UNIVERSIDAD AUTÓNOMA DEL
ESTADO DE MÉXICO
CENTRO UNIVERSITARIO UAEM TEXCOCO

“Propuesta de conjunto de herramientas libres que apoyan en la administración de recursos informáticos”

T E S I S
QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

P R E S E N T A

CESAR IVAN CALLEJAS CORTES

DIRECTORA
M. EN C.C. MA. DOLORES ARÉVALO ZENTENO

REVISORES
M. EN C. JOSUÉ VICENTE CERVANTES BAZÁN
L. EN INF. CINTHYA TERESITA ISLAS RODRÍGUEZ

TEXCOCO, ESTADO DE MÉXICO, FEBRERO DE 2019.

Universidad Autónoma del Estado de México

Centro Universitario UAEM Texcoco

Texcoco, México a 30 de mayo de 2018

M. EN C. E. VIRIDIANA BANDA ARZATE
SUBDIRECTORA ACADEMICA DEL
CENTRO UNIVERSITARIO UAEM
TEXCOCO.
PRESENTE:

AT´N: M. EN C. LETICIA ARÉVALO CEDILLO
RESPONSABLE DEL DEPARTAMENTO DE TITULACION

Con base en las revisiones efectuadas al trabajo escrito titulado "**Propuesta de conjunto de herramientas libres que apoyan en la administración de recursos informáticos**" que para obtener el título de Licenciatura en **Ingeniería en computación** presenta el sustentante **Cesar Iván Callejas Cortes**, con Número de Cuenta **1024198**, se concluye que cumple con los requisitos teorico-metodologicos necesarios para su aprobación, pudiendo continuar con la etapa de ejecución del trabajo escrito.

ATENTAMENTE

L. En I.A. Cinthya Terésita Islas Rodríguez
Nombre y firma del revisor

M. En C. Josué Vicente Cervantes Bazán
Nombre y firma del revisor

M. En C. C. Dolores Arévalo Zenteno
Nombre y firma del director

TITULACION
RECIBIDO
Por Leopoldo
Texcoco, Méx., a 30 de Mayo del 18

c.c.p Cesar Iván Callejas Cortes
c.c.p M. En C. C. Dolores Arévalo Zenteno
c.c.p Titulación/ M. En C. Leticia Arévalo Cedillo

Centro Universitario UAEM Texcoco
Av. Jardín de Zumpango s/n Fracc. El Tejocote, C. P. 56259,
Texcoco, Estado de México
Tels. (595) 9211216/247/ 9210368/493
Email: cutex.uaem@gmail.com

CUTex

AGRADEZCO ESTE TRABAJO A:

Para comenzar iniciaré con la frase:

"A veces solo falta dar un paso para llegar al éxito"

Por este motivo agradezco a mi esposa Perla Belem y a mi hija Arely Naomi, pues ellas fueron el impulso para dar este paso y poder concluir este proyecto, así como ser mi estímulo para que cada día busque ser una mejor persona.

A mis padres

Armando y Maribel que pese a los altibajos de las circunstancias me apoyaron en esta etapa de mi vida, me brindaron la oportunidad, el acompañamiento y legado del conocimiento.

Agradezco a mi cuñada Nidia Bravo por siempre animarme y alentarme en esta etapa.

A mi familia y amigos que han formado parte de este gran recorrido.

A mi asesora Dolores Arévalo Zenteno y a mis revisores Cinthya Teresita Islas Rodríguez y Josué Vicente Cervantes Bazán.

Quienes a pesar de sus extensas actividades y ocupaciones se prestaron el tiempo para guiarme en este proyecto.

DEDICO ESTE TRABAJO A:

Dedico estés trabajo mi esposa e hija que con su motivación y apoyo me acompañaron en el camino de este proyecto pese a los altibajos de la situación.

Dedico este trabajo a mis padres que con su esfuerzo y cariño me ayudaron concluir este trabajo.

A mis familiares, amigos y profesores quienes siempre me alentaban a seguir adelante con la frase "Tú puedes".

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

Introducción

Este trabajo plantea la problemática que las empresas presentan al momento de entrar en el contexto de una correcta administración de sus recursos informáticos como: Administración de red y control de acceso a redes inalámbricas, Respaldos confiables y organizados, Monitoreo de sus diferentes equipos y la inversión a corto y largo plazo que representa sostener un proyecto que satisfaga estas necesidades con proveedores de pago, siendo el factor económico y la falta de opciones accesibles para los encargados de TI una barrera para el crecimiento de la empresa e incluso un riesgo en la operación.

Es por este motivo que el tema de investigación central es satisfacer estas necesidades a través de herramientas de software libre y con una documentación extensa y simple para el entendimiento de los implementadores, que se pretende sean los encargados de área de TI respectivamente además de una operación y configuración simple y comprensible.

Para lograr esta meta se realizará el levantamiento de información analizando las áreas de oportunidad de algunas empresas muestra con problemática real y recreando estas problemáticas en un ambiente controlado para así poder solucionar sus áreas de oportunidad encontradas siempre bajo la premisa de utilizar herramientas de software libre y presentar una solución a los responsables del área de TI que rompa las barreras económicas y la falta de opciones accesibles.

Planteamiento del problema

Es posible observar la falta de recursos informáticos en las empresas por el costo que representa implementar y sostener estas infraestructuras además de la falta de personal capacitado para el manejo de las herramientas.

Es por eso que surge la pregunta ¿**Es posible apoyar en la administración de recursos informáticos usando software libre?**

Justificación

La falta de administración de recursos informáticos es un área de oportunidad que causa problemas a las empresas u organizaciones, Se ha podido identificar el retraso y problema en la operación debido a la falta de administración de recursos informáticos, esencialmente en los puntos de pérdida de información por falta de respaldos eficientes. (En ocasiones el respaldo se lleva acabo manualmente a un dispositivo externo), retrasos por la mala administración de la infraestructura de red. (En algunos de los casos se observa que la división de red no es segura para la empresa), atención tardía ante incidentes (Al no contar con un monitoreo de equipos generalmente las incidencias se atienden al bomberazo como coloquialmente se le conoce al actuar cuando ya se ha reportado un problema por un usuario el cual generalmente lo reporta cuando la incidencia no le permite continuar con sus actividades), aun cuando existen herramientas que cubren estas problemáticas las organizaciones a menudo no las implementan debido a los costos que representa su implementación dejando sin opciones a los administradores del área de tecnologías los cuales padecen las consecuencias de no contar con estas

herramientas, además de la falta de visión por parte de los administradores ejemplo de esto es tener la red de la empresa sin una división adecuada si un invitado o usuario llega a descargar un paquete maligno este podría propagarse sin restricción por toda la red o el caso en que un usuario reporta que no puede cargar algún portal ya que la red es muy lenta, en ocasiones esto se debe a que uno de los usuarios tienen un alta libertad en la red y saturan sin control los canales de comunicación a Internet, el administrador no tiene opción de saber que usuarios están saturando la red, anteriormente se mencionó que la problemática de una falta de administración de recursos informáticos no solo se debe al poco presupuesto que las empresas dedican al área de TI sino que también se debe en ocasiones a la falta de visión de los propios administradores es por este motivo que una alternativa a bajo costo son las herramientas libres (Software Libre).

Hipótesis

Se observa en diferentes empresas la falta de administración de recursos informáticos, debido a la falta de presupuesto para implementar o a la falta de personal capacitado que pueda manejar las solución es por eso que con la ayuda de software libre para administrar los recursos informáticos las empresas contaran con una solución viable y a bajo costo, además tendrán una amplia documentación y guías de forma libre para la implementación y manejo de dichas soluciones, es por eso que se cree que los puntos importantes que se pueden solucionar usando software libre son Administración de Red, Seguridad perimetral, Respaldos de Información y Monitoreo de Recursos Informáticos.

Método

Se realizó una investigación inductiva de acuerdo a los siguientes pasos:

1. Definición de la problemática.
2. Recopilación de información relacionada con el tema.
3. Contacto a empresas que desearán participar en el proyecto.
4. Aplicación de cuestionario a las empresas que aceptaron participar, para el levantamiento de información.
5. Análisis de la información de cada empresa para crear una propuesta que cubra sus necesidades de administración de recursos informáticos.
6. Presentación de propuesta a las empresas para su aprobación y validación.
7. Integración de propuestas en una sola propuesta integrada.
8. Elección de herramientas a utilizar para cubrir las problemáticas detectadas.
9. Solución a las problemáticas en ambiente controlado usando las herramientas elegidas.
10. Ajuste de solución a las necesidades de cada empresa.

Objetivos

Objetivo General

Implementar una solución con software libre que ayude a las empresas a tener una correcta administración y monitoreo de red y sus equipos de cómputo, así como salvaguardar la información de manera administrada.

Objetivos específicos

1. Administrar y proteger la red de la empresa con software libre.
2. Crear túneles VPN seguros para la conexión a la empresa desde el exterior usando software libre.
3. Implementar un monitoreo de equipos de cómputo con software libre.
4. Administrar un control de respaldo de la información de la empresa con software libre.
5. Mostrar opciones de software con alta adaptación de software, así como una amplia documentación accesible y entendible.

CAPITULO 1 REDES COMPUTACIONALES

Para poder entender el concepto de redes computacionales o red de computadoras tomaremos como referencia el concepto de los autores Tanenbaum y Wetherall que mencionan como red de computadoras a "*un conjunto de computadoras autónomas interconectadas mediante una sola tecnología. Se dice que dos computadoras están interconectadas si pueden intercambiar información. La conexión no necesita ser a través de un cable de cobre; también se puede utilizar fibra óptica, microondas, infrarrojos y satélites de comunicaciones. Las redes pueden ser de muchos tamaños, figuras y formas "* (S. Tanenbaum & J. Wetherall, 2012, pág. 2), discrepando solo en el uso de una sola tecnología ya que en la actualidad es posible realizar conexiones de computadora a través de diferentes tecnologías.

1.1 Modelo OSI y Arquitectura TCP/IP

Durante el intercambio de datos entre dispositivos de procesamiento es necesario un camino de comunicación, este camino de comunicación puede ser directo o a través de una red de comunicación. De igual forma el autor Stallings en el libro Comunicaciones y Redes de Computador Séptima Edición, indica que no solo se requiere la transmisión de los datos entre los equipos, sino que hay que tomar en cuenta lo siguientes puntos

1. *"El sistema fuente de información debe activar un camino directo de datos o bien debe proporcionar a la red de comunicación la identificación del sistema destino deseado."* (Stallings, 2004, pág. 22)
2. *"El sistema fuente debe asegurarse de que el destino está preparado para recibir datos."* (Stallings, 2004, pág. 22)

3. *"La aplicación de transferencia de archivos en el origen debe asegurarse de que el programa gestor en el destino está preparado para aceptar y almacenar el archivo para el usuario determinado."* (Stallings, 2004, pág. 23)
4. *"Si los formatos de los dos archivos son incompatibles en ambos sistemas, uno de los dos deberá realizar una operación de traducción."* (Stallings, 2004, pág. 23)

Dejando claro que es necesario un alto grado de coordinación y apoyo entre 1vlos computadores involucrados en lugar de implementar todo el procesamiento lógico en un único punto, de esta forma el problema se divide en subtareas que se realiza por separado, *"En una arquitectura de protocolos, los distintos módulos se disponen formando una pila vertical. Cada capa de la pila realiza el subconjunto de tareas relacionadas entre sí que son necesarias para comunicar con el otro sistema. Por lo general, las funciones más básicas se dejan a la capa inmediatamente inferior, olvidándose en la capa actual de los detalles de estas funciones. Además, cada capa proporciona un conjunto de servicios a la capa inmediatamente superior. Idealmente, las capas deberían estar definidas de forma tal que los cambios en una capa no deberían necesitar cambios en las otras. Evidentemente, para que haya comunicación se necesitan dos entidades, por lo que debe existir el mismo conjunto de funciones en capas en los dos sistemas. La comunicación se consigue haciendo que las capas correspondientes, o pares, intercambien información. Las capas pares se comunican intercambiando bloques de datos que verifican una serie de reglas o convenciones denominadas protocolo. Los aspectos clave que definen o caracterizan a un protocolo son: La sintaxis: establece cuestiones relacionadas con el formato de los bloques de datos. La semántica: incluye información de control para la coordinación y la gestión de errores. La temporización: considera aspectos relativos a la sintonización de velocidades y secuenciación"* (Stallings, 2004, pág. 23)

1.1.1 Modelo OSI

"La labor de ISO consistió en definir el conjunto de capas, así como los servicios a realizar por cada una de ellas. La división debería agrupar a las funciones que fueran conceptualmente próximas en un número suficiente, tal que cada capa fuese lo suficientemente pequeña, pero sin llegar a definir demasiadas para evitar así sobrecargas en el procesamiento" (Stallings, 2004, págs. 29,30,31), Stallings indica que cada sistema debe contener las siete capas del modelo OSI (ver *Ilustración 1*) las cuales se explican a continuación:

1. Capa de Aplicación: Proporciona acceso al entorno OSI pudiendo acceder a las demás capas y define los protocolos que utilizan las aplicaciones para su interacción o intercambio de datos.
2. Capa de Presentación: Proporciona una representación de la información de manera que sea entendible por los diferentes equipos en pocas palabras en esta capa se tratan aspectos como la Sintaxis.
3. Capa de Sesión: Esta capa es la encargada de gestionar el enlace de comunicación de principio a fin durante la transmisión de datos garantizando la transmisión.
4. Capa de Transporte: Es la capa en la que se proporciona el procedimiento de recuperación en caso de errores y control de flujo entre los ordenadores de la conexión, en pocas palabras es la encargada de una transferencia transparente y fiable entre ambos puntos de los ordenadores.
5. Capa de Red: Esta capa es responsable del mantenimiento inicio y cierre de cesión de las conexiones.
6. Capa de Enlace de datos: Esta es la etapa de transferencia de datos mediante el enlace físico mediante él envió de tramas.

7. Capa Física: Se encarga de la topología de red, la transmisión de cadenas de bits no estructurados a través del medio físico.

Ilustración 1: Capas del Modelo OSI.

Para visualizar el funcionamiento del modelo OSI nos basaremos en la explicación del autor Stallings, imaginemos que un equipo A desea enviar un mensaje al equipo B, como ya se dijo anteriormente ambos equipos deberán contar con la misma estructura de modelado en cada uno de sus extremos ver *Ilustración 2*.

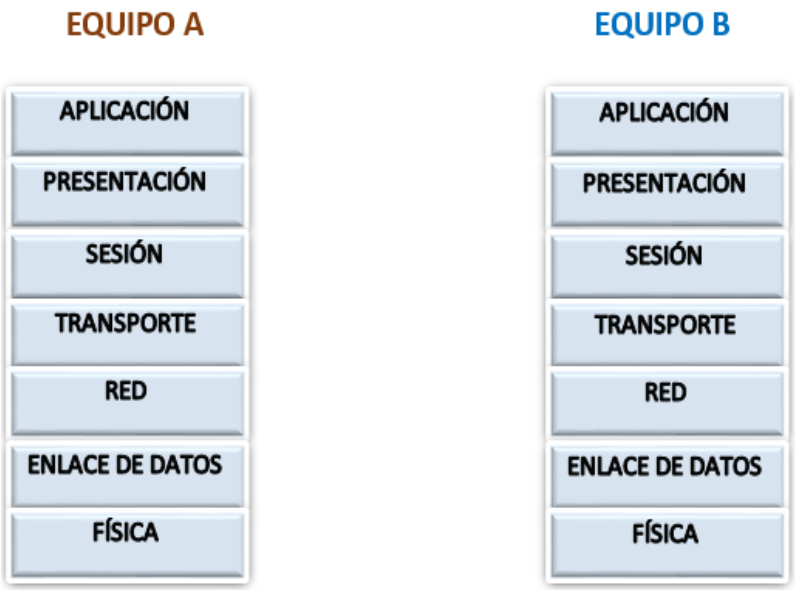

Ilustración 2: Equipo A y Equipo B.

Cuando el equipo A desea enviar el mensaje al equipo Primero se transfieren los datos a la capa de aplicación y se añade información necesaria para la capa 7, a este proceso se le denomina encapsulamiento.

Los datos se envían de la capa de aplicación como una sola unidad a la capa 6 o capa de presentación, una vez recibidos los datos la capa 6 añade su propia cabecera realizando así un segundo encapsulamiento, este proceso continúa hasta la capa 2 o capa de enlace de datos.

En la capa 2 normalmente se añade una cabecera y una cola. La unidad de datos recibida se llama trama, la cual se envía al medio de transmisión mediante la capa 1 o capa física.

El siguiente paso es que la trama es enviada al destino en el cual se realiza el proceso a la inversa, pasando capa a capa en las cuales se va eliminando la cabecera externa que le corresponde.

En el destino, al recibir la trama, ocurre el proceso inverso. Conforme los datos ascienden, cada capa elimina la cabecera más externa, actúa sobre la información de protocolo contenida en ella y pasa el resto de la información hacia la capa inmediatamente superior.

Nota: *"En cada etapa del proceso, cada una de las capas puede fragmentar la unidad de datos que recibe de la capa inmediatamente superior en varias partes, de acuerdo con sus propias necesidades. Estas unidades de datos deben ser ensambladas por la capa par correspondiente antes de pasarlas a la capa superior."* (Stallings, 2004, pág. 31)

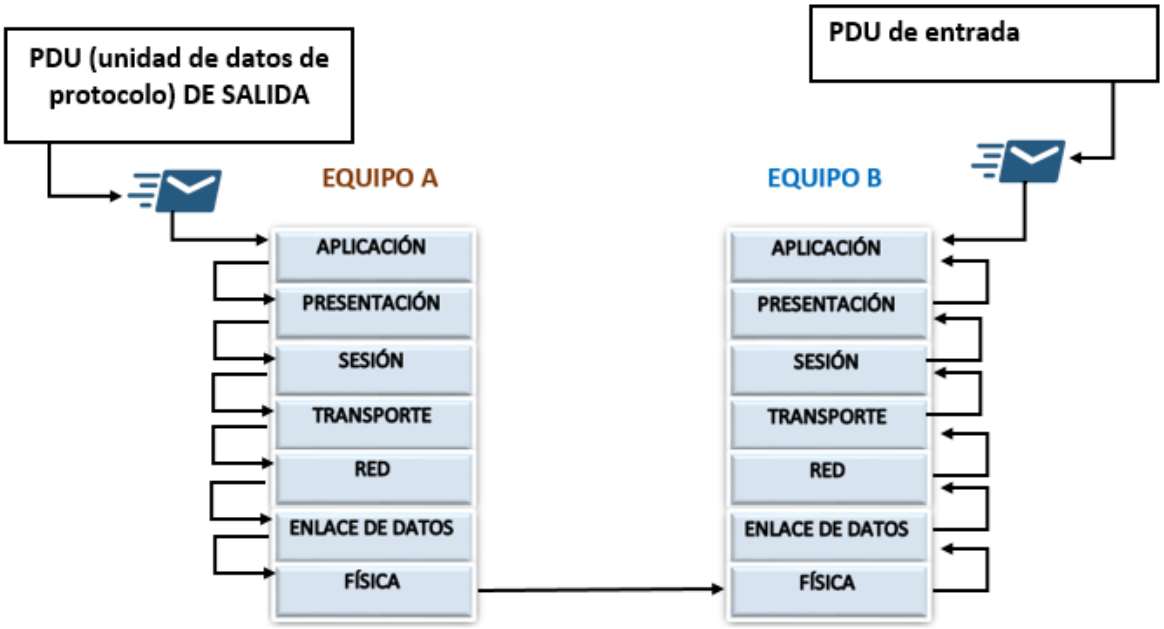

Ilustración 3: Representación del envió de Mensaje de equipo A al equipo B.

1.1.2 Arquitectura TCP/IP

Red de la Agencia de Proyectos de Investigación Avanzada (ARPANET), *"La arquitectura de protocolos TCP/IP es resultado de la investigación y desarrollo llevados a cabo en la red experimental de conmutación de paquetes ARPANET, financiada por la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA, Defense Advanced Research Projects Agency), y se denomina globalmente como la familia de protocolos TCP/IP."* (Stallings, 2004, pág. 40)

En el modelo TCP/IP el problema de comunicación se estructura en 5 capas, para poder explicarlas nos apoyaremos del autor William Stallings.

1. Capa física: En esta capa se define la interfaz entre el equipo de transmisión y la red o medio de transmisión de datos. Siendo en esta capa donde se tratan las especificaciones del tipo de transmisión, naturaleza de señales, velocidad.
2. Capa de acceso a la red: Esta capa es la responsable del intercambio de datos entre el equipo final y la red o medio de transmisión al cual está conectado, siendo el emisor el que proporciona a la red la dirección destino para que los datos puedan ser encaminados correctamente al equipo deseado, estos estándares fueron desarrollados para la comunicación de circuitos, conmutación de paquetes y para redes de área local, por este motivo se separa toda función alejada de estos parámetros, siendo responsabilidad del software de comunicación que esté por encima de la capa de acceso a la red el cual no deberá preocuparse por detalles del envío de paquetes ya que se ha cargado la información necesaria en la capa de acceso a la red.

3. Capa internet: La capa Internet entra en acción cuando los equipos se encuentran conectados en diferentes redes para este caso se aplica una serie de procedimientos para lograr que los paquetes o datos pasen a través de las diferentes redes hasta llegar al destino fijado, en esta capa se utiliza el protocolo internet (IP, Internet Protocol) como encaminador a través de las diferentes redes, es importante resaltar que este protocolo debe ser implementado en los equipos finales como en los encaminadores intermedios, *"Un encaminador es un procesador que conecta dos redes y cuya función principal es retransmitir datos desde una red a otra siguiendo la ruta adecuada para alcanzar al destino."* (Stallings, 2004, pág. 40).
4. Capa extremo-a-extremo o de transporte: Esta capa se encarga de proporcionar fiabilidad en el intercambio de datos independientemente del origen de la aplicación que los envíe de forma segura y en el orden en que fueron enviados(Los protocolos que realizan estas funciones se clasifican dentro de la capa de transporte siendo el protocolo de control de transmisión o TCP el más utilizado para estas funciones).
5. Capa de aplicación: La capa de aplicación posibilita la comunicación entre las diferentes aplicaciones de usuario.

En la *Ilustración 4* se muestra una comparación entre la Arquitectura del modelo OSI y TCP/IP con respecto a la equivalencia de sus capas además de que OSI es de facto y TCP/IP es de hecho.

Ilustración 4: Arquitectura OSI Y TCP/IP.

1.2 Clasificación de las redes

"En general una red es una colección de procesadores débilmente acoplados interconectados por enlaces de comunicaciones usando cables, tecnología inalámbrica, o una combinación de ambas cosas." (Mclver McHoes & M. Flynn, 2010, pág. 284).

Por lo que a continuación se presenta la forma en que las redes de computadora se clasifican según su topología o su tamaño (cobertura), siendo nuestro marco de referencia para la clasificación los autores Mclver McHoes Y M. Flynn en su libro Sistemas Operativos Sexta edición.

1.2.1 Por su topología

Las redes de computadora son catalogadas por la forma en que están conectadas en otras palabras su topología:

- Topología De Estrella ver *Ilustración 5*
- Topología De Anillo ver *Ilustración 6*
- Topología De Bus ver *Ilustración 7*
- Topología De Árbol ver *Ilustración 8*

1.2.1.1 Topología de Estrella

La topología de estrella algunas veces es conocida como topología centralizada ya que los ordenadores interconectados deben pasar por una controladora central para transmitir entre ellos como se muestra en la *Ilustración 5*.

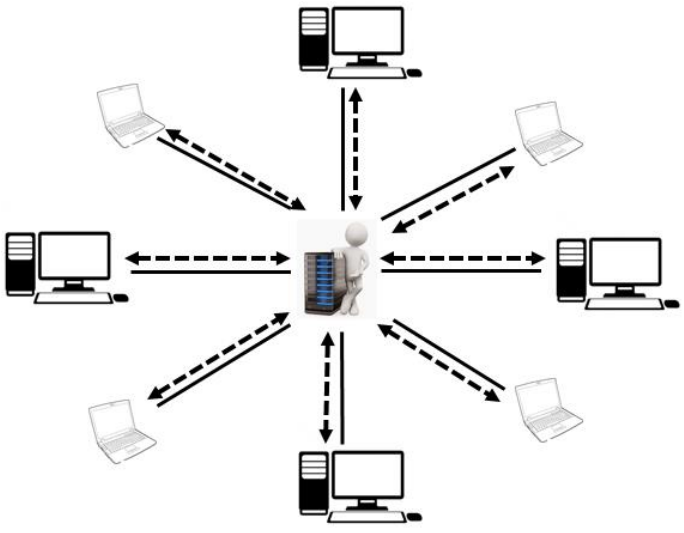

Ilustración 5: Topología de Estrella.

1.2.1.2 Topología de Anillo

Esta topología mantiene la conexión de los equipos mediante un bucle cerrado, yendo en una sola dirección o bidireccionalmente la transmisión de la información, en caso de requerir la transmisión de información con otra red esto se realiza a través de una puerta de enlace la cual se conectara. Ver *Ilustración 6*.

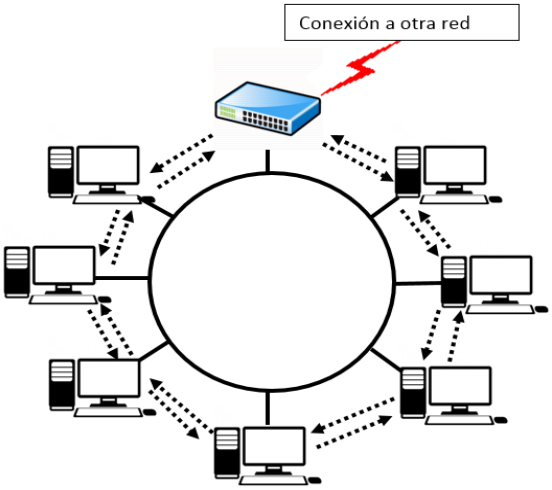

Ilustración 6: Topología de Anillo.

1.2.1.3 Topología de Bus

En la topología de Bus todos los ordenadores se encuentran conectados a una sola línea de comunicación que recorre la red, por este motivo solo uno de ellos puede enviar mensajes exitosamente, pudiendo pasar los datos de ordenador a ordenador o directamente a un controlador de extremo. Ver *Ilustración 7*

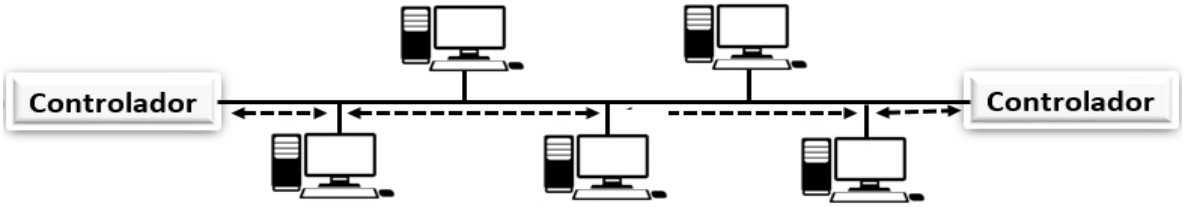

Ilustración 7: Topología de Bus.

1.2.1.4 Topología de Árbol

La topología de árbol consiste en una conexión de bus que se ramifica sin ningún bucle cerrado, iniciando por un extremo que se ramifica, cada enlace puede tener ramificaciones, es posible el uso de puentes en caso que alguna de las ramificaciones utilice diferente protocolo, la forma en que la información circula en esta topología es a través de la línea de comunicación por lo que si un mensaje llega a un controlador de extremo sin haber sido recibido por algún anfitrión este lo retransmitirá, la ventaja de esta topología al igual que la topología de Bus es que aun cuando un anfitrión falla el tráfico del mensaje seguirá fluyendo.

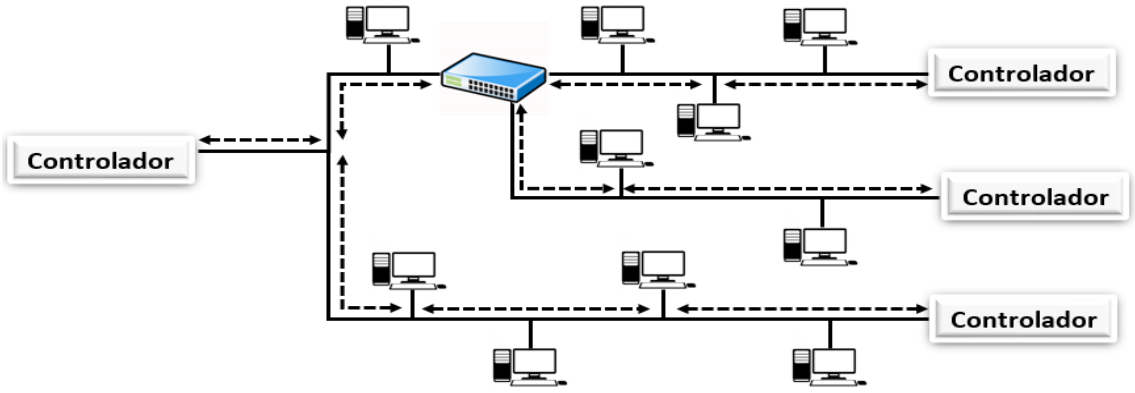

Ilustración 8: Topología de Árbol.

1.2.2 Por su cobertura

Las redes de computadora no solo se clasifican por su forma sino también por su tamaño o cobertura teniendo:

- Redes de Área Local (LAN) ver *Ilustración 9*
- Redes de Área Metropolitana (MAN) ver Ilustración 10
- Redes de Área Amplia (WAN) ver Ilustración 11
- Redes de Área Inalámbrica (WLAN) ver Ilustración 12

1.2.2.1 Redes de Área Local (LAN)

Este tipo de red se limita a un área como podría ser una oficina, edificio, hogar, almacén o cualquier entorno similar, una red LAN grande generalmente es dividida en segmentos más pequeños, en la *Ilustración 9* se presenta una red LAN de dos segmentos un segmento en cada piso del lugar. La red LAN general mente es Operada por una sola organización.

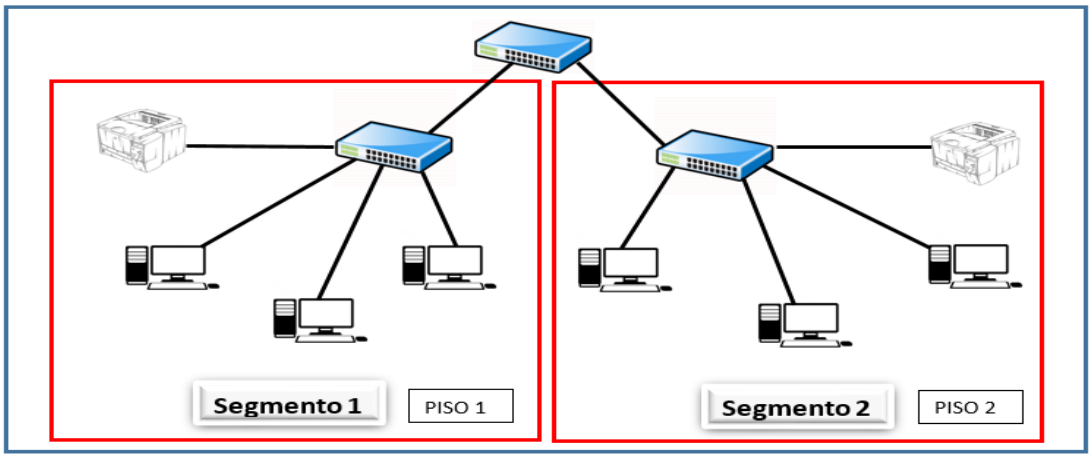

Ilustración 9: Red LAN con dos segmentos.

1.2.2.2 Red de Área Metropolitana (MAN)

Esta Red define una configuración de una red más grande que la red LAN la cual puede abarcar una ciudad entera siempre que entre en un área de 100Km de circunferencia, a pesar que una red MAN puede ser operada por una sola organización generalmente es utilizada por varias Organizaciones.

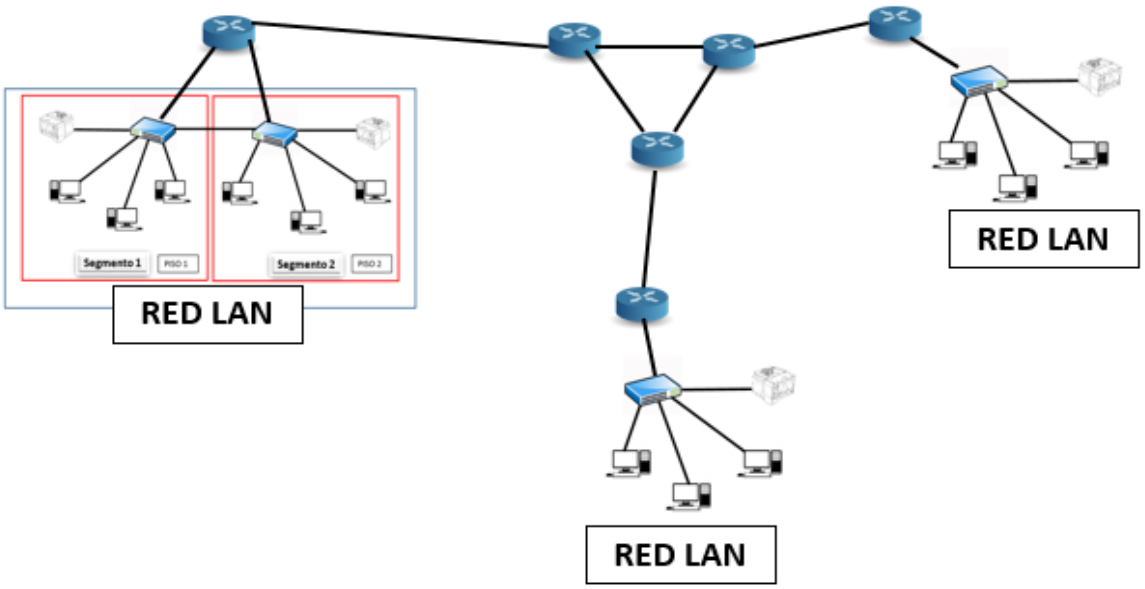

Ilustración 10: Red de Área Metropolitana (MAN).

1.2.2.3 Red de Área Amplia (WAN)

La red de Área Amplia permite la interconexión de partes distantes de un país o inclusive del mundo, generalmente estas redes utilizan las vías de comunicación de portadores comunes que pueden ser empresas privadas reguladas por el gobierno, en estas redes de comunicación es común el uso de satélites y antenas de microondas.

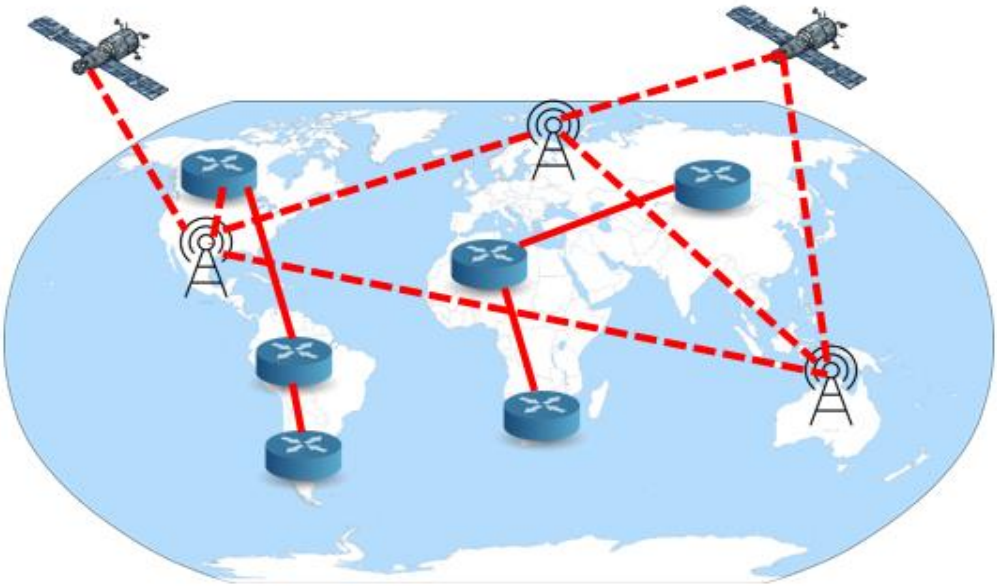

Ilustración 11: Red de Área Amplia (WAN).

1.2.2.4 Red De Área Local Inalámbrica (WLAN)

Este tipo de conexión hace referencia a una red de área local que utiliza como medio de conexión tecnologías inalámbricas para la conexión de equipos dentro del espacio de trabajo, la organización IEEE ha especificado varias normas para redes inalámbricas con diferente alcance. *"IEEE P802.11 es un grupo de trabajo de estándares en redes de área local inalámbricas. El grupo de trabajo es parte de IEEE LMSC (Comité de estándares de LAN MAN) anteriormente denominado Proyecto IEEE 802. IEEE LMSC informa al Consejo de actividad de estándares (SAB) de la Sociedad de informática IEEE."* (IEEE Standards Association (IEEE-SA), 2018).

SAB siglas en ingles Standards Activity Board

Mencionando algunas hasta 2009 según la organización IEEE:
Norma IEEE 802.11a: Velocidad 54 Mbps con un alcance de 25 a 75 pies en interior y frecuencia de 5 GHz, esta podría considerarse la primera norma IEEE inalámbrica.
Norma IEEE 802.11b: Velocidad de 11 Mbps con un alcance de 100 a 150 pies en interior y una frecuencia de 2.4 GHz, no es compatible con la norma IEEE 802.11g.
Norma IEEE 802.11g: Velocidad de 54 Mbps con un alcance de 100 a 150 pies en interior y una frecuencia de 2.4 GHz, es compatible con la norma IEEE 802.11b.
Norma IEEE 802.11n: Velocidad de 600 Mbps con un alcance de 300 pies en interior y una frecuencia de 5 GHz, es compatible con la norma IEEE 802.11g.

En 2018 se denotar las normas según la organización IEEE: 802.11aq ,802.11ak, 802.11aj.
"IEEE 802.11aq-2018 - Estándar de borrador aprobado de IEEE para tecnología de la información - Telecomunicaciones e intercambio de información entre sistemas Redes de área local y metropolitana - Requisitos específicos Parte 11: Especificaciones de control de acceso (MAC) y capa física (PHY) LAN inalámbrica Enmienda 5: Descubrimiento previo a la asociación" (IEEE Standards Association (IEEE-SA), 2018).
"IEEE Std 802.11ak-2018 (Enmienda a IEEE Std 802.11 ™ -2016 modificada por IEEE Std 802.11ai ™ -2016, IEEE Std 802.11ah ™ -2016 y IEEE Std 802.11aj ™ -2018) - Norma IEEE para tecnología de la información- Telecomunicaciones e intercambio de información entre sistemas Redes de área local y metropolitana: requisitos específicos Parte 11: Control de acceso medio (LAN) de la LAN inalámbrica y especificaciones de capa física (PHY) Enmienda 4: Mejoras para enlaces de tránsito dentro de redes puenteadas" (IEEE Standards Association (IEEE-SA), 2018).
"IEEE Std 802.11aj-2018 (Enmienda a IEEE Std 802.11-2016 modificada por IEEE Std 802.11ai-2016 e IEEE Std 802.11ah-2016) - Norma IEEE para tecnología de la

información - Telecomunicaciones e intercambio de información entre sistemas Redes de área local y metropolitana --Requisitos específicos Parte 11: Control de acceso medio (MAC) y especificaciones de capa física (PHY) de la LAN inalámbrica. Enmienda 3: Mejoras para un rendimiento muy alto para soportar bandas de frecuencia de onda milimétrica en chino (60 GHz y 45 GHz)" (IEEE Standards Association (IEEE-SA), 2018).

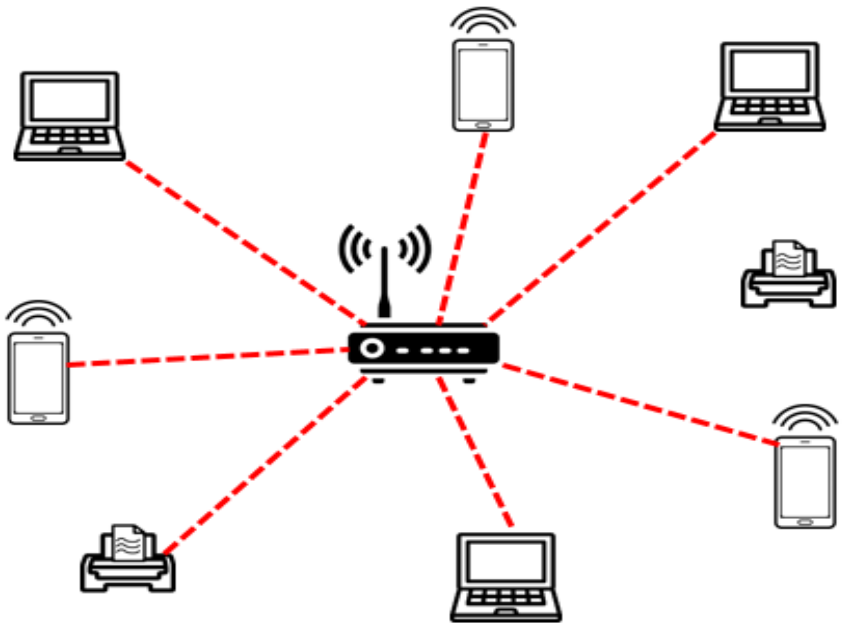

Ilustración 12: Red de Área Local Inalámbrica (WLAN).

1.3 Gestión y seguridad en Red

Gestión de red

"Los servicios de Gestión de Red le brindan mayor visibilidad y control de las operaciones así como la transportación segura de la información de la Empresa, mejorando la experiencia de usuarios y clientes." (Telmex, 2018)

Partiendo de este fragmento informativo podríamos resaltar la importancia de mantener un sistema de red administrado, monitoreado y con una gestión que permita la gobernabilidad ya que hoy en día las comunicaciones son parte fundamental no solo de las personas sino de la operatividad en las empresas, siendo cada vez mayor el número de equipos y aparatos conectados entre sí.

Seguridad y la red

"Durante las primeras décadas de su existencia, las redes de computadoras fueron usadas principalmente por investigadores universitarios para el envío de correo electrónico, así como por empleados corporativos para compartir impresoras. En estas condiciones, la seguridad no recibió mucha atención. Pero ahora, cuando millones de ciudadanos comunes usan redes para sus transacciones bancarias, compras y declaraciones de impuestos, y que se ha encontrado una debilidad tras otra, la seguridad de las redes se ha convertido en un problema de proporciones masivas." (S. Tanenbaum & J. Wetherall, 2012, pág. 657)

1.3.1 Seguridad de red

Hoy en día la protección de las redes de computadora lejos de ser un lujo es una necesidad, por la gran cantidad de transacciones y operaciones que estas representan, podríamos visualizar el entorno de una empresa en que las operaciones de producción, nomina, ventas, facturación e incluso las transacciones bancarias dependen de un sistema el cual se comunica a través de la red a los diferentes equipos anfitriones aunque esta red es una red de área local (LAN) que en ocasiones consta de diferentes segmentos esta comunicada a Internet o la nube siendo esta red LAN vulnerable a ataques ya que el internet representa una puerta hacia el exterior, por esta razón es de suma importancia la protección de la red.

1.3.2 Seguridad perimetral

Con el apoyo del Documento "Seguridad Perimetral. Catálogo de Empresas y Soluciones de Seguridad TIC del Instituto Nacional de Tecnologías de la Comunicación (INTECO)", podemos entender el concepto de Seguridad perimetral como la protección de los equipos dentro del perímetro de nuestra red, en donde el perímetro marca los límites de la conexión de nuestra red y el exterior con otras redes, por este motivo la frontera es vigilada para evitar la intrusión de agentes no autorizados o la fuga de datos, en pocas palabras evitar ataques desde fuera y dentro de nuestra red.

Un ataque sucede cuando desde fuera o desde dentro de la red se usan los fallos o vulnerabilidades en nuestros sistemas para comprometerlos y causar algún tipo de problema operativo, perdida de información o fuga de datos, podríamos definir cuatro diferentes tipos de ataques que afectan nuestro perímetro de red:

1. Denegación de servicio: Ataques denominados como DoS por sus siglas en inglés "Denial of Service", En el libro Hacking Desde Cero coordinado por Daniel Benchimol nos menciona que es uno de los ataques por excelencia que busca saturar algún recurso hardware, software o ambos en un sistema específico.
2. Ataque contra autentificación (Impide o sustituye autentificación a quienes tienen una autentificación legítima).
3. Ataque de modificación y daños (Ataca directamente a Datos y sistemas sensibles): La gravedad de este ataque aumenta cuando el individuo atacante ha obtenido privilegios de administrador, y que la finalidad de este ataque es modificar los datos o el software del equipo infectado.
4. Ataques de puerta trasera o backdoor: Se define como una secuencia especial que evita los pasos de autenticación para acceder a un sistema

En la actualidad la frontera o perímetro de las redes tiende a ser algo complicado debido al tipo de conexiones que se establecen en la actualidad, imaginemos la empresa que hoy en día realiza la carga de pedidos a su servidor en su red interna de forma remota, en este caso el perímetro se ha convertido en un perímetro dinámico lo que se puede definir como perímetro difuso el cual es necesario proteger.

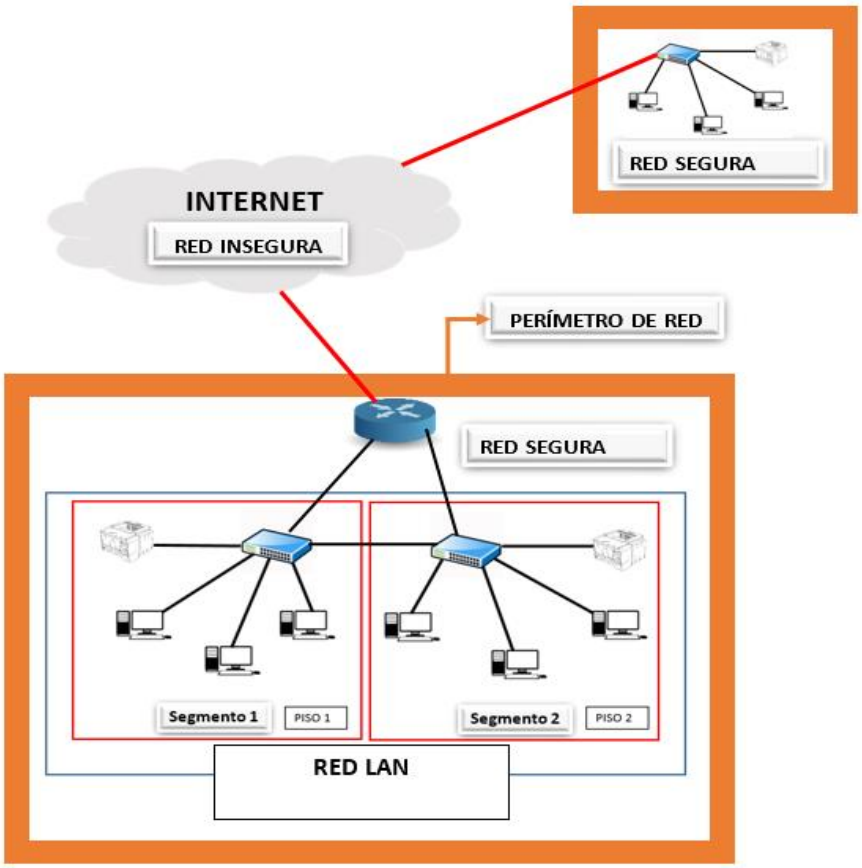

Ilustración 13: Representación de Perímetro de Red y el Internet.

Bajo este criterio de proteger la seguridad perimetral y la seguridad perimetral difusa utilizamos: Cortafuegos (o Firewall en inglés), VPN (del inglés Virtual Prívate Network) e IPS/IDS (del inglés, Intrusion Prevention Systems/Intrusión Detection Systems) acompañada de una gestión de control de acceso e identidadntidad.

Los equipos como Cortafuegos, VPNs e IPS/IDS, están destinados a proteger los sistemas y dispositivos conectados a una red y establecer un perímetro de seguridad en el cual se garantice la comunicación segura, con el fin de evitar accesos no autorizados y proteger la red de ataques externos e internos, mediante la supervisión del cumplimiento de normas o políticas de seguridad establecidas para ello rastrean y controlan las comunicaciones, bloqueando el tráfico, detectando comportamiento anómalo y ataques en la red, para evitar agentes no autorizados en la red.

1.4 Supervisión y Mecanismos de Seguridad

1.4.1 Prácticas recomendadas

En el libro Hacking Desde Cero coordinado por Daniel Benchimol nos da algunas recomendaciones y vulnerabilidades comunes por lo que a continuación se explican las recomendaciones para mejorar la seguridad de una Institución.
Para poder tener una buena seguridad en nuestra institución o nuestra red no solo basta con tener programas y equipos de seguridad, un punto clave en esto son las llamadas buenas prácticas las cuales a menudo no se cumplen en las organizaciones algunas de las prácticas o medidas de seguridad que debemos tomar en la organización son:

1. No usar el usuario de administrador para todo sino solo en caso de que sea estrictamente necesario, debido a que si este usurario o algún proceso que se ejecute con este tipo de privilegios se vieran comprometido este lo hará tomando los privilegios de administrador teniendo acceso a los servicios ejecutados con estas credenciales.

2. Correcta gestión de actualizaciones y parches de sistemas, teniendo en cuenta el previo análisis de impacto que tendrán estas sobre nuestros sistemas.
3. Ajustar las características de los sistemas de forma personalizada para cada organización, esto implica habilitar o deshabilitar las funciones y procesos según sean las necesidades de la organización al igual que tratar de tener actualizadas las aplicaciones.
4. Otorgar los privilegios necesarios a cada usuario no más ni menos solamente los necesarios para desarrollar sus funciones, esto apoyara el disminuir el riesgo de la explotación de un error que comprometa la operación, así mismo tendremos como ventaja una fluidez mayor en el equipo.
5. Mantener siempre tanto un respaldo como un detalle de las modificaciones efectuadas a un determinado programa a esto se le denomina Control de Cambios, esto implica tener documentado cualquier cambio efectuado en algún equipo, red o sistema con la finalidad de determinar alguna falla en caso de que sea provocada a partir de este cambio y las posibles vulnerabilidades derivadas.
6. Definición de cuentas y contraseñas, como ya se mencionó la definición de roles y usuarios es una práctica en la que se otorgan solo los accesos necesarios no más a cada uno de los usuarios para que puedan realizar sus actividades, además de definir que usuarios tiene acceso a qué apartado del sistema o equipo, sigue definir políticas para la creación de contraseñas y la caducidad de las mismas, a continuación, se mencionan algunas recomendaciones para contraseñas:
    - Uso de contraseñas robustas: Contraseñas que ocupen diferentes caracteres alfanuméricos sin sentido ni consecutivos, incluyendo mayúsculas y minúsculas.

- Contraseñas con una longitud larga ya que entre más larga sea la contraseña más segura será se recomienda por lo menos 8 caracteres.
- El cambio de contraseñas incluso las más largas debe ser periódico, (por lo menos cada 60 días aproximadamente).
- No usar más de una vez la misma contraseña.
- Las contraseñas son confidenciales por lo que solo el usuario propietario de la cuenta deberá tenerla de memoria.

7. Revisión de Registros y Logs de sistemas con la finalidad de detectar posibles errores y accesos no autorizados e incluso accesos fallidos.
8. Cambiar siempre las Contraseñas predeterminadas de los sistemas.
9. Uso de herramientas de seguridad perimetral como Firewall (corta fuegos).
10. No abrir ficheros adjuntos con procedencia o extensión dudosa.
11. No ejecutar programas con orígenes desconocidos.
12. Mantener actualizados los sistemas, especialmente en las actualizaciones de seguridad.
13. Definición de políticas para el respaldo de la información, para este caso es importante destacar la importancia de definir el lapso de tiempo en que se realizaran los respaldos de información, tomando en cuenta la importancia de los cambios y cada cuanto tiempo se realizan de forma administrada, además de definir lo que se respaldara y lo que no, siendo las 3 modalidades para respaldo las siguientes:
    - Full o normal
    - Incremental
    - Diferencial

1.4.2 Firewall

1.4.2.1 ¿Qué es un firewall?

Para definir que es un firewall nos apoyaremos en el autor Estrada y su libro Seguridad por Niveles además analizaremos rápidamente los siguientes conceptos:
Sniffer: *"un sniffer sólo captura tráfico y lo presenta de manera más o menos amigable (y nada más)"* (Estrada, Seguridad Por Niveles, 2011, pág. 47)
Libpcap: "*Estar en capacidad de "desarmar" los encabezados de cada protocolo. Esto también lo conocemos y es nuestra conocida librería "libpcap"."* (Estrada, Seguridad Por Niveles, 2011, pág. 187)
En resumidas palabras un Firewall o cortafuegos es una barrera que bloquea el paso de cierta información por lo que el firewall es capaz de escuchar todo el tráfico que se analiza en la red (esta es la técnica que utilizan los sniffer), el firewall es capaz de abrir los encabezados de cada protocolo (libpcap) y tener patrones estandarizados para comprender cada protocolo, también en este firewall se contienen reglas previamente definidas que decidirán que se deja pasar y que no.

1.4.2.2 Tipos de Firewall o cortafuegos

El Instituto Nacional de Tecnologías de la Comunicación (INTECO) nombra algunas clasificaciones de firewall las cuales explicamos a continuación: Los corta fuegos o firewalls se pueden clasificar de diferentes formas una de ellas es según el nivel o capa en la que operan o según el alcance de protección que estos tengan.

Clasificación por el nivel en el que operan

- Firewall de nivel de red: Estos Tienen como característica principal operar en la capa de red, implementando en tiempo real las políticas para la protección,

normalmente en esta categoría entran los routers o enrutadores con este tipo de funciones.

- Firewall a nivel de aplicación: "Operan por encima de la capa de red, a «nivel de aplicación» y son capaces de controlar protocolos específicos y aplicaciones, por ejemplo, los cortafuegos para mensajería instantánea o de aplicaciones web y P2P (del inglés *Peer to Peer*). Dentro de este tipo se incluyen los cortafuegos-proxy (filtran protocolos de nivel de aplicación HTTP, FTP, SMTP,..). Dentro de esta subcategoría están los *Gateways* y *Proxys* a nivel de aplicación." (Instituto Nacional de Tecnologías de la Comunicación (INTECO), 2010, pág. 11)

Clasificación según el alcance de protección.

- Firewalls personales: Son equipos de protección que se encuentran instalados en un ordenador o puesto de trabajo, en esta rama entran los firewalls que generalmente vienen preinstalados en los sistemas operativos.
- Firewall Corporativo: Este tipo de corta fuegos están diseñados para soportar el transito masivo de conexiones que existen en una red corporativa pudiendo así gestionar cientos o miles de conexiones entrantes y salientes, además son capaces de trabajar a nivel de red y de aplicación.

"En cuanto a su formato pueden presentarse integrados en software de aplicación, como en el caso de navegadores, formando parte de sistemas operativos, formando parte de dispositivos de red, o como dispositivos hardware específicos o integrados con otras funcionalidades de seguridad." (Instituto Nacional de Tecnologías de la Comunicación (INTECO), 2010, pág. 11).

- Firewall software: Este tipo de corta fuegos generalmente vienen incorporados en sistemas operativos e incluso podemos tomar estos como los que se distribuyen de forma gratuita.
- Router/Proxy/Gateway con funcionalidad de Firewall: Equipos dedicados que incorporan funcionalidades de cortafuegos.
- Firewall UTM (del inglés *Unified Thread Management)*: Los Firewall de Gestión unificada de amenazas o UTM son servidores o equipos que integran funcionalidades de protección firewall entre otras funcionalidades dentro de una misma interfaz, pudiendo proteger desde pequeñas hasta grandes redes.
- Firewall appliance: Este tipo de firewall hacen referencia a plataformas hardware diseñadas con usos específicos.
- Sistema de prevención y detección de intrusos (IPS / IDS): El IDS (del inglés Intrusión Detection System), se encarga de proporcionar a la red un grado de seguridad preventiva mediante alertas dirigidas a los administradores de sistemas, mientras que los IPS (del inglés Intrusión Prevention System), ejerce el control de acceso en las redes informáticas con la finalidad de brindar protección ante ataques deteniendo los ataques cuando estos se estén llevando a cabo un ejemplo de esto es una serie de reglas en el firewall.
- Filtrado de contenido: Este tipo de herramientas generalmente son utilizadas con la finalidad de controlar, limitar y restringir el acceso a contenido web, generalmente para crear condiciones para el acceso al cierto contenido en internet mediante navegadores, teniendo como principal ejemplo el control parental que incluyen algunos navegadores para controlar el acceso a menores a ciertas páginas web.

1.4.3 VPN

Las redes privadas virtuales (VPN del inglés *Virtual Private Network*) según el Instituto Nacional de Tecnologías de la Comunicación (INTECO), permiten ampliar el perímetro seguro de la red de la organización interconectando sedes, oficinas, o equipos situados en una región geográfica distante o un enlace ajeno al de la red usando túneles cifrados a través de Internet y utilizando técnicas de traducción de direcciones.

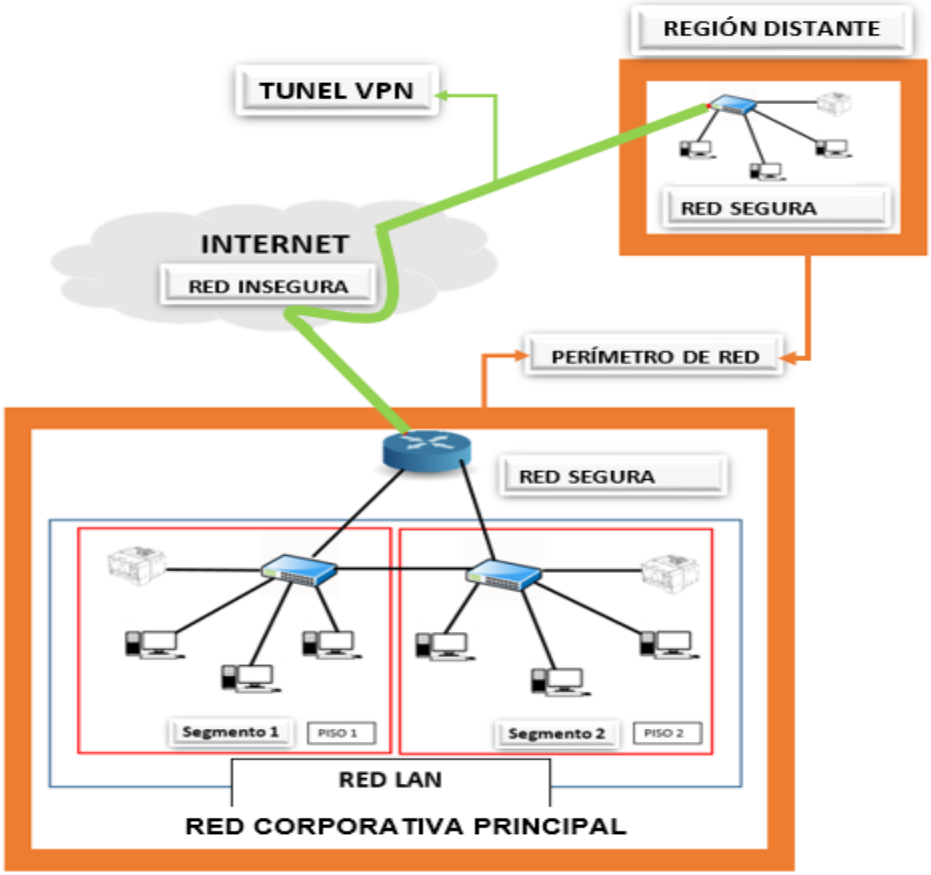

Ilustración 14: Representación de Redes distantes conectadas de manera segura mediante un túnel VPN.

1.4.4 VLAN

Las redes de Área Local Virtual o VLAN (del inglés, Virtual Local Área Network), para poder explicar este tema nos basaremos en los autores Tanenbaum y Wetherall y su libro Redes de computadora Quinta edición, así como en el autor Estrada y su obra Seguridad en Redes:

En los primeros días de las redes de área local, cables amarillos gruesos serpenteaban por los ductos de muchos edificios de oficinas. Conectaban a todas las computadoras por las que pasaban. No importaba cuál computadora pertenecía a cuál LAN. Todos los usuarios de oficinas cercanas se conectaban a la misma LAN aunque no estuvieran relacionados con ella. La geografía triunfaba sobre los gráficos organizacionales corporativos.

Todo cambió con el surgimiento de los cables de par trenzado y los hubs en la década de 1990. El cableado de los edificios se renovó (a un costo considerable) para desechar todas las mangueras amarillas de jardín e instalar cables de par trenzado desde cada oficina hasta gabinetes centrales al final de cada pasillo o en una sala central de máquinas, Si el vicepresidente a cargo del cableado era un visionario, se instalaba cable de par trenzado categoría 5; si era un simple administrador, se instalaba el cable telefónico (categoría 3) existente (que tenía que reemplazarse algunos años más tarde con la aparición de Fast Ethernet).

En la actualidad, los cables han cambiado y los hubs se han convertido en switches, pero el patrón de cableado sigue siendo el mismo. Este patrón hace posible la configuración de redes LAN lógicas en vez de físicas. (S. Tanenbaum & J. Wetherall, 2012, pág. 294)

Para entender cómo funcionan las redes VLAN imaginemos una empresa que desea integrar 10 equipos en 2 oficinas diferentes estos 10 equipos estarán conectados a un segmento de la red diferente ya que 6 son de los administradores en la empresa (Conectadas al servidor administrativo), mientras que los 4 restantes

pertenecen al personal que realiza pruebas (Conectadas al servidor de Pruebas),como se muestra en la Ilustración 15, así mismo podremos ver en la imagen que la forma en que se dividen estas redes es mediante una división lógica y no física ya que todos los equipos se conectan a un solo switch y este es el encargado de crear 2 redes virtuales físicamente unidas pero lógicamente separadas con la finalidad de crear un camino a cada uno de los equipos según su fin, de esta forma si los equipos de prueba llegan a generar un error este no afectará a los equipos administrativos, teniendo así una mayor gobernabilidad en la administración de la red.

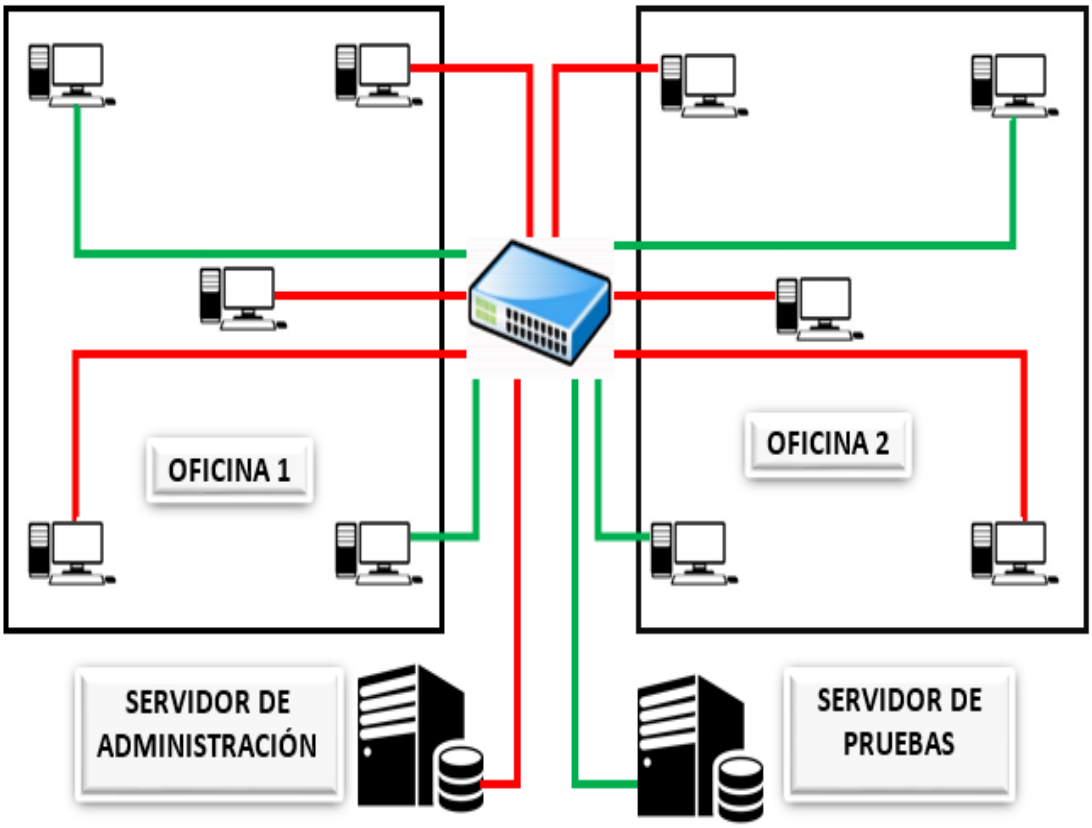

Ilustración 15: Representación de una Red VLAN.

Basándonos en este ejemplo imaginemos que se requiere agregar o encaminar un equipo de pruebas al área administrativa, bastará con agregarlo a la VLAN administrativa, en pocas palabras realizar el cambio de red de forma lógica y no física.

De esta forma el administrador del área de sistemas deberá definir cuantas VLAN necesita en la red y que equipos pertenecerán a que red virtual, para así tener una mayor gobernabilidad y una reacción ante cambios, una forma de poder crear un diagrama que ayude a futuros cambios e identificaciones cuando se tiene más de una red virtual es:

"A menudo se les asignan nombres mediante colores (de manera informal), ya que de esta manera es posible imprimir diagramas a color que muestren la disposición física de las máquinas, con los miembros de la LAN roja en rojo, los de la LAN verde en verde, etc. De esta forma, tanto el diseño físico como el lógico se pueden reflejar en un solo esquema" (S. Tanenbaum & J. Wetherall, 2012, pág. 296)

El instituto IEEE (del inglés Institute of Electrical and Electronics Engineers), estandarizo este tipo de conexiones bajo el estándar IEEE 802.1Q, Este protocolo es el utilizado para la creación de VLANs sobre un mismo Switch bajo el concepto de Trunking.

El estándar IEEE 802.1Q: *"permite la creación de VLANs, agregando un encabezado de 4 bytes dentro de la misma trama Ethernet. Para que un Switch "encapsule 802.1q" debe tener configurada sus interfaces y sus VLAN para ello. Las buenas prácticas, nos indican que si tenemos más de un switch, es mejor hacerlo bajo la idea de Interfaces "Trunk" (o troncal), que no son otra cosa que enlaces físicos entre los dispositivos (generalmente Switchs, aunque no exclusivo de estos) por los cuales "entroncaremos" (aunque suene feo…) varias VLAN, transportando el tráfico de varias de estas a la vez creando una especie de jerarquía entre ellos."* (Estrada, Seguridad en Redes, 2016, pág. 149)

Existe una VLAN por defecto (VLAN1 o VLAN nativa), esta es capaz de trabajar ante cualquier error o sin configuración previa, a través de esta el Switch envía toda trama sin agregar ningún encabezado 802.1Q por lo que está VLAN por defecto debe ser deshabilitada como una medida de seguridad.

La forma en que funcionan las VLAN es relativamente fácil de comprender ya que para distinguir el tráfico entre VLAN a cada trama se le agrega un campo de 4 octetos el cual contiene: Un Tag Protocol Identifier, Priority, CFI (Canonical Format Indicator) y un VLAN ID, a todo el tráfico entrante por un puerto el Switch añade el campo y al ser recibido por la otra parte se le quita el campo quedando intacto el trama original.

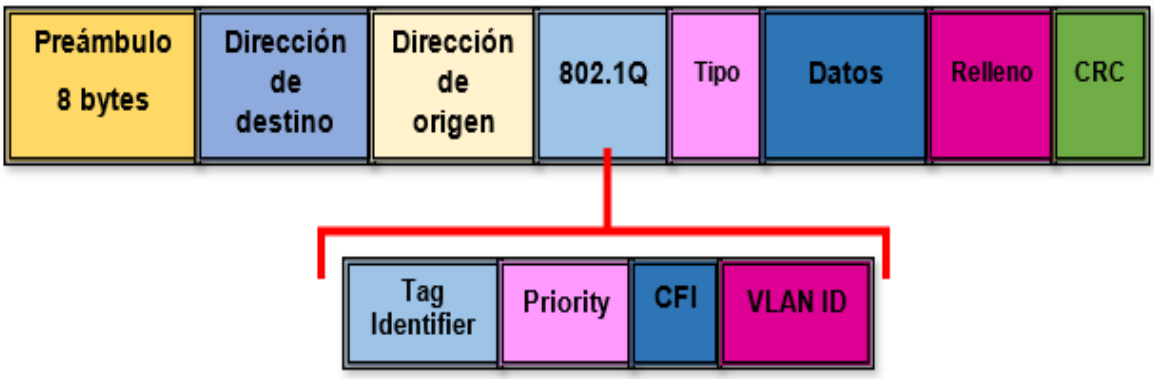

Ilustración 16: Trama 802.1Q.

- Tag Protocol Identifier: Consta de 16 bits y en él se contiene el valor 0x8100 (al encontrarse el valor 8100 se sabe que se deberán procesar cuatro octetos adicionales los cuales identifican al protocolo 802.1Q), mediante esto se identifica la trama como etiquetada.
- Priority: Consta de 3 bits e indica la prioridad de la trama, Siendo 0 el menor y 7 el mayor.
- CFI (Canonical Format Indicator): Consta de 1 bit en él se marca como 0 para Switch Ethernet.

- VLAN ID: En este apartado se especifica la VLAN a la que pertenece la trama y consta de12 bits (se pueden tener 4096 VLAN).que especifican la VLAN a la que pertenece la trama, es posible tener 4096 VLANs.
- Preámbulo: Indica que comienza una trama y permite la sincronización de relojes.
- Tipo o longitud: Al hablar de este campo tenemos que tener presente que si se habla del estándar 802.3 se refiere a la longitud del campo de datos *"En particular, cuando hablamos de redes LAN cableadas, hoy en día el estándar de facto es 802.3 "Ethernet" (o CSMA/CD: Carrier Sence Multiple Access / Collition Detect)"* (Estrada, Seguridad en Redes, 2016, pág. 139)

1.4.5 Redes Inalámbricas

Tomando como referencia el documento Seguridad en redes y seguridad de la información de Miguel Soriano podemos decir que las redes inalámbricas WLAN (del inglés Wireless networks), son redes sumamente populares en la actualidad ya que ofrecen un servicio de conexión que no limita la movilidad y permite tener conexión en casi cualquier punto dentro de la cobertura inalámbrica, pero al poder acceder a la red siempre que este se encuentre al alcance es un riesgo, por ese motivo es de suma importancia tener medidas de seguridad para estas redes que puedan garantizar un cifrado de contenido, autentificación de usuarios y un control de acceso a la red.

1.4.5.1 Seguridad en redes inalámbricas

Usando como referencia la información proporcionada en el documento "Seguridad en redes y seguridad de la información" del autor Miguel Soriano podremos decir

que la seguridad en redes inalámbricas es de suma importancia por lo que es necesario contar con los siguientes puntos.

- Autenticación: Procesó mediante el cual los usuarios acceden a las redes inalámbricas, por lo que solo realizando una autentificación correcta se podrá acceder a la red.
- Confidencialidad: Estas redes son autentificadas mediante el uso de algoritmos criptográficos siendo los más utilizados RC4 (WEP) y AES (WPA2).
- Gestión de claves: Forma en que se distribuyen y administran las claves de acceso a la red.

El protocolo WEP (Wired Equivalent Privacy) se utiliza de manera opcional como complemento al estándar IEEE 802.11a/g/b, ofreciendo los servicios de autenticación, confidencialidad y autenticación WEP.

La autentificación WEP se puede realizar mediante 2 formas:

- Autentificación abierta o clave compartida: Estas usan un identificador de red SSID (del inglés *Service Set Identifier*), el SSID es solo un identificador de red inalámbrico y no una contraseña, al utilizar la autentificación abierta el punto de acceso inalámbrico WAP (Wireless access point), difunde este identificador de forma periódica con intervalos de algunos segundos, mientras que el usuario envía una trama de autenticación con los datos de identificación del usuario para ser analizado para al final permitir o denegar el acceso.

- Autentificación con clave WEP: La clave es la misma para todos los usuarios de la red inalámbrica, es importante cuidar la forma en que se distribuye este dato.

El protocolo WEP usa un cifrado RC4 con claves de 64 o 128 bits la cual se divide en una clave secreta que usara 40 o 104 bits + un vector de inicialización de 24 bits. *"El protocolo WEP no es resistente contra los ataques conocidos (monitorización de actividad, ataque de fuerza bruta, ataque de repetición, etc....) y el algoritmo RC4, tal como se emplea en WEP, se rompió en 1996"* (Soriano, pág. 75)
El protocolo WPA (Wi-Fi Protected Access) fue aceptado en 2002 con la finalidad de eliminar las vulnerabilidades del protocolo WEP como una solución temporal, en ese momento se trabajaba en el nuevo estándar IEEE 802.11i (el estándar IEEE 802.11i se aprobó en 2004). El protocolo WPA al igual que el WEP utiliza el cifrado RC4 con nuevos mecanismos de seguridad, las partes principales que componen este protocolo son:

- Temporary Key Integrity Protocol (TKIP)
- Message Integrity Check (MIC)
- Control de acceso basado en el estándar 802.1x con el protocolo EAP (Extensible Authentication Protocol).

El estándar 802.11i o como se le conoce como WPA2 se utiliza como algoritmo criptográfico a AES con longitud de 128 bits, sus principales mecanismos de seguridad son la confidencialidad, autentificación y la integridad. Es importante resaltar que este fue roto en 2017 y nace el nuevo protocolo WPA3 el cual sustituye a WPA2.

"*WPA3 está disponible en nuevos enrutadores certificados por Wi-Fi Alliance, y depende de cada proveedor si instalará el protocolo en enrutadores existentes con una actualización de software."* (Huatala, 2018)

1.4.5.2 Portal cautivo

Como nos menciona la marca Linksys, Un portal cautivo es una página de inicio de sesión en redes inalámbricas, todos los usuarios invitados deberán acceder antes de conectarse a la red Wiffi, esto es muy útil para controlar el acceso a la red Wiffi por parte de personas invitadas o temporales.

Mediante este portal es posible controlas usuarios específicos y limitar el tiempo de conexión para estos, *"Normalmente un portal cautivo presenta al usuario los términos de servicio y este debe aceptarlos expresamente antes de poder acceder al hotspot Wi-Fi."* (Belkin International, Inc., s.f.)

1.4.6 Herramientas

A continuación se presentan algunas herramientas que pueden apoyar a las organizaciones en la creación y gestión de Firewall, VPN, VLAN y un control de redes inalámbricas como Portal cautivo entre otras herramientas, mediante tablas se realizara la comparación de algunas características, costo requisitos necesarios para su uso con la finalidad de elegir una solución que cubra las necesidades de este proyecto, la información contenida en las Tabla *1*, Tabla *2* y Tabla *3* se obtuvo usando como referencia los siguientes portales:

PfSense, en el portal del proveedor Netgate:

- Documentación oficial *"https://www.netgate.com/docs/pfsense/ "* (Rubicon Communications LLC, s.f.)
- Libro pfSense *"https://www.netgate.com/docs/pfsense/book/ "* (Rubicon Communications, s.f.)
- Aplians "*https://www.netgate.com/products/appliances/"* (Rubicon Communications, LLC, s.f.)

OPNsense, en su portal de documentación y comercial

- Wiki *"https://wiki.opnsense.org/manual.html"* (Deciso B.V., s.f.)
- Apoyo comercial "*https://opnsense.org/support-overview/commercial-support/ "* (Deciso B.V., s.f.)

Cisco serie ASA-5500, información consultada en portal de un distribuidor no filial de Cisco

- Distribuidor Router-switch Ltd. Modelo ASA-5506-K9 *"http://www.router-switch.com/asa5506-k9-p-5695.html* " (Router-switch Ltd., s.f.)
- Distribuidor Router-switch Ltd. Modelo ASA5555-K9 *"http://www.router-switch.com/asa5555-k9-p-4622.html"* (Router-switch Ltd., s.f.)

Es importante resaltar la comparación mostrada en las tablas, en ellas se representan las características principales que cubren con las necesidades del proyecto, en la comparación de equipos dedicados se toma como costo mínimo el equipo más pequeño que cubre las características contenidas en la tabla y en costo máximo los equipos con mayores capacidades para atender un número mayor de usuarios.

Dispositivo o Sistema	PfSense	OPNsense	SERIE ASA500 (ASA5506-K9)
Capacidad Multi WAN	Permite múltiples conexiones WAN, el software se ha probado con hasta 12 redes WAN y se ha soportado, no se conoce límite exacto de conexiones WAN.	Permite la función de múltiples conexiones de redes WAN, no se especifica el número soportado.	No especificada
Balanceo de Cargas	Permite un equilibrio de carga de modo Gateway (para múltiples conexiones WAN) y Servidor (para distribuir tráfico entre múltiples servidores)	Permite equilibrio de cargas entre diferentes redes WAN	No especificada
Servidor DHCP	Permite administrar y gestión un servidor DHCP IPv4 e IPv6, para cada red LAN.	Administra Servidor DHCP	Cuenta con interfaz Gigabit Ethernet 8X1, Permite DHCP
NAT (Network Address Translation)	Permite el reenvió de puertos y direcciones IP.	Permite creación de entradas NAT.	Aplica
Firewall	Permite administración de reglas de firewall para controlar el tráfico decidiendo lo que pasa y lo que no en la red.	Permite administrar reglas de Firewall mediante categorías para definir lo que pasa y lo que no en la red.	Configuración centralizada, registro, monitora e informes
VPN	Contiene diferentes tecnologías para la comunicación VPN *OpenVPN *IPsec *IKEv2 *L2TP / IPsec	Permite VPN *IPsec *PPTP *IPsec *OpenVPN	Permite VPN sitio a sitio mediante IPsec, se requiere licencia para este modulo

Administración de Redes LAN	Permite la creación de Múltiples Redes LAN mediante el uso de las interfaces OPT (pfSense nombra así a los puertos extra siendo puerto WAN, LAN , OPT1,OPT2….),estos puertos OPT se pueden usar como LAN o WAN	No especificado	Permite la creación de Redes según el número de puertos del equipo Interfaz (Gigabit Ethernet 8 x 1)
Administración de Redes VLAN	Permite la creación de LAN Virtuales, siempre que se usen dispositivos basados en el estándar 802.1Q	Permite la compatibilidad con VLAN 802.1Q	Permite administrar redes VLAN, es necesario adquirir licencia para esta función
Portal Cautivo	Permite redireccionar a los usuarios a una página web alojada en el firewall antes de permitir el acceso a internet, obligando al usuario a autenticarse para poder navegar en internet.	Permite forzar la autenticación a una página de inicio, una vez autenticado el usuario podrá acceder a la red.	No especificada
Limitación de ancho de banda a usuarios	Permite la limitación de ancho de banda en el portal cautivo.	Permite la limitación de ancho de banda en el portal cautivo.	No especificada

Tabla 1: Comparación de características principales de herramientas de seguridad de red.

Para analizar los costos de las herramientas se toma en cuenta la capacidad de adaptación del software pfSense, OPNsense y equipos Cisco.

- pfSense permite su uso en hardware dedicado así como la adaptación del software a diferente hardware, los requisitos mínimos para la instalación de pfSense son: CPU mínimo de 600 MHz, RAM mínima de 512 MB, 4 GB mínimo de espacio de almacenamiento, Una o más tarjetas de red compatibles.
- OPNsense no existe hardware dedicado por lo que los requisitos mínimos para su instalación son: CPU mínimo de 500 MHz, RAM mínima de 512 MB, 4 GB mínimo de espacio de almacenamiento.
- Los equipos Cisco son equipos dedicados creados para usos específicos y sus características dependerán del modelo que se adquiera, para nuestro proyecto se nos recomendó la serie Cisco ASA-5500, por parte del distribuidor Router-Switch Ltd. en su página oficial mediante chat en línea.

	PfSense		**OPNsense**	
Precio	Mínimo	Máximo	Mínimo	máximo
Costo de hardware adaptable	$1,000 pesos Mx	$5,000 o mas	$1,000 pesos Mx	$5,000 o mas
Costo de licencia	No Aplica	No Aplica	No Aplica	No Aplica
Costo/hora de análisis para la solución	No Aplica	No Aplica	No Aplica	No Aplica
Costo de Póliza de soporte	$2,124 dólares/36 meses	$9,324 dólares/36 meses	4 horas $399 euros	16 horas $1,439 euros
Costo de Implementación	No Aplica	No Aplica	No Aplica	No Aplica

Tabla 2: Comparación de costo usando Herramientas con Hardware adaptable.

En la Tabla 2 se presenta la comparación de precios entre los software pfSense y OPNsense usando hardware adaptable, en esta tabla no se incluye el equipo de la serie ASA-5500 debido a que estos equipos son de hardware dedicado.

- El rango de precio mínimo y máximo es con referencia a los precios de equipos que cubren sus requisitos mínimos encontrados en mercado libre, es posible que la empresa reutilice equipos o cotice el equipo que mejor le convenga, dadas sus necesidades y presupuesto con cualquier proveedor de tecnologías.
- El rango de precio mínimo y máximo de soporte se toma del portal oficial de cada uno de los software, en la tabla se presenta el costo de la póliza de soporte siendo el valor mínimo la póliza más pequeña que se puede comprar y el valor máximo la póliza más completa que se puede adquirir.

	PfSense Appliance		**Cisco**	
Precio	Mínimo	Máximo	Mínimo	Máximo
Costo de hardware dedicado	$349 dólares	$5,298 dólares	ASA5506-K9 $575 dólares	ASA5525-K9 $4,250 dólares
Costo de licencia	No Aplica	No Aplica	Licencia anyconnect L-AC-VPNO-25, solo 25 usuarios VPN $1,398 dólares	Licencia anyconnect L-AC-VPNO-25, solo 25 usuarios VPN $1,398 dólares
Costo de análisis para la solución	No Aplica	No Aplica	de $0 dólares por hora	$150+IVA dólares por hora
Costo de Póliza de soporte	$588 dólares/1 año	$2,988 dólares/1 año	$150 dólares por hora de consultoría de ingeniería	$150 dólares por hora de consultoría de ingeniería

Tabla 3: Comparación de costo usando Herramientas con Hardware dedicado.

En la Tabla *3* se presenta la comparativa de costo entre equipos con hardware dedicado para esta tabla el software OPNsense no aplica debido a que este no cuenta con hardware dedicado.

- El costo mínimo de hardware representa el equipo más básico de cada herramienta que cubre en gran parte con las necesidades planteadas en este proyecto, mientras que el costo máximo representa el equipo más robusto de estas series el cual cuenta con funciones para una mayor atención de usuarios y velocidad.
- El costo de Licencia representa el costo de la licencia que se adapta mejor a las necesidades planteadas, en el caso del equipo ASA la licencia fue recomendada por el proveedor Router-Switch Ltd. en su página oficial mediante chat en línea.
- La póliza de soporte se toma como costo mínimo la póliza más pequeña ofrecida por el proveedor de equipo y el máximo la póliza más robusta.
- En algunos casos el hecho de solicitar una cotización de un equipo se cuenta como hora de consultoría por lo que el simple hecho de solicitar una cotización Cisco puede representar un costo.

1.5 Monitoreo de recursos informáticos

Tomando como referencia al autor Alejandro Corletti podemos decir que, Tener una supervisión y monitoreo ofrece un grado de disponibilidad y seguridad además de una detección temprana de comportamientos anómalos en los sistemas con la finalidad de tener reacciones tempranas y evitar problemas mayores.

Estas funciones son realizadas a través del NOC (Network Operation Center) y SOC (Security Operation Center), estas deberán ser congruentes al tipo de red, tamaño y necesidades sin importar que tan pequeña o grande sea la red para así garantizar una Supervisión, Monitorización y alarmas que ayuden a prevenir ciertos problemas futuros.

Primero hay que diferenciar los roles de NOC y SOC

NOC Centro de operaciones de red (del inglés Network Operation Center): Este se encarga principalmente del monitoreo y administración de recursos informáticos, todo esto en tiempo real para garantizar una alta disponibilidad de los recursos, algunos de los puntos que debe tomar en cuenta son:

a) Anomalías en el incremento de ancho de banda.
b) Saturación de red.
c) Caídas inesperadas de equipos.
d) Alarmas en almacenamiento, bases de datos, memoria o procesadores.
e) Fallos en los sistemas.
f) Ausencia o pérdida de segmentos de red.
g) Modificación de datos de acceso a sistemas o redes.
h) Notificación de accesos fallidos

SOC Centro de operaciones de seguridad (del inglés Security Operation Center): El SOC esta principalmente encargado de la supervisión de seguridad, encargado de la detección y prevención de amenazas que comprometan los recursos informáticos de la organización.

1.5.1 Objetivos del monitoreo

"Los sistemas de monitoreo permiten la visualización, con o sin grabación, de todo lo que sucede en un recinto" (Benchimol, 2011, pág. 79)

Partiendo de este punto imaginemos una empresa la cual labora 24x7 esta no cuenta con sistema de monitoreo de sus recursos informáticos y aunque tengan personal de sistemas cubriendo en todo momento estos asuntos, atenderá las

incidencias hasta que estas sucedan, por lo que se detendrá el área afectada hasta que el ingeniero logre reestablecer el incidente todo por no tener un sistema que supervise dichos recursos en tiempo real y avise de forma temprana si está sucediendo algún evento anómalo que deba ser atendido.

1.5.2 Herramientas de monitoreo

A continuación se comparan tres herramientas de monitoreo la información se describe en tablas en las cuales se puede encontrar información como:

Tabla 4: Contiene una comparación de sus principales características

Tabla 5: Contiene los requisitos necesarios para la instalación del servidor de monitoreo

Tabla 6: Contiene el costo de implementación de estas herramientas, así como el costo de soporte.

La información contenida en las tablas se obtuvo de los portales:

Herramienta Nagios:

- Especificaciones y licenciamiento: "*https://www.nagios.com/products/nagios-xi/ "* (Nagios Enterprises, LLC., s.f.)
- Costo de soporte: *"https://www.nagios.com/services/nagios-xi-support-plans/"* (Nagios Enterprises, LLC., s.f.)
- Requisitos de sistema: *"https://assets.nagios.com/downloads/nagiosxi/docs/Nagios-XI-Hardware-Requirements.pdf#_ga=2.40112034.1207346008.1537602885-1932980082.1537508595"* (Nagios Enterprises, LLC., 2017)

Herramienta PRTG NETWORK MONITOR:

- Características: *"https://www.es.paessler.com/prtg"* (Paessler AG, s.f.)
- Requisitos de sistema: *"https://www.es.paessler.com/prtg/requirements"* (Paessler AG, s.f.)

- Costo de licencia y soporte: *"https://shop.paessler.com/shop/prtg/new/?preselected_license=1020&_ga=2.187154159.699476633.1536195510-1882227319.1536195510"* (Paessler AG, s.f.)

Herramienta Zabbix:

- Características y requisitos de sistema: *"https://www.zabbix.com/documentation/3.2/manual/introduction/about "* (Zabbix SIA., s.f.)
- Costo de soporte: *"https://www.zabbix.com/support"* (Zabbix LLC., s.f.)

	Nagios XI	**PRTG NETWORK MONITOR**	**Zabbix**
Permite visualizar monitoreo mediante gráficas en tiempo real.	Permite visualizar gráficas sobre el comportamiento de la red.	Permite la creación de gráficas individuales.	Si, el software permite crear gráficas para su visualización en tiempo real.
Permite visualizar mapas con alertas.	No especificado.	Permite crear páginas web con datos de supervisión.	Permite la creación de plantillas o mapas para mostrar las alertas de diferentes puntos.
Permite definir umbrales personalizados para disparar alertas.	Permite definir umbrales, Las notificaciones por alertas se envían mediante correo electrónico o mensaje de texto a móviles.	Permite el ajuste de métricas para el aviso de alertas, compatible con móviles mediante aplicaciones para Android, iOS y Windows Phone.	Es posible ajustar el umbral en el que las alertas entran en acción, permite él envió de notificaciones vía correo electrónico.
Almacenamiento histórico.	Permite él envió de informes programados.	Permite la descarga de informes históricos en formato PDF, HTML, CSV y XML.	Permite configurar el almacenamiento histórico en una base de datos.
Administración y configuración.	Administración mediante un portal WEB para configuración y actualizaciones.	Administración y configuración a través de una interfaz gráfica.	Esta se realiza mediante un portal web de forma gráfica.

Tabla 4: Comparativa de herramientas de monitoreo.

	Nagios XI	PRTG NETWORK MONITOR	Zabbix
Requisitos de sistema	Requisitos mínimos Disco duro: 20 GB Memoria RAM:2 GB CPU: Doble núcleo.	Métrica por sensor o ítem a monitorear, ejemplo si en un pc se monitorea el CPU cuenta como un sensor.	El espacio de disco dependerá de la cantidad de datos que se desean almacenar como históricos.
	50 host Disco: 40 GB CPU: 1-2 Cores RAM: 1-4 GB	1000 sensores (100 dispositivos) Disco: 250 GB CPU: 2 Cores RAM: 3GB	Mínimos RAM:128 MB Disco: 256 MB
	100 host Disco: 80 GB CPU: 2-4 Cores RAM: 4-8 GB	1,000-2,500 sensores (250 dispositivos) Disco: 500 GB CPU: 3 Cores RAM: 5GB	500 anfitriones CPU: 2 Cores RAM: 2 GB
	>500 host Disco: 120 GB CPU: >4 Cores RAM: >8 GB	2,500-5,000 sensores (500 dispositivos) Disco: 1 TB CPU: 5 Cores RAM: 8GB	>1000 anfitriones CPU: 4 Cores RAM: 8 GB
		5,000-10,000 sensores(1,000 dispositivos) Disco: 2 TB CPU: 8 Cores RAM: 16GB	>10,000 anfitriones CPU: 8 Cores RAM: 16 GB
Sistema operativo para instalar	CentOS o Redhat Enterprise Linux(RHEL) versión 6 o 7	Con hardware x64 pc/Server de no más de 2 años de antigüedad o usando Windows Server 2012 R2	Linux IBM AIX FreeBSD NetBSD OpenBSD HP-UX Mac OS X Solaris

Tabla 5: Característica para la instalación de herramientas de Monitoreo

	Nagios XI	PRTG NETWORK MONITOR	Zabbix
Costo de licencia	$3,495 dólares Soporte y mantenimiento incluido por 1 año.	500 sensores $1,600 dólares. 1,000 sensores $2,850 dólares. La compra de cualquier licencia incluye 12 meses de mantenimiento.	Gratuita.
Costo de soporte y/o mantenimiento	Soporte y mantenimiento 100 nodos: $1695 dólares.	Costo de mantenimiento 1 año en plan de licencia 500 sensores, $360 dólares.	Póliza de soporte Bronce Anual: $1,550 dólares 4 Incidentes, No incluye Soporte a proxy Zabbix, no incluye soporte telefónico.
	Soporte y mantenimiento 200 nodos: $2995 dólares.	2 años de mantenimiento en plan de licencia 500 sensores $680 dólares.	Póliza de soporte Anual Silver $2,950 dólares 8 Incidentes Soporte telefónico 8x5 No incluye Soporte a proxy Zabbix.
	Soporte y mantenimiento 300 nodos: $3995 dólares.	Costo de mantenimiento 1 año en plan de licencia 1,000 sensores, $641.26 dólares.	Póliza de soporte Anual Gold $5,950 dólares Incidentes ilimitados Soporte telefónico 8x5 Soporte a proxy Zabbix por $595 dólares extra.
	Es posible sumar un paquete de 10 llamadas por $2,995 dólares o de 5 llamadas por $1,995 dólares.	2 años de mantenimiento en plan de licencia 1,000 sensores $1,211.25 dólares.	Póliza de soporte Platinum Anual $11,900 dólares Incidentes ilimitado Soporte telefónico 24x7 Soporte a proxy Zabbix por $1,190 dólares extra.
	Los soportes solo incluyen 10 incidentes de soporte por correo electrónico al año.	Mantenimiento no incluye soporte solo actualizaciones de la plataforma y corrección de errores.	Póliza de soporte Enterprise Anual $59,900 dólares Incidentes ilimitado Soporte telefónico 24x7 Soporte a proxy Zabbix incluid.

Tabla 6: Comparación de Costo de Herramientas de Monitoreo.

1.6 Respaldo de información en la Red

*"Uno de los activos intangibles más importantes para cualquier organización es la información. Es claro que sin esta, toda empresa o institución dejaría de funcionar, pues se trata de un elemento indubitablemente necesario para su operación diaria. Para garantizar que las instituciones puedan disponer de información en el momento que es requerida cuando se presenta una eventualidad, es necesario llevar a cabo un proceso preventivo denominado "respaldo" o "*backup*". "* (Martínez, 2014)

1.6.1 ¿Qué es un Respaldo o Backup?

Para abordar el tema de Respaldo nos apoyaremos en el autor Alejandro Corletti Estrada, así como en una publicación del Instituto de Ingeniería de la UNAM realizada por parte de Cuauhtémoc Vélez Martínez, Un respaldo es una copia de la información de la organización, usuarios, bases de datos o servidores entre otras aplicaciones importantes para la organización o usuario, la cual se actualiza periódicamente para tener la información al día con la finalidad de garantizar la restauración y portabilidad de la organización ante una contingencia que haga que la información se pierda.

Los respaldos generalmente se almacenan en discos externos, memorias flash, discos compactos, la nube o incluso en servidores locales o remotos.

Como ya se mencionó en el tema 1.4.1 Practicas recomendadas, existen tres formas principales de gestionar los respaldos:

- Full o normal: En esta modalidad se resguardan todos los archivos y carpetas seleccionados sin importar si han sido modificados o no.

- Incremental: Se copian solamente los archivos modificados o creados después del ultimó respaldo.
- Diferencial: Este respaldo es muy similar después de la incremental en su primer ejecución, esto significa que la primera vez que se realice un respaldo diferencial se copiaran los datos que hayan sido creados o modificados solamente pero para los siguientes respaldos seguirá copiando todos los archivos modificados o creados a partir del respaldo original.

El personal de sistemas tendrá la obligación de determinar que respaldo será el más conveniente para la organización con base en qué tipo de respaldo cubra mejor las necesidades de la misma y tomando en cuenta el espacio de almacenamiento con el que cuente.

Las formas o medios más comunes de realizar respaldos son:

a) Cintas de almacenamiento: Son de bajo costo pero su tiempo de lectura y escritura es relativamente alto.
b) Servidores en la nube: Al utilizar Internet ya que los respaldos se alojan en servidores remotos es de suma importancia contar con conexiones de alta velocidad.

   Servidor local o Repositorio local: Los respaldos se almacenan en un servidor conectado a la red LAN de la empresa.
c) Dispositivos extraíbles y discos duros externos: Son dispositivos para almacenar información como memorias flash, discos, o discos duros externos, al no estar integrados a una red se deberán conectar directamente al equipo al que se quiere realizar el respaldo

d) Discos duros internos y servidores espejo: Este tipo de almacenamiento permite que un disco duro se replique sobre un espacio específico con características similares al del respaldo.

1.6.2 Importancia de los Respaldos

"Existen casos documentados de empresas que han desaparecido debido a que, después de un ataque informático, un sismo, una inundación, un incendio o vandalismo, sus equipos de cómputo quedan inservibles y, al no contar con respaldos o tener respaldos obsoletos, les resulta virtualmente imposible recuperar o actualizar la información generada a lo largo de meses e incluso años." (Martínez, 2014)

Por este motivo es de suma importancia establecer políticas y parámetros que definan que se respalda y que no todo dependiendo de las políticas establecidas y la disponibilidad de espacio para almacenar los respaldos.

Tenemos que entender que el personal de sistemas es el responsable de realizar los respaldos de información, pero el usuario es responsable de la información en su equipo por lo que se recomienda al personal de sistemas definir carpetas y tipos de archivos a ser respaldados así como una serie de políticas que deberá transmitir al usuario para estandarizar el respaldo a usuarios.

1.6.3 Buenas prácticas

Como se trató en el tema anterior, el establecer políticas que garanticen la fiabilidad del respaldo es un tema efectivo por lo que a continuación se presentan algunas o recomendaciones:

a) Mantener por lo menos 3 versiones consecutivas del respaldo en caso de que este se llegue a dañar.
b) Mantener los respaldos en más de un dispositivo de almacenamiento en caso de que alguno sufra un daño.
c) Mantener una copia del respaldo fuera del sitio de trabajo de manera segura en caso de un daño en el área de trabajo (Siempre contemplando la seguridad de los datos).
d) Definir la frecuencia con que se realizan los respaldos, tomando como base la frecuencia con que los datos a respaldar sufren modificaciones.
e) Definir no solo fechas exactas para los respaldos sino un horario especifico.
f) Definir condiciones para efectuar los respaldos.
g) Definir políticas de respaldo para los usuarios (Tipos de archivos que se respaldarán y los que no), con la finalidad de optimizar el espacio y evitar posibles infecciones al respaldo
h) Definir políticas de ubicación de respaldo para usuario: Es recomendable establecer ubicaciones o carpetas en las que el usuario deberá introducir los archivos a ser respaldados.

1.6.4 Sistema de respaldo

Hay que tomar en cuenta que el tener un respaldo de información, para una organización que tienen más de un equipo al que debe realizar este respaldo se vuelve complicado hacerlo de forma manual, equipo por equipo usando medios extraíbles como muchas organizaciones lo realizan, al ser una tarea complicada y tediosa tanto para el usuario como para el personal de sistemas existe la posibilidad que este tipo de organizaciones tomen la decisión de realizar el respaldo solo a los servidores de la organización, dejando en el aire la información de los usuarios.
Por este motivo es importante contar con sistemas de respaldo más eficiente, y si los equipos se encuentran en una red es conveniente utilizar esta ventaja para poder acelerar el proceso y garantizar la información.
Una opción es crear un servidor de respaldos que no es otra cosa que un servidor conectado en red y con una gran capacidad el cual se usara para almacenar los respaldos de usuarios y servidores o si bien se prefiere usar un dispositivo NAS.

1.6.4.1 Que es una NAS

Almacenamiento Conectado en Red (NAS del inglés Network Attached Storage*)*
"Un sistema NAS es un dispositivo de almacenamiento conectado a una red que permite almacenar y recuperar los datos en un punto centralizado para usuarios autorizados de la red y multiplicidad de clientes. Los dispositivos NAS son flexibles y expansibles; esto lo que implica es que a medida que vaya necesitando más capacidad de almacenamiento, podrá añadirla a lo que ya tiene." (Seagate Technology LLC, s.f.)

1.6.4.2 RAID

Tomando como referencia el portal de Dell e Intel, podemos decir que un RAID es un grupo de discos físicos que ofrecen un alto rendimiento, el arreglo RAID mejora el rendimiento de tráfico de datos y disponibilidad de los mismos, este sirve como apoyo cuando se produce la perdida de datos por un error en un disco físico regenerando los datos perdidos desde los disco restantes. Las Niveles o tipos más comunes de RAID son:

RAID 0: *""Permite grabar datos en varios discos físicos en vez de hacerlo en un solo disco físico. RAID 0 implica particionar cada espacio de almacenamiento del disco físico en bandas de 64 KB. Estas bandas se intercalan de forma secuencial y repetida. La parte de la banda que hay en un único disco físico se denomina elemento de banda."* (Dell, 2018)

- Ejemplo de este se nos presenta el escenario de cuatro discos usando RAID 0, el segmento 1 se graba en el disco 1 el 2 en el 2, 3 en 3 y 4 en 4, se mejora el rendimiento de acceso pero no proporciona redundancia de datos.

RAID 1: Presenta un grabado simultaneo en otro disco *"Si uno de los discos falla, el contenido del otro disco puede utilizarse para arrancar el sistema y regenerar el disco físico con error."* (Dell, 2018)

RAID 5: *"De tres o más unidades de disco duro con los datos se dividen en bloques administrables denominados divisiones. Las ventajas principales de RAID 5 son la capacidad de almacenamiento y protección de datos."* (Intel Corporation, 2017), En pocas palabras en RAID 5 el tamaño de la unidad más pequeña multiplicado por uno menos de la cantidad de la unidad, ya que una unidad de disco se utilizará para almacenar la información de paridad.

- Un ejemplo planteado por Intel es el de cuatro unidades de disco duro de 120 GB cada una, al usar una matriz RAID 5, el sistema solo vera 360 GB en vez de 480, debido a que una unidad de cada disco duro será utilizada para almacenar la redundancia.

1.6.5 Herramientas de respaldo

Herramientas para la gestión de almacenamiento en red, la información recopilada en la Tabla 7 se obtuvo de los siguientes portales:

Herramienta XigmaNAS

- Compatibilidad de Hardware en *"https://www.xigmanas.com/wiki/doku.php?id=xigmanas_users_hardware"* (XigmaNAS, 2018), es posible consultar la compatibilidad con equipos NAS de diversas marcas.
- Interfaz en *"https://www.xigmanas.com/index.php?id=4"* (XigmaNAS, s.f.)
- Especificaciones y características en *"https://www.xigmanas.com/wiki/doku.php"* (XigmaNAS, 2018)
- Requerimientos de sistema *"https://www.xigmanas.com/wiki/doku.php?id=documentation:setup_and_user_guide:hardware_requirements"* (XigmaNAS, 2018)

Herramienta FreeNAS

- Características y requerimientos: *"http://doc.freenas.org/11/freenas.html"* (iXsystems, s.f.) y *"http://www.freenas.org/about/features/"* (iXsystems, Inc., s.f.)
- Costo de equipos dedicados (Certificados): *"http://www.freenas.org/freenas-certified-servers/"* (iXsystems, Inc., s.f.) y *"http://www.freenas.org/freenas-mini/"* (iXsystems, Inc., s.f.) , para conocer el costo de servidores más es necesario solicitar cotización en el primer enlace y para pequeños equipos el portal de FreeNAS nos proporciona un enlace directo de compra en Amazon.

Herramienta openmediavault

- Características y requerimientos en *"https://openmediavault.readthedocs.io/en/latest/index.html"* (Volker Theile, s.f.)
- Licencia en *"https://www.openmediavault.org/licensing.html"* (Volker Theile, s.f.)

	XigmaNAS	FreeNAS	openmediavault
Hardware dedicado (certificado).	No aplica.	Cuenta con una amplia gama de dispositivos, según las necesidades de las organizaciones.	No aplica.
Hardware adaptable	Aplica, es compatible con diferentes NAS de otros proveedores.	Aplica.	Aplica.
Panel de configuración y gestión.	Panel Grafico mediante Web.	Panel Grafico mediante Web.	Panel Grafico mediante Web.
Documentación y soporte.	Documentación oficial en su sitio, Soporte en Blogs y comunidad Posibilidad de chat en vivo con la comunidad.	Documentación oficial en su sitio, Soporte en Blogs y comunidad Permite la autoayuda al brindar cursos online gratuitos.	Documentación oficial en su sitio Soporte en Blogs y comunidad.
Administración RAID.	RAID admitidos: 0,1,5	Stripe, Mirror, RAIDZ1, RAIDZ2, RAIDZ3.	Niveles de RAID admitidos:0,1,10,5 y 6
Requisitos de instalación.	Procesador Multi núcleo de 64 bits RAM 8 GB Uno o más discos duros.	Procesador a 64 bits RAM 8 GB Una unidad para su instalación Uno o más discos para almacenamiento.	Procesador compatible con x86-64 o ARM RAM: 1GB o más Unidad del sistema Unidad de almacenamiento.
Costo de licencia.	No aplica.	No aplica.	No aplica.
Costo de soporte.	No aplica.	No aplica.	No aplica.
Costo de hardware dedicado.	No aplica.	Equipos desde $1,284.00 dólares.	No aplica.

Tabla 7: Herramientas de Almacenamiento en Red, Características y Costo.

CAPITULO 2 LICENCIA DE SOFTWARE

Hay que tener claro que el uso de un programa dependerá del tipo de licencia que tengamos para usar o modificar este programa, si el programa depende del pago para su uso o modificación y la organización no lo cubre, al usar el programa lo está realizando de forma apócrifa o ilegal por lo que se podría hacer acreedor a algún tipo de sanción.

2.1 Software Libre y Open Source

Cuando hablamos de software libre generalmente pensamos en el proyecto GNU el cual es principalmente financiado por la Free Software Foundation o FSF, *"La FSF patrocina el proyecto GNU, el continuo esfuerzo de proporcionar un sistema operativo completo licenciado como software libre. También financiamos y promovemos importantes desarrollos de software libre y proporcionamos sistemas de desarrollo para los mantenedores de software GNU, incluyendo servicios de correo electrónico, Shell y listas de correo."* (Hine, s.f.)

Como se nos menciona en la página oficial del Proyecto GNU hay que tener en claro la diferencia entre Software libre y Open Source (Código Abierto), *"Cuando decimos que el software es «libre», nos referimos a que respeta las libertades esenciales del usuario: la libertad de utilizarlo, ejecutarlo, estudiarlo y modificarlo, y de distribuir copias con o sin modificaciones. Es una cuestión de libertad y no de precio, por lo tanto piense en «libertad de expresión» y no en «barra libre»"* (Stallman, 2017), mientras que al referirnos a Open Source (Código Abierto), según la Open Source Initiative (OSI), el código abierto debe cumplir los criterios siguientes: Redistribución gratuita, Código fuente, Trabajos derivados, Integridad del código fuente del autor, No discriminación contra personas o grupos, No discriminación contra campos de

esfuerzo, Distribución de la licencia, La licencia no debe ser específica de un producto, La licencia no debe restringir otro software, La licencia debe ser neutra desde el punto de vista tecnológico

2.1.1 Software Libre

Según el proyecto GNU podemos definir al software libre como, "*software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Es decir, el «software libre» es una cuestión de libertad, no de precio. Para entender el concepto, piense en «libre» como en «libre expresión», no como en «barra libre».*" (GNU Operating System, 2018), a continuación se explican las cuatro libertades planteadas por el proyecto GNU:

1. Libertad 0: Nos presenta la libertad de ejecutar el programa a voluntad.
2. Libertad 1: Estudiar y modificar el software para que se ajuste a las necesidades de la organización.
3. Libertad 2: Redistribución de copias.
4. Libertad 3: Distribución de copiar modificadas.

Para que se cumplan las libertades uno, dos y tres es necesario contar con el código fuente del software para su estudio y modificación en caso de ser necesario.

2.1.2 Open Source (Código Abierto)

"La Iniciativa de Código Abierto (OSI) es una corporación de beneficio público de California, con exención de impuestos 501 (c) 3, fundada en 1998." (Open Source Initiative, s.f.)

Como ya se mencionó cuando hablamos de código abierto no solo se habla de código fuente sino que la página oficial de Open Source Initiative, nos presenta diez criterios que resumiremos a continuación:

1. Redistribución gratuita: "*La licencia no debe restringir a ninguna parte de vender o regalar el software como un componente de una distribución agregada de software que contiene programas de varias fuentes diferentes. La licencia no requerirá un canon u otra tarifa por tal venta."* (Open Source Initiative, 2007)
2. Código fuente: "*El programa debe incluir el código fuente y debe permitir la distribución en el código fuente y en el formulario compilado. Cuando alguna forma de producto no se distribuye con el código fuente, debe haber un medio bien publicitado para obtener el código fuente por un costo de reproducción no superior a lo razonable, preferiblemente descargando a través de Internet sin cargo. El código fuente debe ser la forma preferida en que un programador modificará el programa. Código fuente deliberadamente ofuscado no está permitido. No se permiten formularios intermedios, como la salida de un preprocesador o un traductor."* (Open Source Initiative, 2007)
3. Trabajos derivados: "*La licencia debe permitir modificaciones y trabajos derivados, y debe permitir que se distribuyan bajo los mismos términos que la licencia del software original."* (Open Source Initiative, 2007)
4. Integridad del código fuente del autor*: "La licencia puede restringir la distribución del código fuente en forma modificada* solo *si la licencia permite*

la distribución de "archivos de parche" con el código fuente con el fin de modificar el programa en tiempo de compilación. La licencia debe permitir explícitamente la distribución de software creado a partir de código fuente modificada. La licencia puede requerir trabajos derivados para llevar un nombre o número de versión diferente del software original." (Open Source Initiative, 2007)

5. No discriminación contra personas o grupos: "*La licencia no debe discriminar a ninguna persona o grupo de personas."* (Open Source Initiative, 2007)
6. No discriminación contra campos de esfuerzo: "*La licencia no debe restringir a nadie el uso del programa en un campo específico de esfuerzo. Por ejemplo, puede no restringir el uso del programa en un negocio, o ser utilizado para investigación genética."* (Open Source Initiative, 2007)
7. Distribución de la licencia: "*Los derechos adjuntos al programa deben aplicarse a todos aquellos a los que se redistribuye el programa sin la necesidad de la ejecución de una licencia adicional por esas partes."* (Open Source Initiative, 2007)
8. La licencia no debe ser específica de un producto: *"Los derechos adjuntos al programa no deben depender de que el programa sea parte de una distribución de software en particular. Si el programa se extrae de esa distribución y se usa o distribuye dentro de los términos de la licencia del programa, todas las partes a quienes se redistribuye el programa deben tener los mismos derechos que los otorgados junto con la distribución de software original."* (Open Source Initiative, 2007)
9. La licencia no debe restringir otro software: "*La licencia no debe imponer restricciones sobre otro software que se distribuye junto con el software licenciado. Por ejemplo, la licencia no debe insistir en que todos los demás programas distribuidos en el mismo medio deben ser software de código abierto."* (Open Source Initiative, 2007)

10. La licencia debe ser neutra desde el punto de vista tecnológico: *"Ninguna disposición de la licencia puede basarse en ninguna tecnología individual o estilo de interfaz."* (Open Source Initiative, 2007)

Observación: Podemos observar que existe diferencia entre Software Libre y Código abierto pero al final luchan por algunas metas afines como la libertad de distribución de software, por este motivo ambos son una solución accesible y a bajo costo para las organizaciones.

"Casi todo el software de código abierto es software libre" (Stallman, 2017)

2.2 Categoría de Software Libre y no Libre

Características de software libre y no libre planteadas por el proyecto GNU.

- Software libre: Es aquel software que autoriza a cualquiera usar, copiar, modificar, distribuir de forma gratuita o mediante un pago a cualquier persona, por lo que es necesario que el código fuente del software esté disponible para todo público.
- Software de código abierto (*Open Source*): A pesar que la mayoría de las personas utilizan la expresión código abierto (Open Source), para referirse a las categorías de software libre el proyecto GNU nos dice que la diferencia radica en como el proyecto Open Source acepta ciertas licencias que el software libre considera demasiado restrictivas y en algunos casos el Open Source no ha aceptado licencias que el software libre sí.
- Software de dominio público: Cuando se habla de software de dominio público hacemos referencia a software que no tiene derechos de autor solo si el código fuente es de dominio público se habla de un caso de software libre sin copyleft por lo que algunas versiones de este software pueden no ser software libre.

"En el marco del Convenio de Berna, que la mayoría de los países han firmado, todo lo que se escribe queda automáticamente bajo el dominio de los derechos de autor, inclusive los programas informáticos. Por lo tanto, si usted quiere que un programa que ha escrito esté disponible en el dominio público, debe tomar algunas medidas legales para renunciar a esos derechos; de lo contrario el programa quedará sujeto a los derechos de autor." (GNU Operating System, 2018)

- Software con copyleft: El software con copyleft es considerado como software libre y garantiza que todas las copias y modificaciones tengan los mismos términos de distribución, este tipo de licencia generalmente evita que terceros agreguen requisitos adicionales al software (permite un límite de requisitos que se consideren seguros) esto con la finalidad de evitar que el software sea privativo. Es importante resaltar que dos licencias con copyleft generalmente son incompatibles por lo que no es posible combinar el código de dos software con diferente licencia copyleft.
- Software libre sin copyleft: Cuando el software no cuenta con copyleft incluye los permisos de modificación y redistribución así como el de incluir restricciones, por este motivo si un software es software libre y no se encuentra bajo un copyleft es posible que algunas modificaciones o copias del mismo no lo sean, en otras palabras un desarrollador o empresa de software podrá usar el código y compilarlo con una restricción para volverlo privativo.
- Software con licencia permisiva, laxa: Este tipo de licencia permiten usar el código e inclusive la distribución binaria privativa con o sin modificación del código.
- Software con licencia GPL (General Public License): La Licencia Pública General de GNU se conforma por un conjunto de cláusulas de distribución para publicar software con copyleft.

- Software GNU bajo copyright de la FSF: Los desarrolladores de GNU pueden transferir los derechos a la FSF o quedárselos, en caso que se transfieran los derechos a la FSF el software será software GNU con derechos de autor de la FSF quien al adquirir los derechos deberá hacer cumplir la licencia.
- Software que no es libre (nonfree software): En esta categoría entra aquel software que está prohibido su uso, redistribución, modificación, o es necesario tener un permiso.
- Software Privativo: En la actualidad la definición de software Privativo es un sinónimo de Software no libre
- Freeware: Se refiere a software que permite su redistribución pero no su modificación (el código fuente no se encuentra disponible),
- Shareware: Software del que se permite la redistribución de copias pero su uso está sujeto al pago de licencia, los programas shareware no son considerados software libre de ninguna forma ya que su código fuente no está disponible y no se cuenta con permisos para modificarlo además es necesario adquirir una licencia para su uso.
- Software privado: Software que ha sido desarrollado para un usuario u organización específica, por lo que este lo mantiene y no lo publica de ninguna forma, aunque parezca que este software es privativo la realidad es que puede ser software libre si el usuario cuenta con las cuatro libertades del software libre.
- Software comercial: El software comercial es aquel software desarrollado por una empresa como como parte de su operación comercial, no necesariamente es privativo, este tipo de software se pueden encontrar algunos ejemplos de software libre, así como privativos.

2.3 Software de Propietario (Software de Pago)

Cuando hablamos de software Propietario o Software de pago hablamos de software que se protege bajo los derechos de autor y no cumple con las libertades estipuladas por la FSF, generalmente para usar el software es necesario realizar una activación mediante una licencia la cual tiene un costo para el usuario, al no adquirir esta licencia de forma original puede estar incumpliendo las cláusulas de contrato de licencia por lo que se puede hacer acreedor a una sanción, en caso de adquirir la licencia esta no solo podrá ser instalada en el número de equipos estipulados en el contrato de licenciamiento adquirido de lo contrario se podría hacer acreedor a una sanción a continuación se muestra un ejemplo:

"*¿Puedo instalar mi copia de Windows en varios equipos?*
No puedes instalar Windows en más equipos de los que se establece en los términos y condiciones de la licencia de software de Microsoft. Por regla general, solo se puede instalar una copia de Windows en un equipo." (Microsoft, 2017)
Hay que resaltar que al usar software de propietarios o pago incluye un soporte por parte de la empresa (en algunas ocasiones este soporte debe contratarse como módulo extra), como nos indica el soporte de Microsoft el tener licenciado nuestro software podremos recibir actualizaciones de seguridad y características.

2.4 Software Libre o Software Propietario (Software de Pago)

La realidad es que el Software de pago es una solución práctica y con una guía de soporte sustentada bajo el nombre de una empresa que nos vende el software y en ocasiones el soporte, además en este tipo de software las organizaciones solo tendrán acceso a los módulos y soportes que puedan pagar, en muchos casos no cubren con la totalidad de sus necesidades pero ampliar las pólizas resulta un

incremento no rentable por la empresa, muchos de estos software de pago son integrados a un hardware en específico en ese caso si la organización decide implementarlo deberá no solo adquirir las licencias del software sino el hardware y complementos que la empresa proveedora de software estipule elevando aún más la inversión para su implementación algunos puntos importante que podemos denotar del Software de pago son:

- Soporte por la empresa proveedora de software.
- Actualizaciones y parches de seguridad.
- En ocasiones Hardware diseñado específicamente para el uso de Software.
- Documentación y manuales creados por la empresa proveedora del software (en ocasiones esta puede tener un costo extra).
- Los responsables de área no deben preocuparse por incidentes en caso de tener soporte del software ya que el proveedor los asesora.
- En ocasiones el software o la póliza de soporte contratada implica que el administrador de T.I. será un operador con privilegios administrativos dejando al proveedor los cambios mayores en el software.
- Cualquier personalización o modificación se realiza por parte del proveedor del servicio y en ocasiones tiene un costo extra.
- En muchas ocasiones el Software de propietario obliga a las organizaciones a comprar los paquetes de software compatibles con sus sistemas.
- Debido a que el software de propietario es muy comercial es más probable su adaptación para la compatibilidad con software comercial.

A diferencia del software de pago el software libre permite una gran libertad a las organizaciones de adaptar los diferentes sistemas a sus necesidades, aunque el soporte de estas, está sujeto a los conocimientos y documentación proporcionada por el creador del software así como comunidades y foros de discusión donde se

tratan temas relacionados como el proyecto GNU o la FSF además algunos desarrolladores de software libre ofrecen pólizas de soporte por una cuota, el software libre no está sujeto a un hardware especifico por lo que la reutilización de hardware es una opción para las organizaciones, puntos que podemos resaltar del software libre.

- El software libre ayuda a las organizaciones a cubrir a bajo costo las necesidades de software.
- El software libre es flexible, por lo que es posible adaptarlo a cualquier organización.
- El software libre también cuenta con pólizas de soporte por parte de algunos desarrolladores de software.
- El software libre al no estar atado a un hardware en particular permite la adaptación a las necesidades de la empresa.
- El software libre busca ser compatible con otro software y trabajar de manera amigable.
- Al ser un software flexible es necesario que el software se personalice para adaptarse a las necesidades y aplicaciones de la organización.

Observación: El tipo de software a elegir por una organización puede depender de las necesidades, presupuesto, conocimientos del encargado de TI así como la compatibilidad de software usado por la empresa ya que en resumen el software propietario permite a la organización tranquilidad al ser el software respaldado por marcas conocidas y al responsable de TI le quita una carga de trabajo al responsable de TI al dedicarse a realizar soportes primer nivel y canalización de incidentes o personalizaciones al área de soporte del software contratado, siendo el responsable de TI el encargado de coordinar este soporte.

En el caso de software libre, es una alternativa para las organizaciones con la que cubrirán las necesidades de software a bajo costo y de manera flexible, En este caso el rol del administrador de TI. (En caso de no contratar una póliza de soporte para el software que se desea utilizar), será la de asistir no solo en soporte primer nivel de la organización sino el será el encargado de dar soporte completo a los sistemas por lo que tendrá que darse a la tarea de estudiar las diferentes documentaciones a su disposición.

CAPITULO 3 PROYECTO

3.1 Introducción

Se presenta una solución de software sin problemas de licenciamiento al que referiremos como libres, por su libertad de ser utilizado y distribuido sin costo además de contar con amplias opciones de soporte y documentación. Tomando como referencia los puntos planteados en el Método se presenta un diagrama de cómo se realizó el proyecto.

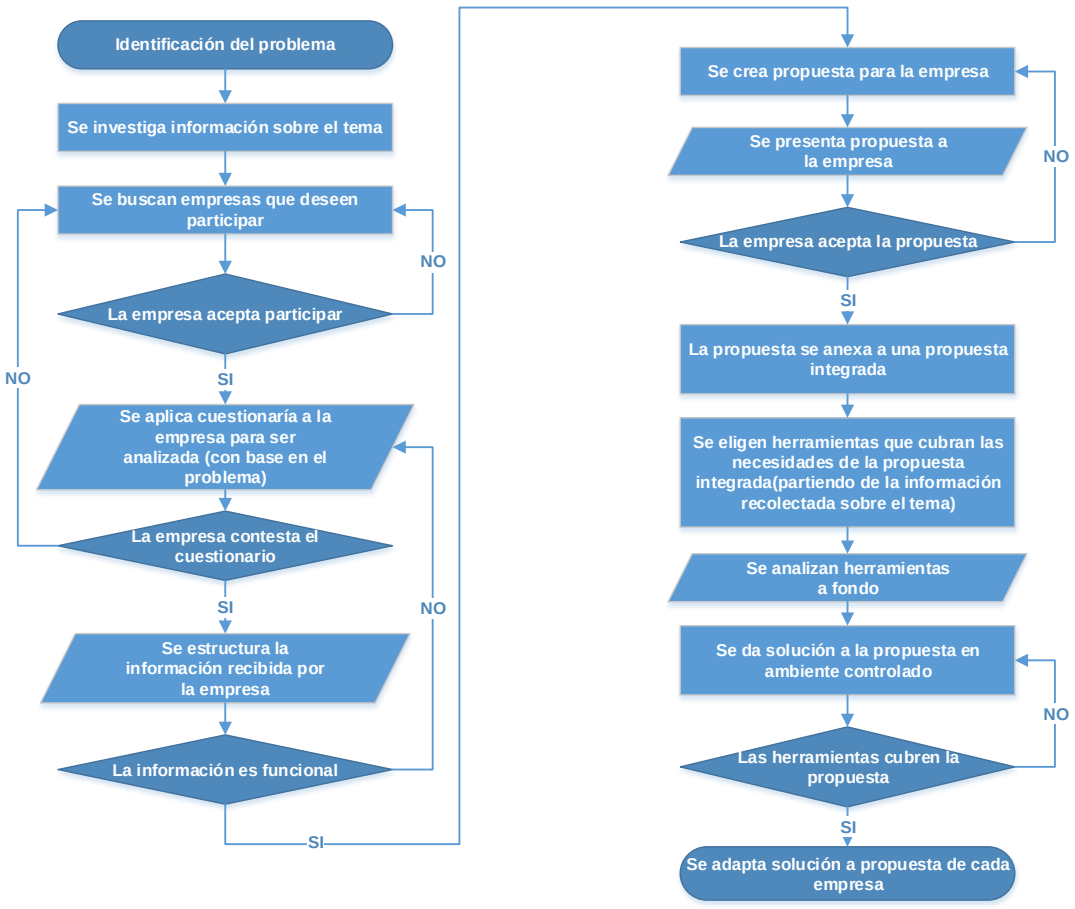

Ilustración 17: Modelo del Proyecto.

3.2 Población Muestra

Para este proyecto se buscó la participación de tres empresas, los datos mostrados fueron recabados mediante un cuestionario contestado por los encargados del área de TI de cada empresa para poder tener una idea real de la problemática que presentan las empresas.

a) Vidrios y Cristales Industrializados S.A. (VYCISA)

1. Empresa dedicada a la manufactura del cristal.
2. Asesor Financiero de la empresa: C.P. Carlos Gallardo como contacto y facilitador de la información
3. Jefe del departamento de TI Ing. Oscar Huerta

b) Industria Nacional de Detergente (INDESA)

1. Empresa dedicada al proceso y empaque de detergente en polvo (Maquila de detergente).
2. Ingeniera Maribel Bocardo, Jefa del departamento de Sistemas

c) Distribuidora de Juguetes ANONIMA

1. Empresa dedicada a la distribución y venta de Juguetes de diferentes tipos y marcas
2. Empresa Anónima.

3.3 Diagnóstico

Se estructura la información recolectada mediante cuestionario (Ver Anexo *4*, Anexo *5*, Anexo *6*, Anexo *9*, Anexo *10*, Anexo *11*) y las páginas oficiales de cada empresa. A partir de la información recolectada se genera la propuesta que cubra individualmente con cada una de sus necesidades (Ver Anexo *7*, Anexo *12*).

3.3.1 Empresa VYCISA

Reseña de la empresa: *"Surge en 1966 como respuesta a las demandas de un mercado de vidrio en crecimiento, consolidándose poco después como una de las empresas líderes en el ramo, adquiriendo con el paso del tiempo maquinaria necesaria para lograr una mayor eficiencia en su producción, ofreciendo así a sus clientes un tiempo de entrega justo y excelente calidad de servicio."* (Vidrios y Cristales Industrializados S.A de C.V., s.f.), como se nos indica en su página oficial "http://vycisa.com", la empresa se dedica al proceso de vidrio, cristal y espejo por más de 40 años y cuenta con la certificación de gestión de calidad ISO 9001.

Datos recolectados:

Nombre: VYCISA (Vidrios y Cristales Industrializados S.A)
Responsable del área: Ingeniero Oscar Huerta
Giro de la empresa: Manufactura de cristales y espejos con un total de 62 empleados actualmente, sus recursos informáticos constan de:

- 26 equipos de cómputo
- 4 servidores
- 1 pequeño firewall incapaz de administrar reglas, VPN y redes virtuales
- Infraestructura de cableado estructurado categoría 5

3.3.1.1 Análisis de información obtenida a través del cuestionario proporcionado por el responsable del área de TI de la empresa.

1. Actualmente no cuenta con una distribución estructurada de su red debido a la falta de un Firewall capaz de realizar estas funciones y al límite de presupuesto para el área.
2. La red actualmente no cuenta con redes virtuales por lo que cualquier usuario conectado a la red Wifi como cableada tiene caminos de acceso a todos los recursos informáticos.
3. La autentificación y control de acceso a las redes inalámbricas depende de la contraseña del modem sin tener control de quien se conecta.
4. Requiere una estructura para conexiones remotas a través de VPN la cual no ha sido implementada debido a recursos físicos y monetarios para su implementación.
5. Actualmente la forma en la que se detectan problemas en los equipos o servicios se dan cuando los equipos fallan y este problema es reportado por un usuario.
6. No se cuenta con un servidor de respaldos.

3.3.1.2 Propuesta teórica de las problemáticas a solucionar en ambiente controlado.

Analizada la información se pretende poder dar solución a los siguientes puntos sustentando la necesidad planteada por la empresa.

1. Implementar de un firewall capas de administrar reglas de red.

2. Implementar la distribución de redes virtuales para controlar el acceso a los recursos informáticos, limitando a cada área un segmento en la red.
3. Implementar un control de acceso restringido a las redes inalámbricas de la empresa brindado un control administrado a través de un portal cautivo.
4. Implementar un túnel de red privado (VPN) con la finalidad de poder acceder de forma segura a los sistemas internos. Teniendo como utilidades:
    a. Ingreso remoto por parte del Encargado de Sistemas para solucionar problemas en tiempo real
    b. Realizar presupuestos por parte de los vendedores de forma remota en tiempo real
    c. En caso de una contingencia se puede tener acceso remoto a los recursos en red y con un sistema administrado.
5. Implementar un Sistema de respaldo en red y un plan de respaldos para administrar la información sensible de la empresa.
6. Implementar un sistema de monitoreo de recursos informáticos Utilidades:
    a. Envió de notificaciones en caso de Problemas en algún recurso o servicio en los equipos.
    b. Notificación visual en caso de problema en un equipo o recurso en específico.

3.3.2 Empresa INDESA

Reseña de la empresa*: "Industria Nacional de Detergentes, S.A. de C.V. nace en el año de 2005 con la misión de satisfacer las crecientes necesidades del mercado nacional e internacional de detergentes, con productos de última generación diseñados y direccionados para las diferentes características y necesidades de*

cada mercado." (Industria Nacional de Detergentes, S.A. de C.V., s.f.), así mismo en la página oficial de la empresa (http://www.indesa.com.mx/), nos da a conocer que es una empresa orientada al desarrollo de proceso de sulfatación y fabricación de detergente en polvo con una producción promedio de 10,000 toneladas mensuales, la empresa cuenta con la certificación de gestión de calidad ISO 9001:2088.

Datos recolectados:

Nombre de la empresa: INDESA (Industria Nacional de Detergentes, S.A. DE C.V.)
Responsable del área: Ingeniera Maribel Bocardo.
Empresa dedicada a la maquila de detergente, con un total de 320 empleados, sus recursos informáticos constan de:

- 117 equipos de cómputo
- 5 servidores
- Infraestructura de cableado estructurado categoría 5

3.3.2.1 Análisis de información obtenida a través del cuestionario proporcionado por el responsable del área de TI de la empresa.

1. Actualmente no cuenta con una distribución estructurada de su red debido a la falta de planeación e infraestructura necesaria.
2. La red actualmente no cuenta con redes virtuales por lo que cualquier usuario conectado a la red Wifi como cableada tiene caminos de acceso a los recursos informáticos.
3. La autentificación y control de acceso a las redes inalámbricas depende de la contraseña del modem sin tener control de quien se conecta.

4. Actualmente la forma en la que se detectan problemas en los equipos o servicios se dan cuando los equipos fallan y este problema es reportado por un usuario.
5. No se cuenta con un servidor de respaldos, el respaldo se realiza solo a servidores de manera manual mediante un dispositivo extraíble.
6. Se analiza la propuesta de centralizar los sistemas mediante un ERP.
7. Cuenta con una conexión VPN a un área determinada de la empresa.
8. Todo cambio o soporte a los servicios de la empresa se deben realizar de forma local (Presencial por parte de las personas encargadas del área de TI).
9. La empresa opera 24x7

3.3.2.2 Propuesta teórica de las problemáticas a solucionar en ambiente controlado.

Analizada la información se pretende poder dar solución a los siguientes puntos sustentando la necesidad planteada por la empresa.

1. Implementar un firewall capaz de administrar reglas de red.
2. Implementar la distribución de redes virtuales para controlar el acceso a los recursos informáticos, limitando a cada área un segmento en la red.
3. Implementar un control de acceso restringido a las redes inalámbricas de la empresa brindado un control administrado a través de un portal cautivo.
4. Implementar un Sistema de respaldo en red y un plan de respaldos para administrar la información de los servidores de la empresa.
5. Implementar un plan para realizar los respaldos de usuario mediante un servicio en red.
6. La implementación de un servicio de VPN es opcional, con la finalidad de poder realizar atenciones de soporte remoto o disponer de archivos en tiempo real.

7. Implementar un sistema de monitoreo de recursos informáticos Utilidades:
    a. Envió de notificaciones en caso de Problemas en algún recurso o servicio en los equipos.
    b. Prevención de incidentes mediante la pronta detección de comportamientos anómalos en los equipos.

3.3.3 Empresa Distribuidora de Juguetes Anónima

Empresa dedicada a la comercialización de Juguetes con más de 50 años en el mercado.

Datos recolectados:
Nombre de la empresa: Distribuidora de Juguetes anónima.
Empresa dedicada a la distribución y venta de Juguetes de diferentes marcas a nivel nacional, su infraestructura corporativa es principalmente completa al contar con proveedores que ofrecen un nivel de seguridad y arrendamiento de equipos en caso de necesitarlos.

- Cuenta con 200 sucursales que dependen de un servicio de internet casero para la realización de transacciones con tarjetas bancarias, así como la contabilidad de ventas en tiempo real.
- Cuenta en promedio con 3 terminales de cobro en cada sucursal.
- El soporte a tiendas se encuentra centralizado en el corporativo y en ocasiones se necesita él envió de paquetes de complemento para los sistemas de ventas y un soporte remoto.

3.3.3.1 Análisis de información

Al contar con servicios de arrendamiento y proveedores tienen áreas sin cubrir debido a la falta de presupuesto como:

- No se cuenta con sistema de monitoreo de equipos por lo que cualquier problema en los sistemas se atiende hasta ser reportado por las áreas lo que representa retraso en la operación pues las áreas muchas veces lo reportan horas después.
- En el caso de las sucursales generalmente no reportan incidentes de conexión de sus equipos en tiempos adecuados, en el momento en que una tienda realiza un reporte de equipos generalmente es cuando ya ninguna de sus terminales de ventas se encuentra en operación por lo que una tienda puede pasar horas sin operar debido a este tipo de problemas.
- Al dar soporte a las tiendas el personal presenta gran dificultad y problemas al intentar realizar el envío de paquetes de gran tamaño para recuperar sistemas de ventas y tener una fuerte restricción de acceso en los equipos a los servicios de internet por seguridad de las terminales.
- La empresa eliminó las conexiones VPN de las tiendas, debido al alto costo que representaba mantenerlas.

3.3.3.2 Propuesta teórica de las problemáticas a solucionar en ambiente controlado.

Analizada la información se pretende poder dar solución a los siguientes puntos sustentando las necesidades analizadas dentro de la empresa.

1. Se propone la implementación de un monitoreo de equipos y servidores para determinar posibles fallas o anomalías dentro de corporativo.

2. Implementar un Sistema Firewall para crear un servicio de VPN aislado a la operación central de la empresa, con la finalidad de crear una intranet a la que se puedan conectar las tiendas.
3. Implementar un repositorio aislado de la operación central de la empresa con la finalidad de agilizar el envío de paquetes necesarios para la reparación de los puntos de venta.
4. Implementar un monitoreo con un mapa geográfico para identificar alertar en las terminales de venta y poder atender estas en tiempo real y así evitar el paro de operación de una tienda.

3.4 Integración de Propuestas.

Con la información recopilada de las empresas muestra podemos determinar que a pesar de ser empresas dedicadas a diferentes giros las necesidades de software y control giran sobre los mismos problemas (Falta de presupuesto, Falta de infraestructura, falta de proyectos viables, falta de conocimiento de alternativas de software), Por estas razones se integran las propuestas presentadas a las empresas y se generara una propuesta general.

Propuesta General:

1. Implementar un firewall capaz de administrar reglas de red.
2. Implementar la distribución de redes virtuales para controlar el acceso a los recursos informáticos, limitando a cada área un segmento en la red.
3. Implementar un control de acceso restringido a las redes inalámbricas de la empresa brindado un control administrado a través de un portal cautivo.

4. Implementar un túnel de red privado (VPN) con la finalidad de poder acceder de forma segura a los sistemas internos. Teniendo como utilidades:
    a. Ingreso remoto por parte del Encargado de Sistemas para solucionar problemas en tiempo real.
    b. Realizar presupuestos por parte de los vendedores de forma remota en tiempo real.
    c. En caso de una contingencia al tener acceso remoto a los recursos en red y con un sistema administrado será posible realizar home office.
    d. Tener un Monitoreo de equipos remotos.
5. Implementar un Sistema de respaldo en red y un plan de respaldos para administrar la información sensible de la empresa.
6. Implementar un modelo de respaldos automáticos para usuarios mediante la red.
7. Implementar un sistema de monitoreo de recursos informáticos tanto locales como remotos, Utilidades:
    a. Envió de notificaciones en caso de Problemas en algún recurso o servicio en los equipos.
    b. Notificación visual en caso de problema en un equipo o recurso en específico.
    c. Atención de incidentes de forma inmediata.
    d. Prevención de incidentes mediante la temprana detección usando disparadores.
    e. Muestra de un mapa que identifique visualmente alertas en recursos informáticos.

3.5 Elección de herramientas

La elección de las herramientas a utilizar para este proyecto se tomó basado en las características de las herramientas:

- La capacidad de cubrir la mayor parte del proyecto.
- La libertad de adaptación a hardware.
- Libertad de instalación y distribución.
- Costo de instalación, mantenimiento.
- Completa documentación y apoyos para la operación y mantenimiento por parte de la misma empresa.
- Posibilidad de adquisición de hardware dedicado
- Posibilidad de adquisición de soporte especifico.

3.5.1 Herramienta Firewall y Administración de Red

Analizadas las características y costos presentados en las tablas: (Tabla 1, Tabla 2 y Tabla 3), se elige como herramienta para este proyecto el software pfSense el cual brinda la capacidad de adaptación no solo en hardware sino también en las necesidades y tamaño de las organizaciones, además de contar con hardware dedicado y soporte especifico además de la amplia documentación oficial del software.

3.5.1.1 Análisis de Herramienta PFSENSE

Como se nos presenta en la página *"https://www.pfsense.org/getting-started/"* (Rubicon Communications, LLC (Netgate), s.f.), página oficial de pfSense, El software incluye las mismas características que los firewall comerciales más caros

y en algunos casos se incluyen soluciones que no se encuentran en firewall de código cerrado, pfSense es un firewall de distribución gratuita, su sistema operativo es basado en FreeBSD (Para más información sobre FreeBSD visite *"https://www.freebsd.org/"* (FreeBSD Project., s.f.)), incluye un Kernel personalizado y una serie de software gratuitos de terceros para las funciones adicionales.

- FreeBSD: *"FreeBSD es un sistema operativo utilizado para alimentar servidores modernos, escritorios y plataformas integradas. Una gran comunidad lo ha desarrollado continuamente durante más de treinta años. Sus funciones avanzadas de redes, seguridad y almacenamiento han convertido a FreeBSD en la plataforma elegida para muchos de los sitios web más activos y los dispositivos de almacenamiento y redes embebidas más penetrantes."* (FreeBSD Project., s.f.)

Para la comodidad del usuario la operación y configuración de los componentes de este firewall se realiza mediante una interfaz web por lo que para su operación no es necesario tener conocimientos sobre UNIX. El proyecto pfSense es un software que se puede adaptar a diferentes hardware según las necesidades a satisfacer, además es posible su uso mediante Live CD o en Memory Stick para su prueba sin la necesidad de instalar en el disco, así como la instalación en tarjetas de memoria flash compactas para sistemas integrados.
Existe la opción de comprar un dispositivo dedicado (Security Gateway Dispositivo) con el distribuidor Netgate (para más información sobre Netgate visite *"https://www.netgate.com/products/appliances/"* (Rubicon Communications, LLC (netgate), 2018), o como ya se mencionó crear la propia infraestructura para la implementación del software mediante una amplia guía de instalación y configuración disponible en la página: *"https://www.netgate.com/docs/pfsense/"* (Rubicon Communications LLC, s.f.), Es posible encontrar tutoriales de diferentes

escenarios para su configuración, además de la posibilidad de adquirir una póliza de soporte a través del proveedor Netgate (para más información de costo en caso de querer contratar soporte visitar *"https://www.netgate.com/support/ "* (Rubicon Communications, LLC (Netgate), 2018), para el software pfSense la seguridad es muy importante es por este motivo que en la página web "*https://www.pfsense.org/security/advisories/"* (Rubicon Communications, LLC (Netgate), s.f.), es posible encontrar las vulnerabilidades detectadas en el software para así poder prevenirlas.

En la documentación presentada por Netgate los requisitos mínimos de hardware para la instalación de PfSense son:

- CPU mínimo de 600 MHz
- RAM mínima de 512 MB
- 4 GB mínimo de espacio de almacenamiento
- Una o más tarjetas de red compatibles

3.5.1.2 Características de Licencia

Una vez más tomando como referencia lo contenido en el portal oficial de pfSense (*"https://www.pfsense.org/about-pfsense/"*, (Rubicon Communications, LLC (Netgate), s.f.)) podemos denotar que este software se encuentra bajo la licencia Apache 2.0

Licencia Apache 2.0: *"Una licencia permisiva cuyas condiciones principales requieren la preservación de derechos de autor y avisos de licencia. Los colaboradores proporcionan una concesión expresa de derechos de patente. Los trabajos con licencia, las modificaciones y los trabajos más grandes se pueden distribuir bajo diferentes términos y sin código fuente." (GitHub , Inc., s.f.),* las libertades o permisos que se nos presentan sobre este tipo de licencia son permiso de uso comercial, modificación, distribución, uso de patente y uso privado.

3.5.1.3 Funciones de pfSense

A continuación se presenta una explicación sobre las funciones descritas en el portal de pfSense (Para más detalles es posible consultar en la página: *"https://www.pfsense.org/about-pfsense/features.html"*, (Rubicon Communications, LLC (Netgate), s.f.)):

Firewall: Dentro de las características que tiene el módulo de firewall de pfSense es el filtrado por IP de origen y destino, Protocolo IP, Puerto de origen para el tráfico TCP y UDP, así como limitar conexiones simultáneas y un filtrado por Sistema Operativo, además de la posibilidad del enrutamiento de políticas flexibles con la opción de seleccionar la puerta de enlace por regla. Es posible agrupar y nombrar las direcciones IP, e incluso ejecutar el Firewall sin IP.
Es posible deshabilitar las funciones de Firewall y permitir usar el sistema solo como un enrutador.

- TCP: Como nos menciona el autor William Stallings, TCP (Protocolo de Control de Transmisión) es uno de los principales protocolos de la capa de transporte en el modelo TCP/IP.
- UDP: *"Se entiende por encapsulamiento al agregado de información de control a las unidades de datos y al tratamiento de ese bloque como un todo llamado UDP (Unidad de Datos del Protocolo)"* (Estrada, Seguridad Por Niveles, 2011)

Tabla de estado: La tabla de estado contiene información sobre las conexiones de red abiertas, esta tabla es ajustable y el tamaño predeterminado varea según la memoria RAM instalada en el sistema (cada estado necesita 1 KB de RAM aproximadamente).

Traducción de direcciones de red (NAT del inglés Network address translation): Esta función nos permite controlar el uso de múltiples IP públicas, por defecto todo el tráfico saliente a la IP WAN.

Alta disponibilidad: El sistema proporciona una alta disponibilidad mediante la combinación de CARP y pfsync, además dos o más servidores de seguridad se pueden configurar de forma sincronizada de manera que si se realizan cambios de configuración en el firewall primario estos cambios también se aplicaran en el firewall secundario.

A continuación se da una breve explicación sobre CARP Y pfsync tomando como referencia la información contenida en el portal oficial de OpenBSD (*"https://www.openbsd.org/faq/pf/carp.html"* (Open BSD PF - Redundancia de cortafuegos (CARP y pfsync), s.f.))

- CARP: Es un protocolo de Redundancia de Direcciones Comunes el cual tiene como objetivo permitir que varios host en el mismo segmento de red compartan una dirección IP, este es gratuito y seguro, este protocolo admite IPV4 e IPV6. Un ejemplo de uso de este CARP es la de crear firewalls redundantes (La dirección IP virtual asignada al grupo de redundancia se configura en os equipos cliente como puerta de enlace, así en caso que el firewall principal falle la IP se moverá a un firewall de respaldo sin detener la operación del servicio).
- pfsync: La interfaz de red pfsync se encarga de exponer algunos cambios en la tabla de estado pf (del inglés packet filter)

Multi-WAN: Permite múltiples conexiones a Internet además de un balanceo de cargas y conmutación por error.

Red privada virtual (VPN): Se ofrecen 3 opciones de conexión privada VPN, IPsec y OpenVPN

- IPsec: Según el portal de Juniper IPsec es un conjunto de protocolos para proteger las comunicaciones IP, definamos DOI (del inglés domain of interpretation , traducción Dominio de Interpretación), *"El IPsec DOI es un documento que contiene definiciones para todos los parámetros de seguridad necesarios para la negociación exitosa de un túnel VPN"* (Juniper Networks, Inc. , 2018)
- OpenVPN: *"OpenVPN Access Server es una solución de software VPN de túnel de red segura que integra capacidades de servidor OpenVPN, capacidades de administración empresarial, interfaz de usuario de OpenVPN Connect simplificada y paquetes de software de cliente OpenVPN que admiten entornos Windows, MAC, Linux, Android e iOS. OpenVPN Access Server es compatible con una amplia gama de configuraciones, incluido el acceso remoto seguro y granular a la red interna y / o recursos de redes privadas en la nube y aplicaciones con control de acceso detallado."* (OpenVPN Inc., 2018)

Servidor PPPoE: Permite implementar un servidor PPPoE y se puede usar una base de datos local para autenticar.

Informes y monitoreo: Permite el monitoreo mediante gráficos RRD manteniendo la información histórica de los siguientes puntos

- CPU
- Rendimiento
- Estados de firewall
- Paquetes por segundo para las interfaces.
- Tiempo de respuesta de la puerta de interfaz WAN (esto mediante ping)
- Colas de trafico Shaper (esta opción aplica si se habilita la configuración de tráfico)

Información en tiempo real: Es posible visualizar las gráficas en tiempo real mediante los gráficos SVG

DNS Dinámico: Incluye DNS dinámico y la opción de definir el método de actualización para proveedores específicos o de forma personalizada para proveedores no mostrados en la lista (para consultar la lista de proveedores DNS predeterminada consultar *"https://www.pfsense.org/about-pfsense/features.html"* (Rubicon Communications, LLC (Netgate), s.f.))

Portal cautivo: El portal cautivo permite a la institución la autenticación o redirección de clic para acceder a la red, algunas funciones son las de limitar el número máximo de conexiones simultaneas, la desconexión por tiempo de inactividad o por un límite de tiempo definido.

Filtrado MAC: Es posible el control de acceso mediante un filtrado por dirección MAC.

Servidor y retransmisión DHCP: Incluye servidor DHCP y una función de retransmitir.

3.5.2 Herramienta de Monitoreo

La herramienta de monitoreo fue elegida por la flexibilidad y requisitos de instalación así como el costo que representa su uso, instalación y mantenimiento, estas características se ven reflejadas en las tablas comparativas: *Tabla 4*, *Tabla 5* y *Tabla 6*. El software elegido para el monitoreo es Zabbix.

3.5.2.1 Análisis de Herramienta Zabbix

Tomando como referencia la página de documentación de Zabbix (*"https://www.zabbix.com/documentation/3.2/manual/introduction/about"* (Zabbix SIA., s.f.)), en la cual nos explica que Zabbix es una solución que monitorea distintos parámetros de una red así como la salud e integridad de los servidores, las notificaciones a usuarios es de forma flexible como ejemplo poder crear alertas mediante correo electrónico para casi cualquier evento definido, además para la

comodidad de los usuarios todos los informes, estadísticas y configuraciones se accede mediante una interfaz web, siendo Zabbix una solución de monitoreo de recursos de TI. Funcional tanto para pequeñas como grandes corporaciones.

Es de suma importancia mencionar que la documentación sobre el software es gratuita y se encuentra en la página oficial de Zabbix (https://www.zabbix.com/documentation/3.0/pt/manual/installation/requirements), se nos presentan algunos de los requerimientos previos.

Para una instalación los requisitos mínimos para memoria RAM es de 128 MB y 256 MB disponibles en disco, hay que tener claro que para almacenar mayores registros y un incremento significativo en los equipos a monitorear se recomienda ampliar tanto el espacio como la memoria de igual forma el procesador se recomienda definirlo con base al número total de servicios a monitorear por ejemplo para un entorno medio de 500 host se recomienda 2 CPU y 2GB de memoria RAM. Zabbix ha sido probado en las plataformas Linux, IBM AIX, FreeBSD, NetBSD, OpenBSD, HP-UX, Mac OS X, Solaris, en los siguientes sistemas solo se instala el Agente de monitoreo Zabbix Windows: 2000, Server 2003, XP, Vista, Server 2008, 7, 8, Server 2012.

- OpenBSD:*" El proyecto OpenBSD produce un sistema operativo GRATUITO y multiplataforma" (OpenBSD, s.f.)*

Como ya se mencionó la Documentación necesaria para la instalación y configuración se puede encontrar en la página oficial de Zabbix (https://www.zabbix.com/documentation/3.0/pt/manual/installation/requirements), por este motivo la herramienta es una excelente opción para usuarios con pocos conocimientos en el tema.

3.5.2.2 Características de Licencia

Zabbix es un software gratuito el cual se distribuye bajo la licencia General GPL version2, *"Significa que su código fuente se distribuye libremente y está disponible para el público en general."* (Zabbix SIA., s.f.).

3.5.2.3 Funciones y características de Zabbix

En la página oficial de documentación Zabbix (*"https://www.zabbix.com/documentation/3.2/manual/introduction/about"* (Zabbix SIA., s.f.)), se nos presentan funciones del software, a continuación se describen algunas.

Recopilación de datos: Permite la disponibilidad y comprobación de rendimiento, soporte para SNMP (captura y sondeo), IPMI, JMX así como el monitoreo de VMware

Definiciones de umbral flexibles: Es posible ajustar los umbrales para activar las alertas.

Alerta altamente configurable: Se pueden personalizar las alertas a modo de escalado, destinatarios o medio de notificación.

Gráficos en tiempo real: La visualización de graficas en tiempo real ayuda a una pronta detección de anomalías.

Amplias opciones de visualización: Permite visualizar y crear gráficas personalizadas, mapas de red entre otras funciones.

Almacenamiento de datos históricos: Permite controlar la configuración de datos históricos los cuales se almacenan en base de datos.

Sistema de permisos: Además de contar con una autentificación segura para usuarios es posible limitar ciertas vistas a ciertos usuarios.

3.5.3 Herramienta de Almacenamiento

Las características presentes en la Tabla 7 son las más relevantes ya que en términos generales las herramientas son útiles y capaces de cumplir las necesidades de almacenamiento en las organizaciones, la herramienta idónea a elegir en este proyecto es FreeNAS por sus características de adaptación de software así como su posibilidad de adquirir hardware dedicado y certificado el cual podría brindar una mayor confianza en las organizaciones que adquieren la solución.

3.5.3.1 Análisis de Herramienta FreeNAS

Según la página oficial de documentación de FreeNAS 11.1-U6 (http://doc.freenas.org/11/intro.html (iXsystems, s.f.)), FreeNAS es un sistema de almacenamiento embebido de código abierto el cual se conecta a la red, en pocas palabras una NAS basado en FreeBSD, el sistema proporciona una interfaz web de forma gráfica, además es posible instalar software adicionales como complementos. Para su instalación es necesario un procesador de 64 bits (Para la última versión de FreeNAS 11.1-U6), la memoria RAM mínima sugerida en el portal es de 8 GB además de la recomendación de incrementar la memoria RAM para tener una mayor velocidad en promedio de forma exagerada se recomienda 1 GB de memoria RAM por Terabyte de información o el aumento de 2 GB de memoria RAM para el uso con demasiados usuarios de Active Directory.

Es importante resaltar que esta herramienta no provee un soporte por parte de un proveedor sino que ayuda en la autoayuda de quienes ocupan el software, además de su amplia documentación accesible es posible estudiar cursos oficiales de forma gratuita, con la finalidad de crear Administradores capacitados, es posible ver los cursos en el siguiente enlace *"https://www.ixsystems.com/ix-university/"* (iXsystems, Inc., s.f.)

3.5.3.2 Licencia y recomendaciones de instalación

Para la instalación de FreeNAS, se nos recomienda en el portal de documentación la instalación en un disco separado de los discos de almacenamiento por ejemplo: disco SSD, memoria USB o un disco en módulo ya que la unidad en que se instale no estará disponible para el almacenamiento de datos, siendo el tamaño mínimo de 16 GB, aunque es recomendable por lo menos 32 Gb para tener una mayor flexibilidad en caso de actualizaciones, además es posible crear un dispositivo de arranque duplicado mediante la inserción de dos dispositivos idénticos y su selección durante la instalación. La licencia del sistema FreeNAS se publica bajo la licencia BSD-2-Clause.

Licencia BSD-2-Clause también conocida como Licencia BSD simplificada según el proyecto Open Source en el portal ("https://opensource.org/licenses/BSD-2-Clause" (Open source, s.f.)), esta licencia permite la redistribución y el uso de código fuente y binario, con o sin modificación, siempre que se cumpla una serie de condiciones las cuales se presentan a continuación

- *"Las redistribuciones del código fuente deben conservar el aviso de copyright anterior, esta lista de condiciones y el siguiente descargo de responsabilidad." (Open source, s.f.)*
- *"Las redistribuciones en formato binario deben reproducir el aviso de copyright anterior, esta lista de condiciones y la siguiente exención de responsabilidad en la documentación y / u otros materiales proporcionados con la distribución." (Open source, s.f.)*

Además de una cláusula la cual se presenta a continuación:

"ESTE SOFTWARE ES PROPORCIONADO POR LOS TITULARES DE LOS DERECHOS DE AUTOR Y SUS COLABORADORES "TAL CUAL" Y SE RENUNCIA A CUALQUIER GARANTÍA EXPRESA O IMPLÍCITA, INCLUIDAS,

ENTRE OTRAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN PROPÓSITO DETERMINADO. EN NINGÚN CASO EL TITULAR DE LOS DERECHOS DE AUTOR O SUS COLABORADORES SERÁN RESPONSABLES DE NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR O CONSECUENCIAL (INCLUIDOS, ENTRE OTROS, LA ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUTOS, LA PÉRDIDA DE USO, LOS DATOS O LAS GANANCIAS; O INTERRUPCIÓN DEL NEGOCIO) SIN EMBARGO Y EN CUALQUIER TEORÍA DE RESPONSABILIDAD, YA SEA EN CONTRATO, RESPONSABILIDAD ESTRICTA O AGRAVIO (INCLUYENDO NEGLIGENCIA O DE OTRO MODO) QUE SURJA DE CUALQUIER FORMA DEL USO DE ESTE SOFTWARE, AUN CUANDO SE HAYA ADVERTIDO DE LA POSIBILIDAD DE DICHO DAÑO." (Open source, s.f.)

3.5.3.3 Características Generales

En el portal de características *("http://www.freenas.org/about/features/"* (iXsystems, Inc., s.f.)), portal oficial de FreeNAS se nos presentan algunas características sobre la utilidad del sistema

Compartir archivos: Esta es una de las características principales de FreeNAS, existe compatibilidad con archivos Windows, Unix, Apple, entre otros.

Interfaz web: Esta es una utilidad que favorece no solo al usuario sino al administrador ya que el sistema permite administrar todos los aspectos mediante una interfaz web además de un asistente de configuración que permite simplificar aún más una instalación o en las futuras configuraciones con la posibilidad de acceder a la configuración avanzada y personalizar las configuraciones para adaptarse a las necesidades de la organización.

Protección de Datos: *"ZFS está diseñado para la integridad de datos de arriba a abajo. RAID-Z, el RAID de software que es parte de ZFS, ofrece protección de*

paridad única como RAID 5, pero sin la vulnerabilidad de "escritura de agujeros" gracias a la arquitectura de copiado en escritura de ZFS. Los niveles adicionales RAID-Z2 y RAID-Z3 ofrecen protección de paridad doble y triple, respectivamente. Una opción de espejo de software también está disponible. La pantalla Volúmenes de FreeNAS enumera cada disposición de paridad posible según la cantidad de discos que seleccione al crear un nuevo volumen." (iXsystems, Inc., s.f.)

- ZFS:*" Es un sistema de archivos de código abierto listo para la empresa y un administrador de volúmenes con una flexibilidad sin precedentes y un compromiso inflexible con la integridad de los datos."* (iXsystems, Inc., s.f.)
- RAID-Z*: "En RAID-Z, ZFS utiliza repartos de discos en bandas de RAID de ancho variable, de manera que todas las escrituras son de reparto total de discos en bandas. Este diseño sólo es posible porque ZFS"* (Oracle Corporation y / o sus afiliados, s.f.)

Instantáneas: Es posible realizar capturas de todo el sistema de archivos para después poder acceder a ellas, de forma programadas o esporádica todo esto desde el portal web de administración del sistema.

Replicación: Gracias a la posibilidad de crear instantáneas es posible realizar réplicas de estas a un espacio de almacenamiento remoto

Cifrado: El sistema FreeNAS permite un cifrado en volúmenes ZFS, por lo que es posible el encriptado de volúmenes completos durante la creación del volumen, estos volúmenes solo podrán ser leídos en sistemas FreeNAS que posean la clave maestra para ese volumen y el usuario podrá crear una contraseña para agregar protección adicional.

3.6 Distribución de Propuesta Integrada

Se realiza la separación de la propuesta contenida en el tema 3.4 Integración de Propuestas., con base a las características o grupo a que pertenece cada una de las necesidades siendo nuestras categorías:

- **Firewall y Administración de Redes**
- **Monitoreo de Recursos y Alertas**
- **Sistema de Almacenamiento en Red**

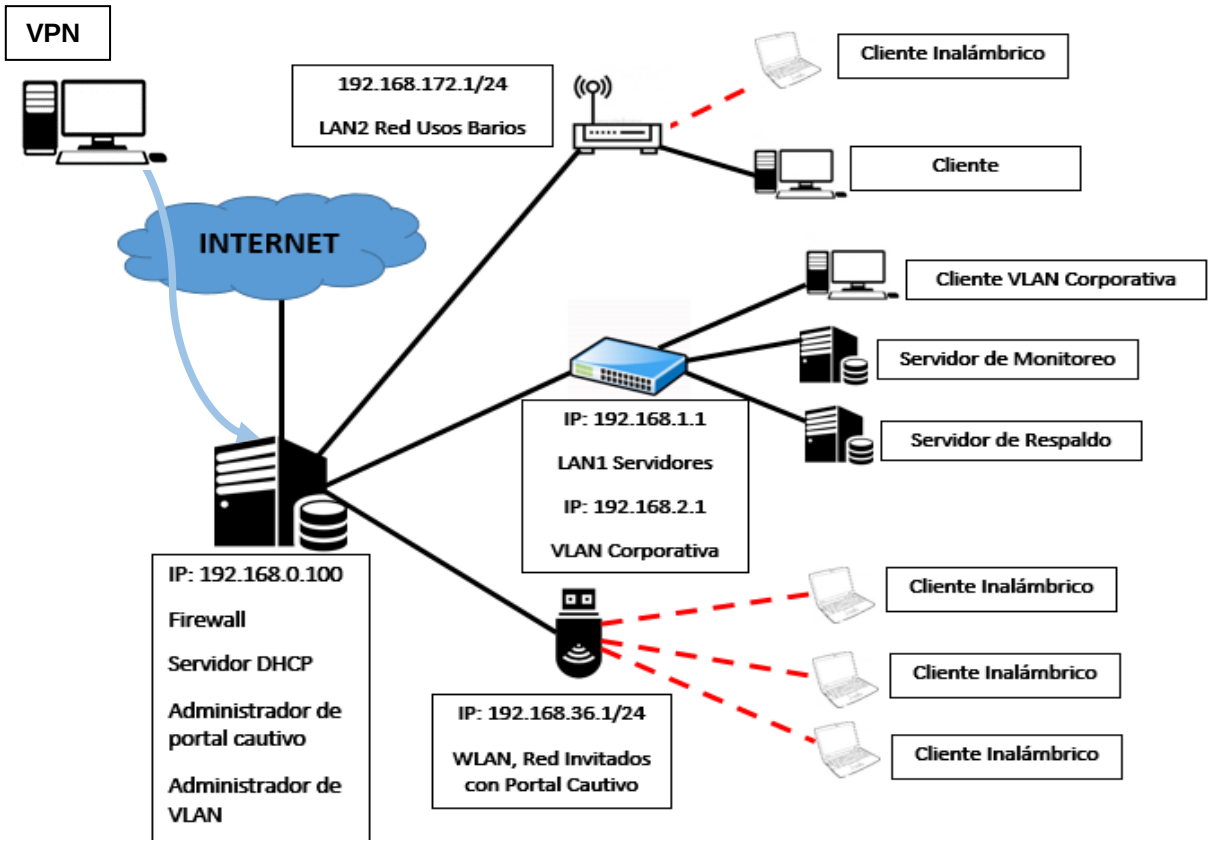

Ilustración 18: Conexión Deseada para Propuesta Integrada.

3.6.1 Firewall y Administración de Redes

El software a utilizar para poder cubrir las necesidades planteadas es pfSense.

- Se implementa un firewall capaz de administrar reglas de red.
- Se implementa la distribución de redes virtuales para controlar el acceso a los recursos informáticos, limitando a cada área un segmento en la red.
- Se implementa un control de acceso restringido a las redes inalámbricas de la empresa brindado un control administrado a través de un portal cautivo.
- Se implementa un túnel de red privado (VPN) con la finalidad de poder acceder de forma segura a los sistemas internos desde el exterior.

3.6.2 Monitoreo de Recursos y Alertas

Se implementa un sistema de monitoreo de recursos informáticos tanto locales como remotos con las siguientes características:

- Envió de notificaciones en caso de Problemas en algún recurso o servicio en los equipos.
- Notificación visual en caso de problema en un equipo o recurso en específico. Prevención de incidentes mediante la temprana detección usando disparadores.
- Muestra de un mapa que identifique visualmente alertas en recursos informáticos.

3.6.3 Sistema de Almacenamiento en Red

- Se implementa un Sistema de respaldo en red y un plan de respaldos para administrar la información sensible de la empresa.
- Se implementa un modelo de respaldos automáticos para usuarios mediante la red.

3.7 Preparación, Instalación, configuración de Firewall y distribución de Red usando pfSense

Se presentan las características del hardware usado para la instalación del software pfSense y las herramientas utilizadas en la instalación y configuración para cubrir el diagrama de la Ilustración 18.

3.7.1 Herramientas Hardware y Software

Características del pc donde se instalara pfSense

- PC sin marca
- Placa base GA-G31M-ES2C
- Procesador: Intel Pentium Inside x64, 2 CPU
- RAM: 1 GB
- Disco duro: 37 GB

Tarjetas de red usadas

- Tarjeta de Red Integrada conexión LAN 10/100 de alta velocidad (GIGA-BYTE Technology Co., Ltd., s.f.)
- Tarjeta de Red Inalámbrica USB Linksys 2.4 GHz, 802.11g
- Tarjeta de Red TP-LINK 10/100
- Tarjeta de Red TP-LINK 10/100

Herramientas Necesarias

- USB 8GB
- ISO pfSense se puede descargar desde: *"https://www.pfsense.org/download/"* (Rubicon Communications, LLC (Netgate), s.f.), se recomienda descargar la versión USB Memstick Installer para la creación sistemas de arranque mediante USB.
- Herramienta para crear USB de instalación con el programa Win32 Disk Imager, es posible descargarlo desde *"https://sourceforge.net/projects/win32diskimager/"* (Slashdot Media, s.f.).

Herramientas usadas para la creación de red.

- Ethernet Hub 8 puertos
- Router Alfa Network R36 en modo puente
- 7 cables Ethernet

3.7.2 Proceso de Instalación

3.7.2.1 Creación de USB de arranque pfSense

Utilizando el programa Win32 Disk Imager-1.0 se cargara la ISO de pfSense en el USB, la imagen ISO de pfSense deberá estar previamente descargada.

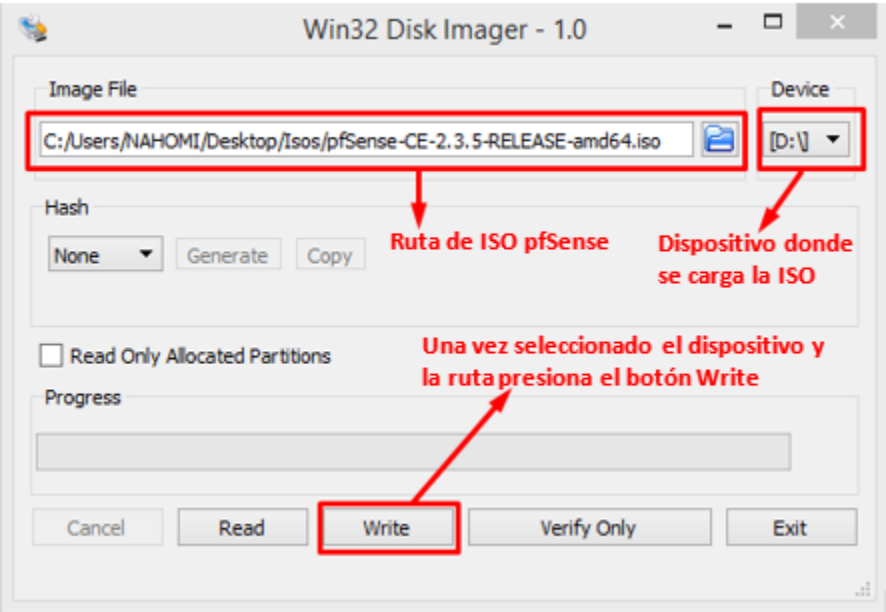

Ilustración 19: Creación de USB de Arranque con Win32 Disk Imager-1.0.

3.7.2.2 Instalación de pfSense

1.- Se arranca el equipo desde el dispositivo USB, al cargar comenzara la instalación guiada del sistema debemos aceptar el aviso de copyright y distribución.

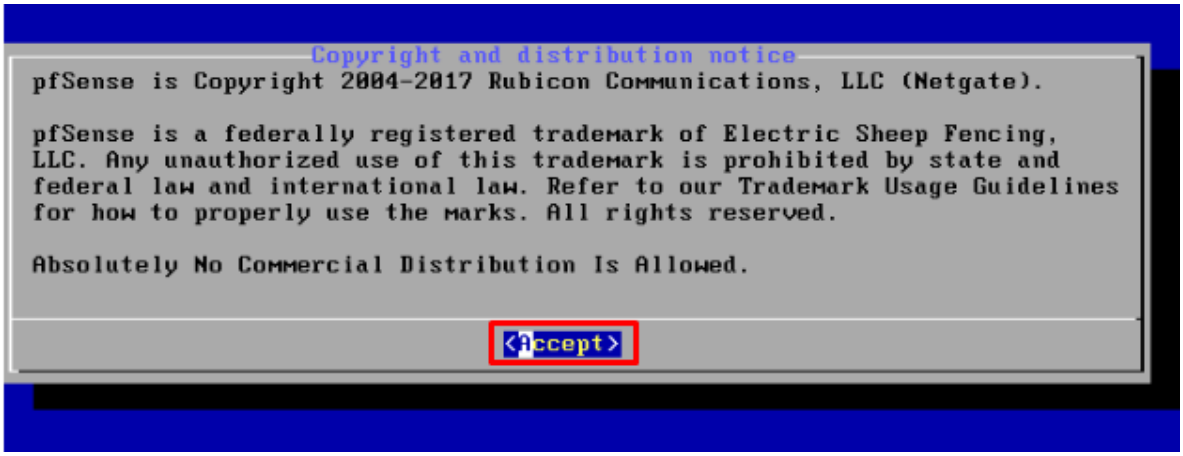

Ilustración 20: Aviso de Copyright y Distribución pfSense.

2.- Seleccionamos la instalación de pfSense y seleccionamos la opción OK para comenzar a instalar.

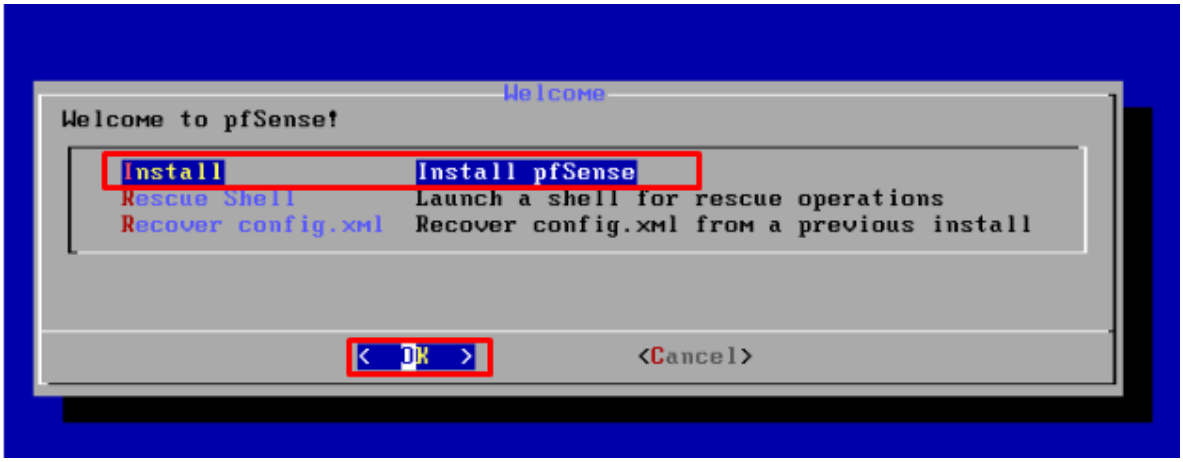

Ilustración 21: Inicio de Instalación Guiada pfSense.

3.-Eleccion de distribución de teclado, seleccionamos Select para continuar dejando los valores de modo predeterminado, al hacer esto la distribución predeterminada es Estándar de Estados Unidos.

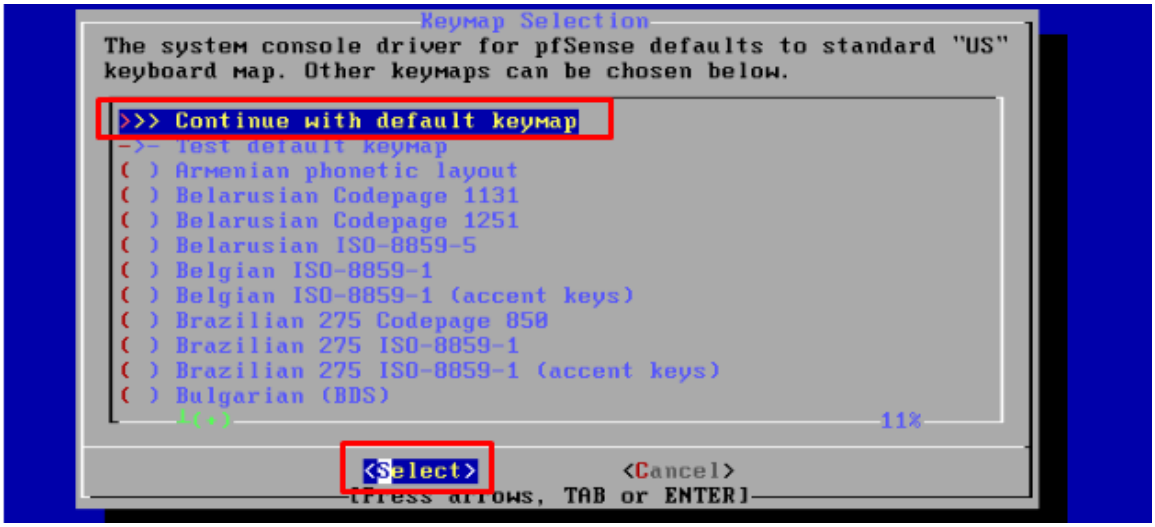

Ilustración 22: Elección de Distribución de Teclado.

4.- Dejamos la opción por defecto y seleccionamos la opción OK, esto configura automáticamente las particiones para la instalación.

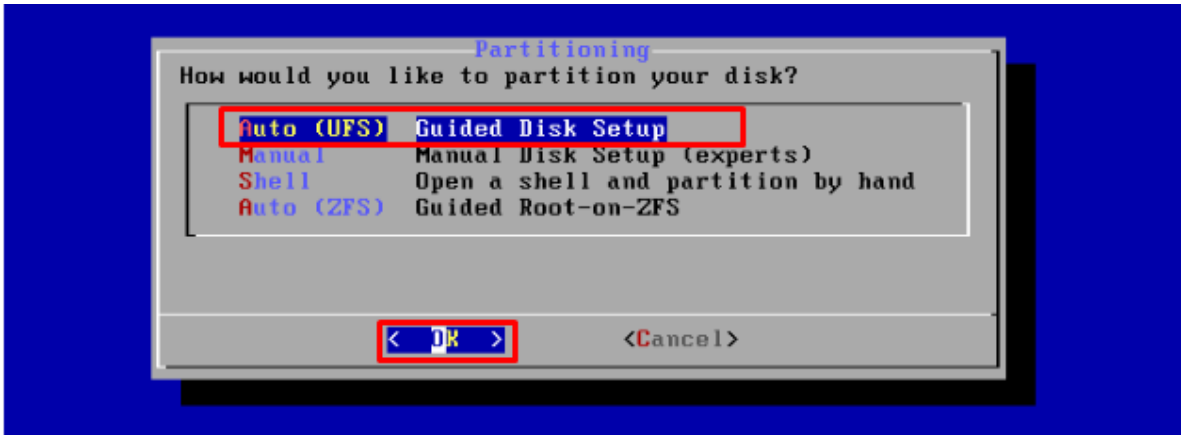

Ilustración 23: Selección de Modo de Particionar Unidad de Disco.

5.-La instalación guiada comenzara a escribir en las particiones creadas.

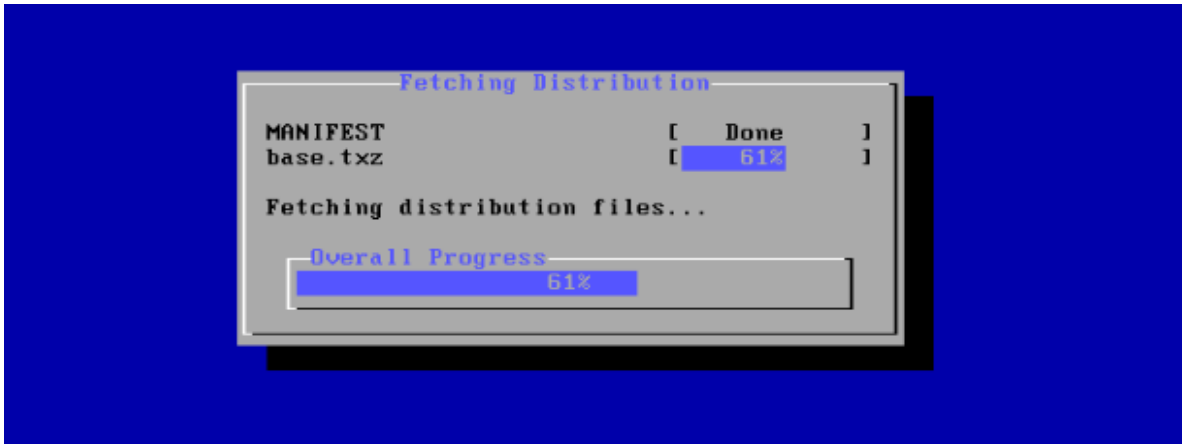

Ilustración 24: Procesó de Grabado en Disco.

6.- En este paso omitiremos la configuración, más adelante se configurara.

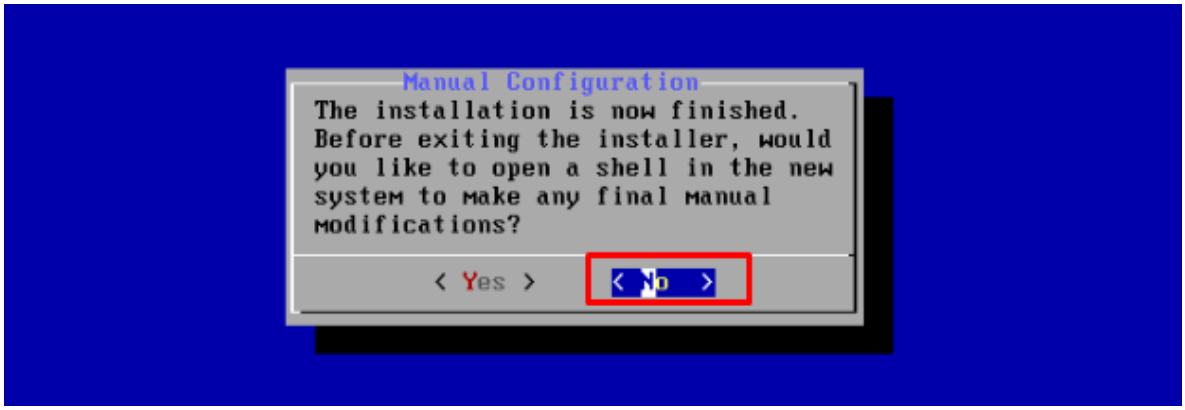

Ilustración 25: Elección de Configuración Manual pfSense.

7.- Reiniciamos el sistema y desconectamos el dispositivo USB para que el sistema arranque desde la partición donde se instaló el sistema.

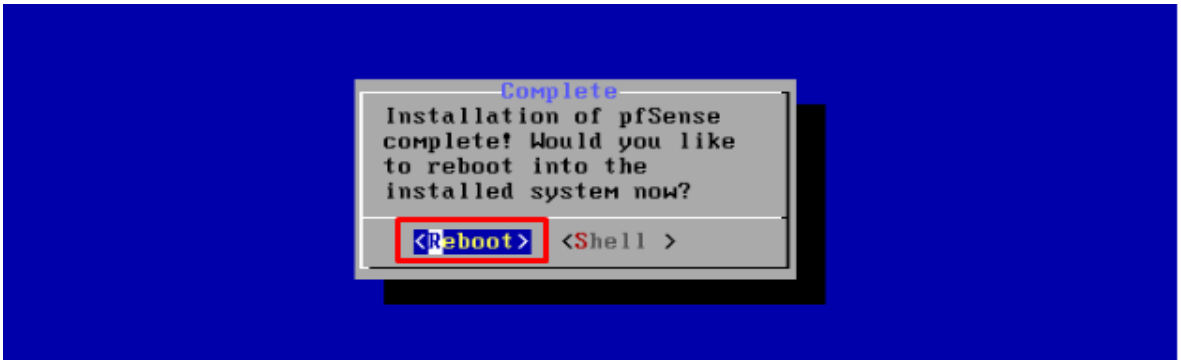

Ilustración 26: Reinicio de Sistema.

8.-Una vez iniciado el sistema se definen las tarjetas de red en el servidor pfSense, para nuestro caso son:

alc0 tarjeta WAN su configuración por defecto es DHCP, para esto se escribe el nombre de la tarjeta que deseemos usar como WAN (La interfaz WAN se refiere a la interfaz de conexión usada como salida al exterior).

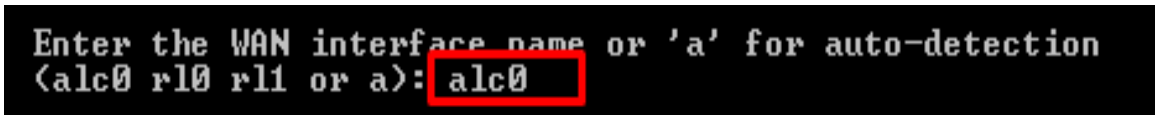

Ilustración 27: Elección de Tarjeta para Conexión WAN.

rl0 tarjeta LAN, se escribe el nombre de la tarjeta que deseamos usar como LAN

Ilustración 28: Elección de Tarjeta para Red LAN.

rl1 Tarjeta OPT 1, al igual que en las anteriores opciones se teclea esta tarjeta o en su defecto es posible seleccionar "a", para que el sistema la asigne automáticamente, si existen más tarjetas se agregaran de la misma forma que la tarjeta rl1.

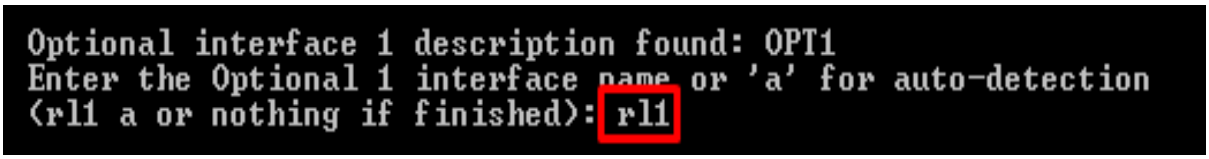

Ilustración 29: Elección de Tarjeta para Red OPT1.

Quedando la distribución de tarjetas como se muestra en la Ilustración 30

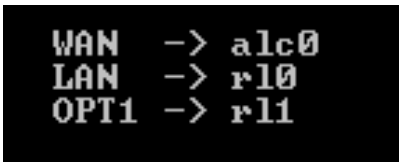

Ilustración 30: Relación de Tarjeta y Red.

3.7.3 Configuración de pfSense

Terminado el proceso de instalación se conectará un pc por medio de cable rj45 al puerto LAN del Servidor pfSense y mediante el navegador se ingresa a la página de configuración en la dirección por defecto: 192.168.1.1

3.7.3.1 Inicio

1.- Para ingresar al panel de configuración grafico de PfSense usaremos las credenciales por defecto:

- Usuario: admin
- Contraseña: pfsense.

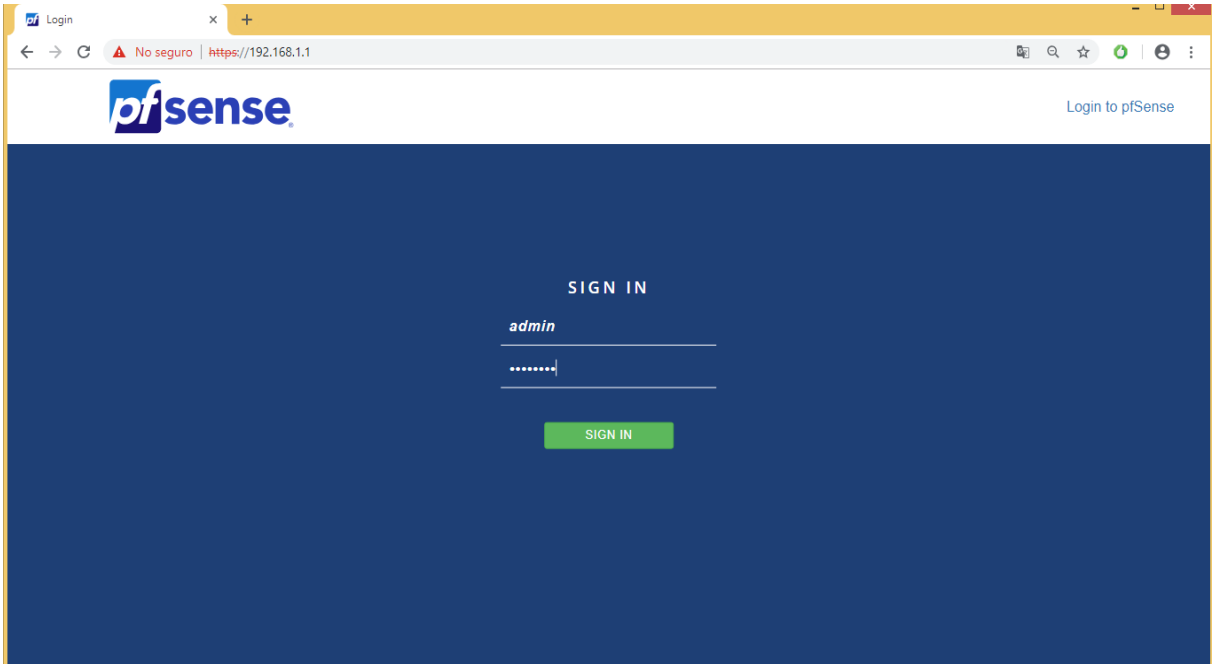

Ilustración 31: Inicio de Sesión pfSense, Interfaz Gráfica.

2.- La primera vez que ingresemos al portal se presenta una página de bienvenida, damos clic sobre la opción Next para continuar al tablero principal de PfSense.

Nota: Al iniciar sesión por primera vez aparecerá un mensaje de advertencia el cual sugiere el cambio de credenciales por defecto.

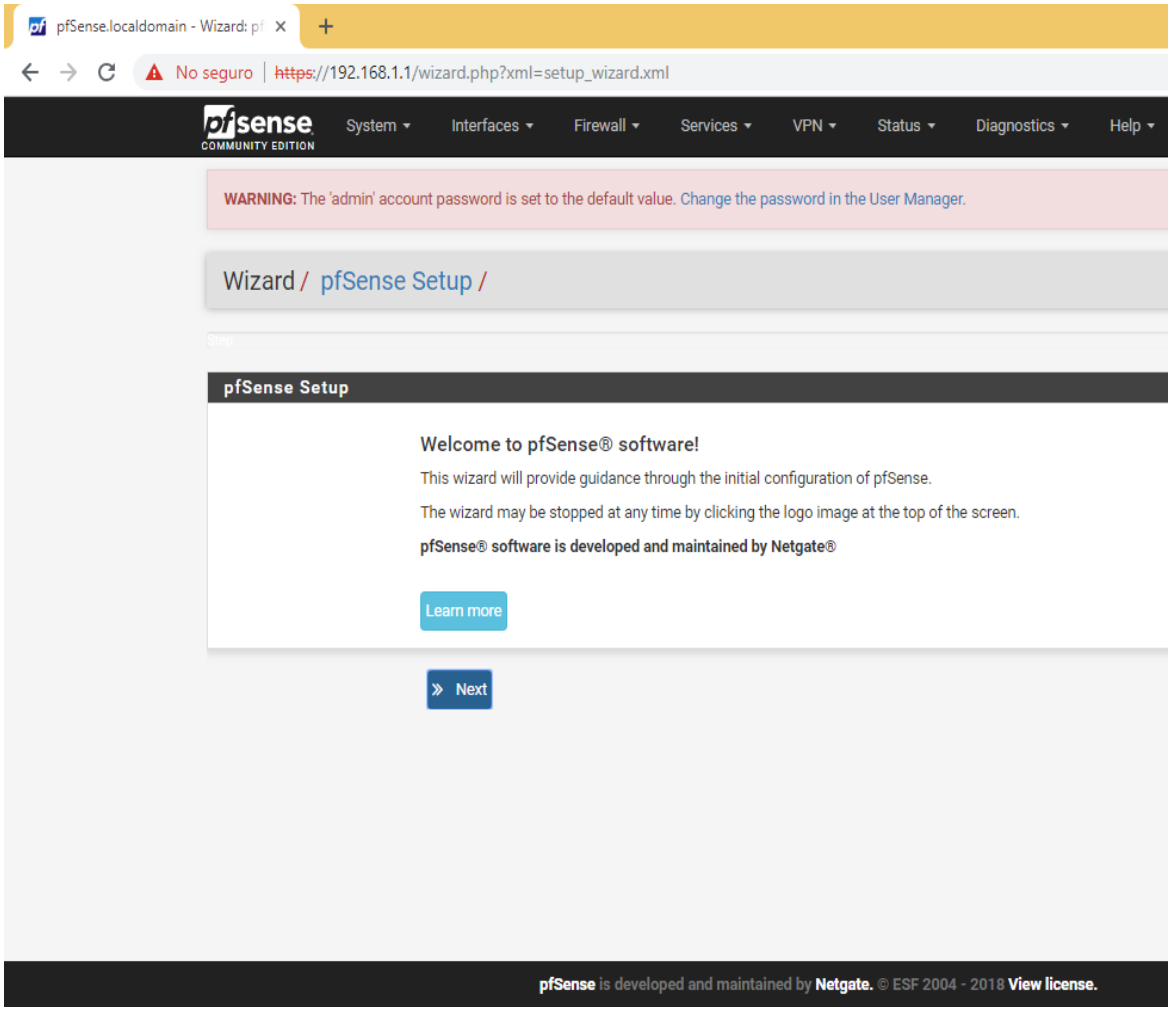

Ilustración 32: Página de Bienvenida pfSense, Interfaz Gráfica.

3.-Dando clic sobre el ícono pfSense nos dirigirá al Panel de información del sistema.

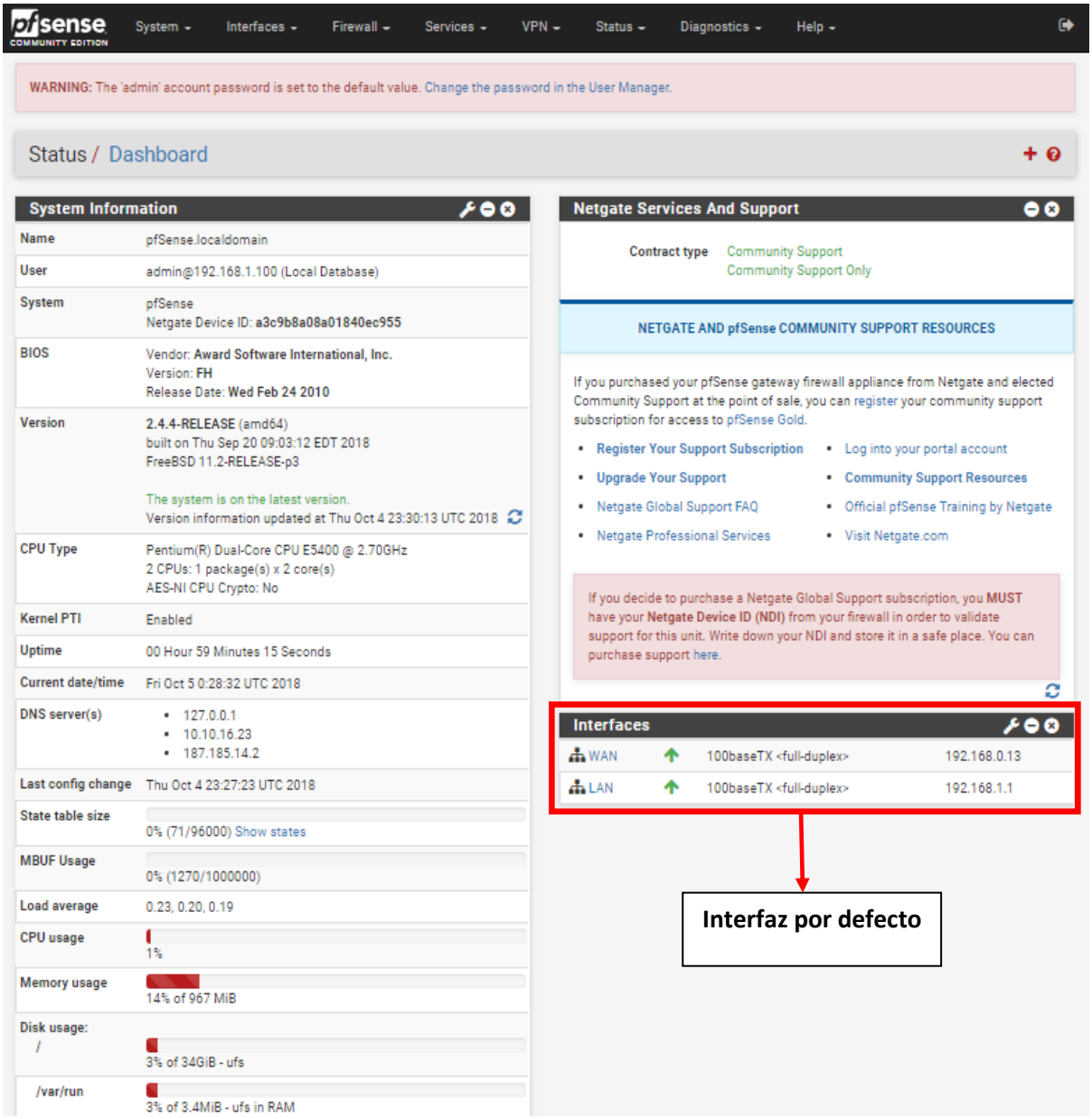

Ilustración 33: Panel de Estado pfSense.

3.7.3.2 Configuración de Interfaces

El Servidor PfSense ajusta por defecto 2 Interfaz de Red, la Interfaz WAN y LAN. La Interfaz WAN permite por defecto el tráfico de datos a la conexión de internet a la que se encuentre conectada, la configuración de la interfaz WAN se encuentra en modo DHCP.

1.- Configuración de la red WAN, la cual por defecto se encuentra en modo DHCP, seleccionamos la Interfaz WAN.

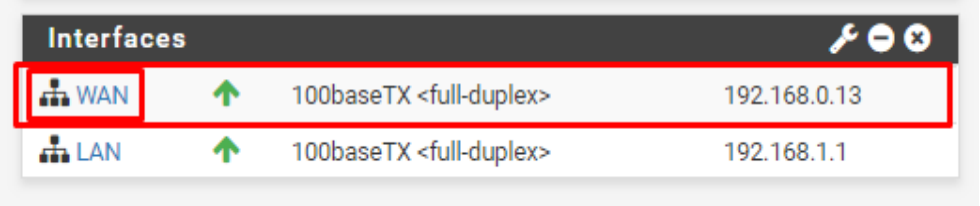

Ilustración 34: Interfaz WAN en el Panel de Estado pfSense.

2.- Modificamos el tipo de configuración de red IPv4 DHCP a estático y se asignará la dirección IP y Puerta de enlace proporcionada por el proveedor. Para nuestro caso virtual los valores serán:

- IP es: 192.168.0.100
- Puerta de acceso a Internet: 192.168.0.1

Una vez realizados los cambios seleccionamos la opción salvar para guardar los cambios.

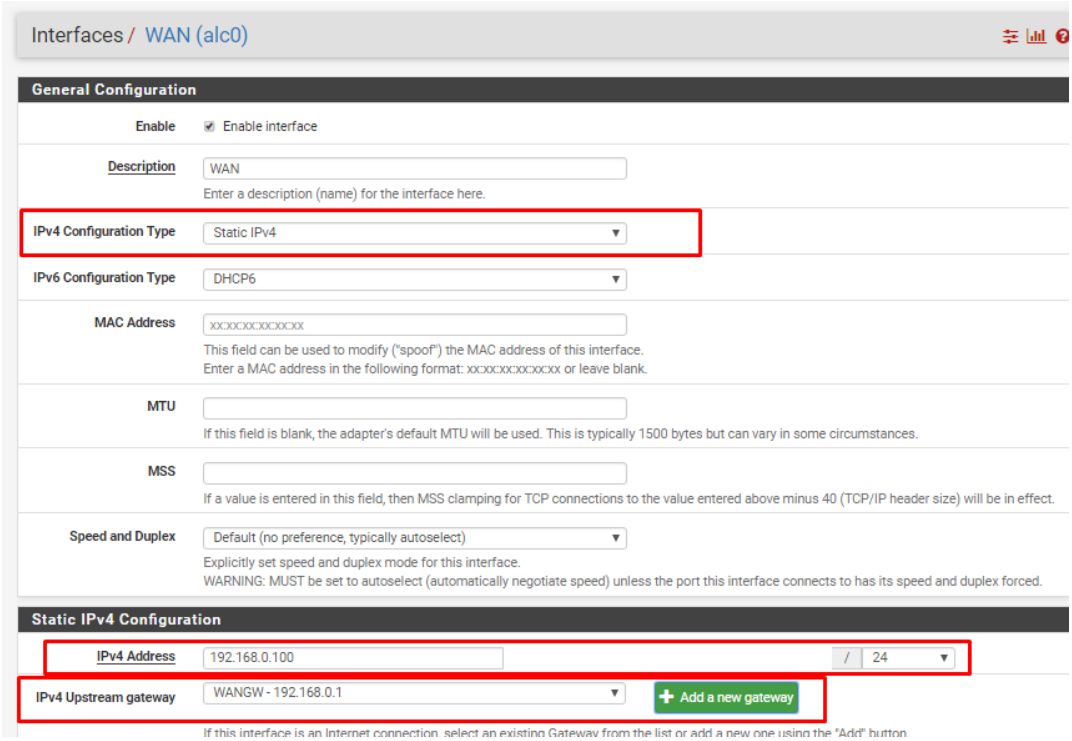

Ilustración 35: Panel de Configuración Interfaz WAN (alc0).

3.- Aplicamos los cambios realizados en la Red WAN.

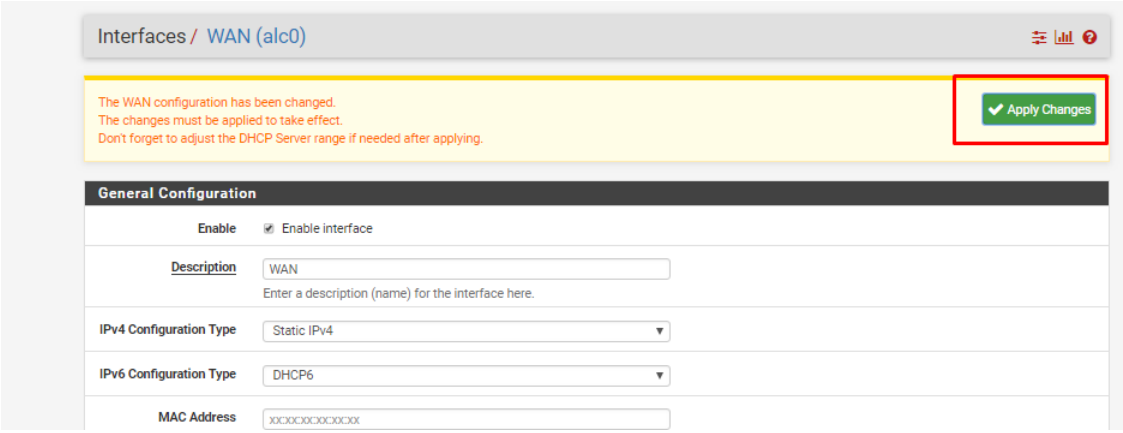

Ilustración 36: Confirmación de Cambios a Interfaz WAN

4.- Por defecto la Red LAN se configura con la IP 192.168.1.1 y como puerta de enlace el Firewall seleccionamos la red LAN para validar la información.

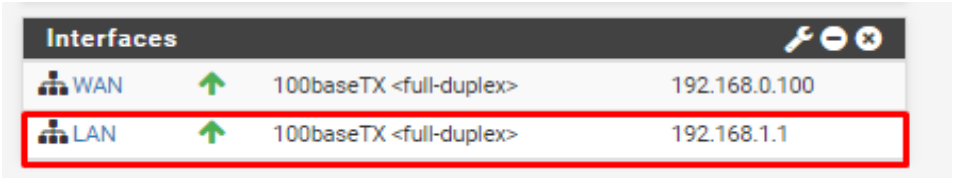

Ilustración 37: Interfaz LAN en el Panel de Estado pfSense.

5.- Si se desea cambiar la dirección IP de LAN es posible realizarlo en el panel de configuración general, en nuestro caso esta permanecerá con la dirección IP 192.168.1.1 de manera estática y como puerta de enlace None lo cual permitirá a la red tomar como puerta predeterminada al Firewall.

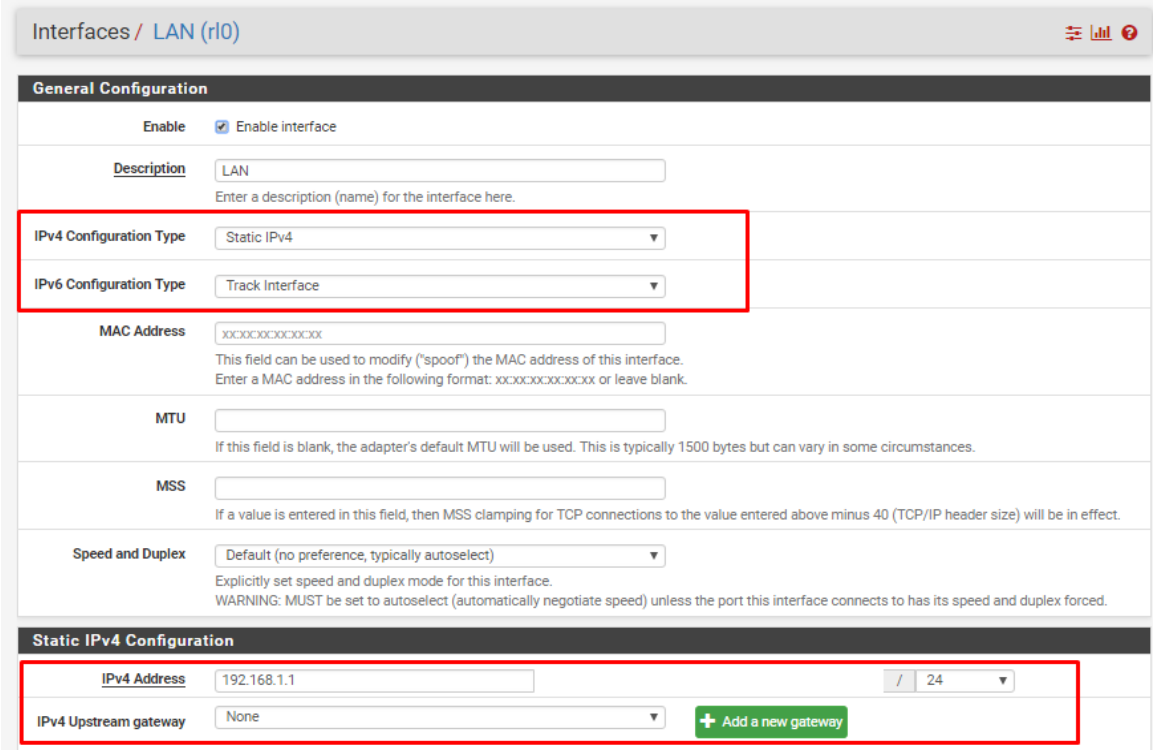

Ilustración 38: Panel de Configuración Interfaz LAN (rl0).

6.- Configuración de Red OPT1, es necesario habilitar esta red, en caso de contar con más tarjetas de red se habilitarán de la misma manera. Haciendo clic sobre la ruta: Interfaces -> Assignments.

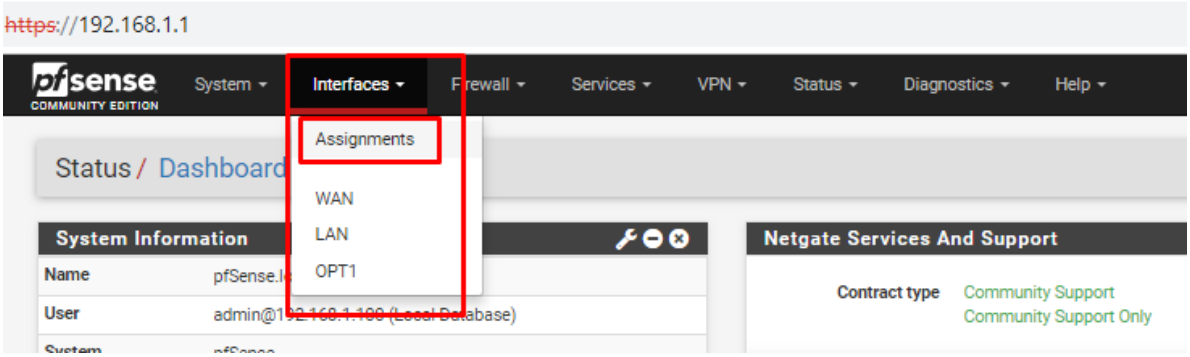

Ilustración 39: Ruta para Asignación de Interfaces.

7.- En la función OPT1 seleccionaremos la Tarjeta que deseamos usar y guardamos el cambio.

Hacemos clic en la Interface OPT1.

Ilustración 40: Asignación de Tarjeta a Interfaz.

8.- Para el caso de las redes OPT es necesario habilitar la Interfaz, definir el tipo de configuración de la dirección IP además es posible modificar el nombre, una vez realizados los cambios salvamos.

Para nuestro caso la Interfaz OPT1 tomará los parámetros:

- Nombre: LAN2
- Dirección IP estática: 192.168.173.1
- Puerta de enlace none, de este modo tomara como puerta de enlace predeterminada al Firewall, en caso de existir otra puerta de enlace es posible agregarla.

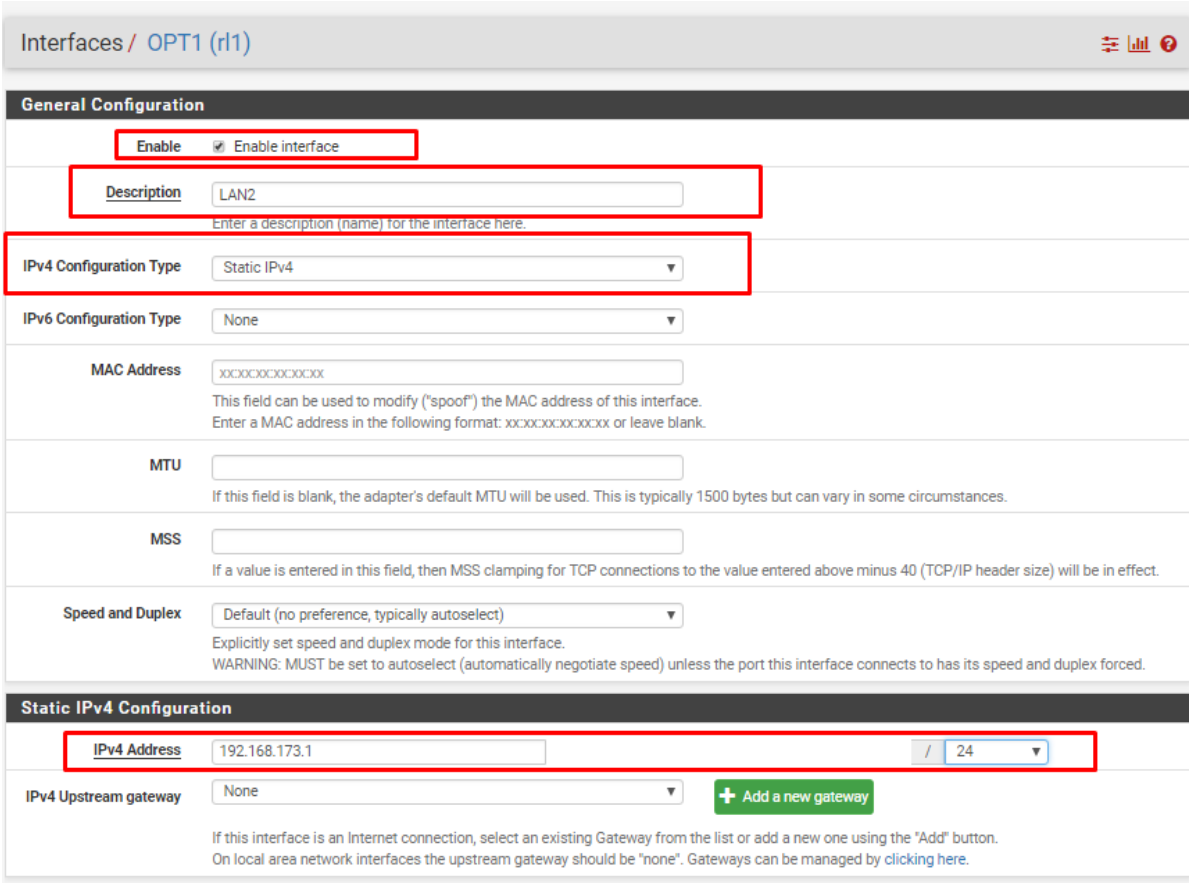

Ilustración 41: Panel de Configuración Interfaz OPT1 (rl1).

9.- Aplicamos los cambios realizados

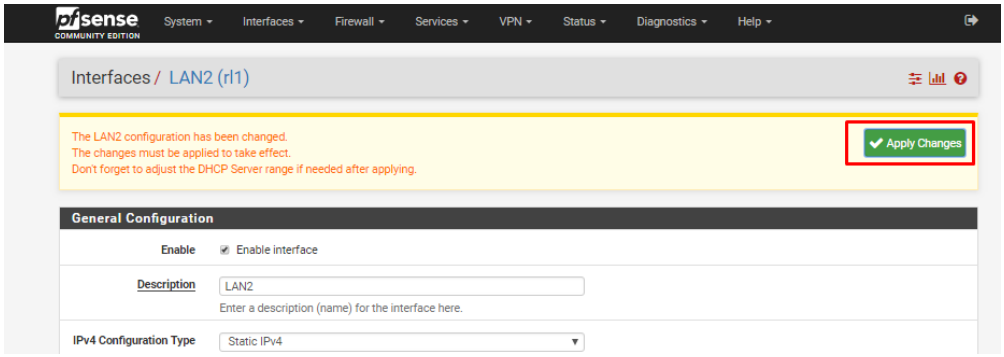

Ilustración 42: Confirmación de Cambios a Interfaz LAN2 (OPT1).

Configuración de Interfaz Wireless

10.- A diferencia de las tarjetas de red alámbricas la tarjeta de red inalámbrica se conectó mediante USB por lo que no ha sido agregada durante la instalación, es por ese motivo que nos dirigimos a la asignación de interfaces y seleccionar el apartado Wireless para agregar la tarjeta como una nueva Interfaz inalámbrica.

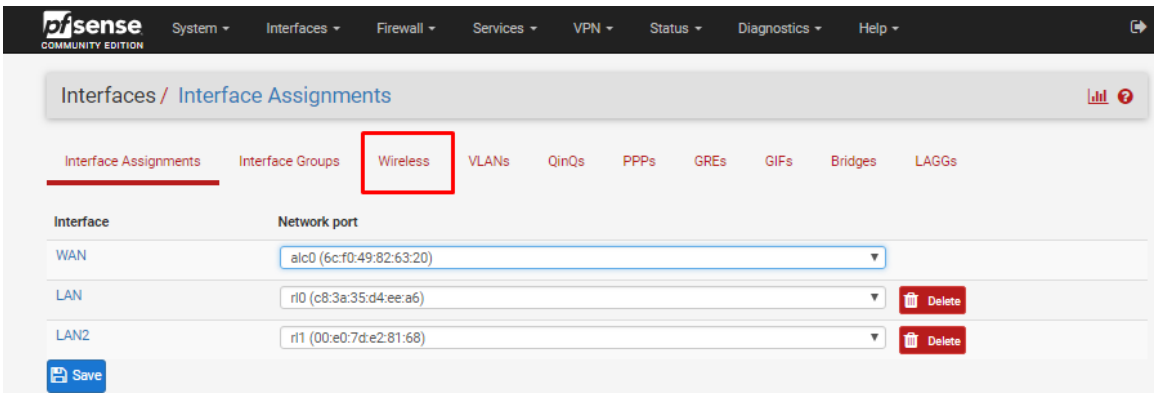

Ilustración 43: Ruta para la Asignación de Nueva Tarjeta Wireless.

11.- En el apartado Wireless seleccionamos el botón Add para agregar la tarjeta como una nueva Interfaz

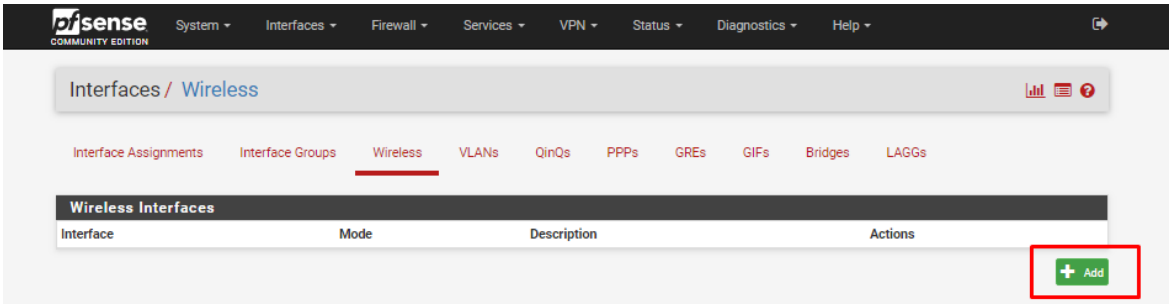

Ilustración 44: Agregar Tarjeta.

12.- En Parent Interface seleccionamos la tarjeta inalámbrica a usar, en modo lo definiremos como punto de acceso y en la descripción daremos un nombre a esta interfaz, una vez realizados los cambios guardamos.

Ilustración 45: Creación de Tarjeta Inalámbrica.

13.- Se agrega la interfaz para poder configurarla dando clic en Add y guardamos.

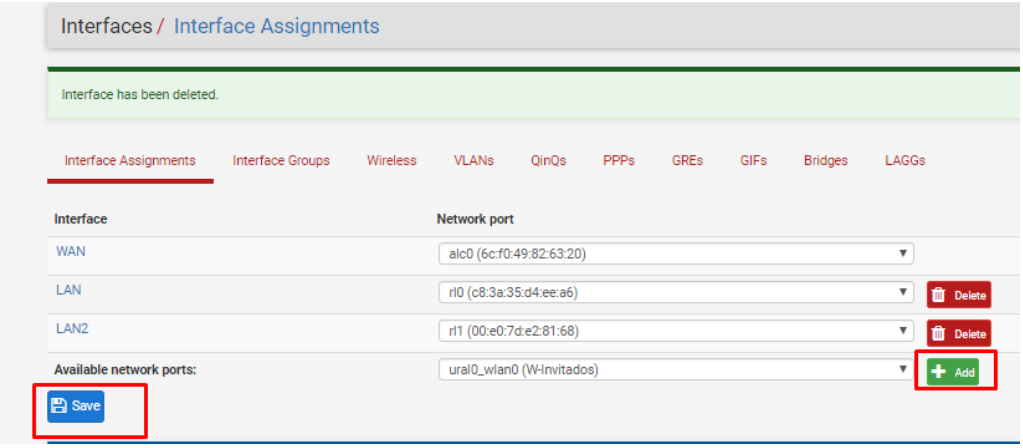

Ilustración 46: Asignación de Tarjeta Inalámbrica a Nueva Interfaz

14.- Una vez agregada la nueva interfaz la seleccionamos para realizar la configuración, al igual que las OPT es necesario habilitar la interfaz, existe la opción de cambiar el nombre de la interfaz, definir el modo de dirección IP, la interfaz será usada como WLAN usando como valores de configuración:

- Nombre de Interfaz: W-Invitados
- IP estática: 192.168.36.1
- Puerta de enlace por default
- Transmisión a través del canal: 11 b/g – 5
- Modo de la interfaz: punto de acceso
- Nombre de la red inalámbrica: Tesis-Invitados
- Contraseña de ingreso a la red: TESISINVITADOS1020

Una vez realizados los cambios Guardamos.

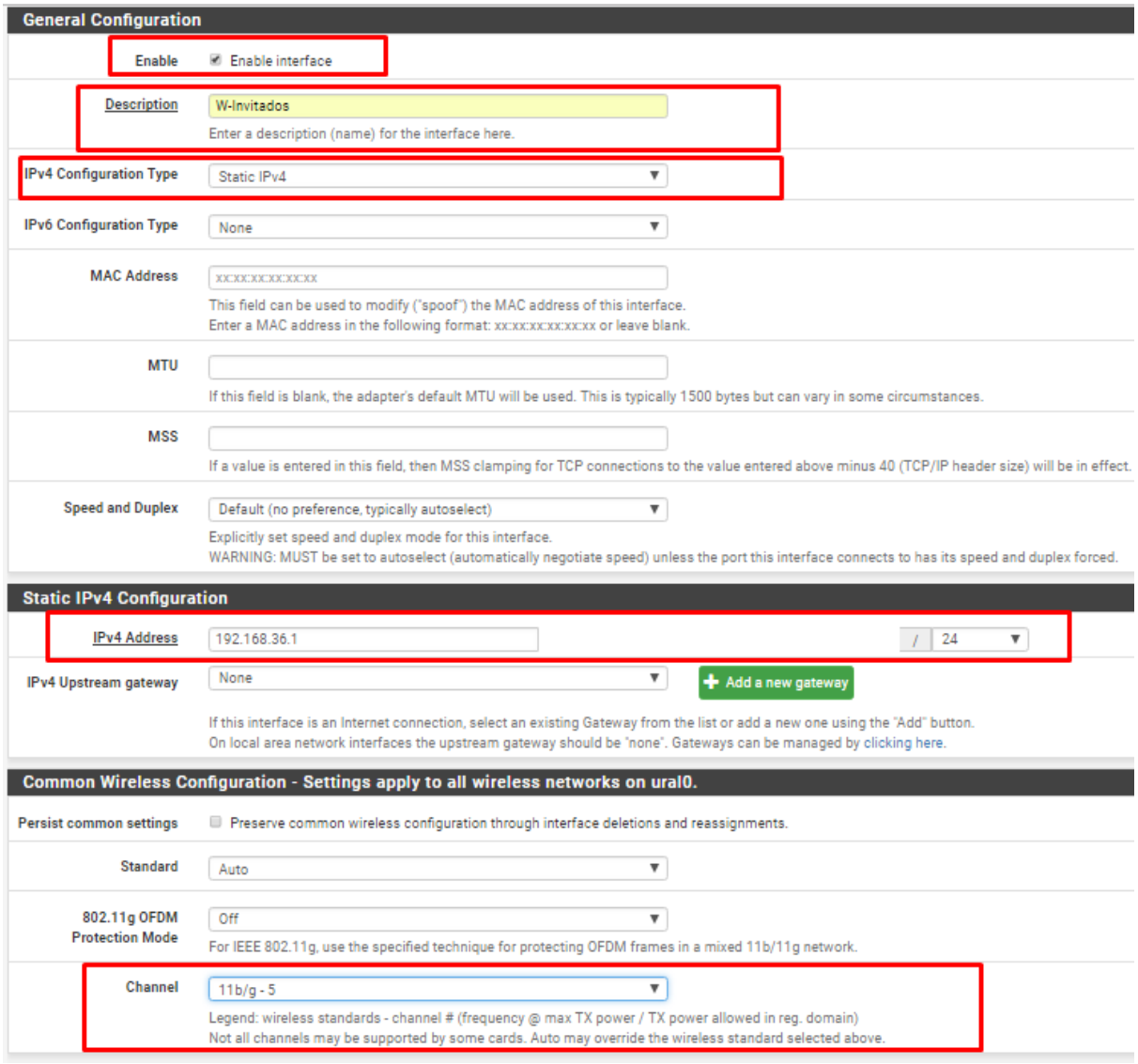

Ilustración 47: Configuración de Red Inalámbrica Parte 1

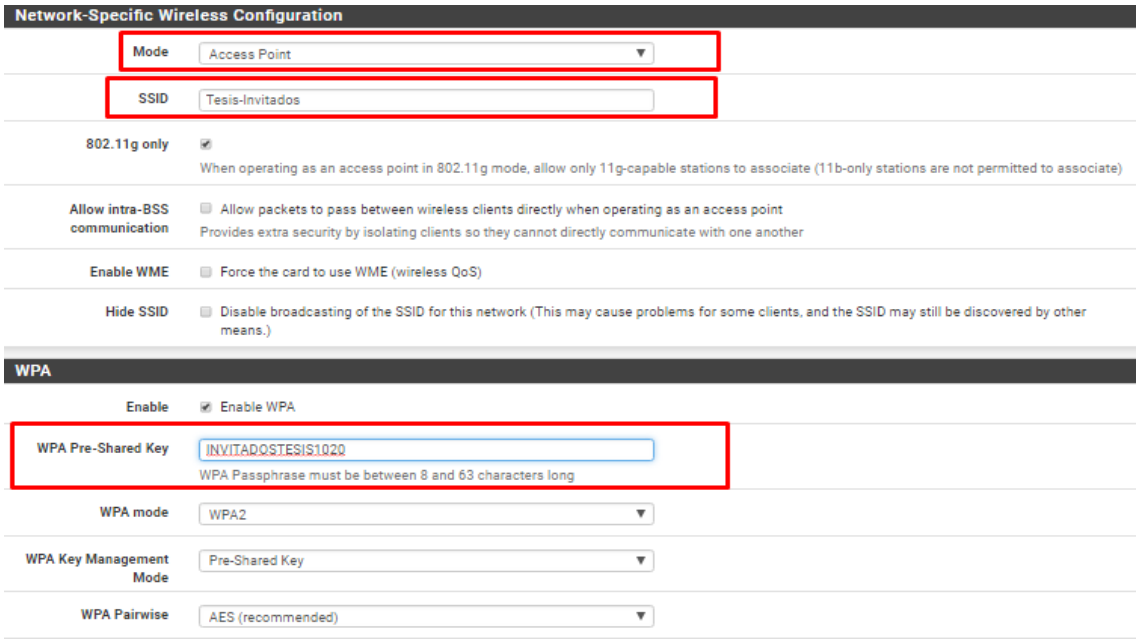

Ilustración 48: Configuración de Red Inalámbrica Parte 2.

3.7.3.3 Configuración de Servidores DHCP

1.- Se configura un servidor DHCP para cada una de las interfaces en la ruta: Services-> DHCP Server.

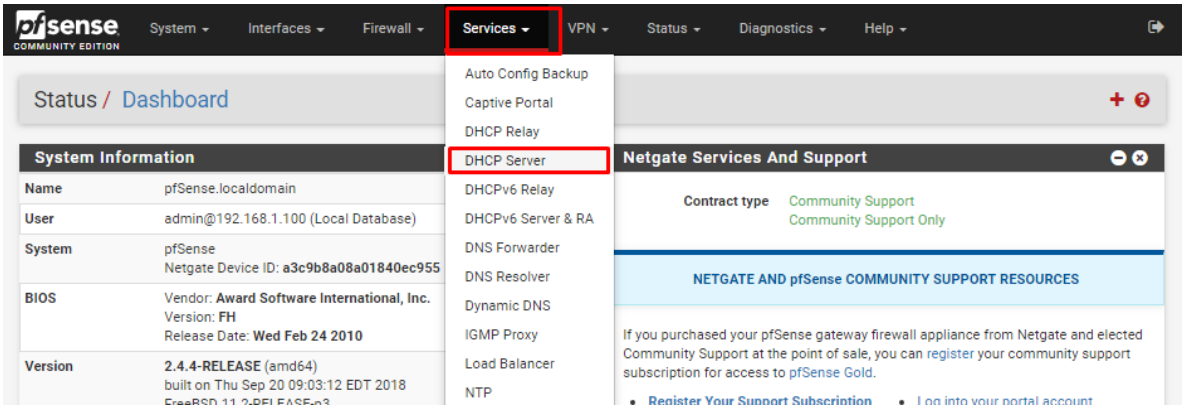

Ilustración 49: Ruta para la Gestión de Servidores DHCP.

2.- Dentro de cada configuración de servidor DHCP es necesario Habilitar la función, y definir el rango de direcciones IP dinámicas que se asignarán.

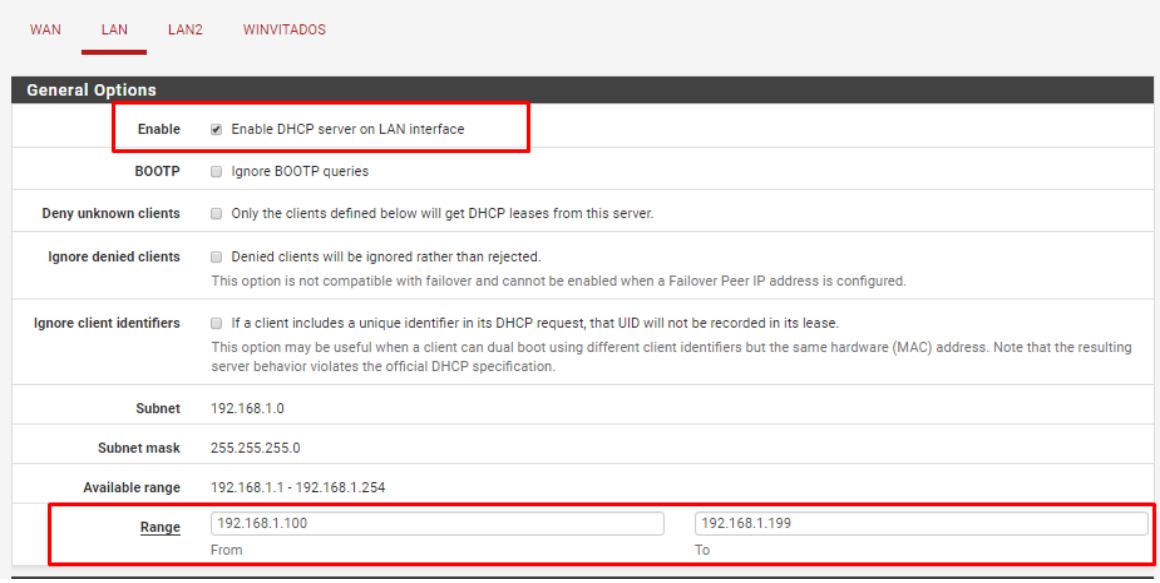

Ilustración 50: Configuración de Servidor DHCP para Interfaz LAN.

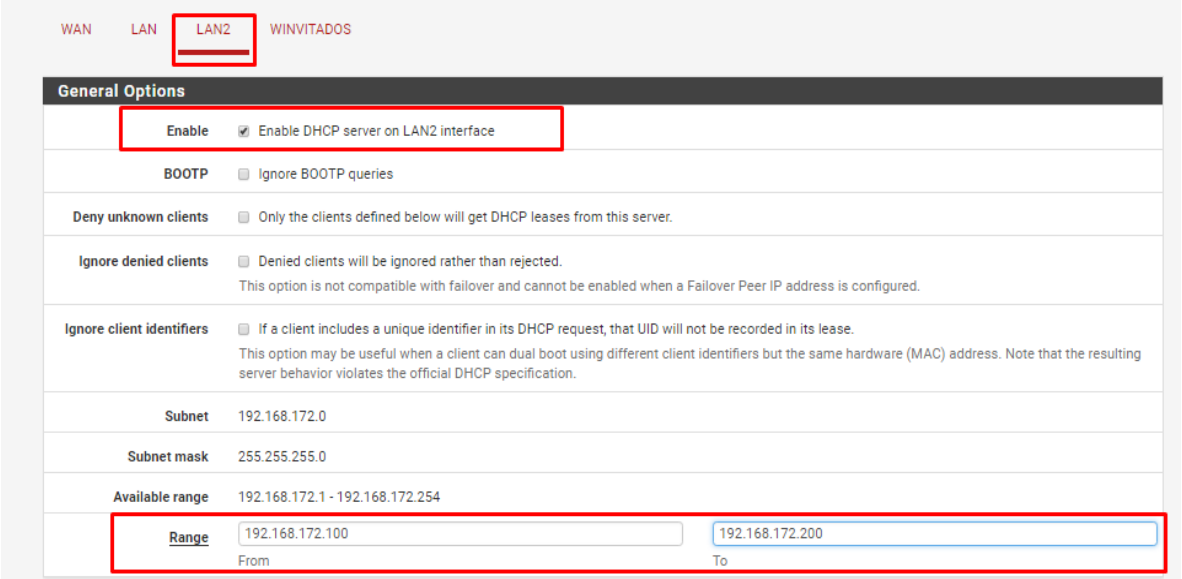

Ilustración 51: Configuración de Servidor DHCP para Interfaz LAN2.

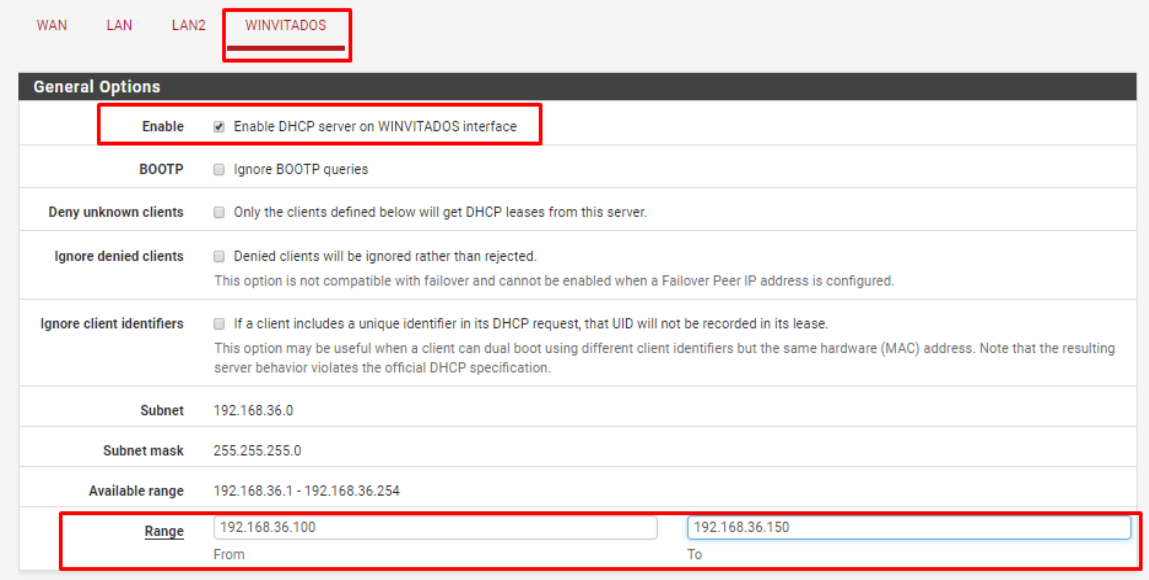

Ilustración 52: Configuración de Servidor DHCP para Interfaz WINVITADOS.

3.7.3.4 Configuración de Portal Cautivo

1.- Para poder dar de alta el control de acceso a la red inalámbrica mediante portal cautivo en pfSense es necesario ir a la pestaña Services-> Captive Portal.

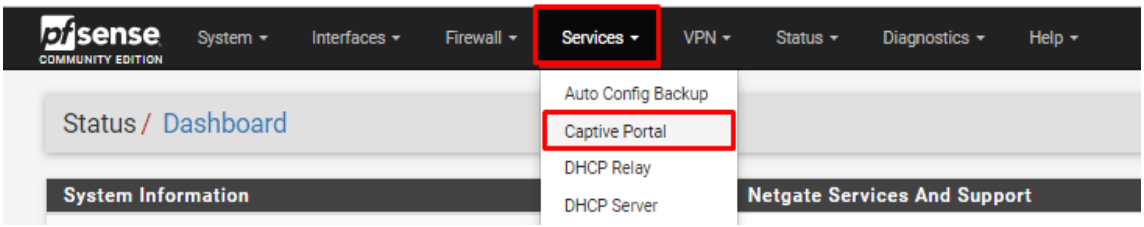

Ilustración 53: Ruta para la Creación de Portal Cautivo

2.- Dentro de Captive Portal se presentan los portales cautivos que se administran, en nuestro caso se creará el portal cautivo para eso seleccionamos Add.

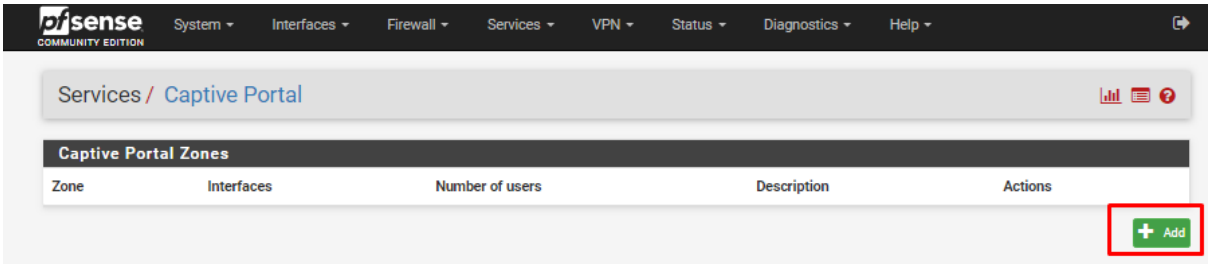

Ilustración 54: Agregar Portal Cautivo.

3.-Se agrega el nombre de la zona o portal cautivo y una breve descripción paso seguido seleccionamos Save & Continue.

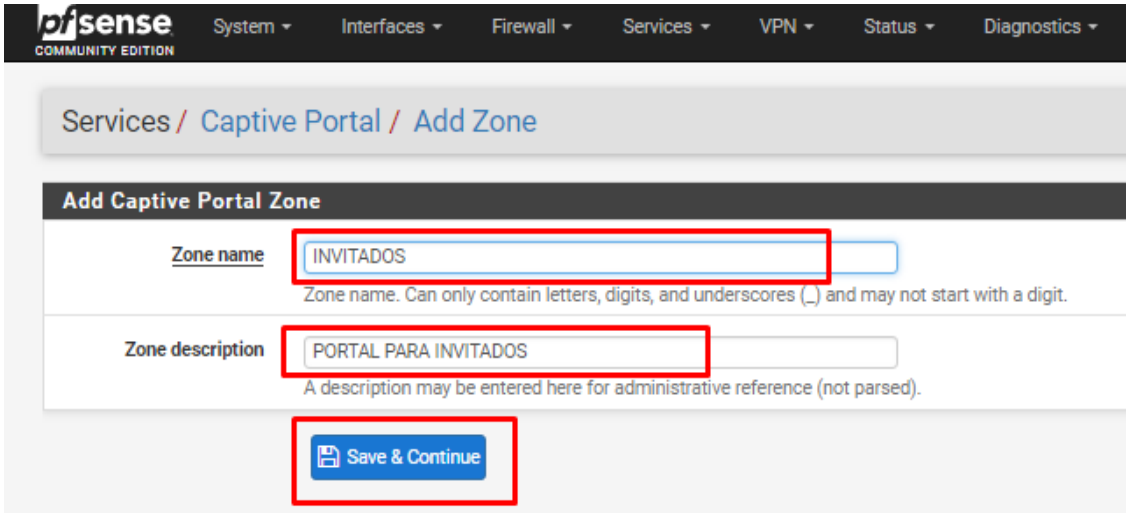

Ilustración 55: Creación de Portal Cautivo.

4.- Una vez creado el portal cautivo lo habilitamos y salvamos para que aparezca la configuración del portal cautivo.

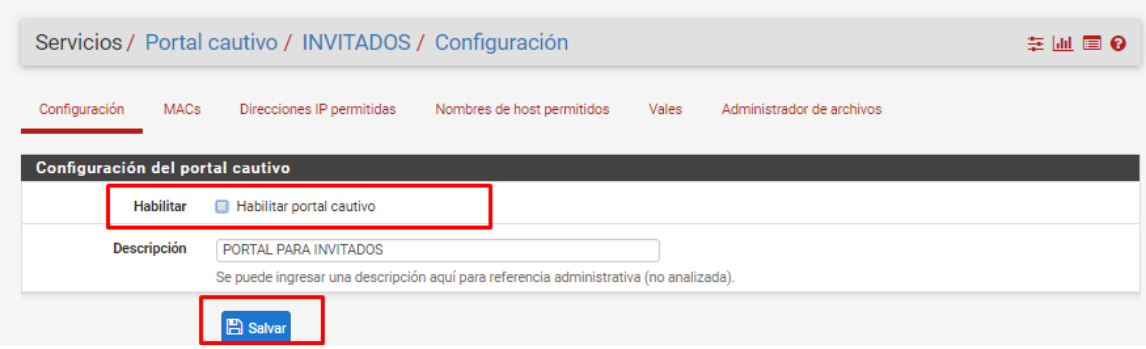

Ilustración 56: Habilitar Portal Cautivo.

5.- Una vez se muestra el panel de configuración del portal cautivo seleccionamos las opciones convenientes para la organización, para nuestro proyecto se tomarán en cuenta los siguientes parámetros.

- Interfaces: El portal cautivo se aplica en la interfaz WINVITADOS
- Idle timeout (Minutes): Tiempo de inactividad después del cual se desconectara al usuario 10 minutos, si se deja en blanco significa por tiempo indefinido.
- Hard timeout (Minutes): Tiempo que durara la sesión del usuario 30 minutos, si se deja en blanco significa por tiempo indefinido.

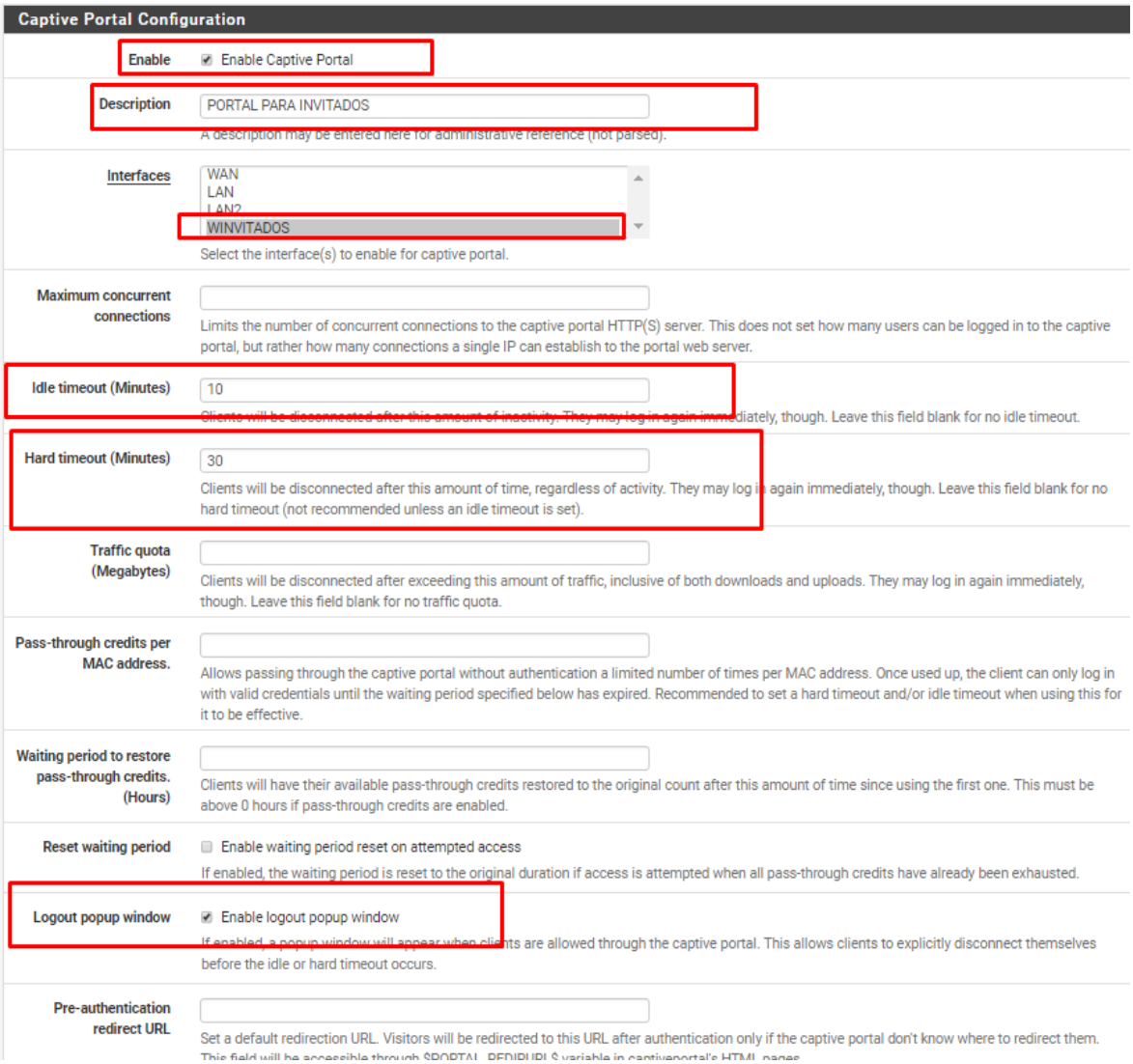

Ilustración 57: Panel de Configuración de Portal Cautivo (Parte 1).

Es posible usar una página personalizada del portal cautivo para ello seleccionamos la opción Use custom captive portal page para que se desplieguen las opciones para cargar la página personalizada.

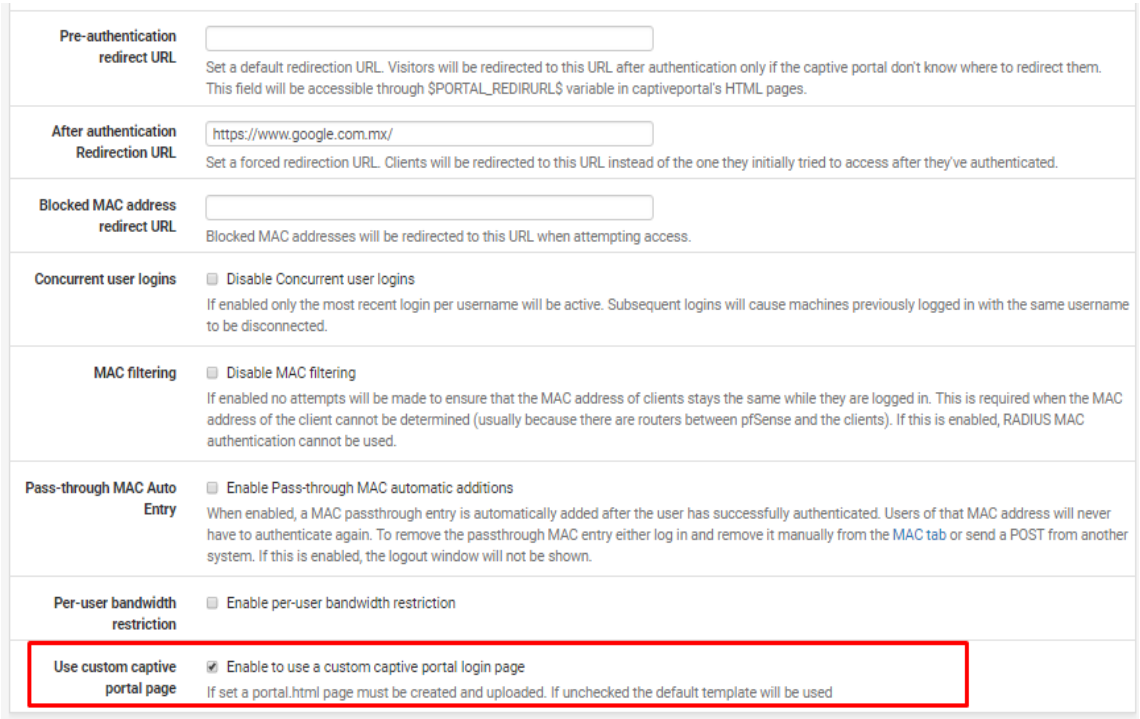

Ilustración 58: Panel de Configuración de Portal Cautivo (Parte 2).

Al desplegarse las opciones para cargar página personalizada, observaremos que pfSense nos presenta un ejemplo de código el cual podremos usar para crear nuestro portal personalizado.

- Portal page contents: Cargamos la página personalizada que usaremos como portal cautivo en formato php.
- Auth error page contents: Cargamos la página que se mostrará en caso de no iniciar sesión por algún error en el usuario y/o contraseña.
- Como portal page contents usaremos el código del Anexo 1
- Auth error page contents usaremos el código del Anexo 2

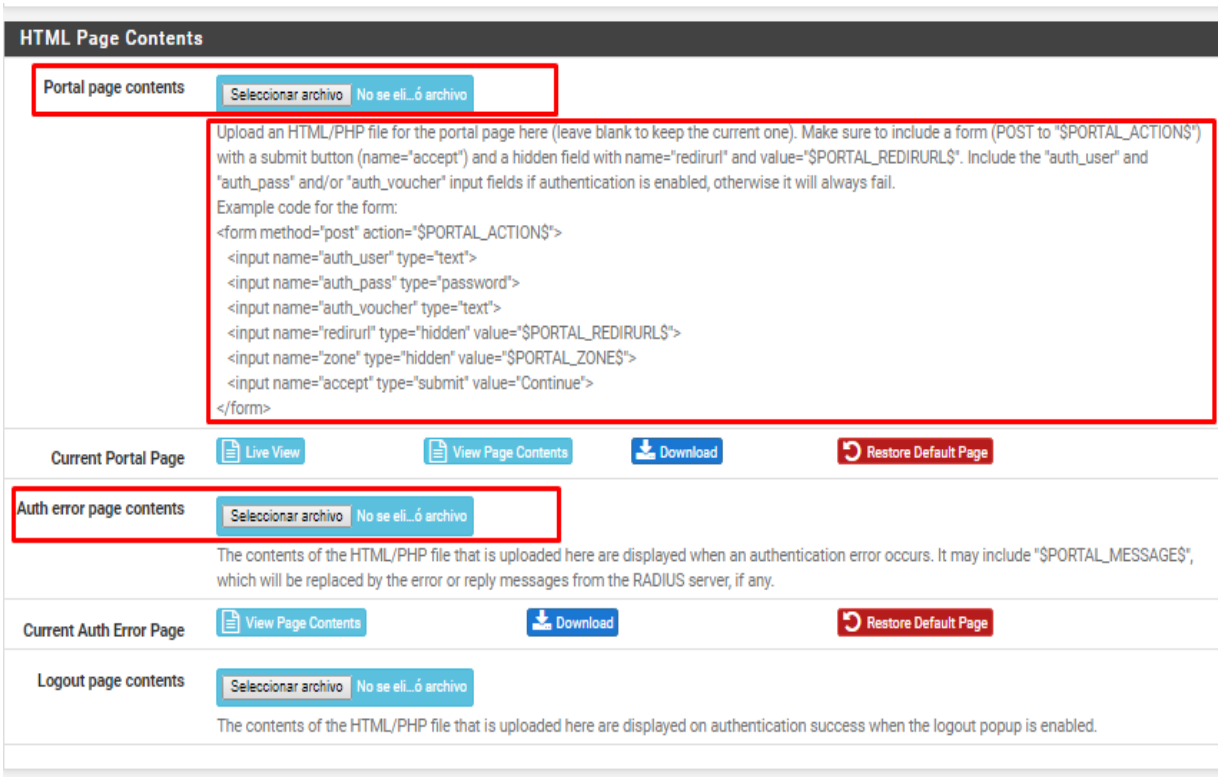

Ilustración 59: Panel de Configuración de Portal Cautivo (Parte 3).

Elegimos el modo de autenticación en el portal cautivo, para nuestro ambiente usaremos:

- Authentication Method: Use an Authentication backend, para usar usuario y contraseña
- Authentication Server: Local Database, para usar la base de datos local de pfSense

Salvamos los cambios.

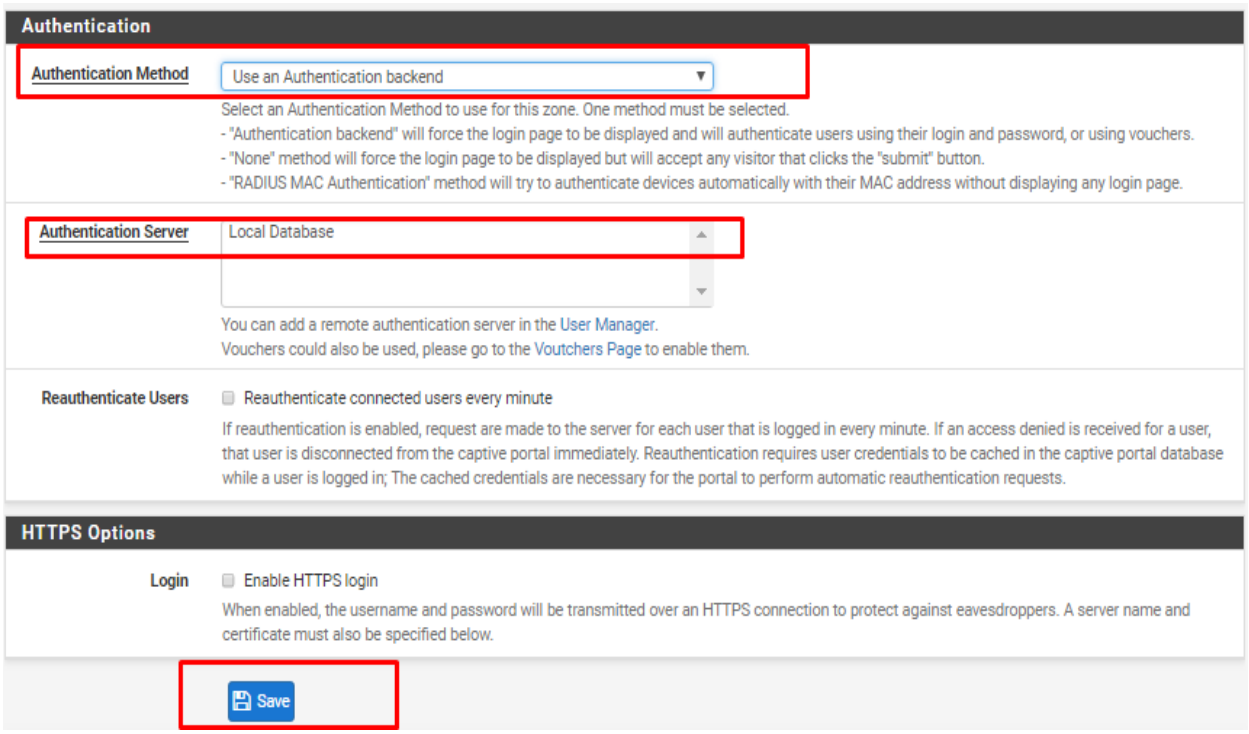

Ilustración 60: Panel de Configuración de Portal Cautivo (Parte 4).

6.- Todas las imágenes que se usen en la página personalizada deberán ser agregadas en la pestaña File Manager.

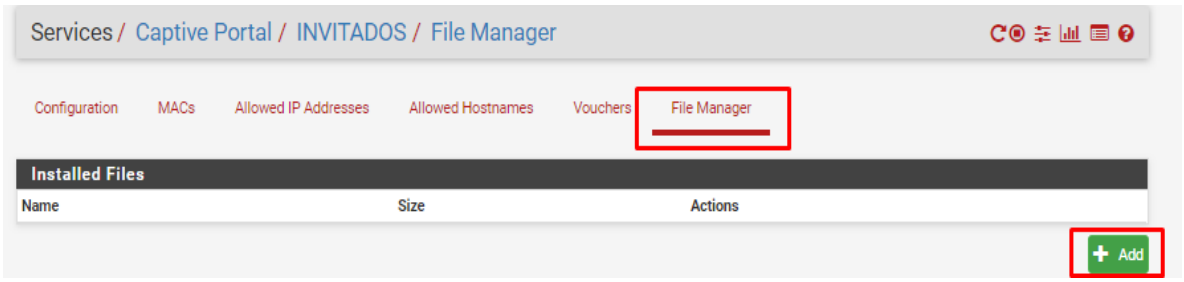

Ilustración 61: Repositorio de Imágenes Para Portal Personalizado.

7.-Para la creación de usuarios es necesario dirigirnos a la pestaña System -> User Manager.

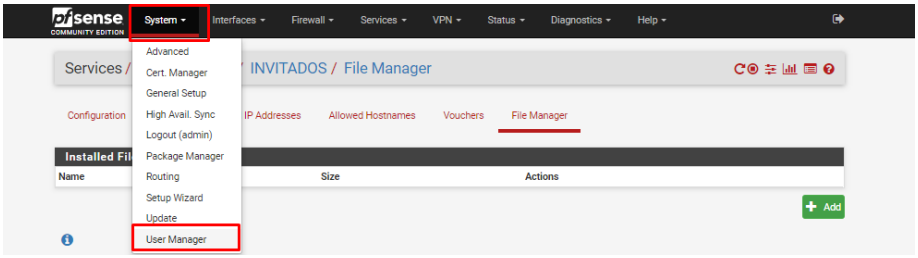

Ilustración 62: Ruta para la Gestión de Usuarios y Grupos.

8.- Una vez dentro nos dirigimos a la opción Groups y agregamos un nuevo grupo.

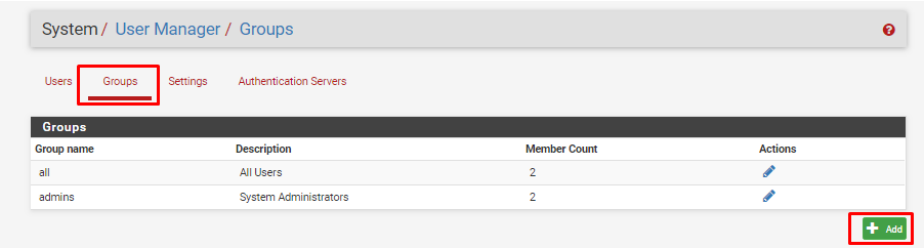

Ilustración 63: Agregar Nuevos Grupos.

9.- Se define el nombre del grupo, alcance, una breve descripción, al tener estos datos salvamos. Para nuestro proyecto se usarán los parámetros:

- Group Name: PORTALCAUTIVO
- Scope: Local (es importante definir el alcance local para el uso de este grupo)
- Description: ACCESO A INTERNET PORTAL CAUTIVO

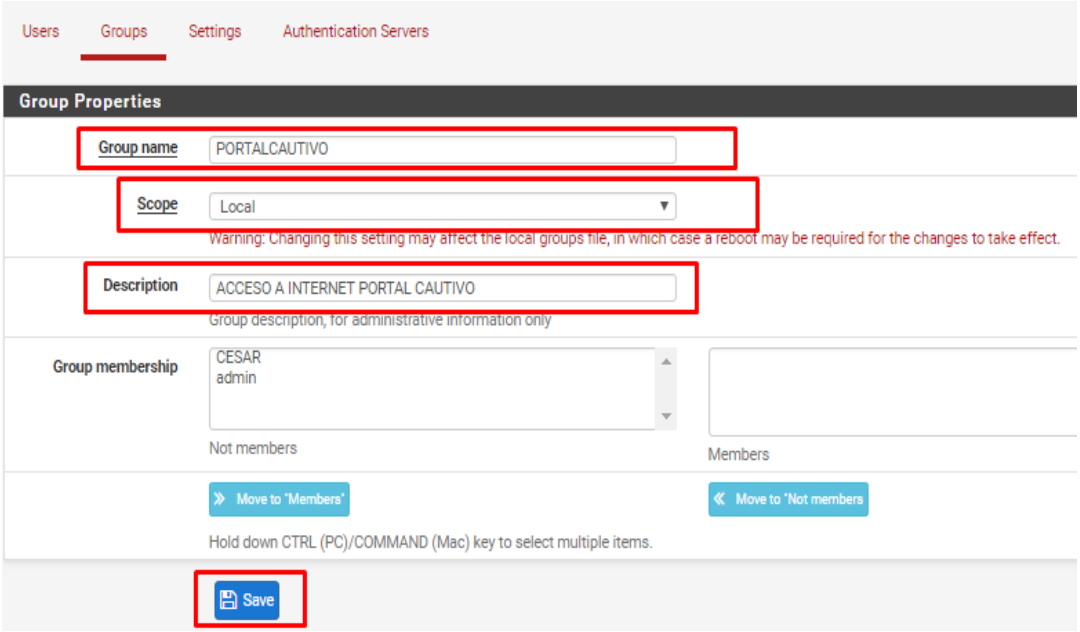

Ilustración 64: Configuración de Nuevo Grupo.

10.-Una vez creado el grupo nos dirigimos a la opción usuarios y agregamos los usuarios para el portal cautivo haciendo clic sobre Add.

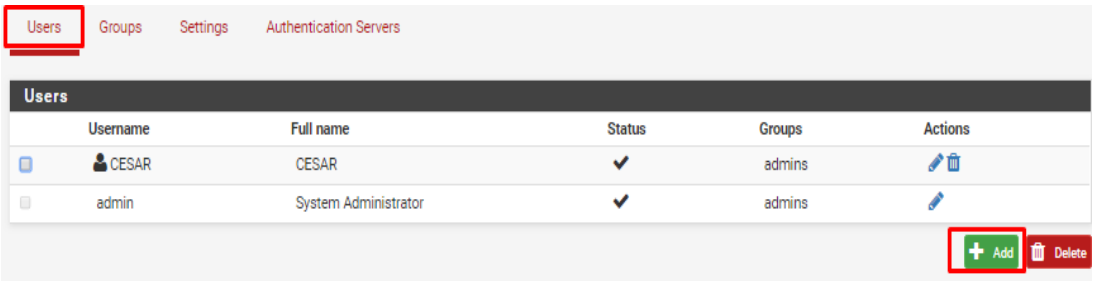

Ilustración 65: Agregar Nuevo Usuario.

11.- Para crear el usuario es necesario colocar un nombre de usuario, una contraseña, es posible establecer una fecha de caducidad para la cuenta, definir a que grupo pertenecerá el usuario y salvar los cambios realizados. Para nuestro caso práctico los datos usados serán:

- Username: INVITADO1 e INVITADO2
- Password: TESIS
- Full name: INVITADO1 e INVITADO2
- Group membership: PORTAL CAUTIVO

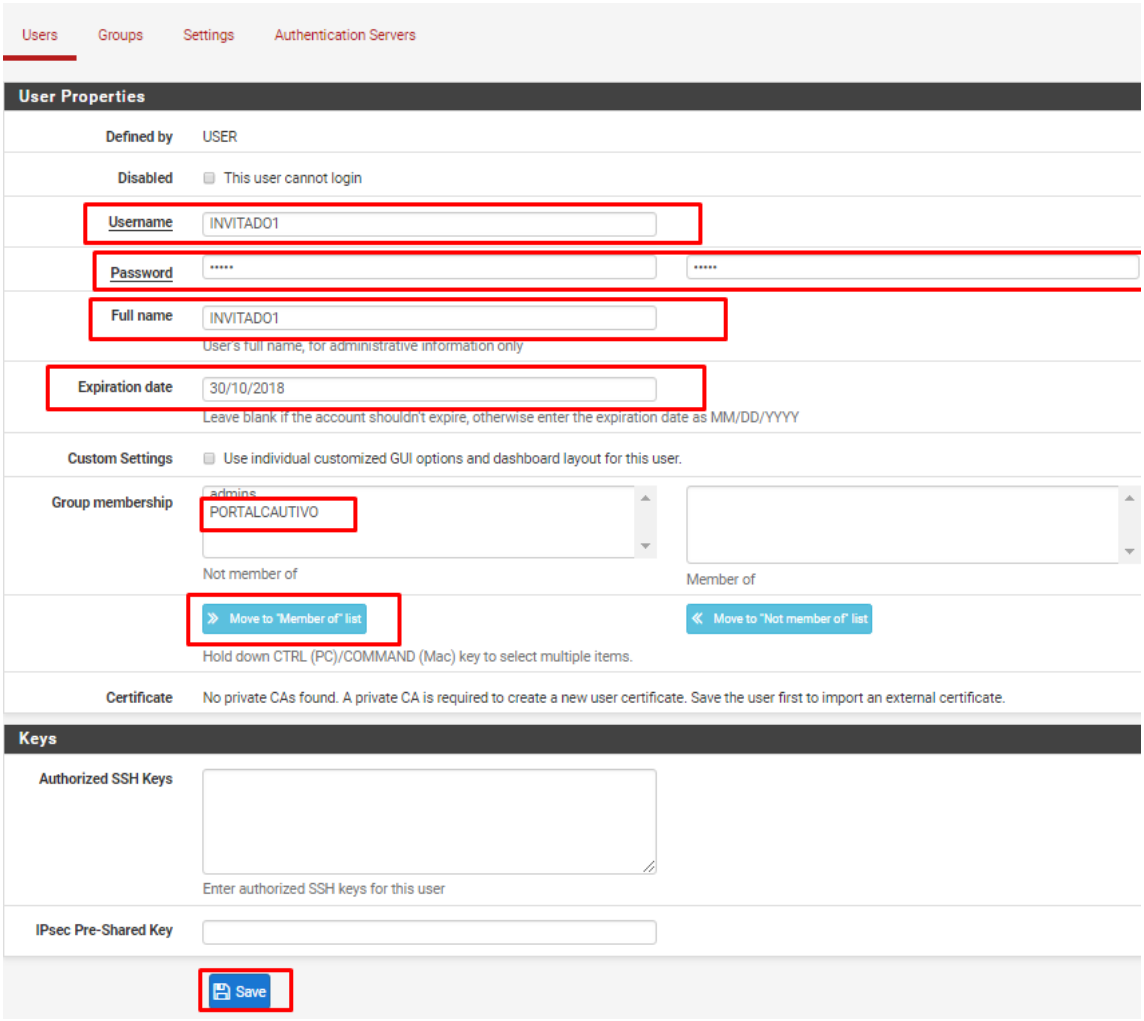

Ilustración 66: Panel de Configuración de Usuario.

12.- Editamos el usuario para poder definir los privilegios.

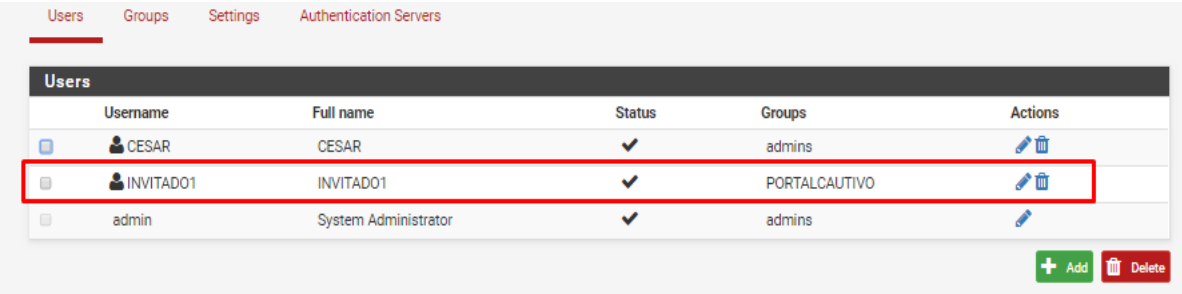

Ilustración 67: Selección de Usuario.

13.- En la sección Effective Privileges, agregaremos el privilegio para este usuario para ello damos clic en Add.

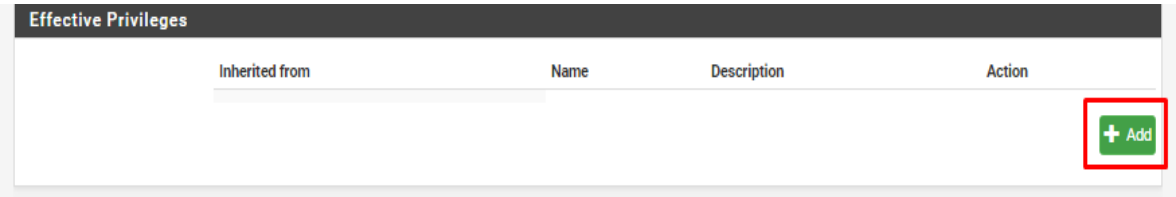

Ilustración 68: Agregar Nuevo Privilegio.

14.- Definimos el privilegio User- Service: Captive Portal login y salvamos.

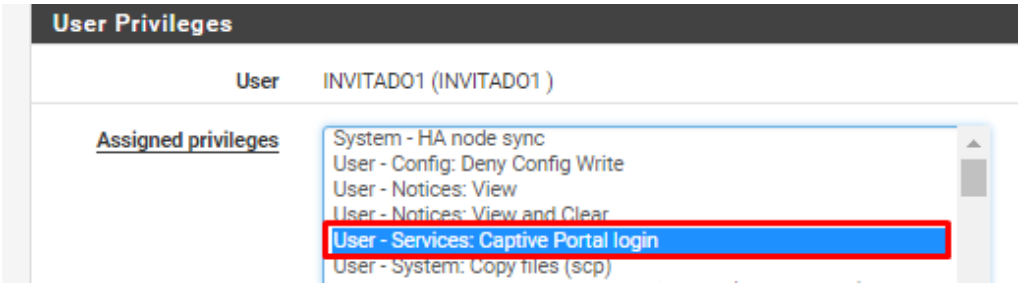

Ilustración 69: Selección de Privilegios.

Verificamos los usuarios creados

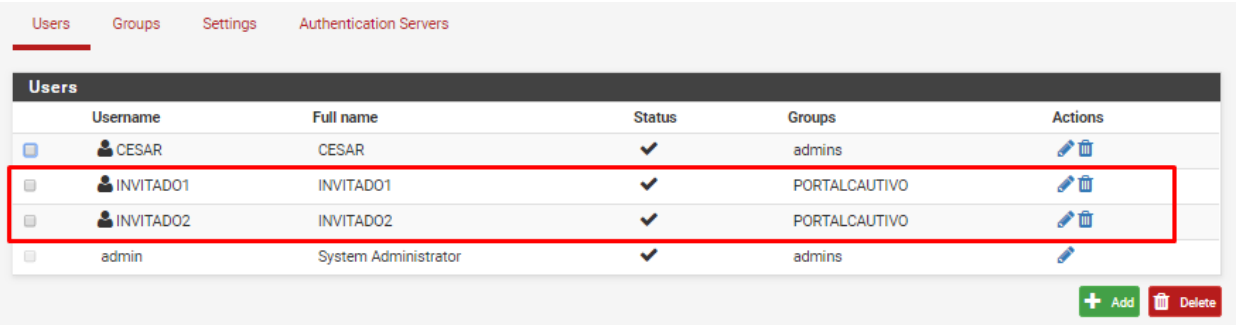

Ilustración 70: Vista de Usuarios Existentes

15.- Para el uso del portal cautivo el usuario se conectara a la red Wiffi Tesis-Invitados en la cual adquirirá una IP del rango especificado para esa red.

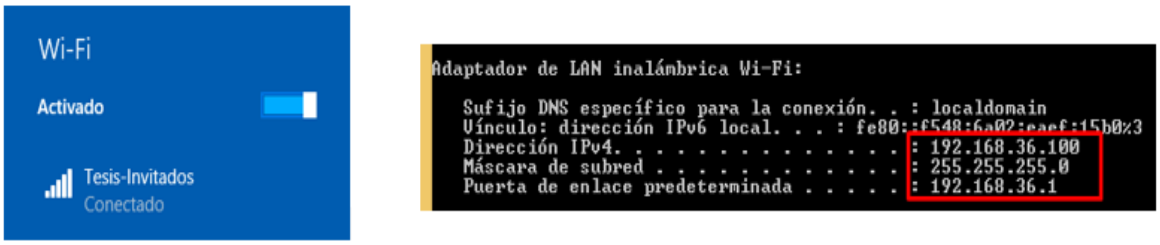

Ilustración 71: Validación de Conexión a Red Tesis-Invitados.

16.- Cuando el usuario desee ingresar a la red será redirigido al portal cautivo, en caso de fallo en la autentificación será dirigido al portal de error donde podrá seguir intentando autenticarse, si es válida la autenticación será redirigido a la página de inicio elegida y podrá navegar en internet.

Ilustración 72: Vista de la Página de Inicio de Sesión para Portal Cautivo.

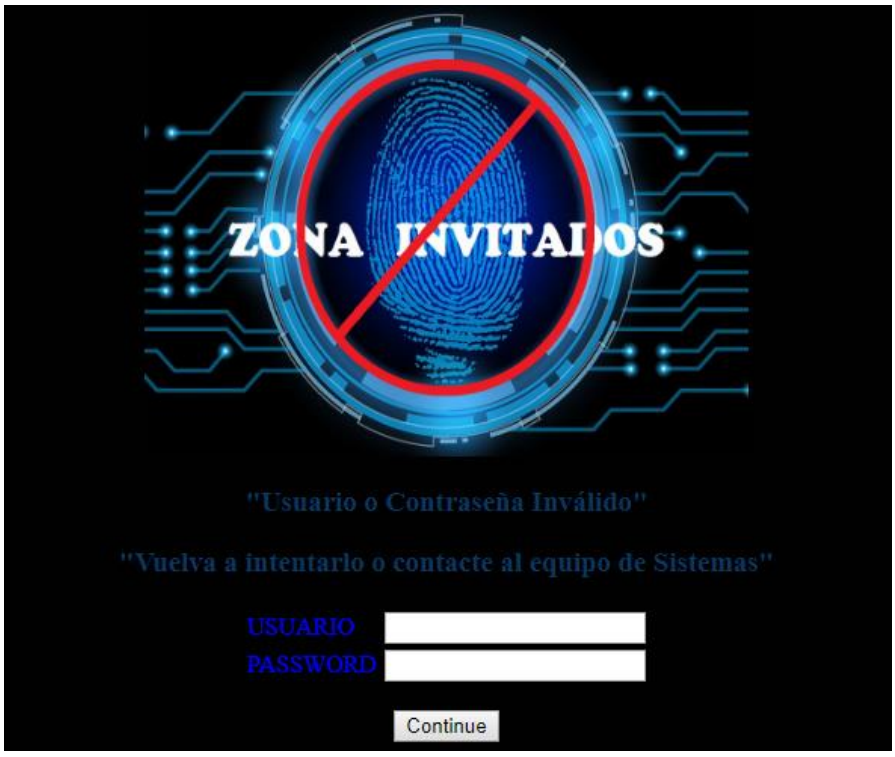

Ilustración 73: Pagina en Caso de Autenticación Fallida.

3.7.3.5 Configuración y Administración de Reglas de Firewall en pfSense

En pfSense la administración de reglas es relativamente simple, además de poder realizar reglas independientes para cada Interfaz.

1.- Para poder acceder a la configuración de Reglas de Firewall es necesario dirigirnos a la ruta Firewall-> Rules

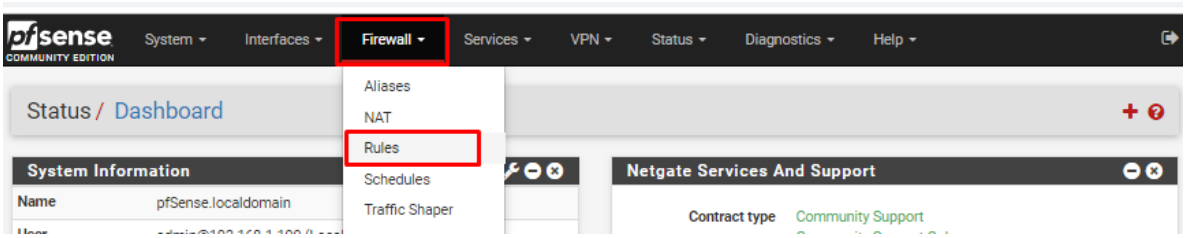

Ilustración 74: Ruta para Administración de Reglas de Firewall

2.- En la opción Rules se nos presenta la configuración independiente de cada una de las Interfaces configuradas, para nuestro caso nos dirigimos a la interfaz LAN2 la cual no tiene definida ninguna regla y seleccionamos Add para agregar la nueva red, la red WAN y LAN tienen configuradas reglas por defecto.

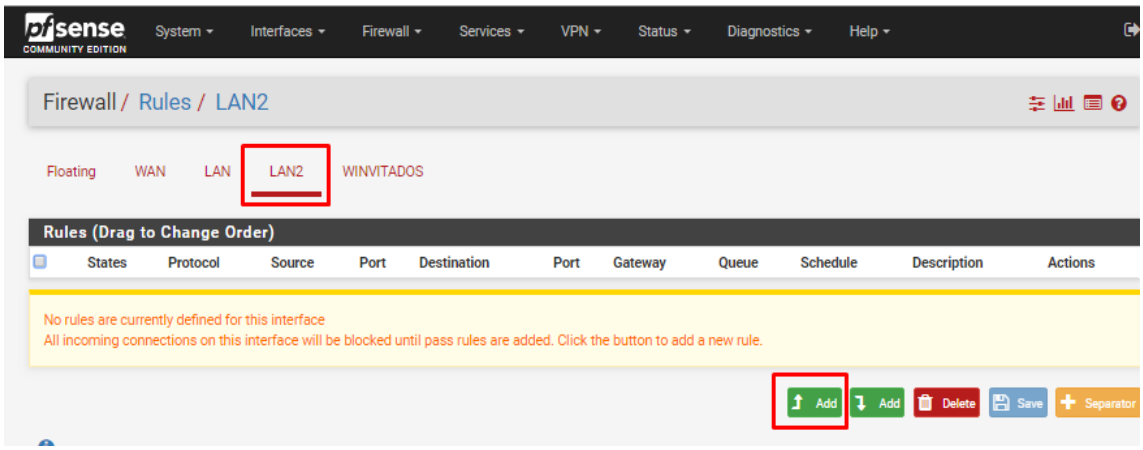

Ilustración 75: Lista de Reglas Bacía LAN2.

3.- Al crear una nueva regla veremos el panel de configuración de la regla donde podremos observar diferentes opciones para esta regla que permite el paso a internet por la red WAN por lo que nuestros puntos importantes a configurar son:

Action: Seleccionamos la acción que realizara la regla (Pass, permitir el paso).

Disabled: Permite deshabilitar la regla sin la necesidad de eliminarla (opción desactivada).

Interface: Red a la que se aplica la regla (LAN2).

Address Family: Representa la familia de direcciones que se permitirá dejar pasar (IPv4).

Source: Fuente de la cual proviene el tráfico (LAN2 net).

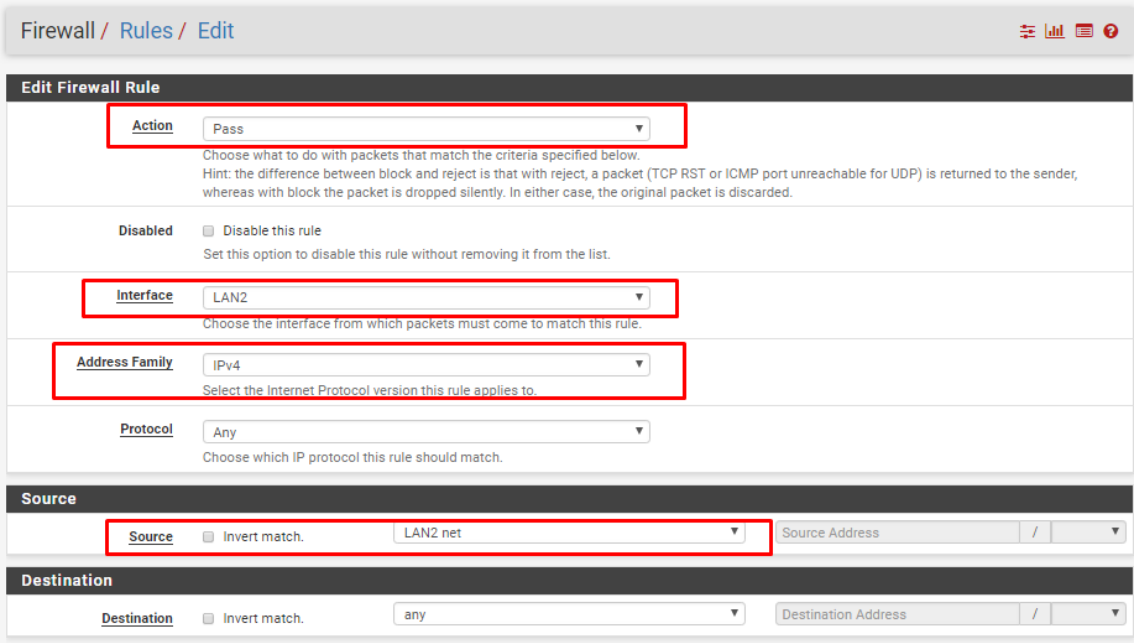

Ilustración 76: Panel de Configuración de Regla Parte 1.

Log: Esta función permite el registro en la conexión, bajo la advertencia de no hacerlo si el registro es muy extenso debido a la limitante en el espacio del servidor

Description: Permite una breve reseña sobre la función de la regla.

Una vez realizada la configuración se selecciona la opción Save para salvar o guardar los cambios.

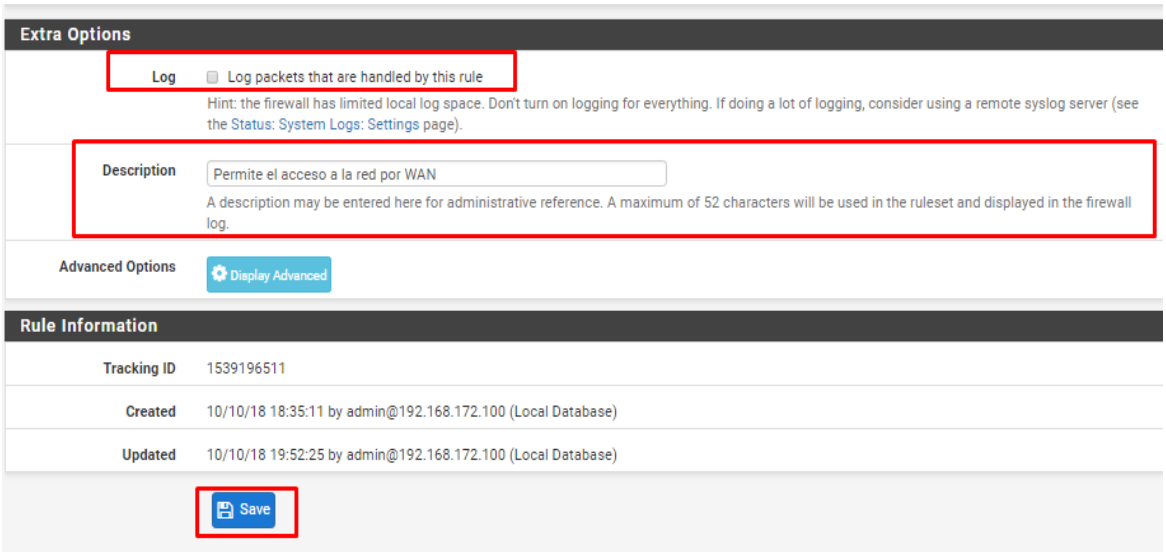

Ilustración 77: Panel de Configuración de Regla Parte 2.

4.- Confirmamos los cambios realizados para que la regla pueda tener efecto.

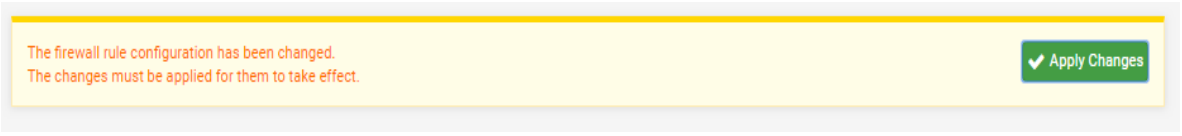

Ilustración 78: Confirmación de Cambio para Aplicar la Regla Creada.

5.-Se presentan las reglas contenidas en cada interfaz y una breve descripción de estas.

En la interfaz WAN se nos presentas 2 reglas por defecto, la primera bloquea la entrada de redes privadas desde el exterior, la segunda bloquea el tráfico de redes reservadas o direcciones falsas.

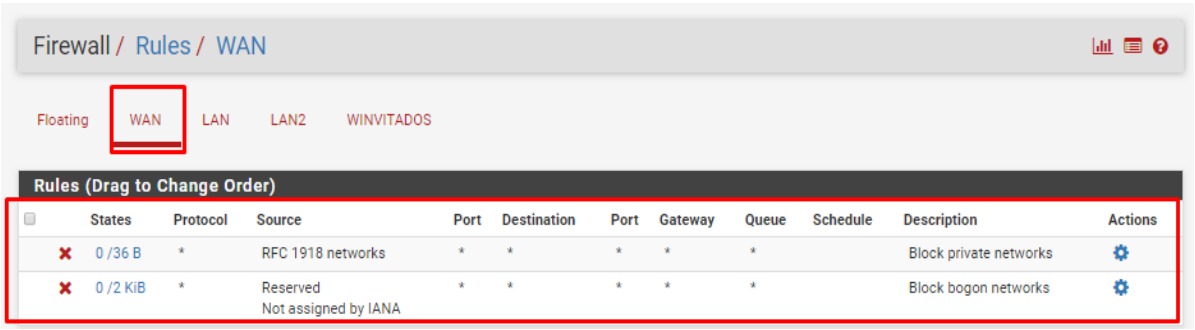

Ilustración 79: Reglas de Firewall Contenidas en Interfaz WAN.

En la interfaz LAN se nos presentas 3 reglas por defecto, la primera permite acceder al portal de configuración de cualquier equipo en LAN, la regla dos permite la conexión a cualquiera de las redes en el formato de conexión IPv4 (Esta configuración permite la conexión a internet de la red LAN), la regla tres realiza lo mismo que la regla dos solo que para el formato de conexión IPv6.

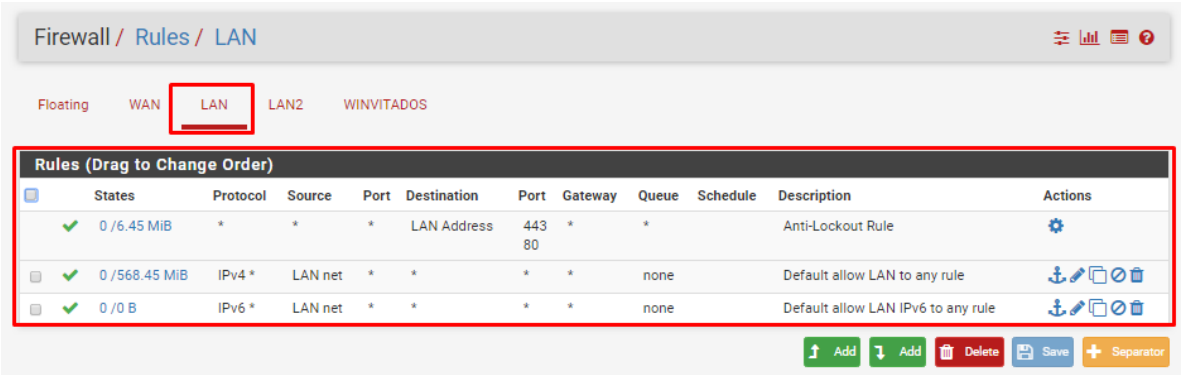

Ilustración 80: Reglas de Firewall Contenidas en Interfaz LAN.

En la interfaz LAN2 no se cuentan con reglas predeterminadas por lo que es necesario agregarlas, en nuestro caso se agrega una regla la cual permite la conexión entre las redes para poder tener acceso a internet.

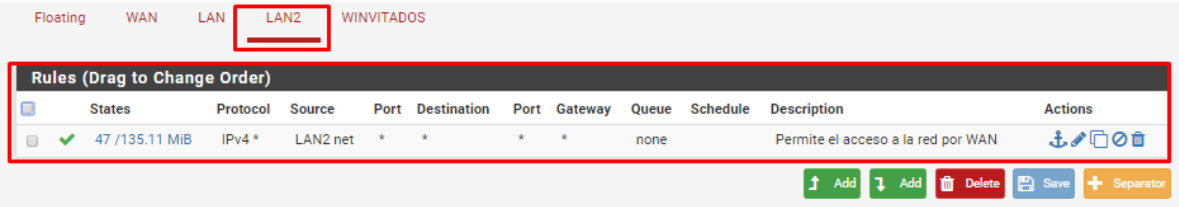

Ilustración 81: Reglas de Firewall Contenidas en Interfaz LAN2.

En la interfaz WINVITADOS no se cuentan con reglas predeterminadas por lo que es necesario agregarlas, en nuestro caso se agrega una regla la cual permite la conexión entre las redes para poder tener acceso a internet.

Ilustración 82: Reglas de Firewall Contenidas en Interfaz WINVITADOS.

3.7.3.6 Configuración VLAN

La configuración de redes virtuales en pfSense permite administrar redes independientes creando Interfaces virtuales a partir de las interfaces existentes.

1.- Para crear VLAN es necesario ir al menú Interfaces->Assignments, ver Ilustración 39.

2.-En el menú de las interfaces seleccionamos la opción VLANs para crear la nueva interfaz, agregamos la nueva interfaz dando clic en Add o añadir.

Ilustración 83: Añadir Nueva Interfaz VLAN.

4.- En la ventana de configuración de nuestra nueva interfaz VLAN seleccionaremos la tarjeta a usar en nuestro caso la tarjeta rl0, Asignamos una etiqueta para la VLAN, definimos la prioridad de uso y colocamos una breve descripción de la interfaz.

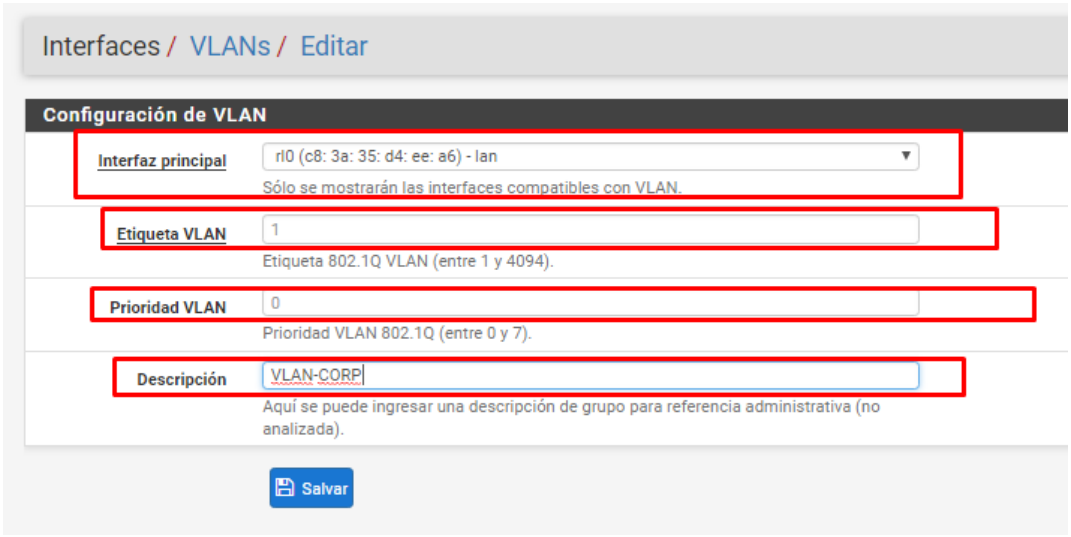

Ilustración 84: Asignación de Tarjeta para Interfaz VLAN.

5.- Validamos que la nueva interfaz se haya creado

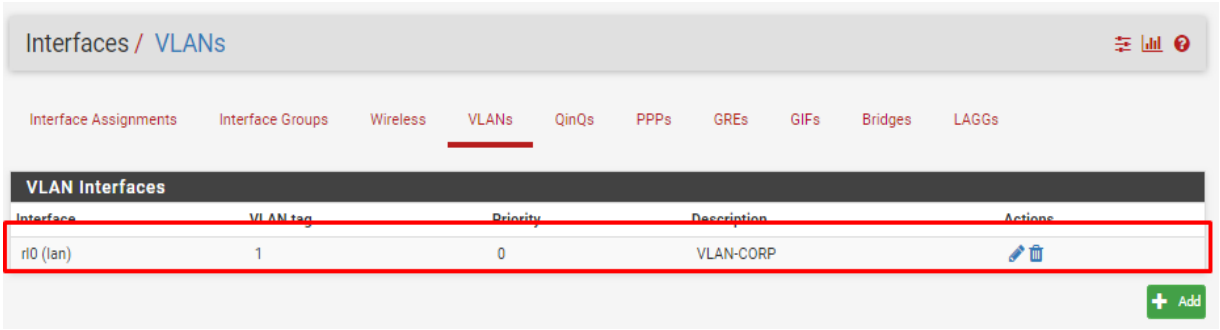

Ilustración 85: Interfaz VLAN Creada

6.- Como las interfaces anteriores es necesario agregarla para poder configurar la nueva conexión.

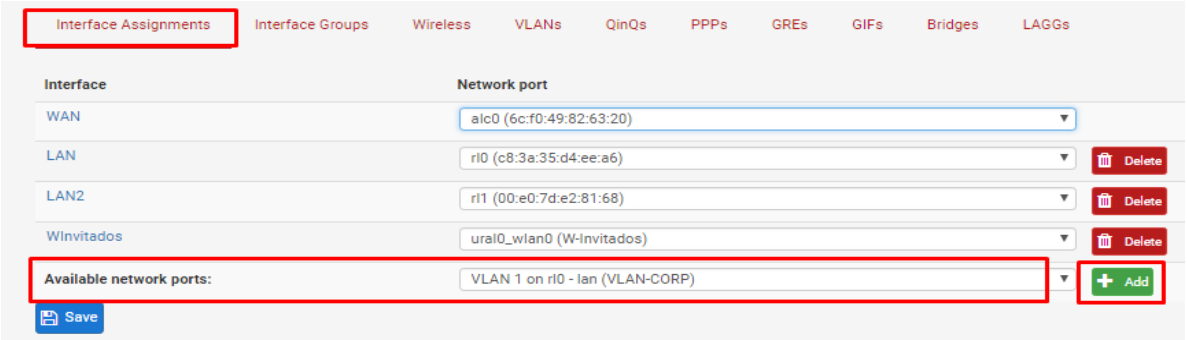

Ilustración 86: Agregar Nueva Interfaz VLAN para su Configuración

7.- Creada la nueva Interfaz se configurara igual que las anteriores Interfaces, se selecciona para configurarla.

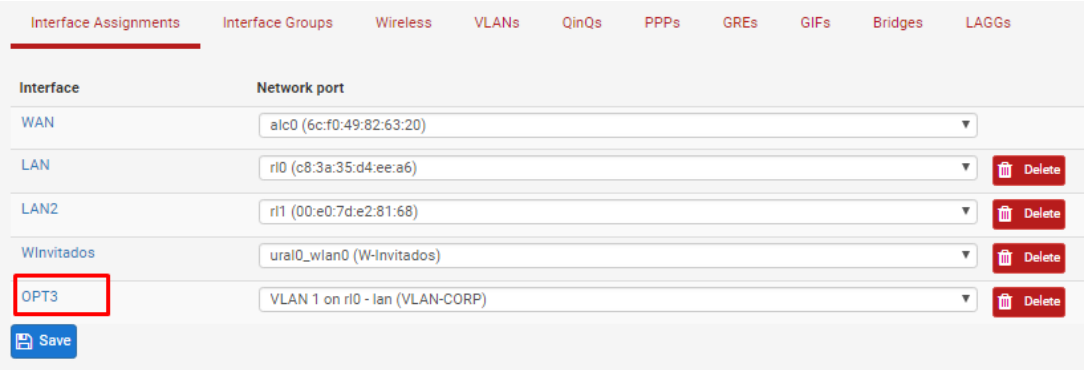

Ilustración 87: Selección de Nueva Interfaz OPT3.

8.- Para nuestro caso la dirección IP asignada a esta Interfaz será estática,IPv4 192.168.2.1/24 y su nombre VLANCORP, una vez realizada la configuración guardamos.

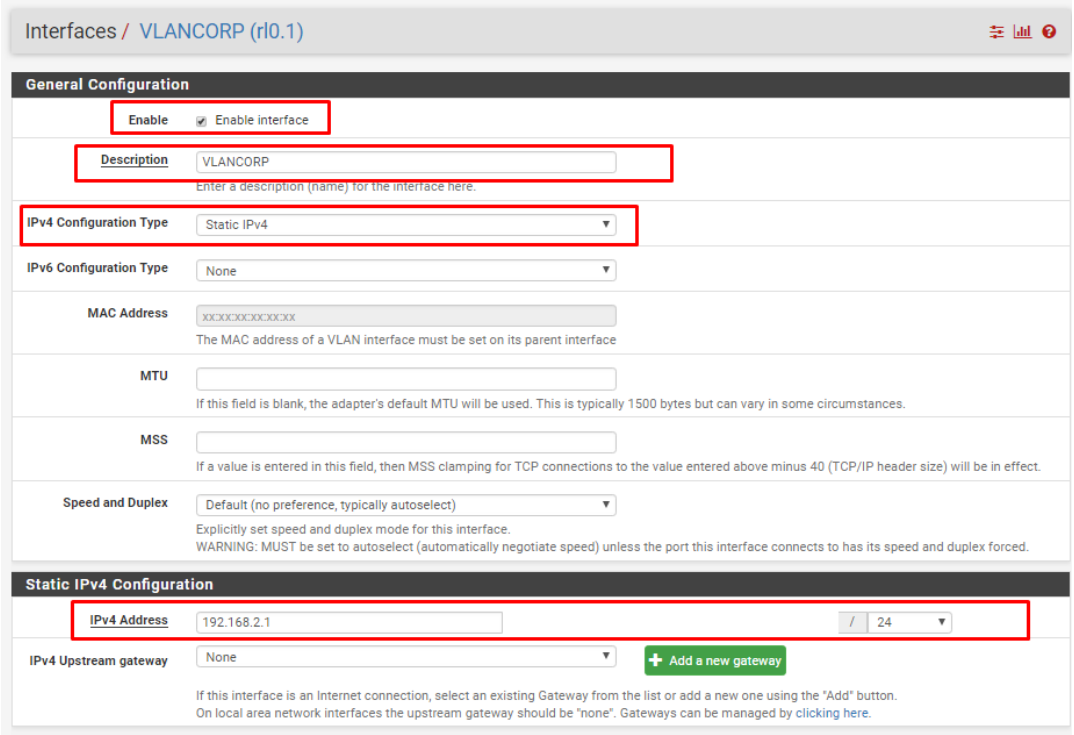

Ilustración 88: Panel de Configuración de Interfaz OPT3 (Interfaz VLAN).

9.- Confirmamos los cambios realizados

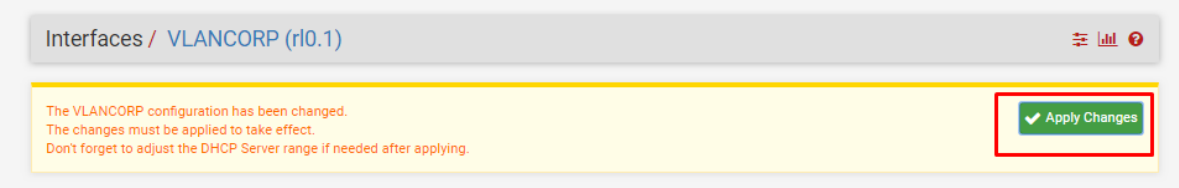

Ilustración 89: Confirmación de Cambios en OPT3 (VLANCORP).

10.- Habilitamos el Servidor DHCP para la interfaz VLANCORP y definimos un rango de IP que se podrán asignar en esta red.

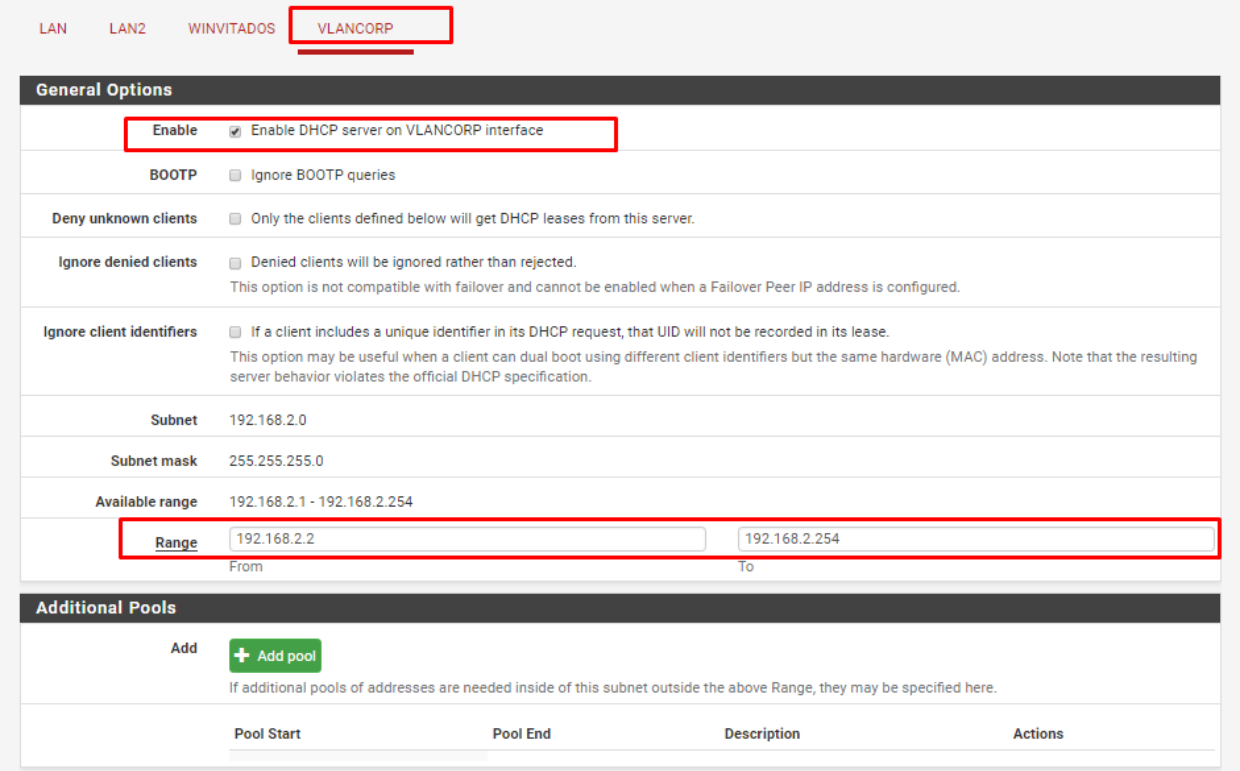

Ilustración 90: Panel de Configuración del Servidor DHCP para VLANCORP.

11.-Creamos la regla para permitir la conexión a internet en la interfaz VLANCORP

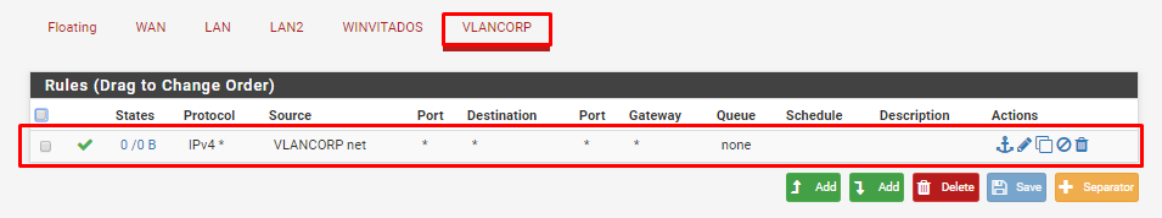

Ilustración 91: Lista de Reglas de Firewall para Interfaz VLANCORP.

3.7.3.7 Configuración VPN

1.-Para poder crear una conexión VPN en pfSense es necesario crear los certificados que validaran la conexión para ello vamos a la ruta System -> Cert. Manager

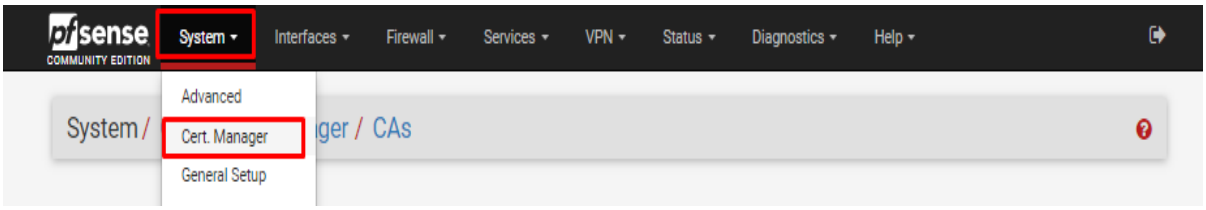

Ilustración 92: Ruta para la Administración de Certificados.

2.- En la opción CAs agregaremos una nueva autoridad certificadora.

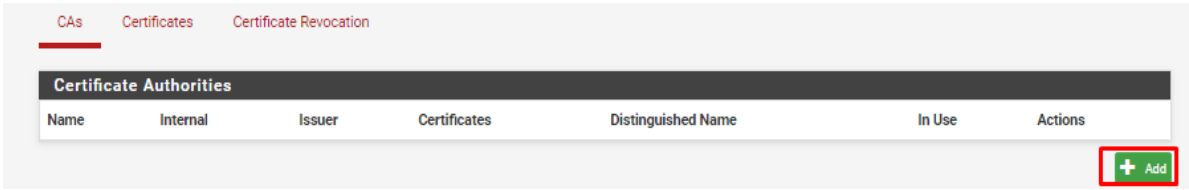

Ilustración 93: Agregar Nueva Autoridad Certificadora.

3.- En el panel de configuración asignaremos una breve descripción, el método del certificado, Los datos de región y nombre de la organización. Los demás datos se dejaran por defecto, una vez realizados los cambios seleccionamos Save para guardar los cambio y crear el certificado.

Nota: Para nuestro caso se selecciona como Method: Create an internal Certificate Authority.

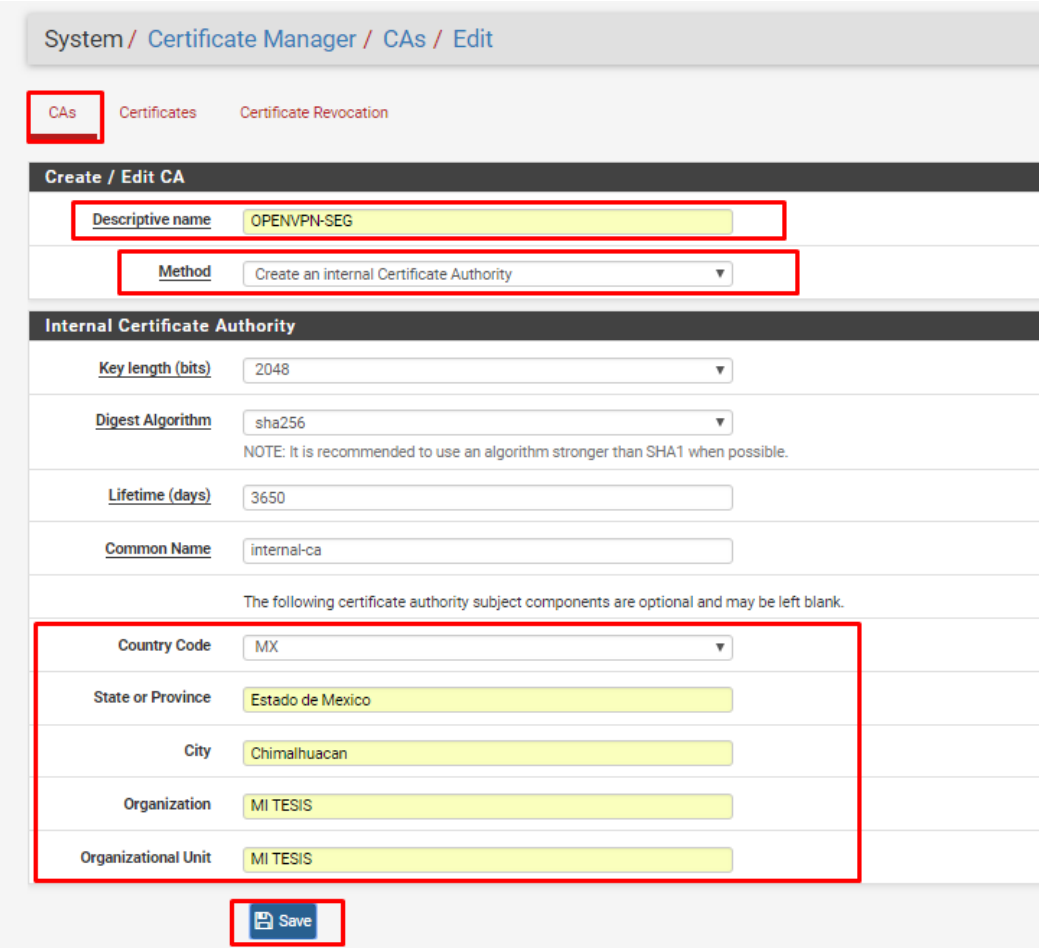

Ilustración 94: Panel de Configuración de Autoridad Certificadora.

4.- Tendremos que crear un certificado de servidor para esto seleccionamos la opción Certificates y agregamos un nuevo certificado.

Ilustración 95: Creación de Nuevo Certificado.

5.- En el panel de configuración seleccionamos el método para este certificado, para nuestro caso Method: Create an internal Certicate, agregamos una descripción para nuestro certificado y en la opción Common Name colocamos como nombre el mismo nombre colocado en la descripción.

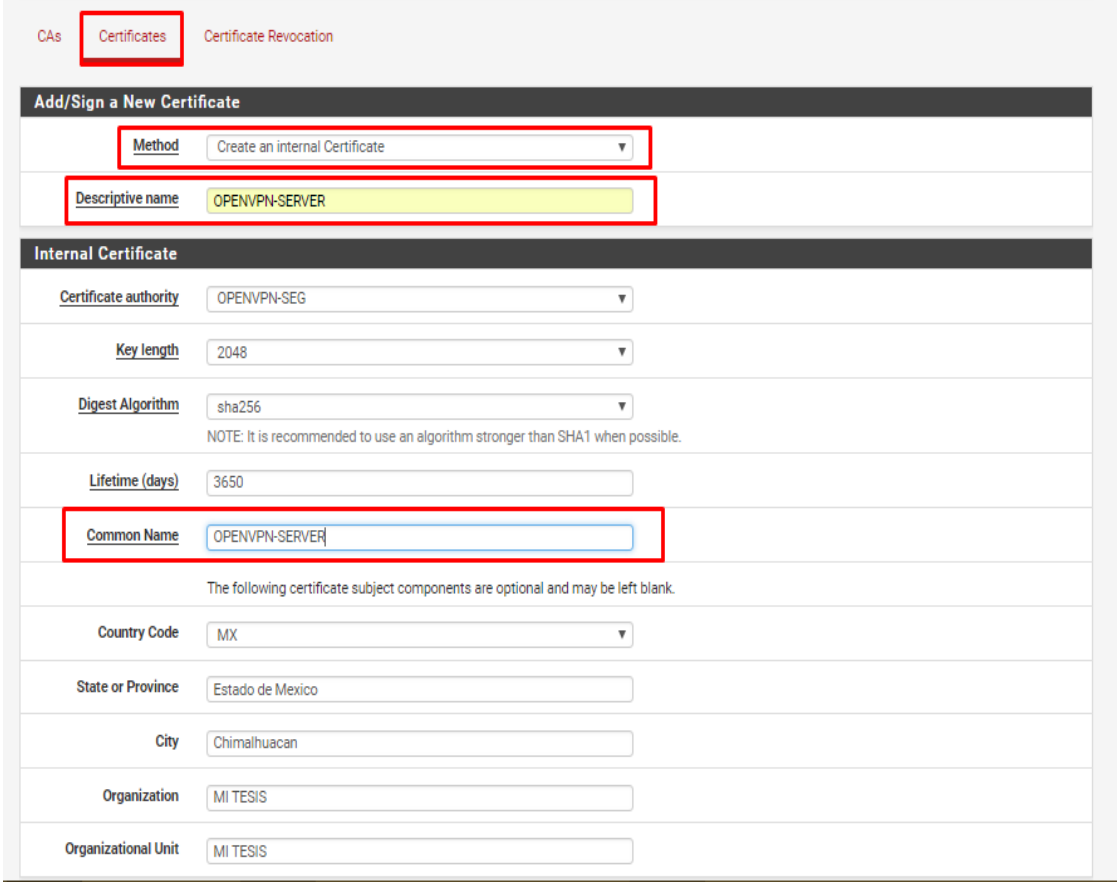

Ilustración 96: Panel de Configuración de Certificado Parte 1.

Seleccionamos el tipo de certificado como Server Certificate ya que será un certificado de servidor.

Los demás campos se dejaran por defecto, una vez realizados los cambio seleccionamos la opción Save para guardar los cambios.

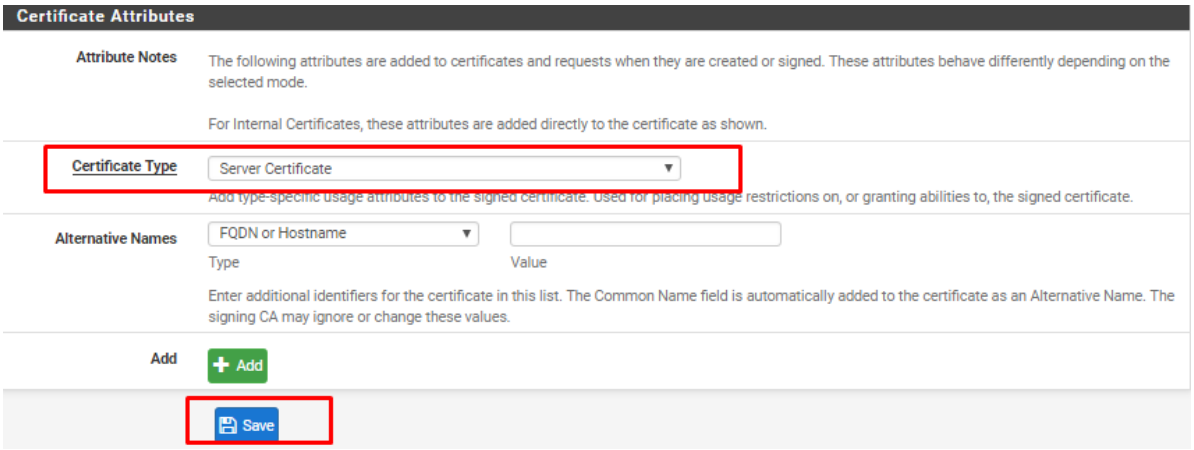

Ilustración 97: Panel de Configuración de Certificado Parte 2.

6.- Crearemos usuarios para la conexión OPENVPN, para ello tenemos que dirigirnos a la gestión de usuarios local ver Ilustración 62 y agregar un nuevo usuario, asignaremos un usuario y una contraseña así como el nombre del usuario. Es importante seleccionar la opción Certificate.

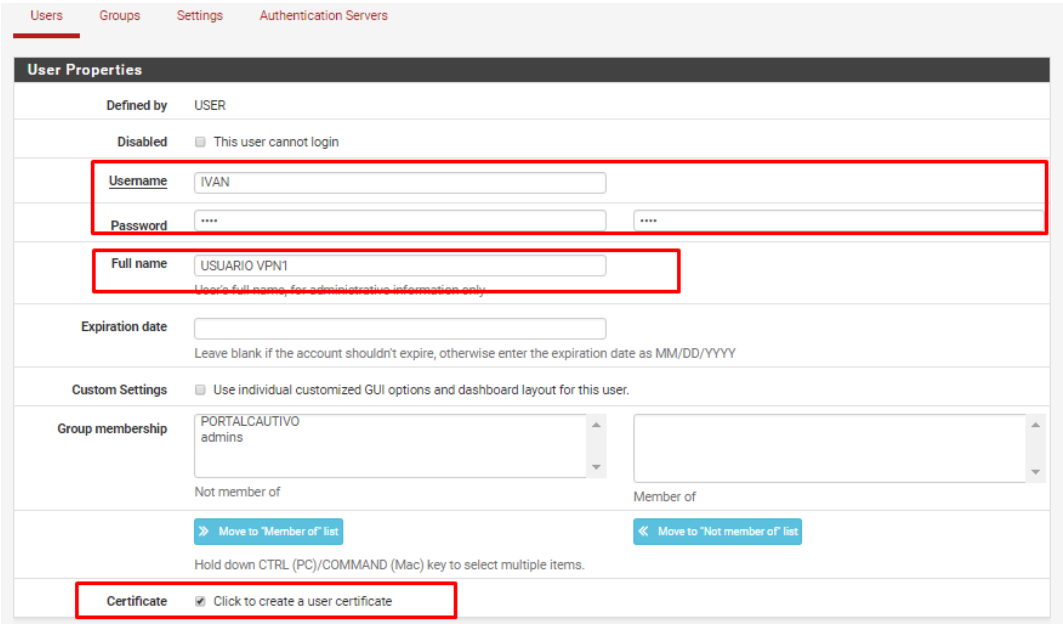

Ilustración 98: Panel de Configuración de Usuario de VPN Parte 1.

Para configurar el certificado, colocaremos una descripción del certificado y seleccionamos la entidad certificadora. Una vez realizados los cambios seleccionamos la opción Save.

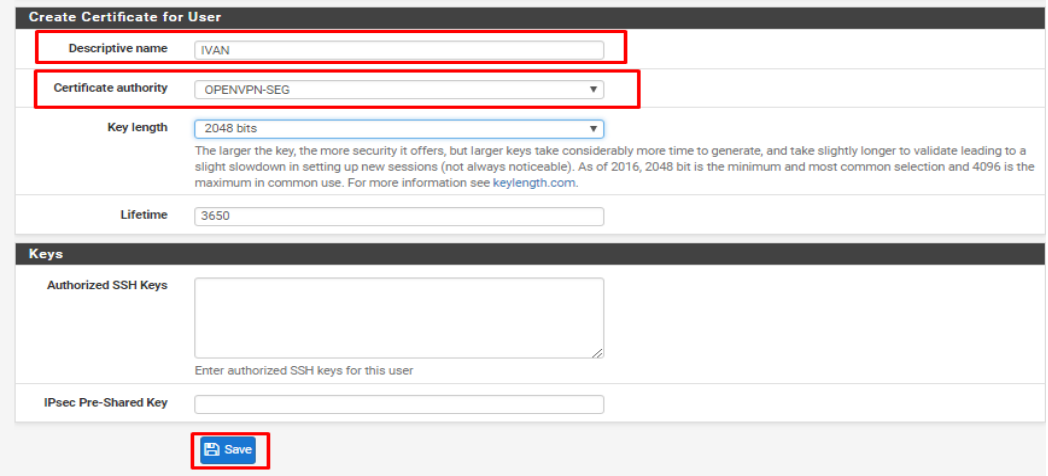

Ilustración 99: Panel de Configuración de Usuario de VPN Parte 2

7.- Crear servidor OpenVPN en la ruta VPN-> OpenVPN.

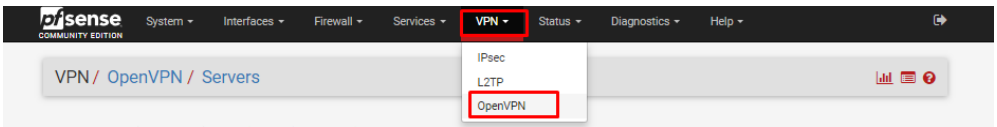

Ilustración 100: Ruta para la Gestión de Servidores VPN.

8.-En la opción Servers agregamos un nuevo servidor.

Ilustración 101: Agregar Nuevo Servidor VPN.

9.- En la configuración del nuevo servidor seleccionaremos como Server mode: Remote Access (SSL/TLS+User Auth), como Backend for Authentication: Local Database, una breve descripción del servidor, seleccionamos nuestra entidad certificadora creada y el certificado de servidor creado.

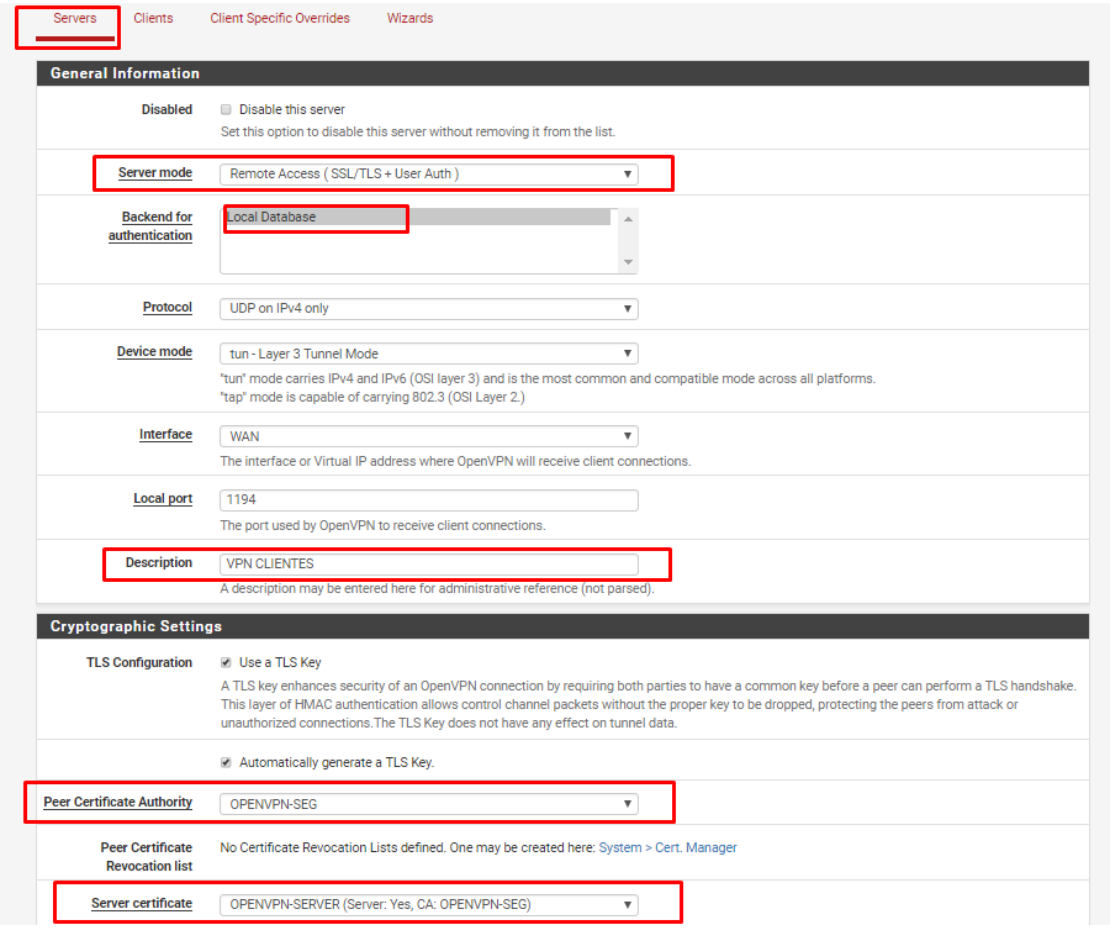

Ilustración 102: Panel de Configuración de Servidor VPN Parte 1.

En la configuración de túnel se presenta la opción IPv4 Tunnel Network en el cual es necesario colocar una IP que no se encuentre en el rango de direcciones usados en nuestra red interna, esta opción define el rango de IP que usará el túnel , tomando como referencia el la sugerencia usaremos la red 10.40.85.0/24. En la opción IPv4 Local networks(s) colocaremos las conexiones a las cuales tendrá acceso el usuario al conectarse al túnel VPN.

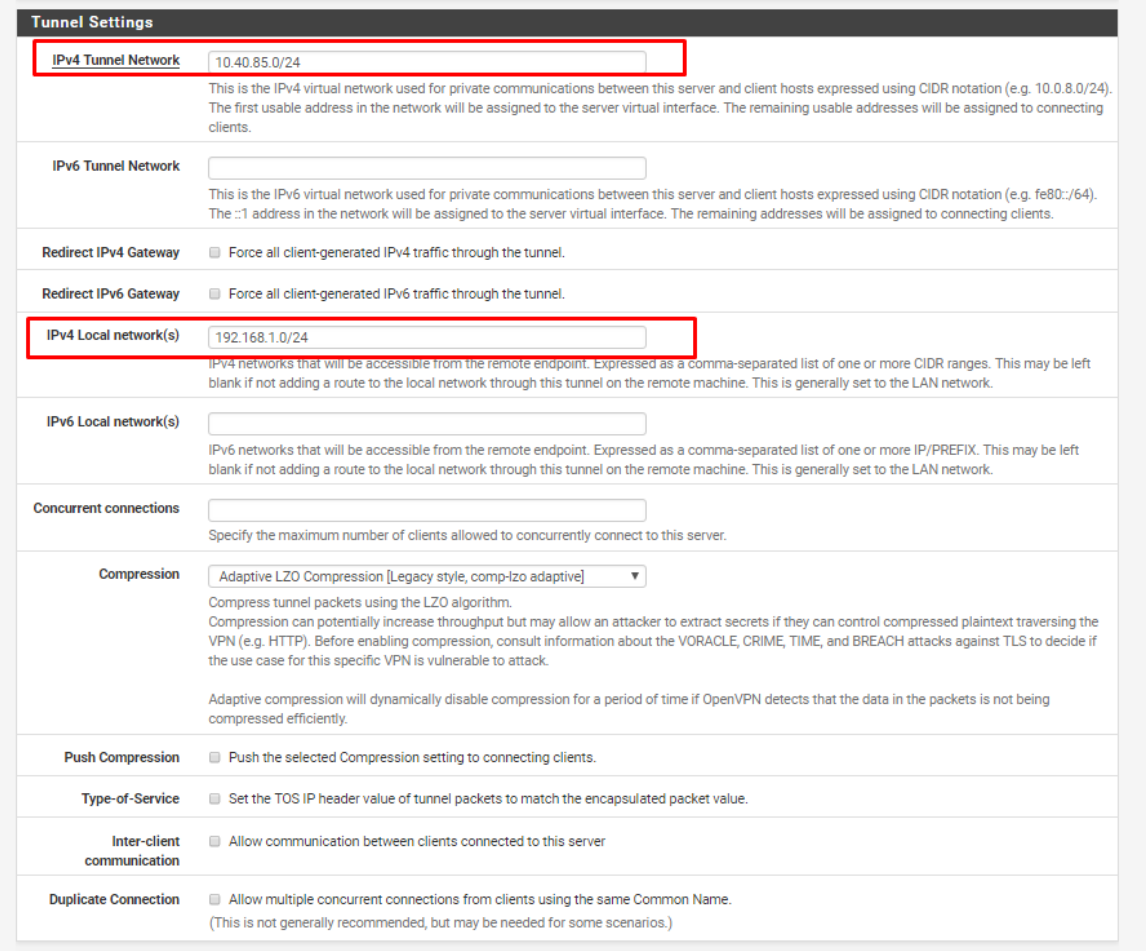

Ilustración 103: Panel de Configuración de Servidor VPN Parte 2.

En la opción Verbosity level seguiremos la sugerencia pfSense por lo que seleccionaremos el nivel 3, una vez realizados los cambios seleccionamos la opcion Save.

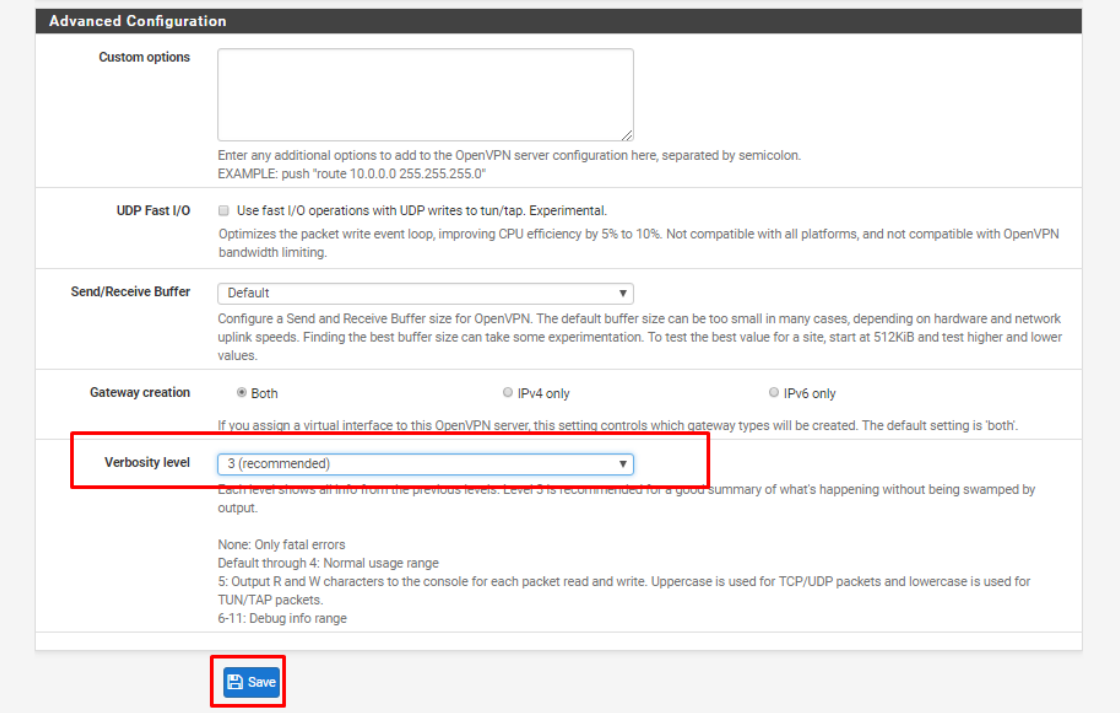

Ilustración 104: Panel de Configuración de Servidor VPN Parte 3.

10.- Creamos una regla en firewall que permita el tráfico de conexiones entrantes de protocolo UDP IPv4 a través de la red WAN a OpenVPN.

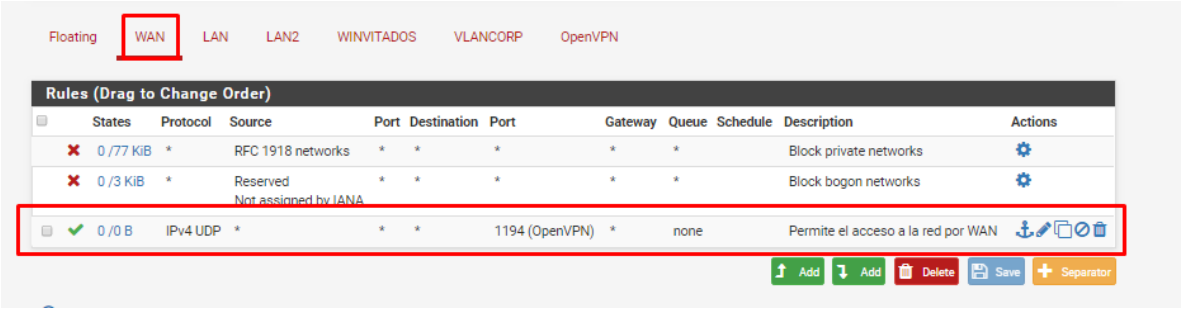

Ilustración 105: Reglas de Firewall (Regla para Tráfico de VPN).

11.- Creamos una regla de firewall en la interfaz OpenVPN que permita el tráfico entre las redes.

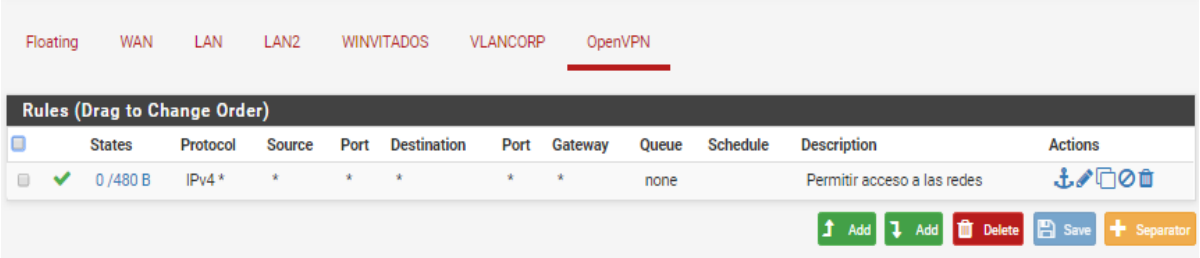

Ilustración 106: Reglas de Firewall de Interfaz OpenVPN.

12.- Es necesario algunos paquetes para poder descargar los certificados para ello nos dirigimos a la ruta System -> Package Manager.

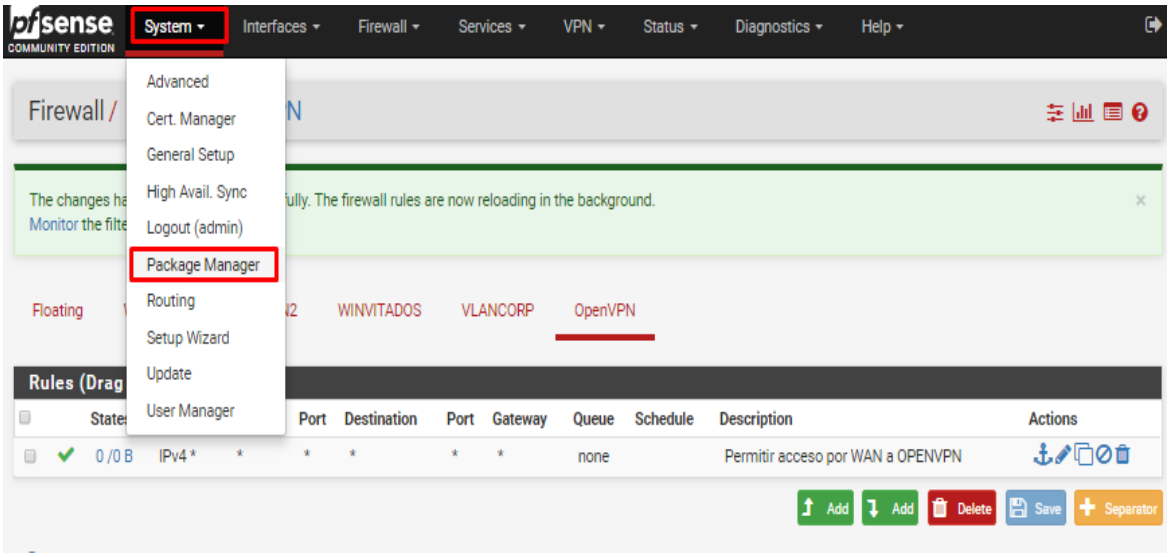

Ilustración 107: Ruta para la Gestión de Paquetes.

13.- Seleccionamos la opción Available Packages, y en Search Term buscamos OPENVPN e instalamos el paquete openvpn-client-export.

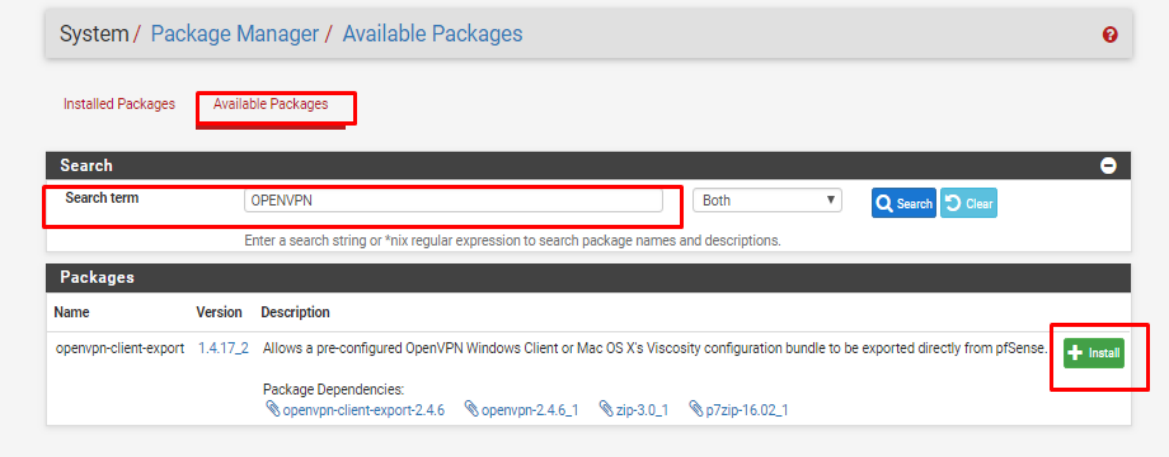

Ilustración 108: Búsqueda e Instalación de Paquete openvpn-client-export.

14.-Confirmamos la instalación del paquete.

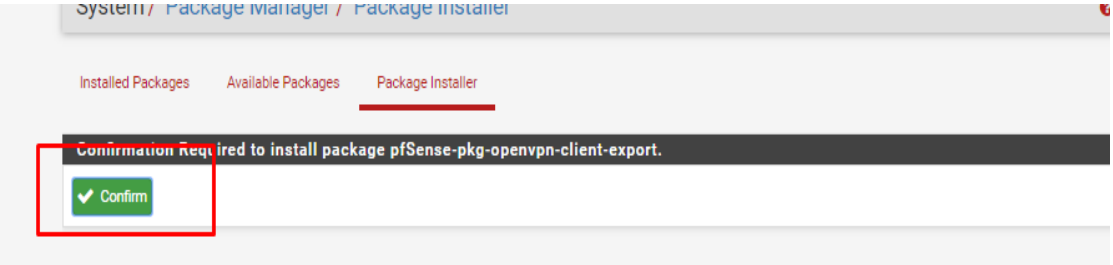

Ilustración 109: Confirmación de Instalación de Paquete.

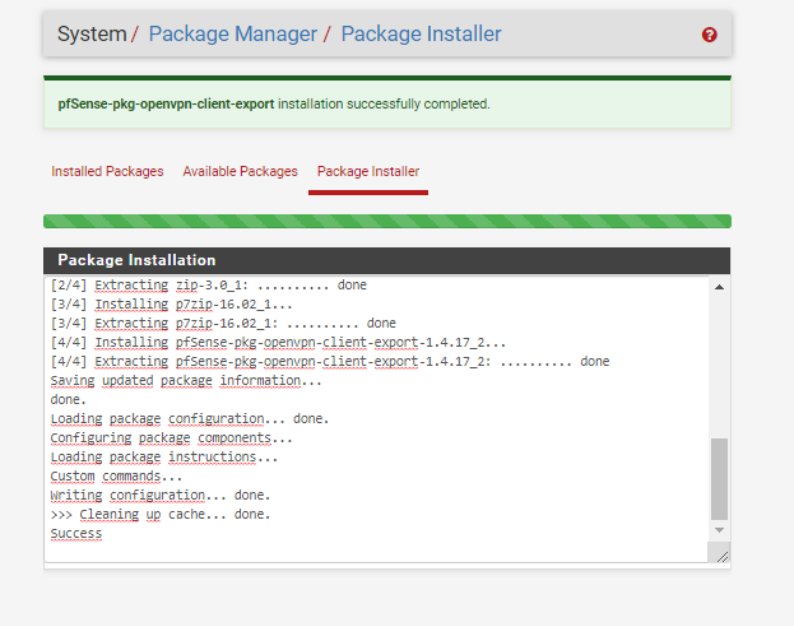

Ilustración 110: Proceso de Instalación de Paquete.

15.- Nos dirigimos a la ruta VPN-> OpenVPN y podremos observar que aparece la opción Client Export, seleccionamos esta opción.

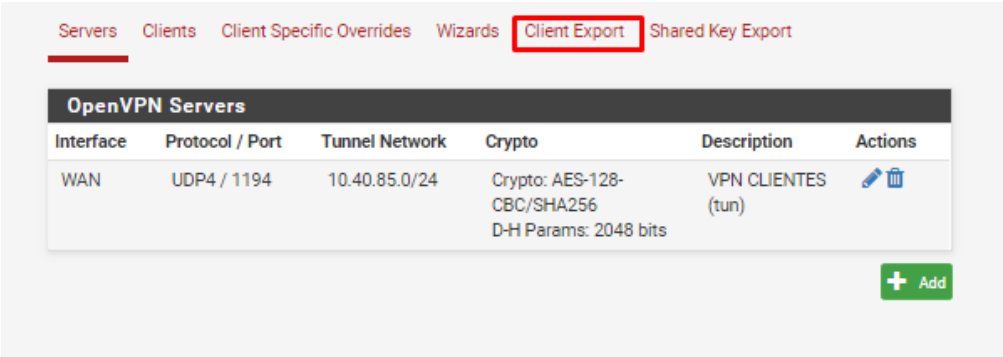

Ilustración 111: Vista de la Opción Creada después de la Instalación del Paquete openvpn.

16.- En esta opción se nos presentan los paquetes disponibles para descargar, para cada usuario que hayamos creado, lo primero que descargaremos será el instalador de OpenVPN, en nuestro caso la versión compatible con versiones superiores a Windows Vista.

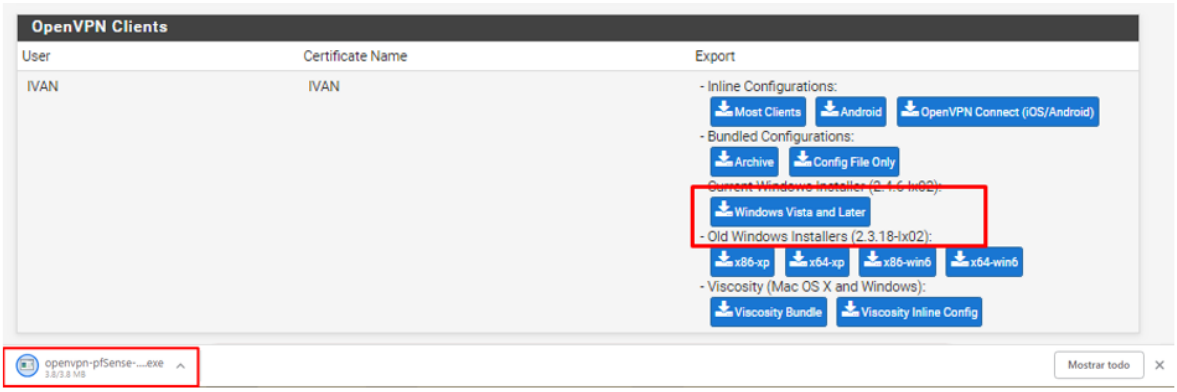

Ilustración 112: Paquetes de Descarga Disponibles para Cada Usuario (Descarga de Instalados OpenVPN).

17.- Descargamos los certificados para el usuario.

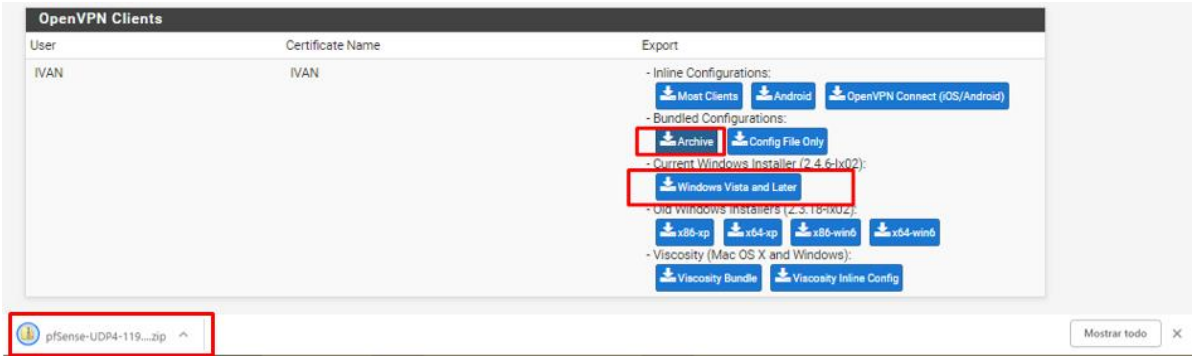

Ilustración 113Paquetes de Descarga Disponibles para Cada Usuario (Descarga de Certificados y Llaves para Usuario).

18.- Los paquetes que se han descargado son 1: Certificados y llave para la conexión, 2: Instalador de OpenVPN para Windows.

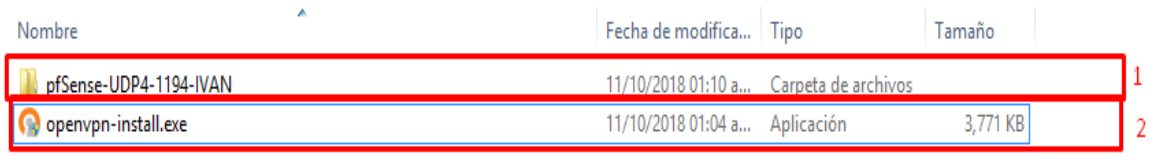

Ilustración 114: Archivos Descargados.

19.- Comenzamos la instalación del paquete OpenVPN, en la pestaña de bienvenida seleccionamos Next.

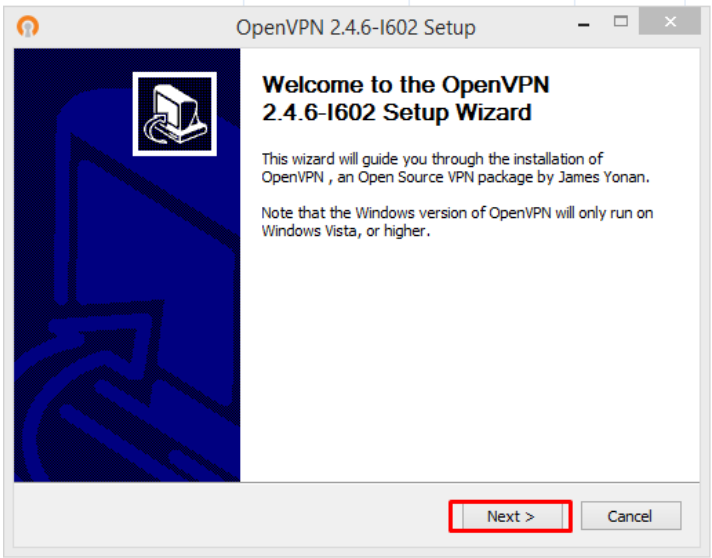

Ilustración 115: Ventana de Bienvenida para la Instalación de OPENVPN.

20.- Aceptamos los términos de uso.

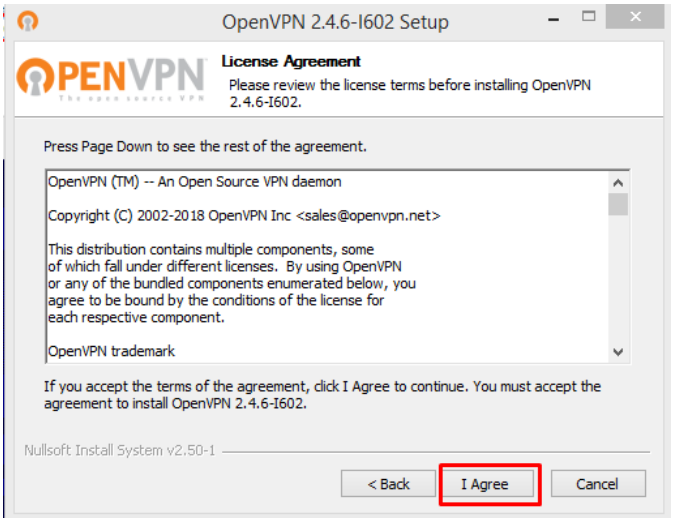

Ilustración 116: Términos de Licencia OPENVPN.

21.- Seleccionamos los paquetes a instalar de manera por defecto y presionamos Next.

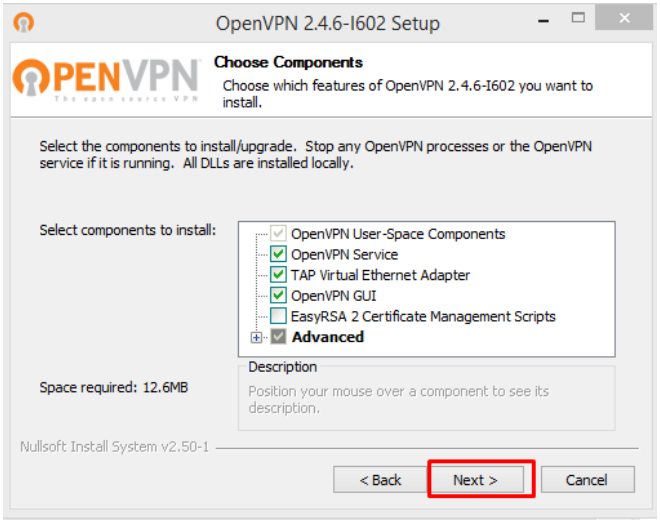

Ilustración 117: Selección de Componentes a Instalar en OPENVPN.

22.- Seleccionamos Install, para instalar los paquetes seleccionados y esperamos a que finalice el proceso.

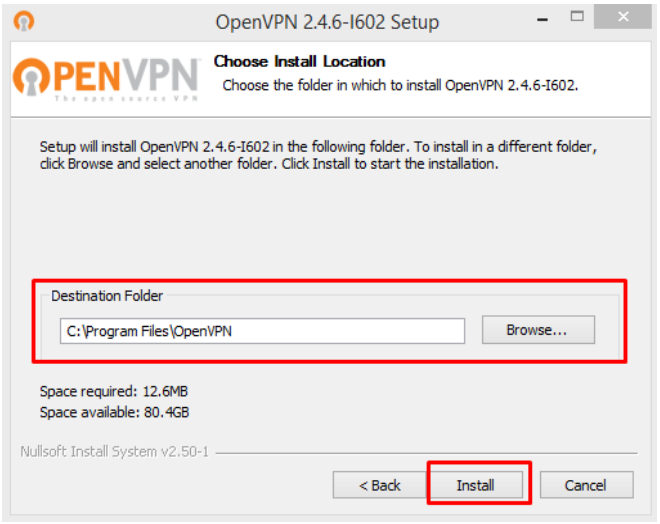

Ilustración 118: Ruta de Instalación de OPENVPN.

23.-Copiamos los certificados descargados, estos se encuentran en la carpeta descargada del pfSense.

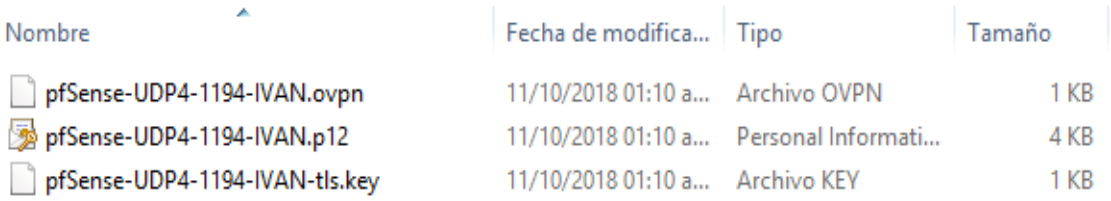

Ilustración 119: Certificados en Carpeta de Descargas.

24.-Pegamos los certificados en la carpeta de configuracion de OpenVPN, la ruta es C->Archivos de programa -> OpenVPN -> config.

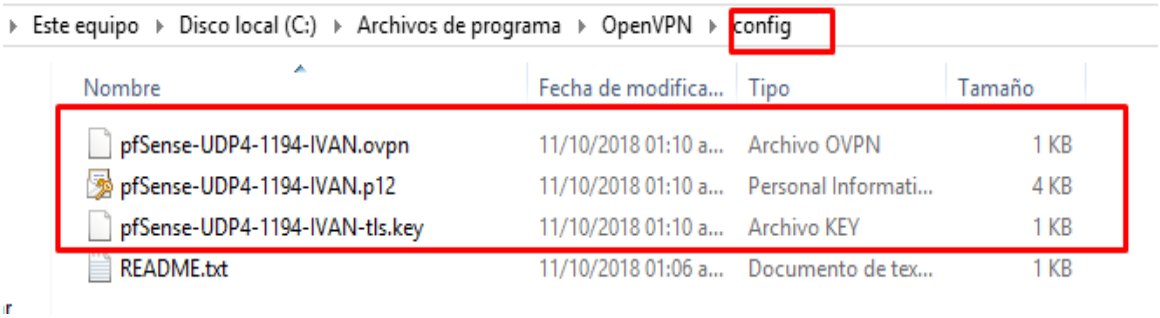

Ilustración 120: Inserción de Certificados en Ruta Config de OPENVPN.

25.- Como podemos observar nos encontramos en una red fuera del perímetro de nuestra red pfSense y no contamos con acceso a la red 192.168.1.1

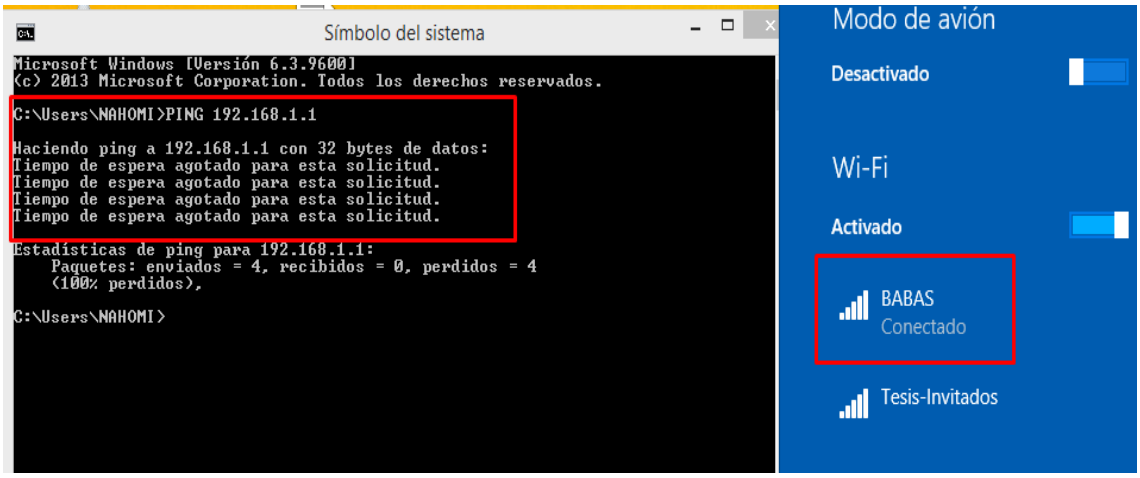

Ilustración 121: Conexión de Red Externa sin Comunicación a Red 192.168.1.1.

26.- Ejecutamos el Programa instalado OpenVPN GUI, de no ejecutarse como administrador es posible que no se permita la comunicación aunque se establezca la conexión.

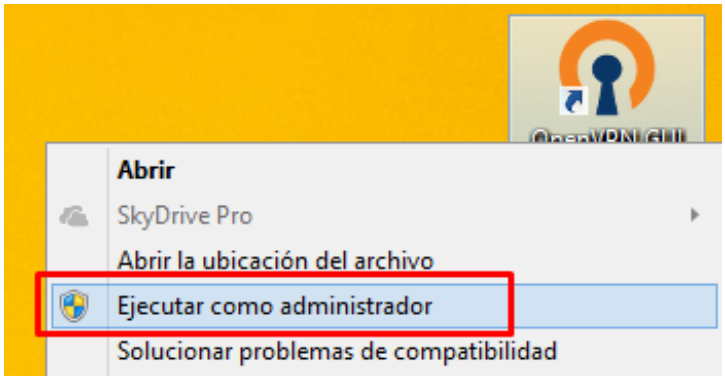

Ilustración 122: Ejecución de OPENVPN como Administrador.

27.- Se nos pedirá ingresar el usuario y contraseña que definimos en pfSense.

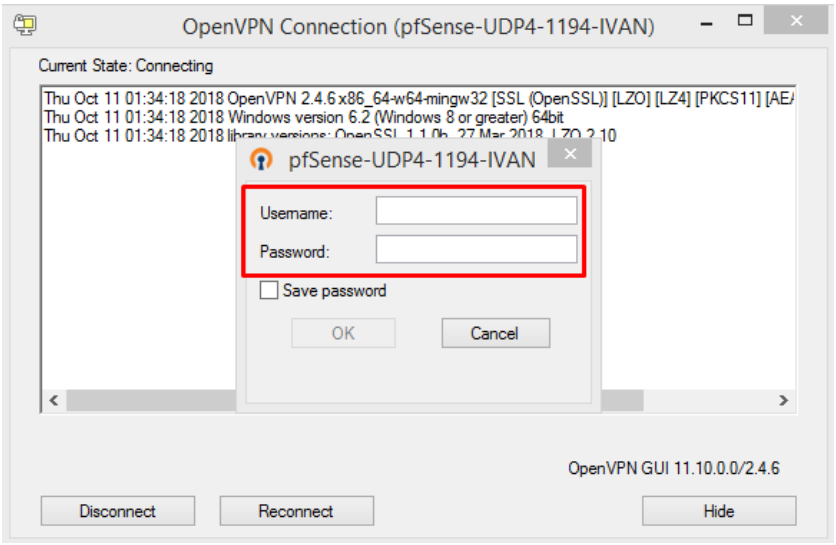

Ilustración 123: Panel de Autenticación de OPENVPN.

28.- Una vez superado el proceso de autenticación veremos que la conexión se ha establecido y tenemos acceso a la red 192.168.1.1

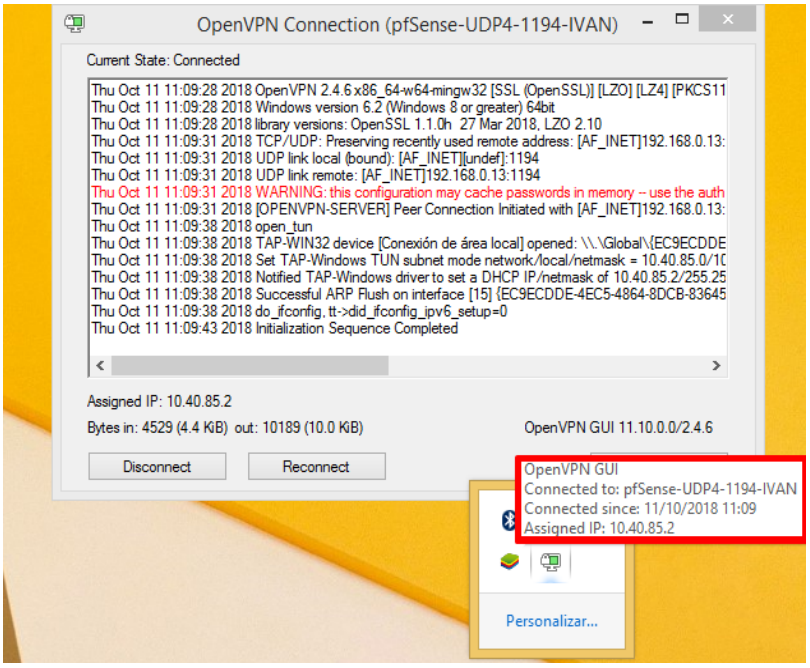

Ilustración 124: Conexión de OPENVPN Establecida.

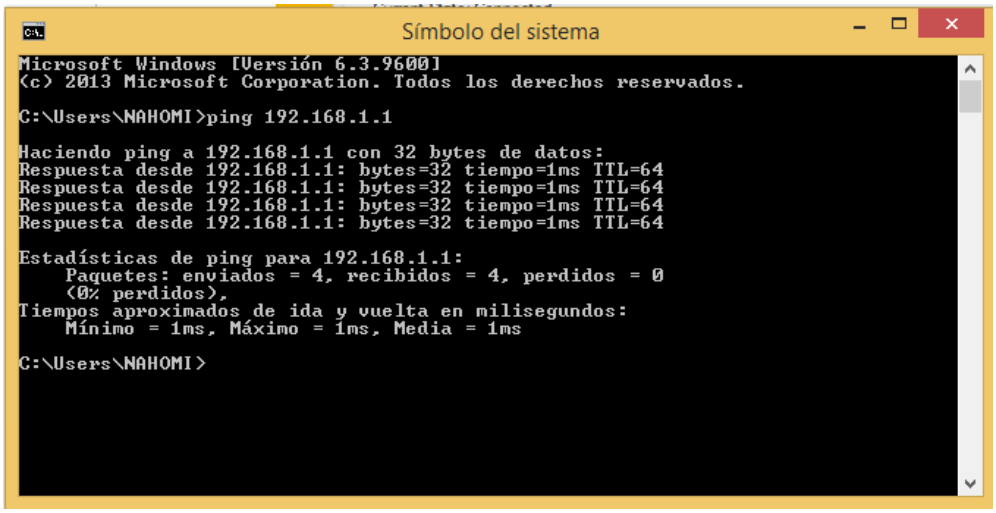

Ilustración 125: Comunicación de Red Externa con Red 192.168.1.1.

3.8 Preparación, Instalación y configuración de monitoreo usando Zabbix

La herramienta Zabbix será usada para el monitoreo de recursos informáticos, su ubicación en la red será definida por el diagrama, ver Ilustración 18, se define su IP: 192.168.1.2.

3.8.1 Herramientas Hardware y Software

Características de PC en el que se instalara el Servidor Zabbix.

- Disco duro: 20 GB
- Memoria RAM: 1GB
- CPU: Arquitectura x64 con 2 CPU

Herramientas necesarias.

- USB 8 GB

Herramientas Software necesarias.

- ISO de instalación Zabbix
- LinuxLive USB Creator, esta herramienta se usara para crear un USB de arranque con el sistema Zabbix

3.8.2 Instalación de Servidor Zabbix

1.- Es posible descargar diferentes versiones del servidor Zabbix, desde el código para personalizar nuestra propia compilación hasta un paquete listo para instalar y funcionar, para nuestro caso usaremos una versión lista para instalar con extensión .iso en específico la versión 3.4.

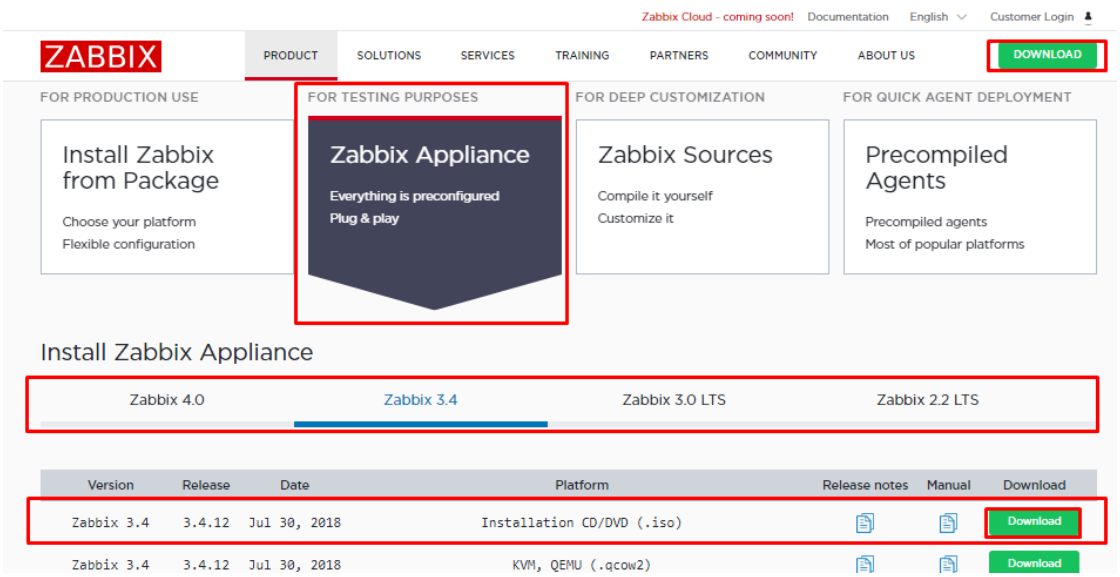

Ilustración 126: Selección de Descarga ISO Zabbix.

2.- Descargamos el programa LinuxLive USB Creator este programa nos ayudara a la creación de un dispositivo USB de arranque con el sistema Zabbix.

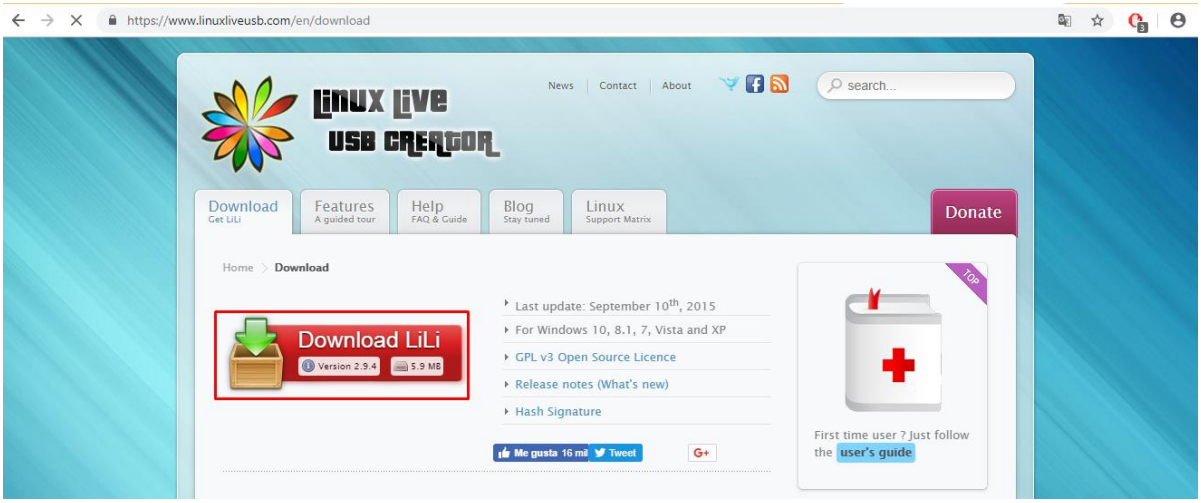

Ilustración 127: Selección de Descarga Linux Live USB Creator.

3.-Verificamos los archivos descargados.

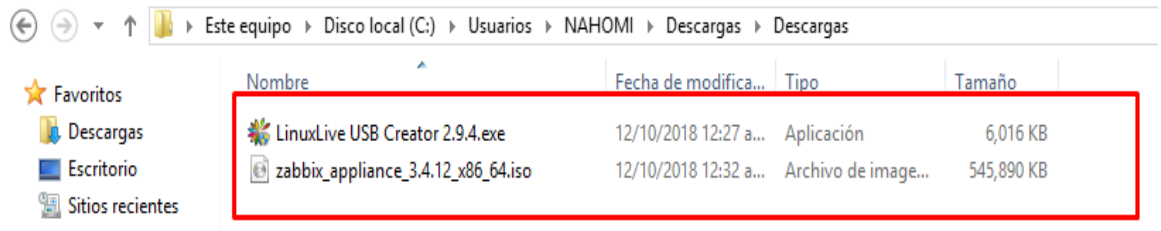

Ilustración 128: Validación de Descargas Zabbix y Linux Live USB Creator.

4.- Instalamos el programa LinuxLive USB Creator haciendo doble clic sobre él, y seleccionamos siguiente en la ventana de Bienvenida a la instalación.

Ilustración 129: Ventana de Inicio de Instalación Linux Live USB Creator.

5.- Verificamos la ruta de instalación y seleccionamos instalar.

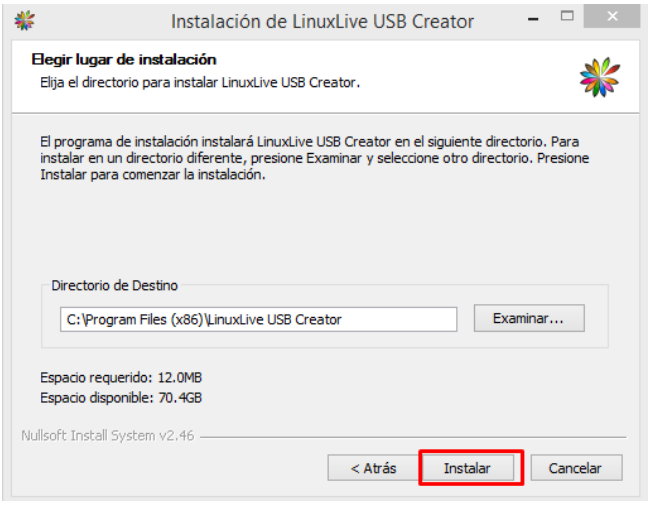

Ilustración 130: Selección de Ruta de Instalación para Linux Live USB Creator.

6.- Esperamos a que finalice la instalación y seleccionamos finalizar, se recomienda mantener seleccionada la opción Ejecutar LinuxLive USB Creator para confirmar que se ejecuta el programa.

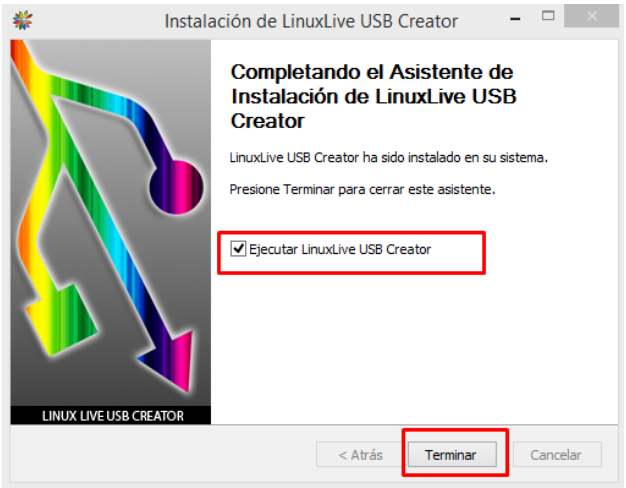

Ilustración 131: Fin del Proceso de Instalación de Linux Live USB Creator.

7.-En el programa LinuxLive USB Creator se nos presentan las opciones para crear el dispositivo de arranque USB, como se nos muestra en el Paso uno: Seleccionamos el dispositivo donde se grabara el ISO, Paso dos: Seleccionamos el Iso desde la ruta donde lo hemos descargado, Paso tres: No aplica, Paso cuatro: Seleccionamos todas las opciones por último seleccionamos el logo de Rayo para iniciar la instalación y esperamos a que finalice.

Ilustración 132: Creación de USB de Arranque Zabbix.

8.- Colocamos el USB de arranque en el dispositivo donde se instalará el sistema, al arrancar se nos presentan las opciones de instalación, seleccionamos "Install Ubuntu Server with Zabbix Server (MySQL)" para iniciar la instalación.

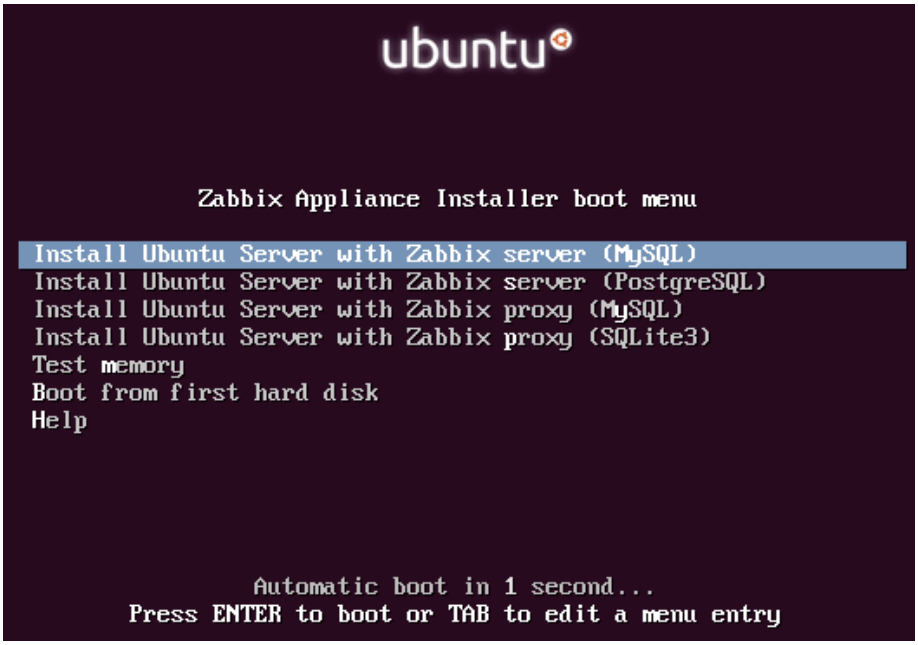

Ilustración 133: Inicio de Instalación Zabbix.

9.- Una vez iniciada la instalación esperamos a que finalice.

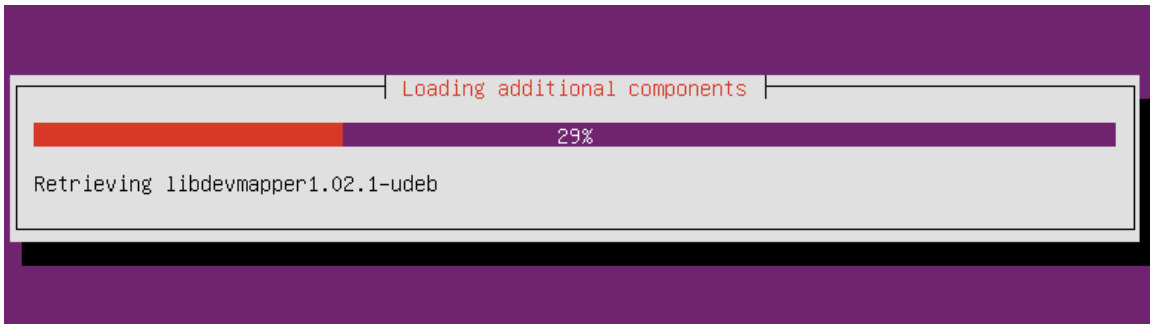

Ilustración 134: Progreso de Instalación Zabbix.

3.8.3 Configuración Zabbix

Por defecto tendremos que el usuario y contraseña son:

- Acceso root desde el servidor

  Usuario: appliance

  Contraseña: zabbix

- Acceso desde el portal Web

  Usuario: Admin

  Contraseña: Zabbix

  Configuración Servidor

3.8.3.1 Configuración de Red en el Servidor Zabbix

1.- Ingresamos al servidor y verificamos la configuración de la dirección IP con el comando ifconfig, por defecto el servidor está configurado en modo DHCP por lo que será necesario colocar una configuración estática.

```
appliance@zabbix:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:48:09:35
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe48:935/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:133 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15308 (15.3 KB)  TX bytes:1744 (1.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:740 errors:0 dropped:0 overruns:0 frame:0
          TX packets:740 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:47562 (47.5 KB)  TX bytes:47562 (47.5 KB)
```

Ilustración 135: Información de Interfaz de Red Zabbix, (Dirección por DHCP).

2.-Para modificar la configuración de DHCO a estática tendremos que modificar el archivo de configuración "interfaces", para ello iremos a la ruta /etc/network.

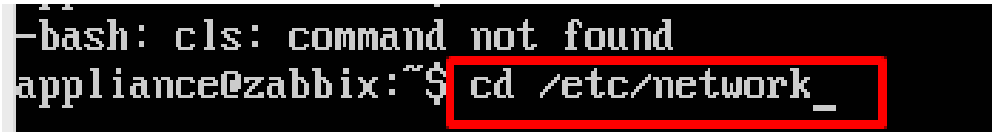

Ilustración 136: Ruta al Archivo de Configuración de Interfaz de Red.

3.- Abrimos el archivo de configuración como súper usuario para modificarlo, en nuestro caso usamos el comando sudo vi interfaces.

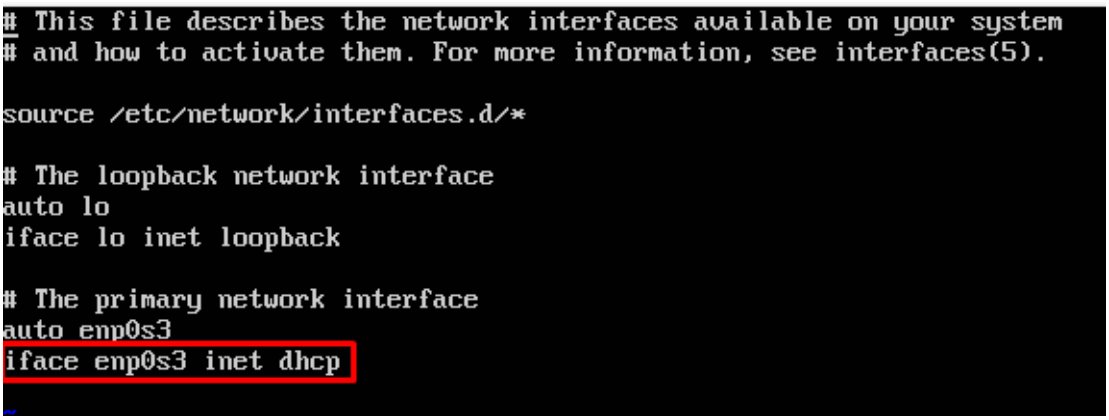

Ilustración 137: Archivo de Configuración de Interfaz de Red, (Configuración Definida como DHCP).

4.- Modificamos el archivo, antes que nada modificamos modo dhcp por static y agregamos los valores de la red, la IP del servidor será: 192.168.1.2, la máscara: 255.255.255.0, la puerta de enlace 192.168.1.1, la red: 192.168.1.0 y broadcast: 192.168.1.254

```
# 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 192.168.1.2
netmask 255.255.255.0
gateway 192.168.1.1
network 192.168.1.0
broadcast 192.168.1.254
```

Ilustración 138: Modificación de Archivo de Configuración de Interfaz de Red, (Modificación a Valores Estáticos).

5.-Validamos que la configuración se haya aplicado, en ocasiones es necesario reiniciar el servidor para aplicar los cambios.

```
Last login: Thu Oct 11 22:41:20 UTC 2018 on tty1
appliance@zabbix:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:48:09:35
          inet addr:192.168.1.2  Bcast:192.168.1.254  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe48:935/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:494 (494.0 B)  TX bytes:672 (672.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:164 errors:0 dropped:0 overruns:0 frame:0
          TX packets:164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:12040 (12.0 KB)  TX bytes:12040 (12.0 KB)
```

Ilustración 139: Información de Interfaz de Red Zabbix, (Dirección Estática).

3.8.3.2 Configuración de Agente Zabbix en equipos a Monitorear

1.- Antes de iniciar con la configuración de los Host es necesario preparar los equipos con su respectivo agente de monitoreo, en el caso de los equipos Windows podemos descargar agentes recompilados listos para ejecutar, seleccionamos la versión de nuestro servidor Zabbix y la arquitectura del equipo donde se instalará el agente

Ilustración 140: Elección de Agente de Monitoreo Pre Compilado para Windows.

2.-Ejecutamos el agente descargado, en la pantalla de bienvenida para la instalación seleccionamos Next.

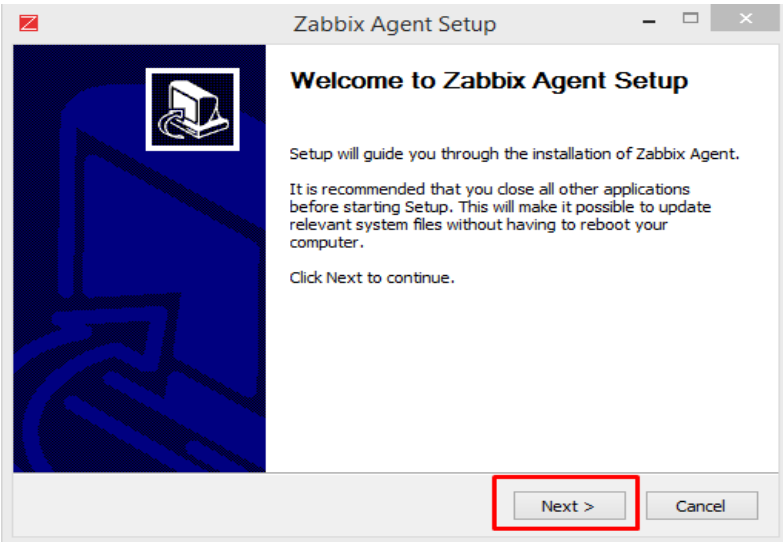

Ilustración 141: Inicio de Instalación de Agente Pre Compilado para Windows.

3.-Aceptamos los términos de Licencia

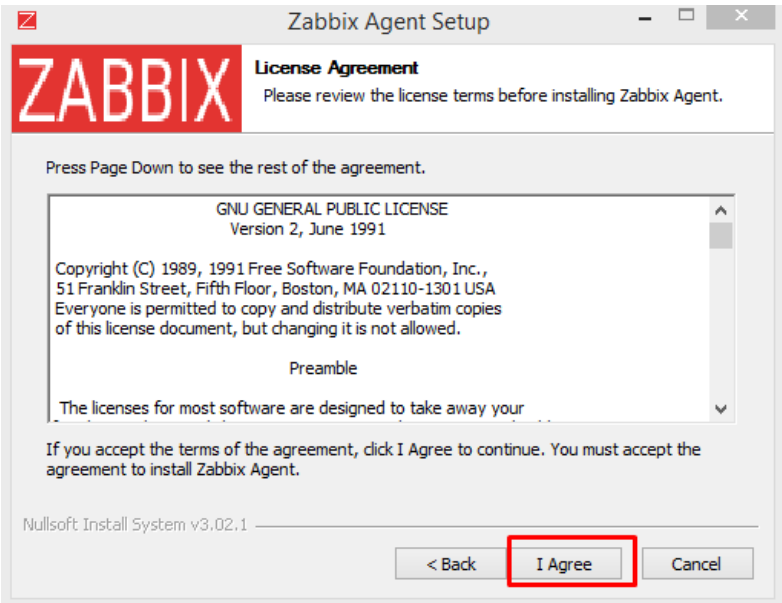

Ilustración 142: Términos de Licencia para Agente Pre Compilado para Windows.

4.-Seleccionamos los componentes a instalar, para nuestro caso dejamos las opciones por defecto. Seleccionamos la opción Next para continuar.

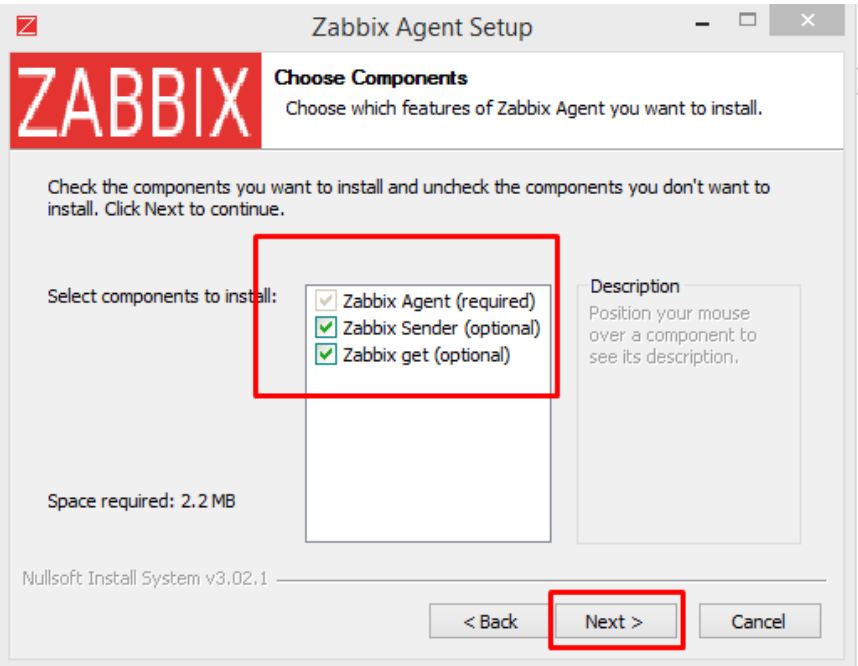

Ilustración 143: Elección de Componentes para Agente Zabbix en Windows

5.-Agregamos el nombre o IP del servidor Zabbix, el nombre del Host a monitorear, dejamos el puerto 10050 por defecto y como Servidor activo el servidor Zabbix. Seleccionamos la opción Next y esperamos a que termine la instalación.

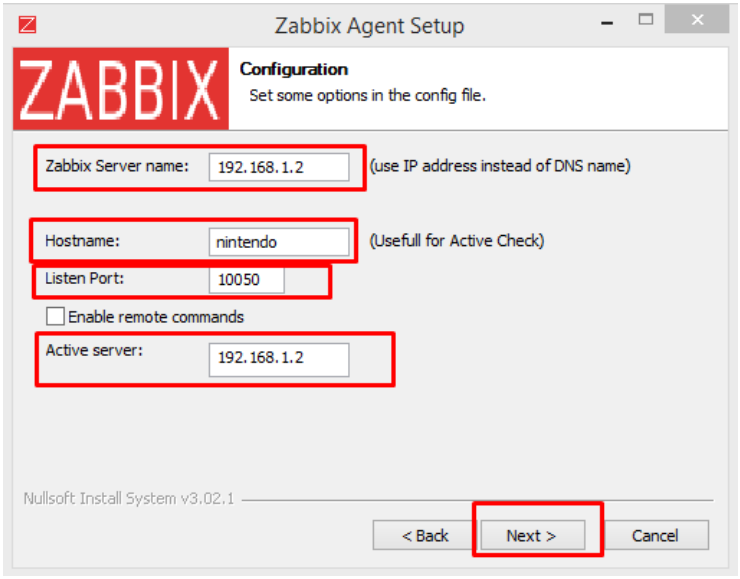

Ilustración 144: Configuración de Agente Zabbix en Windows.

6.- Una vez finalizada la instalación verificamos que el servicio de monitoreo se encuentra activo, en los servicios de Windows.

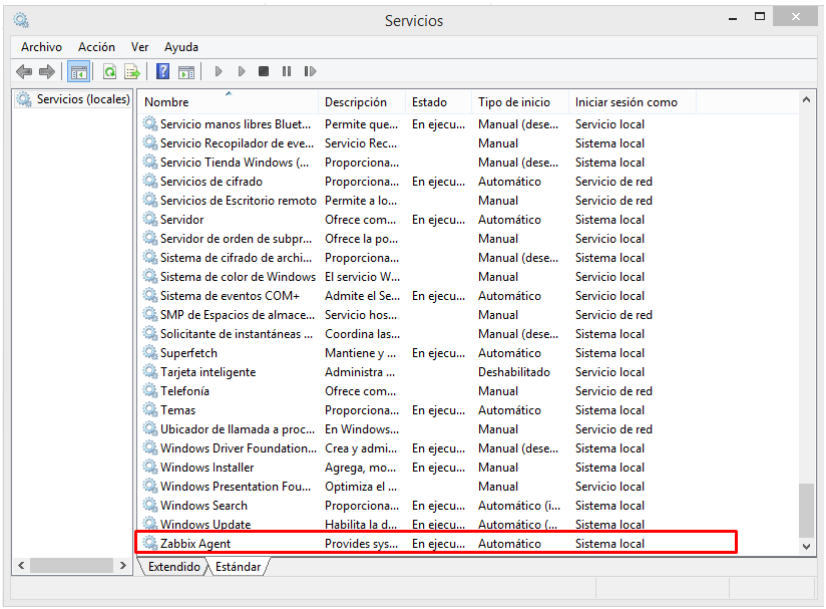

Ilustración 145: Validación de Servicio Activo, (Agente Zabbix).

7.- Para poder monitorear nuestro servidor pfSense es necesario agregar el paquete agente Zabbix, desde el menú de administración de paquetes.

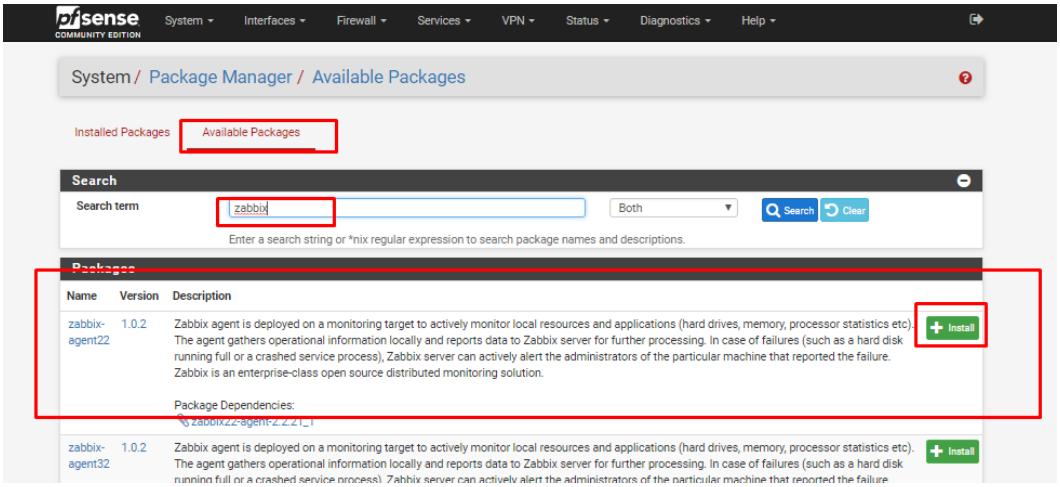

Ilustración 146: Descarga de Agente Zabbix en PfSense.

8.- Una vez instalado el paquete se crea un nuevo servicio en la ruta Service-> Zabbix Agent 3.0

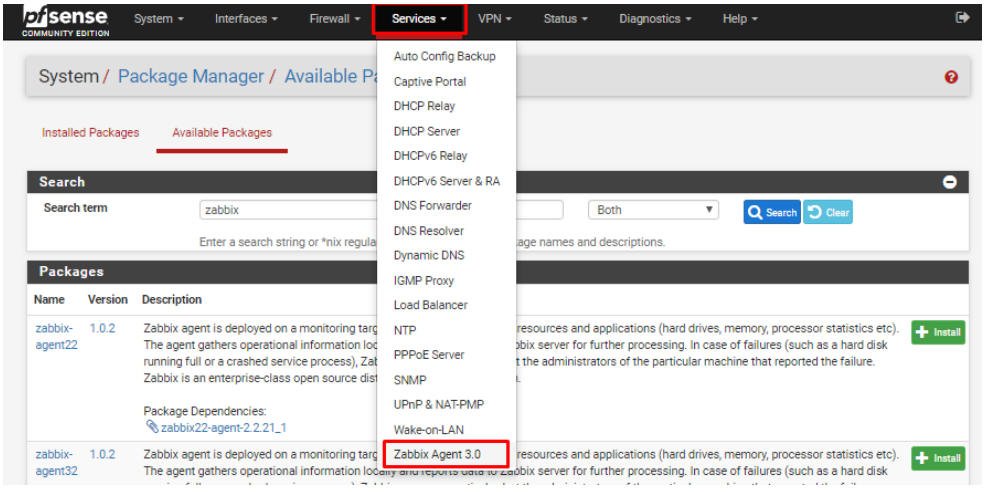

Ilustración 147: Ruta para la Configuración de Agente Zabbix en PfSense

9.-En el panel de configuración del Agente Zabbix, habilitaremos el agente, en la opción Server colocaremos la IP o nombre del servidor Zabbix, como servidor activo la IP del servidor, Hostname, colocamos el nombre del Host a monitorear (pfsense), en la opción Listen IP colocamos las direcciones a monitorear si se deja con los valores por default (0.0.0.0) se monitorearan todas la interfaces del Servidor pfSense, el puerto por defecto es 10050.

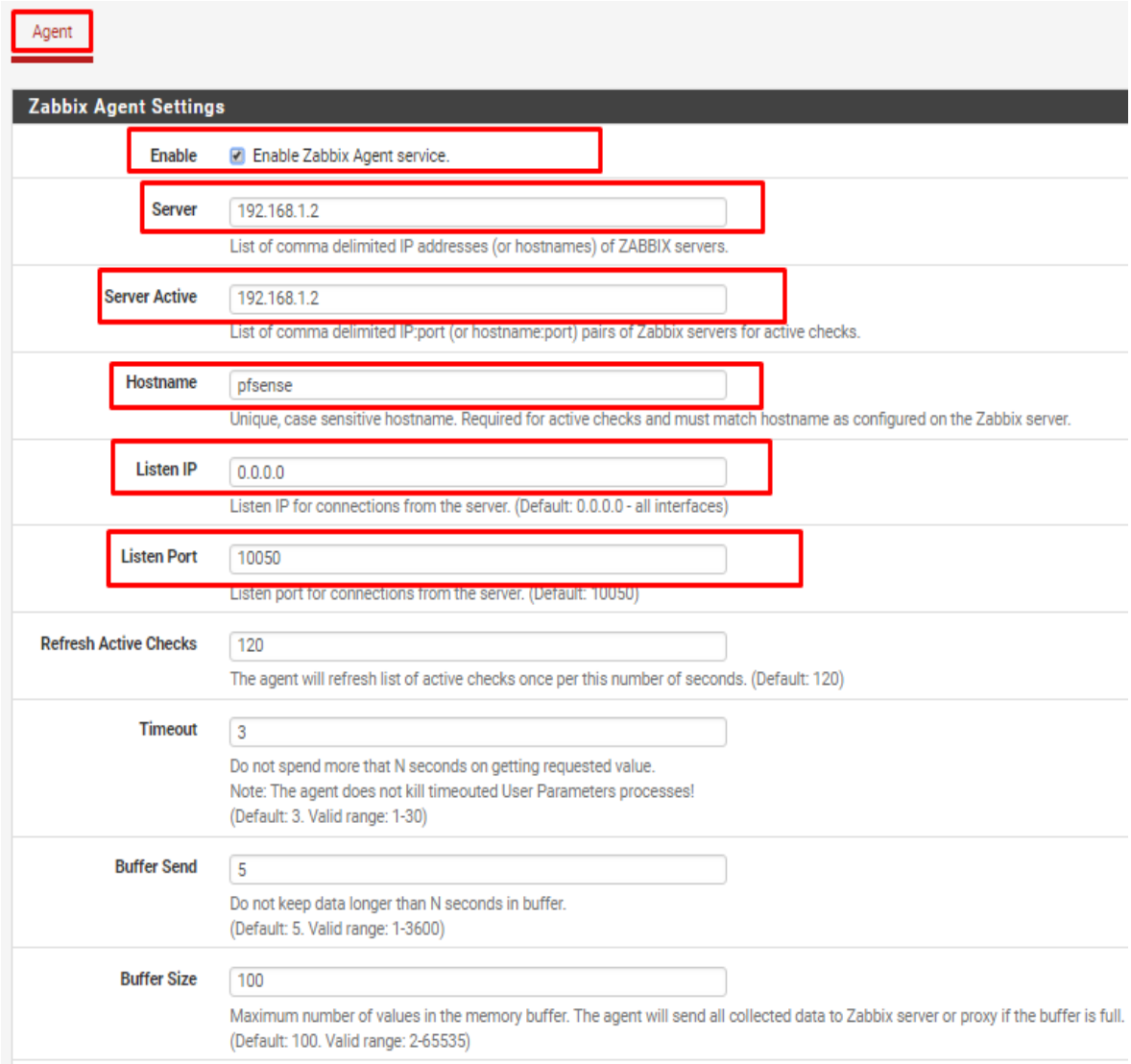

Ilustración 148: Panel de Configuración Agente Zabbix en PfSense, (Parte 1).

Realizados los cambios seleccionamos la opción Save, el agente configurado, comenzará a enviar información de su estado al servidor Zabbix.

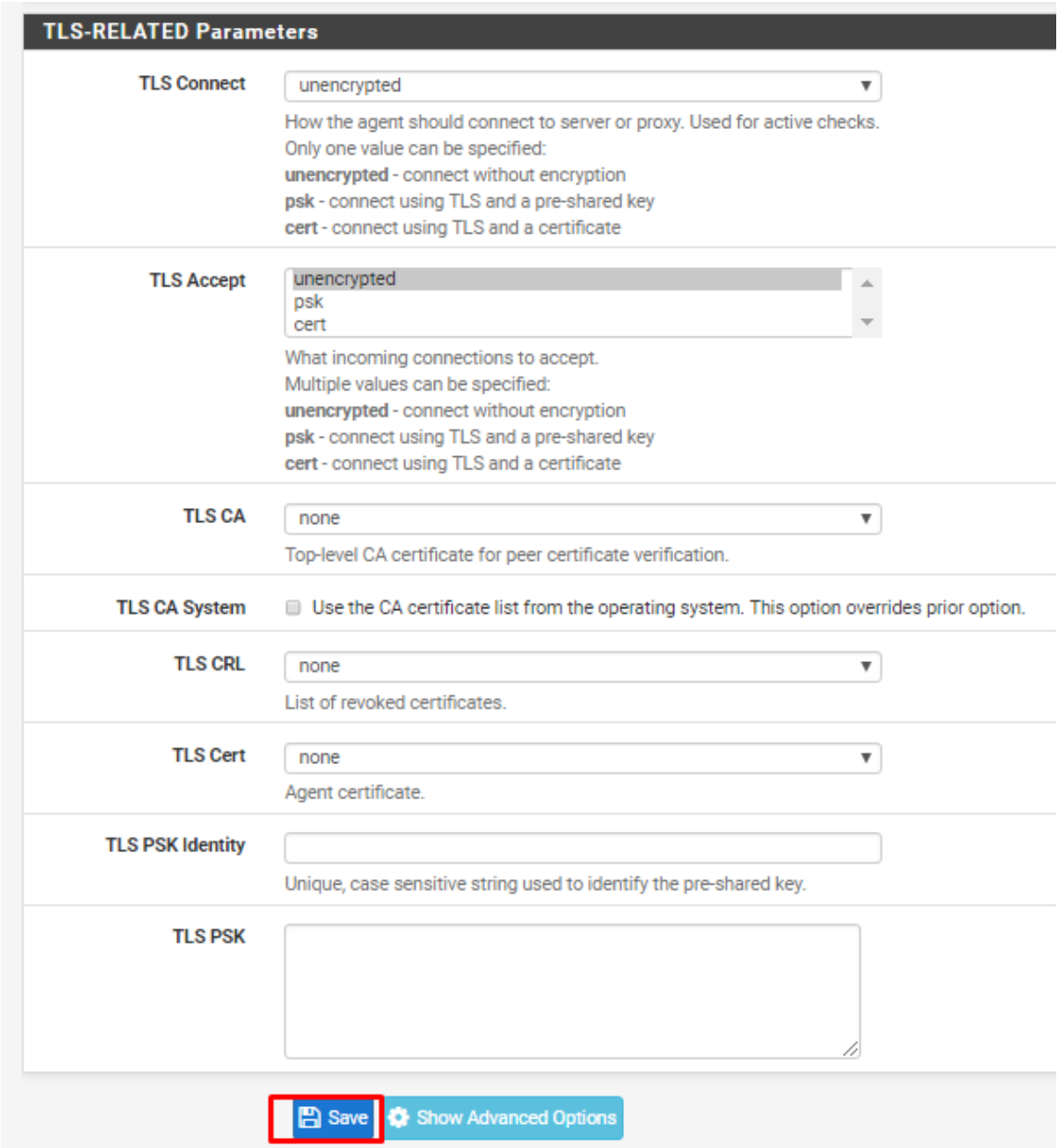

Ilustración 149: Panel de Configuración Agente Zabbix en PfSense, (Parte 2).

3.8.3.3 Configuración de Host en Servidor Zabbix

1.- Ingresamos al portal de administración del servidor Zabbix ingresando a la dirección IP-server/Zabbix/, para nuestro caso 192.168.1.2/Zabbix/ e ingresamos con nuestras credenciales.

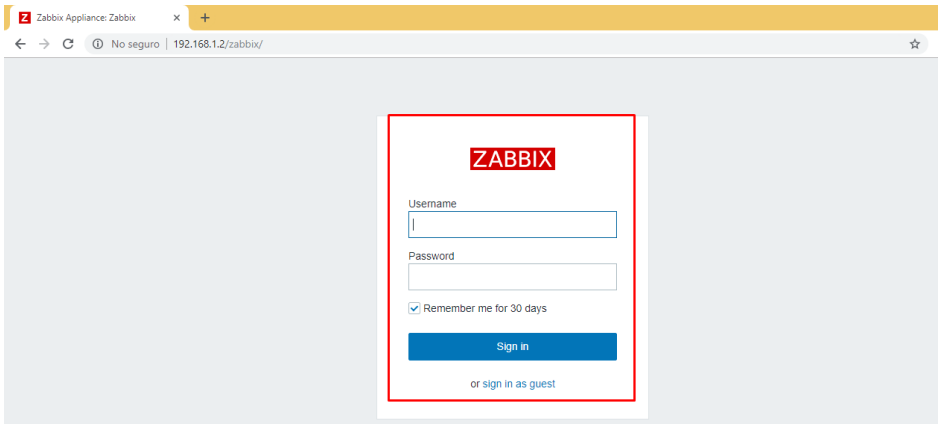

Ilustración 150: Inicio de Sesión Zabbix, Portal Web.

2.-Una vez iniciada la sesión se nos presenta un tablero con información general del estado del servidor Zabbix.

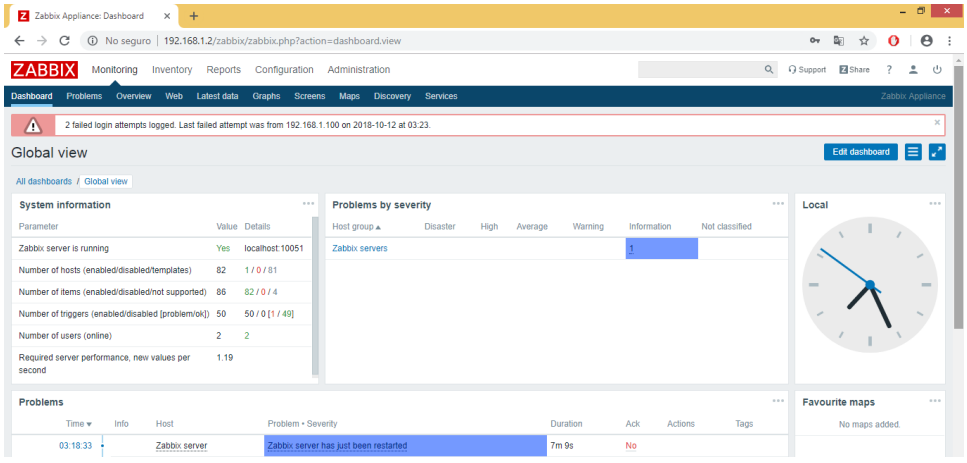

Ilustración 151: Tablero principal Zabbix.

3.- Para agregar un nuevo host en el servidor Zabbix nos dirigimos a la ruta Configuration -> Host, seleccionamos la opción Create host. Este proceso se realiza para el alta de un nuevo host.

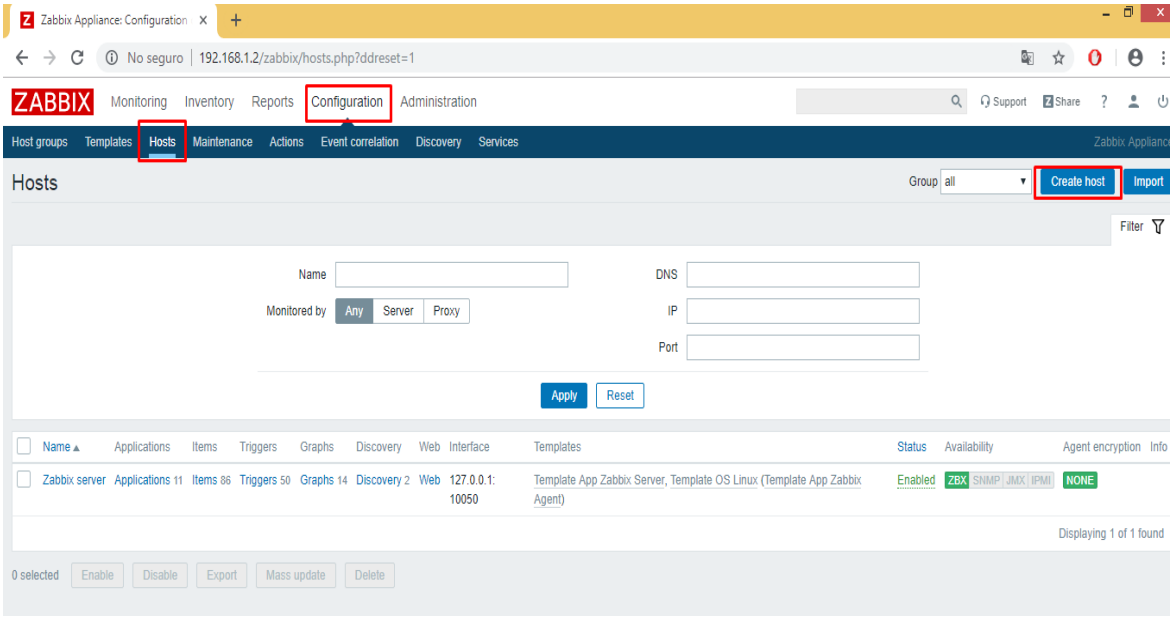

Ilustración 152: Ruta para Crear un Nuevo Host.

3.- En el panel de configuración del host es necesario colocar el Host name: Tal cual se asignó en el agente del equipo, Visible name: Nuevamente colocamos el nombre del host, Groups: elegimos en la opción Select a que grupo pertenecerá el host, Agent interfaces: Colocamos la IP del Host. Seleccionamos la opción Add para guardar los cambios.

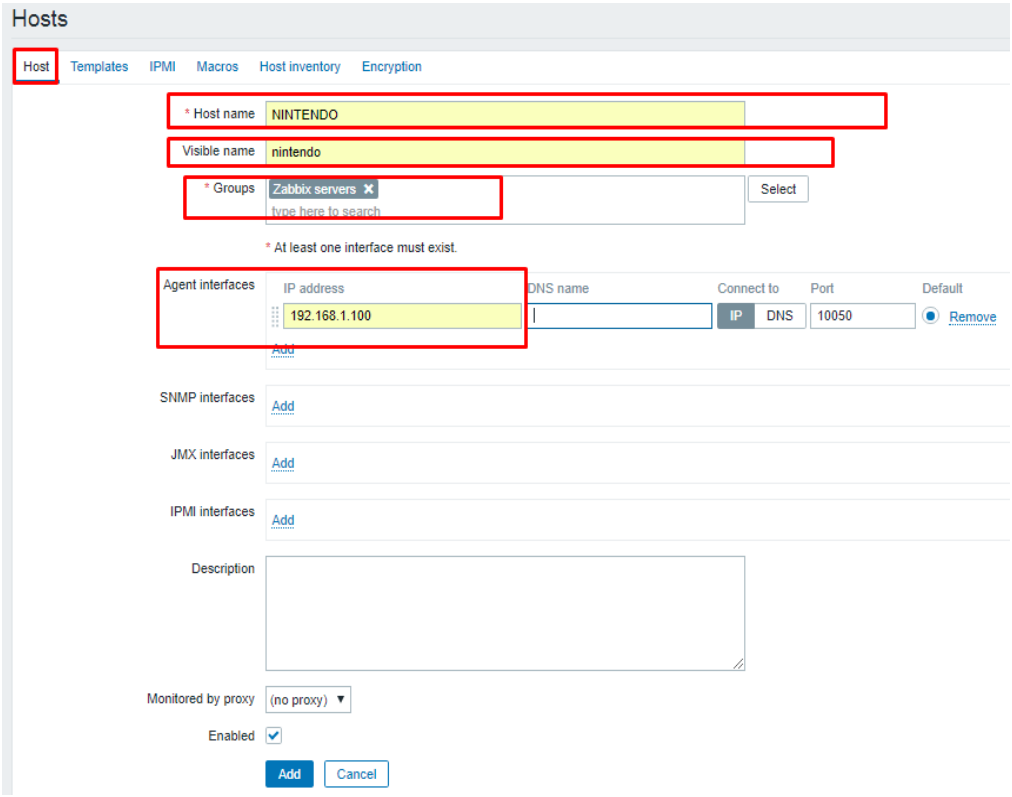

Ilustración 153: Panel de Configuración de Host.

4.- En la opción Templates podremos agregar plantillas de monitoreo predeterminadas para cada sistema operativo, seleccionaremos la opción Select para desplegar las opciones.

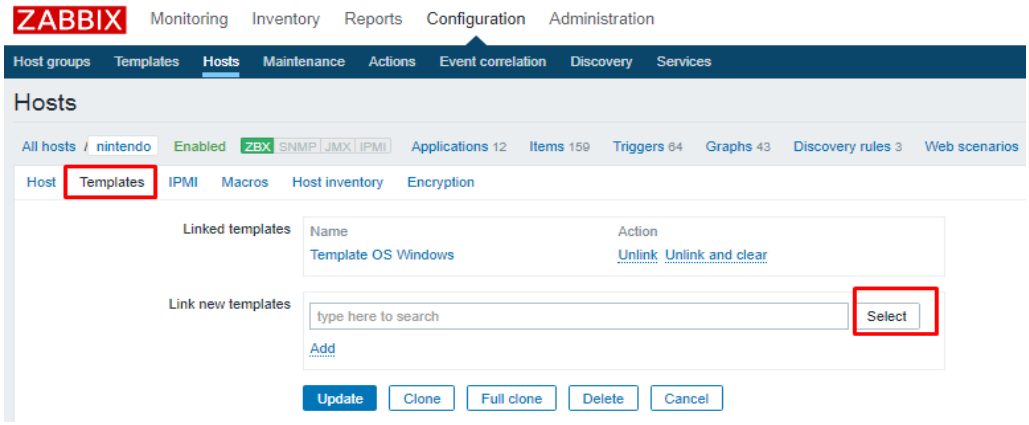

Ilustración 154: Plantillas de Monitoreo para Host

5.-Para este Host al tratarse de un Sistema Operativo Windows seleccionamos la opcion Template OS Windows, seleccionamos la opcion Select para continuar, Add para agregar la plantiya y Update para guardar los cambios realizados.

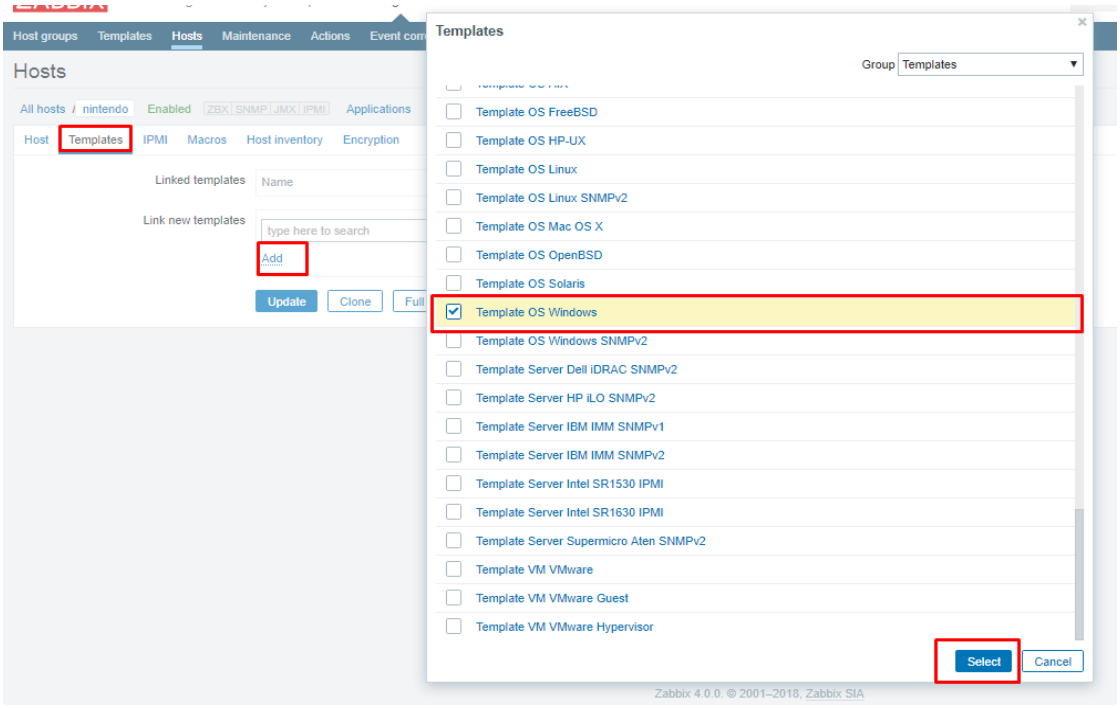

Ilustración 155: Selección de Plantilla de Monitoreo para Host.

6.- En la opción All host podremos observar los Host agregados y la configuración definida para ellos.

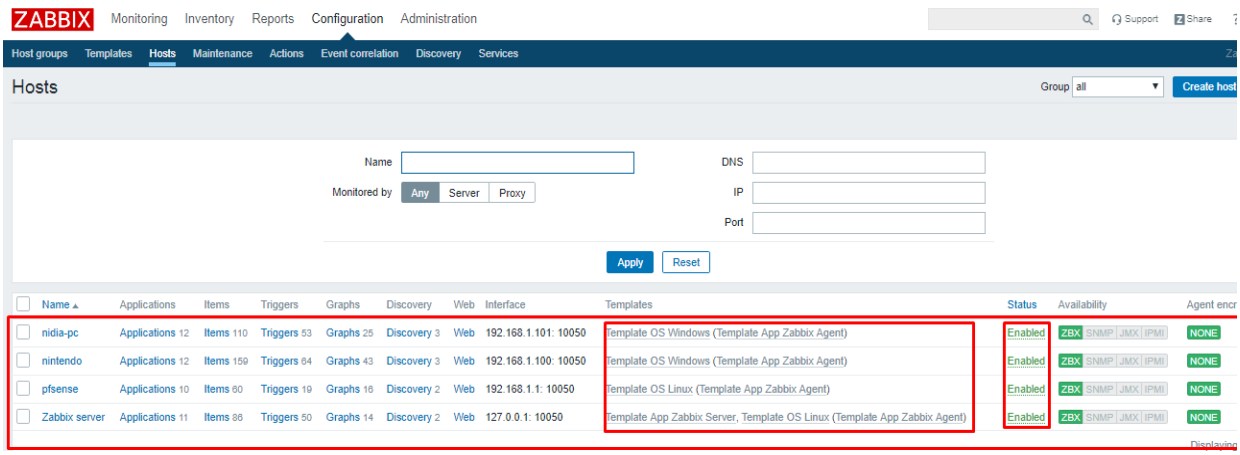

Ilustración 156: Lista de Host en el Servidor.

7.-Es posible ver gráficas a partir de las plantillas de monitoreo predeterminadas, nos dirigimos a la ruta Monitoring -> Graphs, podremos observar algunas opciones para filtrar específicamente la gráfica que deseamos observar, en la Ilustración 157 se muestra el comportamiento de memoria RAM del host nintendo.

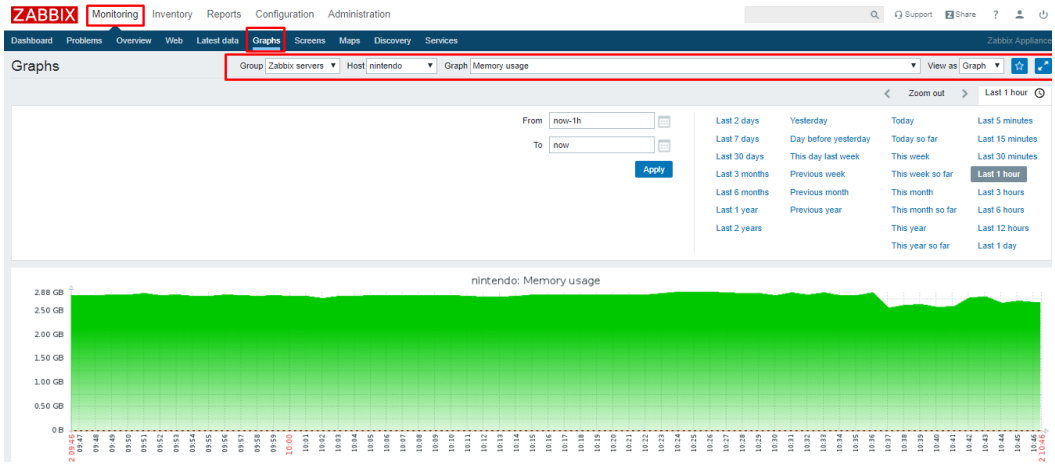

Ilustración 157: Gráfica de Monitoreo Host nintendo.

3.8.3.4 Gráficas y Mapas

Gráficas

1.- Para crear la vista de gráficas en la página principal de Zabbix nos dirigimos a la ruta Monitoring -> Dashboard, en este lugar seleccionaremos la opción Edit dashboard.

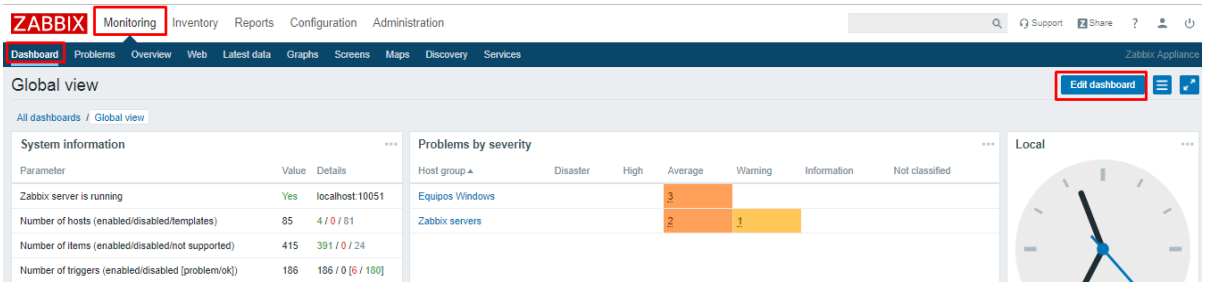

Ilustración 158: Ruta para la Personalización de Tablero Zabbix.

2.-Como se observa en la ilustración… Se habilitan opciones para eliminar o mover las vistas de manera independiente (eliminaremos todas las vistas para tener un tablero en blanco), para agregar nuevas gráficas seleccionamos la opción +Add widget.

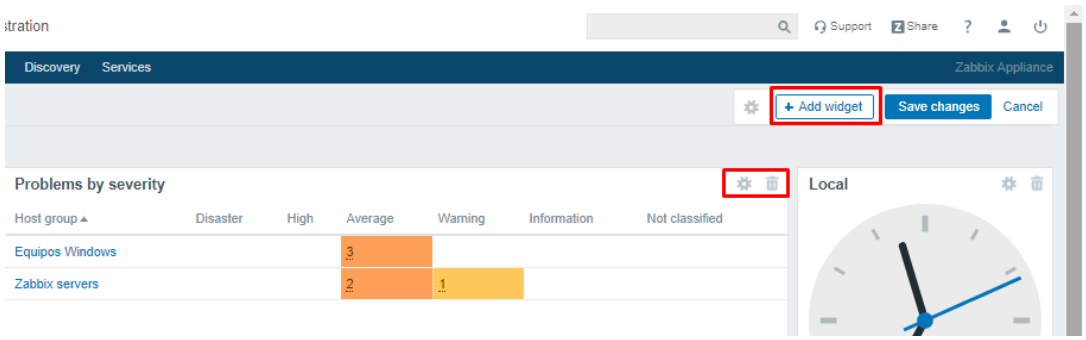

Ilustración 159: Eliminación de Vista en Tablero.

3.-En el panel de configuración de la nueva vista o widget, seleccionaremos como Type: Graph (classic), Name: El nombre que deseemos poner a la gráfica, Refresh Interval: El intervalo de actualización de los datos mostrados, Graph: El valor que deseamos monitorear.

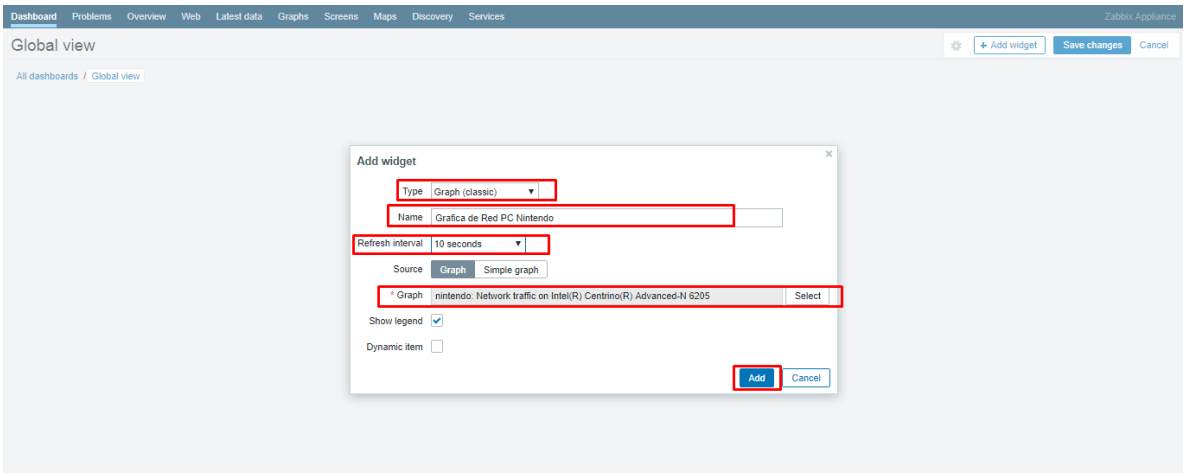

Ilustración 160: Configuración de Widget.

4.-Visualizar la gráfica creada y seleccionar la opción Save changes para guardar los cambios, es posible crear las gráficas deseadas.

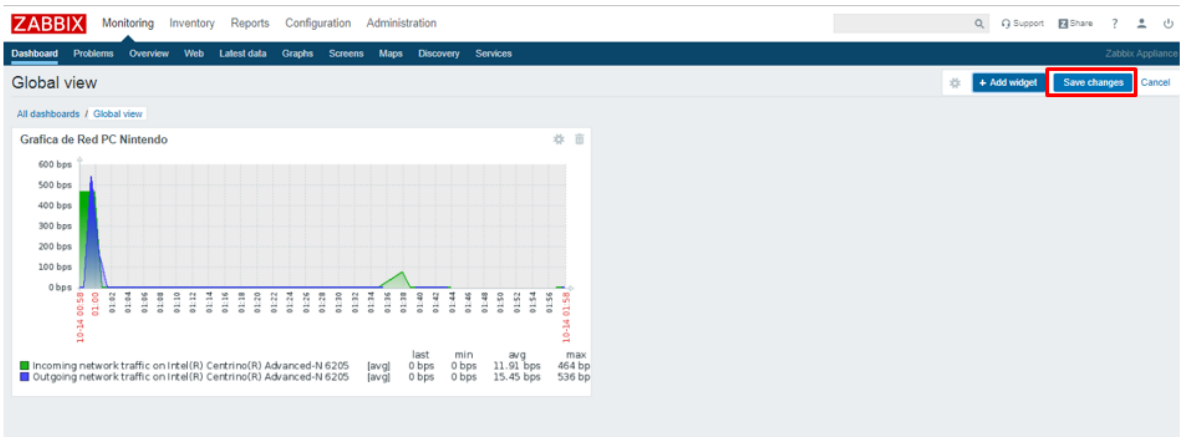

Ilustración 161: Tablero Zabbix Modificado (Parte 1).

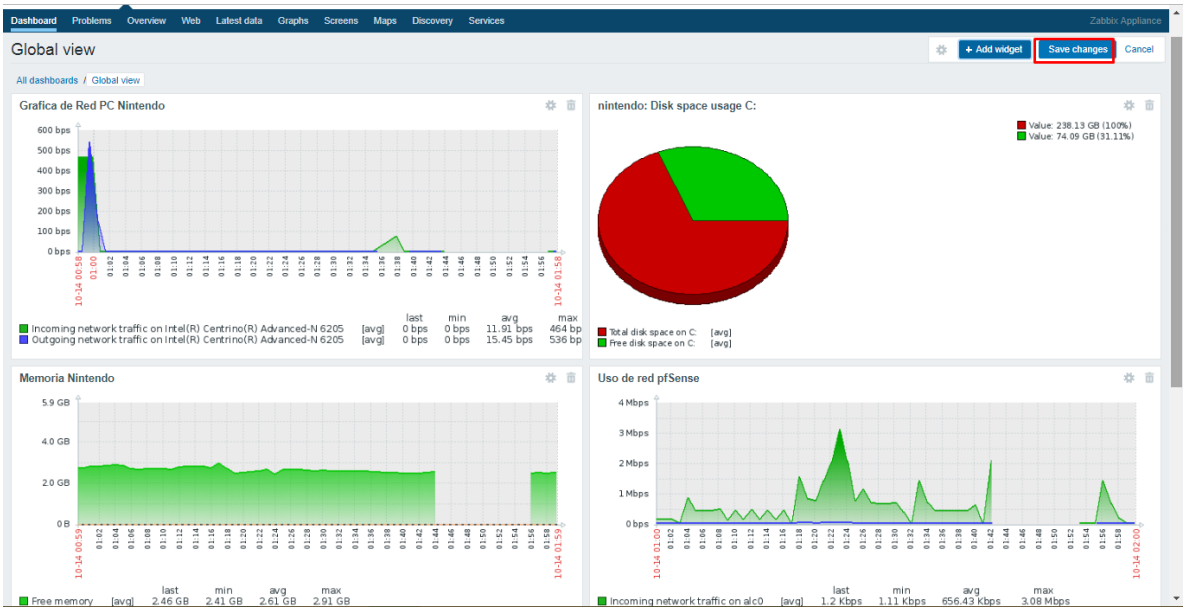

Ilustración 162: Tablero Zabbix Modificado (Parte 2).

Mapas

Una forma práctica de visualizar el comportamiento de una organización es mediante Mapas, Zabbix permite la creación de Mapas personalizados.

1.-Para crear mapas es posible cargar fondos personalizados a las plantillas, en la ruta Administration -> General, seleccionamos el formato Images

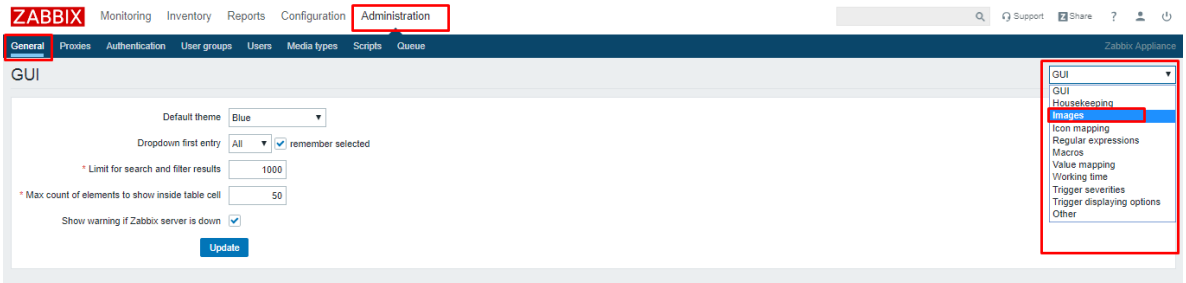

Ilustración 163: Ruta para Anexar Imágenes.

2.- En la opción Tipo seleccionamos Background (El formato que debe tener la imagen que se usara como fondo es jpg), damos clic en Create background.

Ilustración 164: Ruta para el Uso de Imagen como Fondo.

3.-Asignamos un nombre al Fondo, seleccionamos el archivo de la ubicación local, seleccionamos el botón abrir para cargar el archivo en Zabbix y clic sobre la opción Add para guardar los cambios realizados.

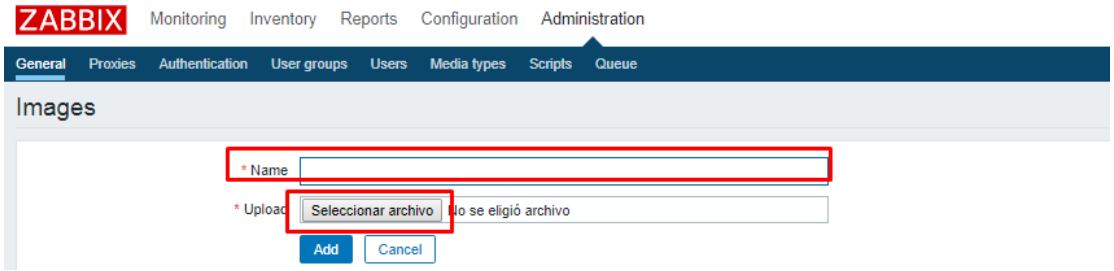

Ilustración 165: Elección de Fondo (Parte 1).

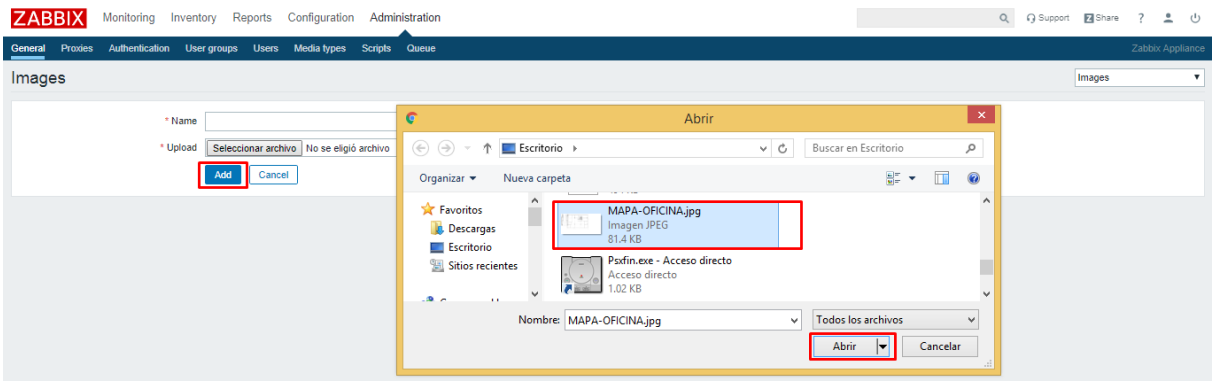

Ilustración 166: Elección de Fondo (Parte 2).

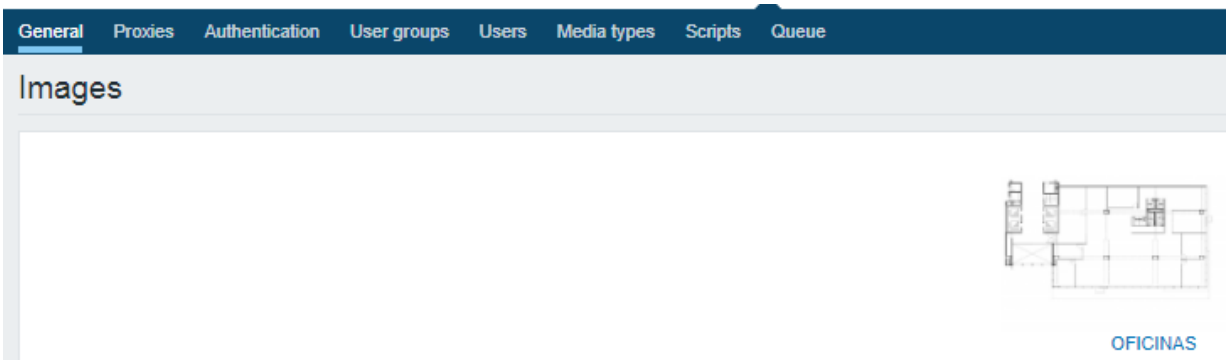

Ilustración 167: Elección de Fondo (Parte 3).

4.-En la ruta Monitoring -> Maps seleccionamos la opción Create map.

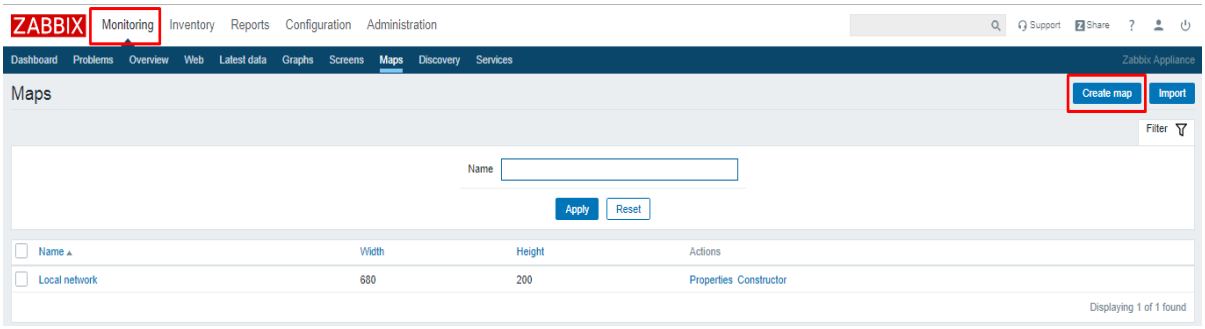

Ilustración 168: Ruta para Creación de Fondo.

5.-En el panel de confuguracion del nuevo mapa asignamos el name: Nombre del mapa, Width y Height: El tamaño del mapa, Background image: Seleccionamos de manera opcional un fondo creado previamente. Una vez realizados los cambios seleccionamos la opcion Update para crear el mapa.

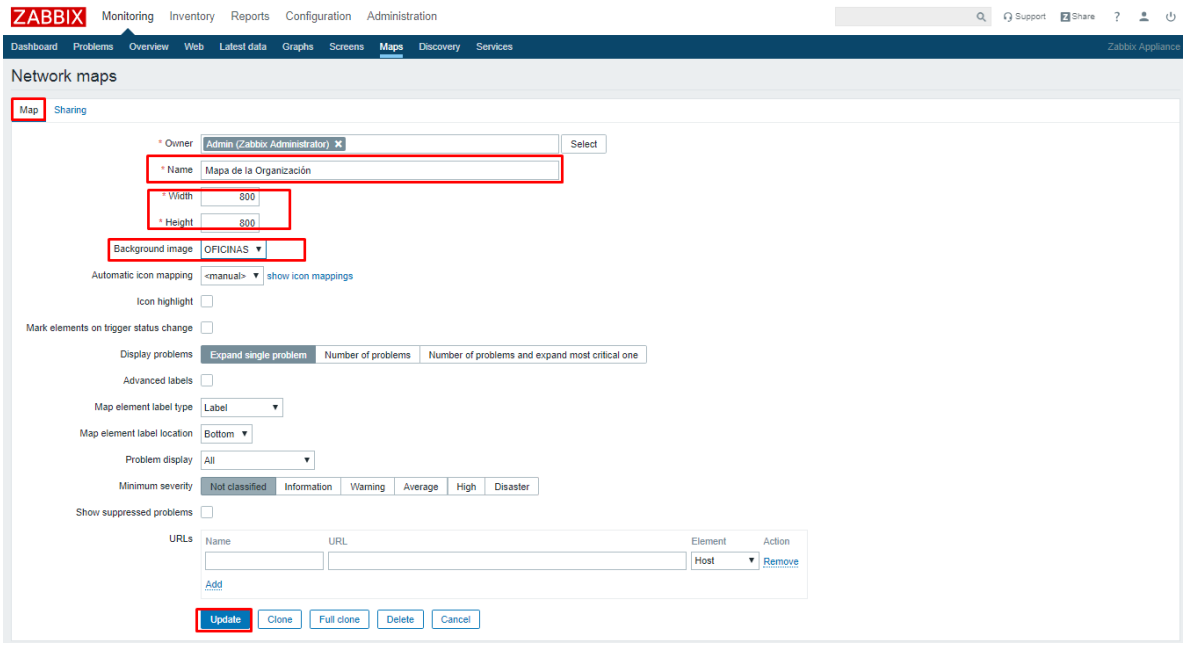

Ilustración 169: Panel de Configuración de Fondo

6.-Seleccionamos la opción Constructor del mapa creado para poder editarlo y crear los equipos a mostrar.

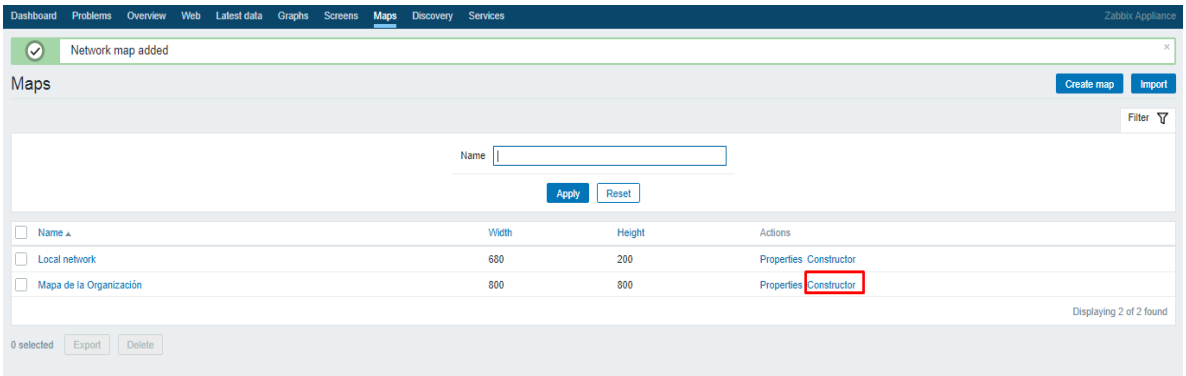

Ilustración 170: Creación de Mapas

7.- Podremos visualizar el fondo seleccionado en el mapa, para agregar los equipos seleccionamos la opción Add de la opción Map element, para agregar los equipos.

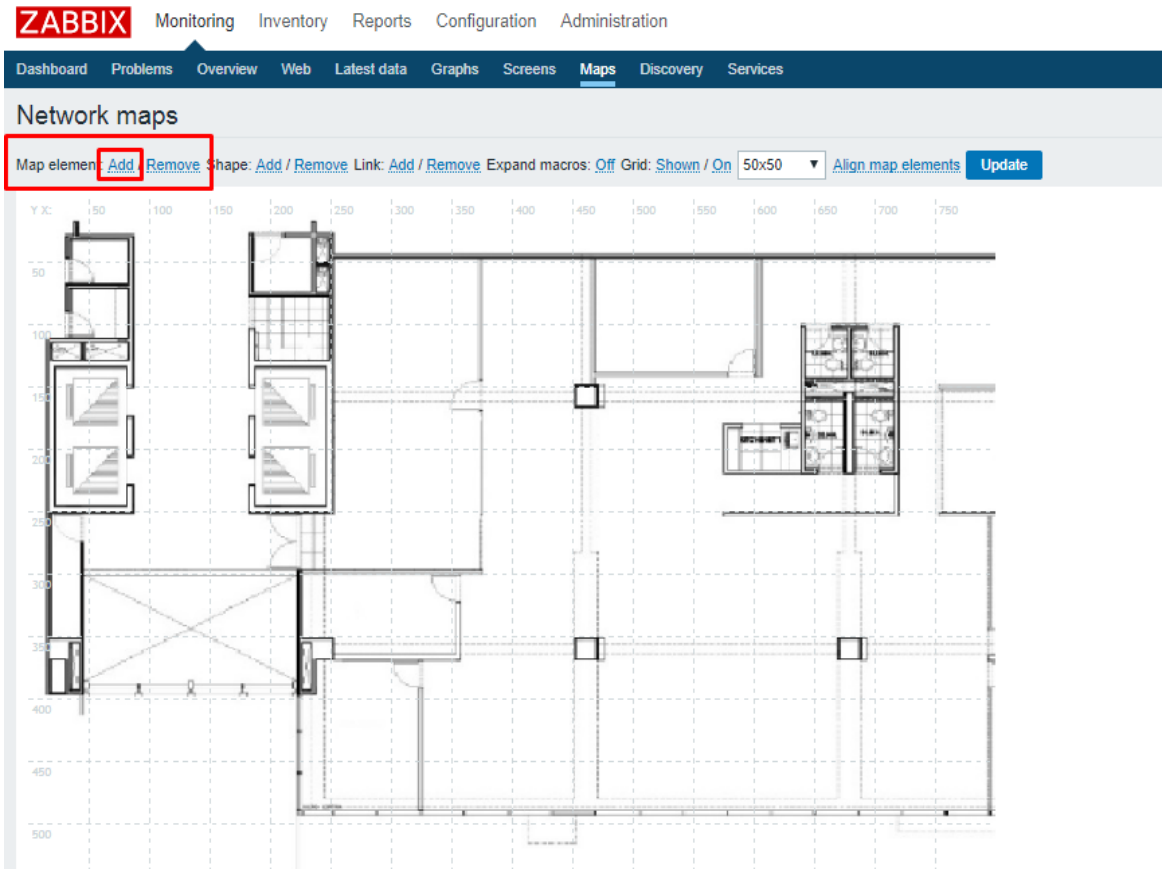

Ilustración 171: Personalización de Mapa (Parte 1).

8.-Se agregará un ícono que representa un equipo de TI, en la opción Icons Default, se deberá seleccionar el ícono que deseamos usar, por defecto en Zabbix existen íconos de diferentes equipos de TI.

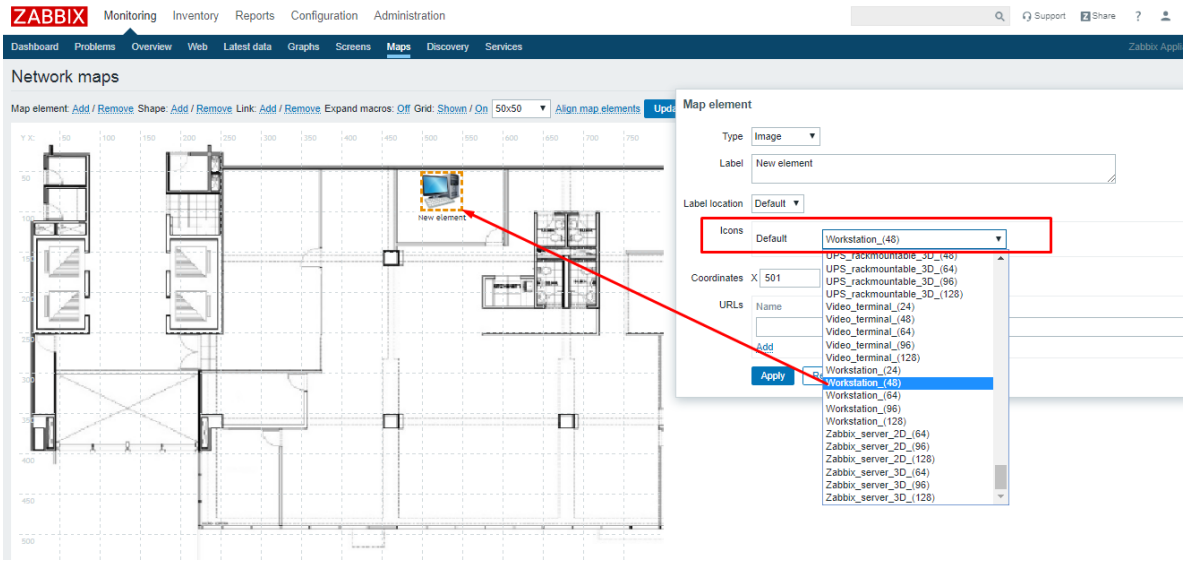

Ilustración 172: Personalización de Mapa (Parte 2).

10.- Para nuestro proyecto se crean los 4 Equipos monitoreados por Zabbix.

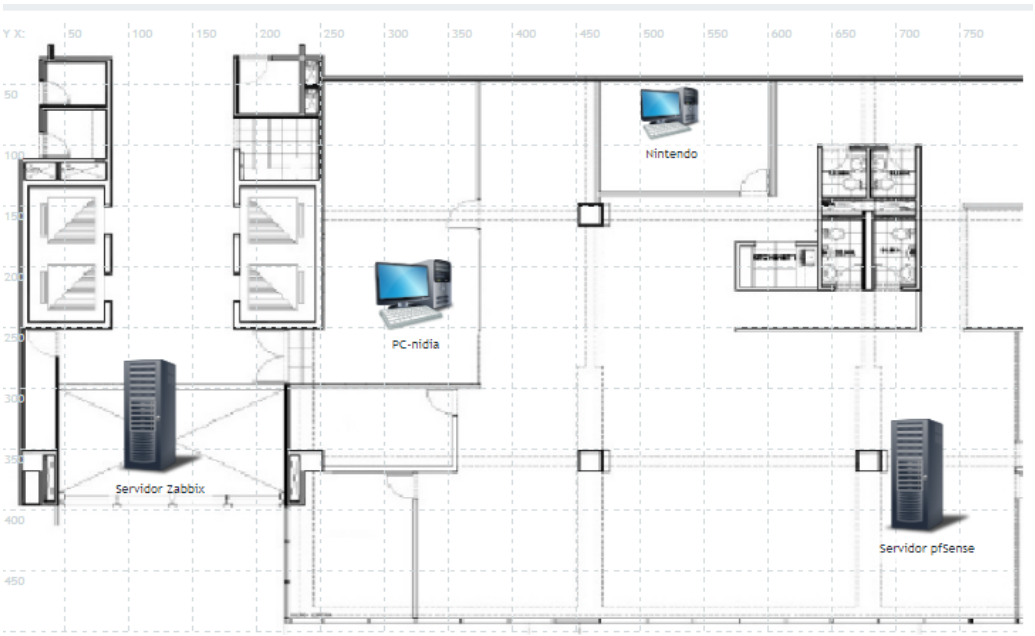

Ilustración 173: Personalización de Mapa (Parte 4).

3.8.3.5 Configuración Alertas Graficas y Notificaciones por Correo Electrónico

Alerta Gráfica

En Zabbix es posible usar los Mapas como alertas gráficas permitiendo usar los íconos en modo Trigger (desencadenante) para ver de forma gráfica los cambios detectados.

1.- En el panel de administración de nuestro mapa seleccionamos el ícono del equipo que deseamos modificar, en la Ilustración 174 Se ha seleccionado el ícono de nintendo, se modifica la opción Type como Trigger por lo que se despliegan nuevas opciones.

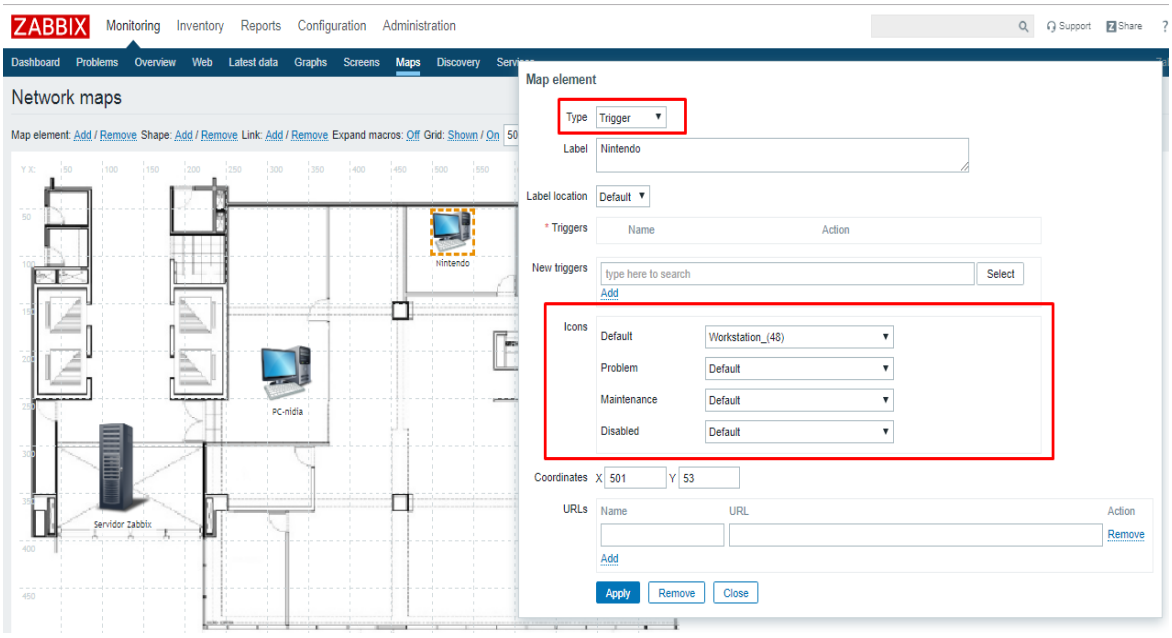

Ilustración 174: Configuración de Alerta Visual (Parte 1).

2.-En el campo New triggers damos clic sobre la opcion Select para elegir el recurso de monitoreo que usaremos como alerta, estos recursos son contenidos en la opcion Templates, en el campo Problem: Seleccionamos el ícono al que cambiara en caso de presentarse un problema.

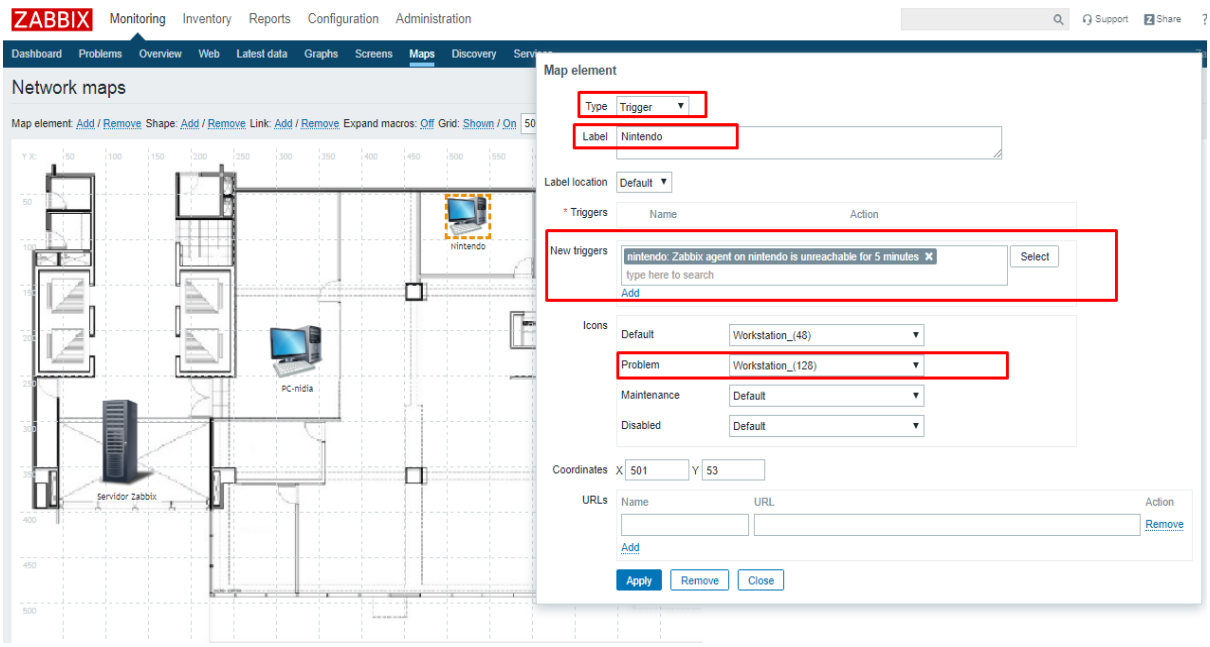

Ilustración 175: Configuración de Alerta Visual Parte 2.

3.-En la Ilustración *176* se muestra un trigger para el ícono nintendo el cual se desencadenará como problema después de 5 minutos de inactividad o pérdida de conexión con el agente Zabbix del host nintendo, si existe un problema se mostrará un ícono con un tamaño mayor. Para guardar los cambios seleccionamos la opción Apply y cerramos la ventana. Se realiza el mismo cambio para el ícono PC-nidia y aplicamos los cambios.

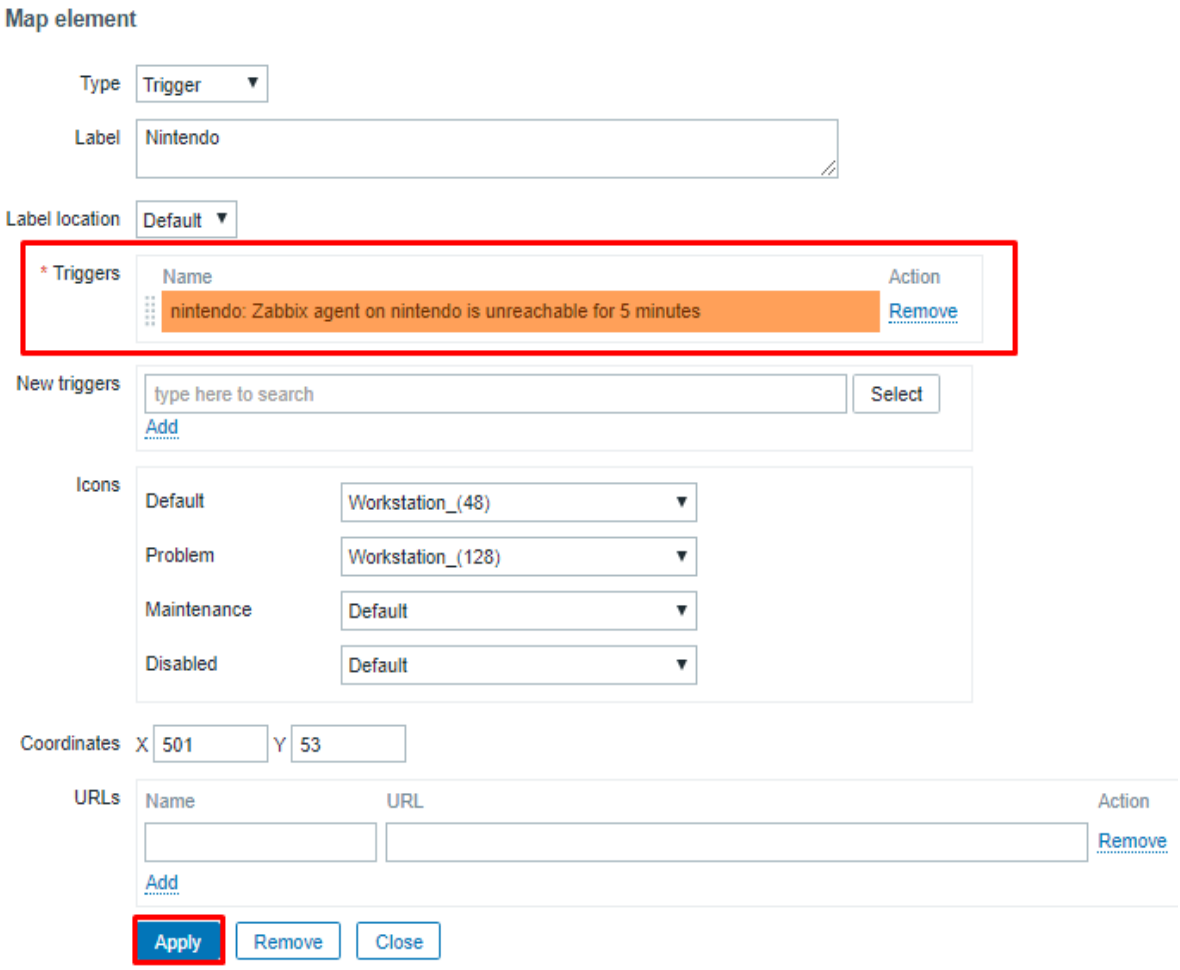

Ilustración 176: Configuración de Alerta Visual (Parte 3).

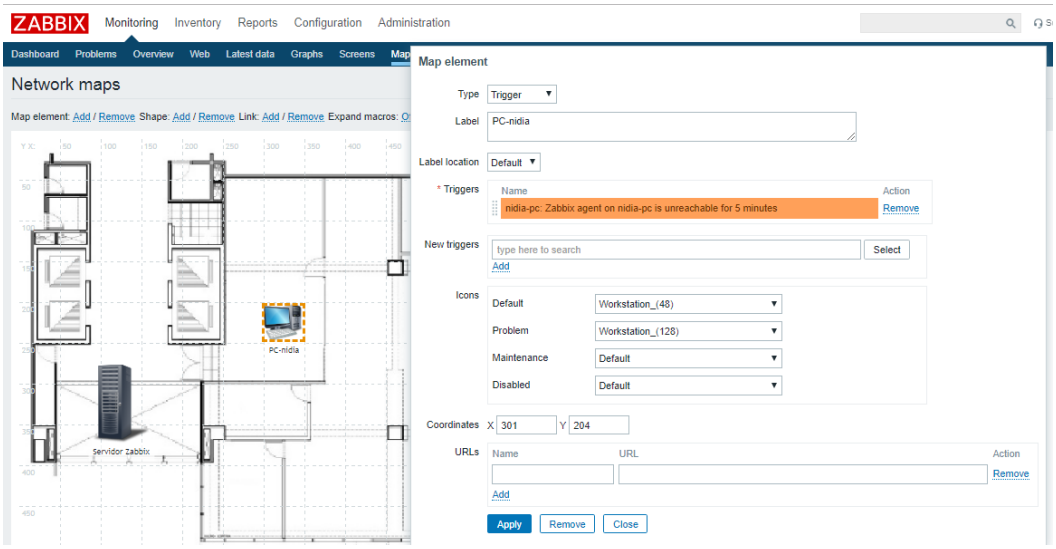

Ilustración 177: Configuración de Alerta Visual (Parte 4).

4.-Una vez terminados los cambios damos clic sobre la opción Update para guardar nuestros cambios sobre el mapa.

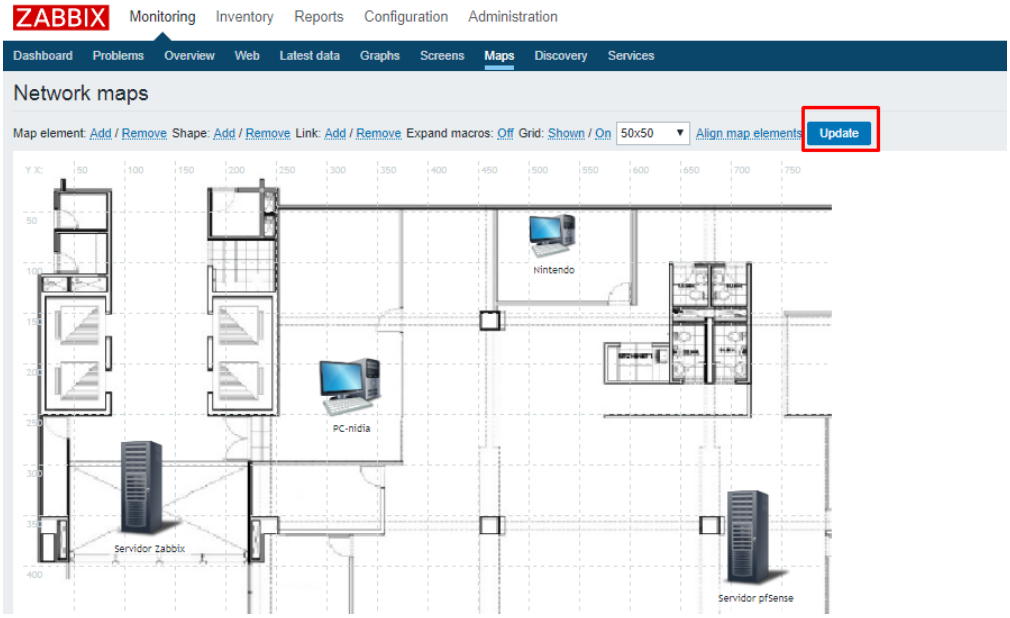

Ilustración 178: Configuración de Alerta Visual (Parte 5).

5.- Los íconos nintendo y PC-nidia se encuentran con normal operación en el mapa.

nintendo (ícono que representa al host nintendo)

ícono PC-nidia (ícono que representa al host pc-nidia)

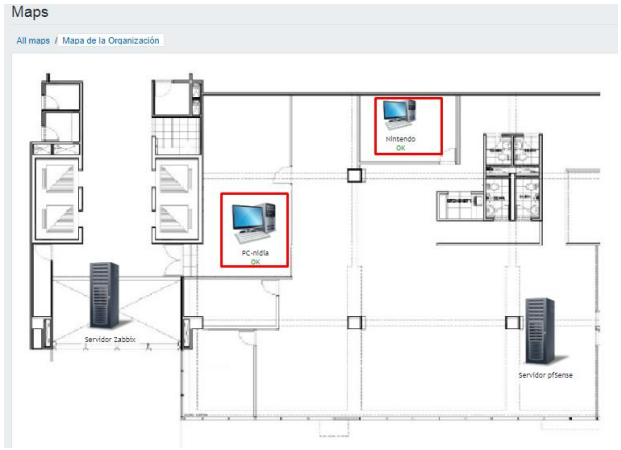

Ilustración 179: Prueba de Alerta Visual (Parte 1).

6.- Desconectamos de la red al host pc-nidia y podremos que una vez cumplida la condición de Trigger el ícono cambia al ícono de estado de problema seleccionado.

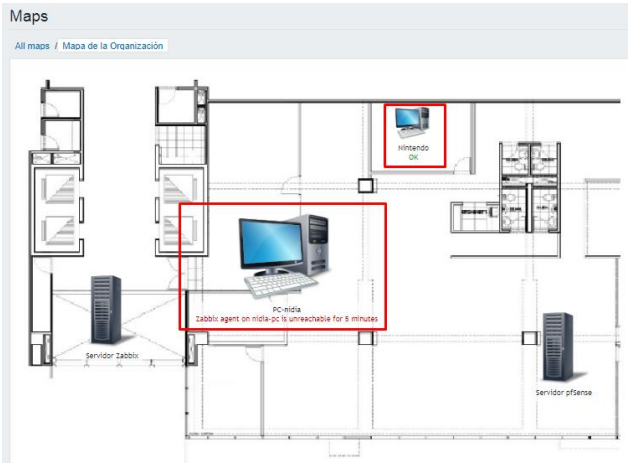

Ilustración 180: Prueba de Alerta Visual (Parte 2).

Notificaciones por correo

En el Zabbix las notificaciones se pueden configurar para ser recibidas en una cuenta de correo electrónico.

1.-Para configurar las notificaciones por correo nos dirigimos a la ruta Configuration -> Media types, seleccionamos la opción Email para configurar las alertas.

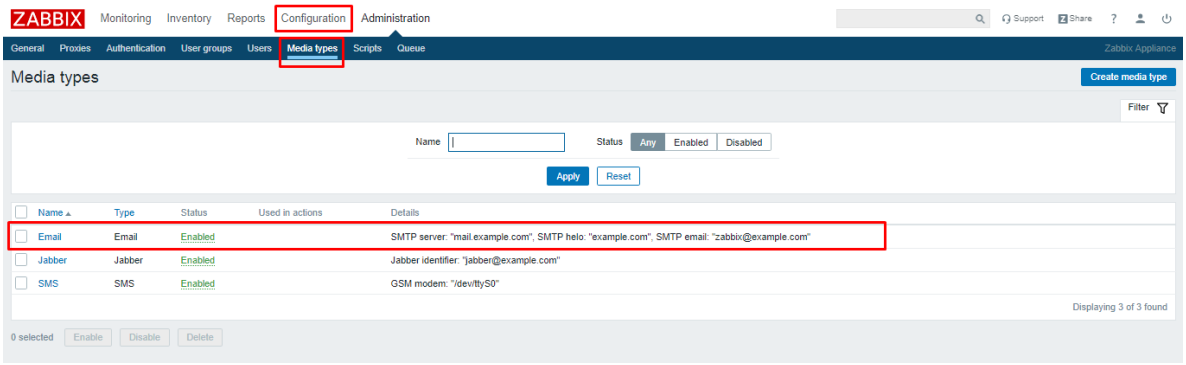

Ilustración 181: Configuración de Alerta por Correo Electrónico.

2.-En el panel de configuración de email asignaremos tendremos que colocar los datos del servicio de correo que deseamos usar, en la Ilustración 182 se muestra una configuración para un correo perteneciente al dominio de Gmail.

- Name: Nombre del Tipo de medio
- Type: Email (Tipo de notificación)
- SMTP server: smtp.gmail.com (Servidor de correo de salida)
- SMTP server port: 25 (puerto de salida de correo)
- SMTP helo: gmail.com (nombre de dominio)
- SMTP email: tesisnotificacion420@gmail.com (Cuenta de usuario desde la cual se enviaran los correos)

- Connection security: STARTTLS (Tipo de seguridad para nuestro servicio de correo)
- Autentication: Username and password (Seleccionamos el método de autenticación para nuestro servicio de correo)
- Usuario: tesisnotificacion420 (usuario de correo)
- Password: TESIS258745 (contraseña de usuario)

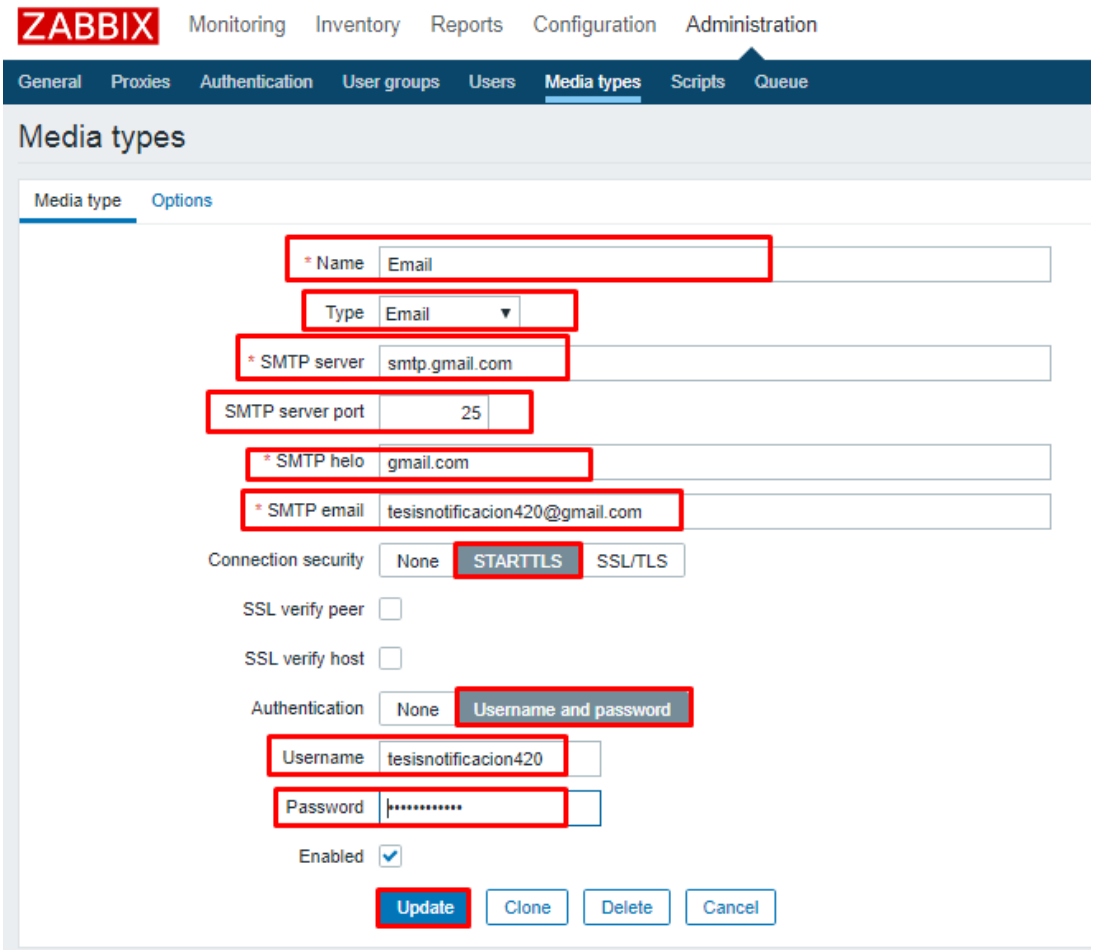

Ilustración 182: Configuración de Correo en Zabbix.

3.-Seleccionamos la pestaña Options se define el número de intentos para enviar la notificación y el intervalo de tiempo para él envío de la notificación, una vez realizados los cambios seleccionamos la opción Update para guardar.

Attempts: 3 (Número de intentos de envío de correo)

Attempt interval: 5s (Los intentos de notificación se envían cada 5 segundos)

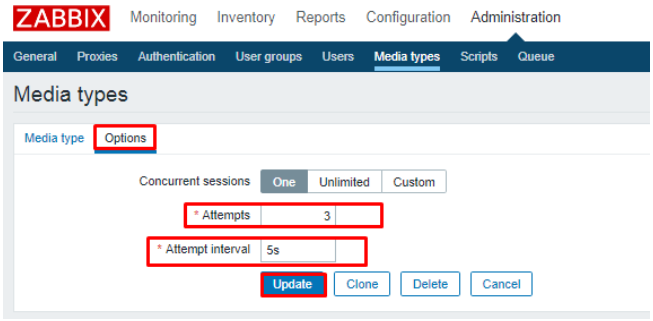

Ilustración 183: Parámetros de Envió de Notificaciones.

4.-Configuraremos el usuario que recibirá las notificaciones, nos dirigimos a Administration -> Users, seleccionamos el usuario Admin para que este reciba las notificaciones.

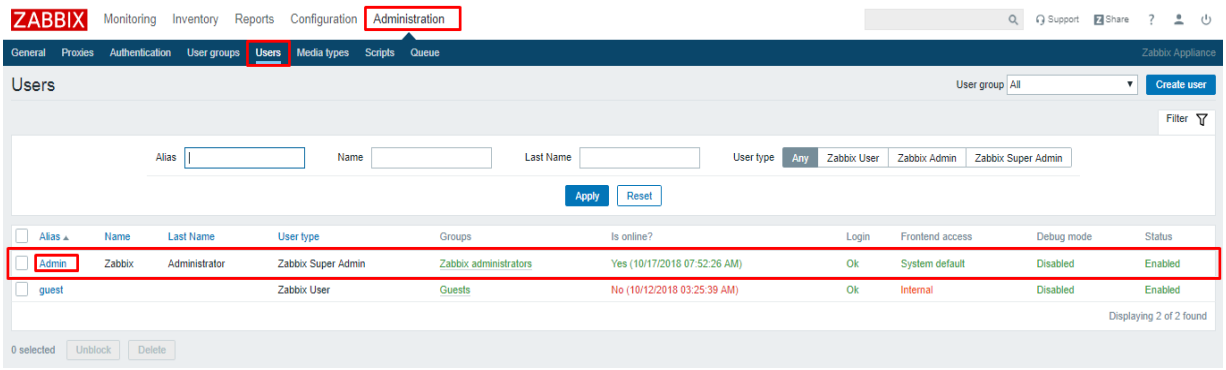

Ilustración 184: Configuración de Usuario que Recibe Notificaciones.

5.- Seleccionamos la pestaña Media, damos clic sobre la opción Add para agregar un medio de comunicación.

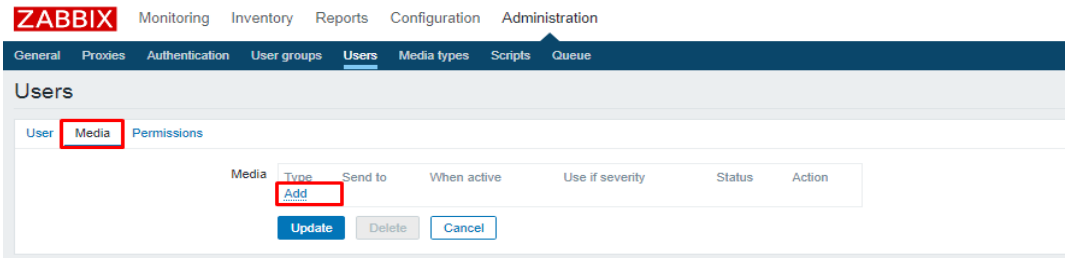

Ilustración 185: Alta de Medio de Comunicación.

6.-En el panel de configuración del nuevo medio de comunicación seleccionamos los valores.

Type: Email (Medio de comunicación que se usará)

Semd to: tesisnotificacion420@gmail.com (Cuenta a la que se enviaran las notificaciones)

Use if severity: Seleccionamos la gravedad de alertas que recibirá este usuario

Seleccionamos la opción Add -> Update , para guardar los cambios.

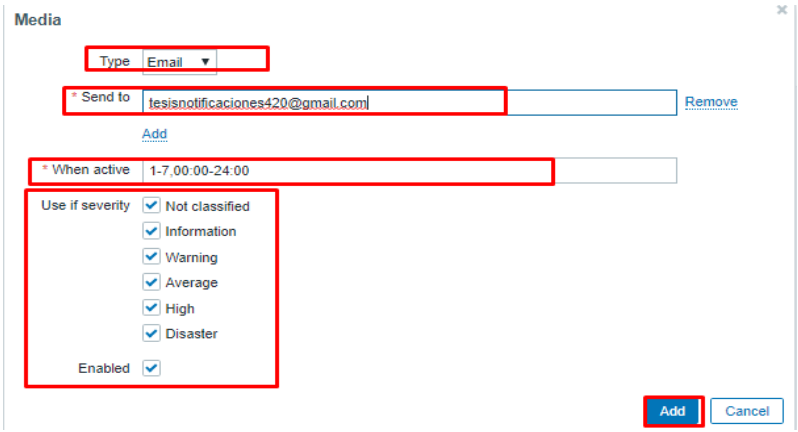

Ilustración 186: Configuración de Medio de Comunicación.

7.-Creamos la notificación y su condición en la ruta Configuration -> Action , y seleccionamos la opción Create action.

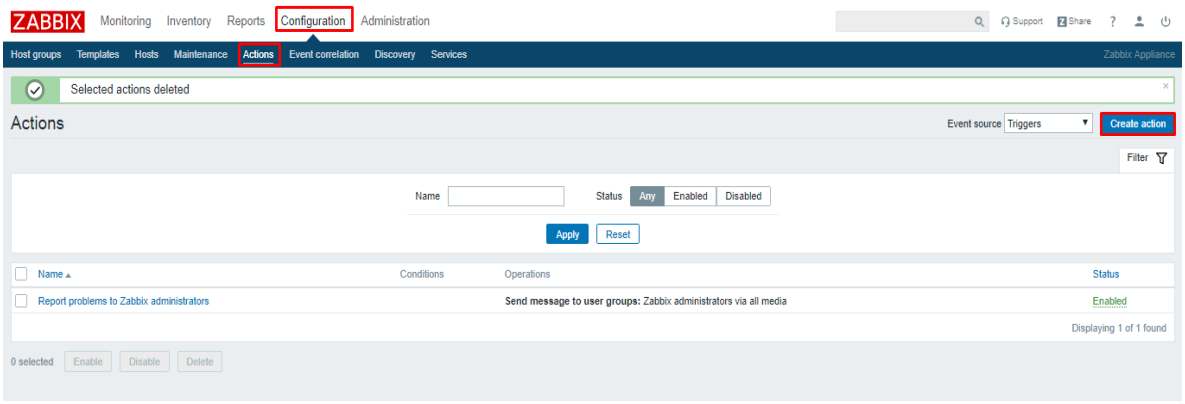

Ilustración 187: Ruta para Configuración de Acciones.

8.- En el panel de configuración de la nueva acción elegimos un nombre, en la sección New condition se define la condición para que esta acción se realice, en la Ilustración *188* Se usan las condiciones Trigger – equals – (damos clic sobre la opción Select para elegir un valor de monitoreo).

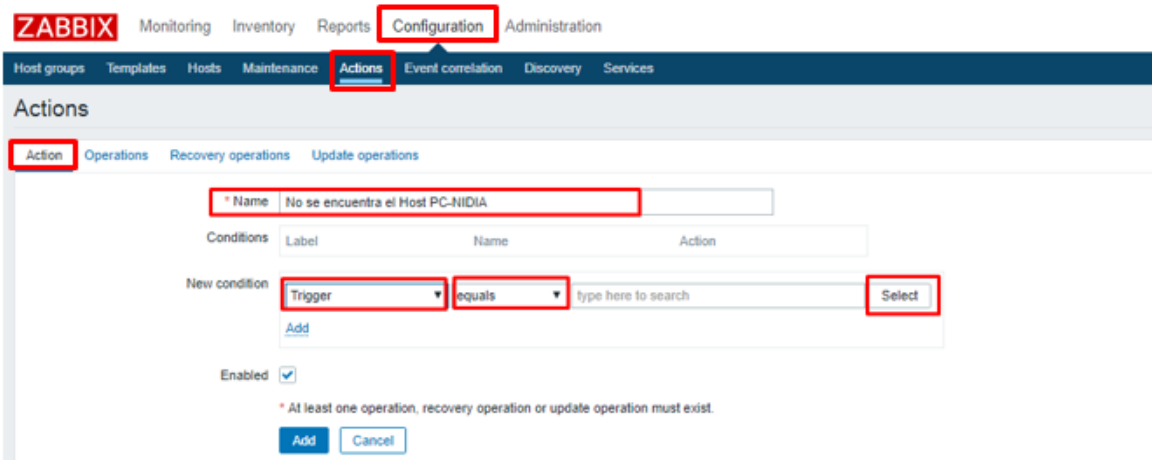

Ilustración 188: Configuración de Actions.

9.-Seleccionamos el host que desatará esta acción así como el trigger que detonará nuestra acción. En la Ilustración 189 se usa el host nidia-pc, el trigger seleccionado detonará la alerta cuando el agente Zabbix de nidia-pc pierda conexión con el servidor.

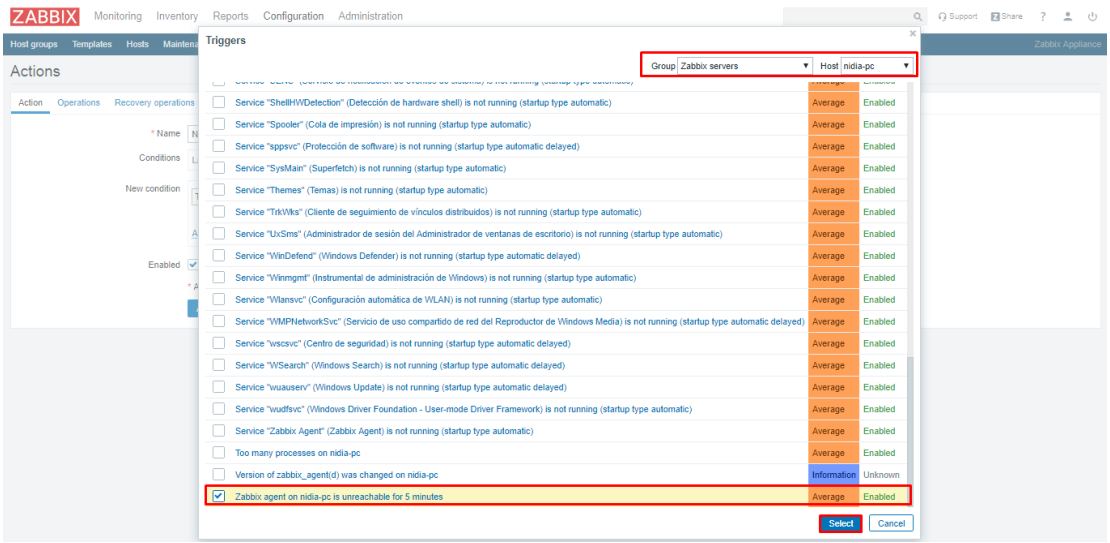

Ilustración 189: Elección de Disparador (Parte 1).

10.- Damos clic sobre la opción Add para agregar la condición.

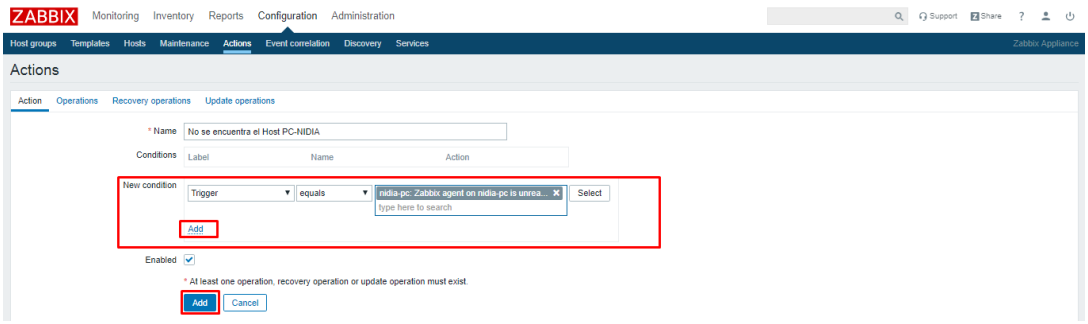

Ilustración 190: Elección de Disparador (Parte 2).

11.-En la pestaña Options se define el mensaje y los destinatarios que reciben la notificación, en la Opcion Send to User groups: Podemos agregar grupos para que todos los usuarios de este grupo reciban el mensaje, en la opción Send to User: Podremos seleccionar usuarios específicos. En la opción Send only to definimos el tipo de envió que realizaremos en nuestro caso Email.

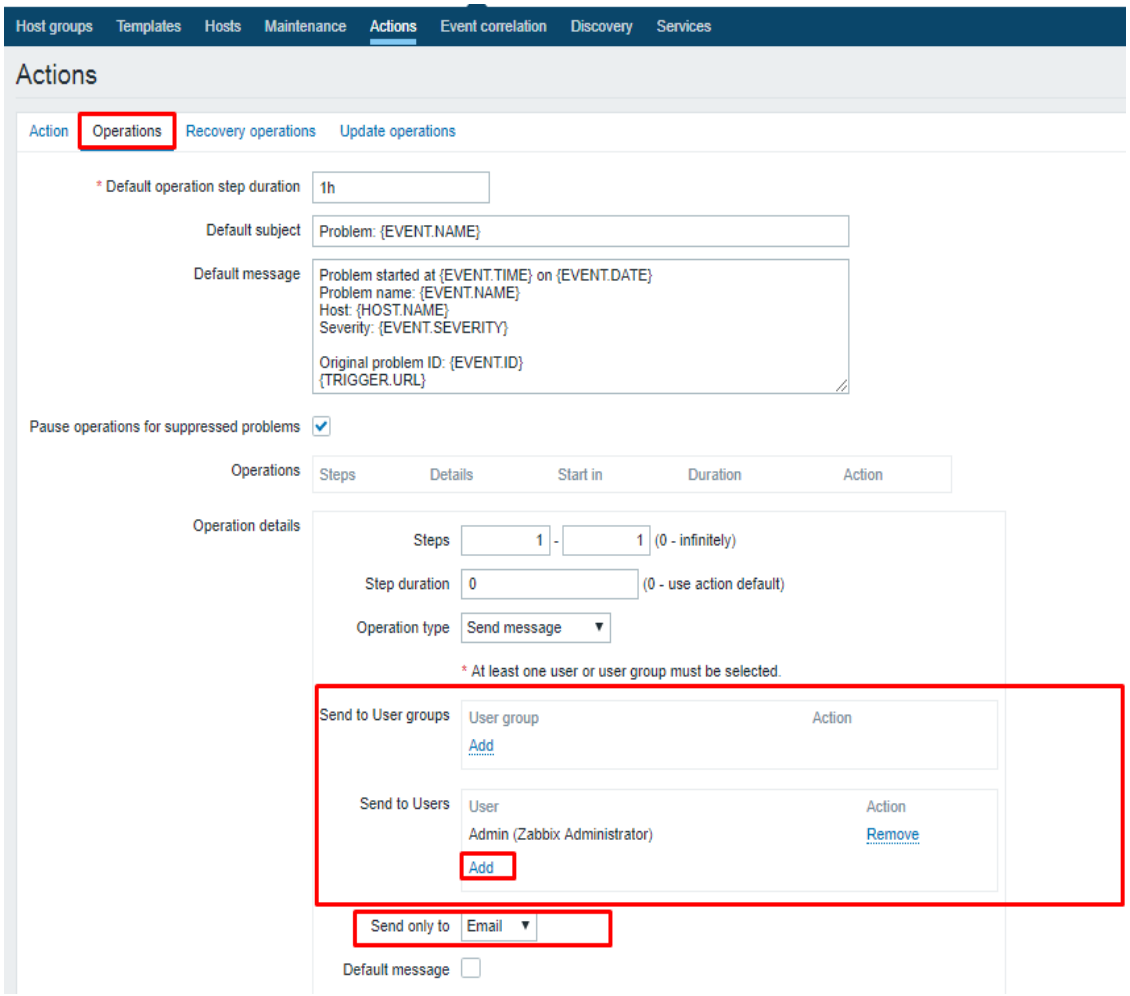

Ilustración 191: Configuración de Contenido en Notificación (Parte 1).

12.-Podremos definir el Asunto y cuerpo del correo que se enviara al detonar la alerta. Una vez realizados los cambios seleccionamos la opción Add para guardar.

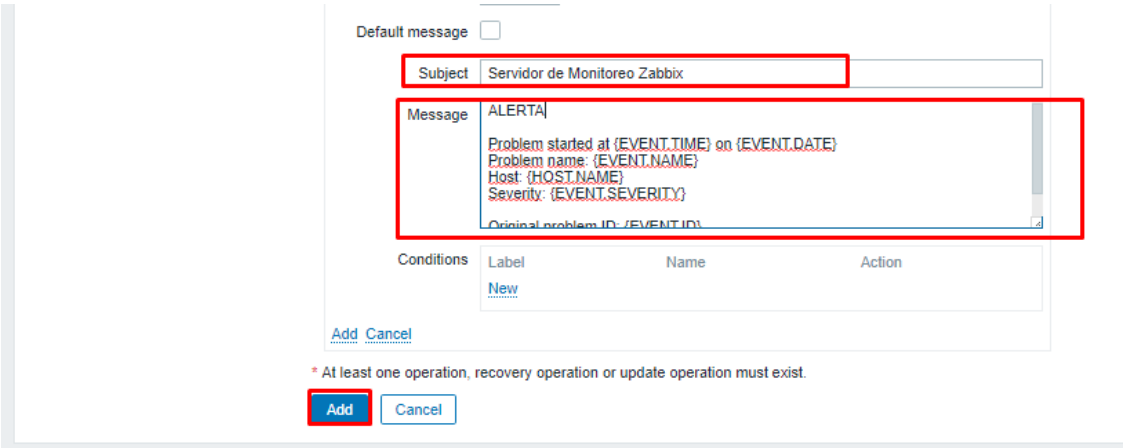

Ilustración 192: Configuración de Contenido en Notificación (Parte 2).

13.- Desconectamos de la Red el host nidia-pc para realizar nuestra prueba, en la ruta Reports -> Action log, podremos ver que el evento se realizó con éxito.

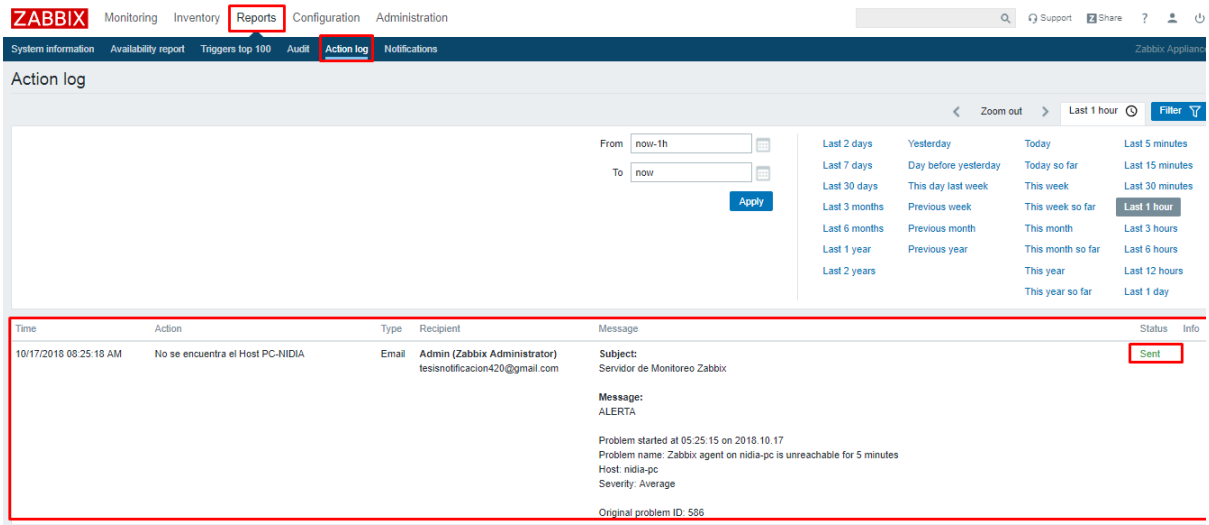

Ilustración 193: Comprobación de Notificación.

14.-Validamos en la cuenta de correo del usuario Admin y veremos el correo notificando sobre el problema del host nidia-pc.

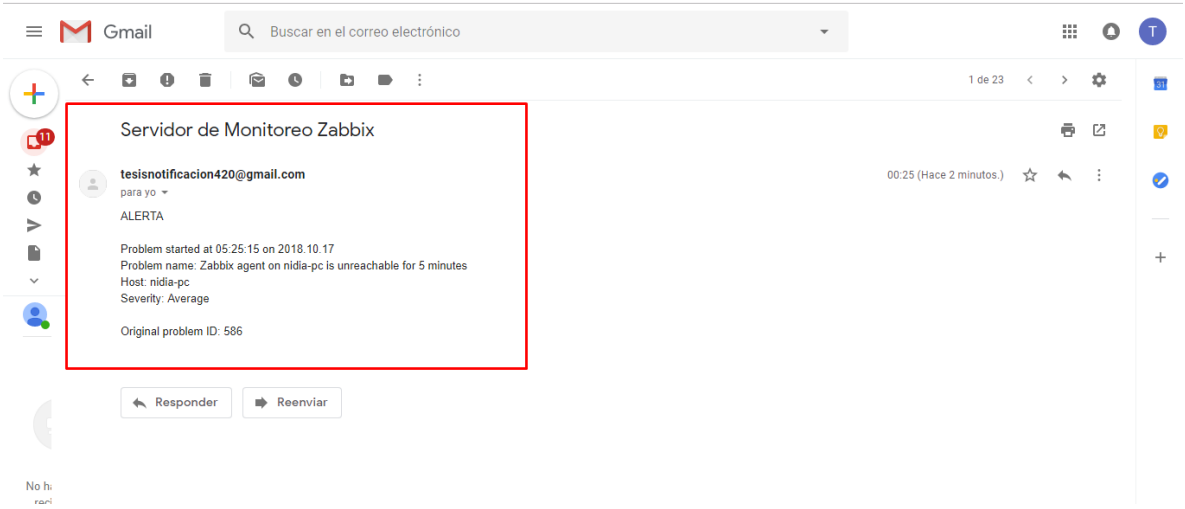

Ilustración 194: Notificación en Correo.

3.9 Preparación, Instalación y configuración de Sistema de Respaldo en Red usando FreeNAS

3.9.1 Herramientas Hardware y Software

Para poder mostrar un arreglo de discos se usara un equipo virtual (Usando la herramienta Virtual Box), el cual cuenta con las características:

- CPU: 64 Bits 2 CPU
- Memoria RAM: 4 GB
- 3 Disco virtuales fijos de 20 GB

Es posible descargar la aplicación Virtual Box en la página https://www.virtualbox.org/wiki/Downloads (Oracle, s.f.)

Para la instalación de FreeNAS en ambiente Físico es posible crear un USB de arranque usando el programa para la creación de dispositivos de arranque, es posible descargar el programa desde la página: https://rufus.ie/es_ES.html_(Pete Batard, s.f.)

Herramientas Para instalación Física

- USB 8GB: Usada para crear dispositivo de arranque
- Rufus

3.9.2 Creación de dispositivo de arranque para entorno Físico

1.- Ejecutamos el programa Rufus 3.3.1400, Es de suma importancia seleccionar en la opción Dispositivo: la memoria que será usada como dispositivo de arranque, en la opción Elección de arranque elegimos la imagen iso de FreeNAS que hemos descargado, dejamos los valores por defecto y seleccionaos la opción empezar.

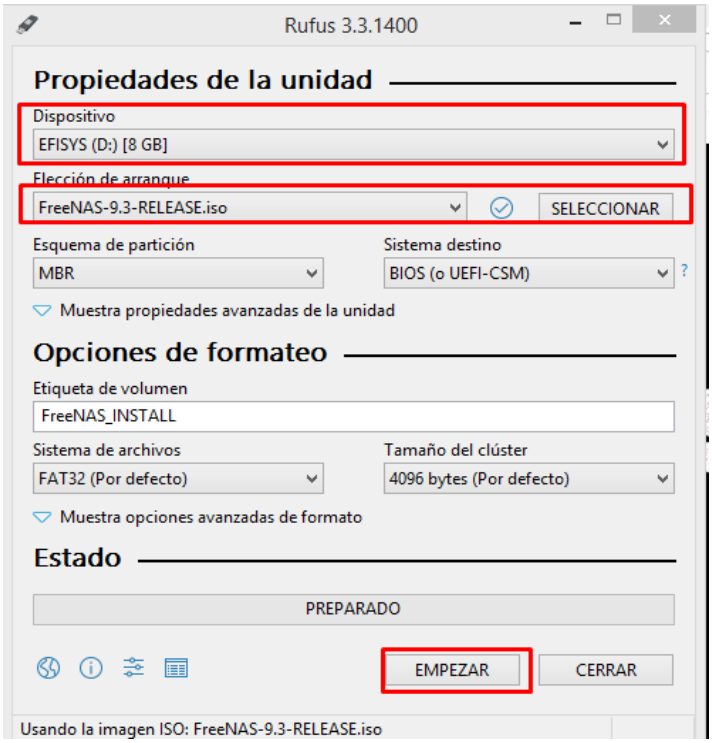

Ilustración 195: Creación de USB de Arranque FreeNAS (Parte 1).

2.-Cuando el programa termine de crear el dispositivo de arranque la barra de estado se pondrá en verde, en este momento es posible usar el dispositivo para arrancar en un equipo físico.

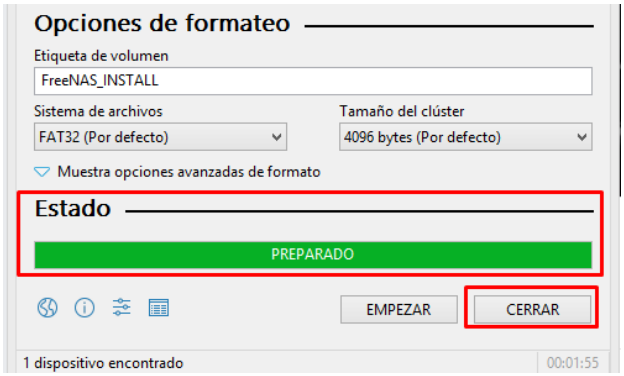

Ilustración 196: Creación de USB de Arranque FreeNAS (Parte 2).

3.9.3 Proceso de Instalación de FreeNAS.

1.- Iniciamos desde el dispositivo de arranque que contiene el sistema FreeNAS, en las opciones que se presente damos Enter para iniciar la instalación.

Ilustración 197: Opciones de Instalación FreeNAS.

2.-En la guía de instalación seleccionamos la Opción 1 Install/Upgrade.

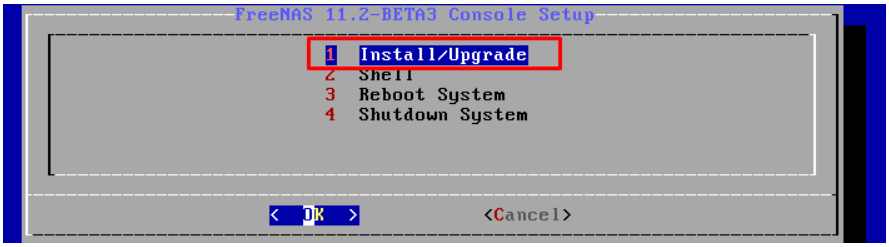

Ilustración 198: Inicio de Instalación FreeNAS.

3.-Debido a que contamos con menos de 8 GB de memoria RAM, aparece el mensaje de advertencia al cual daremos en la opción Yes para continuar con la instalación. Es de suma importancia señalar que se recomiendan 8GB mínimos de memoria para fines de uso en ambientes reales.

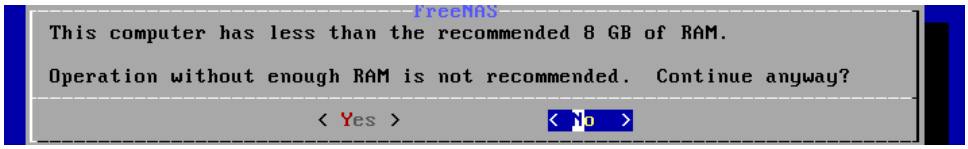

Ilustración 199: Advertencia sobre Memoria RAM FreeNAS.

4.-Seleccionamos el disco donde se instalara el Sistema, en la imagen…. Se elige el disco ada0.

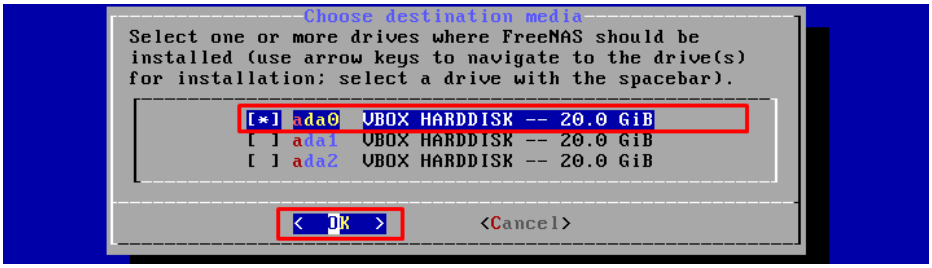

Ilustración 200: Selección de Discos para instalación FreeNAS.

5.- Se nos presentan dos advertencias y una recomendación, ya que el disco además de ser formateado no podrá ser usado como medio de almacenamiento. Seleccionamos la opción Yes para continuar.

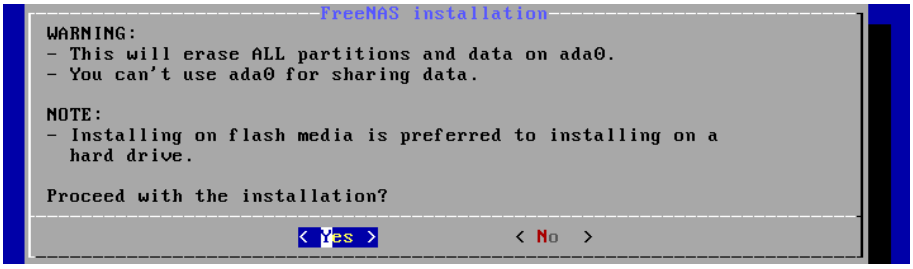

Ilustración 201: Advertencia de Instalación en Disco.

6.-Colocamos una contraseña para nuestro Servidor e Interfaz de configuración Web, el usuario por defecto será root.

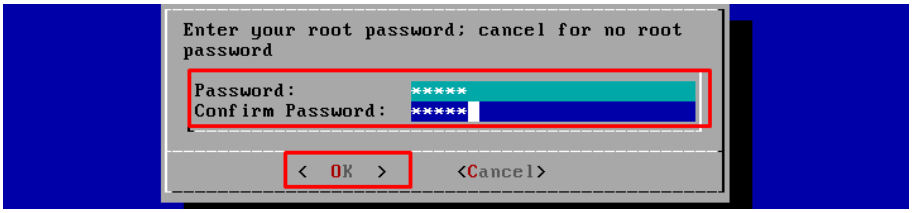

Ilustración 202: Asignación de Contraseña a FreeNAS.

7.-Elegimos el tipo de arranque de nuestra instalación, en nuestro caso es el modo Boot via BIOS una vez seleccionada queda esperar a que termine la instalación.

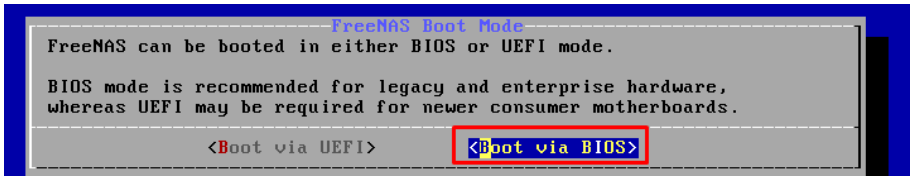

Ilustración 203: Tipo de Arranque del Sistema.

3.9.4 Configuración de Red FreeNAS

1.- Una vez iniciado el sistema configuramos la red, para esto seleccionamos la opción 1.

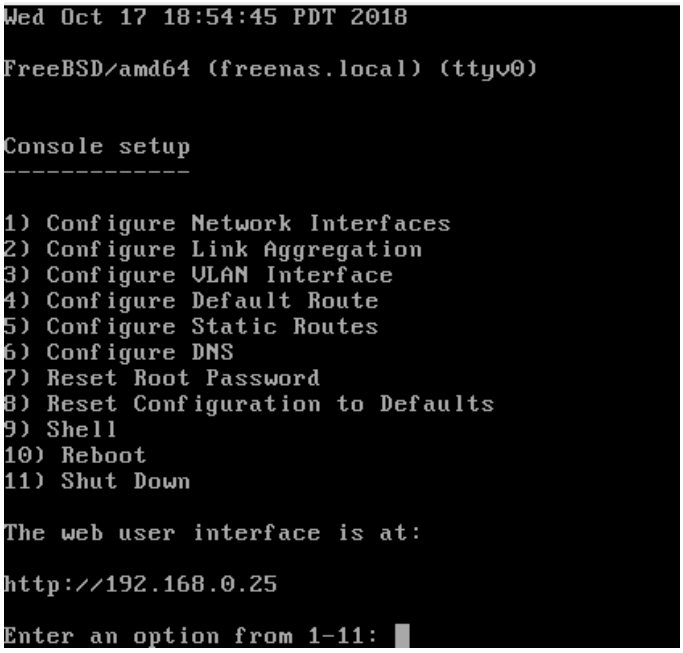

Ilustración 204: Opciones FreeNAS.

2.- Ingresamos el número de la interfaz que deseamos configurar, en la Ilustración 205 solo existe una interfaz de red por lo que usaremos esta interfaz.

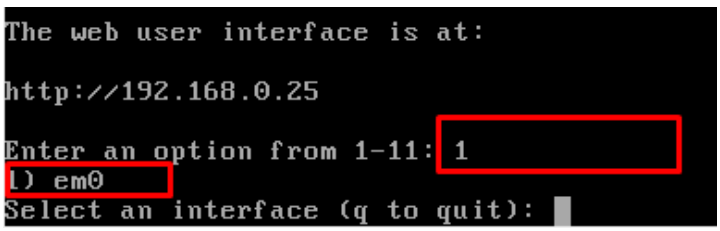

Ilustración 205: Selección de Configuración para Interfaz de Red en Servidor FreeNAS.

3.- Preguntará si deseamos resetear la configuración de red o configurar en modo DHCP a estas daremos que no tecleando "n", asignamos una configuración de red estática, en la pregunta Configure IPv4: tecleamos "y" para configurar.

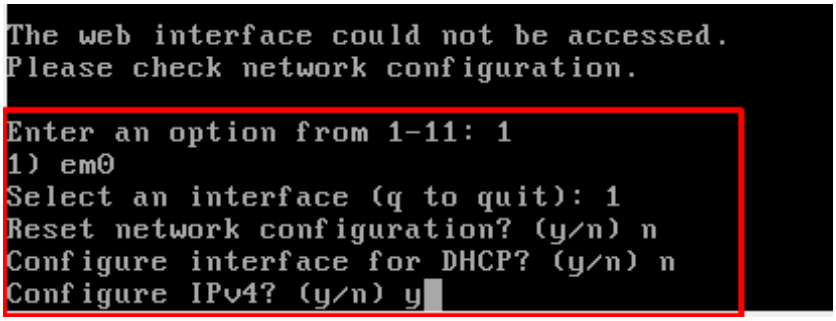

Ilustración 206: Reseteo de Interfaz de Red en FreeNAS.

4.-Ingresamos la configuración de red para la interfaz em0, primero se nos presenta la opción para asignar la dirección IP, usaremos el ejemplo 2.

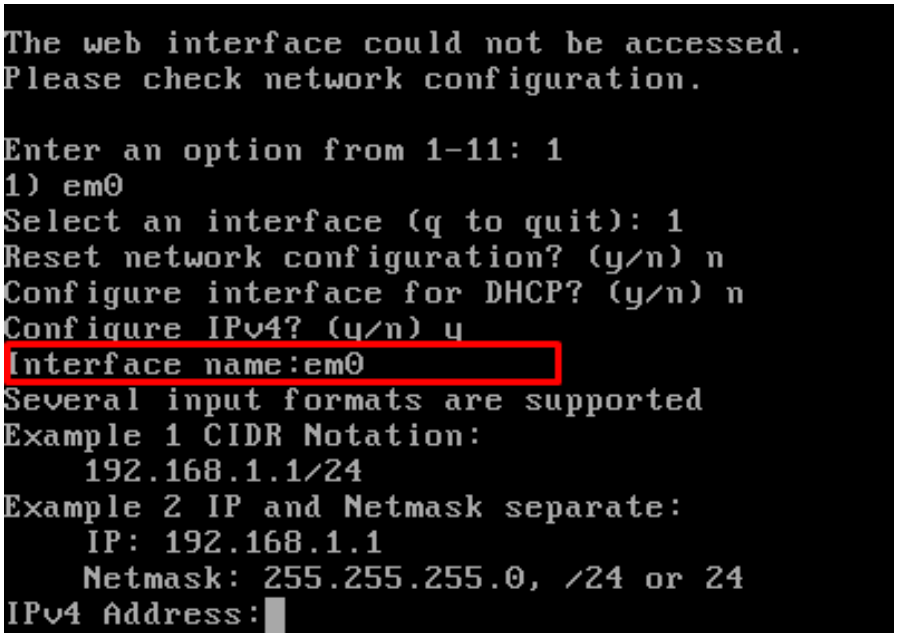

Ilustración 207: Selección de Modo Estático en Interfaz de Red.

Tecleamos la dirección IP 192.168.1.3 y tecleamos la tecla Enter para continuar y teclear la máscara de red 255.255.255.0

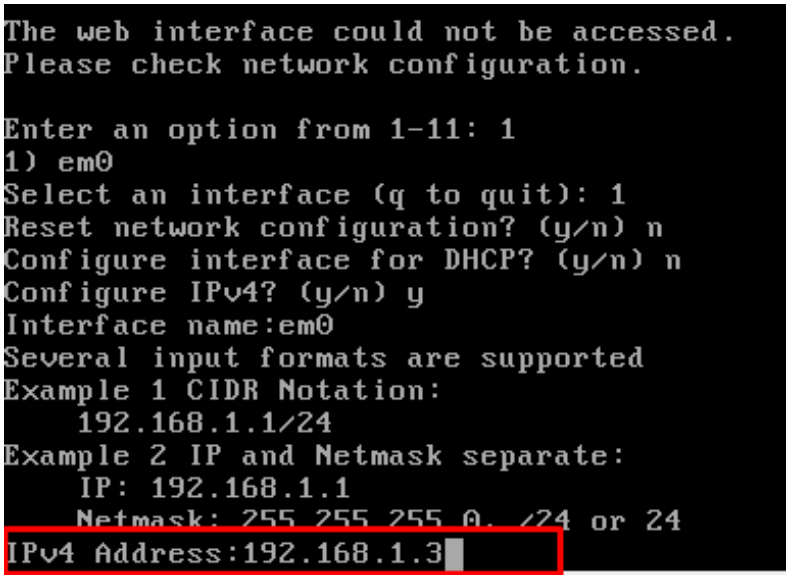

Ilustración 208: Asignación de IP.

Una vez ingresada la máscara de red damos Enter para continuar, como se muestra en la Ilustración 209 veremos un mensaje de confirmación en la configuración de la Interfaz además de la opción para configurar una dirección IPv6.

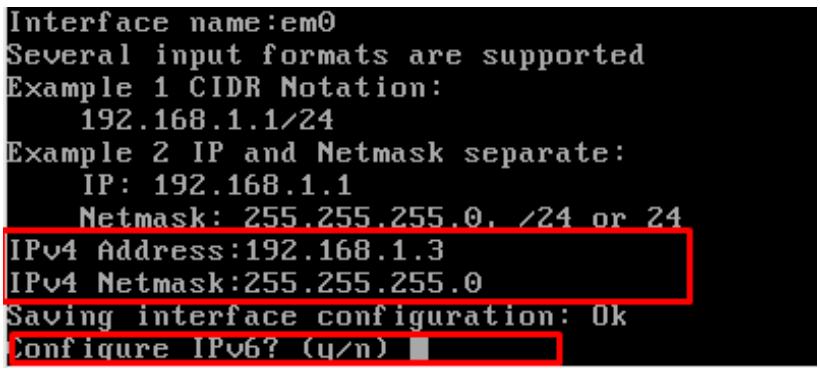

Ilustración 209: IP Asignada a Interfaz de Red.

5.-tecleamos "n" para no configurar una dirección IPv6 y damos enter para continuar, la interfaz de red se reiniciara para aplicar los cambios. Si quisiéramos asignar una configuración IPv6 teclearemos "y" en vez de "n".

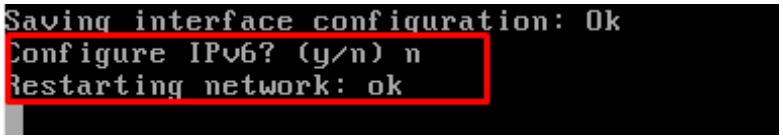

Ilustración 210: Elección de Configuración IPv6

3.9.5 Configuración de FreeNAS mediante interfaz WEB

El sistema FreeNAS permite la configuración y operación mediante una interfaz gráfica a la cual es posible entrar usando el navegador Web.

Inicio de Sesión

1.- Ingresamos mediante el navegar Web de nuestra elección a la dirección IP asignada a nuestro servidor, el usuario por defecto es root y la contraseña corresponde a la contraseña asignada al servidor durante la instalación.

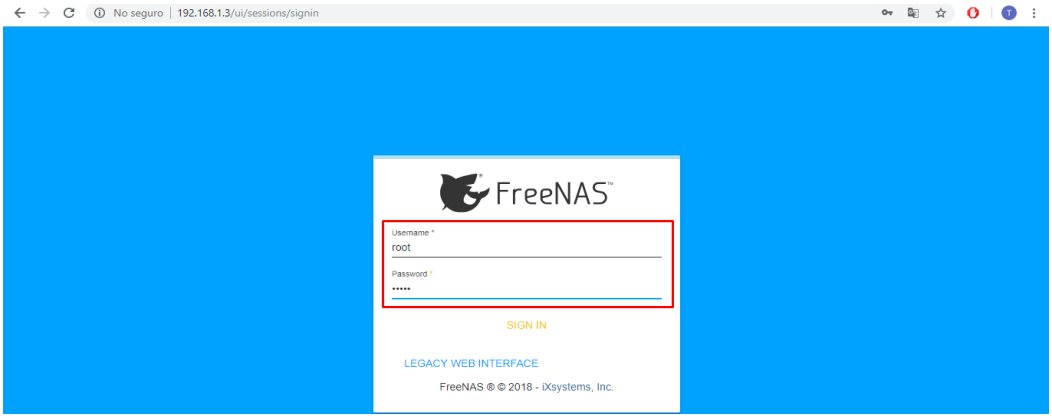

Ilustración 211: Inicio de Sesión a Portal Web FreeNAS.

2.-Una vez superada la autenticación de FreeNAS seremos dirigidos a la pantalla de inicio o Dashboard, podremos observas información básica del sistema y un panel con las opciones de configuración del sistema del lado izquierdo, como se muestra en la Ilustración 212

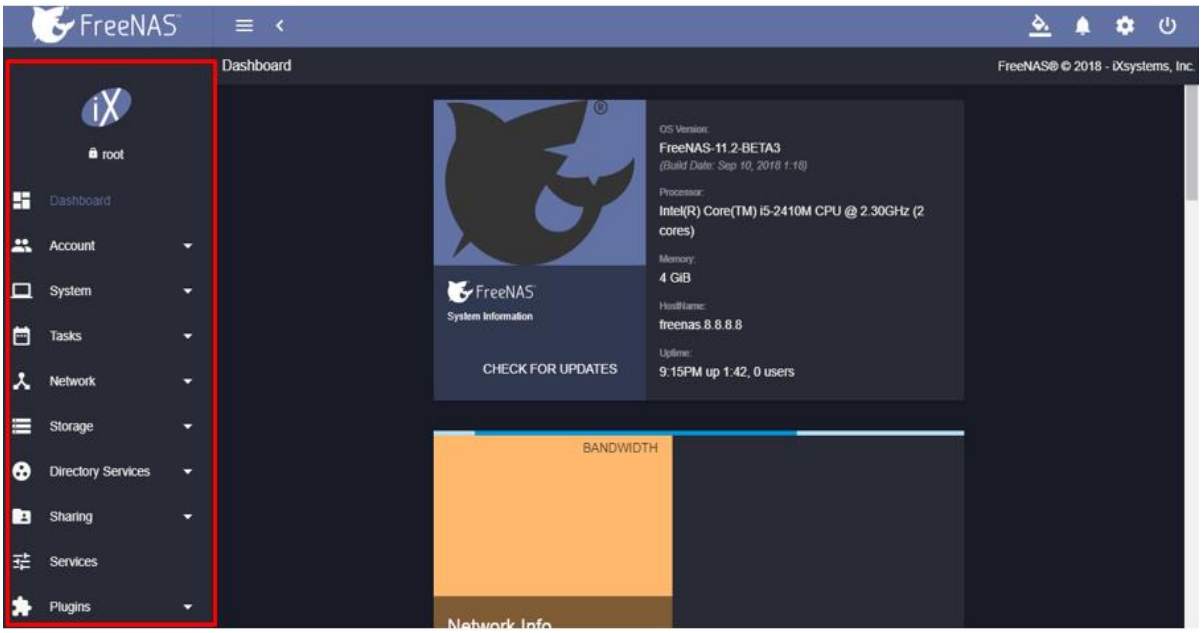

Ilustración 212: Menú Grafico de Configuración FreeNAS.

Configuración de FreeNAS

1.- Configuramos la zona horaria para nuestro servidor FreeNAS, del lado izquierdo seleccionamos la opción System -> General, en el panel de configuración general tenemos la opción Timezone donde podremos definir la zona horaria según nuestra región, En la Ilustración 213 Podemos observar el lenguaje que deseamos usar y la dirección IP para el acceso Web a nuestro servidor. Seleccionamos la opción Save para guardar los cambios.

Ilustración 213: Panel de Configuración General de Sistema FreeNAS.

2.- En la ruta Network -> Global Configuration, configuramos las opciones complementarias de nuestro Servidor, si queremos que tenga acceso a la red definimos el servidor DNS así como la puerta de enlace. En la Ilustración 214 se define la puerta de enlace como 192.168.1.1 y el DNS 8.8.8.8

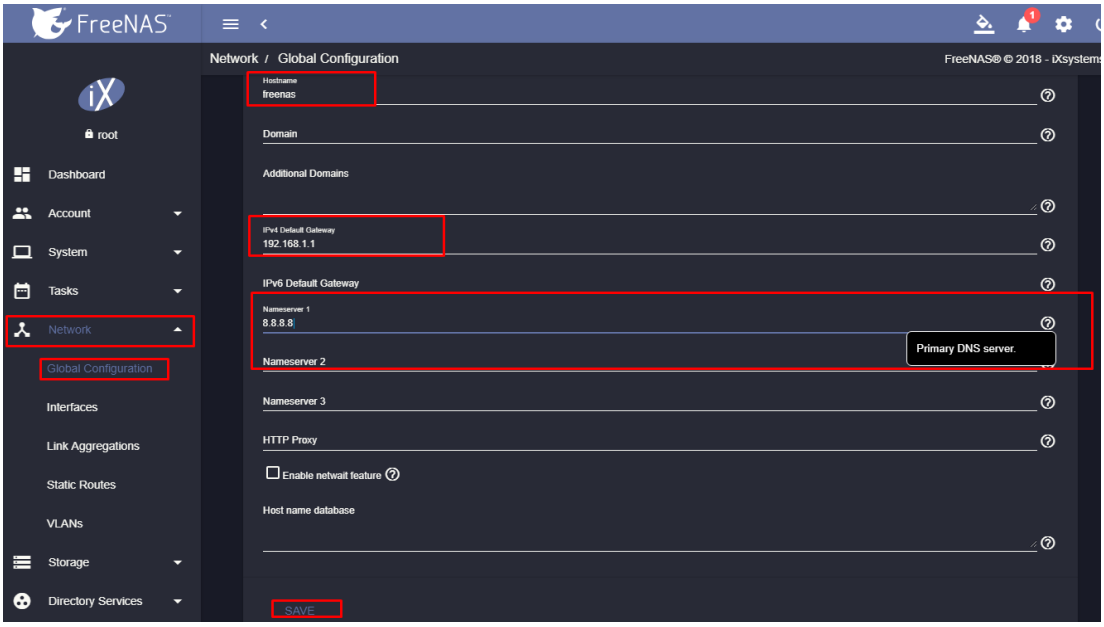

Ilustración 214: configuración Complementaria de Red.

Unidad de almacenamiento

1.-Creamos una unidad de almacenamiento en nuestro servidor FreeNAS, en la ruta Storage -> Pools, seleccionamos el símbolo de más para agregar una nueva unidad.

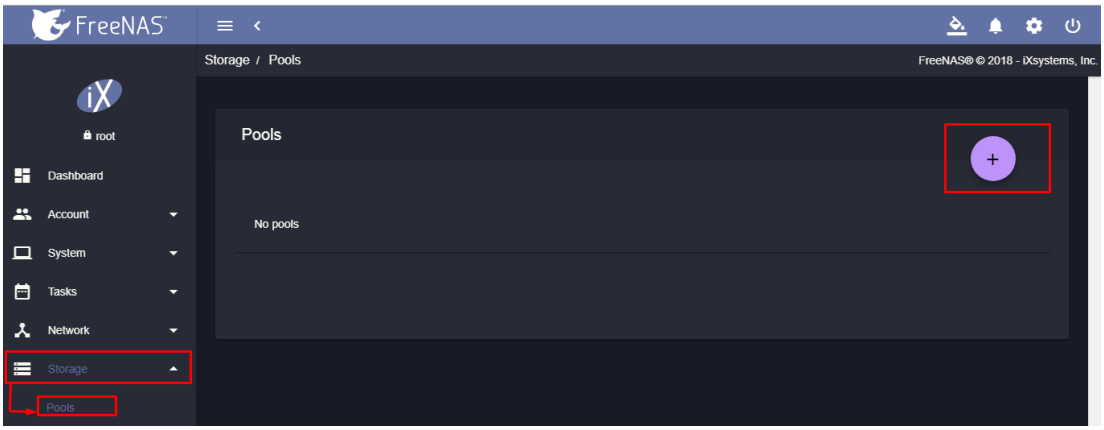

Ilustración 215: Ruta para Agregar Unidades de Almacenamiento en FreeNAS.

2.-Marcamos la opción Create new pool y damos clic sobre CREATE POOL.

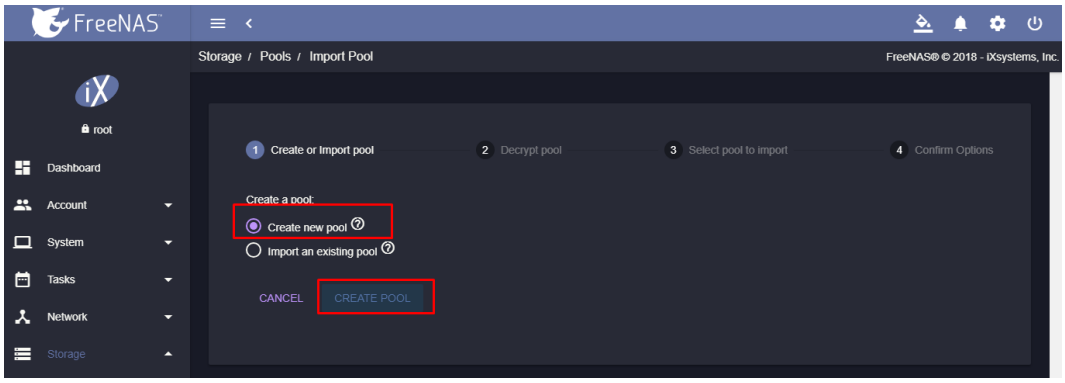

Ilustración 216: Crear Nueva Unidad de Almacenamiento.

3.- Asignamos un nombre a nuestra unidad y seleccionamos los discos que usaremos para el almacenamiento. Damos clic sobre el ícono de flecha apuntando a la derecha para poder asignar el tipo de arreglo que usaremos en nuestro almacenamiento.

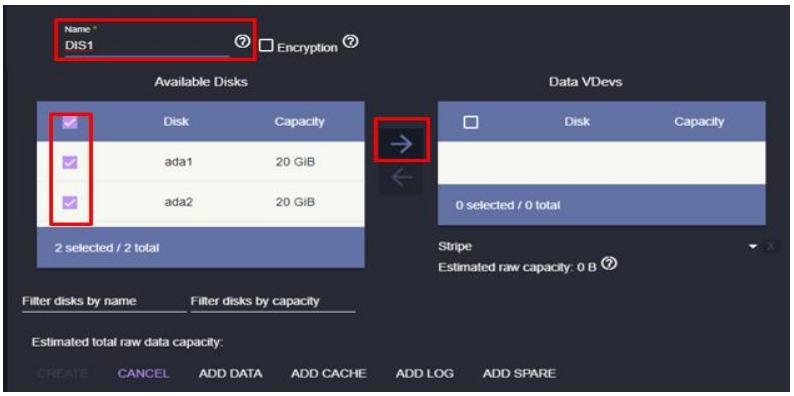

Ilustración 217: Asignación de Discos para Almacenamiento.

4.-Asignamos el tipo de arreglo que usaremos, como solo tenemos dos discos usaremos un arreglo espejo, notemos que usando dos discos de 20 GB en arreglo espejo tendremos 18 GB para ser usados como almacenamiento para los usuarios. Damos clic en la opción CREATE para crear la nueva unidad.

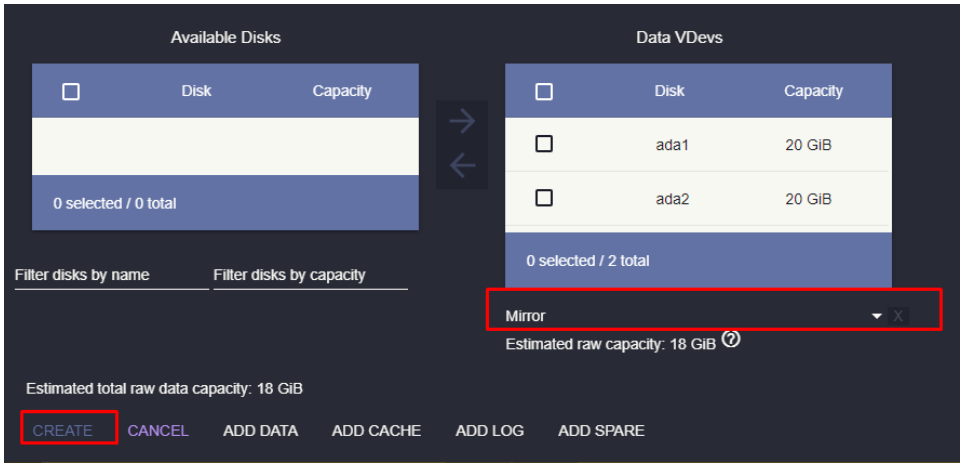

Ilustración 218: Definición del Modo de Almacenamiento.

5.- Marcamos la opción de confirmar, y damos clic sobre CREATE POOL. La unidad de almacenamiento ha sido creada.

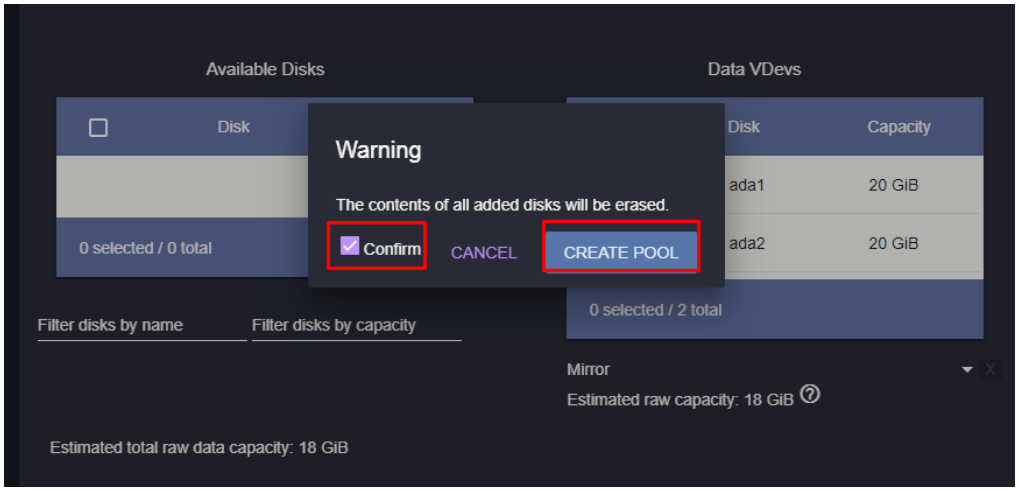

Ilustración 219: Confirmación de Creación de Disco.

6.- En la ruta Storage -> Pools, podremos observar la unidad creada.

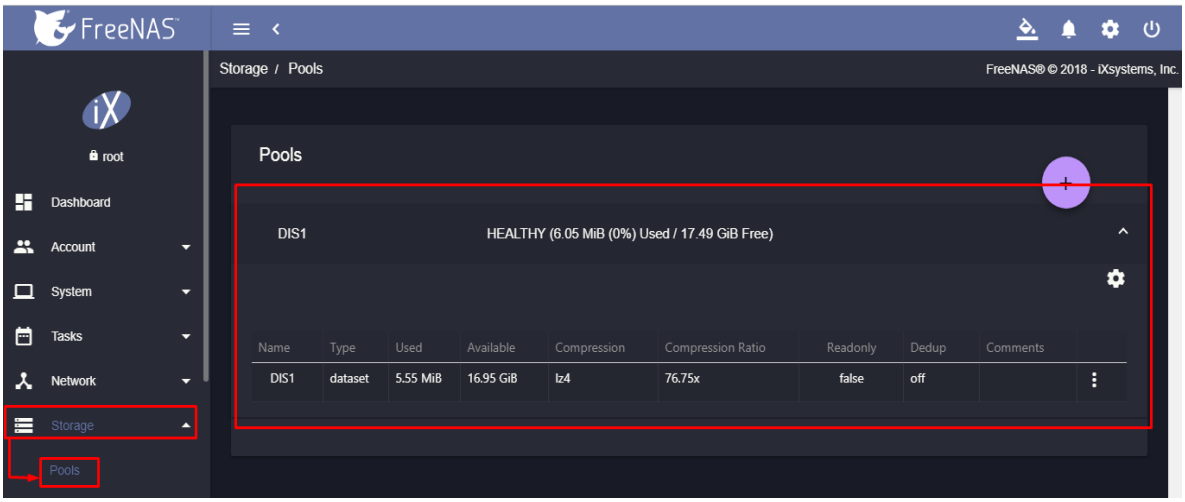

Ilustración 220: Lista de Discos FreeNAS.

Creación de Grupos

1.-En la ruta Account -> Groups, seleccionamos el ícono con el símbolo "mas" para agregar un nuevo grupo.

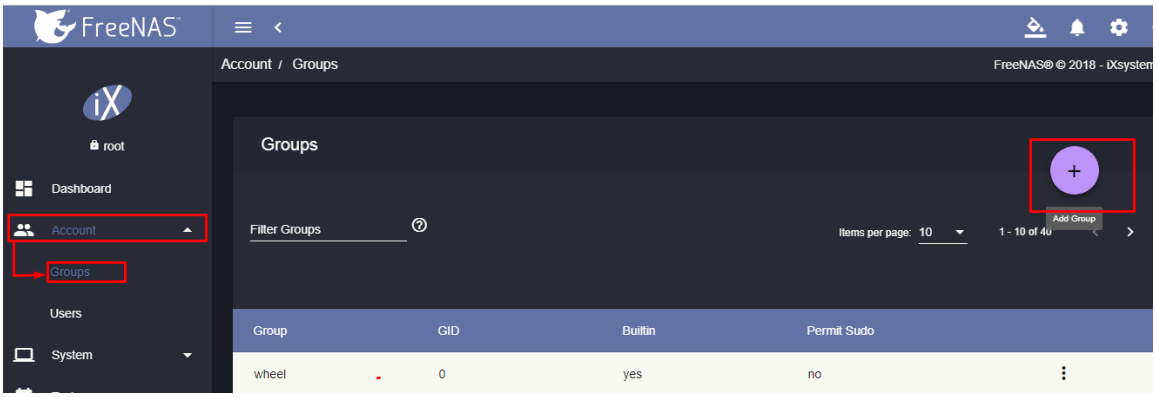

Ilustración 221: Ruta para la Creación de Grupos en FreeNAS.

2.-Definimos algunos parámetros esenciales para la creación del nuevo usuario, GID: Es un número de 4 dígitos que identificara al grupo, Name: Nombre del grupo y la opción para que los usuarios en el grupo puedan ingresar como súper usuarios. Damos clic sobre la opción SAVE para guardar los cambios y crear el grupo.

Ilustración 222: Parámetros de Grupo.

Creación de Usuarios

1.-En la ruta Account -> Users, damos clic sobre el ícono con el símbolo "mas" para agregar un nuevo usuario.

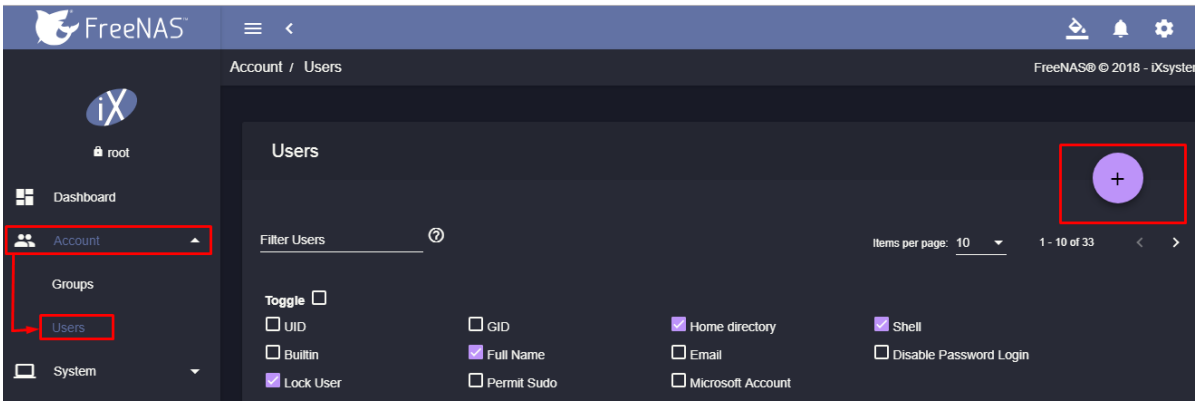

Ilustración 223: Ruta para la Creación de Nuevos Usuarios.

2.-En el panel de configuración llenamos los datos del nuevo usuario, es obligatorio asignar un nombre de usuario, nombre completo y una contraseña.

Ilustración 224: Panel de Configuración de Usuario (Parte 1).

Seleccionamos la ruta o carpetas a las que tendrá acceso el usuario así como los permisos que tendrás sobre esta carpeta. Damos clic en la opción SAVE para guardar los cambios y crear el nuevo usuario.

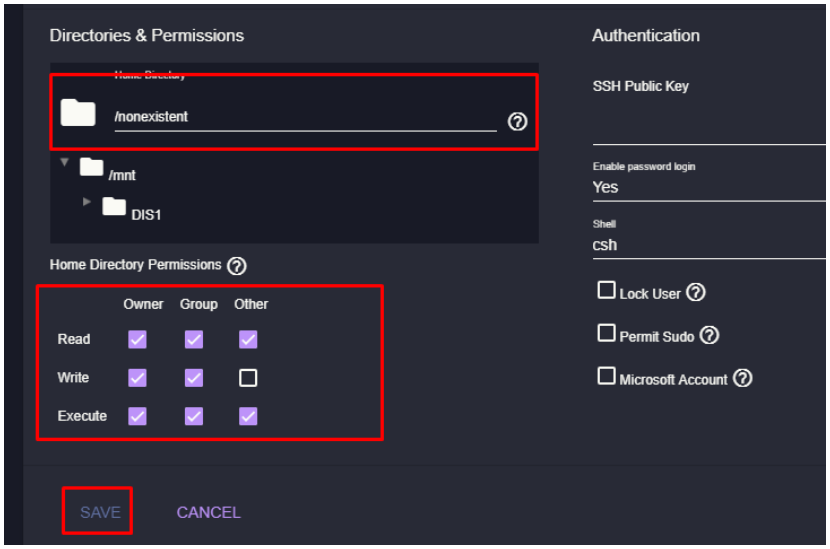

Ilustración 225: Panel de Configuración de Usuario (Parte 2).

3.-Podremos ver que el Usuario se ha creado con los parámetros asignados.

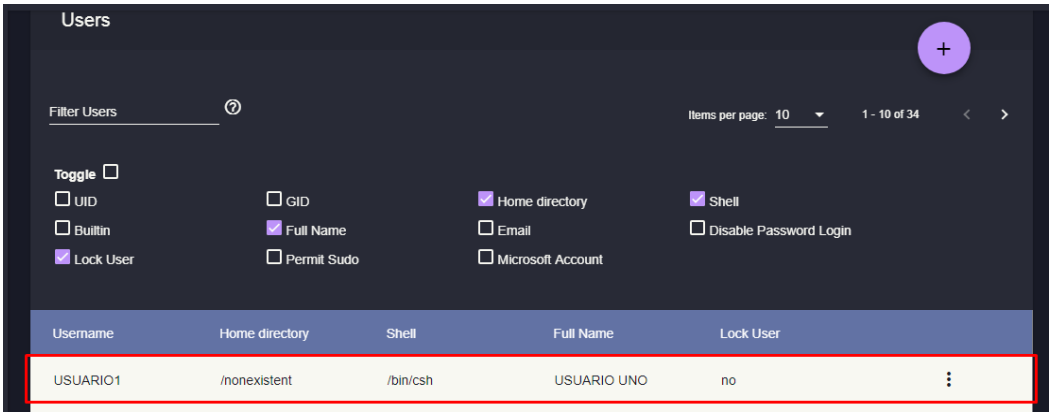

Ilustración 226: Lista de Usuarios.

Unidad compartida

Creamos una unidad compartida para equipos Windows SMB.

SMB: “Windows admite el tráfico para compartir archivos e impresoras mediante el protocolo Bloque de mensajes de servidor (SMB, Server Message Block) que se hospeda directamente en TCP.” https://support.microsoft.com/es-mx/help/204279/direct-hosting-of-smb-over-tcp-ip (Microsoft 2018, 2018)

1.-En la ruta Sharing -> Windows (SMB) Shares, Seleccionamos el ícono con el símbolo “mas” para crear la nueva carpeta.

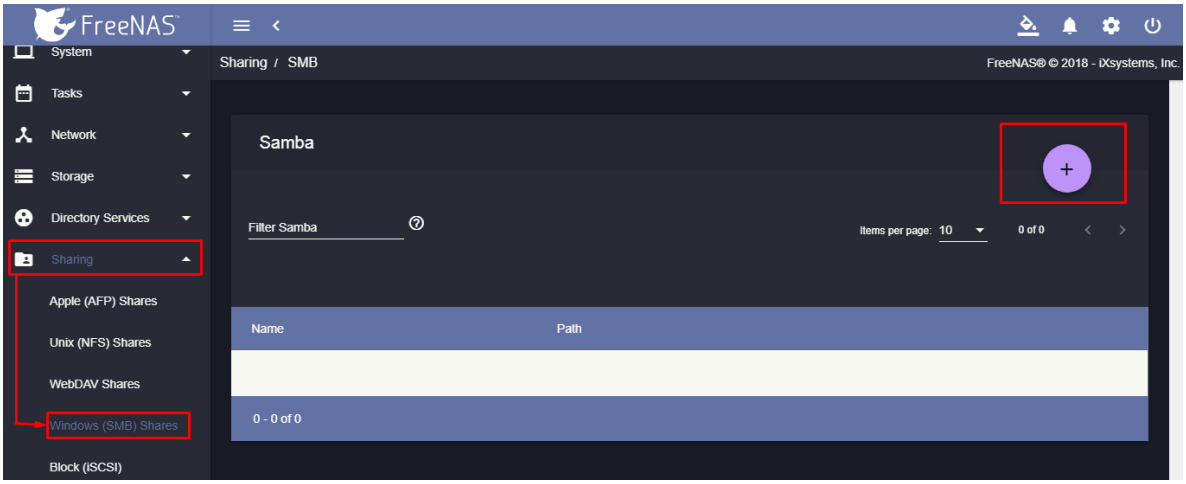

Ilustración 227: Ruta para la Creación de Carpeta SMB.

Elegimos la unidad donde se encontrará la carpeta, en la Ilustración 228 se usa la unidad DS1, asignamos un nombre a nuestra carpeta. Seleccionamos la opción SAVE para guardar los cambios y crear la carpeta.

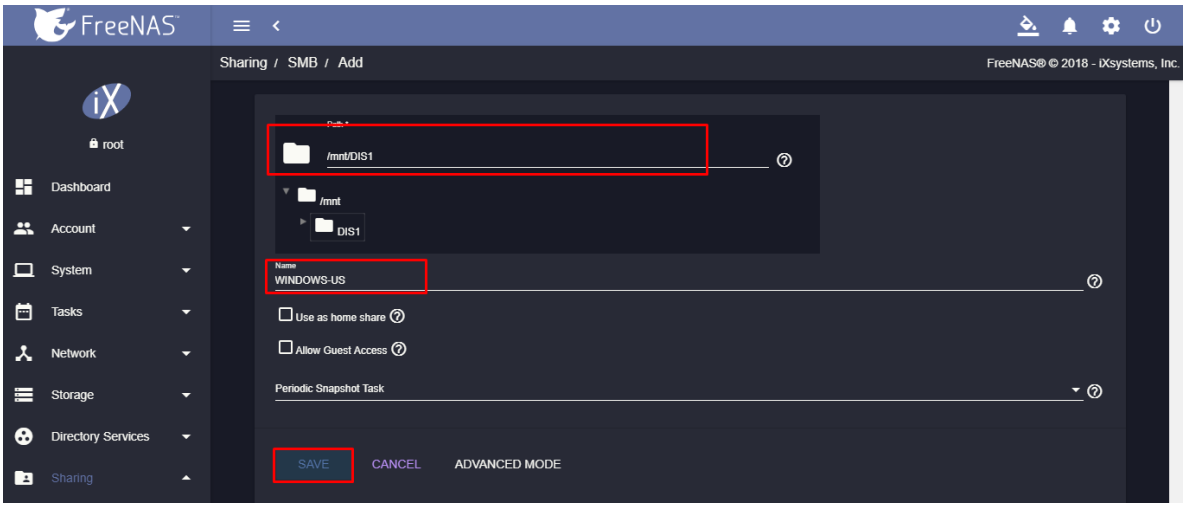

Ilustración 228: Asignación de Ruta.

Asignación de Permisos

1.-En la ruta Account -> Users, seleccionamos la opción Edit del usuario que deseamos otorgar los permisos a la carpeta WINDOWS-US.

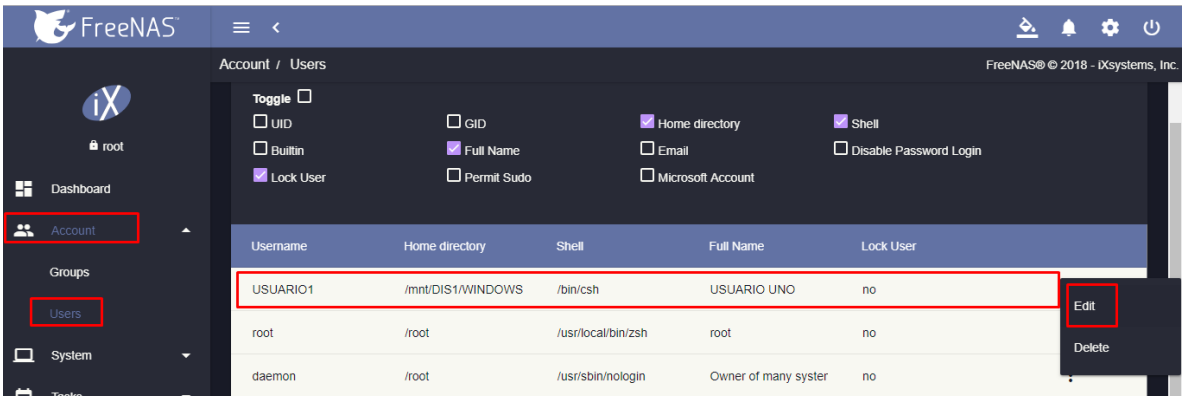

Ilustración 229: Ruta para la Modificación de Usuarios.

2.-En la opción Home Directory podemos elegir la carpeta WINDOWS-US además de definir los permisos que el usuario tendrá en la carpeta. Seleccionamos la opción SAVE para guardar los cambios.

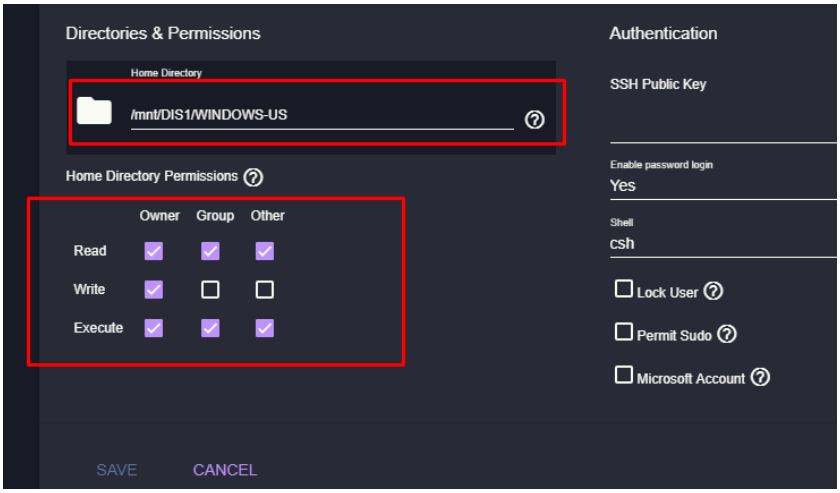

Ilustración 230: Asignación de Permisos a Carpeta.

3.-Probamos el acceso a la carpeta desde un equipo en la red, desde el explorador de archivos ingresamos al servidor FreeNAS con la IP \\192.168.1.3, usamos el usuario y contraseña definidos para el usuario que tendrá acceso a la carpeta.

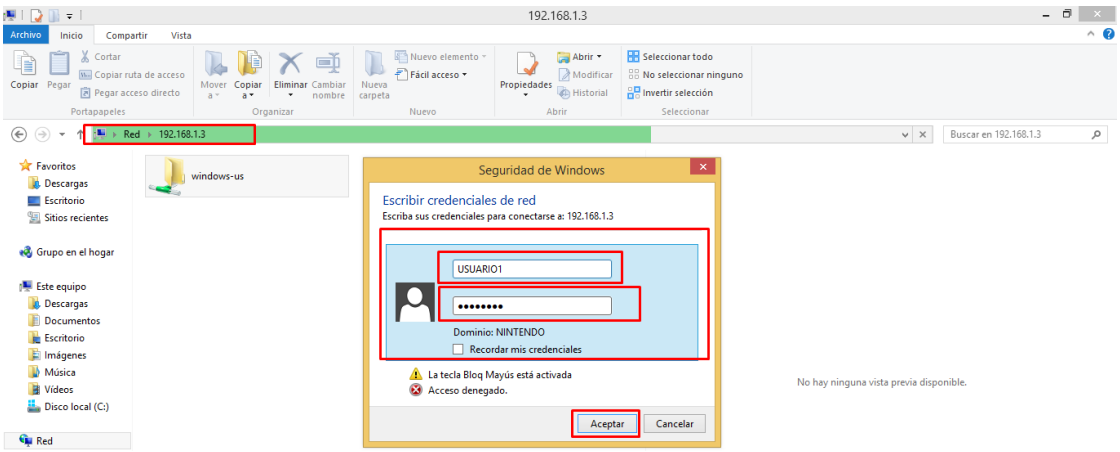

Ilustración 231: Acceso a la Carpeta SMB desde equipo Windows

4.-Veremos que tenemos acceso a la carpeta WINDOWS-US.

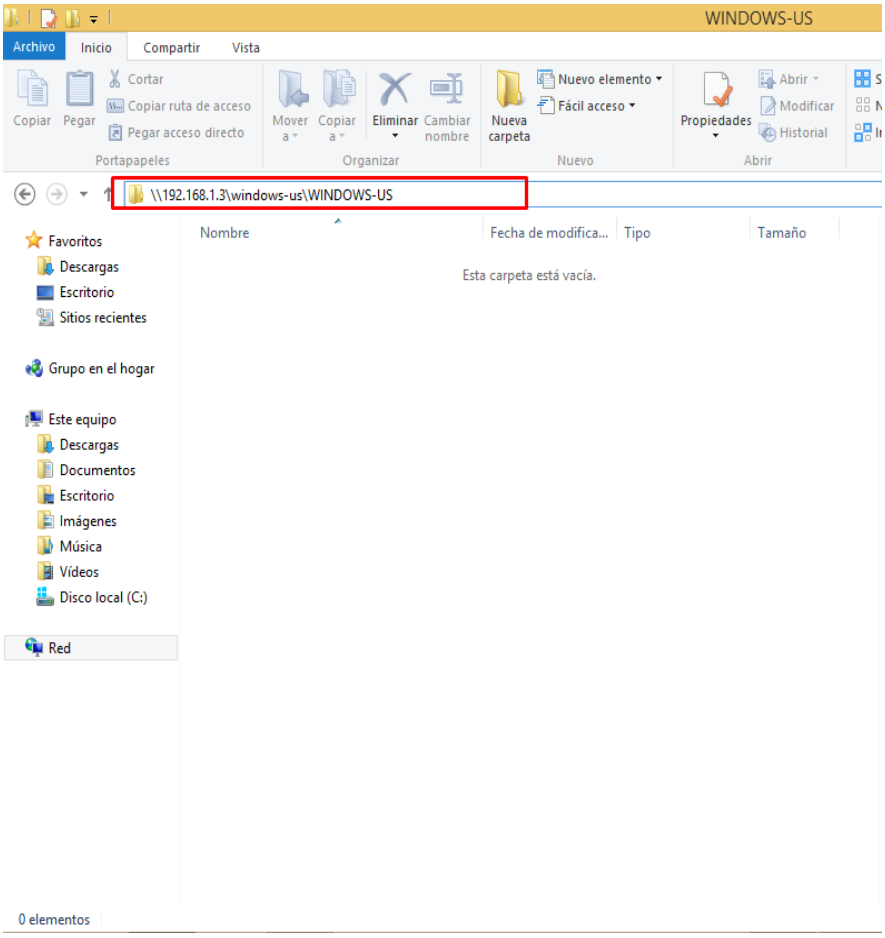

Ilustración 232: Carpeta SMB desde Equipo Windows.

5.- Es posible agregar el espacio de almacenamiento como una unidad de red para que los usuarios almacenen su información en esta carpeta o crear una copia de seguridad programada de los equipos en la unidad en red creada.

3.10 Conclusión

Una vez realizada la instalación en ambiente controlado, se define que el alcance de los sistemas planteados sí cumple con las necesidades de este proyecto y que es posible su adaptación a cualquier tipo de entorno, para todas aquellas organizaciones que busquen la implementación de una correcta administración de los siguientes recursos informáticos: Firewall, Conexiones VPN, Administración de Red, Monitoreo de Recursos Informáticos y Administración de Respaldos. Por tal motivo se considera que los sistemas cumplen con las necesidades del proyecto siendo estas:

- De bajo costo (El costo de Licenciamiento es 0)
- Adaptables a hardware.
- Existe amplia y gratuita documentación en línea.
- Cuentan con equipos dedicados y soporte especializado, si así lo desea la organización.
- Soluciones comparables a aplicaciones de pago.

Estas características y alcances los podemos ver comparados en las siguientes tablas:

- Tabla 1: Comparación de características principales de herramientas de seguridad de red
- Tabla 2: Comparación de costo usando Herramientas con Hardware adaptable
- Tabla 3: Comparación de costo usando Herramientas con Hardware dedicado
- Tabla 4: Comparativa de herramientas de monitoreo
- Tabla 5: Característica para la instalación de herramientas de Monitoreo
- Tabla 6: Comparación de Costo de Herramientas de Monitoreo
- Tabla 7: Herramientas de Almacenamiento en Red, Características y Costo

Por este motivo se plantean las propuestas costo beneficio para las organizaciones en los temas:

- 3.11 **Solución para VYCISA**
- 3.12 **Solución para INDESA**
- 3.13 **Solución para Distribuidora de Juguetes Anónima**

3.11 Solución para VYCISA

Se presenta una solución para la empresa "Vidrios y Cristales Industrializados, S.A. de CV.", la propuesta incluye el uso de las 3 herramientas mostradas en el proyecto. Dadas las características de la empresa se recomienda la implementación de:

- Servidor PfSense
- Servidor Zabbix
- Servidor FreeNAS

3.11.1 Servidor PfSense en VYCISA

Funciones del Servidor PfSense para empresa VYCISA:

- Separación de la RED por áreas.
- Administración de Reglas para cada una de las redes LAN y VLAN a gestionar.
- Creación de Portal cautivo para la gestión de usuarios en la red Wiffi.
- VPN para gestión remota de Servidores y aplicaciones.
- Balanceo de Cargas (Función opcional, requiere el uso de una interfaz de red para la conexión a internet alternativa).

Existen dos opciones a considerar para la instalación de PfSense, usando hardware dedicado y hardware adaptable.

Opción de Implementación usando hardware adaptable:

Las características mínimas para la instalación de un servidor PfSense en hardware no dedicado son:

- CPU mínimo de 600 MHz
- RAM mínima de 512 MB
- 4 GB mínimo de espacio de almacenamiento
- Una o más tarjetas de red compatibles

Se recomienda usar 2 GB de memoria RAM para una operación fluida en el servidor, al reutilizar equipos la empresa solo invertirá en las tarjetas de red que se usaran como interfaz en el servidor.

El costo promedio en línea de una tarjeta de red con 1 Puerto Gigabit Rj45 es de $250 pesos 00/100 M.N.

En caso de realizar la compra de un equipo con características para la implementación de PfSense existe una amplia forma de adaptación por parte del Software pudiendo encontrar en línea equipos desde $2,000 pesos 00/100 M.N.

Opción de Implementación usando hardware dedicado:

Usando un dispositivo dedicado (appliance PfSense), por las características de la empresa se recomienda el uso del appliance SG-3100 con un costo de $349 dólares, el dispositivo SG-3100 cuenta con dos puertos Gigabit Ethernet que pueden ser usados como puertos de conexión WAN (Función usada para el balanceo de cargas), o uno WAN y otro LAN además de cuatro puertos LAN para más información sobre el dispositivo es posible consultar la descripción en: "https://store.netgate.com/SG-3100.aspx" (Rubicon Communications, LLC, s.f.).

3.11.2 Servidor Zabbix en VYCISA

Funciones del Servidor Zabbix para empresa VYCISA:

- Monitoreo de equipos conectados a la red.
- Programación de alertas preventivas.
- Envió de alertas por correo electrónico.

Los requisitos mínimos para la instalación del Servidor Zabbix son:

- RAM: 128 MB (Recomendación para VYCISA 512 MB para el óptimo monitoreo)
- Espacio en disco: 256 MB (Recomendación para VYCISA 10 GB o más para almacenar registros de monitoreo)

Por sus características el Servidor se podrá instalar de forma virtual en algún equipo en la red o realizar una instalación física reutilizando un equipo que cubra las características de instalación.

3.11.3 Servidor FreeNAS en VYCISA

Implementar el Sistema FreeNAS como parte del plan de prevención de desastres, usando el Servidor FreeNAS para crear y gestionar unidades de almacenamiento en red dentro de las cuales se programaran los respaldos de los equipos y servidores deseados, además existe la posibilidad de implementar unidades de almacenamiento en red para los usuarios.

La implementación del Servidor FreeNAS con hardware no dedicado requiere un equipo con:

- 8 GB de memoria RAM.
- 32 GB para la instalación (El disco donde se instale el sistema no podrá ser usado como unidad de almacenamiento).
- Discos duros para la creación de unidades de almacenamiento.

Aunque es posible implementar el servidor FreeNAS con 4 GB de momería se nos recomienda el uso de 8 GB para garantizar la correcta operación del sistema. El costo de equipos con estas características es muy variado entre marcas con la posibilidad de encontrar equipos de un costo de $3,000 00/100 pesos M.N. o mas *"https://listado.mercadolibre.com.mx/cpu-8gb-ram#D[A:cpu-8gb-ram]"* (DeRemate.com de México S. de R.L. de C.V., s.f.), mientras que el costo promedio de unidades de disco duro de 2 TB es de $1,500 pesos 00/100 M.N.

Implementación de FreeNAS con equipo dedicado

Para la empresa VYCISA se recomiendan los dispositivos mini disponibles en el portal Amazon *"https://www.amazon.com/l/9199424011" (Amazon.com, Inc. o sus afiliados, s.f.):*

Modelo FreeNAS	Almacenamiento	Costo
FreeNAS Mini	4TB	$1,284.00 Dólares
FreeNAS Mini	8TB	$1399.00 Dólares
FreeNAS Mini	16TB	$2,149.00 Dólares

Tabla 8: Ejemplo de Costos FreeNAS Mini

Es posible adquirir equipos más robustos solicitando una cotización en el portal: *"http://www.freenas.org/freenas-certified-servers/"* (iXsystems, Inc., s.f.).

3.12 Solución para INDESA

Solución para la empresa "INDUSTRIA NACIONAL DE DETERGENTES S.A. de CV.", la propuesta incluye el uso de las 3 herramientas mostradas en el proyecto:

- Servidor PfSense
- Servidor Zabbix
- Servidor FreeNAS

3.12.1 Servidor PfSense en INDESA

Funciones del Servidor PfSense para empresa INDESA:

- Separación de la RED por áreas.
- Administración de Reglas para cada una de las redes LAN y VLAN a gestionar.
- Creación de Portal cautivo para la gestión de usuarios en la red Wifi.
- VPN para gestión remota de Servidores y aplicaciones.
- Balanceo de Cargas (Función opcional, requiere el uso de una interfaz de red para la conexión a internet alternativa).

Existen dos opciones a considerar para la instalación de PfSense, usando hardware dedicado y hardware adaptable.

Opción de Implementación usando hardware adaptable:

Por las características y dimensiones de la empresa se recomienda el uso de un equipo con las siguientes características:

- CPU con Arquitectura de x64
- RAM mínima de 2 GB
- 10 GB mínimo de espacio de almacenamiento
- Un puerto de Red para cada Área que se desea utilizar
- 1 puerto de Red para cada acceso a internet.

Al reutilizar equipos la empresa solo invertirá en las tarjetas de red que se usarán como interfaz en el servidor. El costo promedio en línea de una tarjeta de red con 1 Puerto Gigabit Rj45 es de $250 pesos 00/100 M.N. o más, En caso de realizar la compra de un equipo con características para la implementación de PfSense existe una amplia forma de adaptación por parte del Software pudiendo encontrar en línea equipos desde $2,000 pesos 00/100 M.N.

Opción de Implementación usando hardware dedicado:

Usando un dispositivo dedicado (appliance PfSense), por las características de la empresa se recomienda el uso del appliance SG-3100 con un costo de $349 dólares, el dispositivo SG-3100 cuenta con dos puertos Gigabit Ethernet que pueden ser usados como puertos de conexión WAN (Función usada para el balanceo de cargas), o uno WAN y otro LAN además de cuatro puertos LAN para más información sobre el dispositivo es posible consultar la descripción en: "https://store.netgate.com/SG-3100.aspx" (Rubicon Communications, LLC, s.f.).

3.12.2 Servidor Zabbix en INDESA

Funciones del Servidor Zabbix para empresa INDESA:

- Monitoreo de equipos conectados a la red.
- Programación de alertas preventivas.
- Envió de alertas por correo electrónico.

Los requisitos para la instalación del Servidor Zabbix son:

- RAM: 128 MB (Recomendación para INDESA 2 GB para el óptimo monitoreo).

- Espacio en disco: 256 MB (Recomendación para INDESA 10 GB para almacenar registros de monitoreo, entre mayor espacio mayor será el número de registros que se podrán almacenar).
- Numero de CPU: Dos.

Es posible la instalación de forma virtual el Servidor en un equipo en la red o su instalación física reutilizando un equipo que cubra con los requisitos de instalación.

3.12.3 Servidor FreeNAS en INDESA

Implementar el Sistema FreeNAS para crear y gestionar unidades de almacenamiento en red dentro de las cuales se programarán los respaldos de los equipos y servidores deseados, además de implementar unidades de almacenamiento en red para los usuarios.

La implementación del Servidor FreeNAS con hardware no dedicado requiere un equipo con:

- 8 GB de memoria RAM.
- 32 GB para la instalación (El disco donde se instale el sistema no podrá ser usado como unidad de almacenamiento).
- Discos duros para la creación de unidades de almacenamiento.

Aunque es posible implementar el servidor FreeNAS con 4 GB de momería es recomendable el uso de 8 GB para garantizar la correcta operación del sistema. Es posible la reutilización de Hardware para el armado de una unidad piloto. Se puede adquirir un equipo dedicado FreeNAS, se recomienda los dispositivos mini disponibles en el portal Amazon *"https://www.amazon.com/l/9199424011" (Amazon.com, Inc. o sus afiliados, s.f.):*

Modelo FreeNAS	Almacenamiento	Costo
FreeNAS Mini	4TB	$1,284.00 Dólares
FreeNAS Mini	8TB	$1399.00 Dólares
FreeNAS Mini	16TB	$2,149.00 Dólares

Tabla 9: Ejemplo de Costos FreeNAS Mini

Es posible adquirir equipos más robustos solicitando una cotización en: *"http://www.freenas.org/freenas-certified-servers/"* (iXsystems, Inc., s.f.).

3.13 Solución para Distribuidora de Juguetes Anónima

Se presenta una solución para la empresa "Distribuidora de Juguetes Anónima", se incluye el uso de las 3 herramientas mostradas en el proyecto:

- Servidor PfSense
- Servidor Zabbix
- Servidor FreeNAS

3.13.1 Servidor PfSense en Distribuidora de Juguetes Anónima

Funciones del Servidor PfSense para empresa Distribuidora de Juguetes Anónima:

- VPN para gestión remota de Sucursales.
- Seguridad perimetral para la conexión remota de sucursales.

Se sugiere la implementación del servidor PfSense para gestionar la conexión remota a las sucursales, existen dos opciones a considerar para la instalación de PfSense, usando hardware dedicado y hardware adaptable.

Opción de Implementación usando hardware adaptable:

Las características mínimas para la instalación de un servidor PfSense en hardware no dedicado son:

- CPU mínimo de 600 MHz
- RAM mínima de 512 MB
- 4 GB mínimo de espacio de almacenamiento
- Una o más tarjetas de red compatibles

Para tener una mejor operación se sugiere el uso de 2 GB de memoria RAM en el servidor, al reutilizar equipos la empresa solo invertirá en las tarjetas de red que se usaran como interfaz en el servidor. El costo promedio en línea de una tarjeta de red con 1 Puerto Gigabit Rj45 es de $250 pesos 00/100 M.N.
En caso de realizar la compra de un equipo con características para la implementación de PfSense existe una amplia forma de adaptación por parte del Software pudiendo encontrar en línea equipos desde $2,000 pesos 00/100 M.N.

Opción de Implementación usando hardware dedicado:

Usando un dispositivo dedicado (appliance PfSense), por las características de la empresa se recomienda el uso del appliance SG-3100 con un costo de $349 dólares, el dispositivo SG-3100 cuenta con dos puertos Gigabit Ethernet que pueden ser usados como puertos de conexión WAN (Función usada para el balanceo de cargas), o uno WAN y otro LAN además de cuatro puertos LAN para más información sobre el dispositivo es posible consultar la descripción en: "https://store.netgate.com/SG-3100.aspx" (Rubicon Communications, LLC, s.f.).

3.13.2 Servidor Zabbix en Distribuidora de Juguetes Anónima

Funciones del Servidor Zabbix para empresa Distribuidora de Juguetes Anónima:

- Monitoreo de equipos remotos y locales.
- Programación de alertas preventivas.
- Monitoreo de recursos gráficos mediante mapas.
- Envió de alertas por correo electrónico.

Los requisitos mínimos para la instalación del Servidor Zabbix son:

- RAM: 128 MB (Recomendación para VYCISA 512 MB para el óptimo monitoreo)
- Espacio en disco: 256 MB (Recomendación para VYCISA 10 GB para almacenar registros de monitoreo)

Por sus características el Servidor se podrá instalar de forma virtual en algún equipo en la red para el monitoreo de equipos locales.

Panorama de instalación Zabbix Remoto mediante VPN:

Monitorear los equipos remotos de las diferentes sucursales, conectando el agente Zabbix mediante una conexión de túnel privado (VPN) creado por la herramienta PfSense.

Panorama de instalación Zabbix Remoto:

Publicar el servidor Zabbix, de esta forma los agentes Zabbix no necesitara una conexión VPN para comunicarse.

3.13.3 Servidor FreeNAS en Distribuidora de Juguetes Anónima

Implementar el Servidor FreeNAS para crear y gestionar unidades de almacenamiento en red dentro de las cuales se programaran los respaldos de los equipos y servidores deseados, creación de repositorio remoto para sucursales.

La implementación del Servidor FreeNAS con hardware no dedicado requiere un equipo con:

- 8 GB de memoria RAM.
- 32 GB para la instalación (El disco donde se instale el sistema no podrá ser usado como unidad de almacenamiento).
- Discos duros para la creación de unidades de almacenamiento.

Aunque es posible implementar el servidor FreeNAS con 4 GB de momería es recomendable el uso de 8 GB para garantizar la correcta operación del sistema. Es posible la reutilización de Hardware para el armado de una unidad piloto.

Implementación con hardware dedicado para FreeNAS, se recomienda los dispositivos mini disponibles en el portal Amazon *"https://www.amazon.com/l/9199424011" (Amazon.com, Inc. o sus afiliados, s.f.):*

Modelo FreeNAS	Almacenamiento	Costo
FreeNAS Mini	4TB	$1,284.00 Dólares
FreeNAS Mini	8TB	$1399.00 Dólares
FreeNAS Mini	16TB	$2,149.00 Dólares

Tabla 10: Ejemplo de Costos FreeNAS Mini

Si se desea adquirir un equipo más robusto es posible solicitar una cotización en: *"http://www.freenas.org/freenas-certified-servers/"* (iXsystems, Inc., s.f.).

Bibliografía

Amazon.com, Inc. o sus afiliados. (s.f.). *Shop IXSYSTEMS, INC*. Recuperado el 1 de Noviembre de 2018, de amazon: https://www.amazon.com/l/9199424011

Belkin International, Inc. (s.f.). *¿Qué es un portal cautivo?* Recuperado el 09 de AGOSTO de 2018, de LINKSYS: https://www.linksys.com/es/r/resource-center/business-solutions/portal-cautivo/

Benchimol, c. p. (2011). *Hacking, Desde Cero* (Primera ed.). Buenos Aires: Fox Andina. Recuperado el 19 de 06 de 2018, de http://www.tugurium.com/docs/HakingCero.pdf

Deciso B.V. (s.f.). *Apoyo Comercial* . Obtenido de OPNsense: https://opnsense.org/support-overview/commercial-support/

Deciso B.V. (s.f.). *Manual de usuario*. Recuperado el 22 de Septiembre de 2018, de Documentos: https://wiki.opnsense.org/manual.html

Dell. (24 de Abril de 2018). *Descripción de los tipos de disco duro, RAID y controladoras RAID en los Servidores Dell PowerEdge y chasis del servidor Blade*. Obtenido de Soporte: https://www.dell.com/support/article/mx/es/mxbsdt1/sln129581/descripci%C3%B3n-de-los-tipos-de-disco-duro-raid-y-controladoras-raid-en-los-servidores-dell-poweredge-y-chasis-del-servidor-blade?lang=es

DeRemate.com de México S. de R.L. de C.V. (s.f.). *Cpu 8gb ram*. Recuperado el 01 de Noviembre de 2018, de mercado libre: https://listado.mercadolibre.com.mx/cpu-8gb-ram#D[A:cpu-8gb-ram]

Estrada, A. C. (2011). *Seguridad Por Niveles.* Madrid: DarFE Learning Consulting, S.L. Recuperado el 20 de 07 de 2018, de http://www.darfe.es/joomla/index.php/descargas/finish/5-seguridad/26-libro-seguridad-por-niveles/0

Estrada, A. C. (2016). *Seguridad en Redes.* Madrid: DarFE Learning Consulting, S.L. Recuperado el 25 de 07 de 2018, de http://www.darfe.es/joomla/index.php/descargas/finish/5-seguridad/1310-libro-seguridad-en-redes/0

FreeBSD Project. (s.f.). *El proyecto FreeBSD*. Recuperado el 27 de Agosto de 2018, de FreeBSD: https://www.freebsd.org/

GIGA-BYTE Technology Co., Ltd. (s.f.). *GA-G31M-ES2C (rev. 1.x)*. Recuperado el 02 de Octubre de 2018, de GIGABYTE: https://www.gigabyte.com/Motherboard/GA-G31M-ES2C-rev-1x#ov

GitHub , Inc. (s.f.). *Apache License 2.0*. Recuperado el 27 de Agosto de 2018, de pfsense/pfsense: https://github.com/pfsense/pfsense/blob/master/LICENSE

GNU Operating System. (12 de Junio de 2018). *¿Qué es el software libre?* Recuperado el 19 de Agosto de 2018, de El sistema operativo GNU: https://www.gnu.org/philosophy/free-sw.es.html#History

GNU Operating System. (17 de 01 de 2018). *Categorías de software libre y software que no es libre*. Obtenido de El sistema operativo GNU: https://www.gnu.org/philosophy/categories.es.html

Hine, C. F. (s.f.). *El Software Libre es una cuestión de libertad, no de precio*. Recuperado el 18 de Agosto de 2018, de Free Software Foundation: https://www.fsf.org/es/about

Huatala, L. (25 de Junio de 2018). *WPA3 Wi-Fi está aquí, y es más difícil de hackear*. Recuperado el 09 de AGOSTO de 2018, de CNET: https://www.cnet.com/news/wpa3-wi-fi-is-here-and-its-harder-to-hack/

IEEE Standards Association (IEEE-SA). (2018). *IEEE STANDARDS ASSOCIATION*. Obtenido de IEEE 802.11aq-2018: https://standards.ieee.org/findstds/standard/802.11aq-2018.html

IEEE Standards Association (IEEE-SA). (2018). *IEEE STANDARDS ASSOCIATION*. Obtenido de IEEE Std 802.11ak-2018: https://standards.ieee.org/findstds/standard/802.11ak-2018.html

IEEE Standards Association (IEEE-SA). (2018). *IEEE Standards Association (IEEE-SA)*. Obtenido de IEEE Std 802.11aj-2018: https://standards.ieee.org/findstds/standard/802.11aj-2018.html

IEEE Standards Association (IEEE-SA). (2018). *WG802.11 - Grupo de trabajo de LAN inalámbrica*. Obtenido de WG802.11 - Grupo de trabajo de LAN inalámbrica: https://standards.ieee.org/findstds/standard/802.11aq-2018.html

Industria Nacional de Detergentes, S.A. de C.V. (s.f.). *Industria Nacional de Detergentes, S.A. de C.V.* Recuperado el 21 de Agosto de 2018, de INDESA MEXICO: http://www.indesa.com.mx/

Instituto Nacional de Tecnologías de la Comunicación (INTECO). (Noviembre de 2010). *Seguridad Perimetral. Catálogo de Empresas y Soluciones de Seguridad TIC.* Obtenido de Instituto Nacional de Ciberseguridad de España: https://www.incibe.es/extfrontinteco/img/File/demostrador/monografico_catalogo_seguridad_perimetral.pdf

Intel Corporation. (02 de Octubre de 2017). *Definición de volúmenes de RAID para Intel® tecnología de almacenamiento rápido*. Obtenido de ASISTENCIA: https://www.intel.la/content/www/xl/es/support/articles/000005867/technologies.html

iXsystems. (s.f.). *Documentos*. Recuperado el 28 de Agosto de 2018, de FreeNAS ® 11.1-U6 Guía del usuario: http://doc.freenas.org/11/freenas.html

iXsystems. (s.f.). *Introduction*. Recuperado el 28 de Septiembre de 2018, de FreeNAS 11.1-U6 User Guide: http://doc.freenas.org/11/intro.html

iXsystems, Inc. (s.f.). *Caracteristicas*. Recuperado el 28 de Agosto de 2018, de FreeNAS: http://www.freenas.org/about/features/

iXsystems, Inc. (s.f.). *FreeNAS Certified Servers*. Recuperado el 25 de Septiembre de 2018, de FreeNAS: http://www.freenas.org/freenas-certified-servers/

iXsystems, Inc. (s.f.). *FreeNAS Mini & Mini XL*. Recuperado el 25 de Septiembre de 2018, de FreeNAS: http://www.freenas.org/freenas-mini/

iXsystems, Inc. (s.f.). *TRAINING FROM THE EXPERTS*. Recuperado el 28 de Septiembre de 2018, de iXsystems: https://www.ixsystems.com/ix-university/

iXsystems, Inc. (s.f.). *ZFS*. Recuperado el 2 de Septiembre de 2018, de FreeNAS: http://www.freenas.org/zfs/

Juniper Networks, Inc. . (21 de Marzo de 2018). *Descripción general de IPsec VPN*. Recuperado el 2 de Septiembre de 2018, de Juniper Networks: https://www.juniper.net/documentation/en_US/junos/topics/concept/vpn-security-overview.html

Martínez, C. V. (Mayo de 2014). *Respaldos de información (backups)*. Recuperado el 10 de AGOSTO de 2018, de Instituto de Ingeniería, UNAM: http://www.iingen.unam.mx/es-mx/Publicaciones/GacetaElectronica/GacetaMayo2014/Paginas/Respaldosdeinformacion.aspx

Mclver McHoes, A., & M. Flynn, I. (2010). *Sistemas Operativos, Sexta edición.* Querétaro: CENGAGE Learning.

Microsoft. (06 de Junio de 2017). *Acerca de Windows original*, Windows 7, Windows 8.1. Recuperado el 20 de Agosto de 2018, de Soporte técnico de Microsoft: https://support.microsoft.com/es-pr/help/15087/windows-genuine

Microsoft 2018. (18 de Abril de 2018). *Asignación directa de hosts de SMB a través de TCP/IP*. Recuperado el 25 de Octubre de 2018, de Soporte técnico de Microsoft: https://support.microsoft.com/es-mx/help/204279/direct-hosting-of-smb-over-tcp-ip

Nagios Enterprises, LLC. (Diciembre de 2017). *Hardware Requirements*. Recuperado el 25 de Septiembre de 2018, de Nagios XI: https://assets.nagios.com/downloads/nagiosxi/docs/Nagios-XI-Hardware-Requirements.pdf#_ga=2.40112034.1207346008.1537602885-1932980082.1537508595

Nagios Enterprises, LLC. (s.f.). *Nagios XI*. Recuperado el 25 de Septiembre de 2018, de Nagios: https://www.nagios.com/products/nagios-xi/

Nagios Enterprises, LLC. (s.f.). *Nagios XI Support & Maintenance Plans*. Recuperado el 25 de Septiembre de 2018, de Nagios: https://www.nagios.com/services/nagios-xi-support-plans/

Open BSD PF - Redundancia de cortafuegos (CARP y pfsync). (s.f.). Recuperado el 28 de Agosto de 2018, de Open BSD PF - Redundancia de cortafuegos (CARP y pfsync): https://www.openbsd.org/faq/pf/carp.html

Open Source Initiative. (22 de Marzo de 2007). *La definición de código abierto*. Recuperado el 20 de Agosto de 2018, de Open Source Initiative: https://opensource.org/osd

Open Source Initiative. (s.f.). *Acerca de la Iniciativa de Código Abierto*. Recuperado el 20 de Agosto de 2018, de Open Source Initiative: https://opensource.org/about

Open source. (s.f.). *La licencia BSD de 2 cláusulas*. Recuperado el 28 de Agosto de 2018, de Iniciativa de código abierto: https://opensource.org/licenses/BSD-2-Clause

OpenBSD. (s.f.). *OpenBSD*. Recuperado el 28 de Agosto de 2018, de OpenBSD: https://www.openbsd.org/

OpenVPN Inc. (2 de Septiembre de 2018). *Vista general del servidor de acceso*. Obtenido de OPENVPN: https://openvpn.net/index.php/access-server/overview.html

Oracle Corporation y / o sus afiliados. (s.f.). *Configuración de agrupaciones de almacenamiento RAID-Z*. Recuperado el 02 de Septiembre de 2018, de Guía de administración de Oracle Solaris ZFS: https://docs.oracle.com/cd/E19253-01/820-2314/gamtu/index.html

Oracle. (s.f.). *Download VirtualBox*. Recuperado el 25 de Octubre de 2018, de VirtualBox: https://www.virtualbox.org/wiki/Downloads

Paessler AG. (s.f.). *Configuraciones recomendadas*. Recuperado el 25 de Septiembre de 2018, de PAESSLER: https://www.es.paessler.com/prtg/requirements

Paessler AG. (s.f.). *PAESSLER SHOP*. Recuperado el 25 de Septiembre de 2018, de PAESSLER: https://shop.paessler.com/shop/prtg/new/?preselected_license=1020&_ga=2.187154159.699476633.1536195510-1882227319.1536195510

Paessler AG. (s.f.). *PRTG Network Monitor*. Recuperado el 25 de Septiembre de 2018, de PAESSLER: https://www.es.paessler.com/prtg

Panda Security, S.L. (2018). *¿Cúal es la diferencia entre un IDS y un IPS?* Obtenido de Panda Soporte Técnico: https://www.pandasecurity.com/peru/support/card?id=31463

Pete Batard. (s.f.). *Cree unidades USB arrancables fácilmente*. Recuperado el 25 de Octubre de 2018, de Rufus: https://rufus.ie/es_ES.html

Router-switch Ltd. (s.f.). *ASA5506-K9*. Recuperado el 25 de Septiembre de 2018, de Router-switch.com: http://www.router-switch.com/asa5506-k9-p-5695.html

Router-switch Ltd. (s.f.). *ASA5555-K9*. Recuperado el 25 de Septiembre de 2018, de Router-switch.com: http://www.router-switch.com/asa5555-k9-p-4622.html

Router-switch.com (HongKong Yejian Technologies Co., Ltd). (30 de Agosto de 2018). *ASA5508-K9*. Obtenido de router-switch.com: http://www.router-switch.com/asa5508-k9-p-23193.html

Rubicon Communications LLC. (s.f.). *Welcome to the pfSense Documentation site*. Recuperado el 25 de Septiembre de 2018, de Netgate Documentation: https://www.netgate.com/docs/pfsense/

Rubicon Communications, L. (. (s.f.). *The pfSense Book*. Recuperado el 20 de Septiembre de 2018, de pfSense: https://www.netgate.com/docs/pfsense/book/

Rubicon Communications, LLC (netgate). (28 de Agosto de 2018). *On Premises Firewall Appliances*. Obtenido de netgate: https://www.netgate.com/products/appliances/

Rubicon Communications, LLC (Netgate). (28 de Agosto de 2018). *Soporte global de Netgate*. Obtenido de netgate: https://www.netgate.com/support/

Rubicon Communications, LLC (Netgate). (s.f.). *Caracteristicas*. Recuperado el 27 de Agosto de 2018, de pfsense: https://www.pfsense.org/about-pfsense/features.html

Rubicon Communications, LLC (Netgate). (s.f.). *Configuración y WebGUI*. Recuperado el 27 de Agosto de 2018, de Documentación de Netgate: https://www.netgate.com/docs/pfsense/config/

Rubicon Communications, LLC (Netgate). (s.f.). *Download*. Recuperado el 02 de Octubre de 2018, de pfsense: https://www.pfsense.org/download/

Rubicon Communications, LLC (Netgate). (s.f.). *Haga un recorrido*. Recuperado el 27 de Agosto de 2018, de Descripción general de pfSense: https://www.pfsense.org/about-pfsense/

Rubicon Communications, LLC (Netgate). (s.f.). *Instalando pfSense*. Recuperado el 27 de Agosto de 2018, de Documentación de Netgate: https://www.netgate.com/docs/pfsense/install/installing-pfsense.html

Rubicon Communications, LLC (Netgate). (s.f.). *pfSense Security Information*. Recuperado el 25 de Septiembre de 2018, de pfSense: https://www.pfsense.org/security/advisories/

Rubicon Communications, LLC (Netgate). (s.f.). *Toma un tour para*. Recuperado el 27 de Agosto de 2018, de pfsense: https://www.pfsense.org/getting-started/

Rubicon Communications, LLC. (s.f.). *On Premises Firewall Appliances*. Recuperado el 25 de Septiembre de 2018, de netgate: https://www.netgate.com/products/appliances/

Rubicon Communications, LLC. (s.f.). *SG-3100 pfSense® Security Gateway Appliance*. Recuperado el 28 de Octubre de 2018, de netgate: https://store.netgate.com/SG-3100.aspx

S. Tanenbaum, A., & J. Wetherall, D. (2012). *Redes de computadoras Quinta edición.* México: Pearson Educación. Recuperado el 10 de 07 de 2018, de https://bibliotecavirtualapure.files.wordpress.com/2015/06/redes_de_computadoras-freelibros-org.pdf

Seagate Technology LLC. (s.f.). *¿Qué es NAS (almacenamiento conectado en red) y Por qué el NAS es importante para una pequeña empresa?* Recuperado el 14 de AGOSTO de 2018, de Seagate: https://www.seagate.com/la/es/tech-insights/what-is-nas-master-ti/

Slashdot Media. (s.f.). *Win32 Disk Imager*. Recuperado el 02 de Octubre de 2018, de SOURCEFORGE: https://sourceforge.net/projects/win32diskimager/

Soriano, M. (s.f.). *Seguridad en redes y seguridad de la información.* Recuperado el 20 de 07 de 2018, de IMPROVET: http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf

Stallings, W. (2004). *Comunicaciones y Redes de Computadores Séptima edición.* Madrid (España): Pearson Educación, S.A. Obtenido de https://www.academia.edu/5011511/Comunicaciones_y_Redes_de_Computadores_7ma_Edici%C3%B3n_-_William_Stallings

Stallman, R. (11 de Octubre de 2017). *Por qué el «código abierto» pierde de vista lo esencial del software libre*. Recuperado el 19 de Agosto de 2018, de El sistema operativo GNU: https://www.gnu.org/philosophy/open-source-misses-the-point.html#TransNote1

Telmex. (18 de Julio de 2018). *Telmex WEB*. Obtenido de telmex.com: http://telmex.com/web/empresas/servicios-de-gestion-de-red?gclid=CjwKCAjwyrvaBRACEiwAcyuzRFBRvs-0HDNUU4x58iagjxv63UAJaK4FGpuMNRktvflzvgfEmvFfPhoC6aYQAvD_BwE&dclid=CLrErOOMqtwCFRKmaQodKTMPCQ

Vidrios y Cristales Industrializados S.A de C.V. (s.f.). *VYCISA*. Recuperado el 21 de Agosto de 2018, de Vidrios y Cristales Industrializados S.A de C.V.: http://vycisa.com/nosotros.html

Volker Theile. (s.f.). *Licensing*. Recuperado el 25 de Septiembre de 2018, de openmediavault: https://www.openmediavault.org/licensing.html

Volker Theile. (s.f.). *openmediavault 4.0 documentation*. Recuperado el 25 de Septiembre de 2018, de openmediavault: https://openmediavault.readthedocs.io/en/latest/index.html

XigmaNAS. (13 de Julio de 2018). *Listas de hardware compatibles*. Recuperado el 25 de Septiembre de 2018, de XigmaNAS: https://www.xigmanas.com/wiki/doku.php?id=xigmanas_users_hardware

XigmaNAS. (30 de Julio de 2018). *Requisitos de hardware*. (zoon01, Editor) Recuperado el 25 de Septiembre de 2018, de XigmaNAS: https://www.xigmanas.com/wiki/doku.php?id=documentation:setup_and_user_guide:hardware_requirements

XigmaNAS. (20 de Septiembre de 2018). *XigmaNAS® - Almacenamiento conectado a la red*. (zoon01, Editor) Recuperado el 25 de Septiembre de 2018, de XigmaNAS: https://www.xigmanas.com/wiki/doku.php

XigmaNAS. (s.f.). *Interfaz de usuario Screenshots*. Recuperado el 25 de Septiembre de 2018, de XigmaNAS: https://www.xigmanas.com/index.php?id=4

Zabbix LLC. (s.f.). *Technical Support*. Recuperado el 25 de Septiembre de 2018, de Zabbix: https://www.zabbix.com/support

Zabbix SIA. (s.f.). *Documentación de Zabbix*. Recuperado el 27 de Agosto de 2018, de Documentación de Zabbix 3.2: https://www.zabbix.com/documentation/3.2/manual/introduction/about

Anexos

```
<html>
<head>
<title>Bienvenido a la Red Invitados</title>
<meta charset="utf-8">
</head>
<body bgcolor="#000100">
<p align="center"><img src="captiveportal-ZONA.jpg" width="400" height="300"></p>
<form method="post" action="$PORTAL_ACTION$">
<h3><tr> <p align="center" style="color:#0B3861";> “Bienvenido para poder navegar es necesario que inicie sesión, si no cuenta con una cuenta contacte al equipo de sistemas”</p> </tr> </h3>
<table align="center">
  <tr><td><p style="color:#0000FF";>USUARIO</td></P><td><input name="auth_user" type="text"></td></tr>
  <tr><td><p style="color:#0000FF";>PASSWORD</td></p><td><input name="auth_pass" type="password"></td></tr>
</table>
  <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
  <input name="zone" type="hidden" value="$PORTAL_ZONE$">
  <p align="center"><input name="accept" type="submit" value="Continue"></p>
<h3><tr> <p align="center" style="color:#0000FF";></p> </tr> </h3>
  </form>
</body>
</HTML>
```

Anexo 1: Código Índex (Inicio de Sesión Portal Cautivo)

```
<html>
<head>
<title>Bienvenido a la Red Invitados</title>
<meta charset="utf-8">
</head>
<body bgcolor="#000100">
<p align="center"><img src="captiveportal-ZONA2.jpg" width="400" height="300"></p>
<form method="post" action="$PORTAL_ACTION$">
<h3><tr> <p align="center" style="color:#0B3861";>"Usuario o Contraseña Inválido"</p> </tr>
</h3>
<h3><tr> <p align="center" style="color:#0B3861";>"Vuelva a intentarlo o contacte al equipo de
Sistemas"</p></tr> </h3>
<table align="center">
  <tr><td><p style="color:#0000FF";>USUARIO</td></P><td><input name="auth_user"
type="text"></td></tr>
  <tr><td><p style="color:#0000FF";>PASSWORD</td></p><td><input name="auth_pass"
type="password"></td></tr>
</table>
  <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
  <input name="zone" type="hidden" value="$PORTAL_ZONE$">
  <p align="center"><input name="accept" type="submit" value="Continue"></p>
<h3><tr> <p align="center" style="color:#0000FF";></p> </tr> </h3>
  </form>
</body>
</HTML>
```

Anexo 2: Código de Página de Error, en Caso de Autentificación Fallida

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
Centro Universitario Texcoco

10 de mayo de 2018

A quien corresponda, Espero tengan un excelente día

Antes que nada permítame presentarme: Mi nombre es **Cesar Iván Callejas Cortes**, Actualmente realizo un proyecto de Tesis para adquirir el titulo como **Ingeniero en Computación** en **la Universidad Autónoma del Estado de México Centro Universitario Texcoco**. Este proyecto tiene como objetivo la presentación de soluciones que cubran las necesidades de organización y ayude en la mejora operativa y de seguridad de una empresa a través de software libre. Por lo que hoy solicito su apoyo para poder aplicar una encuesta mediante la cual se realizará un análisis de requerimientos sin solicitar información de mercadeo ni administrativa, las preguntas son solo para identificar las áreas de oportunidad en cuestión de **administración y seguridad de su red**, **respaldos de información**, **monitoreo de recursos informáticos**, con la finalidad de demostrar que estas se pueden solucionar y ayudar en la optimización de seguridad y administración de sus recursos informáticos, al finalizar el proyecto de Tesis Se presentará una propuesta que podrá ser implementada Si así se desea en su empresa mostrando el costo beneficio que esta representaría para ustedes.

Nota: Los sistemas de software libre no tienen costo por adquisición por lo que serían factibles para implementar mejoras con pocos recursos.

Sin más por el momento me despido de ustedes dejando mis datos de contacto para cualquier duda.

Teléfono: (044) 55-73-21-75-24

Correo electrónico: ivan050891@hotmail.com

Anexo 3: Carta Presentación para INDESA

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
Centro Universitario Texcoco

Nombre de la Empresa: Industria Nacional de Detergentes, S.A. DE C.V.

Nombre y cargo de la o las personas que contestaran el cuestionario: Maribel Bocardo, Jefe de Sistemas.

Cuestionario Informativo

1.- ¿Cuál es el número total de empleados en la empresa?

320

2.- ¿Cuál es el producto o servicio que ofrece la empresa?

Maquila de Detergente

3.- ¿Cuál es el número total de equipos de cómputo y servidores de la institución?

5 Servidores, 117 Equipos

4.- ¿Cuenta usted con una distribución de red segmentada según las necesidades de la organización?

Si: Cual es el costo de inversión que representa esta implementación

No: Cual es el motivo por el que no cuenta con esta infraestructura,

Falta de planeación.

5.- ¿Cuenta con una administración de red de acuerdo a sus expectativas (limitando los accesos a la web o los servicios de red según lo requerido por cada área)?

Si: Cual es el costo de inversión que representa esta implementación

No: Cual es el motivo por el que no cuenta con esta infraestructura

Costo de herramientas de apoyo como firewall.

Anexo 4: Cuestionario para Levantamiento de Información en INDESA (Parte 1)

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
Centro Universitario Texcoco

6.- ¿Cuenta usted con acceso a su red local de forma remota a través de un túnel VPN seguro?

Si: Cual es el costo de inversión que representa esta implementación:

Se realiza mediante el enlace de antena aproximadamente 3000 mensuales.

No: Cual es el motivo por el que no cuenta con esta infraestructura:

No me interesa el servicio de VPN

7.- ¿Conoce usted la importancia de salvaguardar la información de su empresa?

Si

8.- ¿Cuenta usted con un servicio de respaldos?

Si: Cual es el costo de inversión que representa esta implementación

No: Cual es el motivo por el que no cuenta con esta infraestructura

Costo de implementación y planeación, el respaldo se realiza manual solo a servidores.

9.- En caso de no contar con un servicio de respaldos **¿Le seria de utilidad un servidor de respaldo en red?**

Si

10.- ¿Cuenta usted con una administración directa de su servicio de correo electrónico?

Si: En caso de que si cuente con este servicio cuenta con un filtrado anti spam

No cuento con este servicio:

Se hace a través de un portal.

Anexo 5: Cuestionario para Levantamiento de Información en INDESA (Parte 2)

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
Centro Universitario Texcoco

Para poder analizar más a fondo su opinión cual desearía ser la infraestructura y alcances para los siguientes puntos:

1.- Firewall:

Tener un Firewall más administrable.

2.- VLAN:

Poder administrar la red de forma que las áreas queden separadas.

3.- VPN:

4.-Control de acceso a red Wiffi:

Administración de un portal cautivo para el control de acceso a la red Wiffi de la empresa con usuarios y pasword´s personalizados, especialmente para invitados

5.-Respaldos:

Sistema de respaldo automático y programado no solo en servidores sino de igual forma en los equipos con información sensible de la empresa.

6.- Monitoreo:

Monitorear los equipos para prevenir contingencias en servicios de TI antes de que estos sucedan o tener una respuesta antes que el usuario reporte.

7.- Seguridad de correo Electrónico:

Maribel Nayd Bocardo

El cuestionario se integra por 10 preguntas y 7 puntos a contestar de forma informativa

La información de este cuestionario, se usara para el Proyecto de Tesis del **C. Cesar Iván Callejas Cortes**, Titulado: **"Propuesta de conjunto de herramientas libres que apoyan en la administración de recursos informáticos"**, en la **Universidad Autónoma Del Estado De México C.U. Texcoco.**

Nombre de la persona que autoriza y da fe de la veracidad de la información contenida en el cuestionario presentado: Maribel Nayd Bocardo Serra

Cargo: Jefe de Sistemas

Maribel Nayd Bocardo

Firma

INDESA
INDUSTRIA NACIONAL DE DETERGENTES S.A DE C.V.

Sello de la empresa

Anexo 6: Cuestionario para Levantamiento de Información en INDESA (Parte 3)

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
Centro Universitario Texcoco

Propuesta teórica de las problemáticas a solucionar en ambiente controlado para la empresa Industria Nacional de Detergentes, S.A. DE C.V.

Analizada la información se pretende poder dar solución a los siguientes puntos sustentando la necesidad planteada por la empresa.

1. Implementar un firewall capas de administrar reglas de red.
2. Implementar la distribución de redes virtuales para controlar el acceso a los recursos informáticos, limitando a cada área un segmento en la red.
3. Implementar un control de acceso restringido a las redes inalámbricas de la empresa brindado un control administrado a través de un portal cautivo.
4. Implementar un Sistema de respaldo en red y un plan de respaldos para administrar la información de los servidores de la empresa.
5. Implementar un plan para realizar los respaldos de usuario mediante un servicio en red.
6. La implementación de un servicio de VPN es opcional, con la finalidad de poder realizar atenciones de soporte remoto o disponer de archivos en tiempo real.
7. Implementar un sistema de monitoreo de recursos informáticos Utilidades:
   a. Envió de notificaciones en caso de Problemas en algún recurso o servicio en los equipos.
   b. Prevención de incidentes mediante la pronta detección de comportamientos anómalos en los equipos.

Maribel Nayeli Becerdo

La información de propuesta teórica presentada, se usara para el Proyecto de Tesis del **C. Cesar Iván Callejas Cortes**, Titulado: **"Propuesta de conjunto de herramientas libres que apoyan en la administración de recursos informáticos"**, en la **Universidad Autónoma Del Estado De México C.U. Texcoco.**

Nombre de la persona que autoriza y confirma la utilidad de la propuesta para la empresa

INDESA: Maribel Nayeli Becerdo Sierra

Cargo: Jefe de Sistemas

INDESA
INDUSTRIA NACIONAL DE DETERGENTES S.A DE C.V.

Maribel Nayeli Becerdo

Firma

Sello de la empresa

Anexo 7: Propuesta Validada por INDESA

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
Centro Universitario Texcoco

10 de mayo de 2018

A quien corresponda, Espero tengan un excelente día

Antes que nada permítame presentarme: Mi nombre es **Cesar Iván Callejas Cortes**, Actualmente realizo un proyecto de Tesis para adquirir el titulo como **Ingeniero en Computación** en **la Universidad Autónoma del Estado de México Centro Universitario Texcoco**. Este proyecto tiene como objetivo la presentación de soluciones que cubran las necesidades de organización y ayude en la mejora operativa y de seguridad de una empresa a través de software libre. Por lo que hoy solicito su apoyo para poder aplicar una encuesta mediante la cual se realizará un análisis de requerimientos sin solicitar información de mercadeo ni administrativa, las preguntas son solo para identificar las áreas de oportunidad en cuestión de **administración y seguridad de su red**, **respaldos de información**, **monitoreo de recursos informáticos**, con la finalidad de demostrar que estas se pueden solucionar y ayudar en la optimización de seguridad y administración de sus recursos informáticos, al finalizar el proyecto de Tesis Se presentará una propuesta que podrá ser implementada Si así se desea en su empresa mostrando el costo beneficio que esta representaría para ustedes.

Nota: Los sistemas de software libre no tienen costo por adquisición por lo que serían factibles para implementar mejoras con pocos recursos.

Sin más por el momento me despido de ustedes dejando mis datos de contacto para cualquier duda.

Teléfono: (044) 55-73-21-75-24

Correo electrónico: ivan050891@hotmail.com

VIDRIOS Y CRISTALES
INDUSTRIALIZADOS, S. A. de C.V.
Calle Avena 138 Col. Granja Esmeralda
C. P. 09810 Iztapalapa, D. F.

Anexo 8: Carta Presentación para VYCISA

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
Centro Universitario Texcoco

Nombre de la Empresa: Vidrios y Cristales Industrializados S.A de C.V

Nombre y cargo del o las personas que contestarán el cuestionario: Ing. Oscar Huerta Jefe de Sistemas

Cuestionario

El cuestionario consta de 10 preguntas y 7 puntos a contestar de manera abierta.

1.- ¿Cuál es el número total de empleados en la empresa?

62

2.- ¿Cuál es el producto o servicio que ofrece la empresa?

Se dedica al proceso del vidrio, cristal y espejo

3.- ¿Cuál es el número total de equipos de cómputo y servidores de la institución?

26 equipos y 4 Servidores

4.- ¿Cuenta usted con una distribución de red segmentada según las necesidades de la organización?

Si: Cual es el costo de inversión que representa esta implementación

No: Cual es el motivo por el que no cuenta con esta infraestructura

Presupuesto

5.- ¿Cuenta con una administración de red de acuerdo a sus expectativas (limitando los accesos a la web o los servicios de red según lo requerido por cada área)?

Si: Cual es el costo de inversión que representa esta implementación

No: Cual es el motivo por el que no cuenta con esta infraestructura

Presupuesto

VIDRIOS Y CRISTALES INDUSTRIALIZADOS, S. A. de C.V.
Calle Avena 138 Col. Granja Esmeralda
C. P. 09810 Iztapalapa, D. F.

Anexo 9: Cuestionario para Levantamiento de Información en VYCISA (Parte 1)

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
Centro Universitario Texcoco

6.- ¿Cuenta usted con acceso a su red local de forma remota a través de un túnel VPN seguro?

Si: Cual es el costo de inversión que representa esta implementación

No: Cual es el motivo por el que no cuenta con esta infraestructura

Implementación y presupuesto

No me interesa el servicio de VPN

7.- ¿Conoce usted la importancia de salvaguardar la información de su empresa?

Si

8.- ¿Cuenta usted con un servicio de respaldos?

Si: Cual es el costo de inversión que representa esta implementación

No lo sé con exactitud

No: Cual es el motivo por el que no cuenta con esta infraestructura

9.- En caso de no contar con un servicio de respaldos **¿Le seria de utilidad un servidor de respaldo en red?**

Si

10.- ¿Cuenta usted con una administración directa de su servicio de correo electrónico?

Si: En caso de que si cuente con este servicio cuenta con un filtrado anti spam

No cuento con este servicio

No, es administrado directamente pero la empresa cuenta con anti spam dentro de su servidor de Administración

VIDRIOS Y CRISTALES
INDUSTRIALIZADOS, S. A. de C.V.
Calle Avena 138 Col. Granja Esmeralda
C. P. 09810 Iztapalapa, D. F.

Anexo 10: Cuestionario para Levantamiento de Información en VYCISA (Parte 2)

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
Centro Universitario Texcoco

Para poder analizar más a fondo su opinión cual desearía ser la infraestructura y alcances para los siguientes puntos:

1.- Firewall:

Tener un Firewall más robusto y administrable

2.- VLAN:

Tener segmentadas las diferentes áreas en Vlan´s

3.- VPN:

4.- Control de acceso a red Wiffi:

Tener centralizada y Administrado el control del Wiffi

5.- Respaldos:

Tener un Sistema de respaldos automatizado y tener un pequeño DRP en caso de desastre

6.- Monitoreo:

Tener un software de monitoreo de la Red

7.- Seguridad de correo Electrónico:

La información de este cuestionario, se usara para el Proyecto de Tesis del **C. Cesar Iván Callejas Cortes**, Titulado: **"Propuesta de conjunto de herramientas libres que apoyan en la administración de recursos informáticos"**, en la **Universidad Autónoma Del Estado De México C.U. Texcoco.**

Nombre de la persona que autoriza y da fe de la veracidad de la información contenida en el cuestionario presentado: Carlos Gallardo Dominguez

Cargo: Director Administrativo

VIDRIOS Y CRISTALES INDUSTRIALIZADOS, S. A. de C.V.
Calle Avena 138 Col. Granja Esmeralda
C. P. 09810 Iztapalapa, D. F.

Firma

Sello de la empresa

Anexo 11: Cuestionario para Levantamiento de Información en VYCISA (Parte 3)

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
Centro Universitario Texcoco

Propuesta teórica de las problemáticas a solucionar en ambiente controlado para la empresa Vidrios y Cristales Industrializados S.A de C.V

Analizada la información se pretende poder dar solución a los siguientes puntos, sustentando la necesidad planteada por la empresa.

1. Implementar un firewall capas de administrar reglas de red.
2. Implementar la distribución de redes virtuales para controlar el acceso a los recursos informáticos, limitando a cada área un segmento en la red.
3. Implementar un control de acceso restringido a las redes inalámbricas de la empresa brindado un control administrado a través de un portal cautivo.
4. Implementar un túnel de red privado (VPN) con la finalidad de poder acceder de forma segura a los sistemas internos. Teniendo como utilidades:
    a. Ingreso remoto por parte del Encargado de Sistemas para solucionar problemas en tiempo real
    b. Realizar presupuestos por parte de los vendedores de forma remota en tiempo real
    c. En caso de una contingencia al tener acceso remoto a los recursos en red y con un sistema administrado será posible realizar home office.
5. Implementar un Sistema de respaldo en red y un plan de respaldos para administrar la información sensible de la empresa.
6. Implementar un sistema de monitoreo de recursos informáticos Utilidades:
    a. Envió de notificaciones en caso de Problemas en algún recurso o servicio en los equipos.
    b. Prevención de incidentes mediante la pronta detección de comportamientos anómalos en los equipos.

La información de propuesta teórica presentada, se usara para el Proyecto de Tesis del **C. Cesar Iván Callejas Cortes**, Titulado: **"Propuesta de conjunto de herramientas libres que apoyan en la administración de recursos informáticos"**, en la **Universidad Autónoma Del Estado De México C.U. Texcoco.**

Nombre de la persona que autoriza y confirma la utilidad de la propuesta para la empresa

VYCISA: Carlos Gallardo Domínguez

Cargo: Director Administrativo

VIDRIOS Y CRISTALES INDUSTRIALIZADOS, S. de C.V.
Calle Avena 138 Col. Granja Esmeralda
C. P. 09810 Iztapalapa, D. F.

Firma

Sello de la empresa

Anexo 12: Propuesta Validada por VYCISA