UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

INFORME TÉCNICO

IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL EN EL GOBIERNO REGIONAL DE HUANCAVELICA

PRESENTADO POR:

BACH. JAVIER GUSTAVO CHINO MONTES

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS Y COMPUTACIÓN

HUANCAYO - PERÚ

2017

Dr. CASIO AURELIO, TORRES LÓPEZ

PRESIDENTE

……

JURADO

……..

JURADO

……..

JURADO

Mg. MIGUEL ÁNGEL, CARLOS CANALES

SECRETARIO DOCENTE

DEDICATORIA

Dedico este trabajo primeramente a Dios por guiarnos y darnos fuerzas para seguir adelante. A mis progenitores que me inculcan valores de responsabilidad y dedicación hacia la superación y el esfuerzo continuo para cumplir toda meta anhelada y llevarnos por la senda del bien.

Javier Gustavo Chino Montes.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

RESUMEN

El presente informe, trata sobre la implementación de una Red Privada Virtual en el Gobierno Regional de Huancavelica, para ello se tiene identificado el problema general ¿Cómo interconectar la Sede Central del Gobierno Regional de Huancavelica y sus locales descentralizados?, con el problema definido plantearemos los objetivos a alcanzar el cual es interconectar el local central y sus locales descentralizados de la entidad, logrando así la transmisión de voz, datos y video; además de distribuir adecuadamente el servicio de internet en cada una de ellas, priorizando aquellas que manejan sistemas administrativos de la entidad como el Sistema Integrado de Gestión Administrativa – SIGA - MEF, Sistema Integrado de Administración Financiera – SIAF - SP, Sistema Único de Planillas – SUP y Telefonía VoIP, utilizando un ancho de banda considerable en cada uno de los locales involucrados.

Para lograr estos objetivos se ha utilizado la metodología para implementar proyectos de redes de James McCabe (Top Down).

Llegando a la conclusión que se logró interconectar la Sede Central del Gobierno Regional de Huancavelica y todos sus locales descentralizados, por medio de la implementación de una red privada virtual (VPN) a través del software Forefront TMG 2010 con ello mejora la calidad del servicio de transmisión de datos, la escalabilidad y la seguridad en la transmisión de datos, voz y video; podemos remitirnos a las pruebas efectuadas en el capítulo V del presente.

ABSTRACT

This report deals with the implementation of a Virtual Private Network in the Regional Government of Huancavelica, for this the general problem has been identified. How to interconnect the Headquarters of the Regional Government of Huancavelica and its decentralized premises ?, with the defined problem we will pose the objectives to be reached which is to interconnect the central premises and its decentralized premises of the entity, thus achieving the transmission of voice, data and video; In addition to properly distribute the Internet service in each of them, prioritizing those that manage administrative systems of the entity such as the Integrated Management System - SIGA - MEF, Integrated Financial Management System - SIAF - SP, Unique System of Returns - SUP and VoIP Telephony, using a considerable bandwidth in each of the premises involved.

To achieve these objectives, the methodology used to implement network projects by James McCabe (Top Down) has been used.

Arriving at the conclusion that it was possible to interconnect the Headquarters of the Regional Government of Huancavelica and all its decentralized premises, by means of the implementation of a virtual private network (VPN) through the software Forefront TMG 2010 thereby improving the quality of the service of data transmission, scalability and security in data, voice and video transmission; we can refer to the tests carried out in chapter V of the present.

INTRODUCCIÓN

El presente informe consta de 5 capítulos en los cuales describimos detalladamente sobre la implementación de una Red Privada Virtual (VPN) en el Gobierno Regional de Huancavelica, a través del software Forefront TMG 2010.

En el primer capítulo, presentamos el Planteamiento del Problema que contiene Identificación y determinación del problema, formulación del problema, objetivos importancia, Factibilidad y alcances de la investigación.

En el segundo capítulo, se realiza el marco teórico concerniente a antecedentes de estudio, bases teóricas y fundamentos de las redes privadas virtuales, como lo son los protocolos involucrados, definición de términos básicos, que ayudan a conocer y comprender todo el desarrollo del informe técnico, además la metodología para la implementación de la VPN.

El tercer capítulo, hace referencia a la definición de requerimientos que comprende: el diagnóstico y análisis de la rede de comunicación actual, determinación de los requerimientos basados en las necesidades de la organización, diagrama de la red, mapas y planos de ubicación.

El cuarto capítulo, comprende la implementación de la Red Privada Virtual constituyendo la idea central del informe técnico, ya que trata sobre la configuración de los servidores, que va desde la instalación del directorio activo hasta dar de alta al usuario con los privilegios de conexión remota por medio del servidor de VPN.

Se muestra la instalación y configuraciones del software Forefront TMG 2010, se detalla paso a paso su implementación de la VPN y la creación de las directivas de firewall basados en sus requerimientos.

En el capítulo cinco, muestra las pruebas del modelo y el desempeño del mismo desde la configuración de un cliente VPN en un sistema operativo Windows Seven, la verificación de conexiones y servicios que accede el cliente a través de la red VPN mostrando los resultados obtenidos.
Finalizamos, con las conclusiones, recomendaciones y referencia bibliografica.

El Autor.

GENERALIDADES

CAPITULO I

ASPECTOS GENERALES

1.1 SITUACIÓN PROBLEMÁTICA

El Gobierno Regional de Huancavelica es un organismo del sector público cuyo fin es administrar con eficiencia y transparencia la gestión pública regional, ante ello en los últimos años la institución viene presentando problemas e inconvenientes en la plataforma de comunicaciones a nivel institucional entre la Sede central del Gobierno Regional de Huancavelica y sus locales descentralizados ubicados en distintos lugares geográficos de la cuidad de Huancavelica. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes deberían de cumplir con atributos tales como seguridad, fiabilidad, 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 sedes remotas a varios kilómetros de distancia.

El Gobierno Regional de Huancavelica cuenta con sistemas administrativos como el SIAF, SIGA, SUP; una comunicación a través de telefonía VoIp y dominio regional los cuales dependen de un correcto funcionamiento de la red entre la sede central y sus diferentes locales descentralizados.

Ante la necesidad de comunicar puntos remotos, se plantea la forma de utilizar redes públicas para comunicar estas dependencias a través de una Red Privada Virtual (VPN), en la cual los usuarios de los diferentes locales descentralizados del Gobierno Regional de Huancavelica podrán comunicarse de forma libre y segura pudiendo acceder a los sistemas mencionados ubicados en la sede central de la institución a través de las redes públicas.

En este trabajo se propone la implementación de una Red Privada Virtual a través del Forefront TMG 2010 donde se plantea interconectar la sede central a través de un túnel con cada uno de los locales descentralizados del Gobierno Regional de Huancavelica de tal manera que nos permita mejorar la calidad del servicio de transmisión de datos, mejorar la escalabilidad y sobre todo mejorar la seguridad en la transmisión.

1.1.1 Definición del Problema

El problema general del proyecto es: ¿Cómo interconectar la Sede Central del Gobierno Regional de Huancavelica y sus locales descentralizados ubicados en distintos lugares geográficos de la cuidad de Huancavelica?

Del cual sus problemas específicos son los siguientes:

a) ¿Cómo determinar los requerimientos actuales de la infraestructura de comunicaciones del Gobierno Regional de Huancavelica, para mejorar la plataforma de comunicación entre los distintos locales descentralizados de la entidad?
b) ¿Cómo diseñar la Infraestructura de Red del Gobierno Regional de Huancavelica, para mejorar la calidad del servicio de transmisión de datos?

1.2 OBJETIVOS

1.2.1 Objetivo General

Interconectar la Sede Central del Gobierno Regional de Huancavelica y sus locales descentralizados ubicados en distintos lugares geográficos de la cuidad de Huancavelica a través de la implementación de una Red Privada Virtual (VPN).

1.2.2 Objetivos Específicos

a) Determinar los requerimientos actuales de la infraestructura de comunicaciones del Gobierno Regional de Huancavelica, para mejorar la plataforma de comunicación entre los distintos locales descentralizados de la entidad.

b) Diseñar la Infraestructura de Red del Gobierno Regional de Huancavelica, para mejorar la calidad del servicio de transmisión de datos.

1.3 FACTIBILIDAD

1.3.1 Factibilidad Técnica

Evaluamos diferentes consideraciones técnicas para la realización del estudio, así tenemos:

✓ **En Red de Área Local**

El Gobierno Regional de Huancavelica actualmente cuenta con una Red de Área Local, también con un Cableado Estructurado Certificado a nivel de todos sus órganos estructurados.

✓ **Sistemas Operativos de Red**

Las redes evolucionadas tienen capas de servicios que hacen lo que llamamos el ambiente operativo para la red. La interoperabilidad y los servicios integrados basados en redes muy completas o estrechamente

integradas son las características primordiales de un ambiente operativo en red.

En la actualidad existen diferentes sistemas operativos de red que trabajan bajo el esquema cliente/servidor. El sistema operativo de red a utilizar es:

- Windows Server 2008 R2

✓ **Software para la VPN**

- Forefront TMG 2010

✓ **Topología de Red**

- La topología de red implementada es: Topología Estrella

✓ **Tipos de Redes de Transmisión de Datos**

En la actualidad existen tecnologías, normas, protocolos que nos permite la transmisión de diferentes tipos de información (video, voz, gráficos, datos) a través de las redes por diferentes medios físicos (cable de cobre, fibra óptica o radio).

✓ **El tipo de red a utilizar es:**

- Fast Ethernet

✓ **El tipo de medio de transmisión a utilizar es:**

- Par trenzado

✓ **El tipo de acceso al medio a utilizar es:**

Las normas a tener en cuenta serán las Normas 802 del IEEE como Ethernet 802.3u, 802.5, 802.12.

✓ **Sistema de Cableado**

Para el cableado de la red de datos se deben seguir las normas de cableado dadas por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), Norma 568 de Cableado EIA/TIA, los cuales proporcionará facilidades para un futuro crecimiento de la red y configuraciones de la misma.

Por tanto considerando los factores técnicos señalados, se concluye que de acuerdo a las nuevas tecnologías de redes y comunicaciones actuales el proyecto es técnicamente factible.

1.3.2 Factibilidad Económica

La implementación de la Red Privada Virtual (VPN), no generó inversión alguna a la institución, ya que el Gobierno Regional de Huancavelica actualmente cuenta con un servidor de última generación, licencia del Windows Server 2008 R2, Licencia del Forefront TMG 2010 una línea dedicada de 6 Mbps al 100%. En cuanto a los servicios de Instalación y Configuración del servidor y de las estaciones de trabajo, estos serán realizados por el personal de la Sub Gerencia de Desarrollo Institucional e Informática, lo que se podría tomar en cuenta en este punto es el curso de capacitación del personal del área.

Curso de Capacitación (3 meses)

S/. 300.00 mensual * 3 meses = S/. 900.00

1.3.3 Factibilidad Operativa

Mencionaremos diferentes consideraciones operativas, así tenemos:

- ✓ Existe colaboración por parte del personal operativo y funcionario de la Sub Gerencia de Desarrollo Institucional e Informática del Gobierno Regional de Huancavelica, quienes se encuentra involucrados en el proyecto para lo cual nos brindaran parte de la información importante que facilite su desarrollo.
- ✓ Los usuarios que laboran en los locales descentralizados podrán acceder fácilmente a red de la sede central del Gobierno Regional de Huancavelica ya que se encuentran capacitados y cada uno de ellos cuentan con un usuario con permiso para acceder a la red del GRH a través de la VPN para así hacer uso de los sistemas administrativos de la institución.
- ✓ La seguridad de la información que administra la sede central del Gobierno Regional de Huancavelica se encuentra segura a través de copias de respaldo; cada usuario que acceda a la red de la sede central vía VPN únicamente tendrá permiso para acceder a los sistemas administrativos.

- ✓ El diseño propuesto cambiará de alguna manera los métodos actuales de trabajo en el Gobierno Regional de Huancavelica, la rapidez de las operaciones en la red, la interconexión e intercambio de información con otras áreas y amplía las capacidades de comunicación a todo nivel.

Por tanto considerando los factores operativos señalados, se concluye que el proyecto es operativamente factible.

1.4 JUSTIFICACIÓN

1.4.1 Justificación Practica

Todo tipo de personas y organizaciones requieren de metodologías para transmitir o recibir información de forma rápida y eficiente. Además que esta información sea segura y esto ha llevado a idear tecnologías y actualización de las ya existentes con el propósito de satisfacer las necesidades de cada organización y así llevar a cabo una comunicación con otros equipos aprovechando al máximo su capacidad.

El Gobierno Regional de Huancavelica necesita también una garantía de seguridad en las transferencias de información para evitar que sus datos sean interceptados por personas ajenas a la Institución. La primera solución para satisfacer esta necesidad de comunicación segura implica conectar redes remotas mediante líneas dedicadas como medio de transmisión. Las redes de área local (LAN) son las redes internas como la de la sede central, es decir las conexiones entre los equipos de una organización particular que necesitan comunicarse por Internet con los locales descentralizados que puede estar alejado geográficamente.

Una buena solución consiste en utilizar Internet como medio de transmisión con un protocolo de túnel, que significa que los datos se encapsulan antes de ser enviados de manera cifrada. Las Redes Privadas Virtuales (VPN), constituyen una tecnología a la cual se le está dando cada vez mayor importancia puesto que permiten la transmisión de información a grandes distancias sin necesidad de implantar una compleja y costosa infraestructura de red. Por lo tanto, el sistema VPN brinda una conexión

segura a un muy bajo costo, los beneficios generados son: mayor rapidez en la conexión de los sistemas de la institución, actualización de las bases de datos en tiempo real, información confidencial siempre a disposición desde cualquier parte del mundo para el personal con cualidades y privilegios. Por lo anterior la utilidad de esta tecnología (VPN) en el Gobierno Regional de Huancavelica es grande, conllevando con ello al crecimiento y desarrollo de la entidad.

1.4.2 Justificación Metodológica

Al desarrollar la implementación de la red privada virtual (VPN) mediante el Forefront TMG 2010, estableceremos un procedimiento que servirá de guía para futuros trabajos que se realicen en el área.

CAPITULO II

MARCO TEÓRICO

2.1 ANTECEDENTES

2.1.1 Investigaciones Previas

En la tesis: **Implementación de una VPN en una Solución MPLS - VPN Sobre Múltiples Sistemas Autónomos,** del Ing. Ricardo Armando Menéndez Ávila; En este proyecto el autor explica como 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.

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 y se construyó un prototipo demostrativo.

En nuestro proyecto nos ayudará a poder diseñar la implementación y gestión de la seguridad.

En la tesis: **Análisis y rediseño de la red informática para mejorar la comunicación en la Red Pacífico Sur y sus dependencias de Yugoslavo y Hospital San Ignacio usando tecnología VPN**, del Ing. Kene Reyna Rojas, En los últimos años la institución viene presentando problemas e inconvenientes en cuestiones de comunicación de datos e internet, esto ha sido más notorio a inicios del 2012.

La Red Pacifico Sur cuenta con sistemas como el SIAF y el SIGA, los cuales necesitan de un correcto funcionamiento en red, debido al diseño de la red existente consecuentemente a ello hay cortes súbitos de internet además de perdida de comunicación de datos los cuales ocasionan errores en la transmisión del SIAF generando retrasos y malestar en el personal o peor aún perdida de la data.

Para dar solución a esta problemática se realizara el rediseño físico y lógico de la red informática de los tres centros, logrando un mejor uso de los diferentes recursos informáticos con que cuenta los tres centros, integrándolos y distribuyéndolos de la manera más óptima a través de la red VPN propuesta.

En nuestro trabajo nos ayudara a realizar las conexiones de los sistemas administrativos como el SIGA, SIAF a través de la VPN.

En la tesis: **Implementación de una Red Privada Virtual en la Presidencia Municipal de Pachuca de Soto Hidalgo**, del Ing. Marcos Aurelio Guzmán Vite; El presente trabajo tienen como como objetivo proporcionar a la Presidencia de Pachuca de Soto Hidalgo, un documento el cual muestre detalladamente la implementación por software (Windows server 2003) de una Red Privada Virtual, para que el personal con cualidades y derechos accedan a la red interna de modo alámbrico o inalámbrico vía remota utilizando como medio la internet.

Para lograr el objetivo, la presente tesis detalla paso a paso la implementación de una VPN, el cual permitirá que los clientes roaming o remotos autorizados se conecten con facilidad a los recursos corporativos

de la red de área local (LAN) así como las oficinas remotas se conecten entre sí para compartir recursos e información (conexiones de N). Por último, la solución debe garantizar la privacidad y la integridad de los datos al viajar a través de Internet público.

En nuestro trabajo nos ayudara a detallar paso a paso la implementación de la VPN a través del Forefront TMG 2010.

2.2 BASES TEÓRICAS

2.2.1 Red Privada Virtual (VPN)

2.2.1.1 Introducción a las Redes Privadas Virtual (VPN)

En la actualidad es más común escuchar de empresas en las que es necesario tener oficinas muy distantes del lugar geográfico en donde se encuentra la matriz de la empresa, esto nos hace pensar en la forma de conectividad entre estas oficinas y la matriz. La conectividad la podemos obtener de varias formas con costos y tiempos de respuesta muy altos, y algo muy importante la mínima seguridad que estas poseen.

La introducción del término y la tecnología de Redes Privadas Virtuales (en Inglés VPN Virtual Private Network), han evolucionado durante los últimos 7 años (1997), ya que es una tecnología que nació paralelamente con el origen del TCP/IP, en la década de los 70.

Una red VPN es una extensión de una red privada que utiliza enlaces a través de redes públicas o compartidas (una red pública y compartida más común es Internet). Con una VPN se puede enviar datos entre dos computadoras a través de redes públicas o compartidas de una manera que emula las propiedades de un enlace punto a punto privado.

Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe completar tres tareas:

Deben ser capaces de transportar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por una red pública.

La solución debe agregar encriptación, de manera que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado.

La solución debe ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación de modo que un adversario no pueda acceder a los recursos del sistema.

Para emular un enlace punto a punto, los datos son encapsulados o envueltos, con una cabecera que proporciona la información de enrutamiento que le permite atravesar la red pública o compartida para llegar a su destino. Para emular un enlace privado, los datos enviados son encriptados para tener confidencialidad. Los paquetes que son interceptados en la red pública o compartida son indescifrables. El enlace en el cual los datos son encapsulados y encriptados se conoce como una conexión de red privada virtual (VPN)

El grafico 01 ilustra el concepto lógico de una VPN.

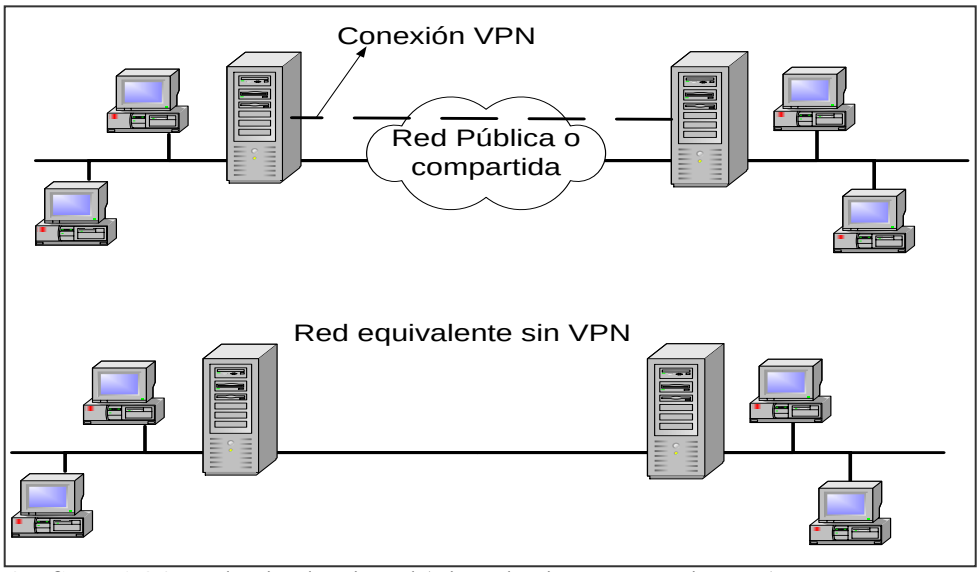


Grafico N° 01 Red Privada Virtual (Virtual Private Network, VPN)
Fuente: Metodología para la implementación de un VPN

Con las conexiones VPN los usuarios que trabajan en casa o de manera móvil pueden tener una conexión de acceso remoto a un servidor de la organización utilizando la infraestructura proporcionada por una red pública como Internet. Desde el punto de vista del usuario, la VPN es una conexión punto a punto entre la computadora (cliente VPN), y el servidor de la organización (servidor VPN). La infraestructura exacta de la red pública o compartida es irrelevante porque desde el punto de vista lógico parece como si los datos fueran enviados por un enlace privado dedicado.

Con las conexiones VPN las organizaciones también pueden tener conexiones enrutadas (routed connections) con sus oficinas geográficamente separadas o con otras organizaciones por una red como Internet, manteniendo a la vez una comunicación segura. Una conexión VPN enrutada a través de Internet opera desde el punto de vista lógico como un enlace WAN dedicado.

Con las conexiones VPN, tanto en las conexiones de acceso remoto como las conexiones enrutadas, una organización puede cambiar de líneas rentadas (leased lines) o accesos telefónicos (dial-up) de larga distancia a accesos telefónicos locales o líneas rentadas con un proveedor de servicio de Internet (Internet Service Provider, ISP).

De acuerdo a estos preámbulos se define a una red privada virtual:

> Un intercambio de información entre dos puntos de una forma segura a través de una red insegura y pública

2.2.1.2 Elementos de una conexión VPN

La tabla 01 y el grafico 02 muestran los elementos de una conexión VPN, los cuales se describen.

Elemento	Detalle
Servidor VPN	Administra clientes VPN
Cliente VPN	Cliente Remotos
Túnel	Encapsulamiento de los datos
Conexión VPN	Encriptación de datos
Protocolos de Túnel	Administracíon de túneles
Datos de Túnel	Datos que se transmiten
Red de Tánsito	Red pública de enlace

Tabla 01 Elementos de una conexión VPN
Fuente: Metodología para la implementación de un VPN

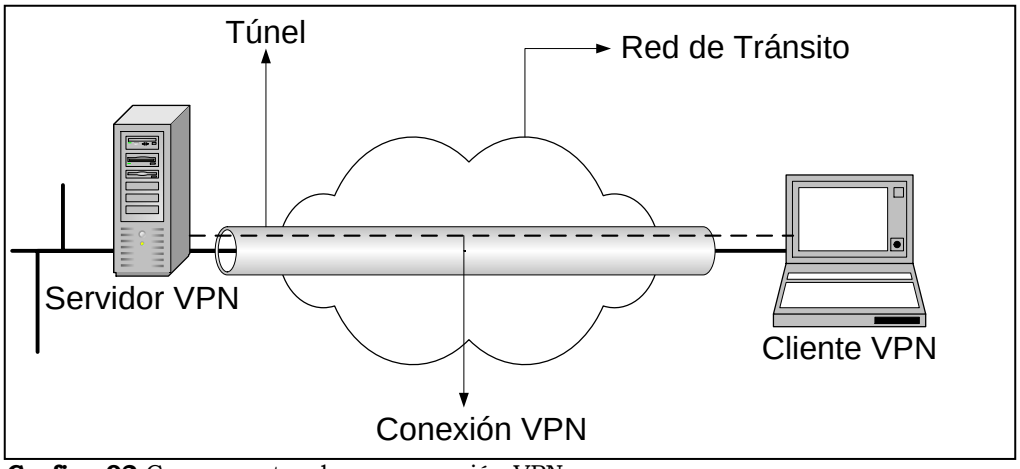


Grafico 02 Componentes de una conexión VPN
Fuente: Metodología para la implementación de un VPN

Servidor VPN.- Computadora que acepta conexiones VPN de clientes VPN. Encargado de administrar todos los clientes VPN y proporcionar la seguridad de la red.

Cliente VPN.- Computadora que inicia una conexión VPN con un servidor VPN.

Túnel.- Porción de la conexión en la que los datos son encapsulados.

Conexión VPN.- Porción de la conexión en la cual los datos son encriptados. Para conexiones VPN seguras, los datos son encriptados y encapsulados en la misma porción de la conexión.

Nota: Es posible crear un túnel y enviar los datos a través del túnel sin encriptación. Esta no es una conexión VPN porque los datos privados viajan a través de la red pública o compartida en una forma no encriptado y fácilmente visible e insegura.

Protocolos de túnel.- Se utilizan para administrar los túneles y encapsular los datos privados. Existen varios protocolos de túnel que se estudiarán más adelante.

Datos del túnel.- Datos que son generalmente enviados a través de un enlace punto a punto.

Red de tránsito.- Red pública o compartida que permite el tránsito de los datos encapsulados. La red de tránsito puede ser Internet o una intranet privada.

2.2.1.3 Implementaciones comunes de una VPN

Entre las implementaciones más comunes se tiene 4 maneras claramente identificadas

TIPO	DETALLE
VPN de Intranet	Creación de conexión entre las oficinas centrales y las oficinas remotas.
VPN de Acceso Remoto	Creación de conexión entre las oficinas centrales y los usuarios móviles remotos.
VPN de Extranet	Creación de conexión entre la empresa y sus socios comerciales.
VPN Interna	Creación de conexión dentro de una LAN

Tabla 02 Implementaciones comunes de una VPN
Fuente: Metodología para la implementación de un VPN

- ✓ **VPN de intranet.**

Este tipo de implementación está dada por la creación de una conexión entre las oficinas centrales corporativas y las oficinas remotas que se encuentran en el exterior. A comparación con una Intranet típica el acceso viene desde el exterior a la red y no desde el interior. La siguiente figura ilustra una Red privada Virtual de Intranet.

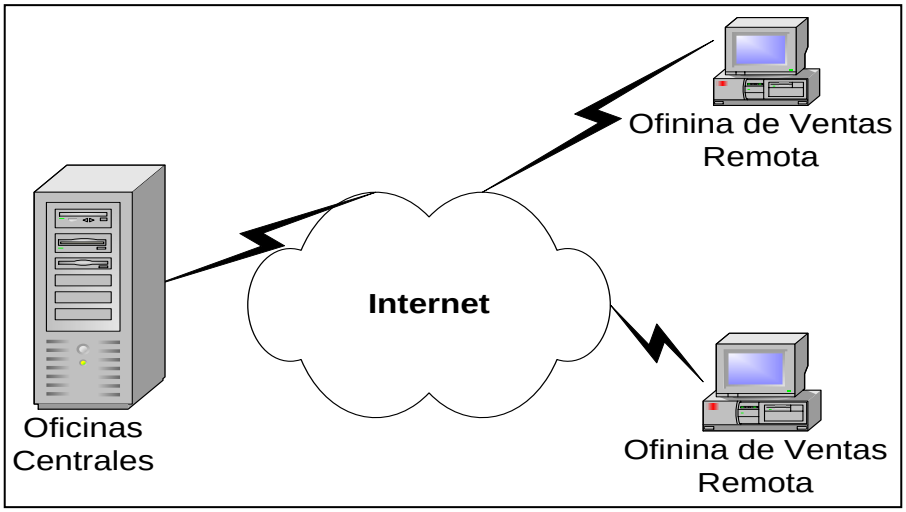


Grafico 03 VPN de Intranet
Fuente: Metodología para la implementación de un VPN

- ✓ **VPN de acceso remoto**

Una red privada virtual de acceso remoto se crea entre las oficinas centrales corporativas y los usuarios móviles remotos a través de un ISP. Como se puede observar en la siguiente figura, el usuario móvil levanta una conexión telefónica con un ISP y crea un túnel de conexión hacia las oficinas centrales corporativas.

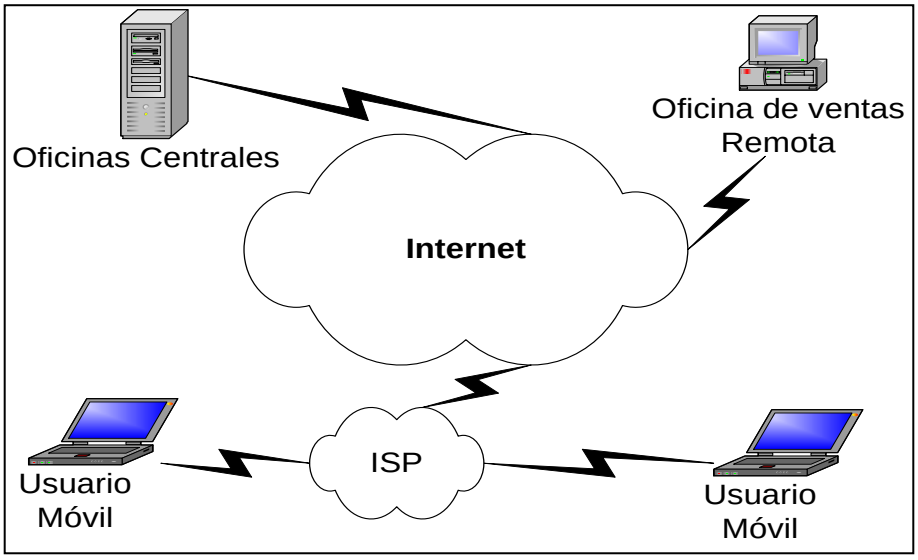


Grafico 04 VPN de Acceso Remoto
Fuente: Metodología para la implementación de un VPN

✓ **VPN de Extranet.**

Una red privada virtual de Extranet se crea entre la empresa y sus socios comerciales (clientes, proveedores), mediante el protocolo HTTP, que es el común de los navegadores de Web, o mediante otro servicio y protocolo ya establecido entre las dos partes involucradas. Esta implementación tiene mayor impacto en todo lo referente al comercio electrónico brindando seguridad y eficacia para las empresas y sus socios comerciales. La figura 5 ilustra una red privada virtual de extranet.

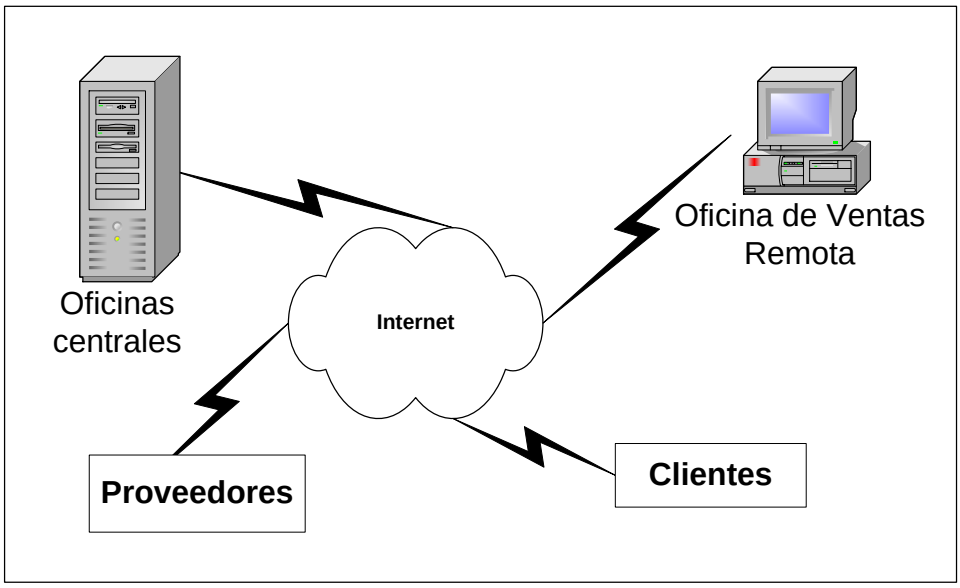


Grafico 05 VPN de Extranet
Fuente: Metodología para la implementación de un VPN

✓ **VPN Interna.**

Una red privada virtual interna, es una implementación que no tiene un uso frecuente en el entorno de las redes. Este tipo de implementación se crea en una LAN, siempre que se considere necesario transferir información con mucha privacidad entre departamentos de una empresa.

Esta red privada virtual interna es necesaria implementarla cuando se cree que se pueden tener ataques informáticos realizados por los mismos empleados de la empresa. La figura 6 ilustra una configuración típica de red privada virtual interna.

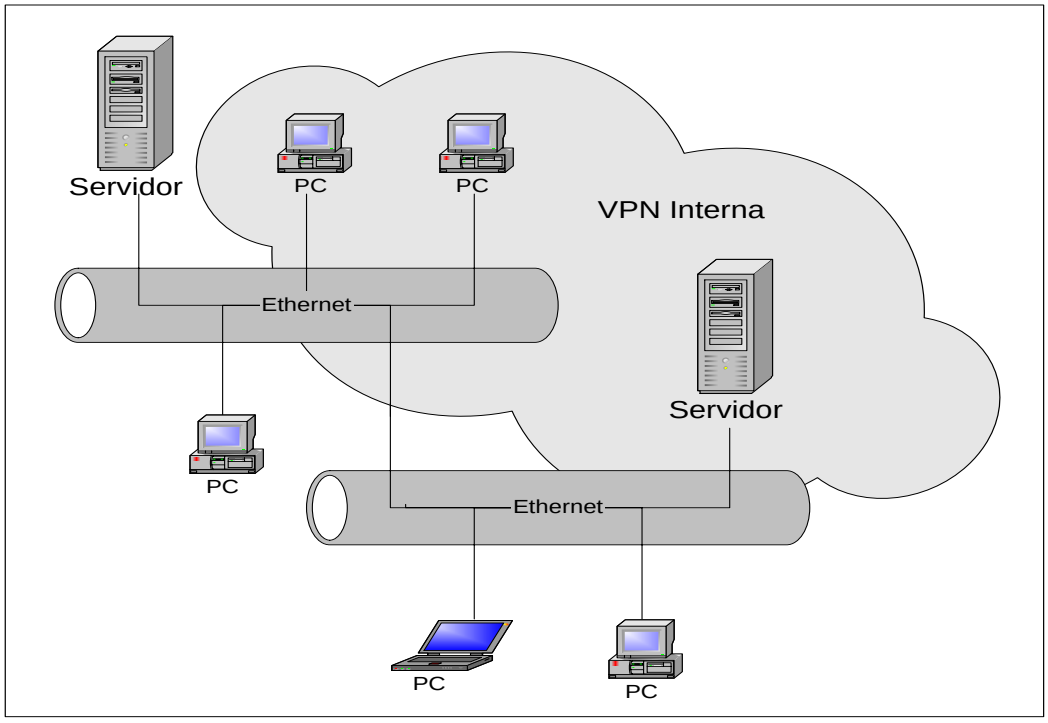


Grafico 06 VPN Interna
Fuente: Metodología para la implementación de un VPN

2.2.1.4 Requisitos de una Red Privada Virtual.

Para garantizar que una red privada virtual sea segura, este disponible y sea fácil de mantener es necesario cumplir con ciertos requisitos esenciales que una empresa debe tomar en cuenta antes de implementar una Red Privada Virtual.

Estos requisitos son los siguientes:

- ✓ Disponibilidad
- ✓ Control
- ✓ Compatibilidad

- ✓ Seguridad
- ✓ Interoperabilidad
- ✓ Confiabilidad
- ✓ Autenticación de datos y usuarios
- ✓ Sobrecarga de tráfico
- ✓ Mantenimiento
- ✓ Sin repudio

Disponibilidad.- La disponibilidad se aplica tanto al tiempo de actualización como al de acceso. No basta que el usuario tenga autorización para acceder a los servidores corporativos, si no puede conectarse debido a problemas de la red, por tanto se debe asegurar la disponibilidad en la parte física de la red.

Control.- El control debe ser implementado por el supervisor o administrador de la Red Privada Virtual, sea este interno o externo dependiendo de cómo se realizó la implementación de VPN.

Debemos tomar en cuenta que por muy grande que sea la organización es posible tener un solo VPN, lo que facilitará al administrador de la VPN el control sobre la misma.

Compatibilidad.- Debido que al utilizar tecnologías de VPN y de internet estas se basan en protocolo IP, por lo que la arquitectura interna del protocolo de red de la compañía debe ser compatible con el protocolo IP.

Seguridad.- Hablar de seguridad y de red privada virtual, hasta cierto punto se podría decir que son sinónimos. La seguridad en una VPN abarca todo, desde el proceso de cifrado que se implementa hasta los servicios de autenticación de usuarios.

Es necesario que se tenga muy en cuenta este término de seguridad, ya que se puede afirmar que una VPN sin seguridad no es una VPN.

Interoperabilidad.- La interoperabilidad de una red privada virtual, es muy importante para la transparencia en la conexión entre las partes involucradas.

Confiabilidad.- La confiabilidad es uno de los requisitos importantes que debe poseer en una Red Privada Virtual, pero esta confiabilidad se ve afectada en gran porcentaje en la VPN de Acceso Remoto en las que se sujeta a la confiabilidad que se tiene por parte del ISP, ya que si el servicio del ISP se interrumpe la conexión también y nosotros no se podrá hacer nada hasta que el ISP nuevamente brinde su servicio a los clientes.

Autenticación de Datos y Usuarios.- La autenticación de datos y de usuarios es sumamente importante dentro de cualquier configuración de Red privada Virtual.

La autenticación de datos afirma que los datos han sido entregados a su destinatario totalmente sin alteraciones de ninguna manera.

La autenticación de usuarios es el proceso en el que se controla que solos los usuarios admitidos tengan acceso a la red y no sufrir ataques por usuarios externos y maliciosos.

Sobrecarga de tráfico.- La sobrecarga de tráfico es un problema de cualquier tipo de tecnología de redes, y por ende también es un problema inevitable, especialmente si tenemos una red privada virtual a través de un ISP. Tomando en cuenta que un paquete enviado en una VPN es encriptado y encapsulado lo que aumenta de manera significativa la sobrecarga de tráfico en la red.

Mantenimiento.- El mantenimiento, aspecto del que no se puede olvidar. Si la red privada virtual es implementada con los propios recursos de la empresa es necesario considerar que el mantenimiento debe estar soportado por el propio personal del departamento de sistemas, el cuál debe estar capacitado para este fin. De no poseer el personal capacitado es preferible contratar servicio externos que se encarguen de la implementación y mantenimiento de la red privada virtual de mi empresa.

Sin repudio.- Consiste en el proceso de identificar correctamente al emisor, con la finalidad de tener claro desde donde proviene la

solicitud. Si se considera que una VPN me va a servir para contactarme con mis clientes es necesario que este bien identificado de donde proviene el pedido. Para poder realizar cualquier transacción comercial (comercio electrónico) por internet es necesario que esta transacción sea un proceso sin repudio. No podemos dar cuenta que nuevamente se está hablando de seguridad, una de las características fundamentales en una VPN.

2.2.1.5 Beneficios de las Redes Privadas Virtuales.

El simple hecho de hablar de redes privadas virtuales, como se indicó anteriormente, viene a la mente el término de seguridad, así como también el bajo costo que esta tecnología necesita para implementarla y además su facilidad de uso.

En resumen se puede decir que la implementación de una red privada virtual nos hace pensar en tres aspectos fundamentales y beneficiosos para nuestra empresa que son:

- ✓ Seguridad
- ✓ Bajos costos
- ✓ Facilidad de uso

Los costos de implementación de las redes privadas virtuales tienen que ver más con la capacitación del personal de sistemas para la implementación y mantenimiento de la red privada virtual así como costos de contratación de servicios de un ISP.

Pero todo esto no debe ser tomado como una desventaja de esta tecnología, sino debe tomarse como una inversión para futuros ahorros que se obtendrán.

A continuación se describe algunos de los beneficios que se tiene en la implementación de redes privadas virtuales:

Ahorro en costos.- el ahorro en costos de las redes privadas virtuales está asociado con diferentes factores que influyen en el

paso de una tecnología anterior a una tecnología de redes privadas virtuales.

La eliminación de líneas rentadas, al igual que las líneas por marcación son dos factores fundamentales que permitirán el ahorro en la implementación de una VPN, tomando en cuenta que al eliminar este tipo de comunicación también se elimina los costos de los demás dispositivos involucrados como puede ser equipos pbx, equipos de acceso remoto. También se eliminarán costos de instalación y configuración de dichos equipos de acceso remoto, entre otros costos.

Diseño de la red.- Uno de los principales beneficios de las redes privadas virtuales se basan en el diseño de estas. Para aclarar de mejor manera estos beneficios observemos el siguiente ejemplo.

En el grafico 07 se puede observar el diseño de una WAN, en la que es necesario que se tenga en cuenta que al diseñar esta WAN con enlaces de líneas rentadas y de marcación, debe existir un gran esfuerzo por el personal de implementación de la WAN para saber que tráfico se va a tener para saber el tipo de líneas que se debe adquirir y en que porcentajes. Además deberán tener en cuenta los problemas que aparecen al usar líneas ya sea rentadas y de marcación en grandes distancias.

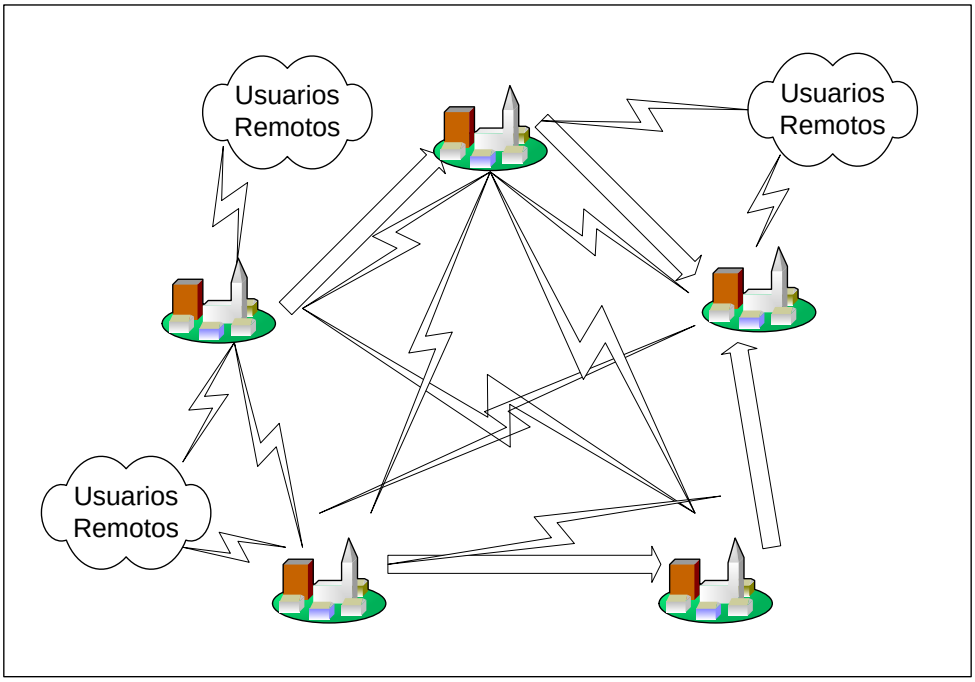


Grafico 07 WAN con líneas rentadas y de marcación
Fuente: Metodología para la implementación de un VPN

En cambio en el grafico 08 se muestra la misma red WAN con la arquitectura de redes privadas virtuales a través de un ISP. Se puede observar que el diseño se simplifica enormemente y todo lo que corresponde al tráfico de información se encarga el Internet, haciendo más fácil la conectividad y la escalabilidad de la red.

Este es uno de los principales beneficios en el diseño de redes WAN con arquitectura VPN. Es por eso que esta tecnología cada vez tiene más adeptos a nivel mundial.

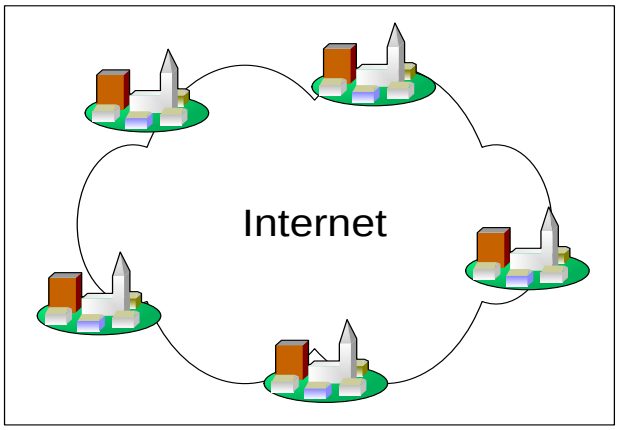


Grafico 08 WAN con internet como enlace.
Fuente: Metodología para la implementación de un VPN

Beneficios para el usuario final.- El usuario final se ve muy beneficiado ya sea un usuario que pertenezca a la propia empresa o un cliente.

En la actualidad las empresas deben llegar al cliente, sin importar donde se encuentre éste, es por eso que se hace necesario que el cliente tenga acceso a los servicios y ya no se lo haga con comunicaciones telefónicas de larga distancia que son muy costosas, sino a través de un ISP local con un enlace más eficiente y menos costoso y además un enlace que va a estar disponible las 24:00h al día los 365 días del año.

El mismo beneficio tendrán los usuarios remotos, facilitándoles el acceso a la información de la empresa en el momento que lo deseen, independiente del lugar en el que se encuentren.

2.2.2 Protocolos de Túnel

2.2.2.1 Introducción.

Un sistema de túnel, es un método para utilizar una infraestructura de red para transferir datos de una red sobre otra. Los datos que serán transferidos (carga útil) pueden ser tramas (paquetes) de otro protocolo. En lugar de enviar una trama a medida que es producida

por el nodo originador, el protocolo de túnel encapsula la trama en un encabezado adicional. El encabezado adicional proporciona información de enrutamiento de tal manera que la carga útil encapsulada pueda viajar a través de la red intermedia.

Entonces, se pueden enrutar los paquetes encapsulados entre los puntos finales del túnel sobre la red. La trayectoria lógica a través de la cual viajan los paquetes encapsulados en la red se le llama un túnel. Una vez que las tramas encapsuladas llegan a su destino sobre la red se desencapsulan y se envían a su destino final. Note que este sistema de túnel incluye todo este proceso (encapsulamiento, transmisión y desencapsulamiento de paquetes).

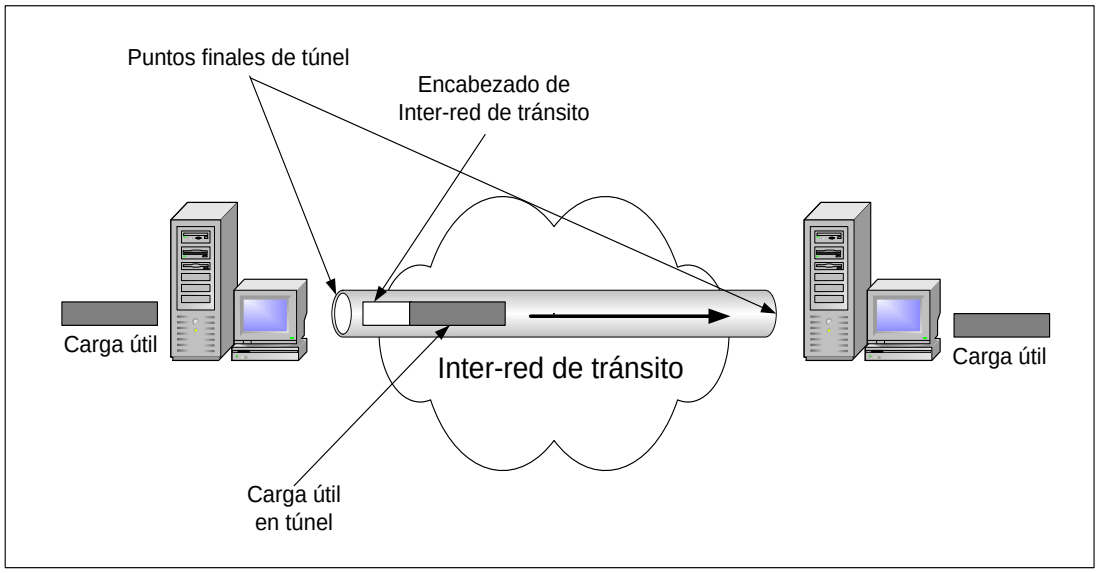


Grafico 09. Túneles

Fuente: Metodología para la implementación de un VPN

Tome en cuenta que la inter-red de tránsito puede ser el Internet, que es una inter-red pública y es el ejemplo del mundo real más conocido. Existen muchos otros ejemplos de túneles que pueden realizarse sobre inter-redes corporativas. Si Internet proporciona una de las inter-redes más penetrantes y económicas, las referencias a Internet se pueden reemplazar por cualquier otra inter-red pública o privada que actúe como una inter-red de tránsito.

Las tecnologías de túnel han existido, pero algunos ejemplos de tecnologías maduras incluyen:

- ✓ **Túneles SNA sobre interredes IP**. Cuando se envía tráfico de la arquitectura de la red del sistema (SNA) a través de una inter-red IP corporativa, la trama SNA se encapsula en un encabezado UDP e IP.
- ✓ **Túneles IPX para Novell NetWare sobre inter-redes IP**. Cuando un paquete IPX se envía a un servidor NetWare o router IPX, el servidor o router envuelve el paquete IPX en un encabezado UDP e IP y, luego lo envía a través de una inter-red IP. El router IP a IPX de destino quita el encabezado UDP e IP, y transmite el paquete al destino IPX.

En los últimos años se han introducido nuevas tecnologías de sistemas de túneles. Entre las tecnologías más nuevas, enfoque principal de este capitulo, incluyen:

- ✓ **Protocolo de túnel de punto a punto (PPTP).** Permite que se encripte el tráfico IP, IPX o NetBEUI y luego se encapsule en un encabezado IP para enviarse a través de una red corporativa IP o red pública IP.
- ✓ **Protocolo de túnel de nivel 2 (L2TP).** Permite que se encripte el tráfico IP, IPX o NetBEUI y luego se envíe sobre cualquier medio que brinde soporte a la entrega de datagramas punto a punto, como IP, X.25, Frame Relay o ATM.
- ✓ **Modo de túnel de seguridad IP (IPSec)**. Permite que se encripten las cargas útiles IP y luego se encapsulen en un encabezado IP para enviarse a través de una red corporativa IP o una red pública IP.

2.2.2.2 Protocolos de túnel.

Para que se establezca un túnel el cliente del túnel como el servidor del túnel deberán utilizar el mismo protocolo de túnel.

En la tabla 3 se puede observar los protocolos de túnel que se describirán más adelante.

Protocolo	Detalle
PPTP	Point to Point Tunneling Protocol (Microsoft)
L2F	Layer Two Forwarding (Cisco)
L2TP	Layer Two Tunneling Protocol (Cisco)

Tabla 3 Protocolos de Túnel
Fuente: Metodología para la implementación de un VPN

También se describirán los protocolos PPP (Point to Point Protocol) y también el protocolo IPSec (IP Security), que aunque no pertenezcan al conjunto de protocolos de túnel, pero si tienen relación con éstos. La tecnología de túnel se puede basar ya sea en el protocolo del túnel de Nivel 2 o de Nivel 3. Estos niveles corresponden al modelo de referencia de interconexión de sistemas abiertos (OSI). Los protocolos de nivel 2 corresponden al nivel de enlace de datos, y utilizan tramas como su unidad de intercambio. PPTP y L2TP son protocolos de túnel de nivel 2; ambos encapsulan la carga útil en una trama del protocolo punto a punto (PPP) que se enviará a través de la red. Los protocolos de nivel 3 corresponden al nivel de la red y utilizan paquetes IP sobre IP y el modo de túnel de seguridad IP (IPSec); estos protocolos encapsulan los paquetes IP en un encabezado adicional IP antes de enviarlos a través de una red IP.

¿Cómo funcionan los túneles?

Para las tecnologías de túnel de nivel 2 como PPTP y L2TP, un túnel es similar a levantar una sesión de comunicación; los dos nodos finales del túnel deben estar de acuerdo al túnel y deben negociar las variables de la configuración, asignación de dirección, los

parámetros de encriptación o de compresión. En la mayoría de los casos, los datos que se transfieren a través del túnel se envían utilizando protocolos basados en datagramas. Se utiliza un protocolo para mantenimiento del túnel como el mecanismo para administrar al mismo.

En general las tecnologías de túnel de nivel 3, suponen que se han manejado fuera de contexto los temas relacionados con la configuración, normalmente por medio de procesos manuales. Sin embargo una fase de mantenimiento de túnel bien puede no existir. Mientras para los protocolos de nivel 2 (PPTP y L2TP) se debe crear, mantener y luego dar por terminado un túnel.

Una vez que se establece el túnel, se puede enviar los datos a través del mismo. El cliente o el servidor del túnel utilizan un protocolo de transferencia de datos del túnel para preparar los datos para su transferencia. Por ejemplo, cuando el cliente del túnel envía una carga útil al servidor del túnel, el cliente del túnel adjunta primero un encabezado de protocolo de transferencia de datos de túnel a la carga útil. Luego, el cliente envía la carga útil encapsulada resultante a través de la red, la cual lo enruta al servidor del túnel. El servidor del túnel acepta los paquetes, quita el encabezado del protocolo de transferencia de datos del túnel y envía la carga útil a la red objetivo. La información que se envía entre el servidor del túnel y el cliente del túnel se comporta de manera similar

Los protocolos de túnel y los requerimientos básicos del túnel.

Debido a que los protocolos de nivel 2 (PPTP y L2TP) se basan en protocolos PPP bien definidos, heredan un conjunto de funciones útiles, estas funciones y sus contrapartes de nivel 3 cubren los requerimientos básicos de la VPN.

- ✓ **Autenticación de usuario.** Los protocolos de túnel de nivel 2 heredan los esquemas de autenticación del usuario de PPP,

incluyendo los métodos EAP (Extensible Authentication Protocol – *Protocolo de Autenticación Ampliable*). Muchos de los esquemas de túnel de nivel 3 suponen que los puntos finales han sido bien conocidos y autenticados antes de que se estableciera el túnel. Una excepción es la negociación IPSec ISAKMP, la cual proporciona una autenticación mutua de los nodos finales del túnel. (Note que la mayor parte de las implementaciones IPSec dan soporte sólo a certificados basados en equipo, más que en certificados de usuarios. Como resultado, cualquier usuario con acceso a uno de los equipos de nodo final puede utilizar el túnel. Se puede eliminar esta debilidad potencial de seguridad cuando se complementa el IPSec con un protocolo de nivel 2 como el L2TP.)

- ✓ **Soporte de tarjeta de señales.** Al utilizar el protocolo de autenticación ampliable (EAP), los protocolos de túnel de nivel 2 pueden dar soporte a una amplia variedad de métodos de autenticación, incluyendo contraseñas de una sola vez, calculadores criptográficos y tarjetas inteligentes. Los protocolos de túnel de nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define la autenticación de los certificados de claves públicas en su negociación ISAKMP/Oakley (protocolo de seguridad).
- ✓ **Asignación de dirección dinámica.** El túnel de nivel 2 da soporte a la asignación dinámica de direcciones de clientes basadas en un mecanismo de negociación de protocolo de control de la red (NCP). Por lo general, los esquemas de túnel de nivel 3 suponen que ya se ha asignado una dirección antes de la iniciación del túnel. Los esquemas para la asignación de direcciones en el modo de túnel IPSec están actualmente en desarrollo.
- ✓ **Compresión de datos.** Los protocolos de túnel de nivel 2 dan soporte a esquemas de compresión basados en PPP. Por ejemplo, las implementaciones de Microsoft tanto de PPTP como L2TP

utilizan Microsoft Point-to-Point Compression (MPPC). La IETF se encuentra investigando mecanismos similares (como la compresión IP) para los protocolos de túnel de nivel 3.

- ✓ **Encriptación de datos**. Los protocolos de túnel nivel 2 dan soporte a mecanismos de encriptación de datos basados en PPP. La implementación de Microsoft de PPTP da soporte al uso opcional de Microsoft Point-to-Point Encription (MPPE), basado en el algoritmo RSA/RC4. Los protocolos de túnel nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define varios métodos de Encriptación opcional de datos que se negocian durante el intercambio ISAKMP/Oakley. La implementación de Microsoft del protocolo L2TP utiliza la encriptación IPSec para proteger el flujo de datos del cliente al servidor del túnel.
- ✓ **Administración de claves.** MPPE, protocolo de nivel 2, se basa en las claves iniciales generadas durante la autenticación del usuario y luego las renueva periódicamente. IPSec negocia explícitamente una clave común durante el intercambio ISAKMP y también las renueva periódicamente.
- ✓ **Soporte de protocolo múltiple**. El sistema de túnel de nivel 2 da soporte a protocolos múltiples de carga útil, lo cual hace más fácil a los clientes de túnel tener acceso a sus redes corporativas utilizando IP, IPX, NetBEUI, etc. En contraste, los protocolos de túnel de nivel 3, como el modo de túnel IPSec, típicamente dan soporte sólo a redes objetivo que utilizan el protocolo IP.

2.2.2.2.1 Protocolo de Punto a Punto (PPP).

El protocolo PPP, no es un protocolo de túnel, pero es la base para el protocolo PPTP, que es el protocolo de túnel punto a punto.

El protocolo PPP proporciona un método estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto

entre dos "pares" (máquinas en los dos extremos del enlace). Estos enlaces proveen operación bidireccional full dúplex y se asume que los paquetes serán entregados en orden.

Consta de tres componentes principales:

- ✓ Un método de encapsulamiento que permite al software de red utilizar un solo enlace serial para múltiples protocolos y manejar la detección de errores.
- ✓ Un protocolo de control de enlace LCP (Link Control Protocol) que el software de red puede utilizar para establecer, configurar y probar las conexiones de enlace de datos. Ambos lados de la conexión PPP utilizan LCP para negociar las opciones de conexión.
- ✓ Una familia de protocolos de control de red NCPs (Network Control Protocols) que permita a las conexiones PPP utilizar diferentes protocolos de la capa de red.

Hay cuatro fases de negociación en una sesión de marcación de PPP. Cada una de éstas debe completarse satisfactoriamente antes de que la conexión de PPP esté lista para transferir los datos del usuario. Estas fases son:

Fase 1. Establecimiento del enlace de PPP: El PPP utiliza el protocolo de control de enlace (LCP) para establecer, mantener y terminar la conexión física. Durante la fase del LCP, se seleccionan las opciones de comunicación básica. Tome en cuenta que durante la fase de establecimiento del enlace (fase 1), se seleccionan los protocolos de autenticación, pero no se implementan realmente hasta la fase de autenticación de usuarios (fase 2). De manera similar, durante el LCP, se toma una decisión en cuanto a que si dos enlaces iguales negocian el uso de compresión y/o encriptación,

la elección real de algoritmos de encriptación/compresión ocurre durante la fase 4.

Fase 2. Autenticación de usuarios: En esta fase, el computador que hace de cliente presenta la identificación del usuario al servidor de acceso remoto(RAS). Un esquema seguro de autenticación proporciona protección contra los ataques de contestación e imitación de clientes remotos.

Las implementaciones del PPP por lo general, proporcionan métodos limitados de autenticación, algunos de éstos son:

- ✓ **Protocolo de Autenticación de Contraseñas (PAP).** Es un esquema simple de autenticación de texto claro, es decir, que no está codificado. El servidor solicita el nombre y contraseña del usuario, y el PAP los entrega en texto claro. Indiscutiblemente, este esquema no es seguro debido a que puede ser interceptado el nombre y contraseña del usuario, y utilizarlos para obtener acceso al servidor y a todos los recursos suministrados por el mismo. El PAP no proporciona protección contra los ataques de reproducción o las imitaciones de cliente remoto, una vez que la contraseña del usuario ha sido violada.
- ✓ **Protocolo de Autenticación de Intercambio de Señales de Reconocimiento (CHAP).** Es un mecanismo de autenticación encriptado que evita la transmisión de contraseñas reales en la conexión. El NAS envía un desafío (challenge), que consiste de una identificación de sesión y una extensión challenge arbitraria al cliente remoto. El cliente remoto deberá utilizar el algoritmo de control unidireccional MD5 para devolver el nombre del usuario y una encriptación del challenge, la identificación de la sesión y la contraseña del cliente. El nombre del usuario se envía sin verificar.

El CHAP es una mejora sobre el PAP en cuanto a que no se envía la contraseña de texto transparente sobre el enlace. En su lugar, se utiliza la contraseña para crear una verificación encriptada del desafío original. El servidor conoce la contraseña del texto transparente del cliente y por lo tanto puede duplicar la operación y comparar el resultado con la contraseña enviada en la respuesta del cliente. El CHAP protege contra ataques de reproducción al utilizar una extensión challenge arbitraria para cada intento de autenticación. El CHAP protege contra la personificación de un cliente remoto al enviar de manera impredecible desafíos repetidos al cliente remoto a todo lo largo de la duración de la conexión.

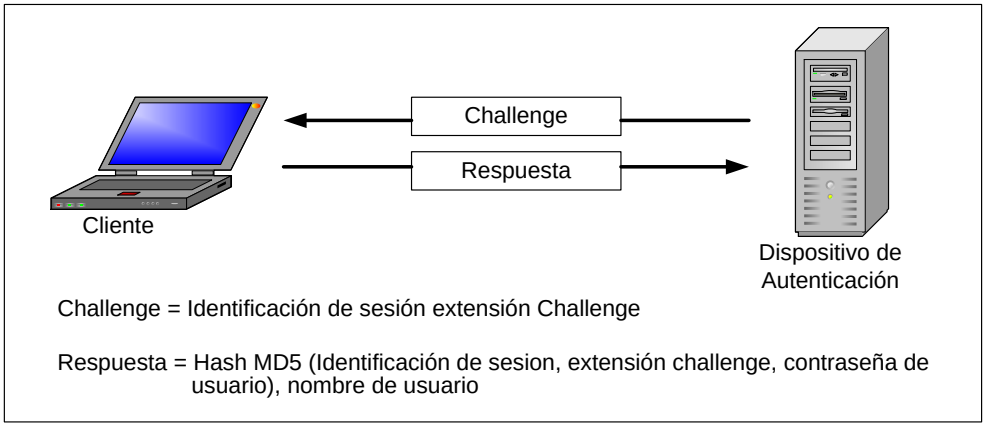


Grafico 10. El proceso CHAP
Fuente: Metodología para la implementación de un VPN

- ✓ **Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP):** El MS-CHAP (Protocolo de Autenticación por desafío mutuo de Microsoft) es un mecanismo de autenticación codificado muy similar al CHAP en donde, el servidor envía al cliente remoto una señal de reconocimiento, que consiste de una ID de sesión y de una cadena de reconocimiento arbitraria. El cliente remoto debe regresar el nombre del usuario y un hash MD4 de la cadena de reconocimiento, la ID de sesión y de la contraseña con el algoritmo de control unidireccional hash MD4. Este diseño, que

manipula una codificación del hash MD4 de la contraseña, proporciona un nivel adicional de seguridad porque permite que el servidor almacene contraseñas codificadas en lugar de contraseñas de texto claro. El servidor reúne los datos de autenticación y después los valida en su propia base de datos de usuarios o basándose en un servidor central de base de datos de autenticación, además, proporciona códigos de error adicionales, incluyendo un código de expiración de contraseña, y mensajes adicionales codificados de cliente-servidor que permiten que los usuarios cambien sus contraseñas.

Durante la fase 2 de la configuración del enlace del PPP, el NAS recopila los datos de autenticación y luego valida los datos contra sus propia base de datos del usuario o contra un servidor central para la autenticación de base de datos.

Fase 3. Control de retorno de llamada de PPP: La implementación del PPP de Microsoft incluye una fase opcional de control de retorno de llamada. Esta fase utiliza el Protocolo de Control de Retorno de Llamada (CBCP – Call Back Control Protocol) inmediatamente después de la fase de autenticación. Si la configuración es para retorno de llamada, después de la autenticación el cliente remoto y el servidor se desconectan. Después, el servidor llama otra vez al cliente remoto a un número telefónico especificado. Esto proporciona un nivel adicional de seguridad para las redes de marcación. El servidor permitirá conexiones de clientes remotos que residen físicamente sólo en números telefónicos específicos.

Fase 4. Invocación de protocolos de nivel de red: En esta fase, el PPP invoca a los protocolos de control de red (NCP) que fueron seleccionados durante la fase de establecimiento del enlace para configurar los protocolos utilizados por el cliente remoto.

Después de culminar las fases de negociación, el PPP comienza a transmitir los datos desde las dos partes. Cada paquete de datos transmitido se encapsula en un encabezado de PPP que es eliminado por el sistema receptor. Si la compresión de datos se seleccionó en la fase del establecimiento del enlace PPP y se negoció en la fase de invocación de protocolos del nivel de red, los datos serán comprimidos antes de la transmisión. Si se seleccionaron y se negociaron de manera similar la encriptación de datos (comprimidos opcionalmente) se encriptarán antes de la transmisión.

2.2.2.2.2 Protocolo de Túnel de Punto a Punto (PPTP).

Point-To-Point Tunneling Protocol (PPTP) es una combinación del protocolo punto a punto(PPP) y del protocolo de control de transmisión/protocolo Internet (TCP/IP), el cual permite el seguro intercambio de datos de un cliente a un servidor formando una red privada virtual, basado en una red de trabajo vía TCP/IP.

PPTP combina funciones del PPP como el multiprotocolo, la autenticación de usuarios y la privacidad con la compresión de paquetes de datos, y TCP/IP ofrece capacidad para enrutar esos paquetes por Internet. PPTP permite el encapsulamiento de datos con el uso de un túnel.

El PPTP es un protocolo de nivel de enlace del modelo de referencia OSI, el cual encapsula las tramas de PPP en datagramas de IP las cuales van a ser transmitidas a través de una red interna de IP, como Internet. (Sobre estos paquetes PPP pueden emplearse cualquiera de los siguientes protocolos: NetBEUI, IPX, SNA o TCP/IP). También se puede utilizar el PPTP en una red privada de LAN a LAN.

El protocolo de túnel de punto a punto (PPTP) utiliza una conexión de TCP (puerto 1723) para el mantenimiento del túnel y las tramas de

PPP encapsuladas, las cuales a su vez son encapsuladas en paquetes de encapsulamiento de enrutamiento genérico (GRE) destinadas a los datos en el túnel. Las cargas de pago de las tramas de PPP encapsuladas pueden codificarse y/o comprimirse.

PPTP permite crear conexiones entre un cliente y un servidor sobre redes IP públicas como puede ser Internet. Lo interesante es que estos enlaces se realizan a través de una especie de túnel que PPTP crea en la red IP y por el que viajan los datos de la conexión. Además este túnel es privado: nadie a excepción del cliente y el servidor viajan por él.

El tráfico PPTP consiste en dos tipos de tráfico para diferentes tipos de datos: paquetes de datos y paquetes de control. Los paquetes de control se emplean para cosas como el estado y la señalización, y los paquetes de datos se emplean para contener los datos del usuario. Los paquetes de datos son paquetes que han sido encapsulados con el protocolo de encapsulamiento para enrutamiento genérico versión 2 (GREv2) de Internet.

La conexión PPTP comienza primero como un reconocimiento entre las dos terminales remotas; éstas acuerdan el esquema de compresión y el método de encapsulamiento que van a usar. Si es necesario, durante la comunicación normal estos paquetes se pueden fragmentar y el encabezado PPP añade un número serial para detectar si se perdió un paquete.

El grafico 11 muestra la forma en que se ensambla el paquete de PPTP antes de la transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de la red. El diseño de la trama final muestra la encapsulación para un cliente de marcación (controlador de dispositivo PPP).

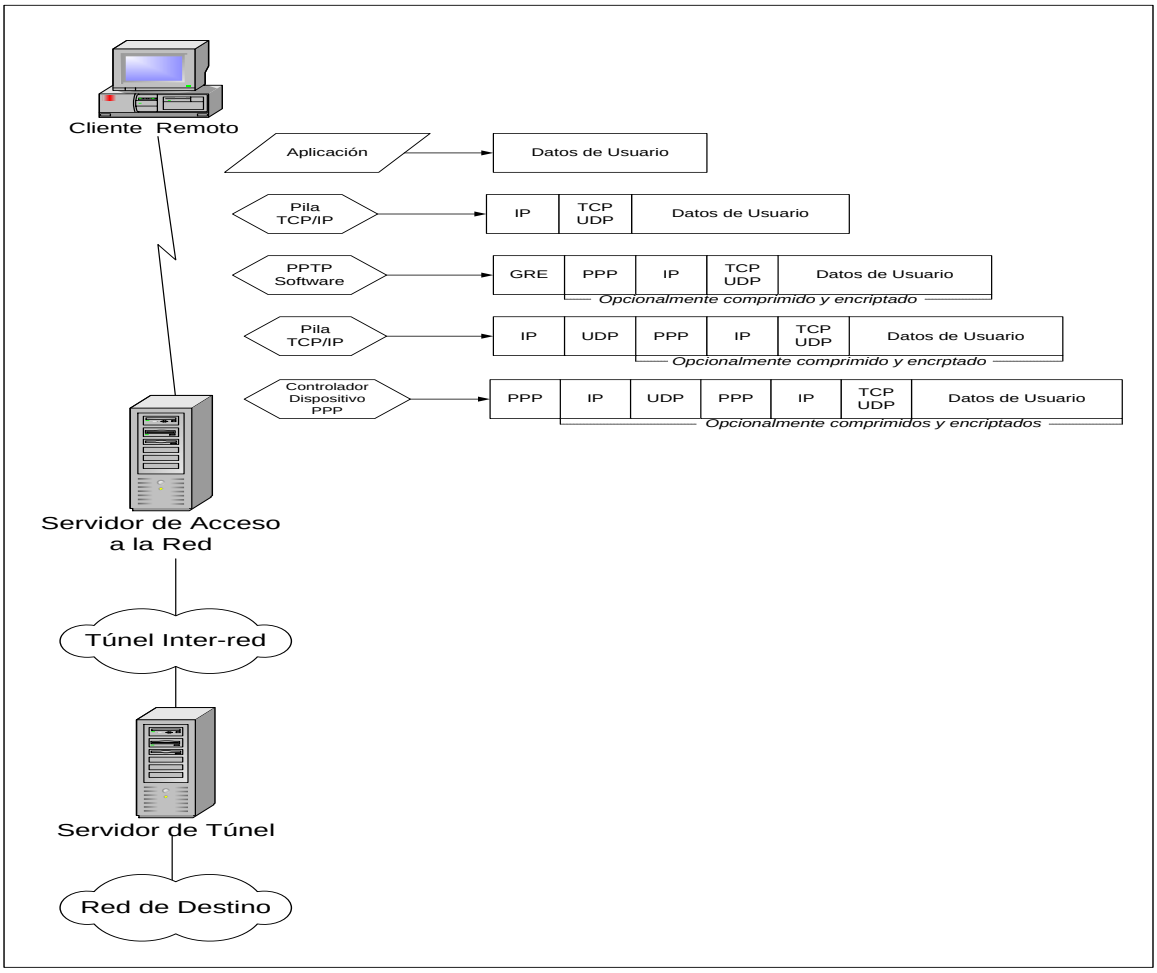


Grafico 11. Construcción de un paquete PPTP
Fuente: Metodología para la implementación de un VPN

La arquitectura del PPTP se compone de tres fases, cada una de las cuales necesita que el anterior haya tenido éxito:

Fase 1. Conexión PPP. Es la conexión con el ISP. PPP es un protocolo de acceso remoto que establece enlaces punto a punto sobre distintos medios físicos. Normalmente, se emplea para establecer conexiones

remotas a través de enlaces telefónicos (como por ejemplo conectar con nuestro ISP). PPP se encarga de las siguientes funciones:

- ✓ Establecer y mantener la conexión punto a punto a nivel físico.
- ✓ Autentifica a los usuarios mediante PAP, SPAP, CHAP ó MS-CHAP comentados anteriormente.
- ✓ Crea tramas que encapsulan paquetes NetBEUI, IPX o TCP/IP encriptados.

Fase 2. Control de la conexión PPTP. Una vez conectado a Internet, o a la red IP que hayamos elegido, debe establecerse conexión con el servidor y controlar la comunicación establecida. En una red TCP/IP, El protocolo TCP se encarga de este trabajo. Sin embargo, en los túneles PPTP, TCP no existe a nivel de transporte porque todo va encapsulado en marcos PPP sobre paquetes IP. Por este motivo PPTP asume este papel utilizando servicios TCP para ello. A esta conexión es a la que se le denomina túnel PPTP. Los principales mensajes empleados por PPTP para el control de la sesión entre los extremos del túnel son los siguientes:

MENSAJE	FUNCION
PPTP_START_SESSION_REQUEST	Inicia la sesión
PPTP_START_SESSION_REPLY	Respuesta a la solicitud de inicio de sesión
PPTP_ECHO_REQUEST	Mantiene la sesión
PPTP_ECHO_REPLY	Respuesta a la solicitud de mantenimiento de sesión
PPTP_WAN_ERROR_NOTIFY	Notifica un error en la conexión PPP
PPTP_SET_LINK_INFO	Configura la conexión cliente/servidor PPTP
PPTP_STOP_SESSION_REQUEST	Finaliza la sesión
PPTP_STOP_SESSION_REPLY	Respuesta a la solicitud de finalización de sesión

Tabla 4. Mensajes de Control de la sesión de PPTP
Fuente: Metodología para la implementación de un VPN

Fase 3. Data Tunneling. Es el proceso de enviar los datos a través del túnel. Los datos se encapsulan y encriptan en paquetes PPP sobre datagramas IP. Como curiosidad, comentar que la creación de éste se

realiza mediante una versión modificada de GRE Protocolo de encapsulación y encaminamiento genérico.

De esta forma, pueden crearse conexiones WAN seguras y de bajo coste. Esta solución sólo tiene una restricción: el rendimiento. Si la red IP está muy saturada, el túnel sufrirá las consecuencias. Por tanto, puede no ser recomendable para aplicaciones que requieran fiabilidad y rapidez.

PPTP es, en la actualidad, un protocolo pendiente de estandarización y, por el momento sólo está disponible para plataformas Win32 (NT y 95/OSR2 y superiores). Sin embargo, goza del apoyo de las empresas integrantes del PPTP Forum, a saber: Ascend Communications, ECI Telematics, 3Com/US Robotics y, como no, Microsoft.

2.2.2.2.3 Transmisión de nivel 2 (L2F).

En 1996, Cisco System desarrolló un protocolo que iba a emplearse en combinación con el protocolo PPTP de Microsoft. Con el crecimiento de los servicios por marcación y la disponibilidad de muchos protocolos diferentes, se necesitaba crear un escenario de marcación virtual donde cualquiera de los protocolos que no fueran IP pudiesen disfrutar de los servicios de Internet.

Cisco definió el concepto de establecimiento de túneles, como el encapsulamiento de paquetes no IP; es decir los usuarios hacen una conexión PPP o SLIP a un proveedor de Internet por marcación, y con el uso de L2F, se conectan a las máquinas de sus empresas. Estos túneles se encuentran en los extremos de la conexión a Internet, y son enrutados con software para establecimiento de túneles, llamados interfaces de túnel. El reenvío de nivel 2 ofrece muchos beneficios como los siguientes:

- ✓ Independencia del Protocolo (IPX, SNA)
- ✓ Autenticación (PPP, CHAP, TACACS)
- ✓ Administración de direcciones (asignadas por destino)
- ✓ Túneles dinámicos y seguros
- ✓ Apertura de cuentas
- ✓ Independencia de medios, por ejemplo sobre L2F (ATM, X.25, tramas)
- ✓ Tanto el establecimiento de túneles L2F como el acceso local a Internet.

En la configuración básica, el usuario realiza una conexión PPP o una conexión similar al proveedor de Internet local. Con la solicitud del usuario, el servidor, mediante el software L2F, inicia un túnel al destino del usuario. El destino pide la contraseña del usuario y, una vez autorizado, le asigna una dirección IP al usuario, igual que un dispositivo de acceso por marcación típico. El punto terminal quita el encabezado del túnel, registra el tráfico y permite que haya comunicación.
A diferencia del PPTP y del L2TP, el L2F no tiene un cliente definido. Asimismo, el L2F sólo funciona en túneles obligatorios.

2.2.2.2.4 Protocolo de túnel de nivel 2 (L2TP).

En 1996 surgieron los protocolos PPTP y L2F. Compañías como Microsoft, Ascend y 3Com trabajaron en PPTP, mientras que Cisco trabajó en L2F. Dos años más tarde, en 1998, estas compañías acordaron una nueva especificación de prueba para la IETF; el protocolo de establecimiento de túneles de nivel 2 (L2TP).

El L2TP esta compuesto por las mejores características del PPTP y del L2F. Este es un protocolo de red que encapsula las tramas de PPP para enviarlas a través de redes de IP, X.25, Frame Relay o modo de transferencia asíncrona (ATM).

L2TP utiliza dos funciones: una función de servidor de línea tipo cliente (LAC), que es concentrador de acceso L2TP, y una función de servidor de red del lado servidor (LNS). Cuando una computadora realiza una conexión a un proveedor de servicios de Internet, la función LAC inicia el túnel y luego agrega los distintos encabezados a la carga PPP. La LAC establece el túnel al dispositivo de terminación LNS; este dispositivo puede ser un enrutador, un servidor o un dispositivo de acceso. Después de que se estableció el túnel, se configura un mecanismo de autenticación de usuario para establecer la identidad de los usuarios. L2TP utiliza mensajes de control para optimizar el túnel [RFC2661].

Cuando se configura para utilizar el IP y su transporte de datagrama, el L2TP puede utilizarse como un protocolo de túnel a través de Internet. Este también puede utilizarse directamente a través de varios medios de WAN media (como el Frame Relay) sin un nivel de transporte de IP.

El L2TP a través de redes internas de IP utiliza el UDP y una serie de mensajes L2TP para mantener el túnel. El L2TP también utiliza al UDP para enviar tramas de PPP encapsuladas L2TP como los datos en el túnel. Las cargas de pago de las tramas de PPP encapsuladas pueden codificarse y/o comprimirse.

El grafico 12 muestra la forma en que se ensambla un paquete L2TP antes de su transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de una red. El diseño final de trama muestra la encapsulación para un cliente de marcación (controlador de dispositivos PPP). La encapsulación supone el L2TP sobre IP.

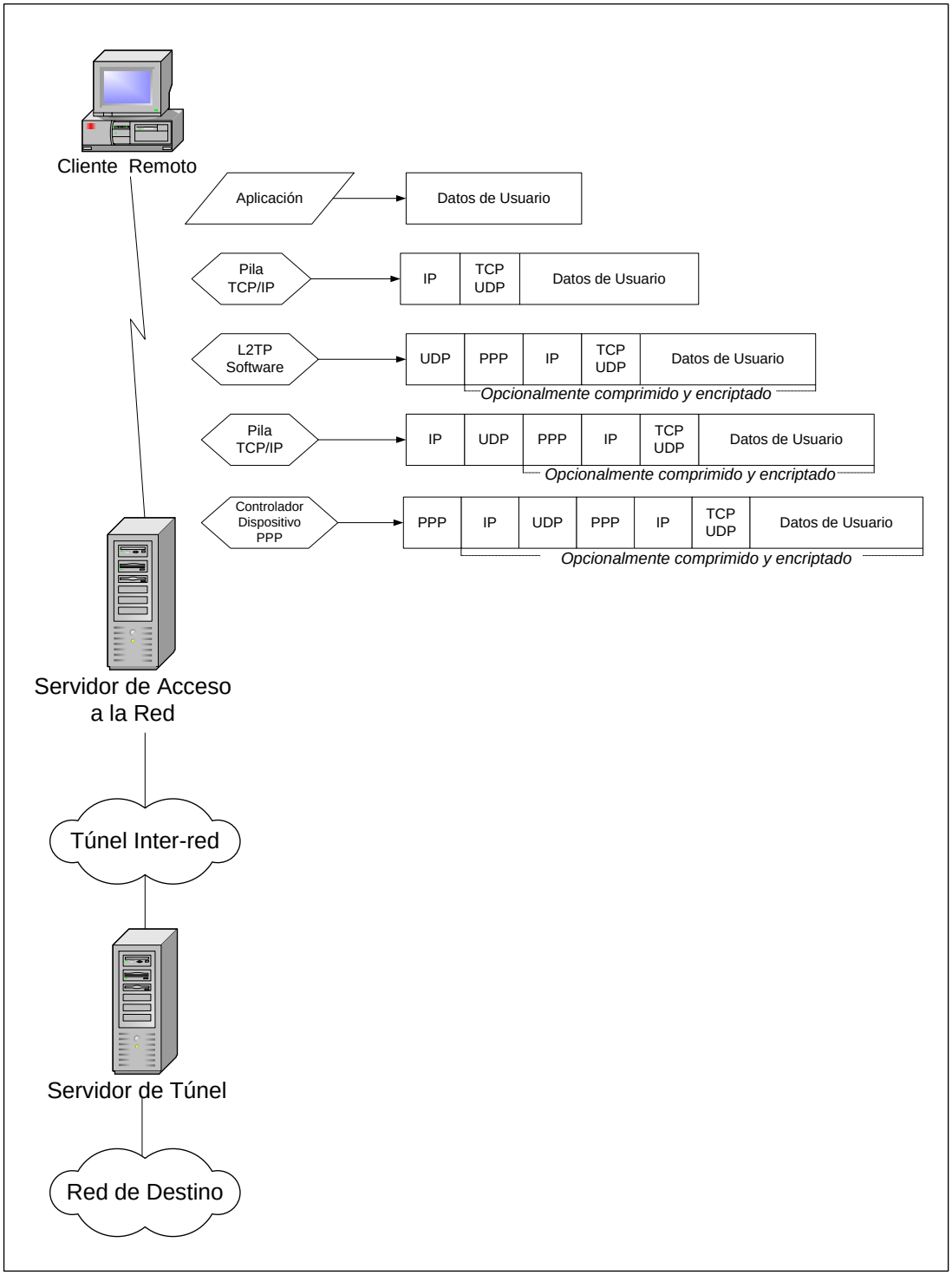


Grafico 12. Construcción de un paquete L2TP
Fuente: Metodología para la implementación de un VPN

PPTP y L2TP ofrecen compresión por software, lo cual reduce los paquetes de usuario, y también las técnicas de compresión añaden otro nivel de cifrado, aunque en pequeñas cantidades.

L2TP es un protocolo de nivel 2, diseñado para encapsular en el nivel 2, e IPSec, que es un protocolo de nivel 3. Por lo tanto IPSec se puede utilizar junto con L2TP para dar más seguridad. Esta es una configuración que se recomienda si se emplea L2TP para instalar seguridad IPSec en un entorno IP.

PPTP comparado con el L2TP

Tanto el PPTP como L2TP utilizan el PPP para proporcionar una envoltura inicial de los datos y luego incluir encabezados adicionales para transportarlos a través de la red. Los dos protocolos son muy similares. Sin embargo, existen diferencias entre el PPTP y L2TP:

- ✓ El PPTP requiere que la red sea de tipo IP. El L2TP requiere sólo que los medios del túnel proporcionen una conectividad de punto a punto orientada a paquetes. Se puede utilizar L2TP sobre IP (utilizando UDP), circuitos virtuales permanentes (PVCs), circuitos virtuales X.25 (VCs) o VCs ATM.
- ✓ El PPTP sólo puede soportar un túnel único entre puntos terminales. El L2TP permite el uso de varios túneles entre puntos terminales. Con el L2TP, uno puede crear diferentes túneles para diferentes calidades de servicio.
- ✓ L2TP proporciona la compresión de encabezados. Cuando se activa la compresión de encabezado, el L2TP opera sólo con 4 bytes adicionales, comparado con los 6 bytes para el PPTP.
- ✓ L2TP proporciona la autenticación de túnel, mientras que el PPTP no. Sin embargo, cuando se utiliza cualquiera de los protocolos sobre IPSec, se proporciona la autenticación de túnel por el IPSec

de tal manera que no sea necesaria la autenticación del túnel nivel 2.

2.2.2.2.5 Protocolo de Internet Seguro (IPSec).

El IPSec (IP Seguro) es un estándar de protocolo de nivel 3 que da soporte a la transferencia protegida de información a través de una red IP.

Se define como un conjunto de protocolos de seguridad que permite agregar encriptado y autenticación a las comunicaciones IP. Mientras el encriptado puede evitar que un usuario no autorizado como típicamente un hacker pueda leer un mensaje, el autenticado puede evitar los ataques a un sitio originados de sitios externos no deseados o hasta de dentro de la propia red del sitio.

Las necesidades de privacidad, autenticación e integridad de un mensaje se cubren con dos de los protocolos incluidos en IPSec: AH y ESP. El primero provee autenticado y por extensión también integridad, y el segundo básicamente encriptado para asegurar la privacidad.

El encabezado de autenticación (AH) describe como autenticar paquetes de datagramas IP (autenticación de datos) y proporciona integridad sin conexión y, si esta implementada, protección contra ataques repetitivos. AH puede utilizarse en los modos de túnel y trasporte. En el modo de transporte, se inserta después del encabezado IP original y protege a los protocolos de nivel superior. En el modo de túnel, se inserta antes del encabezado original y se introduce un nuevo encabezado IP.

La norma de Carga con seguridad de encapsulamiento (ESP) proporciona confianza, autenticación, integridad sin conexión y

servicios contra repeticiones. Este conjunto de servicios en ESP se instala durante el establecimiento de la asociación de seguridad.

Si bien ESP también opcionalmente puede proveer autenticación, no encapsula todo el datagrama dejando abierto el primer encabezamiento, algo que puede ser una necesidad sin exponer mayormente la seguridad. Pero más recomendable resulta usar ambos protocolos juntos cada uno con sus funciones específicas.

IPSec es un protocolo de Capa 3 resultando totalmente transparente a las aplicaciones. Se viene usando cada vez más en las VPNs (Redes Privadas Virtuales) tanto para acceso remoto como intranets extendidas y especialmente en extranets.

Asimismo define los mecanismos de codificación para el tráfico de IP y el formato de un paquete para un IP a través del modo de túnel de IP, mejor conocido como modo de túnel de IPSec. Un túnel de IPSec consta de un cliente de túnel y de un servidor de túnel, los cuales se configuran para utilizar la transmisión en túnel de IPSec y un mecanismo de codificación negociado.

El modo de túnel de IPSec utiliza el método de seguridad negociada para encapsular y codificar todos los paquetes de IP con el fin de lograr una transferencia segura a través de las redes internas de IP públicas o privadas. Después, la carga de pago codificada se encapsula de nuevo en un encabezado de IP de texto plano, y se envía a través de la red interna para que lo reciba el servidor de túnel. Después de recibir este datagrama, el servidor de túnel procesa y descarta el encabezado de IP de texto plano y después decodifica su contenido para recuperar el paquete original de IP de carga útil. Posteriormente, el paquete de IP de carga útil es procesado normalmente y enrutado a su destino.

IPsec se puede usar directamente entre las máquinas que se comunican, o bien a través de un túnel entre los dispositivos periféricos, llamados gateways de seguridad, que las conectan a través de Internet. Las formas de conectividad resultantes se llaman así modo transporte y modo túnel respectivamente.

Un tercer protocolo integrante de IPSec llamado IKE (protocolo Internet Security Association Key Management conocido como ISAKMP/Oakley) se usa para un intercambio seguro de las claves con que se manejan los otros componentes de IPSec. IKE puede operar con claves precompartidas, firmas digitales o con claves públicas basadas en certificados digitales.

El modo de túnel IPSec tiene las siguientes funciones y limitaciones:

- ✓ Sólo da soporte a tráfico IP.
- ✓ Funciona en el fondo de la pila IP; por lo tanto, las aplicaciones y protocolos de niveles más altos heredan su comportamiento.
- ✓ Está controlado por una política de seguridad un conjunto de reglas que se cumplen a través de filtros. Esta política de seguridad establece los mecanismos de encriptación y de túnel disponibles en orden de preferencia y los métodos de autenticación disponibles, también en orden de preferencia. Tan pronto como existe tráfico, los dos equipos realizan una autenticación mutua, y luego negocian los métodos de encriptación que se utilizarán. En lo subsiguiente, se encripta todo el tráfico utilizando el mecanismo negociado de encriptación y luego se envuelve en un encabezado de túnel.
- ✓ Una limitación es que las claves son estáticas y, mientras dura la comunicación, no hay un mecanismo para intercambiar estas claves.

- ✓ Orto problema de IPSec es que cada paquete IP aumenta su tamaño una vez que pasa por el proceso de cifrado. En algunas LAN, el tamaño de MTU (Unidad de Transferencia Máxima) podría obligar a la fragmentación de estos paquetes, lo cual aumenta la carga de red en dispositivos como los enrutadores. La alternativa son los túneles cifrados.

2.2.3 Tipos de túnel.

Se pueden crear túneles de 2 formas diferentes.

Tipo de Tunel	Descripción
Túneles Voluntarios	Una computadora de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, la computadora del usuario es un punto terminal del túnel y actúa como un cliente del túnel
Túneles Obligatorios	Un servidor de acceso de marcación capaz de soportar una VPN configura y crea un túnel obligatorio. Con un túnel obligatorio, la computadora del usuario deja de ser un punto terminal del túnel. Otro dispositivo, el servidor de acceso remoto, entre la computadora del usuario y el servidor del túnel, es el punto terminal del túnel y actúa como el cliente del túnel.

Tabla 5. Tipos de Túnel
Fuente: Metodología para la implementación de un VPN

2.2.3.1 Túneles voluntarios

Una computadora de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, la computadora del usuario es un punto terminal del túnel y actúa como un cliente del túnel.

Un túnel voluntario ocurre cuando una estación de trabajo o un servidor de enrutamiento utilizan el software del cliente del túnel para crear una conexión virtual al servidor del túnel objetivo. Para poder lograr esto se debe instalar el protocolo apropiado de túnel en la computadora cliente. Para los protocolos que se analizan en este documento, los túneles voluntarios requieren una conexión IP (ya sea a través de una LAN o marcación).

En una situación de marcación, el cliente debe establecer una conexión de marcación para conectarse a la red antes de que el cliente pueda establecer un túnel. Este es el caso más común. El mejor ejemplo de esto es el usuario de Internet por marcación, que debe de marcar a un ISP y obtener una conexión a Internet antes de que se pueda crear un túnel sobre Internet.

Para una PC conectada a una LAN, el cliente ya tiene una conexión a la red que le puede proporcionar un enrutamiento a las cargas útiles encapsuladas al servidor del túnel LAN elegido. Este sería el caso para un cliente en una LAN corporativa que inicia un túnel para alcanzar una sub-red privada u oculta en la misma LAN (como sería el caso de la red de Recursos Humanos que se analizó previamente).

Es una equivocación común que las VPNs requieran una conexión de marcación. Sólo requieren de una red IP. Algunos clientes (como las PCs del hogar) utilizan conexiones de marcación al Internet para establecer transporte IP. Esto es un paso preliminar en la preparación para la creación de un túnel, y no es parte del protocolo del túnel mismo.

2.2.3.2 Túneles obligatorios.

Un servidor de acceso de marcación capaz de soportar una VPN configura y crea un túnel obligatorio. Con un túnel obligatorio, la computadora del usuario deja de ser un punto terminal del túnel. Otro dispositivo, el servidor de acceso remoto, entre la computadora del usuario y el servidor del túnel, es el punto terminal del túnel y actúa como el cliente del túnel.

Varios proveedores que venden servidores de acceso de marcación han implementado la capacidad para crear un túnel en nombre del cliente de marcación. La computadora o el dispositivo de red que proporciona el túnel para la computadora del cliente es conocida de

varias maneras como: Procesador frontal (FEP) en PPTP, un Concentrador de acceso a L2TP (LAC) en L2TP o un gateway de seguridad IP en el IPSec. En este capítulo, el término FEP se utilizará para describir esta funcionalidad, sin importar el protocolo de túnel. Para llevar a cabo esta función, el FEP deberá tener instalado el protocolo apropiado de túnel y deberá ser capaz de establecer el túnel cuando se conecte la computadora cliente.

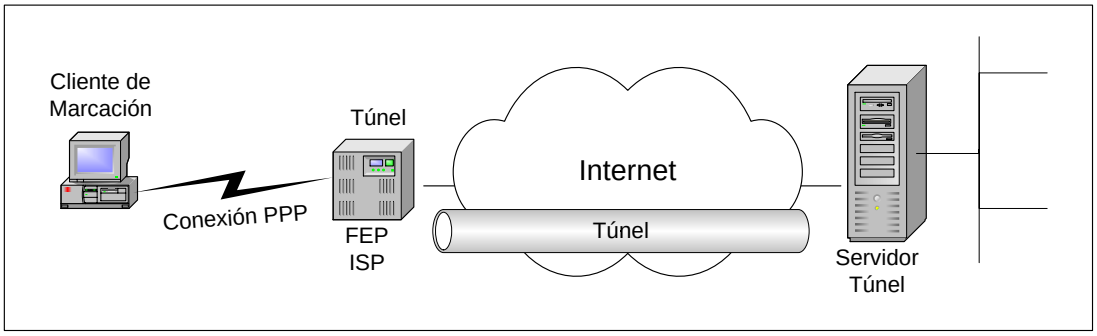


Grafico 13. Túneles obligatorios
Fuente: Metodología para la implementación de un VPN

En el ejemplo de Internet, la computadora cliente coloca una llamada de marcación al NAS activado por los túneles en el ISP. Por ejemplo, una empresa puede haber contratado con un ISP para instalar un conjunto nacional de FEPs. Estos FEPs pueden establecer túneles a través de Internet a un servidor de túnel conectado a la red privada de la empresa, consolidando así las llamadas de diferentes ubicaciones geográficas en una conexión única de Internet en la red corporativa.

Esta configuración se conoce como "túnel obligatorio" debido a que el cliente está obligado a utilizar el túnel creado por FEP. Una vez que se realiza la conexión inicial, todo el tráfico de la red de y hacia el cliente se envía automáticamente a través del túnel. En los túneles obligatorios, la computadora cliente realiza una conexión única PPP y, cuando un cliente marca en el NAS, se crea un túnel y todo el tráfico se enruta automáticamente a través de éste. Se puede configurar un FEP para hacer un túnel a todos los clientes de marcación hacia un

servidor específico del túnel. De manera alterna, el FEP podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.

A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel entre el FEP y servidor del túnel puede estar compartido entre varios clientes de marcación. Cuando un segundo cliente marca al servidor de acceso (FEP) para alcanzar un destino para el cual ya existe un túnel, no hay necesidad de crear una nueva instancia del túnel entre el FEP y el servidor del túnel. El tráfico de datos para el nuevo cliente se transporta sobre el túnel existente. Ya que puede haber varios clientes en un túnel único, el túnel no se termina hasta que se desconecta el último usuario del túnel.

A la fecha, los túneles voluntarios han probado ser el tipo más popular de túnel.

2.3 METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UNA VPN

Para obtener una Red Privada Virtual exitosa es necesario tomar en cuenta algunos factores que son de vital importancia los mismos que se convertirán en pasos para el análisis y posterior implementación de una Red Privada Virtual; estos factores forman parte de la metodología:

2.3.1 Metodología TOP-DOWN

Es una metodología que propone cuatro Fases, para el diseño de la rede privada virtual VPN.

I. Fase 1: Análisis de Negocios Objetivos y limitaciones
II. Fase 2: Diseño Lógico
III. Fase 3: Diseño Físico
IV. Fase 4: Pruebas, Optimización y Documentación de la red

I. Fase de Identificación de Necesidades y Objetivos de los Clientes

En esta fase se identificará los objetivos y restricciones del negocio, y los objetivos y restricciones técnicos del cliente.

1. Análisis de los Objetivos y Restricciones del Negocio
2. Análisis de los Objetivos Técnicos y sus Restricciones
3. Caracterización de la Red Existente
4. Caracterización del tráfico de la red

A. Analizar los objetivos del negocio

- ✓ Conocer línea de negocio y el mercado del cliente
- ✓ Estructura organizacional la empresa
- ✓ Conocer sus proveedores
- ✓ Filiales, Oficinas remotas
- ✓ Determinar la autoridad responsable para la aceptación del Diseño de Red propuesto.
- ✓ Realizar un cuestionario de preguntas a los clientes para conocer sus objetivos hacia su negocio.
- ✓ Identificar los cambios que el proyecto generaría.

II. Fase de Diseño Lógico

En esta fase se diseñará la topología de red, el modelo de direccionamiento y nombramiento, y se seleccionará los protocolos de bridging, switching y routing para los dispositivos de interconexión. El diseño lógico también incluye la seguridad y administración de la red.

1. Diseño de la Topología de red
2. Diseño de Modelo de Direccionamiento y Nombramiento
3. Selección de Protocolos de Switching y Routing
4. Desarrollo de estrategias de seguridad de la red
5. Desarrollo de estrategias de Gestión de la red.

III. Fase de Diseño Físico

Esta fase implica en seleccionar las tecnologías y dispositivos específicos que darán satisfacción a los requerimientos técnicos de acuerdo al diseño lógico propuesto (LAN / WAN).

1. Selección de Tecnologías y dispositivos para la red del Campus
   - ✓ Diseño del Cableado Estructurado
   - ✓ Tecnologías LAN: ATM, Fast Ethernet, Giga Ethernet
   - ✓ VoIP
   - ✓ Switch
   - ✓ Router
   - ✓ Bridge
   - ✓ Inalambrico
   - ✓ Radio enlaces
   - ✓ Otros

2. Selección de Tecnologías y dispositivos para la red Empresarial Tecnología de acceso remoto
   - ✓ Línea de Suscripción Digital (DSL)
   - ✓ Red Privada Virtual (VPN)
   - ✓ Línea Dedicada
   - ✓ Acceso Satelital
   - ✓ Otros

IV. Fase de Prueba, Optimización y Documentación

Cada sistema es diferente; la selección de métodos y herramientas de prueba correctos, requiere creatividad, ingeniosidad y un completo entendimiento del sistema a ser evaluado.

Implementación de un Plan de Pruebas.

1. Prueba del Diseño de la red

- ✓ Usar pruebas de los fabricantes
- ✓ Construir un prototipo de pruebas
- ✓ Herramientas de prueba de diseño de redes
- ✓ Un escenario de prueba del Diseño de red
- ✓ La prueba debe incluir análisis de performance y de fallas:
  - – Prueba de aplicación de tiempo de respuesta
  - – Prueba de Rendimiento
  - – Prueba de la Disponibilidad
  - – Prueba de Regresión

2. Optimización del Diseño de la red
   - ✓ Optimización del uso del ancho de Banda con Tecnología IP Multicast.
   - ✓ Reduciendo el Delay de la serialización.
   - ✓ Optimización de la performance de la red para QoS.
   - ✓ Cisco Internetwork Operating System Features for Optimizing Network
3. Documentación de la red
   - ✓ Respondiendo a la propuesta de los requerimientos del cliente
   - ✓ Los contenidos de los documentos del Diseño de la Red

2.4. ELECCIÓN DE LA METODOLOGÍA DE SOLUCIÓN.

Para el presente trabajo se ha propuesto utilizar la metodología para implementar proyectos de redes propuesta por James McCabe el Top-Down, dicha metodología se adecua al propósito para Interconectar la Sede Central del Gobierno Regional de Huancavelica y sus locales descentralizados ubicados en distintos lugares geográficos de la cuidad de Huancavelica a través de la implementación de una Red Privada Virtual (VPN), y se obtiene resultados positivos, en el logro de los objetivos establecidos.

PRESENTACIÓN DE RESULTADOS

CAPITULO III
ANÁLISIS DE REQUERIMIENTOS

3.1 REQUERIMIENTOS BÁSICOS

Una Red Privada Virtual ha de proveer de los siguientes mecanismos básicos, aunque en ocasiones y situaciones puede obviarse algunos.

3.1.1 Con respecto a la Tecnología.

- ✓ Rendimiento escalable y capacidad de ancho de banda, el cual permita acomodar la demanda de tráfico entre los diferentes locales del Gobierno Regional de Huancavelica.
- ✓ Aplicaciones de red diferenciadas, con la finalidad de compartir aplicaciones entre todos los usuarios con seguridad.
- ✓ Alta disponibilidad de la red, disponiendo de esta las 24 horas del día.
- ✓ Se deberá asegurar que los medios de transmisión soporten voz, datos y video con la finalidad de implementar en el futuro el servicio de VoIP con las diferentes Gerencias Sub Regionales de la Región de Huancavelica.
- ✓ El Servidor VPN deberá contar con un Software que funcione como firewall de Redes, el cual permita brindar un servicio eficiente a las estaciones de trabajo usuarias.

3.1.2 Con respecto al tipo de conexión.

- ✓ **OFICINA CENTRAL:**

  Corresponde a una red corporativa o la red LAN. Esta tendrá que disponer de una IP fija a través de una conexión ADSL para acceso a Internet. Debe disponer además de un dispositivo (Firewall o Router) VPN el cual administre el túnel y que permita dar acceso autentificado y seguro a los usuarios y oficinas remotas.

- ✓ **USUARIOS REMOTOS:**

  Estos deberan de conectarse a un área de trabajo mediante una configuracion al servidor VPN atraves del Internet (con o sin IP fija) el cual permitira el contacto con la red privada (Sede Central del GRH), como si se tratase de un puesto mas de la Red Privada.

- ✓ **OFICINAS REMOTAS:**

  Tendrán que disponer de una conexión a la Internet (no es necesario tener IP fija) y una configuracion de una nueva conexión de red VPN les permitira ponerse en contacto con la Red Privada (Sede Central del GRH) en forma confidencial.

3.1.3 Con respecto a las normas de seguridad

- ✓ **AUTENTIFICACION DEL USUARIO:**

  La configuración VPN deberá verificar la identidad del usuario y permitir el acceso solo a usuarios autorizados.

- ✓ **ENCRIPTACION DE DATOS:**

  Los datos que viajan por la Red Publica fuera de los equipos terminales no podrán ser leídos por clientes no autorizados en la red, por esta razón se utilizan normas de encriptación.

- ✓ **ADMINISTRACION DE DIRECCION:**

  Se deberá asignar a cada cliente de la red interna una dirección de IP privada.

- ✓ **ADMINISTRACION DE LLAVES:**

  La alternativa VPN deberá generar y renovar las llaves de encriptación para el cliente y el servidor.

  Para establecer una conexión VPN entre el servidor VPN de la Sede Central del Gobierno Regional de Huancavelica y un host remoto de uno de los locales desentralizados, ambas partes deben tener la misma llave criptográfica. Esta llave es imprescindible para la autenticación y codificación de su tráfico, lo que garantizará que sus comunicaciones no puedan ser interceptadas por terceros.

  Una llave criptográfica se genera de forma automática y se guarda en un directorio especial durante la instalación del componente. De todas formas, puede que desee reemplazar la llave inicial por la nueva.

- ✓ **SOPORTE DE PROTOCOLO MULTIPLE:**

  Se debe habilitar soporte para los protocolos más comunes o usuales utilizados en las redes públicas. Se incluyen protocolos de Internet (IP), central de paquetes de Internet (IPX), etc.

3.2 FASE DE DIAGNOSTICO Y ANÁLISIS

3.2.1 Diagnostico Actual del GRH

El Gobierno Regional de Huancavelica, cuenta con una red de datos, que data del año 2008, cuenta con un parque informático, compuesto de 500 equipos de cómputo aproximadamente, 200 impresoras láser, 08 servidores, todos ellos distribuidos en los diferentes locales y dependencias administrativas de todo el Gobierno Regional; la infraestructura de comunicaciones no están acorde a las necesidades de los sistemas administrativos como el SIAF, SIGA, SUP; una comunicación a través de telefonía VoIp y

dominio regional los cuales dependen de un correcto funcionamiento de la red entre la sede central y sus diferentes locales descentralizados.

En los últimos años la institución viene presentando problemas e inconvenientes en la plataforma de comunicaciones a nivel institucional entre la Sede Central del Gobierno Regional de Huancavelica y sus locales descentralizados ubicados en distintos lugares geográficos de la cuidad de Huancavelica. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes deberían de cumplir con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos. Se ha demostrado que en la actualidad 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 sedes remotas a varios kilómetros de distancia.

Ante ello la Sede Central del Gobierno Regional, tiene rentado el servicio de internet de 15 Mbps al 10%, una línea dedicada de 6 Mbps al 100%, la cual está previsto soportar el acceso promedio de 100 host y se tiene un promedio de 50 usuarios quienes se conectaran constantemente a la LAN del local central.

Se ha efectuado un test de velocidad al ancho de banda de la línea de internet de la Sede Central del Gobierno Regional de Huancavelica con la ayuda del software generador de tráfico JPerf, como podemos observar en la siguiente imagen la sede central cuenta con una línea de ancho de banda que llega aproximadamente 14 MBytes y de acuerdo a la simulación se puede observar que en un intervalo de 10 segundos se han transferido de 13636 a 14167 MBytes de información en un ancho de banda de 14167 MBytes/sec como máximo; por lo tanto se concluye que la línea de internet del Gobierno Regional de Huancavelica cuenta con un ancho de banda

óptimo para poder realizar las conexiones con las sedes descentralizadas a través de la red privada virtual (VPN).

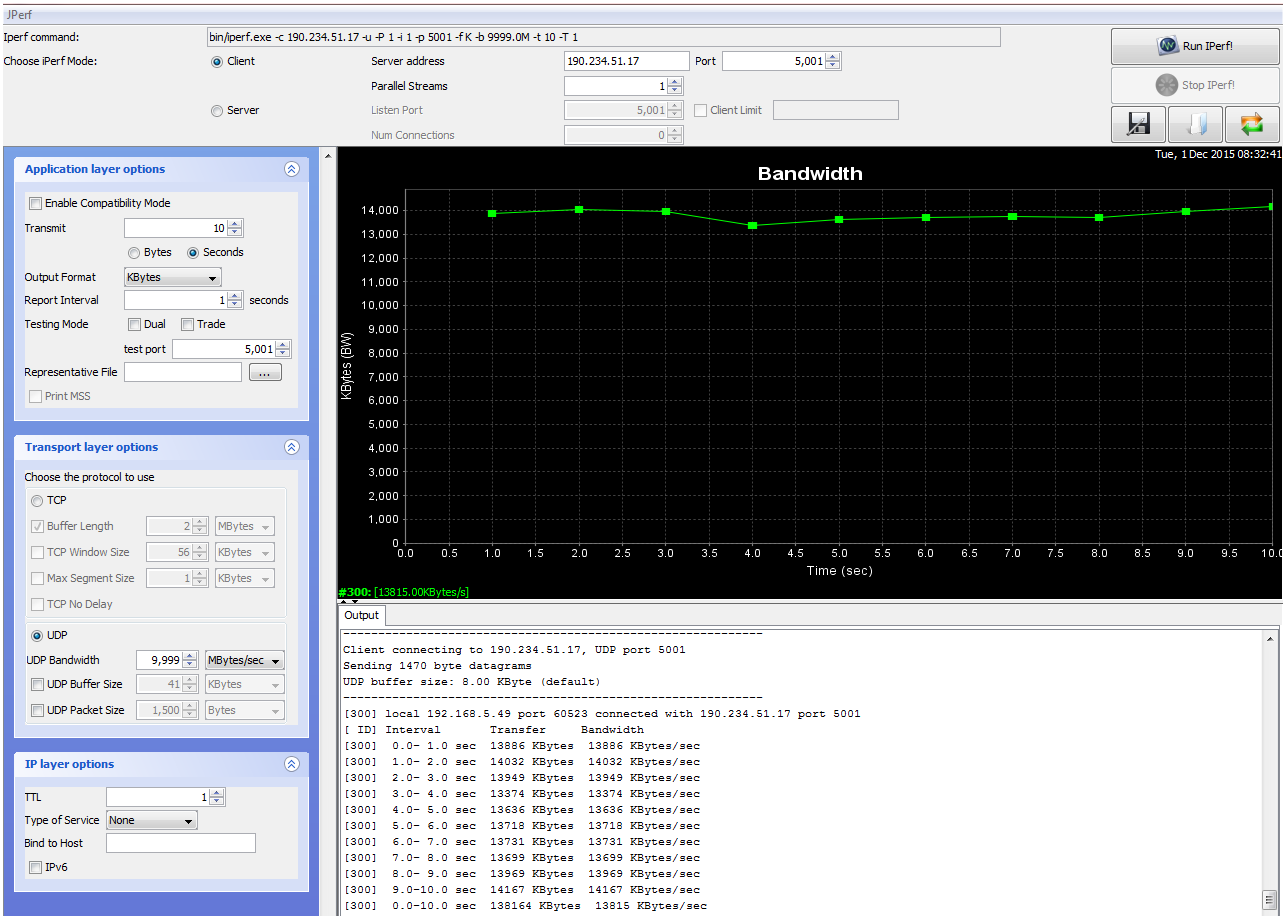


Grafico 14. Testing del ancho de banda del local central.
Fuente: Propia

Se realizó un test de velocidad al ancho de banda de la línea de internet a uno de los locales descentralizados, el local de la Dirección Regional de Transportes y Comunicaciones con la ayuda del software generador de tráfico JPerf, en el test podemos observar que el local cuenta con un ancho de banda que llega aproximadamente a 9 MBytes y de acuerdo a la simulación se puede observar que en un intervalo de 10 segundos se han transferido de 9.114 a 9.811 MBytes de información en un ancho de banda de 7.466 MBytes/sec como máximo; los demás locales descentralizados de igual manera

cuentan con un ancho de banda similar al de la Dirección Regional de Transportes y Comunicaciones.

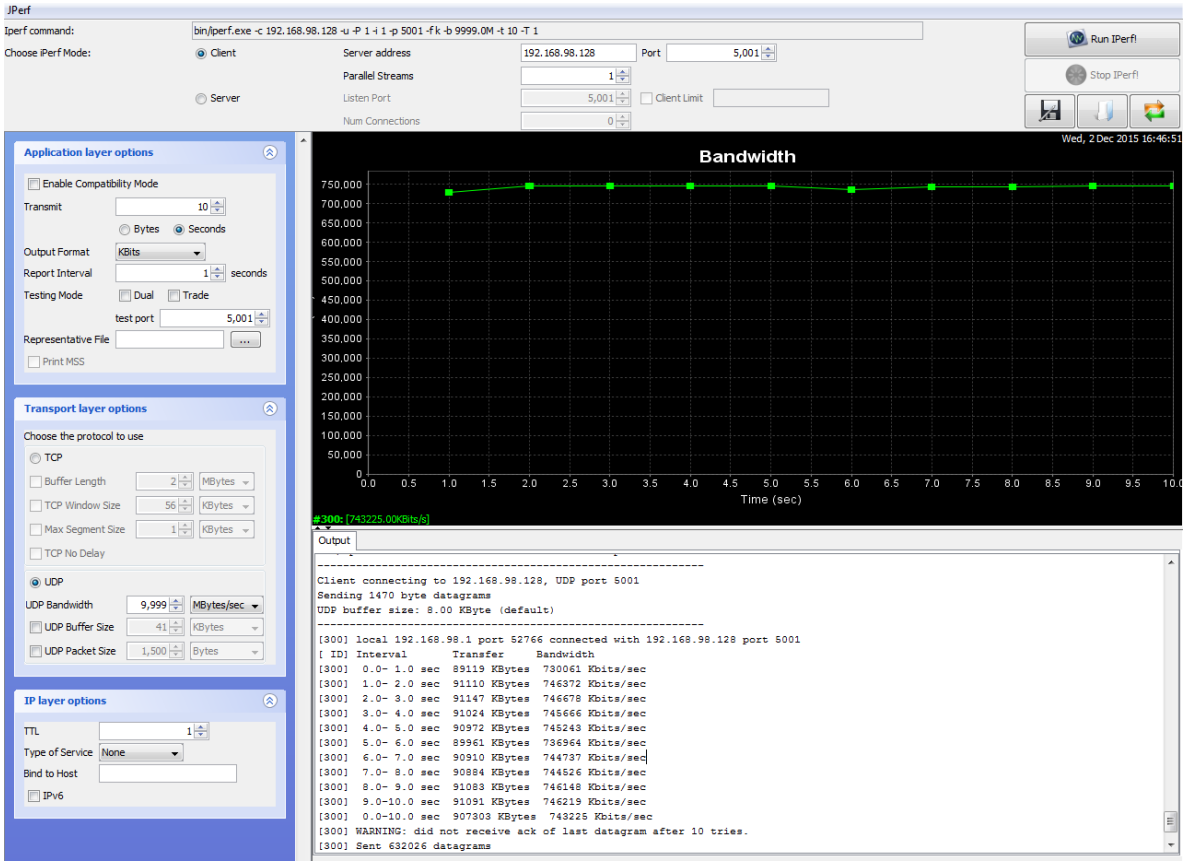


Grafico 15. Testing del ancho de banda de la DRTyC
Fuente: Propia

SITUACIÓN ACTUAL DEL GOBIERNO REGIONAL DE HUANCAVELICA, VISTO POR LOCALES Y DESCRITOS POR GERENCIAS, DIRECCIONES, OFICINAS QUE FUNCIONAN EN ESTOS LOCALES DESCENTRALIZADOS.

1. DESCRIPCIÓN DEL FUNCIONAMIENTO DE LA LAN DREH:

En la LAN 01 (primer local) funcionan todas las áreas de la Dirección Regional de Educación de Huancavelica. Encargado de Formular, aprobar, ejecutar, administrar y evaluar las políticas regionales de educación, ciencia, tecnología, cultura, arte,

deporte y recreación. Compatibiliza Política Educativa Nacional y Proyecto Educativo Regional: Calidad, Equidad e Inclusión.

2. **DESCRIPCIÓN DEL FUNCIONAMIENTO DE LA LAN DRA:**

   En la LAN 02 (segundo local) funcionan todas las áreas de la Dirección Regional de Agricultura. Encargado de Promover el desarrollo económico de la región e impulsar la Competitividad de la actividad agropecuaria en la región Huancavelica, buscando la participación de la inversión pública y privada para mejorar la calidad de vida de los productores Agropecuarios, así como promover el uso adecuado de los recursos

3. **DESCRIPCIÓN DEL FUNCIONAMIENTO DE LA LAN DRTyC:**

   En la LAN 03 (tercer local) funcionan la Gerencia de Infraestructura, la Dirección Regional de Vivienda, Construcción y Saneamiento, Sub Gerencia de Obras, Oficina Regional de Supervisión y Liquidación, la sub Gerencia de estudios. Encargado de Promover y regular los sistemas de transporte y comunicaciones, en el marco de una economía de libre competencia; priorizando la integración regional y transporte terrestre eficiente, con la finalidad de mejorar la calidad de vida de la población

4. **DESCRIPCIÓN DEL FUNCIONAMIENTO DE LA LAN MERCADO:**

   En la LAN 04 (cuarto local) funcionan la Dirección Regional de Producción, Dirección Regional de Comercio, Turismo y Artesanía, Área de Archivo Central, Procuraduría Pública Regional, Dirección Regional de Energía y Minas, Dirección Regional de Energía y Minas, Dirección Regional de Defensa Nacional, Seguridad Ciudadana y Defensa Civil, Dirección Regional de Camélidos Sudamericanos; Dependientes administrativa mente de la sede central.

3.2.2 Mapa de Aplicación

Aquí describimos cada uno de los servidores que están ubicados en cada uno de los locales descentralizados del Gobierno Regional de Huancavelica incluyendo la Sede Central, se especifica el nombre de cada uno de los servidores y los sistemas administrativos con el que cuenta la institución los mismos que serán compartidos a través de la VPN, el mapa de aplicación está basado en un diagrama de todos los locales descentralizados, estas ubicaciones refleja actualmente la situación real que muestra el Gobierno Regional de Huancavelica con sus locales separados geográficamente.

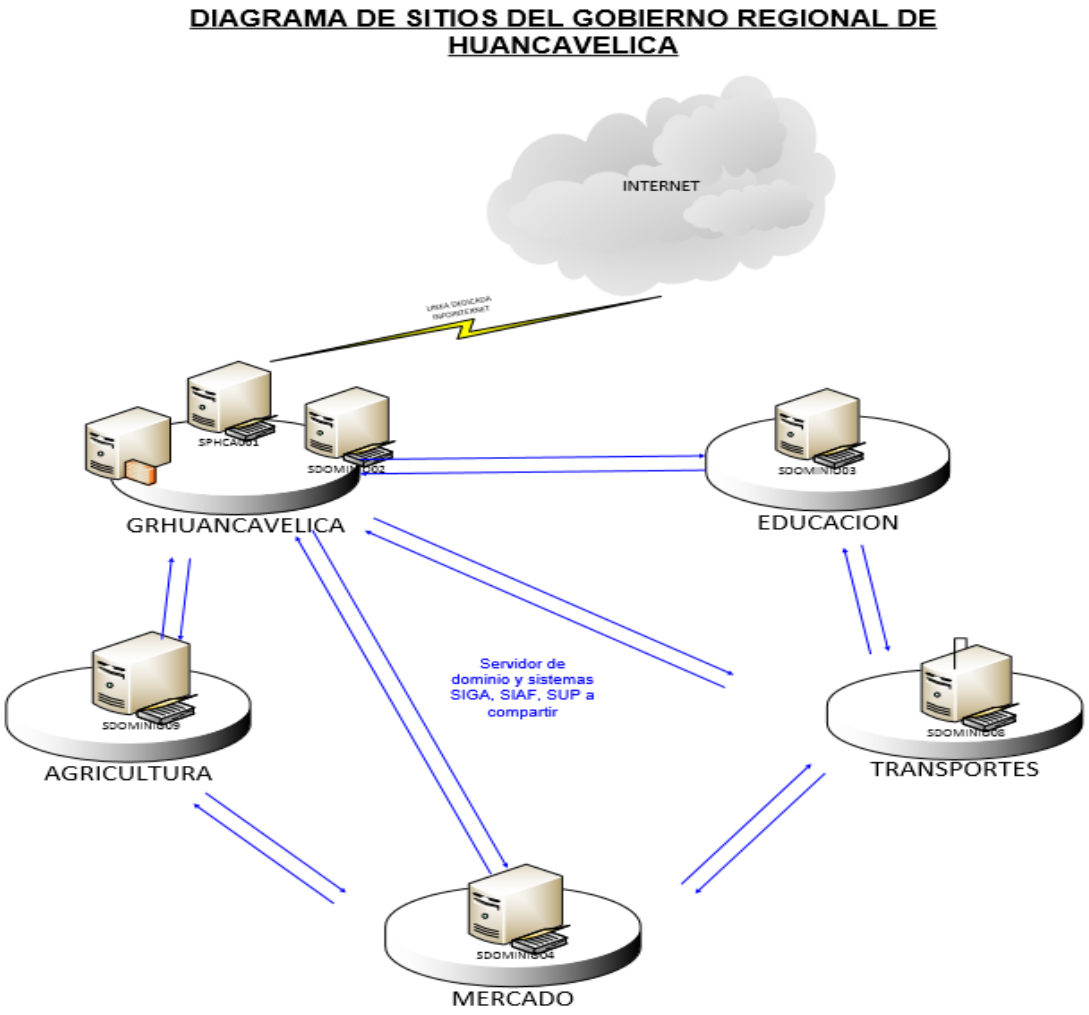


Grafico 16. Diagrama de Locales Descentralizados
Fuente: Propia

3.2.3 Plano de la situación actual de La Institución.

Mostramos a continuación los planos de la organización, por pisos en ella se detalla la ubicación de todas las áreas que funcionan en la sede central y en ello se muestran los equipos de cómputo, cableado de red, equipamiento de comunicaciones de red, en los ANEXO.

En el siguiente diagrama se muestran los servidores con los que cuenta el Gobierno Regional de Huancavelica – Local Central, ahí podemos observar que el Servidor Forefront VPN de marca HP Proliant DL 380G5 se encuentra instalado y conectado en la LAN de la institución a través de un Switch 3com Baseline 2948.

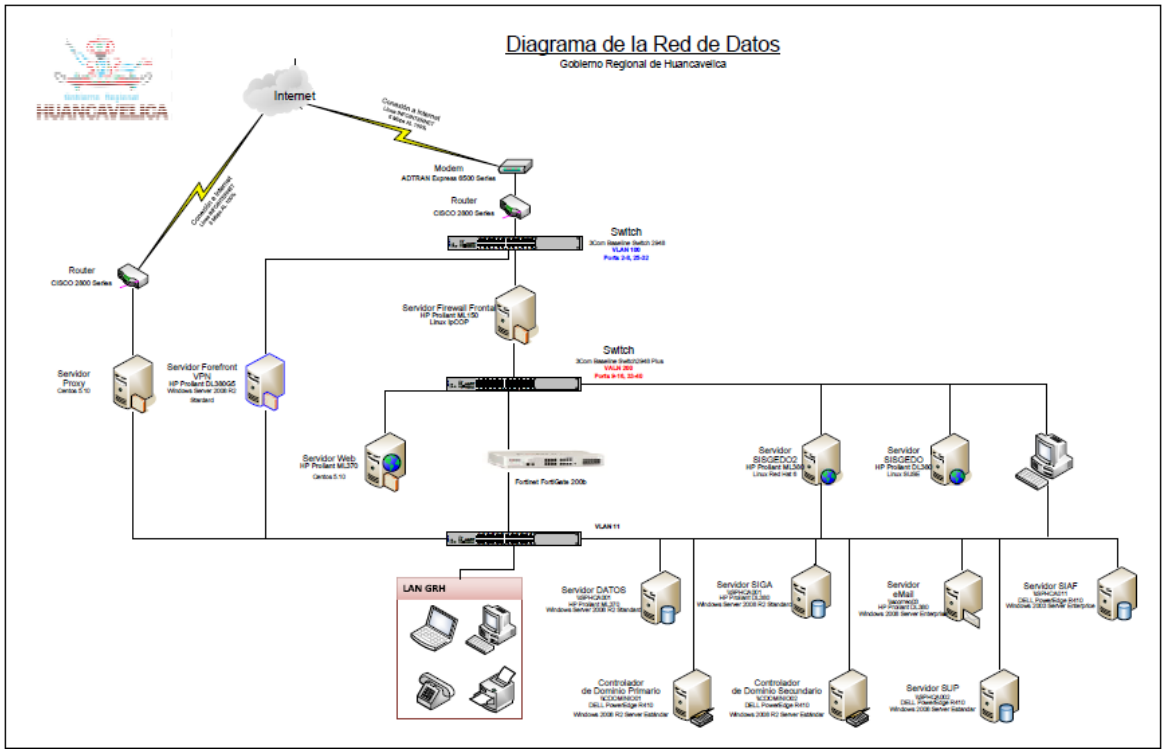


Grafico 17. Diagrama de la Red de Datos
Fuente: Propia

CAPITULO IV

IMPLEMENTACIÓN DE LA VPN

4.1 Implementación del Servidor VPN.

Ahora se procederá a la implementación y configuración de la Red Privada Virtual a través del Microsoft Forefront Threat Management Gateway (TMG) en el Gobierno Regional de Huancavelica, para ello se aplicará todo lo relacionado con los capítulos anteriores, se instalara y configurara un servidor de dominio para la institución, seguidamente se instalará el Microsoft Forefront para levantar el servicio de VPN en un servidor destinado para este servicio. Los 2 servidores a utilizar cuentan con la licencia del sistema operativo Windows Server 2008 R2, el servidor para el servicio de VPN tiene instalado 2 tarjetas de red y un soporte de hardware suficiente para las demandas de todos los usuarios de la institución.

Es importante hacer mención que para la implementación de este proyecto se debe tener acceso total al servidor, además de que la configuración de algunos componentes requerirán del reinicio de este.

4.2 Configuración del Active Directory del Servidor de Dominio.

En el grafico número 18 se visualiza la configuración de la tarjeta de red, la IP asignada es 192. 168.20.20, la máscara 255.255.255.0, la puerta de enlace vendría hacer el IP del servidor de VPN, el DNS vendría a ser la

dirección de la tarjeta de red interna. En el grafico numero 19 muestra el nombre del Bosque asignado al dominio: **GRHUANCAVELICA.GOB.PE**, como también las unidades orgánicas creadas en el Active Directory y el grupo de usuarios quienes tendrán acceso a la VPN.

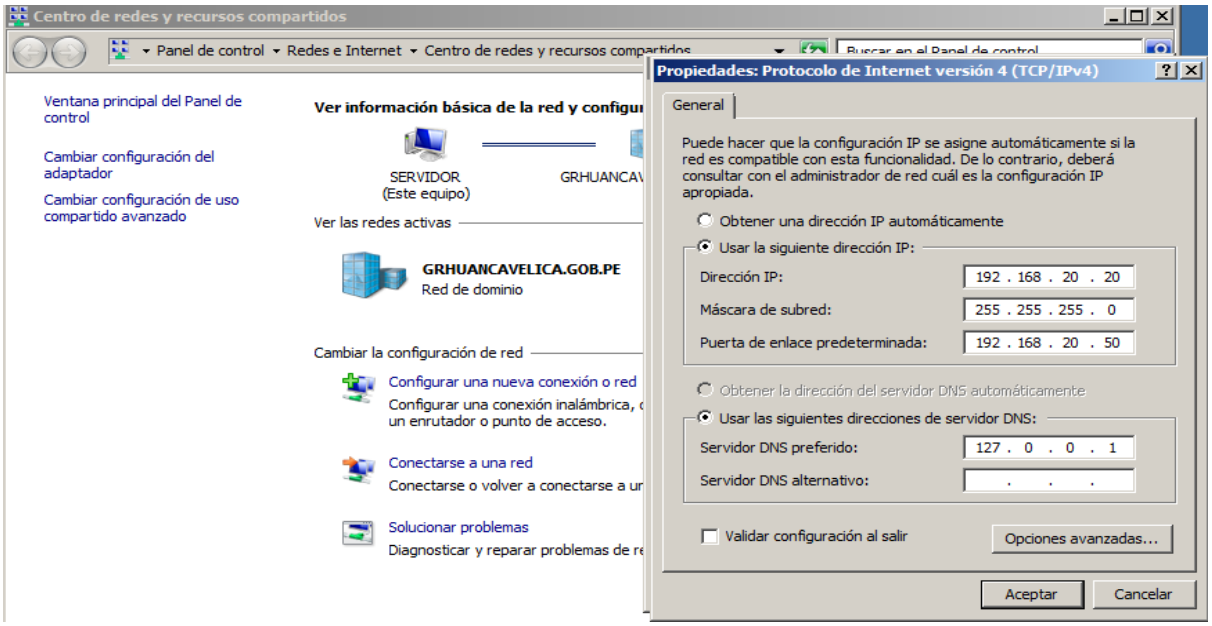


Grafico 18. Configuración de la tarjeta de red.
Fuente: Propia

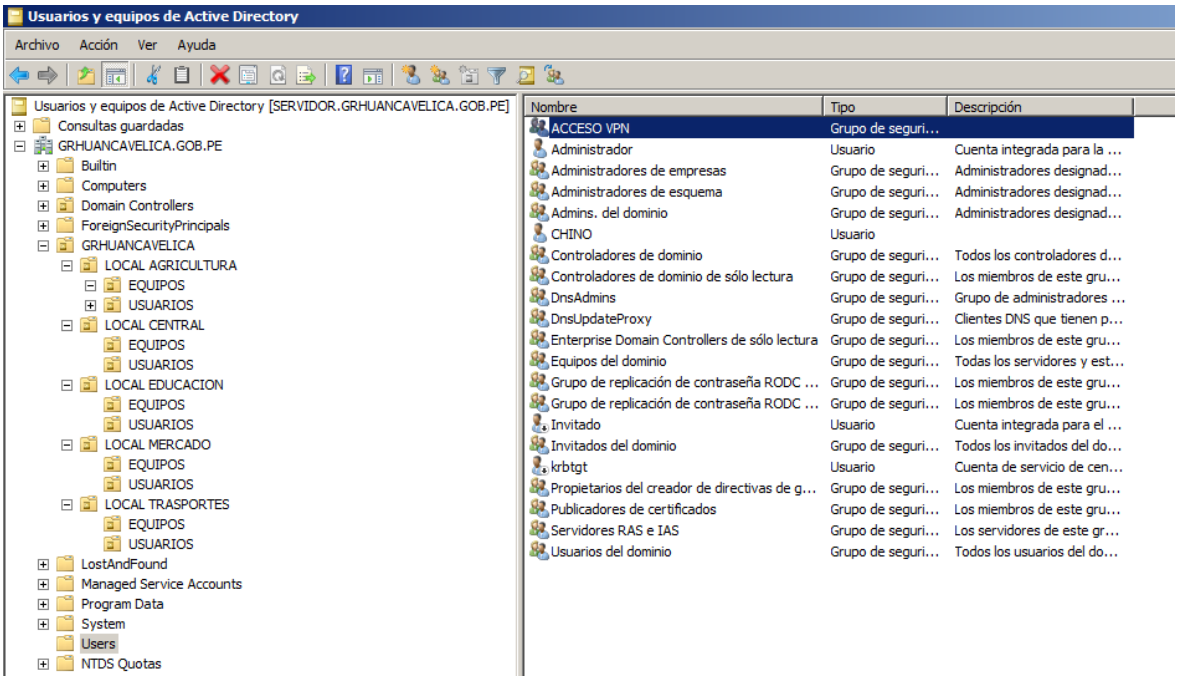
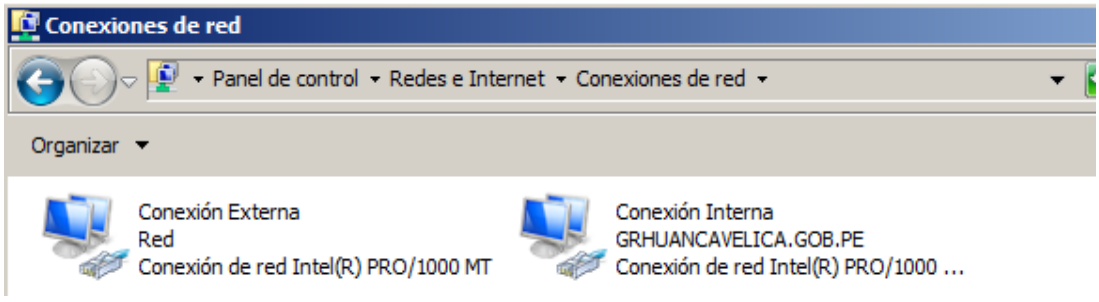


Grafico 19. Configuración de Active Directory.
Fuente: Propia

4.3 Configuración e Instalación del Servidor VPN.

4.3.1 Configuración de las tarjetas de red:

Dentro del menú inicio se da clic en la opción conexiones de red; ahí se encontrara las dos tarjetas de red, seguidamente renombraremos la primera tarjeta a conexión externa es la que permitirá acceso a Internet y que usa una IP WAN, la segunda tarjeta de red será denominada conexión Interna que es de donde se toma la salida para distribuir los servicios internos a la red del Gobierno Regional de Huancavelica.



En el grafico 20 observamos la configuración de la red externa con la siguiente dirección IP: 192.168.206.136, mascar: 255.255.255.0, puerta de enlace 192.168.206.2 y en DNS: 192.168.206.2

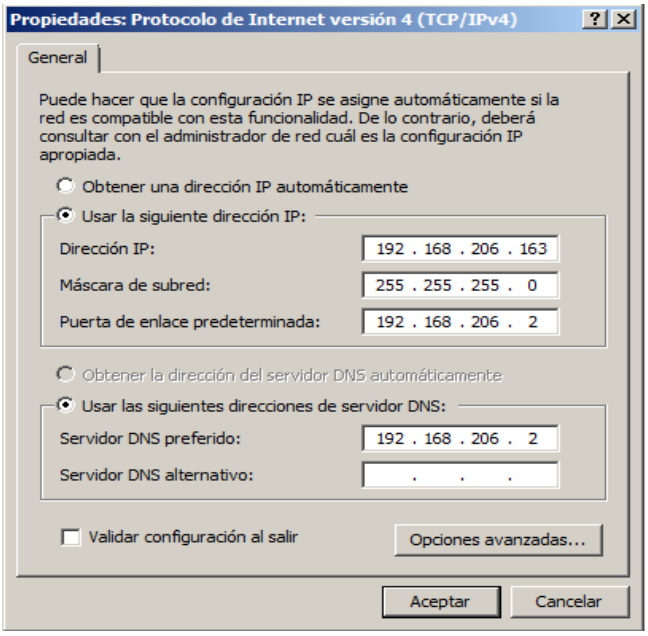


Grafico 20. Configuración de la red externa.
Fuente: Propia

El siguiente grafico muestra la configuración de la red interna con la siguiente dirección IP: 192.168.20.50, mascar: 255.255.255.0 y el DNS: la IP de nuestro servidor de dominio 192.168.20.20

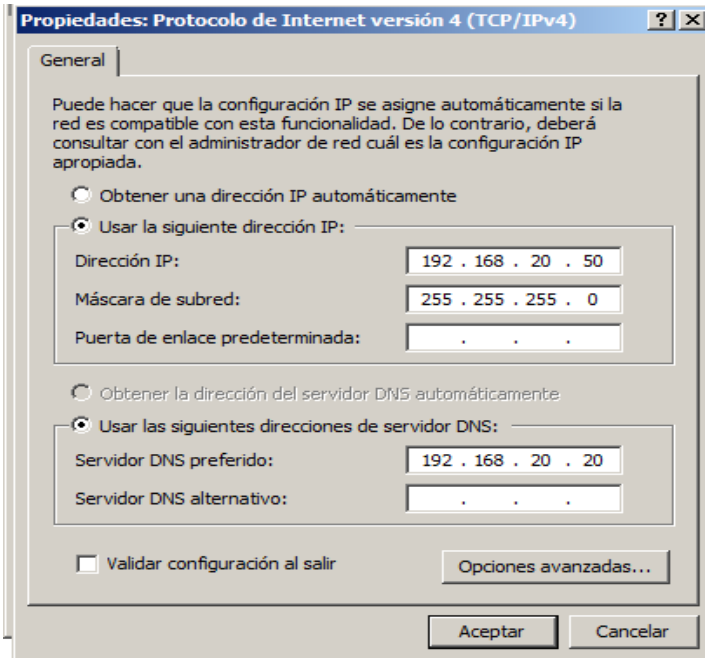


Grafico 21. Configuración de la red interna.
Fuente: Propia

4.3.2 Instalación del Microsoft Forefront Threat Management Gateway (TMG):

Grafico 22. Ventana de instalación del Forefront.
Fuente: Propia

En el grafico 23 se muestra la preparación de herramientas para la instalación del Forefront, tendremos que poner siguiente.

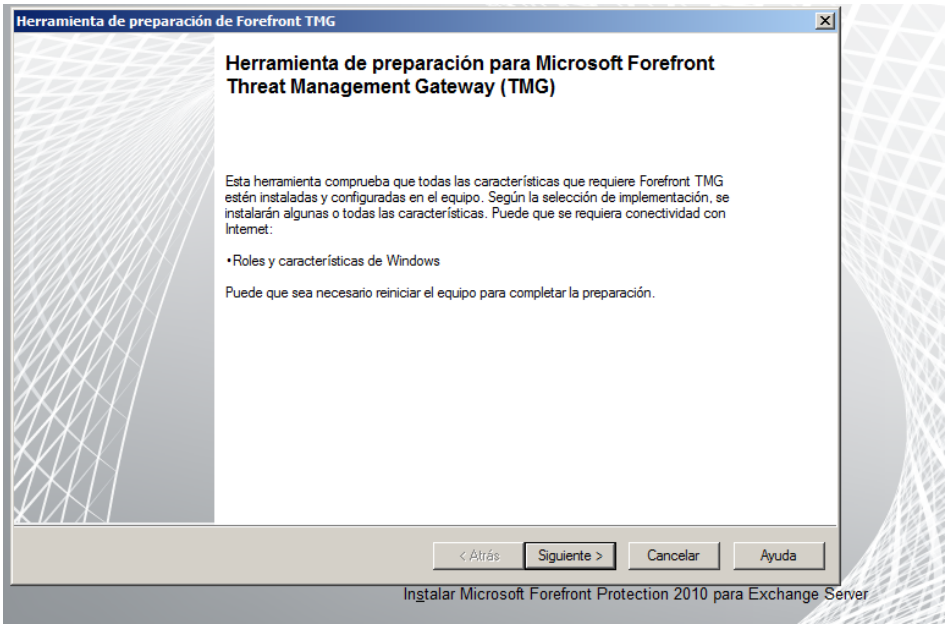


Grafico 23. Herramienta de preparación para TMG.
Fuente: Propia

En el grafico 24 se tendrá que aceptar los términos de licencia y elegir siguiente.

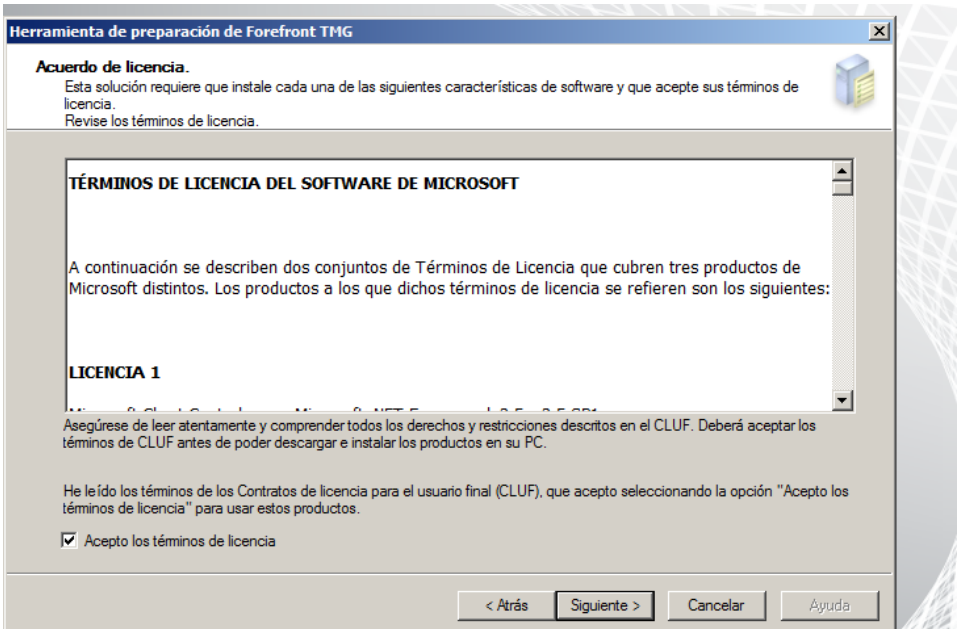


Grafico 24. Términos de licencia del TMG.
Fuente: Propia.

En el grafico 25 se debe de elegir el tipo de instalación: servicios y administración del Forefront TMG

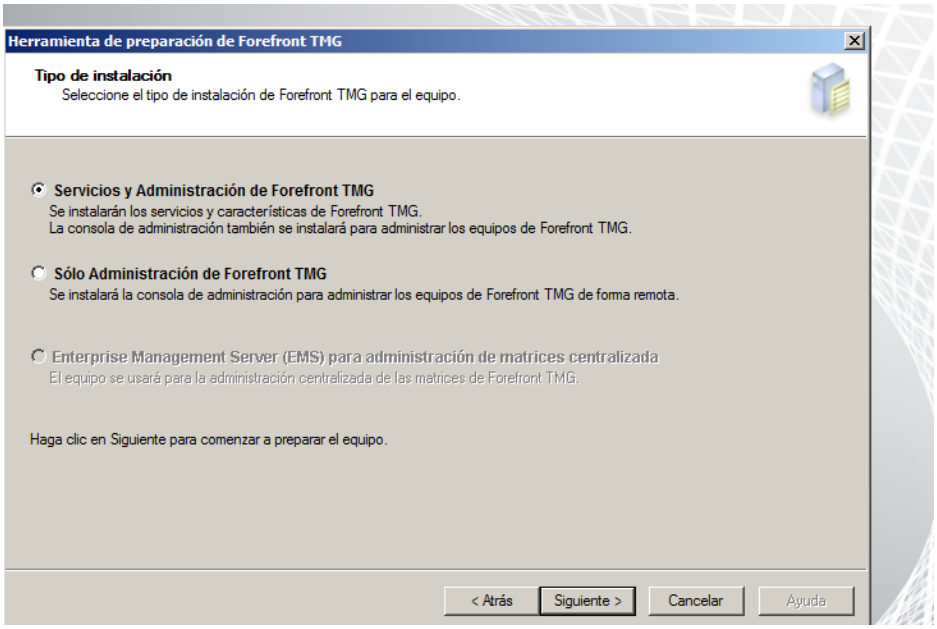


Grafico 25. Tipo de instalación del TMG.
Fuente: Propia

En este grafico nos muestra que todas las características de requisitos previos están instaladas y configurados.

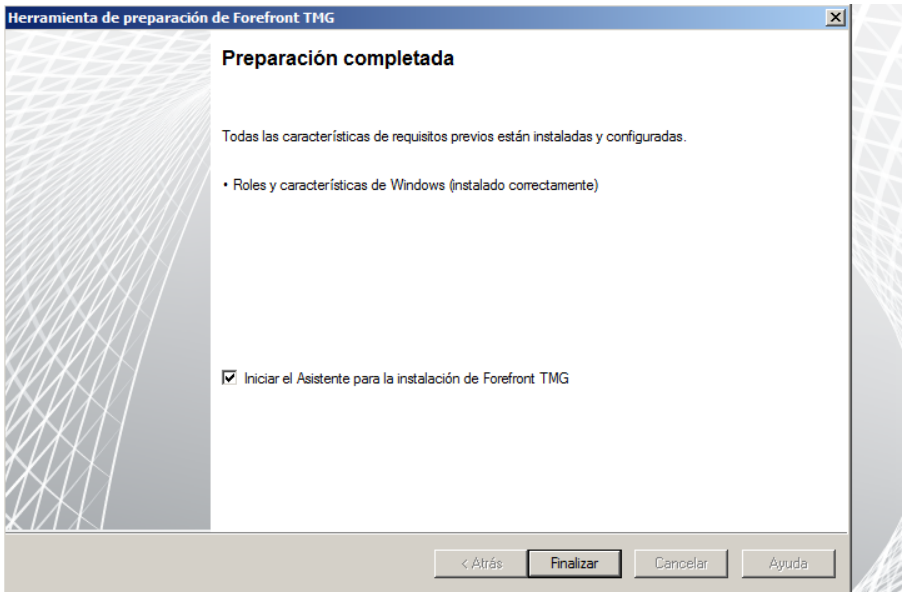


Grafico 26. Preparación completada.
Fuente: Propia

En el grafico 27 se visualiza el asistente para la instalación del Forefront TMG, elegir siguiente

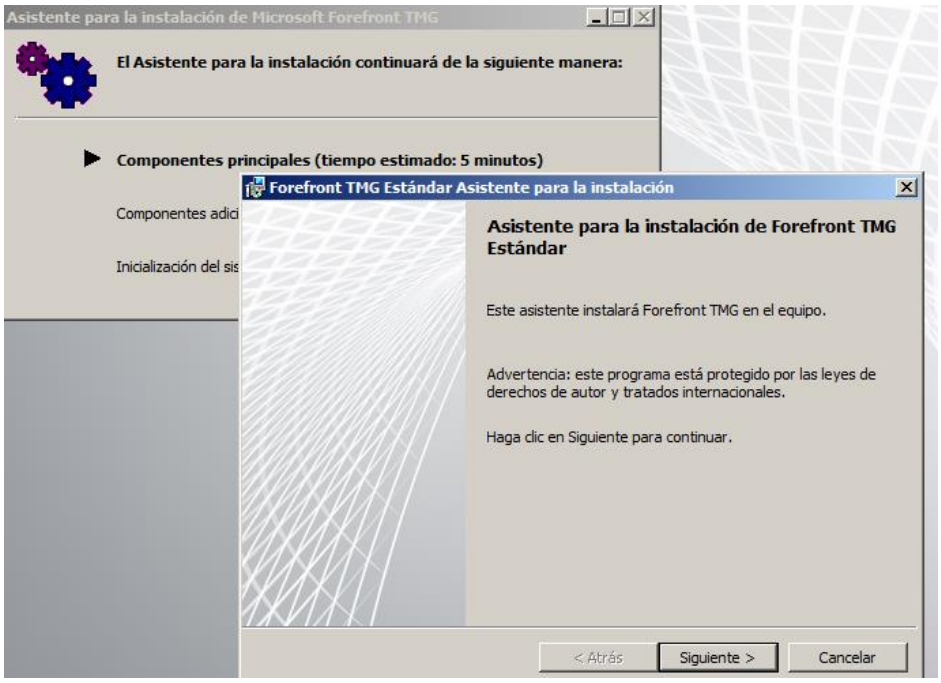


Grafico 27. Asistente para la instalación del TMG.
Fuente: Propia

En el grafico 28 especifica el número de serie del producto, se debe de ingresar el usuario y la organización.

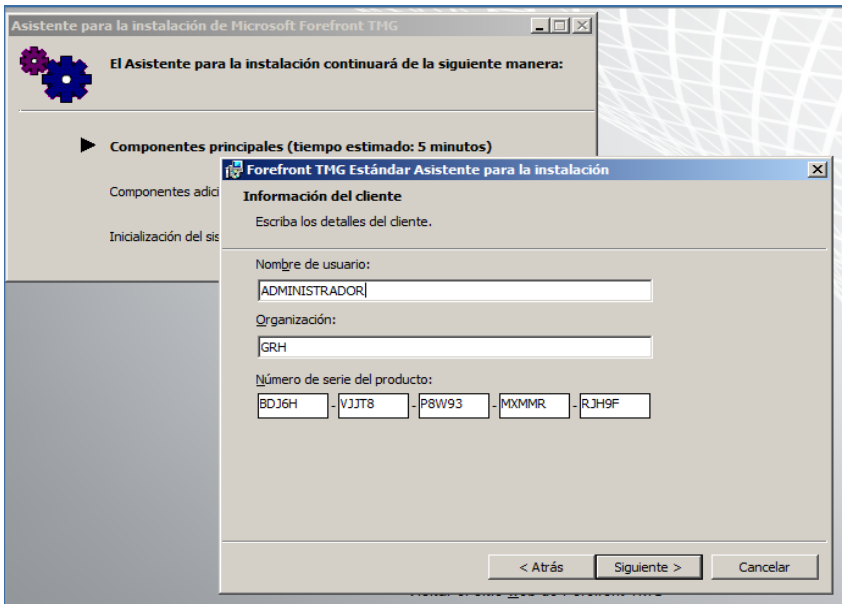


Grafico 28. Información del cliente.
Fuente: Propia

En el grafico 29 seleccionamos la red interna y elegimos siguiente.

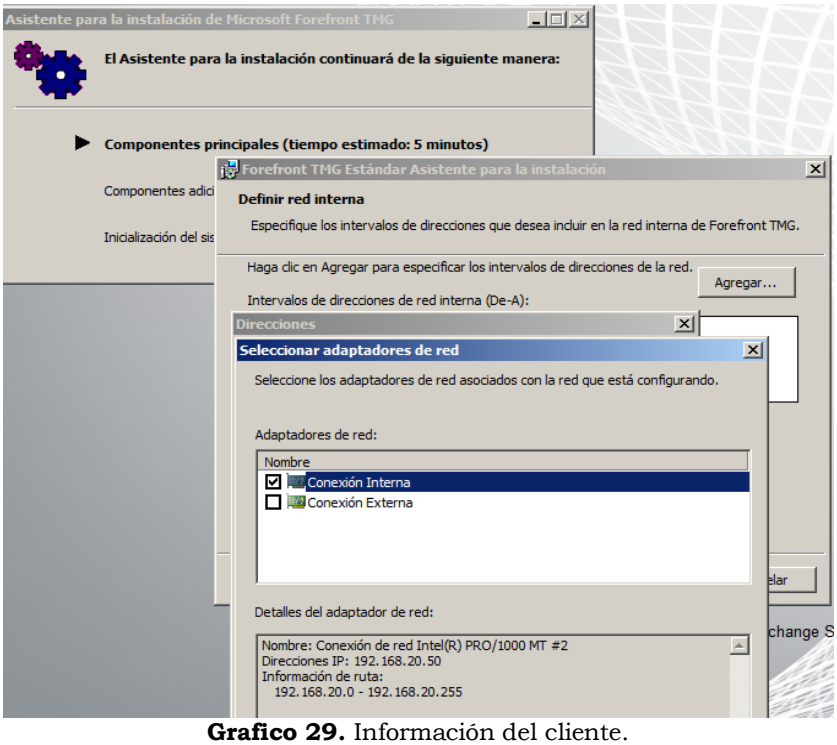


Grafico 29. Información del cliente.
Fuente: Propia

Aquí se puede apreciar los intervalos de direcciones para la red interna.

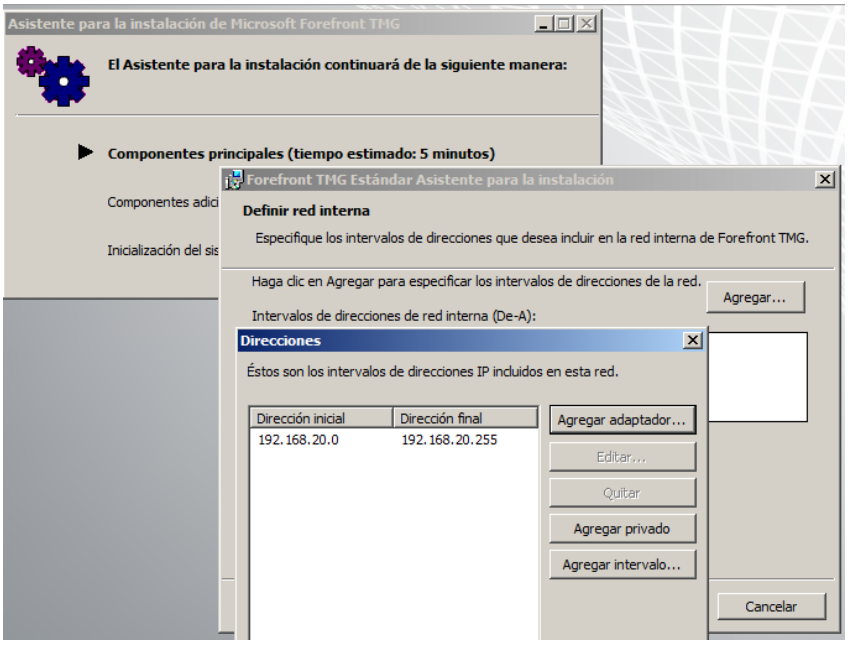


Grafico 30. Intervalo de direcciones de la red.
Fuente: Propia

En el grafico 31 se muestra el proceso de instalación del Forefront.

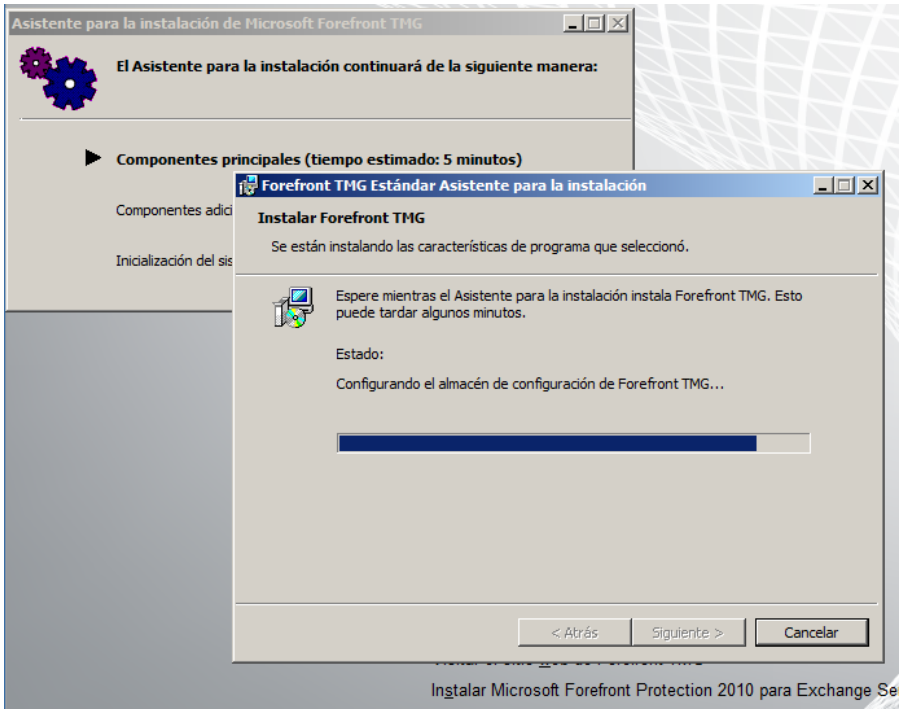


Grafico 31. Proceso de Instalación del TMG.
Fuente: Propia

En el grafico 32 se visualiza el término de la instalación del Forefront

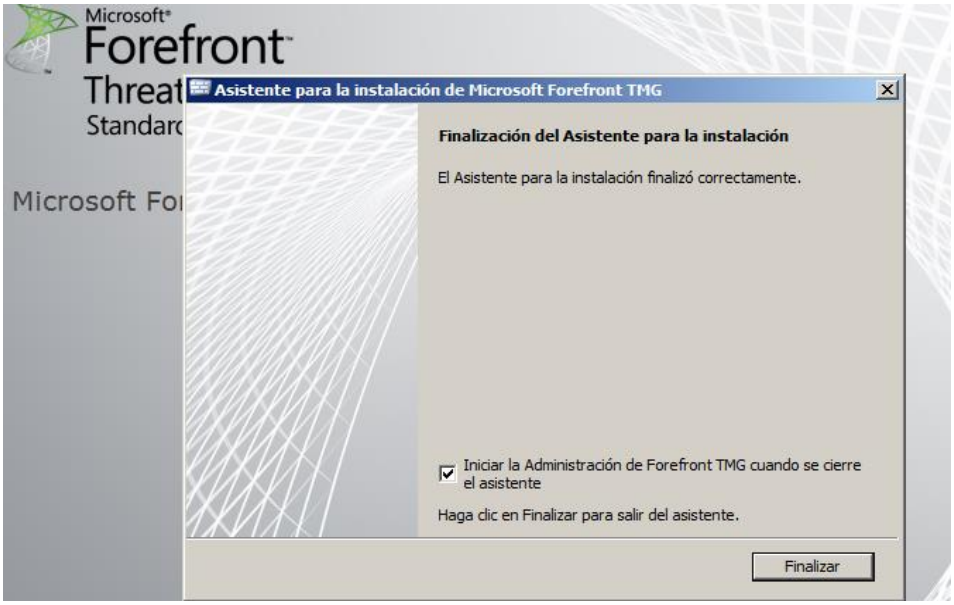


Grafico 32. Finalización del asistente de instalación.
Fuente: Propia

4.3.3 Configuración del Microsoft Forefront Threat Management Gateway (TMG):

Para la configuración del Forefront TMG tendremos que seguir tres pasos importantes los cuales son: Configurar opciones de red, configurar las opciones del sistema y definir las opciones de implementación, grafico 33.

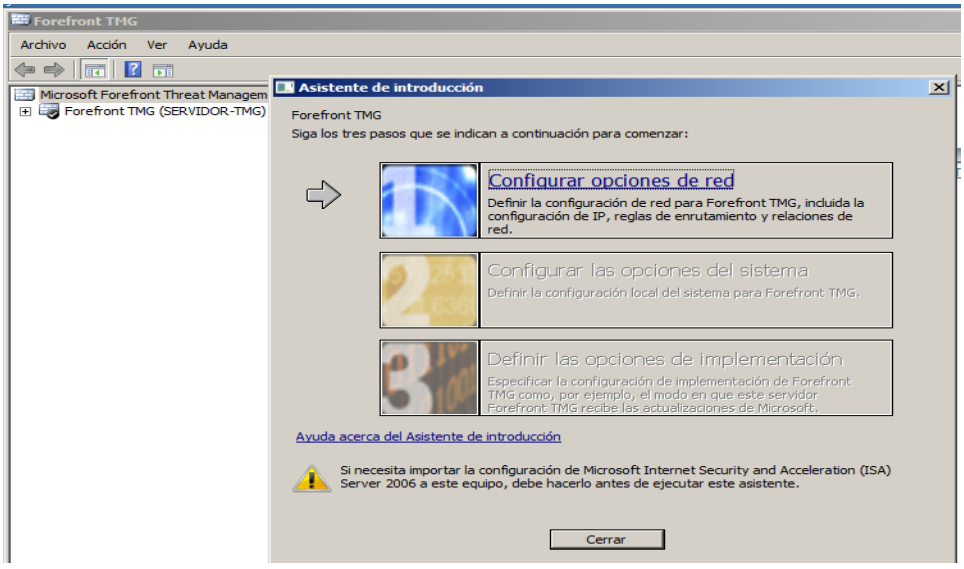


Grafico 33. Configuración opciones de red.
Fuente: Propia

En el grafico 34 se da inicio a la configuración de las opciones de red, debemos elegir siguiente.

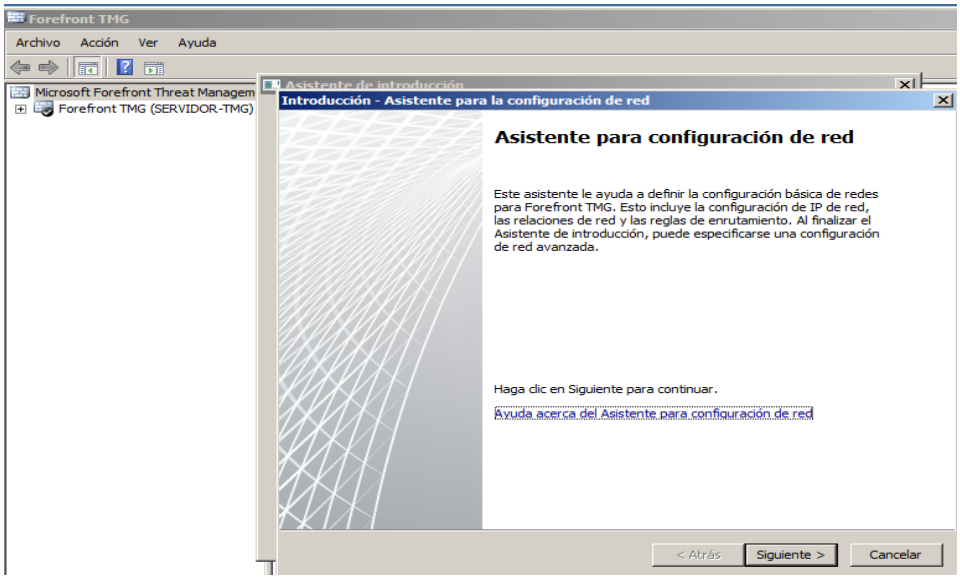


Grafico 34. Asistente para configuración de red.
Fuente: Propia

En el grafico 35 seleccionaremos la plantilla firewall perimetral topología que nos permite conectarnos a través de dos adaptadores de red interna y externa.

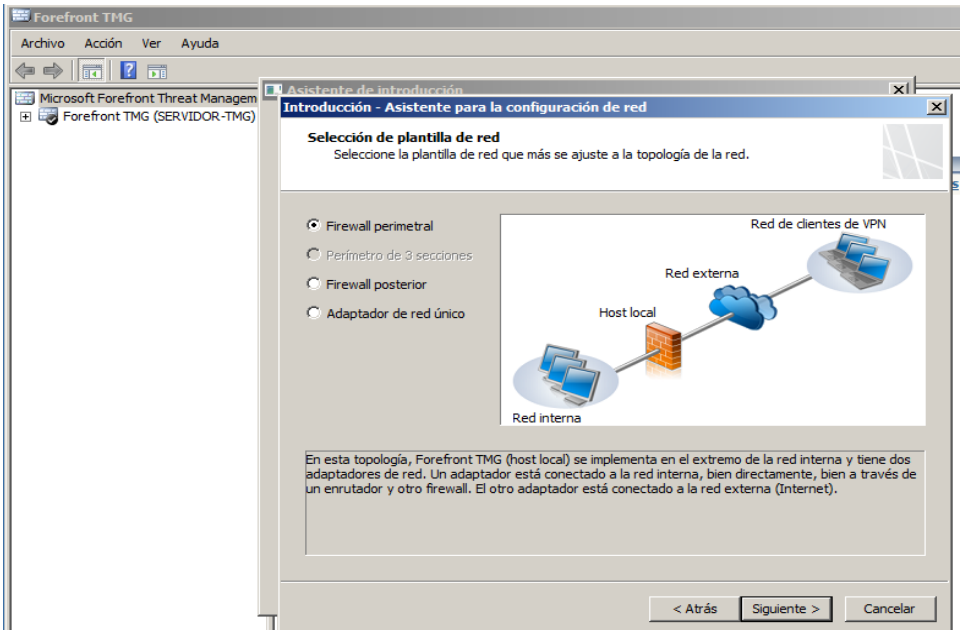


Grafico 35. Selección de plantilla de red.
Fuente: Propia

En el siguiente grafico vemos la configuración de la red externa, elegimos siguiente.

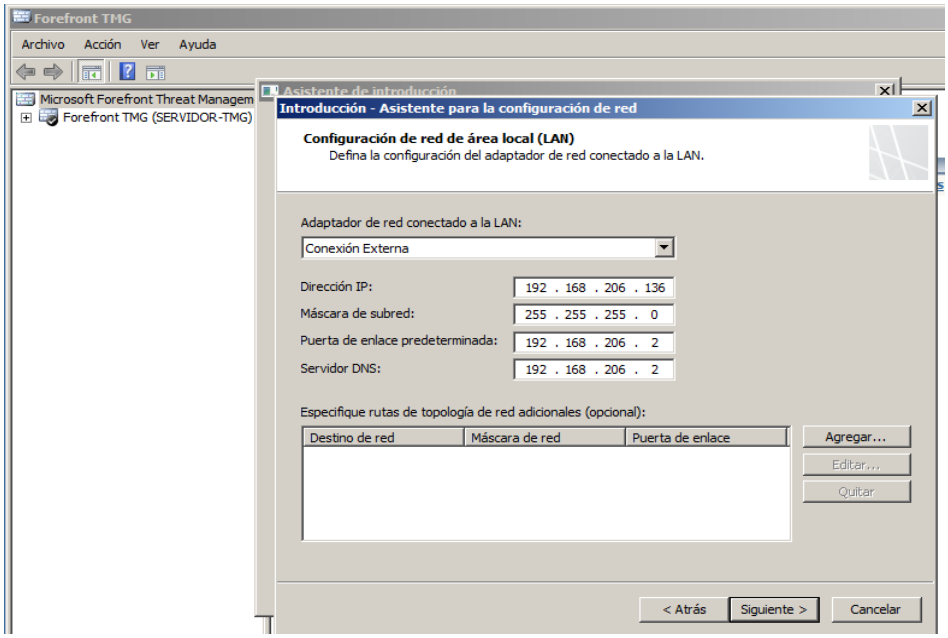


Grafico 36. Configuración de la conexión externa.
Fuente: Propia

En el siguiente grafico vemos la configuración de la red interna, elegimos siguiente.

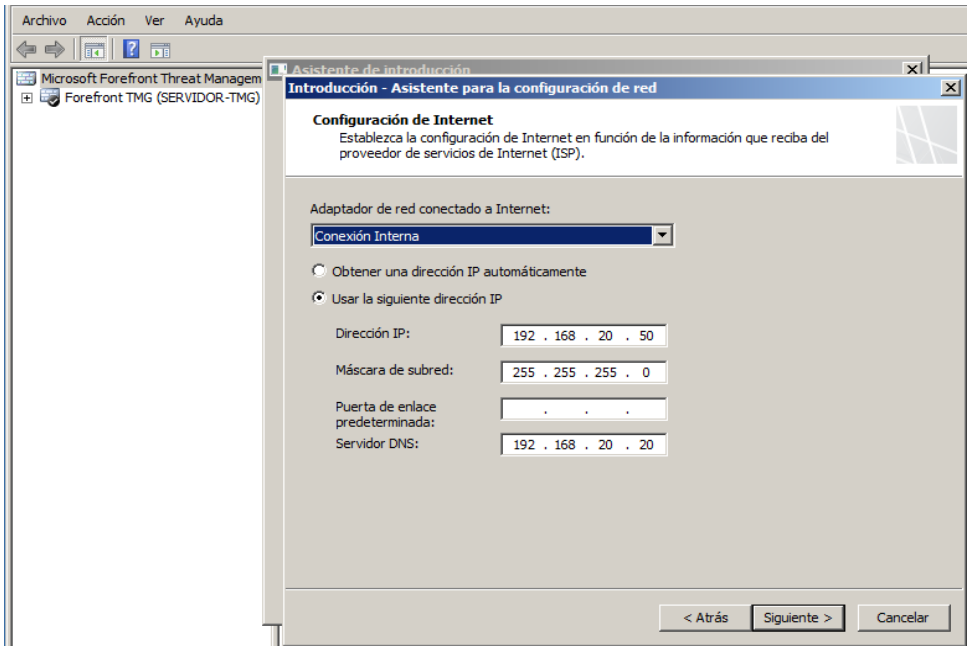


Grafico 37. Configuración de la conexión interna.
Fuente: Propia

En el grafico 38 vemos la finalización del asistente para la configuración de red.

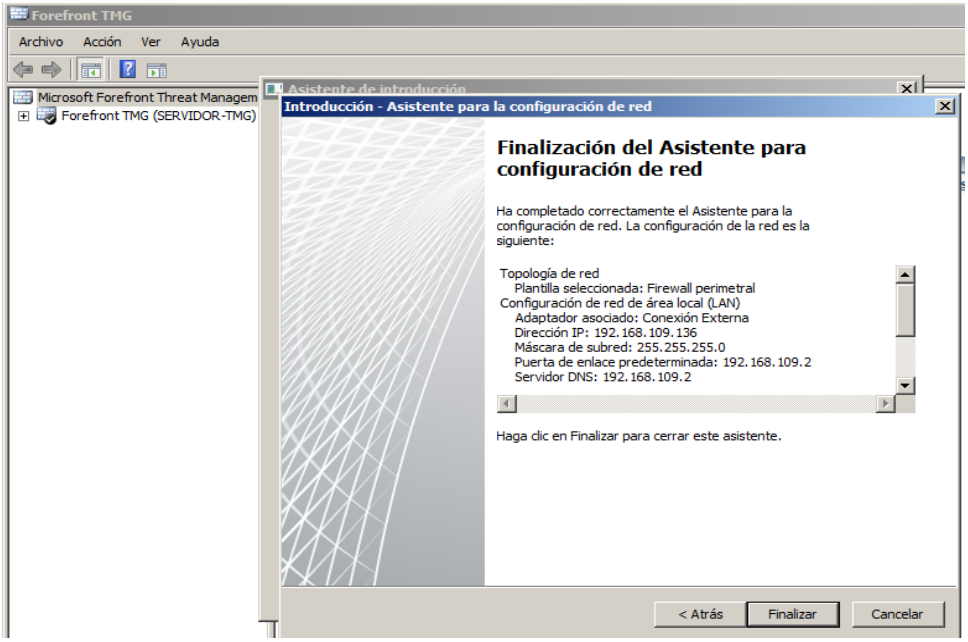


Grafico 38. Finalización del asistente de red.
Fuente: Propia

En este grafico elegiremos y daremos inicio a la configuración de opciones del sistema.

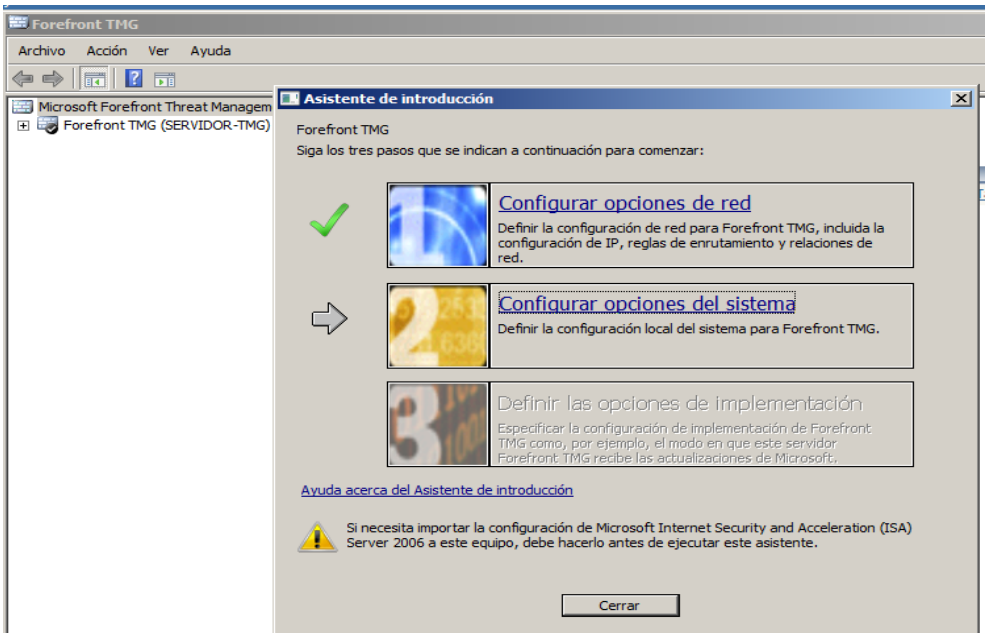


Grafico 39. Configurar opciones del sistema.
Fuente: Propia

Este asistente nos ayuda a definir la configuración del sistema local para el servidor de Forefront, grafico 40.

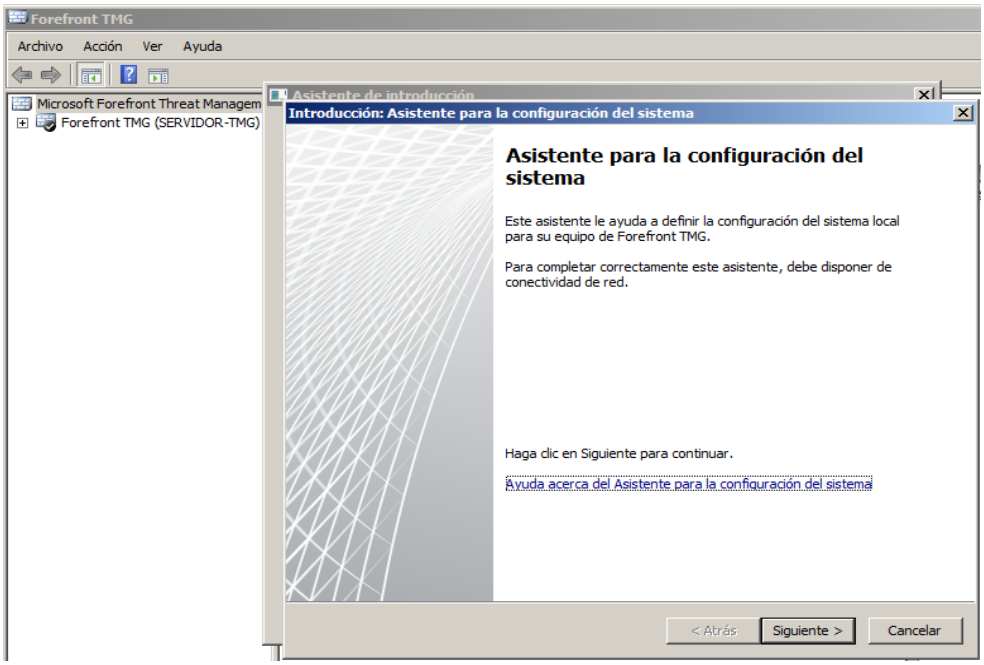


Grafico 40. Asistente para la configuración del sistema.
Fuente: Propia

Aquí vemos los datos de identificación del servidor, nombre de equipo SERVIDOR-TMG, Dominio de Windows GRHUANCAVELICA.GOB.PE

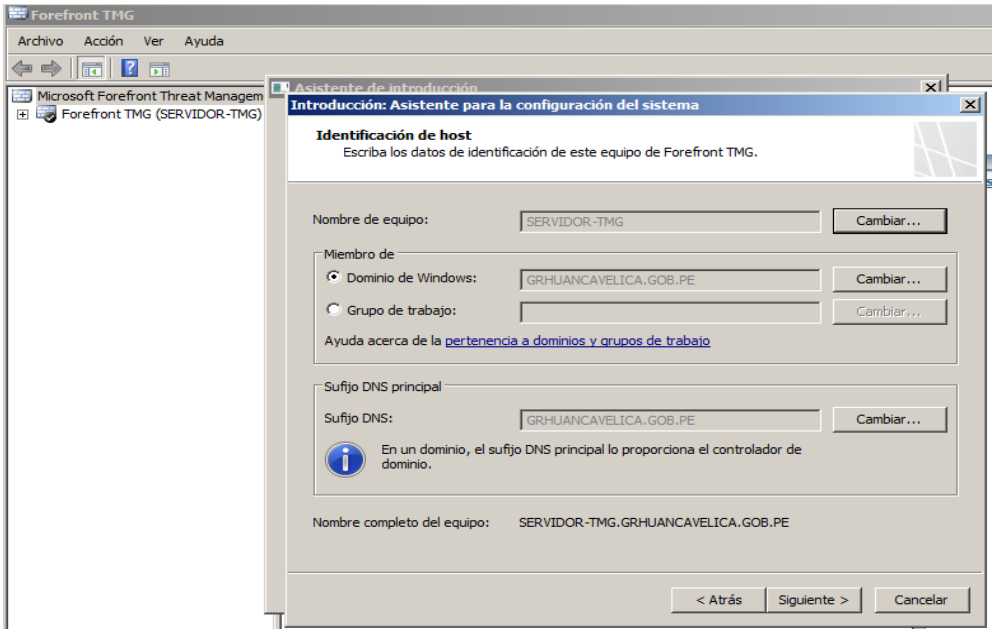


Grafico 41. Identificación de host.
Fuente: Propia

En el grafico 42 vemos la finalización del asistente para la configuración del sistema.

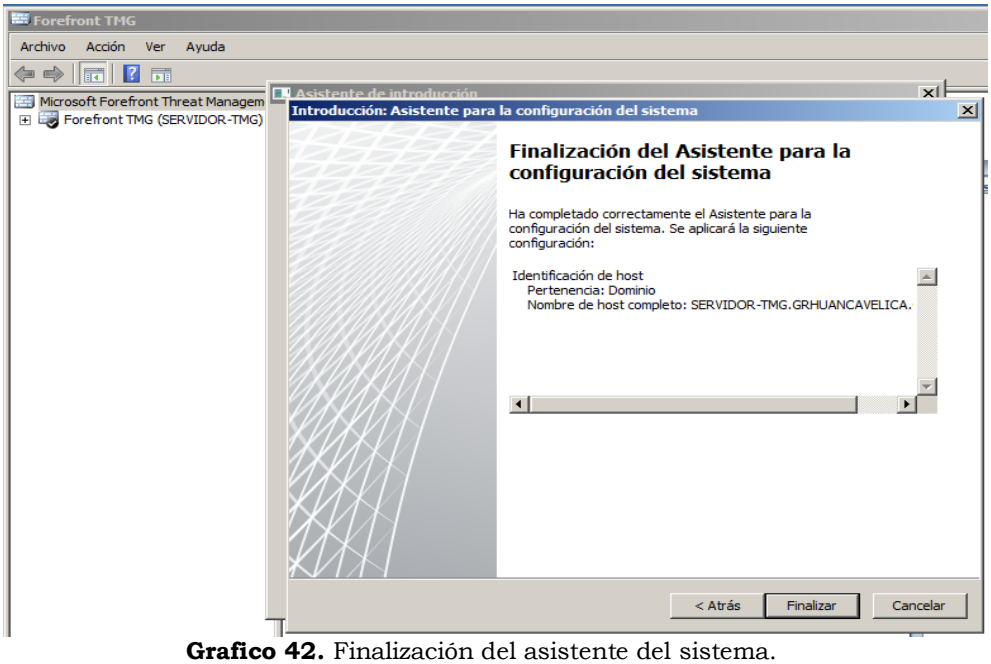


Grafico 42. Finalización del asistente del sistema.
Fuente: Propia

En este grafico elegiremos y daremos inicio a definir opciones de implementación, grafico 43.

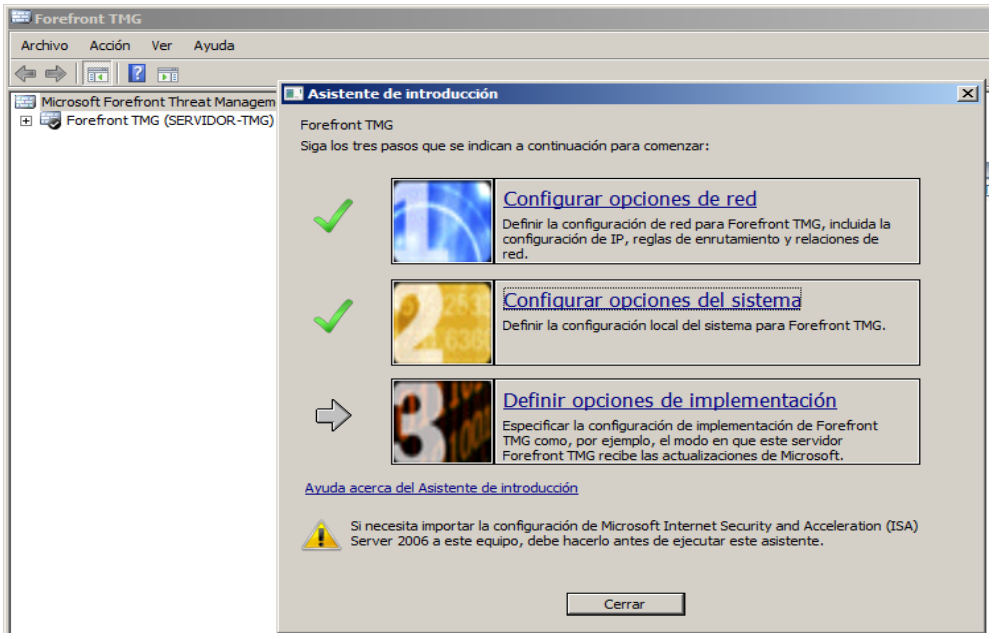


Grafico 43. Definir opciones de implementación.
Fuente: Propia

En este asistente configuraremos las actualizaciones del Forefront TMG.

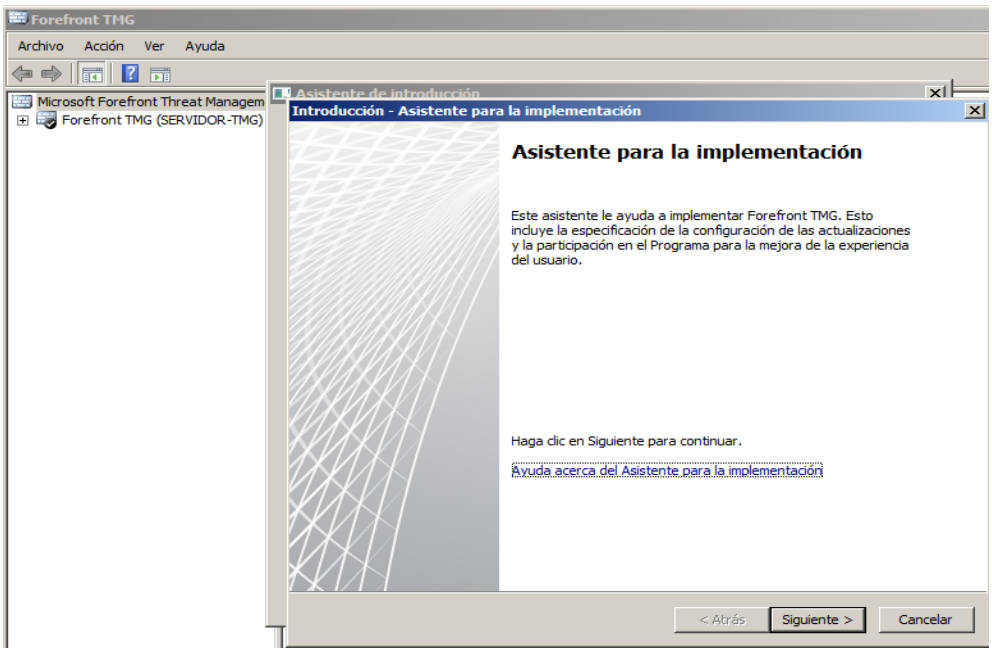


Grafico 44. Asistente para la implementación.
Fuente: Propia

En este grafico debemos seleccionar la opción: usar el servicio Microsoft Update para buscar actualizaciones.

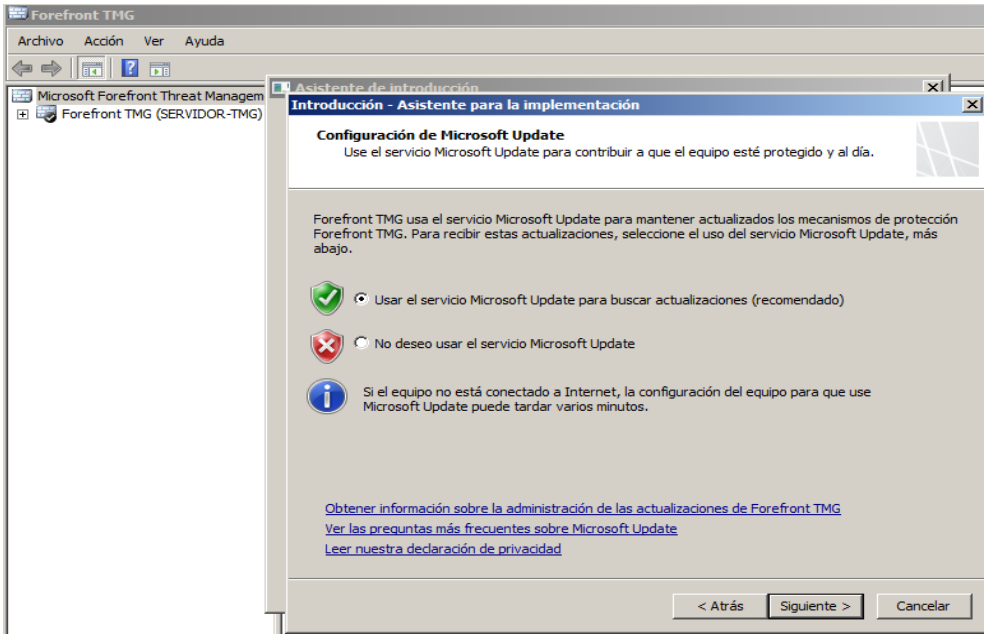


Grafico 45. Configuración de Microsoft Update.
Fuente: Propia

Seleccionar la opción: habilitar inspección de malware y poner siguiente.

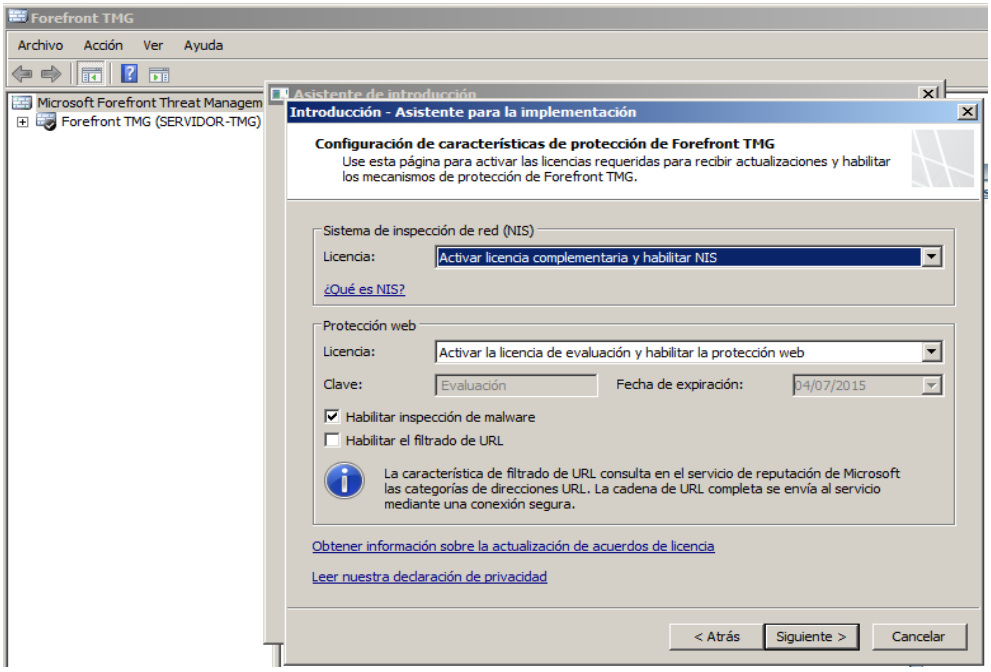


Grafico 46. Configuración de características de protección.
Fuente: Propia

En el grafico 47 vemos la finalización del asistente para la implementación.

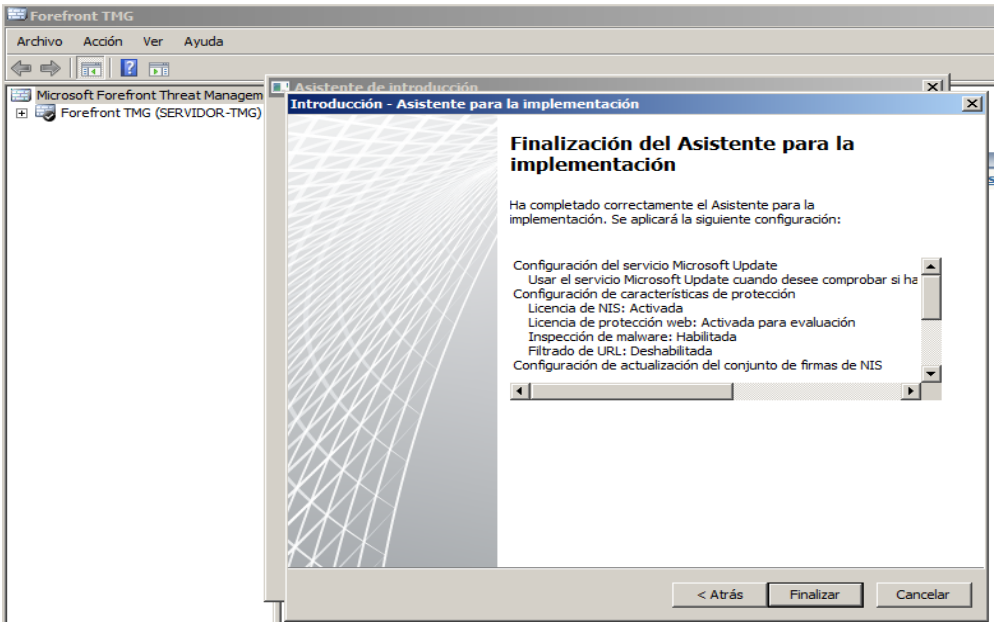


Grafico 47. Finalización del asistente para la implementación.
Fuente: Propia

En la siguiente figura se ve todos los pasos del asistente de introducción finalizaron correctamente.

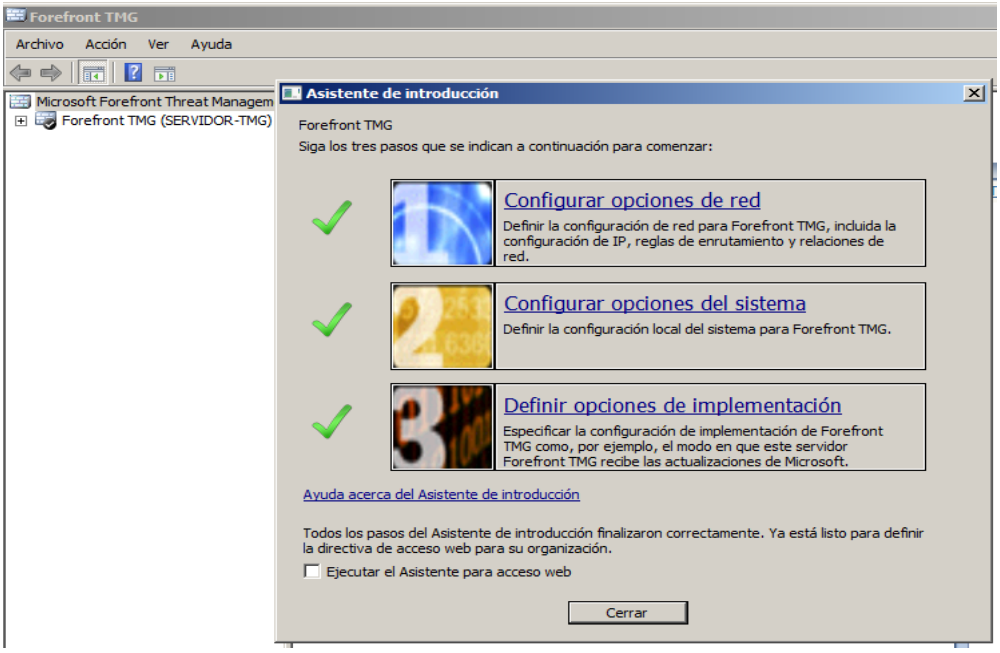


Grafico 48. Asistente de introducción finalizada.
Fuente: Propia

En el siguiente grafico podemos observar el interface del Microsoft Forefront TMG 2010.

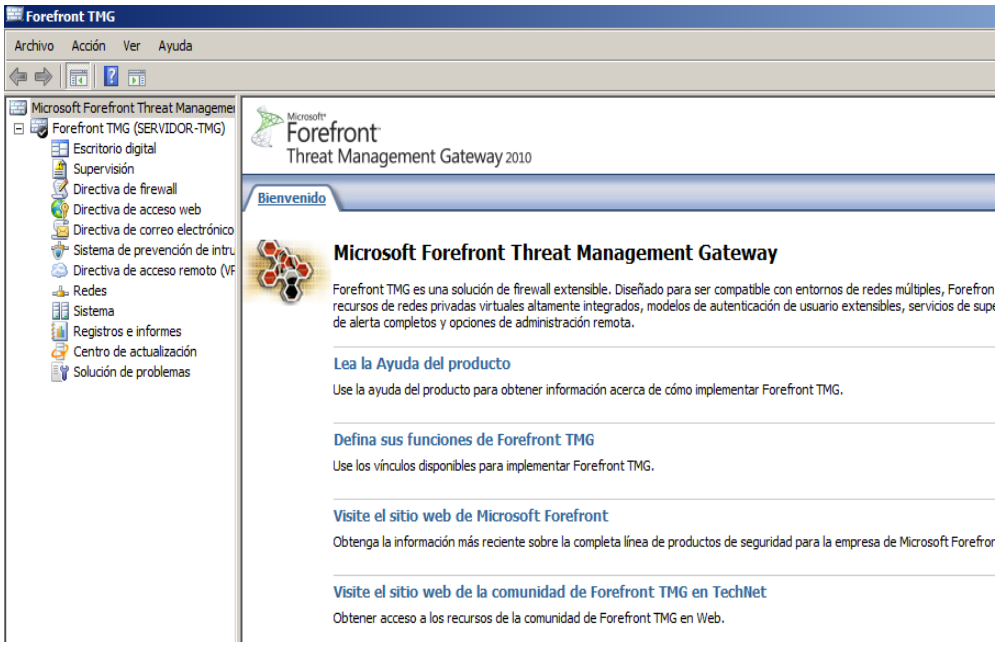


Grafico 49. Configuración de características de protección
Fuente: Propia

En el grafico 50 observamos una directiva de firewall donde restringe y cierra todos los puertos y servicios del servidor VPN.

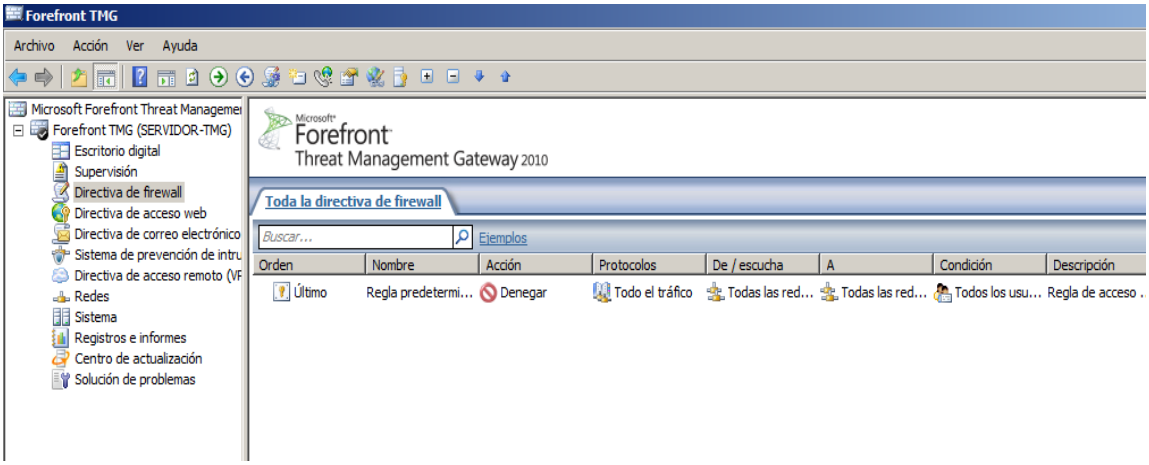


Grafico 50. Directiva que bloquea todos los puertos.
Fuente: Propia

4.3.4 Creación de Regla en el Microsoft Forefront Threat Management Gateway (TMG):

Crearemos una regla de acceso para poder permitir los protocolos http y https y poder tener el servicio de internet en el servidor de VPN, seleccionamos la opción permitir y siguiente.

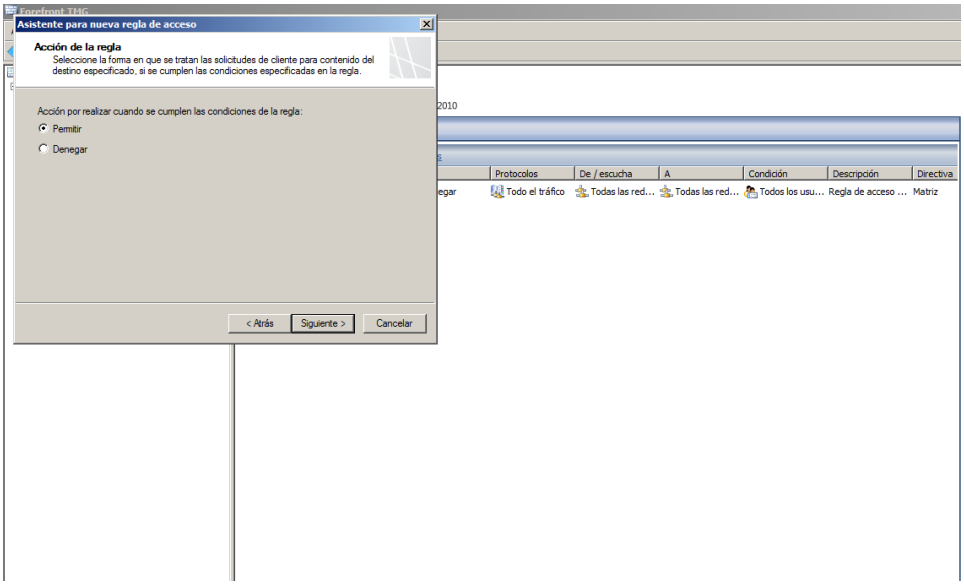


Grafico 51. Creando regla de acceso para permitir protocolos.
Fuente: Propia

En esta ventana agregamos los protocolos http, https, aceptamos y le damos siguiente

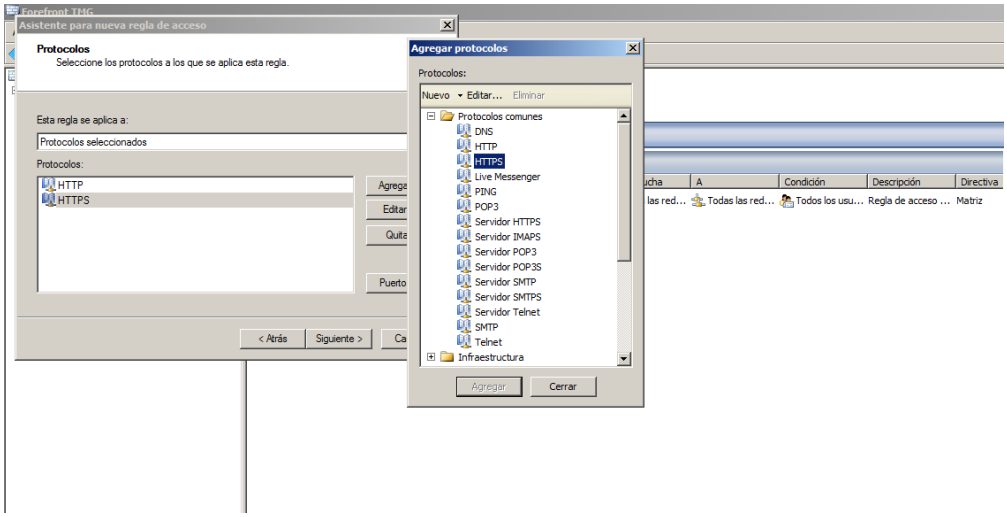


Grafico 52. Seleccionamos los protocolos.
Fuente: Propia

En esta venta seleccionaremos el local host que viene hacer el servidor VPN aceptamos y le damos siguiente.

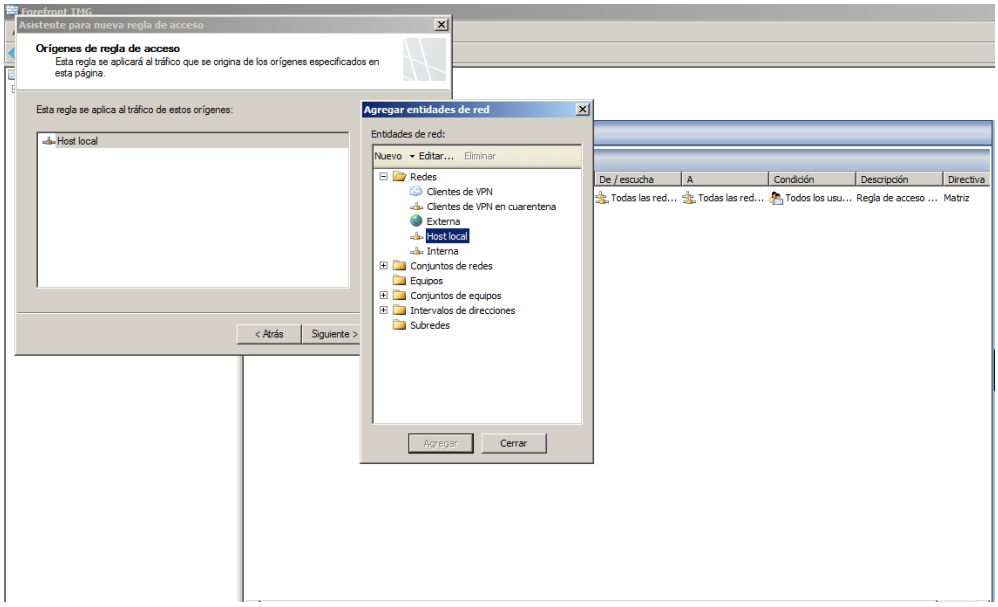


Grafico 53. Selección de del local host.
Fuente: Propia

Seguidamente seleccionamos la red externa, de donde nos conectaremos al internet aceptamos y le damos siguiente.

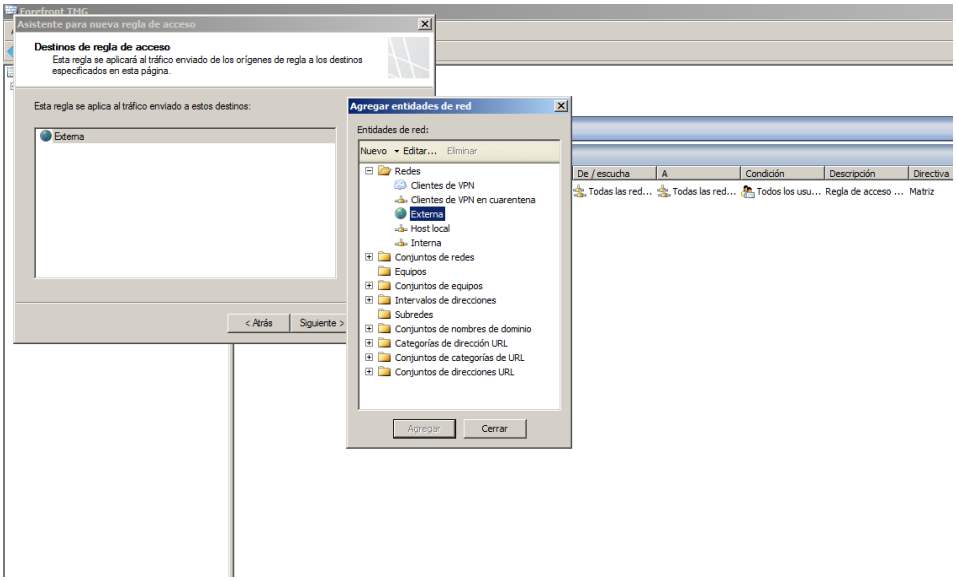


Grafico 54. Seleccionamos la red externa.
Fuente: Propia

Aquí finalizamos la regla de acceso para poder tener internet en el servidor VPN.

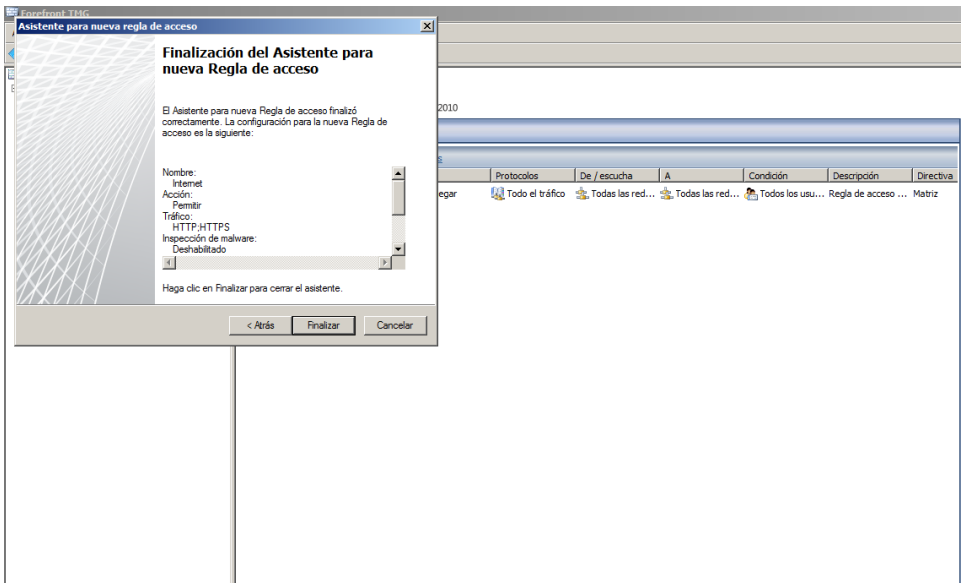


Grafico 55. Finalización de la regla creada
Fuente: Propia

Aquí apreciamos la primera regla creada y aplicada para poder acceder al internet en el servidor.

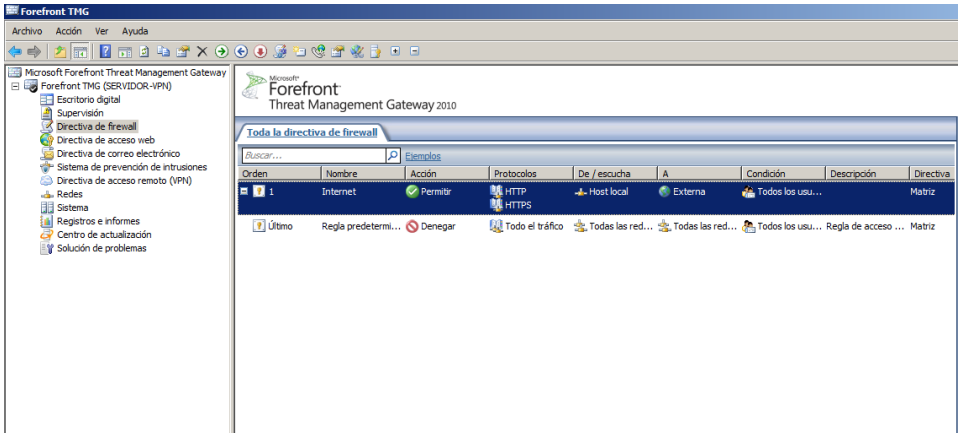


Grafico 56. Regla de internet creada.
Fuente: Propia

Comprobando el acceso a internet en el servidor VPN

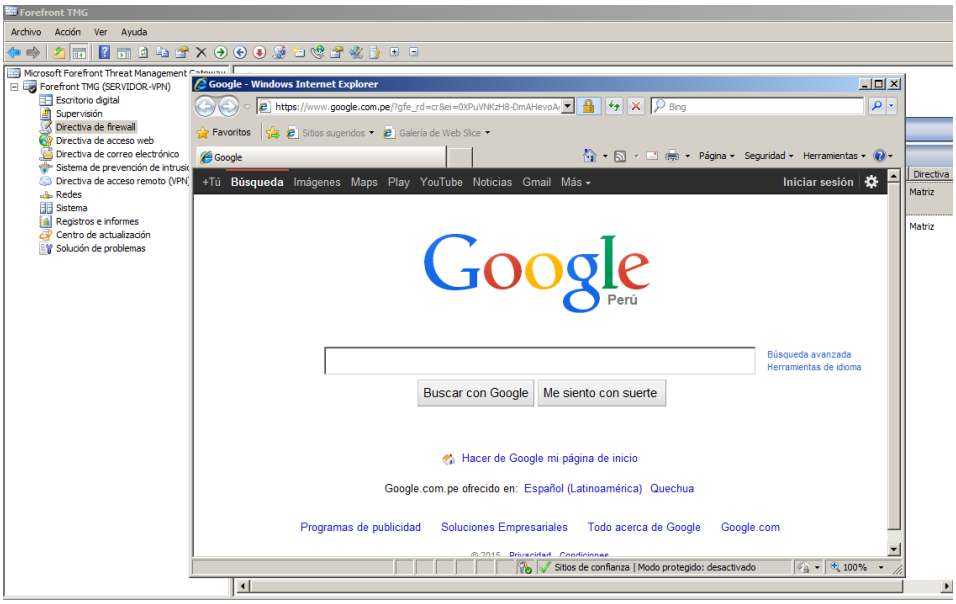


Grafico 57. Accesando al internet en el servidor.
Fuente: Propia

En este grafico empezaremos con la creación de la regla para dar acceso al DNS de nuestro servidor de dominio.

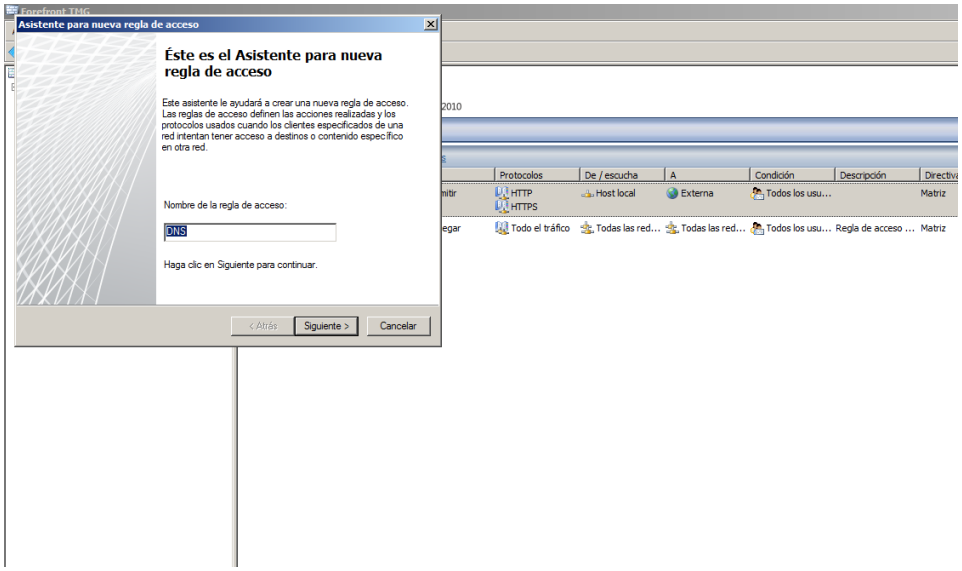


Grafico 58. Creando regla para el DNS.
Fuente: Propia

En esta imagen seleccionamos el protocolo de DNS y le damos siguiente.

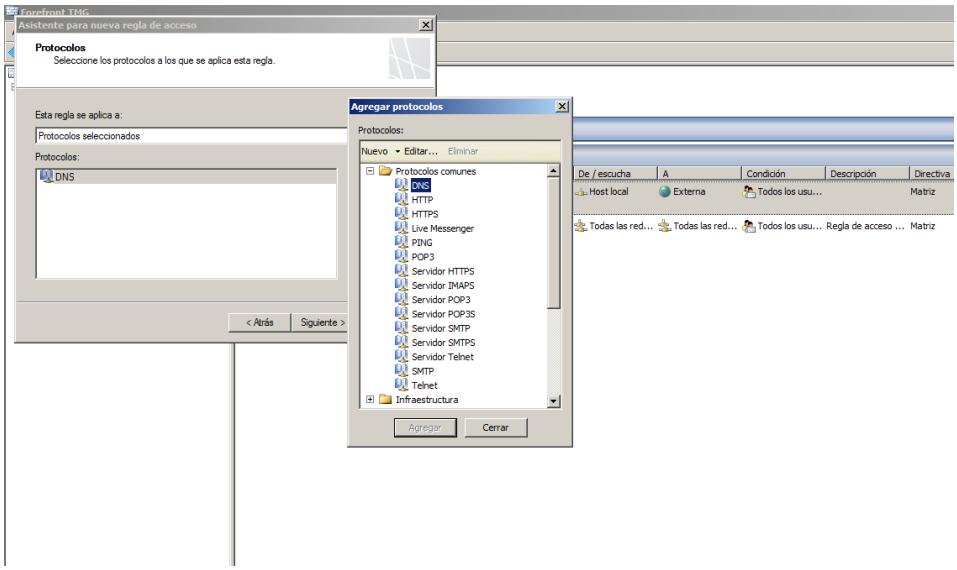


Grafico 59. Selección del protocolo DNS.
Fuente: Propia

Los orígenes de la regla de acceso serán a la red interna y la red externa, siguiente.

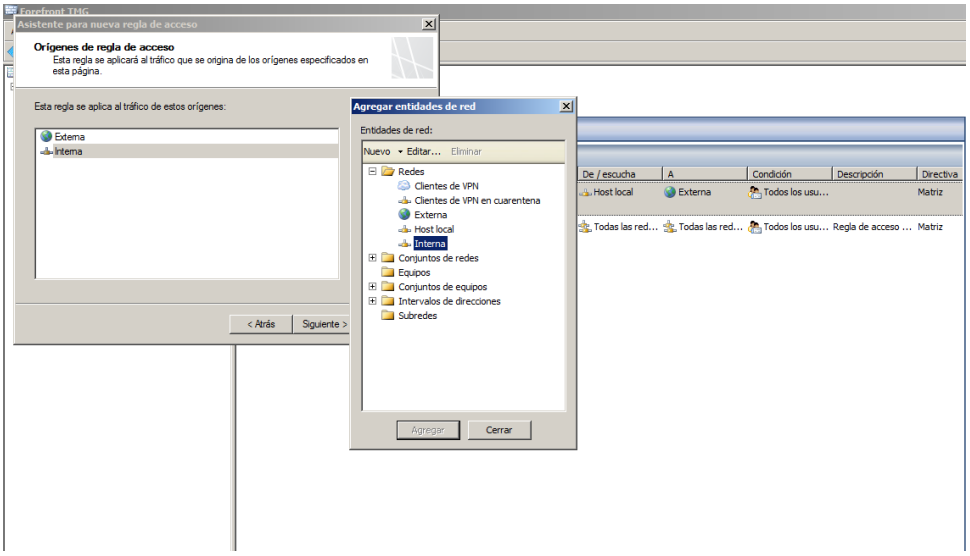


Grafico 60. Selección de la red interna.
Fuente: Propia

Para el destino de la regla agregamos un nuevo elemento de regla de equipo, el cual será el servidor de dominio para ello seleccionaremos el IP del servidor.

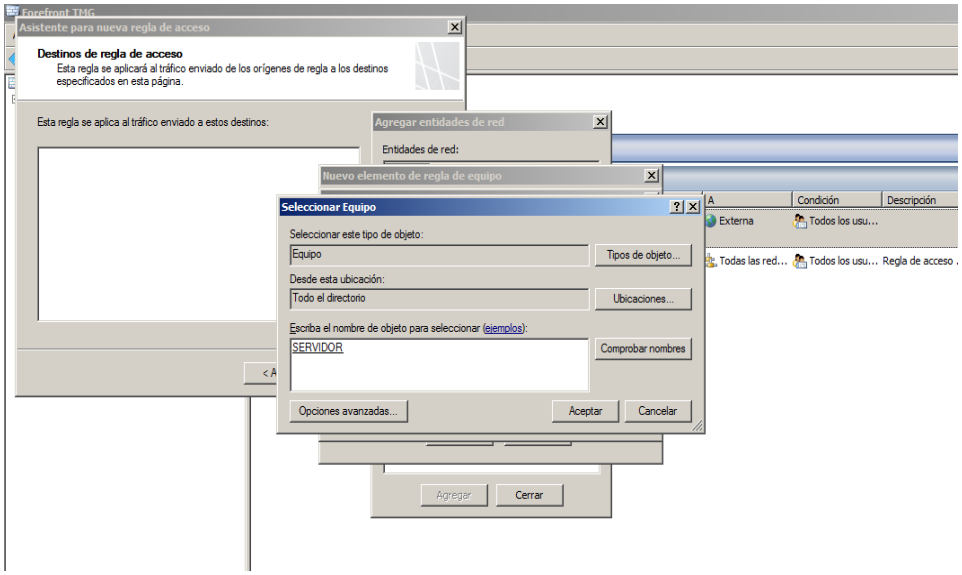


Grafico 61. Seleccionamos el servidor de dominio.
Fuente: Propia

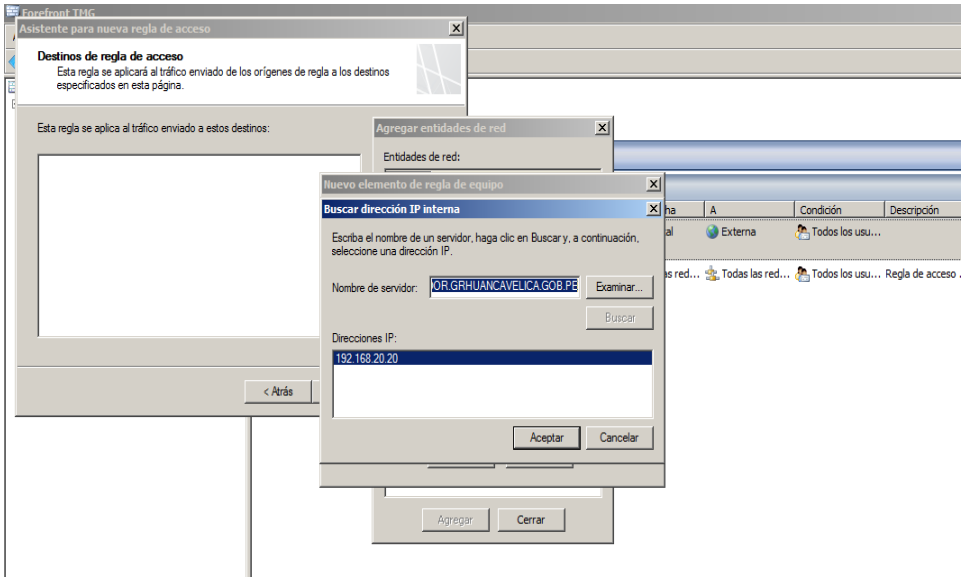


Grafico 62. Seleccionamos el IP del servidor de dominio.
Fuente: Propia

En el siguiente grafico se muestra el destino de la regla de acceso: SERVIDOR.GRHUANCAVELICA.GOB.PE y le damos siguiente.

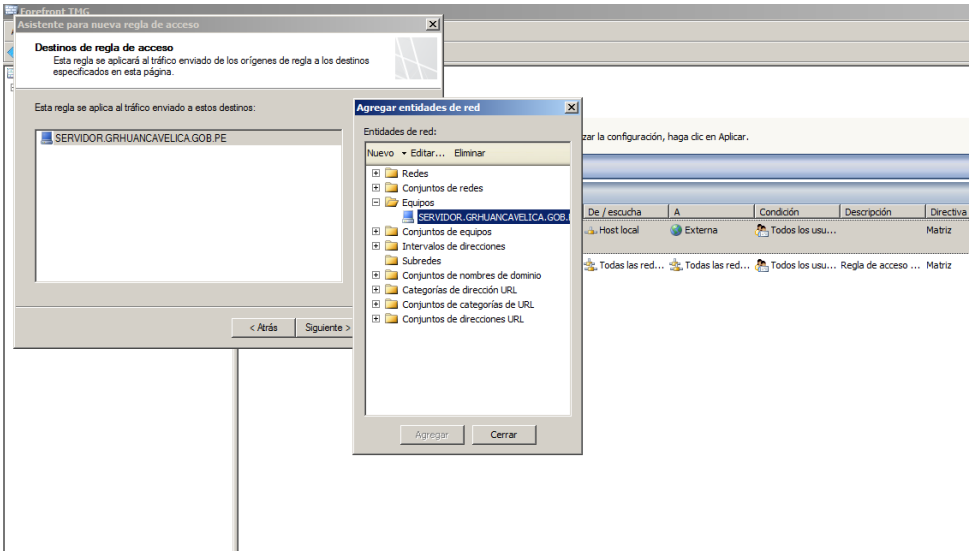


Grafico 63. Selección del servidor del dominio.
Fuente: Propia

En la siguiente imagen se aplicara la regla a todos los usuarios.

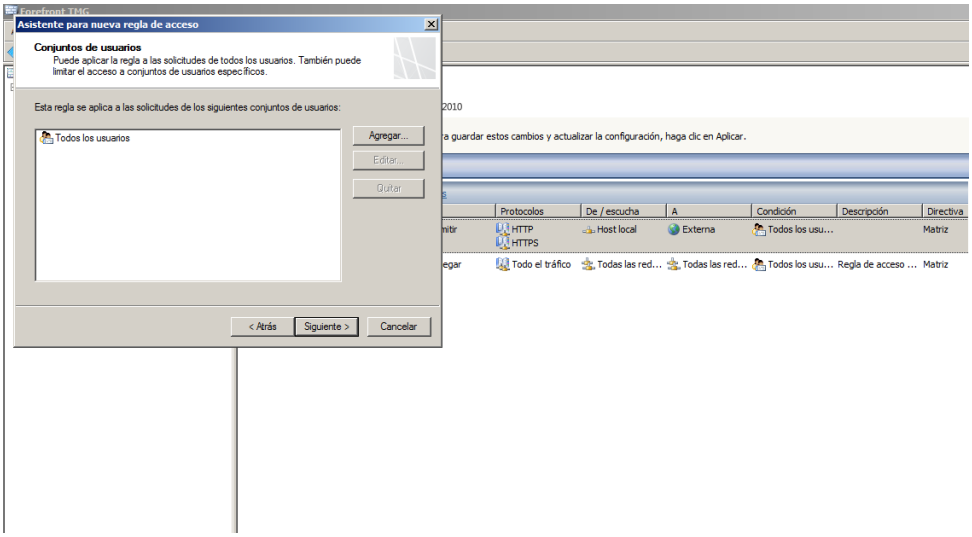


Grafico 64. Seleccionamos a todos los usuarios para la regla.
Fuente: Propia

En el siguiente grafico estaremos listos para configurar el acceso de clientes de VPN.

Grafico 65. Configuración al acceso de clientes de VPN.
Fuente: Propia

Aquí configuramos el método de asignación de direcciones, además seleccionamos la red interna para obtener el servicio de DHCP, DNS.

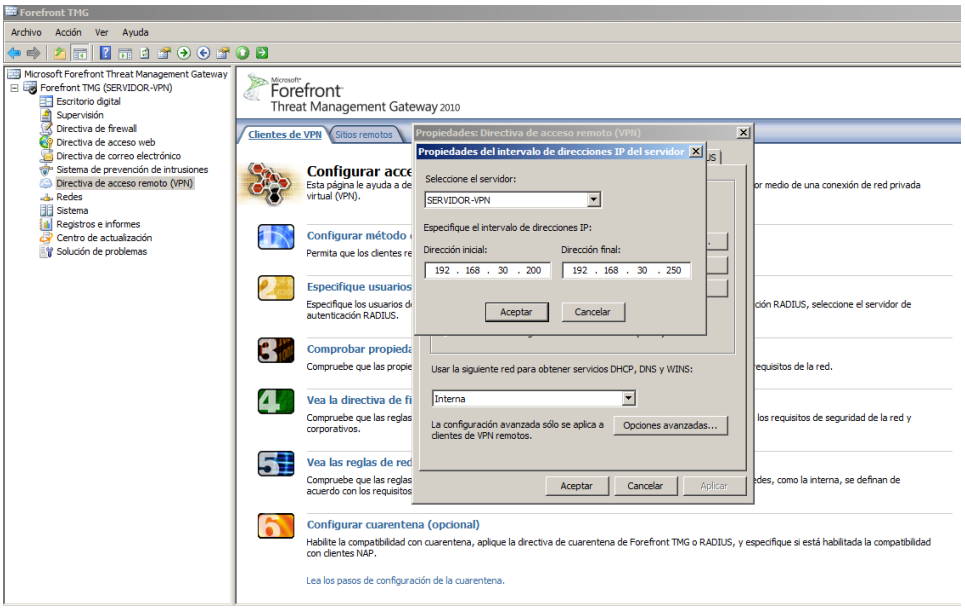


Grafico 66. Asignación de direcciones.
Fuente: Propia

En el siguiente grafico asignamos el número máximo de clientes de VPN permitidos.

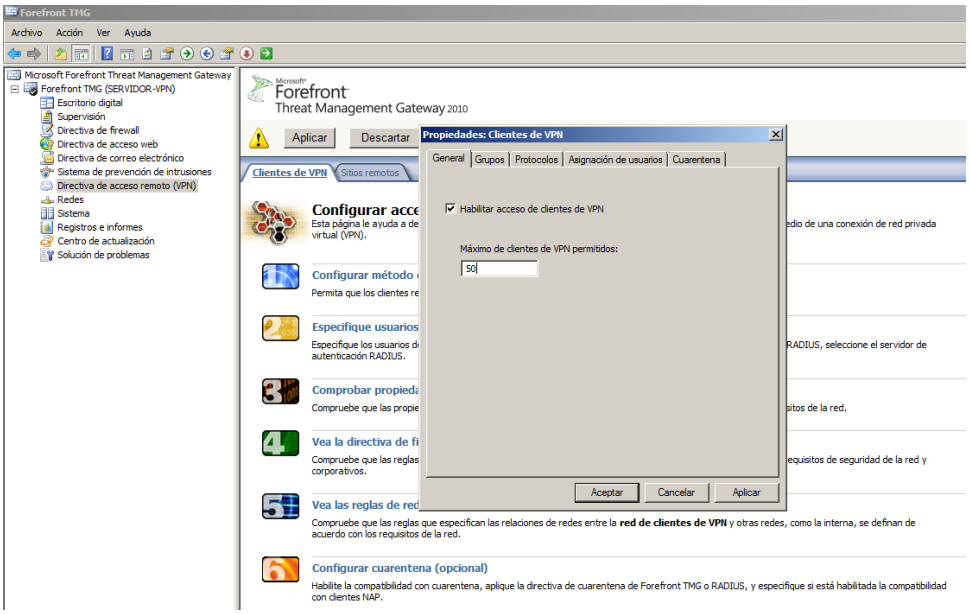


Grafico 67. Número máximo de usuarios a la VPN
Fuente: Propia

En este grafico especificamos los usuarios de Windows, seleccionamos el grupo creado en el dominio de nombre ACCESO VPN y le damos aceptar.

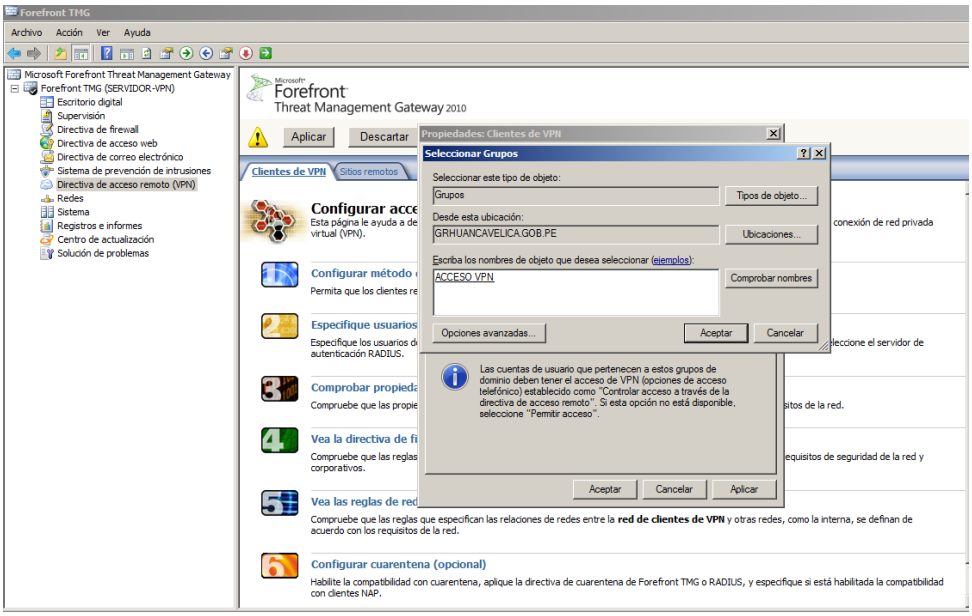


Grafico 68. Selección de grupo de usuarios a la VPN.
Fuente: Propia

En este grafico podemos observar que se seleccionó al grupo ACCESO VPN del dominio GRHUANCAVELICA.

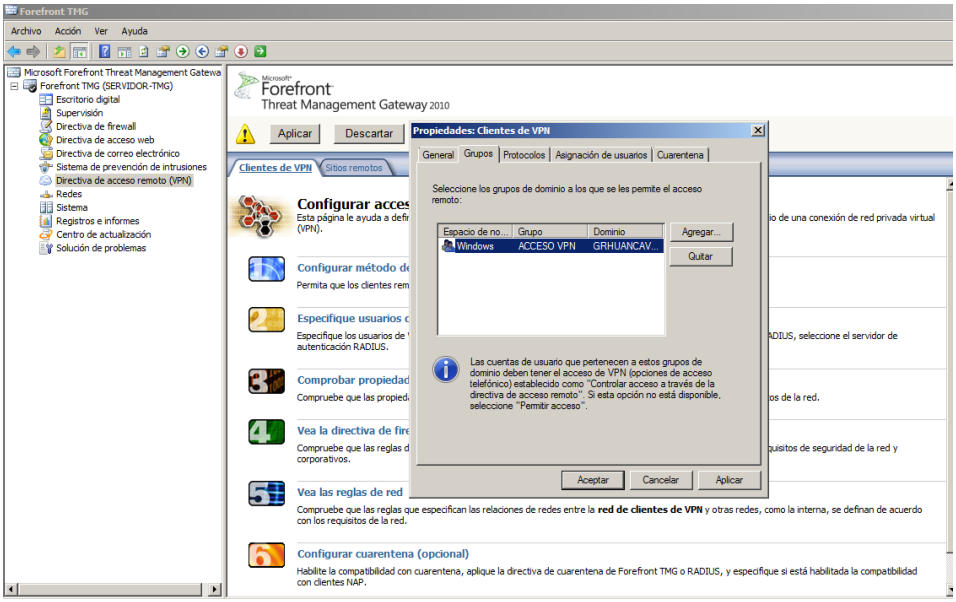


Grafico 69. Selección del grupo de VPN.
Fuente: Propia

Aquí seleccionamos el protocolo de túnel PPTP para la conexión de acceso remoto.

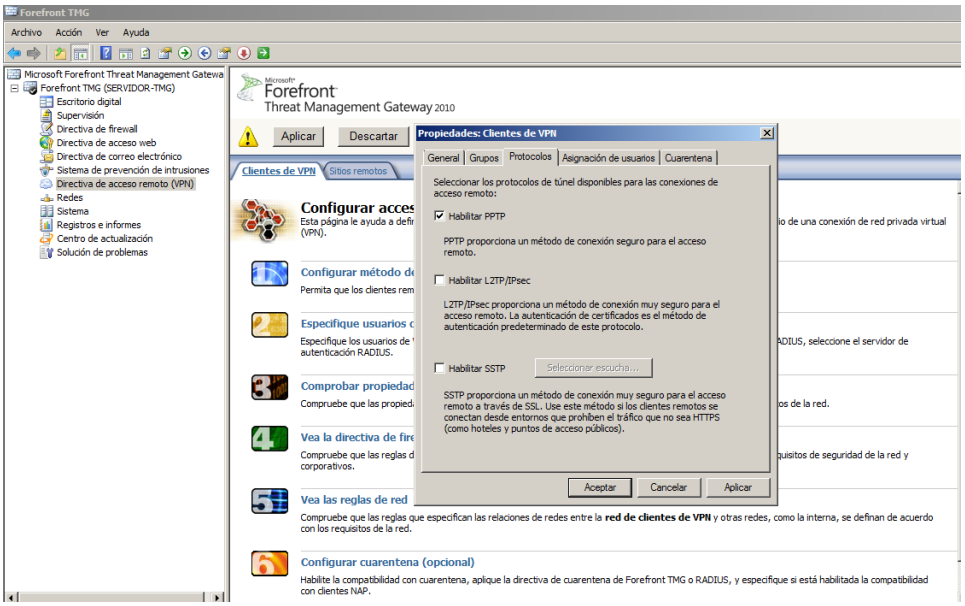


Grafico 70. Selección del protocolo PPTP.
Fuente: Propia

En este grafico habilitaremos la asignación de usuarios, para ellos usaremos el dominio GRHUANCAVELICA y aceptamos.

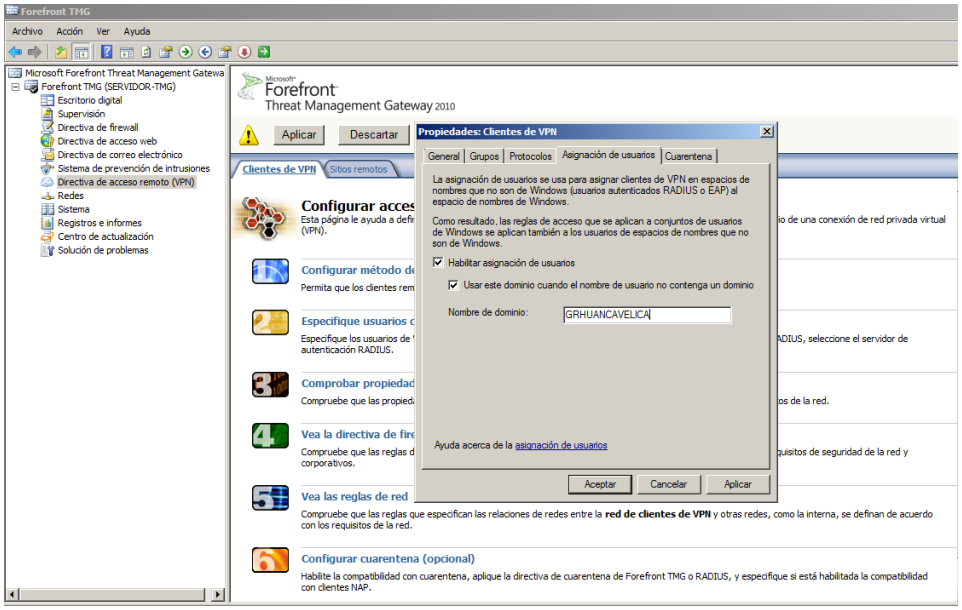


Grafico 71. Ingresamos el nombre del dominio.
Fuente: Propia

Seguidamente aplicamos y guardamos toda la configuración del cliente de VPN.

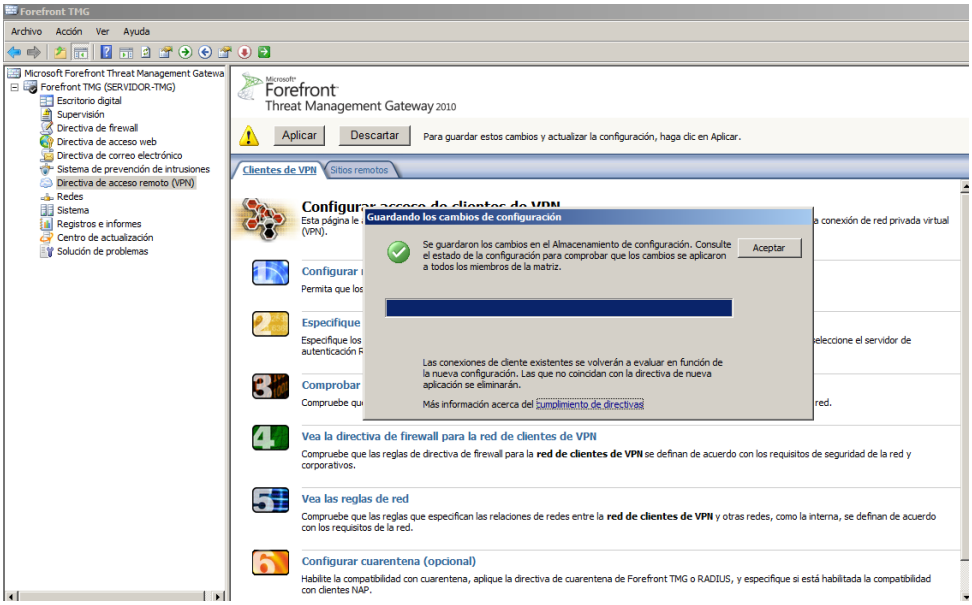


Grafico 72. Guardando cambios de configuración.
Fuente: Propia

Seguidamente crearemos las directivas de firewall, empezaremos creando la regla de acceso a la VPN.

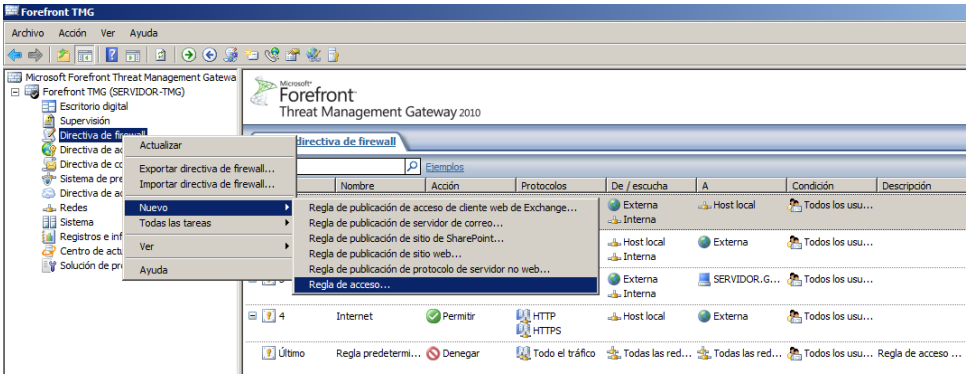


Grafico 73. Creación de regla de acceso a la VPN.
Fuente: Propia

Crearemos la nueva regla de Salida VPN, le damos permitir y siguiente.

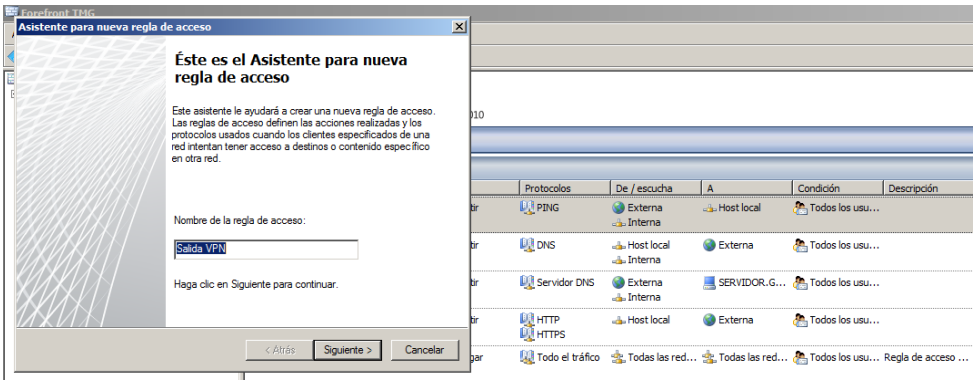


Grafico 74. Ponemos el nombre salida VPN.
Fuente: Propia

En este grafico agregaremos a la red interna y al host local como origen de la regla de acceso a la VPN.

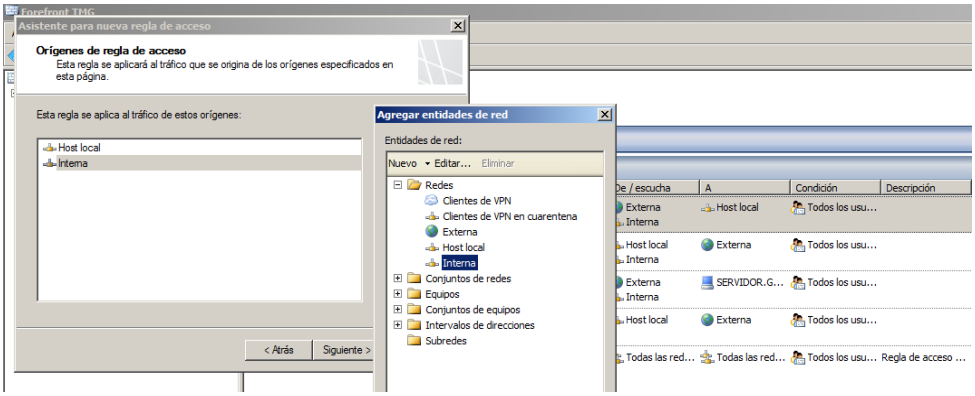


Grafico 75. Selección del host local y la red interna.
Fuente: Propia

En la regla de acceso, agregaremos a los clientes de VPN

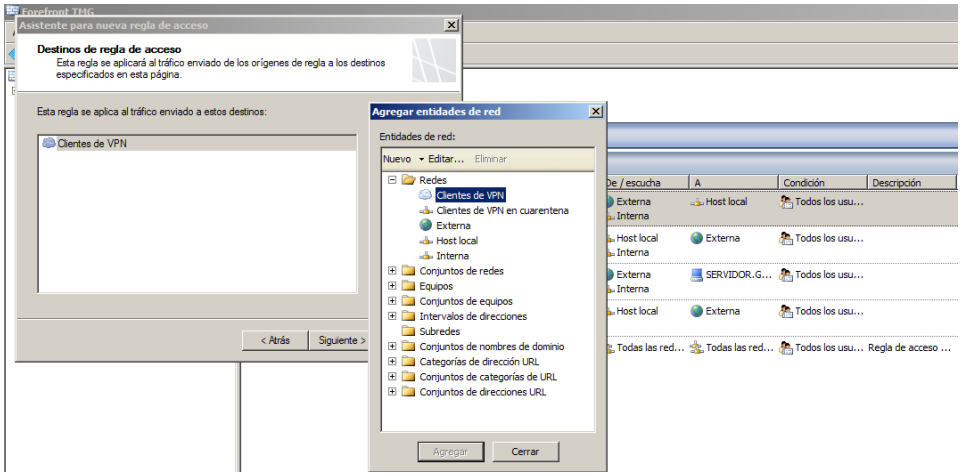


Grafico 76. Selección de clientes de VPN como destino.
Fuente: Propia

En esta imagen agregamos a todos los usuarios para la aplicación de esta regla.

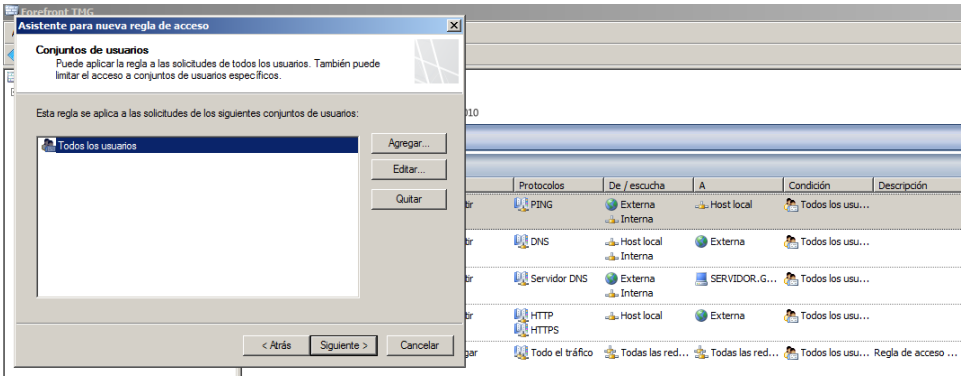


Grafico 77. Agregamos a todos los usuarios de la VPN
Fuente: Propia

En este grafico se visualiza la finalización del asistente para la aplicación de la regla Salida VPN.

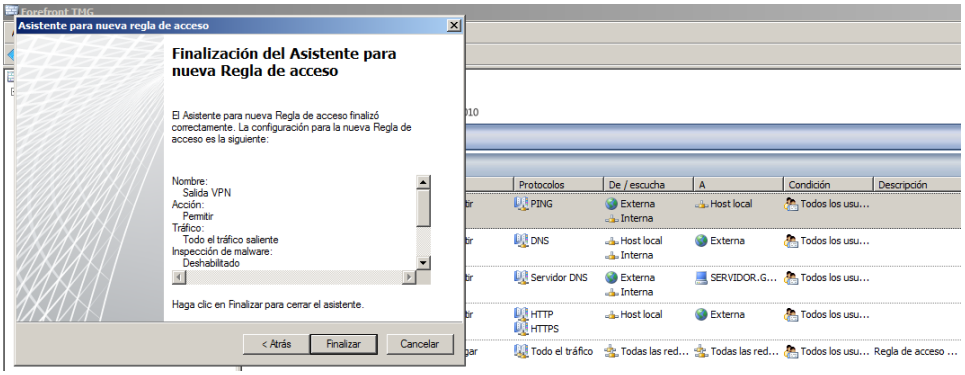


Grafico 78. Finalizando la creación de la regla de Salida VPN.
Fuente: Propia

Aquí crearemos la nueva regla de Entrada VPN, le damos permitir y siguiente.

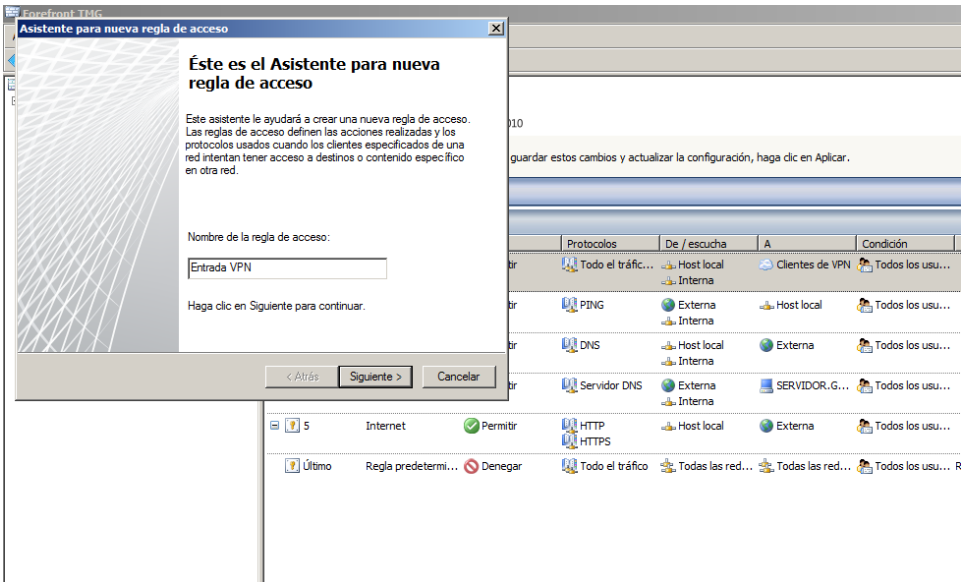


Grafico 79. Ponemos el nombre entrada VPN.
Fuente: Propia

En este grafico seleccionaremos todo el tráfico saliente y siguiente.

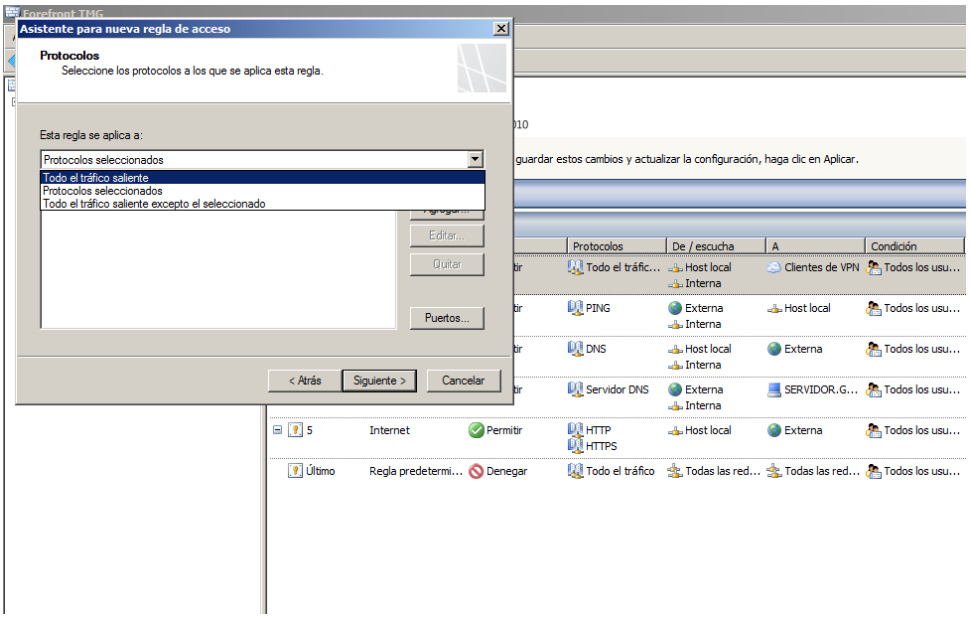


Grafico 80. Selección del tráfico saliente.
Fuente: Propia

En este grafico agregaremos a los Clientes de VPN como orígenes de la regla de acceso a la VPN.

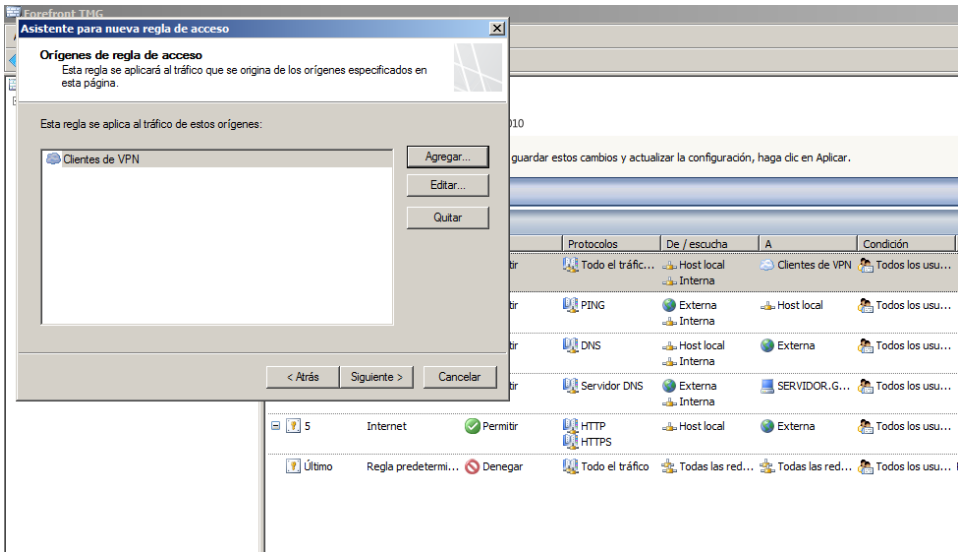


Grafico 81. Agregamos a los clientes de la VPN.
Fuente: Propia

Como destino de la regla de acceso, agregaremos a la red interna.

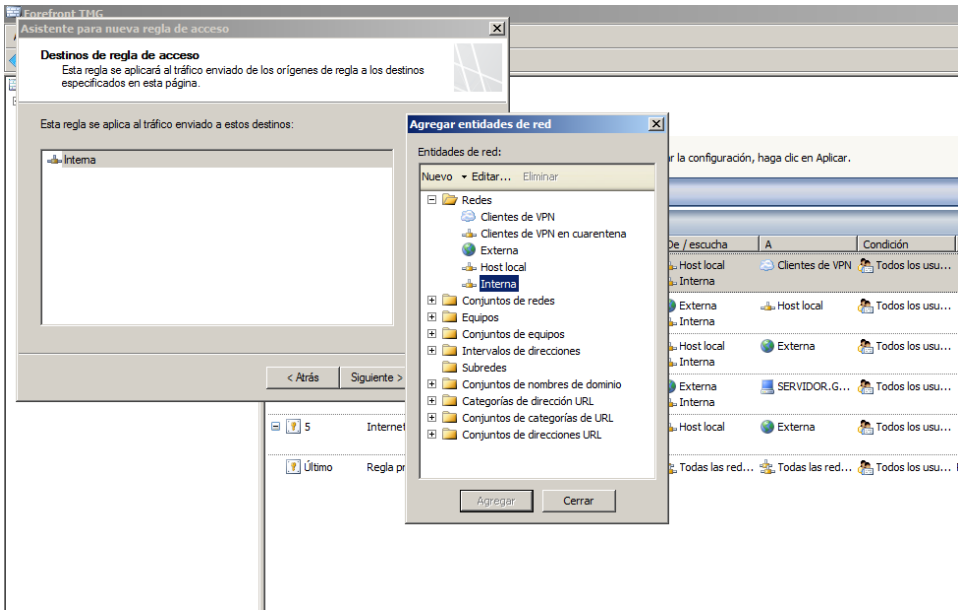


Grafico 82. Agregamos a la red interna.
Fuente: Propia

En este grafico se visualiza la finalización del asistente para la aplicación de la regla Entrada VPN.

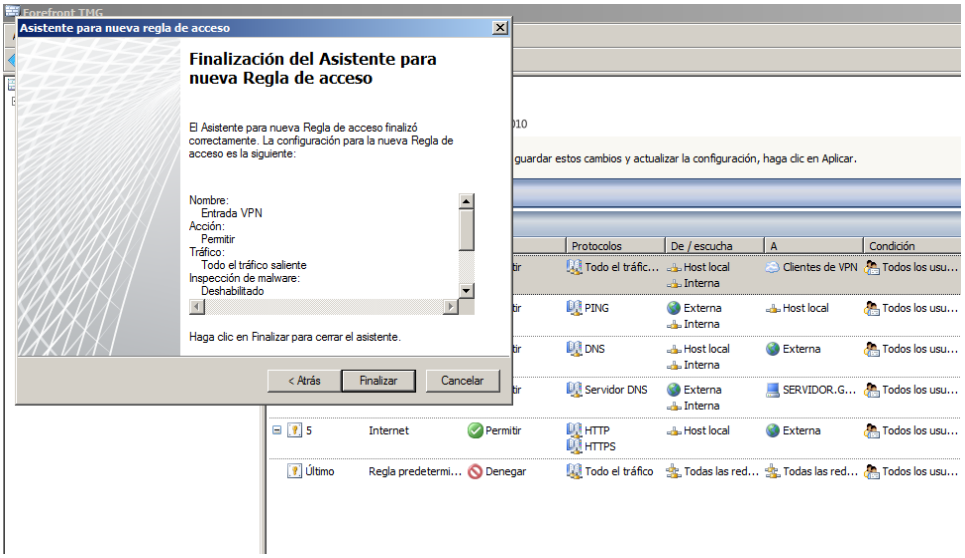


Grafico 83. Finalizando la creación de la regla de entrada VPN.
Fuente: Propia

Seguidamente aplicamos y guardamos toda la creación de la Salida y Entrada VPN.

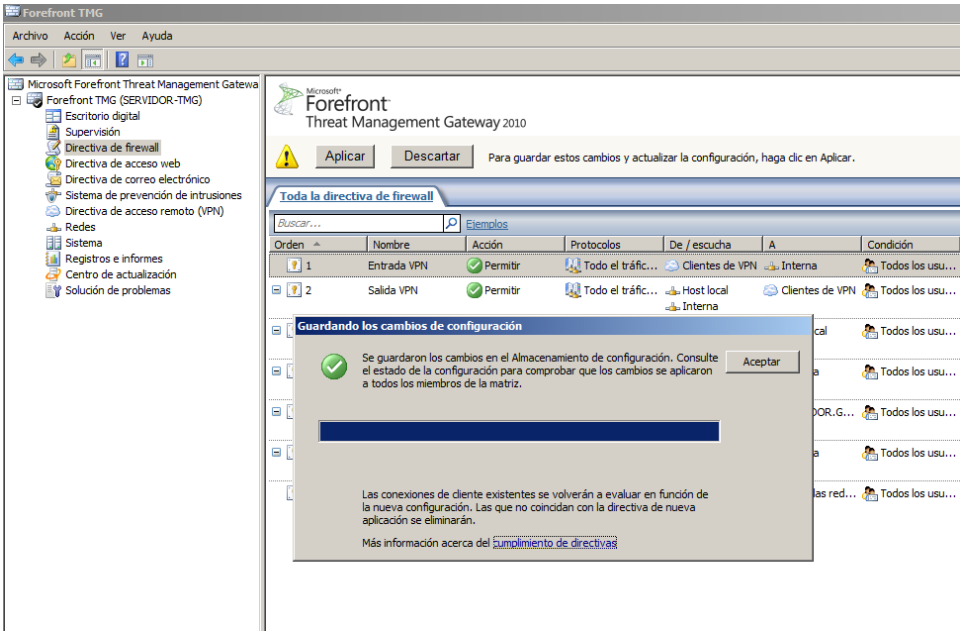


Grafico 84. Guardamos los cambios de entrada y salida VPN.
Fuente: Propia

En el siguiente grafico crearemos la nueva regla de Internet VPN, le damos permitir y siguiente.

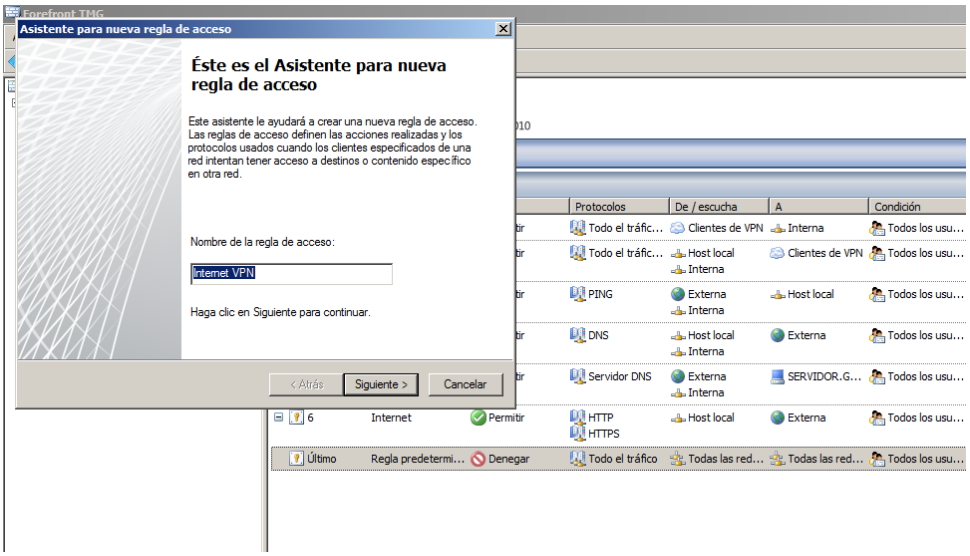


Grafico 85. Regla para que los usuarios accedan a internet
Fuente: Propia

En este grafico seleccionaremos los protocolos DNS, HTTP y HTTPS; le damos siguiente.

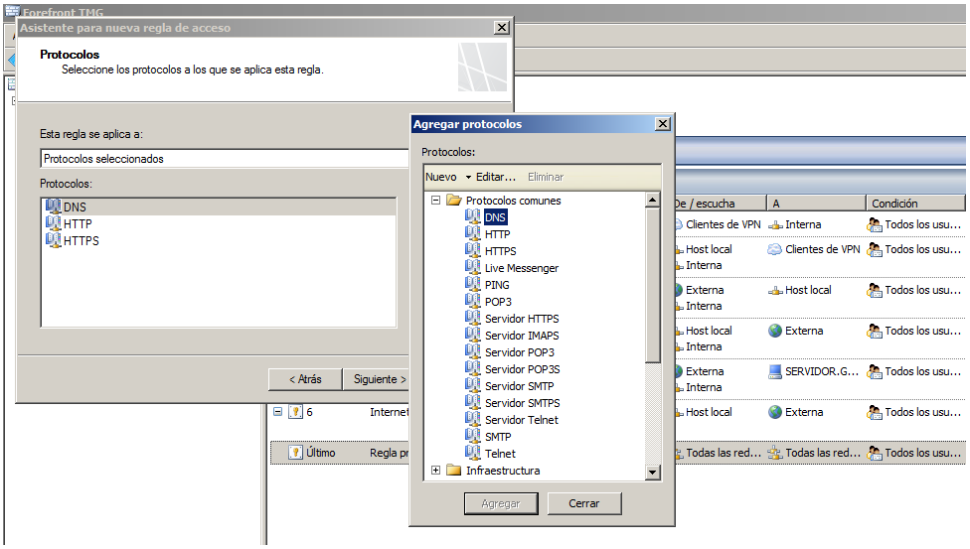


Grafico 86. Selección de protocolos.
Fuente: Propia

En este grafico agregaremos a los Clientes de VPN como orígenes de la regla de acceso a Internet VPN.

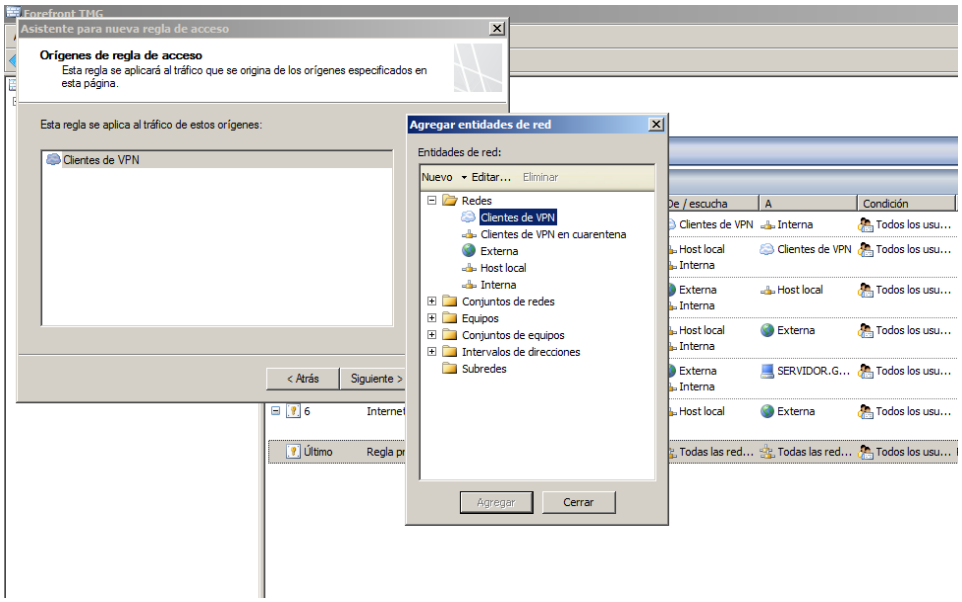


Grafico 87. Seleccionamos a los clientes VPN.
Fuente: Propia

Como destino de la regla de acceso, agregaremos a la Red Externa.

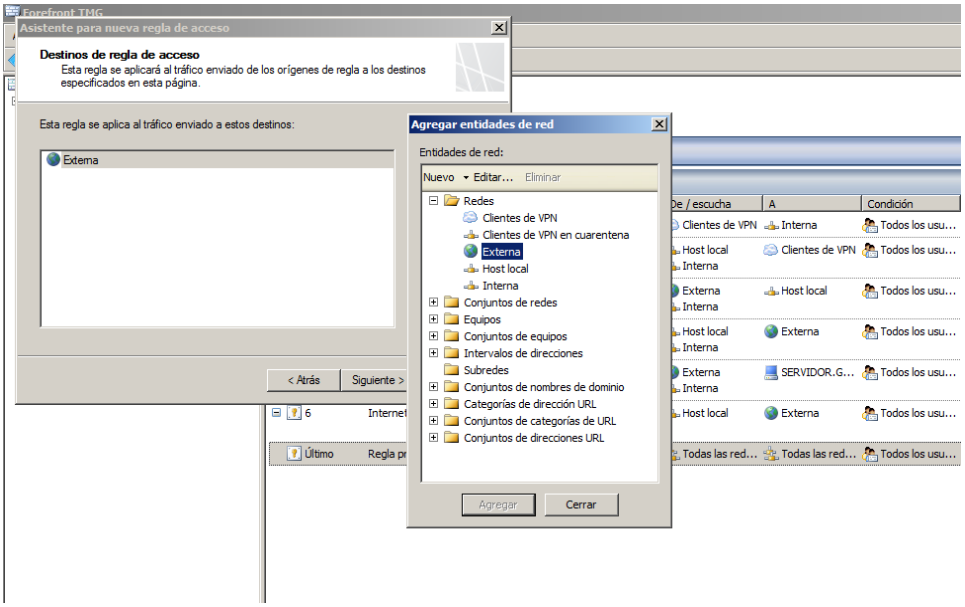


Grafico 88. Seleccionamos la red externa.
Fuente: Propia

En este grafico se visualiza la finalización del asistente para la aplicación de la regla Internet VPN.

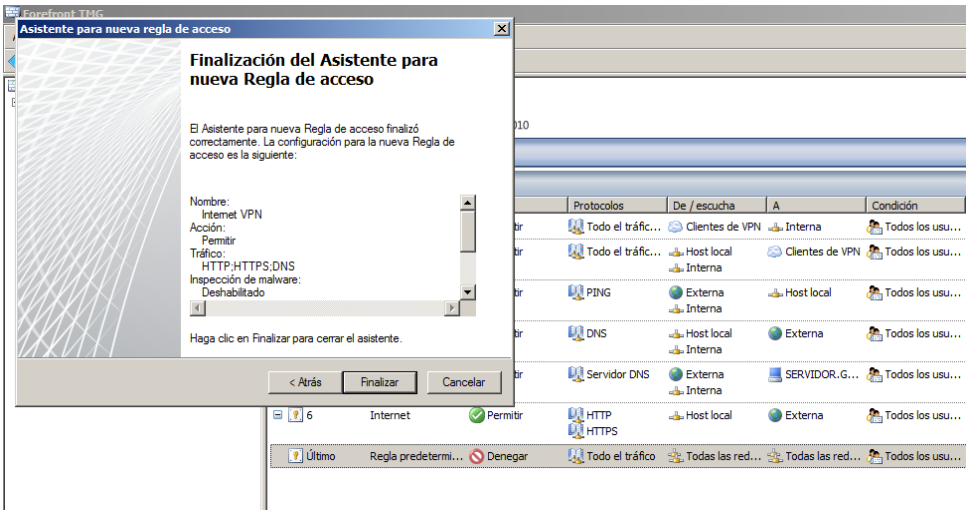


Grafico 89. Finalizando la creación de la regla de Internet VPN.
Fuente: Propia

Seguidamente aplicamos y guardamos toda la creación de todas las reglas para el funcionamiento de la VPN.

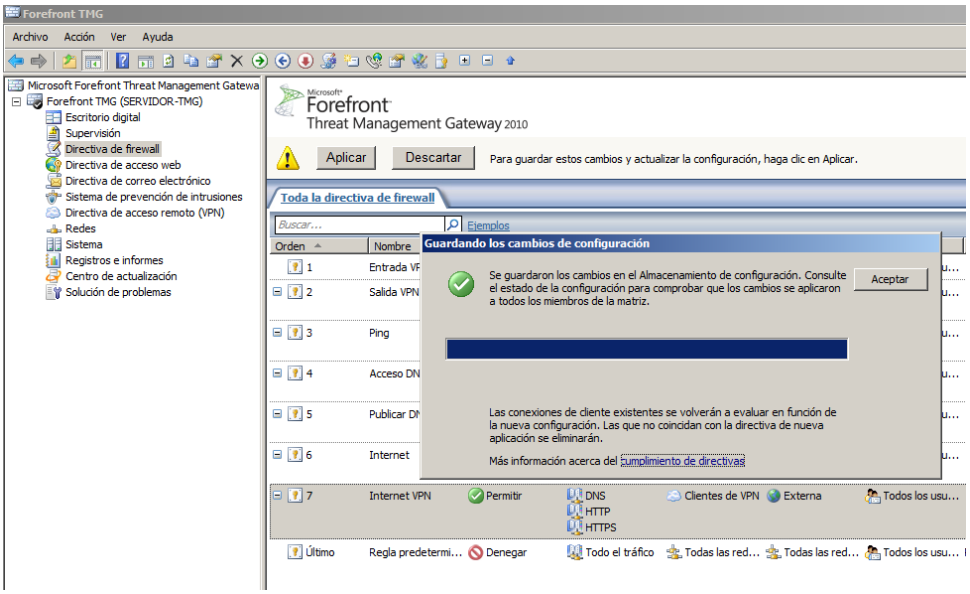


Grafico 90. Guardamos los cambios de Internet VPN.
Fuente: Propia

Finalmente en este grafico podemos visualizar las reglas creadas como: Entrada VPN, Salida VPN, Ping, Acceso DNS, Publicar DNS e Internet VPN.

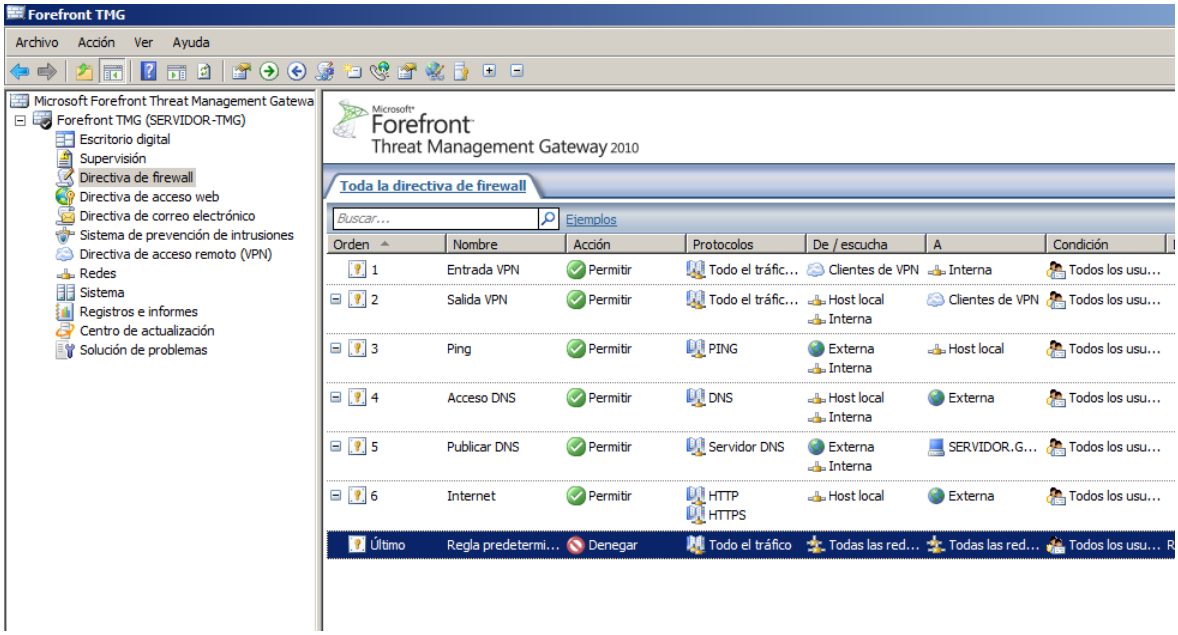


Grafico 91. Reglas creadas para el funcionamiento de la VPN.
Fuente: Propia

DISCUSIÓN DE RESULTADOS

CAPITULO V

PRUEBAS DEL MODELO Y DESEMPEÑO

5.1 Conexión a internet.

El paso inicial para que funcione la VPN es la conexión a Internet, a continuación podemos observar la asignación de IP a una maquina cliente que conectaremos a través de la VPN a la red del Gobierno Regional de Huancavelica, podemos ver que la maquina pertenece a una red de clase A con la IP 10.18.34.14 y tiene acceso a internet.

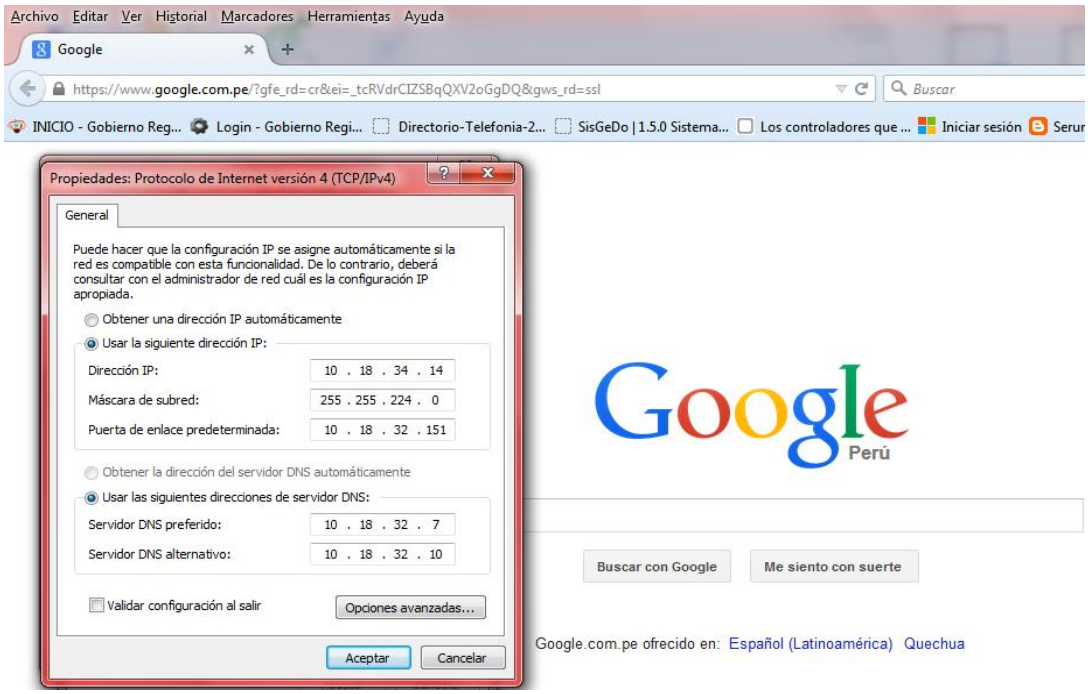


Grafico 92. Configuración de la tarjeta de red del cliente.
Fuente: Propia

5.2 Configuración del cliente VPN en Windows 7.

Ingresamos a la carpeta "**Centro de redes y recursos compartidos**" y en las opciones seleccionamos el enlace "**Configurar una nueva conexión de red**", como se muestra en el grafico 93 hacer clic en ella.

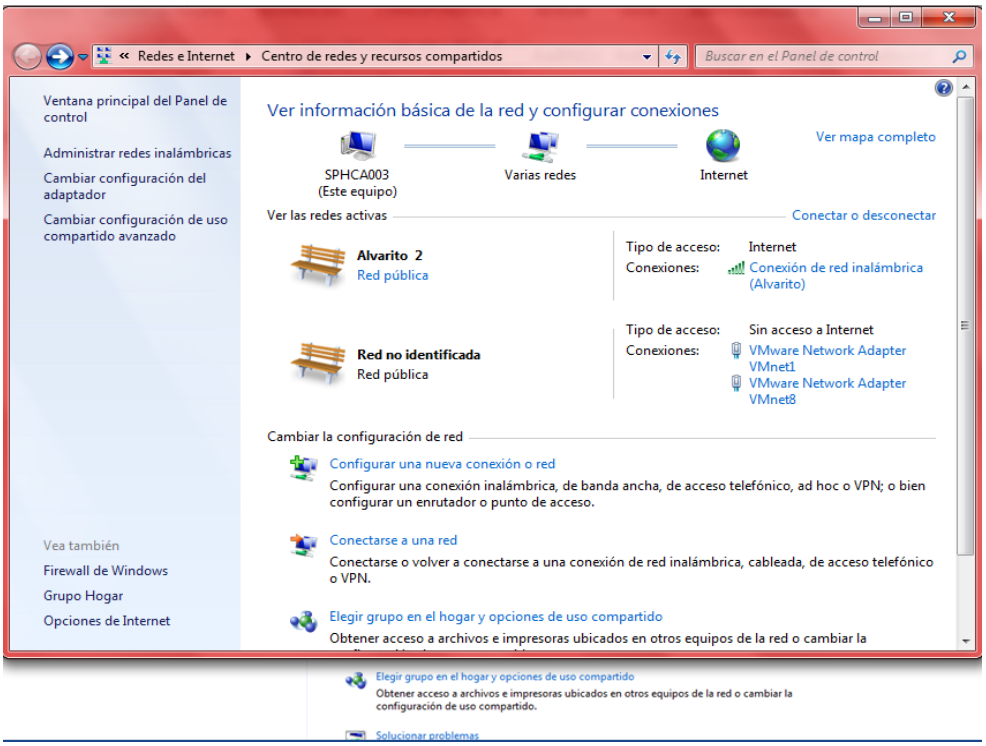


Grafico 93. Configurar una nueva conexión o red.
Fuente: Propia

En el grafico 94 aparece el enlace "**Conectarse a un área de trabajo"**. Se tiene que hacer clic sobre él y darle siguiente.

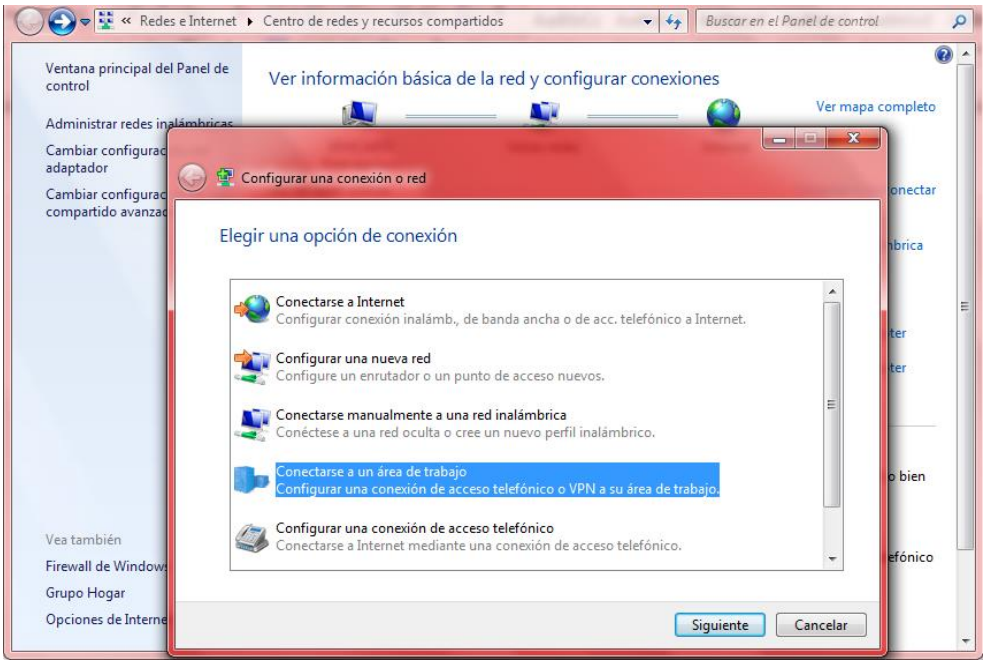


Grafico 94. Conectarse a un área de trabajo.
Fuente: Propia

En la nueva ventana grafico 98 elegir la opción Usar mi conexión a Internet (VPN).

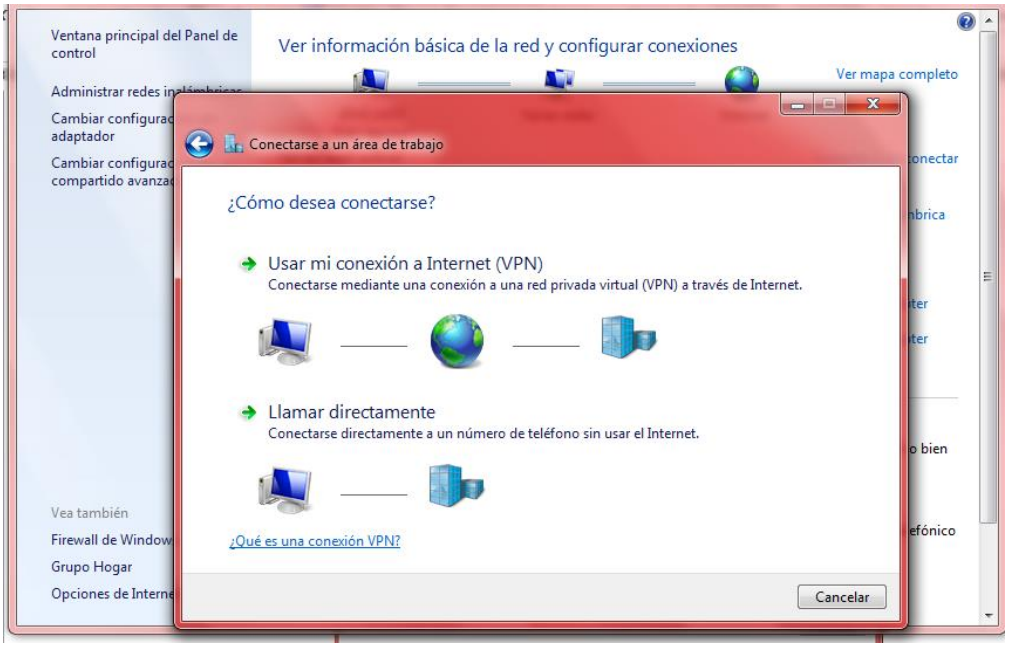


Grafico 95. Conexión a internet (VPN).
Fuente: Propia

En el campo 'Dirección de Internet' se introduce el IP de la tarjeta externa del servidor de túneles 192.168.206.163 y en el campo 'Nombre del destino' se debe escoger un nombre descriptivo para la conexión, grafico 96 dar clic en el botón 'Siguiente'.

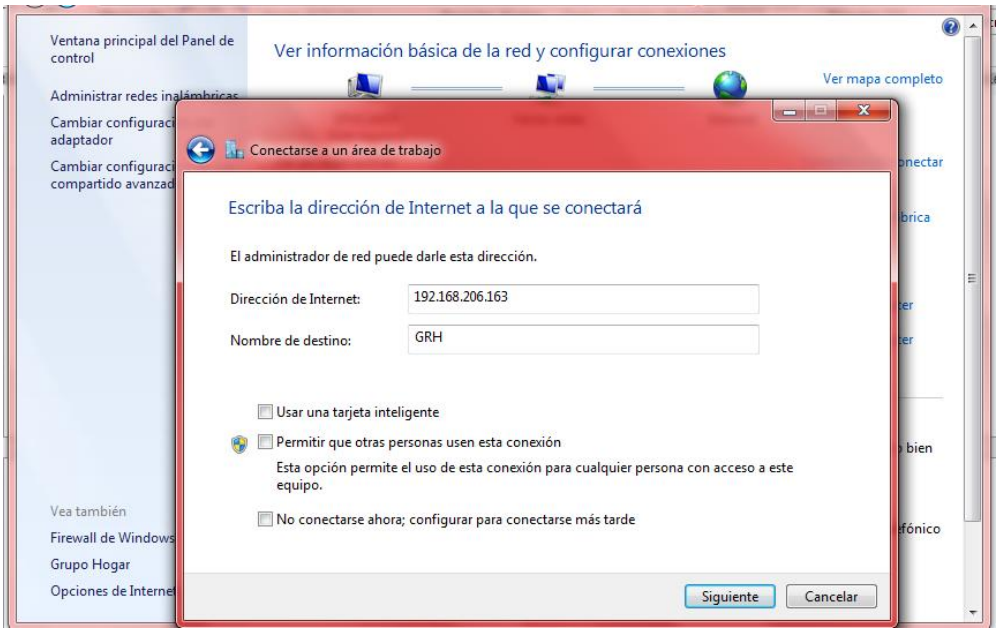


Grafico 96. Conexión a internet (VPN).
Fuente: Propia

Ahora llega el momento de autenticarse como usuario:

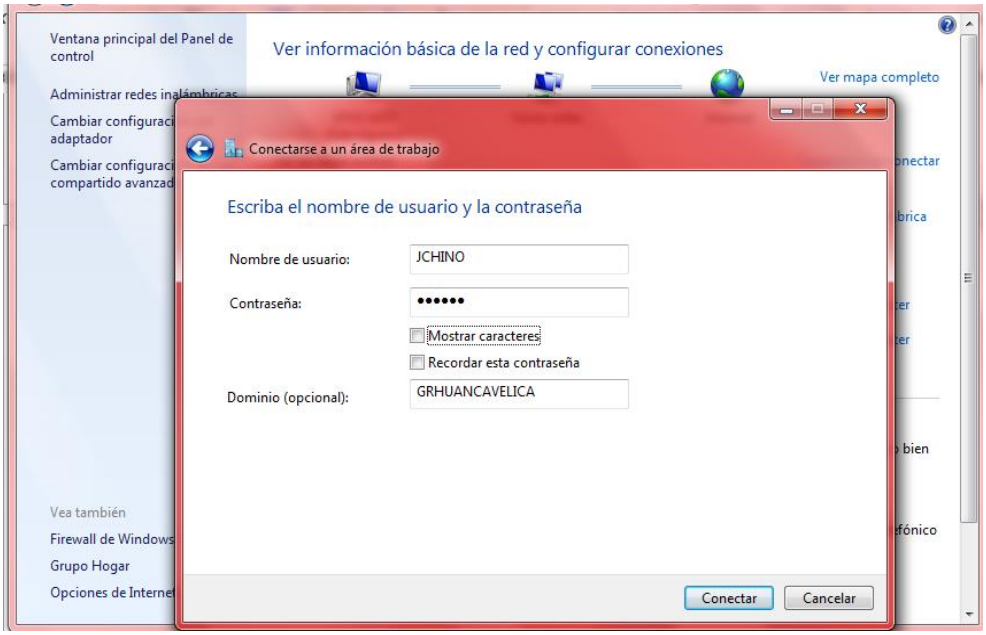


Grafico 97. Ingresamos el usuario, contraseña y dominio.
Fuente: Propia

Ahora se debe introducir el nombre de usuario del grupo Acceso VPN, contraseña y dominio (GRHUANCAVELICA). Clic en el botón 'Conectar', ya solo se debe tener en cuenta que se debe de permitir la conexión en el firewall que maneje ya sea el propio del sistema o firewalls de terceros como el TMG, grafico 98.

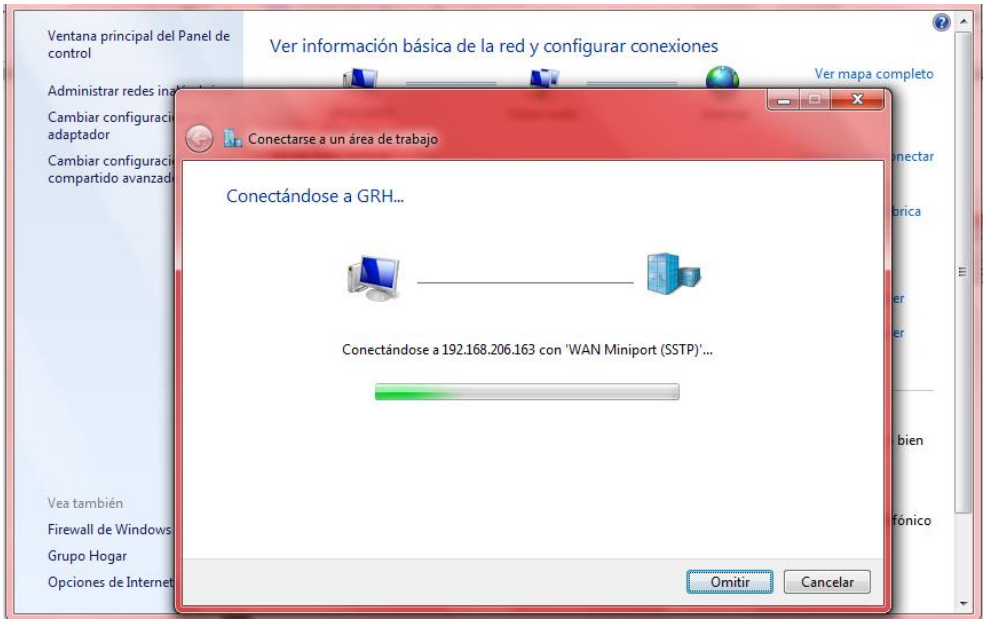


Grafico 98 Conectándose a GRH.
Fuente: Propia

En el grafico 99 vemos que ya se encuentra conectado a la red del Gobierno Regional de Huancavelica a través de la VPN.

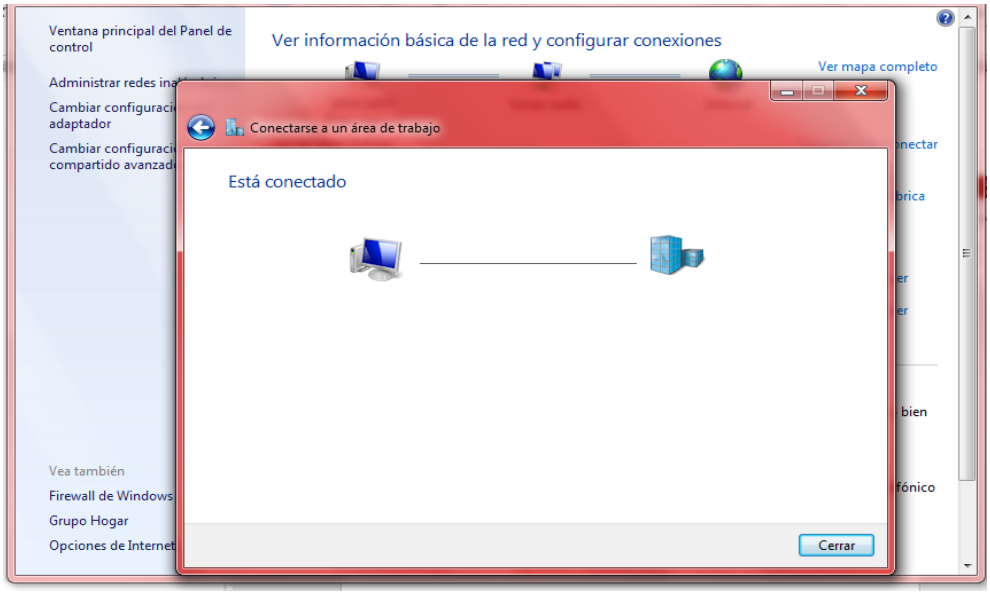


Grafico 99. VPN conectado.
Fuente: Propia

Se ingresó a la opción de enrutamiento y acceso remoto del Servidor TMG, en la lista clientes de acceso remoto podemos observar que se encuentra un usuario conectado: GRHUANCAVELICA\JCHINO, grafico 100.

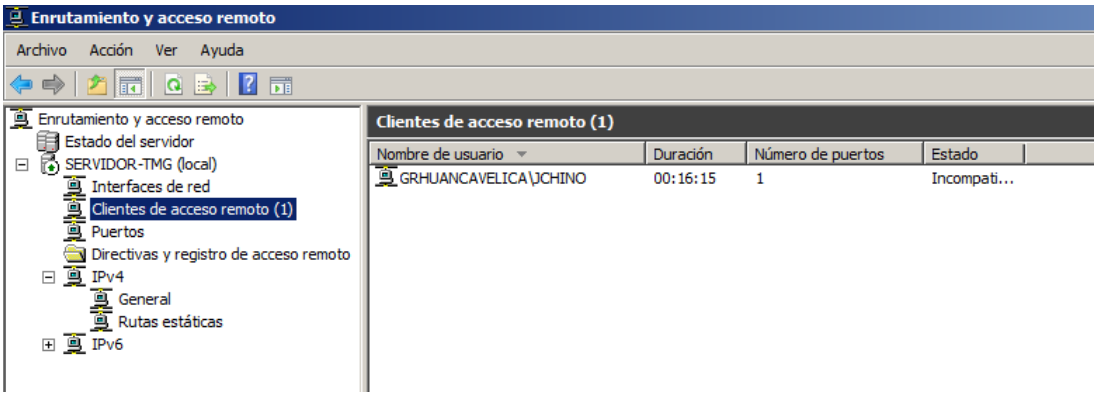


Grafico 100. Usuario conectado a la red.
Fuente: Propia

5.3 Verificación de conexiones y servicios.

Al establecer la VPN entre el host cliente y el Firewall TMG, prácticamente el PC es uno más de la red y puede acceder a los sistemas de la institución a directorios compartidos, conectarse a un servidor, impresoras de red, etc. Para verificar esto, se hicieron las siguientes pruebas:

- ✓ **Latencia**

  Conocida también como tiempo de respuesta, es el tiempo que un paquete de datos transmitido a través de una red, tarda en llegar al destino y regresar.

  La latencia de una conexión puede ser medida con el comando "ping" y se expresa convencionalmente en milisegundos, en este caso, en la conexión VPN se obtuvo una respuesta satisfactoria del servidor de dominio de la institución. Hay que tomar en cuenta que la latencia es sensible a la distancia geográfica.

  La respuesta obtenida de la conexión es de 3 ms de promedio, presentada en el grafico 101.

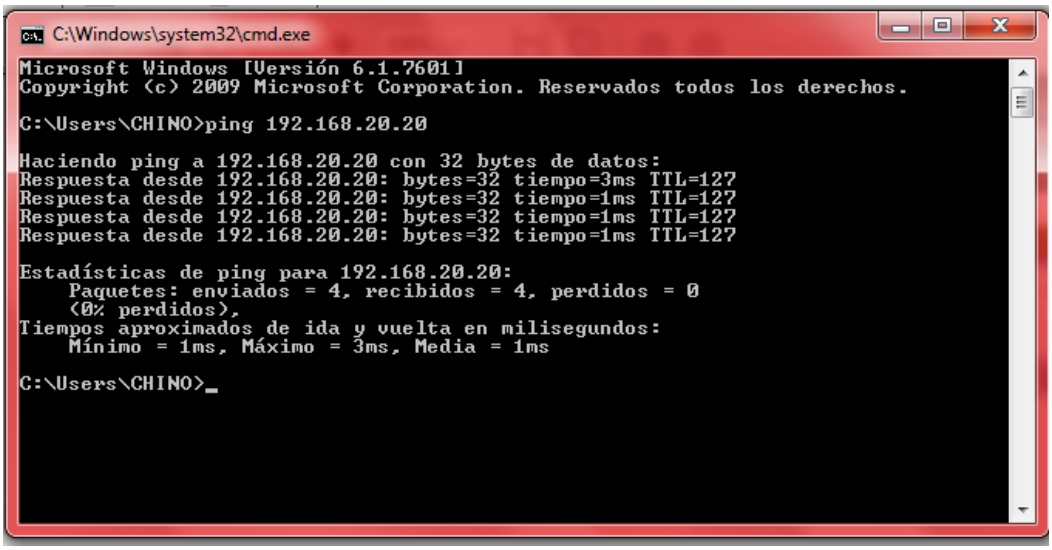


Grafico 101. Latencia de la conexión VPN.
Fuente: Propia

5.4 Resultados de Pruebas.

Este punto es necesario para poder realizar una evaluación del trabajo realizado en la institución, por tanto la evaluación se realizará en todo momento, se evaluará a partir de la puesta en marcha del proyecto y se podrá medir como se está avanzando en la ejecución, en lo posterior se evaluará la utilización de los servicios y por defecto se estará evaluando la conformidad, la aceptación por parte de los usuarios hacia la nueva implementación.

Por último se concluyó que las pruebas resultaron satisfactorias, puesto que la implementación de la VPN a través del Software Forefront TMG 2010 en la simulación realizada funcionó como se esperaba, las mismas que fueron realizadas en presencia del personal y del responsable de la Sub Gerencia de desarrollo Institucional e Informática, así como también los responsables e interesados de las demás unidades ejecutoras y locales descentralizados del Gobierno Regional de Huancavelica.

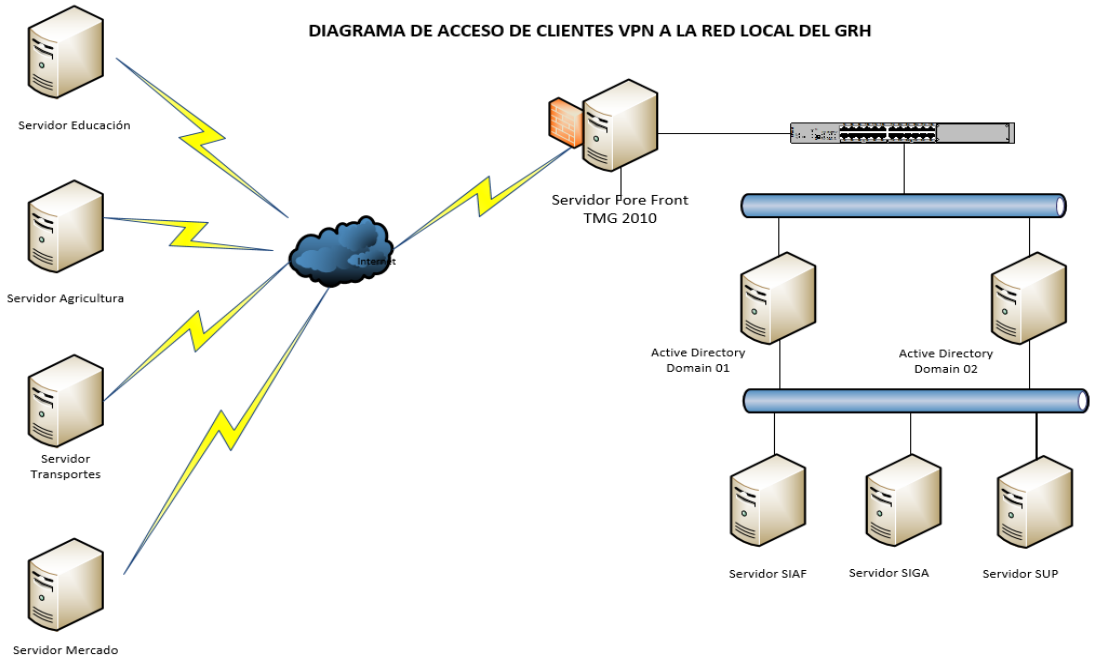


Grafico 102. Diagrama de Acceso a la VPN.
Fuente: Propia

En el siguiente cuadro podemos observar a 08 usuarios que están conectados a través de la VPN cada uno de ellos con sus respectivas cuentas.

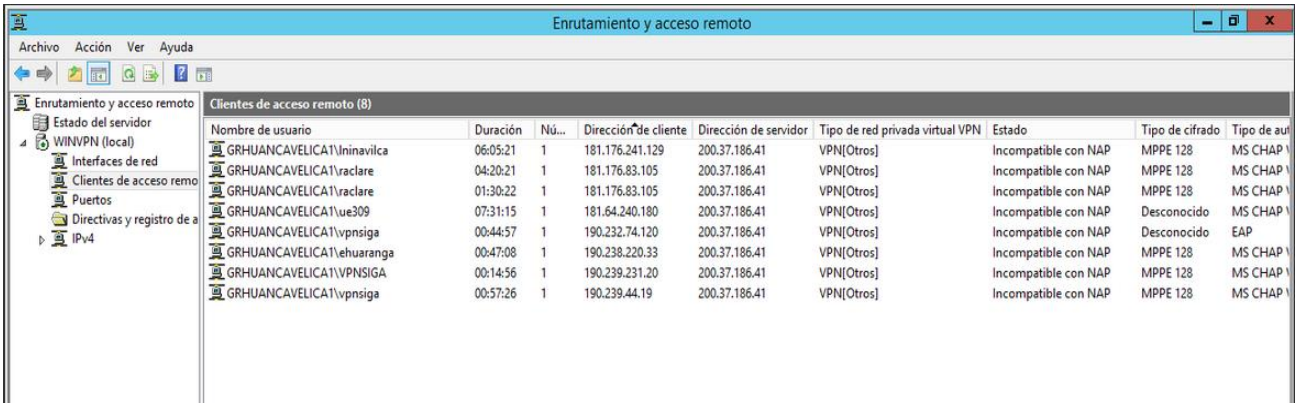


Grafico 103. Usuarios conectados a la VPN.
Fuente: Propia

CONCLUSIONES

1. Se pudo Interconectar la Sede Central del Gobierno Regional de Huancavelica y sus locales descentralizados ubicados en distintos lugares geográficos de la cuidad de Huancavelica a través de la implementación de una Red Privada Virtual (VPN).

2. Se determinó los requerimientos actuales de la infraestructura de comunicaciones del Gobierno Regional de Huancavelica, ello mejorar la plataforma de comunicación entre los distintos locales descentralizados de la entidad.

3. Se diseñó la Infraestructura de Red del Gobierno Regional de Huancavelica, de tal manera que nos permitió mejorar la calidad del servicio de transmisión de datos, mejorar la escalabilidad y sobre todo mejorar la seguridad en la transmisión de datos a través de la Red Privada Virtual.

RECOMENDACIONES

1. Se recomienda mantener la implementación según el modelo propuesto para mejorar la comunicación entre las diferentes sedes y unidades ejecutoras del Gobierno Regional de Huancavelica de acuerdo a los requerimientos determinados.

2. Se debe contar con personal capacitado y dedicado (administrador de red) para las funciones de administración de la VPN y soporte de la red para garantizar la escalabilidad de la solución de manera rápida, segura y confiable.

3. A los usuarios de esta red, tener las precauciones necesarias para evitar fuga de información hacia externos.

4. 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.

5. Dar mantenimiento a la Red cada cierto tiempo.

REFERENCIAS BIBLIOGRÁFICAS

1. Andrew G. Mason, (2002). Arquitecturas MPLS y *VPN*: Redes Privadas Virtuales de Cisco Secure. Editorial Pearson Educación.
2. Cisco Networking Academia, (2013). CCNA Exploration 4.0 Fundamentos Básicos de Networking. http//cisco.netacad.net.
3. Cisco Networking Academia, (2010). CCNA Exploration 4.0 Acceso a la Wan. http//cisco.netacad.net
4. José Luis Ruiz González, (Marzo 2002). VPN - Redes Privadas Virtuales.
5. Kene Reyna Rojas, (2013). Análisis y rediseño de la red informática para mejorar la comunicación en la Red Pacífico Sur y sus dependencias de yugoslavo y Hospital San Ignacio usando tecnología VPN.
6. MacArthur Ortega, (2011). Metodología para la Implementación de Redes Privadas Virtuales.
7. M. en C. Arturo Austria Cornejo, (2008). Implementación de una Red Privada Virtual en la Presidencia Municipal de Pachuca de Soto Hidalgo.
8. Priscilla Oppenheimer, (2011). Top-Down Network Design. Cisco Systems, Inc.