Router Teldat

IPSec

Doc. *DM739* Rev. *10.10*
Agosto, 2003

ÍNDICE

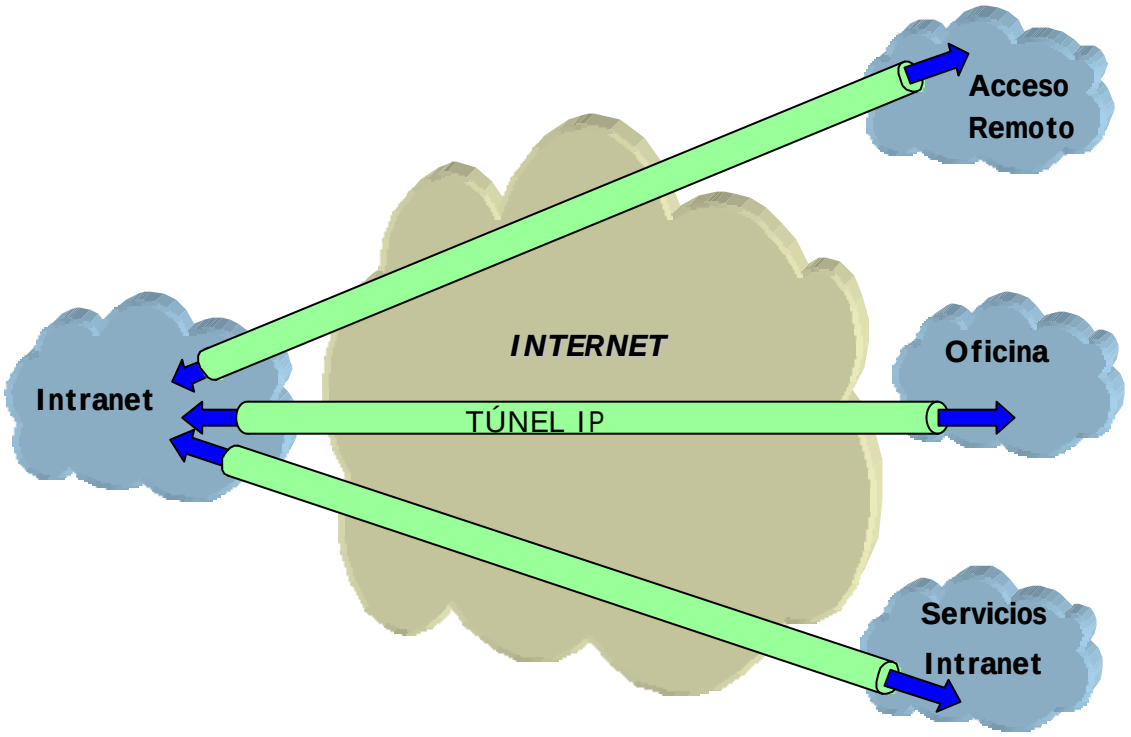
Capítulo 1
Introducción

1. Virtual Private Networks

Hasta ahora, el uso tradicional de Internet para las empresas era promocionar sus servicios y productos a través de los Web Sites. Actualmente, cada vez más empresas utilizan Internet para comunicar sus diferentes delegaciones, oficinas o centros de desarrollo y producción. En definitiva, Internet puede desplazar a las líneas privadas costosas y poco flexibles. Además, el e-business necesita del acceso global (World Wide Web) que ofrece Internet.

Los paquetes que circulan por las redes publicas, como Internet, se desplazan por múltiples nodos que no podemos controlar ni vigilar. El camino de los paquetes para un mismo destino es variable, por lo tanto es necesario establecer mecanismos de seguridad que impidan a cualquier intruso acceder a la información que enviamos a través de este tipo de redes.

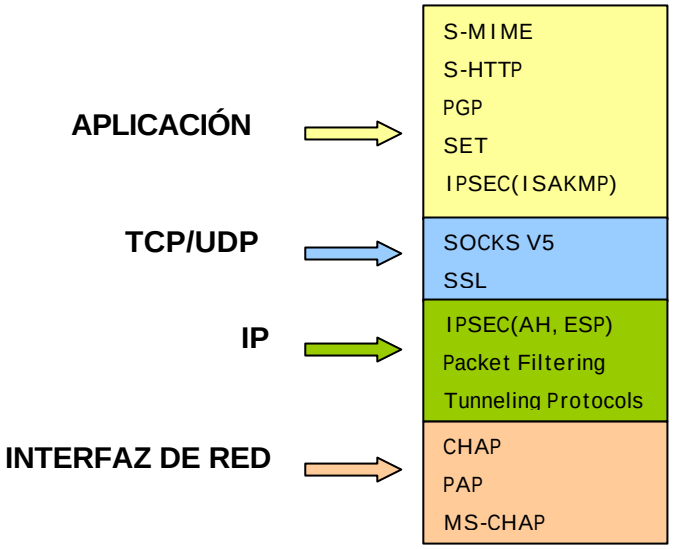
Una Virtual Private Network (VPN) tiene como objetivo extender la Intranet de una empresa a través de una red publica como Internet creando una comunicación segura con Túneles Privados.



Existen diferentes tipos de soluciones VPN´s que se pueden clasificar en función del nivel OSI del protocolo en el que están implementadas:

- Las VPN´s implementadas en el nivel de *aplicación*: Autentican y/o encriptan el mensaje pero no la dirección origen y destino de los paquetes que lo encaminan.
- Las VPN´s basadas en el nivel de *enlace*: Como L2TP, sólo pueden autenticar los nodos extremos del Túnel pero no cada paquete por separado.
- Las VPN´s implementadas en el nivel de *red*: Como IPSec, que protege los datos y las direcciones IP origen y destino sin tener el usuario que modificar las aplicaciones. Sin embargo, fuera del Túnel establecido, por ejemplo en la Intranet de la empresa, no ofrece ninguna protección.

Como conclusión, conviene combinar VPN´s de nivel de aplicación con VPN´s de nivel de red para obtener el nivel de seguridad adecuado.



2. IPSec

IPSec es una plataforma de seguridad a nivel de *red* desarrollada por el *IPSec Working Group* de la *IETF*. Permite acomodar nuevos algoritmos de encriptación y autenticación de forma flexible y robusta.

IPSec se concentra en los siguientes problemas de seguridad:

- Autenticación del origen de los datos: verificar que los datos recibidos han sido enviados por quien dice haberlos enviado.
- Integridad de los datos: verificar que los datos recibidos no han sido modificados por el camino.

  Se suele emplear el término autenticación de datos para indicar tanto la integridad de los datos como la autenticación de su origen.
- Confidencialidad de los datos: ocultar los datos utilizando un algoritmo de encriptación.
- Protección tipo Anti-Replica: evitar que un intruso nos reenvíe alguno de nuestros mensajes y no seamos capaces de detectarlo.
- Gestión automática de claves criptográficas.

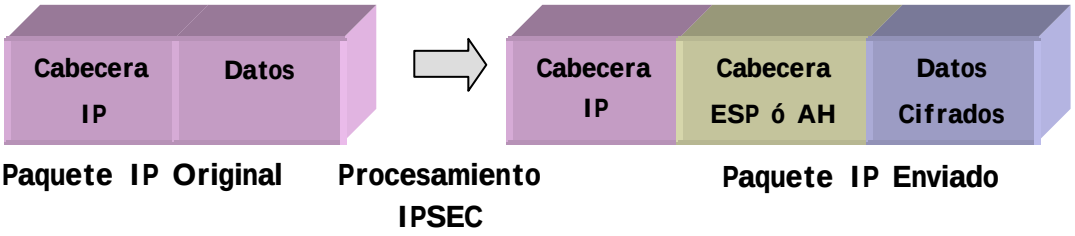
Para solucionar estos aspectos, IPSec define dos servicios distintos de seguridad:

- **ESP:** *Encapsulating Security Payload*: Proporciona confidencialidad, autenticación de dirección origen en cada paquete IP, integridad, y protección ante réplicas.
- **AH:** *Authentication Header*: Proporciona autenticación de dirección origen en cada paquete IP, integridad y protección ante réplicas, pero no ofrece confidencialidad de los datos. Este servicio es apropiado en aquellos casos en que tan sólo se necesita asegurar el origen de los datos.

2.1. Los Túneles IPSec

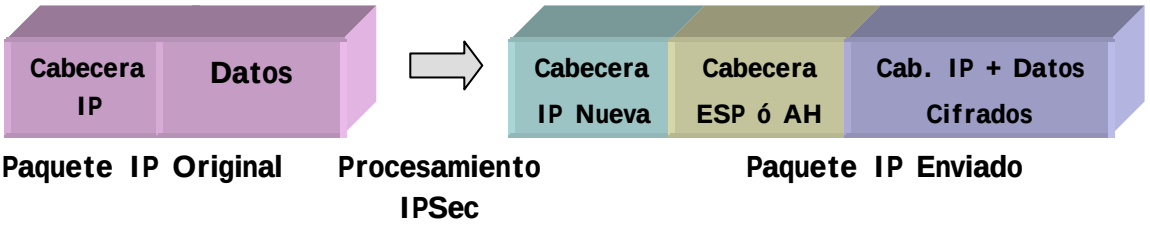
La plataforma IPSec permite dos modos de funcionamiento, pudiendo emplear en cada uno de ellos cualquiera de los dos servicios de seguridad ESP o AH:

- **Modo Transporte:** permite una comunicación segura, normalmente establecida entre dos hosts (por ejemplo, la comunicación entre una estación de trabajo y un servidor, o entre dos servidores) pero en ningún caso enmascara la dirección origen y destino del paquete a enviar. En el modo transporte, IPSec sólo actúa sobre los datos internos del paquete IP, sin modificar la cabecera de éste. Por ejemplo, sobre un segmento TCP o UDP, o un paquete ICMP.



- **Modo Túnel:** se encapsula el paquete IP original entero en un nuevo paquete IP, ocultando así todo el contenido original. De esta forma, la información viaja a través de un 'túnel' desde un

punto de la red a otro, sin que pueda ser examinado su contenido. Este modo es el más apropiado para utilizarlo en las comunicaciones entre un router y un host externo, o entre dos routers.



2.2. Arquitectura IPSec

a) *La base de datos de políticas (SPD)*

La plataforma IPSec necesita saber qué *política de seguridad* aplicar al paquete IP, en función de los campos de cabecera, también llamados *selectores*. Las políticas de seguridad deciden qué algoritmos de cifrado y autenticación se han de usar en la conexión segura.

La base de datos de políticas de seguridad o ***Security Policy Database*** (**SPD**) almacena las entradas que contienen selectores de control, y sus políticas de seguridad asociadas.

Tras mirar en la base de datos de políticas de seguridad, dentro de las acciones aplicables a un paquete IP existen 3 posibilidades:

- Descartar el paquete.
- Enrutar el paquete de forma normal.
- Aplicar Seguridad IPSec con unos determinados algoritmos de encriptación o autenticación, que dependerán del compromiso de seguridad-rendimiento que adoptemos. Por ejemplo, si consideramos más importante la velocidad de procesado que la seguridad, elegiremos una política con encriptación DES en lugar de Triple DES.

b) *Las asociaciones de seguridad (SA's)*

Un paquete cuyos selectores coincidan con una de las entradas de la ***SPD*** se procesará de acuerdo con la política asociada a esa entrada. Una *Security Association* es la conexión de seguridad que se crea una vez consultada la ***SPD*** y contiene la información de seguridad (claves de autenticación y encriptación) necesaria para procesar el paquete.

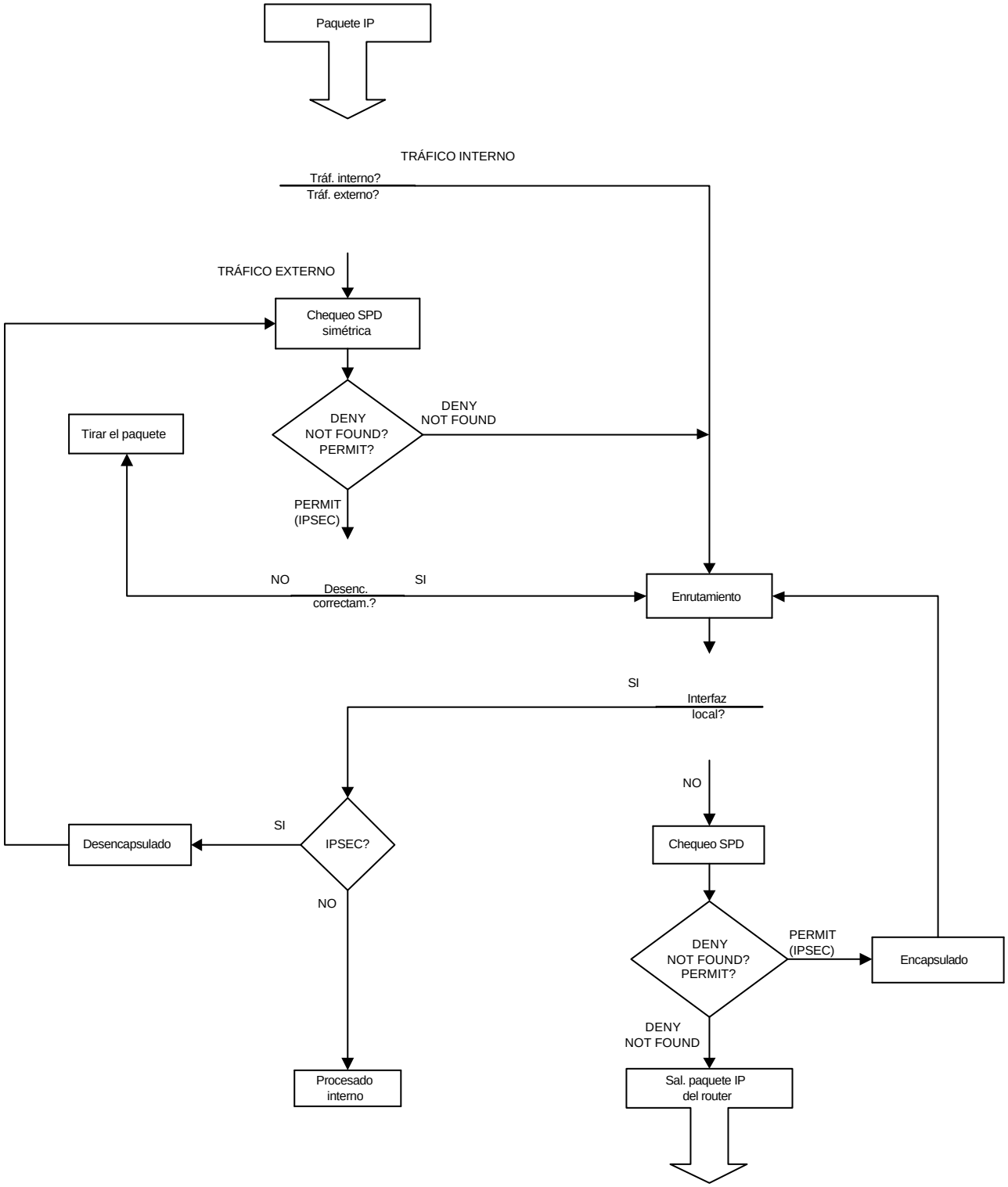
Dentro del servicio de seguridad (ESP o AH) que se defina, podemos elegir diferentes tipos de algoritmos de encriptación (DES, TRIPLE DES, etc.), o autenticación (MD5, SHA1, etc.).

c) *Procesamiento de paquetes con IPSec*

Existe una sola ***SPD*** o base de datos de políticas, que define el usuario. Esta base de datos se define para el tráfico de salida del router, mientras el tráfico de entrada es controlado mediante una ***SPD implícita***, simétrica de la anterior. De esta forma, todo paquete de entrada se procesa en la forma en que se contestaría a ese paquete: si se define que un cierto tráfico de salida debe ser enviado con una política IPSec de seguridad concreta, se espera que el tráfico correspondiente de entrada cumpla con la misma política. De igual forma, si la acción definida para el tráfico de salida fuera enrutar / descartar, el tráfico de entrada sería enrutado / descartado.

Tras hacer el routing interno, se chequea la ***SPD***, esta vez para el tráfico de salida, e igualmente se debe decidir entre su encapsulado previo IPSec, su envío o su eliminación.

El diagrama de la siguiente figura describe el procesamiento de un paquete IP en los **Router Teldat** con el protocolo IPSec.



2.3. IPSec avanzado

a) Gestión de claves

Toda plataforma de seguridad basada en claves secretas deja de ser segura si las claves no se renuevan cada cierto tiempo.

Cuanto menor sea el periodo de refresco, mayor será la seguridad de nuestro sistema frente a herramientas de Criptoanálisis.

Para la gestión de las claves y parámetros de seguridad en IPSec existen dos modos generales de trabajo posibles: manual (IPSec manual) y automático o dinámico (IPSec IKE). Estos modos hacen referencia a la forma en que se acuerda entre extremos los parámetros de seguridad del Túnel a establecer.

b) IPSec manual

En IPSec manual, "manual-keying", las claves que se utilizan en el proceso de encriptación y/o autenticación para cada SA, son introducidas por el usuario. Este último debe introducir los mismos parámetros de seguridad (claves, algoritmos de cifrado y autenticación) para ambos extremos del Túnel para que la comunicación segura se pueda realizar. Esto es práctico para entornos pequeños y relativamente estáticos. Sin embargo, cuando la VPN empieza a crecer, la renovación de claves manualmente puede resultar una tarea demasiado costosa.

c) IPSec IKE

La plataforma IPSec permite automatizar este proceso gracias al protocolo *IKE, Internet Key Exchange* (basado en el protocolo de intercambio de claves OAKLEY y la plataforma ISAKMP). Los dos extremos del Túnel negocian automáticamente los parámetros de la comunicación segura (claves, algoritmos de cifrado y autenticación). Para efectuar esta negociación, los extremos antes han de llevar a cabo una **primera fase**, en la que se ponen de acuerdo en los parámetros de seguridad que protegerán la negociación. En esta primera fase además, se lleva a cabo una autenticación de los extremos del Túnel, utilizando una clave común (*Pre-shared Key*) introducida manualmente en ambos extremos, utilizando firmas digitales o con un algoritmo de clave pública.

Existen dos modos de negociación previa: *Main Mode* y *Aggressive Mode*.

- *Main Mode* enmascara las identidades de los routers extremos del Túnel. En este tipo de negociación es necesario que ambos extremos conozcan las direcciones IP del servidor de seguridad al que se enfrentan.
- *Aggressive Mode* no enmascara estas identidades y mejora la velocidad de procesamiento de la autenticación. Además, no es necesario conocer la dirección IP del otro extremo del Túnel, lo que permite establecer un Túnel con un router de seguridad desconocido si la política de seguridad aplicable al paquete lo permite.

IPSec IKE tiene cuatro modos de funcionamiento para la primera fase, según el tipo de autenticación utilizado para negociar los parámetros de seguridad de las SA´s.

· Autenticación con Pre-shared Key

La misma clave (Pre-shared Key) manualmente introducida en los dos ROUTERS DE SEGURIDAD permite que se autentiquen mutuamente.

Existen dos tipos de intercambio con Pre-shared Key: *Main Mode* y *Aggressive Mode*.

- *Main Mode* enmascara las identidades de los routers extremos del Túnel.
- *Aggressive Mode* no enmascara estas identidades y mejora la velocidad de procesamiento de la autenticación.

Cada vez que el tiempo de vida de la SA expire, un nuevo material de claves se intercambiará entre los dos routers de seguridad, previa autenticación con la clave Pre-shared manual.

Por otra parte, IPSec "manual-keying" e IPSec con Pre-shared Key obligan a conocer la dirección IP del extremo del Túnel (dirección IP del router de seguridad al que nos enfrentamos).

Sin embargo, los siguientes tipos de IPSec IKE permiten, automática y dinámicamente, establecer un Túnel con un router de seguridad desconocido, si la política de seguridad aplicable al paquete lo permite. En estos tipos de IPSec IKE, no es necesario introducir una clave común en los extremos del Túnel, ya que ésta se obtiene automáticamente mediante los procedimientos descritos a continuación.

· *Autenticación con Firmas*

La autenticación de los dos extremos del Túnel se realiza mediante una firma digital y el sistema de intercambio de claves "Diffie Hellman".

Existen también los tipos de intercambio *Main Mode* y *Aggressive Mode*.

- *Main Mode* enmascara las identidades de los routers extremos del Túnel.
- *Aggressive Mode* no enmascara estas identidades pero mejora la velocidad de la autenticación.

· *Autenticación con Cifrado de Clave Pública*

La autenticación se realiza por RSA previo conocimiento de la clave pública del otro router. Las claves públicas del otro extremo del Túnel se pueden obtener mediante *certificados*.

Existen también los tipos de intercambio *Main Mode* y *Aggressive Mode*. Si la clave pública se actualiza con frecuencia, el *Aggressive Mode* es igual de seguro que el *Main Mode* y más rápido.

Además Autenticación con Cifrado de Clave Pública ofrece mayor seguridad con respecto a Autenticación con Firmas y Autenticación con Pre-shared Key, por combinar el sistema de clave pública RSA y el sistema de intercambio de claves "Diffie Hellman". Sin embargo, el tiempo de procesamiento de Autenticación con Cifrado de Clave Pública es mucho mayor.

· *Autenticación con Cifrado de Clave Pública Revisado*

La autenticación se realiza también por RSA previo conocimiento de la clave publica del otro router. Las claves públicas del otro extremo del Túnel se pueden obtener mediante *certificados*.

Sin embargo, se reducen las operaciones con clave pública con una pérdida de seguridad insignificante, pero mejorando las prestaciones de la autenticación.

Existen también los tipos de intercambio *Main Mode* y *Aggressive Mode*. Si la clave pública se actualiza con frecuencia, el *Aggressive Mode* es igual de seguro que el *Main Mode* y más rápido.

d) Alta seguridad

Las claves utilizadas para cifrar o autenticar una comunicación se obtienen de un *Material para Claves*. Si este material no ha originado ni originará otras claves para cifrar o autenticar otras comunicaciones, entonces decimos que se ha conseguido ***Perfect Forward Secrecy***.

Los **Router Teldat** en modo alta seguridad permiten conseguir *Perfect Forward Secrecy* a costa de un mayor coste computacional en el establecimiento de los Túneles IPSec.

El modo alta seguridad genera también un material de claves más seguro utilizando Grupos OAKLEY más resistentes al Criptoanálisis.

e) Certificados

Los certificados permiten conocer las claves públicas de otros routers de seguridad con los que es posible establecer un Túnel IPSec. Estas claves publicas serán utilizadas en los dos modos IKE de autenticación con clave pública.

Capítulo 2
Configuración

1. Introducción

Como hemos visto en el apartado 2.2 “Arquitectura IPSec” del capítulo 1, el procesamiento de un paquete IP por parte del módulo IPSec se basa en aplicar la política de seguridad configurada para dicho paquete. Esta información se almacena en la ***Security Policy Database (SPD)***, donde se encuentran los selectores y las políticas de seguridad asociadas. Por lo tanto, la configuración de IPSec en un equipo se reduce a la definición de los elementos de la ***SPD***.

En los **Router Teldat** la configuración de un elemento de la ***SPD*** se hace en tres pasos. Primero se define un elemento o entrada de la Lista de Control de Acceso (LCA), es decir, unos selectores de control determinados, lo cual se lleva a cabo asignando a IPSec una lista de acceso genérica, previamente configurada. A cada entrada de la lista se le configura un tipo de decisión, que puede ser dejar pasar el paquete sin aplicarle el procesado correspondiente al protocolo o facilidad a que haya sido asignada esa lista (Deny), o bien aplicarle el procesado correspondiente, en este caso IPSec (Permit). Después se crean los **Templates** o políticas de seguridad IPSec, donde se definen los parámetros de seguridad del Túnel IPSec. Y por último, una lista de control de acceso asignada a IPSec se asocia (mapea) con un **Template** concreto.

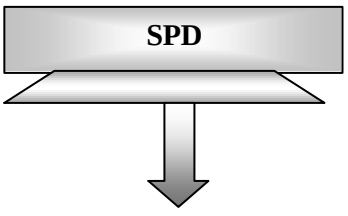
Lista de control de acceso 1	
Entrada 1	✓ IP origen ✓ Permit ✓ Protocolo
Entrada 2	✓ IP origen ✓ Permit ✓ Puertos ✓ Conexión
...	...
Entrada n	✓ IP origen ✓ Deny ✓ Protocolos

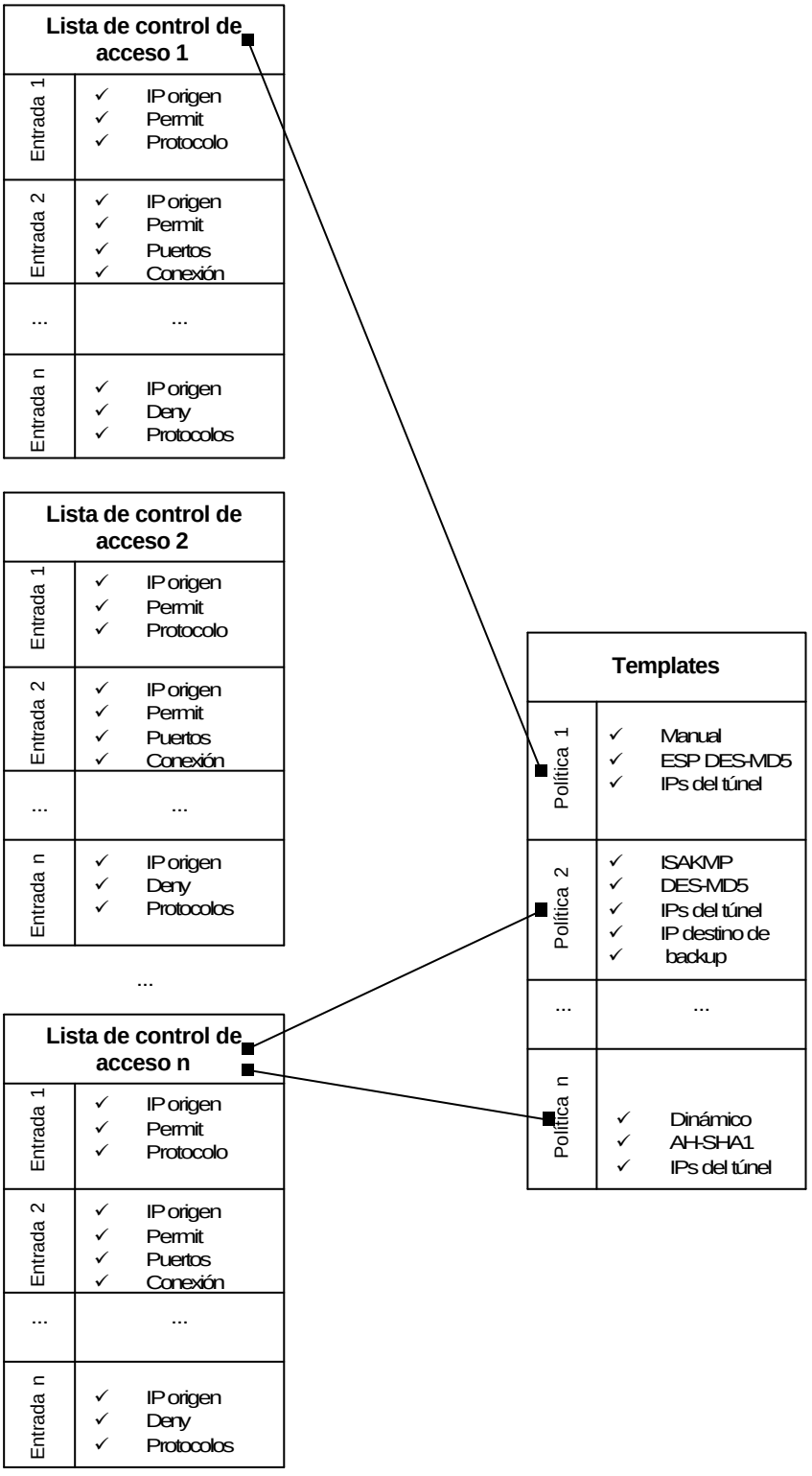
Lista de control de acceso 2	
Entrada 1	✓ IP origen ✓ Permit ✓ Protocolo
Entrada 2	✓ IP origen ✓ Permit ✓ Puertos ✓ Conexión
...	...
Entrada n	✓ IP origen ✓ Deny ✓ Protocolos

...

Lista de control de acceso n	
Entrada 1	✓ IP origen ✓ Permit ✓ Protocolo
Entrada 2	✓ IP origen ✓ Permit ✓ Puertos ✓ Conexión
...	...
Entrada n	✓ IP origen ✓ Deny ✓ Protocolos

Templates	
Política 1	✓ Manual ✓ ESP DES-MD5 ✓ IPs del túnel
Política 2	✓ ISAKMP ✓ DES-MD5 ✓ IPs del túnel ✓ IP destino de ✓ backup
...	...
Política n	✓ Dinámico ✓ AH-SHA1 ✓ IPs del túnel




Lista de control de acceso 1
Entrada 1
✓ IP origen
✓ Permit
✓ Protocolo
Entrada 2
✓ IP origen
✓ Permit
✓ Puertos
✓ Conexión
...
...
Entrada n
✓ IP origen
✓ Deny
✓ Protocolos
Lista de control de acceso 2
Entrada 1
✓ IP origen
✓ Permit
✓ Protocolo
Entrada 2
✓ IP origen
✓ Permit
✓ Puertos
✓ Conexión
...
...
Entrada n
✓ IP origen
✓ Deny
✓ Protocolos
...
Lista de control de acceso n
Entrada 1
✓ IP origen
✓ Permit
✓ Protocolo
Entrada 2
✓ IP origen
✓ Permit
✓ Puertos
✓ Conexión
...
...
Entrada n
✓ IP origen
✓ Deny
✓ Protocolos
Templates
Política 1
✓ Manual
✓ ESP DES-MD5
✓ IPs del túnel
Política 2
✓ ISAKMP
✓ DES-MD5
✓ IPs del túnel
✓ IP destino de
✓ backup
...
...
Política n
✓ Dinámico
✓ AH-SHA1
✓ IPs del túnel

2. Primeros pasos

2.1. Configuraciones iniciales

Puesto que el acceso al equipo permite la modificación de los parámetros de IPSec, primero habrían de configurarse las passwords de acceso por Telnet y por Consola del equipo.

En el caso de usar certificados, hay que configurar adecuadamente la fecha y hora del equipo para no tener problemas con la validez de estos (en esta versión no hace falta).

Si se realiza una actualización de software antiguo a software con IPSec, conviene saber que por defecto IPSec esta deshabilitado, luego no se hace ninguna consulta a la ***SPD***. Ya podemos empezar a configurar la ***SPD*** sin afectar al tráfico. El tráfico se procesa en transparente como antes de la actualización. Una vez configurado y habilitado IPSec, se guarda la configuración y se reinicia el equipo para activarlo.

Si se quisiera instalar el router de seguridad en una nueva red, sin permitir la salida o la entrada de ningún paquete sin consultar la ***SPD***, se conectará el router a la red, no sin antes haber establecido que se descarte cualquier paquete que llegue y habilitado entonces IPSec (esto se verá como hacerlo más adelante). Luego se irá configurando y permitiendo el tráfico que se desee.

Comandos DISABLE / ENABLE

El comando **DISABLE**, dentro del menú de configuración IPSec, permite deshabilitar IPSec.

```
Config>PROTOCOL IP

-- Internet protocol user configuration --
IP config>IPSEC

-- IPSec user configuration --
IPSec config>DISABLE
IPSec config>
```

Tan sólo hay que escribir el comando **ENABLE** para habilitarlo

En los equipos Nucleox Plus, además es necesario habilitar las interrupciones de la tarjeta de cifrado. Si no se cambia, la contraseña de acceso a esta configuración es **teldat.**

```
Config>UCI CHANGE CFG

User Password? ******


Configuration

Interruption mode  (y/other)? (YES) y
Test RSA when starting (y/other)? (NO)
Max NRIs (10-500)? (100)
Flag Crypto? (NO)
You must restart so that the new configuration becomes effective
    Updating encrypt configuration...
```

3. Configuración de IPSec

3.1. Orden correcto para una buena configuración

Una vez conectado el equipo a la red privada y a la red publica, hay que configurar la ***SPD*** para los paquetes de entrada y de salida.

Los pasos a seguir recomendados para generar una configuración son:

a) Configuración de la Lista de Control de Acceso de IPSec
b) Configuración de los Templates (parámetros de seguridad)
c) Creación de la SPD

3.2. Configuración

En este apartado se describen los pasos necesarios para configurar IPSec en los **Router Teldat**. Para acceder al entorno de configuración del protocolo IPSec se deben introducir los siguientes comandos:

```
Config>PROTOCOL IP

-- Internet protocol user configuration --
IP config>IPSEC

-- IPSec user configuration --
IPSec config>
```

Dentro del entorno de configuración del protocolo IPSec (indicado por el prompt **IPSec config**>) se dispone de los siguientes comandos:

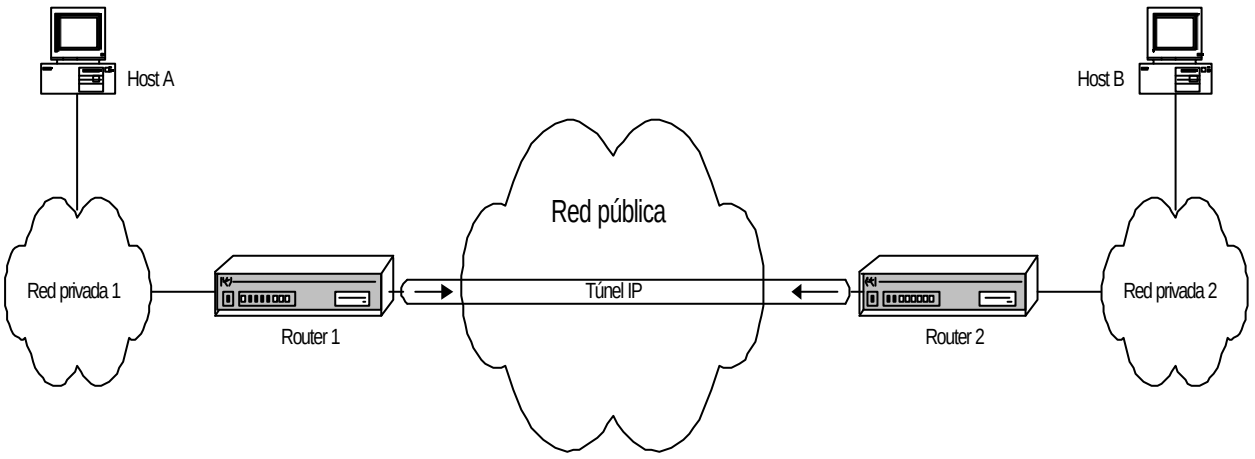
Comando	**Función**
? (AYUDA)	Lista los comandos u opciones disponibles.
ENABLE	Permite habilitar IPSec, y filtrar los eventos a visualizar.
DISABLE	Deshabilita IPSec.
ASSIGN-ACCESS-LIST	Asigna una lista de control de acceso al protocolo IPSec.
TEMPLATE	Comando para configurar los parámetros de las políticas de seguridad de los Túneles IPSec.
MAP-TEMPLATE	Comando que asocia (mapea) un elemento de la lista de control de acceso con un Template.
ASSOCIATE-KEY	Asocia una clave a una lista de control de acceso.
KEY	Usado y definido en el apartado de Templates Dinámicos (IPSec IKE).
EVENT	Permite configurar un filtro para limitar los eventos a visualizar o bien dejar que se muestren todos.
QOS-PRE-CLASSIFY	Habilita el pre-filtrado de paquetes (para BRS).
ADVANCED	Configuración de parámetros avanzados.
LIST	Lista la configuración de IPSec.
NO	Borra elementos de las listas Templates y Access-Control, y deshace mapeados, o bien puede borrar la configuración completa.
EXIT	Sale del prompt de configuración de IPSec.

En general, si no se introducen en la línea de comandos todos los parámetros necesarios para completar un comando, el equipo los irá solicitando, excepto cuando haya opción de escribir subcomandos. En cualquier caso, siempre se puede teclear el comando o subcomando seguido de '**?**' para obtener ayuda.

```
IPSec config>?
ENABLE                  Enables IPSec
DISABLE                 Disables IPSec
ASSIGN-ACCESS-LIST      Assigns access lists to IPSec (used as SPD selectors)
TEMPLATE                Configures security policies params for IPSec tunnels
MAP-TEMPLATE            Associates an element in the LCA with a template
ASSOCIATE-KEY           Associates a key to an access list
KEY                     Adds preshared or RSA keys
EVENT                   Adds a filter for IPSec events or enables all of them
QOS-PRE-CLASSIFY        Enables QOS Preclasiffy
ADVANCED                Configuration of advanced IPSec parameters
LIST                    Lists the IPSec configuration
NO                      Disables options, deletes items or sets default values
EXIT                    Exits IPSec configuration menu
IPSec config>
```

a) Configuración de la Lista de Control de Acceso de IPSec

Como se ha explicado existe una lista de control de acceso. Cada entrada de esta lista es un bloque de selectores y una *acción*, y está identificada por un único número (el identificador o campo ID de la entrada). El bloque de selectores esta compuesto por una dirección IP origen (o rango de direcciones), una dirección IP destino (o rango de direcciones IP destino), un protocolo (o rango de protocolos), puertos origen y destino (o rango de puertos), y el identificador de la conexión entre interfaces por los que viajaría el paquete. No es necesario especificarlos todos, tan sólo el que se desee. La *acción* representa el procesamiento asignado a los paquetes coincidentes con el bloque de selectores asociado: PERMIT o DENY.



Como se explicó al analizar la ***SPD***, la especificación de las entradas o elementos de la LCA se establece siempre para los **paquetes de salida** a través de las interfaces del router. Como ejemplo, en la figura anterior se desea establecer un Túnel seguro IPSec para los paquetes que viajen entre el host A y el host B. Para ello, la entrada de control a establecer en la LCA contendría los siguientes selectores (como mínimo):

- Dirección IP origen: IP del host A;
- Dirección IP destino: IP del host B;
- Acción: PERMIT (procesado IPSec);

Cualquier paquete que viajara de A a B, sería de esta forma encapsulado por IPSec. Implícitamente al definir esta entrada, a cualquier paquete que llegara del extremo B con dirección A se le exigiría venir igualmente encapsulado, quedando así completamente definido el Túnel seguro entre ambos extremos.

El orden en la Lista de Control de Acceso es importante en el caso en el que la información referenciada por los selectores se solape entre diferentes elementos de la LCA.

Sin embargo, este orden no lo da el identificador ID de cada entrada, sino el orden al listarlas de las mismas (que se permite modificar). Es decir, si al recorrer la lista, empezando por el primer elemento o entrada que aparece al listar, se encuentra un elemento que encaja en nuestra búsqueda, no se sigue buscando y se aplica la acción indicada en dicho elemento.

IPSec hace uso de las listas de control de acceso genéricas y extendidas definidas en el menú raíz de configuración del equipo ***Config*>FEATURE ACCESS-LISTS.** Las listas creadas en este menú se deben asignar al protocolo IPSec mediante el comando ***IPSec config*>ASSIGN-ACCESS-LIST.**

Una lista de control de acceso genérica y extendida está formada por una serie de *entradas* que definen las propiedades que debe tener un paquete para que se considere que perteneciente a esa entrada y por consiguiente a esa lista. Después, esa lista de control de acceso genérica se asigna a un protocolo.

El primer paso consiste en crear la lista de control de acceso con el comando **ACCESS-LIST #**. Por ejemplo, **ACCESS-LIST 100**, nos introduce en el menú ***Extended Access List 100*>.** Donde se puede ir dando de alta entradas, con los comandos **ENTRY # subcomando**.

Luego, las listas de control de acceso están formadas por entradas que admiten los siguientes subcomandos:

Comando	Función
PERMIT	Tipo de acción (procesado IPSec en caso de asignar la lista a este protocolo).
DENY	Tipo de acción: no llevar a cabo ningún procesado.
SOURCE ADDRESS	Define el selector dirección IP origen de la entrada de la Lista.
SOURCE PORT-RANGE	Define el selector puerto origen de la entrada.
DESTINATION ADDRESS	Define el selector dirección IP destino de la entrada.
DESTINATION PORT-RANGE	Define el selector puerto destino de la entrada.
PROTOCOL-RANGE	Define el selector protocolo de la entrada.
DSCP	Diff Serv codepoint.
CONNECTION	Selector identificador de la conexión entre interfaces.

Y los comandos especiales

Comando	Función
LIST	Para listar las entradas.
MOVE-ENTRY	Para cambiar el orden de las entradas.
NO	Para borrar una entrada.

Como ejemplo se van a mostrar los formatos de todos los subcomandos y un ejemplo de cada uno en una posible configuración.

"ENTRY [ID] PERMIT"

Identifica la entrada del tipo permitido. Para el caso de IPSec indica que se debe hacer IPSec, por lo tanto, la entrada en la lista de control de acceso con esta acción especifica cuales serán los *clientes del Túnel*, es decir, define el tráfico que pasará por el Túnel. El campo ID es el entero que identifica la entrada o elemento en la lista de control de acceso.

Ejemplo:

```
Extended Access List 100>ENTRY 10 permit
```

"ENTRY [ID] DENY"

Identifica la entrada del tipo no permitido. Para el caso de IPSec indica que no se debe hacer IPSec.

Ejemplo:

```
Extended Access List 100>ENTRY 10 deny
```

"ENTRY [ID] SOURCE ADDRESS [DIR IP] [MASK]"

Para establecer el selector de dirección IP origen de un posible paquete. El rango de direcciones elegido se indica en forma de mascara de subred. De nuevo, el ID es el entero que identifica al elemento o entrada en la lista de control de acceso.

Esta dirección puede ser no numerada, es decir, se puede poner una dirección asociada a un interfaz y que es desconocida en el momento de configurar el equipo porque, por ejemplo, será asignada por algún otro mecanismo, como pudiera ser PPP.

Ejemplo 1:

```
Extended Access List 100>ENTRY 10 source address 192.168.4.5 255.255.255.255
```

Ejemplo 2:

```
Extended Access List 100>ENTRY 10 source address 192.168.4.0 255.255.255.0
```

En el Ejemplo 1, la dirección IP de origen es única, y en el Ejemplo 2, la dirección origen es toda la subred 192.168.4.0 con mascara 255.255.255.0. Nótese que al usar el mismo ID (10), la nueva información se añade o sustituye a la que ya hubiera para ese elemento, y así la entrada final queda modificada como se muestra en el ejemplo segundo.

Como se mencionó, se puede elegir no introducir todos los parámetros de un comando o subcomando, o pedir ayuda ('**?**'), y que sea el router el que los vaya pidiendo progresivamente. En el siguiente ejemplo se muestra como funciona esto en el caso de querer introducir los mismos datos mostrados en el ejemplo anterior (Ejemplo 2):

```
Extended Access List 100>ENTRY 10 source address
Source IP address [0.0.0.0]? 192.168.4.0
Source IP mask [0.0.0.0]? 255.255.255.0
```

"ENTRY [ID] SOURCE PORT-RANGE [LOW] [HIGH]"

Establece el selector para el puerto origen (Source Port). Se puede seleccionar también un rango, usando los campos LOW y HIGH como identificadores de puerto, o un solo puerto dejando ambos valores iguales.

Ejemplo:

```
Extended Access List 100>ENTRY 10 source port-range 21 25
```

"ENTRY [ID] DESTINATION ADDRESS [DIR IP] [MASK]"

Comando similar al que establece el selector de dirección IP origen de un posible paquete, pero para establecer el selector de dirección IP destino.

Ejemplo:

```
Extended Access List 100>ENTRY 10 destination address 192.168.10.0 255.255.255.0
```

"ENTRY [ID] DESTINATION PORT-RANGE [LOW] [HIGH]"

Establece el selector para el puerto destino (Destination Port). Igualmente, se puede seleccionar un rango, usando los campos LOW y HIGH como identificadores de puerto, o un solo puerto dejando ambos valores iguales.

Ejemplo:

```
Extended Access List 100>ENTRY 10 destination port-range 1000 2000
```

Si una vez introducido, se desea eliminar el control del puerto destino (o puerto origen), como originalmente se encuentra, basta con introducir el rango completo. En este caso:

```
Extended Access List 100>ENTRY 10 destination port-range 0 65535
```

Al especificar el rango completo, por defecto ya no aparece el selector correspondiente.

"ENTRY [ID] PROTOCOL-RANGE [LOW] [HIGH]"

Para establecer el selector del protocolo o rangos de protocolos del paquete. El campo LOW es el identificador de protocolo en el límite inferior del rango, y el campo HIGH el identificador en el límite superior. En caso de no desear un rango, basta con poner ambos valores iguales.

Ejemplo:

```
Extended Access List 100> ENTRY 10 protocol-range 1 9
```

"ENTRY [ID] CONNECTION [ID CONN]"

Permite establecer el identificador de la conexión entre interfaces para una entrada de la LCA. Esta conexión identifica la interfaz lógica por la que se enrutaría el paquete; se configura en las reglas de IP. Al establecer esta relación, IPSec puede asociar el tráfico no sólo por la dirección origen, destino, etc, del paquete, sino también por el interfaz concreto de conexión. El campo ID es el entero que identifica la entrada o elemento en la lista de control de acceso.

Ejemplo:
Suponiendo que exista la siguiente regla definida en IP:

ID	Local Address --> Remote Address	Timeout	Firewall	NAPT
1	172.24.70.1 --> 172.24.70.2	0	NO	NO

Esto identifica una conexión concreta, entre una dirección local del router y un extremo (el resto de parámetros no se consideran). Definimos entonces una entrada en la LCA, con el identificador de esta conexión (**1**) como selector:

```
Extended Access List 100>ENTRY 10 connection 1
```

Dejar la conexión sin especificar, o poner conexión cero, hace que la conexión no se considere al mirar la LCA.

Aparecerá una interrogación al lado de la conexión (p. ej, **Conn:1?**) si ésta no existe, junto con un mensaje de aviso.

Con esto quedarían configurados todos los selectores para un elemento de la lista de acceso. Si no se configurara alguno de ellos, simplemente no se tendría en cuenta a la hora de comprobar un paquete contra la lista de control.

Queda por definir por tanto la acción a ejecutar sobre un paquete que coincidiera con esta selección, y también modificar si se considera necesario la prioridad de esta entrada sobre el resto en la lista. Para ello se usan los siguientes subcomandos:

"MOVE-ENTRY [ID_TO_MOVE][ID_BEFORE]"

Modifica la prioridad de una entrada, colocando el elemento "ID_TO_MOVE" por delante del elemento "ID_BEFORE" en la lista de control de acceso, ganando así prioridad el elemento "ID_TO_MOVE" frente a "ID_BEFORE".

Ejemplo:

Para mostrar esto, supongamos que tenemos introducida una segunda entrada:

```
Extended Access List 100, assigned to IPSec

10    PERMIT  SRC=192.168.4.0/24  DES=192.168.10.0/24  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000

11    DENY    SRC=192.168.4.8/32  DES=192.168.10.27/32  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

Esta segunda entrada pretende permitir el paso en claro de cierto tráfico entre dos hosts de las redes 192.168.4.0/24 y 192.168.10.0/24, pero la entrada anterior hace que ésta no tenga efecto. Para evitarlo, se ha de modificar el orden de las entradas:

```
Extended Access List 100>MOVE 11 10
```

El orden de listado y de prioridad ahora es:

```
Extended Access List 100, assigned to IPSec

11    DENY    SRC=192.168.4.8/32  DES=192.168.10.27/32  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000

10    PERMIT  SRC=192.168.4.0/24  DES=192.168.10.0/24  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

Si se enviara algún paquete entre los hosts 192.168.4.8 y 192.168.10.27 (con el protocolo adecuado, etc), éste coincidiría con la entrada con identificador 11 de la LCA, la primera de la lista, y se permitiría su paso en claro. En el tráfico entre el resto de hosts de las redes 192.168.4.0/24 y 192.168.10.0/24, al comprobar la lista no se encontraría coincidencia con la primera entrada, pasando a la segunda (con identificador 10). En caso de que el paquete coincidiera en protocolo, puerto origen, etc, se procesaría entonces por Túnel IPSec.

"LIST ALL-ENTRIES ":

Visualiza todos los elementos de la lista de control de acceso.

Ejemplo:

```
Extended Access List 100>LIST ALL-ENTRIES

Extended Access List 100, assigned to IPSec

11    DENY    SRC=192.168.4.8/32  DES=192.168.10.27/32  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000

10    PERMIT  SRC=192.168.4.0/24  DES=192.168.10.0/24  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

Se obtiene el mismo resultado si se ejecuta el comando "LIST ACCESS-LISTS ALL-ENTRIES" desde el menú IPSec config>:

```
IPSec config>LIST ACCESS-LISTS ALL-ENTRIES

Extended Access List 100, assigned to IPSec

11    DENY    SRC=192.168.4.8/32  DES=192.168.10.27/32  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000

10    PERMIT  SRC=192.168.4.0/24  DES=192.168.10.0/24  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

"LIST ADDRESS-FILTER-ENTRIES [DIR IP] [MASK]"

Visualiza los elementos de la lista de control de acceso con dirección IP origen o destino que este incluida dentro del rango definido por [DIR IP] y [MASK].

Ejemplo:

```
Extended Access List 100>LIST ADDRESS-FILTER-ENTRIES 192.168.4.8 255.255.255.255

Extended Access List 100, assigned to IPSec

11    DENY    SRC=192.168.4.8/32  DES=192.168.10.27/32  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

Se obtiene el mismo resultado si se ejecuta el comando "LIST ACCESS-LISTS ADDRESS-FILTER-ENTRIES" desde el menú IPSec config>:

```
IPSec config>LIST ACCESS-LISTS ADDRESS-FILTER-ENTRIES 192.168.4.8 255.255.255.255

Extended Access List 100, assigned to IPSec

11    DENY    SRC=192.168.4.8/32  DES=192.168.10.27/32  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

"LIST ENTRY [ID]"

Muestra la entrada de identificador [ID] de la lista de control de acceso.

Ejemplo:

```
Extended Access List 100>LIST ENTRY 10

Extended Access List 100, assigned to IPSec

10    PERMIT  SRC=192.168.4.0/24  DES=192.168.10.0/24  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

"NO ENTRY [ID]"

Comando para borrar la entrada de identificador [ID] de la lista de acceso.

Ejemplo:

```
Extended Access List 100>NO ENTRY 10
```

b) Configuración de los Templates (parámetros de seguridad)

Los Templates son políticas de seguridad IPSec que se pueden asociar a uno o varios elementos de la Lista de Control de Acceso. Sólo las listas genéricas que hayan sido previamente asignadas a IPSec podrán ser asociadas a un Template.

En cada Template se definen las direcciones IP de los extremos del Túnel que se quiere establecer (correspondientes a los routers de seguridad), los algoritmos de autenticación o encriptación, y el

modo manual (IPSec manual**)** o **dinámico** (IPSec IKE) de gestión de claves de los Túneles IPSec, además de un número identificador (ID) del Template.

Cada **modo** lleva asociado una serie de comandos; unos son comunes a ambos y otros propios de cada uno, aunque cuando los listemos en el Template aparecerán los significativos del modo configurado.

Se comenzará a describir la configuración de **IPSec manual**, y después se mostrará **IPSec IKE**.

· *Templates manuales*

En IPSec manual, "manual-keying", las claves que se utilizan en el proceso de encriptación y/o autenticación para cada SA, son introducidas por el usuario. Este último debe introducir los mismos parámetros de seguridad (claves, algoritmos de cifrado y autenticación) para ambos extremos del Túnel para que la comunicación segura se pueda realizar.

Para la configuración de Templates manuales, dentro del comando TEMPLATE se dispone de los siguientes subcomandos:

Comando	Función
DEFAULT	Pone los valores por defecto a un Template.
MANUAL	Crea un Template estático con un servicio de seguridad (ESP o AH).
SOURCE-ADDRESS	Introduce la dirección del extremo origen del Túnel en el Template.
DESTINATION-ADDRESS	Introduce la dirección del extremo destino del Túnel en el Template.
SPI	Introduce el número identificativo de la configuración de seguridad (SA) definida por el Template.
KEY	Introduce una clave DES en el Template.
TKEY	Introduce una clave Triple DES en el Template.
MD5KEY	Introduce una clave MD5 en el Template.
SHA1KEY	Introduce una clave SHA1 en el Template.

Lo primero a definir en un Template (manual o dinámico) es el servicio de seguridad que se desea emplear, ESP o AH. El servicio ESP (Encapsulating Security Payload) es un servicio de confidencialidad pues cifra los datos, siendo opcional la autenticación de los mismos; mientras que el servicio AH (Authentication Header) permite tan sólo la autenticación:

"TEMPLATE [ID] DEFAULT]"

Pone los valores por defecto a un Template.

Ejemplo:

```
IPSec config>TEMPLATE 4 default
```

"TEMPLATE [ID] MANUAL ESP [ENCRYPT] [AUTHEN]"

El comando define un Template manual con servicio de seguridad ESP.

Los algoritmos de encriptación posibles son "DES" (Data Encryption Standard) y "TDES" (Triple Data Encryption Standard).

Los algoritmos de autenticación a elegir son "MD5"o "SHA1", o "NONE".

El campo "ID" es el número identificador del Template.

Ejemplo:

```
IPSec config>TEMPLATE 4 manual esp des md5
```

"TEMPLATE [ID] MANUAL AH [AUTHEN]"

Se define un Template manual con servicio de seguridad AH.

Los algoritmos de autenticación posibles son "MD5"o "SHA1".

El campo "ID" identifica al Template.

Ejemplo:

```
IPSec config>TEMPLATE 5 manual ah sha1
```

Tras definir el servicio de seguridad, hay que introducir las direcciones IP de los extremos del Túnel seguro, el identificador de la SA creada a partir del Template (SPI), y las claves que se usarán con los algoritmos de cifrado y autenticación elegidos.

"TEMPLATE [ID] SOURCE-ADDRESS [DIR IP]]"

Introduce la dirección IP local del Túnel para el Template identificado por [ID].

Ejemplo:

```
IPSec config>TEMPLATE 4 source-address 192.100.1.2
```

"TEMPLATE [ID] DESTINATION-ADDRESS [DIR IP]"

Introduce la dirección IP del otro extremo remoto del Túnel.

Ejemplo:

```
IPSec config>TEMPLATE 4 destination-address 192.100.1.1
```

"TEMPLATE [ID] SPI [INTEGER > 256]"

Permite introducir el "Security Parameters Index" para el template identificado por [ID]. Este número es un entero, [INTEGER], que debe ser superior a 256. El **SPI** debe ser el mismo en ambos extremos, e identifica un Template con respecto a otro Template con misma dirección destino de Túnel y con mismo servicio de seguridad (ESP o AH).

Ejemplo:

```
IPSec config>TEMPLATE 4 spi 280
```

No se pueden definir dos políticas que posean valores idénticos para los tres parámetros mencionados: dirección IP destino del Túnel, servicio de seguridad y SPI.

"TEMPLATE [ID] KEY [clave de 8 bytes]"

Para introducir la clave en caso de que hayamos elegido DES como algoritmo de cifrado. "Clave de 8 bytes" representa la clave DES de encriptación del Template (se puede introducir en hexadecimal, empezando por 0x, o en ASCII).

Ejemplo:

```
IPSec config>TEMPLATE 4 key 0x0123456789ABCDEF
```

Notar que si se decide introducir la clave en hexadecimal, se deben introducir el doble de caracteres (entre 0-9 y A-F), pues dos caracteres hexadecimales definen un byte.

"TEMPLATE [ID] TKEY [clave de 24 bytes]"

En caso de haber elegido Triple DES como algoritmo de cifrado. "Clave de 24 bytes" contiene la clave Triple DES (se puede introducir en hexadecimal, empezando por 0x, o en ASCII).

Ejemplo:

```
IPSec config>TEMPLATE 4 tkey 0123456789abcdefghijklmn
```

"TEMPLATE [ID] MD5KEY [clave de 16 bytes]"

Si se ha elegido MD5 para autenticación, se ha de proporcionar una "clave de 16 bytes" (que se puede introducir en hexadecimal, empezando por 0x, o en ASCII).

Ejemplo:

```
IPSec config>TEMPLATE 4 md5key teldatsateldatsa
```

"TEMPLATE [ID] SHA1KEY [clave de 20 bytes]"

En caso de elegirse SHA1 para autenticación, debe introducirse una "clave de 20 bytes" (que se puede introducir en hexadecimal, empezando por 0x, o en ASCII).

Ejemplo:

```
IPSec config>TEMPLATE 4 sha1key teldatsateldatsa1234
```

Definidos todos los parámetros y claves que correspondan, habría que introducir los mismos en el otro router con el que se va a establecer el Túnel. Y tan sólo quedaría el último paso de asociación (mapeo) entre entradas de las LCA y Templates, es decir, la creación de las entradas de las **SPDs**. Esto se verá después de la configuración de Templates dinámicos.

Podemos revisar o borrar los Templates configurados con los mismos comandos **LIST** y **NO** usados para las listas de acceso:

Comando	Función
LIST TEMPLATE	Visualiza elementos de la lista de Templates.
NO TEMPLATE	Elimina elementos de la lista de Templates.

"LIST TEMPLATE ALL"

Visualiza todos los elementos de la lista de Templates.

Ejemplo:

```
IPSec config>LIST TEMPLATE ALL
TEMPLATES
4 manual  ESP-DES  ESP-MD5  SRC=192.100.1.2 DES=192.100.1.1 SPI=280

5 manual  AH-SHA1  SRC=192.100.1.2 DES=192.100.1.10  SPI=280
```

"LIST TEMPLATE ADDRESS-FILTER [DIR IP] [MASK]"

Visualiza los elementos de la lista de Templates con dirección IP origen o destino del Túnel que este incluida dentro del rango definido por [DIR IP] y [MASK].

Ejemplo:

```
IPSec config>LIST TEMPLATE ADDRESS-FILTER 192.100.1.10  255.255.255.255
TEMPLATES
5 manual  AH-SHA1  SRC=192.100.1.2 DES=192.100.1.10  SPI=280
```

"NO TEMPLATE [ID]"

Elimina el elemento de la lista de Templates identificado por [ID].

Ejemplo:

```
IPSec config NO TEMPLATE 5
IPSec config>LIST TEMPLATE ALL
TEMPLATES
4 manual  ESP-DES  ESP-MD5  SRC=192.100.1.2 DES=192.100.1.1 SPI=280
```

· *Templates dinámicos (IPSec IKE)*

La configuración de IPSec IKE (IPSec dinámico) requiere dos tipos de Templates: los denominados **Templates dinámicos**, que son equivalentes a los Templates configurados en modo manual, y los **Templates ISAKMP**. Ahora es necesario negociar entre extremos del Túnel los algoritmos y claves para establecer una SA de comunicación, y esto se realiza en dos fases:

- En la primera fase se acuerdan ciertos parámetros de seguridad que protegerán la negociación, además de autenticarse ambos extremos. Estos parámetros se definen en los Templates ISAKMP.
- La segunda fase es la negociación de la SA para el Túnel, y se basará en los Templates dinámicos.

En cuanto a los subcomandos de TEMPLATE para crear estos Templates, algunos son comunes y otros son sólo aplicables para alguno de los dos tipos.

Comando	**Función**
DYNAMIC	Crea un Template dinámico con un servicio de seguridad (ESP o AH).
ISAKMP	Crea un Template ISAKMP con unos parámetros de seguridad.
SOURCE-ADDRESS	Introduce la dirección del extremo origen del Túnel en el Template.
DESTINATION-ADDRESS	Introduce la dirección del extremo destino del Túnel en el Template.
BACKUP-DESTINATION	Añade una dirección destino de backup.
ANTIREPLAY	Activa el servicio Anti-Réplica en el Template.
NO ANTIREPLAY	Desactiva el servicio Anti-Réplica en el Template.
PADDING-CHECK	Se comprueba que el campo padding de la cabecera IPSec toma el valor indicado en la RFC.
NO PADDING-CHECK	Se ignora el valor que tenga el campo padding de la cabecera IPSec.
UDP-ENCAPSULATION	Para encapsular los paquetes de IPSec en paquetes UDP.
NO UDP-ENCAPSULATION	Para deshabilitar la opción de encapsular los paquetes de IPSec en paquetes UDP.
UDP-IKE	Para encapsular los paquetes de IPSec IKE en paquetes UDP.
NO UDP-IKE	Para deshabilitar la opción de encapsular los paquetes de IPSec IKE en paquetes UDP.
AGGRESSIVE	Configura el envío de cifrado/claro del tercer mensaje IKE en modo agresivo.
ENCAP	Configura el modo de funcionamiento Túnel o Transporte.
LIFE	Introduce el tiempo de vida de las SA´s creadas a partir del Template.
IKE	Configuración de parámetros relativos al modo IPSec IKE.
KEEPALIVE	Para habilitar o deshabilitar los servicios de keepalive disponibles
NO	Borra una dirección de backup o deshabilita una opción.

Se comenzará describiendo los ISAKMP, ya que son el primer paso en las negociaciones.

Lo primero es establecer los parámetros de seguridad para el Template ISAKMP, bajo los cuales se realizará la negociación de la SA de conexión. Por su parte, el Template ISAKMP también da lugar a una SA de negociación, o ISAKMP SA:

"TEMPLATE [ID] ISAKMP [ENCRYPT] [AUTHEN]"

Se crea el Template ISAKMP basado en algoritmos de cifrado y autenticación. Para el cifrado las opciones son DES y Triple DES (TDES), y como autenticación MD5 y SHA1. A pesar de su similitud, esto no es el servicio ESP, y es obligado la elección de un algoritmo de autenticación.

Ejemplo:

```
IPSec config>TEMPLATE 2 isakmp tdes sha1
```

Ahora se ha de especificar la dirección del extremo del Túnel. Los Templates ISAKMP no necesitan la dirección origen.

"TEMPLATE [ID] DESTINATION [DIR IP]"

Ejemplo:

```
IPSec config>TEMPLATE 2 destination-address 192.100.1.1
```

"TEMPLATE [ID] BACKUP-DESTINATION [DIR IP]"

Añade una dirección destino de backup.

Es posible establecer hasta tres direcciones destino de backup en los Templates ISAKMP, de forma que en el caso de que no se pueda establecer el Túnel con la dirección principal se intente con las de backup.

Ejemplo:

```
IPSec config>TEMPLATE 2 backup-destination 192.100.1.2
```

"TEMPLATE [ID] NO BACKUP-DESTINATION [DIR IP]"

Borra una dirección destino de backup.

Ejemplo:

```
IPSec config>TEMPLATE 2 no backup-destination 192.100.1.2
```

Y por último, hay varios parámetros opcionales con valores por defecto pero que se pueden modificar si se necesita:

"TEMPLATE [ID] UDP-ENCAPSULATION"

Este comando indica que se debe encapsular los paquetes IPSec en paquetes UDP. Esto suele usarse para atravesar Firewalls o equipos haciendo NAPT, sin necesidad de cambiar su configuración. Tiene sentido en el caso de Templates ISAKMP.

Ejemplo:

```
IPSec config>TEMPLATE 2 udp-encapsulation
```

"TEMPLATE [ID] NO UDP-ENCAPSULATION"

Este comando indica que no se encapsulan los paquetes IPSec en paquetes UDP, lo cual constituye el funcionamiento habitual. Tiene sentido en el caso de Templates ISAKMP.

Ejemplo:

```
IPSec config>TEMPLATE 2 no udp-encapsulation
```

"TEMPLATE [ID] UDP-IKE"

Este comando indica que se debe encapsular los paquetes IPSec IKE en paquetes UDP. Esto suele usarse para atravesar Firewalls o equipos haciendo NAPT, sin necesidad de cambiar su configuración. Tiene sentido en el caso de Templates ISAKMP.

Ejemplo:

```
IPSec config>TEMPLATE 2 udp-ike
```

"TEMPLATE [ID] NO UDP-IKE"

Este comando indica que no se debe encapsular los paquetes IPSec de negociación en paquetes UDP, aunque se esté realizando esta encapsulación con los paquetes de datos.

Ejemplo:

```
IPSec config>TEMPLATE 2 no udp-ike
```

"TEMPLATE [ID] AGGRESSIVE CIPHER/CLEAR"

Este comando indica si se debe cifrar o no el tercer mensaje de la negociación IKE en modo agresivo.

Ejemplo:

```
IPSec config>TEMPLATE 2 aggressive clear
```

"TEMPLATE [ID] ENCAP TUNNEL/TRANSPORT"

Este comando indica si se va a realizar encapsulado en módo túnel o transporte.

Ejemplo:

```
IPSec config>TEMPLATE 2 encap transport
```

"TEMPLATE [ID] LIFE DURATION SECONDS [VALUE]"

Permite introducir el tiempo de vida de la SA de negociación, que por defecto es 3600 segundos (1 hora).

Ejemplo:

```
IPSec config>TEMPLATE 2 life duration seconds 1000
```

"TEMPLATE [ID] IKE MODE AGGRESSIVE/MAIN"

La fase 1 del intercambio ISAKMP / IKE puede realizarse de dos formas: Agressive Mode y Main Mode. El primer modo es mas rápido que el segundo pero a costa de una disminución de parámetros a negociar.

Ejemplo:

```
IPSec config>TEMPLATE 2 ike mode aggressive
```

"TEMPLATE [ID] IKE METHOD PRESHARED/RSA"

Establece el método de autenticación utilizado por el equipo. En principio sólo está disponible el método Pre-shared Key.

Ejemplo:

```
IPSec config>TEMPLATE 2 ike method preshared
```

"TEMPLATE [ID] IKE IDTYPE IP/FQDN/UFQDN/KEYID/ASN-DN"

La fase 1 del intercambio ISAKMP / IKE puede realizarse usando diferentes tipos de identificadores. IP indica que se usará la dirección IP propia como identificador del equipo. En el resto se usará el nombre del equipo, es decir, lo configurado con el comando SET HOSTNAME del menú de configuración.

Este método sólo se puede usar en modo AGGRESSIVE.

El equipo remoto usará el identificador recibido y lo buscará en su tabla de claves (Pre-shared Keys) asociadas a equipos (direcciones IP o Hostnames), creadas con el comando KEY IP/HOSTNAME (se verá posteriormente).

Ejemplo:

```
IPSec config>TEMPLATE 2 ike idtype ip
```

"TEMPLATE [ID] IKE GROUP ONE/TWO"

Estable el tipo de grupo Oakley. Por defecto se usa grupo 1.

Ejemplo:

```
IPSec config>TEMPLATE 2 ike group one
```

Con esto quedarían configurados todos los parámetros relativos a los Templates ISAKMP. Cuando el router quisiera establecer un Túnel de seguridad, primero enviaría al otro extremo sus propuestas de Templates ISAKMP apropiados (según la dirección IP destino), y entre ambos tendrían que llegar al acuerdo de qué Template usar.

Una vez establecida la SA de negociación, el acuerdo debe ser en cuanto al **Template dinámico** para crear la SA de conexión:

"TEMPLATE [ID] DYNAMIC ESP [ENCRYPT] [AUTHEN]"

Se define un Template dinámico con servicio de seguridad ESP, eligiendo en cifrado entre DES y TDES, y en autenticación entre MD5, SHA1 o NONE.

Ejemplo:

```
IPSec config>TEMPLATE 4 dynamic esp tdes sha1
```

"TEMPLATE [ID] DYNAMIC AH [AUTHEN]"

Se define un Template dinámico con servicio de seguridad AH, eligiendo entre MD5 o SHA1.

Ejemplo:

```
IPSec config>TEMPLATE 3 dynamic ah md5
```

"TEMPLATE [ID] SOURCE-ADDRESS [DIR IP]"

Para introducir la dirección IP local del Túnel. Recordar que sólo es necesario definirla para los Templates dinámicos.

Esta dirección puede ser no numerada, es decir, se puede poner una dirección asociada a un interfaz y que es desconocida en el momento de configurar el equipo porque, por ejemplo, será asignada por algún otro mecanismo, como pudiera ser PPP.

Ejemplo:

```
IPSec config>TEMPLATE 4 source-address 192.100.1.2
```

"TEMPLATE [ID] DESTINATION-ADDRESS [DIR IP]"

Para introducir la dirección IP extremo del Túnel.

Ejemplo:

```
IPSec config>TEMPLATE 4 destination-address 192.100.1.1
```

Si la dirección extremo del Túnel es 0.0.0.0, se considera que es desconocida y que no es un parámetro significativo para seleccionar el Template dinámico durante la negociación. Por supuesto, al desconocer la dirección destino, sólo el extremo remoto podrá comenzar la negociación IKE.

Los siguientes subcomandos hacen referencia a valores por defecto establecidos, pero que puede ser apropiado modificarlos según las situaciones.

"TEMPLATE [ID] ANTIREPLAY"

Este comando habilita el servicio Anti-Réplica, un método de seguridad para evitar los ataques basados en retransmisiones de paquetes.

Ejemplo:

```
IPSec config>TEMPLATE 3 antireplay
```

"TEMPLATE [ID] NO ANTIREPLAY"

Para deshabilitar el servicio Anti-Réplica.

Ejemplo:

```
IPSec config>TEMPLATE 3 no antireplay
```

"TEMPLATE [ID] PADDING-CHECK"

La RFC antigua de IPSec permitía rellenar el campo padding de la cabecera IPSec con cualquier valor aleatorio, mientras que la RFC actualizada especifica un determinado valor para dicho campo. Con objeto de que el router pueda funcionar contra equipos que funcionen según la RFC antigua, se permite configurar un parámetro que indica si debe comprobarse que el campo padding toma el valor definido en la RFC o bien si deben ignorarse esos datos.

Ejemplo:

```
IPSec config>TEMPLATE 3 padding-check
```

"TEMPLATE [ID] NO PADDING-CHECK"

No se comprobará el contenido del campo padding de la cabecera IPSec.

Ejemplo:

```
IPSec config>TEMPLATE 3 no padding-check
```

"TEMPLATE [ID] LIFE TYPE SECONDS/KBYTES/BOTH"

Permite introducir el tipo de tiempo de vida para la SA de comunicación basada en el Template dinámico. En los Templates dinámicos el tiempo de vida puede representarse como límite temporal ("SECONDS"), igual que ocurría para los Templates ISAKMP, o también como límite de cantidad de kilobytes transmitidos ("KBYTES") a través de la SA generada con este Template.

La tercera opción ("BOTH") establece ambos tipos de límite a la vez. En este caso, la SA se elimina cuando uno de los dos límites expire.

Ejemplo:

```
IPSec config>TEMPLATE 4 life type both
```

"TEMPLATE [ID] LIFE DURATION SECONDS/KBYTES [VALUE]"

El tiempo de vida elegido se da en el campo VALUE. En caso de haber elegido BOTH en el subcomando anterior, se tendrá que teclear dos veces el subcomando para dar ambos tipos de valores (segundos y kilobytes).

Ejemplo:

```
IPSec config>TEMPLATE 4 life duration seconds 20000
IPSec config>TEMPLATE 4 life duration kbytes 1000
```

"TEMPLATE [ID] IKE PFS"

Habilita el servicio Perfect Forward Secrecy. Aumenta la seguridad de las SAs creadas, haciendo una mejor gestión de las claves empleadas.

Ejemplo:

```
IPSec config>TEMPLATE 4 ike pfs
```

"TEMPLATE [ID] IKE NO PFS"

Deshabilita el servicio Perfect Forward Secrecy.

Ejemplo:

```
IPSec config>TEMPLATE 4 ike no pfs
```

"TEMPLATE [ID] KEEPALIVE KEEPALIVE"

Habilita el servicio Keep Alive para el mantenimiento de las SAs.

Ejemplo:

```
IPSec config>TEMPLATE 4 keepalive keepalive
```

"TEMPLATE [ID] KEEPALIVE NO KEEPALIVE"

Deshabilita el servicio Keep Alive en el mantenimiento de las SAs.

Ejemplo:

```
IPSec config>TEMPLATE 4 keepalive no keepalive
```

"TEMPLATE [ID] KEEPALIVE DPD"

Habilita el servicio DPD (Dead Peer Detection) para el mantenimiento de las Sas. Tiene sentido en el caso de Templates ISAKMP.

Ejemplo:

```
IPSec config>TEMPLATE 2 keepalive dpd
```

"TEMPLATE [ID] KEEPALIVE NO DPD"

Deshabilita el servicio DPD (Dead Peer Detection) en el mantenimiento de las SAs. Tiene sentido en el caso de Templates ISAKMP.

Ejemplo:

```
IPSec config>TEMPLATE 2 keepalive no dpd
```

En relación con las SAs de conexión creadas a partir de los Templates dinámicos, existe un comando en el menú principal de configuración de IPSec que permite configurar ciertas características avanzadas. Este comando es **ADVANCED**, y da acceso a varios subcomandos:

Comando	Función
DPD	Servicio para asegurarse del mantenimiento de conexión de una SA
KEEP-ALIVE	Servicio para asegurarse del mantenimiento de conexión de una SA.
PURGE-TIMEOUT	Configuración de tiempo de borrado de SAs.
RENEGOTIATION-TIME	Servicio para realizar renegociaciones de SAs.
NO	Establece valores por defecto para los parámetros avanzados de configuración de IPSec.

"ADVANCED DPD"

DPD (Dead Peer Detection) es un servicio que detecta cuando se pierde la comunicación con el otro extremo del Túnel. Para poder usarlo se enviará en la fase 1 de cualquier negociación un vendor ID propio del DPD. Este servicio consiste en el intercambio de notificaciones (una petición R-U-THERE y una respuesta R-U-THERE-ACK) de fase 2 en un Túnel cuando no hay recepción de datos durante cierto tiempo, siendo éste configurable como tiempo de inactividad.

Si está habilitado en un Template ISAKMP, el router envía peticiones DPD de fase 2 en los Túneles creados a partir de dicho Template, y también responde a dichas notificaciones. En caso de no estar habilitado, el router no envía peticiones pero sí responde a las recibidas.

Comando	**Función**
ALWAYS-SEND	Siempre envía keepalive después de la expiración del periodo de inactividad.
ANTI-REPLAY	Habilita la capacidad anti-réplica de paquetes DPD.
IDLE-PERIOD	Periodo de inactividad antes de enviar paquetes DPD.
INTERVAL	Periodo entre DPD keepalives.
PACKETS	Número máximo de paquetes DPDs sin confirmación.
NO	Deshablita una opción o establece en un parámetro sus valores por defecto.

"ADVANCED DPD ALWAYS SEND"

Indica que se deben realizar intercambios de DPD en cuanto termine el tiempo de inactividad.

"ADVANCED DPD NO ALWAYS SEND"

Indica que se debe esperar a tener datos después de haber pasado el tiempo de inactividad para realizar el intercambio.

"ADVANCED DPD ANTI-REPLAY"

Habilita la capacidad de antiréplica para paquetes DPD.

"ADVANCED DPD NO ANTI-REPLAY"

Deshabilita la capacidad de antiréplica para paquetes DPD.

"ADVANCED DPD IDLE-PERIOD [SECONDS]"

Tiempo de inactividad antes de realizar intercambios DPD, esto es, tiempo sin recibir datos en el Túnel. El valor por defecto es 60 segundos, que puede ser reestablecido ejecutando el comando "ADVANCED DPD NO IDLE-PERIOD".

"ADVANCED DPD INTERVAL [SECONDS]"

Tiempo de espera (en segundos) entre envíos de peticiones DPD cuando no se recibe respuesta. El valor por defecto es 5 segundos, que puede ser reestablecido ejecutando el comando "ADVANCED DPD NO INTERVAL".

"ADVANCED DPD PACKETS [MAX_PKTS]"

Máximo número de peticiones DPD sin recibir respuesta. El valor por defecto (3) puede ser reestablecido ejecutando el comando "ADVANCED DPD NO PACKETS".

Ejemplo:

```
IPSec config>ADVANCED DPD ALWAYS-SEND
IPSec config>ADVANCED DPD IDLE-PERIOD 60
IPSec config>ADVANCED DPD INTERVAL 5
```

```
IPSec config>ADVANCED DPD PACKETS 3
IPSec config>ADVANCED DPD ANTI-REPLAY
Keep Alive modified
Do not forget to enable DPD in the template configuration
```

Como indica el mensaje final, hay que habilitar individualmente en cada Template ISAKMP el servicio DPD si se desea, con "TEMPLATE [ID] KEEPALIVE DPD".

"ADVANCED KEEP-ALIVE"

Keep Alive es un servicio que trata de asegurarse de que el otro extremo mantiene su SA abierta, observando el tiempo que permanece éste sin dar señales de vida. Al introducir el comando, se pedirá al usuario que defina dos parámetros:

Comando	Función
PACKETS	Máximo número de paquetes sin recibir respuesta.
TIMEOUT	Tiempo de espera (en segundos) tras último paquete.
NO	Establece el valor por defecto de cualquiera de los parámetros anteriores

Ejemplo:

```
IPSec config>ADVANCED KEEP-ALIVE PACKETS 4
Keep Alive modified
Do not forget to enable Keep Alive in the template configuration.
IPSec config>ADVANCED KEEP-ALIVE TIMEOUT 10
Keep Alive modified
Do not forget to enable Keep Alive in the template configuration.
```

Como indica el mensaje final, hay que habilitar individualmente en cada Template dinámico el servicio Keep Alive si se desea, con "TEMPLATE [ID] KEEPALIVE KEEPALIVE".

"ADVANCED PURGE-TIMEOUT [SECONDS]"

Permite configurar el tiempo de borrado de las SAs. Este es, por ejemplo, el tiempo que tardará en borrarse una SA de negociación cuando se intente una negociación de un Túnel con un destino que no responda. El comando "ADVANCED NO PURGE-TIMEOUT" reestablece el valor por defecto de este parámetro (15 segundos).

Ejemplo:

```
IPSec config>ADVANCED PURGE-TIMEOUT 15
```

"ADVANCED RENEGOTIATION-TIME"

El tiempo de renegociación es un límite que se establece en relación con el final del tiempo de vida de una SA de conexión. Si entre este límite y el final de la SA hay tráfico, el router renegociará automáticamente una nueva SA, antes de que expire el tiempo de vida de la actual. Esto evita que se pierda tráfico por el fin de una SA.

Este límite se interpreta como un tanto por ciento, y se aplica a cada tiempo de vida (en segundos sólo) individual de cada SA, sin dejar que baje nunca de un minuto.

El valor por defecto de este parámetro es 10 (10%), y se puede volver a él mediante el comando "ADVANCED NO RENEGOTIATION-TIME".

Ejemplo:

```
IPSec config>ADVANCED RENEGOTIATION-TIME 20
Check-out time (%) - from SA's end-lifetime - to renegotiate : 20
```

La última línea es de confirmación, y describe el siguiente comportamiento: cuando a una SA le quede el 20% de su tiempo para finalizar, el router comenzará a chequear si hay tráfico, hasta el final de vida. En caso afirmativo, renegociará una nueva SA cuando falte un minuto.

Otros parámetros configurables desde el submenú ADVANCED del menú principal de configuración de IPSec son:

Comando	Función
EXPONENTATION-DEVICE	Servicio para asegurarse del mantenimiento de conexión de una SA
LQUEUE	Longitud de la cola de cifrado.
NO LQUEUE	Establece el valor por defecto para la longitud de la cola de cifrado.

"ADVANCED EXPONENTATION-DEVICE"

Este comando da acceso a otros dos: HARDWARE y SOFTWARE, que permiten configurar la forma en que se van a realizar las operaciones para llevar a cabo el procesamiento de los paquetes cifrados. Si se escoge la opción HARDWARE, se establece que el cifrado se hará a nivel HARDWARE (tarjeta de cifrado), mientras que la opción SOFTWARE implica que las operaciones se efectúan utilizando código software.

Ejemplo:

```
IPSec config>ADVANCED EXPONENTIATION-DEVICE ?
HARDWARE      A hardware device will be used to carry out cipher operations
SOFTWARE      Software will be used to carry out cipher operations
IPSec config>ADVANCED EXPONENTIATION-DEVICE HARDWARE
```

"ADVANCED LQUEUE":

Configura la longitud de la cola de cifrado.

Ejemplo:

```
IPSec config>ADVANCED LQUEUE
Size of the cypher queque:[50]? 25
IPSec config>
```

"ADVANCED NO LQUEUE"

Configura la longitud de la cola de cifrado a su valor por defecto: 50.

Ejemplo:

```
IPSec config>ADVANCED NO LQUEUE
IPSec config>
```

Con esto terminaría la configuración de los Templates ISAKMP y dinámicos necesarios para realizar IPSec IKE, aunque aún quedaría introducir un parámetro más para hacerlos funcionales: se trata de la clave Pre-shared Key que deben poseer ambos routers de seguridad para poder autenticarse mutuamente. Esta clave se introduce desde el menú principal de IPSec:

"KEY PRESHARED IP/HOSTNAME [ADDRESS/NAME] CIPHERED/PLAIN [KEY]"

Permite introducir la Pre-shared key asociada a la dirección IP o nombre de equipo remoto, según se hubiera previsto el Túnel cuando se empleo el comando "TEMPLATE IKE IDTYPE" para los Templates ISAKMP.

Notar que esta clave sin embargo, no va asociada a un Template, sino a una dirección IP o un host remoto, por eso no necesita un identificador [ID] como el resto de comandos.

La Pre-shared key puede introducirse en claro (subcomando PLAIN) o cifrada (subcomando **C**IPHERED). Si se está configurando manualmente desde consola, lo habitual es introducir la clave en claro, mientras que si se utiliza una configuración guardada en modo texto (procedente de una comando "SHOW CONFIG"), la clave irá cifrada. En caso de ir en claro, la clave puede tener una longitud entre 1 y 32 bytes, que se pueden introducir en hexadecimal, empezando por 0x, o en ASCII. Recordar que en caso de introducirla en hexadecimal, se deben introducir el doble de caracteres (entre 0-9 y A-F). Si la clave está cifrada siempre se muestra en hexadecimal.

Ejemplo 1:

```
IPSec config>KEY PRESHARED IP 192.100.1.1 plain 1234567890
IPSec config>KEY PRESHARED HOSTNAME Router2 plain 1234567890teldat
IPSec config>KEY PRESHARED IP 192.100.1.1 plain 0x1234567890abcdef
```

La Pre-shared key admite redes con máscara 0, 8, 16 y 24 bits en direcciones IP.

Ejemplo 2:

```
IPSec config>KEY PRESHARED IP 192.100.1.0 plain 1234567890
```

Se asigna esta clave a toda la red 192.100.1.0 255.255.255.0

La Pre-shared key admite el carácter comodín asterisco al final del nombre de host.

Ejemplo 3:

```
IPSec config>KEY PRESHARED HOSTNAME Router* plain 1234567890teldat
```

Se asigna esta clave a Router1, RouterTeldat, Router, Router_234...

En el caso de existir intersecciones, siempre se toma la más restrictiva.

Ejemplo 4:

```
IPSec config>KEY PRESHARED HOSTNAME Router* plain 1234567890teldat
IPSec config>KEY PRESHARED HOSTNAME Router plain 1111111
```

Si el nombre de host es Router se usará la clave 1111111.

```
IPSec config>KEY PRESHARED IP 192.100.1.0 plain 1234567890
IPSec config>KEY PRESHARED IP 192.100.1.163 plain aaaa
```

Si la IP es 192.100.1.163 se usará la clave aaaa

Pueden verse las claves Pre-shared configuradas utilizando el comando "LIST KEY PRESHARED". Las claves no se imprimen como tal en consola, pero de esta forma es posible saber para qué direcciones IP o hostnames se tiene una clave Pre-shared asociada:

```
IPSec config>LIST KEY PRESHARED
5 key entries
   192.100.1.1 ************
   Router2 ************
   192.100.1.0 ************
   Router* ************
   Router ************
```

Si se desea borrar una clave asociada a una dirección IP o a un hostname, basta con hacer uso del comando "NO KEY PRESHARED IP/HOSTNAME [ADDRESS/NAME]":

```
IPSec config>NO KEY PRESHARED IP 192.100.1.0
```

c) Creación de la SPD

Por último, tras definir la Lista de Control de Acceso y los Templates, tan sólo queda crear la base de datos de políticas o SPD. Cada entrada de esta base de datos está formada por un elemento de la LCA y un Template asociado. A la asociación se le denomina **mapeo**, y el comando y su utilización para mapear las entradas se muestra a continuación:

Comando	Función
ASSIGN-ACCESS-LIST	Asigna una lista de control de acceso al protocolo IPSec
ASSOCIATE-KEY	Asocia una clave a una lista de control de acceso.
MAP-TEMPLATE	Asocia elementos de la lista de control de acceso con Templates.

"ASSIGN-ACCESS-LIST [ID de entrada LCA]"

Asigna una lista de control de acceso genérica y extendida al protocolo IPSec.

Ejemplo:

```
IPSec config>ASSIGN-ACCESS-LIST 100
```

"ASSOCIATE-KEY IP/HOSTNAME [ACCESS_LIST] [ADDRESS/NAME KEY]"

Uno de los parámetros negociados durante la apertura de un Túnel IPSec es el control de acceso, es decir, los *clientes del Túnel*. En principio, el conocimiento de una clave Pre-shared permite al equipo remoto abrir un Túnel contra el equipo local, con independencia de los clientes. Pero a veces esto no es conveniente y se quiere dar ciertos controles a los equipos que conocen una clave y otros a los que conocen otra.

En el ejemplo que se muestra a continuación, se pueden hacer las afirmaciones:

- Sólo los equipos que conozcan la clave asociada al hostname *teldat_router* podrán abrir un Túnel con acceso a toda la red 192.60.64.0/24.
- Los equipos que sólo conozcan la clave asociada a *router*, **no** podrán abrir un Túnel con acceso a toda la red 192.60.64.0/24.
- Como la lista de control de acceso 101 no tiene clave asociada, los equipos que conozcan la clave asociada a *router* y la asociada a *teldat_router* podrán abrir un Túnel con acceso al host 192.60.64.1

Ejemplo:

```
Extended Access List 101, assigned to IPSec

1     PERMIT  SRC=192.60.64.1/32  DES=0.0.0.0/16  Conn:0


Extended Access List 100, assigned to IPSec

10    PERMIT  SRC=192.60.64.0/24  DES=0.0.0.0/16  Conn:0
IPSec config> LIST KEY PRESHARED
2 key entries
   teldat_router ************
   router ************
IPSec config> ASSOCIATE-KEY HOSTNAME 100 teldat_router
```

"MAP [ID de entrada LCA] [ID de Template]"

El comando asocia un elemento de la lista de control de acceso con un Template, creando un elemento de la SPD.

Ejemplo:

```
IPSec config>MAP-TEMPLATE 100 4
```

Cuando se realiza el mapeo, en el listado de entradas de la lista de control de acceso del menú de monitorización de IPSec a veces se pueden observar unas entradas automáticas no introducidas por el usuario, que se distinguen por las palabras DYNAMIC ENTRY. Estas entradas automáticas son necesarias para que ambos extremos del Túnel se puedan comunicar paquetes de control.

```
Extended Access List 101, assigned to IPSec

 ACCESS LIST ENTRIES
65534 DENY    SRC=0.0.0.0/0  DES=192.60.64.1/32  Conn:0
        PROT=17  SPORT=500
        DYNAMIC ENTRY
        Hits: 0

65533 DENY    SRC=0.0.0.0/0  DES=192.60.64.1/32  Conn:0
        PROT=17  SPORT=4500
        DYNAMIC ENTRY
        Hits: 0

65532 DENY    SRC=0.0.0.0/0  DES=192.60.64.1/32  Conn:0
        PROT=50-51
        DYNAMIC ENTRY
        Hits: 0

65531 PERMIT  SRC=192.60.64.2/32  DES=192.60.64.1/32  Conn:0
        DYNAMIC ENTRY
        Hits: 0

1     PERMIT  SRC=0.0.0.6/32  DES=192.60.64.1/32  Conn:0
        Hits: 0
```

El mapeo es el último paso para configurar el servicio completo de seguridad IPSec. Antes de dar por finalizada la configuración, podemos observar lo realizado, modificar algún error e incluso determinar que eventos vamos a querer observar en la monitorización de sus trazas:

Comando	Función
LIST ALL	Visualiza toda la configuración.
SHOW CONFIG	Visualiza los comandos de configuración.
NO ASSIGN-ACCESS-LIST	Elimina la asignación de una lista de control de acceso al protocolo IPSec.
NO ASSOCIATE-KEY	Elimina la asociación de una clave a una lista de control de acceso.
NO MAP-TEMPLATE	Elimina la asociación entre elementos de la LCA y Templates.
EVENT	Habilita ciertos eventos.
LIST ENABLED-EVENTS	Muestra el filtro configurado para la monitorización de los eventos (si lo hay)
QOS-PRE-CLASSIFY	Clasificación de los paquetes en sus respectivas clases BRS.
NO QOS-PRE-CLASSIFY	Deshabilita la clasificación de los paquetes en sus respectivas clases BRS.

"LIST ALL"

Visualiza toda la configuración de políticas que contiene la SPD, los elementos de la LCA, la lista de Templates, etc.

Ejemplo:

```
IPSec config>LIST ALL
IPSec Access Control.
Access Control is: enabled
QOS Preclassify is: disabled

Access Lists assigned to IPSec:
  Extended Access List 101
  Templates: 1


Extended Access List 101, assigned to IPSec

1     PERMIT  SRC=0.0.0.6/32  DES=192.60.64.1/32  Conn:0

TEMPLATES
1 dynamic ESP-3DES ESP-MD5  SRC=0.0.0.6 DES=192.60.64.1
   LifeTime:0h3m0s 100000 kbytes
   PFS disabled

2 dynamic ESP-DES ESP-SHA1  SRC=192.24.51.75 DES=192.24.51.74
   LifeTime:0h50m0s 100000 kbytes
   PFS disabled

3 dynamic AH-MD5  SRC=192.24.51.75 DES=192.24.51.74
   LifeTime:0h50m0s 100000 kbytes
   PFS disabled

4 dynamic AH-SHA1  SRC=192.24.51.75 DES=192.24.51.74
   LifeTime:0h50m0s 100000 kbytes
   PFS disabled

20 isakmp 3DES MD5  DES=192.60.64.1
   LifeTime:0h4m0s
   IKE AGGRESSIVE
   PRESHARED
   fqdn ID TYPE
   OAKLEY GROUP 1

4 key entries
   172.24.51.57 ************
   192.24.51.74 ************
   192.24.78.75 ************
   192.60.64.1 ************
0 rsakey entries
Id.           Date.         Len         CA.                   Cert sn.

KeepAlive Configuration:
   Maximum number of encoded packets without receiving an answer: 0.
   Timeout after last packet encoded: 0 seconds.

DPD Configuration:
Idle period(secs) before sending DPD keepalives: 60
Maximum number of DPD keepalives not acknowledged: 3
Period of time(secs) between DPD keepalives: 5
Always send keepalive after idle period expiration : ENABLED
Anti-replay : DISABLED

Check-out time (%) - from SA's end-lifetime - to renegotiate : 10

SA's purge timeout:  15

Use software exponentiation
```

"SHOW CONFIG":

Visualiza los comandos de configuración. Es importante resaltar que los valores de los campos que coinciden con el valor por defecto no se muestran. En el ejemplo que viene a continuación se expone el resultado de la ejecución del comando *SHOW CONFIG* con la configuración del ejemplo presentado en el comando *LIST ALL*.

Ejemplo:

```
IPSec config>SHOW CONFIG
; Showing System Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

      enable
      assign-access-list 101
;
      template 1 create
      template 1 dynamic esp tdes md5
      template 1 source-address 0.0.0.6
      template 1 destination-address 192.60.64.1
      template 1 life type both
      template 1 life duration seconds 180
      template 1 life duration kbytes 100000
;
      template 2 create
      template 2 dynamic esp des sha1
      template 2 source-address 192.24.51.75
      template 2 destination-address 192.24.51.74
      template 2 life type both
      template 2 life duration seconds 3000
      template 2 life duration kbytes 100000
;
      template 3 create
      template 3 dynamic ah md5
      template 3 source-address 192.24.51.75
      template 3 destination-address 192.24.51.74
      template 3 life type both
      template 3 life duration seconds 3000
      template 3 life duration kbytes 100000
;
      template 4 create
      template 4 dynamic ah sha1
      template 4 source-address 192.24.51.75
      template 4 destination-address 192.24.51.74
      template 4 life type both
      template 4 life duration seconds 3000
      template 4 life duration kbytes 100000
;
      template 20 create
      template 20 isakmp tdes md5
      template 20 destination-address 192.60.64.1
      template 20 life duration seconds 240
      template 20 ike ca THAWTECA.CER
      template 20 ike mode aggressive
      template 20 ike idtype fqdn
;
      map-template 101 1
      key preshared ip 172.24.51.57 holas
      key preshared ip 192.24.51.74 ciphered 0xF85C0CB62556C562120794C28EB9334
      key preshared ip 192.24.78.75 ciphered 0xF85C0CB62556C562120794C28EB9334
      key preshared ip 192.60.64.1 ciphered 0xF85C0CB62556C562120794C28EB9334
IPSec config>
```

"NO ASSIGN-ACCESS-LIST [ID de entrada LCA]"

Elimina la asignación de una lista de control de acceso al protocolo IPSec.

Ejemplo:

```
IPSec config>NO ASSIGN-ACCESS-LIST 100
```

"NO ASSOCIATE-KEY [ID de entrada LCA]"

Elimina la asociación de una clave a una lista de control de acceso.

Ejemplo:

```
IPSec config>NO ASSOCIATE-KEY 100
```

"NO MAP-TEMPLATE [ID de entrada LCA] [ID Template]"

Elimina la asociación o mapeado del elemento de la LCA con el Template.

Ejemplo:

```
IPSec config>NO MAP-TEMPLATE 10 4
```

Aunque se deshaga el mapeo, la entrada automática que generó permanece, así que ha de ser borrada si se desea.

"EVENT ALL"

Permite ver todos los eventos. Dichos eventos se han de habilitar en el proceso de monitorización de eventos (P 3), y se observan en P 2.

Ejemplo:

```
IPSec config>EVENT ALL
```

"EVENT ADDRESS-FILTER [DIR IP][MASK]":

Permite ver sólo los eventos con dirección origen o destino que este incluido dentro del rango definido por [DIR IP][MASK], una vez habilitados.

Ejemplo:

```
IPSec config>EVENT ADD 192.100.1.2 255.255.255.255
```

"LIST ENABLED-EVENTS"

Muestra el filtro configurado para la monitorización de los eventos (si lo hay).

Ejemplo:

```
IPSec config>LIST ENABLED-EVENTS

 Address/Subnet enabled : 192.100.1.2 with MASK : 255.255.255.255
```

"QOS- PRE-CLASSIFY"

Permite habilitar la clasificación de los paquetes en sus respectivas clases BRS antes de que sean cifrados.

```
IPSec config>QOS-PRE-CLASSIFY
IPSec config>
```

Para deshabilitar esta opción basta ejecutar el comando "NO QOS-PRE-CLASSIFY"

```
IPSec config>NO QOS-PRE-CLASSIFY
IPSec config>
```

Si se habilita este modo los paquetes serán clasificados antes de ser cifrados, con lo que se podrán priorizar distintas clases de tráfico dentro de un mismo Túnel IPSec. La clasificación sólo funcionará en aquellos controles de acceso que estén asociados a una regla IP ya que si no no se puede saber por qué interfaz saldrá el paquete antes de ser cifrado y por lo tanto no se puede aplicar el BRS asociado a ese interfaz. Si se deshabilita, todo el tráfico proveniente del Túnel IPSEC se clasificará en la misma clase de BRS ya que la cabecera que será analizada será la del Túnel IPSEC.

· *Modo Configuración de ISAKMP*

Exite un método que permite configurar los parámetros de la fase II que se negociarán después de finalizar la fase I. Con este método podemos definir, de una manera segura, las características que tendrá la sesión IPSec negociada en la fase II para intercambio de datos. En el momento de crear esta documentación las propiedades y modo de funcionamiento de este modo de configuración se encuentran detallados en el draft: *The ISAKMP Configuration Method*.

Este método se suele emplear en configuraciones en estrella, donde el nodo central asigna a cada uno de los extremos que pretenden conectarse a la VPN, las direcciones que van a tener durante la sesión, cuales van a ser sus servidores de nombres, si se utilizará PFS o el puerto sobre el que se hará el NAT-T.

Dentro del menú TEMPLATE se pueden encontrar los siguientes parámetros que permiten configurar este método:

Comando	Función
IKE METHOD	Se incorpora la opción "xauth-init-preshared".
CONFIG	Permite definir si el equipo iniciará el método de configuración, esperará a que le hagan una propuesta o se comportará según marque el método IKE utilizado.

"IKE METHOD XAUTH-INIT-PRESHARED"

Con este comando se añade una funcionalidad nueva al comando IKE METHOD descrito con anterioridad. Esta funcionalidad es la *Autenticación Extendida Preshared,* descrita en el momento de crear esta documentación en el draft *Extended Authentication within ISAKMP/Oakle.* Al activar este parámetro se indica que se quiere realizar una autenticación pre-shared en donde se desea ejecutar un proceso de *Configuración ISAKMP*, en el que el equipo iniciador deberá autenticarse contra un servidor remoto, que le podrá asignar, entre otras cosas, la dirección IP dentro de la VPN.

Ejemplo:

```
IPSec config>TEMPLATE 4 ike method xauth-init-preshared
```

"CONFIG INITIATOR"

Con este comando se indica que el equipo iniciará el método de configuración, haciendo las propuestas iniciales y solicitando los parámetros necesarios.

Este parámetro no tiene efecto si el método de autenticación es xauth-init-preshared.

Ejemplo:

```
IPSec config>TEMPLATE 4 config initiator
```

"CONFIG RESPONDER"

Con este comando se indica que el equipo esperará a que extremo remoto inicie el método de configuración.

Este parámetro no tiene efecto si el método de autenticación es xauth-init-preshared.

Ejemplo:

```
IPSec config>TEMPLATE 4 config responder
```

"CONFIG NONE"

Con este comando se indica que el equipo actuará como iniciador o respondedor según indique el método IKE utilizado.

Ejemplo:

```
IPSec config>TEMPLATE 4 config none
```

"AUTENTICACIÓN EXTENDIDA"

La Autenticación Extendida consiste en la autenticación contra un equipo servidor que nos asignará los parámetros requeridos para poder establecer una conexión. El modo típico de realizar esta autenticación es mediante un usuario y un password.

Los comandos que se describen a continuación permiten asociar un usuario a una password y a una dirección IP o nombre.

Comando	Función
XAUTH-IP	Asocia un usuario a una dirección IP.
XAUTH-HOSTNAME	Asocia un usuario a un nombre.

"XAUTH-IP [dirección IP] USER [nombre de usuario]"

"XAUTH-IP [dirección IP] PASSWORD [password]"

Con estos dos comandos se puede definir el usuario y password que irán asociados a la dirección IP que se introduce como parámetro.

En el caso de ser el iniciador esta dirección IP indicará la dirección con la que se identificó el extremo remoto.

En el caso de ser el respondedor esta dirección IP indicará la dirección que se asignará al extremo iniciador en la negociación del método de Configuración ISAKMP.

Ejemplo:

```
IPSec config>xauth-ip 1.1.1.1 user router1
IPSec config>xauth-ip 1.1.1.1 password plain mykey
```

"XAUTH-HOSTNAME [hostname] USER [nombre de usuario]"

"XAUTH-HOSTNAME [hostname] PASSWORD [password]"

Con estos dos comandos se puede definir el usuario y password que irán asociados al nombre que se introduce como parámetro.

Este nombre indicará el hostname con el que se identificó el extremo remoto.

Ejemplo:

```
IPSec config>xauth-hostname remoterouter user router1
IPSec config>xauth-hostname remoterouter password plain mykey
```

"DESTINO DE LA DIRECCIÓN IP ASIGNADA"

La dirección IP asignada pasará a ser la dirección de NAT utilizada en las reglas de NAPT cuya dirección local coincida con la que se está usando en la negociación.

Es decir, si se tiene un equipo con esta regla:

IP local = 80.33.21.187 // Dirección IP del interfaz ADSL.

IP NAPT = 0.0.0.0

NAPT = Yes

Cuando se negocie el modo de configuración ISAKMP, por el interfaz ADSL, y se reciba la dirección, por ejemplo, 10.123.1.13, se tendrá la siguiente regla:

IP local = 80.33.21.187 // Dirección IP del interfaz ADSL.

IP NAPT = 10.123.1.13

NAPT = Yes

Pudiéndose poner un Lista de Control de Acceso del tipo:

Fuente = 0.0.0.0/0

Destino = 0.0.0.0/0

Que después de la negociación se transforma en:

Fuente = 10.123.1.13/32

Destino = 0.0.0.0/0

De esta forma, se consigue que todos los equipos que estén conectados a la LAN del router y que salgan por ADSL, acaben pasando por la SA abierta en IPSec para acceder a cualquier destino fuera de la LAN.

· *IPComp*

IPComp define una propiedad por la que se permite establecer un contexto o SA en la que los datos irán comprimidos tal y como se especifica en la *RFC 3173 IP Payload Compression Protocol (IPComp).*

Este método de compresión sólo se puede configurar cuando se utiliza IPSec, es decir, de momento no existe una forma de activar este método fuera del contexto de una SA de IPSec.

Dentro del menú TEMPLATE se pueden encontrar los siguientes parámetros que permiten configurar este modo:

Comando	**Función**
IPCOMP	Modo de compresión IP.

"IPCOMP LZS"

Con este comando se activa la funcionalidad de compresión IP (IPComp) utilizando el algoritmo LZS.

Ejemplo:

```
IPSec config>TEMPLATE 4 ipcomp lzs
```

"IPCOMP NONE"

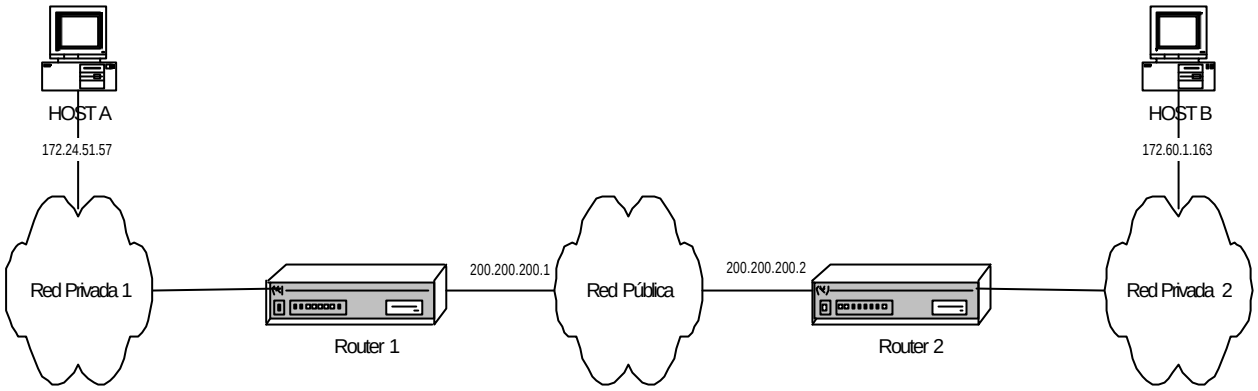
Con este comando se desactiva la funcionalidad de compresión IP (IPComp).

Ejemplo:

```
IPSec config>TEMPLATE 4 ipcomp none
```

4. Ejemplos

4.1. Ejemplo 1: Modo Manual



Se trata de crear una nueva red privada virtual (VPN) entre el host A y el host B. El resto del tráfico entre las redes privadas se dejará pasar de modo normal. Crearemos un Túnel IPSec con cifrado Triple DES y autenticación SHA-1 como requisitos de seguridad.

· *Creación de las listas de control de acceso*

Como ya se ha mencionado, los clientes del Túnel son el host A y el host B.

Router 1:

```
Config>FEATURE ACCESS-LISTS

-- Access Lists user configuration --
Access Lists config> ACCESS-LIST
Access List number (1-99, 100-199)[1]? 101


Extended Access List 101> ENTRY 1
permit              configures type of entry or access control as permit
deny                configures type of entry or access control as deny
source              source menu: subnet or port
destination         destination menu: subnet or port
protocol-range      protocol range
dscp                Diff Serv codepoint
connection          IP connection identifier (rule)
Type an option []? source
address         ip address and mask of the source subnet
port-range      source port range
Type an option [address]?
Source IP address [0.0.0.0]? 172.24.51.57
Source IP mask [0.0.0.0]? 255.255.255.255
Extended Access List 101> ENTRY 1 destination
address         ip address and mask of the destination subnet
port-range      destination port range
Type an option [address]?
Destination IP address [0.0.0.0]? 172.60.1.163
Destination IP mask [0.0.0.0]? 255.255.255.255
Extended Access List 101>
```

La lista de acceso configurada queda por tanto:

```
Extended Access List 101>LIST ALL-ENTRIES

Extended Access List 101, assigned to no protocol

1     PERMIT  SRC=172.24.51.57/32  DES=172.60.1.163/32  Conn:0

Extended Access List 101>
```

Y con el comando "SHOW CONFIG" puede mostrarse la configuración y ser utilizada en otra ocasión introduciendo ésta en la consola tal y como aparece:

```
Access Lists config>SHOW CONFIG
; Showing System Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

   access-list 101
;
      entry 1 permit
      entry 1 source address 172.24.51.57 255.255.255.255
      entry 1 destination address 172.60.1.163 255.255.255.255
;
   exit
;
Access Lists config>
```

Es decir, se podría haber configurado la entrada de la lista de acceso deseada de la siguiente forma:

```
Access Lists config>
   access-list 101
      entry 1 permit
      entry 1 source address 172.24.51.57 255.255.255.255
      entry 1 destination address 172.60.1.163 255.255.255.255
```

Router 2:

```
Access Lists config>
   access-list 101
      entry 1 permit
      entry 1 source address 172.60.1.163 255.255.255.255
      entry 1 destination address 172.24.51.57 255.255.255.255
```

· *Creando Templates*

Se crean a continuación los patrones de seguridad o Templates:

Router 1:

Lo primero es habilitar IPSec:

```
Config>PROTOCOL IP

-- Internet protocol user configuration --
IP config> IPSEC

-- IPSec user configuration --
IPSec config>ENABLE
IPSec config>
```

Ahora se configura el Template que se necesita:

```
IPSec config>TEMPLATE 2
default                  sets default values to a template or creates a new one
dynamic                   dynamic template
manual                    manual template
isakmp                    isakmp template
source-address            tunnel's local IP address
destination-address       IP address of the other remote end of the tunnel
backup-destination        backup destination IP address
spi                       Security Parameter Index
key                       template encryption DES key
tkey                      triple DES key
md5key                    MD5 key
sha1key                   SHA1 key
antireplay                activates the Anti-Replay service
padding-check             enables padding check
udp-encapsulation         enables UDP encapsulation
life                     introduces the SAs life span created from the template
ike                      configures parameters relative to the IPSec IKE mode
keepalive                 enables the available keepalive services
no                        deletes a backup destination or disables an option
Type an option [default]? manual
esp      ESP security service (Encapsulating Security Payload)
ah       AH security service (Authentication Header)
Type an option [esp]?
des       encryption algorithm DES (Data Encryption Standard)
tdes      encryption algorithm TDES (Triple Data Encryption Standard)
Type an option [des]? tdes
md5       authentication algorithm MD5
sha1      authentication algorithm SHA1
none      no authentication algorithm
Type an option [md5]? sha1
IPSec config>TEMPLATE 2 source-address
IP address [0.0.0.0]? 200.200.200.1
IPSec config>TEMPLATE 2 destination-address
IP address [0.0.0.0]? 200.200.200.2
IPSec config>TEMPLATE 2 spi
Enter SPI (SPI > 256):[257]? 280
IPSec config>TEMPLATE 2 tkey h53s45ef46agv4646n2j8qpo

IPSec config>TEMPLATE 2 sha1key b74hd748ghzm67k6m6d1
```

El Template queda configurado como se muestra a continuación:

```
IPSec config>LIST TEMPLATE ALL
TEMPLATES
2 manual ESP-3DES ESP-SHA1  SRC=200.200.200.1 DES=200.200.200.2 SPI=280

IPSec config>
```

Y lo que se obtiene con el comando “SHOW CONFIG” es:

```
IPSec config>SHOW CONFIG
; Showing System Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

      enable
;
      template 2 default
      template 2 manual esp tdes sha1
      template 2 source-address 200.200.200.1
      template 2 destination-address 200.200.200.2
      template 2 spi 280
      template 2 tkey h53s45ef46agv4646n2j8qpo
      template 2 sha1key b74hd748ghzm67k6m6d1
;
IPSec config>
```

Es decir, el Template también podría haber sido configurado así:

```
IPSec config>
      enable
      template 2 default
      template 2 manual esp tdes sha1
      template 2 source-address 200.200.200.1
      template 2 destination-address 200.200.200.2
      template 2 spi 280
      template 2 tkey h53s45ef46agv4646n2j8qpo
      template 2 sha1key b74hd748ghzm67k6m6d1
```

Router 2:

```
IPSec config>
      enable
      template 2 default
      template 2 manual esp tdes sha1
      template 2 source-address 200.200.200.2
      template 2 destination-address 200.200.200.1
      template 2 spi 280
      template 2 tkey h53s45ef46agv4646n2j8qpo
      template 2 sha1key b74hd748ghzm67k6m6d1
```

El SPI debe ser igual en los dos Routers.

· *Creando las SPD´s*

Para completar las bases de datos de políticas de Seguridad (***SPD***), es necesario "mapear" los elementos de la Lista de Control de Acceso a los Templates elegidos.

Router 1:

```
IPSec config>assign-access-list
Enter extended access list id[100]? 101
IPSec config>map-template
Enter extended access list id[100]? 101
Enter template id[1]? 2
IPSec config>
```

O bien:

```
IPSec config>
      assign-access-list 101
      map-template 101 2
```

La configuración de IPSec queda como sigue:

```
IPSec config>LIST ALL
IPSec Access Control.
Access Control is: enabled
QOS Preclassify is: disabled

Access Lists assigned to IPSec:
  Extended Access List 101
  Templates: 2


Extended Access List 101, assigned to IPSec
```

```
1     PERMIT  SRC=172.24.51.57/32  DES=172.60.1.163/32  Conn:0

TEMPLATES
2 manual ESP-3DES ESP-SHA1  SRC=200.200.200.1 DES=200.200.200.2 SPI=280

0 key entries
0 rsakey entries
Id.           Date.         Len         CA.                   Cert sn.

KeepAlive Configuration:
   Maximum number of encoded packets without receiving an answer: 0.
   Timeout after last packet encoded: 0 seconds.

DPD Configuration:
Idle period(secs) before sending DPD keepalives: 60
Maximum number of DPD keepalives not acknowledged: 3
Period of time(secs) between DPD keepalives: 5
Always send keepalive after idle period expiration : ENABLED
Anti-replay : DISABLED

Check-out time (%) - from SA's end-lifetime - to renegotiate : 10

SA's purge timeout:  15

Use software exponentiation

IPSec config>
```

Y con el comando “SHOW CONFIG” se obtiene:

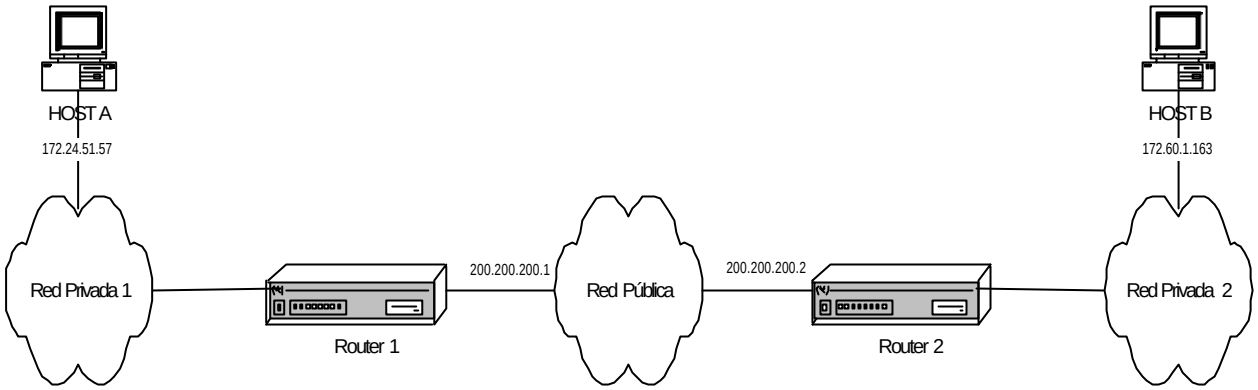
```
IPSec config>SHOW CONFIG
; Showing System Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

      enable
      assign-access-list 101
;
      template 2 default
      template 2 manual esp tdes sha1
      template 2 source-address 200.200.200.1
      template 2 destination-address 200.200.200.2
      template 2 spi 280
      template 2 tkey h53s45ef46agv4646n2j8qpo
      template 2 sha1key b74hd748ghzm67k6m6d1
;
      map-template 101 2
IPSec config>
```

Router 2:

```
IPSec config>
      assign-access-list 101
      map-template 101 2
```

Ahora ya se puede guardar la configuración y reiniciar el equipo para activar la misma, y cualquier comunicación entre los hosts A y B se realizará de forma segura, en lo que a la comunicación se refiere. Aunque la seguridad completa del sistema de comunicaciones, basada también en los equipos, claves introducidas, permisos de modificación, etc, es responsabilidad del usuario.

4.2. Ejemplo 2: Modo dinámico (IPSec IKE Main Mode)



El escenario para este ejemplo es el mismo que el anterior, pero ahora se va a establecer un Túnel basado en Templates dinámicos, para que las comunicaciones, claves, etc, sean negociadas automáticamente utilizando el modo Main.

· *Creación de las listas de control de acceso*

No hay ninguna modificación en la configuración con relación al ejemplo 1.

· *Creando Templates*

Ahora se deben crear los Templates ISAKMP y dinámicos. Se destaca el último comando para introducir la clave Pre-shared, que debe ser la misma en ambos equipos. Por defecto, el modo de negociación es Main Mode, en el que se enmascaran las identidades de los routers extremos del Túnel. Aunque se han introducido también los mismos tiempos de vida, estos parámetro podrían ser diferentes y ser negociados.

Router 1:

```
IPSec config>ENABLE
IPSec config>TEMPLATE 1
default                  sets default values to a template or creates a new one
dynamic                  dynamic template
manual                   manual template
isakmp                   isakmp template
source-address           tunnel's local IP address
destination-address      IP address of the other remote end of the tunnel
backup-destination       backup destination IP address
spi                      Security Parameter Index
key                      template encryption DES key
tkey                     triple DES key
md5key                   MD5 key
sha1key                  SHA1 key
antireplay               activates the Anti-Replay service
padding-check            enables padding check
udp-encapsulation        enables UDP encapsulation
life                     introduces the SAs life span created from the template
ike                      configures parameters relative to the IPSec IKE mode
keepalive                enables the available keepalive services
no                       deletes a backup destination or disables an option
Type an option [default]? isakmp
des       encryption algorithm DES (Data Encryption Standard)
tdes      encryption algorithm TDES (Triple Data Encryption Standard)
Type an option [des]? Tdes
```

```
md5       authentication algorithm MD5
sha1      authentication algorithm SHA1
Type an option [md5]? sha1
IPSec config> TEMPLATE 1 destination-address
IP address [0.0.0.0]? 200.200.200.2
IPSec config> TEMPLATE 1 life
type          type of life duration for the SA
duration      life duration
Type an option [type]? duration
seconds      lifetime in seconds
kbytes       lifetime in kbytes
Type an option [seconds]?
SECONDS[28800]? 43200

IPSec config> TEMPLATE 3 dynamic
esp      ESP security service (Encapsulating Security Payload)
ah       AH security service (Authentication Header)
Type an option [esp]?
des       encryption algorithm DES (Data Encryption Standard)
tdes      encryption algorithm TDES (Triple Data Encryption Standard)
Type an option [des]? tdes
md5       authentication algorithm MD5
sha1      authentication algorithm SHA1
none      no authentication algorithm
Type an option [md5]?
IPSec config> TEMPLATE 3 source-address
IP address [0.0.0.0]? 200.200.200.1
IPSec config> TEMPLATE 3 destination-address
IP address [0.0.0.0]? 200.200.200.2
IPSec config> TEMPLATE 3 life
type          type of life duration for the SA
duration      life duration
Type an option [type]?
seconds      lifetime in seconds
kbytes       lifetime in kbytes
both         lifetime in seconds and kbytes
Type an option [seconds]? both
IPSec config> TEMPLATE 3 life duration
seconds      lifetime in seconds
kbytes       lifetime in kbytes
Type an option [seconds]?
SECONDS[28800]? 14400
IPSec config> TEMPLATE 3 life duration
seconds      lifetime in seconds
kbytes       lifetime in kbytes
Type an option [seconds]? kbytes
KBYTES[0]?
IPSec config> KEY PRESHARED IP 200.200.200.2 plain 1234567890123456

IPSec config>
```

También podría haberse hecho uso de la configuración en modo texto (partiendo de lo obtenido a través de un comando "SHOW CONFIG"):

```
IPSec config>
      enable
      template 1 default
      template 1 isakmp tdes sha1
      template 1 destination-address 200.200.200.2
      template 1 life duration seconds 43200
      template 3 default
      template 3 dynamic esp tdes md5
      template 3 source-address 200.200.200.1
      template 3 destination-address 200.200.200.2
      template 3 life type both
      template 3 life duration seconds 14400
      key preshared ip 200.200.200.2 plain 1234567890123456
```

Router 2:

```
IPSec config>
      enable
      template 1 default
      template 1 isakmp tdes sha1
      template 1 destination-address 200.200.200.1
      template 1 life duration seconds 43200
      template 3 default
      template 3 dynamic esp tdes md5
      template 3 source-address 200.200.200.2
      template 3 destination-address 200.200.200.1
      template 3 life type both
      template 3 life duration seconds 14400
      key preshared ip 200.200.200.1 plain 1234567890123456
```

· *Creando las SPD´s*

Por último, se deben establecer las *SPD's*:

Router 1:

```
IPSec config>ASSIGN-ACCESS-LIST
Enter extended access list id[100]? 101
IPSec config>MAP-TEMPLATE
Enter extended access list id[100]? 101
Enter template id[1]? 3
IPSec config>
```

O bien:

```
IPSec config>
      assign-access-list 101
      map-template 101 3
```

La configuración final de IPSec queda como se muestra a continuación:

```
IPSec config>LIST ALL
IPSec Access Control.
Access Control is: enabled
QOS Preclassify is: disabled

Access Lists assigned to IPSec:
  Extended Access List 101
  Templates: 3


Extended Access List 101, assigned to IPSec

1     PERMIT  SRC=172.24.51.57/32  DES=172.60.1.163/32  Conn:0

TEMPLATES
1 isakmp 3DES SHA1  DES=200.200.200.2
   LifeTime:12h0m0s
   IKE MAIN
   PRESHARED
   addr4 ID TYPE
   OAKLEY GROUP 1

3 dynamic ESP-3DES ESP-MD5  SRC=200.200.200.1 DES=200.200.200.2
   LifeTime:4h0m0s 0 kbytes
   PFS disabled

1 key entries
```

```
   200.200.200.2 ************
0 rsakey entries
Id.           Date.         Len         CA.                    Cert sn.

KeepAlive Configuration:
   Maximum number of encoded packets without receiving an answer: 0.
   Timeout after last packet encoded: 0 seconds.

DPD Configuration:
Idle period(secs) before sending DPD keepalives: 60
Maximum number of DPD keepalives not acknowledged: 3
Period of time(secs) between DPD keepalives: 5
Always send keepalive after idle period expiration : ENABLED
Anti-replay : DISABLED

Check-out time (%) - from SA's end-lifetime - to renegotiate : 10

SA's purge timeout:  15

Use software exponentiation

IPSec config>
```

Con el comando “SHOW CONFIG”:

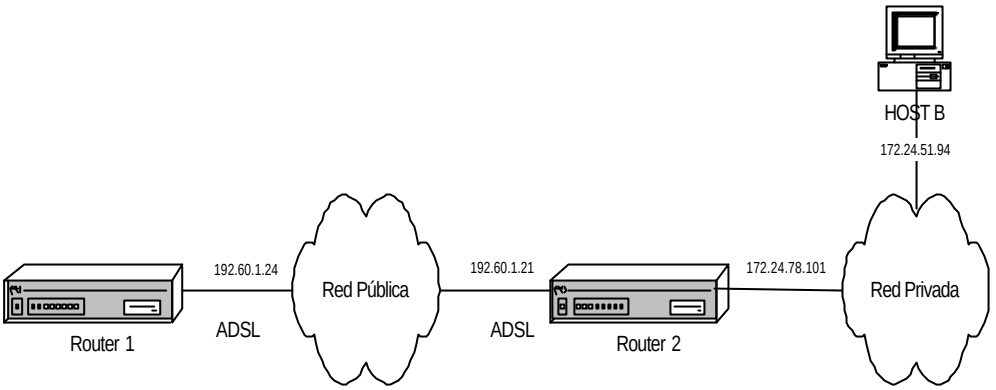
```
IPSec config>SHOW CONFIG
; Showing System Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

      enable
      assign-access-list 101
;
      template 1 default
      template 1 isakmp tdes sha1
      template 1 destination-address 200.200.200.2
      template 1 life duration seconds 43200
;
      template 3 default
      template 3 dynamic esp tdes md5
      template 3 source-address 200.200.200.1
      template 3 destination-address 200.200.200.2
      template 3 life type both
      template 3 life duration seconds 14400
      template 3 life duration kbytes 0
;
      map-template 101 3
      key preshared ip 200.200.200.2 ciphered 0xE21C47018BC8B868FB72F48DC4363FC0
CFABF60C9FFE0286
IPSec config>
```

Router 2:

```
IPSec config>
      assign-access-list 101
      map-template 101 3
```

Tras guardar la configuración y reiniciar el equipo, la comunicación entre los hosts A y B se realizará de forma segura, con la clave Pre-shared como única clave a proteger en este caso.

4.3. Ejemplo 3: Modo dinámico (IPSec IKE Aggressive Mode) con un extremo del Túnel con dirección desconocida



Este escenario refleja cómo conectar dos routers a través de una red privada virtual (VPN) utilizando una línea ADSL como medio para realizar la conexión. Crearemos un Túnel IPSec basado en los Templates dinámicos, con cifrado DES y autenticación MD5 como requisitos de seguridad en la negociación ISAKMP, y servicio ESP con cifrado DES y autenticación SHA1 en la negociación de la SA del Túnel. El Túnel estará basado en Templates dinámicos, para que las comunicaciones, claves, etc., sean negociadas automáticamente utilizando el modo Aggressive.

El modo Aggressive tiene la ventaja que el Router 2 no necesita conocer la dirección IP del otro extremo del Túnel, con lo que esta configuración es adecuada para que muchos equipos se conecten a un único Router 2 conociendo simplemente su *hostname* y la clave común entre ellos. El Router 1 sí necesita conocer la IP del router con el que va a establecer el Túnel, ya que éste es el que inicia la negociación y tiene que saber a qué dirección IP tiene que conectarse.

En primer lugar vamos a describir con detenimiento cómo se configura el Router 1. Una vez configurado este equipo, pasamos a configurar el Router 2, explicando detalladamente aquellos parámetros que difieren de la configuración del Router 1.

a) Configuración del router Router 1

· *Configuración del hostname, direcciones y reglas IP*

Como se ha indicado anteriormente, la autenticación no se va a realizar utilizando las direcciones IP, sino que se realiza mediante el *hostname*. Por este motivo lo primero que tenemos que configurar es el nombre que le vamos a dar al equipo.

```
Teldat              (c)1996-2002

Router model C5i IPSec 1 17 CPU MPC860      S/N: 391/02415
1 LAN, 1 WAN Line, 1 ISDN Line, 1 ADSL Line


*PROCESS 4


Config>SET HOSTNAME GAS1
```

A continuación tenemos que asignar la dirección IP que va a tener nuestro interfaz ADSL. También tenemos que añadir una ruta estática que indique que todos los paquetes que vayamos a mandar a la red privada, lo realice utilizando como puerta de enlace el otro extremo del Túnel IPSec.

Además, se puede especificar un identificador de conexión para el tráfico entre los routers. Sólo es necesario si se desea diferenciar el tratamiento de los paquetes en diferentes conexiones.

```
GAS1 Config>LIST DEVICES

 Interface       Con    Type of interface             CSR     CSR2  int
 ethernet0/0     LAN1   Quicc Ethernet           fa200a00 fa203c00   5e
 serial0/0       WAN1   X25                      fa200a20 fa203d00   5d
 atm0/0          ADSL1  Async Transfer Mode      fa200a60 fa203f00   55
 bri0/0          ISDN1  ISDN Basic Rate Int      fa200a40 fa203e00   5c
 x25-node        ---    Router->Node                    0             0
 ppp1            ---    Generic PPP                     0             0
 ppp2            ---    Generic PPP                     0             0
Config>

GAS1 Config>PROTOCOL IP

-- Internet protocol user configuration --
GAS1 IP config>ADDRESS atm0/0 192.60.1.24 255.255.255.0
GAS1 IP config>ROUTE 172.24.0.0 255.255.0.0 192.60.1.21 1
GAS1 IP config>
```

· *Creación de las listas de control de acceso*

Una vez configurados todos los parámetros propios de IP, pasamos a la configuración de IPSec propiamente dicha.

Lo primero que se debe configurar son las listas de control de acceso. Para esto hay que acceder al menú de configuración de las listas genéricas, escoger un número de lista correspondiente a una lista extendida (entre 100 y 199), indicar un ID de entrada dentro de la lista, en este caso el 1, y dar el valor deseado a los siguientes parámetros:

- La dirección IP de origen, que será la configurada anteriormente en el interfaz ADSL.
- La IP destino, que es el equipo con el que vamos a establecer un Túnel IPSec, en nuestro caso se trata de un Router 2.
- La conexión: tenemos que indicar el ID de conexión asignado al tráfico del Túnel. Este ID se muestra mediante el comando **LIST RULE**. En este ejemplo no es necesario asignar la conexión ya que no se diferencia el tratamiento de los paquetes según la conexión.
- La acción a realizar en los paquetes, en nuestro caso, procesado IPSec (PERMIT).

```
GAS1 Config>FEATURE ACCESS-LISTS

-- Access Lists user configuration --
GAS1 Access Lists config> ACCESS-LIST
Access List number (1-99, 100-199)[1]? 102


GAS1 Extended Access List 102>ENTRY 1
permit              configures type of entry or access control as permit
deny                configures type of entry or access control as deny
source              source menu: subnet or port
destination         destination menu: subnet or port
protocol-range      protocol range
dscp                Diff Serv codepoint
connection          IP connection identifier (rule)
Type an option []? source
address          ip address and mask of the source subnet
```

```
port-range      source port range
Type an option [address]?
Source IP address [0.0.0.0]? 192.60.1.24
Source IP mask [0.0.0.0]? 255.255.255.255
GAS1 Extended Access List 102>entry 1 destination
address         ip address and mask of the destination subnet
port-range      destination port range
Type an option [address]?
Destination IP address [0.0.0.0]? 172.24.0.0
Destination IP mask [0.0.0.0]? 255.255.0.0
GAS1 Extended Access List 102>entry 1 permit
GAS1 Extended Access List 102>
```

O bien:

```
GAS1 Access Lists config>
   access-list 102
      entry 1 permit
      entry 1 source address 192.60.1.24 255.255.255.255
      entry 1 destination address 172.24.0.0 255.255.0.0
```

· *Creando Templates*

Ahora, se deben crear los Templates ISAKMP y dinámicos. Se destaca el último comando para introducir la clave Pre-shared, que debe ser la misma en ambos equipos. A diferencia del ejemplo anterior, en este ejemplo, el modo de negociación es Aggressive Mode, en el que no se enmascaran las identidades de los routers extremos del Túnel, ni se conoce la dirección IP del otro extremo del Túnel.

Aunque se han introducido también los mismos tiempos de vida, estos parámetros podrían ser diferentes y ser negociados, de forma que el resultado de la negociación sería el menor configurado de los extremos del Túnel.

A la hora de crear el Template ISAKMP, hay que indicar el tipo de cifrado (DES) y el tipo de autenticación (MD5) que se va a utilizar, tal y como se indica en las especificaciones iniciales de seguridad.

Al crear el Template, hay que indicar un número de ID, que será el que se utilice en el resto de la configuración de este Template. También hay que indicar la IP destino del Túnel al que se va a conectar, y además indicar que se va a utilizar el modo Aggressive, ya que la autenticación se va a realizar mandando el hostname y no la dirección IP. Esto es muy útil cuando a priori no se conoce la dirección IP del otro extremo del Túnel, como es el caso del Router 2 del ejemplo, en el que no tiene por qué saber la dirección IP de los Routers que se van a conectar a él. Con sólo conocer su hostname, se puede crear el Túnel IPSec.

Mediante el comando **TEMPLATE 1 IKE IDTYPE FQDN** le indicamos que en la autenticación utilice su hostname en vez de la dirección IP que es la opción por defecto.

```
GAS1 Config>PROTOCOL IP

-- Internet protocol user configuration --
GAS1 IP config>IPSEC

-- IPSec user configuration --
GAS1 IPSec config>ENABLE
GAS1 IPSec config>TEMPLATE 1
default                 sets default values to a template or creates a new one
dynamic                  dynamic template
manual                   manual template
isakmp                   isakmp template
source-address           tunnel's local IP address
destination-address      IP address of the other remote end of the tunnel
```

```
backup-destination       backup destination IP address
spi                      Security Parameter Index
key                      template encryption DES key
tkey                     triple DES key
md5key                   MD5 key
sha1key                  SHA1 key
antireplay               activates the Anti-Replay service
padding-check            enables padding check
udp-encapsulation        enables UDP encapsulation
life                     introduces the SAs life span created from the template
ike                      configures parameters relative to the IPSec IKE mode
keepalive                enables the available keepalive services
no                       deletes a backup destination or disables an option
Type an option [default]? isakmp
des       encryption algorithm DES (Data Encryption Standard)
tdes      encryption algorithm TDES (Triple Data Encryption Standard)
Type an option [des]?
md5       authentication algorithm MD5
sha1      authentication algorithm SHA1
Type an option [md5]?
GAS1 IPSec config> TEMPLATE 1 destination-address
IP address [0.0.0.0]? 192.60.1.21
GAS1 IPSec config> TEMPLATE 1 ike
ca          CA
mode        mode in which phase I of the ISAKMP/IKE exchange is carried out
method      establishes the authentication method used by the device
pfs         enables the Perfect Forward Secrecy service
idtype      types of identifiers used during phase 1 of the ISAKMP/IKE exchange
crl         CRL
group       group
jfe         JFE
no          disables an IKE option
Type an option [ca]? mode
aggressive      aggressive mode
main            main mode
Type an option [aggressive]?
GAS1 IPSec config> TEMPLATE 1 ike idtype
ip          IP Address
fqdn        FQDN
ufqdn       UFQDN
keyid       keyid
asn-dn      asn-dn
Type an option [ip]? fqdn
GAS1 IPSec config>
```

O de forma más resumida, si se emplea la configuración en modo texto:

```
GAS1 IPSec config>
    enable
    template 1 default
    template 1 isakmp des md5
    template 1 destination-address 192.60.1.21
    template 1 ike mode aggressive
    template 1 ike idtype fqdn
```

Una vez creado el Template ISAKMP, hay que crear el Template DYNAMIC.

En primer lugar se indica el tipo de servicio, ESP o AH. El servicio ESP proporciona confidencialidad, autenticación de dirección origen en cada paquete IP, integridad, y protección ante réplicas, mientras que el AH no proporciona confidencialidad. Luego hay que indicar que se trata de cifrado (DES) y el tipo de autenticación (SHA1), tal y como se ha indicado en las especificaciones iniciales de seguridad.

A la hora de indicar el ID del Template, debemos elegir uno diferente del Template ISKMP anterior (1), ya que si no se sobrescribiría la configuración anterior con la del Template DYNAMIC. En este ejemplo, se indica que el ID es 2.

Al igual que en el Template ISAKMP, hay que indicar la dirección destino, pero además también hay que indicar cuál va a ser la dirección origen, es decir, la dirección de nuestro interfaz ADSL. En este

Template también hemos habilitado la opción KEEPALIVE, con lo que se asegura que el otro extremo mantiene su SA abierta.

```
GAS1 IPSec config>TEMPLATE 2 dynamic
esp      ESP security service (Encapsulating Security Payload)
ah       AH security service (Authentication Header)
Type an option [esp]?
des       encryption algorithm DES (Data Encryption Standard)
tdes      encryption algorithm TDES (Triple Data Encryption Standard)
Type an option [des]?
md5       authentication algorithm MD5
sha1      authentication algorithm SHA1
none      no authentication algorithm
Type an option [md5]? sha1
GAS1 IPSec config> TEMPLATE 2 source-address
IP address [0.0.0.0]? 192.60.1.24
GAS1 IPSec config> TEMPLATE 2 destination-address
IP address [0.0.0.0]? 192.60.1.21
GAS1 IPSec config> TEMPLATE 2 keepalive
keepalive      enables the available keepalive services
dpd            enables the DPD service (Dead Peer Detection)
no             disables the available keepalive services
Type an option [keepalive]?
GAS1 IPSec config>
```

O bien:

```
GAS1 IPSec config>
      template 2 default
      template 2 dynamic esp des sha1
      template 2 source-address 192.60.1.24
      template 2 destination-address 192.60.1.21
      template 2 keepalive keepalive
```

Por último falta configurar la clave Pre-shared. Esta clave es común para los dos extremos del Túnel.

A la hora de introducir la clave, hay que indicar que se trata de una clave Pre-shared, y que además vamos a introducir un nombre en vez de una dirección IP tal y como se ha explicado anteriormente.

El nombre a introducir se corresponde con el **nombre de dominio** del otro extremo del Túnel.

Además del hostname del equipo, es posible configurar el dominio del equipo. Esto se puede realizar de la siguiente forma:

```
GAS1 IP config>DNS-DOMAIN-NAME
Domain name :  []? madrid.es
Domain name : madrid.es
Domain Name configured.
```

En este ejemplo, no se ha utilizado el nombre de dominio. Por ese motivo, al mostrar el nombre de dominio se nos indica que no está configurado, y que el nombre que utiliza va a ser "**GAS1.**" Éste será el nombre que hay que configurar a la hora de indicar las claves comunes Pre-shared en el otro extremo del Túnel, es decir, en el Router 2.

```
GAS1 IP config>LIST DNS-DOMAIN-NAME
No Domain Name configured.
Partial DNS name : GAS1.
```

En el Router 1, habrá que introducir como hostname a utilizar en la clave "**HOST.**", ya que tampoco se ha configurado el dominio en el Router 2. Sólo se ha configurado el hostname del equipo como HOST.

```
GAS1 IPSec config>KEY PRESHARED HOSTNAME HOST. plain 1234567890123456
```

· *Creando las SPD´s*

Por último, se deben establecer las *SPD's*, es decir, relacionar un control de acceso con un Template creado. En nuestro ejemplo, la lista genérica que se ha configurado es la 102, y el Template que hay que relacionar es el dinámico, es decir, el de ID 2.

```
GAS1 IPSec config>ASSIGN-ACCESS-LIST
Enter extended access list id[100]? 102
GAS1 IPSec config>MAP-TEMPLATE
Enter extended access list id[100]? 102
Enter template id[1]? 2
```

En modo texto:

```
GAS1 IPSec config>
      assign-access-list 102
      map-template 102 2
```

La configuración de IPSec en el Router 1 queda como sigue:

```
GAS1 IPSec config>LIST ALL
IPSec Access Control.
Access Control is: enabled
QOS Preclassify is: disabled

Access Lists assigned to IPSec:
  Extended Access List 102
  Templates: 2


Extended Access List 102, assigned to IPSec

1     PERMIT  SRC=192.60.1.24/32  DES=172.24.0.0/16  Conn:0

TEMPLATES
1 isakmp DES MD5  DES=192.60.1.21
   LifeTime:1h0m0s
   IKE AGGRESSIVE
   PRESHARED
   fqdn ID TYPE
   OAKLEY GROUP 1

2 dynamic ESP-DES ESP-SHA1  SRC=192.60.1.24 DES=192.60.1.21
   LifeTime:1h0m0s
   PFS disabled
   Keep Alive enabled

1 key entries
   HOST. ************
0 rsakey entries
Id.           Date.         Len         CA.                   Cert sn.

KeepAlive Configuration:
   Maximum number of encoded packets without receiving an answer: 0.
   Timeout after last packet encoded: 0 seconds.

DPD Configuration:
Idle period(secs) before sending DPD keepalives: 60
```

```
Maximum number of DPD keepalives not acknowledged: 3
Period of time(secs) between DPD keepalives: 5
Always send keepalive after idle period expiration : ENABLED
Anti-replay : DISABLED

Check-out time (%) - from SA's end-lifetime - to renegotiate : 10

SA's purge timeout:  15

Use software exponentiation

GAS1 IPSec config>
```

Con el comando "SHOW CONFIG" se obtiene lo siguiente:

```
GAS1 IPSec config>SHOW CONFIG
; Showing Menu and Submenus Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

      enable
      assign-access-list 102
;
      template 1 default
      template 1 isakmp des md5
      template 1 destination-address 192.60.1.21
      template 1 ike mode aggressive
      template 1 ike idtype fqdn
;
      template 2 default
      template 2 dynamic esp des sha1
      template 2 source-address 192.60.1.24
      template 2 destination-address 192.60.1.21
      template 2 keepalive keepalive
;
      map-template 102 2
      key preshared hostname HOST. ciphered 0xE21C47018BC8B868FB72F48DC4363FC0CF
ABF60C9FFE0286
GAS1 IPSec config>
```

b) Configuración del router Router 2

· *Configuración del hostname, direcciones y reglas IP*

La configuración del hostname, y de los parámetros del protocolo IP son similares a las realizadas para el Router 1.

```
Teldat              (c)1996-2002

Router model Centrix SEC (c) 1 36 CPU MPC860      S/N: 359/00144
1 LAN

*PROCESS 4
User Configuration
Config>SET HOSTNAME HOST
```

Al configurar el protocolo IP hay que tener cuidado al configurar las direcciones de los interfaces, ya que el interfaz ethernet0/0 conecta la tarjeta de red con la LAN 172.24.0.0, y además hay que asignar la dirección IP al interfaz ADSL donde se va a realizar la conexión del Túnel IPSec.

```
HOST IP config>address atm0/0 192.60.1.24 255.255.255.0
HOST IP config>address ethernet0/0 172.24.78.101 255.255.0.0
```

· Creación de las listas de control de acceso

Una vez configurados todos los parámetros propios de IP, pasamos a la configuración de IPSec propiamente dicha.

La configuración de las listas de control de acceso son similares a las del Router 1, salvo que hay que tener cuidado al configurar las direcciones IP de origen y destino.

```
HOST Access Lists config>
   access-list 103
      entry 1 permit
      entry 1 source address 172.24.0.0 255.255.0.0
      entry 1 destination address 192.60.1.24 255.255.255.255
```

· Creando Templates

Al igual que para el Router 1, se crean los Templates ISAKMP y dinámicos con modo de negociación Aggressive Mode. La clave Pre-shared, que debe ser la misma que la configurada en el Router 1, pero en este caso indicando que la clave corresponde al *hostname* "**GAS1.**".

A la hora de crear el Template ISAKMP, hay que indicar el tipo de cifrado (DES) y el tipo de autenticación (MD5) que se va a utilizar, tal y como se indica en las especificaciones iniciales de seguridad, el cual coincide con el configurado anteriormente en el Router 1.

Al crear el Template, hay que indicar un número de ID, que será el que se utilice en el resto de la configuración de este Template. También hay que indicar la IP destino del Túnel al que se va a conectar, pero como no conocemos qué dirección IP tiene el equipo que se va a conectar con nuestro Router 2, y sólo conocemos su *hostname*, la dirección **IP de destino** será **0.0.0.0**. Además hay que indicar que se va a utilizar el modo Aggressive, y que el IDTYPE será FQDN para que en la autenticación utilice su hostname en vez de la dirección IP que es la opción por defecto.

```
HOST IPSec config>
      enable
      template 1 default
      template 1 isakmp des md5
      template 1 destination-address 0.0.0.0
      template 1 ike mode aggressive
      template 1 ike idtype fqdn
```

Una vez creado el Template ISAKMP, hay que crear el Template DYNAMIC con servicio ESP, cifrado DES y autenticación SHA1, igual que en el Router 1. A la hora de indicar el ID del Template, debemos elegir uno diferente del Template ISAKMP anterior (1), ya que si no se sobrescribiría la configuración anterior con la del Template DYNAMIC. En este ejemplo, se indica que el ID es 2.

Al igual que en el Template ISAKMP, hay que indicar la **dirección destino** (**0.0.0.0**), pero además también hay que indicar cuál va a ser la dirección origen, es decir, la dirección de nuestro interfaz ADSL. En este Template no se habilita la opción KEEPALIVE para liberar tiempo de proceso al Router 2 y que sean los routers que se conecten a él los que tengan que comprobar que está abierta la SA.

```
HOST IPSec config>
      template 2 default
      template 2 dynamic esp des sha1
      template 2 source-address 192.60.1.21
      template 2 destination-address 0.0.0.0
      template 2 life duration seconds 1800
```

Por último falta configurar la clave Pre-shared. Esta clave es común para los dos extremos del Túnel.

A la hora de introducir la clave, hay que indicar que se trata de una clave Pre-shared, y que además vamos a introducir un nombre en vez de una dirección IP tal y como se ha explicado anteriormente.

El nombre a introducir se corresponde con el **nombre de dominio** del otro extremo del Túnel, tal y como se ha explicado en el caso del Router 1.

En este ejemplo, el nombre que tenemos que utilizar es "**GAS1.**" que es el nombre de dominio del Router 1.

```
HOST IPSec config> KEY PRESHARED HOSTNAME GAS1. plain 1234567890123456
HOST IPSec config>
```

Si a este Router se van a conectar más router aparte del Router 1, hay que especificar un hostname y su clave correspondiente para cada uno de ellos.

· *Creando las SPD´s*

Finalmente se deben establecer las *SPD's*, es decir, relacionar un control de acceso con un Template creado. En nuestro ejemplo, la lista genérica extendida que se ha configurado que debe ser asignada a IPSec y asociada con un Template es la 103, y el Template que hay que relacionar es el dinámico, es decir, el de ID 2.

```
HOST IPSec config>
      assign-access-list 103
      map-template 103 2
```

Por último, se puede liberar más tiempo de proceso del Router 2 indicando que no renegocie la SA cuando llegue al porcentaje especificado del tiempo de vida, y que sea el otro extremo del Túnel (Router 1) el que renegocie la SA.

```
HOST IPSec config>ADVANCED RENEGOTIATION-TIME 0
HOST IPSec config>
```

La configuración de IPSec resultante es:

```
HOST IPSec config>LIST ALL
IPSec Access Control.
Access Control is: enabled
QOS Preclassify is: disabled

Access Lists assigned to IPSec:
  Extended Access List 103
  Templates: 2


Extended Access List 103, assigned to IPSec

1     PERMIT  SRC=172.24.0.0/16  DES=192.60.1.0/24  Conn:0

TEMPLATES
1 isakmp DES MD5  DES=0.0.0.0
   LifeTime:1h0m0s
   IKE AGGRESSIVE
   PRESHARED
   fqdn ID TYPE
```

```
   OAKLEY GROUP 1

2 dynamic ESP-DES ESP-SHA1  SRC=192.60.1.21 DES=0.0.0.0
   LifeTime:0h30m0s
   PFS disabled

1 key entries
   GAS1. ************
0 rsakey entries
Id.           Date.         Len         CA.                   Cert sn.

KeepAlive Configuration:
   Maximum number of encoded packets without receiving an answer: 0.
   Timeout after last packet encoded: 0 seconds.

DPD Configuration:
Idle period(secs) before sending DPD keepalives: 60
Maximum number of DPD keepalives not acknowledged: 3
Period of time(secs) between DPD keepalives: 5
Always send keepalive after idle period expiration : ENABLED
Anti-replay : DISABLED

Check-out time (%) - from SA's end-lifetime - to renegotiate : 0

SA's purge timeout:  15

Use software exponentiation

HOST IPSec config>
```

Lo que se muestra al ejecutar un comando “SHOW CONFIG” es:

```
HOST IPSec config>SHOW CONFIG
; Showing System Configuration ...
; Router CENTRIX SEC (c) 1 36 Version 10.0.0CAI

      enable
      assign-access-list 103
;
      template 1 default
      template 1 isakmp des md5
      template 1 ike mode aggressive
      template 1 ike idtype fqdn
;
      template 2 default
      template 2 dynamic esp des sha1
      template 2 source-address 192.60.1.21
      template 2 life duration seconds 1800
;
      map-template 103 2
      key preshared hostname GAS1. ciphered 0xE21C47018BC8B868FB72F48DC4363FC0CF
ABF60C9FFE0286
      advanced renegotiation-time 0
HOST IPSec config>
```

Una vez guardada la configuración de ambos equipos y reiniciados éstos de modo que se active dicha configuración, la comunicación entre los routers se realizará de forma segura, con la clave Pre-shared como única clave a proteger en este caso.

5. CERTIFICADOS

Cuando se aplican los métodos de autenticación basados en RSA se necesita usar claves asimétricas RSA. Estas claves se suelen utilizar dentro de unos encapsulados de nivel superior llamados *Certificados*. Los Routers Teldat permiten la autenticación basada en RSA, y para ello necesitan herramientas que sean capaces de gestionar Certificados.

En este apartado se va a describir la forma de trabajar con Certificados, es decir, como se cargan, se asignan a Templates, se crean, etc.

5.1. Menú CERT

Dentro del menú IPSec se encuentra el menú CERT y dentro de él el comando CERTIFICATE tiene las siguientes opciones:

Comando	Función
LOAD	Carga un CERTIFICADO desde un disco a memoria RAM.
UPDATE	Carga dinámicamente un CERTIFICADO desde un disco a memoria RAM.
DELETE	Borra un CERTIFICADO de un disco.
PRINT	Muestra por pantalla el contenido de un CERTIFICADO .

"CERTIFICATE [CertFile] LOAD"

Con este comando se permite cargar un Certificado desde un disco a la memoria RAM del equipo. Antes de realizar una operación con un Certificado este debe ser cargado en RAM con este comando.

Ejemplo:

```
CERTIFICATES config>certificate router.cer load
```

"CERTIFICATE [CertFile] UPDATE"

Con este comando se permite cargar un Certificado desde un disco a la memoria RAM del equipo haciéndolo dinámicamente, es decir, sin necesidad de reiniciar el equipo.

Ejemplo:

```
CERTIFICATES config>certificate router.cer update
```

"CERTIFICATE [CertFile] DELETE"

Con este comando se permite borrar un Certificado de un disco.

Ejemplo:

```
CERTIFICATES config>certificate router.cer delete
```

"CERTIFICATE [CertFile] PRINT"

Con este comando se permite imprimir el contenido de un certificado previamente cargado.

Ejemplo:

```
CERTIFICATES config>certificate router.cer print
Version                   : V3
Serial Number             : 547E D185 0000 0000 1E6E
Algorithm Identifier      : SHA1 With RSA
Issuer:
  CN (Common Name        ): SECTESTCA1
  OU (Organizational Unit): Microsoft, Interopability Testing Only
  O  (Organization Name  ): Microsoft, Interopability Testing Only
  L  (Locality           ): Redmond
  S  (State or Province  ): WA
  C  (Country Name       ): US
  E  (Email              ): testca@microsoft.com
Valid From                : Wed Jul 25 09:21:24 2001
Valid To                  : Thu Jul 25 09:31:24 2002
Subject:
  E  (Email              ): jiglesias@teldat.es
  CN (Common Name        ): router.teldat.es
  OU (Organizational Unit): ImasD
  O  (Organization Name  ): Teldat
  L  (Locality           ): Tres Cantos
  S  (State or Province  ): Madrid
  C  (Country Name       ): sp
Publick Key               :
  Algorithm Identifier    : RSA
  Modulus Length          : 512 Bits.
  Modulus                 :
    E1CF D175 90EE 43BC 4BC5 D215 695A 74CC D1E8 F301 4F09 2093 7B12 84C0
    2C07 DE4B E458 9D48 43CB 4F14 A075 0D09 FB57 71DB 4FC6 8FDF 1FEF AA6D
    13BB 96FB 88FA 1343
  Exponent                :
    01 00 01
Signature                 :
  Signature Algorithm     : SHA1 With RSA
  Signature Data Info     : 2048 Bits.
  Signature Data          :
    3C10 94F3 CE87 0040 C3D0 A59F 1F0E 84DC E21F CCFD CA7A 2A32 651B 3D27 F9D0
    F87A 6993 E22C 28F5 7954 ED49 1E90 A52C 8098 F686 5E51 18DA D713 D65E 81BB
    267A 1D70 957D FB2F C841 E155 AD3C 3B38 6796 FA62 F6EF 8D76 DEDF 09B2 52C3
    3496 AD4B BF06 1415 3111 DEDD B2BE 9C68 5584 0A3B BF41 90B3 05C4 5CA1 E079
    AADA 43B1 F48D 9DEE 9793 907E 262D 2CC5 325C F3D1 892C 54E7 4736 06A3 4883
    A239 B68D 5477 13A8 BDE0 D7F4 18C1 FD94 3116 48FC C701 BA86 D932 A5C8 C28C
    5FE0 D8CF BE39 CF77 5CCC A104 0189 FF0B 5598 DBB1 2EB5 6269 9683 31DF 19BB
    DDEB 8BC0 FFDA 4587 13E4 42FF 7AF1 BD63 ACE4 D469 37B7 03FA 78DD 4535 49FB
    36AA 4525 F6EF 33A8 F5DB 3934 5079 A536
```

5.2. Comando KEY RSA

Este comando permite trabajar con las claves RSA generadas en el Router.

Comando	Función
GENERATE	Genera un par de claves RSA aleatorias.
CA-CHANGE	Cambia la CA asociada a la clave RSA generada.

"KEY RSA GENERATE [CA NAME][SIZE(512/1024/2048)]"

Con este comando se genera un clave aleatoria RSA y se asocia a una nombre de CA. Es decir, se genera una pareja de clave pública y privada que se almacerán en el disco del equipo al guardar la configuración.

Después de generar la pareja de claves el equipo pregunta si se desea generar un fichero CSR, *Certificate Signing Request*.

Ejemplo:

```
IPSec config>key rsa generate caname 512
RSA Key Generation.
Please, wait for a few seconds.
 RSA Key Generation done.
Checking..OK
Key Generation Process Finished.
Generate CSR?
(Yes/No)? n
Do not forget to save RSA keys.
```

"KEY RSA CA-CHANGE"

Con este comando se permite cambiar la CA asociada a un clave RSA generada con anterioridad.

Ejemplo:

```
IPSec config>lis key rsa all
1 rsakey entries
Id.           Date.         Len         CA.                  Cert sn.
   1   06/18/03  11:46:16    512         caname               ---
atlaslocal IPSec config>key rsa ca-change 1 newca
Do not forget to save RSA keys changes.
IPSec config>lis key rsa all
1 rsakey entries
Id.           Date.         Len         CA.                  Cert sn.
   1   06/18/03  11:46:16    512           newca              ---
```

5.3. Obtener certificados mediante CSR

Se puede obtener un certificado para un equipo Teldat mediante la creación de un Certificate Signing Request (CSR). El objetivo final es conseguir dos ficheros: el certificado de la CA, *caname.cer*, y el del Router, *router.cer*. Los pasos a seguir son los siguientes:

1. Si se tiene una clave privada generada, se debe crear un CSR asociado a esa clave. Para eso se ejecuta el comando make desde el menu de configuración CSR. Si no se tiene una clave privada generada se debe generar (comando *key rsa generate*) y responder afirmativamente cuando el equipo pregunte si se desea generar CSR. La clave privada tendrá asociada una CA mediante un nombre de fichero que corresponde al certificado instalado en el equipo de esa CA, *caname.cer*, (Esta operación se puede realizar aunque aún no se disponga del certificado de la CA).
2. Después de generar el CSR se puede guardar en un fichero que luego se puede obtener por FTP o se puede imprimir por consola ejecutando el comando *print*. Normalmente los CSR se codifican en base64.
3. El CSR se debe entregar a la CA para que devuelva un certificado, *router.cer*. Normalmente en este paso la CA también envía un certificado de la propia CA, *caname.cer*.
4. Los certificados obtenidos se instalarán en el equipo enviándolos por FTP y ejecutando el comando *quote site savebuffer*.
5. Ahora se debe entrar en el menú *CERT* y cargar el certificado del router mediante el comando *certificate **router** update*.
6. Se crea un template que utilice el método RSA, *template **1** ike method rsa*.
7. Por último se asocia el certificado de la CA al template usado, con el comando *template **1** ike ca **caname***.

8. Por último hay que guardar la configuración.

Es decir, la asociación entre los componentes es la siguiente:

- **(Private Key, CSR)** = Asociación por identificador de clave privada.
- **(Private Key, CA)** = Asociación por nombre de CA.
- **(Private Key, Certificado de Equipo)** = Asociación por CA y número de serie del certificado. La CA debe estar asociada a un template y el certificado debe estar cargado.

NOTA: Verisign no admite ciertos caracteres en los campos del CSR. Entre ellos está la arroba (@), por lo que no se puede incluir una dirección de email. El error devuelto por Verisign es el 105. Este campo deberá dejarse en blanco si se va a entregar este CSR a Verisign.

El comando *list template all* mostrará que tal ha ido todo:

```
IPSec config>list template all
TEMPLATES
1 isakmp 3DES MD5  DES=1.1.1.1
   LifeTime:1h0m0s
   IKE MAIN
   RSA SIGNATURE
      CA      : SECTEST.CER. Expired.
      CRL     : disabled
       USER    : ROUTER.CER. Signature ok. Expired. Without Private Key.
   fqdn ID TYPE
   OAKLEY GROUP 1
```

Capítulo 3
Monitorización

1. Introducción

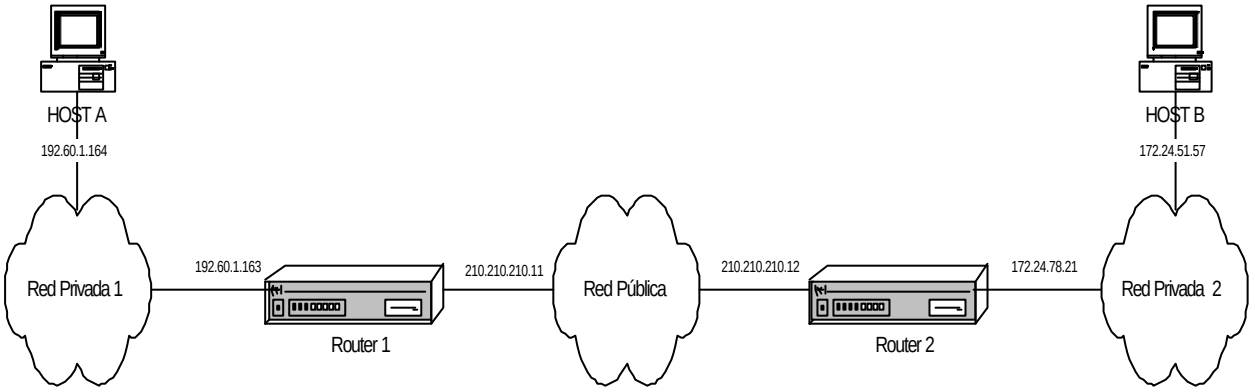
La monitorización de IPSec en los **Router Teldat** se realiza una vez configurados los elementos de la SPD.

La diferencia que hay con respecto a la configuración es que ahora no vamos a variar ningún parámetro, lo que haremos serán listarlos, y si los variamos se hará de forma temporal, ya que los cambios realizados en monitorización sólo tienen efecto mientras no se reinicie el router.

La monitorización muestra un listado del funcionamiento de las conexiones que hemos configurado anteriormente, las ISAKMP SAs o de primera fase y las SAs Dinámicas y Manuales o de segunda fase. Además permite eliminar dichas conexiones.

En primer lugar se describirán los pasos que hay que seguir para poder acceder a dicha monitorización. En segundo lugar se explica la monitorización de las SAs. Después, se verá un comando que nos muestra toda la monitorización. Y por último, se proporciona una relación de problemas y soluciones que normalmente se pueden encontrar en las negociaciones IPSec.

Todos los ejemplos que se verán en cada comando de monitorización están basados en el siguiente escenario.



2. Monitorización de IPSec

2.1. Monitorización Inicial

En este apartado se describen los pasos necesarios para acceder a la monitorización de IPSec en los **Router Teldat**. Para poder entrar en el entorno de monitorización se debe introducir los siguientes comandos:

```
*P 3
+PROTOCOL IP
IP>IPSEC
IPSEC protocol monitor
IPSEC>
```

Dentro del entorno de monitorización del protocolo IPSec se dispone de los siguientes comandos inicialmente:

Comando	Función
? (AYUDA)	Lista los comandos u opciones disponibles.
CLEAR	Borra la memoria cache y las SAs.
LIST	Lista la monitorización de IPSec.
EXIT	Sale del prompt de configuración de IPSec.

2.2. Monitorización de las SAs

Como vimos en la introducción, las SAs (*Security Association*) son conexiones de seguridad que se crean una vez consultada la SPD y contienen la información de seguridad (claves de autenticación y encriptación) necesaria para procesar el paquete. Por tanto cuando creamos una SA lo que tenemos es una conexión establecida para transmitir datos de forma segura, entre los dos extremos del Túnel.

Hay dos tipos de SAs, las SAs de primera fase o ISAKMP SAs, y las SAs de segunda fase, que pueden ser SAs Dinámicas o SAs Manuales.

Algo que hay que tener en cuenta en las SAs, es que hay una diferencia clara entre las SAs Dinámicas y ISAKMP SAs, con respecto a las SAs Manuales. Las SAs Manuales son conexiones permanentes, es decir que en el momento que se configuran los Templates Manuales se establece la conexión entre los extremos del Túnel. En cambio las SAs Dinámicas y ISAKMP SAs como son dinámicas solo aparecerán cuando estemos utilizando la conexión entre los extremos del Túnel, es decir cuando el Túnel se establece.

La monitorización de las SAs nos permite realizar dos operaciones: cortar las conexiones, es decir eliminar las SAs mediante el comando **CLEAR**, o bien hacer un listado de todas las conexiones que tenemos establecidas, es decir de todas las SA. Esto se ejecuta a través del comando **LIST**.

a) CLEAR

A través de este comando podemos cortar la conexión establecida entre los extremos del Túnel. Dicha interrupción dependerá de cual sea el tipo de SA que tengamos.

Si la SA es SA Manual no tiene sentido eliminarla ya que, como hemos visto anteriormente, la conexión es permanente por tanto no la podremos cortar. Lo que si tiene sentido en cambio es eliminar las SAs Dinámicas y las ISAKMP SAs.

Comando	Función
NEGOTIATION	Elimina las ISAKMP SAs o SAs de primera fase.
OUT	Elimina las SAs Dinámicas de salida.
IN	Elimina las SAs Dinámicas de entrada.

"CLEAR SA NEGOTIATION ALL"

Elimina todas las ISAKMP SAs.

Ejemplo:

```
IPSEC>CLEAR SA NEGOTIATION ALL
Connection cleared
IPSEC>
```

"CLEAR SA NEGOTIATION CONNECTION [ID]"

El campo "ID" es el número identificador de la SA. Se eliminará solo la ISAKMP SA definida por el número "ID".

Ejemplo:

```
IPSEC>CLEAR SA NEGOTIATION CONNECTION 1
Connection 1 cleared
IPSEC>
```

"CLEAR SA NEGOTIATION ADDRESS-FILTER [DIR IP][MASK]"

Elimina la ISAKMP SA con dirección origen o destino que esté incluida dentro del rango definido por [DIR IP][MASK].

Ejemplo:

```
IPSEC>CLEAR SA NEGOTIATION ADDRESS-FILTER 210.210.210.12  255.255.255.25
Connection 1 cleared
IPSEC>
```

"CLEAR SA OUT/IN ALL"

Elimina todas las SAs Dinámicas, ya sean de salida o de entrada.

Ejemplo:

```
IPSEC>CLEAR SA OUT ALL
All Connection cleared
IPSEC>
```

"CLEAR SA OUT /IN CONNECTION [ID]"

El campo "ID" es el número identificador de la SA. Se eliminará solo la SA Dinámica definida por el número "ID".

Ejemplo:

```
IPSEC>CLEAR SA OUT CONNECTION 1
Connection 1 cleared
IPSEC>
```

"CLEAR SA OUT/IN ADDRESS-FILTER [DIR IP][MASK]"

Elimina la SA Dinámica o Manual con dirección origen o destino que esté incluida dentro del rango definido por [DIR IP][MASK] .

Ejemplo:

```
IPSEC>CLEAR SA OUT ADDRESS-FILTER 210.210.210.12  255.255.255.255
Connection 1 cleared
IPSEC>
```

b) LIST

Podemos visualizar todas las conexiones de salida o entrada, es decir todas las SAs, a través de este comando. Con ello sabremos si las conexiones están o no en activo.

Las SAs Manuales como son conexiones permanentes, siempre las veremos al listarlas. En cambio las SAs Dinámicas e ISAKMP SAs como son dinámicas solo van a verse listadas si se está utilizando la conexión entre los extremo del Túnel, es decir si estamos transmitiendo datos.

Comando	Función
NEGOTIATION	Lista las ISAKMP SAs o SAs de primera fase.
OUT	Lista las SAs Dinámicas y Manuales de salida.
IN	Lista las SAs Dinámicas y Manuales de entrada.

"LIST SA NEGOTIATION ALL"

Lista todas las ISAKMP SAs que están activas.

Ejemplo:

```
IPSEC>LIST SA NEGOTIATION ALL

SA NEGOTIATION
SA 1  Resp = 210.210.210.11
SRC=210.210.210.12 DES=210.210.210.11 STATE=5
LifeTime:23h59m0s (23h58m53s)
ClientSRC=192.60.1.164 ClientDES=172.24.51.57 ICMP SPORT=2048 DPORT=13416
ISAKMP_SA available:Purgetime=60
ISAKMP_NEGII (0x39330A0E/0x23951B2E)

SA 2  Resp = 200.200.200.1
SRC=200.200.200.2 DES=200.200.200.1 STATE=5
LifeTime:23h59m0s (23h58m53s)
ClientSRC=192.168.10.6 ClientDES= 192.168.4.5 ICMP SPORT=1500 DPORT=6000
ISAKMP_SA available:Purgetime=60
ISAKMP_NEGII (0x40530A0E/0x12351B2E)
IPSEC>
```

"LIST SA NEGOTIATION ADDRESS-FILTER [DIR IP][MASK]"

Lista la ISAKMP SA activa con dirección origen o destino que esté incluida dentro del rango definido por [DIR IP][MASK].

Ejemplo:

```
IPSEC>LIST SA NEGOTIATION ADDRESS-FILTER 210.210.210.12  255.255.255.255

SA NEGOTIATION
SA 1  Resp = 210.210.210.11
SRC=210.210.210.12 DES=210.210.210.11 STATE=5
LifeTime:23h59m0s (23h58m53s)
ClientSRC=192.60.1.164 ClientDES=172.24.51.57 ICMP SPORT=2048 DPORT=13416
ISAKMP_SA available:Purgetime=60
ISAKMP_NEGII (0x39330A0E/0x23951B2E)
IPSEC>
```

"LIST SA OUT/IN ALL"

Lista todas las SAs Dinámicas activas y las SAs Manuales, ya sean de salida o de entrada.

Ejemplo:

```
IPSEC>LIST SA OUT ALL

SA OUT
SA 3 SPI=0x23951B2E
SA UP, ESP-DES ESP-MD5 SRC=210.210.210.12 DES=210.210.210.11
LifeTime:24h0m0s 4608000 kbytes  (23h46m31s 4608000 kbytes )
encode pkts:0 (err:0), decode pkts:0 (err:0)

SA 4 SPI=0x12351B2E
SA UP, ESP-DES ESP-MD5 SRC=200.200.200.2 DES=200.200.200.1
LifeTime:24h0m0s 5008000 kbytes  (23h46m31s 5008000 kbytes )
encode pkts:0 (err:0), decode pkts:0 (err:0)
IPSEC>
```

"LIST SA OUT/IN ADDRESS-FILTER [DIR IP][MASK]"

Lista la SA Dinámica activa o SA Manual con dirección origen o destino que esté incluida dentro del rango definido por [DIR IP][MASK].

Ejemplo:

```
IPSEC>LIST SA OUT ADDRESS-FILTER 210.210.210.12  255.255.255.255

SA OUT
SA 3 SPI=0x23951B2E
SA UP, ESP-DES ESP-MD5 SRC=210.210.210.12 DES=210.210.210.11
LifeTime:24h0m0s 4608000 kbytes  (23h46m31s 4608000 kbytes )
encode pkts:0 (err:0), decode pkts:0 (err:0)
IPSEC>
```

2.3. Listado de la Monitorización

A través del comando **LIST** podemos ver un listado de todo el proceso de monitorización.

Comando	Función
ADDRESS-FILTER	Lista la monitorización para una determinada dirección.
NEGOTIATION	Lista el proceso de negociación IKE.
NOTIFICATION	Muestra mensajes de notificación de las negociaciones IKE.
SA	Monitorización de Sas, vista anteriormente con detalle.
STATISTICS	Muestra estadísticos de las negociaciones IKE.

"LIST ADDRESS-FILTER [DIR IP][MASK]"

Realiza un listado de toda la monitorización con dirección origen o destino que esté incluida dentro del rango definido por [DIR IP][MASK].

Si no indicamos ninguna dirección, listará toda la monitorización con todas las direcciones origen o destino.

Ejemplo:

```
IPSEC>LIST ADDRESS-FILTER 210.210.210.12 255.255.255.255
SA OUT
SA 3 SPI=0x23951B2E
SA UP, ESP-DES ESP-MD5 SRC=210.210.210.12 DES=210.210.210.11
LifeTime:24h0m0s 4608000 kbytes  (23h46m31s 4608000 kbytes )
encode pkts:0 (err:0), decode pkts:0 (err:0)
```

```
SA IN
SA 2 SPI=0x39330A0E
SA UP, ESP-DES ESP-MD5 SRC=210.210.210.11 DES=210.210.210.12
LifeTime:24h0m0s 4608000 kbytes  (23h46m28s 4608000 kbytes )
encode pkts:0 (err:0), decode pkts:0 (err:0)

SA NEGOTIATION
SA 1  Resp = 210.210.210.11
SRC=210.210.210.12 DES=210.210.210.11 STATE=5
LifeTime:23h59m0s (23h58m53s)
ClientSRC=192.60.1.164 ClientDES=172.24.51.57 ICMP SPORT=2048 DPORT=13416
ISAKMP_SA available:Purgetime=60
ISAKMP_NEGII (0x39330A0E/0x23951B2E)
IPSEC>
```

“LIST NEGOTIATION”

Muestra un listado de todo el proceso de negociación IKE entre los dos extremos del Túnel.

Ejemplo:

```
IPSEC>LIST NEGOTIATION

  (Time ************************************ 0h0m23s)
210.210.210.12:
  (* --------- Creating ISAKMP NEG ---------)(# 1(0x1))(HDR 0)(HDR sa)
  (prop 1 iskamp #1)(trans 1 id=1)(encryp des)(hash md5)(grp desc 1)(auth presh)
  (life sec)(duration 86340)
210.210.210.11: (HDR 0)(HDR sa)(prop 1 iskamp #1)(trans 1 id=1)(encryp des)
  (hash md5)(grp desc 1)(auth presh)(life sec)(duration 86340)
210.210.210.12:
  (* --------- Matching template ---------)(# 20(0x14))(HDR 0)(HDR keyx)
  (HDR nonce)
0.0.0.0: (Time ************************************ 0h0m1s)
210.210.210.11: (HDR 0)(HDR keyx)(HDR nonce)(vendor 10)
210.210.210.12:
  (* --------- Creating ISAKMP SA ---------)(HDR 0)(id addr4 prot=17 port=500)
  (# 0xd2d2d20c)(HDR hash)
210.210.210.11: (HDR 0)(id addr4 prot=17 port=500)(# 0xd2d2d20b)(HDR hash)
210.210.210.12:
  (* --------- Creating ISAKMP SA id ---------)(# -1629185295(0x9ee49af1))
  (HDR 9ee49af1)(HDR hash)(HDR sa)(prop 1 esp #1)(# 959646222(0x39330a0e))
  (trans 1 id=des)(encap tunnel)(grp desc presh)(life sec)(duration 86400)
  (life kbytes)(duration 4608000)(auth alg md5)(HDR nonce)(HDR keyx)
  (id addr4 prot=0 port=0)(# 0xc03c01a4)(id addr4 prot=0 port=0)(# 0xac183339)
0.0.0.0: (Time ************************************ 0h0m1s)
210.210.210.11: (HDR 9ee49af1)(HDR hash)(HDR sa)(prop 1 esp #1)
  (# 596974382(0x23951b2e))(trans 1 id=des)(encap tunnel)(life sec)
  (duration 86400)(life kbytes)(duration 4608000)(auth alg md5)(grp desc presh)
  (HDR nonce)(HDR keyx)(id addr4 prot=0 port=0)(# 0xc03c01a4)
  (id addr4 prot=0 port=0)(# 0xac183339)
210.210.210.12:
  (* --------- Matching template ---------)(# 1(0x1))(HDR 9ee49af1)(HDR hash)
  (* --------- Creating SA ---------)(# 959646222(0x39330a0e))
  (* --------- Creating SA ---------)(# 596974382(0x23951b2e))
0.0.0.0: (Time ************************************ 0h0m3s
```

“LIST NOTIFICATION”

Muestra mensajes de notificación de la negociación IKE. Negociaciones fallidas propuestas, no compatibles, borrados de las SAs, etc.

Ejemplo:

```
IPSEC>LIST NOTIFICATION

  (Time ************************************ 0h14m5s)
IPSEC>
```

“LIST STATISTICS”

Son estadísticos de la negociación IKE.

Ejemplo:

```
IPSec>LIST STATISTICS

----ESP/AH Statistics:----

Input Stats
-----------
  Frames ok    0
  Frames error 0
  ---> Out-of-Order frames      0
  ---> Unknown payload protocol 0
  ---> Internal errors          0
Output Stats
------------
  Frames ok    0
  No alg auth known errors 0


----IPSEC Forwarding Statistics:----

Sa in not found                 0
Sa out Template not found       0
Sa out not found(only manual)   0

----IKE Statistics:----
Negotiation phase I             0
Negotiation phase II            0
Check Hash Error phase I        0
Check Hash Error phase II       0
Drops Collision IKE messages    0
Drops Waiting IKE Processing    0

   Cypher queue empty:          0

IPSec>
```

2.4. Diagnóstico de problemas en la negociación IKE

En esta sección se van a exponer algunos ejemplos de problemas típicos que suelen aparecer durante la negociación IKE debidos a errores en la configuración. Es muy importante saber identificar en qué fase se encuentra la negociación, para saberlo basta con comprobar el número que tiene asociado el "header" del mensaje que causó el error. Si es 0 implica que es un mensaje de la fase 1 y si es distinto de cero pertenece a la fase 2. El mensaje que produjo del error suele ser el que precede al mensaje de notificación que indica que hubo tal error. Por ejemplo,

```
172.24.51.57: (HDR 0)(HDR sa)(prop 1 isakmp #1)(trans 1 id=1)(encryp des)
  (hash sha)(grp desc 1)(auth rsa)(life sec)(duration 600)(vendor 14)
172.24.78.15:
  (* --------- Creating ISAKMP NEG ---------)(# 57(0x39))(HDR 24343432)
  (notif isakmp no proposal chosen)
```

El mensaje que provocó el error es el enviado por el 172.24.51.57 cuyo HDR tiene el identificador 0. Luego es un error producido en la fase 1 de la negociación.

Otro dato muy importante es saber quien inició la negociación, es decir, quien fue el *iniciador*.

a) El equipo no inicia la negociación

Origen

La lista de control de acceso no ha sido configurada correctamente.

Este mensaje se produce porque el equipo no puede hacer corresponder el paquete que debe desencadenar la negociación con una entrada de la lista de control de acceso de tipo IPSec.

Solución

Chequear los parámetros de la lista de control de acceso.

Direcciones: Origen y Destino. (Cuidado con la subredes)
Máscara.
Protocolo.
Puertos. Origen y Destino.
Template: Debe tener mapeado el Template dinámico correspondiente.

Si sigue sin encontrarse el origen de fallo, chequear el resultado del comando de monitorización **LIST ACCESS OUT** y comprobar que se incrementan los *hits* en la entrada correspondiente.

b) notif isakmp no proposal chosen. Fase 1

Iniciador: `172.24.51.57`

```
172.24.51.57: (HDR 0)(HDR sa)(prop 1 isakmp #1)(trans 1 id=1)(encryp des)
  (hash sha)(grp desc 1)(auth rsa)(life sec)(duration 600)(vendor 14)
172.24.78.15:
  (* --------- Creating ISAKMP NEG ---------)(# 57(0x39))(HDR 0)
  (notif isakmp no proposal chosen)
```

Origen

El Template isakmp no ha sido configurado correctamente.

Este mensaje se produce porque el equipo con dirección 172.24.78.15 no ha podido aceptar ninguna de las propuestas del equipo 172.24.51.57. En esta fase de la negociación se comparan la propuestas recibidas con las configuradas en la isakmp.

Solución

Chequear los parámetros del Template isakmp.

Método de autenticación: RSA_SIGNATURE, PRE-SHARED...
Sistema de cifrado: DES, TDES...
Sistema de autenticación: SHA1, MD5...
Tipo de tiempo de vida: Segundos, Kbytes, ambos...
Grupo: 1 ó 2.

c) notif isakmp payload malformed. Fase 1

Iniciador: `172.24.51.57`

```
172.24.51.57: (HDR 0)(HDR sa)(prop 1 isakmp #1)(trans 1 id=1)(encryp des)
  (hash md5)(grp desc 1)(auth presh)(life sec)(duration 600)(vendor 14)
172.24.78.15:
  (* --------- Creating ISAKMP NEG ---------)(# 67(0x43))
  (* --------- Matching template ---------)(# 20(0x14))(HDR 0)(HDR sa)
  (prop 1 isakmp #1)(trans 1 id=1)(encryp des)(hash md5)(grp desc 1)(auth presh)
  (life sec)(duration 600)
172.24.51.57: (HDR 0)(HDR keyx)(HDR nonce)
172.24.78.15: (HDR 0)(HDR keyx)(HDR nonce)
  (* --------- Creating ISAKMP SA ---------)
172.24.51.57: (HDR 0)(id none prot=148 port=9841)(# 0x3c068321)(HDR 75 0)
172.24.78.15: (HDR 0)(notif isakmp payload malformed)
```

Origen

La clave Pre-shared no ha sido configurada correctamente.

Este mensaje se produce porque el equipo con dirección 172.24.78.15 no ha podido descifrar correctamente el mensaje cifrado enviado por el equipo 172.24.51.57. De hecho, al analizar el

mensaje erróneo ya se observa que se reciben parámetros extraños: identificador desconocido, con protocolo y puerto diferentes a los configurados, seguido de una cabecera desconocida,.hdr 75 0.

Solución

Chequear la clave de Pre-shared y las asociaciones ip_address- clave, hostname-clave.

d) notif esp no proposal chosen. Fase 2

Iniciador: `172.24.51.57`

```
172.24.51.57: (HDR 53da7bd5)(HDR hash)(HDR sa)(prop 1 esp #2)
  (# -786612676(0xd11d3e3c))(trans 1 id=des)(life sec)(duration 300)
  (life kbytes)(duration 100000)(encap tunnel)(auth alg md5)(trans 2 id=des)
  (life sec)(duration 300)(life kbytes)(duration 100000)(encap tunnel)
  (auth alg sha)(prop 2 ah #2)(# -786612676(0xd11d3e3c))(trans 1 id=md5)
  (life sec)(duration 300)(life kbytes)(duration 100000)(encap tunnel)
  (auth alg md5)(trans 2 id=sha)(life sec)(duration 300)(life kbytes)
  (duration 100000)(encap tunnel)(auth alg sha)(HDR nonce)
  (id addr4 prot=0 port=0)(# 0xac183339)(id addr4 prot=0 port=0)(# 0xac184e0f)
172.24.78.15:
  (* --------- Creating ISAKMP SA id ---------)(# -583852704(0xdd331d60))
  (HDR dd331d60)(HDR hash)(notif esp no proposal chosen)
```

Origen

El Template isakmp no ha sido configurado correctamente.

Este mensaje se produce porque el equipo con dirección 172.24.78.15 no ha podido aceptar ninguna de las propuestas del equipo 172.24.51.57. En esta fase de la negociación se comparan la propuestas recibidas con las configuradas en el Template dinámico asociado a la lista de control de acceso correspondiente.

Solución

Chequear los parámetros del Template dinámico.

Tipo de encapsulado: Túnel o Transporte.
Sistema de cifrado: DES, TDES...
Sistema de autenticación: SHA1, MD5...
Tipo de tiempo de vida: Segundos, Kbytes, ambos...
PFS: Comprobar si el equipo remoto admite PFS.

e) notif esp invalid id inform. Fase 2

Iniciador: `172.24.51.57`

```
172.24.78.15: (HDR 0)(id addr4 prot=17 port=500)(# 0xac184e0f)(HDR hash)
  (* --------- Creating ISAKMP SA id ---------)(# 785093687(0x2ecb9437))
172.24.51.57: (HDR 2ecb9437)(HDR hash)(HDR sa)(prop 1 esp #2)
  (# 291357516(0x115dc34c))(trans 1 id=des)(life sec)(duration 300)(life kbytes)
  (duration 100000)(encap tunnel)(auth alg md5)(trans 2 id=des)(life sec)
  (duration 300)(life kbytes)(duration 100000)(encap tunnel)(auth alg sha)
  (prop 2 ah #2)(# 291357516(0x115dc34c))(trans 1 id=md5)(life sec)
  (duration 300)(life kbytes)(duration 100000)(encap tunnel)(auth alg md5)
  (trans 2 id=sha)(life sec)(duration 300)(life kbytes)(duration 100000)
  (encap tunnel)(auth alg sha)(HDR nonce)(id addr4 prot=0 port=0)(# 0xac183339)
  (id addr4 prot=16 port=0)(# 0xac184e0f)
172.24.78.15:
  (* --------- Creating ISAKMP SA id ---------)(# 1537079449(0x5b9df899))
  (HDR 5b9df899)(HDR hash)(notif esp invalid id inform)
```

Origen

La lista de control de acceso no ha sido configurada correctamente.

Este mensaje se produce porque el equipo con dirección 172.24.78.15 no ha podido aceptar el identificador de cliente del equipo 172.24.51.57 *(id addr4 prot=0 port=0)(# 0xac183339) (id addr4 prot=16 port=0)(# 0xac184e0f).* En esta fase de la negociación se comparan la propuestas de identificador recibidas con las configuradas en la lista de control de acceso.

Solución

Chequear los parámetros de la lista de control de acceso.

Direcciones: Origen y Destino. (Cuidado con la subredes)
Máscara.
Protocolo.
Puertos. Origen y Destino.
Template: Debe tener mapeado el Template dinámico correspondiente.

f) notif isakmp invalid cert authority. Fase 1. Iniciador A

Iniciador: `172.24.78.15`

```
172.24.78.15: (HDR 0)(HDR keyx)(HDR nonce)
172.24.51.57: (HDR 0)(HDR keyx)(HDR nonce)(certreq x509sig CERTREG 8)
172.24.78.15:
  (* --------- Creating ISAKMP SA ---------)(HDR 0)
  (notif isakmp invalid cert authority)
```

Origen

El Template isakmp no ha sido configurado correctamente.

Este mensaje se produce porque el equipo con dirección 172.24.78.15 no ha podido encontrar la CA configurada en el Template isakmp correspondiente.

Solución

Chequear los parámetros de los Templates isakmp.

Nombre de CA.
Comprobar que el nombre de la CA corresponde a un fichero del equipo:

```
Router CERTIFICATES config>LIST EXIST
```

g) notif isakmp invalid cert authority. Fase 1. Iniciador B

Iniciador: `172.24.51.57`

```
172.24.78.15: (HDR 0)(HDR keyx)(HDR nonce)(certreq x509sig CERTREG 6)
  (* --------- Creating ISAKMP SA ---------)
172.24.51.57: (HDR 0)(id der_dn port=0 CERTREG 7)(cert x509sig CERTREG 8)
  (HDR sig)(certreq x509sig CERTREG 9)
172.24.78.15: (HDR 0)(notif isakmp invalid cert authority)
```

Origen

El Template isakmp no ha sido configurado correctamente.

Este mensaje se produce porque el equipo con dirección 172.24.78.15 no ha podido encontrar una CA configurada en algún Template isakmp que se corresponda con la del certificado recibido, en el ejemplo, CERTREG 9

Solución

Chequear los parámetros de los Templates isakmp y comparar con el resultado de la ejecución del comando.

```
Router IPSec>LIST CERTIFICATE_NUMBER 9
```

Nombre de CA.

Comprobar que el nombre de la CA corresponde a un fichero del equipo:

```
Router CERTIFICATES config>LIST EXIST
```

h) notif isakmp invalid cert. Fase 1

Iniciador: `172.24.51.57`

```
172.24.51.57: (HDR 0)(HDR keyx)(HDR nonce)
172.24.78.15: (HDR 0)(HDR keyx)(HDR nonce)(certreq x509sig CERTREG 14)
  (* --------- Creating ISAKMP SA ---------)
172.24.51.57: (HDR 0)(id der_dn port=0 CERTREG 15)(cert x509sig CERTREG 16)
  (HDR sig)(certreq x509sig CERTREG 17)
172.24.78.15: (HDR 0)(notif isakmp invalid cert)
```

Origen

El certificado recibido es inválido.

Solución

Chequear que el certificado recibido es correcto con el comando:

```
Router IPSec>LIST CERTIFICATE_NUMBER 16
```

Fijarse en los parámetros:

Periodo de validez.

El Issuer corresponde con la CA requerida.

```
Router IPSec>LIST CERTIFICATE_NUMBER 14
```

Puede que el certificado esté mal firmado.

i) notif isakmp cert unavailable. Fase 1

Iniciador: `172.24.51.57`

```
172.24.51.57: (HDR 0)(HDR keyx)(HDR nonce)
172.24.78.15: (HDR 0)(HDR keyx)(HDR nonce)(certreq x509sig CERTREG 0)
  (* --------- Creating ISAKMP SA ---------)
172.24.51.57: (HDR 0)(id der_dn port=0 CERTREG 1)(cert x509sig CERTREG 2)
  (HDR sig)(certreq x509sig CERTREG 3)
172.24.78.15: (HDR 0)(notif isakmp cert unavailable)
```

Origen

No hay certificado de usuario cargado para enviar al extremo 172.24.51.57 por el equipo 172.24.78.15.

Solución

Chequear que existe un certificado cargado de la CA requerida.

Primero ver cual es la CA requerida.

```
Router IPSec>LIST CERTIFICATE_NUMBER 3
```

Si la CA requerida coincide con la enviada. Ejecutar un listado de los Templates isakmp y ver el resultado que nos indicará cual es el problema.

Si la CA requerida no coincide con la enviada, buscar en el menú CERTIFICATES que existe un certificado cargado perteneciente a esa CA.

```
Router CERTIFICATES config>LIST LOADED PRINTISSUER <certificate_name>
```

2.5. Resumen de opciones de monitorización

Monitorización de las SA	Clear	"CLEAR SA NEGOTIATION ALL" "CLEAR SA NEGOTIATION CONNECTION [ID]" "CLEAR SA NEGOTIATION ADDRESS-FILTER [DIR IP][MASK]" "CLEAR OUT/IN ALL "CLEAR OUT /IN CONNECTION [ID]" "CLEAR OUT/IN ADDRESS-FILTER [DIR IP][MASK]"
	List	"LIST SA NEGOTIATION ALL" "LIST SA NEGOTIATION ADDRESS-FILTER [DIR IP][MASK]" "LIST SA OUT/IN ALL" "LIST SA OUT/IN ADDRESS-FILTER [DIR IP][MASK]"
Listado de monitorización	"LIST ADDRESS-FILTER[DIR IP][MASK]" "LIST NEGOTIATION" "LIST NOTIFICATION" "LIST STATISTICS"	