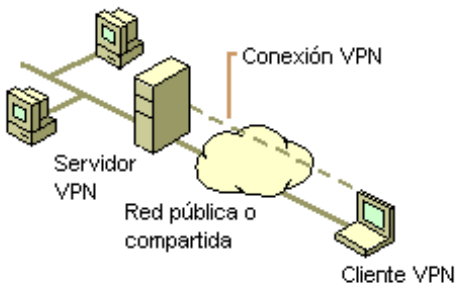
Redes privadas virtuales.

Autor: Enrique V. Bonet Esteban

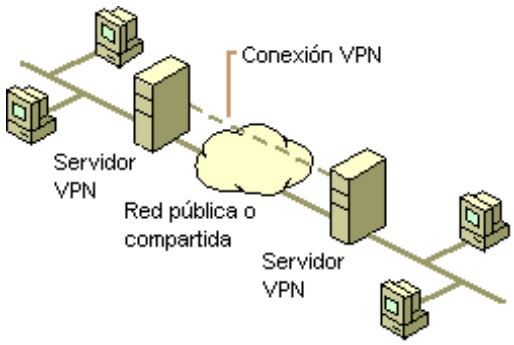
Introducción.

Una red privada virtual (Virtual Private Network) es una tecnología que permite extender una red local sobre una red pública, generalmente Internet. El proceso se realiza encapsulando los paquetes que han de circular por la red pública y, en caso de ser requerida una privacidad en la información enviada, la encriptación de esos paquetes de datos enviados. Básicamente, existen dos tipos de VPN, VPN de acceso remoto y VPN punto a punto.

Una VPN de acceso remoto es aquella que se utiliza para permitir el acceso de un ordenador cliente remoto a una red local, pudiendo adquirir el ordenador remoto la mayoría de privilegios que poseería si se encontrara físicamente dentro de la red local, para lo que se suele asignar al cliente IP mediante la VPN una dirección IP perteneciente a la red local[1].



Una VPN punto a punto es aquella en que dos ordenadores establecen entre ellos una VPN, permitiendo el acceso entre los ordenadores que se encuentran en sus LAN. Generalmente se utilizan para unir distintas sedes de empresas, permitiendo el intercambio de información entre las distintas LAN con la privacidad necesaria, y eliminando el uso de redes punto a punto, generalmente muy costosas económicamente.



[1] Las imágenes utilizadas que ilustran los dos tipos básicos de VPN han sido obtenidas modificando las existentes en la URL de la Universidad de Valencia http://www.uv.es/siuv/cas/zxarxa/vpn.htm.

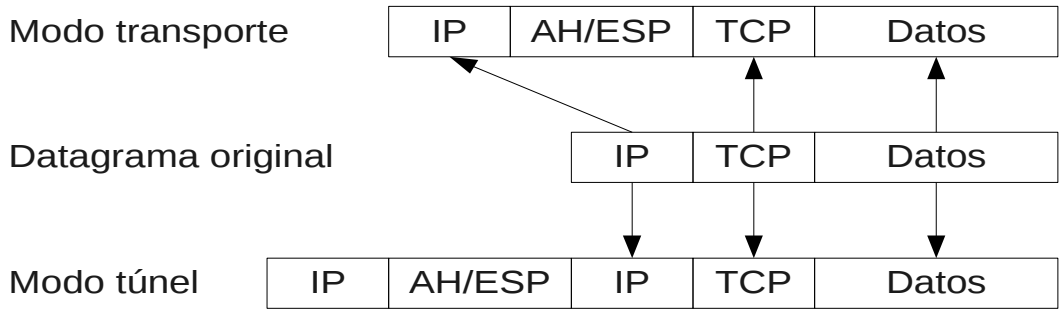
Existen un gran número de protocolos que permiten implementar VPNs, tales como PPTP[2], SSL/TLS e incluso SSH[3], pero el estándar es IPsec.

Introducción a IPsec.

Internet Protocol SECurity es una extensión del protocolo IP que permiten asegurar las comunicaciones sobre IP, autenticando y, si se desea, cifrando los paquetes IP de una comunicación. IPsec trabaja en la capa de red y por ello puede ser utilizado por cualquier aplicación sin necesidad de realizar ninguna modificación en la configuración de la misma.

IPsec puede utilizar uno de dos protocolos, Authentication Header (AH) o Encapsulationg Security Payload (ESP). AH proporciona integridad, autenticación y no repudio de todo el paquete enviado, incluyendo la cabecera IP, mientras que ESP añade a lo anterior el cifrado de toda la información que se envía, pero no incluye en sus cálculos los datos de la cabecera IP. De forma general suele ser más conveniente utilizar ESP, por cifrar la información que se envía, que garantizar la integridad de la cabecera IP[4].

Sea cual sea el protocolo que se utilice, IPsec puede funcionar en dos modos distintos, modo transporte y modo túnel. En modo transporte IPsec solo encapsula los datos del datagrama IP, conservando la cabecera IP original del datagrama, mientras que en modo túnel el datagrama IP es encapsulado completamente dentro de IPsec, por lo que se requiere una nueva cabecera IP para poder enviar el datagrama por la red. En la figura siguiente se muestra esquemáticamente el funcionamiento de ambos modos de IPsec.



Obviamente, el modo transporte solo puede ser utilizado si la IP del datagrama original es una IP pública de Internet, pues si pertenece a una red privada no podrá alcanzar su destino.

Después de esta breve introducción teórica a IPsec, vamos a proceder a analizar como configurar una VPN entre dos ordenadores utilizando IPsec. Para ello,

[2] Point to Point Tunneling Protocol es un protocolo antiguo y es completamente vulnerable, por lo que no debe usarse en la actualidad para configurar una VPN.
[3] Recordar lo que vimos en temas anteriores sobre la capacidad de utilizar SSH para multiplexar conexiones en su canal y poder reenviar puertos, etc., de forma segura.
[4] Es posible encontrar en Internet información sobre los diferentes algoritmos de cifrado, etc., utilizados tanto por AH como por ESP.

utilizaremos la implementación de IPsec llamada Openswan, que es la más utilizada en Linux y se encuentra disponible en la mayoría de distribuciones.

Configuración de Openswan.

El programa que ejecuta Openswan es */usr/sbin/ipsec*, el cual se configura mediante dos dos ficheros, */etc/ipsec.conf* y */etc/ipsec.secrets*, aunque ambos ficheros suelen contener una última línea que indica que se incluyan determinados ficheros que se encuentran dentro del directorio */etc/ipsec.d*.

El fichero ipsec.conf.

El fichero */etc/ipsec.conf* contiene la configuración general del programa y las direcciones IP, redes privadas, y la configuración de cada una de las conexiones VPN a las que da servicio IPSec. Esta formado por dos tipos de secciones las secciones *config* y las secciones *conn*.

Las secciones de tipo *config*, se encuentran limitadas en la actualidad a una única sección *config*, la sección *config setup*, la cual define la configuración del programa. Sus principales valores pueden verse en la tabla siguiente:

Parámetro	Descripción
interfaces	Indica la lista de relaciones entre interfaces virtuales y físicos que utiliza IPSec. Puede ser un único par *<virtual>=<físico>* o una lista de pares encerrada entre comillas. Puede utilizarse un par definido con el *%defaultroute* para indicar que se utilice el interfaz físico que corresponde a la ruta por defecto.
nat_traversal	Indica si se acepta o no enmascaramiento de IP de los paquetes de IPSec. Su uso puede ser necesario para permitir el enrutamiento o el paso a través de cortafuegos en determinados casos. Este parámetro puede modificarse en cada conexión. El valor por defecto es no.
nhelpers	Indica el número de procesos de cifrado que lanzará IPSec para ser ayudado en el cifrado y descifrado de la información. El valor por defecto es n-1, donde n es el número de CPUs (incluído HyperThreading) que tiene el sistema. El valor 0 desactiva la ejecución de procesos de ayuda y obliga a que todo el cifrado y descifrado se realice en el proceso principal[5].
protostack	Pila de protocolos a utilizar para dar soporte a IPSec. Puede tomar los valores *auto*, *klips*, *netkey* y *mast* (variación de *netkey*)[6].
virtual_private	Indica las redes que puede tener el cliente remoto detrás de su servidor de IPSec. Las redes se especifican como la versión del protocolo IP (%v4 o %v6) y las direcciones de red permitidas o bien, si se precede la dirección de red de signo !, las direcciones de red no permitidas.

[5] En las implementaciones de Openswan para Fedora, de forma general debe utilizarse el valor 0, pues se produce un error si se intentan lanzar procesos de cifrado para ayudar al proceso principal.

[6] Klips es el protocolo utilizado en los kernel 2.4 y que fue trasladado a los kernel 2.6, mientras que netkey es el protocolo implementado inicialmente en los kernel 2.6, y soportado por kernels 2.6 y superiores, para permitir IPSec y de forma general es el único soportado por Red Hat y Fedora.

Las secciones *conn <nombre>* contiene la configuración de la conexión identificada por *<nombre>*. Pueden existir una o varias secciones conn en la configuración de IPSec, pero los nombres identificadores no pueden repetirse. Para facilitar su estudio, dividiremos los principales parámetros de las secciones *conn* en dos grupos, parámetros que especifican los valores de negociación, tiempo de vida, etc., de la conexión, y los valores que especifican los valores de red implicados en la conexión.

Los principales parámetros de las secciones *conn* que definen valores de negociación de la conexión son:

Parámetro	Descripción
aggrmode	Especifica si se permite la negociación en modo agresivo (valor yes) o no se permite (valor no, que es el valor por defecto). La negociación en modo agresivo se efectúa de forma más rápida, pero es vulnerable a ataques de denegación de servicio y de fuerza bruta, por lo que no debería utilizarse.
ah	Especifica el tipo de algoritmo utilizado si se utiliza la VPN en modo transporte.
authby	Tipo de autenticación entre los nodos. Los valores posibles son *secret*, para autenticación por secreto compartido, *rsasig* para autenticación mediante clave pública/privada (valor por defecto), *secret|rsasig* para utilizar cualquiera de los dos métodos, y *never* si no se desea que la negociación se produzca y se acepte la conexión.
auto	Operación que debe realizar *ipsec* sobre esta conexión. Los valores posibles son *add*, para añadir y configurar la conexión; *start*, para añadir, configurar y establecer la conexión; *route*, para configurar la ruta de la conexión pero no establecer la misma[7]; e *ignore*, que indica que no se realice ninguna operación sobre la conexión.
ike	Algoritmo (o lista de algoritmos separados por coma) encerrado entre comillas a utilizar en la fase 1 de la negociación. La especificación se realiza como *<algoritmo de cifrado>-<algoritmo de hash>;<grupo Diffie-Hellman>*. Si no se especifica este parámetro, se permite cualquier combinación posible con los valores *{3des,aes}-{sha1,md5}; {modp1024,modp1536}*.
ikelifetime	Duración de la clave de conexión negociada en la fase 1. El valor puede especificarse como un entero, seguido opcionalmente por s, para indicar segundos, o un entero seguido de m, h o d para indicar minutos, horas o días. El valor por defecto es de 1 hora y el valor máximo de 24 horas.
keylife	Duración de la clave de conexión negociada en la fase 2. Sus valores se especifican de igual forma que los valores de *ikelifetime*. El valor por defecto es de 8 horas, y el valor máximo de 24 horas.

[7] Esta opción, que puede parecer extraña, permite eliminar los paquetes que deberían enviarse por esa conexión no establecida, y evitar su envío por el interface de red por defecto.

Parámetro	Descripción
pfs	Perfect Forward Secret indica si se permite el intercambio seguro de las claves. Aunque se pueden especificar los valores yes (valor por defecto) o no, dado que no existe ningún motivo para no utilizar PFS, Openswan siempre utiliza PFS, pues esto no afecta a posteriores fases de la negociación.
phase2	Indica el tipo de modo de transporte que implementará la VPN. Puede tomar los valores esp (valor por defecto) para indicar modo túnel o ah para indicar modo transporte.
phase2alg	Algoritmo (o lista de algoritmos separados por coma) encerrado entre comillas a utilizar en la fase 2 de la negociación. Su especificación, valores por defecto, etc., son iguales a los descritos en el parámetro *ike*. Un sinónimo obsoleto de este parámetro es *esp*.
rekey	Indica si se debe renegociar los valores de las claves de la conexión cuando vayan a expirar (valor yes) o no (valor no). Resaltar que ambos nodos deben utilizar el valor no para indicar que no desean renegociar las claves cuando vayan a expirar, pues este parámetro no límita la aceptación de la negociación de nuevas claves si el otro lado propone dicha negociación.
rekeymargin	Margén temporal en que debe iniciarse la negociación de una nueva clave antes de que expire la anterior. El valor se especifica con la misma sintaxis que el valor del parámetro ike*lifetime*, siendo el valor por defecto de 9 minutos.

Por otro lado, antes de definir los parámetros que definen los valores de red implicados en la conexión, es necesario explicar que en la configuración se utilizan los criterios izquierda (left) y derecha (right), y esos criterios deben mantenerse para ambos nodos, de forma que si en la configuración de un nodo se indica que ese nodo es el izquierdo y el otro nodo es el derecho, debe respetarse este criterio en la configuración del otro nodo y no cambiar esa asignación. Los principales parámetros de los valores de red se encuentran en la siguiente tabla:

Parámetro	Descripción
left	Contiene la dirección IP pública del nodo izquierdo de la VPN. Puede utilizarse el valor *%defaultroute* si esta ha sido utilizado en la configuración de los interfaces en la sección *config setup*.
leftid	Identificador del nodo izquierdo para la autenticación. El valor por defecto es la dirección IP indicada en el parámetro *left*.
lefnexthop	Dirección IP de la puerta de enlace del nodo izquierdo. Si se ha utilizado el valor *%defaultroute* en la configuración del parámetro *left*, se utilizará el valor de la puerta de enlace por defecto de ese interface.
leftsubnet	Subred a la que da servicio el nodo izquierdo de la VPN, expresada como subred/máscara. Si se omite se considera por defecto que la VPN únicamente da servicio al propio nodo.

Parámetro	Descripción
right	Contiene la dirección IP pública del nodo derecho de la VPN. Puede utilizarse el valor *%defaultroute* si esta ha sido utilizado en la configuración de los interfaces en la sección *config setup*.
rightid	Identificador del nodo derecho para la autenticación. El valor por defecto es la dirección IP indicada en el parámetro *right*.
rightnexthop	Dirección IP de la puerta de enlace del nodo derecho. Si se ha utilizado el valor *%defaultroute* en la configuración del parámetro *right*, se utilizará el valor de la puerta de enlace por defecto de ese interface.
rightsubnet	Subred a la que da servicio el nodo derecho de la VPN, expresada como subred/máscara. Si se omite se considera por defecto que la VPN únicamente da servicio al propio nodo.

El fichero ipsec.secrets.

El fichero */etc/ipsec.secrets* contiene las claves RSA, claves precompartidas, etc., que utilizan las diferentes VPNs que puede establecer un nodo para autenticarse con los otros nodos. En la actualidad, el fichero tan solo contiene, en ambos nodos, una línea:

```
include /etc/ipsec.d/*.secrets
```

Que indica que se incluyan el contenido de todos los ficheros del directorio */etc/ipsec.d* que terminen con la extensión *.secrets*.

Las claves precompartidas se incluyen con el formato[8]:

```
@idnodolocal      @idnodoremoto:    PSK "clave secreta precompartida"
```

Donde siempre debe ponerse en primer lugar la identificación del nodo local y después la del nodo remoto, por lo que no se conserva las identificaciones de izquierda y derecha (o similares) que hemos visto antes.

En el caso de una firma digital RSA, se especifica como:

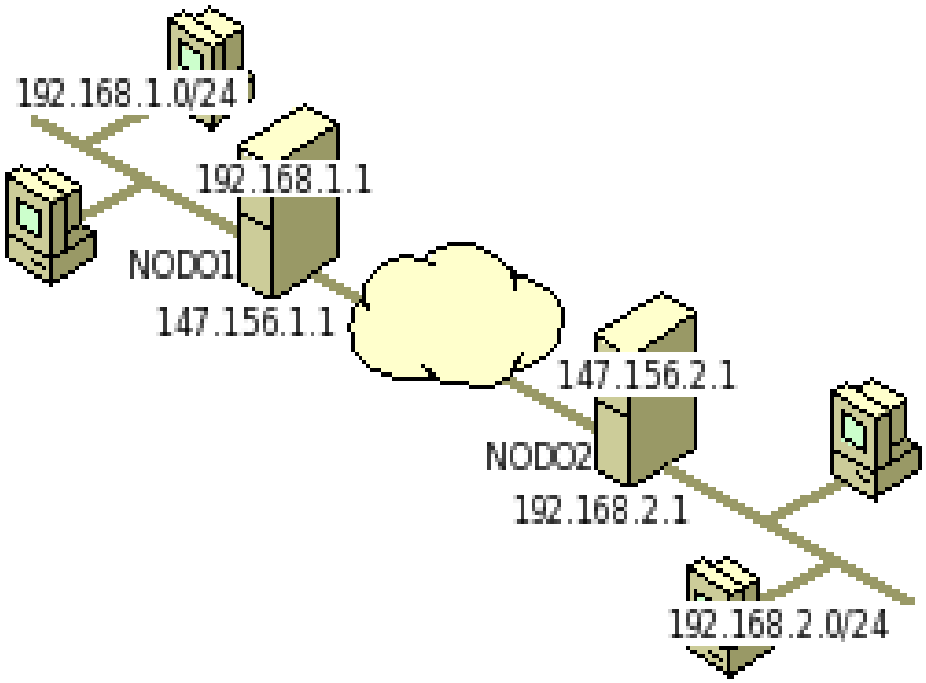
```
@nodo:    rsa {
               Modulus: 0syXpo/6waam+ZhSs8Lt6jnBzu3C4grtt...
               PublicExponent: 0sAw==
               PrivateExponent: 0shlGbVR1m8Z+7rhzSyenCaBN...
               Prime1: 0s8njV7WTxzVzRz7AP+0OraDxmEAt1BL5l...
               Prime2: 0s1LgR7/oUMo9BvfU8yRFNos1s211KX5K0...
               Exponent1: 0soaXj85ihM5M2inVf/NfHmtLutVz4r...
               Exponent2: 0sjdAL9VFizF+BKU4ohguJFzOd55OG6...
               Coefficient: 0sK1LWwgnNrNFGZsS/2GuMBg9nYVZ...
               }
```

[8] La identificación de los nodos locales podría sustituirse por sus direcciones IP.

Pudiendo usar esta firma digital para autenticarse ante todos los nodos necesarios, no necesitando compartir con cada uno de ellos una firma digital propia para cada conexión.

Ejemplo de configuración de Openswan.

En el ejemplo de configuración que utilizaremos supondremos que deseamos crear una VPN punto a punto entre dos nodos, de nombres *nodo1* y *nodo2*, que son los que dan acceso a sus respectivas redes privadas. Para ello supondremos que ambos nodos tienen dos interfaces de red, eth0 que corresponde a una red pública con dirección IP 147.156.1.1 para *nodo1* y 147.156.2.1 para *nodo2*, y eth1, de direcciones IP 192.168.1.1 y 192.168.2.1 para *nodo1* y *nodo2* respectivamente, y que da acceso a dos redes privadas de direcciones IP 192.168.1.0/24 y 192.168.2.0/24, tal y como se pude ver en la figura siguiente:



Por último, supondremos que las direcciones de las puertas de enlace a Internet son 147.156.1.2 para *nodo1* y 147.156.2.2 para *nodo2*.

Con estas valores, el fichero de configuración de *nodo1* sería similar al siguiente:

```
version 2.0

config setup
      nat_traversal=no
      interfaces=%defaultroute
      protostack=netkey
      nhelpers=0
      virtual_private=%v4:10.0.0.0/8,%v4:172.16.0.0/12,
%v4:192.168.0.0/16,%v4:!192.168.1.0/24
```

```
include /etc/ipsec.d/*.conf
```

Mientras que el contenido del fichero en *nodo2* sería:

```
version 2.0

config setup
      nat_traversal=no
      interfaces=%defaultroute
      protostack=netkey
      nhelpers=0
      virtual_private=%v4:10.0.0.0/8,%v4:172.16.0.0/12,
%v4:192.168.0.0/16,%v4:!192.168.2.0/24

include /etc/ipsec.d/*.conf
```

Podemos ver que ambos ficheros son prácticamente idénticos, siendo necesario explicar que la primera línea debe indicar la especificación de la versión de Openswan que cumple el fichero, siendo en nuestro caso la versión 2.0.

A continuación se encuentra la sección de configuración general del programa, en la que indicamos que no se utilice NAT transversal, que el interfaz de red que utilice la VPN sea el interface que corresponde a la ruta por defecto, que utilice la pila de protocolos *netkey*, que el propio proceso sea el que se encargue de efectuar las operaciones criptográficas (valor 0) y los valores de las redes privadas que cada uno de los nodos de la VPN esta dispuesta a admitir.

En nuestro caso, podemos ver que el valor de *virtual_private* es diferente en *nodo1* y *nodo2*. Esto es debido a que *nodo1* indica que permite el acceso de cualquier dirección IP que pertenezca a una subred privada, excepto para aquellas subredes privadas que coincidan con la subred interna (192.168.1.0/24) a la que *nodo1* da acceso a la red pública, mientras que *nodo2* especifica de igual forma que permite el acceso de cualquier IP de una subred privada excepto las IPs que se corresponden con su subred privada interna (192.168.2.0/24).

Por último, en ambos casos se encuentra la línea *include* que especifica que se incluya el contenido de todos los ficheros del directorio */etc/ipsec.d* que tengan como extensión *.conf*, y que son aquellos donde se definirán las distintas VPN que puede establecer cada nodo con otro u otros nodos.

Todas las especificaciones de conexiones VPN empiezan con la línea *conn <nombre>* donde *<nombre>* especifica el nombre de la conexión VPN, que debe ser único, y luego una serie de líneas con la especificación de los lados izquierdo y derecho de la VPN, teniendo en cuenta que si un nodo se considera que es el lado izquierdo, debe preservarse esa consideración en los ficheros de configuración de la conexión VPN en ambos nodos de la VPN. En nuestro caso, un posible fichero de especificación de la conexión en *nodo1* es:

```
conn nodo1-nodo2
      left=147.156.1.1
      leftid=@nodo1.uv.es
```

```
      leftnexthop=147.156.1.2
      leftsubnet=192.168.1.0/24
      right=147.156.2.1
      rightid=@nodo2.uv.es
      rightnexthop=147.156.2.2
      rightsubnet=192.168.2.0/24
      authby=secret
      ikeylifetime=8h
      keylife=60m
      auto=add
```

Y el fichero de especificación de la conexión en *nodo2* es:

```
conn nodo1-nodo2
      left=147.156.1.1
      leftid=@nodo1.uv.es
      leftnexthop=147.156.1.2
      leftsubnet=192.168.1.0/24
      right=147.156.2.1
      rightid=@nodo2.uv.es
      rightnexthop=147.156.2.2
      rightsubnet=192.168.2.0/24
      authby=secret
      ikeylifetime=8h
      keylife=60m
      auto=start
```

Podemos ver que en ambos ficheros se ha definido con igual nombre la conexión (*nodo1-nodo2* en nuestro caso), como izquierda (left) la dirección pública de *nodo1*, el identificador de la izquierda como *@nodo1.uv.es*, el siguiente salto a realizar para salir a Internet desde la izquierda la dirección 147.156.1.2 y la subred privada que se encuentra a la izquierda la 192.168.1.0/24. De forma similar se han definido todos los valores de derecha (right).

Una vez definidos los nodos izquierdo y derecho, se define el mecanismo de autenticación entre los nodos (*authby*), que en nuestro caso es autenticación mediante secreto precompartido. A continuación, definimos la duraciones de la claves negociadas en la primera parte de la autenticación (8 horas) y en la segunda parte (1 hora).

Por último, con el valor auto le indicamos a nodo1 que inicialice la conexión y establezca sus valores, pero que no establezca la conexión, mientra que en nodo2 indicamos que se inicialice la conexión y es establezca la conexión con el otro nodo (nodo1 en nuestro caso). Puede observarse que en nuestro caso unicamente un nodo ejecuta automáticamente la conexión y establece un túnel VPN entre ambos nodos. En caso de que ambos nodos ejecutaran automáticamente la conexión se establecerían dos túneles VPN, lo cual puede ocasionar un excesivo uso de recursos en los nodos. Comentar, por último, que si ambos nodos inicializaran la conexión, pero ninguno de ellos levantara la misma de forma automática, puede levantarse la misma ejecutando en uno de los nodos el comando:

```
ipsec auto --up <nombre>
```

Donde <*nombre*> es el nombre de la conexión, en nuestro caso *nodo1-nodo2*.

Por su parte, el fichero que define la clave secreta precompartida de nuestro de *nodo1* sería:

```
@nodo1.uv.es @nodo2.uv.es: PSK "clave secreta precompartida"
```

Mientras que el fichero que incluye *nodo2* contiene la línea:

```
@nodo2.uv.es @nodo1.uv.es: PSK "clave secreta precompartida"
```

Donde podemos ver como siempre se especifica en primer lugar el identificador del nodo local y luego el identificador del nodo remoto.

Ejemplo de una conexión VPN.

Una vez configurada la VPN entre ambos nodos y establecida la conexión, podemos ejecutar en ambos nodos el comando:

```
ipsec auto --status
```

El cual nos indicará el estado de la VPN en ambos nodos.

En nuestro caso, si ejecutamos el comando en *nodo1*, obtenemos como salida:

```
000 using kernel interface: netkey
...
000 interface eth1/eth1 192.168.1.1
000 interface eth0/eth0 147.156.1.1
...
000 virtual_private (%priv):
000 - allowed 3 subnets: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
000 - disallowed 1 subnet: 192.168.1.0/24
...
000   "nodo1-nodo2":   192.168.1.0/24===147.156.1.1<147.156.1.1>[@nodo1.uv.es,
+S=C]---147.156.1.2...147.156.2.2---147.156.2.1<147.156.2.1>[@nodo2.uv.es,
+S=C]===192.168.2.0/24; erouted; eroute owner: #1229
000 "nodo1-nodo2":     myip=unset; hisip=unset;
000 "nodo1-nodo2":   ike_life: 3600s; ipsec_life: 28800s; rekey_margin: 540s;
rekey_fuzz: 100%; keyingtries: 0
000  "nodo1-nodo2":      policy:  PSK+ENCRYPT+TUNNEL+PFS+IKEv2ALLOW+lKOD+rKOD;
prio: 24,24; interface: eth0;
000 "nodo1-nodo2":   newest ISAKMP SA: #1232; newest IPsec SA: #1229;
000 "nodo1-nodo2":   IKE algorithm newest: AES_CBC_128-SHA1-MODP2048
000
000 #1232: "nodo1-nodo2":500 STATE_MAIN_R3 (sent MR3, ISAKMP SA established);
EVENT_SA_REPLACE in 613s; newest ISAKMP; lastdpd=-1s(seq in:0 out:0); idle;
import:not set
000 #630: "nodo1-nodo2":500 STATE_MAIN_I2 (sent MI2, expecting MR2); none in
-1s; lastdpd=-1s(seq in:0 out:0); idle; import:not set
000 #1229: "nodo1-nodo2":500 STATE_QUICK_I2 (sent QI2, IPsec SA established);
EVENT_SA_REPLACE in 18986s; newest IPSEC; eroute owner; isakmp#1228; idle;
import:not set
000  #1229:  "nodo1-nodo2"  esp.78fa3930@147.156.2.1  esp.b75f7e59@147.156.1.1
tun.0@147.156.2.1 tun.0@147.156.1.1 ref=0 refhim=4294901761
```

Donde podemos ver que se esta usando la pila de protocolos *netkey*, los interfaces del ordenador (192.168.1.1 y 147.156.1.1), las redes privadas permitidas (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16) y las denegadas (192.168.1.0/24). A

continuación, la línea 192.168.1.0/24===..., indica la ruta de la VPN que establecen los nodos entre ambas redes privadas, indicando las líneas posteriores los algoritmos de cifrado, etc., utilizados, el estado de la conexión, el tiempo de validez de las claves de sesión antes de tener que volver a ser intercambiadas, etc.

Si ejecutáramos el comando en *nodo2* obtendríamos una salida similar, con los cambios obvios de estar ejecutando el comando en *nodo2*, con diferentes direcciones IP, etc.