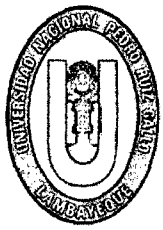


UNIVERSIDAD NACIONAL "PEDRO RUÍZ GALLO"

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

DISEÑO DE UNA DE RED PRIVADA VIRTUAL PARA INTERCONECTAR LAS SUCURSALES DE LA EMPRESA TERRACARGO SAC

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

ELABORADO POR:

Bach. DÍAZ LLATANCE MANUEL AUNER

Bach. VIEYRA DIOSES GINO LUIS ALBERTO

ASESOR:

Ing. Chiclayo Padilla Hugo

Lambayeque – Perú

2015

Universidad Nacional Pedro Ruíz Gallo

Facultad de Ciencias Físicas y Matemáticas

Escuela Profesional de Ingeniería Electrónica

Tesis presentada para obtener el grado de
Ingeniero Electrónico

DISEÑO DE UNA RED PRIVADA VIRTUAL PARA INTERCONECTAR LAS SUCURSALES DE LA EMPRESA TERRACARGO SAC

Por:
Bach. DÍAZ LLATANCE MANUEL AUNER.
Bach. VIEYRA DIOSES GINO LUIS ALBERTO.

Lambayeque – Perú

2015

Tesis presentada por:

Bach. Díaz Llatance Manuel Auner.

Bach. Vieyra Dioses Gino Luis Alberto.

Como requisito para obtener el Título de Ingeniero Electrónico
Aceptada por la Escuela Profesional de Ingeniería Electrónica.

Ing. Manuel Javier Ramírez Castro.
Presidente

Ing. Julio Ernesto Quispe Rojas
Secretario

Ing. Martín Nombera Lossio
Vocal

Bach. Manuel Auner Díaz Llatance
Autor

Bach. Gino Luis Alberto Vieyra Dioses
Autor

Ing. Hugo Javier Chiclayo Padilla
Asesor

Septiembre del 2015

DEDICATORIA

A las personas, más importantes en nuestras vidas, maestros, hermanos y amigos que estuvieron listas para brindarnos todo su apoyo, ahora nos toca contribuir a todos ellos con este logro que es fruto de todos en conjunto.

A nuestras familias, en especial a nuestros padres.

AGRADECIMIENTO

Gracias a Dios y a nuestros Padres. A Dios porque ha estado con nosotros en los momentos más difíciles de nuestra carrera. A nuestros Padres por cuidarnos y brindarnos fortaleza para continuar con nuestras metas propuestas.

A todos nuestros amigos de la vida, con quienes hemos compartido tantas alegrías y penas, y siempre estuvieron ahí para brindarnos sus consejos y apoyo.

A nuestros maestros que nos guiaron y supieron compartirnos todos sus conocimientos con el fin de que podamos lograr ser grandes profesionales y ser exitosos en la vida.

CONTENIDO

RESUMEN

Ésta tesis está centrada en el mejoramiento de la interconexión entre las sucursales de la empresa Terracargo SAC, la cual cuenta con sucursales en distintas ciudades del Perú. Este mejoramiento se hará a través de la implementación de una VPN, permitiendo la intercomunicación en tiempo real entre las sucursales, de manera eficiente y segura. La investigación fue realizada en 3 etapas.

Como primera etapa se realiza un diagnóstico de la actualidad de la empresa, obteniendo datos importantes como la arquitectura actual en cada una de las sucursales, la disponibilidad de hardware, sus usuarios y la forma de interconexión con la que trabajan, toda esta información y algunos requerimientos importantes que solicitamos nos permiten seleccionar y diseñar el modelo de VPN adecuado.

En la segunda etapa se diseña un modelo de red VPN adecuado a los requerimientos de la empresa, esto refiere a la elección del tipo de VPN que debemos utilizar, los equipos adecuados, la arquitectura y protocolos que se deben emplear, teniendo en cuenta todos los datos obtenidos anteriormente y poder brindar la mejor solución sin generar un gasto económico excesivo. También se propone soluciones a posibles problemas como cortes del servicio de internet y servicio eléctrico para evitar caídas en el servidor VPN ubicado en la sede central.

Por último se comprueba la funcionalidad de la VPN obteniendo una sentencia del gerente de la empresa, donde nos acredita sobre el correcto desempeño de la red VPN y todas las ventajas que les brinda. También generamos un usuario de prueba para poder realizar la conexión desde cualquier punto a nuestro servidor VPN.

ABSTRACT

This thesis is focused on improving the interconnection between branches Terracargo SAC company, which has branches in different cities of Peru. This improvement is done through the implementation of a VPN, allowing real-time intercommunication between the branches, efficiently and safely. The research was conducted in 3 stages.

As a first step an analysis of the present enterprise is done, obtaining important data as the current architecture in each of the branches, availability of hardware, its users and the way they work interconnection, all of this information and some important requirements we request allows us to select and design the appropriate VPN model.

In the second stage a model appropriate to the requirements of the company VPN network is designed, this refers to the choice of the type of VPN you must use the appropriate equipment, architecture and protocols to be used, taking into account all data above and to provide the best solution without generating excessive economic cost. Possible solutions to problems like Internet outages and electricity is also proposed to prevent falls in the VPN server in headquarters.

Finally, VPN functionality is checked by obtaining a judgment of the manager of the company, where we credited on the correct performance of the VPN network and all the benefits afforded them. We also generate a test user to connect from anywhere to our VPN server.

INTRODUCCION

Una Red se extiende sobre un área geográfica amplia, entre departamentos, a veces un país o un continente; además, contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones). En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto, dichas redes cumplen con atributos tales como seguridad, confiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que escuchamos hablar tanto de los famosos firewalls y las VPN.

Una Red Privada Virtual (VPN) conecta los componentes de una red sobre otra red. VPN logra este objetivo mediante la conexión de los usuarios de distintas redes a través de un túnel que se construye sobre Internet o sobre cualquier red pública, permitiendo a los usuarios trabajar en sus casas o empresas conectados de una forma segura con el servidor corporativo, usando la infraestructura provista por la red pública (Internet).

Desde el punto de vista del usuario, la VPN es una conexión entre el usuario y el servidor corporativo. La naturaleza de la interconexión que está en el medio de los dos es transparente para el usuario ya que los datos le aparecen como si fueran enviados a través de su red LAN, como si estuviera en la empresa. Esta tecnología también habilita a las empresas a tener conectadas oficinas centrales con sus sucursales sobre cualquier red pública, mientras se mantienen conexiones seguras y confiables.

Es así como hacemos uso de la tecnología VPN para poder resolver el problema de interconexión que tenemos en nuestra empresa con sus sucursales ubicados en un área geográfica distinta de su local central.

ASPECTO INFORMATIVO

1. ASPECTO INFORMATIVO

1.1.TÍTULO.

"Diseño de un modelo de red privada virtual para interconectar las sucursales de la empresa Terracargo SAC"

1.2.AUTORES.

Diaz Llatance, Manuel Auner
Código: 080857-A
E-mail: manudi11d3@gmail.com

Vieyra Dioses, Gino Luis Albeto
Código: 082280-C
E-mail: ginovieyra.d@gmail.com

1.3.ASESOR.

Ing. Hugo Chiclayo Padilla – Ing. Electrónico de la Universidad Nacional Pedro Ruiz Gallo.

1.4.ÁREA DE INVESTIGACIÓN.

Ingeniería electrónica y de telecomunicaciones.

1.5.LUGAR DE EJECUCIÓN.

El proyecto se llevara a cabo en los ambientes de la empresa Terracargo Sac.

1.6.PLANTEAMIENTO DEL PROBLEMA CIENTÍFICO.

La necesidad de conectar las sucursales y filiales de una compañía no se debe solo una cuestión técnica. También es una cuestión de ahorro en costos. Con el fin de mantenerse al día en un entorno global, los operadores de la cadena deben mantener a un nivel bajo su coste y garantizar que los procesos sean rápidos y seguros. Esto significa que las sucursales y filiales deben ser gestionadas y administradas de forma centralizada. Una parte elemental es la infraestructura de IT que conecta a todos los usuarios dentro de la red de forma segura, económica y sin gran esfuerzo.

Si bien los requisitos básicos relacionados con la infraestructura IT solo representan una conexión de datos fiables y seguros a la sede, con el fin de acceder a correos electrónicos y datos gestionados de forma centralizada, las demandas actuales de conexión en sucursales son mucho más extensas. Los nuevos conceptos de sucursal y sus relaciones con la sede conllevan a una complejidad creciente, como sucede con las soluciones de "tienda en tienda" o aplicaciones logísticas como el sistema de venta inversa, que incluye acceso a dispositivos de proveedores de servicio externo. En consecuencia, aumenta la cantidad de requisitos de perfil que deben tenerse en cuenta al diseñar una red y elegir componentes.

Actualmente la empresa de transportes Terracargo SAC. Cuenta con un sistema de interconexión de alto costo y no les brinda la seguridad adecuada.

El problema principal que tiene la empresa es la segregación total de sus redes informáticas y de telecomunicaciones, pues todas sus sedes disponen de routers con distintos ISP y como problema añadido, no se dispone de medidas de seguridad informática. Para que Terracargo SAC pueda brindar un servicio de calidad con los estándares que exige hoy en día el mercado, es necesario que todas sus sedes estén interconectadas.

1.7.FORMULACIÓN DEL PROBLEMA CIENTÍFICO.

¿Cómo mejorar la interconexión entre las sucursales de la empresa Terracargo SAC Para tener un soporte de gestión de la información rápida, segura y confiable?

1.8.OBJETIVOS.

1.8.1. Objetivo General

- Diseñar un modelo de red VPN para mejorar la interconexión entre las sucursales de la empresa Terracargo SAC. para soportar una gestión de la información segura, rápida y confiable.

1.8.2. Objetivo Específico

- Diagnosticar la realidad de la interconexión entre las sucursales de la empresa Terracargo SAC.
- Plantear un modelo de red VPN, para interconectar las sucursales de la empresa Terracargo SAC.
- Seleccionar dispositivos para el diseño de la VPN.
- Comprobar la funcionabilidad y validar el modelo de red VPN.

1.9.JUSTIFICACIÓN E IMPORTANCIA.

Actualmente Terracargo SAC. Cuenta con una conexión por fibra óptica entre sus 02 sucursales en Lima, este enlace es de muy alta calidad pero demanda un muy alto costo a la empresa. Además las sucursales de las ciudades de Piura, Chiclayo y Tumbes no se encuentran interconectadas, esto dificulta la operatividad del sistema de la empresa.

Una Red Privada Virtual permitirá interconectar todas las sucursales, sin necesidad de tener un enlace físico, esto reemplazará al enlace de

fibra óptica y permitirá la interconexión de las demás sucursales en una misma red de forma óptima y segura.

1.10. HIPÓTESIS.

Si se diseña una red VPN para interconectar las oficinas de la empresa Terracargo SAC se mejorara la interconexión para soportar una gestión de la información segura, rápida y confiable.

MARCO TEÓRICO

2. MARCO TEÓRICO.

2.1.ANTECEDENTES

A. TÍTULO: "DISEÑO E IMPLEMENTACION DE UNA VPN EN UNA EMPRESA COMERCIALIZADORA UTILIZANDO IPSEC."

- **AUTOR:** EDISON RAFAEL TRUJILLO MACHADO.

- **OBJETIVO:** Se buscará la mejor alternativa y se elaborará una propuesta técnica que garantice la escalabilidad y calidad de servicio que las grandes empresas requieren para sus VPN.

- **RESUMEN:** El presente trabajo comprende el diseño e implementación de una VPN en una empresa comercializadora utilizando IPSec.

  Ha sido estructurado en 5 capítulos, a continuación se muestra una visión de los contenidos de cada sección:

  Capítulo 1. Presenta una reseña de la evolución del Internet, los diferentes tipos de conexión, los proveedores de este servicio en el Ecuador, y las tecnologías de conexión WAN que se han utilizado hasta la actualidad.

  Capítulo 2. Comprende todo lo relacionado con las Redes Privadas Virtuales como son los tipos, arquitectura, tecnologías de tunneling. También se analiza las funcionalidades y aplicaciones del protocolo IPSec dentro de las VPN.

  Capítulo 3. Se hace un estudio de la situación organizacional y tecnológica de la empresa comercializadora tomada como caso de estudio para este trabajo, y sus posibles implementaciones VPN.

  Capítulo 4. Se documenta la implementación de un prototipo VPN dentro de la empresa comercializadora, se hace un análisis de costos, ventajas, desventajas con respecto a las líneas dedicadas.

  Capítulo 5. Consta de las conclusiones y recomendaciones.

➢ **CONCLUSIONES**

- ✓ Luego de finalizar el proyecto, se puede concluir que se cumplieron con los objetivos propuestos para el mismo. Se llegó a diseñar algunas alternativas de implementación VPN en la empresa comercializadora y se construyó un prototipo demostrativo.
- ✓ La VPN de Acceso Remoto implementada como prototipo, tiene las funcionalidades de las Redes Privadas Virtuales, y se comprobó que es ideal para las personas que viajan constantemente o que se conectan desde su hogar hacia la oficina central, esta facilidad hace que aumente la productividad de los empleados ya que pueden acceder a la red desde cualquier parte.
- ✓ Se analizó que la tecnología VPN es una alternativa totalmente viable, la empresa comercializadora está en la posibilidad de integrar sus sucursales, usuarios móviles y socios estratégicos a un costo efectivo, comparado con las tradicionales líneas dedicadas que arrienda hasta ahora, ya que utilizaría el Internet que está creciendo notoriamente en nuestro país.
- ✓ En este proyecto, el protocolo IPSec es el encargado de brindar la seguridad necesaria a la información de la empresa dentro de la VPN, al ser IPSec un estándar difundido ampliamente, permite la interoperabilidad de los sistemas de diversos fabricantes.

B. TÍTULO: "ESTUDIO DEL DESEMPEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN MPLS-VPN SOBRE MÚLTIPLES SISTEMAS AUTÓNOMOS."

➢ **AUTOR:** RICARDO ARMANDO MENENDEZ AVILA.

➢ **OBJETIVO:** El objetivo de la presente tesis es realizar un estudio de cuatro tipos de implementación de la solución Multi-As VPN. Se dará a conocer las ventajas y desventajas de cada solución mediante pruebas de laboratorio.

- **RESUMEN:** La presente tesis consiste en proporcionar una propuesta técnica para la implementación de una red MPLS-VPN sobre Múltiples Sistemas Autónomos (Multi Autonomous System VPN), a través de un estudio del desempeño de cuatro diferentes modelos de implementación para brindar dicha solución. Durante el desarrollo de la tesis se presenta el marco teórico que permite conocer y entender tanto las redes VPN como las arquitecturas involucradas en su funcionamiento, principalmente la tecnología MPLS. Posteriormente se explica el porqué es necesario contemplar una solución soportada en más de un sistema autónomo. A continuación se presentan los distintos modelos de red para la implementación de las VPN Multi-AS y se realiza un estudio del desempeño de cada uno de ellos. Posteriormente se hace un análisis de los resultados obtenidos durante el estudio de cada opción con el fin de conocer las ventajas, desventajas, problemas y las posibles soluciones que ofrecen. Finalmente se elabora una propuesta técnica para la implementación de la red, utilizando el Modelo de Implementación "Multi Protocol eBGP Multisalto entre Route Reflectors", con los procedimientos detallados necesarios, los aspectos económicos y resultados esperados al final del proceso.

- **DEFINICIÓN DEL PROBLEMA Y JUSTIFICACIÓN:** Los proveedores de servicios de telecomunicaciones buscan constantemente ampliar los alcances de sus redes MPLS. La arquitectura Multi Protocol Label Switching (MPLS) proporciona alta escalabilidad y rapidez en el reenvío de paquetes, siendo su aplicación más empleada las VPNs. Sin embargo, esta arquitectura implica que los clientes de servicios VPN estén conectados a un solo proveedor. Por otro lado, las grandes empresas cuentan generalmente con sedes en diferentes ciudades o regiones, y hacen uso de los servicios VPN para poder interconectar sus sedes. A medida que las empresas crecen, los requerimientos de sus VPNs aumentan. Se hace necesario abarcar diferentes áreas geográficas, muchas veces cruzando más de un país. Inclusive, algunas VPNs necesitan extenderse a través de múltiples proveedores

de servicios VPN. Independientemente de la complejidad que implique este tipo de necesidad, las conexiones que se hagan deben ser totalmente transparentes de cara al cliente. Por ello, es necesario contar con una solución que permita brindar de forma eficiente servicios 14 VPN altamente escalables, que abarque grandes regiones, que sea capaz de integrar a más de un proveedor y sobre todo, que sea segura. La presente tesis desarrollará un estudio de cuatro tipos de implementación de la solución Multi-AS VPN. Se buscará brindar la mejor alternativa y que garantice la escalabilidad y calidad de servicio que las grandes empresas requieren para sus VPNs.

C. **TÍTULO:** "IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL (VPN) BAJO SOFTWARE LIBRE PARA OPTIMIZAR EL MANEJO DE INFORMACIÓN ENTRE LOS LOCALES DE LA CORPORACIÓN EDUCATIVA ADEU, DE LA CIUDAD DE CHICLAYO."

- **AUTOR:** VIRGILIO AMENERO VAZQUEZ.

- **OBJETIVO:** Se buscará la mejor alternativa y se elaborará una propuesta técnica que garantice la escalabilidad y calidad de servicio que las grandes empresas requieren para sus VPN.

- **RESUMEN:** Ésta investigación estuvo centrada en la optimización del acceso a la información entre los locales de la Corporación Educativa ADEU, ubicada en la ciudad de Chiclayo; a través de la implementación de una VPN, la cual fue realizada en software libre, y como tal no incurre en gastos económicos excesivos y constituye un canal de comunicación seguro. La investigación fue realizada en 3 etapas. Como parte de la primera etapa se realizó una entrevista al Jefe del Área de Sistemas, el cual manifestó que actualmente la información a la que accede el personal administrativo de los locales de dicha Corporación no cuenta con un medio de comunicación directo para compartir sus datos, por el contrario, están divididos, por lo cual el

manejo y el acceso a la información es tedioso, ya que se requiere de otros medios tales como, dispositivos magnéticos y cuentas de correo públicas, que en la mayoría de los casos son canales de transferencia de información no seguros. En la segunda etapa, teniendo en cuenta las necesidades planteadas por el Jefe del Área de Sistemas de la Corporación Educativa ADEU, se propuso un bosquejo de la VPN, la cual posteriormente fue modificada y validada por el Jefe del Área de Sistemas. Luego el modelo validado fue implementado en la herramienta de software denominada OpenVPN, realizándose las configuraciones apropiadas a los servidores y equipos necesarios para la realización de la implementación respectiva. Además se realizaron un conjunto de pruebas, a fin de que se asegure la conexión de la red y se descarten posibles vulnerabilidades de la red. Para el desarrollo de la VPN se hizo empleo de la "Metodología para la implementación de redes seguras", desarrollada por la empresa argentina CYBSEC. Finalmente, la tercera etapa estuvo enfocada en la comparación de los resultados obtenidos en las etapas 1 y 2; y la demostración de las mejoras a la problemática de la corporación. Mediante la implementación de la VPN se logró proporcionar un canal que permite transferir los datos de manera óptima y eficaz; permitiendo así, la confidencialidad y seguridad en su transmisión, sin tener que incurrir en gastos excesivos en la contratación de canales privados.

- **RESULTADO:** Analizando estas pruebas se puede demostrar que el paso de la información por la VPN se da a través de un canal seguro, el cual evita los problemas de extracción de la información o de ataques externos. Como aporte a esta investigación se optó por demostrar cómo es posible que nuestra red se vuelva más segura ante ataques externos. Tener vigilados los puertos del ordenador es muy importante tanto para evitar intrusiones desde Internet como para tener controlado en todo momento el ordenador. Luego de analizar el paso de la información a través de la VPN se deben asegurar los diferentes protocolos que pasan a través de la red, ya que podrían ser un medio de vulnerabilidad que pueden ser aprovechados y violentados por

personas con motivos maliciosos. Para este análisis sirve la herramienta ZENMAP 5.51, la cual es una aplicación gráfica para manejar Nmap: un escáner de puertos que nos puede dar mucha información acerca de una máquina.

2.2.REDES DE COMPUTADORAS

2.2.1. DEFINICIÓN DE RED DE COMPUTADORAS

Una red de computadoras es un grupo de computadoras interconectadas entre sí las cuales comparten información y recursos. La interconexión se puede realizar de diferentes maneras, ya sea cable de cobre, fibra óptica, rayos infrarrojos o microondas. Los recursos y la información que se pueden compartir pueden ser los siguientes:

- Archivos
- Aplicaciones
- Correo electrónico
- Impresoras

Las redes de computadoras ofrecen muchas ventajas. Sin ellas todo el envío de la información tendría que hacerse de forma manual o por medio de unidades de almacenamiento.
Esto haría el proceso algo muy lento. Con las redes no sólo se puede intercambiar información a nivel local, sino también a grandes distancias incluso mundiales y de forma instantánea.

2.2.2. CLASIFICACIÓN DE LAS REDES DE COMPUTADORAS

El mundo de las redes de computadoras es muy complejo, por lo que es necesario clasificarlas para facilitar su estudio, ya que existen muchos tipos de redes. Las redes pueden ser clasificadas en cuanto a cobertura, topología y propiedad.

2.2.2.1. Cobertura

La clasificación de las redes en cuanto a cobertura se refiere a la extensión que tiene una red dentro de un área geográfica. Utilizando este criterio, las redes de computadoras se pueden clasificar de acuerdo a la tabla 1.1

Distancia entre procesadores	Procesadores ubicados en el mismo	Clasificación
1m	Metro cuadrado	Red de Área Personal (PAN)
10 m	Cuarto	Red de Área Local (LAN)
100 m	Edificio	
1 km	Campus	Red de Área Campus (CAN)
10 km	Ciudad	Red de Área Metropolitana (MAN)
100 km	País	Red de Área Amplia (WAN)
1000 km	Continente	
10000 km	Planeta	Internet

Tabla 1.1 Clasificación de las redes en cuanto a cobertura

Las principales son:

a) **Red de Área Local (LAN).** Es aquella red donde todas las computadoras conectadas en red están dentro de una habitación, un edificio e incluso varios edificios dentro de una localidad pequeña. Las LAN realizan lo siguiente:
   - Operan dentro de una zona geográfica limitada.
   - Permiten a los usuarios acceder a medios de gran ancho de banda.
   - Proporcionan conectividad de tiempo completo a los servicios locales.
   - Conectan físicamente dispositivos adyacentes.

   Las principales tecnologías LAN son las siguientes:
   - Ethernet
   - Token Ring
   - FDDI

Siendo Ethernet la más popular y más difundida de todas ellas.

Una LAN puede intercomunicarse por medio de un cableado que transmita señales punto a punto; o bien, por medio de una zona de influencia de un punto de acceso (access point) inalámbrico. La velocidad que se puede alcanzar en este tipo de red abarca desde los 10 Mbps hasta los 10 Gbps y se están desarrollando normas para 40 Gbps, 100 Gbps y 160 Gbps.

b) **Red de Área Amplia (WAN).** Es aquella red que está formada por la interconexión de varias LAN. Una WAN abarca una gran área geográfica de varios kilómetros.

Las WAN son útiles cuando los usuarios de una red necesitan acceder a los recursos de otra red. Esto ocurre por ejemplo cuando las oficinas principales de una compañía necesitan utilizar recursos de la red que se encuentra en alguna de sus fábricas ubicada a varios kilómetros de distancia. Las WAN realizan lo siguiente:

- ✓Operan sobre grandes áreas geográficamente separadas
- ✓Permiten que los usuarios mantengan comunicación en tiempo real con otros
- ✓Proporcionan acceso a los recursos remotos de una LAN
- ✓Ofrecen servicios de correo electrónico, web, transferencia de archivos y comercio electrónico

Las principales tecnologías WAN son:

- Módems
- Red Digital de Servicios Integrados (RDSI)
- Línea de Abonado Digital (DSL, Digital Suscriber Line)
- Frame Relay
- Modo de Transferencia Asíncrono (ATM, Asynchronous Transfer Mode)
- Portadoras T1, E1.
- Red Óptica Síncrona (SONET, Synchronous Optical Network)

En la figura 1.2 se pueden observar distintas redes LAN conectadas a una red WAN que puede utilizar diferentes tecnologías.

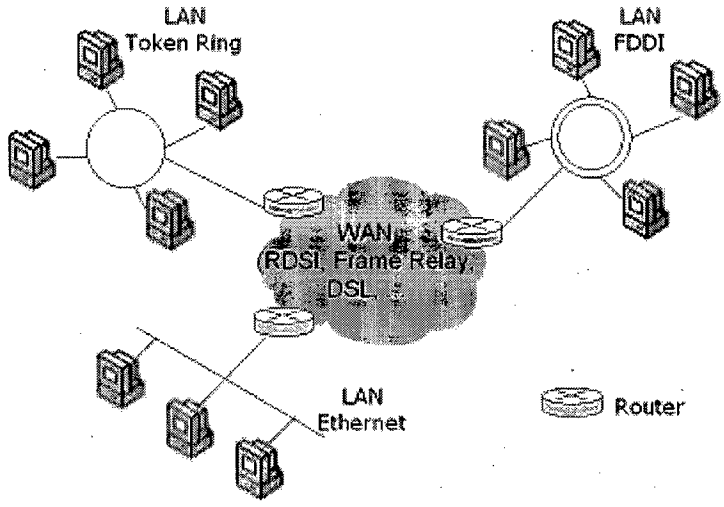


Figura 1.2 LAN y WAN

2.2.2.2. Topología

En cuanto a la topología, como se muestra en la figura 1.3, existen básicamente cuatro tipos de redes de las cuales se desprenden varias combinaciones. Estas topologías son:

- Red tipo bus
- Red tipo estrella
- Red tipo anillo
- Red tipo malla
- Red tipo híbrida

a) **Red tipo bus.** En esta topología se utiliza un cable o serie de cables como eje central al cual se conectan todas las computadoras. En este conductor se efectúan todas las comunicaciones entre las computadoras. Esta red conviene usarse si no son muchas las computadoras que se van a conectar.

b) **Red tipo estrella.** Se caracteriza por tener un núcleo del cual se desprenden líneas guiadas a varios terminales. Fueron las primeras en utilizarse en el mundo de la computación. Esta topología es útil cuando se tiene una computadora central muy potente rodeada de máquinas de menor potencia. Esta topología es la más común porque es la que más utilizan las redes Ethernet.

c) **Red tipo anillo.** Aquí también se utiliza un bus como eje central para conectar todos los equipos, sin embargo, dicho bus forma un anillo. Esta topología es utilizada en redes Token Ring y FDDI además de que es favorecida por los principales proveedores de acceso a Internet.

d) **Red tipo malla.** En esta topología, todos los dispositivos o algunos de ellos son conectados con todos los demás con el fin de conseguir redundancia y tolerancia a fallos. Si un enlace falla, la información puede fluir por otro enlace. Las redes de malla suelen implementarse solamente en redes WAN.

e) **Red tipo híbrida.** La topología híbrida es una red que utiliza combinaciones de las topologías anteriores.

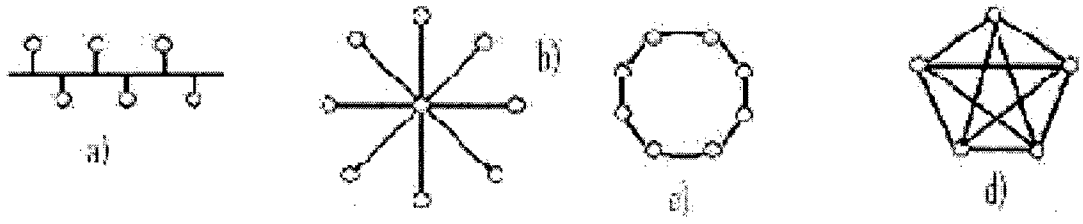


Figura 1.3 Topología de redes: a) Bus b) Estrella c) Anillo d) Malla

2.2.2.3. Propiedad

La clasificación de las redes en cuanto a propiedad se refiere a la forma de administración de la red. Así pues, como se muestra en la figura 1.4, las redes de computadoras se pueden clasificar de la siguiente forma:

- Redes privadas
- Redes públicas

a) **Red privada.** Es aquella red exclusiva de una sola compañía u organización en particular. La información no se comparte con otras compañías u organizaciones.
En una red privada la información estará protegida, se podrá controlar el uso que se le da a la red y se podrá predecir el ancho de banda disponible.

b) **Red pública.** Es una red a través de la cual circula información de muchas compañías y organizaciones. Una red pública siempre será menos segura que una red privada, pero resultan ser más económicas y no se requiere que un administrador de red local de mantenimiento a una de estas redes. Como ejemplo de red pública tenemos a Internet.

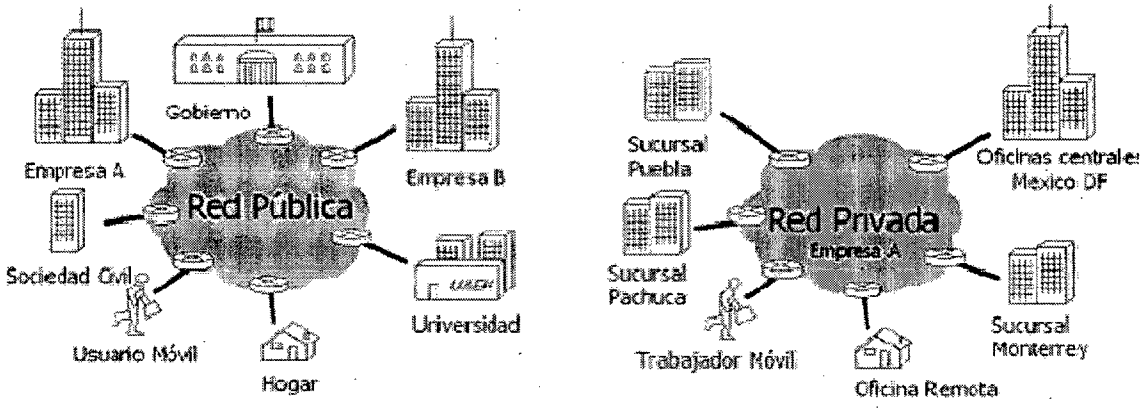


Figura 1.4 Red pública y red privada

2.2.2.4. Dispositivos de interconexión de redes

Los dispositivos de interconexión de redes conectan a los dispositivos terminales de redes para formar la red y controlar el flujo de la información. Estos son:

- Concentrador (hub)
- Conmutador (switch)
- Enrutador (router)

a) **Concentrador o hub:** Es un dispositivo que conecta varios cables de red que llegan desde computadoras cliente a la red. Existen concentradores de diferente tamaño en los cuales se puede conectar desde dos computadoras hasta más de 60 equipos. La información que llega al nodo de un hub es retransmitida a todos los demás nodos conectados a este equipo, lo que puede afectar el desempeño de una red.

b) **Conmutador o switch:** Se trata de un dispositivo que conmuta de forma dinámica sus distintos puertos para crear las conexiones. Un switch es un equipo semejante a un hub con la diferencia de que todas las conexiones de red tienen su propio dominio de colisión, esto hace que cada conexión de red sea privada, lo cual incrementa el desempeño de una red.

c) **Enrutador o Router:** Es un equipo que direcciona los paquetes de datos de una red a otra. Las dos redes se conectan al router usando sus propios cableados y tipos de conexión. Este dispositivo puede determinar cuál es la ruta más corta de un paquete hacia su destino, además de que también pueden optimizar el ancho de banda de la red y ajustarse de manera dinámica a problemas de patrones de tráfico cambiantes dentro de la red. Para que un router funcione de manera correcta, necesita ser programado, esto se puede realizar conectando una PC a una terminal del router y utilizando algún software de terminal o un programa en modo gráfico.

2.2.2.5. Dispositivos terminales de redes o de usuario final

Los dispositivos terminales de redes o de usuario final son aquellos que son conectados por los dispositivos de interconexión de redes y son los puntos finales de una red que transmiten o envían la información. Estos dispositivos son:

- Estación de trabajo (host)
- Servidor
- Tarjeta de Interfaz de Red (NIC)

a) **Estación de trabajo**. Son las computadoras que componen la red. Permiten a los usuarios crear, compartir y obtener información. A las estaciones de trabajo también se les denomina hosts y el término incluye a las impresoras en red.

b) **Servidor.** Es aquella computadora que proporciona funciones o servicios a otras computadoras. Existen diferentes tipos de servidores de acuerdo a la función que realizan como servidores de archivos, de red, de acceso remoto, de Internet, etc.

c) **Tarjeta de Interfaz de Red** (NIC, Network Interface Card). Es un dispositivo electrónico que permite a un ordenador o impresora acceder a una red y compartir recursos entre dos o más equipo.

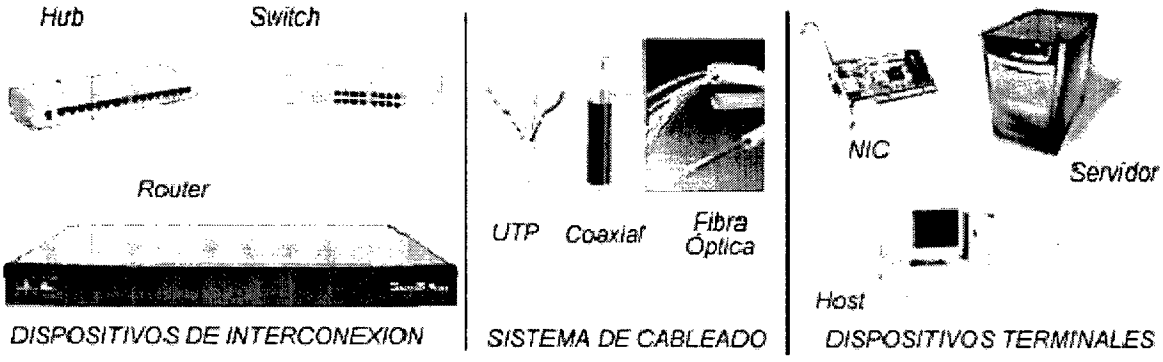


Figura 1.5 Componentes de una red de computadoras

2.3.CONEXIONES WAN Y ACCESO REMOTO

2.3.1. INTERNET, INTRANETS Y EXTRANETS

Internet es una red de redes que ha proporcionado muchas ventajas a toda clase de organizaciones. A las empresas les aporta muchos beneficios económicos el hecho de conectarse a Internet y poder realizar ahí toda clase de negocios. Las corporaciones han descubierto también que llevar la tecnología sobre la cual se basa Internet a sus propias redes privadas les trae muchos beneficios a todos sus usuarios, de ahí el surgimiento de las intranets. Finalmente, las empresas requieren estar conectadas con sus socios y clientes, por lo que pronto surgen las extranets. Internet, intranet y extranet son conceptos muy importantes en el mundo de las VPN y no puede hablarse de una VPN sin antes conocer en qué consisten dichos conceptos.

2.3.1.1. Internet

Internet conecta decenas de millones de computadoras en todo el mundo, permitiéndoles comunicarse entre sí y compartir recursos. Internet es una colección de redes organizada en una estructura multinivel las cuales usan toda una variedad de tecnologías para interconectarse. En el nivel más bajo se encuentra algunas decenas o cientos de computadoras conectadas a un router, formando una LAN. Otras computadoras se conectarán a un router a través de la red telefónica usando un módem. Una empresa o universidad podrá tener varios routers enlazados a un router principal. Estos routers se encuentran conectados mediante líneas alquiladas a un router de un Proveedor de Servicios de Internet (ISP, Internet Service Provider). A su vez, el proveedor conecta sus routers a una WAN de alta velocidad llamada backbone. Un país puede tener varios backbones que conectan a todos los ISP. Finalmente, los backbones de todos los países se interconectan en una malla usando líneas internacionales.

Todo esto es lo que finalmente forma Internet.

La base de Internet es TCP/IP. El éxito de las redes basadas en IP se debe precisamente a Internet. Dos conceptos definen la tecnología de Internet: los paquetes y la forma de direccionamiento.

Paquetes. Internet transporta toda la información en unidades llamadas paquetes. Un paquete consta de dos partes: la información que contiene, la cual se llama carga útil y la información acerca de la información, llamada cabecera. La cabecera contiene información acerca de las direcciones origen y destino, longitud de los datos y tipo de éstos.

Direccionamiento. Las direcciones de la cabecera permiten el envío de la información a través de Internet. Los routers se encargan de realizar esto. Los paquetes recorren diferentes caminos para llegar a su destino y eventualmente pueden ser almacenados dentro del router.

2.3.1.2. Intranet

Una intranet es una Internet orientada a una organización en particular. Los servidores web intranet difieren de los servidores web públicos en que estos últimos no tienen acceso a la intranet de la empresa sin los permisos y las contraseñas adecuadas. Una intranet está diseñada para que accedan a ellas sólo los usuarios con los debidos permisos de acceso a una red interna de una empresa. Una intranet reside dentro de un firewall y éste impide el acceso a los usuarios no autorizados.

2.3.1.3. Extranet

Una extranet es una intranet orientada a las personas u organizaciones que son externas a su empresa, pero necesitan acceder a alguna información, así se les permite el acceso a este contenido adicional,

siempre bajo un sistema de autenticación y control de acceso.
La diferencia entre una intranet y una extranet es el método de acceso, siendo similares en cuanto a las facilidades y funciones, el tipo de recurso que utiliza y su filosofía general, de proporcionar acceso fácil, rápido y seguro a la información requerida.

El concepto extranet nace cuando una empresa quiere dar acceso a unas determinadas personas o grupos de personas a una determinada información de su intranet. Sin hacerla pública, la hace accesible a otras personas que puedan necesitarla o con quien mantienen relaciones comerciales. El ejemplo más claro es la accesibilidad que una empresa da a una parte de sus clientes o proveedores.

2.3.2. ACCESO REMOTO

Conectarse a una red desde una ubicación distante es lo que se denomina acceso remoto. El acceso remoto a una red ha sido algo de gran importancia en el mundo de las redes, ya que muchas compañías que promueven viajes de trabajo de sus empleados o el trabajo desde el hogar o desde una pequeña oficina remota. Y estos empleados necesitan conectarse a la red privada de la compañía para consultar ciertos archivos o correo electrónico. La necesidad del acceso remoto ha sido la causa principal del auge de las redes privadas virtuales, por lo que es preciso analizarlo un poco antes de verlo desde el punto de vista de las VPN.

2.4.DIRECCIÓN IP

Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del Modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48 bits para identificar de

forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se denomina también dirección IP dinámica (normalmente abreviado como IP dinámica).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados generalmente tienen una dirección IP fija (comúnmente, IP fija o IP estática). Esta no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

Las computadoras se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS, que a su vez facilita el trabajo en caso de cambio de dirección IP, ya que basta con actualizar la información en el servidor DNS y el resto de las personas no se enterarán, ya que seguirán accediendo por el nombre de dominio.

2.4.1. DIRECCIONES IPV4

Las direcciones IPv4 se expresan por un número binario de 32 bits, permitiendo un espacio de direcciones de hasta 4.294.967.296 (2^{32}) direcciones posibles. Las direcciones IP se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto está comprendido en el intervalo de 0 a 255 [el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255].

En la expresión de direcciones IPv4 en decimal se separa cada octeto por un carácter único ".". Cada uno de estos octetos puede estar comprendido entre 0 y 255.

Ejemplo de representación de dirección IPv4: 10.128.1.253

En las primeras etapas del desarrollo del Protocolo de Internet, los administradores de Internet interpretaban las direcciones IP en dos partes, los primeros 8 bits para designar la dirección de red y el resto para individualizar la computadora dentro de la red.

Este método pronto probó ser inadecuado, cuando se comenzaron a agregar nuevas redes a las ya asignadas. En 1981 el direccionamiento internet fue revisado y se introdujo la arquitectura de clases. (classful network architecture).

En esta arquitectura hay tres clases de direcciones IP que una organización puede recibir de parte de la Internet Corporation for Assigned Names and Numbers (ICANN): clase A, clase B y clase C. En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{24} - 2 (se excluyen la dirección reservada para broadcast (últimos octetos en 255) y de red (últimos octetos en 0)), es decir, 16□777□214 hosts.

En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hostspor cada red es 2^{16} - 2, o 65□534 hosts.

En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts por cada red es 2^{8} - 2, o 254 hosts.

2.4.1.1. Direcciones privadas

Existen ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se conecten mediante el protocolo NAT. Las direcciones privadas son:

Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).

Clase B: 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.

Clase C: 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits hosts). 256 redes clase C continuas, uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

2.4.1.2. Máscara de subred

La máscara permite distinguir los bits que identifican la red y los que identifican el host de una dirección IP. Dada la dirección de clase A 10.2.1.2 sabemos que pertenece a la red 10.0.0.0 y el host al que se refiere es el 2.1.2 dentro de la misma. La máscara se forma poniendo a 1 los bits que identifican la red y a 0 los bits que identifican el host. De esta forma una dirección de clase A tendrá como máscara 255.0.0.0, una de clase B 255.255.0.0 y una de clase C 255.255.255.0. Los dispositivos de red realizan un AND entre la dirección IP y la máscara para obtener la dirección de red a la que pertenece el host identificado por la dirección IP dada. Por ejemplo un router necesita saber cuál es la red a la que pertenece la dirección IP del datagrama destino para poder consultar la tabla de encaminamiento y poder enviar el datagrama por la interfaz de salida. Para esto se necesita tener cables directos. La máscara también puede ser representada de la siguiente forma 10.2.1.2/8 donde el /8 indica que los 8 bits más

significativos de máscara están destinados a redes, es decir /8 = 255.0.0.0. Análogamente (/16 = 255.255.0.0) y (/24 = 255.255.255.0).

2.4.1.3. IP dinámica

Una **dirección IP dinámica** es una IP asignada mediante un servidor DHCP (**Dynamic Host Configuration Protocol**) al usuario. La IP que se obtiene tiene una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente.
DHCP apareció como protocolo estándar en octubre de 1993. El estándar RFC 2131 especifica la última definición de DHCP (marzo de 1997). DHCP sustituye al protocolo BOOTP, que es más antiguo. Debido a la compatibilidad retroactiva de DHCP, muy pocas redes continúan usando BOOTP puro.

Las IP dinámicas son las que actualmente ofrecen la mayoría de operadores. El servidor del servicio DHCP puede ser configurado para que renueve las direcciones asignadas cada tiempo determinado.

Ventajas

- Reduce los costos de operación a los proveedores de servicios de Internet (ISP).
- Reduce la cantidad de IP asignadas (de forma fija) inactivas.
- El usuario puede reiniciar el router para que le sea asignada otra IP y así evitar las restricciones que muchas webs ponen a sus servicios gratuitos de descarga o visionado multimedia online.

Desventajas

- Obliga a depender de servicios que redirigen un host a una IP.
- Asignación de direcciones IP
- Dependiendo de la implementación concreta, el servidor DHCP tiene tres métodos para asignar las direcciones IP:

2.4.1.4. IP fija

Una **dirección IP fija** es una dirección IP asignada por el usuario de manera manual (Que en algunos casos el ISP o servidor de la red no lo permite), o por el servidor de la red (ISP en el caso de internet, router o switch en caso de LAN) con base en la Dirección MAC del cliente. Mucha gente confunde IP Fija con IP pública e IP dinámica con IP privada.

Una IP puede ser privada ya sea dinámica o fija como puede ser IP pública dinámica o fija.

Una IP pública se utiliza generalmente para montar servidores en internet y necesariamente se desea que la IP no cambie por eso siempre la IP pública se la configura de manera fija y no dinámica, aunque si se podría.

En el caso de la IP privada generalmente es dinámica asignada por un servidor DHCP, pero en algunos casos se configura IP privada fija para poder controlar el acceso a internet o a la red local, otorgando ciertos privilegios dependiendo del número de IP que tenemos, si esta cambiara (fuera dinámica) sería más complicado controlar estos privilegios (pero no imposible).

2.4.2. DIRECCIONES IPV6

La función de la dirección IPv6 es exactamente la misma que la de su predecesor IPv4, pero dentro del protocolo IPv6. Está compuesta por 128 bits y se expresa en una notación hexadecimal de 32 dígitos. IPv6 permite actualmente que cada persona en la Tierra tenga asignados varios millones de IPs, ya que puede implementarse con 2^{128} (3.4×10^{38} hosts direccionables). La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF.

2.5.RED PRIVADA VIRTUAL (VPN)

2.5.1. DEFINICIÓN

Una Virtual Private Network (VPN) es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. La idea es que la red pública sea "vista" desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

Una VPN no es más que una estructura de red corporativa implantada sobre una red de recursos de carácter público, pero que utiliza el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas, al fin y al cabo no es más que la creación en una red pública de un entorno de carácter confidencial y privado que permitirá trabajar al usuario como si estuviera en su misma red local. La configuración de una red privada virtual (VPN) garantiza que los equipos remotos se conecten a través de una conexión confiable (Internet), como si estuvieran en la misma red de área local.

Este proceso es utilizado por una variedad de compañías para permitir que los usuarios se conecten a la red cuando no se encuentran en el sitio de trabajo.

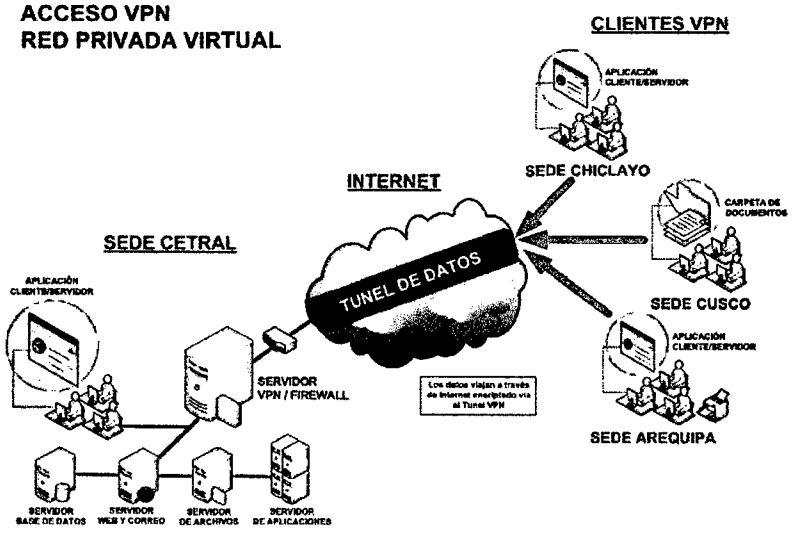


Fig. Ilustración de una VPN

2.5.2. ARQUITECTURA DE UNA VPN

Existen básicamente dos tipos de arquitectura para una VPN. Estos son:

A. VPN de acceso remoto
B. VPN de sitio a sitio

La VPN de sitio a sitio también puede ser llamada VPN LAN a LAN o VPN POP a POP. Las VPN de sitio a sitio se dividen a su vez en VPN extranet y VPN intranet.
Las VPN de acceso remoto se dividen en VPN Dial-up y VPN directas.

2.5.2.1. VPN de acceso remoto

Esta VPN proporciona acceso remoto a una intranet o extranet corporativa. Una VPN de acceso remoto permite a los usuarios acceder a los recursos de la compañía siempre que lo requieran. Con el cliente VPN instalado en un dispositivo, el usuario es capaz de conectarse a la red corporativa, no importa donde se encuentre. La figura 2.4 muestra una VPN de acceso remoto.

Las VPN de acceso remoto ahorran costos a las empresas ya que los usuarios sólo necesitan establecer una conexión con un ISP local, pagándose solamente la llamada local y olvidándose de realizar llamadas de larga distancia. El cliente de acceso remoto inicia una conexión VPN a través de Internet con el servidor VPN de la compañía. Una vez que se ha establecido el enlace, el usuario puede acceder a los recursos de la intranet privada de la empresa.

De acuerdo a la tecnología utilizada para establecer la conexión, las VPN de acceso remoto se puede dividir en VPN dial-up y VPN directas.

VPN dial-up. En esta VPN, el usuario realiza una llamada local al ISP utilizando un módem. Aunque se trata de una conexión lenta es todavía muy común. El uso de este tipo de VPN se da más entre los usuarios móviles, ya que no en todos los lugares a donde se viaja se pueden tener disponibles conexiones de alta velocidad.

VPN directa. En esta VPN, se utilizan las tecnologías de conexión a Internet de alta velocidad, tales como DSL y módem de cable las cuales ya ofrecen muchos ISP.
Este tipo de VPN se puede encontrar principalmente entre los teletrabajadores. Actualmente se pueden obtener conexiones a Internet desde el hogar utilizando estas tecnologías.

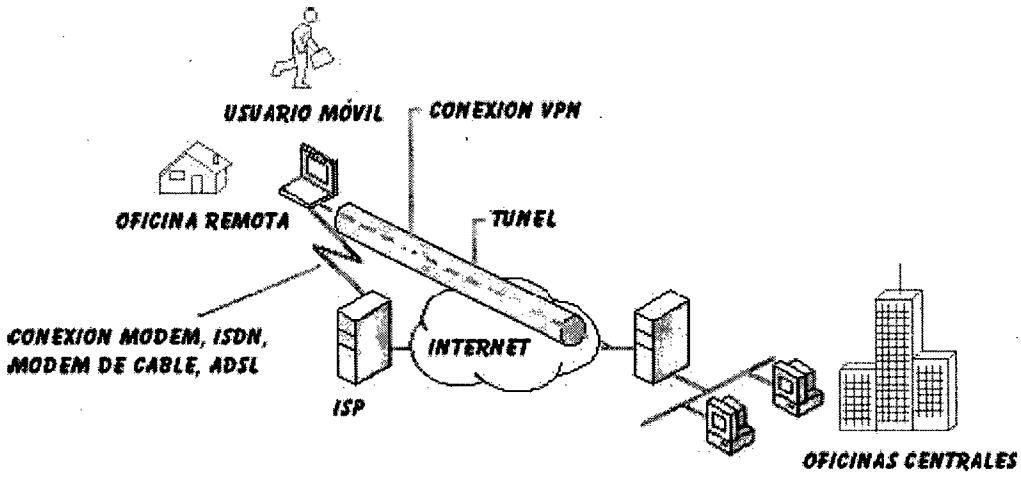


Figura 2.4 VPN de acceso remoto

2.5.2.2. VPN de sitio a sitio

Las VPN de sitio a sitio son utilizadas para conectar sitios geográficamente separados de una corporación. Como ya se explicó anteriormente, en las redes tradicionales las distintas oficinas de una corporación son conectadas utilizando tecnologías como T1, E1, ATM o Frame Relay.
Con una VPN, es posible conectar las LAN corporativas utilizando Internet. El envío de información se realiza a través de una conexión

VPN. De esta forma, se puede crear una WAN utilizando una VPN. Una empresa puede hacer que sus redes se conecten utilizando un ISP local y establezcan una conexión de sitio a sitio a través de Internet.
Los costos de la comunicación se reducen enormemente porque el cliente sólo paga por el acceso a Internet. Las oficinas remotas se conectan a través de túneles creados sobre Internet. Con el uso de la infraestructura de Internet, una empresa puede desechar la difícil tarea de tener que estar administrando los dispositivos como los que se utilizan en las WAN tradicionales.
En base a los problemas comerciales que resuelven, las VPN de sitio a sitio pueden subdividirse a su vez en VPN intranet y VPN extranet.

VPN intranet. Las VPN intranet se utilizan para la comunicación interna de una compañía, como aparece en la figura 2.5. Enlazan una oficina central con todas sus sucursales. Se disfrutan de las mismas normas que en cualquier red privada.
Un enrutador realiza una conexión VPN de sitio a sitio que conecta dos partes de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la que está conectado el servidor VPN.

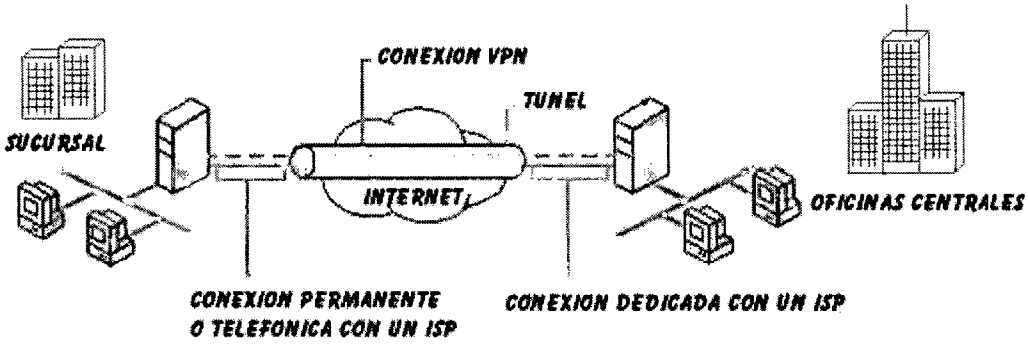


Figura 2.5 VPN intranet

VPN extranet. Estas VPN enlazan clientes, proveedores, socios o comunidades de interés con una intranet corporativa, como se muestra en la figura 2.6. Se puede implementar una VPN extranet mediante acuerdo entre miembros de distintas organizaciones. Las empresas disfrutan de las mismas normas que las de una red privada. Sin

embargo, las amenazas a la seguridad en una extranet son mayores que en una intranet, por lo que una VPN extranet debe ser cuidadosamente diseñada con muchas pólizas de control de acceso y acuerdos de seguridad entre los miembros de la extranet.

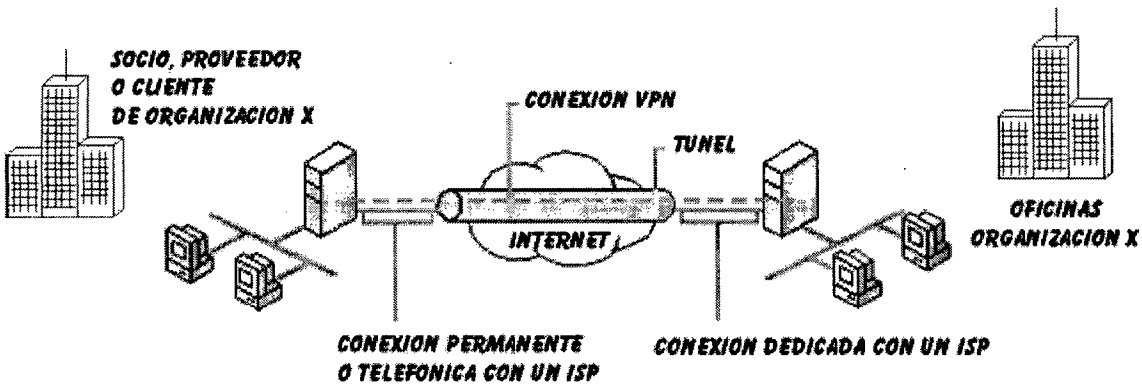


Figura 2.6 VPN extranet

2.5.3. TIPOS DE VPN

Existen diferentes formas de que una organización puede implementar una VPN.

Cada fabricante o proveedor ofrece diferentes tipos de soluciones VPN. Cada corporación tendrá que decidir la que más le convenga. Los tipos diferentes de VPN son:

- **C.** VPN de firewall
- **D.** VPN de router y de concentrador
- **E.** VPN de sistema operativo
- **F.** VPN de aplicación
- **G.** VPN de proveedor de servicios

2.5.3.1. VPN de firewall

Un firewall (llamado también cortafuegos o servidor de seguridad) es un sistema de seguridad que implanta normas de control de acceso entre dos o más redes.

Se trata de un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no. Un firewall puede ser un dispositivo software o hardware.

Es muy común que se utilice un firewall para proporcionar servicios VPN. Empresas como Cisco Systems, Nortel Networks y 3Com ofrecen en muchos de sus dispositivos firewall soporte para VPN. Una VPN basada en firewall tiene la ventaja de que simplifica la arquitectura de la red al establecer un único punto de control de seguridad. Además, los ingenieros de redes sólo tienen que hacerse expertos en una tecnología, en lugar de tener que aprender a administrar un firewall y la VPN de forma separada.

Entre los inconvenientes se puede mencionar que tener la VPN en un firewall convierte al dispositivo en algo más complejo, por lo que se debe ser más cuidadoso en su configuración o de lo contrario cualquier intruso podría tener acceso no autorizado a la red. Otra desventaja ocurre debido a que tener firewall y
VPN juntos, se ejerce presión al rendimiento del firewall. Esto ocurre principalmente si se tienen conectados cientos o incluso miles de usuarios.

2.5.3.2. VPN de router y de concentrador

Empresas como Cisco, Nortel y 3Com entre otros también ofrecen servicios VPN integrados dentro de un router o un dispositivo llamado concentrador VPN. Tanto el router como el concentrador VPN están especialmente diseñado para las conexiones VPN sitio a sitio y acceso remoto. Cuenta con las tecnologías VPN más importantes y los

métodos de autenticación y cifrado para proteger los datos transmitidos.

Este dispositivo está especialmente diseñado para las VPN, por lo que se trata de la solución VPN más rápida. Resulta ser más fácil agregarles tarjetas con el fin de incrementar el rendimiento. Dependiendo de la implementación, estas VPN pueden configurarse para utilizar certificados, servicios de autenticación externos o claves de seguridad.

2.5.3.3. VPN de sistema operativo

Los sistemas operativos como Windows de Microsoft, Netware de Novell o Linux en sus diferentes distribuciones (Red Hat, Debian,) ofrecen servicios de VPN ya integrados. La principal ventaja de esta solución es que resulta ser económica ya que en un mismo sistema operativo se pueden contar con una gran variedad de servicios (servidor Web, de nombres de dominio, acceso remoto, VPN) y además mejora los métodos de autenticación y la seguridad del sistema operativo. Tiene la desventaja de que es vulnerable a los problemas de seguridad del propio sistema operativo. Estas VPN se utilizan más para el acceso remoto.

2.5.3.4. VPN de aplicación

Este tipo de VPN es poco común. Una VPN de aplicación es un programa que añade posibilidades VPN a un sistema operativo. Sin embargo, este programa no queda integrado con el sistema operativo. La ventaja de este tipo de VPN es que la aplicación añade seguridad extra a la que podría ofrecer una VPN integrada al sistema operativo. Un ejemplo de esta VPN es el programa ViPNet de Infotecs.

La desventaja es que estas VPN no soportan una gran cantidad de usuarios y son mucho más lentas que una VPN basada en hardware. Si se utilizan en Internet, son vulnerables a las fallas de seguridad del sistema operativo que contiene a la aplicación.

2.5.3.5. VPN de proveedor de servicios

Este tipo de VPN es proporcionada por un proveedor de servicios. Al principio las VPN de proveedor de servicios se basaban en tecnologías tales como X.25 y Frame Relay, posteriormente ATM y SMDS y finalmente se ofrecen redes basadas en IP. El proveedor de servicios es la empresa propietaria de la infraestructura tales como equipos y líneas de transmisión que ofrece líneas dedicadas virtuales a sus clientes.
El cliente se conecta a la red del proveedor de servicios a través de un dispositivo de equipo terminal del cliente (CPE) como puede ser un router. El CPE se conecta a través de medios de transmisión al equipo del proveedor de servicios, que puede ser X.25, Frame Relay, un conmutador ATM o un router IP. La línea virtual que se le proporciona al cliente mediante el proveedor de servicios se le llama circuito virtual (VC).

El proveedor de servicios puede cargar o una tarifa plana para el servicio VPN, que habitualmente depende del ancho de banda disponible para el cliente, o una tarifa basada en el uso, que puede depender del volumen de datos intercambiados o de la duración del intercambio de datos.

Acuerdos a nivel del servicio (SLA, Service Level Agreements). Los SLA son contratos negociados entre proveedores VPN y sus abonados en los que se plantean los criterios de servicio que el abonado espera tengan los servicios específicos que reciba. La SLA es el único documento que está a disposición del abonado para asegurar que el proveedor VPN entrega el servicio o servicios con el nivel y calidad acordados. Si se ha de implementar una VPN basada en proveedor de servicios, este documento es de vital importancia para asegurar un buen servicio.

2.5.4. TOPOLOGÍAS DE VPN

La topología VPN que necesita una organización debe decidirse en función de los problemas que va a resolver. Una misma topología puede ofrecer distintas soluciones en diferentes compañías u organizaciones. En una VPN podemos encontrar las siguientes topologías:

Para las VPN de sitio a sitio:

H. Topología radial
I. Topología de malla completa o parcial
J. Topología híbrida

Para las VPN de acceso remoto:

K. Topología de acceso remoto

En las VPN basadas en ATM y Frame Relay, los enlaces que conectan las oficinas centrales con sus sucursales son circuitos virtuales (VC), mientras que en las VPN basadas en IP como Internet, estos enlaces son los túneles que se establecen a través de Internet.

2.5.4.1. Topología radial

En una VPN de sitio a sitio, ésta es la topología más común. Aquí, las sucursales remotas se conectan a un sitio central, como se puede ver en la figura 2.7. Las sucursales podrían intercambiar datos entre ellas, sin embargo, este tipo de datos resulta ser muy insignificante. La mayor parte del intercambio de datos se da con las oficinas centrales de la compañía. Los datos intercambiados entre las sucursales siempre viajan a través del sitio central.

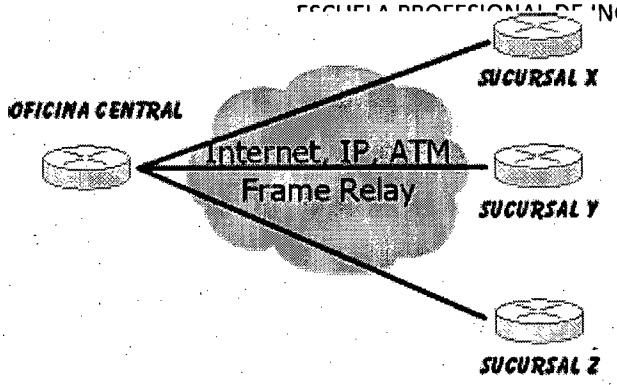


Figura 2.7 Topología radial

2.5.4.2. Topología de malla completa o parcial

Esta topología es implementada en corporaciones que no tienen una estructura demasiado jerárquica. Aquí, las diversas LAN de la compañía pueden realizar un intercambio constante de datos entre ellas. Dependiendo de sus necesidades, una empresa puede utilizar una topología de malla completa si todas las LAN se comunican entre sí o una topología de malla parcial, si sólo algunas LAN mantienen intercambio de datos. En la gran mayoría de los casos se utiliza sólo malla parcial. La figura 2.8 muestra una topología de malla:

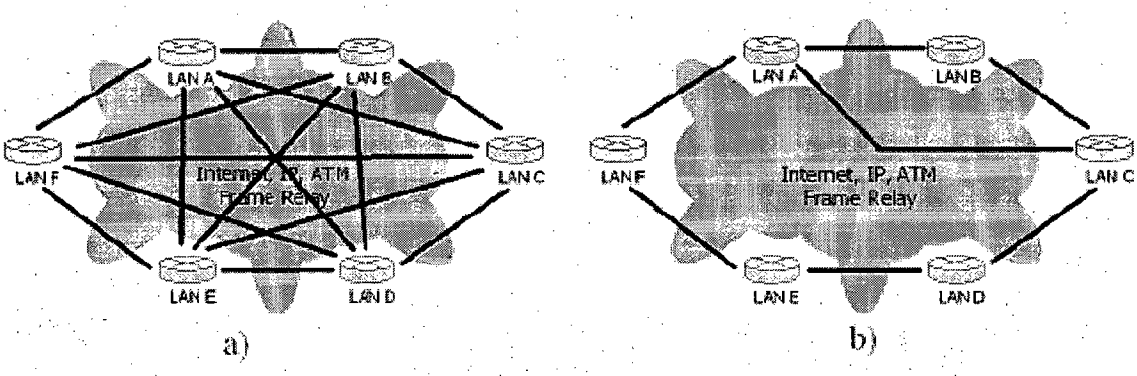


Figura 2.8 Topología de malla: a) completa b) parcial

2.5.4.3. Topología híbrida

Las redes VPN grandes combinan la topología radial con la topología de malla parcial. Como ejemplo, una empresa multinacional podría tener acceso a redes implementadas en cada país con una topología

radial, mientras que la red principal internacional estaría implementada con una tecnología de malla parcial.

2.5.4.4. Topología de acceso remoto

Esta topología consiste en un enlace punto a punto entre el usuario remoto y la oficina central utilizando tramas tunneling PPP intercambiadas entre el usuario remoto y el servidor VPN. El usuario y el servidor establecen conectividad usando un protocolo de capa 3, siendo el más común IP, sobre el enlace PPP entunelado e intercambian paquetes de datos sobre él.

2.5.5. VENTAJAS DE IMPLEMENTAR UN SERVICIO VPN

L. Reducción de Costos

Una VPN permite a una organización aprovecharse de las economías de escala y eficiencia propias de especialistas en transmisión de datos e Internet. Se hace posible entonces eliminar las líneas dedicadas punto-a- punto de muy alto precio que caracterizaron a muchas empresas con presencia regional por años, reemplazándolos por ejemplo, por accesos de tipo ADSL banda ancha y a bajo costo, disponibles en muchas áreas urbanas sin problemas.

M. Seguridad

Una VPN utiliza los más altos estándares de seguridad para la transmisión de datos, como por ejemplo el protocolo de encriptación 3DES (Triple Data Encryption Standard) y el protocolo Ipsec (IP Security Protocol) para el manejo de los "túneles" de software. Asimismo, se usan varios tipos de autenticación de usuarios para asegurarse que quienes se comunican son realmente quienes dicen ser.

N. Escalabilidad

Agregar usuarios a una VPN es casi trivial. No hay que realizar inversiones adicionales y la provisión de servicios se hace con dispositivos fáciles de usar y configurar y básicamente lo que se hace es usar la infraestructura de los proveedores de Internet en la red. La empresa descansa entonces en esa infraestructura de alto nivel.

O. Compatibilidad con tecnologías de banda ancha.

Una VPN puede aprovechar infraestructura existente de TV Cable, banda ancha inalámbrica, conexiones de alta velocidad de tipo ADSL o ISDN, lo que implica un alto grado de flexibilidad y reducción de costos al momento de configurar la red.

P. Mayor productividad.

Si los empleados de la empresa cuentan con una VPN, la usarán. Está probado que la disponibilidad de estas tecnologías aumenta la productividad de los usuarios, que se mantienen "conectados" más tiempo y con mejor nivel de acceso, y se fomenta el tele trabajo con la consiguiente reducción en las necesidades de espacio físico.

Una VPN provee más acceso y más seguridad para sus usuarios. Lo hace con tecnología moderna y a niveles de costo significativamente inferiores a las redes privadas tradicionales, conformadas por infraestructura propia con altos requerimientos de soporte que obligan a la empresa a ocuparse de asuntos que no son estratégicos para el negocio.

2.5.6. CARACTERÍSTICAS Y REQUERIMIENTOS.

Las Redes Privadas Virtuales utilizan tecnología de túnel (tunneling) para la transmisión de datos mediante un proceso de encapsulación y en su defecto de encriptación, esto es importante a

la hora de diferenciar Redes Privadas Virtuales y Redes Privadas, ya que esta última utiliza líneas telefónicas dedicadas para formar la red.

Seguridad, estableciendo un túnel de información encriptado entre su servidor y el proveedor de acceso a Internet.

2.5.7. PROTOCOLOS UTILIZADOS EN LAS VPN

2.5.7.1. PPTP (Point-to-Point Tunneling Protocol)

Fue desarrollado por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual. Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de Internet utilizando PPTP.

Existen dos escenarios comunes para este tipo de VPN:

Para el primero de los escenarios, el usuario remoto estable una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS. Para el segundo escenario, el usuario remoto se conecta al ISP mediante PPP y luego "llama" al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing Encapsulation (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.

El paquete PPTP está compuesto por un header de envío, un header Ip, un header GREv2 y el paquete de carga. El header de envío es el protocolo en marcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, frame relay, PPP. El header IP contiene información relativa al paquete IP, como ser, direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. La siguiente figura ilustra las capas del encapsulamiento PPTP.

Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, standard en el que se intercambia un "secreto" y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un standard propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Autenthication Protocol), que no encripta las contraseñas.
Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

2.5.7.2. PROTOCOLO IPSec

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme. Por confidencialidad se entiende que los datos transferidos sean solo entendidos por los participantes de la sesión.

Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende por la validación de remitente de los datos.

Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino.

ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header. AH sigue al header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del header IP. El header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.

Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway:

El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos

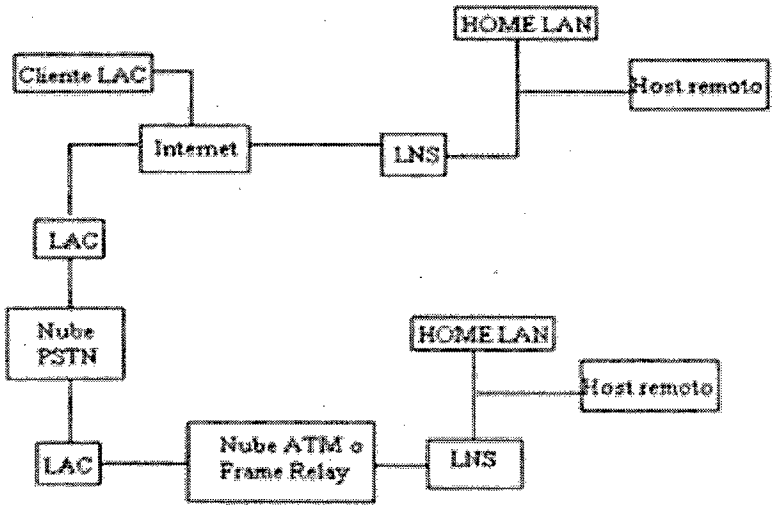
a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.

El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

2.5.7.3. L2TP (Layer-2 Tunneling Protocol)

Layer-2 Tunneling Protocol (L2TP) facilita el enrutamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.

El escenario típico L2TP, cuyo objetivo es la creación de entunelar marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local, es el que se muestra en la siguiente figura:



Protocolo L2TP

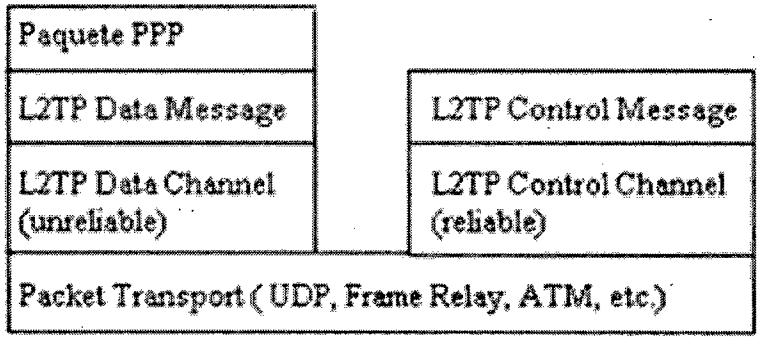
Un L2TP Access Concentrator (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP.

Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC.

Un cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.

El direccionamiento, la autenticación, la autorización y el servicio de cuentas son proveídos por el Home LAN's Management Domain. L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

La siguiente figura muestra la relación entre los marcos PPP y los mensajes de control a través de los canales de control y datos de L2TP.



Los marcos PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Se requiere que haya números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia para reordenar paquetes y detectar paquetes perdidos.

Al correr sobre UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo la parte de datos y el encabezado, viaja en un datagrama UDP. El que inicia un túnel L2TP toma un puerto UDP de origen que esté disponible, pudiendo ser o no el 1701 y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre, que puede ser o no el 1701, y envía la respuesta a la dirección de origen, sobre el mismo puerto iniciador. Luego de establecida la conexión, los puertos quedan estáticos por el resto de la vida del túnel.

En la autenticación de L2TP, tanto el LAC como el LNS comparten un secreto único. Cada extremo usa este mismo secreto al actuar tanto como autenticado como autenticador.

Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión.

2.6.SISTEMA SAP

La gestión de los diversos procesos que existen al interior de las organizaciones constituye uno de los ámbitos de más extensa aplicación de la informática, dados los beneficios en tiempo y dinero que ello supone. Lo anterior implica la necesidad de desarrollar mejores procesos de gestión, que contemplen a un mismo tiempo robustez en cuanto al total de aplicaciones a ejecutar, y flexibilidad por cuanto permita la constante incorporación de nuevos desarrollos tecnológicos, sin que ello signifique la obsolescencia del programa.

En este orden de ideas, surge el SAP como un programa informático diseñado para dotar a las empresas de una herramienta que les facilite una gestión de carácter integral, pues involucra soluciones a los problemas de administración en las áreas de producción, finanzas y recursos humanos. El éxito que ello ha significado en todo el mundo, ha despertado el interés de numerosas administraciones públicas, agobiadas por la necesidad de racionalizar y eficientar costos, de implementar dicho programa, como estrategia que les permita desarrollar sus procesos de manera más rápida y eficiente, y a un costo menor.

2.6.1. ¿QUÉ ES EL SAP?

Bajo el nombre de SAP se hace referencia tanto a un sistema informático diseñado para gestionar de manera más eficiente los recursos y procesos de producción de bienes y servicios al interior de una organización, así como a la empresa creadora de dicho sistema (SAP AG).

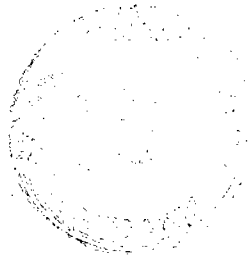
Por lo que respecta a la primera de las acepciones, el SAP, en su versión R/3, constituye un sistema informático de gran complejidad, integrado por varios softwares que se vinculan en una arquitectura cliente-servidor a tres niveles (de allí la designación de la versión), y

concebido para que las organizaciones cuenten con una herramienta que les permita ejercer una gestión más eficiente de cada una de sus áreas. Dicho sistema cuenta con la ventaja de que constante incorpora nuevas soluciones de negocio y herramientas tecnológicas, lo que le permite conservarse actualizado, y por lo tanto, adaptarse a las nuevas necesidades que surgen en materia de gestión de recursos al interior de las organizaciones.

La estructura básica de gestión integral que conforma el sistema SAP R/3 comprende tres aspectos fundamentales: gestión financiera, gestión de recursos humanos y logística

Aunado a lo anterior, el sistema SAP R/3 puede contemplar, si así se desea, las llamadas soluciones industriales, que constituyen paquetes especializados de aplicaciones de negocio, enfocados a diversos sectores productivos, entre los cuales se contempla el sector público.

El SAP constituye un programa informático muy completo, que permite una gestión integral de los recursos asignados a cada una de las áreas que conforman las organizaciones, y que permite ofrecer solución a las necesidades específicas de cada una de ellas.



2.7. DEFINICIÓN DE TÉRMINOS Y CONCEPTOS.

2.7.1. GLOSARIO:

- **Acceso remoto**. Conectarse a una red desde una ubicación distante.
- **Ancho de banda:** Es una medida de recursos disponibles para transmitir datos. También es una medida que se usa para definir la velocidad de Internet o, de forma más precisa, la velocidad de tu conexión de Internet.
- **Backbone**. Se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica
- **Cifrado**. Es un conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Existen muchas algoritmos de cifrado tales como DES, 3DES, RSA, SHA-1, MD5, etc.
- **Clúster.** Conjuntos o conglomerados de computadoras unidos entre sí normalmente por una red de alta velocidad y que se comportan como si fuesen una única computadora
- **Dirección IP:** Es un identificador numérico único que se asigna a una red específica o a una interfaz de red de un dispositivo en una red. Es una dirección de software que se puede traducir directamente a un host o nombre de red comprensible por el usuario. Las direcciones IP de interfaz de red de host también se asocian con una o más direcciones de interfaz de red de hardware.
- **Escalabilidad:** Es un término usado en tecnología para referirse a la propiedad de aumentar la capacidad de trabajo o de tamaño de un sistema sin comprometer su funcionamiento y calidad normales.

- **Extranet**. Una extranet es una intranet orientada a las personas u organizaciones que son externas a su empresa, pero necesitan acceder a alguna información, así se les permite el acceso a este contenido adicional, siempre bajo un sistema de autenticación y control de acceso.
- **Firewall.** Es un sistema de seguridad que implanta normas de control de acceso entre dos o más redes. Se trata de un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso.
- **Frame Relay.** Proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada punto a punto, esto quiere decir que es orientado a la conexión.
- **Hotspot.** Es un lugar que ofrece acceso a Internet a través de una red inalámbrica y un enrutador conectado a un proveedor de servicios de Internet.
- **Internet:** En forma muy resumida, Internet es una red de equipos de cómputo que se comunican entre sí empleando un lenguaje común.
- **Intranet.** Una intranet es una Internet orientada a una organización en particular. Una intranet reside dentro de un firewall y éste impide el acceso a los usuarios no autorizados.
- **IPSec**. Es un marco de estándares abiertos para lograr comunicaciones privadas seguras a través de redes IP mediante el uso de servicios de seguridad criptográfica.
- **ISP.** Es una organización que proporciona servicios de Internet a empresas y particulares.
- **Modem.** Es el dispositivo que convierte las señales digitales en analógicas (modulación) y viceversa (demodulación), permitiendo la comunicación entre computadoras a través de la línea telefónica o del cable módem. Este aparato sirve para enviar la señal moduladora mediante otra señal llamada portadora.
- **OSI.** Es un modelo creado por ISO que define los métodos y protocolos necesarios para lograr la comunicación entre los

equipos en una red. Este modelo define el funcionamiento de las redes en siete capas.

- **Protocolo**. En Informática y Telecomunicación, es el conjunto de reglas y estándares que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red, como teléfonos o computadoras, así como el ser humano tiene una forma de cómo comunicarse así también las computadoras y su comunicación con una red.
- **Protocolo**. Es un conjunto de reglas que definen cómo interactúan las entidades de comunicación. Para que una computadora se pueda comunicar con otra se requieren de varios protocolos los cuales van a definir las reglas de la comunicación.
- **Proxy**. un programa o sistema informático, que sirve de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C).
- **Puerta de enlace:** o pasarela (gateway) es el dispositivo que permite interconectar redes de computadoras con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.
- **Puerto:** Un puerto de red es una interfaz para comunicarse con un programa a través de una red. En el modelo OSI quien se preocupa de la administración de los puertos y los establece en el encabezado de los segmentos es la capa de transporte o capa 4, administrando así el envío y re-ensamblaje de cada segmento enviado a la red haciendo uso del puerto especificado. Un puerto suele estar numerado para de esta forma poder identificar la aplicación que lo usa.
- **Red privada**. Es aquella red exclusiva de una sola compañía u organización en particular. La información no se comparte con otras compañías u organizaciones.
- **Red pública**. Es una red a través de la cual circula información de muchas compañías y organizaciones. Una red pública siempre

será menos segura que una red privada, pero resultan ser más económicas.

- **Router**. Es un equipo que direcciona los paquetes de datos de una red a otra. Este dispositivo puede determinar cuál es la ruta más corta de un paquete hacia su destino, además de que también pueden optimizar el ancho de banda de la red y ajustarse de manera dinámica a problemas de patrones de tráfico cambiantes dentro de la red.
- **Sistema operativo de red**. Es un sistema operativo especialmente diseñado para la configuración y administración de redes. Un sistema operativo de red se instala en aquellas computadoras que van a operar como servidores.
- **Teletrabajador.** Empleado de una empresa que trabaja desde una oficina remota, lo cual generalmente es su hogar. Desde su computadora tiene acceso a ciertos recursos de la red corporativa.
- **Telnet.** es el nombre de un protocolo de red que nos permite viajar a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella
- **Token Ring.** es una arquitectura de red desarrollada por IBM en los años 1970 con topología lógica en anillo y topología física en estrella, y técnica de acceso de paso de testigo, usando un Frame de 3 bytes llamado token que viaja alrededor del anillo.
- **Transmisión por difusión (broadcast**). Un paquete de datos enviado por un dispositivo a todos los nodos de la red.
- **Tunneling.** El tunneling es un método utilizado para encapsular paquetes (conocidos como datos de usuario) dentro de otros paquetes los cuales son enviados utilizando la tecnología de la red por la que viaja. Algunos protocolos que usan esta tecnología son PPTP y L2TP.

2.7.2. SIGLARIO:

- **ACK:** Acknowledgement (acuse de recibo)
- **AD:** Active Directory (Directorio Activo)
- **DHCP:** Dynamic Host Configuration Protocol, (protocolo de configuración dinámica de host)
- **DNS:** Domain Name Server (Servidor de Nombre de Dominio)
- **HA:** High availability (Alta disponibilidad)
- **HTTP:** HiperText Transfer Protocol (Protocolo de transferencia de hipertexto).
- **HTTPS:** Hypertext Transfer Protocol Secure (Protocolo seguro de transferencia de hipertexto).
- **ICMP:** Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet).
- **IP:** Internet Protocol
- **IPSec:**Internet Protocol Security (Protocolo Internet de Seguridad)
- **ISDN:** Red Digital de Servicios Integrados.
- **ISO:** International Organisation for Standarisation (Estandarización para Organismos Internacionales)
- **ISP:** Internet Service Provider (proveedor de servicios de Internet)
- **ISP:** Internet Service Provider (Proveedor de Servicios de Internet)
- **L2TP**: Layer 2 Tunneling Protocol (Protocolo de Entunelamiento de Nivel 2)
- **LAN:** Local Area network (Red de área local)
- **NAP:** Network Access Point (Punto de acceso a red)
- **NAS:** Network Access Server (Servidor de Acceso Remoto)
- **NAT:** Network Access Translator (Traductor de Direcciones de Red)
- **NFS:** Network File Server (Servidor de Archive de Red)
- **NIC:** Network Interface Card (tarjeta de interfaz de red)
- **NIC:** Network Interface Card (Tarjeta de Interface de Red)

- **OSI:** Open Systems Interconection (Interconexión de Sistemas Abiertos)
- **PPTP:** Point to Point Tunneling Protocol (Protocolo de túnel Punto a Punto)
- **RAS:** Remote Access Server (Servidor de Acceso Remoto)
- **RRAS:** Remote and Routing Access Service (Servicios de Acceso Remoto y de Enrutamiento)
- **SNMP:** Simple Network Management Protocol (Protocolo Simple de Administración de Red)
- **TCP/IP:** Transmission Control Protocol / Internet Protocol (Protocolo de Control de Transmisión / Protocolo internet)
- **TCP:** Transmission Control Protocol
- **UDP:** User Datagram Protocol (Protocolo de Datagrama de Usuario)
- **URL:** Uniform resource locator (localizador de recursos uniforme)
- **UTP:** Unshielded Twister Pair, (par trenzado sin apantallar)
- **VLAN:** Virtual Local Área Network (Red de Área Local Virtual)
- **WAN:** Wide Area Network (red de área amplia).
- **WINS:** Windows Internet Naming Service (Servicio de nombres de internet de windows)

SITUACIÓN ACTUAL DE LA EMPRESA

3. SITUACIÓN ACTUAL DE LA EMPRESA

TERRACARGO SAC es una empresa dedicada al transporte de carga pesada y de paquetería, a nivel nacional e internacional con participación en los países de Ecuador, Brasil, Bolivia, Chile y Argentina. Además cuenta con clientes muy importantes como Saga Falabella S.A, Alicorp S.A.A, Ajeper S.A. entre otros los cuales demandan un servicio de mucha calidad

TERRACARGO SAC. Cuenta con 05 sucursales de las cuales 02 se encuentran en la ciudad de Lima en los distritos de Ate y la Victoria, las demás están ubicadas en provincias Tumbes, Piura y Chiclayo.

Misión:

Brindar el servicio de transporte de carga a nivel nacional e internacional con profesionalismo, gran voluntad, destreza y una flota de vehículos modernos que aseguran el transporte de su mercadería en forma oportuna, confiable y segura.

Visión:

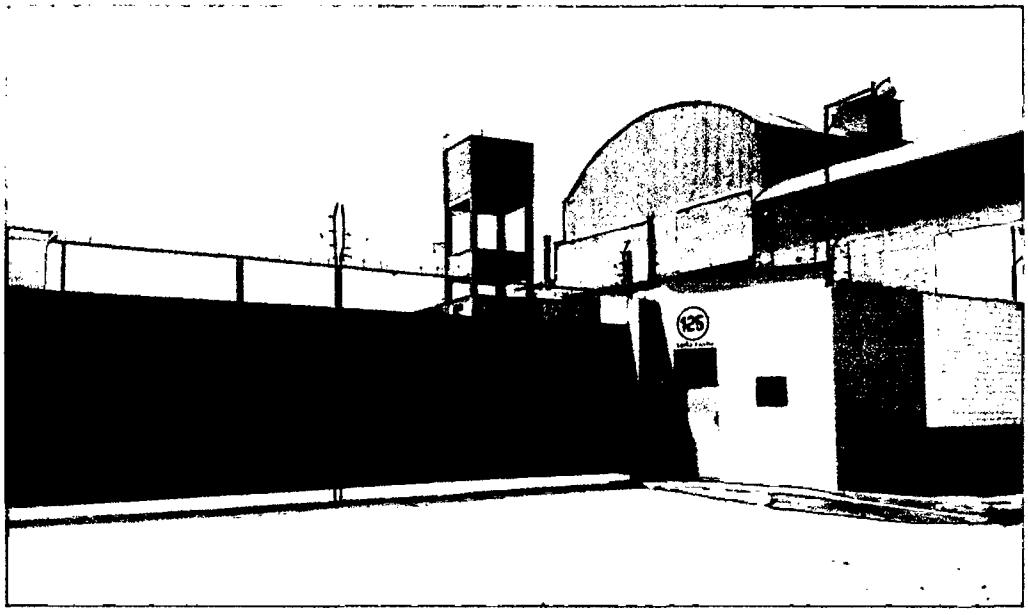
Constituirse en la empresa líder en el servicio de transporte de carga a nivel nacional e internacional, principal socio estratégico de nuestros clientes, y contribuir activamente en el desarrollo nacional

Nuestra empresa está dirigida por un grupo de profesionales altamente capacitados quienes están en condiciones de poner oportunamente a su disposición, todas las herramientas logísticas y tecnológicas, para brindarle a usted el mejor servicio, acompañado esto de un trato amable y confiable. La pieza fundamental de nuestro servicio lo constituye nuestro personal de choferes, los cuales han sido capacitados y entrenados para cumplir la misión encomendada; estando en condiciones de participar activamente en la identificación y solución de problemas en forma proactiva y positiva.

Nuestro personal trabaja bajo el lema de "darle al cliente lo mejor de nuestro servicio, nuestros conocimientos y nuestra experiencia"

3.1.UBICACIÓN DE LA EMPRESA TERRACARGO SAC

La empresa Terracargo SAC. Se encuentre ubicada en la calle Santa Cecilia #126 a la altura de la cuadra número 22 de la avenida Nicolás Ayllón.



Fachada de Terracargo SAC.

Interior de Terracargo SAC.

3.2.INFRAESTRUCTURA DE TERRACARGO SAC.

Actualmente la empresa cuenta con una moderna infraestructura de oficinas administrativas y de mantenimiento. También cuentan con áreas de carga y descarga y estacionamientos para sus vehículos.

3.2.1. Descripción de las Sucursales.

A. Sede Ate

Aquí se ubica la sede central de Terracargo SAC. Donde se realizan todas las funciones administrativas y mantenimiento de flota.

GERENCIA: Es el área considerada la cabeza de la empresa. Establece los objetivos y la dirige hacia ellos. Está relacionada con el resto de áreas funcionales, ya que es quien las controla.

AREA DE FINANZAS: Es el área que se encarga del óptimo control, manejo de recursos económicos y financieros de la empresa, esto incluye la obtención de recursos financieros tanto internos como externos, necesarios para alcanzar los objetivos y metas empresariales.

RECURSOS HUMANOS: Es el área encargada de la dirección eficiente y efectiva del recurso humano de la empresa. Dentro de las principales funciones de esta área, se pueden mencionar: Reclutamiento y selección de personal capaz, responsable y adecuado a los puestos de la empresa, la motivación, capacitación y evaluación del personal; el establecimiento de un medio ambiente agradable para el desarrollo de las actividades.

CENTRO DE CONTROL: Es el área encargada del monitoreo de la flota mediante GPS; los encargados de esta área trabajan 24/7 pues

es indispensable saber la ubicación de las unidades que se encuentran en ruta para poder dar un mejor servicio a los clientes.

OPERACIONES: Es el área encargada de la producción y la fabricación de un bien o servicio conforman la administración de operaciones. La función de operación comprende todo el proceso que se sigue desde que llega la materia prima hasta que esta convierte en un producto determinado. En las empresas de servicio esta función es conocida como operación.

LOGISTICA: Es el área encargada de trasformar la materia prima en productos y servicios terminados, utilizando los recursos humanos, económicos y materiales (herramientas y maquinaria) necesarios para su elaboración. Entre las principales funciones del área de producción, el mantenimiento y reparación de maquinaria o equipo, el almacenamiento de materia prima.

CONTABILIDAD: registra y clasifica las operaciones de la empresa en términos monetarios utilizando diferentes herramientas de registro como la Balanza General, Estado de Resultados y Balances de Comprobación.

ALMACEN: El área de almacén tiene la función de proveer al área de mantenimiento con los repuestos para realizar el mantenimiento a la flota.

SISTEMAS: Se encarga de mantener siempre en buen estado el funcionamiento técnico y tecnológico de la empresa para evitar que aquellas tareas que se realizan por medio de los servidores y dispositivos de la red estén en mal estado y no se lleven a cabo los objetivos de la empresa.

B. Sede La victoria

Administración, despacho y ventas

VENTAS: El departamento de ventas es el encargado de persuadir a un mercado de la existencia de un producto, valiéndose de su fuerza de ventas o de intermediarios, aplicando las técnicas y políticas de ventas acordes con el producto que se desea vender.

DESPACHO: entregar y recoger mercadería.

C. Sede Chiclayo: Despacho

D. Sede Piura: Despacho

E. Sede Tumbes: administración y despacho

3.3. CANTIDAD DE USUARIOS.

3.3.1. OFICINAS EN LA SUCURSAL DE ATE

OFICINAS	*N° Pc*	*Hardware*					*Software*				
		DUAL CORE	*CORE 2 DUO*	*CORE I3*	*CORE I5*	*CORE I7*	*WINDOWS XP*	*WINDOWS 7*	*WINDOWS 8*	*WINDOWS 10*	*SAP BUSSINESS ONE*
FINANZAS	10		3	3	3	1	1	5	1		7
CENTRO DE CONTROL	5	1	2		1	1	1	4			
GERENCIA	3			1	1	1		1	2		1
OPERACIONES	4		1	2	1			3	1		3
RR.HH	5	2	1	2			2	2	1		2
LOGISTICA	2		1	1				2			
ALMACEN	2	1	1				1	1			2
SISTEMAS	1					1				1	1
CONTABILIDAD	6			2	2	2		7			7
TOTAL PCs	**38**										

3.3.2. OTRAS SEDES.

OTRAS SEDES	OFICINAS EN OTRAS SEDES	N° Pc	Hardware					Software				
			DUAL CORE	CORE 2 DUO	CORE I3	CORE I5	CORE I7	WINDOWS XP	WINDOWS 7	WINDOWS 8	WINDOWS 10	SAP BUSSINESS ONE
LA VICTORIA	VENTAS	4				2	2		2	2		4
	DESPACHO	2			2					2		2
	ADMINISTRACIÓN	1		1						1		1
CHICLAYO	DESPACHO	1			1				1			1
	ADMINISTRACIÓN	1			1				1			1
PIURA	DESPACHO	2	1		1				2			2
	ADMINISTRACIÓN	1		1					1			1
TUMBES	DESPACHO	3	1		2				3			3
	ADMINISTRACIÓN	1		1					1			1

TOTAL PCs 16

Oficinas en La Victoria

Oficinas en ATE

3.4.INFRAESTRUCTURA DEL DATA CENTER

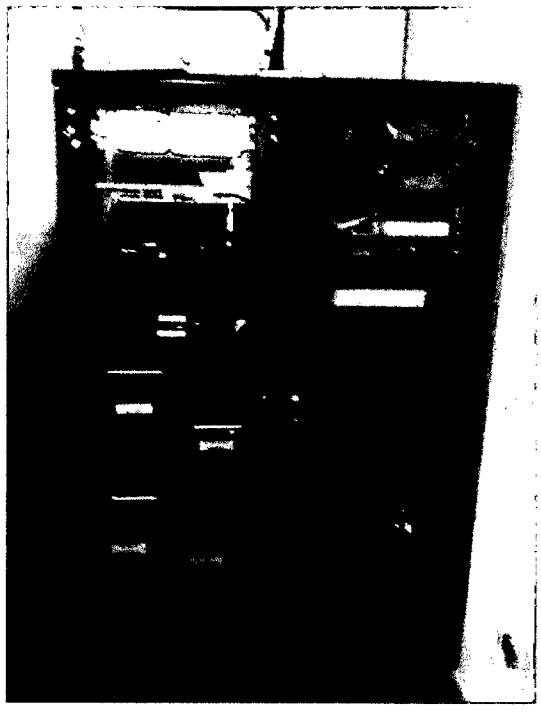
La empresa cuenta con un "Data Center" ubicada en un segundo piso del edificio. Este ambiente no cuenta con los requisitos mínimos de seguridad que debe tener un Data Center. El área de este ambiente es muy pequeño, lo que ocasiona que el diseño de red no sea escalable. No cuenta con un piso técnico para facilitar el paso del cableado y la protección del mismo.

La empresa cuenta con un enlace de fibra óptica, servicio de Optical Network, entre sus sucursales de La victoria y Ate, esto permite la interconexión hacia la central de Ate, este enlace genera a la empresa un costo mensual elevado.

Las sucursales que se encuentran en Chiclayo, Piura y Tumbes se interconectan a la central de Ate mediante TeamViewer que es un software de acceso remoto, este es un método no recomendable por la inseguridad al transportar la información.

3.4.1. EQUIPOS DE TECNOLOGÍA DE LA INFORMACIÓN

Se cuenta con un Gabinete de piso 45 RU.



Gabinete ubicado en el Cuarto de Telecomunicaciones de la Empresa.

EQUIPOS DE TI		
Cantidad	**Modelo**	**Marca**
2	Switch DES-1210-28	3com
1	Router serie 1921	Cisco
1	Modem óptico	Cisco
1	Modem ADSL	Tp-link
1	Servidores System x3500	IBM
1	Monitor	Dell
1	Teclado y mouse	Genius
2	UPS 1KW	Elise
2	DVR	DAHUA

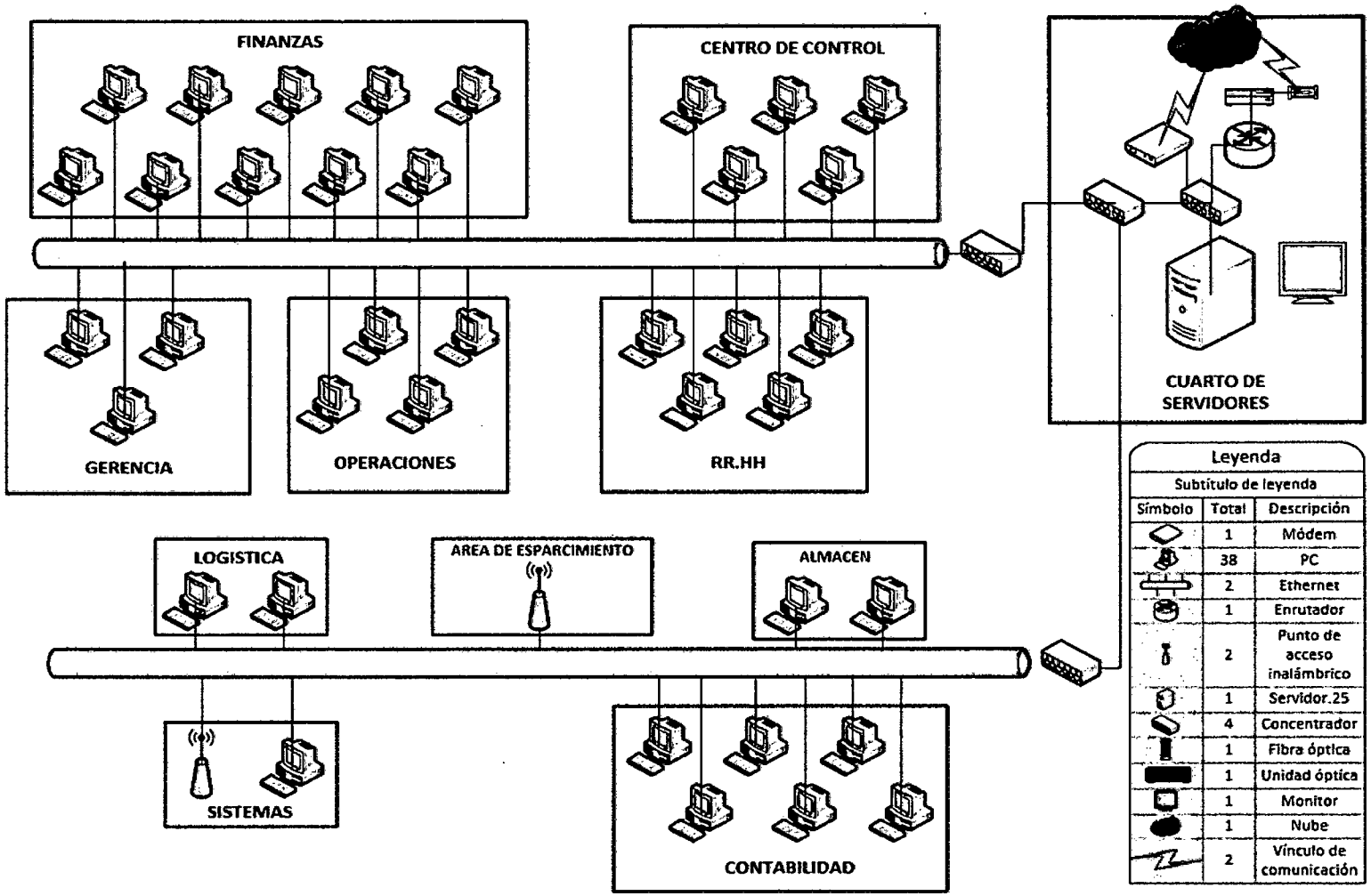
3.4.2. CABLEADO ESTRUCTURADO

Actualmente la Empresa no cuenta con un cableado de backbone o vertical que conecte al proveedor de servicio de internet con el gabinete de telecomunicaciones, con lo que sí cuenta es con un cableado horizontal lo cual interconecta todas las oficinas de la empresa.

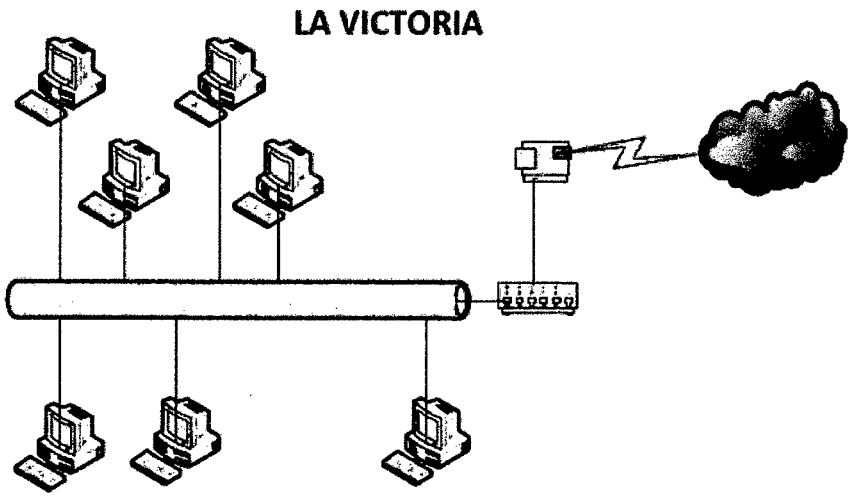
Se tiene instaladas 02 access-point distribuidos en el área de esparcimiento, en la oficina de finanzas.

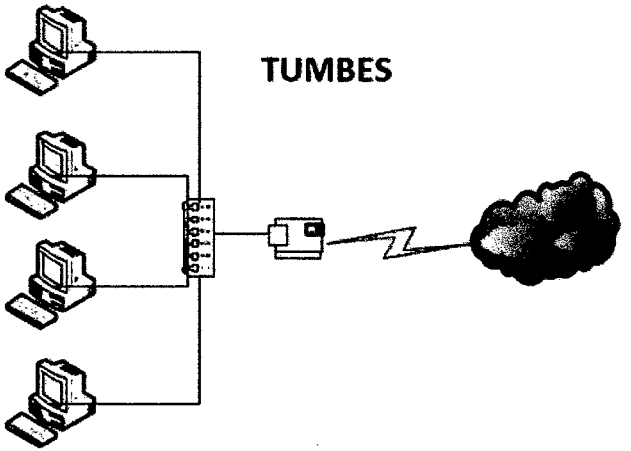
3.4.3. ESTRUCTURA DE LAS REDES LAN

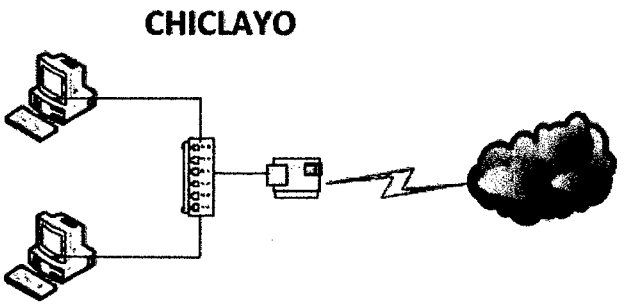
Sede ATE

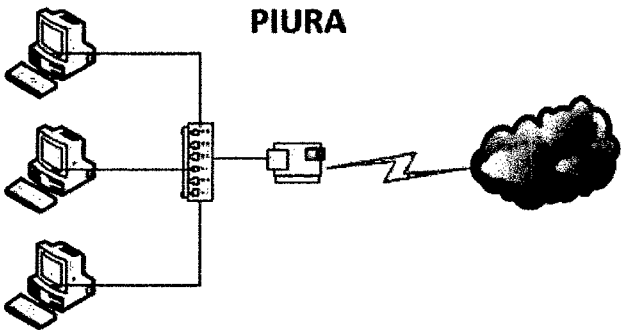


Otras sedes









3.5.SERVICIOS DE INTERNET.

SUCURSAL	*SERVICIO*	*Velocidad Mb/s*
ATE	Internet Fibra óptica Línea dedicada	2
ATE	Internet ADSL Línea comercial	10
VICTORIA	Internet ADSL Línea comercial	2
CHICLAYO	Internet ADSL Línea comercial	2
PIURA	Internet ADSL Línea comercial	1
TUMBES	Internet ADSL Línea comercial	1

3.6. REQUISITOS DE MEJORA.

- Hardware y software apropiados para el diseño.
- Hardware y software para brindar la seguridad de la información
- Servicio de internet, con velocidad adecuada para un funcionamiento rápido.
- Equipos de respaldo para evitar caídas en el servidor VPN y brindar la confiabilidad necesaria en la operación

DISEÑO DE UN MODELO DE RED VPN

4. DISEÑO DE UN MODELO DE RED VPN

4.1. ALTERNATIVAS DE SOLUCIONES

Las formas en que pueden implementar las VPN pueden ser basadas en HARDWARE o a través de SOFTWARE, pero lo más importante es el protocolo que se utilice para la implementación.

4.1.1. SOLUCIONES A NIVEL DE HARDWARE

Son equipos de red dedicada exclusivamente a la finalidad de VPN. Aunque por lo general más caros que el software VPN, hardware VPN puede ofrecer el mejor rendimiento para las organizaciones y empresas que dependen en gran medida de VPN. Hay consideraciones sobre topología de la red a pesar, como un hardware VPN es un aparato adicional y pueden requerir una amplia formación de un departamento de TI.

Hardware VPN Beneficios: Hardware dispositivos VPN se construyen específicamente para el propósito de VPN y pueden proporcionar la capacidad de VPN más eficiente para una organización o empresa. El uso de hardware de VPN se asegura de que otros equipos de la red puede centrarse en sus tareas previstas en lugar de proporcionar recursos para fines VPN. Un ejemplo es un router que se espera para reenviar el tráfico de la red a una velocidad determinada, y si sus recursos se destinan en parte a VPN, puede enviar los datos de red más lenta

4.1.1.1 VPN CISCO

Las redes privadas virtuales proporcionan el mayor nivel posible de seguridad mediante seguridad IP (IPsec) cifrada o túneles VPN de Secure Sockets Layer (SSL) y tecnologías de autenticación. Estas tecnologías protegen los datos que pasan por la red privada virtual contra accesos no autorizados. Las empresas pueden aprovechar la

infraestructura estilo Internet de la red privada virtual, cuya sencillez de abastecimiento permite agregar rápidamente nuevos sitios o usuarios. También pueden aumentar drásticamente el alcance de la red privada virtual sin expandir significativamente la infraestructura.

4.1.1.2. VPN D-LINK

Los routers de servicios unificados D-Link ofrecen soluciones en red seguras y de alto rendimiento para satisfacer las necesidades crecientes de las empresas. Estos routers están repletos de funciones avanzadas de seguridad y administración, como IEE 802.11n, acceso inalámbrico seguro, redundancia WAN 3G, IPv6 y completas funciones VPN que también pueden integrarse con facilidad en su infraestructura actual. Estos routers proporcionan a los trabajadores que tienen que desplazarse un acceso remoto en cualquier momento y lugar usando el potente motor VPN que permite establecer conexiones seguras con los recursos de la empresa.

D-Link ofrece un rendimiento comparable a las redes tradicionales de cable pero con menos limitaciones. La optima seguridad de red se obtiene por medio de características como túneles de red privada virtual (VPN), IPSec (IP Security), PPT (Point-to- Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), y SSL Secure Sockets Layer, que lo convierten en ideal para Pymes y delegaciones que necesitan una conexión segura y fiable a recursos remotos.

4.1.1.3. VPN MICROTIK

MIKROTIK proporciona VPN para unir redes distantes, haciendo un tunel de conexiones seguras a través de redes abiertas o internet, o conectar lugares remotos con conexiones cifradas; router OS soporta varios métodos y protocolos de tunel VPN.

- IPSec: El modo de túnel y de transporte, certificado o PSK, protocolos de seguridad AH y ESP.

- Túneles punto a punto (OpenVPN, PPTP, PPPoE, L2TP).
- Características avanzadas de PPP (MLPPP, BCP).
- Túneles básicos (IPIP, EoIP).
- Soporte de túneles 6 a 4 (IPv6 sobre IPv4 red).
- Soporte VLAN - IEEE802.1q Virtual LAN, Q-in-Q.
- MPLS basado en VPN

Esto significa que usted puede interconectar de forma segura las redes de banca, utilizar sus recursos de trabajo durante el viaje, conectarse a su red doméstica local, o aumentar la seguridad de su enlace de backbone inalámbrico. Incluso puede interconectar dos redes de sucursales de oficinas y que serían capaces de utilizar los recursos del otro, como si las computadoras estarían en el mismo lugar, todo seguro y encriptado

4.1.2. SOLUCIONES A NIVEL DE SOFTWARE

Software tecnología VPN está disponible en varias formas. Una forma es una aplicación añadido a un servidor existente en una red. Otra es una actualización de software para una pieza existente de equipos de red. Un proveedor de hardware puede ofrecer mayor funcionalidad de un dispositivo de red, como un router, como una actualización de software.

Software VPN Beneficios: Software VPN tiene una ventaja de ser de bajo costo en relación con los dispositivos de hardware VPN. Dado que el software puede ser instalado en el equipo existente, puede haber también menos formación necesaria para el personal de TI de una organización porque el mismo proveedor puede mantener una interfaz de aplicación similar. Software VPN es también una manera de mantener una topología de hardware más simple para una red.

4.1.2.1. OPEN VPN (LINUX)

OpenVPN es una solución de conectividad basada en software libre: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas IEEE 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas. Está publicado bajo la licencia GPL, de software libre.

OpenVPN, es un producto de software creado por James Yonan en el año 2001 y que ha estado mejorando desde entonces.

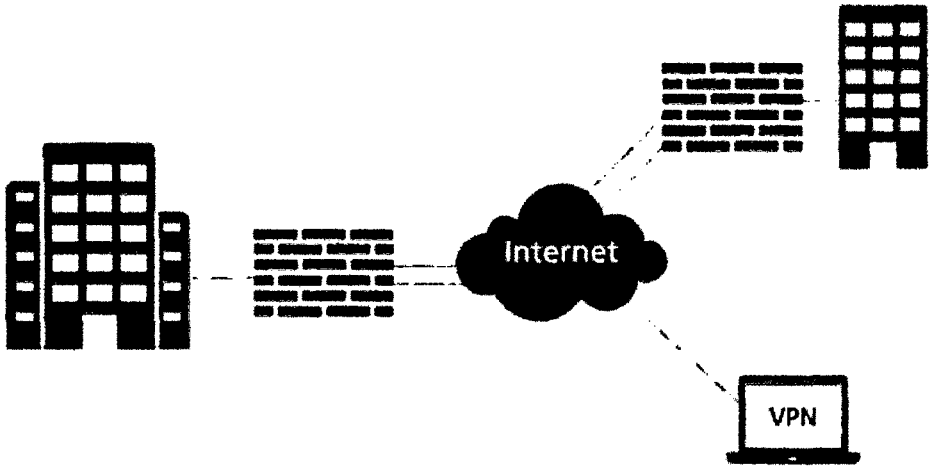
Ofrece una combinación de seguridad a nivel empresarial, seguridad, facilidad de uso y riqueza de características.

Es una solución multiplataforma que ha simplificado la configuración de VPN's frente a otras soluciones más antiguas y difíciles de configurar como IPsec y haciéndola más accesible para gente inexperta en este tipo de tecnología.

4.1.2.2. MCAFEE FIREWALL VPN

Combinando de forma inteligente el estándar VPN con IPsec con la tecnología McAfee Multi-Link, proporcionamos las soluciones VPN más flexibles y resilientes del mercado. Al agregar varios túneles VPN con IPsec con McAfee Multi-Link en dos o más conexiones distintas a ISP para formar un solo túnel VPN lógico, se puede establecer y mantener de forma fácil y rentable una conectividad VPN de alta disponibilidad. La enorme escalabilidad de McAfee Security Management Center hace que configurar y administrar miles de conexiones VPN sitio a sitio o de acceso remoto sea extraordinariamente sencillo.

Se puede controlar el uso de los enlaces agregando varias conexiones con características diferentes a una única VPN consolidada, y a la vez dirigir distintos tipos de tráfico de red a enlaces específicos. Dado que los enlaces de respaldo también se pueden definir por tipo de tráfico.



La solución VPN con IPsec proporciona el mayor nivel de conectividad segura. Admite la encriptación AES de 256 bits; la síntesis de mensajes SHA-2; autenticación RSA, DSS, ECDSA y PSK; y el intercambio de claves Diffie-Hellman hasta el grupo 21 incluido (grupo ECP de 521 bits).

La solución VPN con IPsec también ofrece alta disponibilidad para usuarios remotos y móviles. Un cliente VPN con IPsec mejorado con Multi-Link puede detectar y conectarse de forma automática a los gateway VPN con IPsec de Next Generation Firewall, lo que proporciona una conectividad confidencial y confiable a los usuarios móviles.

4.1.2.3. MICROSOFT FOREFRONT TMG VPN SERVER

Con una red privada virtual puede conectar componentes de red a través de otra red, por ejemplo Internet. Puede convertir un equipo basado en Windows Server 2008 en un servidor de acceso remoto de forma que otros usuarios puedan conectarse a él mediante VPN y, a continuación, puedan iniciar sesión en la red y tener acceso a los recursos compartidos. Las VPN implementan "túneles" a través de Internet o de otra red pública de manera que proporcionan la misma seguridad y funcionalidad que una red privada. Los datos se envían a través de la red pública utilizando su infraestructura de enrutamiento,

pero para el usuario parece como si los datos se enviaran a través de un vínculo privado dedicado.

Una VPN en servidores que ejecutan Windows Server 2008 consiste en un servidor VPN, un cliente VPN, una conexión VPN (la parte de la conexión en la que los datos están cifrados) y el túnel (la parte de la conexión en la que los datos están encapsulados). Los túneles se realizan a través de uno de los protocolos de túnel que se incluyen con los servidores que ejecutan Windows Server 2008, los cuales se instalan con el servicio Enrutamiento y acceso remoto. El servicio Enrutamiento y acceso remoto se instala automáticamente durante la instalación de Windows Server 2008. Sin embargo, de forma predeterminada, el servicio Enrutamiento y acceso remoto está desactivado.

Los dos protocolos de túnel que se incluyen con Windows son:

a) **Protocolo de túnel punto a punto (PPTP):** Proporciona cifrado de datos mediante el cifrado punto a punto de Microsoft.

b) **Protocolo de túnel de capa 2 (L2TP):** Proporciona cifrado de datos, autenticación e integridad mediante IPSec.

La conexión a internet debe utilizar una línea dedicada como T1, T1 fraccional o Frame Relay, El adaptador WAN debe ser configurado con la dirección IP y la máscara de subred asignadas al dominio o proporcionadas por un proveedor de servicios de internet (ISP). El adaptador WAN también debe estar configurado como puerta de enlace predeterminada del enrutador de ISP.

4.2. PARAMETROS PARA DETERMINAR EL DISEÑO DE VPN

Q. La homogeneidad del sistema, dado que el servidor y equipos actualmente en funcionamiento usan Microsoft Windows.

R. La empresa cuenta con licencias para Windows server 2008 R2 Microsoft, esto nos genera un ahorro significativo.

S. La interfaz de Windows es amigable y sencilla de configurar a diferencia de las otras alternativas, nos permite una administración sencilla en la red de la empresa.

T. Dada las necesidades de la empresa, Windows Server es una alternativa de solución Vpn adecuada para los requerimientos técnicos.

4.3. DISEÑO VPN

4.3.1. DETERMINAR NUMERO DE CLIENTES

El número de clientes lo determinan la cantidad de computadores fuera de la sede central de ATE.

SEDE	LA VICTORIA	CHICLAYO	PIURA	TUMBES
CLIENTES	7	2	3	4

4.3.2. TOPOLOGÍA Y PROTOCOLOS A USAR

Utilizamos la Topología de acceso remoto, esta topología consiste en un enlace punto a punto entre el usuario remoto y la oficina central, utilizando tramas tunneling PPP intercambiadas entre el usuario remoto y el servidor VPN. El usuario y el servidor establecen conectividad usando un protocolo de capa 3, siendo el más común IP, sobre el enlace PPP entunelado e intercambian paquetes de datos sobre él.

Y dentro de la configuración del ser Firewall perimetral para maximizar y centralizar la seguridad en cuanto al tráfico, en esta topología, Forefront TMG se encuentra en el perímetro de la red, donde actúa como firewall perimetral de la organización, y está conectado a dos redes: la red interna y la red externa.

El protocolo usado en la implementación de este proyecto es el PPTP, ya que Microsoft Windows Server usa dicho protocolo para tráfico VPN, por lo que también nos brinda una conexión segura de acceso remoto.

4.3.3. BENEFICIOS DE LA VPN

La Red Privada Virtual (VPN) abrió las puertas a una comunicación tanto rápida como confiable. Entre los principales beneficios de la VPN tenemos.

- La Confidencialidad de los datos, en el caso que fuesen interceptados durante la transmisión, no pueden ser decodificados. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma.
- Integridad de los datos, Por medio de una VPN podemos crear túneles en los cuales pasan la información encriptada entre los clientes por lo cual existe una integridad segura de los datos, además de no ser interpretados, los datos no deben ser modificados o alterados durante la transmisión.
- La Autenticación y Autorización, garantiza que los datos están siendo trasmitidos o recibidos desde dispositivos remotos autorizados y no desde un equipo cualquiera haciéndose pasar por él. Además, administra los distintos niveles de accesos y derechos de cada uno de los usuarios que utilizan la VPN.
- Solo se permiten conectarse a los equipos autorizados, por medio de certificados de autenticación, llaves encriptados y usuarios/contraseñas.

- Velocidad: Cuando enviamos o solicitamos información por medio de una red VPN es comprimida y descomprimida entre los 2 clientes de la VPN, esto hace que la VPN funcione más veloz en la transferencia de información.

- Costos: Un VPN nos ahorra en costo de los equipos y otros servicios que se estén ofreciendo dentro de la red local.

4.3.4. DETERMINAR LOS EQUIPOS A UTILIZAR EN LA RED

Servidores.

Los servidores operan a través de una arquitectura cliente-servidor. Los servidores son programas de computadora en ejecución que atienden las peticiones de otros programas, los clientes. Por tanto, el servidor realiza otras tareas para beneficio de los clientes.

Servidor intel Xeon(R) CPU E3-1240 v3.
Características:
Procesador : Intel Xeon 3.40 GHz.
Memoria Ram : 08 GB
Disco Duro : 02 TB

Servidor System x 3 500 E5506
Procesador : Intel Xeon 2.13 GHz.
Memoria Ram : 28 GB
Disco Duro : 500 GB

Servidor core i5 2 400
Procesador : Intel Core i5 3.10 GHz.
Memoria Ram : 04 GB
Disco Duro : 500 GB

Switch.

Es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red.

Switch 3com:

Modelo	: Baseline 2928 Pwr
Número de puertos	: 24
Puerto Giga Ethernet	: 01
Cantidad	: 01

Switch 3com:

Modelo	: 4226T
Número de puertos	: 24
Puerto Giga Ethernet	: 02
Cantidad	: 02

Routers:

También conocido como enrutador o encaminador de paquetes, y españolizado como rúter es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes.

Router Cisco:

Modelo	: 1921
Número de puertos	: 02
Puerto Giga Ethernet	: 02
Cantidad	: 01

MODEM

Es un dispositivo que convierte las señales digitales en analógicas (modulación) y viceversa (desmodulación), y permite así la comunicación entre computadoras a través de la línea telefónica o del cable módem. Sirve para enviar la señal *moduladora* mediante otra señal llamada *portadora*.

Modem Tp-Link adsl2

Modelo	: TD-W8970B
Número de puertos	: 04
Puerto Giga Ethernet	: 00
Cantidad	: 01

UPS:

Sistema de alimentación ininterrumpida, es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados. Otras de las funciones que se pueden adicionar a estos equipos es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna.

Modelo	: Apc Sua 1000i
Número de tomas	: 08
Capacidad	: 1 000 kw
Cantidad	: 02

4.3.5. SERVIDORES DE LA VPN

Debido a que se cuenta con licencias vigentes de Windows Server 2008 R2 y porque se utiliza este mismo sistema operativo para el servidor SAP, es la razón por el cual lo utilizaremos en nuestros servidores de VPN y Active Directory.

A. Servidor VPN (Forefront)

Como ya mencionamos en tiene como sistema operativo Windows Server 2008 R2 pero para poder configurar nuestro servidor VPN utilizaremos una herramienta de Microsoft denominada Forefront TMG, debido a que posteriormente se utilizarán otras funciones con las que cuenta éste:

Microsoft Forefront Threat Management Gateway (TMG)

Microsoft Forefront Client Security (antes conocido como Microsoft Client Protection) brinda una protección unificada contra malware para sistemas operativos de escritorios empresariales, laptops y servidores que es más fácil de administrar y controlar. Basada en la misma tecnología de protección de Microsoft altamente exitosa y ya utilizada por millones de personas en todo el mundo, Forefront Client Security ayuda a proteger contra amenazas emergentes como spyware y rootkits, como también contra amenazas tradicionales como virus, gusanos y Trojan horses y VPN. Proporcionando una administración simplificada a través de la administración central y brindando visibilidad crítica de las amenazas y vulnerabilidades, Forefront Client Security lo ayuda a proteger su empresa con mayor confianza y eficiencia. Forefront Client Security se integra con su software de infraestructura existente, como Active Directory, y complementa otras tecnologías de seguridad para una mayor protección y mejor control.

Microsoft Forefront TMG puede actuar como un router, un gateway de Internet, un servidor de red privada virtual (VPN), un servidor de traducción de direcciones de red (NAT) y un servidor proxy.

Características de Forefront TMG:

- ✓ Protección ante múltiples de ataques gracias a tener integrado un anti-malware y antivirus, protecciones contra ataques de nivel de red y nivel de aplicación y firewall multicapa.
- ✓ Altamente seguro gracias a la protección contra ataques de usuarios web, un sistema altamente fiable y seguro para la publicación por parte de usuarios remotos y un sistema avanzado para VPN.
- ✓ Gestión simplificada gracias a wizards que le ayudarán a configurarlo, un servicio centralizado y un sistema de envío de e-mails integrado.
- ✓ Inspección HTTPS. Inspecciones paquetes cifrados con SSL para descubrir malware, limitar el acceso a ciertas webs a sus empleados e incluso pudiendo creando exclusiones a webs sensibles, como las bancarias, evitando la inspección por parte de Forefront TMG.
- ✓ Entre otras novedades ISP redundancy, sistema de inspección de red, 64 bit, gestión centralizada de versiones Standard y Enterprise

Características de la seguridad:

- ✓ Punto único de contacto LAN- Internet con dos tarjetas de red.
- ✓ La única IP visible es la del proxy
- ✓ Filtra paquetes IP por puerto, tipo y URL, ya que los puertos se abren solo el tiempo imprescindible de paso de información.

B. Servidor Active Directory

Función Servicios de dominio de Active Directory

Servicios de dominio de Active Directory (AD DS) del sistema operativo Windows Server® 2008) almacena información acerca de los usuarios, equipos y otros dispositivos de la red. AD DS ayuda a los administradores a administrar esta información con seguridad y simplifica el uso compartido de recursos y la colaboración entre usuarios. AD DS debe estar instalado en la red para poder instalar aplicaciones habilitadas para el uso de directorios, como Microsoft® Exchange Server, y para aplicar otras tecnologías de Windows Server, como la directiva de grupo.

Dominio de Active Directory

Unidad administrativa de una red de equipos que, por comodidad de administración, agrupa diversas funcionalidades, como las siguientes:

- **Identidad de usuario en la red**. En los dominios, se pueden crear identidades de usuario y después hacer referencia a las mismas en cualquier equipo que esté unido al bosque donde se encuentra el dominio. Los controladores de dominio que forman un dominio almacenan las cuentas de usuario y credenciales de usuario, como contraseñas o certificados, de manera segura.
- **Autenticación**. Los controladores de dominio proporcionan servicios de autenticación para los usuarios. También ofrecen datos de autorización adicionales, como las pertenencias a grupos de usuarios. Los administradores pueden usar estos servicios para controlar el acceso a los recursos de la red.

- **Relaciones de confianza**: Los dominios hacen extensivos los servicios de autenticación a los usuarios de otros dominios del mismo bosque por medio de confianzas bidireccionales automáticas. Los dominios también hacen extensivos los servicios de autenticación a los usuarios de dominios de otros bosques por medio de confianzas de bosque o confianzas externas creadas manualmente.
- **Administración de directivas**. Un dominio es un ámbito de directivas administrativas, como reglas de complejidad y reutilización de contraseñas.
- **Replicación**. Un dominio define una partición del árbol de directorios que proporciona datos que son adecuados para ofrecer los servicios necesarios y que se replican entre los controladores de dominio. De esta forma, todos los controladores de dominio son elementos del mismo nivel en un dominio y se administran como una unidad.

Bosque de Active Directory

Colección de uno o varios dominios de Active Directory que comparten una estructura lógica, un esquema de directorio y una configuración de red comunes, así como relaciones de confianza automáticas, bidireccionales y transitivas. Cada bosque es una sola instancia del directorio y define una barrera de seguridad.

Nivel funcional de Active Directory

Configuración de AD DS que habilita características avanzadas de AD DS en todo el dominio o todo el bosque.

Migración

Proceso a través del cual se traslada un objeto de un dominio de origen a un dominio de destino, manteniendo o modificando sus características para que esté accesible en el nuevo dominio.

Reestructuración de dominios

Proceso de migración que requiere el cambio de la estructura de dominios de un bosque. Una reestructuración de dominios puede requerir la consolidación o incorporación de dominios, y puede tener lugar entre bosques o dentro de un bosque.

Consolidación de dominios

Proceso de reestructuración que requiere la eliminación de dominios de AD DS mediante la combinación de su contenido con el de otros dominios.

Actualización de dominio

Proceso en virtud del cual se actualiza el servicio de directorio de un dominio a una versión posterior. Incluye la actualización del sistema operativo en todos los controladores de dominio y la elevación del nivel funcional de AD DS según corresponda.

Actualización en contexto del dominio

Proceso en virtud del cual se actualizan los sistemas operativos de todos los controladores de dominio de un dominio dado; por ejemplo, se actualiza Windows Server 2003 a Windows Server 2008 y se eleva el nivel funcional del dominio, si es aplicable, manteniendo en su contexto los objetos de dominio, como usuarios y grupos.

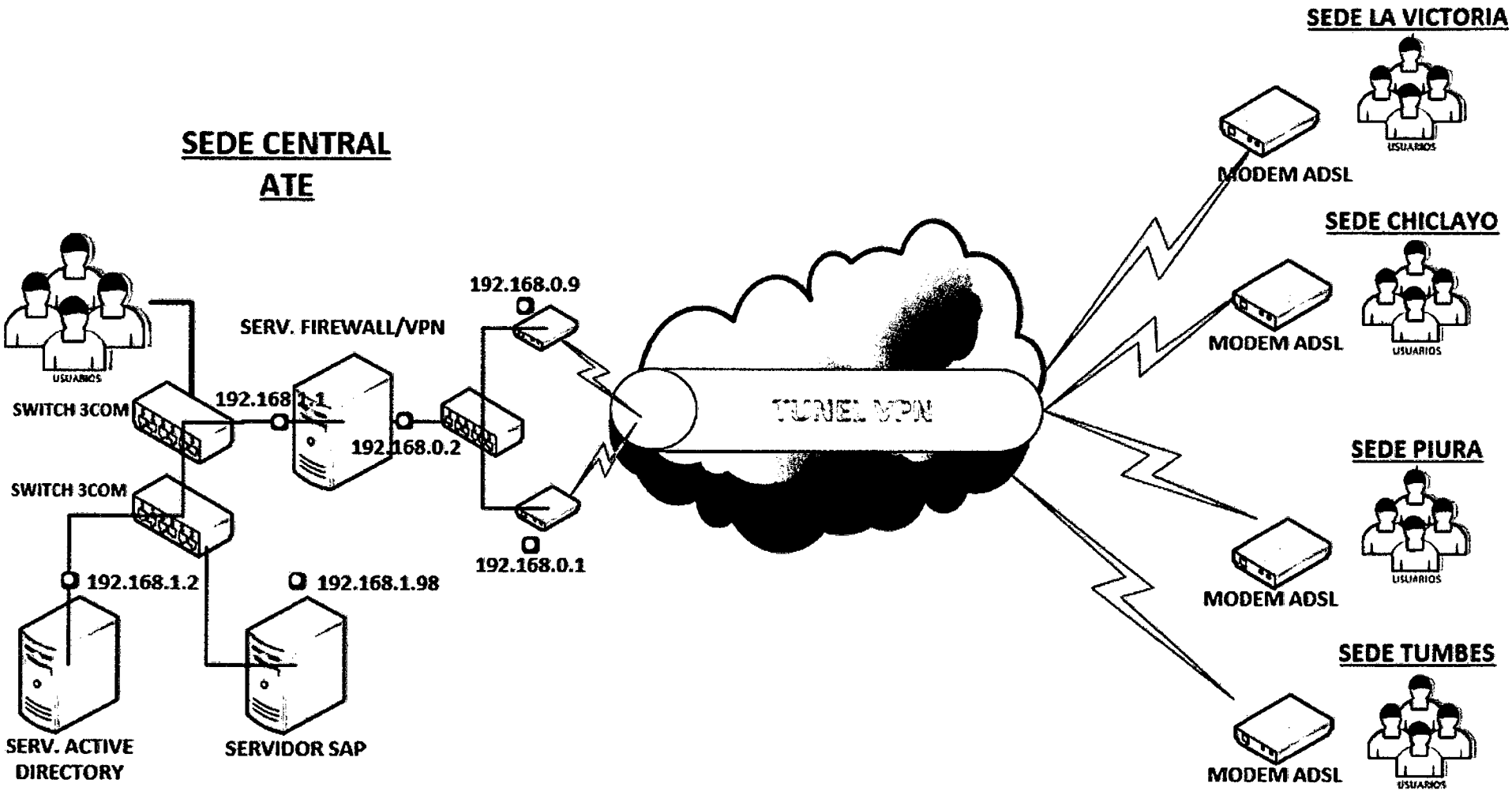
Dominio raíz del bosque

Es el primer dominio que se crea en el bosque de Active Directory. Este dominio se designa automáticamente como dominio raíz del bosque. Proporciona la base de la infraestructura del bosque de Active Directory.

Dominio regional

Dominio secundario que se crea en una zona geográfica para optimizar el tráfico de replicación.

4.4. ESTRUCTURA DE RED FINAL.



CUMPLIMIENTO DE REQUISITOS DE MEJORA

5. CUMPLIMIENTO DE REQUISITOS DE MEJORA

5.1. HARWARE Y SOFTWARE

Requisitos de sistema de Windows Server 2008

Este software está diseñado exclusivamente para fines de planificación de evaluación e implementación. Si tiene la intención de instalar el software en su equipo principal, se recomienda la realización de una copia de seguridad de los datos existentes antes de la instalación.

Componente	Requisito
Procesador	• Mínimo: 1 GHz • Recomendado: 2 GHz • Óptimo: 3 GHz o más **Nota:** Windows Server 2008 para sistemas basados en Itanium precisa un procesador Intel Itanium 2.
Memoria	• Mínimo: 512 MB de RAM • Recomendado: 1 GB de RAM • Óptimo: 2 GB de RAM (instalación completa) o 1 GB de RAM (instalación de Server Core) o más • Máximo (sistemas de 32 bits): 4 GB (Standard) o 64 GB (Enterprise y Datacenter) • Máximo (sistemas de 64 bits): 32 GB (Standard) o 2 TB (Enterprise, Datacenter y sistemas basados en Itanium)
Espacio en disco disponible	• Mínimo: 8 GB • Recomendado: 40 GB (instalación completa) o 10 GB (instalación de Server Core) • Óptimo: 80 GB (instalación completa) o 40 GB (instalación de Server Core) o más **Nota:** los equipos con más de 16 GB de RAM requerirán más espacio en disco para la paginación, para la hibernación y para los archivos de volcado
Unidad	Unidad de DVD-ROM
Pantalla y periféricos	• Super VGA (800 x 600) o monitor con una resolución mayor • Teclado • Mouse de Microsoft o dispositivo señalador compatible

5.2. VELOCIDAD DEL SERVICIO DE INTERNET

Un aspecto importante a considerar es la velocidad de su conexión VPN. Aunque la velocidad de un servicio VPN está relacionada con la velocidad de su Internet proporcionado por el ISP, también pueden ser influenciados por otros factores. La velocidad de conexión puede verse afectada por la ubicación del servidor de VPN, la proximidad más cercana a su servidor.

Por ello se solicitó aumentar la velocidad del servicio de internet en cada una de las sucursales.

SUCURSAL	***SERVICIO***	***Velocidad Mb/s***		***Velocidad***
ATE	Internet Fibra óptica Línea dedicada	2		–
ATE	Internet ADSL Línea comercial	10		–
VICTORIA	Internet ADSL Línea comercial	2		10
CHICLAYO	Internet ADSL Línea comercial	2		10
PIURA	Internet ADSL Línea comercial	1		4
TUMBES	Internet ADSL Línea comercial	1		4

Migración

5.3. PLAN DE ADMINISTRACIÓN

Nuestro Servicios de dominio de Active Directory implementado nos brinda las siguientes ventajas:

Un grupo es un conjunto de cuentas de usuario y de equipo, contactos y otros grupos que se pueden administrar como una sola unidad. Los usuarios y los equipos que pertenecen a un grupo determinado se denominan miembros del grupo.
Los grupos de los Servicios de dominio de Active Directory (AD DS) son objetos de directorio que residen en un dominio y en objetos contenedores de unidad organizativa (OU). AD DS proporciona un conjunto de grupos predeterminados cuando se instala y también incluye una opción para crearlos.
Los grupos de AD DS se pueden usar para:

- Simplificar la administración al asignar los permisos para un recurso compartido a un grupo en lugar de a usuarios individuales. Cuando se asignan permisos a un grupo, se concede el mismo acceso al recurso a todos los miembros de dicho grupo.

- Delegar la administración al asignar derechos de usuario a un grupo una sola vez mediante la directiva de grupo. Después, a ese grupo le puede agregar miembros que desee que tengan los mismos derechos que el grupo.

- Crear listas de distribución de correo electrónico.

Los grupos se caracterizan por su ámbito y su tipo. El ámbito de un grupo determina el alcance del grupo dentro de un dominio o bosque. El tipo de grupo determina si se puede usar un grupo para asignar permisos desde un recurso compartido (para grupos de seguridad) o si se puede usar un grupo sólo para las listas de distribución de correo electrónico (para grupos de distribución).

También existen grupos cuyas pertenencias a grupos no se pueden ver ni modificar. Estos grupos se conocen con el nombre de identidades especiales. Representan a distintos usuarios en distintas ocasiones, en función de las circunstancias. Por ejemplo, el grupo Todos es una identidad especial que representa a todos los usuarios actuales de la red, incluidos invitados y usuarios de otros dominios.

En las secciones siguientes se ofrece más información acerca de las cuentas de grupo de AD DS.

Información acerca de los grupos predeterminados

Los grupos predeterminados, como es el caso del grupo Administradores del dominio, son grupos de seguridad que se crean automáticamente cuando se crea un dominio de Active Directory. Estos grupos predefinidos pueden usarse para ayudar a controlar el acceso a los recursos compartidos y para delegar roles administrativos específicos en todo el dominio.

A muchos grupos predeterminados se les asigna automáticamente un conjunto de derechos de usuario que autorizan a los miembros del grupo a realizar acciones específicas en un dominio, como iniciar sesión en un sistema local o realizar copias de seguridad de archivos y carpetas. Por ejemplo, un miembro del grupo Operadores de copia de seguridad puede realizar operaciones de copia de seguridad para todos los controladores de dominio del dominio.

Cuando se agrega un usuario a un grupo, ese usuario recibe:

- Todos los derechos de usuario asignados al grupo
- Todos los permisos asignados al grupo para los recursos compartidos

Los grupos predeterminados se encuentran en el contenedor Builtin y en el contenedor Users. Los grupos predeterminados del contenedor Builtin tienen el ámbito de grupo Integrado local. Su ámbito de grupo y tipo de grupo no se pueden cambiar. El contenedor Users incluye grupos definidos con ámbito Global y grupos definidos con ámbito Local de dominio. Los grupos ubicados en estos contenedores se pueden mover a

otros grupos o unidades organizativas del dominio, pero no se pueden mover a otros dominios.

Información acerca del ámbito de grupo

Los grupos se caracterizan por un ámbito que identifica su alcance en el bosque o árbol de dominios. Existen tres ámbitos de grupo: local de dominio, global y universal.

Información acerca de los grupos locales de dominio

Los miembros de los grupos locales de dominio pueden incluir otros grupos y cuentas de dominios de Windows Server 2003, Windows 2000, Windows NT, Windows Server 2008 y Windows Server 2008 R2. A los miembros de estos grupos sólo se les pueden asignar permisos dentro de un dominio.

Los grupos con ámbito Local de dominio ayudan a definir y administrar el acceso a los recursos dentro de un dominio único. Estos grupos pueden tener los siguientes miembros:

- Grupos con ámbito Global
- Grupos con ámbito Universal
- Cuentas
- Otros grupos con ámbito Local de dominio
- Una combinación de los anteriores

Por ejemplo, para conceder acceso a una impresora determinada a cinco usuarios, puede agregar las cinco cuentas de usuario a la lista de permisos de la impresora. Sin embargo, si posteriormente desea que esos cinco usuarios tengan acceso a otra impresora, deberá volver a especificar las cinco cuentas en la lista de permisos para la nueva impresora.

Con un poco de previsión, puede simplificar esta tarea administrativa rutinaria al crear un grupo con ámbito Local de dominio y asignarle permisos de acceso a la impresora. Coloque las cinco cuentas de usuario en un grupo con ámbito Global y agregue este grupo al grupo que tiene ámbito Local de dominio. Cuando desee que los cinco usuarios tengan acceso a una nueva impresora, asigne permisos de acceso a la nueva impresora al grupo con ámbito Local de dominio. Todos los miembros del grupo con ámbito Global recibirán automáticamente el acceso a la nueva impresora.

Información acerca de los grupos globales

Los miembros de los grupos globales pueden incluir sólo otros grupos y cuentas del dominio en el que se encuentra definido el grupo. A los miembros de estos grupos se les pueden asignar permisos en cualquier dominio del bosque.

Use los grupos con ámbito Global para administrar objetos de directorio que requieran un mantenimiento diario, como las cuentas de usuario y de equipo. Dado que los grupos con ámbito Global no se replican fuera de su propio dominio, las cuentas de un grupo con ámbito Global se pueden cambiar frecuentemente sin generar tráfico de replicación en el catálogo global.

Información acerca de los grupos universales

Los miembros de los grupos universales pueden incluir otros grupos y cuentas de cualquier dominio del bosque o del árbol de dominios. A los miembros de estos grupos se les pueden asignar permisos en cualquier dominio del bosque o del árbol de dominios.

Use los grupos con ámbito Universal para consolidar los grupos que abarquen varios dominios. Para ello, agregue las cuentas a los grupos con ámbito Global y anide estos grupos dentro de los grupos que tienen ámbito Universal. Si usa esta estrategia, los cambios de pertenencias en los grupos que tienen ámbito Global no afectan a los grupos con ámbito Universal.

Por ejemplo, si una red tiene dos dominios, Europe y UnitedStates, y hay un grupo con ámbito Global denominado GLAccounting en cada dominio, cree un grupo con ámbito Universal denominado UAccounting que tenga como miembros los dos grupos GLAccounting, UnitedStates\GLAccounting y Europe\GLAccounting. Después, podrá usar el grupo UAccounting en cualquier lugar de la organización. Los cambios de pertenencia de los grupos GLAccounting individuales no producirá la replicación del grupo UAccounting.

No cambie la pertenencia de un grupo con ámbito Universal frecuentemente. Los cambios de pertenencia de este tipo de grupo hacen que se replique toda la pertenencia del grupo en cada catálogo global del bosque.

Información acerca de los tipos de grupo

Hay dos tipos de grupos en AD DS: grupos de distribución y grupos de seguridad. Los grupos de distribución se usan para crear listas de distribución de correo electrónico y los grupos de seguridad se usan para asignar permisos para los recursos compartidos.

Los grupos de distribución sólo se pueden usar con aplicaciones de correo electrónico (como Microsoft Exchange Server 2007) para enviar mensajes a conjuntos de usuarios. Los grupos de distribución no tienen seguridad habilitada, lo que significa que no pueden aparecer en las listas de control de acceso discrecional (DACL). Si necesita un grupo para controlar el acceso a los recursos compartidos, cree un grupo de seguridad.

Si se usan con cuidado, los grupos de seguridad son eficaces para conceder acceso a los recursos de la red. Con los grupos de seguridad se puede:

- Asignar derechos de usuario a los grupos de seguridad de AD DS

  Se asignan derechos de usuario a un grupo de seguridad para determinar lo que pueden hacer los miembros de ese grupo en el

ámbito de un dominio (o bosque). A algunos grupos de seguridad se les asignan derechos de usuario automáticamente cuando se instala AD DS para ayudar a los administradores a definir el rol administrativo de una persona en el dominio. Por ejemplo, si se agrega un usuario al grupo Operadores de copia de seguridad de Active Directory, éste puede realizar operaciones de copia de seguridad y restauración de archivos y directorios en cada controlador de dominio del dominio.

- Asignar permisos para recursos a los grupos de seguridad

Los permisos y los derechos de usuario no son lo mismo. Los permisos determinan quién puede obtener acceso a un recurso compartido y el nivel de acceso, como Control total. Los grupos de seguridad se pueden usar para administrar el acceso y los permisos en un recurso compartido. Algunos permisos que se establecen en objetos de dominio se asignan automáticamente para proporcionar varios niveles de acceso a los grupos de seguridad predeterminados, como el grupo Operadores de cuentas o el grupo Administradores del dominio.

Como sucede con los grupos de distribución, los grupos de seguridad también se pueden usar como entidades de correo electrónico. Al enviar un mensaje de correo electrónico al grupo, se envía a todos sus miembros.

Identidades especiales

Además de los grupos de los contenedores Users y Builtin, los servidores en los que se ejecuta Windows Server 2008 R2, Windows Server 2008 o Windows Server 2003 incluyen varias identidades especiales. Por comodidad se las suele llamar grupos. Estos grupos especiales no tienen pertenencias específicas que se puedan modificar. Sin embargo, pueden representar a distintos usuarios en distintas ocasiones, en función de las circunstancias. Los grupos siguientes son identidades especiales:

- **Inicio de sesión anónimo**: Este grupo representa a los usuarios y servicios que obtienen acceso a un equipo y sus recursos a través de la

red sin usar un nombre de cuenta, contraseña o nombre de dominio. En los equipos con Windows NT y versiones anteriores, el grupo Inicio de sesión anónimo es un miembro predeterminado del grupo Todos. En los equipos con Windows Server 2008 R2, Windows Server 2008 o Windows Server 2003, el grupo Inicio de sesión anónimo no es miembro del grupo Todos de manera predeterminada.

- **Todos:** Este grupo representa a todos los usuarios actuales de la red, incluidos invitados y usuarios de otros dominios. Cuando un usuario inicia sesión en la red, se agrega automáticamente al grupo Todos.

- **Red:** Este grupo representa a los usuarios que obtienen acceso en ese momento a un recurso dado a través de la red, frente a los usuarios que obtienen acceso a un recurso mediante un inicio de sesión local en el equipo en el que reside el recurso. Cuando un usuario obtiene acceso a un recurso dado a través de la red, se agrega automáticamente al grupo Red.

- **Interactivo:** Este grupo representa a todos los usuarios que disponen de una sesión iniciada en un equipo determinado y que están obteniendo acceso a un recurso ubicado en ese equipo, frente a los usuarios que obtienen acceso al recurso a través de la red. Cuando un usuario obtiene acceso a un recurso dado en el equipo en el que ha iniciado sesión, se agrega automáticamente al grupo Interactivo.

Aunque a las identidades especiales se les puede conceder derechos y permisos para los recursos, sus pertenencias no se pueden ver ni modificar. Las identidades especiales no tienen ámbitos de grupo. Los usuarios son asignados automáticamente a ellas cuando inician sesión u obtienen acceso a un recurso concreto.

Información acerca de dónde se pueden crear grupos

En AD DS, los grupos se crean en los dominios. Para crear grupos, se usan Usuarios y equipos de Active Directory. Con los permisos necesarios, se pueden crear grupos en el dominio raíz del bosque, en cualquier otro dominio del bosque o en una unidad organizativa.
Además de por el dominio en el que se crea, un grupo también se caracteriza por su ámbito. El ámbito de un grupo determina lo siguiente:

- El dominio desde el que se pueden agregar miembros
- El dominio en el que son válidos los derechos y permisos asignados al grupo

Elija el dominio o la unidad organizativa donde va a crear un grupo en función de las tareas de administración que requiera el grupo. Por ejemplo, si un directorio tiene varias unidades organizativas y cada una tiene un administrador diferente, puede crear grupos con ámbito Global dentro de esas unidades organizativas para que los administradores administren la pertenencia a grupos de los usuarios de las unidades organizativas que les correspondan. Si se necesitan grupos para controlar el acceso fuera de la unidad organizativa, puede anidar los grupos de la unidad organizativa dentro de grupos con ámbito Universal (u otros grupos con ámbito Global) que puede utilizar en otros lugares del bosque.

5.4. SISTEMAS DE RESPALDO

5.5.1. CAÍDAS CONTINUAS DE LA RED

A. Corte del servicio eléctrico.

Cuando se produce un corte eléctrico dentro de las instalaciones de la empresa Terracargo SAC, se activan tres UPS's de respaldo que se encuentran ubicados en el los gabinetes de servidores; son tres equipos de 1 KW que duran aproximadamente 20 minutos. Y están distribuidos de la siguiente manera:

- El primer UPS se encuentra protegiendo los servidores.
- El segundo se encuentra conectado a las cámaras de seguridad.
- Y el tercero y último se encuentra conectado a los otros equipos, como son: modem ADSL de internet, router CISCO del internet de fibra óptica.

B. Corte del servicio de internet.

Nuestra servicio TMG FOREFRONT nos permite una aplicación de Redundancia del proveedor de acceso a Internet (ISP), que permite vincular dos adaptadores de red externos a dos ISP diferentes.
Hay dos modos de redundancia de ISP:

- El **modo de alta disponibilidad** designa un vínculo principal que soporta todo el tráfico saliente de Internet y un vínculo de reserva que se activa automáticamente en caso de que el primer vínculo no funcione.

- El **modo de equilibrio de carga** dirige el tráfico saliente de Internet entre dos vínculos de ISP de manera simultánea y establece el porcentaje de tráfico de Internet total por vínculo. También admite la conmutación por error si uno de los vínculos no funciona.

5.5. Comprobar la funcionalidad y validar del modelo de VPN

5.5.1. Opinión del cliente.

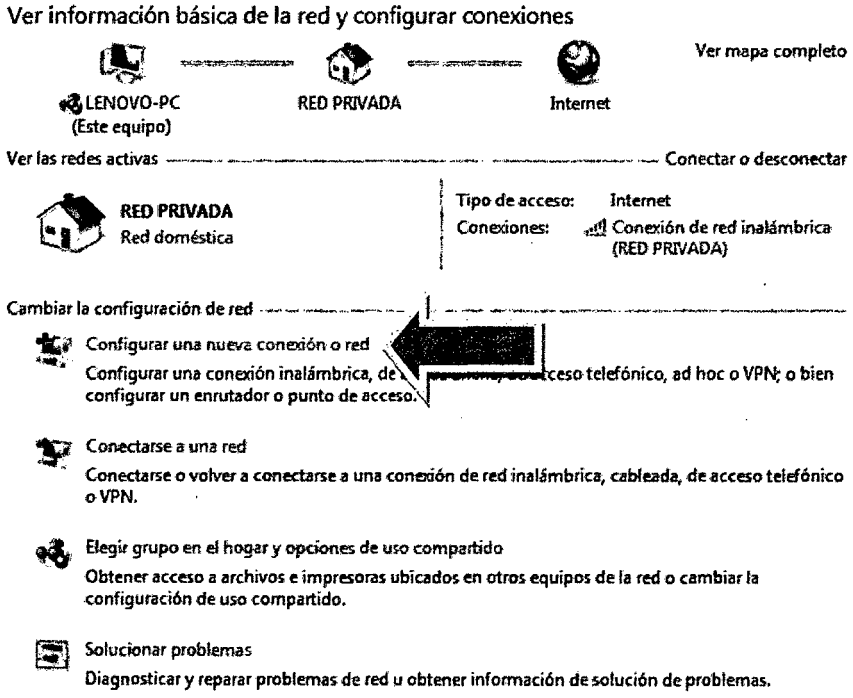
El Gerente general de Terracargo SAC da fidelidad del buen desempeño de la red VPN, emitiendo una carta de conformidad, esto demuestra la funcionalidad correcta de todo lo propuesto.

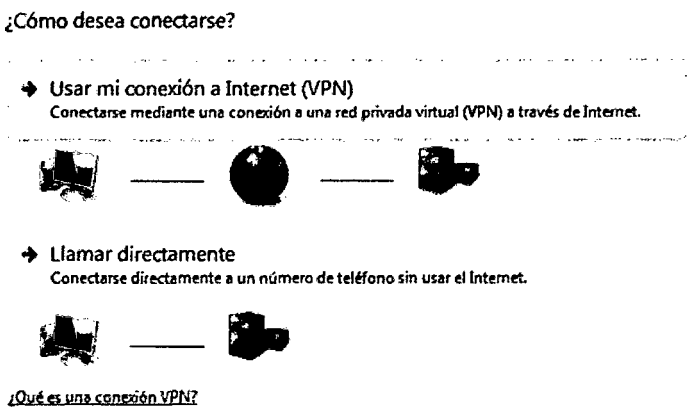
5.5.2. COMPROBACIÓN DE LA CONEXIÓN.

Podemos comprobar la conexión, accediendo a la VPN con una cuenta creada para realizar la prueba correspondiente.

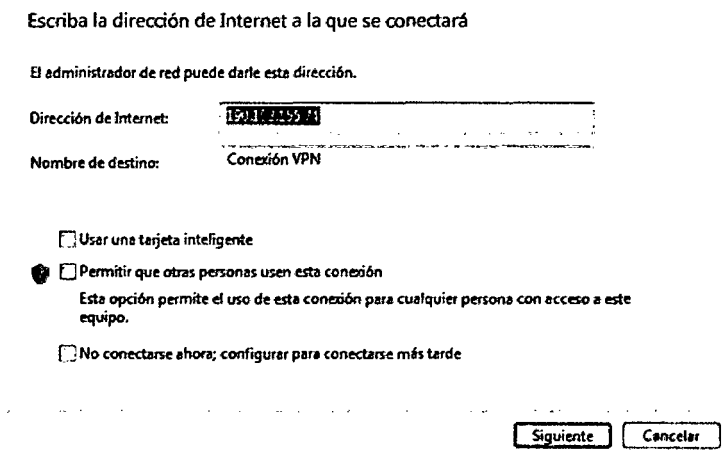
Para ello realizamos los siguientes pasos.

- Se configura una nueva conexión y nos agregamos a un área de trabajo mediante la conexión de internet

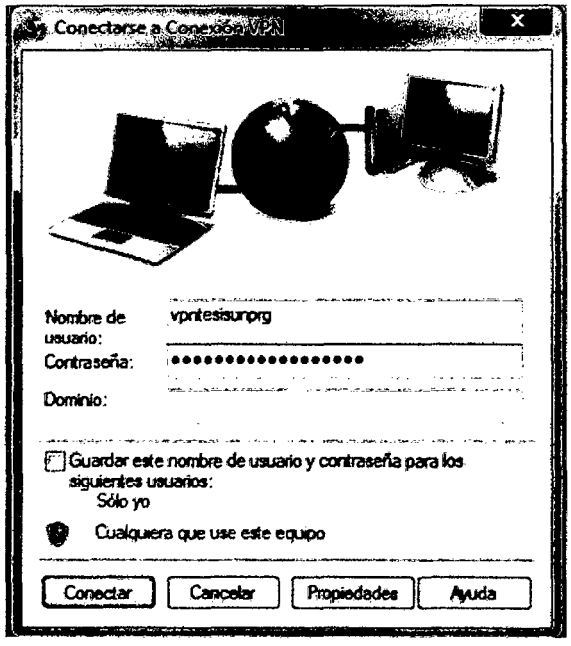




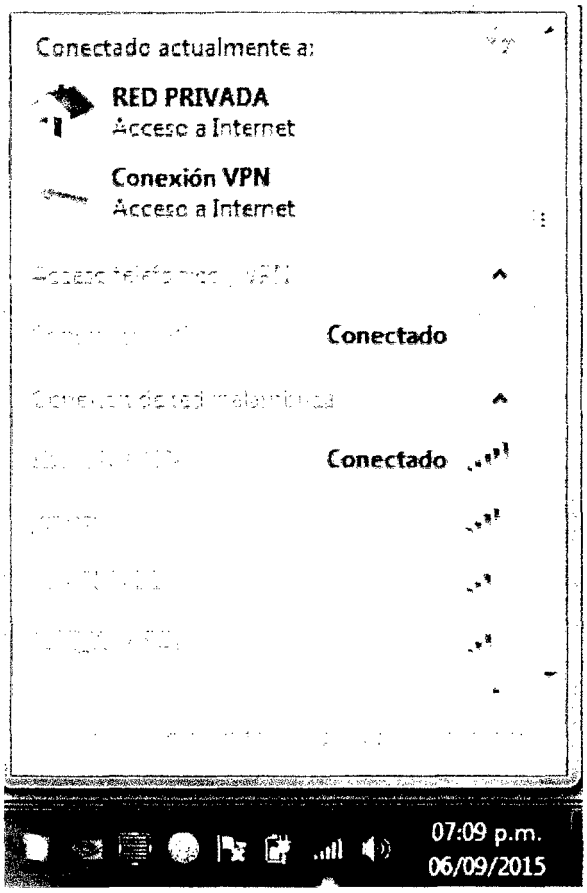
- Agregamos la IP pública estática de nuestro proveedor en la sede central para lograr el acceso a la VPN

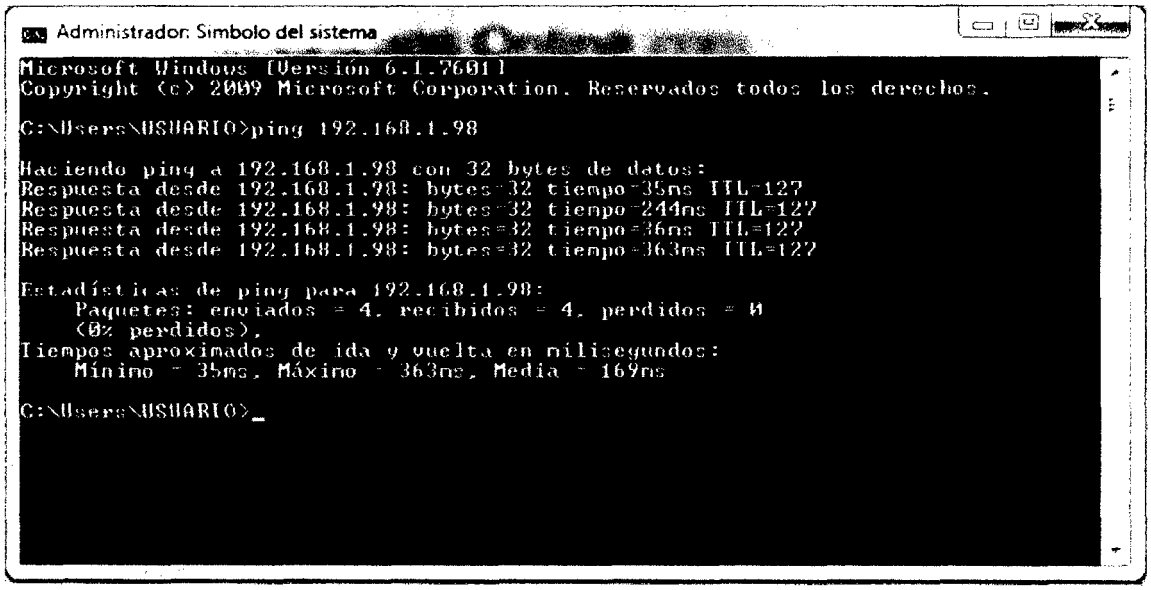


Nos autenticamos con nuestro usuario de prueba y contraseña



- Comprobamos la conexión a la vpn observando el estado de la red y haciendo un test ping al servidor SAP





CONCLUSIONES Y RECOMENDACIONES

6. CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES.

- Debido a las ventajas económicas que ofrecen las Redes Privadas Virtuales se puede concluir que se trata de una excelente tecnología para el acceso remoto, puesto que el uso de una VPN constituye un sustituto indispensable a los métodos tradicionales caros como es la transmisión de datos a través de fibra óptica punto a punto. Además, constituye una buena solución alterna a los métodos de implementación de redes WAN tradicionales.

- La cuestión de la seguridad en una VPN es muy importante. La gran mayoría de las organizaciones podrán ver satisfechas sus necesidades de seguridad con las tecnologías de seguridad existentes, pero siempre será necesario llevar un control estricto de la seguridad y mantener actualizada la VPN con los últimos avances en tecnología.

- Una VPN podrá ser aplicada en todo tipo de entornos, desde las grandes empresas con sucursales en diversas partes del país o del mundo y varios trabajadores móviles hasta las pequeñas empresas que tengan dos o más sucursales en una sola ciudad; así como también las diversas dependencias del gobierno que necesiten intercambiar información entre ellas; e instituciones educativas como universidades y en general cualquiera que necesite acceder a sus archivos desde una ubicación remota de manera segura podrá obtener beneficios con esta tecnología.

- Las VPN permiten brindar servicios a los clientes de la empresa en cualquier lugar del mundo, con lo que los clientes obtendrán la información que el necesita al instante, lo que generará una mayor productividad de la empresa.

6.2. RECOMENDACIONES

- Continuar con el estudio de la tecnología de VPN, ya que es una tecnología que va creciendo y que necesita de una constante actualización de conocimientos debido a las constantes actualizaciones en el software de soporte que se implementan en los sistemas operativos especialmente en Windows.

- Cabe anotar que la metodología expuesta, puede ser no acoplable para determinada situación o empresa, por lo que se recomienda plantear nuevas metodologías de acuerdo a las necesidades particulares que se presenten en cada empresa.

- El único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no está bien definido pueden existir consecuencias serias

- Se deben tener en cuenta los requerimientos mínimos para el servidor en el caso del SO Windows server 2008 es RAM 512, 1GB recomendada procesador P IV o superior y disco duro de 40 GB mínimos.

REVISION BIBLIO GRÁFICA Y LINKOGRÁFICA

7. REVISION BIBLIOGRÁFICA Y LINKOGRÁFICA

7.1. BIBLIOGRAFIA

1. Felipe Castro, G. (2011). Redes de Computadoras.

2. Cangrejo, B., & Albeiro, W. (2014). Implementación de un canal de comunicaciones por medio de VPN (red privada virtual) para las sucursales remotas de la empresa Plexa SA ESP.

3. Bravo, J., & Alberto, C. (2012). Sistemas de Transporte de Datos. Práctica 1: Encaminamiento dinámico con IPv4. *Sistemas de Transporte de Datos*.

4. López Castaño, F. A. (2013). Montaje Servidor Windows Server 2008 R2 y Active Directory.

5. Carrillo Gomero, F. N., & Calderón Alva, A. (2014). Parámetros de Calidad de Servicio en Redes IP. *Electrónica-UNMSM*, (22), 31-39.

6. Atelin, P., & Dordoigne, J. (2006). *Redes informáticas: conceptos fundamentales: normas, arquitectura, modelo OSI, TCP/IP, Ethernet, Wi-Fi...* Ediciones ENI.

7. Comer, D. E. (2007). *Redes de computadoras, Internet e Interredes* (Vol. 2). G. Guerrero (Ed.). Prentice Hall.

8. Comer, D. E., & Soto, H. A. A. (1996). *Redes globales de información con Internet y TCP/IP* (Vol. 1). Prentice hall.

9. Aguirre Hernández, J. A. (2013). Análisis e implementación del firewall forefront TMG 2010.

7.2. LINKOGRAFIA.

1. https://technet.microsoft.com/es-es/library/ee207137.aspx
2. http://en.wikipedia.org/wiki/Microsoft_Forefront_Threat_Management_Gateway
3. http://seguridadit.blogspot.com/2010/02/instalacion-paso-paso-de-forefront-tmg.html
4. https://technet.microsoft.com/es-es/library/dd896981.aspx
5. http://jzel2222.blogspot.com/2008/07/windowstechnologies.html
6. https://technet.microsoft.com/es-es/library/cc771294.aspx
7. https://social.technet.microsoft.com/Forums/es-ES/d77ff7bb-0204-4cfd-94fd-c5160f794793/problema-durante-dcpromo?forum=wsades
8. https://social.technet.microsoft.com/Forums/es-ES/d77ff7bb-0204-4cfd-94fd-c5160f794793/problema-durante-dcpromo?forum=wsades
9. http://windowsespanol.about.com/od/ConoceElnstalaWindows/f/Que-es-Windows-Update.htm
10. http://windows.microsoft.com/es-xl/windows/windows-update
11. http://es.wikipedia.org/wiki/Windows_Server_2008
12. https://technet.microsoft.com/es-es/library/ee207137.aspx
13. http://seguridadit.blogspot.com/2010/02/instalacion-paso-paso-de-forefront-tmg.html
14. https://technet.microsoft.com/es-es/library/dd896981.aspx
15. https://technet.microsoft.com/es-pe/library/cc754923.aspx
16. http://jzel2222.blogspot.com/2008/07/windowstechnologies.html
17. https://technet.microsoft.com/es-es/library/cc771294.aspx
18. https://social.technet.microsoft.com/Forums/es-ES/d77ff7bb-0204-4cfd-94fd-c5160f794793/problema-durante-dcpromo?forum=wsades
19. http://windowsespanol.about.com/od/ConoceElnstalaWindows/f/Que-es-Windows-Update.htm
20. http://windows.microsoft.com/es-xl/windows/windows-update
21. https://technet.microsoft.com/es-es/library/dd896975.aspx
22. https://technet.microsoft.com/es-es/library/dd440984.aspx

ANEXOS

ANEXOS

CARTA DE CONFORMIDAD DEL FUNCIONAMIENTO DE LA VPN

TERRA

SERVICIO DIARIO DE CARGA DE LIMA A:
CHICLAYO - PIURA - SULLANA - TUMBES - AGUAS VERDES - PUERTO MALDONADO
GUAYAQUIL - QUITO - CUENCA (ECUADOR)
IPIALES - MEDELLÍN - CALI - BOGOTÁ - BUCARAMANGA - CÚCUTA (COLOMBIA)
LA PAZ - BOLIVIA

Lima, 2 Agosto del 2015

Srs : Gino Vieyra Dioses – Manuel Díaz Llatance

Asunto : Carta de Conformidad

Por medio de la presente los saludo y hago de su conocimiento que la empresa de transportes Terracargo SAC a la cual represento, está conforme con el servicio de diseño e implementación de una red privada virtual (VPN) que Uds. han realizado en nuestras instalaciones.

Asimismo, le comunico que el trabajo realizado por Uds. estuvo acorde con nuestras expectativas, confirmándoles que la red ya instalada funciona en forma normal.

Agradeciendo su atención y servicio, me despido reiterando nuestra conformidad con el trabajo realizado y esperando mantener nuestra relación laboral.

Atentamente

Manuel Terranova Panta.
Gerénte General Terracargo SAC.

CONFIGURACIONES.

1. INSTALAR WINDOWS SERVER 2008 R2

Para determinar qué sistema operativo vamos a utilizar se han tenido que tener en cuenta varios factores:

- La infraestructura actual de hardware.
- La infraestructura software con la que cuenta la organización.
- Los servicios ya implementados en la organización.

La entidad tiene licenciamiento de Microsoft Windows Server 2008 y 2012, pero por cuestiones de estandarización con los servidores que ya están en producción y usan Windows server 2008, es por lo que se ha decidido que utilizaremos Windows server 2008 R2, también se tuvo que decidir por la versión R2 debido a que FOREFRONT TMG lo requiere para su instalación.

Después de haber realizado una comparación entre las diferentes versiones de sistemas operativos para servidores en la familia de sistemas operativos de Microsoft y las diferentes tecnologías con las que cuentan cada uno de ellos, es que hemos decidido que solo utilizaremos un solo servicio; hemos determinado que para este proyecto que es el servicio de VPN con el software FOREFRONT TMG que actualmente reemplazó la versión anterior llamada ISA SERVER, por lo antes mencionado utilizaremos la edición de Windows server 2008 R2 Standard.

INSTALAR SISTEMA OPERATIVO PARA SERVIDORES WINDOWS SERVER 2008 R2 EN LOS 2 SERVIDORES QUE UTILIZAREMOS PARA ACTIVE DIRECTORY Y PARA FOREFRONT TMG

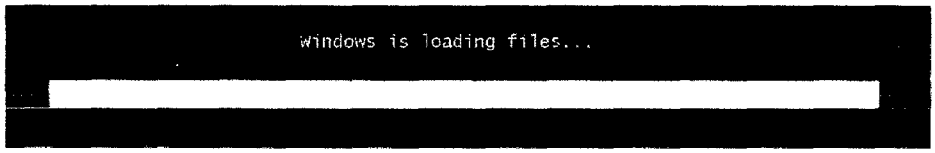
Cabe mencionar que después de haber realizado el estudio para determinar el hardware para los dos servidores, la misma organización financiará los costos, se tendrá que adquirir en el mercado de servidores cotizando en las mejores marcas para adquirirlo.

Luego de adquirir el producto haremos las pruebas de su correcto funcionamiento para poder empezar a trabajar en la instalación y puesta en marcha los servicios planteados, prepararemos e instalaremos los sistemas operativos y las aplicaciones necesarias para lograr nuestros objetivos según las siguientes funciones:

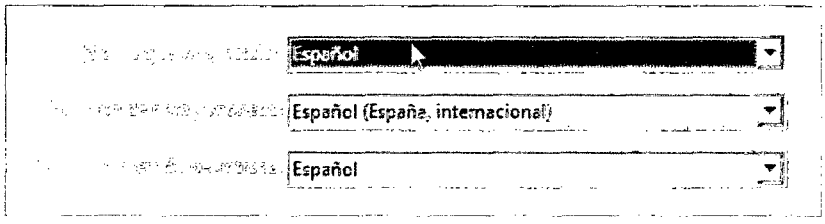
	SISTEMA OPERATIVO	APLICACIÓN/ SERVICIO
SERVIDOR 1	Windows Server 2008 R2	Active Directory/ Domain Controller, DNS
SERVIDOR 2	Windows Server 2008 R2	Forefront TMG/ VPN

Como ya hemos determinado que sistema operativo y en que servidores, descargaremos desde la plataforma de Microsoft la imagen ISO del sistema operativo para luego grabarlo en un DVD en blanco y tenerlo preparado para la instalación. Empezaremos en la explicación de la instalación de nuestro sistema operativo para servidores:

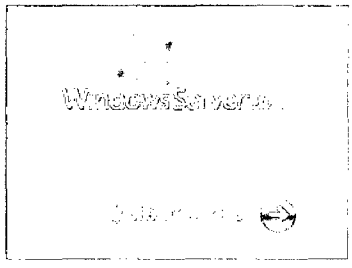
A. Haremos cargar desde una lectora de DVD el Disco de Windows Server 2008 R2 y esperar que carguen los archivos de instalación:



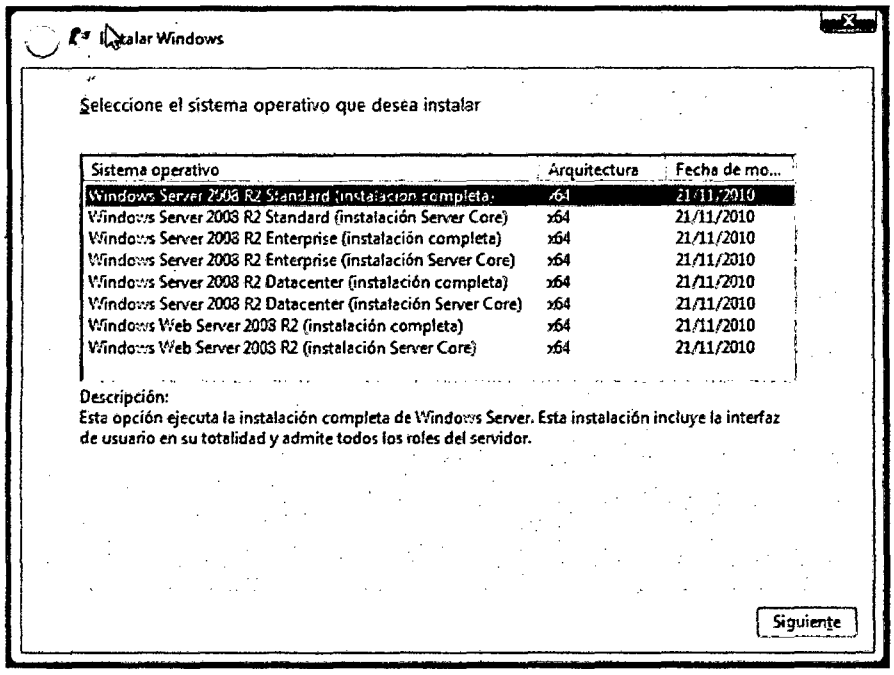
B. Seleccionamos idiomas de instalación (Idioma del sistema operativo, formato de hora y moneda, e idioma del teclado), según nuestro proveedor nos lo haya proporcionado.



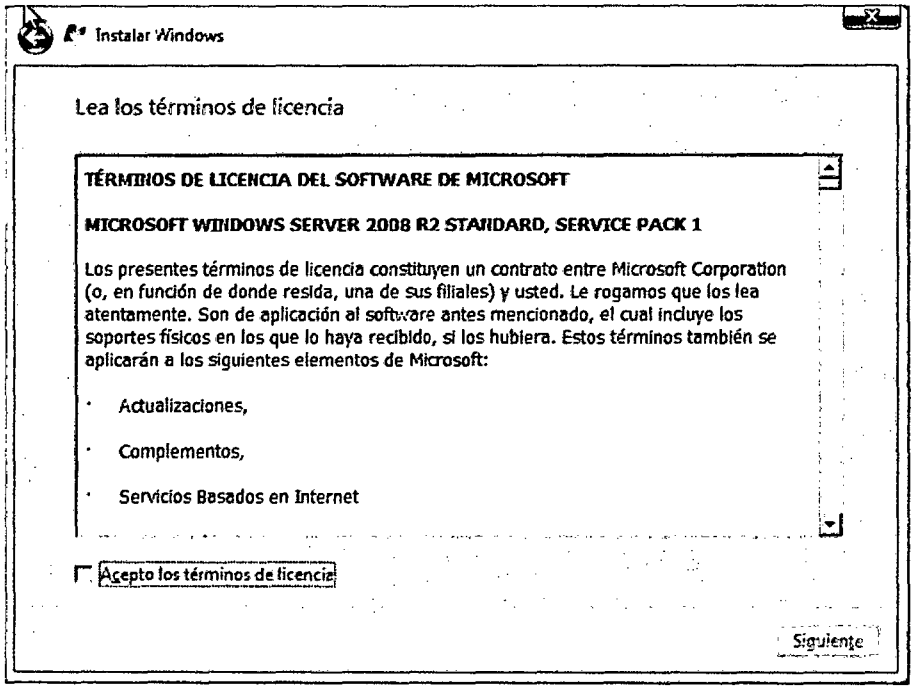
C. Seleccionamos el Botón "Instalar ahora", para comenzar una instalación limpia desde cero, en caso tengamos un server que no arranca el sistema operativo, seleccionamos "Reparar equipo", pero no es nuestro caso.



D. Seleccionamos la edición del sistema operativo que queremos instalar según nuestro hardware permitido y necesario para lo que necesitamos instalar (SERVER1: Active Directory y DNS; SERVER 2: Forefront TMG). Solo necesitamos la edición STANDARD, por su no muy compleja funcionalidad y que aceptan como mínimo el hardware y software que hemos adquirido y vamos a utilizar.

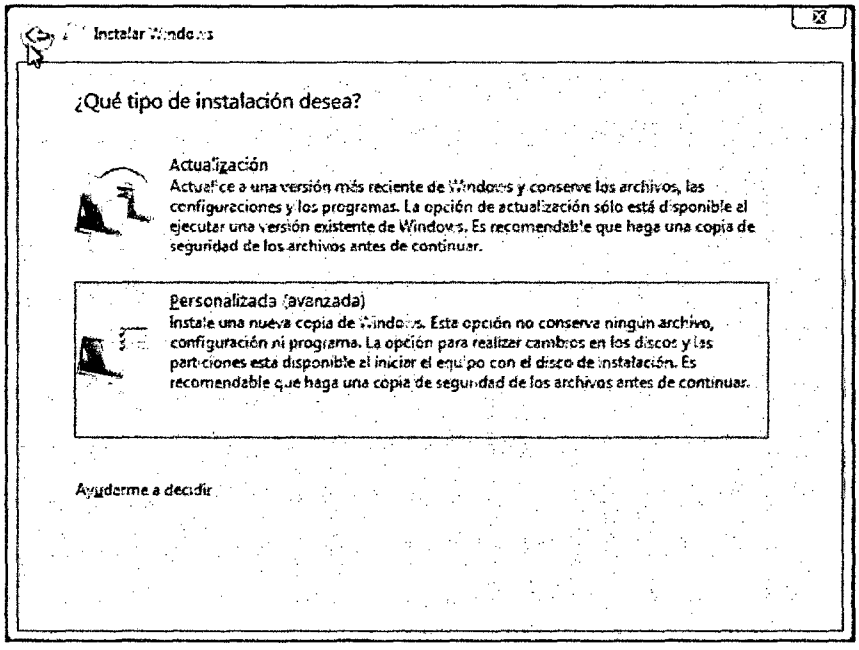


E. Aceptamos los términos y condiciones de la licencia que nos plantea Microsoft para poder usar este sistema operativo, por ello es necesario que leamos detenidamente todos los términos que coloca Microsoft para estar informado a que nos sometemos.

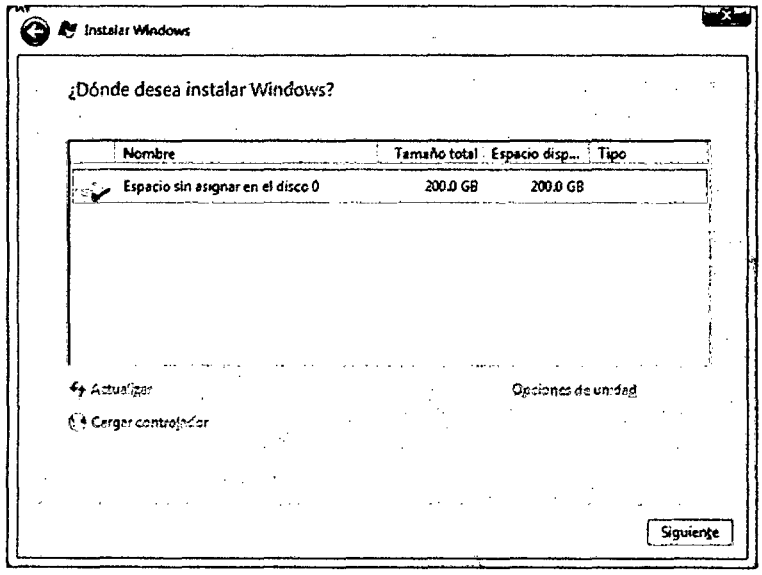


F. Seleccionamos el tipo de instalación que vamos a realizar: ACTUALIZACIÓN: este opción se refiere cuando ya tenemos una versión anterior de Windows server 2008 y la queremos actualizar a la versión ya mencionada, y PERZONALIZADA: Se refiere a una instalación limpia desde cero o queremos instalar otro sistema operativo en otro disco duro:

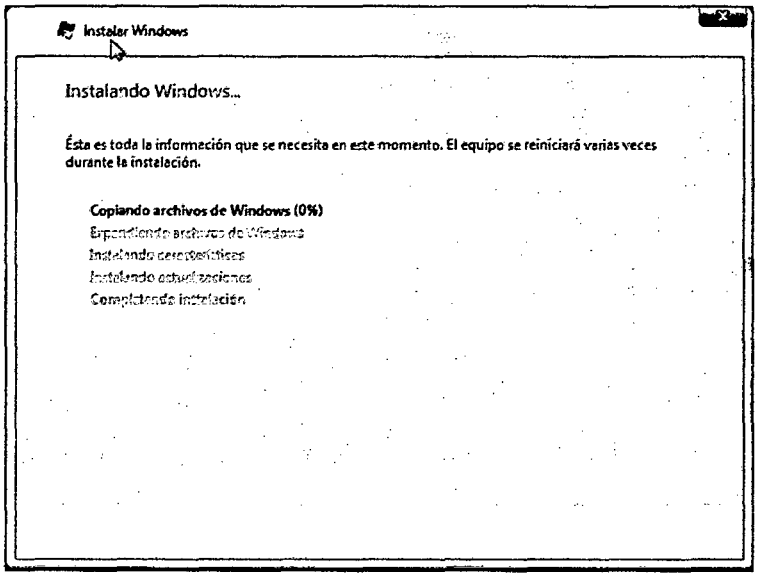
En nuestro caso es una instalación de CERO, por lo cual seleccionaremos "Personalizada".



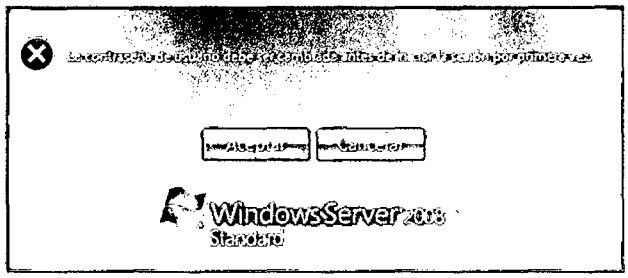
G. Seleccionamos la partición que ya estuviese creada, y en el caso que queramos varias particiones para distribuir por separado los datos que se van a guardar en otra partición por ejemplo los Backup, registros, Forefront, etc., creamos una partición (en Opciones de Unidad) de la capacidad mínima permitida para Windows Server 2008 R2 de 40 GB, o superior, es recomendable mayor a 100 Gb debido a los roles que se van a instalar en nuestro servidor, y las otras particiones de acuerdo como las queramos.



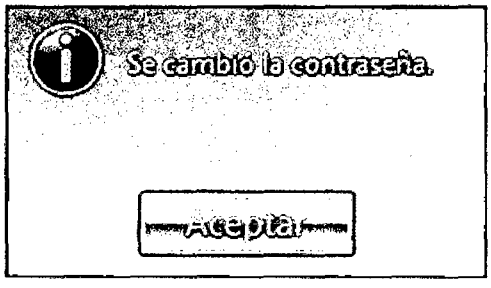
H. Esperamos que el software de instalación haga su trabajo (copie los archivos de instalación al disco duro e instale todas las características del sistema operativo).

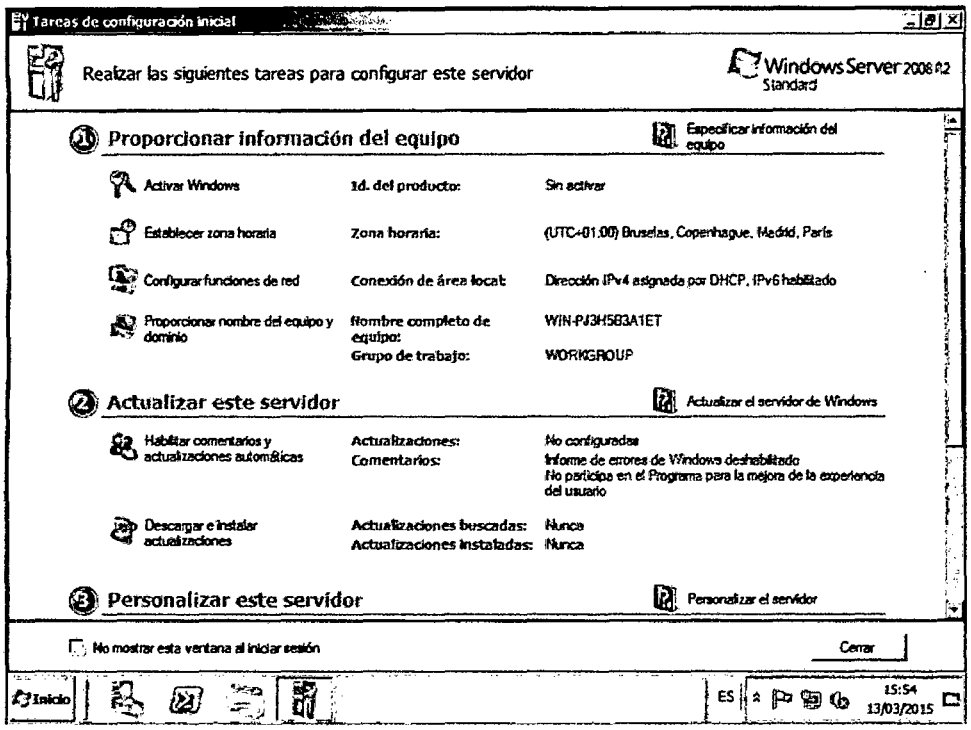


I. La primera pantalla después de instalar el sistema operativo nos sale un error (damos clic en ACEPTAR):

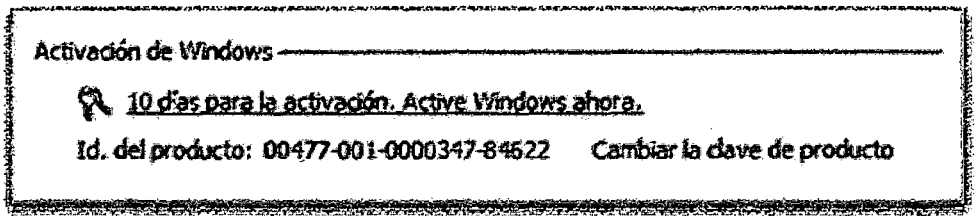


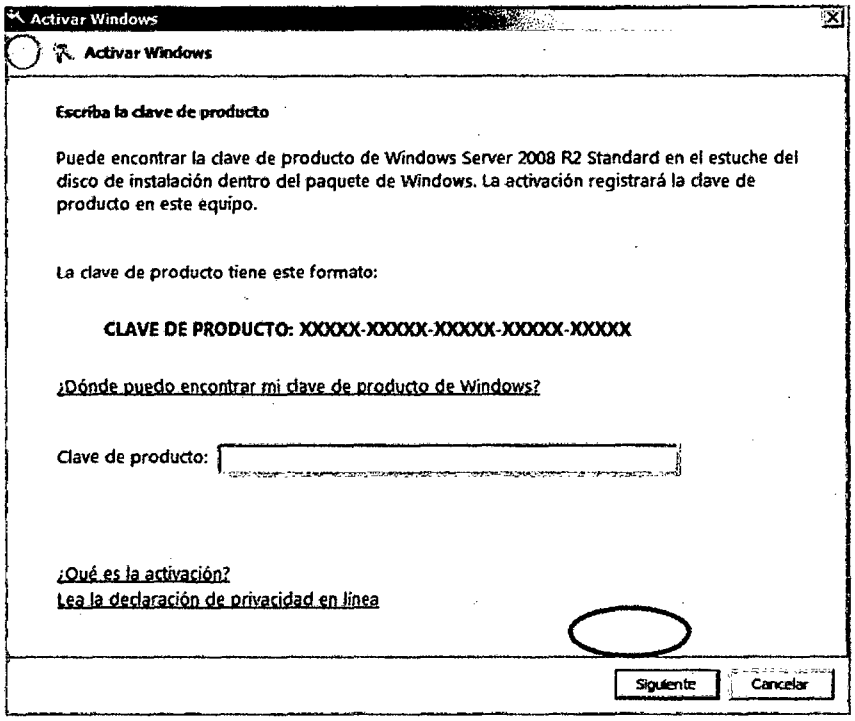
J. Cambiamos la contraseña y la confirmamos.





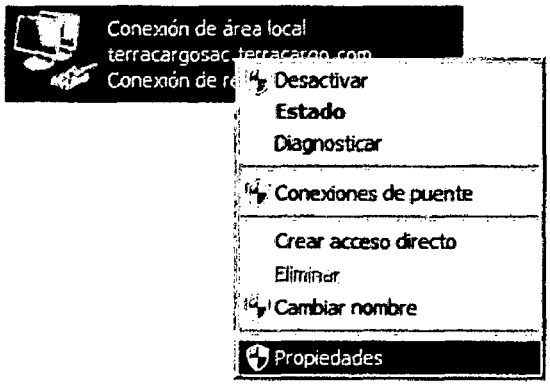
K. Luego damos clic derecho en EQUIPO (en el menú INICIO) y seleccionamos la opción PROPIEDADES para activar el Sistema Operativo. Seleccionamos la opción CAMBIAR CLAVE DEL PRODUCTO e ingresamos la clave de nuestro Windows para activarlo y seleccionamos la opción SIGUIENTE y automáticamente se actica nuestro WINDOWS SERVER 2008 R2.

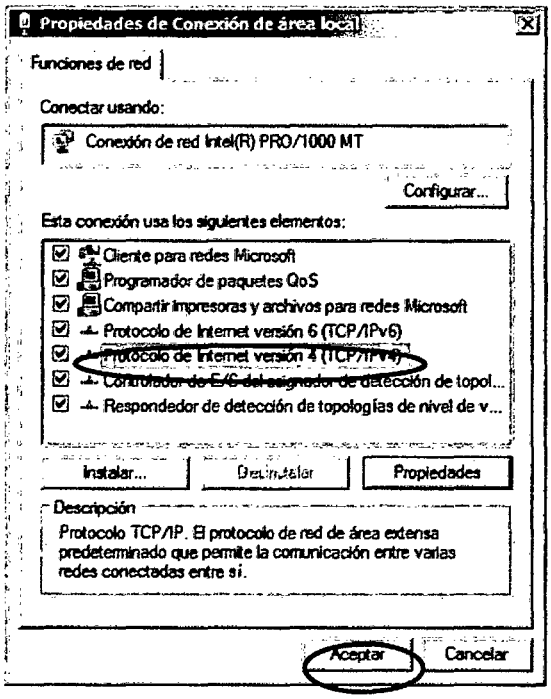


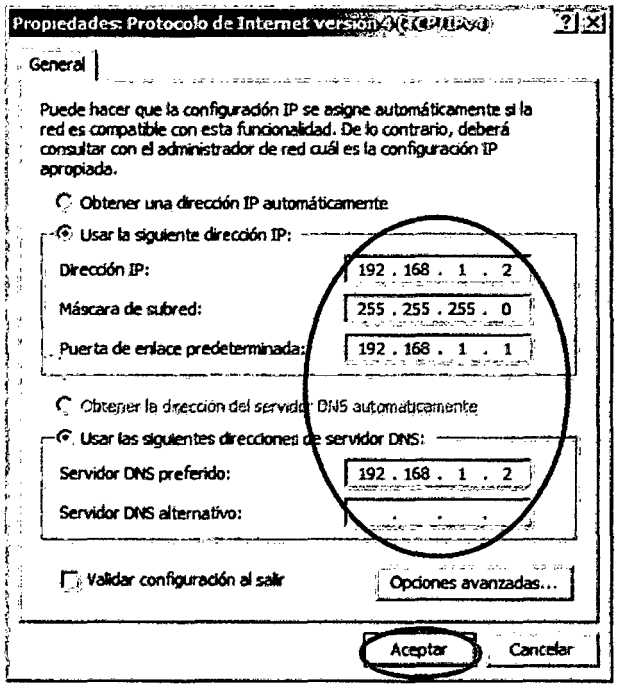


2. CONFIGURAR SERVIDOR - ACTIVE DIRECTORY

A. El primer paso en nuestro servidor es configurar nuestro adaptador de red con las direcciones IP según la topología gráfica, y "Cambiamos la configuración del adaptador" accediendo a la aplicación de "Centro de Redes y recursos compartidos" ubicada en "Panel de control", según muestra la configuración en "Propiedades: Protocolo de Internet versión 4 (TCP/IPv4):

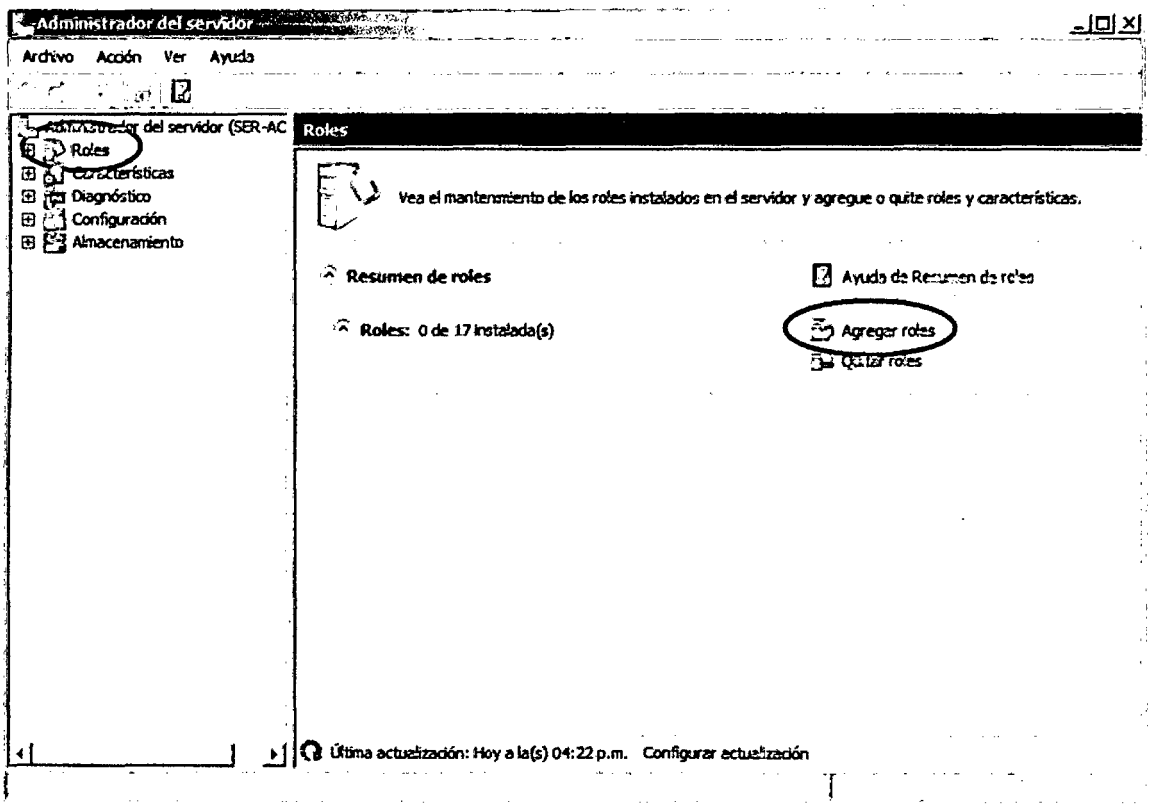

Conexión de área local
Desactivar
Estado
Diagnosticar
Conexiones de puente
Crear acceso directo
Eliminar
Cambiar nombre
Propiedades


Propiedades de Conexión de área local
Funciones de red
Conectar usando:
Conexión de red Intel(R) PRO/1000 MT
Configurar...
Esta conexión usa los siguientes elementos:
Cliente para redes Microsoft
Programador de paquetes QoS
Compartir impresoras y archivos para redes Microsoft
Protocolo de Internet versión 6 (TCP/IPv6)
Protocolo de Internet versión 4 (TCP/IPv4)
Respondedor de detección de topologías de nivel de v...
Instalar...
Propiedades
Descripción
Protocolo TCP/IP. El protocolo de red de área extensa predeterminado que permite la comunicación entre varias redes conectadas entre sí.
Aceptar
Cancelar



B. Instalado ya el Sistema Operativo Windows server 2008 R2 en ambos servidores, en uno de ellos procedemos a Agregar ROLES DE SERVIDOR (Active Directory), para poder administrar cuentas de usuarios para el acceso VPN,

C. Para instalar los Roles de Active Directory y DNS tenemos que abrir la aplicación: "Administrador del Servidor", en la sección ROLES seleccionamos la opción: "Agregar Roles":

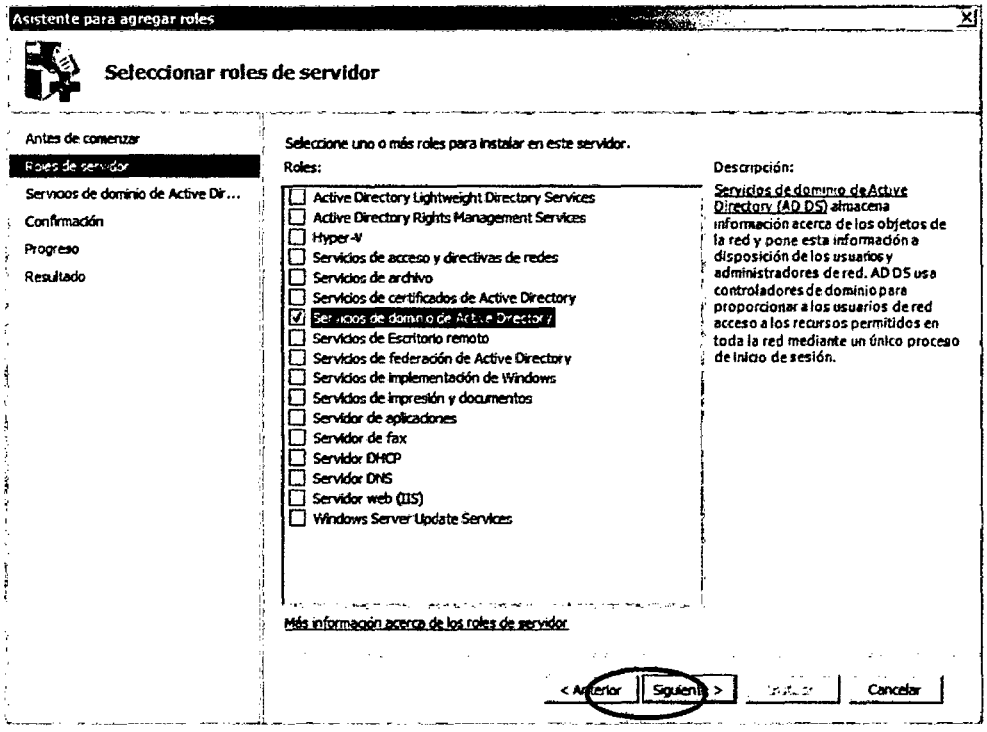


Una vez abierto nuestro asistente para agregar roles, nos haces unas indicaciones previas para agregar los roles a nuestro servidor; seleccionamos "Siguiente". Y luego nos aparecerá la siguiente ventana en la cual nos indica todos los roles disponibles en Windows Server 2008 R2 Standard. Lo que seleccionaremos para este servidor es:

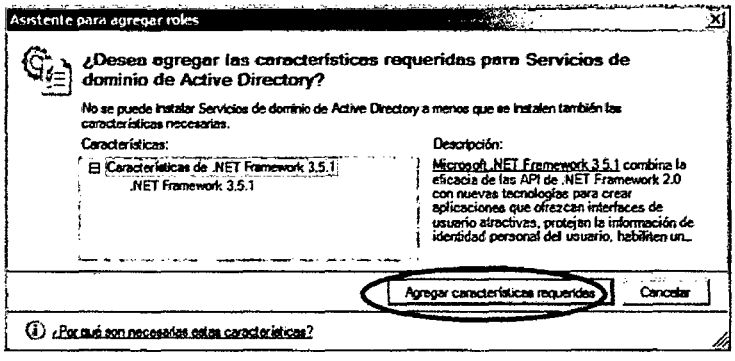
- ✓ Servicios de dominio de Active Directory.
- ✓ Servidor DNS.

La instalación de estos servicios tienen un orden de instalación para poder configurarlo adecuadamente para que no tengamos errores y volvamos a pasos anteriores: **Primero:** ACTIVE DIRECTORY, **Segundo:** DNS

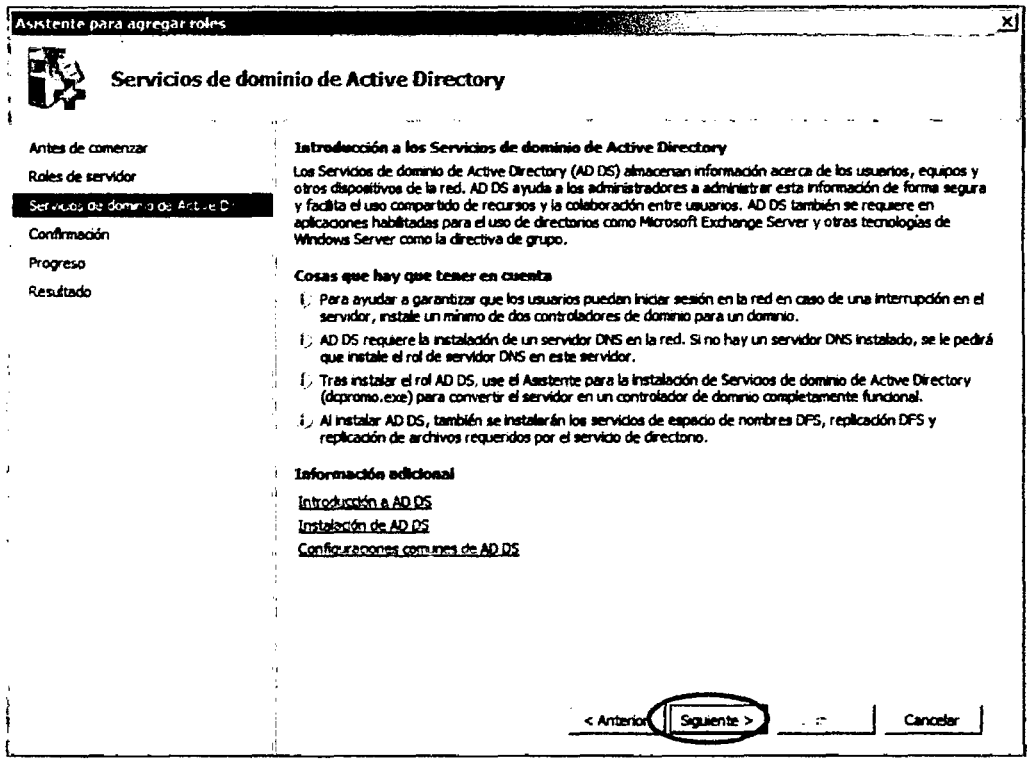
A) ACTIVE DIRECTORY

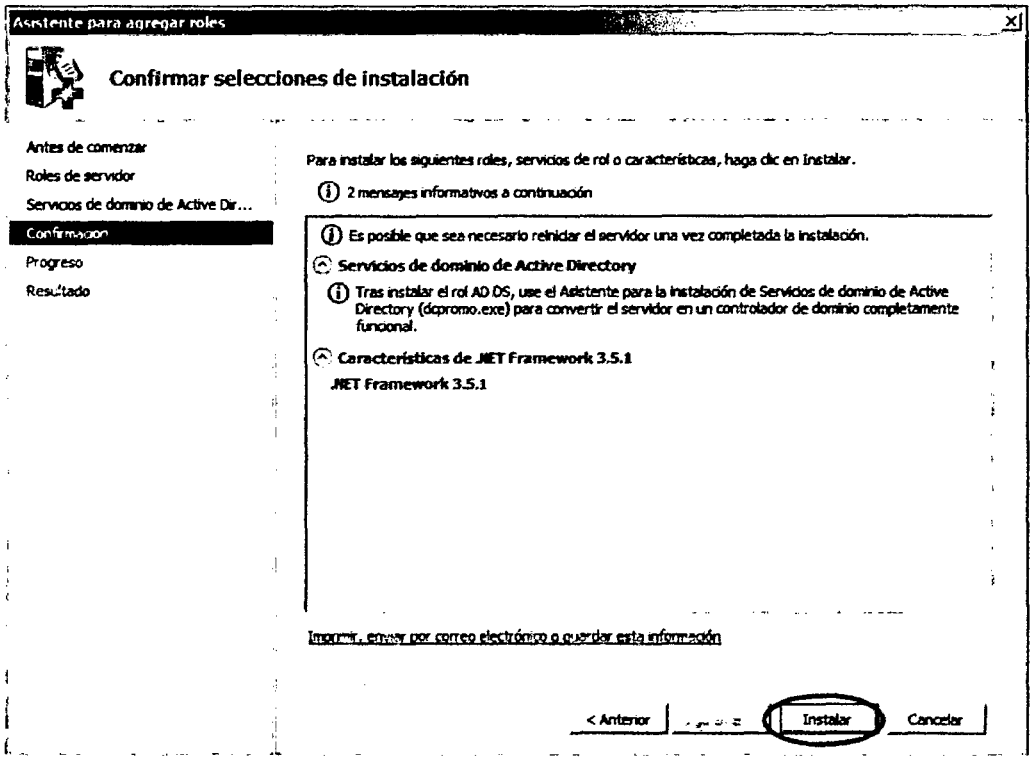


Para poder agregar este servicio se requiere algunas características, en lo cual el asistente de instalación nos indicará y seleccionamos el botón: "Agregar características requeridas".

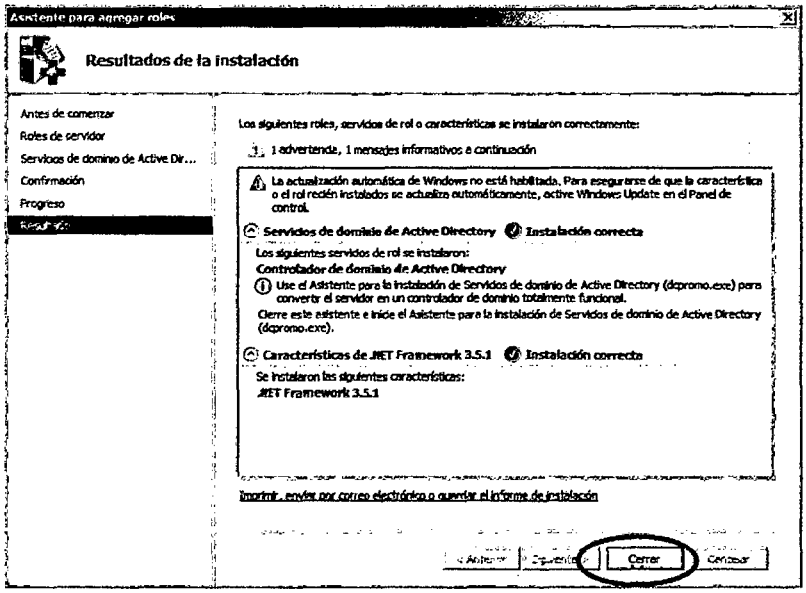


Luego nos aparecerá dos ventanas en las que nos indica algunas cosas previas que deberíamos saber según Microsoft sobre ACTIVE DIRECTORY; presionamos en el botón "Siguiente", y la otra ventana que es la confirmación de la instalación del servicio; presionamos en el Botón "Instalar". Posteriormente esperamos que se Agreguen las características requeridas por el servicio de Active Directory


Asistente para agregar roles
Servicios de dominio de Active Directory
Antes de comenzar
Roles de servidor
Servicios de dominio de Active D...
Confirmación
Progreso
Resultado
Introducción a los Servicios de dominio de Active Directory
Los Servicios de dominio de Active Directory (AD DS) almacenan información acerca de los usuarios, equipos y otros dispositivos de la red. AD DS ayuda a los administradores a administrar esta información de forma segura y facilita el uso compartido de recursos y la colaboración entre usuarios. AD DS también se requiere en aplicaciones habilitadas para el uso de directorios como Microsoft Exchange Server y otras tecnologías de Windows Server como la directiva de grupo.
Cosas que hay que tener en cuenta
Para ayudar a garantizar que los usuarios puedan iniciar sesión en la red en caso de una interrupción en el servidor, instale un mínimo de dos controladores de dominio para un dominio.
AD DS requiere la instalación de un servidor DNS en la red. Si no hay un servidor DNS instalado, se le pedirá que instale el rol de servidor DNS en este servidor.
Tras instalar el rol AD DS, use el Asistente para la instalación de Servicios de dominio de Active Directory (dcpromo.exe) para convertir el servidor en un controlador de dominio completamente funcional.
Al instalar AD DS, también se instalarán los servicios de espacio de nombres DFS, replicación DFS y replicación de archivos requeridos por el servicio de directorio.
Información adicional
Introducción a AD DS
Instalación de AD DS
Configuraciones comunes de AD DS
< Anterior
Siguiente >
Cancelar

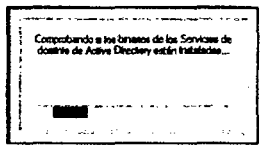

Asistente para agregar roles
Confirmar selecciones de instalación
Antes de comenzar
Roles de servidor
Servicios de dominio de Active Dir...
Confirmación
Progreso
Resultado
Para instalar los siguientes roles, servicios de rol o características, haga clic en Instalar.
2 mensajes informativos a continuación
Es posible que sea necesario reiniciar el servidor una vez completada la instalación.
Servicios de dominio de Active Directory
Tras instalar el rol AD DS, use el Asistente para la instalación de Servicios de dominio de Active Directory (dcpromo.exe) para convertir el servidor en un controlador de dominio completamente funcional.
Características de .NET Framework 3.5.1
.NET Framework 3.5.1
Imprimir, enviar por correo electrónico o guardar esta información
< Anterior
Instalar
Cancelar

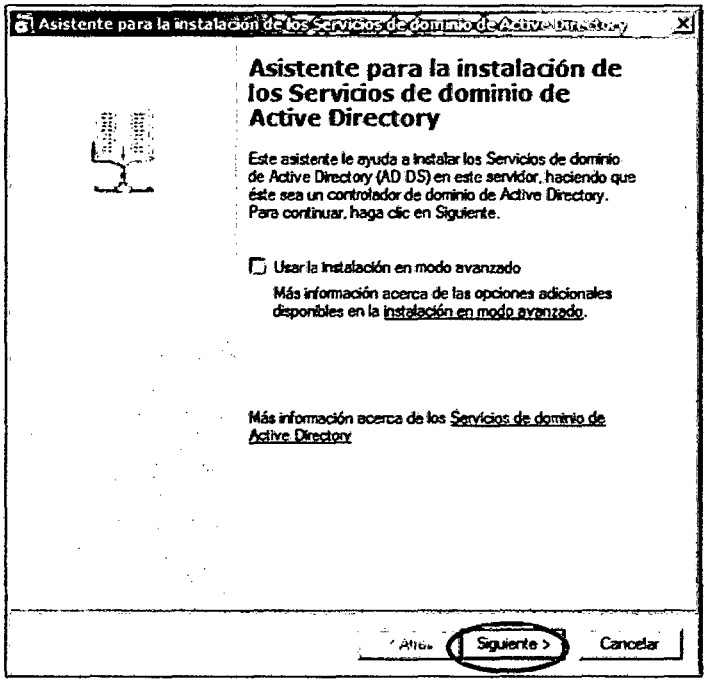
Y Finalmente seleccionaremos el Botón "Cerrar", ya que en esta ventana nos mostrará un reporte los servicios y características instalados correctamente o con errores para poder corregirlos y proseguir con las configuraciones correspondientes al Active Directory.



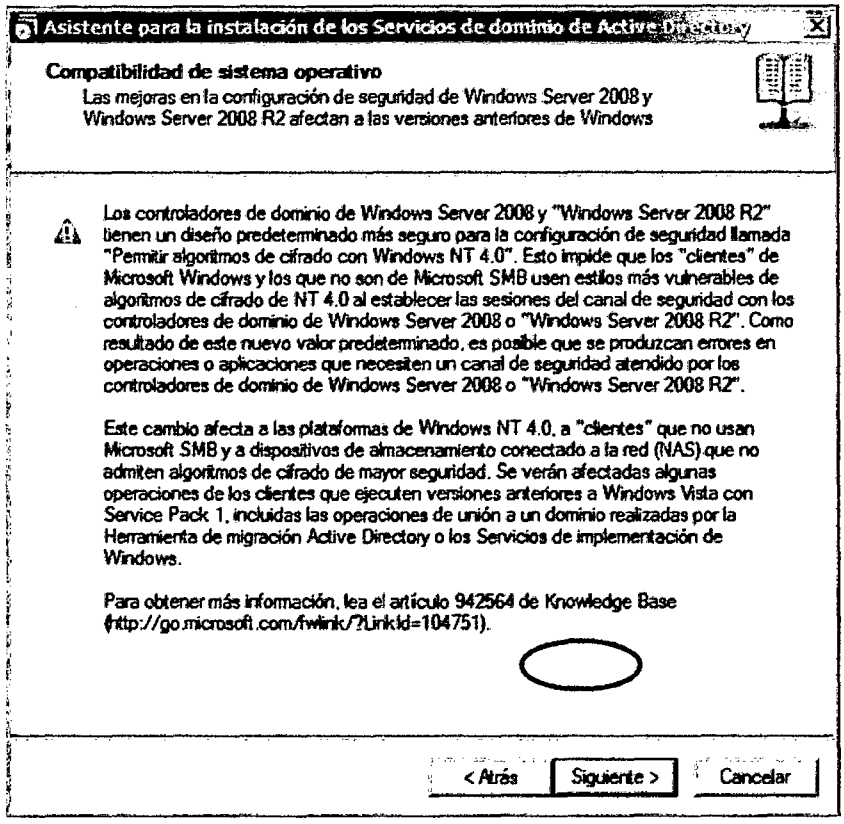
B) DNS

Una vez instalado el Servicio de dominio de Active Directory, usaremos la aplicación llamada "Asistente para la instalación de los servicios de dominio de Active Directory", para ello abrimos la aplicación de Windows "EJECUTAR" y escribimos "dcpromo.exe"



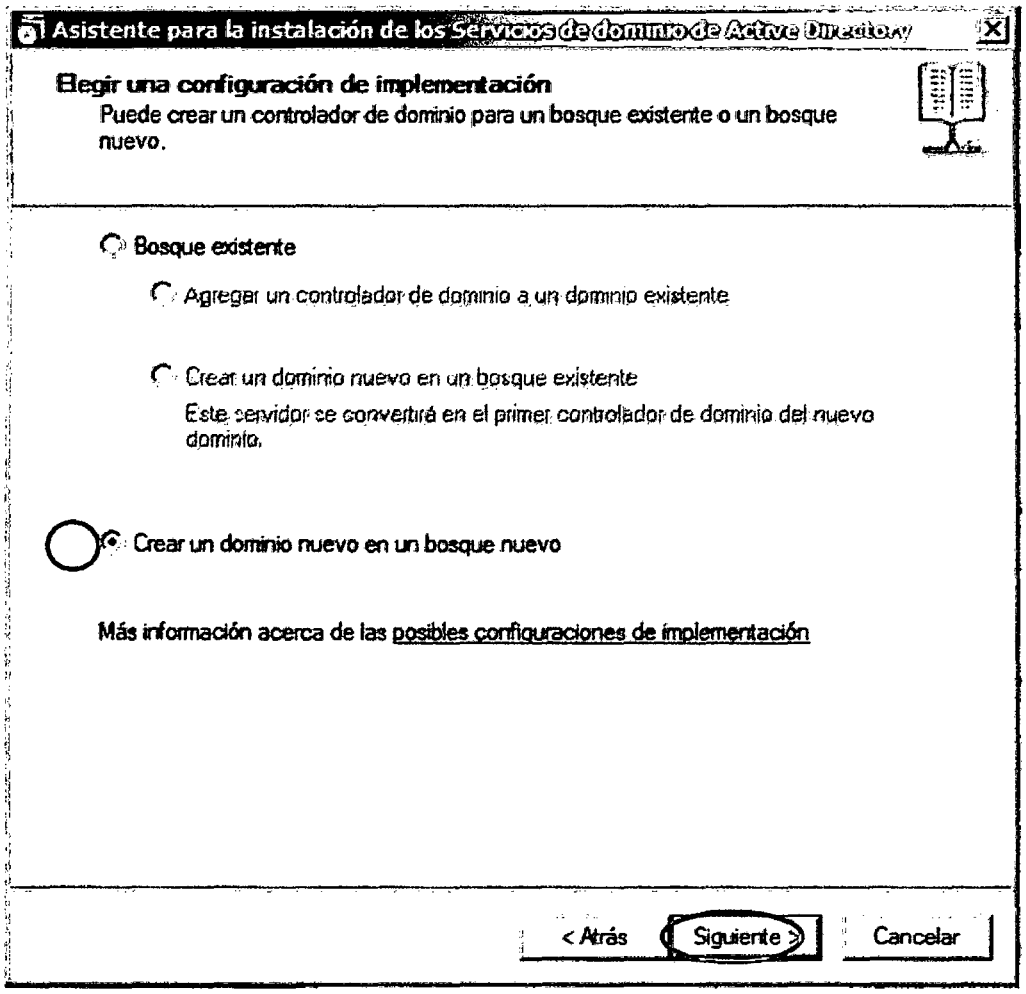


En la siguiente ventana Microsoft no hará una breve explicación que debemos tener encuentra cuando usamos su producto Windows Server 2008 y Windows server 2008 R2, sobre las mejoras en la configuración de seguridad de éste y que afectan a las versiones anteriores de Windows, después de tener conocimiento de lo mencionado seleccionamos la opción "siguiente".

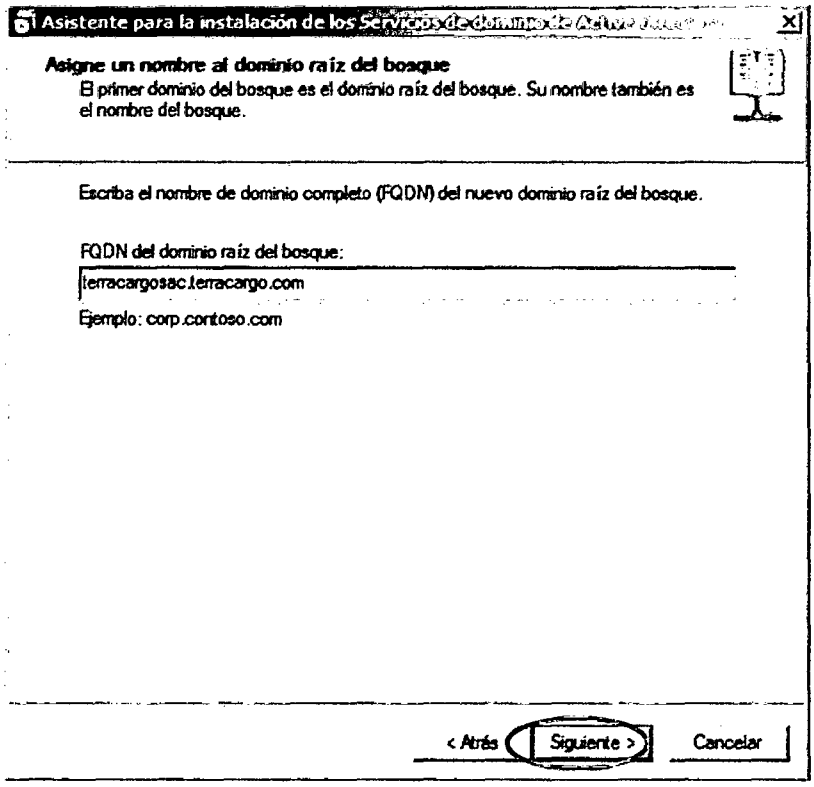


Crearemos un dominio en un bosque de dominios nuevo, ya que no tenemos ningún bosque en nuestra red, pero para entender un poco sobre el manejo de la estructura del Active Directory,

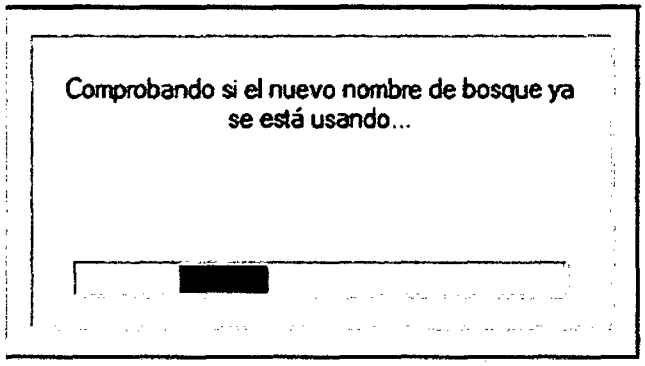
Para hacer lo antes mencionado seleccionamos la opción "Crear un dominio nuevo en un bosque nuevo", y luego en la opción "Siguiente"

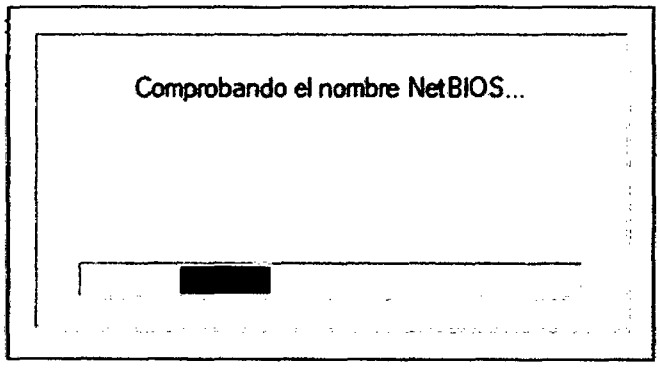


Colocamos nombre de nuestro dominio raíz del bosque: **terracargosac.terracargo.com**

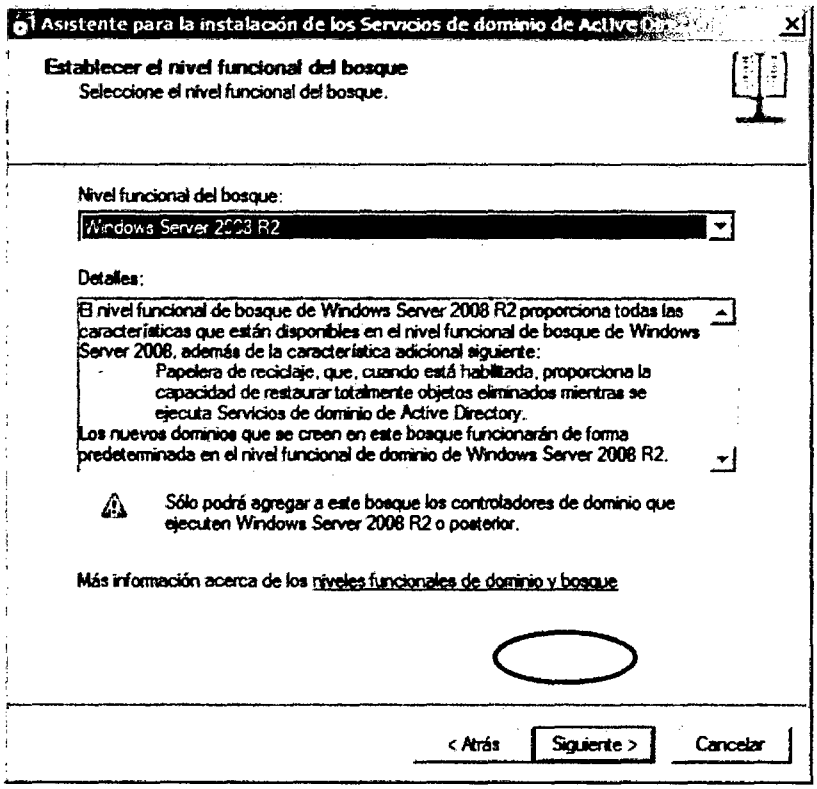


Luego el asistente automáticamente verificará que no exista duplicado del nombre de bosque en la red para evitar conflictos, y la comprobación del nombre NetBIOS en el nombre del dominio

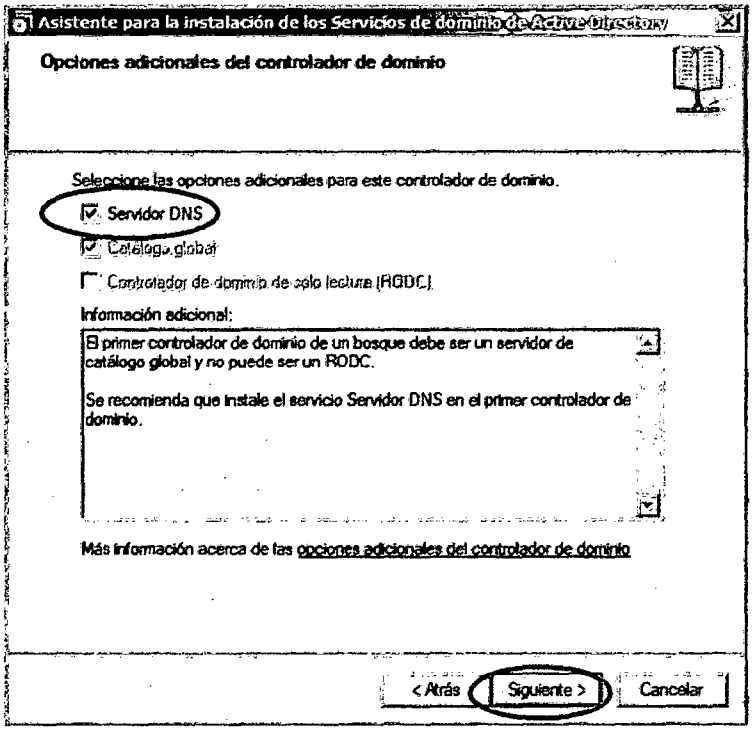


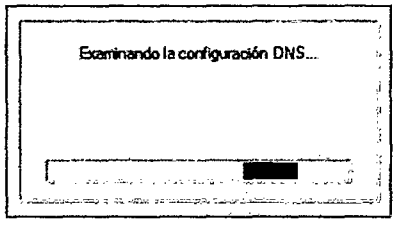


La funcionalidad proporciona una forma de habilitar características para todo el dominio o características de Active Directory para todo el bosque en su entorno de red. Hay disponibles varios niveles de funcionalidad del dominio y funcionalidad del bosque, dependiendo de su entorno de red. Seleccionamos el nivel funcional del bosque; WINDOWS SERVER 2008 R2 para estandarizar todos nuestros servidores y no tener problemas a futuro.



Instalar el Servidor DNS como opción adicional y necesaria para nuestro servidor de Active Directory, como se muestra en la siguiente ventana marcado por defecto:

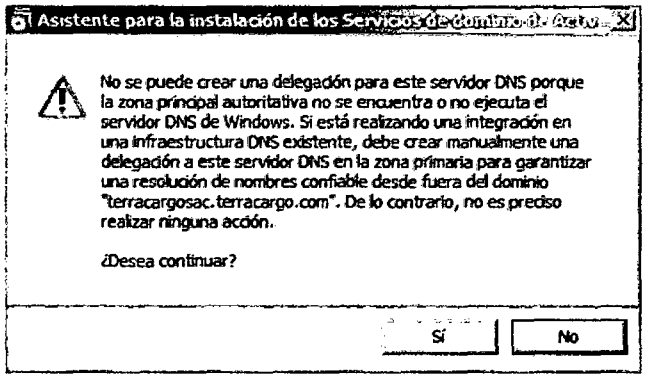




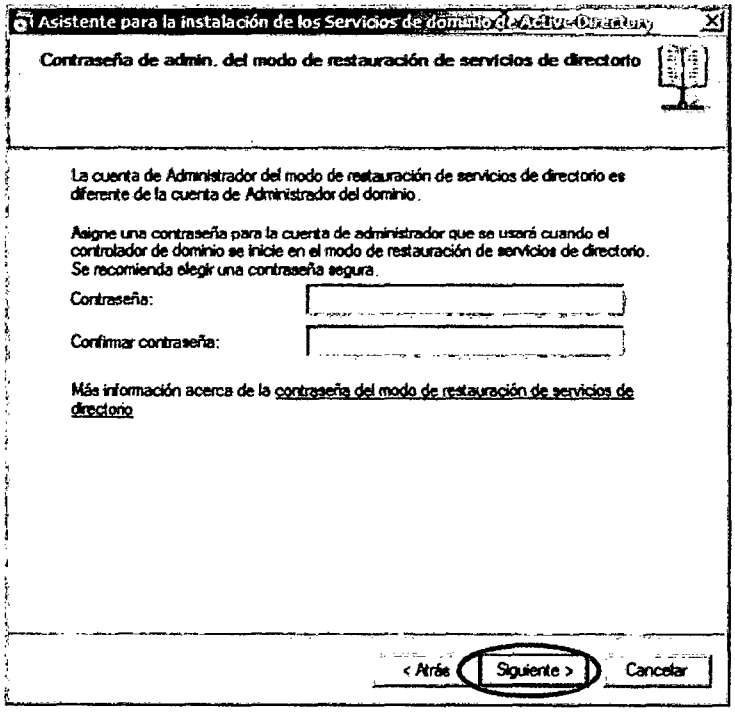
Luego de analizar la configuración de algún otro servidor DNS en la red principal y la configuración predeterminada de nuestro servidor

nos saldrá una advertencia que sólo está avisando que no puede crear la delegación de dominio en un DNS superior.

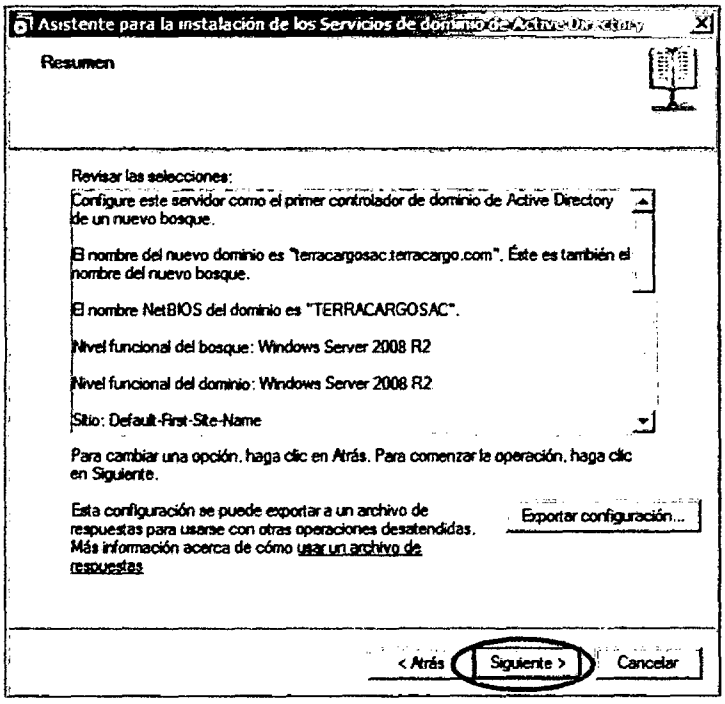
Y como dice el mensaje, salvo que ya tengas una estructura de DNS existente, y tu AD sea un subdominio de uno que ya tienes, no hay que crear delegación (y menos si es un dominio de Internet), como es un dominio nuevo y no un subdominio damos clic en "SI" para continuar con la instalación.

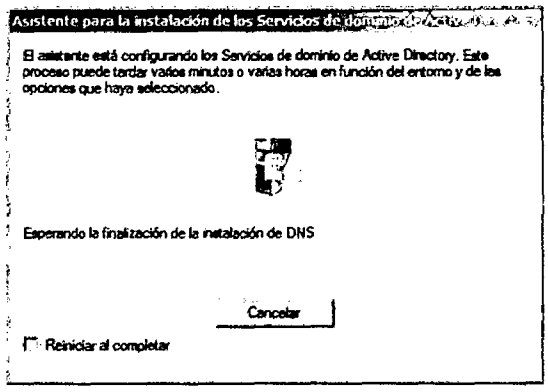


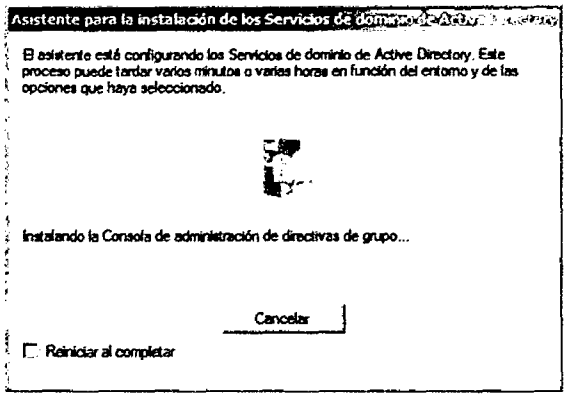
Crear una contraseña segura que lleve letras mayúsculas y minúsculas, números y símbolos.



Finalmente se muestra un resumen de las configuraciones que hemos realizado para proceder con la instalación de nuestro servicio de Active Directory.

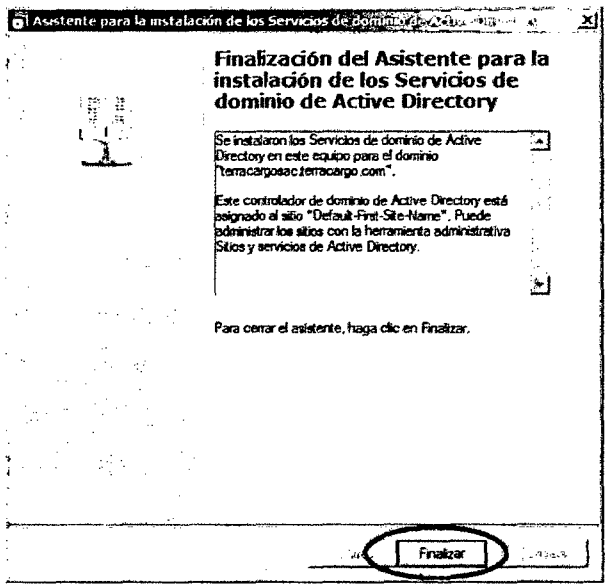






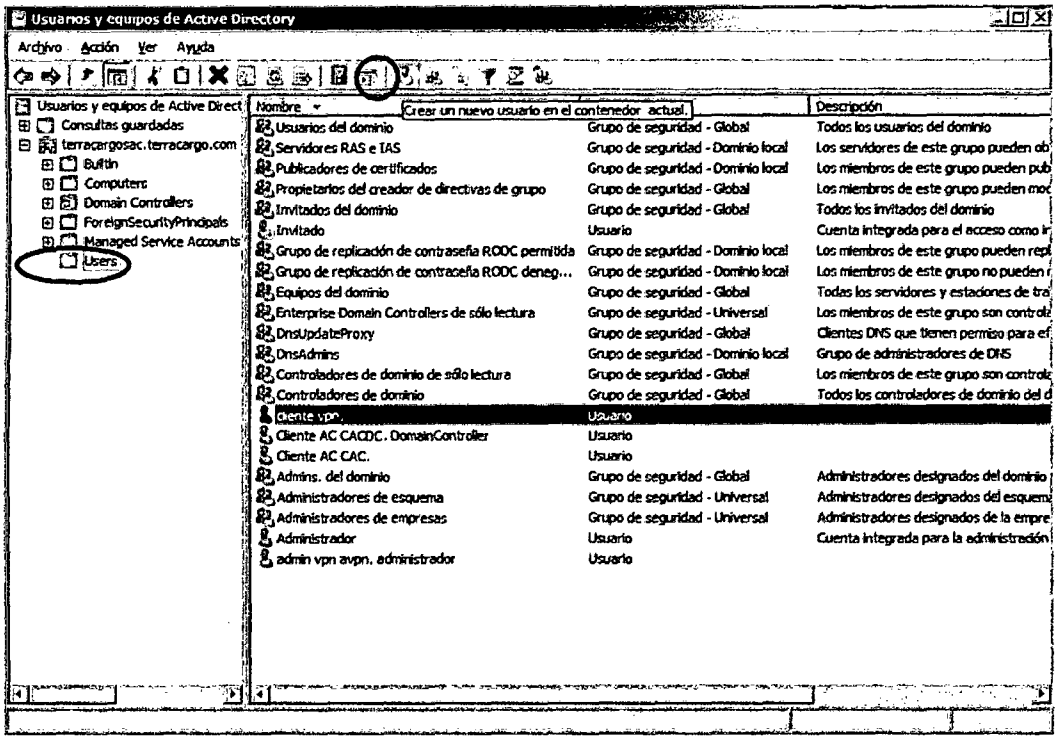
En la siguiente ventana muestra el informe de la instalación sin ningún error debido a la buena configuración que seleccionamos anteriormente de dominio "terracargosac.terracargo.com".

Después pedirá reiniciar para que los cambios realizados sufran efecto en nuestro servidor, lo cual aceptaremos.

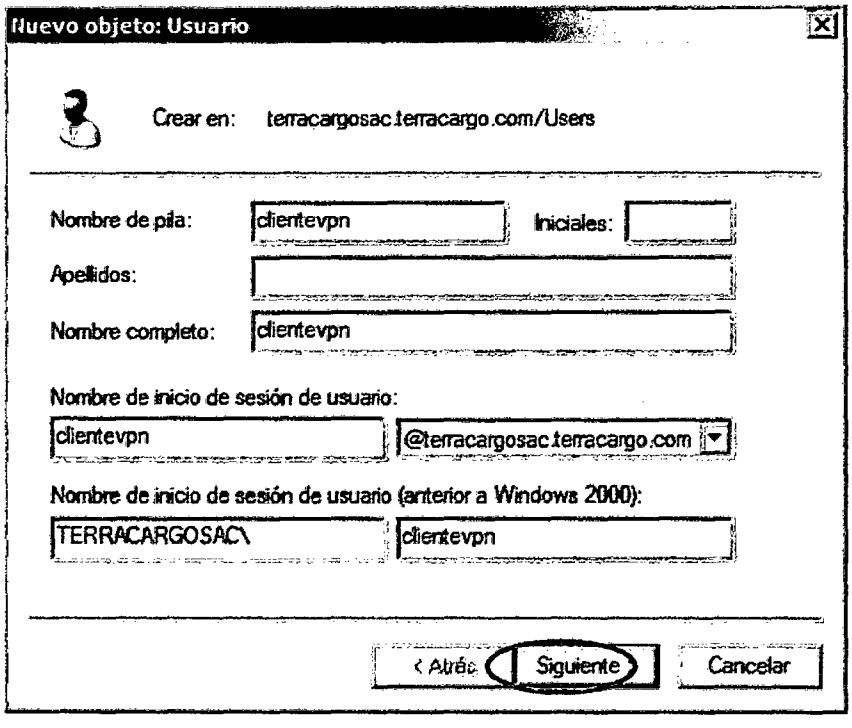


Para crear Usuarios del Dominio abrimos la aplicación de Windows Server llamada "Usuarios y equipos de active directory", en la siguiente ubicación:

"INICIO/HERRAMIENTAS ADMINISTRATIVAS/ Usuarios y equipos de active Directory"
Seleccionamos en la unidad organizativa "USERS", luego damos clic en el ícono que se muestra en la imagen para Crear nuevo usuario

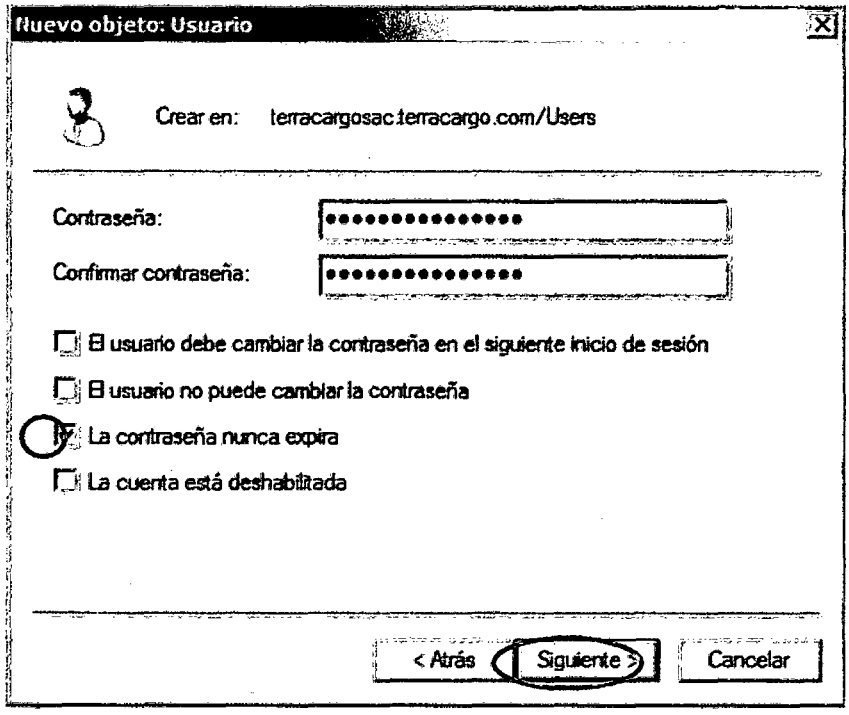


Llenamos todos los datos de nuestros clientes VPN de acuerdo a cada sucursal.

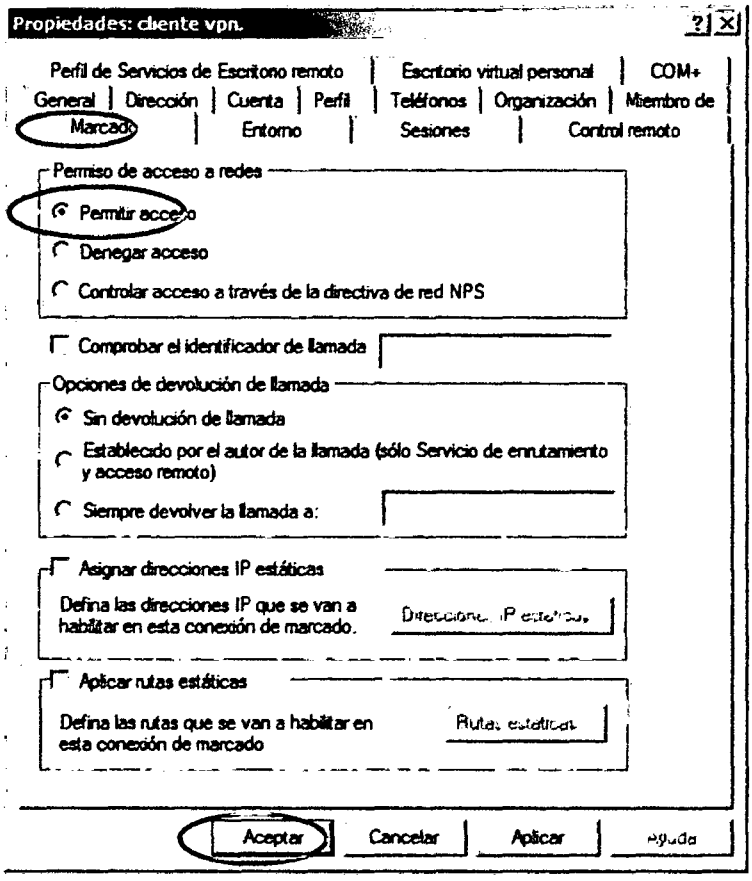


Colocamos una contraseña robusta que contenga letras en mayúsculas y minúsculas, números y caracteres, también deshabilitamos todas las opciones y solo dejamos habilitado opción "La contraseña nunca expira"; luego presionamos el botón "siguiente".

Y en la siguiente ventana mostrará un resumen de la cuenta creada; luego seleccionamos "finalizar" para crear el nuevo usuario y así crearemos un cliente VPN para cada sucursal de la organización.



Y para finalizar la configuración de nuestro usuario del dominio, habilitaremos el permiso para acceso a otras redes (VPN), damos doble clic en el "usuario vpn" de cada sucursal creado y nos saldrá la ventana de propiedades del usuario. Vamos a la pestaña "Marcado" y seleccionamos la opción "Permitir acceso" y aceptamos.



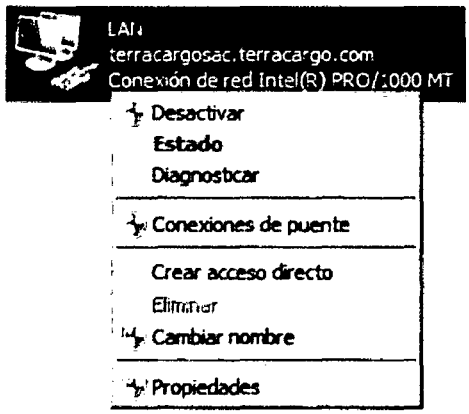
Y ya tenemos configurado nuestro servidor de Active Directory con nuestros usuarios VPN para el acceso a de los recursos de nuestra INTRANET.

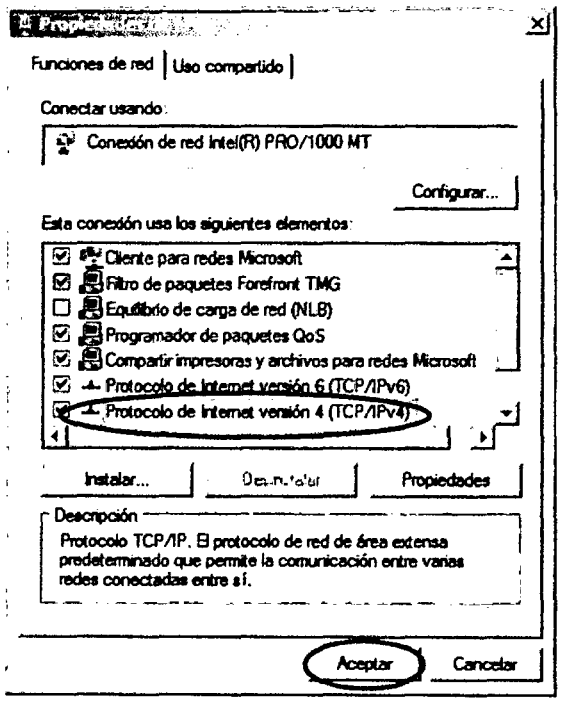
3. CONFIGURAR SERVIDOR - FOREFRONT TMG

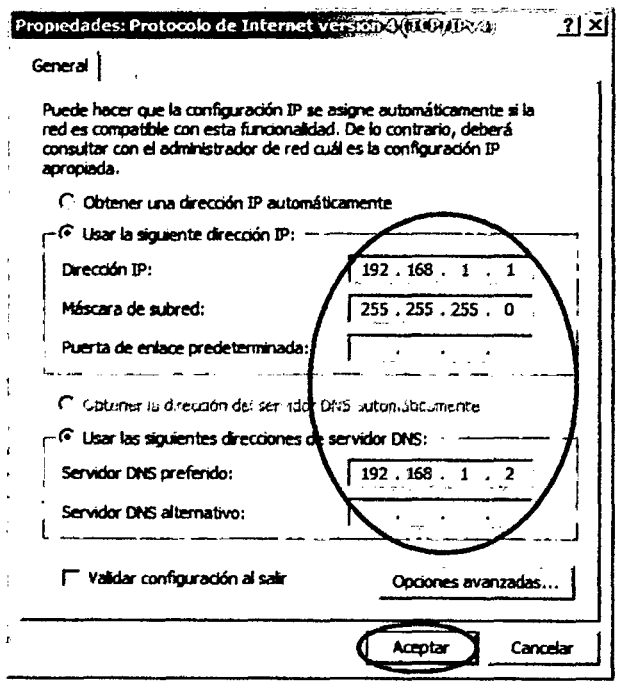
Una vez instalado el sistema operativo de nuestro segundo servidor Windows Server 2008 R2, el primer paso en nuestro servidor es configurar nuestros 2 adaptadores de red para la parte de la WAN y LAN con las direcciones IP según la topología gráfica, y "Cambiamos la configuración del adaptador" accediendo a la aplicación de "Centro de Redes y recursos compartidos" ubicada en "Panel de control", según muestra la configuración en "Propiedades: Protocolo de Internet versión 4 (TCP/IPv4).

Configuración de la Red LAN (RED INTERNA)

- ✓ Red Interna: 192.168.1.0/24
- ✓ DNS Interno: 192.168.1.2

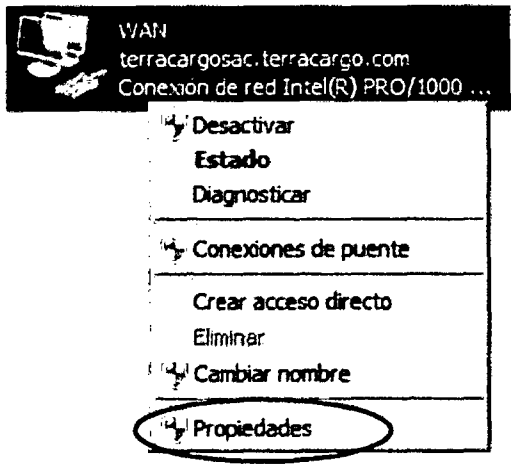


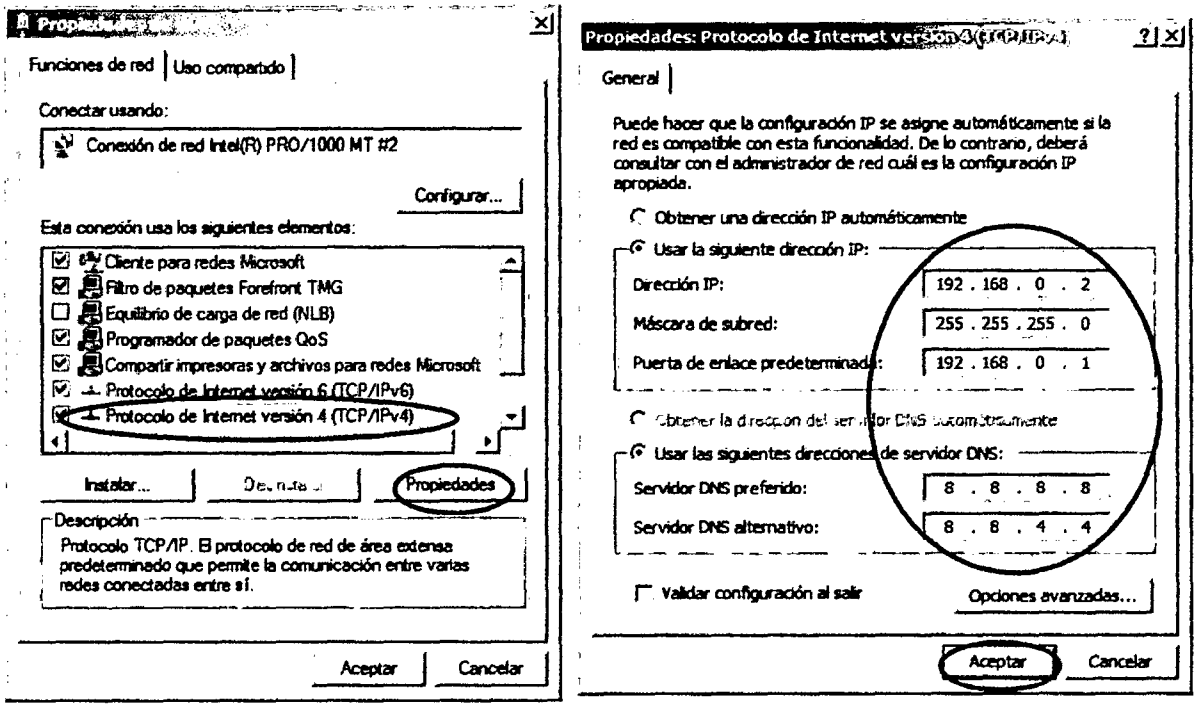




Configuración de la Red WAN (RED EXTERNA)1

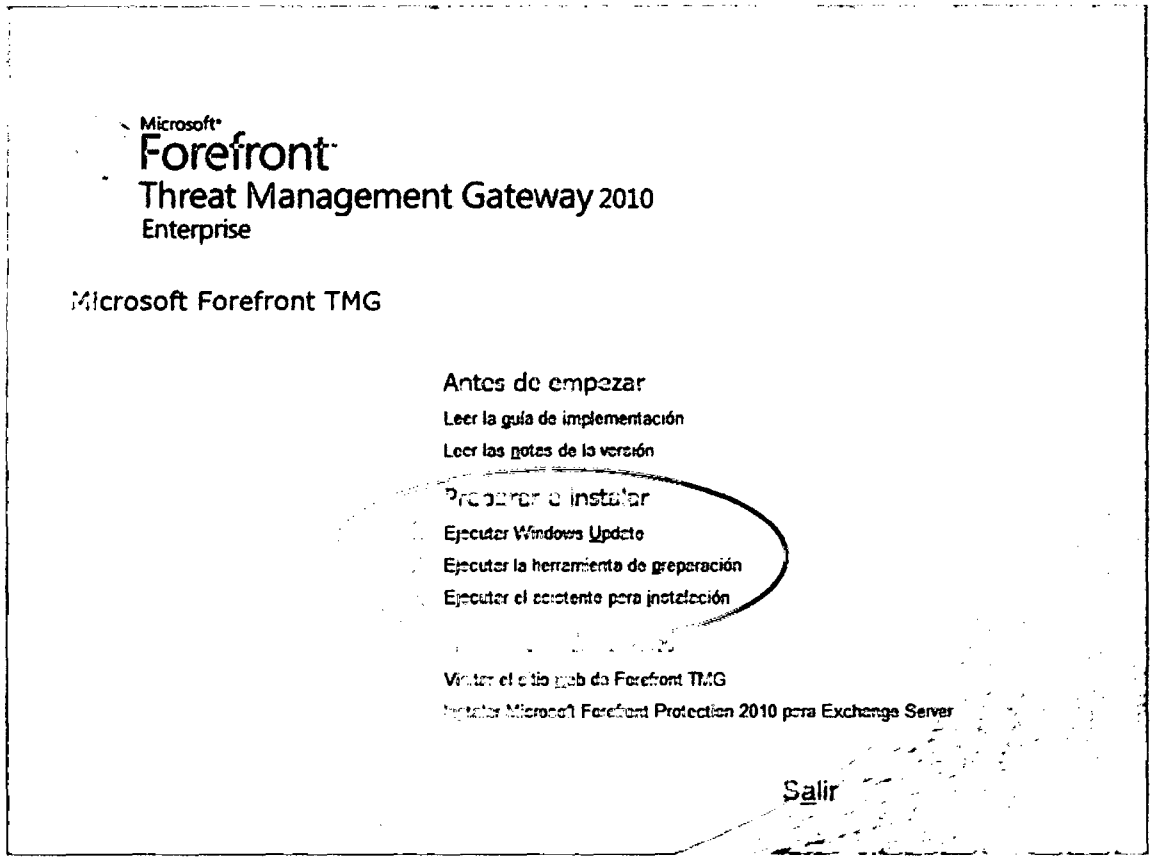
- ✓ Red Externa: 192.168.0.0/24
- ✓ DNS Externos: 8.8.8.8 y 8.8.4.4 (DNS públicos de Google)





Al igual que el servidor de Active Directory, este servidor lo usaremos para el servicio de VPN con la herramienta FOREFRONT TMG descargada desde la página oficial de Microsoft son su correspondiente licenciamiento. Ya instalado Microsoft Windows Server 2008 R2, procederemos a descomprimir en el directorio por defecto "C:\Microsoft Forefront TMG" el paquete FOREFRONT TMG descargado de Internet y

se iniciará automáticamente, en caso tengamos el instalador lo ejecutamos normalmente.



Posteriormente ejecutaremos las acciones señalados en el anterior gráfico para la correcta instalación de Microsoft Forefornt TMG.

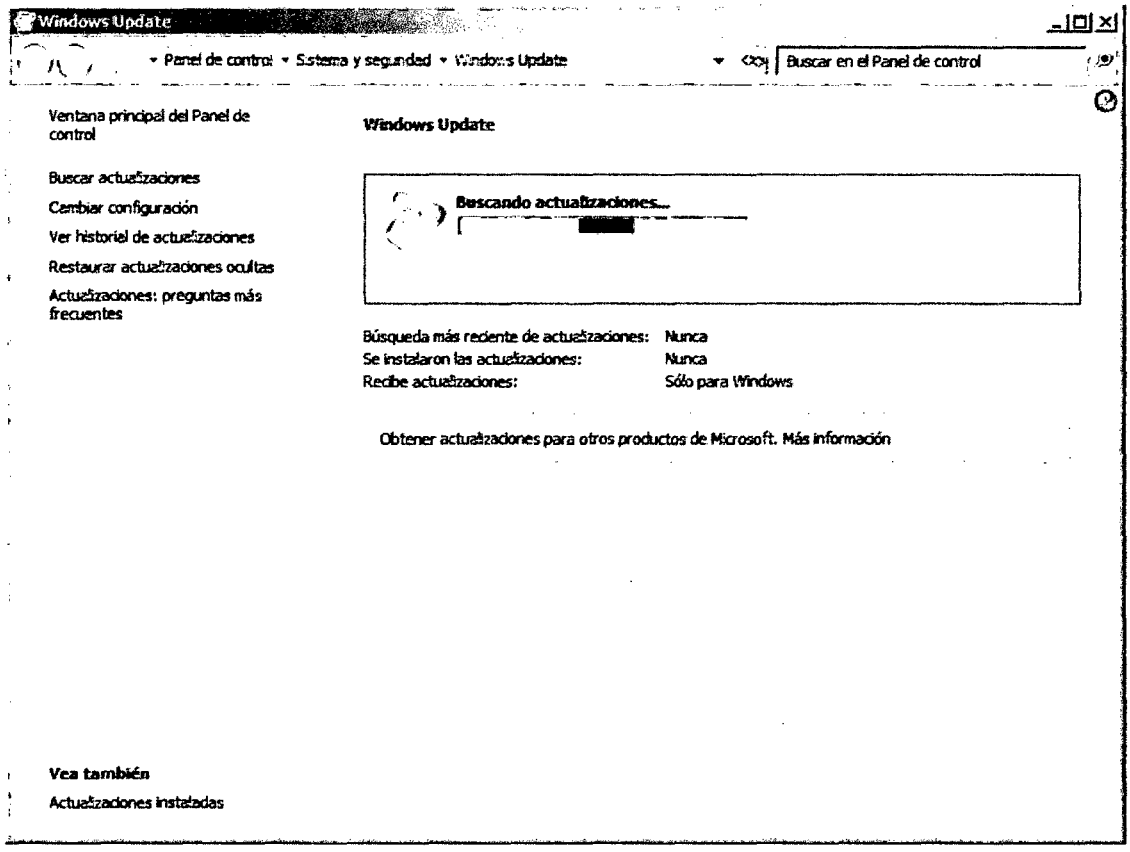
I. EJECUTAR WINDOWS UPDATE.

Es una aplicación que viene incluida en los sistemas operativos de Microsoft Windows el cual permite de manera fácil y gratuita de mantener el equipo más seguro y en perfecto funcionamiento, nos permite mantener actualizado hasta la fecha con los parches que Microsoft lanza para cubrir ciertas vulnerabilidades.

Windows Update determina por sí solo la versión de Windows que tienes instalada, así como la de otros programas de Microsoft que pueda haber en tu computadora.

También detecta los componentes de hardware de tu PC o qué dispositivos tienes conectados a él (impresoras, escáneres, webcams, etc.).

Mediante esa información comprueba si Windows y otros programas están al día. O si los drivers de tu hardware son los más recientes. Cuando no es así, descarga e instala las actualizaciones necesarias.



II. EJECUTAR HERRAMIENTA DE PREPARACIÓN

En este paso el asistente ejecutará la Instalación de servicios y características necesarias como requisitos de Forefront TMG para la administración de Forefront TMG, se realiza en 3 pasos siguientes:

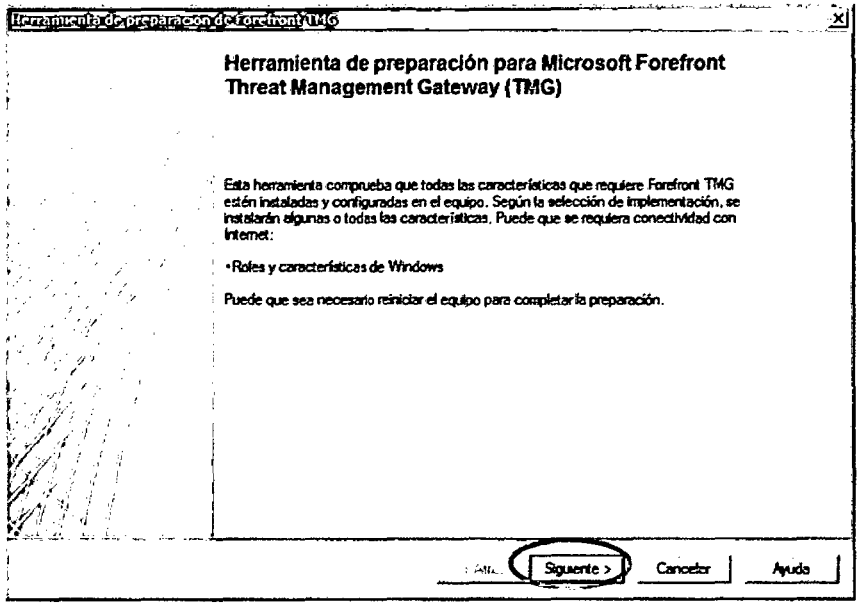
i. Introducción a la herramienta de preparación de Forefront TMG.
ii. Acuerdo de la licencia de software Microsoft

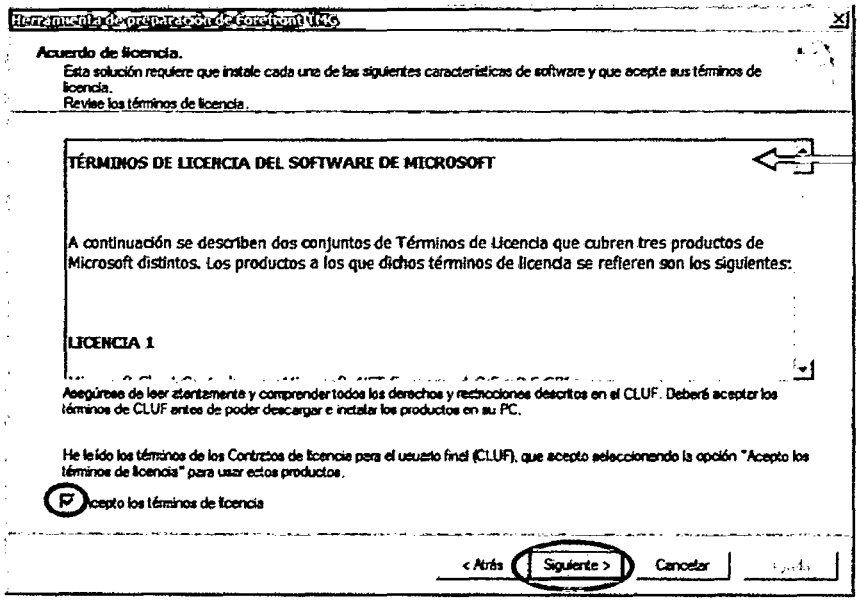
iii. Tipo de instalación:

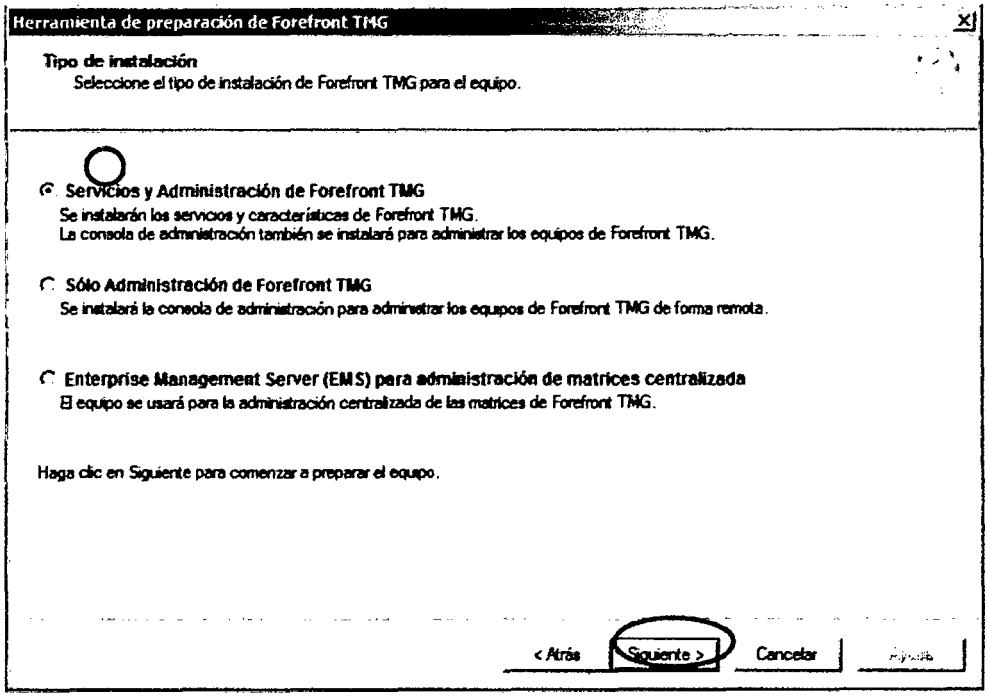
a) Servicios y Administración de Forefront TMG: Instala servicios, características y consola de administración de Forefront TMG (NUESTRO CASO DE IMPLEMENTACIÓN)
b) Solo Administración de Forefront TMG, instala consola de administración remota.
c) Enterprise Management Server (EMS), para administración de matrices centralizada.

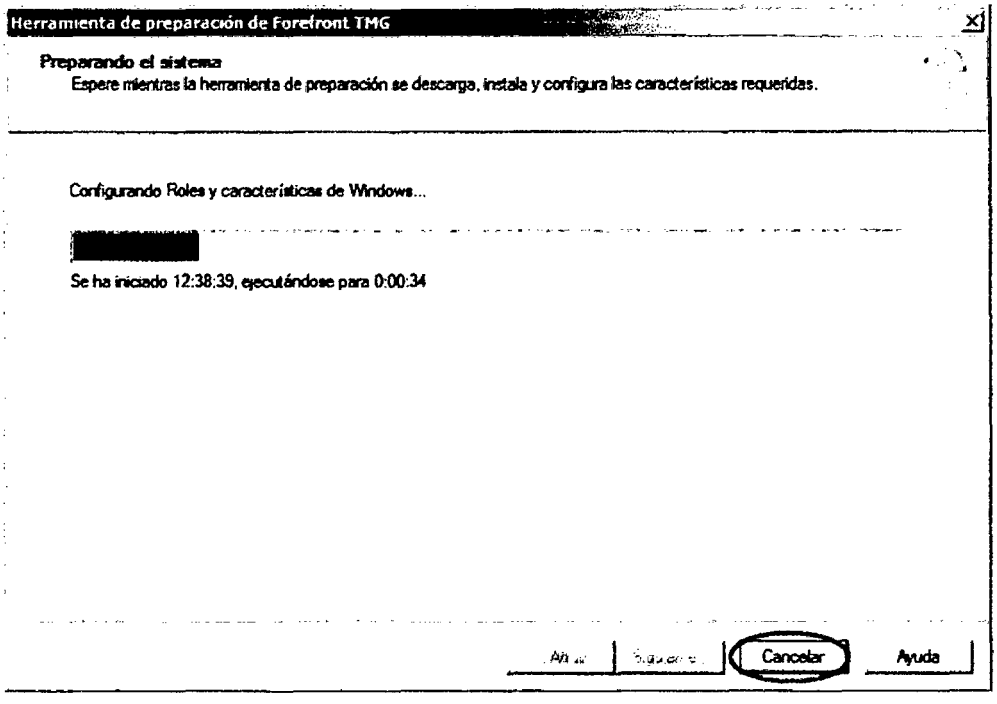
iv. Preparación del Sistema

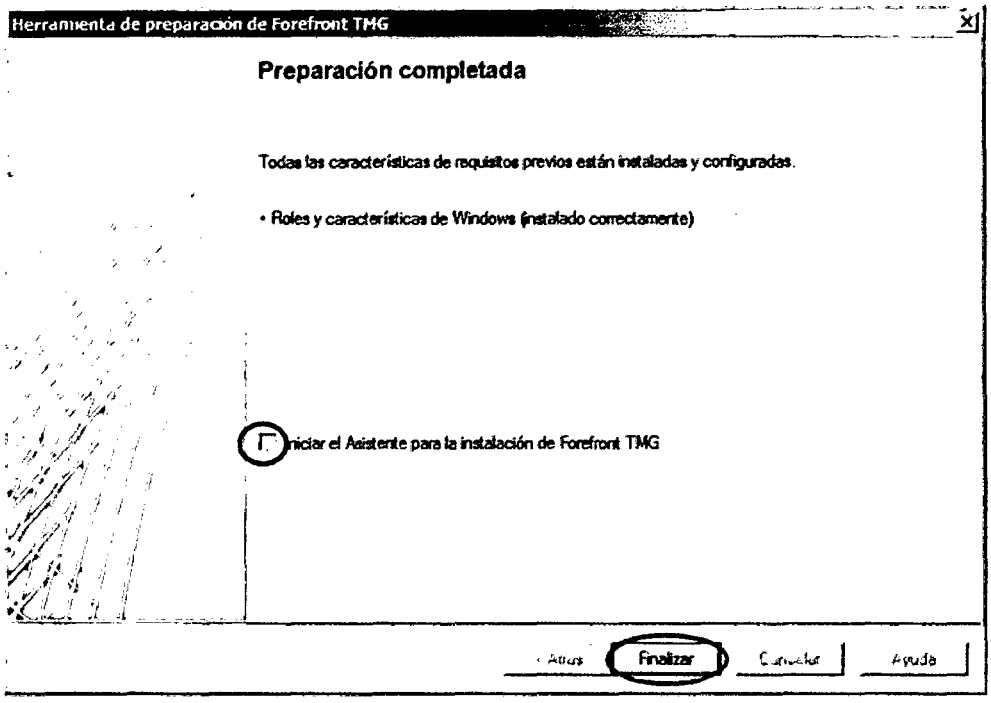
v. Finalización.





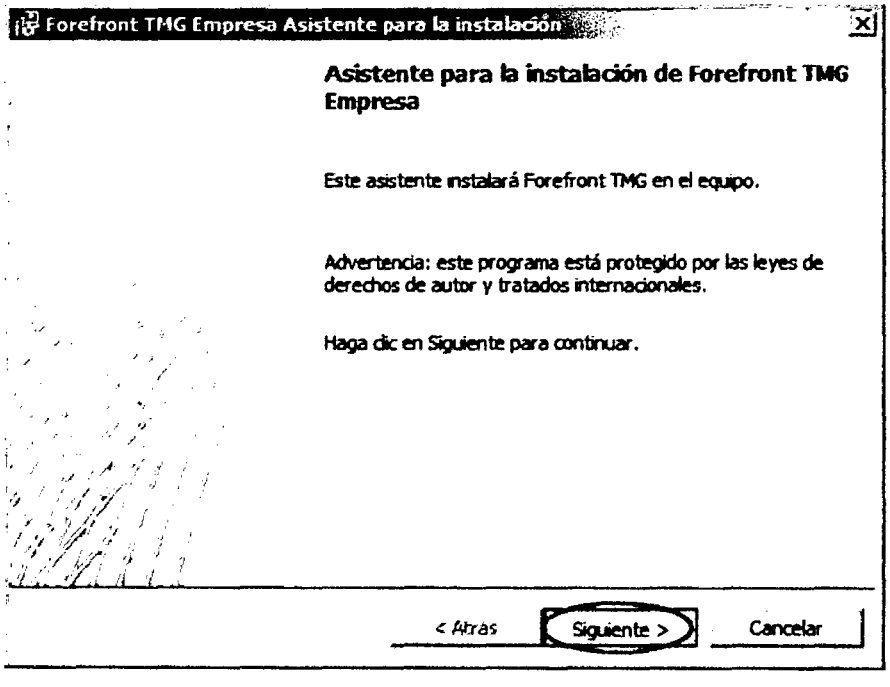

Herramienta de preparación de Forefront TMG
Tipo de instalación
Seleccione el tipo de instalación de Forefront TMG para el equipo.
Servicios y Administración de Forefront TMG
Se instalarán los servicios y características de Forefront TMG.
La consola de administración también se instalará para administrar los equipos de Forefront TMG.
Sólo Administración de Forefront TMG
Se instalará la consola de administración para administrar los equipos de Forefront TMG de forma remota.
Enterprise Management Server (EMS) para administración de matrices centralizada
El equipo se usará para la administración centralizada de las matrices de Forefront TMG.
Haga clic en Siguiente para comenzar a preparar el equipo.
< Atrás
Siguiente >
Cancelar


Herramienta de preparación de Forefront TMG
Preparando el sistema
Espere mientras la herramienta de preparación se descarga, instala y configura las características requeridas.
Configurando Roles y características de Windows...
Se ha iniciado 12:38:39, ejecutándose para 0:00:34
Cancelar
Ayuda

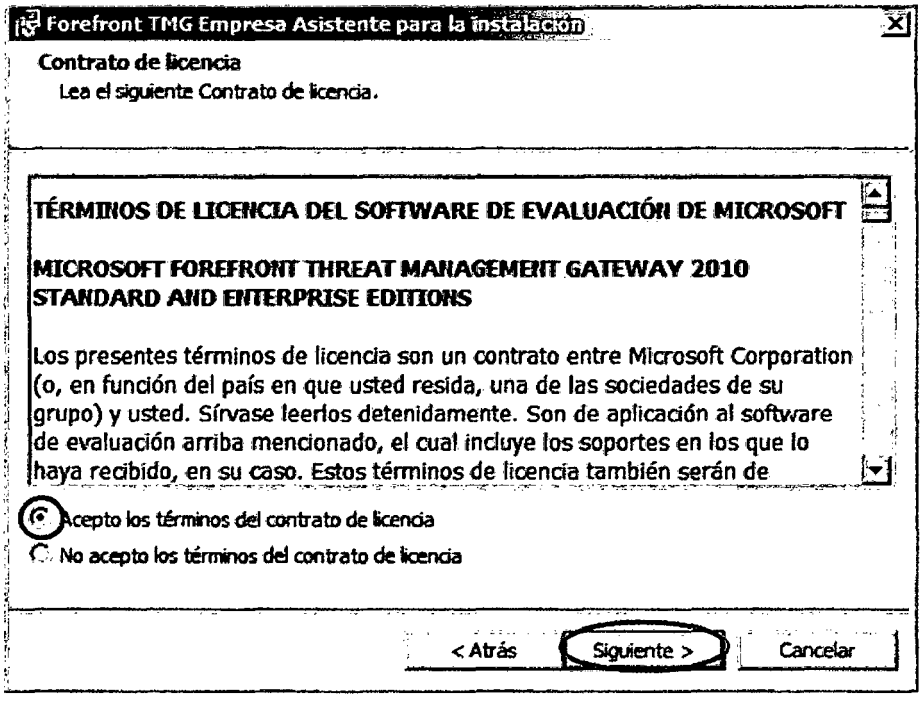


III. PASOS PARA EJECUTAR EL ASISTENTE PARA INSTALACIÓN

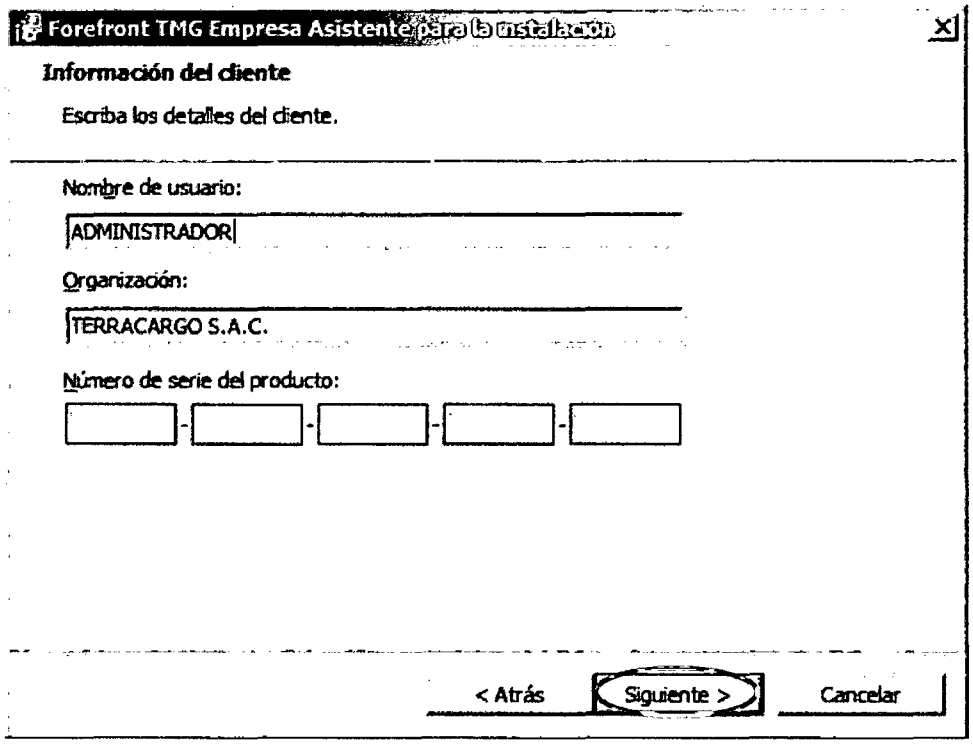
Al finalizar la preparación del sistema para Forefront hay una opción para ejecutar el asistente de instalación de Forefront e iniciará automáticamente, caso contrario damos clic en la pantalla inicial de instalación de Microsoft Forefront TMG en la opción "Ejecutar el asistente para la instalación".



i. Aceptar términos y condiciones de la licencia del Software de Microsoft, posteriormente ingresaremos la clave de licencia para dejar de ser evaluación.



ii. Definir nombre de Usuario (ADMINISTRADOR), organización (TERRACARGO S.A.C.) y serie del producto (lo coloca automáticamente el asistente de instalación).



iii. Definir escenario en el que trabajará nuestro Forefront:

a) Instalar servicios y Administración de Forefront TMG:

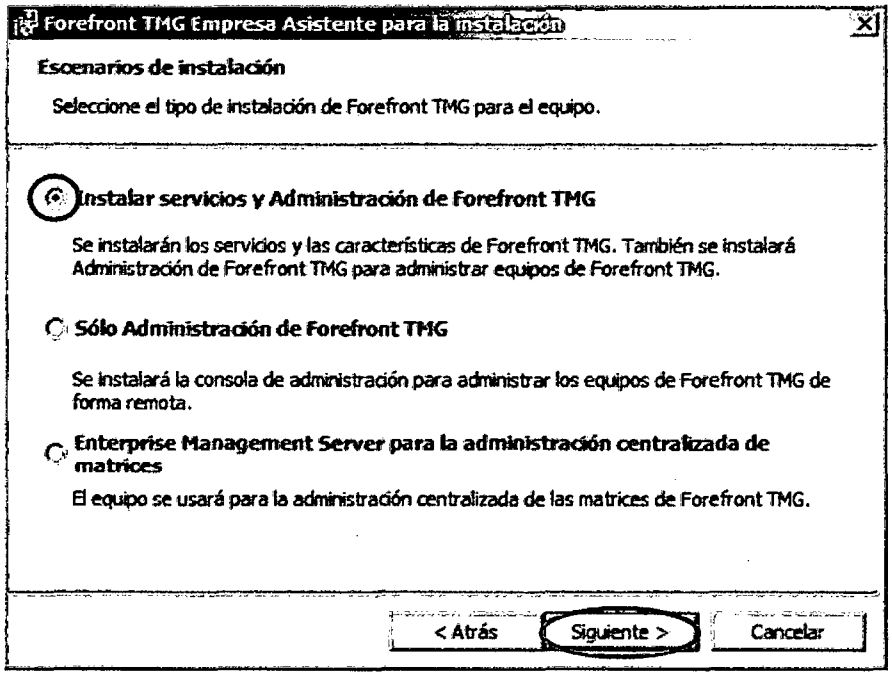
En este escenario instalaremos los servicios necesarios para su correcta instalación de Forefront debido a que usa algunas características como por ejemplo el ROL DEL SERVIDOR llamado "Enrutamiento y Acceso Remoto" necesarias para el funcionamiento de algunas opciones de FOREFRONT TMG como la que vamos a realizar de VPN para poder enrutar tráfico desde las redes externas con la interna.

En nuestro proyecto aplicaremos este escenario por no tener más equipos Forefront configurados en la infraestructura de la organización TERRACARGO SAC.

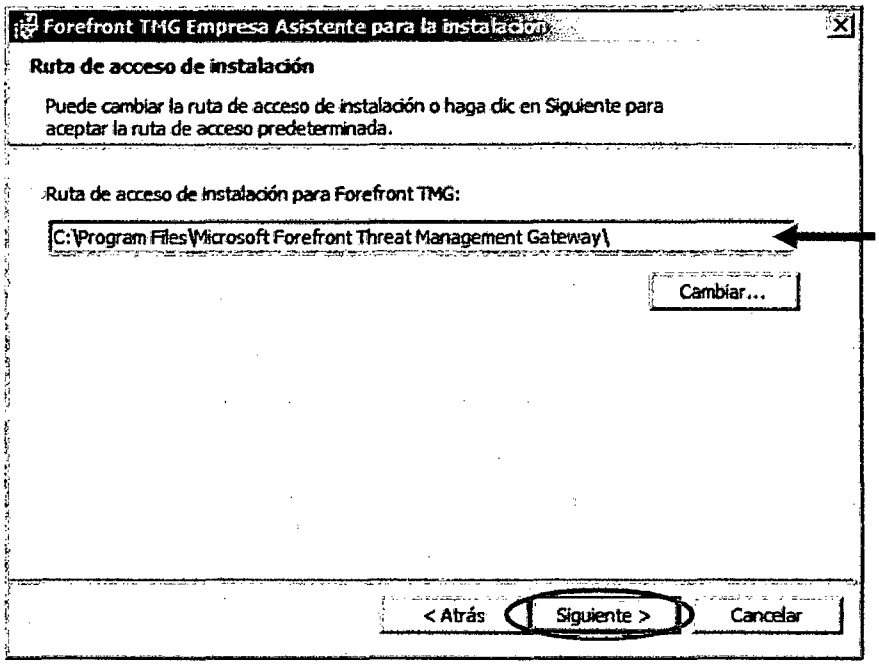
b) Solo Administración de Forefront TMG:

El asistente lo que hará en este escenario es solo instalar la consola de administración para administrar equipos configurado con el escenario anterior de manera remota.

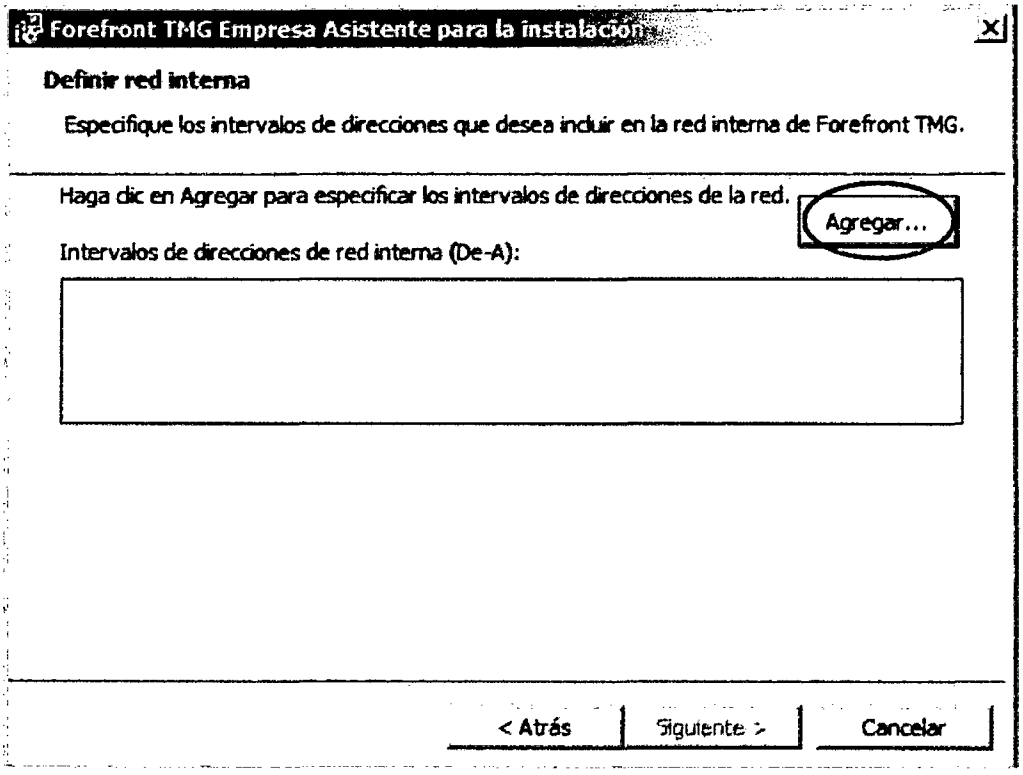
c) Enterprise Management Server para la administración centralizada de matrices: Es parecido al escenario anterior, la deferencia es que tenemos en muchas sucursales equipos configurados con el primer escenario para poder centralizar la administración de ellos en un solo equipo.

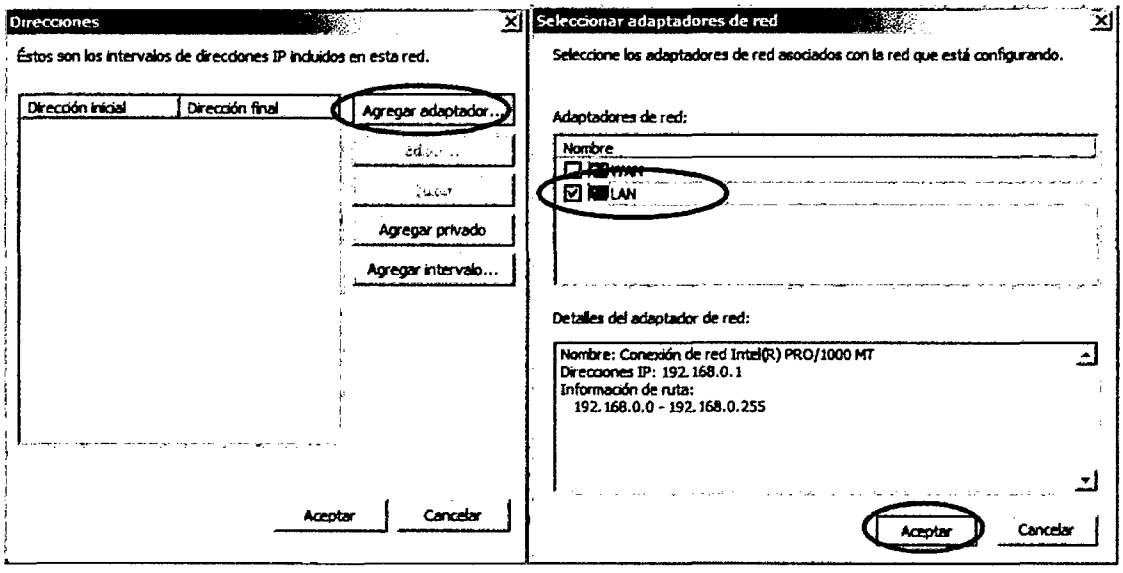


iv. Configurar la Ruta de acceso de Instalación, es fundamental definir para su óptimo funcionamiento, por lo cual hemos decido dejarlo por defecto la ruta de instalación en el disco "C:\Program Files\Microsoft Forefront Threat Management Gateway\"

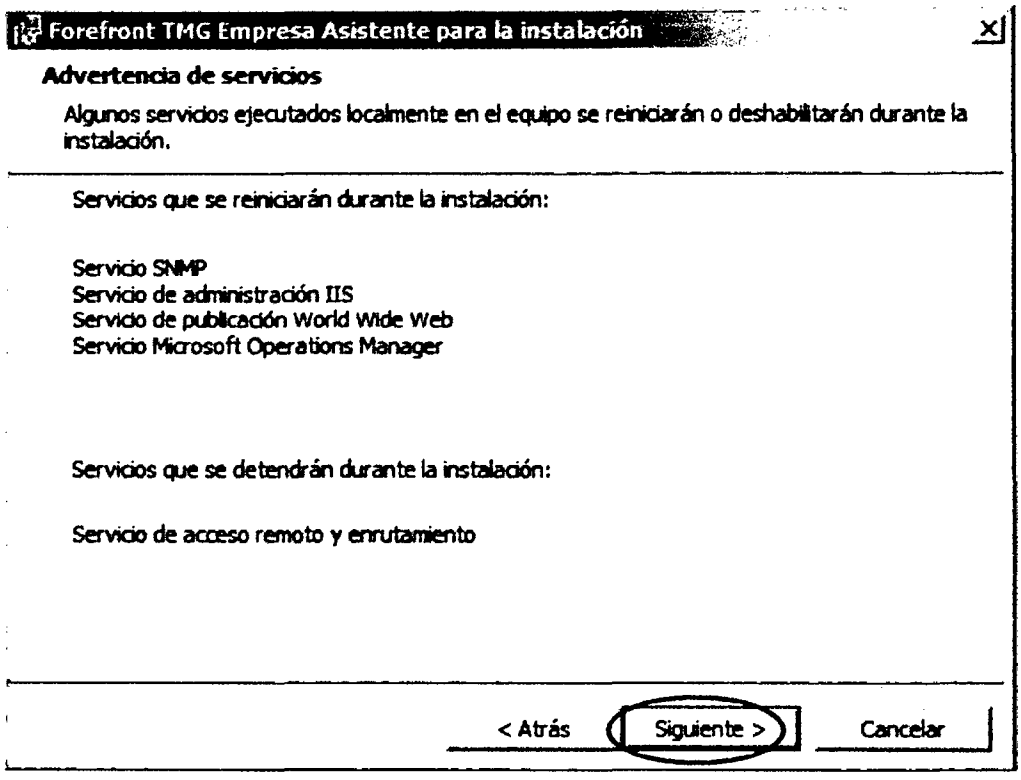


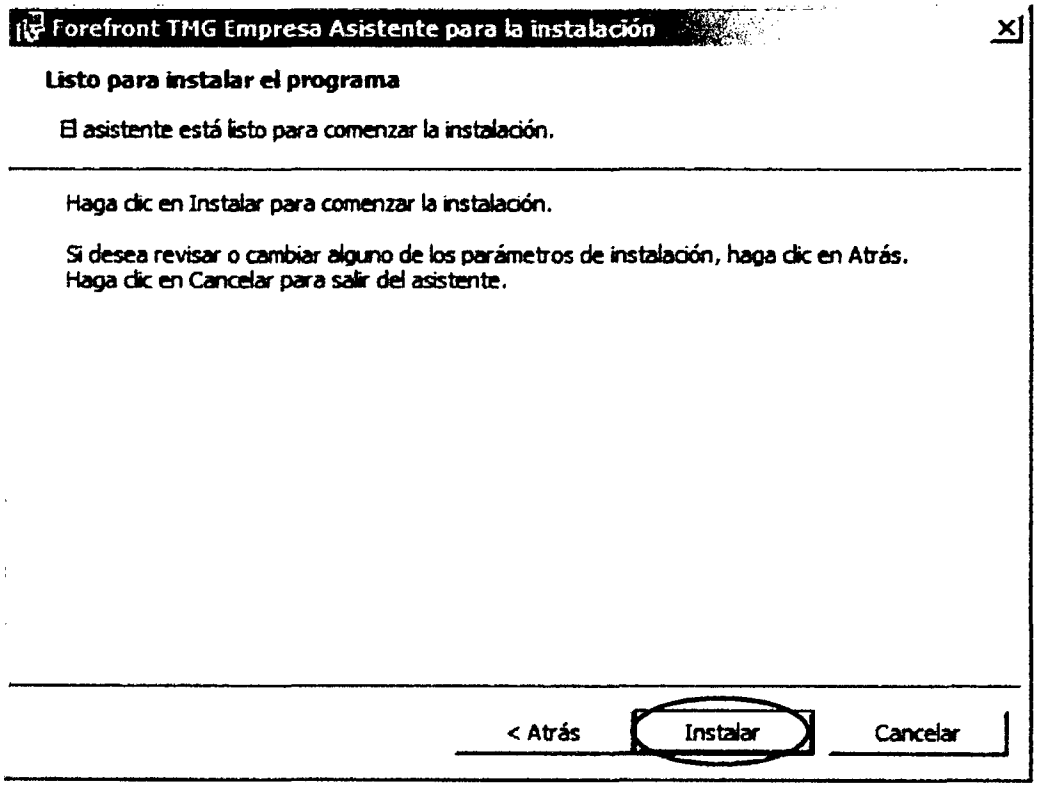
v. Definir adaptador y red interna: una vez ya configurado desde un principio las direcciones IP de nuestro servidor, ahora no tendremos problema para definir este punto, Seleccionamos "Agregar", "Agregar Adaptador", seleccionamos "LAN", posteriormente "ACEPTAMOS" las dos ventana que se abrimos y luego "Siguiente"





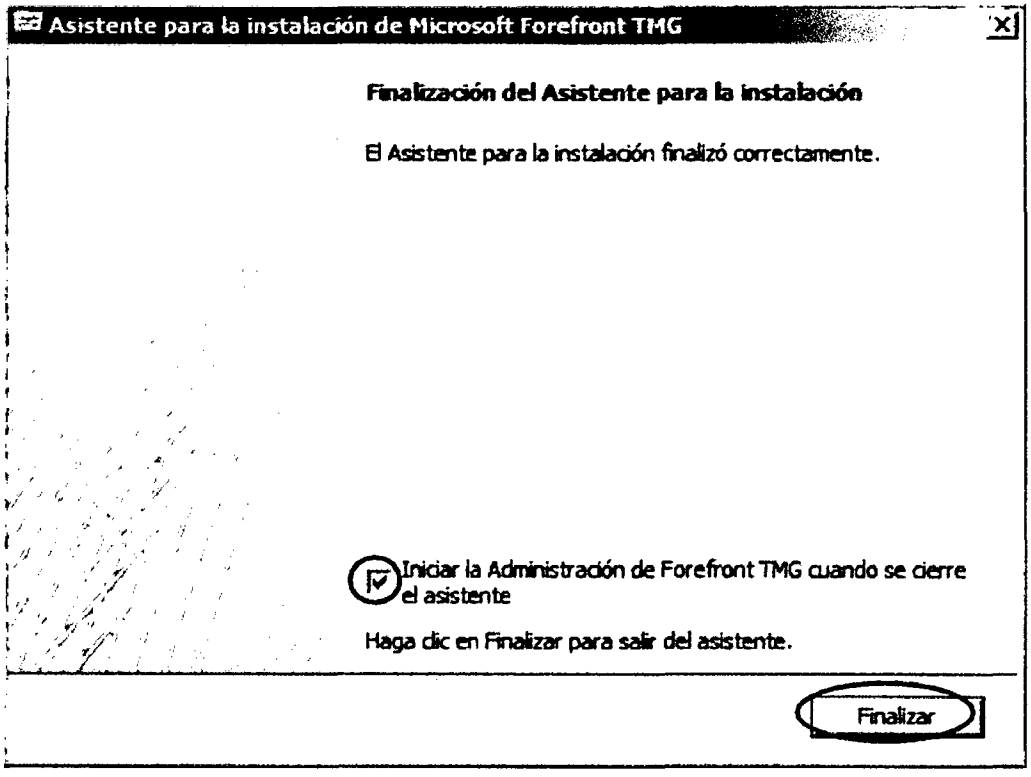
Y finalmente se muestra una advertencia de servicios que se reiniciarán durante la instalación en caso estén corriendo en nuestro servidor, lo cual no afectará en el mismo debido a que no están instalados los servicios que nos muestra. Seleccionamos "Siguiente" y luego "Instalar".

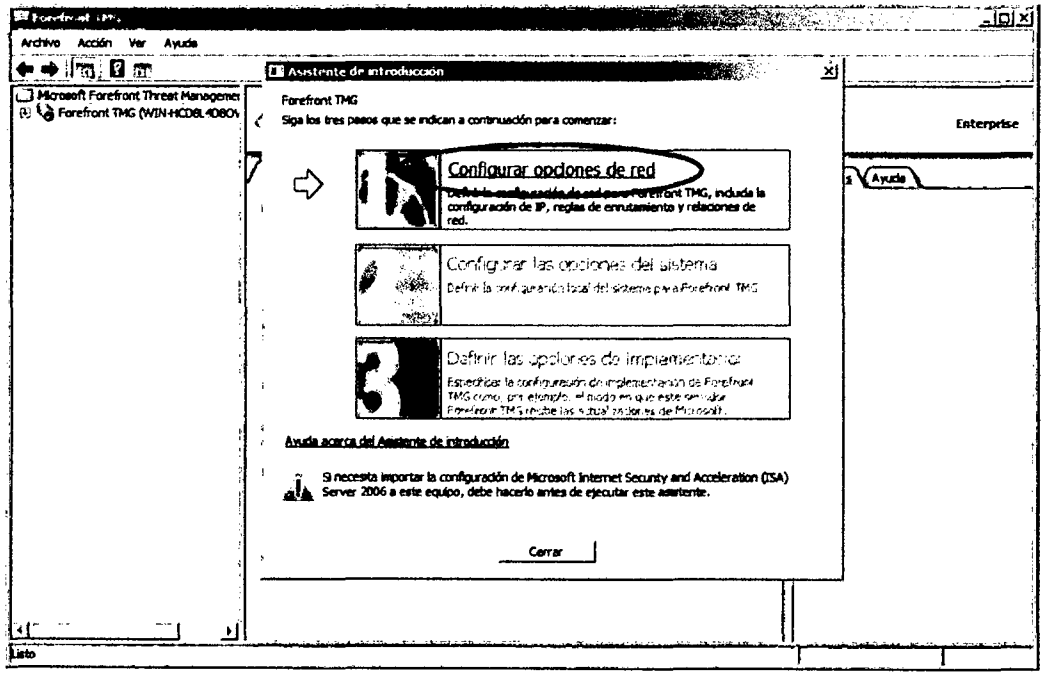

Forefront TMG Empresa Asistente para la instalación
Advertencia de servicios
Algunos servicios ejecutados localmente en el equipo se reiniciarán o deshabilitarán durante la instalación.
Servicios que se reiniciarán durante la instalación:
Servicio SNMP
Servicio de administración IIS
Servicio de publicación World Wide Web
Servicio Microsoft Operations Manager
Servicios que se detendrán durante la instalación:
Servicio de acceso remoto y enrutamiento
< Atrás
Siguiente >
Cancelar


Forefront TMG Empresa Asistente para la instalación
Listo para instalar el programa
El asistente está listo para comenzar la instalación.
Haga clic en Instalar para comenzar la instalación.
Si desea revisar o cambiar alguno de los parámetros de instalación, haga clic en Atrás.
Haga clic en Cancelar para salir del asistente.
< Atrás
Instalar
Cancelar

IV. ADMINISTRACIÓN DE FOREFRONT TMG

Antes de finalizar la instalación podremos habilitar el checkbox que nos permitirá iniciar la consola de Administración de Forefront TMG como se muestra en la imagen siguiente:





I. Configurar Opciones de red.

a) Seleccionar Plantilla de Red según topología de red:

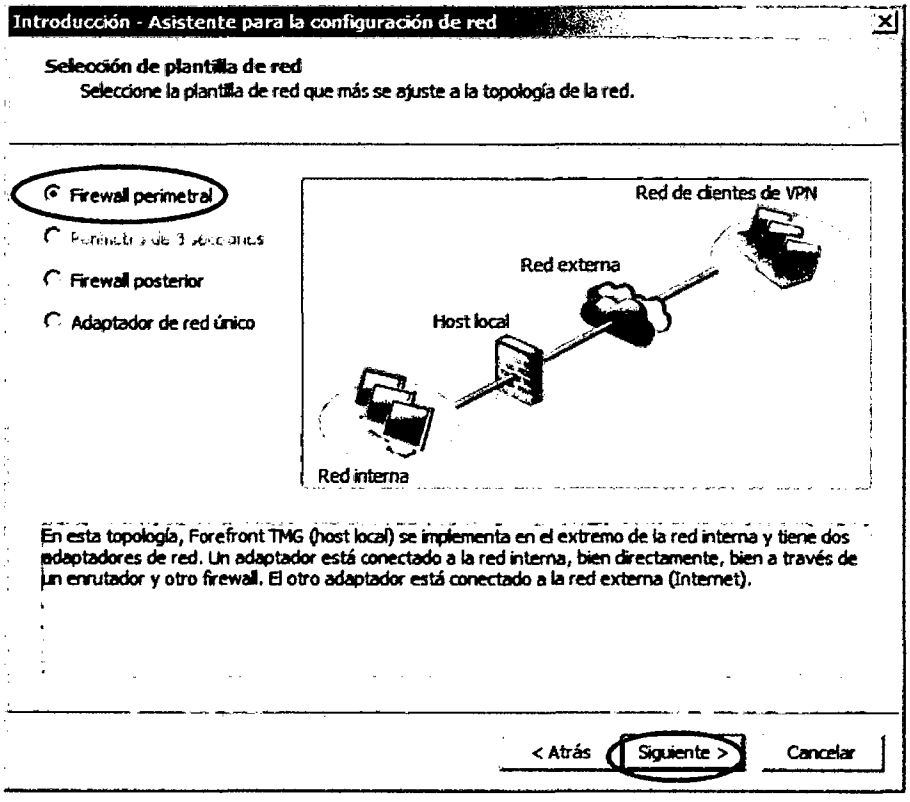
- ✓ **Firewall perimetral**: en esta topología, Forefront TMG se encuentra en el perímetro de la red, donde actúa como firewall perimetral de la organización, y está conectado a dos redes: la red interna y la red externa.

- ✓ **Perímetro de 3 secciones**: esta topología implementa una red perimetral. Forefront TMG está conectado por lo menos a tres redes físicas: la red interna, una o más redes perimetrales, y la red externa.

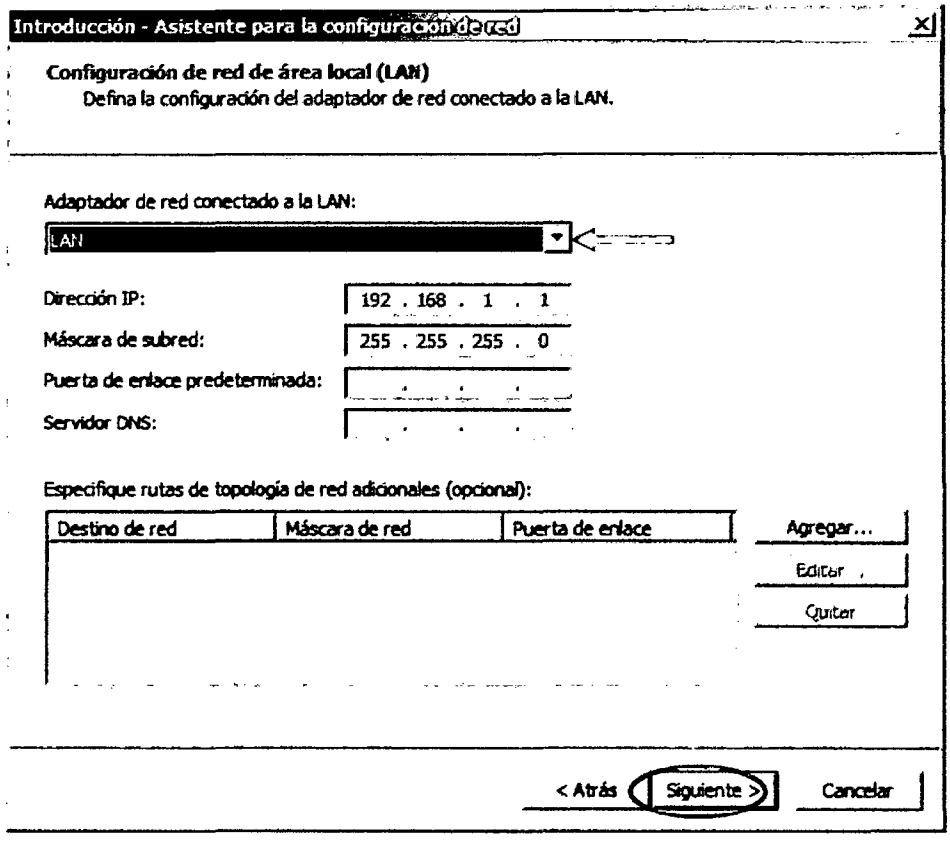
- ✓ **Firewall posterior**: en esta topología, Forefront TMG se encuentra en el back-end de la red. Utilice esta topología cuando otro elemento de red, como una red perimetral o un dispositivo de seguridad perimetral, se encuentre entre Forefront TMG y la red externa. Forefront TMG se conecta a la red interna y al elemento de red situado delante.

- ✓ **Adaptador de red único**: esta topología habilita funcionalidad de Forefront TMG limitada. En esta topología, Forefront TMG está conectado únicamente a una red, bien la red interna o una red perimetral. Normalmente, se utilizaría esta configuración si Forefront TMG se encontrase en la red corporativa interna o en una red perimetral y otro firewall estuviese situado en el perímetro, protegiendo los recursos corporativos de Internet.

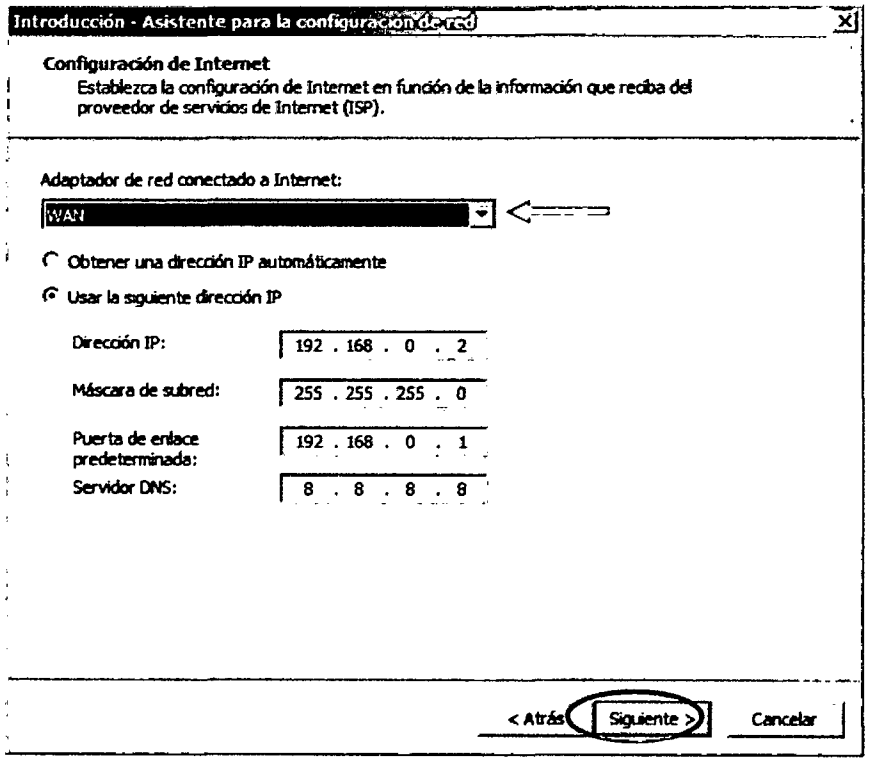
Elegimos la opción de Firewall Perimetral para maximizar y centralizar la seguridad en cuanto al tráfico, debido a que nuestro servidor la hemos configurado con 2 tarjetas de red para que todo el tráfico saliente a INTERNET (Tráfico Web y de VPN) e ingresante a la Red interna de la organización (Trafico VPN), pasará por nuestro servidor y será controlado de una manera centralizada desde la consola de Administración de Forefront TMG.



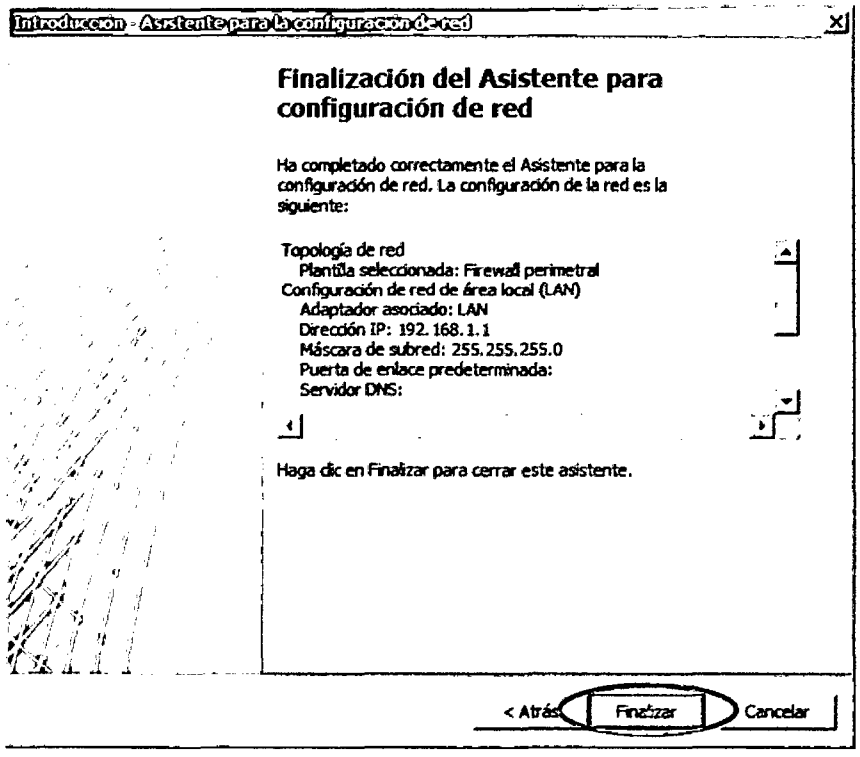
b) Configurar adaptador de red (Red Interna - LAN): Direcciones IP y DNS, en este paso lo que haremos es seleccionar el adaptador de red denominado LAN y automáticamente se colocarán las direcciones IP configuradas en ella.



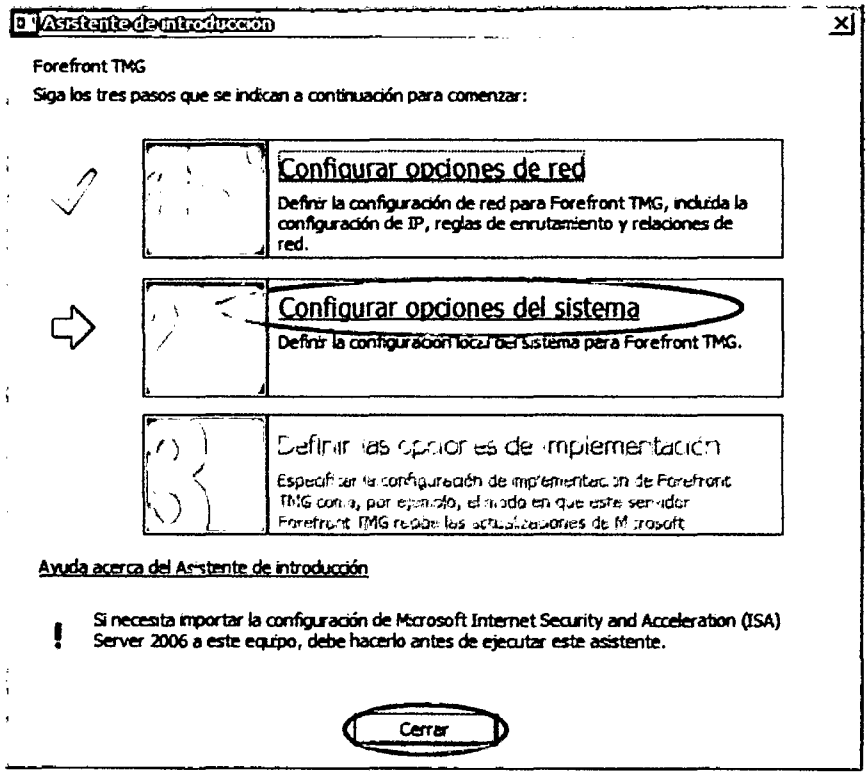
c) Configurar adaptador de red (Red Externa - Internet): Direcciones IP y DNS. Como se muestra en la topología del proyecto, ésta apunta a la red donde están ambos ISP tanto de movistar como de Optical Networks.



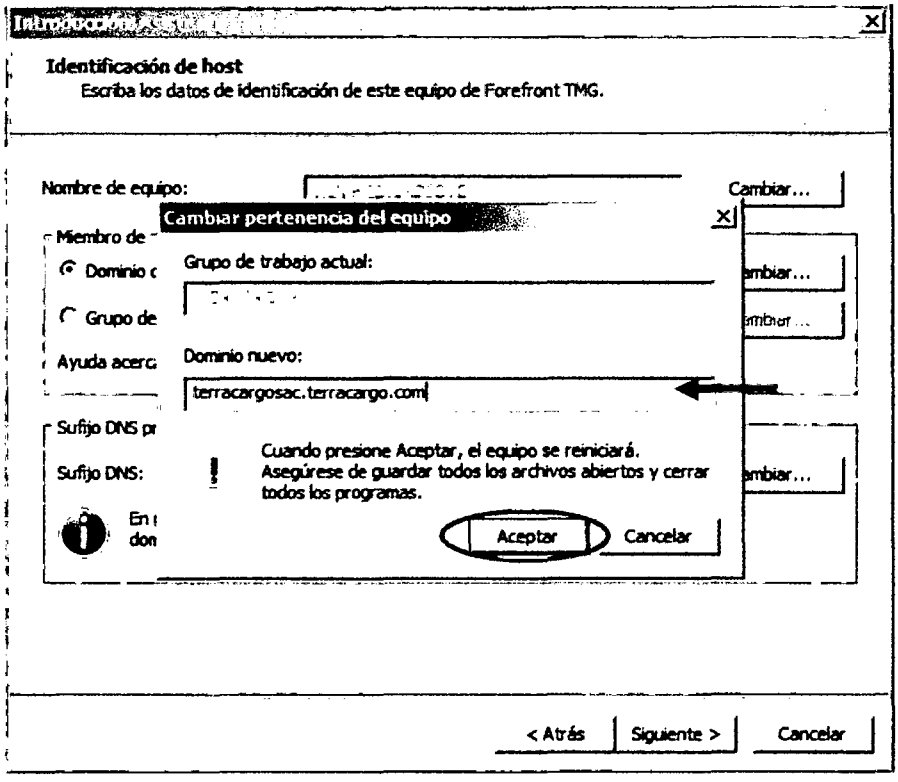
Y finalmente verificaremos en el resumen si verdaderamente estas con las configuraciones hemos hecho, por si se nos esté faltando alguna configuración.

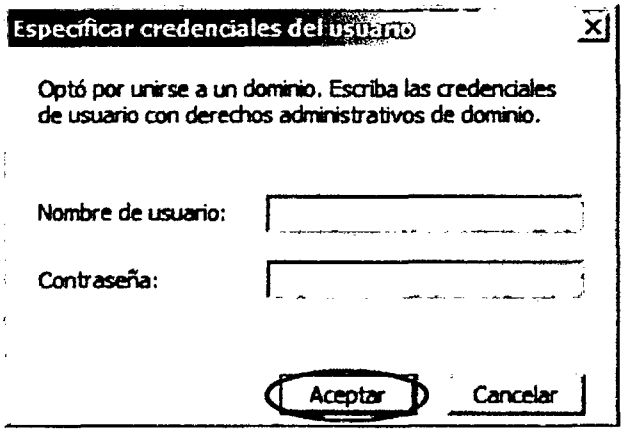


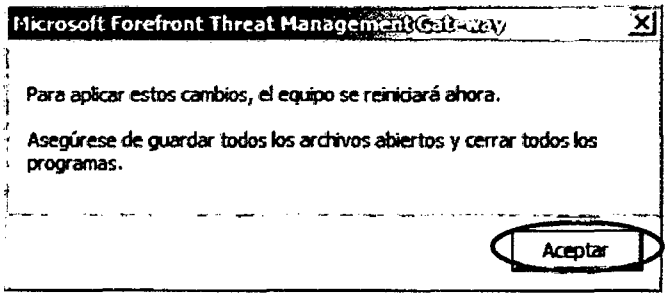
II. Configurar las opciones del sistema.



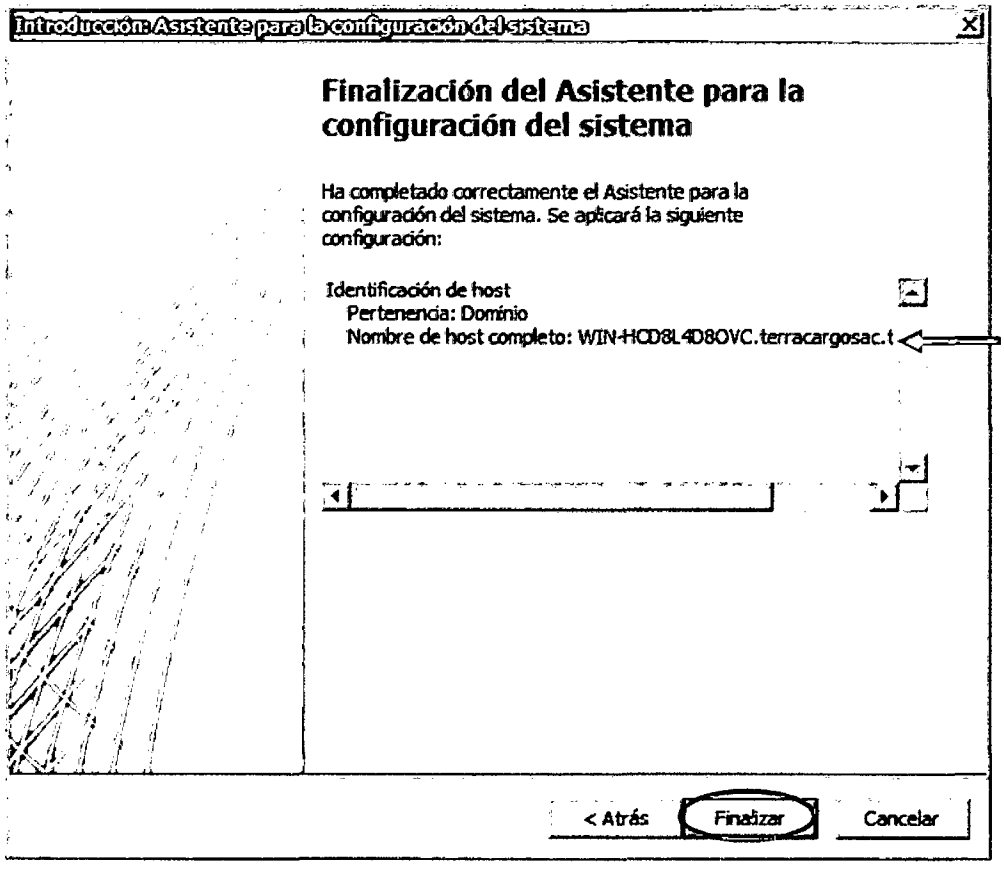
a) Agregamos al dominio el equipo de Forefront TMG para poder direccionar y utilizar los usuarios del dominio y así controlarlos desde el servidor de ACTIVE DIRECTORY. Nos pedirá la autenticación de algún usuario del dominio con permiso respectivos, luego pedirá reiniciar para que los cambios sufran efecto (Aceptar)



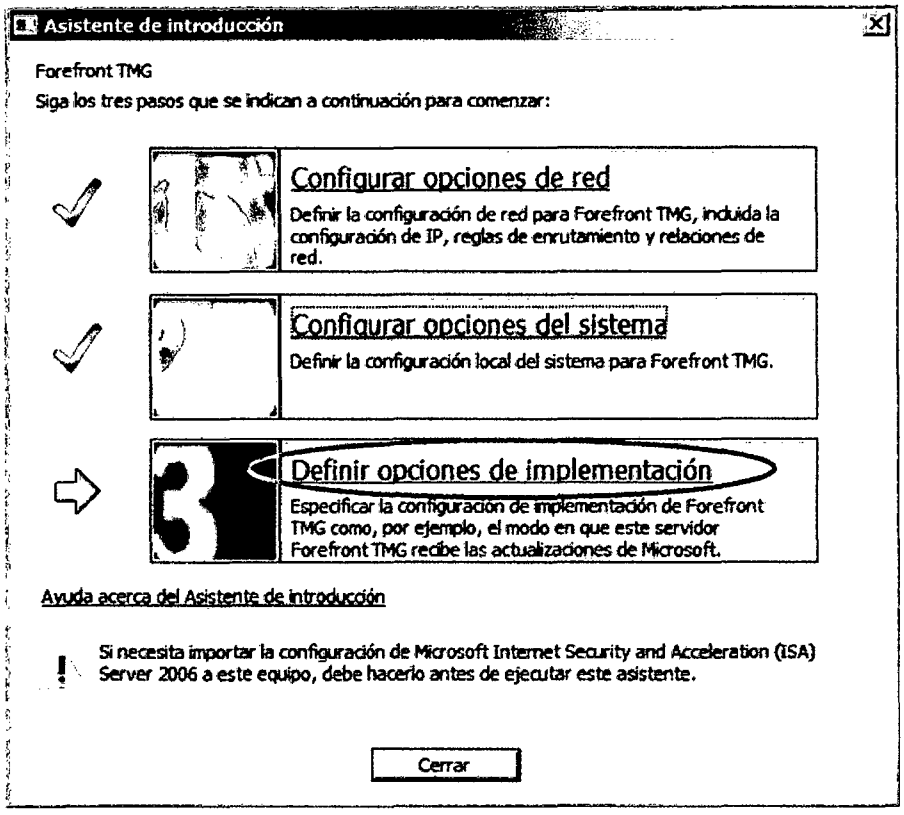




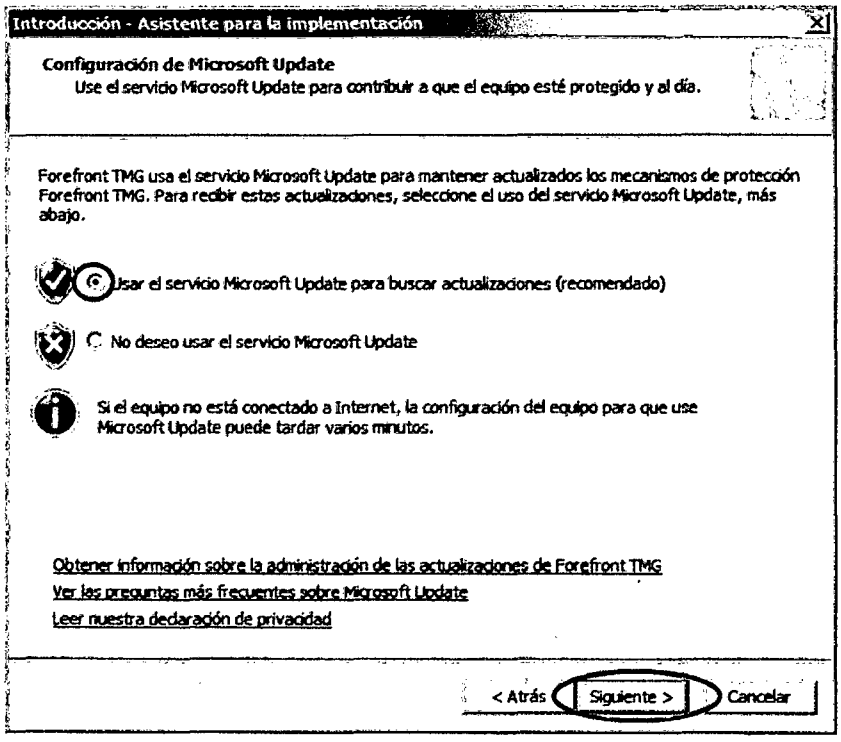
Finalmente verificamos en el resumen de la configuración que todo esté correcto según lo que hemos configurado en los anteriores pasos, luego seleccionamos "Finalizar", en caso falte alguna configuración seleccionar "Atrás" y agregar o corregir algún dato faltante o incorrecto.



III. Definir las opciones de implementación

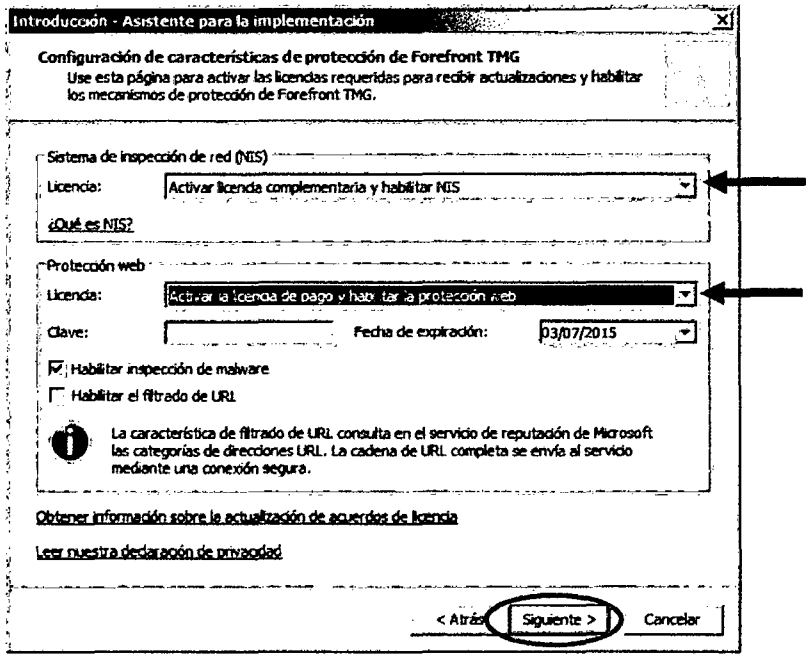


a) Habilitamos Microsoft Windows Update, Para mantener los mecanismos de protección de Forefront TMG.

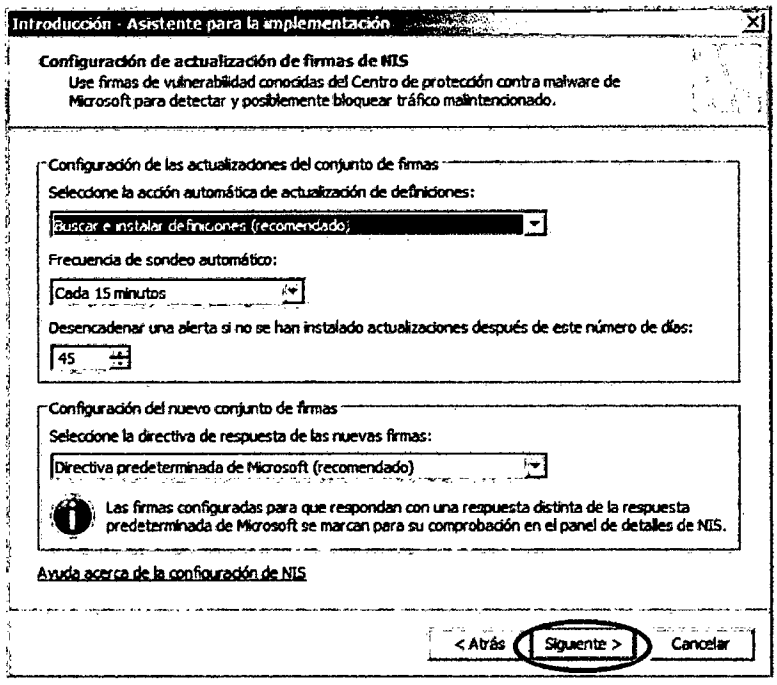


b) Habilitamos las características de protección:

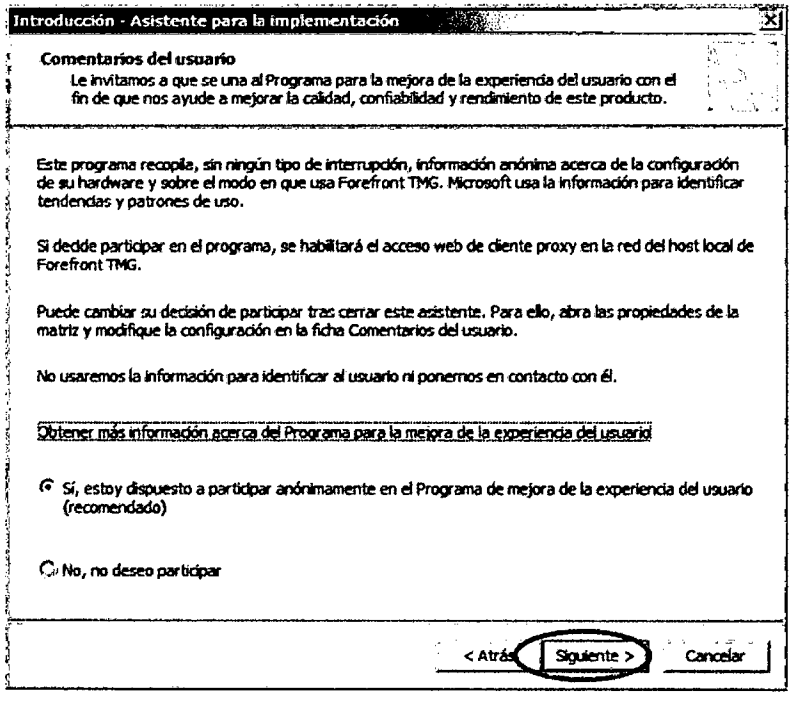
- ✓ Sistema de inspección de red (NIS).
- ✓ Protección Web: Ingresamos la clase de licenciamiento.



Luego de haber habilitado NIS, configuraremos la actualización de firmas NIS, Forefront usa firmas de vulnerabilidades conocidas del centro de protección contra malware de Microsoft para detectar y posiblemente bloquear tráfico malintencionado. Configuraremos estas opciones de acuerdo a lo que queramos optimizar nuestro sistema, en nuestra infraestructura lo configuraremos de la siguiente manera:

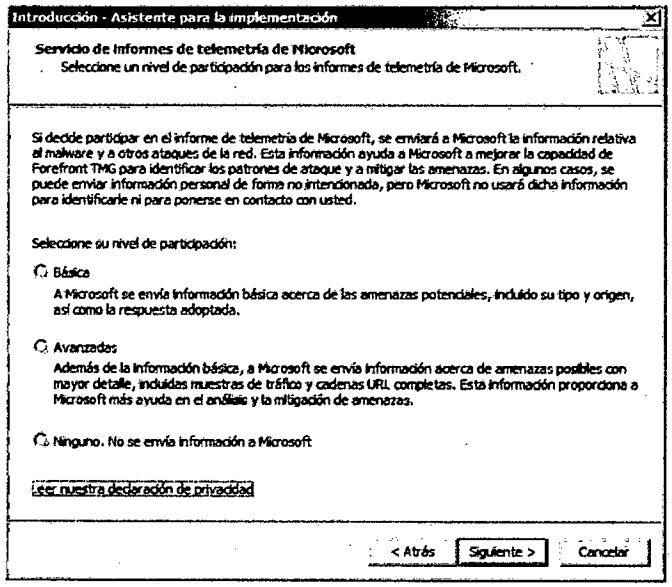


c) Participar en el programa de mejora de la experiencia del usuario: Este programa recopila sin ningún tipo de interrupción, información acerca de la configuración de su hardware y sobre el modo en que usa Forefront TMG. Microsoft usa la información para identificar tendencias y patrones de uso. Se habilitará el acceso web de cliente proxy en la red del host local de Forefront TMG. En este programa se participa anónimamente.

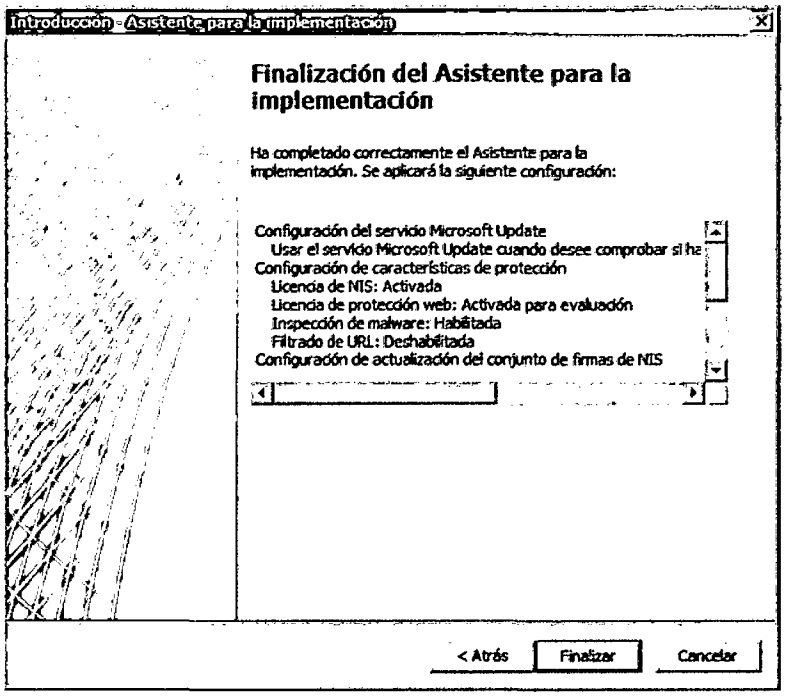


d) Nivel de Participación para los informes de telemetría de Microsoft: Este programa envía a Microsoft la información relativa al Malware y a otros ataques de su red. Esta información ayuda a Microsoft a mejorar la capacidad de Forefront TMG para identificar los patrones de ataques y a mitigar las amenazas. En algunos casos, se puede enviar información personal de forma no intencionada, pero Microsoft no usará dicha información para identificarle ni para ponerse en contacto con la empresa. Existen 3 tipos de nivel de participación:

- ✓ Básica (envía información básica de las amenazas potenciales, incluido su tipo y origen, así como la respuesta adoptada).
- ✓ Avanzadas (Además de la información básica, a Microsoft se envía información acerca de amenazas posibles con mayor detalle, incluidas muestras de tráfico y cadenas URL completas. Esta información proporciona a Microsoft más ayuda en el análisis y la mitigación de amenazas).
- ✓ Ninguno (No envía información).

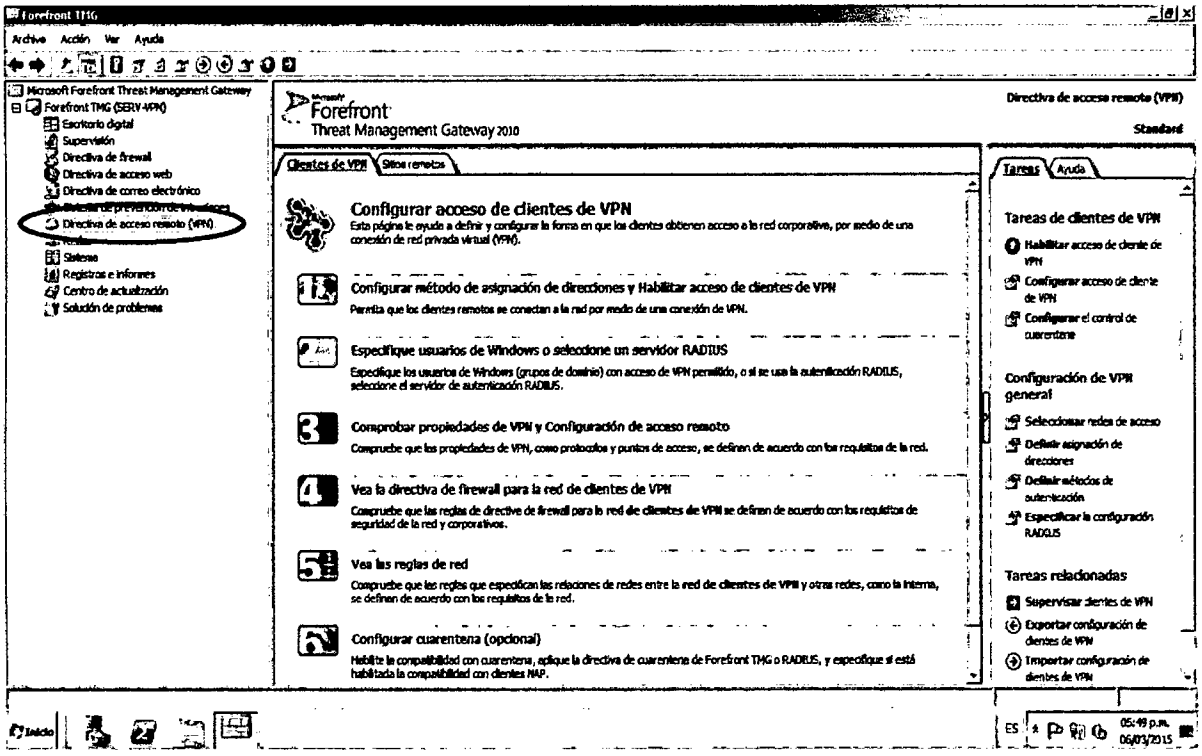


Finalmente se verifica en el resumen de si todas las configuraciones que hemos realizado son correctas para proceder en "Finalizar", caso contrario ir "Atrás" para corregir. Luego de terminar con las configuraciones iniciales que se tienen que realizar, ahora ya podemos proceder a configurar cualquier función de FOREFRONT TMG.

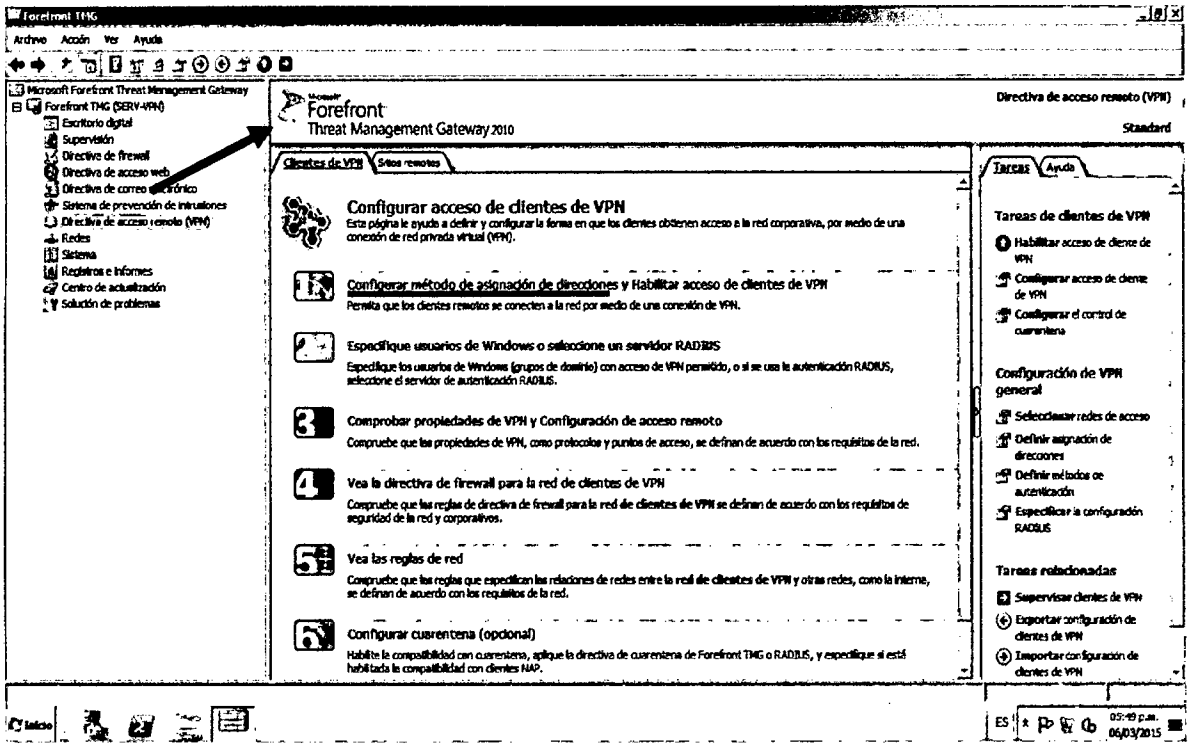


4. CONFIGURAR SERVIDOR - VPN.

Instalado ya Forefront TMG en nuestro segundo servidor, realizaremos la configuración para el servicio VPN. En la consola de administración de Forefront seleccionamos en la opción "Directiva de acceso remoto (VPN)" en la el panel izquierdo de la consola como se muestra a continuación:



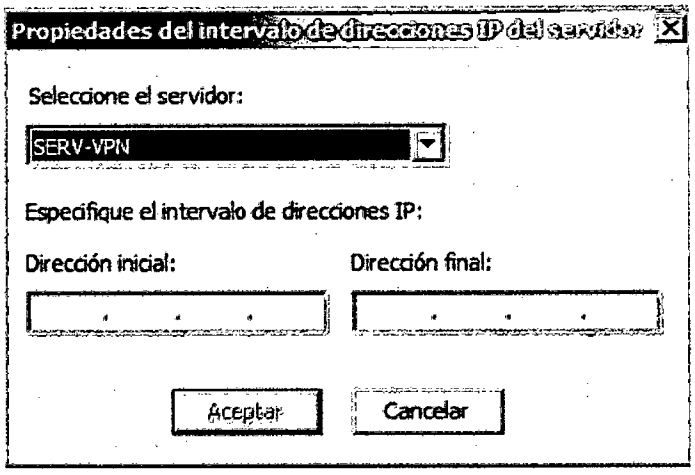
I. Configurar el método de asignación de direcciones



En este paso lo que realizaremos es seleccionar el método de asignación de direcciones, en la cual tenemos dos opciones:

a) Grupo de direcciones estáticas:

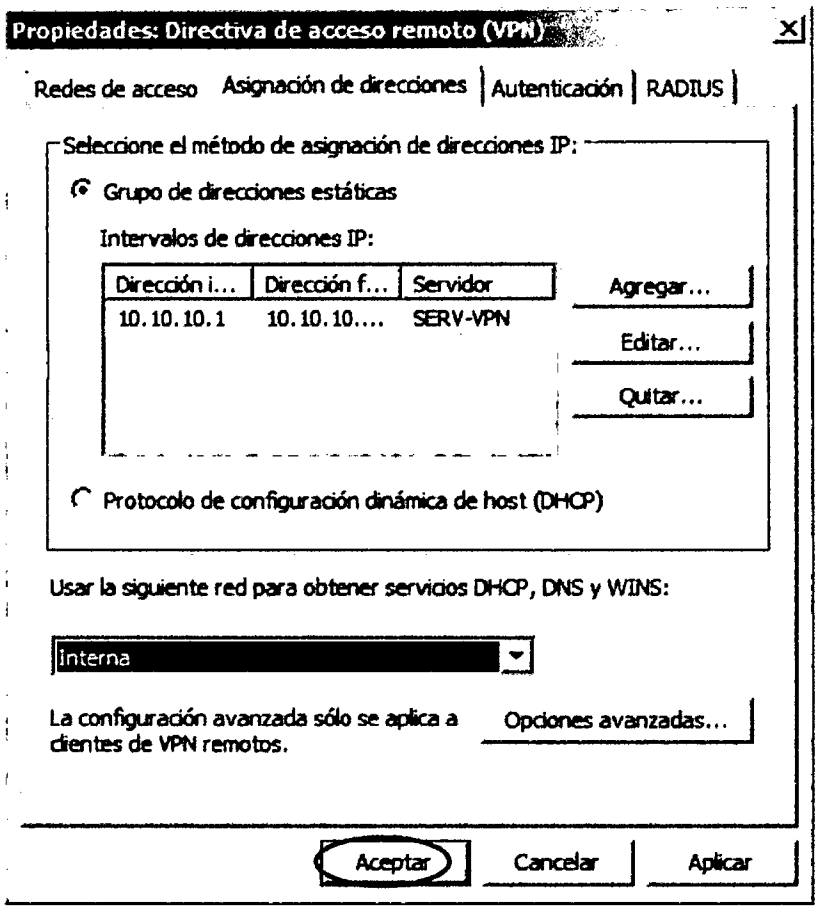
En esta opción lo que se utiliza es asignar un rango de direcciones IP para todos los clientes VPN que se conecten a nuestra red interna con su respectiva autenticación manejado en nuestro servidor de ACTIVE DIRECTORY. Para nuestro diseño utilizaremos esta opción, configurando el rango de direcciones IP desde la 10.10.10.0 hasta la 10.10.10.254.



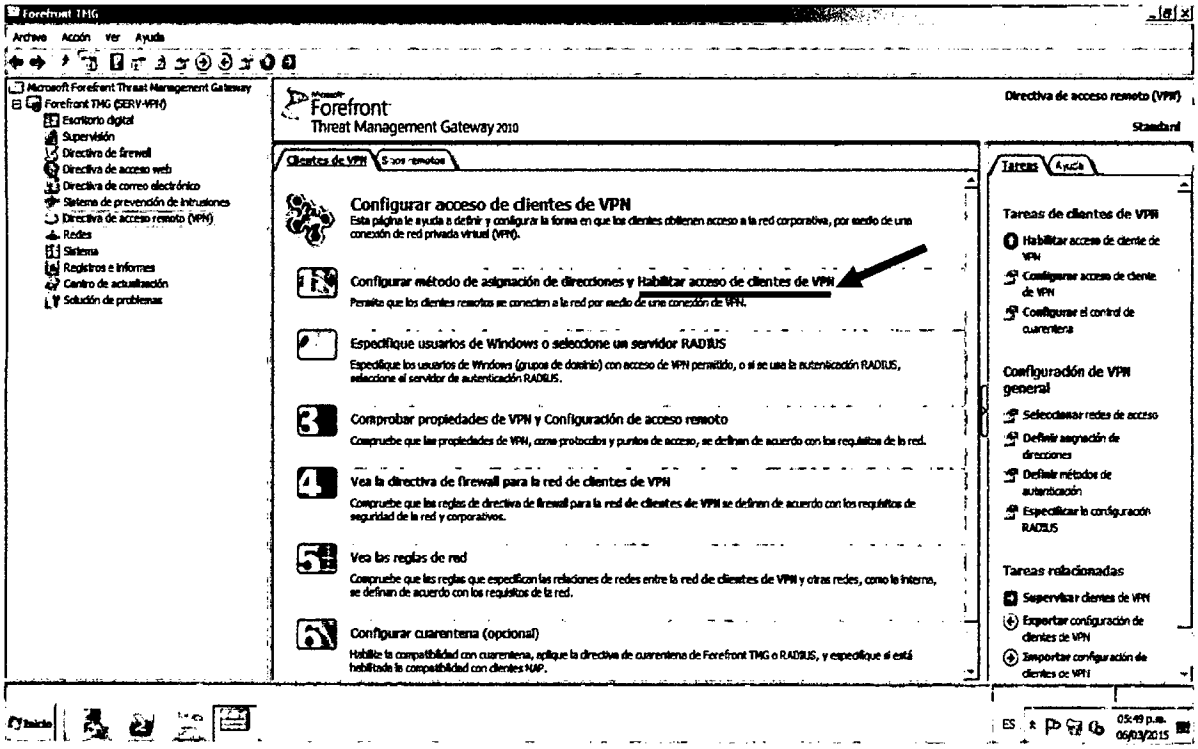
b) Protocolo de configuración dinámica de host (DHCP):

Cuando se maneja un servidor que brinda direcciones IP dinámicamente en nuestra red, podemos crear una directiva para asignar desde éste las direcciones IP para nuestro túnel VPN que configuraremos a continuación:

También se tiene que seleccionar la red (Interna o Externa) para la obtención de los servicios DHCP, DNS y WINS, como nuestros servicios se encuentran en nuestra red LAN, seleccionaremos la red INTERNA de donde va a obtener los servicios mencionados:

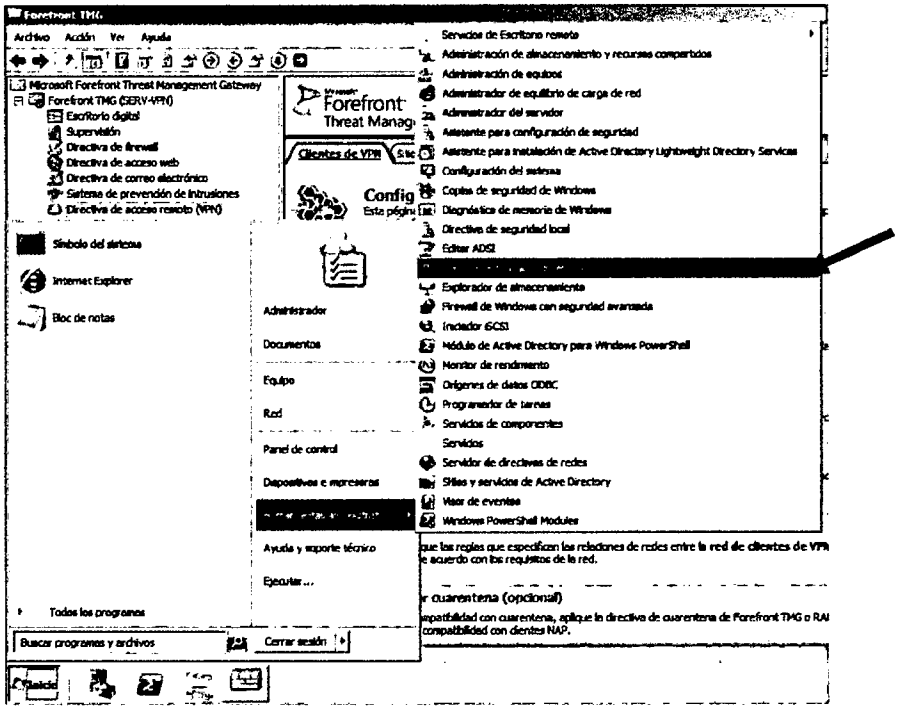


II. Habilitar el acceso de clientes vpn (habilitar roles de enrutamiento y acceso remoto).

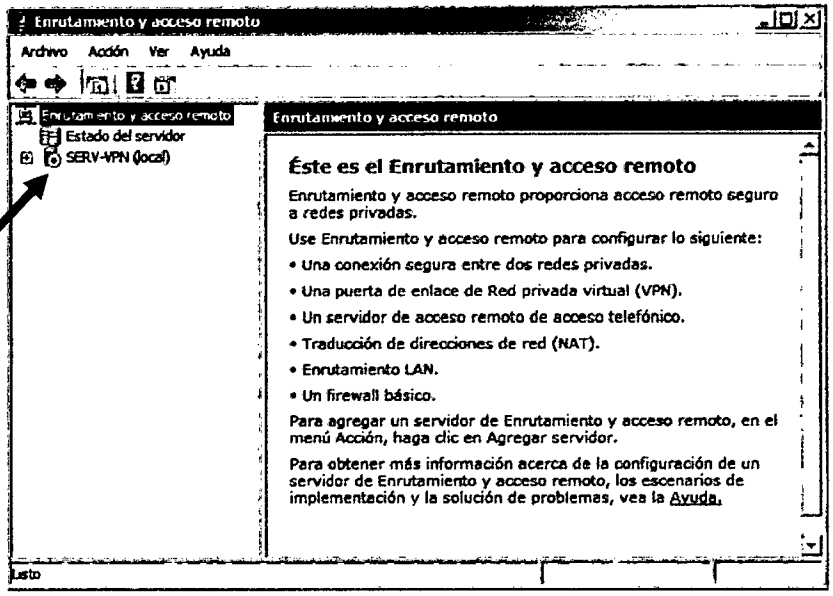


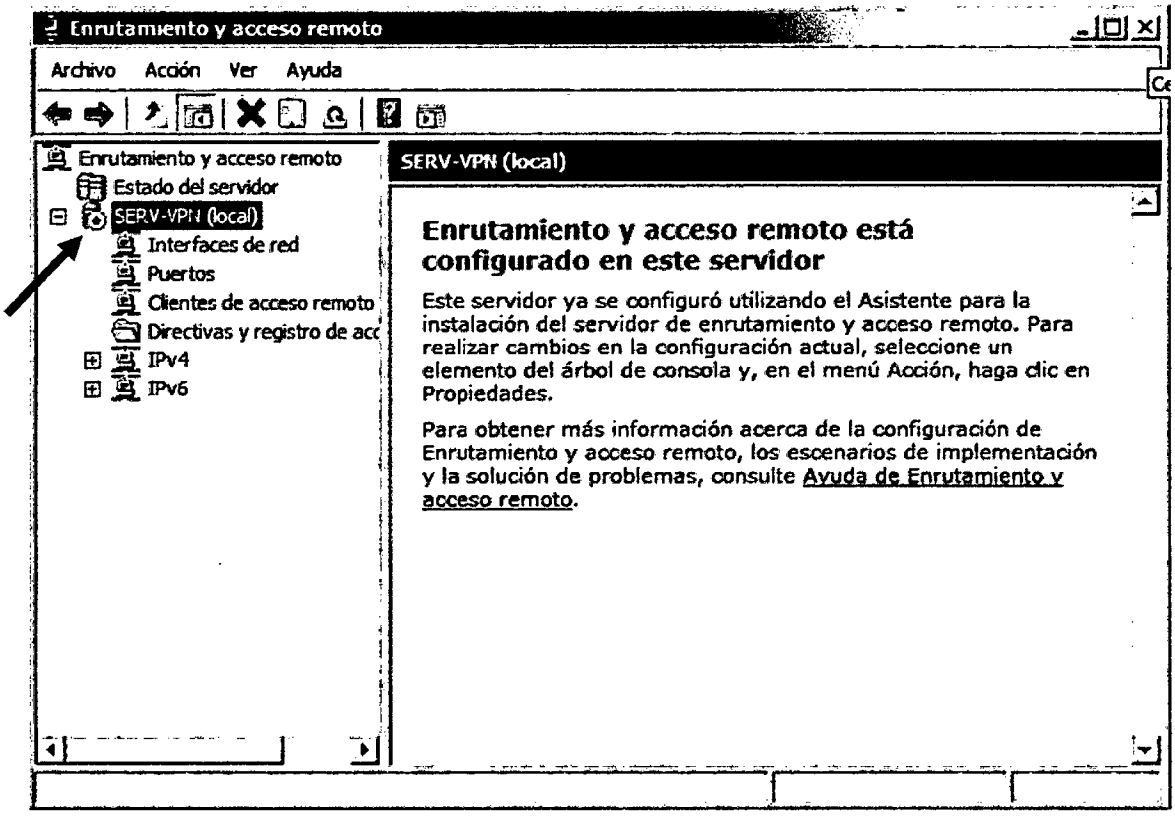
Con esta opción seleccionada estamos habilitando el ROL de Windows Server 2008 R2, con los parámetros predeterminados y establecidos por FOREFRONT TMG para su óptimo funcionamiento acoplándolo a las configuraciones de red ingresadas en FOREFRONT a la hora de la instalación y configuración inicial.

Para verificar lo antes mencionado abrimos la aplicación "Enrutamiento y acceso remoto", ubicada en: "Inicio/Herramientas administrativas/Enrutamiento y acceso remoto":



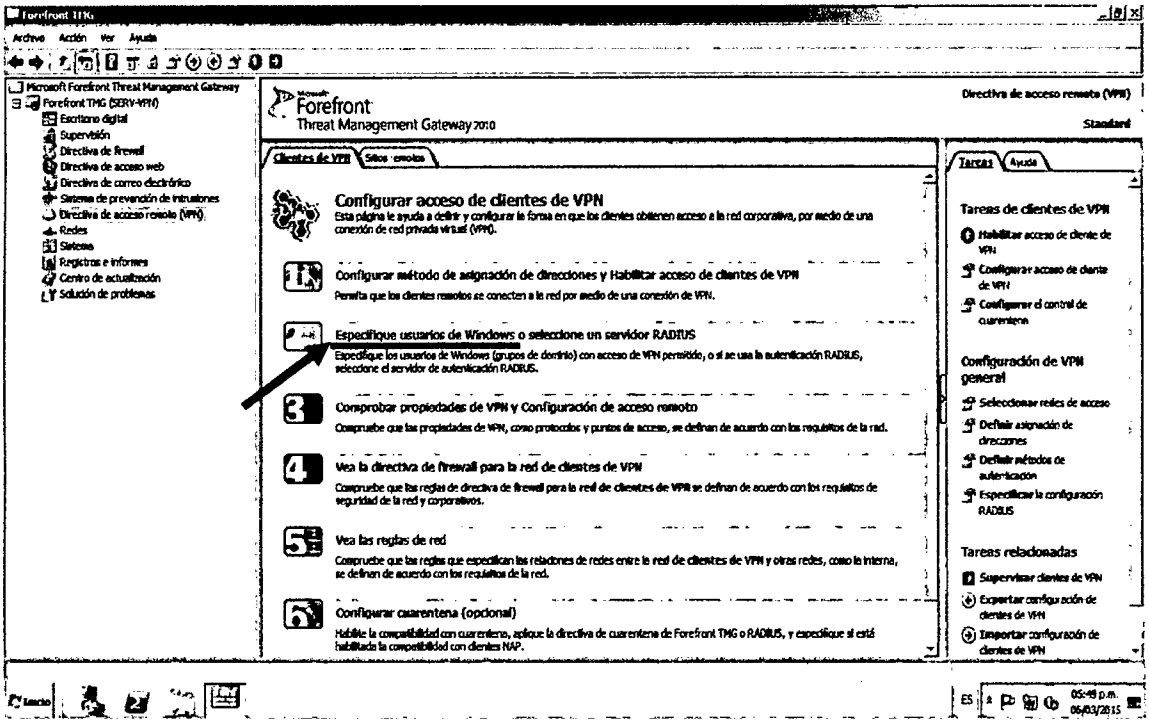
Notablemente vemos que el servicio está detenido, es que demora unos segundos o minutos de acuerdo a la capacidad de nuestro servidor, luego se pondrá en marcha:



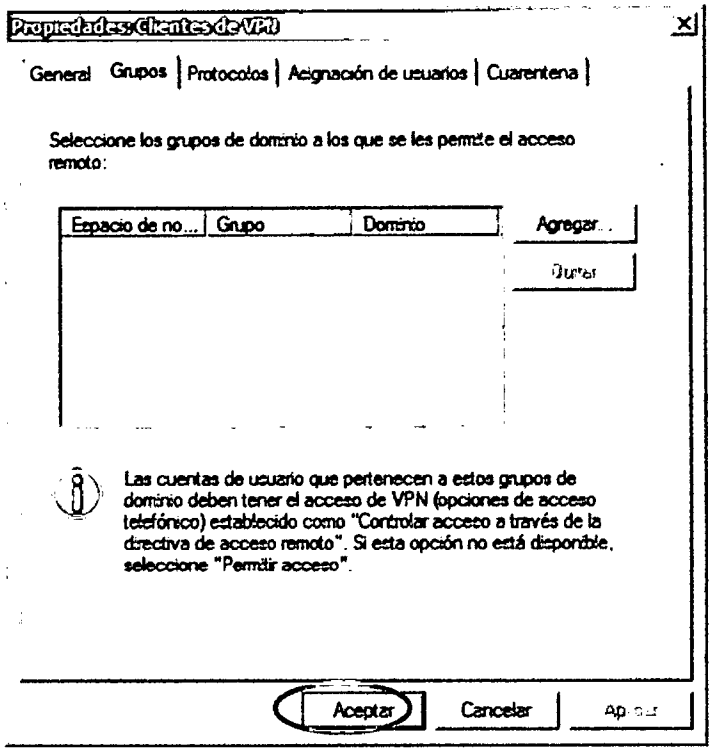


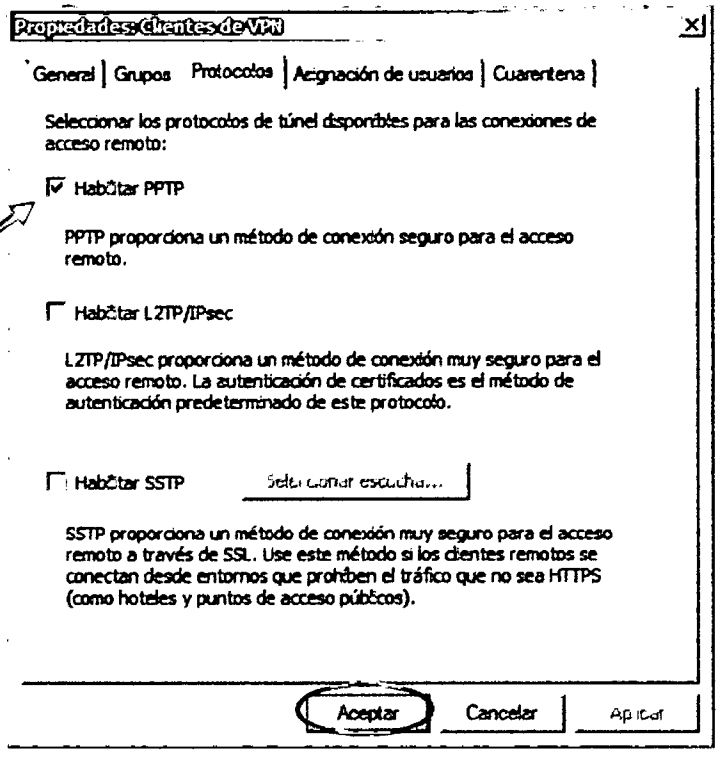
Ahora el Rol de "Enrutamiento y acceso remoto" de WINDOWS SERVER 2008 R2 ya está habilitado para realizar enrutamiento con las restricciones de ciertas políticas configuradas posteriormente en Forefront TMG para el acceso VPN.

III. Especifique usuarios de Windows.

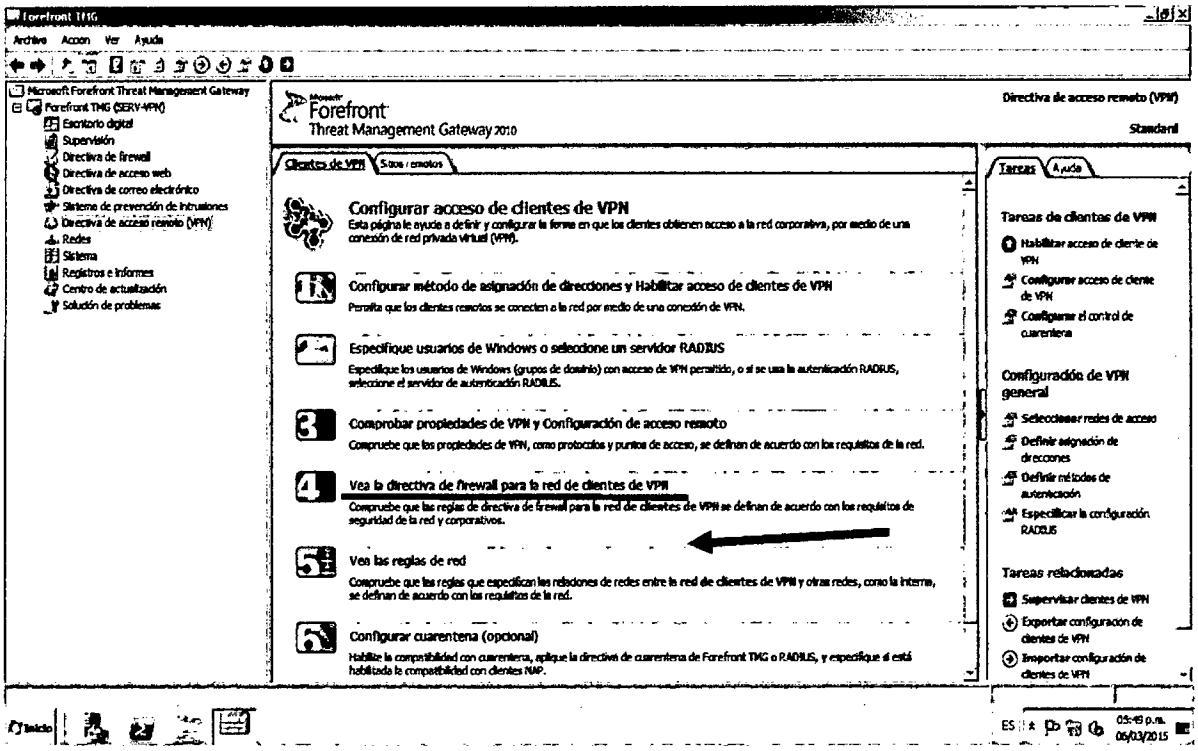


En esta opción lo que configuraremos es agregar un grupo del Dominio que tengamos creado con permisos de acceso remoto, en caso solo tengamos algunos usuarios sin grupo, no hacer cambios. También en la pestaña "Protocolos", habilitaremos el protocolo PPTP, ya que Microsoft Windows Server usa dicho protocolo para tráfico VPN, por lo que también nos brinda una conexión segura de acceso remoto.

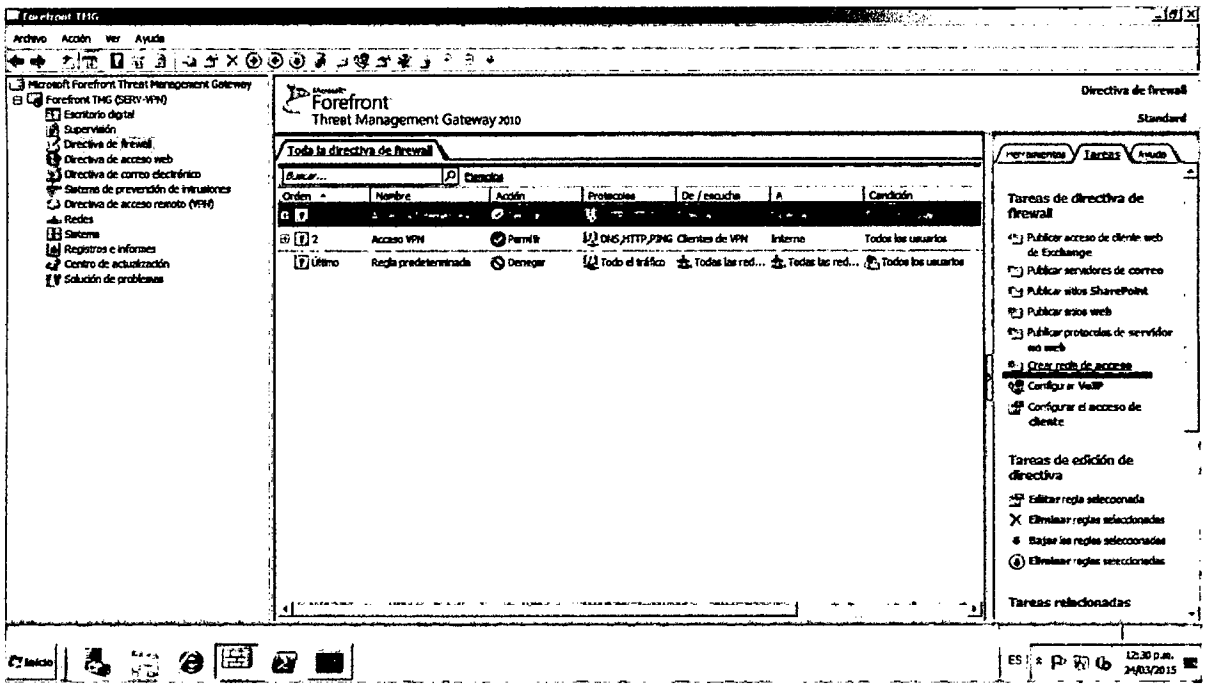




IV. Configurar la directiva de firewall para la red de clientes vpn.

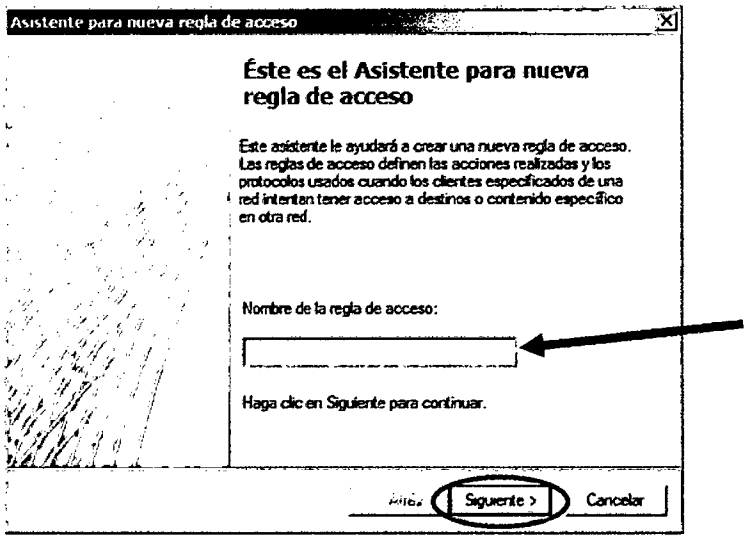


A. Crear regla de acceso: Nuestro Servidor VPN ya está configurado para realizar la conexión VPN a todos los usuarios registrados en el Active Directory con permisos de acceso remoto. Pero en cuanto al tráfico permitido hacia la red interna no lo está, para ello es que vamos a crear una regla de acceso para diversos servicios, como por ejemplo tráfico HTTP, DNS o PING. Para iniciar este proceso damos clic en "Crear regla de acceso" en el panel derecho:

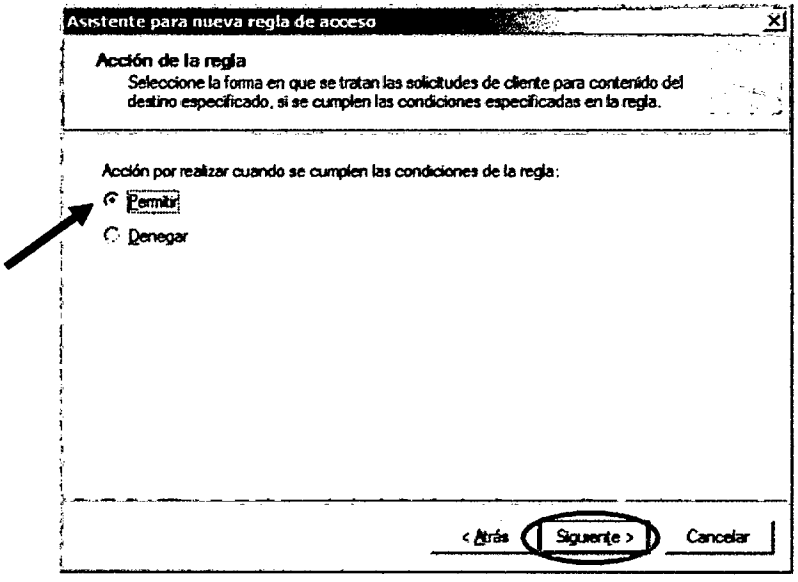


B. Crear nombre de la regla de acceso: Las reglas de acceso permiten definir en nuestro servidor FOREFRONT las acciones en la red realizadas y los protocolos usados cuando ciertos clientes de la organización de TERRACARGO internos o externos intentan tener acceso a destinos o contenidos específicos en otra red. En nuestro caso configuraremos el trafico VPN entrante desde internet y saliente desde nuestra red interna, que tenga que ver con trafico DNS, PING y HTTP para comprobar su funcionamiento.

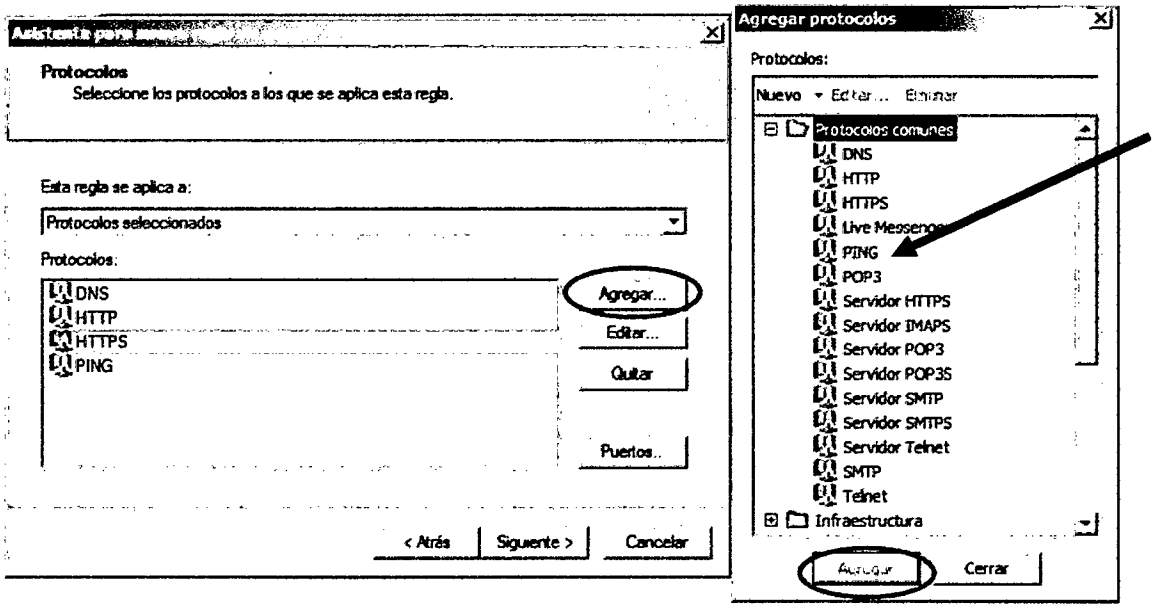
Para ello en la ventana siguiente visualizaremos el Asistente para nueva regla de acceso, en la cual Colocaremos el nombre de la regla de acceso "Acceso VPN".



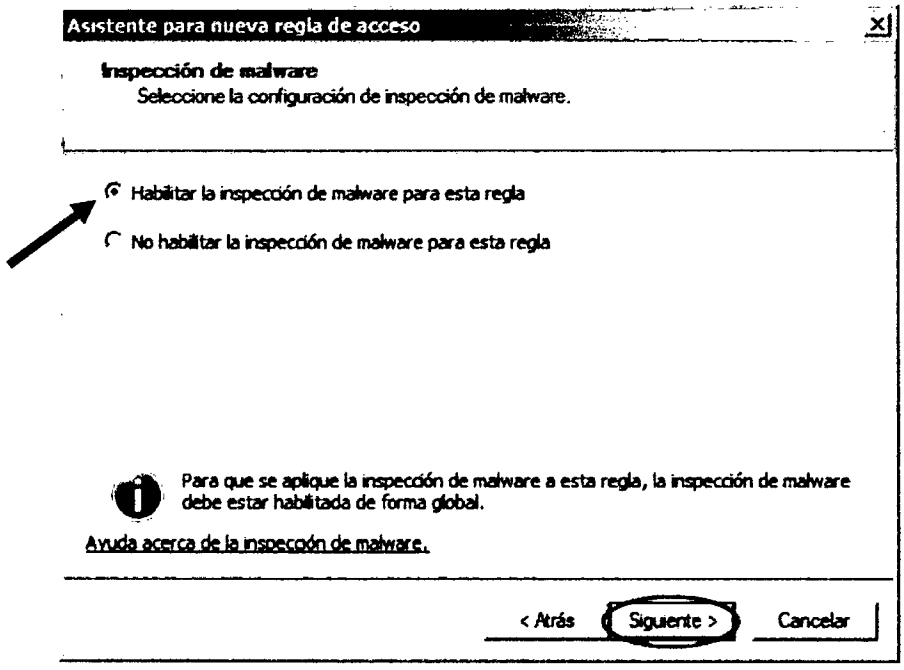
C. **Acción de la Regla**: La regla es creada con ciertas indicaciones y en esta opción indicaremos que hacer cuando se cumplan dichas condiciones. Como lo que deseamos es permitir el tráfico http, dns o ping del exterior a la red interna seleccionamos la opción "Permitir" y luego "siguiente".



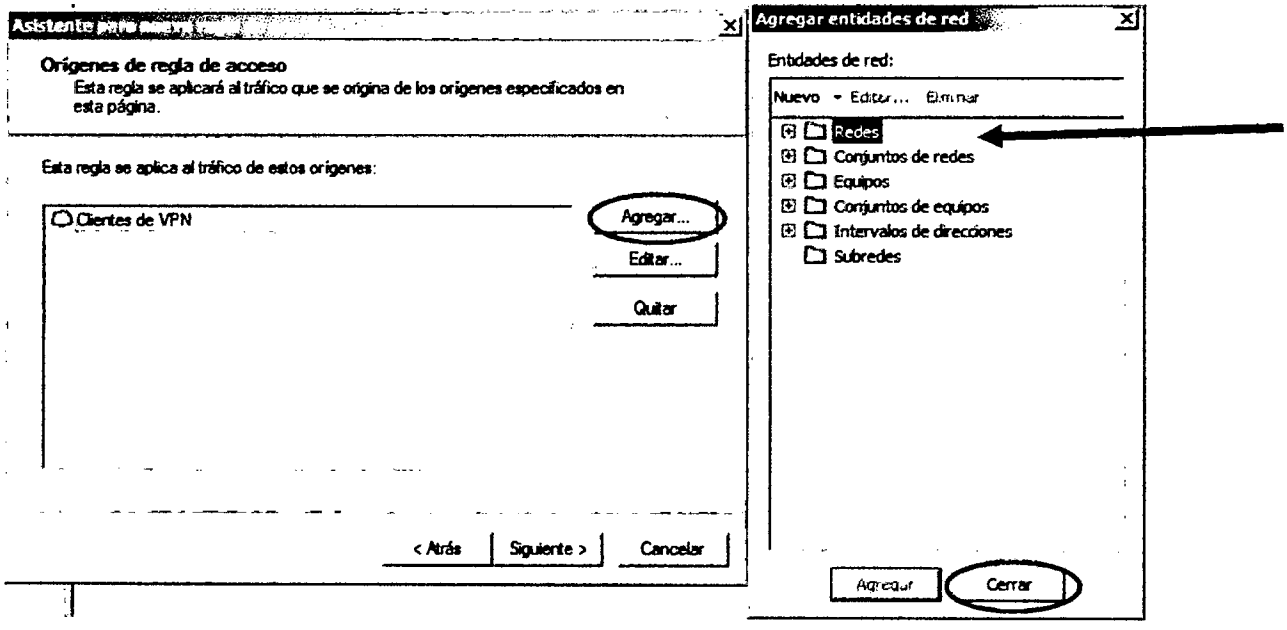
D. Protocolos: Tenemos que tener en cuenta que servicios vamos a permitir que nuestros usuarios VPN tengan acceso, por ejemplo un protocolo muy conocido "PING", lo seleccionaremos en el botón "Agregar", y luego en la ventana de AGREGAR ROLES, seleccionamos en la lista de protocolos a "PING" y seleccionamos "Agregar" y así solo los protocolos con los que trabajan los servicios que deseamos brindarle acceso a los clientes VPN para tener un mayor control de acceso.



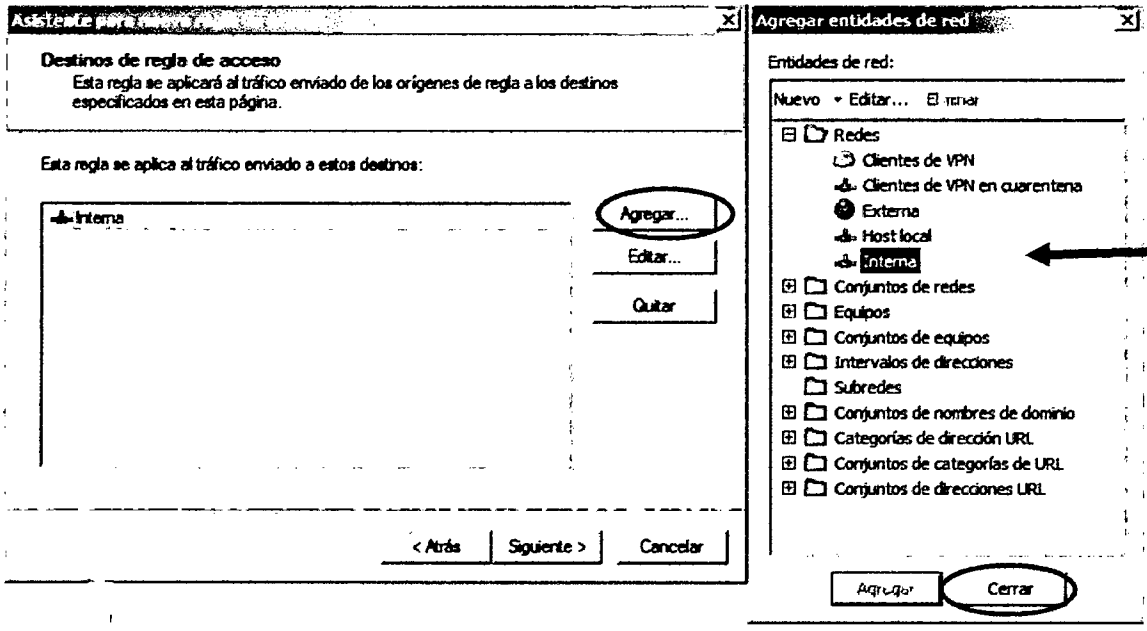
E. Inspección de malware: Todo el tráfico VPN que ingrese desde el exterior es necesario inspeccionar si contiene malware por medidas de seguridad y evitar que se provoque el mal funcionamiento de algún equipo en nuestra red interna, ya que tenemos computadoras, impresoras, servidores, teléfonos IP y otros.



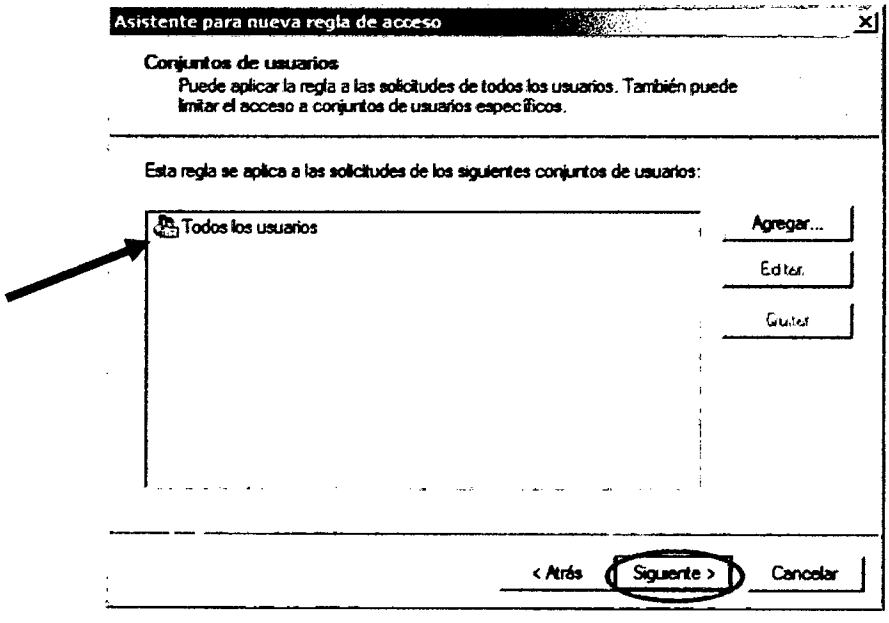
F. Orígenes de regla de acceso: Claramente aquí seleccionaremos los orígenes del tráfico que analice Forefront, seleccionando en el botón "Agregar" y en la ventana "Agregar entidades de red", en el folder REDES encontraremos una serie de orígenes ya sea tráfico exterior, interior, entre otros; en este caso solo agregaremos el tráfico proveniente de los "Clientes VPN":



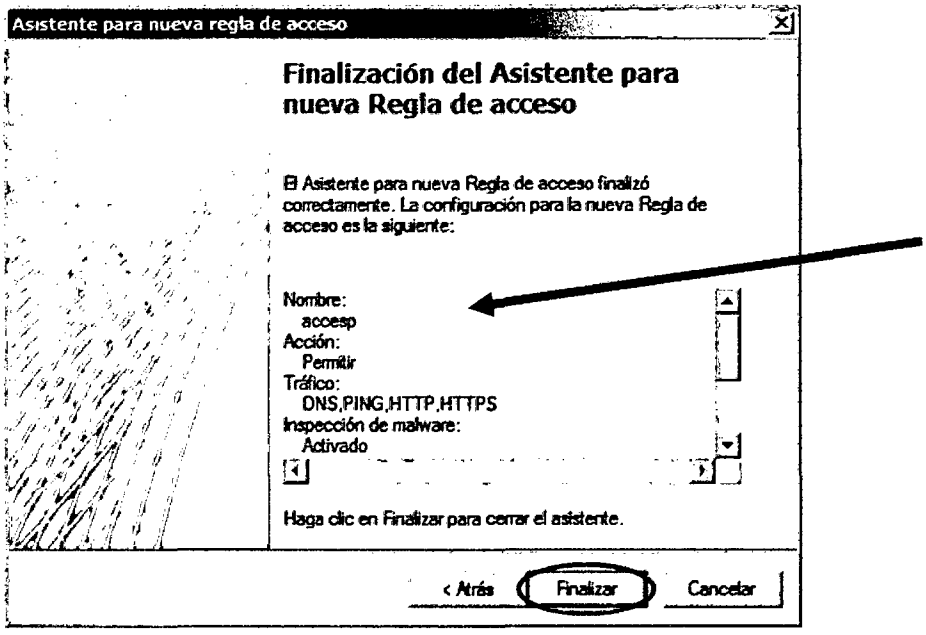
G. **Destinos de regla de acceso:** Seleccionaremos el destino del tráfico que la regla tendrá en cuenta para aplicarse, lo que los clientes VPN hacen es acceder a los servicios de nuestra organización, es decir acceder a la Red Interna, entonces ejecutaremos los pasos como se muestra la imagen:



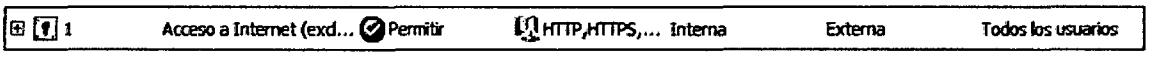
H. **Conjunto de Usuarios:** Como el manejo de todos los clientes VPN es manejado por el servidor de ACTIVE DIRECTORY, dejamos seleccionado por defecto "Todos los usuarios", los cuales son debidamente autenticado para tener acceso.



I. **Protocolos:** Luego Verificamos en el cuadro resumen sobre todas las configuraciones antes realizadas para evitar que hayan errores.



Y finalmente verificamos que la regla está creada en el panel central de nuestra consola de administración Forefront con un resumen de las características como se muestra a continuación:



5. CONFIGURACIÓN DE REDUNDANCIA DE ISP.

En este punto se describe cómo habilitar la redundancia del proveedor de acceso a Internet (ISP), en este diseño se utilizan 2 líneas de internet (Dos ISP diferentes):

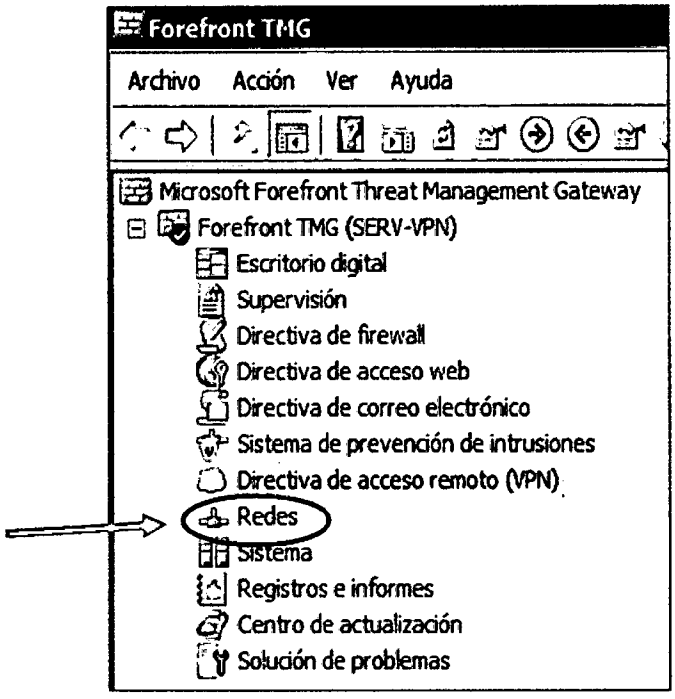
✓ Línea dedicada (2Mb): Su proveedor es Optical Networks.
✓ Línea comercial (8Mb al 10%): Su proveedor es Movistar.

Hay dos modos de redundancia de ISP:

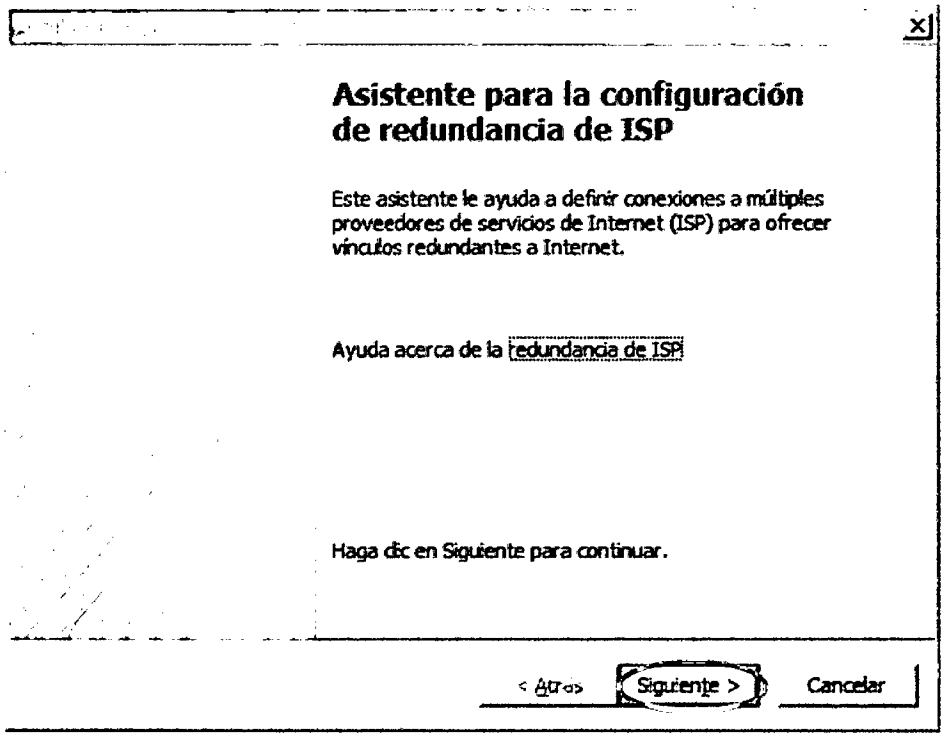
i. **El modo de alta disponibilidad** designa un vínculo principal que soporta todo el tráfico saliente de Internet y un vínculo de reserva que se activa automáticamente en caso de que el primer vínculo no funcione.
ii. **El modo de equilibrio de carga** dirige el tráfico saliente de Internet entre dos vínculos de ISP de manera simultánea y establece el porcentaje de tráfico de Internet total por vínculo. También admite la conmutación por error si uno de los vínculos no funciona.

En nuestro diseño aplicaremos el segundo modo de redundancia de ISP debido a que es mucho más eficiente y útil, ya que a que aparte realizar "balanceo de cargas", en caso de caída de uno de ellos trabaja como el modo "Alta disponibilidad"

Para realizar poder lograr esta funcionalidad, seleccionamos la opción de "Redes" en la parte izquierda del panel de la consola de administración de Forefront TMG

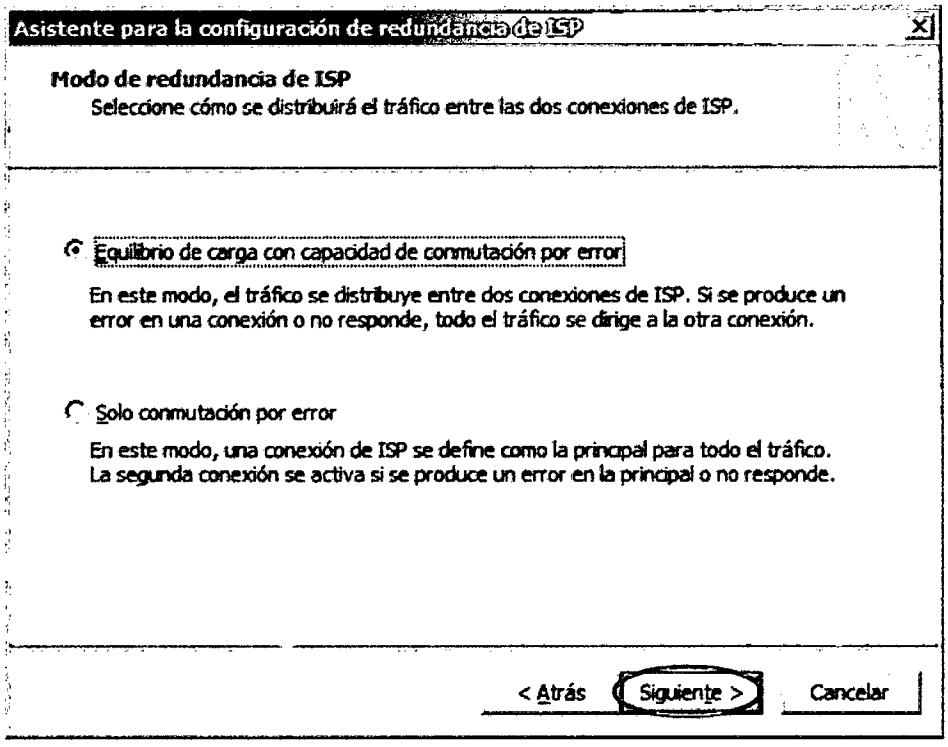


I. Asistente para la configuración de redundancia de ISP:



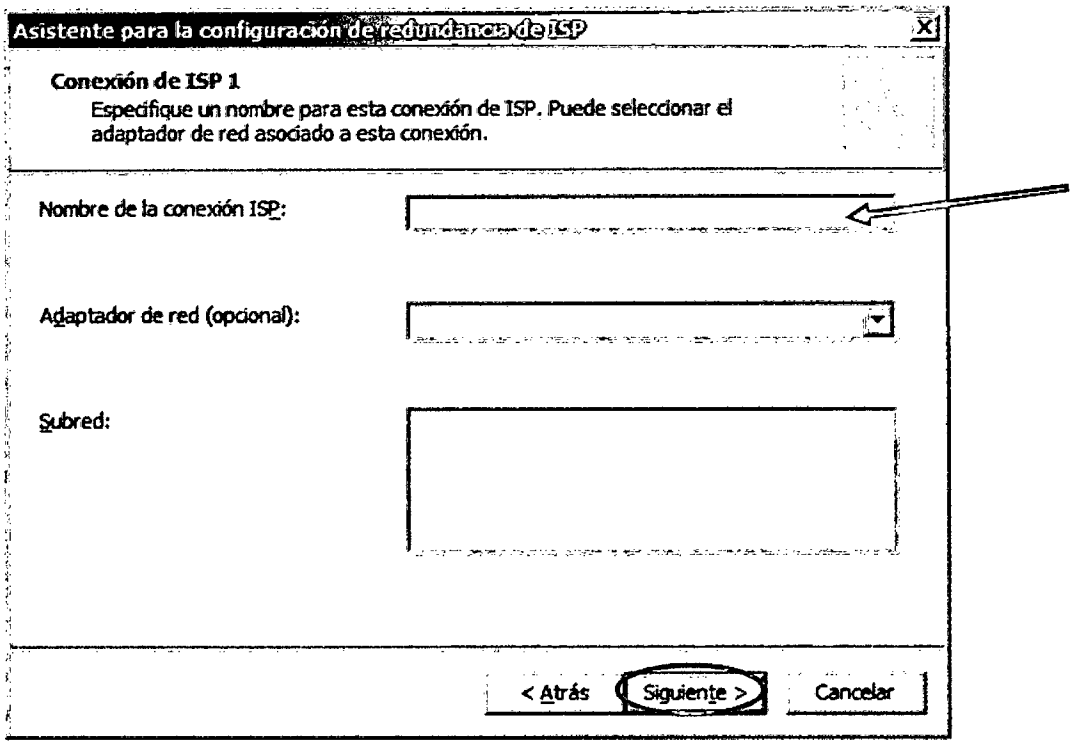
II. Modo de redundancia de ISP:

En este punto solo seleccionamos el modo de redundancia que hemos elegido para nuestro diseño y el más óptimo: "Equilibrio de carga con capacidad de conmutación por error"



III. Conexión de ISP 1:

Esta configuración corresponde a nuestro proveedor de OPTICAL NETWORKS que nos proporciona el mayor ancho de banda entre ambas líneas. Primero colocaremos el nombre de la conexión de ISP: "Optical Networks".

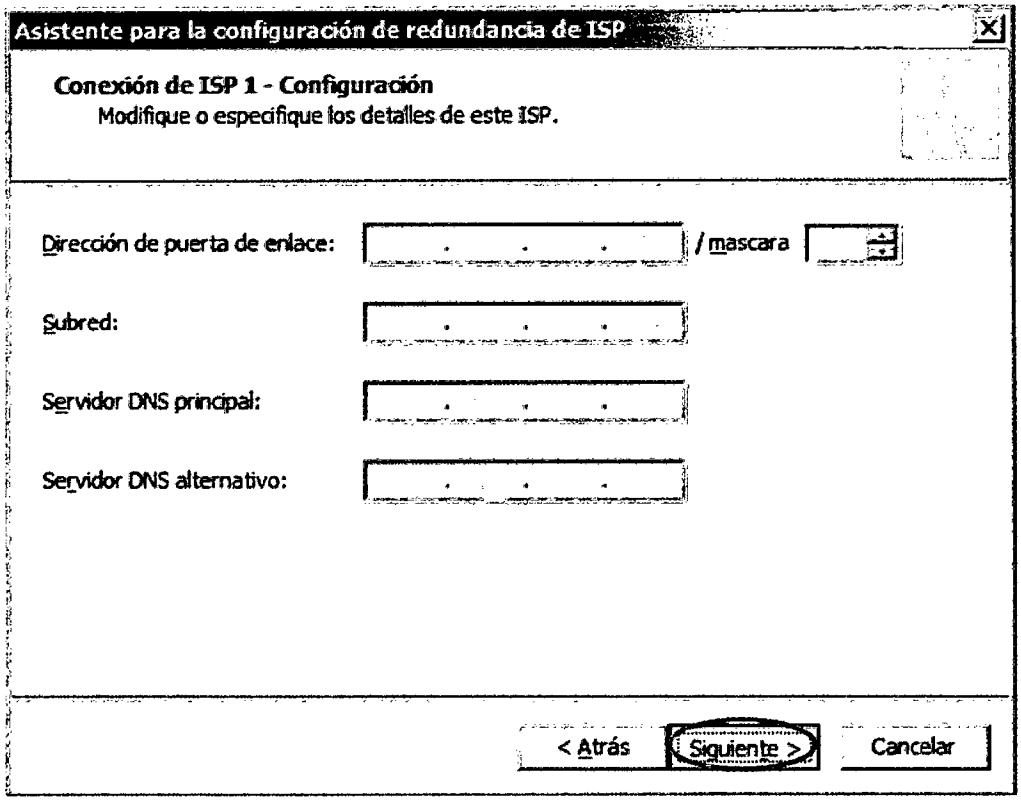


IV. Conexión de ISP 1 - Configuración:

Lo que tenemos que tener en cuenta es que en los router de los ISP están configurados en la red 192.168.0.0/24 y las direcciones IP de nuestros proveedores serán los siguientes

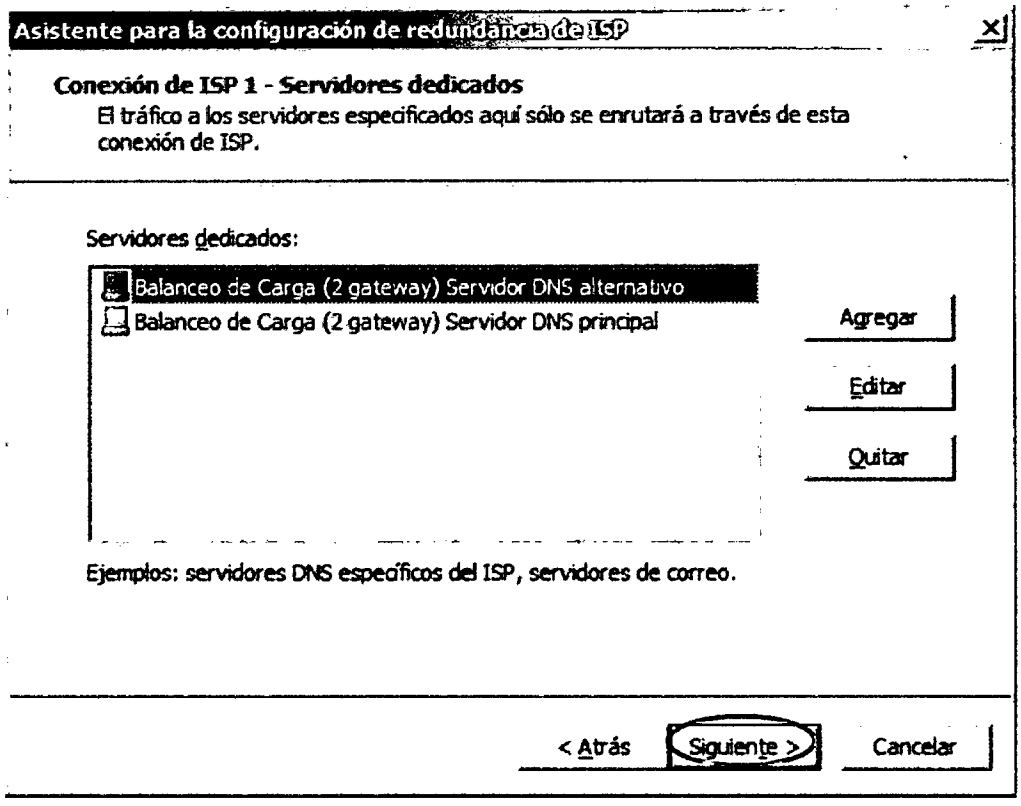
- **OPTICAL NETWORKS (ISP1)**
  - i. Puerta de enlace : 192.168.0.1
  - ii. Subred : 255.255.255.0
  - iii. DNS primario : 8.8.8.8
  - iv. DNS Alternativo : 8.8.4.4

- **INTERNET MOVISTAR (ISP2)**
  - i. Mascara de subred : 255. 255.255.0
  - ii. Puerta de enlace : 192.168.0.9
  - iii. DNS principal : 200.48.225.130
  - iv. DNS Alternativo : 200.48.225.146



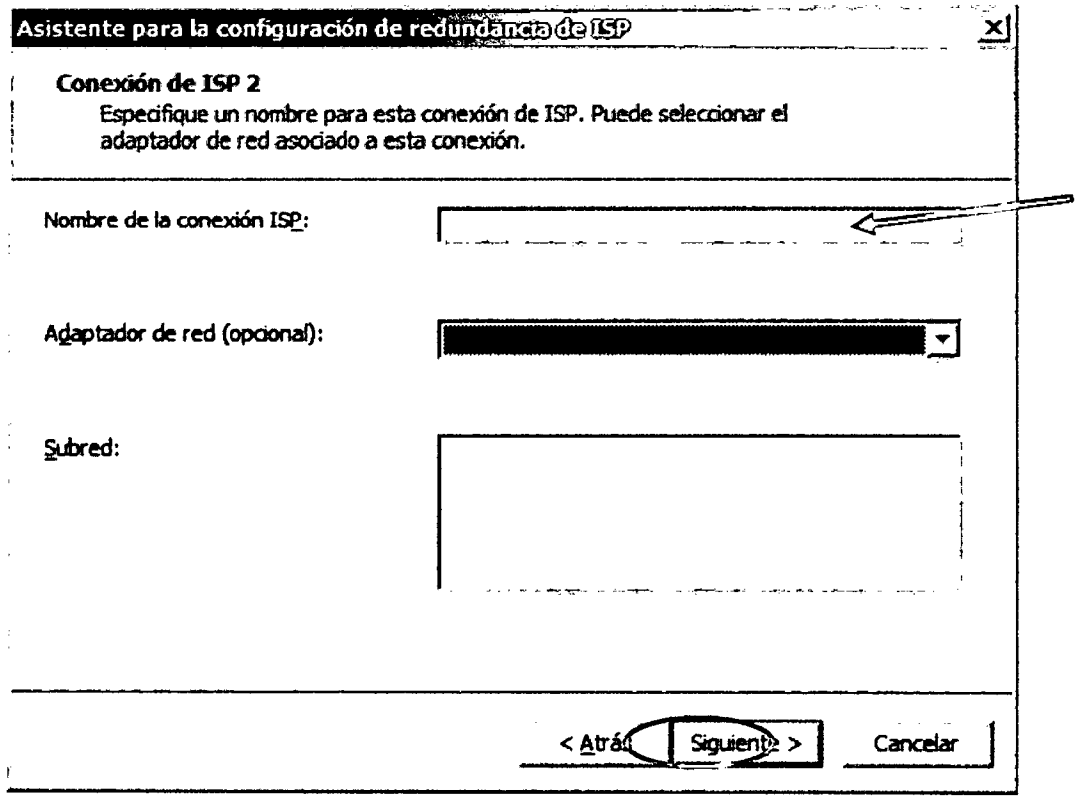
V. Conexión de ISP 1 – servidores dedicados:

Automáticamente el "Asistente para la configuración de redundancia de ISP" selecciona como balanceo de carga a los servidores DNS, ya no es necesario a no ser que deseemos agregar más servidores DNS, pero para nuestro diseño lo dejamos por defecto como se muestra:



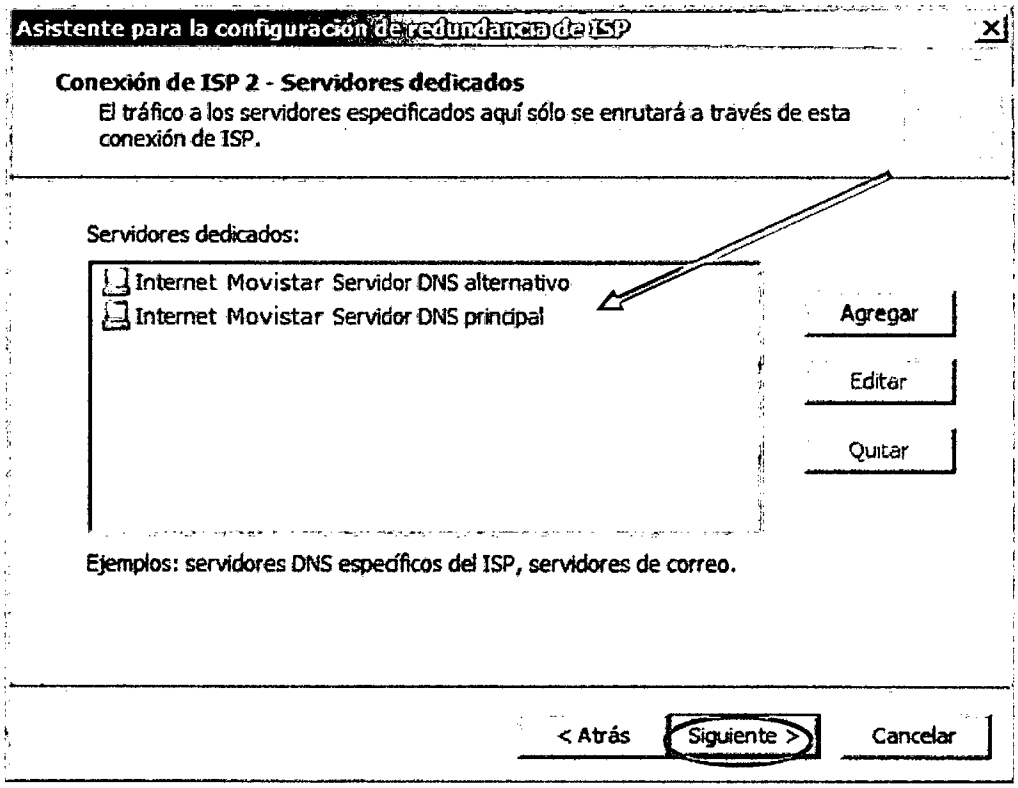
VI. Conexión de ISP 2:

Colocamos el nombre "Internet Movistar"



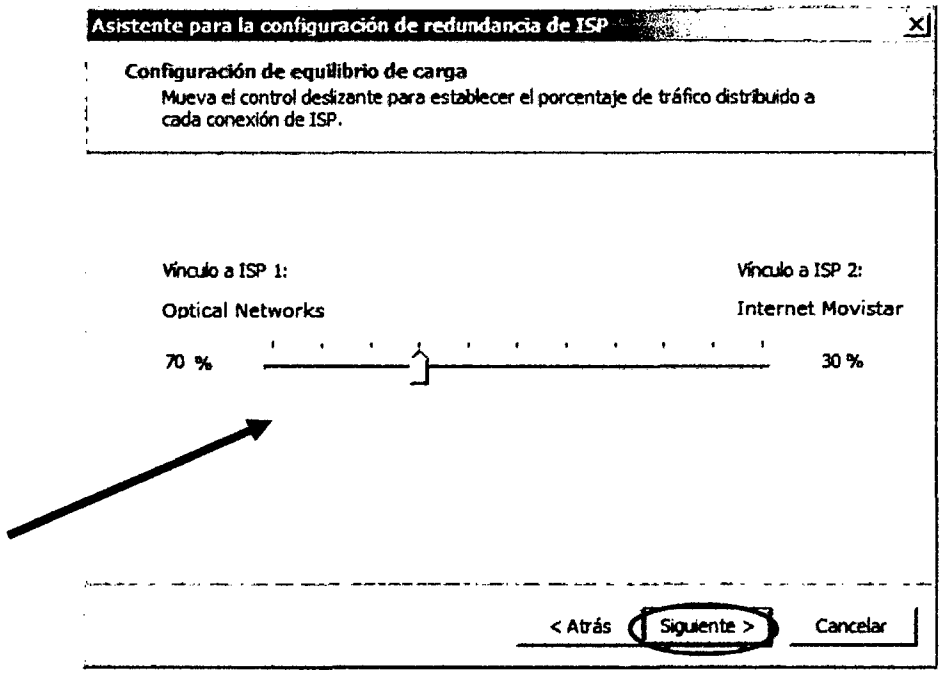
VII. Conexión de ISP 2 – Servidores dedicados:

Configuración de DNS del ISP 2



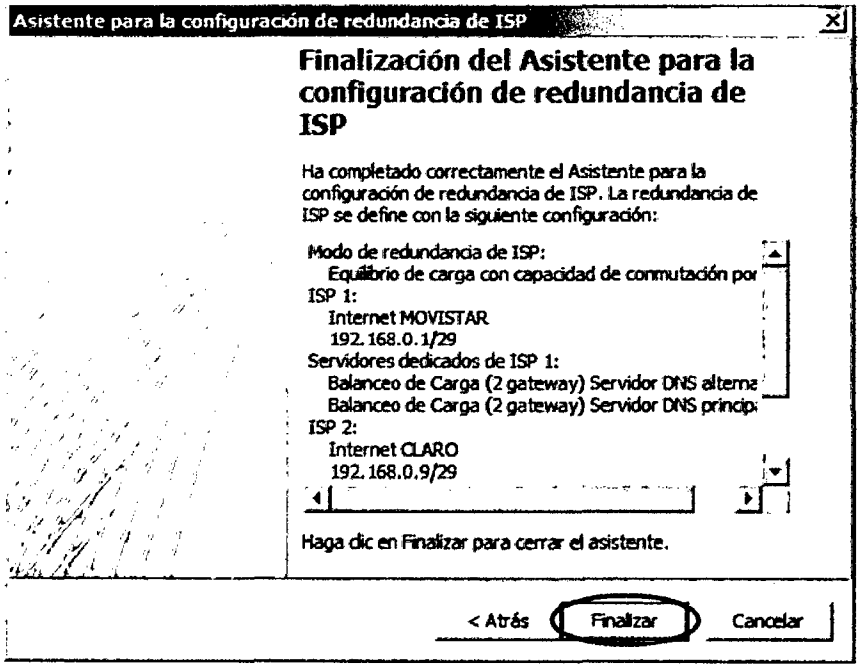
VIII. Configuración de equilibrio de la carga:

El modo configurado en este proyecto permite establecer un porcentaje por ISP para distribuir el tráfico por cada conexión y así lograr un balanceo de cargas más óptimos, En la organización Terracargo como se cuenta con una línea dedicada de 2 Mbps a la cual le asignamos un 70% del tráfico y un 30% al punto de internet de movistar por tener una línea de menor velocidad.

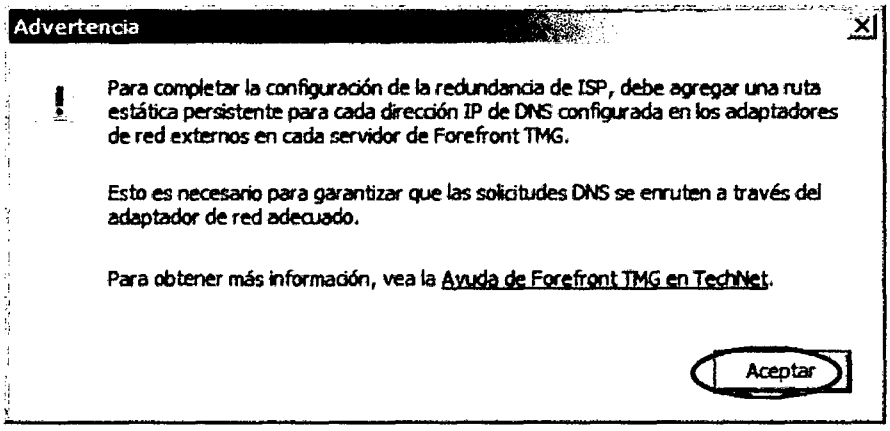


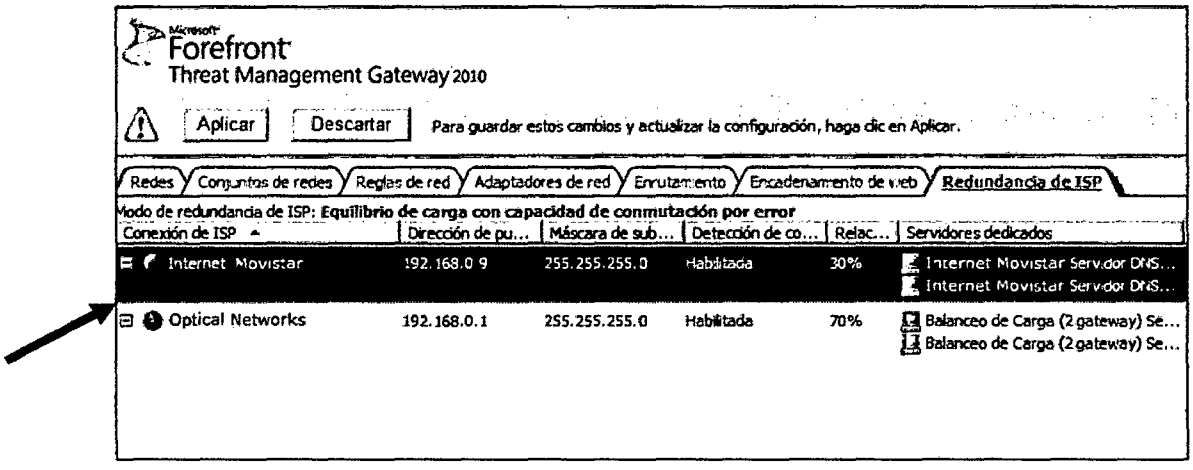
IX. Finalización del Asistente para la configuración de redundancia de ISP:

Verificaremos en la ficha resumen todas las configuraciones que estén correctas,



Nos saldrá este error debido aque tenemos que crear una ruta estática persistente para las direcciones IP de los DNS para que cada DNS sea utilizado por si propio proveedor y la ruta no sea muy larga en la búsquedad DNS. Aceptamos y aplicamos cambios para que la configuración sufra efecto.





Para solucionar la advertencia que nos salió al finalizar la configuración de Redundancia de ISP tenemos que crear rutas estáticas persistentes para asegurarse de que las solicitudes DNS se enrruta al ISP correcto, se debe agregar una ruta estática persistente para cada dirección IP de DNS configurada en el adaptador de red externo.

1. Abra una ventana Comandos y cree una ruta persistente con la siguiente sintaxis:

   route [-p] ADD [destination] MASK [netmask] [gateway] METRIC [metric] [IF interface]

   Es decir:

   route -p ADD 8.8.8.8 MASK 255.255.255.0 192.168.0.1 METRIC 1 1

   route -p ADD 8.8.4.4 MASK 255.255.255.0 192.168.0.1 METRIC 1 1

   route -p ADD 200.48.225.130 MASK 255.255.255.0 192.168.0.9 METRIC 1 1

   route -p ADD 200.48.225.146 MASK 255.255.255.0 192.168.0.9 METRIC 1 1

   Observe los siguientes parámetros:

   - "p", hace que la ruta sea persistente entre arranques del sistema.
   - "METRIC", especifica la prioridad de esta ruta; la ruta con la métrica más baja tiene la máxima prioridad.
   - "IF interface", especifica el número de interfaz de esta ruta.

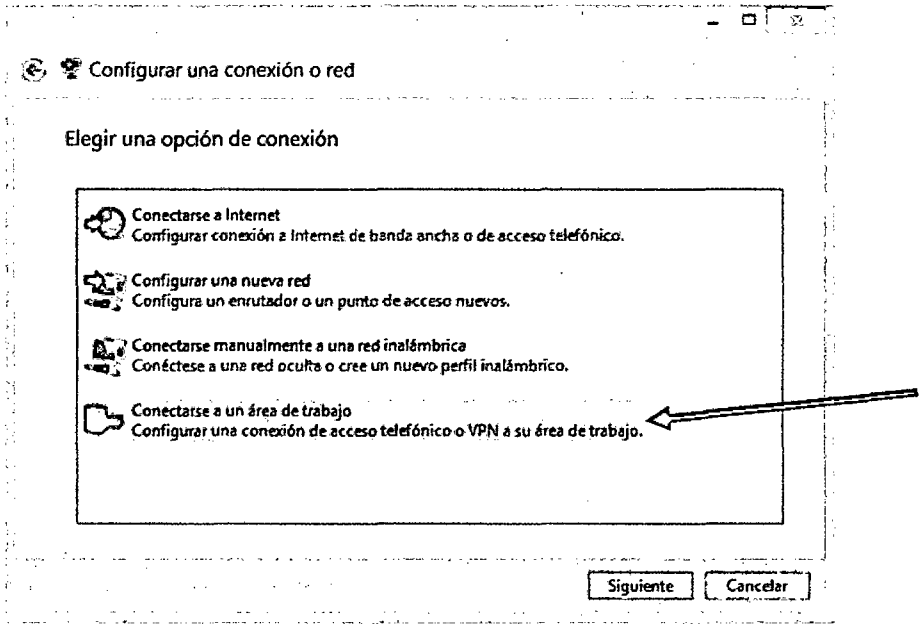
   Para PPTP hay que abrir el puerto TCP 1723 y abrir también el protocolo con el Id. 47 (GRE) en ambos router de cada ISP para que pueda dejar pasar dicho tráfico, direccionado a nuestro servidor VPN con dirección IP 192.168.0.2.

   Y finalmente ya tenemos configurado nuestro servidor VPN con Microsoft Forefront TMG, listo para realizar las conexiones VPN desde cualquier sucursal del Perú de TERRACARGO SAC

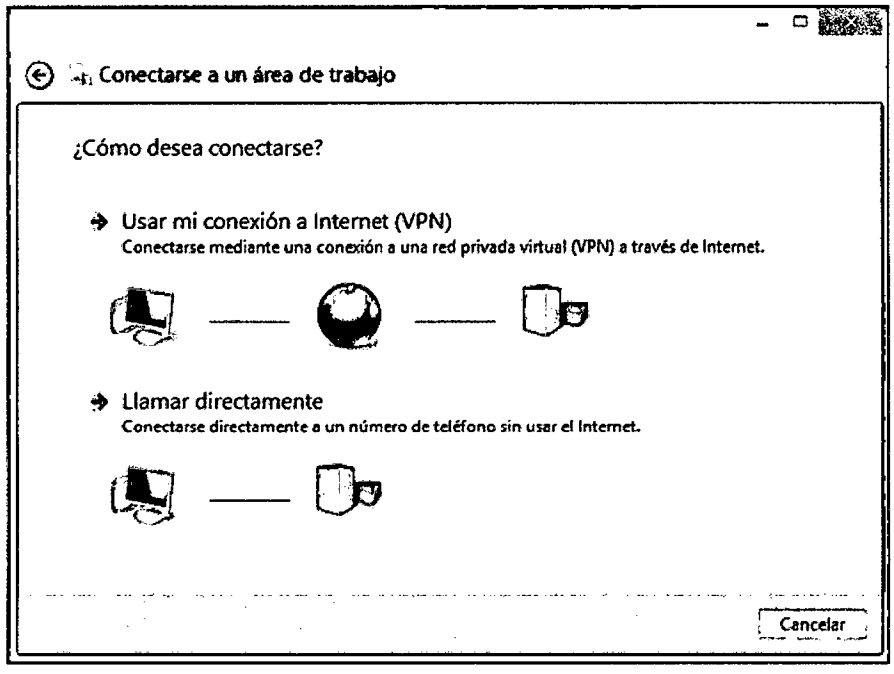
6. CONFIGURAR CLIENTE VPN

Para comprobar el funcionamiento de nuestro servidor VPN vamos a cualquier computadora con internet y realizamos el siguiente procedimiento:

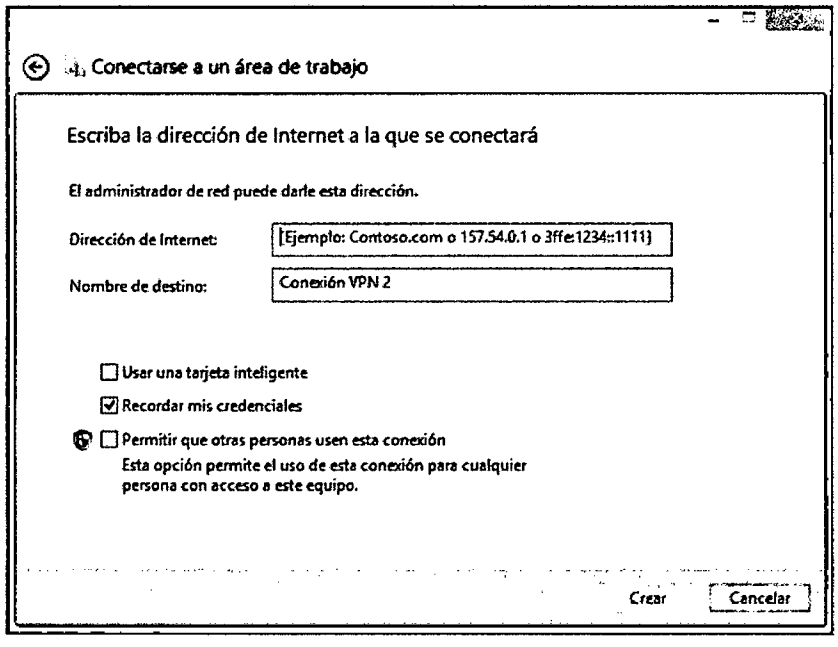
I. Abrimos el "Centro de redes y recursos compartidos" ubicados en el PANEL DE CONTROL y seleccionamos la opción "Agregar una nueva red de trabajo", luego en "Conectarse a un área de trabajo" y "Siguiente".



II. Ahora seleccionamos "Usar mi conexión a Internet (VPN)".



III. Ahora ingresamos la IP pública con la que trabaja nuestro router de "Optical Networks" o de "Internet Movistar" para poder acceder a la VPN.



Y Finalmente damos Conectar conexión VPN en la lista de redes, e Ingresar el Usuario del Domino con su respectiva clave para autenticarse registrados en el servidor de cuentas de usuarios Active Directory con permisos de acceso VPN