Universidad Autónoma Metropolitana Unidad Azcapotzalco

División de Ciencias Básicas e Ingeniería

INGENIERÍA EN COMPUTACIÓN

Modalidad: Estancia profesional

Sistema de seguridad para una red corporativa

Alumno: **Aguirre Sánchez Luis Alberto**

Matricula: 210208238

Asesores

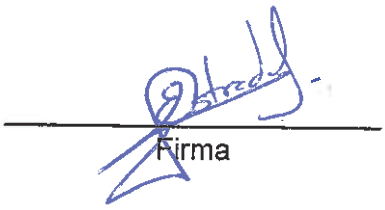
Asesor: **M. en C. José Alfredo Estrada Soto**

Co-asesor: **Ing. Mario Ernesto Gómez Romero**

Trimestre 18-I

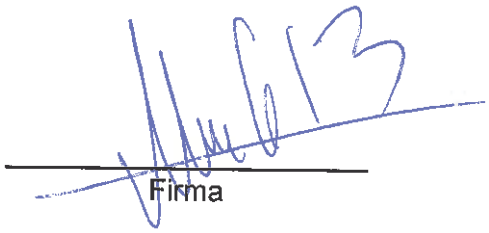
12 de Enero 2018

Yo, ESTRADA SOTO JOSÉ ALFREDO, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.



Firma

Yo, GÓMEZ ROMERO MARIO ERNESTO, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.



Firma

Yo, AGUIRRE SÁNCHEZ LUIS ALBERTO, doy mi autorización a la Coordinación de Servicios de Información de la Universidad Autónoma Metropolitana, Unidad Azcapotzalco, para publicar el presente documento en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

Firma

Resumen

Este reporte presenta información y documentación de cómo se implementó un sistema de seguridad que funcionará dentro de la red de la empresa IAAR con el objetivo de brindar seguridad a la información que se almacena en la red.

El reporte muestra la manera como se llevaron a cabo cada unos de los puntos abarcados en el proyecto, la empresa que proporcionó todos los recursos es T&B Talent S. A. de C. V. en la cual se realizó una estancia profesional de tres meses, solucionando problemas y requerimientos necesitados en la empresa IAAR S. A. de C. V.

El proyecto abarca soluciones de seguridad de la información en donde se implementan políticas de seguridad y políticas de autenticación para los usuarios, estas políticas se adecuan a las políticas de la empresa a la que pertenece la red, también abarca conexiones remotas para los usuarios en donde se presentará un túnel cifrado por el cual se intercambiará y manipulará información importante para el corporativo.

Para implementar los elementos que conforman el sistema de seguridad se hizo uso de un elemento fundamental para su construcción y este fue el cortafuegos Fortigate 90.

En el presente documento se describe cada uno de los procesos, configuraciones y manipulación tanto de software como hardware que se utilizó para concluir el sistema de seguridad.

Tabla de contenido

Índice de figuras

Introducción

Hoy en día, las redes de computadoras son un elemento importante dentro de las empresas debido al tipo de información que se maneja. Por ello, es conveniente contar con mecanismos de protección que garanticen el acceso a tal información únicamente al personal autorizado.

La red dentro de una empresa se le conoce como corporativa y es una red privada que utiliza un conjunto de recursos para proteger información, transferir datos de manera interna y confiable, entre otros. Los elementos que se utilizan en una red corporativa son dispositivos, protocolos y políticas de seguridad que básicamente son los responsables de que ésta opere de manera correcta y segura. Una red tiene que protegerse contra amenazas humanas que pueden causar algún daño a la empresa ya sea robando, eliminando o modificando información de la red, las amenazas son imposibles de controlar e impredecibles, por eso una red debe contar con seguridad para detener y prevenir este tipo de ataques.

Uno de los recursos más empleados para proveer seguridad en una red es el denominado "cortafuegos" o *firewall* en inglés [1]. Este puede ser software o hardware y actúa contra amenazas externas a la red no permitiendo sustracción de datos y bloqueando accesos a personas ajenas a la empresa. Además, el cortafuegos proporciona otro tipo de mecanismos o controles de seguridad para poder proteger y salvaguardar a la empresa y su información: dentro de él se pueden diseñar e implementar políticas de seguridad [2], que son lineamientos y reglas que definen qué puede permitirse y qué no dentro de la red.

La empresa que respaldó el trabajo descrito en este reporte es T&B Talent S. A. de C.V. está lleva más de 17 años ofreciendo distintos servicios a medianas y pequeñas empresas, como son: seguridad perimetral, servicios y mantenimiento de redes e infraestructura, integración de soluciones informáticas dentro de redes corporativas, entre otros servicios.

Figura 1. Logotipo de TB& Talent.

En este reporte se abordará como se fueron solucionando distintos requerimientos y problemáticas dentro de la empresa IAAR (Identificación, análisis y administración de riesgos) que ofrece una gama de servicios de seguridad industrial a otras empresas, esta empresa es uno de los clientes a los que TBT les brinda sus servicios.

Figura 2. Logotipo de IAAR.

Antecedentes

Proyectos terminales

Análisis y gestión de recursos para brindar seguridad en una red empresarial [3]

El proyecto tiene una amplia relación con el trabajo descrito en este documento ya que busca proporcionar seguridad a la información en una red empresarial. Sin embargo, la diferencia está en que la versión del *firewall* es más atrasada a la que se utilizará en esta propuesta y no se hacen implementaciones para usuarios remotos.

Monitoreo de recursos informáticos para una mejor administración y seguridad de los datos en una red corporativa. [4]

En este proyecto también se busca proporcionar seguridad de información mediante un *firewall* fortinet de versión más reciente al que se emplea en la propuesta, pero está limitado exclusivamente a la monitorización de recursos en una red corporativa.

Administración y seguridad de una red corporativa mediante un *firewall* fortigate 90 D [5]

Este proyecto también está enfocado en la seguridad de información en una red corporativa. La diferencia radica en que no aborda implementaciones para usuarios remotos como políticas de seguridad para estos ni la creación de redes virtuales privadas (VPN, por sus siglas en inglés).

Tesis

Seguridad informática (auditoria de sistemas) [6]

Esta tesis está ampliamente relacionada con este proyecto ya que habla sobre cómo poder crear políticas de seguridad, qué hacer en caso de que estas sean violadas por usuarios ya sean externos o internos y si se procederá de forma legal dependiendo del contexto. Este proyecto también aborda la creación de políticas de seguridad pero no aborda la parte de acciones por parte de la empresa ni planes de acción en caso de que la seguridad sea violada.

Seguridad en redes [7]

Esta tesis, al igual que el proyecto, aborda temas de seguridad en redes y cómo crear políticas de seguridad para estas. La diferencia entre los dos es que la tesis aborda de manera más amplia distintas herramientas y el *firewall* que se pueden utilizar para proporcionar la seguridad a una red. Nuestro proyecto contempla solo el uso de un *firewall* como herramienta principal para ello.

Artículos

Firewall – Linux: Una solución de seguridad informática para PyMES (Pequeñas y medianas empresas) [8]

Este artículo tiene relación con el proyecto, ya que en ambos casos la seguridad de una red empresarial pequeña es el elemento principal. La diferencia radica en que en el artículo se hace la implementación de un servidor *firewall* Linux y con ayuda de la herramienta Iptables se tiene control y administración del servidor. En nuestra proyecto se ocupa un *firewall* Fortigate 90D y el control se lleva a través de la interfaz del mismo dispositivo.

Justificación

Con el avance tecnológico se puede observar que actualmente es más fácil que una persona ajena a una red interna pueda acceder a información y usarla de forma inadecuada. Por ello, es de suma importancia proteger y resguardar dicha información ya que su robo puede afectar el desempeño o productividad de una empresa [9].

El empleo de herramientas de seguridad en una red interna tiene como finalidad brindar seguridad y confiabilidad a ésta. Sin embargo, para que una red pueda ser considerada segura debe ser administrada en cuanto a recursos, entrada y salida de datos. Para ello, debe contar con un sistema de seguridad apropiado que permita también realizar la monitorización del tráfico de la red en todo momento. Una de las herramientas o recursos que podemos considerar a la hora de proteger y administrar nuestra red corporativa es el corta fuegos.

Este proyecto busca, por medio de un sistema con base en un firewall Fortigate 90D, proporcionar a una empresa, y a su red interna, la seguridad y confiablidad en el acceso y manejo de su información, así como mejorar el rendimiento de la red interna.

Objetivos

Objetivo general: Diseñar e implementar un sistema de seguridad en una red corporativa con base en un cortafuegos Fortigate 90D.

Objetivos específicos

- Analizar, diseñar e implementar políticas de seguridad para una red corporativa en fortigate 90D.
- Analizar, diseñar e implementar un acceso remoto por medio de una VPN para una red corporativa en fortigate 90D.
- Analizar, diseñar y crear servicios con base en virtualización dentro de una red corporativa.
- Analizar y evaluar diversas herramientas de monitorización que utilicen un protocolo SNMP para poder integrar una de ellas a la red corporativa.
- Analizar y crear políticas de acceso y autenticación para cada uno de los usuarios a de la red corporativa.
- Analizar y crear un enlace redundante para la red corporativa.
- Analizar y administrar los elementos integrados en la red corporativa para mejorar rendimiento e identificar fallas.

Marco teórico

Para entender a fondo cada uno de los puntos abordados en este proyecto, se necesita conocer algunos conceptos los cuales se desglosan a continuación.

Recursos informáticos son todos los elementos como software o hardware dentro de la red que los usuarios de la empresa utilizan para el desempeño de sus actividades de trabajo, como equipos de computo impresoras, maquinas virtuales, etc.

Host son todos los dispositivos conectados a la red y estos pueden proporcionar o requerir servicios de la red de la que forman parte.

Las políticas de seguridad informáticas en una red corporativa son normas o reglas ajustadas y requeridas por la empresa, las cuales ayudarán a proteger los recursos de la red así como asegurar que cada usuario tenga permitido o denegado el acceso a algunas páginas de internet, permitiendo que el personal dentro de la empresa desempeñe de su trabajo sin contratiempos y distracciones, protegiendo además a los recursos de páginas que contengan alguna amenaza informática (virus informáticos).

Acceso remoto, este concepto está enfocado a acceder a información contenida en algún equipo hardware o simplemente a otro equipo para poder manipularlo de forma lejana, es decir con ayuda de tecnología o programas informáticos poder acceder a un recurso en la empresa no estando dentro de la red corporativa.

VPN por sus siglas en ingles *Virtual Private Network* es una tecnología que se utiliza para extender una red privada a través de enlaces de internet públicos, existe diferentes tipos de VPN como: [10]

- VPN de acceso remoto permite a un cliente el traspaso de información a través de internet, haciendo una conexión cifrada hacia una red privada corporativa o empresarial. Este tipo de VPN se basa ya sea en IPSec o SSL.

- VPN site to site permite la conexión segura de toda una red corporativa hacia otra red corporativa.

VPN-SSL por sus siglas en ingles *Virtual Private Network Secure Sockets Layer* se utilizan enlaces públicos de internet para poder tener acceso a una red privada, funciona mediante la creación de un túnel con un cifrado SSL a través de internet, con esta funcionalidad un equipo que está en otra ubicación distinta a la de una red privada puede tener acceso a ella como si estuviera físicamente en la empresa, teniendo la misma privacidad y conectividad.

Protocolo SSL es un protocolo creado para traspasar información entre dos aplicaciones a través de HTTP, teniendo una conexión segura entre un cliente y un servidor, su funcionamiento se explica en la Figura 3.

Figura 3. Funcionamiento de SSL

Virtualización este concepto está enfocado en crear diversos recursos de manera virtual por medio de un software llamado *hypervisor* simulando un entorno físico, en este se pueden crear máquinas virtuales separadas teniendo el mismo funcionamiento que una maquina física, además cada máquina es independiente de la otra, con distintos sistemas operativos, distintas capacidades y todas contenidas en un mismo equipo o hardaware.

Protocolo SNMP por sus siglas en ingles Simple *Network Management Protocol* opera a nivel de la capa de aplicación y es un protocolo para gestión de la red, es utilizado para configurar dispositivos remotos, es decir configurar un equipo sin tener que estar presente para manipularlo e interactuar con esté de manera física, detectar errores en la red o accesos inadecuados y supervisar el uso general de la red, ayuda a monitorear a algún usuario y las acciones que este realice.

SNMP lo componen dos elementos: el agente y el gestor, este protocolo funciona con base a una arquitectura cliente servidor, por lo cual el agente funciona como servidor y el gestor como el cliente.

El agente es un software que se ejecutará en cada uno de los nodos o host de la red que se desean monitorear o gestionar.

El gestor es un software que se ejecutará en la estación encargada de monitorizar la red, recibiendo datos e información sobre los host o nodos de la red que se gestionan.

Enlace redundante este concepto se refiere a tener en la red corporativa un servicio de internet siempre activo, por medio de dos enlaces que proporcionan el servicio, teniendo un enlace principal y un enlace secundario, el enlace secundario solo se convertirá en principal en el caso de que el enlace principal falle, con esto se garantiza que la red siempre tenga internet y que se pueda seguir laborando de manera cotidiana.

Políticas de acceso a la información se refiere a los controles de acceso de directorios o carpetas dentro de la red empresarial que contienen información valiosa y confidencial, servirán para decidir que usuario puede tener acceso o no a cierta información, para su manipulación, por medio de una autenticación para cada uno de los empleados de la empresa.

Protocolo DCHP por sus siglas en ingles *Dynamic Host Configuration Protocol* su objetivo es hacer más simple la configuración de una dirección IP, siendo este protocolo el que asigna la dirección a un equipo o dispositivo de manera dinámica y automática al conectarse a una red, solo hay que configurar el equipo deseado para que encuentre una dirección en la red mediante este protocolo.

Filtro web es un software cuyo objetivo es restringir el acceso a algunos sitos web a los que un usuario puede ingresar.

NAS por sus siglas en ingles *Network Attached Storage*, es un dispositivo el cual contiene varios discos duros donde se guarda la información de una empresa, este funciona como una nube privada dentro de una red corporativa y que solo los miembros de la empresa pueden acceder.

Desarrollo del proyecto

Familiarización con las instalaciones de la empresa

Es importante tener conocimiento sobre lo que la empresa realiza y cuáles son sus actividades cotidianas para tener una visión completa de lo que requieren en su red.

IAAR es una empresa que se dedica a la seguridad industrial y protección civil, ésta proporciona sus servicios a otras empresas dentro de la republica mexicana, la empresa cuenta con tres sucursales: CDMX, Toluca y Querétaro. Siendo la sucursal de la CDMX las oficinas principales y donde se concentra toda la información de las tres sucursales, siendo esta última sucursal en donde se desarrollo el proyecto descrito en este documento.

La mayoría de las personas que trabajan en IAAR no están presentes en las oficinas ya que su trabajo consiste en ir a las diferentes empresas donde brindan sus servicios, de protección civil, seguridad industrial, cursos de entrenamiento, entre otros, cada uno de los empleados es dotado con una laptop o computadora de escritorio que les ayuda a realizar sus actividades de trabajo y que además ellos utilizan para hacer ciertos reportes

de trabajo los cuales deben de entregar a su jefe inmediato diariamente, propiciando que algunos empleados tengan que trasladarse desde la empresa donde brindan sus servicios hacia la sucursal IAAR CDMX para poder proporcionar la información correspondiente, en el caso de de las sucursales IAAR Querétaro y Toluca, se hacen visitas semanales para poder reportar el trabajo hecho durante la semana y tener un control e información sobre los servicios brindados por sus trabajadores para con sus clientes.

En la empresa existen cinco áreas principales y son: recipientes, operaciones, administración, sistemas, recepción y dirección. La mayoría de los empleados de la empresa salen al campo a laborar, especialmente los empleados del área de operaciones aunque también hay quienes se quedan en las oficinas a trabajar y es personal administrativo, como recursos humanos, recepción, entre otros.

Además de familiarizarse con las instalaciones también se procedió a analizar cómo estaba conformada y estructurada la red en sus instalaciones, obteniendo el mapa de red de la Figura 4.

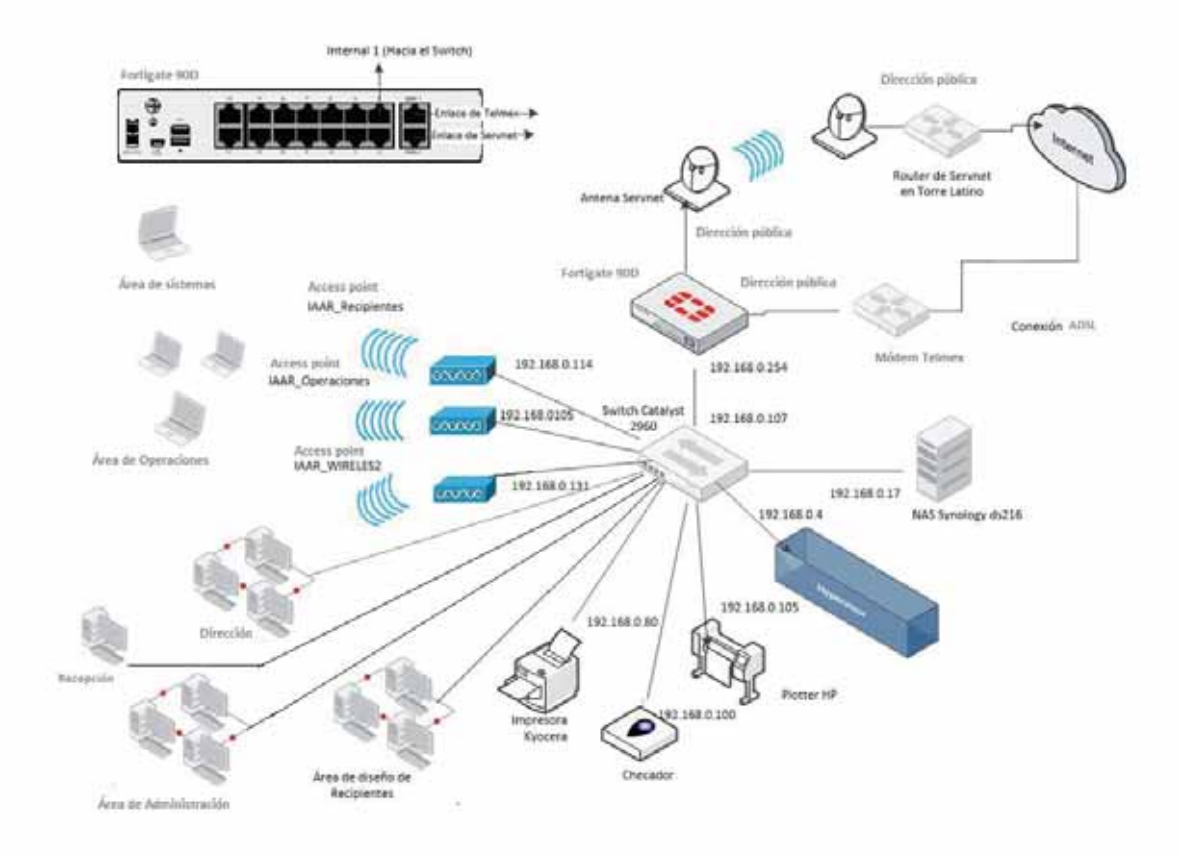


Figura 4. Mapa de red de IAAR.

Análisis políticas de seguridad

En esta sección del proyecto se llevo a cabo un análisis de lo que requería la empresa en cuanto a políticas de seguridad que pudieran ajustarse a su forma de trabajo, fue necesario conocer a cada uno de los usuarios de la empresa y recopilar información

acerca de lo que desempeñan cada uno, esta información la proporciona su jefe inmediato, el cual nos indicó qué actividades desempeñaban y cuáles eran las paginas y sitios web permitidos para cada uno de los trabajadores, a continuación se presenta el análisis de la información recopilada.

IAAR CDMX tiene seis áreas principales dentro de sus oficinas y son: recipientes, operaciones, administración, sistemas, recepción y dirección.

Cada una de estas áreas tiene empleados los cuales cada uno utiliza un equipo distinto, además también cada uno desempeña distintos papeles dentro de la empresa.

Recipientes cuenta con: 4 empleados dentro de las oficinas de la ciudad de México los cuales solo tendrán acceso limitado a internet, evitando sitios como Facebook, Netflix y paginas de descargas de programas y música, pero tendrán acceso a YouTube y a Spotify.

Operaciones cuenta con: 9 empleados dentro de las oficinas de la ciudad de México y tendrán las mismas restricciones que los empleados de recipientes.

Administración con: 3 empleados a cargo en las oficinas de la ciudad de México, este personal tendrá un acceso ilimitado a internet, es decir que podrá navegar sin ninguna restricción.

Recepción cuenta con: 1 empleado en las oficinas de la ciudad de México y tendrá las mismas restricciones que los empleados de recipientes.

Sistemas cuenta con: 1 empleado contratado por medio de la empresa TBT, es el administrador de la red y se tendrá un acceso ilimitado de internet.

Dirección cuenta con: 2 empleados dentro de las oficinas de la ciudad de México, tendrán las mismas restricciones que los empleados de administración.

El acceso a sitios como YouTube es porque los empleados deben consultar dicha plataforma para poder reproducir videos y conferencias subidos por la empresa y que ayuda a su formación laboral, en el caso de Spotify es por política de la empresa a que sus empleados se sientan motivados mientras realizan su trabajo.

Diseño de políticas de seguridad

En esta sección se diseña la inclusión de todos los usuarios dentro de grupos, estos grupos se incluirán en una política de seguridad diferente y que cumplan con los requerimientos dados anteriormente.

Se armarán dos grupos para tres diferentes políticas seguridad, los cuales se desglosan a continuación:

Grupo “Intermedio”: este grupo incluye a los empleados de recipientes operaciones y de recepción.

Grupo “VIP”: este grupo incluye a los empleados de administración, sistemas y dirección.

Política “Intermedio”: esta política se asociara con el grupo “Intermedio” y contendrá todas las restricciones y requerimientos antes expuestos.

Política “VIP”: esta política se asociara con el grupo “VIP” y contendrá todas las restricciones y requerimientos antes expuestos.

Política “Internal”: esta política es para todos aquellos usuarios como clientes y proveedores que no pertenezcan a cualquiera de los dos grupos ya definidos y se conecten a la red interna con cierta autenticación y tendrán un acceso limitado a internet, evitando sitios como YouTube, Netflix, Facebook, entre otros.

Implementación de políticas de seguridad

Después de analizar y diseñar las políticas y grupos se procede a implementarlas.

La red corporativa de IAAR utiliza el segmento de red privado 192.168.0.0 y cuenta con dos ISP’s (Internet Service Provider) o dos proveedores de servicio de internet, un ISP de Telmex y el segundo proveedor es la empresa Servnet.

Cada uno de los equipos de los empleados de IAAR están conectados a la red interna, Fortigate funciona como un servidor de DHCP el cual les asigna direcciones IP a cada uno de los equipos conectados, cuando un equipo nuevo se conecta a la red, Fortigate lo registra a través de su interfaz grafica en System > Monitor > DHCP > Monitor, tal como se muestra en la Figura 5 mostrando el nombre del equipo, su dirección física MAC y la dirección IP asignada. Es así como sabemos qué dirección IP fue asignada a cada equipo y a que empleado corresponde.

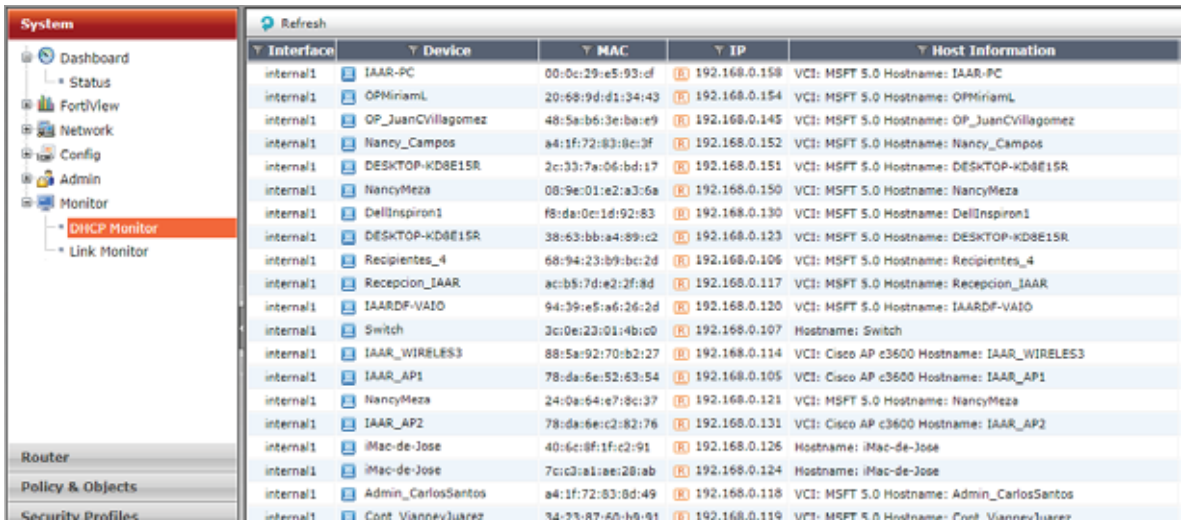


Figura 5. Registro de usuarios de la red.

El primer paso es crear objetos asociados con las máquinas de cada uno de los empleados por medio de una dirección IP asignada. Creamos los objetos con un nombre de tal manera que se pueda identificar a un equipo, se realiza de la siguiente manera:

Entramos a la interfaz de Fortigate y vamos a policy & objects > Objects > Addresses y damos clic en el botón “Create New” > “Object” para crear un objeto como se muestra en la Figura 6.

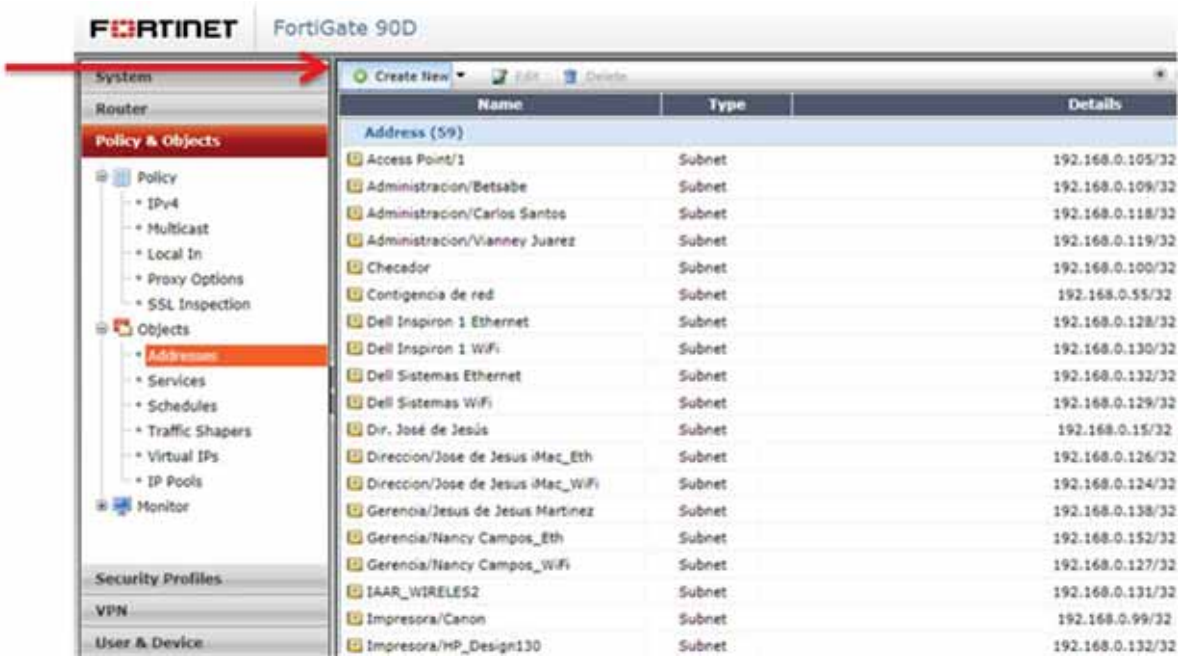


Figura 6. Creación de un objeto nuevo en Fortigate.

Después aparecerá otra pantalla en la cual se definirá el objeto y se categoriza de la siguiente manera:

- En el campo “Name” se coloca el nombre del objeto de tal forma que se pueda identificar y saber a qué equipo o usuario corresponde dicho objeto.
- En el campo “Type” se coloca la opción con base a lo requerido, la opción puede ser “IP/Netmask” para designar la dirección IP específica del usuario, o la opción “FQDN” en caso de que vayamos a escribir el dominio de alguna página web.
- En el campo “Subnet/IP Range” se pondrá una dirección que perteneciente al segmento de red de la empresa y que se haya verificando que no se esté siendo utilizada.
- “Interface” se coloca la interfaz con el nombre “Internal 1”.
- Los comentarios son opcionales en caso de haberlos. La configuración quedará como se muestra en la Figura 7.

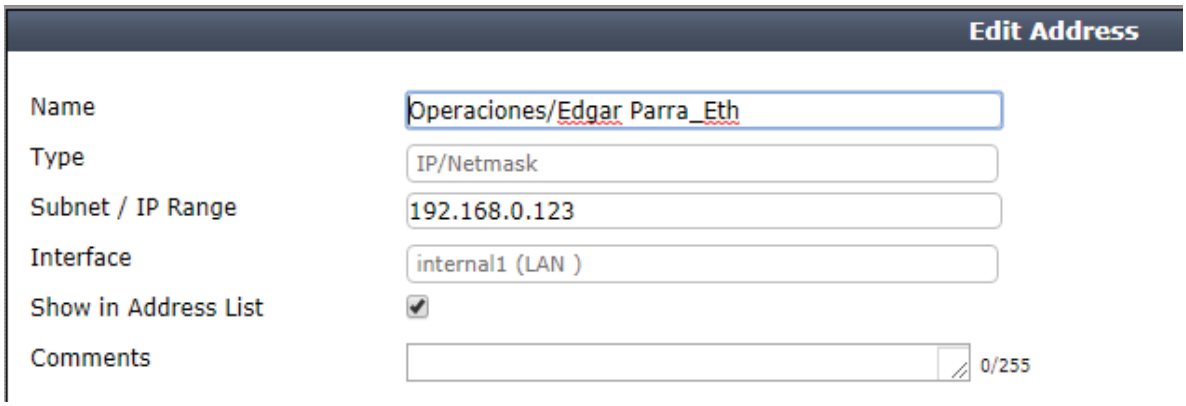


Figura 7. Configuración de un objeto.

Una vez creado el objeto deberá aparecer en la lista de direcciones como se ve en la Figura 8.

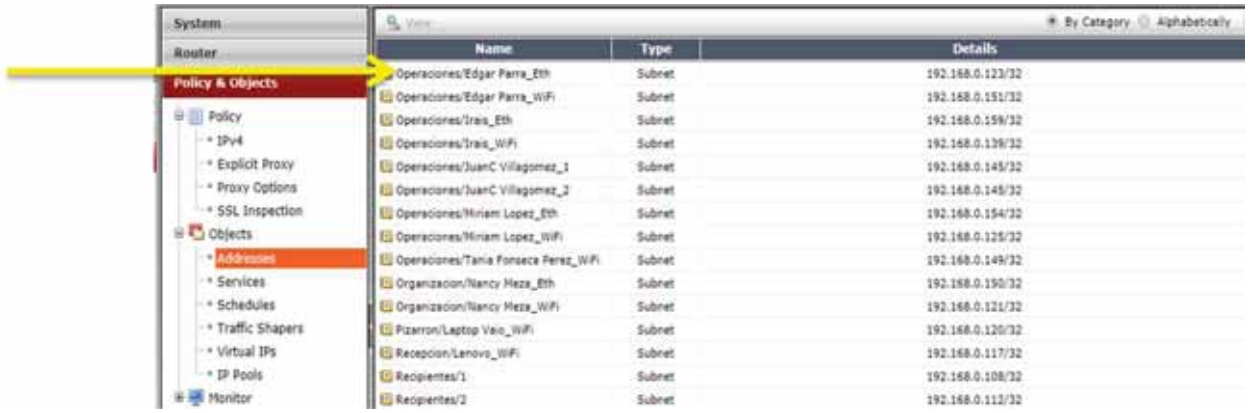


Figura 8. Lista de direcciones.

Así se creará un objeto para cada uno de los equipos dentro de la red corporativa y se procede a crear los grupos, para integrar a todos los objetos creados.

De nuevo entramos a policy & objects > Objects > Addresses y se selecciona el botón “Create New” > “Address Group” para crear un grupo y se configura de la siguiente manera:

- En el campo “Group Name” se coloca el nombre del grupo ya definido anteriormente.
- El campo “Show in Address List” debe estar activado para mostrar el grupo en la lista de direcciones.
- En el campo “Members” se agregan los miembros del grupo dando clic en el icono “+” y se seleccionan los miembros por medio del nombre del objeto con el que están asociados. La configuración descrita es mostrada por Figura 9.

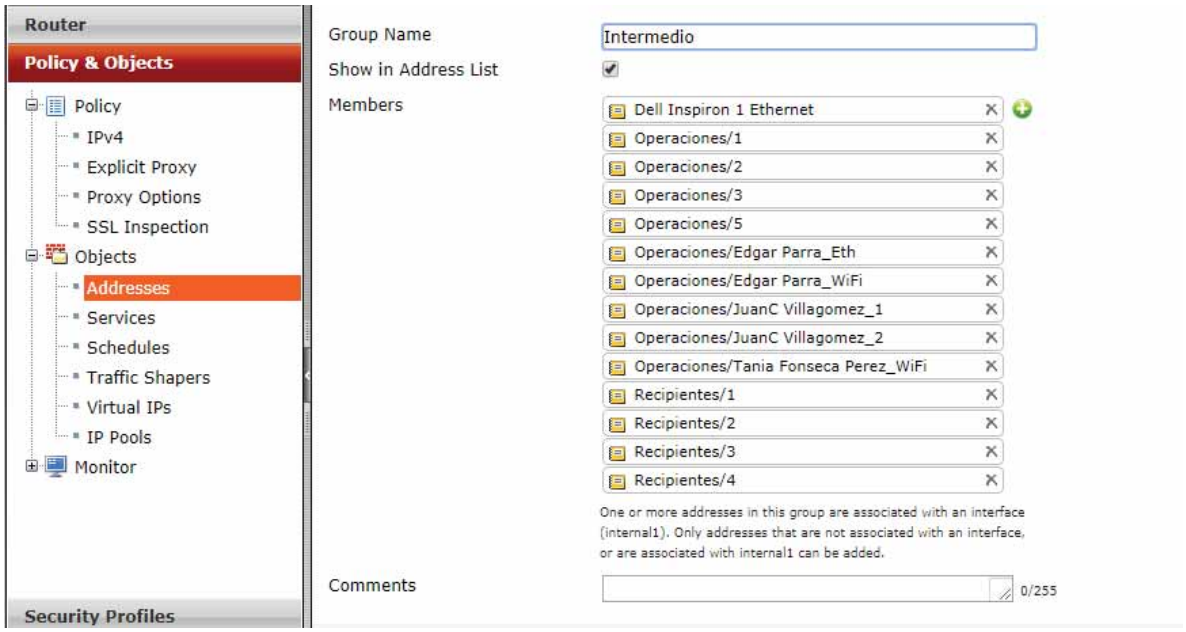


Figura 9. Creación de un grupo de objetos.

En la Figura 9 se muestra la creación del grupo “Intermedio”, la creación del grupo “VIP” se hace exactamente igual y su configuración es la misma. Quedando dos grupos creados, los cuales aparecerán en la lista de direcciones con sus miembros correspondientes tal como se muestra en la Figura 10.

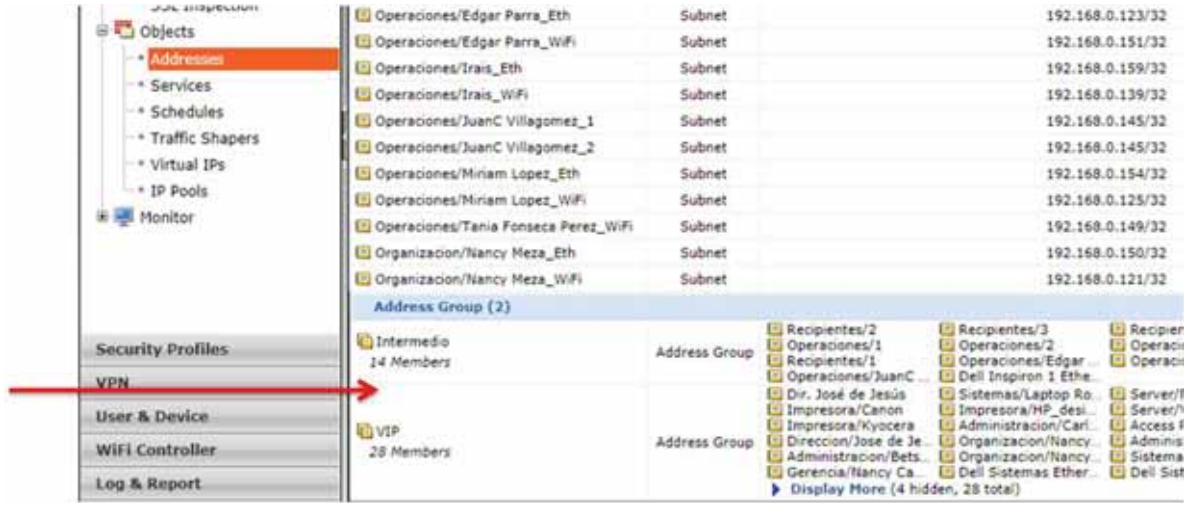


Figura 10. Lista de direcciones y grupos creados.

Se procede a la creación de políticas de seguridad para integrar a los grupos creados. Aunque se diseñaron tres políticas distintas, se crearan seis políticas de las cuales tres se asignarán al enlace de internet proporcionado por la empresa “Telmex” y tres iguales para el enlace de Internet proporcionado por la empresa “Servnet”.

Estos dos enlaces están conectados directamente a las interfaces “WAN” de Fortigate como muestra la Figura 11.

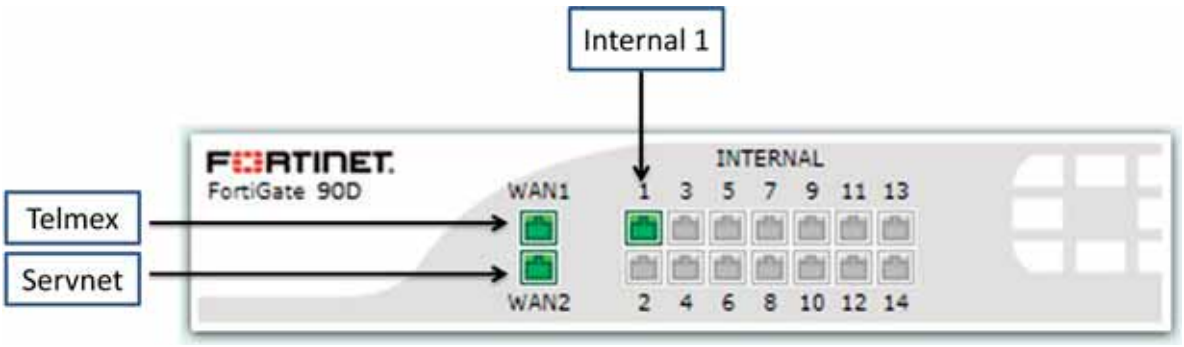


Figura 11. Interfaces físicas de Fortigate.

Estos dos enlaces dan el servicio de internet por medio de la interfaz “Internal 1”, cualquiera de los dos enlaces puede proporcionar el servicio, así que se hacen políticas para estos dos enlaces proporcionando restricciones a los trabajadores independientemente de cuál sea el enlace que se esté utilizando para el servicio.

Iremos a Policy & Objects > Policy > IPv4 y damos clic en el botón “create new” y se selecciona la opción “Policy” tal como se observa en la Figura 12.

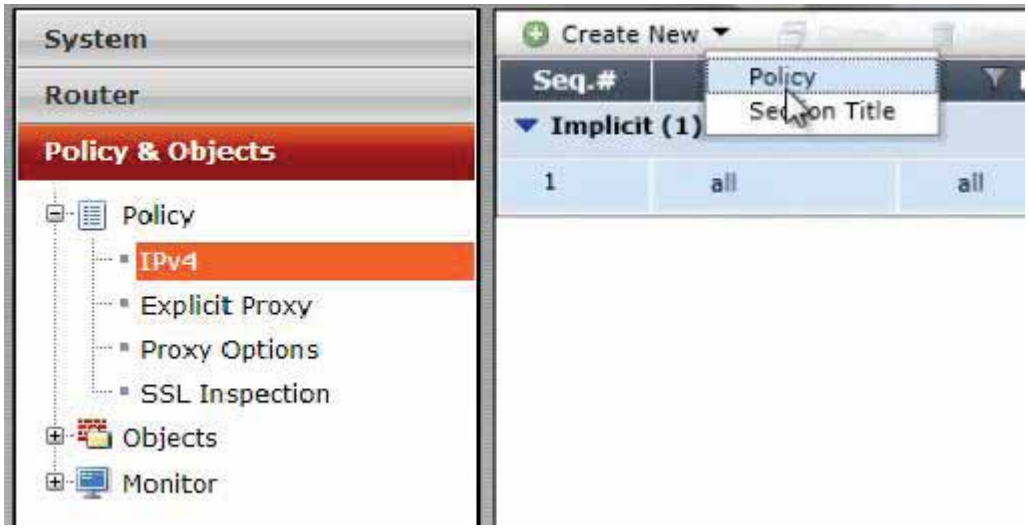


Figura 12. Creación de una nueva política.

Después aparece una pantalla en la cual hay que configurar las restricciones y las características que tendrá dicha política.

- En el campo “Incoming Interface” se selecciona la interfaz “Internal 1” la cual es por donde está entrando el servicio de internet a la red.

- En el campo “Sourse Address” se selecciona el grupo de usuarios a los cuales se les aplicaran las estricciones en esta caso será para el grupo VIP.
- En el campo “Outgoing Interface” se selecciona la interfaz hacia afuera de la red que está proporcionando el servicio, en este caso será para Telmex.
- En el campo “Destination Address” se selecciona la opción “all” ya que se les aplicará las restricciones a todos los que pertenezcan al grupo VIP.
- En el campo “Schedule” se selecciona el tiempo en el que funcionarán la política se elige la opción “always” para que la política funcione siempre.
- En el campo “Service” se selecciona la opción “all” para conceder todos los servicios en cuanto a protocolos.
- En el campo “Action” se elije la opción “ACCEPT” para aplicar la política y dar acceso a todos los usuarios que pertenezcan al grupo.
- Se habilita el campo NAT y el campo de “Use Outgoing Interface Address” para utilizar la dirección de la interfaz de salida. La configuración queda como se muestra en la Figura 13.

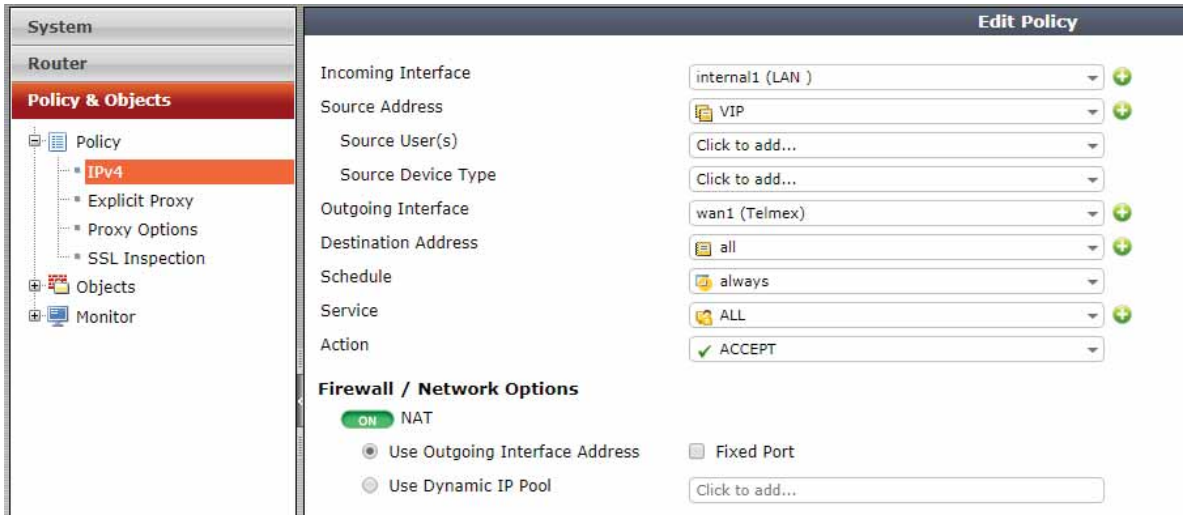


Figura 13. Configuración de la política para el grupo “VIP” para la WAN 1 (Telmex).

La política para el grupo “VIP” no tiene ninguna restricción así que no se configurará nada más de lo que ya se expuso, recordemos que este grupo es para los empleados con mayor rango dentro de la empresa. La política para el grupo “VIP” y la WAN 2 (Servnet) se hace exactamente de la misma forma, quedando la configuración de la Figura 14.

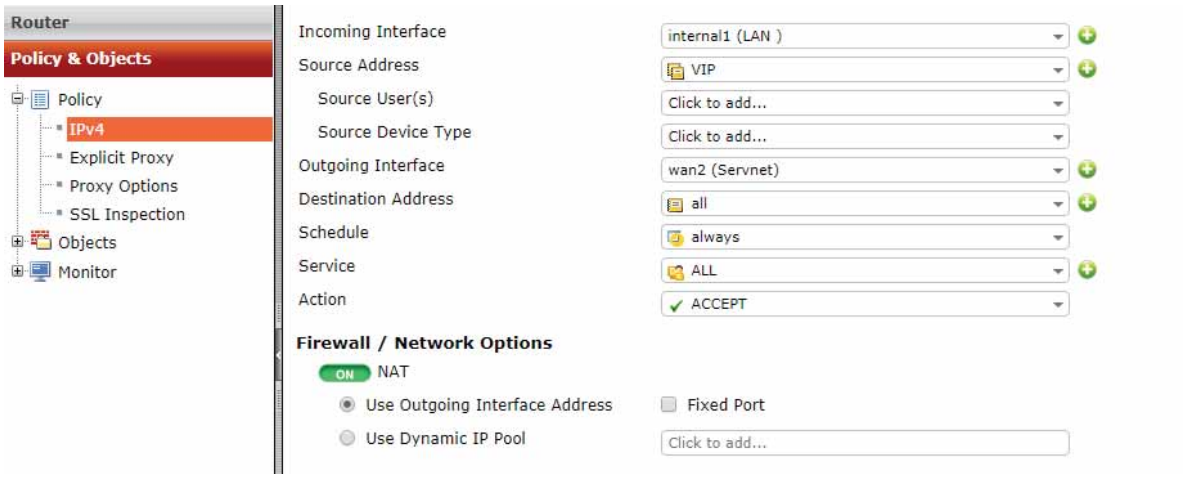


Figura 14.Configuracion de la política para el grupo “VIP” para la WAN 2 (Servnet).

La siguiente política por crear es para el grupo “Intermedio“, se crea con el mismo método como se creó la política para el grupo “VIP” solo que la configuración de está es diferente ya que si hay algunas restricciones que se tomarán en cuenta.

Los primeros campos de la configuración se hacen de manera similar a la política para el grupo “VIP” teniendo algunos cambios en campos como en “Sourse Address” el cual indica a los usuarios a los cuales se les aplicarán las restricciones de esta política, seleccionando el grupo “Intermedio” para la WAN 1 (Telmex) y quedará como se muestra en la Figura 15.

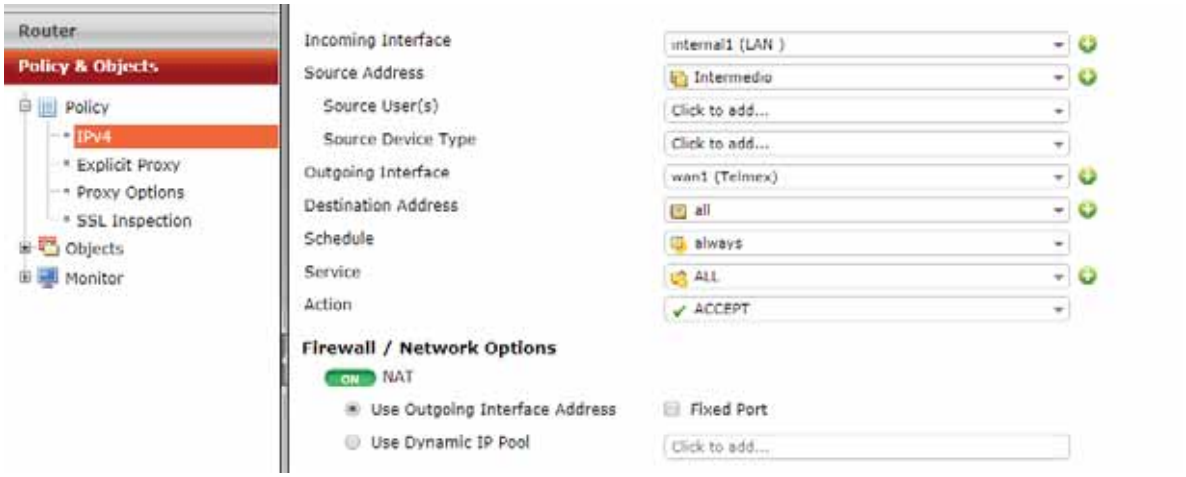


Figura15. Configuración de política para el grupo “Intermedio” para la WAN 1 (Telmex)

Ahora se configurará las restricciones para la política del grupo “Intermedio” se desglosa a continuación.

En la sección “Security Profiles” se activará la casilla “Antivirus” y se creará un perfil, seleccionando la opción “create” como se muestra en la Figura 16.

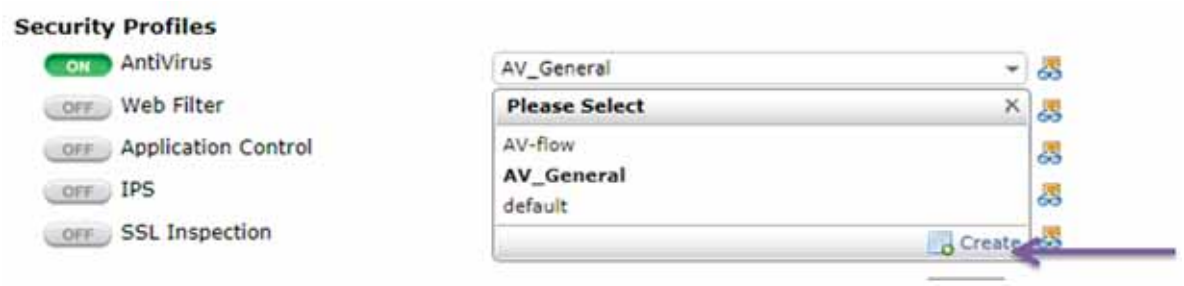


Figura 16. Creación de un perfil para la "AntiVirus".

Aparece una pantalla en la cual se configurará el perfil de la siguiente forma:

- En "Name" se coloca el nombre que tendrá el perfil
- En "Commnets" se colocan algunos comentarios en caso de ser necesarios.
- En "Inspection Mode" esta opción se elije para que el *cortafuegos* inspeccione el contenido de los paquetes de datos a medida que *Fortigate* los recibe para detectar algún virus y realizar una acción o bloqueo.
- En "Detect Viruses" se selecciona "Block" y esto es para que en caso de que se detecte algún virus sea bloqueado.
- Se habilita la opción "Detect Connections to Botnet C&C Servers" y la opción "Block" para detectar alguna conexión de algún servidor externo a la red el cual puede infiltrar *malware* y causar algún tipo de daño a algunos de los elementos de la red corporativa. La configuración del perfil se muestra en la Figura 17.

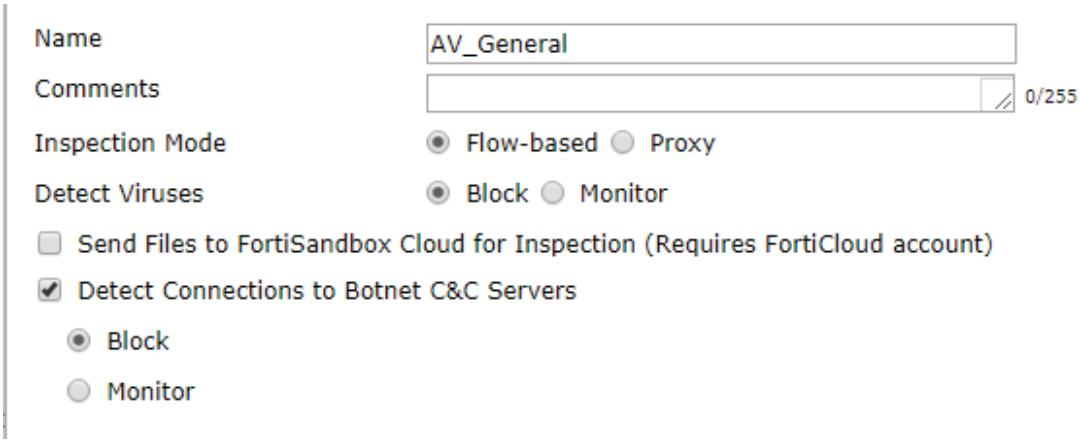


Figura 17. Configuración de un nuevo perfil para la casilla "AntiVirus"

En la sección "Security Profiles" se activará la casilla "Web Filter" y se creará un perfil, seleccionando la opción "create" como se muestra en la Figura 18.

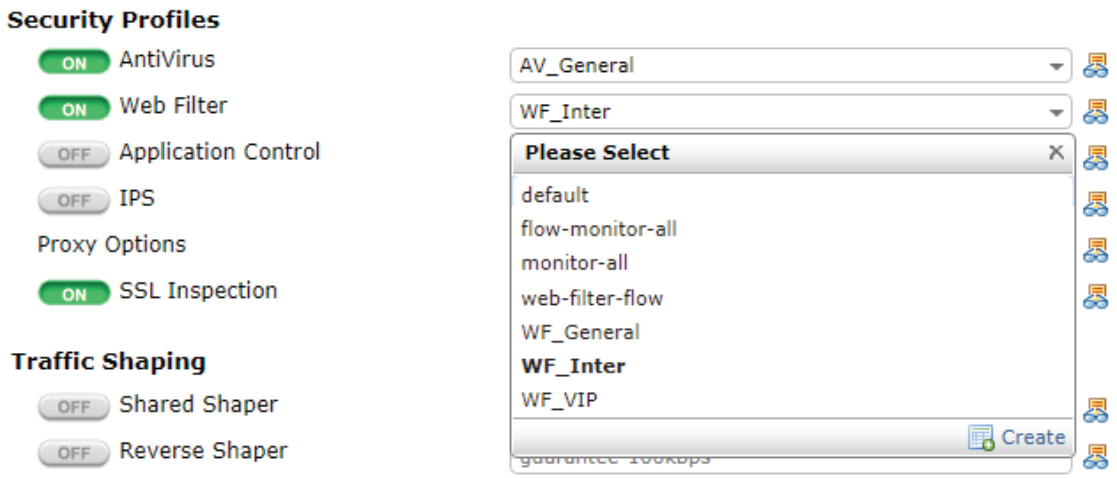


Figura 18. Creación de un nuevo perfil para “Web Filter”.

- En “Name” se coloca el nombre que llevará nuestro perfil
- En “Comments” se escribirán comentarios en caso de ser necesarios.
- En “Inspection Mode” se seleccionará la opción “proxi” en donde todo el tráfico que pasa es analizado después de haber recibido el paquete entero y la configuración se muestra en la Figura 19.

Figura 19. Configuración de un nuevo perfil para “Web Filter”.

Después de estos campos se muestran las categorías de de filtrado web, las cuales contiene subcategorias que hay que revisar para poder dar o denegar el acceso a los usuarios o al grupo al cual se le aplicará la política generada.

- Para la categoría “Potentially Liable” que incluye subcategorias con temas referentes al abuso infantil, discriminación, abuso de drogas, hackeo, entre otros, será denegado el acceso ya que para el desempeño de sus actividades de trabajo no será necesario consultar páginas web con referencia a estos temas.
- Para la categoría de “Adult/Mature Content” que incluye subcategorias con temas referentes a aborto, alcohol, mariguana, pornografía, entre otros, será denegado el acceso.
- Para la categoría “Bandwidth Consuming” (Consumo de ancho de banda) que incluye subcategorias que se revisan para decidir si hay que denegar o permitir el

acceso, las subcategorias con su configuración se desglosan a continuación y se muestran en la Figura 20.

- "File Sharing and storage" (Uso compartido y almacenamiento de archivos) se denegará el acceso a paginas como One Drive o Drop Box.
- Freeware and software downloads" (Descarga de software) se permitirá el acceso ya que el personal utiliza algunos programas para el desempeño de sus actividades pero se monitoreará el consumo de ancho de banda.
- "Internet Radio and TV" (Radio y TV por internet) se permitirá el acceso a la aplicación Spotify.
- "Peer-to-peer File Sharing" (Intercambio de archivos punto a punto) se denegará el acceso.
- Streaming Media and Download (Streaming y descargas) se permitirá el acceso monitoreado.

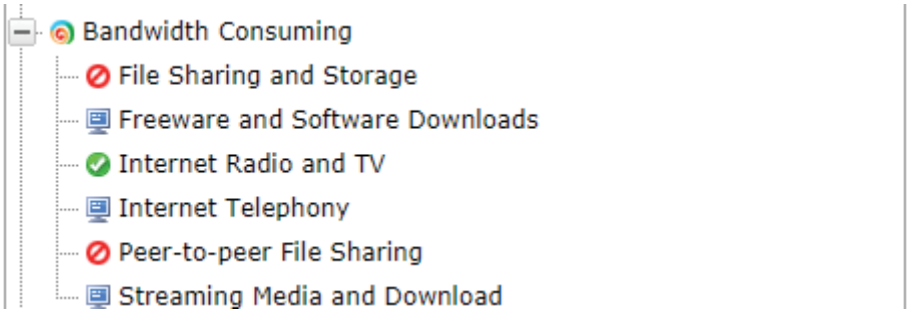


Figura 20. Configuración de la categoría "Bandwidth Consuming"

- Para la categoría "General Interest – Personal" que incluye subcategorias con temas referentes a educación, arte y cultura, referencias, deportes, libros, entre otros temas, se tendrá acceso.
- Para la categoría "General Interest – Business" que incluye subcategorias con temas referentes a negocios, finanzas, buscadores entre otros temas, se tendrá un acceso monitoreado. Las categorías ya configuradas del perfil creado se muestran en la Figura 21.

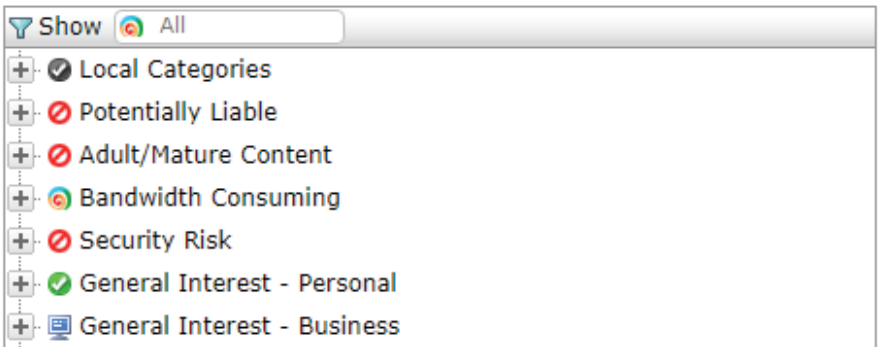


Figura 21. Categorías del perfil WF_Inter.

En la sección “Security Profiles” se activará la casilla “Application Control” y se creará un perfil, seleccionando la opción “create” como se muestra en la Figura 22.

Figura 22. Creación de un perfil para “Application Control”

En el campo “name” se colocará el nombre que le daremos al perfil y en el campo “comments” se colocan comentarios en caso de ser necesario como se muestra en la Figura 23.

Donde aparecerán distintas categorías que hay que configurar con la finalidad de dar acceso o denegarlo a ciertos sitios web, las categorías se desglosan a continuación.

- “Bonet” se refiere servidores que infecta a los equipos con *malware* a través del ingreso a una página web, por lo cual esta categoría será para denegar acceso a sitios maliciosos.
- “Bussines” incluye herramientas como Google Analytics, estos ProCall, entre otras herramientas empresariales, esta categoría será permitida.
- “Cloud.IT” incluye herramientas como Google Cloud Platform, Amazon Alexa, entre otros, que serán permitidas.
- “Collaboration” ” incluye herramientas como Express, Adobe Connect, Microsoft Office Online, entre otras herramientas que serán permitidas.
- “Email” que incluye sitios de correo electrónico como Gmail, Hotmail y protocolos como POP3 y SMTP, que serán permitidos.
- “Games”, que incluye sitios y aplicaciones de video juegos, que serán bloqueados.
- “Social Media” que incluyen redes sociales como Facebook, Twitter, Hi5, entre otras las cuales serán bloqueadas.
- “Video/Audio” incluye el sitio YouTube el cual será permitido.
- “VoIP” incluye herramientas que utilizan voz sobre IP como Face Time, entre otras que serán bloqueadas.

La configuración de todas las categorías se muestra en la Figura 23.

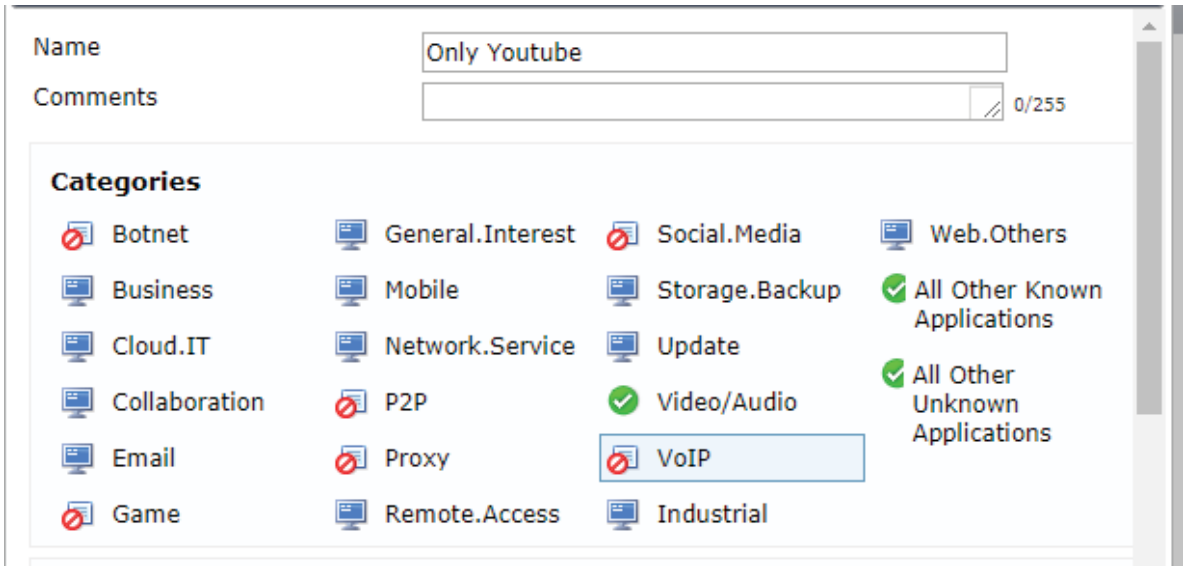


Figura 23.Configuración del perfil “Only Youtube”

Se configura una política para el grupo “Intermedio” pero ahora para la WAN 2 (Servnet) y se hará de la misma forma que la configuración anterior.

Dando por terminada la configuración de la política para el grupo “Intermedio” se procede a hacer una tercera política para todos los demás usuarios que no pertenezcan ni al grupo “VIP” ni al grupo “Intermedio”, es decir todos los que no estén incluidos en los grupos. La configuración es la misma que las políticas anteriores solo que con más restricciones, no se podrá tener acceso a YouTube ni a Spotify, se harán dos políticas iguales para los usuarios que no pertenezcan a los grupos ya descritos uno para la WAN 1 y la WAN 2.

Una vez terminada la configuración de las tres políticas deberán aparecer en Fortigate como se muestra en la Figura 24. Cada una de estas políticas están habilitadas, la toma de decisiones que ayudo a configurar las políticas fueron tomadas gracias a la información recopilada y analizada previamente.

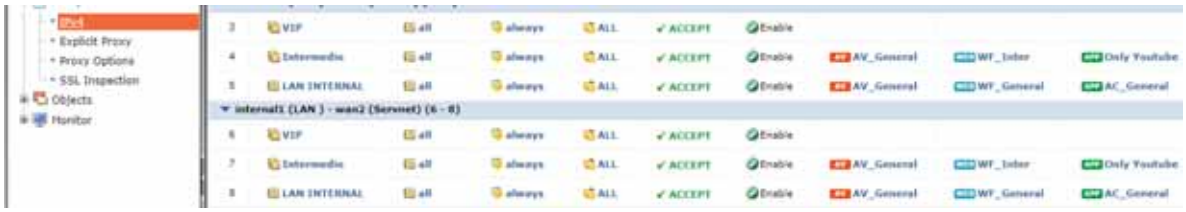


Figura 24. Políticas de seguridad configuradas en Fortigate.

Análisis para la creación de un acceso remoto (VPN)

Para construir un acceso en la red corporativa de IAAR es necesario analizar algunos aspectos y recursos con los que cuenta la red.

IAAR cuenta con dos proveedores de servicio de internet por lo tanto también cuenta con dos enlaces, el primero es un enlace ADSL (Telmex) y el segundo en un enlace dedicado (Servnet), para decidir en cuál de los dos enlaces se construirá un acceso remoto a través de una VPN es necesario saber y distinguir las características que hay en entre estos dos enlaces.

- Enlace ADSL (*Asymmetric Digital Subscriber Line)* es una tecnología de banda ancha que a pesar de que permite una velocidad buena, no garantiza una velocidad constante en la trasmisión de datos. Esta conexión aprovecha una línea telefónica para poder brindar el servicio con un módem a una central telefónica, es decir que depende del modem y de la línea telefónica para brindar un servicio bueno, si la línea telefónica llega a fallar o a caerse el servicio seria cortado hasta la reparación de la falla en la zona.
- Enlace dedicado este es un servicio que está diseñado para tener una conexión las 24 horas los 365 días del año, sin requerir de una línea telefónica para su funcionamiento, no depende de un aparato para poder encender y apagar la conexión, es una conexión permanente de alta calidad y seguridad, además de que ofrece una velocidad constante en la trasmisión de los datos.

Ambos enlaces cuentan con una dirección pública la cual se usará para poder acceder a la red interna.

El acceso remoto debe estar siempre disponible para los empleados de la empresa por lo cual se decide construirlo sobre el enlace dedicado (Servnet).

Este acceso remoto está enfocado a usuarios que laboran la mayoría del tiempo fuera de la empresa y que deben entregar reporte de sus actividades diarias, así como también para empleados específicos de las sucursales de IAAR Querétaro y Toluca. Esta información nos la proporciono el director de la empresa de IAAR CDMX.

Diseño para la creación de un acceso remoto (VPN)

El acceso remoto deberá estar enfocado ciertos trabajadores en la empresa los cuales tendrán que autenticarse para poder ingresar a la red.

Cada uno de los usuarios tendrá su login y su contraseña las cuales serán diferentes para cada uno.

Se configurará una VPN-SSL de acceso remoto ya que esta es la que más se ajusta a los requerimientos de IAAR, cada uno de los usuarios es visto como un cliente y Fortigate será el servidor el cual dará o denegará el acceso a los usuarios a la red.

En Fortigate es posible construir una VPN, permitiendo a los usuarios remotos acceder a la red corporativa conectándose en modo túnel utilizando un software llamado FortiClien, permitiendo que el tráfico de internet también pase a través de Fortigate, para aplicarle un escaneo de seguridad.

Se crearán dos grupos de usuarios los cuales están definidos como: prevención que son todos los usuarios que se conectarán a la red de manera remota (empleados IAAR) y TBT que son los administradores de red, los cuales harán uso de la conexión remota para verificar que todo esté funcionando correctamente.

Implementación de un acceso remoto (VPN)

Vamos a Policy & Objects > Addresses y se crea un objeto el cual será el rango de IPs que le asignaremos a la VPN, este tiene que ser distinto al segmento de red de la red corporativa como se muestra en la Figura 25.

Figura 25. Rango de IP para la VPN.

Una vez creado el objeto se crean los usuarios a los cuales se les permitirá el acceso remoto a la red, vamos a User & Device > User Definition y damos clic en “create new”, la configuración de los usuarios es la siguiente:

- “User Name” se coloca el nombre del usuario el cual usará el acceso remoto.
- “Password” se pondrá una contraseña de autenticación la cual servirá para que el usuario pueda acceder a la red corporativa de manera remota. La configuración se muestra en la Figura 26.

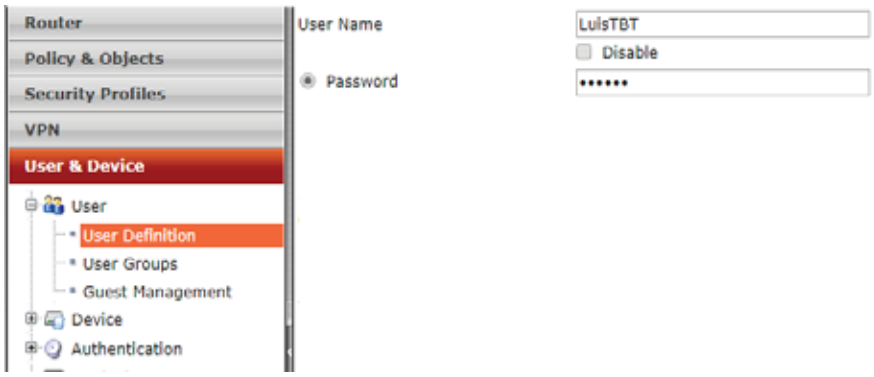


Figura 26. Creación de un usuario.

Los demás usuarios que harán uso del acceso remoto se crean y configuran de la misma forma quedando como resultado una lista de usuarios como se muestra en la Figura 27.

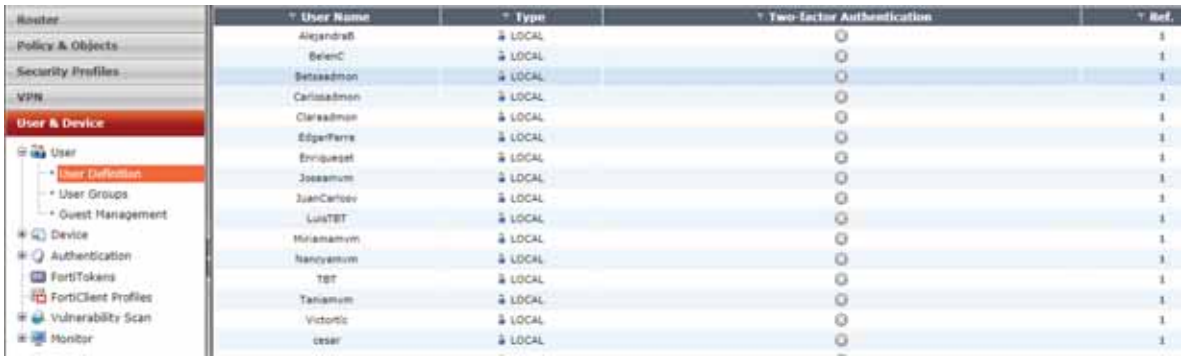


Figura 27. Lista de usuarios.

Después de crear cada usuario se procede a crear grupos de usuarios, para lo cual se crearán dos distintos grupos, vamos a User & Device > User Groups y seleccionamos "create new", la configuración de grupos es la siguiente:

- "Name" se coloca el nombre del grupo.
- "Type" se coloca *Firewall.*
- "Members" se agregan los miembros que pertenecen al grupo con el icono "+", tal como se muestra en la Figura 28.

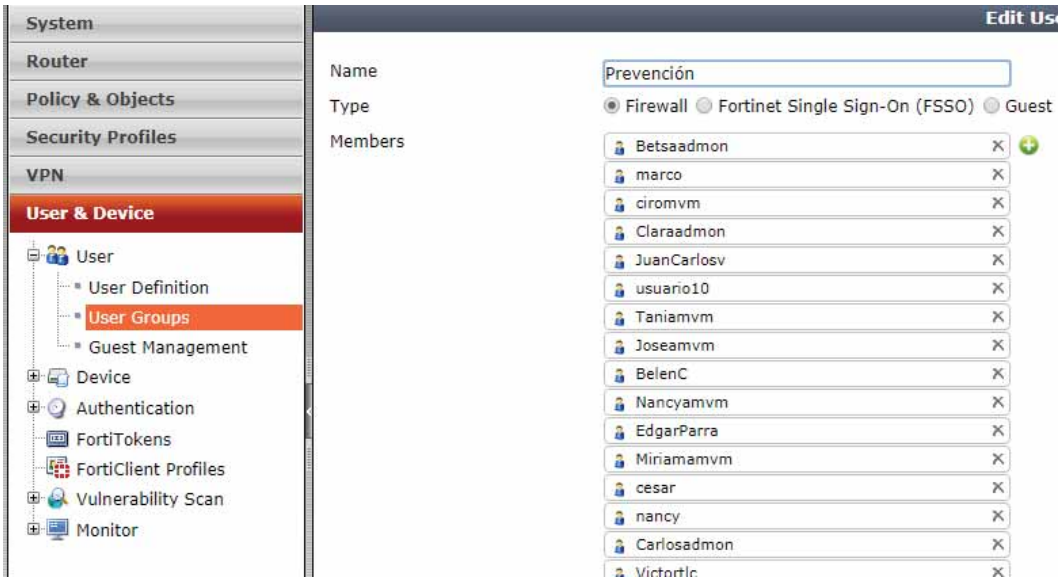


Figura 28. Configuración del grupo prevención en Fortigate.

Para el segundo grupo se aplica la misma fórmula de configuración tal como se muestra en la Figura 29.

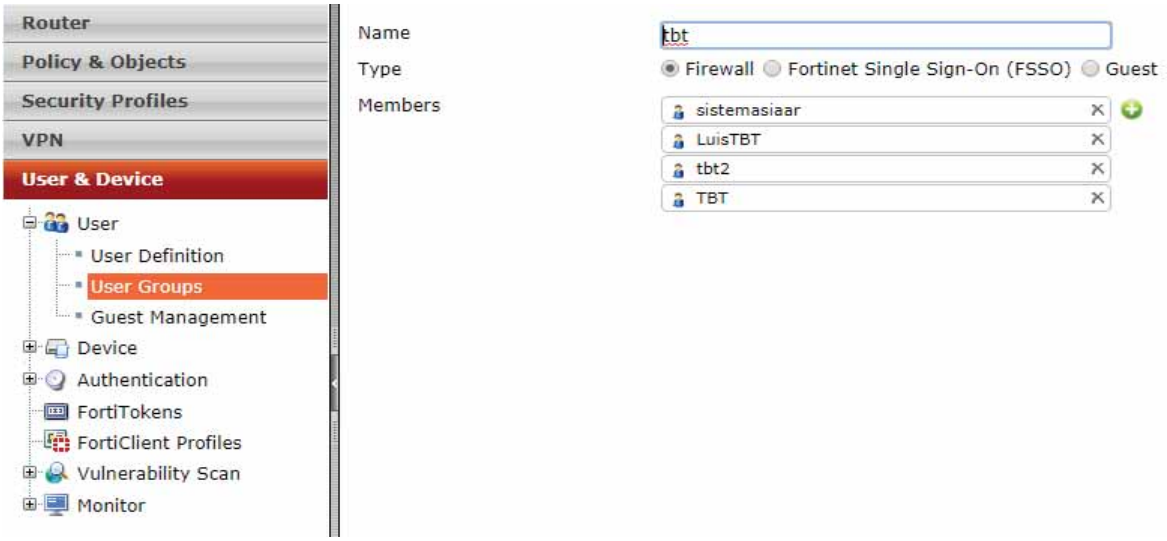


Figura 29. Configuración del grupo TBT en Fortigate.

Una vez concluida la creación de grupos y usuarios se configura el portal VPN-SSL, vamos a VPN > SSL > Portals y creamos un nuevo portal seleccionando la opción "create new", hay que recordar que la creación de VPN se aplica en modo túnel para que los usuarios puedan ingresar a la red corporativa por medio del software Forticlient por lo cual se aplica la siguiente configuración.

- "Name" se pondrá el nombre del túnel.
- "Enable Tunnel Mode" se habilita el modo túnel.
- "Enable Split Tunneling" se habilita, ya que con esta configuración el cliente tendrá acceso seguro a recursos corporativos.

- “Source IP Pools” se selecciona el rango el objeto creado anteriormente “VPN_SSL” que es el rango de IP’s de nuestra VPN tal como se muestra en la Figura 30.

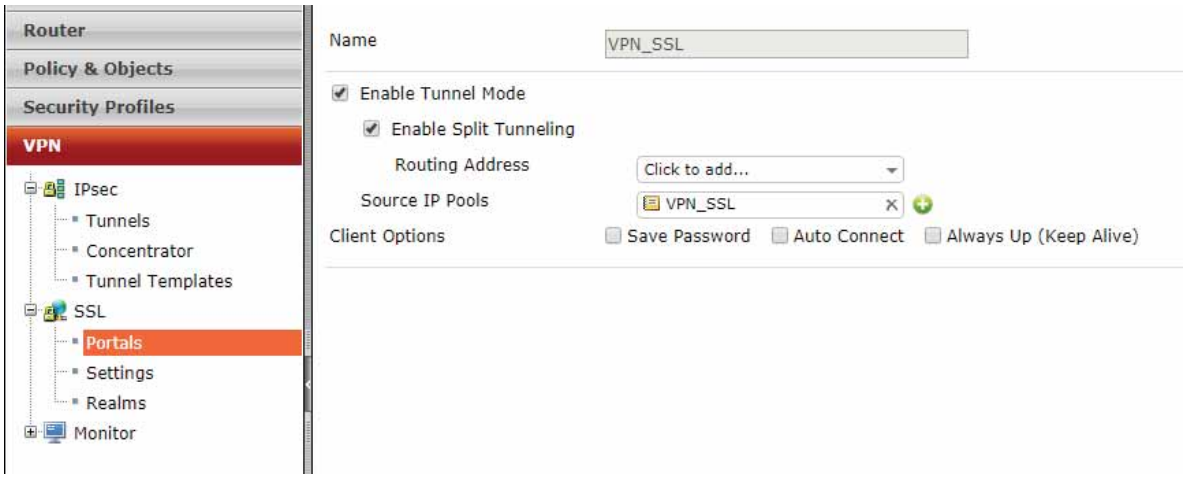


Figura 30. Configuración del portal VPN

Después de configurar a conexión el portal, se configuran algunos ajustes de la VPN, vamos a VPN > SSL > Settings y se coloca la siguiente configuración.

Connection Settings (Configuración de conexión)

- “Listen Interface (s)” se coloca la interfaz por la que se hará la conexión de la VPN en este caso WAN 2 (Servnet).
- “Listen on port” El puerto para acceder al portal web será el predeterminado 10443.
- “Allow access from any host” se habilita para permitir el acceso desde cualquier host o dispositivo.
- “Logout users when inactive for specified period” se habilita para cerrar la sesión de los usuarios cuando estén inactivos por un período de tiempo especificado.
- “Intactive For” se coloca el tiempo de inactividad del usuario para cerrar la sesión.
- “Server Certificate” se deja el certificado predeterminado.

La configuracion se muestra en la Figura 31.

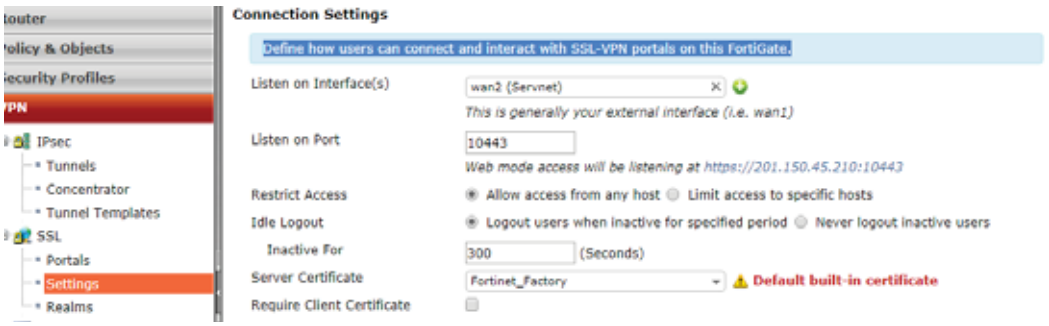


Figura 31. Configuración de conexión para la VPN.

Tunnel Mode Client Settings (Configuración modo túnel)

- “Address Range” para esta opción se selecciona “Specify custom IP range”, para conectar a rangos especificos e de IP’s.
- “IP Ranges” se colocará el rango de IP’s asociados al objeto que se creo anteriormente (VPN_SSL).
- “DNS Server” se selecciona la opción “Same as client system DNS” para ocupar el servidor dns del cliente. La configuración se muesra en la Figura 32.

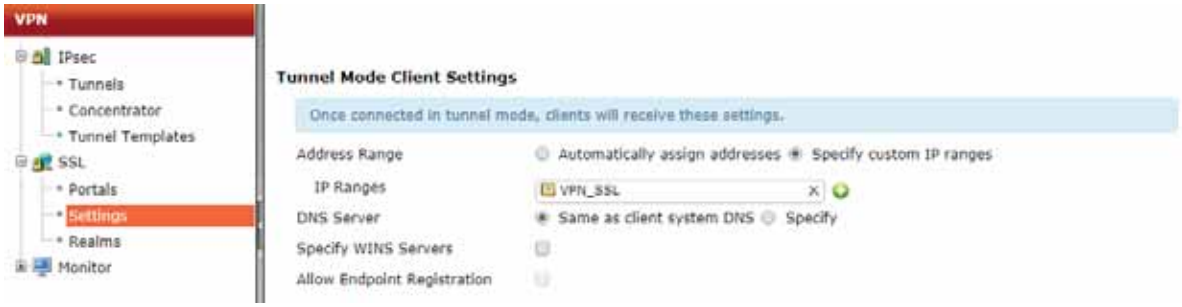


Figura 32. Configuración modo túnel para la VPN.

Authentication/Portal Mapping (Autenticación / Asignación de Portal)

- Se agregan los grupos de usuarios que harán uso de la VPN, como se muestra en la Figura 33.

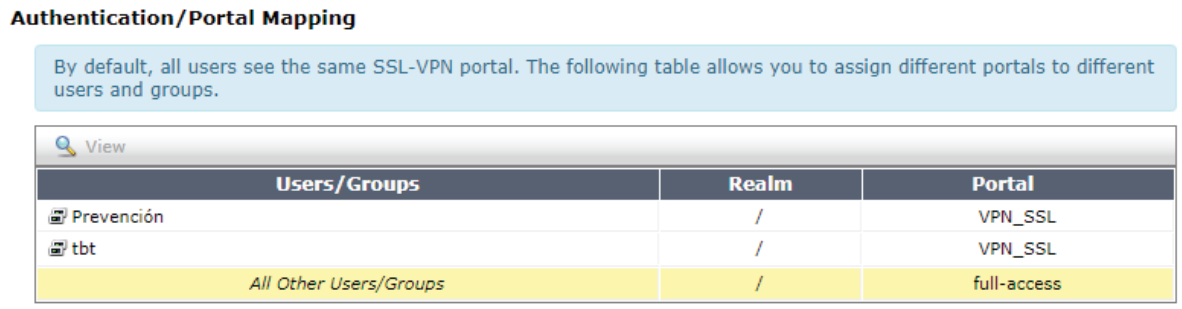


Figura 33. Grupos de usuarios agregados.

Despues de configurar los ajustes de la VPN se procede a crear una politica de seguridad para que los usuarios puedan conectarse a la red interna. Vamos a Policy & Objects > IPv4 y creamos una nueva politica la cual se configura de la siguiente manera:

- En el campo “Incoming Interface” se selecciona la interfaz Internal 1 la cual es por donde está entrara la conexión de la VPN.
- En el campo “Sourse Address se coloca el rango de IP’s de la VPN.
- En el campo “Source User(s)” se seleccionarán los grupos de usuarios que harán uso del acceso remoto.
- En el campo “Outgoing Interface” se selecciona la interfaz “Internal1” que es por donde entrará la conexión.

- En el campo “Destination Address” se selecciona la opción “LAN INTERNAL” ya que esta es la red interna.
- En el campo “Schedule” se selecciona el tiempo en el que funcionará la política se elige la opción “always” para que la política funcione siempre.
- En el campo “Service” se selecciona la opción “all” para conceder todos los servicios en cuanto a protocolos.
- En el campo “Action” se elije la opción “ACCEPT” para poder aplicar la política y darles acceso a todos los usuarios que pertenezcan a los grupos. La configuración es mostrada en la Figura 34.

Figura 34. Configuración de politica para la VPN.

La politica creada se mostrará en conjunto con las politicas de seguridad creadas con anterioridad como se muestra en la Figura 35.

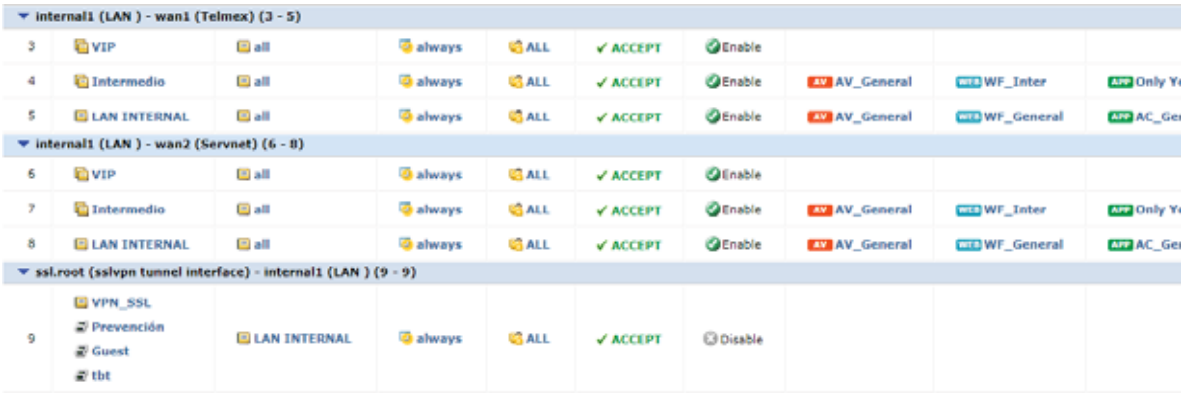


Figura 35. Lista de políticas creadas.

Con estas últimas acciones se termina la configuración de una VPN, los usuarios podrán acceder a la red interna por medio del acceso remoto creado a través de un software llamado FortiClient, la configuración de este programa se muestra a continuación:

Al iniciar el programa se mostrará una pantalla en la cual hay que seleccionar la opción “Acceso Remoto” como se muestra en la Figura 36.

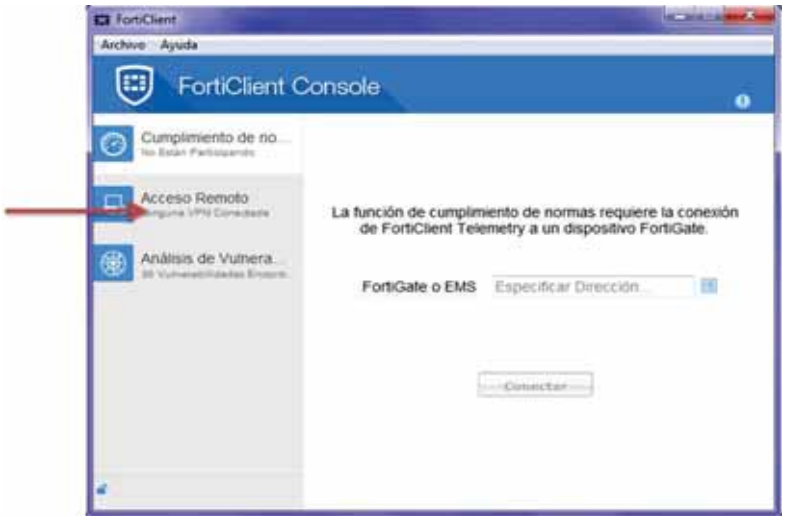


Figura 36. Pantalla de inicio de FortiClient.

Se configuran algunos ajustes para hacer la conexión, seleccionando el icono del engrane y se selecciona la opción “Adicionar una nueva conexión” tal como se muestra en la Figura 37.

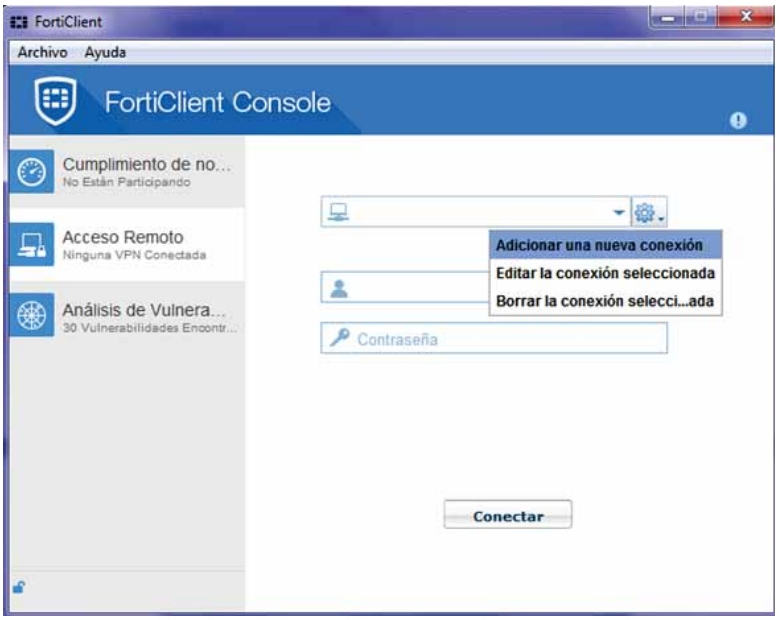


Figura 37. Pantalla de autenticación de usuarios FortiClient.

Aparecerá la siguiente pantalla mostrada en la Figura 38, en donde se coloca la configuración de la siguiente manera:

- “Nombre de la conexión” se coloca una etiqueta con la que podremos identificar a la red
- “Descripción” se colocan algunos comentarios en caso de ser necesarios.
- “Gateway Remoto” se coloca la dirección publica del enlace dedicado de la empresa y por la cual entraremos a través de la VPN a la red corporativa, está en negro por cuestiones de seguridad de la empresa IAAR.

- “Personalizar Puerto” se coloca el puerto en el cual se configuró la VPN, en este caso fue 10443.
- “Autenticación” se seleccionará la opción “Guardar Login” y en “Nombre del usuario” se colocara uno de los usuarios creados anteriormente para el acceso remoto.
- Para finalizar damos clic en cerrar.

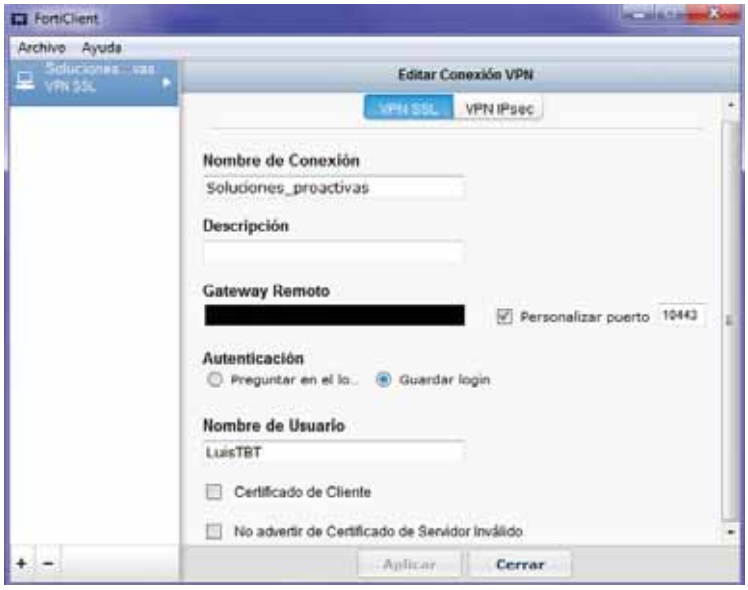


Figura 38. Configuración de la conexión VPN

Después de haber completado la configuración se mostrará la pantalla de la Figura 39 en donde se coloca la contraseña del usuario y se selecciona la opción conectar.

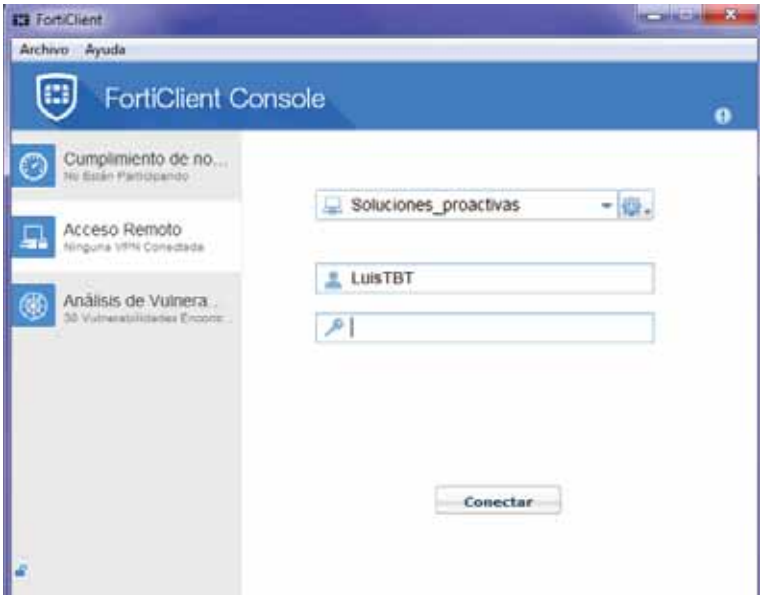


Figura 39. Pantalla de autenticación FortiClient.

Al haber colocado la contraseña correcta se hará la conexión hacia la red interna de IAAR, mostrado en la pantalla de la Figura 40. Se observa que Fortigate nos asigna una dirección dentro del rango de IP's que se configuró, teniendo una conexión exitosa.

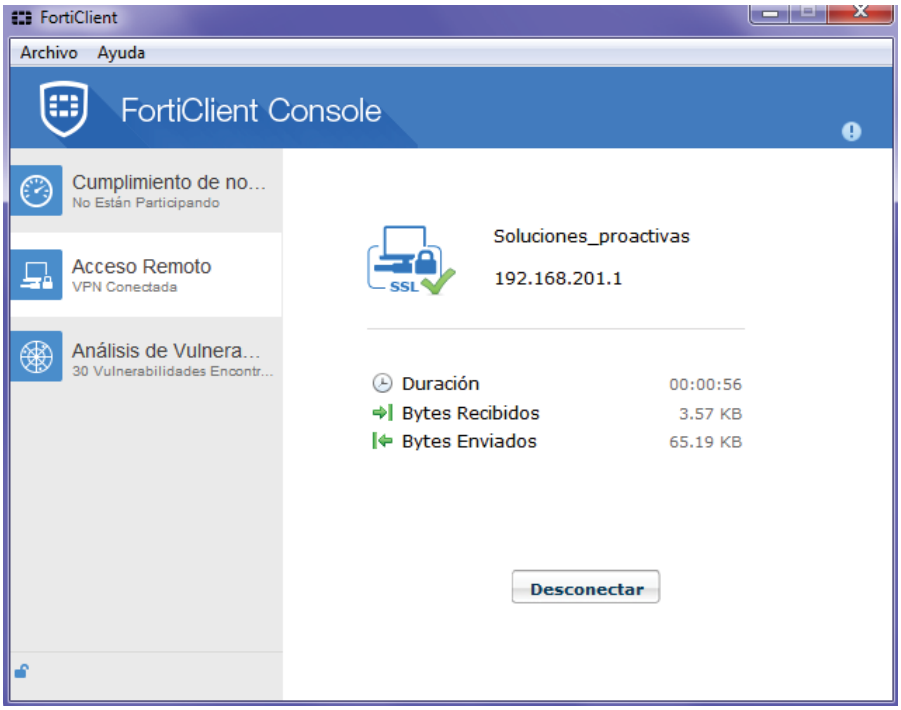


Figura 40. Pantalla de conexión exitosa en FortiClient.

Análisis para la creación de servicios con base en virtualización

Para IAAR se necesitan al servicio dos software especializados como son NOI y Microsip, estos dos programas son necesarios para las actividades administrativas de IAAR y tienen ciertas características que serán analizadas.

- NOI es un software que se utiliza para nomina integral especializado en automatizar los aspectos importantes de la nomina, con ayuda de este programa se obtiene un cálculo exacto de las deducciones y percepciones de los empleados de la empresa, este programa los requieren los empleados del área de administración.
- Microsip ventas en general este programa realiza el registro de todas las ventas hechas por la empresa desde la cotización hasta la entrega de mercancía o de prestación de servicios, este programa lo requieren los empleados del área de operaciones.

Estos dos programas pueden ser instalados en un servidor para que todos los equipos de la red que los requieran puedan acceder a ellos sin mayor problema.

Diseño para la creación de servicios con base en virtualización

Se crearán dos máquinas virtuales dentro de un dispositivo llamado *Hypervisor*, estas dos máquinas funcionarán como servidores, se instalarán los programas en máquinas distintas ya que estos programas serán usados por empleados de dos áreas diferentes.

Máquina 1 → NOI → Área de administración →Grupo VIP

Máquina 2 →Microsip → Área de operaciones → Grupo Intermedio

Se toma esta decisión en base a las políticas de seguridad ya establecidas anteriormente, ya que una máquina virtual funciona exactamente igual que una máquina física, requiriendo una dirección IP y una identidad propia dentro de Fortigate.

Las máquinas virtuales funcionarán con un sistema operativo de Windows server 2008 y serán accesibles para los trabajadores de la empresa por medio de la aplicación de escritorio remoto que ofrecen los equipos Windows. Cabe mencionar que todos los equipos dentro de la empresa cuentan con un sistema operativo de Windows.

Implementación de servicios con base en virtualización

Al igual que si fuera cualquier equipo de trabajo de la empresa, el *hypervisor* se le dotará con una IP la cual estará asociada a un objeto dentro de Fortigate y estará dentro del grupo VIP, para no tener ninguna restricción, las configuraciones son las mismas que para los equipos de computo de los empleados.

Al haber creado estas configuraciones y al ser parte de la red lo siguiente es crear las distintas máquinas para que provean a los usuarios de servicios necesarios en ella.

Entramos al programa VMware client que es el sistema operativo del *hypervisor*, con el cual se crearán las dos máquinas virtuales necesaria, la Figura 41 muestra la pantalla de inicio, donde hay que colocar la dirección IP asignada al *hypervisor* así como el nombre de usuario y contraseña.

Figura 41.Pantalla de inicio de VMware.

Al autenticarse, aparecerá la pantalla de la Figura 42.

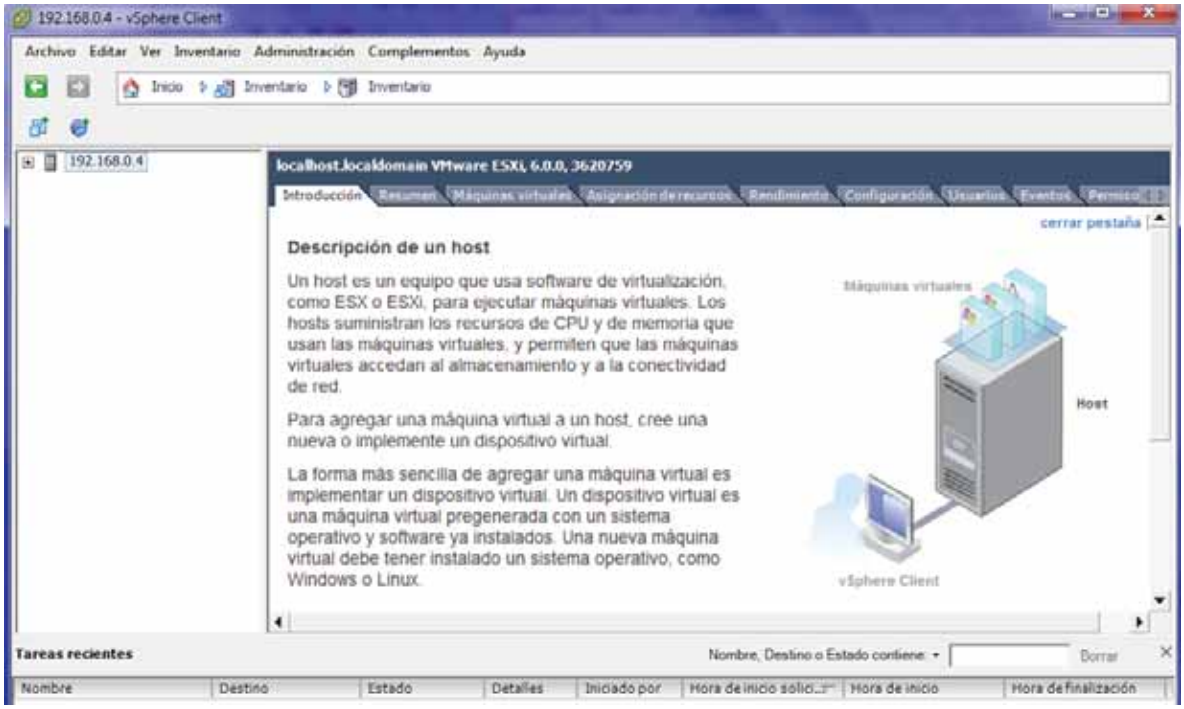


Figura 42. Pantalla principal de VMware.

A continuación se muestra la configuración de la Figura 43 a la Figura 56 para construir las máquinas virtuales.

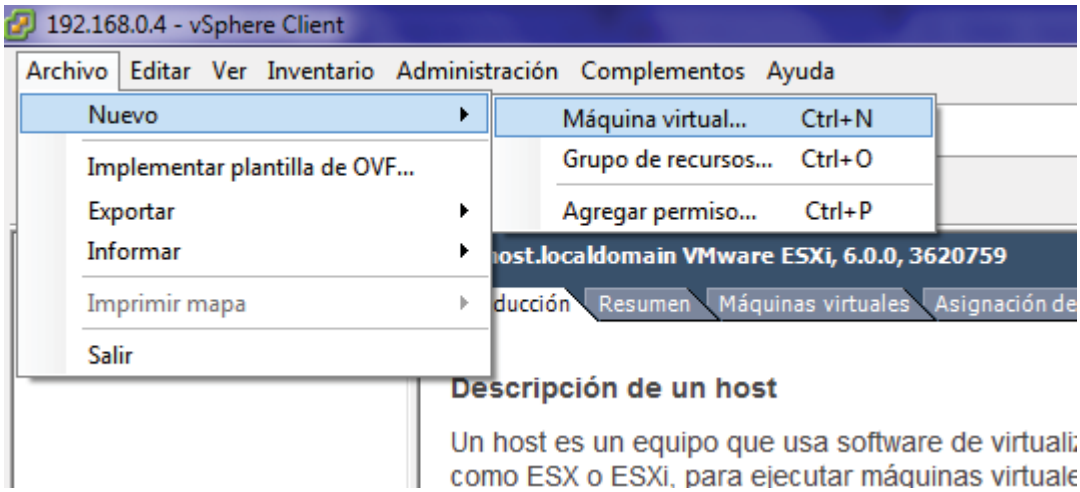


Figura 43. Creación de una nueva máquina virtual

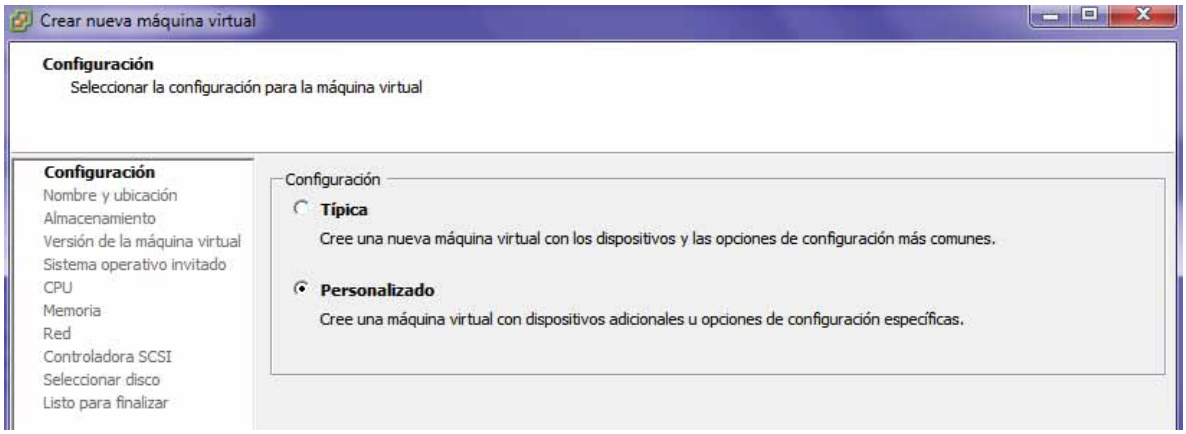


Figura 44. Selección de modo personalizado para la máquina virtual.

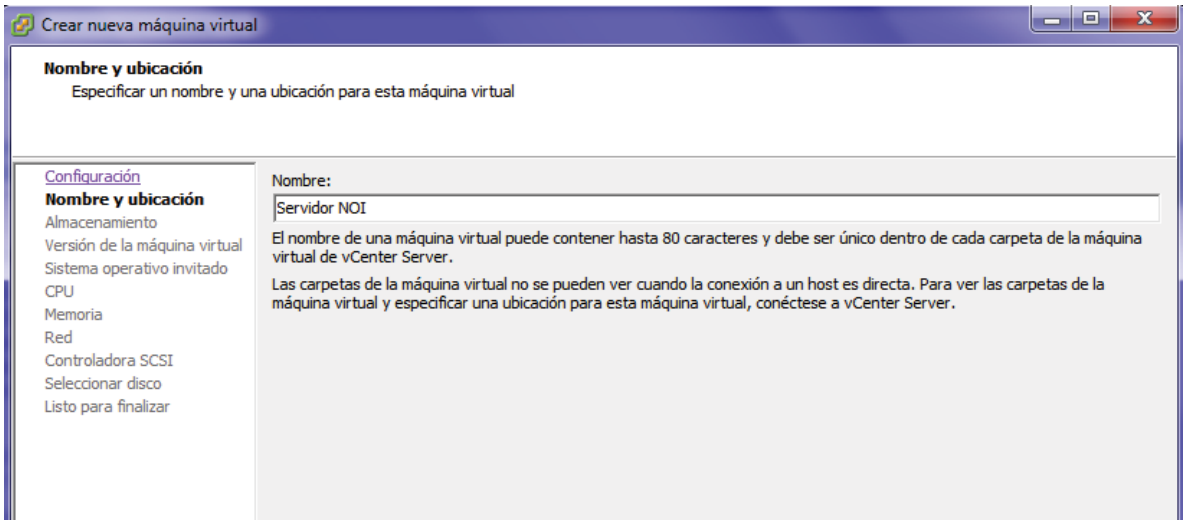


Figura 45. Selección del nombre de la máquina virtual a crear.

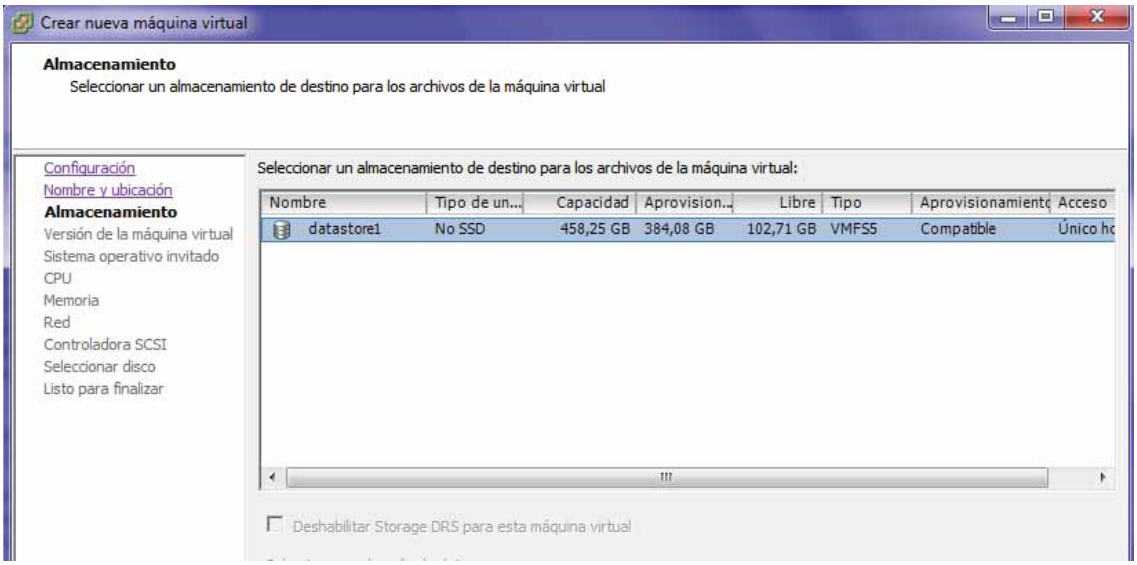


Figura 46.Seleción del medio de almacenamiento de los archivos de la máquina.

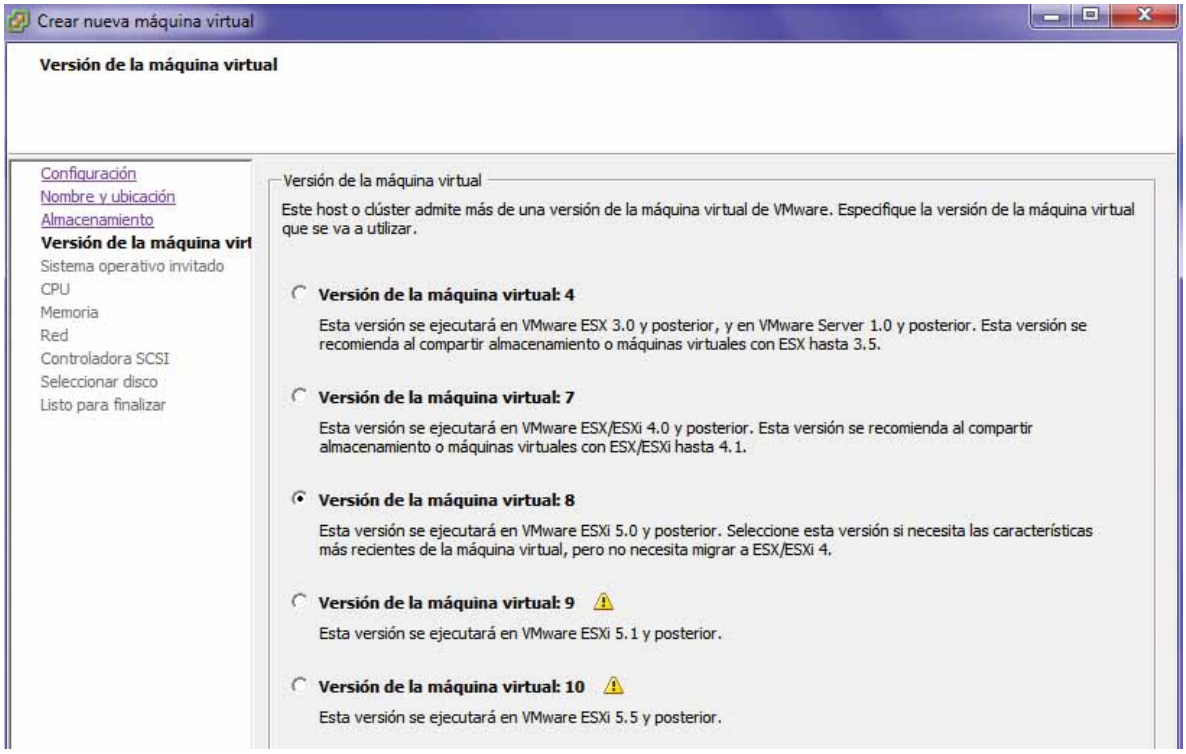


Figura 47. Versión de la máquina virtual.

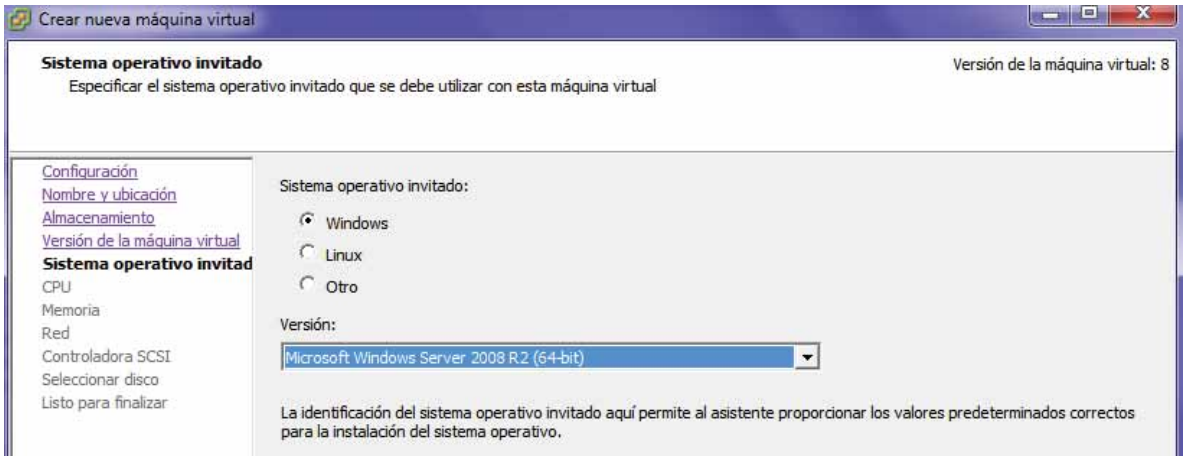


Figura 48. Selección del sistema operativo de la máquina virtual.

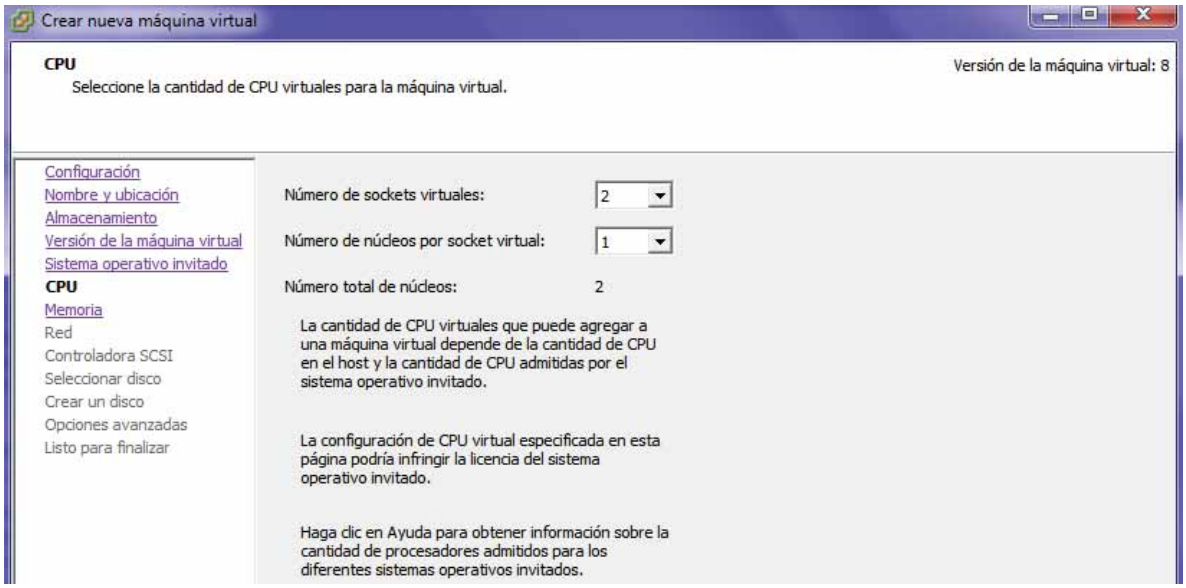


Figura 49. Selección del número de unidades del procesamiento.

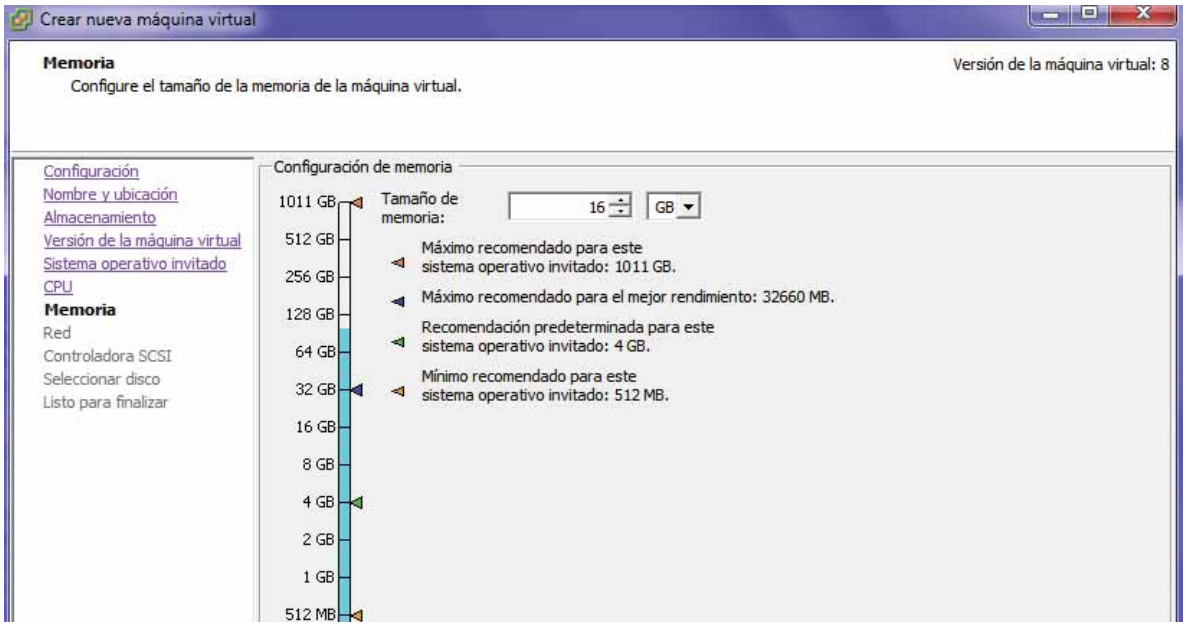


Figura 50. Configuración del tamaño de la RAM.

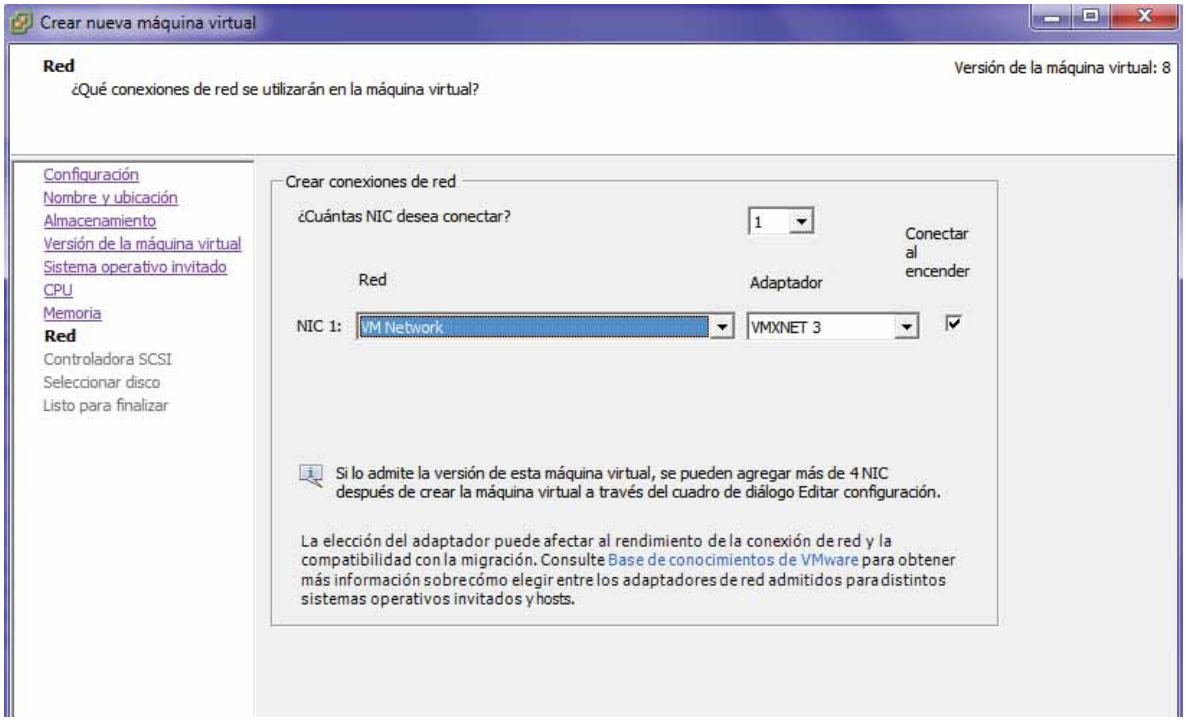


Figura 51. Selección del adaptador de tarjeta de red.

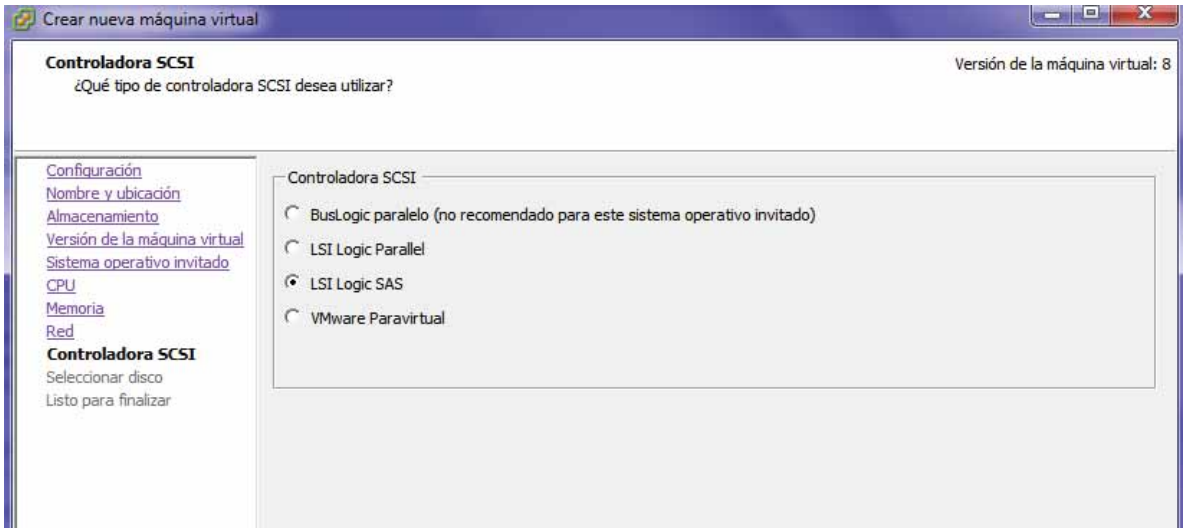


Figura 52. Selección del puerto paralelo para la conexión de dispositivos.

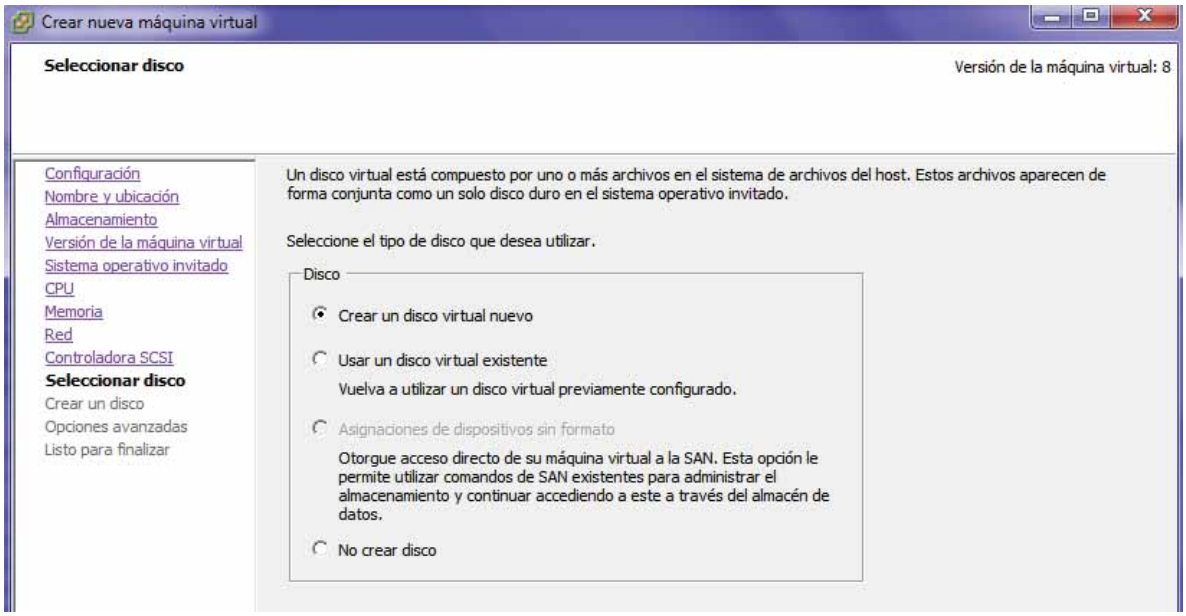


Figura 53. Creación del disco virtual.

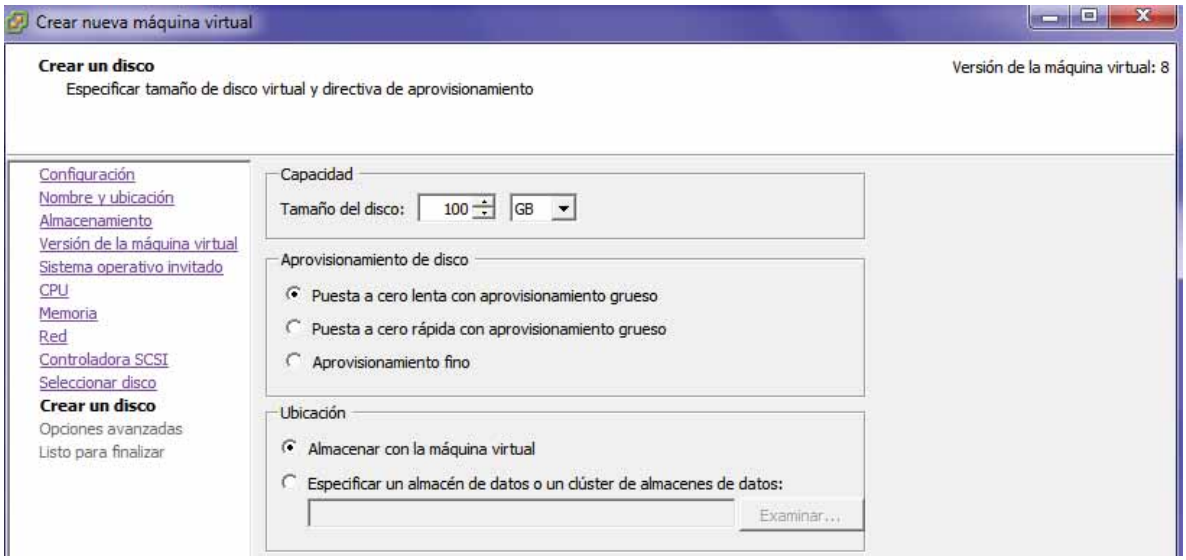


Figura 54. Configuración del tamaño del disco virtual.

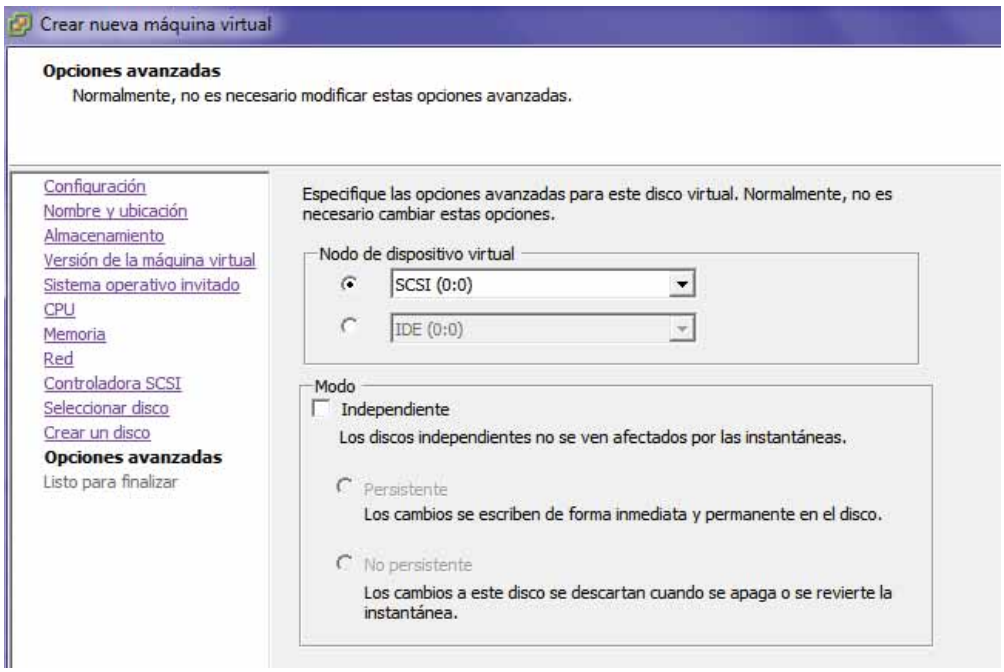


Figura 55. Configuración del adaptador de disco.

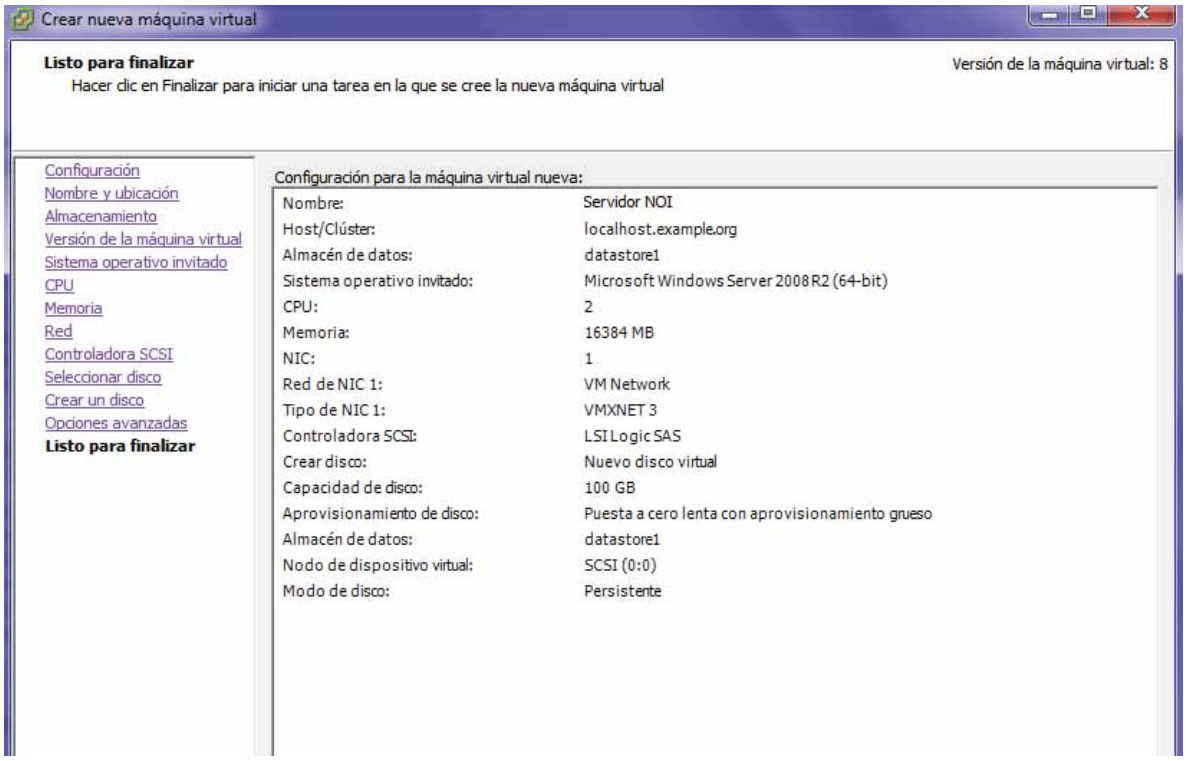


Figura 56. Resumen de la configuración elegida de la máquina virtual.

Después de la configuración anterior se mostrará una pantalla (Figura 57) en la cual hay que seleccionar un disco o una imagen ISO para la instalación de Windows server 2008, hay que tener una licencia vigente para poder instalar el programa en la máquina virtual.

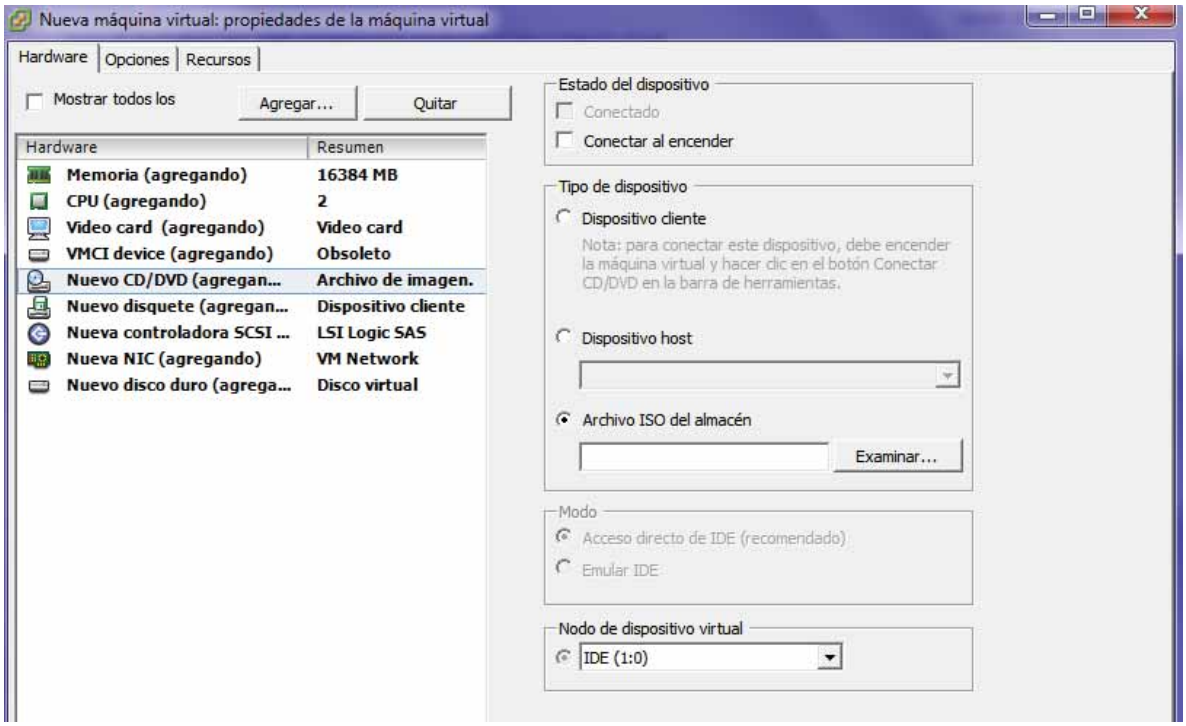


Figura 57. Carga de imagen ISO o CD de instalación de Windows server 2008.

Con este mismo procedimiento se crea la segunda máquina virtual y se mostrarán ya creadas en la interfaz del *hypervisor* como se muestra en la Figura 58.

Figura 58. Máquinas virtuales creadas.

Después de haber creado los servidores virtuales, se instalan los programas especializados a cada una de ellas.

Maquina virtual “Servidor NOI” → Instalar NOI

Maquina Virtual “Servidor Bussines Admin” → Instalación de Microsip

Al instalar cada uno de los programas, se configuran las máquinas virtuales, asignándoles una dirección IP por DHCP como se muestra en la Figura 59.

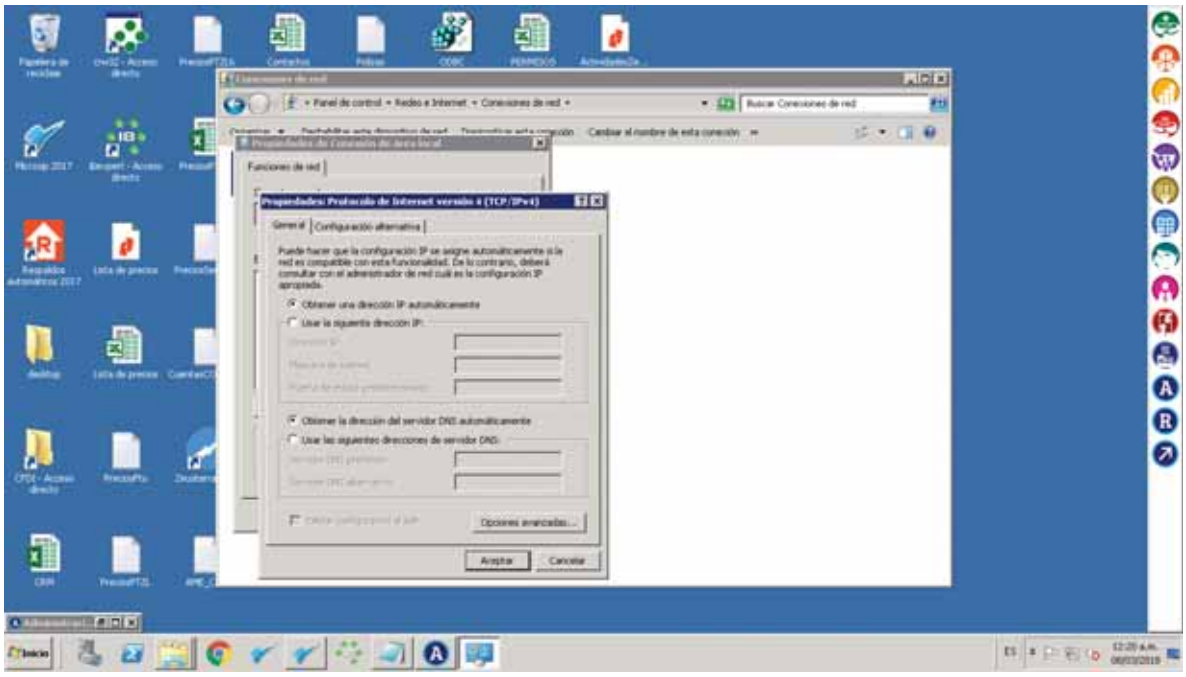


Figura 59. Configuración de IP de una máquina virtual.

Al igual que los equipos físicos las máquinas virtuales deberán ser asociadas con un objeto y una política de seguridad y para esto se hará exactamente lo mismo que como se hizo con los equipos físicos de los empleados de la empresa.

El acceso a los servicios será por medio de la aplicación de escritorio remoto de Windows el cual se muestra en la Figura 60, se coloca la dirección IP de la máquina virtual.

Figura 60. Aplicación de escritorio remoto de Windows.

Para proporcionar los servicios a todos los usuarios que harán uso de ellos se crean varios usuarios dentro de la máquina virtual, así cada usuario podrá hacer uso de esta máquina al mismo tiempo sin ninguna dificultad, los usuarios creados se muestran en la Figura 61.

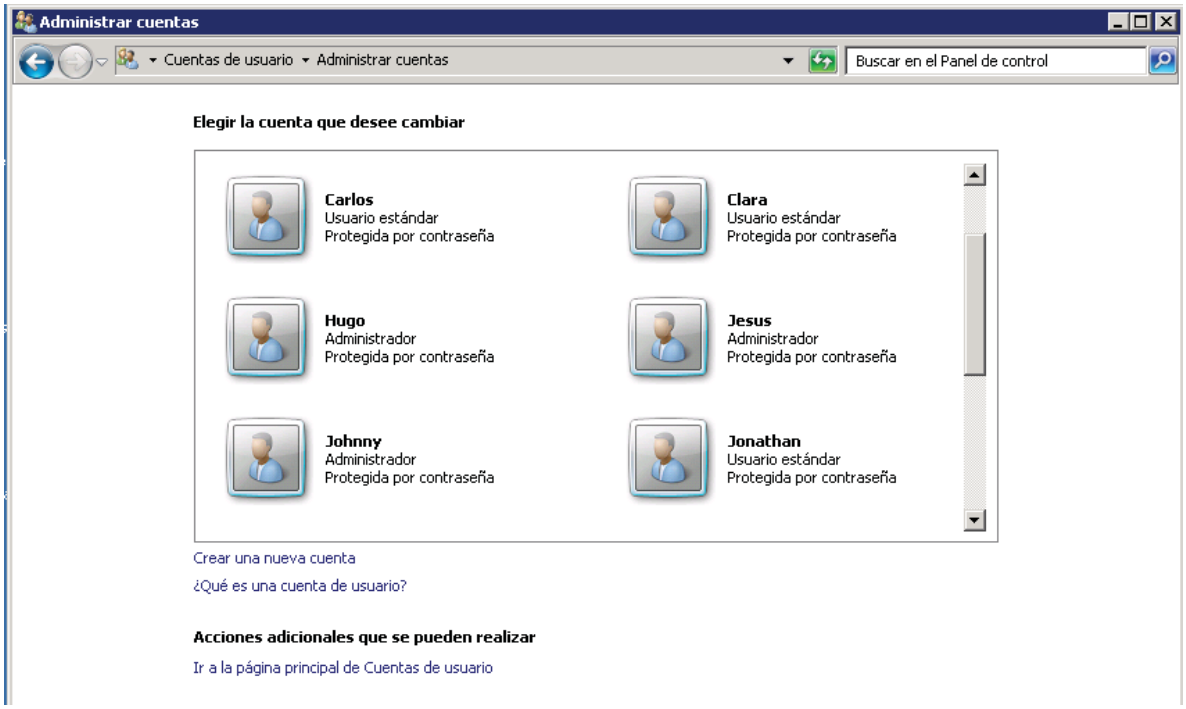


Figura 61. Usuarios de la máquina virtual.

Así se garantiza que cada uno de los empleados que hagan uso de la máquina virtual tengan un usuario asignado y una contraseña por lo cual cada uno de ellos desempeñe sus actividades sin contratiempos.

Al ingresar a la máquina virtual por medio del escritorio remoto la aplicación pedirá que se identifique el usuario como se muestra en la Figura 62.

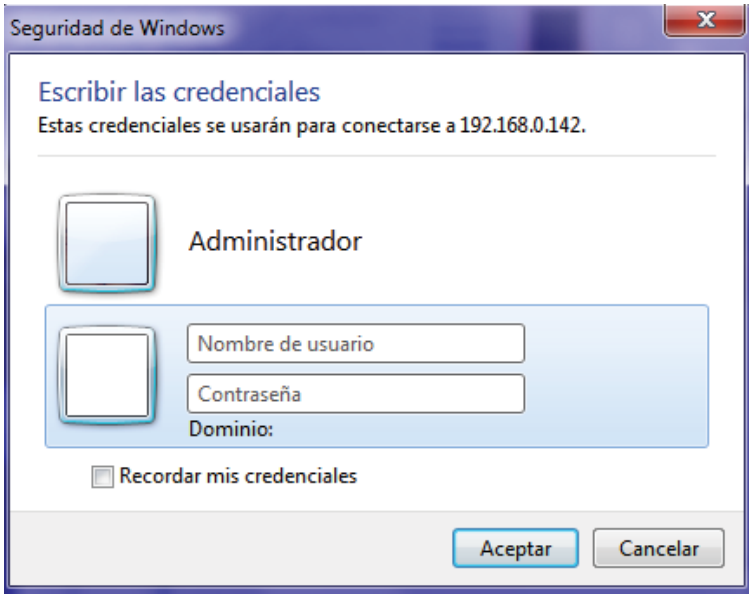


Figura 62. Autenticación del usuario en escritorio remoto.

Se coloca el usuario y la contraseña y se podrá acceder a la máquina y a los servicios que ofrece tal como se muestra en la Figura 63.

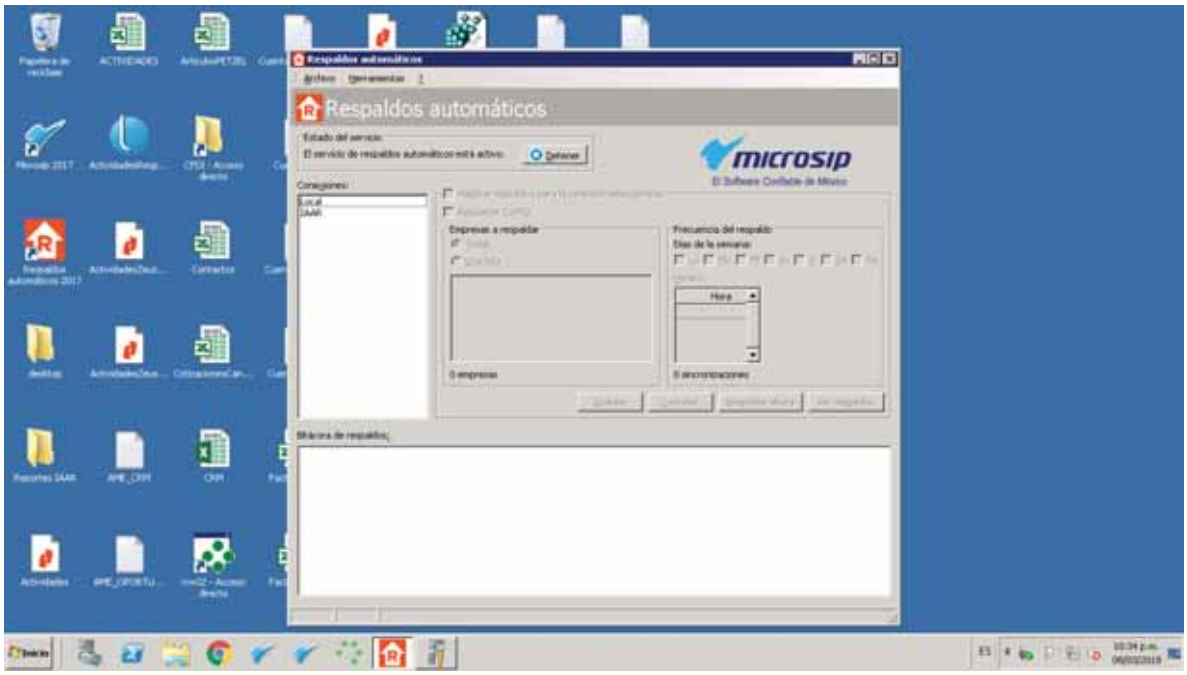


Figura 63. Escritorio de la máquina virtual.

Análisis de una herramienta de monitorización

La herramienta que se eligió para el desarrollo de este proyecto es Panda Cloud System Management que es una solución eficaz para la monitorización y administración remota de dispositivos basada en la nube.

Se decidió trabajar con esta herramienta ya que además de que cumple con uno de los objetivos de este proyecto, también TBT tiene una licitación para poder utilizar la aplicación.

La herramienta ofrece la adición de zonas o empresas de las cuales se lleva a cabo un control y monitorizar cada uno de los equipos añadidos a estas zonas, además la herramienta trabaja bajo un protocolo SNMP con el cual se puede tomar control de un equipo o dispositivo añadido a las zonas creadas, por medio de la instalación de un agente que es un software que ayudará a la monitorización y gestión de los dispositivos.

Integración del protocolo SNMP a la red corporativa

Para integrar la herramienta se debe contar con una licitación y entrar al sistema o la pagina principal del servicio https://www.pandacloudsecurity.com/ donde se debe colocar las credenciales de autenticación para ingresar a la herramienta, como se muestra en la Figura 64.

Figura 64. Pantalla de autenticación de Panda Cloud

En Panda Cloud System Management se agregan zonas en las cuales así mismo se le agregan dispositivos pertenecientes a ellas, estas zonas no son más que una agrupación de dispositivos pertenecientes a la misma oficina o red. Dentro de la interfaz seleccionaremos la opción Zonas > Nueva Zona como se muestra en la Figura 65.

Figura 65. Crear una nueva zona en Panda Cloud.

Se configuran los datos de la zona que se agregará, como se muestra en la Figura 66.

- “Nombre” se coloca el nombre de la zona.
- “Descripción” se colocan comentarios en caso de ser necesario.
- “Tipo“ se habilita la opción “Administrado” que incluye monitorización y administración de la red.

- “Tipo de proxy” se selecciona “ninguno” ya que no se hará uso de ningún proxy.
- “Rol” se selecciona administrador.

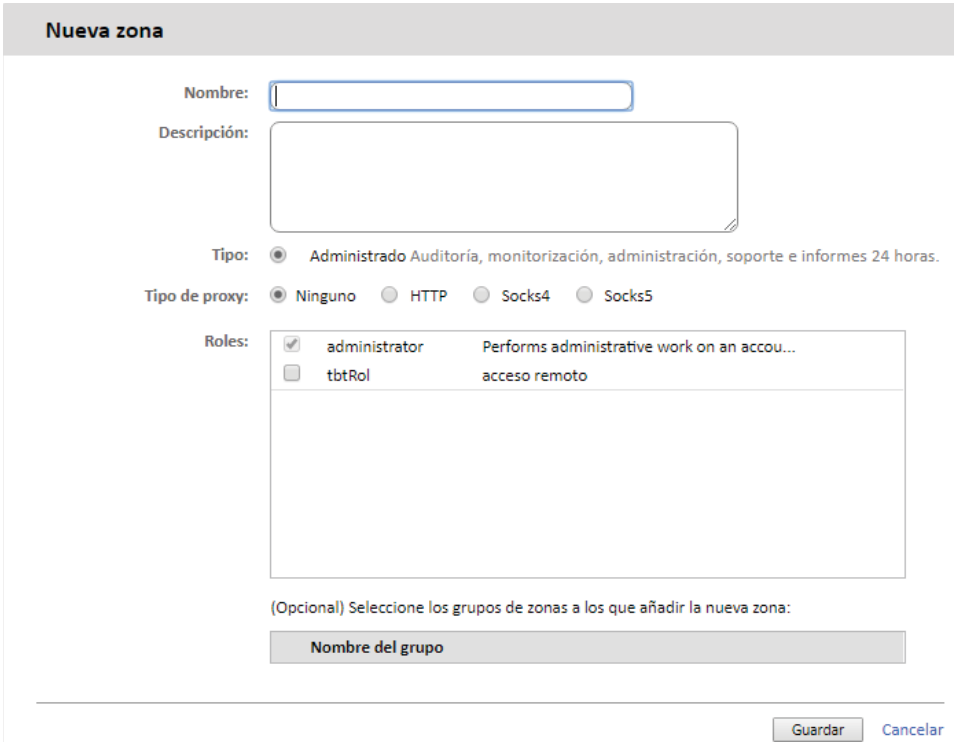


Figura 66. Configuración de una nueva zona.

Después de configurar la zona se agregarán los dispositivos pertenecientes a ella y a la red, en la opción “Añadir dispositivos” como se muestra en la Figura 67.

Figura 67. Añadir dispositivos a una zona

Se seleccionará el tipo de dispositivo (Figura 68) que se agregará a la zona para su administración y monitoreo, en cada una de estas opciones se llenaran algunos campos o datos del dispositivo, como IP, nombre del equipo, entre otros.

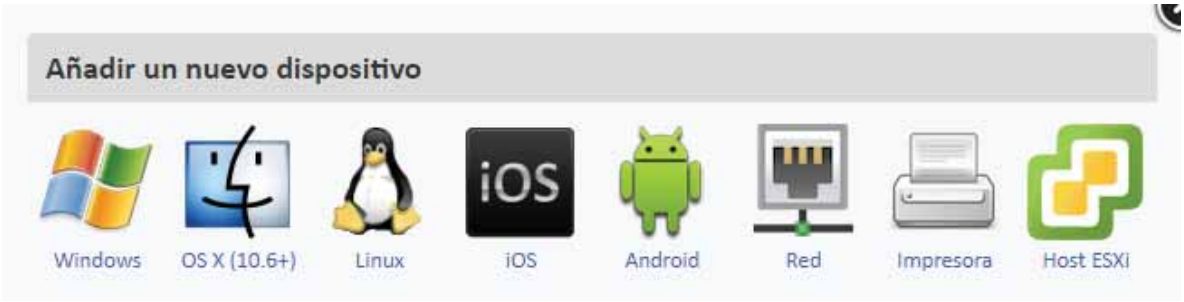


Figura 68. Tipos de dispositivos que se pueden agregar a la zona.

Después haber selecciona el dispositivo y llenado los datos de cada uno, se le enviará al usuario del dispositivo una liga o link por correo electrónico para instalar el agente o se puede instalar de manera física en la computadora del usuario solo dando clic en el icono del tipo de dispositivo que se quiere añadirá la zona, el cual ayuda a que la herramienta realice sus funciones como se muestra en la Figura 69, esto hace excepción para los dispositivos de red tales como NAS, Host ESXI e Impresoras.

Figura 69. Descarga del agente.

Después de haber realizado los pasos anteriores la zona quedara completada y se mostrara como en la figura 70.

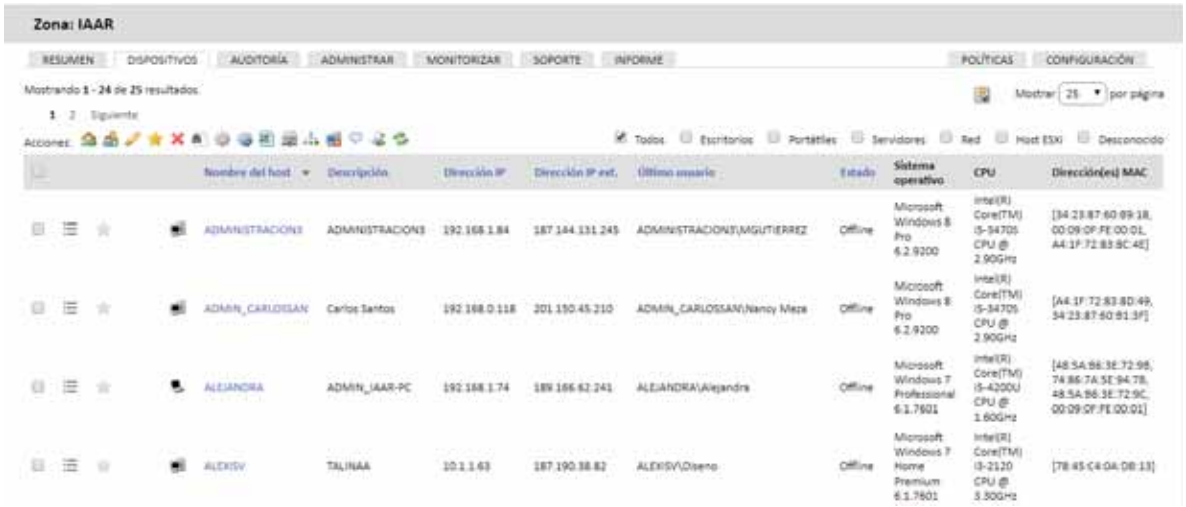


Figura 70. Zona IAAR completada.

La monitorización de los equipos se hace seleccionado el dispositivo agregado a la zona y dando clic en el icono “ojo” como se muestra en la Figura 71.

Figura 71. Monitorización de un equipo.

Con este procedimiento podemos observar lo que el usuario está realizando en su equipo, además se puede tomar control de él si es necesario, esto ayuda a hacer algunas configuraciones en los equipos sin tener la necesidad de manipularlos físicamente, como se muestra en la Figura 72.

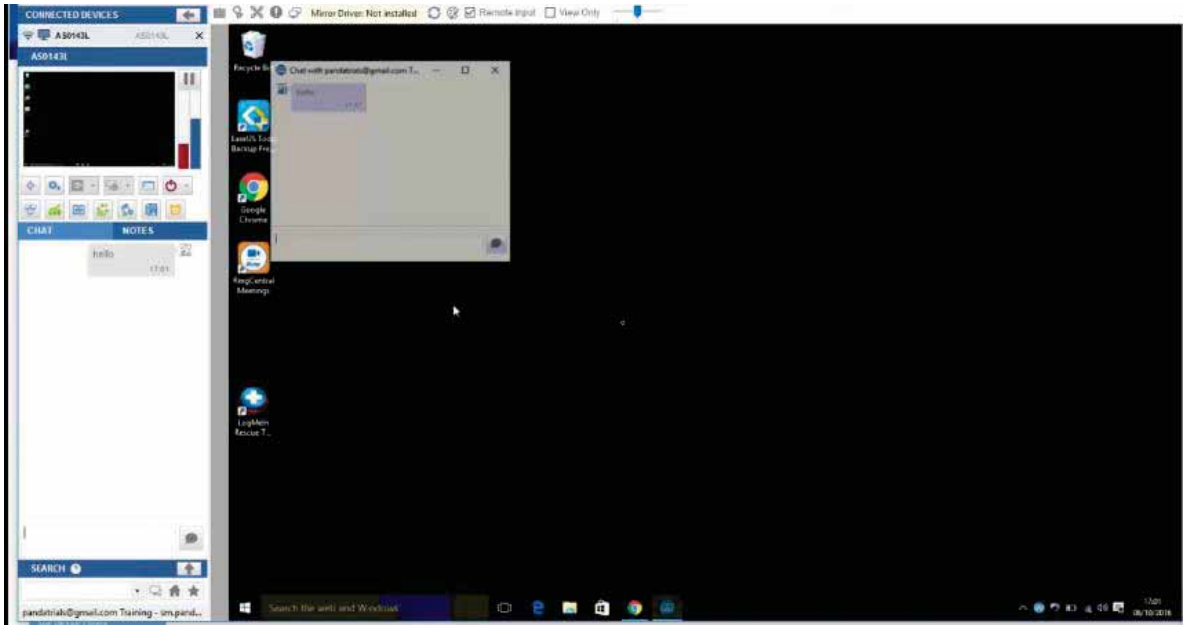


Figura 72. Monitorización de un equipo.

Análisis de políticas de autenticación

Las políticas de autenticación son muy importantes ya que determinarán que usuarios pueden acceder o no a la información contenida en el dispositivo NAS, en IAAR hay varias carpetas o directorios que se comparten en red con los usuarios, pero no todos los usuarios tiene acceso a todas las carpetas, sino que solo tienen acceso a las que ocupan para el desempeño de sus actividades.

Para este caso se recopilo información con el director de la empresa para que indique que información será utilizada o requerida por los usuarios o trabajadores.

Diseño de políticas de seguridad

En IAAR se aplicarán políticas de autenticación de acuerdo al puesto y al departamento al que pertenecen mostrando a continuación los directorios o carpetas que se crearán y cuáles son los empleados que tendrán acceso a su información.

Principalmente se crearán siete carpetas que se presentan a continuación junto con los usuarios que harán uso de ellas y de la información contenida.

Administración General → Usuarios: administración, dirección y sistemas los cuales tendrán permisos de lectura y escritura es decir podrán ver o consultar la in formación así como modificarla.

Desarrollo Organizacional → Usuarios: recepción y sistemas los cuales tendrán permisos de lectura y escritura.

Histórico → Usuarios: administración, dirección, operaciones, administración y sistemas además de algunos usuarios de las sucursales de Querétaro y Toluca los cuales podrán ingresar a ella a través del acceso remoto VPN.

Programas → Esta carpeta contiene algunos programas utilizados en el corporativo y solo tendrá acceso a ella el área de sistemas.

Riesgos → Usuarios: recipientes, operaciones, administración, dirección, recepción y sistemas.

Ventas → Usuarios: administración y dirección.

Sistemas → Solo el área de sistemas tendrá acceso a ella.

Implementación de políticas de seguridad

La implementación de las políticas de seguridad se hace a través de la interfaz del NAS Sygnology entrando desde el navegador web colocando la dirección IP que le fue asignada y que pertenece al segmento de red de la empresa (192.168.0.17) aparecerá la

pantalla mostrada en la Figura 73, donde se tendrá que colocar un usuario y contraseña las cuales solo debe tener el administrador de la red.

Figura 73. Pantalla de inicio del Sygnology.

Al entrar, se mostrará el escritorio de la Figura 74 mostrando varias opciones e iconos.

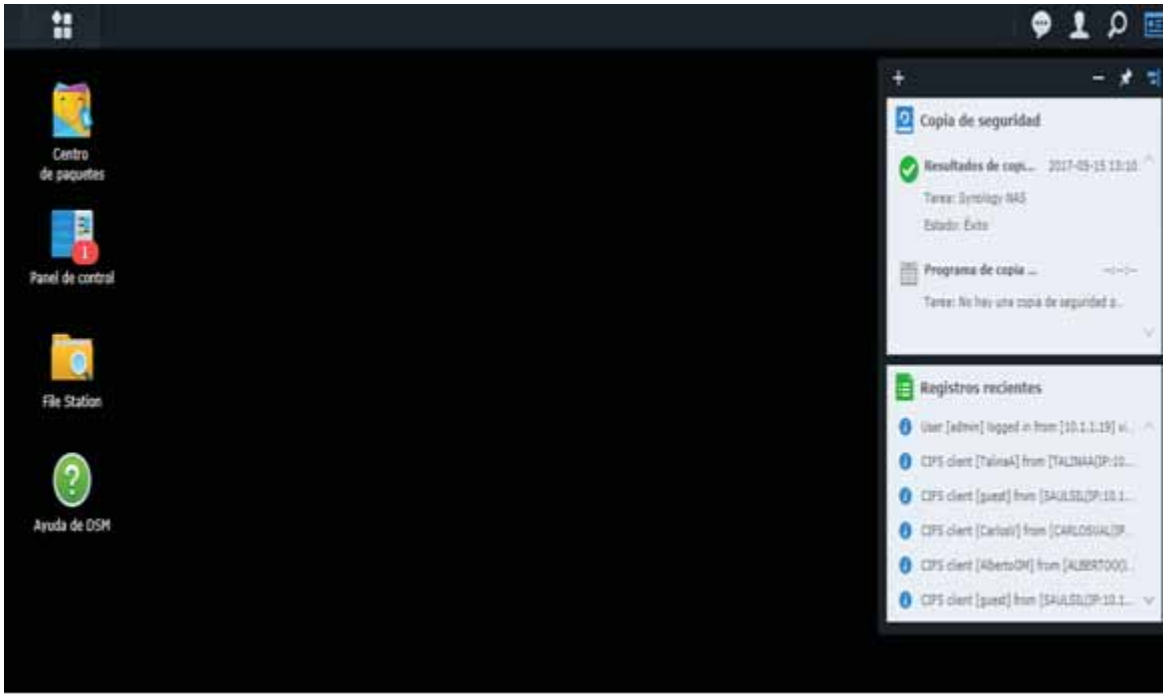


Figura 74. Escritorio del Sygnology.

Para comenzar con la creación de las políticas de acceso y autenticación se crearán los usuarios de la red los cuales utilizaran las carpetas compartidas y la información contenida en ellas. Seleccionamos el ícono de “Panel de Control”, y posteriormente elegimos “Usuario” como se muestra en la Figura 75.

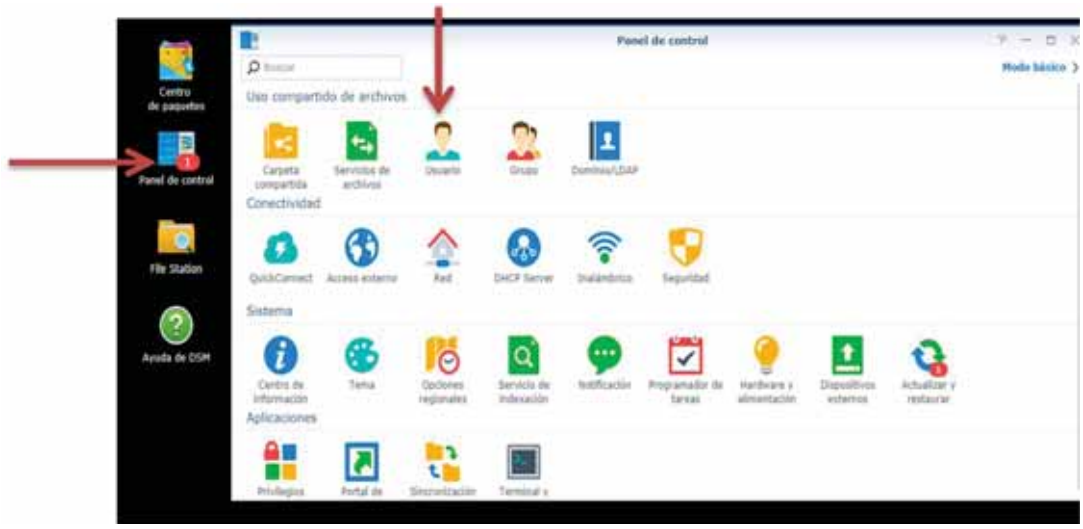


Figura 75. Creación de un nuevo usuario.

Nos desplegará un submenú, donde existe la opción “crear” tal como se muestra en la Figura 76.

Figura 76. Creación de un nuevo usuario.

Después se desplegará un menú donde daremos formato al nuevo usuario llenando los campos y la información que nos pide.

- “Nombre” se coloca el nombre del usuario.
- “Drescripcion” se colocan algun comentario como por ejemplo el departamento al que pertenece el usuario.
- “Correo electronico” se coloca opcionalmente el correo del usuario.
- “Contraseña” se coloca la contraseña con la cual el usuario podra tener acceso a al información.
- “Confirmar contraseña” se volvera a colocar la contraseña para verificar que no haya errores.

- La opción “no permitir que el usuario cambie la contraseña de la cuenta” deberá activarse tal como se muestra en la Figura 77.

Figura 77. Formato de nuevo usuario.

Después de haber creado todos los usuarios con el mismo procedimiento, se crearán las carpetas que contendrán la información confidencial de la empresa.

En el escritorio principal, se selecciona “File Station” y seleccionamos la opción del menú “crear”, para crear una nueva carpeta como se muestra en la Figura 78. El submenú contiene las opciones “nueva carpeta” y “nueva carpeta compartida”, se selecciona la opción de “nueva carpeta compartida” para crear una carpeta raíz que a su vez dentro de ella tendrá subcarpetas que podrán crear los usuarios que ya tengan acceso esta carpeta raíz.

Figura 78. Crear una nueva carpeta compartida.

A continuación se presenta la configuración para la nueva carpeta compartida:

- “Nombre” se coloca el nombre que tendrá la carpeta compartida.
- “Descripción” se colocan comentarios en caso de ser necesarios.
- “Ocultar subcarpetas y archivos de usuarios sin permisos” se habilitará esta opción
- Se habilita la opción “Habilitar papelera de reciclaje” y su opción “Acceso restringido únicamente a administradores”,

La papelera de reciclaje cumple una función importante ya que si alguno de los usuarios borran algún archivo accidentalmente, este se encontrará en la papelera de reciclaje de la carpeta. La configuración se muestra en la Figura 79.

Figura 79. Creación de una carpeta compartida.

Se asignan permisos a los usuarios que podrán acceder a la carpeta compartida, configurando con exactitud los parámetros, ya sea de lectura/escritura, lectura o negar el acceso como se muestra en la Figura 80.

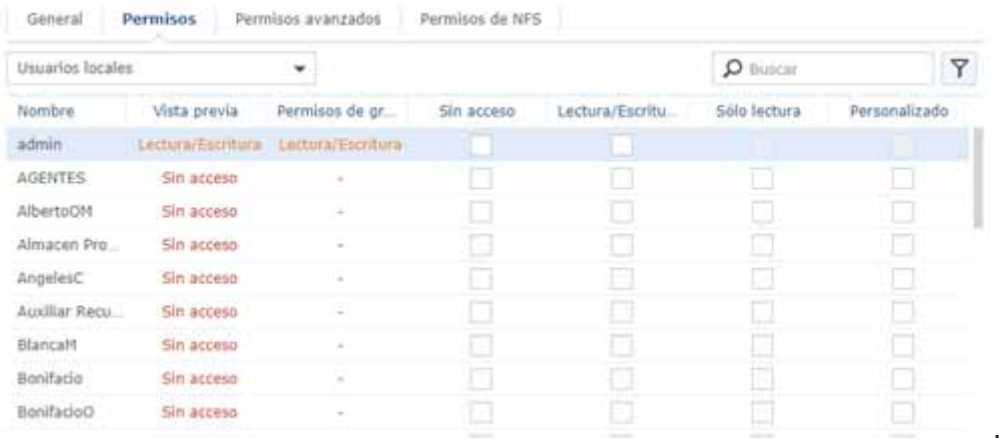


Figura 80. Configuración de permisos de la nueva carpeta compartida.

La carpeta quedará creada y los usuarios tendrán los permisos planteados por la empresa, así se garantiza que cada empleado pueda consultar o modificar la información de las carpetas a las que tiene acceso o permiso. La figura 81 muestra la carpeta “Histórico” con los permisos para cada usuario.

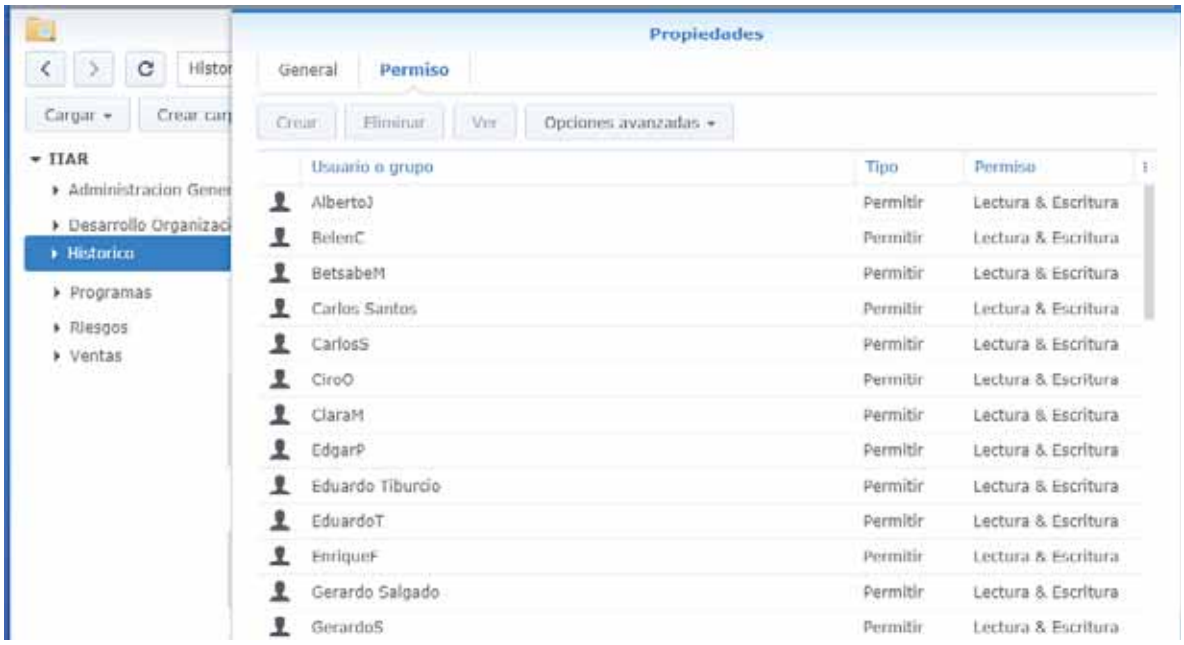


Figura 81. Propiedades de la carpeta “Histórico”.

Para que los usuarios tengan acceso a las carpetas se configuran credenciales Windows en cada uno de sus equipos en panel de control > Cuentas de usuario > Administrador de Credenciales, como se muestra en la Figura 82.

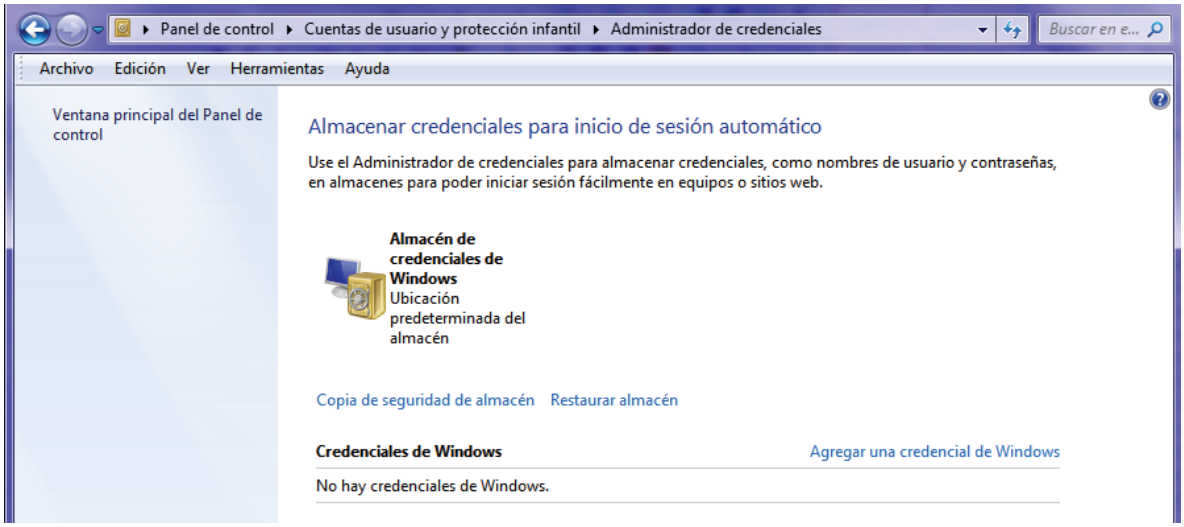


Figura 82. Administrador de credenciales Windows.

Se selecciona la opción “Agregar una credencial de Windows” y aparecerá la pantalla de la Figura 83. Donde se colocará la siguiente configuración:

- “Dirección de red o Internet” se colocará la dirección IP del dispositivo NAS Sygnology.
- “Nombre del usuario” se coloca el nombre del usuario creado en el NAS Sygnology

- “Contraseña” se coloca la contraseña asignada.

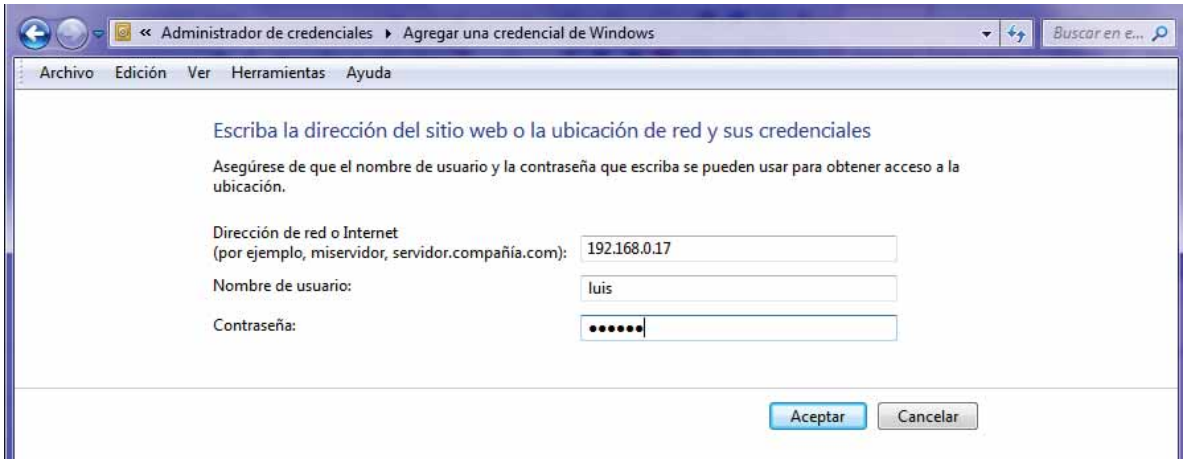


Figura 83. Configuración de credenciales Windows.

Después en el explorador de archivos de Windows se colocará la dirección IP del dispositivo NAS y aparecerán las carpetas compartidas creadas tal como se muestran en la Figura 84.

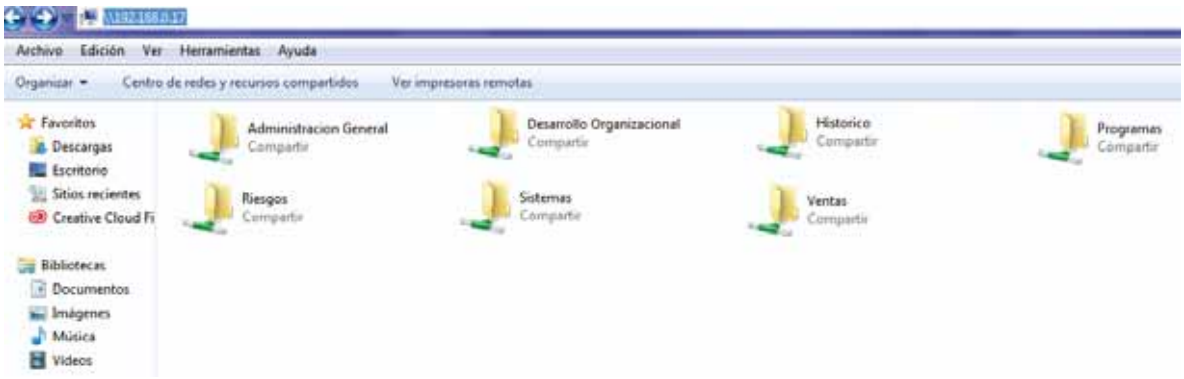


Figura 84. Carpetas compartidas en el explorador de archivos de Windows.

Análisis y creación de un enlace redundante

Dentro del Firewall Fortigate 90D se configuró a los dos enlaces de internet con los que cuenta IAAR de manera redundante, para que se tuviese un enlace principal y un enlace secundario, el cual se convierte en el principal en caso de la pérdida del servicio o de falla del enlace principal.

La forma para lograr esto es configurando al enlace principal con una menor distancia menor que al del enlace secundario ya que Fortigate automáticamente lo tomará como enlace principal al que tenga menor distancia. Vamos a Routers > Static Routers como se muestra en la Figura 85.

Figura 85. Enlaces de IAAR.

Se edita la interfaz WAN 1 y se coloca en “Administrative Distance” una distancia de 10 o un alcance mayor para que este sea el enlace secundario tal como se muestra en la Figura 86.

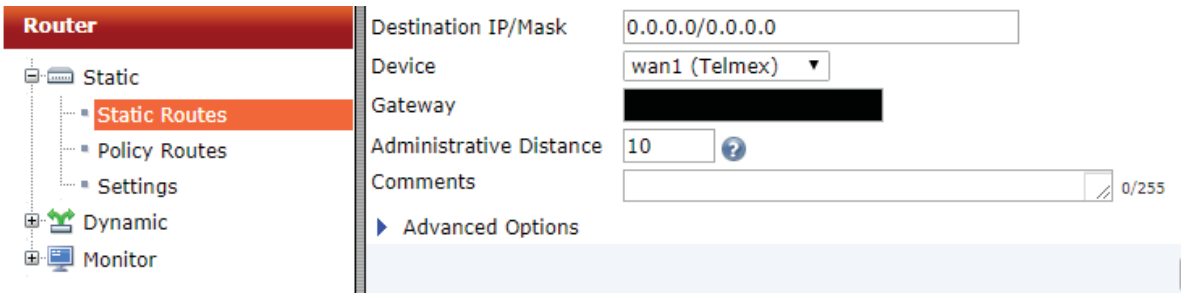


Figura 86. Configuración de la WAN 1

Para la WAN 2 se coloca en “Administrative Distance” una distancia de 5 o un alcance menor para qué este enlace sea el enlace principal tal como se muestra en la Figura 87.

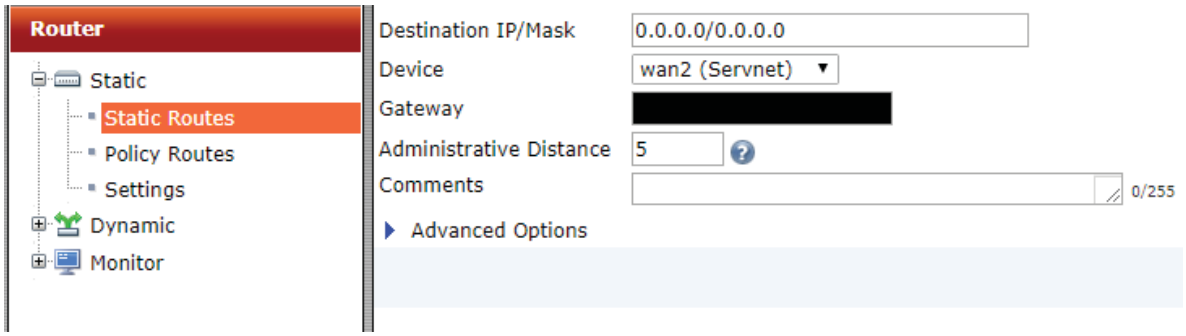


Figura 87. Configuración de la WAN 2

Con esta configuración se cumple uno de los objetivos de este proyecto.

Resultados gestión de red

Para las políticas de seguridad los resultados fueron satisfactorios ya que en todos los equipos de IAAR se restringía el acceso a sitios web como Facebook, por ejemplo la maquina con la dirección IP 192.168.0.142 se hizo la prueba para acceder a esta red social y denegó el acceso como se muestra en la Figura 88, además en Fortigate se registro que la máquina trato de acceder al sitio y se le fue denegado el acceso tal como se muestra en la Figura 89.

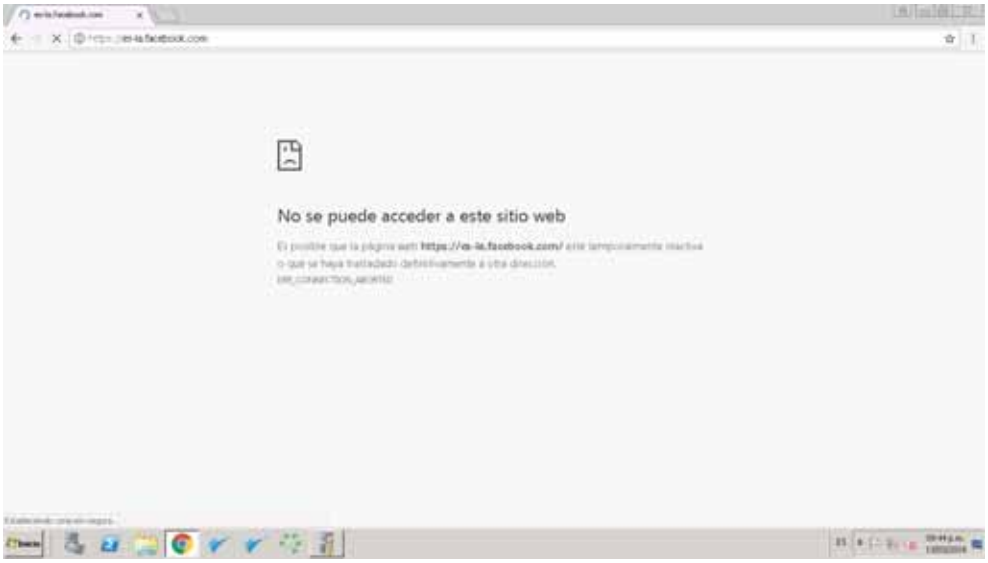


Figura 88. Bloqueo del sitio Facebook para un empleado.

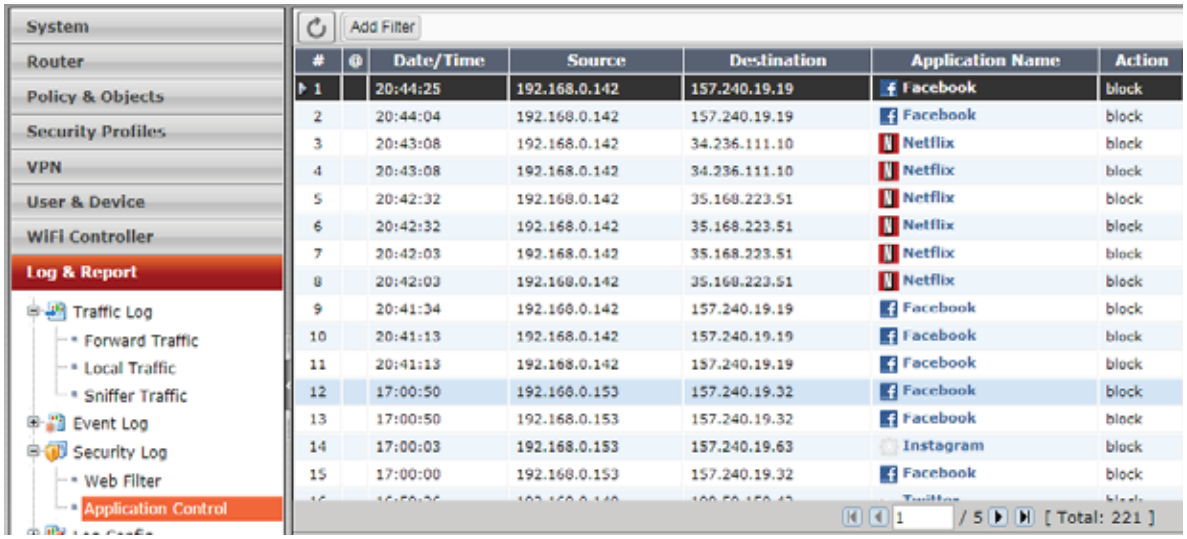


Figura 89. Registro del bloqueo del sitio web Facebook.

Para el acceso remoto se confirmo que todos los que requerían de él pudieran ingresar a la red para consultar información, subir reportes, hacer uso de servicios de red, entre otros, además también se observo que Fortigate monitorea quienes son los que recientemente se conectan a la red interna de forma remota, tal como se muestra en la Figura 90.

Figura 90. Usuarios que recientemente se conectaron a la red interna de forma remota.

La creación de servicios no dio ningún problema todos los usuarios pudieron hacer uso de ellos tanto como los que necesitan los servicios dentro de la red así también como para los que se encuentran fuera de está.

La integración de System Cloud Panda fue exitosa ya que con este pudimos hacer las configuraciones y adecuaciones a los equipos de la sucursal IAAR Querétaro y Toluca para que se conectarán de forma remota a la red interna de IAAR CDMX.

La creación de políticas de acceso y autenticación también resulto de forma satisfactoria ya que los usuarios al tratar de tener acceso a carpetas a las cuales no tienen los permisos para entrar se muestra la pantalla de la Figura 91, la cual se pide que se autentique para conceder permisos en caso de que los tenga.

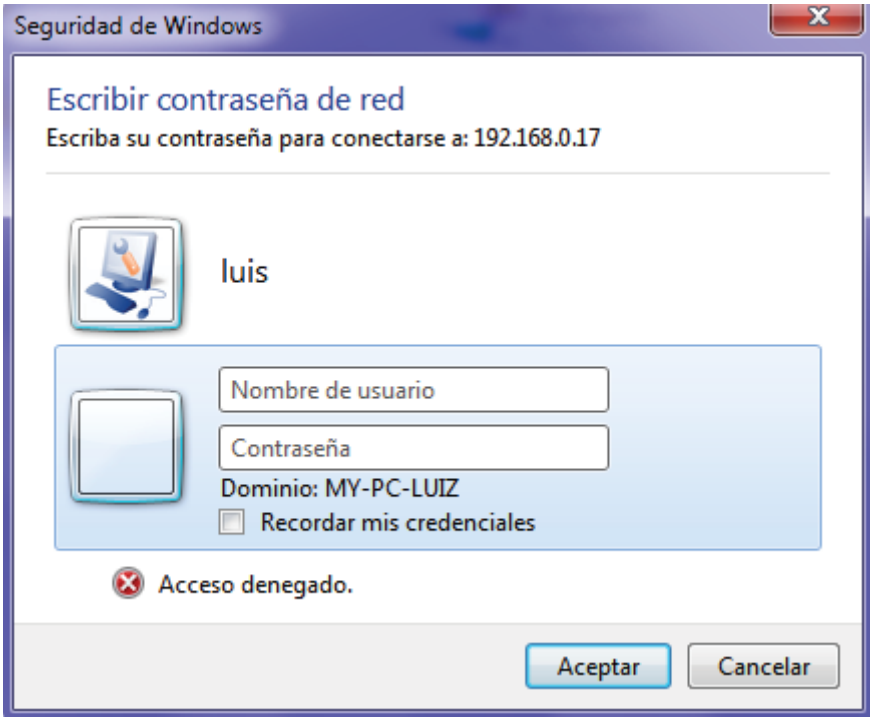


Figura 91. Autenticación para ingresar a una carpeta a la cual no se tiene permiso.

Problemas y dificultades

Durante la administración y gestión de la red, se encontró un problema con respecto a las políticas de seguridad. Las políticas de seguridad impuestas en Fortigate funcionaron solo 6 días y esto era porque el protocolo DHCP activado en Fortigate solo asignaba la misma dirección IP a un mismo equipo solo por determinado tempo, es decir tenían un tiempo de expiración, cada vez que pasaba el tiempo de expiración se volvían a reasignar las direcciones IP's a todos los equipos y estas direcciones no eran las mismas asignadas anteriormente por Fortigate.

La solución para esta problemática fue asociar y reservar las direcciones para equipos específicos. Es decir cada IP se asocio a un equipo respecto a su dirección física también conocida como dirección MAC.

Para resolver el problema se entro a la interfaz de Fortigate, entrando a System > Dashboard > Status y se selecciona la opción Detach como se muestra en la Figura 92 y nos dará acceso a la consola (Figura 93).

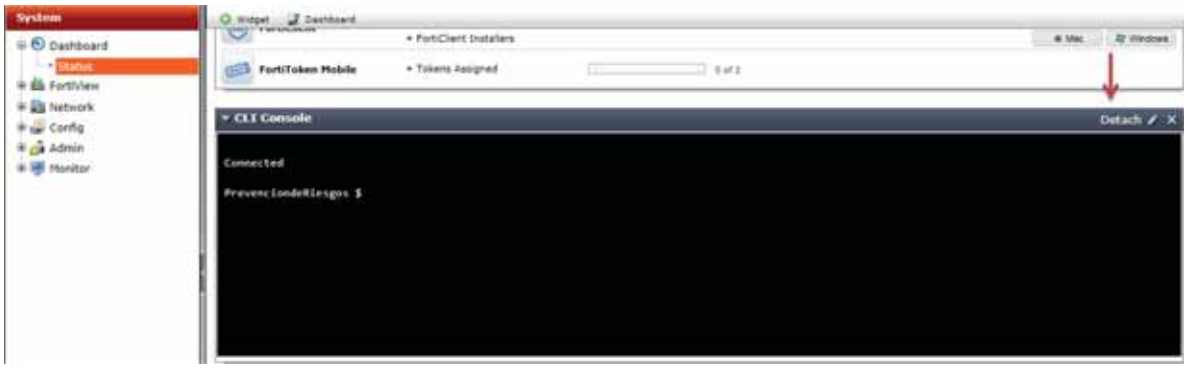


Figura 92. Ruta para entrar a consola de Fortigate.

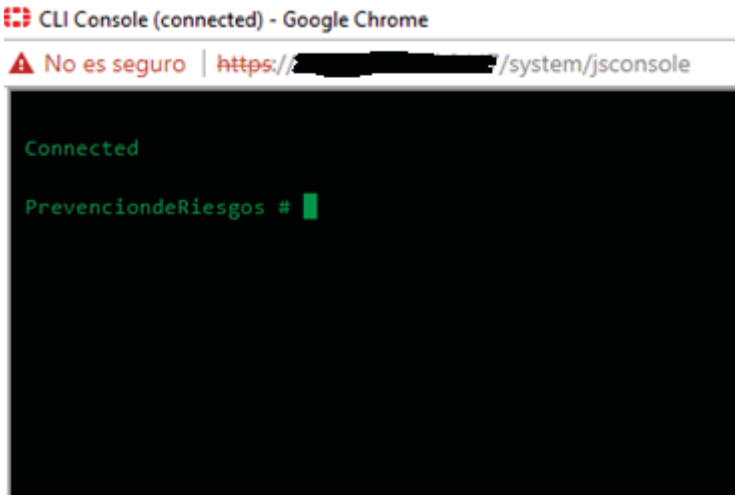


Figura 93. Acceso a la consola de Fortigate.

Se coloca el comando “config system dhcp server” donde se podrá configurar o revisar la tabla de configuración de IP’s como se muestra en la Figura 94.

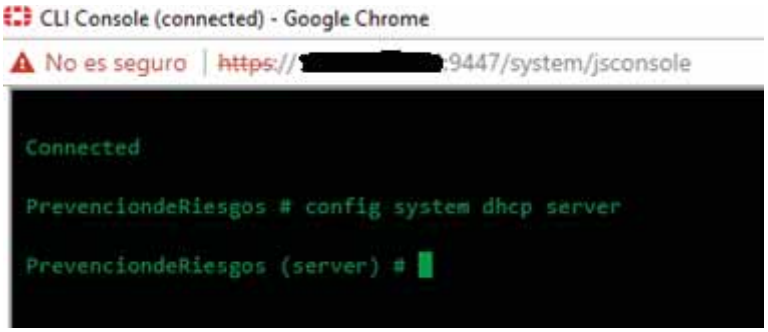


Figura 94. Comandos de Fortigate.

Despues se coloca el comando “Show” donde mostrará una tabla en la cual se observa si ya hay direcciones IP recervadas y a que equipo corresponden estas IP’s tal como se muestra en la Figura 95.

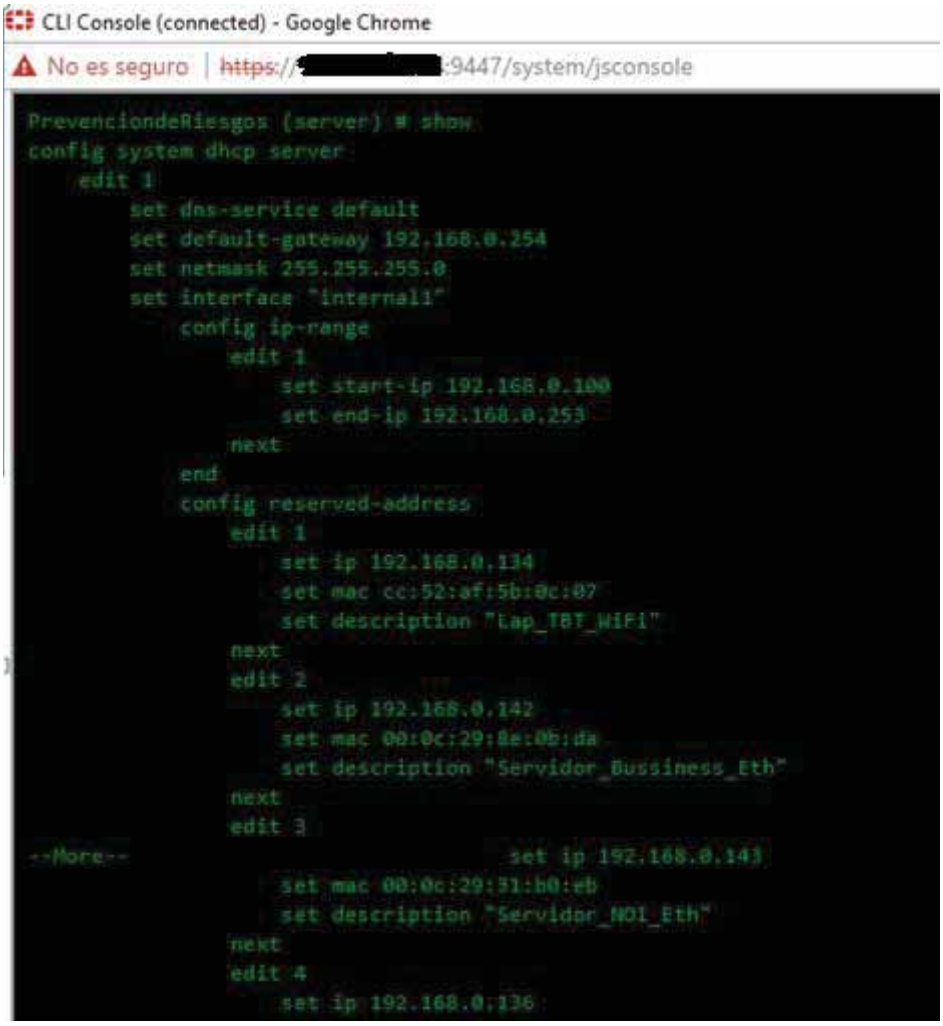


Figura 95. Tabla de configuración DHCP.

Se coloca el comando “edit 1” para configurar la tabla 1 de direcciones IP’s y enseguida se coloca el comando “config reserved- address” para editar o asociar alguna IP con una dirección MAC, tal como se muestra en la Figura 96.

Figura 96. Comandos de Fortigate.

Ahora se coloca el comando “edit 1” para empezar a llenar la tabla de direcciones IP’s asociadas a una dirección MAC de algún equipo de la empresa, tal como se muestra en la Figura 97.

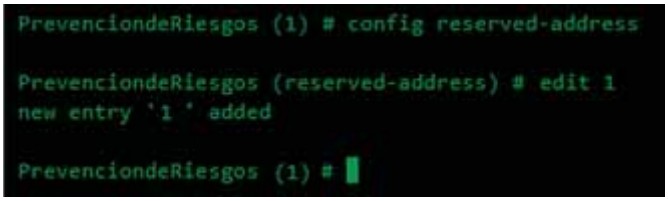


Figura 97. Comandos de Fortigate.

Para finalizar con el proceso se coloca el comando “set ip” y enseguida la dirección IP que vas a asociar a un equipo, después se coloca el “comando set mac” y enseguida la dirección MAC del equipo con que se asociará la dirección IP, para finalizar se escribe el comando “set description” y enseguida un nombre o descripción con el que se identifique a que empleado corresponde el equipo tal como se muestra en la Figura 98.

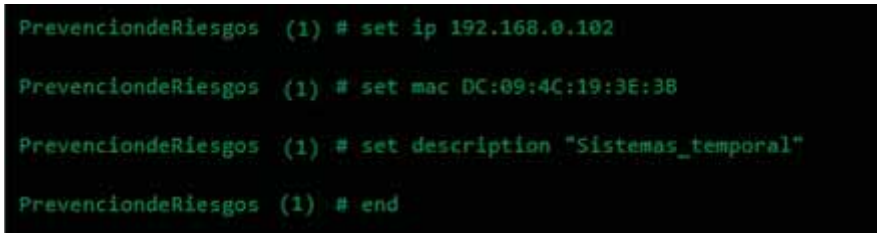


Figura 98. Comandos de Fortigate.

Con este procedimiento se garantiza que las direcciones IP’s se queden reservadas permanentemente para equipos específicos y se puedan aplicar con eficiencia las políticas de seguridad.

Conclusiones

Dentro de una red corporativa es de suma importancia la protección de la información ya que cualquier mal uso de esta puede generar diversas consecuencias para la empresa, es por eso que se puso en marcha el proyecto descrito en este reporte, cumpliendo los objetivos planteados con anterioridad.

La función que se desempeño dentro de lo que fue la estancia profesional, fue la de resolver una serie de problemáticas y requerimientos dentro una empresa, pudiendo poner a prueba nuestras habilidades, también poder relacionarse en un ambiente distinto al académico, abriendo un par de aguas en lo qué significa ser un estudiante en comparación a un trabajador.

Haber sido participe de este proyecto fue una ventaja significativa para por aplicar los conocimientos y las bases adquiridas durante toda la carrera cursada, además de conocer instancias y procedimientos que no conocía, tuve la oportunidad de hacer investigación y la práctica.

Es importante seguir administrando todos los elementos que se integraron a la red corporativa, ya que la tecnología está en constante cambio y se pueden realizar algunas mejoras en el sistema de seguridad integrado, además es de suma importancia mantenerla monitoreada para encontrar posibles vulnerabilidades y poder prevenir robo o perdida de información.

Referencias Bibliográficas

[1] P. servicios, "¿Qué es un firewall?", Cisco, 2017. [Online]. Available: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html. [Accessed: 11- Nov- 2017].

[2] ".:: Seguridad Informática ::.", Redyseguridad.fi-p.unam.mx, 2017. [Online]. Available: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php. [Accessed: 11- Nov- 2017].

[3] D. Avila Castillo, “Análisis y gestión de recursos para brindar seguridad en una red empresarial”, proyecto terminal, división de ciencias básicas e ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2015.

[4] S. Solis Torres, "Monitoreo de recursos informáticos para una mejor administración y seguridad de los datos en una red corporativa", proyecto terminal, división de ciencias básicas e ingenieria, Universidad Autónoma Metropolitana Azcapotzalco, México, 2016.

[5] G. Donaciano Escobar, “Administración y seguridad de una red corporativa mediante un firewall fortigate 90d”, proyecto terminal, división de ciencias básicas e ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2016.

[6] L. Alvares Basaldúa “Seguridad informática (Auditoria en sistemas)”, tesis, Universidad Iberoamericana, México, 2007.

[7] R. Bustamante Sánchez, “Seguridad en redes”, tesis, instituto de ciencias básicas e ingeniería, Universidad Autónoma del Estado de Hidalgo, México.

[8] K. Martínez Molina and J. Pacheco Meneses, "Firewall – Linux: Una solución de seguridad informática para PyMES (Pequeñas y medianas empresas)", revista de la facultad de ingeniería físicomecánicas, vol. 8, no. 2, pp. 155-165, 2009.

[9] "Citar un sitio web - Cite This For Me", *ENTER.CO*, 2018. [Online]. Available: http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/. [Accessed: 03- Jan- 2018].

[10] "¿Qué es Red privada virtual (VPN)? - Definición en WhatIs.com", SearchDataCenter en Español, 2018. [Online]. Available: http://searchdatacenter.techtarget.com/es/definicion/Red-privada-virtual-VPN. [Accessed: 23- Mar- 2018].