Seguridad en Redes
Practica 3.5

David Antuña Rodríguez
Javier Carrión García

1 Conexión IPsec de sitio a sitio con clave secreta

Registros del fichero */var/log/daemon.log*

```
xcbc hmac ctr ccm gcm attr kernel-netlink resolve socket-raw farp stroke updown eap-identity eap-aka eap-md5 eap-gtc
    eap-mschapv2 eap-radius eap-tls eap-ttls eap-tnc dhcp led addrblock
Apr 14 13:39:10 debian charon: 00[JOB] spawning 16 worker threads
Apr 14 13:42:16 debian charon: 00[DMN] signal of type SIGINT received. Shutting down
Apr 14 13:42:19 debian charon: 00[DMN] Starting IKEv2 charon daemon (strongSwan 4.5.2)
Apr 14 13:42:19 debian charon: 00[KNL] listening on interfaces:
Apr 14 13:42:19 debian charon: 00[KNL]   eth0
Apr 14 13:42:19 debian charon: 00[KNL]     10.0.2.15
Apr 14 13:42:19 debian charon: 00[KNL]     fe80::a00:27ff:febe:6b91
Apr 14 13:42:19 debian charon: 00[KNL]   eth1
Apr 14 13:42:19 debian charon: 00[KNL]     192.168.1.1
Apr 14 13:42:19 debian charon: 00[KNL]     fe80::a00:27ff:fe66:bfba
Apr 14 13:42:19 debian charon: 00[KNL]   eth2
Apr 14 13:42:19 debian charon: 00[KNL]     192.168.3.1
Apr 14 13:42:19 debian charon: 00[KNL]     fe80::a00:27ff:fe99:5f2b
Apr 14 13:42:19 debian charon: 00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
Apr 14 13:42:19 debian charon: 00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
Apr 14 13:42:19 debian charon: 00[CFG] loading ocsp signer certificates from '/etc/ipsec.d/ocspcerts'
Apr 14 13:42:19 debian charon: 00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
Apr 14 13:42:19 debian charon: 00[CFG] loading crls from '/etc/ipsec.d/crls'
Apr 14 13:42:19 debian charon: 00[CFG] loading secrets from '/etc/ipsec.secrets'
Apr 14 13:42:19 debian charon: 00[CFG] expanding file expression '/var/lib/strongswan/ipsec.secrets.inc' failed
Apr 14 13:42:19 debian charon: 00[CFG]   loaded IKE secret for %any
Apr 14 13:42:19 debian charon: 00[CFG] sql plugin: database URI not set
Apr 14 13:42:19 debian charon: 00[LIB] plugin 'sql': failed to load - sql_plugin_create returned NULL
Apr 14 13:42:19 debian charon: 00[CFG] loaded 0 RADIUS server configurations
Apr 14 13:42:19 debian charon: 00[LIB] plugin 'medsrv' failed to load: /usr/lib/ipsec/plugins/libstrongswan-medsrv.so:
    cannot open shared object file: No such file or directory
Apr 14 13:42:19 debian charon: 00[CFG] mediation client database URI not defined, skipped
Apr 14 13:42:19 debian charon: 00[LIB] plugin 'medcli': failed to load - medcli_plugin_create returned NULL
Apr 14 13:42:19 debian charon: 00[LIB] plugin 'nm' failed to load: /usr/lib/ipsec/plugins/libstrongswan-nm.so: cannot
    open shared object file: No such file or directory
Apr 14 13:42:19 debian charon: 00[CFG] HA config misses local/remote address
Apr 14 13:42:19 debian charon: 00[LIB] plugin 'ha': failed to load - ha_plugin_create returned NULL
Apr 14 13:42:19 debian charon: 00[DMN] loaded plugins: test-vectors curl ldap aes des sha1 sha2 md5 random x509
    revocation constraints pubkey pkcs1 pgp pem openssl fips-prf gmp agent pkcs11 xcbc hmac ctr ccm gcm attr
    kernel-netlink resolve socket-raw farp stroke updown eap-identity eap-aka eap-md5 eap-gtc eap-mschapv2 eap-radius
    eap-tls eap-ttls eap-tnc dhcp led addrblock
Apr 14 13:42:19 debian charon: 00[JOB] spawning 16 worker threads
Apr 14 13:42:19 debian charon: 11[CFG] received stroke: add connection 'secret'
Apr 14 13:42:19 debian charon: 11[CFG] added configuration 'secret'
Apr 14 13:43:54 debian charon: 11[CFG] received stroke: initiate 'secret'
Apr 14 13:43:54 debian charon: 04[IKE] initiating IKE_SA secret[1] to 192.168.3.2
Apr 14 13:43:54 debian charon: 04[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
Apr 14 13:43:54 debian charon: 04[NET] sending packet: from 192.168.3.1[500] to 192.168.3.2[500]
Apr 14 13:43:54 debian charon: 03[NET] received packet: from 192.168.3.2[500] to 192.168.3.1[500]
Apr 14 13:43:54 debian charon: 03[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(MULT_AUTH) ]
Apr 14 13:43:54 debian charon: 03[IKE] authentication of '192.168.3.1' (myself) with pre-shared key
Apr 14 13:43:54 debian charon: 03[IKE] establishing CHILD_SA secret
Apr 14 13:43:54 debian charon: 03[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr AUTH SA TSi TSr N(MOBIKE_SUP)
    N(ADD_4_ADDR) N(ADD_4_ADDR) N(MULT_AUTH) N(EAP_ONLY) ]
Apr 14 13:43:54 debian charon: 03[NET] sending packet: from 192.168.3.1[4500] to 192.168.3.2[4500]
Apr 14 13:43:54 debian charon: 02[NET] received packet: from 192.168.3.2[4500] to 192.168.3.1[4500]
Apr 14 13:43:54 debian charon: 02[ENC] parsed IKE_AUTH response 1 [ IDr AUTH SA TSi TSr N(AUTH_LFT) N(MOBIKE_SUP)
    N(ADD_4_ADDR) N(ADD_4_ADDR) ]
Apr 14 13:43:54 debian charon: 02[IKE] authentication of '192.168.3.2' with pre-shared key successful
Apr 14 13:43:54 debian charon: 02[IKE] IKE_SA secret[1] established between 192.168.3.1[192.168.3.1]...192.168.3.2[192.168.3.2]
Apr 14 13:43:54 debian charon: 02[IKE] scheduling reauthentication in 9764s
Apr 14 13:43:54 debian charon: 02[IKE] maximum IKE_SA lifetime 10304s
Apr 14 13:43:54 debian charon: 02[IKE] CHILD_SA secret{1} established with SPIs c52f9e44_i c1e4762b_o and TS 192.168.1.0/24 ===
    192.168.2.0/24
Apr 14 13:43:54 debian charon: 02[IKE] received AUTH_LIFETIME of 9883s, scheduling reauthentication in 9343s
Apr 14 13:43:54 debian charon: 02[IKE] peer supports MOBIKE
```

```
usuario@debian:~$ sudo ipsec status
Security Associations:
      secret[1]: ESTABLISHED 3 minutes ago, 192.168.3.1[192.168.3.1]...192.168.3.2[192.168.3.2]
      secret{1}:  INSTALLED, TUNNEL, ESP SPIs: c52f9e44_i c1e4762b_o
      secret{1}:   192.168.1.0/24 === 192.168.2.0/24
```

Figure 1.1 : Detalles de la conexión.

Como se puede ver en la figura 1.2 hay dos asociaciones de seguridad, una por cada

sentido de la conexión. Almacena la firma y la clave de encriptación.

```
usuario@debian:~$ sudo ip xfrm state
src 192.168.3.1 dst 192.168.3.2
        proto esp spi 0xc1e4762b reqid 1 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha1) 0xd21123af701ac9186be4e154b41408483f476b46 96
        enc cbc(aes) 0xf2bd64876fde6aafa241a51123b77d80
src 192.168.3.2 dst 192.168.3.1
        proto esp spi 0xc52f9e44 reqid 1 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha1) 0x97af662558dd8e405496f5fb3335a022148bebc7 96
        enc cbc(aes) 0x7aba230bc11bf98ccae7ecc9e3cc5807
```

Figure 1.2 : Asociaciones de seguridad.

Hay tres politicas según el paquete.

- Si se retransmite (fwd).
- Si va dirigido a la maquina (in)
- Si lo emite la maquina (out)

Todo el tráfico aplicará la acción PROTECT.

```
usuario@debian:~$ sudo ip xfrm policy
src 192.168.2.0/24 dst 192.168.1.0/24
        dir fwd priority 1859 ptype main
        tmpl src 192.168.3.2 dst 192.168.3.1
                proto esp reqid 1 mode tunnel
src 192.168.2.0/24 dst 192.168.1.0/24
        dir in priority 1859 ptype main
        tmpl src 192.168.3.2 dst 192.168.3.1
                proto esp reqid 1 mode tunnel
src 192.168.1.0/24 dst 192.168.2.0/24
        dir out priority 1859 ptype main
        tmpl src 192.168.3.1 dst 192.168.3.2
                proto esp reqid 1 mode tunnel
```

Figure 1.3 : Políticas de seguridad.

Se han intercambiado 4 paquetes ISAKMP como se puede ver en la figura 1.4 . Esta usando la version 2.0, se puede ver al inspeccionar el paquete (figura 1.5).

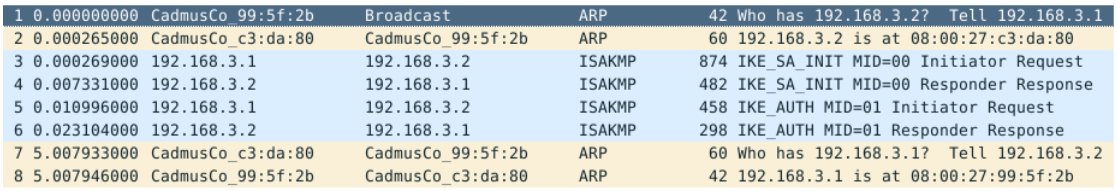

Figure 1.4 : Paquetes ISAKMP capturados.

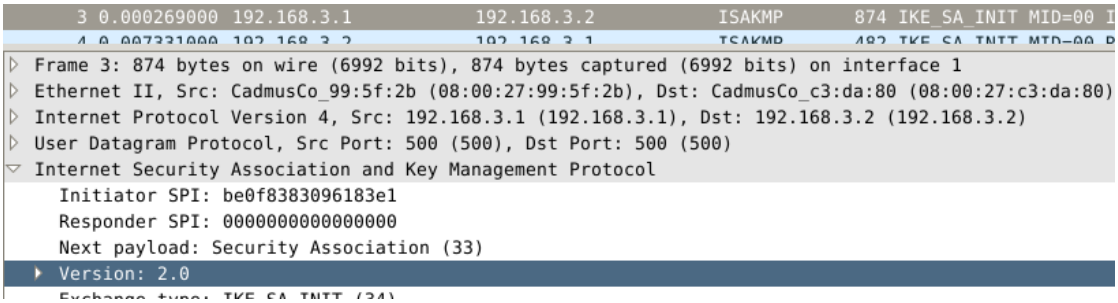

Figure 1.5 : Version ISAKMP.

Si miramos de nuevo la figura 1.5 podemos ver que utiliza User Datagram Protocol (UDP) y el puerto asociado es el 500.

Si inspeccionamos el paquete podemos ver que han acordado usar cbc con aes y que el tamaño de la clave es 128, figura 1.6 .

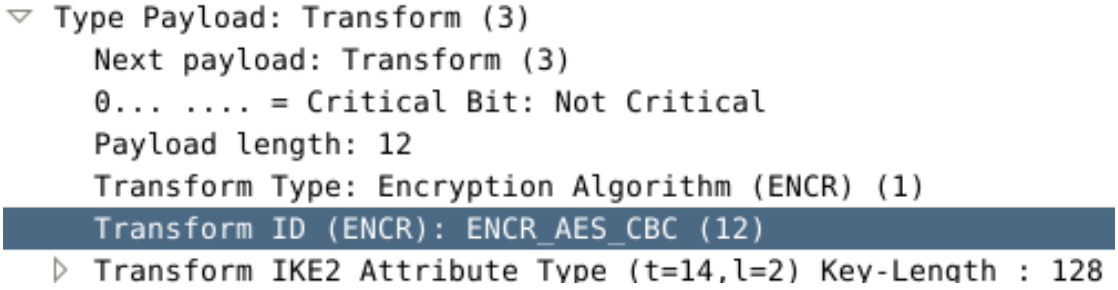

Figure 1.6 : Acuerdo.

Va a usar SHA1, figura 1.7 , con el grupo DH 14(2048 bit modulus), figura 1.8 .

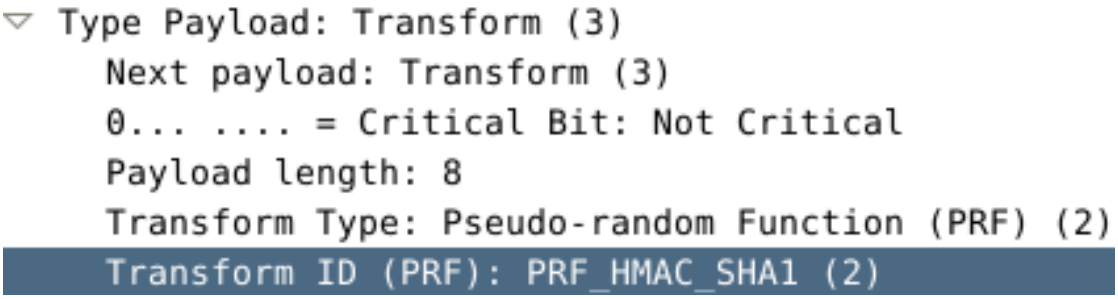

Figure 1.7 : Pseudo Random Function (PRF).

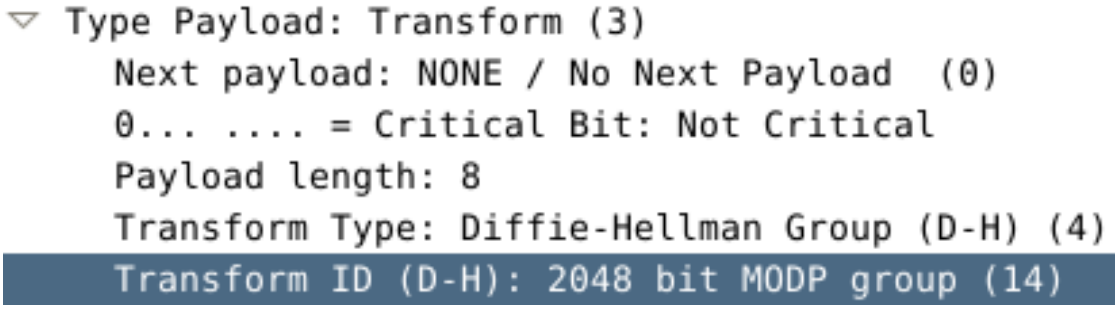

Figure 1.8 : Grupo DH.

El segundo par de mensajes se usan para autenticar ambos extremos, un atacante no puede ver los datos intercambiados porque van cifrados con lo que se ha acordado por ambos extremos en los dos mensajes previos.

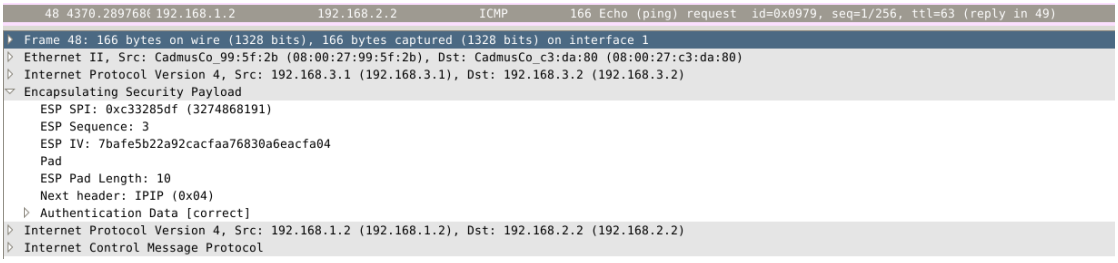

Figure 1.9 : Paquete ESP descifrado.

Como se puede ver en la figura 1.10 no se comparte ni el SPI ni las claves.

Protocol	Src IP	Dest IP	SPI	Encryption	Encryption Key	Authentication	Authentication Key
IPv4	192.168.3.1	192.168.3.2	0xc33285df	AES-CBC [RFC3602]	0xe62a0c3382956c076b72391c2522bbfc	HMAC-SHA-1-96 [RFC2404]	0x4da5eae1061e82baf043c99dd6ab2ad781de79da
IPv4	192.168.3.2	192.168.3.1	0xc4a328ce	AES-CBC [RFC3602]	0x1688d55e1bc93ca752146bf5dd1eeedf	HMAC-SHA-1-96 [RFC2404]	0xb4c97987d515dc0e706e1c2de48d7edffd470be8

Figure 1.10 : Parámetros SAs.

El encapsulado ESP en modo tunel añade una cabecera IP nueva de modo que todo lo

que la siga va firmado, además lo que sigue a la cabecera ESP va también encriptado.

2 Conexión IPsec de sitio a sitio con certificado autofirmado

```
usuario@debian:~$ sudo ipsec statusall
000 Status of IKEv1 pluto daemon (strongSwan 4.5.2):
000 interface lo/lo ::1:500
000 interface lo/lo 127.0.0.1:500
000 interface eth0/eth0 10.0.2.15:500
000 interface eth1/eth1 192.168.1.1:500
000 interface eth2/eth2 192.168.3.1:500
000 %myid = '%any'
000 loaded plugins: test-vectors curl ldap aes des sha1 sha2 md5 random x509 pkcs1 pgp dnskey pem openssl gm
000 debug options: none
000
Status of IKEv2 charon daemon (strongSwan 4.5.2):
  uptime: 120 seconds, since Apr 14 15:21:54 2018
  malloc: sbrk 397312, mmap 0, used 290928, free 106384
  worker threads: 7 idle of 16, job queue load: 0, scheduled events: 3
  loaded plugins: test-vectors curl ldap aes des sha1 sha2 md5 random x509 revocation constraints pubkey pkc
link resolve socket-raw farp stroke updown eap-identity eap-aka eap-md5 eap-gtc eap-mschapv2 eap-radius eap-
Listening IP addresses:
  10.0.2.15
  192.168.1.1
  192.168.3.1
Connections:
      secret:  192.168.3.1...192.168.3.2
      secret:   local:  [192.168.3.1] uses pre-shared key authentication
      secret:   remote: [192.168.3.2] uses pre-shared key authentication
      secret:   child:  192.168.1.0/24 === 192.168.2.0/24
      sscert:  192.168.3.1...192.168.3.2
      sscert:   local:  [CN=gw1] uses public key authentication
      sscert:    cert:  "CN=gw1"
      sscert:   remote: [CN=gw2] uses any authentication
      sscert:    cert:  "CN=gw2"
      sscert:   child:  192.168.1.0/24 === 192.168.2.0/24
Security Associations:
      sscert[1]: ESTABLISHED 79 seconds ago, 192.168.3.1[CN=gw1]...192.168.3.2[CN=gw2]
      sscert[1]: IKE SPIs: 71a5ac908e6bb5d3_i* 1bb6d89abffae4c4_r, public key reauthentication in 2 hours
      sscert[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
      sscert{1}:  INSTALLED, TUNNEL, ESP SPIs: ce610c47_i c22be561_o
      sscert{1}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 42 minutes
      sscert{1}:   192.168.1.0/24 === 192.168.2.0/24
```

Figure 2.1 : sudo ipsec statusall

El establecimiento es igual, solo cambia el método de autenticación.