Universidad de Oviedo

Memoria del trabajo Fin de Master realizado por

Ricardo Guntín García

para la obtención del título

Master en Ingeniería de Automatización e Informática Industrial

TITULO

Monitorización y acceso remoto para sistemas de control de máquinas de manejo de materiales (Bulk Handling)

FECHA DE PRESENTACIÓN

20-07-2015

Título del proyecto

Monitorización y acceso remoto para sistemas de control de máquinas de manejo de materiales (Bulk Handling)

Empresa de desarrollo del proyecto

TSK Electrónica y Electricidad S.A.

Autor del proyecto

Ricardo Guntín García

Tutor del proyecto

Carlos Ruiz

Tutor académico

Antonio Robles

Tabla de contenido

1.1. OBJETO

Con el presente proyecto se desea conseguir el acceso de forma remota a plantas industriales de manejo de materiales (Bulk Handling) de manera que no sea necesario el desplazamiento de ningún operario a dicha planta para realizar las operaciones de mantenimiento necesarias.

Ya que el objetivo principal de este proyecto es la comunicación no se detallará el funcionamiento de este tipo de maquinaría sino que se citará brevemente para conocer el marco en el que se sitúa este documento.

En cuanto a las comunicaciones se procederá a un estudio de los requisitos para así poder realizar una elección adecuada acorde al sistema que se solicita.

1.2. ALCANCE DEL PROYECTO

En este documento se desarrollarán los aspectos necesarios para la realización de este proyecto, incluyendo esquemas de conexión, los componentes necesarios para llevar a cabo la realización del sistema y la configuración necesaria en los distintos componentes para que todo funciones de manera automática.

1.3. PETICIONARIO

Este proyecto ha sido realizado a petición de la empresa TSK Electrónica y Electricidad y de Antonio Robles (Tutor Académico del Proyecto) para la obtención del título **Master en Ingeniería de Automatización e Informática Industrial**.

1.4. SITUACIÓN DE LA PLANTA

Como ya hemos comentado con anterioridad este sistema va a ser implantado en maquinaria de manejo de materiales como por ejemplo en un puerto para cargar barcos o para almacenamiento de minerales.

En este proyecto no se abordará el funcionamiento de estas máquinas ya que para nosotros lo importante es la comunicación con el dispositivo que controla el funcionamiento del sistema.

A continuación se muestran unas imágenes a modo de muestra del aspecto de estas máquinas.

Ilustración 1 - Máquina Bulk Handling 1 (TSK)

Ilustración 2 - Maquinaria Bulk Handling en puerto (TSK)

Tras comentar brevemente el uso que se le va a dar, a continuación se describe el funcionamiento del sistema de acceso remoto.

Este proyecto constará de dos partes que desean tener una comunicación a través de la red pública de Internet con la diferencia que se necesitan unos requisitos de seguridad que por sí misma esta red no nos los proporcionan.

En este proyecto se desea poder controlar múltiples proyectos distribuidos demográficamente por todo el mundo, desde la oficina situada en la ciudad de origen de la empresa sin necesidad de acudir físicamente.

Esto es de vital importancia, no solo por el ahorro que supone a nivel logístico con los desplazamientos de los trabajadores si no que en caso de que sea un

error que provoque la parada total de la máquina también provoca pérdidas importantísimas hasta que el trabajador llegue y solucione el problema.

1.5. CONCEPTOS BÁSICOS

Para comprender este proyecto vamos a introducir los conceptos básicos estudiados previamente para la correcta elección de la solución definitiva. Al ser una comunicación remota a través de internet deberemos conocer de qué manera se transmiten los datos por esta red y cuáles son sus puntos de seguridad o falta de ella para ofrecer una comunicación segura entre la maquinaria de manejo de materiales (Bulk Handling) y el PC de acceso que estará situado en la oficina.

En primer lugar ya que se está hablando de redes de comunicación vamos a definir este concepto como un sistema capaz de proporcionar los elementos necesarios para intercambiar información a distancia.

Debido a que se está hablando de Internet se reflejará a continuación las características de la comunicación TCP/IP.

La comunicación TCP/IP está formada por cuatro capas que se detallan a continuación:

- **Capa de Aplicación**: Envío y recepción de datos para aplicaciones concretas tales como DNS, HTTP, etc.
- **Capa de Transporte**: Esta capa proporciona la comunicación para los datos de la capa de aplicación.
- **Capa de Red**: Esta capa consigue que los datos lleguen del origen al destino.
- **Capa de Datos:** Realiza la transferencia fiable de información a través del circuito.

Las redes TCP/IP no introducen por defecto mecanismos de seguridad. Por tanto, para obtener un esquema seguro es necesario añadir dichos mecanismos. A continuación se detallan las características que deben satisfacerse para proporcionar un acceso seguro.

Internet Protocol Securiry (IPsec) nace como un control de seguridad de la capa de red para proteger las comunicaciones. Se trata de un estándar realizado para garantizar la seguridad en las comunicaciones privadas establecidas a través de redes IP.

Dependiendo de cómo se implemente y configure IPsec puede proporcionar las siguientes protecciones:

- **Autenticación**: Consiste en determinar la verdadera identidad de los usuarios implicados.

- **Privacidad:** Se suele conseguir encriptando los datos con diversos algoritmos de cifrado para impedir que usuarios no autorizados puedan acceder a un contenido.

- **Integridad de los datos:** Consiste en asegurar que los datos no han sido modificados durante el envío. Esto suele garantizarse con códigos calculados a partir de los mensajes enviados que garantizan la integridad de la información enviada.

- **Autorización de usuarios:** Antes que un servidor ejecute la tarea solicitada se debe preguntar que el cliente está autorizado para hacer semejante tarea. Este término hace referencia a la necesidad de que una vez que se ha tomado una acción sobre el sistema bajo control, el usuario remoto no podrá denegar que el quien tomó una decisión determinada.

1.5.1.VPN

Dentro del conjuntos de protocolos IPsec, el método más utilizado para cumplir con los requerimientos anteriormente citados son los túneles VPN.

Se trata de la extensión, de forma segura, de una red local (LAN) a través de Internet.

La intención es la de proporcionar una comunicación segura entre el usuario remoto y la planta a supervisar.

Para implementar de manera segura una red VPN debemos realizar una planificación paso por paso para minimizar los potenciales peligros en el proceso. Estos pasos podemos dividirlos de la siguiente forma.

1. **Identificar los requisitos** para el acceso remoto y determinar como pueden cumplirse.
2. **Diseñar la solución.** Tomar las decisiones de diseño para el control de acceso y los métodos de autenticación.
3. **Implementar y probar un prototipo**
4. **Implementar la solución definitiva.**

Según estas pautas realizaremos nuestro proyecto para llevar a cabo una correcta comunicación libre de peligros y que garantice el correcto funcionamiento de la planta en todo momento**.**

Para poder seleccionar de forma correcta el túnel VPN vamos a proceder con la descripción de las posibles arquitecturas.

1.5.2. Arquitectura Gateway-to-Gateway

Para proporcionar seguridad entre dos redes se despliega una puerta de enlace en cada red, estableciendo posteriormente la conexión VPN entre las dos puertas de enlace. El tráfico entre las dos redes, que necesita ser asegurado, pasa por la VPN realizada entre las dos puertas de enlace. Esta puerta de enlace en cada una de las redes puede implementarse mediante un cortafuegos o un router.

Ya que en la planta remota para la que se está estudiando el caso no existirá una red local, no podremos realizar el túnel VPN de esta forma.

1.5.3. Arquitectura Host-to-Gateway

Este método de conexión es el más utilizado para proporcionar un acceso remoto seguro. La empresa, en este caso la oficina de Gijón de TSK implementa una puerta de enlace VPN en la red local.

Con este modelo se crean conexiones IPsec según se vayan necesitando por cada usuario. Serán clientes remotos del servidor central situado en la oficina.

Cuando la planta necesite comunicarse, iniciará la comunicación con la puerta de enlace de la red local y se le pedirán unas credenciales para autenticarse antes de establecer la comunicación. De esta forma será un equipo más de la red local con los recursos informáticos que se le hayan establecido.

1.5.4. Arquitectura Host-to-Host

Es la arquitectura menos utilizada, ya que normalmente se utiliza para necesidades de propósito especial, como gestión remota de un solo servidor.

Para este modelo se crearan las conexiones IPsec según sea necesario para cada usuario VPN.

A continuación vamos a presentar un cuadro en el que resumiremos las características de cada tipo de arquitectura.

Característica	**Gateway-to-gateway**	**Host-to-gateway**	**Host-to-host**
Proporciona una protección entre el cliente y puerta de enlace local	NO	X	X
Proporciona protección entre los puntos finales de VPN	SI	SI	SI
Proporciona protección entre la puerta de enlace remota y el servidor remoto (detrás de la puerta de enlace)	NO	NO	X
Transparente para los usuarios	SI	NO	NO
Transparente para los sistemas de los usuarios	SI	NO	NO
Transparente para los servidores	SI	SI	NO

Debido a la complejidad en la implementación de una solución mediante IPsec, se ha decidido buscar una alternativa mediante SSL (Secure Sockets Layer), la cuál describiremos a continuación.

1.5.5. SSL

El protocolo SSL (Secure Sockets Layer) proporciona comunicaciones seguras dentro de una red, que normalmente será internet.

Mediante este protocolo podemos proporcionar autenticación y privacidad de la información intercambiada por los extremos de la comunicación mediante el uso de la criptografía.

Para satisfacer este protocolo se deben cumplir las siguientes fases:

- Se negociará entre las dos partes el algoritmo que se usará en la comunicación.
- Se intercambiarán las claves públicas y el modo de autenticación.
- Una vez echo esto se cifrará el trafico entre las partes.

En este protocolo se usan certificados para autentificar a la contraparte con quien se están comunicando, y para intercambiar una llave simétrica. Esta sesión es luego usada para encriptar el flujo de datos entre las partes. Esto permite la confidencialidad del dato/mensaje.

Varias versiones de este protocolo son utilizadas por nosotros en nuestro día a día ya que las implementan aplicaciones ampliamente tan conocidas como navegación web, correo electrónico, fax por Internet, mensajería instantánea, y voice-sobre-IP (VoIP).

Así mismo, podemos añadir que existen aplicaciones sencillas que permiten configurar una comunicación mediante el protocolo SSL, cosa que no sucedía con IPsec.

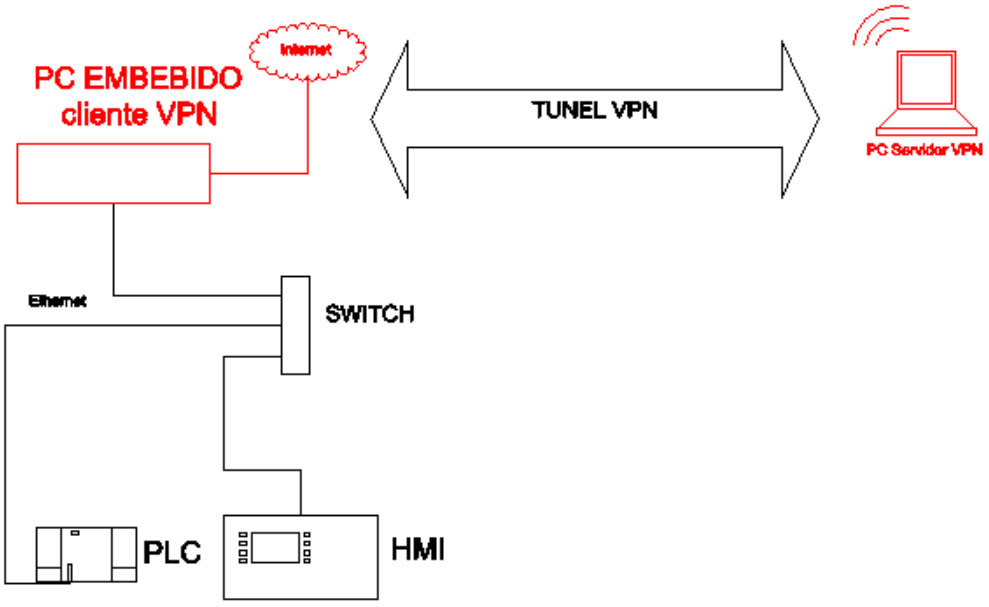
Debido a esto se ha decidido implementar la solución mediante OpenVPN, una aplicación sencilla que nos permitirá disponer de una comunicación segura a través de internet mediante un túnel VPN.

2.1. SELECCIÓN DE LA SOLUCIÓN

En el apartado anterior hemos explicado los requisitos básicos necesarios para implementar una VPN con garantías de funcionamiento seguro y las posibles arquitecturas de las que disponemos para llevarlo a cabo.

Como también se cito anteriormente se va a implementar la solución con un software llamado OpenVPN que implementa una comunicación mediante SSL. En nuestro caso el CLIENTE será el PC situado a bordo de máquina que solicitará la conexión con un PC que hará de SERVIDOR.

Para ello es necesario seguir unos pasos que se detallan a continuación basados en tutoriales que se proporcionan con la aplicación.



En primer lugar descargaremos la aplicación para nuestro sistema operativo, en este caso lo vamos a explicar todo para Windows.

Una vez instalada la aplicación lo primero que debemos hacer será la creación de las claves públicas y privadas.

Crear las llaves para el servidor

EL software OpenVPN usa el protocolo SSL para cifrar los datos enviados por internet, y se cifran para que no nos roben datos privados si llegan a ser interceptados.

EL OpenVPN se suele instalar en la carpeta C:\Archivos de Programa\OpenVPN, por lo tanto vamos a comenzar a realizar los siguientes pasos:

Abrimos el terminal de Windows: Inicio → Ejecutar → CMD

Estando en el terminar nos dirigiremos al directorio easy-rsa de OpenVPN

cd C:\Archivos de Programa\OpenVPNeasy-rsa

Ahora ejecutamos el siguiente comando

init-config

En los pasos siguientes, se nos va a pedir varias veces diferentes datos como País, Estado, Ciudad, Organización, Departamento, Nombre del Servidor y Correo.

Después ejecutaremos los siguiente comandos uno a uno.

vars

clean-all

build-ca

El comando build-ca pedirá valores como Pais, Estado, Ciudad, Organización, Departamento, Nombre del Servidor y Correo, todos estos valores se deben repetir durante todo el proceso cada vez que nos los pida, a excepción del nombre del host (hostname) que cambiará en la parte de configuración de las llaves del cliente.

Lo que hemos hecho hasta ahora es crear el Certificado de Autoridad, que ha sido creado en el directorio *C:\Archivos de Programa\OpenVPN\easy-rsa\keys* junto con varios archivos que usaremos más adelante.

El siguiente paso es crear la llave privada y certificado del servidor.

Para hacer esto ejecutamos los siguientes comandos.

vars

build-key-server NombreDelServidor

Este comando al final nos hará dos preguntas adicionales, a las cuales debemos responder que sí, poniendo la letra "*y".*

Aquí volverá a pedir los datos, los cuáles deben ser los mismos introducidos anteriormente. Además, también pedirá una contraseña que debe ser usada cuándo se creen las llave de los clientes.

Luego ejecutaremos el siguiente comando:

build-dh

En este punto ya hemos creado todas las llaves para el servidor. Ahora vamos a crear las llaves para el cliente.

Crear las llaves del Cliente

Es muy recomendable que por cada cliente que se vaya a usar creen un clave diferente.

Desde la consola estando ubicados en el directorio.

C:\Archivos de programa\OpenVPN\easy-rsa

Ejecutaremos los siguientes comandos.

vars

build-key NombreDelCliente

Nuevamente nos hará las mismas preguntas, en las que solo cambia el hostname. Debemos poner la misma contraseña que pusimos a las llaves del servidor, y si vamos a crear llaves para varios clientes, estas deben tener un Nombre diferente.

En este punto ya tenemos creadas las llaves del cliente y del servidor. Así que los pasos siguientes son configurar el servidor.

Configurar el servidor

Crear una conexión de puente

Cuando instalamos el OpenVPN, se instaló un adaptador de red. Este adaptador es la base del funcionamiento de OpenVPN. Debemos cambiarle el nombre y crear un puente entre el adaptador de red normal (con el que tenemos acceso a internet) y el creado por el programa al instalarse.

Para esto procederemos de la siguiente forma:

- En el Panel de Control, vamos a Conexiones de Red. y renombramos el “Conexión de Área local n” (TAP-Win32 Adapter V9) poniéndole el nombre que queramos.

- Seleccionamos los dos adaptadores de red (el de OpenVPN y el de la red que nos da el acceso a internet), hacemos clic derecho y luego conexiones de puente (también puede poner Crear Puente de Red). Este proceso tardará un poco, mientras se crea el puente.

Con estos pasos ya tenemos creado el puente.

Configuración de la autenticación y la red

Lo siguiente que debemos hacer es ver los archivos que se generaron en el directorio *C:\Archivos de programa\OpenVPN\easy-rsa\keys,* de todos los archivos que hay los más importantes son los siguientes:

NombreDelServidor.crt

NombreDelServidor.key

ca.crt

dh1024.pem

NombreDelCliente.crt

NombreDelCliente.key

Esto es importante, porque todos estos archivos debemos copiarlos al directorio *C:\Archivos de programa\OpenVPN\config.*

Una vez copiados, lo siguiente que vamos a hacer será crear el archivo de configuración del servidor en este mismo directorio, con el nombre de server.ovpn este archivo tendrá el siguiente contenido (basado en el archivo que está en el directorio samples).

```
# Which TCP/UDP port should OpenVPN listen on?

# Aqui va el puerto donde escuchará el servidor OpenVPN, este puerto debe estar abierto en el firewall y
 #redireccionado en el router.

port 1194
```

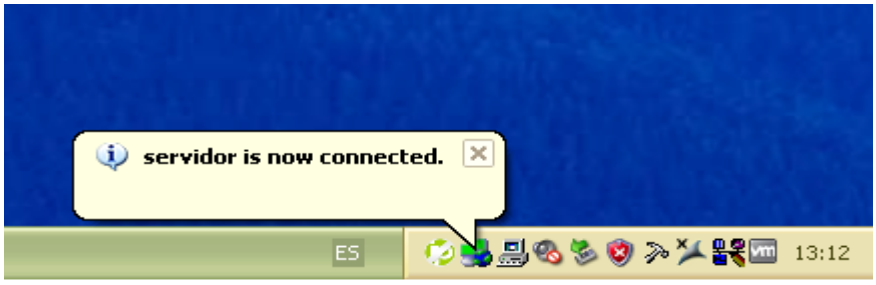
```
# TCP o UDP.


proto tcp


#Como vamos a usar la red Puenteada usamos tap, en caso de ser enrutada sería tun.


dev tap

;dev tun


 #Aqui debe ir el nombre que le pusimos al Adaptador de red, del OpenVPN.


dev-node TAP


#Lo siguiente es indicarle al servidor cuales son los archivos que tienen las llaves.


ca ca.crt

cert servidor.crt

key  servidor.key  # Este archivo debe ser SECRETO!


# Parámetros Diffie hellman.

# Asegurarse de haber copiado este archivo en el directorio config


dh dh1024.pem
```

```
# log donde se guardará la IP virtual del cliente.

ifconfig-pool-persist ipp.txt

#Aqui van los datos en este orden.
#     IPLocal del Servidor Mascara de subred, primer IP de los clientes, última IP de los clientes

server-bridge 192.168.1.104 255.255.255.0, 192.168.1.106, 192.168.1.110

# Activar el servidor como puente.

server-bridge

# En caso de haber varios clientes, y se desea que un cliente pueda ver a otro cliente,
# quítarle el ; a la siguiente línea

;client-to-client

# Si se desea que varios clientes se puedan conectar con la misma firma quítar el ; a la siguiente línea
#Esto no es recomendado, es mejor crear una llave para cada cliente.

;duplicate-cn
```

```
# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.

keepalive 10 120

# Enable compression on the VPN link.
# If you enable it here, you must also
# enable it in the client config file.

comp-lzo

# Descomentar esta linea si quieres dar un límite de
clientes conectados simultaneamente

;max-clients 100

# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.

persist-key
```

```
persist-tun


# Log de Estado

status openvpn-status.log

# Set the appropriate level of log
# file verbosity.
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose

verb 3
```

Ahora lo único que queda será abrir la aplicación OPENVPN GUI que se instaló y activar el servidor, cuando termine este proceso veremos cómo en la barra de herramientas se pondrá el icono del servicio en verde con el mensaje ***"NombreDelServidor is now connected"***.



Configurar el cliente

El objetivo del cliente es poder conectarse al servidor, por lo que desde el pc del cliente también se tiene que hacer un procedimiento, para que las dos redes locales queden conectadas.

Lo primero es descargar el OpenVPN. Después de instalarlo debemos dirigirnos al directorio de instalación (*C:\Archivos de programa\OpenVPN*) donde encontraremos los directorios que necesitaremos.

El primero en el que nos deberemos fijar es en el de sample-config, de donde cogeremos el archivo client.ovpn y lo copiaremos al otro directorio que nos interesa, el directorio config.

Posteriormente copiamos los tres certificados creados en la parte del servidor:

ca.crt

NombreDelCliente.crt

NombreDelCliente.key

Ahora tenemos que abrir el archivo de configuración client.ovpn con el Bloc de notas (importante abrir el editor como administrador). Aquí básicamente deberemos configurar tres cosas*: la dirección de nuestro servidor OpenVPN, la ruta hacia los certificados anteriormente citados y forzar que todo el tráfico se envíe a través de la VPN.*

```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
```

```
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.

client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.

dev tap
;dev tun
# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.

dev-node TAP

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
```

```
proto tcp
;proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.

remote pruebaremoto.ddns.net 1194
;remote 192.168.10.105 1194




# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.

;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.

resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
```

```
Nobind

# Downgrade privileges after initialization (non-Windows only)

;user nobody
;group nobody



# Try to preserve some state across restarts.

persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.

;http-proxy-retry

# retry on connection failures
```

```
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.

;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use

# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.

ca ca.crt
cert cliente.crt
key cliente.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:

#  http://openvpn.net/howto.html
#mitm
```

```
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.

ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.

;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.

;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.

comp-lzo

# Set log file verbosity.

verb 3
```

```
# Silence repeating messages

;mute 20
```

Ya hemos terminado, ejecutamos el programa y se conectará al servidor asignando una IP en el rango del servidor para que estén las dos LAN comunicadas.

Como podemos observar, para todos los pasos citados es necesario que una persona ejecute el programa y proceda con la conexión desde el cliente pero en nuestro caso no existe ni pantalla en el PC a bordo de máquina ni un operario que este continuamente ejecutando dicha secuencia por lo tanto debemos realizar una configuración que nada tiene que ver con el software, para que la conexión se produzca automáticamente siempre que este PC esté conectado a internet.

Para ello debemos seguir los pasos que se detallan a continuación.

En primer lugar debemos eliminar del registro de Windows el arranque de OpenVPN GUI:

"[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] "openvpn-gui"="C:\\Archivos de programa\\OpenVPN\\bin\\openvpn-gui.exe"

Para ello nos dirigimos al [Panel de Control] [Herramientas Administrativas] [Servicios] y buscamos OpenVPN Service. Aquí vamos a ver que está en modo manual, por tanto lo pasaremos a modo Automático y con OpenVPN ya parado arrancamos el programa.

Al cabo de unos segundos la tarjeta TAP que se instaló con el software comenzara a tener conexión sin realizar ninguna acción.

3.1. DESCRIPCIÓN DE LOS COMPONENTES

Para la realización de este proyecto se han utilizado los siguientes componentes:

1. PC Embebido NanoBox Simatic IPC227D (PC a bordo de máquina)
2. Router Vodafone B1000 4G LTE (Conexión a la red en la oficina central)
3. Modem USB Vodafone (Conexión a la red para el PC Embebido)

3.1.1. PC Embebido NanoBOX Simatic IPC227D

Un Pc Embebido tiene una arquitectura muy parecida a la de un PC que todos usamos a diario, por lo que pasamos a describir los componentes que son susceptiblemente diferentes de los que posee nuestro PC.

Microprocesador

Es el encargado de realizar las operaciones de cálculo principales del sistema. Ejecuta código para realizar una determinada tarea y dirige el funcionamiento de los demás elementos que le rodean. Suelen ser menos potentes que los del PC normal ya que están diseñados para el uso en algo concreto y no para la variedad de uso que le damos nosotros.

Memoria

En ella se encuentra almacenado el código de los programas que el sistema puede ejecutar así como los datos. Su característica principal es que debe tener un acceso de lectura y escritura lo más rápido posible para que el microprocesador no pierda tiempo en tareas que no son meramente de cálculo. Al ser volátil el sistema requiere de un soporte donde se almacenen los datos incluso sin disponer de alimentación o energía. La memoria de estos

dispositivos cada vez es mayor pero sigue lejos de la que tiene el PC de nuestra casa o nuestro portátil.

Disco duro

En él la información no es volátil y además puede conseguir capacidades muy elevadas. A diferencia de la memoria que es de estado sólido éste suele ser magnético. Pero su excesivo tamaño a veces lo hace inviable para PC's

embebidos, con lo que se requieren soluciones como unidades de estado sólido. Otro problema que presentan los dispositivos magnéticos, a la hora de integrarlos en sistemas embebidos, es que llevan partes mecánicas móviles, lo que los hace inviables para entornos donde estos estarán expuestos a ciertas condiciones de vibración.

Ranuras de expansión para tarjetas de tareas específicas

Pueden no venir incorporadas en la placa base. Un PC estándar suele tener muchas más ranuras de expansión que un PC embebido. Las ranuras de expansión están asociadas a distintos tipos de bus: VESA, ISA, PCI, NLX (ISA + PCI), etc.

La imagen anterior muestra el PC embebido con el que se ha realizado este proyecto, llamado NanoBOX Simatic IPC 227D.

Las principales características de este dispositivo son las siguientes.

	Fabricante	RAM	Procesador	Memoria	Sistema Operativo
NANOBOX IPC227D	**SIEMENS**	2 GB	2 GHz	320 GB	Windows XP
					Windows 7

3.1.2. Router Vodafone B1000 4G LTE

Es evidente que necesitamos conectaron a internet y para las pruebas se ha decidido realizar las mismas con un router de Vodafone que lleva una tarjeta SIM dentro que es la que proporciona el acceso a internet pero a la hora de implantarlo en la realidad no es de obligatorio cumplimiento que sea este el que se vaya a usar.

La principal característica es la anteriormente citada y es que la tarjeta va internamente oculta y no es necesario tener un proveedor de internet con una cobertura de datos o una instalación de fibra o cobre si no que con la red GPRS que usamos para navegar con nuestro Smartphone podemos tener acceso a la planta.

Otra de las características por las cuales usamos este router es porque posee interiormente el servicio de DNS dinámico para poder estar localizados por la planta en todo momento ya que la la IP de la que disponemos es dinámica.

3.1.3. Modem USB Vodafone

Necesitaremos también que la planta remota este conectada a Internet para asi poder acceder desde cualquier lugar en el que nos encontremos. Para ellos en este caso hemos utilizado un modem USB de Vodafone ya que la empresa en la que nos encontramos cuenta con un contrato con esta marca y así nos lo han facilitado.

Simplemente se debe conectar a un puerto USB del PC para estar conectados a la red.

4.1. PRESUPUESTO

PRESUPUESTO MATERIALES				
COMPONENTE	CANTIDAD	FABRICANTE	PRECIO/UNIDAD	TOTAL
NANOBOX IPC227D	1	SIEMENS	1190,00	1190,00
ROUTER VODAFONE B1000 4G LTE	1	VODAFONE	*	*
Modem USB Vodafone	1	VODAFONE	*	*
			TOTAL	**1190,00**

DOCUMENTACION Y CODIGO				
OPERACIÓN	DURACIÓN(h)	OPERARIO	PRECIO/UNIDAD(€)	TOTAL(€)
Implementación del código	5	Ingeniero Técnico	29,00	145,00
Documentación	15	Ingeniero Técnico	29,00	435,00
			TOTAL	**580,00**

CONSTRUCCIÓN DE LA PCB				
OPERACIÓN	DURACIÓN(h)	OPERARIO	PRECIO/UNIDAD(€)	TOTAL(€)
DISEÑO	3	Ingeniero Técnico	29,00	87,00
CONSTRUCCION	1,5	Oficial 1ª Electrónico	17,00	25,50
			TOTAL	**112,50**

PRESUPUESTO DE EJECUCIÓN MATERIAL	
CONCEPTO	TOTAL(€)
Materiales	1190
Documentación y Código	580,00
Construcción de la PCB	112,50
TOTAL	**1882,5**

INVERSIÓN	
CONCEPTO	TOTAL(€)
Presupuesto de Ejecución Material	1882,5
12% Beneficio Industrial	225,90
TOTAL	**2108,40**

PRESUPUESTO DE LA EJECUCIÓN POR CONTRATA	
CONCEPTO	TOTAL(€)
Inversión	2108,40
21% I.V.A.	442,76
TOTAL	**2551,16**

* El precio correspondiente al modem y router dependerá de la compañía con la que se contrate el servicio de Internet, por tanto no se puede especificar un precio exacto.

5.1. CONCLUSIONES

Para adoptar esta solución como la más segura y apropiada para el caso que nos acontece hemos realizado un estudio de todos los dispositivos/soluciones integradas que existían en el mercado a día de hoy. Esta información se adjunta como anexo para que se pueda comprobar las características de cada uno.

En este anexo se han implementado soluciones de software exclusivamente, es decir sin un dispositivo cortafuegos.

Túnel VPN PPTP

Microsoft desarrollo el protocolo PPTP para permitir a las personas acceder remotamente y de forma segura a las redes locales a través de Internet. Los datos son encapsulados antes de su transporte a través de IP mediante Internet.

La ventaja más destacable de PPTP es su facilidad a la hora de configuración y uso frente al protocolo L2TP (Layer 2 Tunnneling Protocol). Los datos son encriptados sin IPsec, lo cual implica que no es necesario instalar ningún certificado de equipo ni una aplicación de clave pública (PKI).

Al no usar IPsec, tiene como inconveniente que su seguridad es más pobre en comparación con L2TP. No tiene verificación de origen, lo cual implica que no se puede confirmar la integridad de los datos.

Túnel VPN L2TP

Debido a que L2TP utiliza IPsec, no sólo encripta los datos, sino que también ofrece seguridad adicional que PPTP no nos ofrecía.

Al contrario que PPTP, L2TP ofrece integridad de datos y autenticación de los datos de origen. Otra ventaja es el uso de UDP para encapsular los datos, lo que hace L2TP más rápido y más fácil de configurar con algunos firewalls. Con otros firewalls, L2TP puede tener una ligera desventaja en la velocidad, ya que encapsula los datos dos veces.

La desventaja más reseñable sobre este tipo de túnel es que necesitamos mucha más configuración que con PPTP y además necesitamos incluir PKI y certificados de equipo.

Túnel VPN mediante OpenVPN

OpenVPN ofrece seguridad mediante sus mecanismos de cifrado sin necesidad de realizar una compleja configuración como hemos visto en las soluciones anteriores.

No necesitamos tanta configuración ya que poseemos la parte del servidor en nuestro PC en la cual nos muestra toda la información necesaria para poder acceder al equipo remoto.

De esta forma nos comunica la IP pública del equipo remoto y nos revela la IP que se le ha asignado en nuestra red local para así poder acceder a él con una dirección en nuestro rango.

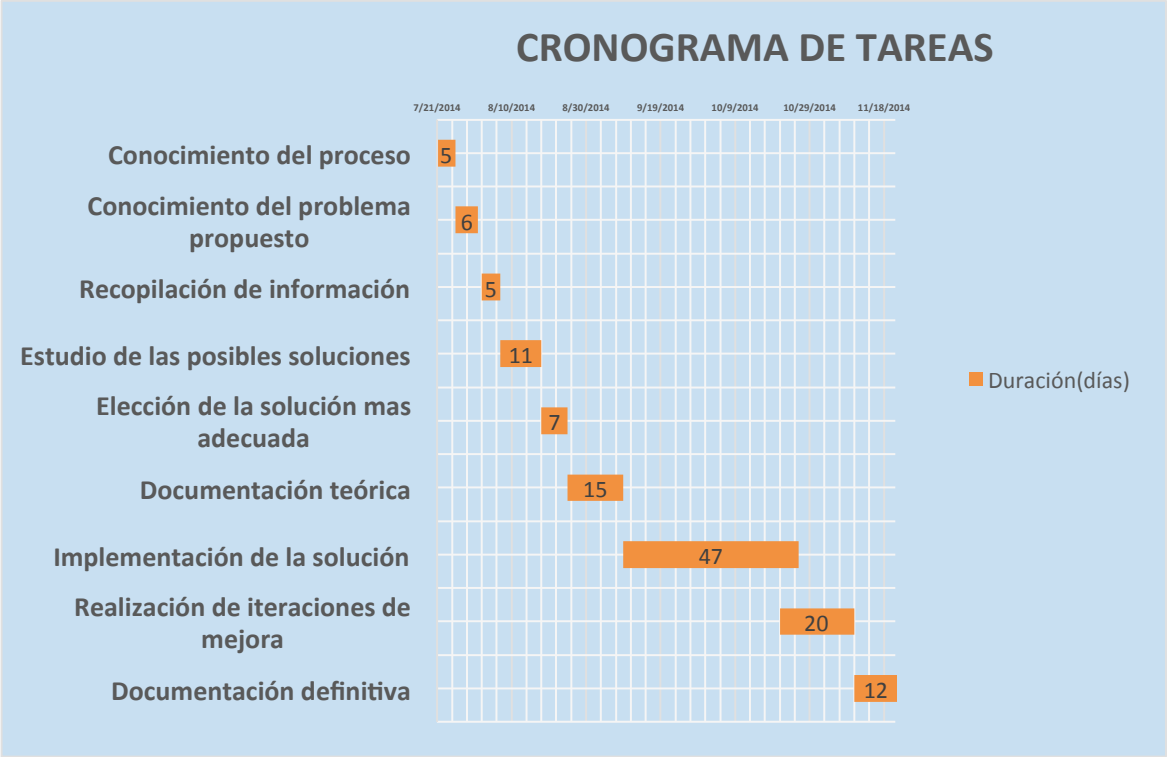
Con una aplicación de escritorio remoto indicaremos dicha IP y así pasaremos a controlar el equipo a distancia.

En cuanto a costes no tiene comparación ya que se trata de un software libre y que requiere de unos pasos sencillos para dejar el sistema completamente operativo para el acceso de forma remota para el mantenimiento y supervisión de las máquinas de Bulk Handling para lo cual fue propuesto este proyecto.

6.1. PLANIFICACIÓN

Este proyecto ha sido realizado en diferentes etapas secuenciales, las cuales son:

Etapa	Actividad	Inicio	Duración(días)	Fin
1	Conocimiento del proceso	21/07/2014	5	25/07/2014
2	Conocimiento del problema propuesto	26/07/2014	6	01/08/2014
3	Recopilación de información	02/08/2014	5	06/08/2014
4	Estudio de las posibles soluciones	07/08/2014	11	17/08/2014
5	Elección de la solución más adecuada	18/08/2014	7	24/08/2014
6	Documentación teórica	25/08/2014	15	08/09/2014
7	Implementación de la solución	09/09/2014	47	20/10/2014
8	Realización de iteraciones de mejora	21/10/2014	20	09/11/2014
9	Documentación definitiva	10/11/2014	12	21/11/2014



7.1 BIBLIOGRAFÍA

Libros:

Redes de Computadoras (Cuarta Edición)

Editorial: PEARSON Prentice Hall

Autor: Andrew S. Tanenbaum

Autómatas Programables

Editorial: MARCOMBO

Autor: Josep Balcells y José Luis Romeral.

Publicaciones:

Metodologías de acceso remoto a plantas industriales

Autor: Isidro Calvo Gordillo.

Supervisión y control de procesos

Autores: David Chacón, Oscar Dijort, Jacinto Castrillo

Catálogos de fabricantes:

SIEMENS	www.siemens.com
WEIDMULLER	www.weidmuller.es
EWON	www.ewon.es
HMS	www.hms-networks.com
BOMGAR	www.bomgar.com
CISCO	www.cisco.com

ANEXO 1.
ALTERNATIVAS

Alternativa Linux – Servidor PPTP de VPN

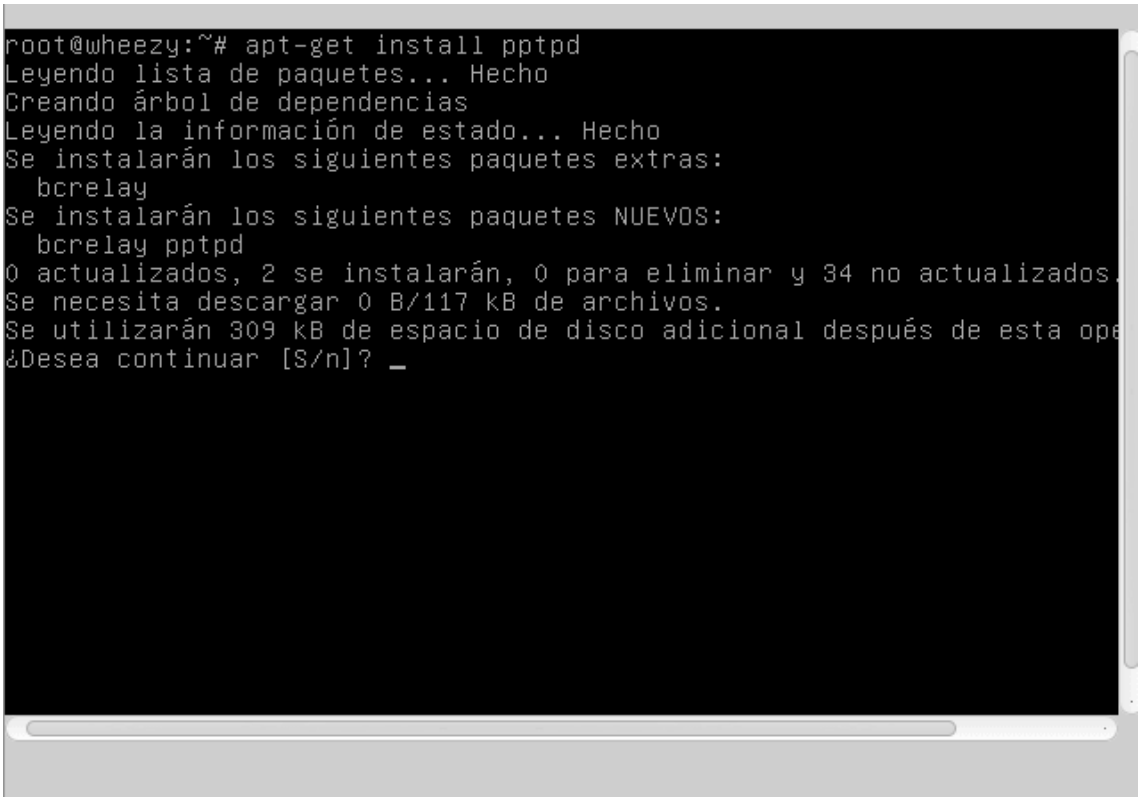
Ya que tener un servidor con Windows sería equiparable o más costoso económicamente que la solución propuesta con el SCALANCE S612 de Siemens hemos decidido investigar una posible solución "libre" mediante el Sistema Operativo LINUX.

Para ello disponemos de la versión más actualizada Ubuntu, la versión 14.04. Debido a que es una configuración a través de terminal a continuación realizaremos un pequeño manual/tutorial de los pasos necesarios para implementar esta solución.

Instalar el servidor

Lo primero es instalar el servidor VPN en nuestro PC:

sudo apt-get install pptpd



Asegurar que nuestro Servidor VPN tenga IP interna fija

Disponer de una IP fija o estática es extremadamente útil básicamente por dos motivos:

1. Si no disponemos de una IP fija, cuando se reciba una petición a nuestro servidor desde el exterior, nuestro router no sabrá donde tiene que redireccionarla ya que la IP del servidor puede ser cualquiera.
2. En el caso que necesitemos conectarnos a un ordenador de nuestra red local, si nuestros ordenadores no disponen de ip fija o estática entonces no sabremos a que equipo estamos dirigiendo nuestra petición.

Copia de seguridad del archivo de configuración

Para conseguir que nuestro servidor o equipo disponga de una IP fija o estática solamente tenemos que seguir unos pasos muy simples. No obstante para evitar todo tipo de riesgo lo primero que realizaremos es realizar una copia de seguridad del fichero /etc/network/interfaces.

Para generar la copia de seguridad lo que haremos es introducir el siguiente comando en la terminal:

```
cp /etc/network/interfaces /etc/network/interfaces.bak
```

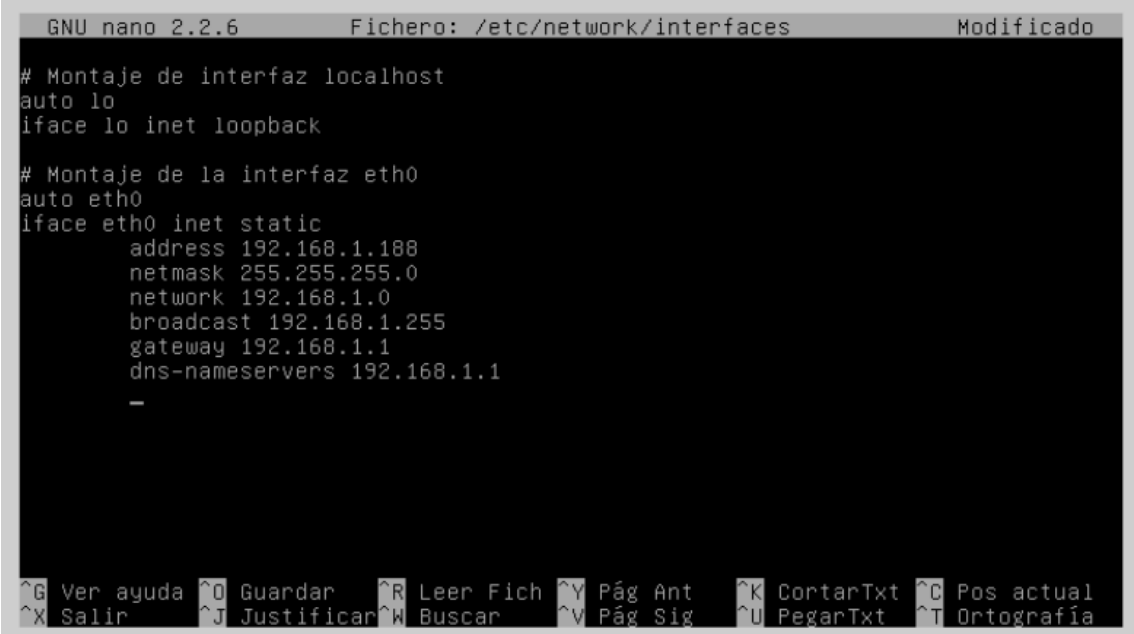
Una vez realizada la copia de seguridad en la ventana de comandos pasaremos a configurar nuestra IP fija.

Pasos para la configuración de una IP fija o estática

Una vez realizados los pasos iniciales pasamos a configurar nuestra red con IP fija o estática. Para ello en el terminal tecleamos el siguiente comando:

```
sudo nano /etc/network/interfaces
```

Una vez tecleado el comando en el terminal se abrirá el editor de textos. Una vez abierto el editor de texto tendremos que reemplazar el contenido existente por el que se muestra en la siguiente captura de pantalla:



El significado de cada uno de los parámetros que se pueden ver en la captura de pantalla es el siguiente:

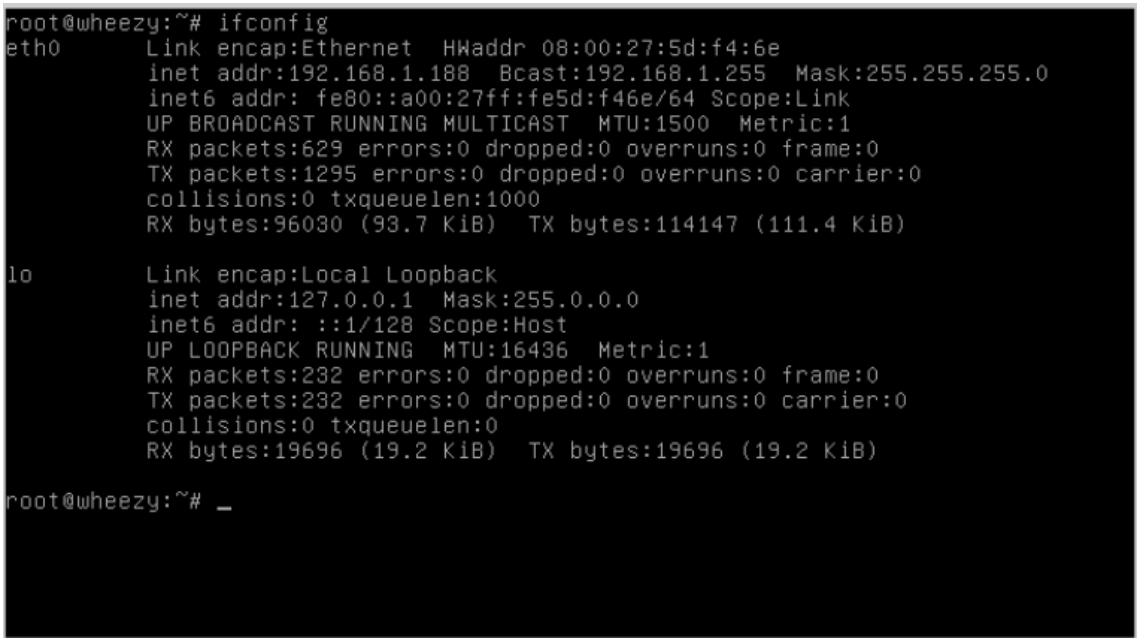
Comando 1 : “auto lo”: Este comando lo que hace es iniciar la interfaz lo (Loopback) automáticamente durante la secuencia de arranque.

Comando 2 : “iface lo inet loopback”: Con este comando lo que estamos haciendo es definir los parámetros de la interfaz lo para IP’s del tipo IPV4. Los parámetros de configuración de esta interfaz se introducen automáticamente en el momento de activar la red.

Comando 3 : “auto eth0”: Este comando lo que hace es iniciar la interfaz eth0 durante la secuencia de arranque del ordenador.

Nota: Es posible que en vuestro caso tengáis que modificar el parámetro eth0 por otro diferente como por ejemplo wlan0, eth0, eth1, etc. Para saber el nombre de interfaz lo podemos hacer introduciendo el siguiente comando en la terminal:

sudo ifconfig –a



Como se puede ver en la captura de pantalla nosotros disponemos únicamente de una interfaz configurable que se reconoce con el nombre eth0. También observamos que nuestra IP actual es la 192.168.1.188 y que nuestra máscara de subred es la 255.255.255.0. Con esta información deducimos que estamos a conectados a una red de clase C que podrá admitir 254 host o usuarios.

Comando 4 : “iface eth0 inet static”: Con este comando lo que estamos indicando es que una vez habilitada la interfaz eth0 se asigne una IP fija o estática del tipo IPV4 a nuestro ordenador. La IP y tipo de red se nos asignará en función de los parámetros que estableceremos en los comandos que van del 5 al 10.

Comando 5 : “address: 192.168.1.188”: En el campo address hemos puesto 192.168.1.188 que se trata de una dirección IP reservada para redes de tipo clase C. Se ha puesto esta IP porqué es la IP que queremos que se asigne a nuestro ordenador como ip fija o estática. En principio podemos elegir cualquier ip comprendida entre la dirección de red (network) y la dirección broadcast.

Nota: Las direcciones IP reservadas para redes clase C van desde 192.168.0.0 hasta 192.168.255.255. Por lo tanto en este campo podríamos haber elegido otras IP como por ejemplo 192.168.100.14, 192.168.0.3, etc. En función de la IP que elijamos hay que tener en cuenta la modificación del resto de parámetros como por ejemplo pueden ser la puerta de entrada, la dirección broadcast, etc.

Comando 6 : “netmask: 255.255.255.0”: Hemos que nuestra máscara de red sea 255.255.255.0. Prácticamente el 100% de redes domésticas utilizan está

máscara de red. La máscara de red define el número máximo de ordenadores o host que puede tener nuestra red. Al usar 255.255.255.0 el número máximo será de 254 ordenadores. En el caso de necesitar construir una red de más de 254 ordenadores tendríamos que montar una red clase B que nos permitirá llegar a tener hasta 65534 ordenadores.

Nota: A modo de ejemplo. Si quisiéramos limitar el número de ordenadores que pueden conectarse a nuestra red a 32, tan solo deberíamos modificar la máscara de red a 225.255.255.224.

Nota: Para cambiar a una red tipo B tendríamos que usar una máscara de red del tipo 255.255.0.0. Las IP que tienen reservadas para las redes de tipo B son 172.16.0.0 a 172.31.255.255.

Comando 7 : “network: 192.168.1.0”: En el campo dirección de red hemos puesto 192.168.1.0 ya que queremos que la IP que identifique la totalidad de la red sea 192.168.1.0. En otras palabras 192.168.1.0 representará a la totalidad de dispositivos conectados a nuestra red. Normalmente con IPv4 la dirección más baja del rango de IP se reserva para hacer referencia a la totalidad de host de la red.

Comando 8 : “broadcast: 192.168.1.255”: Como dirección broadcast ponemos 192.168.1.255. Esta dirección se podrá usar para comunicarse y enviar paquetes a la totalidad de equipos que forman parte de una misma red. La dirección broadcast es la dirección más alta de la red. En nuestro caso como la puerta de entrada es 192.168.1.1 y la máscara de subred es el 255.255.255.0 la dirección broadcast será 192.168.1.255.

Comando 9 : “gateway: 192.168.1.1”: En este campo hay que definir la puerta de entrada del router que en este caso es 192.168.1.1. Este parámetro se puede modificar en vuestro router pero la gran mayoría de personas acostumbra a tener IP 192.168.1.1. Para poder consultar o modificar la puerta de entrada tan solo hay que acceder al apartado LAN de la configuración del router:

Comando 10 :”dns-nameservers: 192.168.1.1:” En los dns-namservers hemos puesto 192.168.1.1 ya que es la puerta de entrada de nuestro Router. De esta forma estamos definiendo que las peticiones DNS de nuestro ordenador sean resueltas mediante los DNS de nuestro proveedor de Internet (ISP). En el caso que se quiera usar otros DNS, como por ejemplo los de google, tan solo tenemos que reemplazar 192.168.1.1 por 8.8.8.8.

Una vez realizados todos los pasos podemos estar seguros que tendremos una IP fija. Por lo tanto siempre que arranquemos nuestro servidor tendremos la misma IP.

Aplicar los cambios de la configuración

Una vez finalizada la configuración tan solo tenemos que reinicializar nuestra red. Para ello tecleamos el siguiente comando:

```
sudo service networking restart
```

En el caso que se precise activar o desactivar alguna interfaz tan solo tenemos que teclear la siguiente serie de comandos.

Para desactivar una interfaz teclearemos:

```
sudo ifdown “nombre de la interfaz”
```

Para activar una interfaz teclearemos:

```
sudo ifup “nombre de la interfaz”
```

Por lo tanto si queremos desactivar la interfaz eth0 teclearemos:

```
sudo ifdown eth0
```

Si a posteriori queremos activar de nuevo la interfaz eth0 teclearemos el siguiente comando en la terminal:

```
sudo ifup eth0
```

Servicio de redireccionamiento dinámico

Para conectarnos desde el exterior tenemos que conocer la IP Pública de nuestro servidor que en la mayoría de casos será dinámica o variable. Esto significa que en el momento de conectarnos es posible que no sepamos la IP Pública de nuestro servidor. Para solucionar este problema lo que vamos a realizar es asociar la IP Pública de nuestro servidor VPN con un dominio fácil de recordar.

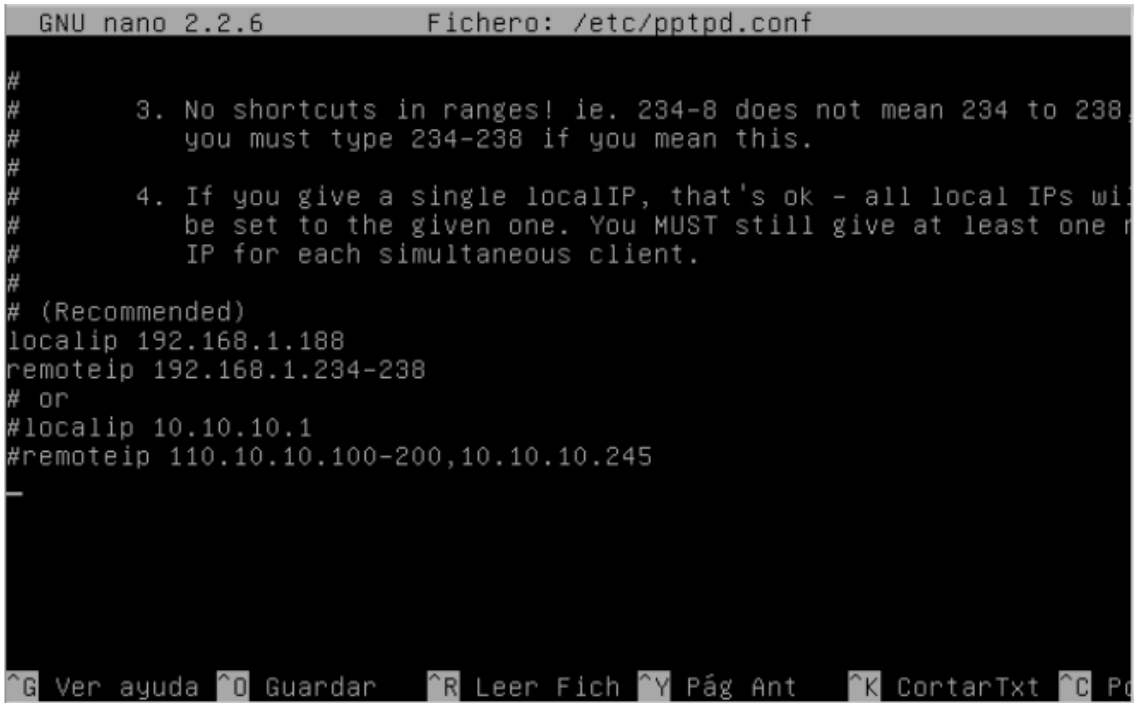
Para asociar vuestra dirección IP Pública a un subdominio tan solo tiene que seguir los pasos que se detallan en el Anexo 1.

Configurar el servidor

Para configurar nuestro servidor tenemos que introducir el siguiente comando en el terminal:

sudo nano /etc/pptpd.conf

Como se puede ver en la imagen, una vez tecleado el comando se abrirá el editor de texto en el que podremos modificar la configuración de nuestro servidor.



En este fichero únicamente vamos a modificar dos parámetros:

- El primero de los parámetros a modificar es localip. En localip tenemos que poner la IP interna de nuestro servidor VPN. Como hemos visto en apartados anteriores la ip de nuestro servidor VPN es la 192.168.1.188. Por lo tanto tenemos asegurarnos que el siguiente comando estará introducido en el navegador:

  localip 192.168.1.188

- El segundo de los parámetros a modificar es remoteip. En remoteip tenemos que indicar un rango de IP que serán las que nuestro servidor asignará a los PC's clientes que se conecten a nuestro servidor VPN. En nuestro caso hemos asignado el siguiente rango:

  remoteip 192.168.1.234-238

Por lo tanto en el servidor VPN que acabamos de configurar como máximo se podrán conectar 4 clientes de forma simultánea que tendrán una IP comprendida entre 192.168.1.234 – 192.168.1.238. Una vez el cliente se haya conectado pasará a formar parte de la red local en la que se encuentra el servidor VPN.

Elegir el nombre del servidor

El nombre de nuestro servidor VPN es pptpd.

En el caso que se quiera cambiar el nombre del servidor VPN se puede hacer de la siguiente forma:

sudo nano /etc/ppp/pptpd-options

Una vez abierto el editor de textos tan solo como tan solo tienen que localizar la línea que pone:

name pptpd

Una vez localizada tan solo hay que reemplazar pptpd por el nombre que queramos ponerle a nuestro servidor VPN.

Dentro de este fichero también es recomendable consultar que las siguientes líneas estén descomentadas:

- requiremschapv2 : Esta línea define que el protocolo de autenticación del cliente al servidor se realizará mediante el protocolo mschap-v2.

- requiremppe128 : Esta línea define que el tráfico entre cliente y servidor irá cifrado con una capa de cifrado de 128 bits MPPE.

- ms-dns 8.8.8.8: Esta línea hay que introducirla para asegurar que las peticiones DNS se resuelvan adecuadamente. En vez de los DNS de google se pueden usar otros.

- ms-dns 8.8.4.4: Esta línea hay que introducirla para asegurar que las peticiones DNS se resuelvan adecuadamente. En vez de los DNS de google se pueden usar otros.

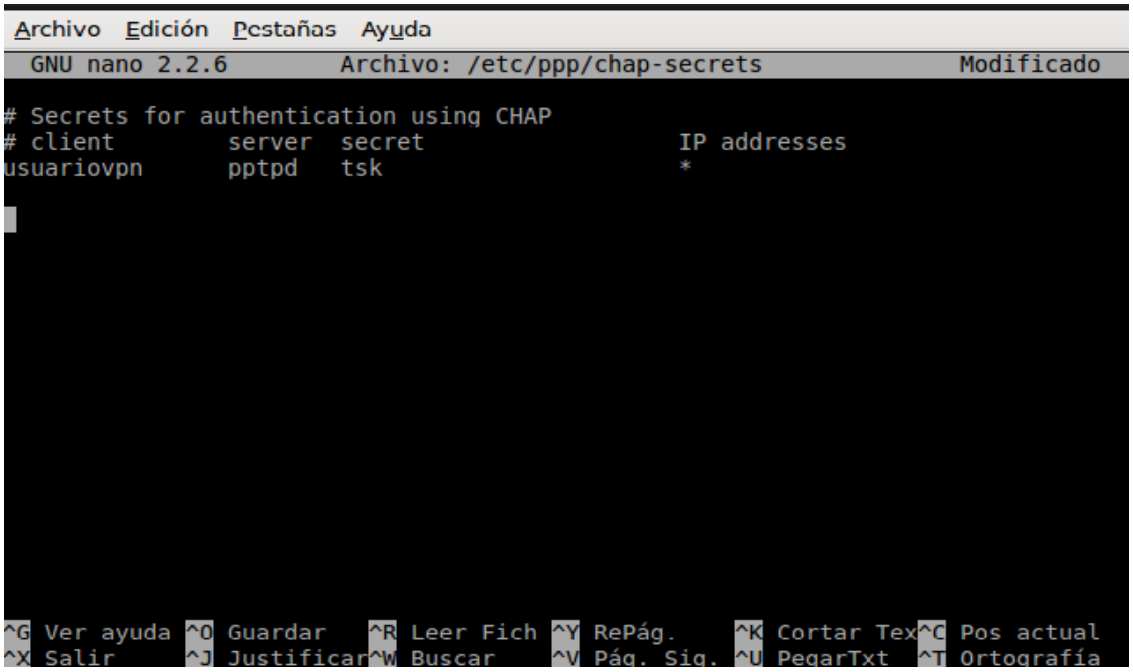
El resto de configuración dentro en principio es válida para nuestras necesidades.

Añadir usuarios a nuestro servidor VPN

Ahora el siguiente paso es crear cada uno de los usuarios que se podrán conectar a nuestro servidor VPN. Para ello en el terminal tan solo hay que teclear el siguiente comando:

sudo nano /etc/ppp/chap-secrets

Una vez tecleado el comando aparecerá el editor de texto con un contenido parecido al siguiente:



Como se puede ver dentro del editor de texto tenemos que introducir los datos para los siguientes parámetros:

- Client: En este campo tenemos que asignar el nombre de usuario. En este caso hemos elegido que el nombre de usuario sea usuariovpn.
- Server: En este campo tenemos que indicar el nombre del servidor. El nombre del servidor por defecto es pptpd. Si en el apartado anterior cuando hemos accedido dentro de /etc/ppp/pptpd-options hemos cambiado el nombre del servidor entonces deberemos sustituir pptpd por el nombre que elegimos.
- Secret: En este campo tenemos que definir la contraseña de conexión para el usuario usuariovpn, al servidor VPN. En mi caso el password que he elegido es “tsk”

- IP addresses: En este campo pondremos un *. De este modo al cliente que se conecta se le asignará cualquier IP comprendida entre 192.168.1.234 y 238. En el caso que quisiéramos que el cliente usuariovpn tuviera siempre la IP 192.168.1.236 tan solo deberíamos reemplazar el * por 192.168.1.236.

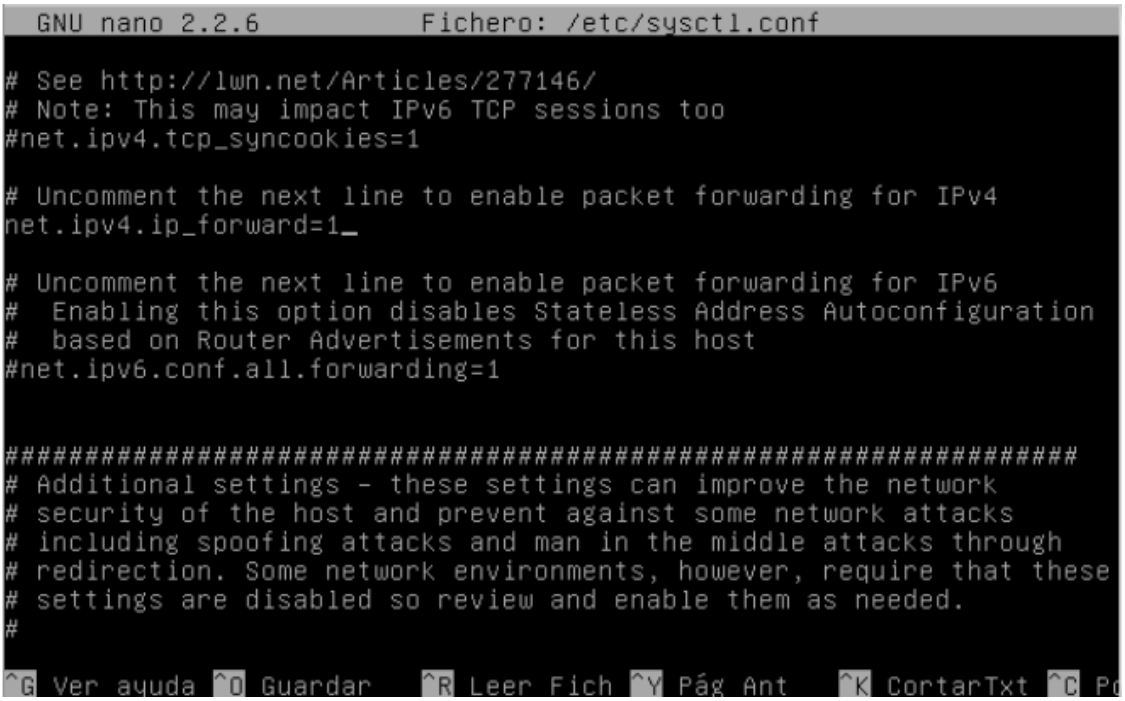
Nota: Dentro de este fichero podemos introducir tantos clientes como nuestra red y rango de IP's definidos nos permitan.

Configurar IPTABLES para el enrutamiento de peticiones

Para que el enrutamiento se realizar correctamente lo primero que tenemos que hacer es habilitar el IP Forwarding. Para habilitar permanentemente el IP Forwarding tenemos que teclear el siguiente comando:

sudo nano /etc/sysctl.conf

Una vez tecleado este comando nos aparecerá la siguiente pantalla:



Una vez abierto el editor de textos tenemos que buscar la siguiente línea:

#net.ipv4.ip_forward=1

Una vez encontrada la tenemos que des comentar. Para des comentarla quitamos el símbolo # quedando de la siguiente forma:

net.ipv4.ip_forward=1

Guardamos los cambios y cerramos el archivo.

En estos momentos el IP forwarding está habilitado y los equipos que forman parte de nuestra red privada VPN se podrán comunicar entre ellos. Pero no lo podrán hacer con redes externas públicas como por ejemplo podría ser conectarse a la página web de facebook.

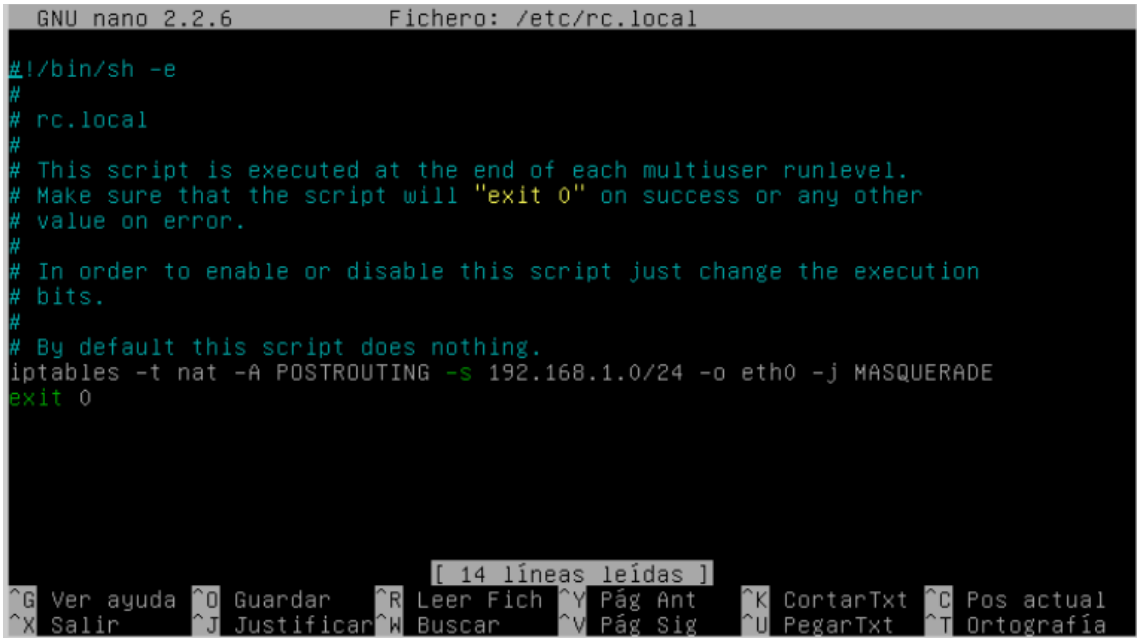
Para solucionar este problema tendremos que introducir una regla en el firewall. Para introducir la regla que soluciona este problema tenemos que introducir el siguiente comando:

sudo nano /etc/rc.local

Una vez se ha abierto el editor de texto tendremos que introducir la siguiente orden:

iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE

Una vez finalizado el proceso la pantalla tiene que tener un aspecto similar al siguiente:



Abrir los puertos del router

Para poder acceder desde el exterior a nuestro servidor VPN tenemos que configurar adecuadamente nuestro router.

El router será el encargado de redirigir la totalidad de peticiones exteriores a nuestro servidor VPN. Para que nuestro router pueda realizar esta función tenemos que abrir nuestro navegador y teclear nuestra puerta de entrada. Seguidamente, se nos pedirá nombre de usuario y contraseña:

Una vez introducida la información accederemos a la configuración de nuestro router. Seguidamente, tenemos que acceder a los menús Advanced / NAT / Virtual Servers:

A continuación presionamos el botón Add.

En el menú desplegable Select a service tienen que elegir la opción PPTP. De este modo estaremos abriendo el puerto 1723 que es el puerto estándar de nuestro servidor VPN pptp.

En el campo Server IP Address tenemos que seleccionar la IP de nuestro servidor que como hemos visto anteriormente es 192.168.1.188.

De esta forma todas las peticiones exteriores que lleguen a nuestro router por el puerto 1723 serán redirigidas a nuestro servidor VPN.

Conclusión de la solución

Microsoft desarrollo el protocolo PPTP para permitir a las personas acceder remotamente y de forma segura a las redes locales a través de Internet. Los datos son encapsulados antes de su transporte a través de IP mediante Internet.

La ventaja más destacable de PPTP es su facilidad a la hora de configuración y uso frente al protocolo L2TP (Layer 2 Tunnneling Protocol). Los datos son encriptados sin IPsec, lo cual implica que no es necesario instalar ningún certificado de equipo ni una aplicación de clave pública (PKI).

Al no usar IPsec, tiene como inconveniente que su seguridad es más pobre en comparación con L2TP. No tiene verificación de origen, lo cual implica que no se puede confirmar la integridad de los datos.

Alternativa Linux 2 – Servidor L2TP de VPN

Debido a problemas de seguridad se ha decidido examinar otra opción de conexión VPN que ofrece mayores garantías de conexión remota.

Los túneles L2TP se crean encriptando una trama en un paquete UDP, el cual se encapsula en un paquete IP mediante la cual se identifican los extremos de dicho túnel.

Para configurar este tipo de túnel son necesarios los siguientes ajustes.

Instalar los servidores

Los programas que hay que instalar en son: *openswan* que se encarga de *IPSec*, *xl2tpd* que se encarga del transporte de datos y ppp que se encarga del tunel. Para instalarlos basta con la orden

```
sudo apt-get install openswan xl2tpd ppp
```

Configuración IPsec

El trabajo duro es el de configuración. Primero IPSec. Hacemos una copia del fichero original y luego lo editamos para que sea cómo el ejemplo:

```
sudo cp /etc/ipsec.conf /etc/ipsec.conf.original
sudo nano /etc/ipsec.conf
```

```
config setup
   nat_traversal=yes
   protostack=netkey
   plutostderrlog=/tmp/log.txt

conn L2TP-PSK
   authby=secret
   pfs=no
   rekey=no
   type=tunnel
   esp=aes128-sha1
   ike=aes128-sha-modp1024
   ikelifetime=8h
   keylife=1h
```

left=10.0.1.205
leftnexthop=%defaultroute
leftprotoport=17/1701
right=%any
rightprotoport=17/%any
rightsubnetwithin=0.0.0.0/0
auto=add
dpddelay=30
dpdtimeout=120
dpdaction=clear

Los detalles que se pueden personalizar son la dirección IP del servidor en la red local y si queremos limitar el acceso desde algunas direcciones.

Lo siguiente es definir el "secreto", una contraseña que todas las conexiones han de conocer. Para ello debemos editar el fichero ipsec.secrets:

sudo nano /etc/ipsec.secrets

%any %any: PSK "cHc0J#7-t4H2sU01OC"

Se puede modificar este secreto si se considera necesario.

Configurar el protocolo de transporte

En tercer lugar hay que configurar el protocolo de transporte xl2tp. Hacemos una copia de seguridad y editamos el fichero hasta que quede como el ejemplo:

sudo cp /etc/xl2tpd/xl2tpd.conf /etc/xl2tpd/xl2tpd.conf.original
sudo nano /etc/xl2tpd/xl2tpd.conf

En este fichero se debe indicar la dirección del servidor y el rango de IP que les daremos a los dispositivos remotos.

[global]
auth file = /etc/l2tpd/l2tp-secrets
debug network = yes
debug tunnel = yes

[lns default]

ip range = 10.0.1.209-10.0.1.240
local ip = 10.0.1.205
require chap = yes
refuse pap = yes

require authentication = yes
name = felip
ppp debug = yes
pppoptfile = /etc/ppp/options.xl2tpd
length bit = yes

Hay que seguir con el fichero de opciones del tunel, ppp.

```
sudo cp /etc/ppp/options.xl2tpd /etc/ppp/options.xl2tpd.original
sudo nano /etc/ppp/options.xl2tpd
```

Es muy recomendable indicar un servidor DNS para nuestra conexión, hemos elegido el servidor IP de google (8.8.8.8)

ipcp-accept-local
ipcp-accept-remote
ms-dns 8.8.8.8
noccp
auth
crtscts
idle 1800
mtu 1410
mru 1410
nodefaultroute
debug
lock
proxyarp
connect-delay 5000

Después hay que añadir el usuario y contraseña que vamos a utilizar en la conexión.

```
sudo nano /etc/ppp/chap-secrets
```

Por ejemplo para el usuario “usuariovpn” le asignamos la contraseña “grupotsk”.

```
usuariovpn   *   grupotsk   *
```

Para acabar la configuración, hay que reiniciar los servicios implicados:

```
sudo service ipsec restart
sudo service xl2tpd restart
sudo service pptpd restart
```

Configurar el servidor

Casi para acabar, un detalle muy importante, nuestro servidor Linux ha de ser capaz de redirigir los datos entre Internet y nuestro dispositivo. Para ello hemos de editar el fichero sysctl.conf

sudo nano /etc/sysctl.conf

Editar el fichero para asegurar que la línea ipforwarding no esté comentada.

net.ipv4.ip_forward=1

Se guarda el fichero y se reinicia el servicio,

sudo sysctl –p

Hasta aquí la configuración en Linux, para configurar el router y los puertos que debemos abrir debemos seguir la misma configuración que en el punto 10.8

Conclusión de la solución

Debido a que L2TP utiliza IPsec, no sólo encripta los datos, sino que también ofrece seguridad adicional que PPTP no nos ofrecía.

Al contrario que PPTP, L2TP ofrece integridad de datos y autenticación de los datos de origen. Otra ventaja es el uso de UDP para encapsular los datos, lo que hace L2TP más rápido y más fácil de configurar con algunos firewalls. Con otros firewalls, L2TP puede tener una ligera desventaja en la velocidad, ya que encapsula los datos dos veces.

La desventaja más reseñable sobre este tipo de túnel es que necesitamos mucha más configuración que con PPTP y además necesitamos incluir PKI y certificados de equipo.

ANEXO 2.

CONFIGURAR UNA CUENTA DNS DINÁMICO

***Este es un tutorial que hemos seguido tal cual viene en la página adslayuda.com**

****

La traducción de DDNS es **Sistema Dinámico de Nombres de Dominio**. Es una herramienta muy útil cuando nuestra línea ADSL tiene un direccionamiento dinámico, es decir, nuestro proveedor de internet nos asigna una IP pública diferente cada vez que nos conectamos.

Si nuestra intención es configurar un servidor web, ftp, montar una VPN, etc, necesitamos tener localizado nuestro router en internet para poder tener acceso. Esto lo conseguimos mediante la función DDNS.

Dicha función permite configurar el router para asociarlo, mediante un nombre de dominio, a una dirección IP. Esto lo lleva a cabo un servidor que proporciona soporte para DNS con IP dinámica. Este router únicamente permite trabajar con DynDNS.org.

El funcionamiento sería el siguiente: Creamos una cuenta (en principio gratuita) con un servidor de DNS dinámicas, en este caso www.dyndns.org. Cuando el router conecta a internet obtiene una dirección IP. En ese momento, envía la información de su IP y del nombre de dominio al servidor www.dyndns.org, mediante la cuenta definida. A partir de ese momento, el nombre de dominio (del tipo xxxxx.dyndns.org) queda asociado a la IP y, por tanto, nuestro router queda localizado en internet con, por ejemplo, un simple ping (es necesario abrir ventana de ms-dos) al nombre de dominio desde cualquier ubicación (**ping xxxxxx.dyndns.org** nos devolvería la ip pública del router).

Por tanto, el proceso consta de dos partes, el primero, activar la función en el router. El segundo definir la cuenta y el nombre de dominio con el servidor dyndns.org.

Accederemos al router introduciendo su IP local en el navegador (puerta de enlace de nuestra red local).

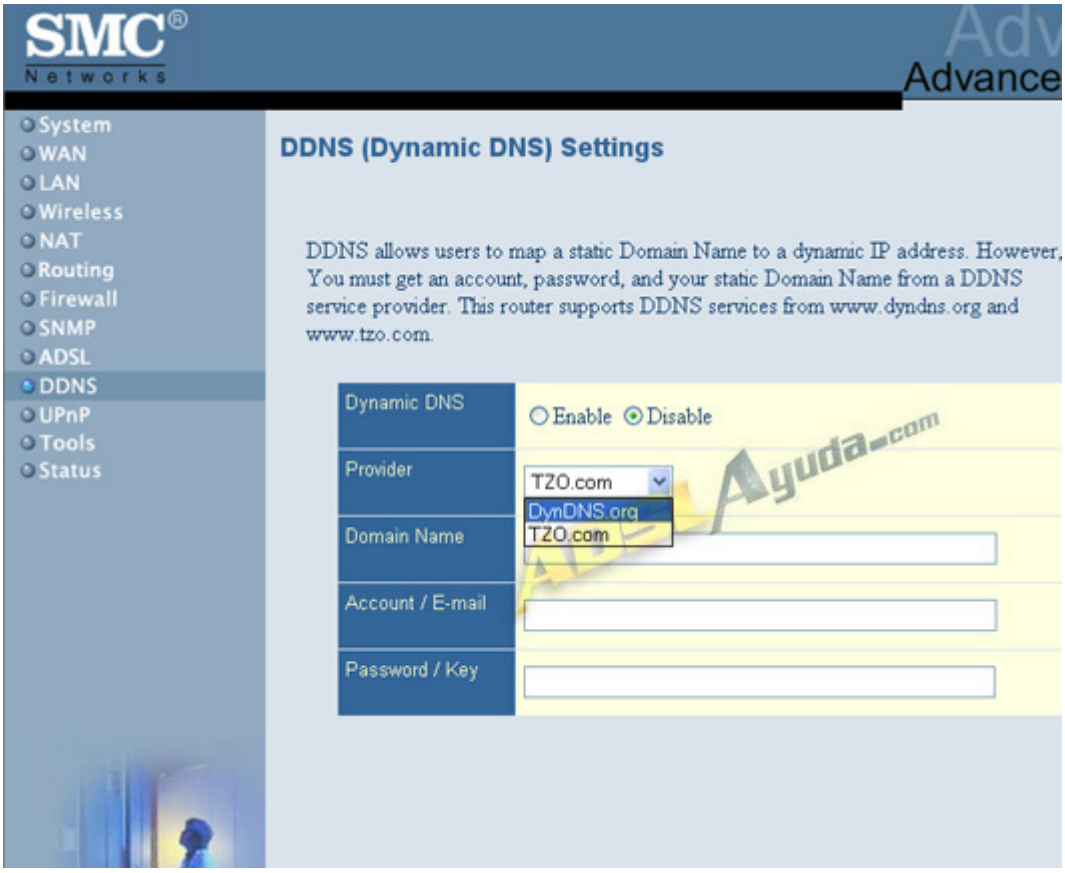
Este router en concreto tiene por defecto la IP 192.168.2.1 (a no ser que se la hayamos cambiado). La introducimos en el navegador y debería abrirse la siguiente pantalla:

La contraseña predeterminada de acceso al router es: **smcadmin**.

Aparecerá la pantalla de bienvenida al router, iremos a la opción **Advanced Setup**.

Entraremos a la configuración avanzada y aparecerá un menú a la izquierda con varias opciones, debemos elegir **DDNS**.

Podremos optar entre dos servidores para DNS dinámica, DynDNS.org y TZO.com. En el presente ejemplo trabajaremos con el primero.



Por lo tanto, en **Provider** seleccionaremos **DynDNS.org**.

Ahora deberemos rellenar los campos: **Domain Name**, **Account / E-mail** y **Password / Key**.

Estos los conseguiremos al configurar nuestra cuenta con DynDNS.org. Describiremos los pasos brevemente, ya que se trata de una gestión que realizaremos en la página web de una corporación, por tanto, el procedimiento podría variar en el momento en que esa web fuera reestructurada.

Entraremos en www.dyndns.org y nos dirigiremos al apartado **Account**.

Allí iremos al enlace **Create Account** para abrir una cuenta (gratuita hasta el momento), ya que en principio, todavía no tenemos ninguna.

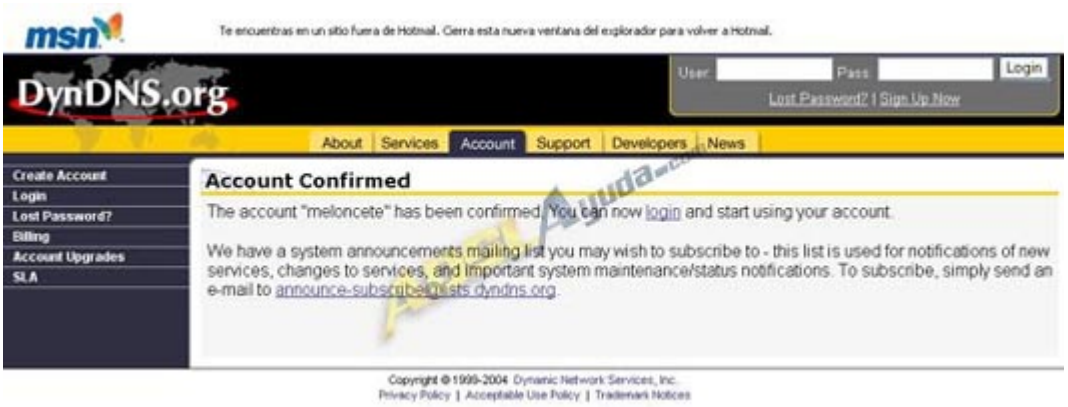
En este apartado deberemos elegir un nombre para la cuenta, una contraseña y poner una dirección e-mail. A ésta dirección nos enviarán la confirmación de que la cuenta está creada, por tanto debemos tenerla necesariamente activa y en uso.

Los datos de **Username** y **Password** que introduciremos nos valdrán tanto para el acceso a nuestra cuenta en dyndns.org como para los apartados correspondientes del router. Pulsamos el Botón Create Account. En ese momento pasaremos a la pantalla de confirmación en la que se nos notifica que se nos ha enviado un e-mail a la dirección de correo introducida anteriormente.

El e-mail tipo debe ser similar a éste. En él nos da un enlace al que necesariamente tendremos que ir para continuar el procedimiento.

```
Your DynDNS.org user account 'meloncete' has been created.  You must visit
the confirmation address below within 48 hours of the time this e-mail was
sent to complete the account creation process.

Our basic service offerings are free, but they are supported by our premium
services.  See http://www.dyndns.org/services/ for a full listing of all of
our available services.

To confirm your account, please go to the address below:

https://www.dyndns.org/account/confirm/[illegible]

Please note: If you did not sign up for this account, this will be the only
communication you will receive.  All non-confirmed accounts are deleted
after 48 hours, and no addresses are kept on file. We apologize for any
inconvenience this correspondence may have caused, and we assure you that
it was only sent at the request of someone visiting our site and requesting
an account.

Sincerely,
The Dynamic Network Services Support Department
support@dyndns.org
```

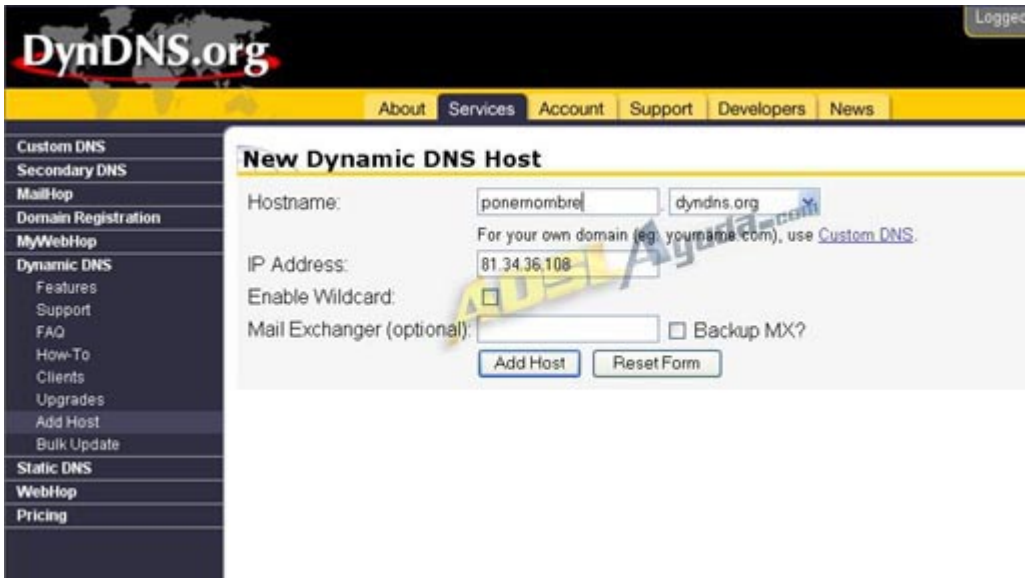
Pulsaremos, por tanto en el enlace.



Lo siguiente es iniciar sesión, iremos al apartado **Login**.

Una vez iniciada, pulsaremos en el apartado **Dynamic DNS** y a continuación en **Add Host**.

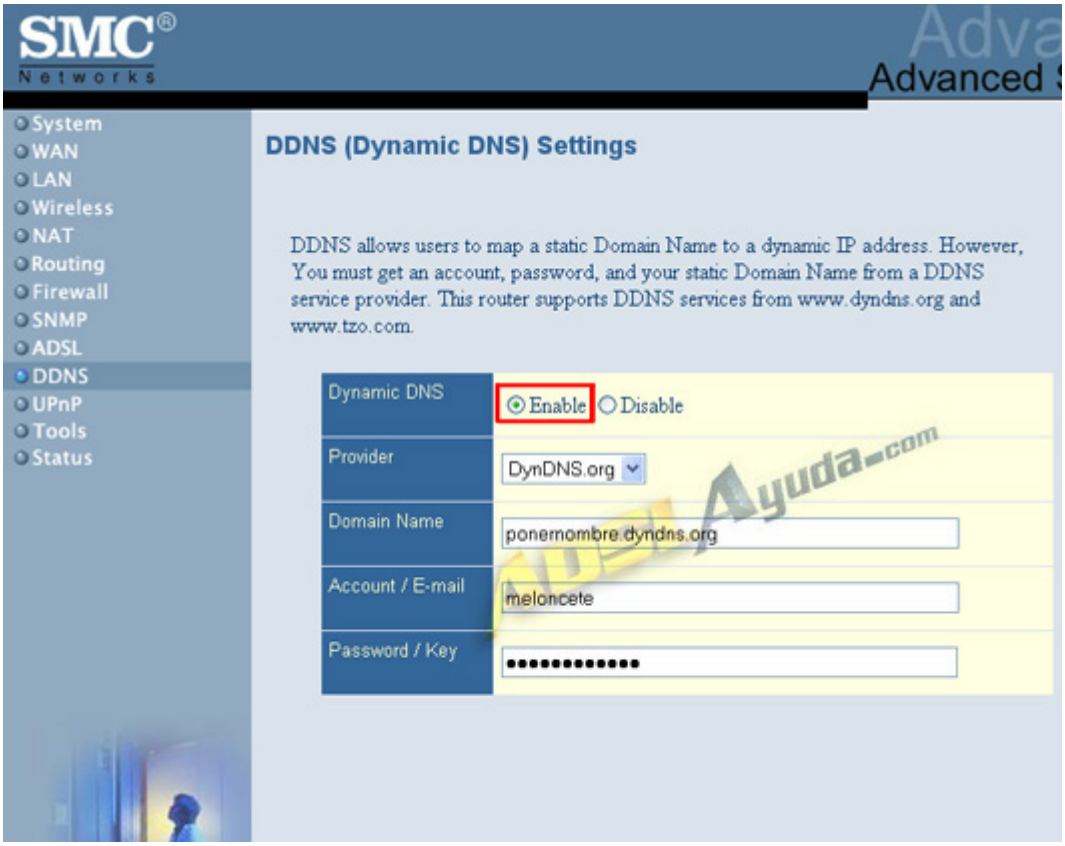
Aquí crearemos el nombre de dominio que queramos asociar a nuestra cuenta (podemos crear varios).



Pantalla de confirmación:

Volveremos a comprobar los datos de nuestra cuenta en la que ya aparecerá el dominio creado.

En este momento podemos terminar de rellenar los campos que nos restaban de la configuración del router:

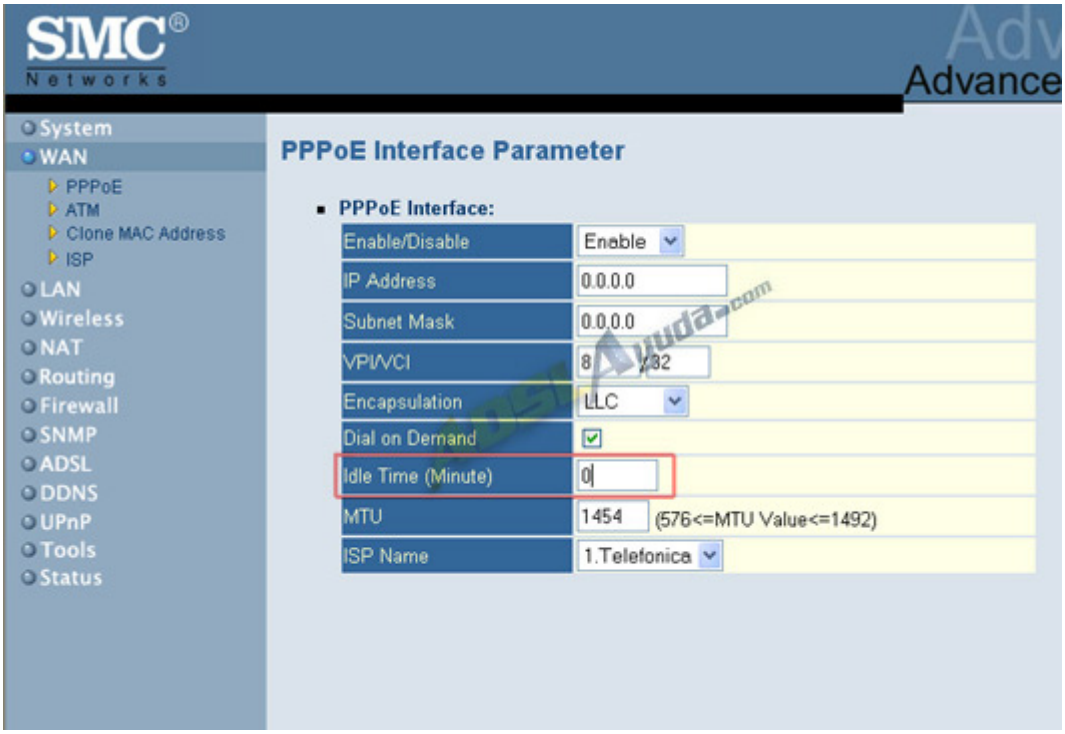


Ahora activaremos el botón **Enable** y pulsamos en **Apply** para guardar y activar los cambios. Si todos los pasos los hemos dado correctamente, debería activarse la función DDNS.

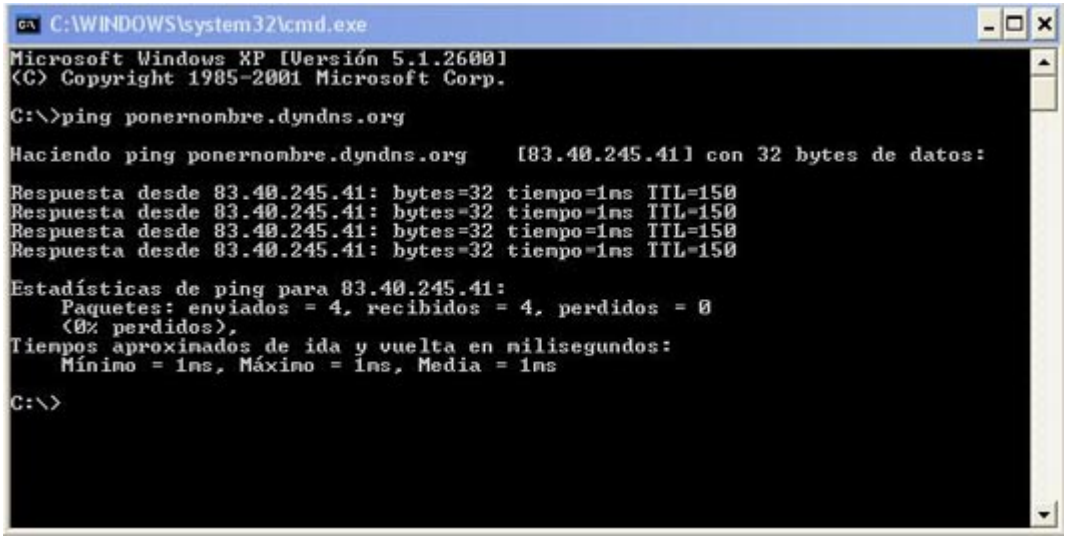
Para finalizar, cambiaremos una opción que viene en el router por defecto. En el menú **WAN** iremos a la opción **PPPoE**.

El valor de **Idle Time (Minute)** está en 5. Esto quiere decir que el router marcará la conexión PPPoE sólo cuando sea demandada por alguno de los ordenadores de nuestra red, desconectando a los 5 minutos de inactividad.

Pero para poder tener el router siempre accesible desde el exterior, es necesario que esté siempre conectado. Por tanto, estableceremos el valor de **Idle Time (Minute)** en 0. Esto hará que la conexión permanezca siempre activa.



A partir de ahora, podemos localizar nuestro router de varias maneras. La más sencilla para obtener nuestra IP pública sería un ping al dominio que tengamos en uso. Para ello abriremos una ventana de ms-dos (En Win XP Inicio, Ejecutar, cmd)



Si tenemos un servidor web instalado en el ordenador, a partir de ahora será accesible en la dirección http://ponernombre.dyndns.org.

ANEXO 3.

ESTUDIO DE MERCADO SOBRE POSIBLES SOLUCIONES

Estudio de posibles soluciones

Dentro de los alcances del presente proyecto, uno de ellos es el de estudiar cómo se encuentra la tecnología a día de hoy y que sistemas existen implantados para conocer la realidad de la industria contemporánea.

En primer lugar hemos decidido realizar un estudio de los dispositivos físico como routers, firewalls, etc. que ofrezcan la seguridad y los requisitos nombrados en el capítulo anterior.

Para ello hemos consultado cuales son los grandes fabricantes en este aspecto y vamos a centrarnos en dos de ellos como son eWon y Siemens.

Después nos centraremos en otro servicio como es el "*cloud computing*" ofertado por empresas como Weidmuller.

Ewon

Gama eWon CD

El eWON CD es un completo router industrial con funcionalidades de enrutado entre la LAN de la fábrica y la LAN de la máquina con características de túnel VPN.

También se puede usar opcionalmente un módem integrado como sistema secundario o de seguridad para acceder a la LAN de la máquina. Integrado perfectamente con el entorno de programación del PLC, El eWON 2005CD/4005CD monitoriza y recolecta datos en variables.

Gama eWon Flexy

El eWON Flexy es el primer router M2M industrial modular y pasarela de datos diseñado para fabricantes OEM e integradores de sistemas.

Este router ofrece la flexibilidad de conectar dispositivos remotos en un entorno en el que las tecnologías de la comunicación avanzan a pasos agigantados, y comunicarse de forma universal con una gran variedad de maquinaria situada en instalaciones remotas, sea cual sea el protocolo utilizado.

Siemens

Siemens → Industrial Remote Comunication. TeleControl

Por su parte Siemens ofrece una solución para sus productos propios como es Industrial Remote Communication.

Industrial Remote Communication ofrece un acceso remoto eficaz a máquinas e instalaciones con SIMATIC. El acceso remoto a instalaciones y máquinas lejanas y aplicaciones móviles en todo el mundo es cada día más importante: tanto en la industria como en los sectores cercanos a ella.

Siemens ofrece, con un amplio abanico de soluciones para el acceso remoto a plantas industriales, la base idónea para la supervisión y el control seguro y eficaz de instalaciones y procesos ampliamente distribuidos de cualquier tamaño. Además del acceso remoto eficaz (Remote Access), Industrial Remote Communication ofrece con sus componentes de red la posibilidad de enlace de datos transparente entre redes remotas a través de redes WAN públicas o privadas.

Telecontrol

El telecontrol es la integración en una o más centrales de control de estaciones de proceso distribuidas en el espacio. Para la comunicación destinada a la monitorización y el control se utilizan distintas redes pública o privadas.

El intercambio cíclico o controlado por eventos de los datos del proceso tiene lugar mediante protocolos de telecontrol especiales y permite a los operadores tener un control efectivo de todo el proceso.

Los sistemas de telecontrol se basan en SIMATIC. Completan dicho sistema con el hardware y software correspondientes y permiten así conectar los distintos componentes mediante WAN (Wide Area Network). La transmisión de datos se efectúa en este caso a través de la clásica WAN como, p. ej., líneas dedicadas, red telefónica, sistemas inalámbricos, pero también a través de redes basadas en IP, como las de telefonía móvil o Internet.

Teleservicio (diagnóstico y mantenimiento remotos)

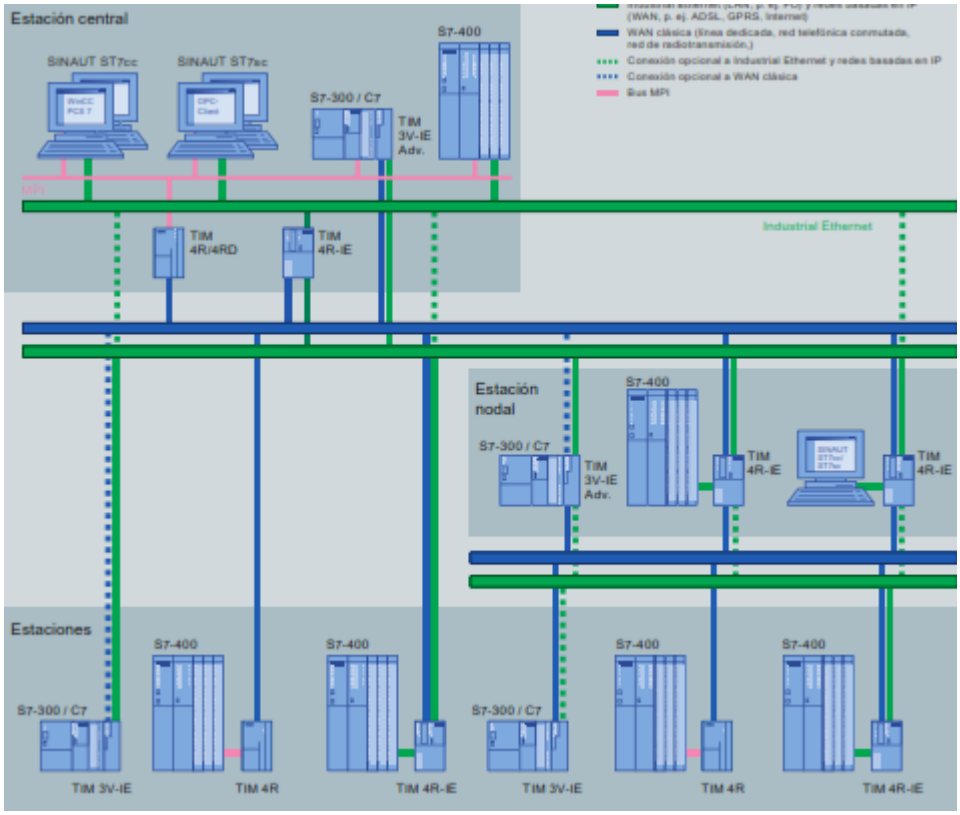
El teleservicio consiste en el intercambio de datos entre instalaciones técnicas alejadas espacialmente con fines de detección de fallos, diagnóstico, mantenimiento, reparación u optimización.

El telediagnóstico y el telemantenimiento de plantas de producción son un componente imprescindible de la tecnología de automatización moderna. Son más eficientes y económicos que tener un empleado del servicio técnico in situ.

Permiten detectar y subsanar los fallos mucho más rápidamente, reducir los tiempos de parada de las máquinas y aumentar su disponibilidad.

Siemens Remote Services

El concepto de "Siemens Remote Services" proporciona una plataforma potente y segura para el acceso remoto a máquinas e instalaciones. Con la integración de "shared experts" se ofrece un soporte efectivo, no sólo por parte de Siemens sino también por especialistas de la propia empresa.



SCALANCE S

Por primera vez existe un concepto que elimina los riesgos que conlleva el uso de estructuras de Ethernet homogéneas y la tecnología de Internet para las áreas de producción y demás sectores sensibles que pueda haber dentro de una empresa.

El hardware y el software de SCALANCE S forman un sistema de seguridad perfeccionado hasta en el más mínimo detalle.

Como todos los productos de SIMATIC NET, SCALANCE S ha sido diseñado para la industria, por lo que satisface los más severos requisitos de la comunicación industrial.

- Ganar en seguridad sin perder en rendimiento.

  SCALANCE S protege las células de automatización contra accesos no autorizados y sobrecargas innecesarias de las comunicaciones. El flujo de datos dentro de la célula de auto-matización permanece inalterado aunque se produzcan perturbaciones en la red externa.

- Los módulos SCALANCE S protegen la comunicación sea cual sea el protocolo de aplicación utilizado.

  Así se aseguran sin la menor dificultad todos los protocolos basados en IP y los protocolos de capa 2 que aún se utilizan con mucha frecuencia en el mundo de la automatización sin restringir el intercambio de datos permitido para la producción.

- La seguridad que necesita la automatización industrial. Redes segmentadas con SCALANCE S.

  El concepto de seguridad de Siemens permite segmentar la red. Así, pues, SCALANCE S ofrece ventajas decisivas.

- SCALANCE S aprende solo.

  Los módulos de seguridad ofrecen un modo de aprendizaje que les permite detectar automáticamente cualquier estación que se halle conectada a la red interna, lo que evita tener que configurar las estaciones.

Y también detectan otros módulos de seguridad integrados en la red.
La ventaja que esto tiene es que no es necesario reconfigurar los módulos de seguridad ya existentes cuando se amplía el sistema.

SCALANCE M

El equipo permite trabajar con HSDPA (High Speed Downlink Packet Access) y HSUPA (High Speed Uplink Packet Access) y, en consecuencia, permite velocidades de transmisión altas de hasta 14.4 Mbit/s en la descarga y de hasta 5.76 MBit/s en la subida (en función del proveedor).

Si no se dispone de una red móvil 3G / UMTS, los datos se pueden transmitir a través de la red móvil GSM usando EGPRS (Edge) y GPRS (General Packet Radio Service).

La seguridad del acceso y de la comunicación se garantiza a través de funciones de seguridad del cortafuegos (firewall) integrado y mediante túnel VPN (encriptación de extremo a extremo de la conexión de comunicación por medio del establecimiento de túneles IPsec).

Gracias a la utilización del router SCALANCE M875 3G/UMTS, se podrá acceder a las unidades de planta distribuidas a lo largo del mundo por medio de una comunicación basada en IP; también es adecuado para su uso en

sistemas de telecontrol, para la programación remota o para el diagnóstico remoto.

El SCALANCE M875 se puede usar en aplicaciones industriales y semi-industriales:

- Programación y mantenimiento remotos en todo el mundo, p. ej. con STEP 7, a través de una interfaz 3G / UMTS de alta velocidad
- Acceso a planta flexible a nivel mundial para tareas de mantenimiento y diagnóstico
- Conexión de usuarios móviles y estacionarios para el control y supervisión.

Weidmuller

mWatcher

El sistema mWatcher (machine Watcher) es la solución diseñada por Weidmüller para gestionar accesos remotos basada en los routers Ethernet industrial de Weidmüller.

EL mWatcher permite acceder a las instalaciones remotas como si se estuviera directamente conectado a ellas, garantizando en todo momento una total seguridad y privacidad, utilizando para conseguirlo las últimas tecnologías existentes.

Solucionar problemas técnicos desde cualquier ubicación, realizar mantenimientos preventivos, evaluaciones on-line, comprobar el estado de la instalación…

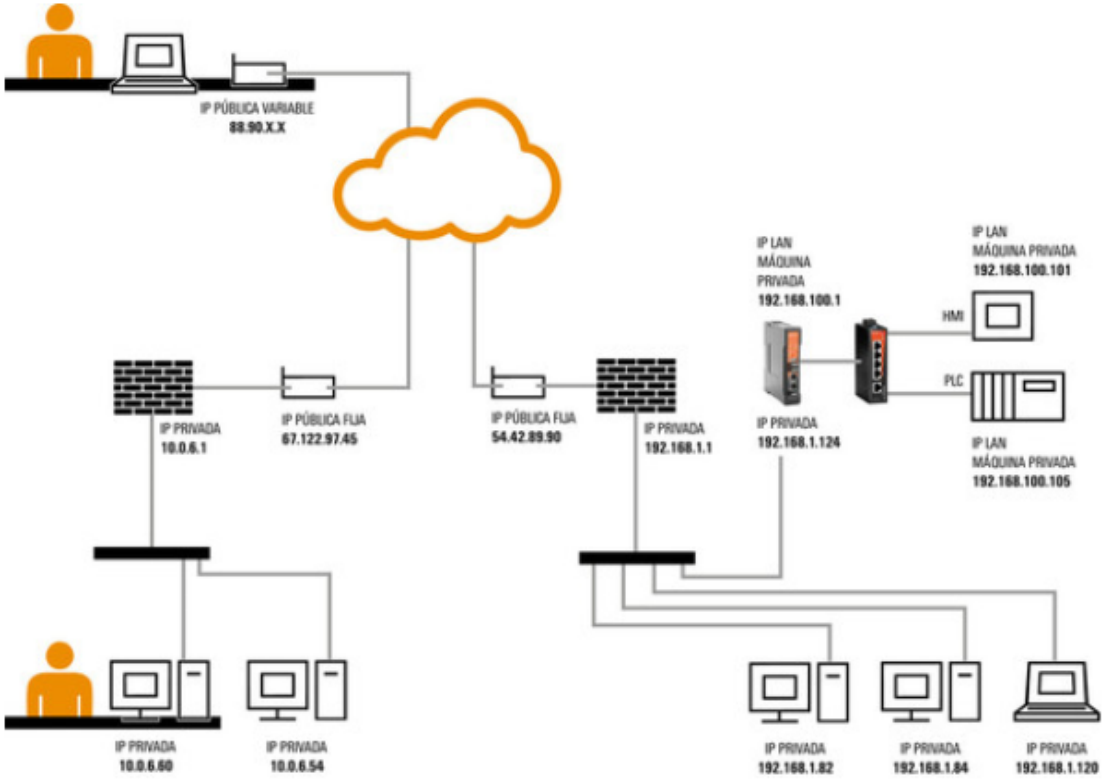
La solución de acceso remoto mWatcher de Weidmüller está basada en un sistema de redes privadas virtuales OpenVPN y en bases de datos MySQL.

Weidmüller pondrá en marcha y se ocupará del mantenimiento de un servidor en la nube (cloud computer) exclusivo para cada cliente. Este servidor actuará como nodo central de unión para las distintas VPN entre los routers y usuarios y contendrá una BBDD en MySQL donde se guardará toda la información de la cuenta.

Mediante una sencilla aplicación software para PC se podrá acceder a máquinas o instalaciones en cualquier parte del mundo.

mWatcher permite añadir instalaciones remotas de forma gradual, incluyendo descripciones e información detallada de las mismas (dispositivos conectados a la red, información de la ubicación y persona de contacto, etc...).

Mediante la **gestión de usuarios y grupos** se puede crear un sistema eficiente y personalizado de permisos para limitar el acceso a cada instalación a los técnicos correspondientes.



Los **usuarios del acceso remoto** pueden estar igualmente conectados a una **red local**, hacerlo a través de una conexión con un módem 3G u otro tipo de conexión

TeamViewer

TeamViewer es un software cuya función es conectarse remotamente a otro equipo. Entre sus funciones están: compartir y controlar escritorios, reuniones en línea, videoconferencias y transferencia de archivos entre ordenadores. Existen versiones para los sistemas operativos Microsoft Windows, Mac OS X, Linux, iOS, y Android.

También es posible el acceso a un equipo remoto mediante un navegador web.

Aunque el principal cometido de la aplicación es el control remoto, también incluye funciones de trabajo en equipo y presentación.

Funcionamiento

El software puede usarse instalándolo en el sistema, aunque la versión 'Quick Support' puede ejecutarse sin necesidad de instalación. Para conectarse a otro equipo, ambos deben estar ejecutando TeamViewer. Para su instalación, requiere acceso de administrador, pero una vez instalado puede ser usado por cualquier usuario del ordenador.

Cuando se inicia en un equipo, el programa genera una ID y una contraseña (también permite que el usuario establezca su propia contraseña). Para establecer una conexión entre un equipo local y otro remoto, el usuario del equipo local debe ponerse en contacto con el otro y este debe indicarle la ID y la contraseña. Una vez hecho esto, se introducen en el programa TeamViewer que se está ejecutado en el ordenador local.

Para comenzar una reunión en línea, el ponente proporciona la ID de dicha reunión a los participantes. Estos se unen a la sesión utilizando la versión completa del programa, o accediendo a la versión para navegador web mediante dicha ID. También es posible programar una reunión con antelación.

Hamachi LogmeIn

Hamachi es una aplicación gratuita (freeware) que configura redes privadas virtuales capaz de establecer vínculos directos entre computadoras que están bajo firewalls de NAT sin necesitar reconfiguración alguna (en la mayoría de los casos). En otras palabras, establece una conexión a través de Internet y simula una red de área local formada por computadoras remotas.

Funcionamiento

Hamachi es un sistema VPN de administración centralizada que consiste en un cluster servidor administrado por el vendedor del sistema y el software cliente, el cual es instalado en los ordenadores de los usuarios.

El software cliente agrega una interfaz de red virtual al ordenador que es utilizada tanto para interceptar el tráfico VPN saliente como para inyectar el tráfico VPN entrante. El tráfico saliente enviado por el sistema operativo a esta interfaz es entregado al software cliente, que lo cifra y lo autentifica y luego lo envía al nodo VPN de destino a través de una conexión UDP iniciada a tal efecto. Hamachi se encarga del tunelamiento del tráfico IP, incluido el broadcast (difusión) y el multicast (multidifusión).

Cada cliente establece y mantiene una conexión de control con el Cluster servidor. Cuando la conexión está establecida, el cliente entra en una secuencia de identificación de usuario, seguida de un proceso de descubrimiento y sincronización de estado. El paso de autentificación de usuario autentifica al cliente contra el servidor y viceversa. El descubrimiento es utilizado para determinar la topología de la conexión a Internet del cliente, y más concretamente para detectar la presencia de dispositivos cortafuegos y servidores NAT. El paso de sincronización extrae una vista del cliente de sus redes privadas sincronizadas con los otros miembros de esas redes.

Cuando un miembro de una red se conecta o se desconecta, el servidor da instrucciones a los otros nodos de la red para que inicien o detengan túneles con dicho miembro. Cuando se establecen túneles entre los nodos, Hamachi utiliza una técnica de NAT transversal asistido por servidor, similar al "UDP hole punching" ("perforadora de agujeros UDP").

En el caso de que se pierda la conexión con el servidor de manera inesperada, el cliente mantiene todos sus túneles e inicia una comprobación de sus estados. Cuando el servidor pierde una conexión de cliente de manera inesperada, se informa a los nodos clientes sobre el hecho y se espera a que inicien sus comprobaciones. Todo esto hace inmune a los túneles Hamachi frente a problemas de red transitorios en el camino entre el cliente y el servidor, y de igual modo quedan operativos en los breves intervalos de indisponibilidad completa del servidor.

Direccionamiento

A cada cliente Hamachi se le asigna una dirección IP desde el bloque de direcciones 5.0.0.0/8 cuando inicia una sesión en el sistema por primera vez, y es en adelante asociada con la clave de cifrado pública del cliente. Mientras el cliente retenga esta clave, puede autentificarse en el sistema y utilizar esa dirección IP 5.X.X.X

Esta asignación es sin embargo no oficial, como RIPE NCC tiene los derechos para realizar asignaciones en ese rango. La dirección IP en adelante se asocia con el cliente público con criptografía asimétrica. Siempre y cuando el cliente conserve su clave, puede conectarse al sistema y utilizar esta dirección IP.

La red 5.0.0.0/8 es utilizada para evitar colisiones con redes IP privadas que podrían estar utilizándose en la parte cliente. Específicamente, las redes privadas 10.0.0.0/8, 172.16.0.0/16 y 192.168.0.0/24.

Seguridad

Como cualquier aplicación de código cerrado o aquellas que no han sido revisadas a fondo, deben aplicarse varias consideraciones de seguridad:

- La ausencia de código fuente que pueda ser revisado
- Su estado beta (si lo hubiere) y el posible impacto de "bugs" de seguridad remanentes

Además, debido al uso de Hamachi como aplicación VPN, deben aplicarse las siguientes consideraciones:

- El riesgo adicional de revelación de datos sensibles que estén almacenados o puedan ser registrados por la mediación del servidor (riesgo que es mínimo cuando los datos no son reenviados)
- Los riesgos de seguridad debidos a servicios vulnerables de las máquinas remotas, no accesibles de otro modo detrás de un NAT, lo cual suele ser habitual en toda VPN

Hamachi utiliza algoritmos sólidos y estandarizados para asegurar y autentificar los datos y su arquitectura de seguridad es abierta. La implementación Hamachi es, sin embargo, de código cerrado y no está disponible para la revisión del público en general.

Para que el producto funcione es necesaria la "mediación del servidor", el cual es operado por el vendedor. El servidor almacena el nombre de usuario, contraseña de mantenimiento, dirección IP estática 5.0.0.0/8 y el "token" de autenticación asociado del usuario. Para cada túnel que se establece, podría registrar la dirección IP real del usuario, tiempo de establecimiento y duración; y lo mismo para los demás usuarios interconectados.

Puesto que todos los nodos que comparten un túnel tienen acceso total de tipo LAN a otros ordenadores, pueden surgir problemas de seguridad si no se utilizan cortafuegos, como se da en cualquier situación insegura. Las características de seguridad de un router/cortafuegos NAT no sirven en este caso. Pero este riesgo no es específico de Hamachi y debe tenerse en cuenta también en cualquier otra VPN.

Bomgar

Bomgar es una empresa líder en soluciones de asistencia a distancia para empresa, que ofrece unos servicios de asistencia seguros y sencillos para dispositivos móviles y sistemas informáticos. Los productos de la empresa permiten a las empresas mejorar el rendimiento y la eficacia de la asistencia tecnológica, haciendo posible que estas sean compatibles de un modo seguro con casi cualquier dispositivo o sistema de cualquier lugar del mundo (incluidos Windows, Mac, Linux, iOS, Android, BlackBerry y más).

Bomgar es una solución de soporte remoto que permite a los técnicos conectarse remotamente a los usuarios finales a través de los sistemas de cortafuegos de su ordenador o dispositivo móvil.

La principal diferencia con los anteriores es que el servidor lo posee el usuario y no el proveedor. De esta manera con una licencia Bomgar podemos conectar tantas estaciones remotas como deseemos.

Cisco Annyconnect

El cliente de Cisco AnyConnect Secure Mobility proporciona acceso remoto seguro y sin problemas a la red local.

- **Experiencia transparente para el usuario**. Aprovechando que AnyConnect garantiza la disponibilidad permanente sobre redes VPN a través del PC (mediante AnyConnect Always On VPN), la aplicación de Cisco optimiza la capacidad del sistema operativo para facilitar de forma nativa conexiones VPN bajo demanda, blindando automáticamente las comunicaciones de empresa a través de un túnel seguro cuando sea necesario.

- **Seguridad optimizada**. Todas las comunicaciones están protegidas con encriptación AES de hasta 256 bits utilizando protocolos de túnel SSL o DTLS. Los administradores de TI también pueden permitir el acceso a los recursos corporativos en función del usuario o del grupo de trabajo, así como revocar el acceso con rapidez en caso de pérdida o robo de los dispositivos o del intento de uso con otro terminal.

- **Acceso ininterrumpido a las aplicaciones**. El acceso seguro a las aplicaciones se mantiene de forma automática al cambiar de red de datos a red WiFi y viceversa, gracias a una opción para configurar el roaming de red.

- **Autenticación empresarial.** La nueva aplicación soporta todas las capacidades de autenticación de Cisco ASA, incluyendo la autenticación multi-factor y los certificados digitales desplegados mediante SCEP (Simple Certificate Enrollment Protocol, Protocolo de Inscripción de Certificados Simple).

Rendimiento mejorado. AnyConnect soporta en modo nativo las conexiones VPN mediante túnel DTLS, proporcionando así un rendimiento óptimo para las aplicaciones con más problemas de latencia como la voz o el vídeo.