

# Trabajo Práctico 3 - IPSec sin Certificados



Integrantes:

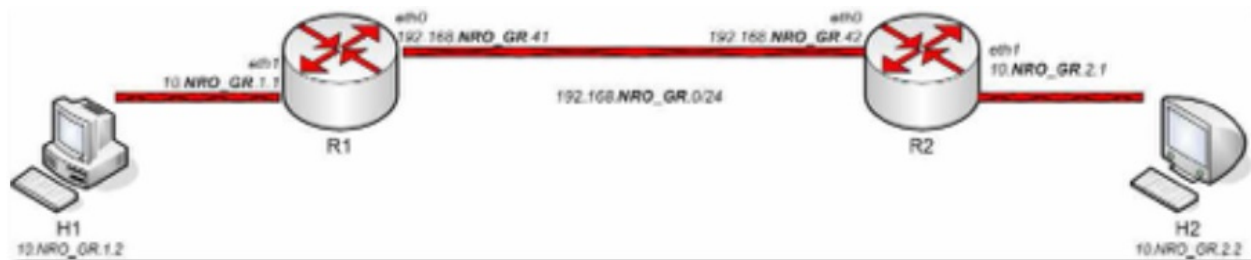
Madariaga, Eduardo	90824	madariagaedu@gmail.com
Canavari, Agustín	91599	agustincanavari@gmail.cm
López Gallo, Marcelo	92563	marce.lopezgallo@gmail.com

## Objetivo del Trabajo Práctico

El presente trabajo práctico consistirá en configurar un túnel Ipsec entre dos routers y analizar el tráfico generado por equipos host conectados a los routers, que actúan como gateways, mediante el analizador de protocolos. Se utilizará para tal fin la distribución de Linux provista por la cátedra y se trabajará con software de virtualización de dispositivos, para lograr que el tráfico generado siempre esté dentro del equipo y no utilice en ningún momento el hardware de red.

## Desarrollo

### Armado del esquema de red



H1: 10.10.1.2

H2: 10.10.2.2

R1: eth0 192.168.10.41, eth1 10.10.1.1

R2: eth0 192.168.10.42, eth1 10.10.2.1

```
crypto:/crypto/ipsec# ./R2-1-preparar.sh
>>>>> Configuración Interfaces para R2 - Inicio
>>>>> Hostname R2 configurado
>>>>> Configurando Interfaz pública eth0
>>>>> ifconfig eth0 192.168.10.42 netmask 255.255.255.0
>>>>> Configurando Interfaz privada eth1
>>>>> ifconfig eth1 10.10.2.1 netmask 255.255.255.0
>>>>> Tabla de hosts creada (/etc/hosts)
>>>>> Configuración Interfaces para R2 - Fin
```

### Verificación de la red:

Una vez configurados los 4 equipos, se realizaron 3 distintos chequeos a nivel red, en la red R1-R2 y en cada red Hx-Rx. En la siguiente figura se muestran los resultados de los ping posibles para R1: de R1 a R2 y de R1 a H1.

```

crypto:/crypto/ipsec# ping 10.10.1.2
PING 10.10.1.2 (10.10.1.2) 56(84) bytes of data.
64 bytes from 10.10.1.2: icmp_seq=1 ttl=64 time=5.48 ns
64 bytes from 10.10.1.2: icmp_seq=2 ttl=64 time=0.280 ns
64 bytes from 10.10.1.2: icmp_seq=3 ttl=64 time=0.186 ns
64 bytes from 10.10.1.2: icmp_seq=4 ttl=64 time=0.400 ns

--- 10.10.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ns
rtt min/avg/max/ndev = 0.186/1.586/5.481/2.250 ns
crypto:/crypto/ipsec# ping 192.168.10.42
PING 192.168.10.42 (192.168.10.42) 56(84) bytes of data.
64 bytes from 192.168.10.42: icmp_seq=1 ttl=64 time=1.97 ns
64 bytes from 192.168.10.42: icmp_seq=2 ttl=64 time=0.232 ns
64 bytes from 192.168.10.42: icmp_seq=3 ttl=64 time=0.174 ns

--- 192.168.10.42 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ns
rtt min/avg/max/ndev = 0.174/0.793/1.973/0.834 ns
crypto:/crypto/ipsec# _

```

## Generación de claves:

Se generó un par de claves (Privada y Pública) para R1 y R2 mediante el algoritmo de RSA para la creación del túnel. La siguiente figura muestra los resultados al aplicarlo en R2:

```

RSA {
# RSA 2192 bits R2 Mon May 26 21:08:49 2014
# for signatures only, UNSAFE FOR ENCRYPTION
# pubkey=0sAQN+2EQRaIrN9MlqUF108KL32XluSc1P2E6YBuHB+Ji8P8nqn3XuhPE7kSpNkL
Un+sWsK/UiLiR5Ip80xMAyUHN5Wfz2a8nbUxfBvKdMonqECn/fryyX7AGxQ6onaxF6dMXttpBdzn5vCz
TXFcz6z2LXX5uYuQIaVP+eDqN0S3uv8gXGD+2W458h66x1NdvdchtyoL0hXu5UFH0kIUPh/cYHPNhNuR
QD9ce22YichAf/QiT73tiGepQlJn0iqv8h0aJA4b09neZglA4V7FClnGzqqESnHUGMELGTFRv85IfJKZ
3TeEG6S/12Y001D3VBdJpU15fJU7LCEUs31NETQTbI2xoSaHtgRnenCT9fia0f1143
Modulus: 0x7ed844116a5acdf5696a505d74f0a2f7d9722e49cd4fd84e9806e1c1f898b
c3fc9ea9f75f084f13b912a4d90b567fac5ac2bf5222e2479229d0ec4c03251637959fcd96bc99b5
717c1bca74ca26a840a7fdaf2c97ec01b143aa266b117a74c5edb6905dce6e6f0b34d715ccc6cf6
2d75f9b90c1021a54ff9e0ea3744b7baff205c60fe656e39f21ebac6535dbdd721b72a0bd215eee5
4147d242143e1fdc6073cd84db91403f5c7b665089c8407ff4224fbded8867a94252663a2aaff21d
1a240e1b3bd9de6602iae18ec5080906ceaa844a71d418c10b193151bfce407c9299dd37841ba4bf
d7660e3b50f7541749a54d797c953b2c2114b379561134136c8db1a12696b6a4667a7093f5f09a39
f940e37
PublicExponent: 0x03
# everything after this point is secret
}
"ipsec.secrets" 15L, 3162C
1,1 Top

```

## Obtención de claves IPsec del equipo remoto:

Una vez generadas las claves, se procedió al copiado de las claves del otro equipo (en cada uno de los Routers), mediante el comando SecureCopy (scp, que permite la copia de archivos entre diferentes host, utilizando transferencia de datos por ssh).

```
crypto:/crypto/ipsec# ./R2-3-obtenerclaveremota.sh
>>>>> Copiado de clave IPSEC de R1 - Inicio
The authenticity of host 'r1 (192.168.10.41)' can't be established.
RSA key fingerprint is 47:38:f8:fa:ac:d6:0b:9b:89:7a:fd:ab:32:aa:78:8f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'r1,192.168.10.41' (RSA) to the list of known hosts.
root@r1's password:
left.key          100% 435      0.4KB/s   00:00
>>>>> Clave IPSEC de R1 copiada
>>>>> Copiado de clave IPSEC de R1 - Fin
crypto:/crypto/ipsec# _
```

## Configuración e iniciación del enlace IPsec y verificación del túnel:

Se inicio el enlace mediante la utilización del script “inciarenlace.sh”

```
/etc/init.d/ipsec restart
NET: Unregistered protocol family 15
ipsec_setup: Stopping Openswan IPsec...
NET: Registered protocol family 15
Initializing IPsec netlink socket
ipsec_setup: Starting Openswan IPsec 2.4.6...
ipsec_setup: insmod /lib/modules/2.6.18-6-486/kernel/net/key/af_key.ko
ipsec_setup: insmod /lib/modules/2.6.18-6-486/kernel/net/ipv4/xfrn4_tunnel.ko
ipsec_setup: insmod /lib/modules/2.6.18-6-486/kernel/net/xfrn/xfrn_user.ko
>>>>> Esperando...
>>>>> Estableciendo conexion...
ipsec auto --up crypto
104 "crypto" #1: STATE_MAIN_I1: initiate
003 "crypto" #1: received Vendor ID payload [Openswan (this version) 2.4.6 X.509-1.5.4 LDAP_V3 PLUTO SENDS_VENDORID PLUTO_USES_KEYRR]
003 "crypto" #1: received Vendor ID payload [Dead Peer Detection]
106 "crypto" #1: STATE_MAIN_I2: sent MI2, expecting MR2
108 "crypto" #1: STATE_MAIN_I3: sent MI3, expecting MR3
004 "crypto" #1: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_RSA_SIG cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp1536}
117 "crypto" #2: STATE_QUICK_I1: initiate
004 "crypto" #2: STATE_QUICK_I2: sent QI2, IPsec SA established {ESP->0x9aee3c7f<0x2db90417 xfrn=AES_0-HMAC_SHA1 NATD=none DPD=none}
>>>>> Establecimiento de conexion IPSEC - Fin
crypto:/crypto/ipsec# _
```

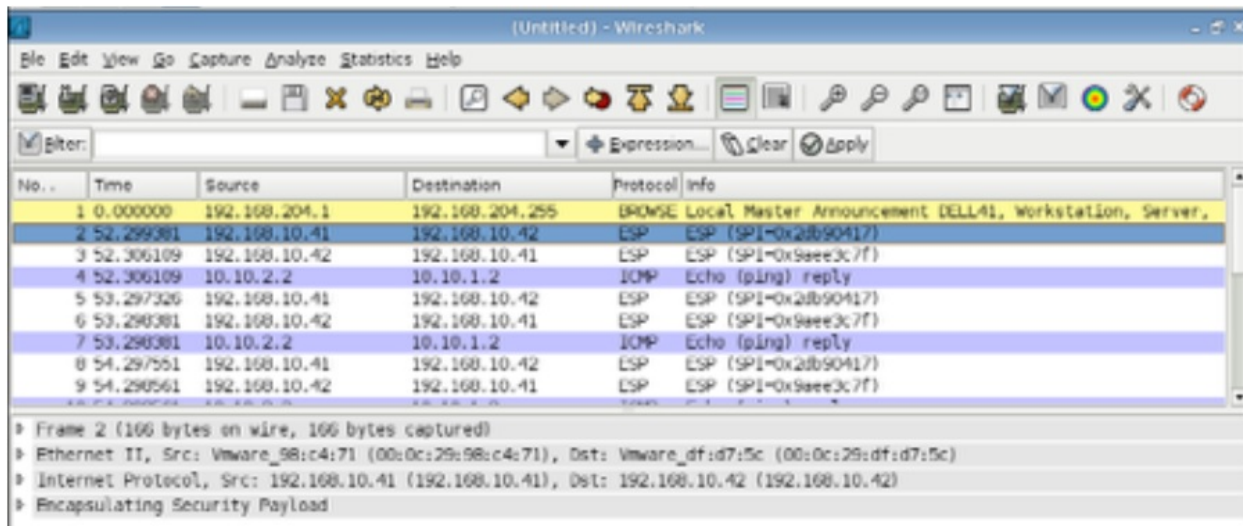
Una vez iniciado el enlace comenzó a haber conectividad entre ambos terminales. Se realizó un ping para verificar la conexión

```
crypto:/crypto/ipsec# route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.2.0        *              255.255.255.0   U      0      0      0 eth0
10.10.1.0        R2             255.255.255.0   UC     0      0      0 eth0
crypto:/crypto/ipsec# ping 10.10.1.2
PING 10.10.1.2 (10.10.1.2) 56(84) bytes of data.
64 bytes from 10.10.1.2: icmp_seq=1 ttl=62 time=17.8 ns
64 bytes from 10.10.1.2: icmp_seq=2 ttl=62 time=0.941 ns
64 bytes from 10.10.1.2: icmp_seq=3 ttl=62 time=0.508 ns
64 bytes from 10.10.1.2: icmp_seq=4 ttl=62 time=0.631 ns
64 bytes from 10.10.1.2: icmp_seq=5 ttl=62 time=0.518 ns
64 bytes from 10.10.1.2: icmp_seq=6 ttl=62 time=0.589 ns
^C64 bytes from 10.10.1.2: icmp_seq=7 ttl=62 time=0.495 ns
64 bytes from 10.10.1.2: icmp_seq=8 ttl=62 time=0.569 ns
64 bytes from 10.10.1.2: icmp_seq=9 ttl=62 time=0.511 ns
64 bytes from 10.10.1.2: icmp_seq=10 ttl=62 time=0.555 ns
```

## Captura del protocolo:

En la próxima figura, una captura del programa wireshark que muestra los paquetes transmitidos con el túnel habilitado y realizando una solicitud ping desde uno de los hosts.

Como puede verificarse, la información está encriptada y solo pueden visualizarse las cabeceras ESP de los paquetes.



## Desencriptado del tráfico transmitido:

Para realizar el desencriptado, se utilizó el comando Setkey -D, el cual muestra todos los parámetros utilizados tanto para el encriptado como para la autenticación en ambos sentidos de la comunicación. Nótese que en un sentido de la comunicación, se utiliza una clave simétrica AES-CBC, mientras que en el otro sentido, la clave es totalmente distinta. Esto obliga a que un ataque del tipo man in the middle deba vulnerar la seguridad tanto en un sentido como en el otro la comunicación. Esta información de claves se introdujo posteriormente en la configuración del protocolo ESP en Wireshark y como era de esperarse, se observó toda la información transmitida y desencriptada, aprovechando que Wireshark da la posibilidad de ingresar estos datos para analizar la seguridad de un protocolo.

```
hl:/crypto/ipsec# setkey -D
192.168.10.42 192.168.10.41
    esp mode=tunnel spi=2113298487(0x7df66037) reqid=16385(0x00004001)
    E: aes-cbc e864c2cc 5b3be727 5ced3098 4c7069c5
    A: hmac-sha1 bca0f1c9 8f4132a8 78f3dd88 2727a3f3 b614aece
    seq=0x00000000 replay=32 flags=0x00000000 state=mature
    created: May 26 21:35:03 2014    current: May 26 21:43:52 2014
    diff: 529(s)    hard: 0(s)    soft: 0(s)
    last:
    current: 0(bytes)    hard: 0(s)    soft: 0(s)
    allocated: 0    hard: 0 soft: 0
    sadb_seq=1 pid=5180 refcnt=0
192.168.10.41 192.168.10.42
    esp mode=tunnel spi=3208298319(0xbf3abf4f) reqid=16385(0x00004001)
    E: aes-cbc 48b20d22 f404ac15 6113aa61 092165c2
    A: hmac-sha1 816bec77 789093c0 83934a72 8f271218 22913547
    seq=0x00000000 replay=32 flags=0x00000000 state=mature
    created: May 26 21:35:03 2014    current: May 26 21:43:52 2014
    diff: 529(s)    hard: 0(s)    soft: 0(s)
    last:
    current: 0(bytes)    hard: 0(s)    soft: 0(s)
    allocated: 0    hard: 0 soft: 0
    sadb_seq=0 pid=5180 refcnt=0
```

Wireshark 1.10.7 - 11e-RingH2 [Wireshark 1.10.7 - 60931a1 from master-1.10]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **esp** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000000	10.10.1.2	10.10.2.2	ICMP	166	Echo (ping) request id=0xb013, seq=1/256, ttl=63 (reply in 4)
4	0.003931	10.10.2.2	10.10.1.2	ICMP	166	Echo (ping) reply id=0xb013, seq=1/256, ttl=63 (request in 3)
6	0.993675	10.10.1.2	10.10.2.2	ICMP	166	Echo (ping) request id=0xb013, seq=2/512, ttl=63 (reply in 7)
7	0.994786	10.10.2.2	10.10.1.2	ICMP	166	Echo (ping) reply id=0xb013, seq=2/512, ttl=63 (request in 6)

Frame 3: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0

Ethernet II, Src: VMware\_98:c4:71 (00:0c:29:98:c4:71), Dst: VMware\_df:d7:5c (00:0c:29:df:d7:5c)

Internet Protocol Version 4, Src: 192.168.10.41 (192.168.10.41), Dst: 192.168.10.42 (192.168.10.42)

Encapsulating Security Payload

ESP SPI: 0x13ed37ff (334313471)

ESP Sequence: 1

ESP IV: 47971877f58f096a37c8872e41453eab

Pad

ESP Pad Length: 10

Next header: IP (0xb0)

Authentication Data (correct)

Good: True

Bad: False

Internet Protocol Version 4, Src: 10.10.1.2 (10.10.1.2), Dst: 10.10.2.2 (10.10.2.2)

Internet Control Message Protocol

Frame (166 bytes) | Decrypted Data (108 bytes)

Frame (frame), 166 bytes

Packets: 13 - Displayed: 6 (46.2%) - Load time: 0:00:005

ESP SAs: Edit - Profile: Default

Protocol: **IPv4**

Src IP: **192.168.10.41**

Dest IP: **192.168.10.42**

SPI: **0x13ed37ff**

Encryption: **AES-CBC [RFC3602]**

Encryption Key: **0xae2fdb798a0382cee339cbd436be48**

Authentication: **HMAC-SHA-1-96 [RFC2404]**

Authentication Key: **0xe26dc8819ce9a3fbae1167fff7a38d4ce2336678**

**Cancel** **OK**