Introducción

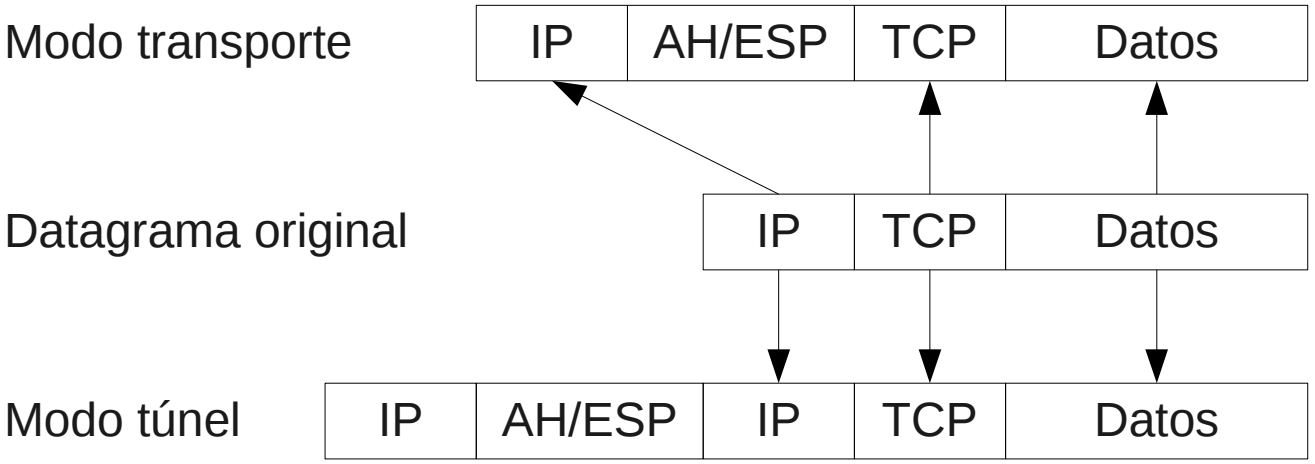
- Una Virtual Private Network permite extender una red local sobre Internet, permitiendo:
  - Conectarse un ordenador a una red local como si se encontrará en la misma (VPN de acceso remoto).
  - Conectar dos redes privadas remotas haciendo segura la comunicación de datos entre ambas redes (VPN punto a punto).
- Existen un gran número de protocolos que permiten implementar una VPN:
  - Point to Point Tunneling Protocol.
  - SSL/TLS.
  - SSH.
  - IPSec.

IPSec (I)

- Es una extensión del protocolo IP.
- Asegura las comunicaciones autenticando los paquetes.
- Cifra si se desea la información.
- Trabaja a nivel de red.
  - Puede ser utilizado por cualquier aplicación sin modificar la misma.
- Posee dos protocolos:
  - Authentication Header: Integridad, autenticación y no repudio, incluyendo la cabecera IP.
  - Encapsulation Security Payload: AH más cifrado de la información, pero sin incluir la cabecera IP.

IPSec (II)

- Puede funcionar en dos modos:
  - Transporte: Solo encapsula los datos, manteniendo la cabecera IP original.
  - Túnel: Encapsula datos y cabecera IP original, por lo que debe añadirse una nueva cabecera IP.



Configuración de Openswan

- Openswan es la implementación de IPSec existente en la mayoría de distribuciones de Linux.
- El programa que se ejecuta es /usr/sbin/ipsec.
- Se configura en dos ficheros:
  - /etc/ipsec.conf: Configuración general del programa, direcciones de red, valores de las VPNs, etc.
  - Dos tipos de secciones:
    - config setup: Configuración del programa.
    - conn <nombre>: Configuración de una conexión.
  - /etc/ipsec.secrets: Claves secretas precompartidas entre los nodos de la VPN.

Fichero ipsec.conf (I)

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.
protostack	Pila de protocolos a utilizar para dar soporte a IPSec. Puede tomar los valores *auto*, *klips*, *netkey* y *mast* (variación de *netkey*).
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.

Fichero ipsec.conf (II)

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 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}*.

Fichero ipsec.conf (III)

Parámetro	Descripción
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.
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*.

Fichero ipsec.conf (IV)

Parámetro	Descripción
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.
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*.

Fichero ipsec.conf (V)

Parámetro	Descripción
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.

Fichero ipsec.conf (VI)

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.

Fichero ipsec.conf (VII)

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

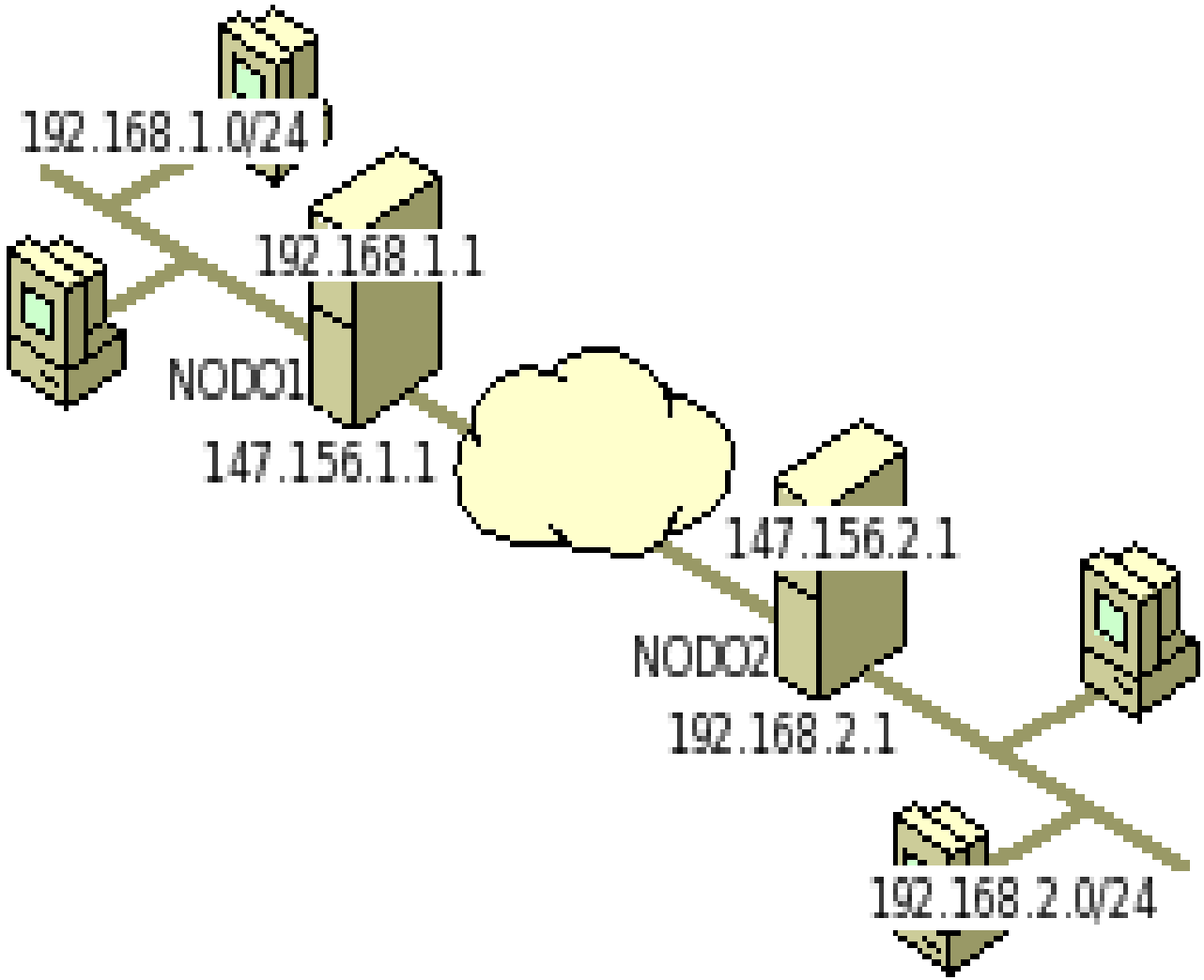
- Contiene las claves precompartidas, firmas digitales RSA, etc.
- Las claves precompartidas se especifican como:

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

- Identificando siempre en primer lugar el nodo local.
- Firma digital RSA:

```
@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...
          }
```

Ejemplo de configuración (I)



Ejemplo de configuración (II)

- nodo1:

```
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
```

Ejemplo de configuración (III)

- nodo2:

```
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
```

Ejemplo de configuración (IV)

- nodo1:

```
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
ikelifetime=8h
keylife=60m
auto=add
```

Ejemplo de configuración (V)

- nodo2:

```
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
ikelifetime=8h
keylife=60m
auto=start
```

Ejemplo de configuración (VI)

- Claves secretas precompartidas:
  - Fichero ipsec.secrets en nodo1:

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

  - Fichero ipsec.secrets en nodo2:

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

- Donde podemos ver que siempre va en primer lugar el nodo local y después el remoto.

Ejemplo de conexión (I)

```
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;
```

Ejemplo de conexión (II)

```
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
```