ES
#
# general.timezone
#
# System's timezone in string format. Supported list:
# http://www.php.net/manual/en/timezones.php
timezone=Madrid
#
# general.memcached
#
# Server list of the memcached server
memcached=127.0.0.1:17887

[registration]
#
# registration.range
#
#
```

```
range=192.168.2.0/24
#
# registration.nbregpages
#
# The number of registration pages to show to the user
nbregpages=1

[guests_admin_registration]
#
# guests_admin_registration.access_duration_choices
#
# These are all the choices offered in the guest management interface as
# possible access duration values for a given registration.
access_duration_choices=3h

[alerting]
#
# alerting.emailaddr
#
# Email address to which notifications of rogue DHCP servers, violations with an action of
"email", or any other
# PacketFence-related message goes to.
emailaddr=beatriz.simo@tradyso.com

[database]
#
# database.pass
#
# Password for the mysql database used by PacketFence.
pass=allfusion8

[expire]
#
# expire.node
#
# Time before a node is removed due to inactivity.
# A value of 0D disables expiration.
# example:
# node=90D
node=7D
#
# expire.iplog
#
# Time which you would like to keep logs on IP/MAC information.
# A value of 0D disables expiration.
# example:
# iplog=180D
iplog=7D
#
# expire.traplog
#
# Time which you would like to keep logs on trap information.
```

```
# A value of 0D disables expiration.
# example:
# traplog=180D
traplog=7D
#
# expire.locationlog
#
# Time which you would like to keep logs on location information
# Please note that this table should not become too big since it
# could degrade pfsetvlan performance.
# A value of 0D disables expiration.
# example:
# locationlog=180D
locationlog=7D

[servicewatch]
#
# servicewatch.restart
#
# Should pfcmd service pf watch restart PF if services are not running?
# You must make sure to call the watch command. Installing it in the cron is the
# recommended approach:
# */5 * * * * /usr/local/pf/bin/pfcmd service pf watch
restart=enabled

[captive_portal]
#
# captive_portal.network_detection_ip
#
# This IP is used as the webserver who hosts the common/network-access-detection.gif which is
used to detect if network
# access was enabled.
# It cannot be a domain name since it is used in registration or quarantine where DNS is
blackholed.
# It is recommended that you allow your users to reach your packetfence server and put your
LAN's PacketFence IP.
# By default we will make this reach PacketFence's website as an easy solution.
#
network_detection_ip=192.168.2.3

[interface eth0.400]
enforcement=vlan
ip=192.168.2.3
type=internal
mask=255.255.255.0

[interface eth0.666]
ip=172.17.8.24
type=management
mask=255.255.255.192
```

Configuració de xarxa.

La configuració està en el directori /usr/local/pf/conf/networks.conf, se pot modificar el fitxer.

```
[192.168.1.0]
dns=8.8.8.8
dhcp_start=192.168.1.25
gateway=192.168.1.2
domain-name=vlan-isolation.solmelia.corp
named=enabled
dhcp_max_lease_time=30
dhcpd=enabled
type=vlan-isolation
netmask=255.255.255.0
dhcp_end=192.168.1.90
dhcp_default_lease_time=30

[192.168.2.0]
dns=192.168.2.3
dhcp_start=192.168.2.10
gateway=192.168.2.3
domain-name=vlan-registration.solmelia.corp
named=enabled
dhcp_max_lease_time=30
dhcpd=enabled
type=vlan-registration
netmask=255.255.255.0
dhcp_end=192.168.2.246
dhcp_default_lease_time=30
```

Configuració del Radius.

L'us de WPA2-Enterprise(Wireles 802.1x), autentificació MAC i Wired 802.1x requereixen Radius Server per autentificar usuaris i workstations, i colocar-los en la correspondent VLAN de l'equip de xarxa. Se recomana instal.lar FreeRadius inclus encara que la planficació no estigui previst emplear-la.

Cada tipus d'autentificació se definirá amb regles, rols i accions.

Autentificació local.

En el següent directori /usr/local/pf/raddb/, hi ha que afegir en el fitxer users:

```
username Cleartext-Password := "password"
```

Autentificació contra OpenLDAP(Directori Actiu de Melia)

Per autentificar contra el directori actiu de Melia s'han fet les següents configuracions:

1. Crear un Source, en usari de la Web Admistradora.
2. Aquesta configuració queda emmagatzemada en el directori /usr/local/pf/conf/authentication.conf
3. Configurar en /usr/local/pf/raddb/modules/ldap
4. Descomentar ldap en /usr/local/pf/raddb/sites-enables/default
5. Configurar el seguent, en el fitxer packetfence-tunnel tal que:

```
Authentificate {
        Auth-Type MS-CHAP{
                Mschap
            }
    Eap
    Ldap
}
```

6. Mirar els logs de FreeRadius, en el directori /usr/local/pf/logs/radius.log. Sino se pot executar el comand debug:

```
debug radius -d -X /usr/local/pf/raddb/
```

PacketFence dóna suport a la assignació de rols en els dispositius que li dóna suport. L'estratègia actual d'assignació de funcions és assignar juntament amb la VLAN (que pot canviar en el futur). Un paper intern especial per assignació de funcions externes s'ha de configurar en el fitxer de configuració de switch (/ usr / local / pf / conf / switches.conf).

Per autentificar un usuari “guest”, es dir que quan un convidat se conecti a la xarxa, mitjançant el portal cautiu, hem definit, un usuari que complesqui una serie de regles i roles, i que per defecte aquest usuari convidat hi vagi a la xarxa “isolation”, que es la 9.

9.2. Llicencia.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct
   from that of the Document, and from those of previous versions
   (which should, if there were any, be listed in the History section
   of the Document). You may use the same title as a previous version
   if the original publisher of that version gives permission.
B. List on the Title Page, as authors, one or more persons or entities
   responsible for authorship of the modifications in the Modified
   Version, together with at least five of the principal authors of the
   Document (all of its principal authors, if it has fewer than five),
   unless they release you from this requirement.
C. State on the Title page the name of the publisher of the
   Modified Version, as the publisher.
D. Preserve all the copyright notices of the Document.
E. Add an appropriate copyright notice for your modifications
   adjacent to the other copyright notices.
F. Include, immediately after the copyright notices, a license notice
   giving the public permission to use the Modified Version under the
   terms of this License, in the form shown in the Addendum below.
G. Preserve in that license notice the full lists of Invariant Sections
   and required Cover Texts given in the Document's license notice.
H. Include an unaltered copy of this License.
I. Preserve the section Entitled "History", Preserve its Title, and add
   to it an item stating at least the title, year, new authors, and
   publisher of the Modified Version as given on the Title Page. If
   there is no section Entitled "History" in the Document, create one
   stating the title, year, authors, and publisher of the Document as
   given on its Title Page, then add an item describing the Modified
   Version as stated in the previous sentence.
J. Preserve the network location, if any, given in the Document for
   public access to a Transparent copy of the Document, and likewise
   the network locations given in the Document for previous versions
   it was based on. These may be placed in the "History" section.
   You may omit a network location for a work that was published at
   least four years before the Document itself, or if the original
   publisher of the version it refers to gives permission.
K. For any section Entitled "Acknowledgements" or "Dedications",
   Preserve the Title of the section, and preserve in the section all
   the substance and tone of each of the contributor acknowledgements
   and/or dedications given therein.
L. Preserve all the Invariant Sections of the Document,
   unaltered in their text and in their titles. Section numbers
   or the equivalent are not considered part of the section titles.
M. Delete any section Entitled "Endorsements". Such a section
   may not be included in the Modified Version.
N. Do not retitle any existing section to be Entitled "Endorsements"
   or to conflict in title with any Invariant Section.
O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or
appendices that qualify as Secondary Sections and contain no material
copied from the Document, you may at your option designate some or all
of these sections as invariant. To do this, add their titles to the
list of Invariant Sections in the Modified Version's license notice.
These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains
nothing but endorsements of your Modified Version by various
parties--for example, statements of peer review or that the text has
been approved by an organization as the authoritative definition of a

standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights

of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version

number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright (c) YEAR YOUR NAME.
> Permission is granted to copy, distribute and/or modify this document
> under the terms of the GNU Free Documentation License, Version 1.2
> or any later version published by the Free Software Foundation;
> with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
> A copy of the license is included in the section entitled "GNU
> Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the
> Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.