Diseño de redes VPN seguras bajo Windows server 2008

Proyecto fin de carrera Ingeniería Técnica de Telecomunicaciones especialidad en Telemática

Antonio Tudela Botella

Nombre: Antonio Tudela Botella TFC ITT Telemática atudelab@uoc.edu

Agradecimientos

En primer lugar, me gustaría agradecer este proyecto a mi mujer Carolina por haberme apoyado durante todo el tiempo, animándome cuando más lo necesitaba. Espero poder devolverte todo lo que me has dado.

A mi hijo Sergi, del que espero y deseo que supere a su padre en todos los aspectos de la vida. También quiero expresar mi agradecimientos a todos mis familiares (madre, hermana, suegros….) por los distintos apoyos recibidos en todos los aspectos para llevar a cabo esta carrera.

Por último, muy especialmente, me gustaría agradecer y dedicar este proyecto a una persona que ya no está aquí, mi padre. Papa, la espina está quitada……

Indice

INDICE DE FIGURAS

INDICE DE TABLAS

1. Descripción del proyecto

La empresa de calzado BATCH SL, con sede en Barcelona se ha encontrado con dificultades en los últimos años debido a la competencia continua de los países asiáticos. Debido a esta situación ha decidido asociarse con otra compañía llamada PICO SL, con sede en Elx (Alicante) y que produce un calzado de alta calidad, pero que se encuentra con los mismos problemas que la primera empresa.

Estas asociaciones con posible éxito económico, han atraído a otros fabricantes del mercado, convenciendo finalmente a un socio-comercial con sede en Milán llamado DANDE, fusionando finalmente las tres empresas y formando un grupo con mayor proyección, posibilidades económicas y mayor volumen de producción.

Sin embargo, uno de los problemas iniciales que se ha encontrado la nueva empresa resultante, es la segregación total de todas sus redes informáticas y de telecomunicaciones. Las tres empresas disponen de routers con distintos ISP y el gasto de integrar nueva electrónica de red junto con un mismo proveedor (seleccionar tecnologías como MetroEthernet o Telefónica Netlan) puede ser muy elevado para una empresa que debe de destinar sus mayores recursos a recuperar la clientela perdida. Como problema añadido, no se dispone de medidas de seguridad informática (Firewall y Proxy).

La finalidad de este proyecto es presentar una solución tanto teórica como práctica basada en Windows server 2008, que permita realizar la conexión de las redes LAN completamente independientes en las tres ciudades, usando tecnología VPN con protocolo L2TP formando una misma red de trabajo y ofreciendo las distintas capacidades de redundancia para evitar interrupciones del servicio.

En una segunda parte, se implementará en dicha red un sistema de seguridad a través de Linux y de su sistema iptables integrado en su propio kernel.

OBJETIVOS	DENOMINACION	DESCRIPCION
OBJETIVO 1	Conectar dos redes geográficamente separadas por VPN con PPTP bajo Windows server 2008. Realizar un mismo procedimiento con la tecnología L2TP/IPSEC y seleccionar la solución más fiable	Conseguir que las dos redes LAN geográficamente separadas que contienen los usuarios se puedan comunicar como si estuvieran trabajando en un mismo site y compartir los recursos. Se utilizará un laboratorio bajo tecnología virtual (Oracle VirtualBox) montando un entorno de test idéntico a los sites de Barcelona y Alicante consiguiendo conectarlos y mostrando imágenes del proceso de configuración con los dos protocolos. Una vez explicados los dos procedimientos y puestos en práctica se realizará una tabla comparativa.
OBJETIVO 2	Añadir tercer site a la red obtenida en el objetivo 1 y analizar el mejor tipo de diseño posible	Evaluar la posibilidad de una tercera conexión que mediante el protocolo seleccionado anteriormente (PPTP o L2TP/IPSEC) resuelva la conexión entre los tres sites. Se deberá de analizar si es mejor realizar una conexión en estrella o por el contrario en malla. Se aplicará un entorno de test con una simulación de la solución seleccionada.
OBJETIVO 3	Instalación y configuración de un sistema firewall aplicable a las distintas redes para defensa	Modificar el entorno de test para la instalación de un sistema firewall por red local que aporte seguridad sin incrementar el costo del proyecto.

Tabla 1: Objetivos del proyecto

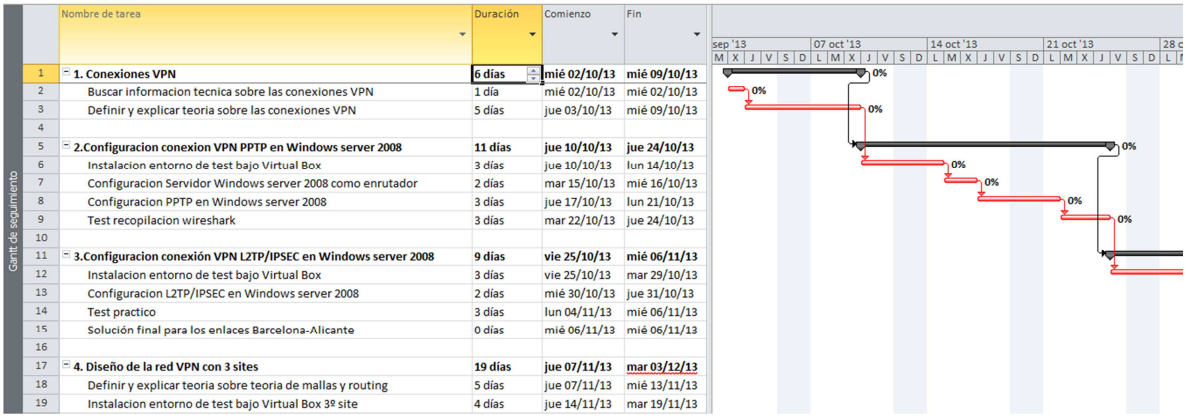
3. Calendario del proyecto

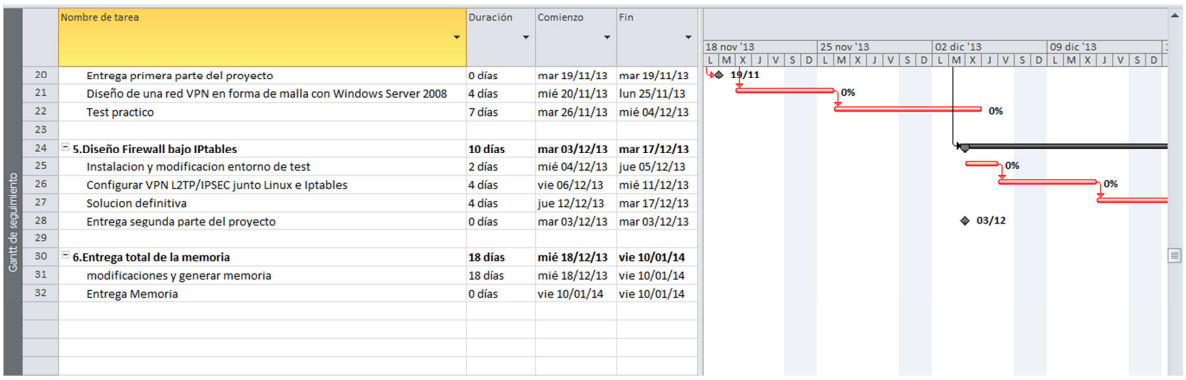
Gantt de seguimiento

	Nombre de tarea	Duración	Comienzo	Fin
1	**1. Conexiones VPN**	**6 días**	**mié 02/10/13**	**mié 09/10/13**
2	Buscar informacion tecnica sobre las conexiones VPN	1 día	mié 02/10/13	mié 02/10/13
3	Definir y explicar teoria sobre las conexiones VPN	5 días	jue 03/10/13	mié 09/10/13
4				
5	**2.Configuracion conexion VPN PPTP en Windows server 2008**	**11 días**	**jue 10/10/13**	**jue 24/10/13**
6	Instalacion entorno de test bajo Virtual Box	3 días	jue 10/10/13	lun 14/10/13
7	Configuracion Servidor Windows server 2008 como enrutador	2 días	mar 15/10/13	mié 16/10/13
8	Configuracion PPTP en Windows server 2008	3 días	jue 17/10/13	lun 21/10/13
9	Test recopilacion wireshark	3 días	mar 22/10/13	jue 24/10/13
10				
11	**3.Configuracion conexión VPN L2TP/IPSEC en Windows server 2008**	**9 días**	**vie 25/10/13**	**mié 06/11/13**
12	Instalacion entorno de test bajo Virtual Box	3 días	vie 25/10/13	mar 29/10/13
13	Configuracion L2TP/IPSEC en Windows server 2008	2 días	mié 30/10/13	jue 31/10/13
14	Test practico	3 días	lun 04/11/13	mié 06/11/13
15	Solución final para los enlaces Barcelona-Alicante	0 días	mié 06/11/13	mié 06/11/13
16				
17	**4. Diseño de la red VPN con 3 sites**	**19 días**	**jue 07/11/13**	**mar 03/12/13**
18	Definir y explicar teoria sobre teoria de mallas y routing	5 días	jue 07/11/13	mié 13/11/13
19	Instalacion entorno de test bajo Virtual Box 3º site	4 días	jue 14/11/13	mar 19/11/13
20	Entrega primera parte del proyecto	0 días	mar 19/11/13	mar 19/11/13
21	Diseño de una red VPN en forma de malla con Windows Server 2008	4 días	mié 20/11/13	lun 25/11/13

Gantt de seguimiento

22	Test practico	7 días	mar 26/11/13	mié 04/12/13
23				
24	**5.Diseño Firewall bajo IPtables**	**10 días**	**mar 03/12/13**	**mar 17/12/13**
25	Instalacion y modificacion entorno de test	2 días	mié 04/12/13	jue 05/12/13
26	Configurar VPN L2TP/IPSEC junto Linux e Iptables	4 días	vie 06/12/13	mié 11/12/13
27	Solucion definitiva	4 días	jue 12/12/13	mar 17/12/13
28	Entrega segunda parte del proyecto	0 días	mar 03/12/13	mar 03/12/13
29				
30	**6.Entrega total de la memoria**	**18 días**	**mié 18/12/13**	**vie 10/01/14**
31	modificaciones y generar memoria	18 días	mié 18/12/13	vie 10/01/14
32	Entrega Memoria	0 días	vie 10/01/14	vie 10/01/14





	Nombre de tarea	Duración	Comienzo	Fin
20	Entrega primera parte del proyecto	0 días	mar 19/11/13	mar 19/11/13
21	Diseño de una red VPN en forma de malla con Windows Server 2008	4 días	mié 20/11/13	lun 25/11/13
22	Test practico	7 días	mar 26/11/13	mié 04/12/13
23				
24	**5.Diseño Firewall bajo IPtables**	**10 días**	**mar 03/12/13**	**mar 17/12/13**
25	Instalacion y modificacion entorno de test	2 días	mié 04/12/13	jue 05/12/13
26	Configurar VPN L2TP/IPSEC junto Linux e Iptables	4 días	vie 06/12/13	mié 11/12/13
27	Solucion definitiva	4 días	jue 12/12/13	mar 17/12/13
28	Entrega segunda parte del proyecto	0 días	mar 03/12/13	mar 03/12/13
29				
30	**6.Entrega total de la memoria**	**18 días**	**mié 18/12/13**	**vie 10/01/14**
31	modificaciones y generar memoria	18 días	mié 18/12/13	vie 10/01/14
32	Entrega Memoria	0 días	vie 10/01/14	vie 10/01/14

4. Viabilidad y beneficios del proyecto

El proyecto se encuentra dentro de los cauces viables en cuanto a capacidad tecnológica y económica.

En el área técnica, el autor de dicho proyecto está certificado como MCTS Windows server 2008 Network infraestructure por lo que conoce la tecnología a aplicar y dispone de la experiencia necesaria para poder hacer frente a los distintos problemas de diseño que vayan surgiendo durante el desarrollo de este proyecto.

En cuanto a la parte económica, todas las simulaciones de servidores y host se ejecutarán bajo una versión gratuita de VirtualBox y los sistemas operativos serán descargables de la página de Microsoft, ofreciendo 6 meses gratuitos para testear dichos productos.

Si finalmente el proyecto se desplegara en una serie de redes separadas geográficamente y en producción habría que tener en cuenta los siguientes precios:

Producto	Precio Unidad	Cantidad	Precio total
Microsoft Windows server 2008 Standard Edition	**528,13**	**3**	**1584,39**
Servidores HP Proliant ML350T06	**1079**	**3**	**3237**
Total			**4821,39**

Tabla 2: Precios de implementación

Sin embargo, este proyecto puede ser llevado a cabo sin necesidad de comprar nuevos componentes utilizando los servidores y licencias ya disponibles en una oficina, siempre y cuando se disponga de la licencia de Windows Server 2008 ya adquirida. Como se puede contemplar no se ha incluido el hardware para diseñar e implementar los sistemas firewall. Esto es debido a que Windows server 2008 incluye el role "Hyper-V" que permite virtualizar gratuitamente otro servidor con distintas funciones y sistema Operativo produciendo un ahorro en los costes.

La finalidad de este proyecto es obtener los siguientes beneficios:

-Posibilidad de utilizar videoconferencia entre sedes ahorrando los costes de viajes de negocios entre distintas sedes.

- Compartir servidores de ficheros, evitando la necesidad de triplicar la infraestructura ubicando dicho dispositivo en un solo site

- Compartir el servidor de correo desde un solo site, evitando el coste triplicado de licencias y mantenimiento de tres servidores de correo independientes.

- Rapidez a la hora de compartir nuevos diseños de productos. Compartir escritorios de trabajo para tomar decisiones conjuntas.

- Aplicación de elementos de seguridad (firewall) que eviten accesos por personal no autorizado, espionaje industrial, keylogging, pérdida de datos…..

5. Conexiones VPN

Definición de redes:

Inicialmente, se define una red de telecomunicaciones como un conjunto de medios de transmisión y conmutación para el envío de información entre puntos separados geográficamente.

Esta definición, es muy general y se puede aplicar a distintos tipos de implementaciones diferentes como pueden ser las redes de acceso a datos, redes sin hilos, redes troncales…. Por lo que la mejor opción es clasificarlas según tres parámetros: velocidad de acceso, cobertura y tipo de propiedad. Especialmente se debe realizar hincapié en estas dos últimas propiedades para definir los tipos de redes existentes.

5.1 Clasificación de redes según propiedad

Red pública: Es una red que alquila líneas de comunicación a usuarios para conectarlos con otros usuarios o con servidores. En estas redes el usuario no administra las líneas de comunicaciones, sino que éstas se encuentran administradas por un operador de telecomunicaciones. La tecnología utilizada se llama WAN.

Red privada: Es una red que administra sus propias líneas de comunicaciones. Son redes que operan con una finalidad determinada y sus usuarios suelen pertenecer a corporaciones con intereses comunes. Suelen ser redes telemáticas formadas por host interconectados entre sí para compartir información.

Red Privada Virtual: El concepto de red privada virtual (de ahora en adelante reconocida por las siglas VPN) es el asunto que interesa especialmente para este proyecto y quedará definido ampliamente en los punto 5,6 y 8. Como resumen previo, una VPN es una red privada (administrada por el propietario) pero que utiliza la red pública para poder unificar distintas redes privadas separadas geográficamente.

5.2 Clasificación de las redes según cobertura:

Según el área de cobertura se definen las redes de la siguiente manera:

Redes LAN (red de área local): Estas redes tienen como principal identidad las altas velocidades cubriendo un área geográfica limitada como puede ser un edifico de X plantas, una red de computadores en una misma área o campus (con un máximo de 5 Km). Las redes LAN utilizan el estándar IEEE y principalmente utilizan tecnología Ethernet, aunque se puede encontrar otras tecnologías como Token Ring o FDDI.

Redes WAN (Red de área amplia): A diferencia de las redes LAN, las redes WAN se caracterizan por tener una velocidad variada (entre 64 Kbits/s a 2 Mbit/s) y están diseñadas para cubrir y dar servicio en todo el planeta. Son construidas por empresas (ISP) que ofrecen sus servicios en todo el país utilizando estándares internacionales.

Una definición muy simple que se puede encontrar en diversos libros es que una red WAN es una red formada por diversas interconexiones de redes LAN. Esta idea que en líneas generales puede tomarse por válida, no es del todo real ya que las redes WAN utilizan sus propias tecnologías como pueden ser:

- RDSI (Red digital de servicios integrados)
- Línea de abonado digital (ADSL)
- Frame Relay
- Modo de transferencia asíncrono
- SONET (Red optima síncrona)

5.2 El modelo OSI

Debido a los conceptos que se tratarán en las distintas configuraciones y explicaciones de este texto, el autor ha creído conveniente el volver a repasar diversos conceptos sobre el modelo OSI, que a buen seguro refrescará antiguos conceptos ya olvidados.

El modelo OSI (sistemas abiertos de interconexión) define los protocolos necesarios para lograr la comunicación entre equipos de una red. El modelo define las funciones en un conjunto jerárquico de capas.

Este sistema sirve especialmente a técnicos para resolver incidencias y problemas de comunicaciones ya que se puede seguir desde la parte inferior hacia arriba para resolver distintos problemas de red. En las siguientes líneas se definen las siete capas que lo componen.

- ***5.2.1 Nivel físico (capa 1):*** Se encarga de las reglas que rigen la transmisión de bits a través de pulsos eléctricos. Es la capa más baja y se suele referir a elementos como cables de cobre o fibra. Cualquier técnico que observe un problema de red deberá de revisar como primer error si no existe ningún problema relacionado con problemas en el área física como cables seccionados o mal conectados.
- ***5.2.2 Nivel de enlace (capa 2):*** Activar, mantener y desactivar. Ésta es la finalidad de la capa de enlace, mantener una conexión entre dos dispositivos. En esta capa también se da la detección de errores. Es importante conocer que los elementos de información en esta capa se denominan tramas y el ensamble y fragmentación de tramas así como su direccionamiento y corrección de errores viene dada por la MAC (Control de acceso a medios). La capa 2 es utilizada por el componente electrónico switch que trocea la información en dichas tramas realizando conmutaciones para entregarlas a sus destinatarios.
- ***5.2.3 Nivel de red (capa 3):*** Posiblemente el más conocido de todos por el concepto IP. El nivel de red se encarga de identificar el enrutamiento entre una o más redes, por lo que es un elemento que suele asociarse con el componente electrónico de red ROUTER. El nivel de red utiliza como unidades de información los llamados PAQUETES a diferencia de la capa de enlace con las TRAMAS. El objetivo claro de esta capa es que los datos lleguen desde el origen al destino.

- ***5.2.4 Nivel de transporte (capa 4):*** Como su nombre indica este nivel se encarga de transportar los datos que se encuentran dentro del paquete desde la máquina origen a destino independientemente de la red elegida. La forma en la que se transmite la información son los llamados datagramas. En este nivel encontramos dos importantes conceptos:
  UDP: El UDP es un protocolo no orientado a la conexión, de manera que no proporciona ningún tipo de control de errores ni de flujo, aunque utiliza mecanismos de detección de errores. En caso de detectar un error, el UDP no entrega el datagrama a la aplicación, sino que lo descarta. Este sistema es ideal para videoconferencias o vozIP

  TCP (protocolo orientado a la conexión): El TCP proporciona fiabilidad a la aplicación; es decir, garantiza la entrega de toda la información en el mismo orden en que ha sido transmitida por la aplicación de origen. Para conseguir esta fiabilidad, el TCP proporciona un servicio orientado a la conexión con un control de flujo y errores.

- ***5.2.5 Capa de sesión (capa 5):*** La misión de esta capa es asegurar que una sesión establecida entre dos máquinas, ésta pueda realizar todas las operaciones de principio a fin, reanudándose en caso de interrupción.

- ***5.2.6 Capa de Presentación (capa 6):*** El objetivo de esta capa es encargarse de la representación de la información, tratándose aspectos como la semántica y la sintaxis de datos transmitidos. Se puede decir que esta capa trabaja el contenido de la comunicación en lugar del "como" comunicarse

- ***5.2.7 Capa de Aplicación (capa 7):*** En esta capa se realiza una pasarela para que los programas o aplicaciones puedan utilizar los servicios de las demás capas y se definen los protocolos a utilizar como puede ser el SMTP, FTP o DNS.

5.3 Definición de red privada virtual (VPN)

Una vez tratados los puntos introductorios 5.1 y 5.2 se está en posición de poder definir y explicar con mayor propiedad que es una red privada virtual.

Se define VPN como una conexión punto a punto de tipo privado a través de una conexión de tipo pública como puede ser internet. Para realizar esta conexión se utilizan los llamados protocolos de tipo túnel. El concepto de túnel es un tanto curioso y debe de ser analizado con detenimiento en las siguientes líneas.

Se define túnel o mejor dicho tunneling a la manera de encapsular paquetes en el interior de otros paquetes los cuales son enviados utilizando la tecnología de red típica de la infraestructura que se está utilizando. De esta manera se permite el transporte de protocolos por redes con diferente esquema de direccionamiento que de otra manera no serían compatibles.

En un esquema VPN típico, se utiliza el tuneling para realizar las llamadas virtuales a un puerto virtual que se encuentran en un servidor VPN. El cliente inicia una conexión punto a punto virtual con un servidor de acceso remoto a través de una conexión pública. Este servidor responde a la llamada, auténtica al usuario y transfiere los datos entre el cliente VPN y la red de la organización.

¿Cómo se puede emular una conexión punto a punto si no existe? Para conseguir el punto a punto virtual, los datos se encapsulan mediante un encabezado. Este encabezado permite la información de enrutamiento permitiendo recorrer la red pública y accediendo a la red privada de destino.

6. Tipos de VPN

Existen 2 tipos principales de VPN:

6.1 VPN de acceso remoto: No es aplicable en este proyecto, pero si se debe de tener en cuenta a modo de estudio de teoría. La VPN de acceso remoto permite que un usuario desde un lugar geográficamente distinto, tenga acceso a un servidor de la red privada que da servicio a una organización mediante la infraestructura de red pública. La conexión PPP se realiza entre el host del usuario y el servidor VPN remoto.

6.2 VPN de sitio a sitio: Será el tipo de VPN a aplicar en este proyecto. Este tipo de VPN permite a las organizaciones tener conexiones enrutadas entre distintas oficinas a través de una red pública. Esta conexión funciona como un vínculo de red WAN dedicado. Para su funcionamiento necesitamos un servidor VPN que hará de enrutador por cada site a conectar. El servidor que hace las veces de enrutador (realiza la llamada) se autentica en el servidor VPN que responde, y se realiza la misma operación a la inversa para obtener autenticación mutua.

7. Seguridad en las redes VPN

El concepto VPN no se puede entender sin aplicar seguridad y criptografía, ya que todo el flujo de información entre los dos enrutadores pasará por una red pública. Si no existe encriptación, los paquetes serían fácilmente capturados y se podría observar su información desde la red WAN.

La seguridad de un sistema de red, y en general, de cualquier sistema informático debe de cumplir los siguientes cuatro puntos:

Confidencialidad: Se intenta exponer un ejemplo para explicar la confidencialidad. Una persona transporta un documento con un mensaje. La persona parte del pueblo A al pueblo B y selecciona un camino que puede ser inseguro por ser de noche y porque puede haber atracadores. Cuando ha realizado la mitad del camino, esta persona es atracada y le sustraen el documento. La capacidad de mantener mediante algún medio el secreto de la información que contiene el documento sustraído, es lo que se llama confidencialidad. Traducido a un sistema de la información, es la posibilidad de enviar un mensaje seguro sin que pueda ser leído por terceros, independientemente del sistema de comunicaciones utilizado.

Autenticación: Es la manera de confirmar que algo o alguien es auténtico es decir es una verificación de identidad y que dicha persona no está siendo suplantada. En términos cotidianos, la autenticación ante un cuerpo de seguridad del estado es el DNI.

En términos informáticos, al recibir un mensaje de alguien es una manera de asegurarnos de que ese alguien es quien nos lo ha enviado y no una tercera persona.

Para hacerlo lo más fácil es depender del User y Password. (El llamado proceso de login).

Integridad: Es la manera de mantener los datos libres de modificaciones de terceros.

No repudio: El no repudio se basa en que cuando alguien autentica un mensaje no puede negar el haberlo autenticado ya que el mensaje vendrá firmado con la firma digital y esto solo se puede realizar con la clave privada que sólo dispone el usuario.

Se deben de cumplir los cuatro puntos principales para considerar una red VPN como una red segura. Se ampliarán otros conceptos de seguridad VPN en el punto 8 de este proyecto.

8. VPN bajo Windows Server 2008

El objetivo del presente documento es realizar una red VPN que permita trabajar a tres sedes distintas geográficamente como si de una LAN se tratara. Se ha seleccionado Windows server 2008 por multitud de factores entre los que caben destacar:

- Soporte: Microsoft ofrece un excelente soporte post-venta ante problemas y nuevas configuraciones. Microsoft ofrece este servicio 24 horas al día durante 365 días al año.
- Facilidad: Intuitivo y simple. Windows server se puede adaptar a cualquier tipo de Hardware (no depende de una plataforma cerrada como Cisco o Apple). Windows puede trabajar en máquinas tanto físicas como virtuales y su entorno de trabajo es conocido por todos los técnicos IT.
- Documentación: Microsoft Windows dispone de un programa llamado Microsoft Technet que reúne recursos e información técnica para millones de expertos en IT. También ofrece certificaciones MCTS de alto reconocimiento.
- Estandarización: Windows Server alcanzó el 75,3% de cuota de mercado en el primer trimestre de 2010 a nivel mundial, según datos de IDC, lo que lo mantiene a la cabeza del mercado de sistemas operativos para servidores.
- Virtualización: Incluye su propio role Hyper-V que permite virtualizar hasta 4 servidores para distintos roles (en este proyecto, un firewall) gratuitamente ahorrando costes de licencia y gasto en hardware (otros fabricantes obligan a adquirir distintos dispositivos según el rol a desempeñar).

Windows Server 2008 se basa en el núcleo Windows NT 6.1. Es un sistema Operativo con un kernel híbrido que soporta plataformas IA-32, x86 e IA-64. Entre las mejoras de esta edición, se destacan nuevas funcionalidades para el Active Directory, nuevas prestaciones de virtualización y administración de sistemas, la inclusión de IIS 7.5 y el soporte para más de 256 procesadores. Hay siete ediciones diferentes: Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server y para Procesadores Itanium.

Su intuitiva interfaz, su multitud de documentación y facilidad de implementación lo hacen ideal para el desarrollo de este proyecto.

Respecto a la implementación de un sistema VPN, Windows Server 2008 permite realizar dos tipos de protocolo de túnel VPN: PPTP y L2TP/IPsec. La base inicial de estas dos conexiones es el protocolo PPP por lo que se estudiará todas estas tecnologías y definiciones en las próximas líneas:

8.1 Protocolo PPP:

Para controlar las conexiones de red se necesitan realizar funciones en la CAPA 2 del modelo OSI. En una red WAN se utiliza el protocolo PPP para lograr dicho control.

PPP proporciona un método para establecer, configurar, mantener y terminar conexiones punto a punto. El procedimiento se divide en las siguientes fases:

- **Fase 1:** Establecer y negociar la configuración
- **Fase 2:** Determinar la calidad del enlace
- **Fase 3:** Negociar la configuración del protocolo de red
- **Fase 4:** Terminar enlace

Con esto PPP ofrece conexiones fiables entre routers siendo uno de los protocolos WAN más utilizados permitiendo varios métodos de autenticación así como compresión y cifrado.

El formato de la tabla PPP es el siguiente:

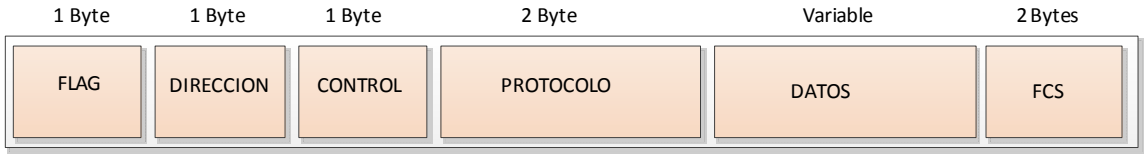


Figura 1: Formato de tabla PPP

Dónde:

- **Flag:** Su misión es delimitar el principio y final de la trama. Su secuencia es 01111110.
- **Dirección:** Define la dirección del transmisor estándar.
- **Control:** Byte con la secuencia 00000011, llama a una transmisión de datos de usuario
- **Protocolo:** 2 Bytes que identifican el protocolo encapsulado de información de la trama
- **Datos:** Contienen el datagrama especificado en el campo protocolo.
- **FCS** = Checksum para errores.

PPP utiliza el protocolo CHAP como protocolo de autenticación. El protocolo CHAP es un método de autenticación que utiliza tres vías. En una autenticación CHAP se dispone de dos nodos A y B. El nodo anfitrión A, envía un reto al dispositivo B, algo como ¿Cuál es la contraseña del usuario? Esta sería la primera vía. Por su parte, el nodo responde con el valor de contraseña. Esta sería la segunda vía. Ya por último, como tercera vía el nodo A verifica si el valor devuelto es correcto, si este no lo es termina la conexión.

8.2 Conexiones PPTP:

El protocolo de túnel punto a punto es un protocolo de red creado por Microsoft Corporation, su principal misión es permitir el tráfico multiprotocolo cifrado y encapsulado en un encabezado IP permitiendo transferencias seguras desde clientes remotos o redes geográficamente dispersas. Para este propósito, Windows server 2008 debe de ser configurado como enrutador con una tarjeta NIC en el rango de red de la IP pública y otra tarjeta de red en el rango privado o LAN. La estructura típica de un paquete PPTP es la siguiente:

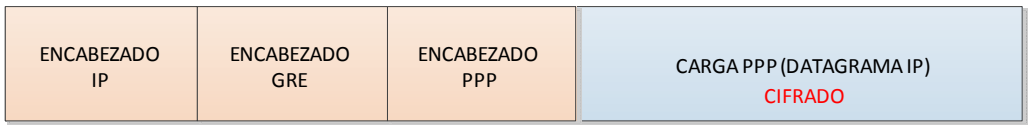


Figura 2: Formato de trama protocolo PPTP

En un escenario típico de PPTP, el servidor que inicie la conexión (cliente) utilizará una conexión de marcado con el servidor de acceso a red del proveedor de servicio utilizando el protocolo PPP. Una vez realizada la conexión entre routers, se establece una segunda conexión con el servidor PPTP que permite acceder a la red privada (LAN separada geográficamente). En realidad el servidor recibirá los datos por su interfaz externa y se encargará de enviarlos a la red interna. PPTP se divide en dos procesos, encapsulación para realizar la segunda comunicación y permitir acceder a la red LAN remota y cifrado para asegurar que los datos viajan seguros.

8.2.1 Proceso de encapsulación en PPTP

El proceso de encapsulación usa una conexión TCP para el establecimiento del túnel y una versión modificada del protocolo GRE.

GRE (Protocolo de encapsulación de enrutamiento genérico) proporciona un mecanismo para encapsular paquetes dentro de un protocolo de transporte. Su finalidad es ser un protocolo para el establecimiento de túneles a través de Internet siendo definido en la RFC1701 y 1702. Este protocolo sería el encargado de redirigir los paquetes desde la red LAN hacia otra red LAN geográficamente separada a través de Internet. La cabecera GRE utilizada por PPTP dispone de una mejora respecto al original ya que incluye un número de reconocimiento para determinar si el

paquete GRE ha alcanzado el otro extremo. A continuación se define la cabecera de un paquete GRE con un tamaño de 32 bits:

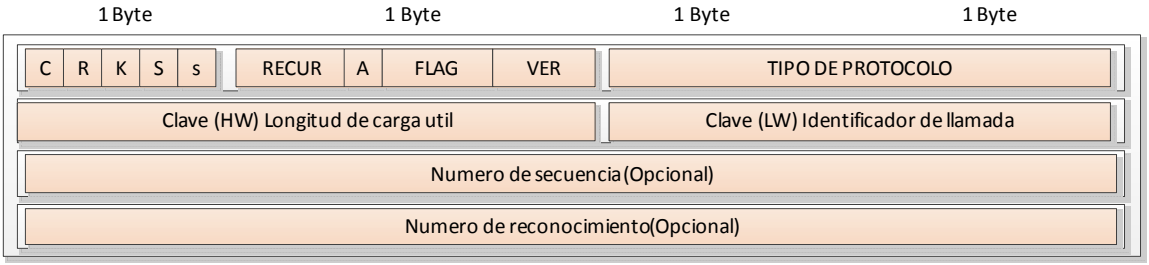


Figura 3: Formato de trama GRE

- C = indica chequeo de suma presente. Se establece en 0
- R = indica que existe un ruteo. Se establece en 0
- K = indica clave presente. Se establece en 1
- S= indica un número de secuencia presente. Si un paquete de datos está presente se establece en 1.
- s= indica la ruta de fuente estricta. Se establece en 0
- A= indica un numero de secuencia de reconocimiento presente. Se establece en 1 si el paquete contiene número de reconocimiento
- Flag = 0
- Versión
- Tipo de protocolo. Por defecto se establece en 880B
- Clave (HW) indica el tamaño de carga útil
- Clave (LW) contiene el indicador de llamada para la sesión a la cual pertenece el paquete.
- Número de secuencia contiene el número de secuencia de carga útil
- Número de reconocimiento contiene el número de paquete GRE más grande recibido durante la sesión. presente si A está a 1.

8.2.2 proceso de cifrado en PPTP

Si se observa la imagen de estructura PPTP (Figura 2: Formato de trama protocolo PPTP), se visualiza que el segmento azul representa la parte de información que deberá llegar al destinatario final (el paquete IP que se entregaría sin encapsular en caso de que se estuviera trabajando en una red LAN). Para proteger esta información en la red pública el paquete se cifra mediante un protocolo propio de Microsoft llamado MPPE. Las claves de cifrado son generadas mediante el proceso de autenticación MS-CHAP v2.

MPPE (Microsoft Point-to-Point Encryption) es un protocolo propio de la empresa Microsoft basado en el algoritmo de cifrado RSA RC4. Dicho sistema basa su funcionamiento en el cifrado en flujo. Consiste en la combinación de un texto claro M (información o datagrama que se envía) junto con un texto cifrado llamado S obtenido a partir de una clave simétrica K que se obtiene mediante el proceso de autenticación MS-CHAPv2.

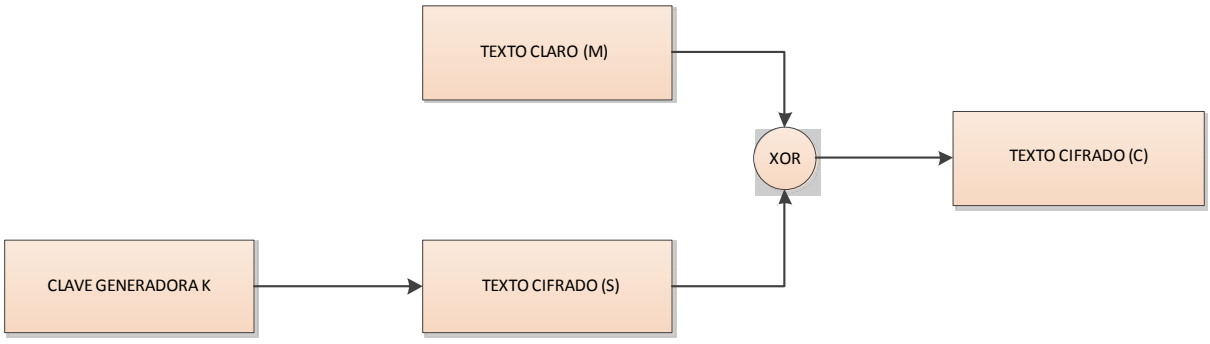


Figura 4: Esquema del cifrado en flujo

En sí, no deja de ser una operación lógica **XOR** entre el mensaje a enviar y un texto cifrado obtenido mediante MS-CHAP, por lo que si un atacante obtuviera S(k) a partir de C podría aplicar un XOR obteniendo el datagrama original y rompiendo la protección del sistema, ya que se cumple que:

$$C = M \oplus S(k)$$
$$M = C \oplus S(k)$$

Sabiendo que la función XOR:

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

Como se puede ver, el cifrado ofrece la ventaja de necesitar muy poca potencia de hardware para operar (poca capacidad de cálculo y consumo de energía) debido a su gran simplicidad. En contra, si un atacante obtiene la clave de cifrado o la función generadora podría aprovechar la simplicidad del protocolo para obtener el mensaje en claro y romper la protección de cifrado del protocolo.

El problema actual del protocolo PPTP es que es susceptible de un ataque Man in the middle, permitiendo robar al atacante el intercambio de información de autenticación al inicio de la conexión VPN. Desde 1999 existe un trabajo de ***Bruce Schneier, Mudge & David Wagner*** llamado **"Cryptoanalysis of Microsoft PPTP Authentication Extension"** que explica las debilidades de las implementaciones MS-CHAPv2 (se recuerda que es la clave generadora) y que fue continuado por **Jochen Eisinger** en **"Exploiting known security holes in Microsoft's PPTP Authentication Extensions (MS-CHAPv2)"** describiendo como implementar dicho ataque. Por ultimo este trabajo fue completado en 2012 por **Moxie Marlinspike**, presentando un trabajo publicado llamado: **"Divide and Conquer: Cracking MS-CHAPv2 with a 100% success rate"** ofreciendo algunas herramientas que podían romper la protección MS-CHAP en cuestión de horas.

El funcionamiento de MS-CHAPv2 es el siguiente. El cliente A (nodo que inicia la conexión) solicita al servidor un desafío de autenticación. El servidor generará un desafío aleatorio de 16 bytes y se lo enviará al cliente. Una vez recibido por el cliente, éste concatena el desafío del servido junto con un número aleatorio de 16 bytes llamado Peer Authenticator Challenge y el nombre de usuario. Con estos valores se obtendrá una cadena hash SHA1. De esta cadena sólo se seleccionarán 8 bytes. Como se puede observar, todo este proceso con tres vías es idéntico al protocolo de autenticación CHAP explicado inicialmente en el protocolo PPP del punto 8 (página 15, párrafo 2). Se analiza a continuación los primeros pasos para obtener MSCHAPv2

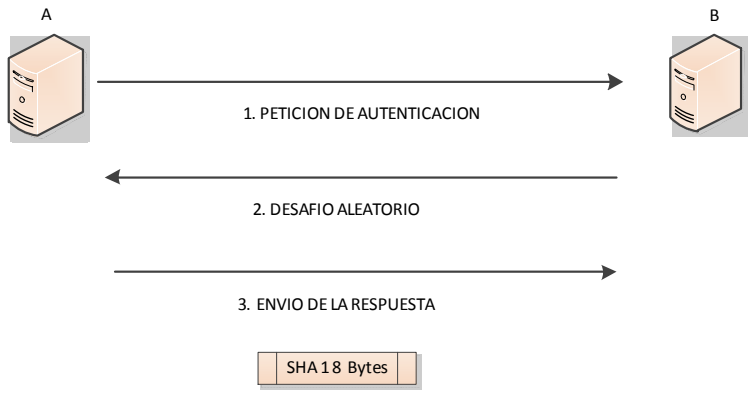


Figura 5: Obtención del SHA1 mediante CHAP en MSCHAPv2

Paralelamente a esta operación CHAP descrita, se ha realizado un cálculo con la contraseña del usuario, aplicándole la función NTPasswordHash, obteniendo un Hash de 16 bytes. Se divide el resultado de esa función en 3 partes de 7 bytes cada una. Como podrá observar el lector, este proceso es imposible de realizar con un tamaño de 16 bytes ya que al dividirlo en 3 partes se obtiene sólo 5 bytes. La solución que ofrece el fabricante es añadir 5 bytes con el valor

0 (esta operación se conoce como bits de sal) para obtener un tamaño sobre NTPasswordHash de 21 bytes y de esta manera tener una división perfecta de 7 bytes en 3 partes:

Figura 6: NT Password Hash de 16 bytes + 5 bytes con valor 0. Se puede observar la división en 3 partes

Llegados a este punto, el lector se estará preguntando ¿Por qué dividir nuestro NT Password Hash junto con la suma de los bytes de sal en partes de 7 Bytes? Es más, si se analiza la figura Figura 5: Obtención del SHA1 mediante CHAP en MSCHAPv2 disponemos también de 8 Bytes obtenidos mediante la aplicación de CHAP. ¿Qué es lo que se realiza a continuación?

Microsoft aplica el algoritmo de cifrado por bloques DES seleccionando el valor SHA1 de 8 bytes (como texto en claro) junto con el valor de los 7 Bytes de la división del NT Password Hash. Esto lo realiza en tres partes separadas completamente, de ahí que necesite completar el NT Password Hash mediante 5 bytes con valor 0. Se debe de tener muy claro que se realizan 3 cifrados DES completamente segregados y no un 3DES que es otro tipo de algoritmo de cifrado. De esta manera se dispone de $2^{56} + 2^{56} + 2^{56} = 2^{57,59}$ claves posibles. También es importante recalcar que en todo momento SHA1 (texto en claro) es el mismo y que no se utiliza uno distinto por cada cifrado DES. Se recomienda consultar la Figura 7: Aplicación del cifrado DES al SHA1 para entender todos estos pasos:

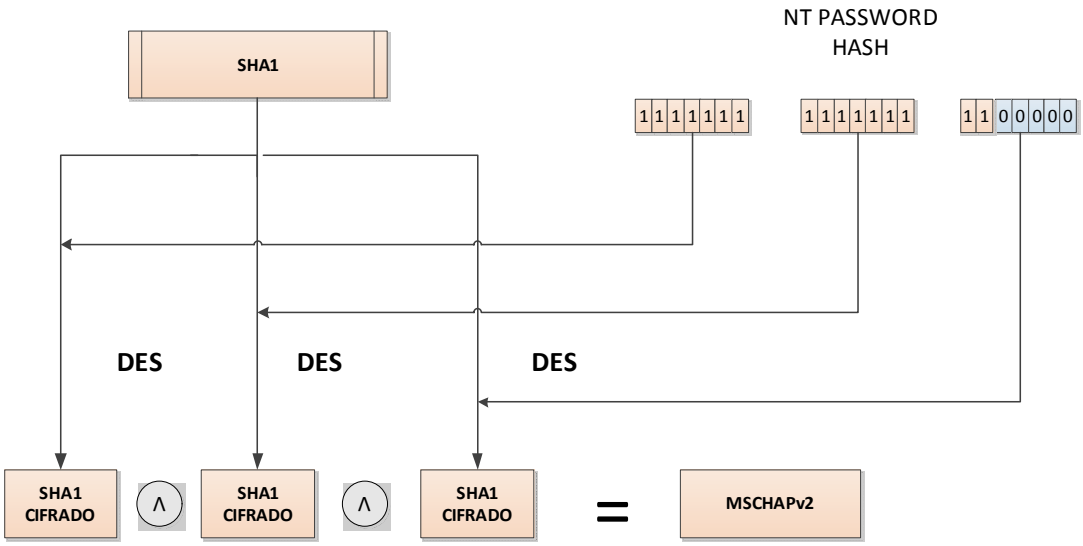


Figura 7: Aplicación del cifrado DES al SHA1

Llegados a este punto, se dispone de 3 SHA1 cifrados segregados, pero con un pequeño matiz. Los dos primeros SHA1 cifrados se han obtenido con un texto claro de 8 Bytes y un bloque para cifrar de 7 bytes, dando como resultado 2^{56} posibilidades, pero el tercer SHA se realiza con un SHA de 8 bytes y un bloque de solo 2 bytes ya que el restante hasta los 7 Bytes se completa con ceros. Esto da como resultado un SHA cifrado con 2^{16} posibles claves.

Siguiendo el trabajo de Jochen Eisinge, con un antiguo Intel celeron a 550 Mhz se puede testear cerca de 2^{16} password por segundo, por lo que si se obtuviera una captura mediante un proceso Man in the middle se obtendría el tercer DES prácticamente al instante. Solo quedaría trabajar con los restantes 14 bytes ya que la tercera clave es trivial, Además, como Microsoft ejecuta cada cifrado por separado, tan solo se tendría que iterar por cada una de las 2^{56}combinaciones de la primera clave, y en cada iteración pasar la combinación DES sobre el desafío de 8 bytes. Esto se realizaría 2 veces, una para cada clave.

Sin embargo, si el lector vuelve a fijarse en la figura 7 en esta misma página, podrá observar el SHA1 que se selecciona como texto en claro es la misma para obtener los 3 resultados cifrados, por lo que las iteraciones pueden ser unidas en una sola obteniendo una complejidad de 2^{56}, dejando la capacidad del protocolo MS-CHAP v2 en una sola operación DES.

Si se consulta información sobre el cifrado DES se puede determinar que existe una máquina de crackeado de DES (Electronic Frontier Foundation) que contiene 1,536 chips y podía romper una clave DES por fuerza bruta en días por lo que queda demostrado que dicho protocolo no es seguro. (Fuente: Wikipedia).

8.3 Conexiones L2TP/Ipsec

Este protocolo permite cifrar tráfico multiprotocolo permitiendo enviar paquetes por cualquier canal punto a punto. L2TP es una combinación de PPTP estudiado anteriormente y L2F desarrollado por **Cisco Systems**. Dicho protocolo trabaja en la capa 2 de enlace a diferencia de PPTP que lo hace en la capa 3.El sistema implementado de L2TP por parte de Microsoft evita utilizar MPPE para cifrar datos tal y como observa en PPTP, en su lugar Microsoft ha apostado por la tecnología IPsec proporcionando mayor integridad y autenticación.

8.3.1 Proceso de encapsulación en L2TP

El principal protocolo que se utilizará para el proceso de encapsulación será el protocolo de túnel de capa 2 (L2TP Layer 2 Tunneling Protocol). Este es un protocolo estándar aprobado por el **IETF** y que puede ser implementado por cualquier desarrollador de tecnología (a diferencia de PPTP que es propiedad de Microsoft) pudiendo encontrarse en el **RFC 2661**. La finalidad principal de este protocolo es encapsular las tramas PPP a través de cualquier tecnología WAN como puede ser IP, Frame Relay, ATM…

Para poder enviar las tramas PPP, L2TP utiliza UDP para montar un túnel entre servidores VPN y enviar PPP encapsulado, ofreciendo cifrar y comprimir la información. El cifrado del protocolo L2TP/IPsec ocupará todo un capítulo de este proyecto debido a su importancia por lo que no será tratado en estas mismas líneas. Sí que sería importante que el lector conociera que L2TP ofrece seguridad propia a través de autenticación de usuarios como CHAP y MS-CHAPv2. Si el lector ha leído con atención los anteriores capítulos entenderá fácilmente el porqué de añadir IPsec como solución de cifrado en lugar de "fiarse" de la seguridad que ofrece L2TP.

La estructura de L2TP se basa en dos partes. Por un lado, un concentrador de acceso llamado LAC. Para comprenderlo fácilmente, LAC actúa en uno de los extremos del túnel L2TP y vendría a ser un dispositivo físico (en este proyecto, un servidor VPN) que iniciaría las llamadas entrantes y receptor de las llamadas salientes. Cada sede debe de tener un LAC.

Por otro lado, tenemos un LNS que sería el receptor de las llamadas entrantes y el emisor de las salientes.

L2TP también contiene varias señales de control. En la siguiente tabla se describen dichas señales:

Codigo	Nombre	Descripcion
0	Reservado	
1	SCCRQ	Inicio del establecimiento L2TP
2	SCCRP	Indica el éxito o el establecimiento de la sesion
3	SCCCN	Respuesta a SCCRP
4	StopCCN	Fin del tunel
5	Reservado	
6	Hello	Envio cliente-servidor para mantener la conexión
7	OCRQ	Peticion del cliente para iniciar el tunel
8	OCRP	Respuesta al mensaje 7. Contiene un identificador unico para el tunel
9	OCCN	Respuesta al mensaje 8.
10	ICRQ	Peticion del cliente para recibir una llamada entrante del servidor
11	ICRP	Indica si la llamada del punto 1 debe ser contestada
12	ICCN	Llamada addicional del servidor como respuesta al mensaje 11
13	Reservado	
14	CDN	Fin de la sesion L2TP
15	WEN	Notifica un error de la conexión WAN
16	SLI	Notifica cambios en el PPP

Figura 8: Cuadro de señales de control protocolo L2TP

Con todos estos datos, se describe cual es el proceso de funcionamiento de L2TP aplicando un túnel:

1) Se establece la conexión de control inicial entre LAC (servidor origen) y LNS (servidor destino) intercambiando mensajes SCCRQ, SCCRP y SCCCN
2) Se autentica el túnel mediante CHAP
3) Se establece una conexión de control creando sesiones individuales e intercambiando los mensajes ICRQ, ICRP e ICCN para llamadas entrantes y OCRQ, OCRP y OCCN para salientes
4) Una vez establecido el túnel, las tramas PPP del sistema remoto son recibidas por LAC y encapsuladas en L2TP enviándose por el túnel adecuado. LNS recibe el paquete desencapsulando PPP.
5) Se envía un mensaje Hello para mantener la conexión sin notar caída.
6) Para finalizar la sesión o bien LAC o bien LNS deben de enviar un mensaje CDN

Por último, se ofrece la trama L2TP, a diferencia de GRE, Microsoft no ofrece modificación alguna cumpliéndose los estándar RFC.

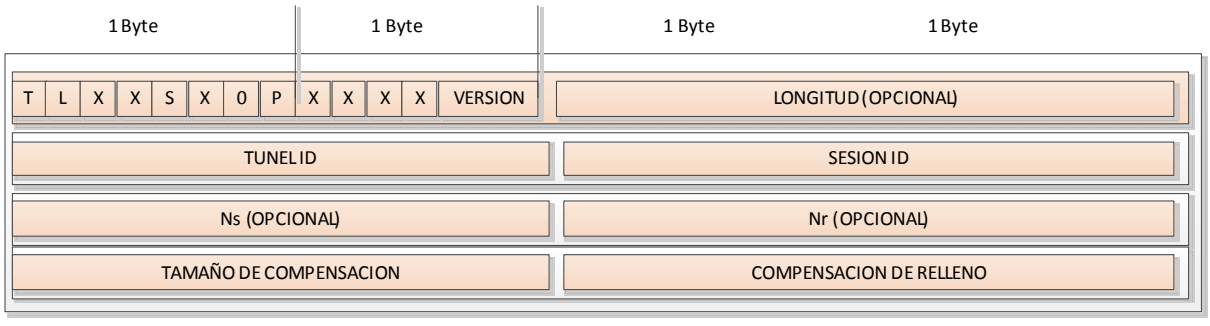


Figura 9: Trama protocolo L2TP

- El bit T indica el tipo de mensaje. Se establece en 0 si es de datos o 1 si es de control
- Cuando está en uno el campo longitud (L) existe. Cuando se trate de un mensaje de control siempre estará en 1
- X se mantiene como una extensión para el futuro por lo que su valor actual es 0.
- Cuando el bit S está en 1, los campos Ns y Nr existen.

- Si el bit O (compensación) está en 1, el campo de compensación existe. En un mensaje de control siempre es 0
- Si el bit P está en 1, este mensaje tiene prioridad durante la transmisión.
- El campo versión indica la cabecera de mensaje L2TP
- El campo Longitud indica la longitud del mensaje en octetos
- El túnel ID indica el identificador para la conexión de control. Este valor identifica al túnel
- La sesión ID indica el identificador para una sesión dentro del túnel
- Ns indica el número de secuencia para el mensaje. Inicia en 0 e incrementa progresivamente
- Nr indica el número de secuencia esperado en el siguiente mensaje.
- La compensación de relleno especifica el número de octetos después de la cabecera

La encapsulación quedaría de la siguiente manera, una trama PPP se encapsula con un encabezado L2TP y UDP:

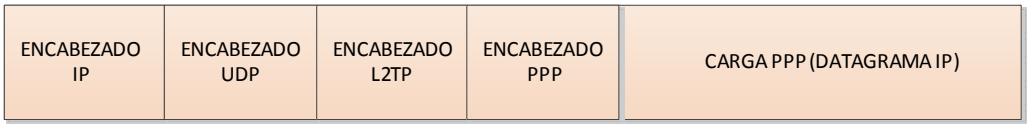


Figura 10: Encapsulación de una trama L2TP

8.3.2 Proceso de cifrado. Protocolo IPsec

IPsec es un conjunto de estándares que trabajan de forma conjunta ofreciendo seguridad en una comunicación de red. IPsec asegura Confidencialidad, integridad y Autenticación. Los principales protocolos que componen IPsec son:

- AH: Protocolo para asegurar la autenticación
- ESP: Protocolo que también se utiliza para ofrecer autenticación y que además añade cifrado
- IKE: Protocolo encargado de realizar la negociación de asociaciones de seguridad (SA)

En los siguientes puntos se ofrecerá una explicación más detallada sobre el concepto IPsec y sus protocolos.

8.3.3 Arquitectura IPSec. El concepto SA

Inicialmente existen dos agentes que intervienen en la arquitectura IPsec. Los nodos extremos de la comunicación que serán los servidores VPN de cada sede. Por otro lado, los nodos intermedios que soporten IPsec, llamados pasarelas seguras como podrían ser los routers y los firewalls.

Una gran ventaja del protocolo IPsec es que en caso de pasar por nodos intermedios que no soporten IPsec, éstos son trasparentes al protocolo ya que el datagrama IPsec es exactamente igual a otro datagrama IP.

La relación que se establece entre dos nodos que se envían datagramas IPSec el uno al otro se llama **asociación de seguridad (SA).** Estos dos nodos pueden ser o no los extremos de la comunicación, en el caso del actual proyecto a

pesar de incluir encaminadores y firewall la conexión se encuentra presente desde el extremo (servidor VPN) que la origina hasta el servidor VPN que recibe los datos.

Las SA siempre funcionarán en modo unidireccional. Si un servidor origen VPN llamado A envía un datagrama IPSEC a un servidor VPN llamado B, no se usaría el mismo SA para que B enviara una contestación a A, es por ello que se tendría dos SA, una en cada sentido. Esto hace que cada nodo deba de guardar información sobre su SA , de esta manera se sabrá el tipo de algoritmo criptográfico utilizado. A la base de datos que contiene información de un SA se le llama SAD **(Segurity association Database)** y a su vez se dispone de un SPI, que es un número incremental que permite identificar el paquete junto con la IP y que evita un ataque REPLAY, el cual consiste en capturar información y re-enviarla con el objetivo de suplantar la identidad.

Por último, el SAD no es la única base de datos con la que trabaja SA, también se dispone una base de datos llamada SPD (Security policy Database) donde se especifican criterios como la aplicación de seguridad con ESP o AH, procesar el datagrama o descartarlo.

8.3.4 El protocolo IKE

Para obtener los SA descritos en el anterior punto, se necesita algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios. El protocolo que se encarga de dicha función es denominado con el nombre de IKE. Éste es un protocolo hibrido que ha resultado de la integración de dos protocolos llamados ISAKMP y Oakley.

Por un lado ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE mientras que Oakley especifica la lógica de cómo se realizará de forma segura el intercambio de claves entre las partes que no se conocen previamente.

El funcionamiento de IKE está compuesto por 2 partes:

1 Parte: En esta primera parte, ambos nodos establecerán un canal seguro y autenticado. Para conseguir dicho canal seguro se utilizará un algoritmo de cifrado simétrico. La clave maestra de este algoritmo se obtiene mediante el algoritmo de claves Diffie-Hellman. Este algoritmo se basa en un cálculo que incluyen un número primo (a partir de ahora se hará referencia a él como p) y una base g. Se dispone en las siguientes líneas de un ejemplo de dos usuarios A y B. Para comunicarse utilizando una clave secreta, Diffie Hellman selecciona un numero primo, en el caso de este ejemplo p=11 y una base g=2.

Los dos usuarios A y B seleccionarán un número secreto llamado a y b respectivamente, siendo [(a || b)<p]. El usuario A selecciona a=5 y el usuario B selecciona b=7. A partir de aquí se realizará la siguiente serie de operaciones matemáticas basadas en la función mod que devuelve el resto de la división de dos números enteros. En primer lugar, el usuario A generará una operación seleccionando la base g y elevándola con el valor de a. El resultado de esta operación se dividirá entre el valor del número entero obteniendo su resto.

$A = g^a \bmod p$ (1)

Donde operando sobre el ejemplo, A obtendría $A = 2^5 \bmod 11 = 10$ (2)

La misma operación realizaría B aplicando la ecuación $B = g^b \bmod p$ (3)

$B = 2^7 \bmod 11 = 7$ (4)

Con estas sencillas operaciones, se obtienen los valores que serán reconocidos como claves públicas y que serán intercambiadas entre los dos usuarios A y B.

Una vez intercambiadas las claves se opera para obtener la clave secreta. El usuario A aplica la siguiente fórmula con la clave pública de B:

$$M = B^a \bmod p \ (5)$$

y por su parte B aplica la misma ecuación número 5 sustituyendo los valores de la clave pública b por a y a por b respectivamente:

$$M = A^b \bmod p \ (6)$$

Donde se obtiene finalmente que A y B coinciden en la clave secreta:

$$M = 7^5 \bmod 11 = 10 \ (7)$$

$$M = 10^7 \bmod 11 = 10 \ (8)$$

La primera parte del protocolo IKE puede operar de dos maneras, en Modo principal y en modo agresivo. En el modo principal, también conocido como main mode, se opera con un intercambio de 6 mensajes. En los 2 primeros mensajes se negocia la seguridad mediante una cookie, los siguientes dos mensajes negocian los valores públicos para el intercambio Diffie Hellman (ecuaciones 1 y 3) y los dos últimos autentifican el intercambio diffie Hellman. Se ha realizado la siguiente imagen para asimilar mejor el intercambio. Las flechas incluyen las ecuaciones numeradas presentadas en el anterior ejemplo.

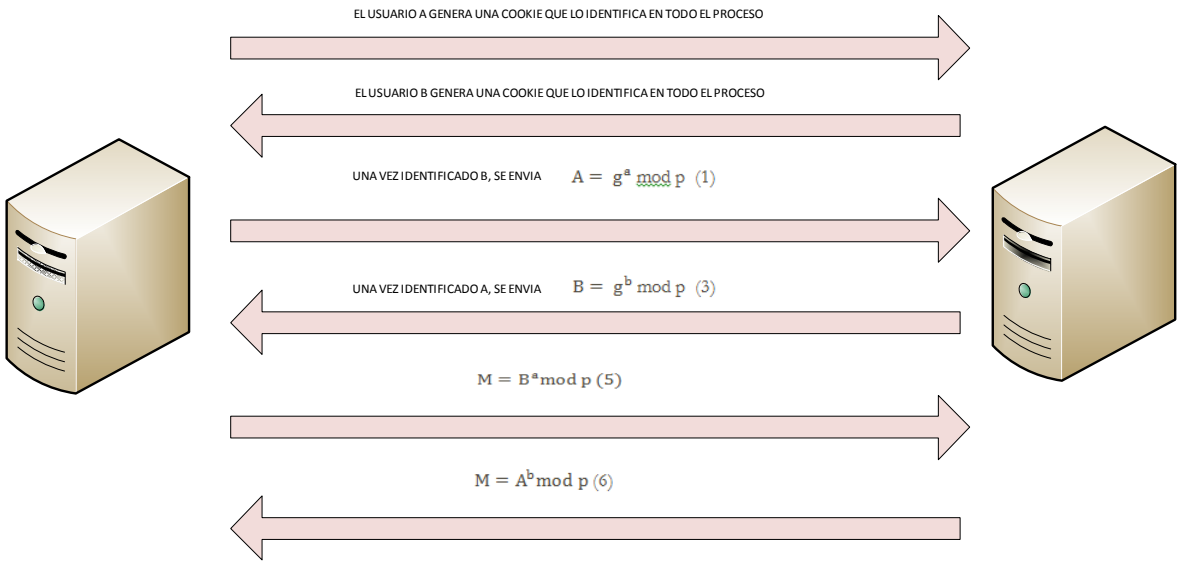


Figura 11: Negociación en modo principal

Por otro lado el modo agresivo dispone solo de 3 mensajes (siendo por lo tanto más rápido) pero a cambio dispone de una vulnerabilidad. Los 2 primeros mensajes negocian los valores públicos para el intercambio Diffie Hellman y las identidades, el segundo mensaje autentica al receptor y el tercero autentica al iniciador.

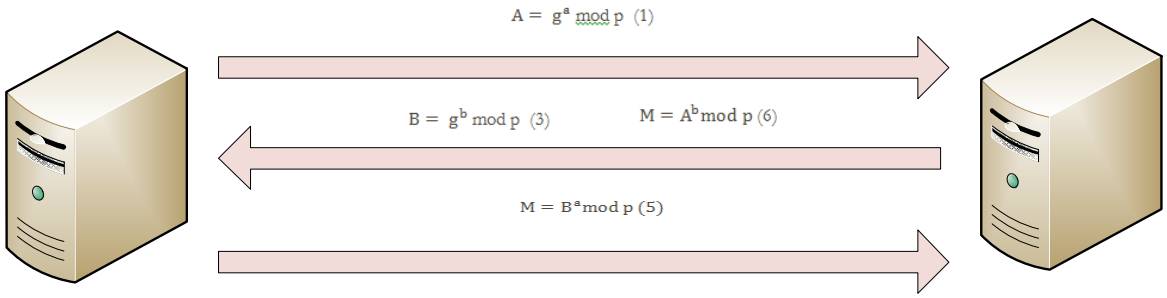


Figura 12: Negociación en modo agresivo

En este último modo, al no existir cookies que identifiquen inicialmente a los usuarios A y B, un atacante puede realizar un ataque man in the middle. Para explicar este tipo de ataques, se hace referencia al anterior ejemplo con el que se explicaba diffie hellman (ecuaciones desde la 1 a la 8). Teníamos un intercambio de claves entre los usuarios A y B. Un atacante llamado C consigue mediante alguna técnica interponerse entre la comunicación de A y B y modificar los paquetes para que se dé la circunstancia de que A <-> C <-> B.

Cuando A envíe g^a mod p (ecuación 1) C interceptará el valor de g^a (base y clave secreta) y lo mismo ocurrirá en la otra dirección con B por lo que el atacante dispondrá de g^b. El atacante C solo tendrá que enviar g^c hacia ambos lados, por lo que acabará conociendo la información entre A y B.

La única manera de evitar esta vulnerabilidad es utilizar la primera fase en modo principal asegurando una autenticación antes de enviar cualquier tipo de claves entre los usuarios A y B.

2 Parte: Es denominada como Quick mode. Su finalidad es negociar un Security Association de propósito general que será utilizada durante toda la conexión.

```
Internet Security Association and Key Management Protocol
  Initiator cookie: 80065213D69A7704
  Responder cookie: 3E3E88969CD7D4EA
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
⊟ Flags: 0x03
    .... ...1 = Encrypted
    .... ..1. = Commit
    .... .0.. = No authentication
  Message ID: 0x00000001
  Length: 236
  Encrypted payload (208 bytes)
```

Figura 13: Captura ISAKMP en su segunda fase o quick mode mediante wireshark

8.3.5 El protocolo ESP

El presente proyecto se enmarca en arquitecturas VPN bajo Windows server 2008 (valiendo para versiones futuras de Microsoft). Esto significa que dicha compañía decidió en su momento aplicar el protocolo ESP y no AH a las tramas generadas a través de IPSec. Es lógico debido a que no tiene sentido aplicar los dos protocolos ya que su finalidad es la misma, implementar cifrado, autenticación e integridad bajo datagramas de protocolo IP.

ESP utiliza la siguiente estructura de tramas:

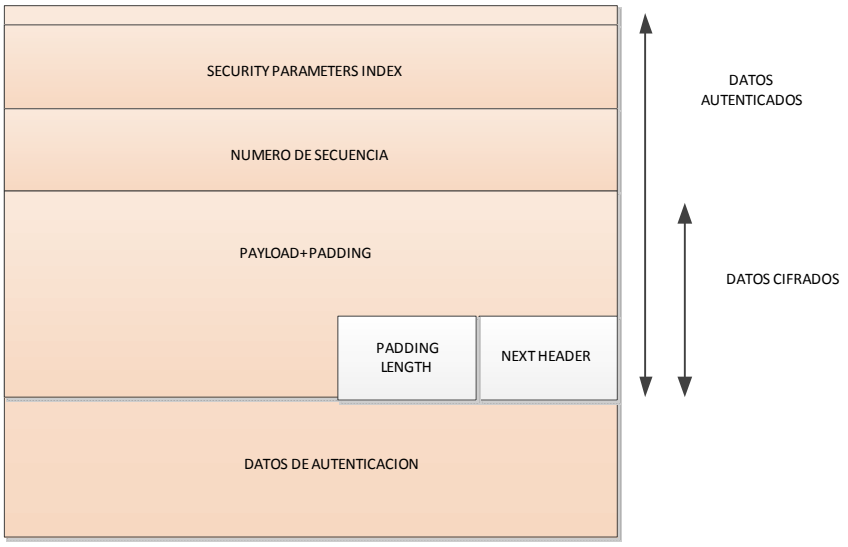


Figura 14: Trama protocolo ESP

El campo SPI sirve para identificar a que SA corresponde la cabecera ESP y el número de secuencia que se utiliza contra repetición de datagramas. Payload contiene los datos del datagrama a enviar y el padding es la definición de bytes adicionales que se pueden enviar (útiles cuando se realiza un cifrado en bloque). Next header indica que protocolos son los datos del datagrama.

El cifrado utilizado por Microsoft es 3DES. En 1970 era muy complicado realizar el cálculo de 2^{56} claves posibles, sin embargo, según evoluciona la **ley de Moore** esta limitación ha sido superada y actualmente podemos obtener una clave DES en cuestión de días. Por este motivo en 1999 se decidió sustituir el algoritmo DES por triple DES. Este protocolo consiste en aplicar 3 veces consecutivas DES (a diferencia de como hacía Microsoft con el protocolo MS-CHAPv2, que concatenaba 3 DES completamente distintos). La longitud total de la clave es de 168 Bits obteniendo una posibilidad de $3{,}74*10^{50}$ claves posibles en lugar de las $7{,}2*10^{16}$que se obtienen con DES.

Mostramos una captura conseguida mediante wireshark:

```
User Datagram Protocol, Src Port: ipsec-nat-t (4500), Dst Port: ipsec-nat-t (4500)
  Source port: ipsec-nat-t (4500)
  Destination port: ipsec-nat-t (4500)
  Length: 156
⊟ Checksum: 0x0000 (none)
    Good Checksum: False
    Bad Checksum: False
UDP Encapsulation of IPsec Packets
Encapsulating Security Payload
  ESP SPI: 0xb0e2fe09
  ESP Sequence: 1
```

Figura 15: Captura de trama ESP mediante wireshark

Finalmente, se muestra cómo quedaría la trama con encapsulado L2TP y cifrada (y encapsulada) a través de IPsec.

Figura 16: Representación trama L2TP/IPsec

8.4 PPTP VS L2TP/IPsec. Que solución escoger para el proyecto.

Como se ha podido observar, PPTP es una tecnología propietaria de Microsoft mientras que L2TP/IPsec cumple los estándares internacionales impuestos por RFC y otros organismos. Que este último protocolo sea una tecnología abierta es una ventaja ya que al ser usado e implementado por distintos fabricantes en todo el mundo, es más fácil que se realicen estudios de seguridad y que se descubran vulnerabilidades y fallos en el cifrado que puedan ser resueltos en nuevas versiones.

Por otro lado, se ha realizado un análisis en profundidad sobre el protocolo de autenticación que utiliza el cifrado MPPE incluido en PPTP, afianzando que este es vulnerable (siendo esto último reconocido por el propio fabricante). El punto 8.2.2 (Página 16) analiza que MSCHAP-V2 utiliza 3 cifrados DES concatenados realizados con una clave de solo 16 Bits (el NT Hash) por lo que al final tan solo se debe trabajar en superar un DES de 56 bits. En cambio IPsec utiliza un cifrado basado en 3DES por lo que el tamaño de la clave es de 168 bits, siendo computacionalmente mucho más complicado de operar y por lo tanto más seguro.

Además, en cuanto al intercambio diffie hellman, Windows server 2008 sólo permite utilizar la negociación de la fase 1 IKE en modo principal evitando que se disponga de un fallo de configuración que permita a un atacante aplicar un ataque man in the middle.

Por estos motivos tan importantes de seguridad, el proyecto se realizará en base a conexiones L2TP/IPsec.

8.5 Requisitos iniciales para configurar VPN bajo Windows server 2008

A continuación se analizará el estado actual de las redes LAN ubicadas en distintos sitios geográficos y sin comunicación ninguna entre ellas. De esta manera se dispondrá de un punto de partida inicial para comenzar a trabajar en el proyecto:

Empresa BATCH SL: Ubicada en la Zona Franca de Barcelona, dispone de una nave industrial y oficinas que dan soporte a 40 usuarios (para simplificar, esta red LAN dispondrá de 40 host). Dispone también de tres servidores. Uno de ellos ejecuta el rol de Dominio Active Directory de Microsoft bajo tecnología Windows Server 2003, el segundo hace las funciones de servidor de ficheros e impresión (es un servidor recientemente adquirido) y un tercero es utilizado como servidor de correo (Bajo Microsoft Exchange). El proveedor de servicios es el grupo Telefónica y dispone de una infraestructura bajo IP pública y tecnología ADSL simétrica.

Empresa PICO SL: Esta empresa está ubicada en el polígono industrial ALTABIX de Elx. Dispone de una nave de fabricación y unas oficinas que dan empleo a unas 20 personas. No dispone de tecnología basada en Active Directory de Microsoft y tan sólo dispone de un servidor de ficheros y de un router basado en tecnología ADSL proporcionada por Orange. El proveedor ofrece IP pública. La empresa dispone de una web alojada en un data center externo y se está estudiando la posibilidad de alojarla internamente ahorrando costes si se puede ofrecer seguridad perimetral.

Empresa DANDE: Esta compañía dispone de una oficina en Milán donde trabajan 40 personas. La compañía disponía de sus sistemas informáticos, pero éstos han quedado obsoletos por lo que la compañía ha decidido que

almacenará sus documentos en el servidor de Barcelona. Para ello, necesita tener acceso a través de la red telemática. Su proveedor ISP e TIM Telecom, y dispone de una red basada en tecnología DSL de 2 Mbits/s.

Como primer objetivo claro, se debe de conseguir comunicar las redes de Alicante y Barcelona de tal manera que mediante una conexión VPN a través de una red WAN permita que las dos redes LAN puedan trabajar como si de una sola red se tratara.

Los datos tanto de la red Pública como de la red LAN de dichas sedes se expone a continuación:

Red empresa BATCH:

	DISPOSITIVO	RED/CIDR	IP	MASK
ETH0 PUBLICA1	ROUTER	80.20.16.0/16	80.20.16.1	255.255.0.0
ETH1 PRIVADA1	ROUTER	192.168.2.0/24	192.168.2.1	255.255.255.0
ETH0 SERVER1	SERVER VPN	192.168.2.0/24	192.168.2.2	255.255.255.0
ETH1 SERVER1	SERVER VPN	192.168.3.0/24	192.168.3.1	255.255.255.0

Tabla 3: interfaces empresa BATCH

Red empresa PICO:

	DISPOSITIVO	RED/CIDR	IP	MASK
ETH0 PUBLICA2	ROUTER	80.20.45.0/16	80.20.45.1	255.255.0.0
ETH1 PRIVADA2	ROUTER	192.168.6.0/24	192.168.6.1	255.255.255.0
ETH0 SERVER2	SERVER VPN	192.168.6.0/24	192.168.6.2	255.255.255.0
ETH1 SERVER2	SERVER VPN	172.20.11.0/24	172.20.11.3	255.255.255.0

Tabla 4: Interfaces empresa PICO

La finalidad es conseguir un sistema funcional como el que se muestra a continuación:

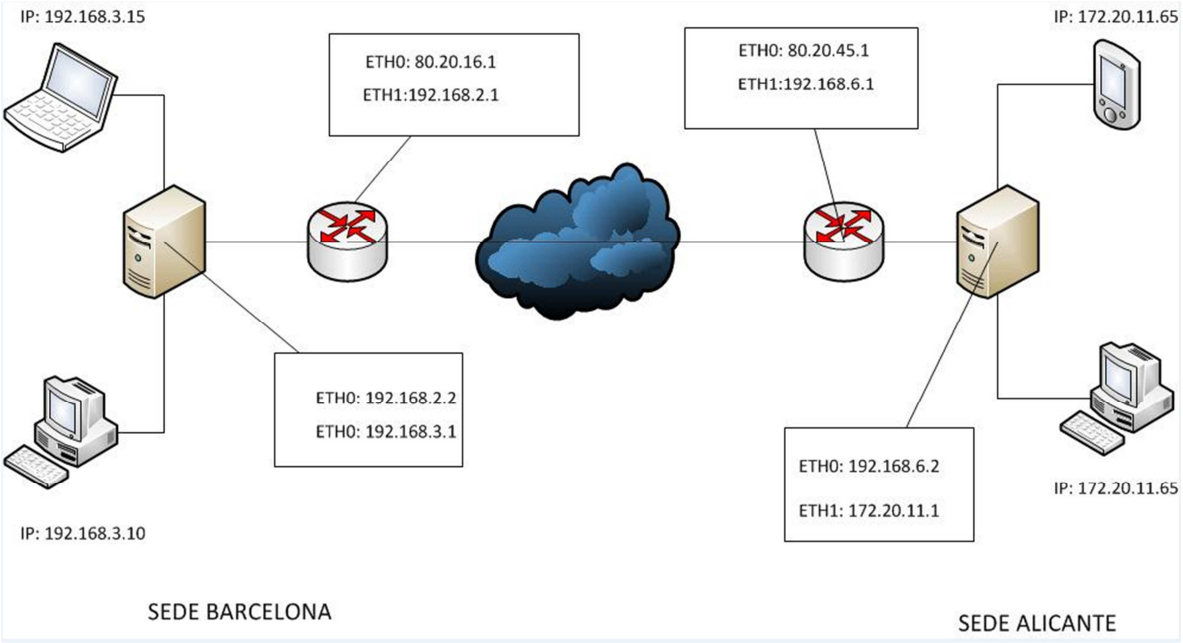


Figura 17: Esquema de conexión sedes Barcelona y Alicante

Como se puede observar, todos los host de la red de LAN 192.168.3.0/24 ubicada en Barcelona tienen configurada la puerta de enlace 192.168.3.1, que es la interfaz ETH1 del servidor VPN ubicado en el mismo site. A su vez, este dispone de la capacidad de encaminar el tráfico al enrutador con salida a internet (red pública 80.20.16.1) a través de la interfaz ETH0 con la IP 192.168.2.2.

El site de Alicante dispone de la misma característica. Una red LAN 172.20.11.0/24 con una puerta de enlace ubicada en la interfaz ETH1 de un servidor VPN. Este a su vez es capaz de encaminar tráfico si es necesario por su interfaz ETH0 res 192.168.6.0/24 hacia un encaminador con salida a Internet.

8.6 Entorno de test bajo VirtualBox.

Una de las premisas de este proyecto, es realizar un entorno de test lo más cercano posible a la realidad. Una razón de peso por la cual se seleccionó Windows server 2008 es su facilidad a la hora de virtualizarlo como si de un servidor físico se tratara. Los actuales entornos de hipervisor permiten simular entornos de red y sistemas operativos idénticos a los sistemas que podemos encontrarnos en producción.

El hipervisor elegido para simular los distintos escenarios de este proyecto se ha seleccionado en virtud de las posibilidades económicas y técnicas de las que se disponía. En el caso que nos ocupa se optó por virtualBox por pertenecer al software freeware, así como por dar una ventaja para las simulaciones que no nos ofrecen otros hipervisores, el modo promiscuo de tarjeta de red. Este modo aprovecha que la información en la capa de enlace (capa 2) se transmite utilizando la dirección MAC del que envía la trama y quien la recibe. Cuando una tarjeta de red está en modo promiscuo no desecha las tramas que tienen como dirección destino otras MAC. Si el paquete circula por un nodo compartido, una tarjeta MAC capturará su tráfico.

Los servidores VPN dispondrán de 2 tarjetas de red. Estas tarjetas serán configuradas como modo interno (entre máquinas virtuales) en distintas redes. Cada red en modo interno verá los host que se asocien con esta red y serán segregados de todas las otras redes. En este proyecto se usará una red interna llamada EXTERNA que simulará la red pública y que estará configurada en los dos servidores VPN, pudiéndose comunicar entre ellas. También se dispondrá de dos redes internas llamadas BCN e ALC. Estas redes internas simularán las conexiones entre host de las oficinas y el enrutador.

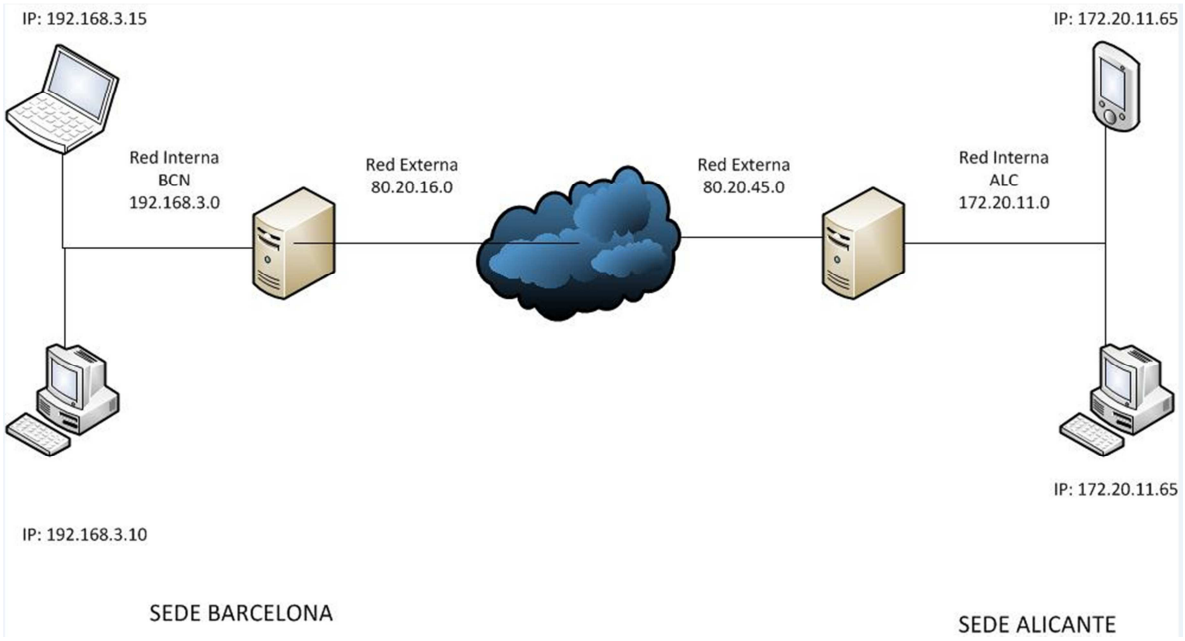


Figura 18: Esquema de conexión sedes Barcelona y Alicante simplificado

Es importante prestar atención en que en este diagrama desaparecen los routers anteriores a los servidores VPN. Esto realmente se hace debido a que no es posible simular dichos dispositivos en VirtualBox, sin embargo son elementos no necesarios en la simulación ya que su función en la práctica real en cuanto a trafico VPN es la modulación/demodulación de señal ya que todo el enrutamiento el trafico VPN recae en los servidores VPN.

8.7 Configuración Servidor Windows server 2008 como enrutador (role routing and remote acces)

Una vez instalados los sistemas operativos en los respectivos servidores se debe de comenzar por instalar el rol "routing and remote access en los distintos servidores VPN de las oficinas a conectar mediante site-to-site.

Un rol en Windows server 2008 es la manera que Microsoft tiene de denominar un tipo específico de infraestructura a implementar en un servidor. Anteriormente esta denominación (Versiones Windows server 2000 y 2003) no recibía esta nomenclatura. Microsoft ha decidido agrupar todas las posibles capacidades que podían desarrollar sus servidores en un apartado propio.

Iniciamos en nuestra infraestructura de test, el servidor que hará la función de VPN en Barcelona. El autor da por sentado que los lectores conocen el proceso de instalación básica de un sistema Operativo Microsoft Windows en una máquina virtual y se mostrarán imágenes de la máquina virtual ejecutando el sistema operativo ya instalado.

Se debe prestar atención en que el servidor ha sido configurado con dos tarjetas de red, tal y como aparecía en la imagen x. Externa contiene 80.20.16.1 e interna la Ip 192.168.3.1.

El servidor recibe el hostname BCN, tal y como se explica en la tabla del punto 8.6 (página 26)

En el punto 3 **"Customize this server"** se puede seleccionar la opción add roles. Si se pulsa aparecerán las siguientes advertencias:

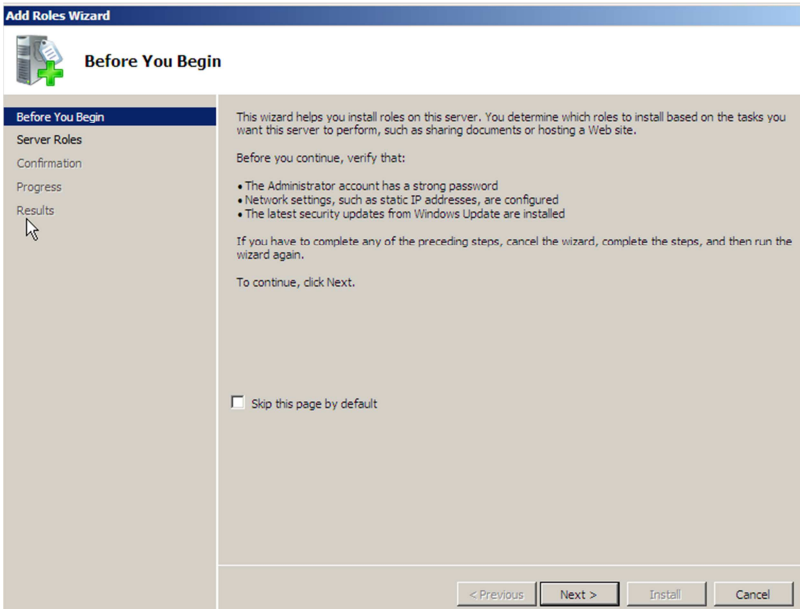


Figura 19: Inicio de instalación de un role en Windows server 2008

Se informa que antes de continuar instalando un role, se debe seleccionar un password seguro, se debe configurar con IP estática el servidor. Como cumplimos estos pasos pulsamos "Next"

A continuación, una parte fundamental a la hora de instalar un role

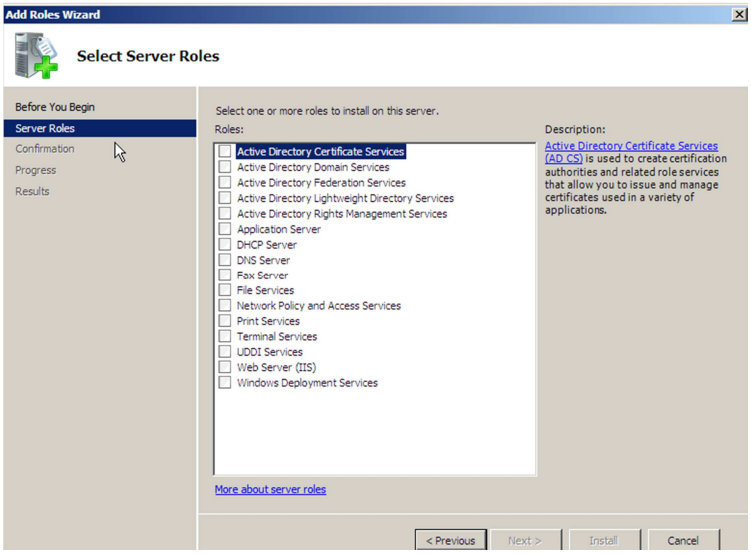


Figura 20: Selección del role a instalar

Como se puede observar, se muestran los 16 roles que puede utilizar Windows server 2008. Desde el famoso Dominio de Active Directory, DNS server o DHCP server hasta el menos conocido Windows deployment services (un rol muy curioso, que si se me permite añadir, he utilizado en otros proyectos como despliegue de imágenes a través del protocolo PXE con gran éxito).

Para conseguir que Windows server funcione como un enrutador se debe marcar la siguiente opción:

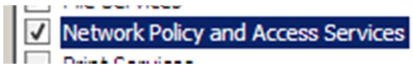


Figura 21: Selección del role Network Policy and Access Services

Marcado el rol, se debe de pulsar "Next", se recibirá la siguiente advertencia:

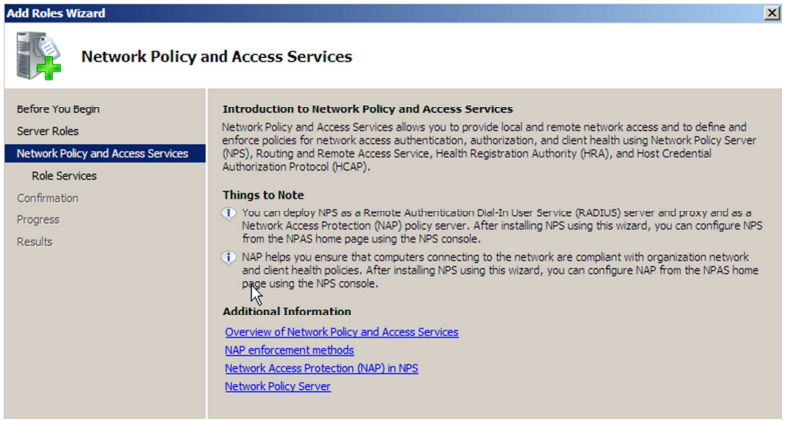


Figura 22: Pantalla de advertencia role Network Policy and Access Services

Pulse next y entonces se deberán seleccionar los servicios que se ejecutarán dentro de este role. Esta parte es muy importante ya que instalar el role "Network policy and Access services" no significa que se obtenga directamente el routing and remote Access. Se debe seleccionar entre los siguientes servicios:

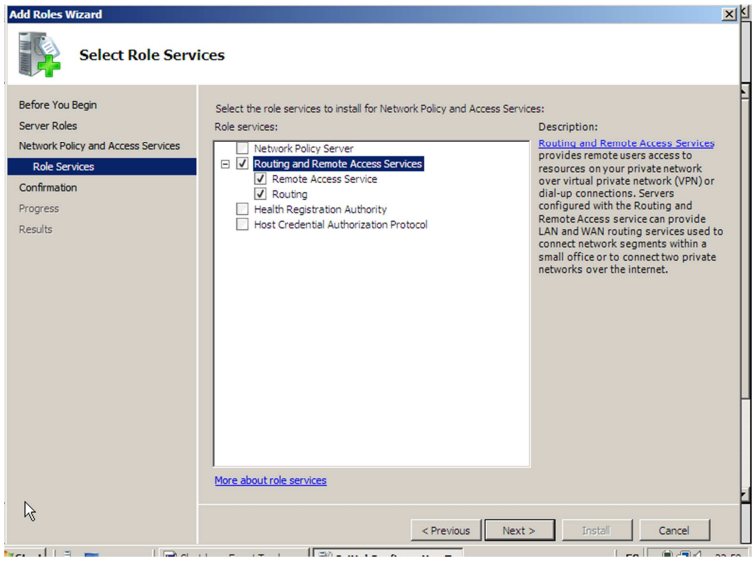


Figura 23: Selección de servicios Route and remote Access

Existen otros servicios asociados a la seguridad de políticas de red que no son necesarios para que este servidor haga de enrutador por lo que no será necesario instalarlos.

Una vez seleccionado se debe pulsar en "Next" y por último pulsar "Install"

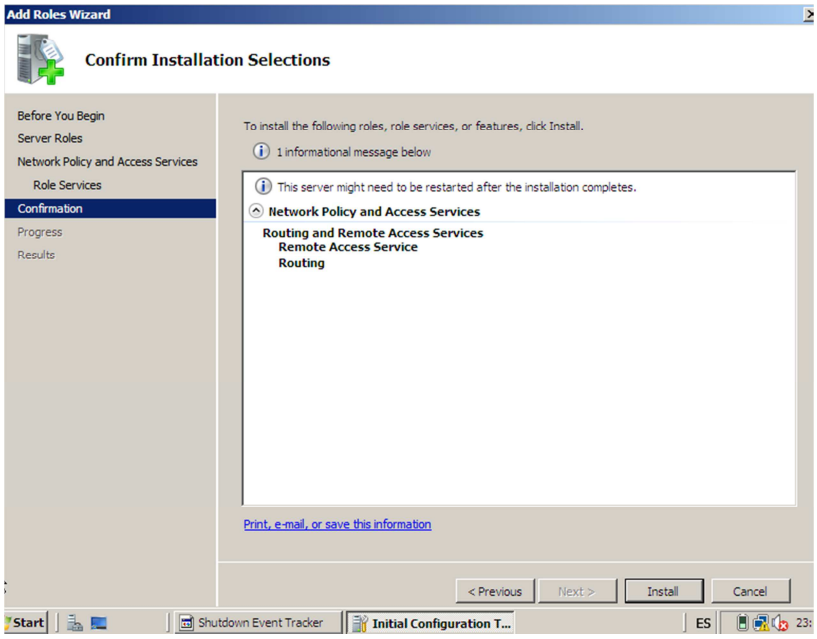


Figura 24: Confirmación de la instalación

Se visualizará que todo ha salido correctamente:

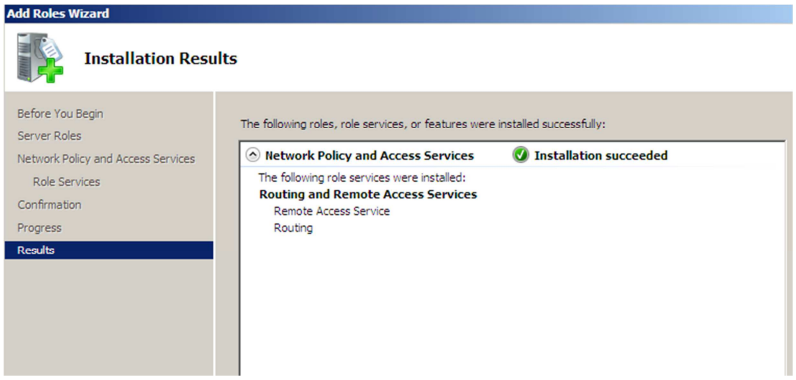


Figura 25: Resultados de la instalación

Se realizará el mismo proceso en el servidor de Alicante dejando los dos servidores con la posibilidad de hacer de enrutadores en sus respectivas redes LAN.

Una vez los dos servidores tengan el rol instalado, se debe acceder al servidor de Barcelona (HOSTNAME: BCN) y pulsar en start → Administrative Tools → Router and remote access

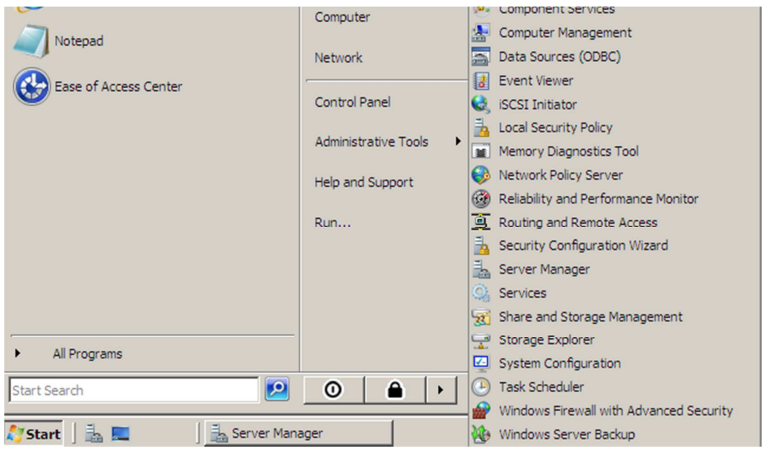


Figura 26: Acceso desde inicio Routing and Remote Access

Se mostrará la siguiente interfaz. Se puede observar un icono de stop en rojo, el servidor todavía no está haciendo las funciones de enrutador:

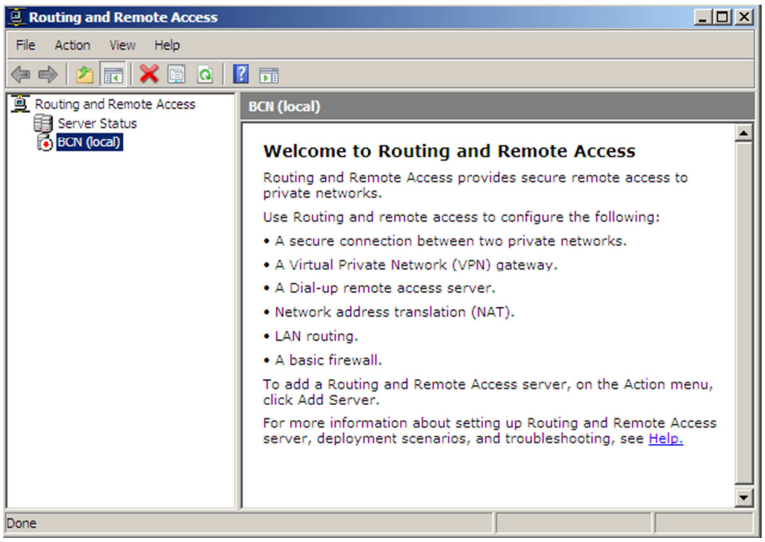


Figura 27: Interfaz general Routing and Remote Access

Se debe pulsar con el botón derecho en BCN(local) y se mostrará un desplegable que permitirá habilitar el servidor como router

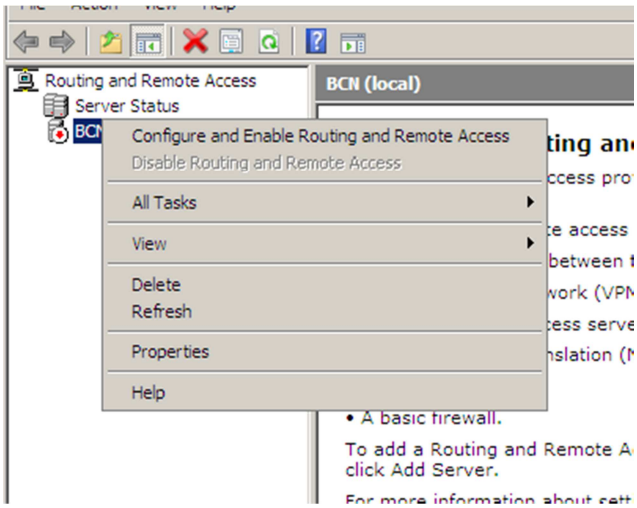


Figura 28: Configuración e inicio del Routing and Remote Access

Aquí viene una de las partes más importantes, como seleccionar la combinación de servicios para el tipo de conexión VPN

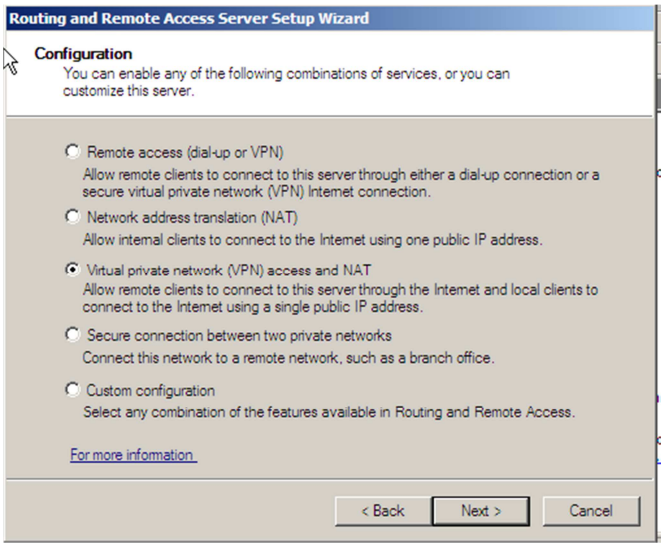


Figura 29: Selección de Red privada Virtual y NAT

Se pueden realizar las siguientes opciones:

- VPN mediante dial-up, es decir, lo que anteriormente se describió como VPN de acceso remoto
- Un servidor NAT que traduzca las direcciones DHCP a las que se da servicios en una misma IP pública de salida para poder comunicarse por la red externa.
- Una red VPN con NAT, imitando el anterior servicio por DHCP y traducción de IP pero dando salida mediante VPN
- Dos conexiones seguras entre redes privadas (sin ofrecer VPN a un rango de equipos, sólo a este terminal)
- Configuración manual.

La mejor opción que se puede seleccionar es la tercera, ya que el futuro servidor VPN hará de servidor DHCP, repartiendo IP's del rango privado a los terminales y encaminándolos para darles salida a través de la red pública mediante un NAT, encapsulando los paquetes.

El autor aprovecha estas líneas para refrescar los conceptos DHCP y NAT.

Un servidor DHCP es aquel que tiene la capacidad de ofrecer a los clientes de una red IP determinada sus parámetros de configuración automáticamente sin necesidad de que un técnico se encargue de dicha configuración. Por otro lado, que este servidor VPN tenga la opción de realizar NAT significa que puede, en tiempo real, convertir las direcciones utilizadas en los paquetes enviados y realizar la conversión inversa, por lo que permite la compatibilidad de redes no compatibles con distinto rango, proporcionando traducción de direcciones IP. Un ejemplo típico de NAT es permitir utilizar direcciones privadas para acceder a Internet. Otro ejemplo clásico es el servidor web alojado en una red LAN interna. Para que los usuarios accedan desde la red pública, se realiza un NAT (PREROUTING) que traduce la dirección pública de dicha red en una dirección privada + puerto, permitiendo el acceso a dicha WEB desde la WAN.

Realizado el paréntesis para explicar estos conceptos, volvamos a nuestra práctica seleccionando la tarjeta que nos dará salida a Internet.

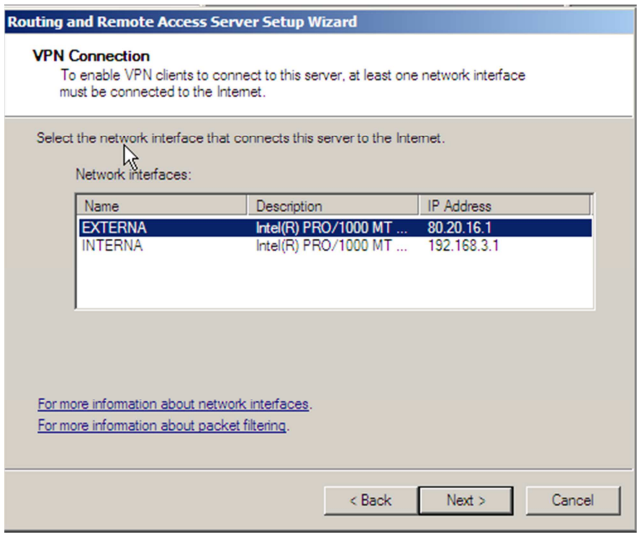


Figura 30: Selección de la dirección IP con salida a Internet

Se debe seleccionar si al ofrecer DHCP se realiza en modo automático o mediante un rango pre-seleccionado por el administrador. En este caso, al ser un test no es necesario reservar rangos para Ip's o denegar rangos para IP's estáticas por lo que el autor ha seleccionado el modo automático.

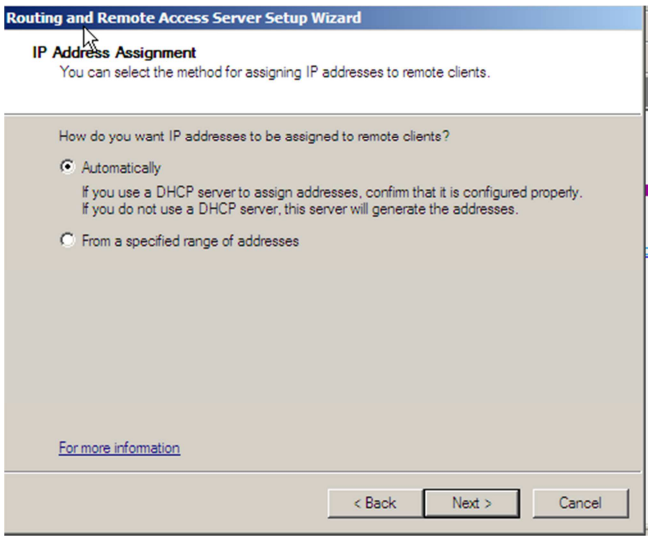


Figura 31: Selección del servicio DHCP automático

Se configuran los servicios DHCP y DNS en el mismo servidor (también se permite la opción de utilizar dichos servicios de otro servidor ya operativo en un mismo segmento de red).

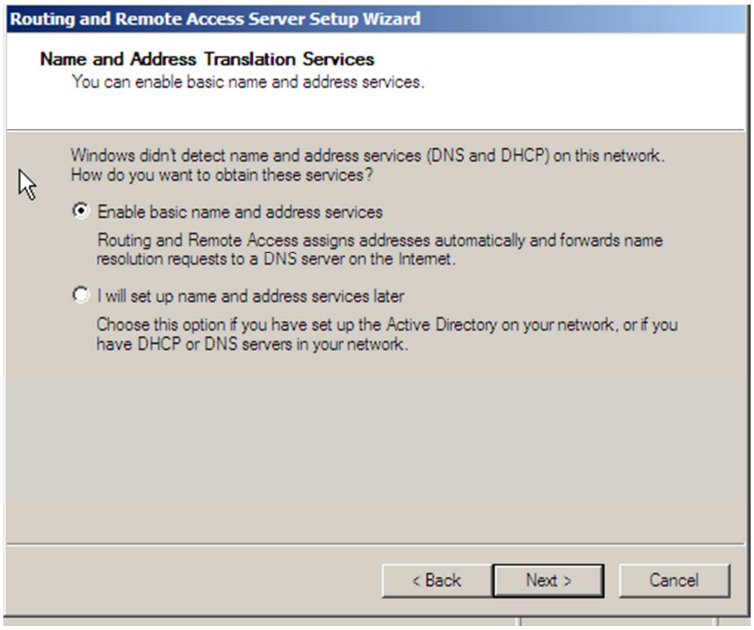


Figura 32: Selección de servicios DNS y DHCP

Se debe pulsar "Next", se recibirá una advertencia de la configuración.

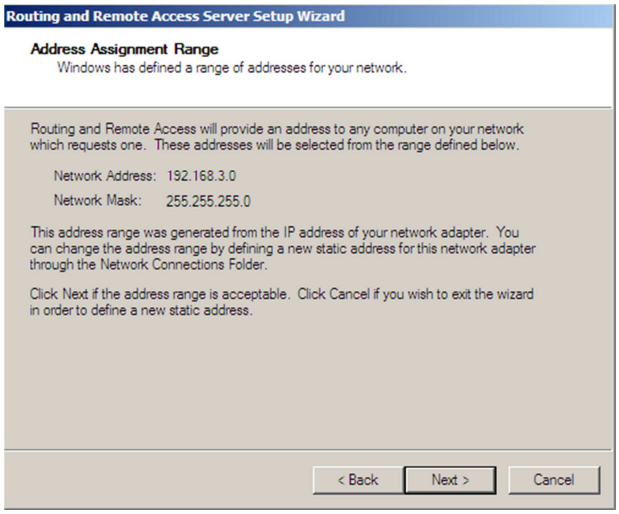


Figura 33: Direccionamiento interno de red ofrecido por servidor RASS

Y por último, el sistema pregunta si se quiere añadir autenticación mediante Radius.

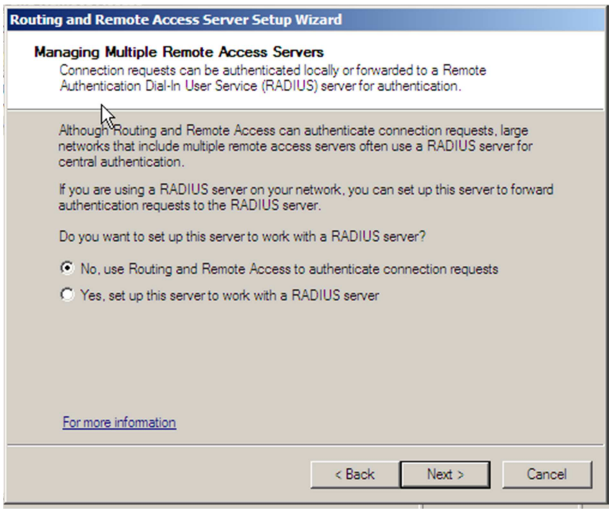


Figura 34: Opción de configuración RADIUS

En el caso del actual proyecto, se marca un No.

Por último, se advierte que debe de configurarse el servicio cliente DHCP de los equipos cliente de nuestra red:

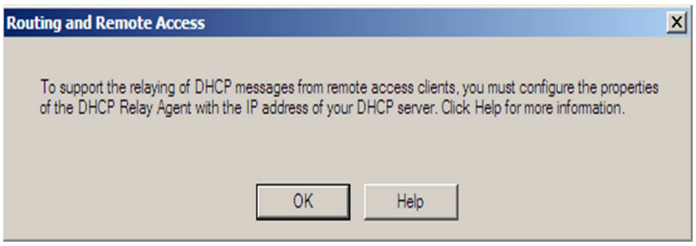


Figura 35: Aviso sobre la configuración DHCP

Si se pulsa Ok, comenzará el despliegue del servicio.

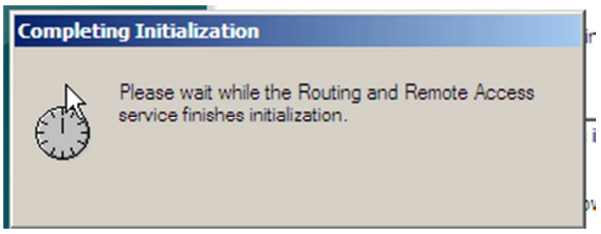


Figura 36: Inicio del servicio Router and remote Access

Y podemos ver como el nuevo servidor ahora está realizando las funciones mostrando un icono en verde y la configuración de todas nuestras interfaces:

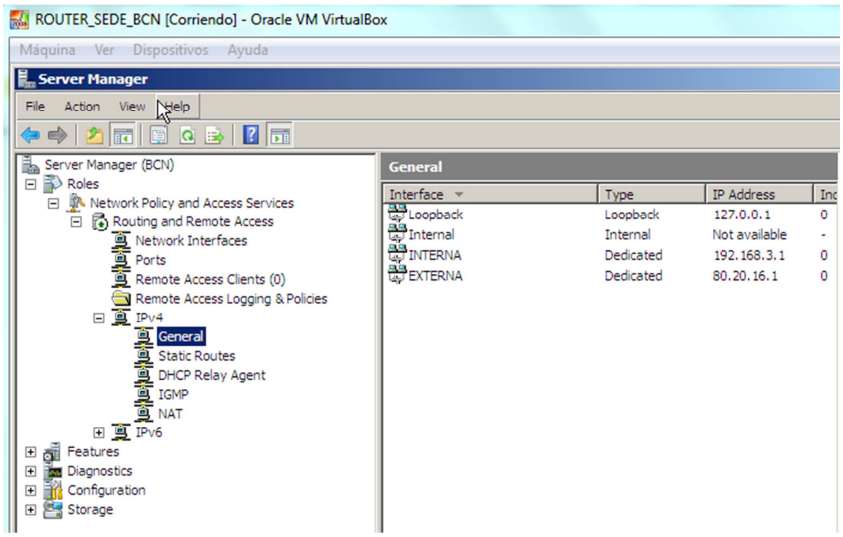


Figura 37: Vista general Route and Remote Access funcionando

Para observar el correcto funcionamiento, se configura un equipo virtual bajo virtualBox mediante Ubuntu conectado a la red interna BCN

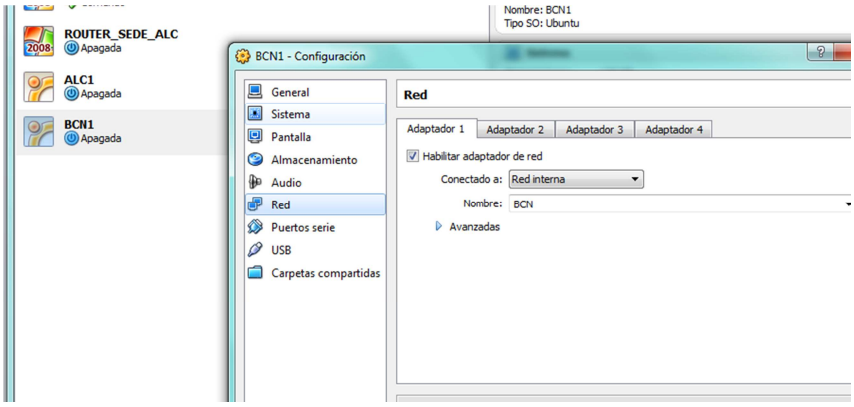


Figura 38: Configuración tarjeta interna en host de Barcelona

Al ejecutarlo, se debe recibir IP en el cliente mediante DHCP del rango 192.168.3.0

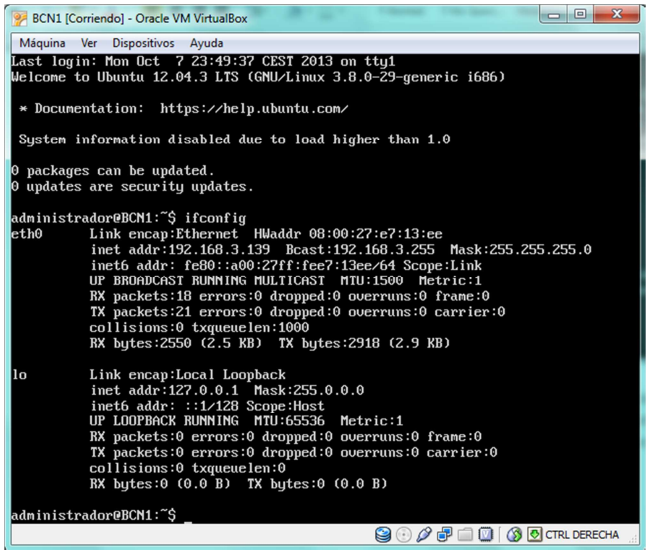


Figura 39: Solución DHCP para equipo cliente

En este caso, se recibe la IP 192.168.3.139, por lo que el servidor de BCN está realizando las funciones de router, NAT y servidor DHCP correctamente. En el caso del servidor de Alicante se realizarán las mismas funciones dando un spool DHCP de 30 host y ofreciendo una IP del rango 172.20.11.0

8.8 Configuración conexión VPN L2TP/IPSEC en Windows server 2008

Se dispondrá de varios clientes en cada sitio y la finalidad será realizar una configuración de estos servidores VPN, para que a través de su conexión IP pública se ofrezca la posibilidad de conectar todos los host como si de una red LAN se tratara sin tener problemas de seguridad al utilizar redes públicas.

Para la correcta configuración se debe de tener "router and remote Access activado en los servidores" tal y como se ha mostrado en el anterior punto junto con la configuración NAT y DHCP en la oficina ofrecida por Windows server 2008.

Desde la consola "Router and remote Access" se debe de pulsar el botón derecho en el icono BCN del servidor que aparece al abrir la aplicación y pulsar en la pestaña Security.

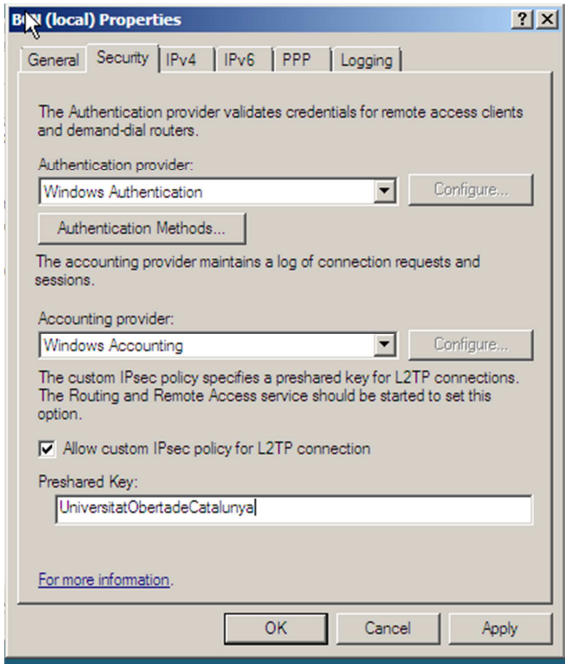


Figura 40: Configuración de la clave PSK en servidor Barcelona

Se debe marcar **"Allow custom IPsec policy for L2TP connection",** esta será la clave PSK que se utilizará como segura entre los dos canales. Se debe recordar que este tipo de claves pertenecen a la criptografía simétrica.

El autor ha decidido utilizar una clave de varios dígitos: **"UniversitatObertadeCatalunya"**

Una vez pulsado apply y OK, se pedirá reiniciar el role router and remote Access para que las políticas relacionadas con IPSEC funcionen correctamente.

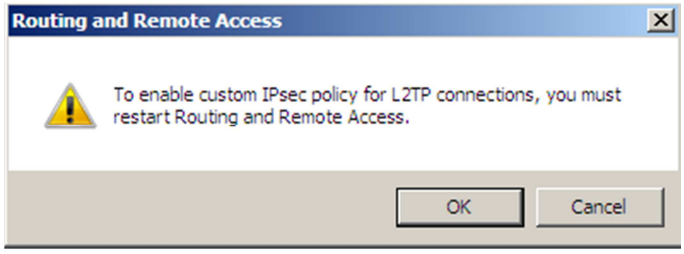


Figura 41: Aviso de reinicio para aplicar la clave

Una vez reiniciado el role, el técnico debe de asegurarse que el protocolo PPTP no interfiere en las comunicaciones, por lo que se debe de deshabilitar de las opciones de los puertos de la siguiente manera:

Pulsar en BCN → Ports (botón derecho) → Propieties

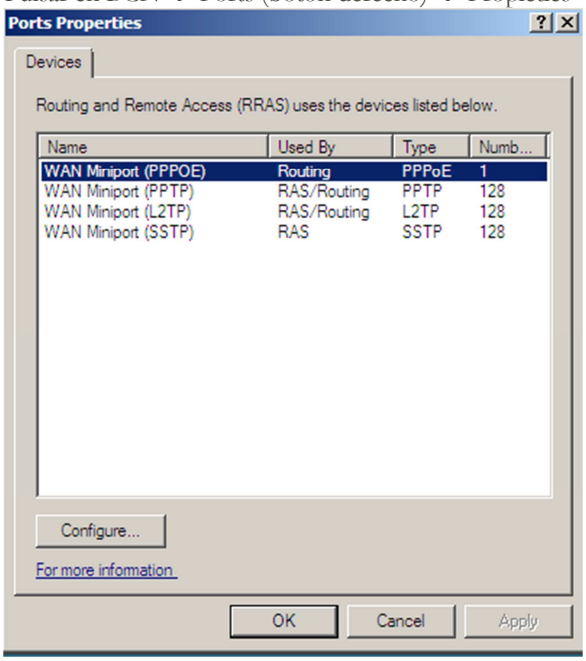


Figura 42: Selección de las propiedades de los puertos para conexión VPN

Se debe seleccionar WAN miniport (PPTP) y desmarcar "Remote Access conection" y "Demand-dial routing connections". De esta manera se evitará que los clientes puedan conectarse por VPN contra este servidor remotamente mediante el protocolo PPTP.

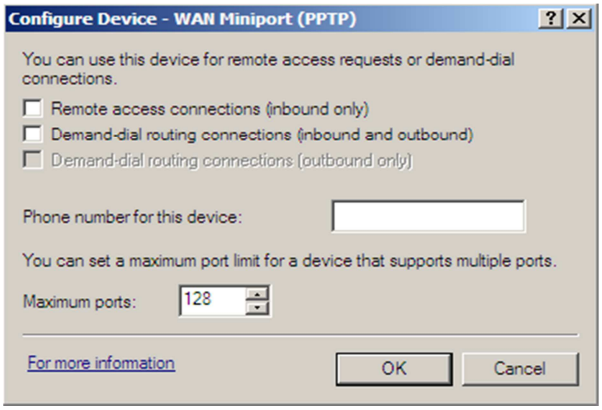


Figura 43: selección para habilitar/deshabilitar PPTP

Una vez finalizada la operación, debemos de configurar una conexión de marcado bajo protocolo L2TP.

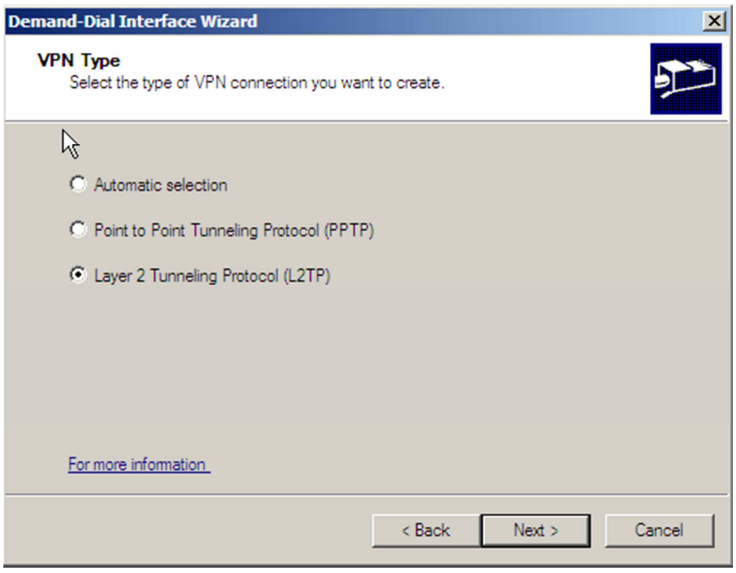


Figura 44: Selección del protocolo L2TP

Se debe de introducir la IP externa.

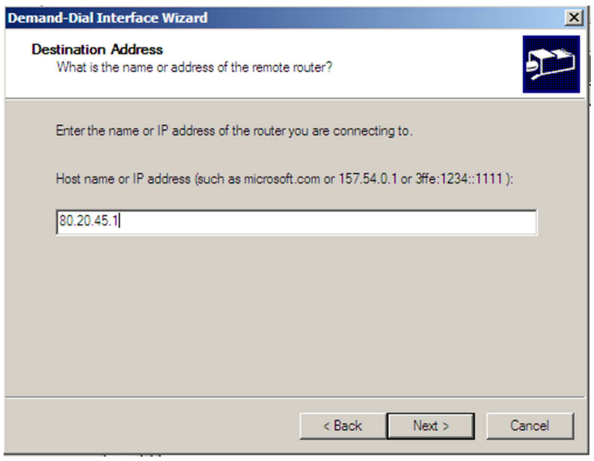


Figura 45: Dirección IP de la dirección pública del Gateway de Alicante

Ahora, es muy importante configurar las opciones que aparecen en la imagen:

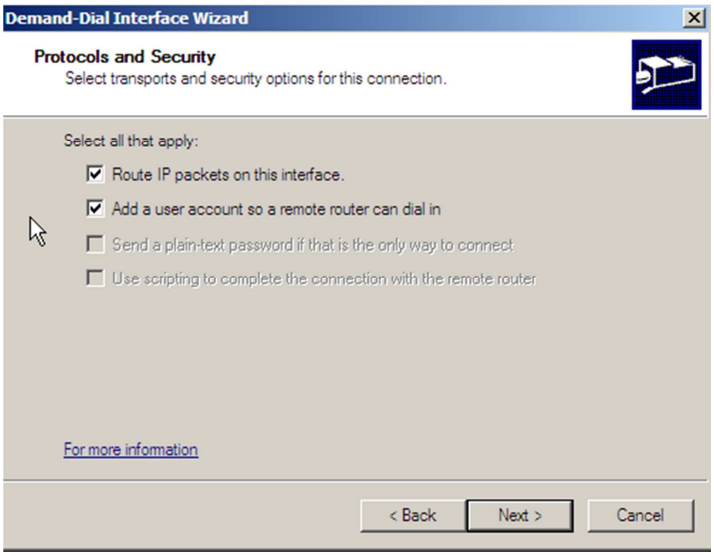


Figura 46: Selección de la seguridad y enrutamiento de paquetes

Se debe añadir un usuario local en el servidor VPN de Alicante que permita aplicar autenticación en el túnel VPN.

Se pulsará Next, y a continuación se pedirá configurar una ruta estática para las redes LAN remotas, en este caso es la red LAN de Alicante 172.20.11.0

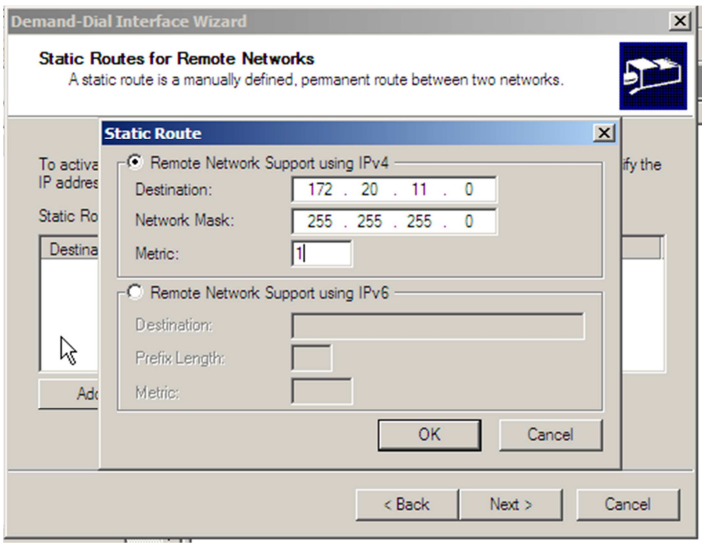


Figura 47: Selección del segmento de red privada remota con la que nos comunicaremos

Ahora se debe de introducir el usuario que utilizará el site de Alicante para mantener la conexión con el servidor de Barcelona. (ALICANTE → BARCELONA) Para todos estos procesos es necesario disponer de privilegios de administrador en los dos servidores.

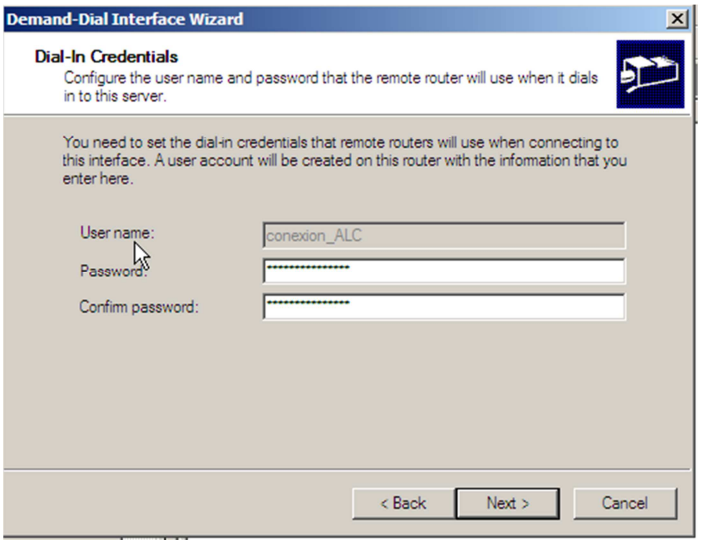


Figura 48: Credenciales para el servidor de Alicante

Se debe pulsar Next, aparecerá la siguiente pantalla. En ella, se configurará el usuario que tendrá privilegios para acceder al servidor de Alicante desde el servidor de Barcelona y mantendrá la comunicación Feed back (ALICANTE ←BARCELONA)

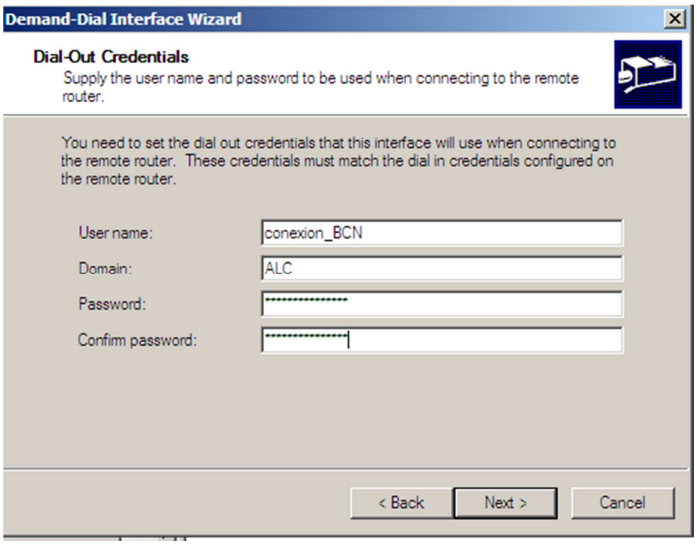


Figura 49: Credenciales servidor Barcelona

Una vez se pulse NEXT → FINISH, se generará una conexión nueva llamada conexión ALC.

Una vez configurada la conexión, se pulsará en ella con el botón derecho y se marcará en propiedades.

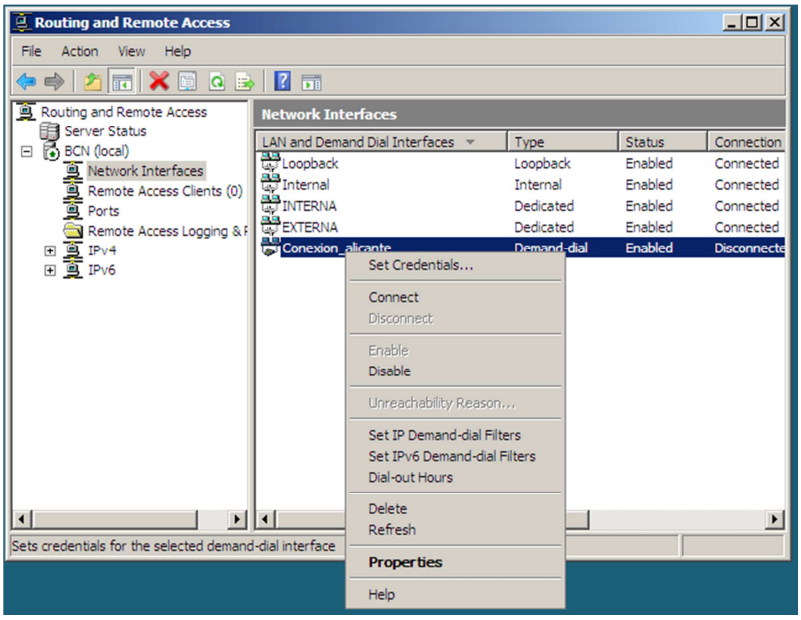


Figura 50: Inicio de la conexión de Barcelona-Alicante

Se pulsará la pestaña Networking

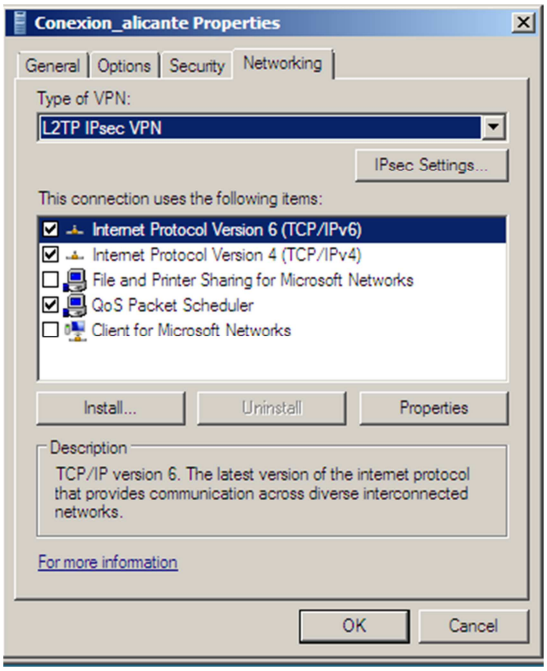


Figura 51: Configuración básica IPsec

Se procederá a configurar la encriptación bajo IPsec.

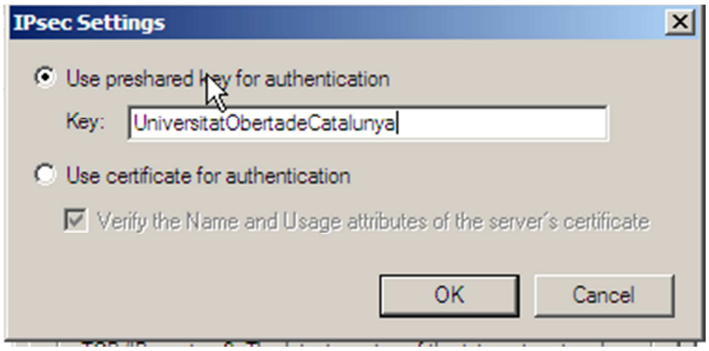


Figura 52: PSK a utilizar con el protocolo IPsec

Como se puede observar, se debe marcar PSK para la conexión remota e introducir la clave descrita en la figura 38 (página 37). La configuración de IPsec permite utilizar PSK simétrico o certificado PKI. Los certificados PKI necesitan del role de Active Directory activado junto con el rol de certification services. Este sistema es más seguro al utilizar el concepto PKI, pero por el contrario necesitan de un sistema Active directory diseñado e implementado, excediéndose de los límites a los que llega el presente documento (se necesitarían otro proyecto distinto para esta implementación). Si se dispusiera de un entorno corporativo con más de 1000 usuarios y diversos sites es posible que se debiera de estudiar dicha implementación.

Una vez configurado el servidor de Barcelona, se debe de configurar de la misma manera el servidor de Alicante.

Realizados estos pasos, se comprobará que nuestra configuración VPN funciona correctamente entre sites.

Se inicia un host con Ubuntu server recibiendo DHCP en el sitio de Barcelona y se observa que la IP asignada es correcta estando en el rango 192.168.3.0

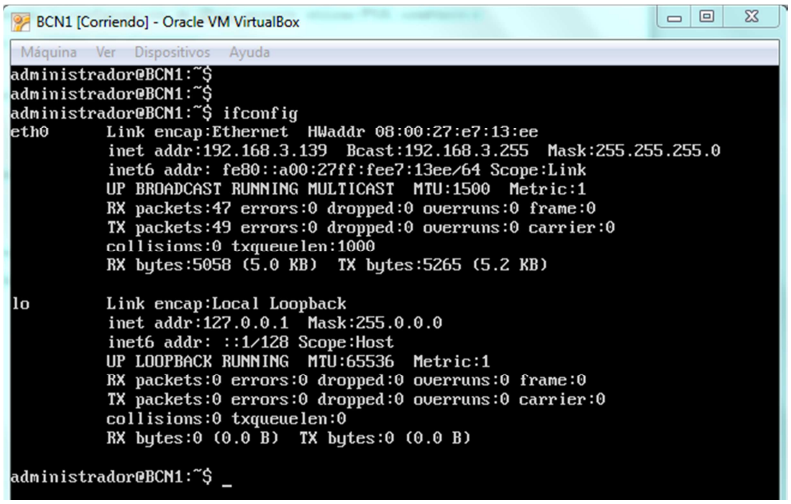


Figura 53: Equipo Linux recibiendo DHCP en la sede de Barcelona

Se comprueba que se puede realizar ping a una IP del rango 172.20.11.0 ubicado en Alicante

```
administrador@BCN1:~$
administrador@BCN1:~$
administrador@BCN1:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e7:13:ee
          inet addr:192.168.3.139  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee7:13ee/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5058 (5.0 KB)  TX bytes:5265 (5.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

administrador@BCN1:~$ ping 172.20.11.211
PING 172.20.11.211 (172.20.11.211) 56(84) bytes of data.
64 bytes from 172.20.11.211: icmp_req=1 ttl=62 time=2.02 ms
64 bytes from 172.20.11.211: icmp_req=2 ttl=62 time=2.81 ms
64 bytes from 172.20.11.211: icmp_req=3 ttl=62 time=2.66 ms
64 bytes from 172.20.11.211: icmp_req=4 ttl=62 time=1.63 ms
64 bytes from 172.20.11.211: icmp_req=5 ttl=62 time=1.27 ms
64 bytes from 172.20.11.211: icmp_req=6 ttl=62 time=2.21 ms
```

Figura 54: Ping a la sede de Alicante desde Barcelona correcto

Se realiza la misma prueba en sentido contrario, un host de Alicante pueda resolver ping contra el equipo de Barcelona

```
ipconfig: no se encontró la orden
administrador@ALC1:~$ ifconfig
eth0      Link encap:Ethernet  direcciónHW 08:00:27:3d:f0:5e
          Direc. inet:172.20.11.211  Difus.:172.20.11.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe3d:f05e/64 Alcance:Enlace
          ACTIVO DIFUSION FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:129 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:58 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:19485 (19.4 KB)  TX bytes:6651 (6.6 KB)

lo        Link encap:Bucle local
          Direc. inet:127.0.0.1  Másc:255.0.0.0
          Dirección inet6: ::1/128 Alcance:Anfitrión
          ACTIVO BUCLE FUNCIONANDO  MTU:65536  Métrica:1
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:0 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:0
          Bytes RX:0 (0.0 B)  TX bytes:0 (0.0 B)

administrador@ALC1:~$ ping 192.168.3.139
PING 192.168.3.139 (192.168.3.139) 56(84) bytes of data.
64 bytes from 192.168.3.139: icmp_req=1 ttl=62 time=2.59 ms
64 bytes from 192.168.3.139: icmp_req=2 ttl=62 time=1.21 ms
64 bytes from 192.168.3.139: icmp_req=3 ttl=62 time=1.30 ms
64 bytes from 192.168.3.139: icmp_req=4 ttl=62 time=1.24 ms
64 bytes from 192.168.3.139: icmp_req=5 ttl=62 time=2.27 ms
64 bytes from 192.168.3.139: icmp_req=6 ttl=62 time=1.16 ms
64 bytes from 192.168.3.139: icmp_req=7 ttl=62 time=1.35 ms
```

Figura 55: Ping desde Alicante a la sede de Barcelona correcto

9. Diseño de la red VPN con 3 sites

9.1 Topología de redes

En este apartado se diseñará la topología de red necesaria para que los 3 sites se puedan comunicar como si de una misma red LAN se tratara sin perder seguridad ni eficiencia. Se define topología de red como la disposición física en la que se conecta una red de terminales o Host. Las topologías más comunes se definen a continuación:

9.1.1 Red Punto a punto: Es un enlace permanente entre dos puntos separados geográficamente (de ahí nace el concepto de point to point tunneling). El valor de una red punto a punto a demandar es proporcional al número de pares posibles de abonados según la ley de Metcalfe.

Dicha ley dice que el número de enlaces aumenta proporcionalmente al número de usuarios del sistema al cuadrado. Sin embargo, debido a que un usuario no puede conectarse a sí mismo, debe de haber una corrección para no exagerar el resultado reduciendo el cálculo al número de aristas de un grafo completo de n vértices. Matemáticamente se expresa como:

$$\frac{n * (n-1)}{2}$$

Donde n es el número de vértices (en nuestro caso sedes).

9.1.2 Red en anillo: Cada estación de una red en anillo dispone de un interfaz de entrada y otro de salida pasando la señal a la siguiente estación. La comunicación se da por el paso de un testigo evitando pérdidas de comunicación debido a colisiones. El grave problema de estas redes es que el concepto es parecido al de un circuito electrónico en serie, si una estación falla, las restantes quedan incomunicadas.

9.1.3 Red en Estrella: Todos los host están conectados directamente a un punto central y todas las comunicaciones se realizan a través de dicho punto. La ventaja es que si un nodo queda inoperativo, los demás no son afectados (siempre y cuando no sea el nodo central el afectado). Que del nodo central o activo dependan todas las comunicaciones es lo que se denomina en el ámbito de IT un SPOF (Singel point of failure). Cuando se genera un SPOF se deben de buscar soluciones de redundancia que impidan que dicho SPOF genere un fallo que afecte a todas las comunicaciones o servicio.

9.1.4 Red en forma de malla: Es una topología en la que todos los nodos están conectados entre sí, es decir, que cada nodo está conectado a todos los otros nodos, pudiéndose llevar los mensajes por distintos caminos, dándose la ventaja de no poder existir ningún corte en las comunicaciones. La única desventaja que poseen las redes en malla es que su precio suele aumentar.

9.2 Estudio de la topología adecuada a nuestro proyecto

9.2.1 Análisis desarrollo redes estrella vs malla

Una vez vista las topologías más utilizadas en el área de redes, se debe seleccionar la que ofrezca mayores ventajas a implementar en la red de trabajo. La empresa que se forme de la unión de las tres zapateras necesitará la mayor fiabilidad posible, evitando que las tres sedes se queden incomunicadas entre ellas o sin conexión sin incrementar el coste excesivamente.

Partiendo de esta base, se descarta realizar una red en anillo, por lo que la infraestructura dispondrá de una conexión o bien en forma de estrella o bien en forma de malla. Si se opta por la primera, se debe de entender que todos los centros conectarán directamente con un punto central. La ubicación del punto central debería de ser seleccionada mediante criterios asignados a la velocidad de las redes y la fiabilidad del centro.

Evidentemente si el punto tiene un problema, todas las redes se quedan sin comunicación VPN y por lo tanto se genera un error de alta criticidad.

Para evitar este problema, se puede utilizar una red en malla que unificará todos los vértices de las distintas redes LAN y evitará que un punto de fallo afecte a todas las VPN. Tan sólo se debe de aplicar la ley de Metcalfe para determinar que disponiendo de tres sedes, el número de enlaces debe de ser de 3

$$\frac{n * (n-1)}{2} = \frac{3 * (3-1)}{2} = 3$$

El diagrama a implementar sería el siguiente:

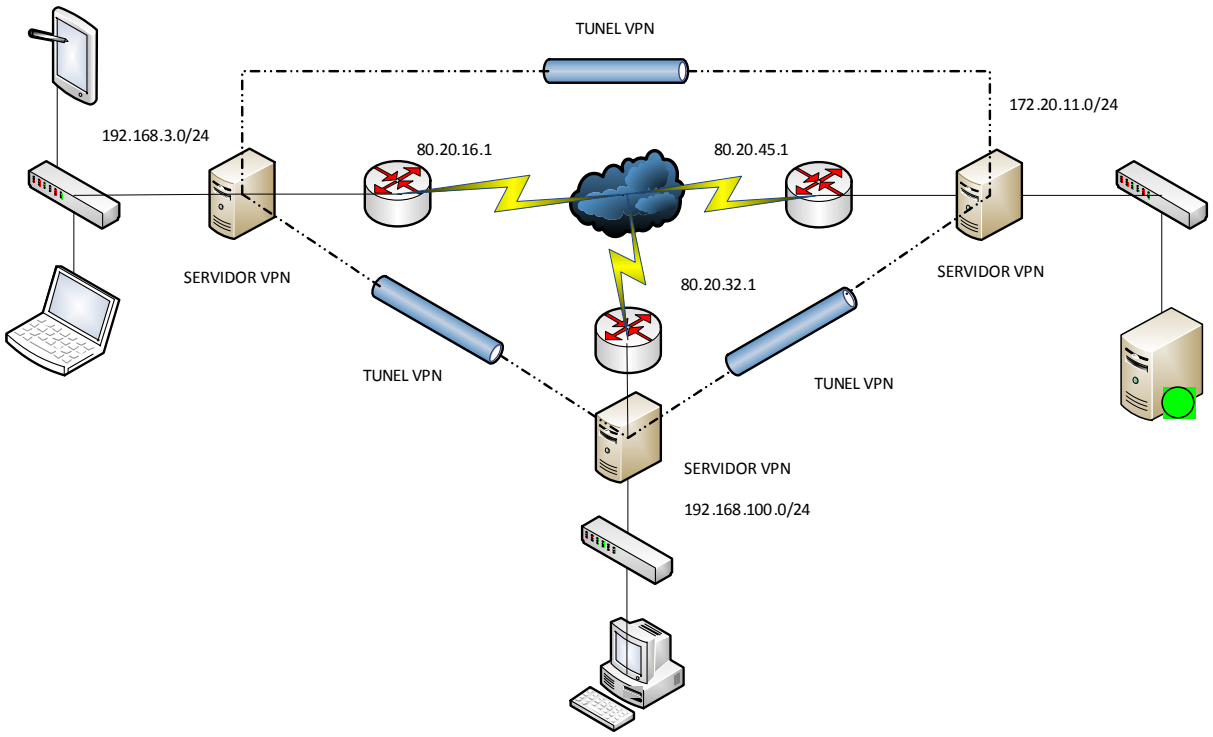


Figura 56: Conexión en malla de los 3 centros

Por lo que claramente se debe de disponer de 2 conexiones de marcado por cada servidor que nos permitirían conectar cada red LAN del centro con las otras redes LAN. El siguiente cuadro muestra las conexiones que debemos de generar:

	CONEXIÓN	CONEXIÓN
SERVIDOR BARCELONA	PPP ALICANTE	PPP MILAN
SERVIDOR ALICANTE	PPP BARCELONA	PPP MILAN
SERVIDOR MILAN	PPP BARCELONA	PPP ALICANTE

Tabla 5: PPP en diversos centros

Aquí se explica en mayor profundidad el esquema de la figura 54 junto con las tablas de direccionamiento IP:

Red empresa BATCH:

	DISPOSITIVO	RED/CIDR	IP	MASK
ETH0 PUBLICA1	ROUTER	80.20.16.0/16	80.20.16.1	255.255.0.0
ETH1 PRIVADA1	ROUTER	192.168.2.0/24	192.168.2.1	255.255.255.0
ETH0 SERVER1	SERVER VPN	192.168.2.0/24	192.168.2.2	255.255.255.0
ETH1 SERVER1	SERVER VPN	192.168.3.0/24	192.168.3.1	255.255.255.0

Tabla 6: Nuevas interfaces empresa BATCH

Red empresa PICO:

	DISPOSITIVO	RED/CIDR	IP	MASK
ETH0 PUBLICA2	ROUTER	80.20.45.0/16	80.20.45.1	255.255.0.0
ETH1 PRIVADA2	ROUTER	192.168.6.0/24	192.168.6.1	255.255.255.0
ETH0 SERVER2	SERVER VPN	192.168.6.0/24	192.168.6.2	255.255.255.0
ETH1 SERVER2	SERVER VPN	172.20.11.0/24	172.20.11.3	255.255.255.0

Tabla 7: Nuevas interfaces empresa PICO

	DISPOSITIVO	RED/CIDR	IP	MASK
ETH0 PUBLICA3	ROUTER	80.20.32.0/16	80.20.32.1	255.255.0.0
ETH1 PRIVADA3	ROUTER	192.168.7.0/24	192.168.7.1	255.255.255.0
ETH0 SERVER3	SERVER VPN	192.168.7.0/24	192.168.7.2	255.255.255.0
ETH1 SERVER3	SERVER VPN	192.168100.0/24	172.168.100.1	255.255.255.0

Tabla 8: Nuevas interfaces empresa DANDE

Cada una de estas tablas muestra una conexión ETH1 SERVER<X> donde X será un número determinado según la empresa que se esté evaluando (como ejemplo el numero 3 hace referencia a la empresa DANTE). Estas tarjetas serán las encargadas de interactuar con los host de cada red LAN y recibir el tráfico para que los servidores VPN lo redireccionen realizando un NAT por la tarjeta ETH0 SERVER<X> que es la encargada de gestionar el tráfico entre el servidor VPN y el router que permitirá una salida a Internet o a otro servidor VPN (y por lo tanto a otro segmento de red LAN ubicado geográficamente separado de la oficina) en función de las necesidades. Como se puede observar, en la tabla se describe el tipo de dispositivo a usar y su configuración IP, máscara de subred y rango junto a CIDR.

10. Rutas en Windows server

10.1 Rutas estáticas en Windows server

Una de los puntos más importantes en el proyecto, es aplicar diversas formas de redundancia para evitar que una red se aísle o desconecte de las demás. Este último punto ha sido solventado aplicando una red en malla, pero, en este tipo de redes cabe la posibilidad de que si falla una de las conexiones PPP, fallaría la conexión VPN desde un centro a otro provocando la caída de comunicaciones.

Analizando la figura 54 (página 46), se observa como el formato de red malla ofrece la posibilidad de que si una conexión lógica falla, sea posible redirigir los paquetes por otra ruta posible. Como se puede observar, la ruta típica para llegar desde Barcelona a Milán podría ser llamada A, sin embargo, si fallara A sería posible redirigir los paquetes por la conexión B:

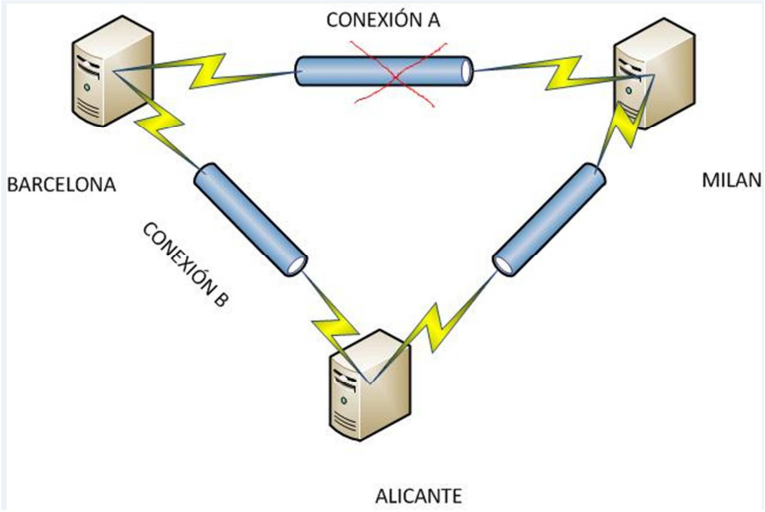


Figura 57: La sede de Alicante Barcelona se comunica con Milán a través de Alicante

Para conseguir este enrutamiento y evitar que uno de los centros quede sin comunicación se dispone la capacidad de realizar rutas estáticas con el comando ROUTE. Este comando permite manipular las tablas de enrutamiento de los servidores, siendo su sintaxis la siguiente:

Route –p ADD <DESTINO> MASK <MASCARA DE RED> <GATEWAY> metric 2

Donde –p indica que la ruta no se borre si se reinicia el sistema y la métrica simplemente es un valor que toman los diferentes protocolos de enrutamiento para poder determinar cuál es la mejor ruta hacia una red de destino

A continuación se presenta un ejemplo práctico:

Inicialmente el servidor de MILAN está configurado con dos conexiones L2TP que permiten conectar la red LAN con las redes de Barcelona y de Alicante mediante VPN. Se observa en la siguiente imagen como los dos túneles están conectados y en rojo, se dispone la captura mediante un route print de las rutas que permiten comunicar dichas redes

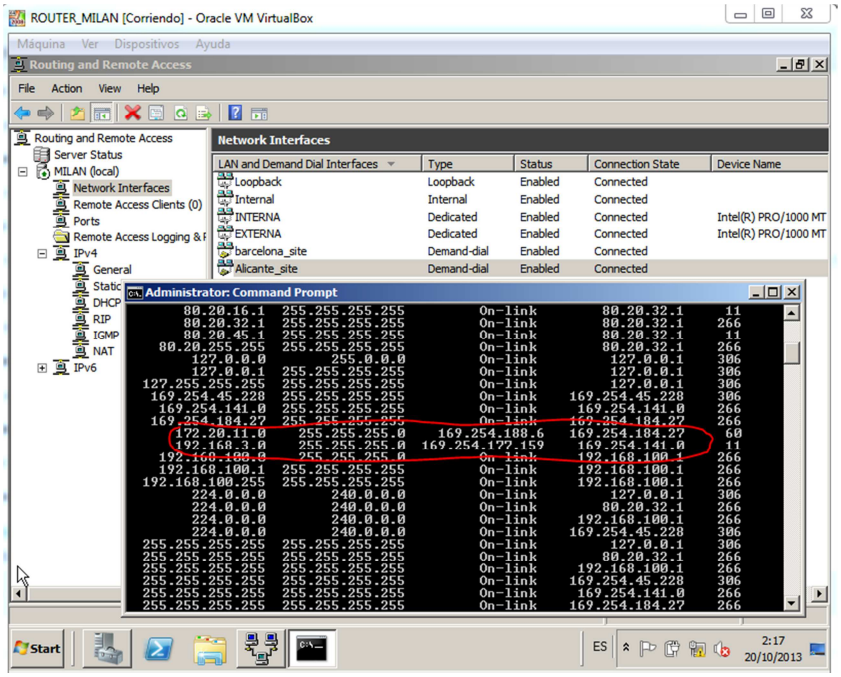


Figura 58: Route Print con una dirección Gateway distinta por cada conexión a un segmento remoto

A continuación se genera una ruta que en lugar de enviar los paquetes dirigidos a la red de Barcelona 192.168.3.0 por le Gateway 169.254.214.159 lo haga por la puerta de enlace 169.254.214.196, que es el PPP inicial para conectar con la red de Alicante.

Ahora, se desconecta la conexión de Barcelona (emulando un fallo lógico en esta conexión de marcado), manteniendo un ping continuo contra dicha sede.

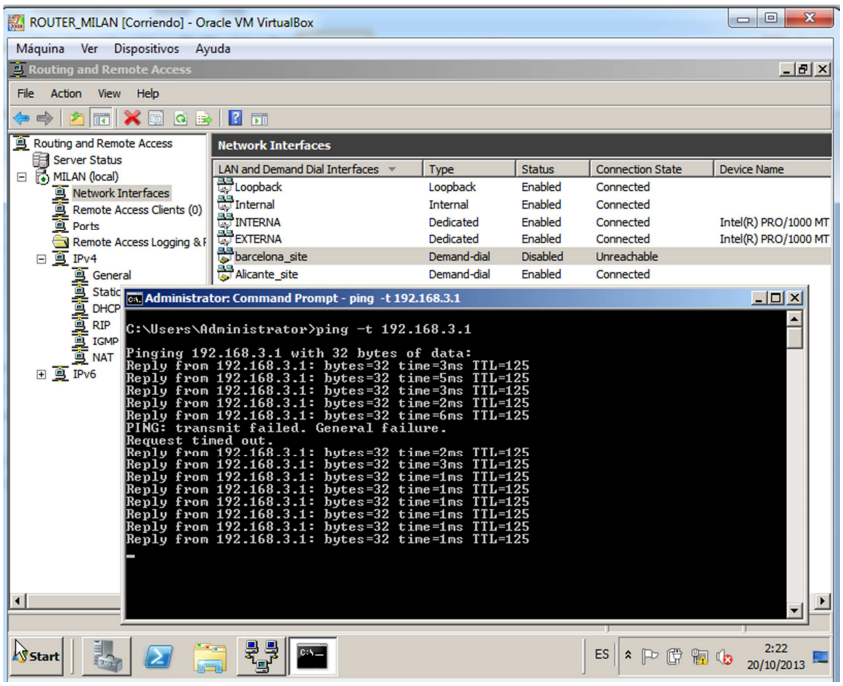


Figura 59: Simulación caída de una conexión PPP junto L2TP y enrutada por otra conexión redundante

A pesar de fallar la conexión, el trafico VPN ha sido redirigido por la conexión VPN generada contra Alicante, ofreciéndose una redundancia en caso de error. Aquí se puede observar una imagen de como varia la ruta obteniendo el mismo Gateway para las conexiones de Barcelona y Alicante. Compárese la figura 56 (página 48) en la que el Gateway PPP aparece en rojo con la IP 169.254.214.159 y como a raíz de la falta de conexión, en la figura 58 es capaz de sustituirlo re-enrutando los paquetes por el Gateway 169.245.188.6 (resaltado en rojo) que inicialmente es el Gateway asignado a los paquetes con destino al servidor de Alicante.

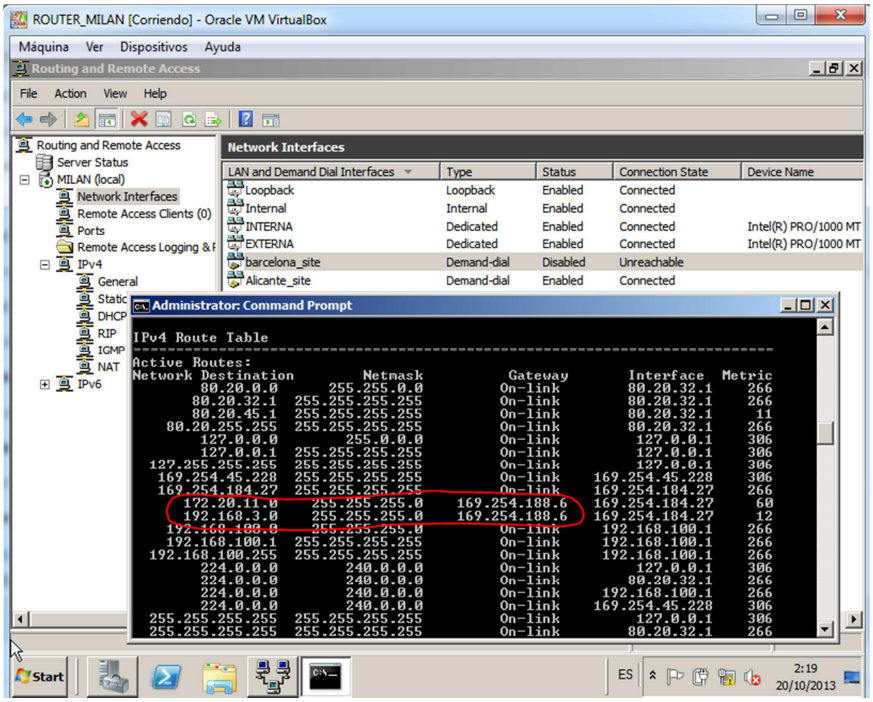


Figura 60: Configuración mismo Gateway para distintas redes remotas.

Como se ha demostrado, el sistema de rutas estáticas ofrece una capacidad de desvío de paquetes en caso de fallo de conexión, ofreciendo la posibilidad de que en caso de que el sistema sea afectado por un error durante el establecimiento inicial de la conexión PPP se puedan re-direccionar los paquetes encapsulándolos mediante protocolo L2TP y cifrándolos con IPsec por otra salida sin perder seguridad y dando el mismo servicio.

11.1 Selección de la tecnología a utilizar

Durante los últimos años, los distintos tipos de ataques informáticos han ascendido notablemente planteando la necesidad de mantener la confidencialidad de la información y obligando a implantar los métodos de seguridad idóneos. En el proyecto que nos ocupa, se dispone de una infraestructura con diferentes accesos a la red pública (uno por servidor VPN), si no se securiza correctamente, cada acceso significa también una puerta de entrada a la red.

Inicialmente, se había planteado la posibilidad de aplicar securización mediante la herramienta de Microsoft Forefront Gateway protection, pero dicho sistema firewall quedó desechado por su elevado precio, necesidad de potencia en cuanto a hardware (ya que era un sistema que securizaba las 7 capas OSI y por lo tanto su consumo era muy elevado) y soporte (Microsoft planea discontinuar su soporte durante el 2014).

Ante esta dificultad se planteó la posibilidad de sustituir dicho producto por el sistema de IPtables integrado en el kernel original de Linux.

Inicialmente esta acción planteaba obtener un nuevo servidor físico por cada sede, un hardware relativamente liviano (ya que Linux es un sistema que funcionando solamente como firewall no necesita grandes recursos) pero que evidentemente involucraba un gasto inicial extra en adquisición de hardware.

A pesar de que esta opción es la más adecuada, existe otra opción que ahorraría dicho coste y que se presenta en este proyecto como una alternativa interesante.

Windows server 2008 incluye el role "Hyper-V". Dicha aplicación es un programa de virtualización basado en un hipervisor para los sistemas de 64-bits con los procesadores basados en AMD-V o Tecnología de virtualización Intel. De esta manera, con este rol, se puede tener instalada una imagen virtual con un Sistema Operativo de la familia Linux que funcionará como puerta de enlace junto con el router. Este servidor ejecuta IPtables y realizará un NAT de entrada y salida con el servidor VPN de Microsoft, alojado en otra máquina virtual en el mismo servidor físico. De esta manera cuando un host perteneciente a un segmento de red determinado quiera comunicarse con otro host de distinta red geográfica, se aplicará un primer NAT por parte del servidor Microsoft insertando las modificaciones para realizar túnel y securización mediante IPsec, a su vez, el servidor virtual en Linux aplicará un segundo NAT, analizando los paquetes mediante IPTable y enrutando a la puerta de enlace dichos paquetes. A partir de ahora, a este concepto le llamaremos NAT transversal.

11.2 Linux IPTables

Esta herramienta viene incorporada en el kernel de Linux y permite el filtrado y monitorización de tráfico TCP/IP. Es una interfaz hacia el módulo netfilter de la serie 2.4 o superior de Linux.

Para comenzar, se debe de estudiar qué modelo de implementación de seguridad se requiere para la instalación de un sistema firewall (en este caso IPtables). Un firewall se puede implementar de dos maneras, aceptando todo el tráfico añadiendo reglas de bloqueo de protocolos y puertos según sea necesario o denegando todo el tráfico y habilitando sólo el que sea necesario. Esta segunda opción es menos costosa de mantener por el administrador de seguridad ya que solo se debe de tener conocimiento de los protocolos y puertos que se utilicen, por otro lado es la medida más segura ya que ante un exploit o ataque mediante un determinado puerto, el comportamiento por defecto es denegar el tráfico. Debido a la criticidad de los servidores VPN de este proyecto, se configurarán todos los firewall en modo denegar.

Una vez seleccionado el modo de implementación, se hace referencia al funcionamiento básico de IPTables. La funcionalidad de esta herramienta incluida en el kernel de Linux es filtrar o modificar paquetes a medida que éstos atraviesan diferentes etapas. Las etapas que es posible encontrar en este proyecto son cinco: INPUT, OUTPUT, FORWARD, POSTROUTING Y PREROUTING. Se incluye el siguiente diagrama de flujo para realizar una explicación más detallada:

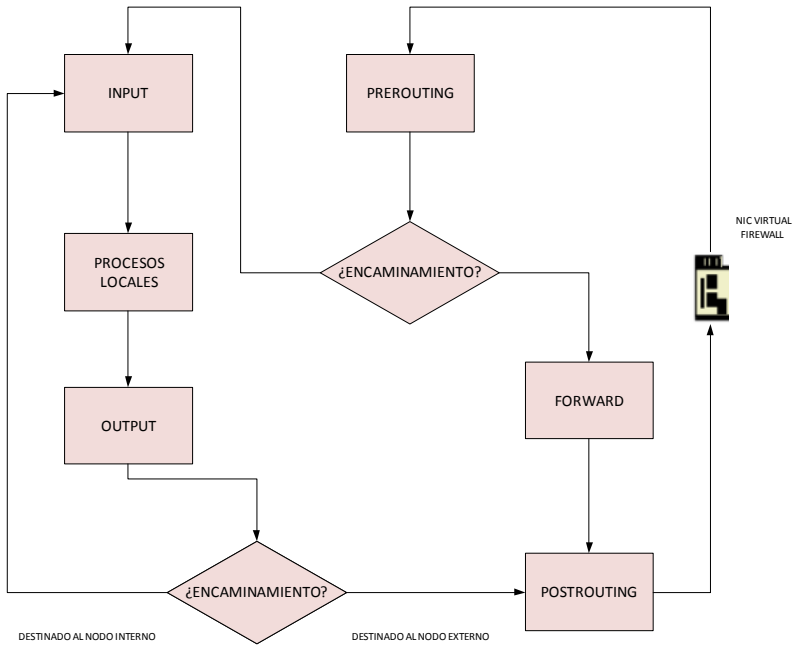


Figura 61: Diagrama de flujo IPTables

Como se puede observar en la anterior imagen, existen 3 etapas de filtrado en el propio host, INPUT que sólo se aplica a los paquetes destinatarios del host local, FORWARD que se aplica a aquellos paquetes con dirección de origen y destino diferentes al host local (encamino, pero no a mismo) y OUTPUT que se aplica a paquetes generados en el host local.

PREROUTING y POSTROUTING son etapas que permiten realizar re-direcciones. En el caso de PREROUTING, se permite redirigir todo el tráfico entrante hacia otro host. Se puede decir que PREROUTING cumple la frase coloquial "todo lo que entre por la interfaz X será re-direccionado a…..)

Por su parte POSTROUTING permite la re-dirección en el tráfico saliente, modificando los paquetes justo antes de devolverlos a la red. Todo lo que salga por la interfaz X será re-direccionado a…

Todas estas etapas tendrán asociadas unas reglas que serán consultadas para conocer qué acción realizar con el paquete. La más común es ACCEPT que permite aceptar los paquetes, DROP que deniega los paquetes, DNAT que irá unido a la etapa PREROUTING y que se puede traducir por destino de NAT y SNAT que puede ser traducido por origen del NAT y que se añade junto a POSTROUTING para modificar el origen de los paquetes.

Por último tenemos el caso de MASQUERADE. Esta regla se utiliza únicamente con la etapa POSTROUTING ya que nos permite re-enviar tráfico en el origen trabajando con un rango de IP's dinámicas que nos ofrece el proveedor ISP.

Con estos principales conceptos más los conocimientos obtenidos sobre sistemas VPN de Microsoft es posible proceder a configurar nuestros Firewalls protegiendo cada red LAN del cliente y permitiendo realizar las conexiones VPN entre redes geográficamente dispersas. La configuración de los diferentes firewalls será ampliamente descrita en el apartado ANEXOS 1. Es importante aclarar al lector que por defecto todas las entradas, salidas y forward de nuestros firewalls estarán denegadas por la orden DROP, y se irán añadiendo sucesivas reglas para abrir lo estrictamente necesario.

11.3 Servidor VPN detrás del Firewall

A la hora de aplicar seguridad a una infraestructura basada en VPN, aparecen con dos alternativas:

11.3.1 Firewall detrás del servidor VPN: Este último servidor se conecta directamente a la puerta de enlace y escapa a la protección ofrecida por el firewall. Se desaconseja utilizar dicho sistema debido a la vulnerabilidad que ofrece ya que no protege la interfaz entre la puerta de enlace y el servidor VPN.

11.3.2 Firewall delante del servidor VPN: El firewall dispone de una interfaz conectada a Internet y otra interfaz conectada al servidor VPN, por lo que el firewall se encontrará entre la puerta de enlace a la red WAN y el servidor VPN, protegiendo a todos los dispositivos de la red LAN.

Para este proyecto se ha seleccionado ubicar los firewall delante del servidor VPN y proteger perimetralmente toda la red. Los puertos necesarios para permitir realizar el túnel bajo L2TP/IPsec son los siguientes:

Protocolo ISAKMP (Puerto 500 UDP): Este protocolo define los pasos necesarios para establecer un SA (security association) dictando las normas para el establecimiento y mantenimiento de todas las claves necesarias para la familia TCP/IP en modo seguro. Es el primer protocolo que se aplica en IPsec.

Protocolo L2TP (Puerto 1701 UDP): Enrutamiento y acceso remoto para L2TP.

Protocolo NAT-Traversal (Puerto 4500 UDP): Es un protocolo fundamental para poder utilizar el firewall delante del servidor VPN ya que se encarga de permitir el NAT trasversal encaminando los paquetes enviados a la interfaz del firewall hacia el servidor VPN y viceversa, haciendo "transparente" la intercesión de los firewalls entre los distintos servidores VPN ubicados geográficamente.

Protocolo ESP (Puerto 50 TCP): protocolo Encapsulated Security Payload (ESP) forma parte de la arquitectura de seguridad del protocolo de Internet (IPSec). ESP proporciona una comprobación de integridad, autenticación y cifrado para los datagramas del protocolo de Internet (IP).

11.4 Escenario y configuración

11.4.1 Esquema de la solución final

A continuación se muestra un diagrama del escenario final del proyecto "Diseño de redes VPN seguras bajo Windows server 2008"

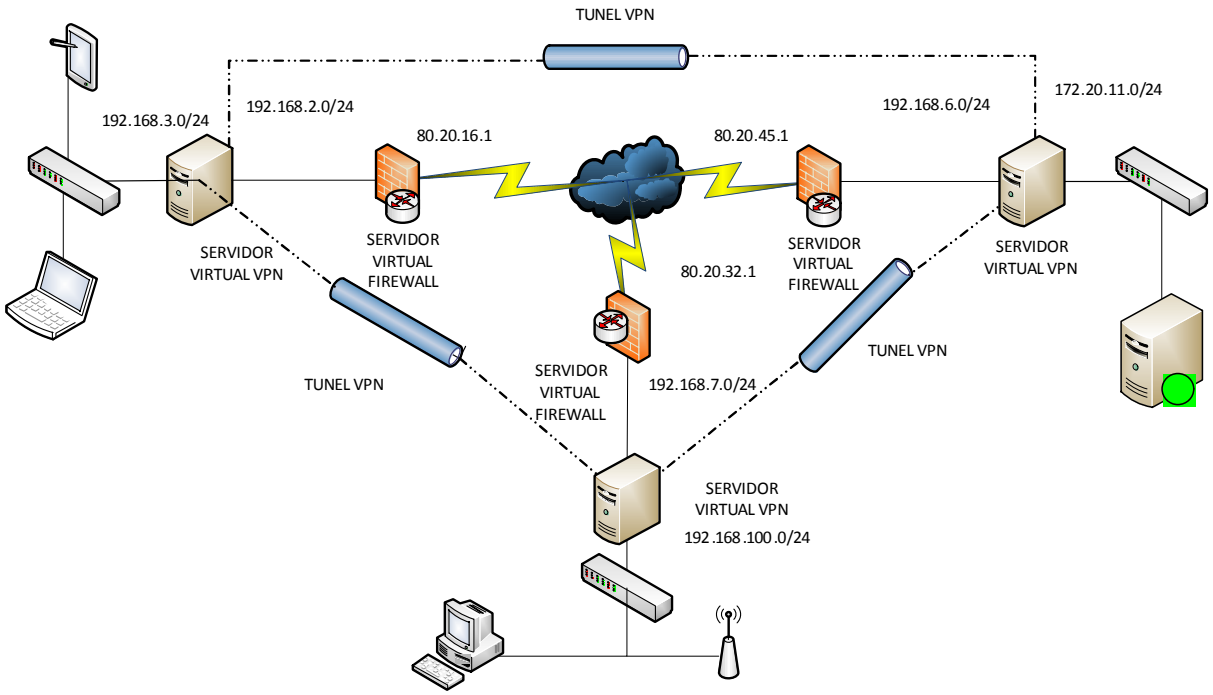


Figura 62: Esquema solución definitiva

Como se puede observar, los túneles VPN generados entre las distintas redes pueden enviar tráfico sin recibir restricciones por parte de los firewall. Todo el tráfico que no circule por alguno de los túneles será inspeccionado

por el firewall y sus paquetes serán filtrados. Cada firewall contiene la misma configuración adaptado al rango de red en el que trabaja. Analizando uno de los centros (en este caso Barcelona) podemos entender cómo funciona cualquier otro centro.

El centro de Barcelona dispone de una dirección pública 80.20.16.1 configurada como ETH0 en el Firewall. Como el servidor VPN se encuentra por detrás del firewall y éste a su vez dispone de un interfaz en la misma red se ha de configurar el firewall para que redireccione los paquetes que entren con destino a la VPN (es decir, protocolos de red como ISAKMP, NAT-T y ESP) permitiendo que la negociación de los SA y envío/recepción de paquetes cifrados con IPsec entre los distintos servidores VPN sea transparente para el firewall, que se estará encargando de denegar otro tipo de conexiones. Para ello utilizamos el concepto de aplicar NAT con la instrucción PREROUTING. Vemos aquí las instrucciones que se deben ejecutar en un script bajo el servidor virtual Linux que funcionará como firewall:

iptables –t nat –A PREROUTING –i eth0 –p tcp 80.20.16.1 –dport isakmp –j DNAT –to-destination 192.168.2.2:500

iptables –t nat –A PREROUTING –i eth0 –p tcp 80.20.16.1 –dport 1701 –j DNAT –to-destination 192.168.2.2:1701

iptables –t nat –A PREROUTING –i eth0 –p tcp 80.20.16.1 –dport 4500 –j DNAT –to-destination 192.168.2.2:4500

iptables –t nat –A PREROUTING –i eth0 –p esp 80.20.16.1 –j DNAT –to-destination 192.168.2.2

Como se puede ver, todo el tráfico relacionado con VPN será re-direccionado desde la NIC conectada a la red pública a la interfaz externa del servidor VPN. Una vez realizada esta operación, debemos de realizar el paso inverso. Permitir que el servidor interno con role VPN pueda direccionar todo su tráfico hacia otros servidores VPN sin que el firewall suponga un problema. Para ello utilizaremos las siguientes instrucciones.

Generaremos un POSTROUTING para enmascarar el tráfico que permita la salida de tráfico por eth0 (red pública)

Iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE

Y permitiremos el FORWARD de todos los paquetes que entren por ETH1 (NIC Interna del firewall) y que su estado sea paquetes nuevos, ya establecidos o relacionados.

iptables –A FORWARD –i eth1 –p udp –dport 500 -m state –state NEW,ESTABLISHED,RELATED –J ACCEPT

iptables –A FORWARD –I eth1 –p udp –dport 1701 -m state –state NEW, ESTABLISHED, RELATED –J ACCEPT

iptables –A FORWARD –I eth1 –p udp –dport 4500 -m state –state NEW, ESTABLISHED, RELATED –J ACCEPT

iptables –A FORWARD –I eth1 –p esp -m state –state NEW, ESTABLISHED, RELATED –J ACCEPT

Con esta configuración aplicada específicamente para cada firewall de las sedes se consigue que las conexiones VPN funcionen completamente trasparentes al funcionamiento del firewall sin afectar a la seguridad de los sites.

11.4.2 Resolviendo problemas con NAT-Transversal en Windows server 2008

Un caso realmente curioso es el aparecido en los primeros test que se desarrollaron para ver la viabilidad de este proyecto. Inicialmente se colocaron dos servidores Firewall delante de los respectivos servidores VPN de Alicante y Barcelona, sustituyendo las interfaces con IP pública de estos servidores por Ip's de un segmento de red compartido entre el firewall y el servidor. De esta manera los servidores Firewall quedaban justo delante de los servidores VPN, protegiendo la red perimetralmente tal y como se ha comentado en el anterior punto 11.4.1 (ver figura 60 para mayor referencia).

La idea principal es que el servidor Firewall ejecute un script llamado **firewall.sh** que contenga las IP tables diseñadas para que los anteriores puertos realicen un FORWARD para poder salir por ETH0 y se disponga de una serie de PREROUTING para que puedan acceder mediante una IP pública asignada al firewall y redirigida al servidor VPN, haciendo estos servidores un papel transparente de cara a los enlaces VPN.

Los sucesivos test que se programaron arrojaron un problema grave a la hora de establecer el SA mediante el protocolo ISAKMP incluido en IKE. Si bien las reglas en los respectivos firewall estaban diseñadas correctamente, un estudio realizado mediante Wireshark mostraba que para el protocolo era imposible de generar la asociación de seguridad si disponía de firewall delante:

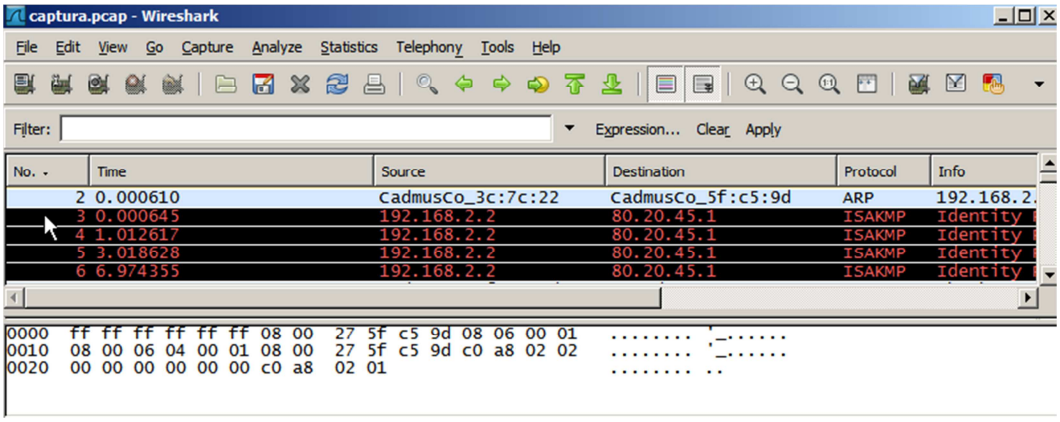


Figura 63: Captura errónea protocolo ISAKMP en wireshark

Por parte de role Route and remote Access se recibía el siguiente error:

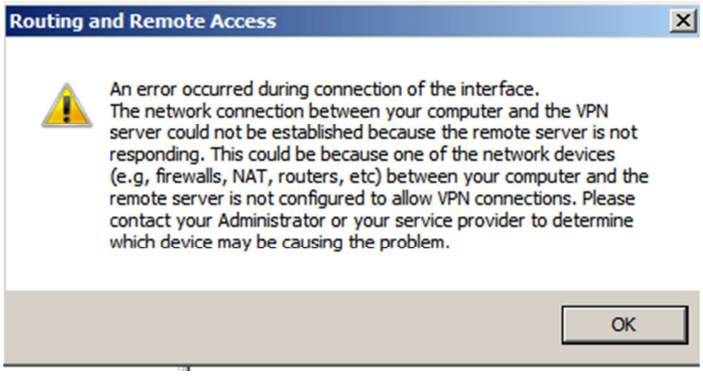


Figura 64: Error de conexión Windows VPN

Recordando el funcionamiento de IKE (punto 8.3.4 de la página 20), en la primera fase de la conexión, se establecerá un canal de comunicaciones seguro usando el algoritmo de intercambio de claves **Diffie-Hellman** para generar una clave de secreto compartido y cifrar la comunicación IKE. Se establecerá entonces un security association mediante

el modo principal o Main mode. Analizando mediante wireshark el protocolo ISAKMP (perteneciente a IKE) en modo principal generado se observa que no es capaz de generar la cookie de respuesta que autentica al servidor

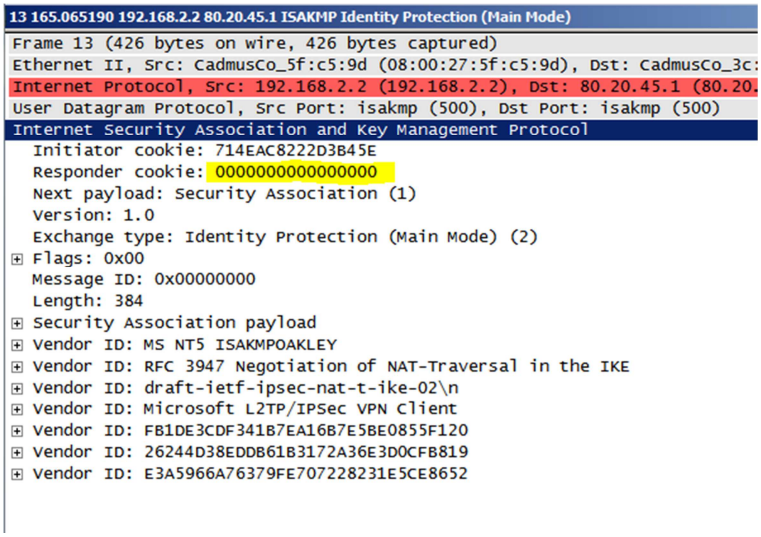


Figura 65: Captura protocolo ISAKMP main mode con Cookie erróneo

Oficialmente Microsoft habla de este curioso error anotando las siguiente observación: "De manera predeterminada, Windows Vista y el sistema operativo Windows Server 2008 no admiten Internet Protocol security (IPsec) red dirección translation (NAT) transversal (NAT-T) asociaciones de seguridad con servidores ubicados tras un dispositivo NAT. Por lo tanto, si el servidor de red privada virtual (VPN) está detrás de un dispositivo NAT, un equipo cliente VPN basado en Windows Vista o en un equipo cliente VPN basados en Windows Server 2008 no puede hacer un protocolo de túnel de capa dos (L2TP) / conexión IPsec al servidor VPN. Este escenario incluye servidores VPN que ejecutan Windows Server 2008 y Microsoft Windows Server 2003. "

Sin embargo, que por defecto no permita realizar esta operación no significa que el fabricante no permita realizar NAT-T delante de su dispositivo con una modificación. Esta se realiza mediante el comando regedit, generando la siguiente clave de registro siguiendo estos pasos:

1) Navegar hasta la siguiente clave de registro:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent

2) Generar la siguiente clave **AssumeUDPEncapsulationContextOnSendRule con valor DWORD (32 bits).**
3) Añadirle el valor 2. Un valor de 2 configura Windows para que pueda establecer las asociaciones de seguridad cuando el servidor y el equipo cliente VPN basado en Windows Server 2008 están detrás de dispositivos NAT.

Si se aplican estos pasos en cada servidor VPN y los comandos iptables están correctamente configurados, una vez reiniciados los servidores VPN, las conexiones se podrán realizar con normalidad.

A continuación, una vez reiniciados los servidores se lanza la conexión desde el servidor de Barcelona al servidor de Alicante, la captura general muestra que la conexión funciona correctamente:

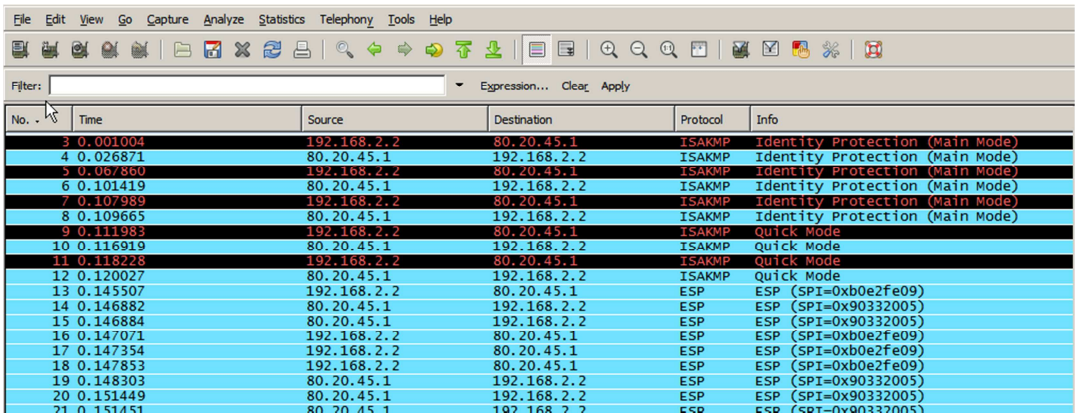


Figura 66: Captura wireshark funcionamiento L2TP/IPsec correcto

De esta manera, con esta modificación realizada, el proyecto funciona perfectamente utilizando NAT transversal, ofreciendo una red VPN a los distintos usuarios y protegiéndolos contra vulnerabilidades y ataques.

12. Conclusiones

El presente proyecto ha mostrado como unificar distintas sedes geográficamente dispersas a través de la tecnología VPN y protegerla mediante firewalls diseñados con software libre (IPtables).

En una primera parte se ha realizado un trabajo académico o estudio sobre las distintas posibilidades de las redes VPN bajo entornos Microsoft, centrándose en la teoría de los protocolos y el cifrado a utilizar.

En una segunda parte, el autor ha querido alejarse de un proyecto típicamente teórico y ha incluido multitud de configuraciones realizadas en laboratorios virtuales. Esto demuestra que el proyecto es 100% aplicable a un marco real y que no existiría problema a la hora de exportarlo como solución definitiva entre pequeñas y medianas empresas. Con leves modificaciones se puede implementar el mismo proyecto para implementar una solución que ofrezca conectar sites empresariales a redes LAN ubicadas en las viviendas de los trabajadores ofreciendo flexibilidad laboral en una época realmente necesaria.

Se ha mostrado especial énfasis en explicar el porqué de utilizar L2TP/IPsec, mostrando la inseguridad descubierta durante el 2012 bajo el cifrado generado con la clave MS-CHAPv2 bajo PPTP. Es posible que muchas empresas a día de hoy sigan utilizando esta tecnología sin conocer que la privacidad y seguridad de sus datos está en peligro.

El autor también ha querido mostrar la importancia de disponer de un cortafuego bien configurado, mostrando configuraciones y soluciones de problemas utilizando esta tecnología junto con VPN. Como se habrá podido observar, la seguridad ha sido uno de los actores principales a tener en cuenta en el texto.

En definitiva, el autor espera que dicho documento ofrezca una explicación fácil, útil e interesante al mundo de las VPN, así como que éste sea de ayuda por si algún lector necesita implementar en un futuro una solución de este tipo de una manera ágil y económica.

13. Anexos

13.1 Script Firewall de Barcelona

```
# Vaciamos todas las reglas y eliminamos las cadenas vacías

iptables –t nat –F

iptables –t nat –X

iptables –F

iptables –X

echo 1 > /proc/sys/net/ipv4/ip_forward

# Inicialmente configuramos una política para que no pase nada de tráfico

iptables –P INPUT DROP

iptables –P OUTPUT DROP

iptables –P FORWARD DROP

# Redireccion: Permitimos hacer prerouting con los puertos 500,1701 y 4500 para operar con L2TP/IPsec

iptables –t nat –A PREROUTING –i eth0 –p tcp 80.20.16.1 –dport isakmp –j DNAT –to-destination 192.168.2.2:500

iptables –t nat –A PREROUTING –i eth0 –p tcp 80.20.16.1 –dport 1701 –j DNAT –to-destination 192.168.2.2:1701

iptables –t nat –A PREROUTING –i eth0 –p tcp 80.20.16.1 –dport 4500 –j DNAT –to-destination 192.168.2.2:4500

iptables –t nat –A PREROUTING –i eth0 –p esp 80.20.16.1 –j DNAT –to-destination 192.168.2.2

iptables –t nat –A POSTROUTNG –o eth0 –j MASQUERADE

iptables –A OUTPUT –m state –state ESTABLISHED –j ACCEPT

iptables –A FORWARD –m state –state ESTABLISHED –j ACCEPT

iptables –A FORWARD –i eth1 –p udp –dport 500 -m state –state NEW,ESTABLISHED,RELATED –J ACCEPT
```

iptables –A FORWARD –I eth1 –p udp –dport 1701 -m state –state NEW, ESTABLISHED, RELATED –J ACCEPT

iptables –A FORWARD –I eth1 –p udp –dport 4500 -m state –state NEW, ESTABLISHED, RELATED –J ACCEPT

iptables –A FORWARD –I eth1 –p esp -m state –state NEW, ESTABLISHED, RELATED –J ACCEPT

13.2 Script Firewall de Alicante

 # Vaciamos todas las reglas y eliminamos las cadenas vacías

iptables –t nat –F

iptables –t nat –X

iptables –F

iptables –X

echo 1 > /proc/sys/net/ipv4/ip_forward

 # Inicialmente configuramos una política para que no pase nada de tráfico

iptables –P INPUT DROP

iptables –P OUTPUT DROP

iptables –P FORWARD DROP

 # redirección: Permitimos hacer prerouting con los puertos 500,1701 y 4500 para operar con L2TP/IPsec

iptables –t nat –A PREROUTING –i eth0 –p tcp 80.20.45.1 –dport isakmp –j DNAT –to-destination 192.168.6.2:500

iptables –t nat –A PREROUTING –i eth0 –p tcp 80.20.45.1 –dport 1701 –j DNAT –to-destination 192.168.6.2:1701

iptables –t nat –A PREROUTING –i eth0 –p tcp 80.20.45.1 –dport 4500 –j DNAT –to-destination 192.168.6.2:4500

iptables –t nat –A PREROUTING –i eth0 –p esp 80.20.45.1 –j DNAT –to-destination 192.168.6.2

iptables –t nat –A POSTROUTNG –o eth0 –j MASQUERADE

iptables –A OUTPUT –m state –state ESTABLISHED –j ACCEPT

iptables –A FORWARD –m state –state ESTABLISHED –j ACCEPT

iptables –A FORWARD –i eth1 –p udp –dport 500 -m state –state NEW,ESTABLISHED,RELATED –J ACCEPT

iptables –A FORWARD –I eth1 –p udp –dport 1701 -m state –state NEW, ESTABLISHED, RELATED –J ACCEPT

iptables –A FORWARD –I eth1 –p udp –dport 4500 -m state –state NEW, ESTABLISHED, RELATED –J ACCEPT

iptables –A FORWARD –I eth1 –p esp -m state –state NEW, ESTABLISHED, RELATED –J ACCEPT

13.3 Script Firewall de Milán

Vaciamos todas las reglas y eliminamos las cadenas vacías

iptables –t nat –F

iptables –t nat –X

iptables –F

iptables –X

echo 1 > /proc/sys/net/ipv4/ip_forward

Inicialmente configuramos una política para que no pase nada de tráfico

iptables –P INPUT DROP

iptables –P OUTPUT DROP

iptables –P FORWARD DROP

redirección: Permitimos hacer prerouting con los puertos 500,1701 y 4500 para operar con L2TP/IPsec

iptables –t nat –A PREROUTING –i eth0 –p tcp 80.20.32.1 –dport isakmp –j DNAT –to-destination 192.168.7.2:500

iptables –t nat –A PREROUTING –i eth0 –p tcp 80.20.32.1 –dport 1701 –j DNAT –to-destination 192.168.7.2:1701

iptables –t nat –A PREROUTING –i eth0 –p tcp 80.20.32.1 –dport 4500 –j DNAT –to-destination 192.168.7.2:4500

iptables –t nat –A PREROUTING –i eth0 –p esp 80.20.32.1 –j DNAT –to-destination 192.168.7.2

iptables –t nat –A POSTROUTNG –o eth0 –j MASQUERADE

iptables –A OUTPUT –m state –state ESTABLISHED –j ACCEPT

iptables –A FORWARD –m state –state ESTABLISHED –j ACCEPT

iptables –A FORWARD –i eth1 –p udp –dport 500 -m state –state NEW,ESTABLISHED,RELATED –J ACCEPT

iptables –A FORWARD –I eth1 –p udp –dport 1701 -m state –state NEW, ESTABLISHED, RELATED –J ACCEPT

iptables –A FORWARD –I eth1 –p udp –dport 4500 -m state –state NEW, ESTABLISHED, RELATED –J ACCEPT

iptables –A FORWARD –I eth1 –p esp -m state –state NEW, ESTABLISHED, RELATED –J ACCEPT

13.4 Prueba de vulnerabilidades. Atacando a un sistema VPN bajo Windows server 2008

Finalizado el proyecto, una vez implementado todo el sistema que permite a las distintas redes geográficamente dispersas comunicarse como si de una misma LAN se tratara y protegerlas mediante servidores virtuales basados en Linux, es posible que debamos de lanzar una pregunta que debe de realizarse todo ingeniero, técnico o profesional IT cuando implementa una nueva tecnología en el área IT ¿Es mi sistema vulnerable a un ataque informático? Evidentemente todos los sistemas, por caros y complejos que sean, pueden ser fruto de un ataque informático, lo que se necesita es implementar las distintas medidas para que el ataque sea costoso de realizar, complejo y el atacante decida darse por vencido ante la complejidad de nuestros sistemas de defensa.

Mientras se desarrollaba este proyecto, el autor tenía en mente que no quería que este fuera un proyecto eminentemente teórico, de ahí que toda la tecnología descrita haya sido puesta a la vez en práctica. Siguiendo esta tendencia, se va a realizar una última prueba de laboratorio en la que se intentará obtener vulnerabilidades entre la red VPN de Barcelona y Alicante simulando ser un atacante conectado en la red externa. Los firewalls bajo IPTables y el cifrado mediante IPsec deberían de ser los principales escollos que debería de encontrarse a la hora de llevar a cabo un ataque en dicha infraestructura.

Para comenzar el test de penetración, mostraremos una imagen de cómo se procederá al intento de ataque. Se dispone de un equipo utilizando una distribución de Linux Backtrack conectado a nuestra red de Internet (red pública). Esta distribución está pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Por otro lado, para comprobar la fiabilidad del sistema se ha decidido utilizar una conexión VPN que una los centros de Barcelona y Alicante. El centro de Barcelona dispondrá del firewall delante del servidor VPN, tal y como mostramos en la solución final del proyecto. El site de Alicante no dispondrá de solución firewall y conectará su servidor directamente a la red pública. De esta manera se comprobará la importancia del dispositivo firewall en nuestra solución al realizar los mismos ataques tanto en un centro con firewall como en un centro sin firewall. La siguiente imagen muestra un esquema del laboratorio en el que se desarrollará el test de penetración:

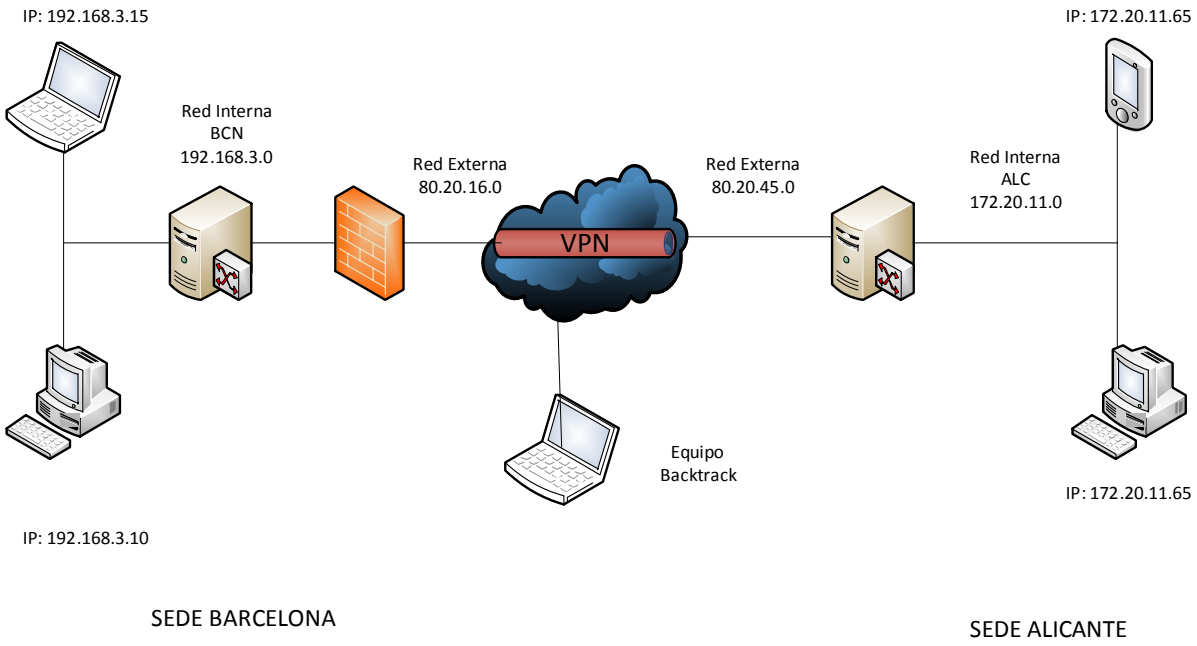


Figura 67: Esquema test vulnerabilidad con firewall en la sede de Barcelona

La primera acción que realiza un atacante, se basa en un reconocimiento y una exploración de los diferentes sistemas. Supongamos que el atacante ya conoce que las direcciones externas de la red pública pertenecen a una empresa y tiene la intuición de que se usa algún tipo de VPN para comunicar las distintas sedes. Lo primero que necesitará saber es qué sistema de VPN se está usando o cuál es el fabricante, para así buscar exploits y vulnerabilidades pudiendo o bien acceder al Sistema Operativo o bien acceder al contenido de los paquetes cifrados. Para recolectar información la mejor herramienta de escáner de puertos es el famoso nmap. Es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich). Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática. Se le considera una herramienta imprescindible para pruebas de penetración (Fuente: Wikipedia). Se lanza nmap para averiguar cuantos puertos tiene abierto el servidor de Alicante con la siguiente instrucción:

Nmap –sS –sU -p 1-10000 80.20.45.1

Nmap –sS –sU –p 1-10000 80.20.16.1

Con –sS no se llega a abrir una conexión TCP completa, enviándose solo un paquete SYN para abrir conexión y recibir SYN/ACK que nos dirá si el puerto está abierto o un RST si está cerrado. Con –sU se realiza el mismo proceso con el protocolo UDP. Si se observan las imágenes 65 y 66 de esta misma página, el escaneo al servidor VPN de Alicante sin firewall delante da como resultado que el puerto 500 está abierto, por lo que el atacante sabrá que se está ante un servidor VPN que funciona mediante L2TP/Ipsec.

```
root@bt:~# nmap -sS -sU -p 1-10000 80.20.45.1

Starting Nmap 6.01 ( http://nmap.org ) at 2013-11-29 13:53 CET
Nmap scan report for 80.20.45.1
Host is up (0.0016s latency).
Not shown: 9999 filtered ports, 9999 open|filtered ports
PORT     STATE  SERVICE
1723/tcp closed pptp
500/udp  open   isakmp
MAC Address: 08:00:27:32:2C:BC (Cadmus Computer Systems)
```

Figura 68: Rastreo de puertos contra sede sin Firewall

En cambio, el servidor firewall de Barcelona realiza su trabajo evitando delatar que se dispone de un servidor VPN en dicha conexión. Se evita dar así información de los puertos abiertos.

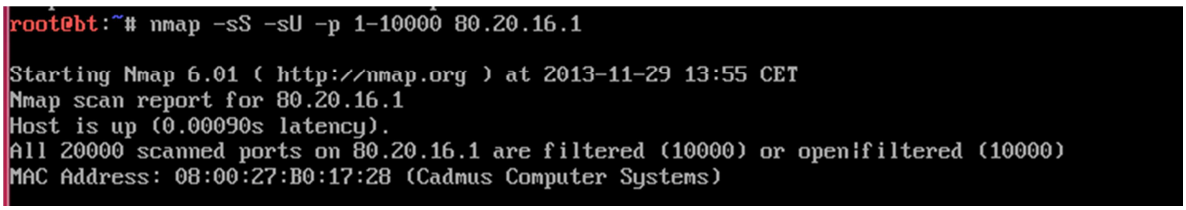


Figura 69: Rastreo de puertos contra sede con firewall

Una vez se está en conocimiento de que la infraestructura usa un servidor con tecnología IPsec en Alicante, se puede lanzar un ataque sobre el protocolo IKE que éste utiliza. En este caso la herramienta ike-scan incluida en backtrack ofrece una importantísima información sobre el servidor VPN (Figura 67 página 63). Captura el Handshake de IKE, informándonos del protocolo de encriptado usado 3DES y del tipo de clave (compartida PSK), el tipo de Hash utilizado (SHA1) y el mod utilizado con diffie Hellman (en este caso mod1024). Si se observa la primera línea VID, vemos las siglas MS NT5, es decir, un servidor bajo tecnología Microsoft.

Figura 70: Captura del Handshake mediante ike-scan en sede sin Firewall

Es muy interesante observar como Microsoft utiliza por defecto el modo principal (Main mode) con el protocolo IKE, protegiendo la identidad de los extremos de conexión y evitando que se pudiera recopilar información en un fichero para luego extraerla y utilizar algún software de análisis por fuerza bruta o diccionario para extraer el PSK.

Se realiza el mismo procedimiento sobre el servidor de Barcelona VPN. Como se puede observar, con el firewall delante evita que IKE-Scan obtenga resultados:

Figura 71: Intento erróneo de captura handshake con sede protegida con firewall

Una vez llegados a este punto, podemos extraer algunas consideraciones:

1. El Firewall evita delatar que se utiliza L2TP/IPsec como estándar VPN por lo que dificultaría la selección del tipo de ataque ya que el atacante no sabría si se está utilizando VPN u otro tipo de tecnología.

2. El Firewall protege ante un escáner de protocolo IKE usado para realizar el security association. Sin embargo, en caso de que este firewall dejara de filtrar paquetes, no se podría realizar un ataque por fuerza bruta para obtener el PSK debido a que se utiliza el modo principal en IKE y no el modo agresivo.

El atacante puede probar con otro software para intentar "crackear" la clave compartida cuando se generan las security association. Se puede observar que la contestación es la misma en ambos equipos. Si la primera parte de la conexión generada con el protocolo IKE no se realiza en modo agresivo, es segura y no se puede vulnerar:

***Fiked* supports IKEv1 in aggressive mode, using pre-shared keys and XAUTH. Supported algorithms are DES, 3DES, AES-128, AES-192, AES-256; MD5, SHA1; and DH groups 1, 2 and 5. IKE main mode is not supported.**

Independiente de esto, se han realizado algunas pruebas más. Por un lado se ha utilizado el software IKEProbe contra el servidor no protegido mediante Firewall. Éste es un excelente software generado para arquitectura Windows que fuerza a las Gateway a trabajar mediante agressive mode y comprobar las vulnerabilidades Utilizando distintos modelos de cifrado, Diffie Hellman y Hashes.

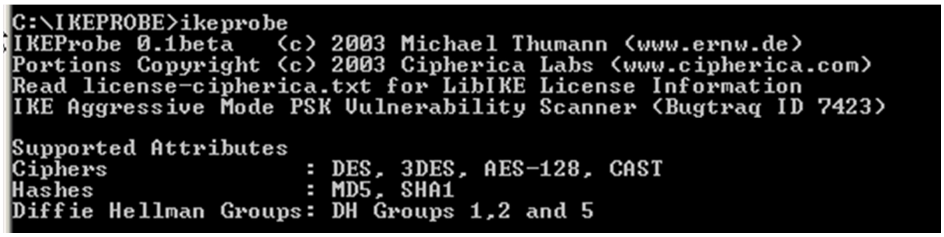


Figura 72: IKEprobe

En el caso que nos ocupa, el servidor no protegido mediante firewall (en teoría el más débil) ha soportado la prueba sin que se le encontraran vulnerabilidades:

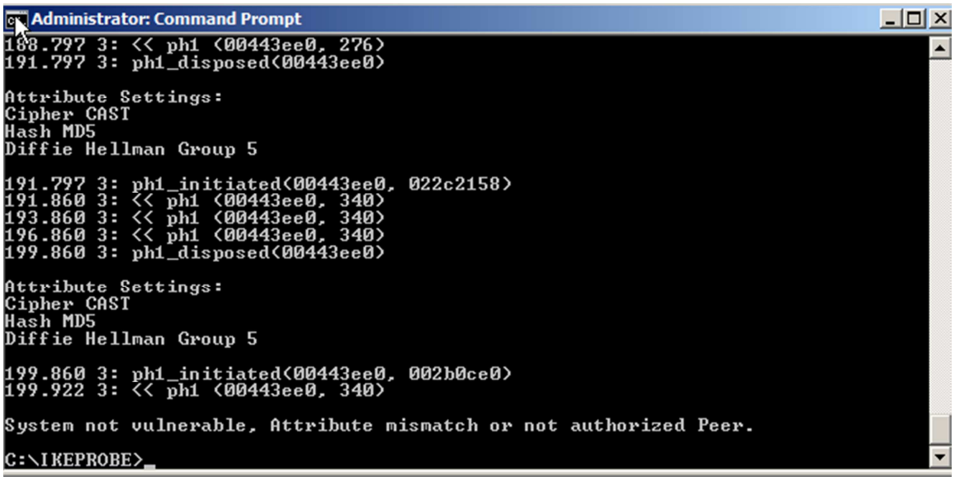


Figura 73: Resultados de IKEprobe contra el servidor VPN de Alicante 80.20.45.1

14Glosario

- **3DES:** Algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES, desarrollado por IBM en 1998. El Triple DES, como su nombre indica, consiste en aplicar el DES tres veces consecutivas. Esto se puede realizar con tres claves (k1 , k2 , k3), o bien con sólo dos (k1 , k2 , y otra vez k1). La longitud total de la clave con la segunda opción es de 112 bits (dos claves de 56 bits), que hoy ya se considera suficiente segura; la primera opción proporciona más seguridad, pero a costa de utilizar una clave total de 168 bits (3 claves de 56 bits), que puede ser un poco más difícil de gestionar e intercambiar.

- **Active Directory:** Es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores.

- **ADSL:** Línea de abonado digital asimétrica. Es un tipo de tecnología de línea DSL. Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre.

- **Ataque de Diccionario:** Método de cracking que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario.

- **Ataque DOS:** Ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

- **Ataque de fuerza bruta:** Forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

- **BSOD:** Parada crítica del sistema como defensa contra una operación que pone en riesgo el núcleo del mismo.

- **CHAP:** Protocolo de autenticación que utiliza tres vías y un desafío de autenticación.

- **Chapcrack:** Herramienta que permite capturar y crackear las contraseñas usadas en conexiones PPTP o WPA2 enterprise.

- **Cifrado de flujo:** El funcionamiento de un cifrado en flujo consiste en la combinación de un texto en claro M con un texto de cifrado S que se obtiene a partir de la clave simétrica k. Para descifrar, sólo se requiere realizar la operación inversa con el texto cifrado y el mismo texto de cifrado S.

- **Cifrado por bloques:** En una cifra de bloque, el algoritmo de cifrado o descifrado se aplica separadamente a bloques de entrada de longitud fija b, y para cada uno de ellos el resultado es un bloque de la misma longitud.

- **Cisco System:** Empresa con sede en San Jose dedicada a la Electrónica de red.

- **Defcon:** Conferencia de seguridad informática.

- **DES:** Algoritmo que admite una clave de 64 bits, pero sólo 7 de cada 8 intervienen en el cifrado, de modo que la longitud efectiva de la clave es de 56 bits. Los bloques de texto a los que se les aplica DES tienen que ser de 64 bits cada uno. La parte central del algoritmo consiste en dividir la entrada en grupos de bits, hacer una sustitución distinta sobre cada grupo y, a continuación una transposición de todos los bits. Esta transformación se repite dieciséis veces: en cada iteración, la entrada es una transposición distinta de los bits de la clave sumada bit a bit (XOR) con la salida de la iteración anterior. Tal como está diseñado el algoritmo, el descifrado se realiza igual que el cifrado pero realizando las transposiciones de la clave en el orden inverso (empezando por la última).

- **Desafío de autenticación:** Método que permite preveer la identidad de un usuario a través de un medio inseguro sin revelar información sensible que pueda ser usada por usuarios malintencionados.

- **DHCP:** Dynamic Host Configuration Protocol, es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

- **Diffie-Hellman:** Protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autentificada).

- **Exploit:** Software que aprovecha una vulnerabilidad del sistema para que realice una función no deseada.

- **Frame Relay:** Técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual

- **Gateway:** Dispositivo que permite conectar redes con protocolos e infraestructura distinta.

- **Handshake:** Proceso automatizado de negociación que establece de forma dinámica los parámetros de un canal de comunicaciones establecido entre dos entidades antes de que comience la comunicación normal por el canal.

- **Hash:** Cadena de bits, de longitud predeterminada, que se obtiene a partir de una secuencia de bits de longitud arbitraria, como "resumen" de esta secuencia.

- **Hyper-V:** Programa de virtualización basado en un hipervisor para los sistemas de 64-bits1 con los procesadores basados en AMD-V o Tecnología de virtualización Intel (el instrumental de gestión también se puede instalar en sistemas x86).

- **IA-32 X86:** IA-32 (Intel Architecture, 32-bit), conocida de manera genérica como x86, x86-32 o i386, es la arquitectura del conjunto de instrucciones del procesador de Intel comercialmente más exitoso. Es una extensión de 32-bit, primero implementada en el Intel 80386, proveniente de los antiguos procesadores Intel 8086,80186 y 80286 de 16-bit y el denominador común de todos los diseños x86subsecuentes.

- **IA64:** Arquitectura de 64 bits desarrollada por Intel en cooperación con Hewlett-Packard para su línea de procesadores Itanium eItanium 2.

- **IEEE:** Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización.

- **Intel Celeron:** Microprocesador de la compañía Intel orientado al mercado de bajo costo. El objetivo era poder, mediante esta segunda marca, penetrar en los mercados cerrados a los Pentium, de mayor rendimiento y precio.

- **IPSec:** Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete en un flujo de datos.

- **Kbits/s:** 8129 bits por segundo enviados por un medio de telecomunicaciones.

- **Kernel:** Parte principal del sistema operativo que ofrece acceso seguro al hardware y ofrece recursos del sistema.

- **L2F:** Protocolo diseñado por Cisco para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas y que funciona en diversas tecnologías.

- **L2TP:** Protocolo permite cifrar tráfico multiprotocolo permitiendo enviar paquetes por cualquier canal punto a punto.

- **Linux:** Linux es un núcleo libre de sistema operativo (también suele referirse al núcleo como kernel) basado en Unix.

- **Man in the middle:** Ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

- **MCTS:** Especialista Tecnológico Certificado Microsoft (MCTS)

- **Metcalfe**: Ingeniero eléctrico de los EE. UU., coinventor de Ethernet, fundador de 3Com, enunció la Ley de Metcalfe.

- **Microsoft:** Empresa multinacional de origen estadounidense, fundada el 4 de abril de 1975 por Bill Gatesy Paul Allen. Dedicada al sector del software

- **Microsoft Role:** Función o servicio asociado a la infraestructura de los sistemas operativos Windows.

- **MSCHAPv2:** Protocolo de Microsoft que funciona como proceso de autenticación mutua unidireccional mediante contraseña cifrada.

- **NAT:** Mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

- **NIC:** Periférico que permite la comunicación con aparatos conectados entre sí

- **PPTP:** Es un protocolo de comunicaciones desarrollado por Microsoft para generar túneles VPN.

- **PSK:** (pre-shared key) Es una clave secreta compartida con anterioridad entre las dos partes usando algún canal seguro antes de que se utilice.

- **RDSI:** Se define como una red evolucionada de la red de telefonía digital integrada que permite la conexión digital extremo a extremo para dar soporte a una amplia gama de servicios.+++++

- **RFC:** Es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

- **RSA RC4:** Es el algoritmo de cifrado en flujo más utilizado en muchas aplicaciones gracias a su simplicidad y velocidad. Por ejemplo, el sistema de protección WEP (Wired Equivalent Privacy) que incorpora el estándar IEEE 802.11 para tecnología LAN

- **SHA1:** Es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST). producen una salida resumen de 160 bits (20 bytes) de un mensaje que puede tener un tamaño máximo de 264 bits.

- **Token Ring:** Arquitectura de red desarrollada por IBM en los años 1970 con topología física en anillo y técnica de acceso de paso de testigo, usando un frame de 3 bytes llamado token que viaja alrededor del anillo.

- **VirtualBox:** Herramienta Hipervisor para virtualización de la empresa Oracle.

- **VPN:** Tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet.

- **Wireshark:** Analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación

15 Referencias bibliográficas

15.1 Libros

1. Mackin J.C; Northrup, Tony (2008).”Configuring IP routing”. En: *MCTS Exam 70-642 Configuring Windows server 2008 Network Infrastructure.* Redmon, Washinton Microsoft Press
2. Herrera Joancomartí Jordi; García Alfaro, Joaquín; Perramón Tornil, Xavier. “Aspectos avanzados de seguridad en redes”. En: *Software Libre* . Barcelona: Editorial UOC
3. Barberán, Pere. “Diseño de redes WAN y nuevas tecnologías”. En: *Redes y servicios*. Barcelona: Editorial UOC.
4. Perramón, Xavier. “Mecanismos de protección”. En: *Seguridad en redes de computadores*. Barcelona: Editorial UOC.
5. McNab ,Chris; (2004). Network Security Assessment. Editorial O’Reilly
6. Lopez i Rocafiguera, Enric. “WAN Redes de gran alcance”. En: *Redes y servicios*. Barcelona: Editorial UOC
7. García Alfaro, Joaquín. Filtrado y registro de paquetes con IPTables. Barcelona: Editorial UOC
8. Barceló Ordinas, José M.; Griera, Jordi Íñigo. “Protocolos de transporte”. En: *Protocolos y aplicaciones de Internet*. Barcelona: Editorial UOC

15.2 Documentos electronicos

1. Schneier , Bruce, Mudge; Wagner, David . (1999) "Cryptoanalysis of Microsoft PPTP Authentication Extension". [artículo en línea]. California: UC Berkeley, [Fecha de consulta: Noviembre-Diciembre 2013], https://www.schneier.com/paper-pptpv2.pdf
2. Eisinger, Jochen . "Exploiting known security holes in Microsoft's PPTP Authentication Extensions (MS-CHAPv2)". [artículo en línea]. Freiburg: University of Freiburg, [Fecha de consulta: Noviembre-Diciembre 2013], http://www.cs.ubc.ca/~eisinger/paper/pptp_mschapv2.pdf
3. Gonzalez Rojas, Michel Arley. "Principios Básicos del Networking", [artículo en línea]. [Fecha de consulta: Noviembre 2013], http://www.slideshare.net/michelarleygonzalezrojas/taller-2-9840952
4. Marlinspike, Moxie . "Divide and Conquer**:** Cracking MS-CHAPv2 with a 100% success rate", [artículo en línea]. cloudcracker.com, [Fecha de consulta: Noviembre-Diciembre 2013], https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/
5. Pérez Iglesias, Santiago. "Análisis del protocolo IPSec: el estándar de seguridad en IP", [artículo en línea]. Telefonica Investigacion y desarrollo. [Fecha de consulta: Diciembre 2013], http://www.movistar.es/on/io/es/atencion/tutoriales_articulos/pdf/IPSec.pdf

15.3 Enlaces web

1. Building a tunnelled VPN using ESP (static IPs, no NAT), [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013]. http://www.mad-hacking.net/documentation/linux/networking/ipsec/nat-vpn.xml
2. Puertos abiertos en iptables para una VPN, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : https://lists.debian.org/debian-user-spanish/2006/03/msg01003.html
3. How to configure an L2TP/IPsec server behind a NAT-T device in Windows Vista and in Windows Server 2008, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://support.microsoft.com/kb/926179/es
4. Rematando MS-CHAP v2: Microsoft aconseja dejar de usarlo sin encapsular, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://unaaldia.hispasec.com/2012/09/rematando-ms-chap-v2-microsoft-aconseja_5.html
5. ISAKMP, Internet Security Association and Key Management Protocol, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://www.networksorcery.com/enp/protocol/isakmp.htm
6. Técnicas de sondeo de puertos, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://nmap.org/man/es/man-port-scanning-techniques.html
7. IKE main mode, aggressive mode, & phase 2, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://ccie-or-null.net/2012/03/26/ike-main-mode-aggressive-mode-phase-2/
8. ipsec-vpn-penetration-testing-backtrack-tools, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://www.linuxforu.com/2012/01/ipsec-vpn-penetration-testing-backtrack-tools/
9. Protocolos de túnel VPN, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://technet.microsoft.com/es-es/library/cc771298(v=ws.10).aspx
10. VPN y firewalls, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://technet.microsoft.com/es-es/library/cc753364(v=ws.10).aspx
11. La autenticación MS-CHAP v2 sin encapsular podría permitir la divulgación de información, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://technet.microsoft.com/es-es/security/advisory/2743314?altTemplate=SecurityAdvisoryPF
12. OSI, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://es.slideshare.net/corista14/osi-9763768
13. Modelo OSI,Wikipedia, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://es.wikipedia.org/wiki/Modelo_OSI

14. Cortafuegos, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://www.bdat.net/documentos/cortafuegos/x295.html
15. Firewall para redes. Filtrado de paquetes, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://marnigro.blogspot.com.es/2010/01/firewall-para-redes-filtrado-de.html
16. Red hart Enterprise Linux manual de seguridad, [artículo en línea], [Fecha de consulta: Noviembre-Diciembre 2013] : http://web.mit.edu/rhel-doc/4/RH-DOCS/pdf/rhel-sg-es.pdf