Universidad de Buenos Aires
Facultad de Ingeniería

66.69 – Criptografía y Seguridad Informática

"Ipsec"

Objetivo del Trabajo Práctico

El presente trabajo práctico consistirá en configurar un tunel Ipsec entre dos PCs funcionando como routers y analizar, utilizando el analizador de protocolos, el tráfico generado por ambos equipos. Se utilizará para tal fin la distribución de Linux provista por la cátedra.

Esquema a armar

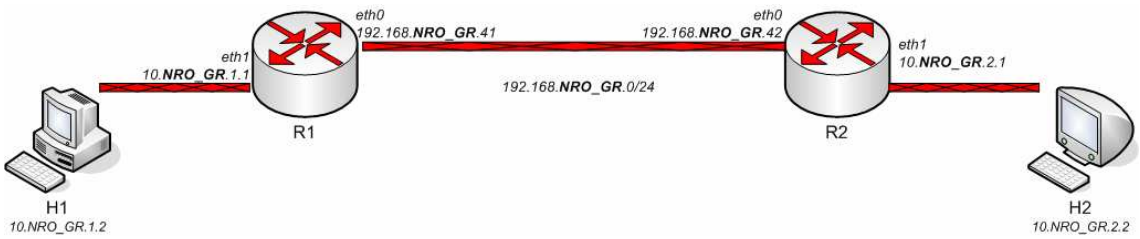


Fig. 1 – Maqueta a Implementar

Pasos para la configuración (Ver notas de implementación)

1) Iniciar al menos 4 PC con el CD de LINUX provisto

2) Configuración de los equipos R1 y R2.

Nota: leer Notas de implementación al final del documento.

a. Verificar archivo de parámetros de configuración (/crypto/conf/config.sh)
   - Modificar el parámetro de número de grupo. Los ejemplos de configuración corresponden al grupo número 1. (**ver nota 1**).
   - Verificar que el tipo de tunel es "esp-rsa"

b. Configuración de R1 (R1-1-preparar.sh)
   - El script realizara los siguientes pasos:
     - hostname R1
     - ifconfig eth0 **192.168.NRO_GR.41 netmask 255.255.255.0**
     - ifconfig eth1 **10. NRO_GR.1.1 netmask 255.255.255.0**
     - Modificar archivo /etc/hosts
       - 127.0.0.1 localhost
       - 192.168.NRO_GR.41 R1
       - 192.168.NRO_GR.42 R2

c. Configuración de R2 (R2-1-preparar.sh)
- El script realizara los siguientes pasos:
  - hostname R2
  - ifconfig eth0 **192.168.NRO_GR.42 netmask 255.255.255.0**
  - ifconfig eth1 **10. NRO_GR.2.1 netmask 255.255.255.0**
  - Modificar archivo /etc/hosts
    - 127.0.0.1 localhost
    - 192.168.**NRO_GR**.41 R1
    - 192.168.**NRO_GR**.42 R2

3) Configuración de los Host

a. Configuración H1 (H1-preparar.sh)
- El script realizara los siguientes pasos:
  - hostname H1
  - ifconfig eth0 10. **NRO_GR**.1.2 netmask 255.255.255.0
  - Agrega ruta a la red 10. **NRO_GR**.1.1 por medio de R1
  - Agregar el host H2 al /etc/hosts

b. Configuración H2 (H2-preparar.sh)
- El script realizara los siguientes pasos:
  - hostname H2
  - ifconfig eth0 10. **NRO_GR**.2.2 netmask 255.255.255.0
  - Agrega ruta a la red 10. **NRO_GR**.2.1 por medio de R2
  - Agregar el host H1 al /etc/hosts

4) Verificar la red

a. Ping de H1 a R1
b. Ping de H2 a R2
c. Ping de R1 a R2

5) Generar claves IPSEC

a. R1 (R1-2-generarclaves.sh)
- El script genera el par de claves RSA. Con los siguientes pasos:
  - ipsec newhostkey --output /etc/ipsec.secrets --hostname R1
  - ipsec showhostkey --left > /tmp/left.key

b. R2 (R2-2generarclaves.sh)
- El script genera el par de claves RSA . Con los siguientes pasos:
  - ipsec newhostkey --output /etc/ipsec.secrets --hostname R2
  - ipsec showhostkey --right > /tmp/right.key

6) Obtener clave IPSEC del equipo remoto

a. R1 (R1-3-obtenerclaveremota.sh)
- El script realizara los siguientes pasos:
  - scp root@R2:/tmp/right.key /tmp/right.key

b. R2 (R2-3-obtenerclaveremota.sh)
- El script realizara los siguientes pasos:
  - scp root@R1:/tmp/left.key /tmp/left.key

7) Configurar IPSEC

   a. R1 (R1-4-configurar.sh)
      - El script generará el archivo /etc/ipsec.conf
      - Inicia de servicio IPSEC
   b. R2 (R2-4-configurar.sh)
      - El script generará el archivo /etc/ipsec.conf
      - Inicia de servicio IPSEC

8) Iniciar el enlace IPSEC

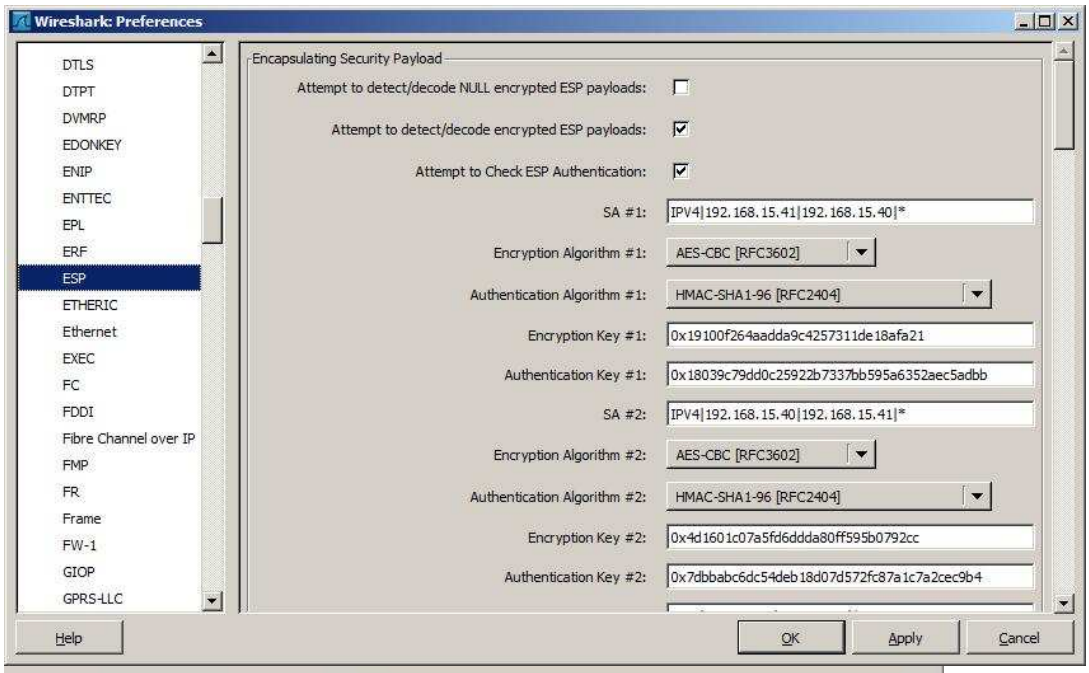
   a. R1 o R2 (iniciarenlace.sh)
      - El script realizara los siguientes pasos:
        - ipsec auto --up crypto

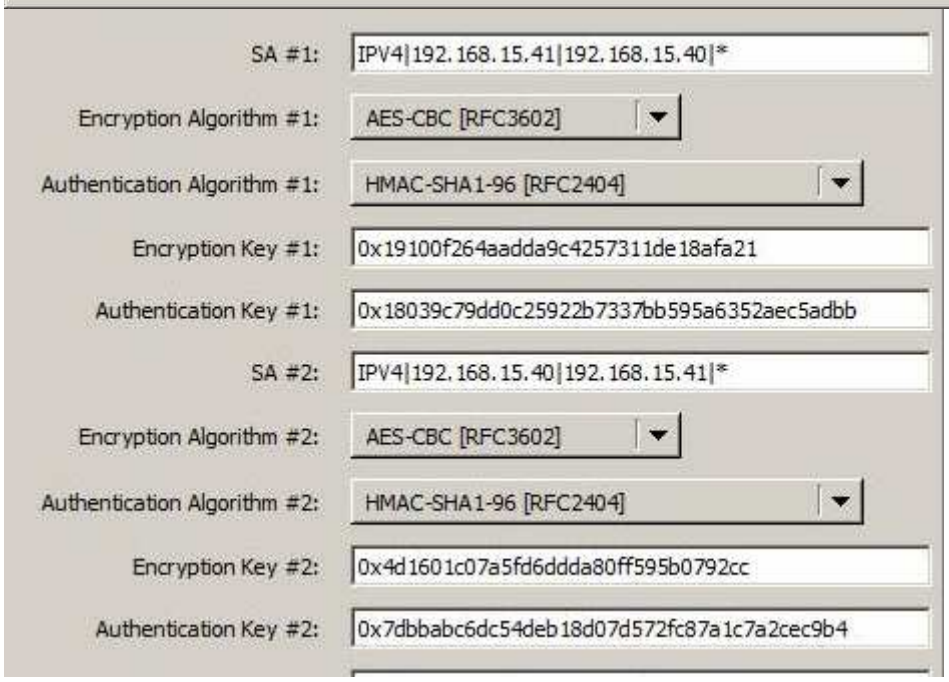
9) Verificación del túnel

   a. Ejecutar *route* y verificar que existan la rutas a las redes privadas conectadas al otro equipo. En R1, se debe visualizar una ruta a 10. **NRO_GR**.2.0. En R2, a 10. **NRO_GR**.1.0
   b. Hacer ping de H1 a H2 y de H2 a H1
   c. Capturar de en R1 o R2 el trafico en eth0 y en ipsec0. Que se observa?

10) Captura del protocolo
   a. Bajar la conexión
   b. Iniciar wireshark en uno de los routers
   c. Iniciar la captura en eth0
   d. Levantar la conexión
   e. Una vez establecida finalizar la captura.
   f. Cuantas fases se ejecutan?
   g. Que se intercambian en cada fase?
   h. Con que algoritmos encripta?
   i. Que modo es el tunel?

11) Desencriptar tráfico
   a. Con el túnel iniciado ejecutar en R1 setkey –D
   b. Obtener las claves de Autenticación y Encripcion y completarlas como se ve en la figura





- El SA #1 se debe poner como ipv4|ip_src|ip_dst|*

a. Iniciar una captura en el canal cifrado.
b. Hacer Ping de H1 a H2.
c. Finalizar la captura
d. Confirmar el funcionamiento al lograr ver el ping descifrado.
e. Reiniciar el tunel y ejecutar nuevamente del paso a al d.
f. Se puede descifrar la captura con el Wireshark en este caso? A que se debe?

12) Variantes (OPCIONAL)
   a. Ejecutar el punto 5 con el modo ah
   b. Hacer el punto 8 nuevamente
   c. Cambiar el archivo ipsec.conf e ipsec.secrets para usar Pre Shared Key
   d. Hacer el punto 8 nuevamente.

Resumen – Comandos útiles, Archivos y su Descripción

	DESCRIPCION	
Comandos	Inicio IPSEC: Detener IPSEC: Reiniciar IPSEC: Iniciar tunel: Detener unnel Ver rutas equipo: Teclado castellano: Debug: Para ver la SA Database Para ver la SPD	/etc/init.d/ipsec unne /etc/init.d/ipsec stop /etc/init.d/ipsec restart ipsec auto –up crypto ipsec auto –down crypto route loadkeys es ipsec look setkey –D setkey –DP
Archivos de sistema	Listado de hosts: Configuración IPSEC: Claves IPSEC:	/etc/hosts /etc/ipsec.conf /etc/ipsec.secrets
Archivos de configuración (scripts)	Configuración completa R1: Configuración completa R2: Configuración básica R1: Configuración básica R2: Creación de claves IPSEC R1: Creación de claves IPSEC R2: Copiado de claves IPSEC R1: Copiado de claves IPSEC R2: Configuración IPSEC R1: Configuración IPSEC R2: Variables de configuración: Iniciar tunel:	R1-0-router.sh R2-0-router.sh R1-1-preparar.sh R2-1-preparar.sh R1-2-generarclaves.sh R2-2-generarclaves.sh R1-3-obtenerclaveremota.sh R2-3-obtenerclaveremota.sh R1-4-configurar.sh R2-4-configurar.sh /crypto/conf/config.sh iniciarenlace.sh

Principales comandos de linux

COMANDO	DESCRIPCION
Hostname	Configura el nombre de host del equipo.
Ifconfig	Permite configurar distintos aspectos de la placa de red. Para mayor detalle ejecutar el comando **“man ifconfig”.**
Route	Permite configurar y manipular la tabla de ruteo del sistema operativo. Para mayor detalle ejecutar el comando **“man route”**.
Scp	Este comando se utiliza para realizar copias de archivos de un host al otro en forma segura. Esto involucra un proceso de autenticación y encriptado de los datos transferidos. Ver **“man scp”** y **“man Ssh”.**
tcpdump	Para capturar paquetes en una interfaz determinada

Notas de implementación

Los scripts pueden ser configurados modificando el archivo /crypto/conf/config.sh

Se debe tener en cuenta que esta práctica se puede realizar de dos maneras:

1. Editar el archivo de configuración en cada router.
2. Ejecutar en cada router el script Rx-0-router.sh. Este script ejecutar todos los pasos intermedios automaticamente. Una vez finalizado se deberá ejecutar el script iniciarenlace.sh en uno de los routers.

O de la siguiente manera

1. Editar el archivo de configuración en cada router.
2. Ejecutar en cada router los scripts numerados según Rx-n-xxxx.sh. El numero n es el orden en que se deben ejecutar dichos scripts. Al final se deberá ejecutar el archivo iniciarenlace.sh en uno de los routers.

Nota 1:
Si se desea implementar más de una maqueta al mismo tiempo, deberán asignarle a cada una un número distinto en la variable GRUPO del archivo de configuración.