Marcos Margulius

Hernán Fernández Brando

**Trabajo Práctico Nº3 - IPSec con Certificados**

**Objetivo del Trabajo Práctico**

El presente trabajo práctico tiene por objetivo principal la creación de una entidad certificante para el establecimiento de una conexión con IP Sec, utilizando el conjunto de scripts *easy-rsa* incluídos en la distribución de Linux provista por la cátedra.

**Introducción a IPSec**

En una comunicación usual entre dos terminales, el transporte de los datagramas IP entre origen y destino puede pasar a través de varias redes intermedias que pueden dar lugar a que los paquetes sean interceptados o comprometidos de algún modo. De este modo, para efectuar comunicaciones en donde se garantice entre otros aspectos básicos integridad de los datos, autenticación y confidencialidad; es necesario proteger la información durante su transporte por redes ajenas o públicas.

Ante este contexto, una organización internacional de normalización, el IETF (del inglés, Grupo de Trabajo en la Ingeniería de Internet) desarrolló a IPSec como un entorno de trabajo de capa 3 que provee conexiones IP seguras, sin limitarse al uso de un algoritmo específico. En otras palabras, IPSec provee autenticación y confidencialidad de una manera flexible y extensible: Flexible porque tanto origen y destino pueden negociar el protocolo a usar y sus parámetros asimétricamente. Y extensible porque el estándar propone un set de algoritmos de encriptado y autenticado que puede variar o ser actualizado a lo largo del tiempo.

Security Association

Dadas las variantes posibles en una misma comunicación, IPSec resume todos los detalles del esquema de seguridad utilizado en un campo denominado Security Parameter Index. Este índice indica el algoritmo de autenticado, la clave o claves que el algoritmo de encriptado utiliza, el tiempo de vida de la asociación, y una lista de direcciones de origen autorizadas a utilizar este esquema de seguridad.

Este parámetro es un fruto de la negociación inicial entre origen y destino.

1. Datagrama IP con Autenticación

El mecanismo de autenticado en IPSec está diseñado para garantizar que un paquete entrante es idéntico al paquete enviado por el origen. Esto se realiza considerando campos mutables, como ser el tiempo de vida (que cambia luego de cada paso por un router). Esto es, IPSec autentica solamente los campos inmutables.

Como es de esperar, dentro de la cabecera de autenticación, además de los datos propios para la autenticación, habrá un campo destinado a la Security Association en uso (número de SPI), así como campos indicando un número de secuencia único para cada datagrama enviado, la longitud de la cabecera y el tipo de datos que se envía a continuación.

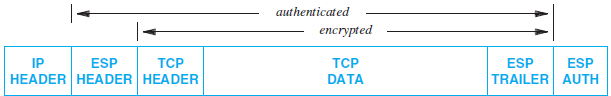


Figura B: Datagrama IP con encriptado y autenticado IPSec mediante E.S.P.

Figura A: Datagrama IP con cabecera de autenticación IPSec

1. Datagrama IP con Confidencialidad E.S.P.

Para garantizar confidencialidad y autenticación, IPSec genera otro tipo de datagrama, agregando varias cabeceras E.S.P (Encapsulating Security Payload), y encriptando el contenido de los datos y de las cabeceras TCP, como se puede ver en la Figura B.



En cuanto a la cabecera ESP, esta contiene simplemente el número de índice SPI y un número de secuencia único para cada datagrama enviado. El ESP Trailer tiene por finalidad realizar un rellenado de bits (para asegurar una longitud determinada de datagramas), y finalmente el último campo contiene información de autenticado de los campos inmutables (mencionados anteriormente).

1. Tuneleo con IPSec

Para mantener las información confidencial a lo largo de comunicaciones intermedias, IPSec también define datagramas para realizar túneles tanto para comunicaciones solamente autenticadas como para comunicaciones autenticadas y con confidencialidad ESP. El contenido de cada campo IPSec es similar a lo detallado anteriormente, sólo que la diferencia radica en que se está autenticando / encriptando un datagrama IP completo (en lugar de un datagrama TCP como se realizaba anteriormente).



Figura C: Tunel IPSec con autenticado.

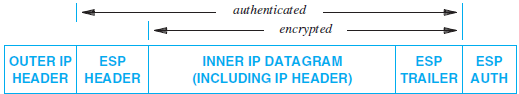


Figura D: Tunel IPSec con encriptado y autenticado mediante E.S.P.

**Proceso de Implementación**

1. Creación de una autoridad certificante

2. Mediante esta entidad se emitirán dos certificados, que serán utilizados en

una conexión autenticada de ipsec.

3. Se anulara uno de los certificados generando la CRL correspondiente, la

conexión no podrá establecerse .

4. Se emitirá un nuevo certificado de servidor para iniciar la conexión

correctamente.

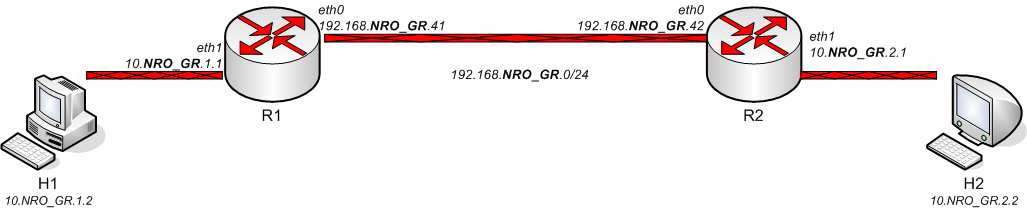
Al igual que en el trabajo previo de IP Sec sin certificados, la implementación del trabajo se realizará con software de virtualización de dispositivos, de manera que el tráfico generado siempre esté dentro del equipo y no se utilize en ningún momento el hardware de red.

Figura 1: Esquema de conexionado de red.

El túnel a implementar estará en la red 192.168.10.0, y la autoridad certificante será R1. Es decir que los certificados de R1 estarán autofirmados.

**Desarrollo del Trabajo Práctico**

**1- Creación de la Autoridad Certificante.**

Inicialmente se procedió al armado de la red de prueba, del mismo modo que el indicado en la Figura 1, y luego se editó el archivo /crypto/conf/config.sh y se completaron las variables de país, provincia, ciudad, organización, e-mail, y deNúmero de grupo.

Luego se generó en R1 la autoridad certificante mediante el script s01-generarCA.sh. que simplemente crea un certificado (ca.crt) y clave privada (ca.key) como se muestra en la Figura 2.

Por lo tanto el router 2 se lo configura para confiar en R1 como autoridad certificante.

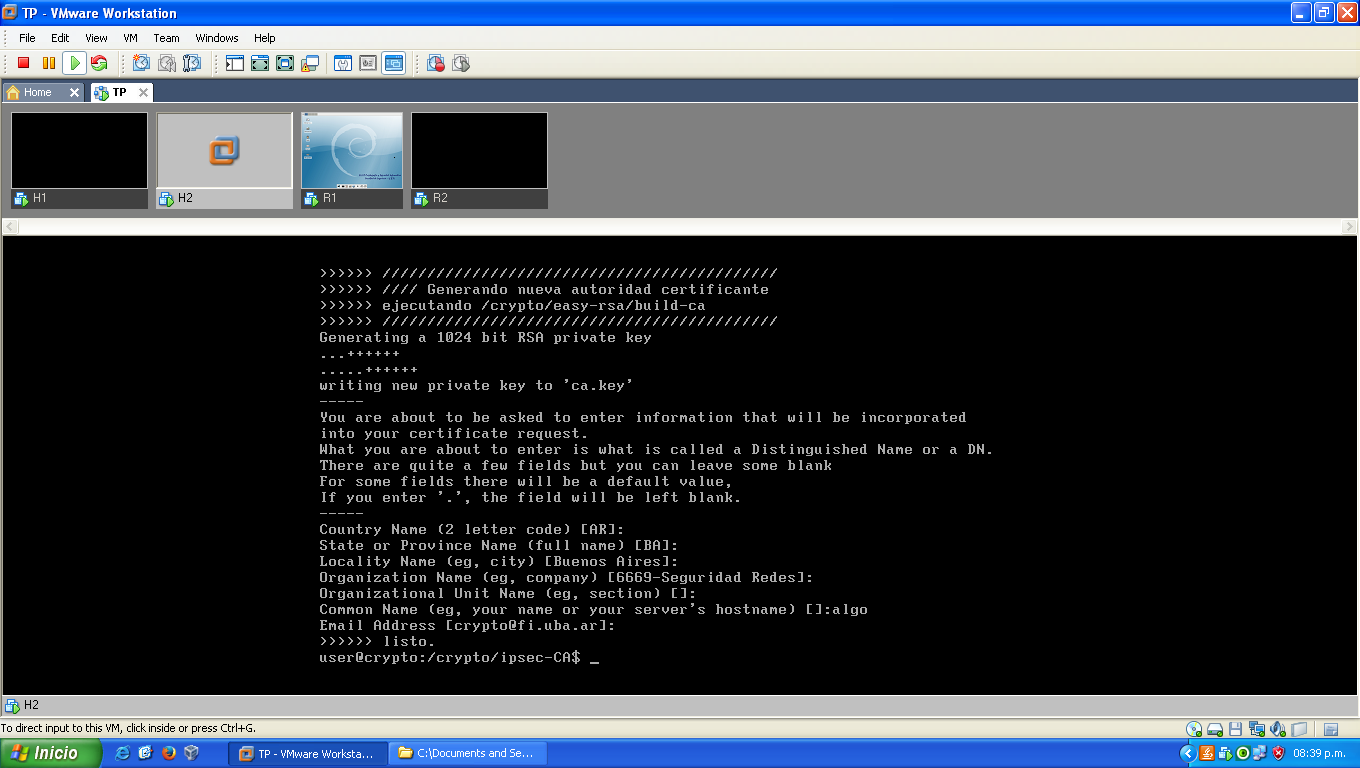


Figura 2: s01-generarCA.sh.

**2- Emisión de certificados e inicialización de enlace bajo IP Sec.**

A- Certificados

Para solicitar la certificación de las identidades de R1 y R2, primero se generó un par de clave pública y privada para cada router. En cuanto a las identidades, resultó importante diferenciar el common name de cada dispositivo y para alcanzar la certificación se verificó que coincida la fecha y hora de todos los dispositivos.

En la Figura 3 se muestran los resultados de realizar el encriptado (o bien la firma) de las solicitudes de la identidad de R1 y R2, creando de este modo los certificados.

En la Figura 4 se observan varios archivos en el directorio de la Autoridad Certificante, /crypto/var/rootCA, entre ellos:

* Serial, Contiene una sola línea con el numero de serie del próximo

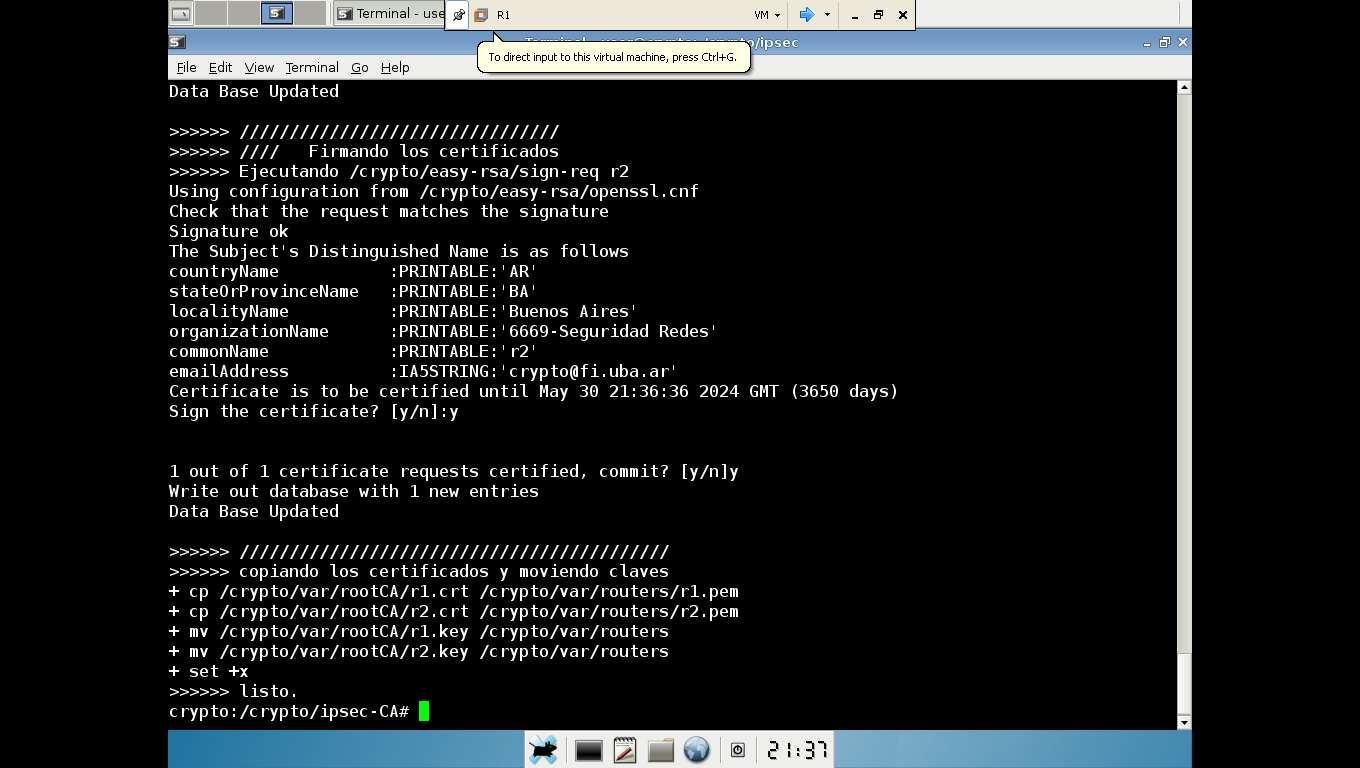
certificado a generar. ( “01”)

* index.txt, Se genera vació. Luego se va incorporando el hash y el cn de cada

certificado generado.

* Ca.crt y ca.key, el certificado y clave de la autoridad certificante.
* R1.crt, r1.key el certificado autofirmado de r1, y
* R2.crt, r2.key el certificado del router 2.

De los cuales los dos últimos pares de certificados – claves de R1 y R2 son copiados satisfactoriamente al directorio /crypto/var/routers.



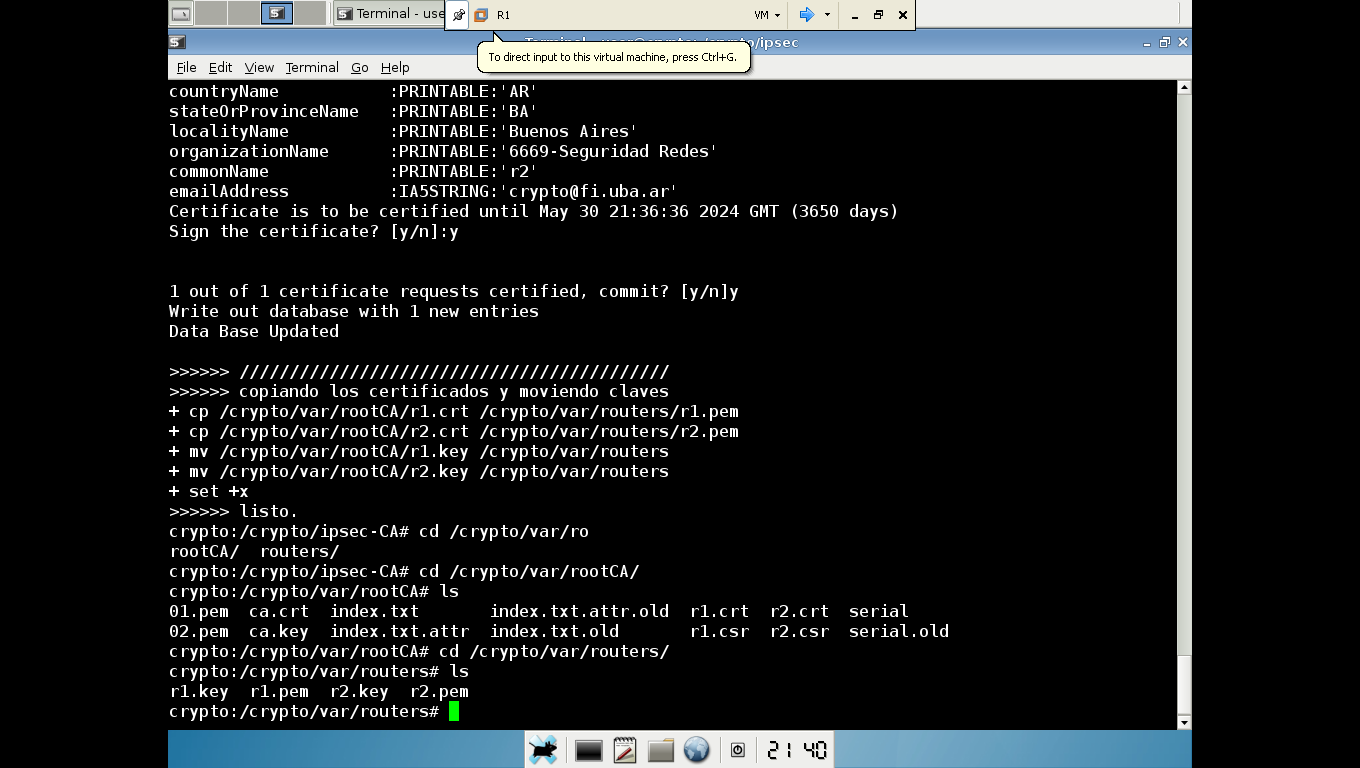


Figura 4: archivos contenidos en los directorios de la CA y en el directorio de los routers.

Figura 3: s03-firmaSolicitudes.sh

Luego verificamos que la lista de certificados revocados está vacía mediante el script s04-generaCRL. (Figura 5).

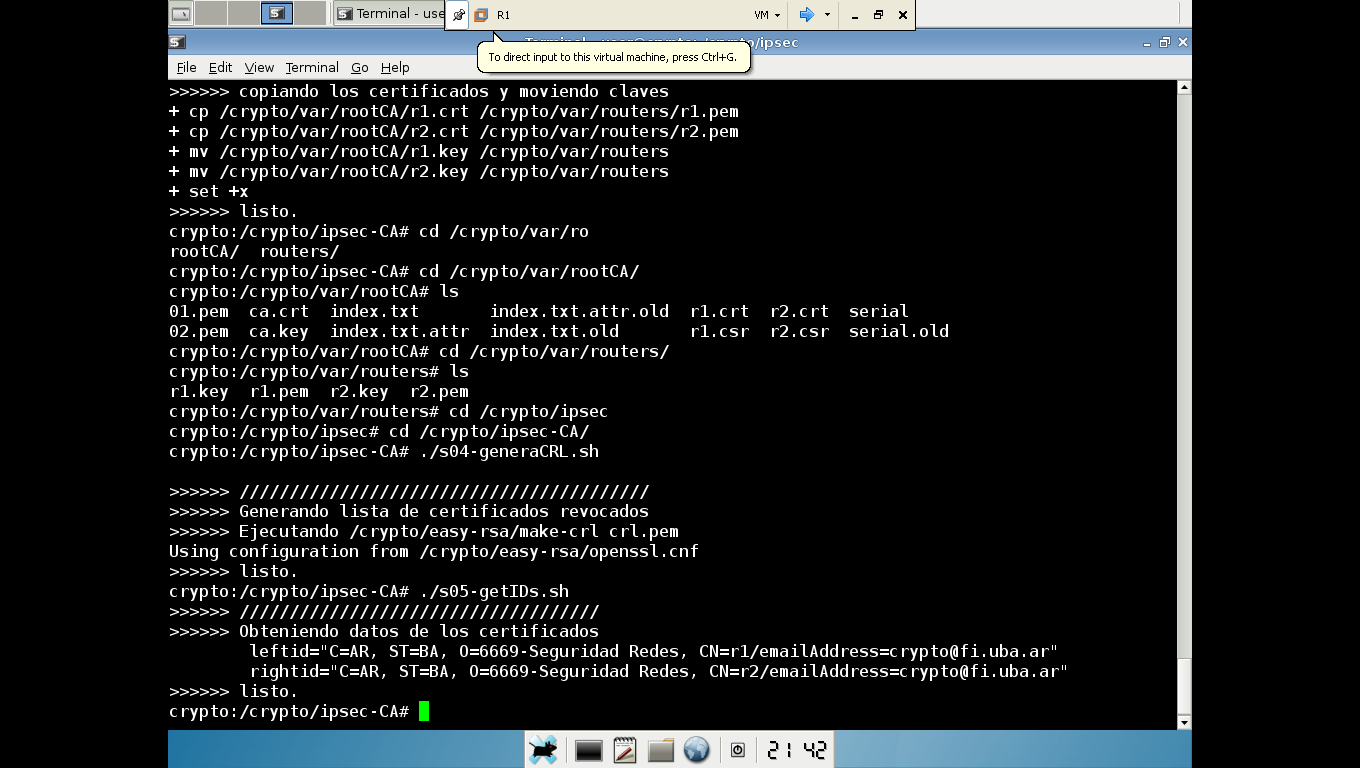


Figura 5: s04-generaCRL.sh

En el paso siguiente, contenido en el script s05-getIDs.sh, se recorren los ficheros de cada certificado, para obtener el nombre de los dueños de los certificados. Esto se hizo con el commando grep; se buscó el campo “Subject:” y copió el texto contiguo a esa palabra. dentro de cada certificado. Esta información se guardó en las variables leftid y rightid, y se guardó en el archivo “ids”, para ser usado posteriormente en la configuración del enlace ipsec.

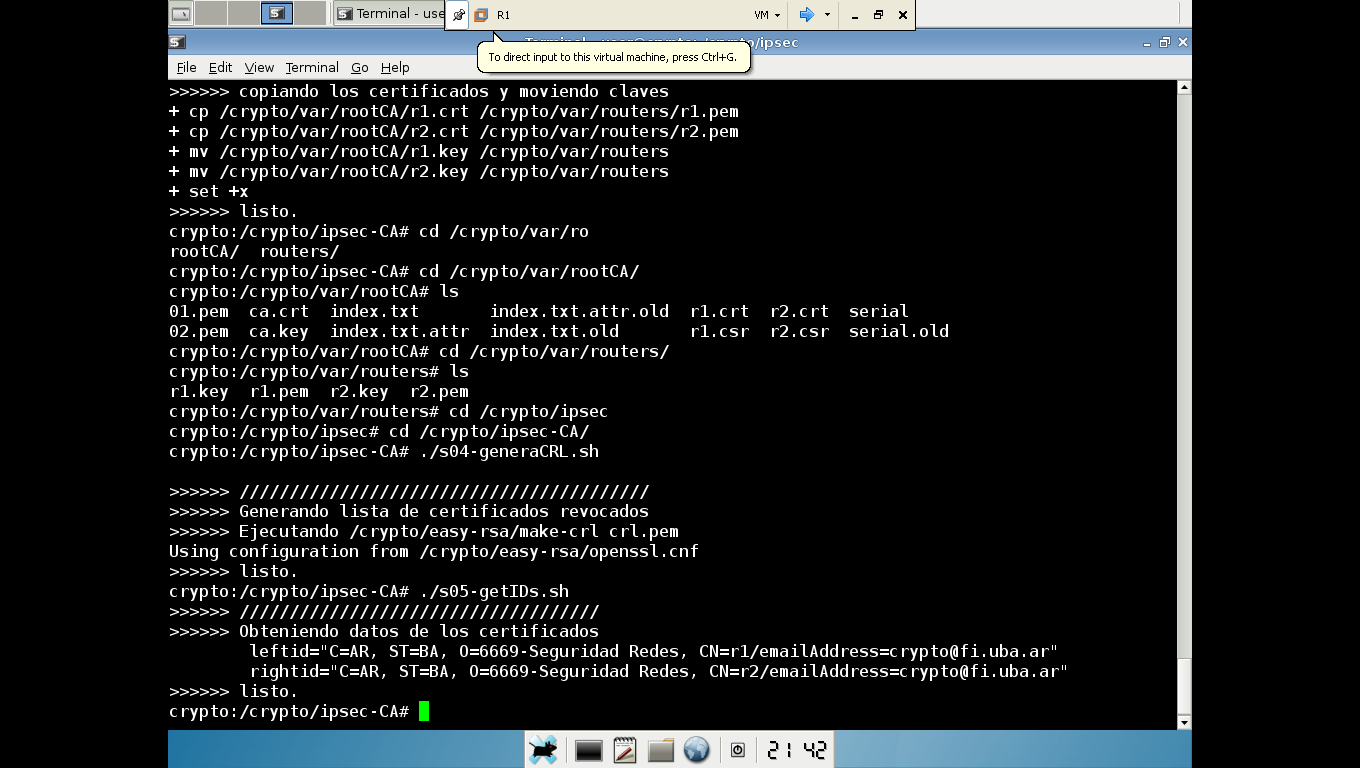


Figura 6: s05-getIDs.sh

B-Configuración enlace IPSec

Primero se configuraron las interfaces del equipo1 con el comando *ifconfig*, donde reside la autoridad certificante (Figura 7).

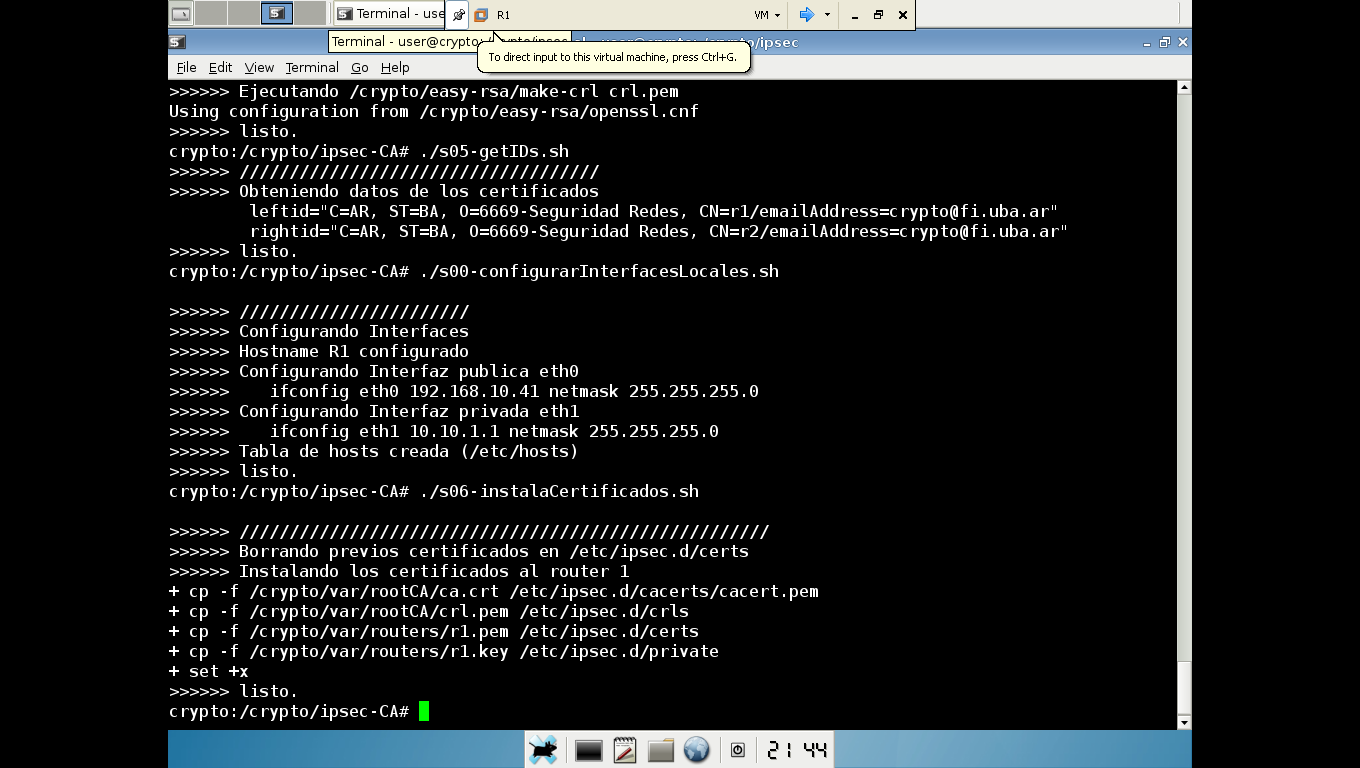


Figura 7: s00-configurarInterfacesLocales.sh

Luego se copiaron los certificados del router 1, de la autoridad certificante y la lista de certificados revocados (hasta el momento vacía) para que sean utilizados por el programa freesWan en el establecimiento del enlace IPSec (Figura 8).

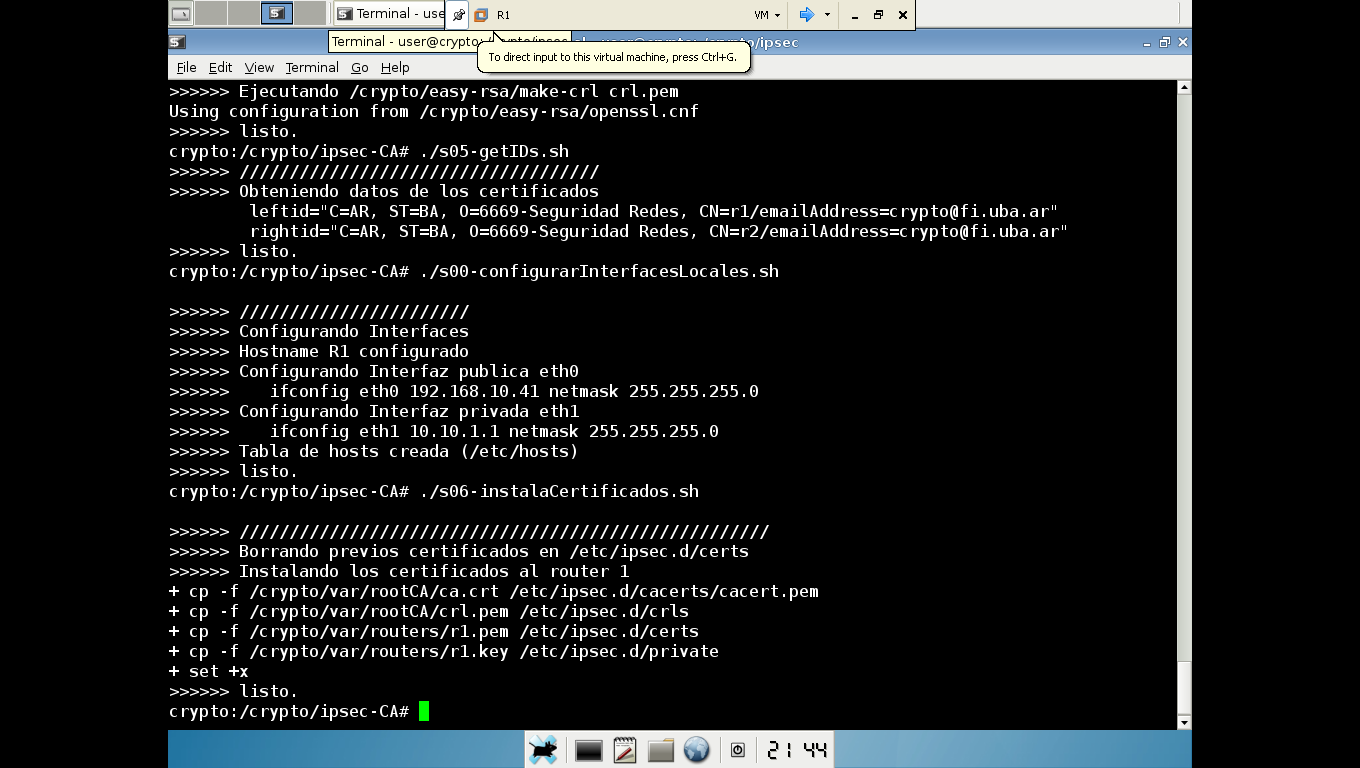
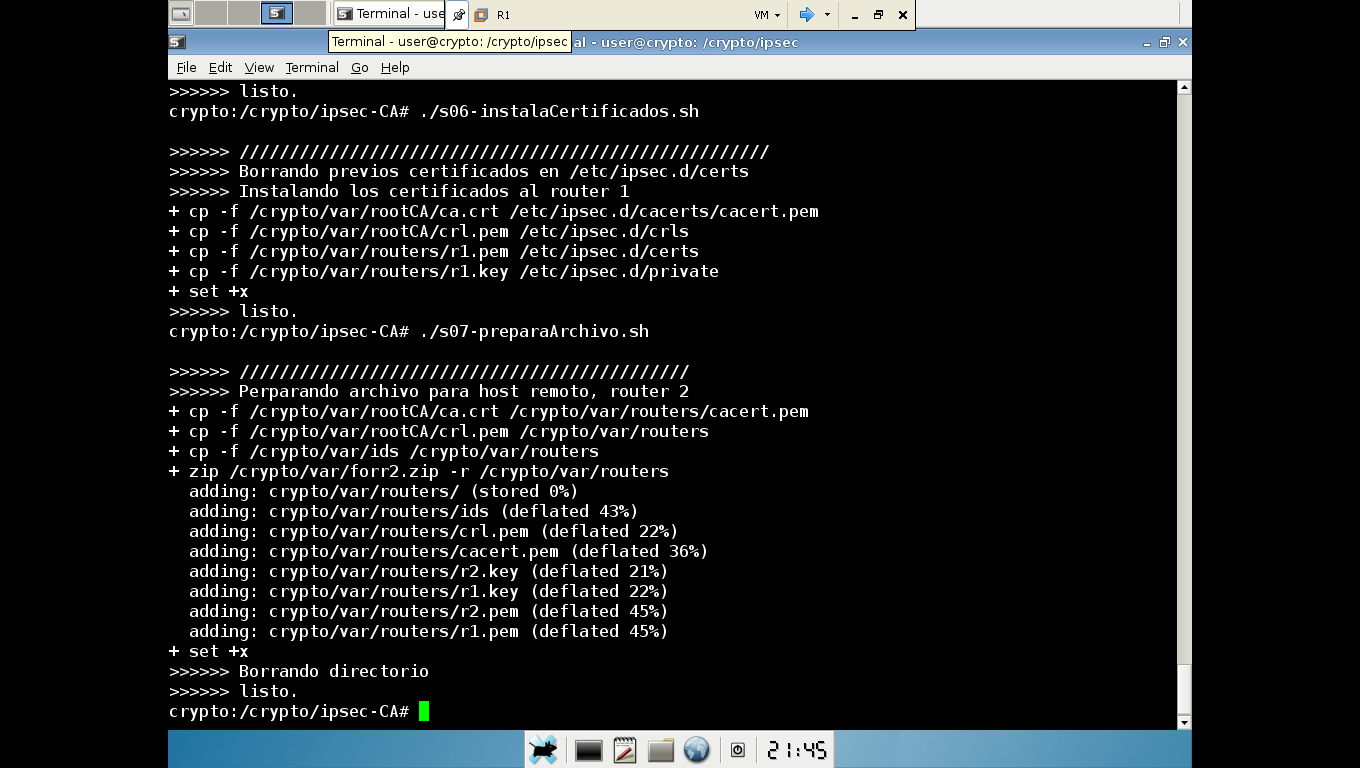


Figura 8: s06-instalaCertificados.sh

En la figura 9 se preparan todos los archivos necesarios para que R2 obtenga su certificado remotamente. Estos archivos son los siguientes:

* Clave y certificado de R1 y R2,
* Listado de los dueños de los certificados,
* Lista de certificados revocados, y
* Certificado de la autoridad certificante.

Se comprimen los archivos en un zip a fin de facilitar su copiado desde R2.



En la figura 10 se ve el resultado de la configuración de las interfaces para R2, con el comando ifconfig.

Figura 9: s07-preparaArchivo.sh

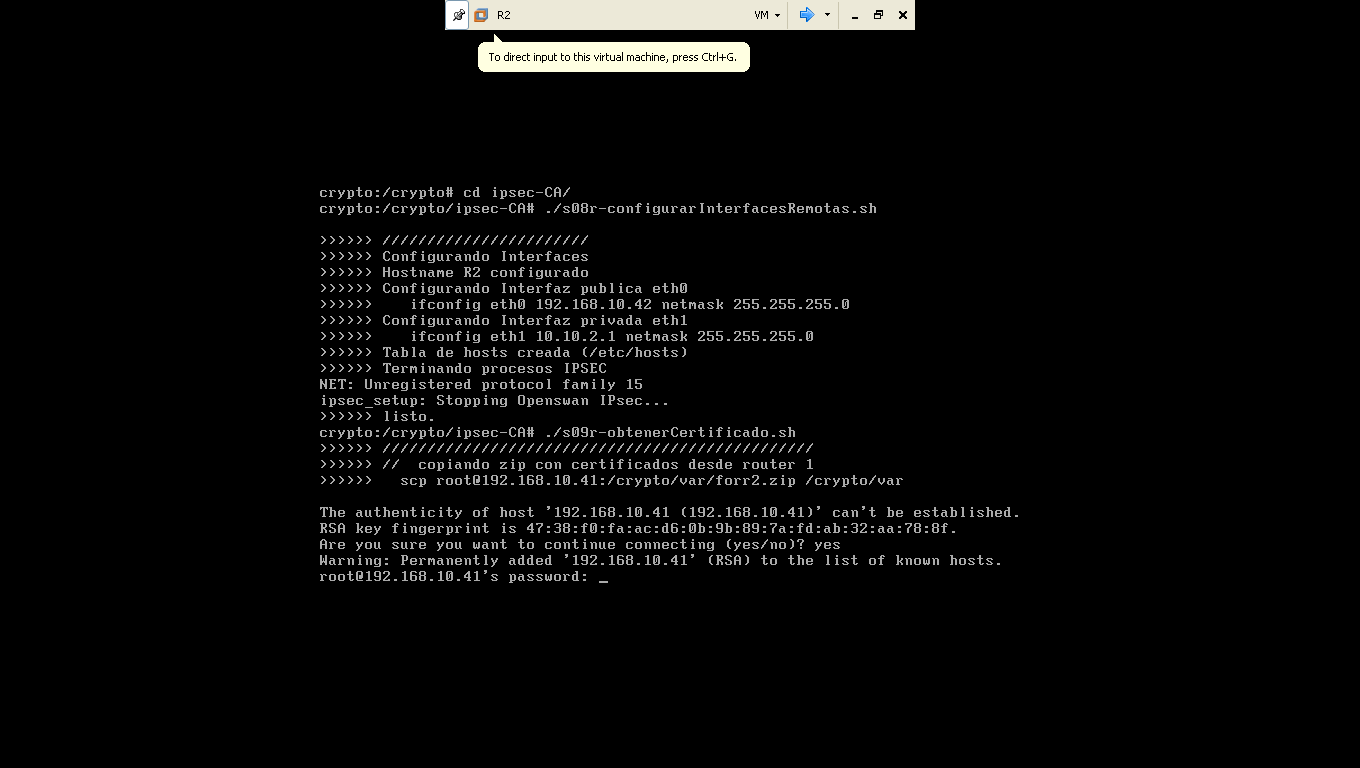
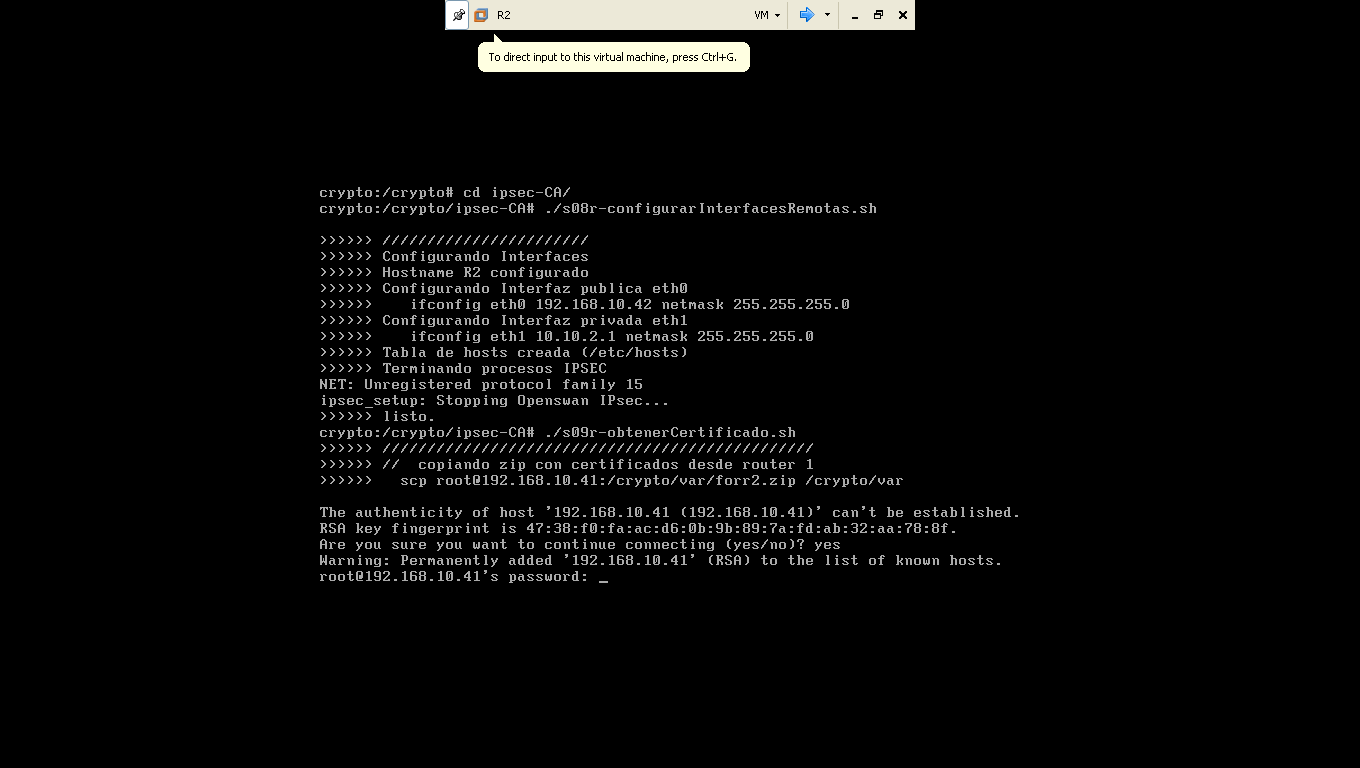


Figura 10: s08r-configurarInterfacesRemotas.sh

Una vez configurada la interfaz de R2, se realiza la copia del archivo zip con los certificados, y los instala en las ubicaciones correspondientes. Para ello, se utilizó el comando SecureCopy (scp, que permite que puedan copiarse archivos entre diferentes host, utilizando transferencia de datos por ssh). Ver Figura 11.



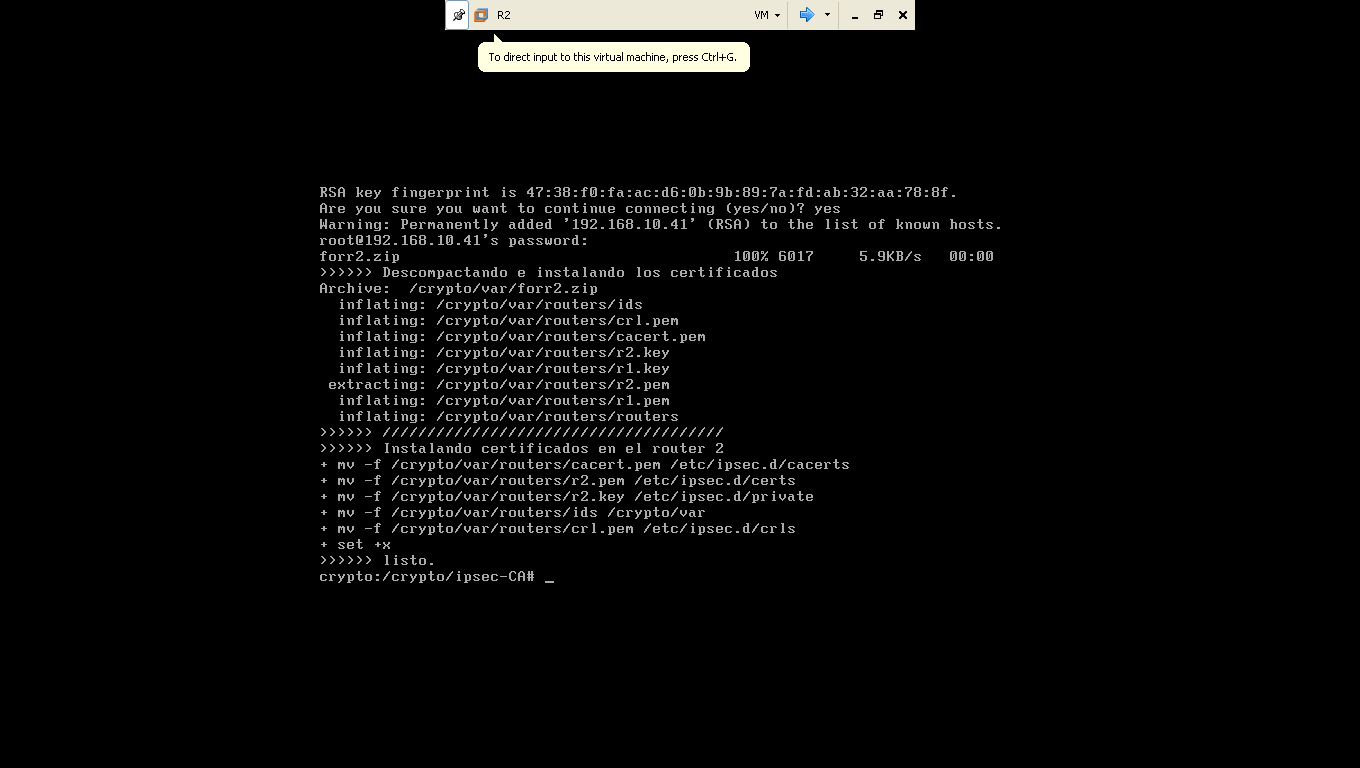


Figura 11: s09-obtenerCertificado.sh

Una vez configuradas las interfaces e instalados los certificados en ambos equipos, el paso siguiente es configurar el enlace IPSec, creando y completando el fichero /etc/ipsec.conf, en cada uno de los equipos (R1 y R2). Para ello, se ejecutó el script 10 (Figura 12). Analizando el código de dicho script, se nota que el empleo de certificados está dado por los campos leftrsasigkey y rightrsasigkey donde se introdujo el valor %cert, el cual indica que las claves públicas utilizadas se cargan desde certificados (cuya ubicación está dada por leftcert y rightcert, respectivamente).

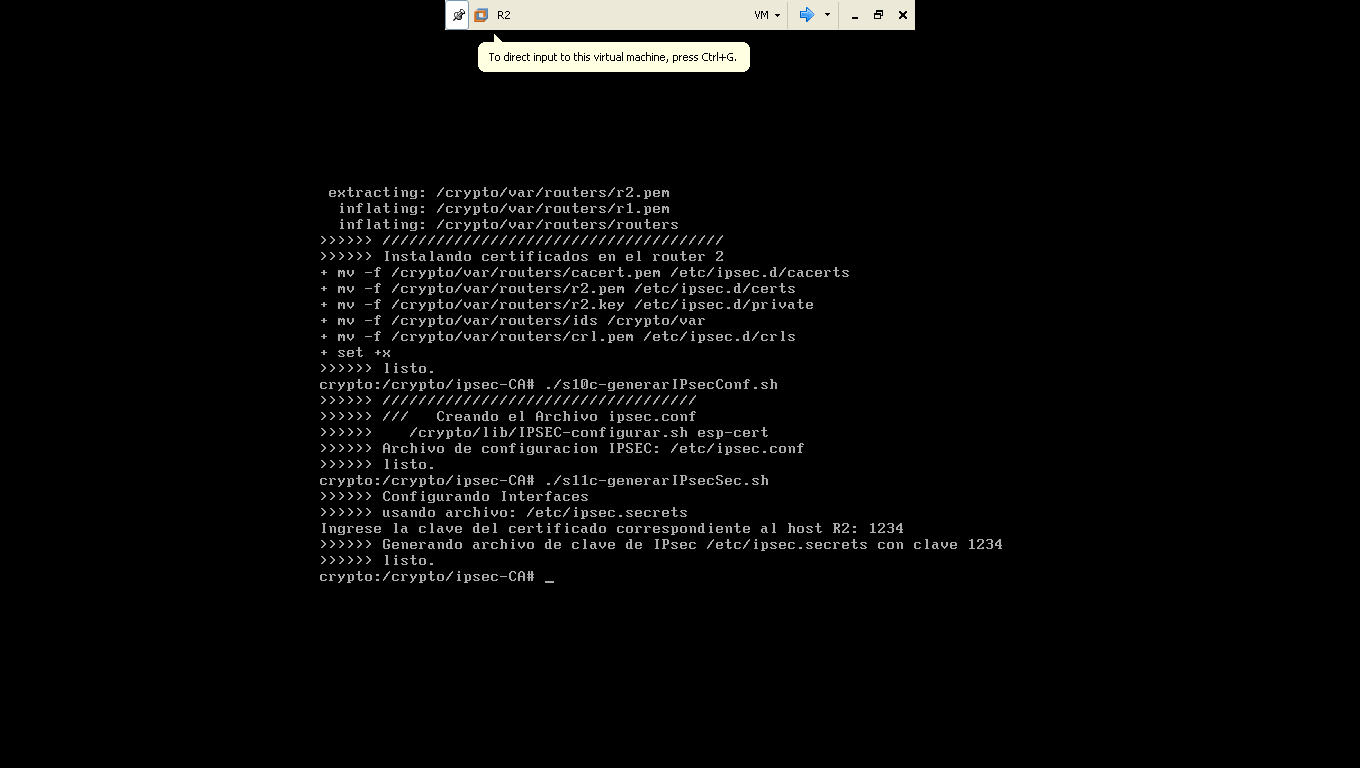


Figura 12: s10c-generarIPsecConf.sh

Por último, con el script s11c-generarIPsecSec.sh (Figura 13), se genera el archivo donde se guarda la clave necesaria para decodificar la clave privada de cada respectivo equipo.

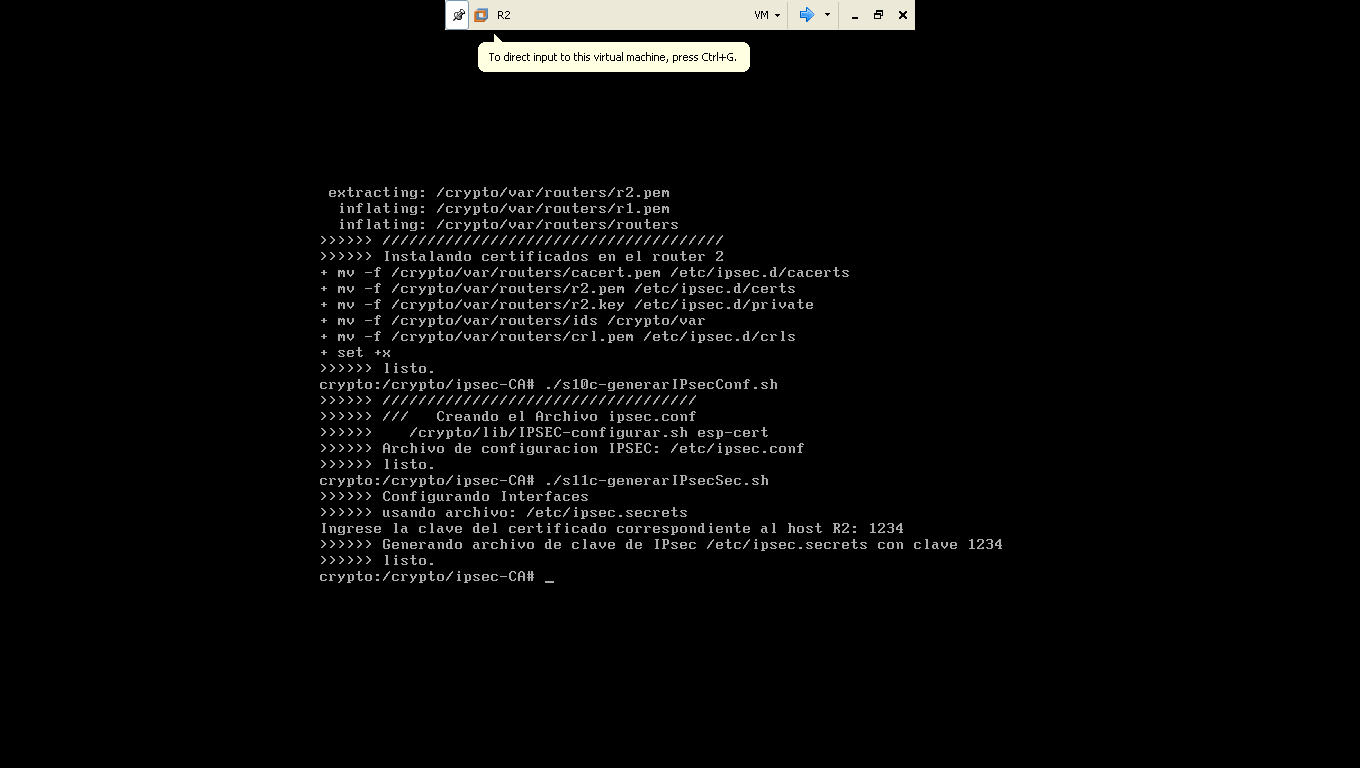


Figura 13: s11c-generarIPsecSec.sh

Una vez realizado esto, se puede iniciar el servicio IPSec en ambos routers, con el comando

**/etc/init.d/ipsec start**

Y el túnel se levanta desde alguno de los routers con el comando:

**ipsec auto --up crypto**

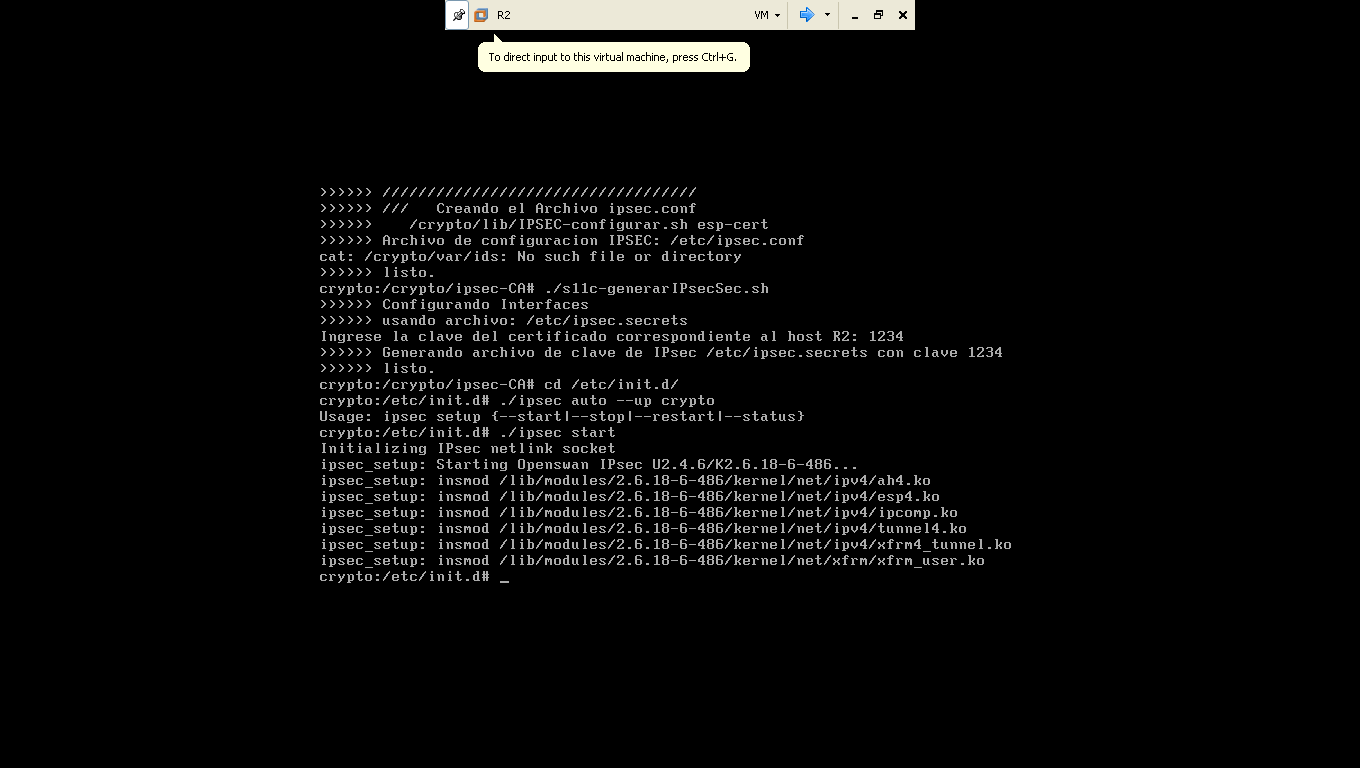


Figura 14: Ipsec start

**3- Anulación de uno de los certificados.**

En esta etapa se ejecutó en R1 el script que revoca el certificado local e instala la nueva lista de certificados revocados (Figura 15). Luego se actualiza la nueva lista de certificados revocados (CRL) en R2 (Figura 16). Nuevamente, para realizar esta actualización se utiliza el comando secure copy (scp).



Figura 15: srs0-revocarR1.sh en R1

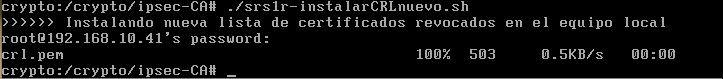


Figura 16: srs1r-instalarCRLnuevo.sh en R2

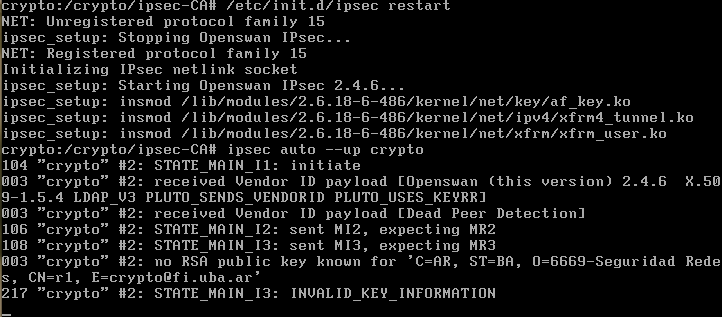
Ahora, a modo de test, se reinició el túnel e intentó levantar con el certificado revocado en R1, con lo que se verificó que surgió un error de clave: El router 2 está rechazando el certificado.

Figura 17: Intento de establecimiento del tunel con el certificado de R1 revocado.

**4- Emisión de un nuevo certificado**

Luego se generó el nuevo certificado y se levantó la conexión mediante el túnel, como lo indica la Figura 18 a y b.

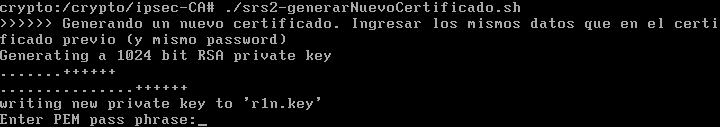


Figura 18a: Generación de nuevo certificado de R1 y establecimiento del tunel.

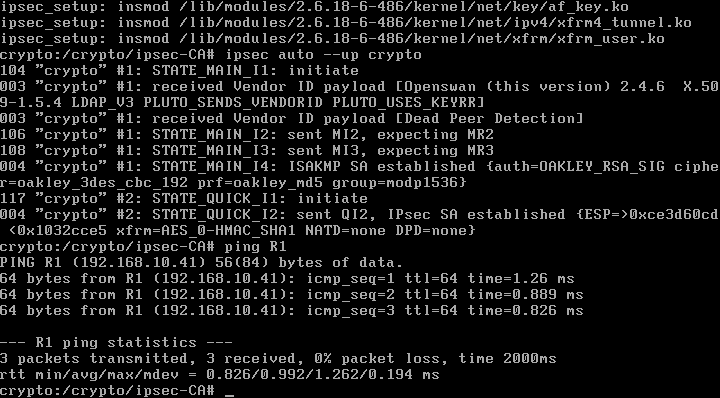


Figura 18b: Generación de nuevo certificado de R1 y establecimiento del tunel.